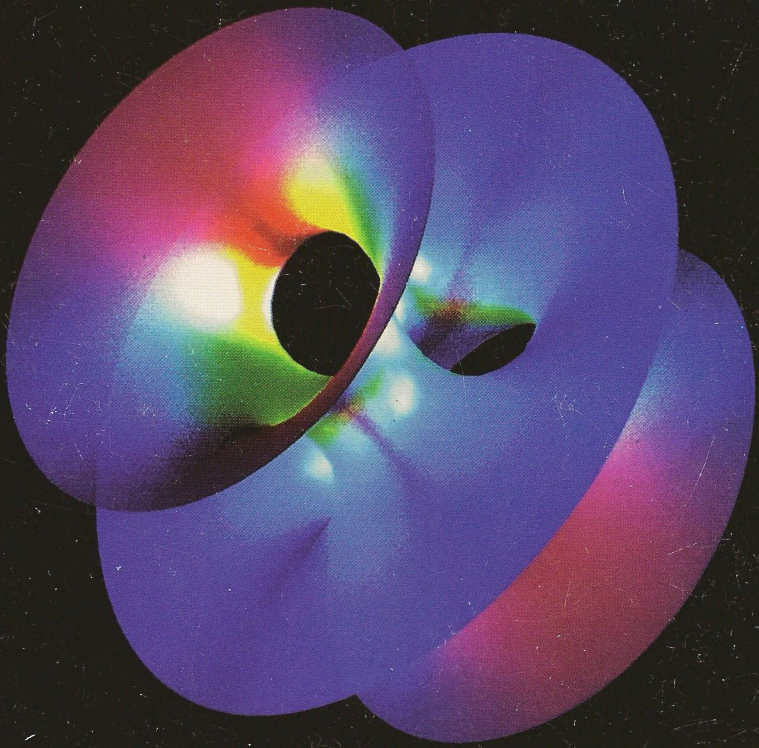
انتشارات
دانشگاه اصفهان
۳۹۶

مقدمه ای بر

جبر مجرد



نوشتهٔ: تی . دبلیو. هانگرفورد

ترجمهٔ: دکتر سعید اعظم
دکتر رضا انشائی

مقدمه‌ای بر

جبر مجرد

تألیف: توماس دبلیو. هنگرفورد

THOMAS W. HUNGERFORD

ترجمهٔ:

دکتر سعید اعظم ـ دکتر رضا انشایی

بسم‌الله‌الرحمن الرحیم

پیشگفتار مترجمان

کتابی که اکنون در پیش روی شماست ترجمه [1] کتاب

"Abstract Algebra, An Introduction"

تألیف T. W. Hungerford است. اعتبار علمی کتاب از حیث منابع علمی و انسجام مطالب آن همچون کتاب جبر این مولف[2] (که برای دوره کارشناسی‌ارشد تدوین شده است و سالهاست در دانشگاههای کشور تدریس می‌شود که از هر حیث دارای اعتبار است) اهمیتی بسزا به آن داده است. این کتاب با نگرشی نو، با پرداختن به حلقه‌ها قبل از گروهها، بین موضوعاتی دیرآشنا (نظیر حساب و جبر چندجمله‌ایها) و جبر مدرن پیوندی مستحکم برقرار می‌کند. ارائه چندین فصل کاربردی به برجستگی کتاب می‌افزاید.

فصول ۱ تا ۸ و بخش‌هایی از فصول ۹ تا ۱۱ را می‌توان برای یک دوره درسی در جبر انتخاب نمود، ترکیبی از فصول ۱۲ تا ۱۶ که سیری در جبر و کاربردهای آن می‌باشد، با مباحث فصل‌های ۱ تا ۷ می‌توانند به یک دورهٔ آموزشی با عنوان جبر کاربردی بخصوص برای گرایش ریاضی کاربردی دانشگاهها مورد استفاده قرار گیرد.

از مساعدت‌های همه‌جانبه حوزه معاونت پژوهشی، اعضای محترم شورای انتشارات دانشگاه و کارکنان چاپخانه دانشگاه کمال تشکر را دارد. از سرکار خانم موری که تایپ کامپیوتری کتاب را بعهده داشته‌اند و آقای محمدباقر سلطانی که در اصلاح کامپیوتری مطالب ما را یاری نموده‌اند، تقدیر و تشکر می‌نماید.

در خاتمه از همه اساتید گرامی و دانشجویانی که کتاب را مطالعه می‌فرمایند استدعا دارد با انتقادات سازنده خود و یادآوری کاستی‌های احتمالی ما را در اصلاح هرچه بهتر کتاب یاری نمایند.

سعید اعظم رضا انشایی

گروه ریاضی دانشگاه اصفهان تیرماه ۱۳۸۰

---

۱) در انتخاب واژه‌های علمی کتاب، "واژه نامه ریاضی و آمار" تألیف انجمن ریاضی ایران با همکاری گروه ریاضی و آمار مرکز نشر دانشگاهی ملاک ترجمه قرار گرفته است.

۲) به [۶] رجوع شود.

پیشگفتار مؤلف

کتاب حاضر به عنوان "اولین درس در جبر مدرن" برای دوره کارشناسی ریاضی تدوین شده است. جبرخطی پیشنیازی برای این درس نمی‌باشد. چون ظرافت ریاضیات موجز اغلب موجب سردرگمی دانشجویان می‌شود، در این کتاب تاکید بر وضوح و در عین حال دقت کافی در مطالب آن می‌باشد. با ارائه مثال‌های گوناگون، مفاهیم به طور کامل توضیح داده شده است. هدف نهایی تهیه کتابی بوده‌است که یک دانشجوی متوسط، با کمترین کمک خارجی قادر به مطالعه آن باشد. در خلال مباحث کتاب بیش از ۱۵۰۰ تمرین که از ساده به مشکل رده‌بندی شده، آمده‌است که دانشجویان را قادر به توسعه مهارت‌های لازم برای کار با ریاضیات می‌نماید. انعطاف‌پذیری طرح کلی کتاب (که به‌طور کامل در قسمت **سخنی با استاد** توضیح داده شده است)، موجب پیدایش دوره‌های درسی مناسب، در سطوح گوناگون ریاضیات عالی با طول زمان‌های متفاوت، گردیده است. از این کتاب می‌توان برای یک دوره درسی در جبر مجرد و یا یک دوره درسی در جبر با نگرش کاربردی، بهره گرفت.

اساساً تجربه قبلی اکثر دانشجویان در دوره پیش‌دانشگاهی در زمینه جبر، عمدتاً با اعداد صحیح، میدان اعداد حقیقی و چندجمله‌ایهای روی اعداد حقیقی می‌باشد. این کتاب با تکیه بر این تجربه، به بحث پیرامون حلقه‌ها، میدان‌ها و چندجمله‌ایها، پیش از گروهها، پرداخته است. در نتیجه، دانشجو می‌تواند بر مبنای موارد آشنا، ارتباط بین جبر دبیرستانی و مفاهیم مجردتر جبر مدرن را بهتر درک کند و آسان‌تر به سطح بالاتری از مجردسازی نایل آید.

اگرچه مؤلف شکی ندارد که پرداختن به حلقه‌ها، قبل از گروهها برای اکثر دانشجویان بهترین کار است، پذیرش این استنتاج برای او نزدیک به ده سال زمان برده است. لذا با اساتیدی که مایل به ترک این سنت که "نظریه گروهها باید ابتدا تدریس شود" نیستند همدردی می‌نماید. اما استدعا دارد که منصفانه به این رویکرد امکان یک تجربه کلاسی بدهند "آزمایش کنید قطعاً دوستش خواهید داشت."

ویژگی‌های برجسته دیگری که این کتاب را ممتاز می‌کند توسعه موضوعی و سازماندهی کلی آن می‌باشد. مباحث اصلی درس (فصول ۸-۱) حول سه موضوع حساب، همنهشتی و ساختارهای مجرد سیر می‌کند. هر کدام از این موضوعات، ابتدا برای اعداد صحیح سپس برای چندجمله‌ایها و سرانجام برای حلقه‌ها و گروهها توسعه یافته است.

این تقسیم‌بندی، دانشجو را قادر می‌سازد تا منشأ پیدایش بسیاری از مفاهیم جبری، چرایی اهمیت آنها، و چگونگی ارتباط آنها با یکدیگر را درک کند. موضوع همنهشتی به‌طور قوی در توسعه مفهوم

حلقه‌های خارج قسمتی مورد تأکید قرار گرفته است. در نتیجه، بجای یک معمای بدون علت، دانشجویان قادرند ایده‌آلها، هم‌مجموعه‌ها و حلقه‌های خارج قسمتی را به‌عنوان تعمیمی طبیعی از مفاهیم آشنا در اعداد صحیح ملاحظه کنند. پرداختن به همنهشتی در دامنه چندجمله‌ای‌ها قبل از حلقه‌های دلخواه، نه تنها باعث ساده‌شدن مسیر بحث نظری می‌گردد، بلکه خیلی زودتر از آنچه متداول است، دست‌یابی به نتایج غیربدیهی روی توسیع‌های میدان را امکان‌پذیر می‌سازد.

برای کمک به دانشجو در دست‌یابی به یک دیدگاه کلی و منسجم، ارتباط مابین قسمت‌ها و مفاهیم اساسی جبر، به دفعات در متن و در **جدول فهرست موضوعی** در صفحه xvii خاطرنشان شده است. خطوط افقیْ جدول نشان می‌دهد که چگونه یک موضوع یا زیرموضوع بخصوص، ابتدا برای اعداد صحیح، سپس برای چندجمله‌ایها و بعد برای حلقه‌ها و گروهها توسعه یافته است. ستون‌های عمودی تأثیر متقابل همه موضوعات را برای یک عنوان بخصوص نشان می‌دهد.

در نسخهٔ نهایی این کتاب از اظهار نظر بسیاری از دانشجویان و ریاضی‌دانانی که نسخه دست‌نویس را مرور یا مورد آزمایش کلاسی قرارداده‌اند بهره برده‌ام. سپاس‌های من به:

Gary D. Crown, Wichita State University,

Richard Grassl, University of New Mexico,

Paul R. Halmos, Santa Clara University,

Robin Hartshorne, University of California, Berkeley,

Peter Jones, Marquette University,

Robert Lax, Louisiana State University,

David Leep, University of Kentucky,

Arthur Lieberman, Cleveland State University,

Steve Monk, University of Washington,

Philip Montgomery, University of Kansas,

Murray Schacher, University of California, Los Angeles,

Daniel B. Shapiro, Ohio State University,

Nick Vaughan, University of North Texas,

Bhushan Wadhwa, Cleveland State University

همچنین مایلم از Ann Melville و Joyce Pluth برای تایپ متخصصانه اولین پیش‌نویس

و کمک صبورانه به من در آموختن "word processing" برای پیش‌نویسهای بعدی تشکر نمایم. یادگیری نرم‌افزار "word"، بدون رایانه‌ای که توسط Georgia Lesh-Laurie، رئیس دانشکده تهیه شد و کمک‌های تکنیکی فراوان همکارم Frank Lozier امکان‌پذیر نبود. بزرگواری آنها موجب قدردانی است. همچنین خوشبختم که از مساعدت Maureen Iannuzzi ،Bob Stern، و بقیه کارکنان Saunders College Pubishing قدردانی نمایم، کارکردن با آنها باعث مسرّت بوده است.

سرانجام، از همسرم، Mary Alice و فرزندانم Anne و Tom، برای بردباری و تفاهم آنها در حین آماده‌سازی کتاب تشکر فراوان می‌نمایم.

T.W.H.

فهرست مطالب

۳) بخشها و فصل‌هایی از قسمت اصلی درس را که علامت * دارند می‌توان حذف و یا به تعویق انداخت. برای جزئیات ابتدای این بخش‌ها را ملاحظه کنید.

۴) Sylow Theorems
۵) Galois Theory

---

۶) Chinese Remainder Theorem

۷) Boolean algebras

۸) Lagrange's Theorem

سخنی با استاد

برای یک دوره آموزشی در جبر مجرد سنتی، می‌توان از **اصل دورهٔ درسی** (فصل‌های ۱ تا ۸) و بخش‌های منتخب از **مباحث پیشرفته** (فصل‌های ۹ تا ۱۱) استفاده کرد. بخش‌ها و فصل‌هایی از **اصل دوره درسی** که در **فهرست مطالب** (صفحه ۷) با علامت "*" مشخص شده‌اند را می‌توان به تعویق انداخت یا در صورت کوتاه بودن طول دوره درسی حذف کرد؛ برای دیدن جزئیات، مقدمه این بخش‌ها را ملاحظه کنید.

برای یک دوره آموزشی با نگرش کاربردی‌تر، می‌توان تقریباً همهٔ مباحث **سیری در جبر و کاربردهای آن** فصل‌های (۱۲ تا ۱۶) را در خلال مباحث فصل‌های ۱ تا ۷ گنجاند، حتی می‌توان این کار را از فصل ۲ آغاز نمود. برای دیدن جزئیات بیشتر، **فهرست مطالب** و **جدول ارتباط متقابل فصل‌ها** را ملاحظه فرمایید. اطلاعات زیر می‌تواند شما را در برنامه‌ریزی دوره‌های متنوع آموزشی برحسب طول دوره و میزان تعالی موضوعات آنها یاری نماید.

مقدمات و پیشنیازها: در پیوست‌های الف–ت مطالب مقدماتی عادی آمده است. بسته به وضعیت کلاس، این پیوست‌ها را می‌توان به عنوان فصل صفر آموزش داد، یا در جای دیگری معرفی کرد و یا به طور کلی از آن‌ها صرف‌نظر کرد. حال به چند عنوان از پیوست‌ها می‌پردازیم:

پیوست الف (منطق و برهان) این پیوست پیشنیازی برای هر درس جبر مجرد می‌باشد ولی مرسوم نیست که به عنوان یک بخش اصلی تدریس شود.

پیوست ب (مجموعه‌ها و توابع) قسمت اوّل این پیوست (اصطلاحات اولیه) از همان ابتدای کتاب مورد نیاز است و احتمالاً بیشتر دانشجویان با مطالب آن آشنایی دارند.

پیوست پ (استقراء) اصلی که به‌نام اصل استقراء کامل ریاضی معروف است نخستین بار در بخش ۱.۴، مورد استفاده قرار می‌گیرد؛ استقراء معمولی اولین بار در بخش ۴.۴ ظاهر می‌شود. هم‌ارزی اصل استقراء و اصل خوش‌ترتیبی (قضیه پ.۴) در هیچ کجای کتاب مورد نیاز نیست.

پیوست ت (رابطه هم‌ارزی) بر مبنای ترجیح شخصی مؤلف کتاب، مثال‌های مهم مربوط به هم‌ارزی (بخش‌های ۱.۲، ۱.۵، ۱.۶ و ۵.۷) قبل از تعریف رسمی رابطه هم‌ارزی ارائه شده است. بنابراین نیازی به تدریس پیوست ت، تا قبل از بخش ۴.۸ نیست.

در صورت تمایل ابتدا رابطه هم‌ارزی را تعریف کرده سپس مثال‌های مهم را به‌عنوان حالت خاصی از آن در نظر بگیرید. بهتر است پیوست ت را قبل از بخش ۱.۲ تدریس کنید، و سپس برهان‌های موردی در بخش‌های فهرست شده بالا را نادیده بگیرید.

مطالب تکمیلی چند موضوع که مناسب متن اصلی کتاب نیستند در پیوست‌های ث – چ آمده‌است.

پیوست ث (قضیه دوجمله‌ای) گرچه که این قضیه تنها در بخش ۶.۹ و تعدادی از تمرین‌های دیگر مورد نیاز است، امّا موضوعی است که به مبحث حساب حلقه‌ها مربوط می‌شود (بخش ۲.۳، مثال ۱۸.۳).

پیوست ج (جبر ماتریسی) مطالب این پیوست پیشنیاز فصل ۱۶ می‌باشد امّا می‌توان آن را برای دانشجویانی که درس جبر خطی را گذرانده‌اند حذف کرد. البته مطالب این پیوست را می‌توان برای ارائه مثال‌های اضافی برای حلقه‌های ناجابجایی در فصل ۳ بکار برد.

پیوست چ (چندجمله‌ایها) تعریف رسمی چندجمله‌ایها و نامعین‌ها (عناصر مجهول) در این پیوست ارائه شده است. همانگونه که در بخش ۱.۴ تذکر داده می‌شود، در صورت تمایل می‌توانید این پیوست را در بخش ۱.۴ بگنجانید.

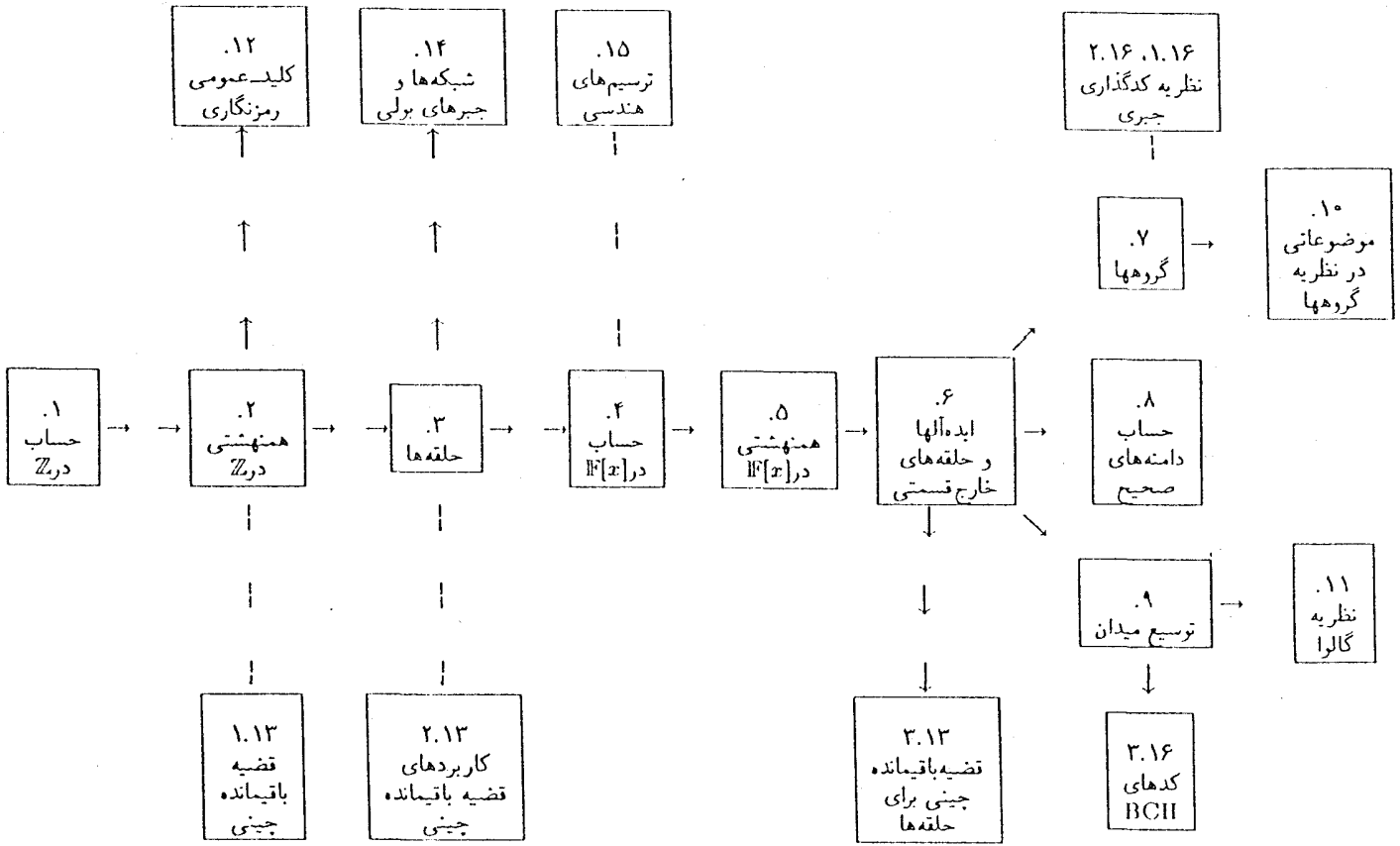
تمرین‌ها تمرین‌های دسته A شامل محاسبات معمولی و مسائلی با برهان‌های سر راست می‌باشد. حل تمرین‌های دسته B نیازمند کمی تعمق است، امّا حل قسمت عمده‌ای از این مسائل برای اکثر دانشجویان مقدور می‌باشد. دسته C شامل تمرین‌های مشکل است.

هرکجا که امکان داشته است، تمرین‌های هر دسته برحسب موضوع مربوط به آن‌ها در متن کتاب، مرتب شده است. در نتیجه پاره‌ای از تمرین‌های نسبتاً ساده در دسته‌های A یا B ممکن است در انتهای دسته ظاهر شود.

برای تقریباً نیمی از تمرین‌های فرد، راه‌حل و پیشنهادهایی در پایان کتاب ارائه شده است. راه‌حل بقیه تمرین‌ها در **راهنمای استاد** آمده است. این راهنما توسط Daniel B. Shapiro تهیه شده و می‌توان آن را از طریق انتشارات Sanders College Publishing بدست آورد.

ارتباط متقابل فصل‌ها و بخش‌ها: بجز در مواردی که در مقدمه هر فصل بیان شده است، هر بخش به بخش قبلی آن در فصل مربوطه وابسته است. در جدول صفحه بعد ارتباط متقابل فصل‌ها آمده‌است، که در آن نماد $B \longrightarrow A$ به معنی آن است که فصل A پیشنیاز فصل B است. یک فلش منقطع $B \dashrightarrow A$ مبین وابستگی فصل B به تنها قسمت‌هایی از فصل A است؛ فهرست موضوعی در صفحه xvii را برای جزئیات بیشتر ملاحظه کنید. در جدول یادشده فصل‌های ۱۳ و ۱۶ به چند قسمت دیگر تقسیم شده‌است.

ارتباط متقابل فصلها



سخنی با دانشجو

نظری اجمالی:

این کتاب با مطالبی که شما قبلاً آنها را دیده‌اید؛ حساب دوره راهنمایی و جبر چندجمله‌ایها از دبیرستان آغاز می‌شود. آنگاه این موضوعات دیرآشنا در چهارچوبی عام‌تر که در واقع حالت‌های خاصی از ساختارهای جبری مجرد می‌باشد، قرار می‌گیرد.

این کتاب حول موضوعاتی متنوع تنظیم گردیده است، تا خواننده بتواند غایت آنچه مباحث گوناگون را به یکدیگر پیوند می‌زند، به طور منسجم درک کند. در اینجا شرحی مختصر از سه موضوع مهم در ارتباط با هشت فصل اول کتاب آمده است:

حساب. خواهید دید که خواص دیرآشنای اعداد صحیح مانند تقسیم، باقیمانده‌ها، تجزیه، و اعداد اول به چندجمله‌ایها و پس از آن به دستگاههای جبری کلی‌تر منتقل می‌شود.

همنهشتی. همنهشتی اعداد صحیح ممکن است از "حساب ساعت دیواری" برایتان آشنا باشد[۹].

برهان‌ها. در این دوره درسی، تاکید بر دقت زیاد مطالب و توسعه منطقی آنها، بیش از آنچه در جبر دبیرستانی آمده است، خواهد بود. اگر شما یکی از آن خیل عظیم دانشجویانی باشید که آشنایی چندانی با منطق ریاضی و خواندن و نوشتن برهان‌ها ندارید، باید از خواندن پیوست الف شروع کنید. این پیوست قواعد اساسی منطق و فنون برهان را که در سراسر این کتاب مورد استفاده قرار گرفته است به اختصار برایتان بیان می‌کند.

قبل از این که به تمرین‌ها نگاه کنید، در حالی که قلم و کاغذ در دست دارید کتاب را بخوانید. وقتی که صورت یک قضیه را خواندید، مطمئن شوید که معانی جملات آن را فهمیده‌اید. برای مثال، اگر این قضیه اظهار می‌دارد که "هر دامنه صحیح متناهی یک میدان است"، تعاریف "دامنه صحیح" و "میدان" را، اگر لازم باشد، دوره کنید. از فهرست مندرجات برای یافتن تعریف‌ها استفاده کنید.

پس از اطمینان از درک صورت قضیه، به برهان آن رجوع کنید. بخاطر داشته باشید که: تفاوت بسیار زیادی بین فهمیدن برهان یک قضیه کتاب و برهانی که برای خودتان اقامه می‌کنید وجود دارد. درست همان‌طور که شما بی‌آنکه یک مهندس معماری باشید یک ساختمان جدید را تایید و تمجید

۹) در یک ساعت دیواری وقتی عقربه ساعت شمار ۳ ساعت یا ۱۵ ساعت از ۱۲ بگذرد، این عقربه دقیقاً به یک محل می‌رسد. از اینرو ۱۵ = ۳، به طور مشابه ۱۲ = ۰. اگر عقربه ساعت‌شمار از ۱۲ آغاز به حرکت کرده، ۸ ساعت جلو رفته، آنگاه ۹ ساعت دیگر حرکت نماید، به ساعت ۵ می‌رسد؛ بنابراین در این ساعت دیواری ۵ = ۹ + ۸.

می‌کنید می‌توانید صحت برهان‌هایی را که توسط دیگران ارائه شده است بررسی کنید اگرچه نتوانید درک کنید که این برهان‌ها را چگونه در ابتدای کار به این صورت اقامه کرده‌اند.

از برهان شروع کرده، به سرعت از آن عبور کنید، بی‌آن که نگران مشروح مطالب در هر مرحله اثبات باشید، تا از آن ایده‌ای بدست آورید. اگر شما تقریباً بدانید که استدلال یک قضیه از کجا نشأت گرفته است فهم آن ساده‌تر خواهدبود. آنگاه به ابتدای برهان برگشته و به‌دقت آن را جمله به جمله بخوانید. اگر اظهار می‌دارد که طبق قضیه ۱۸.۵ چنین و چنان مطلب درست است بررسی کنید تا آنچه را قضیه ۱۸.۵ می‌گوید دیده و مطمئن شوید که آنچه را از آن فهمیده‌اید در اینجا بکار می‌آید. اگر در فهم مطلبی گیر کرده‌اید آن را بطور موقت قبول کرده، بقیه قضیه را تمام کنید. آنگاه برگشته و مشکلات مطلبی را که در آن گیر کرده‌اید ارزیابی کنید. وقتی که حقیقتاً گیر کرده‌اید، از استاد خود سوال کنید. استاد به سوالاتی که از تلاش مجدانه شما بدست آمده است پاسخ مثبت خواهد داد.

تمرین‌ها ریاضیات یک ورزش دیدنی نیست. شما نمی‌توانید ریاضیات را فراگیرید بی آنکه با ریاضیات کار کنید، تا خود را به آب نزنید قادر به شنای در آن نیستید. بدین دلیل است که تعداد زیادی تمرین در این کتاب آمده است.

تمرین‌های گروه A معمولاً ساده هستند. اگر نمی‌توانید که تمام آنها را حل کنید، در حقیقت مطلب را نفهمیده‌اید. تمرین‌های گروه B اغلب و منطقاً به مقدار قابل توجهی تفکر نیاز دارد و برای بیشتر ما با چند آزمون و خطا همراه خواهد بود. ولی اکثریت آنها در حیطه فهم شماست. تمرین‌های گروه C معمولاً مشکل هستند که آزمون خوبی برای دانشجویان با استعداد می‌باشد.

در بسیاری از تمرین‌ها از شما سوال خواهد شد که چیزی را ثابت کنید. اگر با خواندن برهان‌های دیگران مهارت خود را زیاد کرده باشید (همان‌گونه که در بالا اشاره شد) در خواهید یافت که اقامه برهان برایتان ساده‌تر خواهد بود. فنون برهان ارائه شده در پیوست الف هم می‌تواند مفید باشد. جواب‌های (یا راهنمایی‌های) تقریباً نیمی از تمرین‌ها در پایان این کتاب ارائه شده است.

گرایش‌های مختلف جبر به طرق متعددی با یکدیگر ارتباط پیدا می‌کنند که برای افراد تازه‌کار و یا حتی با تجربه‌کاری زیاد نیز ممکن است چندان روشن نباشد. بنابراین تعجب‌آور نخواهد بود که دانشجویان اغلب در درک ارتباط بین مباحث دچار مشکل باشند. بخاطر سپردن سه موضوعی که در بالا به آن اشاره شد، به ویژه توسط شما، مفید خواهد بود.

صفحه	سطر	غلط	صحیح
۳	۴-	خارج قسمت	همان خارج قسمت
۱۸	۳	$(a_۲a_۴\dots$	$(a_۳a_۴\dots$
۴۲	۹	$\oplus$ و	$\oplus([b]\odot[c])$ و
۴۲	۱۰	$([b]\odot[c])$	حذف شود
۴۶	۱۲	$[p]$	$[a]$
۴۶	۴-	شمارندهای	شمارندهای
۵۷	۱	$\mathbb{R}$	R
۶۲	تمرین ۸	$S=\{f\in T\mid$	$S=\{f\in T\mid f(۲)=۰\}$
۶۶	تمرین ۳۹	$\{r,۲r,۳r,\dots$	$\{۰,r,۲r,۳r,\dots$
۷۵	تمرین ۵	$AX=B$ در	$AX=B$ و
۸۱	۳	باشد	باشد.
۸۲	۱۱	$=۱$	$=۱۱$
۸۴	سطر آخر	$=۱_R$	$=۱_S$
۸۶	۹	$[b_{۱۲}]$	$[b]_{۱۲}$
۸۸	تمرین ۶	کیند	کنید
۹۰	سطر ۱ تمرین ۲۲	نشان دهید	فرض کنید $n\equiv ۱\ (m$ (پیمانه $)$. نشان دهید
۹۰	سطر ۲ تمرین ۲۲	پوشا	یک به یک
۹۰	سطر ۳ تمرین ۲۲	۱.۴	۱۴
۹۰	سطر ۱ تمرین ۲۴	همریختی	یکریختی
۹۲	تمرین ۳۴	$([a_m],[a_n])$	$([a]_m,[a]_n)$
۹۲	تمرین ۳۴ (ب)	اثبات مثال بعد از قضیه ۱۰.۳	استدلال مثال ۲۴.۳
۹۵	۲ (پاورقی)	پ	چ
۹۸	۳-	چندجملهایهای	چندجملهای‌های یکتای
۱۰۰	۴	$q(x)=b^{-۱}$	$q(x)=b^{-۱}a$
۱۰۰	۵-	$f(x)=a_nb_m^{-۱}x^{n-m}$	$f(x)-a_nb_m^{-۱}x^{n-m}g(x)$
۱۰۱	۱۴	یکی بیشتر یا برابر	عددی بزرگتر یا مساوی
۱۰۳	تمرین ۱۳	$+a_۱x+$	$a_۰+a_۱x+$
۱۰۳	سطر ۲ تمرین ۱۴	$f(x)$ در R	$g(x)$ در R
۱۰۹	سطر ۲ تمرین ۷	نشان دهید $g(x)$	نشان دهید $f(x)$
۱۱۱	۵	قضیه ۷.۵	قضیه ۷.۴
۱۱۲	۱۸	$r(x)\mid p(x)$	$p(x)\mid r(x)$
۱۱۴	تمرین ۸	غیرصفر	غیرثابت

صفحه	سطر	غلط	صحیح
۱۱۵	سطر ۲ تمرین ۱۶	و یا	یا
۱۱۷	۷	$\mathbb{Z}_۳(x)$	$\mathbb{Z}_۳[x]$
۱۲۰	۲−	$\mathbb{F}$ دارای	$f(x)$ دارای
۱۲۰	۱−	$\mathbb{F}$ دارای	$f(x)$ دارای
۱۲۲	تمرین ۷	$\ldots(x-۳)(x-۵)\ldots$	$\ldots(x-۳)(x-۴)(x-۵)\ldots$
۱۲۵	۱۲	${}^{۸}\mathbb{Q}[x]^*$	${}^{۸}\mathbb{Q}[x]$
۱۲۶	پاورقی	عدد گویا را	عدد گویای ناصفر
۱۲۷	لم ۱۷.۴	$f(x), s(x)$	$f(x), g(x)$
۱۲۸	۸	$g(x)b(x)$	$g(x)h(x)$
۱۲۹	۱	بنابراین $=$	بنابراین $=[pk(x)][dh(x)]$
۱۲۹	۲	$[pk(x)][dh(x)]$	حذف شود
۱۲۹	۱۰	تست گویا	ریشه گویا
۱۲۹	۱۶	$۲x$	cx
۱۳۴	تمرین ۱۵	$p(x)=$	$f(x)=$
۱۴۳	۶−	$\mathbb{F}[x]$	$\mathbb{R}[x]$
۱۵۳	۴−	یکه	تکین
۱۵۴	۸−	$\mathbb{Z}_۲[x]/(x^۲+x+۱)$	$\mathbb{K}=\mathbb{Z}_۲[x]/(x^۲+x+۱)$
۱۵۵	۵	میدان توسیع	توسیع میدان
۱۵۵	۷	است.	است. گیریم $p(x)=a_n x^n+\cdots+a_۱x+a_۰$ که در آن $a_i\in\mathbb{F}$ و از این رو در $\mathbb{K}$ است.
۱۶۰	۴−	$\mathbb{Q}$	$\mathbb{Q}[x]$
۱۸۴	۱−	یکدار	و یکدار R
۱۸۵	۷	مسقوم	مقسوم
۱۸۹	۱۱	مجموعه یکه‌های	مجموعه غیر یکه‌های
۱۸۹	۶−	در R است	در R نیست
۲۰۶	ردیف ۲ جدول تمرین ۲۷	$a \mid b\ a$	$a \mid a\ a$
۲۳۳	سطر ۱ تمرین ۱۲	$G\cong H_۱$	$G\cong G_۱$
۲۳۶	تمرین ۴۲	$\mathbb{Z}_۲\times\mathbb{Z}$	$\mathbb{Z}_۲\times\mathbb{Z}_۲$
۲۴۶	تمرین ۲۹ (ب)	اگر K یک ... $N_H\subseteq K$.	اگر H زیرگروه نرمالی از یک زیرگروه K از G باشد، آنگاه $K\subseteq N_H$.
۲۴۸	۹−	مقال	مثال

صفحه	سطر	غلط	صحیح
۲۴۸	۶−	یا N_v	یا در N_v
۲۴۸	۶−	متمایز و یا برابر	یا مجزا و یا برابرند (نتیجه ۱۹.۷)، هر هم مجموعه N باید برابر
۲۴۸	۴−	$v \circ v = r$	$v \circ v = r_0$
۲۵۱	تمرین ۶	$U_{۲۳}$	$U_{۳۲}$
۲۵۵	۳−	$\mathbb{R}^* \to \mathbb{R}^{**}$	$\mathbb{C}^* \to \mathbb{R}^{**}$
۲۵۵	۳−	$\mathbb{R}^*$	$\mathbb{C}^*$
۲۷۲	سطر ۶−	کمتر	کمتر یا مساوی
۲۹۸	تمرین ۱۶ (ب)	تحویل‌ناپذیر	تحویل‌پذیر
۳۱۶	۱۱	امکان‌پذیر	ممکن
۳۴۹	تمرین ۳	مستقل	وابسته
۳۵۸	تمرین ۳	$c \in \mathbb{F}$ و $0 \neq u \in \mathbb{K}$	$0 \neq c \in \mathbb{F}$ و $u \in \mathbb{K}$
۳۶۰	۲−	$0 \leq i \leq j$	$0 \leq i < j$
۳۷۱	۱۲	ریشه	ریشه در $\mathbb{K}$
۴۰۱	۱۰	$b_۲b_۲$	$a_۲b_۲$
۴۵۰	۱۲	بعد متناهی	مولد متناهی
۴۵۰	۱۳	بعد متناهی	مولد متناهی
۴۷۷	۵	$n \mid (b^{ed-b})$	$n \mid (b^{ed} - b)$
۴۷۷	۸	(پیمانه n)	$c \equiv r$ (پیمانه n)
۴۷۷	۹	$c \equiv r$	حذف شود
۴۷۸	۲−	ادلمان	ادلمن
۴۸۲	۱۶	داشته باشد	باشد
۵۰۲	۱۵	$b \leq a$	$b \geq a$
۵۰۲	۱۶	$a \geq b$	$a \leq b$
۵۰۶	۲−	ایدالهای	ایده‌الهای
۵۰۸	۲	باشد	باید
۵۰۸	۱۲	$(a \vee b)$ است	$(a \wedge b)$
۵۰۸	۱۷	$(a \vee b)$	$(a \wedge b)$
۵۱۱	تمرین ۱۶	$a, b \in L$	$a, b, c \in L$
۵۱۲	تمرین ۱۸	مجموعه ناتهی	مجموعه‌ای ناتهی
۵۱۳	تمرین ۲۵	B	S
۵۱۹	۶	یک تعریف	تعریفی از
۵۲۱	۴	$a \vee (b \vee a') \wedge I$	$a \vee ((b \vee a') \wedge I)$
۵۲۱	۶−	جبر بولی	جبر بولی C, B
۵۲۹	تمرین ۳۴	۱۰_۱۴	۱۰.۱۴
۵۳۶	۴−	$ab + ab$	$ab + ac$

فصل اول

بازنگری حساب در $\mathbb{Z}$

علم جبر ناشی از علم حساب است و بستگی زیادی به آن دارد. بنابراین ما مطالعه خود در جبر مجرد را با مروری بر حقایقی از حساب آغاز می‌کنیم که کراراً در ادامه این کتاب استفاده شده است و الگویی برای بیشتر کارهایی که انجام می‌دهیم فراهم می‌آورد. تأکید اصلی ما به جای روشهای محاسبه، بر روی الگوها و خواص زیربنایی می‌باشد. با این‌حال مفاهیم بنیادی همان‌هایی هستند که قبلاً با آنها آشنا هستید.

۱-۱ الگوریتم تقسیم

سرآغاز سخن ما مجموعه اعداد صحیح $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ می‌باشد. فرض ما بر این است که شما با حساب اعداد صحیح و با رابطه ترتیبی معمولی ($<$) روی مجموعه $\mathbb{Z}$ آشنا هستید. همچنین

اصل زیر را فرض می‌کنیم:

اصل خوش ترتیبی. هر زیرمجموعه غیرتهی از مجموعه اعداد صحیح غیرمنفی شامل یک کوچکترین عضو است.

اگر اعداد صحیح غیرمنفی را روی خط معمولی اعداد در نظر بگیرید، شهوداً پذیرفتنی است که هر زیرمجموعه آن شامل عنصری است که در طرف چپ همه اعضای آن قرار می‌گیرد، این همان کوچکترین عضو است. از طرف دیگر اصل خوش‌ترتیبی در مجموعه اعداد صحیح $\mathbb{Z}$ برقرار نیست (کوچکترین عدد صحیح منفی وجود ندارد). همچنین این اصل در مجموعه اعداد گویای غیرمنفی نیز برقرار نیست (زیرمجموعه همه اعداد گویای مثبت شامل کوچکترین عضو نیست زیرا، برای هر عدد گویای مثبت r، همواره یک عدد گویای مثبت کوچکتر وجود دارد، برای مثال $r/۲$).

مسئله تقسیم زیر با کلیه مراحل آن را در نظر بگیرید:

مقسوم‌علیه	۳۱	۴۵۰۹	مقسوم		
خارج‌قسمت	۱۴۵	۳۱			
		۱۴۰			
		۱۲۴			
		۱۶۹			
		۱۵۵			
باقیمانده		۱۴			

×	۱۴۵	خارج قسمت	
	۳۱	مقسوم‌علیه	
	۱۴۵		
	۴۳۵		
+	۴۴۹۵		
	۱۴	باقیمانده	
	۴۵۰۹	مقسوم	

فرآیند تقسیم زمانی متوقف می‌شود که ما به یک باقیمانده که از مقسوم‌علیه کوچکتر است برسیم. همه حقایق اساسی در مورد فرآیند تقسیم در روند آزمون منظور شده‌اند که می‌توان آن را به صورت زیر خلاصه کرد:

(باقیمانده) + (خارج قسمت) (مقسوم‌علیه) = مقسوم

بیانی رسمی از این ایده در قضیه زیر آمده است که در آن مقسوم با a، مقسوم‌علیه با b، خارج قسمت با q و باقیمانده با r نشان داده شده است:

۱.۱ قضیه (الگوریتم تقسیم). فرض کنید a و b اعداد صحیح باشند با $b > ۰$. در این صورت اعداد صحیح یکتای q و r موجودند به‌طوری که

$$a = bq + r \qquad \text{و} \qquad ۰ \leq r < b \quad .$$

این قضیه امکان منفی‌بودن مقسوم a را بیان می‌کند. این یک علت وجود این گزاره اضافی در صورت قضیه است که خارج قسمت q و باقیماندهٔ r یکتا است. در دبیرستان ایده این‌که یک مسئله تقسیم ممکن است بیشتر از یک جواب صحیح داشته باشد هرگز مطرح نمی‌شود، امّا در اینجا بدون اعمال برخی محدودیتها روی باقیمانده چنین نتیجه‌ای کاملاً محتمل است. الزام این‌که باقیماندهٔ r کمتر از مقسوم‌علیه b باشد به تنهایی یک خارج قسمت یا باقیماندهٔ یکتا را تضمین نمی‌کند. برای مثال اگر $a = -۱۴$ و $b = ۳$، در این صورت برای q و r دو امکان زیر وجود دارد:

$$-۱۴ = ۳(-۴) - ۲ \qquad : q = -۴, \quad r = -۲ \qquad \text{با} \quad -۲ < ۳$$

و

$$-۱۴ = ۳(-۵) + ۱ \qquad : q = -۵, \quad r = ۱ \qquad \text{با} \quad ۱ < ۳ \quad .$$

وقتی باقیمانده r نیز ملزم به غیرمنفی‌بودن شود (همانند قضیه)، در این صورت همچنان که در برهان نشان داده خواهد شد ما خاصیت یکتایی را داریم.

ایده اساسی نهفته در برهان قضیه ۱.۱ این است که تقسیم در واقع چیزی جز تفریق مکّرر نیست. به عنوان مثال همانگونه که قبلاً دیده شد، اولین قدم در تقسیم ۴۵۰۹ بر ۳۱ معادل تفریق زیر می‌باشد:

$$۴۵۰۹ - ۳۱ \times ۱۰۰ = ۴۵۰۹ - ۳۱۰۰ = ۱۴۰۹.$$

(این قدم با قراردادن یک ۱ در مکان صدگان خارج قسمت و «پائین آوردن» یک صفر از مقسوم به اختصار به‌صورت ۱۴ = ۳۱ – ۴۵ نوشته شده است.) به‌طور مشابه قدم دوّم عبارت است از تفریق

$$۱۴۰۹ - ۳۱ \times ۴۰ = ۱۴۰۹ - ۱۲۴۰ = ۱۶۹$$

و قراردادن یک ۴ در مکان دهگان خارج قسمت. با ادامه این تفریق‌ها به یک عدد غیرمنفی کمتر از ۳۱ (در این حالت ۱۴) می‌رسید. این عدد باقیمانده است، و تعداد مضارب ۳۱ (یعنی ۱۴۵) که تفریق شد خارج قسمت است. بنابراین تقسیم در واقع این تفریق است:

$$۴۵۰۹ - ۳۱ \times ۱۴۵ = ۱۴.$$

در برهان قضیه، جایی که a به b تقسیم می‌شود، ما مضاربی از b را از a تفریق می‌کنیم. به عبارت دیگر، ما تعداد $a - bx$ هایی را در نظر می‌گیریم که در آن x یک عدد صحیح می‌باشد (در

مثال بالا اینها اعداد $۳۱x - ۴۵۰۹$ برای انواع x بودند). کوچکترین چنین عدد غیرمنفی باقیمانده است؛ مقدار x متناظر خارج قسمت می‌باشد.

برهان قضیه ۱.۱[۱]. فرض کنید a و b اعداد صحیح ثابتی باشند با $b \neq ۰$. همهٔ اعداد صحیح به صورت $a - bx$، که در آن $x \in \mathbb{Z}$ را در نظر بگیرید. ابتدا نشان می‌دهیم که برخی از این اعداد صحیح باید غیرمنفی باشند. دو احتمال زیر وجود دارد،

۱ـ اگر $a \geq ۰$، در این صورت $a - b \times ۰ = a \geq ۰$. بنابراین در این حالت $a - bx$ برای $x = ۰$ غیرمنفی است.

۲ـ اگر $a < ۰$، در این صورت $-a > ۰$. چون b یک عدد صحیح مثبت است، باید $b \geq ۱$. ضرب این نابرابری آخر در عدد مثبت $-a$ نشان می‌دهد که $b(-a) \geq -a$، یا به‌طور معادل، $a - ba \geq ۰$. بنابراین در این حالت وقتی $x = a$، $a - bx$ غیرمنفی است.

بنابراین مجموعهٔ S متشکل از همهٔ اعداد صحیح غیرمنفی به صورت $a - bx$، با $x \in \mathbb{Z}$، غیرتهی است.

به‌موجب اصل خوش‌ترتیبی S شامل یک کوچکترین عضو است ـ آن را r بنامید. چون $r \in S$، r به صورت $a - bx$ برای برخی x، مثلاً $x = q$ می‌باشد. بنابراین ما اعداد صحیح q و r را چنان یافته‌ایم که $r = a - bq$، یا به‌طور معادل $a = bq + r$. چون $r \in S$، می‌دانیم که $r \geq ۰$. حال نشان می‌دهیم $r < b$. به خلاف فرض کنید که $r \geq b$. در این صورت $r - b \geq ۰$، لذا

$$۰ \leq r - b = (a - bq) - b = a - b(q + ۱).$$

چون $a - b(q + ۱)$ غیرمنفی است به موجب تعریف عضوی از S می‌باشد. اما چون b مثبت است، یقیناً نابرابری $r - b < r$ درست است. بنابراین

$$a - b(q + ۱) = r - b < r.$$

این نابرابری آخر بیان می‌کند که $a - b(q + ۱)$، که عضوی از S است، کمتر از r، که کوچکترین عضو S است می‌باشد. این یک تناقض است. پس باید داشته باشیم $r < b$. بنابراین ما اعداد صحیح q و r را چنان یافته‌ایم که $a = bq + r$ و $۰ \leq r < b$.

۱) در پیوست پ، با استفاده از استقراء، اثبات دیگری برای قسمتی از این قضیه آمده است.

برای تکمیل برهان باید نشان دهیم که q و r تنها اعداد ممکن با این خاصیت هستند. (این معنای «یکتایی» در صورت قضیه است). برای انجام این کار، فرض می‌کنیم که برای برخی اعداد q_1 و r_1 نیز داریم $a = bq_1 + r_1$، با $0 \leq r_1 < b$. سپس ثابت می‌کنیم که $q = q_1$ و $r = r_1$.

در هر حال $r \geq r_1$ یا $r_1 \geq r$؛ مثلاً $r_1 \geq r$. با استفاده از تفریق داریم

$$\begin{aligned} a &= bq + r \\ a &= bq_1 + r_1 \\ \hline 0 &= bq - bq_1 + r - r_1 \\ bq_1 - bq &= r - r_1 \\ b(q_1 - q) &= r - r_1. \end{aligned}$$

معادلهٔ آخر بیان می‌کند که $r - r_1$ مضرب صحیحی از b است. اما $b > 0$ و $r - r_1 \geq 0$ (چون $r \geq r_1$)، و لذا $q_1 - q$ باید یک عدد صحیح غیرمنفی باشد. بنابراین $r - r_1$ یکی از اعداد $0b$، $1b$، $2b$ و غیره می‌باشد. اما $0 \leq r_1 \leq r < b$، بنابراین تفاضل $r - r_1$ نیز اکیداً کوچکتر از b است. چون $0b < 2b < 3b < \cdots$، تنها امکان این است که $r - r_1 = 0b = 0$. بنابراین $r = r_1$. سرانجام، چون $b(q_1 - q) = r - r_1 = 0$ و $b > 0$، باید داشته باشیم $q - q_1 = 0$، بنابراین $q = q_1$.

استدلالی مشابه، با تعویض نقش r و r_1، یکتایی q و r در حالت $r_1 \geq r$ را ثابت کرده و برهان را کامل می‌کند. ■ [۲]

گونه‌ای از الگوریتم تقسیم که در آن مقسوم‌علیه منفی است نیز برقرار می‌باشد:

نتیجه ۲.۱. فرض کنید a و c اعداد صحیح باشند با $c \neq 0$. در این صورت اعداد صحیح یکتای q و r وجود دارند به قسمی که

$$a = cq + r \quad \text{و} \quad 0 \leq r < |c|.$$

برهان. تمرین ۳. ■

۲) نماد ■ معرف پایان یک برهان است.

تمرینها

۱.A. خارج قسمت و باقیمانده تقسیم a بر b را بدست آورید:

(الف) $a = ۳۰۲$، $b = ۱۹$ (ت) $a = ۲۰۰۰$، $b = ۱۷$

(ب) $a = -۳۰۲$، $b = ۱۹$ (ث) $a = ۲۰۰۱$، $b = ۱۷$

(پ) $a = ۰$، $b = ۱۹$ (ج) $a = ۲۰۰۲$، $b = ۱۷$

۲. فرض کنید n یک عدد صحیح مثبت باشد. ثابت کنید باقیمانده تقسیم a و c بر n یکسان است اگر و تنها اگر برای برخی عدد صحیح k، $a - c = nk$.

۳. نتیجه ۲.۱ را ثابت کنید. [راهنمایی: قضیه ۱ـ۱ با $|c| = b$ را بکار برید.]

۴.B. اگر توسط ماشین حساب ۵۹ را بر ۷ تقسیم کنید جواب ۸/۴۲۸۵۷۱۴۲۹ نمایش داده می‌شود. با استفاده از الگوریتم تقسیم، خواهیم دید که خارج قسمت تقسیم ۵۹ بر ۷، عدد ۸ و باقیمانده آن ۳ است. چگونه با استفاده از ماشین‌حساب می‌توانید این خارج قسمت صحیح و باقیمانده را بدست آورید؟ به‌طور کلی‌تر الگوریتمی را برای استفاده از ماشین‌حساب خود ارائه دهید که خارج قسمت و باقیمانده را برای هر مقسوم و مقسوم‌علیه مثبت به دست دهد. اطمینان حاصل کنید که الگوریتم شما تواماً برای هر دو مقسوم‌های مثبت و منفی کار می‌کند.

۵. با استفاده از الگوریتم ماشین حساب ارائه شده در تمرین ۴، خارج قسمت و باقیمانده a بر b را به دست آورید:

(الف) $a = ۵۱۷$، $b = ۸۳$ (ت) $a = ۸۱۲۶۴۹۳$، $b = ۵۴۱$

(ب) $a = -۶۱۲$، $b = ۷۴$ (ث) $a = -۹۲۱۷۶۴۵$، $b = ۶۱۷$

(پ) $a = ۷۹۶۵۵۳۲$، $b = ۱۲۷$ (ج) $a = ۱۷۱۸۱۹۹۲۰$، $b = ۴۳۲۱$

۶. با استفاده از الگوریتم تقسیم ثابت کنید که هر عدد صحیح فرد به صورت $۴k + ۱$ یا به صورت $۴k + ۳$ می‌باشد که در آن k یک عدد صحیح است.

۷. ثابت کنید که مربع هر عدد صحیح a یا به صورت $۳k$، یا به صورت $۳k + ۱$ می‌باشد که در آن k یک عدد صحیح است. [راهنمایی: به موجب الگوریتم تقسیم a باید به صورت $۳q$، $۳q + ۱$ یا $۳q + ۲$ باشد.]

۸. ثابت کنید که برای هر عدد صحیح فرد a، a^2 به صورت $8k+1$ است که در آن k یک عدد صحیح می‌باشد.

۹. ثابت کنید که مکعب هر عدد صحیح باید دقیقاً به صورت یکی از اعداد $9k$، $9k+1$ یا $9k+8$ باشد که در آن k یک عدد صحیح است.

۱-۲ بخش‌پذیری

یک حالت مهم تقسیم زمانی اتفاق می‌افتد که باقی‌مانده ۰ است، یعنی وقتی که مقسوم‌علیه یک عامل مقسوم باشد. تعریف رسمی به صورت زیر است:

تعریف. فرض کنید a و b اعداد صحیح باشند با $b \neq 0$. گوییم که b، a را **می‌شمارد** (یا این‌که b یک شمارنده a است، یا b یک عامل a است) اگر $a = bc$، برای برخی عدد صحیح c. به صورت نمادی، "b، a را می‌شمارد" را با $b|a$ و "b، a را نمی‌شمارد" را با $b \nmid a$ نشان می‌دهند.

مثال ۱.۱. $24|3$ زیرا $24 = 3 \times 8$، اما $17 \nmid 3$. شمارنده‌های منفی قابل پذیرش‌اند: $54|-6$ زیرا $54 = (-6)(-9)$، اما $(-6) \nmid (-13)$.

مثال ۲.۱. هر عدد صحیح غیرصفر b یک شمارنده صفر است زیرا $0 = b \times 0$. برای هر عدد صحیح a، داریم $1|a$ زیرا $a = a \times 1$.

تذکر. اگر b یک شمارنده a باشد، در این صورت $a = bc$، برای برخی c. بنابراین $-a = b(-c)$، لذا $b|(-a)$. استدلالی مشابه نشان می‌دهد که هر شمارندهٔ $-a$ یک شمارندهٔ a نیز هست. بنابراین

a و $-a$ دارای شمارنده‌های یکسان هستند.

تذکر. فرض کنید $a \neq 0$ و $b|a$. در این صورت $a = bc$، لذا $|a| = |b||c|$. در نتیجه، $|a| \geq |b| \geq 0$. این نابرابری آخر معادل است با $|a| \leq |b| \leq -|a|$. بنابراین

(i) هر شمارندهٔ غیر صفر عدد صحیح a کوچکتر یا مساوی $|a|$ است:

(ii) یک عدد صحیح غیر صفر دارای تنها تعداد متناهی شمارنده است.

همه شمارنده‌های عدد صحیح ۱۲ عبارتند از

۱، ۱-، ۲، ۲-، ۳، ۳-، ۴، ۴-، ۶، ۶-، ۱۲، ۱۲-.

به‌طور مشابه، همهٔ شمارنده‌های ۳۰ عبارتند از

۱، ۱-، ۲، ۲-، ۳، ۳-، ۵، ۵-، ۶، ۶-، ۱۰، ۱۰-، ۱۵، ۱۵-، ۳۰، ۳۰-.

مقسوم‌علیه‌های مشترک ۱۲ و ۳۰ اعدادی هستند که هر دو ۱۲ و ۳۰ را می‌شمارند، یعنی اعدادی که در هر دو فهرست قبلی ظاهر می‌شوند:

۱، ۱-، ۲، ۲-، ۳، ۳-، ۶، ۶-.

بزرگترین این شمارنده‌های مشترک یعنی ۶، **بزرگترین مقسوم‌علیه مشترک** ۱۲ و ۳۰ نامیده می‌شود. این مثالی از تعریف زیر است.

تعریف فرض کنید a و b اعداد صحیحی باشند که هر دو با هم صفر نیستند. **بزرگترین مقسوم‌علیه مشترک** (ب‌م‌م) a و b عبارت است از بزرگترین عدد صحیح d که هر دو a و b را می‌شمارد. به عبارت دیگر، d، ب‌م‌م a و b است مشروط به این که

(i) $d|a$ و $d|b$؛

(ii) اگر $c|a$ و $c|b$، در این صورت $c \leq d$.

بزرگترین مقسوم‌علیه مشترک a و b معمولاً با (a, b) نمایش داده می‌شود.

اگر a و b هر دو با هم صفر نباشند، در این صورت ب‌م‌م آنها موجود و یکتا است. دلیل آن این است که یک عدد صحیح غیرصفر تنها دارای تعداد متناهی شمارنده است، و لذا تنها یک تعداد متناهی از مقسوم‌علیه‌های مشترک وجود دارد. بنابراین باید یک بزرگترین مقسوم‌علیه مشترک منحصربه‌فرد وجود داشته باشد. بعلاوه، بزرگترین مقسوم‌علیه مشترک a و b در نابرابری

$$(a, b) \geq ۱$$

صدق می‌کند. زیرا ۱، یک مقسوم‌علیه مشترک a و b است.

مثال ۳.۱. همانگونه که در بالا نشان داده شد $۶ = (۱۲, ۳۰)$. تنها مقسوم علیه‌های مشترک ۲۱ و ۱۰ عبارتند از ۱ و ۱-. بنابراین $۱ = (۱۰, ۲۱)$. دو عدد صحیح که بزرگترین مقسوم‌علیه

مشترک آنها ۱ است، مثل ۲۱ و ۱۰، را **نسبت به هم اول** گویند.

مثال ۴.۱. مقسوم‌علیه‌های مشترک عدد صحیح a و ۰ همان شمارنده‌های a هستند. اگر $a > 0$، در این صورت بزرگترین مقسوم‌علیه a به‌وضوح خود a است. بنابراین اگر $a < 0$، در این صورت $(a, 0) = a$.

فهرست کردن همهٔ شمارنده‌های دو عدد صحیح بزرگ به منظور یافتن ب‌م‌م آنها می‌تواند وقت‌گیر باشد. یک روش نسبتاً سریع برای یافتن ب‌م‌م ها در چنین مواردی در قضیه ۶.۱ ارائه شده است.

قبلاً دیده‌ایم که $(۱۲, ۳۰) = ۶$. مختصر محاسبه‌ای نشان می‌دهد که چیز دیگری نیز در اینجا درست است: ۶ یک **ترکیب خطی** ۳۰ و ۱۲ است. برای مثال،

$$۶ = ۱۲(-۲) + ۳۰(۱) \qquad \text{و} \qquad ۶ = ۱۲(۸) + ۳۰(-۳).$$

به‌سادگی می‌توانید اعداد صحیح دیگر u و v را چنان بیابید که $۱۲u + ۳۰v = ۶$. قضیه زیر نشان می‌دهد که این مطلب در مورد هر بزرگترین مقسوم‌علیه مشترک درست است.

قضیه ۳.۱. فرض کنید a و b اعداد صحیحی باشند که هر دو با هم صفر نیستند و فرض کنید d بزرگترین مقسوم‌علیه مشترک آنها باشد. در این صورت اعداد صحیح u و v وجود دارند (نه الزاماً یکتا) به قسمی که $d = au + bv$.

عکس این قضیه غلط است (تمرین ۲۷)[۳].

برهان قضیه ۳.۱. فرض کنید S مجموعه همه ترکیبات خطی a و b باشد، یعنی

$$S = \{am + bn \mid m, n \in \mathbb{Z}\}.$$

عنصر خاصی از S را خواهیم یافت و نشان می‌دهیم که آن ب‌م‌م است. ابتدا توجه کنید که در S، $a^۲ + b^۲ = aa + bb$ و $a^۲ + b^۲ \geq 0$. چون a و b هر دو با هم صفر نیستند لذا $a^۲ + b^۲$ باید مثبت باشد. بنابراین S اعداد صحیح مثبتی را شامل است و لذا به موجب اصل خوش‌ترتیبی باید شامل یک کوچکترین عدد صحیح مثبت باشد. فرض کنید t نشان‌دهنده این کوچکترین عدد مثبت S باشد. به موجب تعریف S، می‌دانیم که $t = au + bv$ برای برخی اعداد صحیح u و v. ادعا می‌کنیم که t ب‌م‌م a و b است، یعنی $t = d$. برای اثبات این امر، ابتدا نشان می‌دهیم که $t \mid a$. به

۳) کلمهٔ «عکس» در پیوست الف تعریف شده است.

موجب الگوریتم تقسیم اعداد صحیح q و r وجود دارند به قسمی که $a = tq + r$، با $0 \leq r < t$. در نتیجه

$$r = a - tq,$$
$$r = a - (au + bv)q = a - aqu - bvq,$$
$$r = a(1 - qu) + b(-vq).$$

بنابراین r یک ترکیب خطی از a و b است و لذا $r \in S$. چون $t > r$ (کوچکترین عضو مثبت S)، می‌دانیم که r مثبت نیست. چون $r \geq 0$، تنها احتمال این است که $r = 0$. بنابراین $a = tq + r = tq + 0 = tq$، لذا $t|a$. استدلالی مشابه نشان می‌دهد که $t|b$. بنابراین t یک مقسوم‌علیه مشترک a و b است.

فرض کنید c هر مقسوم‌علیه مشترک دیگر a و b باشد، بنابراین $c|a$ و $c|b$. پس $a = cr$ و $b = cs$، برای برخی اعداد صحیح r و s. در نتیجه،

$$t = au + bv = (cr)u + (cs)v = c(ru + sv).$$

اولین و آخرین قسمت این معادله نشان می‌دهد که $c|t$. پس $|t| \leq c$. امّا t مثبت است، لذا $t = |t|$. بنابراین $c \leq t$. این نشان می‌دهد که t بزرگترین مقسوم‌علیه مشترک است و برهان قضیه کامل می‌شود. ■

نتیجه ۴.۱. فرض کنید a و b اعداد صحیحی باشند که هر دو با هم صفر نیستند و فرض کنید d یک عدد صحیح مثبت باشد. در این صورت d بزرگترین مقسوم‌علیه مشترک a و b است اگر و تنها اگر d در شرایط زیر صدق کند:

(i) $d|a$ و $d|b$؛

(ii) اگر $c|a$ و $c|b$، در این صورت $c|d$.

برهان. فرض کنید $d = (a, b)$، در این صورت $d \geq 1$ و به موجب تعریف، d در شرط (i) صدق می‌کند. آخرین بند از برهان قضیه ۳.۱ (با d به جای t) نشان می‌دهد که d در شرط (ii) نیز صدق می‌کند. بالعکس، فرض کنید d یک عدد صحیح مثبت باشد که در دو شرط (i) و (ii) صدق کند. در این صورت به موجب (i)، d یک مقسوم‌علیه مشترک a و b است. اگر c هر

مقسوم‌علیه مشترک دیگر باشد، در این صورت به موجب (ii) داریم $c|d$. بنابراین $|d| \leq |c|$. امّا d مثبت است لذا $|d| = d$. پس $c \leq d$ و لذا d بزرگترین مقسوم‌علیه مشترک است. ■

جواب سؤال زیر در چندین موقعیت مورد نیاز خواهد بود. اگر $a|bc$، تحت چه شرایطی این مطلب درست است که $a|b$ یا $a|c$؟ همانگونه که مثال زیر نشان می‌دهد، یقیناً این گونه نیست که این مطلب همواره درست باشد:

$$۶|۳ \times ۴ \quad \text{امّا} \quad ۶ \not| ۳ \quad \text{و} \quad ۶ \not| ۴ .$$

توجه کنید که ۶ یک عامل مشترک غیربدیهی با ۳ و یکی با ۴ دارد. اگر این اتفاق نیافتد، در این صورت سوال فوق دارای جواب مثبت است:

قضیه ۱.۵. اگر $a|bc$ و $(a,b) = ۱$، در این صورت $a|c$.

برهان. چون $(a,b) = ۱$، قضیه ۳.۱ نشان می‌دهد که برای برخی اعداد صحیح u و v، $au + bv = ۱$. ضرب این معادله در c نشان می‌دهد که $acu + bcv = c$. امّا $a|bc$ لذا $bc = ar$ برای برخی r. بنابراین

$$c = acu + bcv = acu + (ar)v = a(cu + rv).$$

اولین و آخرین قسمت این معادله نشان می‌دهد که $a|c$. ■

برای هر عدد صحیح b، می‌دانیم که b و $-b$ دارای شمارنده‌های یکسان هستند. در نتیجه مقسوم‌علیه‌های مشترک a و b یا مقسوم‌علیه‌های مشترک a و $-b$ یکسان هستند. پس بزرگترین مقسوم‌علیه مشترک آنها یکسان است، یعنی $(a,b) = (a,-b)$.
با بکار بردن استدلالی مشابه، می‌بینیم که

$$(a,b) = (a,-b) = (-a,b) = (-a,-b).$$

بنابراین هر روشی که در یافتن ب‌م‌م دو عدد صحیح مثبت استفاده می‌شود را برای یافتن ب‌م‌م هر دو عدد صحیح دلخواه نیز می‌توان بکار رود. قضیه زیر روش نسبتاً مؤثری بدست می‌دهد.

قضیه ۶.۱. (الگوریتم اقلیدسی) [۴] فرض کنید a و b اعداد صحیح مثبت باشند و $a \geq b$. اگر $b|a$ در این صورت $(a,b) = b$. اگر $b \nmid a$، در این صورت الگوریتم تقسیم را به‌طور مکرر همانگونه که در زیر می‌آید بکار برید:

$$\begin{aligned}
a &= bq_0 + r_0 && 0 \leq r_0 < b \\
b &= r_0 q_1 + r_1 && 0 \leq r_1 < r_0 \\
r_0 &= r_1 q_2 + r_2 && 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && 0 \leq r_3 < r_2 \\
r_2 &= r_3 q_4 + r_4 && 0 \leq r_4 < r_3 \\
&\vdots
\end{aligned}$$

این فرآیند هنگامی که به باقیمانده صفر برسد پایان می‌یابد. این امر باید پس از تعداد متناهی بار تکرار اتفاق افتد؛ یعنی برای برخی عدد صحیح t:

$$\begin{aligned}
r_{t-2} &= r_{t-1} q_t + r_t && 0 \leq r_t < r_{t-1} \\
r_{t-1} &= r_t q_{t+1} + 0.
\end{aligned}$$

در این صورت r_t، آخرین باقیمانده غیرصفر، بزرگترین مقسوم‌علیه مشترک a و b است.

قبل از برهان قضیه مثالی عددی را در نظر می‌گیریم که می‌تواند این فرآیند را روشن نماید. می‌خواهیم الگوریتم اقلیدسی را برای یافتن $(۳۲۴, ۱۴۸)$ بکار بریم. داریم $a = ۳۲۴$، $b = ۱۴۸$؛ با استفاده از الگوریتم تقسیم بدست می‌آوریم $q = ۲$ و $r_0 = ۲۸$:

$$\begin{aligned}
۳۲۴ &= ۱۴۸ \times ۲ + ۲۸ && (۱) \\
۱۴۸ &= ۲۸ \times ۵ + ۸ && (۲) \\
۲۸ &= ۸ \times ۳ + ۴ \\
۸ &= ۴ \times ۲ + ۰ && (۳)
\end{aligned}$$

در عبارت فوق توجه کنید که مقسوم‌علیه در هر خط در خط بعد مقسوم می‌شود و باقیمانده در هر خط در خط بعد مقسوم‌علیه می‌شود.

۴) (Euclidean Algorithm) از این قضیه تنها در پاره‌ای از تمرینها استفاده خواهد شد.

آخرین باقیمانده غیرصفر ۴ است و بنابراین ۴ = (۳۲۴, ۱۴۸). اکنون با جایگذاری برگشتی در معادلات فوق، ۴ را به صورت یک ترکیبی خطی از ۳۲۴ و ۱۴۸ می‌نویسیم.

$$۴ = ۲۸ - ۸ \times ۳$$ [این همان معادله (۳) است.]

$$۴ = ۲۸ - (۱۴۸ - ۲۸ \times ۵)۳$$ [معادله (۲) بکار رفته است تا عدد ۸ بازنویسی شود.]

$$۴ = ۲۸ - ۱۴۸ \times ۳ + ۲۸ \times ۱۵$$

$$۴ = ۲۸ \times ۱۶ - ۱۴۸ \times ۳$$

$$۴ = (۳۲۴ - ۱۴۸ \times ۲)۱۶ - ۱۴۸ \times ۳$$ [معادله (۱) بکار رفته است تا عدد ۲۸ بازنویسی شود.]

$$۴ = ۳۲۴ \times ۱۶ - ۱۴۸ \times ۳۲ - ۱۴۸ \times ۳$$

$$۴ = ۳۲۴ \times ۱۶ + ۱۴۸(-۳۵)$$

برهان قضیه ۶.۱ نتیجه‌ای فوری از لم زیر خواهد بود.

لم ۷.۱. اگر $a, b, q, r \in \mathbb{Z}$ و $a = bq + r$، در این صورت $(a, b) = (b, r)$.

برهان. اگر c یک مقسوم‌علیه مشترک a و b باشد، در این صورت $a = cs$ و $b = ct$. برای برخی اعداد صحیح t, s. در نتیجه،

$$r = a - bq = cs - (ct)q = c(s - tq).$$

بنابراین $c|r$ و لذا c یک مقسوم‌علیه مشترک b و r نیز هست. بالعکس، فرض کنید e یک مقسوم‌علیه مشترک b و r باشد، بنابراین $b = ex$ و $r = ey$. پس

$$a = bq + r = (ex)q + ey = e(xq + y).$$

بنابراین $e|a$، لذا e یک مقسوم‌علیه مشترک a و b نیز هست. در نتیجه مجموعه S متشکل از همه مقسوم‌علیه‌های مشترک a و b و مجموعه T متشکل از همه مقسوم‌علیه‌های مشترک b و r یکسان هستند. بنابراین بزرگترین عضو S، یعنی (a, b) همان بزرگترین عضو T، یعنی (b, r) است. ■

برهان قضیه ۶.۱. اگر $b|a$ در این صورت $a = bq + ۰$، بنابراین به موجب لم ۷.۱، $(a, b) = (b, ۰) = b$. اگر $b \nmid a$، در این صورت کاربرد مکرر لم ۱ـ۷ (به هر کدام از تقسیم فهرست شده درگزاره قضیه) نشان می‌دهد که

$$(a.b) = (b, r_۰) = (r_۰, r_۱) = (r_۱, r_۲) = \dots$$
$$= (r_{t-۲}, r_{t-۱}) = (r_{t-۱}, r_t) = (r_t, ۰) = r_t.$$

به این ترتیب برهان کامل می‌شود. ■

تمرینها

۱.A. بزرگترین مقسوم‌علیه مشترک هر یک را بیابید:

(الف) $(۵۶, ۷۲)$ (ب) $(۲۴, ۱۳۸)$
(پ) $(۱۴۳, ۲۲۷)$ (ت) $(۳۱۴, ۱۵۹)$
(ث) $(۳۰۶, ۶۵۷)$ (ج) $(۲۷۲, ۱۴۷۹)$
(چ) $(۳۱۴۴, ۷۶۹۶)$ (ح) $(۱۲۳۷۸, ۳۰۵۴)$

۲. ثابت کنید که $b|a$ اگر و تنها اگر $b|(-a)$.

۳. اگر $a|b$ و $b|c$، ثابت کنید $a|c$.

۴. (الف) اگر $a|b$ و $a|c$، ثابت کنید $a|(b + c)$.

(ب) اگر $a|b$ و $a|c$، ثابت کنید که $a|(br + ct)$ برای هر $r, t \in \mathbb{Z}$.

۵. اگر $a|b$ و $b|a$، ثابت کنید $a = \pm b$.

۶. اگر $a|b$ و $c|d$، ثابت کنید که $ac|bd$.

۷. ثابت یا رد کنید: اگر $a|(b + c)$، در این صورت $a|b$ یا $a|c$.

۸. اگر $r \in \mathbb{Z}$ و r یک جواب غیرصفر $x^۲ + ax + b = ۰$ (جایی که $a, b \in \mathbb{Z}$) باشد، ثابت کنید که $r|b$.

۹. اگر $(a, ۰) = ۱$، a احتمالاً چه می‌تواند باشد؟

۱۰. ثابت کنید که برای هر عدد صحیح n، $(n, n+1) = 1$.

۱۱. اگر $n \in \mathbb{Z}$، مقادیر ممکن زیر چه می‌تواند باشد؟

(الف) $(n, n+2)$ (ب) $(n, n+6)$.

۱۲. ثابت کنید که $((a,b),b) = (a,b)$.

۱۳. اگر $k = abc + 1$، در این صورت ثابت کنید که $(k,a) = (k,b) = (k,c) = 1$.

۱۴. کوچکترین عدد صحیح مثبت در مجموعه‌های زیر را بیابید:

(الف) $\{6u + 15v \mid u, v \in \mathbb{Z}\}$ (ب) $\{12r + 17s \mid r, s \in \mathbb{Z}\}$.

۱۵.B. هر کدام از بزرگترین مقسوم‌علیه‌های مشترک (a,b) در تمرین ۱ را به صورت یک ترکیب خطی از a و b بیان کنید.

۱۶. اگر $(a,b) = d$، ثابت کنید که $(a/d, b/d) = 1$.

۱۷. اگر $a|c$ و $b|c$ و $(a,b) = 1$، ثابت کنید که $ab|c$. [همچنین تمرین ۲۸ را ملاحظه کنید.]

۱۸. اگر $c > 0$، ثابت کنید که $(ca, cb) = c(a,b)$.

۱۹. اگر $a|(b+c)$ و $(b,c) = 1$، ثابت کنید که $(a,b) = 1 = (a,c)$.

۲۰. اگر $(a,4) = 2$ و $(b,4) = 2$، ثابت کنید که $(a+b,4) = 4$.

۲۱. ثابت کنید که $(a, a+b) = d$ اگر و تنها اگر $(a,b) = d$.

۲۲. ثابت کنید که برای هر $t \in \mathbb{Z}$، $(a,b) = (a, b+at)$.

۲۳. ثابت کنید که $(a,(b,c)) = ((a,b),c)$.

۲۴. اگر $(a,c) = 1$ و $(b,c) = 1$، ثابت کنید که $(ab,c) = 1$.

۲۵. با استفاده از استقراء نشان دهید که اگر $(a,b) = 1$، در این صورت برای هر $n \geq 1$، $(a,b^n) = 1$.[۵]

۲۶. فرض کنید $a, b, c \in \mathbb{Z}$. ثابت کنید معادله $ax + by = c$ دارای جوابهای صحیح است اگر و تنها اگر $(a,b)|c$.

۵) استقراء در پیوست پ بحث شده است.

۲۷. (الف) اگر $a, b, u, v \in \mathbb{Z}$ چنان باشند که $au + bv = ۱$، ثابت کنید که $(a, b) = ۱$.
(ب) با مثال نشان دهید که اگر $au + bv = d > ۰$، در این صورت ممکن است (a, b) برابر d نباشد.

۲۸. اگر $a|c$ و $b|c$ و $(a, b) = d$، ثابت کنید که $ab|cd$. [تمرین ۱۷ حالت $d = ۱$ است.]

۲۹. اگر $c|ab$ و $(c, a) = d$، ثابت کنید که $c|db$.

۳۰. اگر $a_۱$، $a_۲$، ...، a_n اعداد صحیحی باشند که همه با هم صفر نیستند، در این صورت بزرگترین مقسوم‌علیه مشترک آنها بزرگترین عدد صحیح d است به‌طوری که $d|a_i$ برای هر i. ثابت کنید اعداد صحیح u_i وجود دارند به قسمی که $d = a_۱u_۱ + a_۲u_۲ + \cdots + a_nu_n$.
[راهنمایی: برهان قضیه ۱ـ۳ را جرح و تعدیل کنید.]

۳۱. کوچکترین مضرب مشترک اعداد صحیح غیرصفر a و b که با $[a, b]$ نشان داده می‌شود، عبارت است از کوچکترین عدد صحیح مثبت m به قسمی که $a|m$ و $b|m$. ثابت کنید که
(الف) هرگاه $a|k$ و $b|k$، در این صورت $[a, b]|k$؛
(ب) اگر $a > ۰$ و $b > ۰$، $[a, b] = ab/(a, b)$.

۳۲. ثابت کنید که یک عدد صحیح مثبت بر ۳ بخش‌پذیر است اگر و تنها اگر مجموع ارقام آن بر ۳ بخش‌پذیر باشد. [راهنمایی: $۱۰^۲ = ۹۹۹ + ۱$ و به‌طور مشابه برای توانهای دیگر ۱۰.]

۳۳. ثابت کنید که یک عدد صحیح مثبت بر ۹ بخش‌پذیر است اگر و تنها اگر مجموع ارقام آن بر ۹ بخش‌پذیر باشد. [تمرین ۳۲ را ملاحظه کنید.]

۳۴.C اگر $a \not| ۲$ و $a \not| ۳$، ثابت کنید که $۲۴|(a^۲ - ۱)$.

۳۵. ثابت کنید که
(الف) $(a, b)|(a + b, a - b)$ ؛
(ب) برای هر n، $(n + ۱, n^۲ - n + ۱)$ برابر ۱ یا ۳ است.

۱-۳ اعداد اول و یکتایی تجزیه

بجز ± 1 هر عدد صحیح غیرصفر n دارای حداقل چهار شمارنده متمایز، یعنی ۱، ۱-، n، $-n$ می‌باشد. اعداد صحیحی که دارای تنها همین چهار شمارنده هستند نقش بسیار مهمی را ایفا می‌کنند.

تعریف. یک عدد صحیح p را اول گویند اگر $p \neq 0$، $p \neq \pm 1$ و تنها شمارنده‌های آن ± 1 و $\pm p$ باشند.

مثال ۵.۱. ۳، ۵-، ۷، ۱۱-، ۱۳- و ۱۷- اول هستند اما ۱۵ اول نیست (زیرا ۱۵ دارای شمارنده‌هایی غیر از ± 1 و ± 15، مانند ۳ و ۵ است). عدد صحیح ۴۵۶۷ اول است؛ اثبات این مطلب با استفاده از تعریف، مستلزم یک بررسی خسته کننده از همهٔ شمارنده‌های ممکن آن است.

نشان دادن این‌که تعداد نامتناهی اعداد اول متمایز وجود دارد مشکل نیست (تمرین ۲۵). چون شمارنده‌های هر عدد صحیح p با شمارنده‌های $-p$ یکسان است، دیده می‌شود که

p اول است اگر و تنها اگر $-p$ اول باشد.

اگر p و q هر دو اول باشند و $p|q$، در این صورت p باید یکی از اعداد ۱، ۱-، q، $-q$ باشد. اما چون p اول است، $p \neq \pm 1$. بنابراین

اگر p و q اول باشند و $p|q$، در این صورت $p = \pm q$.

قضیه ۸.۱. فرض کنید p یک عدد صحیح باشد با $p \neq 0$، $p \neq \pm 1$. در این صورت p اوّل است اگر و تنها دارای این خاصیت باشد:

هرگاه $p|bc$، در این صورت $p|b$ یا $p|c$.

برهان. فرض کنید p اول باشد و $p|bc$. بم‌م دو عدد p و b را در نظر بگیرید. حال (p,b) باید یک شمارنده مثبت عدد اول p باشد. بنابراین تنها احتمالات ممکن عبارتند از $(p,b) = 1$ و $(p,b) = \pm p$ (هرکدام که مثبت باشد). اگر $(p,b) = \pm p$ در این صورت $p|b$. اگر $(p,b) = 1$ در این صورت به‌موجب قضیه ۵.۱، $p|c$. بنابراین در هر حال $p|b$ یا $p|c$. برهان عکس قضیه به خواننده واگذار شده است (تمرین ۴). ■

نتیجه ۹.۱. اگر p اول باشد و $p|a_1a_2\cdots a_n$، در این صورت p حداقل یکی از a_i ها را می‌شمارد.

برهان. اگر $p|a_1(a_2a_3\cdots a_n)$، در این‌صورت به‌موجب قضیه ۸.۱، $p|a_1$ یا $p|a_2a_3\cdots a_n$. اگر $p|a_1$، کار ما پایان‌یافته است. اگر $p|a_2(a_3a_4\ldots a_n)$، در این صورت مجدداً بنابه قضیه ۸.۱، $p|a_2$ یا $p|a_3a_4\cdots a_n$. اگر $p|a_2$، کار پایان‌یافته است؛ در غیراینصورت با استفاده مکرر از قضیه ۸.۱ این فرایند را ادامه دهید. پس از حداکثر n بار تکرار باید یک a_i موجود باشد که بر p بخش‌پذیر است. ■

عدد صحیحی را بجز ۰ و ± 1 انتخاب کنید. اگر آن را "تا حد ممکن" تجزیه کنید، خواهید دید که حاصل‌ضربی از یک یا تعداد بیشتری اعداد اول است. به‌عنوان مثال

$$۱۲ = ۴ \times ۳ = ۲ \times ۲ \times ۳,$$

$$۶۰ = ۱۲ \times ۵ = ۲ \times ۲ \times ۳ \times ۵,$$

$$۱۱۳ = ۱۱۳ \quad \text{(عدد اول)}.$$

در این مبحث ما امکان یک "حاصل‌ضرب" با تنها یک عامل را می‌پذیریم، که در واقع در این حالت عدد مورد نظر ما یک عدد اول است. قضیه زیر مبین آن است که آنچه که در این مثال‌ها انجام شد همواره قابل انجام است:

قضیه ۱۰.۱. هر عدد صحیح n به غیر از ۰ و ± 1، حاصل‌ضربی از اعداد اول است.

برهان. ابتدا توجه کنید که اگر n حاصل‌ضربی از اعداد اول باشد، مثلاً $n = p_1p_2\ldots p_k$، در این صورت $-n = (-p_1)p_2\ldots p_k$ نیز حاصل‌ضربی از اعداد اول است. در نتیجه ما تنها نیاز داریم قضیه را برای حالتی که $n > 1$ است اثبات کنیم. فرض کنید S مجموعه همه اعداد صحیح بزرگتر از ۱ باشد که حاصل‌ضربی از اعداد اول نیستند. نشان خواهیم داد که S تهی است. به خلاف، فرض کنید که S غیرتهی باشد. در این صورت بنا به اصل خوش‌ترتیبی، S شامل یک کوچکترین عضو m می‌باشد. چون $m \in S$، m خودش اول نیست. بنابراین m باید دارای شمارنده‌های مثبتی بجز ۱ یا m باشد، مثلاً $m = ab$ با $1 < a < m$ و $1 < b < m$. چون هر دوی a و b کوچکتر از m (کوچکترین عضو S) هستند، هیچکدام از a و b در S نیستند. به موجب تعریف S، هر دو a و b حاصل‌ضربی از اعداد اول هستند، مثلاً

$$a = p_1p_2\ldots p_r \quad \text{و} \quad b = q_1q_2\ldots q_s,$$

با $r \geq ۱$، $s \geq ۱$، و هر p_i، q_j اول است. بنابراین $m = p_۱p_۲ \dots p_r q_۱q_۲ \dots q_s$ حاصل‌ضربی از اعداد اول است، لذا $m \notin S$. ما به یک تناقض رسیده‌ایم: $m \in S$ و $m \notin S$. بنابراین S باید تهی باشد. ■

یک عدد صحیح به غیر از ۰، ± ۱ را که اول نیست، **مرکب** گویند. گرچه که یک عدد صحیح مرکب ممکن است دارای چندین تجزیه به عوامل اول متفاوت باشد، مثلاً

$$۴۵ = ۳ \times ۳ \times ۵,$$
$$۴۵ = (-۳) \times ۵ \times (-۳),$$
$$۴۵ = ۵ \times ۳ \times ۳,$$
$$۴۵ = (-۵) \times (-۳) \times ۳.$$

با این‌حال تجزیه‌ها، اساساً یکی هستند. تنها اختلاف، ترتیب عوامل و درج علامات منفی است. به‌سادگی می‌توانید خودتان را متقاعد نمایید که هر تجزیه به عوامل اول عدد ۴۵ دارای دقیقاً سه عامل اول مثلاً $q_۱$، $q_۲$، $q_۳$ می‌باشد. بعلاوه با مرتب‌کردن و نمایه‌گذاری مجدد qها، همواره خواهید داشت $\pm q_۱ = ۳$، $\pm q_۲ = ۳$ و $\pm q_۳ = ۵$. این مثالی از قضیه زیر است.

قضیه ۱.۱۱. (قضیه اساسی حساب) هر عدد صحیح n به غیر از ۰ و ± ۱، حاصل‌ضربی از اعداد اول است. این تجزیه به عوامل اول منحصر به فرد، به مفهوم زیر است: اگر

$$n = p_۱p_۲ \dots p_r \qquad \text{و} \qquad n = q_۱q_۲ \dots q_s$$

که در آن هر p_i، q_j اول باشد، در این صورت $r = s$ (یعنی تعداد عوامل یکسان است) و پس از مرتب کردن و نمایه‌گذاری مجدد q ها خواهیم داشت

$$p_۱ = \pm q_۱, \quad p_۲ = \pm q_۲ \quad p_۳ = \pm q_۳, \dots, p_r = \pm q_r.$$

برهان. به موجب قضیه ۱.۱۰، هر عدد صحیح به غیر از ۰، ± ۱ دارای حداقل یک تجزیه به عوامل اول می‌باشد. فرض کنید همانگونه که درگزاره قضیه آمده است، n دارای دو تجزیه به عوامل اول باشد. در این صورت

$$p_۱(p_۲p_۲ \dots p_r) = q_۱q_۲q_۳ \dots q_s,$$

لذا $p_1|q_1q_2\dots q_s$. به موجب نتیجه ۹.۱، p_1 باید یکی از q_j ها را بشمارد. با مرتب کردن و نمایه‌گذاری مجدد، در صورت لزوم، می‌توانیم فرض کنیم $p_1|q_1$. چون p_1 و q_1 اولند، باید $p_1 = \pm q_1$. در نتیجه

$$\pm q_1p_2p_3\dots p_r = q_1q_2q_3\dots q_s.$$

از تقسیم دو طرف بر q_1 بدست می‌آوریم

$$p_2(\pm p_3p_4\dots p_r) = q_2q_3q_4\dots q_s,$$

لذا $p_2|q_2q_3\dots q_s$. به موجب نتیجه ۹.۱، p_2 باید یکی از q_j ها را بشمارد؛ همانند بالا می‌توانیم فرض کنیم $p_2|q_2$. بنابراین $p_2 = \pm q_2$ و

$$\pm q_2p_2p_4\dots p_r = q_2q_3q_4\dots q_s.$$

از تقسیم دوطرف بر q_2 بدست می‌آوریم

$$p_3(\pm p_4\dots p_r) = q_3q_4\dots q_s.$$

ما این روند را با استفاده مکرر از نتیجه ۱ـ۹ و حذف یک عدد اول از هر طرف در هر مرحله ادامه می‌دهیم. اگر $r > s$، در این صورت پس از s مرحله، همه q ها حذف شده و خواهیم داشت $\pm p_{s+1}p_{s+2}\dots p_r = 1$. چون تنها شمارنده‌های ۱ عبارتند از ± 1 و داریم $p_r \neq \pm 1$ (چون p_r اوّل است)، این نتیجه‌گیری یک تناقض است. استدلالی مشابه نشان می‌دهد که فرض $s > r$ نیز به یک تناقض منجر خواهد شد. بنابراین باید $r = s$، و پس از r مرحله فرآیند حذف پایان خواهد یافت با $p_1 = \pm q_1$، $p_2 = \pm q_2$، ...، $p_r = \pm q_r$. ■

اگر فقط اعداد صحیح مثبت در نظر گرفته شوند، نوع قوی‌تری از تجزیه یکتا وجود دارد:

نتیجه ۱۲.۱. هر عدد صحیح $n > 1$ را می‌توان به یک و تنها یک صورت $n = p_1p_2p_3\dots p_r$ نوشت که در آن p_i ها اعداد اول مثبت هستند به‌طوری که $p_1 \leq p_2 \leq p_3 \leq \dots \leq p_r$.

برهان تمرین ۵. ■

تمرینها

۱.A. هرکدام از اعداد زیر را به صورت حاصل‌ضربی از اعداد اول بیان کنید:

(الف) ۵۰۴۰ (ب) -۲۳۴۵

(پ) ۴۵۶۷۰ (ت) ۲۰۴۲۰۴۰

۲. فرض کنید p یک عدد صحیح به غیر از ۰ و ± ۱ باشد. ثابت کنید که p اول است اگر و تنها اگر برای هر $a \in \mathbb{Z}$ یا $(a,p) = ۱$ یا $p|a$.

۳. فرض کنید p یک عدد صحیح به غیر از ۰ و ± ۱ باشد. ثابت کنید که p اول است اگر و تنها اگر دارای این خاصیت باشد که: هرگاه r و s اعداد صحیحی باشند به‌طوری که $p = rs$، در این صورت $r = \pm ۱$ یا $s = \pm ۱$.

۴. فرض کنید p یک عدد صحیح به غیر از ۰ و ± ۱ با این خاصیت باشد که: هرگاه b و c اعداد صحیحی باشند به‌طوری که $p = bc$، در این صورت $p|b$ یا $p|c$. ثابت کنید که p اول است. [راهنمایی: اگر d یک شمارنده p باشد، مثلاً $p = dt$، در این صورت $p|d$ یا $p|t$. نشان دهید که این نتیجه می‌دهد $d = \pm p$ یا $d = \pm ۱$.]

۵. نتیجه ۱۲.۱ را ثابت کنید.

۶. اگر p اول باشد و $p|a^n$، ثابت کنید $p^n|a^n$.

۷. (الف) همه شمارنده‌های $۵^t \times ۳^s$ را که در آن $s,t \in \mathbb{Z}$ و $s,t > ۰$، فهرست کنید.
(ب) اگر $r,s,t \in \mathbb{Z}$ مثبت باشند، عدد $۵^t \times ۳^s \times ۲^r$ چند شمارنده دارد؟

۸. ثابت کنید که $(a,b) = ۱$ اگر و تنها اگر هیچ عدد اول p وجود نداشته باشد به‌طوری که $p|a$ و $p|b$.

۹. اگر p اول باشد و $(a,b) = p$، در این صورت $(a^۲,b^۲) = ?$.

۱۰. هر یک از گزاره‌های زیر را ثابت یا رد کنید:

(الف) اگر p اول باشد و $p|(a^۲+b^۲)$ و $p|(c^۲+d^۲)$ در این صورت $p|(a^۲-c^۲)$.

(ب) اگر p اول باشد و $p|(a^۲+b^۲)$ و $p|(c^۲+d^۲)$، در این صورت $p|(a^۲+c^۲)$.

(پ) اگر p اول باشد و $p|a$ و $p|(a^۲+b^۲)$، در این صورت $p|b$.

B.۱۱. اگر $a = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_k^{r_k}$ و $b = p_1^{s_1} p_2^{s_2} p_3^{s_3} \dots p_k^{s_k}$، به‌طوری که p_1، p_2، ...، p_k اعداد اول مثبت متمایز باشند و هر $r_i, s_i \geq 0$، در این صورت ثابت کنید:

(الف) $(a,b) = p_1^{n_1} p_2^{n_2} p_3^{n_3} \dots p_k^{n_k}$، که در آن برای هر i، n_i مینیمم r_i و s_i است.

(ب) $[a,b] = p_1^{t_1} p_2^{t_2} p_3^{t_3} \dots p_k^{t_k}$، که در آن برای هر i، t_i ماکسیمم r_i و s_i است. [تمرین ۳۱ در بخش ۲.۱ را ملاحظه کنید.]

۱۲. (الف) اگر $3 | (a^2 + b^2)$، ثابت کنید که $3 | a$ و $3 | b$. [راهنمایی: اگر $3 \nmid a$، در این صورت $a = 3k + 1$ یا $a = 3k + 2$.]

(ب) اگر $5 | (a^2 + b^2 + c^2)$، ثابت کنید که $5 | a$ یا $5 | b$ یا $5 | c$.

۱۳. اگر $c^2 = ab$ و $(a,b) = 1$، ثابت کنید که a و b مربع کامل هستند.

۱۴. اگر $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$، به‌طوری که p_1، p_2، ...، p_k اعداد اول متمایز باشند و هر $r_i \geq 0$، ثابت کنید که n یک مربع کامل است اگر و تنها اگر هر r_i، زوج باشد.

۱۵. ثابت کنید که $a | b$ اگر و تنها اگر $a^3 | b^3$.

۱۶. اگر n یک عدد صحیح مثبت باشد، ثابت کنید n عدد صحیح غیراول متوالی وجود دارد. [راهنمایی: اعداد $(n+1)! + 2$، $(n+1)! + 3$، $(n+1)! + 4$، ... را در نظر بگیرید.]

۱۷. اگر $p \geq 5$ اول باشد، ثابت کنید $p^2 + 2$ غیراول است. [راهنمایی: باقیمانده‌های ممکن تقسیم p بر ۶ را در نظر بگیرید.]

۱۸. ثابت یا رد کنید. مجموع‌های

$$1 + 2 + 4, \quad 1 + 2 + 4 + 8, \quad 1 + 2 + 4 + 8 + 16, \dots$$

یک در میان بترتیب اول و مرکب هستند.

۱۹. اگر $n \in \mathbb{Z}$ و $n \geq 0$، ثابت کنید که n را می‌توان به‌طور منحصر به فردی به‌صورت $n = 2^k m$ نوشت، جایی که $k \geq 0$ و m فرد است.

۲۰. (الف) ثابت کنید هیچ دو عدد صحیح غیرصفر a و b وجود ندارند طوری که $a^2 = 2b^2$. [راهنمایی: قضیه اساسی حساب یا قضیه ۸.۱ را بکار برید.]

(ب) ثابت کنید $\sqrt{2}$ یک عدد اصم است. [راهنمایی: از برهان خلف استفاده کنید

(پیوست الف). فرض کنید $\sqrt{۲} = \frac{a}{b}$ (با $a, b \in \mathbb{Z}$) و قسمت (الف) را بکار برید تا به یک تناقض برسید.]

۲۱. اگر p یک عدد اول مثبت باشد، ثابت کنید $\sqrt{p}$ اصم است. [تمرین ۲۰ را ملاحظه کنید.]

۲۲. (الف) ثابت کنید که $\sqrt{۳۰}$ اصم است.

(ب) ثابت کنید که $\sqrt[۳]{۲}$ اصم است.

۲۳.C اگر $r^۲ | s^۲$، ثابت کنید $r | s$.

۲۴. ثابت یا رد کنید: اگر n یک عدد صحیح مثبت باشد، در این صورت $n = p + a^۲$، که در آن $a \in \mathbb{Z}$، و p یا اول است یا $p = ۱$.

۲۵. (اقلیدس[۶]) ثابت کنید که تعداد بی‌پایانی عدد اوّل وجود دارد. [راهنمایی: از برهان خلف استفاده کنید (پیوست الف). فرض کنید که تنها تعداد متناهی اعداد اول $p_۱, p_۲, \ldots, p_k$ وجود دارد و با نشان دادن این‌که عدد $(p_۱ p_۲ \ldots p_k) + ۱$ توسط هیچ یک از p_i ها شمرده نمی‌شود به یک تناقض برسید.]

۲۶. فرض کنید $S = \{۴n + ۱ \mid n \in \mathbb{Z}, n \geq ۰\}$. اگر $a, b \in S$ در این صورت a را یک S–شمارنده b گوییم مشروط به این‌که $b = ac$ برای برخی $c \in S$. یک S–اول عبارت است از یک عضو $q \neq ۱$ از S که تنها S– شمارنده‌های آن خودش و ۱ باشند.

(الف) ثابت کنید که هر عضو S (بجز ۱) حاصل‌ضربی از S–اول‌ها است. [راهنمایی: برهان قضیه ۱۰.۱ را کپی کنید. آیا چیزی باید تغییر کند؟]

(ب) عدد ۴۴۱ را بکار برید تا نشان دهید که تجزیه به حاصل‌ضرب S–اول‌ها لزوماً یکتا نیست.

۲۷. فرض کنید a یک عدد صحیح مثبت باشد. ثابت کنید که $\sqrt{a}$ گویا است اگر و تنها اگر $\sqrt{a}$ یک عدد صحیح باشد.

۲۸. فرض کنید p و q اعداد اول باشند با $p \geq ۵$ و $q \geq ۵$. ثابت کنید $۲۴ | (p^۲ - q^۲)$.

۲۹. فرض کنید $n \in \mathbb{Z}$ با $n > ۲$. ثابت کنید که عدد اول p وجود دارد به‌طوری که $n < p < n!$. [راهنمایی: اگر $n! - ۱$ اول نباشد، دارای یک شمارنده اول مثل p است، نشان دهید که

۶) Euclid

$p \leq n$ به یک تناقض منجر می‌شود.]

۱-۴ آزمون اول بودن[۷]

استفاده از نتایج بخشهای قبلی برای اعداد بزرگ (۲۰۰ رقمی یا بیشتر) مشکل می‌باشد. درگذشته این امر موضوع مهمی نبود. امّا اخیراً نیاز به کدهای محرمانه در ارتباطات الکترونیک در تجارت، ارتش، و اطلاعات علمی اهمیت تازه‌ای به آزمون اول بودن و فاکتورگیری داده است. یکی از امیدبخش‌ترین روشهای رمزگذاری، دستگاه رمز RSA، که در فصل ۱۲ به آن پرداخته شده است، از اعداد اوّل بزرگ استفاده می‌کند. ضریب ایمنی این روش به این حقیقت بستگی دارد که فاکتورگیری اعداد بزرگ بسیار مشکل است.

از دید نظری تعیین اوّل بودن یک عدد صحیح مثبت مفروض n ساده است. به‌سادگی بررسی می‌کنید که n بر هیچ کدام از اعداد صحیح از ۲ تا n (بزرگترین عامل ممکن n) بخش‌پذیر نیست. چون هر شمارنده n خود حاصلضربی از اعداد اوّل است، تنها لازم است بررسی کنید که آیا n بر اعداد اول از ۲ تا $\frac{n}{2}$ بخش‌پذیر است یا نه. ولی این کار حتی با استفاده از کامپیوتر نیز ممکن است کار طاقت‌فرسایی باشد. آزمون اول‌بودن زیر مقدار کار را به‌طور چشمگیری کاهش می‌دهد.

قضیه ۱.۱۳. فرض کنید $n > ۱$. اگر n دارای هیچ عامل اول کوچکتر یا مساوی $\sqrt{n}$ نباشد، در این صورت n اول است.

با استفاده از این قضیه، چون تنها ۱۶۸ عدد اول کوچکتر از $\sqrt{۱۰۰۰۰۰۰} = ۱۰۰۰$ وجود دارد، لذا اول بودن هر عدد کوچکتر از ۱۰۰۰۰۰۰ با انجام حداکثر ۱۶۸ تقسیم بررسی می‌شود.

برهان قضیه ۱.۱۳. به موجب قضیه ۱.۱۰، $n = p_۱p_۲ \dots p_k$ که در آن هر p_i اول است. بنا به فرض، $p_i > \sqrt{n}$ برای هر i. اگر در این تجزیه تعداد عوامل اوّل دو تا یا بیشتر باشد، در این صورت

$$n = p_۱p_۲p_۳ \dots p_k > \sqrt{n}\sqrt{n}p_۳ \dots p_k = np_۳ \dots p_k \geq n.$$

بنابراین $n > n$ که یک تناقض است. پس باید داشته باشیم $n = p_۱$. ■

۷) این بخش اختیاری بوده و می‌تواند حذف شود.

با استفاده از قضیه ۱۳.۱ به صورت زیر می‌توان همه اعداد اول کوچکتر یا مساوی یک عدد صحیح مثبت مفروض n را یافت. همه اعداد از ۲ تا n را فهرست کنید. فرض کنید ۲، ۳، ۵، ...، p_k همه اعداد اول کوچکتر یا مساوی $\sqrt{n}$ باشند. سپس همه مضارب ۳، مضارب ۵ و غیره را ضربدر بزنید. آنقدر ادامه دهید تا همه مضارب p_k ضربدر زده شوند. اعدادی که در فهرست باقی می‌ماند توسط هیچکدام از اعداد اول کوچکتر یا مساوی $\sqrt{n}$ شمرده نمی‌شود. چنین عددی باید اول باشد (زیرا $t \leq n$ نتیجه می‌دهد $\sqrt{t} \leq \sqrt{n}$). این فرآیند، **غربال اِراتُستِن** [۸] نامیده می‌شود.

کارآمدی روش پیش در یافتن اعداد اوّل، به‌وضوح به تعداد اعداد اول کوچکتر یا مساوی n مربوط است. این تعداد را می‌توان توسط قضیه زیر که برهان آن خارج از حوزه این کتاب است تقریب زد.

قضیه ۱۴.۱. اگر n یک عدد صحیح مثبت بزرگ باشد، در این صورت $\Pi(n)$، تعداد اعداد اوّل کوچکتر یا مساوی n تقریباً برابر $n/(\ln n)$ (که در آن ln لگاریتم طبیعی را نشان می‌دهد) می‌باشد. به‌طور دقیق‌تر،

$$\lim_{n\to\infty} \left(\frac{\frac{\Pi(n)}{n}}{\ln n} \right) = ۱.$$

بررسی اول بودن یک عدد صحیح n توسط قضیه ۱۳.۱، مستلزم تقسیم n بر هر عدد اول کوچکتر یا مساوی $\sqrt{n}$ می‌باشد. به موجب قضیه ۱-۱۴، تعداد اعداد اول کوچکتر یا مساوی $\sqrt{n}$، تقریباً برابر $\sqrt{n}/\ln\sqrt{n} = ۲\sqrt{n}/\ln n$ می‌باشد. سریعترین کامپیوترها حداقل $(\ln n)/۱۰^۶$ ثانیه برای انجام چنین تقسیمی زمان می‌برند. بنابراین با فرض این‌که همهٔ اعداد اول کوچکتر یا مساوی با $\sqrt{n}$ را از پیش بدانیم، بررسی این‌که n اول است تقریباً $۲\sqrt{n}/۱۰^۶ = ۲\sqrt{n}/\ln n \cdot \ln n/۱۰^۶$ ثانیه زمان می‌برد. با استفاده از این روش مستقیم، بررسی این‌که یک عدد سی‌رقمی اول است ۶۳ سال زمان می‌برد.

آزمونهای جاری تعیین اول بودن اعداد بزرگ که به کمک کامپیوتر انجام می‌شود تا حدودی به روشهای مبتنی بر احتمال بستگی دارد. به عنوان مثال، می‌توان نشان داد که هر عدد اول فرد n دارای این خاصیت است که $۱ - ۲^{n-۱}$ بر n بخش‌پذیر است (لم ۲.۱۲). متأسفانه معکوس این مطلب درست نیست: اعداد مرکب n ای وجود دارند که n عدد $۱ - ۲^{n-۱}$ را می‌شمارد. البته تعداد آنها نسبتاً کم است. بنابراین اگر n عدد $۱ - ۲^{n-۱}$ را بشمارد، احتمال بالایی وجود دارد که n اول باشد.

۸) Sieve of Eratosthenes

گرچه که بالا بودن احتمال معادل قطعیت نیست، امّا آزمونهای مبتنی بر احتمال می‌تواند برای تعیین نامزدهای مناسب مورد استفاده قرارگیرد. سپس با استفاده از آزمونهای دیگر می‌توان اوّل بودن را اثبات نمود. در حال حاضر با سریعترین روشهای کامپیوتری می‌توان اول بودن یک عدد ۱۰۰ رقمی را در ۳۳ ثانیه تعیین کرد. یک عدد ۲۰۰ رقمی ۸ دقیقه و یک عدد ۱۰۰۰ رقمی یک هفته زمان می‌برد[۹].

تعداد کمی اعداد بسیار بزرگتر وجود دارند که اول بودن آنها اثبات شده است. اینها اعداد اول مرسنی[۱۰] هستند ـ اعداد اولی به صورت $۲^p - ۱$. البته همهٔ اعداد به صورت فوق اول نیستند بلکه برخی از آنها از جمله $۲^۳ - ۱ = ۷$ و $۲^{۲۱۶۰۹۱} - ۱$ اول می‌باشند. عدد آخر دارای ۶۵۰۵۰ رقم می‌باشد.

بعد از ذکر این کارهای عظیم محاسباتی در مورد آزمونهای اول بودن، ممکن است قدری عجیب بنظر برسد که هیچ نتیجه مشابهی در مورد تجزیه کردن وجود ندارد. حتی اگر بدانید که یک عدد حاصلضربی از تنها دو عدد اول بزرگ است تجزیه آن ممکن است عملاً غیرممکن باشد. جدول زیر که با استفاده از قدرت رایانه‌ها و کارآمدترین الگوریتم‌های شناخته‌شده به‌دست آمده است نشان دهنده زمان لازم برای تجزیه به عوامل اول اعداد صحیح با اندازه‌های متفاوت می‌باشد.[۱۱]

تعداد ارقام ده‌دهی	زمان تقریبی
۱۰۰	۱ ماه
۲۰۰	۴۲۷۹۰۰ سال
۳۰۰	$۵/۵ \times ۱۰^{۱۲}$ سال
۵۰۰	$۴/۷ \times ۱۰^{۲۲}$ سال

زمانهای فوق در سالهای آینده و با بهتر شدن الگوریتم‌ها و توسعه ابررایانه‌های قوی‌تر کاهش خواهندیافت. البته بدون تردید مسئلهٔ تجزیه اعداد بزرگ برای سالهای متمادی به‌صورت مسئله‌ای شاق باقی خواهد ماند.

---

۹) توضیح مترجم: کلیه اعداد و ارقام ارائه شده در مورد سرعت و ظرفیت رایانه‌ها مربوط به زمان تألیف کتاب می‌باشد.

۱۰) Mersenne primes

۱۱) این اعداد و ارقام به مشکل‌ترین حالتها مربوط می‌شوند ـ اعدادی که حاصلضربی از اعداد اول بزرگی هستند که طول ارقام آنها تقریباً برابر با طول ارقام خود آن عدد است. یک عدد با عوامل اول کوچکتر اغلب با سرعت بسیار بیشتری تجزیه می‌شود.

تمرینها

A.۱. کدامیک از اعداد زیر اولند:

(الف) ۷۰۱ (ب) ۱۰۰۹

(پ) ۱۹۴۹ (ت) ۱۹۵۱

۲. با استفاده از غربال اراتستن همه اعداد اول مثبت کوچکتر از ۳۰۰ را بیابید.

۳. اعداد اول p و q را اعداد اول دوقلو گویند اگر $q = p + 2$. برای مثال ۳ و ۵ و همچنین ۱۱ و ۱۳ اعداد اول دوقلو هستند. همه زوجهای اعداد اول دوقلو مثبت کوچکتر از ۲۰۰ را بیابید.

۴. (الف) بررسی کنید که $2^5 - 1$ و $2^7 - 1$ اولند.

(ب) نشان دهید که $2^{11} - 1$ اول نیست.

۵. نشان دهید که هر عدد صحیح مثبت سه رقمی غیر اول دارای یک عامل اول کوچکتر یا مساوی ۳۱ است.

B.۶. فرض کنید $n > 1$. اگر n دارای هیچ عامل اول کوچکتر یا مساوی $\sqrt{n}$ نباشد، ثابت کنید که یا n اول است یا حاصلضربی از دو عدد اول است.

۷. فرض کنید $p > 1$. اگر $2^p - 1$ اول باشد، ثابت کنید که p اول است. [راهنمایی: عکس نقیض آن را ثابت کنید: اگر p غیراول باشد، $2^p - 1$ نیز چنین است. توجه: به موجب تمرین ۴ (ب)، عکس این مسئله غلط است.]

۸. فرض کنید a و b اعداد صحیح غیرمنفی باشند که حداقل یکی از آنها مخالف ۱ است. اگر k فرد باشد و $k \geq 3$، ثابت کنید که $a^k + b^k$ اول نیست.

۹. اگر $k \geq 1$ و $2^k + 1$ اول باشد، ثابت کنید که برای برخی l، $k = 2^l$. [راهنمایی: تمرین ۸ بالا و تمرین ۱۹ بخش ۱-۳ را بکار برید.]

۱۰. اگر n یک عدد صحیح مثبت به صورت $4k + 3$ باشد، ثابت کنید که n دارای یک عامل اول به صورت $4k + 3$ است.

۱۱. نشان دهید که تعداد بی‌پایانی عدد اول به صورت $4k + 3$ وجود دارد. [تمرین ۱۰ را ملاحظه کنید.]

۱۲. همه اعداد صحیح مثبت n را بیابید به قسمی که n، $n+2$ و $n+4$ اول باشند.

۱۳. فرض کنید p اول باشد و $1 \leq k < p$. ثابت کنید که p ضریب دوجمله‌ای $\binom{p}{k}$ را می‌شمارد. [بخاطر آورید که $\binom{p}{k} = p!/k!(p-k)!$.]

۱۴. فرض کنید p_n، n-اُمین عدد اول مثبت در ترتیب معمولی باشد. با استفاده از استقراء نشان دهید که $p_n \leq 2^{2^{n-1}}$. [راهنمایی: ابتدا بررسی کنید که $2^n - 1 = 1 + 2^1 + 2^2 + \ldots + 2^{n-1}$؛ سپس این را در برهان خود به کار برید.]

* * * * *

فصل دوم

همنهشتی در $\mathbb{Z}$ و حساب پیمانه‌ای

فصل حاضر پلی است بین حسابی که در فصل پیش مطالعه شد و مفاهیمی از جبر مجرد که در فصل بعدی معرفی می‌شود. در این فصل مفاهیم اساسی حساب به‌منظور شمول آنها بر مفهوم همنهشتی تعمیم‌داده شده است. رابطه همنهشتی منجر به ساختن مجموعه $\mathbb{Z}_n$ متشکل از همه کلاس‌های همنهشتی می‌شود. به‌علاوه این مطلب نخستین مثال ما از یک دستگاه حساب را ارائه می‌کند که در بسیاری از خواص اساسی با حساب معمولی مشترک بوده، در عین حال به‌طور قابل ملاحظه‌ای از آن متفاوت است.

۲-۱ همنهشتی و کلاس‌های همنهشتی

مفهوم "همنهشتی" می‌تواند به‌عنوان تعمیمی از رابطه برابری در نظر گرفته شود. دو عدد صحیح a و b برابرند اگر تفاضل آنها صفر باشد یا، به‌طور معادل، اگر تفاضل آنها مضربی از صفر باشد. اگر n

یک عدد صحیح مثبت باشد، دو عدد صحیح a و b را همنهشت به پیمانه n گوییم اگر تفاضل آنها مضربی از n باشد، یعنی برای برخی k، $a - b = nk$. این بدین معنی است که n تفاضل $a - b$ را می‌شمارد. بنابراین ما تعریف رسمی زیر را داریم:

تعریف. فرض کنید a، b، n اعداد صحیح باشند و $n > 0$. در این صورت a همنهشت با b به پیمانه n است [نوشته می‌شود "$a \equiv b$ (پیمانه n)"]، مشروط به این که n تفاضل $a - b$ را بشمارد.

مثال ۱.۲. $17 \equiv 5$ (پیمانه ۶) زیرا $12 = 5 - 17$، ۶ را می‌شمارد. بطور مشابه $25 \equiv 4$ (پیمانه ۷) زیرا $-21 = 4 - 25$، ۷ را می‌شمارد، و $-4 \equiv 6$ (پیمانه ۵) زیرا $10 = (-4) - 6$، ۵ را می‌شمارد.

تذکر. در نمایش "$a \equiv b$ (پیمانه n)"، نمادهای " $\equiv$ " و "(پیمانه n)" در واقع قسمتهایی از یک نماد واحد هستند، " $a \equiv b$ " به تنهایی بدون معنی است. در بعضی متون به جای "$a \equiv b$ (پیمانه n)" نماد "$a \equiv_n b$" نوشته می‌شود. گرچه این نمایش تک ـ نمادی مقرون به صرفه است، با این‌حال ما در این کتاب نماد سنتی "(پیمانه n)" را برگزیده‌ایم.

نماد بکار گرفته شده برای همنهشتی شباهت بسیار زیادی به علامت تساوی دارد. این امر اتفاقی نیست زیرا رابطه همنهشتی دارای بسیاری از همان خواصی است که رابطه برابری دارد. برای مثال می‌دانیم که رابطه برابری

انعکاسی: $a = a$ برای هر عدد صحیح a؛
متقارن: اگر $a = b$ در این صورت $b = a$؛
متعدی: اگر $a = b$ و $b = c$، در این صورت $a = c$؛

می‌باشد. اکنون می‌بینیم که رابطه همنهشتی به پیمانه n نیز، انعکاسی، متقارن و متعدی است.

قضیه ۱.۲. فرض کنید n یک عدد صحیح مثبت باشد. برای $a, b, c \in \mathbb{Z}$،

(۱) $a \equiv a$ (پیمانه n)؛
(۲) اگر $a \equiv b$ (پیمانه n)، در این صورت $b \equiv a$ (پیمانه n)؛
(۳) اگر $a \equiv b$ (پیمانه n) و $b \equiv c$ (پیمانه n)، در این صورت $a \equiv c$ (پیمانه n).

برهان. (۱) $a - a = 0$ و $n | 0$. بنابراین $a \equiv a$ (پیمانه n).

(۲) ($a \equiv b \ (n$ پیمانه) بدین معنی است که برای برخی عدد صحیح k، $a - b = nk$. بنابراین $b - a = -(a - b) = -nk = n(-k)$. اولین و آخرین قسمت این معادله بیان می‌کند که $n|(b - a)$. بنابراین $b \equiv a \ (n$ پیمانه).

(۳) اگر $a \equiv b \ (n$ پیمانه) و $b \equiv c \ (n$ پیمانه)، در این صورت به موجب تعریف همنهشتی، اعداد صحیح k و t وجود دارد به قسمی که $a - b = nk$ و $b - c = nt$. بنابراین

$$(a - b) + (b - c) = nk + nt$$

$$a - c = n(k + t).$$

در نتیجه $n|(a - c)$ و بنابراین $a \equiv c \ (n$ پیمانه). ■

بسیاری از عملیات بنیادی جبری و حسابی بستگی به این حقیقت کلیدی دارد که:

اگر $a = b$ و $c = d$، در این صورت $a + c = b + d$ و $ac = bd$.

اکنون نشان می‌دهیم که این مطلب عیناً برای مفهوم همنهشتی نیز درست است.

قضیه ۲.۲. اگر $a \equiv b \ (n$ پیمانه) و $c \equiv d \ (n$ پیمانه)، در این صورت

(۱) $a + c \equiv b + d \ (n$ پیمانه)؛

(۲) $ac \equiv bd \ (n$ پیمانه).

برهان. (۱) به موجب تعریف همنهشتی اعداد صحیح k و t وجود دارند به قسمی که $a - b = nk$ و $c - d = nt$. بنابراین

$$(a - b) + (c - d) = nk + nt$$

$$a + c - b - d = n(k + t)$$

$$(a + c) - (b + d) = n(k + t).$$

در نتیجه n، $(a + c) - (b + d)$ را می‌شمارد و لذا $a + c \equiv b + d \ (n$ پیمانه).

(۲) با استفاده از این حقیقت که $-bc + bc = 0$، داریم

$$ac - bd = ac + 0 - bd = ac - bc + bc - bd = (a - b)c + b(c - d)$$

$$= (nk)c + b(nt) = n(kc + bt).$$

اولین وآخرین قسمت این معادله بیان می‌کندکه $n|(ac-bd)$. بنابراین $ac \equiv bd (n$پیمانه$)$. ■

در مورد رابطه برابری، تنها عددی که با یک عدد داده شده a برابر است، خود a می‌باشد. امّا این موضوع در مورد همنهشتی متفاوت بوده و منجر به برخی نتایج جالب می‌شود.

تعریف. فرض کنید a و n اعداد صحیح باشند و $n > ۰$. **کلاس همنهشتی a به پیمانه n** (که با $[a]$ نشان داده می‌شود) عبارت از مجموعه همه اعداد صحیحی است که همنهشت با a به پیمانه n می‌باشد، یعنی

$$[a] = \{b \mid b \in \mathbb{Z}, b \equiv a (n \text{ پیمانه})\}$$

بیان این‌که $b \equiv a$ (n پیمانه) بدین معنی است که برای برخی عدد صحیح k، $b - a = kn$ یا به‌طور معادل $b = a + nk$. بنابراین

$$[a] = \{b \mid b \equiv a \ (n \text{ پیمانه}) \} = \{b \mid b = a + kn, k \in \mathbb{Z}\}$$
$$= \{a + kn \mid k \in \mathbb{Z}\}.$$

مثال ۲.۲. در همنهشتی به پیمانه ۵ داریم،

$$[۹] = \{۹ + ۵k \mid k \in \mathbb{Z}\} = \{۹, ۹ \pm ۵, ۹ \pm ۱۰, ۹ \pm ۱۵, \dots\}$$
$$= \{\dots, -۱۱, -۶, -۱, ۴, ۹, ۱۴, ۱۹, ۲۴, \dots\}.$$

مثال ۳.۲. نماد کلاس‌های همنهشتی به معنای واقعی کلمه نمادی دوپهلو می‌باشد. به‌عنوان مثال در همنهشتی به پیمانه ۳،

$$[۲] = \{۲ + ۳k \mid k \in \mathbb{Z}\} = \{\dots, -۷, -۴, -۱, ۲, ۵, ۸, \dots\},$$

امّا در همنهشتی به پیمانه ۵، کلاس همنهشتی $[۲]$ عبارت است از مجموعه

$$\{۲ + ۵k \mid k \in \mathbb{Z}\} = \{\dots, -۱۳, -۸, -۳, ۲, ۷, ۱۲, \dots\}.$$

این ابهام مشکلی را در آنچه که در پی می‌آید ایجاد نخواهد کرد، زیرا در هر زمان تنها یک پیمانه مورد بحث قرار می‌گیرد.

مثال ۴.۲. در همنهشتی به پیمانه ۳، کلاس همنهشتی ۲ عبارت است از $[۲] = \{\ldots, -۷, -۴, -۱, ۲, ۵, ۸, \ldots\}$. در عین حال توجه کنید که $[-۱]$ نیز همین کلاس است زیرا

$$[-۱] = \{-۱ + ۳k \mid k \in \mathbb{Z}\} = \{\ldots, -۷, -۴, -۱, ۲, ۵, \ldots\}.$$

به‌علاوه (پیمانه ۳) $-۱ \equiv ۲$. این امر مثالی از قضیه زیر است.

قضیه ۳.۲. (پیمانه n) $a \equiv c$ اگر و تنها اگر $[a] = [c]$.

مشاهده کنید که در اثبات این قضیه از تعریف همنهشتی استفاده‌ای نمی‌شود. در عوض در برهان تنها از این حقیقت استفاده می‌شود که رابطه همنهشتی، انعکاسی، متقارن و متعدی است (قضیه ۱.۲).

برهان قضیه ۳.۲. فرض کنید (پیمانه n) $a \equiv c$. به منظور اثبات $[a] = [c]$ ابتدا نشان می‌دهیم $[c] \subseteq [a]$. برای انجام این فرض کنید $b \in [a]$. پس به موجب تعریف (پیمانه n) $b \equiv a$. چون (پیمانه n) $a \equiv c$، بنا به تعدی بدست می‌آوریم (پیمانه n) $b \equiv c$. بنابراین $b \in [c]$ و لذا $[c] \subseteq [a]$. با تعویض نقش a و c در این استدلال و بکارگیری این حقیقت که بنابه تقارن (پیمانه n) $c \equiv a$، نشان دهید $[a] \subseteq [c]$. بنابراین $[a] = [c]$. بالعکس، فرض کنید $[c] = [a]$. چون به موجب خاصیت انعکاسی (پیمانه n) $a \equiv a$، داریم $a \in [a]$ و بنابراین $a \in [c]$. به موجب تعریف $[c]$، می‌بینیم که (پیمانه n) $a \equiv c$. ■

برای دو مجموعه A و C معمولاً سه امکان وجود دارد، یا A و C مجزا هستند، یا $A = C$ و یا $A \cap C$ غیر تهی است امّا $A \neq C$. با این حال در مورد کلاس‌های همنهشتی تنها دو امکان وجود دارد:

نتیجه ۴.۲. هر دو کلاس همنهشتی به پیمانه n یا مجزا هستند و یا برابرند.

برهان. اگر $[a]$ و $[c]$ مجزا باشند، چیزی برای اثبات باقی نمی‌ماند. فرض کنید که $[a] \cap [c]$ غیر تهی‌است. پس عدد صحیح b وجود دارد که $b \in [a]$ و $b \in [c]$. بنابه تعریف کلاس همنهشتی، (پیمانه n) $b \equiv a$ و (پیمانه n) $b \equiv c$. بنابراین بنا به تقارن و تعدی (پیمانه n) $a \equiv c$. پس

به‌موجب قضیه ۳.۲، $[a] = [c]$. ■

نتیجه ۵.۲. دقیقاً n کلاس همنهشتی متمایز به پیمانه n، یعنی $[0]$، $[1]$، $[2]$، ...، $[n-1]$ وجود دارد.

برهان. ابتدا ادعا می‌کنیم که هیچ دوتا از اعداد $0, 1, 2, \ldots, n-1$ همنهشت به پیمانه n نیستند. برای دیدن این فرض کنید که $0 \leq s < t < n$. در این صورت $t - s$ یک عدد صحیح مثبت و کوچکتر از n است. بنابراین $t - s$، n را نمی‌شمارد و لذا $t \not\equiv s$ (پیمانه n). چون هیچ دوتای $0, 1, 2, \ldots, n-1$ همنهشت نیستند، بنا به قضیه ۳.۲، کلاس‌های $[0]$، $[1]$، ...، $[n-1]$ متمایزند. برای کامل شدن برهان کافی است اثبات کنیم که هر کلاس همنهشتی یکی از این n کلاس می‌باشد. فرض کنید $a \in \mathbb{Z}$. بنابه الگوریتم تقسیم، $a = nq + r$ با $0 \leq r < n$. بنابراین $a - r = qn$، لذا $a \equiv r$ (پیمانه n). به موجب قضیه ۳.۲، $[a] = [r]$. چون $0 \leq r < n$، $[a]$ یکی از $[0]$، $[1]$، $[2]$، ...، $[n-1]$ می‌باشد. ■

تعریف. مجموعهٔ همهٔ کلاسهای همنهشتی به پیمانه n با $\mathbb{Z}_n$ (که خوانده می‌شود "$\mathbb{Z}$ به‌پیمانه n") نشان داده می‌شود.

در اینجا چند نکته وجود دارد که باید در مورد آنها دقت کرد. عناصر $\mathbb{Z}_n$ کلاس هستند و نه اعداد صحیح صرف. بنابراین گزارهٔ $[5] \in \mathbb{Z}_n$ درست است اما گزارهٔ $5 \in \mathbb{Z}_n$ درست نیست. به‌علاوه، هر عنصر $\mathbb{Z}_n$ به طرق بسیار مختلفی قابل نشان دادن است. برای مثال می‌دانیم که

$$۲ \equiv ۱۴ \text{ (پیمانه ۳)} \qquad ۲ \equiv -۱ \text{ (پیمانه ۳)} \qquad ۲ \equiv ۵ \text{ (پیمانه ۳)}.$$

بنابراین، به‌موجب قضیه ۳.۲، $[14] = [-1] = [5] = [2]$ در $\mathbb{Z}_3$. گرچه هر عنصر $\mathbb{Z}_n$ (یعنی هر کلاس همنهشتی) دارای تعداد نامتناهی نمایش متفاوت است، اما به موجب نتیجه ۵.۲ که در واقع مبین این است که مجموعهٔ $\mathbb{Z}_n$ دارای دقیقاً n عنصر است، تنها تعداد متناهی کلاس‌های متمایز وجود دارد.

مثال ۵.۲. مجموعهٔ $\mathbb{Z}_3$ متشکل از سه عنصر $[0]$، $[1]$ و $[2]$ می‌باشد.

تمرینها

۱.A. ثابت کنید (پیمانه n) $a \equiv b$ اگر و تنها اگر باقیمانده تقسیم a و b بر n یکسان باشد.

۲. اگر (پیمانه n) $a \equiv b$ و $k|n$، ثابت کنید (پیمانه k) $a \equiv b$.

۳. اگر (پیمانه ۴) $k \equiv ۱$، در این صورت (پیمانه ۴)؟$\equiv ۶k + ۵$.

۴. ثابت کنید که هر عدد فرد اول همنهشت با ۱ یا با ۳ به پیمانه ۴ است.

۵. اگر $a \in \mathbb{Z}$، ثابت کنید که $a^۲$ همنهشت با ۲ یا با ۳ به پیمانه ۴ نیست.

۶. ثابت کنید که (پیمانه n) $a \equiv b$ اگر و تنها اگر (پیمانه $n^۲$) $a^۲ + b^۲ \equiv ۲ab$.

۷. اگر a و b اعداد صحیحی باشند به قسمی که برای هر عدد اول مثبت p، (پیمانه p) $a \equiv b$ ثابت کنید $a = b$.

۸. اگر $a, m, n \in \mathbb{Z}$ که در آن $m > ۰$ و $n > ۰$، ثابت کنید $[a^m] = [a^n]$ در $\mathbb{Z}_۲$. [راهنمایی: قضیه ۳.۲.]

۹. ثابت کنید

(الف) (پیمانه n) $(n - a)^۲ \equiv a^۲$ (ب) (پیمانه $۴n$) $(۲n - a)^۲ \equiv a^۲$.

۱۰. برای p و a داده شده، نشان دهید که (پیمانه p) $a^{p-۱} \equiv ۱$:

(الف) $a = ۲$، $p = ۵$ (ب) $a = ۴$، $p = ۷$ (پ) $a = ۳$، $p = ۱۱$

۱۱. همه جوابهای هر یک از این همنهشتی‌ها را بیابید:

(الف) (پیمانه ۵) $۲x \equiv ۳$ (ب) (پیمانه ۷) $۳x \equiv ۱$

(پ) (پیمانه ۱۵) $۶x \equiv ۹$ (ت) (پیمانه ۱۵) $۶x \equiv ۱۰$

۱۲. کدام یک از همنهشتی‌های زیر دارای جواب است:

(الف) (پیمانه ۳) $x^۲ \equiv ۱$ (ب) (پیمانه ۷) $x^۲ \equiv ۲$ (پ) (پیمانه ۱۱) $x^۲ \equiv ۳$

۱۳. (الف) اگر (پیمانه $۲n$) $a \equiv b$، ثابت کنید که (پیمانه $۴n$) $a^۳ \equiv b^۳$

(ب) اگر (پیمانه $۳n$) $a \equiv b$، ثابت کنید که (پیمانه $۳n$) $a^۳ \equiv b^۳$.

۱۴. اگر $p \geq ۵$ و p اول باشد، ثابت کنید که $[۱] = [p]$ یا $[۵] = [p]$ در $\mathbb{Z}_۶$. [راهنمایی: قضیه ۳.۲ و نتیجه ۵.۲.]

۱۵. اگر (پیمانه ۴) $a \equiv ۳$، ثابت کنید که هیچ دو عدد صحیح c و d وجود ندارد به قسمی که $a = c^۲ + d^۲$.

۱۶. اگر (پیمانه ۴) $a \equiv ۲$، ثابت کنید که هیچ دو عدد صحیح c و d وجود ندارد به قسمی که $a = c^۲ - d^۲$.

۱۷. (الف) اگر a یک عدد صحیح غیرمنفی باشد، ثابت کنید که a همنهشت با آخرین رقمش به پیمانه ۱۰ می‌باشد [برای مثال (پیمانه ۱۰) $۷ \equiv ۲۷$].
(ب) ثابت کنید که هیچ مربع کاملی دارای آخرین رقم ۲، ۳، ۷ یا ۸ نمی‌باشد.

۱۸. اگر $a \in \mathbb{Z}$، ثابت کنید که آخرین رقم $a^۲$ یکی از اعداد ۰، ۱، ۵ یا ۶ است. [راهنمایی: تمرین ۱۷ را ملاحظه کنید.]

۱۹.B. (الف) رد یا اثبات کنید: اگر (پیمانه n) $a^۲ \equiv b^۲$، در این صورت (پیمانه n) $a \equiv b$ یا (پیمانه n) $a \equiv -b$.
(ب) قسمت (الف) را وقتی n اول است انجام دهید.

۲۰. اگر $[a] = [۱]$ در $\mathbb{Z}_n$، ثابت کنید که $(a, n) = ۱$. با مثال نشان دهید که عکس این مطلب ممکن است غلط باشد.

۲۱. اگر $[a] = [b]$ در $\mathbb{Z}_n$، ثابت کنید که $(a, n) = (b, n)$.

۲۲. اگر (پیمانه ۲) $a^۲ \equiv ۱$، ثابت کنید که (پیمانه ۴) $a^۲ \equiv ۱$.

۲۳. (الف) نشان دهید که برای هر عدد صحیح مثبت n، (پیمانه ۹) $۱۰^n \equiv ۱$.
(ب) نشان دهید که هر عدد صحیح مثبت همنهشت با مجموع ارقامش به پیمانه ۹ می‌باشد. [برای مثال (پیمانه ۹) $۳۸ \equiv ۱۱$].

۲۴. با استفاده از همنهشتی‌ها (و نه یک ماشین حساب)، نشان دهید که

$$(۱۲۵۶۹۸)(۲۳۷۹۷) \neq ۲۸۹۱۲۳۵۳۰۶.$$

[راهنمایی: تمرین ۲۳ را ملاحظه کنید.]

۲۵. ثابت کنید که برای هر عدد صحیح مثبت n، (پیمانه ۱۱) $۱۰^n \equiv (-۱)^n$.

۲۶. (الف) با ارائه مثالی نشان دهید که گزاره زیر غلط است: اگر $ab \equiv ac \pmod{n}$ و $a \not\equiv 0 \pmod{n}$، در این صورت $b \equiv c \pmod{n}$.
(ب) ثابت کنید که گزاره قسمت (الف) در حالتی‌که $(a, n) = 1$ درست است.

۲۷. (الف) رد یا اثبات کنید: اگر $ab \equiv 0 \pmod{n}$، در این صورت $a \equiv 0 \pmod{n}$ یا $b \equiv 0 \pmod{n}$.
(ب) قسمت (الف) را وقتی که n اول است انجام دهید.

۲۸. (الف) اگر $a \equiv b \pmod{rs}$ ثابت کنید که $a \equiv b \pmod{r}$.
(ب) اگر $a \equiv c \pmod{r}$ و $c \equiv b \pmod{s}$، ثابت کنید که $a \equiv b \pmod{(r, s)}$.

۲۹. اگر $a^2 \equiv 6 \pmod{10}$، ثابت کنید که $a^2 - 6 \equiv 10 \pmod{20}$.

۳۰. ثابت کنید که $a^5 \equiv a \pmod{30}$ برای هر عدد صحیح a.

۳۱. اگر $(a, n) = 1$، ثابت کنید که عدد صحیح b وجود دارد به قسمی که $ab \equiv 1 \pmod{n}$.

۳۲. فرض کنید a، b و n اعداد صحیحی باشند با $n > 0$. اگر (a, n)، b را نشمارد، ثابت کنید که همنهشتی $ax \equiv b \pmod{n}$ دارای هیچ جوابی نیست.

۳۳.C اگر $(a, n) = 1$، ثابت کنید که همنهشتی $ax \equiv b \pmod{n}$ دارای دقیقاً یک جواب t است به قسمی که $0 \leq t < n$.

۲-۲ حساب پیمانه‌ای

مجموعه متناهی $\mathbb{Z}_n$ رابطه تنگاتنگی با مجموعه نامتناهی $\mathbb{Z}$ دارد. بنابراین طبیعی است سؤال شود که آیا می‌توان به شکلی جمع و ضرب را در $\mathbb{Z}_n$ تعریف کرد و نوعی از حساب قابل قبول را در آن انجام داد. برای تعریف جمع در $\mathbb{Z}_n$ باید راهی برای برداشتن دو کلاس از $\mathbb{Z}_n$ و ایجاد کلاسی دیگر، مجموع آنها، پیدا نمود. چون جمع اعداد صحیح تعریف شده است، به‌نظر می‌رسد تعریف پیشنهادی زیر ارزش بررسی را داشته باشد:

مجموع کلاس‌های $[a]$ و $[c]$ کلاسی است که $a + c$ را شامل باشد، یا به‌طور نمادین

$$[a] \oplus [c] = [a + c],$$

جایی که جمع کلاسها با $\oplus$ نشان داده شده‌است تا از جمع معمولی اعداد صحیح متمایز باشد.

می‌توانیم تعریف آزمایشی مشابهی را برای ضرب امتحان کنیم:

حاصلضرب $[a]$ و $[c]$ کلاسی است که ac را شامل باشد:

$$[a] \odot [c] = [ac],$$

جایی که $\odot$ ضرب کلاسها را نشان می‌دهد.

مثال ۶.۲. در $\mathbb{Z}_5$ برابری‌های زیر برقرار است: $[2] = [7] = [3 + 4] = [3] \oplus [4]$ و $[1] = [6] = [2 \times 3] = [2] \odot [3]$. تا اینجا به‌نظر می‌رسد که همه چیز خوب کار می‌کند، امّا یک مشکل احتمالی وجود دارد. هر عنصر $\mathbb{Z}_n$ می‌تواند به طرق بسیار زیادی نوشته شود. برای مثال در $\mathbb{Z}_5$، $[13] = [3]$ و $[9] = [4]$. در مثال قبلی، دیدیم که در $\mathbb{Z}_5$، $[2] = [4] + [3]$. آیا اگر ما $[13]$ را به جای $[3]$ و $[9]$ را به جای $[4]$ بکار ببریم به همان جواب می‌رسیم؟ در این حالت جواب "مثبت" است زیرا

$$[13] \oplus [9] = [13 + 9] = [22] = [2]$$

امّا چگونه بدانیم که در حالت کلی جواب، صرف نظر از این که کلاسها را به چه طریقی نمایش دهیم همواره همان خواهد بود؟

برای به‌دست آوردن ایده‌ای از این‌که چه چیزهایی ممکن است در عمل نادرست درآید، پنج کلاس زیر از اعداد صحیح را در نظر بگیرید:

$$A = \{\ldots, -14, -8, -2, 4, 6, 12, 18, \ldots\},$$
$$B = \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\},$$
$$C = \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\},$$
$$D = \{\ldots, -16, -10, -4, 2, 8, 14, 20, \ldots\},$$
$$E = \{\ldots, -18, -12, -6, 4, 10, 16, 22, \ldots\}.$$

این کلاسها، مشابه کلاسهایی در $\mathbb{Z}_5$، دارای خواص بنیادی زیر هستند: هر عدد صحیح در یکی از آنها قرار دارد و هر دو تای از آنها مجزا و یا برابرند. چون ۱ در B است و ۷ در C، می‌توانیم

$B+C$ را به‌عنوان کلاسی که $۸ = ۷ + ۱$ را شامل است، تعریف کنیم، یعنی $B+C=D$. امّا B همچنین کلاسی است که -۳ را شامل است و C کلاسی است که ۱۵ را شامل است، و لذا $B+C$ باید کلاسی باشد که $۱۲ = ۱۵ + ۳-$ را شامل است. امّا ۱۲ در A است و لذا $B+C=A$. بنابراین برحسب این‌که چه "نماینده‌هایی" از کلاس‌های B و C انتخاب کنید به جوابهای متفاوتی می‌رسید. به‌وضوح نمی‌توانید مفهوم معنی‌داری از جمع داشته باشید وقتی که این بار به یک جواب و وقت دیگر به جواب دیگری برسید.

به منظور حذف کلمه "پیشنهادی" از تعریف جمع و ضرب در $\mathbb{Z}_n$، ابتدا باید ثابت کنیم که این دو عمل، مستقل از انتخاب نمایندهٔ کلاس‌های مختلف می‌باشد. آنچه که لازم است در قضیه زیر آمده است:

قضیه ۶.۲. اگر $[b]=[a]$ و $[c]=[d]$ در $\mathbb{Z}_n$، در این صورت

$$[a+c]=[b+d] \quad \text{و} \quad [ac]=[bd].$$

برهان. چون $[b]=[a]$، می‌دانیم که به موجب قضیه ۳.۲، (پیمانه n) $a \equiv b$. به‌طور مشابه $[c]=[d]$ نتیجه می‌دهد (پیمانه n) $c \equiv d$. بنابراین به موجب قضیه ۲.۲،

$$\text{(پیمانه } n\text{) } a+c \equiv b+d \quad \text{و} \quad \text{(پیمانه } n\text{) } ac \equiv bd.$$

مجدداً بنابه قضیه ۳.۲،

$$[a+c]=[b+d] \quad \text{و} \quad [ac]=[bd]. \qquad \blacksquare$$

بنابه قضیه ۶.۲، می‌دانیم که تعریف رسمی زیر از جمع و ضرب مستقل از انتخاب نماینده هر کلاس می‌باشد:

تعریف. جمع و ضرب در $\mathbb{Z}_n$ توسط

$$[a] \oplus [c] = [a+c] \quad \text{و} \quad [a] \odot [c] = [ac]$$

تعریف می‌شود.

مثال ۷.۲. جداول کامل مربوط به جمع و ضرب[۱] برای $\mathbb{Z}_۵$ در زیر آمده است (بررسی کنید که این محاسبات صحیح هستند):

$\oplus$	$[۰]$	$[۱]$	$[۲]$	$[۳]$	$[۴]$
$[۰]$	$[۰]$	$[۱]$	$[۲]$	$[۳]$	$[۴]$
$[۱]$	$[۱]$	$[۲]$	$[۳]$	$[۴]$	$[۰]$
$[۲]$	$[۲]$	$[۳]$	$[۴]$	$[۰]$	$[۱]$
$[۳]$	$[۳]$	$[۴]$	$[۰]$	$[۱]$	$[۲]$
$[۴]$	$[۴]$	$[۰]$	$[۱]$	$[۲]$	$[۳]$

$\odot$	$[۰]$	$[۱]$	$[۲]$	$[۳]$	$[۴]$
$[۰]$	$[۰]$	$[۰]$	$[۰]$	$[۰]$	$[۰]$
$[۱]$	$[۰]$	$[۱]$	$[۲]$	$[۳]$	$[۴]$
$[۲]$	$[۰]$	$[۲]$	$[۴]$	$[۱]$	$[۳]$
$[۳]$	$[۰]$	$[۳]$	$[۱]$	$[۴]$	$[۲]$
$[۴]$	$[۰]$	$[۴]$	$[۳]$	$[۲]$	$[۱]$

و جداول مربوط به $\mathbb{Z}_۶$ نیز در زیر آمده‌است:

$\oplus$	$[۰]$	$[۱]$	$[۲]$	$[۳]$	$[۴]$	$[۵]$
$[۰]$	$[۰]$	$[۱]$	$[۲]$	$[۳]$	$[۴]$	$[۵]$
$[۱]$	$[۱]$	$[۲]$	$[۳]$	$[۴]$	$[۵]$	$[۰]$
$[۲]$	$[۲]$	$[۳]$	$[۴]$	$[۵]$	$[۰]$	$[۱]$
$[۳]$	$[۳]$	$[۴]$	$[۵]$	$[۰]$	$[۱]$	$[۲]$
$[۴]$	$[۴]$	$[۵]$	$[۰]$	$[۱]$	$[۲]$	$[۳]$
$[۵]$	$[۵]$	$[۰]$	$[۱]$	$[۲]$	$[۳]$	$[۴]$

۱) این جداول به‌صورت زیر خوانده می‌شوند: اگر برای مثال $[a]$ در ستون عمودی سمت چپ و $[c]$ در ردیف افقی بالای جدول جمع ظاهر شود، در این صورت مجموع $[c] \oplus [a]$ در مقطع ردیف افقی شامل $[a]$ و ردیف عمودی شامل $[c]$ ظاهر می‌شود.

$\odot$	$[۰]$	$[۱]$	$[۲]$	$[۳]$	$[۴]$	$[۵]$
$[۰]$	$[۰]$	$[۰]$	$[۰]$	$[۰]$	$[۰]$	$[۰]$
$[۱]$	$[۰]$	$[۱]$	$[۲]$	$[۳]$	$[۴]$	$[۵]$
$[۲]$	$[۰]$	$[۲]$	$[۴]$	$[۰]$	$[۲]$	$[۴]$
$[۳]$	$[۰]$	$[۳]$	$[۰]$	$[۳]$	$[۰]$	$[۳]$
$[۴]$	$[۰]$	$[۴]$	$[۲]$	$[۰]$	$[۴]$	$[۲]$
$[۵]$	$[۰]$	$[۵]$	$[۴]$	$[۳]$	$[۲]$	$[۱]$

حال که جمع و ضرب در $\mathbb{Z}_n$ تعریف شده است، مایلیم تا خواص این "حساب‌های ظریف" را با خواص شناخته شده $\mathbb{Z}$ مقایسه کنیم. حقایق کلیدی در مورد حساب در $\mathbb{Z}$ (و عناوین متداول برای این خواص) در زیر آمده‌است. برای $a, b, c \in \mathbb{Z}$:

۱. اگر $a, b \in \mathbb{Z}$، در این صورت $a + b \in \mathbb{Z}$. [بسته بودن جمع]

۲. $a + (b + c) = (a + b) + c$. [شرکت‌پذیری جمع]

۳. $a + b = b + a$. [جابجایی جمع]

۴. $a + ۰ = ۰ + a = a$. [همانی جمعی]

۵. برای هر $a \in \mathbb{Z}$، معادله $a + x = ۰$ دارای یک جواب در $\mathbb{Z}$ است.

۶. اگر $a, b \in \mathbb{Z}$، در این صورت $ab \in \mathbb{Z}$. [بسته‌بودن ضرب]

۷. $(ab)c = a(bc)$. [شرکت‌پذیری ضرب]

۸. $a(b + c) = ab + ac$ و $(a + b)c = ac + bc$. [قوانین توزیع‌پذیری]

۹. $ab = ba$ [جابجایی ضرب]

۱۰. $a.۱ = a = ۱.a$ [همانی ضربی]

۱۱. اگر $ab = ۰$، در این صورت $a = ۰$ یا $b = ۰$.

با استفاده از جداول ارائه شده در مثال بالا، می‌توانید بررسی کنید که ۱۰ خاصیت اوّل بالا در $\mathbb{Z}_۵$ و $\mathbb{Z}_۶$ برقرار است امّا خاصیت ۱۱ در $\mathbb{Z}_۵$ برقرار و در $\mathbb{Z}_۶$ برقرار نیست. امّا استفاده از جداول، یک روش مؤثر اثبات (بویژه برای بررسی شرکت‌پذیری و توزیع‌پذیری) نیست. بنابراین اثبات این که خواص ۱۰-۱ برای هر $\mathbb{Z}_n$ برقرار است بر مبنای تعریف دو عمل جمع و ضرب در $\mathbb{Z}_n$ و این حقیقت که اعتبار این خواص در $\mathbb{Z}$ شناخته شده‌اند بنا شده است.

قضیه ۷.۲. برای همه کلاس‌های $[a]$، $[b]$، $[c]$ در $\mathbb{Z}_n$،

۱. اگر $[a] \in \mathbb{Z}_n$ و $[b] \in \mathbb{Z}_n$، در این صورت $[a] \oplus [b] \in \mathbb{Z}_n$.

۲. $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$.

۳. $[a] \oplus [b] = [b] \oplus [a]$.

۴. $[a] \oplus [0] = [a] = [0] \oplus [a]$.

۵. برای هر $[a] \in \mathbb{Z}_n$، معادله $[a] \oplus X = [0]$ دارای یک جواب در $\mathbb{Z}_n$ است.

۶. اگر $[a] \in \mathbb{Z}_n$ و $[b] \in \mathbb{Z}_n$، در این صورت $[a] \odot [b] \in \mathbb{Z}_n$.

۷. $[a] \odot ([b] \odot [c]) = ([a] \odot [b]).[c]$.

۸. $([a] \oplus [b]) \odot [c] = ([a] \odot [c]) \oplus ([b] \odot [c])$ و $[a] \odot ([b] \oplus [c]) = ([a] \odot [b]) \oplus ([a] \odot [c])$.

۹. $[a] \odot [b] = [b] \odot [a]$.

۱۰. $[a] \odot [1] = [a] = [1] \odot [a]$.

برهان. خواص ۱ و ۶ نتیجه فوری تعریف $\oplus$ و $\odot$ در $\mathbb{Z}_n$ هستند. برای اثبات ۲ توجه کنید که بنا به تعریف جمع

$$[a] \oplus ([b] \oplus [a]) = [a] \oplus [b + c] = [a + (b + c)].$$

می‌دانیم که در $\mathbb{Z}$، $a + (b + c) = (a + b) + c$. بنابراین کلاس‌های این اعداد صحیح باید در $\mathbb{Z}_n$ یکسان باشد؛ یعنی، $[a + (b + c)] = [(a + b) + c]$. بنابه تعریف جمع در $\mathbb{Z}_n$ داریم

$$[(a + b) + c] = [a + b] \oplus [c] = ([a] \oplus [b]) \oplus [c].$$

این امر ۲ را اثبات می‌کند. اثباتهای ۳، ۷، ۸ و ۹ مشابهند (تمرین ۴). خواص ۴ الی ۱۰ با محاسبه مستقیم اثبات می‌شوند؛ برای مثال $[a].[1] = [a] \odot [1]$. برای خاصیت ۵، به‌سادگی می‌توان دید که $X = [-a]$ یک جواب معادله است زیرا $[a] \oplus [-a] = [a + (-a)] = [0]$. ■

نمادگذاری جدید

ما دقت زیادی کرده‌ایم تا اعداد صحیح در $\mathbb{Z}$ و کلاس‌های در $\mathbb{Z}_n$ را متمایز کنیم و نمادهای متفاوتی برای اعمال جمع و ضرب در این دو دستگاه بکار برده‌ایم. با این‌حال، باید تاکنون به‌طور

نسبی با مفاهیم بنیادیِ $\mathbb{Z}_n$ احساس راحتی کرده، با حساب در آن آشنا شده باشید. بنابراین ما نماد جدیدی را که به‌طور وسیعی در ریاضیات بکار می‌رود خواهیم پذیرفت. این نماد جدید گرچه دارای این عیب است که در آنِ واحد دو کلاس کاملاً متفاوت از پدیده‌ها را نمایش می‌دهد ولی بعید است که هیچگونه ابهامی را در روند کار به‌وجود آورد.

هرگاه از متن واضح باشد که ما با $\mathbb{Z}_n$ سروکار داریم، ما نماد کلاسی "$[a]$" را خلاصه کرده و به‌سادگی می‌نویسیم "a". برای مثال در $\mathbb{Z}_۶$، می‌توانیم بگوییم $۶ = ۰$ که یقیناً برای کلاس‌های در $\mathbb{Z}_۶$ صحیح است، گرچه این مطلب بی‌معنی است اگر ۰ و ۶ به‌عنوان اعداد صحیح معمولی در نظر گرفته شوند. ما علامت جمع معمولی را برای جمع در $\mathbb{Z}_n$، و "یک نقطه کوچک[۲]" و یا "کنار هم قراردادن" را برای ضرب بکار می‌بریم. برای مثال، ممکن است در $\mathbb{Z}_۵$ بنویسیم

$$۴ + ۱ = ۰ \quad \text{یا} \quad ۴ \times ۴ = ۱ \quad \text{یا} \quad ۴ + ۴ = ۳.$$

در موارد نادری که این نماد ممکن است باعث سردرگمی شود، مجدداً نماد کروشه را بکار خواهیم برد.

مثال ۸.۲. در این نماد جدید، جداول جمع و ضرب برای $\mathbb{Z}_۳$ عبارتند از

+	۰	۱	۲
۰	۰	۱	۲
۱	۱	۲	۰
۲	۲	۰	۱

·	۰	۱	۲
۰	۰	۰	۰
۱	۰	۱	۲
۲	۰	۲	۱

همان نماد نمایی (توان) که در حساب معمولی بکار می‌رود، نماد مناسبی در $\mathbb{Z}_n$ نیز هست. اگر $a \in \mathbb{Z}_n$ و k یک عدد صحیح مثبت باشد، در این صورت a^k، حاصل‌ضرب $aaa\cdots a$ (k مرتبه) در $\mathbb{Z}_n$ را نشان می‌دهد.

مثال ۹.۲. در $\mathbb{Z}_۵$، $۳^۲ = ۳ \times ۳ = ۴$ و $۳^۴ = ۳ \times ۳ \times ۳ \times ۳ = ۱$.

دقّت کنید نماها اعداد صحیح معمولی هستند ـ نه عناصر $\mathbb{Z}_n$. برای مثال، در $\mathbb{Z}_۳$، $۲^۴ = ۲ \times ۲ \times ۲ \times ۲ = ۱$ و $۲^۱ = ۲$، لذا $۲^۱ \neq ۲^۴$ گرچه $۴ = ۱$ در $\mathbb{Z}_۳$.

---

۲) پاورقی مترجم: در نگارش فارسی، گاهی برای ضرب نماد " $\times$ " به‌جای نماد نقطه کوچک " $\cdot$ " بکار می‌رود.

تمرینها

A.۱. جداول جمع و ضرب را در موراد زیر بنویسید:

(الف) $\mathbb{Z}_۲$ (ب) $\mathbb{Z}_۴$ (پ) $\mathbb{Z}_۷$ (ت) $\mathbb{Z}_{۱۲}$

۲. مجموعه $\mathbb{Z}_n$ تنها n عضو را شامل است. برای حل یک معادله در $\mathbb{Z}_n$، کافی است که این n عنصر را در معادله جایگذاری کرده تا ببینید کدام یک جواب است. این معادلات را حل کنید:

(الف) $x^۲ = ۱$ در $\mathbb{Z}_۸$ (ب) $x^۴ = ۱$ در $\mathbb{Z}_۵$

(پ) $x^۲ + ۳x + ۲ = ۰$ در $\mathbb{Z}_۶$ (ت) $x^۲ + ۱ = ۰$ در $\mathbb{Z}_{۱۲}$

۳. (الف) عضوی از $\mathbb{Z}_۷$ را چنان بیابید که هر عضو $\mathbb{Z}_۷$، توانی از a باشد.

(ب) قسمت (الف) را در $\mathbb{Z}_۵$ انجام دهید.

(پ) آیا می‌توانید قسمت (الف) را در $\mathbb{Z}_۶$ انجام دهید؟

۴. قسمتهای ۳، ۷، ۸ و ۹ از قضیه ۷.۲ را ثابت کنید.

۵. (الف) معادله $x + x + x + x + x = ۰$ را در $\mathbb{Z}_۵$ حل کنید.

(ب) معادله $x + x + x = ۰$ را در $\mathbb{Z}_۳$ حل کنید.

(پ) معادله $x + x + x + x = ۰$ را در $\mathbb{Z}_۴$ حل کنید.

۶. رد یا اثبات کنید: اگر $ab = ۰$ در $\mathbb{Z}_n$، در این صورت $a = ۰$ یا $b = ۰$.

۷. رد یا اثبات کنید: اگر $ab = ac$ و $a \neq ۰$ در $\mathbb{Z}_n$، در این صورت $b = c$.

B.۸. (الف) معادله $x^۲ + x = ۰$ را در $\mathbb{Z}_۵$ حل کنید.

(ب) معادله $x^۲ + x = ۰$ را در $\mathbb{Z}_۶$ حل کنید.

(پ) اگر p اول باشد، ثابت کنید تنها جوابهای معادله $x^۲ + x = ۰$ در $\mathbb{Z}_p$ عبارتند از ۰ و $p - ۱$.

۹. (الف) $(a + b)^۵$ را در $\mathbb{Z}_۵$ محاسبه کنید. [راهنمایی: تمرین ۵ (الف) می‌تواند مفید باشد.]

(ب) $(a + b)^۳$ را در $\mathbb{Z}_۳$ محاسبه کنید. [راهنمایی: تمرین ۵ (ب) را ملاحظه کنید.]

(پ) $(a + b)^۲$ را در $\mathbb{Z}_۲$ محاسبه کنید.

(ت) براساس نتایج قسمتهای (الف) ـ (پ)، فکر می‌کنید $(a + b)^۷$ برابر با چه در $\mathbb{Z}_۷$ است؟

۱۰. (الف) همه عناصر a در $\mathbb{Z}_5$ را که برای آنها معادله $ax = 1$ دارای جواب است بیابید. همین مطلب را برای موارد زیر انجام دهید:

(ب) $\mathbb{Z}_4$ (پ) $\mathbb{Z}_3$ (ت) $\mathbb{Z}_6$.

۱۱. ترتیب معمولی $\mathbb{Z}$ توسط $<$، متعدی است و نسبت به جمع خوش‌رفتار می‌باشد. نشان دهید که هیچ ترتیبی روی $\mathbb{Z}_n$ وجود ندارد که در دو شرط زیر صدق کند:

(الف) اگر $a < b$ و $b < c$، در این صورت $a < c$؛

(ب) اگر $a < b$، در این صورت برای هر $c \in \mathbb{Z}_n$، $a + c < b + c$.

[راهنمایی: اگر چنین ترتیبی وجود داشته باشد با $1 > 0$، در این صورت به موجب (ب) اضافه کردن مکرر ۱ به هر دو طرف، نشان می‌دهد که $0 < 1 < 2 < \cdots < n - 1$. بنابراین به موجب (الف)، $n - 1 < 1$. به دو طرف ۱ را اضافه کرده و به یک تناقض برسید. استدلال مشابهی برای حالت $1 > 0$ بکار برید.]

۲-۳ ساختار $\mathbb{Z}_p$ وقتی که p اوّل است

بعضی از $\mathbb{Z}_n$ها همه خواص خوب $\mathbb{Z}$ را ندارند. برای مثال حاصل ضرب اعداد صحیح غیرصفر در $\mathbb{Z}$ همواره غیرصفر است، امّا در $\mathbb{Z}_6$ داریم $2 \times 3 = 0$، گرچه که $2 \neq 0$ و $3 \neq 0$. از طرف دیگر جدول ضرب در مثال ۷.۲ نشان می‌دهد که حاصل‌ضرب عناصر غیرصفر در $\mathbb{Z}_5$ همواره غیرصفر است. در واقع $\mathbb{Z}_5$ دارای یک خاصیت بسیار قوی‌تر از $\mathbb{Z}$ است. وقتی $a \neq 0$، معادله $ax = 1$ دارای یک جواب در $\mathbb{Z}$ است اگر و تنها اگر $a = \pm 1$. امّا جدول ضرب $\mathbb{Z}_5$ نشان می‌دهد که برای هر $a \neq 0$، معادله $ax = 1$ دارای یک جواب در $\mathbb{Z}_5$ است؛ برای مثال

$x = 3$ یک جواب $2x = 1$ است،

$x = 4$ یک جواب $4x = 1$ است.

به‌طورکلی‌تر، هرگاه n اوّل باشد $\mathbb{Z}_n$ دارای خواص ویژه‌ای است:

قضیه ۸.۲. اگر $p > 1$ یک عدد صحیح باشد، در این صورت شرایط زیر معادلند[۳]:

۳) برای معنی "شرایط زیر معادلند" و این که چه چیزی باید برای اثبات چنین گزاره‌ای انجام شود، به پیوست الف مراجعه کنید.

(۱) p اول است.

(۲) برای هر a غیرصفر در $\mathbb{Z}_p$، معادله $ax = ۱$ دارای یک جواب در $\mathbb{Z}_p$ است.

(۳) هرگاه $ab = ۰$ در $\mathbb{Z}_p$، در این صورت $a = ۰$ یا $b = ۰$.

اثبات این قضیه دو راهکار اساسی برای اثبات گزاره‌هایی که حساب در $\mathbb{Z}_n$ را شامل می‌شوند نشان می‌دهد:

(i) معادلات در $\mathbb{Z}_n$ را به گزاره‌های همنهشتی معادل در $\mathbb{Z}$ ترجمه کنید. در این صورت خواص همنهشتی و حسابی $\mathbb{Z}$ می‌تواند مورد استفاده قرار گیرد. برای پرهیز از سردرگمی و اشتباه ممکن است استفاده از نماد کروشه ضروری باشد.

(ii) خواص حسابی $\mathbb{Z}_n$ را بدون دخالت دادن خواص حسابی $\mathbb{Z}$ بکار برید. در این حالت استفاده از نماد کروشه در $\mathbb{Z}_n$ لازم نیست.

برهان قضیه ۸.۲. (۱)$\Leftarrow$ (۲) ما راهکار اول را بکار می‌بریم. فرض کنید p اول باشد و $[۰] \neq [p]$ در $\mathbb{Z}_p$. در این صورت به موجب قضیه ۳.۲، در $\mathbb{Z}$، (پیمانه p) $a \not\equiv ۰$. لذا بنابه تعریف همنهشتی، $p \nmid a$. حال بم‌م a و p یک شمارنده مثبت p است و بنابراین باید برابر p یا ۱ باشد. چون (a,p) یک شمارنده a نیز هست و $p \nmid a$، باید $(a,p) = ۱$. به موجب قضیه ۳.۱، برای برخی اعداد صحیح u و v داریم، $au + pv = ۱$. بنابراین $au - ۱ = p(-v)$، لذا (پیمانه p) $au \equiv ۱$. پس به موجب قضیه ۳.۲، $[au] = [۱]$ در $\mathbb{Z}_p$. بنابراین $[a][u] = [au] = [۱]$، پس $x = [u]$ یک جواب $[a]x = [۱]$ است.

(۲) $\Leftarrow$ (۳) ما راهکار دوّم را بکار می‌بریم. فرض کنید $ab = ۰$ در $\mathbb{Z}_p$. اگر $a = ۰$، چیزی برای اثبات وجود ندارد. اگر $a \neq ۰$، در این صورت به موجب (۲)، عضو $u \in \mathbb{Z}_p$ وجود دارد به قسمی که $au = ۱$. در این صورت

$$۰ = u \cdot ۰ = u(ab) = (ua)b = ۱ \cdot b = b.$$

بنابراین در هر حالت داریم $a = ۰$ یا $b = ۰$.

(۳) $\Leftarrow$ (۱) به راهکار اول برمی‌گردیم. فرض کنید a هر شمارنده‌ای از p باشد، مثلاً $p = ab$. برای اثبات این که p اول است، باید نشان دهیم که $a = \pm ۱$ یا $a = \pm p$. حال $p = ab$ نتیجه می‌دهد که (پیمانه p) $ab \equiv ۰$، لذا به موجب قضیه ۳.۲، $[a][b] = [ab] = [۰]$ در $\mathbb{Z}_p$. در این صورت به موجب (۳)، یا $[a] = [۰]$ یا $[b] = [۰]$. اینک از برابری $[a] = [۰]$ نتیجه می‌گیریم که

(پیمانه p) $a \equiv 0$، لذا $p|a$، مثلاً $a = pw$. بنابراین $p = ab = pwb$. تقسیم دوطرف بر p نشان می‌دهد که $wb = 1$. چون w و b اعداد صحیح هستند، تنها احتمال این است که $w = \pm 1$ و $b = \pm 1$. بنابراین $b = \pm 1$ و $a = pw = p(\pm 1) = \pm p$. از طرف دیگر استدلالی مشابه نشان می‌دهد که $[b] = [0]$ نتیجه می‌دهد که $a = \pm 1$. بنابراین p اول است. ■

بنابر قضیه ۸.۲، وقتی که n اول باشد هر معادله در $\mathbb{Z}_n$ به شکل $ax = 1$ (با $a \neq 0$) دارای یک جواب است. وقتی که n اول نباشد، تنها بعضی از معادلات به این صورت ممکن است دارای جواب باشند. برای مثال، در $\mathbb{Z}_{10}$، $x = 7$ یک جواب $3x = 1$ است.

نتیجه ۹.۲. فرض کنید a و n اعداد صحیح باشند با $n > 1$. در این صورت $(a, n) = 1$ در $\mathbb{Z}$ اگر و تنها اگر معادله $ax = 1$ در $\mathbb{Z}_n$ دارای یک جواب باشد.

برهان. فرض کنید $(a, n) = 1$. در قضیهٔ ۲ـ۸، در برهان قسمت (۱) $\Leftarrow$ (۲)، از اول بودن p تنها در اثبات این که $(a, p) = 1$ استفاده شد. سپس تنها با استفاده از این حقیقت، اثبات شد که $ax = 1$ دارای یک جواب است. در نتیجه، این قسمت از اثبات برای هر $\mathbb{Z}_n$ با $(a, n) = 1$ معتبر است.

برعکس، فرض کنید $ax = 1$ دارای یک جواب u در $\mathbb{Z}_n$ باشد. در این صورت در $\mathbb{Z}_n$، $au = 1$، یا به‌طور معادل (با در نظر گرفتن a و u به عنوان اعداد صحیح) در $\mathbb{Z}$ (پیمانه n) $au \equiv 1$. بنابراین n یک شمارنده $au - 1$ است و لذا برای برخی عدد صحیح v، $au - 1 = nv$، پس $au - nu = 1$. از این معادله نتیجه می‌شود که هر شمارنده مشترک a و n باید 1 را بشمارد. بنابراین $(a, n) = 1$. ■

تمرینها

۱.A. برای چه a هایی، معادله $ax = 1$ دارای جواب است:

(الف) در $\mathbb{Z}_7$ ؟ (ب) در $\mathbb{Z}_8$ ؟

(پ) در $\mathbb{Z}_9$ ؟ (ت) در $\mathbb{Z}_{10}$ ؟

۲. اگر n غیر اول باشد، ثابت کنید که $a, b \in \mathbb{Z}_n$ وجود دارد به‌طوری که $a \neq 0$ و $b \neq 0$ امّا $ab = 0$.

۳. بدون استفاده از قضیه ۸.۲، ثابت کنید که اگر p اول باشد و $ab = 0$ در $\mathbb{Z}_p$، در این صورت $a = 0$ یا $b = 0$. [راهنمایی: قضیه ۸.۱.]

۴.B معادله $58x = 1$ را در $\mathbb{Z}_{127}$ حل کنید. [راهنمایی ۱۲۷ اول است؛ از الگوریتم اقلیدسی و روشی که در اثبات قسمت اول قضیه ۲ـ۸ بکار رفت استفاده کنید.]

۵. فرض کنید p یک عدد اول باشد و $a \neq 0$ در $\mathbb{Z}_p$. ثابت کنید که برای هر $b \in \mathbb{Z}_p$، معادله $ax = b$ دارای یک جواب است.

۶.C فرض کنید $a \neq 0$ در $\mathbb{Z}_n$. ثابت کنید که $ax = 0$ دارای یک جواب غیرصفر در $\mathbb{Z}_n$ است اگر و تنها اگر $ax = 1$ دارای هیچ جوابی نباشد.

* * * * *

فصل سوم

حلقه‌ها

در فصل‌های قبل دیدیم که بسیاری از قوانین حساب معمولی نه تنها در $\mathbb{Z}$ بلکه در مجموعه ظریف $\mathbb{Z}_n$ نیز برقرار است. شما با دستگاههای ریاضی دیگری مانند اعداد حقیقی نیز آشنا هستید که در آنها بسیاری از همین قوانین برقرار است. همچنین در دروس جبر دبیرستانی با حساب چندجمله‌ای‌ها آشنا شده‌اید.

با توجه به این حقیقت که قوانین مشابهی از حساب در دستگاههای مختلفی برقرار است، به‌نظر می‌رسد که ملاحظه ویژگی‌های مشترک چنین دستگاههایی می‌تواند راهگشا باشد. در درازمدت، این امر می‌تواند باعث صرفه‌جویی مقدار زیادی از کار شود: اگر بتوان قضیه‌ای را که مربوط به یک دستگاه است تنها توسط خواصی از آن اثبات کرد که یک دستگاه دومی نیز این خواص را داراست در این صورت قضیه در دستگاه دیگر نیز برقرار است. با "تجرید" ویژگی‌های اساسی مشترک بین دستگاهها، می‌توانیم یک نظریه کلی را بسط دهیم که حالت‌های خاصی مثل $\mathbb{Z}$، $\mathbb{Z}_n$ و دستگاههای آشنای دیگر را شامل شود. در این صورت نتایج اثبات شده برای این نظریه کلی، همزمان قابل

بکارگیری در همه دستگاههایی که مشمول این نظریه می‌شوند خواهد بود. این فرآیند مجردسازی به ما اجازه می‌دهد بدون درگیرشدن در جزئیات غیرضروری، دلایل واقعی که بر مبنای آنها یک گزاره بخصوص درست (یا غلط، برای آن موضوع) است را کشف نمائیم. این روش، می‌تواند به درک عمیق‌تری از همه دستگاههای مشمول منجر شود.

پس اینک به بسط و توسعه جبرد مجرد می‌پردازیم. این فصل تنها اولین گام بوده و عمدتاً تعاریف، مثال‌ها و اصطلاحات علمی را شامل می‌شود. دستگاههایی که در حداقل خواص بنیادی با $\mathbb{Z}$ و $\mathbb{Z}_n$ مشترک هستند، **حلقه** نامیده می‌شوند.

همانگونه که در بخش ۱.۳ خواهید دید برای حلقه‌هایی که ممکن است خواص اضافی‌تری داشته باشند نام‌های دیگری بکار می‌رود. در بخش ۲.۳، حقایق مقدماتی در مورد حساب و جبر در حلقه‌های دلخواه را بسط می‌دهیم. در بخش ۳.۳، حلقه‌هایی را در نظر می‌گیریم که متفاوت از یکدیگر به نظر می‌رسند امّا در واقع به‌جز در نشان‌گذاری عناصرشان، "اساساً فرقی ندارند". برای دیدن مثالی ساده، اعداد صحیح را یک‌بار با اعداد عربی و یک‌بار با اعداد رومی بنویسید.

۳-۱ تعریف و مثال‌هایی از حلقه‌ها

فرایند مجردسازی ویژگی‌های مشترک دستگاههای آشنای جبری را با تعریف زیر آغاز می‌کنیم:

تعریف. یک **حلقه** یک مجموعه غیرتهی R است که با دو عمل[1] (معمولاً به‌عنوان ضرب و جمع نوشته می‌شود) که در اصول زیر صدق می‌کنند مجهز شده است. برای هر a، b و c در R:

۱. اگر $a, b \in R$ آنگاه $a+b \in R$.	[بسته‌بودن نسبت به جمع]
۲. $a+(b+c)=(a+b)+c$	[شرکت‌پذیری جمع]
۳. $a+b=b+a$	[جابجایی جمع]
۴. عضو 0_R در R چنان موجود است که $a+0_R=a=0_R+a$ برای هر $a \in R$.	[همانی جمعی یا عضو صفر]

۱) "عمل" و "بسته‌بودن" در پیوست ب تعریف شده است.

۵. برای هر $a \in R$، معادله $a + x = 0_R$ دارای یک جواب در R است. [وجود عضو قرینه نسبت به جمع]

۶. اگر $a, b \in R$ در این صورت $ab \in R$. [بسته‌بودن نسبت به ضرب]

۷. $a(bc) = (ab)c$ [شرکت‌پذیری ضرب]

۸. $a(b + c) = ab + ac$ و $(a + b)c = ac + bc$. [قوانین توزیع‌پذیری]

اینها حداقل اصول لازم برای یک دستگاه جبری است که بخواهد مشابه $\mathbb{Z}$ یا $\mathbb{Z}_n$ باشد. امّا $\mathbb{Z}$ و $\mathbb{Z}_n$ دارای چندین خاصیت اضافی دیگر است که ارزش بیان مستقل را دارد:

تعریف. یک حلقه جابجایی یک حلقه R است که در اصل زیر صدق کند:

۹. برای هر $a, b \in R$، $ab = ba$. [جابجایی ضرب]

تعریف. یک حلقه یکدار یک حلقه R است که یک عضو 1_R که اصل زیر را ارضا می‌کند شامل باشد.

۱۰. برای هر $a \in R$، $a1_R = a = 1_R a$.

بررسی برقراری اصول فوق در مثال‌های زیر در بیشتر موارد به خواننده واگذار شده است.

مثال ۱.۳. اعداد صحیح $\mathbb{Z}$ همراه با جمع و ضرب معمولی یک حلقه جابجایی یکدار تشکیل می‌دهد.

مثال ۲.۳. طبق قضیه ۷.۲، مجموعه $\mathbb{Z}_n$ همراه با جمع و ضرب کلاسها یک حلقه جابجایی یکدار است.

مثال ۳.۳. فرض کنید E مجموعه اعداد صحیح زوج همراه با جمع و ضرب معمولی باشد. چون جمع و ضرب دو عدد صحیح زوج نیز زوج است، اصول بسته‌بودن (۱ و ۶) برقرار است. چون 0 یک عدد صحیح زوج است، E دارای یک عضو همانی جمعی است (اصل ۴). اگر a زوج باشد،

در این‌صورت جواب معادله $a + x = 0$ (یعنی $-a$) نیز زوج است و بنابراین اصل ۵ برقرار است. اصول دیگر (شرکت‌پذیری، جابجایی، توزیع‌پذیری) برای همه اعداد صحیح برقرار است و بنابراین برای هر a، b و c زوج نیز برقرار می‌باشد. در نتیجه E یک حلقه جابجایی است. با این حال E یک حلقه یکدار نیست، زیرا هیچ عدد زوج e وجود ندارد به قسمی که برای هر عدد زوج a، $ae = a = ea$.

مثال ۴.۳. مجموعه اعداد صحیح فرد با جمع و ضرب معمولی یک حلقه نیست، زیرا برای مثال اصل ۱ برقرار نیست: مجموع دو عدد صحیح فرد، فرد نیست.

مثال قبل نشان می‌دهد که یک زیرمجموعه از یک حلقه لزوماً یک حلقه نیست. وقتی یک زیرمجموعه S از یک حلقه R تحت جمع و ضرب در R خود یک حلقه باشد در این صورت S را یک **زیرحلقه** از R می‌نامیم. عضو صفر زیرحلقه S همان عضو 0_R حلقه R است. (تمرین ۱۸ بخش ۲.۳).

اصول ۲، ۳، ۷ و ۸ برای همه اعضای یک حلقه R برقرار است و لذا لزوماً برای هر زیرمجموعه S از R نیز برقرار می‌باشد. در نتیجه، برای اثبات زیرحلقه بودن S تنها لازم است بررسی شود که:

- S تحت ضرب و جمع بسته است (اصول ۱ و ۶)؛
- $0_R \in S$ (اصل ۴)؛
- برای هر $a \in S$، معادله $a + x = 0_R$ دارای یک جواب در S است (اصل ۵).

گرچه تعریف حلقه از الگوهای $\mathbb{Z}$ و $\mathbb{Z}_n$ نشأت گرفته است، حلقه‌های زیادی وجود دارند که ابداً مانند این الگوها نیستند. در این حلقه‌ها اعضاء ممکن است اعداد یا کلاسهایی از اعداد نباشند و اعمال آنها نیز ممکن است هیچ رابطه‌ای با جمع و ضرب "معمولی" نداشته باشد.

مثال ۵.۳. مجموعه $T = \{r, s, t, z\}$ با دو عمل جمع وضرب تعریف شده توسط جداول زیر یک حلقه است:

$+$	z	r	s	t
z	z	r	s	t
r	r	z	t	s
s	s	t	z	r
t	t	s	r	z

$\cdot$	z	r	s	t
z	z	z	z	z
r	z	z	r	r
s	z	z	s	s
t	z	z	t	t

برای بررسی اصول حلقه، می‌توانید تضمین ما مبنی بر برقراری اصول ۲، ۷ و ۸ را بپذیرید. عضو z عضو همانی جمعی است، یعنی عضوی که در اصل ۴ با 0_R نشان داده شده است. این عضو مشابه عدد صفر در $\mathbb{Z}$ رفتار می‌کند (به این دلیل نماد 0_R برای این اصل بکار رفته است). امّا z عدد صحیح صفر نیست، در واقع z یک عدد نیست. در عین حال ما z را "عضو صفر" حلقه T می‌نامیم. برای اصل ۵ بررسی کنید که معادلات

$$r+x=z \qquad s+x=z \qquad t+x=z \qquad z+x=z$$

در T دارای جواب است. این را می‌توان به سادگی از جدول جمع دید؛ برای مثال $x=r$ جواب $r+x=z$ است زیرا $r+r=z$. توجه کنید که T یک حلقه جابجایی نیست: برای مثال $rs=r$ و $sr=z$، بنابراین $rs\neq sr$.

مثال ۶.۳. فرض کنید $M(\mathbb{R})$ مجموعه ماتریس‌های 2×2 روی میدان اعداد حقیقی باشد، یعنی $M(\mathbb{R})$ از همه ماتریس‌های $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$، که در آن a، b، c و d اعداد حقیقی هستند، تشکیل شده است. دو ماتریس در $M(\mathbb{R})$ برابر است اگر درایه‌های نظیرشان برابر باشد: یعنی

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \quad \text{اگر و تنها اگر} \quad a=r،\ b=s،\ c=t \text{ و } d=u.$$

برای مثال

$$\begin{pmatrix} 4 & 0 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} 2+2 & 0 \\ 1-4 & 1 \end{pmatrix} \quad \text{امّا} \quad \begin{pmatrix} 1 & 3 \\ 5 & 2 \end{pmatrix} \neq \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}.$$

جمع ماتریسها توسط ضابطه

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$

تعریف شده است. برای مثال

$$\begin{pmatrix} ۳ & -۲ \\ ۵ & ۱ \end{pmatrix} + \begin{pmatrix} ۴ & ۷ \\ ۶ & ۰ \end{pmatrix} = \begin{pmatrix} ۳+۴ & -۲+۷ \\ ۵+۶ & ۱+۰ \end{pmatrix} = \begin{pmatrix} ۷ & ۵ \\ ۱۱ & ۱ \end{pmatrix}.$$

ضرب ماتریسها نیز توسط ضابطه

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} aw+by & ax+bz \\ cw+dy & cx+dz \end{pmatrix}$$

تعریف شده است. برای مثال

$$\begin{pmatrix} ۲ & ۳ \\ ۰ & -۴ \end{pmatrix} \begin{pmatrix} ۱ & -۵ \\ ۶ & ۷ \end{pmatrix} = \begin{pmatrix} ۲\times ۱ + ۳\times ۶ & ۲(-۵)+۳\times ۷ \\ ۰\times ۱ + (-۴)۶ & ۰(-۵)+(-۴)۷ \end{pmatrix} = \begin{pmatrix} ۲۰ & ۱۱ \\ -۲۴ & -۲۸ \end{pmatrix}.$$

همانند مثال زیر، تعویض ترتیب عوامل در ضرب ماتریسی ممکن است جواب دیگری به دست دهد:

$$\begin{pmatrix} ۱ & -۵ \\ ۶ & ۷ \end{pmatrix} \begin{pmatrix} ۲ & ۳ \\ ۰ & -۴ \end{pmatrix} = \begin{pmatrix} ۱\times ۲ + (-۵)۰ & ۱\times ۳ + (-۵)(-۴) \\ ۶\times ۲ + ۷\times ۰ & ۶\times ۳ + ۷(-۴) \end{pmatrix} = \begin{pmatrix} ۲ & ۲۳ \\ ۱۲ & -۱۰ \end{pmatrix}.$$

بنابراین ضرب جابجایی نیست. با کمی تلاش می‌توانید بررسی کنید که $M(\mathbb{R})$ یک حلقه یکدار است. عضو صفر $M(\mathbb{R})$ ماتریس

$$\begin{pmatrix} ۰ & ۰ \\ ۰ & ۰ \end{pmatrix}$$

است و

$$X = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

جواب معادله

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + X = \begin{pmatrix} ۰ & ۰ \\ ۰ & ۰ \end{pmatrix}$$

در $M(\mathbb{R})$ می‌باشد. عضو همانی ضربی (اصل ۱۰) ماتریس

$$I = \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix}$$

است؛ برای مثال

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} = \begin{pmatrix} a \times ۱ + b \times ۰ & a \times ۰ + b \times ۱ \\ c \times ۱ + d \times ۰ & c \times ۰ + d \times ۱ \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

توجه کنید که حاصل‌ضرب اعضای غیرصفر $M(\mathbb{R})$ ممکن است عضو صفر باشد؛ برای مثال

$$\begin{pmatrix} ۴ & ۶ \\ ۲ & ۳ \end{pmatrix} \begin{pmatrix} -۳ & -۹ \\ ۲ & ۶ \end{pmatrix} = \begin{pmatrix} ۴(-۳) + ۶ \times ۲ & ۴(-۹) + ۶ \times ۶ \\ ۲(-۳) + ۳ \times ۲ & ۲(-۹) + ۳ \times ۶ \end{pmatrix} = \begin{pmatrix} ۰ & ۰ \\ ۰ & ۰ \end{pmatrix}.$$

مثال ۷.۳. $M(\mathbb{Z})$، $M(\mathbb{Q})$، $M(\mathbb{C})$ و $M(\mathbb{Z}_n)$ به‌ترتیب مجموعه ماتریس‌های ۲×۲ با درایه‌های در $\mathbb{Z}$، اعداد گویای $\mathbb{Q}$، اعداد مختلط $\mathbb{C}$ و حلقه $\mathbb{Z}_n$ را نشان می‌دهد [۲]. با جمع و ضرب تعریف شده در مثال قبلی، $M(\mathbb{Z})$، $M(\mathbb{Q})$، $M(\mathbb{C})$ و $M(\mathbb{Z}_n)$ حلقه‌های غیرجابجایی یکدار هستند.

مثال ۸.۳. فرض کنید T مجموعه همه توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$ باشد، جایی که $\mathbb{R}$ مجموعه اعداد حقیقی است. همانگونه که در حسابان دیده‌اید، $f+g$ و fg توابعی هستند که به صورت

$$(f+g)(x) = f(x) + g(x) \qquad \text{و} \qquad (fg)(x) = f(x)g(x)$$

تعریف می‌شوند. در حسابان ثابت شده است که مجموع و حاصل‌ضرب توابع پیوسته، پیوسته است و لذا T تحت جمع و ضرب بسته است (اصول ۱ و ۶). می‌توانید بررسی کنید که T یک حلقه جابجایی یکدار است. عضو صفر تابع h است که به صورت $h(x) = ۰$ برای هر $x \in \mathbb{R}$ تعریف

۲) سرتاسر این کتاب $\mathbb{P}$ همواره اعداد حقیقی، $\mathbb{Q}$ اعداد گویا و $\mathbb{C}$ اعداد مختلط را نشان می‌دهد.

می‌شود. عضو همانی تابع e است که به صورت $e(x) = ۱$ برای هر $x \in \mathbb{R}$ تعریف می‌شود. مجدداً حاصل‌ضرب اعضای غیرصفر T ممکن است تابع صفر را به دست دهد؛ تمرین ۲۷ را ملاحظه کنید.

دیده‌ایم که برخی حلقه‌ها فاقد این خاصیت‌اند که حاصل‌ضرب دو عضو غیرصفر همواره غیرصفر باشد. با این حال، تعداد حلقه‌های واجد این خاصیت، مانند $\mathbb{Z}$، به آن اندازه‌ای هست که تعریف مستقلی برای آنها ارائه دهیم.

تعریف. یک **دامنه صحیح** یک حلقه جابجایی R است با همانی $۱_R \neq ۰_R$ که در شرط زیر صدق کند:

۱۱. هرگاه $a, b \in R$ و $ab = ۰$ آنگاه یا $a = ۰_R$ یا $b = ۰_R$.

شرط $۰_R \neq ۱_R$ لازم است تا حلقه صفر از کلاس دامنه‌های صحیح کنار گذاشته شود. توجه کنید که اصل ۱۱ منطقاً معادل عکس نقیضش[۳] می‌باشد:

هرگاه $a \neq ۰_R$ و $b \neq ۰_R$ آنگاه $ab \neq ۰_R$.

مثال ۹.۳. حلقه اعداد صحیح $\mathbb{Z}$ یک دامنه صحیح است. اگر p اول باشد، در این صورت (طبق قضیه ۸.۲)، $\mathbb{Z}_p$ یک دامنه صحیح است.

حتماً با مجموعه اعداد گویا $\mathbb{Q}$ شامل همه کسرهای a/b با $a, b \in \mathbb{Z}$ و $b \neq ۰$ آشنا هستید. برابری، جمع و ضرب کسرها در $\mathbb{Q}$ توسط قوانین معمولی

$$\frac{a}{b} = \frac{r}{s} \quad \text{اگر و تنها اگر} \quad as = br$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

تعریف می‌شود. بررسی دامنه صحیح بودن $\mathbb{Q}$ ساده است. در عین حال $\mathbb{Q}$ دارای یک خاصیت اضافی است که در $\mathbb{Z}$ نیست: هر معادله به صورت $ax = ۱$ (با $a \neq ۰$) دارای جوابی در $\mathbb{Q}$ است. بنابراین $\mathbb{Q}$ مصداقی از تعریف بعدی است.

تعریف. حلقه R با همانی $۱_R \neq ۰_R$ که در اصل زیر صدق کند یک **حلقه تقسیمی** نامیده می‌شود:

---

۳) برای بحث عکس نقیض پیوست **الف** را ملاحظه کنید.

۱۲. برای هر $a \neq 0_R$ در R، معادلات $ax = 1_R$ و $xa = 1_R$ دارای جوابی در $\mathbb{R}$ هستند.

یک **میدان** یک حلقه‌تقسیمی است که در آن عمل ضرب جابجایی است.

اگر بکار در حلقه‌های جابجایی نظیر $\mathbb{Z}$ و $\mathbb{Q}$ عادت کرده باشید، ممکن است معادله‌ای به صورت $xa = 1$ کمی عجیب به‌نظر برسد. اما چنین معادلاتی باید در حلقه‌های ناجابجایی که در آن xa ممکن است برابر ax نباشد در نظر گرفته شود. با این‌حال، عمده تأکید ما روی میدانها خواهد بود و لذا ابتدا مثال‌هایی از این نوع را در نظر می‌گیریم.

مثال ۱۰.۳. مجموعه اعداد حقیقی $\mathbb{R}$ با جمع و ضرب معمولی یک میدان است. چون زیرمجموعه اعداد گویای $\mathbb{Q}$ با همان اعمال $\mathbb{R}$ یک میدان است، $\mathbb{Q}$ را یک **زیرمیدان** $\mathbb{R}$ می‌نامیم.

مثال ۱۱.۳. مجموعه اعداد مختلط $\mathbb{C}$ از همه اعدادی به صورت $a + bi$ تشکیل شده است که در آن $a, b \in \mathbb{R}$ و $i^2 = -1$. برابری در $\mathbb{C}$ به صورت زیر تعریف می‌شود:

$$a + bi = v + si \quad \text{اگر و تنها اگر} \quad a = v \ \text{و} \ b = s$$

مجموعه $\mathbb{C}$ با جمع و ضرب تعریف شده در زیر یک میدان است:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

میدان اعداد حقیقی $\mathbb{R}$ یک زیرمیدان $\mathbb{C}$ است، زیرا $\mathbb{R}$ از همه اعداد مختلط به صورت $a + 0i$ تشکیل شده است. اگر $a + bi \neq 0$ در $\mathbb{C}$، در این صورت جواب معادله $(a + bi)x = 1$، $x = c + di$ می‌باشد که در آن

$$c = a/(a^2 + b^2) \in \mathbb{R} \quad \text{و} \quad d = -b/(a^2 + b^2) \in \mathbb{R}$$ (بررسی کنید!).

مثال ۱۲.۳. اگر p اول باشد در این صورت طبق قضیه ۸.۲، $\mathbb{Z}_p$ یک میدان است.

مثال ۱۳.۳. فرض کنید K مجموعه ماتریس‌های 2×2 بصورت $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ باشد، که در آن a

و b اعداد حقیقی هستند. ادعا می‌کنیم که K یک میدان است. برای هر دو ماتریس در K، داریم

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$$

در هر مورد ماتریس طرف راست در K است زیرا درایه‌های روی قطر اصلی (گوشه چپ بالایی تا گوشه راست پائینی) برابرند و درایه‌های روی قطر غیر اصلی (راست بالایی و چپ پائینی) منفی یکدیگر هستند. بنابراین K تحت جمع و ضرب بسته است. K جابجایی است زیرا

$$\begin{pmatrix} c & d \\ -d & c \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix}.$$

بوضوح ماتریس صفر و ماتریس I در K است. اگر

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

بررسی کنید که جواب $AX = I$،

$$X = \begin{pmatrix} a/d & -b/d \\ b/d & a/d \end{pmatrix} \in K$$ است که در آن $d = a^2 + b^2$.

حلقه‌های تقسیمی غیرجابجایی نقشی را در باقیمانده مطالب این کتاب ایفا نمی‌کنند، با این‌حال به منظور کامل بودن مثالی از این نوع حلقه‌ها را ارائه می‌کنیم. این مثال لزوماً یک حلقه نامتناهی است زیرا قضیه مشهوری از وِدبِرن[۴] نشان می‌دهد که هر حلقه تقسیمی متناهی یک میدان است.

مثال ۱۴.۳. در حلقه $M(\mathbb{C})$ فرض کنید،

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

(۴ Wedderburn

حاصل‌ضرب یک عدد حقیقی و یک ماتریس یک ماتریس است که طبق قانون زیر تعریف می‌شود:

$$r\begin{pmatrix} t & u \\ v & w \end{pmatrix} = \begin{pmatrix} rt & ru \\ rv & rw \end{pmatrix}$$

بنابه تعریف، مجموعه چهارگانه حقیقی H از همه ماتریسهایی به صورت

$$\begin{aligned} a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} &= a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ &= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} bi & 0 \\ 0 & -bi \end{pmatrix} + \begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix} + \begin{pmatrix} 0 & di \\ di & 0 \end{pmatrix} \\ &= \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}, \end{aligned}$$

تشکیل می‌شود که در آن a، b، c و d اعداد حقیقی هستند. تحت جمع و ضرب معمولی ماتریسها، H یک حلقه تقسیمی غیرجابجایی است. برای جزئیات تمرین ۳۱ را ملاحظه کنید.

هرگاه ذکری از حلقه‌های ارائه شده در مثال‌های قبل به میان آید، می‌توانید فرض کنید جمع و ضرب همان اعمالی باشد که در بالا تعریف شد، مگر آنکه به‌طور مشخص خلاف آن بیان شود. با این‌حال باید هشیار بود که یک مجموعه مفروض (مثل $\mathbb{Z}$) می‌تواند به طرق مختلف با ارائه تعاریفی متفاوت برای اعمال جمع و ضرب به یک حلقه تبدیل شود. برای مثال‌هایی از این نوع، تمرینهای ۳ و ۲۰-۱۷ را ملاحظه کنید.

اینک که با انواع مختلفی از حلقه‌ها آشنا شده‌ایم می‌توانیم با بکار بردن آنها حلقه‌های جدیدی به صورت زیر تولید کنیم:

مثال ۱۵.۳. فرض کنید T حاصل‌ضرب دکارتی $\mathbb{Z} \times \mathbb{Z}_۶$ باشد که در پیوست ب تعریف شده است. جمع در T را طبق قانون زیر تعریف کنید:

$$(a, z) + (a', z') = (a + a', z + z').$$

در اینجا علامت جمع به سه صورت بکار رفته است: علامت جمع در مختص اول زوج مرتب طرف راست تساوی، جمع در $\mathbb{Z}_۶$ را نشان می‌دهد؛ در مختص دوم، علامت $+$، جمع در $\mathbb{Z}$ را نشان می‌دهد؛

علامت + در طرف چپ تساوی، جمع در T است که در حال تعریف آن هستم. چون $\mathbb{Z}_6$ یک حلقه است و $a, a' \in \mathbb{Z}_6$، لذا اولین مختص طرف راست یعنی $a + a'$، در $\mathbb{Z}_6$ است. به طور مشابه $z + z' \in \mathbb{Z}$. بنابراین جمع در T بسته است. ضرب به‌طور مشابه تعریف می‌شود:

$$(a, z)(a', z') = (aa', zz').$$

بـــرای مثـــال $(3, 5) + (4, 9) = (3 + 4, 5 + 9) = (1, 14)$ و

$$(3, 5)(4, 9) = (3 \cdot 4, 5 \cdot 9) = (0, 45).$$

به‌سادگی می‌توانید بررسی کنید که T یک حلقه جابجایی یکدار است. عضو صفر $(0, 0)$ است و عضو همانی ضربی، (1,1) است. آنچه که در اینجا انجام گرفت می‌تواند برای هر دو حلقه دلخواه انجام شود.

قضیه ۱.۳. فرض کنید R و S دو حلقه باشند. جمع و ضرب را روی حاصل‌ضرب دکارتی $R \times S$ به صورت

$$(r, s) + (r', s') = (r + r', s + s')$$
$$(r, s)(r', s') = (rr', ss')$$

تعریف کنید. در این صورت $R \times S$ یک حلقه است. اگر R و S هر دو جابجایی باشند در این صورت $R \times S$ نیز جابجایی است. اگر R و S هر دو یکدار باشند در این صورت $R \times S$ نیز یکدار است.

برهان. تمرین ۳۲. ■

تمرینها

۱.A. زیرمجموعه‌های زیر از $\mathbb{Z}$ (با جمع و ضرب معمولی) در همه اصول یک حلقه به جز یک اصل صدق می‌کنند. در هر مورد کدام اصل برقرار نیست؟

(الف) مجموعه S شامل همه اعداد صحیح فرد و صفر،

(ب) مجموعه اعداد صحیح غیرمنفی.

۲. (الف) نشان دهید مجموعه R شامل همه مضارب ۳ یک زیرحلقه $\mathbb{Z}$ است.

(ب) فرض کنید k یک عدد صحیح ثابت باشد. نشان دهید مجموعه همه مضارب k یک زیرحلقه $\mathbb{Z}$ است.

۳. ضرب جدیدی در $\mathbb{Z}$ توسط قانون "$ab = ۰$ برای هر $a, b \in \mathbb{Z}$" تعریف کنید. نشان دهید با جمع معمولی و این ضرب جدید، $\mathbb{Z}$ یک حلقه جابجایی است.

۴. ضرب جدیدی در $\mathbb{Z}$ توسط قانون "$ab = ۱$ برای هر $a, b \in \mathbb{Z}$" تعریف کنید. آیا با جمع معمولی و این ضرب جدید، $\mathbb{Z}$ یک حلقه است؟

۵. فرض کنید $R = \{۰, e, b, c\}$ و جمع و ضرب روی R توسط جداول زیر تعریف شود. برقراری شرکت‌پذیری و توزیع‌پذیری را فرض کرده و نشان دهید که R یک حلقه یکدار است. آیا R جابجایی است؟

$+$	۰	e	b	c
۰	۰	e	b	c
e	e	۰	c	b
b	b	c	۰	e
c	c	b	e	۰

$\cdot$	۰	e	b	c
۰	۰	۰	۰	۰
e	۰	e	b	c
b	۰	b	e	c
c	۰	c	c	۰

۶. فرض کنید $F = \{۰, e, b, c\}$ و جمع و ضرب روی F توسط جداول زیر تعریف شود. برقراری شرکت‌پذیری و توزیع‌پذیری را فرض کرده و نشان دهید که F یک میدان است.

$+$	۰	e	a	b
۰	۰	e	a	b
e	e	۰	b	a
a	a	b	۰	e
b	b	a	e	۰

$\cdot$	۰	e	a	b
۰	۰	۰	۰	۰
e	۰	e	a	b
a	۰	a	b	e
b	۰	b	e	a

۷. کدام یک از این پنج مجموعه زیرحلقه‌ای از $M(\mathbb{R})$ است؟ کدام‌یک یکدار است؟

(الف) همه ماتریس‌های به صورت $\begin{pmatrix} ۰ & r \\ ۰ & ۰ \end{pmatrix}$ با $r \in \mathbb{Q}$.

(ب) همه ماتریس‌های به صورت $\begin{pmatrix} a & b \\ ۰ & c \end{pmatrix}$ با $a,b,c \in \mathbb{Z}$.

(پ) همه ماتریس‌های به صورت $\begin{pmatrix} a & a \\ b & b \end{pmatrix}$ با $a,b \in \mathbb{R}$.

(ت) همه ماتریس‌های به صورت $\begin{pmatrix} a & ۰ \\ a & ۰ \end{pmatrix}$ با $a \in \mathbb{R}$.

(ث) همه ماتریس‌های به صورت $\begin{pmatrix} a & ۰ \\ ۰ & a \end{pmatrix}$ با $a \in \mathbb{R}$.

۸. فرض کنید T حلقه همه توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$ باشد. فرض کنید $S = \{f \in T \mid f(۲) = ۰\}$. آیا S یک زیرحلقه T است؟

۹. فرض کنید R و S دو حلقه باشند. نشان دهید زیرمجموعه $\bar{R} = \{(r, ۰_S) \mid r \in R\}$ یک زیرحلقه $R \times S$ است. همین را برای زیرمجموعه $\bar{S} = \{(۰_R, s) \mid s \in S\}$ انجام دهید.

۱۰. اگر R یک حلقه باشد، نشان دهید که $R^* = \{(r,r) \mid r \in R\}$ یک زیرحلقه $R \times R$ است.

۱۱. فرض کنید $S = \{a,b,c\}$ و فرض کنید $P(S)$ مجموعه همه زیرمجموعه‌های S باشد، عناصر $P(S)$ عبارتند از:

$$S = \{a,b,c\}; \quad D = \{a,b\}; \quad E = \{a,c\}; \quad F = \{b,c\};$$
$$A = \{a\}; \quad B = \{b\}; \quad C = \{c\}; \quad ۰ = \varnothing.$$

جمع و ضرب در $P(S)$ را با قوانین زیر تعریف کنید:

$$M + N = (M - N) \cup (N - M), \qquad MN = M \cap N.$$

جداول جمع و ضرب را برای $P(S)$ بنویسید. تمرین ۳۶ را نیز ملاحظه کنید.

۱۲. مجموعه $\{a + b\sqrt{۲} \mid a,b \in \mathbb{Z}\}$ را با $\mathbb{Z}[\sqrt{۲}]$ نمایش دهید. نشان دهید که $\mathbb{Z}[\sqrt{۲}]$ یک زیرحلقه $\mathbb{R}$ است.

۱۳. مجموعه $\{a+bi \mid a,b \in \mathbb{Z}\}$ را با $\mathbb{Z}[i]$ نمایش دهید. نشان دهید که $\mathbb{Z}[i]$ یک زیرحلقه $\mathbb{C}$ است.

۱۴. آیا زیرمجموعه $\{1,-1,i,-i\}$ یک زیرحلقه $\mathbb{C}$ است؟

۱۵. جداول جمع و ضرب را برای حلقه‌های زیر بنویسید:

(الف) $\mathbb{Z}_2 \times \mathbb{Z}_2$ (ب) $\mathbb{Z}_2 \times \mathbb{Z}_3$ (پ) $\mathbb{Z}_3 \times \mathbb{Z}_3$

۱۶. فرض کنید R یک حلقه و t عضو ثابتی از R باشد. قرار دهید $T = \{rt \mid r \in R\}$. ثابت کنید T یک زیرحلقه R است.

۱۷.B. مجموعه اعداد صحیح زوج با جمع معمولی را با E نمایش دهید. توسط قانون "$a * b = ab/2$" ضرب جدید $*$ را روی E تعریف کنید (جایی که ضرب طرف راست ضرب معمولی است). ثابت کنید که با این اعمال E یک حلقه جابجایی یکدار است.

۱۸. روی $\mathbb{Z}$، جمع جدید $\oplus$ و ضرب جدید $\odot$ را توسط

$$a \oplus b = a + b - 1 \qquad \text{و} \qquad a \odot b = a + b - ab$$

تعریف کنید، جایی که اعمال طرف راست تساوی، جمع، تفریق و ضرب معمولی هستند. ثابت کنید که با اعمال جدید $\oplus$ و $\odot$، $\mathbb{Z}$ یک دامنه صحیح است.

۱۹. روی $\mathbb{Z}$ جمع و ضرب جدیدی را به صورت

$$a \oplus b = a + b - 1 \quad , \quad a \odot b = ab - (a+b) + 2$$

تعریف کنید. ثابت کنید که با این اعمال جدید، $\mathbb{Z}$ یک دامنه صحیح است.

۲۰. روی $\mathbb{Q}$ جمع و ضرب جدیدی را به صورت

$$r \oplus s = r + s + 1 \quad , \quad r \odot s = rs + r + s$$

تعریف کنید. ثابت کنید که با اعمال جدید $\mathbb{Q}$ یک حلقه جابجایی یکدار است. آیا یک دامنه صحیح نیز هست؟

۲۱. نشان دهید زیرمجموعه $S = \{0,2,4,6,8\}$ از $\mathbb{Z}_{10}$ یک زیرحلقه است. آیا S یکدار است؟

۲۲. نشان دهید زیرمجموعه $R = \{0, 3, 6, 9, 12, 15\}$ از $\mathbb{Z}_{18}$ یک زیرحلقه است. آیا R یکدار است؟

۲۳. فرض کنید p یک عدد اول مثبت و R مجموعه همه اعداد گویای r/p^i باشد که در آن $r, i \in \mathbb{Z}$ و $i \geq 0$. توجه کنید که $\mathbb{Z} \subseteq R$، زیرا هر $n \in \mathbb{Z}$ را می‌توان به صورت n/p^0 نوشت. نشان دهید که R یک زیرحلقه $\mathbb{Q}$ است.

۲۴. جدول جمع و قسمتی از جدول ضرب یک حلقه سه عضوی در زیر داده شده است. با بکارگیری قوانین توزیع‌پذیری جدول ضرب را کامل کنید.

$+$	r	s	t
r	r	s	t
s	s	t	r
t	t	r	s

$\cdot$	r	s	t
r	r	r	r
s	r	t	
t	r		

۲۵. تمرین ۲۴ را برای حلقه چهارعضوی زیر انجام دهید:

$+$	w	x	y	z
w	w	x	y	z
x	x	y	z	w
y	y	z	w	x
z	z	w	x	y

$\cdot$	w	x	y	z
w	w	w	w	w
x	w	y		
y	w		w	
z	w		w	y

۲۶. نشان دهید $M(\mathbb{Z}_2)$ (همه ماتریس‌های 2×2 با درایه‌های در $\mathbb{Z}_2$) یک حلقه ناجابجایی ۱۶ـ عضوی یکدار است.

۲۷. فرض کنید T حلقه توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$ باشد و f و g توسط

$$f(x) = \begin{cases} 0 & \text{اگر } x \leq 2 \\ x - 2 & \text{اگر } 2 < x \end{cases} \quad \text{و} \quad g(x) = \begin{cases} 2 - x & \text{اگر } x \leq 2 \\ 0 & \text{اگر } 2 < x \end{cases}.$$

تعریف شود. نشان دهید $f, g \in T$ و این که $fg = 0_T$ و بنابراین T یک دامنه صحیح نیست.

۲۸. فرض کنید $\mathbb{Q}(\sqrt{۲}) = \{r + s\sqrt{۲} \mid r, s \in \mathbb{Q}\}$. نشان دهید $\mathbb{Q}(\sqrt{۲})$ یک زیرمیدان $\mathbb{R}$ است. [راهنمایی: برای نشان دادن این که جواب $(r + s\sqrt{۲})x = ۱$ واقعاً در $\mathbb{Q}(\sqrt{۲})$ است، $(r - s\sqrt{۲})/(r - s\sqrt{۲})$ را در $۱/(r + s\sqrt{۲})$ ضرب کنید.]

۲۹. فرض کنید d یک عدد صحیح باشد که مربع کامل نیست. نشان دهید $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ یک زیرمیدان $\mathbb{C}$ است. [راهنمایی: تمرین ۲۸ را ملاحظه کنید.]

۳۰. فرض کنید S مجموعه همه عناصر $a + b\sqrt[۳]{۲} + c\sqrt[۳]{۴}$ با $a, b, c \in \mathbb{Q}$ باشد.

(الف) نشان دهید S یک زیرحلقه $\mathbb{R}$ است.

(ب) (مشکل‌تر) نشان دهید S یک زیرمیدان $\mathbb{R}$ است.

۳۱. فرض کنید H مجموعه چهارگانهای حقیقی و ۱، $\mathbf{i}$، $\mathbf{j}$ و $\mathbf{k}$ ماتریس‌های تعریف شده در مثال ۱۴.۳ باشد.

(الف) ثابت کنید

$$\mathbf{i}^۲ = \mathbf{j}^۲ = \mathbf{k}^۲ = -۱ \quad ، \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}$$
$$\mathbf{jk} = -\mathbf{kj} = \mathbf{i} \quad ، \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

(ب) نشان دهید H یک حلقه ناجابجایی یکدار است.

(پ) نشان دهید H یک حلقه تقسیمی است. [راهنمایی: اگر $M = a۱ + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$، در این صورت بررسی کنید که جواب معادله $Mx = ۱$ ماتریس $ta۱ - tb\mathbf{i} - tc\mathbf{j} - td\mathbf{k}$ است که در آن $t = ۱/(a^۲ + b^۲ + c^۲ + d^۲)$.]

۳۲. قضیه ۱.۳ را ثابت کنید.

۳۳. اثبات یا رد کنید:

(الف) اگر R و S دامنه‌های صحیح باشند، در این صورت $R \times S$ یک دامنه صحیح است.

(ب) اگر R و S میدان باشند، در این صورت $R \times S$ یک میدان است.

۳۴. فرض کنید $J = \{۰, ۲\} \subseteq \mathbb{Z}_۴$ و $K = \{۰, ۳, ۶, ۹\} \subseteq \mathbb{Z}_{۱۲}$. نشان دهید $J \times K$ یک زیرحلقه $\mathbb{Z}_۴ \times \mathbb{Z}_{۱۲}$ است.

۳۵. مجموعه $\mathbb{Z} \times \mathbb{Z}$ با جمع مؤلفه به مؤلفه معمولی (مانند قضیه ۱.۳) و یک ضرب جدید داده شده توسط قانون $(a,b)(c,d) = (ac + ۲bd, ad + bc)$ را در نظر بگیرید. نشان دهید که با این اعمال $\mathbb{Z} \times \mathbb{Z}$ یک حلقه جابجایی یکدار است.

۳۶. فرض کنید S یک مجموعه و $P(S)$ مجموعه همه زیرمجموعه‌های S باشد. جمع و ضرب در $P(S)$ را طبق قوانین $M + N = (M - N) \cup (N - M)$ و $MN = M \cap N$ تعریف کنید.

(الف) ثابت کنید $P(S)$ یک حلقه جابجایی یکدار است. [بررسی مستقیم شرکت‌پذیری و توزیع‌پذیری جمع کمی پیچیده و خسته‌کننده است، امّا چنانچه به کمک نمودارهای ون[۵] استدلالی غیررسمی ارائه دهید، این مثال لذت‌بخش خواهد بود. برای یک حالت خاص تمرین ۱۱ را ملاحظه کنید.]

(ب) نشان دهید هر عضو $P(S)$ در معادلات $x^۲ = x$ و $x + x = ۰_{P(S)}$ صدق می‌کند.

۳۷.C $\mathbb{R} \times \mathbb{R}$ را با جمع مؤلفه به مؤلفه معمولی (مانند قضیه ۱.۳) و یک ضرب جدید داده شده توسط

$$(a,b)(c,d) = (ac - bd, ad + bc)$$

در نظر بگیرید. نشان دهید با این اعمال $\mathbb{R} \times \mathbb{R}$ یک میدان است.

۳۸. (الف) همه ماتریس‌های A در $M(\mathbb{R})$ را با این خاصیت که برای هر $B \in M(\mathbb{R})$، $AB = BA$ بیابید.

(ب) نشان دهید مجموعه ماتریس‌های به‌دست آمده در قسمت (الف) یک زیرحلقه $M(\mathbb{R})$ است. این زیرحلقه **مرکز** $M(\mathbb{R})$ نامیده می‌شود.

۳۹. فرض کنید r و s اعداد صحیح مثبت باشد به طوری که برای برخی k، $۱ \leq k < r$، عدد $ks + ۱$ را بشمارد. ثابت کنید زیرمجموعه $\{r, ۲r, ۳r, \ldots, (s-۱)r\}$ از $\mathbb{Z}_{rs}$ تحت جمع و ضرب معمولی در $\mathbb{Z}_{rs}$ یک حلقه، با عضو همانی $ks + ۱$ است. تمرین ۲۱ حالت خاصی از این تمرین است.

---

۵) Venn diagrams

۳-۲ خواص اساسی حلقه‌ها

هنگام انجام محاسبات در حلقه $\mathbb{Z}$، اغلب از اصول یک دامنه صحیح فراتر می‌رویم. برای مثال عمل تفریق و عمل حذف در اغلب محاسبات ظاهر می‌شود. همچنین انواع قوانین ضرب اعداد منفی، و این حقیقت که $a \cdot ۰ = ۰$ نیز در موارد مختلف ظاهر می‌شود. حال نشان می‌دهیم که بسیاری از این نوع خواص در هر حلقه‌ای برقرار می‌باشد.

تفریق جزو خواص یک حلقه ذکر نشده است و ما نمی‌توانیم وجود چنین عملی در یک حلقه را فرض شده بدانیم. در صورت تمایل به تعریف "یک عمل تفریق" در حلقه بایستی آن را بر حسب جمع، ضرب و دیگر اصول حلقه انجام داد.

قضیه ۲.۳. برای هر عضو a در یک حلقه R، معادله $a + x = ۰_R$ دارای یک جواب یکتا است.

برهان. طبق اصل ۵ می‌دانیم که $a + x = ۰_R$ دارای حداقل یک جواب u است. اگر v جواب دیگری باشد، در این صورت $a + u = ۰_R$ و $a + v = ۰_R$ و لذا

$$v = ۰_R + v = (a + u) + v = (u + a) + v = u + (a + v) = u + ۰_R = u.$$

بنابراین u تنها جواب است. ■

حال می‌توانیم منفی یک عنصر و تفریق عناصر در یک حلقه را با نسخه‌برداری از آنچه که در حلقه‌های آشنا مثل $\mathbb{Z}$ اتفاق می‌افتد تعریف کنیم. فرض کنید R یک حلقه باشد و $a \in R$. طبق قضیه ۳.۲، معادله $a + x = ۰_R$ دارای یک جواب یکتا است. با بکارگیری نماد رایج "ـ" در حلقه $\mathbb{Z}$، این جواب یکتا را با نماد "$-a$" نشان می‌دهیم. چون جمع جابجایی است،

$-a$ عضو یکتای R است به طوری که

$$a + (-a) = ۰_R = (-a) + a.$$

در حلقه‌های آشنا، این تعریف با مفهوم شناخته شده منفی یک عضو مطابقت دارد. مهم‌تر آن که این امر معنایی برای "منفی" در هر حلقه فراهم می‌کند.

مثال ۱۶.۳. در حلقه $\mathbb{Z}_۶$ جواب معادله $x + ۲ = ۰$، عدد ۴ است و بنابراین در این حلقه $۴ = -۲$. به‌طور مشابه در $\mathbb{Z}_{۱۲}$، $۵ = -۹$ زیرا ۵ جواب $x + ۹ = ۰$ است. پس تفریق $b - a$

در یک حلقه به‌وسیله قانون

$$b + (-a)$$

تعریف می‌شود. در $\mathbb{Z}$ و حلقه‌های آشنای دیگر، این همان تفریق معمولی است در حالی که در حلقه‌های دیگر یک عمل جدید داریم:

مثال ۱۷.۳. در $\mathbb{Z}_۶$ داریم $۵ = ۴ + ۱ = (-۲) + ۱ = ۲ - ۱$.

در دبیرستان با بسیاری از قوانین محاسباتی و جبری در ارتباط با منفی‌ها و تفریق آشنا شده‌اید. دو قضیه زیر نشان می‌دهد که همین قوانین در هر حلقه‌ای معتبر هستند. اگرچه این قوانین فی‌نفسه چندان جالب توجه نیستند، با این حال اثبات معتبربودن آنها به منظور بکارگیری در محاسبات در حلقه‌های دلخواه ضروری است.

قضیه ۳.۳. اگر در یک حلقه R، $a + b = a + c$ در این صورت $b = c$.

برهان. با اضافه کردن $-a$ به دو طرف $a + b = a + c$ و آنگاه استفاده از شرکت‌پذیری و منفی‌ها می‌بینید که

$$-a + (a + b) = -a + (a + c)$$
$$(-a + a) + b = (-a + a) + c$$
$$۰_R + b = ۰_R + c$$
$$b = c,$$

که نتیجه مطلوب است. ■

قضیه ۴.۳. برای هر دو عضو a و b از یک حلقه R،

$$a \cdot {}^\circ_R = {}^\circ_R = {}^\circ_R \cdot a \qquad (۱)$$

$$a(-b) = -(ab) = (-a)b \qquad (۲)$$

$$-(-a) = a \qquad (۳)$$

$$-(a+b) = -a - b \qquad (۴)$$

$$-(a-b) = -a + b \qquad (۵)$$

$$(-a)(-b) = ab. \qquad (۶)$$

اگر R یکدار باشد در این صورت

$$(-1_R)a = -a. \qquad (۷)$$

برهان. (۱) چون ${}^\circ_R = {}^\circ_R + {}^\circ_R$، قانون توزیع‌پذیری نشان می‌دهد که

$$a \cdot {}^\circ_R + a \cdot {}^\circ_R = a({}^\circ_R + {}^\circ_R) = a \cdot {}^\circ_R = a \cdot {}^\circ_R + {}^\circ_R.$$

بکارگیری قضیه ۳.۳ برای قسمتهای اول و آخر این معادله نشان می‌دهد که $a \cdot {}^\circ_R = {}^\circ_R$. اثبات این که ${}^\circ_R \cdot a = {}^\circ_R$ به‌طور مشابه انجام می‌شود.

(۲) طبق تعریف، $-(ab)$ جواب یکتای معادله $ab + x = {}^\circ_R$ است، و لذا هر جواب دیگر این معادله بایستی برابر $-(ab)$ باشد. امّا طبق قانون توزیع‌پذیری و (۱)، $x = a(-b)$ یک جواب است زیرا

$$ab + a(-b) = a[b + (-b)] = a[{}^\circ_R] = {}^\circ_R.$$

بنابراین $-(ab) = a(-b)$. قسمتهای دیگر به‌طور مشابه اثبات می‌شود،

(۳) طبق تعریف، $-(-a)$ جواب یکتای $(-a) + x = {}^\circ_R$ است. امّا a یک جواب این معادله است چون $a + (-a) = {}^\circ_R$. بنابراین طبق یکتایی $-(-a) = a$.

(۴) طبق تعریف، $-(a+b)$ جواب یکتای $(a+b) + x = {}^\circ_R$ است امّا $(-a) + (-b)$ نیز یک جواب است:

$$\begin{aligned}(a+b) + [(-a) + (-b)] &= b + [a + (-a)] + (-b) \\ &= (b + {}^\circ_R) + (-b) \\ &= b + (-b) = {}^\circ_R\end{aligned}$$

بنابراین طبق یکتایی $-(a+b) = (-a) + (-b)$.

(۵) طبق تفریق و (۴) و (۳) داریم

$$-(a-b) = -(a+(-b)) = (-a)+(-(-b)) = -a+b.$$

(۶) طبق (۳) و استفاده مکرر از (۲) داریم

$$(-a)(-b) = -[a(-b)] = -[-(ab)] = ab.$$

(۷) طبق (۲)، $(-1_R)a = -(1_R a) = -(a) = -a$. ■

هنگام انجام حساب معمولی، نماد توان مانند مشابه جمعی آن (برای مثال، $a+a+a = 3a$) یک نماد کاملاً مناسب است. اکنون این مفاهیم را به حلقه‌های دلخواه انتقال می‌دهیم.

اگر R یک حلقه دلخواه، $a \in R$ و n یک عدد صحیح مثبت باشد، در این صورت تعریف می‌کنیم:

$$a^n = aa\ldots a \qquad (n \text{ عامل}).$$

به‌سادگی بررسی می‌شود که برای هر $a \in R$ و اعداد صحیح مثبت m و n،

$$a^m a^n = a^{m+n} \quad \text{و} \quad (a^m)^n = a^{mn}.$$

اگر R یکدار و a مخالف 0_R باشد، در این صورت a^0 را عضو 1_R تعریف می‌کنیم. در این حالت قوانین توان فوق برای هر $m, n \geq 0$ برقرار است.

اگر R یک حلقه، $a \in R$ و n یک عدد صحیح مثبت باشد، در این صورت تعریف می‌کنیم

$$na = a+a+a+\cdots+a \qquad (n \text{ جمعوند})$$
$$-na = (-a)+(-a)+(-a)+\cdots+(-a) \qquad (n \text{ جمعوند}).$$

سرانجام تعریف می‌کنیم $0a = 0_R$. تعریف na، در حلقه‌های معمولی چیز جدیدی نیست امّا در حلقه‌های دیگر به "ضرب" یک عدد صحیح n در یک عضو a از حلقه تعبیر می‌شود.

مثال ۱۸.۳. فرض کنید R یک حلقه و $a, b \in R$. در این صورت

$$(a+b)^2 = (a+b)(a+b) = a(a+b)+b(a+b)$$
$$= aa+ab+ba+bb = a^2+ab+ba+b^2$$

دقت کنید اگر $ab \neq ba$ در این صورت جملات میانی عبارت فوق را نمی‌توان ترکیب کرد. با این‌حال اگر R جابجایی باشد در این صورت $ab = ba$ و فرمول آشنای

$$(a+b)^2 = a^2 + ab + ba + b^2 = a^2 + ab + ab + b^2 = a^2 + 2ab + b^2$$

را داریم. برای محاسبه $(a+b)^n$ در یک حلقه جابجایی، با $n > 2$، قضیه دوجمله‌ای در پیوست **ث** را ملاحظه کنید.

با پایه‌ریزی مفاهیم اساسی درباره حساب در حلقه‌ها اکنون به مبحث جبر و جواب معادلات می‌پردازیم.

قضیه ۵.۳. فرض کنید R یک حلقه باشد و $a, b \in R$. در این صورت معادله $a + x = b$ دارای جواب یکتای $x = b - a$ است.

برهان. $x = b - a$ یک جواب است زیرا

$$\begin{aligned} a + [b - a] &= a + [b + (-a)] = a + [-a + b] \\ &= [a + (-a)] + b = 0_R + b = b. \end{aligned}$$

اگر w هر جواب دیگر این معادله باشد در این صورت $a + w = b = a + (b - a)$. لذا طبق قضیه ۳.۳، $w = b - a$. بنابراین $x = b - a$ تنها جواب است. ■

معادله ضربی $ax = b$ ممکن است دارای جواب نباشد. برای مثال، $4x = 11$ در $\mathbb{Z}$ دارای جواب نیست. امّا حالتی وجود دارد که در آن این معادله دارای جواب است. اگر a یک عضو غیرصفر یک حلقه تقسیمی R باشد، در این صورت طبق اصل ۱۲، معادله $ax = 1_R$ دارای یک جواب u و معادله $xa = 1_R$ دارای یک جواب v است. با بکارگیری این حقیقت که $au = 1_R$ و $va = 1_R$ می‌بینیم که $u = 1_R u = (va)u = v(au) = v1_R = v$. بنابراین برای هر عضو غیرصفر a در یک حلقه‌تقسیمی، عضو u چنان موجود است که $au = ua = 1_R$. برای توصیف این وضعیت به چند اصطلاح علمی نیازمندیم.

تعریف. عضو a در یک حلقه یکدار R **یکه** نامیده می‌شود اگر $u \in R$ وجود داشته باشد به طوری که $au = ua = 1_R$. در این حالت عنصر u **وارون** یا **معکوس (ضربی)** a نامیده شده و با a^{-1} نشان داده می‌شود.

نماد استفاده‌شده برای نمایش وارون یک عضو یکه، از نماد توان معمولی در اعداد حقیقی، که در آنجا $a^{-1} = 1/a$، الگو گرفته است. همانگونه که در بالا ذکر شد، هر عضو غیرصفر یک حلقه تقسیمی یکه است. عناصر یکه در حلقه‌های دیگر نیز موجودند.

مثال ۱۹.۳. در $\mathbb{Z}_{10}$، عنصر ۷ یکه است زیرا $7 \cdot 3 = 21 = 1$. در این حالت $7^{-1} = 3$. به‌طور کلی‌تر بنابه قضیه ۹.۲، a در $\mathbb{Z}_n$ یکه است اگر و تنها اگر $(a, n) = 1$ در $\mathbb{Z}$.

مثال ۲۰.۳. تنها یکه‌های $\mathbb{Z}$، ۱ و ۱- هستند (چرا؟). امّا در حلقه ماتریسی غیرجابجایی $M(\mathbb{Z})$ تعداد زیادی یکه وجود دارد: برای مثال

$$\begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$$

یکه است زیرا

$$\begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix} \begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}.$$

عناصر یکه در یک حلقه ماتریسی، ماتریس‌های **وارون‌پذیر** نامیده می‌شوند.

قضیه ۶.۳. فرض کنید R یک حلقه یکدار باشد و $a, b \in R$. اگر a یکه باشد در این صورت هر یک از معادلات $ax = b$ و $ya = b$ دارای جواب یکتا در R است.

گرچه هر معادله دارای یک جواب یکتا است امّا در حالت حلقه‌های ناجابجایی ممکن است جواب $ax = b$ برابر جواب $ya = b$ نباشد؛ به‌عنوان مثال تمرین ۵ را ملاحظه کنید.

برهان قضیه ۶.۳. چون a یکه است، دارای یک وارون $a^{-1} \in R$ می‌باشد به‌طوری که $a^{-1}a = 1_R = aa^{-1}$. پس $x = a^{-1}b$ یک جواب $ax = b$ است زیرا $a(a^{-1}b) = (aa^{-1})b = 1_R b = b$. اگر $x = c$ جواب دیگری باشد در این صورت $ac = b$ و $c = 1_R c = (a^{-1}a)c = a^{-1}(ac) = a^{-1}b$. بنابراین $x = a^{-1}b$ تنها جواب است. اثباتی مشابه نشان می‌دهد که $y = ba^{-1}$ جواب یکتای $ya = b$ است. ■

در حساب معمولی در $\mathbb{Z}$ اغلب از قانون حذف استفاده می‌شود: اگر $a \neq 0$ و $ab = ac$ در این صورت $b = c$. با این‌حال قانون حذف در هر حلقه‌ای کار نمی‌کند. برای مثال در $\mathbb{Z}_{12}$، $10 \cdot 204 = 2010$ امّا $10 \neq 4$. این تفاوت از آنجا ناشی می‌شود که $\mathbb{Z}$ دامنه صحیح است و $\mathbb{Z}_{12}$ نیست.

قضیه ۷.۳. فرض کنید R یک حلقه جابجایی یکدار باشد. در این صورت R یک دامنه صحیح است اگر و تنها اگر دارای خاصیت حذف زیر باشد:

هرگاه $a \neq 0_R$ و $ab = ac$ در R آنگاه $a = c$.

برهان. در هر حلقه اگر $ab = ac$ آنگاه $ab - ac = 0_R$، لذا $a(b-c) = 0_R$. اگر R یک دامنه صحیح باشد و $a \neq 0_R$، در این صورت طبق اصل ۱۱ باید داشته باشیم $b - c = 0_R$ یا به‌طور معادل $b = c$. بالعکس، فرض کنید که خاصیت حذف در R برقرار است. برای نشان دادن این که R یک دامنه صحیح است کافی است بررسی کنیم که اصل ۱۱ برقرار است. اگر $ab = 0_R$ در این صورت یا $a = 0_R$ و یا $a \neq 0_R$. اگر $a \neq 0_R$ در این صورت بکارگیری قانون حذف برای $ab = 0_R = a0_R$ نشان می‌دهد که $b = 0_R$. در هر حال یا $a = 0_R$ یا $b = 0_R$. بنابراین R یک دامنه صحیح است. ■

نتیجه ۸.۳. هر میدان R یک دامنه صحیح است.

برهان. هر میدان یک حلقه جابجایی یکدار است. فرض کنید $ab = ac$ و $a \neq 0_R$. پس a یکه است و از ضرب دو طرف $ab = ac$ در a^{-1} به‌دست می‌آید $b = c$. بنابراین طبق قضیه ۷.۳، R یک دامنه صحیح است. ■

عکس نتیجه ۸.۳ در حالت کلی درست نیست ($\mathbb{Z}$ یک دامنه صحیح است که میدان نیست)، با این‌حال در صورت متناهی بودن حلقه، درست می‌باشد.

قضیه ۹.۳. هر دامنه صحیح متناهی R یک میدان است.

برهان. چون R یک حلقه جابجایی یکدار است کافی است نشان دهیم که برای هر $a \neq 0_R$، معادله $ax = 1_R$ دارای یک جواب است. فرض کنید a_1، a_2، ...، a_n همه عناصر (متمایز) R باشند و فرض کنید $a_t \neq 0_R$. به‌منظور نشان دادن این که $a_t x = 1_R$ دارای یک جواب

است، ضربهای a_ta_1، a_ta_2، a_ta_3، ...، a_ta_n را در نظر بگیرید. اگر $a_i \neq a_j$ در این صورت $a_ta_i \neq a_ta_j$ (زیرا طبق قانون حذف، $a_ta_i = a_ta_j$ برابری $a_i = a_j$ را به‌دست می‌دهد). بنابراین a_ta_1، a_ta_2، ...، a_ta_n، n عضو متمایز از R هستند. امّا R دقیقاً دارای n عضو است و لذا اینها باید ترتیبی از همه عناصر R باشند. بویژه برای برخی j، $a_ta_j = 1_R$. بنابراین معادله $a_tx = 1_R$ دارای یک جواب است و لذا R میدان است. ■

این بخش را با ارائه چند اصطلاح علمی مناسب دیگر به پایان می‌بریم.

تعریف. یک عضو غیر صفر a در یک حلقه جابجایی R یک **مقسوم‌علیه‌صفر** است اگر عضو غیرصفر b از R موجود باشد به‌قسمی که $ab = 0_R$.

به‌عنوان مثال در $\mathbb{Z}_6$، ۳ یک مقسوم‌علیه صفر است زیرا $3 \cdot 2 = 0$. توجه کنید که 0_R یک مقسوم‌علیه صفر نیست. می‌توان یک دامنه صحیح را به عنوان یک حلقه جابجایی غیرصفر یکدار که دارای هیچ مقسوم‌علیه صفر نیست توصیف نمود. هیچ عضو یکه، یک مقسوم‌علیه صفر نیست (تمرین ۹)، امّا عضوی که مقسوم‌علیه صفر نباشد لزوماً یکه نیست (برای مثال، ۲ در $\mathbb{Z}$ نه یک مقسوم‌علیه صفر و نه یک یکه است).

تمرینها

A.۱. فرض کنید R یک حلقه باشد و $a, b \in R$.

(الف) $(a+b)(a-b) = ?$ (ب) $(a+b)^2 = ?$

(پ) اگر R جابجایی باشد جوابهای (الف) و (ب) چه هستند؟

۲. عضو e از یک حلقه R **خودتوان** نامیده می‌شود اگر $e^2 = e$.

(الف) چهار عضو خودتوان در $M(\mathbb{R})$ بیابید.

(ب) همه خودتوانهای $\mathbb{Z}_{12}$ را بیابید.

۳. ثابت کنید 0_R و 1_R تنها خودتوانهای یک دامنه صحیح R هستند.

۴. اگر e یک عضو خودتوان در یک حلقه R باشد و $x \in R$، نشان دهید $(xe - exe)^2 = 0_R$.

۵. در حلقه $M(\mathbb{R})$ فرض کنید

$$A=\begin{pmatrix}۱ & ۲\\ ۰ & ۱\end{pmatrix} \quad B=\begin{pmatrix}۴ & ۱\\ ۱ & -۱\end{pmatrix} \quad C=\begin{pmatrix}۲ & ۳\\ ۱ & -۱\end{pmatrix} \quad D=\begin{pmatrix}۴ & -۷\\ ۱ & -۳\end{pmatrix}.$$

نشان دهید معادلات $AX=B$ در $XA=B$ جوابهای متفاوت دارد. [راهنمایی: بررسی کنید که آیا C یا D جواب هر یک از این معادلات می‌باشد.]

۶. اثبات یا رد کنید: مجموعه یکه‌ها در یک حلقه R یک زیرحلقه R است.

۷. (الف) اگر a و b یکه‌هایی در یک حلقه یکدار R باشند، ثابت کنید که ab نیز یک یکه است و $(ab)^{-۱}=b^{-۱}a^{-۱}$.

(ب) مثالی بزنید که نشان دهد اگر a و b یکه باشند آنگاه $(ab)^{-۱}$ ممکن است برابر $a^{-۱}b^{-۱}$ نباشد. [راهنمایی: ماتریس‌های i و k در حلقه چهارگانی H را در نظر بگیرید.]

۸. فرض کنید R یک حلقه یکدار باشد و $a\in R$. اگر $a^{۲}=۰_R$، ثابت کنید $a+۱_R$ و $a-۱_R$ یکه است.

۹. ثابت کنید یک یکه در یک حلقه جابجایی نمی‌تواند یک مقسوم‌علیه صفر باشد.

۱۰. همه یکه‌ها و مقسوم‌علیه‌های صفر حلقه P متشکل از همه زیرمجموعه‌های $\{a,b,c\}$ را بیابید. [تمرین ۱۱ بخش ۱.۳ را ملاحظه کنید.]

۱۱. همه یکه‌ها و مقسوم‌علیه‌های صفر حلقه $R\times\mathbb{Z}_۴$ را که در آن R حلقه تمرین ۵ بخش ۱.۳ می‌باشد را بیابید.

۱۲. اگر R و S حلقه‌های جابجایی غیرصفر باشند، نشان دهید که $R\times S$ همیشه دارای مقسوم‌علیه صفر است.

۱۳. فرض کنید R یک حلقه‌یکدار جابجایی باشد و $a\in R$. اگر $a^{۲}=۱_R$ و $a\neq\pm۱_R$ ثابت کنید که $a+۱_R$ و $a-۱_R$ مقسوم‌علیه صفر هستند.

۱۴. (الف) اگر ab یک مقسوم‌علیه صفر در یک حلقه جابجایی R باشد، ثابت کنید که a یا b یک مقسوم‌علیه صفر است.

(ب) اگر a یا b در R مقسوم‌علیه صفر باشد و $ab\neq۰_R$، ثابت کنید که ab یک مقسوم‌علیه صفر است.

۱۵. فرض کنید R یک حلقه جابجایی باشد و $a \in R$. فرض کنید $a \neq 0_R$ و a یک مقسوم‌علیه صفر نباشد. ثابت کنید هرگاه $ab = ac$ در R، در این صورت $b = c$.

۱۶. فرض کنید R یک حلقه جابجایی باشد و $a, b \in R$. فرض کنید m و n اعداد صحیح مثبت باشند.

(الف) نشان دهید $a^m a^n = a^{m+n}$ و $(a^m)^n = a^{mn}$.

(ب) تحت چه شرایطی برابری $(ab)^n = a^n b^n$ برقرار است؟

۱۷.B. فرض کنید S یک زیرمجموعه غیرتهی از یک حلقه R باشد. ثابت کنید S یک زیرحلقه R است اگر و تنها اگر برای هر $a, b \in S$ هر دو $a - b$ و ab در S باشند.

۱۸. (الف) اگر S یک زیرحلقه R باشد، ثابت کنید که $0_S = 0_R$. [راهنمایی: برای $a \in S$، معادله $a + x = a$ را در نظر بگیرید.]

(ب) فرض کنید S یک زیرحلقه R باشد. اگر R و S یکدار باشند با مثال نشان دهید که ممکن است 1_S و 1_R یکسان نباشند.

(پ) اگر هر دو R و S میدان باشند ثابت کنید که $1_S = 1_R$.

۱۹. فرض کنید R یک مجموعه مجهز به دو عمل جمع و ضرب باشد که در اصول ۱، ۲ و ۱۰-۴ اولین تعریف بخش ۳-۱ صدق کند. ثابت کنید R یک حلقه است. [راهنمایی: برای نشان دادن $a + b = b + a$، به دو طریق، $(a + b)(1_R + 1_R)$ را بسط دهید.]

۲۰. (الف) فرض کنید R یک حلقه باشد و $a, b \in R$. فرض کنید m و n اعداد صحیح غیر منفی باشند و ثابت کنید که

$$(m + n)a = ma + na \qquad \text{(i)}$$

$$m(a + b) = ma + mb \qquad \text{(ii)}$$

$$m(ab) = (ma)b = a(mb) \qquad \text{(iii)}$$

$$(ma)(nb) = mn(ab) \qquad \text{(iv)}$$

(ب) قسمت (الف) را برای حالتی که m و n دو عدد صحیح دلخواه باشد انجام دهید.

۲۱. یک حلقه بولی [۶] یک حلقه یکدار R است که در آن برای هر $x \in R$، $x^2 = x$. به عنوان مثال تمرینهای ۱۱ و ۳۶ در بخش ۱.۳ را ملاحظه کنید. اگر R یک حلقه بولی باشد ثابت

۶) Boolean Ring

کنید که

(الف) $a + a = 0_R$ برای هر $a \in R$. [راهنمایی: $(a+a)^2$ را بسط دهید.]

(ب) R جابجایی است. [راهنمایی، $(a+b)^2$ را بسط دهید.]

۲۲. فرض کنید R یک حلقه جابجایی یکدار باشد و $t \in R$. فرض کنید T زیرحلقه R شامل همه مضارب t باشد (تمرین ۱۶ در بخش ۱.۳ را ملاحظه کنید). اگر u یک یکه در R باشد و $u \in T$، ثابت کنید $T = R$.

۲۳. فرض کنید که $R = \{0_R, 1_R, a, b\}$ یک حلقه است و این که a و b یکه هستند. جدول ضربی R را بنویسید.

۲۴. فرض کنید R و S حلقه‌های یکدار باشند. یکه‌های حلقه $R \times S$ چه هستند؟

۲۵. (الف) ثابت کنید یک عضو غیرصفر $\mathbb{Z}_n$ یک مقسوم‌علیه صفر است اگر و تنها اگر یکه نباشد.

(ب) مثالی از یک حلقه بزنید که در آن قسمت (الف) نادرست است.

۲۶. عضو a از یک حلقه را **پوچ‌توان** گویند اگر برای برخی عدد صحیح مثبت n، $a^n = 0_R$. ثابت کنید که R دارای هیچ عضو پوچ‌توان غیرصفر نیست اگر و تنها اگر 0_R تنها جواب معادلهٔ $x^2 = 0_R$ باشد.

۲۷. فرض کنید R یک حلقه باشد و $a \in R$. فرض کنید $S = \{r \in R \mid ra = 0_R\}$. ثابت کنید S یک زیرحلقه Rاست.

۲۸. فرض کنید R یک حلقه یکدار باشد. اگر یک کوچکترین عدد صحیح مثبت n چنان موجود باشد که $n1_R = 0_R$، در این صورت R یک حلقه دارای **مشخصه n** نامیده می‌شود. اگر چنین n ای موجود نباشد، R یک حلقه دارای **مشخصه صفر** نامیده می‌شود. نشان دهید که $\mathbb{Z}$ دارای مشخصه صفر و $\mathbb{Z}_n$ دارای مشخصه n است. مشخصه $\mathbb{Z}_4 \times \mathbb{Z}_6$ چیست؟

۲۹. فرض کنید R یک حلقه یکدار از مشخصه $n > 0$ باشد.

(الف) ثابت کنید برای هر $a \in R$، $na = 0_R$.

(ب) اگر R یک دامنه صحیح باشد، ثابت کنید که n اول است.

۳۰. ثابت کنید

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

یک یکه در $M(\mathbb{R})$ است اگر و تنها اگر $ad - bc \neq 0$. در این حالت بررسی کنید که وارون آن

$$\begin{pmatrix} d/t & -b/t \\ -c/t & a/t \end{pmatrix}$$

است که در آن $t = ad - bc$.

۳۱. فرض کنید R یک حلقه بدون عضو همانی باشد. فرض کنید T مجموعه $R \times \mathbb{Z}$ باشد. جمع و ضرب در T را توسط قوانین زیر تعریف کنید:

$$(r, m) + (s, n) = (r + s, m + n)$$
$$(r, m)(s, n) = (rs + ms + nr, mn).$$

(الف) ثابت کنید T یک حلقه یکدار است.

(ب) فرض کنید R^* شامل همه عناصر به صورت $(r, 0)$ در T باشد. ثابت کنید R^* یک زیرحلقه T است.

۳۲. (الف) فرض کنید a و b عناصر پوچ‌توان در یک حلقه جابجایی R باشند (تمرین ۲۶ را ملاحظه کنید). ثابت کنید ab و $a + b$ نیز پوچ‌توانند. [به قضیه دوجمله‌ای در پیوست ث نیاز خواهید داشت.]

(ب) فرض کنید N مجموعه همه عناصر پوچ‌توان R باشد. نشان دهید N یک زیرحلقه R است.

۳۳. فرض کنید R یک حلقه باشد که در آن برای هر $x \in R$، $x^3 = x$. نشان دهید R جابجایی است.

۳۴. فرض کنید R یک حلقه جابجایی متناهی غیرصفر باشد که دارای هیچ مقسوم‌علیه صفر نیست. ثابت کنید R یک میدان است.

۳-۳ یکریختـــی

چنانچه با دستگاه عددنویسی رومی آشنا نباشید و وارد بحثی از حساب اعداد صحیح شوید که صرفاً با دستگاه عددنویسی رومی نوشته شده باشد، در این صورت ممکن است مدتی طول بکشد تا تشخیص دهید که به جز نمایه‌گذاری عناصر، این حساب اساساً همان حساب آشنای در $\mathbb{Z}$ است. ذیلاً یک مثال کمتر بدیهی ارائه می‌شود.

مثال ۲۱.۳. زیرمجموعه $S = \{0, 2, 4, 6, 8\}$ از $\mathbb{Z}_{10}$ را در نظر بگیرید. همانگونه که از جداول زیر دیده می‌شود، با جمع و ضرب $\mathbb{Z}_{10}$، S در واقع یک حلقه جابجایی است.

$+$	۰	۶	۲	۸	۴
۰	۰	۶	۲	۸	۴
۶	۶	۲	۸	۴	۰
۲	۲	۸	۴	۰	۶
۸	۸	۴	۰	۶	۲
۴	۴	۰	۶	۲	۸

$\cdot$	۰	۶	۲	۸	۴
۰	۰	۰	۰	۰	۰
۶	۰	۶	۲	۸	۴
۲	۰	۲	۴	۶	۸
۸	۰	۸	۶	۴	۲
۴	۰	۴	۸	۲	۶

بررسی دقیق این جداول نشان می‌دهد که S یک میدان پنج عضوی است و این که عضو همانی ضربی این میدان ۶ است.

ادعا می‌کنیم که S "اساساً همان" میدان $\mathbb{Z}_5$ است. این را می‌توانید از آنچه در پی می‌آید ملاحظه کنید. جداول جمع و ضرب برای $\mathbb{Z}_5$ را بنویسید. به‌منظور جلوگیری از هرگونه احتمال اشتباه با عناصر S، اعضای $\mathbb{Z}_5$ را با $\bar{0}$، $\bar{1}$، $\bar{2}$، $\bar{3}$ و $\bar{4}$ نشان دهید. سپس درایه‌های جداول مربوط به $\mathbb{Z}_5$ را بدین طریق نمایه‌گذاری مجدد نمائید: نشان ۰ به جای $\bar{0}$، نشان ۶ به جای $\bar{1}$، نشان ۲ به جای $\bar{2}$، نشان ۸ به جای $\bar{3}$ و نشان ۴ به جای $\bar{4}$. ملاحظه کنید چه اتفاق می‌افتد:

+	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{8}$	$\bar{4}$	$\bar{0}$	$\bar{6}$
$\bar{8}$	$\bar{8}$	$\bar{4}$	$\bar{0}$	$\bar{6}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$

	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{8}$	$\bar{0}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{2}$	$\bar{6}$

با نمایه‌گذاری مجدد عناصر $\mathbb{Z}_5$، جداول جمع و ضرب برای S را بدست می‌آورید. بنابراین کارکرد اعمال در $\mathbb{Z}_5$ و S دقیقاً به یک صورت است، تنها تفاوت در روشی است که عناصر نمایه‌گذاری شده‌اند. تا آنجا که ساختار حلقه‌ای مطرح است، S همان $\mathbb{Z}_5$ با نمایه‌گذاری جدیدی روی عناصر آن است. به بیان فنی‌تر، $\mathbb{Z}_5$ و S یکریخت می‌باشند.

در حالت کلی، حلقه‌های یکریخت، حلقه‌هایی هستند که دارای ساختار یکسانند، به این مفهوم که با نمایه‌گذاری مجدد و مناسب عناصر، جداول جمع و ضرب یکی به جداول دیگری تبدیل می‌شود. اگرچه این ایده برای دستگاههای متناهی کوچک مناسب است، با این‌حال به یک تعریف دقیق ریاضی از یکریختی نیاز داریم که با این ایده شهودی هماهنگ و قابل بکارگیری در حلقه‌های بزرگ نیز باشد. در درکِ شهودی مفهوم "R و S یکریختند"، دو جنبه وجود دارد: نمایه‌گذاری مجدد و مقایسه جداول. معنی نمایه‌گذاری مجدد این است که هر عضو R با یک عضو یکتای S (نشان جدیدش) مقایسه شود. به عبارت دیگر، تابع $f : R \to S$ وجود دارد که به هر $r \in R$ نشان جدیدش $f(r) \in S$ را نظیر می‌کند. در مثال بالا، ما از تابع نمایه‌گذاری مجدد $f : \mathbb{Z}_5 \to S$ که توسط

$$f(\bar{0}) = 0, \quad f(1) = 6 \quad f(\bar{2}) = 2 \quad f(\bar{3}) = 8 \quad f(\bar{4}) = 4$$

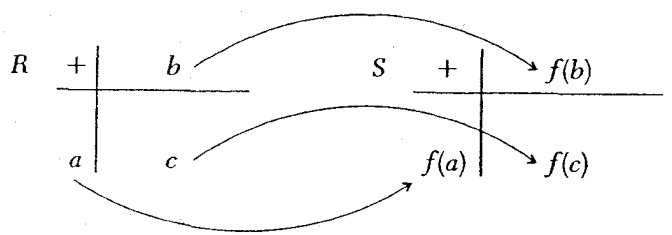
تعریف می‌شود، استفاده کردیم. چنین تابعی باید خواص اضافی زیر را دارا باشد:

(i) نشان‌های جدید عناصر متمایز R بایستی متمایز باشند؛ اگر $r \neq r'$ در R، در این صورت $f(r) \neq f(r')$ در S.

(ii) هر عضو S بایستی نشان عضوی از R باشد[۷]

گزاره‌های (i) و (ii) در واقع بیان می‌کنند که f باید هم یک به یک و هم پوشا باشد[۸]، یعنی f باید دوسویی باشد.

با این حال، یک دوسویی f (طرح نمایه‌گذاری) یک یکریختی نخواهد بود مگر این که پس از تأثیر f، جداول R به جداول S تبدیل شود. در این حالت اگر در R، $a + b = c$، در این صورت جداول R و S بایستی به صورت زیر به‌نظر آیند:



جدول S نشان می‌دهد که $f(a) + f(b) = f(c)$. ولی $a + b$ و c در R برابرند، لذا $f(a + b) = f(c)$ و بنابراین

$$f(a + b) = f(a) + f(b).$$

این شرطی است که f به‌منظور تبدیل جدول جمع R به جدول جمع S باید در آن صدق کند. شرط مشابه روی f برای جدول ضرب عبارت است از $f(ab) = f(a)f(b)$. حال می‌توانیم تعریف رسمی یکریختی را بیان کنیم:

تعریف. حلقه R **یکریخت** با حلقه S است (به صورت نمادین $R \cong S$) اگر تابع $f : R \to S$ چنان موجود باشد که

(i) f یک به یک باشد؛

۷) در غیر این‌صورت به هیچ وجه ممکن جداول کامل S را از جداول R به دست نمی‌آوریم.

۸) توابع یک به یک، پوشا و دوسویی در پیوست ب بحث شده‌اند.

(ii) f پوشا باشد؛

(iii) برای هر $a, b \in R$، $f(a+b) = f(a) + f(b)$ و $f(ab) = f(a)f(b)$.

در این حالت f یک **یکریختی** نامیده می‌شود. تابعی که در شرط (iii) صدق کند امّا لزوماً یک به یک یا پوشا نباشد یک **همریختی** نامیده می‌شود.

هشدار: برای این که یک تابع یکریختی باشد باید در هر سه شرط تعریف صدق کند. این کاملاً امکان‌پذیر است که یک تابع تنها در دو شرط از شروط تعریف صدق کند اما در شرط سوم صدق نکند: تمرین ۹.۲ و ۲۲ را ملاحظه کنید.

هشدار: شرط (iii) تعریف، تنها بازی کردن با نمادها نیست. بسیاری از توابع، از جمله تابع $f : \mathbb{R} \to \mathbb{R}$ که توسط $f(x) = x + ۲$ تعریف می‌شود، همریختی نیستند. این تابع در شرط (iii) صدق نمی‌کند زیرا به عنوان مثال:

$$f(۳ + ۴) = f(۷) = ۹، \text{ امّا } ۱ = ۵ + ۶ = f(۳) + f(۴)؛$$
$$f(۳ \times ۴) = f(۱۲) = ۱۴، \text{ امّا } ۳۰ = ۵ \times ۶ = f(۳)f(۴).$$

مثال ۲۲.۳. در مثال ۱۳.۳، میدان $\mathbb{K}$ متشکل از ماتریس‌های ۲×۲ به صورت

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

که در آن a و b اعداد حقیقی هستند را در نظر گرفتیم. ادعا می‌کنیم $\mathbb{K}$ یکریخت با میدان اعداد مختلط $\mathbb{C}$ است. برای اثبات، تابع $f : \mathbb{K} \to \mathbb{C}$ را توسط قانون

$$f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi$$

تعریف کنید. برای اثبات یک به یک بودن f، فرض کنید

$$f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = f\begin{pmatrix} r & s \\ -s & r \end{pmatrix}.$$

در این صورت طبق تعریف f، $a+bi=r+si$ در $\mathbb{C}$. طبق قوانین برابری در $\mathbb{C}$، باید $a=r$ و $b=s$. بنابراین در $\mathbb{K}$ داریم،

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} r & s \\ -s & r \end{pmatrix}$$

و لذا f یک به یک است. تابع f پوشا است زیرا هر عدد مختلط $a+bi$، تصویر ماتریس

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

در $\mathbb{K}$ تحت تابع f است. سرانجام برای هر دو ماتریس A و B در $\mathbb{K}$ باید نشان دهیم که $f(A+B)=f(A)+f(B)$ و $f(AB)=f(A)f(B)$. داریم

$$\begin{aligned} f\left[\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right] &= f\begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \\ &= (a+c)+(b+d)i \\ &= (a+bi)+(c+di) \\ &= f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + f\begin{pmatrix} c & d \\ -d & c \end{pmatrix} \end{aligned}$$

و

$$\begin{aligned} f\left[\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right] &= f\begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} \\ &= (ac-bd)+(ad+bc)i \\ &= (a+bi)(c+di) \\ &= f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} f\begin{pmatrix} c & d \\ -d & c \end{pmatrix}. \end{aligned}$$

بنابراین f یک یکریختی است.

این کاملاً امکان‌پذیر است که عناصر یک حلقه را به طریقی نمایه‌گذاری مجدد نمود که حلقه‌ای جدید یکریخت با خودش به دست آید.

مثال ۲۳.۳. فرض کنید $f : \mathbb{C} \to \mathbb{C}$ نگاشت مزدوجی مختلط تعریف شده توسط $f(a+bi) = a-bi$ باشد[۹]. تابع f یک همریختی است زیرا

$$\begin{aligned} f[(a+bi)+(c+di)] &= f[(a+c)+(b+d)i] \\ &= (a+c)-(b+d)i = (a-bi)+(c-di) \\ &= f(a+bi)+f(c+di) \\ f[(a+bi)(c+di)] &= f[(ac-bd)+(ad+bc)i] \\ &= (ac-bd)-(ad+bc)i = (a-bi)(c-di) \\ &= f(a+bi)f(c+di). \end{aligned}$$

به سادگی بررسی می‌شود که f یک به یک و پوشا است (تمرین ۱۳). بنابراین f یکریختی است.

اگر حدس می‌زنید که دو حلقه یکریخت باشند، هیچ قانون ساده و سریعی برای یافتن تابعی که یک یکریختی بین آنها تعریف کند وجود ندارد. یافتن چنین تابعی ممکن است مقدار زیادی آزمایش و خطا در بر داشته باشد و همواره این احتمال وجود دارد که هیچ یکریختی بین آنها موجود نباشد. با این حال آگاهی به شرایطی که یک یکریختی بایستی در آن صدق کند بعضاً می‌تواند ما را به چگونگی ساختن چنین تابعی رهنمون کند.

قضیه ۱۰.۳. فرض کنید $f : R \to S$ یک همریختی حلقه‌ای باشد. در این صورت

(۱) $f(0_R) = 0_S$.

(۲) $f(-a) = -f(a)$ برای هر $a \in R$.

اگر R و S هر دو یکدار باشند و f یک یکریختی باشد، در این صورت

(۳) $f(1_R) = 1_R$.

---

۹) چنانچه در صفحه مختلط نقطه $a+bi$ با نقطه (a,b) یکی گرفته می‌شود، تابع f دارای یک تعبیر هندسی است: f صفحه را نسبت به محور x–ها منعکس می‌کند.

برهان. (۱) چون f یک همریختی است و $0_R + 0_R = 0_R$ در R، لذا در S

$$f(0_R) + f(0_R) = f(0_R + 0_R) = f(0_R).$$

تفریق $f(0_R)$ از دو طرف عبارت بالا نشان می‌دهد که $f(0_R) = 0_S$.

(۲) $f(a) + f(-a) = f(a + (-a)) = f(0_R) = 0_S$. بنابراین $f(-a)$ یک جواب معادلهٔ $f(a) + x = 0_S$ است؛ امّا طبق قضیه ۲.۳، جواب منحصر به‌فرد این معادله $-f(a)$ است. بنابراین طبق یکتایی جواب، $f(-a) = -f(a)$.

(۳) چون f پوشا است برای برخی $r \in R$، $1_S = f(r)$. بنابراین

$$f(1_R) = 1_S \cdot f(1_R) = f(r)f(1_R) = f(r1_R) = f(r) = 1_S.$$ ■

مثال ۲۴.۳. چنانچه یک یکریختی f از $\mathbb{Z}_{12}$ به حلقه $\mathbb{Z}_3 \times \mathbb{Z}_4$ موجود باشد، در این صورت طبق قسمت (۳) قضیه ۱۰.۳، $f(1) = (1, 1)$. چون f یک همریختی است، در برابری‌های زیر صدق می‌کند:

$$f(2) = f(1 + 1) = f(1) + f(1) = (1, 1) + (1, 1) = (2, 2)$$
$$f(3) = f(2 + 1) = f(2) + f(1) = (2, 2) + (1, 1) = (0, 3)$$
$$f(4) = f(3 + 1) = f(3) + f(1) = (0, 1) + (1, 1) = (1, 0).$$

ادامه فرایند فوق نشان می‌دهد که اگر f یک یکریختی باشد، در این صورت f باید تابع دوسویی زیر باشد:

$f(1) = (1, 1)$	$f(4) = (1, 0)$	$f(7) = (1, 3)$	$f(10) = (1, 2)$
$f(2) = (2, 2)$	$f(5) = (2, 1)$	$f(8) = (2, 0)$	$f(11) = (2, 3)$
$f(3) = (0, 3)$	$f(6) = (0, 2)$	$f(9) = (0, 1)$	$f(12) = (0, 0)$

آنچه که تاکنون نشان داده‌ایم این است که تابع دوسویی f تنها امکان برای یکریختی موردنظر است. برای نشان دادن این که f در واقع یک یکریختی است، باید بررسی کنیم که یک همریختی است. این کار را می‌توان یا به‌وسیله نوشتن جداول انجام داد (که کاری ملال‌آور است)، و یا با مشاهدهٔ این که ضابطه f می‌تواند به صورت:

$$f([a]_{12}) = ([a]_3, [a]_4)$$

توصیف شود، که در آن $[a]_{۱۲}$ کلاس همنهشتی عدد صحیح a در $\mathbb{Z}_{۱۲}$، $[a]_۳$ کلاس a در $\mathbb{Z}_۳$ و $[a]_۴$ کلاس a در $\mathbb{Z}_۴$ را نشان می‌دهد (صحت آخرین گزاره را بررسی کنید). پس

$$\begin{aligned}
f([a]_{۱۲}+[b]_{۱۲}) &= f([a+b]_{۱۲}) && (\text{تعریف جمع در } \mathbb{Z}_{۱۲})\\
&= ([a+b]_۳,[a+b]_۴) && (\text{تعریف } f)\\
&= ([a]_۳+[b]_۳,[a]_۴+[b]_۴) && (\text{تعریف جمع در } \mathbb{Z}_۳ \text{ و } \mathbb{Z}_۴)\\
&= ([a]_۳+[a]_۴)+([b]_۳+[b]_۴) && (\text{تعریف جمع در } \mathbb{Z}_۴ \text{ و } \mathbb{Z}_۳)\\
&= f([a]_{۱۲})+(f[b]_{۱۲}) && (\text{تعریف } f)
\end{aligned}$$

استدلالی مشابه، با بکارگیری ضرب به جای جمع، نشان می‌دهد که $f([a]_{۱۲}[b]_{۱۲}) = f([a]_{۱۲})f([b_{۱۲}])$. بنابراین f یک یکریختی است و $\mathbb{Z}_{۱۲} \cong \mathbb{Z}_۳ \times \mathbb{Z}_۴$.

درک شهودی ما از یکریختی متقارن است: "R یکریخت با S است "به همان معنی است که "S یکریخت با R است". با این حال تعریف رسمی یکریختی متقارن نیست، زیرا تعریف وجود یک تابع از R به روی S را ایجاب می‌کند، امّا مستلزم وجود هیچ تابعی از S به روی R نیست. این عدم تقارن ظاهری به‌سادگی قابل رفع است. اگر $f : R \to S$ یک یکریختی باشد، در این صورت f یک تابع دوسویی از مجموعه‌ها است. بنابراین f دارای یک تابع وارون[۱۰] $g : S \to R$ است به طوری که $g \circ f = \iota_R$ (ι_R تابع همانی روی R است). اثبات این که تابع g در واقع یک یکریختی می‌باشد مشکل نیست (تمرین ۲۴). بنابراین $R \cong S$ نتیجه می‌دهد $S \cong R$ و تقارن به‌دست می‌آید.

تا حال تمرکز ما معطوف به نشان دادن یکریختی بین حلقه‌های گوناگون شده است. اما بعضاً نشان دادن عدم یکریختی دو حلقه نیز به همان اندازه مهم است. بدین منظور باید نشان دهیم هیچ تابعی از یکی به دیگری که بتواند در سه شرط تعریف صدق کند وجود ندارد.

مثال ۲۵.۳. $\mathbb{Z}_۶$ با حلقه‌های $\mathbb{Z}_{۱۲}$ و $\mathbb{Z}$ یکریخت نیست زیرا وجود یک تابع پوشا از یک مجموعه شش عضوی به یک مجموعه بزرگتر (یا یک تابع یک به یک از مجموعه بزرگتر به $\mathbb{Z}_۶$) امکان‌پذیر نیست.

برای نشان دادن این که دو حلقه نامتناهی یا دو حلقه متناهی با تعداد عناصر یکسان یکریخت نیستند بهترین کار معمولاً بررسی غیر مستقیم است.

۱۰) برای جزئیات پیوست ب را ملاحظه کنید.

مثال ۲۶.۳. حلقه‌های $\mathbb{Z}_۴$ و $\mathbb{Z}_۲ \times \mathbb{Z}_۲$ یکریخت نیستند. برای اثبات این، به خلاف فرض کنید که $f : \mathbb{Z}_۴ \to \mathbb{Z}_۲ \times \mathbb{Z}_۲$ یک یکریختی است. در این صورت طبق قضیه ۱۰.۳، $f(۰) = (۰, ۰)$ و $f(۱) = (۱, ۱)$. در نتیجه

$$f(۲) = f(۱ + ۱) = f(۱) + f(۱) = (۱, ۱) + (۱, ۱) = (۰, ۰).$$

چون f یک به یک است و $f(۲) = f(۰)$ به یک تناقض می‌رسیم. بنابراین هیچ یکریختی امکان‌پذیر نیست.

معمول‌ترین روش اثبات این که دو حلقه با اندازه یکسان یکریخت نیستند در نظرگرفتن خواصی است که توسط یکریختی حفظ می‌شود، به این مفهوم که: اگر R واجد چنین خاصیتی باشد و R یکریخت با S باشد در این صورت S نیز لزوماً واجد همان خاصیت است. اگر یکی از حلقه‌ها واجد چنین خاصیتی بوده و دیگری نباشد، در این صورت دو حلقه نمی‌توانند یکریخت باشند.

مثال ۲۷.۳. هیچ حلقه جابجایی با یک حلقه ناجابجایی یکریخت نیست زیرا همانگونه که اکنون بررسی می‌کنیم خاصیت جابجایی توسط یکریختی حفظ می‌شود. فرض کنید R یک حلقه جابجایی و $f : R \to S$ یک یکریختی باشد. اگر $c, d \in S$ در این صورت بنا به پوشا بودن f، عناصر a و b در R وجود دارند به قسمی که $c = f(a)$ و $d = f(b)$. چون $ab = ba$ در R، داریم

$$cd = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = dc.$$

بنابراین S جابجایی است.

مثال ۲۸.۳. فرض کنید $f : R \to S$ یک یکریختی از حلقه‌های یکدار باشد. اگر a در R یکه باشد در این صورت برای برخی $u \in R$، $au = ۱_R = ua$. بنابراین طبق قضیه ۱۰.۳، $f(a)f(u) = f(au) = f(۱_R) = ۱_S$ و به طور مشابه $f(u)f(a) = ۱_S$. بنابراین $f(a)$ در S یکه است. پس خاصیت یکه بودن تحت یکریختی حفظ می‌شود. حلقه $\mathbb{Z}_۸$ دارای چهار یکه است (۱، ۳، ۵، ۷، طبق نتیجه ۹.۲)، لذا هر یکریختی از $\mathbb{Z}_۸$ به هر حلقه دیگر این چهار یکه را به یکه‌های حلقه دیگر می‌نگارد. از این نتیجه می‌شود که $\mathbb{Z}_۸$ یکریخت با $\mathbb{Z}_۲ \times \mathbb{Z}_۴$ نیست زیرا به سادگی می‌توانید بررسی کنید که حلقه $\mathbb{Z}_۲ \times \mathbb{Z}_۴$ تنها دارای دو یکه یعنی $(۱, ۱)$ و $(۳, ۱)$ می‌باشد. به طور مشابه $\mathbb{Z}$ یکریخت با $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ نیست زیرا $\mathbb{Z}$ دارای دقیقاً دو یکه، ۱ و -۱، است در حالی

که هر عضو غیرصفر در میدانهای $\mathbb{Q}$ و $\mathbb{R}$ و $\mathbb{C}$ یک یکه است.

تمرینها

A.۱. جداول جمع و ضرب را برای $\mathbb{Z}_۶$ و برای $\mathbb{Z}_۲ \times \mathbb{Z}_۳$ بنویسید. با استفاده از این جداول نشان دهید $\mathbb{Z}_۶ \cong \mathbb{Z}_۲ \times \mathbb{Z}_۳$.

۲. زیرحلقه $S = \{۰, ۲, ۴, ۶, ۸\}$ از $\mathbb{Z}_{۱۰}$ را در نظر بگیرید و فرض کنید $\mathbb{Z}_۵ = \{۰, ۱, ۲, ۳, ۴\}$. با استفاده از جداول نشان دهید دوسویی زیر از $\mathbb{Z}_۵$ به S یکریختی نیست:

$$۰ \to ۰ \quad ۱ \to ۲ \quad ۲ \to ۴ \quad ۳ \to ۶ \quad ۴ \to ۸.$$

۳. فرض کنید R یک حلقه و R^* زیرحلقه R متشکل از همه عناصری به صورت (a, a) باشد. نشان دهید تابع $f : R \to R^*$ که توسط $f(a) = (a, a)$ تعریف می‌شود یکریختی است.

۴. فرض کنید R و S دو حلقه و $\bar{R}$ زیرحلقهٔ $R \times S$ متشکل از همه عناصری به صورت $(a, ۰_S)$ باشد. نشان دهید تابع $f : R \to \bar{R}$ که توسط $f(a) = (a, ۰_S)$ تعریف می‌شود یک یکریختی است.

۵. ثابت کنید میدان اعداد حقیقی $\mathbb{R}$ یکریخت با حلقه ماتریس‌های ۲×۲ متشکل از همه عناصری به صورت $\begin{pmatrix} ۰ & ۰ \\ ۰ & a \end{pmatrix}$ با $a \in \mathbb{R}$، می‌باشد. [راهنمایی: تابع f که توسط $f(a) = \begin{pmatrix} ۰ & ۰ \\ ۰ & a \end{pmatrix}$ تعریف می‌شود را در نظر بگیرید.]

۶. ثابت کنید $\mathbb{R}$ یکریخت با حلقه ماتریس‌های ۲×۲ متشکل از همه عناصری به صورت $\begin{pmatrix} a & ۰ \\ ۰ & a \end{pmatrix}$ است، که در آن $a \in \mathbb{R}$.

۷. فرض کنید $\mathbb{Q}(\sqrt{۲})$ مجموعه تعریف شده در تمرین ۲۸ از بخش ۱.۳ باشد. ثابت کنید تابع $f : \mathbb{Q}(\sqrt{۲}) \to \mathbb{Q}(\sqrt{۲})$ که توسط $f(a + b\sqrt{۲}) = a - b\sqrt{۲}$ تعریف می‌شود یکریختی است.

۸. اگر $f : \mathbb{Z} \to \mathbb{Z}$ یک یکریختی باشد، ثابت کنید که f تابع همانی است. [راهنمایی: $f(۱)$، $f(۱ + ۱)$، ... چه هستند؟]

۹. نشان دهید تابع $f : \mathbb{Z} \to \mathbb{Z}_n$ که توسط $f(a) = [a]$ تعریف می‌شود یک همریختی پوشا است امّا یک یکریختی نیست.

۱۰. اگر R و S دو حلقه بوده، $f : R \to S$ یک همریختی باشد ثابت کنید که $f(R) = \{f(a) \mid a \in R\}$ یک زیرحلقه S است.

۱۱.B. فرض کنید T، R و F حلقه‌های چهارـ عنصری باشند که جداول آنها در مثال ۵.۳ و تمرینهای ۵ و ۶ بخش ۱.۳ داده شد. نشان دهید هیچ یک از این حلقه‌ها با یکدیگر یکریخت نیستند.

۱۲. فرض کنید $P(S)$ حلقه همه زیرمجموعه‌های $\{a, b, c\}$ باشد (تمرین ۱۱ بخش ۱.۳ را ملاحظه کنید). جداول را بکار برده تا نشان دهید که $P(S)$ با حلقه $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ یکریخت است.

۱۳. نشان دهید که تابع مزدوجی مختلط $f : \mathbb{C} \to \mathbb{C}$ (که ضابطه آن $f(a + bi) = a - bi$ است) یک دوسویی است.

۱۴. نشان دهید یکریختی $\mathbb{Z}_5$ و S در مثال ۲۱.۳ این بخش توسط تابعی به‌دست می‌آید که ضابطه آن $f([x]_5) = [6x]_{10}$ است، جایی که $[u]_n$ کلاس عدد صحیح $u \in \mathbb{Z}_n$ را نشان می‌دهد. اثبات مستقیمی ارائه دهید (بدون استفاده از جداول) که این نگاشت یک همریختی است.

۱۵. نشان دهید $S = \{0, 4, 8, 12, 16, 20, 24\}$ یک زیرحلقه $\mathbb{Z}_{28}$ است. سپس ثابت کنید که نگاشت $f : \mathbb{Z}_7 \to S$ که توسط $f([x]_7) = [8x]_{28}$ تعریف می‌شود یک یکریختی است (نمادگذاری همانند تمرین ۱۴ می‌باشد).

۱۶. فرض کنید E حلقه اعداد صحیح زوج باشد با عمل ضربی که در تمرین ۱۷ بخش ۱.۳ تعریف شد. نشان دهید که نگاشت $f : E \to \mathbb{Z}$ که توسط $f(x) = x/2$ تعریف می‌شود یک یکریختی است.

۱۷. فرض کنید $\mathbb{Z}^*$ حلقه اعداد صحیح با اعمال $\oplus$ و $\odot$ تعریف شده در مثال ۱۸ بخش ۱.۳ باشد. ثابت کنید $\mathbb{Z}$ با $\mathbb{Z}^*$ یکریخت است.

۱۸. فرض کنید $\bar{\mathbb{Z}}$ حلقه اعداد صحیح با اعمال $\oplus$ و $\odot$ تعریف شده در مثال ۱۹ بخش ۱.۳

باشد. ثابت کنید $\bar{\mathbb{Z}}$ با $\mathbb{Z}$ یکریخت است.

۱۹. فرض کنید $\mathbb{R} \times \mathbb{R}$ میدان تمرین ۳۷ بخش ۱.۳ باشد. نشان دهید $\mathbb{R} \times \mathbb{R}$ با میدان اعداد مختلط $\mathbb{C}$ یکریخت است.

۲۰. (الف) نشان دهید $\mathbb{R} \times \mathbb{R}$ با جمع مؤلفه به مؤلفه معمولی (همانند قضیه ۱.۳) و ضرب تعریف شده توسط ضابطه $(a,b)(c,d) = (ac, bc)$ یک حلقه است.

(ب) نشان دهید حلقه قسمت (الف) با حلقه همه ماتریس‌های در $M(\mathbb{R})$ به صورت $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ یکریخت است.

۲۱. فرض کنید L حلقه همه ماتریس‌های در $M(\mathbb{Z})$ به صورت $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$ باشد. نشان دهید که تابع $f : L \to \mathbb{Z}$ که توسط $f \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = a$ تعریف می‌شود یک همریختی پوشا است امّا یک یکریختی نیست.

۲۲. نشان دهید تابع $f : \mathbb{Z}_m \to \mathbb{Z}_{mn}$ که توسط $f([x]_m) = [nx]_{mn}$ تعریف می‌شود یک همریختی پوشا است امّا وقتی $n \geq 2$ باشد یک یکریختی نیست (نمادها همانند نمادهای تمرین ۱.۴ است).

۲۳. (الف) اگر f و g دو یکریختی باشند نشان دهید gof نیز یک یکریختی است.

۲۴. فرض کنید $f : R \to S$ یک همریختی حلقه‌ای بوده، فرض کنید $g : S \to R$ تابع وارون آن (همچنان‌که در پیوست (ب) تعریف شده است) باشد. نشان دهید g نیز یک یکریختی است. [راهنمایی: برای نشان دادن $g(a+b) = g(a) + g(b)$، تصاویر طرف چپ و راست را تحت f در نظر گرفته و از این که f یک همریختی است و fog تابع همانی است استفاده کنید.]

۲۵. (الف) فرض کنید R یک حلقه یکدار و $f : R \to S$ یک همریختی پوشای حلقه‌ای باشد. ثابت کنید که S یکدار است و $f(1_R) = 1_S$.

(ب) با ارائه یک مثال نشان دهید که اگر f پوشا نباشد نتیجه‌گیری قسمت (الف) ممکن است غلط باشد.

۲۶. اگر $f : R \to S$ یک یکریختی حلقه‌ای باشد، کدامیک از خواص زیر تحت این یکریختی حفظ می‌شود؟ چرا؟

(الف) $a \in R$ یک مقسوم‌علیه صفر است.

(ب) R یک دامنه صحیح است.

(پ) R یک زیرحلقه $\mathbb{Z}$ است.

(ت) $a \in R$ یک جواب $x = x^2$ است.

(ث) R حلقه ماتریسها است.

۲۷. از خواصی که تحت یکریختی حفظ می‌شوند استفاده کنید تا نشان دهید که در هر یک از موارد زیر دو حلقه داده شده یکریخت نیستند:

(الف) E و $\mathbb{Z}$ (ب) $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ و $M(\mathbb{R})$

(پ) $\mathbb{Z}_{۱۲} \times \mathbb{Z}_۴$ و $\mathbb{Z}_{۱۶}$ (ت) $\mathbb{Q}$ و $\mathbb{R}$

(ث) $\mathbb{Z} \times \mathbb{Z}_۲$ و $\mathbb{Z}$ (ج) $\mathbb{Z}_۴ \times \mathbb{Z}_۴$ و $\mathbb{Z}_{۱۶}$

۲۸. اگر $f : R \to S$ یک همریختی از حلقه‌های یکدار باشد، آیا این درست است که R و S دارای مشخصه‌های یکسان هستند؟ [تمرین ۲۸ بخش ۲.۳ را ملاحظه کنید.]

۲۹. فرض کنید T حلقه توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$ باشد. اگر $f \in T$ و $f = f^2$، نشان دهید که f یا تابع ثابت $f(x) = ۰$ است و یا تابع ثابت $f(x) = ۱$. [راهنمایی: برای هر $a \in \mathbb{R}$، $f(a)$ بایستی یک جواب $x = x^2$ بوده و f پیوسته است.]

۳۰. ثابت کنید حلقه T در تمرین ۲۹ یکریخت با $\mathbb{R} \times \mathbb{R}$ نیست. [راهنمایی: چهارجواب $x = x^2$ در $\mathbb{R} \times \mathbb{R}$ را بیابید؛ از تمرینهای ۲۶ (ت) و ۲۹ استفاده کنید.]

۳۱. آیا حلقه T در تمرین ۲۹ با $P(\mathbb{R})$ یعنی حلقه همه زیرمجموعه‌های $\mathbb{R}$ یکریخت است؟ (تمرین ۳۶ بخش ۱.۳ را ملاحظه کنید.)

۳۲. فرض کنید R یک حلقه بدون عضو همانی باشد. فرض کنید T حلقه یکدار تمرین ۳۱ بخش ۲.۳ باشد. نشان دهید R یکریخت با زیرحلقه R^* از T است. بنابراین اگر R با R^* یکی گرفته شود، در این صورت R زیرحلقه یک حلقه یکدار است.

۳۳. برای هر عدد صحیح مثبت k، فرض کنید $k\mathbb{Z}$ حلقه همه ضرایب صحیح k را نشان دهد (تمرین ۲ بخش ۱.۳) را ملاحظه کنید. ثابت کنید اگر $m \neq n$ در این صورت $m\mathbb{Z}$ یکریخت با $n\mathbb{Z}$ نیست.

۳۴. فرض کنید $m, n \in \mathbb{Z}$ با $(m, n) = ۱$ و $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ توسط $f([a]_{mn}) = ([a_m], [a_n])$ تعریف شود (نمادها همانند نمادهای مثال بعد از قضیه ۱۰.۳ است ـ حالت $m = ۳$، $n = ۴$).

(الف) نشان دهید نگاشت f خوش‌تعریف است، یعنی نشان دهید اگر $[a]_{mn} = [b]_{mn}$ در $\mathbb{Z}_{mn}$ آنگاه $[a]_m = [b]_m$ در $\mathbb{Z}_m$ و $[a]_n = [b]_n$ در $\mathbb{Z}_n$.

(ب) ثابت کنید f یک یکریختی است. [راهنمایی: اثبات مثال بعد از قضیه ۱۰.۳ را به وضعیت جدید تطبیق‌دهید. تفاوت در این است که در اینجا اثبات دوسویی بودن f کار بیشتری می‌برد.]

۳۵. اگر $(m, n) \neq ۱$، ثابت کنید $\mathbb{Z}_{mn}$ یکریخت با $\mathbb{Z}_m \times \mathbb{Z}_n$ نیست.

* * * * *

فصل چهارم

حساب در $\mathbb{F}[x]$

در فصل اول، حساب دبیرستانی را از دیدگاهی پیشرفته‌تر بررسی نمودیم و تعدادی از خواص مهم حلقه اعداد صحیح $\mathbb{Z}$ را بسط و توسعه دادیم. در این فصل روندی مشابه را دنبال می‌کنیم با این تفاوت که کار خود را بجای حساب، از جبر دبیرستانی و به طور مشخص از چندجمله‌ایها و حساب چندجمله‌ایها آغاز می‌نمائیم. چندجمله‌ایهایی که در دبیرستان مطالعه می‌شود معمولاً دارای ضرایب حقیقی، یعنی از میدان حقیقی $\mathbb{R}$، است. اکنون که با حلقه و میدان آشنا شده‌اید این محدودیت غیرضروری است. لذا چندجمله‌ایها را با ضرایب از حلقه‌های دلخواه در نظر خواهیم گرفت. با این حال توجه عمده ما روی حلقه چندجمله‌ایهای $\mathbb{F}[x]$، با ضرایب متعلق به میدان $\mathbb{F}$ می‌باشد.

خواهیم دید که ساختار حلقه چندجمله‌ایهای $\mathbb{F}[x]$ به‌طور قابل ملاحظه‌ای شبیه به ساختار حلقه اعداد صحیح $\mathbb{Z}$ است؛ در هر دو مفاهیم الگوریتم تقسیم، بزرگترین مقسوم‌علیه مشترک، اعداد اول و یکتایی تجزیه وجود دارد. در موارد زیادی برهان‌های ارائه شده در فصل اول برای حلقه $\mathbb{Z}$، تقریباً بدون هیچ تغییری قابل انتقال به حلقه $\mathbb{F}[x]$ است. لذا موضوع اصلی بخش‌های ۴ـ۱ تا ۴ـ۳،

انتقال نتایج مشابه از $\mathbb{Z}$ به $\mathbb{F}[x]$ است.

در بخش‌های ۴ـ۴ تا ۴ـ۶ آزمونهایی را در نظر می‌گیریم که تحویل‌ناپذیری یک چندجمله‌ای را تعیین می‌کنند (مانند آزمون اول بودن یک عدد صحیح). به‌دلیل وجود مفاهیمی چون تابع چندجمله‌ای و ریشه یک چندجمله‌ای که مشابهی در حلقه اعداد صحیح ندارد، روند کار در اینجا شباهت چندانی با آنچه که در حلقه $\mathbb{Z}$ انجام شد، ندارد. وجود این مفاهیم نتایج چشمگیری به دست می‌دهد که در فصل‌های بعدی خواهیم دید.

۴-۱ حساب چندجمله‌ایها و الگوریتم تقسیم

قسمت زیادی از جبر دبیرستانی به حساب چندجمله‌ایهای با ضرایب حقیقی مانند

$$x^{۱۲} - ۱ \qquad ۶x^۳ - ۳x^۲ + ۷x + ۴ \qquad x^۲ + ۳x - ۵$$

اختصاص دارد که شما با آن آشنا هستید. اکنون چندجمله‌ایها را در قالب عام‌تری در نظر می‌گیریم.

فرض کنید R یک حلقه باشد. یک چندجمله‌ای با ضرایب در R، عبارتی است به صورت

$$a_۰ + a_۱x + a_۲x^۲ + a_۳x^۳ + \cdots + a_nx^n$$

که در آن $a_i \in R$. a_i ها **ضرایب** این چندجمله‌ای و x یک **مجهول** (یا **عنصر متعالی** روی R) نامیده می‌شوند.

اکنون این سؤال پیش می‌آید که "یک مجهول چیست؟" و "ضرب یک مجهول در یک عضو حلقه و یا جمع کردن چنین جملاتی با یکدیگر به چه معنی است؟". جواب متداولی که در کلاس‌های جبر مقدماتی داده می‌شود این است که "با مجهول x به عنوان عضوی از حلقه R رفتار کنید". در این صورت عبارت $a_۰ + a_۱x + a_۲x^۲ + \cdots + a_nx^n$ مفهوم پیدا می‌کند. امّا گاهی چنین پاسخی کافی نیست.

حتی در دبیرستان نیز با چندجمله‌ایها اغلب به عنوان عباراتی مجرد رفتار می‌شود، بدون این که به x به عنوان عددی مشخص ارجاع داده شود. بعلاوه اعداد حقیقی نیز به عنوان چندجمله‌ای (چندجمله‌ایهای ثابت) در نظر گرفته می‌شود. دیدگاه ما در این کتاب نیز چنین خواهد بود.

به ازای یک حلقه R، ثابت می‌شود که حلقه بزرگتری (که با $R[x]$ نشان داده می‌شود) وجود

دارد که R را به عنوان یک زیرحلقه شامل است و عنصری بخصوص مانند x دارد که خواص زیر را داراست:

(i) $xa = ax$ برای هر $a \in R$.

(ii) هر عنصر $R[x]$ را می‌توان به صورت

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad \text{با} \quad n \geq 0 \quad \text{و} \quad a_i \in R$$

نوشت.

(iii) نمایش عناصر $R[x]$ در (ii) به مفهوم زیر منحصر به فرد است: اگر $n \leq m$ و

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$$

در این صورت $a_i = b_i$ برای $i \leq n$ و $b_i = 0_R$ برای $i > n$.

عناصر حلقه بزرگتر $R[x]$ را **چندجمله‌ای** [۱] و عنصر خاص x را یک **مجهول** می‌نامیم [۲].

چون حاصلضرب هر عضو حلقه با عضو 0_R همان 0_R است لذا در یک چندجمله‌ای، جملات دارای ضریب صفر را می‌توان در صورت لزوم حذف یا اضافه کرد.

مثال ۱.۴. در $R[x]$ چندجمله‌ای $2 + 0x - x^2 + 0x^3 + 5x^4$ معمولاً به صورت $2 - x^2 + 5x^4$ نوشته می‌شود.

چنانچه مایل باشیم همه توانهای x در چندجمله‌ایهای $x^2 + 1$ و $4 + x + 2x^3$ ظاهر شوند می‌نویسیم:

$$4 + x + 0x^2 + 2x^3. \quad , \quad 1 + 0x + x^2 + 0x^3$$

۱) بعضی از مدرسین منجمله مؤلف بر این باورند که همه باید یک بحث رسمی از چندجمله‌ایها و اثبات‌هایی از گزاره‌های بالا را ببینند. موافقین این دیدگاه بایستی ابتدا پیوست پ را تدریس کرده و سپس این بخش را آغاز کنند. کسانی که این دیدگاه را ندارند می‌توانند مطالعه این بخش را ادامه دهند.

۲) اگرچه در استفاده مصطلح، واژه "مجهول" به معنای چیزی ناشناخته است امّا همانگونه که در پیوست چ نشان داده شده است، هیچ چیز مجهول یا مبهم در مورد x وجود ندارد. به ویژه x عضوی از R نیست و بجای هیچ عضوی از R نیز قرار نمی‌گیرد؛ x عضو بخصوصی از یک حلقه بزرگتر که R را شامل است می‌باشد.

در عین حال، نماد "x" بعضاً به طریق دیگری نیز استفاده می‌شود ـ به عنوان یک متغیر در معادله‌ای مانند $x^2 - 3x = 0$. در چنین وضعیتی x ممکن است عضوی از R را نمایش دهد. چنین کاربردی در بخش ۴ـ۴ بحث شده‌است؛ تا آن زمان "x" همواره یک مجهول (عضوی از $R[x]$ با خواص (i)ـ (iii)) را نمایش می‌دهد.

قوانین جمع و ضرب چندجمله‌ایها مستقیماً از این حقیقت که $R[x]$ یک حلقه است پیروی می‌کند.

مثال ۲.۴. اگر $f(x) = ۱ + ۵x - x^۲ + ۴x^۳ + ۲x^۴$ و $g(x) = ۴ + ۲x + ۳x^۲ + x^۳$ در $\mathbb{Z}_۷[x]$ باشند، در این صورت قوانین جابجایی، شرکت‌پذیری و توزیع‌پذیری نشان می‌دهد که

$$\begin{aligned} f(x) + g(x) &= (۱ + ۵x - x^۲ + ۴x^۳ + ۲x^۴) + (۴ + ۲x + ۳x^۲ + x^۳ + ۰x^۴) \\ &= (۱ + ۴) + (۵ + ۲)x + (-۱ + ۳)x^۲ + (۴ + ۱)x^۳ + (۲ + ۰)x^۴ \\ &= ۵ + ۰x + ۲x^۲ + ۵x^۳ + ۲x^۴ = ۵ + ۲x^۲ + ۵x^۳ + ۲x^۴. \end{aligned}$$

مثال ۳.۴. حاصل‌ضرب $x^۲ + ۷x - ۱$ و $۳x + ۲$ در $\mathbb{Q}[x]$ با استفاده مکرر از قانون توزیع‌پذیری به‌دست می‌آید:

$$\begin{aligned} (۱ - ۷x + x^۲)(۲ + ۳x) &= ۱(۲ + ۳x) - ۷x(۲ + ۳x) + x^۲(۲ + ۳x) \\ &= ۱(۲) + ۱(۳x) - ۷x(۲) - ۷x(۳x) + x^۲(۲) + x^۲(۳x) \\ &= ۲ + ۳x - ۱۴x - ۲۱x^۲ + ۲x^۲ + ۳x^۳ \\ &= ۲ - ۱۱x - ۱۹x^۲ + ۳x^۳ \end{aligned}$$

مثال‌های قبلی نمونه‌ای است از آنچه که در حالت کلی رخ می‌دهد. جمع چندجمله‌ایها با جمع ضرایب نظیر انجام می‌شود و ضرب آنها با استفاده از قانون توزیع‌پذیری و دسته‌بندی توانهای برابر x انجام می‌گردد. بنابراین جمع چندجمله‌ایها توسط قانون:

$$\begin{aligned} &(a_۰ + a_۱x + a_۲x^۲ + \cdots + a_nx^n) + (b_۰ + b_۱x + b_۲x^۲ + \cdots + b_nx^n) \\ &\quad = (a_۰ + b_۰) + (a_۱ + b_۱)x + (a_۲ + b_۲)x^۲ + \cdots + (a_n + b_n)x^n \end{aligned}$$

انجام می‌شود و ضرب چندجمله‌ایها توسط قانون:

$$\begin{aligned} &(a_۰ + a_۱x + a_۲x^۲ + \cdots + a_nx^n)(b_۰ + b_۱x + b_۲x^۲ + \cdots + b_mx^m) \\ &= a_۰b_۰ + (a_۰b_۱ + a_۱b_۰)x + (a_۰b_۲ + a_۱b_۱ + a_۲b_۰)x^۲ + \cdots + a_nb_mx^{n+m}. \end{aligned}$$

صورت می‌گیرد. برای هر $k \geq ۰$، ضریب x^k در حاصل‌ضرب فوق عبارت است از

$$a_۰b_k + a_۱b_{k-۱} + a_۲b_{k-۲} + \cdots + a_{k-۲}b_۲ + a_{k-۱}b_۱ + a_kb_۰ = \sum_{i=۰}^{k} a_ib_{k-i}$$

جایی که $a_i = 0_R$ اگر $i > n$ و $b_j = 0_R$ اگر $j > m$.

از تعریف ضرب در $R[x]$ به سادگی نتیجه می‌شود که اگر R جابجایی باشد در این صورت $R[x]$ نیز چنین است (تمرین ۳). بعلاوه اگر R دارای عضو همانی ضربی 1_R باشد در این‌صورت 1_R عضو همانی ضربی $R[x]$ نیز هست (تمرین ۴).

تعریف. فرض کنید $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ یک چندجمله‌ای در $R[x]$ باشد با $a_n \neq 0_R$. a_n **ضریب پیشرو** $f(x)$ نامیده می‌شود. **درجه** $f(x)$ عبارت است از عدد صحیح n که با "$\deg f(x)$" نمایش داده می‌شود. به عبارت دیگر $\deg f(x)$ بزرگترین نمایی از x است که با ضریب غیرصفر ظاهر می‌شود و این ضریب، ضریب پیشرو است.

مثال ۴.۴. در $\mathbb{R}[x]$ درجه $7x^3 - 4x^2 - x + 3$ برابر ۳ و ضریب پیشرو -7 است. به طور مشابه $\deg(3 + 5x) = 1$ و $\deg(x^{12}) = 12$. درجه $0x^5 + 0x^3 + 4x^2 + x + 2$ برابر ۲ (بزرگترین نمای x با یک ضریب غیرصفر) و ضریب پیشروی آن ۴ است.

حلقه R که ابتدا بحث خود را از آن شروع کردیم یک زیرحلقه از حلقه چندجمله‌ایهای $R[x]$ است. به عنوان چندجمله‌ایهایی در $R[x]$ عناصر R، **چندجمله‌ایهای ثابت** نامیده می‌شوند. چندجمله‌ایهای از درجه صفر در $R[x]$ دقیقاً چندجمله‌ایهای ثابت غیرصفر می‌باشند. توجه کنید که

چندجمله‌ای ثابت 0_R دارای هیچ درجه‌ای نیست،

(به‌دلیل این که هیچ توانی از x با ضریب غیرصفر ظاهر نمی‌شود).

قضیه ۱.۴. اگر R یک دامنه صحیح و $f(x)$ و $g(x)$ چندجمله‌ایهای غیرصفر در $R[x]$ باشند در این صورت

$$\deg[f(x)g(x)] = \deg f(x) + \deg g(x).$$

برهان. فرض کنید $f(x) = a_0 + a_1x + \cdots + a_nx^n$ و $g(x) = b_0 + b_1x + \cdots + b_mx^m$ با $a_n \neq 0_R$ و $b_m \neq 0_R$. بنابراین $\deg f(x) = n$ و $\deg g(x) = m$. پس

$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots + a_nb_mx^{n+m}$$

بزرگترین نمای x که احتمالاً می‌تواند ضریب غیرصفر داشته باشد $n+m$ است. امّا $a_nb_m \neq 0$، زیرا R یک دامنه صحیح است و $a_n \neq 0_R$ و $b_m \neq 0_R$. بنابراین $f(x)g(x)$ غیرصفر است و $\deg[f(x)g(x)] = n+m = \deg f(x) + \deg g(x)$.

نتیجه ۲.۴. اگر R یک دامنه صحیح باشد، $R[x]$ نیز چنین است.

برهان. چون R یک حلقه جابجایی یکدار است لذا $R[x]$ نیز چنین است (تمرین ۳ و ۴). اثبات قضیه ۱.۴ نشان می‌دهد که حاصل‌ضرب چندجمله‌ایهای غیرصفر در $R[x]$ غیرصفر است. بنابراین $R[x]$ یک دامنه صحیح است. ■

مشاهده کنید که قسمت اول اثبات قضیه ۱.۴ برای هر حلقه دلخواه معتبر بوده و نشان می‌دهد که

اگر $f(x)$، $g(x)$ و $f(x)g(x)$ غیر صفر باشند در این صورت
$$\deg[f(x)g(x)] \leq \deg f(x) + \deg g(x).$$

اگر حلقه R دارای مقسوم‌علیه صفر باشد نابرابری اکید نیز می‌تواند اتفاق بیافتد. برای مثال در $\mathbb{Z}_8[x]$، $2x^2$ دارای درجه ۴ و $3x^2+1$ دارای درجه ۲ است امّا حاصل‌ضرب آنها دارای درجه $6 = 2+4$ نیست:

$$2x^2(1+3x^2) = 2x^2 + 2\times 3x^6 = 2x^2 + 0\cdot x^6 = 2x^2.$$

برای آگاهی از درجه مجموع چندجمله‌ایها تمرین‌های ۸ و ۱۰ را ملاحظه کنید.

در قسمت باقیمانده این فصل توجه خود را عمدتاً به چندجمله‌ای‌هایی معطوف می‌کنیم که ضرایب آنها متعلق به یک میدان $\mathbb{F}$ (مثل $\mathbb{Q}$، $\mathbb{R}$ یا $\mathbb{Z}_5$) است. همانگونه که در مقدمه این فصل ذکر شد دامنه صحیح $\mathbb{F}[x]$ بسیاری از همان خواصی را داراست که دامنه صحیح اعداد صحیح $\mathbb{Z}$ دارا می‌باشد، از جمله قضیه زیر را داریم.

قضیه ۳.۴. (الگوریتم تقسیم در $\mathbb{F}[x]$) فرض کنید $\mathbb{F}$ یک میدان باشد و $f(x), g(x) \in \mathbb{F}[x]$ با $g(x) \neq 0_{\mathbb{F}}$. در این صورت چندجمله‌ایهای $q(x)$ و $r(x)$ وجود دارند به قسمی که

$$f(x) = g(x)q(x) + r(x)$$

که در آن $r(x) = 0_{\mathbb{F}}$ و یا $\deg r(x) < \deg g(x)$.

این گزاره را با الگوریتم تقسیم در $\mathbb{Z}$ (قضیه ۱.۱) مقایسه کنید که بیان می‌کند برای هر عدد صحیح a و هر عدد صحیح مثبت b، اعداد صحیح یکتای q و r وجود دارند به قسمی که

$$a = bq + r \qquad \text{و} \qquad 0 \leq r < b.$$

تنها تفاوت در این است که گزاره‌هایی مثل "$r < b$" در $\mathbb{Z}$ را با گزاره‌هایی در $\mathbb{F}[x]$ که دربردارندهٔ مفهوم درجه‌اند جایگزین کرده‌ایم. احتمالاً شما نیز از الگوریتم تقسیم برای امتحان درستی تقسیم‌هایی نظیر مثال زیر استفاده می‌کنید، یعنی بررسی می‌کنید که $f(x) = g(x)q(x) + r(x)$؛

$$\begin{array}{rl|l}
 & 3x^5 + 2x^4 + 2x^3 + 4x^2 + x - 2 & 2x^3 + 1 \\
\hline
 & 3x^5 + \qquad\quad \tfrac{3}{2}x^2 & \tfrac{3}{2}x^2 + x + 1 \\
\hline
 & 2x^4 + 2x^3 + \tfrac{5}{2}x^2 + x - 2 & \\
 & 2x^4 \qquad\quad + x & \\
\hline
 & 2x^3 + \tfrac{5}{2}x^2 - 2 & \\
 & 2x^3 \qquad\quad + 1 & \\
\hline
 & \tfrac{5}{2}x^2 - 3 &
\end{array}$$

مقسوم $f(x)$ — مقسوم‌علیه $g(x)$ —
$(\frac{3}{2}x^2)g(x)$ — خارج قسمت $q(x)$
$f(x) - (\frac{3}{2}x^2)g(x)$ —
— باقیمانده $r(x)$

با بررسی فرآیند تقسیم فوق می‌توانیم سرنخی برای اثبات قضیه ۳.۴ به‌دست آوریم. اولین جمله خارج قسمت یعنی $\frac{3}{2}x^2$ از تقسیم جمله پیشرو مقسوم یعنی $3x^5$ بر جمله پیشرو مقسوم‌علیه یعنی $2x^3$ به‌دست آمده‌است: $3x^5/2x^3 = \frac{3}{2}x^2$. سپس حاصل‌ضرب این جمله و مقسوم‌علیه، $(\frac{3}{2}x^2)g(x)$، از مقسوم کم می‌شود. مجدداً این فرایند با مقسوم‌علیه و عبارت $2x^4 + 2x^3 + \frac{5}{2}x^2 + x - 2$ به عنوان مقسوم جدید تکرار می‌شود (توجه کنید که درجه این، یکی کمتر از مقسوم اصلی است) تا دوّمین جمله خارج قسمت یعنی $2x^4/2x^3 = x$ بدست آید، و این فرآیند را به همین ترتیب ادامه می‌دهیم. این روند اثباتی استقرایی را پیشنهاد می‌نماید.

برهان قضیه ۳.۴. ابتدا وجود چندجمله‌ایهای $q(x)$ و $r(x)$ را اثبات می‌کنیم.

حالت ۱: اگر $f(x) = 0_{\mathbb{F}}$ یا اگر $\deg f(x) < \deg g(x)$، در این صورت با قراردادن $q(x) = 0_{\mathbb{F}}$ و $r(x) = f(x)$ قضیه درست است زیرا $f(x) = g(x)0_{\mathbb{F}} + f(x)$.

حالت ۲: اگر $f(x) \neq 0_{\mathbb{F}}$ و $\deg g(x) \leq \deg f(x)$ در این صورت اثبات وجود $q(x)$ و $r(x)$

با استقراء روی درجه مقسوم $f(x)$ انجام می‌شود[۳]. اگر $\deg f(x) = 0$ در این صورت $g(x) = b$ و $f(x) = a$، داریم $a, b \in \mathbb{F}$ بنابراین برای برخی $\deg g(x) = 0$.

چون $\mathbb{F}$ یک میدان است لذا b یکه است و $a = b(b^{-1}a) + 0_{\mathbb{F}}$. بنابراین قضیه با قراردادن $q(x) = b^{-1}$ و $r(x) = 0_{\mathbb{F}}$ درست است.

حال به استقراء فرض کنید که قضیه برای حالتی که درجه مقسوم کمتر از n باشد درست است. باید نشان دهیم که قضیه برای حالتی که $f(x)$ دارای درجه n است درست می‌باشد. فرض کنید $f(x) = a_n x^n + \cdots + a_1 x + a_0$ با $a_n \neq 0_{\mathbb{F}}$. مقسوم‌علیه $g(x)$ بایستی به صورت $g(x) = b_m x^m + \cdots + b_1 x + b_0$ با $b_m \neq 0_{\mathbb{F}}$ و $m \leq n$ باشد. اکنون $f(x)$ را بر $g(x)$ همانند مثال قبل از این قضیه (که در آن $a_n x^n = 3x^5$، $b_m x^m = 2x^3$ و اولین جمله خارج قسمت برابر $3 \times 2^{-1} x^{5-3} = \frac{3}{2} x^2 = \frac{3x^5}{2x^3}$ است) تقسیم می‌کنیم. چون $\mathbb{F}$ یک میدان است و $b_m \neq 0_{\mathbb{F}}$ لذا b_m یکه است. $g(x)$ را در $a_n b_m^{-1} x^{n-m}$ ضرب می‌کنیم:

$$\begin{aligned} a_n b_m^{-1} x^{n-m} g(x) &= a_n b_m^{-1} x^{n-m} (b_m x^m + \cdots + b_0) \\ &= a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \cdots + a_n b_m^{-1} b_0 x^{n-m} \end{aligned}$$

همانند مثال قبلی (که در آن $a_n b_m^{-1} x^{n-m} g(x) = 3x^5 + \frac{3}{2} x^2$)، چندجمله‌ای $a_n b_m^{-1} x^{n-m} g(x)$ دارای درجه n و ضریب پیشرو a_n است که همان درجه و ضریب پیشرو $f(x)$ می‌باشد. بنابراین تفاضل $f(x) - a_n b_m^{-1} x^{n-m} g(x)$ یک چندجمله‌ای از درجه کمتر از n (یا احتمالاً چندجمله‌ای صفر) است: در مثال بالا، این تفاضل برابر $2x^4 + 2x^3 + \frac{5}{2} x^2 + x - 2$ می‌باشد. حال فرض استقراء را برای $g(x)$ به عنوان مقسوم‌علیه و چندجمله‌ای $f(x) = a_n b_m^{-1} x^{n-m}$ را به عنوان مقسوم بکار برید (یا اگر مقسوم صفر است از حالت ۱ استفاده کنید). چندجمله‌ایهای $q_1(x)$ و $r(x)$ چنان موجودند که

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = g(x) q_1(x) + r(x) \quad \text{و}$$

$$r(x) = 0_{\mathbb{F}} \quad \text{یا} \quad \deg r(x) < \deg g(x).$$

---

۳) اصل استقراء کامل را بکار می‌بریم: پیوست پ را ملاحظه کنید.

بنابراین

$$f(x) = g(x)[a_n b_m^{-1} x^{n-m} + q_1(x)] + r(x) \quad \text{و}$$
$$r(x) = 0_{\mathbb{F}} \quad \text{یا} \quad \deg r(x) < \deg g(x).$$

بنابراین در حالت $\deg f(x) = n$ نیز قضیه درست است با $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$.
این کار استقراء را کامل نموده و نشان می‌دهد که $q(x)$ و $r(x)$ همواره برای هر مقسوم‌علیه و مقسوم موجوداست.

برای اثبات یکتایی $q(x)$ و $r(x)$ فرض کنید $q_1(x)$ و $r_1(x)$ چندجمله‌ایهایی باشند با

$$f(x) = g(x)q_1(x) + r_1(x) \quad \text{و} \quad r_1(x) = 0_{\mathbb{F}} \quad \text{یا} \quad \deg r_1(x) < \deg g(x).$$

پس

$$g(x)q(x) + r(x) = f(x) = g(x)q_1(x) + r_1(x)$$

و لذا

$$g(x)[q(x) - q_1(x)] = r_1(x) - r(x).$$

اگر $q(x) - q_1(x)$ غیرصفر باشد در این صورت طبق قضیه ۱.۴ درجه طرف چپ برابر $\deg g(x) + deg[q(x) - q_1(x)]$ بوده که یکی بیشتر یا برابر درجه $g(x)$ است. امّا هر دو $r_1(x)$ و $r(x)$ دارای درجه‌های اکیداً کوچکتر از $\deg g(x)$ می‌باشند و بنابراین طرف راست برابری بایستی دارای درجه اکیداً کوچکتر از درجه $g(x)$ باشد (تمرین ۱۰). این یک تناقض است. بنابراین $q(x) - q_1(x) = 0_{\mathbb{F}}$ یا به‌طور معادل $q(x) = q_1(x)$. چون طرف چپ صفر است لذا باید داشته باشیم $r_1(x) - r(x) = 0_{\mathbb{F}}$ و لذا $r_1(x) = r(x)$. بنابراین چندجمله‌ایهای $q(x)$ و $r(x)$ یکتا هستند. ■

تمرینها

توجه: R یک حلقه و $\mathbb{F}$ یک میدان را نشان می‌دهد.

۱.A. اعمال خواسته شده را انجام دهید و جواب خود را ساده کنید:

(الف) $(3x^4 + 2x^3 - 4x^2 + x + 4) + (4x^3 + x^2 + 4x + 3)$ در $\mathbb{Z}_5[x]$

(ب) $(x+1)^3$ در $\mathbb{Z}_3[x]$

(پ) $(x-1)^5$ در $\mathbb{Z}_5[x]$

(ت) $(x^2-3x+2)(2x^3-4x+1)$ در $\mathbb{Z}_7[x]$

۲. کدام یک از زیرمجموعه‌های $R[x]$ که در زیر آمده است یک زیرحلقه $R[x]$ است؟ جواب خود را توجیه کنید:

(الف) همه چندجمله‌ایهای با جمله ثابت 0_R.

(ب) همه چندجمله‌ایهای از درجه ۲.

(پ) همه چندجمله‌ایهای از درجه $\geq k$، جایی که k یک عدد صحیح مثبت ثابت است.

(ت) همه چندجمله‌ایهایی که در آنها توانهای فرد x دارای ضریب صفر هستند.

(ث) همه چندجمله‌ایهایی که در آنها توانهای زوج x دارای ضریب صفر هستند.

۳. اگر R جابجایی باشد، نشان دهید $R[x]$ نیز جابجایی است.

۴. اگر R دارای همانی ضربی 1_R باشد، نشان دهید 1_R همانی ضربی $R[x]$ نیز هست.

۵. (الف) همه چندجمله‌ایهای با درجه ۳ در $\mathbb{Z}_2[x]$ را فهرست کنید.

(ب) همه چندجمله‌ایهای با درجه کوچکتر از ۳ در $\mathbb{Z}_2[x]$ را فهرست کنید.

۶. (الف) چه تعداد از چندجمله‌ایهای در $\mathbb{Z}_5[x]$ دارای درجه ۵ و ضریب پیشرو ۱ هستند؟

(ب) چه تعداد از چندجمله‌ایهای در $\mathbb{Z}_n[x]$ دارای درجه k هستند، جایی که k یک عدد صحیح مثبت است؟

۷. چندجمله‌ایهای $q(x)$ و $r(x)$ را چنان بیابید که $f(x)=g(x)q(x)+r(x)$ و $r(x)=0$ و یا $\deg r(x) < \deg g(x)$:

(الف) $f(x)=3x^4-2x^3+6x^2-x+2$ و $g(x)=x^2+x+1$ در $\mathbb{Q}[x]$.

(ب) $f(x)=x^4-7x+1$ و $g(x)=2x-1$ در $\mathbb{Z}_5[x]$.

(پ) $f(x)=2x^4+x^2-x+1$ و $g(x)=2x-1$ در $\mathbb{Z}_5[x]$.

(ت) $f(x)=3x^4+2x^3+6x^2+4x^5$ و $g(x)=3x^2+2$ در $\mathbb{Z}_7[x]$.

۸. در هر قسمت مثالی از چندجمله‌ایهای $f(x)$ و $g(x)$ ارائه دهید که در شرط داده شده صدق کند:

(الف) درجه $f(x)+g(x)$ کمتر از ماکزیمم $\deg f(x)$ و $\deg g(x)$ باشد.

(ب) $\deg[f(x)+g(x)] = \max\{\deg f(x), \deg g(x)\}$.

۹. اگر $c \in R$ یک مقسوم‌علیه صفر در یک حلقه جابجایی R باشد، آیا در $R[x]$ نیز یک مقسوم‌علیه صفر است؟

B ۱۰. اگر $f(x), g(x) \in R[x]$ و $f(x)+g(x) \neq 0_R$، نشان دهید

$$\deg[f(x)+g(x)] \leq \max\{\deg f(x), \deg g(x)\}$$

۱۱. اگر $\mathbb{F}$ یک میدان باشد نشان دهید $\mathbb{F}[x]$ یک میدان نیست. [راهنمایی: آیا x در $\mathbb{F}[x]$ یکه است؟]

۱۲. فرض کنید $\mathbb{F}$ یک میدان و $f(x)$ یک چندجمله‌ای غیرصفر در $\mathbb{F}[x]$ باشد. نشان دهید $f(x)$ در $\mathbb{F}[x]$ یکه است اگر و تنها اگر $\deg f(x) = 0$.

۱۳. فرض کنید R یک حلقه‌جابجایی باشد. اگر $a_n \neq 0_R$ و $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ یک مقسوم‌علیه صفر در $R[x]$ باشد، ثابت کنید که a_n یک مقسوم علیه صفر در R است.

۱۴. (الف) فرض کنید R یک دامنه صحیح باشد و $f(x), g(x) \in R[x]$. فرض کنید ضریب پیشرو $f(x)$ در R یکه باشد. نشان دهید برای $f(x)$ به عنوان مقسوم و $g(x)$ به عنوان مقسوم‌علیه، الگوریتم تقسیم برقرار است. [راهنمایی: اثبات قضیه ۳.۴ را به وضعیت جدید تطبیق دهید. درکجای آن اثبات از فرض میدان بودن $\mathbb{F}$ استفاده شد؟]

(ب) مثالی در $\mathbb{Z}[x]$ ارائه دهید که نشان دهد اگر ضریب پیشرو $g(x)$ یکه نباشد قسمت (الف) ممکن است غلط باشد. [راهنمایی: تمرین ۷ (ب)]

۱۵. فرض کنید R یک دامنه صحیح باشد و فرض کنید الگوریتم تقسیم در $R[x]$ برقرار است. ثابت کنید R یک میدان است.

۱۶. فرض کنید $\varphi : R[x] \to R$ یک تابع بوده که هر چندجمله‌ای در $R[x]$ را به جمله ثابت آن (یک عضو R) بنگارد. نشان دهید φ یک همریختی پوشای حلقه‌ای است.

۱۷. فرض کنید $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ تابعی باشد که چندجمله‌ای $a_0 + a_1x + \cdots + a_kx^k$ در $\mathbb{Z}[x]$ را بر چندجمله‌ای $[a_0] + [a_1]x + \cdots + [a_k]x^k$ در $\mathbb{Z}[x]$ بنگارد، جایی که $[a]$ کلاس عدد صحیح a در $\mathbb{Z}_n$ را نشان می‌دهد. نشان دهید φ یک همریختی پوشای حلقه‌ای است.

۱۸. فرض کنید $D : \mathbb{R}[x] \to \mathbb{R}[x]$ نگاشت مشتق باشد که به صورت

$$D(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_1 + 2a_2x + 3a_3x^2 + \cdots + na_nx^{n-1}$$

تعریف می‌شود. آیا D یک همریختی حلقه‌ای است؟ آیا D یک یکریختی است؟

۱۹.C. فرض کنید $h : R \to S$ یک همریختی حلقه‌ای بوده و تابع $\bar{h} : R[x] \to S[x]$ را توسط ضابطهٔ $\bar{h}(a_0 + a_1x + \cdots + a_nx^n) = h(a_0) + h(a_1)x + \cdots + h(a_n)x^n$ تعریف کنید. ثابت کنید که

(الف) $\bar{h}$ یک همریختی حلقه‌ای است.

(ب) $\bar{h}$ یک به یک است اگر و تنها اگر h یک به یک باشد.

(پ) $\bar{h}$ پوشا است اگر و تنها اگر h پوشا باشد.

(ت) اگر $S \cong R$، در این صورت $S[x] \cong R[x]$.

۲۰. فرض کنید R یک حلقه جابجایی و $k(x)$ یک چندجمله‌ای در $R[x]$ باشد. ثابت کنید همریختی یکتای $\varphi : R[x] \to R[x]$ وجود دارد به قسمی که

$$\varphi(r) = r \text{ برای هر } r \in R \quad \text{و} \quad \varphi(x) = k(x).$$

۲۱. توضیح دهید چرا اثبات قضیه ۱.۱ نمی‌تواند مستقیماً برای $\mathbb{F}[x]$ بکار رود. چرا کاربرد استقراء در اثبات قضیه ۳.۴ ضروری است؟

۲-۴ بخش‌پذیری در $\mathbb{F}[x]$

در این بخش کلیه نتایج بخش ۲.۱ در مورد بخش‌پذیری و مقسوم‌علیه مشترک در $\mathbb{Z}$ را باندکی تغییرات جزیی به حلقه چندجمله‌ایهای روی یک میدان انتقال می‌دهیم. در واقع در اغلب اثباتهای این بخش از شما تنها خواسته میشود که اثباتهای متناظر ارائه شده برای $\mathbb{Z}$ را به $\mathbb{F}[x]$ تطبیق دهید. انجام عملی این کار متضمن درک صحیح تشابه بین حلقه $\mathbb{Z}$ و حلقه چندجمله‌ایها می‌باشد. سرتاسر این بخش $\mathbb{F}$ همواره یک میدان را نشان می‌دهد.

تعریف. فرض کنید $\mathbb{F}$ یک میدان باشد و $f(x), g(x) \in \mathbb{F}[x]$ با $f(x) \neq 0$. گوئیم $f(x)$ چندجمله‌ای $g(x)$ را می‌شمارد [یا $f(x)$ یک عامل $g(x)$ است] و می‌نویسیم $f(x)|g(x)$، هرگاه برای برخی $h(x) \in \mathbb{F}[x]$، $g(x) = f(x)h(x)$.

مثال ۵.۴. در $\mathbb{Q}[x]$ داریم $(۲x+۱)|(۶x^۲-x-۲)$ زیرا $۶x^۲-x-۲ = (۲x+۱)(۳x-۲)$. بعلاوه هر مضرب ثابتی از $(۲x+۱)$ نیز $۶x^۲-x-۲$ را می‌شمارد. برای مثال $۵(۲x+۱) = ۱۰x+۵$ چندجمله‌ای $۶x^۲ - x - ۲$ را می‌شمارد زیرا $۶x^۲ - x - ۲ = ۵(۲x + ۱)[۱/۵(۳x - ۲)]$. در حالت کلی استدلالی مشابه نشان می‌دهد که

اگر $f(x)$، چندجمله‌ای $g(x)$ را بشمارد، در این صورت برای هر عنصر غیرصفر $c \in \mathbb{F}$، $cf(x)$ نیز $g(x)$ را می‌شمارد.

مثال فوق نشان می‌دهد که یک چندجمله‌ای غیرصفر می‌تواند تعداد نامتناهی شمارنده داشته باشد، در حالی که یک عدد صحیح غیرصفر تنها دارای تعداد متناهی شمارنده است. این مثال همچنین این حقیقت را نمایش می‌دهد که: اگر $g(x)$ غیرصفر باشد، در این صورت

هر شمارنده $g(x)$ دارای درجه کوچکتر یا مساوی $\deg g(x)$ است.

برای دیدن این، فرض کنید $f(x)|g(x)$، یعنی $g(x) = f(x)h(x)$. به موجب قضیه ۱.۴، $\deg g(x) = \deg f(x) + \deg h(x)$. بنابراین $0 \leq \deg f(x) \leq \deg g(x)$.

همانگونه که قبلاً آموخته‌ایم، بزرگترین مقسوم‌علیه مشترک دو عدد صحیح عبارت است از بزرگترین عدد صحیحی که هر دو آنها را می‌شمارد. به‌طور مشابه، بزرگترین مقسوم‌علیه مشترک دو چندجمله‌ای $f(x), g(x) \in \mathbb{F}[x]$ می‌بایست چندجمله‌ای با بزرگترین درجه باشد که هر دو آنها را بشمارد. امّا چنین بزرگترین مقسوم‌علیه مشترک یکتا نخواهد بود زیرا هر مضرب ثابتی از آن نیز دارای همان درجه بوده و هر دو $f(x)$ و $g(x)$ را نیز می‌شمارد. برای تضمین یکتایی ب‌م‌م، تعریف را با معرفی مفهومی جدید اصلاح می‌نمائیم. یک چندجمله‌ای در $\mathbb{F}[x]$ **تکین** نامیده می‌شود هرگاه ضریب پیشرو آن $1_{\mathbb{F}}$ باشد. به عنوان مثال $x^۳ + x + ۲$ در $\mathbb{Q}[x]$ تکین است، امّا $۲x + ۱$ تکین نیست.

تعریف. فرض کنید $\mathbb{F}$ یک میدان باشد و $f(x), g(x) \in \mathbb{F}[x]$ تواماً صفر نباشند. بزرگترین مقسوم علیه مشترک (ب‌م‌م) $f(x)$ و $g(x)$ عبارت است از چندجمله‌ای تکین $d(x)$ با بزرگترین

درجه که هر دو $f(x)$ و $g(x)$ را بشمارد. به بیان دیگر، $d(x)$ ب‌مم $f(x)$ و $g(x)$ است مشروط بر این که $d(x)$ تکین بوده و

(i) $d(x)|f(x)$ و $d(x)|g(x)$؛

(ii) اگر $c(x)|f(x)$ و $c(x)|g(x)$ در این صورت $\deg c(x) \leq \deg d(x)$.

چون درجه هر مقسوم‌علیه مشترک $f(x)$ و $g(x)$ از $\deg f(x)$ و $\deg g(x)$ بیشتر نیست، واضح است که حداقل یک ب‌مم برای $f(x)$ و $g(x)$ وجود دارد. در قضیه ۴.۴ نشان می‌دهیم که این ب‌مم یکتاست. بنابراین ارجاع تعریف به بزرگترین مقسوم‌علیه مشترک موجه می‌باشد.

مثال ۶.۴. برای یافتن ب‌مم $۳x^۲ + x + ۶$ و ۰ در $\mathbb{Q}[x]$، توجه می‌کنیم که مقسوم‌علیه‌های مشترک با بزرگترین درجه، مقسوم‌علیه‌های با درجه ۲ چندجمله‌ای $۳x^۲ + x + ۶$ می‌باشند که شامل خود $۳x^۲ + x + ۶$ و همه مضارب ثابت غیرصفر این چندجمله‌ای و به‌ویژه، چندجمله‌ای تکین $x^۲ + \frac{۱}{۳}x + ۲ = \frac{۱}{۳}(۳x^۲ + x + ۶)$ است. بنابراین $x^۲ + \frac{۱}{۳}x + ۲$ یک ب‌مم $۳x^۲ + x + ۶$ و ۰ است.

مثال ۷.۴. تجزیه‌های زیر در $\mathbb{Q}[x]$ به سادگی قابل بررسی هستند:

$$f(x) = ۲x^۴ + ۵x^۳ - ۵x - ۲ = (۲x + ۱)(x + ۲)(x + ۱)(x - ۱),$$
$$g(x) = ۲x^۳ - ۳x^۲ - ۲x = (۲x + ۱)(x - ۲)x.$$

به نظر می‌رسد که $۲x + ۱$ یک مقسوم‌علیه مشترک با بزرگترین درجه از $f(x)$ و $g(x)$ است. در این حالت، مضرب ثابتی از آن یعنی $x + \frac{۱}{۲} = \frac{۱}{۲}(۲x + ۱)$ یک مقسوم‌علیه مشترک تکین با بیشترین درجه است. اثبات این که $x + \frac{۱}{۲}$ در واقع بزرگترین مقسوم‌علیه مشترک می‌باشد در پایان این بخش آمده است. همچنین می‌توانید بررسی کنید که این بزرگترین مقسوم‌علیه مشترک می‌تواند به صورت $f(x)u(x) + g(x)v(x)$ نوشته شود:

$$x + \frac{۱}{۲} = (۲x^۴ + ۵x^۳ - ۵x - ۲)(\frac{۷}{۴۸}x - \frac{۱}{۴}) + (۲x^۳ - ۳x^۲ - ۲x)(-\frac{۷}{۴۸}x^۲ - \frac{۱}{۳}x - \frac{۱}{۴۸}).$$

قضیه ۴.۴. فرض کنید $\mathbb{F}$ یک میدان باشد و $f(x), g(x) \in \mathbb{F}[x]$، همزمان صفر نباشند. در این صورت $f(x)$ و $g(x)$ دارای یک بزرگترین مقسوم‌علیه مشترک یکتاست. بعلاوه، اگر $d(x)$ این

بزرگترین مقسوم‌علیه مشترک باشد، در این صورت چندجمله‌ای‌های $u(x)$ و $v(x)$ (که لزوماً یکتا نیستند) وجود دارد به طوری که $d(x) = f(x)u(x) + g(x)v(x)$.

برهان. فرض کنید $t(x)$ یک چندجمله‌ای تکین با کوچکترین درجه در مجموعهٔ $S = \{f(x)m(x) + g(x)n(x) \mid m(x), n(x) \in \mathbb{F}[x]\}$ باشد. به موجب تعریف S، $t(x) = f(x)u(x) + g(x)v(x)$، برای برخی $u(x), v(x) \in \mathbb{F}[x]$. حال اثبات قضیه ۳.۱ را برای $\mathbb{F}[x]$ به صورت زیر سازگار کنید؛ نابرابریهای بین اعداد صحیح را با نابرابریهایی که درجه چندجمله‌ایها را شامل می‌شوند جایگزین کرده و نشان دهید که $t(x)$ بزرگترین مقسوم‌علیه مشترک $f(x)$ و $g(x)$ است.

سپس فرض کنید $d(x)$ ب‌م‌م دلخواهی از $f(x)$ و $g(x)$ باشد. برای اثبات یکتایی باید نشان دهیم که $d(x) = t(x)$. چون $d(x)$ یک مقسوم‌علیه مشترک است لذا برای برخی $a(x), b(x) \in \mathbb{F}[x]$، داریم $f(x) = d(x)a(x)$ و $g(x) = d(x)b(x)$. بنابراین

$$\begin{aligned} t(x) &= f(x)u(x) + g(x)v(x) = [d(x)a(x)]u(x) + [d(x)b(x)]v(x) \\ &= d(x)[a(x)u(x) + b(x)v(x)]. \end{aligned}$$

به موجب قضیه ۱.۴، $\deg t(x) = \deg d(x) + \deg[a(x)u(x) + b(x)v(x)]$. امّا $t(x)$ و $d(x)$ هر دو ب‌م‌م اند و لذا دارای درجه یکسان هستند. بنابراین $\deg[a(x)u(x)+b(x)v(x)] = 0$ و لذا برای برخی عضو غیرصفر $c \in \mathbb{F}$، $a(x)u(x) + b(x)v(x) = c$. بنابراین $t(x) = d(x)c$. حال $d(x)$ یک ب‌م‌م تکین است، گیریم $d(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. بنابراین $cd(x) = cx^n + \cdots + ca_1 x + ca_0$. امّا $cd(x)$ چندجمله‌ای تکین $t(x)$ است. پس $c = 1_{\mathbb{F}}$ و $d(x) = t(x)$. بنابراین $d(x) = f(x)u(x) + g(x)v(x)$ یکتا است و $d(x)$ ب‌م‌م یکتا است.

نتیجه ۵.۴. فرض کنید $\mathbb{F}$ یک میدان باشد و $f(x), g(x) \in \mathbb{F}[x]$، همزمان صفر نباشند. یک چندجمله‌ای تکین $d(x) \in \mathbb{F}[x]$ بزرگترین مقسوم‌علیه مشترک $f(x)$ و $g(x)$ است اگر و تنها اگر $d(x)$ در شرایط زیر صدق کند:

(i) $d(x)|f(x)$ و $d(x)|g(x)$؛

(ii) اگر $c(x)|f(x)$ و $c(x)|g(x)$ در این صورت $c(x)|d(x)$.

برهان. اثبات نتیجه ۴.۱ را به $\mathbb{F}[x]$ تطبیق دهید. ■

چندجمله‌ایهای $f(x)$ و $g(x)$ را نسبت به هم اوّل گوییم هرگاه بزرگترین مقسوم‌علیه مشترک آنها $1_{\mathbb{F}}$ باشد.

قضیه ۶.۴. فرض کنید $\mathbb{F}$ یک میدان باشد و $f(x), g(x), h(x) \in \mathbb{F}[x]$. اگر $f(x)|g(x)h(x)$ و $f(x)$ و $g(x)$ نسبت به هم اوّل باشند در این صورت $f(x)|h(x)$.

برهان. اثبات قضیه ۵.۱ را به $\mathbb{F}[x]$ تطبیق دهید. ■

الگوریتم اقلیدسی (قضیه ۶.۱) در $\mathbb{Z}$ را نیز می‌توان به $\mathbb{F}[x]$ انتقال داد و این روش مؤثری برای محاسبه بزرگترین مقسوم‌علیه‌های مشترک فراهم می‌کند. تنها تفاوت نسبت به $\mathbb{Z}$ در این است که آخرین باقیمانده در فرایند الگوریتم، یک مقسوم‌علیه مشترک با بزرگترین درجه بوده ولی لزوماً تکین نیست. پس بایستی در یک ثابت مناسب ضرب شود تا ب‌م‌م را تولید کند.

مثال ۸.۴. برای یافتن ب‌م‌م $f(x) = 2x^4 + 5x^3 - 5x - 2$ و $g(x) = 2x^3 - 3x^2 - 2x$ در $\mathbb{Q}[x]$ الگوریتم تقسیم را به طور مکرر بکار می‌بریم تا جایی که به باقیمانده صفر برسیم. مقسوم‌علیه و باقیمانده هر مرحله، مقسوم و مقسوم‌علیه مرحله بعد می‌شود:

$$2x^4 + 5x^3 - 5x - 2 = (2x^3 - 3x^2 - 2x)(x + 4) + (14x^2 + 3x - 2)$$

$$2x^3 - 3x^2 - 2x = (14x^2 + 3x - 2)(\frac{1}{7}x - \frac{12}{49}) + (-\frac{48}{49}x - \frac{24}{49})$$

$$14x^2 + 3x - 2 = (-\frac{48}{49}x - \frac{24}{49})(-\frac{343}{24}x + \frac{49}{12}) + 0.$$

بنابراین آخرین باقیمانده غیرصفر یعنی $-\frac{48}{49}x - \frac{24}{49}$، یک مقسوم‌علیه مشترک با بزرگترین درجه بوده و لذا ب‌م‌م چندجمله‌ای تکین $x + \frac{1}{2} = (-\frac{48}{49}x - \frac{24}{49})(\frac{-49}{48})$ است.

تمرینها

توجه: $\mathbb{F}$ یک میدان را نشان می‌دهد.

A.۱. اگر $f(x) \in \mathbb{F}[x]$، نشان دهید که هر چندجمله‌ای ثابت غیرصفر، $f(x)$ را می‌شمارد.

۲. اگر $f(x) = c_n x^n + \cdots + c_0$ با $c_n \neq 0_{\mathbb{F}}$، ب‌م‌م $f(x)$ و $0_{\mathbb{F}}$ چیست؟

۳. اگر $a, b \in \mathbb{F}$ و $a \neq b$، نشان دهید که $x + a$ و $x + b$ در $\mathbb{F}[x]$ نسبت به هم اولند.

۴. (الف) فرض کنید $f(x), g(x) \in \mathbb{F}[x]$. اگر $f(x)|g(x)$ و $g(x)|f(x)$، نشان دهید که برای برخی مقدار غیرصفر $c \in \mathbb{F}$، $f(x) = cg(x)$.
(ب) اگر $f(x)$ و $g(x)$ در قسمت (الف) تکین باشند، نشان دهید که $f(x) = g(x)$.

۵. الگوریتم اقلیدسی را بکار برید تا ب‌مم چندجمله‌ایهای داده شده را بیابید:
(الف) $x^4 - x^3 - x^2 + 1$ و $x^3 - 1$ در $\mathbb{Q}[x]$
(ب) $x^5 + x^4 + 2x^3 - x^2 - x - 2$ و $x^4 + 2x^3 + 5x^2 + 4x + 4$ در $\mathbb{Q}[x]$.
(پ) $x^4 + 3x^3 + 2x + 4$ و $x^3 - 1$ در $\mathbb{Z}_5[x]$
(ت) $4x^4 + 2x^3 + 6x^2 + 4x + 5$ و $6x^3 + 5x^2 + 3$ در $\mathbb{Z}_7[x]$
(ث) $x^3 - ix^2 + 4x - 4i$ و $x^2 + 1$ در $\mathbb{C}[x]$
(ج) $x^4 + x + 1$ و $x^2 + x + 1$ در $\mathbb{Z}_2[x]$

۶. هر کدام از ب‌مم های تمرین ۵ را برحسب یک ترکیب خطی از دو چندجمله‌ای داده شده بیان کنید.

۷.B فرض کنید $f(x) \in \mathbb{F}[x]$ و این‌که برای هر چندجمله‌ای غیرثابت $g(x) \in \mathbb{F}[x]$، $f(x)|g(x)$. نشان دهید $g(x)$ یک چندجمله‌ای ثابت است. [راهنمایی: تمرین ۳ را ملاحظه کنید.]

۸. فرض کنید $f(x), g(x) \in \mathbb{F}[x]$، همزمان صفر نباشند، و فرض کنید $d(x)$ ب‌مم آنها باشد. اگر $h(x)$ یک مقسوم‌علیه مشترک با بزرگترین درجه ممکن از $f(x)$ و $g(x)$ باشد، در این صورت ثابت کنید که برای برخی ثابت غیرصفر $c \in \mathbb{F}$، $h(x) = cd(x)$.

۹. اگر $f(x)$ نسبت به $0_{\mathbb{F}}$ اول باشد، در مورد $f(x)$ چه می‌توان گفت؟

۱۰. ب‌مم $x + a + b$ و $x^3 - 3abx + a^3 + b^3$ در $\mathbb{Q}[x]$ را بیابید.

۱۱. جزئیات اثبات قضیه ۴.۴ را کامل کنید.

۱۲. نتیجه ۵.۴ را اثبات کنید.

۱۳. قضیه ۶.۴ را ثابت کنید.

۱۴. فرض کنید $f(x), g(x), h(x) \in \mathbb{F}[x]$، و $f(x)$ و $g(x)$ نسبت به هم اول باشند. اگر $f(x)|h(x)$ و $g(x)|h(x)$، ثابت کنید $f(x)g(x)|h(x)$.

۱۵. فرض کنید $f(x), g(x), h(x) \in \mathbb{F}[x]$، و $f(x)$ و $g(x)$ نسبت به هم اول باشند. اگر $h(x)|f(x)$، ثابت کنید که $h(x)$ و $g(x)$ نسبت به هم اولند.

۱۶. فرض کنید $f(x), g(x), h(x) \in \mathbb{F}[x]$، و $g(x), f(x)$ نسبت به هم اول باشند. ثابت کنید که ب‌مم $f(x)h(x)$ و $g(x)$ همان ب‌مم $h(x)$ و $g(x)$ است.

۳-۴ تحویل‌ناپذیری و یکتایی تجزیه

قبل از این که نتایج بخش ۱ـ۳ در مورد یکتایی تجزیه در $\mathbb{Z}$ را به حلقه چندجمله‌ایها روی یک میدان $\mathbb{F}$ انتقال دهیم، ابتدا بخشی که در آن $\mathbb{Z}$ به طور قابل ملاحظه‌ای متفاوت از $\mathbb{F}[x]$ رفتار می‌کند را مورد بررسی قرار دهیم. می‌دانیم که تنها یکه‌های $\mathbb{Z}$، ± 1 هستند، امّا برای چندجمله‌ایها داریم:

قضیه ۷.۴. فرض کنید $\mathbb{F}$ یک میدان باشد. در این صورت $f(x)$ در $\mathbb{F}[x]$ یکه است اگر و تنها اگر $f(x)$ یک چندجمله‌ای ثابت غیرصفر باشد.

برهان. فرض کنید $f(x)$ در $\mathbb{F}[x]$ یکه باشد، لذا برای برخی $g(x)$، $f(x)g(x) = 1_{\mathbb{F}}$. به موجب قضیه ۱.۴،

$$\deg f(x) + \deg g(x) = \deg[f(x)g(x)] = \deg[1_{\mathbb{F}}] = 0.$$

چون درجه یک عدد صحیح غیرمنفی است، $\deg f(x) = 0$ و $\deg g(x) = 0$. بنابراین $f(x)$ و $g(x)$ چندجمله‌ایهای ثابت غیرصفرند. بالعکس، فرض کنید $f(x) = b$ با $b \in \mathbb{F}$ $b \neq 0_{\mathbb{F}}$. در این صورت b در $\mathbb{F}$ یکه است، لذا $g(x) = b^{-1}$ یک چندجمله‌ای ثابت در $\mathbb{F}[x]$ است و $f(x)g(x) = bb^{-1} = 1_{\mathbb{F}}$. بنابراین $f(x)$ در $\mathbb{F}[x]$ یکه است. ■

قضیه ۷.۴ نشان می‌دهد که هر یک از حلقه‌های $\mathbb{Q}[x]$ و $\mathbb{C}[x]$ دارای تعداد نامتناهی یکه هستند. با این حال اگر $\mathbb{F}$ میدان نباشد، قضیه ممکن است غلط باشد. برای مثال چندجمله‌ای

ثابت ۲ $= f(x)$ در $\mathbb{Z}[x]$ یکه نیست چون وارون آن، ۱/۲، در $\mathbb{Z}$ قرار نمی‌گیرد. چندجمله‌ای $۳x + ۱$ در $\mathbb{Z}_۱[x]$ یکه است زیرا $(۳x + ۱)(۶x + ۱) = ۱$ (بررسی کنید!).

یک چندجمله‌ای $f(x) \in \mathbb{F}[x]$ **وابسته** $g(x) \in \mathbb{F}[x]$ گفته می‌شود اگر برای برخی ثابت غیرصفر $c \in \mathbb{F}$، $f(x) = cg(x)$. برای مثال، برخی از وابسته‌های $x^۲ + ۱$ در $\mathbb{Q}[x]$ عبارتند از $۵(x^۲ + ۱)$ و $\frac{۱}{۷}(x^۲ + ۱)$. به موجب قضیه ۷.۵، هر وابسته $g(x)$ به صورت حاصل‌ضرب $g(x)$ در یک یکه $\mathbb{F}[x]$ است. بنابراین وابسته‌های $g(x)$ همان نقش $\pm n$ در $\mathbb{Z}$ (حاصل‌ضرب n با یک یکه در $\mathbb{Z}$) را در $\mathbb{F}[x]$ ایفا می‌کنند. توجه کنید که اگر $f(x)$ یک وابسته $g(x)$ باشد، یعنی $f(x) = cg(x)$، در این صورت $c^{-۱}f(x) = c^{-۱}(cg(x)) = g(x)$. بنابراین

$f(x)$ یک وابسته $g(x)$ است اگر و تنها اگر $g(x)$ یک وابسته $f(x)$ باشد.

به خاطر آورید که یک عدد صحیح (به‌جز ۰ یا ± ۱) در $\mathbb{Z}$ اول است اگر تنها شمارنده‌های آن ± ۱ (یکه‌های $\mathbb{Z}$) و $\pm p$ (وابسته‌های p در $\mathbb{Z}$) باشد. در زیر تعریف مشابه برای چندجمله‌ایها آمده است.

تعریف. فرض کنید $\mathbb{F}$ یک میدان باشد. یک چندجمله‌ای غیرثابت $p(x) \in \mathbb{F}[x]$ **تحویل‌ناپذیر**[۴] گفته می‌شود اگر تنها شمارنده‌های آن وابسته‌ها و چندجمله‌ایهای ثابت غیرصفر (یکه‌ها) باشند. یک چندجمله‌ای غیرثابت که تحویل‌ناپذیر نیست، **تحویل‌پذیر** گفته می‌شود.

مثال ۹.۴. چندجمله‌ای $x + ۲$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است زیرا به موجب قضیه ۱.۴، همه شمارنده‌های آن باید دارای درجه ۰ یا ۱ باشند. شمارنده‌های از درجه ۰، چندجمله‌ایهای ثابت غیرصفر هستند. اگر $f(x)|(x + ۲)$، مثلاً $x + ۲ = f(x)g(x)$ و اگر $\deg f(x) = ۱$، در این صورت $g(x)$ دارای درجه ۰ است، لذا $g(x) = c$. بنابراین $f(x) = c^{-۱}(x + ۲)$ و $f(x)$ یک وابسته $x + ۲$ است. در حالت کلی استدلالی مشابه نشان می‌دهد که

هر چندجمله‌ای از درجه ۱ در $\mathbb{F}[x]$ تحویل‌ناپذیر در $\mathbb{F}[x]$ است.

در بخشهای ۴.۴ تا ۶.۴ آزمونهای متنوعی برای تحویل‌ناپذیری آورده شده است. در حال حاضر، باید توجه کنیم که مفهوم تحویل‌ناپذیری یک مفهوم مطلق نیست. برای مثال $x^۲ + ۱$ در $\mathbb{C}[x]$

۴) می‌توانید چنین چندجمله‌ای را "اول" نیز بنامید، امّا "تحویل‌ناپذیر" اصطلاح معمول برای چندجمله‌ایهایی از این نوع است.

تحویل‌پذیر است زیرا $x^2+1=(x+i)(x-i)$ و هیچکدام از عوامل آن ثابت و یا یک وابسته x^2+1 نیست، امّا x^2+1 در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. (تمرین ۶).

قضیه زیر نشان می‌دهد که عناصر تحویل‌ناپذیر در $\mathbb{F}[x]$ اساساً همان خواص بخش‌پذیری اعداد اول در $\mathbb{Z}$ را دارا می‌باشند. خاصیت (۳) در قضیه، اغلب برای اثبات این که یک چندجمله‌ای تحویل‌ناپذیر است بکار برده می‌شود. در بسیاری از کتاب‌ها، خاصیت (۳) به عنوان تعریف تحویل‌ناپذیری آمده است.

قضیه ۸.۴. فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای غیرثابت در $\mathbb{F}[x]$ باشد. در این صورت شرایط زیر هم‌ارزند:

(۱) $p(x)$ تحویل‌ناپذیر است.

(۲) اگر $b(x)$ و $c(x)$ دو چندجمله‌ای باشند طوری که $p(x)|b(x)c(x)$، در این صورت یا $p(x)|b(x)$ یا $p(x)|c(x)$.

(۳) اگر $r(x)$ و $s(x)$ دوچندجمله‌ای باشند طوری که $p(x)=r(x)s(x)$، در این صورت یا $r(x)$ یا $s(x)$ یک چندجمله‌ای ثابت غیرصفر است.

برهان. (۱) $\Leftarrow$ (۲) اثبات قضیه ۸.۱ را به $\mathbb{F}[x]$ تطبیق دهید. گزاره‌های درباره $\pm p$ را با گزاره‌هایی درباره وابسته‌های $p(x)$ عوض کنید؛ گزاره‌های درباره ± 1 را با گزاره‌هایی درباره یکه‌ها (چندجمله‌ایهای ثابت غیرصفر) در $\mathbb{F}[x]$ عوض کنید؛ قضیه ۶.۴ را بجای قضیه ۵.۱ بکار ببرید.

(۲) $\Leftarrow$ (۳) اگر $p(x)=r(x)s(x)$، در این صورت به موجب (۲)، $p(x)|r(x)$ یا $p(x)|s(x)$. اگر $r(x)|p(x)$ ، یعنی داشته‌باشیم $r(x)=p(x)v(x)$، در این صورت $p(x)=r(x)s(x)=p(x)v(x)s(x)$. چون $\mathbb{F}[x]$ یک دامنه صحیح است، به موجب قضیه ۷.۳ می‌توانیم $p(x)$ را حذف کنیم و نتیجه بگیریم که $1_{\mathbb{F}}=v(x)s(x)$. بنابراین $s(x)$ یکه است و لذا به موجب قضیه ۷.۴، $s(x)$ یک ثابت غیرصفر است. استدلالی مشابه نشان می‌دهد که اگر $p(x)|s(x)$، در این صورت $r(x)$ یک ثابت غیرصفر است.

(۳) $\Leftarrow$ (۱) فرض کنید $c(x)$ شمارنده دلخواهی از $p(x)$ باشد، فرض کنید $p(x)=c(x)d(x)$. در این صورت به موجب (۳)، یا $c(x)$ یا $d(x)$ یک ثابت غیرصفر است. اگر $d(x)=d\neq 0_{\mathbb{F}}$، در این صورت ضرب کردن دو طرف $p(x)=c(x)d(x)=dc(x)$ در d^{-1} نشان می‌دهد که $c(x)=d^{-1}p(x)$. پس در هر صورت $c(x)$ یک ثابت غیرصفر و یا یک وابسته $p(x)$ است. بنابراین $p(x)$ تحویل‌ناپذیر است. ■

نتیجه ۹.۴. فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}[x]$ باشد. اگر $p(x)|a_1(x)a_2(x)\cdots a_n(x)$، در این صورت $p(x)$ حداقل یکی از $a_i(x)$ ها را می‌شمارد.

برهان. اثبات نتیجه ۹.۱ را به $\mathbb{F}[x]$ تطبیق دهید. ■

قضیه ۱۰.۴. فرض کنید $\mathbb{F}$ یک میدان باشد. در این صورت هر چندجمله‌ای غیرثابت $f(x)$ در $\mathbb{F}[x]$ حاصل‌ضربی [۵] از چندجمله‌ایهای تحویل‌ناپذیر در $\mathbb{F}[x]$ است. این تجزیه به مفهوم زیر یکتاست: اگر

$$f(x) = p_1(x)p_2(x)\cdots p_r(x) \quad \text{و} \quad f(x) = q_1(x)q_2(x)\cdots q_s(x)$$

که در آن هر $p_i(x)$ و $q_j(x)$ تحویل‌ناپذیر است، در این صورت $r = s$ (یعنی تعداد عوامل تحویل‌ناپذیر در هر دو یکسان است). بعلاوه پس از احتمالاً تغییر ترتیب عناصر و نمایه‌گذاری مجدد داریم $p_i(x)$ یک وابسته $q_i(x)$ است $(i = 1, 2, 3, \ldots, r)$.

برهان. برای نشان دادن این که $f(x)$ حاصل‌ضربی از عوامل تحویل‌ناپذیر است، اثبات قضیه ۱۰.۱ را به $\mathbb{F}[x]$ تطبیق دهید: فرض کنید S مجموعه همه چندجمله‌ایهای غیرثابتی باشد که حاصل‌ضربی از عوامل تحویل‌ناپذیر نیستند. برهان خلف را بکار برید تا نشان دهید که S تهی است. برای اثبات این که این تجزیه تا حد وابسته‌ها یکتا است، فرض کنید $f(x) = p_1(x)p_2(x)\cdots p_r(x) = q_1(x)q_2(x)\cdots q_s(x)$ که در آن هر $p_i(x)$ و $q_j(x)$ تحویل‌ناپذیر است. در این صورت $p_1(x)|q_1(x)q_2(x)\cdots q_s(x)$. بنابراین $p_1(x)[p_2(x)\cdots p_r(x)] = q_1(x)q_2(x)\cdots q_s(x)$ حاصل‌ضرب $p_1(x)$ را می‌شمارد. نتیجه ۹.۴ نشان می‌دهد که برای برخی j، $p_1(x)|q_j(x)$. پس از تغییر ترتیب و نمایه‌گذاری مجدد، در صورت لزوم، می‌توان فرض کرد $p_1(x)|q_1(x)$. چون $q_1(x)$ تحویل‌ناپذیر است، $p_1(x)$ بایستی ثابت و یا یک وابسته $q_1(x)$ باشد. ولی $p_1(x)$ تحویل‌ناپذیر است و لذا ثابت نیست. بنابراین $p_1(x)$ یک وابسته $q_1(x)$ است. پس برای برخی ثابت c_1، $p_1(x) = c_1q_1(x)$. بنابراین

$$q_1(x)[c_1p_2(x)p_2(x)\cdots p_r(x)] = p_1(x)p_2(x)\cdots p_r(x) = q_1(x)q_2(x)\cdots q_s(x).$$

با حذف $q_1(x)$ از دو طرف داریم

$$p_2(x)[c_1p_2(x)\cdots p_r(x)] = q_2(x)q_2(x)\cdots q_s(x).$$

۵) ما احتمال یک حاصل‌ضرب با تنها یک عامل را در حالتی که $f(x)$ خودش تحویل‌ناپذیر است می‌پذیریم.

استدلال را با تطبیق اثبات قضیه ۱۱.۱ به $\mathbb{F}[x]$ کامل کنید؛ گزاره‌های مربوط به $\pm q_j$ را با گزاره‌های مربوط به وابسته‌های $q_j(x)$ عوض کنید. ■

تمرینها

توجه: $\mathbb{F}$ یک میدان و p یک عدد صحیح اول را نشان می‌دهد.

۱.A. یک وابسته تکین از هر یک از چندجمله‌ای‌های زیر بیابید.

(الف) $3x^3 + 2x^2 + x + 5$ در $\mathbb{Q}[x]$ (ب) $3x^5 - 4x^2 + 1$ در $\mathbb{Z}_5[x]$

(پ) $ix^3 + x - 1$ در $\mathbb{C}[x]$

۲. ثابت کنید که هر عضو غیرصفر $f(x) \in \mathbb{F}[x]$ دارای یک وابسته تکین یکتا در $\mathbb{F}[x]$ است.

۳. همه وابسته‌های هر یک از چندجمله‌ایهای زیر را فهرست کنید:

(الف) $x^2 + x + 1$ در $\mathbb{Z}_5[x]$ (ب) $3x + 2$ در $\mathbb{Z}_7[x]$

۴. نشان دهید هر چندجمله‌ای غیر صفر در $\mathbb{Z}_p[x]$ دارای دقیقاً $p - 1$ وابسته است.

۵. ثابت کنید $f(x)$ و $g(x)$ در $\mathbb{F}[x]$ وابسته‌اند اگر و تنها اگر $f(x)|g(x)$ و $g(x)|f(x)$.

۶. نشان دهید $x^2 + 1$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. [راهنمایی: در غیر اینصورت دارای تجزیه‌ای به صورت $(ax + b)(cx + d)$ با $a, b, c, d \in \mathbb{Q}$ است؛ نشان دهید این غیر ممکن است.]

۷. ثابت کنید $f(x)$ تحویل‌ناپذیر در $\mathbb{F}[x]$ است اگر و تنها اگر هرکدام از وابسته‌های آن تحویل‌ناپذیر باشند.

۸. ثابت کنید یک چندجمله‌ای غیرصفر $f(x)$ تحویل‌ناپذیر در $\mathbb{F}[x]$ است اگر و تنها اگر $f(x)$ حاصل‌ضربی از دوچندجمله‌ای در $\mathbb{F}[x]$ با درجات کمتر از درجه $f(x)$ نباشد.

۹. همه چندجمله‌ایهای تحویل‌ناپذیر از

(الف) درجه ۲ در $\mathbb{Z}_2[x]$ (ب) درجه ۳ در $\mathbb{Z}_2[x]$

(پ) درجه ۲ در $\mathbb{Z}_3[x]$

را بیابید.

۱۰. آیا چندجمله‌ایهای داده شده زیر تحویل‌ناپذیرند:

(الف) $x^۲ - ۳$ در $\mathbb{Q}[x]$؟ در $\mathbb{R}[x]$؟

(ب) $x^۲ + x - ۲$ در $\mathbb{Z}_۳[x]$؟ در $\mathbb{Z}_۷[x]$؟

۱۱. نشان دهید $x^۳ - ۳$ تحویل‌ناپذیر در $\mathbb{Z}_۷[x]$ است.

۱۲. $x^۴ - ۴$ را به عنوان حاصل‌ضربی از چندجمله‌ایهای تحویل‌ناپذیر در $\mathbb{Q}[x]$، در $\mathbb{R}[x]$ و در $\mathbb{C}[x]$ بیان کنید.

۱۳. یکتایی تجزیه را بکاربرید تا ب.م.م $(x-۱)(x-۳)(x-۴)^۳$ و $(x-۲)^۲(x-۴)^۲(x-۳)^۳$ را در $\mathbb{C}[x]$ بیابید.

۱۴. نشان دهید که هر عامل تحویل‌ناپذیر $x^۴ - ۱$ در $\mathbb{R}[x]$ یک وابسته $x+۱$، $x-۱$ و یا $x^۲+۱$ است.

۱۵.B فرض کنید R یک دامنه صحیح باشد. نشان دهید $f(x)$ در $R[x]$ یکه است اگر و تنها اگر $f(x) = c$ که در آن c در R یکه است.

۱۶. ثابت کنید $p(x)$ تحویل‌ناپذیر در $\mathbb{F}[x]$ است اگر و تنها اگر برای هر $g(x) \in \mathbb{F}[x]$، یا $p(x)|g(x)$ و یا $p(x)$ نسبت به $g(x)$ اول است.

۱۷. قضیه ۸.۴ را ثابت کنید.

۱۸. در قضیه ۸.۴، بدون استفاده از گزاره (۲)، مستقیماً ثابت کنید که گزاره (۱) هم‌ارز گزاره (۳) است.

۱۹. نتیجه ۹.۴ را ثابت کنید.

۲۰. اگر $p(x)$ و $q(x)$ تحویل‌ناپذیر و غیر وابسته در $\mathbb{F}[x]$ باشند، ثابت کنید که $p(x)$ و $q(x)$ نسبت به هم اولند.

۲۱. (الف) با شمارش حاصل‌ضربهایی به صورت $(x+a)(x+b)$ نشان دهید که دقیقاً $(p^۲+p)/۲$ چندجمله‌ای تکین از درجه ۲ وجود دارد که در $\mathbb{Z}_p[x]$ تحویل‌ناپذیر نیستند.

(ب) نشان دهید که دقیقاً $(p^۲-p)/۲$ چندجمله‌ای تکین تحویل‌ناپذیر از درجه ۲ در $\mathbb{Z}_p[x]$ وجود دارد.

۲۲. (الف) نشان دهید که برای هر $a \in \mathbb{Z}_3$، چندجمله‌ای $x^3 + a$ در $\mathbb{Z}_3[x]$ تحویل‌پذیر است.
(ب) نشان دهید که برای هر $a \in \mathbb{Z}_5$ چندجمله‌ای $x^5 + a$ در $\mathbb{Z}_5[x]$ تحویل‌پذیر است.

۲۳. (الف) نشان دهید $x^2 + 2$ در $\mathbb{Z}_5[x]$ تحویل‌ناپذیر است.
(ب) $x^4 - 4$ را به عنوان حاصل ضربی از عوامل تحویل‌ناپذیر در $\mathbb{Z}_5[x]$ تجزیه کنید.

۲۴. قضیه ۱۰.۴ را ثابت کنید.

۲۵. ثابت کنید هر عضو غیرثابت $f(x) \in \mathbb{F}[x]$ را می‌توان به صورت $cp_1(x)p_2(x)\cdots p_n(x)$ تجزیه کرد که در آن $c \in \mathbb{F}$ و هر $p_i(x)$ یک چندجمله‌ای تحویل‌ناپذیر تکین در $\mathbb{F}[x]$ است. بعلاوه نشان دهید که اگر $f(x) = dq_1(x)q_2(x)\cdots q_m(x)$ با $d \in \mathbb{F}$ و هر $q_j(x)$ یک چندجمله‌ای تحویل‌ناپذیر تکین در $\mathbb{F}[x]$ باشد، در این صورت $m = n$، $c = d$، و پس از احتمالاً تغییر ترتیب عناصر و نمایه‌گذاری مجدد، $p_i(x) = q_i(x)$ برای هر i.

۲۶.C ثابت کنید که هیچ چندجمله‌ای تحویل‌ناپذیر از درجه ۲ در $\mathbb{C}[x]$ وجود ندارد.

۴-۴ توابع چندجمله‌ای، ریشه‌ها و تحویل‌پذیری

در بسط و توسعه موازی $\mathbb{F}[x]$ و $\mathbb{Z}$، گام بعدی در نظرگرفتن محک‌هایی برای تحویل‌ناپذیری چندجمله‌ایها (مشابه آزمونهای اول بودن برای اعداد صحیح) می‌باشد. برخلاف وضعیتی که در مورد اعداد صحیح داریم، در مورد چندجمله‌ایها محک‌هایی وجود دارد که به استفاده از رایانه بستگی ندارد، بلکه بیشتر به این حقیقت متکی است که هر چندجمله‌ای در $\mathbb{F}[x]$ یک تابع از $\mathbb{F}$ به $\mathbb{F}$ را القاء می‌کند. خواص این تابع (به ویژه نقاطی که تابع در آن صفر است) رابطه تنگاتنگی با تحویل‌پذیری یا تحویل‌ناپذیری این چندجمله‌ایها دارد.

در سرتاسر این بخش، R یک حلقه جابجایی است. نظیر به هر چندجمله‌ای $a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$ در $R[x]$ یک تابع $f : R \to R$ وجود دارد که ضابطه آن

$$f(r) = a_n r^n + \cdots + a_2 r^2 + a_1 r + a_0$$

برای هر $r \in R$ می‌باشد. تابع f که توسط این چندجمله‌ای القاء می‌شود را یک **تابع چندجمله‌ای** می‌نامند.

مثال ۱۰.۴. چندجمله‌ای $x^۲ + ۵x + ۳ \in R[x]$ یک تابع چندجمله‌ای $f : R \to R$ القاء می‌کند که ضابطه آن $f(r) = r^۲ + ۵r + ۳$ برای هر $r \in R$ می‌باشد.

مثال ۱۱.۴. چندجمله‌ای $x^۴ + x + ۱ \in \mathbb{Z}_۳[x]$ تابع $f : \mathbb{Z}_۳ \to \mathbb{Z}_۳$ را القاء می‌کند که ضابطه آن $f(r) = r^۴ + r + ۱$ می‌باشد. بنابراین

$$f(۰) = ۰^۴ + ۰ + ۱ = ۱, \qquad f(۱) = ۱^۴ + ۱ + ۱ = ۰,$$
$$f(۲) = ۲^۴ + ۲ + ۱ = ۱.$$

چندجمله‌ای $x^۳ + x^۲ + ۱ \in \mathbb{Z}_۳(x)$ تابع $g : \mathbb{Z}_۳ \to \mathbb{Z}_۳$ با ضابطه

$$g(۰) = ۰^۳ + ۰^۲ + ۱ = ۱, \qquad g(۱) = ۱^۳ + ۱^۲ + ۱ = ۰,$$
$$g(۲) = ۲^۳ + ۲^۲ + ۱ = ۱$$

را القاء می‌کند. بنابراین f و g روی $\mathbb{Z}_۳$ برابرند[۶]، گرچه که توسط چندجمله‌ایهای متفاوتی در $\mathbb{Z}_۳[x]$ القاء شده‌اند. با وجود این که تفاوت بین یک چندجمله‌ای و تابع چندجمله‌ای القاء شده توسط آن واضح است امّا نمادگذاری رایج در مورد آنها کاملاً مبهم است. برای مثال با گزاره‌هایی مانند $f(x) = x^۲ - ۳x + ۲$ برخورد خواهیم کرد که برحسب متن ممکن است چندجمله‌ای $x^۲ - ۳x + ۲ \in R[x]$ و یا ضابطه تابع القایی $f : R \to R$ را نشان دهد. در اینجا نماد x به دو طریق مختلف بکار رفته است. در چندجمله‌ای $x^۲ - ۳x + ۲$، x یک مجهول (عنصر متعالی) از حلقه $R[x]$ است[۷]. اما در تابع چندجمله‌ای $f : R \to R$، نماد x به عنوان یک متغیر بکار رفته است تا ضابطه تابع را توصیف کند. گرچه که استفاده از دو نماد متفاوت برای دو مفهوم "مجهول" و "متغیر" ممکن است مناسبت‌تر باشد، امّا استفاده همزمان از x برای هر دو مورد چنان متداول است که بهتر است شما نیز به آن عادت کنید.

استفاده از نماد یکسان برای هر دو مفهوم چندجمله‌ای و تابع القاء شده توسط آن روی بیان ریاضی ما نیز تأثیر می‌گذارد. به عنوان نمونه، می‌گوئیم "مقدار چندجمله‌ای $۳x^۲ - ۵x + ۴$ را در $x = ۲$ به‌دست آورید" یا "$x = ۲$ را در $۳x^۲ - ۵x + ۴$ جایگذاری کنید" در حالی که منظور واقعی ما این است که $f(۲)$ را بیابید جایی که f تابع القاء شده توسط چندجمله‌ای $۳x^۲ - ۵x + ۴$ باشد.

۶) بخاطر آورید که دو تابع f و g برابرند اگر برای هر r در دامنه آنها $f(r) = g(r)$.

۷) برای اطلاعات بیشتر پیوست چ را ملاحظه کنید.

درستی یا غلطی برخی گزاره‌ها بستگی به این دارد که آیا x به عنوان یک مجهول و یا به عنوان یک متغیر در نظر گرفته شود. برای نمونه، در حلقه $R[x]$، که در آن x یک مجهول است (عنصر بخصوصی از حلقه)، گزاره $x^۲ - ۳x + ۲ = ۰$ *غلط* است، زیرا به موجب قضیه چ.۴ از پیوست چ، یک چندجمله‌ای صفر است اگر و تنها اگر همه ضرایب آن صفر باشد. امّا وقتی که x یک متغیر باشد وضعیت متفاوت است. به عنوان مثال در مورد تابع چندجمله‌ای $f(x) = x^۲ - ۳x + ۲$، این یک سؤال کاملاً منطقی است که کدام عناصر R تحت تابع f به ۰ نگاشته می‌شوند، یعنی به ازای چه مقادیری از متغیر x، $x^۲ - ۳x + ۲ = ۰$. به خاطر داشتن این که گزاره‌هایی که درباره متغیر x صحبت می‌کنند در یک حلقه R رخ می‌دهند در حالی که گزاره‌هایی که درباره مجهول x هستند در یک حلقه چندجمله‌ایهای $R[x]$ رخ می‌دهند می‌تواند کمکی در این زمینه باشد.

سؤالاتی درباره تحویل‌پذیری یک چندجمله‌ای بعضاً با در نظرگرفتن تابع چندجمله‌ای آنها قابل جواب دادن است. کلید این کار درک و تحلیل مفهوم یک "ریشه" است.

تعریف. فرض کنید R یک حلقه باشد و $f(x) \in R[x]$. عنصر a از حلقه R یک **ریشه** چندجمله‌ای $f(x)$ نامیده می‌شود اگر $f(a) = ۰_R$، یعنی اگر تابع القایی $f : R \to R$، a را به ۰_R بنگارد.

مثال ۱۲.۴. ریشه‌های چندجمله‌ای $f(x) = x^۲ - ۳x + ۲ \in \mathbb{R}[x]$ مقادیری از متغیر x هستند که برای آنها $f(x) = ۰$ است، یعنی جوابهای $x^۲ - ۳x + ۲ = ۰$. به سادگی می‌توان دید که این ریشه‌ها ۱ و ۲ هستند.

مثال ۱۳.۴. چندجمله‌ای $x^۲ + ۱ \in \mathbb{R}[x]$ دارای هیچ ریشه‌ای در $\mathbb{R}$ نیست زیرا هیچ جواب حقیقی برای معادله $x^۲ + ۱ = ۰$ وجود ندارد. با این حال اگر $x^۲ + ۱$ به عنوان یک چندجمله‌ای در $\mathbb{C}[x]$ در نظرگرفته شود در این صورت دارای دو ریشه i و $-i$ است زیرا اینها جوابهای معادلهٔ $x^۲ + ۱ = ۰$ در $\mathbb{C}$ هستند.

همانگونه که در مثال‌های قبلی نشان داده شد، هر پرسشی درباره ریشه‌های چندجمله‌ایها دقیقاً پرسشی درباره جوابهای معادلات چندجمله‌ای است. چنین پرسش‌هایی قسمت عمده‌ای از جبر کلاسیک و جبر مدرن را تشکیل می‌دهد و ما مکرراً به آنها رجوع خواهیم کرد. با این حال، در حال

حاضر روی موضوعاتی مربوط به حل‌پذیری در $\mathbb{F}[x]$ تمرکز می‌کنیم جایی که $\mathbb{F}$ یک میدان است.

قضیه ۱۱.۴ (قضیه باقیمانده). فرض کنید $\mathbb{F}$ یک میدان باشد، $f(x) \in \mathbb{F}[x]$ و $a \in \mathbb{F}$. باقیمانده تقسیم $f(x)$ بر چندجمله‌ای $x - a$ برابر $f(a)$ است.

این قضیه بیان می‌کند که به عنوان مثال باقیمانده تقسیم $f(x) = x^۳ - ۴x^۲ + ۳x + ۴$ بر $x - ۲$ برابر $f(۲) = ۲^۳ - ۴ \times ۲^۲ + ۳ \times ۲ + ۵ = ۳$ است که می‌توانید آن را با یک تقسیم معمولی امتحان کنید. برای یافتن باقیمانده تقسیم $f(x)$ بر $x + ۱$ توجه کنید که $x + ۱ = x - (-۱)$. بنابراین باقیمانده برابر $f(-۱) = (-۱)^۳ - ۴(-۱)^۲ + ۳(-۱) + ۵ = -۳$ است.

برهان قضیه ۱۱.۴. به موجب الگوریتم تقسیم، $f(x) = (x - a)q(x) + r(x)$ که در آن باقیمانده $r(x)$ یا $۰_{\mathbb{F}}$ است یا دارای درجه کمتر از مقسوم‌علیه $x - a$ است. بنابراین $\deg r(x) = ۰$ یا $r(x) = ۰_{\mathbb{F}}$. در هر حال $r(x) = c$ برای برخی $c \in \mathbb{F}$. بنابراین $f(x) = (x - a)q(x) + c$ و لذا $f(a) = (a - a)q(a) + c = ۰_{\mathbb{F}} + c$. ■

فرض کنید $\mathbb{F}$، $f(x)$ و a همانند قضیه باقیمانده باشند. در این صورت $(x - a)$ یک عامل چندجمله‌ای $f(x)$ است اگر و تنها اگر باقیمانده $f(x)$ بر $x - a$ صفر باشد، یعنی اگر و تنها اگر $f(a) = ۰_{\mathbb{F}}$. پس قضیه زیر اثبات شده است:

قضیه ۱۲.۴ (قضیه عامل). فرض کنید $\mathbb{F}$ یک میدان، $f(x) \in \mathbb{F}[x]$ و $a \in \mathbb{F}$، در این صورت a یک ریشه چندجمله‌ای $f(x)$ است اگر و تنها اگر $x - a$ یک عامل $f(x)$ در $\mathbb{F}[x]$ باشد.

مثال ۱۴.۴. برای نشان دادن این که $x^۷ - x^۵ + ۲x^۴ - ۳x^۳ - x + ۲$ در $\mathbb{Q}[x]$ تحویل‌پذیر است، توجه کنید که ۱ یک ریشه این چندجمله‌ای است. بنابراین $x - ۱$ یک عامل است.

نتیجه ۱۳.۴. فرض کنید $\mathbb{F}$ یک میدان و $f(x)$ یک چندجمله‌ای غیرصفر از درجه n در $\mathbb{F}[x]$ باشد. در این صورت $f(x)$ دارای حداکثر n ریشه در $\mathbb{F}$ است.

این نتیجه برای دامنه‌های صحیح نیز درست است (تمرین ۲۱) امّا برای حلقه‌های دیگر، حتی

حلقه‌های تقسیمی، ممکن است غلط باشد (تمرین ۱۷ این بخش و همچنین تمرین ۳۱ (ت) در بخش ۱.۳ را ملاحظه کنید).

برهان نتیجه ۱۳.۴. اثبات به وسیله استقراء روی درجه n است. اگر $n = 0$ در این صورت $f(x)$ یک چندجمله‌ای ثابت غیرصفر است و بنابراین دارای هیچ ریشه‌ای نیست لذا قضیه برای $n = 0$ درست است.

به طور استقرایی فرض کنید که نتیجه برای همه چندجمله‌ای‌های از درجه $k - 1$ درست است و فرض کنید $\deg f(x) = k$. اگر $f(x)$ دارای هیچ ریشه‌ای در $\mathbb{F}$ نباشد در این صورت حکم برقرار است. اگر $f(x)$ دارای یک ریشه $a \in \mathbb{F}$ باشد در این صورت به موجب قضیه عامل $f(x) = (x - a)g(x)$. اگر $c \in \mathbb{F}$ هر ریشه $f(x)$ به‌جز a باشد در این صورت $0_{\mathbb{F}} = f(c) = (c - a)g(c)$. چون $c - a \neq 0$ و $\mathbb{F}[x]$ یک دامنه صحیح است بایستی $g(c) = 0_{\mathbb{F}}$. بنابراین تنها ریشه‌های $f(x)$ در $\mathbb{F}$، a و ریشه‌های $g(x)$ می‌باشد. به موجب قضیه ۱.۴، $k = \deg f(x) = \deg(x - a) + \deg g(x) = 1 + \deg g(x)$، بنابراین $\deg g(x) = k - 1$. به موجب فرض استقراء $g(x)$ دارای حداکثر $k - 1$ ریشه در $\mathbb{F}$ است. بنابراین حکم برای $n = k$ و در نتیجه به موجب استقراء برای هر n برقرار است. ■

نتیجه ۱۴.۴. فرض کنید $\mathbb{F}$ یک میدان باشد و $f(x) \in \mathbb{F}[x]$ با $\deg f(x) \geq 2$.

(۱) اگر $f(x)$ در $\mathbb{F}[x]$ تحویل‌ناپذیر باشد در این صورت $f(x)$ دارای هیچ ریشه‌ای در $\mathbb{F}$ نیست.

(۲) اگر $f(x)$ دارای درجه ۲ یا ۳ باشد و هیچ ریشه‌ای در $\mathbb{F}$ نداشته باشد در این صورت $f(x)$ در $\mathbb{F}[x]$ تحویل‌ناپذیر است.

قسمت (۲) این نتیجه برای درجه ≤ 4 غلط است. برای مثال $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$ در $\mathbb{Q}[x]$ تحویل‌پذیر است و دارای هیچ ریشه‌ای در $\mathbb{Q}$ نیست.

برهان نتیجه ۱۴.۴. (۱) اگر $f(x)$ تحویل‌ناپذیر باشد، در این صورت دارای هیچ عاملی به صورت $x - a$ در $\mathbb{F}[x]$ نیست. بنابراین به موجب قضیه عامل دارای هیچ ریشه‌ای در $\mathbb{F}$ نیست.

(۲) فرض کنید $\mathbb{F}$ دارای درجه ۲ یا ۳ باشد و هیچ ریشه‌ای در $\mathbb{F}$ نداشته باشد. در این صورت $\mathbb{F}$ دارای هیچ عامل درجه اول در $\mathbb{F}[x]$ نیست زیرا هر چندجمله‌ای درجه اول $cx + d$ در $\mathbb{F}[x]$ دارای

یک ریشه یعنی $-c^{-1}d$ است. بنابراین اگر $f(x) = r(x)s(x)$، هیچکدام از $r(x)$ یا $s(x)$ دارای درجه ۱ نیست. چون $f(x)$ دارای درجه ۲ یا ۳ است، به موجب قضیه ۱.۴ یا $r(x)$ یا $s(x)$ باید دارای درجه ۰ باشد، یعنی یا $r(x)$ یا $s(x)$ یک ثابت غیرصفر است. بنابراین به موجب قضیه ۸.۴ $f(x)$ تحویل‌ناپذیر است. ■

مثال ۱۵.۴. برای نشان دادن این که $x^۳ + x + ۱$ در $\mathbb{Z}_۵[x]$ تحویل‌ناپذیر است کافی است بررسی کنید که هیچکدام از $۰, ۱, ۲, ۳, ۴ \in \mathbb{Z}_۵$ یک ریشه نیست.

این بخش را با بازگشت به نقطه‌ای که از آن شروع کردیم یعنی توابع چندجمله‌ای به پایان می‌بریم. مثال ۱۱.۴ نشان می‌دهد که دو چندجمله‌ای متفاوت در $\mathbb{F}[x]$ ممکن است تابع یکسانی را از $\mathbb{F}$ به $\mathbb{F}$ القاء کنند. نشان می‌دهیم که این در صورتی که $\mathbb{F}$ نامتناهی باشد امکان‌پذیر نیست.

نتیجه ۱۵.۴. فرض کنید $\mathbb{F}$ یک میدان نامتناهی و $f(x), g(x) \in \mathbb{F}[x]$. در این صورت $f(x)$ و $g(x)$ تابع یکسانی را از $\mathbb{F}$ به $\mathbb{F}$ القاء می‌کنند اگر و تنها اگر $f(x) = g(x)$ در $\mathbb{F}[x]$.

برهان. فرض کنید که $f(x), g(x)$ تابع یکسانی از $\mathbb{F}$ به $\mathbb{F}$ را القاء کنند. در این صورت برای هر $a \in F$، $f(a) = g(a)$ و لذا $f(a) - g(a) = ۰_{\mathbb{F}}$. این یعنی که هر عضو $\mathbb{F}$ یک ریشه چندجمله‌ای $f(x) - g(x)$ است. چون $\mathbb{F}$ نامتناهی است، به موجب نتیجه ۱۳.۴ این امکان‌پذیر نیست مگر این که $f(x) - g(x)$ چندجمله‌ای صفر باشد یعنی $f(x) = g(x)$. برعکس واضح است. ■

تمرینها

توجه: $\mathbb{F}$ یک میدان را نشان می‌دهد.

A.۱. (الف) یک چندجمله‌ای غیرصفر در $\mathbb{Z}_۲[x]$ بیابید که‌تابع صفر را روی $\mathbb{Z}_۲$ القا کند.
(ب) قسمت (الف) را برای $\mathbb{Z}_۳[x]$ انجام دهید.

۲. در هر یک از موارد زیر باقیمانده تقسیم $f(x)$ بر $g(x)$ را بیابید:

(الف) $f(x) = x^{۱۰} + x^{۶}$ و $g(x) = x - ۱$ در $\mathbb{Q}[x]$

(ب) $f(x) = ۲x^{۵} - ۳x^{۴} + x^{۳} - ۲x^{۲} + x - ۸$ و $g(x) = x - ۱۰$ در $\mathbb{Q}[x]$

(پ) $f(x) = ۱۰x^{۲۵} - ۸x^{۲۵} + ۴x^{۱۵} + ۵$ و $g(x) = x + ۱$ در $\mathbb{Q}[x]$

(ت) $f(x) = ۲x^{۵} - ۳x^{۴} + x^{۳} + ۲x + ۳$ و $g(x) = x - ۳$ در $\mathbb{Z}_{۵}[x]$

۳. تعیین کنید که آیا $h(x)$ یک عامل $f(x)$ است:

(الف) $h(x) = x + ۲$ و $f(x) = x^{۳} - ۳x^{۲} - ۴x - ۱۲$ در $\mathbb{R}[x]$

(ب) $h(x) = x - \frac{۱}{۲}$ و $f(x) = ۲x^{۴} + x^{۳} + x - \frac{۳}{۴}$ در $\mathbb{Q}[x]$

(پ) $h(x) = x + ۲$ و $f(x) = ۳x^{۵} + ۴x^{۴} + ۲x^{۳} - x^{۲} + ۲x + ۱$ در $\mathbb{Z}_{۵}[x]$

(ت) $h(x) = x - ۳$ و $f(x) = x^{۶} - x^{۳} + x - ۵$ در $\mathbb{Z}_{۷}[x]$.

۴. (الف) برای چه مقدار k، $x - ۲$ یک عامل $x^{۴} - ۵x^{۳} + ۵x^{۲} + ۳x + k$ در $\mathbb{Q}[x]$ است؟

(ب) برای چه مقدار k، $x + ۱$ یک عامل $x^{۴} + ۲x^{۳} - ۳x^{۲} + kx + ۱$ در $\mathbb{Z}_{۵}[x]$ است؟

۵. نشان دهید که $x - ۱_{\mathbb{F}}$ چندجمله‌ای $a_n x^n + \cdots + a_۲x^۲ + a_۱x + a_۰$ را می‌شمارد اگر و تنها اگر $a_۰ + a_۱ + a_۲ + \cdots + a_n = ۰_{\mathbb{F}}$.

۶. (الف) بررسی کنید که هر عضو $\mathbb{Z}_۳$ یک ریشه $x^{۳} - x \in \mathbb{Z}_۳[x]$ است.

(ب) بررسی کنید که هر عضو $\mathbb{Z}_۵$ یک ریشه $x^{۵} - x \in \mathbb{Z}_۵[x]$ است.

(پ) ریشه‌های $x^{p} - x \in \mathbb{Z}_p[x]$ (p اول) را حدس بزنید.

۷. بدون انجام هرگونه ضرب چندجمله‌ایها، قضیه عامل را بکار برید تا نشان دهید که $x^{۷} - x$ در $\mathbb{Z}_۷[x]$ به صورت $x(x-۱)(x-۲)(x-۳)(x-۵)(x-۶)$ تجزیه می‌شود.

۸. تعیین کنید آیا چندجمله‌ای داده شده تحویل‌ناپذیر است:

(الف) $x^{۲} - ۷$ در $\mathbb{R}[x]$ (ب) $x^{۲} - ۷$ در $\mathbb{Q}[x]$

(پ) $x^{۲} + ۷$ در $\mathbb{C}[x]$ (ت) $۲x^{۳} + x^{۲} + ۲x + ۲$ در $\mathbb{Z}_۵[x]$

(ث) $x^{۲} - ۹$ در $\mathbb{Z}_{۱۱}[x]$ (ج) $x^{۴} + x^{۲} + ۱$ در $\mathbb{Z}_۳[x]$

۹. همه چندجمله‌ایهای تحویل‌ناپذیر تکین از درجه ۲ در $\mathbb{Z}_۳[x]$ را فهرست کنید.

۱۰. همه توابع ممکن از $\mathbb{Z}_۳$ به $\mathbb{Z}_۳$ (۲۷ تا وجود دارند) را فهرست کنید. چه تعداد آنها پوشا

هستند؟

۱۱. عدد p را چنان بیابید که $x-۲$ یک شمارنده $x^۴+x^۳+۳x^۲+x+۱$ در $\mathbb{Z}_p[x]$ باشد.

۱۲.B. اگر $a \in F$ یک ریشه غیرصفر $c_nx^n+c_{n-۱}x^{n-۱}+\ldots+c_۱x+c_۰ \in \mathbb{F}[x]$ باشد، نشان دهید که $a^{-۱}$ یک ریشه $c_۰x^n+c_۱x^{n-۱}+\ldots+c_{n-۱}x+c_n$ است.

۱۳. (الف) اگر $f(x)$ و $g(x)$ در $\mathbb{F}[x]$ وابسته باشند، نشان دهید که دارای ریشه‌های یکسانی در $\mathbb{F}$ هستند.
(ب) اگر $f(x), g(x) \in \mathbb{F}[x]$ دارای ریشه‌های یکسانی در $\mathbb{F}$ باشند، آیا در $\mathbb{F}[x]$ وابسته‌اند؟

۱۴. (الف) فرض کنید $r, s \in \mathbb{F}$ ریشه‌های $ax^۲+bx+c \in \mathbb{F}[x]$ (با $a \neq ۰_{\mathbb{F}}$) باشند. با استفاده از قضیه عامل نشان دهید که $r+s=-a^{-۱}b$ و $rs=a^{-۱}c$.
(ب) فرض کنید $r, s, t \in \mathbb{F}$ ریشه‌های $ax^۳+bx^۲+cx+d \in \mathbb{F}[x]$ (با $a \neq ۰_{\mathbb{F}}$) باشند. نشان دهید که $r+s+t=-a^{-۱}b$، $rs+st+rt=a^{-۱}c$ و $rst=-a^{-۱}d$.

۱۵. ثابت کنید که $x^۲+۱$ در $\mathbb{Z}_p[x]$ تحویل‌پذیر است اگر و تنها اگر اعداد صحیح a و b وجود داشته باشند به قسمی که $p=a+b$ و (پیمانه p) $ab \equiv ۱$.

۱۶. فرض کنید $f(x), g(x) \in \mathbb{F}[x]$ دارای درجه $\geq n$، و $c_۰$، $c_۱$، ...، c_n عناصر متمایزی از $\mathbb{F}$ باشند. اگر $f(c_i)=g(c_i)$ برای $i=۰,۱,\ldots,n$، ثابت کنید که $f(x)=g(x)$ در $\mathbb{F}[x]$.

۱۷. یک چندجمله‌ای از درجه ۲ در $\mathbb{Z}_۶[x]$ بیابید که دارای ۴ ریشه در $\mathbb{Z}_۶$ باشد. آیا این نتیجه ۱۳.۴ را نقض می‌کند؟

۱۸. فرض کنید $\varphi : \mathbb{C} \to \mathbb{C}$ یک یکریختی حلقه‌ای باشد به قسمی که برای هر $a \in \mathbb{Q}$، $\varphi(a)=a$. فرض کنید $r \in \mathbb{C}$ یک ریشه $f(x) \in \mathbb{Q}[x]$ باشد. ثابت کنید که $\varphi(r)$ نیز یک ریشه $f(x)$ است.

۱۹. گوئیم $a \in \mathbb{F}$ **یک ریشه چندگانه** $f(x) \in \mathbb{F}[x]$ است اگر برای برخی $k \geq ۲$، $(x-a)^k$ یک عامل $f(x)$ باشد.
(الف) ثابت کنید $a \in \mathbb{F}$ یک ریشه چندگانه $f(x) \in \mathbb{F}[x]$ است اگر و تنها اگر a ریشه هر دو $f(x)$ و $f'(x)$ باشد، جایی که $f'(x)$ مشتق $f(x)$ است.

(ب) اگر $f(x) \in \mathbb{F}[x]$ نسبت به $f'(x)$ اول باشد، ثابت کنید که $f(x)$ دارای هیچ ریشه چندگانه در $\mathbb{F}$ نیست.

۲۰. فرض کنید R یک دامنه صحیح باشد. در این صورت، به موجب تمرین ۱۴ بخش ۱.۴، هرگاه مقسوم‌علیه تکین باشد، الگوریتم تقسیم برقرار است. با بکار بردن این حقیقت نشان دهید که قضایای باقیمانده و عامل در $R[x]$ برقرار است.

۲۱. اگر R یک دامنه صحیح باشد و $f(x)$ یک چندجمله‌ای غیرصفر از درجه n در $R[x]$ باشد، ثابت کنید که $f(x)$ دارای حداکثر n ریشه در R است. [راهنمایی: تمرین ۲۰]

۲۲. نشان دهید که اگر $\mathbb{F}$ یک دامنه صحیح نامتناهی باشد نتیجه ۱۵.۴ برقرار است. [راهنمایی: تمرین ۲۱ را ملاحظه کنید.]

۲۳. فرض کنید $f(x), g(x), h(x) \in \mathbb{F}[x]$ و $a \in \mathbb{F}$.

(الف) اگر $f(x) = g(x) + h(x)$ در $\mathbb{F}[x]$، نشان دهید که $f(a) = g(a) + h(a)$ در $\mathbb{F}$.

(ب) اگر $f(x) = g(x)h(x)$ در $\mathbb{F}[x]$، نشان دهید که $f(a) = g(a)h(a)$ در $\mathbb{F}$. این حقایق در چه قسمتهایی از این بخش استفاده شده بود؟

۲۴. فرض کنید a یک عنصر ثابت $\mathbb{F}$ باشد و نگاشت $\varphi_a : \mathbb{F}[x] \to \mathbb{F}$ را توسط $\varphi_a(f(x)) = f(a)$ تعریف کنید. ثابت کنید که φ_a یک همریختی حلقه‌ای پوشا است. نگاشت φ_a، یک **همریختی ارزشی** نامیده می‌شود؛ برای هر $a \in \mathbb{F}$، یک φ_a وجود دارد.

۲۵. فرض کنید T مجموعه همه توابع چندجمله‌ای از $\mathbb{F}$ به $\mathbb{F}$ باشد و نشان دهید که T با اعمال تعریف شده در حسابان یک حلقه با عضو همانی است: برای هر $r \in \mathbb{F}$،

$$(f+g)(r) = f(r) + g(r) \quad \text{و} \quad (fg)(r) = f(r)g(r).$$

[راهنمایی: برای نشان دادن این که T تحت جمع و ضرب بسته است، تمرین ۲۳ را بکار برده تا بررسی کنید که $f+g$ و fg توابع چندجمله‌ای هستند که به ترتیب توسط چندجمله‌ای‌های جمع $f(x)+g(x)$ و حاصل‌ضرب $f(x)g(x)$ القاء شده‌اند.]

۲۶. فرض کنید T حلقه توابع چندجمله‌ای از $\mathbb{Z}_2$ به $\mathbb{Z}_2$ باشد (تمرین ۲۵ را ملاحظه کنید).

(الف) نشان دهید که T یک حلقه متناهی با مقسوم‌علیه صفر است. [راهنمایی، تمرین ۱۰ را ملاحظه کنید و $f(x) = x + 1$ و $g(x) = x^2 + 2x$ را در نظر بگیرید.]

(ب) نشان دهید که T یکریخت با $\mathbb{Z}_۳[x]$ نیست. سپس تمرین ۲۷ را ملاحظه کنید.

۲۷.C اگر $\mathbb{F}$ یک میدان نامتناهی باشد، ثابت کنید که حلقه چندجمله‌ای $\mathbb{F}[x]$ یکریخت با حلقه T متشکل از همه توابع چندجمله‌ای از $\mathbb{F}$ به $\mathbb{F}$ است (تمرین ۲۵). [راهنمایی: با نظیرکردن تابع القایی هر چندجمله‌ای $f(x) \in \mathbb{F}[x]$ به آن، یک تابع $\varphi : \mathbb{F}[x] \to T$ تعریف کنید: به موجب نتیجه ۱۵.۴، φ یک به یک است.]

۲۸. فرض کنید $\varphi : \mathbb{F}[x] \to \mathbb{F}[x]$ یک یکریختی باشد به قسمی که برای هر $a \in \mathbb{F}$، $\varphi(a) = a$. نشان دهید که $f(x)$ در $\mathbb{F}[x]$ تحویل‌ناپذیر است اگر و تنها اگر $\varphi(f(x))$ تحویل‌ناپذیر باشد.

۲۹. (الف) نشان دهید که نگاشت $\varphi : \mathbb{F}[x] \to \mathbb{F}[x]$ که توسط $\varphi(f(x)) = f(x + ۱_{\mathbb{F}})$ تعریف شده است یک یکریختی است به قسمی که برای هر $a \in \mathbb{F}$، $\varphi(a) = a$.

(ب) با استفاده از تمرین ۲۸ نشان دهید که $f(x)$ در $\mathbb{F}[x]$ تحویل‌ناپذیر است اگر و تنها اگر $f(x + ۱_{\mathbb{F}})$ تحویل‌ناپذیر باشد.

۵-۴ تحویل‌ناپذیری در $\mathbb{Q}[x]$* [۸]

موضوع اصلی این بخش این است که تجزیه در $\mathbb{Q}[x]$ می‌تواند به تجزیه در $\mathbb{Z}[x]$ تحویل یابد. سپس نظریه اعداد مقدماتی می‌تواند مورد استفاده قرارگیرد تا تحویل‌ناپذیری چندجمله‌ایهای با ضرایب صحیح مورد بررسی قرارگیرد. این بخش را با خاطرنشان کردن حقیقتی که اغلب مورد استفاده قرار خواهد گرفت آغاز می‌کنیم:

اگر $f(x) \in \mathbb{Q}[x]$، در این صورت برای برخی عدد ثابت غیرصفر c، $cf(x)$ دارای ضرایب صحیح است.

برای مثال

$$f(x) = x^۵ + \frac{۲}{۳}x^۴ + \frac{۳}{۴}x^۳ - \frac{۱}{۶}$$

۸) از این بخش تنها در فصل‌های ۹، ۱۱ و ۱۵ استفاده می‌شود. در صورت تمایل می‌توان تا آن موقع این بخش را نادیده گرفت، بخش ۶.۴ مستقل از این بخش است.

را در نظر بگیرید. کوچکترین مخرج مشترک ضرایب $f(x)$، ۱۲ است، و $۱۲f(x)$ دارای ضرایب صحیح است:

$$۱۲f(x) = ۱۲[x^۵ + \frac{۲}{۳}x^۴ + \frac{۳}{۴}x^۴ + \frac{۳}{۴}x^۳ - \frac{۱}{۶}] = ۱۲x^۵ + ۸x^۴ + ۹x^۳ - ۲$$

طبق قضیه عامل، یافتن عوامل درجه اول یک چندجمله‌ای $g(x) \in \mathbb{Q}[x]$ معادل یافتن ریشه‌های $g(x)$ در $\mathbb{Q}$ است. حال برای هر ثابت غیرصفر c، $g(x)$ و $cg(x)$ دارای ریشه‌های یکسانند. وقتی c چنان انتخاب شود که $cg(x)$ دارای ضرایب صحیح باشد می‌توانیم ریشه‌های $g(x)$ را با استفاده از قضیه زیر بیابیم.

قضیه ۱۶.۴.(آزمون ریشه گویا). اگر $f(x) = a_n x^n + a_{n-۱}x^{n-۱} + \cdots + a_۱x + a_۰$ یک چندجمله‌ای با ضرایب صحیح باشد، و کسر ساده[۹] r/s (با $r \neq ۰$) یک ریشه $f(x)$ باشد، در این صورت $r|a_۰$ و $s|a_n$.

برهان. چون r/s یک ریشه $f(x)$ است، داریم

$$a_n(\frac{r^n}{s^n}) + a_{n-۱}(\frac{r^{n-۱}}{s^{n-۱}}) + \cdots + a_۱(\frac{r}{s}) + a_۰ = ۰.$$

از ضرب دو طرف در s^n، مرتب کردن مجدد و فاکتورگیری به دست می‌آوریم

$$a_n r^n + a_{n-۱}sr^{n-۱} + \cdots + a_۱s^{n-۱}r + a_۰s^n = ۰ \qquad (*)$$

$$a_۰s^n = -a_n r^n - a_{n-۱}sr^{n-۱} - \cdots - a_۱s^{n-۱}r$$

$$a_۰s^n = r[-a_n r^{n-۱} - a_{n-۱}sr^{n-۲} - \cdots - a_۱s^{n-۱}]$$

برابری آخری بیان می‌کند که r، $a_۰s^n$ را می‌شمارد. چون r/s یک کسر ساده‌است، داریم $(r,s) = ۱$. در نتیجه $(r,s^n) = ۱$ (به موجب نتیجه ۹.۱ یک عدد اول که s^n را بشمارد، s را نیز می‌شمارد). چون $r|a_۰s^n$ و $(r,s^n) = ۱$، قضیه ۵.۱ نشان می‌دهد که $r|a_۰$. استدلالی مشابه ثابت می‌کند که $s|a_n$ (تنها کافی است $(*)$ را چنان مرتب کنید که $a_n r^n$ در یک طرف و بقیه جملات در طرف دیگر قرار گیرد.) ■

۹) مترجمان: عدد گویای r/s را یک **کسر ساده** گوییم هرگاه $(r,s) = ۱$. هر عدد گویا را می‌توان به صورت یک کسر ساده نوشت.

مثال ۱۶.۴. ریشه‌های ممکن برای $f(x) = ۲x^۴ + x^۳ - ۲۱x^۲ - ۱۴x + ۱۲$ در $\mathbb{Q}$ به صورت r/s هستند جایی که r یکی از اعداد ± ۱، ± ۲، ± ۳، ± ۴، ± ۶ یا ± ۱۲ (شمارنده‌های جمله ثابت ۱۲) می‌باشد و s، $۱ \pm$ یا $۲ \pm$ (شمارنده‌های ضریب پیشرو ۲) است. بنابراین آزمون ریشهٔ گویا جستجو برای یافتن ریشه‌های $f(x)$ را به فهرست متناهی زیر از جوابهای ممکن، کاهش می‌دهد: $۱, -۱, ۲, -۲, ۳, -۳, ۴, -۴, ۶, -۶, ۱۲, -۱۲, ۱/۲, -۱/۲, ۳/۲, -۳/۲$. گرچه که وقت‌گیر است امّا می‌توان هرکدام از اینها را مستقیماً در $f(x)$ جایگذاری کرد و دید که -۳ و $۱/۲$ تنها ریشه‌های $f(x)$ در $\mathbb{Q}$ هستند[۱۰]. به موجب قضیه عامل هر دو $x + ۳ = x - (-۳)$ و $x - ۱/۲$ عامل‌های $f(x)$ هستند. با تقسیم معمولی می‌توان دید که

$$f(x) = (x + ۳)(x - \frac{۱}{۲})(۲x^۲ - ۴x - ۸).$$

فرمول درجه دوّم نشان می‌دهد که ریشه‌های $۲x^۲ - ۴x - ۸$ عبارتند از $۱ \pm \sqrt{۵}$ که هیچکدام در $\mathbb{Q}$ نیستند. بنابراین به موجب نتیجه ۱۴.۴، $۲x^۲ - ۴x - ۸$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. از اینرو ما $f(x)$ را به صورت حاصل‌ضربی از چندجمله‌ایهای تحویل‌ناپذیر در $\mathbb{Q}[x]$ تجزیه کرده‌ایم.

مثال ۱۷.۴. تنها ریشه‌های ممکن $g(x) = x^۳ + ۴x^۲ + x - ۱$ در $\mathbb{Q}$ عبارتند از ۱ و -۱ (چرا؟). بررسی کنید که هیچکدام از ۱ و -۱ یک ریشه $g(x)$ نیست. بنابراین به موجب نتیجه ۱۴.۴، $g(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

اگر $f(x) \in \mathbb{Q}[x]$، در این صورت برای یک عدد صحیح c، $cf(x)$ دارای ضرایب صحیح است. هر تجزیه $cf(x)$ در $\mathbb{Z}[x]$ منجر به یک تجزیه $f(x)$ در $\mathbb{Q}[x]$ می‌شود. بنابراین آشکار می‌شود که آزمونهای بررسی تحویل‌ناپذیری در $\mathbb{Q}[x]$ را می‌توان به بررسی چندجمله‌ایهای با ضرایب صحیح محدود کرد. البته ابتدا باید این امکان را که یک چندجمله‌ای با ضرایب صحیح در $\mathbb{Q}[x]$ قابل تجزیه‌بوده ولی در $\mathbb{Z}[x]$ تحویل‌ناپذیر باشد را رد کنیم. به منظور انجام این کار لم زیر را نیاز داریم.

لم ۱۷.۴. فرض کنید $f(x), s(x), h(x) \in \mathbb{Z}[x]$ با $f(x) = g(x)h(x)$. اگر عدد اول p

---

۱۰) یک ماشین‌حساب گرافیکی به‌طور چشمگیری مقدار محاسبات را کاهش خواهد داد. چون نمودار $y = f(x)$ محور x–ها را در ریشه‌های $f(x)$ قطع می‌کند، می‌توانید هر عددی از فهرست را که نزدیک یک نقطه تقاطع نیست حذف کنید. در این حالت نمودار نشان می‌دهد که تنها لازم است -۳، $۱/۲$ و $-۳/۲$ را امتحان کنید.

موجود باشد به قسمی که هر ضریب $f(x)$ را بشمارد، در این صورت یا p همه ضرایب $g(x)$ را می‌شمارد، یا p همه ضرایب $h(x)$ را می‌شمارد.

برهان. فرض کنید $f(x) = a_0 + a_1x + \cdots + a_kx^k$، $g(x) = b_0 + b_1x + \cdots + b_mx^m$ و $h(x) = c_0 + c_1x + \cdots + c_nx^n$. اثبات را به کمک برهان خلف انجام می‌دهیم. اگر حکم برقرار نباشد در این صورت p برخی از ضرایب $g(x)$ و برخی از ضرایب $h(x)$ را نمی‌شمارد. فرض کنید b_r اولین ضریب $g(x)$ باشد که توسط p عاد نمی‌شود، و فرض کنید c_t اولین ضریب $h(x)$ باشد که توسط p عاد نمی‌شود. در این صورت $p|b_i$ برای $i < r$ و $p|c_j$ برای $j < t$. ضریب a_{r+t} از $f(x)$ را در نظر بگیرید. چون $f(x) = g(x)b(x)$ داریم

$$a_{r+t} = b_0c_{r+t} + \cdots + b_{r-1}c_{t+1} + b_rc_t + b_{r+1}c_{t-1} + \cdots + b_{r+t}c_0$$

در نتیجه

$$b_rc_t = a_{r+t} - [b_0c_{r+t} + \cdots + b_{r-1}c_{t+1}] - [b_{r+1}c_{t-1} + \cdots + b_{r+t}c_0].$$

حال به موجب فرض $p|a_{r+t}$. همچنین p هر جمله عبارت داخل اولین کروشه را می‌شمارد زیرا r چنان انتخاب شده بود که $p|b_i$ برای هر $i < r$. به‌طور مشابه p هرجمله دومین عبارت داخل کروشه را می‌شمارد زیرا $p|c_j$ برای هر $j < t$. چون p همه جملات طرف راست را می‌شمارد، ملاحظه می‌کنیم که $p|b_rc_t$. بنابراین به موجب قضیه ۸.۱، $p|b_r$ یا $p|c_t$. امّا این ناقض این واقعیت است که هیچکدام از b_r و c_t توسط p عاد نمی‌شود. ■

قضیه ۱۸.۴. فرض کنید $f(x)$ یک چندجمله‌ای با ضرایب صحیح باشد. در این صورت $f(x)$ به صورت حاصل‌ضربی از چندجمله‌ایهایی از درجه m و n در $\mathbb{Q}[x]$ تجزیه می‌شود اگر و تنها اگر $f(x)$ به صورت حاصل‌ضربی از چندجمله‌ایهای از درجه m و n در $\mathbb{Z}[x]$ تجزیه شود.

برهان. بوضوح هر تجزیه $f(x)$ در $\mathbb{Z}[x]$ یک تجزیه در $\mathbb{Q}[x]$ است. برعکس، فرض کنید $f(x) = g(x)h(x)$ در $\mathbb{Q}[x]$. فرض کنید c و d اعداد صحیح غیرصفری باشد به قسمی که $cg(x)$ و $dh(x)$ دارای ضرایب صحیح باشد. در این صورت تساوی $cdf(x) = [cg(x)][dh(x)]$ در $\mathbb{Z}[x]$ برقرار است با $\deg cg(x) = \deg g(x)$ و $\deg dh(x) = \deg h(x)$. فرض کنید p یک شمارنده cd باشد، مثلاً $cd = pt$. در این صورت p یا همه ضرایب $cg(x)$، یا همه ضرایب $dh(x)$ را می‌شمارد. فرض کنید اولی برقرار باشد. در این صورت $cg(x) = pk(x)$ با

$k(x) \in \mathbb{Z}[x]$ و $\deg k(x) = \deg g(x)$. بنابراین $ptf(x) = cdf(x) = [cg(x)][dh(x)] = [pk(x)][dh(x)]$. با حذف p از دو طرف داریم $tf(x) = k(x)[dh(x)]$ در $\mathbb{Z}[x]$.

حال همین استدلال را با هر شمارنده اول t تکرار و آن عدد اول را از دو طرف حذف کنید. این روند را آنقدر ادامه دهید تا هر عامل اول cd حذف شود. در این صورت طرف چپ برابری، $\pm f(x)$ خواهد بود و طرف راست حاصل‌ضرب دو چندجمله‌ای در $\mathbb{Z}[x]$ می‌باشد، یکی با درجه برابر درجه $g(x)$ و یکی با درجه برابر درجه $h(x)$. ■

مثال ۱۸.۴. ادعا می‌کنیم که $f(x) = x^4 - 5x^2 + 1$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است. اثبات توسط برهان خلف انجام می‌شود. در صورت تحویل‌پذیر بودن، $f(x)$ می‌تواند به صورت حاصل‌ضربی از دو چندجمله‌ای غیر ثابت در $\mathbb{Q}[x]$ تجزیه شود. اگر یکی از این عوامل دارای درجه ۱ باشد، در این صورت $f(x)$ دارای یک ریشه در $\mathbb{Q}$ است. امّا آزمون تست گویا نشان می‌دهد که $f(x)$ دارای هیچ ریشه‌ای در $\mathbb{Q}$ نیست. (تنها احتمالات ± 1 است و هیچکدام یک ریشه نیست.) بنابراین اگر $f(x)$ تحویل‌پذیر باشد، به موجب قضیه ۱.۴، تنها تجزیه ممکن به صورت حاصل‌ضربی از دوچندجمله‌ای درجه دوم است. در این حالت قضیه ۱۸.۴ نشان می‌دهد که یک چنین تجزیه‌ای در $\mathbb{Z}[x]$ وجود دارد. بعلاوه به موجب تمرین ۱۰، یک تجزیه به صورت حاصل‌ضرب چندجمله‌ایهای درجه دوّم و تکین در $\mathbb{Z}[x]$ وجود دارد، مثلاً

$$(x^2 + ax + b)(x^2 + 2x + d) = x^4 - 5x^2 + 1$$

با $a, b, c, d \in \mathbb{Z}$. با محاسبه حاصل‌ضرب طرف چپ داریم

$$x^4 + (a + c)x^3 + (ac + b + d)x^2 + (bc + ad)x + bd$$
$$= x^4 + 0x^3 - 5x^2 + 0x + 1$$

چندجمله‌ایهای برابر دارای ضرایب برابر هستند؛ بنابراین

$$a + c = 0 \qquad ac + b + d = -5 \qquad bc + ad = 0 \qquad bd = 1$$

چون $a + c = 0$، داریم $a = -c$، بنابراین

$$-5 = ac + b + d = -c^2 + b + d,$$

یا به‌طور معادل

$$۵ = c^۲ - b - d.$$

امّا $bd = ۱$ در $\mathbb{Z}$ نتیجه می‌دهد که $b = d = ۱$ و یا $b = d = -۱$، و لذا تنها دو احتمال

$$۵ = ۲^۲ - ۱ - ۱ \qquad \text{یا} \qquad ۵ = c^۲ + ۱ + ۱$$
$$۷ = c^۲ \qquad\qquad ۳ = c^۲$$

وجود دارد. چون هیچ یک از ۳ و ۷ مربع کامل نیست لذا هیچ تجزیه‌ای از $f(x)$ به صورت حاصل‌ضربی از چندجمله‌ایهای درجه دوّم در $\mathbb{Z}[x]$ و بنابراین در $\mathbb{Q}[x]$ وجود ندارد. پس $f(x)$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است.

روش‌های کارآمد مثال قبل، در مورد چندجمله‌ای‌های با درجات بالاتر کمتر مؤثر است، زیرا کنترل روش‌مند دستگاه معادلاتی که باید حل شود پیچیده و مشکل است. با این حال تحویل‌ناپذیری برخی چند جمله‌ایهای با درجه بالا به سادگی توسط قضیه زیر اثبات می‌شود.

قضیه ۱۹.۴ (محک آیزنشتاین)[۱۱]. فرض کنید $f(x) = a_n x^n + \cdots + a_۱ x + a_۰$ یک چندجمله‌ای غیرثابت با ضرایب صحیح باشد. اگر عدد اول p موجود باشد به قسمی که p هر کدام از $a_۰$، $a_۱$، ...، $a_{n-۱}$ را بشمارد امّا a_n را نشمارد و $p^۲$، $a_۰$ را نشمارد در این صورت $f(x)$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است.

برهان. اثبات توسط برهان خلف انجام می‌شود. اگر $f(x)$ تحویل‌پذیر باشد در این صورت به موجب قضیه ۱۸.۴ می‌توان $f(x)$ را به صورت مثلاً

$$f(x) = (b_۰ + b_۱ x + \cdots + b_r x^r)(c_۰ + c_۱ x + \cdots + c_s x^s)$$

در $\mathbb{Z}[x]$ تجزیه کرد که در آن $b_i, c_j \in \mathbb{Z}$، $r \geq ۱$ و $s \geq ۱$. توجه کنید که $a_۰ = b_۰ c_۰$. به موجب فرض، $p|a_۰$ و بنابراین طبق قضیه ۸.۱، $p|b_۰$ یا $p|c_۰$، مثلاً گیریم $p|b_۰$. چون $a_۰$، $p^۲$ را عاد نمی‌کند، می‌بینیم که $c_۰$ توسط p عاد نمی‌شود. همچنین داریم $a_n = b_r c_s$. در نتیجه p، b_r را عاد نمی‌کند (در غیر این‌صورت a_n باید به وسیله p عاد شود که متناقض با فرض است). ممکن است b_i دیگری نیز موجود باشد که آن هم به وسیله p عاد نشود. فرض کنید k اولین نمایه‌ای باشد طوری که b_k توسط p عاد نمی‌شود. در این صورت $۰ < k \leq r < n$ و

(۱۱) Eisenstein's criterion

$$p|b_i \quad \text{برای} \quad i<k \quad \text{و} \quad p\nmid b_k.$$

به موجب قوانین ضرب چندجمله‌ایها

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0,$$

لـــذا

$$b_kc_0 = a_k - b_0c_k - b_1c_{k-1} - \cdots - b_{k-1}c_1.$$

چون $p|a_k$ و $p|b_i$ برای $i<k$، لذا p هرجمله طرف راست این برابری را عاد می‌کند. بنابراین $p|b_kc_0$. بنابر قضیه ۸.۱، p بایستی b_k یا c_0 را عاد کند، ولی این با این حقیقت که هیچکدام از b_k و c_0 توسط b عاد نمی‌شود در تناقض است. بنابراین $f(x)$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است. ■

مثال ۱۹.۴. به موجب محک آیزنشتاین چندجمله‌ای $x^{17}+6x^{13}-15x^4+3x^2-9x+12$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است با $p=3$.

مثال ۲۰.۴. به موجب محک آیزنشتاین چندجمله‌ای x^9+5 تحویل‌ناپذیر در $\mathbb{Q}[x]$ است با $p=5$. به طور مشابه x^n+5 تحویل‌ناپذیر در $\mathbb{Q}[x]$ است برای هر $n\geq 1$. بنابراین

چندجمله‌ایهای تحویل‌ناپذیر از هر درجه ممکن در $\mathbb{Q}[x]$ وجود دارد.

گرچه محک آیزنشتاین بسیار کارآمد است، با این حال چندجمله‌ایهای زیادی وجود دارد که این محک برای آنها کاربرد ندارد. در چنین حالتی یافتن راهکارهای دیگری ضروری است. یکی از این راهکارها کاهش یک چندجمله‌ای به پیمانه p به مفهوم زیر می‌باشد. فرض کنید p یک عدد اول مثبت باشد. برای هر عدد صحیح a، فرض کنید $[a]$ کلاس همنهشتی a در $\mathbb{Z}_p$ را نشان دهد. اگر $f(x)=a_kx^k+\cdots+a_1x+a_0$ یک چندجمله‌ای با ضرایب صحیح باشد، فرض کنید $\bar{f}(x)$ چندجمله‌ای $[a_k]x^k+\cdots+[a_1]x+[a_0]$ در $\mathbb{Z}_p[x]$ را نشان دهد. به عنوان مثال اگر $f(x)=2x^4-3x^2+5x+7$ در $\mathbb{Z}[x]$، در این صورت در $\mathbb{Z}_3[x]$،

$$\begin{aligned}\bar{f}(x) &= [2]x^4-[3]x^2+[5]x+[7]\\ &= [2]x^4-[0]x^2+[2]x+[1] = [2]x^4+[2]x+[1].\end{aligned}$$

توجه کنید که $f(x)$ و $\bar{f}(x)$ دارای درجه یکسان هستند. در واقع این امر در صورتی که ضریب پیشرو $f(x)$ توسط p عاد نشود همواره برقرار است (یعنی وقتی ضریب پیشرو $\bar{f}(x)$ کلاس صفر در $\mathbb{Z}_p$ نباشد).

قضیه ۲۰.۴. فرض کنید $f(x) = a_k x^k + \cdots + a_1 x + a_0$ یک چندجمله‌ای با ضرایب صحیح باشد و p عدد اول مثبتی باشد که a_k را عاد نکند. اگر $\bar{f}(x)$ تحویل‌ناپذیر در $Z_p[x]$ باشد، در این صورت $f(x)$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است.

برهان. به خلاف فرض کنید که $f(x)$ تحویل‌پذیر در $\mathbb{Q}[x]$ باشد. در این صورت به موجب قضیه ۱۸.۴، $f(x) = g(x)h(x)$ که در آن $g(x)$ و $h(x)$ چندجمله‌ایهای غیرثابت در $\mathbb{Z}[x]$ هستند. چون p ضریب پیشرو a_k از $f(x)$ را عاد نمی‌کند، p نمی‌تواند ضریب‌های پیشرو $g(x)$ یا $h(x)$ (که حاصل‌ضربشان a_k است) را عاد کند. در نتیجه $\deg \bar{g}(x) = \deg g(x)$ و $\deg \bar{h}(x) = \deg h(x)$. به‌ویژه هیچکدام از $\bar{g}(x)$ و $\bar{h}(x)$ یک چندجمله‌ای ثابت در $\mathbb{Z}_p[x]$ نیست.

بررسی کنید که تساوی $f(x) = g(x)h(x)$ در $\mathbb{Z}[x]$ نتیجه می‌دهد که $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ در $\mathbb{Z}_p[x]$ (تمرین ۱۹). این امر تحویل‌ناپذیری $f(x)$ در $\mathbb{Z}_p[x]$ را نقض می‌کند. بنابراین $f(x)$ بایستی تحویل‌ناپذیر در $\mathbb{Q}[x]$ باشد. ■

مفیدبودن قضیه ۲۰.۴ به این حقیقت بستگی دارد که: برای هر عدد صحیح غیرمنفی k، تنها تعداد متناهی چندجمله‌ای از درجه k در $\mathbb{Z}_p[x]$ وجود دارد (تمرین ۱۷). بنابراین از جنبه نظری با امتحان تعداد متناهی عوامل ممکن، همواره امکان تعیین این که آیا یک چندجمله‌ای مفروض در $\mathbb{Z}_p[x]$ تحویل‌ناپذیر است وجود دارد. این امر را اغلب برحسب اندازه p و درجه $f(x)$ می‌توان در یک مدت زمان معقول انجام داد.

مثال ۲۱.۴. برای نشان دادن تحویل‌ناپذیری $f(x) = x^5 + 8x^4 + 3x^3 + 4x + 7$ در $\mathbb{Q}[x]$، ما مسئله را به پیمانه ۲ کاهش می‌دهیم. در $\mathbb{Z}_2[x]$، $\bar{f}(x) = x^5 + x^3 + 1$[۱۲]. به‌سادگی دیده می‌شود که $\bar{f}(x)$ دارای هیچ ریشه‌ای در $\mathbb{Z}_2$ نیست و بنابراین دارای هیچ عامل درجه اول در $\mathbb{Z}_2[x]$ نیست. تنها چندجمله‌ایهای درجه دوّم در $\mathbb{Z}_2[x]$ عبارتند از x^2، $x^2 + x$، $x^2 + 1$ و $x^2 + x + 1$.

۱۲) وقتی امکان اشتباه نباشد ما کروشه‌ها را برای عناصر $\mathbb{Z}_2$ حذف می‌کنیم.

با استفاده از تقسیم معمولی می‌توانید نشان دهید که هیچ کدام از آنها یک عامل $\bar{f}(x)$ نیست. سرانجام، $\bar{f}(x)$ نمی‌تواند یک عامل درجه ۳ یا ۴ داشته باشد (در غیر این صورت عامل دیگر باید دارای درجه ۲ یا ۱ باشد که غیر ممکن است). بنابراین $\bar{f}(x)$ تحویل‌ناپذیر در $\mathbb{Z}_2[x]$ است. بنابراین $f(x)$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است.

هشدار: اگر یک چندجمله‌ای در $\mathbb{Z}[x]$ به یک چندجمله‌ای تحویل‌پذیر در $\mathbb{Z}_p[x]$ به پیمانه p کاهش یابد، در این صورت هیچ نتیجه‌ای از قضیه ۲۰.۴ نمی‌توان حاصل کرد. متأسفانه حتی با وجود تحویل‌ناپذیر بودن $f(x)$ در $\mathbb{Q}[x]$ ممکن است تعداد زیادی p وجود داشته باشد که برای آنها کاهش $f(x)$ در $\mathbb{Z}_p[x]$ تحویل‌پذیر باشد. بنابراین بکار بردن قضیه ۲۰.۴ ممکن است از آنچه که در ابتدا به نظر می‌رسید زمان بیشتری ببرد.

تمرینها

۱.A. آزمون ریشه‌گویا را بکار برید تا هرکدام از چندجمله‌ایهای زیر را به صورت حاصل‌ضربی از چندجمله‌ایهای تحویل‌ناپذیر در $\mathbb{Q}[x]$ بنویسید:

(الف) $-x^4+x^3+x^2+x+2$ (ب) $x^5+4x^4+x^3-x^2$

(پ) $3x^5+2x^4-7x^3+2x^2$ (ت) $2x^4-5x^3+3x^2+4x-6$

(ث) $2x^4+7x^3+5x^2+7x+3$ (ج) $6x^4-31x^3+25x^2+33x+7$

۲. نشان دهید که برای هر عدد اول مثبت p، $\sqrt{p}$ اصم است. [راهنمایی، ریشه‌های x^2-p کدام است؟ آیا این اثبات را به روش ارائه شده در تمرین‌های ۲۰ و ۱۱ بخش ۳.۱ ترجیح می‌دهید؟]

۳. اگر یک چندجمله‌ای با ضرایب صحیح تکین دارای یک ریشه در $\mathbb{Q}$ باشد، نشان دهید که این ریشه باید یک عدد صحیح باشد.

۴. همانند مثال بعد از قضیه ۱۸.۴، نشان دهید هر یک از چندجمله‌ایهای زیر تحویل‌ناپذیر در $\mathbb{Q}[x]$ است:

(الف) x^4+2x^3+x+1 (ب) x^4-2x^2+8x+1.

۵. محک آیزنشتاین را بکار برید تا نشان دهید که هر یک از چندجمله‌ایهای زیر تحویل‌ناپذیر در $\mathbb{Q}[x]$ است:

(الف) $x^5 - 4x + 22$ (ب) $10 - 15x + 25x^2 - 7x^3$

(پ) $5x^{11} - 6x^4 + 12x^3 + 36x - 6$.

۶. نشان دهید که تعداد نامتناهی عدد صحیح k وجود دارد به قسمی که $x^9 + 12x^5 - 21x + k$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است.

۷. در هر یک از موارد زیر با یافتن یک عدد اوّل p به طوری که چندجمله‌ای $f(x)$ در $\mathbb{Z}_p[x]$ تحویل‌ناپذیر باشد نشان دهید که $f(x)$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است،

(الف) $7x^3 + 6x^2 + 4x + 6$ (ب) $9x^4 + 4x^3 - 3x + 7$.

۸. مثالی از یک چندجمله‌ای $f(x) \in \mathbb{Z}[x]$ و یک عدد اول p ارائه دهید به‌طوری که $f(x)$ تحویل‌پذیر در $\mathbb{Q}[x]$ باشد امّا $\bar{f}(x)$ تحویل‌ناپذیر در $\mathbb{Z}_p[x]$ باشد. آیا این قضیه ۲۰.۴ را نقض می‌کند؟

۹. مثالی از یک چندجمله‌ای در $\mathbb{Z}[x]$ ارائه دهید که در $\mathbb{Q}[x]$ تحویل‌ناپذیر است امّا وقتی به پیمانه‌های ۲، ۳، ۴ و ۵ کاهش می‌یابد تجزیه می‌شود.

۱۰. اگر یک چندجمله‌ای با ضرایب صحیح تکین به صورت حاصل‌ضربی از چندجمله‌ایهای با درجات m و n در $\mathbb{Z}[x]$ تجزیه شود، ثابت کنید که قابل تجزیه به صورت حاصل‌ضربی از چندجمله‌ایهای تکین با درجات m و n در $\mathbb{Z}[x]$ نیز هست.

۱۱.B. ثابت کنید که $30x^n - 91$ (که در آن $n \in \mathbb{Z}$ و $n > 1$) دارای هیچ ریشه‌ای در $\mathbb{Q}$ نیست.

۱۲. فرض کنید $\mathbb{F}$ یک میدان باشد و $f(x) \in \mathbb{F}[x]$. اگر $c \in \mathbb{F}$ و $f(x+c)$ تحویل‌ناپذیر در $\mathbb{F}[x]$ باشد، ثابت کنید که $f(x)$ تحویل‌ناپذیر در $\mathbb{F}[x]$ است. [راهنمایی: عکس نقیض آن را ثابت کنید.]

۱۳. تحویل‌ناپذیری $f(x+1)$ در $f(x) = x^4 + 4x + 1$ را با نشان دادن تحویل‌ناپذیری $\mathbb{Q}[x]$ به کمک محک آیزنشتاین و بکار بردن تمرین ۱۲ ثابت کنید.

۱۴. ثابت کنید که $f(x) = x^4 + x^3 + x^2 + x + 1$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است. [راهنمایی: راهنمایی تمرین ۲۰ را با $p = 5$ بکار برید.]

۱۵. فرض کنید $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ یک چندجمله‌ای با ضرایب صحیح باشد. اگر p یک عدد اول باشد به طوری که $p|a_1$، $p|a_2$، ...، $p|a_n$ امّا $p \nmid a_0$

و $a_n \nmid p^2$. ثابت کنید که $f(x)$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است. [راهنمایی: در $x^n f(1/x)$ قرار دهید $y = 1/x$. به موجب قضیه ۱۹.۴، چندجمله‌ای حاصل تحویل‌ناپذیر است.]

۱۶. با مثال نشان دهید که این گزاره غلط است: اگر $f(x) \in \mathbb{Z}[x]$ و عدد اول p وجود نداشته باشد که در مفروضات قضیه ۱۹.۴ صدق کند، در این صورت $f(x)$ تحویل‌پذیر در $\mathbb{Q}[x]$ است.

۱۷. نشان دهید که تعداد $n^{k+1} - n^k$ چندجمله‌ای از درجه k در $\mathbb{Z}_n[x]$ وجود دارد.

۱۸. کدام یک از چندجمله‌ایهای زیر تحویل‌ناپذیر در $\mathbb{Q}[x]$ است:

(الف) $x^4 - x^2 + 1$ (ب) $x^4 + x + 1$

(پ) $x^5 + 4x^4 + 2x^3 + 2x^2 - x + 5$ (ت) $x^5 + 5x^2 + 4x + 7$

۱۹. اگر $f(x) = a_n x^n + \cdots + a_1 x + a_0$، $g(x) = b_m x^m + \cdots + b_1 x + b_0$ و $h(x) = c_s x^s + \cdots + c_1 x + c_0$ چندجمله‌ایهای در $\mathbb{Z}[x]$ باشند به قسمی که $f(x) = g(x)h(x)$، نشان دهید که در $\mathbb{Z}_n[x]$، $f(x) = \bar{g}(x)\bar{h}(x)$. همچنین تمرین ۱۷ بخش ۱.۴ را ملاحظه کنید.

۲۰.C. ثابت کنید که برای عدد اول p، $f(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ تحویل‌ناپذیر در $\mathbb{Q}[x]$ است. [راهنمایی: $(x-1)f(x) = x^p - 1$، بنابراین $f(x) = (x^p - 1)/(x-1)$ و $f(x+1) = [(x+1)^p - 1]/x$. به وسیله قضیه دوجمله‌ای (پیوست ث)، $(x+1)^p$ را بسط دهید و توجه کنید که وقتی $0 < k$ آنگاه p، $\binom{p}{k}$ را می‌شمارد. محک آیزنشتاین را بکار برید تا نشان دهید که $f(x+1)$ تحویل‌ناپذیر است؛ تمرین ۱۲ را بکار برید.]

۶-۴ تحویل‌ناپذیری در $\mathbb{R}[x]$ و $\mathbb{C}[x]$ [۱۳]

برخلاف وضعیتی که در $\mathbb{Q}[x]$ داشتیم، این امکان وجود دارد تا توصیف صریحی از همه چندجمله‌ایهای تحویل‌ناپذیر در $\mathbb{R}[x]$ و $\mathbb{C}[x]$ را چنان ارائه دهیم که بدون نیاز به هیچ‌گونه آزمون یا محکی تحویل‌ناپذیری یک چندجمله‌ای در آنها را فوراً تعیین کنیم. اینها نتیجه‌ای از قضیه زیر است که اولین بار توسط

۱۳) از این بخش تنها در فصل‌های ۹ و ۱۱ استفاده می‌شود، لذا می‌توانید مطالعه آن را تا فصل‌های مذکور به تعویق اندازید.

گوس[۱۴] در ۱۷۹۹ ثابت شد:

قضیه ۲۱.۴. (قضیه اساسی جبر) هرچندجمله‌ای غیرثابت در $\mathbb{C}[x]$ دارای یک ریشه در $\mathbb{C}$ است.

در اصطلاح علمی، این قضیه بعضاً با گفتن این که میدان $\mathbb{C}$ **بسته جبری** است بیان می‌شود. تمام اثباتهای شناخته‌شده این قضیه به‌طور قابل ملاحظه‌ای به حقایقی از آنالیز و یا نظریه توابع یک متغیره مختلط بستگی دارد. به این دلیل، ما تنها برخی از استلزامات قضیه اساسی جبر در مورد تحویل‌ناپذیری در $\mathbb{C}[x]$ و $\mathbb{R}[x]$ را در نظر خواهیم گرفت. برای دیدن برهانی از این قضیه، مک کوی[۱۵] و برگر[۱۶] [۶] یا هانگرفورد[۱۷] [۷] را ملاحظه کنید.

نتیجه ۲۲.۴. یک چندجمله‌ای در $\mathbb{C}[x]$ تحویل‌ناپذیر است اگر و تنها اگر دارای درجه ۱ باشد.

برهان. به موجب قضیه ۲۱.۴، یک چندجمله‌ای $f(x)$ از درجه ≥ 2 در $\mathbb{C}[x]$ دارای یک ریشه در $\mathbb{C}$ است و بنابراین به موجب قضیه عامل دارای یک عامل درجه اول است. لذا $f(x)$ تحویل‌پذیر در $\mathbb{C}[x]$ است، و هر چندجمله‌ای تحویل‌ناپذیر در $\mathbb{C}[x]$ باید دارای درجه ۱ باشد. بالعکس، هرچندجمله‌ای درجه اول تحویل‌ناپذیر است (قضیه ۸.۴). ■

نتیجه ۲۳.۴. هرچندجمله‌ای غیرثابت $f(x)$ از درجه n در $\mathbb{C}[x]$ را می‌توان به صورت $c(x-a_1)(x-a_2)\cdots(x-a_n)$ نوشت که در آن $c, a_1, a_2, \ldots, a_n \in \mathbb{C}$. این تجزیه به‌جز در ترتیب عوامل یکتاست.

برهان. به موجب قضیه ۱۰.۴، $f(x)$ حاصل‌ضربی از چندجمله‌ایهای تحویل‌ناپذیر در $\mathbb{C}[x]$ است. به موجب نتیجه ۲۲.۴، هرکدام از این چندجمله‌ایها دارای درجه ۱ است و به موجب قضیه

---

۱۴) Gauss
۱۵) McCoy
۱۶) Berger
۱۷) Hungerford

۱.۴ دقیقاً n چندجمله‌ای به این صورت وجود دارد. بنابراین

$$\begin{aligned} f(x) &= (r_1x + s_1)(r_2x + s_2)\cdots(r_nx + s_n) \\ &= r_1(x - (-r_1^{-1}s_1))r_2(x - (-r_2^{-1}s_2)\cdots r_n(x - (-r_n^{-1}s_n)) \\ &= c(x - a_1)(x - a_2)\cdots(x - a_n), \end{aligned}$$

که در آن $c = r_1r_2\cdots r_n$ و $a_i = r_i^{-1}s_i$. یکتایی از قضیه ۱۰.۴ نتیجه می‌شود: تمرین ۲۵ بخش ۴ـ۳ را ملاحظه کنید. ■

برای به‌دست آوردن توصیفی از همه چندجمله‌ایهای تحویل‌ناپذیر در $\mathbb{R}[x]$، به لم زیر نیاز داریم:

لم ۲۴.۴. اگر $f(x)$ یک چندجمله‌ای در $\mathbb{R}[x]$ باشد و $a + bi$ یک ریشه $f(x)$ در $\mathbb{C}$ باشد، در این صورت $a - bi$ نیز یک ریشه $f(x)$ است.

برهان. اگر $c = a + bi \in \mathbb{C}$ (با $a, b \in \mathbb{R}$)، فرض کنید $\bar{c}$، $a - bi$ را نشان دهد. بررسی کنید که برای هر $c, d \in \mathbb{C}$،

$$\overline{(c + d)} = \bar{c} + \bar{d} \qquad \text{و} \qquad \overline{cd} = \bar{c}\bar{d}.$$

همچنین توجه کنید که $\bar{c} = c$ اگر و تنها اگر c یک عدد حقیقی باشد. حالا اگر $f(x) = a_nx^n + \cdots + a_1x + a_0$ و c یک ریشه $f(x)$ باشد، در این صورت $f(c) = 0$، لذا

$$\begin{aligned} 0 = \bar{0} = \overline{f(c)} &= \overline{a_nc^n + \cdots + a_1c + a_0} \\ &= \bar{a}_n\bar{c}^n + \cdots + \bar{a}_1\bar{c} + \bar{a}_0 \\ &= a_n\bar{c}^n + \cdots + a_1\bar{c} + a_0 \qquad (\text{زیرا هر } a_i \in \mathbb{R}) \\ &= f(\bar{c}) \end{aligned}$$

بنابراین $\bar{c} = a - bi$ یک ریشه $f(x)$ است. ■

قضیه ۲۵.۴. یک چندجمله‌ای $f(x)$ در $\mathbb{R}[x]$ تحویل‌ناپذیر است اگر و تنها اگر $f(x)$ یک چندجمله‌ای درجه اول باشد یا

$$f(x) = ax^2 + bx + c \qquad \text{با} \qquad b^2 - 4ac < 0.$$

برهان. اثبات این که تنها چندجمله‌ایهای تحویل‌ناپذیر در واقع همان دو نوع ذکر شده در صورت قضیه است به خواننده واگذار می‌شود (تمرین ۷). بالعکس، فرض کنید $f(x)$ دارای درجه ≥ 2 است و تحویل‌ناپذیر در $\mathbb{R}[x]$ می‌باشد. در این صورت به موجب قضیه ۲۱.۴، $f(x)$ دارای یک ریشه w در $\mathbb{C}$ است. لم ۲۴.۴ نشان می‌دهد که $\bar{w}$ نیز یک ریشه $f(x)$ است. بعلاوه $w \neq \bar{w}$ (در غیر این صورت w بایستی یک ریشه حقیقی $f(x)$ باشد، که تحویل‌ناپذیری $f(x)$ در $\mathbb{R}[x]$ را نقض می‌کند). در نتیجه، به موجب قضیه عامل، $x - w$ و $x - \bar{w}$ عامل‌هایی از $f(x)$ در $\mathbb{C}[x]$ هستند؛ یعنی برای برخی $h(x) \in \mathbb{C}[x]$، $f(x) = (x - w)(x - \bar{w})h(x)$. فرض کنید $g(x) = (x - w)(x - \bar{w})$؛ در این صورت $f(x) = g(x)h(x)$ در $\mathbb{C}[x]$. بعلاوه اگر $w = r + si$ (با $r, s \in \mathbb{R}$)، در این صورت

$$\begin{aligned} g(x) &= (x - w)(x - \bar{w}) = (x - (r + si))(x - (r - si)) \\ &= x^2 - 2rx + (r^2 + s^2). \end{aligned}$$

بنابراین ضرایب $g(x)$ اعداد حقیقی هستند.

اینک نشان می‌دهیم که $h(x)$ نیز دارای ضرایب حقیقی است. بکارگیری الگوریتم تقسیم در $\mathbb{R}[x]$ نشان می‌دهد که چندجمله‌ایهای $q(x)$ و $r(x)$ در $\mathbb{R}[x]$ وجود دارند به قسمی که $f(x) = g(x)q(x) + r(x)$، با $r(x) = 0$ یا $\deg r(x) < \deg g(x)$. امّا در $\mathbb{C}[x]$ داریم $f(x) = g(x)h(x) + 0$. چون $q(x)$ و $r(x)$ را می‌توان به عنوان چندجمله‌ایهایی در $\mathbb{C}[x]$ در نظر گرفت، قسمت یکتایی قضیه الگوریتم تقسیم در $\mathbb{C}[x]$ نشان می‌دهد که $q(x) = h(x)$ و $r(x) = 0$. بنابراین $h(x) = q(x) \in \mathbb{R}[x]$. چون $f(x) = g(x)h(x)$ و $f(x)$ تحویل‌ناپذیر در $\mathbb{R}[x]$ است و $\deg g(x) = 2$، $h(x)$ بایستی یک ثابت $d \in \mathbb{R}$ باشد. در نتیجه $f(x) = dg(x)$ یک چندجمله‌ای درجه دوم در $\mathbb{R}[x]$ است و بنابراین برای برخی $a, b, c \in \mathbb{R}$ به صورت $ax^2 + bx + c$ می‌باشد. چون $f(x)$ دارای هیچ ریشه‌ای در $\mathbb{R}$ نیست، فرمول درجه دوم (تمرین ۶) نشان می‌دهد که $b^2 - 4ac < 0$. ■

نتیجه ۲۶.۴. هر چندجمله‌ای از درجه فرد $f(x)$ در $\mathbb{R}[x]$ دارای یک ریشه در $\mathbb{R}$ است.

برهان. به موجب قضیه ۱۰.۴، $f(x) = p_1(x)p_2(x)\cdots p_k(x)$ که در آن هر $p_i(x)$ تحویل‌ناپذیر در $\mathbb{R}[x]$ است. به موجب قضیه ۲۵.۴، هر $p_i(x)$ دارای درجه ۱ یا ۲ است. قضیه ۱.۴ نشان می‌دهد که

$$\deg f(x) = \deg p_1(x) + \deg p_2(x) + \cdots + \deg p_k(x).$$

چون $f(x)$ دارای درجه فرد است، لذا حداقل یکی از $p_i(x)$ ها باید دارای درجه ۱ باشد. پس $f(x)$ دارای یک عامل درجه اول در $\mathbb{R}[x]$ است و بنابراین دارای یک ریشه در $\mathbb{R}$ است. ■

ممکن است این چنین به‌نظر برسد که قضیه اساسی و نتایج آن به همه سؤالات اساسی درباره معادلات چندجمله‌ای پاسخ می‌دهد. متأسفانه مسئله به این سادگی نیست. هیچ یک از اثباتهای قضیه اساسی یک روش ساختاری برای یافتن ریشه‌های یک چندجمله‌ای مشخص را ارائه نمی‌کند[۱۸]. بنابراین، اگرچه می‌دانیم که هر معادله چندجمله‌ای دارای یک جواب در $\mathbb{C}$ است، با این حال ممکن است قادر به حل یک معادله بخصوص نباشیم.

تمرینها

۱.A. همه ریشه‌های هر یک از چندجمله‌ایهای زیر را بیابید (یک ریشه از پیش داده شده است):

(الف) $x^4 - 3x^3 + x^2 + 7x - 30$؛ ریشه $1 - 2i$

(ب) $x^4 - 2x^3 - x^2 + 6x - 6$؛ ریشه $1 + i$

(پ) $x^4 - 4x^3 + 3x^2 + 14x + 26$؛ ریشه $3 + 2i$

۲. چندجمله‌ای در $\mathbb{R}[x]$ را بیابید که در شرایط زیر صدق کند:

(الف) تکین از درجه ۳ باشد و 2 و $3 + i$ دو ریشه آن باشند.

(ب) تکین از کوچکترین درجه ممکن باشد و $i - 1$ و $2i$ دو ریشه آن باشند.

(پ) تکین از کوچکترین درجه ممکن باشد و 3 و $1 - 4i$ دو ریشه آن باشند.

۱۸) ممکن است عجیب به‌نظر برسد که بتوان اثباتی برای وجود یک ریشه داد بدون در واقع ارائه چنین ریشه‌ای، امّا چنین "قضایای وجودی" در ریاضیات کاملاً معمول هستند. در مقایسه‌ای کلی این مثل وضعیتی است که شخصی توسط یک گلوله اسلحه کشته می‌شود، پلیس می‌داند که قاتلی وجود دارد، امّا در واقع یافتن قاتل می‌تواند مشکل و یا غیرممکن باشد.

۳. هر چندجمله‌ای را به صورت حاصل‌ضربی از چندجمله‌ایهای تحویل‌ناپذیر در $\mathbb{Q}[x]$، در $\mathbb{R}[x]$، و در $\mathbb{C}[x]$ تجزیه کنید:

(الف) $x^۴ - ۲$ (ب) $x^۳ + ۱$ (پ) $x^۳ - x^۲ - ۵x + ۵$

۴. $x^۲ + x + ۱ + i$ را در $\mathbb{C}[x]$ تجزیه کنید.

۵.B نشان دهید که یک چندجمله‌ای از درجه فرد که دارای ریشه چندگانه در $\mathbb{R}[x]$ نباشد باید دارای تعداد فردی از ریشه‌های حقیقی باشد.

۶. فرض کنید $f(x) = ax^۲ + bx + c \in \mathbb{R}[x]$ با $a \neq ۰$. ثابت کنید که ریشه‌های $f(x)$ در $\mathbb{C}$ عبارتند از $(-b + \sqrt{b^۲ - ۴ac})/۲a$ و $(-b - \sqrt{b^۲ - ۴ac})/۲a$. [راهنمایی: نشان دهید که $ax^۲ + bx + c = ۰$ معادل $x^۲ + (b/a)x = -c/a$ می‌باشد؛ سپس با کامل‌کردن مربع، x را بیابید.]

۷. ثابت کنید که هر $ax^۲ + bx + c \in \mathbb{R}[x]$ با $b^۲ - ۴ac < ۰$ تحویل‌ناپذیر در $\mathbb{R}[x]$ است. [راهنمایی: تمرین ۶ را ملاحظه کنید.]

۸. اگر $a + bi$ یک ریشه $x^۳ - ۳x^۲ + ۲ix + i - ۱ \in \mathbb{C}[x]$ باشد، در این صورت آیا این درست است که $a - bi$ نیز یک ریشه است؟

* * * * *

فصل پنجم

همنهشتی در $\mathbb{F}[x]$ و حساب کلاس‌های همنهشتی

در این فصل به کاوش خود در مورد شباهت بین حلقه اعداد صحیح $\mathbb{Z}$ و حلقه چندجمله‌ای‌های $\mathbb{F}[x]$ با ضرایب در یک میدان $\mathbb{F}$ ادامه می‌دهیم. خواهیم دید که تقریباً بدون هیچ تغییری مفاهیم همنهشتی و حساب کلاس‌های همنهشتی از $\mathbb{Z}$ به $\mathbb{F}[x]$ منتقل می‌شود. به دلیل وجود برخی مفاهیم ویژه در حلقه چندجمله‌ای‌های $\mathbb{F}[x]$ (مانند توابع چندجمله‌ای و ریشه‌ها)، این حلقه‌های کلاس همنهشتی دارای ساختار خیلی غنی‌تری از حلقه‌های $\mathbb{Z}_n$ است و همین امر منجر به این نتیجه درخور توجه می‌شود که: به ازای هر چندجمله‌ای مفروض روی یک میدان $\mathbb{F}$، می‌توان ریشه‌ای از آن را در یک میدان بزرگتر یافت.

۱-۵ همنهشتی در $\mathbb{F}[x]$ و کلاس‌های همنهشتی

مفهوم همنهشتی اعداد صحیح تنها بستگی به برخی حقایق اساسی در مورد بخش‌پذیری در $\mathbb{Z}$ دارد. اگر $\mathbb{F}$ یک میدان باشد، در این صورت حلقه چندجمله‌ای‌های $\mathbb{F}[x]$ اساساً دارای همان خواص بخش‌پذیری $\mathbb{Z}$ است. بنابراین تعجب‌آور نیست که مفهوم همنهشتی در $\mathbb{Z}$ و خواص اساسی آن (بخش ۱.۲) تقریباً کلمه به کلمه قابل انتقال به $\mathbb{F}[x]$ باشد.

تعریف. فرض کنید $\mathbb{F}$ یک میدان باشد و $f(x), g(x), p(x) \in \mathbb{F}[x]$، که در آن $p(x)$ غیرصفر است. در این صورت $f(x)$ را همنهشت با $g(x)$ به پیمانه $p(x)$ گوییم و می‌نویسیم $f(x) \equiv g(x)\ (p(x))$ (پیمانه $p(x)$)، هرگاه $p(x)$ تفاضل $f(x) - g(x)$ را بشمارد.

مثال ۱.۵. در $\mathbb{Q}[x]$ داریم $x^2 + x + 1 \equiv x + 2\ (x + 1)$، زیرا

$$(x^2 + x + 1) - (x + 2) = x^2 - 1 = (x + 1)(x - 1).$$

مثال ۲.۵. در $\mathbb{R}[x]$ داریم $3x^4 + 4x^2 + 2x + 2 \equiv x^3 + 3x^2 + 3x + 4\ (x^2 + 1)$ زیرا با انجام تقسیم معمولی می‌توان دید که

$$\begin{aligned}(3x^4 + 4x^2 + 2x + 2) - (x^3 + 3x^2 + 3x + 4) \\ &= 3x^4 - x^3 + x^2 - x - 2 \\ &= (x^2 + 1)(3x^2 - x - 2).\end{aligned}$$

قضیه ۱.۵. فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای غیرصفر در $\mathbb{F}[x]$ باشد. در این صورت رابطه همنهشتی به پیمانه $p(x)$ دارای خواص زیر است:

(۱) انعکاسی: برای هر $f(x) \in \mathbb{F}[x]$، $f(x) \equiv f(x)\ (p(x))$؛

(۲) متقارن: اگر $f(x) \equiv g(x)\ (p(x))$، در این صورت $g(x) \equiv f(x)\ (p(x))$؛

(۳) متعدّی: اگر $f(x) \equiv g(x)\ (p(x))$ و $g(x) \equiv h(x)\ (p(x))$، در این صورت $f(x) \equiv h(x)\ (p(x))$.

برهان. برهان قضیه ۱.۲ را با $p(x)$، $f(x)$، $g(x)$ و $h(x)$ بجای n، a، b و c بکار برید. ■

قضیه ۲.۵. فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای غیرصفر در $\mathbb{F}[x]$ باشد. اگر $f(x) \equiv g(x)$ (پیمانه $p(x)$) و $h(x) \equiv k(x)$ (پیمانه $p(x)$)، در این صورت

(۱) $f(x) + h(x) \equiv g(x) + k(x)$ (پیمانه $p(x)$)،

(۲) $f(x)h(x) \equiv g(x)k(x)$ (پیمانه $p(x)$).

برهان. برهان قضیه ۲.۲ را با $p(x)$، $f(x)$، $g(x)$، $h(x)$ و $k(x)$ بجای n، a، b، c و d بکار برید. ■

تعریف. فرض کنید $\mathbb{F}$ یک میدان باشد و $f(x), p(x) \in \mathbb{F}[x]$، جایی که $p(x)$ غیرصفر است. **کلاس همنهشتی (یا ردهٔ مانده‌های)** $f(x)$ به پیمانه $p(x)$ با $[f(x)]$ نشان داده می‌شود و شامل همه چندجمله‌ای‌های در $\mathbb{F}[x]$ است که همنهشت با $f(x)$ به پیمانه $p(x)$ هستند، یعنی

$$[f(x)] = \{g(x) \mid g(x) \in \mathbb{F}[x] \text{ و } g(x) \equiv f(x) \text{ } (p(x) \text{ پیمانه})\}.$$

چون همنهشتی $g(x) \equiv f(x)$ $(p(x)$ پیمانه$)$ بدین معنی است که $k[x] \in \mathbb{F}[x]$ وجود دارد به قسمی که $g(x) - f(x) = k(x)p(x)$ و یا به طور معادل $g(x) = f(x) + k(x)p(x)$، می‌بینیم که

$$\begin{aligned}[f(x)] &= \{g(x) \mid g(x) \equiv f(x) \text{ } (p(x) \text{ پیمانه})\} \\ &= \{f(x) + k(x)p(x) \mid k(x) \in \mathbb{F}[x]\}.\end{aligned}$$

مثال ۳.۵. همنهشتی به پیمانه $x^2 + 1$ در $\mathbb{R}[x]$ را در نظر بگیرید. کلاس همنهشتی $2x + 1$ مجموعه

$$\{(2x + 1) + k(x)(x^2 + 1) \mid k(x) \in \mathbb{F}[x]\}$$

می‌باشد. الگوریتم تقسیم نشان می‌دهد که عناصر این مجموعه چندجمله‌ای‌هایی در $\mathbb{R}[x]$ هستند که باقیمانده تقسیم آنها بر $x^2 + 1$ عبارت از $2x + 1$ است.

مثال ۴.۵. همنهشتی به پیمانه $x^2 + x + 1$ در $\mathbb{Z}_2[x]$ را در نظر بگیرید. برای یافتن کلاس همنهشتی x^2، توجه می‌کنیم که در $\mathbb{Z}_2$ داریم $1 + 1 = 0$، لذا $-1 = 1$. پس $x^2 - (x + 1) = x^2 - x - 1 = x^2 + x + 1$، بنابراین $x^2 \equiv x + 1$ (پیمانه $x^2 + x + 1$).

لذا $x+1$ یک عضو کلاس همنهشتی $[x^2]$ است. در حقیقت، قضیه بعدی نشان می‌دهد که $[x+1]=[x^2]$.

قضیه ۳.۵. (پیمانه $p(x)$) $f(x)\equiv g(x)$ اگر و تنها اگر $[f(x)]=[g(x)]$.

برهان. برهان قضیه ۳.۲ را با $f(x)$، $g(x)$ و $p(x)$ بجای a، b و c بکار برید و از قضیه ۱.۵ بجای قضیه ۱.۲ استفاده کنید.

نتیجه ۴.۵. هر دو کلاس همنهشتی به پیمانه $p(x)$ مجزا و یا برابرند.

برهان. نتیجه ۴.۲ را ملاحظه کنید. ■

تحت همنهشتی به پیمانه n در $\mathbb{Z}$، دقیقاً n کلاس همنهشتی مجزا وجود دارد (نتیجه ۵.۲). این کلاسها عبارتند از $[0]$،$[1]$،...،$[n-1]$. توجه کنید که برای هر باقیمانده ممکن تقسیم بر n، یک کلاس وجود دارد. در $\mathbb{F}[x]$ باقیمانده‌های ممکن تقسیم بر یک چندجمله‌ای از درجه n، عبارتند از همه چندجمله‌ای‌های از درجه کوچکتر از n (و البته ۰). بنابراین مشابه نتیجه ۵.۲، نتیجه زیر است.

نتیجه ۵.۵. فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای از درجه n در $\mathbb{F}[x]$ باشد. فرض کنید مجموعه S شامل چندجمله‌ای صفر و همه چندجمله‌ای‌های از درجه کوچکتر از n در $\mathbb{F}[x]$ باشد. در این صورت هر کلاس همنهشتی به پیمانه $p(x)$، کلاس یکی از چندجمله‌ای‌های در S است، و کلاس‌های همنهشتی چندجمله‌ای‌های متفاوت در S متمایزند.

برهان. دو چندجمله‌ای در S نمی‌تواند همنهشت به پیمانه $p(x)$ باشد زیرا اختلاف آنها دارای درجه کمتر از n است و لذا بر $p(x)$ بخش‌پذیر نیست. بنابراین طبق قضیه ۳.۵، چندجمله‌ای‌های متفاوت در S باید در کلاس‌های همنهشتی متمایز باشند. مانند قسمت آخر اثبات نتیجه ۵.۲، الگوریتم تقسیم را بکار برید تا نشان دهید که هر چندجمله‌ای در $\mathbb{F}[x]$ همنهشت با یک چندجمله‌ای در S به پیمانه $p(x)$ است. بنابراین، طبق قضیه ۳.۵، هر کلاس همنهشتی برابر با کلاس یکی از چندجمله‌ای‌های در S است. ■

مشابه نمادی که برای $\mathbb{Z}_n$ بکار بردیم، مجموعهٔ کلاس‌های همنهشتی به پیمانه $p(x)$ را با $\mathbb{F}[x]/(p(x))$ نشان می‌دهیم.

مثال ۵.۵. همنهشتی به پیمانه $x^۲+۱$ در $\mathbb{R}[x]$ را در نظر بگیرید. برای هر باقیمانده ممکن تقسیم بر $x^۲+۱$، یک کلاس همنهشتی وجود دارد. حال باقیمانده‌های ممکن عبارتند از چندجمله‌ای‌هایی به صورت $rx+s$ (با $r,s\in\mathbb{R}$؛ یکی یا هر دو r، s ممکن است ۰ باشد). بنابراین $\mathbb{R}[x]/(x^۲+۱)$ شامل تعداد نامتناهی کلاس همنهشتی متمایز، از جمله

$$[۰],[x],[x+۱],[۵x+۳],[\frac{۷}{۹}x+۲],[x-۷],\dots$$

می‌باشد. نتیجه ۵.۵ بیان می‌کند که $[rx+s]=[cx+d]$ اگر و تنها اگر $rx+s$ برابر (نه فقط همنهشت) با $cx+d$ باشد. بنابه تعریف برابری چندجمله‌ای‌ها، $rx+s=cx+d$ اگر و تنها اگر $r=c$ و $s=d$. بنابراین هر عضو $\mathbb{R}[x]/(x^۲+۱)$ به صورت منحصربه‌فردی به شکل $[rx+s]$ نوشته می‌شود.

مثال ۶.۵. همنهشتی به پیمانه $x^۲+x+۱$ در $\mathbb{Z}_۲[x]$ را در نظر بگیرید. باقیمانده‌های ممکن تقسیم بر $x^۲+x+۱$ عبارتند از چندجمله‌ای‌هایی به صورت $ax+b$ با $a,b\in\mathbb{Z}_۲$. لذا تنها چهار باقیمانده ممکن وجود دارد: ۰، ۱، x و $x+۱$. بنابراین $\mathbb{Z}_۲[x]/(x^۲+x+۱)$ از چهارکلاس همنهشتی $[۰]$، $[۱]$، $[x]$ و $[x+۱]$ تشکیل شده است.

مثال ۷.۵. الگوی مثال قبلی در حالت کلی نیز کارآمد است. اگر $p(x)\in\mathbb{Z}_n[x]$ دارای درجه k باشد، در این صورت باقیمانده‌های ممکن تقسیم بر $p(x)$ به صورت $a_۰+a_۱x+\cdots+a_{k-۱}x^{k-۱}$ می‌باشند با $a_i\in\mathbb{Z}_n$. برای هر یک از k ضریب $a_۰,\dots,a_{k-۱}$، n امکان وجود دارد و بنابراین n^k چندجمله‌ای متفاوت به این شکل وجود دارد. در نتیجه، طبق قضیه ۵.۵، دقیقاً n^k کلاس همنهشتی متمایز در $\mathbb{Z}_n[x]/(p(x))$ وجود دارد.

تمرینها

توجه. $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای غیرصفر در $\mathbb{F}[x]$ را نشان می‌دهد.

A.۱. ثابت کنید که (پیمانه $p(x)$) $f(x)\equiv g(x)$ اگر و تنها اگر باقیمانده تقسیم $f(x)$ و $g(x)$ بر $p(x)$ برابر باشد.

۲. اگر $p(x)$ یک چندجمله‌ای ثابت غیرصفر در $\mathbb{F}[x]$ باشد، نشان دهید که هر دو چندجمله‌ای در $\mathbb{F}[x]$ همنهشت به پیمانه $p(x)$ هستند.

۳.B. اگر $p(x)$ نسبت به $k(x)$ اول باشد و $f(x)k(x) \equiv g(x)k(x)$ (پیمانه $p(x)$)، ثابت کنید که $f(x) \equiv g(x)$ (پیمانه $p(x)$).

۴. اگر $p(x)$ تحویل‌ناپذیر در $\mathbb{F}[x]$ باشد و $f(x)g(x) \equiv {}^{\circ}_{\mathbb{F}}$ (پیمانه $p(x)$)، ثابت کنید که $f(x) \equiv {}^{\circ}_{\mathbb{F}}$ (پیمانه $p(x)$) یا $g(x) \equiv {}^{\circ}_{\mathbb{F}}$ (پیمانه $p(x)$).

۵. اگر $p(x)$ تحویل‌ناپذیر در $\mathbb{F}[x]$ نباشد، ثابت کنید $f(x), g(x) \in \mathbb{F}[x]$ وجود دارند به طوری که $f(x) \not\equiv {}^{\circ}_{\mathbb{F}}$ (پیمانه $p(x)$) و $g(x) \not\equiv {}^{\circ}_{\mathbb{F}}$ (پیمانه $p(x)$) ولی $f(x)g(x) \equiv {}^{\circ}_{\mathbb{F}}$ (پیمانه $p(x)$).

۶. اگر $f(x)$ نسبت به $p(x)$ اوّل باشد، ثابت کنید چندجمله‌ای $g(x) \in \mathbb{F}[x]$ وجود دارد به طوری که $f(x)g(x) \equiv {}^{1}_{\mathbb{F}}$ (پیمانه $p(x)$).

۷. فرض کنید $f(x), g(x) \in \mathbb{R}[x]$ و $f(x) \equiv g(x)$ (پیمانه $p(x)$). درباره نمودارهای $y = f(x)$ و $y = g(x)$ چه می‌توان گفت؟

۸. نشان دهید که تحت همنهشتی به پیمانه $x^3 + 2x + 1$ در $\mathbb{Z}_3[x]$، دقیقاً ۲۷ کلاس همنهشتی متمایز وجود دارد.

۹. چه تعداد کلاس همنهشتی متمایز به پیمانه $x^3 + x + 1$ در $\mathbb{Z}_2[x]$ وجود دارد؟ آنها را فهرست کنید.

۱۰. اگر $p(x)$ دارای درجه k در $\mathbb{Z}_n[x]$ باشد، چه تعداد کلاس همنهشتی به پیمانه $p(x)$ وجود دارد؟

۱۱. نشان دهید که تعداد نامتناهی کلاس همنهشتی متمایز به پیمانه $x^2 - 2$ در $\mathbb{Q}[x]$ وجود دارد. آنها را توصیف کنید.

۱۲. فرض کنید $a \in \mathbb{F}$. کلاس‌های همنهشتی در $\mathbb{F}[x]$ به پیمانه چندجمله‌ای $x - a$ را توصیف کنید.

۵-۲ حساب کلاس‌های همنهشتی

مفهوم همنهشتی در اعداد صحیح منجر به ایجاد حلقه‌های $\mathbb{Z}_n$ گردید. به طور مشابه، مفهوم همنهشتی در $\mathbb{F}[x]$ نیز حلقه‌ها و میدانهای جدیدی را ایجاد می‌کند. خواهیم دید که اینها از نظر ساختاری بسیار غنی‌تر از حلقه‌های $\mathbb{Z}_n$ هستند. روند پیشرفت مطالب این بخش کاملاً به موازات مطالب بخش ۲.۲ انجام می‌گیرد.

قضیه ۶.۵. فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای غیرثابت در $\mathbb{F}[x]$ باشد. اگر $[f(x)] = [g(x)]$ و $[h(x)] = [k(x)]$ در $\mathbb{F}[x]/(p(x))$، در این صورت $[f(x) + h(x)] = [g(x) + k(x)]$ و $[f(x)h(x)] = [g(x)k(x)]$.

برهان. همان اثبات قضیه ۶.۲ را بکار برید. ■

طبق قضیه ۶.۵، اینک می‌توانیم جمع و ضرب کلاس‌های همنهشتی را دقیقاً مشابه آنچه در مورد اعداد صحیح انجام شد تعریف کنیم و مطمئن باشیم که این دو عمل مستقل از انتخاب نماینده در هر یک از کلاس‌های همنهشتی است.

تعریف. فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای غیرثابت در $\mathbb{F}[x]$ باشد. جمع و ضرب در $\mathbb{F}[x]/(p(x))$ توسط

$$[f(x)] + [g(x)] = [f(x) + g(x)]$$
$$[f(x)][g(x)] = [f(x)g(x)]$$

تعریف می‌شود.

مثال ۸.۵. همنهشتی به پیمانه $x^2 + 1$ را در $\mathbb{R}[x]$ در نظر بگیرید. مجموع دو کلاس $[2x + 1]$ و $[3x + 5]$ کلاس

$$[(2x + 1) + (3x + 5)] = [5x + 6]$$

است. حاصل ضرب آنها عبارت است از

$$[2x + 1][3x + 5] = [(2x + 1)(3x + 5)] = [6x^2 + 13x + 5].$$

همانگونه که در مثال ۵.۵ تذکر داده شد، هر کلاس همنهشتی در $\mathbb{R}[x]/(x^2+1)$ می‌تواند به صورت $[ax+b]$ نوشته شود. برای نوشتن $[6x^2+13x+5]$ به شکل مذکور، با تقسیم $6x^2+13x+5$ بر x^2+1 درمی‌یابیم که

$$6x^2+13x+5 = 6(x^2+1)+(13x-1).$$

در نتیجه (پیمانه x^2+1) $6x^2+13x+5 \equiv 13x-1$، و بنابراین $[6x^2+13x+5] = [13x-1]$.

مثال ۹.۵. در مثال ۶.۵، دیدیم که $\mathbb{Z}_2[x]/(x^2+x+1)$ متشکل از چهارکلاس $[0]$، $[1]$، $[x]$ و $[x+1]$ است. با استفاده از تعریف جمع کلاسها، می‌بینیم که $[x]=[x+1+1]=[1]+[x+1]$ (به خاطر آورید که $1+1=0$ در $\mathbb{Z}_2$). با انجام محاسباتی مشابه، جدول جمع زیر برای $\mathbb{Z}_2[x]/(x^2+x+1)$ بدست می‌آید.

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

بیشتر قسمت‌های جدول ضرب برای $\mathbb{Z}_2[x]/(x^2+x+1)$ به سادگی از تعریف بدست می‌آید:

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$		
$[x+1]$	$[0]$	$[x+1]$		

برای پرکردن باقیمانده جدول، برای مثال توجه کنید که

$$[x]\cdot[x+1] = [x(x+1)] = [x^2+x].$$

اینک باانجام تقسیم و یا جمع‌معمولی در $\mathbb{Z}_2[x]$ می‌بینیم که $x^2+x = (x^2+x+1)+1$. بنابراین (پیمانه x^2+x+1) $x^2+x \equiv 1$ و $[x^2+x] = [1]$. بطور مشابه می‌بینیم که

$[x]\cdot[x]=[x^2]=[x+1]$ (زیرا $x^2=(x^2+x+1)+(x+1)$ در $\mathbb{Z}_2[x]$).

اگر جداول مثال قبل را امتحان کنید، خواهید دید که $\mathbb{Z}_2[x]/(x^2+x+1)$ یک حلقه جابجایی یکدار است (در واقع، یک میدان). این امر با توجه به تجربه‌ای که در مورد $\mathbb{Z}$ و $\mathbb{Z}_m$ داشتیم چندان تعجب‌آور نیست. آنچه که غیرقابل انتظار است، گوشه سمت چپ بالایی دو جدول است (مجموع و حاصل‌ضربهای $[0]$ و $[1]$). به سادگی دیده می‌شود که زیرمجموعهٔ $\{[0],[1]\}=\mathbb{F}^*$ در واقع یک زیرحلقه $\mathbb{Z}_2[x]/(x^2+x+1)$ است و این که $\mathbb{F}^*$ یکریخت با $\mathbb{Z}_2$ است (به‌جز کروشه‌هایی که در جدول $\mathbb{F}^*$ ظاهر می‌شوند، جداول دو دستگاه یکسان است). این حقایق ما را به قضیه بعدی رهنمون می‌کند.

قضیه ۷.۵. فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای غیرثابت در $\mathbb{F}[x]$ باشد. در این صورت مجموعه $\mathbb{F}[x]/(p(x))$ متشکل از کلاس‌های همنهشتی به پیمانه $p(x)$ یک حلقه جابجایی یکدار است. بعلاوه، $\mathbb{F}[x]/(p(x))$ دارای یک زیرحلقه $\mathbb{F}^*$ است که با $\mathbb{F}$ یکریخت می‌باشد.

برهان. برای اثبات این که $\mathbb{F}[x]/(p(x))$ یک حلقه جابجایی یکدار است، اثبات قضیه ۷.۲ را به وضعیت حاضر تطبیق دهید. فرض کنید $\mathbb{F}^*$ زیرمجموعه‌ای از $\mathbb{F}[x]/(p(x))$ باشد که از کلاس‌های همنهشتی همه چندجمله‌ای‌های ثابت تشکیل شده است؛ یعنی، $\mathbb{F}^*=\{[a]\mid a\in\mathbb{F}\}$. بررسی کنید که $\mathbb{F}^*$ یک زیرحلقه $\mathbb{F}[x]/(p(x))$ است (تمرین ۱۲). نگاشت $\varphi:\mathbb{F}\to\mathbb{F}^*$ را توسط $\varphi(a)=[a]$ تعریف کنید. از تعریف دیده می‌شود که φ پوشا است. تعاریف جمع و ضرب در $\mathbb{F}[x]/(p(x))$ نشان می‌دهد که

$$\varphi(a+b)=[a+b]=[a]+[b]=\varphi(a)+\varphi(b)$$
$$\varphi(ab)=[ab]=[a]\cdot[b]=\varphi(a)\cdot\varphi(b).$$

بنابراین φ یک همریختی است.

برای دیدن این که φ یک به یک است، فرض کنید $\varphi(a)=\varphi(b)$. در این صورت $[a]=[b]$، لذا (پیمانه $p(x)$) $a\equiv b$. بنابراین $p(x)$، $a-b$ را می‌شمارد. امّا $p(x)$ دارای درجه ≥ 1 است و $a-b\in\mathbb{F}$. این امکان‌پذیر نیست مگر این که $a-b=0$. پس $a=b$ و φ یک به یک است. بنابراین $\varphi:\mathbb{F}\to\mathbb{F}^*$ یک یکریختی است.

با شروع از میدان $\mathbb{F}$ و چندجمله‌ای $p(x)$، حلقه $\mathbb{F}[x]/(p(x))$ را چنان ساختیم که زیرحلقه‌ای یکریخت با $\mathbb{F}$ را شامل است. آنچه که ما واقعاً به آن علاقه‌مندیم حلقه‌ای است که حقیقتاً $\mathbb{F}$ را به عنوان زیرمجموعه‌ای از خود شامل باشد. همانگونه که در مثال زیر نشان داده می‌شود، دو روش ممکن برای انجام این امر وجود دارد.

مثال ۱۰.۵. در مثال قبل از قضیه ۷.۵، چندجمله‌ای $x^۲ + x + ۱$ در $\mathbb{Z}_۲[x]$ را به کار بردیم تا حلقه $\mathbb{Z}_۲[x]/(x^۲ + x + ۱)$ را که شامل یک زیرمجموعه $\mathbb{F}^* = \{[۰], [۱]\}$ که یکریخت با $\mathbb{Z}_۲$ است بسازیم. فرض کنید که $\mathbb{Z}_۲$ را با نسخه یکریختش $\mathbb{F}^*$ داخل $\mathbb{Z}_۲[x]/(x^۲ + x + ۱)$ یکی بگیریم و عناصر $\mathbb{F}^*$ را به‌عنوان اعضایی از $\mathbb{Z}_۲$ در نظر بگیریم. در این صورت جداول مثال ۹.۵ به صورت زیر درخواهد آمد.

$+$	۰	۱	$[x]$	$[x+۱]$
۰	۰	۱	$[x]$	$[x+۱]$
۱	۱	۰	$[x+۱]$	$[x]$
$[x]$	$[x]$	$[x+۱]$	۰	۱
$[x+۱]$	$[x+۱]$	$[x]$	۱	۰

$\cdot$	۰	۱	$[x]$	$[x+۱]$
۰	۰	۰	۰	۰
۱	۰	۱	$[x]$	$[x+۱]$
$[x]$	۰	$[x]$	$[x+۱]$	۱
$[x+۱]$	۰	$[x+۱]$	۱	$[x]$

اینک حلقه‌ای داریم که $\mathbb{Z}_۲$ را به‌عنوان یک زیرحلقه دارد. اگر این یکی‌گیری شما را آزار می‌دهد (که آیا $\mathbb{Z}_۲$ واقعاً یک زیرمجموعه است) می‌توانید از روش جایگزین زیر که به همان نتیجه منتهی می‌شود استفاده کنید. فرض کنید E هر مجموعه چهارعضوی باشد که حقیقتاً $\mathbb{Z}_۲$ را به عنوان یک زیرمجموعه شامل باشد، مثلاً $E = \{۰, ۱, r, s\}$. جمع و ضرب را در E به صورت زیر تعریف کنید:

$+$	0	1	r	s
0	0	1	r	s
1	1	0	s	r
r	r	s	0	1
s	s	r	1	0

$\cdot$	0	1	r	s
0	0	0	0	0
1	0	1	r	s
r	0	r	s	1
s	0	s	1	r

مقایسهٔ جداول مربوط به $\mathbb{Z}_2[x]/(x^2+x+1)$ و جداول مربوط به E نشان می‌دهد که این دو حلقه یکریخت هستند (جایگزینی $[x]$ با r و $[x+1]$ با s، جداول یکی را به جداول دیگری تبدیل می‌کند). بنابراین E اساساً همان حلقه‌ای است که ما قبلاً بدست آوردیم. با این حال E حقیقتاً $\mathbb{Z}_2$ را بدون هیچگونه یکی‌گیری شامل است.

آنچه که در مثال قبلی انجام شد می‌تواند در حالت کلی نیز انجام گیرد. به ازای یک میدان مفروض $\mathbb{F}$ و یک چندجمله‌ای $p(x)$ در $\mathbb{F}[x]$، می‌توانیم حلقه‌ای را بسازیم که $\mathbb{F}$ را به عنوان یک زیرمجموعه شامل باشد. روش معمول برای انجام این کار عبارت است از این که $\mathbb{F}$ را با نسخه یکریختش $\mathbb{F}^*$ داخل $\mathbb{F}[x]/(p(x))$ یکی بگیریم، یعنی $\mathbb{F}$ را به عنوان زیرمجموعه‌ای از $\mathbb{F}[x]/(p(x))$ در نظر بگیریم. اگر مایل به انجام این کار نیستید، به خاطر داشته باشید که همانند مثال قبل، همواره می‌توان حلقه‌ای یکریخت با $\mathbb{F}[x]/(p(x))$ ساخت که حقیقتاً $\mathbb{F}$ را به عنوان یک زیرمجموعه شامل باشد. به دلیل پیچیدگی موجود در روش دوم، روش معمول را دنبال می‌کنیم و از اینجا به بعد $\mathbb{F}$ را با $\mathbb{F}^*$ یکی می‌گیریم. در نتیجه برای $a, b \in \mathbb{F}$، بجای $[b][x]$ می‌نویسیم $b[x]$ و بجای $[a]+[b][x] = [a+bx]$ می‌نویسیم $a+b[x]$. بنابراین، صورت قضیه ۷.۵ را می‌توان به شکل زیر تغییر داد:

قضیه ۸.۵. فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای غیرثابت در $\mathbb{F}[x]$ باشد. در این صورت $\mathbb{F}[x]/(p(x))$ یک حلقه جابجایی یکدار است که $\mathbb{F}$ را شامل می‌باشد.

تمرینها

A. در تمرین‌های ۱-۴، جداول جمع و ضرب را برای حلقه کلاس همنهشتی $\mathbb{F}[x]/(p(x))$ بنویسید. در هر مورد تعیین کنید آیا $\mathbb{F}[x]/(p(x))$ یک میدان است.

۱. $\mathbb{F} = \mathbb{Z}_2$؛ $p(x) = x^2 + x + 1$

۲. $\mathbb{F} = \mathbb{Z}_۳$؛ $p(x) = x^۲ + ۱$

۳. $\mathbb{F} = \mathbb{Z}_۲$؛ $p(x) = x^۲ + ۱$

۴. $\mathbb{F} = \mathbb{Z}_۵$؛ $p(x) = x^۲ + ۱$

B. در تمرین‌های ۵-۸، هر عضو از حلقه کلاس همنهشتی داده شده را می‌توان به صورت $[ax + b]$ نوشت (چرا؟). قوانین جمع و ضرب کلاس‌های همنهشتی را تعیین کنید. (به عبارت دیگر، اگر حاصل $[ax + b][cx + d]$ کلاس $[rx + s]$ باشد، شرح دهید چگونه می‌توان r و s را از a، b، c و d به دست آورد، و به طور مشابه برای جمع.)

۵. $\mathbb{R}[x]/(x^۲ + ۱)$ [راهنمایی: مثال ۸.۵ را ملاحظه کنید.]

۶. $\mathbb{Q}[x]/(x^۲ - ۲)$

۷. $\mathbb{Z}[x]/(x^۲ - ۳)$

۸. $\mathbb{Q}[x]/(x^۲)$

۹. در $\mathbb{Q}[x]/(x^۲ - ۲)$ یک چندجمله‌ای $g(x) \in \mathbb{Q}[x]$ را چنان بیابید که $[g(x)][۲x - ۳] = [۱]$.

۱۰. در $\mathbb{R}[x]/(x^۲ + ۱)$، با بررسی این که هر کلاس همنهشتی غیرصفر $[ax + b]$ یک یکه است نشان دهید که این حلقه یک میدان است. [راهنمایی: نشان دهید که وارون $[ax + b]$ عبارت است از $[cx + d]$، که در آن $c = -a/(a^۲ + b^۲)$ و $d = b/(a^۲ + b^۲)$.]

۱۱. نشان دهید حلقه تمرین ۸ یک میدان نیست.

۱۲. فرض کنید $\mathbb{F}$ یک میدان باشد و $p(x) \in \mathbb{F}[x]$. ثابت کنید که $\mathbb{F}^* = \{[a] \mid a \in \mathbb{F}\}$ یک زیرحلقه $\mathbb{F}[x]/(p(x))$ است.

۱۳. اثبات کاملی از قضیه ۶.۵ را بنویسید (یعنی اثبات قضیه مشابه برای $\mathbb{Z}$ را به $\mathbb{F}[x]$ انتقال دهید).

۱۴. اولین گزاره قضیه ۷.۵ را ثابت کنید.

۱۵.C. یک چندجمله‌ای درجه چهار در $\mathbb{Z}_۲[x]$ بیابید که ریشه‌های آن چهار عضو

میدان $\mathbb{Z}_2[x]/(x^2+x+1)$ باشد که جداول آن در مثال ۱۰.۵ آمده‌است. [راهنمایی: قضیه عامل می‌تواند مفید باشد.]

۱۶. نشان دهید که $\mathbb{Q}[x]/(x^2-2)$ یک میدان است. [راهنمایی: تمرین‌های ۹ و ۱۰ را ملاحظه کنید.]

۱۷. فرض کنید $\mathbb{F}$ یک میدان باشد و $f(x), p(x) \in \mathbb{F}[x]$. اگر $f(x)$ نسبت به $p(x)$ اول باشد، ثابت کنید که $[f(x)]$ یک یکه در حلقه $\mathbb{F}[x]/(p(x))$ است. [راهنمایی، قضیه ۸.۲ و نتیجه ۹.۲.]

۵-۳ ساختار $\mathbb{F}[x]/(p(x))$ وقتی $p(x)$ تحویل‌ناپذیر است

وقتی که p یک عدد صحیح اول باشد، $\mathbb{Z}_p$ یک میدان است (و البته یک دامنه صحیح). احتمالاً می‌توانید نتیجه مشابهی را برای $\mathbb{F}[x]$ حدس بزنید (قضیه ۹.۵). امّا در اینجا علاوه بر مشابهت‌های با $\mathbb{Z}$، نتایج خیلی بیشتری نیز وجود دارد. قبلاً دیده‌ایم که $\mathbb{F}[x]/(p(x))$ میدان $\mathbb{F}$ را شامل است. در این بخش خواهیم دید که یک ریشه $p(x)$ را نیز شامل است.

قضیه ۹.۵. فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای غیرثابت در $\mathbb{F}[x]$ باشد. در این صورت گزاره‌های زیر معادلند:

(۱) $p(x)$ تحویل‌ناپذیر در $\mathbb{F}[x]$ است

(۲) $\mathbb{F}[x]/(p(x))$ یک میدان است.

(۳) $\mathbb{F}[x]/(p(x))$ یک دامنه صحیح است.

برهان. قضیه ۸.۲ را با جایگزینی $\mathbb{F}[x]$ بجای $\mathbb{Z}$، $\mathbb{F}[x]/(p(x))$ بجای $\mathbb{Z}_p$، قضیه ۴.۴ بجای قضیه ۳.۱، و قضیه ۳.۵ بجای قضیه ۳.۲ تطبیق دهید. مشاهدات زیر می‌تواند مفید باشد.

(۱) $\Leftarrow$ (۲) توجه کنید که وقتی $p(x)$ تحویل‌ناپذیر است، ب‌م‌م $a(x)$ و $p(x)$ یا $1_{\mathbb{F}}$ و یا یک وابسته یکه $p(x)$ است. اگر $a(x)$ بر $p(x)$ بخش‌پذیر نباشد، در این صورت بخش‌پذیر بر هیچ وابسته $p(x)$ نیز نیست. بنابراین اگر $a(x) \nmid p(x)$، در این صورت ب‌م‌م آنها باید $1_{\mathbb{F}}$ باشد.

(۲) $\Leftarrow$ (۳) توجه کنید که در اینجا استفاده از قضیه ۸.۲ به هیچ وجه مفید نیست؛ این مطلب فوراً از نتیجه ۸.۳ بدست می‌آید.

(۳) $\Leftarrow$ (۱) توجه کنید که اگر $p(x) = a(x)b(x)$ و $w(x)b(x) = 1_{\mathbb{F}}$، در این صورت $b(x)$ یک ثابت است، بنابراین $a(x)$ یک وابسته $p(x)$ است. این مشابه این است که بگوییم در $\mathbb{Z}$، $a = \pm p$. ■

قضیه ۹.۵ را در ساختن میدان‌های متناهی می‌توان بکار برد. اگر p یک عدد اول و $f(x)$ تحویل‌ناپذیر در $\mathbb{Z}_p[x]$ و از درجه k باشد، در این صورت طبق قضیه ۹.۵، $\mathbb{Z}_p[x]/(f(x))$ یک میدان است. مثال ۷.۵ نشان می‌دهد که این میدان دارای p^k عضو است. بحث بیشتر در مورد میدان‌های متناهی را در بخش ۹.۶ خواهید دید، در آنجا نشان داده می‌شود که چندجمله‌ای‌های تحویل‌ناپذیر از هر درجه مثبت در $\mathbb{Z}_p[x]$ وجود دارد و بنابراین میدان‌هایی متناهی از مرتبه هرتوانی از یک عدد اول موجود است.

فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}[x]$ باشد. میدان $\mathbb{F}[x]/(p(x))$ متشکل از کلاس‌های همنهشتی را با $\mathbb{K}$ نشان دهید. طبق قضایای ۸.۵ و ۹.۵، $\mathbb{F}$ زیرمیدانی از میدان $\mathbb{K}$ است. $\mathbb{K}$ یک **توسیع میدان** $\mathbb{F}$ نیز نامیده می‌شود. چندجمله‌ای‌های در $\mathbb{F}[x]$ را می‌توان با ضرایب در میدان بزرگتر $\mathbb{K}$ در نظر گرفت، و بنابراین می‌توان از ریشه‌های چنین چندجمله‌ای‌هایی در $\mathbb{K}$ صحبت به میان آورد. بویژه می‌توان از ریشه‌های چندجمله‌ای $p(x)$ که بحث خود را ابتدا از آن شروع کردیم سؤال کرد. اگرچه $p(x)$ در $\mathbb{F}[x]$ تحویل‌ناپذیر است، با این حال ممکن است دارای ریشه‌هایی در توسیع میدان $\mathbb{K}$ باشد.

مثال ۱۱.۵. چندجمله‌ای $p(x) = x^2 + x + 1$ دارای هیچ ریشه‌ای در $\mathbb{Z}_2$ نیست و بنابراین طبق نتیجه ۱۴.۴، تحویل‌ناپذیر در $\mathbb{Z}_2[x]$ است. در نتیجه طبق قضیه ۹.۵، $\mathbb{Z}_2[x]/(x^2 + x + 1)$ یک توسیع میدان $\mathbb{Z}_2$ است. با استفاده از جدول مربوط به $\mathbb{K}$ در مثال ۱۰.۵ می‌بینیم که

$$[x^2] + [x] + 1 = [x + 1] + [x] + 1 = 1 + 1 = 0.$$

در صورت استفاده از نمادی متفاوت، این مطلب ممکن است کمی ساده‌تر درک شود. قرار دهید $\alpha = [x]$. در این صورت طبق محاسبات بالا $\alpha^2 + \alpha + 1 = 0$؛ یعنی، α یک ریشه $p(x) = x^2 + x + 1$ در $\mathbb{K}$ است. نکته مهم در اینجا این است که در واقع برای اثبات این که α یک ریشه $p(x)$ است نیازی به جداول مربوط به $\mathbb{K}$ نداریم زیرا می‌دانیم که (پیمانه $x^2 + x + 1$) $x^2 + x + 1 \equiv 0$. در نتیجه $[x^2 + x + 1] = 0$ در $\mathbb{K}$، و طبق تعریف

حساب کلاس‌های همنهشتی،

$$\alpha^۲ + \alpha + ۱ = [x]^۲ + [x] + ۱ = [x^۲ + x + ۱] = ۰.$$

در حالت کلی قضیه زیر را داریم:

قضیه ۱۰.۵. فرض کنید $\mathbb{F}$ یک میدان و $p(x)$ یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}[x]$ باشد. در این صورت $\mathbb{F}[x]/(p(x))$ یک میدان توسیع $\mathbb{F}$ است و ریشه‌ای از $p(x)$ را شامل می‌باشد.

برهان. فرض کنید $\mathbb{K} = \mathbb{F}[x]/(p(x))$. در این صورت طبق قضایای ۸.۵ و ۹.۵، $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ است. فرض کنید $\alpha = [x]$ در $\mathbb{K}$. نشان خواهیم داد که α یک ریشه $p(x)$ است. طبق تعریف حساب کلاس‌های همنهشتی در $\mathbb{K}$،

$$\begin{aligned} a_n\alpha^n + \cdots + a_۱\alpha + a_۰ &= a_n[x]^n + \cdots + a_۱[x] + a_۰ \\ &= [a_n x^n + \cdots + a_۱ x + a_۰] \\ &= [p(x)] = ۰_{\mathbb{F}} \qquad [p(x) \equiv ۰_{\mathbb{F}} \ (p(x)) \text{ زیرا (پیمانه}]. \end{aligned}$$

بنابراین α یک ریشه $p(x)$ است. ■

نتیجه ۱۱.۵. فرض کنید $\mathbb{F}$ یک میدان و $f(x)$ یک چندجمله‌ای غیرثابت در $\mathbb{F}[x]$ باشد. در این صورت یک توسیع میدان $\mathbb{K}$ از $\mathbb{F}$ وجود دارد که یک ریشه $f(x)$ را شامل است.

برهان. طبق قضیه ۱۰.۴، $f(x)$ دارای یک عامل تحویل‌ناپذیر $p(x)$ در $\mathbb{F}[x]$ است. طبق قضیه ۱۰.۵، $\mathbb{K} = \mathbb{F}[x]/(p(x))$ یک توسیع میدان $\mathbb{F}$ است که یک ریشه از $p(x)$ را شامل است. چون هر ریشه $p(x)$ یک ریشه $f(x)$ است، $\mathbb{K}$ یک ریشه $f(x)$ را شامل است. ■

نتایج قضیه ۱۰.۵ از آنچه که در ابتدا به نظر می‌رسید بسیار عمیق‌تر است. در سرتاسر تاریخ ریاضیات، عبور از یک دستگاه اعداد شناخته شده به یک دستگاه بزرگتر جدید اغلب با شک و سوءظن روبرو بوده است. در قرون وسطی، بعضی از ریاضیدانان از پذیرش وجود اعداد منفی اجتناب می‌کردند. هنگامی که اعداد مختلط در قرن هفدهم معرفی شد تردیدهایی در مورد آن وجود داشت که تا قرن نوزدهم نیز ادامه یافت، زیرا برخی از ریاضیدانان ایدهٔ وجود عددی با مربع -۱ را نمی‌پذیرفتند. یکی از دلایل بروز چنین مشکلاتی فقدان یک چهارچوب نظری مناسب برای نگرش

به چنین مسائلی بود. جبر مجرد چنین چهارچوبی را مهیا می‌کند. قضیه ۱۰.۵ و نتیجه آن این شک و عدم اطمینان را برطرف می‌نماید.

یک دیدگاه سازنده برای درنظرگرفتن اعداد مختلط این است که بجای سؤال در مورد عددی با مربع ۱−، پرسیده شود که"آیا میدانی وجود دارد که میدان حقیقی $\mathbb{R}$ را شامل بوده و چندجمله‌ای x^2+1 در آن دارای یک ریشه باشد؟" چون x^2+1 در $\mathbb{R}[x]$ تحویل‌ناپذیر است. قضیه ۱۰.۵ به ما می‌گوید که جواب مثبت است: $\mathbb{K}=\mathbb{R}[x]/(x^2+1)$ یک توسیع میدان $\mathbb{R}$ است که ریشه‌ای از x^2+1، یعنی $\alpha=[x]$ را شامل است. در میدان $\mathbb{K}$، α عنصری است که مربع آن ۱− است. امّا میدان $\mathbb{K}$ چگونه با میدان اعداد مختلط که پیشتر در این کتاب معرفی شد مرتبط است؟

همانگونه که در مثال ۵.۵ توجه داده شد، هر عضو $\mathbb{K}=\mathbb{R}[x]/(x^2+1)$ را می‌توان به طور منحصر به فردی به صورت $[ax+b]$ نوشت که در آن $a,b\in\mathbb{R}$. چون هر عضو r در $\mathbb{R}$ با عضو $[r]$ در $\mathbb{K}$ یکی‌گیری می‌شود، می‌بینیم که هر عضو $\mathbb{K}$ را می‌توان به طور منحصر به‌فردی به صورت زیر نوشت:

$$[a+bx]=[a]+[b][x]=a+b\alpha.$$

جمع در $\mathbb{K}$ توسط قانون زیر داده شده است:

$$\begin{aligned}(a+b\alpha)+(c+d\alpha)&=[a+bx]+[c+dx]=[(a+bx)+(c+dx)]\\&=[(a+c)+(b+d)x]=[a+c]+[b+d][x].\end{aligned}$$

بنابراین

$$(a+b\alpha)+(c+d\alpha)=(a+c)+(b+d)\alpha.$$

ضرب در $\mathbb{K}$ طبق قانون زیر داده شده است:

$$\begin{aligned}(a+b\alpha)(c+d\alpha)&=[a+bx][c+dx]=[(a+bx)(c+dx)]\\&=[ac+(ad+bc)x+bdx^2]\\&=ac+(ad+bc)\alpha+bd\alpha^2.\end{aligned}$$

امّا، α یک ریشه x^2+1 است، و لذا $\alpha^2=-1$. بنابراین قانون ضرب در $\mathbb{K}$ به صورت زیر در می‌آید:

$$(a+b\alpha)(c+d\alpha)=(ac-bd)+(ad+bc)\alpha.$$

اگر بجای نماد α نماد i را قرار دهیم در این صورت این قوانین به قوانین معمولی برای جمع و ضرب اعداد مختلط تبدیل می‌شود. به زبان رسمی، میدان $\mathbb{K}$ یکریخت با میدان $\mathbb{C}$ است، تحت یکریختی f که توسط ضابطهٔ $f(a+b\alpha)=a+bi$ تعریف می‌شود.

تا این لحظه میدان اعداد مختلط $\mathbb{C}$ را شناخته شده فرض کرده بودیم. اکنون دیدیم که میدان $\mathbb{K}$ که در بالا ساخته شد با میدان $\mathbb{C}$ یکریخت است. بنابراین بجای فرض هرگونه اطلاع قبلی در مورد اعداد مختلط می‌توان از مثال قبل به عنوان یک تعریف استفاده کرد. به عبارت دیگر، می‌توان $\mathbb{C}$ را میدان $\mathbb{R}[x]/(x^2+1)$ تعریف کرد. به وضوح چنین تعریفی پیچیده‌تر از آن است که برای دانش‌آموزان دبیرستانی بکار رود، لیکن این تعریف برای دانشجویان جاافتاده دارای این مزیت مسلّم است که هرگونه سوءظن مداوم دربارهٔ اعتبار اعداد مختلط و اعمال حسابی آنها را برطرف می‌کند[1]. احتمالاً در صورت وجود چنین تعریفی در چندین قرن پیش، اعداد مختلط می‌توانست بدون ایجاد هیچگونه اضطرابی معرفی شود.

تمرینها

توجه. $\mathbb{F}$ همواره یک میدان را نشان می‌دهد.

۱.A. اگر $a\in\mathbb{F}$، میدان $\mathbb{F}[x]/(x-a)$ را توصیف کنید.

۲.B. (الف) بررسی کنید که $\mathbb{Q}(\sqrt{2})=\{r+s\sqrt{2}\mid r,s\in\mathbb{Q}\}$ یک زیرمیدان $\mathbb{R}$ است.

(ب) نشان دهید که $\mathbb{Q}(\sqrt{2})$ یکریخت با $\mathbb{Q}[x]/(x^2-2)$ است. [راهنمایی: تمرین ۶ بخش ۲.۵ می‌تواند مفید باشد.]

۳. (الف) بررسی کنید که $\mathbb{Q}(\sqrt{3})=\{r+s\sqrt{3}\mid r,s\in\mathbb{Q}\}$ یک زیرمیدان $\mathbb{R}$ است.

(ب) نشان دهید که $\mathbb{Q}(\sqrt{3})$ یکریخت با $\mathbb{Q}[x]/(x^2-3)$ است.

۴. فرض کنید $p(x)$ تحویل‌ناپذیر در $\mathbb{F}[x]$ باشد. بدون استفاده از قضیه ۹.۵، ثابت کنید که اگر در $\mathbb{F}[x]/(p(x))$ داشته باشیم $[f(x)][g(x)]=[0_{\mathbb{F}}]$ در این صورت $[f(x)]=[0_{\mathbb{F}}]$ یا $[g(x)]=[0_{\mathbb{F}}]$. [راهنمایی: تمرین ۴ بخش ۱.۵]

---

۱) تنها تغییری جزئی در تنظیم کتاب لازم است تا چنین تعریفی جا داده شود. تعداد کمی از مثال‌های فصل ۳ می‌بایست حذف شود، و بحث تحویل‌ناپذیری در $\mathbb{C}[x]$ و $\mathbb{R}[x]$ (بخش ۶.۴) می‌بایست به تعویق افتد. کلیه مطالب میانی فصل ۵ مستقل از هر اطلاع رسمی در مورد اعداد مختلط می‌باشد.

۵. فرض کنید $p(x)$ تحویل‌ناپذیر در $\mathbb{F}[x]$ باشد. اگر در $\mathbb{F}[x]/(p(x))$ داشته باشیم $[f(x)] \neq [0_{\mathbb{F}}]$ و $h(x) \in \mathbb{F}[x]$، ثابت کنید که $g(x) \in \mathbb{F}[x]$ وجود دارد به قسمی که در $\mathbb{F}[x]/(p(x))$، $[f(x)][g(x)] = [h(x)]$. [راهنمایی: تمرین ۵ بخش ۳.۲ را ملاحظه کنید.]

۶. اگر $p(x)$ یک چندجمله‌ای درجه دوم تحویل‌ناپذیر در $\mathbb{F}[x]$ باشد، نشان دهید که $\mathbb{F}[x]/(p(x))$ همه ریشه‌های $p(x)$ را شامل است.

۷. اگر $f(x) \in \mathbb{F}[x]$ دارای درجه n باشد، ثابت کنید که یک توسیع $\mathbb{E}$ از میدان $\mathbb{F}$ وجود دارد به قسمی که برای برخی $c_i \in \mathbb{E}$ (که لزوماً متمایز نیستند)، $f(x) = c_0(x-c_1)(x-c_2)\cdots(x-c_n)$. به عبارت دیگر، $\mathbb{E}$ همه ریشه‌های $f(x)$ را شامل است.

۸. (الف) نشان دهید که $\mathbb{Z}_2[x]/(x^3+x+1)$ یک میدان است.

(ب) نشان دهید که میدان $\mathbb{Z}_2[x]/(x^3+x+1)$ هر سه ریشهٔ x^3+x+1 را شامل است.

۹. نشان دهید که $\mathbb{Q}[x]/(x^2-2)$ با $\mathbb{Q}[x]/(x^2-3)$ یکریخت نیست. [راهنمایی: تمرین‌های ۲ و ۳ می‌تواند مفید باشد.]

۱۰.C. نشان دهید که هر چندجمله‌ای از درجه ۱، ۲ یا ۴ در $\mathbb{Z}_2[x]$ دارای یک ریشه در $\mathbb{Z}_2[x]/(x^4+x+1)$ می‌باشد.

* * * * *

فصل ششم

ایده‌آلها و حلقه‌های خارج قسمتی

مفهوم همنهشتی در مجموعه اعداد صحیح ما را به مجموعه متناهی $\mathbb{Z}_n$ و انجام اعمال حسابی در آن رهنمون ساخت و کمکی در ترغیب ما برای تعریف یک حلقه نیز بود. همنهشتی در حلقه چندجمله‌ای‌های $\mathbb{F}[x]$ کلاس جدیدی از حلقه‌ها متشکل از انواع حلقه‌های $\mathbb{F}[x]/(p(x))$ را بدست داد. این حلقه‌ها ما را قادر ساخت تا توسیع‌های میدان $\mathbb{F}$ را که ریشه‌های چندجمله‌ای $p(x)$ را شامل است بسازیم. در این فصل مفهوم همنهشتی به حلقه‌های دلخواه تعمیم داده می‌شود. این امر موجب تولید حلقه‌های بیشتر، و درک عمیق‌تر از ساختار جبری آنها می‌شود.

خواهید دید که بیشتر مباحث این فصل، دقیقاً مشابه توسعه بحث همنهشتی در $\mathbb{Z}$ (فصل ۲) و در $\mathbb{F}[x]$ (فصل ۵) می‌باشد. البته نتایج بدست آمده در این فصل به طور چشمگیری وسیع‌تر از نتایج قبلی هستند.

۱-۶ ایده‌آلها و همنهشتی

هدف این است که مفهومی از همنهشتی در حلقه‌های دلخواه را چنان بسط و توسعه دهیم که به‌عنوان حالات خاص، همنهشتی به پیمانه n در $\mathbb{Z}$ و همنهشتی به پیمانه $p(x)$ در $\mathbb{F}[x]$ را در برگیرد. اینک بحث خود را با نگاهی مجدد ولی متفاوت به برخی از مثال‌های همنهشتی در $\mathbb{Z}$ و $\mathbb{F}[x]$ آغاز می‌کنیم.

مثال ۱.۶. در حلقه $\mathbb{Z}$، $a \equiv b$ (پیمانه ۳) بدین معنی است که $a-b$ مضربی از ۳ است. فرض کنید I مجموعه همه مضارب ۳ باشد، لذا

$$I = \{0, \pm 3, \pm 6, \dots\}.$$

در این صورت همنهشتی به پیمانه ۳ می‌تواند به صورت زیر مشخص شود:

$$a \equiv b \text{ (پیمانه ۳)} \quad \text{یعنی} \quad a-b \in I.$$

مشاهده کنید که زیرمجموعه I، در واقع یک زیرحلقه $\mathbb{Z}$ است (مجموع و حاصل‌ضرب مضارب ۳، مضاربی از ۳ هستند). به علاوه، حاصل‌ضرب هر عدد صحیح در مضربی از ۳، مضربی از ۳ خواهد بود. بنابراین زیرحلقه I دارای خاصیت زیر است:

هرگاه $k \in \mathbb{Z}$ و $i \in I$، در این صورت $ki \in I$.

مثال ۲.۶. نماد $f(x) \equiv g(x)$ (x^2-2) (پیمانه ۲ $-x^2$) در حلقه چندجمله‌ای‌های $\mathbb{Q}[x]$ بدین معنی است که $f(x)-g(x)$ مضربی از x^2-2 است. فرض کنید I مجموعه همه مضارب x^2-2 در $\mathbb{Q}[x]$ باشد، یعنی $I = \{h(x)(x^2-2) \mid h(x) \in \mathbb{Q}[x]\}$. بررسی این که I زیر حلقه‌ای از $\mathbb{Q}[x]$ با خاصیت زیر است چندان مشکل نیست:

هرگاه $h(x) \in \mathbb{Q}$ و $t(x) \in I$، در این صورت $h(x)t(x) \in I$.

(حاصل ضرب هرچندجمله‌ای در مضربی از x^2-2، مضربی از x^2-2 است.) همنهشتی به پیمانه x^2-2 می‌تواند برحسب I چنین توصیف شود:

$$f(x) \equiv g(x) \text{ (پیمانه } x^2-2) \quad \text{یعنی} \quad f(x)-g(x) \in I.$$

این مثال‌ها پیشنهاد می‌کند که همنهشتی در یک حلقه R می‌تواند برحسب برخی زیرحلقه‌های R تعریف شود. اگر I چنین زیرحلقه‌ای باشد، می‌توانیم (پیمانه I) $a \equiv b$ را به معنی $a - b \in I$ تعریف کنیم. زیرحلقه I ممکن است همانند مثال بالا مشتمل بر همه مضارب یک عضو ثابت باشد، امّا هیچ دلیلی بر محدودشدن به این وضعیت وجود ندارد. مثال‌های بالا نشان می‌دهد که خاصیت کلیدی برای چنین زیرحلقه I این است که I "حاصل‌ضربها را جذب کند". هرگاه عضوی از I را با هر عضو دلخواهی از حلقه (داخل یا خارج I) ضرب کنیم، نتیجه حاصل‌ضرب، عضوی از I است. مجموعه همه مضارب حلقه‌ای یک عضو ثابت دارای این خاصیت جذب است. خواهیم دید که بسیاری از زیرحلقه‌ای دیگر نیز دارای این خاصیت هستند. بدلیل نقش حیاتی چنین حلقه‌هایی در مباحث بعدی، لحظه‌ای درنگ می‌کنیم تا آنها را نامگذاری و خواص اساسی آنها را در نظر بگیریم.

تعریف. زیرحلقه I از یک حلقه R یک **ایده‌آل** نامیده می‌شود هرگاه

اگر $r \in R$ و $a \in I$، در این صورت $ra \in I$ و $ar \in I$.

لحاظ کردن هر دو شرط جذب $ra \in I$ و $ar \in I$ در این تعریف برای حلقه‌های ناجابجایی ضروری است. وقتی که R همانند مثال‌های قبلی جابجایی باشد، این شرط به $ra \in I$ کاهش می‌یابد.

مثال ۳.۶. ایده‌آل صفر در یک حلقه R عبارت است از مجموعه تک عضوی $\{0_R\}$. این یک زیرحلقه است که همه حاصل‌ضربها را جذب می‌کند زیرا برای هر $r \in R$، $r0_R = 0_R = 0_R r$. خود حلقه R نیز یک ایده‌آل است.

مثال ۴.۶. پیشتر دیده‌ایم که مجموعه I متشکل از همه مضارب ۳ یک ایده‌آل در $\mathbb{Z}$ است. به طور کلی‌تر، فرض کنید R هر حلقه جابجایی یکدار باشد و $c \in R$. فرض کنید I مجموعه همه مضارب c باشد، یعنی، $I = \{rc \mid r \in R\}$. در این صورت I یک ایده‌آل در R است (تمرین ۱). I ایده‌آل اصلی تولیدشده توسط c نامیده شده و معمولاً با (c) نشان داده می‌شود.

مثال ۵.۶. در حلقه چندجمله‌ای‌های با ضرایب صحیح $\mathbb{Z}[x]$، فرض کنید I مجموعه همه چندجمله‌ای‌هایی باشد که جمله ثابت آنها یک عدد صحیح زوج است. بنابراین $x^3 + x + 6$ در I است، امّا $4x^2 + 3$ در I نیست. بررسی کنید که I یک ایده‌آل در $\mathbb{Z}[x]$ است (تمرین ۲). ادعا

می‌کنیم که I یک ایده‌آل اصلی نیست. برای اثبات این مطلب، به خلاف فرض کنید که I از همه مضارب یک چندجمله‌ای $p(x)$ تشکیل شده است. چون چندجمله‌ای ثابت ۲ در I است، ۲ باید ضریبی از $p(x)$ باشد. طبق قضیه ۱.۴، این تنها در صورتی ممکن است که $p(x)$ دارای درجه ۰ باشد، یعنی اگر $p(x)$ ثابت باشد، مثلاً $p(x) = c$. چون $p(x) \in I$، ثابت c باید زوج باشد. چون ۲ یک مضرب $p(x) = c$ است، تنها احتمالات ممکن $c = \pm 2$ است. از طرف دیگر $x \in I$، زیرا این چندجمله‌ای دارای جمله ثابت زوج ۰ است. بنابراین x باید مضربی از $p(x) = \pm 2$ باشد. این غیرممکن است زیرا همه چندجمله‌ای‌های مورد بحث دارای ضرایب صحیح هستند. بنابراین I از همه مضارب $p(x)$ تشکیل نشده است و یک ایده‌آل اصلی نیست.

مثال ۶.۶. فرض کنید T حلقه تمام توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$ باشد که در مثال ۸.۳ توصیف شد. فرض کنید I زیرمجموعه‌ای از T باشد که از همه توابع g با $g(2) = 0$ تشکیل شده است. در این صورت I یک زیرحلقه T است (تمرین ۸ بخش ۱.۳). اگر f تابعی دلخواه در T باشد و اگر $g \in I$، در این صورت

$$(fg)(2) = f(2)g(2) = f(2) \cdot 0 = 0.$$

بنابراین $fg \in I$. به طور مشابه $gf \in I$. لذا I یک ایده‌آل در T است.

مثال ۷.۶. زیرحلقه $\mathbb{Z}$ در مجموعه اعداد گویا، یک ایده‌آل در $\mathbb{Q}$ نیست زیرا $\mathbb{Z}$ خاصیت جذب را دارا نیست. برای مثال $1/2 \in \mathbb{Q}$ و $5 \in \mathbb{Z}$، امّا $5/2$ در $\mathbb{Z}$ نیست.

مثال ۸.۶. اگر $M(\mathbb{R})$ حلقه ماتریس‌های 2×2 روی میدان اعداد حقیقی باشد، بررسی کنید که مجموعه I متشکل از همه ماتریسهایی به صورت $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ با $a, b \in \mathbb{R}$، یک زیرحلقه $M(\mathbb{R})$ است. به سادگی دیده می‌شود که I ضربهای از طرف چپ را جذب می‌کند:

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ra + sb & 0 \\ ta + ub & 0 \end{pmatrix}.$$

با این حال I یک ایده‌آل در $M(\mathbb{R})$ نیست زیرا ممکن است I ضربهای از طرف راست را جذب

نکند، برای مثال

$$\begin{pmatrix} ۱ & ۰ \\ ۲ & ۰ \end{pmatrix}\begin{pmatrix} ۳ & ۴ \\ ۵ & ۶ \end{pmatrix} = \begin{pmatrix} ۳ & ۴ \\ ۶ & ۸ \end{pmatrix}.$$

بعضاً گفته می‌شود که I یک **ایده‌آل چپ** است، امّا یک ایده‌آل دوطرفه در $M(\mathbb{R})$ نیست.

قضیه زیر اغلب بررسی ایده‌آل بودن یک زیرمجموعه بخصوص از یک حلقه را ساده می‌نماید.

قضیه ۱.۶. یک زیرمجموعه غیرتهی I از یک حلقه R یک ایده‌آل است اگر و تنها اگر دارای خواص زیر باشد:

(i) اگر $a, b \in I$، در این صورت $a - b \in I$؛

(ii) اگر $r \in R$ و $a \in I$ در این صورت $ra \in I$ و $ar \in I$.

برهان. بوضوح هر ایده‌آل دارای این دو خاصیت است. بالعکس، فرض کنید I دارای خواص (i) و (ii) باشد. برای اثبات زیرحلقه بودن I، لازم است بررسی کنیم که I تحت جمع و ضرب بسته است، که $۰_R \in I$، و این که وارون جمعی هر عضو I، در I است. بقیه اصول حلقه (شرکت‌پذیری، توزیع‌پذیری، غیره) به طور خودکار برقرار است، زیرا آنها برای تمام عناصر R برقرارند. چون I غیرتهی است، عضو a وجود دارد با $a \in I$. با بکار بردن (i) با $a = b$، می‌بینیم که $a - a = ۰_R$ در I است. حال اگر $d \in I$، در این صورت طبق (i)، $۰_R - d = -d$ نیز در I است. سرانجام اگر $c, d \in I$، در این صورت $-d \in I$ و لذا طبق (i)، $c - (-d) = c + d$ در I است. بنابراین I تحت جمع بسته است.

خاصیت (ii) نشان می‌دهد که ضرب در یک عضو I همواره عضوی از I را تولید می‌کند. بویژه، حاصلضرب هر دو عضو از I باید در I باشد. بنابراین I تحت ضرب بسته است، و یک ایده‌آل می‌باشد. ■

حال که با ایده‌آلها آشنا شده‌اید می‌توانیم همنهشتی در یک حلقه دلخواه را تعریف کنیم:

تعریف. فرض کنید I یک ایده‌آل در حلقه R باشد و $a, b \in R$. در این صورت **a همنهشت با b به پیمانه I** است [نوشته می‌شود $a \equiv b \ (I)$ (پیمانه I)] اگر $a - b \in I$.

مثال ۱.۶ نشان می‌دهد که همنهشتی به پیمانه ۳ در اعداد صحیح همان همنهشتی به پیمانه

ایده‌آل I است، که در آن I ایده‌آل اصلی (۳) متشکل از همه مضارب ۳ می‌باشد. به طور مشابه، مثال ۲.۶ نشان می‌دهد که همنهشتی به پیمانه $x^۲ - ۲$ در $\mathbb{Q}[x]$ همان همنهشتی به پیمانه ایده‌آل اصلی $(x^۲ - ۲)$ است. بنابراین همنهشتی به پیمانه یک ایده‌آل به‌عنوان یک حالت خاص، مفاهیم همنهشتی در $\mathbb{Z}$ و $\mathbb{F}[x]$ را که پیشتر در این کتاب بکار برده شد، در بر دارد.

مثال ۹.۶. فرض کنید T حلقه همه توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$ باشد و I ایده‌آل همه توابع پیوسته g باشد به قسمی که $g(۲) = ۰$. اگر $f(x) = x^۲ + ۶$ و $h(x) = ۵x$، در این صورت تابع $f - h$ در I است زیرا

$$(f - h)(۲) = f(۲) - h(۲) = (۲^۲ + ۶) - (۵ \times ۲) = ۰$$

بنابراین $f \equiv h$ (پیمانه I).

قضیه ۲.۶. فرض کنید I ایده‌آلی در حلقه R باشد. در این صورت رابطه همنهشتی به پیمانه I دارای خواص زیر است:

(۱) انعکاسی: برای هر $a \in R$ (پیمانه I) $a \equiv a$؛

(۲) متقارن: اگر (پیمانه I) $a \equiv b$، در این صورت (پیمانه I) $b \equiv a$ ؛

(۳) متعدی: اگر (پیمانه I) $a \equiv b$ و (پیمانه I) $b \equiv c$ در این صورت (پیمانه I) $a \equiv c$.

این قضیه، قضایای ۱.۲ و ۱.۵ را تعمیم می‌دهد. مشاهده کنید که اثبات زیر تقریباً با اثبات قضیه ۱.۲ یکسان است ـ تنها عبارت "بخشپذیری بر n" را با عبارت "یک عضو I است" عوض کنید.

برهان قضیه ۲.۶. (۱) $a - a = ۰_R \in I$ ؛ بنابراین (پیمانه I) $a \equiv a$.

(۲) (پیمانه I) $a \equiv b$ بدین معنی است که برای برخی $i \in I$، $a - b = i$. بنابراین $b - a = -(a - b) = -i$. چون I یک ایده‌آل است، منفی یک عضو I نیز در I قرار دارد، و لذا $b - a = -i \in I$. بنابراین (پیمانه I) $b \equiv a$.

(۳) اگر (پیمانه I) $a \equiv b$ و (پیمانه I) $b \equiv c$، در این صورت طبق تعریف همنهشتی، عناصر i و j در I وجود دارد به قسمی که $a - b = i$ و $b - c = j$. بنابراین $a - c = (a - b) + (b - c) = i + j$. چون ایده‌آل I تحت جمع بسته است، $i + j \in I$ و بنابراین (پیمانه I) $a \equiv c$. ■

قضیه ۳.۶. فرض کنید I ایده‌آلی در یک حلقه R باشد. اگر $a \equiv b\ (I$ پیمانه$)$ و $c \equiv d\ (I$ پیمانه$)$، در این صورت

(۱) $a + c \equiv b + d\ (I$ پیمانه$)$؛

(۲) $ac \equiv bd\ (I$ پیمانه$)$.

این قضیه، قضایای ۲.۲ و ۱.۵ را تعمیم می‌دهد. وقتی عبارات را به زبان ایده‌آلها تغییر دهیم اثبات این قضیه کاملاً مشابه اثبات قضایای یادشده می‌باشد.

برهان قضیه ۳.۶. (۱) طبق تعریف همنهشتی، $i, j \in I$ وجود دارند به قسمی که $a - b = i$ و $c - d = j$. پس $(a + c) - (b + d) = (a - b) + (c - d) = i + j \in I$. بنابراین داریم $a + c \equiv b + d\ (I$ پیمانه$)$.

(۲) $ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d) = ic + bj$. چون ایده‌آل I حاصل‌ضربهای از طرف چپ و راست را جذب می‌کند، $ic \in I$ و $bj \in I$. بنابراین $ac - bd = ic + bj \in I$. پس $ac \equiv bd\ (I$ پیمانه$)$. ■

اگر I ایده‌آلی در یک حلقه R باشد و $a \in R$، در این صورت کلاس همنهشتی a به پیمانه I عبارت است از مجموعه همه عناصر R که همنهشت با a به پیمانه I هستند، یعنی، مجموعه

$$\begin{aligned}\{b \in R \mid b \equiv a\ (I \text{ پیمانه})\} &= \{b \in R \mid b - a \in I\} \\ &= \{b \in R \mid b - a = i,\ \ i \in I\} \\ &= \{b \in R \mid b = a + i,\ \ i \in I\} \\ &= \{a + i \mid i \in I\}.\end{aligned}$$

به این دلیل، کلاس همنهشتی a به پیمانه I را با نماد $a + I$ به جای نماد $[a]$ که در $\mathbb{Z}$ و $\mathbb{F}[x]$ بکار برده شد نشان می‌دهیم. علامت جمع در $a + I$ تنها یک نماد رسمی است؛ ما جمع یک عنصر و یک ایده‌آل را تعریف نکرده‌ایم. در این سیاق، کلاس همنهشتی $a + I$ معمولاً **یک هم‌مجموعه (چپ)** نامیده می‌شود.

قضیه ۴.۶. فرض کنید I ایده‌آلی در یک حلقه R باشد و $a, c \in R$. در این صورت

(پیمانه I) $a \equiv c$ اگر و تنها اگر $a + I = c + I$.

برهان. با تغییرات جزیی در نمادها، اثبات قضیه ۳.۲ تقریباً بدون کم و کاست در اینجا بکار می‌رود. صرفاً، "پیمانه n" را با "پیمانه I" و "$[a]$" را با "$a + I$" عوض کنید؛ قضیه ۲.۶ را به جای قضیه ۱.۲ بکار برید. ■

قضیه ۵.۶. فرض کنید I ایده‌آلی در یک حلقه R باشد. در این صورت هر دو هم‌مجموعه I یا مجزا و یا برابرند.

برهان. همان اثبات نتیجه ۲.۴ را پس از تغییرات مناسب در نمادها، بکار برید. ■

اگر I ایده‌آلی در یک حلقه R باشد، در این صورت مجموعهٔ همه هم‌مجموعه‌های I (کلاس‌های همنهشتی به پیمانه I) با R/I نشان داده می‌شود.

مثال ۱۰.۶. فرض کنید I ایده‌آل اصلی (۳) در حلقه $\mathbb{Z}$ باشد. در این صورت هم‌مجموعه‌های I همان کلاس‌های همنهشتی به پیمانه ۳ هستند و لذا سه هم‌مجموعهٔ متمایز وجود دارد: $[۰] = ۰ + I$، $[۱] = ۱ + I$ و $[۲] = ۲ + I$. مجموعه هم‌مجموعه‌های $\mathbb{Z}/I$، دقیقاً مجموعه $\mathbb{Z}_۳$ در نماد قبلی ما می‌باشد.

مثال ۱۱.۶. فرض کنید I ایده‌آلی در $\mathbb{Z}[x]$ باشد که از همه چندجمله‌ای‌هایی تشکیل شده است که دارای جمله ثابت زوج هستند. ادعا می‌کنیم که $\mathbb{Z}[x]/I$ دقیقاً از دو هم‌مجموعه متمایز $I + ۰$ و $I + ۱$ تشکیل شده است. برای دیدن این موضوع، یک هم‌مجموعه دلخواه $f(x) + I$ را در نظر بگیرید. جمله ثابت $f(x)$ یا زوج است و یا فرد. اگر $f(x)$ زوج باشد، در این صورت $f(x) \in I$ و لذا (پیمانه I) $f(x) \equiv ۰$. بنابراین طبق قضیه ۴.۶، $f(x) + I = ۰ + I$. اگر $f(x)$ دارای جمله ثابت فرد باشد، در این صورت $f(x) - ۱$ دارای جمله ثابت زوج است، در نتیجه (پیمانه I) $f(x) \equiv ۱$. بنابراین طبق قضیه ۴.۶، $f(x) + I = ۱ + I$.

مثال ۱۲.۶. فرض کنید T حلقه توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$ باشد و فرض کنید I ایده‌آل همه توابع پیوسته g باشد به قسمی که $g(۲) = ۰$. توجه کنید که برای هر عدد حقیقی r، تابع ثابت f_r (که ضابطهٔ آن $f_r(x) = r$ می‌باشد) یک عضو T است. فرض کنید $h(x)$ عضوی از T باشد. در

این صورت $h(۲)$ یک عدد حقیقی است، مثلاً $h(۲) = c$، و

$$(h - f_c)(۲) = h(۲) - f_c(۲) = c - c = ۰.$$

پس $h - f_c \in I$، لذا (پیمانه I) $h \equiv f_c$ و بنابراین $h + I = f_c + I$. در نتیجه، هر هم‌مجموعه از I را می‌توان به صورت $f_r + I$، برای برخی عدد حقیقی r نوشت. به‌علاوه اگر $c \neq d$، در این صورت $f_c(۲) \neq f_d(۲)$، پس $[f_c - f_d](۲) \neq ۰$ و $f_c - f_d \notin I$. لذا (پیمانه I) $f_c \not\equiv f_d$ و $f_c + I \neq f_d + I$. بنابراین تعداد نامتناهی هم‌مجموعه متمایز از I وجود دارد، یکی برای هر عدد حقیقی r.

تمرینها

توجه. R یک حلقه را نشان می‌دهد (که لزوماً جابجایی نیست).

A.۱. اگر R جابجایی و $c \in R$، ثابت کنید که $I = \{rc \mid r \in R\}$ یک ایده‌آل در R است. [تمرین ۹ را نیز ملاحظه کنید.]

۲. نشان دهید مجموعه I از همه چندجمله‌ای‌های با جمله ثابت زوج یک ایده‌آل در $\mathbb{Z}[x]$ است.

۳. نشان دهید مجموعه K از همه چندجمله‌ای‌های ثابت در $\mathbb{Z}[x]$ یک زیرحلقه است امّا یک ایده‌آل در $\mathbb{Z}[x]$ نیست.

۴. (الف) نشان دهید که مجموعه $I = \{(k, ۰) \mid k \in \mathbb{Z}\}$ یک ایده‌آل در حلقه $\mathbb{Z} \times \mathbb{Z}$ است.
(ب) نشان دهید که مجموعه $T = \{(k, k) \mid k \in \mathbb{Z}\}$ یک ایده‌آل در $\mathbb{Z} \times \mathbb{Z}$ نیست.

۵. در هر یک از حلقه‌های زیر ایده‌آلهای اصلی متمایز را فهرست کنید:

(الف) $\mathbb{Z}_۵$ (ب) $\mathbb{Z}_۹$ (پ) $\mathbb{Z}_{۱۲}$

۶. آیا مجموعه $J = \left\{ \begin{pmatrix} ۰ & ۰ \\ ۰ & r \end{pmatrix} \mid r \in \mathbb{R} \right\}$ یک ایده‌آل در حلقه $M(\mathbb{R})$ متشکل از ماتریس‌های ۲×۲ روی $\mathbb{R}$ است؟

۷. نشان دهید که مجموعه $K = \left\{ \begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ یک زیرحلقه $M(\mathbb{R})$ است که حاصل‌ضربهای از طرف راست را جذب می‌کند. نشان دهید K یک ایده‌آل نیست زیرا ممکن

است حاصل‌ضربهای از طرف چپ را جذب نکند. گاهی چنین مجموعه K یک ایده‌آل راست نامیده می‌شود.

۸. (الف) بررسی کنید که $I = \{۰, ۳\}$ یک ایده‌آل در $\mathbb{Z}_۶$ است و همه هم‌مجموعه‌های متمایز آن را فهرست کنید.

(ب) بررسی کنید که $I = \{۰, ۳, ۶, ۹, ۱۲\}$ یک ایده‌آل در $\mathbb{Z}_{۱۵}$ است و همه هم‌مجموعه‌های متمایز آن را فهرست کنید.

۹. فرض کنید R جابجایی باشد و $c \in R$. آیا c در ایده‌آل I که در تمرین ۱ تعریف شد قرار دارد؟ [راهنمایی، ایده‌آل $\{۲k \mid k \in E\}$ در حلقه اعداد زوج E را در نظر بگیرید. تمرین ۲۳ را نیز ملاحظه کنید.]

۱۰. (الف) نشان دهید که مجموعهٔ عناصر غیریکه در $\mathbb{Z}_۸$ یک ایده‌آل است.

(ب) قسمت (الف) را برای $\mathbb{Z}_۹$ انجام دهید. [تمرین ۲۴ را نیز ملاحظه کنید.]

۱۱. فرض کنید R یک حلقه یکدار باشد و فرض کنید I یک ایده‌آل در R باشد.

(الف) اگر $۱_R \in I$، ثابت کنید $I = R$.

(ب) اگر I یک یکه را شامل باشد، ثابت کنید $I = R$.

۱۲. نشان دهید که زیرمجموعه غیرتهی S از R یک زیرحلقه است اگر و تنها اگر S تحت ضرب بسته باشد و دارای این خاصیت باشد که: هرگاه $a, b \in S$، در این صورت $a - b \in S$. [با قضیه ۱.۶ مقایسه کنید.]

۱۳. اگر I ایده‌آلی در یک میدان $\mathbb{F}$ باشد، ثابت کنید که $I = (۰_{\mathbb{F}})$ یا $I = \mathbb{F}$. [راهنمایی: تمرین ۱۱.]

۱۴. (الف) اگر I و J ایده‌آلهایی در R باشند، ثابت کنید که $I \cap J$ یک ایده‌آل است.

(ب) اگر $\{I_k\}$ یک خانواده (احتمالاً نامتناهی) از ایده‌آلهای در R باشد، ثابت کنید که اشتراک همهٔ I_k ها یک ایده‌آل است.

۱۵. با ارائه مثالی در $\mathbb{Z}$ نشان دهید که اجتماع دو ایده‌آل (به‌عنوان دو مجموعه) ممکن است یک ایده‌آل نباشد (در حقیقت، ممکن است حتی یک زیرحلقه هم نباشد).

۱۶. اگر I یک ایده‌آل در R و S یک زیرحلقه R باشد، ثابت کنید که $I \cap S$ یک ایده‌آل در S است.

۱۷. فرض کنید I و J ایده‌آلهایی در R باشند. ثابت کنید که مجموعه $K = \{a + b \mid a \in I, b \in J\}$ یک ایده‌آل در R است که هر دو I و J را شامل است. K را **مجموع I و J** نامند و با $I + J$ نشان می‌دهند.

۱۸. اگر I یک ایده‌آل در R و J یک ایده‌آل در حلقه S باشد، ثابت کنید که $I \times J$ یک ایده‌آل در حلقه $R \times S$ است.

۱۹. با ارائه مثالی نشان دهید که در یک حلقه ناجابجایی R با $c \in R$، مجموعه $\{rc \mid r \in R\}$ لزوماً یک ایده‌آل نیست. [با تمرین ۱ مقایسه کنید.]

۲۰.B. فرض کنید I و J ایده‌آلهایی در R باشند. فرض کنید IJ مجموعه همه مجموع‌های متناهی از عناصر R به صورت ab (با $a \in I$ و $b \in J$) را نشان دهد. ثابت کنید که IJ یک ایده‌آل است.

۲۱. اگر در $\mathbb{Z}$، $(m, n) = 1$ ثابت کنید که $(m) \cap (n)$ برابر ایده‌آل (mn) است.

۲۲. فرض کنید R یک حلقه جابجایی یکدار باشد که تنها ایده‌آلهای آن 0_R و R است. ثابت کنید که R یک میدان است. [راهنمایی: اگر $a \neq 0_R$ با بکار بردن ایده‌آل (a) یک وارون ضربی برای a بیابید.]

۲۳. فرض کنید R یک حلقه جابجایی بدون عضو یک باشد و فرض کنید $a \in R$. نشان دهید که $A = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$ یک ایده‌آل است که a را شامل می‌شود، و این که هر ایده‌آل شامل a، A را نیز شامل است. A **ایده‌آل! اصلی تولیدشده توسط a** نامیده می‌شود.

۲۴. فرض کنید R یک حلقه جابجایی یکدار و N مجموعه عناصر غیریکه R باشد. با ارائه مثالی نشان دهید که N لزوماً یک ایده‌آل نیست.

۲۵. فرض کنید R یک دامنه صحیح باشد و $a, b \in R$. نشان دهید که $(a) = (b)$ اگر و تنها اگر برای برخی عضو یکه $u \in R$، $a = bu$.

۲۶. فرض کنید J ایده‌آلی در حلقه R باشد و فرض کنید I ایده‌آلی در J (که خود نیز یک حلقه

است) باشد. آیا I یک ایده‌آل در R است؟ اگر J یکدار باشد چه؟ (راهنمایی: اگر R یکدار باشد عضو یک در J لزوماً عضو 1_R حلقه R نیست.)

۲۷. اگر M ایده‌آلی در یک حلقه جابجایی و یکدار R باشد و اگر $a \in R$ با $a \notin M$، ثابت کنید که مجموعه

$$J = \{m + ra \mid r \in R, m \in M\}$$

یک ایده‌آل است و $M \subsetneq J$.

۲۸. اگر I یک ایده‌آل در R باشد، ثابت کنید که $I[x]$ (چندجمله‌ای‌های با ضرایب در I) یک ایده‌آل در حلقه چندجمله‌ای‌های $R[x]$ است.

۲۹. فرض کنید $f : R \to S$ یک همریختی حلقه‌ای باشد و فرض کنید

$$K = \{r \in R \mid f(r) = 0\}.$$

ثابت کنید K یک ایده‌آل در R است.

۳۰. فرض کنید J یک ایده‌آل در R باشد. ثابت کنید که مجموعه

$$I = \{r \in R \mid t \in J \text{ برای هر } rt = 0\}$$

یک ایده‌آل است.

۳۱. فرض کنید I یک ایده‌آل در R باشد، ثابت کنید که مجموعه

$$K = \{a \in R \mid r \in R \text{ برای هر } ra \in I\}$$

یک ایده‌آل است.

۳۲. فرض کنید T یک زیرمجموعه غیرتهی از حلقه R باشد. فرض کنید I اشتراک همه ایده‌آلهای در R که T را شامل هستند باشد (حداقل یک چنین ایده‌آلی وجود دارد، خود R). ثابت کنید که I یک ایده‌آل است. I **ایده‌آل تولیدشده توسط مجموعه** T نامیده می‌شود.

۳۳. فرض کنید I یک ایده‌آل در $\mathbb{Z}$ باشد به قسمی که $\mathbb{Z} \subseteq I \subseteq (۳)$. ثابت کنید که یا $I = (۳)$ یا $I = \mathbb{Z}$.

۳۴. ثابت کنید مجموعه عناصر پوچ‌توان در یک حلقه جابجایی R تشکیل یک ایده‌آل می‌دهد. [راهنمایی: تمرین ۳۲ بخش ۲.۳ را ملاحظه کنید.]

۳۵. (الف) ثابت کنید که مجموعه S متشکل از تمام کسرهای ساده گویا با مخرج فرد زیرحلقه‌ای از $\mathbb{Q}$ است.

(ب) فرض کنید I مجموعه عناصری از S با صورت زوج باشد. ثابت کنید که I یک ایده‌آل S است.

(پ) نشان دهید S/I دقیقاً از دو هم‌مجموعه متمایز تشکیل شده است.

۳۶. (الف) فرض کنید p یک عدد اول باشد و فرض کنید T مجموعه تمام کسرهای ساده گویایی باشد که مخرج آنها بر p بخش‌پذیر نیست. ثابت کنید که T یک حلقه است.

(ب) فرض کنید I مجموعه عناصری از T باشد که صورت آنها بر p بخش‌پذیر است. ثابت کنید که I یک ایده‌آل در T است.

(پ) نشان دهید که T/I از دقیقاً p هم‌مجموعه متمایز تشکیل شده است.

۳۷. فرض کنید J مجموعه همه چندجمله‌ای‌های با جمله ثابت صفر در $\mathbb{Z}[x]$ باشد.

(الف) نشان دهید J ایده‌آل اصلی (x) در $\mathbb{Z}[x]$ است.

(ب) نشان دهید که $\mathbb{Z}[x]/J$ از تعداد نامتناهی هم‌مجموعه‌های متمایز، یکی برای هر $n \in \mathbb{Z}$، تشکیل شده است.

۳۸. (الف) ثابت کنید مجموعه T متشکل از ماتریس‌های به صورت $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ با $a, b \in \mathbb{R}$ یک زیرحلقه $M(\mathbb{R})$ است.

(ب) ثابت کنید که مجموعه I متشکل از همه ماتریس‌های به صورت $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ با $b \in \mathbb{R}$ یک ایده‌آل در حلقه T است.

(پ) نشان دهید که هر هم‌مجموعه در T/I را می‌توان به صورت $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + I$ نوشت.

۳۹. (الف) ثابت کنید مجموعه S متشکل از ماتریس‌های به صورت $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ با $a, b, c \in \mathbb{R}$،

یک زیرحلقه $M(\mathbb{R})$ است.

(ب) ثابت کنید که مجموعه I متشکل از ماتریس‌های به صورت $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ با $b \in \mathbb{R}$ یک ایده‌آل در حلقه S است.

(پ) نشان دهید که تعداد نامتناهی هم‌مجموعه متمایز در S/I، یکی برای هر زوج در $\mathbb{R} \times \mathbb{R}$، وجود دارد.

۴۰. (الف) ثابت کنید که مجموعه J متشکل از همه چندجمله‌ای‌های در $\mathbb{Z}[x]$ که جمله ثابت آنها بر ۳ بخش‌پذیر است، یک ایده‌آل می‌باشد.

(ب) نشان دهید که J یک ایده‌آل اصلی نیست.

۴۱.C. ثابت کنید که هر ایده‌آل در $\mathbb{Z}$ یک ایده‌آل اصلی است. [راهنمایی: اگر I یک ایده‌آل غیرصفر در $\mathbb{Z}$ باشد، نشان دهید که I باید عدد مثبتی را شامل باشد؛ الگوریتم تقسیم را بکار برید تا نشان دهید که $I = (c)$، که در آن c کوچکترین عدد صحیح مثبت در I است.]

۴۲. فرض کنید $\mathbb{F}$ یک میدان باشد. ثابت کنید که هر ایده‌آل در $\mathbb{F}[x]$ یک ایده‌آل اصلی است. [راهنمایی: الگوریتم تقسیم را بکار برید تا نشان دهید که هر ایده‌آل غیرصفر I در $\mathbb{F}[x]$ برابر $(p(x))$ است که در آن $p(x)$ یک چندجمله‌ای با کوچکترین درجه مثبت در I است.]

۴۳. ثابت کنید که یک زیرحلقه S از $\mathbb{Z}_n$ یکدار است اگر و تنها اگر عضو u در S موجود باشد به قسمی که $u = u^2$ و S برابر ایده‌آل (u) باشد.

۴۴. نشان دهید که حلقه $M(\mathbb{R})$ دارای هیچ ایده‌آلی به جز ایده‌آل صفر و خود $M(\mathbb{R})$ نیست، با این حال $M(\mathbb{R})$ یک حلقه تقسیمی نیست.

۶-۲ حلقه‌های خارج قسمتی و همریختی‌ها

اینک نشان می‌دهیم که مجموعه کلاس‌های همنهشتی به پیمانه یک ایده‌آل، خود یک حلقه است. همان طور که احتمالاً انتظار دارید، این تعمیمی سرراست از آنچه که ما با کلاس‌های همنهشتی در $\mathbb{Z}$ و $\mathbb{F}[x]$ انجام دادیم می‌باشد. با این حال، احتمالاً انتظار این را نداشته‌اید که حلقه‌های کلاس‌های همنهشتی اخیر روابط نزدیکی با مباحث یکریختی‌ها و همریختی‌ها که در فصل ۳ مطالعه شد داشته

باشد. این روابط را به تفصیل مورد تحقیق قرار می‌دهیم و تصویر جدیدی از ساختار حلقه‌ها ارائه می‌کنیم.

فرض کنید I ایده‌آلی در یک حلقه R باشد. عناصر مجموعه R/I هم‌مجموعه‌های I (کلاس‌های همنهشتی به پیمانه I) می‌باشند، یعنی، همهٔ مجموعه‌هایی به صورت $a+I=\{a+i \mid i\in I\}$. به منظور تعریف جمع و ضرب هم‌مجموعه‌ها، همانگونه که با کلاس‌های همنهشتی در $\mathbb{Z}$ و $\mathbb{F}[x]$ انجام دادیم، به قضیه زیر احتیاج داریم:

قضیه ۶.۶. فرض کنید I ایده‌آلی از یک حلقه R باشد. اگر در R/I داشته باشیم، $a+I=c+I$ و $b+I=d+I$، در این صورت

$$(a+b)+I=(c+d)+I \qquad \text{و} \qquad ab+I=cd+I.$$

برهان. با تغییرات جزیی در نمادها، این تعمیمی از قضیه ۶.۲ است. $[a]$ را با $a+I$ جایگزین نمائید و با بکار بردن قضایای ۳.۶ و ۴.۶ بجای قضایای ۲.۲ و ۳.۲، اثبات قضیه ۶.۲ را عیناً بکار برید. ■

حال دقیقاً همانند آنچه که ما در مورد $\mathbb{Z}_n$ و $\mathbb{F}[x]/(p(x))$ انجام دادیم می‌توانیم جمع و ضرب در R/I را تعریف کنیم: مجموع دو هم‌مجموعه $a+I$ (کلاس همنهشتی a) و $c+I$ (کلاس همنهشتی c) عبارت است از هم‌مجموعه $(a+c)+I$ (کلاس همنهشتی $a+c$). به‌صورت نمادی،

$$(a+I)+(c+I)=(a+c)+I.$$

این گزاره ممکن است کمی مبهم باشد زیرا علامت جمع با سه معنی کاملاً متفاوت بکار رفته است:

به عنوان یک نماد رسمی برای نشان دادن یک هم‌مجموعه: $a+I$ ؛

به عنوان یک عمل روی عناصر R: $a+c$ ؛

به عنوان عمل جمع روی هم‌مجموعه‌ها که در حال تعریف آن می‌باشیم[۱].

۱) برای رفع این ابهام می‌توان از یک نماد متفاوت مانند $[a]$ برای هم‌مجموعه‌ها و یک نماد متفاوت مانند $\oplus$ برای جمع هم‌مجموعه‌ای استفاده کرد. با این حال استفاده از نماد فوق متداول است و هنگامی که به آن عادت کنید نباید ابهامی پیش بیاید.

نکته مهم این است که بدلیل قضیه ۶.۶ جمع هم‌مجموعه‌ای مستقل از انتخاب عناصر نماینده در هر هم‌مجموعه است. حتی اگر $a+I$ را با یک هم‌مجموعه برابر مانند $b+I$، و $c+I$ را با یک هم‌مجموعه برابر مانند $d+I$ جایگزین کنیم، هم‌مجموعه حاصل‌جمع، یعنی $(b+d)+I$، برابر $(a+b)+I$ است.

ضرب هم‌مجموعه‌ها به طور مشابه تعریف می‌شود و طبق قضیه ۶.۶ مستقل از انتخاب نماینده است:

$$(a+I)(c+I)=ac+I.$$

مثال ۱۳.۶. اگر I ایده‌آل (۳) در $\mathbb{Z}$ باشد، در این صورت جمع و ضرب هم‌مجموعه‌ها در $\mathbb{Z}/I$ همان جمع و ضرب کلاس‌های همنهشتی در فصل ۲ است. بنابراین $\mathbb{Z}/I$ چیزی نیست مگر $\mathbb{Z}_3$.

مثال ۱۴.۶. فرض کنید I ایده‌آل چندجمله‌ای‌های با جمله ثابت زوج در $\mathbb{Z}[x]$ باشد. همانگونه که در مثال ۱۱.۶ دیدیم، $\mathbb{Z}[x]/I$ تنها از دو هم‌مجموعه متمایز $0+I$ و $1+I$ تشکیل شده است. داریم $(1+1)+I=2+I=(1+I)+(1+I)$، اما $2\in I$، لذا (پیمانه I) $2\equiv 0$ و بنابراین $2+I=0+I$. محاسباتی مشابه جداول زیر را برای $\mathbb{Z}[x]/I$ تولید می‌کند. بسادگی دیده می‌شود که $\mathbb{Z}[x]/I$ یک حلقه (در حقیقت یک میدان) یکریخت با $\mathbb{Z}_2$ است:

$+$	$0+I$	$1+I$
$0+I$	$0+I$	$1+I$
$1+I$	$1+I$	$0+I$

$\cdot$	$0+I$	$1+I$
$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$

این مثال‌ها قضیه زیر را که از نقطه نظر آشنایی ما با خواص $\mathbb{Z}$ و $\mathbb{Z}[x]$ چندان تعجب‌آور نیست، نمایش می‌دهد.

قضیه ۷.۶. فرض کنید I ایده‌آلی از حلقه R باشد. در این صورت

(۱) R/I با جمع و ضرب هم‌مجموعه‌ای تعریف شده در بالا یک حلقه است.

(۲) اگر R جابجایی باشد، در این صورت R/I یک حلقه جابجایی است.

(۳) اگر R یکدار باشد، در این صورت حلقه R/I نیز یکدار است.

برهان. (۱) چنانچه در قضیه ۷.۲، نماد "$[a]$" را به نماد "$a+I$" تغییر دهید در این صورت برهان قضیه ۷.۲ به وضعیت حاضر انتقال می‌یابد، زیرا برهان تنها بستگی به این حقیقت دارد که $\mathbb{Z}$ یک حلقه است. به رغم این مطلب این حرف را حجت قرار نداده و برهان را به تفصیل برای خودتان بنویسید.

(۲) اگر R جابجایی باشد و $a,c \in R$، در این صورت $ac = ca$. در نتیجه، در R/I داریم $(a+I)(c+I) = ac+I = ca+I = (c+I)(a+I)$. بنابراین R/I جابجایی است.

(۳) عضو یک در R/I هم‌مجموعه 1_R+I است زیرا $(a+I)(1_R+I) = a1_R+I = a+I$ و به‌طور مشابه $(1_R+I)(a+I) = a+I$. ■

حلقه R/I، **حلقه خارج قسمتی** (یا **حلقه عامل**) R بوسیله I نامیده می‌شود. گاهی گفته می‌شود که ایده‌آل I را فاکتورگرفته تا حلقه خارج‌قسمتی R/I بدست آید. حلقه‌های خارج قسمتی تعمیم طبیعی حساب کلاس همنهشتی در $\mathbb{Z}$ و $\mathbb{F}[x]$ می‌باشند. با این حال همانگونه که اغلب در ریاضیات اتفاق می‌افتد مفهومی که با یک ایده فکری پرورش می‌یابد ممکن است با مفاهیم مهم دیگر ریاضی مرتبط باشد. این دقیقاً وضعیت موجود است. اینک خواهیم دید که مفهوم همریختی که در مطالعه یکریختی حلقه‌ها در فصل ۳ ظاهر شد رابطه نزدیکی با ایده‌آلها و حلقه‌های خارج قسمتی دارد.

قضیه ۸.۶. فرض کنید $f : R \to S$ یک همریختی حلقه‌ای باشد و فرض کنید $K = \{r \in R \mid f(r) = 0_S\}$. در این صورت K یک ایده‌آل در حلقه R است.

برهان. اگر $a,b \in K$ در این صورت $f(a-b) = f(a) - f(b) = 0_S - 0_S = 0_S$. بنابراین $a,b \in K$ نتیجه می‌دهد $a-b \in K$. اگر $r \in R$ و $a \in K$، در این صورت $f(ar) = f(a)f(r) = 0_S f(r) = 0_S$ و $f(ra) = f(r)f(a) = f(r)0_S = 0_S$. پس $ra \in K$ و $ar \in K$. بنابراین طبق قضیه ۱.۶، K یک ایده‌آل است. ■

ایده‌آل K در قضیه ۸.۶، **هسته همریختی** f نامیده می‌شود. وقتی که هسته یک ایده‌آل در R "بزرگ" باشد، در این صورت تعداد زیادی از عناصر غیرصفر R تحت f به 0_S نگاشته می‌شوند.

طرف دیگر این مسئله این است که هسته‌ای با کوچکترین اندازه ممکن داشته باشیم، یعنی، ایده‌آل صفر. در این حالت قضیه زیر را داریم.

قضیه ۹.۶. فرض کنید $f : R \to S$ یک همریختی حلقه‌ای با هسته K باشد. در این صورت $K = (0_R)$ اگر و تنها اگر f یک به یک باشد.

برهان. فرض کنید $K = (0_R)$ و $f(a) = f(b)$. در این صورت چون f یک همریختی است، $f(a-b) = f(a) - f(b) = 0_S$. پس $a-b$ در هسته K است، لذا $a - b = 0_R$ و $a = b$. بنابراین f یک به یک است. برعکس، اگر f یک به یک باشد و $f(c) = 0_S$، در این صورت طبق قضیه ۱۰.۳، $f(c) = f(0_R)$، از یک به یک بودن بدست می‌آوریم $c = 0_R$. پس هسته K از تک عنصر 0_R تشکیل شده است. ■

قضیه ۸.۶ بیان می‌کند که هر هسته یک ایده‌آل است، برعکس هر ایده‌آل، هسته یک همریختی است:

قضیه ۱۰.۶. فرض کنید I ایده‌آلی از یک حلقه R باشد. در این صورت نگاشت $\pi : R \to R/I$ که توسط $\pi(r) = r + I$ تعریف می‌شود یک همریختی پوشا با هسته I است.

نگاشت π، **همریختی طبیعی** از R به R/I نامیده می‌شود.

برهان قضیه ۱۰.۶. نگاشت π پوشا است زیرا به ازای هر هم‌مجموعه مفروض $r + I$ در R/I، $\pi(r) = r + I$. تعریف جمع و ضرب در R/I نشان می‌دهد که π یک همریختی است:

$$\pi(r+s) = (r+s) + I = (r+I) + (s+I) = \pi(r) + \pi(s),$$

$$\pi(rs) = rs + I = (r+I)(s+I) = \pi(r)\pi(s).$$

هسته π عبارت است از مجموعه عناصر $r \in R$ به قسمی که $\pi(r) = 0_R + I$ (عضو صفر در R/I). امّا $\pi(r) = 0_R + I$ اگر و تنها اگر $r + I = 0_R + I$ و این اتفاق می‌افتد اگر و تنها اگر $r \equiv 0_R$ (پیمانه I)، یعنی اگر و تنها اگر $r \in I$. بنابراین I هسته π است. ■

همریختی طبیعی π در قضیه ۱۰.۶ حالت خاصی از یک وضعیت عمومی‌تر است. اگر $f : R \to S$ یک همریختی پوشای حلقه‌ای باشد، S را یک **تصویر همریختی** R می‌نامیم. اگر

f یک یکریختی باشد (بنابراین S یک تصویر یکریختی R است)، در این صورت می‌دانیم که R و S دارای ساختاری یکسان هستند. هرگاه یکی از آنها دارای خاصیت جبری بخصوصی باشد، دیگری نیز دارای آن است. اگر f یکریختی نباشد، در این صورت خواص یک حلقه ممکن است در حلقه دیگر برقرار نباشد. با این حال خواص S و همریختی f، اغلب اطلاعات مفیدی درباره R بدست می‌دهند. مقایسه این موضوع با مجسمه‌سازی و عکس‌برداری می‌تواند مفید باشد: اگر $f : R \to S$ یک یکریختی باشد، در این صورت S یک کپی سه- بعدی دقیق از R است. اگر f تنها یک همریختی پوشا باشد، در این صورت S یک تصویر عکسبرداری دو - بعدی از R است که در آن برخی ویژگیهای R به‌طور دقیقی انعکاس می‌یابد امّا خواص دیگر تغییر شکل‌یافته و یا از دست می‌روند. قضیه بعد دقیقاً به ما می‌گوید که چگونه R، S و هسته f به یکدیگر مربوط هستند.

قضیه ۱۱.۶. (**اولین قضیه یکریختی**) فرض کنید $f : R \to S$ یک همریختی پوشای حلقه‌ای با هسته K باشد. در این صورت حلقه خارج قسمتی R/K یکریخت با S است.

این قضیه بیان می‌کند که هر تصویر همریختی یک حلقه R به صورت R/K، برای برخی ایده‌آل K است. بنابراین حلقه‌های خارج قسمتی ممکن R عیناً همان تصویرهای همریختی R هستند. ایده‌آل K میزان از دست رفتن اطلاعات در عبور از حلقه R به تصویر همریختی R/K را اندازه می‌گیرد. وقتی $K = (0_R)$، در این صورت طبق قضیه ۹.۶، f یک یکریختی است و هیچ اطلاعاتی از بین نمی‌رود. امّا وقتی K بزرگ باشد، اطلاعات نسبتاً زیادی ممکن است از دست رود.

برهان قضیه ۱۱.۶. اگر $r + K = t + K$، در این صورت طبق قضیه ۴.۶، $r - t \in K$. در نتیجه، چون f یک همریختی است، $f(r) - f(t) = f(r - t) = 0_S$. بنابراین $r + K = t + K$ نتیجه می‌دهد که $f(r) = f(t)$. پس، مستقل از این که هم‌مجموعه $r + K$ چگونه نوشته شود، نگاشت $\varphi : R/K \to S$ که توسط ضابطهٔ $\varphi(r + K) = f(r)$ داده می‌شود یک تابع خوش‌تعریف است. اگر $s \in S$، در این صورت چون f پوشا است، برای برخی $r \in R$، $s = f(r)$. پس $s = f(r) = \varphi(r + K)$ و لذا φ پوشا است. اگر $\varphi(r + K) = \varphi(c + K)$، در این صورت $f(r) = f(c)$، لذا $f(r) - f(c) = f(r - c) = 0_S$. بنابراین $r - c \in K$ که طبق قضیه ۴.۶ نتیجه می‌دهد $r + K = c + K$. پس φ یک به یک است. سرانجام φ یک همریختی است

چون f چنین است:

$$\varphi[(c+K)(d+K)] = \varphi(cd+K) = f(cd) = f(c)f(d)$$
$$= \varphi(c+K)\varphi(d+K)$$

و

$$\varphi[(c+K)+(d+K)] = \varphi[(c+d)+K] = f(c+d) = f(c)+f(d)$$
$$= \varphi(c+K)+\varphi(d+K).$$

بنابراین $\varphi : R/K \to S$ یک یکریختی است. ■

همانگونه که در مثال‌های زیر خواهید دید، اولین قضیه یکریختی ابزار مفیدی برای تعیین ساختار حلقه‌های خارج قسمتی است.

مثال ۱۵.۶. اگر $f(x)$ یک چندجمله‌ای در $\mathbb{Z}[x]$ باشد، در این صورت جمله ثابت آن عنصری از $\mathbb{Z}$ است. تابع $\theta : \mathbb{Z}[x] \to \mathbb{Z}$ را با نگاشتن هر چندجمله‌ای در $\mathbb{Z}[x]$ به جمله ثابت آن در $\mathbb{Z}$ تعریف کنید. مطمئناً نگاشت θ پوشاست زیرا هر $k \in \mathbb{Z}$ تصویر چندجمله‌ای $x+k$ در $\mathbb{Z}[x]$ است. بررسی این که θ یک همریختی حلقه‌ای است مشکل نیست (تمرین ۱). هسته θ متشکل از چندجمله‌ای‌هایی است که به‌صفر $\mathbb{Z}$ نگاشته می‌شوند، یعنی چندجمله‌ای‌هایی در $\mathbb{Z}[x]$ با جمله ثابت صفر. امّا چندجمله‌ای‌های با جمله ثابت صفر دقیقاً چندجمله‌ای‌هایی هستند که x را به‌عنوان یک عامل دارند. برطبق قضیه ۱۱.۶، حلقه خارج قسمتی $\mathbb{Z}[x]/(x)$ یکریخت با $\mathbb{Z}$ است.

مثال ۱۶.۶. فرض کنید T حلقه توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$ باشد و I ایده‌آل همه توابع g باشد به قسمی که $g(۲) = ۰$. در مثال ۱۲.۶ دیدیم که T/I تشکیل شده است از هم‌مجموعه‌های $f_r + I$، یکی برای هر عدد حقیقی r، که در آن $f_r : \mathbb{R} \to \mathbb{R}$ تابع ثابتی است که توسط $f_r(x) = r$، برای هر x، تعریف می شود. این امر، امکان یکریخت بودن حلقه T/I با میدان $\mathbb{R}$ را پیشنهاد می‌کند. اینک با بکاربردن قضیه ۱۱.۶ و ساختن یک همریختی پوشا از T به $\mathbb{R}$ که هسته آن ایده‌آل I است، نشان می‌دهیم که این مطلب در واقع درست است. فرض کنید $\varphi : T \to \mathbb{R}$ تابعی باشد که توسط

$\varphi(f) = f(۲)$ تعریف شده است. در این صورت φ پوشا است زیرا برای هر عدد حقیقی r، $r = f_r(۲) = \varphi(f_r)$. به‌علاوه φ یک همریختی حلقه‌ای است:

$$\varphi(f+h) = (f+h)(۲) = f(۲) + h(۲) = \varphi(f) + \varphi(h),$$
$$\varphi(fh) = (fh)(۲) = f(۲)h(۲) = \varphi(f)\varphi(h).$$

بنا به تعریف، هسته φ عبارت است از مجموعه $\{g \in T \mid g(۲) = ۰\} = \{g \in T \mid \varphi(g) = ۰\}$. بنابراین هسته φ دقیقاً برابر ایده‌آل I است. برطبق قضیه ۱۱.۶، T/I یکریخت با $\mathbb{R}$ است.

تمرینها

۱.A. نشان دهید که نگاشت $\theta : \mathbb{Z}[x] \to \mathbb{Z}$ که هرچندجمله‌ای $f(x)$ را به جمله ثابت آن می‌نگارد یک همریختی است.

۲. نشان دهید که تنها تصاویر همریختی یک میدان $\mathbb{F}$ (تا حد یکریختی) خود $\mathbb{F}$ و حلقه صفر می‌باشد. [راهنمایی: تمرین ۱۳ بخش ۱.۶ را ملاحظه کنید.]

۳. اگر $\mathbb{F}$ یک میدان، R یک حلقه ناصفر، و $f : \mathbb{F} \to R$ یک همریختی پوشا باشد، ثابت کنید که f یک یکریختی است.

۴. فرض کنید $[a]_n$ کلاس همنهشتی عدد صحیح a به پیمانه n را نشان دهد.

(الف) نشان دهید که نگاشت $f : \mathbb{Z}_{۱۲} \to \mathbb{Z}_۴$ که $[a]_{۱۲}$ را به $[a]_۴$ می‌نگارد یک همریختی پوشای خوش‌تعریف است.

(ب) هسته f را بیابید.

۵. فرض کنید I یک ایده‌آل در یک دامنه صحیح R باشد. آیا این درست است که R/I نیز یک دامنه صحیح است؟

۶. (الف) همه ایده‌آلهای $\mathbb{Z}_{۱۲}$ را فهرست کنید.

(ب) برای هر ایده‌آل در قسمت (الف)، جداول جمع و ضرب $\mathbb{Z}_{۱۲}/I$ را بنویسید.

(پ) نشان دهید که هر تصویر همریختی $\mathbb{Z}_{۱۲}$ یکریخت با یکی از حلقه‌های ۰، $\mathbb{Z}_۲$، $\mathbb{Z}_۳$، $\mathbb{Z}_۴$، $\mathbb{Z}_۶$ و یا $\mathbb{Z}_{۱۲}$ می‌باشد.

۷. فرض کنید که T حلقه مضارب ۳ در $\mathbb{Z}$ باشد. فرض کنید $I = \{0, \pm 6, \pm 12, \pm 18, \ldots\}$.

(الف) نشان دهید که I یک ایده‌آل در (۳) است.

(ب) جداول جمع و ضرب T/I را بنویسید و بررسی کنید که T/I یک میدان است. توجه کند که T/I دارای یک همانی ضربی است حتی اگر T فاقد چنین عضوی باشد.

۸. (الف) در $\mathbb{Z}_6$ فرض کنید $I = \{0, 3\}$. بررسی کنید که I یک ایده‌آل است و نشان دهید که $\mathbb{Z}_6/I \cong \mathbb{Z}_3$.

(ب) در $\mathbb{Z}_{10}$ فرض کنید $J = \{0, 5\}$. بررسی کنید که J یک ایده‌آل است و نشان دهید که $\mathbb{Z}_{10}/J \cong \mathbb{Z}_5$.

۹. اگر R یک حلقه باشد، نشان دهید که $R/(0_R) \cong R$.

۱۰.B. فرض کنید R و S حلقه باشند. نشان دهید که $\pi : R \times S \to R$ که توسط $\pi(r, s) = r$ تعریف می‌شود یک همریختی پوشا است که هسته آن یکریخت با S است.

۱۱. فرض کنید I و K ایده‌آلهایی در یک حلقه R باشند با $K \subseteq I$. ثابت کنید که $I/K = \{a + K \mid a \in I\}$ یک ایده‌آل در حلقه خارج قسمتی R/K است.

۱۲. (الف) فرض کنید $f : R \to S$ یک همریختی پوشای حلقه‌ای باشد و فرض کنید I یک ایده‌آل در R باشد. ثابت کنید که $f(I) = \{s \in S \mid s = f(a)$ برای برخی $a \in I\}$ یک ایده‌آل در S است.

(ب) با مثال نشان دهید که اگر f پوشا نباشد قسمت (الف) ممکن است غلط باشد.

۱۳. نشان دهید که نگاشت $\varphi : \mathbb{R}[x] \to \mathbb{R}$ که توسط $\varphi(f(x)) = f(1)$ تعریف می‌شود یک همریختی پوشا است که هسته آن ایده‌آل اصلی $(x - 1)$ است.

۱۴. فرض کنید I یک ایده‌آل در یک حلقه ناجابجایی R باشد به قسمی که برای هر $a, b \in R$، $ab - ba \in I$. ثابت کنید که R/I جابجایی است.

۱۵. فرض کنید I یک ایده‌آل در حلقه R باشد. ثابت کنید که هر عضو R/I دارای یک ریشه دوم است اگر و تنها اگر برای هر $a \in R$، عنصر $b \in R$ وجود داشته باشد به قسمی که $a - b^2 \in I$.

۱۶. فرض کنید I یک ایده‌آل در یک حلقه باشد. ثابت کنید که هر عضو در R/I یک جواب معادله $x^2 = x$ است اگر و تنها اگر برای هر $a \in R$، $a^2 - a \in I$.

۱۷. فرض کنید I ایده‌آلی در یک حلقه جابجایی R باشد. ثابت کنید R/I دارای یک عضو همانی است اگر و تنها اگر $e \in R$ وجود داشته باشد به قسمی که برای $a \in R$، $ea - a \in I$. [راهنمایی: برای مثال، تمرین ۷ را ملاحظه کنید.]

۱۸. فرض کنید $I \neq R$ ایده‌آلی در یک حلقه جابجایی یکدار R باشد. ثابت کنید که R/I یک دامنه صحیح است اگر و تنها اگر هرگاه $ab \in I$ آنگاه یا $a \in I$ یا $b \in I$.

۱۹. همه تصاویر همریختی ممکن $\mathbb{Z}$ را توصیف کنید. [راهنمایی: می‌توانید تمرین ۴۱ بخش ۱.۶ را فرض شده در نظر بگیرید.]

۲۰. فرض کنید R یک حلقه جابجایی یکدار باشد با این خاصیت که هر ایده‌آل در R یک ایده‌آل اصلی است. ثابت کنید که هر تصویر همریختی R نیز این خاصیت را دارد.

۲۱. (الف) نشان دهید که $R = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}$ یک حلقه یکدار است.

(ب) نشان دهید که نگاشت $f : R \to \mathbb{Z}$ که توسط $f \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = a$ تعریف می‌شود یک همریختی پوشا است.

(پ) هسته f چیست؟

۲۲. فرض کنید $f : R \to S$ یک همریختی حلقه‌ای با هسته K باشد. فرض کنید I یک ایده‌آل R باشد به قسمی که $I \subseteq K$. نشان دهید که $f : R/I \to S$ که توسط $\bar{f}(r+I) = f(r)$ داده شده است یک همریختی خوش‌تعریف است.

۲۳. اولین قضیه یکریختی را بکار برید تا نشان دهید که $\mathbb{Z}_{20}/(5) \cong \mathbb{Z}_5$.

۲۴. فرض کنید $f : R \to S$ یک همریختی حلقه‌ای باشد. اگر J یک ایده‌آل در S باشد و $I = \{r \in R \mid f(r) \in J\}$، ثابت کنید که I یک ایده‌آل در R است که هسته f را شامل می‌باشد.

۲۵. (الف) فرض کنید R یک حلقه یکدار باشد. نشان دهید که نگاشت $f : \mathbb{Z} \to R$ که توسط

$f(k) = k1_R$ تعریف می‌شود یک همریختی است.

(ب) نشان دهید که هسته f ایده‌آل (n) است، که در آن n مشخصهٔ R است. [راهنمایی: تمرین ۲۸ بخش ۲.۳ و تمرین ۴۱ بخش ۱.۶ را ملاحظه کنید.]

۲۶. حداقل سه عنصر خودتوان در حلقه خارج قسمتی $\mathbb{Q}[x]/(x^4 + x^2)$ بیابید. [تمرین ۲ بخش ۲.۳ را ملاحظه کنید.]

۲۷. فرض کنید R یک حلقه جابجایی و J ایده‌آل متشکل از همه عناصر پوچ‌توان R باشد. (همانند تمرین ۳۴ در بخش ۱.۶). ثابت کنید که حلقه خارج قسمتی R/J دارای هیچ عضو پوچ‌توان غیرصفر نیست.

۲۸. فرض کنید S و I همانند تمرین ۳۵ بخش ۱.۶ باشند. ثابت کنید که $S/I \cong \mathbb{Z}_2$.

۲۹. فرض کنید T و I همانند تمرین ۳۶ بخش ۱.۶ باشند. ثابت کنید که $T/I \cong \mathbb{Z}_p$.

۳۰. فرض کنید T و I همانند تمرین ۳۸ بخش ۱.۶ باشند. ثابت کنید که $T/I \cong \mathbb{R}$.

۳۱. فرض کنید S و I همانند تمرین ۳۹ بخش ۱.۶ باشند. ثابت کنید که $S/I \cong \mathbb{R} \times \mathbb{R}$.

۳۲.C. (دومین قضیه یکریختی) فرض کنید I و J ایده‌آلهایی در یک حلقه R باشند. در این صورت بنا به تمرین‌های ۱۶ و ۱۷ بخش ۱.۶، $I \cap J$ یک ایده‌آل در I است و J یک ایده‌آل در $I + J$ می‌باشد. ثابت کنید که $\frac{I}{I \cap J} \cong \frac{I+J}{J}$. [راهنمایی: نشان دهید که $f : I \to (I + J)/J$ که توسط $f(a) = a + J$ تعریف می‌شود یک همریختی پوشا با هسته $I \cap J$ است.]

۳۳. (سومین قضیه یکریختی) فرض کنید I و K ایده‌آلهایی در یک حلقه R باشند به قسمی که $K \subseteq I$. در این صورت بنا به تمرین ۱۱، I/K یک ایده‌آل در R/K است. ثابت کنید که $(R/K)/(I/K) \cong R/I$. [راهنمایی: نشان دهید که نگاشت $f : R/K \to R/I$ که توسط $f(r + K) = r + I$ تعریف می‌شود، یک همریختی پوشای خوش‌تعریف، با هستهٔ I/K است.]

۳۴. (الف) فرض کنید K یک ایده‌آل در یک حلقه R باشد. ثابت کنید که هر ایده‌آل در حلقه خارج قسمتی R/K به صورت I/K، برای برخی ایده‌آل I در R، می‌باشد. [راهنمایی: تمرین‌های ۱۱ و ۲۴.]

(ب) اگر $f : R \to S$ یک همریختی پوشای حلقه‌ای با هسته K باشد، ثابت کنید یک تابع یک به یک و پوشا از مجموعهٔ همه ایده‌آلهای S به مجموعه همه ایده‌آلهای R که K را شامل می‌باشند وجود دارد. [راهنمایی: قسمت (الف) و تمرین ۱۲.]

۶-۳ ساختار R/I وقتی که I اوّل یا بیشین است

حلقه‌های خارج قسمتی به عنوان تعمیمی طبیعی از حلقه‌های $\mathbb{Z}_p$ و $\mathbb{F}[x]/(p(x))$ توسعه یافتند. وقتی که p اول و $p(x)$ تحویل‌ناپذیر باشد، در این صورت $\mathbb{Z}_p$ و $\mathbb{F}[x]/(p(x))$ میدان هستند. در این بخش مشابه این وضعیت را برای حلقه‌های خارج قسمتی حلقه‌های جابجایی کاوش می‌کنیم و شرایط لازم را برای این که یک حلقه خارج قسمتی یک دامنه صحیح یا یک میدان باشد، تعیین خواهیم کرد.

اعداد اوّل در $\mathbb{Z}$ و چندجمله‌ای‌های تحویل‌ناپذیر در $\mathbb{F}[x]$ اساساً نقش یکسانی را در ساختار حلقه‌های کلاس همنهشتی بازی می‌کنند. اولین وظیفه ما در حلقه‌های دلخواه این است که راههای معقولی برای توصیف این نقش براساس ایده‌آلها بیابیم. بر طبق قضیه ۸.۱، یک عدد صحیح p (بجز ± 1) اوّل است اگر و تنها اگر p دارای این خاصیت باشد که: هرگاه $p|bc$ در این صورت $p|b$ یا $p|c$. گفتن این که $p|a$ بدین معنی است که a یک مضرب p است، یعنی a عضوی از ایده‌آل اصلی (p) متشکل از همه مضارب p است. این خاصیت اعداد اوّل را می‌توان برحسب ایده‌آلها به صورت زیر جمله‌بندی نمود:

اگر $p \neq \pm 1$، در این صورت p اول است اگر و تنها اگر
هرگاه $bc \in (p)$، در این صورت $b \in (p)$ یا $c \in (p)$.

شرط $p \neq \pm 1$ تضمین می‌کند که ۱ یک مضرب p نیست و بنابراین ایده‌آل (p) همه $\mathbb{Z}$ نیست. با بکار بردن این وضعیت به عنوان یک الگو، تعریف زیر را داریم.

تعریف. یک ایده‌آل P در یک حلقه جابجایی R **اول** نامیده می‌شود اگر $P \neq R$ و هرگاه $bc \in P$، در این صورت $b \in P$ یا $c \in P$.

مثال ۱۷.۶. همانگونه که در بالا نشان داده شد، هرگاه p یک عدد صحیح اول باشد، ایده‌آل اصلی (p) در $\mathbb{Z}$ اول است. از طرف دیگر، ایده‌آل $P = (۶)$ در $\mathbb{Z}$ اول نیست، زیرا $۲ \times ۳ \in P$

امّا $۲ \notin P$ و $۳ \notin P$.

مثال ۱۸.۶. ایده‌آل صفر در هر دامنه صحیح R اول است زیرا $ab = ۰_R$ نتیجه می‌دهد $a = ۰_R$ یا $b = ۰_R$.

مثال ۱۹.۶. قضیه ۸.۴ نشان می‌دهد که اگر $\mathbb{F}$ یک میدان و $p(x)$ در $\mathbb{F}[x]$ تحویل‌ناپذیر باشد، در این صورت ایده‌آل اصلی $(p(x))$ در $\mathbb{F}[x]$ اول است.

مثال ۲۰.۶. فرض کنید I ایده‌آل چندجمله‌ای‌های با جمله ثابت زوج در $\mathbb{Z}[x]$ باشد. در این صورت I ایده‌آل اصلی نیست (مثال ۵.۶) و به‌وضوح $I \neq \mathbb{Z}[x]$. فرض کنید $f(x) = a_n x^n + \cdots + a_۰$ و $g(x) = b_m x^m + \cdots + b_۰$ چندجمله‌ای‌هایی در $\mathbb{Z}[x]$ باشند به قسمی که $f(x)g(x) \in I$. در این صورت جمله ثابت $f(x)g(x)$، یعنی $a_۰b_۰$ باید زوج باشد. چون حاصل‌ضرب دو عدد صحیح فرد، فرد است نتیجه می‌گیریم که یا $a_۰$ زوج است (یعنی $f(x) \in I$) یا $b_۰$ زوج است (یعنی $g(x) \in I$). بنابراین I یک ایده‌آل اول است.

ایده‌آل I در مثال قبلی اول است و حلقه خارج قسمتی $\mathbb{Z}[x]/I$ یک میدان است (مثال ۱۴.۶ را ملاحظه کنید). به طور مشابه وقتی p اول باشد $\mathbb{Z}/(p) = \mathbb{Z}_p$ یک میدان است. با این حال، مثال بعدی نشان می‌دهد که با وجود اول بودن P ممکن است R/P یک میدان نباشد.

مثال ۲۱.۶. ایده‌آل اصلی (x) در حلقه $\mathbb{Z}[x]$ متشکل از چندجمله‌ای‌هایی است که مضارب x هستند، یعنی، چندجمله‌ای‌هایی با جمله ثابت صفر. بنابراین $(x) \neq \mathbb{Z}[x]$. فرض کنید $f(x) = a_n x^n + \cdots + a_۰$، $g(x) = b_m x^m + \cdots + b_۰$ و $f(x)g(x) \in (x)$، در این صورت جمله ثابت $f(x)g(x)$ یعنی $a_۰b_۰$ باید ۰ باشد. این تنها زمانی اتفاق می‌افتد که $a_۰ = ۰$ یا $b_۰ = ۰$، یعنی تنها اگر $f(x) \in (x)$ یا $g(x) \in (x)$. بنابراین (x) یک ایده‌آل اوّل است. با این حال طبق مثال ۱۵.۶ حلقه خارج قسمتی $\mathbb{Z}[x]/(x)$ یکریخت با $\mathbb{Z}$ است. بنابراین $\mathbb{Z}[x]/(x)$ یک دامنه صحیح است امّا یک میدان نیست.

از منظر مثال قبل، قضیه بعدی بهترین چیزی است که ما می‌توانیم با ایده‌آلهای اول انجام دهیم.

قضیه ۱۲.۶. فرض کنید P یک ایده‌آل در یک حلقه جابجایی یکدار باشد. در این صورت P

یک ایده‌آل اول است اگر و تنها اگر حلقه خارج قسمتی R/P یک دامنه صحیح باشد.

برهان. ما به دفعات از حقیقت زیر که نتیجه‌ای از قضیه ۴.۶ می‌باشد استفاده خواهیم کرد:

$$a + P = 0_R + P \quad \text{اگر و تنها اگر} \quad a \in P. \qquad (\star)$$

توجه کنید که طبق قضیه ۷.۶، R/P یک حلقه جابجایی یکدار است. شرط $P \neq R$ معادل بااین است که گفته شود $1_R \notin P$، زیرا هر ایده‌آل شامل 1_R باید همه حلقه باشد. امّا طبق $(\star)$، $1_R \notin P$ اگر و تنها اگر $1_R + P \neq 0_R + P$. تحت این شرایط R/P یک دامنه صحیح است اگر و تنها اگر R/P دارای هیچ مقسوم‌علیه صفر نباشد.

فرض کنید R/P یک دامنه صحیح باشد. اگر $bc \in P$، در این صورت بنا به $(*)$، $(b + P)(c + P) = bc + P = 0_R + P$. بنابراین P اول است.

حال فرض کنید P اول باشد. اگر $(b + P)(c + P) = 0_R + P$، در این صورت $bc + P = 0_R + P$ و بنا به $(*)$، $bc \in P$. بنابراین $b \in P$ یا $c \in P$. لذا $b + P = 0_R + P$ یا $c + P = 0_R + P$، بنابراین R/P دارای هیچ مقسوم‌علیه صفر نیست. پس R/P یک دامنه صحیح است. ■

چون حلقه خارج قسمتی به پیمانه یک ایده‌آل اول لزوماً یک میدان نیست، طبیعی است پرسیده شود که یک ایده‌آل در چه شرایطی باید صدق کند تا حلقه خارج قسمتی حاصل یک میدان باشد.

مثال ۲۲.۶. ایده‌آل (۳) در $\mathbb{Z}$ را در نظر بگیرید. می‌دانیم که $\mathbb{Z}/(۳) \cong \mathbb{Z}_۳$ یک میدان است. حال ایده‌آل (۳) را در نظر بگیرید. فرض کنید J یک ایده‌آل باشد به قسمی که $(۳) \subseteq J \subseteq \mathbb{Z}$. اگر $J \neq (۳)$ در این صورت $a \in J$ وجود دارد با $a \notin (۳)$. بویژه، $a \nmid ۳$، لذا ۳ و a نسبت به هم اول هستند. بنابراین اعداد صحیح u و v وجود دارد به قسمی که $۳u + av = ۱$. چون ۳ و a در ایده‌آل J هستند نتیجه می‌شود که $۱ \in J$. پس بنابه تمرین ۱۱ بخش ۱.۶، $J = \mathbb{Z}$ و لذا *هیچ ایده‌آلی به طور اکید بین (۳) و $\mathbb{Z}$ قرار ندارد.*

مثال ۲۳.۶. حلقه خارج قسمتی $\mathbb{Z}[x]/(x)$ یک میدان نیست. به‌علاوه ایده‌آل I متشکل از همه چندجمله‌ای‌های با جمله ثابت زوج، به طور اکید بین (x) و $\mathbb{Z}[x]$ قرار دارد، یعنی $(x) \subsetneq I \subsetneq \mathbb{Z}[x]$.

در اینجا یک تعریف رسمی از خاصیتی که توسط مثال‌های بالا پیشنهاد شد ارائه می‌شود:

تعریف. ایده‌آل M در یک حلقه R **بیشین** گفته می‌شود اگر $M \neq R$ و هرگاه J یک ایده‌آل باشد به قسمی که $M \subseteq J \subseteq R$، در این صورت یا $J = M$ یا $J = R$.

برای مثال ایده‌آل (۳) در $\mathbb{Z}$ بیشین است و ایده‌آل (x) در $\mathbb{Z}[x]$ بیشین نیست. توجه کنید که یک حلقه ممکن است بیشتر از یک ایده‌آل بیشین داشته باشد. هر دو ایده‌آل‌های $\{۰, ۲, ۴\}$ و $\{۰, ۳\}$ در $\mathbb{Z}_۶$ بیشین هستند. تعداد نامتناهی ایده‌آل بیشین در $\mathbb{Z}$ وجود دارد (تمرین ۳). ایده‌آلهای بیشین جواب زیر به سؤالی که در بالا مطرح شد را فراهم می‌کنند:

قضیه ۱۳.۶. فرض کنید M یک ایده‌آل در یک حلقه جابجایی یکدار R باشد. در این صورت M یک ایده‌آل بیشین است اگر و تنها اگر حلقه خارج قسمت R/M یک میدان باشد.

برهان. همانند اثبات قضیه ۱۲.۶، R/M یک حلقه جابجایی یکدار است و $M \neq R$ اگر و تنها اگر $1_R + M \neq 0_R + M$. در نتیجه R/M یک میدان است اگر و تنها اگر هر عضو غیرصفر دارای یک وارون ضربی باشد.

فرض کنید R/M یک میدان باشد و برای برخی ایده‌آل J، $M \subseteq J \subseteq R$. اگر $M \neq J$، در این صورت $a \in J$ وجود دارد با $a \notin M$. بنابراین در میدان R/M داریم $a + M \neq 0_R + M$، و لذا $a + M$ دارای یک وارون $b + M$ است یعنی $(a + M)(b + M) = ab + M = 1_R + M$. برطبق قضیه ۴.۶، (پیمانه M) $ab \equiv 1$، لذا برای برخی $m \in M$، $ab - 1_R = m$. بنابراین $1_R = ab - m$. چون a و m درایده‌آل J قرار دارند، نتیجه می‌شود که $1_R \in J$ و $J = R$. بنابراین M یک ایده‌آل بیشین است.

حال فرض کنید M بیشین باشد. اگر $a + M$ یک عضو غیرصفر R/M باشد، در این صورت $a \notin M$ (در غیر اینصورت $a + M$ باید هم‌مجموعه صفر باشد). بنابه تمرین ۲۷ بخش ۱.۶، مجموعهٔ $J = \{m + ra \mid r \in R, m \in M\}$ یک ایده‌آل در R است که M را شامل می‌شود. به‌علاوه $a = 0_R + 1_R a$ در J قرار دارد، لذا $M \neq J$. بدلیل بیشین بودن M، باید داشته باشیم $J = R$. بنابراین $1_R \in J$، که نتیجه می‌دهد برای برخی $m \in M$ و $c \in R$، $1_R = m + ca$. توجه کنید که $ca - 1_R = m \in M$، لذا (پیمانه M) $ca \equiv 1_R$ و بنابراین بر طبق قضیه ۴.۶، $ca + M = 1_R + M$. در نتیجه هم‌مجموعه $c + M$ وارون $a + M$ در R/M است:

$$(c + M)(a + M) = ca + M = 1_R + M.$$

بنابراین R/M یک میدان است. ■

نتیجه ۱۴.۶. در یک حلقه جابجایی یکدار R، هر ایده‌آل بیشین اوّل است.

برهان. اگر M یک ایده‌آل بیشین باشد، در این صورت طبق قضیه ۱۳.۶، R/M یک میدان است. لذا برطبق نتیجه ۸.۳، R/M یک دامنه صحیح است. بنابراین طبق قضیه ۱۲.۶، M اول است. ■

با استفاده از قضیه ۱۳.۶ می‌توان نشان داد که تعدادی از ایده‌آل‌های آشنا، بیشین هستند.

مثال ۲۴.۶. ایده‌آل I متشکل از همه چندجمله‌ای‌های با جمله ثابت زوج در $\mathbb{Z}[x]$ بیشین است. زیرا $\mathbb{Z}[x]/I$ یک میدان است (مثال ۱۴.۶ را ملاحظه کنید).

مثال ۲۵.۶. فرض کنید T حلقه توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$ باشد و فرض کنید I ایده‌آل همه توابع g باشد به قسمی که $g(۲) = ۰$. در مثال ۱۶.۶ دیدیم که T/I یک میدان یکریخت با $\mathbb{R}$ است. بنابراین I یک ایده‌آل بیشین در T است. می‌توان نشان داد که هر ایده‌آل بیشین در T از این نوع است.

تمرینها

A ۱. اگر n یک عدد صحیح مرکب باشد، ثابت کنید که (n) یک ایده‌آل اول در $\mathbb{Z}$ نیست.

۲. با ارائه یک مثال نشان دهید که اشتراک دو ایده‌آل اوّل لزوماً اول نیست.

۳. (الف) ثابت کنید که یک عدد صحیح غیرصفر p اول است اگر و تنها اگر ایده‌آل (p) در $\mathbb{Z}$ بیشین باشد.

(ب) فرض کنید $\mathbb{F}$ یک میدان باشد و $p(x) \in \mathbb{F}[x]$. ثابت کنید که $p(x)$ تحویل‌ناپذیر است اگر و تنها اگر ایده‌آل $(p(x))$ بیشین باشد.

۴. فرض کنید R یک حلقه جابجایی یکدار باشد. ثابت کنید که R یک دامنه صحیح است اگر و تنها اگر (۰_R) یک ایده‌آل اول باشد.

۵. همه ایده‌آلهای بیشین در $\mathbb{Z}_۶$ را فهرست کنید. همین کار را برای $\mathbb{Z}_{۱۲}$ انجام دهید.

۶. (الف) نشان دهید که دقیقاً یک ایده‌آل بیشین در $\mathbb{Z}_8$ وجود دارد. همین کار را برای $\mathbb{Z}_9$ انجام دهید.

(ب) نشان دهید که $\mathbb{Z}_{10}$ و $\mathbb{Z}_{12}$ بیشتر از یک ایده‌آل بیشین دارند.

۷. فرض کنید R یک حلقه جابجایی یکدار باشد. ثابت کنید که R یک میدان است اگر و تنها اگر (0_R) یک ایده‌آل بیشین باشد.

۸. اگر R یک حلقه جابجایی متناهی یکدار باشد، ثابت کنید که هر ایده‌آل اول در R بیشین است. [راهنمایی: قضیه ۹.۳.]

۹. فرض کنید R یک دامنه صحیح باشد که در آن هر ایده‌آل اصلی است. اگر (p) یک ایده‌آل اول در R باشد؛ ثابت کنید که p دارای این خاصیت است که: هرگاه p به صورت $p = cd$ تجزیه شود، در این صورت c یا d در R یکه است.

B ۱۰. فرض کنید p یک عدد اول ثابت و J مجموعه چندجمله‌ای‌های در $\mathbb{Z}[x]$ باشد که جمله ثابت آنها بر p بخش‌پذیر است. ثابت کنید که J یک ایده‌آل بیشین در $\mathbb{Z}[x]$ است.

۱۱. نشان دهید که ایده‌آل اصلی $(x-1)$ در $\mathbb{Z}[x]$ اول است امّا بیشین نیست.

۱۲. اگر p یک عدد صحیح اول باشد، ثابت کنید که $M = \{(pa, b) \mid a, b \in \mathbb{Z}\}$ یک ایده‌آل بیشین در $\mathbb{Z} \times \mathbb{Z}$ است.

۱۳. ایده‌آلی در $\mathbb{Z} \times \mathbb{Z}$ بیابید که اول است ولی بیشین نیست.

۱۴. اگر P یک ایده‌آل اول در یک حلقه جابجایی R باشد، آیا ایده‌آل $P \times P$ یک ایده‌آل اول در $R \times R$ است؟

۱۵. (الف) مجموعه اعداد صحیح با جمع معمولی و ضربی که توسط $ab = 0$ برای هر $a, b \in R$ تعریف می‌شود را با R نمایش دهید. نشان دهید که R یک حلقه جابجایی است.

(ب) نشان دهید که $M = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$ یک ایده‌آل بیشین در R است که اول نیست. توضیح دهید چرا این تمرین، نتیجه ۱۴.۶ را نقض نمی‌کند.

۱۶. نشان دهید که $M = \{0, \pm 4, \pm 8, \ldots\}$ یک ایده‌آل بیشین در حلقه اعداد صحیح زوج E است، امّا E/M یک میدان نیست. توضیح دهید چرا این امر، قضیه ۱۳.۶ را نقض نمی‌کند.

۱۷. فرض کنید $f : R \to S$ یک همریختی پوشا از حلقه‌های جابجایی باشد. اگر J یک ایده‌آل اول در S باشد و $I = \{r \in R \mid f(r) \in J\}$، ثابت کنید که I یک ایده‌آل اول در R است.

۱۸. فرض کنید P یک ایده‌آل در یک حلقه جابجایی R باشد و $P \neq R$. ثابت کنید که P اول است اگر و تنها اگر دارای این خاصیت باشد که: هرگاه A و B ایده‌آلهایی در R باشند به قسمی که $AB \subseteq P$، در این صورت $A \subseteq P$ یا $B \subseteq P$. [AB در تمرین ۲۰ بخش ۱.۶ تعریف شده است. این خاصیت به عنوان تعریف ایده‌آل اول در حلقه‌های غیرجابجایی بکار می‌رود.]

۱۹. فرض کنید که وقتی R یک حلقه غیرصفر یکدار باشد، در این صورت هر ایده‌آل R به جز خود R در یک ایده‌آل بیشین قرار دارد (اثبات این حقیقت خارج از حوزه این کتاب است). ثابت کنید که یک حلقه جابجایی یکدار R دارای یک ایده‌آل بیشین یکتاست اگر و تنها اگر مجموعه یکه‌های در R یک ایده‌آل باشد (چنین حلقه‌ای یک **حلقه موضعی** نامیده می‌شود).

۲۰.C. (الف) ثابت کنید که $R = \{a + bi \mid a, b \in \mathbb{Z}\}$ یک زیرحلقه $\mathbb{C}$ است و این که مجموعه $M = \{a + bi \mid ۳|b \text{ و } ۳|a\}$ یک ایده‌آل بیشین در R است. [راهنمایی: اگر $r + si \notin M$، در این صورت $r^۲ + s^۲ = (r+si)(r-si)$، $۳ \not| r$ یا $۳ \not| s$. نشان دهید که $۳ \not| r^۲ + s^۲$ را نمی‌شمارد. سپس نشان دهید که هر ایده‌آل شامل $r + si$ و M، ۱ را نیز شامل است.]
(ب) نشان دهید که R/M یک میدان است که ۹ عضو دارد.

۲۱. فرض کنید R همانند تمرین ۲۰ باشد. نشان دهید که $J = \{a + bi \mid ۵|b \text{ و } ۵|a\}$ یک ایده‌آل بیشین در R است. [راهنمایی: ایده‌آل اصلی $K = (۲ + i)$ را در R در نظر بگیرید.]

۲۲. فرض کنید R و J همانند تمرین ۲۱ باشند. نشان دهید که $R/J \cong \mathbb{Z}_۵ \times \mathbb{Z}_۵$.

۲۳. اگر R و K همانند تمرین ۲۱ باشند، نشان دهید که $R/K \cong \mathbb{Z}_۵$.

۲۴. ثابت کنید که $T = \{a + b\sqrt{۲} \mid a, b \in \mathbb{Z}\}$ یک زیرحلقه $\mathbb{R}$ است و $M = \{a + b\sqrt{۵} \mid ۵|b \text{ و } ۵|a\}$ یک ایده‌آل بیشین در T است.

* * * * *

فصل هفتم

گروهها

مبحث حلقه‌ها نقطه شروع طبیعی برای مطالعه جبر مجرد بود زیرا از پیش تا حد زیادی با بعضی حلقه‌های خاص (نظیر اعداد صحیح، اعداد حقیقی، و چندجمله‌ایها) آشنایی داشتید. اکنون وقت آن رسیده است که بعضی از دستگاههای جبری ناآشناتر مطرح در علوم و ریاضیات را در نظر بگیریم. مهمترین آنها مفهوم گروه می‌باشد که دستگاهی جبری است که تنها یک تک عمل دارد. گروهها به‌طور طبیعی در مطالعه تقارن، تبدیلات هندسی، نظریه کدگذاری جبری، و در تحلیل ریشه‌های معادلات چندجمله‌ای ظاهر می‌شوند.

در هفت بخش اوّل این فصل به بسط و توسعه برخی مفاهیم گروهی مشابه مفاهیمی که در مطالعه حلقه‌ها مفید بودند مانند زیرگروهها، یکریختی‌ها، همنهشتی‌ها، گروههای خارج قسمتی و همریختی‌ها می‌پردازیم. در دو بخش پایانی این فصل ساختار گروههای متناهی را، که موضوعی است با سبکی کاملاً متفاوت از نظریه حلقه‌ها، بررسی می‌کنیم.

۱-۷ تعریف گروه و مثال‌هایی از آن

گروه دستگاهی جبری با یک عمل است. همانگونه که خواهیم دید بعضی از گروهها با نادیده گرفتن یکی از اعمال حلقه‌ها و تمرکز روی عمل دیگر حلقه بدست می‌آیند. در عین حال بسیاری از گروهها دارای چنین ارتباط مستقیمی با حلقه‌ها نیستند. مهمترین این گروهها (آنهایی که از نظر تاریخی نقطه شروع نظریه گروهها بودند) از مطالعه جایگشتها بدست آمدند در نتیجه ما بحث خود را با مطالعه جایگشتها آغاز می‌کنیم.

به زبان ساده، یک جایگشت از یک مجموعه T، تنها یک جابجایی مکان عناصر T می‌باشد. برای مثال، شش جایگشت ممکن برای مجموعه $T = \{۱, ۲, ۳\}$ وجود دارد:

۱۲۳ ۱۳۲ ۲۱۳ ۲۳۱ ۳۱۲ ۳۲۱

هر ترتیبی این چنین، یک تابع دوسویی از T به T تعیین می‌کند: ۱ را به اولین عضو ترتیب، ۲ را به دومین عضو و ۳ را به سومین عضو می‌نگارد. برای مثال ترتیب ۱ ۳ ۲ تابع $f : T \to T$ با ضابطه $f(۱) = ۲$؛ $f(۲) = ۳$؛ $f(۳) = ۱$ را تعیین می‌کند. برعکس، هر تابع دوسویی از T به T یک جابجایی مکان از عناصر ۱، ۲، ۳ به $f(۱)$، $f(۲)$، $f(۳)$ را تعیین می‌کند. در نتیجه، ما یک **جایگشت از یک مجموعه** T را یک تابع دوسویی از T به T تعریف می‌کنیم. این تعریف ایدهٔ غیررسمی جابجایی مکان عناصر را در بردارد و دارای این مزیت است که قابل بکارگیری در مجموعه‌های نامتناهی است. با این حال، هم‌اکنون روی مجموعه‌های متناهی تمرکز می‌کنیم و نماد مناسبی برای پرداختن به جایگشتهای آنها تعیین می‌نمائیم.

مثال ۱.۷. فرض کنید $T = \{۱, ۲, ۳\}$. جایگشت f با ضابطهٔ $f(۱) = ۲$، $f(۲) = ۳$، $f(۳) = ۱$ را می‌توان با آرایه $\begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix}$ نمایش داد که در آن تصویر یک عضوِ ردیف اول در زیر

آن در ردیف دوم نوشته شده‌است. با بکار بردن این نماد [۱] شش جایگشت T عبارتند از

$$\begin{pmatrix}۱ & ۲ & ۳\\ ۱ & ۲ & ۳\end{pmatrix} \quad \begin{pmatrix}۱ & ۲ & ۳\\ ۱ & ۳ & ۲\end{pmatrix} \quad \begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۱ & ۳\end{pmatrix}$$
$$\begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۳ & ۱\end{pmatrix} \quad \begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۱ & ۲\end{pmatrix} \quad \begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۲ & ۱\end{pmatrix}.$$

چون ترکیب دو تابع دوسویی، خود دوسویی است[۲] ترکیب هر دو تا از این جایگشتها یکی از شش جایگشتِ فهرست بالاست. برای مثال اگر $f = \begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۲ & ۱\end{pmatrix}$ و $g = \begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۱ & ۳\end{pmatrix}$، در این صورت $f \circ g$ تابعی است که توسط

$$(f \circ g)(۱) = f(g(۱)) = f(۲) = ۲$$
$$(f \circ g)(۲) = f(g(۲)) = f(۱) = ۳$$
$$(f \circ g)(۳) = f(g(۳)) = f(۳) = ۱$$

داده شده است. بنابراین $f \circ g = \begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۳ & ۱\end{pmatrix}$. معمولاً ساده‌تر است که انجام این نوع محاسبات به صورت بصری و با دنبال کردن مسیر عناصر همان‌طوری که ابتدا g و سپس f را بکار می‌بریم دنبال شود؛ برای مثال،

$$\begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۲ & ۱\end{pmatrix} \circ \begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۱ & ۳\end{pmatrix} = \begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۳ & ۱\end{pmatrix}.$$

چنانچه مجموعه جایگشتهای T را با $S_۳$ نشان دهیم، در این صورت ترکیب توابع ($\circ$) یک عمل روی مجموعه $S_۳$ است با این خاصیت که:

اگر $f \in S_۳$ و $g \in S_۳$ در این صورت $f \circ g \in S_۳$.

---

۱) در اوایل قرن نوزدهم، هنگامی که تلاش می‌شد تا فرمول‌هایی مشابه به فرمول درجه دوم که بتواند در حل معادلات چندجمله‌ای با درجه بالاتر بکار رود، جایگشتها نقش کلیدی ایفا کردند. برای اطلاعات بیشتر فصل ۱۱ را ملاحظه کنید.

۲) پیوست ب را ملاحظه کنید.

چون ترکیب توابع شرکت‌پذیر است،[۳] می‌بینیم که

$$\text{برای هر } f,g,h \in S_3 \text{،} \quad (f \circ g) \circ h = f \circ (g \circ h).$$

بررسی کنید که جایگشت همانی $I = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۲ & ۳ \end{pmatrix}$ دارای این خاصیت است که

$$\text{برای هر } f \in S_3 \text{،} \quad I \circ f = f \quad \text{و} \quad f \circ I = f.$$

هر تابع دو سویی دارای وارون است؛[۴] در نتیجه اگر $f \in S_3$، در این صورت $g \in S_3$ وجود دارد به قسمی که

$$f \circ g = I \quad \text{و} \quad g \circ f = I.$$

برای مثال اگر $f = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۱ & ۲ \end{pmatrix}$، در این صورت $g = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix}$ زیرا

$$\begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۱ & ۲ \end{pmatrix} \circ \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix} = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۲ & ۳ \end{pmatrix}$$

و

$$\begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix} \circ \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۱ & ۲ \end{pmatrix} = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۲ & ۳ \end{pmatrix}.$$

وارون جایگشتهای دیگر در S_3 را تعیین کنید (تمرین ۱). سرانجام توجه کنید که $f \circ g$ ممکن است برابر $g \circ f$ نباشد؛ برای مثال

$$\begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۲ & ۱ \end{pmatrix} \circ \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۱ & ۳ \end{pmatrix} = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix}$$

امّا

$$\begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۱ & ۳ \end{pmatrix} \circ \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۲ & ۱ \end{pmatrix} = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۱ & ۲ \end{pmatrix}.$$

---

۳) پیوست ب را ملاحظه کنید.

۴) پیوست ب را ملاحظه کنید.

با تجرید خواص کلیدی S_3 تحت عمل ترکیب توابع، تعریف زیر را بدست می‌آوریم.

تعریف. مجموعه غیرتهی G همراه با یک عمل $*$ یک **گروه** نامیده می‌شود هرگاه در اصول زیر صدق کند:

۱. بسته‌بودن: اگر $a \in G$ و $b \in G$: در این صورت $a * b \in G$.

۲. شرکت‌پذیری: برای هر $a, b, c \in G$، $a * (b * c) = (a * b) * c$.

۳. عنصر $e \in G$ (که **عضو همانی** نامیده می‌شود) وجود دارد به قسمی که برای هر $a \in G$، $a * e = a = e * a$.

۴. برای هر $a \in G$، یک عنصر $d \in G$ وجود دارد (که **وارون** یا **معکوس** a نامیده می‌شود) به قسمی که $a * d = e$ و $d * a = e$.

گروه G **آبلی**[۵] نامیده‌می‌شود هرگاه در اصل زیر صدق کند:

۵. جابجایی: برای هر $a, b \in G$، $a * b = b * a$.

گروه G **متناهی** (یا از **مرتبه متناهی**) نامیده می‌شود اگر دارای تعداد متناهی عضو باشد. در این حالت، تعداد عناصر G را **مرتبه** G نامیده و با $|G|$ نشان می‌دهند. یک گروه با تعداد نامتناهی عضو را از **مرتبه نامتناهی** می‌نامند.

مثال ۲.۷. بحث قبل از تعریف نشان می‌دهد که S_3 یک گروه غیرآبلی از مرتبه ۶ است که عمل $*$ در آن، عمل ترکیب توابع است.

اگر R یک حلقه باشد، در این صورت R دارای دو عمل شرکت‌پذیر است و لذا این سوال طبیعی مطرح می‌شود که تحت کدام یک از این عمل‌ها، R یک گروه است. بررسی پنج اصل اول از اصول یک حلقه (اولین تعریف بخش ۱.۳) نشان می‌دهد که اینها با اصول پنج‌گانه یک گروه آبلی یکی هستند جایی که در آن عمل $*$، عمل $+$ است، عضو همانی e، عضو 0_R است، و وارون a، $-a$ است. بنابراین

هر حلقه تحت عمل جمع یک گروه آبلی است.

از اینجا به بعد هرگاه کلمه "گروه" را بدون هیچ قیدی در مورد $\mathbb{Z}$، $\mathbb{Z}_n$، $\mathbb{R}$ و یا حلقه‌های معروف دیگر بکار بریم منظور ما از عمل گروه، عمل جمع است.

اگرچه تحت عمل ضرب، یک حلقه غیرصفر هرگز یک گروه نیست (تمرین ۴)، امّا برخی

۵) به افتخار ریاضیدان نروژی آبل (N. H. Abel).

زیرمجموعه‌های یک حلقه ممکن است تحت عمل ضرب گروه باشند.

مثال ۳.۷. زیرمجموعه $\{1, -1, i, -i\}$ از اعداد مختلط تحت عمل ضرب یک گروه آبلی از مرتبه ۴ تشکیل می‌دهد. بسته بودن و این که ۱ عضو همانی است را می‌توانید به‌سادگی بررسی کنید. چون $i(-i) = 1$ لذا i و $-i$ وارون یکدیگر هستند؛ -1 وارون خودش است زیرا $(-1)(-1) = 1$. بنابراین اصل ۴ برقرار است.

مثال ۴.۷. اعداد گویای مثبت $\mathbb{Q}^{**}$ تحت ضرب تشکیل یک گروه آبلی نامتناهی می‌دهد، زیرا حاصل‌ضرب اعداد مثبت، مثبت است و ۱ عضو همانی است. وارون a، $1/a$ است. به‌طور مشابه اعداد حقیقی مثبت تحت عمل ضرب یک گروه آبلی تشکیل می‌دهد. با این حال، اعداد صحیح مثبت تحت عمل ضرب یک گروه نیست زیرا معادلهٔ $ax = 1$ (با $a \geq 2$) دارای هیچ جوابی در $\mathbb{Z}$ نیست، لذا a دارای هیچ وارونی تحت ضرب نیست (اصل ۴ برقرار نیست).

فرض کنید R یک حلقه یکدار و U مجموعهٔ یکه‌های[۶] در R باشد. هر حاصل‌ضربی از یکه‌ها، یک یکه است (تمرین ۷ بخش ۲.۳)، 1_R عضو همانی است و طبق تعریف عنصر یکه، اصل ۴ در U برقرار است. بنابراین

مجموعهٔ یکه‌های یک حلقه یکدار تحت عمل ضرب یک گروه است.

مثال ۵.۷. گروه ضربی یکه‌های $\mathbb{Z}_n$ را با U_n نشان دهید. بر طبق نتیجه ۹.۲، U_n متشکل از همه $a \in \mathbb{Z}_n$ است به قسمی که $(a, n) = 1$ (وقتی که a به‌عنوان یک عدد صحیح معمولی در نظر گرفته شود). بنابراین گروه یکه‌های $\mathbb{Z}_8$، $U_8 = \{1, 3, 5, 7\}$ می‌باشد و گروه یکه‌های $\mathbb{Z}_{15}$، $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ می‌باشد. در اینجا جدول عمل U_8 آمده است:

·	۱	۳	۵	۷
۱	۱	۳	۵	۷
۳	۳	۱	۷	۵
۵	۵	۷	۱	۳
۷	۷	۵	۳	۱

مثال ۶.۷. گروه یکه‌های حلقه $M(\mathbb{R})$، متشکل از همه ماتریس‌های 2×2 روی اعداد حقیقی،

۶) یکه‌ها در تعریف بعد از قضیه ۵.۳ معرفی شده‌اند.

با $GL(۲,\mathbb{R})$ نشان داده می‌شود و **گروه خطی عام** نام دارد. طبق تمرین ۲۰ بخش ۲.۳، یک ماتریس $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ در $GL(۲,\mathbb{R})$ است اگر و تنها اگر $ad - bc \neq ۰$. در نتیجه، هر دو ماتریس $\begin{pmatrix} ۱ & -۱ \\ ۲ & ۳ \end{pmatrix}$ و $\begin{pmatrix} ۱ & ۱ \\ ۲ & ۰ \end{pmatrix}$ در $GL(۲,\mathbb{R})$ هستند. با ضرب این دو از هر دو طرف می‌توانید بررسی کنید که $GL(۲,\mathbb{R})$ یک گروه غیرآبلی است. همین نماد در موقعیتهای دیگر نیز بکار برده می‌شود: $GL(۲,K)$ گروه ضربی یکه‌های حلقه ماتریس‌های ۲×۲ با درایه‌های در حلقه K را نشان می‌دهد.

اگر $\mathbb{F}$ یک میدان باشد، در این صورت ضرب جابجایی است و هر عضو غیرصفر یک یکه است (تعریف بعد از قضیه ۵.۳ را ملاحظه کنید)؛ بنابراین

تحت عمل ضرب، عناصر غیرصفر یک میدان تشکیل یک گروه آبلی می‌دهند.

گروه ضربی عناصر غیرصفر یک میدان $\mathbb{F}$ با $\mathbb{F}^*$ نشان داده می‌شود.

برخلاف مثال‌های قبل، برخی از جالب‌ترین و مفیدترین گروهها از حلقه‌ها بوجود نمی‌آیند.

مثال ۷.۷. گروه جایگشتی $S_۳$ حالت خاصی از وضعیت کلی‌تر زیر است. فرض کنید n یک عدد صحیح مثبت ثابت باشد و $T = \{۱, ۲, ۳, \ldots, n\}$. فرض کنید S_n مجموعهٔ همه جایگشتهای T باشد (یعنی، همه دوسویی‌های $T \to T$). ما همان نمادی را که برای توابع در $S_۳$ بکار بردیم برای توابع در S_n نیز بکار می‌بریم. برای مثال در $S_۶$، آرایه $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۴ & ۶ & ۲ & ۳ & ۵ & ۱ \end{pmatrix}$ جایگشتی را نشان می‌دهد که درایه ۱ را به ۴، ۲ را به ۶، ۳ را به ۲، ۴ را به ۳، ۵ را به ۵ و ۶ را به ۱ می‌برد. چون ترکیب هر دو تابع دوسویی، دوسویی [۷] است، S_n تحت عمل ترکیب بسته است. برای مثال در $S_۶$

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۳ & ۵ & ۲ & ۴ & ۱ & ۶ \end{pmatrix} \circ \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۶ & ۴ & ۲ & ۳ & ۵ & ۱ \end{pmatrix} = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۶ & ۴ & ۵ & ۲ & ۱ & ۳ \end{pmatrix}$$

(به یاد آورید که در ترکیب توابع، ابتدا تابع دست راست و سپس تابع دست چپ را اثر می‌دهیم. در این حالت همان‌طور که توسط فلش‌ها نشان داده شده است، $۲ \to ۳ \to ۴$). ادعا می‌کنیم

۷) برای جزئیات پیوست ب را ملاحظه کنید.

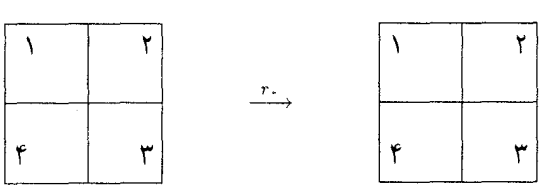
که S_n تحت این عمل یک گروه است. می‌دانیم که ترکیب توابع شرکت‌پذیر است و این که تحت ترکیب توابع هر دو سویی دارای یک تابع وارون[۸] است. به‌سادگی بررسی می‌شود که جایگشت همانی $\begin{pmatrix} ۱ & ۲ & ۳ & \dots & n \\ ۱ & ۲ & ۳ & \dots & n \end{pmatrix}$ عضو همانی S_n است. S_n **گروه متقارن روی n حرف** نامیده می‌شود. مرتبه S_n، $n!$ است (تمرین ۱۸).

مثال ۸.۷. مثال قبل را می‌توان به‌سادگی تعمیم داد. فرض کنید T یک مجموعه غیرتهی دلخواه، احتمالاً نامتناهی، باشد. فرض کنید $A(T)$ مجموعه همه جایگشتهای T باشد (همه توابع دوسویی $T \to T$). بحث ارائه شده بالا برای S_n را به $A(T)$ منتقل کنید و نشان دهید که تحت عمل ترکیب توابع $A(T)$ یک گروه است (تمرین ۱۰).

مثال ۹.۷. صفحه را مانند یک ورقهٔ نازک پلاستیکی صلب در نظر بگیرید. فرض کنید مربعی را بریده، آن را از جای خود برداشته و پس از مقداری حرکت به اطراف[۹] آن را دقیقاً در محل بریده شده جای دهید. هشت طریق انجام این کار در زیر نشان داده شده است (طوری که مربع در مبدأ متمرکز گردیده و گوشه‌های آن برای مراجعه آسان شماره‌گذاری شده است). ادعا می‌کنیم که نتیجه هر حرکت مربع یکی از این هشت حالت می‌باشد (تمرین ۱۲). برای مثال، دورانی به اندازه ۳۶۰° + ۱۸۰° = ۵۴۰° این مربع را به همان وضعیت یک دوران ۱۸۰° می‌برد.

همهٔ دورانها، خلاف حرکت عقربه‌های ساعت حول مرکز انجام می‌گیرد:

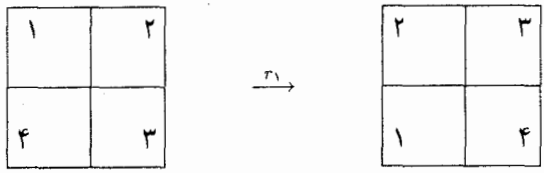
$r_۰$ = دوران ۰°



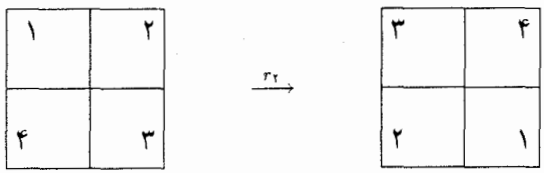
$r_۱$ = دوران ۹۰°

۸) برای جزئیات پیوست ب را ملاحظه کنید.

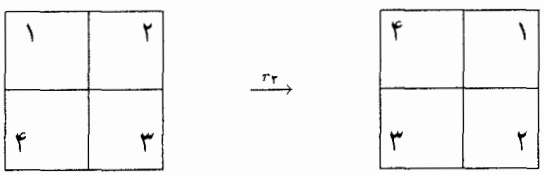
۹) تا زمانی که آن را تا نکنید، نشکنید و یا کج و کوله نکنید هر نوع حرکتی مثل تلنگر زدن، چرخاندن و برگرداندن را می‌توانید انجام دهید.



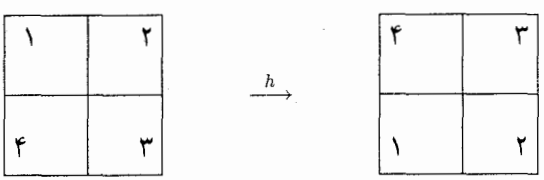
r_2 = دوران 180°



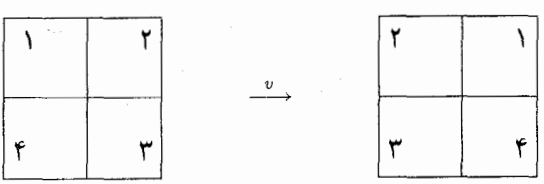
r_3 = دوران 270°



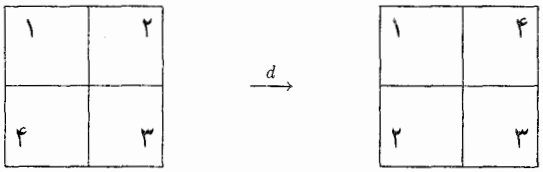
h = انعکاس نسبت به محور x–ها



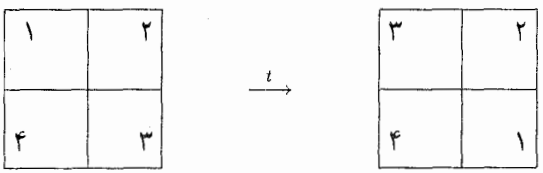
ν = انعکاس نسبت به محور y–ها



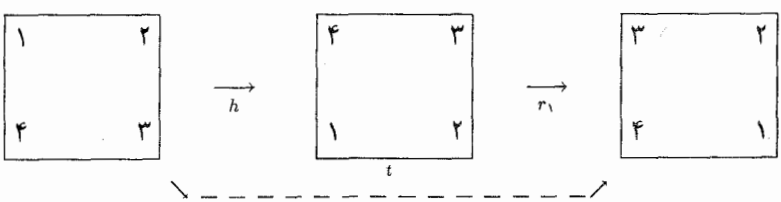
d = انعکاس نسبت به محور $y = -x$



t = انعکاس نسبت به محور $y = x$



نتیجه انجام پی‌درپی این حرکات مجدداً یکی از هشت حالت فهرست شده در بالاست؛ برای مثال



اگر هر حرکت را به‌عنوان تابعی از یک مربع به خودش در نظر بگیرید، در این صورت مفهوم انجام حرکتی در پی حرکت دیگر همان ترکیب توابع است. در نمایش بالا (تأثیر h و بدنبال آن r_1 عبارت است از t)، می‌توانیم بنویسیم $r_1 \circ h = t$ (به یاد آورید $r_1 \circ h$ بدین معنی است که ابتدا h و سپس r_1 را اثر دهید). بررسی کنید که مجموعهٔ

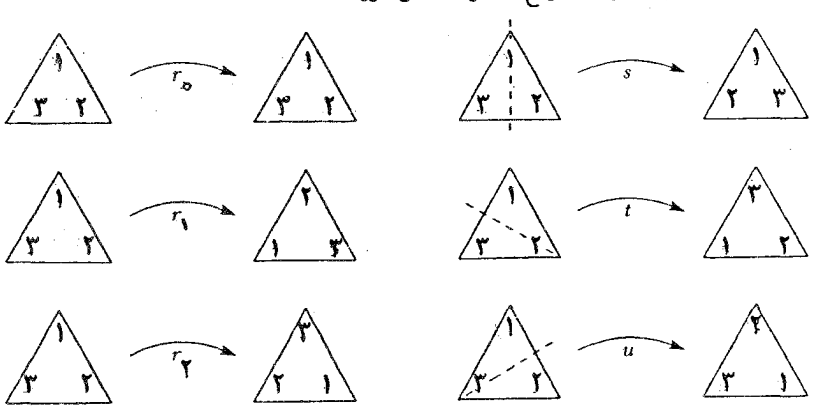
$$D_4 = \{r_0, r_1, r_2, r_3, h, v, d, t\}$$

مجهز به عمل ترکیب توابع دارای جدول زیر است:

$\circ$	r_0	r_1	r_2	r_3	h	ν	d	t
r_0	r_0	r_1	r_2	r_3	h	ν	d	t
r_1	r_1	r_2	r_3	r_0	t	d	h	ν
r_2	r_2	r_3	r_0	r_1	ν	h	t	d
r_3	r_3	r_0	r_1	r_2	d	t	ν	h
h	h	d	ν	t	r_0	r_2	r_1	r_3
ν	ν	t	h	d	r_2	r_0	r_3	r_1
d	d	ν	t	h	r_3	r_1	r_0	r_2
t	t	h	d	ν	r_1	r_3	r_2	r_0

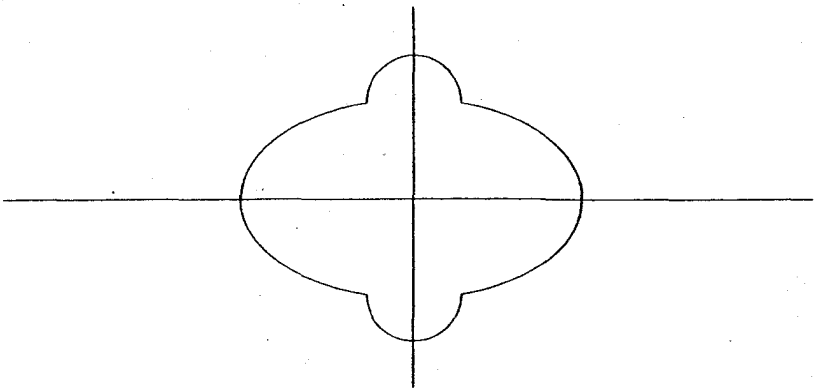
به‌وضوح D_4 تحت $\circ$ بسته‌است، و می‌دانیم که ترکیب توابع شرکت‌پذیر است. جدول بالا نشان می‌دهد که r_0 عضو همانی است و این که هر عضو D_4 دارای یک وارون است. برای مثال $r_3 \circ r_1 = r_0 = r_1 \circ r_3$. بنابراین D_4 یک گروه است. D_4 آبلی نیست زیرا برای مثال $h \circ d \neq d \circ h$. D_4 **گروه دووجهی از درجه ۴ یا گروه تقارنهای مربع** نامیده می‌شود.

مثال ۱۰.۷. گروه تقارنهای مربع تنها یکی از انواع گروههای تقارن می‌باشد. فرآیند مشابهی را می‌توان برای هر n ضلعی منظم انجام داد. گروه حاصل D_n، **گروه دووجهی از درجه** n نامیده می‌شود. برای مثال گروه D_3، متشکل از شش تقارن یک مثلث متساوی‌الاضلاع است (با دورانهای حول مرکز در خلاف جهت حرکت عقربه‌های ساعت 0°، 120° و 240°؛ و سه انعکاس حول خطوط نشان داده شده در زیر) با ترکیب توابع به‌عنوان عمل گروه:



مثال ۱۱.۷. گروه تقارنهای شکل زیر از چهار عضو (دورانهای حول مرکز 0° و 180° و انعکاس‌های

حول محور x و محور y) تشکیل شده‌است:



گروههای تقارن اغلب در هنر، معماری و علوم ظاهر می‌شوند. در بلورشناسی و فیزیک بلورها از گروههای تقارن انواع اشکال سه بعدی استفاده می‌شود. ساخت اولین مدل دقیق دی‌اِن‌اِ (DNA) (که منجر به اعطاء جایزه نوبل برای ابداع‌کنندگان آن شد) بدون تشخیص تقارن مولکول دی‌اِن‌اِ امکان‌پذیر نبود. گروههای تقارن توسط فیزیکدانان برای پیشگویی وجود برخی ذرات بنیادی که بعداً به طور تجربی پیدا شدند بکار رفته است.

ضرب دکارتی، با اعمالی که به صورت مؤلفه به مؤلفه تعریف می‌شود، به ما اجازه ساخت حلقه‌های جدید از حلقه‌های قبلی را می‌دهد. این کار عیناً برای گروهها هم درست است.

قضیه ۱.۷. فرض کنید G و H دو گروه باشند. عملِ $\blacksquare$ را روی $G \times H$ به صورت

$$(g,h) \blacksquare (g',h') = (g * g', h * h')$$

تعریف کنید. در این صورت $G \times H$ یک گروه است. اگر G و H آبلی باشند، $G \times H$ نیز چنین است. اگر G و H متناهی باشند، در این صورت $G \times H$ نیز چنین است و $| G \times H | = | G | \, | H |$.

برهان. تمرین ۲۴. $\blacksquare$

مثال ۱۲.۷. $\mathbb{Z}$ و $\mathbb{Z}_۶$ هر دو تحت عمل جمع، گروه هستند. در $\mathbb{Z}_۶ \times \mathbb{Z}$ داریم

$$(۳,۵) \blacksquare (۷,۴) = (۳+۷, ۵+۴) = (۱۰,۳).$$

عضو همانی $(۰, ۰)$ است و وارون $(۷, ۴)$ عضو $(-۷, ۲)$ می‌باشد.

مثال ۱۳.۷. $\mathbb{R}^* \times D_۴$ که در آن $\mathbb{R}^*$ گروه ضربی اعداد حقیقی غیرصفر می‌باشد را در نظر بگیرید. جدول مثال ۹.۷ نشان می‌دهد که

$$(۲, r_۱) \blacksquare (۹, \nu) = (۲ \times ۹, r_۱ \circ \nu) = (۱۸, d).$$

عضو همانی $(۱, r_۰)$ است و وارون $(۸, r_۳)$ عضو $(۱/۸, r_۱)$ است.

تمرینها

۱.A. وارون هر جایگشت در $S_۳$ را بیابید.

۲. همه اعضای f در $S_۳$ را که $f \circ f \circ f = I$ بیابید.

۳. مرتبه هر یک از گروههای زیر چیست:

(الف) $\mathbb{Z}_{۱۸}$ (ب) $D_۴$ (پ) $S_۴$ (ت) $S_۵$ (ث) $U_{۱۸}$.

۴. ثابت کنید که یک حلقهٔ غیرصفر R تحت عمل ضرب یک گروه نیست. [راهنمایی: وارون ۰_R چیست؟]

۵. جدول عمل گروه $D_۳$ که در مثال ۱۰.۷ توصیف شد را بنویسید.

۶. با استفاده از نتیجه ۹.۲، اعضای هرکدام از گروههای: $U_۴$، $U_۶$، $U_۱۰$، $U_{۲۰}$ را فهرست کنید.

۷. نشان دهید که $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a, b \in \mathbb{R}, (a, b) \neq (۰, ۰) \right\}$ تحت ضرب ماتریسی یک گروه است.

۸. گروه جمعی $\mathbb{Z}_۲$ و گروه ضربی $G = \{\pm ۱, \pm i\}$ از اعداد مختلط را در نظر بگیرید. جدول عمل گروه $\mathbb{Z}_۲ \times G$ را بنویسید.

۹. فرض کنید n یک عدد صحیح مثبت و z عدد مختلط $\cos(۲\pi/n) + i \sin(۲\pi/n)$ باشد. ثابت کنید که $G = \{۱, z, z^۲, \ldots, z^{n-۱}\}$ تحت عمل ضرب $\mathbb{C}$ یک گروه است. [راهنمایی: طبق قضیه دِموآور[۱۰]، $z^n = ۱$.]

[۱۰] De Moiver

۱۰. فرض کنید T یک مجموعه غیرتهی و $A(T)$ مجموعه جایگشتهای T باشد. نشان دهید که تحت عمل ترکیب توابع $A(T)$ یک گروه است.

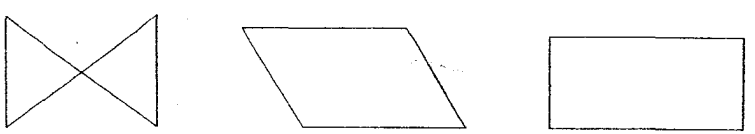
۱۱. (الف) مثال‌هایی از گروههای غیرآبلی از مرتبه‌های ۱۲، ۱۶، ۳۰ و ۴۸ ارائه دهید. [راهنمایی: قضیه ۱.۷ می‌تواند مفید باشد.]

(ب) مثالی از یک گروه آبلی از مرتبه ۴ بزنید که در آن هر عضو غیرهمانی x در $x * x = e$ صدق کند.

۱۲.B. نشان دهید که نتیجه هر حرکت صلب مربع (همان‌طور که در مثال ۹.۷ توصیف شد) یک عضو D_4 است. [راهنمایی: مکان مربع پس از هر حرکت به‌طور کامل توسط مکان گوشه ۱ و جهت مربع، وجه به طرف بالا یا به طرف پائین، معین می‌شود.]

۱۳. جدول عمل گروههای تقارن هر یک از اشکال زیر را بنویسید.

(الف) (ب) (پ)



۱۴. با نوشتن جدول ضربی بررسی کنید که مجموعه ماتریس‌های زیر، با درایه‌های مختلط، تحت عمل ضرب ماتریسی تشکیل یک گروه می‌دهد (که گروه **چهارگانی** نامیده می‌شود):

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \quad \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

۱۵. در موارد زیر اگر G تحت عمل بیان شده یک گروه باشد، آن را ثابت کنید؛ اگر نیست، مثال نقضی ارائه کنید:

(الف) $G = \mathbb{Q}$؛ $a * b = a + b + 3$.

(ب) $G = \{r \in \mathbb{Q} \mid r \neq 0\}$؛ $a * b = ab/3$.

(پ) $G = \{r \in \mathbb{Q} \mid r \neq -1\}$؛ $a * b = a + b + ab$.

۱۶. فرض کنید $K = \{r \in \mathbb{R} \mid r \neq 0, r \neq 1\}$. فرض کنید G از شش تابع زیر از K به K تشکیل شده باشد،

$$h(x) = \frac{1}{x} \qquad g(x) = \frac{x-1}{x} \qquad f(x) = \frac{1}{1-x}$$
$$k(x) = \frac{x}{x-1} \qquad j(x) = 1 - x \qquad i(x) = x.$$

آیا تحت عمل ترکیب توابع، G یک گروه است؟

۱۷. آیا اعداد حقیقی غیرصفر تحت عمل داده شده بوسیلهٔ $a * b = |a| b$ که در آن $|a|$، قدرمطلق a است تشکیل یک گروه می‌دهد؟

۱۸. ثابت کنید که مرتبه S_n، $n!$ است. [راهنمایی: برای ۱، n تصویر ممکن وجود دارد؛ بعد از انتخاب یک تصویر، برای ۲، $n-1$ تصویر ممکن وجود دارد؛ و غیره.]

۱۹. فرض کنید G یک گروه با عمل $*$ باشد. عمل جدید $a\#b = b * a$ را روی G تعریف کنید. ثابت کنید که G تحت $\#$ یک گروه است.

۲۰. اعضای گروه D_5 را فهرست کنید (تقارنهای یک پنج ضلعی منظم). [راهنمایی: این گروه دارای مرتبهٔ ۱۰ است.]

۲۱. فرض کنید $SL(2,\mathbb{R})$ مجموعهٔ همه ماتریس‌های 2×2، $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ باشد به قسمی که $a, b, c, d \in \mathbb{R}$ و $ad - bc = 1$. ثابت کنید که $SL(2,\mathbb{R})$ تحت ضرب ماتریسی یک گروه است. این گروه، **گروه خطی خاص** نامیده می‌شود.

۲۲. ثابت کنید مجموعه اعداد حقیقی غیرصفر تحت عمل $*$ که توسط

$$a * b = \begin{cases} ab & \text{اگر } a > 0 \\ a/b & \text{اگر } a < 0 \end{cases}$$

تعریف می‌شود، یک گروه می‌باشد.

۲۳. ثابت کنید که $\mathbb{R}^* \times \mathbb{R}$ تحت عمل $*$ که توسط $(a,b) * (c,d) = (ac, bc + d)$ تعریف می‌شود یک گروه است.

۲۴. قضیه ۱.۷ را ثابت کنید.

۲۵. اگر در یک گروه G، $ab = ac$، ثابت کنید $b = c$.

۲۶. ثابت کنید که هر عضو یک گروه متناهی G دقیقاً یکبار در هر سطر و دقیقاً یکبار در هر ستون جدول عمل G ظاهر می‌شود. [راهنمایی: تمرین ۲۵.]

۲۷. در اینجا قسمتی از جدول عمل گروه G که اعضای آن a، b، c و d هستند آمده است. بقیه جدول را کامل کنید. [راهنمایی: تمرینهای ۲۵ و ۲۶.]

	a	b	c	d
a	b	a		
b	b	a		
c	c		a	
d	d			

۲۸. ذیلاً قسمتی از جدول عمل گروه $G = \{e, a, b, c, d, f\}$ نشان داده شده است. جدول را کامل کنید: [راهنمایی: تمرین‌های ۲۵ و ۲۶.]

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d		
b	b					
c	c	f				a
d	d					
f	f					

۲۹. فرض کنید T یک مجموعه با حداقل سه عضو باشد. نشان دهید که گروه جایگشتهای $A(T)$ (تمرین ۱۰) غیرآبلی است.

۳۰. فرض کنید T یک مجموعه نامتناهی و $A(T)$ گروه جایگشتهای T باشد (تمرین ۱۰). ثابت کنید که مجموعهٔ $M = \{f \in A(T) \mid t \in T$ برای تنها تعداد متناهی $f(t) \neq t\}$ یک گروه است.

۳۱. اگر $a, b \in \mathbb{R}$ با $a \neq 0$، فرض کنید $T_{a,b} : \mathbb{R} \to \mathbb{R}$ تابعی باشد که توسط $T_{a,b}(x) = ax + b$

تعریف شده است. ثابت کنید که مجموعهٔ $G = \{T_{a,b} \mid a, b \in \mathbb{R}\}$ تحت ترکیب توابع یک گروه غیرآبلی تشکیل می‌دهد.

۳۲. فرض کنید $H = \{T_{1,b} \mid b \in \mathbb{R}\}$ (نماد همانند تمرین ۳۱). ثابت کنید که H تحت ترکیب توابع یک گروه آبلی است.

۳۳.C اگر $f \in S_n$، ثابت کنید که برای برخی عدد صحیح مثبت k، $f^k = I$، که در آن f^k به معنی $f \circ f \circ \cdots \circ f$ (k بار) می‌باشد و I جایگشت همانی است.

۳۴. فرض کنید $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$ و فرض کنید G تحت عمل $*$ یک گروه باشد با این خواص که:

(i) برای هر $a, b \in G$، $a * b \leq a + b$؛

(ii) برای هر $a \in G$، $a * a = 0$.

جدول عمل G را بنویسید. [راهنمایی: تمرین‌های ۲۵ و ۲۶ می‌تواند مفید باشد.]

۲-۷ خواص اساسی گروهها

قبل از کاوش در مفاهیم عمیق‌تر نظریه گروهها ابتدا چند اصطلاح دیگر را مطرح کرده برخی حقایق مقدماتی مورد نیاز را اثبات می‌نمائیم. کار را با یک تغییر در نمادگذاری آغاز می‌کنیم.

در بخش قبلی برای پرهیز از هرگونه اشتباه با عمل حلقه‌ها، عمل یک گروه دلخواه با $*$ نشان داده شد. حال که با گروهها خوگرفته‌اید می‌توانیم به **نماد استاندارد ضربی** برگردیم. وقتی درباره گروههای مجرد بحث می‌کنیم بجای $a * b$ خواهیم نوشت ab، با این حال در مورد برخی گروهها که دارای عمل $+$ هستند (مثل $\mathbb{Z}$) از همان نماد جمعی استفاده خواهیم کرد.

گرچه که ما در مورد وارون یک عضو یا عضو همانی در یک گروه صحبت کرده‌ایم امّا تعریف گروه چیزی در مورد یکتایی عضو وارون و یا یکتایی عضو همانی بیان نمی‌کند. اولین قضیه این بخش به این سوال پاسخ می‌دهد.

قضیه ۲.۷. فرض کنید G یک گروه و $a, b, c \in G$. در این صورت

(۱) G دارای یک عضو همانی یکتا است.

(۲) قوانین حذف در G برقراراست:

اگر $ab = ac$، در این صورت $b = c$؛ اگر $ba = ca$، در این صورت $b = c$.

(۳) هر عضو G دارای یک وارون یکتاست.

برهان. (۱) طبق تعریف، G حداقل دارای یک عضو همانی است. اگر e و e' دو عضو همانی برای G باشند، در این صورت برای هر $a \in G$، $ea = a = ae$ و $e'a = a = ae'$. معادله اول به ازای $a = e'$ بیان می‌کند که $ee' = e'$. معادله دوم به‌ازای $a = e$ بیان می‌کند که $e = ee'$. بنابراین $e' = ee' = e$، لذا دقیقاً یک عضو همانی وجود دارد.

(۲) طبق تعریف گروه، عضو a دارای حداقل یک وارون d است به قسمی که $da = e = ad$. اگر $ab = ac$، در این صورت $d(ab) = d(ac)$. بنا به شرکت‌پذیری و خواص عضو وارون و عضو همانی،

$$(da)b = (da)c$$
$$eb = ec$$
$$b = c.$$

گزاره دوم به‌طور مشابه ثابت می‌شود.

(۳) فرض کنید که هر دو d و d' وارون $a \in G$ باشند. در این صورت $ad = e = ad'$، لذا طبق (۲)، $d = d'$. بنابراین a دارای دقیقاً یک وارون است. ■

از اینجا به بعد وارون یکتای عضو a در یک گروه را با a^{-1} نشان می‌دهیم. یکتایی a^{-1} بدین معنی است که

هرگاه $ay = e = ya$، در این صورت $y = a^{-1}$.

نتیجه ۳.۷. اگر G یک گروه باشد و $a, b \in G$، در این صورت

(۱) $(ab)^{-1} = b^{-1}a^{-1}$.

(۲) $(a^{-1})^{-1} = a$.

به ترتیب عناصر در گزاره (۱) توجه کنید. یک اشتباه رایج این است که وارون ab را $a^{-1}b^{-1}$ قلمداد کنیم که البته این در گروههای غیرآبلی ممکن است درست نباشد. برای نمونه، تمرین ۳ را

ملاحظه کنید.

برهان نتیجه ۳.۷. (۱) داریم

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e,$$

و به‌طور مشابه $(b^{-1}a^{-1})(ab) = e$. چون طبق قضیه ۲.۷ وارون ab یکتاست، $b^{-1}a^{-1}$ باید این وارون باشد، یعنی $(ab)^{-1} = b^{-1}a^{-1}$.

(۲) طبق تعریف، $a^{-1}a = e$ و $(a^{-1})(a^{-1})^{-1} = e$. لذا $a^{-1}a = a^{-1}(a^{-1})^{-1}$.

طبق قضیه ۲.۷، حذف a^{-1} نشان می‌دهد که $a = (a^{-1})^{-1}$. ■

فرض کنید G یک گروه باشد و $a \in G$. برای هر عدد صحیح مثبت n، تعریف می‌کنیم $a^2 = aa$، $a^3 = aaa$، و به‌طور کلی

$$a^n = aaa\cdots a \quad (n \text{ عامل}).$$

همچنین تعریف می‌کنیم $a^0 = e$ و

$$a^{-n} = a^{-1}a^{-1}a^{-1}\cdots a^{-1} \quad (n \text{ عامل}).$$

به وضوح این تعاریف از علامت توان معمولی در $\mathbb{R}$ و دیگر حلقه‌های شناخته شده نشأت گرفته است. امّا در صورت غیرآبلی بودن G باید مواظب بود زیرا مثلاً $(ab)^n$ ممکن است برابر a^nb^n نباشد. با این حال، بعضی از قوانین معمولی توان در مورد گروهها نیز برقرار است:

قضیه ۴.۷. فرض کنید G یک گروه باشد و $a \in G$. در این صورت برای هر $m, n \in \mathbb{Z}$

$$(a^m)^n = a^{mn} \quad \text{و} \quad a^m a^n = a^{m+n}.$$

برهان. اثبات شامل بررسی هرکدام ازگزاره‌ها در همه حالتهای ممکن است ($m \geq 0$، $n \geq 0$، $m \geq 0$، $n < 0$ و غیره) که به خواننده واگذار می‌شود. (تمرین ۱۹). ■

تذکر درباره نماد جمعی برای پرهیز از اشتباه، عمل برخی گروهها باید به صورت جمعی نوشته شود (برای مثال در مورد گروه جمعی اعداد حقیقی، زیرا در این حالت ضرب دارای معنی کاملاً

متفاوتی است). وقتی که عمل گروه به‌صورت جمعی نوشته شود، در این صورت عضو همانی بجای e با ۰ و وارون a بجای a^{-1} با $-a$ نشان داده می‌شود. در این حالت به توان رساندن و قضیه ۴.۷ شکل متفاوتی می‌یابد. مشابه جمعی $aa\cdots a$ (n عامل) عبارت است از $a+a+\cdots+a$ (n جمعوند)، و لذا بجای $a^n = aa\cdots a$ می‌نویسیم $na = a+a+\cdots+a$. به‌طور مشابه نماد جمعی برای a^{-n} عبارت از $(-n)a$ است و در نتیجه قضیه ۴.۷ به‌صورت

$$m(na) = (mn)a \qquad \text{و} \qquad ma + na = (m+n)a$$

تعبیر می‌شود. این نماد با آنچه که ما با جمع در حلقه‌ها انجام دادیم سازگار است.

حال به نماد ضربی برای گروههای مجرد باز می‌گردیم. عضو a از گروه G را از **مرتبه متناهی** گویند اگر برای برخی عدد صحیح مثبت k، $a^k = e$ [۱۱]. در این حالت **مرتبه** a عبارت است از کوچکترین عدد صحیح مثبت n به قسمی که $a^n = e$. مرتبه a با $|\ a\ |$ نشان داده می‌شود. عضو a را از **مرتبه نامتناهی** می‌نامند اگر برای هر عدد صحیح مثبت k، $a^k \neq e$.

مثال ۱۴.۷. درگروه ضربی اعداد حقیقی غیرصفر، ۲ دارای مرتبه نامتناهی است زیرا برای هر $k \geq 1$، $2^k \neq 1$. درگروه $G = \{\pm 1, \pm i\}$، تحت ضرب اعداد مختلط، مرتبه i، ۴ است زیرا $i^2 = -1$، $i^3 = -i$ و $i^4 = 1$. به‌طور مشابه، $|\ -i\ | = 4$. عضو $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ در S_3 دارای مرتبه ۳ است زیرا

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \text{و} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

عضو همانی در یک گروه دارای مرتبه ۱ است.

مثال ۱۵.۷. درگروه جمعی $\mathbb{Z}_{12}$، عضو ۸ دارای مرتبه ۳ است زیرا $8+8=4$ و $8+8+8=0$.

درگروه ضربی اعداد حقیقی غیرصفر، عضو ۲ دارای مرتبه نامتناهی است و همه توانهای ۲ (2^{-3}، 2^0، 2^5 و غیره) متمایزند. از طرف دیگر درگروه ضربی $G = \{\pm 1, \pm i\}$ عضو i دارای

۱۱) در نماد جمعی این شرط به صورت $ka = 0$ در می‌آید

مرتبه ۴ است و توانهای آن متمایز نیستند؛ برای مثال

$$i^{۱۰} = (i^{۴})^{۲} i^{۲} = i^{۲} \quad \text{و} \quad i^{۴} = ۱ = i^{۰}.$$

مشاهده کنید که $i^{۱۰} = i^{۲}$ و (پیمانه ۴) $۲ \equiv ۱۰$. این مثال‌ها مصداق‌هایی از قضیه زیر هستند.

قضیه ۵.۷. فرض کنید G یک گروه باشد و $a \in G$.

(۱) اگر a دارای مرتبه نامتناهی باشد، در این صورت همه عناصر a^k، به ازای $k \in \mathbb{Z}$، متمایزند.

(۲) اگر a دارای مرتبه متناهی nباشد، در این صورت

$$a^k = e \quad \text{اگر و تنها اگر} \quad n \mid k$$

و

$$a^i = a^j \quad \text{اگر و تنها اگر} \quad i \equiv j \ (n \text{ پیمانه})$$

(۳) اگر a دارای مرتبه n باشد و $n = td$ با $d > ۰$، در این صورت a^t دارای مرتبه d است.

برهان. (۱) ما عکس نقیض را اثبات خواهیم کرد (اگر a^kها متمایز نباشند در این صورت a دارای مرتبه متناهی است). فرض کنید که $a^i = a^j$ با $i > j$. در این صورت ضرب دو طرف در a^{-j} بدست می‌دهد $a^{i-j} = a^{j-j} = a^{۰} = e$. چون $i - j > ۰$ این مطلب بیان می‌کند که a دارای مرتبه متناهی است.

(۲) اگر n، k را بشمارد، مثلاً $k = nt$، در این صورت $a^k = a^{nt} = (a^n)^t = e^t = e$.

برعکس فرض کنید که $a^k = e$. طبق الگوریتم تقسیم، $k = nq + r$ با $۰ \leq r < n$. در نتیجه

$$e = a^k = a^{nq+r} = a^{nq} a^r = (a^n)^q a^r = e^q a^r = a^r.$$

طبق تعریف مرتبه، n کوچکترین عدد صحیح مثبتی است که $a^n = e$. چون $r < n$، برابری $a^r = e$ تنها در صورتی می‌تواند رخ دهد که $r = ۰$. بنابراین $k = nq + ۰$ و لذا n، k را می‌شمارد. سرانجام توجه کنید که $a^i = a^j$ اگر و تنها اگر $a^{i-j} = a^{۰} = e$. طبق آنچه که ما الان اثبات کردیم $a^{i-j} = e$ اگر و تنها اگر n، $i - j$ را بشمارد، یعنی اگر و تنها اگر $i \equiv j \ (n \text{ پیمانه})$.

(۳) چون $n = |a|$، داریم $(a^t)^d = a^{td} = a^n = e$. باید نشان دهیم d کوچکترین عدد صحیح مثبت با این خاصیت است. اگر k هر عدد صحیح مثبت باشد به قسمی که $(a^t)^k = e$،

در این صورت $a^{tk} = e$. بنابراین برطبق (۲)، $n \mid tk$، مثلاً $tk = nr = (td)r$. پس $k = dr$.
چون k و d مثبت هستند و $d \mid k$، داریم $d \leq k$. ■

نتیجه زیر فوراً از گزاره (۱) قضیه بالا بدست می‌آید.

نتیجه ۶.۷. فرض کنید G یک گروه باشد و $a \in G$. اگر $a^i = a^j$ با $i \neq j$، در این صورت a دارای مرتبه متناهی است.

این نتیجه یکی از مواردی را که رفتار توانها در گروهها متفاوت از حلقه‌ها است بیان می‌کند. برای مثال، در حلقه $\mathbb{Z}_8$ (که اعضای غیرصفر آن تحت ضرب یک گروه تشکیل نمی‌دهند)، $2^1 = 2^3$ امّا $2^k \neq 1$ برای هر عدد صحیح مثبت k.

تمرینها

توجه: G یک گروه با عنصر همانی e است، مگر خلاف آن ذکر شود.

A.۱. اگر در یک گروه $c^2 = c$، ثابت کنید که $c = e$.

۲. فرض کنید $a \in G$ و فرض کنید $f : G \to G$ تابعی باشد که توسط $f(c) = ac$ تعریف شده است. ثابت کنید که f دوسویی است.

۳. فرض کنید $a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ و $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ در S_3. بررسی کنید که $(ab)^{-1} \neq a^{-1}b^{-1}$.

۴. اگر $a, b, c, d \in G$، در این صورت $(abcd)^{-1} =$?

۵. فرض کنید $f : G \to G$ توسط $f(a) = a^{-1}$ داده شده باشد. ثابت کنید که f یک دوسویی است.

۶. اگر $a, b \in G$ و $ab = e$، ثابت کنید که $ba = e$.

۷. مثالی از یک گروه بزنید که در آن معادله $x^2 = e$ بیشتر از دو جواب داشته باشد.

۸. مرتبهٔ $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 5 & 1 & 4 & 6 \end{pmatrix}$ در S_7 چیست؟

۹. مرتبهٔ $\begin{pmatrix} ۰ & -۱ \\ ۱ & ۱ \end{pmatrix}$ و مرتبهٔ $\begin{pmatrix} -۱/۲ & ۱/۲ \\ -۳/۲ & -۱/۲ \end{pmatrix}$ در $GL(۲,\mathbb{R})$ را بیابید.

۱۰. مرتبهٔ عناصر گروههای زیر را بیابید:

(الف) $\mathbb{Z}_۴$ (ب) $\mathbb{Z}_۵$ (پ) $S_۳$ (ت) $D_۴$ (ث) $\mathbb{Z}$

۱۱. (الف) مرتبهٔ گروههای $U_{۱۰}$، $U_{۱۲}$ و $U_{۲۴}$ را بیابید.

(ب) مرتبه‌های عناصر گروه $U_{۲۰}$ را فهرست کنید.

۱۲. درست است یا نادرست: یک گروه از مرتبه n شامل عنصری با مرتبهٔ n است. جواب خود را توجیه کنید.

۱۳. ثابت کنید که هر عنصر یک گروه متناهی دارای مرتبهٔ متناهی است. [عکس این نادرست است: مثال قبل از قضیه ۲۴.۷ را برای یک گروه نامتناهی که در آن هر عضو دارای مرتبه متناهی است ملاحظه کنید.]

۱۴. (الف) اگر $a \in G$ و $a^{۱۲} = e$، مقادیر ممکن مرتبه a چیست؟

(ب) اگر $e \neq b \in G$ و برای یک عدد اول p، $b^p = e$ مرتبه b چیست؟

۱۵. (الف) اگر $a, b \in G$، ثابت کنید که هر یک از معادلات $ax = b$ و $ya = b$ دارای جواب منحصر به فردی در G است. [دو کار برای هر معادله باید انجام شود: ابتدا یک جواب پیدا کنید و سپس نشان دهید که این تنها جواب است.]

(ب) با مثال نشان دهید که جواب $ax = b$ ممکن است برابر جواب $ya = b$ نباشد. [راهنمایی: $S_۳$ را در نظر بگیرید.]

۱۶. فرض کنید $G = \{a_۱, a_۲, \ldots, a_n\}$ یک گروه آبلی متناهی از مرتبه n باشد. فرض کنید $x = a_۱a_۲\cdots a_n$. ثابت کنید که $x^۲ = e$.

۱۷. اگر $a, b \in G$، ثابت کنید که $| b | = | aba^{-۱} |$.

۱۸. (الف) نشان دهید که $a = \begin{pmatrix} ۰ & ۱ \\ -۱ & -۱ \end{pmatrix}$ دارای مرتبه ۳ در $GL(۲,\mathbb{R})$ است و $b = \begin{pmatrix} ۰ & -۱ \\ ۱ & ۰ \end{pmatrix}$ دارای مرتبهٔ ۴ است.

(ب) نشان دهید که ab دارای مرتبهٔ نامتناهی است.

۱۹.B. قضیه ۴.۷ را ثابت کنید.

۲۰. ثابت کنید که G آبلی است اگر و تنها اگر برای هر $a, b \in G$، $(ab)^{-1} = a^{-1}b^{-1}$.

۲۱. اگر هر عضو غیرهمانی G دارای مرتبه ۲ باشد، ثابت کنید که G آبلی است. [راهنمایی: $|a| = 2$ اگر و تنها اگر $a = a^{-1}$. چرا؟]

۲۲. ثابت کنید که هر گروه غیرآبلی G دارای مرتبه حداقل ۶ است؛ بنابراین هر گروه از مرتبه ۲، ۳، ۴ یا ۵ آبلی است. [راهنمایی: اگر $a, b \in G$ و $ab \neq ba$، نشان دهید که اعضای زیرمجموعه $H = \{e, a, b, ab, ba\}$ از G متمایز هستند. نشان دهید که یا $a^2 \notin H$ یا $a^2 = e$؛ در حالت دوم بررسی کنید که $aba \notin H$.]

۲۳. اگر $a, b, c \in G$، ثابت کنید که عنصر یکتای $x \in G$ وجود دارد به قسمی که $axb = c$.

۲۴. اگر $a \in G$، ثابت کنید که $|a^{-1}| = |a|$.

۲۵. اگر $a, b \in G$، ثابت کنید که $|ba| = |ab|$.

۲۶. اگر $|G|$ زوج باشد، ثابت کنید که G عضوی از مرتبه ۲ را شامل است. [راهنمایی: راهنمایی تمرین ۲۱ را ملاحظه کنید.]

۲۷. (الف) اگر $a, b \in G$ و $ab = ba$، ثابت کنید که $(ab)^{|a||b|} = e$.
(ب) نشان دهید اگر $ab \neq ba$، قسمت (الف) ممکن است نادرست باشد.

۲۸. اگر برای هر $a, b \in G$ داشته باشیم $(ab)^2 = a^2b^2$، ثابت کنید که G آبلی است.

۲۹. فرض کنید که $a, b \in G$ و $ab = ba$. اگر $|a|$ و $|b|$ نسبت به هم اول باشند، ثابت کنید که ab دارای مرتبهٔ $|b||a|$ است. [راهنمایی: تمرین ۲۷ را ملاحظه کنید.]

۳۰. فرض کنید $a, b \in G$ با $|a| = 5$، $b \neq e$ و $bab^{-1} = b^2$. $|b|$ را بیابید.

۳۱. اگر $a, b \in G$، $b^6 = e$، $ab = b^4a$، ثابت کنید که $b^3 = e$ و $ab = ba$.

۳۲. اگر برای سه عدد صحیح متوالی i و هر $a, b \in G$، $(ab)^i = a^ib^i$، ثابت کنید که G آبلی است.

۳۳. اگر برای هر $a, b \in G$، $(ab)^3 = a^3b^3$ و $(ab)^5 = a^5b^5$ ثابت کنید که G آبلی است.

۳۴.C (الف) فرض کنید G یک مجموعه غیرتهی متناهی باشد که به یک عمل شرکت‌پذیر چنان مجهز شده است که برای هر $a, b, c, d \in G$: اگر $ab = ac$، در این صورت $b = c$ و اگر $bd = cd$، در این صورت $b = c$. ثابت کنید که G یک گروه است.

(ب) نشان دهید که اگر G نامتناهی باشد، قسمت (الف) ممکن است نادرست باشد.

۳۵. فرض کنید G یک مجموعه غیرتهی باشد که به یک عمل شرکت‌پذیر با خواص زیر مجهز باشد:

(i) عنصر $e \in G$ وجود دارد به قسمی که برای هر $a \in G$، $ea = a$.

(ii) برای هر $a \in G$، عضو $d \in G$ وجود دارد به قسمی که $da = e$.

ثابت کنید که G یک گروه است.

۳۶. فرض کنید G یک مجموعه غیرتهی باشد که با یک عمل شرکت‌پذیر مجهز شده است به قسمی که برای هر $a, b \in G$، معادلات $ax = b$ و $ya = b$ دارای جواب باشد. ثابت کنید که G یک گروه است.

۳-۷ زیرگروهها

بحث خود در مورد خواص اساسی گروهها را با توجه ویژه به زیرگروهها ادامه می‌دهیم.

تعریف. زیرمجموعهٔ H از یک گروه G یک **زیرگروه** G است اگر H خودش تحت عمل G یک گروه باشد.

هر گروه G دارای دو زیرگروه بدیهی است: خود G و گروه تک عضوی $\{e\}$. هر زیرگروه دیگر G یک **زیرگروه سره** زیرگروه! سره نامیده می‌شود.

مثال ۱۶.۷. مجموعه $\mathbb{R}^*$ متشکل از اعداد حقیقی غیرصفر تحت عمل ضرب یک گروه است. گروه $\mathbb{R}^{**}$ متشکل از همه اعداد حقیقی مثبت یک زیرگروه سره $\mathbb{R}^*$ است.

مثال ۱۷.۷. هر حلقه R تحت عمل جمع یک گروه است. اگر S یک زیرحلقه R باشد، در این صورت S (وقتی به‌عنوان یک گروه جمعی در نظر گرفته شود) به طور خودکار یک زیرگروه R است. بویژه، هر ایده‌آل R یک زیرگروه جمعی R است.

مثال ۱۸.۷. جدول عمل D_4 در مثال ۹.۷ نشان می‌دهد که $H = \{r_0, r_1, r_2, r_3\}$ یک زیرگروه D_4 است.

مثال ۱۹.۷. در گروه جمعی $\mathbb{Z}_4 \times \mathbb{Z}_6$، فرض کنید $H = \{(0,0),(3,0),(0,2),(3,2)\}$. با نوشتن جدول جمعی H، بررسی کنید که H یک زیرگروه است.

برای اثبات زیرگروه بودن یک زیرمجموعه از یک گروه، هیچ الزامی به بررسی شرکت‌پذیری نیست. چون قانون شرکت‌پذیری برای همه اعضای گروه برقرار است، به‌طور خودکار برای اعضای هر زیرمجموعهٔ آن نیز برقرار است. در حقیقت، تنها نیاز به بررسی دو اصل از اصول یک گروه را داریم:

قضیه ۷.۷. یک زیرمجموعه غیرتهی از یک گروه G، یک زیرگروه است مشروط به این که

(i) اگر $a, b \in H$، در این صورت $ab \in H$؛ و

(ii) اگر $a \in H$، در این صورت $a^{-1} \in H$.

برهان. خواص (i) و (ii) اصول بسته بودن و وارون‌پذیری برای یک گروه را بیان می‌کند. همانگونه که در بالا گفته شد، شرکت‌پذیری در H برقرار است. بنابراین تنها نیاز داریم اثبات کنیم که $e \in H$. چون H غیرتهی است، یک عضو $c \in H$ وجود دارد. طبق (ii)، $c^{-1} \in H$ و طبق (i)، $cc^{-1} = e$ در H است. بنابراین H یک گروه است. ■

مثال ۲۰.۷. فرض کنید H متشکل از تمام ماتریس‌های 2×2 به صورت $b = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ باشد که در آن $b \in \mathbb{R}$. چون $1 \times 1 - b \times 0 = 1$ لذا H یک زیرمجموعه غیرتهی از گروه $GL(2.\mathbb{R})$ است که در مثال ۶.۷ تعریف شد. حاصل‌ضرب هر دو ماتریس واقع در H در H است زیرا

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+c \\ 0 & 1 \end{pmatrix}.$$

وارون $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ عبارت است از $\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}$، که باز هم در H قرار دارد. بنابراین طبق قضیه ۷.۷، H یک زیرگروه $GL(2,\mathbb{R})$ است.

وقتی H متناهی است زیرگروه بودن آن با برقراری تنها یک اصل تضمین می‌شود.

قضیه ۸.۷. فرض کنید H یک زیرمجموعه متناهی غیرتهی از یک گروه G باشد. اگر H تحت عمل G بسته باشد، در این صورت H یک زیرگروه G است.

برهان. طبق قضیه ۷.۷، تنها نیاز به بررسی این داریم که وارون هر عضو H، همچنان در H قرار دارد. اگر $a \in H$، بسته بودن نتیجه می‌دهد که برای هر عدد صحیح k، $a^k \in H$. چون H متناهی است، همه این توانها نمی‌توانند متمایز باشند. بنابراین طبق نتیجه ۶.۷، a دارای مرتبه متناهی مثلاً n است و $a^n = e$. چون (پیمانه n) $n-1 \equiv -1$ لذا طبق قضیه ۵.۷ داریم $a^{n-1} = a^{-1}$. اگر $n > 1$، در این صورت $n-1$ مثبت است و $a^{-1} = a^{n-1}$ در H قرار دارد. اگر $n = 1$، در این صورت $a = e$ و $a^{-1} = e = a$، بنابراین در هر حال a^{-1} در H است. ■

مثال ۲۱.۷. فرض کنید H متشکل از همه جایگشتهایی در S_5 باشد که عضو ۱ را ثابت نگه می‌دارند. به عبارت دیگر $H = \{f \in S_5 \mid f(1) = 1\}$. H یک مجموعه متناهی است زیرا S_5 یک گروه متناهی است. اگر $g, h \in H$، در این صورت $g(1) = 1$ و $h(1) = 1$. بنابراین $(goh)(1) = g(h(1)) = g(1) = 1$. پس $goh \in H$ و H بسته است. بنابراین طبق قضیه ۸.۷، H یک زیرگروه S_5 است.

نوع مهمی از زیرگروهها را می‌توان به صورت زیر ساخت. اگر G یک گروه باشد و $a \in G$، فرض کنید $< a >$ مجموعه همه توانهای a را نشان دهد:

$$< a >= \{\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots\} = \{a^n \mid n \in \mathbb{Z}\}.$$

حاصلضرب هر دو عضو $< a >$ همچنان در $< a >$ قرار دارد زیرا $a^i a^j = a^{i+j}$. وارون a^k عبارت است از a^{-k} که همچنان در $< a >$ قرار دارد. به موجب قضیه ۷.۷، $< a >$ یک زیرگروه G است. پس قضیه زیر را اثبات کرده‌ایم:

قضیه ۹.۷. اگر G یک گروه باشد و $a \in G$، در این صورت $< a >= \{a^n \mid n \in \mathbb{Z}\}$ یک زیرگروه G است.

گروه $< a >$، **زیرگروه دوری تولیدشده بوسیله** a نامیده می‌شود. اگر زیرگروه $< a >$ تمام‌گروه G باشد، گوییم G یک **گروه دوری** است. توجه کنید که هر گروه دوری آبلی است زیرا $a^i a^j = a^{i+j} = a^j a^i$.

مثال ۲۲.۷. طبق نتیجه ۹.۲، $U_{۱۵} = \{۱, ۲, ۴, ۷, ۸, ۱۱, ۱۳, ۱۴\}$ گروه ضربی یکه‌های حلقه $\mathbb{Z}_{۱۵}$ است. به منظور تعیین زیرگروه دوری تولیدشده توسط ۷، محاسبه می‌کنیم:

$$۷^۱ = ۷ \qquad ۷^۲ = ۴ \qquad ۷^۳ = ۱۳ \qquad ۷^۴ = ۱ = ۷^۰.$$

بنابراین عضو ۷ دارای مرتبه ۴ در $U_{۱۵}$ است. فرض کنید ۷^i هر عضوی از $< ۷ >$ باشد. عدد صحیح i باید همنهشت با یکی از اعداد ۰، ۱، ۲ یا ۳ به پیمانه ۴ باشد. بنابراین به موجب قضیه ۵.۷، ۷^i برابر یکی از $۷^۰$، $۷^۱$، $۷^۲$ یا $۷^۳$ است. پس $< ۷ > = \{۷, ۴, ۱۳, ۱\}$. این زیرگروه دوری دارای مرتبه‌ای برابر مرتبه عضوی است که آن را تولید می‌کند (یعنی ۴). توجه کنید که زیرگروه دوری $< ۱۳ >$ تولید شده بوسیله ۱۳ همان زیرگروه دوری $< ۷ >$ است زیرا $۱۳^۲ = ۴$، $۱۳^۳ = ۷$ و $۱۳^۴ = ۱$. بنابراین یک زیرگروه دوری ممکن است توسط عناصر متفاوتی تولید شود.

استدلال بکار رفته در مثال قبلی در حالت کلی نیز کارآمد است و ارتباط بین دو کاربرد از کلمه "مرتبه" را بدست می‌دهد. در واقع، مضمون آن، این است که مرتبه هر عضو a برابر مرتبهٔ زیرگروه تولیدشده بوسیله a است.

قضیه ۱۰.۷. فرض کنید G یک گروه باشد و فرض کنید $a \in G$.

(۱) اگر a دارای مرتبه نامتناهی باشد، در این صورت $< a >$ یک زیرگروه نامتناهی است که از عناصر متمایز a^k با $k \in \mathbb{Z}$ تشکیل شده است.

(۲) اگر a دارای مرتبه متناهی n باشد، در این صورت $< a >$ یک زیرگروه از مرتبه n است و $< a > = \{e = a^۰, a^۱, a^۲, a^۳, \ldots, a^{n-۱}\}$.

برهان. (۱) این یک نتیجه فوری از قسمت (۱) قضیه ۵.۷ است.

(۲) فرض کنید a^i عضوی دلخواه از $< a >$ باشد. در این صورت i با یکی از اعداد ۰، ۱، ۲، ... و $n - ۱$ همنشهت به پیمانه n می‌باشد. در نتیجه، طبق قسمت (۲) قضیه ۵.۷، a^i

باید برابر با یکی از a^0، a^1، a^2، ...، a^{n-1} باشد. به علاوه هیچ دو تای از این توانها برابر نیستند، زیرا هیچ دو تای از اعداد صحیح ۰، ۱، ۲، ...، $n-1$ همنهشت به پیمانه n نیست. بنابراین $< a >= \{a^0, a^1, a^2, \ldots, a^{n-1}\}$ یک گروه از مرتبه n است. ■

وقتی که عمل گروه با نماد جمعی نوشته شود، در این صورت توانهای یک عضو a عبارت است از

$$a, \quad a+a=2a, \quad a+a+a=3a, \ldots$$
$$-a, \quad -a-a=-2a, \quad -a-a-a=-3a, \ldots$$

و $0a = 0$. بنابراین $< a >= \{na \mid n \in \mathbb{Z}\}$. به‌عنوان مثال، مجموعه E متشکل از همه اعداد صحیح زوج یک زیرگروه از گروه جمعی $\mathbb{Z}$ است، زیرا $E = \{n2 \mid n \in \mathbb{Z}\} = < 2 >$.

مثال ۲۳.۷. چون $\mathbb{Z} = \{n1 \mid n \in \mathbb{Z}\}$، لذا $\mathbb{Z}$ یک گروه دوری نامتناهی با مولد ۱ است، یعنی، $\mathbb{Z} = < 1 >$. به‌طور مشابه برای هر n، گروه $\mathbb{Z}_n$ یک گروه دوری است زیرا $\mathbb{Z}_n$ از "توانهای" ۱ تشکیل شده است: ۱، $1+1=2$، $1+1+1=3$، و غیره.

حال که ساختار گروههای دوری را دیدیم، قدم بعدی بررسی زیرگروههای ممکن یک گروه دوری است.

قضیه ۱۱.۷. هر زیرگروه از یک گروه دوری، خود دوری است.

برهان. فرض کنید $G = < a >$ و H یک زیرگروه G باشد. اگر $H = < e >$، در این صورت H زیرگروه دوری تولیدشده به وسیله e است (همه توانهای آن برابر e است). اگر $H \neq < e >$، در این صورت H شامل یک عضو غیرهمانی از G، مثلاً a^i با $i \neq 0$ می‌باشد. چون H یک زیرگروه است، عضو وارون a^{-i} نیز در H است. یکی از i یا $-i$ مثبت است و لذا H توان مثبتی از a را شامل است. فرض کنید k کوچکترین عدد صحیح مثبت باشد به قسمی که $a^k \in H$. ادعا می‌کنیم که H زیرگروه دوری تولیدشده به وسیله a^k است. برای اثبات این، باید نشان دهیم که هر عضو H توانی از a^k است. اگر $h \in H$، در این صورت $h \in G$، لذا برای برخی m، $h = a^m$. طبق الگوریتم تقسیم $m = kq + r$ با $0 \leq r < k$، در نتیجه

$$a^r = a^{m-kq} = a^m a^{-kq} = a^m (a^k)^{-q}.$$

چون a^m و a^k هر دو در H هستند، لذا بدلیل بسته بودن، $a^r \in H$. چون a^k کوچکترین

توان مثبت a در H است و چون $r < k$، باید داشته باشیم $r = 0$. بنابراین $m = kq$ و $h = a^m = a^{kq} = (a^k)^q \in < a^k >$. بنابراین $H = < a^k >$. ■

برای کسب آگاهی بیشتر در مورد ساختار گروههای دوری و زیرگروههای آنها، تمرین‌های ۳۶-۳۴ را ملاحظه کنید.

فرض کنید G یک گروه باشد و $a \in G$. زیرگروه دوری $< a >$ را به عنوان گروهی که از یک مجموعه تک عضوی $S = \{a\}$ به‌صورت زیر ساخته می‌شود در نظر بگیرید. همه حاصل‌ضربهای ممکن a و a^{-1} با هر ترتیب ممکن را تشکیل دهید. البته، هرکدام از این حاصل‌ضربها به عضوی به‌صورت a^n کاهش می‌یابد. می‌خواهیم این فرآیند را به یک مجموعه S که ممکن است بیشتر از یک عضو داشته باشد تعمیم دهیم.

قضیه ۱۲.۷. فرض کنید S زیرمجموعه‌ای غیرتهی از یک گروه G باشد. فرض کنید $< S >$ مجموعه همه حاصل‌ضربهای ممکن، با هر ترتیب، از اعضای S و وارونهای آنها باشد[۱۲]. در این صورت

(۱) $< S >$ یک زیرگروه G است که مجموعه S را شامل است.

(۲) اگر H یک زیرگروه G باشد که مجموعه S را شامل است، در این صورت H تمام زیرگروه $< S >$ را شامل است.

این قضیه نشان می‌دهد که $< S >$ کوچکترین زیرگروه G است که مجموعه S را شامل است. در حالت خاص وقتی که $S = \{a\}$، گروه $< S >$ همان زیرگروه $< a >$ است که کوچکترین زیرگروه G می‌باشد که a را شامل است. گروه $< S >$، **زیرگروه تولیدشده توسط S** نامیده می‌شود. اگر $< S >$ همه G باشد، گوییم S، G را تولید می‌کند و عناصر S **مولدهای** G نامیده می‌شوند.

برهان قضیه ۱۲.۷. (۱) چون مجموعه S غیرتهی است، $< S >$ غیرتهی است و هر عضو S (وقتی که به عنوان یک حاصل‌ضرب تک عضوی در نظر گرفته شود) عضوی از $< S >$ است. اگر $a, b \in < S >$، آنگاه a به صورت $a_1 a_2 \cdots a_k$ است که در آن $k \geq 1$ و هر a_i یا یک عضو S است یا وارون یک عضو S می‌باشد. به طور مشابه $b = b_1 b_2 \cdots b_t$، که در آن $t \geq 1$ و هر b_i یا یک عضو S است یا وارون یک عضو S می‌باشد. بنابراین حاصل‌ضرب $ab = a_1 a_2 \cdots a_k b_1 b_2 \cdots b_t$ از اعضای S یا وارون اعضای S تشکیل شده است. پس $ab \in < S >$ و $< S >$ بسته است. طبق نتیجه ۳.۷، وارون عضو $a = a_1 a_2 \cdots a_k$ از $< S >$ عضو $a^{-1} = a_k^{-1} \cdots a_2^{-1} a_1^{-1}$ است.

۱۲) ما وجود حاصل‌ضربهایی با یک عضو را می‌پذیریم لذا عناصر S در $< S >$ خواهند بود.

چون هر a_i یا یک عضو S است یا وارون یک عضو S می‌باشد، همین مطلب برای a_i^{-1} نیز درست است. بنابراین $a^{-1} \in < S >$. پس طبق قضیه ۷.۷، $< S >$ یک زیرگروه G است.

(۲) هر زیرگروهی که مجموعه S را شامل باشد باید وارون هر عضو S را نیز شامل باشد. طبق بسته بودن، این زیرگروه باید همه حاصلضربهای ممکن، با هر ترتیب، از عناصر S و وارونهای آنها را شامل باشد. بنابراین هر زیرگروهی که مجموعه S را شامل باشد باید همچنین تمام $< S >$ را شامل باشد. ■

مثال ۲۴.۷. گروه $U_{۱۵} = \{۱, ۲, ۴, ۷, ۸, ۱۱, ۱۳, ۱۴\}$ توسط مجموعه $\{۷, ۱۱\}$ تولید شده است، چون

$$۷^۱ = ۷ \qquad ۷^۲ = ۴ \qquad ۷^۳ = ۱۳ \qquad ۷^۴ = ۱$$
$$۱۱^۱ = ۱۱ \qquad ۷ \cdot ۱۱ = ۲ \qquad ۷^۲ \cdot ۱۱ = ۱۴ \qquad ۷^۳ \cdot ۱۱ = ۸$$

مجموعه‌های متمایز ممکن است گروه یکسانی را تولید کنند. برای مثال می‌توانید به‌سادگی بررسی کنید که مجموعه $\{۲, ۱۳\}$ نیز $U_{۱۵}$ را تولید می‌کند (تمرین ۱۱)

مثال ۲۵.۷. با استفاده از جدول عمل واقع در مثال ۹.۷، می‌بینیم که در گروه $D_۴$،

$$(r_۱)^۱ = r_۱ \qquad (r_۱)^۲ = r_۲ \qquad (r_۱)^۳ = r_۳ \qquad (r_۱)^۴ = r_۰$$
$$h^۱ = h \qquad r_۱ \circ h = t \qquad (r_۱)^۲ \circ h = r \qquad (r_۱)^۳ \circ h = d$$

بنابراین $D_۴$ توسط $\{r_۱, h\}$ تولید شده است. توجه کنید که نمایش عناصر گروه بر حسب مولدها یکتا نیست؛ برای مثال

$$r_۱ \circ h \circ (r_۱)^۲ = d \qquad \text{و} \qquad (r_۱)^۳ \circ h = d.$$

تمرینها

A ۱. فرض کنید H زیرگروهی از گروه G باشد. اگر e_G عضو همانی G و e_H عضو همانی H باشد، ثابت کنید که $e_G = e_H$.

۲. نشان دهید که مشابه تمرین ۱ برای حلقه‌ها ممکن است نادرست باشد: اگر G حلقه‌ای با عضو همانی ضربی e_G و H زیرحلقه‌ای با عضو همانی e_H باشد، در این صورت e_H ممکن

است برابر با e_G نباشد. [راهنمایی: زیرحلقه $\{(n,0) \mid n \in \mathbb{Z}\}$ از $\mathbb{Z} \times \mathbb{Z}$ را در نظر بگیرید.]

۳. (الف) فرض کنید H و K زیرگروههایی از یک گروه G باشند. ثابت کنید که $H \cap K$ یک زیرگروه G است.

(ب) فرض کنید $\{H_i\}$ گردایه دلخواهی از زیرگروههای G باشد. ثابت کنید که $\cap H_i$ یک زیرگروه G است.

۴. فرض کنید H و K زیرگروههایی از یک گروه G باشند.

(الف) با مثال نشان دهید که $H \cup K$ لزوماً یک زیرگروه G نیست.

(ب) ثابت کنید که $H \cup K$ زیرگروهی از G است اگر و تنها اگر $H \subseteq K$ یا $K \subseteq H$.

۵. فرض کنید G_1 زیرگروهی از G و H_1 زیرگروهی از H باشد. ثابت کنید که $G_1 \times H_1$ زیرگروهی از $G \times H$ است.

۶. فرض کنید G یک گروه آبلی و T مجموعه عناصر با مرتبه متناهی G باشد. ثابت کنید که T یک زیرگروه G است؛ T **زیرگروه تابدار** G نامیده می‌شود. (اگر G غیرآبلی باشد این نتیجه ممکن است برقرار نباشد؛ تمرین ۱۸ بخش ۲.۷ را ملاحظه کنید.)

۷. همه زیرگروههای دوری U_{15} را فهرست کنید.

۸. همه زیرگروههای دوری U_{30} را فهرست کنید.

۹. عناصر زیرگروه $< a >$ از S_7 که در آن $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 6 & 5 & 1 & 4 \end{pmatrix}$ را فهرست کنید.

۱۰. فرض کنید G یک گروه و $a \in G$. ثابت کنید که $< a > = < a^{-1} >$.

۱۱. نشان دهید U_{15} توسط مجموعه $\{2, 13\}$ تولید شده است.

۱۲. نشان دهید که گروه واقع در تمرین ۱۶ بخش ۱.۷ می‌تواند توسط ۲ عضو تولید شود

۱۳. نشان دهید که تنها مولدهای گروه دوری جمعی $\mathbb{Z}$، ۱ و ۱− هستند.

۱۴. نشان دهید که $(1, 0)$ و $(2, 0)$ گروه جمعی $\mathbb{Z} \times \mathbb{Z}_7$ را تولید می‌کنند.

۱۵. (الف) نشان دهید که گروه جمعی $\mathbb{Z}_۲ \times \mathbb{Z}_۳$ دوری است.

(ب) نشان دهید که گروه جمعی $\mathbb{Z}_۲ \times \mathbb{Z}_۲$ دوری نیست ولی توسط دو عنصر تولید شده است.

۱۶. نشان دهید که $(۳,۱)$، $(۱-,۲-)$ و $(۴,۳)$ گروه جمعی $\mathbb{Z} \times \mathbb{Z}$ را تولید می‌کنند.

۱۷.B. ثابت کنید که زیرمجموعه غیرتهی H از گروه G زیرگروهی از G است اگر و تنها اگر هرگاه $a, b \in H$، در این صورت $ab^{-۱} \in H$.

۱۸. فرض کنید G گروهی آبلی و n یک عدد صحیح مثبت ثابت باشد.

(الف) ثابت کنید که $H = \{a \in G \mid a^n = e\}$ زیرگروهی از G است.

(ب) با مثال نشان دهید که اگر G غیرآبلی باشد، قسمت (الف) ممکن است نادرست باشد. [راهنمایی: $S_۳$.]

۱۹. **مرکز** گروه G عبارت است از مجموعه

$$Z(G) = \{a \in G \mid ag = ga \quad \text{برای هر } g \in G\}.$$

نشان دهید $Z(G)$ یک زیرگروه G است.

۲۰. نشان دهید که $\{r_۰, r_۲\}$ مرکز $D_۴$ است.

۲۱. فرض کنید G یک گروه باشد و $a \in G$. **مرکزساز** a عبارت است از مجموعهٔ $C(a) = \{g \in G \mid ga = ag\}$. ثابت کنید که $C(a)$ زیرگروهی از G است.

۲۲. اگر G یک گروه باشد، ثابت کنید که $Z(G) = \bigcap_{a \in G} C(a)$ (نماد همانند تمرینهای ۱۹ و ۲۱ می‌باشد).

۲۳. ثابت کنید یک عضو a در مرکز G قرار دارد اگر و تنها اگر $C(a) = G$.

۲۴. فرض کنید $A(T)$ گروه جایگشتهای مجموعه T باشد و فرض کنید $T_۱$ یک زیرمجموعه غیرتهی از T باشد. ثابت کنید { برای هر $H = \{f \in A(T) \mid f(t) = t, t \in T_۱\}$ یک زیرگروه $A(T)$ است.

۲۵. فرض کنید T و $T_۱$ مثل آنچه در تمرین ۲۴ است باشند. ثابت کنید که $K = \{f \in A(T) \mid f(T_۱) = T_۱\}$ زیرگروهی از T است که زیرگروه H واقع در تمرین

۲۴ را شامل است. بررسی کنید که اگر T_1 بیشتر از یک عضو داشته باشد در این صورت $K \neq H$.

۲۶. (الف) فرض کنید H و K زیرگروههایی از یک گروه آبلی G باشند. قرار دهید، $HK = \{ab \mid a \in H, b \in K\}$. ثابت کنید که HK یک زیرگروه G است.

(ب) نشان دهید که اگر G غیرآبلی باشد، قسمت (الف) ممکن است نادرست باشد.

۲۷. فرض کنید H زیرگروهی از G باشد و برای $x \in G$، فرض کنید $x^{-1}Hx$ مجموعه $\{x^{-1}ax \mid a \in H\}$ را نشان دهد. ثابت کنید $x^{-1}Hx$ یک زیرگروه G است.

۲۸. فرض کنید H زیرگروهی از G باشد و فرض کنید برای هر $x \in G$، $x^{-1}Hx \subseteq H$ (نماد مثل تمرین ۲۷). ثابت کنید که برای هر $x \in G$، $x^{-1}Hx = H$.

۲۹. اگر H زیرگروهی از G باشد، در این صورت **نرمالساز** H عبارت است از مجموعهٔ $N_H = \{x \in G \mid x^{-1}Hx = H\}$ (نماد مثل تمرین ۲۷). ثابت کنید که N_H یک زیرگروه G است که H را شامل است.

۳۰. فرض کنید H مجموعه ماتریسهایی به صورت $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ باشد که در آن $a \in \{1, -1\}$ و $b \in \mathbb{R}$. ثابت کنید که H یک زیرگروه $GL(2, \mathbb{Q})$ است.

۳۱. فرض کنید G یک گروه آبلی و n یک عدد صحیح مثبت باشد. ثابت کنید که $H = \{a^n \mid a \in G\}$ یک زیرگروه G است.

۳۲. فرض کنید k یک شمارندهٔ مثبت عدد صحیح مثبت n باشد. ثابت کنید که مجموعه $H_k = \{a \in U_n \mid a \equiv 1 \ (k \text{ پیمانه})\}$ یک زیرگروه U_n است.

۳۳. همه زیرگروههای $\mathbb{Z}_{12}$ را فهرست کنید. همین مطلب را برای $\mathbb{Z}_{20}$ انجام دهید.

۳۴. فرض کنید $G =< a >$ یک گروه دوری از مرتبه n باشد.

(الف) ثابت کنید که زیرگروه دوری تولیدشده توسط a^m با زیرگروه دوری تولیدشده توسط a^d، که در آن $d = (m, n)$ یکسان است. [راهنمایی: کافی است نشان دهید که a^d توانی از a^m است و بالعکس. (چرا؟) توجه کنید که طبق قضیه ۳.۱، اعداد صحیح u و v وجود دارند به قسمی که $d = mu + nv$.]

(ب) ثابت کنید که a^m مولد G است اگر و تنها اگر $(m, n) = ۱$.

۳۵. فرض کنید $G =< a >$ گروهی دوری از مرتبه n باشد. اگر H یک زیرگروه G باشد، نشان دهید که $| H |$ یک شمارندهٔ n است. [راهنمایی: تمرین ۳۴ و قضیه ۱۱.۷.]

۳۶. فرض کنید $G =< a >$ یک گروه دوری از مرتبه n باشد. اگر k یک شمارنده مثبت n باشد، ثابت کنید که G دارای یک زیرگروه یکتا از مرتبهٔ k است. [راهنمایی: زیرگروه تولیدشده بوسیله $a^{n/k}$ را در نظر بگیرید.]

۳۷. فرض کنید G یک گروه آبلی از مرتبه mn باشد که در آن $(m, n) = ۱$. فرض کنید G شامل یک عنصر a از مرتبه m و یک عنصر b از مرتبهٔ n باشد. ثابت کنید که G دوری با مولد ab است.

۳۸. نشان دهید که گروه ضربی $\mathbb{R}^*$ متشکل از اعداد حقیقی غیرصفر دوری نیست.

۳۹. نشان دهید که گروه جمعی $\mathbb{Q}$ دوری نیست.

۴۰. فرض کنید G و H گروه باشند. اگر $G \times H$ یک گروه دوری باشد ثابت کنید که G و H هر دو دوری هستند. (تمرین ۱۵ (ب) نشان می‌دهد که عکس این مطلب درست نیست.)

۴۱. ثابت کنید که $\mathbb{Z}_m \times \mathbb{Z}_n$ دوری است اگر و تنها اگر $(m, n) = ۱$.

۴۲. ثابت کنید که $\left\{ \begin{pmatrix} ۱ & n \\ ۰ & ۱ \end{pmatrix} \mid n \in \mathbb{Z} \right\}$ یک زیرگروه دوری $GL(۲, \mathbb{R})$ است.

۴۳. اگر $G \neq < e >$ گروهی باشد که دارای هیچ زیرگروه سره‌ای نیست، ثابت کنید که G یک گروه دوری از مرتبه اول است.

۴۴. آیا گروه جمعی $G = \{a + b\sqrt{۲} \mid a, b \in \mathbb{Z}\}$ دوری است؟

۴۵. (الف) نشان دهید که گروه $U_{۱۸}$ متشکل از یکه‌های $\mathbb{Z}_{۱۸}$ دوری است.

(ب) نشان دهید که گروه $U_{۲۰}$ متشکل از یکه‌های $\mathbb{Z}_{۲۰}$ دوری نیست.

۴۶. اگر S زیرمجموعه‌ای غیرتهی از گروه G باشد، نشان دهید که $< S >$ اشتراک خانواده همه زیرگروههای H است به قسمی که $S \subseteq H$.

۴-۷ یکریختی

دو گروه را، به بیان غیررسمی، یکریخت گویند اگر دارای ساختار یکسانی باشند، یعنی تفاوت آنها تنها در طرز نمایه‌گذاری آنها باشد. برای گروههای متناهی، این بدان معنی است که جدول عمل یک گروه با یک تغییر نمایه‌گذاری مناسب قابل بدست آمدن از جدول عمل گروه دیگر است. چنین تغییر نمایه‌گذاری معادل با یک تابع دوسویی است و لذا ما تعریف رسمی زیر را داریم (که تقریباً با تعریف ارائه شده برای حلقه‌ها یکسان است):

تعریف. فرض کنید G و H دو گروه باشند و فرض کنید عمل هر دو گروه با $*$ نشان داده شده باشد. G **یکریخت** با H است (نوشته می‌شود $G \cong H$) اگر یک تابع $f : G \to H$ وجود داشته باشد به قسمی که

(i) f یک به یک باشد؛

(ii) f پوشا باشد؛

(iii) برای هر $a, b \in G$، $f(a * b) = f(a) * f(b)$.

در این حالت، تابع f یک **یکریختی** نامیده می‌شود. یک تابع که در شرط (iii) صدق کند امّا لزوماً یک به یک یا پوشا نباشد، یک **همریختی** نامیده می‌شود.

دقیقاً مثل مبحث حلقه‌ها، تعریف یکریختی متقارن است. اگر $f : G \to H$ یک یکریختی باشد، در این صورت f یک نگاشت دوسویی از مجموعه‌هاست و بنابراین دارای یک تابع وارون دوسویی $g : H \to G$ است به قسمی که fog نگاشت همانی روی H و gof نگاشت همانی روی G است.[۱۳] یک بررسی ساده (تمرین ۲۰) نشان می‌دهد که g نیز یک یکریختی است، یعنی برای هر $c, d \in H$، $g(c * d) = g(c) * g(d)$. بنابراین $G \cong H$ اگر و تنها اگر $H \cong G$.

ما به طور موقت نماد $*$ را برای نشان دادن عمل گروهها بکار بردیم تا یادآوری کنیم که عمل یک گروه خاص ممکن است جمع، یا ضرب، یا ترکیب، یا چیز دیگری باشد. برای مثال، وقتی G یک گروه جمعی و H یک گروه ضربی باشد، در این صورت شرط (iii) تعریف به‌صورت $f(a+b) = f(a)f(b)$ تعبیر می‌شود. وقتی G ضربی و H جمعی باشد، در این صورت شرط (iii) به‌صورت $f(ab) = f(a) + f(b)$ در می‌آید

---

۱۳) پیوست ب را ملاحظه کنید

مثال ۲۶.۷. گروه ضربی $U_8 = \{1,3,5,7\}$ متشکل از یکه‌های $\mathbb{Z}_8$ یکریخت با گروه جمعی $\mathbb{Z}_2 \times \mathbb{Z}_2$ است. برای اثبات این مطلب فرض کنید $f : U_8 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ به صورت زیر تعریف شده باشد.

$$f(1) = (0,0) \quad f(3) = (1,0) \quad f(5) = (0,1) \quad f(7) = (1,1)$$

واضح است که f یک دوسویی است. اثبات این که برای هر $a, b \in U_8$، $f(ab) = f(a) + f(b)$. معادل با این است که نشان دهیم جدول عمل $\mathbb{Z}_2 \times \mathbb{Z}_2$ تنها با جایگزین کردن هر $a \in U_8$ توسط $f(a) \in \mathbb{Z}_2 \times \mathbb{Z}_2$، قابل بدست آمدن از جدول عمل U_8 است[۱۴] با استفاده از جداول زیر تحقیق کنید که این مطلب در واقع درست است. بنابراین f یک یکریختی است.

$\mathbb{Z}_2 \times \mathbb{Z}_2$

+	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

U_8

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

مثال ۲۷.۷. گروه جمعی اعداد حقیقی $\mathbb{R}$، یکریخت با گروه ضربی اعداد حقیقی مثبت $\mathbb{R}^{**}$ می‌باشد. برای اثبات این مطلب، فرض کنید $f : \mathbb{R} \to \mathbb{R}^{**}$ توسط $f(r) = 10^r$ داده شده باشد. اگر $f(r) = f(s)$، در این صورت $10^r = 10^s$، لذا $r = \log 10^r = \log 10^s = s$. بنابراین f یک به یک است. اگر $k \in \mathbb{R}^{**}$، در این صورت $r = \log k$ یک عدد حقیقی خوش‌تعریف است و $f(r) = 10^r = 10^{\log k} = k$. بنابراین f پوشا است. سرانجام f یک همریختی است زیرا $f(r+s) = 10^{r+s} = 10^r 10^s = f(r)f(s)$. بنابراین f یک یکریختی است و $\mathbb{R} \cong \mathbb{R}^{**}$.

مثال ۲۸.۷. هر یکریختی حلقه‌ای $f : R \to S$ یک یکریختی از گروههای آبلی نیز می‌باشد زیرا f دوسویی است و برای هر $a, b \in R$، $f(a+b) = f(a) + f(b)$. همانگونه که در مثال بعدی می‌بینیم عکس این گزاره ممکن است نادرست باشد.

---

۱۴) برای توضیحی در این مورد، بحث یکریختی حلقه‌ها را که بعد از مثال ۲۱۳ ارائه شد ملاحظه کنید.

مثال ۲۹.۷. فرض کنید E گروه جمعی اعداد صحیح زوج باشد و فرض کنید $f : \mathbb{Z} \to E$ توسط $f(a) = ۲a$ تعریف شده باشد. می‌توانید به‌سادگی بررسی کنیدکه f یک دوسویی است. به‌علاوه برای $a, b \in \mathbb{Z}$ داریم $f(a+b) = ۲(a+b) = ۲a + ۲b = f(a) + f(b)$. بنابراین f یک یکریختی از گروههای آبلی است. با این حال f یک یکریختی حلقه‌ای نیست؛ در واقع هیچ یکریختی حلقه‌ای بین $\mathbb{Z}$ و E موجود نیست زیرا $\mathbb{Z}$ یک حلقه یکدار است و E چنین نیست.

مثال ۳۰.۷. گروههای $S_۳$ و $\mathbb{Z}_۶$ هر دو دارای مرتبه ۶ هستند امّا یکریخت نیستند. در واقع، هیچ گروه آبلی (مانند $\mathbb{Z}_۶$) نمی‌تواند با یک گروه غیرآبلی (مانند $S_۳$) یکریخت باشد. اثبات این حقیقت اساساً مثل اثبات در حالت حلقه‌هاست؛ مثال۲۷.۳ را ملاحظه کنید.

مثال ۳۱.۷. یک یکریختی از یک گروه G به خودش را یک **خودریختی** از G گویند. در اینجا روشی برای ساختن دسته‌ای از خودریختی‌های G را ارائه می‌کنیم. یک عضو ثابت c از G را در نظر گرفته و $f : G \to G$ را توسط $f(a) = c^{-۱}ac$ تعریف کنید[۱۵]. در این صورت f یک همریختی است زیرا

$$f(a)f(b) = (c^{-۱}ac)(c^{-۱}bc) = c^{-۱}a(cc^{-۱})bc = c^{-۱}abc = f(ab).$$

اگر $g \in G$، در این صورت $g = c^{-۱}(cgc^{-۱})c = f(c^{-۱}gc)$، لذا f پوشا است. اگر $f(a) = f(b)$، در این صورت $c^{-۱}ac = c^{-۱}bc$. طبق قضیه ۲.۷ با حذف c از طرف راست و $c^{-۱}$ از طرف چپ خواهیم داشت $a = b$؛ بنابراین f یک به یک است. پس f یک یکریختی است. این یکریختی را **خودریختی داخلی** G، القا شده توسط c نامند. برای اطلاعات بیشتر درباره خودریختیها، تمرین‌های ۲۲، ۲۳، ۳۸ و ۳۹ را ملاحظه کنید.

قضیه زیر به‌طور کامل همه گروههای دوری را تا حد یکریختی مشخص می‌کند.

قضیه ۱۳.۷. هر گروه دوری نامتناهی یکریخت با $\mathbb{Z}$ است. هر گروه دوری متناهی از مرتبه n، یکریخت با $\mathbb{Z}_n$ است.

این قضیه، به عنوان مثال بیان می‌کند که زیرگروه $< r, s >$ از $D_۴$ (یک گروه از مرتبه ۴) یکریخت

۱۵) اگر G آبلی باشد در این صورت $f(a) = c^{-۱}ac = c^{-۱}ca = a$، لذا f نگاشت همانی است. امّا اگر G غیرآبلی باشد، f ممکن است یک تابع غیرهمانی باشد.

با گروه جمعی $\mathbb{Z}_4$ است. به طور مشابه زیرگروه دوری نامتناهی $< 2 >$ از گروه ضربی اعداد حقیقی غیرصفر $\mathbb{R}^*$ یکریخت با گروه جمعی $\mathbb{Z}$ است.

برهان قضیه ۱۳.۷. فرض کنید $G =< a >$ یک گروه دوری نامتناهی باشد و $f : \mathbb{Z} \to G$ را توسط $f(i) = a^i$ تعریف کنید. طبق تعریف یک گروه دوری، f پوشاست و طبق قضیه ۱۰.۷ f یک به یک است، چون $f(i)f(j) = a^i a^j = a^{i+j} = f(i+j)$، f یک یکریختی است بنابراین $G \cong \mathbb{Z}$.

حال فرض کنید $G =< b >$ و b دارای مرتبه n باشد. در این صورت $\mathbb{Z}_n$ عبارت است از مجموعهٔ $\{0, 1, 2, \ldots, n-1\}$ و طبق قضیه ۱۰.۷، $G = \{b^0, b^1, b^2, \ldots, b^{n-1}\}$، لذا تابع $f : \mathbb{Z}_n \to G$ که توسط $f(i) = b^i$ داده می‌شود یک دوسویی است. برای نشان دادن این که f یک همریختی نیز هست، بخاطر آورید که وقتی از نماد کروشه استفاده نشود، چگونه جمع در $\mathbb{Z}_n$ عمل می‌کند: $i + j = k$ یعنی (پیمانه n) $i + j \equiv k$ و $0 \leq k \leq n-1$ بنابراین طبق قضیه ۵.۷، در G داریم $b^{i+j} = b^k$. در نتیجه

$$f((i+j)) = f(k) = b^k = b^{i+j} = b^i b^j = f(i)f(j)$$

بنابراین f یک یکریختی است و $\mathbb{Z}_n \cong G$. ■

بخاطر آورید که **تصویر** یک تابع $f : G \to H$، یک زیرمجموعه H است، در واقع داریم $\text{Im}f = \{h \in H \mid h = f(a)$ برای برخی $a \in G\}$. تابع f می‌تواند به عنوان یک نگاشت پوشا از G به $\text{Im}f$ در نظر گرفته شود.

قضیه ۱۴.۷. فرض کنید G و H گروههایی با عضوهای همانی به ترتیب e_G و e_H باشند و $f : G \to H$ یک همریختی باشد، در این صورت

(۱) $f(e_G) = e_H$.

(۲) برای هر $a \in G$، $f(a^{-1}) = f(a)^{-1}$.

(۳) $\text{Im}f$ یک زیرگروه H است.

(۴) اگر f یک به یک باشد، در این صورت $G \cong \text{Im}f$.

برهان. (۱) چون f یک همریختی است، e_G عضو همانی G و e_H عضو همانی H است، داریم

$$f(e_G)f(e_G) = f(e_G e_G) = f(e_G) = e_H f(e_G).$$

بنابراین طبق قانون حذف (قضیه ۲.۷)، $f(e_G) = e_H$.

(۲) داریم

$$f(a^{-1})f(a) = f(a^{-1}a) = f(e_G) = e_H = f(a)^{-1}f(a)$$

با حذف $f(a)$ از دو طرف بدست می‌آوریم $f(a^{-1}) = f(a)^{-1}$.

(۳) طبق (۱)، $e_H \in \mathrm{Im}f$ و لذا $\mathrm{Im}f$ غیرتهی است. چون $f(a)f(b) = f(ab)$، $\mathrm{Im}f$ بسته است. وارون هر $f(a) \in \mathrm{Im}f$ همچنان در $\mathrm{Im}f$ است زیرا طبق (۲)، $f(a)^{-1} = f(a^{-1})$. بنابراین طبق قضیه ۷.۷، $\mathrm{Im}f$ یک زیرگروه H است.

(۴) همان‌طور که قبل از قضیه تذکر داده شد، f می‌تواند به عنوان یک تابع پوشا از G به $\mathrm{Im}f$ در نظر گرفته شود. اگر f یک همریختی یک به یک باشد، آنگاه f یک یکریختی است. ■

نظریه گروهها با مطالعه جایگشتها و گروههایی از جایگشتها آغاز شد. تعریف یک گروه مجرد که بعدها تعریف شد ممکن است بسیار کلی‌تر از مفهوم یک گروه از جایگشتها بنظر برسد. قضیه زیر نشان می‌دهد که مطلب این چنین نیست. در اصل این قضیه بیان می‌کند که گروههای جایگشتی (تا حد یکریختی) تنها گروههای ممکن هستند. بویژه این قضیه نتیجه می‌دهد زیرگروههای گروههای متقارن S_n $(n \geq 1)$ تنها گروههای متناهی ممکن (تا حد یکریختی) هستند

قضیه ۱۵.۷. (**قضیه کیلی**[۱۶]) هر گروه G یکریخت با یک گروه از جایگشتها است.

برهان. گروه $A(G)$ متشکل از همه جایگشتهای مجموعه G را در نظر بگیرید. به یاد آورید که $A(G)$ از همه توابع دوسویی از G به G تشکیل شده است و عمل گروه، عمل ترکیب توابع است. این توابع لزوماً همریختی نیستند. برای اثبات قضیه، زیرگروهی از $A(G)$ را که یکریخت با G است می‌یابیم[۱۷] این کار را با ساختن یک همریختی گروهی یک به یک $f : G \to A(G)$ انجام می‌دهیم؛ در این صورت بنا به قضیه ۱۴.۷، G یکریخت با زیرگروه $\mathrm{Im}f$ از $A(G)$ است.

اگر $a \in G$، در این صورت ادعا می‌کنیم که نگاشت $\varphi_a : G \to G$ که توسط $\varphi_a(x) = ax$ تعریف می‌شود، یک دوسویی از مجموعه‌هاست (یعنی عضوی از $A(G)$ است). این مطلب از این حقیقت نتیجه می‌شود که اگر $b \in G$، در این صورت $\varphi_a(a^{-1}b) = a(a^{-1}b) = b$؛ بنابراین φ_a

(۱۶ Cayley's Theorem

(۱۷ گروه $A(G)$ اغلب بسیار بزرگتر از آن است که بتواند با G یکریخت باشد. برای مثال اگر G دارای مرتبه n باشد در این صورت به موجب تمرین ۱۸ بخش ۱۷ $A(G)$ دارای مرتبه $n!$ است

پوشاست. اگر $\varphi_a(b) = \varphi_a(c)$ در این صورت $ab = ac$. طبق قضیه ۲.۷، حذف a، نتیجه می‌دهد $b = c$. پس φ_a یک به یک و لذا یک دوسویی است. بنابراین $\varphi_a \in A(G)$.

حال $f : G \to A(G)$ را بوسیله $f(a) = \varphi_a$ تعریف کنید. برای هر $a, b \in G$، $f(ab) = \varphi_{ab}$ یک نگاشت از G به G است که توسط $\varphi_{ab}(x) = abx$ داده شده است. از طرف دیگر داریم $f(a) \circ f(b) = \varphi_a \circ \varphi_b$. بنابراین $f(ab) = f(a) \circ f(b)$ و f یک همریختی گروهی است. سرانجام، فرض کنید $f(a) = f(c)$، لذا برای هر $x \in G$، $\varphi_a(x) = \varphi_c(x)$. در این‌صورت $a = ae = \varphi_a(e) = \varphi_c(e) = ce = c$. پس f یک به یک است. لذا طبق قضیه ۱۴.۷ $G \cong \operatorname{Im} f$. ■

نتیجه ۱۶.۷. هر گروه متناهی G از مرتبه n یکریخت با زیرگروهی از گروه متقارن S_n است.

برهان. طبق قضیه ۱۵.۷، G یکریخت با یک زیرگروه H از $A(G)$ است. چون G یک مجموعه n عضوی است، طبق تمرین ۱۸، $A(G)$ یکریخت با S_n است. در نتیجه، طبق تمرین ۱۰، H یکریخت با یک زیرگروه K از S_n است. بنابراین طبق تمرین ۷، $G \cong K$. ■

یک **نمایش** از گروه G یک همریختی از G به گروهی از جایگشتها است. در این حالت گفته می‌شود که G **توسط یک گروه از جایگشتها نمایش** داده شده است. همریختی $G \to A(G)$ در اثبات قضیه ۱۵.۷، **نمایش منظم چپ** G نامیده می‌شود. با استفاده از چنین نمایشهایی، تحقیق در نظریه گروهها به مطالعهٔ گروههای جایگشتی تحویل می‌یابد. این رویکرد بعضاً بسیار مفید است زیرا جایگشتها اشیاء ملموسی هستند که به‌سادگی قابل تجسم هستند. انجام محاسبات با جایگشتها ساده است، در حالی که در پاره‌ای از گروهها انجام چنین محاسباتی همواره ساده نیست. در برخی حالات، نمایش‌های گروهی ابزار بسیار مؤثری هستند.

از طرف دیگر نمایش توسط جایگشتها دارای برخی نقاط ضعف است. به عنوان مثال، یک گروه ممکن است به طرق مختلف به‌عنوان گروهی از جایگشتها نمایش داده شود ـ همریختی $G \to A(G)$ در قضیه ۱۵.۷، تنها یکی از طرق ممکن نمایش G است (تمرین‌های ۲۴، ۳۱ و ۳۳ را برای نمایش‌های دیگر ملاحظه کنید). بسیاری از این نمایش‌ها ممکن است کاملاً بی‌فایده باشند. برای مثال، طبق قضیه ۱۶.۷، هر گروه از مرتبه ۱۲ یکریخت با زیرگروهی از S_{12} است، امّا S_{12} دارای مرتبه $۴۷۹۰۰۱۶۰۰ = 12!$ می‌باشد. بدست آوردن اطلاعات مفیدی درباره زیرگروهی از مرتبه ۱۲ در گروهی به این بزرگی در خوش‌بینانه‌ترین حالت، احتمالاً مشکل است.

به جز در برخی حالات خاص، مطالعه نظریه مقدماتی گروهها از طریق تعریف مجرد گروه (همانگونه که انجام داده‌ایم) بجای مطالعه آن از طریق نمایش‌های جایگشتی خاص احتمالاً مؤثرتر است. رویکرد مجرد دارای این مزّیت است که با حذف جنبه‌های غیراساسی، روی ساختار اصلی متمرکز می‌شود. این امر معمولاً منجر به اثباتهای ساده‌تر و قابل فهم‌تر می‌گردد.

تمرینها

۱.A. (الف) نشان دهید که تابع $f : \mathbb{R} \to \mathbb{R}$ که توسط $f(x) = ۳x$ داده شده است یک یکریختی از گروههای جمعی است.

(ب) فرض کنید $\mathbb{R}^{**}$ گروه ضربی اعداد حقیقی مثبت باشد. نشان دهید که $f : \mathbb{R}^{**} \to \mathbb{R}^{**}$ که توسط $f(x) = ۳x$ داده شده است، یک همریختی گروهی نیست.

۲. نشان دهید که تابع $g : \mathbb{R}^{**} \to \mathbb{R}^{**}$ که توسط $g(x) = \sqrt{x}$ داده شده است یک یکریختی است.

۳. (الف) عناصر گروه $GL(۲, \mathbb{Z}_۲)$ را فهرست کنید.

(ب) با نوشتن جداول عمل نشان دهید که دو گروه $GL(۲, \mathbb{Z}_۲)$ و $S_۳$ یکریخت هستند.

۴. نشان دهید که $U_۵$ با گروه جمعی $\mathbb{Z}_۴$ یکریخت است.

۵. نشان دهید که $U_۵$ با $U_{۱۰}$ یکریخت است.

۶. آیا $U_{۱۲}$ با گروه جمعی $\mathbb{Z}_۶$ یکریخت است؟

۷. اگر $f : G \to H$ و $g : H \to K$ یکریختی‌های گروهی باشند، ثابت کنید که تابع مرکب $gof : G \to K$ نیز یک یکریختی است.

۸. اگر $f : G \to H$ یک همریختی پوشای گروهی باشد و G آبلی باشد، ثابت کنید H آبلی است.

۹. فرض کنید $f : G \to H$ یک همریختی گروهی باشد. ثابت کنید که برای هر $a \in G$ و هر عدد صحیح n، $f(a^n) = f(a)^n$.

۱۰. اگر $f : G \to H$ یک یکریختی گروهی باشد و اگر T زیرگروهی از G باشد، ثابت کنید که $f(T) = \{f(a) \mid a \in T\}$ یکریخت با زیرگروه T است.

۱۱. (الف) فرض کنید H زیرگروهی از گروه G باشد و $a \in G$. ثابت کنید که $a^{-1}Ha = \{a^{-1}ha \mid h \in H\}$ یک زیرگروه G است که با H یکریخت است. [راهنمایی: تمرین ۱۰ را بکار برید، جایی که f خودریختی داخلی القاء شده توسط a باشد.]
(ب) اگر H متناهی باشد، ثابت کنید که $|H| = |a^{-1}Ha|$.

۱۲. فرض کنید G، H، G_1 و H_1 گروههایی باشند به قسمی که $G \cong H_1$ و $H \cong H_1$. ثابت کنید که $G \times H \cong G_1 \times H_1$.

۱۳. ثابت کنید که گروه G آبلی است اگر و تنها اگر تابع $f : G \to G$ که توسط $f(x) = x^{-1}$ داده شده است، یک همریختی گروهی باشد. در این حالت، نشان دهید که f یک یکریختی است.

۱۴.B. فرض کنید G یک گروه ضربی و c عضو ثابتی از G باشد. فرض کنید H همان مجموعه G باشد که با عمل جدید $a * b = acb$ مجهز شده است.
(الف) ثابت کنید که H یک گروه است.
(ب) ثابت کنید که نگاشت $f : G \to H$ تعریف شده بوسیله $f(x) = c^{-1}x$ یک یکریختی است.

۱۵. فرض کنید G یک گروه ضربی باشد. فرض کنید G^{op} همان مجموعه G باشد که با عمل جدید $a * b = ba$ مجهز شده است.
(الف) ثابت کنید G^{op} یک گروه است.
(ب) ثابت کنید $G \cong G^{op}$. [راهنمایی: نتیجه ۳.۷ می‌تواند مفید باشد.]

۱۶. اگر $G =< a >$ یک گروه دوری و $f : G \to G$ یک خودریختی باشد، نشان دهید که $f(a)$ یک مولد G است، یعنی $G =< f(a) >$.

۱۷. فرض کنید که هر دو عنصر a و b مولدهایی از گروه دوری G باشند، لذا $G =< a >$ و $G =< b >$. ثابت کنید که تابع $f : G \to G$ داده شده بوسیله $f(a^i) = b^i$ یک خودریختی از G است.

۱۸. فرض کنید T یک مجموعه n عضوی و $A(T)$ گروه جایگشتهای T باشد. ثابت کنید که $A(T) \cong S_n$. [راهنمایی: اگر عناصر T با یک ترتیب دلخواه توسط ۱، ۲، ...، n

نمایه‌گذاری شوند، در این صورت هر جایگشت از T یک جایگشت از ۱، ۲، ...، n می‌باشد.]

۱۹. اگر $f : G \to H$ یک همریختی گروهی یک به یک باشد و $a \in G$، ثابت کنید که $|a| = |f(a)|$.

۲۰. فرض کنید $f : G \to H$ یک یکریختی گروهی و $g : H \to G$ تابع وارون f که در **پیوست ب** تعریف شده است باشد. ثابت کنید که g نیز یک یکریختی گروهی است. [راهنمایی: تمرین ۲۴ بخش ۳.۳.]

۲۱. فرض کنید $f : G \to H$ یک همریختی گروهی و K یک زیرگروه H باشد. ثابت کنید که مجموعهٔ $\{a \in G \mid f(a) \in K\}$ زیرگروهی از G است.

۲۲. فرض کنید G یک گروه باشد و فرض کنید $\mathrm{Aut}G$ مجموعه همه خودریختیهای G باشد. ثابت کنید که $\mathrm{Aut}G$ تحت عمل ترکیب توابع یک گروه است. [راهنمایی: تمرین ۷ می‌تواند مفید باشد.]

۲۳. فرض کنید G یک گروه و $\mathrm{Aut}G$ همان‌طور که در تمرین ۲۲ بود باشد. فرض کنید $\mathrm{Inn}G$ مجموعه همه خودریختیهای داخلی G باشد (یعنی یکریختیهایی به شکل $f(a) = c^{-1}ac$ برای برخی $c \in G$، همان‌طور که در مثال ۳۱.۷ آمده است). ثابت کنید که $\mathrm{Inn}G$ زیرگروهی از $\mathrm{Aut}G$ است. [توجه کنید: دو عضو متفاوت G ممکن است خودریختی داخلی یکسانی را القاء کنند، یعنی ممکن است برای هر $a \in G$، داشته باشیم $c^{-1}ac = d^{-1}ad$. بنابراین $|\mathrm{Inn}G| \leq |G|$.]

۲۴. (الف) نشان دهید که $D_4 \cong S_4$. [راهنمایی: D_4 در مثال ۱۰.۷ توصیف شده است. هر حرکت در D_4، رئوس را جابجا می‌کند: این مطلب را بکار برده تا تابعی از D_4 به S_4 تعریف کنید.]

(ب) نشان دهید که D_4 یکریخت با زیرگروهی از S_4 است. [راهنمایی: راهنمایی قسمت (الف) را ملاحظه کنید. این یکریختی، D_4 را که یک گروه از مرتبه ۸ است به‌عنوان زیرگروهی از یک گروه جایگشتی از مرتبهٔ $4! = 24$ نمایش می‌دهد، در حالی که نمایش منظم چپ ارائه شده در نتیجه ۱۶.۷، G را به‌عنوان زیرگروهی از S_8 که یک گروه از مرتبه $8! = 40320$ است نمایش می‌دهد.]

۲۵. نشان دهید که گروههای جمعی $\mathbb{Z}$ و $\mathbb{Q}$ یکریخت نیستند.

۲۶. توضیح دهید که چرا هر یک از جفت گروههای داده‌شده یکریخت نیستند.

(الف) $\mathbb{Z}_4$ و S_3 (ب) $\mathbb{Z}_2 \times \mathbb{Z}_2$ و D_4

(پ) $\mathbb{Z}_2 \times \mathbb{Z}_2$ و $\mathbb{Z}_4 \times \mathbb{Z}_2$ (ت) $\mathbb{Z}$ و $\mathbb{R}$

۲۷. (الف) نشان دهید که U_8 یکریخت با U_{10} نیست.
(ب) نشان دهید که U_{10} یکریخت با U_{12} نیست.
(پ) آیا U_8 یکریخت با U_{12} است؟

۲۸. ثابت کنید که گروه جمعی اعداد حقیقی $\mathbb{R}$ با گروه ضربی اعداد حقیقی غیر صفر $\mathbb{R}^*$ یکریخت نیست. [راهنمایی: اگر یکریختی $f : \mathbb{R} \to \mathbb{R}^*$ وجود می‌داشت، در این صورت برای برخی k، $f(k) = -1$. این حقیقت را بکار برده تا به یک تناقض برسید.]

۲۹. نشان دهید که D_4 با گروه چهارگانی ارائه شده در تمرین ۱۴ بخش ۱.۷ یکریخت نیست.

۳۰. اگرچه $\mathbb{R}$ و $\mathbb{R}^{**}$ یکریختند، ثابت کنید که گروه جمعی $\mathbb{Q}$ با گروه ضربی اعداد گویای مثبت $\mathbb{Q}^{**}$ یکریخت نیست.

۳۱. فرض کنید G یک گروه و $A(G)$ گروه جایگشتهای مجموعه G باشد. با نظیرکردن هر $d \in G$ به خودریختی داخلی القاء شده توسط d^{-1} (مشابه مثال ۳۱.۷ با $c = d^{-1}$) یک تابع g از G به $A(G)$ تعریف کنید. ثابت کنید که g یک همریختی گروهی است.

۳۲. فرض کنید G یک گروه باشد و $h \in A(G)$. فرض کنید برای هر $a \in G$، $h \circ \varphi_a = \varphi_a \circ h$ (که در آن φ_a همریختی تعریف شده در اثبات قضیه ۱۵.۷ است). ثابت کنید عضو $b \in G$ وجود دارد به قسمی که برای هر $x \in G$، $h(x) = xb^{-1}$.

۳۳. (الف) فرض کنید G یک گروه باشد و $c \in G$. ثابت کنید که نگاشت $\theta_c : G \to G$ داده شده بوسیله $\theta_c(x) = xc^{-1}$، یک عضو $A(G)$ است.
(ب) ثابت کنید که تابع $h : G \to A(G)$ تعریف شده بوسیله $h(c) = \theta_c$ یک همریختی گروهی یک به یک است. بنابراین G یکریخت با زیرگروه $\mathrm{Im}h$ از $A(G)$ است. **این نمایش منظم راست** G است.

۳۴. نمایش منظم چپ هرکدام از گروههای زیر را بیابید (یعنی مانند اثبات قضیه ۱۵.۷، هر گروه را به عنوان یک گروه جایگشتی بیان کنید).

(الف) $\mathbb{Z}_۳$ (ب) $\mathbb{Z}_۴$ (پ) $S_۳$.

۳۵. (الف) ثابت کنید که $H = \left\{ \begin{pmatrix} ۱-n & -n \\ n & ۱+n \end{pmatrix} \mid n \in \mathbb{Z} \right\}$ تحت ضرب ماتریسی یک گروه است.

(ب) ثابت کنید که $H \cong \mathbb{Z}$.

۳۶. (الف) ثابت کنید که $K = \left\{ \begin{pmatrix} ۱-۲n & n \\ -۴n & ۱+۲n \end{pmatrix} \mid n \in \mathbb{Z} \right\}$ تحت ضرب ماتریسی یک گروه است.

(ب) آیا K یکریخت با $\mathbb{Z}$ است؟

۳۷. ثابت کنید که گروه جمعی $\mathbb{Z}[x]$ با گروه ضربی اعداد گویای مثبت $\mathbb{Q}^{**}$ یکریخت است. [راهنمایی: فرض کنید $p_۰$، $p_۱$، $p_۲$، ... اعداد اول مثبت متمایزی با ترتیب معمول خود باشند. تابع $\varphi : \mathbb{Z}[x] \to \mathbb{Q}^{**}$ را توسط

$$\varphi(a_۰ + a_۱x + a_۲x^۲ + \cdots + a_nx^n) = p_۰^{a_۰} p_۱^{a_۱} \cdots p_n^{a_n}$$

تعریف کنید.]

۳۸. ثابت کنید که G گروهی آبلی است اگر و تنها اگر $\mathrm{Inn}G$ شامل تنها یک عضو باشد. [راهنمایی: تمرین ۲۳ را ملاحظه کنید.]

۳۹. (الف) بررسی کنید که گروه $\mathrm{Inn}D_۴$ دارای مرتبهٔ ۴ است. [راهنمایی، تمرین ۲۳ را ملاحظه کنید.]

۴۰. ثابت کنید که $\mathrm{Aut}\mathbb{Z} \cong \mathbb{Z}_۲$. [راهنمایی: مولدهای ممکن گروه دوری $\mathbb{Z}$ چه می‌تواند باشد؟ تمرینهای ۱۶ و ۱۷ را ملاحظه کنید.]

۴۱. ثابت کنید که $\mathrm{Aut}\mathbb{Z}_n \cong U_n$. [راهنمایی: تمرین ۱۷ بالا و تمرین ۳۴ بخش ۷-۳ را ملاحظه کنید.]

۴۲. ثابت کنید که $\mathrm{Aut}(\mathbb{Z}_۲ \times \mathbb{Z}) \cong S_۳$.

۵-۷ همنهشتی و زیرگروههای نرمال

در این بخش و بخش بعدی مشابه گروهی مفاهیمی چون ایده‌آلها، همنهشتی‌ها و حلقه‌های خارج قسمتی را ارائه می‌کنیم. به جز تغییرات نمادی لازم، همانگونه که در جدول زیر نشان داده شده است، نتایج این بخش با نتایجی که پیشتر برای اعداد صحیح و حلقه‌ها ثابت شده‌اند در اصل یکسان می‌باشند. قبل از خواندن هر قضیه در این بخش، بهتر است قضیه نظیر آن را برای اعداد صحیح و حلقه‌ها بازخوانی کرده تا پیشرفت هماهنگ مباحث را ببینید.

گروهها	حلقه‌ها	اعداد صحیح
قضیه ۱۷.۷	قضیه ۲.۶	قضیه ۱.۲
قضیه ۱۸.۷	قضیه ۴.۶	قضیه ۳.۲
نتیجه ۱۹.۷	نتیجه ۵.۶	نتیجه ۴.۲
قضیه ۲۰.۷	قضیه ۳.۶	قضیه ۲.۲

همنهشتی به پیمانه یک ایده‌آل I در یک حلقه R صرفاً برحسب گروه جمعی حلقه تعریف شد: (پیمانه I) $a \equiv c$ بدین معنی است که $a - c \in I$. در نتیجه تعریف و خواص اساسی مستقیماً قابل انتقال به گروهها هستند. تنها تفاوت در این است که حلقه گروهی جمعی است در حالی که در گروهها ما معمولاً از نماد ضربی استفاده می‌کنیم. بنابراین ما باید گزاره‌های با نماد جمعی را به گزاره‌هایی معادل با نماد ضربی ترجمه کنیم[۱۸].

واژه‌نامه زیر می‌تواند برای این ترجمه مفید باشد.

نماد ضربی	نماد جمعی
ab	$a + b$
e	0
c^{-1}	$-c$
ab^{-1}	$a - b$

اگر تعریف همنهشتی برای ایده‌آلها را از نماد جمعی به نماد ضربی ترجمه کنیم، تعریف زیر را بدست می‌آوریم.

۱۸) در اینجا احتمال خلط مبحث می‌رود، زیرا حلقه‌ها دارای یک عمل ضرب نیز هستند. در انتقال نتایج همنهشتی از حلقه‌ها به گروهها، تنها ساختار جمعی حلقه را در نظر گرفته، به‌طور کامل از ساختار ضربی آنها چشم‌پوشی می‌کنیم.

تعریف. فرض کنید K زیرگروهی از گروه G باشد و $a, b \in G$. در این صورت a همنهشت با b به پیمانه K است [نوشته می‌شود $a \equiv b\ (K$ پیمانه$)$] اگر $ab^{-1} \in K$.

مثال ۳۲.۷. فرض کنید K زیرگروه $\{r_0, r_1, r_2, r_3\}$ از D_4 باشد. در این صورت جدول عمل مثال ۹.۷ نشان می‌دهد که $d^{-1} = d$ و $hod^{-1} = hod = r_1 \in K$. بنابراین $h \equiv d\ (K$ پیمانه$)$.

قضیه ۱۷.۷. فرض کنید K زیرگروهی از گروه G باشد. در این صورت رابطه همنهشتی به پیمانه K دارای خواص زیر است:

(۱) انعکاسی: برای هر $a \in G$؛ $a \equiv a\ (K$ پیمانه$)$.

(۲) متقارن: اگر $a \equiv b\ (K$ پیمانه$)$ آنگاه $b \equiv a (K$ پیمانه$)$.

(۳) متعدی: اگر $a \equiv b\ (K$ پیمانه$)$ و $b \equiv c\ (K$ پیمانه$)$، در این صورت $a \equiv c\ (K$ پیمانه$)$.

برهان. تمرین: اثبات قضیه ۲.۶ را از نماد جمعی به نماد ضربی ترجمه کنید. K و G را بجای I و R قرار دهید و از واژه‌نامه بالا استفاده کنید.

اگر K زیرگروهی از گروه G باشد و اگر $a \in G$، در این صورت **کلاس همنهشتی** a به پیمانه K عبارت از مجموعه همه عناصری از G است که همنهشت با a به پیمانه K می‌باشد یعنی، مجموعه

$$\{b \in G \mid b \equiv a\ (K \text{ پیمانه})\} = \{b \in G \mid ba^{-1} \in K\}$$
$$= \{b \in G \mid ba^{-1} = k, k \in K\}.$$

ضرب a از طرف راست نشان می‌دهد که $ba^{-1} = k$ معادل $b = ka$ است. بنابراین کلاس همنهشتی a به پیمانه K عبارت است از مجموعه

$$\{b \in G \mid b = ka, k \in K\} = \{ka \mid k \in K\}.$$

در نتیجه، کلاس همنهشتی a به پیمانه K با Ka نشان داده می‌شود. مجموعه Ka یک **هم‌مجموعه راست** K در G نامیده می‌شود. مجموعه هم‌مجموعه‌های راست K در G، یعنی همه کلاس‌های همنهشتی به پیمانه K با G/K نشان داده می‌شود. وقتی که عمل گروه G جمع است، هم مجموعه‌های راست با نماد جمعی $K + a$ نوشته می‌شوند.

اگر G یک گروه آبلی باشد (که همواره در مورد گروه جمعی یک حلقه چنین است)، در این صورت برای هر $k \in K$، $ka = ak$. در این حالت، هم مجموعه راست $Ka = \{ka \mid k \in K\}$ برابر

مجموعه $aK = \{ak \mid k \in K\}$ (که یک **هم‌مجموعه چپ** K در G نامیده می‌شود) می‌باشد[۱۹]. بدین دلیل است که هم مجموعه‌های یک ایده‌آل در یک حلقه با $a + I$ بجای $I + a$ نشان داده می‌شود و هیچ تمایزی بین چپ و راست وجود ندارد. با این حال وقتی که G یک گروه غیرآبلی است، هم مجموعه راست Ka ممکن است برابر هم مجموعه چپ aK نباشد.

مثال ۳۳.۷. فرض کنید K زیرگروه $\{r_0, v\}$ از D_4 باشد. جدول عمل مثال ۹.۷ نشان می‌دهد که هم‌مجموعه راست Kd مجموعه $\{r_0 \circ d, v \circ d\} = \{d, r_3\}$ است، امّا هم‌مجموعه چپ dK مجموعهٔ $\{d \circ r_1, d \circ v\} = \{d, r_1\}$ است. بنابراین $Kd \neq dK$.

قضیه ۱۸.۷. فرض کنید K زیرگروهی از یک گروه G باشد و $a, c \in G$. در این صورت $a \equiv c$ (پیمانه K) اگر و تنها اگر $Ka = Kc$.

برهان. با تغییرات جزیی در نمادها، اثبات اساساً همان برهان قضیه ۳.۲ یا ۴.۶ می‌باشد. تنها (پیمانه m) را با (پیمانه K) و $[a]$ را با Ka جایگزین کنید و از قضیه ۱۷.۷ بجای قضیه ۱.۲ استفاده نمائید. ■

نتیجه ۱۹.۷. فرض کنید K زیرگروهی از گروه G باشد. در این صورت هر دو هم‌مجموعه راست K یا مجزا هستند و یا برابرند.

برهان. برهان نتیجه ۴.۲ یا نتیجه ۵.۶ را با تغییرات ساده نمادها دنبال کنید. ■

تاکنون همه، به جز تنها یکی، از نتایج همنهشتی اثبات شده در فصل ۶ در مورد حلقه‌ها و ایده‌آلها را به گروهها انتقال داده‌ایم. تنها مورد باقیمانده در مورد حلقه‌ها (قضیه ۳.۶) بیان می‌کند که برای هر ایده‌آل I، اگر $a \equiv b$ $(I$ پیمانه $)$ و $c \equiv d$ $(I$ پیمانه $)$، آنگاه $a + c \equiv b + d$ $(I$ پیمانه $)$. با ترجمه این به نماد ضربی، نتیجه متناظر برای گروهها عبارت خواهد بود از: برای زیرگروه K از یک گروه G،

اگر $a \equiv b$ $(K$ پیمانه $)$ و $c \equiv d$ $(K$ پیمانه $)$، در این صورت $ac \equiv bd$ $(K$ پیمانه $)$.

---

۱۹) برای گروهها عبارت خواهد بود از: برای زیرگروه K از یک گروه G، در نماد جمعی یک هم مجموعه چپ به‌صورت $a + K$ نوشته می‌شود

اگر G یک گروه آبلی باشد در این صورت این گزارش درست است همان طور که شما به‌سادگی می‌توانید این را با ترجمه اثبات قسمت (۱) قضیه ۳.۶ از نماد جمعی به نماد ضربی نشان دهید امّا متأسفانه این گزاره برای برخی گروههای غیرآبلی ممکن است غلط باشد.

مثال ۳۴.۷. فرض کنید K زیرگروه $\{r_0, r\}$ از D_4 باشد. در این صورت (پیمانه K) $r_1 \equiv l$ زیرا $r_1 \circ l^{-1} = r_1 \circ l = r \in K$. جدول عمل مثال ۹.۷ را بکار برید تا بررسی نمائید که (پیمانه K) $r_2 \equiv h$ امّا (پیمانه K) $r_1 \circ r_2 \not\equiv t \circ h$.

این مطلب که مشابه گروهی قضیه ۳.۶ برای ایده‌آلها، در مورد زیرگروههای دلخواه برقرار نیست نباید تعجب‌آور به‌نظر برسد. از اینها گذشته، یک ایده‌آل، نوع خاصی از زیرحلقه است و حقایق همنهشتی در مورد ایده‌آلها لزوماً برای هر زیرحلقه برقرار نیست. پس آنچه که احتمالاً درست بنظر می‌رسد این است که مشابهی از قضیه ۳.۶ باید برای برخی زیرگروههای خاص یک گروه برقرار باشد.

چون مشکل انتقال قضیه ۳.۶ به گروهها، به شرط جابجایی گروه برمی‌گردد، بدیهی بنظر می‌رسد که این زیرگروههای خاص باید در نوعی شرط جابجایی صدق کنند. بحث کلاس‌های همنهشتی بالا احتمالی را پیشنهاد می‌کند که به شرح آن می‌پردازیم. کلاس همنهشتی به پیمانه K از یک عضو a در یک گروه G عبارت است از هم مجموعه راست $Ka = \{ka \mid k \in K\}$ که ممکن است مساوی هم مجموعه‌چپ $aK = \{ak \mid k \in K\}$ نباشد. البته در گروههای آبلی، این هم‌مجموعه‌ها برابرند. مثال بعدی نشان می‌دهد که این هم‌مجموعه‌ها در برخی گروههای غیرآبلی نیز ممکن است برابر باشند.

مثال ۳۵.۷. فرض کنید K زیرگروه $\{r_0, r_1, r_2, r_3\}$ از D_4 باشد. در این صورت هم مجموعه راست Kv مجموعه

$$\{r_0 \circ v, r_1 \circ v, r_2 \circ v, r_3 \circ v\} = \{v, d, h, t\}$$

و هم مجموعه چپ vK از مجموعه

$$\{v \circ r_0, v \circ r_1, v \circ r_2, v \circ r_3\} = \{v, t, h, d\}$$

است. پس $Kv = vK$. عملیات مشابه نشان می‌دهد که برای هر $a \in D_4$، $Ka = aK$. آن حقایق همنهشتی که ما می‌خواهیم برای زیرگروههای K که دارای این خاصیت هستند که برای هر $a \in G$، $aK = Ka$ ممکن است قابل اثبات باشد. شرط $Ka = aK$ بدین معنی نیست که

برای هر $k \in K$، $ka = ak$. این شرط تنها بیان می‌کند که اگر $ka \in Ka$، آنگاه ka یک عضو مجموعه aK نیز هست ـ یعنی، عضو $l \in K$ وجود دارد به قسمی که $ka = al \in aK$. برای نمونه در مثال بالا $r_1 \circ c = d = c \circ r_3$ که در آن r_1 و r_3 در زیرگروه K می‌باشد. بنابراین گرچه $Ka = aK$ نوعی شرط جابجایی است اما ضعیف‌تر از شرط جابجایی گروه است.

تعریف. زیرگروه N از یک گروه G را **نرمال**زیرگروه! نرمال گویند اگر برای هر $a \in G$، $Na = aN$.

مثال ۳۶.۷. مثال پیش از تعریف نشان می‌دهد که زیرگروه $\{r_0, r_1, r_2, r_3\}$ از D_4 نرمال است. مثال ۳۳.۷ نشان می‌دهد که $K = \{r_0, c\}$ یک زیرگروه نرمال D_4 نیست زیرا $Kd \neq dK$.

مثال ۳۷.۷. هر زیرگروه N از یک گروه آبلی G نرمال است زیرا برای همه عناصر $n \in N$ و $a \in G$، $an = na$. بنابراین به‌طور خودکار برای هر $a \in G$ داریم $Na = aN$.

مثال‌های دیگری از زیرگروههای نرمال در تمرین‌های ۹-۳ ظاهر می‌شود. زیرگروههای نرمال درست آن چیزی هستند که برای انتقال قضیه ۳.۶ به گروهها مورد نیاز می‌باشد.

قضیه ۲۰.۷. فرض کنید N که زیرگروه نرمال گروه G باشد. اگر $a \equiv b \ (N)$ و $c \equiv d \ (N)$، در این صورت $ac \equiv bd \ (N)$.

برهان. طبق تعریف همنهشتی، عناصر $m, n \in N$ وجود دارند به قسمی که $ab^{-1} = m$ و $cd^{-1} = n$. طبق نتیجه ۳.۷، $(ac)(bd)^{-1} = acd^{-1}b^{-1} = anb^{-1}$. عنصر an در هم‌مجموعه چپ aN قرار دارد. چون N نرمال است، $aN = Na$. بنابراین برای برخی $n_1 \in N$، $an = n_1 a$. در نتیجه، $(ac)(bd)^{-1} = anb^{-1} = n_1 ab^{-1} = n_1 m \in N$. پس $ac \equiv bd \ (N)$. ■

ایده‌آلها مفهوم مناسب برای انتقال حقایق مربوط به همنهشتی در $\mathbb{Z}$ به حلقه‌های دلخواه بودند. هم‌اینک دیدیم که زیرگروههای نرمال نقش مشابهی را در نظریه گروهها بازی می‌کنند. در بخش بعد خواهیم دید که همانگونه که مفهوم ایده‌آل به تعریف حلقه‌های خارج قسمتی منجر شد، مفهوم زیرگروههای نرمال نیز به تعریف گروههای خارج قسمتی منجر می‌شود. این بخش را با قضیه‌ای که

توصیف دیگری از نرمال‌بودن را ارائه می‌کند به پایان می‌رسانیم. بررسی شرط (۲) در این قضیه، اغلب ساده‌ترین راه اثبات نرمال بودن یک زیرگروه مفروض است.

قضیه ۲۱.۷. شرایط زیر در مورد یک زیرگروه N از یک گروه G معادلند:

(۱) N یک زیرگروه نرمال G است.

(۲) برای هر $a \in G$، مجموعهٔ $a^{-1}Na = \{a^{-1}na \mid n \in N\}$ یک زیرمجموعه N است.

(۳) برای هر $a \in G$، $a^{-1}Na = N$.

توجه کنید که گزاره $a^{-1}Na = N$ بدین معنی نیست که برای هر $n \in N$، $a^{-1}na = n$؛ این گزاره تنها بدین معنی است که برای برخی $n_1 \in N$، $a^{-1}na = n_1$.

برهان قضیه ۲۱.۷. (۱) $\Leftarrow$ (۲) فرض کنید $n \in N$ و $a^{-1}na \in a^{-1}Na$. باید نشان دهیم که $a^{-1}na \in N$. توجه کنید که na عضوی از هم‌مجموعه راست Na است. چون طبق (۱)، N نرمال است، $Na = aN$. از اینرو برای برخی $n_1 \in N$، $na = an_1$. بنابراین $a^{-1}na = a^{-1}an_1 = n_1 \in N$. پس $a^{-1}Na \subseteq N$.

(۲) $\Leftarrow$ (۳) اگر (۲) برای همهٔ اعضای G برقرار باشد، در این صورت برای a^{-1} بجای a نیز برقرار است، یعنی $(a^{-1})^{-1}Na^{-1} \subseteq N$. چون $a = (a^{-1})^{-1}$، می‌بینیم که برای هر $a \in G$،

$$aNa^{-1} \subseteq N, \qquad (*)$$

که در آن $aNa^{-1} = \{ana^{-1} \mid n \in N\}$. برای اثبات (۳)، فرض کنید $n \in N$، در این صورت $n = a^{-1}(ana^{-1})a$. طبق (*) برای برخی $n_2 \in N$، $ana^{-1} = n_2$. از اینرو $n = a^{-1}n_2a \in a^{-1}Na$، که ثابت می‌شود $N \subseteq a^{-1}Na$. رابطه شمول عکس طبق (۲) بدست می‌آید. بنابراین $N = a^{-1}Na$.

(۳) $\Leftarrow$ (۱) فرض کنید $n \in N$ و $na \in Na$. چون $a^{-1}na \in a^{-1}Na$، لذا برای برخی $n_3 \in N$، $a^{-1}na = n_3$. با ضرب a از طرف چپ بدست می‌آوریم $na = an_3 \in aN$. بنابراین $Na \subseteq aN$. برای اثبات رابطه شمول عکس، توجه کنید که چون (۳) برای هر عضو G برقرار است، رابطه (۳) به ازای a^{-1} بجای a نیز برقرار است:

$$aNa^{-1} = \{ana^{-1} \mid n \in N\} \quad \text{که در آن} \quad N = (a^{-1})^{-1}Na^{-1} = aNa^{-1} \qquad (**)$$

اگر $an \in aN$، در این صورت طبق (**)، $ana^{-1} \in aNa^{-1} = N$، مثلاً $ana^{-1} = n_1 \in N$. با ضرب a از طرف راست بدست می‌آید $an = n_1 a \in Na$. از اینرو $aN \subseteq Na$. لذا $Na = aN$. بنابراین N یک زیرگروه نرمال است. ■

تمرینها

۱.A. فرض کنید K زیرگروهی از گروه G باشد و $a \in G$. ثابت کنید که $Ka = K$ اگر و تنها اگر $a \in K$.

۲. (الف) فرض کنید K زیرگروهی از گروه G باشد و $a \in G$. ثابت کنید که تابع $f : K \to Ka$ تعریف شده بوسیله $f(x) = xa$ یک دوسویی است.

(ب) اگر K متناهی باشد، نتیجه بگیرید که تعداد اعضای هر دو هم‌مجموعه راست K یکسان و برابر $|K|$ است.

۳. با فهرست کردن همهٔ هم‌مجموعه‌های چپ و راست زیرگروه

$$\left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\right\}$$

از S_3 ثابت کنید که این یک زیرگروه نرمال S_3 است.

۴. ثابت کنید که $\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\}$ یک زیرگروه S_3 است امّا نرمال نیست.

۵. (الف) ثابت کنید که $G = \left\{\begin{pmatrix}a&b\\0&d\end{pmatrix} \mid a,b,d \in \mathbb{R}, ad \neq 0\right\}$ تحت عمل ضرب ماتریسها یک گروه است و این که $N = \left\{\begin{pmatrix}1&b\\0&1\end{pmatrix} \mid b \in \mathbb{R}\right\}$ یک زیرگروه G است.

(ب) قضیه ۲۱.۷ را بکار برید تا نشان دهید که N در G نرمال است.

۶. (الف) همه زیرگروههای دوری گروه چهارگانی را فهرست کنید (تمرین ۱۴ بخش ۱.۷).

(ب) نشان دهید که هر زیرگروه قسمت (الف) نرمال است.

۷. فرض کنید G و H دو گروه باشند. ثابت کنید که $G^* = \{(a,e) \mid a \in G\}$ یک زیرگروه نرمال $G \times H$ است.

۸. ثابت کنید که مرکز $Z(G)$ از گروه G یک زیرگروه نرمال است. [تمرین ۱۹ بخش ۳.۷ را ملاحظه کنید.]

۹. ثابت کنید که $\{r_0, r_1\}$ یک زیرگروه نرمال D_8 است. [راهنمایی: این تمرین می‌تواند به طور مستقیم یا با استفاده از تمرین ۸ بالا همراه با تمرین ۲۰ بخش ۳.۷ انجام شود.]

۱۰. فرض کنید N زیرگروهی از گروه G باشد. ثابت کنید N نرمال است اگر و تنها اگر برای هر خودریختی داخلی f از G، $f(N) = N$.

۱۱. یک زیرگروه N از گروه G یک زیرگروه **مشخصه** نامیده می‌شود اگر برای هر خودریختی f از G، $f(N) \subseteq N$. ثابت کنید که هر زیرگروه مشخصه نرمال است. (عکس این مطلب غلط است، امّا اثبات آن سخت‌تر است.)

۱۲. ثابت کنید که در هر گروه G، مرکز $Z(G)$ یک زیرگروه مشخصه است [تمرین ۱۹ بخش ۳.۷ را ملاحظه کنید.]

۱۳. با مثال نشان دهید که اگر M یک زیرگروه نرمال N و N یک زیرگروه نرمال یک گروه G باشد، در این صورت M لزوماً یک زیرگروه نرمال G نیست؛ به عبارت دیگر، نرمال بودن متعدی نیست. [راهنمایی: $M = \{e, r_2\}$ و $N = \{e, r_2, r_4, r_6\}$ را در D_8 در نظر بگیرید.]

۱۴.B. فرض کنید $f : G \to H$ یک همریختی گروهی باشد و فرض کنید $K = \{a \in G \mid f(a) = e_H\}$. ثابت کنید که K یک زیرگروه نرمال G است.

۱۵. اگر $f : G \to H$ یک همریختی پوشای گروهی و N یک زیرگروه نرمال G باشد، ثابت کنید که $f(N)$ یک زیرگروه نرمال H است.

۱۶. اگر K و N زیرگروههای نرمال یک گروه G باشند، ثابت کنید $K \cap N$ یک زیرگروه نرمال G است.

۱۷. اگر N و K زیرگروههایی از گروه G باشند و اگر N در G نرمال باشد، ثابت کنید که $N \cap K$ یک زیرگروه نرمال K است.

۱۸. (الف) فرض کنید N و K زیرگروههایی از گروه G باشند. اگر N در G نرمال باشد، ثابت کنید که $NK = \{nk \mid n \in N, k \in K\}$ یک زیرگروه G است. [با تمرین ۲۶ بخش ۳.۷ مقایسه کنید.]

(ب) اگر N و K دو زیرگروه نرمال G باشند، ثابت کنید که NK یک زیرگروه نرمال G است.

۱۹. اگر K و N دو زیرگروه نرمال یک گروه G باشند به قسمی که $K \cap N = \{e\}$، ثابت کنید که برای هر $n \in N$ و $k \in K$، $nk = kn$.

۲۰. فرض کنید N زیرگروهی از گروه G باشد به قسمی که دارای دقیقاً دو هم‌مجموعه راست متمایز در G باشد. ثابت کنید که N در G نرمال است. [راهنمایی: یکی از هم‌مجموعه‌ها باید $N = Ne$ باشد؛ اگر Na هم‌مجموعه دیگر باشد، در این صورت $N \cup Na = G$؛ نشان دهید که $aN \cap N$ تهی است.]

۲۱. ثابت کنید که تابع $f : \mathrm{GL}(2,\mathbb{R}) \to \mathbb{R}^*$، که توسط $f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$ تعریف می‌شود یک همریختی از گروههای ضربی است.

۲۲. ثابت کنید که $\mathrm{SL}(2,\mathbb{R})$ یک زیرگروه نرمال $\mathrm{GL}(2,\mathbb{R})$ است. [راهنمایی: $\mathrm{SL}(2,\mathbb{R})$ در تمرین ۲۱ بخش ۱.۷ تعریف شده است. تمرین‌های ۱۴ و ۲۱ بالا را بکار برید.]

۲۳. فرض کنید H یک زیرگروه از مرتبه n در گروه G باشد. اگر H تنها زیرگروه از مرتبه n باشد، ثابت کنید که H نرمال است.

۲۴. ثابت کنید که زیرگروه N از گروه G نرمال است اگر دارای این خاصیت باشد که: $a \equiv c\ (N)$ اگر و تنها اگر $aN = cN$.

۲۵. ثابت کنید که زیرگروه N از گروه G نرمال است اگر و تنها اگر دارای این خاصیت باشد که: برای هر $a, b \in G$، $ab \in N$ اگر و تنها اگر $ba \in N$.

۲۶. ثابت کنید که زیرگروه دوری $< a >$ از گروه G نرمال است اگر و تنها اگر برای هر $g \in G$، $k \in \mathbb{Z}$ وجود داشته باشد به قسمی که $ga = a^k g$.

۲۷. فرض کنید G یک گروه متناهی، N یک زیرگروه دوری نرمال در G و H زیرگروهی دلخواه از N باشد. ثابت کنید که H یک زیرگروه نرمال G است. [با تمرین ۱۳ مقایسه کنید.]

۲۸. فرض کنید A و B زیرگروههای نرمالی از یک گروه G باشند به قسمی که $A \cap B = < e >$ و $AB = G$ (تمرین ۱۸ را ملاحظه کنید). ثابت کنید که $A \times B \cong G$. [راهنمایی: تابع $f : A \times B \to G$ را به صورت $f(a,b) = ab$ تعریف کنید و تمرین ۱۹ را بکار برید.]

۲۹. فرض کنید H زیرگروهی از یک گروه G باشد و N_H نرمالساز آن باشد (تمرین ۲۹ بخش ۳.۷ را ملاحظه کنید). ثابت کنید که

(الف) H یک زیرگروه نرمال N_H است.

(ب) اگر K یک زیرگروه نرمال G باشد به قسمی که $H \subseteq K$، در این صورت $N_H \subseteq K$.

۳۰. ثابت کنید که $\mathrm{Inn}G$ یک زیرگروه نرمال $\mathrm{Aut}G$ است. [تمرین ۲۳ بخش ۴.۷ را ملاحظه کنید.]

۳۱. فرض کنید T یک مجموعه با سه یا تعداد بیشتری عضو باشد و فرض کنید $A(T)$ گروه همه جایگشتهای T باشد. اگر $a \in T$، قرار دهید $H_a = \{f \in A(T) \mid f(a) = a\}$. ثابت کنید که H_a یک زیرگروه $A(T)$ است که نرمال نیست.

۳۲. اگر N یک زیرگروه نرمال از مرتبه ۲ در یک گروه G باشد، ثابت کنید که $N \subseteq Z(G)$. [تمرین ۱۹ بخش ۳.۷ را ملاحظه کنید.]

۳۳. فرض کنید H زیرگروهی از یک گروه G باشد و فرض کنید $N = \bigcap_{a \in G} a^{-1}Ha$. ثابت کنید که N یک زیرگروه نرمال G است.

۳۴. فرض کنید G یک گروه باشد که حداقل یک زیرگروه از مرتبه n را شامل است. فرض کنید $N = \cap K$، که در آن اشتراک روی همه زیرگروههای K از مرتبهٔ n گرفته می‌شود. ثابت کنید که N یک زیرگروه نرمال G است. [راهنمایی: برای هر $a \in G$، بررسی کنید که $a^{-1}Na = \bigcap a^{-1}Ka$، که در آن اشتراک روی همه زیرگروههای K از مرتبه n گرفته می‌شود، از تمرین ۱۱ بخش ۴.۷ استفاده کنید.]

۳۵. فرض کنید G گروهی باشد که همه زیرگروههای آن نرمال باشند. اگر $a, b \in G$، ثابت کنید که عدد صحیح k وجود دارد به قسمی که $ab = ba^k$.

۳۶. اگر M یک زیرگروه مشخصه N باشد و N زیرگروه نرمالی از یک گروه G باشد، ثابت کنید که M یک زیرگروه نرمال G است. [راهنمایی: تمرین ۱۱ را ملاحظه کنید.]

۳۷. فرض کنید K زیرگروهی از گروه G باشد و $a, b \in G$. گوئیم a **همنهشت چپ** b به پیمانه K است (نوشته می‌شود $a \sim b$) اگر $ab^{-1} \in K$.

(الف) ثابت کنید اگر در قضیه ۱۷.۷ بجای $\equiv$ قرار دهید $\sim$، باز هم قضیه برقرار است.

(ب) طبق تعریف، کلاس همنهشتی چپ a مجموعه همه عناصر $b \in G$ است به قسمی که $b \sim a$. نشان دهید که این مجموعه همان هم‌مجموعه چپ aK است.

۳۸. فرض کنید K زیرگروهی از گروه G باشد و فرض کنید $\sim$ همانند آنچه در تمرین ۳۷ آمده است باشد. ثابت کنید که K نرمال است اگر و تنها اگر K در شرط، (پیمانه K) $a \equiv b$ اگر و تنها اگر $a \sim b$، صدق کند.

۶-۷ گروههای خارج قسمتی

فرض کنید N زیرگروهی نرمال از گروه G باشد. مجموعه همه هم‌مجموعه‌های راست N در G (کلاس‌های همنهشتی به پیمانه N) با G/N نشان داده می‌شود. اولین هدف ما این است که یک عمل روی هم‌مجموعه‌ها تعریف کنیم به قسمی که G/N یک گروه شود. برپایه تجربه‌ای که از $\mathbb{Z}$ و دیگر حلقه‌ها داریم روش طبیعی برای تعریف چنین عملی بدین صورت است: حاصل‌ضرب هم‌مجموعه Na (کلاس همنهشتی a) و هم‌مجموعه Nb (کلاس همنهشتی b) هم‌مجموعه Nab (کلاس همنهشتی ab) است. این تعریف، به صورت نمادی چنین نوشته می‌شود:

$$(Na)(Nb) = Nab.$$

مثل قبل، باید بررسی کنیم که این تعریف به عناصری که به‌عنوان نماینده هم‌مجموعه‌های مختلف انتخاب می‌شود بستگی ندارد و بنابراین باید قضیه زیر را ثابت کنیم.

قضیه ۲۲.۷. فرض کنید N زیرگروهی نرمال از گروه G باشد. اگر در G/N داشته باشیم $Na = Nc$ و $Nb = Nd$، در این صورت $Nab = Ncd$.

برهان. طبق قضیه ۱۸.۷، $Na = Nc$ نتیجه می‌دهد که (پیمانه N) $a \equiv c$، به‌طور مشابه $Nb = Nd$ نتیجه می‌دهد که (پیمانه N) $b \equiv d$. بنابراین طبق قضیه ۲۰.۷، (پیمانه N) $ab \equiv cd$. از اینرو طبق قضیه ۱۸.۷، $Nab = Ncd$. ■

قضیه ۲۳.۷. اگر N زیرگروهی نرمال از گروه G باشد، در این صورت تحت عمل تعریف‌شده بوسیله $(Na)(Nc) = Nac$، G/N یک گروه است. اگر G یک گروه آبلی باشد، G/N نیز چنین

است.

برهان. طبق قضیه ۲۲.۷، عمل روی G/N خوش‌تعریف است. هم‌مجموعه $N = Ne$ عضو همانی G/N است زیرا $(Na)(Ne) = Nae = Na$ و برای هر Na در G/N، $(Ne)(Na) = Nea = Na$. عضو وارون Na هم‌مجموعه Na^{-1} است زیرا داریم $(Na)(Na^{-1}) = Naa^{-1} = Ne$ و به‌طور مشابه $(Na^{-1})(Na) = Ne$. شرکت‌پذیری در G/N از شرکت‌پذیری در G نتیجه می‌شود.

$$[(Na)(Nb)](Nc) = N(ab)Nc = N(ab)c = Na(bc) = Na(Nbc)$$
$$= (Na)[(Nb)(Nc)].$$

بنابراین G/N یک گروه است. اثبات گزاره آخر به خواننده واگذار شده‌است (تمرین ۹). ■

گروه G/N **گروه خارج قسمتی** یا **گروه عامل** G توسط N نامیده می‌شود. حالت خاصی از این وضعیت وقتی اتفاق می‌افتد که I ایده‌آلی از حلقه R باشد. تحت جمع، I یک زیرگروه نرمال R است زیرا جمع در یک حلقه جابجایی است. گروه خارج قسمتی R/I همان گروه جمعی حلقه خارج قسمتی R/I است. در اینجا چند مثال ارائه می‌شود که از مباحث نظریه حلقه‌ها نتیجه نمی‌شوند.

مثال ۳۸.۷. در مثال ۳۷.۷ دیدیم که $N = \{r_0, r_1, r_2, r_3\}$ زیرگروه نرمالی از D_4 است. جدول عمل D_4 در مثال ۹.۷ نشان می‌دهد که

$$Nr_0 = \{r_0 \circ r_0, r_1 \circ r_0, r_2 \circ r_0, r_3 \circ r_0\} = \{r_0, r_1, r_2, r_3\}$$
$$Nv = \{r_0 \circ v, r_1 \circ v, r_2 \circ v, r_3 \circ v\} = \{v, d, h, t\}$$

چون هر عضو D_4 یا در Nr_0 یا Nv قرار دارد و چون هر دو هم‌مجموعه N متمایز و یا برابر Nr_0 یا Nv باشد. به عبارت دیگر، $D_4/N = \{Nr_0, Nv\}$. چون $r_0 \circ v = v = v \circ r_0$ و $v \circ v = r_0$، جدول عمل برای گروه خارج قسمت D_4/N عبارت است از

	Nr_0	Nv
Nr_0	Nr_0	Nv
Nv	Nv	Nr_0

به‌سادگی می‌توان دید که D_4/N یکریخت با گروه جمعی $\mathbb{Z}_2$ است (Nr_0 را به ۰ و Nr را به ۱ نظیر کنید؛ سپس جداول را مقایسه نمائید).

مثال ۳۹.۷. در تمرین ۹ بخش ۵.۷، دیدیم که $M = \{r_0, r_2\}$ زیرگروه نرمالی از D_4 است. با استفاده از جدول عمل D_4 می‌یابیم که D_4/M از چهار هم‌مجموعه زیرتشکیل شده است:

$$Mr_0 = \{r_0, r_2\} = Mr_2 \qquad Mr_1 = \{r_1, r_3\} = Mr_3$$
$$Mh = \{h, r\} = Mr \qquad Md = \{d, t\} = Mt.$$

با انتخاب نماینده‌ای برای هر هم‌مجموعه، عناصر D_4/M را به صورت Mr_0، Mr_1، Mh و Md فهرست می‌کنیم. وقتی حاصل‌ضرب عناصر در D_4/M را محاسبه می‌کنیم، جوابها را برحسب این چهار هم‌مجموعه بیان می‌نمائیم. برای نمونه، چون در D_4، $d \circ r_1 = r$، داریم $(Md)(Mr_1) = M(d \circ r_1) = Mr$؛ امّا $Mr = Mh$، بنابراین در جدول زیر می‌نویسیم $(Md)(Mr_1) = Mh$. محل‌های خالی را پرکنید.

	Mr_0	Mr_1	Mh	Md
Mr_0	Mr_0	Mr_1	Mh	Md
Mr_1	Mr_1	Mr_0		
Mh	Mh		Mr_0	
Md	Md	Mh		

جدول کامل‌شده نشان می‌دهد که D_4/M یک گروه آبلی است که در آن هر عضو غیرهمانی دارای مرتبهٔ ۲ است. با مقایسه جداول بررسی کنید که D_4/M یکریخت با $\mathbb{Z}_2 \times \mathbb{Z}_2$ است.

مثال ۴۰.۷. تحت جمع، گروه اعداد صحیح $\mathbb{Z}$ یک زیرگروه نرمال گروه آبلی اعداد گویای $\mathbb{Q}$ است. در نتیجه گروه خارج قسمتی $\mathbb{Q}/\mathbb{Z}$ یک گروه آبلی جمعی است (امّا یک حلقه خارج قسمتی نیست زیرا $\mathbb{Z}$ یک ایده‌آل در $\mathbb{Q}$ نیست). اگر $\mathbb{Z}+a$ و $\mathbb{Z}+c$ عناصری از $\mathbb{Q}/\mathbb{Z}$ باشند، در این صورت تعریف همنهشتی به پیمانه $\mathbb{Z}$ و قضیه ۱۸.۷ نشان می‌دهد که[۲۰]

$$\mathbb{Z}+a = \mathbb{Z}+c \quad \text{اگر و تنها اگر} \quad a-c \in \mathbb{Z}.$$

۲۰) به یاد آورید که در یک گروه جمعی هم‌مجموعه‌ها با نماد جمعی نوشته می‌شوند.

در نتیجه اگر $0 < c < a < 1$، دراین صورت $\mathbb{Z}+a$ و $\mathbb{Z}+c$ عناصر متمایزی از $\mathbb{Q}/\mathbb{Z}$ می‌باشند (زیرا $0 < a-c < 1$ و بنابراین $a-c$ نمی‌تواند یک عدد صحیح باشد). چون تعداد نامتناهی عدد گویا بین 0 و 1 وجود دارد، $\mathbb{Q}/\mathbb{Z}$ یک گروه نامتناهی است. با این حال هر عضو $\mathbb{Q}/\mathbb{Z}$ دارای مرتبه متناهی است (تمرین ۱۵).

اگر N زیرگروه نرمالی از یک گروه G باشد، در این صورت ساختار هر یک از گروههای N، G و G/N به دیگری وابسته است. اگر ما اطلاعات کافی درباره دو تا از این گروهها داشته باشیم، در این صورت همانگونه که در قضیه زیر نشان داده می‌شود می‌توانیم اطلاعات مفیدی راجع به سومی بدست آوریم.

قضیه ۲۴.۷. فرض کنید N زیرگروه نرمالی از یک گروه G باشد. در این صورت G/N آبلی است اگر و تنها اگر برای هر $a, b \in G$، $aba^{-1}b^{-1} \in N$.

برهان. G/N آبلی است اگر و تنها اگر برای هر $a, b \in G$، $Nab = NaNb = NbNa = Nba$. امّا طبق قضیه ۱۸.۷، $Nab = Nba$ اگر و تنها اگر $(ab)(ba)^{-1} \in N$؛ و طبق نتیجه ۳.۷، $(ab)(ba)^{-1} = aba^{-1}b^{-1}$. بنابراین G/N آبلی است اگر و تنها اگر برای هر $a, b \in G$، $aba^{-1}b^{-1} \in N$. ■

به یادآورید که $Z(G)$، مرکز یک گروه G، مجموعه

$$\{a \in G \mid ax = xa \text{ برای هر } x \in G\}$$

است. طبق تمرین ۸ بخش ۵.۷، $Z(G)$ یک زیرگروه نرمال G است.

قضیه ۲۵.۷. اگر G گروهی باشد به‌قسمی که گروه خارج قسمتی $G/Z(G)$ دوری باشد، در این صورت G آبلی است.

برهان بخاطر سادگی نمادها، $Z(G)$ را با C نشان دهید. چون G/C دوری است، این گروه دارای یک مولد Cd است، و هر هم‌مجموعه در G/C به صورت $(Cd)^k = Cd^k$ می‌باشد که در آن k یک عدد صحیح است، فرض کنید a و b عضوهایی از G باشند. چون $a = ea$ در هم‌مجموعه Ca قرار دارد و چون برای برخی i، $Ca = Cd^i$ لذا برای برخی $c_1 \in C$ داریم $a = c_1 d^i$. به طور مشابه، برای برخی $c_2 \in C$ و یک عدد صحیح j داریم، $b = c_2 d^j$. حال $d^i d^j = d^{i+j} = d^j d^i$

و طبق تعریف مرکز G، c_1 و c_2 با هر عضو G جابجا می‌شوند. در نتیجه،

$$ab = (c_1d^i)(c_2d^j) = c_1c_2d^id^j = c_2c_1d^jd^i = (c_2d^j)(c_1d^i) = ba.$$

بنابراین G آبلی است. ■

تمرینها

۱.A. بررسی کنید که $N = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$ زیرگروه نرمالی از S_3 است و نشان دهید که $S_3/N \cong \mathbb{Z}_2$.

۲. نشان دهید که $\mathbb{Z}_6/N \cong \mathbb{Z}_3$، جایی که N زیرگروه $\{0, 3\}$ است.

۳. نشان دهید که $\mathbb{Z}_{18}/M \cong \mathbb{Z}_6$، که در آن M زیرگروه دوری $< 6 >$ از $\mathbb{Z}_{18}$ است.

۴. فرض کنید $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ و فرض کنید N زیرگروه دوری تولیدشده توسط $(3, 2)$ باشد. نشان دهید که $G/N \cong \mathbb{Z}_4$.

۵. فرض کنید $G = \mathbb{Z}_6 \times \mathbb{Z}_2$ و فرض کنید N زیرگروه دوری $< (1, 1) >$ باشد. گروه G/N را تا حد یکریختی توصیف کنید.

۶. نشان دهید که $U_{24}/N \cong U_{16}$، که در آن N زیرگروه $\{1, 17\}$ می‌باشد.

۷. فرض کنید M و N زیرگروههای نرمالی از یک گروه G باشند به قسمی که $M \cong N$. با ارائه مثالی نشان دهید که G/M لزوماً با G/N یکریخت نیست. [راهنمایی: زیرگروههای $< (1, 0) >$ و $< (0, 2) >$ در $\mathbb{Z}_4 \times \mathbb{Z}_4$ را در نظر بگیرید.]

۸. اگر N زیرگروه نرمالی از یک گروه G باشد و اگر برای هر $x \in G$، $x^2 \in N$، ثابت کنید که هر عضو غیرهمانی گروه خارج قسمتی G/N دارای مرتبه ۲ است.

۹. اگر N زیرگروهی از یک گروه آبلی G باشد، ثابت کنید که G/N آبلی است.

۱۰. (الف) مثالی از یک گروه G با مرکز C بزنید که G/C آبلی باشد.

(ب) مثالی از یک گروه G با مرکز C بزنید که G/C آبلی نباشد.

۱۱. (الف) نشان دهید که

$$V=\left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$$

زیرگروه نرمالی از S_4 است.

(ب) جدول عمل گروه S_4/V را بنویسید.

۱۲.B. فرض کنید $\mathbb{R}^*$ گروه ضربی اعداد حقیقی غیرصفر و N زیرگروه $\{1,-1\}$ از آن باشد. ثابت کنید که $\mathbb{R}^*/N$ یکریخت با گروه ضربی اعداد حقیقی مثبت $\mathbb{R}^{**}$ است.

۱۳. گروه خارج قسمتی $\mathbb{R}^{**}/\mathbb{R}^*$ که در آن $\mathbb{R}^*$ و $\mathbb{R}^{**}$ مانند آنچه در تمرین ۱۲ آمده است باشد را توصیف کنید.

۱۴. اگر G گروهی دوری باشد، برای هر زیرگروه N از G ثابت کنید G/N دوری است.

۱۵. (الف) ثابت کنید که هر عضو $\mathbb{Q}/\mathbb{Z}$ دارای مرتبه متناهی است.

(ب) ثابت کنید که $\mathbb{Q}/\mathbb{Z}$ عناصری با هر مرتبه متناهی ممکن را شامل است.

۱۶. ثابت کنید که مجموعه عناصر با مرتبهٔ متناهی در گروه $\mathbb{R}/\mathbb{Z}$ یک زیرگروه $\mathbb{Q}/\mathbb{Z}$ است.

۱۷. فرض کنید G و H دو گروه باشند و G^* زیرمجموعه‌ای از $G\times H$ متشکل از همه عناصر (a,e)، $a\in G$ باشد.

(الف) نشان دهید G^* یکریخت با G است.

(ب) نشان دهید G^* زیرگروه نرمالی از $G\times H$ است.

(پ) نشان دهید که $(G\times H)/G^*\cong H$.

۱۸. اگر N زیرگروه نرمالی از یک گروه G باشد و اگر هر عضو از N و G/N دارای مرتبه متناهی باشند، ثابت کنید که هر عضو G دارای مرتبهٔ متناهی است.

۱۹. یک گروه H، با **مولد متناهی** نامیده می‌شود اگر زیرمجموعه متناهی S از H موجود باشد به قسمی که $H=<S>$ (قضیه ۱۲.۷ را ملاحظه کنید). اگر N زیرگروه نرمالی از یک گروه G باشد به قسمی که گروههای N و G/N با مولدمتناهی باشند، ثابت کنید که G با مولد متناهی است.

۲۰. فرض کنید G یک گروه و S مجموعه همه عناصر به صورت $aba^{-1}b^{-1}$ با $a, b \in G$ باشد. زیرگروه G' تولیدشده توسط مجموعه S (مثل آنچه در قضیه ۱۲.۷ آمده است) **زیرگروه جابجاگر** G نامیده می‌شود. ثابت کنید که:

(الف) G' در G نرمال است. [راهنمایی: برای هر $g, a, b \in G$، نشان دهید که $(g^{-1}ag)(g^{-1}bg)(g^{-1}a^{-1}g)(g^{-1}b^{-1}g) = g^{-1}(aba^{-1}b^{-1})g$ در S است.]

(ب) G/G' آبلی است.

۲۱. فرض کنید G گروه جمعی $\mathbb{R} \times \mathbb{R}$ باشد.

(الف) نشان دهید که $N = \{(x, y) \mid y = -x\}$ یک زیرگروه G است.

(ب) گروه خارج قسمت G/N را توصیف کنید.

۲۲. فرض کنید N زیرگروه نرمالی از یک گروه G و G' زیرگروه جابجاگر تعریف شده در تمرین ۲۰ باشد. اگر $N \cap G' =< e >$، ثابت کنید که:

(الف) $N \subseteq C$، که در آن C مرکز G است.

(ب) C/N مرکز G/N است.

۲۳. فرض کنید C مرکز گروه G باشد. ثابت کنید که G/C یکریخت با گروه $\mathrm{Inn}C$ متشکل از همه خودریختیهای داخلی G است (تمرین ۲۳ بخش ۴.۷ را ملاحظه کنید).

۲۴.C. فرض کنید A، B و N زیرگروههای نرمالی از یک گروه G باشند به قسمی که $N \subseteq A$ و $N \subseteq B$. اگر $G = AB$ و $A \cap B = N$، ثابت کنید که $G/N \cong A/N \times B/N$. (حالت خاص $N =< e >$، تمرین ۲۸ بخش ۵.۷ می‌باشد.)

۷-۷ همریختی‌ها و گروههای خارج قسمتی

با عنایت به تجربه‌ای که در مورد حلقه‌ها داریم، نباید عجیب بنظر برسد که رابطه نزدیکی بین زیرگروههای نرمال، گروههای خارج قسمتی و همریختی‌ها وجود داشته باشد. نخستین گام در بسط این رابطه این است که مفهوم هسته را به گروهها منتقل کنیم. به یاد آورید که هسته یک همریختی حلقه‌ای مجموعهٔ عناصری است که به عنصر صفر (عضو همانی گروه جمعی) نگاشته می‌شود. با انتقال این مفهوم

به گروههای ضربی تعریف زیر را داریم.

تعریف. فرض کنید $f : G \to H$ یک همریختی گروهی باشد. در این صورت **هستهٔ** f مجموعهٔ $\{a \in G \mid f(a) = e_H\}$ می‌باشد.

هسته یک همریختی حلقه‌ای یک ایده‌آل است. زیرگروههای نرمال مشابه گروهی ایده‌آلها هستند. در این رابطه قضیه زیر را داریم.

قضیه ۲۶.۷. فرض کنید $f : G \to H$ یک همریختی گروهی با هسته K باشد. در این صورت K یک زیرگروه نرمال G است.

برهان. اگر $c, d \in K$ در این صورت طبق تعریف هسته، $f(c) = e_H$ و $f(d) = e_H$. بنابراین $f(cd) = f(c)f(d) = e_H e_H = e_H$، لذا $cd \in K$. اگر $c \in K$، در این صورت طبق قضیه ۱۴.۷، $f(c^{-1}) = f(c)^{-1} = (e_H)^{-1} = e_H$. بنابراین $c^{-1} \in K$. از اینرو طبق قضیه ۷.۷، K یک زیرگروه G است. برای نشان دادن این که K نرمال است، باید بررسی کنیم که برای هر $a \in G$ و $c \in K$، $a^{-1}ca \in K$ (قضیه ۲۱.۷). امّا $f(a^{-1}ca) = f(a^{-1})f(c)f(a) = f(a)^{-1}e_H f(a) = f(a)^{-1}f(a) = e_H$. بنابراین $a^{-1}ca \in K$ و K نرمال است. ■

مثل آنچه در مورد حلقه‌ها دیده شد، هسته یک همریختی f میزان دوری آن را از یک به یک بودن اندازه‌گیری می‌کند.

قضیه ۲۷.۷. فرض کنید $f : G \to H$ یک همریختی گروهی با هسته K باشد. در این صورت f یک به یک است اگر و تنها اگر $K = < e_G >$.

برهان. برهان قضیه ۹.۶ را از نماد جمعی به نماد ضربی ترجمه کنید[۲۱]؛ R را با G، S را با H، 0_R را با e_G و قضیه ۱۰.۳ را با قضیه ۱۴.۷ عوض کنید. ■

قضیه ۲۶.۷ بیان می‌کند که هر هسته یک زیرگروه نرمال است. برعکس، هر زیرگروه نرمال یک هسته است:

---

۲۱) در اینجا و در ادامه این فصل، کلمهٔ "ترجمه" یعنی تغییر نماد جمعی به نماد ضربی در مورد قسمت‌هایی از برهان مطلب مشابه در نظریه حلقه‌ها که مربوط به گروه جمعی است و چشم‌پوشی از قسمت‌هایی از برهان که مربوط به ضرب حلقه‌ای می‌باشد.

قضیه ۲۸.۷. اگر N زیرگروهی نرمال از گروه G باشد، در این صورت نگاشت $\pi : G \to G/N$ تعریف شده بوسیله $\pi(a) = Na$ یک همریختی پوشا با هسته N است.

برهان. برهان قضیه ۱۰.۶ را از نماد جمعی به نماد ضربی ترجمه کنید، R را با G، S را با H، I را با N و $r + I$ را با Nr عوض کنید. ■

قضیه ۲۹.۷. **(اولین قضیه یکریختی برای گروهها)** فرض کنید $f : G \to H$ یک همریختی پوشای گروهی با هسته K باشد. در این صورت گروه خارج قسمتی G/K یکریخت با H است.

برهان. تابع $\varphi : G/K \to H$ را به صورت $\varphi(Ka) = f(a)$ تعریف کنید. برای نشان دادن این که φ یک یکریختی خوش‌تعریف است، اثبات قضیه ۱۱.۶ را از نماد جمعی به نماد ضربی ترجمه نمائید، R را با G، S را با H، $r + K$ را با Kr، $r - t$ را با rt^{-1} و 0_S را با e_H عوض کنید. ■

اولین قضیه یکریختی، شناسایی بعضی از گروههای خارج قسمتی را آسان‌تر می‌سازد.

مثال ۴۱.۷. اگر G و H دوگروه باشند، در این صورت ادعا می‌کنیم که ضرب مستقیم $G \times H$ یک زیرگروه نرمال G^* را که با G یکریخت است شامل می‌شود، و گروه خارج قسمت $(G \times H)/G^*$ یکریخت با H است. برای اثبات این موضوع فرض کنید $f : G \times H \to H$ تابعی باشد که توسط $f(a, b) = b$ تعریف شده است. بررسی کنید که f یک همریختی پوشا است (تمرین ۲). فرض کنید G^* هسته f باشد، یعنی

$$G^* = \{(a, b) \mid f(a, b) = e\} = \{(a, b) \mid b = e\} = \{(a, e) \mid a \in G\}.$$

طبق اولین قضیه یکریختی $(G \times H)/G^* \cong H$، و به سادگی می‌توان نشان داد که G یکریخت با G^* است (تمرین ۳).

مثال ۴۲.۷. گروه ضربی اعداد مختلط غیرصفر، $\mathbb{C}^*$ را در نظر بگیرید. فرض کنید N مجموعه همه اعداد مختلط با قدرمطلق ۱ باشد، یعنی $N = \{a + bi \mid a^2 + b^2 = 1\}$. ادعا می‌کنیم که N یک زیرگروه نرمال $\mathbb{C}^*$ است و این که گروه خارج قسمت $\mathbb{C}^*/N$ یکریخت با گروه ضربی اعداد حقیقی مثبت $\mathbb{R}^{**}$ است. برای اثبات این مطلب، تابع $f : \mathbb{R}^* \to \mathbb{R}^{**}$ را به صورت $f(a + bi) = a^2 + b^2$ تعریف کنید. بررسی کنید که f یک همریختی پوشا از گروههای ضربی است (تمرین ۴). چون ۱ عضو همانی $\mathbb{R}^{**}$ است، هسته f عبارت از مجموعه اعداد مختلط با

قدرمطلق ۱ است. یعنی مجموعه N. طبق قضیه ۲۹.۷، N زیرگروه نرمالی از $\mathbb{C}^*$ است و گروه خارج قسمت $\mathbb{C}^*/N$ یکریخت با $\mathbb{R}^{**}$ است.

فرض کنید N زیرگروه نرمالی از یک گروه G باشد. ساختار زیرگروههای گروه G/N چگونه است و چگونه با زیرگروههای G مرتبط می‌باشد؟ می‌توانیم با ارائه روشی برای ساختن زیرگروههای G/N، به قسمتی از این سوال پاسخ بدهیم. فرض کنید K زیرگروهی از G باشد که N را شامل است. در این صورت یقیناً N زیرگروهی از K است. چون برای هر $a \in G$، $Na = aN$، لذا به ویژه برای هر $a \in K$، $Na = aN$. بنابراین N یک زیرگروه نرمال K است، لذا طبق ۲۳.۷، K/N یک گروه است. عناصر K/N هم‌مجموعه‌های Na با $a \in K$ می‌باشد. به‌وضوح، هر هم‌مجموعه‌ای این چنین یک هم‌مجموعه در $G/N = \{Nc \mid c \in G\}$ نیز هست. بنابراین K/N یک زیرگروه G/N است. اگر گروه K که بحث خود را با آن شروع کردیم در G نرمال باشد، در این صورت قضیه زیر را داریم.

قضیه ۳۰.۷. (**سومین قضیه یکریختی برای گروهها** [۲۲]) فرض کنید K و N زیرگروههای نرمالی از یک گروه G با شرط $N \subseteq K \subseteq G$ باشند. در این صورت K/N زیرگروه نرمالی از G/N است و گروه خارج قسمت $(G/N)/(K/N)$ یکریخت با G/K است.

برهان. ایده اصلی اثبات این است که یک همریختی پوشا از G/N به G/K که هسته آن K/N باشد تعریف کنیم. در این صورت گزاره‌های ذکر شده در صورت قضیه فوراً از اولین قضیه یکریختی بدست می‌آیند. ابتدا توجه کنید که اگر در G/N، $Na = Nc$، در این صورت طبق قضیه ۱۸.۷ و تعریف همنهشتی به پیمانه N داریم $ac^{-1} \in N$. چون $N \subseteq K$، این بدین معنی است که $ac^{-1} \in K$. در نتیجه مجدداً طبق قضیه ۱۸.۷، در G/K داریم $Ka = Kc$. بنابراین نگاشت $f : G/N \to G/K$ که توسط $f(Na) = Ka$ تعریف می‌شود یک تابع خوش‌تعریف است، یعنی مستقل از انتخاب نمایندهٔ هم‌مجموعه‌ها در G/N است. به وضوح f پوشا است زیرا هر Ka در G/K تصویر Na در G/N است. تعریف عمل هم‌مجموعه‌ها نشان می‌دهد که

$$f(NaNb) = f(Nab) = Kab = KaKb = f(Na)f(Nb).$$

بنابراین f یک همریختی است. چون عضو همانی Ke، G/K است: هم‌مجموعه Na در هسته f قرار دارد اگر و تنها اگر $f(Na) = Ke$، یعنی اگر و تنها اگر

۲۲) برای دومین قضیه یکریختی، تمرین ۲۴ را ملاحظه کنید.

$Ka = Ke$. امّا طبق قضیهٔ ۱۸.۷، $Ka = Ke$ اگر و تنها اگر $a \in K$. بنابراین هسته f متشکل از همه هم‌مجموعه‌های Na با شرط $a \in K$ است؛ به عبارت دیگر، K/N هسته f است. بنابراین K/N یک زیرگروه نرمال G/N است (قضیه ۲۶.۷) و طبق اولین قضیه یکریختی،

$$(G/N)/(K/N) = (G/N)/\text{kernel} f \cong G/K. \quad \blacksquare$$

اینک اطلاع کاملی در مورد آن زیرگروههایی از G/N که از زیرگروههای G بدست می‌آیند داریم. آیا اینها همه زیرگروههای G/N هستند؟ قضیهٔ بعدی آنچه را انجام داده‌ایم به اختصار بیان می‌کند و به این سوال پاسخ مثبت می‌دهد.

قضیه ۳۱.۷. فرض کنید N زیرگروه نرمالی از گروه G باشد. فرض کنید K زیرگروهی دلخواه از G باشد که N را شامل است. دراین صورت

(۱) K/N یک زیرگروه G/N است.

(۲) K/N نرمال در G/N است اگر و تنها اگر K در G نرمال باشد.

(۳) اگر T زیرگروهی دلخواه از G/N باشد، در این صورت زیرگروه H از G وجود دارد به قسمی که $N \subseteq H$ و $T = H/N$.

برهان. قضیه ۳۰.۷ و بند قبل از آن، گزاره (۱) و نیمی از گزاره (۲) را اثبات می‌کند. استلزام دیگر (۲) در تمرین ۱۳ آمده است.

(۳) فرض کنید $H = \{a \in G \mid Na \in T\}$. اگر $a, b \in H$، در این صورت $Na \in T$ و $Nb \in T$. چون T یک زیرگروه است، $Nab = NaNb \in T$. بنابراین $ab \in H$ و H بسته است. اگر $a \in H$، در این صورت $Na \in T$. چون T یک زیرگروه است، $Na^{-1} = (Na)^{-1}$ نیز در T قرار دارد. بنابراین $a^{-1} \in H$ و طبق قضیه ۷.۷، H یک زیرگروه است. توجه کنید که اگر $a \in N$ در این صورت طبق قضیه ۱۸.۷، $Na = Ne$ زیرا $a \equiv e$ (پیمانه N). بنابراین $Na = Ne \in T$، لذا $a \in H$. پس $N \subseteq H$. طبق تعریف H، گروه خارج قسمت H/N متشکل از همه هم‌مجموعه‌های Na با $a \in H$ است، یعنی مجموعه همه Naهای در T. بنابراین $H/N = T$. $\blacksquare$

تمرینها

۱.A. بررسی کنید که هر یک از نگاشت‌های زیر یک همریختی گروهی است و هسته آن را بیابید:

(الف) $f : \mathbb{Z}_{۱۲} \to \mathbb{Z}_{۱۲}$ که در آن $f(x) = ۳x$.

(ب) $f : \mathbb{Z} \to \mathbb{Z}_۲ \times \mathbb{Z}_۴$ که در آن $f(k) = ([k]_۲, [k]_۴)$ و $[k]_n$ کلاس همنهشتی k در $\mathbb{Z}_n$ را نشان می‌دهد.

(پ) $f : \mathbb{Z}_۸ \to \mathbb{Z}_۲$ که در آن $f([k]_۸) = [k]_۲$.

(ت) $\varphi : S_n \to S_{n+۱}$ که در آن برای هر $f \in S_n$، $\varphi(f) \in S_{n+۱}$ توسط

$$\varphi(f)(k) = \begin{cases} f(k) & \text{اگر } ۱ \le k \le n \\ n+۱ & \text{اگر } k = n+۱ \end{cases}$$

تعریف شده است.

(ث) $h : \mathbb{Z}_{۱۸} \to \mathbb{Z}_۳$ که در آن $h([x]_{۱۸}) = [۲x]_۳$.

۲. فرض کنید G و H دو گروه باشند و $f : G \times H \to H$ توسط $f(a, b) = b$ تعریف شده باشد. نشان دهید که f یک همریختی پوشا است.

۳. فرض کنید G و H گروه باشند و فرض کنید $G^* = \{(a, e_H) \mid a \in G\}$ و $H^* = \{(e_G, b) \mid b \in H\}$.

(الف) نشان دهید که G^* و H^* زیرگروههای نرمال $G \times H$ هستند.

(ب) نشان دهید که $G \cong G^*$ و $H \cong H^*$.

(پ) نشان دهید که $(G \times H)/G^* \cong H$ و $(G \times H)/H^* \cong G$.

۴. ثابت کنید که تابع $f : \mathbb{C}^* \to \mathbb{R}^{**}$ تعریف شده بوسیله $f(a + bi) = a^۲ + b^۲$ یک همریختی پوشای گروهی است.

۵. (الف) همه تصاویر همریختی (تا حد یکریختی) $\mathbb{Z}_{۱۲}$ را فهرست کنید. [راهنمایی: تمرین ۳۳ بخش ۳.۷ را ملاحظه کنید.]

(ب) همین کار را برای $\mathbb{Z}_{۲۰}$ انجام دهید.

۶. (الف) همه زیرگروههای $\mathbb{Z}_{۱۲}/H$، که در آن $H = \{۰, ۶\}$، را فهرست کنید.

(ب) همه زیرگروههای $\mathbb{Z}_{۲۰}/K$ که در آن $K = \{۰, ۴, ۸, ۱۲, ۱۶\}$ را فهرست کنید.

۷. یک گروه G **ساده** نامیده می‌شود اگر G دارای هیچ زیرگروه نرمالی بجز خودش و $< e >$ نباشد. فرض کنید $f : G \to H$ یک همریختی پوشای گروهی و G ساده باشد. ثابت کنید که یا f یک یکریختی است یا $H = < e >$.

۸. اگر $k \mid n$ و $f : U_n \to U_k$ توسط $f([x]_n) = [x]_k$ تعریف شده باشد، نشان دهید که f یک همریختی است و هسته آن را بیابید (نمادها مثل تمرین ۱ می‌باشد).

۹. فرض کنید $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ تابعی باشد که توسط $\varphi(f(x)) = f(۳)$ تعریف شده‌است. نشان دهید که φ یک همریختی از گروههای جمعی است و هسته آن را بیابید.

۱۰. فرض کنید G یک گروه آبلی باشد.

(الف) نشان دهید که $K = \{a \in G \mid\mid |a| \leq ۲\}$ یک زیرگروه G است.

(ب) نشان دهید که $H = \{x^۲ \mid x \in G\}$ یک زیرگروه G است.

(پ) ثابت کنید که $G/K \cong H$. [راهنمایی: یک همریختی پوشا از G به H با هسته K تعریف کنید.]

۱۱. اولین قضیه یکریختی را بکار برید تا ثابت کنید که $\mathbb{R}^*/ < ۱, -۱ > \cong \mathbb{R}^{**}$.

۱۲. فرض کنید G و H گروههای ارائه شده در تمرین‌های ۳۱ و ۳۲ بخش ۱.۷ باشد. اولین قضیه یکریختی را بکار برید تا نشان دهید که H در G نرمال است و این که G/H یکریخت با گروه ضربی اعداد حقیقی غیرصفر $\mathbb{R}^*$ می‌باشد. [راهنمایی: تابع $f : G \to \mathbb{R}^*$ تعریف شده بوسیله $f(T_{a,b}) = a$ را در نظر بگیرید.]

۱۳. فرض کنید N زیرگروه نرمالی از یک گروه G و K هر زیرگروهی از G باشد که N را شامل است. در این صورت طبق قسمت (۱) قضیه ۳۱.۷، K/N یک زیرگروه G/N است. اگر K/N نرمال در G/N باشد، ثابت کنید که K نرمال در G است.

۱۴. فرض کنید M زیرگروه نرمالی از یک گروه G و N زیرگروه نرمالی از یک گروه H باشد. اولین قضیه یکریختی را بکار برید تا ثابت کنید که $M \times N$ زیرگروه نرمالی از $G \times H$ است و این که $(G \times H)/(M \times N) \cong G/M \times H/N$.

۱۵. ثابت کنید که $\mathrm{SL}(۲,\mathbb{R})$ زیرگروه نرمالی از $\mathrm{GL}(۲,\mathbb{R})$ است و این که $\mathrm{GL}(۲,\mathbb{R})/\mathrm{SL}(۲,\mathbb{R})$ یکریخت با گروه ضربی اعداد حقیقی غیرصفر $\mathbb{R}^*$ است. [راهنمایی: تمرین ۲۱ بخش ۵.۷.]

۱۶. فرض کنید R یک حلقه باشد و $r \in R$. فرض کنید $f : R \to R$ تابعی باشد که توسط $f(x) = rx$ تعریف شده است.

(الف) نشان دهید که f یک همریختی از گروههای جمعی است.

(ب) با مثال نشان دهید که f لزوماً یک همریختی حلقه‌ای نیست.

(پ) اعمال چه شرایطی روی R و یا r تضمین می‌کند که f یک همریختی حلقه‌ای باشد؟

۱۷. (این تمرینی است برای کسانی که ضرب ماتریس‌های ۳ × ۳ را می‌دانند.) فرض کنید G مجموعه ماتریس‌های به صورت

$$\begin{pmatrix} ۱ & a & b \\ ۰ & ۱ & c \\ ۰ & ۰ & ۱ \end{pmatrix}$$

باشد که در آن $a, b, c \in \mathbb{Q}$.

(الف) نشان دهید که تحت ضرب ماتریسی، G یک گروه است.

(ب) مرکز C از G را بیابید و نشان دهید که C یکریخت با گروه جمعی $\mathbb{Q}$ است.

(پ) نشان دهید که G/C یکریخت با گروه جمعی $\mathbb{Q} \times \mathbb{Q}$ است.

۱۸. فرض کنید $f : G \to H$ یک همریختی پوشای گروهی با هسته K باشد و فرض کنید M یک زیرگروه H باشد.

(الف) ثابت کنید زیرگروه N از G وجود دارد به قسمی که $K \subseteq N \subseteq G$ و $N/K \cong M$.

(ب) اگر M در H نرمال باشد، ثابت کنید که N در G نرمال است و $G/N \cong H/M$.

۱۹. فرض کنید $f : G \to H$ یک همریختی پوشای گروهی با هسته K باشد. ثابت کنید که یک دوسویی بین مجموعه همه زیرگروههای H و مجموعه زیرگروههایی از G که K را شامل هستند وجود دارد.

۲۰. فرض کنید N زیرگروه نرمالی از یک گروه G باشد و فرض کنید $f : G \to H$ یک همریختی گروهی باشد به قسمی که تحدید f به N یک یکریختی $N \cong H$ باشد. ثابت کنید که $G \cong N \times K$ که در آن K هسته f است. [راهنمایی: تمرین ۲۸ بخش ۵.۷.]

۲۱. یک گروه G **فراآبلی** نامیده می‌شود اگر دارای یک زیرگروه آبلی N باشد که در G نرمال بوده و G/N آبلی باشد.

(الف) نشان دهید که S_3 فراآبلی است.

(ب) ثابت کنید که هر تصویر همریختی یک گروه فراآبلی، فراآبلی است.

(پ) ثابت کنید که هر زیرگروه یک گروه فراآبلی،فراآبلی است.

۲۲. فرض کنید N زیرگروه نرمالی از یک گروه G باشد. ثابت کنید G/N ساده است اگر و تنها اگر هیچ زیرگروه نرمال H موجود نباشد به قسمی که $N \subsetneqq H \subsetneqq G$. [راهنمایی: تمرین‌های ۷ و ۱۳.]

۲۳. گروه جمعی $\mathbb{Z}[x]$، اعداد صحیح $\mathbb{Z}$ (مجموعه چندجمله‌ایهای ثابت) را به عنوان یک زیرگروه نرمال شامل است. نشان دهید که $\mathbb{Z}[x]/\mathbb{Z}$ یکریخت با $\mathbb{Z}[x]$ است. این مثال نشان می‌دهد که $G \cong G/N$ لزوماً نتیجه نمی‌دهد $N =< e >$. [راهنمایی، نگاشت $T : \mathbb{Z}[x] \to \mathbb{Z}[x]/\mathbb{Z}$ که توسط $T(f(x)) = \mathbb{Z} + xf(x)$ تعریف می‌شود را در نظر بگیرید.]

۲۴.C. **(دومین قضیه یکریختی برای گروهها)** فرض کنید K و N زیرگروههایی از یک گروه G باشند و N در G نرمال باشد. در این صورت طبق تمرین ۱۸ بخش ۵.۷، $NK = \{nk \mid n \in N, k \in K\}$ یک زیرگروه G است که تواماً K و N را شامل است.

(الف) ثابت کنید که N یک زیرگروه نرمال NK است.

(ب) ثابت کنید که تابع $f : K \to NK/N$ که توسط $f(k) = Nk$ تعریف می‌شود یک همریختی پوشا با هسته $K \cap N$ است.

(پ) نتیجه بگیرید که $K/(N \cap K) \cong NK/N$.

۲۵. قضیه کیلی ۱۵.۷، یک گروه G را به عنوان زیرگروهی از گروه جایگشتهای $A(G)$ نمایش می‌دهد. روش کارآمدتری برای نمایش G به عنوان یک گروه جایگشتی، از تعمیم قضیه کیلی

که در اینجا به آن می‌پردازیم حاصل می‌شود. فرض کنید K یک زیرگروه G و T مجموعه همه هم‌مجموعه‌های راست متمایز K باشد.

(الف) اگر $a \in G$، نشان دهید که نگاشت $f_a : T \to T$ که توسط $f_a(Kb) = Kba$ تعریف می‌شود یک جایگشت از مجموعه T است.

(ب) ثابت کنید که تابع $\varphi : G \to A(T)$ که توسط $\varphi(a) = f_{a^{-1}}$ تعریف می‌شود یک همریختی گروهی است که هسته آن در K قرار دارد.

(پ) اگر K در G نرمال باشد، ثابت کنید که $K = \text{kernel } \varphi$.

(ت) قضیه کیلی را با بکار بردن قسمتهای (ب) و (پ) با $K = < e >$ ثابت کنید.

۸-۷ ساختار گروههای متناهی

تا اینجا، توسعه گروهها به موازات توسعه اعداد صحیح، چندجمله‌ایها و حلقه‌ها پیش رفته است. اکنون ما این مسیر موازی را رها کرده و نظریه گروههای متناهی که هیچ مشابهی در کار قبلی ما نداشت را در نظر می‌گیریم.

یک هدف عمده در نظریه گروهها، رده‌بندی گروههای متناهی تا حد یکریختی است. یعنی مایلیم فهرستی از گروهها بدست آوریم به قسمی که هر گروه متناهی یکریخت با دقیقاً یکی از گروههای این فهرست باشد. این مسئله‌ای فوق‌العاده مشکل است، با این حال در این راستا تعدادی از نتایج جزیی قبلاً بدست آمده‌اند، برای مثال، قضیه ۱۳.۷، رده‌بندی همه گروههای دوری را بدست می‌دهد. (هر گروه دوری متناهی یکریخت با دقیقاً یک گروه از فهرست: $\mathbb{Z}_1$، $\mathbb{Z}_2$، $\mathbb{Z}_3$، $\mathbb{Z}_4$، ... می‌باشد). در این بخش آن حقایق اساسی را که بیشتر قضایای رده‌بندی به آنها بستگی دارد فراهم کرده، به طور کامل گروههای با مرتبه اول و گروههای با مرتبه کمتر از ۸ را رده‌بندی می‌کنیم.

مرتبه یک گروه متناهی یک عدد صحیح مثبت است. موضوع زیربنایی این بخش رابطه بین خواص حسابی این عدد صحیح و ساختار گروه است. به منظور بسط این رابطه، نیاز به مرور برخی حقایق اساسی درباره هم‌مجموعه‌ها داریم.

قضیه ۳۲.۷. فرض کنید H زیرگروهی از یک گروه G باشد. در این صورت

(۱) G برابر اجتماع هم‌مجموعه‌های راست H است: $G = \bigcup_{a \in G} Ha$.

(۲) هر دو هم‌مجموعه راست H یا برابرند یا مجزا: $Ha = Hb$ یا $Ha \cap Hb = \varnothing$.

(۳) برای هر $a \in G$، یک دوسویی $f : H \to Ha$ وجود دارد. در نتیجه، اگر H متناهی باشد، هر دو هم‌مجموعه راست H دارای تعداد یکسانی عضو هستند.

برهان. (۱) چون هر هم‌مجموعه از عناصر G تشکیل شده است، داریم $\bigcup_{a\in G} Ha \subseteq G$. اگر $b \in G$، در این صورت $b = eb \in Hb \subseteq \bigcup_{a\in G} Ha$، لذا $G \subseteq \bigcup_{a\in G} Ha$. بنابراین $G = \bigcup_{a\in G} Ha$.

(۲) نتیجه ۱۹.۷ را ملاحظه کنید.

(۳) تابع $f : H \to Ha$ را با $f(x) = xa$ تعریف کنید. در این صورت طبق تعریف Ha، f پوشا است. اگر $f(x) = f(y)$ در این صورت $xa = ya$، لذا طبق قضیه ۲.۷، $x = y$. پس f یک به یک است و بنابراین یک دوسویی است. در نتیجه اگر H متناهی باشد، تعداد عناصر هر هم‌مجموعه Ha برابر با تعداد عناصر H، یعنی $|H|$ می‌باشد. ■

اگر H زیرگروهی از یک گروه G باشد، در این صورت تعداد هم‌مجموعه‌های راست متمایز H در G، **شاخص** H در G نامیده شده و با $[G : H]$ نشان داده می‌شود. اگر G یک گروه متناهی باشد، در این صورت فقط تعداد متناهی هم‌مجموعه راست متمایز H می‌تواند وجود داشته باشد؛ بنابراین شاخص $[G : H]$ متناهی است. اگر G یک گروه نامتناهی باشد، در این صورت شاخص ممکن است متناهی یا نامتناهی باشد.

مثال ۴۳.۷. $\mathbb{Z}$ یک زیرگروه از گروه جمعی $\mathbb{Q}$ است و همانگونه که در مثال ۴۱.۷ دیدیم تعداد نامتناهی هم‌مجموعه متمایز از $\mathbb{Z}$ در $\mathbb{Q}$ وجود دارد. بنابراین شاخص $[\mathbb{Q} : \mathbb{Z}]$ نامتناهی است.

مثال ۴۴.۷. فرض کنید H زیرگروه دوری $< ۳ >$ از گروه جمعی $\mathbb{Z}$ باشد. در این صورت H متشکل از همه مضارب ۳ است و هم‌مجموعه‌های H همان کلاس‌های همنهشتی به پیمانه ۳ هستند؛ برای مثال $H + ۲ = \{h + ۲ \mid h \in H\} = \{۳z + ۲ \mid z \in \mathbb{Z}\} = [۲]$. چون دقیقاً سه کلاس همنهشتی متمایز به پیمانه ۳ وجود دارد (هم‌مجموعه‌های H)، داریم $[\mathbb{Z} : H] = ۳$.

مثال ۴۵.۷. فرض کنید M زیرگروه $\{r_۰, r_۲\}$ از $D_۴$ باشد. در مثال ۴۰.۷ دیدیم که M دارای

چهارهم‌مجموعه متمایز زیر است،

$$Mr_0 = \{r_0, r_2\}, \quad Mr_1 = \{r_1, r_3\}, \quad Mh = \{h, v\}, \quad Md = \{d, t\}.$$

بنابراین $[D_4, M] = 4$. به‌علاوه $|D_4| = 2 \times 4 = |M|\,[D_4 : M]$. این مصداقی از قضیه زیر است.

قضیه ۳۳.۷. (قضیه لاگرانژ)[۲۳] اگر H زیرگروهی از یک گروه متناهی G باشد، در این صورت مرتبه H مرتبه G را می‌شمارد؛ در حقیقت $|G| = |H|\,[G : H]$.

برهان. برای راحتی کار مناسب است نمادگذاری را که به دنبال می‌آید بپذیریم: اگر A یک مجموعه متناهی باشد، در این صورت $|A|$ تعداد عناصر A را نشان می‌دهد. مشاهده کنید که اگر A و B مجموعه‌های متناهی مجزا باشند، آنگاه $|A \cup B| = |A| + |B|$. حال فرض کنید که $[G : H] = n$ و n هم‌مجموعه متمایز H در G را با Hc_1، Hc_2، ...، Hc_n نشان دهید. در این صورت طبق قضیه ۳۲.۷، $G = Hc_1 \cup Hc_2 \cup \cdots \cup Hc_n$. چون همه این هم‌مجموعه‌ها متمایزند، طبق قضیه ۳۲.۷ دوبدو مجزا هستند. در نتیجه $|G| = |Hc_1| + |Hc_2| + \cdots + |Hc_n|$. اما طبق قضیه ۳۲.۷، برای هر c_i، $|Hc_i| = |H|$. بنابراین

$$|G| = \underbrace{|H| + |H| + \cdots + |H|}_{n \text{ جمعوند}} = |H|\,n = |H|\,[G : H].$$

به این ترتیب برهان کامل می‌شود. ■ قضیه لاگرانژ نشان می‌دهد که مرتبه‌های ممکن برای زیرگروههای یک گروه مفروض محدود است. برای نمونه، یک زیرگروه از یک گروه با مرتبه ۱۲ باید یکی از مرتبه‌های ۱، ۲، ۳، ۴، ۶ یا ۱۲ (تنها شمارنده‌های ۱۲) را داشته باشد. با این حال دقت کنید که اینها تنها مرتبه زیرگروههای ممکن هستند، قضیه لاگرانژ بیان نمی‌کند که به ازای هر شمارنده k از $|G|$، G باید دارای زیرگروهی از مرتبه k باشد. در واقع مثالی از یک گروه از مرتبه ۱۲ را خواهیم دید که دارای هیچ زیرگروهی از مرتبه ۶ نیست (تمرین ۲۸ بخش ۹.۷). قضیه لاگرانژ همچنین محدودیت‌هایی را روی مرتبه‌های ممکن عناصر یک گروه اعمال می‌کند.

نتیجه ۳۴.۷. فرض کنید G یک گروه متناهی باشد.

۲۳) Lagrange's Theorem

(۱) اگر $a \in G$ در این صورت مرتبه a مرتبه G را می‌شمارد.

(۲) اگر $|G| = k$، در این صورت برای هر $a \in G$، $a^k = e$.

(۳) اگر N یک زیرگروه نرمال G باشد، آنگاه $|G/N| = |G| / |N|$.

برهان. (۱) اگر a دارای مرتبه n باشد، در این صورت طبق قضیه ۱۰.۷، زیرگروه دوری $< a >$ از G دارای مرتبه n است. در نتیجه طبق قضیه لاگرانژ، n مرتبه G را می‌شمارد.

(۲) اگر $a \in G$ دارای مرتبه n باشد، در این صورت به موجب (۱)، $n \mid k$، مثلاً $k = nt$. بنابراین $a^k = a^{nt} = (a^n)^t = e^t = e$.

(۳) $|G/N|$ تعداد هم‌مجموعه‌های راست متمایز N در G است، یعنی $|G/N| = [G : N]$. طبق قضیه لاگرانژ، $|G/N| = [G : N] = |G| / |N|$ و بنابراین $|G/N| = |G| / |N|$. ■

قضیه لاگرانژ و نتیجه آن ابزار اصلی برای تعیین ساختار انواع گروههای متناهی هستند. رده‌بندی را از گروههایی که دارای مرتبهٔ اول هستند شروع می‌کنیم.

قضیه ۳۵.۷. فرض کنید p یک عدد صحیح اول باشد. هر گروه از مرتبه p دوری و یکریخت با $\mathbb{Z}_p$ است.

برهان. اگر G یک گروه از مرتبه p و a هر عضو غیرهمانی G باشد، در این صورت زیرگروه دوری $< a >$ یک گروه با مرتبه بزرگتر از ۱ است. چون مرتبه گروه $< a >$ باید p را بشمارد و چون p اول است، $< a >$ باید گروهی از مرتبه p باشد. بنابراین $< a >$ همه G است، و G یک گروه دوری از مرتبه p است. پس طبق قضیه ۱۳.۷، $G \cong \mathbb{Z}_p$. ■

حال به رده‌بندی گروههای با مرتبه کوچک می‌پردازیم. طبق قضیه ۳۵.۷، یک گروه از مرتبه ۲، ۳، ۵ یا ۷ دوری است. دو قضیه بعدی به رده‌بندی گروههای از مرتبه ۴ و ۶ می‌پردازد[۲۴]. در اثبات‌های این دو قضیه به اندازه کافی محاسبات مورد نیاز گنجانده شده‌است تا چگونگی روند استدلال نشان داده شود، امّا در عین حال بهتر است قلم و کاغذ را برداشته و محاسبات انجام نشده را کامل کنید.

---

۲۴) قضایای ۳۶.۷ و ۳۷.۷ و نتایج ۳۹.۷ و ۴۰.۷ حالات خاص نتایجی هستند که در فصل ۱۰ اثبات خواهد شد. اگر قصد خواندن فصل ۱۰ را دارید، در صورت تمایل می‌توانید از مطالعه اثباتهای مقدماتی ارائه شده در اینجا صرف‌نظر کنید.

قضیه ۳۶.۷. هر گروه از مرتبه ۴ یکریخت با $\mathbb{Z}_4$ یا $\mathbb{Z}_2 \times \mathbb{Z}_2$ است.

برهان. فرض کنید G گروهی از مرتبه ۴ باشد. حال G یا عضوی از مرتبه ۴ را شامل است و یا نیست. اگر چنین عضوی را شامل باشد در این صورت طبق قضیه ۱۰.۷، زیرگروه دوری تولیدشده بوسیله این عنصر دارای مرتبه ۴ است و بنابراین باید همه G باشد. بنابراین G یک گروه دوری از مرتبه ۴ است و طبق قضیه ۱۳.۷، $G \cong \mathbb{Z}_4$. حال فرض کنید که G عضوی از مرتبه ۴ را شامل نباشد. فرض کنید e، a، b، c اعضای متمایز G باشند که در آن e عضو همانی G است. چون طبق نتیجه ۳۴.۷، مرتبهٔ هر عضو G باید ۴ را بشمارد و چون e تنها عضو از مرتبه ۱ است، لذا هر یک از a، b و c باید دارای مرتبهٔ ۲ باشد. بنابراین جدول عمل G باید به صورت زیر باشد:

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

به منظور پرکردن مکان‌های خالی، ابتدا حاصل‌ضرب ab را در نظر می‌گیریم. اگر $ab = e$، در این صورت $ab = aa$ و بنابراین طبق قانون حذف، $a = b$. این یک تناقض است و لذا $ab \neq e$. اگر $ab = a$ در این صورت $ab = ae$ و طبق قانون حذف $b = e$ که مجدداً یک تناقض است. به‌طور مشابه $ab = b$، تناقض $a = e$ را نتیجه می‌دهد. بنابراین تنها احتمال این است که $ab = c$. استدلال‌هایی مشابه نشان می‌دهد که تنها جدول عمل ممکن برای G عبارت است از

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	b
c	c	b	a	e

فرض کنید $f : G \to \mathbb{Z}_2 \times \mathbb{Z}_2$ توسط $f(e) = (0,0)$، $f(a) = (1,0)$، $f(b) = (0,1)$ و $f(c) = (1,1)$ تعریف شده باشد. با مقایسه جداول اعمال نشان دهید که دوگروه یکریختند. ■

قضیه ۳۷.۷. هر گروه غیرآبلی G از مرتبه ۶ یکریخت با S_3 است.

برهان. گروه G نمی‌تواند عنصری از مرتبه ۶ را شامل باشد زیرا در این صورت G باید دوری و در نتیجه آبلی باشد. طبق نتیجه ۳۴.۷ هر عنصر غیرهمانی G دارای مرتبهٔ ۲ یا ۳ است، امّا همه عناصر غیرهمانی G نمی‌توانند دارای مرتبه ۲ باشند زیرا در این صورت طبق تمرین ۲۱ بخش ۲.۷، G آبلی است. بنابراین G باید یک عنصر a از مرتبه ۳ را شامل باشد. فرض کنید N زیرگروه دوری $\{e, a, a^2\} = < a >$ و b هر عنصری از G باشد که در N نیست. هم‌مجموعه‌های $Ne = \{e, a, a^2\}$ و $Nb = \{b, ab, a^2b\}$ برابر نیستند زیرا $b \notin N = Ne$ و بنابراین باید مجزا باشند (قضیه ۳۲.۷). پس G از شش عنصر e، a، a^2، b، ab و a^2b تشکیل شده‌است.

حال نشان می‌دهیم که تنها یک جدول عمل ممکن برای G وجود دارد. چه احتمالاتی برای b^2 وجود دارد؟ ادعا می‌کنیم که b^2 نمی‌تواند هیچ کدام از a، a^2، b، ab و یا a^2b باشد. برای نمونه، اگر $b^2 = a$، در این صورت $b^4 = a^2$. امّا b یا دارای مرتبه ۲ است (که در این حالت $a^2 = b^4 = b^2b^2 = ee = e$، که یک تناقض است) یا b دارای مرتبه ۳ است (که در این حالت $a^2 = b^4 = b^3b = eb = b$، که یک تناقض دیگر است زیرا $b \notin N$). استدلال‌های مشابهی نشان می‌دهد که تنها احتمال این است که $b^2 = e$. سپس به سادگی می‌توان دید که ba نمی‌تواند هیچ کدام از b، e، a یا a^2 باشد (برای نمونه، $ba = a$ نتیجه می‌دهد $b = e$). هم‌چنین تساوی $ba = ab$ ممکن نیست زیرا در این صورت G آبلی خواهد بود (چرا؟). بنابراین باید داشته باشیم $ba = a^2b$. اینک با بکار بردن حقایق:

$$b^2 = e \quad \text{و} \quad ba = a^2b$$

می‌توانیم هر حاصل‌ضرب را در G محاسبه کنیم. برای مثال

$$ba^2 = (ba)a = a^2(ba) = a^2a^2b = a^4b = ab.$$

بررسی کنید که جدول عمل G باید به صورت زیر باشد:

	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

با مقایسه جداول نشان دهید که G تحت تناظر زیر با S_3 یکریخت است:

$$\begin{array}{cccccc} e & a & a^2 & b & ab & a^2b \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} & \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} & \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} & \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} & \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} & \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \end{array}$$

■

دو اثبات قبلی روشی از توصیف یا تعریف گروهها برحسب **مولدها و روابط** آنها را نشان می‌دهد. برای مثال S_3 گروه منحصر به فرد G با مولدهای a و b است که در روابط زیر صدق می‌کند،

$$a^3 = e \qquad b^2 = e \qquad ba = a^2b.$$

به‌طور مشابه $\mathbb{Z}_2 \times \mathbb{Z}_2$ گروه منحصربه‌فرد G با مولدهای a و b است که در روابط زیر صدق می‌کند:

$$a^2 = e \qquad b^2 = e \qquad ba = ab.$$

توجه کنید که لزومی به ذکر عنصر c که در اثبات قضیه ۳۶.۷ ظاهر شد نمی‌باشد، زیرا $c = ab$.

همانگونه که در بالا ذکر شد، عکس قضیه لاگرانژ ممکن است غلط باشد: این حقیقت که k مرتبه گروه G را می‌شمارد تضمین کننده این نیست که G دارای زیرگروهی از مرتبه k است. در عین حال کلید اثبات قضیه ۳۷.۷ دقیقاً این حقیقت بود که: ۳ مرتبه G را می‌شمارد و این که G دارای عنصری از مرتبه ۳ و لذا شامل زیرگروهی از مرتبه ۳ بود. این موضوع پیشنهاد می‌کند که عکس قضیه لاگرانژ ممکن است برای شمارنده‌های اول درست باشد.

قضیه ۳۸.۷. (قضیه کُشی برای گروههای آبلی) اگر G یک گروه آبلی متناهی و p یک عدد اول باشد که مرتبه G را بشمارد، در این صورت G شامل عنصری از مرتبه p است.

این قضیه در واقع برای همه گروههای متناهی درست است (نتیجه ۱۴.۱۰ را ملاحظه کنید).

برهان قضیه ۳۸.۷. برهان با استفاده از اصل استقراء کامل[۲۵]، با استقراء روی مرتبه G انجام می‌شود. برای انجام این کار، ابتدا باید نشان دهیم که قضیه وقتی که $|G| = 2$ درست است. در این حالت اگر p مرتبه G را بشمارد، در این صورت $p = 2$. طبق قسمت (۱) نتیجه ۳۴.۷، عنصر غیرهمانی G باید دارای مرتبه ۲ باشد و بنابراین قضیه درست است.

حال فرض کنید که قضیه برای همه گروههای آبلی از مرتبه کمتر از n درست باشد و فرض کنید $|G| = n$. فرض کنید a هر عنصر غیرهمانی G باشد. در این صورت مرتبه a یک عدد صحیح مثبت است و بنابراین توسط عددی اول مثل q شمرده می‌شود (قضیه ۱۱.۱). مثلاً $|a| = qt$. طبق قضیه ۵.۷، عضو $b = a^t$ دارای مرتبه q است. اگر $q = p$ قضیه اثبات شده‌است. اگر $q \neq p$، فرض کنید N زیرگروه دوری $< b >$ باشد. N نرمال است چون G آبلی است، و طبق قضیه ۱۰.۷، N دارای مرتبه q است. بنابر نتیجه ۳۴.۷، گروه خارج قسمت G/N دارای مرتبه $|G/N| = |G| / |N| = n/q < n$ می‌باشد. در نتیجه طبق فرض استقراء قضیه برای گروه G/N درست است. عدد اول p، $|G|$ را می‌شمارد و $|G/N| = q$ $|G/N|$ $|N| = |G|$. چون q یک عدد اول به غیر از p است، طبق قضیه ۸.۱، p باید $|G/N|$ را بشمارد. بنابراین G/N شامل عنصری از مرتبه p، مثلاً Nc است. چون Nc در G/N دارای مرتبه p است، داریم $Nc^p = (Nc)^p = Ne$ و بنابراین $c^p \in N$. چون N دارای مرتبه q است، بنابه قسمت (۲) نتیجه ۳۴.۷، $c^{pq} = (c^p)^q = e$. بنابراین طبق قضیه ۵.۷، مرتبهٔ c باید pq را بشمارد. امّا c نمی‌تواند دارای مرتبه ۱ باشد زیرا در این صورت Nc در G/N باید بجای p دارای مرتبه ۱ باشد. همچنین c نمی‌تواند دارای مرتبه q باشد زیرا در این صورت در G/N داریم $(Nc)^q = Nc^q = Ne$، بنابراین طبق قضیه ۵.۷، p (مرتبه Nc) باید q را بشمارد که ممکن نیست. تنها احتمال این است که c دارای مرتبه p یا pq باشد؛ در حالت دوم، طبق قضیه ۵.۷، c^q دارای مرتبه p است. در هر حالت، G شامل عنصری از مرتبه p است. بنابراین قضیه برای گروههای آبلی از مرتبه n و از آنجا بنا به استقراء برای همه گروههای آبلی متناهی درست است. ■

۲۵) پیوست چ را ملاحظه کنید.

نتیجه ۳۹.۷. فرض کنید p و q اعداد اول مثبت متمایز باشند. هرگروه آبلی از مرتبه pq یکریخت با $\mathbb{Z}_{pq}$ است.

برهان. اگر G دارای مرتبه pq باشد، در این صورت طبق قضیه کشی، G شامل یک عضو a از مرتبه p و یک عضو b از مرتبه q است. چون G آبلی است، طبق تمرین ۲۹ بخش ۲.۷، عضو ab دارای مرتبه pq است. بنابراین زیرگروه دوری $< ab >$ دارای مرتبه pq است (قضیه ۱۰.۷) و لذا همه G می‌باشد. بنابراین طبق قضیه ۱۳.۷، $G \cong \mathbb{Z}_{pq}$. ■

نتیجه ۴۰.۷. هرگروه از مرتبه ۶ یکریخت با $\mathbb{Z}_۶$ یا $S_۳$ است.

برهان. اگر G آبلی باشد در این صورت نتیجه ۳۹.۷ (با $p = ۲$ و $q = ۳$) نشان می‌دهد که $G \cong \mathbb{Z}_۶$. اگر G غیرآبلی باشد، در این صورت طبق‌قضیه ۳۷.۷، $G \cong S_۳$. ■

تا اینجا همه گروههای از مرتبه ≥ ۷ را رده‌بندی کرده‌ایم. ثابت می‌شود (گرچه که ما این اثبات را ارائه نمی‌کنیم) که (تا حد یکریختی) پنج گروه مختلف از مرتبه ۸ وجود دارد. سه تای آنها که آبلی هستند عبارتند از $\mathbb{Z}_۸$، $\mathbb{Z}_۴ \times \mathbb{Z}_۲$ و $\mathbb{Z}_۲ \times \mathbb{Z}_۲ \times \mathbb{Z}_۲$. غیرآبلی‌ها عبارتند از $D_۴$ و گروه چهارگانی (تمرین ۱۴ بخش ۱.۷). تا اینجا به‌سختی قادر بوده‌ایم رخنه کوچکی در سطح مسئله رده‌بندی گروههای متناهی وارد کنیم. در فصل ۱۰، کارهای بیشتری انجام می‌دهیم، برای مثال همه گروههای آبلی متناهی تا حد یکریختی رده‌بندی خواهند شد.

البته این معرفی مختصر مسئله رده‌بندی نیز بدون ذکر گروههایی که کلید حل این مسئله می‌باشند کامل بنظر نمی‌رسد. یک گروه G **ساده** نامیده می‌شود اگر تنها زیرگروههای نرمال آن $< e >$ و خود G باشند. بنابه تمرین ۱۱، تنها گروههای آبلی ساده، گروههای $\mathbb{Z}_p$ که در آن p اول است می‌باشند. در بخش بعد، تعدادی از گروههای غیرآبلی ساده، گروههای تناوبی، معرفی خواهد شد. همانگونه که اکنون خواهیم دید، گروههای ساده، اجزاء اصلی ساختمان گروهها هستند.

اگر G گروهی متناهی و $G_۱$ یک زیرگروه نرمال آن با بزرگترین مرتبه ممکن باشد، در این صورت هیچ زیرگروه نرمالی بین $G_۱$ و G وجود ندارد. در نتیجه طبق قضیه ۳۱.۷، گروه خارج قسمت $G/G_۱$ ساده است. به‌طور مشابه اگر $G_۲$ زیرگروه نرمالی از $G_۱$ با بزرگترین مرتبه ممکن باشد در این صورت $G_۱/G_۲$ ساده است. با ادامه این روند می‌توانیم دنباله‌ای از گروههای $G = G_۰, G_۱, G_۲, \ldots, G_{n-۱}, G_n =< e >$ بدست آوریم به قسمی که هر یک زیرگروه نرمالی

از گروه قبلی بوده و G_i/G_{i+1} ساده باشد. می‌توان نشان داد که فهرست گروههای ساده‌ای که بدین طریق به دست می‌آیند مستقل از روشی است که در آن G_i–ها انتخاب می‌شوند. به عبارت دیگر، این گروههای ساده **(که عوامل ترکیبی G نامیده می‌شوند)** به‌طور کامل توسط گروه G معین می‌شوند. این راهکاری را برای حل مسئله رده‌بندی پیشنهاد می‌کند که به آن می‌پردازیم. اگر همه گروههای ساده تا حد یکریختی رده‌بندی شوند و اگر بتوان نشان داد که چگونه عوامل ترکیبی ساختار G را تعیین می‌کنند، رده‌بندی همه گروههای متناهی تا حد یکریختی ممکن می‌شود.

نکته مثبت این است که قسمت اول این کار قبلاً با موفقیت انجام شده است. در یک دوره ۲۵ ساله که در سال ۱۹۸۱ پایان یافت، تعدادی از صاحب‌نظران نظریه گروهها در اقصی‌نقاط جهان روی جنبه‌های مختلف این مسئله کارکردند و سرانجام رده‌بندی همه گروههای ساده تا حد یکریختی بدست آمد. اثبات کامل این نتیجه شگفت‌آور متجاوز از ۱۰۰۰۰ صفحه است!

از قضیه آخر این بخش که اینک به آن می‌پردازیم تا بخش ۵.۹ استفاده نخواهد شد. در صورت تمایل می‌توانید مطالعه آن را تا آن بخش به تاخیر اندازید. این قضیه به این دلیل در اینجا آمده است که قضیه ساختاری مفیدی است و اثبات آن، کاربردی زیبا از برخی مفاهیم مقدماتی نظریه گروهها می‌باشد. اثبات ژرفتری از این قضیه را می‌توانید در نتیجه ۱۱.۱۰ ملاحظه کنید.

قضیه ۴۱.۷. فرض کنید $\mathbb{F}$ یک میدان و G یک زیرگروه متناهی گروه ضربی $\mathbb{F}^*$ از عناصر غیرصفر $\mathbb{F}$ باشد. در این صورت G دوری است.

اثبات این قضیه به یک لم و یک تعریف نیاز دارد.

لم ۴۲.۷. فرض کنید G یک گروه، b یک عضو G از مرتبه d و k یک عدد صحیح مثبت باشد. در این صورت b^k دارای مرتبه d است اگر و تنها اگر $(k,d)=1$.

برهان. ($\Leftarrow$) فرض کنید $|b^k|=d$. به خلاف فرض کنید که $(k,d)=r>1$. در این صورت $k=rk'$ و $d=rd'$ با $d'<d$. چون $(b^k)^{d'}=b^{rk'd'}=b^{k'd}=(b^d)^{k'}=e^{k'}=e$، قضیه ۵.۷ نتیجه می‌دهد که $d \mid d'$. این یک تناقض است زیرا هر دو مثبت هستند و $d'<d$. بنابراین $(k,d)=1$.

($\Rightarrow$) فرض کنید $|b^k|=t$. چون $(b^k)^d=(b^d)^k=e^k=e$، قضیه ۵.۷ نتیجه می‌دهد که $t \mid d$. به‌طور مشابه چون $(b^k)^t=e$ و $|b|=d$، قضیه ۵.۷ نتیجه می‌دهد که $d \mid kt$. اگر

$(k,d) = ۱$ در این صورت طبق قضیه ۵.۱، $d \mid t$. بنابراین $t \mid d$ و $d \mid t$ (که در آن هر دو t و d مثبت هستند)، لذا $d = t = \mid b^k \mid$. ■

اینک به معرفی **تابع ϕ–اویلر**[۲۶] که ضابطه آن به‌صورت زیر تعریف می‌شود می‌پردازیم: $\phi(۱) = ۱$ و برای هر عدد صحیح مثبت $n > ۱$، $\phi(n)$ برابر تعداد اعداد صحیح مثبت k ای است که $k \leq n$ و $(k,n) = ۱$. برای مثال $\phi(۶) = ۲$ زیرا ۱ و ۵ تنها اعداد صحیح بین ۱ و ۶ هستند که نسبت به ۶ اولند. این تابع در قسمت‌های مختلف ریاضیات و از جمله در اینجا ظاهر می‌شود:

برهان قضیه ۴۱.۷. اگر $n = \mid G \mid$ در این صورت طبق نتیجه ۳۴.۷، مرتبه هر عضو G، n را می‌شمارد. فرض کنید $d_۱, d_۲, \ldots, d_t = n$ $۱ = d_۱$ همه شمارنده‌های مثبت n باشند. در این صورت $n = \mid G \mid = n_۱ + \cdots + n_t$ که در آن n_i تعداد عناصری از G است که مرتبهٔ d_i دارند. فرض کنید K هر گروه دوری از مرتبه n باشد. استدلالی مشابه نشان می‌دهد که $n = \mid K \mid = m_۱ + \cdots + m_t$ که در آن m_i تعداد عناصری از K است که مرتبه d_i دارند. ادعا می‌کنیم که برای هر i، $۰ \leq n_i \leq m_i$؛ برای لحظه‌ای فرض کنید این حقیقت برقرار باشد. اگر G دوری نباشد، در این صورت G دارای هیچ عنصری از مرتبه $d_t = n$ نیست و بنابراین $n_t = ۰$. امّا یقیناً K دارای عنصری از مرتبهٔ n است و لذا $m_t \geq ۱$. بنابراین $n_t < m_t$. چون برای هر $۱ \leq i \leq t-۱$، $n_i \leq m_i$، داریم

$$n = n_۱ + \cdots + n_t < m_۱ + \cdots + m_t = n,$$

که منجر به تناقض $n < n$ می‌شود. پس G شامل عنصری از مرتبه n می‌باشد و بنابراین یک گروه دوری است.

برای تکمیل اثبات، باید ادعای بکار رفته در بالا را بررسی کنیم و نشان دهیم که برای هر شمارنده مثبت d از n، تعداد عناصری از G که دارای مرتبهٔ d هستند از تعداد عناصری از K که دارای مرتبهٔ d هستند کمتر است. این را با شمارش عناصری از گروه دوری K، که دارای مرتبه d هستند آغاز می‌کنیم. اگر a یک مولد K باشد در این صورت a دارای مرتبه n است و طبق قسمت (۳) قضیه ۵.۷، $b = a^{n/d}$ دارای مرتبه d است. عناصر b، $b^۲$، ...، $b^d = e$ همه متمایزند. طبق لم ۴۲.۷، تعداد b^iهایی که دارای مرتبه d هستند برابر تعداد اعداد صحیح k ای است که $۱ \leq k \leq d$ و $(d,k) = ۱$، یعنی برابر $\phi(d)$ می‌باشد. بنابراین K حداقل دارای $\phi(d)$ عنصر از مرتبه d است.

اکنون تنها لازم است نشان دهیم که G حداکثر $\phi(d)$ عنصر از مرتبه d دارد. مسلماً این مطلب

---

۲۶) Euler ϕ–function

در صورتی که G هیچ عنصری از مرتبه d نداشته باشد درست است، پس فرض کنید G دارای یک عنصر c از مرتبه d باشد. طبق نتیجه ۱۳.۴، همه d عنصر متمایز

$$c, c^2, c^3, \cdots, c^{d-1}, c^d = 1_{\mathbb{F}}$$

ریشه‌های $x^d - 1_{\mathbb{F}}$ می‌باشند زیرا برای هر i، $(c^i)^d = (c^d)^i = 1_{\mathbb{F}}$. امّا هر عنصر از مرتبه d در G یک ریشه $x^d - 1_{\mathbb{F}}$ است و بنابراین باید در فهرست بالا باشد. لم ۲۴.۷ (با $b = c$) نشان می‌دهد که در این فهرست دقیقاً $\phi(d)$ عنصر از مرتبه d وجود دارد. پس در هر حالت G دارای حداکثر $\phi(d)$ عنصر از مرتبه d است. ■

تمرینها

۱.A. شاخص $[G : H]$ را بیابید وقتی که

(الف) $H = \{r_0, r_2\}$ و $G = D_4$

(ب) $H =< 3 >$ و $G = \mathbb{Z}_{12}$

(پ) $H =< 3 >$ و $G = \mathbb{Z}_{20}$

(ت) $G = \mathbb{Z}_{40}$ و H زیرگروه تولیدشده توسط ۱۲ و ۲۰ باشد.

(ث) $G = S_4$ و H زیرگروه تولیدشده توسط $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ باشد.

۲. مثال‌هایی بجز آنهایی که در متن آمده‌است از گروههای نامتناهی G و H ارائه دهید که:

(الف) $[G : H]$ متناهی باشد. (ب) $[G : H]$ نامتناهی باشد.

۳. مرتبه‌های ممکن زیرگروههای G را وقتی که G یکی از گروههای زیر باشد تعیین کنید.

(الف) $\mathbb{Z}_{24}$ (ب) S_4 (پ) $D_4 \times \mathbb{Z}_{10}$

۴. اگر تعداد عناصر G کمتر از ۱۰۰ باشد و G زیرگروههایی از مرتبه‌های ۱۰ و ۲۵ داشته باشد، مرتبه G چیست؟

۵. فرض کنید G گروهی متناهی باشد که عناصری از مرتبه‌های ۱ تا ۱۲ را شامل است. کمترین مقدار ممکن $|G|$ چیست ؟

۶. اگر H و K زیرگروههایی از یک گروه متناهی G باشند. ثابت کنید که $|H \cap K|$ یک شمارنده مشترک $|H|$ و $|K|$ است.

۷. فرض کنید H و K زیرگروههایی از یک گروه G و هر دو دارای مرتبه اول p باشند. اگر $H \neq K$، ثابت کنید که $H \cap K = \langle e \rangle$.

۸. اگر H زیرگروهی از یک گروه G باشد به قسمی که $[G : H] = ۲$، ثابت کنید که H نرمال است.

۹. طبق قضیه ۴۰.۷، همه گروههای ضربی زیر دوری هستند. برای هر یک مولدی بیابید:
(الف) $\mathbb{Z}_۷^*$ (ب) $\mathbb{Z}_{۱۱}^*$ (پ) $\mathbb{Z}_{۱۹}^*$.

۱۰. فرض کنید $\mathbb{F}$ یک میدان و n یک عدد صحیح مثبت باشد. ثابت کنید که مجموعه ریشه‌های $x^n - ۱_{\mathbb{F}}$ در $\mathbb{F}$ تحت عمل ضرب یک گروه دوری است.

B ۱۱. اگر G گروهی باشد که دارای هیچ زیرگروه سره نیست، ثابت کنید که برای یک عدد اول p، G یکریخت با $\mathbb{Z}_p$ است.

۱۲. اگر G گروهی از مرتبه ۲۵ باشد، ثابت کنید که یا G دوری است و یا هر عضو غیرهمانی G دارای مرتبه ۵ است.

۱۳. فرض کنید a عضوی از مرتبه ۳۰ در یک گروه G باشد. شاخص $\langle a^۴ \rangle$ در گروه $\langle a \rangle$ چیست؟

۱۴. فرض کنید H و K زیرگروههایی از یک گروه متناهی G باشند به قسمی که $[G : H] = p$ و $[G : K] = q$ که در آن p و q اعداد اول متمایز هستند. ثابت کنید که $[G : H \cap K]$، pq را می‌شمارد.

۱۵. (الف) فرض کنید p یک عدد اول و c عنصری غیرصفر در $\mathbb{Z}_p$ باشد. نشان دهید $c^{p-۱} = ۱$.
[راهنمایی: $\mathbb{Z}_p$ یک میدان است.]

(ب) **قضیه کوچک فرما**[۲۷] را ثابت کنید: اگر p یک عدد اول و a هر عدد صحیح باشد، در این صورت (پیمانه p) $a^p \equiv a$. به‌علاوه اگر $(a, p) = ۱$ آنگاه (پیمانه p) $a^{p-۱} \equiv ۱$.
[راهنمایی: فرض کنید c کلاس همنهشتی a در $\mathbb{Z}_p$ باشد و قسمت (الف) را بکار برید.]

۲۷) Fermat's Little Theorem

۱۶. اگر $f : G \to H$ یک همریختی پوشا از گروههای متناهی باشد، ثابت کنید که $|H|$، $|G|$ را می‌شمارد.

۱۷. اگر $f : G \to H$ یک همریختی گروهی و اگر $a \in G$ دارای مرتبه متناهی باشد، ثابت کنید که $f(a)$ دارای مرتبه متناهی در H است و $|f(a)|$ | $|a|$.

۱۸. فرض کنید H و K زیرگروههایی از یک گروه G باشند به قسمی که $K \subseteq H$ و $[G : H]$ و $[H : K]$ متناهی باشند. ثابت کنید که $[G : K]$ متناهی است و $[G : K] = [G : H][H : K]$.

۱۹. اگر p و q اعداد اول باشند، نشان دهید که هر زیرگروه سره یک گروه از مرتبه pq دوری است.

۲۰. (الف) اگر G یک گروه آبلی از مرتبه $2n$ باشد که در آن n فرد است، ثابت کنید که G دقیقاً دارای یک عنصر از مرتبه ۲ است.

(ب) با مثال نشان دهید که اگر G غیرآبلی باشد قسمت (الف) ممکن است غلط باشد.

۲۱. فرض کنید G یک گروه آبلی از مرتبه n و k یک عدد صحیح مثبت باشد. ثابت کنید که تابع $f : G \to G$ که توسط $f(a) = a^k$ تعریف می‌شود یکریختی است اگر و تنها اگر $(k, n) = 1$.

۲۲. اگر G گروهی از مرتبه n باشد که دارای 2^{n-1} زیرگروه است، ثابت کنید که $G =< e >$ یا $G \cong \mathbb{Z}_2$.

۲۳. فرض کنید G یک گروه از مرتبه pq باشد که در آن p و q اعداد اوّلند (که لزوماً متمایز نیستند). ثابت کنید که مرکز G باید دارای مرتبه ۱ یا pq باشد.

۲۴. فرض کنید a و b عناصری از یک گروه G باشند به قسمی که $a^5 = e$، $aba^{-1} = b^2$ و $b \neq e$. مرتبه b چیست؟

۲۵. ثابت کنید که یک گروه غیرآبلی از مرتبه ۱۰، دارای پنج عنصر از مرتبه ۲ است. [راهنمایی: تمرین ۷ و برهان قضیه ۳۷.۷ را ملاحظه کنید.]

۲۶. ثابت کنید که یک گروه از مرتبه ۳۳ دارای عضوی از مرتبه ۳ است.

۲۷. فرض کنید G گروهی از مرتبه p^2 باشد که در آن p اول و مرکز آن غیربدیهی است. ثابت کنید که G آبلی است.

۲۸. اگر N یک زیرگروه نرمال متناهی از گروه G و اگر G/N عضوی از مرتبه n داشته باشد، ثابت کنید که G عضوی از مرتبه n دارد. [راهنمایی: تمرین ۱۷ می‌تواند مفید باشد.]

۲۹. اگر عدد اول p مرتبه یک گروه متناهی G را بشمارد، ثابت کنید که تعداد عناصری از G که دارای مرتبه p هستند مضربی از $p-1$ است.

۳۰. فرض کند n حاصل‌ضربی از اعداد اول مثبت متمایز باشد. ثابت کنید که هر گروه آبلی از مرتبه n یکریخت با $\mathbb{Z}_n$ است. [نتیجه ۳۹.۷ یک حالت خاص آن است.]

۳۱. فرض کنید G یک گروه آبلی متناهی و p یک عدد اول مثبت باشد. اگر H زیرمجموعه‌ای از G متشکل از e و همه عناصر از مرتبه p باشد، ثابت کنید که H زیرگروهی از مرتبه p^k است که در آن k یک عدد طبیعی است.

۳۲. **قضیه کشی** را برای حالت $p = ۲$ ثابت کنید: اگر G گروهی باشد که مرتبه آن بر ۲ بخش‌پذیر باشد، در این صورت G شامل عنصری از مرتبه ۲ است. [راهنمایی: اگر G دارای هیچ عنصری از مرتبه ۲ نباشد، نشان دهید که مجموعه عناصر غیرهمانی G اجتماعی از مجموعه‌های دو عضوی دوبه‌دو مجزا به‌صورت $\{a, a^{-۱}\}$ می‌باشد و بنابراین تعداد عناصر آن زوج است که یک تناقض می‌باشد.]

۳۳. فرض کنید m، n و p اعداد صحیح مثبت، و p اول باشد. ثابت کنید که تابع ϕ-اویلر دارای خواص زیر است.

(الف) $\phi(p) = p - ۱$

(ب) $\phi(p^n) = p^{n-۱}(p-۱)$

(پ) اگر $(m,n) = ۱$ آنگاه $\phi(mn) = \phi(m)\phi(n)$.

۳۴.C فرض کنید G گروهی باشد که توسط عناصر a و b تولید شده‌است به قسمی که $|a| = ۴$، $|b| = ۲$ و $ba = a^۳b$. نشان دهید که G یک گروه از مرتبه ۸ است، و این که G یکریخت با $D_۴$ است.

۳۵. فرض کنید G گروهی باشد که توسط a و b تولید شده‌است به قسمی که $|a| = ۴$، $b^۲ = a^۲$ و $ba = a^۳b$. نشان دهید که G یک گروه از مرتبه ۸ است، و این که G با گروه چهارگانی تمرین ۱۴ بخش ۱.۷ یکریخت می‌باشد.]

۳۶. قضیه اویلر[۲۸] را ثابت کنید: اگر n یک عدد صحیح مثبت و a عدد صحیحی باشد که $(a, n) = ۱$، در این صورت (پیمانه n) $a^{\phi(n)} \equiv ۱$. [راهنمایی: توجه کنید که تمرین ۱۵ (ب) یک حالت خاص این است.]

۳۷. ثابت کنید که **عکس قضیه لاگرانژ برای گروههای آبلی** برقرار است: اگر G یک گروه آبلی متناهی باشد و k مرتبه G را بشمارد، در این صورت G دارای زیرگروهی از مرتبه k است. [راهنمایی: از استقراء روی $|G|$ استفاده کنید؛ فرض کنید $n = |G|$. اگر قضیه برای گروههای از مرتبه کمتر از n درست باشد و $k \mid n$، فرض کنید p یک شمارنده اول k باشد. در این صورت G دارای یک عنصر a از مرتبه p است (چرا؟) و اگر $N = <a>$، آنگاه G/N گروهی است که مرتبه آن کمتر از n است و توسط k/p شمرده می‌شود. از استقراء، قضیه ۳۱.۷ و نتیجه ۳۴.۷ استفاده کنید.]

۹-۷ گروههای متقارن

گروههای متقارن متناهی S_n با اهمیت هستند زیرا همانگونه که در نتیجه ۱۶.۷ دیدیم هر گروه متناهی یکریخت با زیرگروهی از یک گروه S_n است. برخی از زیرگروههای S_n که در اینجا معرفی خواهند شد نیز مورد توجه‌اند زیرا آنها گروههای غیرآبلی ساده هستند. همانگونه که در بخش ۸.۷ دیدیم این گروهها اجزاء اصلی تشکیل‌دهنده ساختمان همه گروهها می‌باشند.

نمادی که تاکنون برای نمایش عناصر گروههای متقارن بکار رفته‌است چندان مناسب نیست زیرا نماد دیگری وجود دارد که نکات مفید بیشتری را در مورد گروههای متقارن نشان می‌دهد. پس به معرفی این نماد جدید می‌پردازیم.

جایگشت $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۱ & ۴ & ۳ & ۶ & ۲ & ۵ \end{pmatrix}$ در $S_۶$ را در نظر بگیرید. توجه کنید که ۲ به ۴، ۴ به ۶ و ۶ به ۵ نگاشته شده‌است و ۵ به ۲ برگشته است و دو عنصر دیگر ۱ و ۳ به خودشان نگاشته شده‌اند. همه اطلاعات اساسی در مورد این جایگشت را می‌توان در نمودار زیر خلاصه نمود:

۲۸) Euler's Theorem

که البته اگر ترتیب عناصر به‌صورت فوق حفظ شود لزومی به لحاظ کردن فلش‌ها نیست. می‌توان توصیف کاملی از این جایگشت را توسط نماد $\begin{pmatrix} ۵ & ۶ & ۴ & ۲ \end{pmatrix}$ بدست آورد در صورتی که بدانیم:

- هر عنصر به عنصری که بلافاصله در سمت راست آن نوشته شده نگاشته می‌شود؛
- آخرین عنصر در این ردیف به اولین عنصر نگاشته می‌شود؛
- عناصری که فهرست نشده‌اند به خودشان نگاشته می‌شوند.

این مثالی از نماد دُور است که اینک تعریف رسمی آن را ارائه می‌کنیم.

تعریف. فرض کنید $a_۱$، $a_۲$، $a_۳$، ...، a_k (با $k \geq ۱$) عناصر متمایزی از مجموعه $\{۱, ۲, ۳, \ldots, n\}$ باشند. در این صورت $(a_۱a_۲a_۳\cdots a_k)$ جایگشتی در S_n را نمایش می‌دهد که $a_۱$ را به $a_۲$، $a_۲$ را به $a_۳$، ...، $a_{k-۱}$ را به a_k و a_k را به $a_۱$ می‌نگارد و هر عنصر دیگر $\{۱, ۲, ۳, \ldots, n\}$ را به خودش می‌نگارد. $(a_۱a_۲a_۳\cdots a_k)$ یک **دور به طول k** یا یک **$k-$دُور** نامیده‌می‌شود.

مثال ۴۶.۷. در $S_۴$، $\begin{pmatrix} ۳ & ۴ & ۱ \end{pmatrix}$ یک ۳ دور است که ۱ را به ۴، ۴ را به ۳، ۳ را به ۱ و ۲ را به خودش می‌نگارد؛ این جایگشت در نماد قدیمی به صورت $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۴ & ۲ & ۱ & ۳ \end{pmatrix}$ نوشته می‌شد. توجه کنید که $\begin{pmatrix} ۳ & ۴ & ۱ \end{pmatrix}$ را می‌توان با $\begin{pmatrix} ۱ & ۳ & ۴ \end{pmatrix}$ و یا $\begin{pmatrix} ۴ & ۱ & ۳ \end{pmatrix}$ نیز نمایش داد، زیرا هر یک از اینها تابعی را نشان می‌دهد که ۱ را به ۴، ۴ را به ۳، ۳ را به ۱ و ۲ را به ۲ می‌نگارد.

مثال ۴۷.۷. برطبق تعریف بالا ۱-دور (۳) در S_n جایگشتی است که ۳ را به ۳ و هر عضو دیگر $\{۱, ۲, \ldots, n\}$ را به خودش می‌نگارد؛ به عبارت دیگر (۳) جایگشت همانی است. به طور مشابه برای هر k در $\{۱, ۲, \ldots, n\}$، ۱-دور (k) جایگشت همانی است.

اگر بخواهیم دقیق باشیم، نماد دور یک نماد مبهم است زیرا برای مثال $\begin{pmatrix} ۳ & ۶ & ۱ \end{pmatrix}$ می‌تواند نشان‌دهنده یک جایگشت در $S_۶$، در $S_۷$ یا در هر S_n با $n \geq ۶$ باشد. با این حال این امر در عمل مشکلی را پدید نمی‌آورد زیرا در متن همواره تصریح خواهد شد که کدام گروه S_n مورد بحث ما است.

همانند وقتی که از نماد قدیمی استفاده می‌شد، در نماد جدید نیز می‌توان حاصل‌ضرب دورها را

با دنبال‌کردن بصری عناصر انجام داد. برای مثال می‌دانیم که

$$\begin{pmatrix}۱&۲&۳&۴\\۱&۴&۲&۳\end{pmatrix}\circ\begin{pmatrix}۱&۲&۳&۴\\۲&۴&۱&۳\end{pmatrix}=\begin{pmatrix}۱&۲&۳&۴\\۴&۳&۱&۲\end{pmatrix}$$

(به یاد آورید که حاصل‌ضرب در S_n، ترکیب توابع است و لذا جایگشت سمت راست ابتدا عمل می‌کند.) در نماد دوری این حاصل‌ضرب[۲۹] به صورت زیر در می‌آید:

$$(۲\ ۴\ ۳)\circ(۱\ ۲\ ۴\ ۳)=(۱\ \ ۴\ \ ۲\ \ ۳).$$

فلشها مبین این فرآیند است که: ۱ به ۲ و ۲ به ۴ نگاشته می‌شود، بنابراین عمل ضرب، ۱ را به ۴ می‌نگارد. به‌طور مشابه ۴ به ۳ و ۳ به ۲ نگاشته می‌شود، لذا عمل ضرب ۴ را به ۲ می‌نگارد.

دو دور را **مجزا** گویند، اگر هیچ عنصر مشترکی نداشته باشند. برای مثال (۱۳) و (۲۵۴۶) دو دور مجزا در $S_۶$ هستند امّا (۱۳) و (۳۴۵) مجزا نیستند زیرا ۳ در هر دو دور ظاهر می‌شود.

اگرچه که هر جایگشت یک دور نیست امّا هر جایگشت را می‌توان به صورت حاصل‌ضربی از دورهای مجزا بیان کرد. برای مثال جایگشت $\begin{pmatrix}۱&۲&۳&۴&۵&۶&۷\\۵&۱&۷&۲&۴&۶&۳\end{pmatrix}$ را در $S_۷$ در نظر می‌گیریم. عنصری مانند ۱ را که به خودش نگاشته نشده بیابید و با دنبال کردن آن معین کنید که تحت این جایگشت به کجا فرستاده می‌شود:

۱ به ۵ نگاشته شده است، ۵ به ۴ نگاشته شده است، ۴ به ۲ نگاشته شده است و ۲ به ۱ (عنصری که از آن شروع کردیم) نگاشته می‌شود.

بنابراین جایگشت فوق و دور (۱۵۴۲) دارای اثر یکسانی روی این چهار عنصر هستند. حال هر عنصر دیگر به غیر از ۱، ۵، ۴ و ۲ که به خودش نگاشته نشده‌است، مثل ۳، را در نظر بگیرید. توجه کنید که

۳ به ۷ نگاشته شده است و ۷ به ۳ نگاشته شده است.

تنها عنصر باقیمانده ۶ است که به خودش نگاشته می‌شود. حال می‌توانید به سادگی بررسی کنید که

۲۹) از اینجا به بعد نماد ترکیب $\circ$ را حذف می‌کنیم و عمل S_n را ضربی می‌نویسیم.

جایگشت مفروض حاصل‌ضرب دو دور (۱۵۴۲) و (۳۷) است، یعنی

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۵ & ۱ & ۷ & ۲ & ۴ & ۶ & ۳ \end{pmatrix} = (۱\ ۵\ ۴\ ۲)\,(۳\ ۷).$$

در حالت کلی گرچه باید دقت بیشتری شود و نمادها پیچیده‌تر می‌شوند، امّا اساساً همان روند بالا کارساز بوده، قضیه زیر ثابت می‌شود.

قضیه ۴۳.۷. هر جایگشت در S_n حاصل‌ضربی از دورهای مجزا است[۳۰].

برهان. روند مثال قبل را سازگار نمائید؛ تمرین ۳۵ را ملاحظه کنید. ■

توجه کنید که جایگشت همانی می‌تواند به‌صورت (۱۲)(۱۲) = (۱) نوشته شود. به‌طور مشابه، دور (۱۲۳۴) نیز حاصل‌ضربی از ۲-دورهای (غیرمجزا) است زیرا (۱۲)(۱۳)(۱۴) = (۱۲۳۴). یک ۲-دور معمولاً یک **ترانهش** نامیده می‌شود. به‌سادگی می‌توانید بررسی کنید که هر دور $(a_۱a_۲\cdots a_k)$ حاصل‌ضربی از ترانهش‌ها است،

$$(a_۱a_۲\cdots a_k) = (a_۱a_k)(a_۱a_{k-۱})\cdots(a_۱a_۳)(a_۱a_۲).$$

بنابراین قضیه ۴۳.۷ نتیجه زیر را بدست می‌دهد.

نتیجه ۴۴.۷. هر جایگشت در S_n حاصل‌ضربی از ترانهش‌ها است.

این نتیجه را می‌توان مستقیماً با استقراء و بدون استفاده از قضیه ۴۳.۷ نیز اثبات نمود (تمرین ۲۱).

تجزیه یک جایگشت به صورت حاصل‌ضربی از دورهای مجزا، بجز در مورد ترتیب دورها، یکتاست (تمرین ۲۰)، امّا تجزیه به صورت حاصل‌ضربی از ترانهش‌ها فاصله زیادی از یکتابودن دارد. برای مثال

$$(۱۵)(۱۳)(۱۲) = (۱۲۳۵) = (۱۳)(۲۴)(۳۵)(۱۴)(۲۴).$$

در واقع چون هر ترانهش وارون خودش است (برای نمونه (۱) = (۱۲)(۱۲)) همواره می‌توانید زوج $(ab)(ab)$ را در هر تجزیه‌ای از یک جایگشت به عنوان حاصل‌ضربی از ترانهش‌ها وارد کنید بدون این‌که روی حاصل تأثیری گذاشته شود.

۳۰) مانند قبل، ما امکان حاصل‌ضربی‌هایی با تنها یک دور را می‌پذیریم.

یک جایگشت در S_n را **زوج** گویند اگر بتوان آن را به صورت حاصلضرب تعداد زوجی از ترانهش‌ها نوشت و **فرد** نامیده می‌شود اگر بتوان آن را به صورت حاصلضرب تعداد فردی از ترانهش‌ها نوشت. برای مثال دو جایگشت (۱۲۳) و (۲۵۴۳)(۱۲) زوج هستند زیرا (۱۲)(۱۳) = (۱۲۳) و (۲۵)(۲۴)(۲۳)(۱۲) = (۲۵۴۳)(۱۲) و (۱۲۳۴) فرد است زیرا (۱۲)(۱۳)(۱۴) = (۱۲۳۴). جایگشت همانی زوج است زیرا (۱۲)(۱۲) = (۱).

نتیجه ۴۴.۷ نشان می‌دهد که هر جایگشت یا زوج یا فرد است. با این حال چون یک جایگشت مفروض را می‌توان به طرق بسیار زیادی به صورت حاصلضربی از ترانهش‌ها تجزیه کرد این واضح نیست که آیا یک جایگشت می‌تواند هم‌زوج و هم فرد باشد. در زیر نشان می‌دهیم که این ممکن نیست امّا ابتدا برخی از حقایق اساسی در مورد جایگشت‌های زوج را بدست می‌دهیم.

مجموعه همه جایگشتهای زوج در S_n با A_n نشان داده می‌شود و آن را **گروه تناوبی از درجه** n گویند. کلمه "گروه" در اینجا توسط قضیه زیر توجیه می‌شود.

قضیه ۴۵.۷. A_n زیرگروه نرمالی از S_n است.

برهان. اگر $\alpha \in A_n$ حاصلضربی از s ترانهش و اگر $\beta \in A_n$ حاصلضربی از t ترانهش، باشد که در آن s و t زوج هستند در این صورت $\alpha\beta$ حاصلضربی از $s+t$ ترانهش است. چون $s+t$ زوج است، $\alpha\beta \in A_n$. بنابراین طبق قضیه ۸.۷، A_n یک زیرگروه است.

اگر τ هر عضوی از S_n باشد، در این صورت طبق نتیجه ۴۴.۷، $\tau = \tau_1\tau_2\cdots\tau_r$ که در آن هر τ_i یک ترانهش است. چون هر ترانهش وارون خودش است، نتیجه ۳.۷ نشان می‌دهد که

$$\tau^{-1} = \tau_r^{-1}\cdots\tau_2^{-1}\tau_1^{-1} = \tau_r\cdots\tau_2\tau_1.$$

اگر $\sigma \in A_n$ حاصلضربی از تعداد زوج مثلاً k ترانهش باشد، در این صورت $\tau\sigma\tau^{-1}$ حاصلضربی از $r+k+r = k+2r$ ترانهش است. چون $k+2r$ زوج است، $\tau\sigma\tau^{-1} \in A_n$. بنابراین طبق قضیه ۲۱.۷، A_n نرمال است. ■

گروههای تناوبی A_n با $n \geq 5$ مهم هستند زیرا اولین مثال‌هایی از گروههای غیرآبلی ساده می‌باشند[۳۱]، این حقیقت در فصل ۱۰ ثابت می‌شود. در حال حاضر باید به مسئله‌ای اساسی‌تر بپردازیم.

یافتن عناصری از گروه A_n آسان است، امّا چگونه می‌توان فهمید که آیا اینها همه عناصر A_n

۳۱) بند دوم بعد از نتیجه ۴۰.۷ را برای تعریف گروه ساده ملاحظه کنید.

هستند؟ برای مثال، دور (۱۲) فرد است امّا آیا امکان زوج‌بودن آن نیز هست؟ به منظور پاسخگویی به این سؤال و تعیین مرتبه A_n، ابتدا باید نشان دهیم که یک جایگشت نمی‌تواند هم‌زوج و هم فرد باشد. باقیمانده این بخش به اثبات این حقیقت و استفاده ازآن در نشان دادن این که A_n دارای مرتبه $n!/۲$ است و این که دارای شاخص ۲ در S_n می‌باشد اختصاص یافته‌است. از این اطلاعات تنها در بخش ۵.۱۰ استفاده خواهد شد.

لم ۴۶.۷. جایگشت همانی در S_n فرد نیست.

برهان. به خلاف فرض کنید که $(۱) = \tau_k \cdots \tau_۲\tau_۱$ که در آن هر τ_i یک ترانهش و k فرد است. فرض کنید c عددی باشد که حداقل در یکی از این ترانهش‌ها ظاهر شده‌است. فرض کنید τ_r اولین ترانهش (از راست به چپ) باشد که در آن c ظاهر می‌شود، مثلاً $\tau_r = (cd)$. در این صورت c در $\tau_۱$، $\tau_۲$، ...، $\tau_{r-۱}$ ظاهر نمی‌شود و بنابراین توسط این ترانهش‌ها ثابت نگه داشته می‌شود. اگر $r = k$، در این صورت c توسط همهٔ τها بجز τ_k ثابت نگه‌داشته می‌شود، پس این حاصل‌ضرب، یعنی جایگشت همانی، c را به d می‌نگارد که یک تناقض است. بنابراین $r < k$ و ما می‌توانیم ترانهش $\tau_{r+۱}$ را در نظر بگیریم. این ترانهش باید به یکی از صورتهای زیر باشد (که در آن x، y، c و d عناصر متمایزی از $\{۱, ۲, \ldots, n\}$ را نشان می‌دهد):

I. (xy) II. (xd) III. (cy) IV. (cd)

در نتیجه چهار امکان برای حاصل‌ضرب $\tau_{r+۱}\tau_r$ وجود دارد:

I. $(xy)(cd)$ II. $(xd)(cd)$ III.$(cy)(cd)$ IV. $(cd)(cd)$

در حالت I، بررسی کنید که $(xy)(cd) = (cd)(xy)$. حال $(cd)(xy)$ را جایگزین $(xy)(cd)$ کنید؛ این کار اولین محل ظهور c را در حاصل‌ضرب یکی به سمت چپ انتقال می‌دهد. در حالت II، بررسی کنید که $(xd)(cd) = (xc)(xd)$؛ اگر $(xc)(xd)$ را جایگزین $(xd)(cd)$ کنیم، در این صورت مجدداً محل ظهور c یکی بیشتر به سمت چپ انتقال می‌یابد. با بررسی این که $(cy)(cd) = (cd)(dy)$ نشان دهید که در حالت III نیز نتیجه‌گیری مشابهی برقرار است.

هر بار که روند انجام شده در حالتهای I-III تکرار شود، اولین ظهور c را یکی بیشتر به سمت چپ انتقال می‌دهد. سرانجام در مرحله‌ای IV باید رخ دهد زیرا در غیراینصورت می‌توانیم آن را آنقدر

حرکت دهیم تا زمانی‌که اولین محل ظهور c آخرین جایگشت سمت چپ یعنی τ_k باشد که همانگونه که‌در بند اول برهان دیدیم غیرممکن است، امّا در حالت IV داریم $\tau_r\tau_{r+1} = (cd)(cd) = (1)$. بنابراین می‌توانیم با حذف این دو ترانهش، (۱) را به‌عنوان حاصل‌ضربی از ترانهش‌هایی که تعدادشان دو تا کمتر از قبل هستند بنویسیم. به‌وضوح می‌توانیم همین استدلال را برای هر عددی که در یکی از ترانهش‌های موجود در حاصل‌ضرب ظاهر می‌شود انجام دهیم. اگر حاصل‌ضرب اصلی تعداد فردی از ترانهش‌ها را شامل باشد، با حذف دو تا از آنها در هر مرحله، سرانجام حاصل به یک تک ترانهش $(ab) = (1)$ کاهش می‌یابد که یک تناقض است. بنابراین (۱) نمی‌تواند به صورت حاصل‌ضرب تعداد فردی از ترانهش‌ها نوشته شود. ■

قضیه ۴۷.۷. هیچ جایگشتی در S_n هم فرد و هم زوج نیست.

برهان. فرض کنید $\alpha \in S_n$ را بتوان به دو صورت $\sigma_1\sigma_2\cdots\sigma_k$ و $\tau_1\tau_2\cdots\tau_r$ نوشت که در آن هر σ_i، τ_j ترانهش بوده، k فرد و r زوج است. مانند اثبات قضیه ۴۵.۷، داریم

$$\begin{aligned}(1) = \alpha\alpha^{-1} &= (\sigma_1\cdots\sigma_k)(\tau_1\cdots\tau_r)^{-1}\\ &= \sigma_1\cdots\sigma_k\tau_r^{-1}\cdots\tau_1^{-1}\\ &= \sigma_1\cdots\sigma_k\tau_r\cdots\tau_1.\end{aligned}$$

چون k فرد و r زوج است، $k+r$ فرد و (۱) به صورت حاصل‌ضربی از تعداد فردی از ترانهش‌ها نوشته شده‌است. این موضوع لم ۴۶.۷ را نقض می‌کند و بنابراین α نمی‌تواند هم زوج و هم فرد باشد. ■

اکنون می‌توانیم مرتبه A_n را تعیین کنیم ضمن این که در روند کار، اثبات دیگری برای این که A_n زیرگروه نرمالی از S_n است ارائه می‌کنیم؛ برای اثباتی مقدماتی‌تر، تمرین ۲۶ را ملاحظه کنید.

قضیه ۴۸.۷. A_n زیرگروه نرمالی با مرتبهٔ $n!/2$ و شاخص ۲ در S_n است.

برهان. تابع $f : S_n \to \mathbb{Z}_2$ را توسط $f(\sigma) = 0$ اگر σ زوج باشد و $f(\sigma) = 1$ اگر σ فرد باشد تعریف کنید. چون هیچ جایگشتی هم‌زوج و هم فرد نیست، f خوش‌تعریف است. به سادگی می‌توان دید که حاصل‌ضرب هر دو جایگشت زوج یا هر دو جایگشت فرد، زوج است و این که حاصل‌ضرب یک جایگشت فرد و یک جایگشت زوج، فرد است. با استفاده از این حقایق بررسی

کنید که f یک همریختی گروهی پوشا با هسته A_n است. بنابراین طبق قضیه ۲۶.۷، A_n یک زیرگروه نرمال است و نتیجه ۳۴.۷ نشان می‌دهد که A_n دارای شاخص ۲ در S_n است و دارای مرتبه $|S_n|/2 = n!/2$ می‌باشد. ■

تمرینها

۱.A. هر جایگشت را با نماد دوری بنویسید:

(الف) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\7&2&1&4&5&6&3&8&9\end{pmatrix}$ (ب) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&4&3&5&7&6&8&9&1\end{pmatrix}$

(پ) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&8&1&7&5&2&6&3&9\end{pmatrix}$ (ت) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&2&5&4&7&6&9&3&8\end{pmatrix}$

۲. هر یک از این حاصل‌ضرب‌ها را محاسبه کنید:

(الف) (۱۲)(۲۳)(۳۴) (ب) (۲۴۶)(۱۴۷)(۱۳۵)

(پ) (۲۳)(۵۳۲۱۴)(۱۲) (ت) (۱۲۳۴)(۲۳۴۵)

۳. هر یک را به صورت حاصل‌ضربی از دورهای مجزا بیان کنید:

(الف) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&1&3&5&4&7&9&8&6\end{pmatrix}$ (ب) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&5&1&2&4&6&8&9&7\end{pmatrix}$

(پ) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&5&1&2&4&9&8&7&6\end{pmatrix}$ (ت) (۱۴)(۲۷)(۵۲۳)(۳۴)(۱۴۷۲)

(ث) (۷۲۳۶)(۸۵)(۵۷۱)(۱۵۳۷)(۴۸۶)

۴. هرکدام از جایگشتهای تمرین ۳ را به صورت حاصل‌ضربی از ترانهش‌ها بنویسید.

۵. کدام یک از این جایگشتها زوج هستند:

(الف) (۲۴۶۸) (ب) (۲۴۶)(۱۳۴) (پ) (۱۲)(۱۲۳)(۱۲۳۴)

۶. عناصر هر گروه را فهرست کنید:

(الف) A_2 (ب) A_3 (پ) A_4

۷. مرتبه هر یک از گروههای زیر را تعیین کنید:

(الف) $A_۳$ (ب) $A_۴$ (پ) $A_۵$ (ت) $A_{۱۰}$

۸. فرض کنید $\sigma = (a_۱a_۲a_۳a_۴a_۵a_۶)$. σ^i را برای $i = ۱, ۲, \ldots, ۶$ بیابید.

۹.B. ثابت کنید که یک $k-$دور در گروه S_n دارای مرتبهٔ k است.

۱۰. نشان دهید که در S_n وارون $(a_۱a_۲\cdots a_k)$ دور $(a_۱a_k a_{k-۱}\cdots a_۳a_۲)$ است.

۱۱. ثابت کنید که دور $(a_۱a_۲\cdots a_k)$ زوج است اگر و تنها اگر k فرد باشد.

۱۲. فرض کنید $\sigma = (a_۱a_۲\cdots a_k)$ و $\tau = (b_۱b_۲\cdots b_r)$ دورهای مجزایی در S_n باشند. ثابت کنید که $\sigma\tau = \tau\sigma$. [راهنمایی: باید نشان دهید که $\sigma\tau$ و $\tau\sigma$ روی هر i در $\{۱, ۲, \cdots n\}$ یکسان عمل می‌کنند. این سه حالت را در نظر بگیرید: i یکی از a_jها است؛ i یکی از b_jها است؛ i نه از a_jها و نه از b_jها است.]

۱۳. اگر $\tau \in S_n$، ثابت کنید که مرتبه τ برابر کوچکترین مضرب مشترک طول دورهای مجزایی است که حاصلضرب آنها برابر τ است. [راهنمایی: تمرینهای ۹ و ۱۲ می‌تواند مفید باشد.]

۱۴. اگر σ جایگشت $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۳ & ۷ & ۸ & ۹ & ۴ & ۵ & ۲ & ۱ & ۶ \end{pmatrix}$ باشد، مرتبه $\sigma^{۱۰۰۰}$ را بیابید.

۱۵. نشان دهید که زیرگروه G از $S_۴$ تولیدشده به وسیله $\sigma = (۱۴۳۲)$ و $\tau = (۲۴)$ یکریخت با $D_۴$ است.

۱۶. ثابت کنید که مرکز $S_n (n > ۲)$ زیرگروه همانی است.

۱۷. اگر σ یک $k-$دور باشد که در آن k فرد است، ثابت کنید که یک دور τ وجود دارد به قسمی که $\tau^۲ = \sigma$.

۱۸. فرض کنید σ یک $k-$دور در S_n باشد.

(الف) ثابت کنید که $\sigma^۲$ یک دور است اگر و تنها اگر k فرد باشد.

(ب) اگر $k = ۲t$، ثابت کنید که $t-$دورهای τ و β وجود دارند به قسمی که $\sigma^۲ = \tau\beta$.

۱۹. فرض کنید σ حاصلضربی از دورهای مجزای با طول یکسان باشد. ثابت کنید که σ توانی از یک دور است.

۲۰. ثابت کنید که تجزیه یک جایگشت به دورهای مجزا، بجز در ترتیب نوشتن دورها، یکتاست.

۲۱. با استفاده از استقراء روی n اثبات دیگری از نتیجه ۴۴.۷ ارائه کنید: هر عضو S_n حاصلضربی از ترانهشها است. [راهنمایی: اگر گزاره برای $n = k - ۱$ درست باشد و اگر $\tau \in S_k$، ترانهش (kr) را که در آن $r = \tau(k)$ در نظر بگیرید. توجه کنید که $(kr)\tau$، k را ثابت نگه میدارد و بنابراین میتوان آن را به عنوان جایگشتی از $\{۱, ۲, \ldots, k-۱\}$ در نظر گرفت.]

۲۲. اگر $n \geq ۳$ ؛ ثابت کنید که هر عضو S_n حاصلضربی از حداکثر $n - ۱$ ترانهش است.

۲۳. فرض کنید τ یک ترانهش باشد و $\sigma \in S_n$، ثابت کنید که $\sigma\tau\sigma^{-۱}$ یک ترانهش است.

۲۴. فرض کنید τ، k-دور $(a_۱a_۲\cdots a_k)$ باشد و فرض کنید $\sigma \in S_n$. ثابت کنید که $\sigma\tau\sigma^{-۱} = (\sigma(a_۱)\sigma(a_۲)\cdots\sigma(a_k))$.

۲۵. فرض کنید G یک زیرگروه S_n باشد که حداقل یک جایگشت فرد را شامل است. ثابت کنید که تعداد جایگشتهای زوج در G برابر تعداد جایگشتهای فرد در G است (یعنی $G \cap A_n$ یک زیرگروه با شاخص ۲ در G است).

۲۶. بدون استفاده از قضیه ۴۸.۷ ثابت کنید که A_n دارای شاخص ۲ در S_n است. [راهنمایی: نشان دهید که A_n و $A_n(۱۲)$ هممجموعههای متمایزی هستند که اجتماع آنها برابر S_n است.]

۲۷. ثابت کنید که $\{(۱), (۱۲)(۳۴), (۱۳)(۲۴), (۱۴)(۲۳)\}$ یک زیرگروه نرمال $A_۴$ است.

۲۸. ثابت کنید $A_۴$ یک گروه از مرتبه ۱۲ است که دارای هیچ زیرگروهی از مرتبه ۶ نیست. نتیجه بگیرید که عکس قضیه لاگرانژ غلط است.

۲۹. فرض کنید σ و τ ترانهشهایی در S_n باشند با $n \geq ۳$. ثابت کنید که $\sigma\tau$ حاصلضربی از ۳-دورها (که لزوماً متمایز نیستند) میباشد.

۳۰. ثابت کنید که هر عضو A_n حاصلضربی از ۳-دورهاست.

۳۱.C. ثابت کنید که هر عضو A_n حاصلضربی از n-دورهاست.

۳۲. ثابت کنید که ترانهشهای $(۱n), \ldots, (۱۴), (۱۳), (۱۲)$، S_n را تولید میکنند.

۳۳. ثابت کنید که (۱۲) و $(۱۲۳\cdots n)$، S_n را تولید میکنند.

۳۴. اگر f یک خودریختی از $S_۳$ باشد، ثابت کنید که $\sigma \in S_۳$ وجود دارد به قسمی که برای هر $\tau \in S_۳$، $f(\tau) = \sigma\tau\sigma^{-۱}$.

۳۵. با استفاده از مراحل زیر قضیه ۴۳.۷ را اثبات کنید: هر جایگشت τ در S_n حاصل‌ضربی از دورهای مجزاست.

(الف) فرض کنید $a_۱$ عضوی دلخواه از $\{۱, ۲, \ldots, n\}$ باشد به قسمی که $\tau(a_۱) \neq a_۱$. فرض کنید $a_۲ = \tau(a_۱)$، $a_۳ = \tau(a_۲)$، $a_۴ = \tau(a_۳)$ و غیره. فرض کنید k اولین نمایه‌ای باشد به قسمی که $\tau(a_k)$ یکی از $a_۱, \ldots, a_{k-۱}$ است. ثابت کنید $\tau(a_k) = a_۱$. نتیجه بگیرید که اثر τ روی $a_۱$، ...، a_k با اثر دور $(a_۱a_۲\cdots a_k)$ یکسان است.

(ب) فرض کنید $b_۱$ عضوی دلخواه از $\{۱, ۲, \ldots, n\}$ به غیر از $a_۱, \ldots, a_k$ باشد که توسط τ به خودش نگاشته نشده باشد. فرض کنید $b_۲ = \tau(b_۱)$، $b_۳ = \tau(b_۲)$ و غیره. نشان دهید که $\tau(b_i)$ هرگز یکی از $a_۱$، ...، a_k نیست. استدلال قسمت (الف) را تکرار کنید تا یک عضو b_r را بیابید به قسمی که $\tau(b_r) = b_۱$ و اثر τ و دور $(b_۱b_۲\cdots b_r)$ روی b_jها یکسان باشد.

(پ) فرض کنید $c_۱$ عضوی دلخواه از $\{۱, ۲, \ldots, n\}$ به غیراز a_jها و b_jهای بالا باشد به قسمی که $\tau(c_۱) \neq c_۱$. فرض کنید $c_۲ = \tau(c_۱)$ و غیره. همانند بالا c_s را چنان بیابید که اثر τ و دور $(c_۱c_۲\cdots c_s)$ روی c_jها یکسان باشد.

(ت) این فرآیند را ادامه دهید تا جایی که تنها عناصر به حساب نیامده آنهایی باشند که تحت τ به خودشان نگاشته می‌شوند. بررسی کنید که τ حاصل‌ضربی از دورهای

$$(a_۱\cdots a_k)(b_۱\cdots b_r)(c_۱\cdots c_s)\ldots$$

می‌باشد و این که این دورها مجزا هستند.

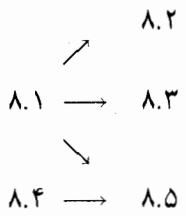
* * * * *

فصل هشتم

حساب در دامنه‌های صحیح

در این فصل دامنه‌های صحیحی را در نظر می‌گیریم که خواص حسابی آنها مشابه $\mathbb{Z}$ است. بویژه خاصیت یکتایی تجزیه مد نظر است.

در واقع، در یک دامنه صحیح، یکتایی تجزیه عناصر، رابطه نزدیکی با ایده‌آلهای آن دارد. از یک طرف، یکتایی تجزیه بدون این که ایده‌آل‌های اصلی دامنه صحیح در برخی شرایط صدق کنند امکان‌پذیر نیست، و از طرف دیگر، با استفاده از ایده‌آل‌ها می‌توان شکلی از یکتایی تجزیه را که برخی دامنه‌های صحیح فاقد آن هستند، به آنها بازگرداند. در واقع، همانگونه که در بخش ۳.۸ خواهیم دید، ایده‌آل‌ها در اصل بدین‌منظور ابداع شده‌اند. وابستگی بخش‌های این فصل به شرح زیر است:



بخش ۴.۸ (میدان خارج قسمتهای یک دامنه‌صحیح) مستقل از دیگر بخش‌های این فصل است و می‌توان آن را هر زمانی مطالعه کرد. بجز بخش ۲.۸ و قسمت پایانی بخش ۳.۸ که به فصل ۶ وابستگی دارند، بقیه این فصل را می‌توان پس از فصل ۴ مطالعه کرد.

۸-۱ دامنه‌های یکتایی تجزیه

ابتدا مفاهیم اصلی حساب و اصطلاحات علمی آن را از حلقه‌های $\mathbb{Z}$ و $\mathbb{F}[x]$ به حلقه‌های دامنه صحیح دلخواه انتقال می‌دهیم. سپس به بررسی آن دامنه‌های صحیحی می‌پردازیم که در آنها شکلی از یکتایی تجزیه موجود است. در سرتاسر این بخش R یک دامنه صحیح است.

فرض کنید $\mathbb{Z}[\sqrt{d}] = \{r + s\sqrt{d} \mid r, s \in \mathbb{Z}\}$، که در آن d یک عدد صحیح ثابت است. از این دسته از حلقه‌ها، اغلب در ارائه مثال استفاده می‌شود. بررسی این که $\mathbb{Z}[\sqrt{d}]$ یک دامنه صحیح است که در مجموعهٔ اعداد مختلط $\mathbb{C}$ قرار دارد چندان مشکل نیست؛ اگر $d > 0$، در این صورت $\mathbb{Z}[\sqrt{d}]$ یک زیرحلقه اعداد حقیقی است (تمرین ۱). وقتی $d = -1$، $\mathbb{Z}[\sqrt{-1}]$ را اغلب با $\mathbb{Z}[i]$ نشان می‌دهند، و آن را **حلقه اعداد صحیح گوسی** نامند[۱].

فرض کنید $a, b \in R$ و $a \neq 0$. گوییم a یک **شمارندهٔ** b است (یا a یک **عامل** b است) و می‌نویسیم $a|b$ هرگاه برای برخی $c \in R$، $b = ac$. به خاطر آورید که عنصر u در R **یکه** است هرگاه برای برخی $v \in R$، $uv = 1_R$. بنابراین یکه‌های R همان شمارنده‌های 1_R هستند.

مثال ۱.۸. تنها یکه‌های $\mathbb{Z}$، ۱ و -1 هستند. اگر $\mathbb{F}$ یک میدان باشد، یکه‌های حلقه چندجمله‌ای‌های $\mathbb{F}[x]$، چندجمله‌ای‌های ثابت‌اند (قضیه ۷.۴). عضو $\sqrt{2} + 1$ در $\mathbb{Z}[\sqrt{2}]$ یکه است زیرا $(\sqrt{2} + 1)(\sqrt{2} - 1) = 1$.

---

۱) Ring of Gaussian integers

تذکر. فرض کنید $u \in R$ یک یکه با وارون v باشد، لذا $uv = 1_R$. برای هر $b \in R$، داریم $u(vb) = (uv)b = 1_R b = b$. بنابراین

یک عضو یکه، هر عضو R را می‌شمارد.

یک عضو $a \in R$ یک **وابسته** $b \in R$ است هرگاه برای برخی یکه u، $a = bu$. حال u دارای یک وارون است، مثلاً $uv = 1_R$، و v نیز یک یکه است. ضرب دو طرف $a = bu$ در v نشان می‌دهد که $av = buv = b1_R = b$. با استفاده از این حقایق بررسی کنید که

هر عضو غیر صفر R بر هر یک از وابسته‌های خود بخش‌پذیر است.

مثال ۲.۸. هر عدد صحیح غیرصفر n دارای دقیقاً دو وابسته n و $-n$ در $\mathbb{Z}$ است. اگر $\mathbb{F}$ یک میدان باشد، وابسته‌های $f(x) \in \mathbb{F}[x]$، مضربهای ثابت $f(x)$ می‌باشند. در حلقه $\mathbb{Z}[\sqrt{2}]$، دو عنصر $\sqrt{2}$ و $\sqrt{2} - 2$ وابسته‌اند زیرا $(\sqrt{2} + 1)(\sqrt{2} - 2) = \sqrt{2}$ و $\sqrt{2} + 1$ یکه است.

یک عضو غیرصفر $p \in R$ را **تحویل‌ناپذیر** گویند هرگاه p یکه نباشد و تنها شمارنده‌های p وابسته‌های آن و یکه‌های در R باشند.

مثال ۳.۸. تنها عناصر تحویل‌ناپذیر $\mathbb{Z}$ اعداد اول هستند زیرا تنها شمارنده‌های یک عدد اول p عبارتند از $\pm p$ (وابسته‌های آن) و ± 1 (یکه‌های $\mathbb{Z}$). وقتی که $\mathbb{F}$ یک میدان باشد، تعریف تحویل‌ناپذیری بالا با تعریف تحویل‌ناپذیری چندجمله‌ایها در دامنه صحیح $\mathbb{F}[x]$ معادل است (تعریف بعد از قضیه ۷.۴). در بخش ۳.۸ خواهید دید که $i + 1$ در حلقه $\mathbb{Z}[i]$ تحویل‌ناپذیر است.

قضیه بعدی معمولاً ساده‌ترین راه برای اثبات تحویل‌ناپذیری یک عنصر را به دست می‌دهد و بعضاً به عنوان تعریف تحویل‌ناپذیری بکار برده می‌شود. قضیه ۸.۴ حالت خاص قضیه زیر است، وقتی که $R = \mathbb{F}[x]$.

قضیه ۱.۸. فرض کنید p یک عضو غیر یکه غیرصفر در یک دامنه صحیح R باشد. در این صورت p تحویل‌ناپذیر است اگر و تنها اگر

هرگاه $p = rs$، آنگاه r یا s یکه باشند.

برهان. اگر p تحویل‌ناپذیر باشد و $p = rs$، در این صورت r یک شمارندهٔ p است. بنابراین r باید یا یک یکه یا یک وابسته p باشد. اگر r یکه باشد، چیزی برای اثبات وجود ندارد. اگر r یک

وابسته p باشد، مثلاً $r = pv$، در این صورت $p = rs = pvs$. حذف p از دو طرف (قضیه ۷.۳) نشان می‌دهد که $vs = 1_R$. بنابراین s یک یکه است.

برای اثبات طرف عکس، فرض کنید p دارای خاصیت بیان شده‌باشد. فرض کنید c یک شمارنده p باشد، مثلاً $p = cd$. در این صورت طبق فرض یا c یا d یکه است. اگر d یکه باشد آنگاه d^{-1} نیز یکه است. ضرب دو طرف $p = cd$ در d^{-1} نشان می‌دهد که $c = d^{-1}p$. بنابراین در هر حالت یا c یکه است و یا یک وابسته p است. پس p تحویل‌ناپذیر است. ■

اعداد صحیح توسط رابطه $\leq$ مرتب شده‌اند و چندجمله‌ایها توسط درجه خود، جزئاً مرتب شده‌اند. از اینرو *طبیعی* بنظر می‌رسد که بزرگترین مقسوم علیه مشترک عناصر در $\mathbb{Z}$ و $\mathbb{F}[x]$ را برحسب اندازه یا درجه تعریف کنیم. متأسفانه ممکن است هیچ روش مشابهی برای تعیین "اندازه" در یک دامنه صحیح دلخواه وجود نداشته باشد، بنابراین بزرگترین مقسوم علیه مشترک عناصر بایستی تنها برحسب خواص بخش‌پذیری تعریف شود:

تعریف. فرض کنید a_1، a_2، ...، a_n عناصری (که هیچ‌کدام صفر نیستند) از یک دامنه صحیح R باشند. یک **بزرگترین مقسوم علیه مشترک** a_1، a_2، ...، a_n یک عنصر d از R است به قسمی که

(i) d هر یک از a_iها را بشمارد؛

(ii) اگر $c \in R$ و c هر یک از a_iها را بشمارد، آنگاه $c|d$.

این تعریف با آنچه که در مورد $\mathbb{Z}$ و $\mathbb{F}[x]$ انجام شد سازگاری دارد امّا معادل تعاریف قبلی ما از ب‌م‌م نیست. اگر d ب‌م‌م اعداد صحیح a_1 و a_2 بر طبق تعریف فصل ۱ باشد (یعنی، d بزرگترین مقسوم علیه مشترک باشد) در این صورت طبق نتیجه ۴.۱، d دارای خواص (i) و (ii) این تعریف است. به طور مشابه اگر $\mathbb{F}$ یک میدان باشد، در این صورت طبق نتیجه ۵.۴، ب‌م‌م دو چندجمله‌ای در $\mathbb{F}[x]$ (مطابق تعریف فصل ۴) دارای خواص (i) و (ii) است. تفاوت در تعریف جدید این است که دیگر ب‌م‌م لزوماً یکتا نیست.

مثال ۴.۸. بر طبق این تعریف، هر دو عدد ۲ و ۲− بزرگترین مقسوم‌علیه مشترک ۱۰ و ۱۸ در $\mathbb{Z}$ هستند. توجه کنید که ۲ و ۲− وابسته‌اند.

قضیه ۲.۸. فرض کنید d یک بزرگترین مقسوم‌علیه مشترک a_1، a_2، ...، a_n در دامنه صحیح R باشد. در این صورت

(۱) هر وابسته d یک ب‌م‌م a_1، a_2، ...، a_n نیز هست.

(۲) هر دو بزرگترین مقسوم‌علیه مشترک a_1، a_2، ...، a_n وابسته‌اند.

برهان. (۱) تمرین ۹.

(۲) فرض کنید هر دو عنصر d و t ب‌م‌م‌های a_1، a_2، ...، a_n باشند. در این صورت t تمام a_iها را می‌شمارد، بنابراین طبق قسمت (ii) تعریف بزرگترین مقسوم‌علیه مشترک برای d، داریم $t|d$. امّا d نیز تمام a_iها را می‌شمارد و بنابراین طبق (ii) تعریف ب‌م‌م برای t، $d|t$. چون $t|d$ و $d|t$، طبق تمرین ۴ می‌دانیم که d و t وابسته‌اند. ■

هشدار در برخی از دامنه‌های صحیح، یک مجموعه متناهی از عناصر ممکن است دارای هیچ بزرگترین مقسوم‌علیه مشترک نباشد (تمرین ۱۳ بخش ۳.۸ را ملاحظه کنید).

یکتایی تجزیه در $\mathbb{Z}$ و $\mathbb{F}[x]$ رابطه تنگاتنگی با خواص تحویل‌ناپذیری، وجود بزرگترین مقسوم‌علیه‌های مشترک و حقایق مختلف درباره بخش‌پذیری دارد. بنابراین نخستین نامزدهای حلقه‌های دامنه صحیحی که واجد این خواص "خوب" $\mathbb{Z}$ و $\mathbb{F}[x]$ هستند، دامنه‌های صحیحی هستند که در آنها یکتایی تجزیه به مفهوم زیر برقرار باشد:

تعریف. دامنه صحیح R یک **دامنه یکتایی تجزیه (دی‌ت)** است به شرطی که هر عضو غیرصفر غیریکه در R حاصل‌ضربی از عناصر تحویل‌ناپذیر [۲] بوده و این تجزیه تا حد وابسته‌ها یکتا باشد، یعنی اگر

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

که در آن هر p_i و q_j تحویل‌ناپذیر است، در این صورت $r = s$ و در صورت لزوم پس از تغییر ترتیب و تغییر نمایه‌ها

$$p_i \text{ یک وابسته } q_i \text{ باشد} \qquad (\text{برای } i = 1, 2, \dots, r).$$

مثال ۵.۸. قضایای ۱۱.۱ و ۱۰.۴ نشان می‌دهند که $\mathbb{Z}$ و $\mathbb{F}[x]$ (که در آن $\mathbb{F}$ یک میدان است) دامنه‌های یکتایی تجزیه هستند. در بخش ۲.۸ خواهیم دید که دامنه اعداد صحیح گوسی $\mathbb{Z}[i]$ نیز

۲) در صورتی که یک عنصر خودش تحویل‌ناپذیر باشد، ما امکان حاصل‌ضربهایی با تنها یک عامل را می‌پذیریم.

یک **دی‌ت** است. با این‌حال همانگونه که در بخش ۳.۸ خواهیم دید بسیاری از دامنه‌های $\mathbb{Z}[\sqrt{d}]$ **دی‌ت** نیستند. اثباتی برای **دی‌ت** بودن $\mathbb{Z}[x]$ در بخش ۵.۸ ارائه شده است.

در $\mathbb{Z}$ همواره می‌توان تجزیه دو عنصر را به صورتی نوشت که در هر دو توانهای یکسانی ظاهر شوند؛ برای مثال، $-۱۸ = (-۱)۲^۱ \times ۳^۲ \times ۵^۰$ و $۴۰ = ۲^۳ \times ۵$ را می‌توان به صورت $-۱۸ = (-۱)(-۲)(-۳)^۲$ و $۴۰ = (۱)۲^۳ \cdot ۳^۰ \cdot ۵^۱$ نوشت. این مطلب در هر **دی‌ت** صحیح است.

قضیه ۳.۸. اگر c و d عناصر غیرصفری در یک دامنه یکتایی تجزیه R باشند، در این صورت یکه‌های u و v و تحویل‌ناپذیرهای $p_۱$، $p_۲$، ...، p_k که هیچ دوتای آنها وابسته نیستند وجود دارند به قسمی که

$$c = up_۱^{m_۱}p_۲^{m_۲}\dots p_k^{m_k} \quad \text{و} \quad d = vp_۱^{n_۱}p_۲^{n_۲}\dots p_k^{n_k}$$

که در آن هر m_i و n_i یک عدد صحیح نامنفی می‌باشد. به‌علاوه

$c|d$ اگر و تنها اگر برای هر $i = ۱, ۲, \dots, k$، $m_i \le n_i$.

برهان. اولاً اگر عناصر $q_۲$ و $q_۳$ وابسته‌های یک عنصر $q_۱$ باشند، در این صورت یکه‌های $u_۲$ و $u_۳$ وجود دارند به قسمی که $q_۲ = u_۲q_۱$ و $q_۳ = u_۳q_۱$. بنابراین حاصل ضرب $q_۱q_۲q_۳$ می‌تواند به صورت $q_۱^۳(u_۲u_۳)$ نوشته شود. ثانیاً حاصل‌ضرب یکه‌ها یک یکه است (تمرین ۷ بخش ۲.۳). بنابراین $q_۱q_۲q_۳ = uq_۱^۳$ که در آن u یک یکه است. ثالثاً برای هر عنصر غیرصفر q، $q^۰ = ۱_R$. بنابراین برای هر دو عنصر غیرصفر R مثل $q_۴$ و $q_۵$، داریم $q_۱q_۲q_۳ = uq_۱^۳q_۴^۰q_۵^۰$. این سه حقیقت را بکار برید تا همه وابسته‌های تحویل‌ناپذیر c و d را دسته‌بندی کرده، یکه‌های مختلف را ترکیب نموده و سپس اولین گزاره قضیه را ثابت نمایید.

برای اثبات آخرین گزاره، توجه کنید که $c|d$ بدین معنی است که $ct = d$. چون تحویل‌ناپذیر p_i دقیقاً n_i بار در تجزیه d ظاهر می‌شود، لذا باید دقیقاً n_i بار نیز در تجزیه ct ظاهر شود. امّا p_i قبلاً m_i بار در تجزیه c ظاهر شده‌است و بنابراین باید داشته باشیم $m_i \le n_i$. ■

هر عنصر یک دامنه صحیح بر همه وابسته‌هایش بخش‌پذیر است. گوییم b یک **شمارنده سره** a است اگر $b|a$ و b یک وابسته a نباشد. بنابراین p تحویل‌ناپذیر است اگر و تنها اگر، تنها شمارنده‌های سره آن یکه‌ها باشند. روش معمول برای بیان یک عنصر به صورت حاصل‌ضربی از تحویل‌ناپذیرها این است که آن را به طور مکرر توسط شمارنده‌های سره غیر یکه آن فاکتورگیری کرده تا زمانی که به جایی برسیم که هر عامل یا یکه و یا تحویل‌ناپذیر باشد. این روش در صورتی مؤثر خواهد بود که

هیچ عنصری دارای دنباله‌ای نامتناهی از شمارنده‌های سره نباشد چرا که در غیر این صورت فرآیند فاکتورگیری برای همیشه ادامه پیدا می‌کند. خوشبختانه این چیزی است که در یک **دی‌ت** اتفاق می‌افتد:

نتیجه ۴.۸. در یک دامنه یکتایی تجزیه R، هیچ دنباله نامتناهی a_1، a_2، a_3، ... وجود ندارد به قسمی که هر $a_i (i > 1)$ یک شمارنده سره عنصر قبلی باشد.

برهان. فرض کنید که یک چنین دنباله‌ای موجود باشد. چون R یک **دی‌ت** است، داریم $a_1 = vp_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$، که در آن v یکه است و p_iها تحویل‌ناپذیرند و هیچ دوتای آنها وابسته نیستند. هر $a_i (i > 1)$ یک شمارنده a_1 است و بنابراین طبق قضیه ۳.۸، به صورت $up_1^{m_1}p_2^{m_2}\dots p_k^{m_k}$ می‌باشد که در آن u یکه و برای هر j، $0 \leq m_j \leq n_j$. بررسی کنید که a_{i+1} یک شمارنده سره a_i است اگر و تنها اگر هر یک از نماهای m_j که در a_{i+1} ظاهر می‌شود، کوچکتر یا مساوی نمای نظیر در a_i بوده و حداقل یکی از آنها اکیداً کوچکتر باشد. پس از تعداد متناهی مرحله باید یک a_t به صورت $a_t = up_1^{*}p_2^{*}\dots p_k^{*} = u$ موجود باشد. بنابراین a_t یکه است و لذا دارای هیچ شمارنده سره‌ای نیست (تمرین ۱۳). ولی این با این حقیقت که a_{t+1} یک شمارنده سره a_t است در تناقض می‌باشد. ■

به منظور درک کامل مفهوم نتیجه ۴.۸، در نظرگرفتن دامنه صحیحی که در آن این نتیجه غلط است می‌تواند سازنده باشد.

مثال ۶.۸. فرض کنید $\mathbb{Q}_{\mathbb{Z}}[x]$ زیردامنه‌ای از $\mathbb{Q}[x]$ را نشان دهد که متشکل از همه چندجمله‌ای‌هایی باشد که جمله ثابت آنها یک عدد صحیح است. در این صورت تنها یکه‌های $\mathbb{Q}_{\mathbb{Z}}[x]$ عبارتند از ± 1 (تمرین ۲۸) و هر عدد صحیح اول (اگر به عنوان یک چندجمله‌ای ثابت در نظرگرفته شود) در $\mathbb{Q}_{\mathbb{Z}}[x]$ تحویل‌ناپذیر است (تمرین ۲۹). بنابراین هر عنصر در دنباله نامتناهی $x, \frac{1}{2}x, \frac{1}{4}x, \frac{1}{8}x, \dots, \frac{1}{2^n}x, \dots$ یک شمارنده سره از عنصر قبل از خود می‌باشد. برای نمونه، $x = 2(\frac{1}{2}x)$، $(\frac{1}{2}x) = 2(\frac{1}{4}x)$، و غیره. بنابراین $\mathbb{Q}_{\mathbb{Z}}[x]$ یک **دی‌ت** نیست.

نتیجه ۵.۸. فرض کنید a_1، a_2، ...، a_n (که بعضی از آنها غیرصفرند) عناصری در یک دامنه یکتایی تجزیه R باشند. در این صورت a_1، a_2، ...، a_n دارای یک بزرگترین مقسوم‌علیه مشترک

در R هستند.

برهان. ب‌م‌م هر مجموعه از عناصر عبارت از ب‌م‌م اعضای غیرصفر این مجموعه است، بنابراین می‌توانیم فرض کنیم که هر a_i غیرصفر است. طبق قضیه ۳.۸، عناصر تحویل‌ناپذیر p_1، p_2، ...، p_t (که هیچ دوتای آنها وابسته نیستند)، یکه‌های u_1، ...، u_n و اعداد صحیح غیرمنفی m_{ij} وجود دارند به قسمی که

$$\begin{aligned} a_1 &= u_1 p_1^{m_{11}} p_2^{m_{12}} \dots p_t^{m_{1t}} \\ a_2 &= u_2 p_1^{m_{21}} p_2^{m_{22}} \dots p_t^{m_{2t}} \\ &\vdots \\ a_n &= u_n p_1^{m_{n1}} p_2^{m_{n2}} \dots p_t^{m_{nt}}. \end{aligned}$$

فرض کنید k_1 کوچکترین نمایی باشد که برای p_1 ظاهر می‌شود؛ یعنی k_1 مینیمم m_{11}، m_{21}، m_{31}، ...، m_{n1} باشد. به طور مشابه فرض کنید k_2 کوچکترین نمایی باشد که برای p_2 ظاهر می‌شود و غیره. با استفاده از قضیه ۳.۸ بررسی کنید که $d = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ یک ب‌م‌م a_1، ...، a_n است. ■

هشدار برخلاف $\mathbb{Z}$ و $\mathbb{F}[x]$، ممکن است در یک دی‌ت دلخواه نوشتن ب‌م‌م عناصر a و b به صورت یک ترکیب خطی از a و b امکان‌پذیر نباشد (برای مثال تمرین ۲۵ را ملاحظه کنید).

سرانجام توجه می‌کنیم که عناصر تحویل‌ناپذیر در یک دامنه یکتایی تجزیه R دارای خاصیتی هستند که ما به دفعات در حالات خاص $R = \mathbb{Z}$ و $R = \mathbb{F}[x]$ از آن استفاده کرده‌ایم:

قضیه ۶.۸. فرض کنید p یک عنصر تحویل‌ناپذیر در یک دامنه یکتایی تجزیه R باشد. اگر $p|bc$ در این صورت $p|b$ یا $p|c$.

برهان. اگر b یا c، عنصر 0_R باشد در این صورت چیزی برای اثبات باقی نمی‌ماند زیرا $p|0_R$. اگر c یکه باشد و $p|bc$، در این صورت برای برخی $t \in R$، $pt = bc$ و $ptc^{-1} = b$. بنابراین $p|b$؛ به طور مشابه اگر b یکه باشد در این صورت $p|c$. اگر هر دو b و c غیریکه‌های غیرصفر باشند، در این صورت $b = q_1 \dots q_r$ و $c = q_{r+1} \dots q_s$ جایی که در آن q_iها (که لزوماً متمایز نیستند) تحویل‌ناپذیرند. چون $p|bc$، برای برخی $r \in R$ داریم $pr = bc = q_1 \dots q_s$. طبق یکتایی تجزیه،

عنصر تحویل‌ناپذیر p باید یک وابسته یکی از q_iها باشد. پس p، یکی از q_iها را می‌شمارد و بنابراین b یا c را می‌شمارد. ■

تمرینها

توجه: R یک دامنه صحیح را نشان می‌دهد، مگر خلاف آن ذکر شود.

۱.A. نشان دهید که $\mathbb{Z}[\sqrt{d}]$ یک زیرحلقه $\mathbb{C}$ است. اگر $d \geq 0$، نشان دهید که $\mathbb{Z}[\sqrt{d}]$ یک زیرحلقه $\mathbb{R}$ است.

۲. فرض کنید $d \neq \pm 1$ یک عدد صحیح **مربع‌آزاد** باشد (یعنی d بجز $(\pm 1)^2$ دارای هیچ شمارنده دیگری به صورت c^2 نیست). ثابت کنید که در $\mathbb{Z}[\sqrt{d}]$، تساوی $r + s\sqrt{d} = r_1 + s_1\sqrt{d}$ برقرار است، اگر و تنها اگر $r = r_1$ و $s = s_1$. با ارائه مثالی نشان دهید که اگر d مربع‌آزاد نباشد، این نتیجه می‌تواند نادرست باشد.

۳. اگر گزاره زیر درست است، آن را ثابت کنید؛ اگر غلط است یک مثال نقض ارائه کنید:

(الف) اگر $a|b$ و $c|d$ در R، در این صورت $ac|bd$.

(ب) اگر $a|b$ و $c|d$ در R، در این صورت $(a+c)|(b+d)$.

۴. ثابت کنید که c و d در R وابسته‌اند اگر و تنها اگر $c|d$ و $d|c$.

۵. اگر $a = bc$ با $a \neq 0$ و b و c غیریکه باشند، نشان دهید که a یک وابسته b نیست.

۶. گزاره "a یک وابسته b است" را با $a \sim b$ نشان دهید. ثابت کنید که $\sim$ یک رابطه هم‌ارزی است؛ یعنی برای هر $r, s, t \in R$: (i) $r \sim r$. (ii) اگر $r \sim s$ در این صورت $s \sim r$. (iii) اگر $r \sim s$ و $s \sim t$ در این صورت $r \sim t$.

۷. (الف) ثابت کنید که هر وابسته یک عنصر تحویل‌ناپذیر، تحویل‌ناپذیر است.

(ب) اگر u و v یکه باشند، ثابت کنید که u و v وابسته‌اند.

۸. آیا $x + 2$ تحویل‌ناپذیر در $\mathbb{Z}[x]$ است؟ اگر نیست چرا؟

۹. فرض کنید d یک ب‌م‌م a_1، a_2، ...، a_k باشد. ثابت کنید که هر وابسته d نیز یک ب‌م‌م a_1، ...، a_k است.

۱۰. فرض کنید p یک عنصر تحویل‌ناپذیر باشد. ثابت کنید که 1_R یک ب‌م‌م p و a است اگر و تنها اگر $p \nmid a$.

۱۱. با ارائه مثالی نشان دهید که یک زیردامنه از یک دامنه یکتایی تجزیه لزوماً یک **دی‌ت** نیست.

۱۲. آیا یک میدان یک **دی‌ت** است؟

۱۳. ثابت کنید که u در R یکه است اگر و تنها اگر u دارای هیچ شمارنده سره نباشد.

B ۱۴. اگر هر دو عنصر غیرصفر R وابسته باشند، ثابت کنید که R یک میدان است.

۱۵. اگر هر عضو غیرصفر R یا تحویل‌ناپذیر و یا یک یکه باشد، ثابت کنید که R یک میدان است.

۱۶. (الف) نشان دهید که $i+1$ در $\mathbb{Z}[i]$ یکه نیست. (راهنمایی: وارون $i+1$ در $\mathbb{C}$ چیست؟)
(ب) نشان دهید که ۲ در $\mathbb{Z}[i]$ تحویل‌ناپذیر است.

۱۷. فرض کنید p یک عنصر غیریکه غیرصفر R باشد به قسمی که هرگاه $p|cd$ در این صورت $p|c$ یا $p|d$. ثابت کنید که p تحویل‌ناپذیر است.

۱۸. اگر $f : R \to S$ یک همریختی پوشا از دامنه‌های صحیح باشد، p تحویل‌ناپذیر در R باشد و $f(p) \neq 0_S$، آیا $f(p)$ در S تحویل‌ناپذیر است؟

۱۹. فرض کنید (r,s) هر ب‌م‌م r و s را نشان دهد. مانند تمرین ۶، نماد $\sim$ را برای نشان دادن وابسته‌ها بکار برید. ثابت کنیدکه برای هر $r,s,t \in R$:

(الف) اگر $s \sim t$، در این صورت $rs \sim rt$.

(ب) اگر $s \sim t$، در این صورت $(r,s) \sim (r,t)$.

(پ) $r(s,t) \sim (rs,rt)$.

(ت) $(r,(s,t)) \sim ((r,s),t)$. [راهنمایی: نشان دهید که هر دو، ب‌م‌م‌های r، s و t هستند.]

۲۰. با نماد بکاررفته در تمرین ۱۹، ثابت کنید که اگر $(b,c) \sim 1_R$ و $(b,d) \sim 1_R$، در این صورت $(b,cd) \sim 1_R$. [راهنمایی: طبق قسمت‌های (الف) و (پ)، $d \sim (bd,cd)$، لذا $(b,d) \sim (b,(bd,cd)) \sim 1_R$.]

۲۱. فرض کنید R یک دامنه صحیح باشد که در آن هر دو عضو (که تواماً صفر نیستند) دارای یک ب‌م‌م باشند. فرض کنید p یک عنصر تحویل‌ناپذیر R باشد. ثابت کنید که هرگاه $p|cd$ در این صورت $p|c$ یا $p|d$. [راهنمایی: تمرین‌های ۱۰ و ۲۰.]

۲۲. اگر R یک **دی‌ت** باشد، اگر a، b و c عناصری از R باشند به قسمی که $a|c$ و $b|c$، و اگر 1_R یک ب‌م‌م a و b باشد، ثابت کنید که $ab|c$.

۲۳. فرض کنید R یک **دی‌ت** باشد. اگر $a|bc$ و اگر 1_R یک ب‌م‌م a و b باشد، ثابت کنید که $a|c$.

۲۴. اگر a_1، a_2، ... عناصری از R باشند به قسمی که هر a_{i+1} یک شمارنده سره a_i باشد، ثابت کنید که هر a_i (با $i > 1$) یک شمارنده سره غیریکه از a_1 است.

۲۵. نشان دهید که ۱ یک ترکیب خطی از چندجمله‌ایهای ۲ و x در $\mathbb{Z}[x]$ نیست. امّا بخش ۵.۸ نشان می‌دهد که ۱ یک ب‌م‌م x و ۲ در $\mathbb{Z}[x]$ است.

۲۶. **یک کوچکترین مضرب مشترک (ک‌م‌م)** عناصر غیرصفر a_1، ...، a_k عبارت از یک عنصر b است به قسمی که (i) هر a_i، b را می‌شمارد (ii) اگر هر a_i یک عنصر c را بشمارد در این صورت $b|c$. ثابت کنید که هر مجموعه متناهی از عناصر غیرصفر در یک **دی‌ت** دارای یک کوچکترین مضرب مشترک است.

۲۷. ثابت کنید که عناصر غیرصفر a و b در R دارای کوچکترین مضرب مشترک هستند اگر و تنها اگر اشتراک ایده‌آلهای اصلی (a) و (b) نیز یک ایده‌آل اصلی باشد.

۲۸. ثابت کنید که تنها یکه‌های $\mathbb{Q}_{\mathbb{Z}}[x]$ عبارتند از ۱ و ۱−. [مثال ۶.۸ را ملاحظه کنید.]

۲۹. (الف) اگر p یک عدد اول در $\mathbb{Z}$ باشد، ثابت کنید که چندجمله‌ای ثابت p در $\mathbb{Q}_{\mathbb{Z}}[x]$ تحویل‌ناپذیر است. [راهنمایی: چون $\mathbb{Q}_{\mathbb{Z}}[x] \subseteq \mathbb{Q}[x]$، قضیه ۱.۴ قابل کاربرد است؛ همچنین تمرین ۲۸ را ملاحظه کنید].

(ب) اگر $p \neq q$ و p و q اعداد اول مثبت در $\mathbb{Z}$ باشند، ثابت کنید که p و q در $\mathbb{Q}_{\mathbb{Z}}[x]$ وابسته نیستند.

۳۰. (الف) نشان دهید که تنها شمارنده‌های x در $\mathbb{Q}_{\mathbb{Z}}[x]$ عبارتند از اعداد صحیح و چندجمله‌ایهای درجه اول به صورت rx با $r = 1/n$ و $n \in \mathbb{Z}$.

(ب) نشان دهید که x را نمی‌توان به صورت حاصل‌ضرب متناهی از عناصر تحویل‌ناپذیر در $\mathbb{Q}_{\mathbb{Z}}[x]$ نوشت.

۳۱.C. ثابت کنید که $p(x)$ تحویل‌ناپذیر در $\mathbb{Q}_{\mathbb{Z}}[x]$ است اگر و تنها اگر $p(x)$ یا یک عدد صحیح اول و یا یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{Q}[x]$ با جمله ثابت ± 1 باشد. نتیجه بگیرید که هر چندجمله‌ای تحویل‌ناپذیر $p(x)$ در $\mathbb{Q}_{\mathbb{Z}}[x]$ دارای این خاصیت است که هرگاه $p(x)|c(x)d(x)$، در این صورت $p(x)|c(x)$ یا $p(x)|d(x)$.

۳۲. نشان دهید که هر چندجمله‌ای غیرصفر $f(x)$ در $\mathbb{Q}_{\mathbb{Z}}[x]$ را می‌توان به صورت $cx^n p_1(x)\cdots p_k(x)$ نوشت که در آن $c \in \mathbb{Q}$، $n \geq 0$ و هر $p_i(x)$ یک چندجمله‌ای تحویل‌ناپذیر غیرثابت در $\mathbb{Q}_{\mathbb{Z}}[x]$ است و این که این تجزیه به مفهومی که در پی می‌آید یکتاست. اگر $f(x) = dx^m q_1(x)\cdots q_t(x)$ که در آن $d \in \mathbb{Q}$، $m \geq 0$ و هر $q_i(x)$ یک چندجمله‌ای تحویل‌ناپذیر غیرثابت در $\mathbb{Q}_{\mathbb{Z}}[x]$ است، در این صورت $c = \pm d$، $m = n$، $k = t$ و پس از تغییر نمایه‌ها اگر لازم باشد، برای هر i، $p_i(x) = \pm q_i(x)$.

۳۳. ثابت کنید که هر دو چندجمله‌ای غیرصفر در $\mathbb{Q}_{\mathbb{Z}}[x]$ دارای یک ب‌م‌م هستند.

۳۴. (الف) ثابت کنید که $f(x)$ تحویل‌ناپذیر در $\mathbb{Z}[x]$ است اگر و تنها اگر $f(x)$ یا یک عدد صحیح اول و یا یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{Q}[x]$ باشد به قسمی که ب‌م‌م ضرایب $f(x)$ در $\mathbb{Z}$ برابر ۱ باشد.

(ب) ثابت کنید که $\mathbb{Z}[x]$ یک دی‌ت است. [راهنمایی: قضایای ۱۰.۴ و ۱۸.۴ را ملاحظه کنید.]

۸-۲ یکتایی تجزیه و ایده‌آل‌های اصلی

در این بخش نشان می‌دهیم که هر دامنه صحیح R که در دو شرط زیر صدق کند لزوماً یک دی‌ت است:

I. هیچ دنباله نامتناهی $a_1, a_2, \ldots$ وجود ندارد به قسمی که هر a_{i+1} یک شمارنده سره a_i باشد.

II. اگر p تحویل‌ناپذیر باشد و $p|bc$، در این صورت $p|b$ یا $p|c$.

سپس چندین رده از دامنه‌های صحیحی را که در این شرایط صدق می‌کنند و در نتیجه دی‌ت هستند

معرفی می‌کنیم.

انتخاب این دو شرط از غور در خواص دی‌ت‌ها بدست آمده است. در عین حال به‌سادگی می‌توان دید که چرا این دو شرط انتخاب‌های مناسبی هستند. برای مثال در تجزیه یک عدد صحیح a، ابتدا یک شمارنده سره a را فاکتور می‌گیریم، سپس همین کار را با این فاکتور انجام می‌دهیم و آنقدر این کار را تکرار می‌کنیم تا به یک عدد اوّل و یا ۱ برسیم. این روش در حالت کلی نیز روش کارآمدی است البته منوط به برقراری شرط I که متناهی بودن فرآیند فاکتورگیری را تضمین می‌کند. شرط II همان خاصیت کلیدی است که در اثبات یکتایی تجزیه در $\mathbb{Z}$ و $\mathbb{F}[x]$ بکار رفت (اثبات قضیه ۱۱.۱ را ملاحظه کنید). شرط II را در حالت کلی نیز می‌توان به طریق مشابه بکار برد، البته در صورتی که بدانیم هر عضو حداقل دارای یک تجزیه است.

این بخش را با بسط ارتباط بین بخش‌پذیری و ایده‌آل‌های اصلی در یک دامنه صحیح آغاز می‌کنیم. این امر به ما اجازه می‌دهد تا شرط I را به شکل مفیدتری صورت‌بندی کنیم. در یک دامنه صحیح R، ایده‌آل اصلی (b) مجموعه همه مضارب b است، یعنی همه عناصری که بر b بخش‌پذیرند. بنابراین

$$a \in (b) \text{ اگر و تنها اگر } b|a.$$

به علاوه هرگاه $a \in (b)$ آنگاه هر مضرب a در ایده‌آل (b) قرار دارد، لذا $(a) \subseteq (b)$. برعکس، وقتی که $(a) \subseteq (b)$، آنگاه a در ایده‌آل (b) قرار دارد، پس $b|a$. بنابراین

$$(a) \subseteq (b) \text{ اگر و تنها اگر } b|a.$$

با تعویض نقش a و b بدست می‌آوریم

$$(a) = (b) \text{ اگر و تنها اگر } a|b \text{ و } b|a.$$

تمرین ۴ بخش ۱.۸ نشان می‌دهد که $a|b$ و $b|a$ اگر و تنها اگر b یک وابسته a باشد. بنابراین $(a) \subsetneqq (b)$ اگر و تنها اگر $b|a$ و b یک وابسته a نباشد، یعنی

$$(a) \subsetneqq (b) \text{ اگر و تنها اگر } b \text{ یک شمارنده سره } a \text{ باشد.}$$

در نتیجه، شرط I معادل است با

I′. هیچ زنجیر نامتناهی از ایده‌آلهای اصلی به صورت زیر وجود ندارد:

$$(a_1) \subsetneqq (a_2) \subsetneqq (a_3) \subsetneqq \cdots.$$

این شرط معمولاً به صورت معادل زیر و به شکل اثباتی بیان می‌شود.

تعریف. دامنه صحیح R دارای **شرط زنجیر صعودی (ش‌زص)** روی ایده‌آلهای اصلی است مشروط به این‌که هرگاه $(a_1) \supseteq (a_2) \supseteq (a_3) \supseteq \cdots$، آنگاه عدد صحیح مثبت n وجود داشته باشد به قسمی که برای هر $i > n$، $(a_i) = (a_n)$.

قضیه ۷.۸. دامنه صحیح R یک دامنه یکتایی تجزیه است اگر و تنها اگر

(۱) R دارای شرط زنجیر صعودی روی ایده‌آلهای اصلی باشد؛ و

(۲) هرگاه p در R تحویل‌ناپذیر باشد و $p|cd$، آنگاه $p|c$ یا $p|d$.

برهان. اگر R یک **دی‌ت** باشد آنگاه طبق قضیه ۶.۸، R در (۲) صدق می‌کند. بحث بالا نشان می‌دهد که (۱) معادل شرط I است. طبق نتیجه ۴.۸، هر **دی‌ت** در شرط I صدق می‌کند.

برعکس، فرض کنید که R در (۱) و (۲) صدق کند. فرض کنید a عضو غیریکه غیرصفری در R باشد. باید نشان دهیم که a دارای حداقل یک تجزیه است. به خلاف، فرض کنید که a حاصل‌ضربی از عناصر تحویل‌ناپذیر نباشد. پس a خودش تحویل‌ناپذیر نیست. لذا عناصر غیریکه a_1 و b_1 وجود دارد به قسمی که $a = a_1 b_1$ (در غیر این صورت هر تجزیه a باید یک یکه را در بر داشته باشد و طبق قضیه ۱.۸ باید تحویل‌ناپذیر باشد). اگر هر دو a_1 و b_1 حاصل‌ضربی از عناصر تحویل‌ناپذیر باشند، در این صورت a نیز چنین است. بنابراین حداقل یکی از آنها مثلاً a_1 حاصل‌ضربی از عناصر تحویل‌ناپذیر نیست. چون b_1 یکه نیست، a_1 وابسته a نیست (تمرین ۵ بخش ۱.۸ را ملاحظه کنید). بنابراین a_1 یک شمارنده سره a است لذا $(a_1) \subsetneqq (a)$ که در آن a_1 یک عنصر غیریکه غیرصفر است که حاصل‌ضربی از عناصر تحویل‌ناپذیر نیست. اینک استدلال قبلی را با a_1 به جای a تکرار کنید. این منجر به یک غیریکه غیرصفر a_2 می‌شود به قسمی که $(a_1) \subsetneqq (a_2)$ و a_2 حاصل‌ضربی از عناصر تحویل‌ناپذیر نیست. تکرار نامحدود این فرآیند منجر به یک زنجیر اکیداً صعودی $\cdots \subsetneqq (a_3) \subsetneqq (a_2) \subsetneqq (a_1)$ از ایده‌آل‌های اصلی می‌شود که (۱) را نقض می‌کند. بنابراین a باید حداقل دارای یک تجزیه به عنوان حاصل‌ضربی از عناصر تحویل‌ناپذیر باشد. برای نشان دادن این که این تجزیه تا حد وابسته‌ها یکتاست، اثبات قضیه ۱۰.۴ (حالتی که $R = \mathbb{F}[x]$) را با جایگزینی کلمه "یکه" به جای "ثابت" و استفاده از (۲) و تمرین ۲ به جای نتیجه ۹.۴، به وضعیت کلی تطبیق دهید. ■

چون ایده‌آل‌های اصلی نقش اساسی را در قضیه ۷.۸ بازی می‌کنند، کلاس آشکاری از دامنه‌های صحیح وجود دارد که این قضیه را می‌توان در مورد آنها بکار برد:

تعریف. یک **دامنه ایده‌آل اصلی (داا)** یک دامنه صحیح است که در آن هر ایده‌آل یک ایده‌آل اصلی باشد.

مثال ۷.۸. اگر $\mathbb{F}$ یک میدان باشد، در این صورت دامنه چندجمله‌ای‌های $\mathbb{F}[x]$ یک دااست. برای اثبات، فرض کنید I یک ایده‌آل غیرصفر در $\mathbb{F}[x]$ باشد. در این صورت I یک چندجمله‌ای $g(x)$ با کوچکترین درجه ممکن را شامل است (بنا به اصل خوش‌ترتیبی، مجموعه درجه‌های چندجمله‌ای‌های غیرصفر در I یک مجموعه غیرتهی از اعداد صحیح غیرمنفی است). ادعا می‌کنیم که I ایده‌آل اصلی $(g(x))$ می‌باشد. چون $g(x) \in I$ و I یک ایده‌آل است، $t(x)g(x) \in I$ برای هر $t(x) \in \mathbb{F}[x]$. بنابراین $(g(x)) \subseteq I$. برعکس، اگر $f(x) \in I$ در این صورت طبق الگوریتم تقسیم $q(x), r(x) \in \mathbb{F}[x]$ وجود دارند به قسمی که $f(x) = g(x)q(x) + r(x)$ و $r(x) = 0_{\mathbb{F}}$ یا $\deg r(x) < \deg g(x)$. امّا $r(x) = f(x) - g(x)q(x)$ و $f(x), g(x) \in I$، لذا $r(x)$ در ایده‌آل I قرار دارد. اگر $r(x) \neq 0_{\mathbb{F}}$ در این صورت $\deg r(x) < \deg g(x)$، و این ممکن نیست زیرا $g(x)$ یک چندجمله‌ای با کوچکترین درجه ممکن در I است. بنابراین $r(x) = 0_{\mathbb{F}}$ و لذا $f(x) = g(x)q(x) + r(x) = g(x)q(x) \in (g(x))$. پس $I \subseteq (g(x))$ و از اینجا $I = (g(x))$. بنابراین $\mathbb{F}[x]$ یک دااست.

مثال ۸.۸. مجموعه اعداد صحیح $\mathbb{Z}$ یک دااست. این را می‌توانید با انتقال برهان دامنه ایده‌ال اصلی بودن $\mathbb{F}[x]$ به $\mathbb{Z}$ اثبات کنید (تمرین ۱). بویژه اگر I یک ایده‌آل غیرصفر در $\mathbb{Z}$ باشد، در این صورت $I = (c)$، که در آن c کوچکترین عدد صحیح مثبت در I است.

مثال ۹.۸. در نتیجه ۱۲.۸ زیر می‌بینیم که حلقه اعداد صحیح گوسی $\mathbb{Z}[i]$ یک دااست.

مثال ۱۰.۸. همانگونه که در مثال ۵.۶ دیدیم، در حلقه $\mathbb{Z}[x]$، ایده‌آل I متشکل از همه چندجمله‌ای‌هایی که جمله ثابت آنها زوج است ایده‌آل اصلی نیست. بنابراین $\mathbb{Z}[x]$ دااست.

لم ۸.۸. هر دامنه ایده‌آل اصلی R در شرط زنجیر صعودی روی ایده‌آلهای اصلی صدق می‌کند.

برهان. اگر $(a_1) \subseteq (a_2) \subseteq \cdots$ یک زنجیر صعودی از ایده‌آلها در R باشد، A را اجتماع مجموعه‌های (a_t)، یعنی $\bigcup_{t\geq 1}(a_t)$ قرار دهید. ادعا می‌کنیم که A یک ایده‌آل است. فرض کنید $a, b \in A$؛ در این صورت برای برخی $j, k \geq 1$، $a \in (a_j)$ و $b \in (a_k)$. داریم $j \leq k$ یا $k \leq j$، فرض کنید مثلاً $j \leq k$. در این صورت $(a_j) \subseteq (a_k)$، لذا $a, b \in (a_k)$. چون (a_k) یک ایده‌آل است می‌دانیم که $a - b \in (a_k) \subseteq A$ و برای هر $r \in R$، $ra \in (a_k) \subseteq A$. بنابراین طبق قضیه ۱.۶، A یک ایده‌آل است. چون R یک دالا است، برای برخی $c \in R$، $A = (c)$. چون $A = \bigcup_{t\geq 1}(a_t)$، می‌دانیم که برای برخی n، $c \in (a_n)$. در نتیجه $(a_n) \subseteq (c)$ و برای هر $i \geq n$،

$$(a_n) \subseteq (a_i) \subseteq \bigcup_{t\geq 1}(a_t) = A = (c) \subseteq (a_n).$$

بنابراین برای هر $i \geq n$، $(a_i) = (a_n)$. ■

لم ۹.۸. فرض کنید R یک دامنه ایده‌آل اصلی باشد. اگر p در R تحویل‌ناپذیر باشد و $p|bc$، در این صورت $p|b$ یا $p|c$.

برهان[۳]. اگر $p|bc$، در این صورت bc در ایده‌آل (p) قرار دارد. در صورتی که بدانیم (p) یک ایده‌آل اول است، نتیجه می‌گیریم که $b \in (p)$ یا $c \in (p)$، یعنی $p|b$ یا $p|c$. امّا طبق نتیجه ۱۴.۶، هر ایده‌آل بیشین اول است، پس تنها لازم است نشان دهیم که (p) یک ایده‌آل بیشین است. فرض کنید I ایده‌آلی باشد با $(p) \subseteq I \subseteq R$. چون R یک دالا است، برای برخی $d \in R$ داریم $I = (d)$. در این صورت $(p) \subseteq (d) = I$ نتیجه می‌دهد که $d|p$. چون p تحویل‌ناپذیر است، d باید یکه یا یک وابسته p باشد. اگر d یکه باشد، در این صورت طبق تمرین ۱۱ بخش ۱.۶، $I = (d) = R$. اگر d یک وابسته p باشد، مثلاً $d = pu$، در این صورت $p|d$ و بنابراین $(p) \subseteq (d)$. در این حالت $(p) \subseteq (d) \subseteq (p)$، لذا $I = (d) = (p)$. بنابراین (p) بیشین است و اثبات کامل می‌شود. ■

لم‌های ۸.۸ و ۹.۸ همراه با قضیه ۷.۸ قضیه زیر را ثابت می‌کند.

قضیه ۱۰.۸. هر دامنه ایده‌آل اصلی یک دامنه یکتایی تجزیه است.

---

۳) تمرین ۲۰ را برای برهان دیگری که در آن از نتیجه ۱۶.۴ استفاده نمی‌شود، ملاحظه کنید.

هشدار عکس قضیه ۱۰.۸ غلط است. در بخش ۵.۸ می‌بینیم که حلقه چندجمله‌ای‌های $\mathbb{Z}[x]$ یک دامنه یکتایی تجزیه است امّا یک PID نیست.

حلقه‌های $\mathbb{Z}$ و $\mathbb{F}[x]$ از نظر محاسباتی دارای مزیت‌هایی هستند که حلقه‌های PID دلخواه فاقد آن می‌باشند. برای نمونه در $\mathbb{Z}$ و $\mathbb{F}[x]$، ب.م.م عناصر را می‌توان به سادگی با استفاده پی درپی از الگوریتم تقسیم بدست آورد. بنابراین در نظر گرفتن دامنه‌های صحیح دیگری که دارای خاصیتی مشابه الگوریتم تقسیم هستند می‌تواند مفید باشد[۴]. برای دیدن این‌که چگونه می‌توان چنین خاصیت مشابهی را توصیف کرد، توجه کنید که درجه یک چندجمله‌ای در $\mathbb{F}[x]$ را می‌توان به عنوان تابعی از چندجمله‌ای‌های غیرصفر در $\mathbb{F}[x]$ به اعداد صحیح غیرمنفی قلمداد کرد. با تشخیص خواص کلیدی این تابع، تعریف زیر بدست می‌آید:

تعریف. دامنه صحیح R یک **دامنه اقلیدسی** است اگر تابع δ از عناصر غیرصفر R به اعداد صحیح غیرمنفی موجود باشد که در دو شرط زیر صدق کند:

(i) برای هر دو عنصر غیرصفر a و b در R، $\delta(a) \leq \delta(ab)$.

(ii) اگر $a, b \in R$ و $b \neq 0_R$، در این صورت عناصر q و r در R وجود دارند به قسمی که $a = bq + r$ و $r = 0_R$ یا $\delta(r) < \delta(b)$.

مثال ۱۱.۸. اگر $\mathbb{F}$ یک میدان باشد، دامنه چندجمله‌ای‌های $\mathbb{F}[x]$ یک دامنه اقلیدسی است با تابع δ که توسط $\delta(f(x)) = \deg f(x)$ تعریف می‌شود. خاصیت (i) تعریف از قضیه ۱.۴ نتیجه می‌شود زیرا

$$\begin{aligned}\delta(f(x)g(x)) = \deg(f(x)g(x)) &= \deg f(x) + \deg g(x) \\ &\geq \deg f(x) = \delta(f(x))\end{aligned}$$

و خاصیت (ii) همان الگوریتم تقسیم است (قضیه ۳.۴).

مثال ۱۲.۸. $\mathbb{Z}$ یک دامنه‌اقلیدسی است با تابع δ که به صورت $\delta(a) = |a|$ داده شده است. خاصیت (i) برقرار است زیرا برای هر $a \neq 0$، $|b| \geq |a||b| = |ab|$. همانگونه که در نتیجه

۴) از مطالب باقیمانده این بخش در بخش‌های بعدی استفاده نمی‌شود.

۲.۱ بیان شد، الگوریتم تقسیم نشان می‌دهد که خاصیت (ii) برقرار است.

مثال ۱۳.۸. اثبات خواهیم کرد که حلقه اعداد صحیح گوسی $\mathbb{Z}[i] = \{s + ti \mid s, t \in \mathbb{Z}\}$ یک دامنه اقلیدسی است با تابع δ که به صورت $\delta(s + ti) = s^2 + t^2$ داده شده است. چون $s + ti = 0$ اگر وتنها اگر $s = t = 0$ لذا $\delta(s + ti) \geq 1$ هرگاه $s + ti \neq 0$. ثابت کنید که برای هر $a = s + ti$ و $b = u + vi$ در $\mathbb{Z}[i]$، $\delta(ab) = \delta(a)\delta(b)$ (تمرین ۵). در این صورت وقتی $b \neq 0$ داریم

$$\delta(a) = \delta(a).1 \leq \delta(a)\delta(b) = \delta(ab).$$

بنابراین خاصیت (i) برقرار است. اگر $b \neq 0$، بررسی کنید که a/b یک عدد مختلط است که می‌توان برای برخی $c, d \in \mathbb{Q}$ آن را به صورت $c + di$ نوشت (تمرین ۶). چون $c \in \mathbb{Q}$، می‌توان آن را بین دو عدد صحیح متوالی قرار داد، و به‌طور مشابه برای d. بنابراین اعداد صحیح m و n وجود دارند به قسمی که $|m - c| \leq 1/2$ و $|n - d| \leq 1/2$. چون $a/b = c + di$، داریم

$$\begin{aligned} a &= b[c + di] = b[(c - m + m) + (d - n + n)i] \\ &= b[(m + ni) + ((c - m) + (d - n)i)] \\ &= b[m + ni] + b[(c - m) + (d - n)i] \\ &= bq + r, \end{aligned}$$

که در آن $q = m + ni \in \mathbb{Z}[i]$ و $r = b[(c - m) + (d - n)i]$. چون $r = a - bq$ و $a, b, q \in \mathbb{Z}[i]$، می‌بینیم که $r \in \mathbb{Z}[i]$. خاصیت (ii) برقرار است زیرا

$$\begin{aligned} \delta(r) &= \delta(b)\delta[(c - m) + (d - n)i] = \delta(b)[(c - m)^2 + (d - n)^2] \\ &\leq \delta(b)[(\tfrac{1}{2})^2 + (\tfrac{1}{2})^2] = (\tfrac{1}{2}) \cdot \delta(b) < \delta(b). \end{aligned}$$

قضیه ۱۱.۸. هر دامنه اقلیدسی یک دامنه ایده‌آل اصلی است و بنابراین یک دامنه یکتایی تجزیه می‌باشد.

برهان. برهان ارائه شده در مثال ۷.۸ مبنی بر این که $\mathbb{F}[x]$ یک dا است را می‌توان برای هر دامنه

اقلیدسی دلخواه بکار برد. کافی است جای چندجمله‌ای‌ها را با عناصر R و جای درجه را با تابع δ عوض کنید. سپس یکتایی تجزیه از قضیه ۱۰.۸ نتیجه می‌شود. ■

قضیه ۱۱.۸ و مثال قبل از آن نتیجه زیر را ثابت می‌کند:

نتیجه ۱۲.۸. دامنه اعداد صحیح گوسی $\mathbb{Z}[i]$ یک دامنه ایده‌آل اصلی است و بنابراین یک دامنه یکتایی تجزیه می‌باشد.

عکس قضیهٔ ۱۱.۸ غلط است: دامنه‌های ایده‌آل اصلی وجود دارند که اقلیدسی نیستند (ویلسون[۵] [۲۳] را ملاحظه کنید). بنابراین کلاس دامنه‌های اقلیدسی به‌طور اکید در کلاس دامنه‌های ایده‌آل اصلی قرار دارد. البته باید توجه کرد که می‌توان یکتایی تجزیه در دامنه‌های اقلیدسی را مستقیماً و تنها با سازگارکردن برهان ارائه شده برای $\mathbb{F}[x]$ به حالت کلی، ثابت نمود. در واقع همه نتایج بدست آمده برای $\mathbb{Z}$ و $\mathbb{F}[x]$ که عمدتاً به الگوریتم تقسیم بستگی دارند (مثل الگوریتم اقلیدسی) با اندکی تغییرات قابل انتقال به دامنه‌های اقلیدسی می‌باشد (تمرین ۲۹).

تمرینها

۱.A. ثابت کنید که $\mathbb{Z}$ یک daii است. [اثبات ارائه شده برای $\mathbb{F}[x]$ در مثال ۷.۸ را بکار برید.]

۲. اگر p عضوی تحویل‌ناپذیر در یک daii باشد و $p|a_1a_2\dots a_n$، با استفاده از لم ۹.۸ ثابت کنید که p حداقل یک a_i را می‌شمارد.

۳. اگر a و b عناصر غیرصفری از یک دامنه صحیح باشند و a غیریکه باشد، ثابت کنید که $(ab) \subsetneq (b)$.

۴. فرض کنید $\mathbb{F}$ یک میدان باشد. ثابت کنید که $\mathbb{F}$ یک دامنه اقلیدسی است با تابع δ که به صورت $\delta(a) = 0$ برای هر عنصر غیرصفر $a \in \mathbb{F}$ داده شده است.

۵. اگر $a = s+ti$ و $b = u+vi$ عناصری از $\mathbb{Z}[i]$ باشند، نشان دهید که $\delta(ab) = \delta(a)\delta(b)$، که در آن $\delta(r+si) = r^2+s^2$.

۶. اگر $a = s+ti$ و $b = u+vi$ در $\mathbb{Z}[i]$ باشند و $b \neq 0$، نشان دهید که $a/b = c+di$ که در آن $c = (su+tv)/(u^2+v^2)$ و $d = (tu-sv)/(u^2+v^2)$.

۵) Wilson

B.۷. نشان دهید که عناصر q و r در تعریف یک دامنه اقلیدسی لزوماً یکتا نیستند. [راهنمایی: در $\mathbb{Z}[i]$ فرض کنید $a = -۴ + i$ و $b = ۵ + ۳i$؛ در نظر بگیرید $q = -۱ + i$ و $q = -۱$.]

۸. فرض کنید R یک داا باشد. اگر (c) یک ایده‌آل غیرصفر در R باشد، نشان دهید که تنها تعداد متناهی ایده‌آل در R وجود دارند که (c) را شامل هستند. [راهنمایی: شمارنده‌های c را در نظر بگیرید.]

۹. فرض کنید p یک عدد اول ثابت باشد و فرض کنید R مجموعه همه اعداد گویایی باشد که قابل نوشتن به صورت a/b هستند که در آن b بر p بخش‌پذیر نیست. ثابت کنید:

(الف) R یک دامنه صحیح است که $\mathbb{Z}$ را شامل است. [توجه کنید که $n = n/۱$].

(ب) اگر $a/b \in R$ و $p \nmid a$، در این صورت a/b در R یکه است.

(پ) اگر I یک ایده‌آل غیرصفر در R باشد و $I \neq R$، در این صورت برای یک $t > ۰$، I شامل p^t است.

(ت) R یک داا است. (اگر I یک ایده‌آل باشد، نشان دهید که $I = (p^k)$، جایی‌که p^k کوچکترین توان p در I است.)

۱۰. ثابت کنید که در یک داا، یک ایده‌آل (p) بیشین است اگر و تنها اگر p تحویل‌ناپذیر باشد.

۱۱. ثابت کنید که هر ایده‌آل در یک دامنه ایده‌آل اصلی R (بجز خود R) در یک ایده‌آل بیشین مشمول است. [تمرین ۱۰ را ملاحظه کنید.]

۱۲. ثابت کنید که در یک داا، یک ایده‌آل غیرصفر اوّل است اگر و تنها اگر بیشین باشد. [تمرین ۱۰ را ملاحظه کنید.]

۱۳. فرض کنید $f : R \to S$ یک همریختی پوشا از حلقه‌های یکدار باشد:

(الف) اگر R یک داا باشد، ثابت کنید که هر ایده‌آل در S اصلی است.

(ب) با مثال نشان دهید که S لزوماً یک دامنه صحیح نیست.

۱۴. فرض کنید R یک حلقه جابجایی یکدار باشد و $a_۱, a_۲, \cdots, a_n \in R$. ثابت کنید که $I = \{r_۱a_۱ + \cdots + r_na_n \mid r_i \in R\}$ یک ایده‌آل در R است. ایده‌آل I را با **مولدمتناهی** گویند و آن را **ایده‌آل تولیدشده توسط** $a_۱, \cdots, a_n$ می‌نامند. یک ایده‌آل اصلی یک ایده‌آل تولیدشده توسط تنها یک عضو است.

۱۵. نشان دهید که حلقه $\mathbb{Q}_{\mathbb{Z}}[x]$، در **ش‌زص** روی ایده‌ال‌های اصلی صدق نمی‌کند و بنابراین یک داا نیست. [ایده‌ال‌های $(\frac{1}{2}x)$، $(\frac{1}{4}x)$، $(\frac{1}{8}x)$، ...، $(\frac{1}{2^n}x)$، ... را در نظر بگیرید.]

۱۶. گوییم یک حلقه R در **شرط زنجیر صعودی (ش‌زص)** روی ایده‌آل‌ها صدق می‌کند اگر هرگاه $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ یک زنجیر از ایده‌آل‌ها در R باشد، در این صورت عدد صحیح n موجود باشد به قسمی که برای هر $j \geq n$، $I_j = I_n$. ثابت کنید که اگر هر ایده‌آل حلقه جابجایی R با مولد متناهی باشد، در این صورت R در **ش‌زص** صدق می‌کند. [تمرین ۱۴ و لم ۸.۸ را ملاحظه کنید.]

۱۷. فرض کنید R یک داا و $a, b \in R$ تواماً صفر نباشند. ثابت کنید که a و b دارای یک بزرگترین مقسوم‌علیه مشترک است که می‌تواند به‌صورت یک ترکیب خطی از a و b نوشته شود. [راهنمایی: فرض کنید I ایده‌آل تولیدشده توسط a و b باشد (تمرین ۱۴ را ملاحظه کنید)؛ در این صورت برای برخی $d \in R$، $I = (d)$. نشان دهید که d یک ب‌م‌م a و b است.]

۱۸. تمرین ۱۷ را به هر تعداد متناهی از عناصر تعمیم دهید.

۱۹. فرض کنید R یک داا و S یک دامنه صحیح باشد که R را شامل است. فرض کنید $a, b, d \in R$. اگر d یک ب‌م‌م a و b در R باشد، ثابت کنید که d یک ب‌م‌م a و b در S است. [تمرین ۱۷ را ملاحظه کنید.]

۲۰. اثبات دیگری از لم ۹.۸ مطابق آنچه در پی می‌آید ارائه دهید: اگر $p|b$، چیزی برای اثبات وجود ندارد. اگر $p \nmid b$ در این صورت به موجب تمرین ۱۰ بخش ۱.۸، 1_R یک ب‌م‌م p و b است. حال با کپی کردن اثبات قضیه ۵.۱ با p به جای a و تمرین ۱۷ به جای قضیه ۳.۱، نشان دهید که $p|c$.

۲۱. فرض کنید R یک دامنه صحیح باشد. ثابت کنید که R یک داا است اگر و تنها اگر در دو شرط زیر صدق کند:

(i) هر ایده‌آل R با مولدمتناهی باشد (تمرین ۱۴) و (ii) هرگاه $a, b \in R$، در این صورت ایده‌آل مجموع $(b) + (a)$ یک ایده‌آل اصلی باشد. [ایده‌آل مجموع در تمرین ۱۷ بخش ۱.۶ تعریف شده است.]

۲۲. فرض کنید R یک دامنه اقلیدسی باشد. ثابت کنید که

(الف) برای هر عنصر غیر صفر $a \in R$، $\delta(1_R) \leq \delta(a)$.

(ب) $\delta(u) = \delta(1_R)$ اگر وتنها اگر u در R یکه باشد.

(پ) اگر a و b وابسته باشند، در این صورت $\delta(a) = \delta(b)$.

(ت) اگر $a|b$ و $\delta(a) = \delta(b)$، در این صورت a و b وابسته‌اند.

۲۳. نشان دهید که $\mathbb{Z}[\sqrt{-2}]$ یک دامنه اقلیدسی است با $\delta(r + s\sqrt{-2}) = r^2 + 2s^2$.

۲۴. فرض کنید $w = (-1 + \sqrt{-3})/2$ و $\mathbb{Z}[w] = \{r + sw \mid r, s \in \mathbb{Z}\}$. ثابت کنید که $\mathbb{Z}[w]$ یک دامنه اقلیدسی است با $\delta(r+sw) = (r+sw)(r+sw^2) = r^2 - rs + s^2$.
[توجه کنید که $w^3 = 1$ و $w^2 + w + 1 = 0$ (چرا؟).]

۲۵. فرض کنید R یک دامنه اقلیدسی باشد. اگر تابع δ یک تابع ثابت باشد، ثابت کنید که R یک میدان است.

۲۶. اثبات یا رد کنید: فرض کنید R یک دامنه اقلیدسی باشد، در این صورت $I = \{a \in R \mid \delta(a) > \delta(1_R)\}$ یک ایده‌آل در R است.

۲۷. فرض کنید I یک ایده‌آل غیرصفر در $\mathbb{Z}[i]$ باشد. نشان دهید که حلقه خارج قسمت $\mathbb{Z}[i]/I$ متناهی است.

۲۸. (الف) ثابت کنید که $i - 1$ در $\mathbb{Z}[i]$ تحویل‌ناپذیر است. [راهنمایی: اگر $a|(1 - i)$، در این صورت $ab = i - 1$؛ تمرین ۵ و ۲۲ را ملاحظه کنید.]

(ب) ۲ را به صورت حاصل‌ضربی از عناصر تحویل‌ناپذیر در $\mathbb{Z}[i]$ بنویسید. [راهنمایی: $i - 1$ را به عنوان یک عامل ۲ امتحان کنید.]

۲۹.C الگوریتم تقسیم برای یافتن ب‌م‌م دو عنصر از یک دامنه اقلیدسی را بیان و اثبات کنید.

۳۰. فرض کنید R یک دامنه اقلیدسی باشد به قسمی که برای هر دو عنصر غیرصفر a و b در R، $\delta(a + b) \leq \max\{\delta(a), \delta(b)\}$. ثابت کنید که عناصر q و r در تعریف دامنه اقلیدسی یکتا هستند.

۳۱. مطابق آنچه که در پی می‌آید ثابت کنید که هر ایده‌آل I در $\mathbb{Z}[\sqrt{d}]$ با مولدمتناهی (همانگونه که در تمرین ۱۴ تعریف شد) می‌باشد. فرض کنید $I_0 = I \cap \mathbb{Z}$ و

$$I_1 = \{b \in \mathbb{Z} \mid a \in \mathbb{Z} \text{ برای برخی } a + b\sqrt{d} \in I\}.$$

(الف) ثابت کنید که I_0 و I_1 ایده‌آل‌هایی در $\mathbb{Z}$ هستند. بنابراین برای برخی $r_i \in \mathbb{Z}$، $I_0 = (r_0)$ و $I_1 = (r_1)$.

(ب) ثابت کنید $I_0 \subseteq I_1$.

(پ) بنا به تعریف I_1، $a_1 \in \mathbb{Z}$ وجود دارد به قسمی که $a_1 + r_1\sqrt{d}$ در I است. ثابت کنید که ایده‌آل I توسط r_0 و $a_1 + r_1\sqrt{d}$ تولیدشده است. [راهنمایی: اگر $r + s\sqrt{d} \in I$، در این صورت $s \in I_1$، لذا $s = r_1 s_1$. نشان دهید که $(r + s\sqrt{d}) - s_1(a_1 + r_1\sqrt{d}) \in I_0$؛ با استفاده از این، $r + s\sqrt{d}$ را به‌عنوان یک ترکیب خطی از r_0 و $a_1 + r_1\sqrt{d}$ بنویسید.]

۸-۳ تجزیه اعداد صحیح درجه دوم

در این بخش دامنه‌های $\mathbb{Z}[\sqrt{d}]$ را مورد توجه بیشتری قرار می‌دهیم. دامنه‌های $\mathbb{Z}[\sqrt{d}]$ اغلب فاقد خاصیت یکتایی تجزیه هستند و لذا نمونه مناسبی از مسائلی هستند که به طور تاریخی نقش محوری در ظهور مفهوم ایده‌آل داشته‌اند. همچنین دامنه‌های $\mathbb{Z}[\sqrt{d}]$ نشان می‌دهند که چگونه مفهوم ایده‌آل می‌تواند در "بازگرداندن" یکتایی تجزیه به برخی از دامنه‌هایی که فاقد این خاصیت هستند بکار رود. ابتدا به شرح مختصری از تاریخچه این موضوع می‌پردازیم.

در اوایل قرن نوزدهم گوس[۶] "قانون تقابل دومجذوری[۷]" را ثابت کرد. این قانون روش سریعتری برای تعیین این که آیا همنهشتی (پیمانه n) $x^4 \equiv c$ دارای جواب هست یا خیر فراهم می‌کند. گرچه که صورت این قضیه تنها اعداد صحیح را در برداشت امّا اثبات گوس در دامنه بزرگتر $\mathbb{Z}[i]$ بنا شده بود. او این حقیقت را که $\mathbb{Z}[i]$ یک دامنه یکتایی تجزیه است اثبات کرد و از آن استفاده نمود.

چون اثبات گوس دامنه $\mathbb{Z}[i]$ را در برداشت که در آن i ریشه چهارم مختلط ۱ بود، ریاضی‌دان آلمانی کومر[۸] را در این فکر فرو برد که در اثبات قضایای مشابه برای همنهشتی‌های از درجه p ممکن است بتوان از خاصیت یکتایی تجزیه در دامنهٔ

$$\mathbb{Z}[w] = \{a_0 + a_1 w + a_2 w^2 + \cdots + a_{p-1} w^{p-1} \mid a_i \in \mathbb{Z}\}$$

۶) Gauss

۷) Law of Biquadratic Reciprocity

۸) E. Kummer

استفاده کرد که در آن $w = \cos(\frac{2\pi}{p}) + i\sin(\frac{2\pi}{p})$ یک ریشه p-ام ۱ است. او قادر به توسعه قضایای تقابل از مرتبه بالاتر نشد، زیرا کشف نمود که $\mathbb{Z}[w]$ ممکن است یک **دی‌ت** [۹] نباشد.

بعدها در طی همان قرن سؤالاتی در مورد یکتایی تجزیه در ارتباط با مسئله‌ای که اکنون به شرح آن می‌پردازیم مطرح شد: به‌سادگی می‌توان جواب‌های صحیح غیرصفر زیادی از جمله ۳، ۴، ۵ و یا ۵، ۱۲، ۱۳ برای معادله $x^2 + y^2 = z^2$ یافت. امّا تاکنون هیچکس قادر به یافتن جواب‌های صحیح غیرصفری برای $x^3 + y^3 = z^3$ یا $x^4 + y^4 = z^4$ نشده است. این امر منجر به این حدس شد که

وقتی $n > 2$، معادلهٔ $x^n + y^n = z^n$ دارای هیچ جواب صحیح غیرصفری نیست.

این حدس ریاضی‌دانان را برای قرن‌ها مجذوب خود کرد، ولی هرگز اثبات نشد[۱۰]. حدس فوق به "**قضیه آخر فرما**[۱۱] " معروف شده است زیرا در اواخر دههٔ ۱۶۳۰، فرما در حاشیه نسخه‌ای که از کتاب "حساب دیوفانتی" [۱۲] داشت این حدس را نوشته و اضافه کرده بود که "من برهان حقیقتاً چشمگیری کشف کرده‌ام که در این حاشیه نمی‌گنجد". متأسفانه "برهان" فرما تاکنون یافت نشده است. در واقع، امروزه بیشتر ریاضی‌دانان مطمئن نیستند که آیا او برهان معتبری برای این حدس داشت یا خیر.

در سال ۱۸۴۷، ریاضی‌دان فرانسوی لَمه[۱۳] بر این باور بود که برهانی از قضیه آخر فرما وقتی که n یک عدد اول باشد یافته است[۱۴]. او از این حقیقت استفاده کرد که برای هر عدد اول مثبت فرد p معادله $x^p + y^p$ می‌تواند به‌صورت زیر در دامنه $\mathbb{Z}[w]$ که در بالا توصیف شد، تجزیه شود:

$$x^p + y^p = (x + y)(x + wy)(x + w^2y)\cdots(x + w^{p-1}y).$$

برهان او براین فرض مبتنی بود که $\mathbb{Z}[w]$ یک دامنه یکتایی تجزیه است. هنگامی که او از کارکومر اطلاع یافت متوجه شد که اثبات او معتبر نیست.

کومر از پیش راهی را برای پرهیز از این مشکل یافته بود. او آنچه را که او "اعداد ایده‌آل" نامید ابداع نمود و ثابت کرد که یکتایی تجزیه برای این اعداد ایده‌آل برقرار است. سرانجام کار او به اثبات

۹) دامنه $\mathbb{Z}[w]$ برای هر عدد اول w کوچکتر از ۲۳، یک دی‌ت است و برای اعداد اول بزرگتر از ۲۳ یک دی‌ت نیست.

۱۰) مترجمان: این قضیه در سال ۱۹۹۳ توسط Andrew Wiles اثبات شد.

۱۱) Fermat's Last Theorem

۱۲) Diophantus' Arithmetica

۱۳) G. Lama

۱۴) اگر قضیه برای نماهای اول درست باشد، در این صورت برای همه نماها درست است، تمرین ۱ را ملاحظه کنید.

قضیه فرما برای ردهٔ بزرگی از اعداد اول که شامل تقریباً همه اعداد اول کوچکتر از ۱۰۰ است شد. این پیشرفت چشمگیر به طور عمیقی تقریباً بر همه کارهایی که بعدهاروی این مسئله انجام گرفت تأثیر گذاشت [۱۵]. امّا کار او حتی اهمیت بیشتری در توسعه جبر مدرن داشت، زیرا "اعداد ایده‌آل "کومر چیزهایی هستند که ما امروزه آنها را ایده‌آل می‌نامیم.

در انتهای این بخش به بررسی ایده‌آل‌ها برخواهیم گشت. اکنون به بررسی تجزیه در دامنه $\mathbb{Z}[\sqrt{d}]$ می‌پردازیم. این دامنه‌ها مشابه دامنه‌های کومر هستند و به طور ساده‌ای مسائلی را که او با آنها مواجه بود و روش جواب او را نشان می‌دهد. فرض می‌کنیم که عدد صحیح d، مربع ـ آزاد است، بدین معنی که d دارای هیچ عامل صحیح به‌صورت c^2 نیست (البته بجز $(\pm 1)^2$). تابع زیر کلید تجزیه در $\mathbb{Z}[\sqrt{d}]$ است.

تعریف. تابع $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ که توسط

$$N(s + t\sqrt{d}) = (s + t\sqrt{d})(s - t\sqrt{d}) = s^2 - dt^2$$

داده شده است، تابع نُرم نامیده می‌شود.

برای مثال در $\mathbb{Z}[\sqrt{3}]$،

$$N(2 - 4\sqrt{3}) = 2^2 - 3(-4)^2 = -44. \quad \text{و} \quad N(5 + 2\sqrt{3}) = 5^2 - 3 \times 2^2 = 13$$

توجه کنید که

وقتی $d < 0$، نرم هر عنصر نامنفی است.

برای مثال در $\mathbb{Z}[\sqrt{-5}]$،

$$N(s + t\sqrt{-5}) = s^2 - (-5)t^2 = s^2 + 5t^2 \geq 0.$$

در بخش قبل دیدیم که تابع نرم، $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ را به یک دامنه اقلیدسی تبدیل می‌کند. هرچند این مطلب در حالت کلی درست نیست، امّا قضیه زیر را در این مورد داریم:

---

۱۵) روش‌های کامپیوتری مدرن نشان داده‌اند که هرگاه n دارای یک عامل اول کوچکتر از ۱۰۰۰۰۰ باشد قضیه فرما درست است، و در ۱۹۸۳، G. Faltings ثابت کرد که برای هر n، حداکثر تعداد متناهی جوابهای صحیح غیرصفر وجود دارد.

قضیه ۱۳.۸. اگر d یک عدد صحیح مربع ـ آزاد باشد، در این صورت برای هر $a, b \in \mathbb{Z}[\sqrt{d}]$،

(۱) $N(a) = ۰$ اگر و تنها اگر $a = ۰$.

(۲) $N(ab) = N(a)N(b)$.

برهان. (۱) اگر $a = s + t\sqrt{d}$، $N(a) = s^۲ - dt^۲$، لذا $N(a) = ۰$ اگر و تنها اگر $s^۲ = dt^۲ \in \mathbb{Z}$. هر عامل اول در تجزیه $s^۲$ و $t^۲$ به تعداد زوجی از دفعات تکرار می‌شود. امّا عوامل اول d تکرار نمی‌شوند زیرا d مربع‌آزاد است. بنابراین اگر p یک عامل اول d باشد، باید به تعداد فردی از دفعات در تجزیه $dt^۲$ اتفاق افتد. بنا به یکتایی تجزیه در $\mathbb{Z}$، معادله $s^۲ = dt^۲$ غیرممکن است مگر این که $t = ۰ = s$، یعنی $a = ۰$.

(۲) فرض کنید $a = r + s\sqrt{d}$ و $b = m + n\sqrt{d}$. اثبات با انجام محاسبه‌ای مستقیم انجام می‌شود (تمرین ۳). ■

قضیه ۱۴.۸. فرض کنید d یک عدد صحیح مربع ـ آزاد باشد. در این صورت $u \in \mathbb{Z}[\sqrt{d}]$ یکه است اگر و تنها اگر $N(u) = \pm ۱$.

برهان. اگر u یکه باشد، در این صورت برای برخی $v \in \mathbb{Z}[\sqrt{d}]$، $uv = ۱$. طبق قضیه ۱۳.۸، $N(u)N(v) = N(uv) = N(۱) = ۱^۲ - d \times ۰^۲ = ۱$. چون $N(u)$ و $N(v)$ اعداد صحیح هستند تنها احتمالات ممکن عبارتند از $N(u) = \pm ۱$ و $N(v) = \pm ۱$. برعکس اگر $u = s + t\sqrt{d}$ و $N(u) = \pm ۱$، قرار دهید $\bar{u} = s - t\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. در این صورت طبق تعریف نرم، $u\bar{u} = N(u) = \pm ۱$. بنابراین $u(\pm\bar{u}) = ۱$ و u یکه است. ■

مثال ۱۴.۸. در $\mathbb{Z}[\sqrt{۲}]$ عنصر $۳ + ۲\sqrt{۲}$ یکه است زیرا $N(۳+۲\sqrt{۲}) = ۳^۲ - ۲ \times ۲^۲ = ۱$. همانگونه که در اثبات بالا نشان داده شد، وارون $۳ + ۲\sqrt{۲}$ عبارت است از $۳ - ۲\sqrt{۲}$. هر توانی از یک یکه خود نیز یکه است، لذا $\mathbb{Z}[\sqrt{۲}]$ دارای تعداد نامتناهی یکه از جمله $(۳ + ۲\sqrt{۲})$، $(۳ + ۲\sqrt{۲})^۲$، $(۳ + ۲\sqrt{۲})^۳$، ... می‌باشد.

برطبق قضیه ۱۴.۸ با یافتن همه جوابهای صحیح (برای s و t) معادلات $s^۲ - dt^۲ = \pm ۱$، می‌توانیم تمام یکه‌های $s + t\sqrt{d}$ در $\mathbb{Z}[\sqrt{d}]$ را تعیین کنیم. وقتی $d > ۱$، این معادلات دارای تعداد نامتناهی جواب می‌باشند (مثال بالا و بارتن [۱۶] [۱۴، صفحه ۳۳۶] را ملاحظه کنید). وقتی

[۱۶] Burton

$d = -1$، این معادلات به معادله $s^2 + t^2 = 1$ کاهش می‌یابد[۱۷]. تنها جوابهای صحیح عبارتند از $s = \pm 1$، $t = 0$ و $s = 0$، $t = \pm 1$. بنابراین تنها یکه‌های $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ عبارتند از ± 1 و $\pm i$. اگر $d < -1$، مثلاً $d = -k$ با $k > 1$، در این صورت معادلات به $s^2 + kt^2 = 1$ کاهش می‌یابد[۱۸]. چون $k > 1$، تنها جوابهای صحیح عبارتند از $s = \pm 1$، $t = 0$. بنابراین نتیجه زیر را داریم.

نتیجه ۱۵.۸. فرض کنید d یک عدد صحیح مربع ـ آزاد باشد. اگر $d > 1$، در این صورت $\mathbb{Z}[\sqrt{d}]$ دارای تعداد نامتناهی یکه است. یکه‌های $\mathbb{Z}[\sqrt{-1}]$ عبارتند از ± 1 و $\pm i$. اگر $d < -1$، در این صورت یکه‌های $\mathbb{Z}[\sqrt{d}]$ عبارتند از ± 1.

نتیجه ۱۶.۸. فرض کنید d یک عدد صحیح مربع ـ آزاد باشد. اگر $p \in \mathbb{Z}[\sqrt{d}]$ و $N(p)$ یک عدد صحیح اول در $\mathbb{Z}$ باشد، در این صورت p در $\mathbb{Z}[\sqrt{d}]$ تحویل‌ناپذیر است.

برهان. چون $N(p)$ اول است، $N(p) \neq \pm 1$، لذا طبق قضیه ۱۴.۸، p در $\mathbb{Z}[\sqrt{d}]$ یکه نیست. اگر $p = ab$ در $\mathbb{Z}[\sqrt{d}]$، در این صورت طبق قضیه ۱۱.۸، $N(p) = N(a)N(b)$ در $\mathbb{Z}$. چون $N(a)$، $N(b)$ و $N(p)$ اعداد صحیح هستند و $N(p)$ اول است باید داشته باشیم $N(a) = \pm 1$ یا $N(b) = \pm 1$. بنابراین طبق قضیه ۱۴.۸، a یا b یکه است. پس طبق قضیه ۱.۸، p تحویل‌ناپذیر است. ■

مثال ۱۵.۸. عنصر $i - 1$ در $\mathbb{Z}[i]$ تحویل‌ناپذیر است زیرا $N(1 - \sqrt{-1}) = 2$. به طور مشابه $i + 1$ نیز تحویل‌ناپذیر است. بنابراین تجزیه ۲ به عنوان حاصل‌ضربی از عناصر تحویل‌ناپذیر در $\mathbb{Z}[i]$ به‌صورت $2 = (1 + i)(1 - i)$ می‌باشد.

عکس نتیجه ۱۶.۸ غلط است. برای نمونه، در $\mathbb{Z}[\sqrt{-5}]$ نرم $\sqrt{-5} + 1$ برابر ۶ است که اول نمی‌باشد. امّا مثال بعدی نشان می‌دهد که $\sqrt{-5} + 1$ تحویل‌ناپذیر است.

مثال ۱۶.۸. برای نشان دادن این که $\sqrt{-5} + 1$ در $\mathbb{Z}[\sqrt{-5}]$ تحویل‌ناپذیر است، فرض کنید $\sqrt{-5} + 1 = ab$. طبق قضیه ۱.۸، تنها لازم است نشان دهیم که a یا b یکه هستند. طبق

۱۷) جواب ۱- غیرممکن است زیرا طرف چپ معادله همواره نامنفی است.

۱۸) پاورقی ۱۷ را ملاحظه کنید.

قضیه ۱۳.۸، $N(a)N(b) = N(ab) = N(۱ + \sqrt{-۵}) = ۶$. چون $N(a)$ و $N(b)$ اعداد صحیح نامنفی هستند، تنها احتمالات ممکن برای $N(a)$ عبارت از ۲، ۳، یا ۶ می‌باشد. اگر $a = s + t\sqrt{-۵}$ و $N(a) = ۲$، در این صورت $s^۲ + ۵t^۲ = ۲$. به‌سادگی می‌توان دید که این معادله دارای هیچ جواب صحیحی برای s و t نیست؛ بنابراین $N(a) = ۲$ غیر ممکن است. استدلالی مشابه نشان می‌دهد که $N(a) = ۳$ نیز غیرممکن است. اگر $N(a) = ۱$، در این صورت طبق قضیه ۱۴.۸، a یکه است. اگر $N(a) = ۶$، در این صورت $N(b) = ۱$ و b یکه است. بنابراین $۱ + \sqrt{-۵}$ تحویل‌ناپذیر است.

پیشتر مثالی از یک دامنه صحیح را که یک عضو غیریکه غیرصفر آن قابل تجزیه به‌صورت حاصل‌ضربی از عوامل تحویل‌ناپذیر نیست دیده‌ایم (تمرین ۳۰ در بخش ۱.۸). اینک می‌بینیم که $\mathbb{Z}[\sqrt{d}]$ نیز ممکن است به‌خاطر دلیلی متفاوت یک **دی‌ت** نباشد، البته تجزیه عناصر به صورت حاصل‌ضربی از عوامل تحویل‌ناپذیر در $\mathbb{Z}[\sqrt{d}]$ همواره ممکن است، اما این تجزیه امکان‌پذیر است یکتا نباشد.

قضیه ۱۷.۸. فرض کنید d یک عدد صحیح مربع‌آزاد باشد. در این صورت هر عضو غیریکه، غیرصفر در $\mathbb{Z}[\sqrt{d}]$ حاصل‌ضربی از عناصر تحویل‌ناپذیر است[۱۹].

برهان. فرض کنید S مجموعه همه غیریکه‌های غیرصفر در $\mathbb{Z}[\sqrt{d}]$ باشد که حاصل‌ضربی از عناصر تحویل‌ناپذیر نیستند. باید نشان دهیم که S تهی است. به خلاف فرض کنید که S غیرتهی باشد. در این صورت مجموعه $W = \{|\, N(t) \,|: t \in S\}$ مجموعه‌ای غیرتهی از اعداد صحیح مثبت است. طبق اصل خوش‌ترتیبی W دارای یک کوچکترین عضو است. پس عنصر $a \in S$ وجود دارد به قسمی که برای هر $|\, N(a) \,| \leq |\, N(t) \,| : t \in S$. چون $a \in S$، لذا خود a تحویل‌ناپذیر نیست. بنابراین غیریکه‌های $b, c \in \mathbb{Z}[\sqrt{d}]$ وجود دارند به قسمی که $a = bc$. حداقل یکی از b، c باید در S باشد (در غیر این‌صورت a باید حاصل‌ضربی از عناصر تحویل‌ناپذیر باشد و بنابراین در S نیست)، مثلاً $b \in S$. چون b و c غیریکه‌اند طبق قضیه ۱۴.۸، $|\, N(b) \,| > ۱$ و $|\, N(c) \,| > ۱$. امّا طبق قضیه ۱۳.۸، $|\, N(a) \,| = |\, N(b) \,|\, |\, N(c) \,|$ لذا باید داشته باشیم $|\, N(a) \,| > |\, N(b) \,| > ۱$. اما $b \in S$، پس بدلیل انتخاب a، $|\, N(a) \,| \leq |\, N(b) \,|$ که یک تناقض است. بنابراین S تهی است. این اثبات قضیه را کامل می‌کند. ■

۱۹) طبق معمول، ما یک "حاصل‌ضرب" با تنها یک عامل را می‌پذیریم.

مثال ۱۷.۸. دامنه $\mathbb{Z}[\sqrt{-5}]$ یک دامنه یکتایی تجزیه نیست. عضو ۶ در $\mathbb{Z}[\sqrt{-5}]$ دارای دو تجزیه است:

$$۶ = ۲ \times ۳ \quad \text{و} \quad ۶ = (۱ + \sqrt{-5})(۱ - \sqrt{-5}).$$

اثبات این‌که $۱ + \sqrt{-5}$ تحویل‌ناپذیر است در مثال قبل از قضیه ۱۷.۸ آمده‌است. اثبات این‌که ۲، ۳ و $۱ - \sqrt{-5}$ تحویل‌ناپذیرند مشابه می‌باشد. برای مثال، اگر $ab = ۲$، در این صورت $N(a)N(b) = N(ab) = N(۲) = ۴$، لذا $N(a)$ برابر ۱، ۲ یا ۴ است. امّا $N(a) = ۲$ غیرممکن است زیرا معادلهٔ $s^۲ + ۵t^۲ = ۲$ دارای هیچ جواب عدد صحیحی نیست. بنابراین یا $N(a) = ۱$ و a یکه است یا $N(a) = ۴$. در حالت دوّم $N(b) = ۱$ و b یکه است. بنابراین طبق قضیه ۱.۸، ۲ تحویل‌ناپذیر است. چون تنها یکه‌های $\mathbb{Z}[\sqrt{-5}]$ عبارتند از ± ۱، به‌وضوح هیچ کدام از ۲ یا ۳ یک وابسته $\sqrt{-5} + ۱$ یا $\sqrt{-5} - ۱$ نیست. بنابراین با تقریب وابسته‌ها، تجزیه ۶ به‌عنوان حاصل‌ضربی از عوامل تحویل‌ناپذیر یکتا نیست و $\mathbb{Z}[\sqrt{-5}]$ یک **دی‌ت** نمی‌باشد.

مثال قبلی نشان می‌دهد که عنصر تحویل‌ناپذیر ۲، عضو $(\sqrt{-5} - ۱)(\sqrt{-5} + ۱)$ را در $\mathbb{Z}[\sqrt{-5}]$ می‌شمارد، اما هیچ‌کدام از عناصر $\sqrt{-5} + ۱$ و $\sqrt{-5} - ۱$ را نمی‌شمارد. بنابراین وقتی که یکتایی تجزیه برقرار نیست، یک عنصر تحویل‌ناپذیر p، ممکن است فاقد این خاصیت باشد که $p|cd$ نتیجه دهد $p|c$ یا $p|d$"[۲۰]. پیامد دیگری از فقدان یکتایی تجزیه، احتمال عدم وجود بزرگترین مقسوم‌علیه مشترک است (تمرین ۱۳).

اینک در همان وضعیتی هستیم که کومر[۲۱] در بیش از یک قرن و نیم پیش قرار داشت، و پرسش این است که: چگونه می‌توان نوعی از یکتایی تجزیه را در دامنه‌هایی نظیر $\mathbb{Z}[\sqrt{-5}]$ برقرار نمود؟ پاسخ کومر، تمرکز روی ایده‌آل‌ها به جای عناصر بود[۲۲]. **حاصل‌ضرب** IJ از دو ایده‌آل I و J بنابه تعریف عبارت است از مجموع همه عناصری به صورت ab که در آن $a \in I$ و $b \in J$؛ یعنی

$$IJ = \{a_۱b_۱ + a_۲b_۲ + \cdots + a_nb_n | n \geq ۱, a_k \in I, b_k \in J\}.$$

تمرین ۲۰ بخش ۱.۶ نشان می‌دهد که IJ یک ایده‌آل است. کومر به جای تجزیه یک عنصر a به

۲۰) از دیدگاه قضیه ۷.۸، این چندان تعجب‌آور نیست.

۲۱) Kummer

۲۲) کومر اصطلاح علمی دیگری را به جای کلمه ایده‌آل بکار برد. البته ایده‌آل‌ها همان مفاهیمی را در بردارند که مورد نظر کومر بود. اصطلاح علمی جدید ایده‌آل که ما آن را اینجا به کار می‌بریم توسط R. Dedekind که قضیه کومر را تعمیم داد، معرفی شد.

حاصل‌ضرب عناصر تحویل‌ناپذیر، ایده‌آل اصلی (a) را به حاصل‌ضربی از ایده‌آل‌های اول تجزیه کرد.

مثال ۱۸.۸. می‌خواهیم ایده‌آل اصلی (۶) در $\mathbb{Z}[\sqrt{-5}]$ را به حاصل‌ضربی از ایده‌آل‌های اوّل تجزیه کنیم. طبیعی است که کار خود را با تجزیه ۶ به اعداد اول $۶ = ۲ \times ۳$ شروع کنیم. به سادگی می‌توان دید که ایده‌آل (۶) برابر ایده‌آل حاصل‌ضرب (۳)(۲) می‌باشد (تمرین ۱۶). امّا (۲) یک ایده‌آل اول نیست (برای مثال در (۲) داریم $۶ = (۱ - \sqrt{-5})(۱ + \sqrt{-5})$ امّا هیچ یک از عوامل این تجزیه در (۲) قرار ندارند). بنابراین باید به طریق دیگری عمل کنیم. فرض کنید P ایده‌آلی در $\mathbb{Z}[\sqrt{-5}]$ باشد که توسط ۲ و $۱ + \sqrt{-5}$ تولید شده است، یعنی

$$P = \{۲a + (۱ + \sqrt{-5})b \mid a, b \in \mathbb{Z}[\sqrt{-5}]\}.$$

طبق تمرین ۱۴ بخش ۲.۸، P یک ایده‌آل است. تمرین ۱۷ نشان می‌دهد که $r + s\sqrt{-5} \in P$ اگر و تنها اگر r و s یا هر دو زوج و یا هر دو فرد باشند. در نتیجه تنها هم‌مجموعه‌های متمایز در $\mathbb{Z}[\sqrt{-5}]/P$ عبارتند از $P + ۰$ و $P + ۱$؛ برای این‌که اگر در عضو دلخواه $m + n\sqrt{-5}$، m فرد و n زوج باشد در این صورت $(m + n\sqrt{-5}) - ۱ = (m - ۱) + n\sqrt{-5} \in P$ زیرا $m - ۱$ و n زوج هستند. بنابراین $(m + n\sqrt{-5}) + P = ۱ + P$. به‌طور مشابه اگر m زوج و n فرد باشد، در این صورت $(m - ۱) + n\sqrt{-5} \in P$ زیرا $m - ۱$ و n فرد هستند. در نتیجه حلقه خارج قسمتی $\mathbb{Z}[\sqrt{-5}]/P$ یکریخت با $\mathbb{Z}_۲$ است. بنابراین طبق قضیه ۱۲.۶، P یک ایده‌آل اول در $\mathbb{Z}[\sqrt{-5}]$ است. استدلالی مشابه (تمرین ۱۹) نشان می‌دهد که $Q_۱$ و $Q_۲$ ایده‌آلهایی اول می‌باشند، جایی که

$$Q_۱ = \{۳a + (۱ + \sqrt{-5})b \mid a, b \in \mathbb{Z}[\sqrt{-5}]\},$$
$$Q_۲ = \{۳a + (۱ - \sqrt{-5})b \mid a, b \in \mathbb{Z}[\sqrt{-5}]\}.$$

تمرین‌های ۱۸ و ۱۹ نشان می‌دهند که ایده‌آل حاصل‌ضرب $P^۲ = PP$ دقیقاً برابر ایده‌آل (۲) است و این‌که $(۳) = Q_۱Q_۲$. بنابراین ایده‌آل (۶) حاصل‌ضربی از چهار ایده‌آل اول می‌باشد: $(۶) = (۲)(۳) = P^۲Q_۱Q_۲$.

کومر موفق شد نشان دهد که در دامنه‌های مورد نظر او، بجز احتمالاً در ترتیب عوامل، تجزیه یک ایده‌آل به حاصل ضربی از ایده‌آل‌های اول یکتاست. این نتیجه بعداً توسط ددکیند[۲۳] تعمیم داده شد.

۲۳) R. Dedekind

به منظور بیان دقیق این تعمیم لازم است برخی مقدمات را ذکر نماییم.

یک **عدد جبری** عبارت است از یک عدد مختلط که ریشه یک چندجمله‌ای تکین ناصفر با ضرایب گویا باشد. اگر t یک عدد جبری بوده و ریشه یک چندجمله‌ای از درجه n در $\mathbb{Q}[x]$ باشد، در این صورت $\mathbb{Q}(t) = \{a_0 + a_1 t + a_2 t^2 + \cdots + a_{n-1} t^{n-1} | a_i \in \mathbb{Q}\}$ یک زیرمیدان $\mathbb{C}$ است و هر عضو $\mathbb{Q}(t)$ یک عدد جبری است[۲۴]. یک **عدد صحیح جبری** عبارت است از یک عدد مختلط که ریشه یک چندجمله‌ای تکین ناصفر با ضرایب صحیح باشد. می‌توان نشان داد که مجموعه همه اعداد صحیح جبری در $\mathbb{Q}(t)$، یک دامنه صحیح است (بیرخوف و مک لین [۲۵] [۱؛ صفحه ۴۴۵] را ملاحظه کنید). اگر w یک ریشه مختلط $x^p - 1$ باشد در این صورت دامنه $\mathbb{Z}[w]$ که کومر مورد استفاده قرار داد، در واقع دامنه همه اعداد صحیح جبری در $\mathbb{Q}(w)$ است (آریلند و رُزِن[۲۶] [۱۶؛ صفحه ۱۹۹] را ملاحظه کنید). بنابراین نتایج کومر حالت خاصی از قضیه زیر می‌باشد.

قضیه ۱۸.۸. فرض کنید t یک عدد جبری و R دامنه همه اعداد صحیح جبری در $\mathbb{Q}(t)$ باشد. در این صورت هر ایده‌آل در R (بجز ۰ و R) حاصل‌ضربی از ایده‌آل‌های اول است و این تجزیه، بجز در ترتیب عوامل، یکتاست.

برای دیدن برهانی از این قضیه، آریلند و رزن [۱۶؛ صفحه ۱۹۹] را ملاحظه کنید.

بیشتر حلقه‌های $\mathbb{Z}[\sqrt{d}]$ نیز حالات خاصی از قضیه ۱۸.۸ می‌باشند، زیرا اگر d یک عدد صحیح مربع ـ آزاد باشد، در این صورت $t = \sqrt{d}$ یک عدد جبری است (زیرا یک ریشه $x^2 - d$ است) و $\mathbb{Q}(\sqrt{d}) = \{a_0 + a_1\sqrt{d} | a_i \in \mathbb{Q}\}$. اعداد صحیح جبری در میدان $\mathbb{Q}(\sqrt{d})$، **اعداد صحیح درجه دوم** نامیده می‌شوند. هر عضو $r + s\sqrt{d}$ از حلقه $\mathbb{Z}[\sqrt{d}]$ یک عدد صحیح درجه دوم در $\mathbb{Q}(\sqrt{d})$ است زیرا ریشه یک چندجمله‌ای تکین در $\mathbb{Z}[x]$ می‌باشد:

$$x^2 - 2rx + (r^2 - ds^2) = (x - (r + s\sqrt{d}))(x - (r - s\sqrt{d})).$$

هنگامی که (پیمانه ۴) $d \equiv 3$ یا 2، در این صورت $\mathbb{Z}[\sqrt{d}]$ عبارت از دامنه R، متشکل از همه اعداد صحیح درجه دوم در $\mathbb{Q}(\sqrt{d})$ است، امّا وقتی (پیمانه ۴) $d \equiv 1$، اعداد صحیح درجه دومی در

۲۴) برهانی از این مطلب را در قضایای ۷.۹ و ۹.۹ ملاحظه کنید.

۲۵) MacLane and Birkhoff

۲۶) Rosen and Ireland

۲۷) چون d است لذا (پیمانه ۴) $d \not\equiv 0$.

R وجود دارند که در $\mathbb{Z}[\sqrt{d}]$ نیستند (تمرین ۲۱ را ملاحظه کنید)[۲۷]. در رابینسون[۲۸] [۲۱]، برهانی مقدماتی از قضیه ۱۸.۸ برای حالت اعداد صحیح درجه دوّم ارائه شده است.

قضیه ۱۸.۸ در نظریه اعداد جبری بسیار مفید واقع شده است. با این حال این قضیه به بسیاری از سوالات در مورد یکتایی تجزیه عناصر پاسخ نمی‌دهد، مثلاً: اگر R دامنه همه اعداد صحیح درجه دوم در $\mathbb{Q}(\sqrt{d})$ باشد، برای چه مقادیری از d، R یک **دی‌ت** است؟ وقتی که $d < 0$، R یک **دی‌ت** است اگر و تنها اگر d یکی از اعداد ۱-، ۲-، ۳-، ۷-، ۱۱-، ۱۹-، ۴۳-، ۶۷-، ۱۶۳- باشد (استارک[۲۹] [۲۲] را ملاحظه کنید). وقتی $d > 0$، ثابت شده است که برای dهایی مثل ۲، ۳، ۵، ۶، ۷، ۱۱، ۱۳، ۱۷، ۱۹، ۲۱،۲۲، ۲۳، ۲۹ و بسیاری مقادیر دیگر، R یک **دی‌ت** است، اما در این حالت هیچ فهرست کاملی مانند آنچه برای حالت $d < 0$ ارائه شد وجود ندارد. حدس زده شده است که برای تعداد نامتناهی مقادیر d، R یک **دی‌ت** است.

تمرینها

۱.A. اگر $x^k + y^k = z^k$ دارای هیچ جواب صحیح غیرصفر نباشد و $k|n$، در این صورت نشان دهید که $x^n + y^n = z^n$ نیز دارای هیچ جواب صحیح غیرصفری نیست.

۲. فرض کنید w یک عدد مختلط باشد به طوریکه $w^p = 1$. نشان دهید که $\mathbb{Z}[w] = \{a_0 + a_1 w + a_2 w^2 + \cdots + a_{p-1} w^{p-1} | a_i \in \mathbb{Z}\}$ یک دامنه صحیح است. [راهنمایی: $w^p = 1$ نتیجه می‌دهد $w^{p+1} = w$ و $w^{p+2} = w^2$ و غیره.]

۳. اگر $a = r + s\sqrt{d}$ و $b = m + n\sqrt{d}$ عناصری از $\mathbb{Z}[\sqrt{d}]$ باشند، نشان دهید که $N(ab) = N(a)N(b)$.

۴. توضیح دهید که چرا برای هیچ تابع δ، $\mathbb{Z}[\sqrt{-5}]$ یک دامنه اقلیدسی نیست.

۵. اگر $a \in \mathbb{Q}$ یک عدد صحیح جبری باشد (که در بند قبل از قضیه ۱۸.۸ تعریف شد) نشان دهید که $a \in \mathbb{Z}$. [راهنمایی: قضیه ۱۶.۴.]

۶.B. درکدام یک از دامنه‌های زیر، عدد ۵ یک عضو تحویل‌ناپذیر است؟

(الف) $\mathbb{Z}$ (ب) $\mathbb{Z}[i]$ (پ) $\mathbb{Z}[\sqrt{-2}]$

۲۸) Robinson

۲۹) Stark

۷. در $\mathbb{Z}[\sqrt{-۷}]$، عدد ۸ را به هر دو صورت حاصل‌ضربی از دو عضو تحویل‌ناپذیر و حاصل‌ضربی از سه عضو تحویل‌ناپذیر تجزیه کنید. [راهنمایی: حاصل‌ضرب $(۱+\sqrt{-۷})(۱-\sqrt{-۷})$ را در نظر بگیرید.]

۸. هر یک از عناصر زیر را به صورت حاصل‌ضربی از عناصر تحویل‌ناپذیر در $\mathbb{Z}[i]$ تجزیه کنید. [راهنمایی: نرم هر عامل a باید $N(a)$ را بشمارد.]

(الف) ۳ (ب) ۷ (پ) $۴+۳i$ (ت) $۱۱+۷i$

۹. (الف) بررسی کنید که هر کدام از عناصر $۲+۵\sqrt{۲}$، $-۲+\sqrt{۲}$، $۱۱-۷\sqrt{۲}$ و $۲+\sqrt{۲}$ در $\mathbb{Z}[\sqrt{۲}]$ تحویل‌ناپذیر است.

(ب) توضیح دهید که چرا برابری

$$(۵+\sqrt{۲})(۲-\sqrt{۲}) = (۱۱-۷\sqrt{۲})(۲+\sqrt{۲})$$

دامنه یکتایی تجزیه در $\mathbb{Z}[\sqrt{۲}]$ را نقض نمی‌کند.

۱۰. دو تجزیه متفاوت از ۹ به عنوان حاصل‌ضربی از عوامل تحویل‌ناپذیردر $\mathbb{Z}[\sqrt{-۵}]$ بیابید.

۱۱. نشان دهید که $\mathbb{Z}[\sqrt{-۶}]$ یک **دی‌ت** نیست. [راهنمایی: ۱۰ را به دو روش مختلف تجزیه کنید.]

۱۲. نشان دهید که $\mathbb{Z}[\sqrt{۱۰}]$ یک **دی‌ت** نیست. [راهنمایی: ۶ را به دو روش مختلف تجزیه کنید.]

۱۳. نشان دهید که ۶ و $۲+۲\sqrt{-۵}$ دارای هیچ بزرگترین مقسوم‌علیه مشترک در $\mathbb{Z}[\sqrt{-۵}]$ نیستند. [راهنمایی: اگر a یک مقسوم‌علیه مشترک ۶ و $۲+۲\sqrt{-۵}$ باشد، در این صورت نُرم آن باید هر دو $N(۶)=۳۶$ و $N(۲+۲\sqrt{-۵})=۲۴$ را بشمارد؛ بنابراین $a=r+s\sqrt{-۵}$ با $r^۲+۵s^۲=N(a)=۱,۲,۳,۴,۶,۱۲$. با استفاده از این مطلب مقسوم‌علیه‌های مشترک را بیابید. بررسی کنید که هیچ کدام یک شمارنده بقیه نیست، چنانچه این امر لازمه **ب‌م‌م** بودن است. مثال ۱۷.۸ را نیز ملاحظه کنید.]

۱۴. نشان دهید که ۱ یک **ب‌م‌م** ۲ و $۱+\sqrt{-۵}$ در $\mathbb{Z}[\sqrt{-۵}]$ است امّا ۱ را نمی‌توان به صورت $۲a+(۱+\sqrt{-۵})b$ نوشت که در آن $a,b\in\mathbb{Z}[\sqrt{-۵}]$.

۱۵. ثابت کنید که هر ایده‌آل اصلی در یک **دی‌ت** به طور منحصربه‌فرد، به جز در ترتیب عوامل، حاصل‌ضربی از ایده‌آل‌های اول است.

۱۶. نشان دهید که در $\mathbb{Z}[\sqrt{-5}]$، $(3)(2) = (6)$. (حاصل‌ضرب ایده‌آل‌ها در بند قبل از مثال ۱۸.۸ تعریف شده‌است.)

۱۷. فرض کنید P ایده‌آل $\{2a + (1 + \sqrt{-5})b \mid a, b \in \mathbb{Z}[\sqrt{-5}]\}$ در $\mathbb{Z}[\sqrt{-5}]$ باشد. ثابت کنید $r + s\sqrt{-5} \in P$ اگر و تنها اگر (پیمانه ۲) $r \equiv s$ (یعنی r و s هردو زوج و یا هردو فردند).

۱۸. فرض کنید P مانند تمرین ۱۷ باشد. ثابت کنید P^2 ایده‌آل اصلی (۲) است.

۱۹. فرض کنید Q_1 ایده‌آل $\{3a + (1 + \sqrt{-5})b \mid a, b \in \mathbb{Z}[\sqrt{-5}]\}$ و Q_2 ایده‌آل $\{3a + (1 - \sqrt{-5})b \mid a, b \in \mathbb{Z}[\sqrt{-5}]\}$ در $\mathbb{Z}[\sqrt{-5}]$ باشد.

(الف) ثابت کنید که $r + s\sqrt{-5} \in Q_1$ اگر و تنها اگر (پیمانه ۳) $r \equiv s$.

(ب) نشان دهید که $\mathbb{Z}[\sqrt{-5}]/Q_1$ دارای دقیقاً سه هم‌مجموعهٔ متمایز است.

(پ) ثابت کنید که $\mathbb{Z}[\sqrt{-5}]/Q_1$ یکریخت با $\mathbb{Z}_3$ است؛ نتیجه‌گیری کنید که Q_1 یک ایده‌آل اول است.

(ت) ثابت کنید که $Q_1Q_2 = (3)$ یک ایده‌آل اول است. [راهنمایی: قسمت‌های (الف)ـ(پ) را تطبیق دهید.]

۲۰. اگر $r + s\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ با $s \neq 0$، در این صورت ثابت کنید که ۲ در ایده‌آل اصلی $(r + s\sqrt{-5})$ نیست.

۲۱.C. فرض کنید d یک عدد صحیح مربع ـ آزاد باشد و فرض کنید $\mathbb{Q}(\sqrt{d})$ مجموعه تعریف شده در بند بعد از قضیه ۱۸.۸ باشد. می‌دانیم که $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}(\sqrt{d})$ و هر عضو $\mathbb{Z}[\sqrt{d}]$ یک عدد صحیح درجه دوم است. مطابق آنچه درپی می‌آید همه اعداد صحیح درجه دوم را در $\mathbb{Q}(\sqrt{d})$ تعیین کنید.

(الف) نشان دهید که هر عضو $\mathbb{Q}(\sqrt{d})$ به صورت $(r + s\sqrt{d})/t$ است که در آن $r, s, t \in \mathbb{Z}$ و ب.م.م (r, s, t) برابر ۱ است. از اینجا به بعد، $a = (r + s\sqrt{d})/t$ را عضو دلخواهی از $\mathbb{Q}(\sqrt{d})$ در نظر می‌گیریم.

(ب) نشان دهید که a یک ریشهٔ

$$p(x) = x^2 - (\frac{2r}{t})x + (\frac{r^2 - ds^2}{t^2}) \in \mathbb{Q}[x]$$

است. [راهنمایی: نشان دهید که $p(x) = (x-a)(x-\bar{a})$ که در آن $\bar{a} = (r - s\sqrt{d})/t$.]

(پ) اگر $s \neq 0$ نشان دهید که $p(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

(ت) ثابت کنید که a یک عدد صحیح درجه دوم است اگر و تنها اگر $p(x)$ دارای ضرایب صحیح باشد. [راهنمایی: اگر $s = 0$، تمرین ۵ را بکار برید؛ اگر $s \neq 0$ و a ریشه یک چندجمله‌ای تکین $f(x) \in \mathbb{Z}[x]$ باشد، قضیه ۱۸.۴ را بکار برید تا نشان دهید که a ریشه‌ای از چندجمله‌ای تکین $g(x) \in \mathbb{Z}[x]$ است، که در آن $g(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. قسمت (پ) و قضیه ۱۰.۴ را بکار برید تا نشان دهید که $g(x) = p(x)$.]

(ث) اگر a یک عدد صحیح درجه دوم باشد نشان دهید که $t|2r$ و $t^2|4ds^2$. با بکار بردن این حقیقت نشان دهید که t باید برابر ۱ یا ۲ باشد. [راهنمایی: d مربع‌ـ آزاد است، $(r, s, t) = 1$؛ (ب) و (ت) را بکار برید.]

(ج) اگر (پیمانه ۴) $d \equiv 3$ یا 2، نشان دهید که a یک عدد صحیح درجه دوم است اگر و تنها اگر $t = 1$. [راهنمایی: اگر $t = 2$، آنگاه طبق (ب) و (ت)، (پیمانه ۴) $r^2 \equiv ds^2$. اگر s زوج باشد از این حقیقت که $(r, s, t) = 1$ به یک تناقض برسید؛ اگر s فرد باشد تمرین ۵ بخش ۱.۲ را بکار برید تا به یک تناقض برسید.]

(چ) اگر (پیمانه ۴) $d \equiv 1$ و $a \in \mathbb{Q}(\sqrt{d})$، نشان دهید که a یک عدد صحیح درجه دوم است اگر و تنها اگر $t = 1$ یا $t = 2$ و هر دو r و s فرد باشند. [راهنمایی: (ت) را بکار برید.]

(ح) با استفاده از قسمت‌های (ج) و (چ) نشان دهید که اگر (پیمانه ۴) $d \equiv 3$ یا 2، آنگاه مجموعه همه اعداد صحیح درجه دوم، مجموعه $\mathbb{Z}[\sqrt{d}]$ است و اگر (پیمانه ۴) $d \equiv 1$، آنگاه مجموعه همه اعداد صحیح درجه دوم، مجموعه $\{m + n\sqrt{d}/2 \mid m, n \in \mathbb{Z}$ و $m \equiv n$ (پیمانه ۲)$\}$ است.

۴-۸ میدان خارج قسمتهای یک دامنه صحیح[۳۰]

برای هر دامنه صحیح R می‌خواهیم میدان $\mathbb{F}$ را چنان بسازیم که R را شامل بوده و متشکل از همهٔ "خارج قسمتهای" عناصر R باشد. وقتی که دامنهٔ R، حلقهٔ $\mathbb{Z}$ باشد، در این صورت $\mathbb{F}$ میدان اعداد گویای $\mathbb{Q}$ است. پس این فرآیند را می‌توان فرمول‌بندی دقیقی از ساختن $\mathbb{Q}$ توسط $\mathbb{Z}$ و یا به عنوان تعمیمی از این ساختار، به دامنه‌های صحیح دلخواه در نظر گرفت. در بخش ۵.۸، میدان $\mathbb{F}$ ابزار اساسی برای مطالعه تجزیه در $R[x]$ خواهد بود.

تجربه گذشته ما در کار با اعداد گویا ما را در این فرمول‌بندی رسمی هدایت خواهد کرد. با این حال همه اثبات‌ها مستقل از هر دانش قبلی از اعداد گویا است.

یک عدد گویای a/b توسط زوج اعداد صحیح a و b (با $b \neq 0$) مشخص می‌شود. امّا زوج‌های مختلف ممکن است معرف یک عدد گویا باشند: به‌عنوان مثال، $۴/۸ = ۳/۶ = ۱/۲$، و در حالت کلّی

$$\frac{a}{b} = \frac{c}{d} \quad \text{اگر و تنها اگر} \quad ad = bc.$$

این پیشنهاد می‌کند که اعداد گویا از نوعی رابطهٔ هم‌ارزی روی زوج‌های اعداد صحیح (زوجهای هم‌ارز، عدد گویای یکسانی را تعیین می‌کنند) بدست می‌آیند. اکنون به فرمول‌بندی این ایده می‌پردازیم.

فرض کنید R یک دامنهٔ صحیح و S مجموعه زیر از زوج‌های عناصر موجود در R باشد:

$$S = \{(a,b) \mid a,b \in R, b \neq 0_R\}.$$

رابطه $\sim$ را روی S به صورت زیر تعریف کنید:

$$(a,b) \sim (c,d) \quad \text{اگر و تنها اگر} \quad ad = bc \text{ در } R.$$

قضیه ۱۹.۸. رابطه $\sim$ یک رابطهٔ هم‌ارزی روی S است.

برهان. انعکاسی: چون R جابجایی است $ab = ba$، بنابراین برای هر زوج (a,b) در S $(a,b) \sim (a,b)$. متقارن: اگر $(a,b) \sim (c,d)$، در این صورت $ad = bc$. بنا به خاصیت جابجایی $cb = da$، بنابراین $(c,d) \sim (a,b)$. متعدی: فرض کنید که $(a,b) \sim (c,d)$ و $(c,d) \sim (r,s)$. در این صورت $ad = bc$ و $cs = dr$. از ضرب s در دو طرف $ad = bc$ و بکار بردن این که $cs = dr$ بدست می‌آوریم $ads = (bc)s = b(cs) = bdr$. چون طبق تعریف

۳۰) این بخش مستقل از بقیه فصل ۸ است. پیش‌نیازهای این بخش فصل ۳ و پیوست ت می‌باشد.

S، $d \neq 0_R$ و چون R یک دامنه صحیح است می‌توانیم d را از دو طرف $ads = bdr$ حذف کنیم و نتیجه‌گیری کنیم که $as = br$. بنابراین $(a,b) \sim (r,s)$. ■

طبق نتیجه ت.۲ در پیوست ت، رابطهٔ هم‌ارزی $\sim$، S را به کلاس‌های هم‌ارزی متمایز افراز می‌کند. برای راحتی، کلاس هم‌ارزی (a,b) را با $[a,b]$ به جای نماد پیچیده‌تر $[(a,b)]$ نشان می‌دهیم. فرض کنید $\mathbb{F}$ مجموعهٔ همهٔ کلاس‌های هم‌ارزی تحت رابطهٔ $\sim$ را نشان دهد. توجه کنید که طبق قضیهٔ ت.۱،

$$[a,b] = [c,d] \text{ در } \mathbb{F} \quad \text{اگر و تنها اگر} \quad (a,b) \sim (c,d) \text{ در } S.$$

بنابراین طبق تعریف $\sim$،

$$[a,b] = [c,d] \text{ در } \mathbb{F} \quad \text{اگر و تنها اگر} \quad ad = bc \text{ در } R.$$

می‌خواهیم $\mathbb{F}$ را به یک میدان تبدیل کنیم. جمع و ضرب کلاس‌های هم‌ارزی توسط برابری‌های

$$[a,b] + [c,d] = [ad + bc, bd]$$

و

$$[a,b][c,d] = [ac, bd]$$

تعریف می‌شوند[۳۱]. برای این‌که نشان دهیم این تعاریف با معنی هستند، ابتدا باید ثابت کنیم طرف راست هر دو علامت برابری در واقع عناصری از مجموعهٔ $\mathbb{F}$ هستند. حال $[a,b]$ کلاس هم‌ارزی زوج (a,b) در S است. بنابه تعریف S داریم: $b \neq 0_R$؛ به طور مشابه، $d \neq 0_R$. چون R یک دامنهٔ صحیح است، $bd \neq 0_R$. بنابراین $(ad + bc, bd)$ و (ac, bd) در S قرار دارند، لذا کلاس‌های هم‌ارزی $[ad + bc, bd]$ و $[ac, bd]$ عناصری از $\mathbb{F}$ هستند. اما کار بیشتری برای نشان دادن این‌که جمع و ضرب در $\mathbb{F}$ خوش‌تعریف هستند لازم است.

در حسابان معمولی، $\frac{۳}{۱۰} = \frac{۳}{۵} \times \frac{۱}{۲}$ و جایگزین کردن $\frac{۱}{۲}$ توسط $\frac{۴}{۸}$ همان جواب را بدست می‌دهد، زیرا $\frac{۳}{۱۰} = \frac{۱۲}{۴۰} = \frac{۳}{۵} \times \frac{۴}{۸}$. این جواب بستگی به این که کسرها چگونه نمایش داده می‌شوند ندارد.

۳۱) این تعاریف از قوانین حسابان برای اعداد گویا الهام گرفته شده است (تنها کسر r/s را با کلاس هم‌ارزی $[r,s]$ جایگزین کنید):

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{و} \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

به طور مشابه، باید نشان دهیم جمع و ضرب در $\mathbb{F}$ به انتخاب نماینده‌های کلاس‌های هم‌ارزی بستگی ندارد.

لم ۲۰.۸. جمع و ضرب در $\mathbb{F}$ به انتخاب نماینده کلاس‌های هم‌ارزی بستگی ندارد. به عبارت دیگر اگر $[a,b]=[a',b']$ و $[c,d]=[c',d']$، دراین صورت

$$[ad+bc,bd]=[a'd'+b'c',b'd']$$

و

$$[ac,bd]=[a'c',b'd'].$$

برهان. همانگونه که در بالا توجه داده شد برابری $[ab+bc,bd]=[a'd'+b'c',b'd']$ در $\mathbb{F}$ برقرار است اگر و تنها اگر برابری $(ad+bc)b'd'=bd(a'd'+b'c')$ در R برقرار باشد. بنابراین باید برابری آخری را ثابت کنیم. چون $[a,b]=[a',b']$ و $[c,d]=[c',d']$ می‌دانیم که

$$ab'=ba' \quad \text{و} \quad cd'=dc'. \qquad (*)$$

ضرب معادله اول در dd' و معادلهٔ دوم در bb' و جمع نتایج نشان می‌دهد که

$$ab'dd'=ba'dd'$$

$$cd'bb'=dc'bb'$$

$$\overline{ab'dd'+cd'bb'=ba'dd'+dc'bb'}$$

$$(ad+bc)b'd'=bd(a'd'+b'c').$$

بنابراین $[ad+bc,bd]=[a'd'+b'c',b'd']$.

برای قسمت دوم اثبات معادلهٔ اول $(*)$ را در cd' و معادلهٔ دوم را در ba' ضرب کرده تا بدست آورید

$$ab'cd'=ba'cd' \quad \text{و} \quad cd'ba'=dc'ba'.$$

بنابه خاصیت جابجایی، طرف راست معادلهٔ اول برابر طرف چپ معادلهٔ دوم است. بنابراین طرف‌های دیگر دو معادله برابرند: $ab'cd'=dc'ba'$. در نتیجه،

$$(ac)(b'd')=ab'cd'=dc'ba'=(bd)(a'c').$$

دو طرف انتهایی این معادله نشان می‌دهد که $[ac, bd] = [a'c', b'd']$. ■

لم ۲۱.۸. اگر R یک دامنهٔ صحیح و $\mathbb{F}$ همانند بالا باشد، در این صورت برای عناصر غیرصفر $a, b, c, d, k \in R$ داریم:

(۱) $[\circ_R, b] = [\circ_R, d]$

(۲) $[a, b] = [ak, bk]$

(۳) $[a, a] = [c, c]$.

برهان. تمرین ۱. ■

لم ۲۲.۸. با جمع و ضرب تعریف شده در بالا، $\mathbb{F}$ یک میدان است.

برهان. بسته بودن جمع و ضرب از لم ۲۰.۸ و تذکرات قبل از آن نتیجه می‌شود. جمع در $\mathbb{F}$ جابجایی است زیرا جمع و ضرب در R جابجایی است:

$$[a, b] + [c, d] = [ad + bc, bd] = [cb + da, db] = [c, d] + [a, b].$$

برای هر عضو غیرصفر $b \in R$ فرض کنید $\circ_{\mathbb{F}}$ کلاس هم‌ارزی $[\circ_R, b]$ باشد (طبق (۱) در لم ۲۱.۸ همهٔ زوجهایی به صورت $(\circ_R, b)$ با $b \neq \circ_R$ در یک کلاس هم‌ارزی قرار دارند). اگر $[a, b] \in \mathbb{F}$، در این صورت طبق (۲) در لم ۲۱.۸ (با $k = b$) داریم:

$$[a, b] + \circ_{\mathbb{F}} = [a, b] + [\circ_R, b] = [ab + b \cdot \circ_R, bb] = [ab, bb] = [a, b].$$

بنابراین $\circ_{\mathbb{F}}$ عنصر صفر $\mathbb{F}$ است. منفی $[a, b]$ در $\mathbb{F}$ کلاس $[-a, b]$ است زیرا

$$[a, b] + [-a, b] = [ab - ba, b^2] = [\circ_R, b^2] = \circ_{\mathbb{F}}.$$

اثبات شرکت‌پذیری جمع و شرکت‌پذیری و جابجایی بودن ضرب به خواننده واگذار شده است (تمرین ۲). همچنین است بررسی این که $[1_R, 1_R]$ عضو همانی ضربی $\mathbb{F}$ است. اگر $[a, b]$ یک عنصر غیرصفر $\mathbb{F}$ باشد در این صورت $a \neq \circ_R$. بنابراین $[b, a]$ عضو خوش‌تعریفی از $\mathbb{F}$ است و طبق (۳) در لم ۲۱.۸،

$$[a, b][b, a] = [ab, ba] = [1_R ab, 1_R ab] = [1_R, 1_R].$$

بنابراین $[b,a]$ وارون ضربی $[a,b]$ است. برای دیدن این‌که قانون توزیع‌پذیری در $\mathbb{F}$ برقرار است، توجه کنید که

$$\begin{aligned}[a,b]([c,d]+[r,s]) &= [a,b][cs+dr,ds]\\ &= [a(cs+dr),b(ds)]\\ &= [acs+adr,bds].\end{aligned}$$

از طرف دیگر، طبق (۲) در لم ۲۱.۸ (با $k=b$)

$$\begin{aligned}[a,b][c.d]+[a,b][r,s] &= [ac,bd]+[ar,bs]\\ &= [(ac)(bs)+(bd)(ar),(bd)(bs)]\\ &= [(acs+adr)b,(bds)b]\\ &= [acs+adr,bds].\end{aligned}$$

بنابراین $[a,b]([c,d]+[r,s]) = [a,b][c,d]+[a,d][r,s]$. ■

معمولاً اعداد صحیح را با اعداد گویایی به‌صورت $a/1$ یکی می‌گیریم. این ایده در حالت کلی نیز کارآیی دارد.

لم ۲۳.۸. فرض کنید R یک دامنه صحیح و $\mathbb{F}$ میدان ساخته شده در بالا باشد. در این صورت زیرمجموعه $R^* = \{[a,1_R] \mid a \in R\}$ از $\mathbb{F}$ یک دامنه صحیح است که با R یکریخت می‌باشد.

برهان. بررسی کنید که R^* یک زیرحلقه $\mathbb{F}$ است (تمرین ۳). به‌وضوح $[1_R,1_R]$، عضو همانی $\mathbb{F}$، در R^* قرار دارد و لذا R^* یک دامنه صحیح است. نگاشت $f : R \to R^*$ را توسط $f(a) = [a,1_R]$ تعریف کنید. در این صورت f یک همریختی است:

$$\begin{aligned}f(a)+f(c) &= [a,1_R]+[c,1_R] = [a1_R+1_Rc,1_R1_R]\\ &= [a+c,1_R] = f(a+c)\\ f(a)f(c) &= [a,1_R][c,1_R] = [ac,1_R] = f(ac).\end{aligned}$$

اگر $f(a)=f(c)$ در این صورت $[a,1_R]=[c,1_R]$، که نتیجه می‌دهد $a1_R = 1_Rc$. بنابراین $a=c$ و f یک به یک است. چون به‌وضوح f پوشا است، f یک یکریختی است. ■

نماد کلاس هم‌ارزی که برای عناصر $\mathbb{F}$ بکار رفت، نمادی نامناسب‌است و ایدهٔ "خارج‌قسمت‌ها" را که مورد نظر بود انتقال نمی‌دهد. این اشکال به سادگی و با تغییر نماد کلاس هم‌ارزی اصلاح می‌شود. به جای نمایش کلاس هم‌ارزی (a,b) با $[a,b]$،

کلاس هم‌ارزی (a,b) را با a/b نشان دهید.

چنانچه ما گزاره‌های مختلف بالا را از نماد براکت به نماد جدید خارج قسمت ترجمه کنیم، در این صورت همه، گزاره‌هایی طبیعی بنظر می‌رسند:

قضیه ۲۴.۸. فرض کنید R یک دامنه صحیح باشد. در این صورت یک میدان $\mathbb{F}$ وجود دارد که عناصرش به صورت a/b می‌باشند، جایی که $a,b \in R$ و $b \neq 0_R$، و در شرط برابری زیر صدق می‌کنند

$$a/b = c/d \text{ در } \mathbb{F} \text{ اگر و تنها اگر } ad = bc \text{ در } R .$$

جمع و ضرب در $\mathbb{F}$ توسط

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \qquad \text{و} \qquad \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

داده شده است. مجموعهٔ عناصر $\mathbb{F}$ به صورت $a/1_R$، $(a \in R)$ یک دامنه صحیح است که با R یکریخت می‌باشد.

برهان. به لم‌های ۲۲.۸ و ۲۳.۸ و تغییر نمادی که پیش از قضیه انجام گرفت مراجعه شود. ■

اکنون آشکار است که اگر $R = \mathbb{Z}$، در این صورت میدان $\mathbb{F}$ دقیقاً $\mathbb{Q}$ است. بنابراین قضیه ۲۴.۸ می‌تواند به عنوان تولید رسمی $\mathbb{Q}$ از $\mathbb{Z}$ در نظر گرفته شود. در حالت کلّی ما باید همان عادت معمول خودمان در مورد $\mathbb{Q}$ را بکار بریم، حلقهٔ R را با کپی یکریختش در $\mathbb{F}$ یکی بگیریم. پس می‌توانیم بگوییم R زیرمجموعه‌ای از $\mathbb{F}$ است که متشکل از عناصری به‌صورت $a/1_R$ می‌باشد. میدان $\mathbb{F}$ **میدان خارج قسمتهای** [۳۲] R نامیده می‌شود.

---

۳۲) در اینجا ممکن است سوال شود که "چرا نماد خارج قسمت را زودتر بکار نبردیم؟" جواب بیشتر روانشناسانه است تا مربوط به ریاضیات. نماد خارج قسمت همه چیز را آنقدر شبیه اعداد گویای آشنا می‌سازد که ممکن است به جای بررسی رسمی (و خسته کنندهٔ) جزئیات یک کار دقیق و موشکافانه این تمایل بوجود آید که همه‌چیز همواره درست کار می‌کند.

مثال ۱۹.۸. فرض کنید $\mathbb{K}$ یک میدان باشد. میدان خارج قسمتهای دامنهٔ چندجمله‌ای‌های $\mathbb{K}[x]$ توسط $\mathbb{K}(x)$ نمایش داده می‌شود و متشکل از همهٔ $f(x)/g(x)$هایی است که در آن $f(x), g(x) \in \mathbb{K}[x]$ و $g(x) \neq 0_{\mathbb{K}}$. میدان $\mathbb{K}(x)$ میدان **توابع گویا** روی $\mathbb{K}$ نامیده می‌شود.

میدان خارج قسمتهای یک دامنهٔ صحیح R کوچکترین میدانی است که R را به مفهوم زیر شامل است[۳۳].

قضیه ۲۵.۸. فرض کنید R یک دامنهٔ صحیح و $\mathbb{F}$ میدان خارج قسمتهای آن باشد. اگر $\mathbb{K}$ میدانی شامل R باشد، در این صورت $\mathbb{K}$ شامل زیرمیدانی مانند $\mathbb{E}$ است به طوری که $R \subseteq \mathbb{E} \subseteq \mathbb{K}$ و $\mathbb{E}$ با $\mathbb{F}$ یکریخت است.

برهان. اگر $a/b \in \mathbb{F}$، در این صورت $a, b \in R$ و b غیرصفر است. چون $R \subseteq \mathbb{K}$، b^{-1} موجود است. نگاشت $f : \mathbb{F} \to \mathbb{K}$ را توسط $f(a/b) = ab^{-1}$ تعریف کنید. تمرین ۹ نشان می‌دهد که f خوش‌تعریف است، یعنی، $a/b = c/d$ در $\mathbb{F}$ نتیجه می‌دهد $f(a/b) = f(c/d)$ در $\mathbb{K}$. تمرین ۱۰ نشان می‌دهد که f یک همریختی یک به یک است. اگر $\mathbb{E}$ تصویر $\mathbb{F}$ تحت f باشد، در این صورت $\mathbb{E} \cong \mathbb{F}$. برای هر $a \in R$، $a = a1_R^{-1} = f(a/1_R) \in \mathbb{E}$. بنابراین $R \subseteq \mathbb{E} \subseteq \mathbb{K}$. ■

تمرینها

توجه: R یک دامنه صحیح و $\mathbb{F}$ میدان خارج قسمت‌های آن است، مگر خلاف آن ذکر شود.

A.۱. لم ۲۱.۸ را ثابت کنید.

۲. اثبات لم ۲.۸ را با نشان دادن موارد زیر کامل کنید:

(الف) جمع کلاس‌های هم‌ارزی شرکت‌پذیر است.

(ب) ضرب کلاس‌های هم‌ارزی شرکت‌پذیر است.

(پ) ضرب کلاس‌های هم‌ارزی جابجایی است.

۳. نشان دهید که $R^* = \{[a, 1_R] \mid a \in R\}$ یک زیرحلقه $\mathbb{F}$ است.

B.۴. اگر R خود یک میدان باشد، نشان دهید $R = \mathbb{F}$.

۳۳) از قضیه ۲۵.۸ در ادامه استفاده نشده است.

۵. اگر $R = \mathbb{Z}[i]$، در این صورت نشان دهید که $\mathbb{F} \cong \{r + si \mid r, s \in \mathbb{Q}\}$.

۶. اگر $R = \mathbb{Z}[\sqrt{d}]$، در این صورت نشان دهید که $\mathbb{F} \cong \{r + s\sqrt{d} \mid r, s \in \mathbb{Q}\}$.

۷. نشان دهید که تعداد نامتناهی دامنه صحیح R با میدان خارج‌قسمت‌های $\mathbb{Q}$ وجود دارد به طوری که $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$. [راهنمایی: تمرین ۲۳ بخش ۱.۳.]

۸. فرض کنید $f : R \to R_1$ یک یکریختی از دامنه‌های صحیح باشد. فرض کنید $\mathbb{F}$ میدان خارج قسمت‌های R و $\mathbb{F}_1$ میدان خارج‌قسمت‌های R_1 باشد. نشان دهید نگاشت $f^* : \mathbb{F} \to \mathbb{F}_1$ با ضابطهٔ $f^*(a/b) = f(a)/f(b)$ یک یکریختی است.

۹. اگر R در میدان $\mathbb{K}$ قرار داشته باشد و $a/b = c/d$ در $\mathbb{F}$، نشان دهید که $ab^{-1} = cd^{-1}$ در $\mathbb{K}$. [راهنمایی: $a/b = c/d$ نتیجه می‌دهد $ad = bc$ در $\mathbb{K}$.]

۱۰. (الف) ثابت کنید نگاشت f در اثبات قضیه ۲۵.۸ یک به یک است. [راهنمایی: $f(a/b) = f(c/d)$ نتیجه می‌دهد $ab^{-1} = cd^{-1}$؛ نشان دهید که $ad = bc$.]
(ب) با محاسبه مستقیم نشان دهید که f یک همریختی است.

۱۱. فرض کنید $a, b \in R$. فرض کنید اعداد صحیح مثبت m و n وجود داشته باشد به قسمی که $a^m = b^m$ و $a^n = b^n$ و $(m, n) = 1$. ثابت کنید که $a = b$. [به خاطر آورید که توانهای منفی a و b لزوماً در R تعریف شده نیستند امّا در میدان $\mathbb{F}$ دارای مفهوم هستند؛ به عنوان مثال $a^{-2} = 1_R/a^2$.]

۱۲. فرض کنید R یک دامنه صحیح با مشخصه ۰ باشد (تمرین ۲۸ بخش ۳.۲ را ملاحظه کنید).
(الف) ثابت کنید که R دارای یک زیرحلقه یکریخت با $\mathbb{Z}$ است. [راهنمایی: مجموعه $\{n1_R | n \in \mathbb{Z}\}$ را در نظر بگیرید.]
(ب) ثابت کنید که هر میدان با مشخصهٔ ۰ دارای زیرمیدانی یکریخت با $\mathbb{Q}$ است. [راهنمایی: قضیه ۲۵.۸.]

۱۳. ثابت کنید که قضیه ۲۴.۸ در حالتی که R یک حلقه جابجایی بدون مقسوم‌علیه صفر (نه لزوماً یک دامنه صحیح) باشد معتبر است. [راهنمایی: نشان دهید که برای هر عضو غیرصفر $a \in R$، کلاس $[a, a]$ به‌عنوان یک همانی ضربی برای $\mathbb{F}$ عمل می‌کند و مجموعهٔ $\{[ra, a] | r \in R\}$ یک زیرحلقه $\mathbb{F}$ یکریخت با R است. اعداد صحیح زوج الگوی خوبی

از این وضعیت می‌باشد.]

۸-۵ یکتایی تجزیه در دامنه‌های چندجمله‌ای

در سرتاسر این بخش R یک دامنه یکتایی تجزیه است. اثبات خواهیم کرد که حلقه چندجمله‌ای‌های $R[x]$ یک **دی‌ت** است. ایدهٔ اصلی برهان کاملاً ساده است. به ازای یک چندجمله‌ای $f(x)$، با فاکتورگیری مکرر، آن را به صورت حاصل‌ضربی از چند جمله‌ای‌های با درجات کمتر تجزیه کنید تا زمانی که $f(x)$ به صورت حاصل‌ضربی از چندجمله‌ای‌های تحویل‌ناپذیر درآید. برای اثبات یکتایی، چندجمله‌ای $f(x)$ را در $\mathbb{F}[x]$ در نظر بگیرید که در آن $\mathbb{F}$ میدان خارج قسمت‌های R است. با استفاده از این حقیقت که $\mathbb{F}[x]$ یک **دی‌ت** است (قضیه ۱۰.۴)، نشان دهید که تجزیه در $R[x]$ یکتاست. البته در تحقق برنامه فوق با مشکلاتی نیز مواجه می‌شویم:

مثال ۲۰.۸. چندجمله‌ای $۳x^۲ + ۶$ قابل تجزیه شدن به صورت حاصل‌ضربی از دو چندجمله‌ای با درجهٔ کمتر در $\mathbb{Z}[x]$ نیست و در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. امّا $۳x^۲ + ۶$ در $\mathbb{Z}[x]$ تحویل‌پذیر است زیرا $۳x^۲ + ۶ = ۳(x^۲ + ۲)$ و هیچکدام از ۳ و $x^۲ + ۲$ در $\mathbb{Z}[x]$ یکه نیست.

پس اولین گام بررسی نقش چندجمله‌ای‌های ثابت در $R[x]$ است. با استفاده از قضیه ۱.۴ و تمرینهای ۱ و ۳ بررسی کنید که

یکه‌های در $R[x]$ در R یکه هستند

و

چندجمله‌ای‌های ثابت تحویل‌ناپذیر در $R[x]$ عناصر تحویل‌ناپذیر R هستند.

برای مثال یکه‌های $\mathbb{Z}[x]$ عبارتند از ± ۱. چندجمله‌ای ثابت ۳ در $\mathbb{Z}[x]$ تحویل‌ناپذیر است گرچه که در $\mathbb{Q}[x]$ یک یکه است.

عوامل تحویل‌ناپذیر ثابت یک چندجمله‌ای در $R[x]$ را می‌توان با فاکتورگیری همهٔ ثابت‌ها و بیان آنها به صورت حاصل‌ضربی از عناصر تحویل‌ناپذیر در R یافت.

مثال ۲۱.۸. در $\mathbb{Z}[x]$

$$۶x^۲ + ۱۸x + ۱۲ = ۶(x^۲ + ۳x + ۲) = ۲ \times ۳(x^۲ + ۳x + ۲).$$

توجه کنید که $x^۲ + ۳x + ۲$ یک چندجمله‌ای است که تنها شمارنده‌های ثابت آن در $\mathbb{Z}[x]$ یکه‌های ± ۱ هستند. این مثال راهکاری را برای حالت کلی پیشنهاد می‌نماید.

فرض کنید R یک دامنه صحیح باشد. یک چندجمله‌ای غیرصفر در $R[x]$ را **اولیه** گویند هرگاه تنها ثابت‌هایی که آن را می‌شمارند یکه‌های R باشند. برای مثال، $x^۲ + ۳x + ۲$ و $۳x^۴ - ۵x^۳ + ۲x$ در $\mathbb{Z}[x]$ اولیه هستند. چندجمله‌ایهای اولیه با درجه ۰ یکه‌ها هستند. طبق قضیه ۱.۸ هرچندجمله‌ای اولیه با درجه ۱ باید تحویل‌ناپذیر باشد (زیرا هر تجزیه، یک ثابت را شامل می‌شود (قضیه ۱.۴) و هر چنین ثابتی باید یک یکه باشد). امّا چندجمله‌ای‌های اولیه با درجات بالاتر الزاماً تحویل‌ناپذیر نیستند (به‌عنوان مثال، $x^۲ + ۳x + ۲ = (x + ۱)(x + ۲)$ در $\mathbb{Z}[x]$.) از طرف دیگر، طبق قضایای ۱.۴ و ۱.۸، یک چندجمله‌ای تحویل‌ناپذیر با درجه مثبت دارای هیچ شمارنده ثابتی بجز یکه‌ها نیست. بنابراین

یک چندجمله‌ای تحویل‌ناپذیر با درجه مثبت اولیه است.

به‌علاوه همانگونه که مثال بالا نشان می‌دهد،

هر چندجمله‌ای غیرصفر $f(x) \in R[x]$ به‌صورت
$f(x) = cg(x)$ تجزیه می‌شود که در آن $g(x)$ اولیه است.

برای اثبات این ادعا، فرض کنید c بزرگترین مقسوم‌علیه مشترک ضرایب $f(x)$ باشد[۳۴]. پس چندجمله‌ای $g(x)$ وجود دارد طوری که $f(x) = cg(x)$. اگر $d \in R$ چندجمله‌ای $g(x)$ را بشمارد در این صورت $g(x) = dh(x)$ و لذا $f(x) = cdh(x)$. چون cd یک شمارنده ثابت $f(x)$ است، بایستی ضرایب $f(x)$ را بشمارد و بنابراین باید ب‌م‌م آنها یعنی c را نیز بشمارد. پس $u \in R$ وجود دارد طوری که $cdu = c$. چون $c \neq ۰_R$، ملاحظه می‌کنیم که $du = ۱_R$ و d یکه است. بنابراین $g(x)$ اولیه است.

اینک به کمک حقایقی که درباره چندجمله‌ای‌های اولیه دیدیم، می‌توانیم بحثی را که در ابتدای این بخش ارائه شد اصلاح کنیم و شرط اول از دو شرط لازم برای دی‌ت بودن $R[x]$ را ثابت نماییم.

---

۳۴) طبق نتیجه ۵.۸، ب‌م‌م، موجود است.

قضیه ۲۶.۸. فرض کنید R یک دامنه یکتایی تجزیه باشد. در این صورت هر چندجمله‌ای غیرصفر غیریکه $f(x) \in R[x]$ حاصل‌ضربی از چندجمله‌ایهای تحویل‌ناپذیر است[۳۵].

برهان. فرض کنید $f(x) = cg(x)$ که در آن $g(x)$ اولیه است. چون R یک **دی‌ت** است، c یا یک یکه است یا حاصل‌ضربی از عناصر تحویل‌ناپذیر در R (و بنابراین در $R[x]$) است. بنابراین تنها لازم است ثابت کنیم که $g(x)$ یا یک یکه است یا حاصل‌ضربی از عوامل تحویل‌ناپذیر در $R[x]$ است. اگر $g(x)$ یکه و یا خودش تحویل‌ناپذیر باشد، چیزی برای اثبات باقی نمی‌ماند. در غیر این صورت طبق قضیه ۱.۸، $g(x) = h(x)k(x)$ که در آن هیچکدام از $h(x)$ و $k(x)$ یکه نیستند. چون $g(x)$ اولیه است، تنها شمارنده‌های با درجه صفر آن یکه‌ها هستند، بنابراین باید داشته باشیم $0 < \deg h(x) < \deg g(x)$ و $0 < \deg k(x) < \deg g(x)$. به علاوه $h(x)$ و $k(x)$ اولیه هستند (هر ثابتی که یکی از آنها را بشمارد باید $g(x)$ را بشمارد و بنابراین باید یکه باشد). اگر $h(x)$ و $k(x)$ تحویل‌ناپذیر باشند، کار تمام است، در غیر این‌صورت بحث قبلی را تکرار کرده و آنها را به حاصل‌ضربی از چندجمله‌ایهای اولیه با درجات کمتر تجزیه می‌کنیم و غیره. این فرآیند پس از یک تعداد متناهی تکرار باید متوقف شود زیرا درجه‌های عوامل در هر مرحله کوچکتر شده و هر چندجمله‌ای اولیه از درجه ۱ تحویل‌ناپذیر است. بنابراین $g(x)$ حاصل‌ضربی از چندجمله‌ایهای تحویل‌ناپذیر در $R[x]$ است. ■

اثبات یکتایی تجزیه در $R[x]$ بستگی به چندین نکته فنی دارد که در بخش آینده به آنها خواهیم پرداخت. برای بدست آوردن ایده‌ای از این که چگونه همه‌چیز به‌طور هماهنگ با هم مرتبط می‌شود، ممکن است ترجیح دهید ابتدا اثبات قضیه ۳۲.۸ را مطالعه کرده و هر کجا لازم باشد به نتایج میانی مراجعه کرده و بدون اثبات آنها را بپذیرید. بعداً می‌توانید به این نقطه بازگشته و با آگاهی از این که بحث چگونه پیش خواهد رفت اثبات‌ها را مطالعه کنید.

لم ۲۷.۸. فرض کنید R یک دامنه یکتایی تجزیه باشد و $g(x), h(x) \in R[x]$. اگر p یک عنصر تحویل‌ناپذیر R باشد که $g(x)h(x)$ را بشمارد، در این صورت p، $g(x)$ یا $h(x)$ را می‌شمارد.

برهان. اثبات لم ۱۷.۴ که حالت خاص $R = \mathbb{Z}$ است را تکرار کنید. تنها جای $\mathbb{Z}$ را با R و "اول" را با "تحویل‌ناپذیر" عوض کنید و قضیه ۶.۸ را بجای قضیه ۸.۱ بکار برید. ■

---

۳۵) طبق معمول یک "حاصل‌ضرب" با تنها یک عامل را می‌پذیریم.

نتیجه ۲۸.۸. (**لم گوس**[۳۶]) فرض کنید R یک دامنه یکتایی تجزیه باشد. در این صورت حاصل‌ضرب چندجمله‌ای‌های اولیه در $R[x]$، اولیه است.

برهان. اگر $g(x)$ و $h(x)$ اولیه باشند و $g(x)h(x)$ اولیه نباشد، در این صورت $g(x)h(x)$ توسط یک عنصر غیریکه $c \in R$ شمرده می‌شود. در نتیجه هر عامل تحویل‌ناپذیر p از c، $g(x)h(x)$ را می‌شمارد. طبق لم ۲۷.۸، p، $g(x)$ یا $h(x)$ را می‌شمارد که متناقض با اولیه بودن آنها است. بنابراین $g(x)h(x)$ اولیه است. ■

قضیه ۲۹.۸. فرض کنید R یک دامنه یکتایی تجزیه و r و s عناصر غیرصفری از R باشند. فرض کنید $f(x)$ و $g(x)$ چندجمله‌ایهای اولیه‌ای در $R[x]$ باشند به قسمی که $rf(x) = sg(x)$. در این صورت r و s در R وابسته‌اند و $f(x)$ و $g(x)$ در $R[x]$ وابسته‌اند.

برهان. اگر r یکه باشد در این صورت $f(x) = r^{-1}sg(x)$. چون $r^{-1}s$ چندجمله‌ای اولیه $f(x)$ را می‌شمارد باید یکه باشد، مثلاً $(r^{-1}s)u = 1_R$. بنابراین $f(x)$ و $g(x)$ در $R[x]$ وابسته‌اند. به‌علاوه u یک یکه در R است و $su = r$، بنابراین r و s در R وابسته‌اند. اگر r غیر یکه باشد در این صورت $r = p_1p_2 \dots p_k$ که در آن هر p_i تحویل‌ناپذیر است. پس $p_1p_2 \dots p_k f(x) = sg(x)$ و لذا p_1، $sg(x)$ را می‌شمارد. طبق لم ۲۷.۸، p_1، s یا $g(x)$ را می‌شمارد. چون p_1، غیریکه و $g(x)$ اولیه است، p_1 باید s را بشمارد، مثلاً $s = p_1t$. پس $p_1p_2 \dots p_k f(x) = sg(x) = p_1tg(x)$. با حذف p_1 از دو طرف بدست می‌آوریم $p_2 \dots p_k f(x) = tg(x)$. تکرار این بحث با p_2 نشان می‌دهد که $p_3 \dots p_k f(x) = zg(x)$ که در آن $p_2z = t$ و بنابراین $p_1p_2z = p_1t = s$. بعد از k بار تکرار، برای برخی $w \in R$ خواهیم داشت $f(x) = wg(x)$ و $s = p_1p_2 \dots p_k w$. چون w چندجمله‌ای اولیه $f(x)$ را می‌شمارد، w یکه است. بنابراین $f(x)$ و $g(x)$ در $R[x]$ وابسته‌اند. چون $s = p_1 \dots p_k w = rw$، r و s در R وابسته‌اند. ■

نتیجه ۳۰.۸. فرض کنید R یک دامنه یکتایی تجزیه و $\mathbb{F}$ میدان خارج قسمت‌های آن باشد. فرض کنید $f(x)$ و $g(x)$ در $R[x]$ اولیه باشند. اگر $f(x)$ و $g(x)$ در $\mathbb{F}[x]$ وابسته باشند، در این صورت در $R[x]$ نیز وابسته‌اند.

برهان. اگر $f(x)$ و $g(x)$ در $\mathbb{F}[x]$ وابسته باشند در این صورت طبق قضیه ۷.۴، برای برخی

---

۳۶) Gauss's lemma

عنصر غیرصفر $r/s \in \mathbb{F}$ داریم $g(x) = (r/s)f(x)$. در نتیجه $sg(x) = rf(x)$ در $R[x]$. بنابراین طبق قضیه ۲۹.۸، $f(x)$ و $g(x)$ در $R[x]$ وابسته‌اند. ■

نتیجه ۳۱.۸. فرض کنید R یک دامنه یکتایی تجزیه و $\mathbb{F}$ میدان خارج قسمت‌های آن باشد. اگر $f(x) \in R[x]$ دارای درجه مثبت و تحویل‌ناپذیر در $R[x]$ باشد، در این صورت $f(x)$ تحویل‌ناپذیر در $\mathbb{F}[x]$ است.

برهان. اگر $f(x)$ در $\mathbb{F}[x]$ تحویل‌ناپذیر نباشد، در این صورت چندجمله‌ای‌های با درجه مثبت $h(x) \in \mathbb{F}[x]$ و $g(x)$ وجود دارند به قسمی که $f(x) = g(x)h(x)$. فرض کنید b کوچکترین مخرج مشترک ضرایب $g(x)$ باشد. در این صورت $bg(x)$ دارای ضرایب در R است. بنابراین $bg(x) = ag_1(x)$ که در آن $a \in R$ و $g_1(x)$ اولیه و از درجه مثبت در $R[x]$ است. بنابراین $g(x) = \frac{a}{b}g_1(x)$. به طور مشابه $h(x) = \frac{c}{d}h_1(x)$ که در آن $c, d \in R$ و $h_1(x)$ اولیه و از درجه مثبت در $R[x]$ است. پس

$$f(x) = g(x)h(x) = \frac{a}{b}g_1(x)\frac{c}{d}h_1(x) = \frac{ac}{bd}g_1(x)h_1(x).$$

لذا $bdf(x) = acg_1(x)h_1(x)$ در $R[x]$. اکنون بدلیل این که $f(x)$ تحویل‌ناپذیر است، $f(x)$ اولیه است و طبق نتیجه ۲۸.۸، $g_1(x)h_1(x)$ اولیه است. بنابراین طبق قضیه ۲۹.۸، bd یک وابسته ac است، یعنی برای برخی یکه u، $bdu = ac$. پس $f(x) = \frac{ac}{bd}g_1(x)h_1(x) = ug_1(x)h_1(x)$. امّا این تحویل‌ناپذیری $f(x)$ را نقض می‌کند زیرا $ug_1(x)$ و $h_1(x)$ چندجمله‌ای‌های با درجه مثبت در $R[x]$ هستند. بنابراین $f(x)$ باید در $\mathbb{F}[x]$ تحویل‌ناپذیر باشد. ■

قضیه ۳۲.۸. اگر R یک دامنه یکتایی تجزیه باشد، در این صورت $R[x]$ نیز چنین است.

برهان. طبق قضیه ۲۶.۸، هر چندجمله‌ای غیرصفر غیریکه $f(x)$ در $R[x]$ حاصل‌ضربی از چندجمله‌ای‌های تحویل‌ناپذیر است. هر چنین تجزیه‌ای، تحویل‌ناپذیرهای ثابت (یعنی، تحویل‌ناپذیرهای در R) و چندجمله‌ای‌های تحویل‌ناپذیر از درجه مثبت را شامل می‌شود. فرض کنید

$$c_1 \cdots c_m p_1(x) \cdots p_k(x) = d_1 \cdots d_n q_1(x) \cdots q_t(x)$$

که در آن هر c_i، d_j تحویل‌ناپذیر در R و هر $p_i(x)$، $q_j(x)$ تحویل‌ناپذیر از درجه مثبت در $R[x]$

(و بنابراین اولیه) باشد[۳۷]. در این صورت طبق نتیجه ۲۸.۸، $p_1(x)\cdots p_k(x)$ و $q_1(x)\cdots q_t(x)$ اولیه هستند. بنابراین قضیه ۲۹.۸ نشان می‌دهد که $c_1\cdots c_m$ یک وابسته $d_1\cdots d_n$ در R است و $p_1(x)\cdots p_k(x)$ یک وابسته $q_1(x)\cdots q_t(x)$ در $R[x]$ است. بنابراین برای برخی یکه $u\in R$، $c_1\cdots c_m = ud_1d_2\cdots d_n$. وابسته‌های عناصر تحویل‌ناپذیر، تحویل‌ناپذیرند (تمرین ۷ بخش ۱.۸)، لذا ud_1 تحویل‌ناپذیر است. چون R یک **دی‌ت** است باید داشته باشیم $m=n$ و (بعد از نمایه‌گذاری مجدد در صورت لزوم) c_1 یک وابسته ud_1 (و بنابراین وابسته d_1)، و c_i یک وابسته d_i برای $i\geq 2$ است. فرض کنید $\mathbb{F}$ میدان خارج‌قسمت‌های R باشد. طبق نتیجه ۳۱.۸، هرکدام از $p_i(x)$، $q_j(x)$ها تحویل‌ناپذیر در $\mathbb{F}[x]$ هستند. یکتایی تجزیه در $\mathbb{F}[x]$ (قضیه ۱۰.۴) و استدلالی مشابه آنچه که لحظه‌ای پیش برای R ارائه شد، نشان می‌دهد که $k=t$ و (بعد از نمایه‌گذاری مجدد در صورت لزوم) هر $p_i(x)$ یک وابسته $q_i(x)$ در $\mathbb{F}[x]$ است. لذا طبق نتیجه ۳۰.۸، $p_i(x)$ و $q_i(x)$ در $R[x]$ وابسته‌اند. بنابراین $R[x]$ یک **دی‌ت** است. ■

نتیجه زیر از قضایای ۱۱.۱ و ۳۲.۸ و مثال ۵.۶، فوراً بدست می‌آید:

نتیجه ۳۳.۸. $\mathbb{Z}[x]$ یک دامنه یکتایی تجزیه است که یک دامنه ایده‌آل اصلی نیست.

همانگونه که در بحث قبلی نشان داده شد امکان انتقال قضایای مربوط به $\mathbb{Z}[x]$ و $\mathbb{Q}[x]$ به **دی‌ت**های دلخواه و میدان خارج قسمت‌های آن بسیار بالا است. از جملهٔ چنین نتایجی آزمون ریشه گویا و محک آیزنشتاین[۳۸] می‌باشد (تمرین‌های ۱۳ـ۱۱).

---

۳۷) ممکن است که هیچ‌کدام از تجزیه‌ها عوامل ثابت را شامل نشوند، امّا این امر تأثیری بر استدلال ندارد. در هر حال، غیرممکن است که در یکی از تجزیه‌ها عوامل ثابت تحویل‌ناپذیر وجود داشته و در دیگری وجود نداشته باشد (تمرین ۵ را ملاحظه کنید).

۳۸) Eisentein's Criterion

تمرینها

توجه: R یک **دی‌ت** و $\mathbb{F}$ میدان خارج قسمت‌های آن است، مگر خلاف آن ذکر شود.

۱.A. اگر R دامنه صحیح باشد، ثابت کنید که یکه‌های $R[x]$ دقیقاً چندجمله‌ای‌های ثابتی هستند که در R یکه می‌باشند. [راهنمایی: قضیه ۱.۴.]

۲. نشان دهید که تمرین ۱، در صورتی که R یک حلقه جابجایی یکدار باشد که یک دامنه صحیح نیست، ممکن است غلط باشد.

۳. فرض کنید R یک دامنه صحیح باشد و $p \in R$. ثابت کنید که p در R تحویل‌ناپذیر است اگر و تنها اگر چندجمله‌ای ثابت p در $R[x]$ تحویل‌ناپذیر باشد. [تمرین ۱ می‌تواند مفید باشد.]

۴. مثالی از چندجمله‌ایهای $f(x), g(x) \in R[x]$ ارائه دهید به‌قسمی که $f(x)$ و $g(x)$ در $\mathbb{F}[x]$ وابسته بوده امّا در $R[x]$ وابسته نباشند.

۵. اگر $c_1 \cdots c_m f(x) = g(x)$ که در آن $c_i \in R$ و $g(x)$ اولیه در $R[x]$ است، ثابت کنید که هر c_i یک یکه است.

۶. اگر $g(x)$ در $R[x]$ اولیه باشد، ثابت کنید که هر چندجمله‌ای غیر ثابت در $R[x]$ که $g(x)$ را بشمارد نیز اولیه است.

۷.B. ثابت کنید که یک چندجمله‌ای اولیه است اگر و تنها اگر 1_R یک بزرگترین مقسوم‌علیه مشترک ضرایب آن باشد. این خاصیت اغلب به عنوان تعریف "اولیه بودن" در نظرگرفته می‌شود.

۸. اگر $f(x)$ در $R[x]$ اولیه و در $\mathbb{F}[x]$ تحویل‌ناپذیر باشد، ثابت کنید که $f(x)$ در $R[x]$ تحویل‌ناپذیر است.

۹. اگر R یک حلقه باشد به قسمی که $R[x]$ یک **دی‌ت** باشد، ثابت کنید که R یک **دی‌ت** است.

۱۰. اگر R یک حلقه باشد به قسمی که $R[x]$ یک دامنه ایده‌آل اصلی باشد، ثابت کنید که R یک میدان است.

۱۱. ثابت کنید که آزمون ریشه گویا (قضیه ۱۶.۴) در صورتی‌که به جای $\mathbb{Z}$ و $\mathbb{Q}$، R و $\mathbb{F}$ را قرار دهیم نیز معتبر است.

۱۲. بررسی کنید که قضیه ۱۸.۴ در صورتی که به جای $\mathbb{Z}$ و $\mathbb{Q}$، R و $\mathbb{F}$ قرار دهیم نیز معتبر است.

۱۳. بررسی کنید که محک آیزنشتاین (قضیه ۱۹.۴) در صورتی که جای $\mathbb{Z}$ و $\mathbb{Q}$ را با R و $\mathbb{F}$ و جای "اول بودن" را با "تحویل‌ناپذیری" عوض کنیم، نیز معتبر است.

۱۴. ثابت کنید $x^3 - 6x^2 + 4ix + 1 + 3i$ در $(\mathbb{Z}[i])[x]$ تحویل‌ناپذیر است. [راهنمایی: تمرین ۱۳]

* * * * *

فصل نهم

توسیع‌های میـــدان

جبر دبیرستان در اصل با سه میدان $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$، و هندسه مسطحه با مجموعه $\mathbb{R} \times \mathbb{R}$ سروکار دارد. حسابان با توابع از $\mathbb{R}$ به $\mathbb{R}$ ارتباط دارد. در واقع بیشتر ریاضیات کلاسیک در میدان $\mathbb{C}$ و زیرمیدان‌های آن انتظام‌یافته است. میدان‌های دیگر نیز همان نقش مهم را در ریاضیات جدیدتر ایفا می‌کنند. برای مثال، این میدان‌ها در آنالیز، هندسه جبری و بخش‌هایی از نظریه اعداد بکار می‌روند، و کاربردهای متعددی، از جمله در نظریه کدگذاری و رمزگشایی جبری دارند.

در این فصل به بسط و توسعه حقایق اساسی در مورد میدان‌هایی می‌پردازیم که برای اثبات برخی دستاوردهای مشهور نظریه معادلات (فصل ۱۱) و مطالعه برخی مباحث فهرست شده در فوق مورد نیاز هستند. موضوع اصلی، رابطه میدان و زیرمیدان‌های گوناگون آن می‌باشد.

۹-۱ پایـــه و بعـــد

اگر $\mathbb{F}$ و $\mathbb{K}$ میدان‌هایی با شرط $\mathbb{F} \subseteq \mathbb{K}$ باشند، گوییم $\mathbb{K}$ یک **توسیع میدان** $\mathbb{F}$ است. *در سراسر این بخش $\mathbb{K}$ همواره یک توسیع میدان $\mathbb{F}$ است.* علاقه اصلی ما بررسی این است که چگونه‌میدان $\mathbb{F}$ و زیرمجموعه‌های مشخصی از $\mathbb{K}$ تمام عناصر توسیع میدان $\mathbb{K}$ را معین می‌کند. مثالی ساده از این مفهوم توسیع میدان $\mathbb{C}$ از میدان $\mathbb{R}$ است. هر عضو $\mathbb{C}$ را می‌توان به صورت $a+bi$، که در آن $a, b \in \mathbb{R}$ نوشت. از اینرو عضو $\mathbb{C}$ توسط میدان $\mathbb{R}$ و زیرمجموعه $\{1, i\}$ از $\mathbb{C}$ تعیین می‌گردد.

به طور کلی فرض کنید $v_1, \ldots, v_n$ عضوهایی از $\mathbb{K}$ باشند. اگر $w \in \mathbb{K}$ را بتوان به صورت $w = a_1v_1 + a_2v_2 + \cdots + a_nv_n$ نوشت که در آن $a_i \in \mathbb{F}$، گوییم w یک **ترکیب خطی** از $v_1, \ldots, v_n$ است. اگر هر عضو $\mathbb{K}$ ترکیبی خطی از $v_1, \ldots, v_n$ باشد، گوییم که مجموعه $\{v_1, \ldots, v_n\}$ میدان $\mathbb{K}$ را روی $\mathbb{F}$ پدید می‌آورد[۱].

مثال ۱.۹. تذکرات بند اول نشان می‌دهد که مجموعه $\{1, i\}$، $\mathbb{C}$ را روی $\mathbb{R}$ پدید می‌آورد. مجموعه $\{1+i, 5i, 2+3i\}$ نیز $\mathbb{C}$ را پدید می‌آورد زیرا عنصر $a+bi$ در $\mathbb{C}$ ترکیبی خطی از این سه عضو با ضرایب در $\mathbb{R}$ می‌باشد:

$$a + bi = 3a(1+i) + \frac{b}{5}(5i) + (-a)(2+3i)$$

مثال ۲.۹. میدان چهارعضوی $\mathbb{Z}_2[x]/(x^2+x+1)$ که جدول آن در مثال ۱۰.۵ آمده‌است یک توسیع میدان $\mathbb{Z}_2$ است. این میدان توسط مجموعه $\{1, [x]\}$ پدید آمده است زیرا هر یک از عناصرش را می‌توان به صورت $a1 + b[x]$، با شرط $a, b \in \mathbb{Z}_2$ نوشت.

مجموعه $\{1, i\}$ نه تنها توسیع میدان $\mathbb{C}$ از $\mathbb{R}$ را پدید می‌آورد، بلکه دارای این خاصیت نیز هست که اگر $a1 + bi = 0$ آنگاه $a = 0$ و $b = 0$. به بیان دیگر وقتی یک ترکیب خطی از 1 و i صفر باشد، آنگاه تمام ضرایبش صفر است. از جهت دیگر مجموعه $\{1+i, 5i, 2+3i\}$ این خاصیت را ندارد زیرا یک ترکیب خطی از این عناصر وجود دارد که برابر صفر است اگرچه ضرایب آن صفر

---

۱) اگر درس جبرخطی را گرفته باشید این جمله را، همین‌طور مباحث گوناگون ذیل آن‌را، متوجه خواهید شد. هر آنچه در این بخش انجام می‌گیرد بسط و توسعه حقایقی استاندارد درباره پایه و بعد است در حالت ویژه‌ای که توسیع میدان $\mathbb{K}$ را به عنوان فضایی برداری روی میدان $\mathbb{F}$ در نظر می‌گیرند.

نیست، برای مثال

$$۲(۱+i)+\frac{۱}{۵}(۵i)-(۲+۳i)=۰$$

تمایز بین این دو وضعیت در مطالعه توسیع‌های میدان مهم است.

زیرمجموعه $\{v_۱,\dots,v_n\}$ از $\mathbb{K}$ را **مستقل خطی** روی $\mathbb{F}$ گویند مشروط به این که هرگاه برای برخی $c_i\in\mathbb{F}$ داشته باشیم

$$c_۱v_۱+c_۲v_۲+\cdots+c_nv_n=۰_{\mathbb{F}}{}^{۲}$$

آنگاه برای هر i، $c_i=۰_{\mathbb{F}}$. به مجموعه‌ای که مستقل خطی نباشد **وابسته خطی** گفته می‌شود. بنابراین یک مجموعه $\{u_۱,\dots,u_m\}$ وابسته خطی روی $\mathbb{F}$ است اگر عضوهای $b_۱,\dots,b_m$ در $\mathbb{F}$ موجود باشد که همگی صفر نیستند به طوری که $b_۱u_۱+\cdots+b_mu_m=۰_{\mathbb{F}}$.

مثال ۳.۹. تذکرات بند ماقبل‌آخر نشان می‌دهد که زیرمجموعه $\{۱,i\}$ از $\mathbb{C}$ روی $\mathbb{R}$ مستقل خطی است ولی مجموعه $\{۱+i,۵i,۲+۳i\}$ وابسته خطی است. توجه کنید که، بهرحال، هر دو این مجموعه‌ها $\mathbb{C}$ را پدید می‌آورند.

مثال ۴.۹. برای نشان دادن این که زیرمجموعه $\{۱,\sqrt{۲}\}$ از $\mathbb{R}$ مستقل خطی روی $\mathbb{Q}$ است، فرض کنید $r۱+s\sqrt{۲}=۰$ که در آن $r,s\in\mathbb{Q}$. اگر $s\neq ۰$ آنگاه $\sqrt{۲}=-r/s$، که با این واقعیت که $\sqrt{۲}$ اصم است (تمرین ۲ از بخش ۵.۴) متناقض است. بنابراین باید داشته باشیم $s=۰$ و از اینرو $r=۰$. ولی $\mathbb{R}$، $\{۱,\sqrt{۲}\}$ را پدید نمی‌آورد زیرا برای مثال، $\sqrt{۳}$ یک ترکیب خطی از ۱ و $\sqrt{۲}$ نیست (تمرین ۱۴).

مثال‌های قبل نشان می‌دهد که استقلال خطی و پدیدآوردن یکدیگر را نتیجه نمی‌دهند. یک زیرمجموعه از $\mathbb{K}$ ممکن است یک، هر دو و یا هیچ یک از این خواص را نداشته باشد. زیرمجموعه‌ای که هر دو خاصیت را داشته باشد نامی ویژه دارد. به یک زیرمجموعه $\{v_۱,\dots,v_n\}$ از $\mathbb{K}$ یک **پایه** روی $\mathbb{F}$ گفته می‌شود اگر این مجموعه $\mathbb{K}$ را پدید آورد و روی $\mathbb{F}$ مستقل خطی باشد. برای مثال، $\{۱,i\}$ یک پایه $\mathbb{C}$ روی $\mathbb{R}$ است.

---

۲) چون $\mathbb{F}$ زیرمیدان $\mathbb{K}$ است، طبق تمرین ۱۸ از بخش ۲.۳، $۰_{\mathbb{F}}=۰_{\mathbb{K}}$ و $۱_{\mathbb{F}}=۱_{\mathbb{K}}$. ما معمولاً $۰_{\mathbb{F}}$ و $۱_{\mathbb{F}}$ را بکار می‌بریم، البته در برخی موارد که موجب ابهام نشود، از $۰_{\mathbb{K}}$ و $۱_{\mathbb{K}}$ و یا حتی ۰ و ۱ نیز استفاده می‌کنیم.

مثال ۵.۹. ادعا می‌کنیم که مجموعه $\{1+i, 2i\}$ نیز یک پایه $\mathbb{C}$ روی $\mathbb{R}$ است. اگر $c_1, c_2 \in \mathbb{R}$ طوری باشد که $c_1(1+i) + c_2(2i) = 0$، آنگاه $c_1 1 + (c_1 + 2c_2)i = 0$ و این تنها وقتی می‌تواند بوقوع پیوندد که $c_1 = 0, c_1 + 2c_2 = 0$. ولی این ایجاب می‌کند که $2c_2 = 0$ و بدین جهت $c_2 = 0$. بنابراین مجموعه $\{1+i, 2i\}$ مستقل خطی است. برای دیدن این که $\mathbb{C}$ توسط $\{1+i, 2i\}$ پدید می‌آید، دقت کنید که هر عضو $a+bi \in \mathbb{C}$ را می‌توان به صورت $a(1+i) + (b - a/2)2i$ نوشت.

اینک به ذکر وضعیتی می‌پردازیم که همیشه منجر به وابستگی خطی می‌شود. فرض کنید $v, u_1, \ldots, u_t$ چند عضو یک زیرمجموعه S از $\mathbb{K}$ باشد و این که v ترکیبی خطی از $u_1, \ldots, u_t$ باشد. مثلاً $v = a_1u_1 + \cdots + a_tu_t$. اگر $w_1, \ldots, w_r$ بقیه عضوهای S باشد، آنگاه $v = a_1u_1 + \cdots + a_tu_t + 0_{\mathbb{F}}w_1 + \cdots + 0_{\mathbb{F}}w_r$ و از اینرو

$$-1_{\mathbb{F}}v + a_1u_1 + \cdots + a_tu_t + 0_{\mathbb{F}}w_1 + 0_{\mathbb{F}}w_2 + \ldots 0_{\mathbb{F}}w_r = 0_{\mathbb{F}}$$

چون لااقل یکی از این ضرایب ناصفر است (یعنی $-1_{\mathbb{F}}$) لذا S یک مجموعه وابسته خطی است. پس ما ثابت کرده‌ایم که

اگر $v \in \mathbb{K}$ یک ترکیب خطی از $u_1, \ldots, u_t \in \mathbb{K}$ باشد، آنگاه هر مجموعه شامل v و تمام‌این u_iها وابسته خطی است.

در واقع، قدری بیشتر درست است.

لم ۱.۹. گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد. زیرمجموعه $\{u_1, u_2, \ldots, u_n\}$ از $\mathbb{K}$ وابسته خطی است اگر و تنها اگر یک u_k ترکیبی خطی از عناصر قبلی‌اش، $u_1, \ldots, u_{k-1}$ باشد.

برهان. اگر یک u_k ترکیبی خطی از عناصر قبلی‌اش باشد آنگاه این مجموعه طبق تذکرات ماقبل از قضیه وابسته خطی است. بالعکس فرض کنید $\{u_1, \ldots, u_n\}$ وابسته خطی باشد. آنگاه باید عناصر $c_1, \ldots, c_n \in \mathbb{F}$ وجود داشته باشد که همگی صفر نیستند به طوری که

$$c_1u_1 + c_2u_2 + \cdots + c_nu_n = 0_{\mathbb{F}}.$$

گیریم k بزرگترین نمایه‌ای باشد که c_k ناصفر است. در این صورت برای $i > k$، $c_i = 0_{\mathbb{F}}$ و $c_1u_1 + c_2u_2 + \cdots + c_ku_k = 0_{\mathbb{F}}$. بدین دلیل

$$c_ku_k = -c_1u_1 - c_2u_1 - \cdots - c_{k-1}u_{k-1}.$$

چون $\mathbb{F}$ میدان است و $c_k \neq 0$، لذا c_k^{-1} وجود دارد. از ضرب طرفین معادله قبل در c_k^{-1} بدست می‌آید که u_k ترکیبی خطی از u_iهای قبلی است:

$$u_k = (-c_1 c_k^{-1})u_1 + (-c_2 c_k^{-1})u_2 + \cdots + (-c_{k-1} c_k^{-1})u_{k-1}.$$

به این ترتیب برهان کامل می‌شود. ■

لم بعدی یک کران بالا روی اندازه زیرمجموعه‌های مستقل خطی ارائه می‌کند. در اصل، این لم اظهار می‌کند که اگر $\mathbb{K}$ بتواند توسط n عضو روی $\mathbb{F}$ پدید آید، آنگاه هر زیرمجموعه مستقل خطی $\mathbb{K}$ حداکثر n عضو دارد.

لم ۲.۹. گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد که توسط $\{v_1, \ldots, v_n\}$ پدید آمده است. اگر $\{u_1, \ldots, u_m\}$ زیرمجموعه‌ای مستقل خطی از $\mathbb{K}$ باشد، آنگاه $m \leq n$.

برهان. طبق تعریف پدیدآوردن، هر عضو $\mathbb{K}$ (به ویژه u_1) ترکیبی خطی از $v_1, \ldots, v_n$ است. بنابراین مجموعه $\{u_1, v_1, v_2, \ldots, v_n\}$ وابسته خطی است. طبق لم ۱.۹ یکی از عضوهای این مجموعه ترکیبی خطی از عضوهای قبلی‌اش می‌باشد، مثلاً $v_i = a_1 u_1 + b_1 v_1 + \cdots + b_{i-1} v_{i-1}$. اگر v_i حذف شود، آنگاه مجموعه باقیمانده

$$\{u_1, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\} \qquad (*)$$

بازهم $\mathbb{K}$ را پدید می‌آورد زیرا هر عضو $\mathbb{K}$ ترکیبی خطی از vهاست و هر جا v_i ظاهر شود می‌توان آن را با $a_1 u_1 + b_1 v_1 + \cdots + b_{i-1} v_{i-1}$ جایگزین کرد. بویژه u_2 ترکیبی خطی از عضوهای مجموعه $(*)$ است. در نتیجه مجموعه $\{u_1, u_2, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\}$ وابسته خطی است. مجدداً طبق لم ۱.۹ یکی از عضوهای این مجموعه ترکیبی خطی از عضوهای قبلی‌اش می‌باشد. این عضو نمی‌تواند یکی از uها باشد زیرا این ایجاب می‌کند که uها وابسته خطی باشند. بنابراین یک v_j ترکیبی خطی از u_1، u_2 و vهای قبلی‌اش می‌باشد. حذف v_j مجموعه

$$\{u_1, u_2, \ldots, v_{i-1} v_{i+1}, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n\}$$

را ایجاد می‌کند. این مجموعه باز هم $\mathbb{K}$ را پدید می‌آورد زیرا هر عضو $\mathbb{K}$ ترکیبی خطی از vهاست و v_i و v_j را می‌توان با ترکیب‌های خطی از u_1، u_2 و vهای دیگر جایگزین کرد. به ویژه، u_2 ترکیبی

خطی از عضوهای مجموعهٔ جدید است. می‌توانیم این فرآیند را ادامه دهیم، در هر مرحله یک u اضافه و یک v حذف کنیم و مجموعه‌ای بسازیم که $\mathbb{K}$ را پدید آورد. اگر $m > n$، تمام vها را قبل از این که تمام uها درج شوند حذف می‌کنیم. مجموعه‌ای به صورت $\{u_1, \ldots, u_n\}$ حاصل می‌شود که $\mathbb{K}$ را پدید می‌آورد. ولی این بدین معنی است که u_m ترکیبی خطی از u_1، ...، u_n است که متناقض با مستقل‌خطی بودن $\{u_1, \ldots, u_m\}$ است. بنابراین $m \leq n$. ■

قضیه ۳.۹. گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد. آنگاه هر دو پایه متناهی $\mathbb{K}$ روی $\mathbb{F}$ دارای تعداد عضوهای یکسان می‌باشند.

برهان. فرض کنید $\{u_1, \ldots, u_m\}$ و $\{v_1, \ldots, v_n\}$ پایه‌های $\mathbb{K}$ روی $\mathbb{F}$ باشند. آنگاه vها $\mathbb{K}$ را پدید می‌آورند و uها مستقل خطی‌اند، بنابراین طبق لم ۲.۹، $m \leq n$. اکنون نقش‌ها را عوض کنید، uها $\mathbb{K}$ را پدید می‌آورند و vها مستقل خطی‌اند، در نتیجه بازهم طبق لم ۲.۹، $n \leq m$ بنابراین $m = n$. ■

طبق قضیه ۳.۹ تعداد عضوهای یک پایه $\mathbb{K}$ روی $\mathbb{F}$ بستگی به این که چه پایه‌ای انتخاب می‌شود ندارد. بنابراین این عدد یک خاصیت پایای توسیع است.

تعریف. اگر $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد که پایه‌ای متناهی دارد، آنگاه گفته می‌شود که $\mathbb{K}$ روی $\mathbb{F}$ با **بعد متناهی** است. **بعد** $\mathbb{K}$ روی $\mathbb{F}$ تعداد عضوهای پایه دلخواهی از $\mathbb{K}$ است و با $[\mathbb{K} : \mathbb{F}]$ نشان داده می‌شود. اگر $\mathbb{K}$ پایه متناهی نداشته باشد، آنگاه گفته می‌شود که $\mathbb{K}$ **بعد نامتناهی** روی $\mathbb{F}$ دارد.

مثال ۶.۹. $[\mathbb{C} : \mathbb{R}] = ۲$ زیرا $\{۱, i\}$ پایه‌ای از $\mathbb{C}$ روی $\mathbb{R}$ است. از جهت دیگر $\mathbb{R}$ یک توسیع میدان با بعد نامتناهی روی $\mathbb{Q}$ است. برهان این واقعیت در اینجا حذف شده است زیرا حقایقی نابدیهی درباره کاردینال مجموعه‌های نامتناهی را می‌طلبد.

تذکر. اگر $[\mathbb{K} : \mathbb{F}] = ۱$ و $\{u\}$ یک پایه باشد، آنگاه هر عضو $\mathbb{K}$ به‌صورت cu برای برخی $c \in \mathbb{F}$ می‌باشد. به ویژه، $cu = ۱_{\mathbb{F}}$ و از اینرو $u = c^{-۱} \in \mathbb{F}$. بدین دلیل $\mathbb{K} = \mathbb{F}$. از جهت دیگر، اگر $\mathbb{K} = \mathbb{F}$، به سادگی می‌توان دید که $\{۱_{\mathbb{F}}\}$ یک پایه است و بدین جهت $[\mathbb{K} : \mathbb{F}] = ۱$. بنابراین

$$[\mathbb{K} : \mathbb{F}] = ۱ \text{ اگر و تنها اگر } \mathbb{K} = \mathbb{F}.$$

قضیه ۴.۹. گیریم $\mathbb{F}$، $\mathbb{K}$ و $\mathbb{L}$ میدان‌هایی باشند که $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$. اگر $[\mathbb{K} : \mathbb{F}]$ و $[\mathbb{L} : \mathbb{K}]$

متناهی باشند، آنگاه $\mathbb{L}$ یک توسیع با بعدمتناهی $\mathbb{F}$ است و $[\mathbb{L}:\mathbb{F}]=[\mathbb{L}:\mathbb{K}][\mathbb{K}:\mathbb{F}]$.

برهان. فرض کنید $m=[\mathbb{K}:\mathbb{F}]$ و $n=[\mathbb{L}:\mathbb{K}]$. آنگاه یک پایه $\{u_1,\dots,u_m\}$ از $\mathbb{K}$ روی $\mathbb{F}$ و یک پایه $\{v_1,\dots,v_n\}$ از $\mathbb{L}$ روی $\mathbb{K}$ وجود دارد. طبق تمرین ۱۳ تمام حاصل‌ضرب‌های u_iv_j ناصفرند. مجموعه تمام حاصل‌ضرب‌های $\{u_iv_j \mid 1\le i\le m, 1\le j\le n\}$ دارای دقیقاً mn عضو است (هیچ دوتا از آن‌ها نمی‌تواند برابر باشد زیرا $u_iv_j=u_kv_t$ ایجاب می‌کند که $u_iv_j-u_kv_t=0$ که در آن $u_i,u_k\in\mathbb{K}$، که متناقض با استقلال vها روی $\mathbb{K}$ است). تنها کافی است نشان دهیم که این مجموعه mn عضوی، پایه‌ای از $\mathbb{L}$ روی $\mathbb{F}$ است زیرا در این صورت $[\mathbb{L}:\mathbb{F}]=mn=[\mathbb{L}:\mathbb{K}][\mathbb{K}:\mathbb{F}]$.

اگر w عضوی دلخواه از $\mathbb{L}$ باشد، آنگاه w ترکیبی خطی از عناصر پایه v_1، ...، v_n است، مثلاً

$$w=b_1v_1+b_2v_2+\cdots+b_nv_n \qquad (*)$$

که در آن $b_j\in\mathbb{K}$ برای هر j.

از طرفی هر $b_j\in\mathbb{K}$ ترکیبی خطی از عناصر پایه $u_1,\dots,u_m$ است، بنابراین $a_{ij}\in\mathbb{F}$ وجود دارد به طوری که

$$\begin{aligned}
b_1&=a_{11}u_1+\cdots+a_{m1}u_m\\
b_2&=a_{12}u_1+\cdots+a_{m2}u_m\\
&\vdots\\
b_n&=a_{1n}u_1+\cdots+a_{mn}u_m.
\end{aligned}$$

جایگزینی طرف راست هر یک از این عبارات در $(*)$ نشان می‌دهد که w مجموعی از جملات به صورت $a_{ij}u_iv_j$ است که در آن $a_{ij}\in\mathbb{F}$. بنابراین مجموعه حاصل‌ضرب‌های u_iv_j، $\mathbb{L}$ را روی $\mathbb{F}$ پدید می‌آورد.

برای اثبات استقلال خطی، فرض کنید $c_{ij}\in\mathbb{F}$ و

$$\sum_{i,j}c_{ij}u_iv_j=c_{11}u_1v_1+c_{12}u_1v_2+\cdots+c_{mn}u_mv_n=0_{\mathbb{F}} \qquad (**)$$

با جمع‌آوری تمام جملات شامل v_1، بعد تمام آنهایی که شامل v_2 هستند، و همین طور الی‌آخر، می‌توان

(**) را به صورت

$$(c_{11}u_1 + c_{21}u_2 + \cdots + c_{m1}u_m)v_1 + (c_{12}u_2 + c_{22}u_2 + \cdots + c_{m2}u_m)v_2 +$$
$$\cdots + (c_{1n}u_1 + c_{2n}u_2 + \cdots + c_{mn}u_m)v_n = 0_{\mathbb{F}}$$

ضرایب vها عضوهای $\mathbb{K}$ هستند، بنابراین استقلال vها ایجاب می‌کند که برای هر $j = 1, \ldots, n$

$$c_{1j}u_1 + c_{2j}u_2 + \cdots + c_{mj}u_m = 0_{\mathbb{F}}$$

چون $c_{ij} \in \mathbb{F}$ و uها مستقل خطی روی $\mathbb{F}$ هستند باید داشته باشیم $c_{ij} = 0_{\mathbb{F}}$ برای هر i و j. این برهان استقلال خطی را کامل می‌کند، و قضیه ثابت می‌شود. ■

قضیه زیر برای برهان قضیه ۱۵.۹ در بخش ۴.۹ مورد نیاز خواهد بود.

قضیه ۵.۹. گیریم $\mathbb{K}$ و $\mathbb{L}$ توسیع‌های میدان $\mathbb{F}$ و گیریم $f : \mathbb{K} \to \mathbb{L}$ یک یکریختی باشد به طوری که برای هر $c \in \mathbb{F}$، $f(c) = c$. آنگاه $[\mathbb{L} : \mathbb{F}] = [\mathbb{K} : \mathbb{F}]$.

برهان. فرض کنید $[\mathbb{K} : \mathbb{F}] = n$ و $\{u_1, \ldots, u_n\}$ یک پایه $\mathbb{K}$ روی $\mathbb{F}$ باشد. برای این که ثابت کنیم که $[\mathbb{L} : \mathbb{F}]$ هم برابر n است، تنها لازم است نشان دهیم که $\{f(u_1), \ldots, f(u_n)\}$ یک پایه $\mathbb{L}$ روی $\mathbb{F}$ است. گیریم $v \in \mathbb{L}$، آنگاه چون f یکریختی است یک $u \in \mathbb{K}$ وجود دارد به طوری که $v = f(u)$. طبق تعریف پایه، $u = c_1u_1 + \cdots + c_nu_n$ که در آن $c_i \in \mathbb{F}$. بدین دلیل

$$v = f(u) = f(c_1u_1 + \cdots + c_nu_n) = f(c_1)f(u_1) + \cdots + f(c_n)f(u_n).$$

ولی برای هر i، $f(c_i) = c_i$، لذا $v = c_1f(u_1) + \cdots + c_nf(u_n)$. بنابراین مجموعه $\{f(u_1), \ldots, f(u_n)\}$، $\mathbb{L}$ را پدید می‌آورد. برای نشان دادن استقلال خطی، فرض کنید $d_1f(u_1) + \cdots + d_nf(u_n) = 0_{\mathbb{F}}$ که در آن $d_i \in \mathbb{F}$، آنگاه چون $f(d_i) = d_i$، داریم

$$f(d_1u_1 + \cdots + d_nu_n) = f(d_1)f(u_1) + \cdots + f(d_n)f(u_n)$$
$$= d_1f(u_1) + \cdots + d_n(fu_n) = 0_{\mathbb{F}}$$

چون یکریختی f یک به یک است، طبق قضیه ۹.۶، $d_1u_1 + \cdots + d_nu_n = 0_{\mathbb{F}}$. ولی uها در $\mathbb{K}$ مستقل خطی هستند و از اینرو $d_i = 0_{\mathbb{F}}$. بدین دلیل $\{f(u_1), \ldots, f(u_n)\}$ مستقل خطی

است و بنابراین یک پایه می‌باشد. ■

تمرینها

توجه: $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ است.

A.۱. نشان دهید که $\{i, ۱ + ۲i, ۱ + ۳i\}$، $\mathbb{C}$ را روی $\mathbb{R}$ پدید می‌آورد.

۲. اگر $\{v_۱, v_۲, \ldots, v_n\}$، $\mathbb{K}$ را روی $\mathbb{F}$ پدید آورد و w عضو دلخواهی از $\mathbb{K}$ باشد، نشان دهید که $\{w, v_۱, v_۲, \ldots, v_n\}$ نیز $\mathbb{K}$ را پدید می‌آورد.

۳. نشان دهید که $\{\sqrt{۲}, \sqrt{۲} + i, \sqrt{۳} - i\}$ روی $\mathbb{R}$ مستقل خطی است.

۴. اگر v عضو ناصفری از $\mathbb{K}$ باشد، ثابت کنید که $\{v\}$ مستقل خطی روی $\mathbb{F}$ است.

۵. ثابت کنید که هر زیرمجموعه از $\mathbb{K}$ که شامل $۰_{\mathbb{F}}$ باشد وابسته خطی روی $\mathbb{F}$ است.

۶. اگر زیرمجموعه $\{u, v, w\}$ از $\mathbb{K}$ مستقل خطی روی $\mathbb{F}$ باشد، ثابت کنید که زیرمجموعه $\{u, u + v, u + v + w\}$ مستقل خطی است.

۷. اگر $S = \{v_۱, \ldots, v_k\}$ یک زیرمجموعه وابسته خطی از $\mathbb{K}$ باشد، ثابت کنید که هر زیرمجموعه از $\mathbb{K}$ که شامل S باشد نیز وابسته خطی روی $\mathbb{F}$ است.

۸. اگر زیرمجموعه $T = \{u_۱, \ldots, u_t\}$ از $\mathbb{K}$ مستقل خطی روی $\mathbb{F}$ باشد، ثابت کنید که هر زیرمجموعه ناتهی از T نیز مستقل خطی است.

۹. گیریم b و d دو عدد حقیقی ناصفر متمایز و c عدد حقیقی دلخواهی باشد. ثابت کنید که $\{b, c + di\}$ یک پایه $\mathbb{C}$ روی $\mathbb{R}$ است.

۱۰. اگر $\mathbb{K}$ یک توسیع میدان nـبعدی میدان $\mathbb{Z}_p$ باشد، بیشترین تعداد عضو ممکن در $\mathbb{K}$ چقدر است؟

۱۱. گیریم $\{v_۱, \ldots, v_n\}$ پایه‌ای از $\mathbb{K}$ روی $\mathbb{F}$ و گیریم $c_۱$، ...، c_n عضوهای ناصفری از $\mathbb{F}$ باشد. ثابت کنید که $\{c_۱v_۱, c_۲v_۲, \ldots, c_nv_n\}$ نیز یک پایه $\mathbb{K}$ روی $\mathbb{F}$ است.

۱۲. نشان دهید که $\{۱, [x]\}$ یک پایهٔ $\mathbb{Z}_۲[x]/(x^۲ + x + ۱)$ روی $\mathbb{Z}_۲$ است.

۱۳. گیریم $\mathbb{F}$، $\mathbb{K}$، $\mathbb{L}$ و u_i، v_j همان‌هایی باشند که در برهان قضیه ۴.۹ آمده است. ثابت کنید که تمام حاصل‌ضرب‌های u_iv_j ناصفر هستند.

۱۴.B. ثابت کنید که $\sqrt{۳}$ یک ترکیب خطی از ۱ و $\sqrt{۲}$ روی $\mathbb{Q}$ نیست.

۱۵. (الف) نشان دهید که $\{۱, \sqrt{۲}, \sqrt{۳}\}$ مستقل خطی روی $\mathbb{Q}$ است.

(ب) نشان دهید که $\{۱, \sqrt{۲}, \sqrt{۳}, \sqrt{۶}\}$ روی $\mathbb{Q}$ مستقل خطی است.

۱۶. گیریم v یک عدد حقیقی ناصفر باشد. ثابت کنید که $\{۱, v\}$ روی $\mathbb{Q}$ مستقل خطی است اگر و تنها اگر v اصم باشد.

۱۷. ثابت کنید که $\mathbb{K}$ دقیقاً یک پایه روی $\mathbb{F}$ دارد اگر و تنها اگر $\mathbb{K} = \mathbb{F} \cong \mathbb{Z}_۲$.

۱۸. فرض کنید $۱_{\mathbb{F}} + ۱_{\mathbb{F}} \neq ۰_{\mathbb{F}}$. اگر $\{u, v, w\}$ یک پایه $\mathbb{K}$ روی $\mathbb{F}$ باشد، ثابت کنید که مجموعه $\{u+v, v+w, u+w\}$ نیز یک پایه است.

۱۹. ثابت کنید که $\{v_۱, \ldots, v_n\}$ یک پایه $\mathbb{K}$ روی $\mathbb{F}$ است اگر و تنها اگر هر عضو $\mathbb{K}$ را بتوان به طور یکتایی به صورت یک ترکیب خطی از $v_۱$، ...، v_n نوشت ("یکتایی" به این معنی است که اگر $w = c_۱v_۱ + \cdots + c_nv_n$ و $w = d_۱v_۱ + \cdots + d_nv_n$، آنگاه برای هر i، $c_i = d_i$).

۲۰. گیریم $p(x) = a_۰ + a_۱x + \cdots + a_nx^n$ در $\mathbb{F}[x]$ تحویل‌ناپذیر باشد و گیریم $\mathbb{L}$ توسیع میدان $\mathbb{F}[x]/(p(x))$ از $\mathbb{F}$ باشد. ثابت کنید که $\mathbb{L}$ روی $\mathbb{F}$ دارای بعد n است. [نتیجه ۵.۵، قضیه ۸.۵ و ۹.۵ و تمرین ۱۹ می‌تواند مفید باشد.]

۲۱. اگر زیرمجموعه $\{u_۱, \ldots, u_t\}$ از $\mathbb{K}$ روی $\mathbb{F}$ مستقل خطی باشد و $w \in \mathbb{K}$ ترکیبی خطی از uها نباشد، ثابت کنید که $\{u_۱, \ldots, u_t, w\}$ مستقل خطی است.

۲۲. اگر $S = \{v_۱, \ldots, v_t\}$، $\mathbb{K}$ را روی $\mathbb{F}$ پدید آورد، ثابت کنید که یک زیرمجموعه از S پایه‌ای از $\mathbb{K}$ روی $\mathbb{F}$ است. [راهنمایی: لم ۱.۹ را مکرراً بکار برید تا vها را حذف نمایید و به مجموعه‌ای تنزل کنید که هنوز $\mathbb{K}$ را پدید می‌آورد و مستقل خطی است.]

۲۳. فرض کنید که زیرمجموعه $\{v_۱, \ldots, v_n\}$ از $\mathbb{K}$ روی $\mathbb{F}$ مستقل خطی باشد. ثابت کنید که اگر $w = c_۱v_۱ + \cdots + c_nv_n$، که در آن $c_i \in \mathbb{F}$، آنگاه مجموعه $\{w - v_۱, w - v_۲, \ldots, w - v_n\}$ روی $\mathbb{F}$ مستقل خطی است اگر و تنها اگر $c_۱ + \cdots + c_n \neq ۱_{\mathbb{F}}$.

۲۴. فرض کنید که $\mathbb{K}$ روی $\mathbb{F}$ با بعدمتناهی باشد و S یک زیرمجموعه مستقل خطی $\mathbb{K}$ باشد. ثابت کنید که S در یک پایهٔ $\mathbb{K}$ قرار دارد. [راهنمایی: گیریم $n = [\mathbb{K} : \mathbb{F}]$ و $S = \{u_1, \ldots, u_m\}$؛ آنگاه طبق لم ۲.۹، $m \leq n$. اگر S، $\mathbb{K}$ را پدید نیاورد، آنگاه باید یک w وجود داشته باشدکه ترکیبی خطی از uها نیست. تمرین ۲۱ را بکار برید تا مجموعهٔ مستقل بزرگتری بدست آید، اگر این مجموعه $\mathbb{K}$ را پدید نیاورد، این استدلال را تکرار کنید. از لم ۲.۹ استفاده کنید تا نشان دهید که این فرایند باید به پایه‌ای که S را شامل است خاتمه یابد.]

۲۵. فرض کنید که $n = [\mathbb{K} : \mathbb{F}]$. ثابت کنید که شرایط زیر هم‌ارزند:

(الف) $\{v_1, \ldots, v_n\}$، $\mathbb{K}$ را روی $\mathbb{F}$ پدید می‌آورد.

(ب) $\{v_1, \ldots, v_n\}$ روی $\mathbb{F}$ مستقل خطی است.

(پ) $\{v_1, \ldots, v_n\}$ پایه‌ای برای $\mathbb{K}$ روی $\mathbb{F}$ است.

۲۶. اگر $\mathbb{F}$، $\mathbb{K}$ و $\mathbb{L}$ میدان‌هایی باشد که $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ و $[\mathbb{L} : \mathbb{F}]$ متناهی باشد، ثابت کنید که $[\mathbb{K} : \mathbb{F}]$ متناهی است و $[\mathbb{K} : \mathbb{F}] \leq [\mathbb{L} : \mathbb{F}]$. [راهنمایی گیریم $n = [\mathbb{L} : \mathbb{F}]$ مجموعه $\{1_{\mathbb{K}}\}$ طبق تمرین ۴ مستقل خطی است، اگر این مجموعه $\mathbb{K}$ را پدید نیاورد، مثل راهنمایی تمرین ۲۴ عمل کنید تا زیرمجموعه مستقل خطی بزرگ و بزرگتری از $\mathbb{K}$ بسازید، از لم ۲.۹ و این واقعیت که $n = [\mathbb{L} : \mathbb{F}]$ استفاده کنید تا نشان دهید که این فرایند باید به پایه‌ای از $\mathbb{K}$ که حداکثر n عضو دارد، خاتمه یابد.]

۲۷. اگر $p = [\mathbb{K} : \mathbb{F}]$ که در آن p اول است، ثابت کنید که هیچ میدان $\mathbb{E}$ وجود ندارد به طوری که $\mathbb{F} \subsetneq \mathbb{E} \subsetneq \mathbb{K}$. [راهنمایی: تمرین ۲۶ و قضیه ۴.۹]

۹-۲ توسیع‌های ساده

توسیع‌های میدان را می‌توان از دو جهت بررسی کرد. از طرف بالا می‌توان به توسیع‌های آن نگریست و از طرف پایین زیر میدان‌های آن را مورد توجه قرار داد. در فصل ۵ مثالی از نگاه به طرف بالا ارائه شد، یک میدان $\mathbb{F}$ و یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}[x]$ اختیار کردیم و میدان کلاس‌های همنهشتی (یعنی، میدان خارج قسمت) $\mathbb{F}[x]/(p(x))$ را تشکیل دادیم. قضیه ۱۰.۵ نشان می‌دهد که $\mathbb{F}[x]/(p(x))$ توسیعی از میدان $\mathbb{F}$ است که ریشه‌ای از $p(x)$ را شامل است.

در این بخش دیدگاه به طرف پایین را اختیار می‌کنیم، از یک میدان $\mathbb{K}$ و یک زیرمیدان $\mathbb{F}$ شروع می‌کنیم. اگر $u \in \mathbb{K}$، در مورد زیرمیدان‌هایی از $\mathbb{K}$ که u و $\mathbb{F}$ را تواماً شامل است چه می‌توان گفت؟ آیا کوچکترین چنین میدان‌هایی وجود دارد؟ اگر u ریشه‌ای از یک چندجمله‌ای تحویل‌ناپذیر $p(x)$ در $\mathbb{F}[x]$ باشد، این کوچکترین زیرمیدان چگونه با توسیع میدان $\mathbb{F}[x]/(p(x))$، که این میدان نیز ریشه‌ای از $p(x)$ را شامل است، مرتبط است؟

پاسخ نظری به دو سوال اول کاملاً ساده است. گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ و $u \in \mathbb{K}$. گیریم $\mathbb{F}(u)$ نمایش اشتراک تمام زیرمیدان‌هایی از $\mathbb{K}$ باشد که تواماً $\mathbb{F}$ و u را شامل است (این خانواده از زیرمیدان‌ها ناتهی است زیرا حداقل $\mathbb{K}$ در آن است). چون اشتراک هر خانواده از زیرمیدان‌های $\mathbb{K}$ خود یک میدان است (تمرین ۱)، $\mathbb{F}(u)$ یک میدان است. $\mathbb{F}(u)$، طبق تعریفش، در هر زیرمیدانی از $\mathbb{K}$ که $\mathbb{F}$ و u را شامل است، قرار دارد و از اینرو $\mathbb{F}(u)$ کوچکترین زیرمیدانی از $\mathbb{K}$ است که $\mathbb{F}$ و u را شامل است. $\mathbb{F}(u)$ را یک **توسیع سادهٔ** $\mathbb{F}$ گویند.

از جنبه ساختاری این پاسخ رضایت‌بخشی نیست. توصیف روشنتری از توسیع میدان ساده $\mathbb{F}(u)$ ضرورت دارد. معلوم می‌شود که ساختار $\mathbb{F}(u)$ بستگی به این دارد که آیا u ریشه یک چندجمله‌ای در $\mathbb{F}[x]$ هست یا نه. بنابراین لازم است ابتدا چند اصطلاح علمی در مورد چنین uهایی را بیان کنیم.

عضو u از یک توسیع میدان $\mathbb{K}$ از $\mathbb{F}$ را روی $\mathbb{F}$ **جبری** گویند اگر u ریشه یک چندجمله‌ای ناصفر $\mathbb{F}[x]$ باشد. به عضوی از $\mathbb{K}$ که ریشه هیچ چندجمله‌ای ناصفر $\mathbb{F}[x]$ نباشد، **عضو متعالی** روی $\mathbb{F}$ گفته می‌شود.

مثال ۷.۹. در توسیع میدان $\mathbb{C}$ از $\mathbb{R}$، i روی $\mathbb{R}$ جبری است زیرا i ریشهٔ $x^2 + 1 \in \mathbb{R}[x]$ است. به سادگی می‌توانید تحقیق کنید که عضو $i + 2$ از $\mathbb{C}$ ریشه‌ای از $x^3 - x^2 - 7x + 15 \in \mathbb{Q}[x]$ است. بدین دلیل $i + 2$ روی $\mathbb{Q}$ جبری است. به طور مشابه، $\sqrt[5]{3}$ روی $\mathbb{Q}$ جبری است زیرا ریشه‌ای از $x^5 - 3$ می‌باشد.

مثال ۸.۹. هر عضو c در یک میدان $\mathbb{F}$ روی $\mathbb{F}$ جبری است زیرا c ریشه $x - c \in \mathbb{F}[x]$ است.

مثال ۹.۹. اعداد حقیقی π و e روی $\mathbb{Q}$ متعالی هستند. این حقایق غیربدیهی اوّل بار در قرن

نوزدهم ثابت شد. برای اثباتی از آن، نی‌ون[۳] [۳۱] را ملاحظه کنید. از این به بعد توجه خود را به عناصر جبری معطوف خواهیم کرد. برای اطلاع بیشتر از عناصر متعالی، تمرین‌های ۱۰ و ۲۶-۲۴ را ملاحظه فرمایید.

اگر u عضو جبری از یک توسیع میدان $\mathbb{K}$ از $\mathbb{F}$ باشد، آنگاه ممکن است چندجمله‌ای‌های مختلفی در $\mathbb{F}[x]$ موجود باشد که u یک ریشه آنها است، قضیه بعد نشان می‌دهد که همه این چندجمله‌ای‌ها مضاربی از یک چندجمله‌ای هستند؛ این چندجمله‌ای به ما کمک می‌کند تا توصیفی دقیق از توسیع ساده $\mathbb{F}(u)$ ارائه کنیم.

قضیه ۶.۹. گیریم $\mathbb{K}$ توسیع میدان $\mathbb{F}$ و u یک عضو جبری روی $\mathbb{F}$ باشد. آنگاه یک چندجمله‌ای تکین تحویل‌ناپذیر یکتای $p(x)$ در $\mathbb{F}[x]$ وجود دارد که u را به عنوان یک ریشه دارد. به علاوه، اگر u ریشه‌ای از $g(x) \in \mathbb{F}[x]$ باشد، آنگاه $p(x)$، $g(x)$ را می‌شمارد.

برهان. گیریم S مجموعه تمام چندجمله‌ای‌های ناصفر در $\mathbb{F}[x]$ باشد که u را به عنوان ریشه دارد. آنگاه S ناتهی است زیرا u روی $\mathbb{F}$ جبری است. درجات چندجمله‌ای‌های واقع در S زیرمجموعه‌ای از اعداد صحیح نامنفی است که طبق اصل خوش‌ترتیبی باید یک کوچکترین عضو داشته باشد. فرض کنید $p(x)$ یک چندجمله‌ای ازکمترین درجه در S باشد. هر مضرب ثابت ناصفر $p(x)$ یک چندجمله‌ای از همان درجه است که u ریشه آن است. پس می‌توانیم $p(x)$ را تکین اختیارکنیم (اگر چنین نباشد، در وارون ضریب پیشروش ضرب کنید).

اگر $p(x)$ در $\mathbb{F}[x]$ تحویل‌ناپذیر نباشد، چندجمله‌ای‌های $k(x)$ و $t(x)$ وجود خواهند داشت به طوری که $p(x) = k(x)t(x)$، که در آن $\deg k(x) < \deg p(x)$ و $\deg t(x) < \deg p(x)$. در نتیجه، در $\mathbb{K}$ داریم $k(u)t(u) = p(u) = 0_{\mathbb{F}}$. چون $\mathbb{K}$ میدان است یا $k(u) = 0_{\mathbb{F}}$ یا $t(u) = 0_{\mathbb{F}}$، یعنی یا $k(x)$ یا $t(x)$ در S است. این غیرممکن است زیرا $p(x)$ یک چندجمله‌ای ازکمترین درجه در S اختیار شد. از اینرو $p(x)$ تحویل‌ناپذیر است.

اینک نشان می‌دهیم که $p(x)$ هر چندجمله‌ای $g(x)$ در S را می‌شمارد. طبق الگوریتم تقسیم، $g(x) = p(x)q(x) + r(x)$، که در آن $r(x) = 0_{\mathbb{F}}$ یا $\deg r(x) < \deg p(x)$. چون u ریشه‌ای از هر دو $g(x)$ و $p(x)$ می‌باشد لذا

$$r(u) = g(u) - p(u)q(u) = 0_{\mathbb{F}} + 0_{\mathbb{F}}q(u) = 0_{\mathbb{F}}$$

۳) Niven

بنابراین u یک ریشه $r(x)$ است. اگر $r(x)$ ناصفر باشد، آنگاه $r(x)$ در S خواهد بود که متناقض با این واقعیت است که $p(x)$ یک چندجمله‌ای از کمترین درجه در S است. بنابراین $r(x) = ۰_{\mathbb{F}}$، یعنی $g(x) = p(x)q(x)$. پس $p(x)$ هر چندجمله‌ای واقع در S را می‌شمارد.

برای این که ثابت کنیم $p(x)$ یکتاست، فرض کنید $t(x)$ یک چندجمله‌ای تکین تحویل‌ناپذیر در S باشد آنگاه $p(x)|t(x)$. چون $p(x)$ تحویل‌ناپذیر است (و بنابراین غیرثابت) و $t(x)$ تحویل‌ناپذیر است، باید برای یک $c \in \mathbb{F}$ داشته باشیم $t(x) = cp(x)$. ولی $p(x)$ تکین است، بنابراین c ضریب پیشرو $cp(x)$ است و از اینرو ضریب پیشرو $t(x)$ است. چون $t(x)$ تکین است، باید داشته باشیم $c = ۱_{\mathbb{F}}$. بنابراین $p(x) = t(x)$ و $p(x)$ یکتاست. ■

اگر $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد و $u \in \mathbb{K}$ روی $\mathbb{F}$ جبری باشد، آنگاه چندجمله‌ای تکین تحویل‌ناپذیر $p(x)$ در قضیه ۶.۹، **چندجمله‌ای کمین** u روی $\mathbb{F}$ نامیده می‌شود. بیان یکتایی در قضیه ۶.۹ بدین معنی است که وقتی یک چندجمله‌ای تکین تحویل‌ناپذیر در $\mathbb{F}[x]$ یافتیم که u را به عنوان ریشه دارد، این چندجمله‌ای باید چندجمله کمین u روی $\mathbb{F}$ باشد.

مثال ۱۰.۹. $x^۲ - ۳$ در $\mathbb{Q}[x]$ یک چندجمله‌ای تحویل‌ناپذیر کمین است که $\sqrt{۳} \in \mathbb{R}$ ریشه آن می‌باشد. بنابراین $x^۲ - ۳$ چندجمله‌ای کمین $\sqrt{۳}$ روی $\mathbb{Q}$ است. توجه داشته باشید که $x^۲ - ۳$ روی $\mathbb{R}$ تحویل‌پذیر است زیرا به صورت $(x + \sqrt{۳})(x - \sqrt{۳})$ در $\mathbb{R}[x]$ تجزیه می‌شود. بنابراین چندجمله‌ای کمین $\sqrt{۳}$ روی $\mathbb{R}$، $x - \sqrt{۳}$ است که تکین و تحویل‌ناپذیر در $\mathbb{R}[x]$ است.

مثال ۱۱.۹. گیریم $u = \sqrt{۳} + \sqrt{۵} \in \mathbb{R}$. آنگاه $u^۲ = ۳ + ۲\sqrt{۳}\sqrt{۵} + ۵ = ۸ + ۲\sqrt{۱۵}$. از اینرو $۲\sqrt{۱۵} = u^۲ - ۸$ و لذا $(u^۲ - ۸)^۲ = ۶۰$). بنابراین $u = \sqrt{۳} + \sqrt{۵}$ یک ریشه $(x^۲ - ۸)^۲ - ۶۰ = x^۴ - ۱۶x^۲ + ۴ \in \mathbb{Q}[x]$ است. تحقیق کنید که این چندجمله‌ای در $\mathbb{Q}[x]$ تحویل‌ناپذیر است (تمرین ۱۴). بدین دلیل باید چندجمله‌ای کمین $\sqrt{۵} + \sqrt{۳}$ روی $\mathbb{Q}$ باشد.

چندجمله‌ای کمین u بین دیدگاه‌های به طرف بالا و پایین در توسیع‌های میدان ساده ارتباط برقرار می‌کند و به ما اجازه می‌دهد که توصیفی مفید از $\mathbb{F}(u)$ ارائه کنیم.

قضیه ۷.۹. گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ و $u \in \mathbb{K}$ یک عضو جبری روی $\mathbb{F}$ با چندجمله‌ای کمین $p(x)$ از درجه n باشد. آنگاه

(۱) $\mathbb{F}(u) \cong \mathbb{F}[x]/(p(x))$

(۲) $\{1_{\mathbb{F}}, u, u^2, \ldots, u^{n-1}\}$ یک پایه $\mathbb{F}(u)$ روی $\mathbb{F}$ است.

(۳) $[\mathbb{F}(u) : \mathbb{F}] = n$.

قضیه ۷.۹ نشان می‌دهد که وقتی u روی $\mathbb{F}$ جبری است، آنگاه $\mathbb{F}(u)$ بستگی به $\mathbb{K}$ ندارد ولی به طور کامل توسط $\mathbb{F}[x]$ و چندجمله‌ای کمین $p(x)$ تعیین می‌گردد. در نتیجه، بعضاً می‌گوییم که $\mathbb{F}(u)$ میدانی است که از **الحاق (اتصال) u به $\mathbb{F}$ بدست آمده‌است.**

برهان قضیه ۷.۹. (۱) چون $\mathbb{F}(u)$ میدانی است که شامل u است، باید هر توان مثبت u را شامل باشد. چون $\mathbb{F}(u)$، $\mathbb{F}$ را هم شامل است، $\mathbb{F}(u)$ هر عضو به صورت $b_0 + b_1u + b_2u^2 + \cdots + b_tu^t$ که در آن $b_i \in \mathbb{F}$ را نیز شامل است یعنی برای هر $f(x) \in \mathbb{F}[x]$، عضو $f(u)$ را شامل است. تحقیق کنید که نگاشت $\varphi : \mathbb{F}[x] \to \mathbb{F}(u)$ که توسط $\varphi(f(x)) = f(u)$ تعریف می‌شود یک همریختی حلقه‌ای است. یک چندجمله‌ای در $\mathbb{F}[x]$ در هسته φ قرار دارد، دقیقاً وقتی که u را به عنوان یک ریشه داشته باشد. طبق قضیه ۶.۹، هسته φ ایده‌آل اصلی $(p(x))$ است. قضیه اول یکریختی ۱۱.۶، نشان می‌دهد که $\mathbb{F}[x]/(p(x))$ یکریخت با $\mathrm{Im}\varphi$ است تحت نگاشتی که کلاس همنهشتی (هم‌مجموعه) $[f(x)]$ را به $f(u)$ می‌فرستد. به‌علاوه چون $p(x)$ تحویل‌ناپذیر است، طبق قضیه ۹.۵ حلقه خارج قسمت $\mathbb{F}[x]/(p(x))$، و در نتیجه $\mathrm{Im}\varphi$، میدان می‌باشد. هر چندجمله‌ای ثابت تحت φ بخودش تصویر می‌شود و $\varphi(x) = u$. بنابراین $\mathrm{Im}\varphi$ زیرمیدانی از $\mathbb{F}(u)$ است که هر دو $\mathbb{F}$ و u را شامل است. چون $\mathbb{F}(u)$ کوچکترین زیرمیدانی است که $\mathbb{F}$ و u را شامل است، باید داشته باشیم $\mathbb{F}(u) = \mathrm{Im}\varphi \cong \mathbb{F}[x]/(p(x))$.

(۲) و (۳) چون $\mathbb{F}(u) = \mathrm{Im}\varphi$، هر عضو ناصفر $\mathbb{F}(u)$ به صورت $f(u)$ برای یک $f(x) \in \mathbb{F}[x]$ می‌باشد. اگر $\deg p(x) = n$، آنگاه طبق الگوریتم تقسیم $f(x) = p(x)q(x) + r(x)$ که در آن $r(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} \in \mathbb{F}[x]$. در نتیجه،

$$f(u) = p(u)q(u) + r(u) = 0_{\mathbb{F}}q(u) + r(u) = r(u) = b_0 1_{\mathbb{F}} + b_1u + \cdots + b_{n-1}u^{n-1}$$

بنابراین مجموعه $\{1_{\mathbb{F}}, u, u^2, \ldots, u^{n-1}\}$، $\mathbb{F}(u)$ را پدید می‌آورد. برای این که نشان دهیم این مجموعه مستقل خطی است فرض کنید $c_0 + c_1u + \cdots + c_{n-1}u^{n-1} = 0_{\mathbb{F}}$ که در آن $c_i \in \mathbb{F}$. آنگاه u یک ریشهٔ $c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ است، بنابراین این چندجمله‌ای (که دارای درجه کوچکتر یا مساوی $n-1$ است) باید بر $p(x)$ بخش‌پذیر باشد (که درجه n دارد). این تنها وقتی

می‌تواند پیش بیاید که $c_i = 0_{\mathbb{F}}$ برای $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ چندجمله‌ای صفر باشد، یعنی هر i. از اینرو $\{1_{\mathbb{F}}, u, \ldots, u^{n-1}\}$ روی $\mathbb{F}$ مستقل خطی است و بنابراین یک پایه $\mathbb{F}(u)$ است. بدین دلیل $[\mathbb{F}(u) : \mathbb{F}] = n$.

مثال ۱۲.۹. چندجمله‌ای کمین $\sqrt{3}$ روی $\mathbb{Q}$، $x^2 - 3$ است. با بکارگیری قضیه ۷.۹، برای $n = 2$، می‌بینیم که $\{1, \sqrt{3}\}$ یک پایه $\mathbb{Q}(\sqrt{3})$ روی $\mathbb{Q}$ است و به این دلیل $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. به طور مشابه $\sqrt{5} + \sqrt{3}$ دارای چندجمله‌ای کمین $x^4 - 16x^2 + 4$ روی $\mathbb{Q}$ می‌باشد، بنابراین $[\mathbb{Q}(\sqrt{3} + \sqrt{5}) : \mathbb{Q}] = 4$ و $\{1, \sqrt{3} + \sqrt{5}, (\sqrt{3} + \sqrt{5})^2, (\sqrt{3} + \sqrt{5})^3\}$ یک پایه است.

نتیجه‌ای فوری از قضیه ۷.۹ آن است که

اگر u و v دارای چندجمله‌ای کمین یکسان $p(x)$ در $\mathbb{F}[x]$ باشند، آنگاه $\mathbb{F}(u)$ یکریخت با $\mathbb{F}(v)$ است.

علت آن است که هر دوی $\mathbb{F}(u)$ و $\mathbb{F}(v)$ با $\mathbb{F}[x]/(p(x))$ یکریخت هستند و از اینرو با یکدیگر یکریختند. توجه کنید که این نتیجه حتی وقتی که u و v در یک توسیع میدان $\mathbb{F}$ نباشد برقرار است. در بقیه این بخش، که تا بخش ۴.۹ مورد نیاز نیست، به تعمیم این مفهوم می‌پردازیم. ما نه تنها توسیع‌های سادهٔ یک میدان را در نظر می‌گیریم بلکه توسیع‌های ساده دو میدان متفاوت، ولی یکریخت، را نیز در نظر می‌گیریم.

فرض کنید $\mathbb{F}$ و $\mathbb{E}$ میدان باشند و $\sigma : \mathbb{F} \to \mathbb{E}$ یک یکریختی باشد. تحقیق کنید که نگاشتی از $\mathbb{F}[x]$ به $\mathbb{E}[x]$ که $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ را به چندجمله‌ای $\sigma f(x) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$ می‌نگارد یک یکریختی حلقه‌ای است. (تمرین ۱۹ در بخش ۱.۴). توجه کنید که اگر $f(x) = c$ یک چندجمله‌ای ثابت در $\mathbb{F}[x]$ (یعنی، یک عضو $\mathbb{F}$) باشد، آنگاه این یکریختی c را به $\sigma(c) \in \mathbb{E}$ می‌نگارد. در نتیجه، می‌گوییم که **یکریختی $\sigma : \mathbb{F} \to \mathbb{E}$ را تعمیم می‌دهد**، یکریختی $\mathbb{F}[x] \to \mathbb{E}[x]$، و یکریختی تعمیم‌یافته را نیز با σ نشان می‌دهیم.

نتیجه ۸.۹. گیریم $\sigma : \mathbb{F} \to \mathbb{E}$ یک یکریختی میدان‌ها باشد، گیریم u یک عضو جبری در یک توسیع میدان $\mathbb{F}$ با چندجمله‌ای کمین $p(x) \in \mathbb{F}[x]$. فرض کنید v یک عنصر جبری در یک

توسیع میدان $\mathbb{E}$ با چندجمله‌ای کمین $\sigma p(x) \in \mathbb{E}[x]$ باشد. آنگاه σ به یک یکریختی میدان‌ها $\bar{\sigma} : \mathbb{F}(u) \to \mathbb{E}(v)$ تعمیم می‌یابد به طوری که $\bar{\sigma}(u) = v$ و برای هر $c \in \mathbb{F}$، $\bar{\sigma}(c) = \sigma(c)$.

در حالت خاصی که σ نگاشت همانی $\mathbb{F} \to \mathbb{F}$ باشد این نتیجه بیان می‌کند که وقتی u و v چندجمله‌ای کمین یکسان داشته باشند، آنگاه تحت تابعی که u را به v و هر عضو $\mathbb{F}$ را به خودش می‌نگارد، $\mathbb{F}(u) \cong \mathbb{F}(v)$.

برهان نتیجه ۸.۹. طبق تذکرات قبل از نتیجه، یکریختی σ به یک یکریختی $\mathbb{F}[x] \to \mathbb{E}[x]$ (که آن هم با σ نشان داده می‌شود) تعمیم می‌یابد. برهان قضیه ۷.۹ نشان می‌دهد که یک یکریختی $\bar{\tau} : \mathbb{E}[x]/(\sigma(p(x)) \to \mathbb{E}(v)$ که با $\bar{\tau}([g(x)]) = g(v)$ تعریف می‌شود وجود دارد. گیریم π همریختی پوشای

$$\mathbb{E}[x] \to \mathbb{E}[x]/(\sigma(p(x))$$

باشد که $g(x)$ را به $[g(x)]$ می‌نگارد و ترکیب

$$\mathbb{F}[x] \xrightarrow{\sigma} \mathbb{E}[x] \xrightarrow{\pi} \mathbb{E}[x]/(\sigma p(x)) \xrightarrow{\bar{\tau}} \mathbb{E}(v)$$
$$f(x) \mapsto \sigma f(x) \mapsto [\sigma f(x)] \mapsto \sigma f(v)$$

را در نظر بگیرید. چون هرسه نگاشت پوشا می‌باشد، ترکیب آنها نیز پوشا است، هسته تابع ترکیب شامل تمام $h(x) \in \mathbb{F}[x]$هایی است که $\sigma h(v) = 0_{\mathbb{E}}$. چون $\bar{\tau}$ یک یکریختی است، $\sigma h(v) = 0_{\mathbb{E}}$ اگر و تنها اگر $[\sigma h(x)]$ کلاس صفر در $\mathbb{E}[x]/(\sigma p(x))$ باشد، یعنی اگر و تنها اگر $\sigma h(x)$ مضربی از $\sigma p(x)$ باشد. ولی اگر $\sigma h(x) = k(x) \cdot \sigma p(x)$، آنگاه بکارگیری یکریختی وارون σ نشان می‌دهد که $h(x) = \sigma^{-1}k(x)p(x)$. بدین دلیل هسته تابع ترکیب، ایده‌ال اصلی $(p(x))$ در $\mathbb{F}[x]$ است. بنابراین طبق قضیه اول یکریختی ۱۱.۶، $\mathbb{F}[x]/(p(x)) \cong \mathbb{E}(v)$، برهان آن قضیه نشان می‌دهد که این یکریختی(آن را θ بنامید) با $\theta([f(x)]) = \sigma f(v)$ ارائه می‌شود. توجه کنید که $\theta([x]) = v$ و این که برای هر $c \in \mathbb{F}$، $\theta([c]) = \sigma(c)$. بنابراین وضعیت زیر را داریم، که در آن $\bar{\varphi}$ یکریختی قضیه ۷.۹ می‌باشد و $c \in \mathbb{F}$:

$$\mathbb{F}(u) \xleftarrow{\bar{\varphi}} \mathbb{F}[x]/(p(x)) \xrightarrow{\theta} \mathbb{E}(v)$$
$$f(u) \longleftarrow [f(x)] \longmapsto \sigma f(v)$$
$$c \longleftarrow [c] \longmapsto \sigma(c).$$

تابع ترکیب $\theta \circ \bar{\varphi}^{-1} : \mathbb{F}(u) \to \mathbb{E}(v)$ یک یکریختی است که σ را تعمیم می‌دهد و u را به v می‌نگارد. ■

مثال ۱۳.۹. چندجمله‌ای $x^3 - 2$ طبق محک ایزنشتاین تحویل‌ناپذیر است. این چندجمله‌ای دارای ریشه $\sqrt[3]{2}$ در $\mathbb{R}$ است. تحقیق کنید که $\sqrt[3]{2}w$ نیز یک ریشه $x^3 - 2$ در $\mathbb{C}$ است، که در آن $w = (-1 + \sqrt{3}i)/2$ یک ریشه مختلط ۱ است. با بکارگرفتن نتیجه ۸.۹ برای نگاشت همانی $\mathbb{Q} \to \mathbb{Q}$ می‌بینیم که زیرمیدان حقیقی $\mathbb{Q}(\sqrt[3]{2})$ با زیرمیدان مختلط $\mathbb{Q}(\sqrt[3]{2}w)$ تحت نگاشتی که $\sqrt[3]{2}$ را به $\sqrt[3]{2}w$ و هر عضو $\mathbb{Q}$ را به خودش می‌فرستد، یکریخت است.

تمرینها

توجه: $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ است، مگر خلاف آن ذکر شود.

A.۱. گیریم $\{\mathbb{E}_i \mid i \in I\}$ خانواده‌ای از زیرمیدان‌های $\mathbb{K}$ باشد. ثابت کنید که $\bigcap_{i \in I} \mathbb{E}_i$ زیرمیدانی از $\mathbb{K}$ است.

۲. اگر $u \in \mathbb{K}$، ثابت کنید $\mathbb{F}(u^2) \subseteq \mathbb{F}(u)$.

۳. اگر $u \in \mathbb{K}$ و $0 \neq c \in \mathbb{F}$، ثابت کنید که $\mathbb{F}(u + c) = \mathbb{F}(u) = \mathbb{F}(cu)$.

۴. ثابت کنید که $\mathbb{Q}(3 + i) = \mathbb{Q}(1 - i)$.

۵. ثابت کنید که هرکدام از عناصر زیر یک عضو جبری روی $\mathbb{Q}$ است.

(الف) $3 + 5i$ (ب) $\sqrt{i - \sqrt{2}}$ (پ) $1 + \sqrt[3]{2}$.

۶. اگر $u \in \mathbb{K}$ و u^2 روی $\mathbb{F}$ جبری باشد، ثابت کنید که u روی $\mathbb{F}$ جبری است.

۷. اگر $\mathbb{L}$ میدانی باشد که $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ و $u \in \mathbb{L}$ روی $\mathbb{F}$ جبری باشد، نشان دهید که u روی $\mathbb{K}$ جبری است.

۸. اگر $u, v \in K$ و $u + v$ روی $\mathbb{F}$ جبری باشد، ثابت کنید که u روی $\mathbb{F}(v)$ جبری است.

۹. ثابت کنید که $\sqrt{\pi}$ روی $\mathbb{Q}(\pi)$ جبری است.

۱۰. اگر $u \in \mathbb{K}$ روی $\mathbb{F}$ متعالی باشد و $0_{\mathbb{F}} \neq c \in \mathbb{F}$، ثابت کنید که هرکدام از $u + 1_{\mathbb{F}}$، cu و u^2 روی $\mathbb{F}$ متعالی است.

۱۱. $[\mathbb{Q}(\sqrt[۳]{۲}) : \mathbb{Q}]$ را پیدا کنید.

۱۲. اگر $a + bi \in \mathbb{C}$ و $b \neq ۰$، ثابت کنید که $\mathbb{C} = \mathbb{R}(a + bi)$.

۱۳. اگر $[\mathbb{K} : \mathbb{F}]$ اول باشد و $u \in \mathbb{K}$ روی $\mathbb{F}$ جبری باشد، نشان دهید که یا $\mathbb{F}(u) = \mathbb{K}$ یا $\mathbb{F}(u) = \mathbb{F}$.

۱۴. ثابت کنید که $x^۴ - ۱۶x^۲ + ۴$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

۱۵.B. نشان دهید که هر عضو $\mathbb{C}$ روی $\mathbb{R}$ جبری است [لم ۲۴.۴ را ملاحظه بفرمایید.]

۱۶. اگر $u \in \mathbb{K}$ روی $\mathbb{F}$ جبری باشد و $c \in \mathbb{F}$، ثابت کنید که $۱_{\mathbb{F}} + u$ و cu روی $\mathbb{F}$ جبری هستند.

۱۷. چندجمله‌ای کمین عضو داده شده را روی $\mathbb{Q}$ پیدا کنید:

(الف) $\sqrt{۱ + \sqrt{۵}}$ (ب) $\sqrt{۳}i + \sqrt{۲}$

۱۸. چندجمله‌ای کمین $\sqrt{۲} + i$ را روی $\mathbb{Q}$ و روی $\mathbb{R}$ پیدا کنید.

۱۹. گیریم u عضوی جبری از $\mathbb{K}$ باشد که چندجمله‌ای کمین آن در $\mathbb{F}[x]$ دارای درجه اول باشد. اگر $\mathbb{E}$ میدانی باشد که $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{F}(u)$، نشان دهید که $\mathbb{E} = \mathbb{F}$ یا $\mathbb{E} = \mathbb{F}(u)$.

۲۰. گیریم u یک عضو جبری از $\mathbb{K}$ باشد که چندجمله‌ای کمین آن در $\mathbb{F}[x]$ دارای درجه فرد است. ثابت کنید که $\mathbb{F}(u) = \mathbb{F}(u^۲)$.

۲۱. گیریم $\mathbb{F} = \mathbb{Q}(\pi^۴)$ و $\mathbb{K} = \mathbb{Q}(\pi)$. نشان دهید که π روی $\mathbb{F}$ جبری است و یک پایه $\mathbb{K}$ روی $\mathbb{F}$ را پیدا کنید.

۲۲. اگر r و s ناصفر باشند، ثابت کنید که $\mathbb{Q}(\sqrt{s}) = \mathbb{Q}(\sqrt{r})$ اگر وتنها اگر برای یک $t \in \mathbb{Q}$، $r = t^۲s$.

۲۳. اگر $\mathbb{K}$ توسیعی از میدان $\mathbb{Q}$ باشد که $[\mathbb{K} : \mathbb{Q}] = ۲$، ثابت کنید که برای یک عدد صحیح مربع ـ آزاد d، $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. [مربع ـ آزاد یعنی برای هر عدد اول p، d بخش‌پذیر بر $p^۲$ نیست.]

۲۴. اگر $u \in \mathbb{K}$ روی $\mathbb{F}$ متعالی باشد، ثابت کنید که $\mathbb{F}(x) \cong \mathbb{F}(u)$، که در آن $\mathbb{F}(x)$ میدان خارج قسمت‌های $\mathbb{F}[x]$ است، که در بخش ۴.۸ ساخته شد. [راهنمایی: نگاشتی از $\mathbb{F}[x]$ به $\mathbb{F}(u)$ را در نظر بگیرید که $f(x)/g(x)$ را به $f(u)g(u)^{-۱}$ می‌فرستد.]

۲۵. اگر $u \in \mathbb{K}$ عضو متعالی روی $\mathbb{F}$ باشد، ثابت کنید که همه عضوهای $\mathbb{F}(u)$، به جز آن‌هایی که در $\mathbb{F}$ اند، روی $\mathbb{F}$ متعالی هستند.

۲۶. گیریم $\mathbb{F}(x)$ همان باشد که در تمرین ۲۴ آمده است. نشان دهید که $\frac{x^۳}{x+۱} \in \mathbb{F}(x)$ روی $\mathbb{F}$ متعالی است.

۹-۳ توسیع‌های جبـــری

در بخش قبل تاکید روی یک تک عنصر جبری بود. اکنون توسیع‌هایی را در نظر می‌گیریم که تمام عضوهای آن جبری هستند.

یک توسیع میدان $\mathbb{K}$ از میدان $\mathbb{F}$ را یک **توسیع جبری** $\mathbb{F}$ گوییم اگر هر عضو $\mathbb{K}$ روی $\mathbb{F}$ جبری باشد.

مثال ۱۴.۹. اگر $a+bi \in \mathbb{C}$، آنگاه $a+bi$ یک ریشه

$$(x-(a+bi))(x-(a-bi)) = x^۲ - ۲ax + (a^۲+b^۲) \in \mathbb{R}[x]$$

می‌باشد. بنابراین $a+bi$ روی $\mathbb{R}$ جبری است و از اینرو $\mathbb{C}$ یک توسیع جبری $\mathbb{R}$ است. از جهت دیگر، نه $\mathbb{C}$ ونه $\mathbb{R}$ توسیعی جبری از $\mathbb{Q}$ می‌باشد زیرا اعداد حقیقی (مثل π و e) وجود دارند که روی $\mathbb{Q}$ جبری نیستند.

طبق قضیه ۷.۹ هر عضو جبری u روی $\mathbb{F}$ در یک توسیع میدان با بعدمتناهی $\mathbb{F}(u)$، قرار دارد. از جهت دیگر، اگر با یک توسیع با بعدمتناهی $\mathbb{F}$ شروع کنیم خواهیم داشت:

قضیه ۹.۹. اگر $\mathbb{K}$ یک توسیع میدان با بعدمتناهی $\mathbb{F}$ باشد، در این صورت $\mathbb{K}$ یک توسیع جبری $\mathbb{F}$ است.

برهان. طبق فرض $\mathbb{K}$ دارای یک پایه متناهی روی $\mathbb{F}$، مثل $\{v_۱, v_۲, \ldots, v_n\}$ است. چون این n عضو $\mathbb{K}$ را پدید می‌آورد، لم ۲.۹ ایجاب می‌کند که هر مجموعه مستقل خطی در $\mathbb{K}$ باید n یا کمتر از n عضو داشته باشد. اگر $u \in \mathbb{K}$ و $u^i = u^j$، با شرط $۰ \le i \le j$، آنگاه u ریشه‌ای از $x^i - x^j \in \mathbb{F}[x]$ است. برای هر u دیگر در $\mathbb{K}$، $\{۱_{\mathbb{F}}, u, u^۲, \ldots, u^n\}$ مجموعه‌ای از $n+۱$

عضو $\mathbb{K}$ است و بنابراین باید روی $\mathbb{F}$ وابسته خطی باشد. در نتیجه، عضوهای $c_i \in \mathbb{F}$ وجود دارند، که همگی صفر نیستند، به طوری که $c_0 1_{\mathbb{F}} + c_1 u + c_2 u^2 + \cdots + c_n u^n = 0_{\mathbb{F}}$. بنابراین u ریشه چندجمله‌ای ناصفر $c_0 + c_1 x + \cdots + c_n x^n$ در $\mathbb{F}[x]$ است و بدین دلیل روی $\mathbb{F}$ جبری است. ■

اگر یک توسیع میدان $\mathbb{K}$ از $\mathbb{F}$ یک عضو متعالی u را شامل باشد، آنگاه $\mathbb{K}$ باید از بعد نامتناهی روی $\mathbb{F}$ باشد (در غیر این‌صورت طبق قضیه ۹.۹، u یک عضو جبری خواهد بود). با این وجود، عکس قضیه ۹.۹ غلط است زیرا توسیع‌های جبری با بعد بینهایت وجود دارد (تمرین ۱۹).

توسیع‌های ساده دارای این خاصیت خوب هستند که لازم است فقط بررسی کنید که تک عضو u روی $\mathbb{F}$ جبری است تا نتیجه بگیرید که تمام میدان $\mathbb{F}(u)$ یک توسیع جبری است (زیرا طبق قضیه ۷.۹، $\mathbb{F}(u)$ با بعدمتناهی است و بدین دلیل طبق ۹.۹ جبری است). این موضوع پیشنهاد می‌کند که تعمیم مفهوم توسیع ساده می‌تواند منجر به میدان‌هایی شود که جبری بودن آن را می‌توان با بررسی تنها تعداد متناهی عضو تعیین کرد.

اگر u_1، u_2، ...، u_n عضوهایی از توسیع‌میدان $\mathbb{K}$ از $\mathbb{F}$ باشند، گیریم $\mathbb{F}(u_1, u_2, \ldots, u_n)$ نمایش اشتراک تمام زیر میدان‌هایی از $\mathbb{K}$ باشد که $\mathbb{F}$ و هر u_i را شامل است. مانند حالت توسیع‌های ساده، $\mathbb{F}(u_1, u_2, \ldots, u_n)$ کوچکترین زیرمیدانی از $\mathbb{K}$ است که $\mathbb{F}$ و تمام u_iها را شامل است. $\mathbb{F}(u_1, \ldots, u_n)$ را **یک توسیع با مولد متناهی از $\mathbb{F}$** گویند که توسط u_1، ...، u_n تولید شده است.

مثال ۱۵.۹. میدان $\mathbb{Q}(\sqrt{3}, i)$ کوچکترین زیرمیدان $\mathbb{C}$ است که میدان $\mathbb{Q}$ و عناصر $\sqrt{3}$ و i را شامل است.

مثال ۱۶.۹. یک توسیع با مولد متناهی می‌تواند به واقع یک توسیع ساده باشد. برای مثال، میدان $\mathbb{Q}(i)$ تواماً i و $-i$ را شامل است، بنابراین $\mathbb{Q}(i, -i) = \mathbb{Q}(i)$.

مثال ۱۷.۹. هر توسیع با بعدمتناهی یک توسیع با مولد متناهی نیز هست. اگر $\{u_1, \ldots, u_n\}$ یک پایه $\mathbb{K}$ روی $\mathbb{F}$ باشد آنگاه تمام ترکیبات خطی u_iها (با ضرایب در $\mathbb{F}$) در $\mathbb{F}(u_1, \ldots, u_n)$ است. بنابراین $\mathbb{K} = \mathbb{F}(u_1, \ldots, u_n)$.

کلید کار در مواجهه با توسیع‌های با مولدمتناهی آن است که متوجه باشید که آنها را می‌توان با محاسبه متوالی توسیع‌های ساده بدست آورد. برای مثال اگر $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد و $u, v \in \mathbb{K}$، آنگاه $\mathbb{F}(u, v)$ زیرمیدانی از $\mathbb{K}$ است که هر دو $\mathbb{F}$ و u را شامل است و از اینرو باید $\mathbb{F}(u)$ را شامل‌باشد. چون v در $\mathbb{F}(u, v)$ است لذا $\mathbb{F}(u, v)$ باید $\mathbb{F}(u)(v)$، کوچکترین میدانی که هر دو $\mathbb{F}(u)$ و v را مشتمل است، شامل باشد ولی $\mathbb{F}(u)(v)$ میدانی است که شامل $\mathbb{F}$، u و v است و از اینرو باید $\mathbb{F}(u, v)$ را شامل باشد. از اینرو $\mathbb{F}(u, v) = \mathbb{F}(u)(v)$. بنابراین توسیع با مولدمتناهی $\mathbb{F}(u; v)$ را می‌توان از یک زنجیر توسیع‌های ساده بدست آورد:

$$\mathbb{F} \subseteq \mathbb{F}(u) \subseteq \mathbb{F}(u)(v) = \mathbb{F}(u, v).$$

مثال ۱۸.۹. توسیع میدان $\mathbb{Q}(\sqrt{۳}, i)$ را می‌توان توسط این دنباله از توسیع‌های ساده بدست آورد:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{۳}) \subseteq \mathbb{Q}(\sqrt{۳})(i) = \mathbb{Q}(\sqrt{۳}, i).$$

در مثال ۱۲.۹ دیدیم که $[\mathbb{Q}(\sqrt{۳}) : \mathbb{Q}] = ۲$. به‌علاوه i ریشه‌ای از $x^۲ + ۱$ است که ضرایبش در $\mathbb{Q}(\sqrt{۳})$ است. بنابراین i روی $\mathbb{Q}(\sqrt{۳})$ جبری است، و از اینرو طبق قضیه ۹.۷، $[\mathbb{Q}(\sqrt{۳})(i) : \mathbb{Q}(\sqrt{۳})]$ متناهی است. در نتیجه، طبق قضیه ۴.۹،

$$[\mathbb{Q}(\sqrt{۳}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{۳})(i) : \mathbb{Q}(\sqrt{۳})][\mathbb{Q}(\sqrt{۳}) : \mathbb{Q}]$$

متناهی است. بدین دلیل توسیع با مولدمتناهی $\mathbb{Q}(\sqrt{۳}, i)$ با بعدمتناهی است و از اینرو طبق قضیه ۹.۹ روی $\mathbb{Q}$ جبری است.

اساساً همین استدلال در حالت کلی کار می‌کند و راهی کارآمد برای تعیین این که یک توسیع جبری است ارائه می‌کند:

قضیه ۱۰.۹. اگر $\mathbb{K} = \mathbb{F}(u_۱, \ldots, u_n)$ یک توسیع با مولدمتناهی میدان $\mathbb{F}$ باشد و هر u_i روی $\mathbb{F}$ جبری باشد، آنگاه $\mathbb{K}$ یک توسیع جبری با بعدمتناهی $\mathbb{F}$ است.

برهان. میدان $\mathbb{K}$ را می‌توان از این زنجیر از توسیع‌ها بدست آورد.

$$\mathbb{F} \subseteq \mathbb{F}(u_۱) \subseteq \mathbb{F}(u_۱, u_۲) \subseteq \mathbb{F}(u_۱, u_۲, u_۳) \subseteq \cdots$$
$$\subseteq \mathbb{F}(u_۱, \ldots, u_{n-۱}) \subseteq \mathbb{F}(u_۱, \ldots, u_n) = \mathbb{K}.$$

به‌علاوه $\mathbb{F}(u_1, u_2, u_3) = \mathbb{F}(u_1, u_2)(u_3)$ ،$\mathbb{F}(u_1, u_2) = \mathbb{F}(u_1)(u_2)$ و در حالت کلی $\mathbb{F}(u_1, \ldots, u_i)$ توسیع ساده $\mathbb{F}(u_1, \ldots, u_{i-1})(u_i)$ است. هر u_i روی $\mathbb{F}$ جبری است و از اینرو طبق تمرین ۷ بخش ۲.۹، روی $F(u_1, \ldots, u_{i-1})$ جبری است. ولی طبق قضیه ۷.۹ هر توسیع ساده یک عضو جبری، با بعدمتناهی است. بنابراین برای هر $i = 2, \ldots, n$

$$[\mathbb{F}(u_1, \ldots, u_i) : \mathbb{F}(u_1, \ldots, u_{i-1})]$$

متناهی است. در نتیجه، با بکارگرفتن مکرر قضیه ۴.۹، می‌بینیم که $[\mathbb{K} : \mathbb{F}]$ حاصل‌ضرب زیر است:

$$[\mathbb{K} : \mathbb{F}(u_1, \ldots, u_{n-1})] \cdots [\mathbb{F}(u_1, u_2, u_3) : \mathbb{F}(u_1, u_2)][\mathbb{F}(u_1, u_2) : \mathbb{F}(u_1)][\mathbb{F}(u_1) : \mathbb{F}]$$

بدین دلیل $[\mathbb{K} : \mathbb{F}]$ متناهی است، و از اینرو طبق قضیه ۹.۹، $\mathbb{K}$ روی $\mathbb{F}$ جبری است. ■

مثال ۱۹.۹. هر دو عدد $\sqrt{3}$ و $\sqrt{5}$ روی $\mathbb{Q}$ جبری هستند. پس طبق قضیه ۱۰.۹، $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ یک توسیع جبری با بعدمتناهی میدان $\mathbb{Q}$ است. می‌توانیم بعد $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ را روی $\mathbb{Q}$ با در نظر گرفتن زنجیر توسیع‌های ساده:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3})(\sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$$

محاسبه کنیم. می‌دانیم که $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. برای تعیین $[\mathbb{Q}(\sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{3})]$ چندجمله‌ای کمین $\sqrt{5}$ را روی $\mathbb{Q}(\sqrt{3})$ پیدا می‌کنیم. نامزد واضح این امر $x^2 - 5$ می‌باشد؛ این چندجمله‌ای در $\mathbb{Q}[x]$ تحویل‌ناپذیر می‌باشد، ولی برای این که نتیجه بگیریم که چندجمله‌ای کمین است، باید ثابت کنیم روی $\mathbb{Q}(\sqrt{3})$ تحویل‌ناپذیر است. اگر $\sqrt{5}$ یا $-\sqrt{5}$ در $\mathbb{Q}(\sqrt{3})$ باشد، آنگاه $\pm\sqrt{5} = a + b\sqrt{3}$ که در آن $a, b \in \mathbb{Q}$. مربع‌گیری از دو طرف نشان می‌دهد که $5 = a^2 + 2ab\sqrt{3} + 3b^2$. پس اگر $a \neq 0$ و $b \neq 0$ داریم $\sqrt{3} = \frac{5 - a^2 - 3b^2}{2ab}$، که متناقض با اصم‌بودن $\sqrt{3}$ است. اگر $a = 0$ یا $b = 0$ تناقضی مشابه بدست می‌آید، بنابراین $\pm\sqrt{5}$ در $\mathbb{Q}(\sqrt{3})$ نیست و از اینرو طبق نتیجه ۱۴.۴، $x^2 - 5$ روی $\mathbb{Q}(\sqrt{3})$ تحویل‌ناپذیر است. بنابراین طبق قضیه ۷.۹، $[\mathbb{Q}(\sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 2$. در نتیجه، طبق قضیه ۴.۹،

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \times 2 = 4.$$

از مطالب باقیمانده این بخش در آینده استفاده نمی‌شود. قضیه ۴.۹ به ما می‌گوید که میدان بالایی یک زنجیر از توسیع‌های با بعد متناهی روی میدان زمینه، با بعدمتناهی است. در اینجا نتیجه‌ای مشابه برای توسیع‌هایی جبری که ممکن است با بعدمتناهی نباشد آمده است.

نتیجه ۱۱.۹. اگر $\mathbb{L}$ یک توسیع جبری میدان $\mathbb{K}$ و $\mathbb{K}$ یک توسیع جبری میدان $\mathbb{F}$ باشد، آنگاه $\mathbb{L}$ یک توسیع جبری میدان $\mathbb{F}$ است.

برهان. گیریم $u \in \mathbb{L}$، چون u روی $\mathbb{K}$ جبری است $a_i \in \mathbb{K}$ وجود دارد به طوری که $a_. + a_. u + a_۲ u^۲ + \cdots + a_m u^m = ۰_{\mathbb{K}}$. چون هر a_i در میدان $\mathbb{F}(a_., \ldots, a_m)$ است، در واقع u روی $\mathbb{F}(a_., \ldots, a_m)$ جبری است. در نتیجه طبق قضیه ۱۰.۹ (با شرط $\mathbb{F}(a_., \ldots, a_m)$ به جای $\mathbb{F}$، $n = ۱$، $u = u_۱$)، در زنجیر توسیع

$$\mathbb{F} \subseteq \mathbb{F}(a_., \ldots, a_m) \subseteq \mathbb{F}(a_., \ldots, a_m)(u) = \mathbb{F}(a_., \ldots, a_m, u)$$

توسیع $\mathbb{F}(a_., \ldots, a_m)(u)$ روی $\mathbb{F}(a_., \ldots, a_m)$ با بعدمتناهی است. به‌علاوه چون هر a_i روی $\mathbb{F}$ جبری است، طبق قضیه ۱۰.۹، $[\mathbb{F}(a_., \ldots, a_m) : \mathbb{F}]$ متناهی است. بنابراین طبق قضیه ۴.۹، $\mathbb{F}(a_۱, \ldots, a_m, u)$ روی $\mathbb{F}$ با بعدمتناهی است و از اینرو بنابر قضیه ۹.۹ روی $\mathbb{F}$ جبری است. بدین دلیل u روی $\mathbb{F}$ جبری است. چون u عضو دلخواهی از $\mathbb{L}$ بود، $\mathbb{L}$ یک توسیع جبری $\mathbb{F}$ است. ■

نتیجه ۱۲.۹. گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ و $\mathbb{E}$ مجموعه تمام عضوهایی از $\mathbb{K}$ باشد که روی $\mathbb{F}$ جبری هستند. آنگاه $\mathbb{E}$ زیرمیدانی از $\mathbb{K}$ است و یک توسیع جبری میدان $\mathbb{F}$ است.

برهان. هر عضو $\mathbb{F}$ روی $\mathbb{F}$ جبری است، بنابراین $\mathbb{F} \subseteq \mathbb{E}$. اگر $u, v \in \mathbb{E}$، آنگاه u و v طبق تعریف روی $\mathbb{F}$ جبری هستند. زیرمیدان $\mathbb{F}(u, v)$ طبق قضیه ۱۰.۹ یک توسیع جبری $\mathbb{F}$ است، و از اینرو $\mathbb{F}(u, v) \subseteq \mathbb{E}$. چون $\mathbb{F}(u, v)$ یک میدان است، $u + v, uv, -u, -v \in \mathbb{F}(u, v) \subseteq \mathbb{E}$. به طور مشابه، اگر u ناصفر باشد آنگاه $u^{-۱} \in \mathbb{F}(u, v) \subseteq \mathbb{E}$. بنابراین $\mathbb{E}$ تحت جمع و ضرب بسته است. قرینه و وارون عضوهای $\mathbb{E}$ نیز در $\mathbb{E}$ هستند. بدین دلیل $\mathbb{E}$ یک میدان است.

مثال ۲۰.۹. اگر در نتیجه ۱۲.۹، $\mathbb{K} = \mathbb{C}$ و $\mathbb{F} = \mathbb{Q}$، آنگاه میدان $\mathbb{E}$، میدان **اعداد جبری** نامیده می‌شود. این میدان $\mathbb{E}$ یک توسیع جبری با بعد نامتناهی $\mathbb{Q}$ است (تمرین ۱۹). اعداد جبری

در زمینه‌ای نسبتاً متفاوت در بند قبل از قضیه ۱۸.۸ مورد بحث واقع گردید.

تمرینها

توجه: $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ است، مگر خلاف آن بیان شود.

A.۱. اگر $u, v \in \mathbb{K}$، تحقیق کنید که $\mathbb{F}(u)(v) = \mathbb{F}(v)(u)$.

۲. اگر $\mathbb{K}$ میدان متناهی باشد نشان دهید که $\mathbb{K}$ یک توسیع جبری روی $\mathbb{F}$ است.

۳. پایه‌ای برای توسیع میدان ارائه شده روی $\mathbb{Q}$ پیدا کنید.

(الف) $\mathbb{Q}(\sqrt{5}, i)$ (ب) $\mathbb{Q}(\sqrt{5}, \sqrt{7})$

(پ) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ (ت) $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$

۴. یک پایه $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ روی $\mathbb{Q}(\sqrt{3})$ را پیدا کنید.

۵. نشان دهید که $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$.

۶. تحقیق کنید که $[\mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{10}) : \mathbb{Q}] = 4$.

۷. اگر $[\mathbb{K} : \mathbb{F}]$ متناهی باشد و u روی $\mathbb{K}$ جبری باشد، ثابت کنید که $[\mathbb{K}(u) : \mathbb{K}] \leq [\mathbb{F}(u) : \mathbb{F}]$.

۸. اگر $[\mathbb{K} : \mathbb{F}]$ متناهی باشد و u روی $\mathbb{K}$ جبری باشد، ثابت کنید که $[\mathbb{K}(u) : \mathbb{F}(u)] \leq [\mathbb{K} : \mathbb{F}]$.
[راهنمایی: نشان دهید که هر پایه $\mathbb{K}$ روی $\mathbb{F}$، $\mathbb{K}(u)$ روی $\mathbb{F}(u)$ را پدید می‌آورد.]

۹. اگر $[\mathbb{K} : \mathbb{F}]$ متناهی باشد و u روی $\mathbb{K}$ جبری باشد، ثابت کنید که $[\mathbb{F}(u) : \mathbb{F}]$، $[\mathbb{K}(u) : \mathbb{F}]$ را می‌شمارد.

B.۱۰. ثابت کنید که $[\mathbb{K} : \mathbb{F}]$ متناهی است اگر و تنها اگر $\mathbb{K} = \mathbb{F}(u_1, \ldots, u_n)$ که در آن هر u_i روی $\mathbb{F}$ جبری باشد. [این بیان قویتر قضیه ۱۰.۹ می‌باشد.]

۱۱. فرض کنید $u, v \in \mathbb{K}$ روی $\mathbb{F}$ جبری باشند و $p(x)$ و $q(x)$ بترتیب چندجمله‌ای‌های کمین آن‌ها باشد.

(الف) اگـــر $\deg p(x) = m$، $\deg q(x) = n$ و $(m, n) = 1$، ثابـــت کنیـــد کـــه $[\mathbb{F}(u, v) : \mathbb{F}] = mn$.

(ب) با مثال نشان دهید که اگر m و n نسبت به هم اول نباشند حکم قسمت (الف) ممکن است غلط باشد.

(پ) $[\mathbb{Q}(\sqrt{۲}, \sqrt[۳]{۲}) : \mathbb{Q})]$ برابر چیست؟

۱۲. گیریم D حلقه‌ای باشد که $\mathbb{F} \subseteq D \subseteq \mathbb{K}$. اگر $[\mathbb{K} : \mathbb{F}]$ متناهی باشد، ثابت کنید که D یک میدان است. [راهنمایی: برای این که وارون یک عضو ناصفر $u \in D$ را پیدا کنید، از قضایای ۹.۹ و ۷.۹ استفاده کنید تا نشان دهید که $\mathbb{F}(u) \subseteq D$.]

۱۳. گیریم $p(x)$ و $q(x)$ در $\mathbb{F}[x]$ تحویل‌ناپذیر باشند، و $\deg p(x)$ نسبت به $\deg q(x)$ اول باشد. گیریم u ریشه‌ای از $p(x)$ و v ریشه‌ای از $q(x)$ در یک توسیع میدان $\mathbb{F}$ باشد. ثابت کنید که $q(x)$ روی $\mathbb{F}(u)$ تحویل‌ناپذیر است.

۱۴. (الف) گیریم $\mathbb{F}_۱ \subseteq \mathbb{F}_۲ \subseteq \mathbb{F}_۳ \subseteq \cdots$ زنجیری از میدان‌ها باشد. ثابت کنید که اجتماع تمام $\mathbb{F}_i$ها نیز یک میدان است.

(ب) اگر هر $\mathbb{F}_i$ روی $\mathbb{F}_۱$ جبری باشد، نشان دهید که اجتماع $\mathbb{F}_i$ها توسیعی جبری از $\mathbb{F}_۱$ است.

۱۵. همان‌طور که در نتیجه ۱۲.۹ آمده است، گیریم $\mathbb{E}$ میدان تمام عضوهایی از $\mathbb{K}$ باشد که روی $\mathbb{F}$ جبری است. ثابت کنید که هر عضو مجموعه $\mathbb{K} - \mathbb{E}$ روی $\mathbb{E}$ متعالی است.

۱۶. فرض کنید $۱_{\mathbb{F}} + ۱_{\mathbb{F}} \neq ۰_{\mathbb{F}}$. اگر $u \in \mathbb{F}$، گیریم $\sqrt{u}$ ریشه $x^۲ - u$ در $\mathbb{K}$ باشد. ثابت کنید که $\mathbb{F}(\sqrt{u} + \sqrt{v}) = \mathbb{F}(\sqrt{u}, \sqrt{v})$. [راهنمایی: به موجب قضیه ۷.۹، $۱_{\mathbb{F}}$، $(\sqrt{u} + \sqrt{v})$، $(\sqrt{u} + \sqrt{v})^۲$، $(\sqrt{u} + \sqrt{v})^۳$، ...، باید $\mathbb{F}(\sqrt{u} + \sqrt{v})$ را پدید آورد. از این مطلب استفاده کنید تا نشان دهید $\sqrt{u}$ و $\sqrt{v}$ در $\mathbb{F}(\sqrt{u} + \sqrt{v})$ می‌باشد.

۱۷. اگر $n_۱$، ...، n_t اعداد صحیح مثبت متمایز باشند، نشان دهید که $[\mathbb{Q}(\sqrt{n_۱}, \ldots, \sqrt{n_t}) : \mathbb{Q}] \leq ۲^t$.

۱۸.C اگر هر n_i در تمرین ۱۷ اول باشد، نشان دهید که " $\leq$ " را می‌توان با " $=$ " جایگزین کرد.

۱۹. گیریم $\mathbb{E}$ میدان اعداد جبری باشد (مثال ۲۰.۹ را ملاحظه کنید). ثابت کنید که $\mathbb{E}$ یک توسیع جبری با بعد نامتناهی روی $\mathbb{Q}$ است [راهنمایی: کافی است نشان دهیم که برای هر عدد صحیح مثبت n، $[\mathbb{E} : \mathbb{Q}] \geq ۲^n$. گیریم $p_۱$، ...، p_n اولین n عدد اول مثبت باشند. نشان دهید که $\mathbb{E}$ شامل $\mathbb{Q}(\sqrt{p_۱}, \ldots, \sqrt{p_n})$ است و از تمرین ۱۸ استفاده کنید.]

۹-۴ میدان‌های شکافنده

گیریم $\mathbb{F}$ یک میدان و $f(x)$ یک چندجمله‌ای در $\mathbb{F}[x]$ باشد. قبلاً توسیع‌هایی از $\mathbb{F}$ را در نظر گرفتیم که ریشه‌ای از $f(x)$ را شامل بودند. اکنون توسیع میدان‌هایی را بررسی می‌کنیم که *تمام* ریشه‌های $f(x)$ را شامل باشد.

کلمه "تمام" در این متن نیاز به یک توضیح دارد. فرض کنید $f(x)$ درجه n داشته باشد، آنگاه طبق نتیجه ۱۳.۴، $f(x)$ دارای حداکثر n ریشه در هر میدان می‌باشد. بنابراین اگر یک توسیع میدان $\mathbb{K}$ از $\mathbb{F}$، n ریشه متمایز از $f(x)$ را داشته باشد، می‌توان به طور منطقی گفت که $\mathbb{K}$ "تمام" ریشه‌های $f(x)$ را دارد، گرچه ممکن است توسیع دیگری هم از $\mathbb{F}$ موجود باشد که n ریشه $f(x)$ را شامل باشد. از جهت دیگر، فرض کنید که $\mathbb{K}$ کمتر از n ریشه $f(x)$ را داشته باشد. این امر که بتوان یک توسیع میدان از $\mathbb{K}$ یافت که ریشه‌های اضافی $f(x)$ را شامل باشد مقدور است. ولی اگر هیچ توسیعی این چنین از $\mathbb{K}$ موجود نباشد، منطقی به نظر می‌رسد که بگوییم $\mathbb{K}$ تمام ریشه‌ها را شامل است. می‌توانیم این شرط را به صورت قابل استفاده زیر بیان کنیم.

گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ و $f(x)$ یک چندجمله‌ای غیرثابت از درجه n در $\mathbb{F}[x]$ باشد. اگر $f(x)$ در $\mathbb{K}[x]$ به صورت

$$f(x) = c(x-u_1)(x-u_2)\cdots(x-u_n)$$

تجزیه شود آنگاه می‌گوییم که $f(x)$ **روی میدان $\mathbb{K}$ شکافته می‌شود.** در این حالت عناصر (نه لزوماً مجزای) $u_1, \ldots, u_n$ تنها ریشه‌های $f(x)$ در $\mathbb{K}$ یا در هر توسیع میدان $\mathbb{K}$ هستند. زیرا اگر v در یک توسیع $\mathbb{K}$ باشد و $f(v) = 0_{\mathbb{F}}$، آنگاه $c(v-u_1)(v-u_2)\cdots(v-u_n) = 0_{\mathbb{F}}$. حال c ناصفر است زیرا $f(x)$ چندجمله‌ای غیرثابت است. بنابراین یکی از $v-u_i$ها باید صفر باشد. یعنی $v = u_i$. بنابراین اگر $f(x)$ روی $\mathbb{K}$ شکافته شود می‌توانیم منطقاً بگوییم که $\mathbb{K}$ تمام ریشه‌های $f(x)$ را شامل است.

قدم بعدی آن است که کوچکترین توسیع میدانی که تمام ریشه‌های $f(x)$ را شامل است در نظر بگیریم. اگر $\mathbb{F}$ یک میدان باشد و $f(x) \in \mathbb{F}[x]$، آنگاه یک توسیع میدان $\mathbb{K}$ از $\mathbb{F}$ **یک میدان شکافندهٔ** (میدان ریشه) $f(x)$ روی $\mathbb{F}$ نامیده می‌شود مشروط به آن که

(i) $f(x)$ روی $\mathbb{K}$ شکافته شود، مثلاً $f(x) = c(x-u_1)(x-u_2)\cdots(x-u_n)$ و

(ii) $\mathbb{K} = \mathbb{F}(u_1, u_2, \ldots, u_n)$.

مثال ۲۱.۹. اگر $x^۲+۱$ به عنوان یک چندجمله‌ای در $\mathbb{R}[x]$ در نظر گرفته شود، آنگاه $\mathbb{C}$ یک توسیع میدان شکافنده می‌باشد زیرا در $\mathbb{C}[x]$، $x^۲+۱=(x+i)(x-i)$ و $\mathbb{C}=\mathbb{R}(i)=\mathbb{R}(i,-i)$. به طور مشابه $\mathbb{Q}(\sqrt{۲})$ یک میدان شکافندهٔ چندجمله‌ای $x^۲-۲$ است زیرا $x^۲-۲=(x+\sqrt{۲})(x-\sqrt{۲})$ و $\mathbb{Q}(\sqrt{۲})=\mathbb{Q}(\sqrt{۲},-\sqrt{۲})$.

مثال ۲۲.۹. چندجمله‌ای $f(x)=x^۴-x^۲-۲$ در $\mathbb{Q}[x]$ به‌صورت $(x^۲-۲)(x^۲+۱)$ تجزیه می‌شود، در نتیجه ریشه‌های آن در $\mathbb{C}$، $\pm\sqrt{۲}$ و $\pm i$ می‌باشند. بنابراین $\mathbb{Q}(\sqrt{۲},i)$ یک میدان شکافنده $f(x)$ روی $\mathbb{Q}$ است.

مثال ۲۳.۹. هر چندجمله‌ای درجه اول $cx+d$ در $\mathbb{F}[x]$ روی $\mathbb{F}$ شکافته می‌شود زیرا $cx+d=c(x-(-c^{-۱}d))$ که در آن $-c^{-۱}d\in\mathbb{F}$. واضح است $\mathbb{F}$ کوچکترین میدانی است که هر دو $\mathbb{F}$ و $c^{-۱}d$ را شامل است، یعنی $\mathbb{F}=\mathbb{F}(c^{-۱}d)$، بنابراین خود $\mathbb{F}$ میدان شکافنده $cx+d$ روی $\mathbb{F}$ است.

مثال ۲۴.۹. مفهوم میدان شکافنده بستگی به چندجمله‌ای و میدان مبنا دارد. برای مثال $\mathbb{C}$ میدان شکافنده $x^۲+۱$ روی $\mathbb{R}$ است ولی روی $\mathbb{Q}$ نیست زیرا $\mathbb{C}$ برابر توسیع $\mathbb{Q}(i)=\mathbb{Q}(i,-i)$ نیست. برای آوردن برهان، تمرین ۱ را ملاحظه کنید.

در اینجا لازم است به دو سوال اصلی در مورد میدان‌های شکافنده پاسخ دهیم: آیا هر چندجمله‌ای در $\mathbb{F}[x]$ دارای یک میدان شکافنده روی $\mathbb{F}$ است؟ اگر این چندجمله‌ای دارای بیشتر از یک میدان شکافنده روی $\mathbb{F}$ باشد، این میدان‌های شکافنده چگونه با هم ارتباط دارند؟

پاسخ غیر رسمی به سوال اول ساده است: اگر $f(x)\in\mathbb{F}[x]$، طبق نتیجه ۱۱.۵ می‌توان یک توسیع $\mathbb{F}(u)$ یافت که یک ریشه u از $f(x)$ را داشته باشد. طبق قضیه عامل، در $\mathbb{F}(u)[x]$ می‌دانیم که $f(x)=(x-u)g(x)$. مجدداً طبق نتیجه ۱۱.۵ یک توسیع $\mathbb{F}(u)(v)$ از $\mathbb{F}(u)$ موجود است که یک ریشه v از $g(x)$ را دارد. با ادامه این فرآیند نهایتاً به یک توسیع میدان شکافنده $f(x)$ می‌رسیم. می‌توان این استدلال را از طریق استقراء فرمولبندی نمود و کمی بیشتر ثابت کرد:

قضیه ۱۳.۹. گیریم $\mathbb{F}$ یک میدان باشد و $f(x)$ یک چندجمله‌ای غیرثابت از درجه n در $\mathbb{F}[x]$ باشد. آنگاه یک میدان شکافنده $\mathbb{K}$ از $f(x)$ موجود است به طوری که $[\mathbb{K} : \mathbb{F}] \leq n!$.

برهان. برهان با استقراء روی درجه $f(x)$ می‌باشد. اگر $f(x)$ درجه ۱ داشته باشد، آنگاه $\mathbb{F}$ خودش میدان شکافنده $f(x)$ است و $[\mathbb{F} : \mathbb{F}] = ۱ \leq ۱!$. فرض کنید قضیه برای تمام چندجمله‌ای‌های از درجه $n - ۱$ درست باشد و این که $f(x)$ دارای درجه n باشد. طبق قضیه ۱۰.۴، $f(x)$ دارای یک عامل تحویل‌ناپذیر در $\mathbb{F}[x]$ می‌باشد. از ضرب این چندجمله‌ای در معکوس ضریب پیشروش یک عامل تکین تحویل‌ناپذیر $p(x)$ از $f(x)$ بدست می‌آید. طبق قضیه ۱۰.۵ یک توسیع میدان وجود دارد که یک ریشه u از $p(x)$ را شامل است (از اینرو یک ریشه از $f(x)$). علاوه بر این $p(x)$ لزوماً چندجمله‌ای کمین u است. در نتیجه طبق ۷.۹، $[\mathbb{F}(u) : \mathbb{F}] = \deg p(x) \leq \deg f(x) = n$. قضیه عامل ۱۲.۴ نشان می‌دهد که برای یک $g(x) \in \mathbb{F}(u)[x]$، $f(x) = (x - u)g(x)$. چون $g(x)$ درجه $n - ۱$ دارد، فرض استقراء وجود میدان شکافنده $\mathbb{K}$ از $g(x)$ روی $\mathbb{F}(u)$ را تضمین می‌کند به طوری که $[\mathbb{K} : \mathbb{F}(u)] \leq (n - ۱)!$. در $\mathbb{K}[x]$،

$$g(x) = c(x - u_۱)(x - u_۲) \cdots (x - u_{n-۱})$$

و بدین دلیل $f(x) = c(x - u)(x - u_۱) \cdots (x - u_{n-۱})$. چون

$$\mathbb{K} = \mathbb{F}(u)(u_۱, \ldots, u_{n-۱}) = \mathbb{F}(u, u_۱, \ldots, u_{n-۱})$$

می‌بینیم که $\mathbb{K}$ یک میدان شکافنده $f(x)$ روی $\mathbb{F}$ است به طوری که

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{F}(u)][\mathbb{F}(u) : \mathbb{F}] \leq (n - ۱)!n = n!.$$

این امر استقراء را تکمیل می‌کند و قضیه ثابت می‌شود. ■

رابطه بین دومیدان شکافندهٔ یک چندجمله‌ای به سادگی بیان می‌شود:

هر دو میدان شکافنده یک چندجمله‌ای در $\mathbb{F}[x]$ یکریخت می‌باشند

عجیب آن است که راحت‌ترین راه اثبات این واقعیت آن است که نتیجه‌ای قویتر از این حالت ویژه را ثابت کنیم.

قضیه ۱۴.۹. گیریم $\sigma : \mathbb{F} \to \mathbb{E}$ یک یکریختی میدان‌ها، $f(x)$ یک چندجمله‌ای غیرثابت در $\mathbb{F}[x]$ و $\sigma f(x)$ چندجمله‌ای متناظر در $\mathbb{E}[x]$ باشد. اگر $\mathbb{K}$ یک میدان شکافنده $f(x)$ روی $\mathbb{F}$ و $\mathbb{L}$ یک میدان شکافنده $\sigma f(x)$ روی $\mathbb{E}$ باشد، آنگاه σ به یک یکریختی $\mathbb{K} \cong \mathbb{L}$ تعمیم می‌یابد.

اگر $\mathbb{F} = \mathbb{E}$ و σ نگاشت همانی $\mathbb{F} \to \mathbb{F}$ باشد، آنگاه این قضیه بیان می‌کند که دو میدان شکافنده $f(x)$ یکریخت می‌باشند.

برهان قضیه ۱۴.۹. برهان با استقراء روی درجه $f(x)$ می‌باشد، اگر $\deg f(x) = ۱$، آنگاه طبق تعریف میدان شکافنده $f(x) = c(x - u)$ در $\mathbb{K}[x]$ و $\mathbb{K} = \mathbb{F}(u)$. ولی $f(x) = cx - cu$ در $\mathbb{F}[x]$ قرار دارد، بنابراین باید c و cu در $\mathbb{F}$ باشد. از اینرو $u = c^{-۱}cu$ نیز در $\mathbb{F}$ است. بنابراین $\mathbb{K} = \mathbb{F}(u) = \mathbb{F}$. دیده‌ایم که σ یک یکریختی $\mathbb{E}[x] \cong \mathbb{F}[x]$ القاء می‌کند، بدین دلیل $\sigma f(x)$ نیز درجه ۱ دارد، و استدلالی مشابه نشان می‌دهد که $\mathbb{E} = \mathbb{L}$. در این حالت σ خودش یک یکریختی با خواص مطلوب می‌باشد.

فرض کنید قضیه برای چندجمله‌ای‌های از درجه $n - ۱$ درست باشد و این که $f(x)$ درجه n داشته باشد. مثل آنچه در برهان قضیه ۱۳.۹ آمده است، طبق قضیه ۱۰.۴ چندجمله‌ای $f(x)$ دارای یک عامل تحویل‌ناپذیر تکین $p(x)$ در $\mathbb{F}[x]$ می‌باشد. چون $\sigma : \mathbb{F}[x] \cong \mathbb{E}[x]$ یک یکریختی است، $\sigma p(x)$ یک عامل تکین تحویل‌ناپذیر از $\sigma f(x)$ در $\mathbb{E}[x]$ است. هر ریشه $p(x)$ نیز یک ریشه $f(x)$ است، بنابراین $\mathbb{K}$ تمام ریشه‌های $p(x)$ را شامل است، و به طور مشابه $\mathbb{L}$ تمام ریشه‌های $\sigma p(x)$ را شامل است. گیریم u ریشه‌ای از $p(x)$ در $\mathbb{K}$ و v ریشه‌ای از $\sigma p(x)$ در $\mathbb{L}$ باشد. آنگاه طبق ۸.۹، σ به یک یکریختی $\mathbb{F}(u) \to \mathbb{E}(v)$ تعمیم می‌یابد که u را به v می‌نگارد، و این وضعیت بدین صورت می‌باشد:

$$\begin{array}{ccc} \mathbb{K} & & \mathbb{L} \\ \cup| & & \cup| \\ \mathbb{F}(u) & \xrightarrow{\cong} & \mathbb{E}(v) \\ \cup| & & \cup| \\ \mathbb{F} & \xrightarrow{\sigma} & \mathbb{E} \end{array}$$

قضیه عامل ۱۲.۴ نشان می‌دهد که $f(x) = (x - u)g(x)$ در $\mathbb{F}(u)[x]$، و از اینرو در $\mathbb{E}(v)[x]$

داریم

$$\sigma f(x) = \sigma(x-u)\sigma g(x) = (x-\sigma(u))\sigma g(x) = (x-v)\sigma g(x).$$

حال $f(x)$ روی $\mathbb{K}$ شکافته می‌شود، مثلاً $f(x) = c(x-u)(x-u_2)\cdots(x-u_n)$. چون $f(x) = (x-u)g(x)$، داریم $g(x) = c(x-u_2)\cdots(x-u_n)$. کوچکترین زیرمیدان شامل تمام ریشه‌های $g(x)$ و میدان $\mathbb{F}(u)$ برابر است با $\mathbb{K} = \mathbb{F}(u, u_2, \ldots, u_n)$، بنابراین $\mathbb{K}$ یک میدان شکافنده $g(x)$ روی $\mathbb{F}(u)$ است، به طور مشابه، $\mathbb{L}$ یک میدان شکافنده $\sigma g(x)$ روی $\mathbb{E}(v)$ است. چون $g(x)$ درجه $n-1$ دارد. فرض استقراء ایجاب می‌کند که یکریختی $\mathbb{F}(u) \cong \mathbb{E}(v)$ را بتوان به یک یکریختی $\mathbb{K} \cong \mathbb{L}$ تعمیم داد. این مطلب استقراء و برهان قضیه را تکمیل می‌کند. ■

یک میدان شکافنده یک چندجمله‌ای روی $\mathbb{F}$ طبق تعریف تمام ریشه‌های این چندجمله‌ای را دارد. بهرحال شگفت‌انگیز است که میدان شکافنده دارای خاصیت قویتری است که اکنون آن را تعریف می‌کنیم. یک توسیع جبری میدان $\mathbb{K}$ از $\mathbb{F}$ **نرمال** است مشروط به آن که وقتی یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}[x]$ یک ریشه داشته باشد، آنگاه این چندجمله‌ای روی $\mathbb{K}$ شکافته شود (یعنی تمام ریشه‌هایش در $\mathbb{K}$ باشد).

قضیه ۱۵.۹. میدان $\mathbb{K}$ یک میدان شکافنده، روی میدان $\mathbb{F}$، یک چندجمله‌ای در $\mathbb{F}[x]$ است اگر و تنها اگر $\mathbb{K}$ یک توسیع با بعدمتناهی و نرمال $\mathbb{F}$ باشد.

برهان. اگر $\mathbb{K}$ یک میدان شکافنده $f(x) \in \mathbb{F}[x]$ باشد، آنگاه $\mathbb{K} = \mathbb{F}(u_1, \ldots, u_n)$ که در آن u_iها تمام ریشه‌های $f(x)$ می‌باشد. در نتیجه طبق قضیه ۱۰.۹، $[\mathbb{K} : \mathbb{F}]$ متناهی است. گیریم $p(x)$ یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}[x]$ باشد که یک ریشه v در $\mathbb{K}$ دارد. $p(x)$ را به عنوان یک چندجمله‌ای در $\mathbb{K}[x]$ در نظر گیرید و $\mathbb{L}$ را یک میدان شکافنده $p(x)$ روی $\mathbb{K}$ اختیار کنید، به طوری که $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$. برای این که ثابت کنیم $p(x)$ روی $\mathbb{K}$ شکافته می‌شود تنها لازم است نشان دهیم که هر ریشه $p(x)$ در $\mathbb{L}$ واقع در $\mathbb{K}$ است.

گیریم $w \in \mathbb{L}$ ریشه دلخواهی از $p(x)$ غیر از v باشد. طبق نتیجه ۸.۹ (با شرط $\mathbb{E} = \mathbb{F}$ و σ نگاشت همانی)، یک یکریختی $\mathbb{F}(v) \cong \mathbb{F}(w)$ وجود دارد که v را به w می‌نگارد و هر عضو $\mathbb{F}$ را به

خودش تصویر می‌کند. زیر میدان $\mathbb{K}(w)$ از $\mathbb{L}$ را در نظر بگیرید، وضعیت به صورت زیر می‌باشد:

$$\begin{array}{ccc} \mathbb{K} & & \mathbb{K}(w) \\ \cup| & & \cup| \\ \mathbb{F}(v) & \xrightarrow{\cong} & \mathbb{F}(w) \\ \cup| & & \cup| \\ \mathbb{F} & = & \mathbb{F} \end{array}$$

چون

$$\mathbb{K}(w) = \mathbb{F}(u_1, \ldots, u_n)(w) = \mathbb{F}(u_1, \ldots, u_n, w) = \mathbb{F}(w)(u_1, \ldots, u_n)$$

می‌بینیم که $\mathbb{K}(w)$ یک میدان شکافنده $f(x)$ روی $\mathbb{F}(w)$ است. علاوه بر این، چون $v \in \mathbb{K}$ و $\mathbb{K}$ میدان شکافنده $f(x)$ روی $\mathbb{F}$ است. $\mathbb{K}$ نیزمیدان شکافنده $f(x)$ روی زیر میدان $\mathbb{F}(v)$ است. در نتیجه، طبق قضیه ۱۴.۹، یکریختی $\mathbb{F}(v) \cong \mathbb{F}(w)$ به یک یکریختی $\mathbb{K}(w) \to \mathbb{K}$ تعمیم می‌یابد که v را به w و هر عضو $\mathbb{F}$ را به خودش می‌نگارد. بنابراین طبق قضیه ۵.۹، $[\mathbb{K} : \mathbb{F}] = [\mathbb{K}(w) : \mathbb{F}]$. در زنجیر توسیع $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{K}(w)$، طبق قضیه ۷.۹، $[\mathbb{K}(w) : \mathbb{K}]$ متناهی‌و طبق تذکرات بند اول برهان $[\mathbb{K} : \mathbb{F}]$ متناهی است. بنابراین قضیه ۴.۹ ایجاب می‌کند که

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K}(w) : \mathbb{F}] = [\mathbb{K}(w) : \mathbb{K}][\mathbb{K} : \mathbb{F}].$$

حذف $[\mathbb{K} : \mathbb{F}]$ از طرفین نشان می‌دهد که $[\mathbb{K}(w) : \mathbb{K}] = 1$ و بنابراین $\mathbb{K}(w) = \mathbb{K}$. ولی این به معنی آن است که w در $\mathbb{K}$ است، بنابراین هر ریشه $p(x)$ در $\mathbb{L}$، در $\mathbb{K}$ قرار دارد، و $p(x)$ روی $\mathbb{K}$ شکافته می‌شود بنابراین $\mathbb{K}$ روی $\mathbb{F}$ نرمال است.

برعکس، فرض کنید که $\mathbb{K}$ یک توسیع با بعدمتناهی و نرمال $\mathbb{F}$ با پایه $\{u_1, \ldots, u_n\}$ باشد. آنگاه $\mathbb{K} = \mathbb{F}(u_1, \ldots, u_n)$. طبق قضیه ۹.۹، هر u_i روی $\mathbb{F}$ جبری می‌باشد و دارای یک چندجمله‌ای کمین مثل $p_i(x)$ است. چون طبق نرمال بودن $p_i(x)$ روی $\mathbb{K}$ شکافته می‌شود، $f(x) = p_1(x) \cdots p_n(x)$ نیز روی $\mathbb{K}$ شکافته می‌شود. بنابراین $\mathbb{K}$ توسیع میدان شکافنده $f(x)$ است. ■

مثال ۲۵.۹. میدان $\mathbb{Q}(\sqrt[3]{2})$ دارای ریشه حقیقی $\sqrt[3]{2}$ از چند جمله‌ای تحویل‌ناپذیر $x^3 - 2 \in \mathbb{Q}[x]$ می‌باشد ولی ریشه مختلط $\sqrt[3]{2}w$ را شامل نیست (همان‌طورکه در مثال ۱۳.۹ گفته شد). بنابراین

$\mathbb{Q}(\sqrt[3]{2})$ یک توسیع نرمال $\mathbb{Q}$ نیست و از اینرو میدان شکافنده هیچ چندجمله‌ای در $\mathbb{Q}[x]$ نمی‌تواند باشد.

در اینجا این سوال طبیعی مطرح است که برای یک میدان $\mathbb{F}$ آیا توسیعی وجود دارد که هر چندجمله‌ای واقع در $\mathbb{F}[x]$ نسبت به آن شکافته شود؟ به بیان دیگر آنکه آیا توسیع میدانی وجود دارد که تمام ریشه‌های همه چندجمله‌ای‌های موجود در $\mathbb{F}[x]$ را شامل باشد. به میدانی که روی آن هر چندجمله‌ای غیرثابت شکافته می‌شود، **بسته جبری** گفته شود. برای مثال قضیه اساسی جبر و نتیجه ۲۳.۴ نشان می‌دهد که میدان اعداد مختلط $\mathbb{C}$، بسته جبری است.

طبق قضیه‌ای مشابه قضیه ۱۴.۹، ثابت می‌شود که هر دو بستار جبری $\mathbb{F}$ یکریخت هستند. اگر $\mathbb{K}$ توسیعی جبری از $\mathbb{F}$ باشد و $\mathbb{K}$ بسته جبری باشد، آنگاه $\mathbb{K}$ **بستار جبری** $\mathbb{F}$ نامیده می‌شود. برای مثال $\mathbb{C}$ بستار جبری $\mathbb{R}$ است زیرا $\mathbb{C} = \mathbb{R}[i]$ یک توسیع جبری از $\mathbb{R}$ است که بسته جبری است. با این حال، $\mathbb{C}$ بستار جبری $\mathbb{Q}$ نمی‌باشد، زیرا $\mathbb{C}$ روی $\mathbb{Q}$ جبری نیست. میدان $\mathbb{E}$ از اعداد جبری (مثال ۲۰.۹ را ملاحظه کنید) بستار جبری $\mathbb{Q}$ می‌باشد (تمرین ۲۰).

تمرینها

۱.A. نشان دهید که $\sqrt{2}$ در $\mathbb{Q}(i)$ نیست و بنابراین $\mathbb{C} \neq \mathbb{Q}(i)$. [راهنمایی: نشان دهید که اگر $\sqrt{2} = a + bi$ که در آن $a, b \in \mathbb{Q}$، آنگاه این امر منجر به یک تناقض می‌شود.]

۲. نشان دهید $x^2 - 3$ و $x^2 - 2x - 2$ در $\mathbb{Q}[x]$ تحویل‌ناپذیرند و دارای میدان شکافنده یکسان، یعنی $\mathbb{Q}(\sqrt{3})$ می‌باشند.

۳. یک میدان شکافنده $x^4 - 4x - 5$ روی $\mathbb{Q}$ را بیابید و نشان دهید که بعد آن روی $\mathbb{Q}$، ۴ است.

۴. اگر $f(x) \in \mathbb{R}[x]$، ثابت کنید که $\mathbb{R}$ یا $\mathbb{C}$ یک میدان شکافنده $f(x)$ روی $\mathbb{R}$ می‌باشد.

۵. گیریم $\mathbb{K}$ میدان شکافنده $f(x)$ روی $\mathbb{F}$ باشد. اگر $\mathbb{E}$ میدانی باشد که $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$، نشان دهید که $\mathbb{K}$ یک میدان شکافنده $f(x)$ روی $\mathbb{E}$ است.

۶. گیریم که $\mathbb{K}$ یک میدان شکافنده $f(x)$ روی $\mathbb{F}$ باشد. اگر $[\mathbb{K} : \mathbb{F}]$ عددی اول، $u \in \mathbb{K}$ ریشه‌ای از $f(x)$ باشد و $u \notin \mathbb{F}$، نشان دهید که $\mathbb{K} = \mathbb{F}(u)$.

۷. اگر u روی $\mathbb{F}$ جبری و $\mathbb{K} = \mathbb{F}(u)$ یک توسیع نرمال $\mathbb{F}$ باشد، ثابت کنید که $\mathbb{K}$ یک میدان شکافنده چندجمله‌ای کمین u روی $\mathbb{F}$ است.

۸. کدام یک از اینها توسیع نرمال $\mathbb{Q}$ می‌باشند.

(الف) $\mathbb{Q}(\sqrt{3})$ (ب) $\mathbb{Q}(\sqrt[3]{2})$ (پ) $\mathbb{Q}(\sqrt{5}, i)$

۹. ثابت کنید که هیچ میدان متناهی، بسته جبری نیست. [راهنمایی: اگر عناصر این میدان $a_1, \ldots, a_n$ باشند که در آن a_1 ناصفر است چندجمله‌ای $a_1 + (x - a_1)(x - a_2)\cdots(x - a_n) \in \mathbb{F}[x]$ را در نظر بگیرید.]

B۱۰. با یافتن عامل‌های درجه دوم، نشان دهید که $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ یک میدان شکافنده $x^4 + 2x^3 - 8x^2 - 6x - 1$ روی $\mathbb{Q}$ است.

۱۱. میدان شکافنده $x^4 + 1$ روی $\mathbb{Q}$ را بیابید و آن را توصیف کنید.

۱۲. یک میدان شکافنده $x^4 - 2$ را روی میدان‌های زیر پیدا کنید.

(الف) روی $\mathbb{Q}$ (ب) روی $\mathbb{R}$

۱۳. یک میدان شکافنده $x^6 + x^3 + 1$ روی $\mathbb{Q}$ را پیدا کنید.

۱۴. نشان دهید که $\mathbb{Q}(\sqrt{2}, i)$ یک میدان شکافنده $x^2 - 2\sqrt{2}x + 3$ روی $\mathbb{Q}(\sqrt{2})$ است.

۱۵. یک میدان شکافنده $x^2 + 1$ روی $\mathbb{Z}_3$ را پیدا کنید.

۱۶. یک میدان شکافنده $x^3 + x + 1$ روی $\mathbb{Z}_2$ را پیدا کنید.

۱۷. اگر یک توسیع $\mathbb{K}$ از میدان $\mathbb{F}$ طوری باشد که $[\mathbb{K} : \mathbb{F}] = 2$، ثابت کنید که $\mathbb{K}$ نرمال است.

۱۸. گیریم $\mathbb{F}$، $\mathbb{E}$ و $\mathbb{K}$ میدان‌هایی باشند که $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ و $\mathbb{E} = \mathbb{F}(u_1, \ldots, u_t)$ که در آن u_iها برخی از ریشه‌های $f(x) \in \mathbb{F}[x]$ می‌باشد. ثابت کنید که $\mathbb{K}$ میدان شکافنده $f(x)$ روی $\mathbb{F}$ است اگر و تنها اگر $\mathbb{K}$ میدان شکافنده $f(x)$ روی $\mathbb{E}$ است.

۱۹. ثابت کنید که شرایط زیر روی میدان $\mathbb{K}$ هم‌ارزند.

(الف) هر چندجمله‌ای غیر ثابت در $\mathbb{K}[x]$ یک ریشه در $\mathbb{K}$ دارد.

(ب) هر چندجمله‌ای غیرثابت در $\mathbb{K}[x]$ روی $\mathbb{K}$ شکافته‌می‌شود (یعنی $\mathbb{K}$ بسته‌جبری است).

(پ) هر چندجمله‌ای تحویل‌ناپذیر در $\mathbb{K}[x]$ از درجه ۱ است.

(ت) هیچ توسیع جبری از میدان $\mathbb{K}$ بجز خود $\mathbb{K}$ وجود ندارد.

۲۰. گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد و $\mathbb{E}$ زیر میدان تمام عناصری از $\mathbb{K}$ باشد که روی $\mathbb{F}$ جبری است، همان‌طور که در نتیجه ۱۲.۹ آمده است. اگر $\mathbb{K}$ بسته جبری باشد، ثابت کنید که $\mathbb{E}$ یک بستار جبری از $\mathbb{F}$ است. [حالت خاصی که $\mathbb{F} = \mathbb{Q}$ و $\mathbb{K} = \mathbb{C}$ نشان می‌دهد که میدان $\mathbb{E}$ متشکل از عناصر جبری، بستار جبری $\mathbb{Q}$ است.]

۲۱. گیریم $\mathbb{K}$ یک توسیع جبری میدان $\mathbb{F}$ باشد که هر چندجمله‌ای واقع در $\mathbb{F}[x]$ روی $\mathbb{K}$ شکافته شود. ثابت کنید که $\mathbb{K}$ بستار جبری $\mathbb{F}$ است.

۲۲.C. ثابت کنید که یک توسیع با بعدمتناهی $\mathbb{K}$ از $\mathbb{F}$ نرمال است اگر و تنها اگر دارای این ویژگی باشد: وقتی که $\mathbb{L}$ یک توسیع میدان $\mathbb{K}$ و $\sigma : \mathbb{K} \to \mathbb{L}$ یک همریختی یک به یک باشد که برای هر $c \in \mathbb{F}$، $\sigma(c) = c$، آنگاه $\sigma(\mathbb{K}) \subseteq \mathbb{K}$.

۹-۵ تفکیک پذیـــری

هر چندجمله‌ای دارای میدانی شکافنده است که تمام ریشه‌هایش را شامل است. این ریشه‌ها ممکن است همگی متمایز بوده و یا بعضی از آن‌ها ریشه مکرر باشد[۴]. در این بخش حالتی را در نظر می‌گیریم که همه ریشه‌ها متمایز باشند و از اطلاعات بدست آمده استفاده می‌کنیم تا واقعیت مفیدی را دربارهٔ توسیع‌های با بعدمتناهی ثابت کنیم.

گیریم $\mathbb{F}$ یک میدان باشد. یک چندجمله‌ای $f(x) \in \mathbb{F}[x]$ از درجه n را **تفکیک‌پذیر** گویند اگر این چندجمله‌ای دارای n ریشه متمایز در یک میدان شکافنده باشد[۵]. به طور معادل $f(x)$ تفکیک‌پذیر است اگر این چندجمله‌ای در هر میدان شکافنده ریشه مکرر نداشته باشد. یک توسیع میدان $\mathbb{K}$ از $\mathbb{F}$ را **توسیع تفکیک‌پذیر** (یا تفکیک‌پذیر روی $\mathbb{F}$) گویند اگر هر عنصر $\mathbb{K}$ ریشه یک چندجمله‌ای تفکیک‌پذیر در $\mathbb{F}[x]$ باشد. بنابراین هر توسیع تفکیک‌پذیر لزوماً جبری است.

مثال ۲۶.۹. چندجمله‌ای $x^2 + 1 \in \mathbb{Q}[x]$ تفکیک‌پذیر است زیرا دارای ریشه‌های متمایز i و $-i$ در $\mathbb{C}$ است، ولی $f(x) = x^4 - x^3 - x + 1$ تفکیک‌پذیر نیست زیرا به صورت $(x-1)^2(x^2+x+1)$ تجزیه می‌شود. بدین دلیل $f(x)$ دارای یک ریشه مکرر است و مجموعاً

۴) ریشه مکرر وقتی پیدا می‌شود که در میدان شکافنده داشته باشیم $f(x) = c(x-u_1)\cdots(x-u_n)$ و برای برخی $i \neq j$، $u_i = u_j$.

۵) چون هر دو میدان شکافنده یکریختند این یعنی که $f(x)$، n ریشه متمایز در هر میدان شکافنده دارد.

سه ریشه متمایز در $\mathbb{C}$ دارد. آزمون‌های گوناگونی برای تفکیک‌پذیری وجود دارد که در آنها از مفهوم زیر استفاده می‌شود: **مشتق** چندجمله‌ای

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n \in \mathbb{F}[x]$$

به صورت چندجمله‌ای[۶]

$$f'(x) = c_1 + 2c_2x + \cdots + nc_nx^{n-1} \in \mathbb{F}[x]$$

تعریف می‌شود. تمرین‌های ۴ و ۵ را بکار برید تا تحقیق کنید که مشتقات تعریف شده به این روش جبری دارای خواص آشنای

$$(f+g)'(x) = f'(x) + g'(x)$$
$$(fg)'(x) = f(x)g'(x) + f'(x)g(x)$$

می‌باشد.

لم ۱۶.۹. گیریم $\mathbb{F}$ یک میدان باشد و $f(x) \in \mathbb{F}[x]$. اگر $f(x)$ و $f'(x)$ در $\mathbb{F}[x]$ نسبت به هم اول باشند، آنگاه $f(x)$ تفکیک‌پذیر است.

توجه کنید که این لم در $\mathbb{F}[x]$ کارکرد دارد و برای تعیین تفکیک‌پذیری، هیچ اطلاعی از میدان شکافنده لازم نیست. برای دیگر معیارهای تفکیک‌پذیری تمرینهای ۱۰-۸ را ملاحظه کنید.

برهان لم ۱۶.۹. گیریم $\mathbb{K}$ یک میدان شکافنده $f(x)$ باشد و به خلاف، فرض کنید $f(x)$ تفکیک‌پذیر نباشد. آنگاه $f(x)$ باید دارای یک ریشه مکرر u در $\mathbb{K}$ باشد. پس برای برخی $g(x) \in \mathbb{K}[x]$ داریم $f(x) = (x-u)^2g(x)$ و

$$f'(x) = (x-u)^2g'(x) + 2(x-u)g(x).$$

بنابراین $f'(u) = 0_{\mathbb{F}}g'(u) + 0_{\mathbb{F}}g(u) = 0_{\mathbb{F}}$ و u یک ریشه $f'(x)$ نیز می‌باشد. اگر $p(x) \in \mathbb{F}[x]$ چندجمله‌ای کمین u باشد، آنگاه $p(x)$ غیر ثابت است و هر دو $f(x)$ و $f'(x)$ را می‌شمارد. بنابراین

۶) وقتی $\mathbb{F} = \mathbb{R}$، این همان مشتق معمولی حسابان مقدماتی است. ولی تعریف ما صرفاً جبری است و برای چندجمله‌ای‌های روی هر میدان بکار می‌رود، در صورتی که مفهوم حد که در حسابان در تعریف مشتق بکار می‌رود ممکن است در بعضی از میدان‌ها تعریف نشود.

$f(x)$ و $f'(x)$ نسبت به هم اول نیستند که یک تناقض است. از اینرو $f(x)$ تفکیک‌پذیر است. ■

بخاطر آورید که برای یک عدد صحیح مثبت n و $c \in \mathbb{F}$، nc عضو $c + c + \cdots + c$ (n جمعوند) می‌باشد. یک میدان را از **مشخصه صفر** گویند اگر برای هر عدد صحیح مثبت n، $n1_{\mathbb{F}} \neq 0_{\mathbb{F}}$. برای مثال $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ همه مشخصهٔ صفر دارند، ولی $\mathbb{Z}_2$ مشخصه صفر ندارد (زیرا در $\mathbb{Z}_2$، $1 + 1 = 0$). هر میدان با مشخصه صفر نامتناهی است (تمرین ۳). اگر $\mathbb{F}$ مشخصه صفر داشته باشد، آنگاه برای هر عدد صحیح مثبت n و $c \in \mathbb{F}$،

$$nc = c + \cdots + c = (1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}})c = (n1_{\mathbb{F}})c$$

که در آن $n1_{\mathbb{F}} \neq 0_{\mathbb{F}}$. بنابراین $nc = 0$ اگر و تنها اگر $c = 0_{\mathbb{F}}$. این امر کلید تفکیک‌پذیری در میدان‌های با مشخصه صفر است.

قضیه ۱۷.۹. گیریم $\mathbb{F}$ میدانی از مشخصه صفر باشد. آنگاه هر چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}[x]$ تفکیک‌پذیر است و هر توسیع جبری میدان $\mathbb{K}$ از $\mathbb{F}$ یک توسیع تفکیک‌پذیر است.

این قضیه در صورتی که مشخصه $\mathbb{F}$ صفر نباشد، ممکن است غلط باشد (تمرین ۱۵).

برهان قضیه ۱۷.۹. یک چندجمله‌ای تحویل‌ناپذیر $p(x) \in \mathbb{F}[x]$ غیرثابت است و بدین دلیل

$$p(x) = cx^n + \text{(جملات از درجه کمتر)} \quad \text{که در آن} \quad c \neq 0_{\mathbb{F}} \text{ و } n \geq 1.$$

آنگاه

$$p'(x) = ncx^{n-1} + \text{(جملات از درجه کمتر)} \quad \text{که در آن} \quad nc \neq 0_{\mathbb{F}}$$

بنابراین $p'(x)$ یک چندجمله‌ای از درجه کمتر از درجه چندجمله‌ای تحویل‌ناپذیر $p(x)$ است. بنابراین $p(x)$ و $p'(x)$ باید نسبت به هم اول باشند. بدین دلیل $p(x)$ طبق لم ۱۶.۹ تفکیک‌پذیر است. بخصوص، چندجمله‌ای کمین هر $u \in \mathbb{K}$ تفکیک‌پذیر است. بنابراین $\mathbb{K}$ یک توسیع تفکیک‌پذیر است. ■

توسیع‌های تفکیک‌پذیر دارای زیبایی خاصی هستند زیرا درواقع هر توسیع تفکیک‌پذیر با مولدمتناهی (بویژه، هر توسیع با بعدمتناهی) ساده است:

قضیه ۱۸.۹[۷]. اگر $\mathbb{K}$ یک توسیع با مولدمتناهی تفکیک‌پذیر $\mathbb{F}$ باشد، آنگاه برای یک $u \in \mathbb{K}$، $\mathbb{K} = \mathbb{F}(u)$.

برهان. طبق فرض $\mathbb{K} = \mathbb{F}(u_1, \ldots, u_n)$. برهان با استقراء روی n است. وقتی $n = 1$ چیزی برای اثبات نمی‌ماند و $\mathbb{K} = \mathbb{F}(u_1)$. در بند بعد نشان خواهیم داد که قضیه برای $n = 2$ درست است. به استقراء فرض کنید که برای $n = k - 1$ قضیه درست است و فرض کنید $n = k$. طبق استقراء و حالت $n = 2$، $t, u \in \mathbb{K}$ وجود دارد به طوری که

$$\mathbb{K} = \mathbb{F}(u_1, \ldots, u_k) = \mathbb{F}(u_1, \ldots, u_{k-1})(u_k) = \mathbb{F}(t)(u_k) = \mathbb{F}(t, u_k) = \mathbb{F}(u).$$

برای اتمام برهان فرض می‌کنیم $\mathbb{K} = \mathbb{F}(v, w)$ و نشان می‌دهیم که $\mathbb{K}$ یک توسیع ساده $\mathbb{F}$ است. اول فرض کنید که $\mathbb{F}$ نامتناهی است (که همیشه در مشخصه صفر طبق تمرین ۳ چنین است). گیریم $p(x) \in \mathbb{F}[x]$ چندجمله‌ای کمین v و $q(x) \in \mathbb{F}[x]$ چندجمله‌ای کمین w باشد. گیریم $\mathbb{L}$ یک میدان شکافنده $p(x)q(x)$ روی $\mathbb{F}$ باشد. گیریم $w = w_1, w_2, \ldots, w_n$ ریشه‌های $q(x)$ در $\mathbb{L}$ باشند. طبق تعریف تفکیک‌پذیری، w ریشه یک چندجمله‌ای $f(x) \in \mathbb{F}[x]$ با ریشه‌های متمایز در یک میدان شکافنده است. چون طبق ۶.۹، $q(x) | f(x)$، تمام w_iها ریشه‌های $f(x)$ هستند و بنابراین باید مجزا باشند. گیریم $v = v_1, v_2, \ldots, v_m$ ریشه‌های $p(x)$ در $\mathbb{L}$ باشد. چون $\mathbb{F}$ نامتناهی است، باید $c \in \mathbb{F}$ موجود باشد به طوری که

$$c \neq \frac{v_i - v}{w - w_j}, \qquad 1 \leq j \leq n, \qquad \text{برای هر } 1 \leq i \leq m \qquad (*)$$

گیریم $u = v + cw$. ادعا می‌کنیم که $\mathbb{K} = \mathbb{F}(u)$. برای این که نشان دهیم $w \in \mathbb{F}(u)$، گیریم $h(x) = p(u - cx) \in \mathbb{F}(u)[x]$ و توجه کنید که w ریشه $h(x)$ است:

$$h(w) = p(u - cw) - p(v) = 0$$

فرض کنید یک w_j (با $j \neq 1$) نیز یک ریشه $h(x)$ باشد. آنگاه $p(u - cw_j) = 0$، بنابراین $u - cw_j$ یکی از ریشه‌های $p(x)$، مثلاً $v_i = u - cw_j$، می‌باشد. چون $u = v + cw$، خواهیم داشت $v + cw - cw_j = v_i$ یا به طور معادل $c = (v_i - v)/(w - w_j)$. این متناقض با $(*)$ است. بنابراین w تنها ریشه مشترک $q(x)$ و $h(x)$ می‌باشد.

۷) از این قضیه فقط در بخش ۲.۱۱ استفاده می‌شود.

گیریم $r(x)$ چندجمله‌ای کمین w روی $\mathbb{F}(u)$ باشد. آنگاه $r(x)$ چندجمله‌ای تفکیک‌پذیر $q(x)$ را می‌شمارد، لذا $r(x)$ در $\mathbb{L}[x]$ شکافته می‌شود، و تمام ریشه‌هایش متمایزند. ولی $r(x)$، $h(x)$ را نیز می‌شمارد، پس هر ریشه آن یک ریشه $h(x)$ است. طبق بند قبل، $r(x)$ دارای یک تک ریشه w در $\mathbb{L}$ است. بنابراین $r(x) \in \mathbb{R}(u)[x]$ باید درجه ۱ داشته باشد، و بدین دلیل ریشه‌اش w در $\mathbb{F}(u)$ است. چون $v = u - cw$ و $w \in \mathbb{F}(u)$، لذا $v \in \mathbb{F}(u)$ و بدین دلیل $\mathbb{K} = \mathbb{F}(v, w) \subseteq \mathbb{F}(u)$. ولی $u = v + cw \in \mathbb{K}$، بنابراین $\mathbb{F}(u) \subseteq \mathbb{K}$، و از اینرو $\mathbb{K} = \mathbb{F}(u)$. این امر برهان را وقتی که $\mathbb{F}$ نامتناهی است تمام می‌کند. برای حالتی که $\mathbb{F}$ متناهی است، قضیه ۲۸.۹ بخش بعدی را ملاحظه کنید. ■

مثال ۲۷.۹. با بکارگیری برهان قضیه‌برای $\mathbb{Q}(\sqrt{۳}, \sqrt{۵})$، داریم $v = \sqrt{۳}$، $v_۲ = -\sqrt{۳}$، $w = \sqrt{۵}$، $w_۲ = -\sqrt{۵}$، بنابراین می‌توان اختیار کرد $c = ۱$. آنگاه $u = \sqrt{۳} + \sqrt{۵}$ و $\mathbb{Q}(\sqrt{۳}, \sqrt{۵})$ توسیع ساده $\mathbb{Q}(\sqrt{۳} + \sqrt{۵})$ است.

تمرینها

تذکّر: $\mathbb{K}$ همواره یک توسیع میدان $\mathbb{F}$ است.

A.۱. اگر $\mathbb{K}$ روی $\mathbb{F}$ تفکیک‌پذیر و $\mathbb{E}$ یک میدان باشد به طوری که $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$، نشان دهید که $\mathbb{K}$ روی $\mathbb{E}$ تفکیک‌پذیر است.

۲. اگر $\mathbb{F}$ مشخصه صفر داشته باشد، نشان دهید که $\mathbb{K}$ مشخصه صفر دارد.

۳. نشان دهید که هر میدان به مشخصه صفر نامتناهی است.

B.۴. اگر $f(x)$ و $g(x) \in \mathbb{F}[x]$، ثابت کنید:

(الف) $(f + g)'(x) = f'(x) + g'(x)$

(ب) اگر $c \in \mathbb{F}$، آنگاه $(cf)'(x) = cf'(x)$

۵. (الف) اگر $f(x) = cx^n \in \mathbb{F}[x]$ و $g(x) = b_۰ + b_۱x + \cdots + b_kx^k \in \mathbb{F}[x]$، ثابت کنید که $(fg)'(x) = f(x)g'(x) + f'(x)g(x)$.

(ب) اگر $f(x)$ و $g(x)$ چندجمله‌ای‌های دلخواه در $\mathbb{F}[x]$ باشد، ثابت کنید که $(fg)'(x) = f(x)g'(x) + f'(x)g(x)$. [راهنمایی: قسمت الف و تمرین ۴

را بکار برید؛ توجه کنید که اگر $f(x) = a_0 + a_1x + \cdots + a_nx^n$ آنگاه $(fg)(x) = a_0g(x) + a_1xg(x) + \cdots + a_nx^ng(x)$ [راهنمایی: استقراء روی n].

۶. اگر $f(x) \in \mathbb{F}[x]$ و n یک عدد صحیح مثبت باشد، ثابت کنید که مشتق $(f(x))^n$ برابر $nf(x)^{n-1}f'(x)$ می‌باشد. [راهنمایی: از استقراء روی n و تمرین ۵ استفاده کنید.]

۷. (الف) اگر $\mathbb{F}$ مشخصه صفر داشته باشد، $f(x) \in \mathbb{F}[x]$ و $f'(x) = 0_{\mathbb{F}}$، ثابت کنید که برای یک $c \in \mathbb{F}$ و $f(x) = c$.

(ب) با ارائه یک مثال در $\mathbb{Z}_2[x]$ نشان دهید که اگر $\mathbb{F}$ مشخصه صفر نداشته باشد، قسمت (الف) ممکن است غلط باشد.

۸. ثابت کنید که $u \in \mathbb{K}$ یک ریشه مکرر $f(x) \in \mathbb{K}[x]$ است اگر و تنها اگر u ریشه مشترک $f(x)$ و $f'(x)$ باشد. [راهنمایی: $f(x) = (x-u)^m g(x)$ که در آن $m \geq 1$، $g(x) \in \mathbb{K}[x]$، $g(u) \neq 0_{\mathbb{F}}$؛ u یک ریشه مکرر $f(x)$ است اگر و فقط اگر $m > 1$، تمرین‌های ۵ و ۶ را بکار برید تا $f'(x)$ را محاسبه کنید.]

۹. ثابت کنید که $f(x) \in \mathbb{F}[x]$ تفکیک‌پذیر است اگر و تنها اگر $f(x)$ و $f'(x)$ نسبت به‌هم اول باشند. [لم ۱۶.۹ و تمرین ۸ را ببینید.]

۱۰. گیریم $p(x)$ در $\mathbb{F}[x]$ تحویل‌ناپذیر باشد ثابت کنید $p(x)$ تفکیک‌ناپذیر است اگر و تنها اگر $p'(x) \neq 0_{\mathbb{F}}$.

۱۱. فرض کنید $\mathbb{F}$ مشخصه صفر دارد و $\mathbb{K}$ یک میدان شکافنده $f(x) \in \mathbb{F}[x]$ است. اگر $d(x)$ بزرگترین مقسوم‌علیه مشترک $f(x)$ و $f'(x)$ باشد و $h(x) = f(x)/d(x) \in \mathbb{F}[x]$، ثابت کنید:

(الف) $f(x)$ و $h(x)$ ریشه‌های یکسان در $\mathbb{K}$ دارند.

(ب) $h(x)$ تفکیک‌پذیر است.

۱۲. از برهان قضیه ۱۸.۹ استفاده کنید تا هر یک از موارد زیر را به صورت توسیع‌های ساده $\mathbb{Q}$ بیان کنید.

(الف) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ (ب) $\mathbb{Q}(\sqrt{3}, i)$ (پ) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

۱۳. اگر p و q اعداد اول متمایز باشند، ثابت کنید که $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.

۱۴. فرض کنید $\mathbb{F}$ نامتناهی بوده، $v, w \in \mathbb{K}$ روی $\mathbb{F}$ جبری باشند و این که w ریشه یک چندجمله‌ای تفکیک‌پذیر در $\mathbb{F}[x]$ باشد. ثابت کنید که $\mathbb{F}(v, w)$ یک توسیع ساده $\mathbb{F}$ است. [راهنمایی: برهان قضیه ۱۸.۹ را پس از سازگاری بکار برید.]

۱۵. در اینجا یک مثال از یک چندجمله‌ای تحویل‌ناپذیر آمده است که تفکیک‌پذیر نیست. گیریم $\mathbb{F} = \mathbb{Z}_۲(t)$ میدان خارج قسمتی $\mathbb{Z}_۲[t]$ (حلقه چندجمله‌ای‌های با متغیر t و ضرایب در $\mathbb{Z}_۲$) باشد، همانگونه که در بخش ۴.۸ تعریف شده است.

(الف) ثابت کنید که $x^۲ - t$ در $\mathbb{F}[x]$ یک چندجمله‌ای تحویل‌ناپذیر است [راهنمایی: اگر $x^۲ - t$ یک ریشه در $\mathbb{F}$ داشته باشد، آنگاه چندجمله‌ای‌های $g(t)$ و $h(t)$ در $\mathbb{Z}_۲[t]$ وجود دارند به طوری که $t = [g(t)/h(t)]^۲$؛ این منجر به تناقض می‌شود؛ نتیجه ۱۴.۴ را بکار برید.]

(ب) ثابت کنید که $x^۲ - t \in \mathbb{F}[x]$ تفکیک‌پذیر نیست. [راهنمایی: نشان دهید که مشتق آن صفر است و تمرین ۹ را بکار برید.]

۹-۶ میدان‌های متناهی

میدان‌های متناهی، کاربردهایی در شاخه‌های مختلف از جمله هندسه تصویری، ریاضی ترکیبیاتی، طرح آزمایش و رمزنگاری دارد. در این بخش میدان‌های متناهی برحسب توسیع‌های میدان و میدان‌های شکافنده سرشت‌نمایی شده‌اند، و ساختار آن‌ها به طور کامل تا حد یکریختی تعیین گردیده است.

این بخش را با بیان چند تعریف و نتیجه در مورد حلقه‌هایی که لزوماً میدان و یا حتی متناهی نیستند آغاز می‌کنیم. با این حال علاقه اصلی ما استفاده از نتایج آنها برای میدان‌های متناهی خواهد بود.

گیریم R حلقه‌ای‌یکدار باشد. بخاطر آورید که برای یک عدد صحیح مثبت m و $c \in R$، منظور از mc عضو $c + c + \cdots + c$ (m جمعوند) می‌باشد. حلقه R را از **مشخصهٔ صفر** گویند اگر برای هر عدد صحیح مثبت m، $m1_R \neq 0$. از طرف دیگر اگر برای یک m مثبت، $m1_R = 0_R$، آنگاه طبق اصل خوش‌ترتیبی کوچکترین چنین mای وجود دارد. حلقه R را از **مشخصه n** گویند هرگاه n کوچکترین عدد مثبتی باشد که $n1_R = 0_R$[۸]. برای مثال، $\mathbb{Q}$ مشخصه صفر دارد و $\mathbb{Z}_۲$

۸) اگر فصل ۷ را خوانده‌اید، درخواهید یافت که وقتی مشخصه R مثبت باشد، مشخصه همان مرتبه 1_R در گروه

مشخصه ۳ دارد.

لم ۱۹.۹. اگر R یک دامنه صحیح باشد، آنگاه مشخصه R صفر و یا یک عدد اول مثبت است.

برهان. اگر R مشخصه صفر داشته باشد، چیزی برای اثبات وجود ندارد، بنابراین فرض کنید مشخصه R، $n > 0$ باشد. اگر n اول نباشد آنگاه اعداد صحیح مثبت k، t با $k < n$ و $1 < t$ وجود دارند به طوری که $n = kt$. قوانین توزیع‌پذیری نشان می‌دهد

$$\begin{aligned}(k1_R)(t1_R) &= \underbrace{(1_R + \cdots + 1_R)}_{k \text{ جمعوند}}\underbrace{(1_R + \cdots + 1_R)}_{t \text{ جمعوند}} \\ &= 1_R 1_R + \cdots + 1_R 1_R = 1_R + \cdots + 1_R \quad (kt \text{ جمعوند}) \\ &= (kt)1_R = n1_R = 0.\end{aligned}$$

چون R دامنه صحیح است یا $k1_R = 0$ یا $t1_R = 0$ که متناقض با این واقعیت است که n کوچکترین عدد صحیح مثبتی است که $n1_R = 0$. بنابراین n اول است. ■

لم ۲۰.۹. گیریم R حلقه‌ای یکدار با مشخصه $n > 0$ باشد. آنگاه $k1_R = 0_R$ اگر و تنها اگر $n|k$.[۹]

برهان. اگر $n|k$، مثلاً $k = nd$، آنگاه

$$k1_R = nd1_R = (n1_R)(d1_R) = 0_R(d1_R) = 0_R.$$

برعکس، فرض کنید $k1_R = 0$. طبق الگوریتم تقسیم، $k = nq + r$ با شرط $0 \leq r < n$. حال $n1_R = 0$، بنابراین

$$r1_R = r1_R + 0_R = r1_R + nq1_R = (r + nq)1_R = k1_R = 0_R.$$

چون $r < n$ و طبق تعریف مشخصه، n کوچکترین عدد صحیح مثبتی است که $n1_R = 0_R$، باید داشته باشیم $r = 0$. بنابراین $k = nq$ و $n|k$. ■

جمعی R است.

۹) این لم دقیقاً حالت خاصی (در نماد جمعی) از قسمت (۲) قضیه ۵.۷، با شرط $a = 1_R$ و $e = 0_R$ می‌باشد.

قضیه ۲۱.۹. گیریم R حلقه‌ای یکدار باشد. آنگاه

(۱) مجموعه $P = \{k1_R : k \in \mathbb{Z}\}$ زیرحلقه‌ای از R است.

(۲) اگر R مشخصه صفر داشته باشد، آنگاه $P \cong \mathbb{Z}$.

(۳) اگر R مشخصه n ($n > 0$) داشته باشد، آنگاه $P \cong \mathbb{Z}_n$.

برهان. نگاشت $f : \mathbb{Z} \to R$ با ضابطه $f(k) = k1_R$ را تعریف کنید. آنگاه

$$f(k+t) = (k+t)1_R = k1_R + t1_R = f(k) + f(t).$$

قوانین توزیع‌پذیری (همانگونه که در برهان لم ۹.۹ آمده است) نشان می‌دهد که

$$f(kt) = (kt)1_R = (k1_R)(t1_R) = f(k)f(t).$$

بنابراین f یک همریختی است. برد f دقیقاً مجموعه P است و بنابراین طبق تمرین ۱۰ بخش ۳.۳، P یک حلقه است. در نتیجه f، می‌تواند به عنوان یک همریختی پوشا از $\mathbb{Z}$ به روی P در نظر گرفته شود، آنگاه طبق قضیه اول یکریختی، قضیه ۱۱.۶، $P \cong \mathbb{Z}/ker f$. اگر R مشخصهٔ صفر داشته باشد، آنگاه $k = 0$ تنها عدد صحیحی است که $k1_R = 0_R$. بنابراین هسته f ایده‌ال (0) در $\mathbb{Z}$ است و $P \cong \mathbb{Z}/(0) \cong \mathbb{Z}$. اگر R مشخصه $n > 0$ داشته باشد، آنگاه لم ۲۰.۹، نشان می‌دهد که هسته f ایده‌ال‌اصلی (n) متشکل‌از تمام مضارب n است. بدین دلیل $P \cong \mathbb{Z}/(n) = \mathbb{Z}_n$. ■

طبق قضیه ۲۱.۹، هر میدان از مشخصه صفر یک نسخه از $\mathbb{Z}$ را شامل است و بدین دلیل باید نامتناهی باشد. بنابراین طبق لم ۱۹.۹، داریم:

نتیجه ۲۲.۹. هر میدان متناهی به ازاء یک عدد اول p، مشخصه p دارد.

با این حال، عکس نتیجه ۲۲.۹ غلط است، زیرا میدان‌های نامتناهی از مشخصه p وجود دارد (تمرین ۸).

اگر $\mathbb{K}$ میدانی از مشخصه p باشد (بویژه، اگر $\mathbb{K}$ متناهی باشد)، آنگاه قضیه ۲۱.۹ نشان می‌دهد که $\mathbb{K}$ یک زیرمیدان $\mathbb{P}$ یکریخت با $\mathbb{Z}_p$ دارد. این میدان $\mathbb{P}$ **زیرمیدان اول** $\mathbb{K}$ نامیده می‌شود و در هر زیرمیدان $\mathbb{K}$ قرار دارد (زیرا هر زیرمیدان، $1_{\mathbb{K}}$ را شامل است و از اینرو برای هر عدد صحیح t شامل

$t1_{\mathbb{K}}$ است[۱۰]). تمرین ۴ را برای توصیف دیگری از $\mathbb{P}$ ملاحظه کنید. ما زیرمیدان اول $\mathbb{P}$ را با نسخه یکریختش $\mathbb{Z}_p$ یکی می‌گیریم، آنگاه

هر میدان با مشخصه p، $\mathbb{Z}_p$ را شامل است.

تعداد عناصر یک میدان متناهی $\mathbb{K}$، **مرتبه** $\mathbb{K}$ نامیده می‌شود. برای تعیین مرتبه یک میدان متناهی $\mathbb{K}$ با مشخصه p، $\mathbb{K}$ را به عنوان توسیعی از زیرمیدان $\mathbb{Z}_p$ در نظر می‌گیریم:

قضیه ۲۳.۹. اگر میدان متناهی $\mathbb{K}$ از مشخصه p باشد آنگاه $\mathbb{K}$ دارای مرتبه p^n است، که در آن $n = [\mathbb{K} : \mathbb{Z}_p]$.

برهان. مسلماً یک مجموعه متناهی از عناصر وجود دارد که روی $\mathbb{Z}_p$، $\mathbb{K}$ را پدید می‌آورد (برای مثال خود مجموعه $\mathbb{K}$). در نتیجه، طبق تمرین ۲۲ از بخش ۱.۹، $\mathbb{K}$ یک پایه متناهی $\{u_1, u_2, \ldots, u_n\}$ روی $\mathbb{Z}_p$ دارد. طبق تمرین ۹ بخش ۱.۹، هر عضو $\mathbb{K}$ را می‌توان به طور یکتایی به صورت

$$c_1u_1 + c_2u_2 + \cdots + c_nu_n \qquad (*)$$

نوشت، که در آن هر $c_i \in \mathbb{Z}_p$. چون دقیقاً p امکان برای هر c_i وجود دارد. دقیقاً p^n ترکیب خطی متمایز به صورت $(*)$ وجود دارد. بنابراین $\mathbb{K}$ مرتبه p^n دارد، که در آن $n = [\mathbb{K} : \mathbb{Z}_p]$ تعداد عناصر پایه‌است. ■

قضیه ۲۳.۹، محدودیت‌هایی را روی اندازه ممکن یک میدان اعمال می‌کند. برای مثال یک میدان از مرتبه ۶ نمی‌تواند وجود داشته باشد زیرا ۶ توانی از یک عدد اول نیست. این مطلب پرسش‌های گوناگونی را مطرح می‌کند. آیا برای هر عدد اول p میدانی از مرتبه p^n وجود دارد؟ دو میدان از مرتبه p^n چه ربطی با یکدیگر دارند؟ پاسخ این سوالات در قضیه ۲۵.۹ و نتایج آن آمده است. برای اثبات این قضیه به یک لم فنی نیاز است.

---

۱۰) اگر $\mathbb{K}$ مشخصه صفر داشته باشد، آنگاه $\mathbb{K}$ یک نسخه یکریخت $\mathbb{P}$ از $\mathbb{Z}$ را دارد. چون $\mathbb{K}$ وارون ضربی هر عضو ناصفر $\mathbb{P}$ را دارد، نتیجه می‌شود که $\mathbb{K}$ نسخه‌ای از $\mathbb{Q}$ را شامل است. مثل حالت مشخصه p، این میدان (**زیرمیدان اول** نامیده می‌شود) در هر زیرمیدان، $\mathbb{K}$ قرار دارد. برای دیدن بیان دقیق‌تری از این مطلب، قضیه ۲۵.۸ را (با شرط $R = P \cong \mathbb{Z}$ و $\mathbb{F} \cong \mathbb{Q}$) ملاحظه کنید.

لم ۲۴.۹. (**رویای سال‌اولی‌ها**[۱۱]) گیریم p عددی اول و R حلقه‌ای یکدار به مشخصه p باشد. آنگاه برای $a, b \in R$ و هر عدد صحیح مثبت n

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

برهان. برهان با استقراء روی n است. اگر $n = ۱$، آنگاه قضیه دوجمله‌ای در پیوست **ث** نشان می‌دهد که

$$(a+b)^p = a^p + \binom{p}{۱}a^{p-۱}b + \cdots + \binom{p}{r}a^{p-r}b^r + \cdots + \binom{p}{p-۱}ab^{p-۱} + b^p.$$

هرکدام از ضرایب میانی $\binom{p}{r} = \frac{p!}{r!(p-r)!}$ طبق تمرین ۶ در پیوست **ث** عددی صحیح است. چون هر جمله مخرج اکیداً کمتر از عدد اول p است، عامل p در صورت حذف نمی‌شود و بنابراین $\binom{p}{r}$ بر p بخش‌پذیر است، مثلاً $\binom{p}{r} = tp$. چون R مشخصه p دارد،

$$\binom{p}{r}a^{p-r}b^r = tp۱_R a^{p-r}b^r = t(p۱_R)a^{p-r}b^r = t(۰_R)a^{p-r} = ۰_R.$$

بنابراین تمامی جمله‌های میانی صفرند و $(a+b)^p = a^p + b^p$. بنابراین وقتی که $n = ۱$ قضیه درست است.

فرض کنید برای $n = k$ نیز قضیه درست باشد. استفاده از این فرض و حالت $n = ۱$ نشان می‌دهد که

$$(a+b)^{p^{k+۱}} = ((a+b)^{p^k})^p = (a^{p^k} + b^{p^k})^p = (a^{p^k})^p + (b^{p^k})^p = a^{p^{k+۱}} + b^{p^{k+۱}}.$$

بنابراین برای $n = k+۱$ نیز قضیه درست است و بدین دلیل طبق استقراء برای هر n درست است. ■

قضیه ۲۵.۹. گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{Z}_p$ و n عدد صحیح مثبتی باشد. آنگاه $\mathbb{K}$ مرتبه p^n دارد اگر و تنها اگر $\mathbb{K}$ میدان شکافنده $x^{p^n} - x$ روی $\mathbb{Z}_p$ باشد.

برهان[۱۲]. فرض کنید $\mathbb{K}$ میدان شکافنده $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ باشد. چون

۱۱) این اصطلاح منسوب به وین‌سنت‌مک برآین (Vincent O. McBrien) است.

۱۲) با استفاده از نظریه گروهها، برهانی کوتاه در تمرین ۲۲ آمده است.

$f'(x) = p^n x^{p^n-1} - 1 = 0 x^{p^n-1} - 1 = -1$، طبق لم ۱۶.۹، $f(x)$ تفکیک‌پذیر است. گیریم $\mathbb{E}$ زیرمجموعه‌ای از $\mathbb{K}$ متشکل از p^n ریشه متمایز $x^{p^n} - x$ باشد. توجه کنید که $c \in \mathbb{E}$ اگر وتنها اگر $c^{p^n} = c$. نشان خواهیم داد که مجموعه $\mathbb{E}$ در واقع زیرمیدانی از $\mathbb{K}$ است. اگر $a, b \in \mathbb{E}$، آنگاه طبق لم ۲۴.۹،

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b.$$

بنابراین $a + b \in \mathbb{E}$، و $\mathbb{E}$ تحت جمع بسته است. مجموعه $\mathbb{E}$ تحت ضرب بسته است زیرا $(ab)^{p^n} = a^{p^n} b^{p^n} = ab$. به وضوح $0_{\mathbb{K}}$ و $1_{\mathbb{K}}$ در $\mathbb{E}$ هستند. اگر a عضو ناصفری از $\mathbb{E}$ باشد، آنگاه $-a$ و a^{-1} در $\mathbb{E}$ است، زیرا برای مثال

$$(a^{-1})^{p^n} = a^{-p^n} = (a^{p^n})^{-1} = a^{-1}.$$

روش استدلال برای $-a$ مشابه است (تمرین ۷). بنابراین $\mathbb{E}$ یک زیرمیدان $\mathbb{K}$ است. چون میدان شکافنده $\mathbb{K}$ کوچکترین میدان شامل $\mathbb{E}$، مجموعه ریشه‌ها، است باید داشته باشیم $\mathbb{E} = \mathbb{K}$. بنابراین $\mathbb{K}$ مرتبه p^n دارد.

برعکس، فرض کنید $\mathbb{K}$ مرتبه p^n داشته باشد. تنها لازم است نشان دهیم که هر عضو $\mathbb{K}$ ریشه‌ای از $x^{p^n} - x$ است، زیرا در این حالت، p^n عضو متمایز $\mathbb{K}$ تمام ریشه‌های ممکن هستند و $\mathbb{K}$ یک میدان شکافنده $x^{p^n} - x$ است. به وضوح $0_{\mathbb{K}}$ یک ریشه است، بنابراین فرض کنید c هر عضو ناصفر $\mathbb{K}$ باشد. گیریم c_1، c_2، ...، c_k تمام عضوهای ناصفر $\mathbb{K}$ باشند (که در آن $k = p^n - 1$ و c یکی از این c_iها است) و فرض کنید u حاصل‌ضرب، $u = c_1 c_2 c_3 \cdots c_k$ باشد. k عضو cc_1، cc_2، ...، cc_k همگی متمایز هستند (زیرا $cc_i = cc_j$ ایجاب می‌کند $c_i = c_j$)، لذا این k عضو، ترتیب دیگری از همه عضوهای ناصفر $\mathbb{K}$ می‌باشند و حاصل‌ضرب آنها عضو u است. بنابراین

$$u = (cc_1)(cc_2)\cdots(cc_k) = c^k(c_1 c_2 \cdots c_k) = c^k u.$$

حذف u از دو طرف، نشان می‌دهد که $c^k = 1_{\mathbb{K}}$ وبدین دلیل $c^{k+1} = c$ یا به طور معادل، $c^{k+1} - c = 0_{\mathbb{K}}$. چون $k + 1 = p^n$، c ریشه‌ای از $x^{p^n} - x$ است. ■

قضیه ۲۵.۹ نتایج گوناگون مهمی دارد؛ این نتایج همراه با خود قضیه، سرشتنمایی کاملی از تمام میدان‌های متناهی بدست می‌دهد.

نتیجه ۲۶.۹. برای هر عدد اول مثبت p و عدد صحیح n، میدانی از مرتبه p^n وجود دارد.

برهان. طبق قضیه ۱۳.۹ یک میدان شکافنده برای $x^{p^n}-x$ روی $\mathbb{Z}_p$ وجود دارد، طبق قضیه ۲۵.۹ این میدان مرتبه p^n دارد. ■

نتیجه ۲۷.۹. دو میدان متناهی هم‌مرتبه یکریختند.

برهان. اگر $\mathbb{K}$ و $\mathbb{L}$ میدان‌هایی از مرتبه p^n باشند، آنگاه طبق قضیه ۲۵.۹ هر دو، میدان شکافنده $x^{p^n}-x$ روی $\mathbb{Z}_p$ هستند و از اینرو طبق قضیه ۱۴.۹ (وقتی که σ نگاشت همانی روی $\mathbb{Z}_p$ باشد) یکریخت هستند. ■

گاهی میدان یکتای از مرتبه p^n (تا حد یکریختی) را **میدان گالوای مرتبه p^n** نامند. برای یک عدد اول p و نمای n مفروض، می‌توانیم فنون بخش ۵ را بکار بریم تا میدان گالوای مرتبه p^n را بسازیم مشروط به آن که یک چندجمله‌ای تحویل‌ناپذیر $p(x)$ از درجه n در $\mathbb{Z}_p[x]$ بتوانیم پیدا کنیم. در این حالت، طبق قضیه ۹.۵، داریم $\mathbb{K}=\mathbb{Z}_p[x]/(p(x))$. نتیجه ۵.۵ نشان می‌دهد که عناصر $\mathbb{K}$ کلاس‌های متمایز $[r(x)]$ هستند، که در آن $r(x)\in\mathbb{Z}_p[x]$ به صورت $c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ می‌باشد، جایی که $c_i\in\mathbb{Z}_p$. از این که برای هر c_i، p امکان وجود دارد نتیجه می‌شود که $\mathbb{K}$ دارای مرتبه p^n است.

لااقل از جنبه نظری، یافتن چندجمله‌ای تحویل‌ناپذیر درجه n، که ساختار میدان $\mathbb{Z}_p[x]/(p(x))$ از مرتبه n بدان بستگی دارد، کاملاً ساده است. تنها تعدادی متناهی چندجمله‌ای درجهٔ n در $\mathbb{Z}_p[x]$ وجود دارد و هر کدام آن‌ها تعداد باپایانی شمارنده دارد. پس یک چندجمله‌ای خاص را به تعدادی متناهی مرحله می‌توان برای تحویل‌ناپذیری بررسی کرد. این جستجو تنها وقتی ممکن است به شکست بیانجامد که چندجمله‌ای‌های تحویل‌ناپذیراز درجه n در $\mathbb{Z}_p[x]$ موجود نباشد. خواهیم دید که چنین وضعیتی بیش نخواهد آمد. برهان‌های دو نتیجه بعدی بستگی به بخش ۸.۷ دارد.

قضیه ۲۸.۹. گیریم $\mathbb{K}$ میدانی متناهی و $\mathbb{F}$ یک زیرمیدان آن باشد. آنگاه $\mathbb{K}$ یک توسیع با مولد متناهی $\mathbb{F}$ است.

برهان. طبق قضیه ۴۱.۷، گروه ضربی متشکل از عناصر ناصفر $\mathbb{K}$ دوری است. اگر u مولدی از این گروه باشد، آنگاه زیر میدان $\mathbb{F}(u)$، عنصر 0 و تمام توان‌های u را شامل است، و از اینرو هر عضو $\mathbb{K}$ را شامل است. بنابراین $\mathbb{K}=\mathbb{F}(u)$. ■

نتیجه ۲۹.۹. گیریم p یک عدد اول مثبت باشد. برای هر عدد صحیح مثبت n، یک چندجمله‌ای تحویل‌ناپذیر از درجه n در $\mathbb{Z}_p[x]$ وجود دارد.

برهان. طبق نتیجه ۲۶.۹، یک توسیع میدان $\mathbb{K}$ از $\mathbb{Z}_p$ به مرتبه p^n وجود دارد. طبق قضیه ۲۸.۹، برای یک $u \in \mathbb{K}$، $\mathbb{K} = \mathbb{Z}_p(u)$. طبق قضیه ۷.۹، چندجمله‌ای کمین u در $\mathbb{Z}_p[x]$ تحویل‌ناپذیر از درجه $[\mathbb{K} : \mathbb{Z}_p]$ است. قضیه ۲۳.۹ نشان می‌دهد که $n = [\mathbb{K} : \mathbb{Z}_p]$. ■

تمرینها

۱.A. اگر R حلقه‌ای یکدار باشد و $m, n \in \mathbb{Z}$، ثابت کنید که $(m1_R)(n1_R) = (mn)1_R$. [حالت m و n مثبت در برهان لم ۱۹.۹ آمده است.]

۲. مشخصه حلقه‌های زیر چیست؟

(الف) $\mathbb{Q}$ (ب) $\mathbb{Z}_2 \times \mathbb{Z}_6$ (پ) $\mathbb{Z}_3[x]$

(ت) $M(\mathbb{Z}_2)$ (ث) $M(\mathbb{R})$

۳. گیریم R حلقه‌ای یکدار با مشخصه $n > 0$ باشد. ثابت کنید که برای هر $a \in R$، $na = 0_R$.

۴. اگر $\mathbb{K}$ میدانی با مشخصه اول p باشد، ثابت کنید که زیرمیدان اول آن اشتراک تمام زیرمیدان‌های $\mathbb{K}$ است.

۵. گیریم $\mathbb{F}$ زیرمیدانی از یک میدان متناهی $\mathbb{K}$ باشد. اگر $\mathbb{F}$ میدانی از مرتبه q باشد، نشان دهید که $\mathbb{K}$ مرتبه q^n دارد، که در آن $n = [\mathbb{K} : \mathbb{F}]$.

۶. نشان دهید که میدانی از مرتبه p^n تمام ریشه‌های k ام را شامل است، جایی‌که $k = p^n - 1$.

۷. گیریم $\mathbb{E}$ مجموعه ریشه‌های $x^{p^n} - x \in \mathbb{Z}_p[x]$ در یک میدان شکافنده باشد. اگر $a \in \mathbb{E}$، ثابت کنید که $-a \in \mathbb{E}$.

۸.B. گیریم p اول باشد و $\mathbb{Z}_p(x)$ میدان خارج‌قسمتهای حلقه چندجمله‌ای‌های $\mathbb{Z}_p[x]$ (همان‌طور که در مثال ۱۹.۸ آمده است) باشد. نشان دهید که $\mathbb{Z}_p(x)$ میدانی نامتناهی با مشخصه p است.

۹. گیریم R حلقه‌ای جابجایی و یکدار با مشخصه اول p باشد اگر $a, b \in R$ و $n \geq 1$، ثابت کنید که $(a - b)^{p^n} = a^{p^n} - b^{p^n}$.

۱۰. گیریم $\mathbb{K}$ میدانی متناهی با مشخصه p باشد. ثابت کنید که نگاشت $f : \mathbb{K} \to \mathbb{K}$ تعریف شد با $f(a) = a^p$ یک یکریختی است. نتیجه بگیرید که هر عضو $\mathbb{K}$ یک ریشه p ام در $\mathbb{K}$ دارد.

۱۱. نشان دهید که رویای سال‌اولی‌ها (لم ۲۴.۹) در صورتی که مشخصه اول نباشد یا اگر R غیرجابجایی باشد ممکن است غلط باشد. [راهنمایی: $\mathbb{Z}_۴$ و $M(\mathbb{Z}_۲)$ را در نظر بگیرید.]

۱۲. اگر c ریشه‌ای از $f(x) \in \mathbb{Z}_p[x]$ باشد. ثابت کنید که c^p نیز یک ریشه است.

۱۳. **قضیه کوچک فرما** را ثابت کنید: اگر p اول و $a \in \mathbb{Z}$، آنگاه (پیمانه p) $a^p \equiv a$. اگر a نسبت به p اول باشد، آنگاه (پیمانه p) $a^{p-۱} \equiv ۱$. [راهنمایی: گزاره‌های همنهشتی در $\mathbb{Z}$ را به گزاره‌های برابری در $\mathbb{Z}_p$ ترجمه کنید و قضیه ۲۵.۹ را بکار برید.]

۱۴. گیریم $\mathbb{F}$ یک میدان و $f(x)$ یک چندجمله‌ای تکین در $\mathbb{F}[x]$ باشد، که همه ریشه‌هایش در هر میدان شکافنده $\mathbb{K}$ متمایزند. گیریم $\mathbb{E}$ مجموعه ریشه‌های $f(x)$ در $\mathbb{K}$ باشد. اگر مجموعه $\mathbb{E}$ به واقع زیرمیدانی از $\mathbb{K}$ باشد، ثابت کنید که برای یک عدد اول p، $\mathbb{F}$ مشخصه p دارد و این که برای یک $n \geq ۱$، $f(x) = x^{p^n} - x$.

۱۵. (الف) نشان دهید که $x^۳ + x + ۱$ در $\mathbb{Z}_۳[x]$ تحویل‌ناپذیر است و میدانی از مرتبه ۸ بسازید.
(ب) نشان دهید که $x^۳ - x + ۱$ در $\mathbb{Z}_۳[x]$ تحویل‌ناپذیر است و میدانی از مرتبه ۲۷ بسازید.
(پ) نشان دهید که $x^۴ + x + ۱$ در $\mathbb{Z}_۲[x]$ تحویل‌ناپذیر است و میدانی از مرتبه ۱۶ بسازید.

۱۶. گیریم $\mathbb{K}$ میدانی متناهی با مشخصه p، $\mathbb{F}$ زیرمیدانی از $\mathbb{K}$ و m یک عدد صحیح مثبت باشد. اگر $\mathbb{L} = \{a \in \mathbb{K} : a^{p^n} \in \mathbb{F}\}$، ثابت کنید که $\mathbb{L} = \mathbb{F}$. [راهنمایی: اگر $u_۱$، ...، u_n یک پایه $\mathbb{L}$ روی $\mathbb{F}$ باشد از تمرین ۱۰ و لم ۲۴.۹ استفاده کنید تا نشان دهید که $u_۱^{p^m}$، ...، $u_n^{p^m}$ روی $\mathbb{F}$ مستقل خطی است، که ایجاب می‌کند $n = ۱$.]

۱۷. اگر $\mathbb{E}$ و $\mathbb{F}$ زیرمیدان‌های یک میدان متناهی $\mathbb{K}$ و $\mathbb{E}$ یکریخت با $\mathbb{F}$ باشد ثابت کنید که $\mathbb{E} = \mathbb{F}$.

۱۸. گیریم $\mathbb{K}$ یک میدان و k، n اعداد صحیح مثبت باشند.
(الف) ثابت کنید که $x^k - ۱_{\mathbb{K}}$، $x^n - ۱_{\mathbb{K}}$ را در $\mathbb{K}[x]$ می‌شمارد اگر و تنها اگر در $\mathbb{Z}$، $k|n$. [راهنمایی: طبق الگوریتم تقسیم $n = kq + r$، ثابت کنید که $x^n - ۱_{\mathbb{K}} = (x^k - ۱_{\mathbb{K}})h(x) + (x^r - ۱_{\mathbb{K}})$

که در آن $h(x) = x^{n-k} + x^{n-2k} + \cdots + x^{n-qk}$.]

(ب) اگر $p \geq 2$ یک عدد صحیح باشد، ثابت کنید که $(p^k - 1) | (p^n - 1)$ اگر و تنها اگر $k|n$. [راهنمایی: برهان قسمت (الف) را با جایگزینی p بجای x تکرار کنید.]

۱۹. گیریم $\mathbb{K}$ میدانی متناهی از مرتبه p^n باشد.

(الف) اگر $\mathbb{F}$ زیرمیدانی از $\mathbb{K}$ باشد، ثابت کنید که برای یک d که $d|n$، $\mathbb{F}$ مرتبه p^d دارد. [راهنمایی: تمرین ۱۸ می‌تواند مفید باشد.]

(ب) اگر $d|n$، ثابت کنید که $\mathbb{K}$ زیرمیدان یکتایی از مرتبه p^d دارد. [برای قسمت یکتایی، تمرین ۱۷ و نتیجه ۲۷.۹ را ملاحظه کنید.]

۲۰. گیریم p عددی اول باشد و $f(x)$ یک چندجمله‌ای تحویل‌ناپذیر از درجه ۲ در $\mathbb{Z}_p[x]$ باشد. اگر $\mathbb{K}$ یک توسیع میدان $\mathbb{Z}_p$ از مرتبه p^3 باشد، نشان دهید که $f(x)$ در $\mathbb{K}[x]$ تحویل‌ناپذیر است.

۲۱. ثابت کنید که هر عضو در یک میدان متناهی را می‌توان به صورت مجموع دو مربع نوشت.

۲۲. با استفاده از قسمت (۲) نتیجه ۳.۷ ثابت کنید که هر عنصر ناصفر یک میدان متناهی $\mathbb{K}$ از مرتبه p^n در $c^{p^n-1} = 1_{\mathbb{K}}$ صدق می‌کند. نتیجه بگیرید که c ریشه‌ای از $x^{p^n} - x$ است و از این واقعیت استفاده کنید تا قضیه ۲۵.۹ را ثابت کنید.

* * * * *

فصل دهم

مباحثی در نظریه گروه

فصل حاضر نظر ژرفتری به جنبه‌های گوناگون مسئله رده‌بندی گروههای متناهی، که در بخش ۸.۷ معرفی شد، دارد. پس از مقدمات لازم که در بخش ۱.۱۰ بسط و توسعه می‌یابد، تمام گروههای آبلی در بخش ۲.۱۰ (قضیه اساسی گروههای آبلی) تا حد یکریختی رده‌بندی می‌شود. گروههای غیرآبلی به طور قابل ملاحظه‌ای پیچیده هستند. ابزارهای مبنایی برای تجزیه و تحلیل آنها (قضایا سیلو) و بعضی کاربردها در بخش‌های ۳.۱۰ و ۴.۱۰ ارائه می‌شوند. همانگونه که در بخش ۸.۷ تذکر داده شده است معلوم می‌شود که گروههای ساده کلید حل مسئله رده‌بندی می‌باشند. در بخش ۵.۱۰، رده بزرگی از گروههای غیرآبلی (گروههای تناوبی، با شرط $n > ۴$) را عرضه می‌کنیم.

بخش ۱.۱۰ پیشنیاز بخش ۲.۱۰ و قسمت آخر بخش ۳.۱۰ است. ولی بخش‌های ۲.۱۰ تا ۵.۱۰ مستقل از یکدیگرند و می‌توانند به ترتیب دلخواه مطالعه شوند.

۱۰-۱ ضرب‌های مستقیم

اگر G و H گروه باشند، آنگاه حاصل‌ضرب دکارتی آن‌ها $G \times H$ نیز یک گروه است، که عمل آن مؤلفه به مؤلفه تعریف می‌شود (قضیه ۱.۷). در این بخش این مفهوم را به بیشتر از دو گروه تعمیم می‌دهیم. آنگاه شرایطی که تحت آنها یک گروه (یکریخت با) حاصل‌ضربی از زیرگروههای معینی از خودش می‌باشد را می‌آزماییم. وقتی این گروهها از نوع ساده بخصوصی باشند، در این صورت ساختار گروه را به طور کامل می‌توان تعیین کرد، همانگونه که در بخش ۲.۱۰ آمده است. در سراسر مبحث کلی تمام گروهها به صورت ضربی نوشته شده‌اند، ولی مثال‌های مشخص از گروههای جمعی به طور معمول به صورت جمعی نوشته می‌شوند.

اگر G_1، G_2، ...، G_n گروه باشند، عملی مولفه به مولفه روی حاصلضرب دکارتی $G_1 \times G_2 \times \cdots \times G_n$ تعریف می‌کنیم:

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

بررسی این که $G_1 \times G_2 \times \cdots \times G_n$ تحت این عمل یک گروه می‌باشد ساده است: اگر e_i عضو همانی G_i باشد، آنگاه $(e_1, e_2, \ldots, e_n)$ عضو همانی $G_1 \times G_2 \times \cdots \times G_n$ است و $(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$ وارون $(a_1, a_2, \ldots, a_n)$ است. این گروه **حاصل‌ضرب مستقیم** G_1، G_2، ...، G_n نامیده می‌شود[1].

مثال ۱.۱۰. بخاطر آورید که U_n گروه ضربی یکه‌های $\mathbb{Z}_n$ است و این که $U_4 = \{1, 3\}$ و $U_6 = \{1, 5\}$. حاصل‌ضرب $U_4 \times U_6 \times \mathbb{Z}_3$ متشکل از ۱۲ سه تایی است:

$$(1,1,0), (1,1,1), (1,1,2), (1,5,0), (1,5,1), (1,5,2)$$
$$(3,1,0), (3,1,1), (3,1,2), (3,5,0), (3,5,1), (3,5,2)$$

توجه کنید که U_4 مرتبه ۲، U_6 مرتبه ۲ و $\mathbb{Z}_3$ مرتبه سه دارد و حاصل‌ضرب مستقیم $U_4 \times U_6 \times \mathbb{Z}_3$ دارای مرتبه $12 = 3 \times 2 \times 2$ است. به طور مشابه، در حالت کلی،

اگر G_1، G_2، ...، G_n گروههای متناهی باشند، آنگاه

$G_1 \times G_2 \times \cdots \times G_n$ دارای مرتبه $|G_1| \times |G_2| \times \cdots \times |G_n|$ است.

۱) وقتی که هر G_i یک گروه آبلی جمعی است، حاصل‌ضرب مستقیم G_1، ...، G_n گاهی **جمع مستقیم** نامیده می‌شود و به صورت $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ نشان داده می‌شود.

در مثال قبلی توجه به این نکته مهم است که هیچ یک از $U_۴$، $U_۶$، و $\mathbb{Z}_۳$ مشمول در حاصل‌ضرب مستقیم $U_۴ \times U_۶ \times \mathbb{Z}_۳$ نیست. برای مثال ۵ عضوی از $U_۶$ است، ولی ۵ در $U_۴ \times U_۶ \times \mathbb{Z}_۳$ نیست زیرا عضوهای $U_۴ \times U_۶ \times \mathbb{Z}_۳$ سه‌تایی‌ها هستند، در حالت کلی، برای $۱ \leq i \leq n$

G_i زیرگروه حاصل‌ضرب مستقیم $G_۱ \times G_۲ \times \cdots \times G_n$ نیست.

این وضعیت چندان مطلوب نیست، ولی با تغییر دیدگاه خود، به طور نسبی می‌توانیم یک مفهوم از حاصل‌ضرب مستقیم را بسط و توسعه دهیم که در آن گروههای مؤلفه می‌تواند به عنوان زیرگروه در نظر گرفته شود.

مثال ۱۰.۲. تحقیق این که $M = \{۰, ۳\}$ و $N = \{۰, ۲, ۴\}$ زیرگروههای نرمال $\mathbb{Z}_۶$ هستند، ساده است (این کار را انجام دهید). مشاهده می‌کنید که هر عضو $\mathbb{Z}_۶$ را تنها به یک طریق می‌توان به صورت مجموع یک عضو از M و یک عضو از N نوشت:

$$۰ = ۰ + ۰ \qquad ۱ = ۳ + ۴ \qquad ۲ = ۰ + ۲$$
$$۳ = ۳ + ۰ \qquad ۴ = ۰ + ۴ \qquad ۵ = ۳ + ۲$$

تحقیق کنید که وقتی عضوهای $\mathbb{Z}_۶$ بدین طریق به صورت جمع نوشته شود، آنگاه جدول جمع $\mathbb{Z}_۶$ به صورت زیر در می‌آید:

	۰ + ۰	۳ + ۴	۰ + ۲	۳ + ۰	۰ + ۴	۳ + ۲
۰ + ۰	۰ + ۰	۳ + ۴	۰ + ۲	۳ + ۰	۰ + ۴	۳ + ۲
۳ + ۴	۳ + ۴	۰ + ۲	۳ + ۰	۰ + ۴	۳ + ۲	۰ + ۰
۰ + ۲	۰ + ۲	۳ + ۰	۰ + ۴	۳ + ۲	۰ + ۰	۳ + ۴
۳ + ۰	۳ + ۰	۰ + ۴	۳ + ۲	۰ + ۰	۳ + ۴	۰ + ۲
۰ + ۴	۰ + ۴	۳ + ۲	۰ + ۰	۳ + ۴	۰ + ۲	۳ + ۰
۳ + ۲	۳ + ۲	۰ + ۰	۳ + ۴	۰ + ۲	۳ + ۰	۰ + ۴

جدول $\mathbb{Z}_۶$ را با جدول عمل حاصل‌ضرب مستقیم $M \times N$ مقایسه کنید:

	$(0,0)$	$(3,4)$	$(0,2)$	$(3,0)$	$(0,4)$	$(3,2)$
$(0,0)$	$(0,0)$	$(3,4)$	$(0,2)$	$(3,0)$	$(0,4)$	$(3,2)$
$(3,4)$	$(3,4)$	$(0,2)$	$(3,0)$	$(0,4)$	$(3,2)$	$(0,0)$
$(0,2)$	$(0,2)$	$(3,0)$	$(0,4)$	$(3,2)$	$(0,0)$	$(3,4)$
$(3,0)$	$(3,0)$	$(0,4)$	$(3,2)$	$(0,0)$	$(3,4)$	$(0,2)$
$(0,4)$	$(0,4)$	$(3,2)$	$(0,0)$	$(3,4)$	$(0,2)$	$(3,0)$
$(3,2)$	$(3,2)$	$(0,0)$	$(3,4)$	$(0,2)$	$(3,0)$	$(0,4)$

تنها تفاوت این دو جدول این است که هر عضو در اولی به صورت $a+b$ و در دومی به صورت (a,b) نوشته شده‌است. به‌علاوه، این جداول نشان می‌دهد که حاصل‌ضرب مستقیم $M \times N$ تحت یکریختی‌ای که زوج $(a,b) \in M \times N$ را به مجموع مختصاتش $a+b \in \mathbb{Z}_۶$ نظیر می‌کند با $\mathbb{Z}_۶$ یکریخت است. در نتیجه می‌توانیم $\mathbb{Z}_۶$ را، بدون در نظر گرفتن $M \times N$، که نسبت به $\mathbb{Z}_۶$ جنبه خارجی دارد به صورت حاصل‌ضربی مستقیم در سیمایی صرفاً داخلی بیان کنیم: هر عضو را به طور یکتایی به صورت یک مجموع $a+b$ بنویسید، که $a \in M$ و $b \in N$. اکنون، با جایگزینی نشان ضربی بجای جمع در $\mathbb{Z}_۶$، همین مفهوم را در حالت کلی بسط و توسعه می‌دهیم.

قضیه ۱.۱۰. گیریم $N_۱$، $N_۲$، ...، N_k زیرگروههای نرمال یک گروه G باشند به طوری که هر عضو G را بتوان به طور یکتایی به صورت $a_۱a_۲\cdots a_k$ نوشت، که در آن $a_i \in N_i$ [۲]. آنگاه G یکریخت با حاصل‌ضرب مستقیم $N_۱ \times N_۲ \times \cdots \times N_k$ است.

برهان قضیه بستگی به این واقعیت سودمند دارد:

لم ۲.۱۰. گیریم M و N زیرگروههای نرمال G باشند به طوری که $M \cap N = < e >$. اگر $a \in M$ و $b \in N$، آنگاه $ab = ba$.

برهان. $a^{-۱}b^{-۱}ab$ را در نظر بگیرید. چون M نرمال است طبق قضیه ۲۱.۷، $b^{-۱}ab \in M$، بسته بودن M نشان می‌دهد $a^{-۱}b^{-۱}ab = a^{-۱}(b^{-۱}ab) \in M$. به طور مشابه نرمال بودن N ایجاب می‌کند که $a^{-۱}b^{-۱}a \in N$ و بدین دلیل $a^{-۱}b^{-۱}ab = (a^{-۱}b^{-۱}a)b \in N$. بنابراین $a^{-۱}b^{-۱}ab \in M \cap N = < e >$. ضرب طرفین $a^{-۱}b^{-۱}ab = e$ در ba از طرف چپ، نشان

۲) یکتایی به معنی آن است که اگر $a_۱a_۲\cdots a_k = b_۱b_۲\cdots b_k$ که در آن $a_i, b_i \in N_i$، آنگاه برای هر i، $a_i = b_i$.

می‌دهد که $ab = ba$. ■

برهان قضیه ۱.۱۰. با الهام از مثال قبل از قضیه (البته با استفاده از نشان ضربی) نگاشت $f : N_1 \times N_2 \times \cdots \times N_k \to G$ با ضابطه $f(a_1, a_2, \ldots, a_k) = a_1 a_2 \cdots a_k$ را تعریف می‌کنیم. چون بنابر فرض، هر عضو G را می‌توان به صورت $a_1 a_2 \ldots a_k$ (با شرط $a_i \in N_i$) نوشت، f پوشاست. اگر $f(a_1, a_2, \ldots, a_k) = f(b_1, b_2, \ldots, b_k)$ آنگاه $a_1 a_2 \ldots a_k = b_1 b_2 \ldots b_k$. بنابر فرض یکتایی، برای هر $i (1 \le i \le k)$، $a_i = b_i$. بنابراین در $N_1 \times N_2 \times \cdots \times N_k$، $(a_1, a_2, \ldots, a_k) = (b_1, b_2, \ldots, b_k)$ و f یک به یک است.

برای آن که ثابت کنیم f یک همریختی است باید نشان دهیم که N_iها زیرگروههای دوبه‌دو نسبت به‌هم مجزا هستند، یعنی وقتی $i \neq j$، $N_i \cap N_j =< e >$. اگر $a \in N_i \cap N_j$، آنگاه a را می‌توان به صورت حاصل‌ضربی از عضوهای N_iها به دو طریق متفاوت نوشت:

$$\underset{\uparrow N_1}{e} \cdots \underset{\uparrow N_i}{e\, a\, e} \cdots \underset{\uparrow N_j}{e} \cdots \underset{\uparrow N_k}{e} = a = \underset{\uparrow N_1}{e} \cdots \underset{\uparrow N_i}{e} \cdots \underset{\uparrow N_j}{e\, a\, e} \cdots \underset{\uparrow N_k}{e}$$

فرض یکتایی ایجاب می‌کند که مولفه‌های واقع در N_i باید برابر باشند: $a = e$. بنابراین برای $i \neq j$، $N_i \cap N_j =< e >$. این واقعیت همراه با لم ۲.۱۰، ایجاب می‌کند که برای $a_i \in N_i$ و $b_j \in N_j$، $a_i b_j = b_j a_i$. اینک با استفاده مکرر از این حقیقت نشان می‌دهیم که f یک همریختی است:

$$\begin{aligned} f[(a_1, \ldots, a_k)(b_1, \ldots, b_k)] &= f(a_1 b_1, \ldots, a_k b_k) \\ &= a_1 b_1 a_2 b_2 a_3 b_3 \cdots a_k b_k \\ &= a_1 a_2 b_1 b_2 a_3 b_3 \cdots a_k b_k \\ &= a_1 a_2 b_1 a_3 b_2 b_3 \cdots a_k b_k \\ &= a_1 a_2 a_3 b_1 b_2 b_3 \cdots a_k b_k. \end{aligned}$$

با ادامه این فرآیند، متوالیاً a_2، a_3، ...، a_k را به طرف چپ حرکت می‌دهیم تا بدست آوریم

$$\begin{aligned} f[(a_1, \ldots, a_k)(b_1, \ldots, b_k)] &= (a_1 a_2 \cdots a_k)(b_1 b_2 \cdots b_k) \\ &= f(a_1, \ldots, a_k) f(b_1, \ldots, b_k) \end{aligned}$$

بنابراین f یک همریختی است و بدین دلیل یک یکریختی است. ■

وقتی G یک گروه و N_1، ...، N_k زیرگروههایی باشند که در شرایط قضیه ۱.۱۰ صدق می‌کنند، گوییم G **حاصل‌ضرب مستقیم** N_1، ...، N_k است و می‌نویسیم $G = N_1 \times N_2 \times \cdots \times N_k$. هر N_i **یک عامل مستقیم** G نامیده می‌شود. بسته به موقعیت، می‌توان G را به صورت حاصل‌ضرب مستقیم خارجی N_iها (هر عضو یک k-تایی $(a_1, a_2, \ldots, a_k) \in N_1 \times \cdots \times N_k$) در نظر گرفت یا به صورت حاصل‌ضرب مستقیم *داخلی* (هر عضو به طور یکتایی به صورت $a_1 a_2 \ldots a_k \in G$ نوشته شود) در نظر گرفت.

برای این که ثابت کنیم که یک گروه حاصل‌ضرب مستقیم زیرگروههای معینی از خودش می‌باشد استفاده از قضیه بعد اغلب ساده‌تر از قضیه ۱.۱۰ می‌باشد. در صورت قضیه بعد از این نماد استفاده می‌شود که اگر M و N زیرگروههای گروه G باشند، آنگاه MN مجموعه تمام حاصل‌ضرب‌های mn را نشان می‌دهد که در آن $m \in M$ و $n \in N$.

قضیه ۳.۱۰. اگر M و N زیرگروههای نرمال یک گروه G باشند به طوری که $G = MN$ و $M \cap N = \langle e \rangle$، آنگاه $G = M \times N$.

برای حالت بیش از دو زیرگروه، تمرین ۲۵ را ملاحظه کنید.

برهان قضیه ۳.۱۰. طبق فرض هر عضو G به صورت mn است، که در آن $m \in M$، $n \in N$. فرض کنید که یک عضو دارای دو نمایش مثلاً $mn = m_1 n_1$ باشد، که در آن $m, m_1 \in M$ و $n, n_1 \in N$. آنگاه ضرب طرفین از طرف چپ در m_1^{-1} و از طرف راست در n^{-1} نشان می‌دهد که $m_1^{-1} m = n_1 n^{-1}$. ولی $m_1^{-1} m \in M$، $n_1 n^{-1} \in N$ و $M \cap N = \langle e \rangle$. بدین دلیل $m_1^{-1} m = e$ و $m = m_1$؛ به طور مشابه $n = n_1$. بنابراین هر عضو G را می‌توان به طور یکتایی به صورت $mn (n \in N, m \in M)$ نوشت، و از اینرو طبق قضیه ۱.۱۰، $G = M \times N$. ■

مثال ۳.۱۰. گروه ضربی یکه‌های $\mathbb{Z}_{15}$، $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ می‌باشد. گروههای $M = \{1, 11\}$ و $N = \{1, 2, 4, 8\}$ در U_{15} نرمال هستند و اشتراک آن‌ها $\langle 1 \rangle$ است. هر عضو N در MN است (برای مثال $2 = 1 \times 2$) و به طور مشابه برای M چنین است.

چون $۷ = ۲ \times ۱۱$، $۱۳ = ۸ \times ۱۱$، و $۱۴ = ۴ \times ۱۱$، می‌بینیم که $U_{۱۵} = MN$. بنابراین طبق قضیه ۳.۱۰، $U_{۱۵} = M \times N$. چون N دوری از مرتبه ۲ و M دوری از مرتبه ۴ است (۲ یک مولد است)، نتیجه می‌گیریم که $U_{۱۵}$ یکریخت با $\mathbb{Z}_۲ \times \mathbb{Z}_۴$ است (تمرین ۱۰ و قضیه ۱۳.۷ را نگاه کنید).

تمرینها

تذکر: $G_۱$، ...، G_n گروه هستند، مگر خلاف آن بیان شود.

A.۱. مرتبه هر عضو را در گروه داده شده پیدا کنید.

(الف) $\mathbb{Z}_۲ \times \mathbb{Z}_۴$ (ب) $\mathbb{Z}_۳ \times \mathbb{Z}_۳ \times \mathbb{Z}_۲$ (پ) $D_۴ \times \mathbb{Z}_۲$.

۲. مرتبه گروه $U_۵ \times U_۶ \times U_۷ \times U_۸$ چند است؟

۳. (الف) تمام زیرگروههای $\mathbb{Z}_۲ \times \mathbb{Z}_۲$ را فهرست کنید.

(ب) همین کار را برای $\mathbb{Z}_۲ \times \mathbb{Z}_۲ \times \mathbb{Z}_۲$ انجام دهید.

۴. اگر G و H گروه باشد، ثابت کنید $G \times H \cong H \times G$.

۵. مثالی بزنید تا نشان دهید که حاصل‌ضرب گروههای دوری لازم نیست که دوری باشد.

۶. (الف) $\mathbb{Z}_{۱۲}$ را به صورت حاصل‌ضرب مستقیم دو تا از زیرگروههایش بنویسید.

(ب) همین کار را برای $\mathbb{Z}_{۱۵}$ انجام دهید.

(پ) $\mathbb{Z}_{۳۰}$ را به سه طریق مختلف به صورت دو یا بیشتر از دو زیرگروه آن بنویسید [راهنمایی: قضیه ۳.۱۰.]

۷. گیریم $G_۱$، ...، G_n گروه باشند. ثابت کنید که $G_۱ \times \cdots \times G_n$ آبلی است اگر و تنها اگر هر G_i آبلی باشد.

۸. گیریم i عدد صحیحی باشد که $۱ \leq i \leq n$. ثابت کنید که تابع

$$\pi_i : G_۱ \times G_۲ \times \cdots \times G_n \to G_i$$

که توسط $\pi_i(a_۱, a_۲, \ldots, a_n) = a_i$ تعریف می‌شود، یک همریختی پوشای گروهی است.

۹. آیا $\mathbb{Z}_8$ یکریخت با $\mathbb{Z}_4 \times \mathbb{Z}_2$ است؟

B ۱۰. (الف) اگر $f : G_1 \to H_1$ و $g : G_2 \to H_2$ یکریختی‌های گروهی باشند، ثابت کنید که نگاشت $\theta : G_1 \times G_2 \to H_1 \times H_2$ که توسط $\theta(a, b) = (f(a), g(b))$ داده شده است، یک یکریختی است.

(ب) اگر برای هر $i = 1, 2, \ldots, n$، $G_i \cong H_i$ ثابت کنید که

$$G_1 \times \cdots \times G_n \cong H_1 \times \cdots \times H_n$$

۱۱. گیریم H، K، M و N گروه‌هایی باشند که $K \cong M \times N$. ثابت کنید که $H \times K \cong H \times M \times N$.

۱۲. گیریم i عدد صحیحی باشد که $1 \leq i \leq n$. گیریم G_i^* زیرمجموعه $G_1 \times \cdots \times G_n$ متشکل از آن عناصری باشد که i امین مؤلفه‌اش عنصر دلخواهی از G_i است و مؤلفه‌های دیگرش هرکدام عضو همانی باشد، یعنی،

$$G_i^* = \{(e_1, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots e_n) \mid a_i \in G_i\}$$

ثابت کنید که

(الف) G_i^* زیرگروهی نرمال از $G_1 \times \cdots \times G_n$ است.

(ب) $G_i^* \cong G_i$.

(پ) $G_1 \times \cdots \times G_n$ حاصل‌ضرب داخلی زیرگروههای G_1^*، ...، G_n^* می‌باشد. [راهنمایی: نشان دهید که هر عضو $G_1 \times \cdots \times G_n$ را می‌توان به طور یکتایی به صورت $a_1 a_2 \cdots a_n$ نوشت که در آن $a_i \in G_i^*$، قضیه ۱.۱۰ را بکار برید.]

۱۳. گیریم G یک گروه باشد و $D = \{(a, a, a) \mid a \in G\}$

(الف) ثابت کنید که D زیرگروهی از $G \times G \times G$ است.

(ب) ثابت کنید که D در $G \times G \times G$ نرمال است اگر و تنها اگر G آبلی باشد.

۱۴. اگر G_1، ...، G_n گروههای متناهی باشند، ثابت کنید که مرتبه $(a_1, a_2, \ldots, a_n)$ در $G_1 \times \cdots \times G_n$ کوچکترین مضرب مشترک مرتبه‌های $|a_1|$، $|a_2|$، ...، $|a_n|$ است.

۱۵. گیریم i_1، i_2، ...، i_n جایگشتی از اعداد صحیح ۱، ۲، ...، n باشد. ثابت کنید که $G_1 \times G_2 \times \cdots \times G_n$ با $G_{i_1} \times G_{i_2} \times \cdots \times G_{i_n}$ یکریخت است. [تمرین ۴ حالت $n = 2$ است.]

۱۶. اگر N و K زیرگروههای یک گروه G باشند که $G = N \times K$ و M یک زیرگروه نرمال N باشد، ثابت کنید که M یک زیرگروه نرمال G است. [این تمرین را با تمرین ۱۳ بخش ۵.۷ مقایسه کنید.]

۱۷. گیریم $\mathbb{Q}^*$ گروه ضربی اعداد گویای ناصفر، $\mathbb{Q}^{**}$ زیرگروه اعداد گویای مثبت، و H زیرگروه $\{1, -1\}$ باشد. ثابت کنید که $Q^* = \mathbb{Q}^{**} \times H$.

۱۸. گیریم $\mathbb{C}^*$ گروه ضربی اعداد مختلط ناصفر و $\mathbb{R}^{**}$ گروه ضربی اعداد حقیقی مثبت باشد. ثابت کنید که $\mathbb{C}^* \cong \mathbb{R}^{**} \times \mathbb{R}/\mathbb{Z}$ که در آن $\mathbb{R}$ گروه جمعی اعداد حقیقی است.

۱۹. گیریم G یک گروه و $f_1 : G \to G_1$، $f_2 : G \to G_2$، ...، $f_n : G \to G_n$ همریختی باشند. برای $i = 1, 2, \ldots, n$، گیریم π_i همریختی تمرین ۸ باشد. گیریم $f^* : G \to G_1 \times \cdots \times G_n$ نگاشت تعریف شده با ضابطه $f^*(a) = (f_1(a), \ldots, f_n(a))$ باشد.

(الف) ثابت کنید که f^* یک همریختی است به قسمی که برای هر i، $\pi_i \circ f^* = f_i$.

(ب) ثابت کنید که f^* تنها همریختی از G به $G_1 \times \cdots \times G_n$ است که برای هر i، $\pi_i \circ f^* = f_i$.

۲۰. گیریم N_1، ...، N_k زیرگروههای یک گروه آبلی G باشند. فرض کنید هر عضو G را بتوان به صورت $a_1 a_2 \cdots a_k$ نوشت (که در آن $a_i \in N_i$) و این که وقتی $a_1 a_2 \cdots a_n = e$، آنگاه برای هر i، $a_i = e$. ثابت کنید که $G = N_1 \times N_2 \times \cdots \times N_k$.

۲۱. گیریم G یک گروه آبلی جمعی با زیرگروههای H و K باشد. ثابت کنید که $G = H \times K$ اگر و تنها اگر همریختی‌های

$$H \underset{\delta_1}{\overset{\pi_1}{\rightleftarrows}} G \underset{\delta_2}{\overset{\pi_2}{\rightleftarrows}} K$$

وجود داشته باشد به طوری که برای هر $x \in G$، $\delta_1(\pi_1(x)) + \delta_2(\pi_2(x)) = x$ و $\pi_1 \circ \delta_1 = \iota_H$، $\pi_2 \circ \delta_2 = \iota_K$، $\pi_1 \circ \delta_2 = 0$ و $\pi_2 \circ \delta_1 = 0$ که در آن ι_X نگاشت همانی

روی X، و $\circ$ نگاشتی است که هر عضو را به عضو $\circ$ (همانی) می‌فرستد. [راهنمایی: π_i را مانند تمرین ۸ در نظر بگیرید.]

۲۲. گیریم G و H گروههای دوری متناهی باشند. ثابت کنید که $G \times H$ دوری است اگر و تنها اگر $(|G|, |H|) = ۱$.

۲۳. (الف) با مثال نشان دهید که اگر N نرمال نباشد لم ۲.۱۰ ممکن است نادرست باشد. (ب) همین کار را برای قضیه ۳.۱۰ انجام دهید.

۲۴. گیریم N و K زیرگروههای یک گروه G باشند و N در G نرمال باشد. اگر N و K گروههای آبلی و $G = NK$، آیا G حاصل‌ضرب مستقیم N و K است؟

۲۵. گیریم $N_۱$، ...، N_k زیرگروههای نرمال یک گروه G باشند، گیریم $N_۱N_۲\cdots N_k$ مجموعهٔ تمام عضوهایی به صورت $a_۱a_۲\cdots a_k$ را نشان دهد که در آن $a_j \in N_j$. فرض کنید که $G = N_۱N_۲\cdots N_k$ و این که برای هر $i (۱ \leq i \leq n)$،

$$N_i \cap N_۱\cdots N_{i-۱}N_{i+۱}\cdots N_k =< e >.$$

ثابت کنید که $G = N_۱ \times N_۲ \times \cdots \times N_k$.

۲۶. گیریم $N_۱$، ...، N_k زیرگروه‌های نرمال یک گروه متناهی G باشند. اگر $G = N_۱N_۲\cdots N_k$ (نماد مانند آنچه در تمرین ۲۵ آمده است می‌باشد) و $|G| = |N_۱| \times |N_۲| \times \cdots \times |N_k|$، ثابت کنید که $G = N_۱ \times N_۲ \times \cdots \times N_k$.

۲۷. گیریم N و H زیرگروههای یک گروه G باشند. G را **حاصل‌ضرب نیم‌مستقیم** N و H گویند اگر N در G نرمال باشد، $G = NH$ و $N \cap H =< e >$. نشان دهید که هر کدام از گروههای زیر حاصل‌ضرب نیم‌مستقیم دوتا از زیرگروههای خودش می‌باشد.

(الف) $S_۳$ (ب) $D_۴$ (پ) $\mathbb{Z}$

۲۸. یک گروه را **تجزیه‌ناپذیر** گویند، اگر حاصل‌ضرب مستقیم هیچ دوتا از زیرگروههای سره‌اش نباشد. ثابت کنید که هر کدام از این گروهها تجزیه‌ناپذیر است.

(الف) $S_۳$ (ب) $D_۴$ (پ) $\mathbb{Z}$

۲۹. اگر p عددی اول و n یک عدد صحیح مثبت باشد، ثابت کنید که $\mathbb{Z}_{p^n}$ تجزیه‌ناپذیر است.

۳۰. ثابت کنید که $\mathbb{Q}$ یک گروه تجزیه‌ناپذیر است.

۳۱. با ذکر مثال نشان دهید که تصویر همریختی یک گروه تجزیه‌ناپذیر لازم نیست تجزیه‌ناپذیر باشد.

۳۲. ثابت کنید که یک گروه G تجزیه‌ناپذیر است اگر و تنها اگر وقتی H و K زیرگروههای نرمال G باشند و $G = H \times K$، آنگاه $H =< e >$ یا $K =< e >$.

۳۳. گیریم I مجموعه اعداد صحیح مثبت باشد و فرض کنید که برای هر $i \in I$، G_i یک گروه باشد[۳]. **حاصل‌ضرب مستقیم نامتناهی** این G_iها با $\Pi_{i\in I}G_i$ نشان داده می‌شود و متشکل از تمام دنباله‌های $(a_1, a_2, \dots)$، با شرط $a_i \in G_i$، می‌باشد. ثابت کنید که $\Pi_{i\in I}G_i$، تحت عمل مؤلفه به مولفه

$$(a_1, a_2, \dots)(b_1, b_2, \dots) = (a_1b_1, b_2b_2, \dots)$$

یک گروه می‌باشد.

۳۴.C. با نمادهای تمرین ۳۳، گیریم $\sum_{i\in I} G_i$ زیرمجموعه‌ای از $\Pi_{i\in I}G_i$ را نمایش دهد که مشتمل بر تمام دنباله‌های $(c_1, c_2, \dots)$ می‌باشد به طوری که برای تعدادی متناهی j، $c_j \neq e_j$ که در آن e_j عضو همانی G_j است. ثابت کنید $\sum_{i\in I} G_i$ زیرگروهی نرمال از $\Pi_{i\in I}G_i$ است. $\sum_{i\in I} G_i$ **جمع مستقیم نامتناهی** این G_iها نامیده می‌شود.

۳۵. گیریم G یک گروه باشد و برای هر عدد صحیح مثبت i، N_i زیرگروه نرمال G باشد. اگر هر عضو G را بتوان به طور یکتایی به صورت $n_{i_1}n_{i_2}\cdots n_{i_k}$ نوشت که در آن $i_1 < i_2 < \cdots < i_k$ و $n_{i_j} \in N_{i_j}$، ثابت کنید که $G \cong \sum_{i\in I} N_i$ (تمرین ۳۴ را نگاه کنید)[۴]. [راهنمایی: با تعریف کردن $f(a_1, a_2, \dots)$ به صورت حاصل‌ضرب آن a_iهایی که عضو همانی نیستند، برهان قضیه ۱.۱۰ را مطابقت دهید.]

۳۶. اگر $(m, n) = 1$، ثابت کنید که $U_{mn} \cong U_m \times U_n$.

---

۳) به جای I هر مجموعه نمایه‌گذار نامتناهی دیگر را در اینجا می‌توان بکار برد، اما کارکردن با اعداد صحیح مثبت، نمایه‌گذاری را ساده می‌کند.

۴) یکتایی به‌معنی آن است که اگر $a_{i_1}\cdots a_{i_k} = b_{j_1}\cdots b_{j_t}$ با شرط $i_1 < i_2 < \cdots < i_k$ و $j_1 < j_2 < \cdots < j_t$ آنگاه $k = t$ و برای $r = 1, 2, \dots, k$: $i_r = j_r$ و $a_{i_r} = b_{j_r}$.

۳۷. گیریم H یک گروه و $\tau_1 : H \to G_1$، $\tau_2 : H \to G_2$، ... ، $\tau_n : H \to G_n$ همریختی‌هایی با این ویژگی باشند که:وقتی G یک گروه و $g_1 : G \to G_1$، $g_2 : G \to G_2$، ... ، $g_n : G \to G_n$ همریختی‌هایی باشند، آنگاه یک همریختی یکتای $g^* : G \to H$ وجود داشته باشد به طوری که برای هر i، $\tau_i \circ g^* = g_i$. ثابت کنید که $H \cong G_1 \times G_2 \times \cdots \times G_n$. [تمرین ۱۹ را نگاه کنید.]

۲-۱۰ گروههای آبلی متناهی

در این بخش تمام گروههای آبلی متناهی تا حد یکریختی رده‌بندی می‌شوند. ثابت می‌کنیم که هر گروه آبلی متناهی جمع مستقیم زیرگروههای دوری است و این که مرتبه این زیرگروههای دوری به طور یکتا توسط G تعیین می‌شود. بجز بخش ۱.۱۰، تنها پیشنیازهای لازم دیگر، نظریه اعداد مقدماتی (بخش ۲.۱) و نظریه گروهها (فصل ۷، تا انتهای قضیه لاگرانژ) می‌باشد. بویژه، آگاهی از قضیهٔ کُشی برای گروههای آبلی را فرض شده نمی‌دانیم.

مطابق رسم معمول در مورد گروههای آبلی، در این بخش **تمام گروهها با نماد جمعی نوشته می‌شوند.** واژه‌نامه زیر می‌تواند در ترجمه از نماد جمعی به ضربی مفید باشد.

نماد ضربی	نماد جمعی
ab	$a+b$
e	0
a^k	ka
$a^k = e$	$ka = 0$
$MN = \{mn \mid m \in M, n \in N\}$	$M + N = \{m+n \mid m \in M, n \in N\}$
حاصلضرب مستقیم $M \times N$	حاصلجمع مستقیم $M \oplus N$
M عامل ضرب مستقیم	M جمعوند مستقیم

در اینجا، قضایای ۵.۷، ۱.۱۰، ۳.۱۰ از نتایج قبلی را که به طور مکرر استفاده خواهیم کرد، با نماد جمعی بیان می‌کنیم:

قضیه ۵.۷. گیریم G یک گروه باشد و $a \in G$.

(۲) اگر a مرتبه n داشته باشد، در این صورت $ka = 0$ اگر و تنها اگر $n|k$.
(۳) اگر a مرتبه td داشته باشد، آنگاه ta مرتبه d دارد.[۵]

قضیه ۱.۱۰. اگر N_1، ...، N_k زیرگروههای نرمال یک گروه G باشند به قسمی که هر عضو G را بتوان به طور یکتایی به صورت $a_1 + a_2 + \cdots + a_k$ نوشت که در آن $a_i \in N_i$، آنگاه $G \cong N_1 \oplus N_2 \oplus \cdots \oplus N_k$.

قضیه ۳.۱۰. اگر M و N زیرگروههای نرمال یک گروه G باشند به طوری که $G = M + N$ و $M \cap N = < e >$ آنگاه $G = M \oplus N$.

بالاخره متذکر می‌شویم که از تمرین ۱۱ بخش ۱.۱۰ در جاهای مختلف و بدون اشاره صریح به آن استفاده می‌شود.

اگر G گروهی آبلی و p عددی اول باشد، آنگاه $G(p)$ مجموعه تمام عضوهایی از G را نمایش می‌دهد که مرتبه آن‌ها توانی از p باشد، یعنی

$$G(p) = \{a \in G \mid \mid a \mid = p^n \quad \text{برای یک } n \geq 0\}.$$

تحقیق این که $G(p)$ تحت جمع بسته است و این که وارون هر عضو $G(p)$ در $G(p)$ قراردارد کار ساده‌ای می‌باشد (تمرین ۱). بنابراین $G(p)$ یک زیرگروه G است.

مثال ۴.۱۰. اگر $G = \mathbb{Z}_{12}$، آنگاه $G(2)$ مجموعه عناصری است که مرتبه 2^0، 2^1، 2^2 و غیره دارند. بررسی کنید که $G(2)$ زیرگروه $\{0, 3, 6, 9\}$ می‌باشد، به طور مشابه $G(3) = \{0, 4, 8\}$. اگر $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3$، آنگاه $G(3) = G$ زیرا هر عضو ناصفر G مرتبه ۳ دارد.

نخستین مرحله در اثبات این که یک گروه آبلی G، جمع مستقیم زیرگروههای دوری است این است که نشان دهیم G جمع مستقیم زیرگروهای $G(p)$ خودش می‌باشد، که در آن pها اعداد اول متمایزی هستند که مرتبه G را می‌شمارند و برای هر p، تنها یک جمعوند $G(p)$ وجود دارد. برای انجام این کار به لم زیر نیاز می‌باشد.

لم ۴.۱۰. گیریم G یک گروه آبلی باشد و $a \in G$ عنصری دارای مرتبه متناهی باشد. آنگاه

۵) این قضیه، در واقع بیان قسمت‌های (۲) و(۳) قضیه ۵.۷، با نماد جمعی است.

$a = a_1 + a_2 + \cdots + a_k$ که در آن $a_i \in G(p_i)$ و p_1، ...، p_k اعداد اول متمایز مثبتی هستند که مرتبه a را می‌شمارند.

برهان. برهان با استفاده از استقراء روی تعداد اعداد اولی است که مرتبه a را می‌شمارد. اگر $|\ a\ |$ بخش‌پذیر بر تنها یک عدد اول p_1 باشد، آنگاه مرتبه a توانی از p_1 است و بدین دلیل $a \in G(p_1)$. پس لم در این حالت درست است. به استقراء فرض کنید که لم برای تمام عناصری که مرتبه آنها بر حداکثر $k-1$ عدد اول متمایز بخش‌پذیر است، درست باشد و این که $|\ a\ |$ بر اعداد اول متمایز p_1، ...، p_k بخش‌پذیر باشد. آنگاه $|\ a\ | = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$، که در آن $r_i > 0$. گیریم $m = p_2^{r_2} \dots p_k^{r_k}$ و $n = p_1^{r_1}$، بنابراین $|\ a\ | = mb$. آنگاه $(m,n) = 1$ و طبق قضیه ۱.۳، اعداد صحیح u و v وجود دارند به طوری که $mu + nv = 1$. در نتیجه،

$$a = 1a = (mu + nv)a = mua + nva.$$

ولی $mua \in G(p_1)$، زیرا a دارای مرتبه mn است، و بدین جهت

$$p_1^{r_1}(mua) = (nm)ua = u(mna) = u0 = 0.$$

به طور مشابه $m(nva) = 0$. بنابراین طبق قضیه ۵.۷، مرتبه nva، m را می‌شمارد که عدد صحیحی با فقط $k-1$ شمارنده اول متمایز می‌باشد. بنابراین طبق فرض استقراء $nva = a_2 + a_3 + \cdots + a_k$، که در آن $a_i \in G(p_i)$. گیریم $a_1 = mua$، آنگاه

$$a = mua + nva = a_1 + a_2 + \cdots + a_k$$

که در آن $a_i \in G(p_i)$. ■

قضیه ۵.۱۰. اگر G یک گروه آبلی متناهی باشد، آنگاه

$$G = G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_t)$$

که در آن p_1، ...، p_t اعداد اول متمایزی هستند که مرتبه G را می‌شمارند.

برهان. اگر $a \in G$، آنگاه طبق نتیجه ۳۴.۷، مرتبه a، $|\ G\ |$ را می‌شمارد. بدین دلیل طبق لم ۴.۱۰، $a = a_1 + \cdots + a_t$، با شرط $a_i \in G(p_i)$ (که در آن $a_j = 0$ اگر p_i، $|\ a\ |$ را نشمارد).

برای این که ثابت کنیم که این عبارت یکتاست، فرض کنید $a_1 + \cdots + a_t = b_1 + \cdots + b_t$، با شرط $a_i, b_i \in G(p_i)$. چون G آبلی است

$$a_1 - b_1 = (b_2 - a_2) + (b_3 - a_3) + \cdots + (b_t - a_t).$$

برای هر i، $b_i - a_i \in G(p_i)$ و بدین جهت مرتبه آن توانی از p_i، مثلاً $p_i^{r_i}$ است. اگر $m = p_2^{r_2} \dots p_t^{r_t}$، آنگاه برای $i \geq 2$، $m(b_i - a_i) = 0$. لذا

$$m(a_1 - b_1) = m(b_2 - a_2) + \cdots + m(b_t - a_t) = 0 + \cdots + 0 = 0.$$

در نتیجه طبق قضیه ۵.۷، مرتبه $a_1 - b_1$ باید m را بشمارد. ولی $a_1 - b_1 \in G(p_1)$، پس مرتبه آن توانی از p_1 است. تنها توانی از p_1 که $m = p_2^{r_2} \dots p_t^{r_t}$ را می‌شمارد ۱ = p_1^0 است. بنابراین $a_1 - b_1 = 0$ و $a_1 = b_1$. استدلال‌های مشابه برای $i = 2, \dots, t$ نشان می‌دهد که برای هر i، $a_i = b_i$. بنابراین هر عضو G را می‌توان به طور یکتایی به صورت $a_1 + \cdots + a_t$ نوشت که در آن $a_i \in G(p_i)$ و از اینرو طبق قضیه ۱.۱۰، $G = G(p_1) \oplus \cdots \oplus G(p_t)$. ■

اگر p عددی اول باشد، آنگاه گروهی که هر عضو آن دارای مرتبه توانی از p باشد را یک **p–گروه** نامند. در قضیه ۵.۱۰ هرکدام از $G(p_i)$ها طبق تعریف آنها p_i–گروه هستند. یک عضو a از یک p–گروه B را یک **عضو از مرتبه بیشین** نامند، اگر برای هر $b \in B$، $| a | \geq | b |$. اگر $| a | = p^n$ و $b \in B$ آنگاه b دارای مرتبه p^j می‌باشد که در آن $j \leq n$. چون $p^n = p^j p^{n-j}$ می‌بینیم که برای هر $b \in B$، $p^n b = p^{n-j}(p^j b) = 0$. توجه فرمایید که در یک p–گروه متناهی همواره عناصری از مرتبه بیشین وجود دارد.

مرحله بعد در رده‌بندی گروههای آبلی متناهی اثبات این مطلب است که هر p–گروه آبلی متناهی دارای یک جمعوند مستقیم دوری است. سپس می‌توانیم ثابت کنیم که هر p–گروه آبلی متناهی جمع مستقیمی از زیرگروههای دوری است.

لم ۶.۱۰. گیریم G یک p–گروه آبلی متناهی و a یک عضو از مرتبه بیشین در G باشد. آنگاه یک زیرگروه K از G وجود دارد به طوری که $G = < a > \oplus K$.

برهان زیر پیچیدگی بیشتری از برهان‌هایی که پیش از این در این کتاب آمده است دارد. با این وجود، در این برهان تنها از نظریه گروههای مقدماتی استفاده شده است، بنابراین اگر آن را به دقت

مطالعه کنید نباید در تعقیب استدلال با مشکلی مواجه شوید.

برهان لم ۶.۱۰. آن زیرگروههای H از G را در نظر بگیرید که $H \cap < a > = < ۰ >$. لااقل یک زیرگروه ($H = < ۰ >$) وجود دارد، و چون G متناهی است یک بزرگترین زیرگروه K، با این خاصیت باید وجود داشته باشد. در این صورت $K \cap < a > = < ۰ >$، و طبق قضیه ۳.۱۰، تنها لازم است نشان دهیم که $G = K + < a >$. اگر چنین نباشد آنگاه یک عضو ناصفر b وجود دارد به طوری که $b \notin K + < a >$. گیریم h کوچکترین عدد صحیح مثبتی باشد که $p^h b \in K + < a >$ (باید یک چنین عضوی وجود داشته باشد زیرا G یک p–گروه است و بدین دلیل برای یک j مثبت، $p^j b = ۰ = ۰ + ۰ \in K + < a >$). در این صورت

$$c = p^{h-۱} b \quad \text{در} \quad K + < a > \quad \text{نیست} \tag{۱}$$

و $pc = p^h b$ در $K + < a >$ است، مثلاً

$$pc = ta + k \qquad (t \in \mathbb{Z}, k \in K). \tag{۲}$$

اگر a مرتبه p^n داشته باشد، آنگاه برای هر $x \in G$، $p^n x = ۰$ زیرا a مرتبه بیشین دارد. در نتیجه، طبق (۲)

$$p^{n-۱} ta + p^{n-۱} k = p^{n-۱}(ta + k) = p^{n-۱}(pc) = p^n c = ۰.$$

بنابراین $p^{n-۱} ta = -p^{n-۱} k \in K \cap < a > = < ۰ >$ و $p^{n-۱} ta = ۰$. قضیه ۲۰.۷ نشان می‌دهد که p^n (مرتبه a)، $p^{n-۱} t$ را می‌شمارد، و از آن نتیجه می‌شود که $p | t$. بنابراین برای یک m، $pc = ta + k = pma + k$ و در نتیجه،

$$k = pc - pma = p(c - ma).$$

گیریم

$$d = c - ma. \tag{۳}$$

آنگاه $pd = p(c - ma) = k \in K$، ولی $d \notin K$ (چون $c - ma = k' \in K$ ایجاب خواهد کرد که $c = ma + k' \in K + < a >$، که در تناقض با (۱) است). با استفاده از قضیه ۸.۷،

تحقیق کنید که $H = \{x + zd \mid x \in K, z \in \mathbb{Z}\}$ یک زیرگروه G است و $K \subseteq H$. چون $d = ۰ + ۱d \in H$ و $d \notin K$، H بزرگتر از K است، ولی K بزرگترین زیرگروهی بود که $< a > \cap K =< ۰ >$. بنابراین باید داشته باشیم $< a > \cap H \neq< ۰ >$. اگر w یک عضو ناصفر $< a > \cap H$ باشد، آنگاه

$$w = sa = k_۱ + rd \qquad (k_۱ \in K; r, s \in \mathbb{Z}). \tag{۴}$$

ادعا می‌کنیم که $p \nmid r$؛ زیرا اگر $r = py$، در این صورت چون $pd \in K$، داریم $w = sa = k_۱ + ypd \in < a > \bigcap K$، و طبق قضیه ۱.۳، $(p, r) = ۱$، که تناقض است. در نتیجه $w \neq ۰$، و طبق قضیه ۱.۳، اعداد صحیح u و v وجود دارند که $pu + rv = ۱$. در این صورت

$$\begin{aligned} c = ۱c = (pu + rv)c &= u(pc) + v(rc) \\ &= u(ta + k) + v(r(d + ma)) \qquad [\text{طبق } (۲), (۳)] \\ &= u(ta + k) + v(rd + rma) \\ &= u(ta + k) + v(sa - k_۱ + rma) \qquad [\text{طبق } (۴)] \\ &= (ut + vs + rm)a + (uk - vk_۱) \in < a > + K. \end{aligned}$$

این متناقض با (۱) است. بنابراین $G =< a > + K$، و بدین دلیل طبق ۳.۱۰، $G =< a > \oplus K$. ■

قضیه ۷.۱۰. (قضیه اساسی گروههای آبلی متناهی) هر گروه آبلی متناهی G جمع مستقیم گروههای دوری است، که مرتبه هر کدام توانی از یک عدد اول است.

برهان. طبق قضیه ۵.۱۰، G جمع مستقیم زیرگروههای $G(p)$ خودش می‌باشد، که در آن تنها یک جمعوند مستقیم $G(p)$ برای هر p که $| G |$ را بشمارد وجود دارد. هر $G(p)$ یک p–گروه است. پس برای تکمیل کردن برهان فقط لازم است نشان دهیم که هر p–گروه آبلی H جمع مستقیمی از گروههای دوری است که هر کدام مرتبه‌ای برابر با توانی از p دارند. این موضوع را با استقراء روی مرتبه H ثابت می‌کنیم. طبق قضیه ۱۳.۷، وقتی که H دارای مرتبه ۲ می‌باشد حکم درست است. به استقراء فرض کنید که حکم برای تمام گروههایی که مرتبه آنها کمتر از $| H |$ است درست باشد و گیریم a یک عضو از مرتبه بیشین p^n در H باشد. آنگاه طبق لم ۶.۱۰، $H =< a > \oplus K$.

بنابر استقراء K جمع مستقیم زیرگروههای دوری است، که هرکدام مرتبه‌ای برابر با توانی از p دارند. بنابراین همین مطلب برای $H =< a > \oplus K$ نیز درست است. ■

مثال ۵.۱۰. عدد ۳۶ را می‌توان دقیقاً به چهار طریق به صورت حاصل‌ضربی از توانهای اول نوشت:

$$۳۶ = ۲ \times ۲ \times ۳ \times ۳ = ۲ \times ۲ \times ۳^۲ = ۲^۲ \times ۳ \times ۳ = ۲^۲ \times ۳^۲.$$

در نتیجه طبق قضیه ۷.۱۰، هر گروه آبلی از مرتبه ۳۶ باید یکریخت با یکی از گروههای زیر باشد:

$$\mathbb{Z}_۲ \oplus \mathbb{Z}_۲ \oplus \mathbb{Z}_۳ \oplus \mathbb{Z}_۳. \qquad \mathbb{Z}_۲ \oplus \mathbb{Z}_۲ \oplus \mathbb{Z}_۹. \qquad \mathbb{Z}_۴ \oplus \mathbb{Z}_۳ \oplus \mathbb{Z}_۳. \qquad \mathbb{Z}_۴ \oplus \mathbb{Z}_۹.$$

به سادگی می‌توانید بررسی کنید که هیچ دوتا از این گروهها یکریخت نیستند (تعداد عناصر از مرتبه ۲ یا ۳ برای هر گروه متفاوت است). بنابراین یک رده‌بندی کامل از تمام گروههای آبلی از مرتبه ۳۶ تا حد یکریختی داریم. احتمالاً توجه کرده‌اید که یک گروه شناخته شده از مرتبه ۳۶، یعنی $\mathbb{Z}_{۳۶}$ به صراحت در فهرست بالا ظاهر نمی‌شود. با این حال، این گروه یکریخت با $\mathbb{Z}_۴ \oplus \mathbb{Z}_۹$ است، همانگونه که اکنون ثابت می‌کنیم.

لم ۸.۱۰. اگر $(m,k) = ۱$، آنگاه $\mathbb{Z}_m \oplus \mathbb{Z}_k \cong \mathbb{Z}_{mk}$.

برهان. مرتبه عضو $(۱,۱)$ در $\mathbb{Z}_m \oplus \mathbb{Z}_k$ کوچکترین عدد صحیح مثبت t است که $(t,t) = t(۱,۱) = (۰,۰)$. بدین دلیل (پیمانه m) $t \equiv ۰$ و (پیمانه k) $t \equiv ۰$. لذا $m|t$، $k|t$ و $(m,k) = ۱$ ایجاب می‌کند که طبق تمرین ۱۷ در بخش ۲.۱، $mk|t$. بدین جهت $mk \leq t$. چون $mk(۱,۱) = (mk,mk) = (۰,۰)$ باید داشته باشیم $|(۱,۱)| = t = mk$. بنابراین $\mathbb{Z}_m \oplus \mathbb{Z}_k$ (یک گروه از مرتبه mk)، گروه دوری پدیدآمده توسط $(۱,۱)$ می‌باشد و بدین دلیل طبق قضیه ۱۳.۷، یکریخت با $\mathbb{Z}_{mk}$ است. ■

قضیه ۹.۱۰. اگر $n = p_۱^{n_۱} p^{n_۲} \dots p_t^{n_t}$ که در آن p_iها اعداد اول متمایزند، آنگاه

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_۱^{n_۱}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}.$$

برهان. قضیه برای گروههای از مرتبه ۲ درست است. به استقراء فرض کنید که قضیه برای گروههای از مرتبه کمتر از n درست باشد. قضیه ۸.۱۰ را با شرط $m = p_1^{n_1}$ و $k = p_2^{n_2} \dots p_t^{n_t}$ بکار برید. در این صورت $\mathbb{Z}_n = \mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_k$. فرض استقراء نشان می‌دهد که $\mathbb{Z}_k \cong \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$. به این ترتیب اثبات کامل می‌شود. ■

از ترکیب قضایای ۷.۱۰ و ۹.۱۰ روش دیگری برای بیان یک گروه آبلی متناهی به صورت جمع مستقیمی از گروههای دوری استنتاج می‌شود.

مثال ۶.۱۰. گروه

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$$

را در نظر بگیرید. به ازای هر عدد اول، توانهایی از آن را که در تجزیه فوق، به‌عنوان مرتبه یکی از عوامل دوری تجزیه ظاهر شده‌اند برحسب اندازه، از کوچک به بزرگ، مرتب نموده در یک ردیف بنویسید.

۲	۲	$۲^۲$	$۲^۳$
	۳	۳	۳
		۵	$۵^۲$

اکنون با استفاده از ستونهای آرایه فوق، ترتیب دیگری از عامل‌های دوری G بوجود آورید (تمرین ۱۵ از بخش ۱.۱۰ را ملاحظه کنید) و قضیه ۹.۱۰ را بکار برید:

$$G \cong (\mathbb{Z}_2) \oplus \underbrace{(\mathbb{Z}_2 \oplus \mathbb{Z}_2)}_{\mathbb{Z}_4} \oplus \underbrace{(\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5)}_{\mathbb{Z}_{60}} \oplus \underbrace{(\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25})}_{\mathbb{Z}_{600}}$$

$$G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{600}$$

این تجزیه اخیر G به صورت مجموع گروههای دوری گاهی مناسبتر از تجزیه ابتدایی G (به صورت جمع مستقیمی از زیرگروههای دوری که مرتبه هر یک توانی از یک عدد اول است) می‌باشد. عامل‌های دوری کمتری وجود دارند، و مرتبه هر عامل دوری مرتبه بعدی را می‌شمارد. همین فرآیند در حالت کلی نیز عمل نموده قضیه زیر ثابت می‌شود، البته در اثبات از نمادهای بیشتری استفاده می‌شود.

قضیه ۱۰.۱۰. هر گروه آبلی متناهی جمع مستقیم گروههای دوری از مرتبه‌های $m_1, \dots, m_2, m_1$ است که در آن $m_{i-1} | m_i, \dots, m_3 | m_4, m_2 | m_3, m_1 | m_2$.

این امر ارزش آن را دارد که موقتاً از خط سیر اصلی منحرف شده تا متذکر شویم که قضیه ۱۰.۱۰ برهان دیگری از قضیه ۴۱.۷ عرضه می‌نماید که اینجا به بیان مجدد آن می‌پردازیم.

نتیجه ۱۱.۱۰. اگر G زیرگروهی متناهی از گروه ضربی عناصر ناصفر یک میدان متناهی $\mathbb{F}$ باشد، در این صورت G دوری است.

برهان. چون G یک گروه آبلی متناهی است، قضیه ۱۰.۱۰ ایجاب می‌کند که $G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}$، که در آن هر m_i، m_t را می‌شمارد. هر عضو b در $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}$ در رابطه $m_t b = 0$ صدق می‌کند (چرا؟). در نتیجه، هر عضو g از گروه ضربی G باید در $g^{m_t} = 1_{\mathbb{F}}$ صدق کند (یعنی، باید ریشه‌ای از چندجمله‌ای $x^{m_t} - 1_{\mathbb{F}}$ باشد). چون G مرتبه $m_1 m_2 \cdots m_t$ دارد و طبق نتیجه ۱۳.۴، $x^{m_t} - 1$ حداکثر m_t ریشه متمایز در $\mathbb{F}$ دارد، باید داشته باشیم $t = 1$ و $G \cong \mathbb{Z}_{m_1}$. ■

اگر G یک گروه آبلی متناهی باشد، در این صورت اعداد صحیح m_1، ...، m_t مطرح شده در قضیه ۱۰.۱۰، **عامل‌های پایای** G نامیده می‌شوند. وقتی که G به صورت جمع مستقیم گروههای دوری از مرتبه‌های توان اعداد اول باشد، این توانهای اول **شمارنده‌های مقدماتی** G نامیده می‌شوند. قضایای ۷.۱۰ و ۱۰.۱۰ نشان می‌دهد که مرتبه G حاصل‌ضرب شمارنده‌های مقدماتی آن و همچنین حاصل‌ضرب عامل‌های پایای G می‌باشد.

مثال ۷.۱۰. تمام گروههای آبلی از مرتبه ۳۶ را می‌توان تا حدّ یکریختی برحسب شمارنده‌های مقدماتی (مثل آنچه در مثال پیش از لم ۸.۱۰ آمده است) یا برحسب عامل‌های پایای آنها رده‌بندی نمود.

گروه یکریخت	عامل‌های پایا	شمارنده‌های مقدماتی	گروه
$\mathbb{Z}_6 \oplus \mathbb{Z}_6$	$6, 6$	$2, 2, 3, 3$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
$\mathbb{Z}_2 \oplus \mathbb{Z}_{18}$	$2, 18$	$2, 2, 3^2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$
$\mathbb{Z}_3 \oplus \mathbb{Z}_{12}$	$3, 12$	$2^2, 3, 3$	$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
$\mathbb{Z}_{36}$	36	$2^2, 3^2$	$\mathbb{Z}_4 \oplus \mathbb{Z}_9$

از قضیه اساسی ۷.۱۰ می‌توان استفاده کرد تا فهرستی از تمام گروههای آبلی ممکن از مرتبه مفروض را بدست آورد. برای تکمیل کردن رده‌بندی چنین گروههایی باید نشان دهیم که هیچ دو

گروه از این فهرست یکریخت نیستند، یعنی این که شمارنده‌های مقدماتی یک گروه به طور یکتا تعیین می‌شوند[۶].

قضیه ۱۲.۱۰. گیریم G و H گروههای آبلی متناهی باشند. در این صورت G یکریخت با H است اگر و تنها اگر G و H شمارنده‌های مقدماتی یکسان داشته باشند.

همچنین این مطلب درست است که $G \cong H$ اگر و تنها اگر G و H عامل‌های پایای یکسان داشته باشند (تمرین ۲۴).

برهان قضیه ۱۲.۱۰. اگر G و H دارای شمارنده‌های مقدماتی یکسان باشند، آنگاه G و H هر دو یکریخت با جمع مستقیم گروههای دوری یکسانی هستند و بدین دلیل یکدیگرند. بالعکس، اگر $f : G \to H$ یک یکریختی باشد، برای هر $a \in G$، عناصر a و $f(a)$ دارای مرتبه یکسان هستند. از این نتیجه می‌شود که برای هر عدد اول p، $f(G(p)) = H(p)$ و بدین دلیل $G(p) \cong H(p)$. شمارنده‌های مقدماتی از G که توانهای عدد اول p هستند دقیقاً شمارنده‌های $G(p)$ می‌باشند، و به طور مشابه برای H این مطلب درست است. پس تنها لازم است ثابت کنیم که p–گروههای یکریخت دارای شمارنده‌های مقدماتی یکسان هستند. به بیان دیگر لازم است که فقط این قضیه را برای حالتی که G و H، p–گروه هستند ثابت کنیم.

برای p–گروههای یکریخت، برهان با استفاده از استقراء روی مرتبه G می‌باشد. طبق قضیه ۱۳.۷، تمام گروههای از مرتبه ۲ به وضوح شمارنده‌های مقدماتی یکسان، ۲، دارند. بنابراین فرض کنید که گزاره برای تمام گروههای از مرتبه کمتر از $|G|$ درست باشد. فرض کنید شمارنده‌های مقدماتی G اعداد زیر باشند:

$$p^{n_1}, p^{n_2}, \ldots, p^{n_t}, \underbrace{p, p, \ldots, p}_{r-\text{نسخه}} \quad (\text{با شرط } n_1 \geq n_2 \geq \cdots \geq n_t > 1).$$

و این که شمارنده‌های مقدماتی H اعداد زیر باشند،

$$p^{m_1}, p^{m_2}, \ldots, p^{m_k}, \underbrace{p, p, \ldots, p}_{s-\text{نسخه}} \quad (\text{با شرط } m_1 \geq m_2 \geq \cdots \geq m_k > 1).$$

بررسی کنید که $pG = \{px \mid x \in G\}$ یک زیرگروه G است (تمرین ۲). اگر G جمع مستقیم گروههای C_i باشد، تحقیق کنید که pG جمع مستقیم گروههای pC_i است (تمرین ۴). اگر C_i گروهی

۶) بقیه این بخش اختیاری است. قضیه ۱۲.۱۰ اغلب به عنوان قسمتی از قضیه اساسی گروههای آبلی متناهی در نظر گرفته می‌شود.

دوری با مولد a از مرتبه p^n باشد، آنگاه pC_i گروهی دوری با مولد pa می‌باشد. چون طبق قسمت (۳) قضیه ۵.۷، pa دارای مرتبه p^{n-1} می‌باشد، pC_i دوری از مرتبه p^{n-1} است. توجه فرمایید که وقتی $n = 1$ (یعنی، وقتی C_i دوری از مرتبه p باشد)، در این صورت $pC_i =< 0 >$. در نتیجه، شمارنده‌های مقدماتی pG عبارتند از:

$$p^{n_1-1}, p^{n_2-1}, \ldots, p^{n_t-1}$$

استدلال مشابهی نشان می‌دهد که شمارنده‌های مقدماتی pH اعداد

$$p^{m_1-1}, p^{m_2-1}, \ldots, p^{m_k-1}$$

هستند.

اگر $f : G \to H$ یک یکریختی باشد، تحقیق کنید که $f(pG) = pH$ و لذا $pG \cong pH$. به علاوه، $pG \neq G$ (تمرین ۹)، و بدین دلیل pG و pH، طبق فرض استقراء، شمارنده‌های مقدماتی یکسان دارند، یعنی $t = k$ و $p^{n_i-1} = p^{m_i-1}$. پس برای $i = 1, 2, \ldots, t$، $n_i - 1 = m_i - 1$. بنابراین برای هر i، $n_i = m_i$. پس تنها تفاوت ممکن در شمارنده‌های مقدماتی G و H تعداد نسخه‌های pای است که در هر فهرست ظاهر می‌شود. چون $|G|$ حاصلضرب شمارنده‌های مقدماتی است و همین مطلب برای $|H|$ نیز درست می‌باشد و چون $G \cong H$، داریم

$$p^{n_1}p^{n_2}\ldots p^{n_t}p^r = |G| = |H| = p^{m_1}p^{m_2}\ldots p^{m_k}p^s.$$

بنابراین $p^r = p^s$ و بدین دلیل $r = s$. بنابراین G و H شمارنده‌های مقدماتی یکسان دارند. ■

تمرینها

توجه: تمام گروهها به صورت جمعی نوشته می‌شوند، p همواره عدد اول مثبت است، مگر خلاف آن ذکر شود.

A.۱. اگر G یک گروه آبلی باشد، ثابت کنید که $G(p)$ یک زیرگروه است.

۲. اگر G یک گروه آبلی باشد ثابت کنید که $pG = \{px \mid x \in G\}$ یک زیرگروه G است.

۳. تمام گروههای آبلی با مرتبه داده شده را (تا حد یکریختی) فهرست کنید:

(الف) ۱۲ (ب) ۱۵ (پ) ۳۰ (ت) ۷۲
(ث) ۹۰ (ج) ۱۴۴ (چ) ۶۰۰ (ح) ۱۱۶۰

۴. اگر G و G_iها گروههای آبلی باشند به طوری که $G = G_1 \oplus \cdots \oplus G_n$، نشان دهید که $pG = pG_1 \oplus \cdots \oplus pG_n$.

۵. شمارنده‌های مقدماتی گروههای داده شده را پیدا کنید:

(الف) $\mathbb{Z}_{۲۵۰}$ (ب) $\mathbb{Z}_۶ \oplus \mathbb{Z}_{۱۲} \oplus \mathbb{Z}_{۱۸}$
(پ) $\mathbb{Z}_{۱۰} \oplus \mathbb{Z}_{۲۰} \oplus \mathbb{Z}_{۳۰} \oplus \mathbb{Z}_{۴۰}$ (ت) $\mathbb{Z}_{۱۲} \oplus \mathbb{Z}_{۳۰} \oplus \mathbb{Z}_{۱۰۰} \oplus \mathbb{Z}_{۲۴۰}$

۶. عامل‌های پایای هرکدام از گروههای تمرین ۵ را پیدا کنید.

۷.B شمارنده‌های مقدماتی و عامل‌های پایای گروه داده شده را پیدا کنید. توجه فرمایید که عمل گروه در سه تای اول ضرب و در گروه آخر جمع است.

(الف) $U_۸$ (ب) $U_{۱۷}$ (پ) $U_{۱۵}$ (ت) $M(\mathbb{Z}_۲)$

۸. اگر G گروه جمعی $\mathbb{Q}/\mathbb{Z}$ باشد، عضوهای زیرگروه $G(۲)$ چیست؟ برای هر عدد اول مثبت p عضوهای $G(p)$ چیست؟

۹. (الف) اگر G یک p–گروه آبلی متناهی باشد، ثابت کنید که $pG \neq G$.
(ب) نشان دهید که اگر G نامتناهی باشد، قسمت (الف) می‌تواند نادرست باشد. [گروه $G(۲)$ در تمرین ۸ را در نظر بگیرید.]

۱۰. اگر G یک p–گروه آبلی و $(n, p) = ۱$، ثابت کنید که نگاشت $f : G \to G$ تعریف شده توسط $f(a) = na$ یک یکریختی است.

۱۱. اگر G یک p–گروه آبلی متناهی باشد به طوری که $pG = \{۰\}$، ثابت کنید که برای تعدادی متناهی نسخه $\mathbb{Z}_p$، $G \cong \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$.

۱۲. **(قضیه کُشی برای گروههای آبلی)** اگر G یک گروه آبلی متناهی و p یک عدد اول باشد که $p \mid |G|$ را بشمارد، ثابت کنید که G یک عضو از مرتبه p دارد. [راهنمایی: از قضیه اساسی استفاده کنید تا نشان دهید که G دارای یک زیرگروه دوری از مرتبه p^k است؛ از قضیه ۵.۷ استفاده کنید تا یک عضو از مرتبه p پیدا کنید.]

۱۳. ثابت کنید که یک p–گروه آبلی متناهی دارای مرتبه توانی از p می‌باشد.

۱۴. اگر G یک گروه آبلی از مرتبه $p^t m$، با شرط $(p, m) = ۱$ باشد، ثابت کنید که $G(p)$ دارای مرتبه p^t است.

۱۵. اگر G یک گروه آبلی متناهی و p عدد اولی باشد به طوری که p^n، $| G |$ را بشمارد، در این صورت ثابت کنید که G یک زیرگروه از مرتبه p^n دارد.

۱۶. برای کدام اعداد صحیح مثبت n، دقیقاً یک گروه آبلی از مرتبه n (تا حد یکریختی) وجود دارد؟

۱۷. گیریم G، H و K گروههای آبلی متناهی باشند.

(الف) اگر $G \oplus G \cong H \oplus H$، ثابت کنید که $G \cong H$.

(ب) اگر $G \oplus H \cong G \oplus K$، ثابت کنید که $H \cong K$.

۱۸. اگر G یک گروه آبلی از مرتبه n و $k|n$، ثابت کنید که یک گروه H از مرتبه k و یک همریختی پوشای $G \to H$ وجود دارد.

۱۹. گیریم G یک گروه آبلی و T مجموعه عناصر از مرتبه متناهی G باشد. ثابت کنید که

(الف) T یک زیرگروه G است (که **زیرگروه تابدار** نامیده می‌شود).

(ب) هر عضو ناصفر گروه خارج قسمت G/T دارای مرتبه نامتناهی است.

۲۰. اگر G یک گروه آبلی باشد آیا عناصر از مرتبه نامتناهی در G (همراه با صفر) یک زیرگروه است؟ [راهنمایی: $\mathbb{Z} \oplus \mathbb{Z}_۲$ را در نظر بگیرید.]

۲۱.C. اگر G یک گروه آبلی و $f : G \to \mathbb{Z}$ یک همریختی پوشا با هسته K باشد، ثابت کنید که G یک زیرگروه H دارد به طوری که $H \cong \mathbb{Z}$ و $G = K \oplus H$.

۲۲. گیریم G و H گروههای آبلی با این ویژگی باشند که برای هر عدد صحیح مثبت m تعداد عناصر از مرتبه m در G برابر با تعداد عناصر از مرتبه m در Hباشد. ثابت کنید که $G \cong H$.

۲۳. گیریم که G یک گروه آبلی متناهی با این ویژگی باشد که برای هر عدد صحیح مثبت m که $| G |$ را بشمارد، دقیقاً m عضو در G وجود دارد که مرتبه آنها m را می‌شمارد. ثابت کنید که G دوری است.

۲۴. گیریم G و H گروههای آبلی متناهی باشند. ثابت کنید که $G \cong H$ اگر و تنها اگر G و H دارای عامل‌های پایای یکسان باشند.

۲۵. اگر G **یک گروه تابدار** (یعنی این که هر عضو G دارای مرتبه متناهی است) آبلی نامتناهی باشد، ثابت کنید که G جمع مستقیم نامتناهی $\sum G(p)$ است، که در آن جمع روی تمام اعداد اول مثبت p گرفته می‌شود. [راهنمایی: تمرین‌های ۳۵ـ۳۴ در بخش ۱.۱۰ را ملاحظه کنید و برهان قضیه ۵.۱۰ را تطبیق نمایید.]

۱۰-۳ قضایای سیلو و کاربردها

گروههای غیرآبلی متناهی بسیار پیچیده‌تر از گروههای آبلی است، که تا حد یکریختی در بخش قبل رده‌بندی گردید. قضایای سیلو نخستین مرحله اساسی در فهم ساختار گروههای غیرآبلی متناهی است. چون برهان این قضایا به میزان زیادی به طریقی که این قضیه‌ها به واقع بکار می‌روند تا گروهها را تجزیه و تحلیل کنند نامربوط است، برهان آنها به بخش بعد موکول می‌شود[۷]. در این بخش تلاش می‌کنیم تا درک صحیحی از قضایای سیلو بدست آوریم و چند مثال از کاربردهای گوناگون آن نیز ارائه کنیم.

در سرتاسر این بخش تمام گروهها به صورت ضربی نوشته می‌شود و تمام اعداد صحیح، نامنفی فرض می‌شوند. باز هم ارتباط نزدیک بین ساختار یک گروه G و خواص حسابی عدد صحیح $|G|$، موضوع اصلی است. یکی از مهمترین دستاوردهای از این نوع، قضیهٔ لاگرانژ است که بیان می‌کند که اگر G دارای یک زیرگروه H باشد، آنگاه $|H|$، $|G|$ را می‌شمارد. اولین قضیه سیلو، عکس قضیه لاگرانژ را (به طور نسبی) بدست می‌دهد:

قضیه ۱۳.۱۰. (**اولین قضیه سیلو**) گیریم G یک گروه متناهی باشد. اگر p عددی اول باشد و p^k، $|G|$ را بشمارد، در این صورت G دارای زیرگروهی از مرتبه p^k می‌باشد.

مثال ۸.۱۰. گروه متقارن S_6 دارای مرتبه $5 \times 3^2 \times 2^4 = 6!$ می‌باشد. اولین قضیه سیلو (با شرط $p = 2$) تضمین می‌کند که S_6 دارای زیرگروههایی از مرتبه ۲، ۴ و ۸، و ۱۶ است. البته ممکن

۷) کسانی که به اثباتهای محض علاقه دارند و معتقدند که ابتدا باید سختی کشید و بعد لذّت برد، می‌توانند ابتدا بخش ۴.۱۰ را مطالعه کرده و سپس این بخش را ادامه دهند.

است بیشتر از یک گروه از هر یک از این مرتبه‌ها وجود داشته باشد. برای مثال، لااقل ۶۰ زیرگروه از مرتبه ۴ وجود دارد (تمرین ۱). استفاده از این قضیه برای $p = ۳$ نشان می‌دهد که $S_۶$ دارای زیرگروههایی از مرتبه‌های ۳ و ۹ می‌باشد. به طور مشابه $S_۶$ دست کم یک زیرگروه از مرتبه ۵ دارد.

اگر p عدد اولی باشد که مرتبه یک گروه G را بشمارد، آنگاه طبق اولین قضیه سیلو، G شامل یک زیرگروه K از مرتبه p است. چون طبق قضیه ۳۵.۷، K دوری است، مولد آن عضوی از مرتبه p در G است. این مطلب نتیجه زیر را ثابت می‌کند.

نتیجه ۱۴.۱۰ (قضیه کشی). اگر G، یک گروه متناهی باشد که مرتبه آن بر عدد اول p بخش‌پذیر باشد، آنگاه G عضوی از مرتبه p دارد.

گیریم G یک گروه متناهی و p یک عدد اول باشد. اگر p^n بزرگترین توانی از p باشد که $| G |$ را بشمارد، آنگاه یک زیرگروه از G از مرتبه p^n را **$p-$زیرگروه سیلو** می‌نامند. وجود $p-$زیرگروههای سیلو نتیجه فوری اولین قضیه سیلو است.

مثال ۹.۱۰. چون $S_۴$ دارای مرتبه $۳ \times ۲^۳ = ۲۴ = ۴!$ می‌باشد هر زیرگروه از مرتبه ۸ یک ۲ زیرگروه سیلو است. به سادگی می‌توانید بررسی کنید که

$$\{(۱), (۱۲۳۴), (۱۳)(۲۴), (۱۴۳۲), (۲۴), (۱۲)(۳۴), (۱۳), (۱۴)(۳۲)\}$$

یک زیرگروه از مرتبه ۸ است و بدین دلیل یک ۲ـ زیرگروه سیلو است. تعداد دو، ۲ـ زیرگروه سیلوی دیگر وجود دارد (تمرین ۲). هر زیرگروه $S_۴$ از مرتبه ۳ یک ۳ـ زیرگروه سیلو است. مجموعه‌های $\{(۱), (۱۲۳), (۱۳۲)\}$ و $\{(۱), (۱۴۳), (۱۳۴)\}$ دو تا از چهار ۳ـ زیرگروه سیلوی $S_۴$ می‌باشند.

مثال ۱۰.۱۰.[۸] گیریم p عددی اول باشد و G یک گروه آبلی متناهی از مرتبه $p^n m$ باشد که $p \nmid m$. در این صورت $\{$برای برخی $k \geq ۰$، $G(p) = \{a \in G \mid\mid a \mid = p^k$ یک $p-$گروه سیلوی G است زیرا طبق تمرین ۱۴ از بخش ۲.۱۰، $G(p)$ دارای مرتبه p^n می‌باشد. همانگونه که در زیر خواهیم دید، $G(p)$، $p-$زیرگروه سیلوی یکتای G است. قضیه ۵.۱۰ نشان می‌دهد که G جمع مستقیم تمام زیرگروههای سیلوی خودش (یک زیر گروه سیلو برای هر کدام از اعداد اول متمایزی که $| G |$ را می‌شمارد) می‌باشد.

۸) اگر بخش ۲.۱۰ را مطالعه نکرده‌اید، از خواندن این مثال صرف‌نظر کنید.

گیریم G یک گروه باشد و $x \in G$. مثال ۳۱.۷ نشان می‌دهد که نگاشت $f : G \to G$ تعریف شده توسط $f(a) = x^{-1}ax$ یک یکریختی است. اگر K یک زیرگروه G باشد، آنگاه $x^{-1}Kx = \{x^{-1}kx \mid k \in K\}$، تصویر K تحت f می‌باشد. بدین دلیل، $x^{-1}Kx$ زیرگروهی از G است که یکریخت با K است. به ویژه، $x^{-1}Kx$ همان مرتبه K را دارد. در نتیجه،

اگر K یک p–زیرگروه سیلوی G باشد، آنگاه $x^{-1}Kx$ نیز چنین است.

قضیه بعد نشان می‌دهد که هر p–زیرگروه سیلوی G را می‌توان بدین طریق بدست آورد.

قضیه ۱۵.۱۰ (دومین قضیه سیلو). اگر P و K، p–زیرگروههای سیلوی یک گروه G باشند، آنگاه $x \in G$ وجود دارد به طوری که $P = x^{-1}Kx$.

قضیه ۱۵.۱۰، همراه با این حقیقت که $x^{-1}Kx$ یکریخت با K است، نشان می‌دهد که

هر دو p–زیرگروه سیلوی G یکریختند.

نتیجه ۱۶.۱۰. گیریم G یک گروه متناهی و K یک p–زیرگروه سیلو، برای یک عدد اول p باشد. در این صورت، K در G نرمال است اگر و تنها اگر K تنها p–زیرگروه سیلوی G باشد.

برهان. می‌دانیم که برای هر $x \in G$، $x^{-1}Kx$ یک p–زیرگروه سیلو است. اگر K تنها p–زیرگروه سیلوی G باشد، آنگاه برای هر $x \in G$ باید داشته باشیم، $x^{-1}Kx = K$. بنابراین طبق قضیه ۲۱.۷، K نرمال است. بالعکس، فرض کنید K نرمال است و گیریم P، p–زیرگروه سیلوی دلخواهی باشد. طبق دومین قضیه سیلو، $x \in G$ وجود دارد به طوری که، $P = x^{-1}Kx$. چون K نرمال است، $P = x^{-1}Kx = K$. بنابراین K تنها p– زیرگروه سیلو است. ■

قضایای قبل وجود p–زیرگروههای سیلو و رابطه بین هر دو تا از این زیرگروهها را نهادینه می‌کنند. قضیه بعد بیان می‌کند که یک گروه مفروض می‌تواند چند p–زیرگروه سیلو داشته باشد.

قضیه ۱۷.۱۰ (سومین قضیه سیلو). تعداد p– زیرگروههای سیلوی یک گروه متناهی G، مرتبه G را می‌شمارد و این تعداد به صورت $pk + 1$ برای یک عدد صحیح نامنفی k، می‌باشد.

گروههای ساده (آنهایی که زیرگروههای نرمال سره ندارد) بلوکهای اساسی ساختمان تمام گروهها هستند. بنابراین اگر بتوانیم بگوییم که زیرگروههای ساده از مرتبه بخصوص وجود دارد، مفید خواهد بود. سومین قضیه سیلو همراه با بحث‌های شمارشی مناسب و نتیجه ۱۶.۱۰، اغلب می‌تواند مورد

استفاده قرار گیرد تا وجود یک زیرگروه نرمال سره یک گروه G را ثابت نماید و بدین بدلیل نشان داده می‌شود که G ساده نیست.

مثال ۱۱.۱۰. اگر G گروهی از مرتبه $۴۵ = ۳^۲ \times ۵$ باشد، در این صورت هر ۳ـ زیرگروه سیلو، دارای مرتبه ۹ است و تعداد این چنین زیرگروههایی شمارنده‌ای از ۴۵ به صورت $۳k + ۱$ است. شمارنده‌های ۴۵ اعداد ۱، ۳، ۵، ۹، ۱۵، ۴۵ و اعداد صحیح به صورت $۳k + ۱$ (با شرط $k \geq ۰$) به صورت ۱، ۴، ۷، ۱۰، ۱۳، ۱۶، ۱۹، ۱۱، ۲۵ و غیره هستند. چون ۱ تنها عدد مشترک در هر دو فهرست است. بنابراین G، دقیقاً یک ۳ـ گروه سیلو دارد. این زیرگروه طبق نتیجه ۱۶.۱۰، نرمال است. در نتیجه، هیچ گروه از مرتبه ۴۵ نمی‌تواند ساده باشد.

مثال ۱۲.۱۰. ثابت خواهیم کرد که هیچ گروه ساده از مرتبه $۵۶ = ۲^۳ \times ۷$ وجود ندارد. تنها شمارنده‌های ۵۶ به صورت $۷k + ۱$ اعداد ۱ و ۸ هستند، بنابراین G دارای یک یا هشت ۷−زیرگروه سیلو می‌باشد که هر کدام دارای مرتبه هفت هستند. اگر دقیقاً یک ۷−زیرگروه سیلو وجود داشته باشد، باید طبق نتیجه ۱۶.۱۰ نرمال باشد. پس در این حالت G ساده نیست. اگر G دارای هشت ۷−زیرگروه سیلو باشد. آنگاه هر کدام از آنها دارای شش عضو غیرهمانی است و طبق نتیجه ۳۴.۷، هر عضو غیرهمانی دارای مرتبه ۷ است. علاوه بر این، اشتراک هر دو تا از این زیرگروهها، طبق تمرین ۷ بخش ۸.۷، برابر $< e >$ است در نتیجه $۴۸ = ۶ \times ۸$ عضو از مرتبه ۷ در G وجود دارد. هر ۲−زیرگروه سیلوی G مرتبه ۸ دارد. طبق نتیجه ۳۴.۷، هر عضو یک ۲ـ زیرگروه سیلو باید مرتبه‌ای داشته باشد که ۸ را بشمارد و بنابراین نمی‌تواند در مجموعه ۴۸ عضوی باشد که مرتبه ۷ دارند، پس G می‌تواند تنها یک زیرگروه از مرتبه ۸ را شامل باشد. بنابراین در این حالت طبق نتیجه ۱۶.۱۰، تنها ۲ـ زیرگروه سیلوی از مرتبه ۸ نرمال است و G ساده نیست.

در مثال‌های قبل، قضایای سیلو مورد استفاده قرار گرفتند تا به نتایج منفی برسیم (گروه مورد نظر ساده نیست). ولی همان فنون می‌تواند منتج به دستاوردهای مثبت گردد. به ویژه این قضایا رده‌بندی کلاس‌های معینی از گروههای متناهی را تا حد یکریختی برای ما ممکن می‌سازد.

نتیجه ۱۸.۱۰. گیریم G یک گروه از مرتبه pq باشد، که در آن p و q اعداد اول هستند و $p > q$. اگر $q \nmid (p - ۱)$، در این صورت $G \cong \mathbb{Z}_{pq}$.

برهان. چون تنها شمارنده‌های $|G|$، ۱، p و q هستند، طبق سومین قضیه سیلو، ۱ یا q تا $p-$زیرگروه سیلو وجود دارد. ولی q به صورت $pk+1$ نیست زیرا $p>q$. پس یک $p-$زیرگروه سیلو یکتای H از مرتبه p وجود دارد، که طبق نتیجه ۱۶.۱۰ نرمال است. به طور مشابه یا ۱ یا p تا $q-$زیرگروه سیلو وجود دارد. چون $q \nmid (p-1)$، نمی‌توانیم داشته باشیم $p=1+qk$. پس یک $q-$ زیرگروه سیلو یکتای K از مرتبه q وجود دارد، که طبق نتیجه ۱۶.۱۰ نرمال است. چون $H\cap K$ یک زیرگروه از هر دو گروه H و K است طبق قضیه لاگرانژ مرتبه آن باید هر دو عدد $|H|=p$ و $|K|=q$ را بشمارد. بدین دلیل $H\cap K=<e>$. تمرین ۱۶ نشان می‌دهد که $G=HK$. بنابراین طبق قضیه ۳.۱۰، $G=H\times K$. اما طبق قضیه ۳۵.۷، $H\cong \mathbb{Z}_p$ و $K\cong \mathbb{Z}_q$. در نتیجه، طبق لم ۸.۱۰ [۹]، $G=H\times K\cong \mathbb{Z}_p\times \mathbb{Z}_q\cong Z_{pq}$. ■

مثال ۱۳.۱۰. اکنون رده‌بندی تمام گروههای از مرتبه $۳\times ۵=۱۵$ آسان است. نتیجه ۱۸.۱۰ را با شرط $p=۵$، $q=۳$ بکار برید تا نتیجه بگیرید که دقیقاً یک گروه از مرتبه ۱۵ تا حد یکریختی وجود دارد، و آن $\mathbb{Z}_{۱۵}$ است. به طور مشابه تنها یک گروه یکتا (تا حد یکریختی) برای هر یک از مرتبه‌های زیر وجود دارد:

$$۳۳=۱۱\times ۳,\quad ۳۵=۷\times ۵,\quad ۶۵=۱۳\times ۵,\quad ۷۷=۱۱\times ۷,\quad ۹۱=۱۳\times ۷.$$

این بخش را با قسمتی دیگر از مسئله رده‌بندی به پایان می‌رسانیم. چون که استدلال ما به یک قضیه از بخش آخر و یک تمرین از بخش بعد وابسته است، می‌توانید موقتاً این نتایج را باور نمایید.

مثال ۱۴.۱۰. تمام گروههای از مرتبه ۴۵ را تا حد یکریختی رده‌بندی خواهیم کرد. مثال ۱۱.۱۰ نشان می‌دهد که یک گروه G از مرتبه ۴۵ لزوماً دارای یک زیرگروه نرمال H از مرتبه ۹ است. این گروه G دارای یک ۵−زیرگروه سیلو یکتای K از مرتبه ۵ است زیرا عدد ۱ تنها شمارنده ۴۵ است که به شکل $5k+1$ است. این زیرگروه K طبق نتیجه ۱۶.۱۰ نرمال است. چون طبق قضیه لاگرانژ مرتبه $H\cap K$ باید اعداد $|H|=۹$ و $|K|=۵$ را بشمارد، $H\cap K=<e>$. تمرین ۱۶ نشان می‌دهد که $G=HK$. بنابراین طبق قضیه ۳.۱۰، $G=H\times K$. حال می‌دانیم که طبق قضیه ۳۴.۷، $K\cong \mathbb{Z}_۵$. تمرین ۱۲ از بخش بعد نشان می‌دهد که هر گروه از مرتبه $۳^۲$ آبلی است.

۹) برهان این لم مستقل از بقیه بخش ۲.۱۰ است، پس اگر آن بخش را نخوانده‌اید حالا می‌توانید این لم را مطالعه کنید.

در نتیجه طبق قضیه ۷.۱۰، H یکریخت با $\mathbb{Z}_9$ یا $\mathbb{Z}_3 \times \mathbb{Z}_3$ می‌باشد. بنابراین $G = H \times K$ یکریخت با $\mathbb{Z}_5 \times \mathbb{Z}_9$ یا $\mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ است.

تمرینها

توجه: G یک گروه متناهی و p عددی اول است، مگر خلاف آن ذکر شود.

۱.A. نشان دهید که S_4 دارای لااقل ۶۰ زیرگروه از مرتبه ۴ است [راهنمایی: زیرگروههای دوری پدیدآمده توسط یک ۴ـ دور (مثل $< (1234) >$)، یا پدیدآمده توسط حاصلضرب یک ۴-دور و یک ترانهش مجزا (مثل $< (56)(1234) >$) را در نظر بگیرید. همچنین به زیرگروههای غیردوری، مانند $\{(34)(12), (34), (12), (1)\}$ نگاه کنید.]

۲. (الف) سه، ۲-زیرگروه سیلو از S_4 را فهرست کنید.
(ب) چهار، ۳-زیرگروه سیلو از S_4 را فهرست کنید.

۳. ۲-زیرگروههای سیلو و ۳-زیرگروههای سیلوی A_4 را فهرست کنید.

۴. ۲-زیرگروههای سیلو، ۳-زیرگروههای سیلو و ۵-زیرگروههای سیلوی $\mathbb{Z}_{10} \times \mathbb{Z}_{12} \times \mathbb{Z}_{12}$ را فهرست کنید. [بخش ۲.۱۰ برای این تمرین یک پیشنیاز می‌باشد.]

۵. یک گروه G احتمالاً دارای چند p-زیرگروه سیلو است وقتی که

(الف) $p = 3$، $|G| = 72$ (ب) $p = 5$، $|G| = 60$.

۶. تمام گروههای از مرتبه داده شده را تا حد یکریختی رده‌بندی کنید:

(الف) ۱۱۵ (ب) ۱۴۳ (پ) ۳۹۱

۷. ثابت کنید که هیچ گروه ساده از مرتبه‌های داده شده وجود ندارد:

(الف) ۴۲ (ب) ۲۰۰ (پ) ۲۳۱ (ت) ۲۵۵

۸.B. یک گروه G (که لزوماً متناهی نیست) که در آن هر عضو دارای مرتبه توانی از عدد اول p است یک **p-گروه** نامیده می‌شود. از قضیه کشی استفاده کنید تا ثابت کنید که یک p-گروه متناهی، برای برخی $n \geq 0$، دارای مرتبه p^n است.

۹. اگر N یک زیرگروه نرمال یک گروه G (که لزوماً متناهی نیست) باشد و هر دو N و G/N، p-گروه باشند، آنگاه ثابت کنید که G یک p-گروه است.

۱۰. اگر f یک خودریختی از G و K یک p-زیرگروه سیلوی G باشد، آیا درست است که $f(K) = K$؟

۱۱. اگر K یک p-زیرگروه سیلوی G و H زیرگروه دلخواهی از G باشد، آیا $K \cap H$ یک p-زیرگروه سیلوی H است؟ [راهنمایی: S_4 را در نظر بگیرید.]

۱۲. گیریم K یک p-زیرگروه سیلوی G و N یک زیرگروه نرمال G باشد. ثابت کنید که $K \cap N$ یک p-زیرگروه سیلوی N است.

۱۳. اگر هر زیرگروه سیلوی G نرمال باشد، ثابت کنید که G حاصلضرب مستقیم زیرگروههای سیلوی خودش (یک عامل برای هر عدد اولی که $| G |$ را می‌شمارد) می‌باشد. یک گروه با این ویژگی **پوچتوان** نامیده می‌شود.

۱۴. اگر G یک گروه پوچتوان (تمرین ۱۳ را ملاحظه کنید) باشد، ثابت کنید که G دارای این ویژگی است که اگر m، $| G |$ را بشمارد، آنگاه G دارای یک زیرگروه از مرتبه m است. [می‌توانید تمرین ۲۳ بخش ۴.۱۰ را بپذیرید.]

۱۵. اگر G یک گروه غیردوری از مرتبه ۲۱ باشد، G چندتا ۳ـ زیرگروه سیلو دارد؟

۱۶. (الف) اگر H و K زیرگروههای G باشند، آنگاه HK مجموعه $\{hk \in G \mid h \in H, k \in K\}$ را نشان می‌دهد. اگر $H \cap K = < e >$، ثابت کنید که $| HK | = | H | \cdot | K |$. [راهنمایی: اگر $hk = h_1k_1$، آنگاه $h_1^{-1}h = kk_1^{-1}$.]

(ب) اگر H و K زیرگروههای دلخواه G باشند، ثابت کنید که

$$| HK | = (| H | \cdot | K |)/ | H \cap K | .$$

۱۷. اگر G یک گروه ساده از مرتبه ۱۶۸ باشد. ثابت کنید که G دارای هشت، ۷-زیرگروه سیلو می‌باشد.

۱۸. اگر p عددی اول باشد، ثابت کنید که هیچ گروه ساده از مرتبه $2p$ وجود ندارد.

۱۹. ثابت کنید که هیچ زیرگروه ساده از مرتبه ۳۰ وجود ندارد.

۲۰. اگر p و q اعداد اول متمایز باشند، ثابت کنید که هیچ گروه ساده از مرتبه p^2q وجود ندارد.

۲۱. اگر p، q، r اعداد اولی باشند که $p < q < r$، ثابت کنید یک گروه از مرتبه pqr دارای یک $r-$زیرگروه سیلوی نرمال است و بدین دلیل ساده نیست.

۲۲. (الف) اگر $|G| = ۱۰۵$. ثابت کنید که G دارای یک زیرگروه از مرتبه ۳۵ است.

(ب) اگر $|G| = ۳۷۵$، ثابت کنید که G دارای یک زیرگروه از مرتبه ۱۵ است.

۲۳.C ثابت کنید که هیچ گروه غیرآبلی ساده از مرتبه کمتر از ۶۰ وجود ندارد. [تمرین‌های ۱۲ و۲۳ بخش ۴.۱۰ را می‌توانید قبول کنید.]

۲۴. تمام گروههای از مرتبه ۲۱ را تا حدّ یکریختی رده‌بندی کنید.

۴-۱۰ کلاس‌های مزدوجی و برهان قضایای سیلو

پیشنیازهای این بخش قضیه لاگرانژ و نتایج آن، همراه با قضیه کُشی برای گروههای آبلی می‌باشد که تمام آنها در بخش ۸.۷ و پیوست ت آمده است. برهان قضایای سیلو بستگی زیادی به مفهوم کلاس‌های مزدوجی دارد، که اکنون به بسط آن می‌پردازیم.

گیریم G یک گروه باشد و $a, b \in G$. گوییم a **مزدوج** با b است اگر $x \in G$ وجود داشته باشد به طوری که $b = x^{-1}ax$. برای مثال، ترانهش (۱۲) مزدوج (۱۳) در S_3 است زیرا

$$(۱۲۳)^{-1}(۱۲)(۱۲۳) = (۱۳۲)(۱۲)(۱۲۳) = (۱۳).$$

واقعیت کلیدی در مورد رابطه مزدوجی قضیه زیر است.

قضیه ۱۹.۱۰. رابطه مزدوجی یک رابطه هم‌ارزی در G است.

برهان. اگر a مزدوج b باشد می‌نویسیم، $a \sim b$. انعکاسی: چون $a = eae = e^{-1}ae$، پس $a \sim a$. متقارن: اگر $a \sim b$، آنگاه برای یک x در G، $b = x^{-1}ax$. از ضرب x از طرف چپ و x^{-1} از طرف راست بدست می‌آید $a = xbx^{-1} = (x^{-1})^{-1}bx^{-1}$. بدین دلیل $b \sim a$. متعدّی: اگر $a \sim b$ و $b \sim c$، آنگاه برای برخی $x, y \in G$، $b = x^{-1}ax$ و $c = y^{-1}by$. پس $c = y^{-1}(x^{-1}ax)y = (y^{-1}x^{-1})a(xy) = (xy)^{-1}a(xy)$. در نتیجه $a \sim c$ و بنابراین $\sim$ یک رابطه هم‌ارزی است. ■

رده‌های هم‌ارزی در G تحت رابطه مزدوجی **رده‌های مزدوجی** نامیده می‌شود. مبحث رابطه‌های هم‌ارزی در پیوست ت نشان می‌دهد که

- رده مزدوجی یک عضو a شامل تمام عضوهایی در G است که مزدوج با a است.
- دو رده مزدوجی یا مجزا هستند یا برابر.
- گروه G اجتماع تمام رده‌های مزدوجی متمایزش می‌باشد.

مثال ۱۰.۱۵. رده مزدوجی (۲ ۱) در $S_۳$ مشتمل بر تمام عناصر به صورت $x^{-۱}(۱۲)x$ با شرط $x \in S_۳$، می‌باشد. محاسبه‌ای ساده نشان می‌دهد که به ازاء هر $x \in S_۳$، $x^{-۱}(۱۲)x$ یکی از عناصر (۱۲)، (۱۳)، یا (۲۳) می‌باشد: برای مثال،

$$(۲۳)^{-۱}(۱۲)(۲۳) = (۲۳)(۱۲)(۲۳) = (۱۳)$$
$$(۱۳۲)^{-۱}(۱۲)(۱۳۲) = (۱۲۳)(۱۲)(۱۳۲) = (۲۳).$$

بنابراین $\{(۱), (۱۳), (۲۳)\}$ رده هم‌ارزی (۱۲) می‌باشد. محاسبات مشابهی نشان می‌دهد که سه رده مزدوجی مجزا در $S_۳$ وجود دارد:

$$\{(۱)\}, \quad \{(۱۲۳), (۱۳۲)\}, \quad \{(۱۲), (۱۳), (۲۳)\}.$$

اگرچه این رده‌های مزدوجی اندازه‌های مختلفی دارند، توجه کنید که تعداد عضوهای هر رده مزدوجی (۱، ۲ یا ۳) شمارنده‌ای از ۶، مرتبه $S_۳$ است. بزودی خواهیم دید که در حالت کلی نیز این پدیده بخوبی برقرار است.

گیریم G یک گروه باشد و $a \in G$. **مرکزساز** a با $C(a)$ نمایش داده می‌شود و مشتمل بر تمام عناصری از G است که با a جابجا می‌شوند، یعنی

$$C(a) = \{g \in G \mid ga = ag\}.$$

اگر برای مثال، $G = S_۳$ و $a = (۱۲۳)$، به سادگی می‌توانید بررسی کنید که $C(a) = \{(۱), (۱۲۳), (۱۳۲)\}$. اگر a یک عدد غیرصفر گویا در گروه ضربی $\mathbb{Q}^*$ باشد، هر عضو $\mathbb{Q}^*$ با a جابجا می‌شود، بنابراین $C(a)$ تمام گروه $\mathbb{Q}^*$ است. این مثال‌ها، مثال‌هایی تشریحی

از قضیه زیر می‌باشند.

قضیه ۲۰.۱۰. اگر G یک گروه باشد و $a \in G$، آنگاه این صورت $C(a)$ یک زیرگروه G است.

برهان. اگر $g, h \in C(a)$، در این صورت

$$(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh).$$

بنابراین $gh \in C(a)$ و $C(a)$ بسته است. از ضرب طرفین $ga = ag$ از چپ و راست در g^{-1} ثابت می‌شود که $ag^{-1} = g^{-1}a$. بدین دلیل $g \in C(a)$ ایجاب می‌کند که $g^{-1} \in C(a)$. بنابراین طبق قضیه ۷.۷، $C(a)$ یک زیرگروه است. ■

مفهوم مرکزساز به یک واقعیت بسیار مفید درباره اندازه رده‌های مزدوجی می‌انجامد:

قضیه ۲۱.۱۰. گیریم G یک گروه باشد و $a \in G$. تعداد مزدوج‌های متمایز a (یعنی تعداد عناصر واقع در رده مزدوجی a) برابر با $[G : C(a)]$، شاخص $C(a)$ در G است، و بنابراین $|G|$ را می‌شمارد.

برهان. $C(a)$ را با C نشان دهید و فرض کنید $x, y \in G$. در این صورت

$$\begin{aligned}
x^{-1}ax = y^{-1}ay &\iff a = xy^{-1}ayx^{-1} && \text{[از طرف چپ در } x \text{ و از طرف راست در } x^{-1} \text{ ضرب کنید]} \\
&\iff a = (yx^{-1})^{-1}ayx^{-1} && \text{[نتیجه ۳.۷]} \\
&\iff (yx^{-1})a = ayx^{-1} && \text{[از طرف چپ در } yx^{-1} \text{ ضرب کنید]} \\
&\iff yx^{-1} \in C && \text{[تعریف } C\text{]} \\
&\iff Cy = Cx. && \text{[قضیه ۱۸.۷]}
\end{aligned}$$

بنابراین x و y مزدوج یکسانی از a را ایجاد می‌کنند اگر و تنها اگر x و y در یک هم‌مجموعه C باشند. به طور معادل، اگر x و y در هم مجموعه‌های متفاوتی از C باشند، در این صورت $x^{-1}ax \neq y^{-1}ay$. حال G اجتماع هم‌مجموعه‌های متمایز C است، مثلاً $G = Cx_1 \cup Cx_2 \cup \cdots \cup Cx_t$، و مزدوج‌های a تمام عناصر به صورت $z^{-1}az$ است، که z در G تغییر می‌کند. پس مزدوج‌های مجزای a، t عضو

$$x_1^{-1}ax_1, x_2^{-1}ax_2, x_3^{-1}ax_3, \ldots, x_t^{-1}ax_t$$

خواهند بود. ولی t برابر با تعداد هم‌مجموعه‌های متمایز C در G یعنی $[G : C]$ می‌باشد. این شاخص طبق قضیه لاگرانژ، قضیه ۳۳.۷، $|G|$ را می‌شمارد. ■

گیریم G یک گروه متناهی باشد و $C_1, C_2, \cdots, C_t$ رده‌های مزدوجی متمایز G باشند. آنگاه $G = C_1 \cup C_2 \cup \cdots \cup C_t$. چون رده‌های مزدوجی متمایز دوبدو مجزا هستند،

$$|G| = |C_1 \cup C_2 \cup \cdots \cup C_t| = |C_1| + |C_2| + \cdots + |C_t|, \qquad (۱)$$

که در آن $|C_i|$ تعداد عناصر رده C_i است. اکنون یک عضو مثل a_i در هر رده C_i انتخاب کنید. در این صورت C_i متشکل از تمام مزدوج‌های a_i است. طبق قضیه ۲۱.۱۰، $|C_i|$ دقیقاً برابر است با $[G : C(a_i)]$ که شمارنده‌ای از $|G|$ است. بنابراین معادله (۱) به صورت

$$|G| = [G : C(a_1)] + [G : C(a_2)] + \cdots + [G : C(a_t)] \qquad (۲)$$

درمی‌آید. این معادله (به صورت (۱) یا (۲)) **معادله رده‌ای** G نامیده می‌شود. این معادله ابزار اساسی برای اثبات قضایای سیلو خواهد بود. کاربردهای دیگر معادله رده‌ای G، نظیر این واقعیت که هر گروه از مرتبه p^2 (p اول) آبلی است، در تمرین‌های ۱۱ و ۱۲ مطرح می‌گردد.

مثال ۱۰.۱۶. در مثال بعد از قضیه ۱۹.۱۰ دیدیم که S_3 سه رده مزدوجی متمایز به اندازه‌های ۱، ۲ و ۳ دارد. چون $|S_3| = 6$، معادله رده‌ای S_3 برابر با $6 = 1 + 2 + 3$ می‌باشد.

بخاطر آورید که مرکز G مجموعه $Z(G)$ مشتمل بر آن عناصری از G است که با هر عضو G جابجا می‌شود، یعنی

$$Z(G) = \{c \in G \mid cx = xc \quad \text{برای هر } x \in G\}.$$

طبق تمرین ۸ بخش ۵.۷، $Z(G)$ یک زیرگروه آبلی نرمال از G است [۱۰]. ملاحظه کنید که $cx = xc$ اگر و تنها اگر $x^{-1}cx = c$. بنابراین c در مرکز G است اگر و تنها اگر c دقیقاً یک مزدوج (یعنی خودش) داشته باشد. در نتیجه، $Z(G)$ اجتماع رده‌های مزدوجی تک عضوی G است، و **معادله رده‌ای** G را می‌توان به صورت

$$|G| = |Z(G)| + |C_1| + |C_2| + \cdots + |C_r| \qquad (۳)$$

۱۰) گروه G آبلی است اگر و تنها اگر $G = Z(G)$.

نوشت، که در آن C_1، ...، C_r رده‌های مزدوجی متمایز G هستند که هر کدام بیشتر از یک عضو دارند و هر $|C_i|$، $|G|$ را می‌شمارد.

اکنون تمام ابزارهای لازم برای اثبات اولین قضیه سیلو را داریم:

برهان اولین قضیه سیلو، قضیه ۱۳.۱۰. برهان با استفاده از استقراء روی مرتبه G است. اگر $|G|=1$ آنگاه p^0 تنها توان اولی است که $|G|$ را می‌شمارد، و G خودش یک زیرگروه از مرتبه p^0 است. فرض کنید $|G|>1$ و به استقراء فرض کنید که قضیه برای تمام گروههای از مرتبه کمتر از $|G|$ درست باشد. از ترکیب صورت‌های دوم و سوم معادله رده‌ای G ثابت می‌شود که

$$|G| = |Z(G)| + [G : C(a_1)] + [G : C(a_2)] + \cdots + [G : C(a_r)]$$

که در آن برای هر i، $[G : C(a_i)] > 1$. به علاوه، $|Z(G)| \geq 1$ (چون $e \in Z(G)$)، و $|C(a_i)| < |G|$ (در غیر این صورت، $[G : C(a_i)] = 1$).

فرض کنید که نمایهٔ j وجود داشته باشد به طوری که p، $[G : C(a_j)]$ را نشمارد. آنگاه p^k باید $|C(a_j)|$ را بشمارد زیرا طبق فرض p^k، $|G|$ را می‌شمارد و طبق قضیه لاگرانژ $[G : C(a_j)] \cdot |C(a_j)| = |G|$. چون زیرگروه $C(a_j)$ دارای مرتبه کمتر از $|G|$ می‌باشد، فرض استقراء ایجاب می‌کند که $C(a_j)$، و بدین دلیل G زیرگروهی از مرتبه p^k داشته باشد.

از طرف دیگر، اگر برای هر i، p، $[G : C(a_i)]$ را بشمارد، آنگاه چون p، $|G|$ را می‌شمارد، همچنین p باید

$$|G| - [G : C(a_1)] - \cdots - [G : C(a_r)] = |Z(G)|$$

را بشمارد. چون $|Z(G)|$ آبلی است، طبق قضیه ۳۸.۷، $Z(G)$ شامل یک عضو c از مرتبه p است. گیریم N زیرگروه دوری پدید آمده توسط c باشد، آنگاه N دارای مرتبه p است و در G نرمال است (تمرین ۸). در نتیجه، مرتبه گروه خارج قسمت G/N، یعنی $|G|/p$، کمتر از $|G|$ و بر p^{k-1} بخش‌پذیر است. طبق فرض استقراء G/N یک زیرگروه T از مرتبه p^{k-1} دارد. طبق قضیه ۳۱.۷، زیرگروه H از G وجود دارد به طوری که $N \subseteq H$ و $T = H/N$. قضیه لاگرانژ نشان می‌دهد که

$$|H| = |N| \cdot |H|/|N| = |N| \cdot |T| = pp^{k-1} = p^k.$$

پس در این حالت نیز G دارای یک زیرگروه از مرتبه p^k است. ■

ابزارهای اساسی مورد نیاز برای اثبات دو قضیه سیلوی دیگر خیلی شبیه آنهایی است که در بالا استفاده شد. بجز آن که به جای عضوهای مزدوج با زیرگروههای مزدوج سروکار خواهیم داشت. دقیقتر بگوییم، گیریم H زیرگروهی ثابت از گروه G باشد و فرض کنیم A و B زیرگروههای دلخواهی از G باشند. گوییم A، H-**مزدوج** با B است اگر یک $x \in H$ وجود داشته باشد به طوری که

$$B = x^{-1}Ax = \{x^{-1}ax \mid a \in A\}.$$

در حالت خاص وقتی H خود گروه G باشد به سادگی می‌گوییم که A مزدوج B است.

قضیه ۲۲.۱۰. گیریم H زیرگروهی از گروه G باشد. در این صورت رابطه H-مزدوجی یک رابطه هم‌ارزی روی مجموعه تمام زیرگروههای G است.

برهان. برهان قضیه ۱۹.۱۰ را تطبیق کرده، بجای a، b و c زیرگروههای A، B و C را بکار برید. ■

گیریم A زیرگروهی از گروه G باشد. **نرمالساز** A مجموعه $N(A)$ است که توسط

$$N(A) = \{g \in G \mid g^{-1}Ag = A\}$$

تعریف می‌شود. بررسی این که $A \subseteq N(A)$ ساده است (تمرین ۷).

قضیه ۲۳.۱۰. اگر A زیرگروهی از گروه G باشد، آنگاه $N(A)$ زیرگروهی از G است و A یک زیرگروه نرمال $N(A)$ است.

برهان. اگر $a, a_1 \in A$، آنگاه $g^{-1}ag = a_1$ اگر و تنها اگر $ag = ga_1$. در نتیجه، $g \in N(A)$ اگر و تنها اگر $Ag = gA$. با استفاده از این واقعیت، برهان قضیه ۲.۱۰ را می‌توان به سادگی تطبیق کرد تا ثابت کنیم که $N(A)$ یک زیرگروه است. تعریف $N(A)$ نشان می‌دهد که A نرمال در $N(A)$ است. ■

قضیه ۲۴.۱۰. گیریم H و A زیرگروههایی از یک گروه متناهی G باشند. تعداد H-مزدوجهای مجزای A (یعنی، تعداد عناصر در رده هم‌ارزی A تحت رابطه H-مزدوجی) برابر $[H : H \cap N(A)]$

است و بنابراین $|H|$ را می‌شمارد.

برهان. چنانچه به جای G، a و C به ترتیب H، A و $H \cap N(A)$ را قرار دهید، آنگاه برهان قضیه ۲۱.۱۰ قابل تطبیق به وضعیت حاضر است. ■

لم ۲۵.۱۰. گیریم Q یک p–زیرگروه سیلوی یک گروه متناهی G باشد. اگر $x \in G$ دارای مرتبه توانی از p باشد و $x^{-1}Qx = Q$، در این صورت $x \in Q$.

برهان. چون طبق قضیه ۲۳.۱۰، Q در $N(Q)$ نرمال است، گروه خارج قسمت $N(Q)/Q$ تعریف شده است. طبق فرض، $x \in N(Q)$. چون $|x|$ توانی از p است، هم مجموعه Qx در $N(Q)/Q$ نیز دارای توانی از p است. اکنون Qx یک زیرگروه دوری T از $N(Q)/Q$ است را تولید می‌کند که مرتبه‌اش توانی از p است. طبق قضیه ۳۱.۷، $T = H/Q$، که در آن H زیرگروهی از G است که Q را شامل است. چون مرتبه‌های گروههای Q و T هر کدام توانی از p است و طبق قضیه لاگرانژ $|T| \cdot |Q| = |H|$ لذا $|H|$ باید توانی از p باشد. ولی $Q \subseteq H$ و طبق تعریف p–زیرگروه سیلو، $|Q|$ بزرگترین توانی از p است که $|G|$ را می‌شمارد. بنابراین $Q = H$، و بدین دلیل $T = H/Q$ زیرگروه همانی است. پس مولد Qx از T باید هم‌مجموعه همانی Qe باشد. تساوی $Qx = Qe$ ایجاب می‌کند که $x \in Q$. ■

برهان قضیه دوم سیلو، قضیه ۱۵.۱۰. چون K یک p–زیرگروه سیلو است، K دارای مرتبه p^n است جایی که $|G| = p^n m$ و $p \nmid m$. گیریم $K = K_1, K_2, \ldots, K_t$ مزدوج‌های مجزای K در G باشند. طبق قضیه ۲۴.۱۰ (با شرط $H = G$ و $K = A$)، $t = [G : N(K)]$. توجه کنید که t، p را نمی‌شمارد [دلیل: $t \cdot |N(K)| = [G : N(K)] \cdot |N(K)| = |G| = p^n m$ و p^n، $|N(K)|$ را می‌شمارد زیرا K زیرگروه $N(K)$ است]. باید ثابت کنیم که p–زیرگروه سیلوی P، مزدوج K است، یعنی این که P یکی از K_iهاست. برای انجام این کار از رابطه P–مزدوجی استفاده می‌کنیم.

چون هر K_i مزدوج K_1 و رابطه مزدوجی، متعدی است، هر مزدوج K در G با K_1 نیز مزدوج است. به بیان دیگر هر مزدوج، K_i یک K_j است. در نتیجه، رده هم‌ارزی K_i تحت رابطه P–مزدوجی فقط K_jهای گوناگون را شامل است. بنابراین مجموعه $S = \{K_1, K_2, \ldots, K_t\}$ از تمام مزدوج‌های K، اجتماعی از رده‌های هم‌ارزی متمایز تحت رابطه P–مزدوجی است. تعداد زیرگروهها

در هر کدام از این رده‌های هم‌ارزی توانی از p است زیرا طبق قضیه ۲۴.۱۰، تعداد زیرگروههایی که P–مزدوج با K_i است برابر با $[P : P \cap N(K_i)]$ می‌باشد، که طبق قضیه لاگرانژ شمارنده‌ای از $|P| = p^n$ است. بنابراین t (تعداد زیرگروههای واقع در S) مجموع توانهای مختلف p است (که هر کدام از این توانها برابر تعداد زیرگروههای واقع در رده‌های هم‌ارزی متمایزی است که اجتماع آنها S است). چون p، t را نمی‌شمارد، لااقل یکی از این توانهای p باید، $p^0 = 1$ باشد. بدین ترتیب یکی از K_iها در یک رده هم‌ارزی با خودش می‌باشد، یعنی این که برای هر $x \in P$، $x^{-1}K_i x = K_i$. لم ۲۵.۱۰ (با شرط $Q = K_i$) ایجاب می‌کند که برای تمام این xها، $x \in K_i$، لذا $P \subseteq K_i$. چون هر دوی P و K_i، p–زیرگروه سیلو هستند، دارای مرتبه یکسان می‌باشند. بدین دلیل $P = K_i$. ■

برهان سومین قضیه سیلو، قضیه ۱۷.۱۰. گیریم $S = \{K_1, \ldots, K_t\}$ مجموعه تمام p–زیرگروههای سیلوی G باشد. طبق دومین قضیه سیلو، تمام آنها با K_1 مزدوج می‌باشند، گیریم P یکی از این K_iها باشد و رابطه P–مزدوجی را در نظر بگیرید. طبق اصل بسته‌بودن تنها P–مزدوج P خود P است. برهان دومین قضیه سیلو نشان می‌دهد که تنها رده هم‌ارزی که مشتمل بر تنها یک زیرگروه است، رده‌ای است که شامل خود P باشد. همان برهان هم نشان می‌دهد که S اجتماع رده‌های هم‌ارزی متمایز است و این که تعداد زیرگروههای واقع در هر رده، توانی از p می‌باشد. تنها یکی از این رده‌ها شامل P است، پس تعداد زیرگروههای در هر یک از رده‌های دیگر توانی مثبت از p است. بدین‌دلیل عدد t یعنی تعداد p–زیرگروههای سیلو برابر با مجموع عدد ۱ و توانهای مثبت مختلف p است و بنابراین می‌توان آن را به صورت $kp + 1$، برای یک عدد صحیح k، نوشت. ■

تمرینها

توجه: G یک گروه متناهی و p عددی اول است، مگر خلاف آن ذکر شود.

۱.A. تمام رده‌های مزدوجی متمایز گروه داده شده را فهرست کنید.

(الف) D_4 (ب) S_4 (پ) A_4

۲. اگر $a \in G$، در این صورت با مثال نشان دهید که $C(a)$ ممکن است آبلی نباشد. [راهنمایی: اگر در S_5، $a = (12)$، در این صورت (34) و (345) در $C(a)$ هستند.]

۳. اگر H زیرگروهی از G باشد و $a \in H$، با مثال نشان دهید که رده مزدوجی a در H ممکن

است همان رده مزدوجی a در G نباشد.

۴. مرکز S_4 چیست؟ [جواب خود را با تمرین ۱۱ مقایسه کنید.]

۵. تمام مزدوج‌های ۳ـ گروه سیلوی $< (۱۲۳) >$ در S_4 را فهرست کنید.

۶. اگر H و K زیرگروههایی از G و H نرمال در K باشد ثابت کنید که K زیرگروهی از $N(H)$ است. به بیان دیگر، $N(H)$ بزرگترین زیرگروه G است که H زیرگروه نرمال آن است.

۷. اگر A زیرگروهی از G باشد، ثابت کنید که A زیرگروه $N(A)$ است.

۸. اگر N زیرگروهی از $Z(G)$ باشد، ثابت کنید که N زیرگروه نرمال G است.

۹.B. اگر C یک رده مزدوجی در G و f یک خودریختی از G باشد، ثابت کنید که $f(C)$ نیز یک رده مزدوجی G است.

۱۰. گیریم G یک گروه نامتناهی باشد و H مجموعه تمام عضوهای G باشد که دارای فقط تعداد متناهی مزدوج متمایز در G هستند. ثابت کنید که H زیرگروهی از G است.

۱۱. اگر $| G | = p^n$، ثابت کنید $| Z(G) | \geq p$. [راهنمایی: صورت سوم معادله رده‌ای G نشان می‌دهد که $| G | - | C_1 | - \cdots - | C_r | = | Z(G) |$، که در آن هر $| C_i |$ شمارنده‌ای از $| G |$، بزرگتر از ۱ می‌باشد.]

۱۲. ثابت کنید که هر گروه از مرتبه p^2 آبلی است. [راهنمایی: طبق تمرین ۱، $Z(G)$ دارای مرتبه p^2 یا p است. در حالت دوم، $G/Z(G)$ و قضیه ۲۵.۷ را در نظر بگیرید.]

۱۳. گیریم K یک $p-$زیرگروه سیلوی G و N زیرگروهی نرمال از G باشد. اگر K یک زیرگروه نرمال N باشد، ثابت کنید که K در G نرمال است.

۱۴. گیریم N زیرگروهی نرمال از G، $a \in G$ و C رده مزدوجی a در G باشد.

(الف) ثابت کنید که $a \in N$ اگر و تنها اگر $C \subseteq N$.

(ب) اگر C_i رده مزدوجی دلخواهی در G باشد، ثابت کنیدکه $C_i \subseteq N$ یا $C_i \cap N = \emptyset$.

(پ) با استفاده از معادله رده‌ای ثابت کنید که $| N | = | C_1 | + \cdots + | C_k |$، که در آن C_1، ...، C_k همهٔ آن رده‌های مزدوجی G هستند که در N قرار دارند.

۱۵. اگر $N \neq < e >$ زیرگروهی نرمال از G باشد و $|G| = p^n$، ثابت کنید که $N \cap Z(G) \neq < e >$. [راهنمایی: تمرین ۱۴ (پ) می‌تواند مفید باشد.]

۱۶. قضیه ۲۲.۱۰ را ثابت کنید.

۱۷. برهان قضیه ۲۳.۱۰ را تکمیل کنید.

۱۸. قضیه ۲۴.۱۰ را ثابت کنید.

۱۹. اگر K یک p-زیرگروه سیلوی G باشد، ثابت کنید که $N(N(K)) = N(K)$.

۲۰. اگر K یک p-زیرگروه سیلوی G باشد و H زیرگروهی باشد که $N(K)$ را شامل است، ثابت کنید که (پیمانه p) $[G : H] \equiv ۱$.

۲۱. اگر H زیرگروهی نرمال از G و $|H| = p^k$، ثابت کنید که H در هر p-زیرگروه سیلوی G قرار دارد. [می‌توانید تمرین ۲۵ را بپذیرید.]

۲۲. اگر H زیرگروهی سره از G باشد، ثابت کنید که G اجتماع تمام مزدوج‌های H نمی‌باشد. [راهنمایی: بخاطر آورید که H زیرگروهی نرمال از $N(H)$ است، قضیه ۲۴.۱۰ می‌تواند مفید باشد.]

۲۳.C. اگر $|G| = p^n$، ثابت کنید که G دارای زیرگروهی نرمال از مرتبه $p^{n-۱}$ است. [راهنمایی: از استقراء روی n استفاده کنید. فرض کنید $N =< a >$، که در آن $a \in Z(G)$ دارای مرتبه p است (چرا چنین aای وجود دارد؟)، در این صورت G/N زیرگروهی از مرتبه $p^{n-۲}$ دارد. از قضیه ۳۱.۷ استفاده کنید.]

۲۴. اگر $|G| = p^n$، ثابت کنید که هر زیرگروه G از مرتبه $p^{n-۱}$ نرمال است.

۲۵. اگر H زیرگروهی از G و H دارای مرتبه توانی از p باشد، ثابت کنید که H در یک p-زیرگروه سیلوی G قرار دارد. [راهنمایی: مانند برهان‌های قضایای دوم و سوم سیلو پیش بروید ولی بجای رابطه P-مزدوجی از رابطه H-مزدوجی روی مجموعه تمام p-زیرگروههای سیلو $\{K_۱, \ldots, K_t\}$ استفاده کنید.]

۱۰-۵ ساده‌بودن A_n

همانگونه که در بحث بعد از نتیجه ۴۰.۷ متذکر شدیم بنظر می‌رسد که گروههای ساده راه‌حل مسئله رده‌بندی برای گروههای متناهی باشد. نخستین رده بزرگ گروههای ساده غیرآبلی اوایل قرن نوزدهم توسط گالوا کشف شد. این رده مشتمل بر گروههای متناوب A_n (با شرط $n \geq 5$) می‌باشد. در این بخش برهانی مقدماتی از سادگی A_n ارائه می‌کنیم. این برهان فقط به حقایق اساسی در مورد نرمال‌بودن (بخش ۵.۷) و خواص گروههای متقارن (بخش ۹.۷) بستگی دارد.

چون در متن اثبات با محاسبات متعددی در مورد دورها مواجه می‌شویم، بی‌مناسبت نیست تا پیش از ادامه کار، عمل ضرب دورها در S_n را بازنگری کنیم. مثال‌های زیادی وجود دارد که با جایگشت‌هایی مانند $(abcd)$ یا $(a2b)$ یا $(ab)(cd)$ سروکار خواهیم داشت. در تمام این حالات

حروف متمایز عضوهای متمایز $\{1, 2, \ldots, n\}$ را نشان می‌دهد.

توصیه می‌شود که: هنگام خواندن برهان، نگران این نباشید که چگونه انجام یک ضرب بخصوص پیشنهادشده است؛ فقط بررسی کنید که تساوی داده شده درست است.

بیاد آورید که A_n زیرمجموعه گروه متقارن S_n مشتمل بر تمام جایگشت‌های زوج (جایگشت‌هایی که می‌توان آنها را به صورت حاصل‌ضرب تعدادی زوج از ترانهش‌ها نوشت) می‌باشد. طبق قضیه ۴۸.۷، A_n زیرگروهی نرمال از S_n از مرتبه $n!/2$ و دارای شاخص ۲ می‌باشد. هر ۳-دور (abc) در A_n واقع است زیرا $(abc) = (ac)(ab)$. در واقع ۳-دورها A_n را پدید می‌آورند:

لم ۲۶.۱۰. هر عضو A_n (با شرط $n \geq 3$) حاصل‌ضربی از ۳ـ دورهاست.

برهان. بنابه تعریف، هر عضو A_n یک حاصل‌ضرب از جفت‌هایی از ترانهش‌ها می‌باشد. ولی هر چنین جفتی باید به یکی از این سه صورت باشد: $(ab)(cd)$ یا $(ab)(ac)$ یا $(ab)(ab)$. بررسی کنید که در حالت اول $(ab)(cd) = (adb)(adc)$، در حالت دوم $(ab)(ac) = (acb)$، و در حالت آخر $(ab)(ab) = (1) = (abc)(acb)$. بدین ترتیب هر جفت از ترانهش‌ها یا یک ۳ـ دور است یا حاصل‌ضربی از دو تا ۳ـ دور است. بدین دلیل هر حاصل‌ضربی از جفت‌هایی از ترانهش‌ها حاصل‌ضربی از ۳ـدورهاست. ■

حقیقت کلیدی در اثبات این که A_n ساده است واقعیت زیر درباره ۳ـ دورهاست.

لم ۲۷.۱۰. اگر N زیرگروهی نرمال از $A_n (n \geq ۳)$ باشد و N شامل یک ۳ـ دور باشد، در این صورت $N = A_n$.

برهان. برای راحتی در بکارگیری علائم، فرض کنید که $(۱۲۳) \in N$ [استدلال برای وقتی که N یک ۳–دور دلخواه (rst) را شامل باشد عیناً یکی است، بترتیب ۱، ۲، ۳ را با r، s، t عوض کنید]. چون $(۱۲۳) \in N$، ملاحظه می‌کنیم که $(۱۲۳)(۱۲۳) = (۱۳۲)$ نیز در N است. برای $k \geq ۴$، گیریم $x = (۱۲)(۳k)$ و تحقیق کنید که $x^{-۱} = (۳k)(۱۲)$. بنابر قضیه ۲۱.۷ (با شرط $a = x^{-۱}$) نرمال بودن N ایجاب می‌کند که $x(۱۳۲)x^{-۱} \in N$. اما

$$x(۱۳۲)x^{-۱} = (۱۲)(۳k)(۱۳۲)(۳k)(۱۲) = (۱۲k).$$

بنابراین

N تمام ۳–دورهای به صورت $(۱۲k)$ با شرط $k \geq ۳$ را شامل است. $(*)$

بررسی کنید که هر ۳ـ دور دیگر را می‌توان به یکی از این صورت‌ها نوشت:

$$(abc), \quad (۲ab), \quad (۱ab), \quad (۱a۲),$$

که در آن $a, b, c \geq ۳$. طبق $(*)$ و خاصیت بسته بودن N،

$$(۱a۲) = (۱۲a)(۱۲a) \in N;$$
$$(۱ab) = (۱۲b)(۱۲a)(۱۲a) \in N;$$
$$(۲ab) = (۱۲b)(۱۲b)(۱۲a) \in N;$$
$$(abc) = (۱۲a)(۱۲a)(۱۲c)(۱۲b)(۱۲b)(۱۲a) \in N.$$

بنابراین N تمام ۳ـ دورها را شامل است و بدین دلیل N طبق خاصیت بسته بودن، تمام حاصل‌ضرب‌های ۳-دورها را شامل است. بنابراین طبق لم ۲۶.۱۰، $N = A_n$. ■

اکنون در جایگاهی هستیم که ساده‌بودن A_n را اثبات کنیم. برای فهم برهان آن، لازم است بخاطر آورید که وارون دور $(a_۱a_۲ \cdots a_k)$ برابر $(a_۱a_k a_{k-۱} \cdots a_۲a_۲)$ است. برای مثال می‌توانید به‌سادگی بررسی کنید که $(۱۵۴۳۲) = (۱۲۳۴۵)^{-۱}$ و $(۶۸۷) = (۶۷۸)^{-۱}$. همچنین بیادآورید

که دو دور را **مجزا** گویند اگر آنها هیچ نمادمشترکی نداشته باشند، برای مثال، (۱۳۵) و (۲۴۶۹۷) مجزا هستند. هر جایگشت حاصل‌ضربی از دورهای مجزا می‌باشد (قضیه ۴۳.۷). اگر σ و τ دورهای مجزا باشند، در این صورت طبق تمرین ۱۲ از بخش ۹.۷، $\sigma\tau = \tau\sigma$.

قضیه ۲۸.۱۰. برای هر $n \geq 5$، گروه تناوبی A_n یک گروه ساده غیرآبلی است.
A_2 و A_3 گروههای ساده آبلی هستند (تمرین ۲)، و A_4 ساده نیست (تمرین ۱۰).

برهان قضیه ۲۸.۱۰. باید ثابت کنیم که A_n هیچ زیرگروه نرمال سره ندارد. گیریم N زیرگروه نرمال دلخواهی از A_n، با شرط $N \neq (1)$، باشد. فقط لازم است ثابت کنیم $N = A_n$. وقتی که هر عنصر غیرهمانی N به صورت دورهای مجزا نوشته شود، آنگاه سه احتمال برای طول این دورها وجود دارد:

۱. بعضی از دورها طول ≤ 4 دارند.
۲. هر دور طول ≥ 3 دارد، و بعضی طول ۳ دارند.
۳. هر دور طول ≥ 2 دارد.

نشان می‌دهیم که در هرکدام از این حالات $N = A_n$.

حالت ۱ N یک عضو σ دارد که حاصل‌ضربی از دورهای مجزاست، که دست کم یکی از آن‌ها طول $r \geq 4$ دارد. برای راحتی در استفاده از نمادها فرض می‌کنیم $\sigma = (123\cdots r)\tau$ که در آن τ حاصل‌ضربی از دورهای مجزاست که هیچکدام از آنها شامل نمادهای ۱، ۲، ۳، ...، r نیست.[11] عنصر $\delta = (123) \in A_n$ را در نظر بگیرید. چون N یک زیرگروه نرمال است و $\sigma \in N$، طبق قضیه ۲۱.۷ (با شرط $a = \delta^{-1}$)، $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$. با استفاده از نتیجه ۳.۷ و این واقعیت که دورهای مجزا جابجا می‌شوند، داریم

$$\begin{aligned}\sigma^{-1}(\delta\sigma\delta^{-1}) &= [(1234\cdots r)\tau)]^{-1}(123)[(1234\cdots r)\tau](123)^{-1}\\ &= \tau^{-1}(1r\cdots 432)(123)(1234\cdots r)\tau(132)\\ &= \tau^{-1}\tau(1r\cdots 432)(123)(1234\cdots r)(132) = (13r).\end{aligned}$$

۱۱) همین استدلال با یک r–دور دلخواه $(abcd\ldots t)$ بجای $(123\ldots r)$ نیز کار می‌کند، فقط ۱ را با a، ۲ را با b، و غیره تعویض کنید. این تذکر در حالات دیگری نیز که ما برای سادگی در تعقیب استدلال از دورهای مشخصی استفاده می‌کنیم، مفید است.

بنابراین $N \in (۱۳۲)$، و بدین دلیل طبق لم ۲۷.۱۰، $N = A_n$.

حالت ۲ الف N یک عنصر σ دارد که حاصل‌ضرب دورهای مجزا می‌باشد، که لااقل دو تا از آنها طول ۳ دارند. برای راحتی فرض می‌کنیم که $\sigma = (۱۲۳)(۴۵۶)\tau$ که در آن τ حاصل‌ضربی از دورهای مجزا می‌باشد، که هیچکدام شامل نمادهای ۱، ۲، ۳، ...، ۶ نیست[۱۲]. عنصر $\delta = (۱۲۴) \in A_n$ را در نظر بگیرید. در این صورت، مانند حالت ۱، N شامل $\sigma^{-1}(\delta\sigma\delta^{-1})$ می‌باشد. ولی

$$\begin{aligned}\sigma^{-1}(\delta\sigma\delta^{-1}) &= [(۱۲۳)(۴۵۶)\tau]^{-1}(۱۲۴)(۱۲۳)(۴۵۶)\tau(۱۲۴)^{-1}\\ &= \tau^{-1}(۴۵۶)(۱۳۲)(۱۲۴)(۱۲۳)(۴۵۶)\tau(۱۴۲)\\ &= \tau^{-1}\tau(۴۵۶)(۱۳۲)(۱۲۴)(۱۲۳)(۴۵۶)(۱۴۲) = (۱۴۲۶۳).\end{aligned}$$

بنابراین $N \in (۱۴۲۶۳)$، و طبق حالت ۱، $N = A_n$.

حالت ۲ ب N یک عضو σ دارد که حاصل‌ضربی از یک ۳ـ دور و چند ۲ـ دور است. فرض کنیم که $\sigma = (۱۲۳)\tau$، که در آن τ حاصل‌ضربی از ترانهش‌های مجزاست که هیچکدام از آنها شامل نمادهای ۱، ۲، ۳ نیست[۱۳]. چون یک حاصل‌ضرب از ترانهش‌های متمایز وارون خودش می‌باشد (تمرین ۵)، داریم

$$\sigma^2 = (۱۲۳)\tau(۱۲۳)\tau = (۱۲۳)(۱۲۳)\tau\tau = (۱۲۳)(۱۲۳) = (۱۳۲).$$

ولی چون $\sigma \in N$، داریم $\sigma^2 \in N$. بنابراین $N \in (۱۲۳)$، و طبق لم ۲۷.۱۰، $N = A_n$.

حالت ۲ پ N یک ۳–دور را شامل است. در این صورت طبق لم ۲۷.۱۰، $N = A_n$.

حالت ۳ هر عضو N حاصل‌ضرب یک تعداد زوج از ۲ـ دورهای مجزاست. در این صورت یک عنصر نمونه σ از N به صورت $\sigma = (۱۲)(۳۴)\tau$ است، که در آن τ حاصل‌ضربی از ترانهش‌های متمایز است، که هیچکدام از آن‌ها شامل نمادهای ۱، ۲، ۳، ۴ نیست[۱۴]. عنصر

۱۲) پاورقی ۱۰ را ملاحظه کنید.
۱۳) پاورقی ۱۰ را ملاحظه کنید.
۱۴) پاورقی ۱۰ را ملاحظه کنید.

$\delta = (۱۲۳) \in A_n$ را در نظر بگیرید. در این صورت، مثل آنچه در بالا آمده است، $\sigma^{-۱}(\delta\sigma\delta^{-۱}) \in N$ و

$$\sigma^{-۱}(\delta\sigma\delta^{-۱}) = \tau^{-۱}(۳۴)(۱۲)(۱۲۳)(۱۲)(۳۴)\tau(۱۳۲) = (۱۳)(۲۴).$$

چون $n \geq ۵$، یک عضو k در $\{۱, ۲, \ldots, n\}$ وجود دارد که متمایز از ۱، ۲، ۳، ۴ است. قرار دهید $\alpha = (۱۳k) \in A_n$. گیریم $\beta = (۱۳)(۲۴)$، که تازه ثابت شد که در N است. در این صورت طبق نرمال بودن N و بسته بودن آن، $\beta(\alpha\beta\alpha^{-۱}) \in N$. ولی

$$\beta(\alpha\beta\alpha^{-۱}) = (۱۳)(۲۴)(۱۳k)(۱۳)(۲۴)(۱k۳) = (۱۳k).$$

بنابراین $N \in (۱۳k)$ و طبق لم ۲۷.۱۰، $N = A_n$. ■

می‌توان نشان داد که (تا حد یکریختی) تنها دوگروه ساده غیرآبلی از مرتبه کمتر از ۲۰۰ وجود دارد. یکی از آنها $A_۵$ است که دارای مرتبه ۶۰ است، و دیگری زیرگروهی از $S_۷$ از مرتبه ۱۶۸ می‌باشد. بحث درباره دیگر گروههای ساده غیرآبلی خارج از محدوده این کتاب است. برای تاریخچه‌ای مختصر از پژوهش انجام شده پیرامون گروههای ساده، گالیان [۲۴] و استین[۱۵] [۲۷] را ملاحظه کنید. این مقالات برای کسانی که این فصل را خوانده‌اند قابل فهم است. قضیه ۲۸.۱۰ منجر به واقعیت زیر در مورد زیرگروههای نرمال S_n می‌گردد:

نتیجه ۲۹.۱۰. اگر $n \geq ۵$، آنگاه گروه بدیهی (۱)، A_n و S_n تنها زیرگروههای نرمال S_n هستند.

برهان. تمرین ۱۱ را ملاحظه کنید. ■

تمرینها

A ۱. (الف) تمام ۳ـ دورهای واقع در $S_۴$ را فهرست کنید.

(ب) تمام عناصر $A_۴$ را فهرست کنید و هر کدام را به صورت حاصلضربی از ۳ـ دورها بیان کنید.

۲. (الف) بررسی کنید که $A_۲ = (۱)$.

(ب) نشان دهید که $A_۳$ گروهی دوری از مرتبه سه است.

۱۵) Gallian ،Steen

۳. مرکز گروه A_4 را پیدا کنید.[۱۶]

۴. اگر $n \geq 5$، مرکز A_n چیست؟

۵.B اگر $\sigma \in S_n$ حاصل‌ضربی از ترانهش‌های مجزا باشد، ثابت کنید که $\sigma^2 = (1)$.

۶. نشان دهید که برای $n \geq 3$، مرکز S_n برابر (1) است.

۷. گیریم N زیرگروهی از S_n باشد به طوری که برای عضوهای غیرهمانی $\sigma, \tau \in N$، $\sigma\tau = (1)$. ثابت کنید که $N = (1)$ یا N دوری از مرتبه ۲ است.

۸. ثابت کنید که هیچ زیرگروه از مرتبه ۲ در S_n $(n \geq 3)$ نرمال نمی‌باشد.

۹. اگر $\sigma \in S_n$ و $(a_1 a_2 \cdots a_k)$ یک k–دور دلخواه در S_n باشد، نشان دهید که $\sigma(a_1 a_2 \cdots a_k)\sigma^{-1}$، k–دور $(\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))$ است (یعنی دوری که $\sigma(a_1)$ را به $\sigma(a_2)$، $\sigma(a_2)$ را به $\sigma(a_3)$ و همین طور الی آخر می‌نگارد) می‌باشد.

۱۰. ثابت کنید مجموعه $\{(1), (12)(34), (13)(24), (14)(23)\}$ زیرگروه نرمالی از A_4 است. [این کار را می‌توان مستقیماً با استفاده از تمرین ۱ یا تمرین ۹ انجام داد.]

۱۱. نتیجه ۲۹.۱۰ را ثابت کنید. [راهنمایی: اگر N زیرگروهی نرمال از S_n باشد، آنگاه طبق تمرین ۱۷ ازبخش ۵.۷، $N \cap A_n$ زیرگروهی نرمال از A_n است. طبق قضیه ۲۸.۱۰، $N \cap A_n$ برابر با A_n یا (1) است. در حالت اول یعنی $A_n \subseteq N$، از قضیه لاگرانژ و قضیه ۴۸.۷ استفاده کنید تا ثابت کنید که $N = A_n$ یا $N = S_n$. در حالت دوم تمام عناصر غیرهمانی N فرد هستند. این موضوع ایجاب می‌کند که حاصل‌ضرب هر دوتای آنها برابر (1) باشد. از تمرین‌های ۷ و ۸ استفاده کنید.]

۱۲. ثابت کنید که A_n تنها زیرگروه از شاخص ۲ در S_n است. [راهنمایی: نشان دهید که یک زیرگروه از شاخص ۲ باید تمام ۳ـ دورها را شامل باشد و از لم ۲۶.۱۰ استفاده کنید.]

۱۳. اگر $f : S_n \to S_n$ یک همریختی باشد، ثابت کنید که $f(A_n) \subseteq A_n$.

۱۴. گیریم $\sigma, \tau \in S_n$ جایگشتهایی باشند که هرکدام به صورت حاصل‌ضرب دورهای مجزا بیان شده‌اند. ثابت کنید که σ و τ مزدوج هستند اگر و تنها اگر تعداد دورهای با طول یکسان در σ

۱۶) مرکز یک گروه در بند قبل از قضیه ۲۵.۷ تعریف شده است.

و τ برابر باشد.

فصل یازدهم

نظریه گالــوا

درگذشته یک سوال اصلی در جبر کلاسیک این بود که آیا فرمول‌هایی برای حل معادلات چندجمله‌ای از درجه بالاتر (مشابه فرمول درجه دوم برای معادلات درجه دوم) وجود دارد یا نه؟ اگرچه فرمول‌هایی برای معادلات درجه سوم و درجه چهارم در قرن شانزدهم پیدا شد، پیشرفت بیشتری برای نزدیک به ۳۰۰ سال حاصل نگردید. در این هنگام روفینی [۱] و آبل [۲] این جواب اعجاب‌انگیز را مطرح کردند که: وقتی $n \geq 5$ است هیچ فرمولی برای حل تمام معادلات چندجمله‌ای از درجه n وجود ندارد. این دستاورد در مورد احتمال این که جواب‌های بعضی معادلات مشخص ممکن است از یک فرمول بدست آید، حکمی نمی‌کند. جواب مذکور هیچ نشانی دال بر این که چه معادله‌هایی ممکن است با فرمول حلپذیر باشند عرضه نکرد.

این کار حیرت‌آور و بدیع گالوا بود که شرح کاملی را، از جمله معیاری برای تشخیص این که کدام

۱) Ruffini

۲) Abel

معادلات چندجمله‌ای را می‌توان با یک فرمول حل کرد، فراهم آورد. آراء گالوا، خیلی بیشتر از میدان عمل مسئله اصلی حلپذیری، در بسط و توسعه ریاضیات مؤخر تأثیر عمیق گذاشت.

جواب‌های معادله $f(x) = 0$ در یک توسیع میدان ضرایب چندجمله‌ای $f(x)$ قرار دارند. اکتشاف برجسته گالوا ارتباط نزدیک بین چنین توسیع میدان‌ها و گروهها (بخش ۱.۱۱) بود. توصیف مشروح این ارتباط توسط قضیه اساسی نظریه گالوا (در بخش ۲.۱۱) ارائه شده است. این قضیه وسیله اصلی برای اثبات معیار گالوا برای حلپذیری با فرمول (بخش ۳.۱۱) می‌باشد.

۱۱-۱ گروه گالوا

کلید مطالعه توسیع‌های میدان آن است که به هر توسیع، گروهی را که گروه گالوای آن توسیع نامیده می‌شود، متناظر می‌کند. سپس خواص گروه گالوا و قضایای نظریه گروهها را می‌توان بکار برد تا واقعیت‌های مهمی درباره توسیع میدان ثابت کرد. ما در این بخش گروه گالوا را تعریف می‌کنیم و به بسط و توسعه خواص اساسی آن می‌پردازیم.

گیریم $\mathbb{K}$ یک توسیع از میدان $\mathbb{F}$ باشد. یک $\mathbb{F}$**-خودریختی** $\mathbb{K}$ یک یکریختی $\sigma : \mathbb{K} \to \mathbb{K}$ است که $\mathbb{F}$ را عنصروار ثابت نگه می‌دارد. (یعنی، برای هر $c \in C$، $\sigma(c) = c$). مجموعه تمام $\mathbb{F}$-خودریختی‌های $\mathbb{K}$ با، $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ نشان داده می‌شود. حداقل یک خودریختی در $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$، نگاشت همانی $\iota : \mathbb{K} \to \mathbb{K}$، وجود دارد[۳].

قضیه ۱.۱۱. اگر $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد، آنگاه $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ با عمل ترکیب توابع یک گروه‌است.

$\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ **گروه گالوای** $\mathbb{K}$ روی $\mathbb{F}$ نامیده می‌شود.

برهان قضیه ۱.۱۱. اگر $\sigma, \tau \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ آنگاه طبق تمرین ۲۳ از بخش ۳.۳، $\sigma \circ \tau$ یک یکریختی از $\mathbb{K}$ به $\mathbb{K}$ است. برای هر $c \in \mathbb{F}$، $\sigma \circ \tau(c) = \sigma(\tau(c)) = \sigma(c) = c$. به این دلیل $\sigma \circ \tau \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ و $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ بسته‌است. ترکیب توابع شرکت‌پذیر است، و نگاشت همانی، عنصر همانی $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ است. هر تابع دوسویی، طبق قضیه ب.۱ پیوست ب، دارای یک تابع معکوس است. اگر $\sigma \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ آنگاه بنابر تمرین ۲۴ از بخش ۳.۳، σ^{-1} یک یکریختی از $\mathbb{K}$ به $\mathbb{K}$ است. تحقیق کنید که برای هر $c \in \mathbb{F}$، $\sigma^{-1}(c) = c$ (تمرین ۱). بنابراین $\sigma^{-1} \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ و $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ یک گروه است. ■

۳) در سراسر این فصل، ι نگاشت همانی روی میدان مورد بحث را نشان می‌دهد.

مثال ۱.۱۱. نگاشت مزدوج مختلط $\sigma : \mathbb{C} \to \mathbb{C}$ که با ضابطه $\sigma(a+bi) = a - bi$ تعریف شده است، همانگونه که در مثال ۲۳.۳ ثابت شد، یک خودریختی از $\mathbb{C}$ است. برای هر عدد حقیقی a،

$$\sigma(a) = \sigma(a + ۰i) = a - ۰i = a$$

بنابراین σ در $\mathrm{Gal}_{\mathbb{R}}\mathbb{C}$ است. توجه داشته باشید که i و $-i$ ریشه‌های $x^۲ + ۱ \in \mathbb{R}[x]$ هستند و σ این ریشه‌ها را به یکدیگر می‌نگارد: $\sigma(i) = -i$ و $\sigma(-i) = i$. این موضوع مصداقی از قضیه زیر است.

قضیه ۲.۱۱. گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد و $f(x) \in \mathbb{F}[x]$. اگر $u \in \mathbb{K}$ یک ریشه $f(x)$ باشد و $\sigma \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$، آنگاه $\sigma(u)$ نیز یک ریشه $f(x)$ می‌باشد.

برهان. اگر $f(x) = c_۰ + c_۱x + c_۲x^۲ + \cdots + c_nx^n$، آنگاه

$$c_۰ + c_۱u + c_۲u^۲ + \ldots + c_nu^n = ۰_{\mathbb{F}}.$$

چون σ یک همریختی است و برای هر $c_i \in \mathbb{F}$، $\sigma(c_i) = c_i$، لذا

$$\begin{aligned} ۰_{\mathbb{F}} = \sigma(۰_{\mathbb{F}}) &= \sigma(c_۰ + c_۱u + c_۲u^۲ + \cdots + c_nu^n) \\ &= \sigma(c_۰) + \sigma(c_۱)\sigma(u) + \sigma(c_۲)\sigma(u)^۲ + \cdots + \sigma(c_n)\sigma(u)^n \\ &= c_۰ + c_۱\sigma(u) + c_۲\sigma(u)^۲ + \cdots + c_n\sigma(u)^n = f(\sigma(u)). \end{aligned}$$

بنابراین $\sigma(u)$ یک ریشه $f(x)$ می‌باشد. ■

گیریم $u \in \mathbb{K}$ روی $\mathbb{F}$ جبری باشد و چندجمله‌ای کمین آن $p(x) \in \mathbb{F}[x]$ باشد. قضیه ۲.۱۱ بیان می‌کند که هر تصویر u تحت یک خودریختی از گروه گالوا نیز باید یک ریشه $p(x)$ باشد. برعکس، آیا هر ریشه $p(x)$ در $\mathbb{K}$ تصویر u تحت یک خودریختی از $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ است. در اینجا حالتی که جواب آری است آمده است.

قضیه ۳.۱۱. گیریم $\mathbb{K}$ میدان شکافنده یک چندجمله‌ای روی $\mathbb{F}$ باشد و $u, v \in \mathbb{K}$. آنگاه u و v دارای چندجمله‌ای‌های کمین یکسان در $\mathbb{F}[x]$ هستند اگر و تنها اگر $\sigma \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ موجود باشد به قسمی که $\sigma(u) = v$.

برهان. اگر u و v دارای چندجمله‌ای‌های کمین یکسان باشند، آنگاه طبق نتیجه ۸.۹ یک یکریختی $\sigma : \mathbb{F}(u) \cong \mathbb{F}(v)$ وجود دارد به طوری که $\sigma(u) = v$، σ و $\mathbb{F}$ را عنصروار ثابت نگه می‌دارد. چون $\mathbb{K}$ یک میدان شکافنده یک چندجمله‌ای روی $\mathbb{F}$ است، میدان شکافنده همان چندجمله‌ای روی $\mathbb{F}(u)$ و $\mathbb{F}(v)$ نیز می‌باشد. بنابراین طبق قضیه ۱۴.۹، σ به یک $\mathbb{F}$–خودریختی از $\mathbb{K}$ تعمیم پیدا می‌کند (که آن نیز با σ نشان داده می‌شود). به بیان دیگر $\sigma \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ و $\sigma(u) = v$. عکس قضیه نتیجهٔ فوری قضیه ۲.۱۱ است. ■

مثال ۲.۱۱. مثال ۱.۱۱ نشان می‌دهد که $\mathrm{Gal}_{\mathbb{R}}\mathbb{C}$ لااقل دارای دو عضو می‌باشد، نگاشت همانی ι و نگاشت مزدوج مختلط σ. اکنون ثابت می‌کنیم که این دو عضو تنها عضوهای $\mathrm{Gal}_{\mathbb{R}}\mathbb{C}$ می‌باشند. گیریم τ خودریختی دلخواهی در $\mathrm{Gal}_{\mathbb{R}}\mathbb{C}$ باشد. چون i یک ریشه $x^2 + 1$ است، بنابر قضیه ۲.۱۱، $\tau(i) = \pm i$. اگر $\tau(i) = i$ آنگاه چون τ هر عضو $\mathbb{R}$ را ثابت نگه می‌دارد.

$$\tau(a + bi) = \tau(a) + \tau(b)\tau(i) = a + bi$$

و به این دلیل $\tau = \iota$. به طور مشابه اگر $\tau(i) = -i$، آنگاه

$$\tau(a + bi) = \tau(a) + \tau(b)\tau(i) = a + b(-i) = a - ib$$

و بنابراین $\tau = \sigma$. بدین ترتیب $\mathrm{Gal}_{\mathbb{R}}\mathbb{C} = \{\iota, \sigma\}$ یک گروه از مرتبه ۲ است و در نتیجه طبق قضیه ۳۵.۷ با $\mathbb{Z}_2$ یکریخت می‌باشد.

مثال قبل نشان می‌دهد که یک $\mathbb{R}$–خودریختی از $\mathbb{C} = \mathbb{R}(i)$ با عمل آن خودریختی روی i به طور کامل تعیین می‌شود. همین امر در حالت کلی نیز درست است.

قضیه ۴.۱۱. گیریم $\mathbb{K} = \mathbb{F}(u_1, \ldots, u_n)$ یک توسیع جبری میدان $\mathbb{F}$ باشد. اگر $\sigma, \tau \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ و $\sigma(u_i) = \tau(u_i)$ برای هر $i = 1, 2, \ldots, n$، آنگاه $\sigma = \tau$. به بیان دیگر یک خودریختی در $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ به طور کامل با عمل‌آن خودریختی روی u_1، ...، u_n تعیین می‌شود.

برهان. قرار دهید $\beta = \tau^{-1} \circ \sigma \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$. نشان خواهیم داد که β نگاشت همانی ι است. چون برای هر i، $\sigma(u_i) = \tau(u_i)$، لذا

$$\beta(u_i) = (\tau^{-1} \circ \sigma)(u_i) = \tau^{-1}(\sigma(u_i)) = \tau^{-1}(\tau(u_i) = \tau^{-1}\tau(u_i) = \iota(u_i) = u_i.$$

گیریم $v \in \mathbb{F}(u_1)$. طبق قضیه ۷.۹، $c_i \in \mathbb{F}$ وجود دارد به طوری که

$$v = c_0 + c_1 u_1 + c_2 u_1^2 + \cdots + c_{n-1} u_1^{n-1}.$$

چون β همریختی‌ای است که u_1 و هر عضو $\mathbb{F}$ را ثابت نگه می‌دارد، داریم؛

$$\begin{aligned}\beta(v) &= \beta(c_0 + c_1 u_1 + c_2 u_1^2 + \cdots + c_{n-1} u_1^{n-1}) \\ &= \beta(c_0) + \beta(c_1)\beta(u_1) + \beta(c_2)\beta(u_1)^2 + \cdots + \beta(c_{n-1})\beta(u_1)^{n-1} \\ &= c_0 + c_1 u_1 + c_2 u_1^2 + \cdots + c_{n-1} u_1^{n-1} = v.\end{aligned}$$

بنابراین برای هر $v \in \mathbb{F}(u_1)$، $\beta(v) = v$. این استدلال را با جایگزینی $\mathbb{F}(u_1)$ بجای $\mathbb{F}$ و u_2 بجای u_1 تکرارکرده تا بدست آورید که برای هر $v \in \mathbb{F}(u_1)(u_2) = \mathbb{F}(u_1, u_2)$، $\beta(v) = v$. تکرار مجدد روند فوق، با جایگزینی $\mathbb{F}(u_1, u_2)$ بجای $\mathbb{F}$ و u_3 بجای u_1، بدست می‌دهد که برای هر $v \in \mathbb{F}(u_1, u_2, u_3)$، $\beta(v) = v$. پس از تعداد متناهی بار تکرار، برای هر $v \in \mathbb{F}(u_1, u_2, \ldots, u_n) = \mathbb{K}$، خواهیم داشت $\beta(v) = v$ یعنی، $\beta = \tau^{-1} \circ \sigma = \iota$. بنابراین

$$\tau = \tau \circ \iota = \tau \circ (\tau^{-1} \circ \sigma) = (\tau \circ \tau^{-1}) \circ \sigma = \iota \circ \sigma = \sigma.$$

به این ترتیب اثبات کامل می‌شود. ■

مثال ۳.۱۱. طبق قضیه ۲.۱۱ هر خودریختی در گروه گالوای $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ روی $\mathbb{Q}$، $\sqrt{3}$ را به ریشه‌های $x^2 - 3$، $\sqrt{3}$ یا $-\sqrt{3}$ می‌برد. به طور مشابه، این خودریختی باید $\sqrt{5}$ را به ریشه‌های $x^2 - 5$، $\pm\sqrt{5}$ ببرد. چون طبق قضیه ۴.۱۱، یک خودریختی به طور کامل با عملش روی $\sqrt{3}$ و $\sqrt{5}$ معین می‌شود، حداکثر چهار خودریختی در $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{3}, \sqrt{5})$ وجود دارد، که متناظر با چهار عمل ممکن روی $\sqrt{3}$ و $\sqrt{5}$ می‌باشد:

$\sqrt{3} \xrightarrow{\iota} \sqrt{3}$	$\sqrt{3} \xrightarrow{\tau} -\sqrt{3}$	$\sqrt{3} \xrightarrow{\alpha} \sqrt{3}$	$\sqrt{3} \xrightarrow{\beta} -\sqrt{3}$
$\sqrt{5} \to \sqrt{5}$	$\sqrt{5} \to \sqrt{5}$	$\sqrt{5} \to -\sqrt{5}$	$\sqrt{5} \to -\sqrt{5}$

اکنون با ساختن خودریختی‌های غیرهمانی τ، α، β با این اعمال نشان خواهیم داد که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{3}, \sqrt{5})$ یک گروه از مرتبه ۴ است. برای ساختن τ، توجه کنید که $x^2 - 3$ چندجمله‌ای کمین $\sqrt{3}$ و $-\sqrt{3}$ روی $\mathbb{Q}$ است. طبق نتیجه ۸.۹ یک یکریختی $\sigma : \mathbb{Q}(\sqrt{3}) \cong \mathbb{Q}(-\sqrt{3})$

وجود دارد که $\sigma(\sqrt{۳}) = -\sqrt{۳}$ و σ عنصروار $\mathbb{Q}$ را ثابت نگه می‌دارد. مثال ۱۹.۹ نشان می‌دهد که $x^۲ - ۵$ چندجمله‌ای کمین $\sqrt{۵}$ روی $\mathbb{Q}(\sqrt{۳})$ است. دوباره طبق نتیجه ۸.۹، σ به یک $\mathbb{Q}$-خودریختی τ از $\mathbb{Q}(\sqrt{۳})(\sqrt{۵}) = \mathbb{Q}(\sqrt{۳}, \sqrt{۵})$ تعمیم پیدا می‌کند که در آن $\tau(\sqrt{۵}) = \sqrt{۵}$. بنابراین $\tau \in \mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{۳}, \sqrt{۵})$ و $\tau(\sqrt{۳}) = \sigma(\sqrt{۳}) = -\sqrt{۳}$ و $\tau(\sqrt{۵}) = \sqrt{۵}$. یک استدلال دومرحله‌ای مشابه، خودریختی‌های α و β را با اعمالی که در بالا نوشته شده است، ایجاد می‌کند، به علاوه، هر یک از τ، α و β دارای مرتبه ۲ در $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{۳}, \sqrt{۵})$ می‌باشد؛ برای مثال،

$$(\tau \circ \tau)(\sqrt{۳}) = \tau(\tau(\sqrt{۳})) = \tau(-\sqrt{۳}) = -\tau(\sqrt{۳}) = -(-\sqrt{۳}) = \sqrt{۳} = \iota(\sqrt{۳}),$$
$$(\tau \circ \tau)(\sqrt{۵}) = \tau(\sqrt{۵}) = \sqrt{۵} = \sqrt{۵} = \iota(\sqrt{۵}).$$

بنابراین طبق قضیه ۴.۱۱، $\tau \circ \tau = \iota$. از قضیه ۳۶.۷ و یا با محاسبه مستقیم جدول اعمال (تمرین ۴)، نتیجه بگیرید که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{۳}, \sqrt{۵}) \cong \mathbb{Z}_۲ \times \mathbb{Z}_۲$. برای مثال می‌توان به سادگی بررسی کرد که $\tau \circ \alpha(\sqrt{۳}) = \beta(\sqrt{۳})$ و $\tau \circ \alpha(\sqrt{۵}) = \beta(\sqrt{۵})$ و بدین ترتیب طبق قضیه ۴.۱۱، $\tau \circ \alpha = \beta$.

در مثال قبل، $\mathbb{Q}(\sqrt{۳}, \sqrt{۵})$ میدان شکافنده $f(x) = (x^۲ - ۳)(x^۲ - ۵)$ می‌باشد، و هر خودریختی درگروه گالوای آن ریشه‌های $\sqrt{۳}$، $-\sqrt{۳}$، $\sqrt{۵}$ و $-\sqrt{۵}$ از $f(x)$ را جابجا می‌کند. این مثال مصداقی از نتیجه زیر می‌باشد.

نتیجه ۵.۱۱. اگر $\mathbb{K}$ میدان شکافنده یک چندجمله‌ای تفکیک‌پذیر $f(x)$ از درجه n در $\mathbb{F}[x]$ باشد، آنگاه $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ با یک زیرگروه S_n یکریخت است.

برهان. طبق تفکیک‌پذیری، $f(x)$ دارای n ریشه متمایز مثل $u_۱$، ...، u_n است. S_n را گروه جایگشت‌های مجموعهٔ $R = \{u_۱, \ldots, u_n\}$ بگیرید. اگر $\sigma \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$، آنگاه طبق قضیه ۲.۱۱، $\sigma(u_۱)$، $\sigma(u_۲)$، ...، $\sigma(u_n)$ ریشه‌های $f(x)$ می‌باشند، به علاوه چون σ یک به یک است همه آنها متمایز هستند و به این دلیل باید ترتیبی از $u_۱$، ...، u_n باشند. به بیانی دیگر، تحدید σ به مجموعه R (که با $\sigma_{|_R}$ نشان داده می‌شود) یک جایگشت R است. نگاشت $\theta : \mathrm{Gal}_{\mathbb{F}}\mathbb{K} \to S_n$ با ضابطه $\theta(\sigma) = \sigma_{|_R}$ را تعریف کنید. طبق تعریف میدان شکافنده چون عمل هر دو گروه، ترکیب توابع است، به سادگی تحقیق می‌شود که θ یک همریختی گروهی است. طبق تعریف میدان شکافنده، $\mathbb{K} = \mathbb{F}(u_۱, \ldots, u_n)$. اگر $\sigma_{|_R} = \tau_{|_R}$، آنگاه برای هر i، $\sigma(u_i) = \tau(u_i)$ و به این دلیل طبق قضیه ۴.۱۱، $\sigma = \tau$. بنابراین θ یک همریختی یک به یک است، و بدین ترتیب $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ با $\mathrm{Im}\theta$ که زیرگروهی از S_n است یکریخت است. ■

اگر $\mathbb{K}$ میدان شکافنده $f(x)$ باشد، ما به طور معمول با یکی‌گرفتن هر خودریختی $\mathbb{K}$ با آن جایگشتی که روی ریشه‌های $f(x)$ القا می‌شود

$\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ را با زیرگروه یکریختش در S_n یکی می‌گیریم،

مثال ۴.۱۱. گیریم $\mathbb{K}$ میدان شکافنده $x^۳-۲$ روی $\mathbb{Q}$ باشد. بررسی کنید که ریشه‌های $x^۳-۲$، $\sqrt[۳]{۲}$، $\sqrt[۳]{۲}w$ و $\sqrt[۳]{۲}w^۲$ می‌باشد، که در آن $w=(-۱+\sqrt{۳}i)/۲$ یک ریشه سوم مختلط ۱ است، پس $\mathrm{Gal}_{\mathbb{Q}}\mathbb{K}$ یک زیرگروه $S_۳$ می‌باشد. طبق قضیه ۳.۱۱، لااقل یک خودریختی σ موجود است که اولین ریشه یعنی $\sqrt[۳]{۲}$ را به دومین ریشه یعنی $\sqrt[۳]{۲}w$ می‌نگارد. این خودریختی طبق قضیه ۲.۱۱ باید ریشه سوم یعنی $\sqrt[۳]{۲}w^۲$ را به خودش یا به ریشه اول یعنی $\sqrt[۳]{۲}$ ببرد. پس σ یا جایگشت (۱۲) و یا (۱۲۳) در $S_۳$ می‌باشد.

گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد. یک میدان $\mathbb{E}$ به طوری که $\mathbb{F}\subseteq\mathbb{E}\subseteq\mathbb{K}$، یک **میدان میانی** از این توسیع نامیده می‌شود. در این حالت می‌توان $\mathbb{K}$ را به عنوان توسیعی از $\mathbb{E}$ لحاظ نمود. گروه گالوای $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ شامل تمام خودریختی‌هایی از $\mathbb{K}$ می‌باشد که عناصر $\mathbb{E}$ را عنصروار ثابت نگاه می‌دارد و هر چنین خودریختی به طور خودکار هر عضو $\mathbb{F}$ را ثابت نگاه می‌دارد زیرا $\mathbb{F}\subseteq\mathbb{E}$. بدین دلیل هر خودریختی در $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ در $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ است، یعنی

اگر $\mathbb{E}$ یک میدان میانی باشد، $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ زیرگروه $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ می‌باشد.

مثال ۵.۱۱. $\mathbb{Q}(\sqrt{۳})$ یک میدان میانی توسیع $\mathbb{Q}(\sqrt{۳},\sqrt{۵})$ از $\mathbb{Q}$ است. مثال ۳.۱۱ نشان می‌دهد که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{۳},\sqrt{۵})=\{\iota,\tau,\alpha,\beta\}$. خودریختی‌هایی که هر عضو $\mathbb{Q}(\sqrt{۳})$ را ثابت نگاه می‌دارند طبق قضیه ۴.۱۱ درست همان‌هایی هستند که $\sqrt{۳}$ را بخودش می‌نگارند. بنابراین گروه گالوای $\mathrm{Gal}_{\mathbb{Q}(\sqrt{۳})}\mathbb{Q}(\sqrt{۳},\sqrt{۵})$ زیرگروه $\{\iota,\alpha\}$ از $\{\iota,\tau,\alpha,\beta\}$ است.

اکنون یک راه طبیعی برای متناظرکردن یک زیرگروه از گروه گالوا با هر میدان میانی توسیع داریم. برعکس، اگر H یک زیرگروه گروه گالوا باشد، می‌توانیم یک میدان میانی را به H با استفاده از قضیه زیر متناظر کنیم.

قضیه ۶.۱۱. گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد. اگر H یک زیرگروه $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ باشد، گیریم

$$\mathbb{E}_H=\{k\in\mathbb{K}\mid \sigma(k)=k, \sigma\in H \text{ برای هر}\}.$$

آنگاه $\mathbb{E}_H$ یک میدان میانی این توسیع است.

میدان $\mathbb{E}_H$ **میدان ثابت** زیرگروه H نامیده می‌شود.

برهان قضیه ۶.۱۱. اگر $c,d \in \mathbb{E}_H$ و $\sigma \in H$، آنگاه

$$\sigma(c+d) = \sigma(c) + \sigma(d) = c + d, \qquad \sigma(cd) = \sigma(c)\sigma(d) = cd.$$

بنابراین $\mathbb{E}_H$ تحت جمع وضرب بسته است. چون برای هر خودریختی σ داریم $\sigma(0_{\mathbb{F}}) = 0_{\mathbb{F}}$ و $\sigma(1_{\mathbb{F}}) = 1_{\mathbb{F}}$، لذا $0_{\mathbb{F}}$ و $1_{\mathbb{F}}$ در $\mathbb{E}_H$ هستند. قضایای ۱۰.۳ و ۱۴.۷ نشان می‌دهد که برای هر c ناصفر در $\mathbb{E}_H$ و هر σ در H،

$$\sigma(-c) = -\sigma(c) = -c, \qquad \sigma(c^{-1}) = \sigma(c)^{-1} = c^{-1}.$$

پس $c^{-1} \in \mathbb{E}_H, -c \in \mathbb{E}_H$. به این دلیل $\mathbb{E}_H$ زیرمیدان $\mathbb{K}$ است. چون H زیرگروه $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ است، برای هر $c \in \mathbb{F}$ و هر $\sigma \in H$ داریم $\sigma(c) = c$. بنابراین $\mathbb{F} \subseteq \mathbb{E}_H$. ■

مثال ۶.۱۱. زیرگروه $H = \{\iota, \alpha\}$ از گروه گالوای $\{\iota, \tau, \alpha, \beta\}$ از $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ روی $\mathbb{Q}$ را در نظر بگیرید. چون $\alpha(\sqrt{3}) = \sqrt{3}$، زیرمیدان $\mathbb{Q}(\sqrt{3})$ در میدان ثابت $\mathbb{E}_H$ از H جا می‌گیرد. برای این که ثابت کنیم $\mathbb{E}_H = \mathbb{Q}(\sqrt{3})$، باید نشان دهید که عضوهای $\mathbb{Q}(\sqrt{3})$ تنها عضوهایی می‌باشند که توسط ι و α ثابت هستند، تمرین ۱۴ را ببینید.

مثال ۷.۱۱. همان‌طورکه در مثال ۲.۱۱ دیدیم $\mathrm{Gal}_{\mathbb{R}}\mathbb{C} = \{\iota, \sigma\}$، که در آن σ نگاشت مزدوج مختلط است. به وضوح، میدان ثابتِ زیرگروه همانی، تمام میدان $\mathbb{C}$ می‌باشد. چون σ هر عدد حقیقی را ثابت نگه می‌دارد و هر عدد غیرحقیقی را تغییر می‌دهد، میدان ثابت $\mathrm{Gal}_{\mathbb{R}}\mathbb{C}$ میدان $\mathbb{R}$ است. برخلاف موقعیت مثال پیش، میدان زمینهٔ $\mathbb{F}$ همیشه لازم نیست میدان ثابت گروه $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ باشد.

مثال ۸.۱۱. طبق قضیه ۲.۱۱ هر خودریختی در گروه گالوای $\mathbb{Q}(\sqrt[3]{2})$ روی $\mathbb{Q}$ باید $\sqrt[3]{2}$ را به یک ریشه $x^3 - 2$ بنگارد. مثال ۴.۱۱ نشان می‌دهد که $\sqrt[3]{2}$ تنها ریشه حقیقی این چندجمله‌ای است. چون طبق قضیه ۷.۹، $\mathbb{Q}(\sqrt[3]{2})$ به طور کامل در اعداد حقیقی قرار دارد، هر خودریختی در $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})$ باید $\sqrt[3]{2}$ را به خودش بنگارد. بنابراین طبق قضیه ۴.۱۱، $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})$ تنها شامل

خودریختی همانی است. در نتیجه میدان ثابت $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})$ تمام میدان $\mathbb{Q}(\sqrt[3]{2})$ می‌باشد.

تمرینها

توجه کنید: $\mathbb{K}$ همواره یک توسیع میدان $\mathbb{F}$ است.

A.۱. اگر σ یک $\mathbb{F}$–خودریختی $\mathbb{K}$ باشد، نشان دهید که σ^{-1} نیز یک $\mathbb{F}$–خودریختی $\mathbb{K}$ است.

۲. فرض کنید $[\mathbb{K}:\mathbb{F}]$ متناهی باشد. آیا درست است که هر $\mathbb{F}$–خودریختی $\mathbb{K}$ به طور کامل با عملش روی یک پایهٔ $\mathbb{K}$ روی $\mathbb{F}$ معین می‌شود؟

۳. فرض کنید $[\mathbb{K}:\mathbb{F}]$ متناهی باشد. اگر $\sigma \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ و $u \in \mathbb{K}$ طوری باشد که $\sigma(u) = u$، ثابت کنید که $\sigma \in \mathrm{Gal}_{\mathbb{F}(u)}\mathbb{K}$.

۴. جدول ضرب گروه $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{3},\sqrt{5}) = \{\iota,\tau,\alpha,\beta\}$ را بنویسید [مثال ۳.۱۱ را ببینید].

۵. گیریم $f(x) \in \mathbb{F}[x]$ تفکیک‌پذیر از درجه n و $\mathbb{K}$ یک میدان شکافنده $f(x)$ باشد. ثابت کنید که مرتبه $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$، $n!$ را می‌شمارد.

۶. اگر $\mathbb{K}$ یک توسیع میدان $\mathbb{Q}$ و σ یک خودریختی $\mathbb{K}$ باشد، ثابت کنید که σ یک $\mathbb{Q}$–خودریختی است. [راهنمایی: $\sigma(1) = 1$ ایجاب می‌کند که $\sigma(n) = n$ برای هر $n \in \mathbb{Z}$.]

B.۷. (الف) ثابت کنید که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2})$ دارای مرتبه ۲ است و از اینرو با $\mathbb{Z}_2$ یکریخت است.
(ب) اگر $d \in \mathbb{Q}$ و $\sqrt{d} \notin \mathbb{Q}$، ثابت کنید که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{d})$ یکریخت با $\mathbb{Z}_2$ است.

۸. ثابت کنید که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2}) \neq <\iota>$.

۹. (الف) گیریم $w = (-1+\sqrt{3}i)/2$ یک ریشه سوم مختلط ۱ باشد. $p(x)$ چندجمله‌ای کمین w روی $\mathbb{Q}$ را پیدا کنید و ثابت کنید که w^2 نیز یک ریشه $p(x)$ است. [راهنمایی: w یک ریشه $x^3 - 1$ است.]
(ب) $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(w)$ چیست؟

۱۰. (الف) $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},\sqrt{3})$ را پیدا کنید. [راهنمایی: مثال ۳.۱۱ را ببینید.]
(ب) اگر p و q اعداد اول متمایز مثبت باشند $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$ را پیدا کنید.

۱۱. $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},i)$ را پیدا کنید. [راهنمایی: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},i)$ را در نظر بگیرید و مانند مثال ۳.۱۱ عمل کنید.]

۱۲. ثابت کنید که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

۱۳. اگر $\mathbb{F}$ از مشخصه صفر و $\mathbb{K}$ میدان شکافنده $f(x) \in \mathbb{K}[x]$ باشد، ثابت کنید که مرتبه $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ برابر $[\mathbb{K} : \mathbb{F}]$ می‌باشد. [راهنمایی: طبق قضایای ۱۷.۹ و ۱۸.۹ $\mathbb{K} = \mathbb{F}(u)$.]

۱۴. گیریم H زیرگروه $\{\iota, \tau, \alpha, \beta\}$ از $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{3},\sqrt{5}) = \{\iota, \alpha\}$ باشد. نشان دهید که میدان ثابت H، $\mathbb{Q}(\sqrt{3})$ می‌باشد. [راهنمایی: تحقیق کنید که $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{E}_H \subseteq \mathbb{Q}(\sqrt{3},\sqrt{5})$؛ عدد $[\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}(\sqrt{3})]$ چیست؟]

۱۵. (الف) ثابت کنید که هر خودریختی $\mathbb{R}$ عناصر مثبت را به عناصر مثبت می‌نگارد. [راهنمایی: هر عضو مثبت $\mathbb{R}$ یک مربع کامل است.]

(ب) اگر $a, b \in \mathbb{R}$، $a < b$ و $\sigma \in \mathrm{Gal}_{\mathbb{Q}}\mathbb{R}$، ثابت کنید که $\sigma(a) < \sigma(b)$. [راهنمایی: $a < b$ اگر و تنها اگر $0 < b - a$.]

(پ) ثابت کنید که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{R} = <\iota>$. [راهنمایی: اگر $c < r < d$ با شرط $c, d \in \mathbb{Q}$، آنگاه $c < \sigma(r) < d$؛ نشان دهید که این ایجاب می‌کند $\sigma(r) = r$.]

۱۶.C. فرض کنید ζ، ζ^2، ...، $\zeta^n = 1$، nریشه متمایز $x^n - 1$ در یک توسیع میدان $\mathbb{Q}$ باشد. ثابت کنید که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta)$ آبلی است.

۱۷. گیریم $\mathbb{E}$ یک میدان میانی باشد که روی $\mathbb{F}$ نرمال است و $\sigma \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$. ثابت کنید که $\sigma(\mathbb{E}) = \mathbb{E}$.

۲-۱۱ قضیه اساسی نظریه گالوا

در سراسر این بخش، $\mathbb{K}$ یک توسیع *میدان متناهی میدان* $\mathbb{F}$ است. آرمان اساسی نظریه گالوا آن است که ویژگی‌های توسیع را به ویژگی‌های گروه گالوای $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ مربوط می‌کند. رمز انجام چنین کاری قضیه اساسی نظریه گالوا است، که در این بخش ثابت خواهد شد. این قضیه به ویژه بیان می‌کند که تحت شرایط مناسب، یک تناظر یک به یک بین میدان‌های میانی یک توسیع و زیرگروههای گروه گالوا وجود دارد[۴].

مرحله اول ایجاد این تناظر ساده می‌باشد: اگر $\mathbb{E}$ میدان میانی مفروضی باشد، یک زیرگروه

۴) یعنی یک نگاشت یک به یک از مجموعه همه میدان‌های میانی به مجموعه همه زیرگروههای گروه گالوا.

$\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$، یعنی $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$، زیرگروه خودریختی‌هایی از $\mathbb{K}$ که $\mathbb{E}$ را عنصروار ثابت نگاه می‌دارد، وجود دارد که به طور طبیعی با $\mathbb{E}$ متناظر می‌باشد. در نتیجه یک تابع از مجموعه S شامل تمام میدان‌های میانی به مجموعه T شامل تمام زیرگروههای $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ با ضابطه $\mathbb{E} \to \mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ می‌توان تعریف کرد. این تابع **تناظر گالوا** نامیده می‌شود.

تحت تناظر گالوا میدان‌های میانی بدیهی، $\mathbb{F}$ و $\mathbb{K}$، به زیرگروههای بدیهی گروه گالوا نگاشته می‌شوند: $\mathbb{K}$ به زیرگروه همانی $\mathrm{Gal}_{\mathbb{K}}\mathbb{K}$ و $\mathbb{F}$ به گروه گالوای کامل $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ متناظر می‌شود.

مثال ۹.۱۱. تناظر گالوا برای توسیع $\mathbb{Q}(\sqrt{۳},\sqrt{۵})$ از $\mathbb{Q}$ و میدان میانی $\mathbb{Q}(\sqrt{۳})$ را در نظر بگیرید. طبق تذکرات پیش و مثال ۵.۱۱ در بخش ۱.۱۱، داریم

$$\mathbb{Q}(\sqrt{۳},\sqrt{۵}) \to \mathrm{Gal}_{\mathbb{Q}(\sqrt{۳},\sqrt{۵})}\mathbb{Q}(\sqrt{۳},\sqrt{۵}) = \{\iota\}.$$
$$\mathbb{Q}(\sqrt{۳}) \to \mathrm{Gal}_{\mathbb{Q}(\sqrt{۳})}\mathbb{Q}(\sqrt{۳},\sqrt{۵}) = \{\iota,\alpha\}.$$
$$\mathbb{Q} \to \mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{۳},\sqrt{۵}) = \{\iota,\tau,\alpha,\beta\}.$$

طبق مثال ۶.۱۱، میدان ثابت زیرگروه $H = \{\iota,\alpha\} = \mathrm{Gal}_{\mathbb{Q}(\sqrt{۳})}\mathbb{Q}(\sqrt{۳},\sqrt{۵})$، میدان $\mathbb{E} = \mathbb{Q}(\sqrt{۳})$ می‌باشد. به‌علاوه، $\mathbb{K} = \mathbb{Q}(\sqrt{۳},\sqrt{۵}) = \mathbb{Q}(\sqrt{۳})(\sqrt{۵})$ یک توسیع نرمال تفکیک‌پذیر از میدان ثابت $\mathbb{E} = \mathbb{Q}(\sqrt{۳})$ است، زیرا میدان شکافندهٔ $x^۲ - ۵$ می‌باشد (قضیه ۱۵.۹) و مشخصه آن صفر است (قضیه ۱۷.۹). این مصداقی از لم زیر است.

لم ۷.۱۱. گیریم $\mathbb{K}$ یک توسیع با بعد متناهی میدان $\mathbb{F}$ باشد. اگر H یک زیرگروه گروه گالوای $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ و $\mathbb{E}$ میدان ثابت H باشد، آنگاه $\mathbb{K}$ یک توسیع ساده، نرمال و تفکیک‌پذیر $\mathbb{E}$ است.

برهان. طبق قضیه ۹.۹، هر $u \in \mathbb{K}$ روی $\mathbb{F}$ جبری است و بدین دلیل طبق تمرین ۷ از بخش ۲.۹ u روی $\mathbb{E}$ جبری می‌باشد. هر خودریختی H باید u را طبق قضیه ۲.۱۱ به ریشه‌ای از چندجمله‌ای کمین آن، $p(x) \in \mathbb{E}[x]$ بنگارد. بنابراین u دارای تعداد متناهی تصویر متمایز تحت خودریختی‌های H می‌باشد، مثلاً $u = u_۱, u_۲, \ldots, u_t \in \mathbb{K}$.

اگر $\sigma \in H$ و $u_i = \tau(u)$ (با شرط $\tau \in H$)، آنگاه $\sigma(u_i) = \sigma(\tau(u))$. چون $\sigma\circ\tau \in H$، می‌بینیم که $\sigma(u_i)$ نیز یک تصویر u است و بدین دلیل در مجموعه $\{u_۱, u_۲, \ldots, u_t\}$ قرار دارد. چون σ یک به یک است عناصر $\sigma(u_۱), \ldots, \sigma(u_t)$ تصاویر متمایز u هستند و بنابراین باید یک

ترتیب از عناصر u_1، u_2، ...، u_t باشند. به بیان دیگر، هر خودریختی واقع در H عناصر u_1، ...، u_t را جابجا می‌کند. گیریم

$$f(x) = (x - u_1)(x - u_2)\cdots(x - u_t).$$

چون u_iها متمایزند، $f(x)$ تفکیک‌پذیر می‌باشد. ادعا می‌کنیم که $f(x)$ در واقع در $\mathbb{E}[x]$ می‌باشد. برای اثبات این موضوع، فرض کنید $\sigma \in H$ و بخاطر بیاورید که همانگونه که در بند قبل از نتیجه ۸.۹ گفته شد σ یک یکریختی $\mathbb{K}[x] \cong \mathbb{K}[x]$ القا می‌کند (که آن نیز با σ نشان داده می‌شود). آنگاه

$$\sigma f(x) = (x - \sigma(u_1))(x - \sigma(u_1))\cdots(x - \sigma(u_t)).$$

چون σ، u_iها را جابجا می‌کند، لذا تنها اثر آن روی $f(x)$ جابجایی عوامل آن می‌باشد، از اینرو $\sigma f(x) = f(x)$. بنابراین هر خودریختی H ضرایب چندجمله‌ای تفکیک‌پذیر $f(x)$ را به خودش می‌نگارد، و به این دلیل این ضرایب در $\mathbb{E}$، میدان ثابت H، می‌باشند. چون $u = u_1$ یک ریشه $f(x) \in \mathbb{E}[x]$ است، u روی $\mathbb{E}$ تفکیک‌پذیر است. از اینرو $\mathbb{K}$ یک توسیع تفکیک‌پذیر $\mathbb{E}$ است.

میدان $\mathbb{K}$ روی $\mathbb{F}$ با بعد متناهی است (زیرا $[\mathbb{K} : \mathbb{F}]$ متناهی است؛ مثال ۱۷.۹ را ملاحظه کنید) در نتیجه، $\mathbb{K}$ روی $\mathbb{E}$ با بعد متناهی می‌باشد، و بدین دلیل طبق قضیه ۱۸.۹ برای برخی $u \in \mathbb{K}$، $\mathbb{K} = \mathbb{E}(u)$. گیریم $f(x)$ مانند بند قبل باشد، در این صورت $f(x)$ در $\mathbb{K}[x]$ شکافته می‌شود، و بدین دلیل $\mathbb{K} = \mathbb{E}(u)$ میدان شکافنده $f(x)$ روی $\mathbb{E}$ است. بنابراین $\mathbb{K}$ طبق قضیه ۱۵.۹ روی $\mathbb{E}$ نرمال است. ■

قضیه ۸.۱۱. گیریم $\mathbb{K}$ یک توسیع با بعد متناهی میدان $\mathbb{F}$ باشد. اگر H یک زیرگروه گالوای $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ و $\mathbb{E}$ میدان ثابت H باشد، آنگاه $H = \mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ و $|H| = [\mathbb{K} : \mathbb{E}]$. بنابراین تناظر گالوا پوشاست.

برهان. لم ۷.۱۱ نشان می‌دهد که $\mathbb{K} = \mathbb{E}(u)$. اگر $p(x)$، چندجمله‌ای کمین u روی $\mathbb{E}$، دارای درجه n باشد، آنگاه طبق قضیه ۷.۹، $[\mathbb{K} : \mathbb{E}] = n$. طبق قضیه ۲.۱۱ و ۴.۱۱ خودریختی‌های متمایز $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$، u را به ریشه‌های متمایز $p(x)$ می‌نگارد. حال طبق تعریف میدان ثابت $\mathbb{E}$، $H \subseteq \mathrm{Gal}_{\mathbb{E}}\mathbb{K}$. در نتیجه

$$|H| \leq |\mathrm{Gal}_{\mathbb{E}}\mathbb{K}| \leq n = [\mathbb{K} : \mathbb{E}].$$

گیریم $f(x)$ مثل آنچه در برهان لم ۷.۱۱ بود، باشد. آنگاه H لااقل دارای t خودریختی (تعداد تصاویر متمایز u تحت H) می‌باشد چون $u = u_1$ یک ریشه $f(x)$ است، $p(x)$، $f(x)$ را می‌شمارد. به این دلیل

$$| H | \geq t = \deg f(x) \geq \deg p(x) = n = [\mathbb{K} : \mathbb{E}].$$

از ترکیب این نامساویها، داریم

$$| H | \leq | \mathrm{Gal}_{\mathbb{E}}\mathbb{K} | \leq [\mathbb{K} : \mathbb{E}] \leq | H | .$$

بنابراین $[\mathbb{K} : \mathbb{E}] = | \mathrm{Gal}_{\mathbb{E}}\mathbb{K} |$ و از اینرو $H = \mathrm{Gal}_{\mathbb{E}}\mathbb{K}$. ■

مثال ۱۰.۱۱. طبق مثال ۴.۱۱، $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2}) = < \iota >$، بنابراین تحت تناظر گالوا هر دو میدان میانی $\mathbb{Q}(\sqrt[3]{2})$ و $\mathbb{Q}$ متناظر با $< \iota >$ می‌شوند. توجه داشته باشید که $\mathbb{Q}(\sqrt[3]{2})$ توسیع نرمال $\mathbb{Q}$ نیست [ریشه‌های مختلط $x^3 - 2$ در آن نیست، پس این چندجمله‌ای یک ریشه دارد ولی در $\mathbb{Q}(\sqrt[3]{2})$ تجزیه نمی‌شود].

اگرچه طبق قضیه ۸.۱۱ تناظر گالوا پوشا می‌باشد، مثال قبل نشان می‌دهد که این تناظر لزوماً یک به یک نیست. برای این که یک به یک بودن تضمین گردد اِعمال فرض‌های اضافی روی توسیع ضرورت دارد. از برهان‌ها و مثال پیش چنین برمی‌آید که نرمال بودن و تفکیک‌پذیری نامزدهای احتمالی باشند.

اگر $\mathbb{K}$ یک توسیع با بعد متناهی، نرمال و تفکیک‌پذیر میدان $\mathbb{F}$ باشد، گوییم $\mathbb{K}$ یک **توسیع گالوای** $\mathbb{F}$ است یا این که $\mathbb{K}$ **روی** $\mathbb{F}$ **گالوا** می‌باشد. بنابر قضایای ۱۵.۹ و ۱۷.۹، هر توسیع گالوای با مشخصه ۰ یک میدان شکافنده است.

قضیه ۹.۱۱. گیریم $\mathbb{K}$ یک توسیع گالوای $\mathbb{F}$ و $\mathbb{E}$ یک میدان میانی باشد. آنگاه $\mathbb{E}$ میدان ثابت زیرگروه $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ است.

اگر $\mathbb{E}$ و $\mathbb{L}$ میدان‌هایی باشند که $\mathrm{Gal}_{\mathbb{E}}\mathbb{K} = \mathrm{Gal}_{\mathbb{L}}\mathbb{K}$، آنگاه قضیه ۹.۱۱ نشان می‌دهد که $\mathbb{E}$ و $\mathbb{L}$ هر دو میدان‌های ثابت یک گروه می‌باشند و بدین دلیل $\mathbb{E} = \mathbb{L}$. بنابراین تناظر گالوا برای توسیع‌های گالوا یک به یک می‌باشد.

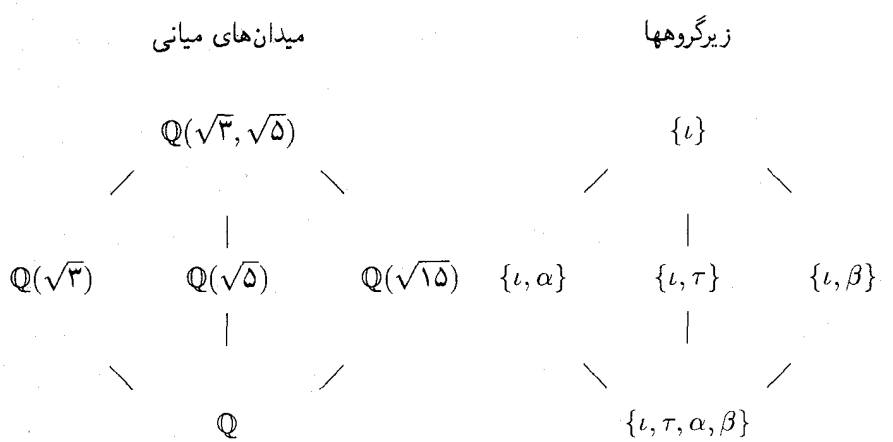
برهان قضیه ۹.۱۱. بنابر تعریف اگر $\mathbb{E}$. میدان ثابت $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ باشد آنگاه $\mathbb{E}$. شامل $\mathbb{E}$ است. برای اثبات این که $\mathbb{E} \subseteq \mathbb{E}$.، عکس نقیض آن را ثابت می‌کنیم: اگر $u \notin \mathbb{E}$، آنگاه u توسط یک خودریختی واقع در $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ تغییر می‌کند و بدین دلیل $u \notin \mathbb{E}$. چون $\mathbb{K}$ توسیع گالوای میدان میانی $\mathbb{E}$ (طبق قضیه ۱۵.۹ و تمرین ۵ بخش ۴.۹ نرمال می‌باشد و بنابر تمرین ۱ بخش ۵.۹ تفکیک‌پذیر است) می‌باشد پس یک توسیع جبری $\mathbb{E}$ است. در نتیجه، u روی $\mathbb{E}$ جبری است و چندجمله‌ای کمین آن، $p(x) \in \mathbb{E}[x]$، از درجه $\deg p(x) = ۱$ (اگر ≥ ۲ است)، آنگاه u در $\mathbb{E}$ می‌باشد). ریشه‌های $p(x)$ طبق تفکیک‌پذیری متمایزند، و تمام آن‌ها طبق نرمال بودن در $\mathbb{K}$ هستند. گیریم v ریشه‌ای از $p(x)$ غیر از u باشد. آنگاه طبق قضیه ۳.۱۱، $\sigma \in \mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ وجود دارد به طوری که $\sigma(u) = v$. بنابراین $u \notin E$. و بدین دلیل $E = E$.. ■

نتیجه ۱۰.۱۱. گیریم $\mathbb{K}$ یک توسیع با بعد متناهی $\mathbb{F}$ باشد آنگاه $\mathbb{K}$ روی $\mathbb{F}$ گالواست اگر و فقط اگر $\mathbb{F}$ میدان ثابت گروه گالوای $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ باشد.

برهان. اگر $\mathbb{K}$ روی $\mathbb{F}$ گالوا باشد، قضیه ۹.۱۱ (با شرط $\mathbb{E} = \mathbb{F}$) نشان می‌دهد که $\mathbb{F}$ میدان ثابت $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ است. بالعکس، اگر $\mathbb{F}$ میدان ثابت $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ باشد، آنگاه لم ۷.۱۱ (با شرط $\mathbb{E} = \mathbb{F}$) نشان می‌دهد که $\mathbb{K}$ روی $\mathbb{F}$ گالواست. ■

با توجه به نتیجه۱۰.۱۱، اغلب یک توسیع گالوا را یک توسیع با بعد متناهی تعریف می‌کنند که در آن $\mathbb{F}$ میدان ثابت $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ باشد. وقتی کتاب‌های دیگری راجع به نظریه گالوا مطالعه می‌کنید دقت کنید که از چه تعریفی استفاده شده است تا فرض‌های تضمین نشده نکنید.

مثال ۱۱.۱۱. میدان $\mathbb{Q}(\sqrt{۳}, \sqrt{۵})$ توسیع گالـوای $\mathbb{Q}$ می‌باشد زیـرا میـدان شکافنـده $f(x) = (x^۲ - ۳)(x^۲ - ۵)$ است. پس طبق قضیه ۸.۱۱ و تذکرات بعد از قضیه ۹.۱۱، تناظر گالوا دوسویی می‌باشد. طبق مثال ۳.۱۱، $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{۳}, \sqrt{۵}) = \{\iota, \tau, \alpha, \beta\}$. درستی نمودار زیر را، که در آن زیرمیدان‌ها و زیرگروهها در همان مکان مربوط به خود با یکدیگر تحت تناظر گالوا متناظرند، تحقیق کنید. به عنوان نمونه، $\mathbb{Q}(\sqrt{۳})$، بنابر مثال ۵.۱۱ با $\{\iota, \alpha\}$ متناظر است.



توجه کنید که تمام میدان‌های میانی، توسیع‌های گالوای $\mathbb{Q}$ می‌باشند (برای مثال، $\mathbb{Q}(\sqrt{5})$ میدان شکافنده x^2-5 می‌باشد). به‌علاوه زیرگروههای متناظر گروه گالوا همگی نرمال می‌باشند. موقعیتی مشابه در حالت کلی برقرار است:

قضیه ۱۱.۱۱. (**قضیه اساسی نظریه گالوا**) اگر $\mathbb{K}$ یک توسیع گالوای میدان $\mathbb{F}$ باشد، آنگاه

۱. بین مجموعه S متشکل از تمام میدان‌های میانی این توسیع و مجموعه T شامل تمام زیرگروههای گروه گالوای $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ یک دوسویی وجود دارد که از متناظر ساختن هر میدان میانی $\mathbb{E}$ با زیرگروه $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ حاصل می‌شود. به‌علاوه

$$[\mathbb{K}:\mathbb{E}] = |\ \mathrm{Gal}_{\mathbb{E}}\mathbb{K}\ | \quad \text{و} \quad [\mathbb{E}:\mathbb{F}] = [\mathrm{Gal}_{\mathbb{F}}\mathbb{K} : \mathrm{Gal}_{\mathbb{E}}\mathbb{K}].$$

۲. یک میدان میانی $\mathbb{E}$ یک توسیع نرمال $\mathbb{F}$ است اگر و تنها اگر گروه متناظر $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ یک زیرگروه نرمال $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ باشد، در این حالت $\mathrm{Gal}_{\mathbb{F}}\mathbb{E} \cong \mathrm{Gal}_{\mathbb{F}}\mathbb{K}/\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$.

برهان. قضیه ۸.۱۱ و تذکرات بعد از قضیه ۹.۱۱، گزاره اول قسمت ۱ را ثابت می‌نماید. هر میدان میانی $\mathbb{E}$ طبق قضیه ۹.۱۱ میدان ثابت $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ می‌باشد. در نتیجه، طبق قضیه ۸.۱۱، $[\mathbb{K}:\mathbb{E}] = |\ \mathrm{Gal}_{\mathbb{E}}\mathbb{K}\ |$. به ویژه اگر $\mathbb{F}=\mathbb{E}$، آنگاه $[\mathbb{K}:\mathbb{F}] = |\ \mathrm{Gal}_{\mathbb{F}}\mathbb{K}\ |$. بنابراین طبق قضیهٔ لاگرانژ ۳۳.۷ و قضیه ۴.۹،

$$[\mathbb{K}:\mathbb{E}][\mathbb{E}:\mathbb{F}] = [\mathbb{K}:\mathbb{F}] = |\ \mathrm{Gal}_{\mathbb{F}}\mathbb{K}\ | = |\ \mathrm{Gal}_{\mathbb{E}}\mathbb{K}\ |\ [\mathrm{Gal}_{\mathbb{F}}\mathbb{K} : \mathrm{Gal}_{\mathbb{E}}\mathbb{K}].$$

از تقسیم دوطرف این معادله بر $|\mathrm{Gal}_{\mathbb{E}}\mathbb{K}| = [\mathbb{K}:\mathbb{E}]$ بدست می‌آوریم

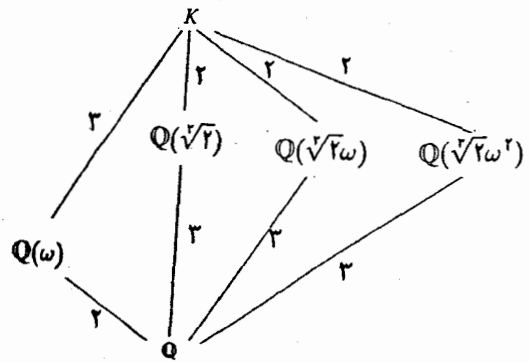
$$[\mathbb{E}:\mathbb{F}] = [\mathrm{Gal}_{\mathbb{F}}\mathbb{K} : \mathrm{Gal}_{\mathbb{E}}\mathbb{K}].$$

برای اثبات قسمت ۲، ابتدا فرض کنید $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ زیرگروه نرمال $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ باشد. اگر $p(x)$ یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}[x]$ باشد که در $\mathbb{E}$ یک ریشه u داشته باشد، باید ثابت کنیم که $p(x)$ در $\mathbb{E}[x]$ تجزیه می‌شود. چون $\mathbb{K}$ روی $\mathbb{F}$ نرمال است، می‌دانیم که $p(x)$ در $\mathbb{K}[x]$ تجزیه می‌شود. پس لازم است فقط ثابت کنیم هر ریشه v از $p(x)$ در $\mathbb{K}$ به واقع در $\mathbb{E}$ است. طبق قضیه ۳.۱۱، خودریختی σ در $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ وجود دارد به قسمی که $\sigma(u) = v$. اگر τ عضوی از $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ باشد، آنگاه نرمال بودن ایجاب می‌کند که برای یک $\tau_1 \in \mathrm{Gal}_{\mathbb{E}}\mathbb{K}$، $\tau\circ\sigma = \sigma\circ\tau_1$. چون $u \in \mathbb{E}$، داریم $\tau(v) = \tau(\sigma(u)) = \sigma(\tau_1(u)) = \sigma(u) = v$. از اینرو v تحت هر عضو $\tau \in \mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ ثابت می‌ماند و بنابراین باید در میدان ثابت $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ یعنی $\mathbb{E}$ باشد (به قضیه ۹.۱۱ رجوع کنید).

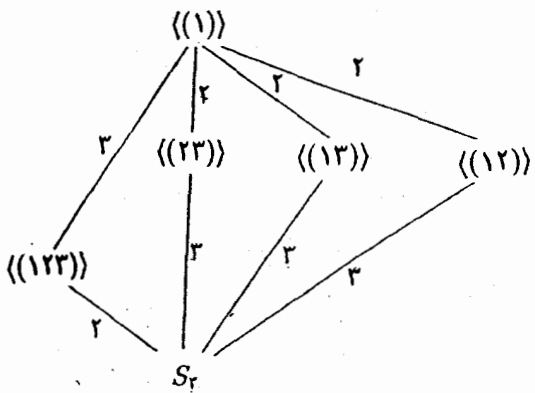
بالعکس، فرض کنید که $\mathbb{E}$ یک توسیع نرمال $\mathbb{F}$ باشد. طبق قسمت ۱، $\mathbb{E}$ روی $\mathbb{F}$ با بعد متناهی است. بنابر لم ۱۲.۱۱، که در زیر اثبات خواهد شد یک همریختی گروهی پوشای $\theta : \mathrm{Gal}_{\mathbb{F}}\mathbb{K} \to \mathrm{Gal}_{\mathbb{F}}\mathbb{E}$ با هسته $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ وجود دارد. پس بنابر قضیـــه ۲۶.۷، $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ زیرگروه نرمال $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ می‌باشد و طبق قضیه اول یکریختی ۲۹.۷، $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}/\mathrm{Gal}_{\mathbb{E}}\mathbb{K} \cong \mathrm{Gal}_{\mathbb{F}}\mathbb{E}$. ■

مثال ۱۲.۱۱. طبق مثال ۴.۱۱ [۵] میدان شکافندهٔ $\mathbb{K}$ چندجمله‌ای $x^3 - 2$ یک توسیع گالوای $\mathbb{Q}$ می‌باشد که گروه گالوای آن زیرگروهی از S_3 است. چون $x^3 - 2$ چندجمله‌ای کمین $\sqrt[3]{2}$ است، طبق قضیه ۷.۹، $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. هیچکدام از ریشه‌های دیگر ($w\sqrt[3]{2}$ و $w^2\sqrt[3]{2}$) حقیقی نیستند و لذا هیچکدام در $\mathbb{Q}(\sqrt[3]{2})$ نمی‌باشند. پس $[\mathbb{K}:\mathbb{Q}] > 3$. چون $[\mathbb{K}:\mathbb{Q}] \le 6$ (قضایای ۱۳.۹، ۱۴.۹) و $[\mathbb{K}:\mathbb{Q}]$ بر ۳ بخش‌پذیراست (قضیه ۴.۹)، باید داشته باشیم $[\mathbb{K}:\mathbb{Q}] = 6$. پس طبق قضیه ۱۱.۱۱، $\mathrm{Gal}_{\mathbb{Q}}\mathbb{K}$ مرتبه ۶ دارد و برابر S_3 می‌باشد. تنها زیرگروههای S_3 گروه دوری $<(۱۲۳)>$ از مرتبه ۳ و سه زیرگروه دوری از مرتبه ۲: $<(۲۳۱)>$، $<(۱۳)>$ و $<(1,2)>$ می‌باشد. بررسی کنید که تناظر گالوا به صورت زیر است، جایی‌که زیرگروهها و زیرمیدان‌های واقع در یک مکان نسبی با یکدیگر متناظرند. عدد کنار خط رابط بین دو زیرمیدان بعد میدان بزرگتر روی میدان کوچکتر می‌باشد و عدد کنار خط رابط بین زیرگروهها شاخص گروه کوچکتر در گروه بزرگتر است.

۵) S_3 را گروه جایگشت‌های ریشه‌های $\sqrt[3]{2}$، $w\sqrt[3]{2}$ و $w^2\sqrt[3]{2}$، با همین ترتیب. برای مثال، (۱۲) جای $\sqrt[3]{2}$ و $w\sqrt[3]{2}$ را با هم عوض می‌کند و $w^2\sqrt[3]{2}$ را ثابت نگه‌می‌دارد.



میدانهای میانی



زیر گروهها

میدان $\mathbb{Q}(w)$ یک میدان میانی می‌باشد زیرا $w = \frac{1}{2}(\sqrt[3]{2})^2(\sqrt[3]{2}w) \in \mathbb{K}$. $\mathbb{Q}(w)$ میدان شکافنده $x^2 + x + 1$ می‌باشد (تمرین ۳) و بدین دلیل روی $\mathbb{Q}$ گالوا است. زیرگروه متناظر آن زیرگروه نرمال $< (123) >$ می‌باشد. از طرف دیگر، مثال ۱۰.۱۱ نشان می‌دهد که $\mathbb{Q}(\sqrt[3]{2})$ روی $\mathbf{Q}$ گالوا نیست، زیرگروه متناظر آن $< (123) >$ در S_3 نرمال نیست.

مثال قبل یک واقعیت مهم را طرح می‌کند:

در تناظر گالوا رابطه شمولی برعکس می‌شود.

برای مثال، $\mathbb{Q} \subseteq \mathbf{Q}(w)$، ولی زیرگروههای متناظر آن‌ها در رابطه شمول برعکس $S_3 \supseteq < (123) >$ صدق می‌کنند. سرانجام با اثبات لم زیر برهان قضیه اساسی را تمام می‌کنیم.

لم ۱۲.۱۱. گیریم $\mathbb{K}$ یک توسیع میدان با بعد متناهی $\mathbf{F}$، و $\mathbf{E}$ یک میدان میانی باشد که روی $\mathbb{F}$ نرمال است، آنگاه یک همریختی گروهی پوشای $\theta : \mathrm{Gal}_{\mathbf{F}}\mathbb{K} \to \mathrm{Gal}_{\mathbf{F}}\mathbf{E}$ موجود است که هسته آن

$\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ می‌باشد.

برهان. گیریم $\sigma \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ و $u \in E$. آنگاه u روی $\mathbb{F}$ جبری با یک چندجمله‌ای کمین $p(x)$ است. چون $\mathbb{E}$ توسیع نرمال $\mathbb{F}$ است، $p(x)$ در $\mathbb{E}[x]$ تجزیه می‌شود، یعنی تمام ریشه‌های $p(x)$ در $\mathbb{E}$ می‌باشد. چون طبق قضیه ۲.۱۱، $\sigma(u)$ باید یک ریشه $p(x)$ باشد، می‌بینیم که $\sigma(u) \in \mathbb{E}$. بنابراین برای هر $\sigma \in \mathrm{Gal}_{\mathbb{E}}\mathbb{K}$، $\sigma(\mathbb{E}) \subseteq \mathbb{E}$. بدین دلیل تحدید σ به $\mathbb{E}$ (که با $\sigma_{|_{\mathbb{E}}}$ نشان داده می‌شود) یک $\mathbb{F}$-یکریختی $\sigma(\mathbb{E}) \cong \mathbb{E}$ القاء می‌کند. بنابراین طبق قضیه ۵.۹، $[\mathbb{E} : \mathbb{F}] = [\sigma(\mathbb{E}) : \mathbb{F}]$. چون $\mathbb{E} \subseteq \sigma(\mathbb{E}) \subseteq \mathbb{F}$، طبق قضیه ۹.۴ داریم $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \sigma(\mathbb{E})][\sigma(\mathbb{E}) : \mathbb{F}]$، که لزوماً $[\mathbb{E} : \sigma(\mathbb{E})] = ۱$. بنابراین $\mathbb{E} = \sigma(\mathbb{E})$، و در حقیقت $\sigma_{|_{\mathbb{E}}}$ یک خودریختی در $\mathrm{Gal}_{\mathbb{F}}\mathbb{E}$ است.

تابع $\theta : \mathrm{Gal}_{\mathbb{F}}\mathbb{K} \to \mathrm{Gal}_{\mathbb{F}}\mathbb{E}$ با ضابطه $\theta(\sigma) = \sigma_{|_{\mathbb{E}}}$ را تعریف کنید به سادگی بررسی می‌شود که θ یک همریختی گروهی است. هسته آن شامل خودریختی‌هایی از $\mathbb{K}$ است که تحدیدشان به $\mathbb{E}$ نگاشت همانی است. یعنی زیرگروه $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ می‌باشد.

برای این که ثابت کنیم θ پوشاست، به این نکته توجه می‌کنیم که طبق قضیه ۱۵.۹، $\mathbb{K}$ یک میدان شکافنده $\mathbb{F}$ است و از اینرو $\mathbb{K}$ میدان شکافنده همان چندجمله‌ای روی $\mathbb{E}$ است. در نتیجه طبق قضیه ۱۴.۹، هر $\tau \in \mathrm{Gal}_{\mathbb{F}}\mathbb{E}$ قابل توسیع به یک $\mathbb{F}$-خودریختی σ در $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ می‌باشد. این بدان معنی است که $\tau = \sigma_{|_{\mathbb{E}}}$، یعنی $\tau = \theta(\sigma)$. بنابراین θ پوشاست. ■

در برهان قبل از متناهی‌بودن بعد و نرمال بودن $\mathbb{K}$ تا بند سوم استفاده نشد. بنابراین بند اول این حقیقت مفید را ثابت می‌کند:

نتیجه ۱۳.۱۱. گیریم $\mathbb{K}$ یک توسیع $\mathbb{F}$ و $\mathbb{E}$ یک میدان میانی باشد که روی $\mathbb{F}$ نرمال است. اگر $\sigma \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$، آنگاه $\sigma_{|_{\mathbb{E}}} \in \mathrm{Gal}_{\mathbb{F}}\mathbb{E}$.

تمرینها

توجه: $\mathbb{K}$ همیشه یک توسیع میدان $\mathbb{F}$ را نشان می‌دهد.

A.۱. اگر $\mathbb{K}$ روی $\mathbb{F}$ گالوا باشد، ثابت کنید که فقط تعداد با پایانی میدان میانی وجود دارد.

۲. اگر $\mathbb{K}$ یک توسیع نرمال $\mathbb{Q}$ باشد و $[\mathbb{K} : \mathbb{Q}] = p$، که در آن p اول است، نشان دهید که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{K} \cong \mathbb{Z}_p$.

۳. (الف) ثابت کنید که $w = (-۱ + \sqrt{۳}i)/۲$ یک ریشه $x^۳ - ۱$ می‌باشد.

(ب) ثابت کنید که w و w^2 ریشه‌های x^2+x+1 می‌باشند. بدین دلیل $\mathbb{Q}(w)$ میدان شکافنده x^2+x+1 می‌باشد.

۴. تناظر گالوای میدان‌های میانی و زیرگروههای توسیع مفروض $\mathbb{Q}$ را مشخص بفرمایید.

(الف) $\mathbb{Q}(\sqrt{d})$، که در آن $d \in \mathbb{Q}$ ولی $\sqrt{d} \notin \mathbb{Q}$.

(ب) $\mathbb{Q}(w)$، که در آن w همان است که در تمرین ۳ آمده است.

۵. اگر $\mathbb{K}$ روی $\mathbb{F}$ گالوا و $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ یک گروه آبلی از مرتبه ۱۰ باشد، این توسیع چند میدان میانی دارد و بعد آنها روی $\mathbb{F}$ چند است؟

۶. یک مثال از توسیع میدان‌های $\mathbb{K}$ و $\mathbb{L}$ برای $\mathbb{F}$ بیاورید که $\mathbb{K}$ و $\mathbb{L}$ هر دو روی $\mathbb{F}$ گالوا باشند، $\mathbb{K} \neq \mathbb{L}$، و $\mathrm{Gal}_{\mathbb{F}}\mathbb{K} \cong \mathrm{Gal}_{\mathbb{F}}\mathbb{L}$.

۷. برای توسیع‌های مفروض $\mathbb{Q}$، تناظر گالوا را مشخص کنید:

(الف) $\mathbb{Q}(\sqrt{2},\sqrt{3})$ (ب) $\mathbb{Q}(i,\sqrt{2})$

۸. اگر $\mathbb{K}$ روی $\mathbb{F}$ گالوا، $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ آبلی و $\mathbb{E}$ یک میدان میانی باشد که روی $\mathbb{F}$ نرمال است، ثابت کنید که $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ و $\mathrm{Gal}_{\mathbb{F}}\mathbb{E}$ آبلی می‌باشند.

۹. گیریم $\mathbb{K}$ روی $\mathbb{F}$ گالوا و فرض کنیم $\mathrm{Gal}_{\mathbb{F}}\mathbb{K} \cong \mathbb{Z}_n$.

(الف) اگر $\mathbb{E}$ یک میدان میانی باشد که روی $\mathbb{F}$ نرمال است، ثابت کنید $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ و $\mathrm{Gal}_{\mathbb{F}}\mathbb{E}$ دوری می‌باشند.

(ب) ثابت کنید که برای هر شمارنده مثبت n تنها یک میدان میانی وجود دارد و این‌ها تنها میدان‌های میانی می‌باشند.

۱۰. دو میدان میانی $\mathbb{E}$ و $\mathbb{L}$ را **مزدوج** گویند اگر $\sigma \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ وجود داشته باشد به طوری که $\sigma(\mathbb{E}) = \mathbb{L}$. ثابت کنید $\mathbb{E}$ و $\mathbb{L}$ مزدوج می‌باشند اگر و تنها اگر $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$ و $\mathrm{Gal}_{\mathbb{L}}\mathbb{K}$ زیرگروههای مزدوج $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ باشند (همان‌طور که در بند قبل از قضیه ۲۲.۱۰ تعریف شده‌است).

۱۱. (الف) ثابت کنید $K = \mathbb{Q}(\sqrt[4]{2}, i)$ یک میدان شکافنده x^4-2 روی $\mathbb{Q}$ می‌باشد.

(ب) ثابت کنید $[\mathbb{K} : \mathbb{Q}] = 8$ و از قضیه ۱۱.۱۱ نتیجه بگیرید که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{K}$ مرتبهٔ ۸ دارد. [راهنمایی: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$.]

(پ) ثابت کنید $\sigma \in \mathrm{Gal}_{\mathbb{Q}}\mathbb{K}$ وجود دارد که $\sigma(\sqrt[۴]{۲}) = (\sqrt[۴]{۲})i$ و $\sigma(i) = i$ و این که مرتبه σ برابر ۴ می‌باشد.

(ت) طبق قضیه ۱۳.۱۱، تحدید نگاشت مزدوج مختلط به $\mathbb{K}$ یک عضو τ از $\mathrm{Gal}_{\mathbb{Q}}\mathbb{K}$ می‌باشد. ثابت کنید که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{K} = \{\sigma, \sigma^۲, \sigma^۳, \sigma^۴ = \iota, \tau, \sigma\tau, \sigma^۲\tau, \sigma^۳\tau\}$. [راهنمایی، قضیه ۴.۱۱ را بکار برده تا ثابت کنید که این عناصر متمایز می‌باشند.]

(ث) ثابت کنید که $\mathrm{Gal}_{\mathbb{Q}}\mathbb{K} \cong D_۴$. [راهنمایی: σ را به $r_۱$ و τ را به d بنگارید.]

۱۲. گیریم $\mathbb{K}$ مثل تمرین ۱۱ باشد. ثابت کنید که $\mathrm{Gal}_{\mathbb{Q}(i)}\mathbb{K} \cong \mathbb{Z}_۴$.

۱۳. گیریم $\mathbb{K}$ مثل تمرین ۱۱ باشد. تناظر گالوا را برای این توسیع مشخص کنید. [$\mathbb{Q}((۱+i)\sqrt[۴]{۲})$ و $\mathbb{Q}((۱-i)\sqrt[۴]{۲})$ از جمله میدان‌های میانی می‌باشند.]

۱۴. برای توسیع $\mathbb{Q}(\sqrt{۲}, \sqrt{۳}, \sqrt{۵})$ از $\mathbb{Q}$ تناظر گالوا را مشخص کنید. [گروه گالوا هفت زیرگروه از مرتبه ۲ و هفت زیرگروه از مرتبه ۴ دارد.]

۳-۱۱ حلپذیری با رادیکالهـــا

جواب‌های معادله درجه دوم $ax^۲ + bx + c = ۰$ توسط فرمول

$$x = \frac{-b \pm \sqrt{b^۲ - ۴ac}}{۲a}$$

ارائه می‌شود. این حقیقت از دوران باستان شناخته شده بود. در قرن شانزدهم فرمول‌هایی برای حل معادلات درجه دوم و درجه سوم کشف شد. برای مثال جواب‌های معادله $x^۳ + bx + c = ۰$ توسط

$$x = \sqrt[۳]{(-c/۲) + \sqrt{d}} + \sqrt[۳]{(-c/۲) - \sqrt{d}}$$
$$x = w(\sqrt[۳]{(-c/۲) + \sqrt{d}} + w^۲\sqrt[۳]{(-c/۲) - \sqrt{d}}$$
$$x = w^۲(\sqrt[۳]{(-c/۲) + \sqrt{d}} + w\sqrt[۳]{(-c/۲) - \sqrt{d}},$$

عرضه می‌شود که در آن $d = (b^3/27 + c^2/4)$ و $w = (-1 + \sqrt{3}i)/2$ یک ریشه سوم مختلط ۱ می‌باشد، ریشه‌های سوم دیگر طوری انتخاب شده‌اند که [۶]

$$(\sqrt[3]{(-c/2) + \sqrt{d}})(\sqrt[3]{(-c/2) - \sqrt{d}}) = -b/3.$$

روفینی و آبل در سال‌های اول ۱۸۰۰ میلادی مستقلاً ثابت کردند که برای $n \geq 5$، هیچ فرمولی برای حل تمام معادلات درجه n وجود ندارد. ولی تجزیه و تحلیل کامل این مسئله به گالوا منتسب می‌شود که معیاری برای تعیین این که کدام معادلات با فرمول حلپذیرند ارائه کرد. این معیار، که در اینجا آمده است، به‌ما کمک می‌کند که بتوانیم چندجمله‌ای درجه پنجمی ارائه کنیم که با یک دستورالعمل قابل حل نیست. برای ساده کردن این مبحث فرض می‌کنیم که تمامی میدان‌ها مشخصه صفر داشته باشند.

همانگونه که در بالا مطرح گردید یک فرمول روش مشخصی است که با ضرایب چندجمله‌ای $f(x) \in \mathbb{F}[x]$ شروع می‌شود و فقط با استفاده از اعمال میدان (جمع، تفریق، ضرب و تقسیم) و استخراج ریشه (ریشه‌های دوم، سوم، چهارم و غیره) به جواب معادله $f(x) = 0_F$ می‌رسد. در این زمینه، یک **ریشه n–ام** یک عضو c در $\mathbb{F}$، ریشهٔ دلخواهی از چندجمله‌ای $x^n - c$ در یک توسیع میدان $\mathbb{F}$ است.

اگر $f(x) \in \mathbb{F}[x]$، آنگاه انجام اعمال میدان، ما را از میدان ضرایب $\mathbb{F}$ بیرون نخواهد برد (بسته بودن!)، ولی ریشه n–ام گرفتن ممکن است شما را در یک توسیع میدان قرار دهد. گرفتن m–امین ریشه مجدد بعد از آن ممکن است ما را باز به توسیع دیگری سوق دهد. بدین دلیل وجود فرمولی برای $f(x) = 0_F$ ایجاب می‌کند که این جواب‌ها در توسیعی خاص از توسیع میدان $\mathbb{F}$ باشد.

مثال ۱۳.۱۱. بکارگیری فرمول ریشه سوم بالا با شرط $b = 3$ و $c = 2$ نشان می‌دهد که جوابهای معادله $x^3 + 3x + 2 = 0$ عبارتند از:

$$\sqrt[3]{-1 + \sqrt{2}} + \sqrt[3]{-1 - \sqrt{2}},$$
$$w\sqrt[3]{-1 + \sqrt{2}} + w^2\sqrt[3]{-1 - \sqrt{2}},$$
$$w^2\sqrt[3]{-1 + \sqrt{2}} + w\sqrt[3]{-1 - \sqrt{2}}$$

۶) فرمولهای معادلات درجه سوم کلی و درجه چهارم مشابه ولی پیچیده‌تر می‌باشند.

تمام این جوابها در زنجیر توسیع:

$$\begin{array}{ccccccccc} \mathbb{Q} & \subseteq & \mathbb{Q}(w) & \subseteq & \mathbb{Q}(w,\sqrt{2}) & \subseteq & \mathbb{Q}(w,\sqrt{2},\sqrt[3]{-1+\sqrt{2}}) & \subseteq & \mathbb{Q}(w,\sqrt{2},\sqrt[3]{-1+\sqrt{2}},\sqrt[3]{-1-\sqrt{2}}) \\ \| & & \| & & \| & & \| & & \| \\ F_0 & \subseteq & F_1 & \subseteq & F_2 & \subseteq & F_3 & \subseteq & F_4 \end{array}$$

قرار دارند. هر میدان این زنجیر توسیعی ساده از میدان قبل و به صورت $\mathbb{F}_j(u)$ است که در آن برای یک n، $u^n \in \mathbb{F}_j$ (یعنی، u یک n–امین ریشه یک عضو $\mathbb{F}_j$ می‌باشد.):

- $\mathbb{F}_1 = \mathbb{F}_0(w)$ که در آن $w^3 = 1 \in \mathbb{F}_0$.
- $\mathbb{F}_2 = \mathbb{F}_1(\sqrt{2})$ که در آن $(\sqrt{2})^2 = 2 \in \mathbb{F}_0 \subseteq \mathbb{F}_1$.
- $\mathbb{F}_3 = \mathbb{F}_2(\sqrt[3]{-1+\sqrt{2}})$ که در آن $(\sqrt[3]{-1+\sqrt{2}})^3 = -1+\sqrt{2} \in \mathbb{F}_2$.
- $\mathbb{F}_4 = \mathbb{F}_3(\sqrt[3]{-1-\sqrt{2}})$ که در آن $(\sqrt[3]{-1-\sqrt{2}})^3 = -1-\sqrt{2} \in \mathbb{F}_2 \subseteq \mathbb{F}_3$.

چون $\mathbb{F}_4$ تمام جواب‌های $x^2+3x+2=0$ را شامل است، یک میدان شکافنده x^2+3x+2 را نیز شامل می‌باشد.

یک میدان $\mathbb{K}$ یک **توسیع رادیکال** یک میدان $\mathbb{F}$ نامیده می‌شود اگر یک زنجیر از میدان‌های

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_t = \mathbb{K}$$

موجود باشد به طوری که برای هر $i = 1, 2, \ldots, t$، $\mathbb{F}_i = \mathbb{F}_{i-1}(u_i)$ و توانی از u_i در $\mathbb{F}_{i-1}$ باشد. در مثال اخیر، برای نمونه $\mathbb{Q}(w, \sqrt{2}, \sqrt[3]{-1+\sqrt{2}}, \sqrt[3]{-1-\sqrt{2}})$ یک توسیع رادیکال $\mathbb{Q}$ می‌باشد. هر توسیع رادیکال $\mathbb{F}$ روی $\mathbb{F}$ با بعد متناهی می‌باشد (تمرین ۳).

گیریم $f(x) \in \mathbb{F}[x]$، معادله $f(x) = 0_{\mathbb{F}}$ را **حلپذیر با رادیکالها** گوییم اگر یک توسیع رادیکال $\mathbb{F}$ موجود باشد که شامل یک توسیع میدان شکافنده $f(x)$ باشد. مثال فوق نشان می‌دهد که $x^3+3x+1=0$ با رادیکالها حلپذیر است.

بحث پیشین نشان داد که اگر فرمولی برای جواب‌های معادله $f(x) = 0_{\mathbb{F}}$ وجود داشته باشد، معادله حلپذیر با رادیکالها می‌باشد. متقابلاً، اگر $f(x) = 0_{\mathbb{F}}$، با رادیکالها حلپذیر نباشد آنگاه فرمولی که جوابهایش را پیدا کنیم (در مفهومی که در بالا بحث کردیم) نمی‌تواند وجود داشته باشد.

اگر $f(x) \in \mathbb{F}[x]$، آنگاه **گروه گالوای** چندجمله‌ای $f(x)$، $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ می‌باشد، که در آن $\mathbb{K}$ یک میدان شکافنده $f(x)$ روی $\mathbb{F}$ است[۷]. **معیار گالوا** بیان می‌کند که $f(x) = 0$ با رادیکالها حلپذیر

۷) چون طبق قضیه ۱۴.۹ هر دو میدان شکافنده $f(x)$ یکریخت می‌باشند، نتیجه می‌شود که گروههای گالوای متناظر یکریخت می‌باشند. پس گروه گالوای $f(x)$ مستقل از انتخاب $\mathbb{K}$ می‌باشد.

است اگر و تنها اگر گروه گالوای $f(x)$ یک گروه حلپذیر باشد، همان‌طور که در زیر تعریف شده است:

تعریف. گروه G را **حلپذیر** گوییم اگر زنجیری از زیرگروههای

$$G = G_0 \supseteq G_1 \supseteq G_2 \cdots \supseteq G_{n-1} \supseteq G_n = < e >$$

داشته باشد که هر G_i زیرگروهی نرمال از گروه پیشین G_{i-1} باشد و گروه خارج قسمت G_{i-1}/G_i آبلی باشد.

مثال ۱۴.۱۱. هر گروه آبلی G حلپذیر است زیرا هر گروه خارج قسمت G آبلی است. بنابراین دنباله $G \supseteq < e >$ در شرایط این تعریف صدق می‌کند.

مثال ۱۵.۱۱. گیریم $< (۱۲۳) >$ زیرگروه دوری از مرتبه ۳ در S_3 باشد. زنجیر $S_3 \supseteq < (۱۲۳) > \supseteq < (۱) >$ نشان می‌دهد که S_3 حلپذیر است. در حالت کلی قضیه زیر را برای گروههای متقارن دیگر داریم:

قضیه ۱۴.۱۱. برای $n \geq 5$ گروه S_n حلپذیر نیست.

برهان. به خلاف، فرض کنید که S_n حلپذیر باشد و این که

$$S_n = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t = < (1) >$$

یک زنجیر از زیرگروهها باشد که در تعریف حلپذیری صدق کند، گیریم (rst) یک ۳–دور در S_n باشد و گیریم u و v عضوهای دلخواهی از $\{1, 2, \ldots, n\}$ به غیر از r، s و t باشد (u و v وجود دارد زیرا $n \geq 5$). چون S_n/G_1 آبلی است، قضیه ۲۴.۷ (با شرط $a = (tus)$، $b = (srv)$) نشان می‌دهد که G_1 باید شامل

$$(tus)(srv)(tus)^{-1}(srv)^{-1} = (tus)(srv)(tsu)(svr) = (rst)$$

باشد. بنابراین G_1 تمام ۳–دورها را شامل است. چون G_1/G_2 آبلی است، می‌توانیم این استدلال را با شرط G_1 بجای S_n و G_2 بجای G_1 تکرار کنیم و نتیجه بگیریم که G_2 تمام ۳–دورها را شامل است. این واقعیت که هر G_{i-1}/G_i آبلی است و تکرار روند فوق منجر به این حکم می‌شود که زیرگروه همانی G_t تمام ۳–دورها را شامل است که یک تناقض می‌باشد. پس S_n حلپذیر نیست. ■

یک خاصیت کلیدی گروههای حلپذیر که در ادامه مورد نیاز خواهد بود قضیه زیر است:

قضیه ۱۵.۱۱. هر تصویر همریختی یک گروه حلپذیر، حلپذیر است.

برهان. فرض کنید که G یک گروه حلپذیر و $f : G \to H$ یک همریختی پوشا باشد. زنجیر حلپذیری $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t = \langle e_G \rangle$ از G را در نظر بگیرید. برای هر i، گیریم $H_i = f(G_i)$ و این زنجیر از زیرگروهها

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_t = f(\langle e_G \rangle) = \langle e_H \rangle$$

را در نظر بگیرید. بررسی کنید که برای هر $i = 1, 2, \ldots, t$، H_i زیرگروه نرمال H_{i-1} است. گیریم $a, b \in H_{i-1}$. آنگاه $c, d \in G_{i-1}$ وجود دارد به طوری که $f(c) = a$ و $f(d) = b$. چون طبق تعریف حلپذیری G_{i-1}/G_i آبلی است، طبق قضیه ۲۴.۷، $cdc^{-1}d^{-1} \in G_i$. در نتیجه

$$aba^{-1}b^{-1} = f(c)f(d)f(c^{-1})f(d^{-1}) = f(cdc^{-1}d^{-1}) \in f(G_i) = H_i.$$

بنابراین طبق قضیه ۲۴.۷، H_{i-1}/H_i آبلی است و H حلپذیر می‌باشد. ■

برای این که معیار حلپذیری گالوا را ثابت کنیم به اطلاعات بیشتری در مورد توسیع‌های رادیکال و ریشه‌های n–ام احتیاج داریم. اگر $\mathbb{K}$ یک میدان و $\zeta \in \mathbb{K}$ یک جواب $x^n - 1_{\mathbb{K}} = 0_{\mathbb{K}}$ باشد، آنگاه ζ را **n–امین ریشه واحد** می‌نامند. چون nx^{n-1}، مشتق $x^n - 1_K$، مخالف صفر می‌باشد (زیرا $\mathbb{K}$ دارای مشخصهٔ صفر می‌باشد) و نسبت به $x^n - 1_{\mathbb{K}}$ اول است، بنابراین طبق لم ۱۶.۹، $x^n - 1_{\mathbb{K}}$ تفکیک‌پذیر می‌باشد. در نتیجه درست n ریشه متمایز واحد در $\mathbb{K}$ وجود دارد. اگر ζ و t ریشه n–ام واحد باشند آنگاه

$$(\zeta t)^n = \zeta^n t^n = 1_{\mathbb{K}} 1_{\mathbb{K}} = 1_{\mathbb{K}}.$$

بدین دلیل مجموعه ریشه‌های n–ام واحد تحت ضرب بسته است و بنابراین زیرگروهی از گروه ضربی میدان $\mathbb{K}$ می‌باشد (قضیه ۸.۷). طبق قضیه ۴۱.۷ (یا نتیجه ۱۱.۱۰) این گروه دوری است. هر مولد این گروه دوری را یک **n–امین ریشه اولیه واحد** می‌نامند. بنابراین ζ یک n–امین ریشه اولیه واحد است اگر و فقط اگر ζ، ζ^2، ζ^3، ...، $\zeta^n = 1_{\mathbb{F}}$، n ریشه متمایز n–ام واحد باشد.

مثال ۱۶.۱۱. ریشه‌های چهارم واحد در $\mathbb{C}$، ۱، -۱، i، $-i$ می‌باشد. چون $i^۲ = -۱$، $i^۳ = -i$ و $i^۴ = ۱$، i یک چهارمین ریشه اولیه واحد است. قضیهٔ دموآور نشان می‌دهد که برای هر عدد صحیح مثبت n،

$$\cos(۲\pi/n) + i\sin(۲\pi/n) \text{ یک } n\text{-امین ریشه اولیه واحد در } \mathbb{C} \text{ است.}$$

وقتی $n = ۳$، بنابر این قضیه، $w = \cos(۲\pi/۳) + i\sin(۲\pi/۳) = (-۱/۲) + (\sqrt{۳}/۲)i$ یک ریشه سوم اولیه واحد می‌باشد.

لم ۱۶.۱۱. گیریم $\mathbb{K}$ یک میدان و ζ یک n-امین ریشه اولیه واحد در $\mathbb{K}$ باشد آنگاه برای هر شمارنده مثبت d از n، $\mathbb{K}$ یک d-امین ریشه اولیه واحد را شامل است.

برهان. طبق فرض، مرتبه ζ در گروه ضربی $\mathbb{K}$ برابر n می‌باشد. اگر $n = dt$، آنگاه طبق قضیه ۵.۷ مرتبه ζ^t برابر d است. بنابراین ζ^t یک زیرگروه از مرتبه d را تولید می‌کند که طبق نتیجه ۳۴.۷ هر یک از عضوهای آن باید مرتبه‌ای داشته باشد که d را بشمارد. به بیان دیگر برای هر k، $((\zeta^t)^k)^d = ۱_{\mathbb{K}}$). بدین دلیل d عنصر متمایز ζ^t، $(\zeta^t)^۲$، $(\zeta^t)^{d-۱}$، ...، $(\zeta^t)^d = ۱_{\mathbb{K}}$ ریشه‌های $x^d - ۱_{\mathbb{K}}$ می‌باشند. چون $x^d - ۱_{\mathbb{K}}$ دارای حداکثر d ریشه می‌باشد و هر ریشه d-ام واحد یک ریشه $x^d - ۱_{\mathbb{K}}$ است، ζ^t یک d-امین ریشه اولیه واحد است. ■

اکنون می‌توانیم مطالب پیش را بهم پیوند بزنیم و دو قضیه را ثابت کنیم که حالت‌های خاص معیار گالوا می‌باشند و به‌علاوه ابزارهای اساسی برای اثبات حالت کلی نیز می‌باشند.

قضیه ۱۷.۱۱. گیریم $\mathbb{F}$ یک میدان با مشخصه صفر و ζ یک n-امین ریشه اولیه واحد در یک توسیع میدان $\mathbb{F}$ باشد. آنگاه $\mathbb{K} = \mathbb{F}(\zeta)$ یک توسیع نرمال $\mathbb{F}$ است و $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ آبلی می‌باشد.

برهان. میدان $\mathbb{K} = \mathbb{F}(\zeta)$ تمام توانهای ζ را شامل است [۸] و بنابراین یک میدان شکافنده $x^n - ۱_{\mathbb{F}}$ است. پس طبق قضیه ۱۵.۹، $\mathbb{K}$ روی $\mathbb{F}$ نرمال است. هر خودریختی در گروه گالوا باید طبق قضیه ۲.۱۱، ζ را به یک ریشه $x^n - ۱_{\mathbb{F}}$ بنگارد. بنابراین اگر $\sigma, \tau \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$، آنگاه برای برخی اعداد

۸) میدان $\mathbb{K} = \mathbb{F}(\zeta)$ یک توسیع رادیکال $\mathbb{F}$ است زیرا $\zeta^n = ۱_{\mathbb{F}}$. بنابراین $x^n - ۱_{\mathbb{F}} = ۰$ با رادیکالها حلپذیر است. بنابراین قضیه‌ای که بیان می‌کند، $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ (گروه گالوای $x^n - ۱_{\mathbb{F}}$) آبلی است و درنتیجه حلپذیر است، حالتی خاص از معیار گالوا می‌باشد.

صحیح مثبت k، $\sigma(\zeta) = \zeta^k$ و $\tau(\zeta) = \zeta^t$. در نتیجه،

$$(\sigma \circ \tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^t) = \sigma(\zeta)^t = (\zeta^k)^t = \zeta^{kt}.$$
$$(\tau \circ \sigma)(\zeta) = \tau(\sigma(\zeta)) = \tau(\zeta^k) = \tau(\zeta)^k = (\zeta^t)^k = \zeta^{kt}.$$

بنابراین طبق قضیه ۴.۱۱، $\sigma \circ \tau = \tau \circ \sigma$ و $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ آبلی است. ■

قضیه ۱۸.۱۱. گیریم $\mathbb{F}$ میدانی با مشخصه صفر باشد که یک n–امین ریشه اولیه واحد را شامل است. اگر u یک ریشه $x^n - c \in \mathbb{F}[x]$ در یک توسیع میدان $\mathbb{F}$ باشد، آنگاه $\mathbb{K} = \mathbb{F}(u)$ یک توسیع نرمال $\mathbb{F}$ است و $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ آبلی است.

برهان[۹]. طبق فرض، $u^n = c$. اگر ζ یک n–امین ریشه اولیه واحد در $\mathbb{F}$ باشد آنگاه برای هر k،

$$(\zeta^k u)^n = (\zeta^k)^n u^n = (\zeta^n)^k u^n = 1_{\mathbb{F}} c = c.$$

در نتیجه، چون ζ، ζ^2، ...، $\zeta^n = 1_{\mathbb{F}}$ عضوهای متمایز $\mathbb{F}$ می‌باشند عضوهای ζu، $\zeta^2 u$، ...، $\zeta^n u = u$، n–ریشه متمایز $x^n - c$ می‌باشند. بدین ترتیب $\mathbb{K} = \mathbb{F}(u)$ یک میدان شکافنده $x^n - c$ روی $\mathbb{F}$ است و بنابراین طبق قضیه ۱۵.۹ روی $\mathbb{F}$ نرمال است.[۱۰] اگر $\sigma, \tau \in \mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ آنگاه طبق قضیه ۲.۱۱، برای برخی k، t، $\sigma(u) = \zeta^k u$ و $\tau(u) = \zeta^t u$. در نتیجه

$$(\sigma \circ \tau)(u) = \sigma(\tau(u)) = \sigma(\zeta^t u) = \sigma(\zeta^t)\sigma(u) = \zeta^t(\zeta^k u) = \zeta^{t+k} u.$$
$$(\tau \circ \sigma)(u) = \tau(\sigma(u)) = \tau(\zeta^k u) = \tau(\zeta^k)\tau(u) = \zeta^k(\zeta^t u) = \zeta^{t+k} u.$$

بنابراین طبق قضیه ۴.۱۱، $\sigma \circ \tau = \tau \circ \sigma$ و $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ آبلی است. ■

قضیه ۱۹.۱۱. (معیار گالوا) گیریم $\mathbb{F}$ میدانی با مشخصه صفر و $f(x) \in \mathbb{F}[x]$ باشد. آنگاه $f(x) = 0_{\mathbb{F}}$ حلپذیر با رادیکال‌ها است اگر و تنها اگر گروه گالوای $f(x)$ حلپذیر باشد.

ما فقط آن نیمه از قضیه را که در ادامه مورد نیـاز اسـت ثابـت می‌کنیم. بـرای اثبـات نیمه

۹) برای اثبات دیگری که نشان می‌دهد $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ به واقع دوری است تمرین ۲۲ را نگاه کنید.

۱۰) میدان $\mathbb{K} = \mathbb{F}(u)$ نیز یک توسیع رادیکال $\mathbb{F}$ است زیرا $u^n = c \in \mathbb{F}$، بنابراین $x^n - c = 0$ حلپذیر با رادیکالها می‌باشد. از اینرو این قضیه حالت خاص دیگری از معیار گالوا است.

دیگر به هانگرفورد[۱۱] [۷] یا جیکوبسن[۱۲] [۸] مراجعه کنید.

برهان قضیه ۱۹.۱۱. فرض کنید که $f(x) = 0_{\mathbb{F}}$ حلپذیر با رادیکالها باشد. برهان در سه مرحله زیر کامل می‌شود:

۱. قضیه ۲۱.۱۱: یک توسیع نرمال رادیکال $\mathbb{K}$ از $\mathbb{F}$ وجود دارد که شامل یک میدان شکافنده $f(x)$ است.[۱۳]

۲. طبق قضیه ۱۵.۹، میدان $\mathbb{E}$ روی $\mathbb{F}$ نرمال است.

۳. قضیه ۲۲.۱۱: هر میدان میانی $\mathbb{K}$ که روی $\mathbb{F}$ نرمال است یک گروه گالوای حلپذیر دارد؛ به ویژه، $\mathrm{Gal}_{\mathbb{F}}\mathbb{E}$ (گروه گالوای $f(x)$) حلپذیر است. ■

قبل از تکمیل اثبات قضیه ۱۹.۱۱، از آن استفاده می‌کنیم تا حلپذیر نبودن معادلات درجه پنجم را ثابت کنیم.

مثال ۱۷.۱۱. ادعا می‌کنیم که گروه گالوای $f(x) = 2x^5 - 10x + 5 \in \mathbb{Q}[x]$، S_5 است، که طبق قضیه ۱۹.۱۱ حلپذیر با رادیکالها نمی‌باشد. بنابراین **هیچ فرمولی (شامل فقط اَعمال میدان و استخراج ریشه‌ها) برای جواب تمام معادلات درجه پنجم وجود ندارد.**

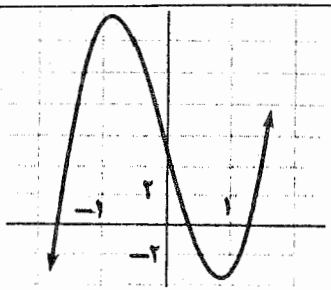
برای اثبات مدّعای خود، توجه می‌کنیم که مشتق $f(x)$، $10x^4 - 10$ است که تنها ریشه‌های حقیقی آن ± 1 است (ریشه‌های دیگر $\pm i$ می‌باشد). چون $f''(x) = 40x^3$، آزمون مشتق دوم از حسابان مقدماتی نشان می‌دهد که $f(x)$ دارای درست یک ماکزیمم نسبی در نقطه $x = -1$، یک مینیمم نسبی در $x = 1$ و یک نقطه عطف در $x = 0$ است. بنابراین شمای کلی نمودار آن باید به صورت زیر باشد، به ویژه $f(x)$ دارای درست سه ریشه حقیقی است.

---

۱۱) Hungerford

۱۲) Jacobson

۱۳) این یک نکته فنی بسیار مهم است. تعریف حلپذیری توسط رادیکالها، تنها متضمن یک توسیع رادیکال $\mathbb{F}$ است که $\mathbb{E}$ را شامل می‌باشد. اما یک توسیع رادیکال لزوماً روی $\mathbb{F}$ نرمال نیست (تمرین ۱۹)، و در این صورت قضیه اساسی ۱۱.۱۱ را نمی‌توان بکار برد.



توجه کنید که طبق معیار آیزنشتاین، $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است (با $p = 5$). اگر $\mathbb{K}$ توسیع میدان شکافنده $f(x)$ در $\mathbb{C}$ باشد، آنگاه طبق قضیه اساسی، $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ دارای مرتبه $[\mathbb{K} : \mathbb{Q}]$ است. اگر r ریشه دلخواهی از $f(x)$ باشد، آنگاه طبق قضیه ۴.۹، $[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}(r)][\mathbb{Q}(r) : \mathbb{Q}]$. و طبق قضیه ۷.۹، $[\mathbb{Q}(r) : \mathbb{Q}] = 5$. بنابراین مرتبه $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ بر ۵ بخش‌پذیر است. می‌توان ثابت کرد که $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ یک عضو از مرتبه ۵ دارد[۱۴].

گروه $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$، که به عنوان یک گروه از جایگشت‌های ریشه‌های $f(x)$ در نظرگرفته شده است، زیرگروهی از S_5 می‌باشد (نتیجه ۵.۱۱) ولی تنها عناصر از مرتبه ۵ در S_5، ۵−دورها می‌باشند (بخش ۹.۷ تمرین ۱۳ را ببینید). پس $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ شامل یک ۵−دور است. عمل مزدوج مختلط یک خودریختی روی $\mathbb{K}$ القاء می‌کند (نتیجه ۱۳.۱۱). این خودریختی دو ریشه غیرحقیقی $f(x)$ را جابجا می‌کند و سه ریشه حقیقی را ثابت نگه می‌دارد. بدین دلیل $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ شامل یک دور دوتایی است. تمرین ۸ نشان می‌دهد که تنها زیرگروه S_5 که شامل یک ۵ـ دور و یک دور دوتایی است خود S_5 است، پس همان طور که ادعا کردیم $\mathrm{Gal}_{\mathbb{F}}\mathbb{K} = S_5$.

اینک، تکمیل برهان معیار گالوا را با بیان یک لم فنی آغاز می‌کنیم که اهمیت آن در قضیه بعد آشکار می‌شود.

لم ۲۰.۱۱. گیریم $\mathbb{F}$، $\mathbb{E}$، $\mathbb{L}$ میدان‌هایی از مشخصه صفر باشد، به طوری که

$$v^k \in \mathbb{E} \quad \text{و} \quad \mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{L} = \mathbb{E}(v)$$

اگر $\mathbb{L}$ روی $\mathbb{F}$ با بعد متناهی و $\mathbb{E}$ روی $\mathbb{F}$ نرمال باشد، آنگاه یک توسیع میدان $\mathbb{M}$ از $\mathbb{L}$ وجود دارد که یک توسیع رادیکال $\mathbb{E}$ می‌باشد و یک توسیع نرمال $\mathbb{F}$ است.

برهان. طبق قضیه ۱۵.۹، $\mathbb{E}$ میدان شکافنده یک $g(x) \in \mathbb{F}[x]$ روی $\mathbb{F}$ است. گیریم $p(x) \in \mathbb{F}[x]$ چندجمله‌ای کمین v روی $\mathbb{F}$ و $\mathbb{M}$ یک میدان شکافنده $g(x)p(x)$ روی $\mathbb{F}$ باشد.

۱۴) اگر فصل ۱۰ را خوانده‌اید از نتیجه ۱۴.۱۰ استفاده کنید، در غیر این‌صورت، از تمرین ۹ استفاده کنید.

آنگاه طبق قضیه ۱۵.۹، $\mathbb{M}$ روی $\mathbb{F}$ نرمال است. به‌علاوه $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{L} \subseteq \mathbb{M}$ (زیرا $\mathbb{L} = \mathbb{E}(v)$) و $\mathbb{E}$ روی $\mathbb{F}$ توسط ریشه‌های $g(x)$ پدید آمده است. گیریم $v = v_1, v_2, \ldots, v_r$، تمام ریشه‌های $p(x)$ در M باشد. طبق قضیه ۳.۱۱، برای هر i، $\sigma_i \in \mathrm{Gal}_{\mathbb{E}}\mathbb{M}$ وجود دارد به طوری که $\sigma_i(v) = v_i$. نتیجه ۱۳.۱۱ نشان می‌دهد که $\sigma_i(\mathbb{E}) \subseteq \mathbb{E}$. طبق فرض، $v^k = b \in \mathbb{E}$؛ بنابراین برای هر i،

$$(v_i)^k = \sigma_i(v)^k = \sigma_i(v^k) = \sigma_i(b) \in \mathbb{E} \subseteq \mathbb{E}(v_1, \ldots, v_{i-1}).$$

در نتیجه،

$$\mathbb{E} \subseteq \mathbb{L} = \mathbb{E}(v_1) \subseteq \mathbb{E}(v_1, v_2) \subseteq \mathbb{E}(v_1, v_2, v_3) \subseteq \cdots \subseteq \mathbb{E}(v_1, v_2, \ldots, v_r) = M$$

یک توسیع رادیکال $\mathbb{E}$ است. ■

قضیه ۲۱.۱۱. گیریم $\mathbb{F}$ میدانی از مشخصهٔ صفر باشد و $f(x) \in \mathbb{F}[x]$. اگر $f(x) = 0_{\mathbb{F}}$ حلپذیر با رادیکال‌ها باشد، آنگاه یک توسیع میدان نرمال رادیکال $\mathbb{F}$ وجود دارد که شامل یک میدان شکافندهٔ $f(x)$ است.

برهان. طبق تعریف، یک میدان شکافنده $\mathbb{K}$ از $f(x)$ در یک توسیع رادیکال

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_t$$

قرار دارد که در آن $\mathbb{F}_i = \mathbb{F}_{i-1}(u_i)$ و برای هر $i = 1, 2, \ldots, t$، $(u_i)^{n_i} \in \mathbb{F}_{i-1}$ می‌باشد. استفاده از لم ۲۰.۱۱ با شرط $\mathbb{E} = \mathbb{F}$، $\mathbb{L} = \mathbb{F}_1$، و $v = u_1$ یک توسیع میدان نرمال رادیکال $\mathbb{M}_1$ ایجاد می‌کند. بنا به فرض $(u_2)^{n_2} \in \mathbb{F}_1 \subseteq \mathbb{M}_1$. با استفاده از لم ۲۰.۱۱ با شرط $\mathbb{E} = \mathbb{M}_1$، $v = u_2$ و $\mathbb{L} = \mathbb{M}_1(u_2)$ یک توسیع میدان نرمال $\mathbb{M}_2$ از $\mathbb{F}$ ایجاد می‌شود که توسیع رادیکال $\mathbb{M}_1$ و در نتیجه یک توسیع رادیکال $\mathbb{F}$ است، به‌علاوه، $\mathbb{M}_2$ شامل $\mathbb{F}_2 = \mathbb{F}_1(u_2)$ است. تکرار متوالی این استدلال به یک توسیع میدان نرمال رادیکال $\mathbb{M}_t$ از $\mathbb{F}$ منجر می‌شود که شامل $\mathbb{F}_t$ است و بنابراین $\mathbb{K}$ را شامل می‌باشد. ■

قضیه ۲۲.۱۱. گیریم $\mathbb{K}$ یک توسیع میدان نرمال رادیکال $\mathbb{F}$ و $\mathbb{E}$ یک میدان میانی باشد که همگی مشخصه صفر دارند. اگر $\mathbb{E}$ روی $\mathbb{F}$ نرمال باشد، آنگاه $\mathrm{Gal}_{\mathbb{F}}\mathbb{E}$ یک گروه حلپذیر است.

برهان. طبق فرض یک زنجیر از زیرمیدان‌های

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_t = \mathbb{K}$$

وجود دارد که در آن $\mathbb{F}_i = \mathbb{F}_{i-1}(u_i)$ و برای هر $i = 1, 2, \ldots, t$، $(u_i)^{n_i}$ در $\mathbb{F}_{i-1}$ قرار دارد. گیریم n کوچکترین مضرب مشترک $n_1, n_2, \ldots, n_t$ و ζ یک n–امین ریشه اولیه واحد باشد. برای هر $i \geq 0$، گیریم $\mathbb{E}_i = \mathbb{F}_i(\zeta)$. آنگاه برای هر $i \geq 1$،

$$\mathbb{E}_i = \mathbb{F}_i(\zeta) = \mathbb{F}_{i-1}(u_i)(\zeta) = \mathbb{F}_{i-1}(u_i, \zeta) = \mathbb{F}_{i-1}(\zeta)(u_i) = \mathbb{E}_{i-1}(u_i).$$

چون برای هر $i \geq 1$، $(u_i)^{n_i} \in \mathbb{F}_{i-1} \subseteq \mathbb{E}_{i-1}$ و $\zeta^n \in \mathbb{F}$، زنجیر

$$\mathbb{F} \subseteq \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \mathbb{E}_2 \subseteq \mathbb{E}_3 \subseteq \cdots \subseteq \mathbb{E}_t = \mathbb{L}$$

یک توسیع رادیکال $\mathbb{F}$ است که شامل $\mathbb{K}$ (و همین‌طور $\mathbb{E}$) می‌باشد[۱۵]. طبق قضیه ۱۵.۹، توسیع نرمال $\mathbb{L} = \mathbb{E}_t = \mathbb{F}_t(\zeta)$ میدان شکافنده یک چندجمله‌ای $p(x) \in \mathbb{F}[x]$ است و بنابراین $\mathbb{L} = \mathbb{E}_t = \mathbb{F}_t$ میدان شکافنده $p(x)(x^n - 1_{\mathbb{F}})$ روی $\mathbb{F}$ است. درنتیجه، طبق قضیه‌های ۱۵.۹ و ۱۷.۹، $\mathbb{L}$ روی $\mathbb{F}$ گالوا است.

زنجیر زیر از زیرگروههای $\mathrm{Gal}_{\mathbb{F}}\mathbb{L}$ را در نظر بگیرید:

$$\mathrm{Gal}_{\mathbb{F}}\mathbb{L} \supseteq \mathrm{Gal}_{\mathbb{E}_0}\mathbb{L} \supseteq \mathrm{Gal}_{\mathbb{E}_1}\mathbb{L} \supseteq \mathrm{Gal}_{\mathbb{E}_2}\mathbb{L} \supseteq \cdots \supseteq \mathrm{Gal}_{\mathbb{E}_{t-1}}\mathbb{L} \supseteq \mathrm{Gal}_{\mathbb{L}}\mathbb{L} = <\iota>.$$

نشان خواهیم داد که هر زیرگروه در زیرگروه قبلی نرمال و هر خارج قسمت آبلی است. چون هر n_i، n را می‌شمارد. طبق لم ۱۶.۱۱، $\mathbb{E}_0$ یک n_i–امین ریشه اولیهٔ واحد را شامل می‌باشد. درنتیجه، بنابر قضیه ۱۸.۱۱ هر $\mathbb{E}_i$ (با شرط $i \geq 1$) یک توسیع نرمال $\mathbb{E}_{i-1}$ می‌باشد وگروه گالوای $\mathrm{Gal}_{\mathbb{E}_{i-1}}\mathbb{E}_i$ آبلی است. چون $\mathbb{L}$ روی $\mathbb{F}$ گالوا می‌باشد، $\mathrm{Gal}_{\mathbb{E}_{i-1}}\mathbb{L}/\mathrm{Gal}_{\mathbb{E}_i}\mathbb{L}$، با گروه آبلی $\mathrm{Gal}_{\mathbb{E}_{i-1}}\mathbb{E}_i$ یکریخت است. به طور مشابه طبق قضایای ۱۱.۱۱ و ۱۷.۱۱، $\mathbb{E}_0$ روی $\mathbb{F}$ نرمال است، $\mathrm{Gal}_{\mathbb{E}_0}\mathbb{L}$ در $\mathrm{Gal}_{\mathbb{F}}\mathbb{L}$ نرمال است و $\mathrm{Gal}_{\mathbb{F}}\mathbb{L}/\mathrm{Gal}_{\mathbb{E}_0}\mathbb{L}$ با گروه آبلی $\mathrm{Gal}_{\mathbb{F}}\mathbb{E}_0$ یکریخت می‌باشد. بنابراین $\mathrm{Gal}_{\mathbb{F}}\mathbb{L}$ یک گروه حلپذیر است.

۱۵) ساختار $\mathbb{L}$ به فرض این که $\mathbb{K}$ روی $\mathbb{F}$ نرمال است بستگی ندارد و همانگونه که در زیر خواهیم دید هر میدان در این زنجیر، توسیع نرمال میدان بلافصل قبل از خود می‌باشد، ولی این برای تضمین نرمال بودن $\mathbb{L}$ (بنابراین گالوا بودن) روی $\mathbb{F}$ کافی نیست (تمرین ۱۹). ما فرض نرمال بودن $\mathbb{K}$ روی $\mathbb{F}$ را برای تضمین این مطلب نیاز داریم تا بتوانیم قضیه اساسی را روی $\mathbb{L}$ بکار ببریم.

چون $\mathbb{E}$ روی $\mathbb{F}$ نرمال است، قضیه اساسی نشان می‌دهد که $\mathrm{Gal}_{\mathbb{E}}\mathbb{L}$ در $\mathrm{Gal}_{\mathbb{F}}\mathbb{L}$ نرمال می‌باشد و $\mathrm{Gal}_{\mathbb{F}}\mathbb{L}/\mathrm{Gal}_{\mathbb{E}}\mathbb{L}$ با $\mathrm{Gal}_{\mathbb{F}}\mathbb{E}$ یکریخت است. پس $\mathrm{Gal}_{\mathbb{F}}\mathbb{E}$ تصویر همریختی گروه حلپذیر $\mathrm{Gal}_{\mathbb{F}}\mathbb{L}$ است (قضیه ۲۸.۷ را ملاحظه کنید) و بنابراین طبق قضیه ۱۵.۱۱ حلپذیر می‌باشد. ■

تمرینها

توجه: $\mathbb{F}$ یک میدان را نشان می‌دهد و تمام میدان‌ها مشخصهٔ صفر دارند.

۱.A. یک توسیع رادیکال $\mathbb{Q}$ که شامل عدد مفروض باشد را پیدا کنید:

(الف) $\sqrt[۴]{۱+\sqrt{۷}}-\sqrt[۵]{۲+\sqrt{۵}}$

(ب) $(\sqrt[۵]{\sqrt{۲}+i})/(\sqrt[۳]{۵})$

(پ) $(\sqrt[۳]{۳-\sqrt{۲}})/(۴+\sqrt{۲})$

۲. نشان دهید که $x^۳-۲x-۲\in\mathbb{Q}[x]$ و $x^۳-۳$ دارای گروه گالوای یکسان می‌باشند. [راهنمایی: میدان شکافنده هر کدام چیست؟]

۳. اگر $\mathbb{K}$ یک توسیع رادیکال $\mathbb{F}$ باشد، ثابت کنید که $[\mathbb{K}:\mathbb{F}]$ متناهی است [راهنمایی: قضایای ۹.۷ و ۹.۴.]

۴. نشان دهید که $D_۴$ یک گروه حلپذیر است.

۵. نشان دهید که $S_۴$ گروهی حلپذیر است. [راهنمایی: زیرگروه $H=\{(۱۲)(۳۴),(۱۳)(۲۴),(۱۴)(۲۳),(۱)\}$ از $A_۴$ را در نظر بگیرید.]

۶. اگر G یک گروه ساده غیرآبلی باشد، ثابت کنید که G حلپذیر نیست. نتیجه بگیرید که برای $n\geq ۵$، A_n حلپذیر نیست (قضیه ۲۸.۱۰ را ملاحظه فرمایید).

۷. تمام n–امین ریشه‌های واحد در $\mathbb{C}$ را بنویسید وقتی n برابر است با:

(الف) ۲ (ب) ۳ (پ) ۴ (ت) ۵ (ث) ۶

۸.B. گیریم G زیرگروهی از $S_۵$ باشد که یک دور دوتایی $\sigma=(rs)$ و یک ۵–دور α را شامل باشد. با اثبات مراحل زیر نشان دهید که $G=S_۵$.

(الف) نشان دهید که برای برخی k، α^k به صورت $(rsxyz)$ است. گیریم $\tau=\alpha^k\in G$؛ با نمایه‌گذاری مجدد می‌توانیم فرض کنیم که $\sigma=(۱۲)$ و $\tau=(۱۲۳۴۵)$.

(ب) ثابت کنید که (۱۲)، (۲۳)، (۳۴) و (۴۵) در G هستند. [راهنمایی: برای $k \geq ۱$، $\tau^k \sigma \tau^{-k}$ را در نظر بگیرید.].

(پ) ثابت کنید که $(۱۵), (۱۴), (۱۳) \in G$. [راهنمایی: ?= (۱۲)(۲۳)(۱۲)].

(ت) ثابت کنید که هر دور دوتایی در G قرار دارد. بنابراین طبق نتیجه ۴۴.۷، $G = S_۵$.

۹. گیریم G یک گروه از مرتبه n باشد. اگر $۵|n$، با اثبات مراحل زیر نشان دهید که G یک عنصر از مرتبه ۵ دارد. گیریم S مجموعه تمام ۵–تایی‌های (r, s, t, u, v) باشد، با شرط $r, s, t, u, v \in G$ و $rstuv = e$.

(الف) نشان دهید که S دقیقاً $n^۴$، ۵–تایی را شامل است. [راهنمایی: اگر $r, s, t, u \in G$ و $v = (rstu)^{-۱}$، آنگاه $(r, s, t, u, v) \in S$.]

(ب) دو ۵–تایی در S هم‌ارز نامیده می‌شوند اگر یکی از آن دو یک جایگشت دوری از دیگری باشد.[۱۶] ثابت کنید که این رابطه یک رابطه هم‌ارزی روی S است.

(پ) ثابت کنید که یک کلاس هم‌ارزی در S یا دقیقاً پنج ۵–تایی دارد و یا تنها یک ۵–تایی به صورت (r, r, r, r, r) را شامل است.

(ت) ثابت کنید که حداقل دو کلاس هم‌ارزی در S وجود دارد که شامل تنها یک ۵–تایی است. [راهنمایی: $\{(e, e, e, e, e)\}$ یکی از دو کلاس است. اگر این تنها کلاس باشد، نشان دهید که (پیمانه ۵) $n^۴ \equiv ۱$. اما $۵ \mid n$، بنابراین (پیمانه ۵) $n^۴ \equiv ۰$، که یک تناقض است.]

(ث) اگر $\{(c, c, c, c, c)\}$ با شرط $c \neq e$، یک کلاس هم‌ارزی تک ـعضوی باشد، ثابت کنید که c دارای مرتبه ۵ می‌باشد.

۱۰. اگر N یک زیرگروه نرمال G، و N و G/N حلپذیر باشند، ثابت کنید که G حلپذیر است.

۱۱. ثابت کنید که یک زیرگروه H از یک گروه حلپذیر G، حلپذیر است. [راهنمایی: اگر $G = G_۰ \supseteq G_۱ \supseteq \cdots \supseteq G_n = \langle e \rangle$ سری حلپذیر برای G باشد، گروههای $H_i = H \cap G_i$ را در نظر بگیرید. برای اثبات این که $H_{i-۱}/H_i$ آبلی است، بررسی کنید که نگاشت $H_{i-۱}/H_i \to G_{i-۱}/G_i$ که با ضابطه $H_i x \longmapsto G_i x$ تعریف می‌شود یک همریختی خوش‌تعریف یک به یک است.]

۱۶) برای مثال (r, s, t, u, v) با هر یک از (s, t, u, v, r)، (t, u, v, r, s)، (u, v, r, s, t) و (v, r, s, t, u) هم‌ارز است و با هیچ ۵–تایی دیگر در S هم‌ارز نیست.

۱۲. ثابت کنید که گروه گالوای یک چندجمله‌ای درجه دوم تحویل‌ناپذیر با $\mathbb{Z}_2$ یکریخت است.

۱۳. ثابت کنید که گروه گالوای یک چندجمله‌ای درجه سوم تحویل‌ناپذیر با $\mathbb{Z}_3$ یا S_3 یکریخت است.

۱۴. ثابت کنید که گروه گالوای یک چندجمله‌ای درجه چهارم تحویل‌ناپذیر حلپذیر است. [راهنمایی: نتیجه ۵.۱۱ تمرین‌های ۵ و ۱۱.]

۱۵. گیریم $p(x)$، $q(x)$ چندجمله‌ایهای درجه دوم تحویل‌ناپذیر باشند. ثابت کنید که گروه گالوای $f(x) = p(x)q(x)$ یکریخت با $\mathbb{Z}_2 \times \mathbb{Z}_2$ یا $\mathbb{Z}_4$ می‌باشد. [راهنمایی: اگر u یک ریشه $p(x)$ و v یک ریشه $q(x)$ باشد، آنگاه دو حالت پیش می‌آید: $v \in \mathbb{F}(u)$ و $v \notin \mathbb{F}(u)$.]

۱۶. با استفاده از معیار گالوا ثابت کنید که هر چندجمله‌ای از درجه ≥ 4 حلپذیر با رادیکالها است. [راهنمایی تمرینهای ۱۲ـ۱۵.]

۱۷. گروه گالوای G (تا حد یکریختی) چندجمله‌ای‌های مفروض زیر در $\mathbb{Q}[x]$ را پیدا کنید:

(الف) $x^6 - 4x^3 + 4$، [راهنمایی: تجزیه کنید.]

(ب) $x^4 - 5x^2 + 6$

(پ) $x^5 + 6x^3 + 9x$

(ت) $x^4 + 3x^3 - 2x - 6$

(ث) $x^5 - 10x - 5$ [مثال ۱۷.۱۱ را ملاحظه بفرمایید.]

۱۸. تعیین کنید که آیا معادله داده شده روی $\mathbb{Q}$ حلپذیر با رادیکال‌ها است یا نه:

(الف) $x^6 + 2x^3 + 1 = 0$ (ب) $3x^5 - 15x + 5 = 0$

(پ) $2x^5 - 5x^4 + 5 = 0$ (ت) $x^5 - x^4 - 16x + 16 = 0$

۱۹. (الف) با نشان دادن این که $\mathbb{Q}(\sqrt{2}i)$ میدان شکافنده $x^2 + 2$ می‌باشد ثابت کنید که $\mathbb{Q}(\sqrt{2}i)$ روی $\mathbb{Q}$ نرمال است.

(ب) با نشان دادن این که $\mathbb{Q}(\sqrt[4]{2}(1-i))$ میدان شکافنده $x^2 + 2\sqrt{2}i$ می‌باشد ثابت کنید $\mathbb{Q}(\sqrt[4]{2}(1-i))$ روی $\mathbb{Q}(\sqrt{2}i)$ نرمال است.

(پ) نشان دهید که $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}i) \subseteq \mathbb{Q}(\sqrt[4]{2}(1-i))$ یک توسیع رادیکال $\mathbb{Q}$ است با

$[\mathbb{Q}(\sqrt[4]{2}(1-i):\mathbb{Q})=4$ و توجه داشته باشید که $\mathbb{Q}$ تمامی ریشه‌های دوم واحد (یعنی ± 1) را شامل است.

(ت) گیریم $\mathbb{L}=\mathbb{Q}(\sqrt[4]{2}(1-i))$. نشان دهید که $v=\sqrt[4]{2}(1+i)$ در L نیست. [راهنمایی اگر $v\in\mathbb{L}$ و $u=\sqrt[4]{2}(1-i)\in\mathbb{L}$، ثابت کنید که $v/u=i$ و $(v-u)/2i=\sqrt{2}\in\mathbb{L}$، که ایجاب می‌کند $[L:\mathbb{Q}]\geq[\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}]$، که متناقض با (پ) و تمرین ۱۱ (ب) بخش ۲.۱۱ می‌باشد.]

(ث) ثابت کنید که $\mathbb{L}=\mathbb{Q}(\sqrt[4]{2}(1-i))$ روی $\mathbb{Q}$ نرمال نیست [راهنمایی: u و v (همان‌طور که در (ت) آمده است) ریشه‌های چندجمله‌ای تحویل‌ناپذیر x^4+8 می‌باشند.]

۲۰. گیریم ζ یک ۵–امین ریشه اولیه واحد باشد. تمرین ۲۰ بخش ۵.۴ را فرض کنید و ثابت کنید $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta)$، گروه گالوای x^5-1، دوری از مرتبه ۴ است.

۲۱. گروه گالوای x^5+32 روی $\mathbb{Q}$ چیست؟ [راهنمایی: نشان دهید که $\mathbb{Q}(\zeta)$ یک میدان شکافنده است، که در آن ζ یک ۵–امین ریشه اولیه واحد است. تمرین ۲۰ را ملاحظه کنید.]

۲۲. ثابت کنید که گروه گالوای $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ در قضیه ۱۸.۱۱ دوری است. [راهنمایی: یک نگاشت f از $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ به گروه جمعی $\mathbb{Z}_n$ با ضابطه $f(\sigma)=k$ تعریف کنید، جایی‌که $\sigma(u)=\zeta^k u$. ثابت کنید که f یک همریختی خوش‌تعریف یک به یک است و از قضیه ۱۱.۷ استفاده کنید.]

۲۳.C. اگر p عددی اول و G زیرگروهی از S_p باشد که شامل یک دور دوتایی و یک p–دور باشد، ثابت کنید که $G=S_p$. [تمرین ۸ حالت $p=5$ می‌باشد.]

۲۴. اگر $f(x)\in\mathbb{Q}[x]$ تحویل‌ناپذیر از درجه اول p باشد و $f(x)$ دقیقاً دو ریشه غیرحقیقی داشته باشد، ثابت کنید که گروه گالوای $f(x)$ برابر S_p است. [مثال ۱۷.۱۱ اساساً حالت $p=5$ می‌باشد].

۲۵. یک چندجمله‌ای درجه ۷ در $\mathbb{Q}[x]$ بسازید که گروه گالوای آن S_7 باشد.

* * * * *

فصل دوازدهم

کلید-عمومی[1]، رمز نویسی

پیشنیاز: بخش ۳.۲.

برای قرون متمادی تجّار، جاسوس‌ها، نظامیان و دیپلمات‌ها از کدها (اسمهای رمز) برای ارسال پیام‌های محرمانه استفاده می‌کرده‌اند. در عصر حاضر، قسمت عظیمی از اسناد حساس دولتی و بانک‌های اطلاعاتی که به صورت کامپیوتری ثبت شده‌اند (که بیشتر آنها توسط ماهواره‌ها یا خطوط تلفن مخابره می‌شوند) نیاز به کدهای موثر و با ایمنی بالا را افزایش داده‌اند.

ساختن کدهای ناگشودنی که برای یکبار از آن استفاده می‌شود کار آسانی می‌باشد. این "رمز کد" را ملاحظه کنید

کلمه واقعی: صبح عصر دوشنبه سه‌شنبه حمله

کلمه کد: خفاش گلست شاه تکمه فیگل

---

۱) Public-Key

اگر پیام "فیگل تکمه خفاش" ارسال شود راهی برای این که دشمن بتواند به طور مطمئن بفهمد که این پیام یعنی "حمله سه‌شنبه صبح"، وجود ندارد مگر این که او یک نسخه از رمز کد را داشته باشد. البته اگر از همان کد دوباره استفاده شود، دشمن ممکن است با تجزیه و تحلیل وقایعی که پس از هر پیام رخ داده است قادر به شکستن آن باشد.

اگرچه رمز کدهای یکبار مصرف ناگشودنی هستند ولی استفاده از آن‌ها در ارسال پیام‌های بسیار طولانی و روزمره دردسرآور و بیفایده می‌باشد. حتی اگر این کدسازی و کدگشایی با کامپیوتر انجام شود، باز هم ضروری است که یک رمز کد جدید (لااقل به اندازه هر پیام) برای مشترکین آن و بخاطر این که تمام نسخه‌های این رمز کدها از اشخاص غیرمسئول در امان بماند، طراحی و تهیه گردد. وقتی که صدها هزار کلمه روزانه باید کدسازی و کدگشایی شود این کار گرانقیمت بوده، عملی نخواهد بود. دستگاه کد ایده‌ال برای اغلب ارتباط‌های رایانه‌ای بین طرف‌های مختلف، دستگاهی خواهد بود که در آن

۱. هر شخص الگوریتم‌های رایانه‌ای مؤثر که قابل استفاده مجدد هستند برای کدسازی و کدگشایی پیام‌ها داشته باشد.

۲. الگوریتم کدگشایی هر شخص را نتوان از الگوریتم کدساز او در مدت زمان معقول بدست آورد.

یک دستگاه کد با این ویژگی‌ها را یک **دستگاه کلید ـ عمومی** نامیده‌اند. اگرچه ممکن است معلوم نباشد که چگونه شرط ۲ می‌تواند برقرار باشد، به سادگی می‌توان فوائد یک دستگاه کلید ـ عمومی را ملاحظه کرد.

الگوریتم کدسازی مشترکین را می‌توان به طور عمومی اعلام کرد، شاید (مثل یک دفتر راهنمای تلفن) در یک کتاب منتشر شود. بدین ترتیب احتیاج به پیک و مسائل ایمنی مربوط به توزیع رمز کدها برطرف می‌شود. این امر به علت شرط ۲، سری بودن را به مخاطره نمی‌اندازد: دانستن الگوریتم کدساز یک شخص شما را به تشخیص آلگوریتم کدگشای او قادر نخواهد کرد. بنابراین راهی برای کدگشایی پیام‌هایی که برای آن شخص با کدهای مربوط به خودش ارسال می‌شود وجود ندارد، حتی اگر قادر به ارسال پیام‌های کدشده برای آن شخص باشید.

چون الگوریتم‌های کدساز برای یک دستگاه کلید ـ عمومی در دسترس همه هست، امکان جعل اسناد به نظر محتمل می‌آید. برای مثال، فرض کنید که بانک پیامی کد شده را که ظاهراً از طرف رضا فرستاده شده‌است دریافت می‌کند مبنی بر درخواست انتقال پول از حسابجاری او به حساب سعید. بانک چگونه می‌تواند مطمئن شود که این پیام در واقع توسط رضا ارسال شده است؟

جواب آنقدر ساده است که نیاز به توضیح ندارد. کدسازی و کدگشایی عکس یکدیگرند: در واقع بکارگیری یکی بعد از دیگری (باهر ترتیب دلخواه) همان کلمه‌ای را ایجاد می‌کند که با آن شروع کرده‌اید. بنابراین رضا ابتدا الگوریتم سری کدگشای خود را بکار می‌برد تا نامش را بنویسد؛ مثلاً نامش Gybx می‌شود. آنگاه الگوریتم کدساز عمومی بانک را برای Gybx بکار می‌برد و نتیجه را (امضایش را) همراه با پیامش می‌فرستد. بانک الگوریتم کدگشای خودش را روی این "امضاء" بکار می‌برد و Gybx را بدست می‌آورد. بعد بانک الگوریتم کدساز عمومی رضا را به Gybx بکار می‌برد، که تبدیل به رضا می‌شود. بانک در این صورت می‌تواند مطمئن باشد که این پیام از رضا است، زیرا هیچکس دیگری بجز رضا نمی‌تواند الگوریتم کدگشای او را بکار برد تا واژه Gybx که به عنوان رضا کدسازی شده است را ایجاد کند.

یک دستگاه کلید ـ عمومی در سال ۱۹۷۷ توسط ریوست، شامیر و اَدلمَن[۲] به ظهور پیوست. دستگاه آنها که اکنون دستگاه RSA نامیده می‌شود روی نظریه اعداد مقدماتی پایه‌گذاری شده است. ایمنی این دستگاه مربوط به دشواری تجزیه اعداد بزرگ (همانگونه که در بخش ۴.۱ گفتیم) می‌باشد. در اینجا پیشنیازهای لازم ریاضی برای فهم دستگاه RSA آمده است:

لم ۱.۱۲. گیریم $c \in \mathbb{Z}$، s، r، p و p اول باشد. اگر $p \nmid c$ و $rc \equiv sc \ (p$ پیمانه$)$، آنگاه $r \equiv s \ (p$ پیمانه$)$.

برهان. چون $rc = sc \ (p$ پیمانه$)$، پس $rc - sc = (r-s)c$ را می‌شمارد. طبق قضیه ۸.۱، $p|(r-s)$ یا $p|c$، چون $p \nmid c$، خواهیم داشت $p|r-s$ و بدین دلیل $r \equiv s \ (p$ پیمانه$)$. ■

لم ۲.۱۲. (**قضیه کوچک فرما**)[۳] اگر p اول باشد، $a \in \mathbb{Z}$ و $p \nmid a$، آنگاه $a^{p-1} \equiv 1 \ (p$ پیمانه$)$.

برهان. طبق تمرین ۱، هیچکدام از اعداد a، $2a$، ...، $(p-1)a$ در پیمانه p با صفر همنهشت نیستند. در نتیجه طبق نتیجه ۵.۲ و قضیه ۳.۲ هرکدام از آنها با یکی از اعداد ۱، ۲، ...، $(p-1)$ باید همنهشت باشد. اگر دوتای از آنها با یک عدد همنهشت باشد، مثلاً $ra \equiv i \equiv sa \ (p$ پیمانه$)$ جایی که

$$1 \leq i, r, s \leq p-1,$$

۲) R. Rivest, A. Shamir, L. Adleman

۳) FERMAT'S LITTLE THEOREM

آنگاه طبق لم ۱.۱۲ (با شرط $c = a$) خواهیم داشت (پیمانه p) $r \equiv s$. این امر غیرممکن است زیرا هیچ دو عدداز اعداد ۱، ۲، ...، $p-1$ با یکدیگر در پیمانه p همنهشت نیستند (تفاضل هر دوتای آنها کمتر از p است و از اینرو بر p بخش‌پذیر نیست). پس اعداد a، $2a$، ...، $(p-1)a$ با اعداد ۱، ۲، ...، $p-1$ همنهشت هستند (پس از احتمالاً یک تغییر ترتیب عناصر). با استفاده مکرر از قضیه ۲.۲، خواهیم داشت،

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \quad (\text{پیمانه } p).$$

بازآرایی طرف چپ نشان می‌دهد که

$$a \cdot a \cdots a \times 1 \times 2 \times 3 \times \cdots \times (p-1) \equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \quad (\text{پیمانه } p)$$

$$a^p(1 \times 2 \times 3 \times \cdots \times (p-1)) \equiv 1(1 \times 2 \times 3 \times \cdots \times (p-1)) \quad (\text{پیمانه } p)$$

حال $p \nmid ((1 \times 2 \times 3 \times \cdots \times (p-1))$ (اگر چنین بود، باید طبق نتیجه ۹.۱ یکی از عامل‌ها را بشمارد). بنابراین طبق لم ۱.۱۲ (باشرط $c = 1 \times 2 \times 3 \times \cdots \times (p-1)$) داریم $a^{p-1} \equiv 1$ (پیمانه p). ■

درکلیه مطالب باقیمانده این مبحث p و q اعداد اول متمایز مثبت می‌باشند. گیریم $n = pq$ و $k = (p-1)(q-1)$. عدد d را طوری انتخاب کنید که $(d,k) = 1$. در این صورت طبق نتیجه ۹.۲، معادله $dx = 1$ در $\mathbb{Z}_k$ دارای یک جواب است. بنابراین معادله $dx \equiv 1$ (پیمانه k) در $\mathbb{Z}$ یک جواب دارد، آن را e بنامید.

قضیه ۳.۱۲. گیریم p، q، n، k، e، d مثل بالا باشند. آنگاه برای هر $b \in \mathbb{Z}$، $b^{ed} \equiv b$ (پیمانه n).

برهان[۴]. چون e یک جواب $dx \equiv 1$ (پیمانه k) می‌باشد برای برخی t، $de - 1 = kt$. بدین ترتیب $ed = kt + 1$ و لذا

$$b^{ed} = b^{kt+1} = b^{kt}b^1 = b^{(p-1)(q-1)t}b = (b^{p-1})^{(q-1)t}b.$$

اگر $p \nmid b$، آنگاه طبق لم ۲.۱۲،

$$b^{ed} = (b^{p-1})^{(q-1)t}b \equiv (1)^{(q-1)t}b \equiv b \quad (\text{پیمانه } p).$$

۴) خطوط کلی برهان کوتاه دیگری با استفاده از نظریه گروهها، در تمرین ۱۵ بخش ۸.۷ آمده‌است.

اگر $p|b$ آنگاه b و هر یک از توان‌های آن در پیمانه p با صفر همنهشت هستند. بنابراین در هر حالت (پیمانه p) $b^{ed} \equiv b$. استدلالی مشابه نشان می‌دهد که (پیمانه q) $b^{ed} \equiv b$. طبق تعریف همنهشتی،

$$p|(b^{ed}-b) \quad \text{و} \quad q|(b^{ed}-b).$$

بنابراین طبق تمرین ۲، $pq|(b^{ed}-b)$. چون $pq = n$، این بدان معنی است که $n|(b^{ed-b})$، و بدین دلیل (پیمانه n) $b^{ed} \equiv b$. ■

کوچکترین باقیمانده به پیمانه n برای عدد صحیح c باقیمانده r است که از تقسیم c بر n بدست می‌آید. طبق الگوریتم تقسیم، $c = nq + r$، و لذا $c - r = nq$. بنابراین (پیمانه n) $c \equiv r$. چون دو عدد که اکیداً بین ۰ و n باشند نمی‌توانند به پیمانهٔ n همنهشت باشند، کوچکترین باقیمانده r تنها عدد صحیح بین ۰ و n است که همنهشت با c به پیمانه n است.

اکنون می‌توانیم کارکرد دستگاه RSA را، پس از آن که نشان دادیم که چگونه در شرایط دستگاه کلید عمومی صدق می‌کند، توصیف کنیم. پیامی که باید ارسال شود، با جایگذاری هر حرف یا جای خالی با یک عدد دو رقمی، ابتدا به صورت عددی تبدیل می‌شود[۵]:

$$\text{جای خالی} = ۰۰, \quad A = ۰۱, \quad B = ۰۲, \ldots, Y = ۲۵, \quad Z = ۲۶.$$

برای مثال واژه GO به صورت ۰۷۱۵ و WEST به صورت ۲۳۰۵۱۹۲۰ در می‌آید، بنابراین که پیام "GO WEST" عدد ۰۷۱۵۰۰۲۳۰۵۱۹۲۰ می‌شود، که آن را با B نشان خواهیم داد.

گیریم p، q، n، k، d، e همانهایی باشند که در قضیه ۳.۱۲ آمد، با این شرط که p و q طوری انتخاب شده‌اند که $B < pq = n$. برای کد گذاری پیام B، کوچکترین باقیمانده B^e به پیمانه n را محاسبه کرده، آن را با C نشان دهید. آنگاه C شکل کُد شدهٔ B است. C را بهر طریق مناسب ارسال کنید.

کسی که C را دریافت می‌کند آن را با محاسبه کوچکترین باقیمانده C^d به پیمانه n کدگشایی می‌نماید. این کار بدلایل زیر پیام اصلی را تولید می‌کند. چون B^e با کوچکترین باقیمانده‌اش C در پیمانه n همنهشت است، قضیه ۳.۱۲ نشان می‌دهد که

$$C^d \equiv (B^e)^d = B^{ed} \equiv B \quad (\text{پیمانه } n)$$

۵) اعداد بیشتری را می‌توان برای علائم نقطه‌گذاری، اعداد، نمادهای خاص و غیره بکار برد. ولی همین اعداد ارائه شده در اینجا برای نشان دادن مفاهیم اساسی کافی می‌باشد.

کوچکترین باقیمانده C^d تنها عددی است بین ۰ و n که همنهشت با C^d به پیمانه n می‌باشد و $0 < B < n$. بنابراین پیام اصلی B کوچکترین باقیمانده C^d است.

قبل از ارائه یک مثال عددی، ثابت می‌کنیم دستگاه RSA در شرایط یک دستگاه کلید ـ عمومی صدق می‌کند:

۱. وقتی که دستگاه RSA عملاً مورد استفاده واقع می‌شود، p و q اعداد اول بزرگ می‌باشند (اعداد ۱۰۰ رقمی). همان‌طورکه در بخش ۱.۴ اشاره شد چنین اعداد اولی را می‌توان با یک رایانه سریعاً مشخص نمود. اگرچه B، e، C و d اعدادی بزرگ می‌باشند، الگوریتم‌های سریعی برای یافتن کوچکترین باقیمانده‌های B^e و C^d به پیمانه n وجود دارد. این الگوریتم‌ها بر مبنای نمایش دوتایی توان‌ها پایه‌گذاری شده‌اند و محاسبه مستقیم B^e یا C^d را (که اعداد فوق‌العاده بزرگی هستند) نیاز ندارند. بنابراین الگوریتم‌های کُد گذاری و کُد گشایی دستگاه RSA از نظر محاسباتی مفیدند.

۲. برای استفاده از دستگاه RSA، هر کاربر شبکه با استفاده از رایانه، اعداد p، q، d مناسب را انتخاب می‌نماید و آنگاه n، k، e را مشخص می‌کند. اعداد e و n برای الگوریتم کُد گذاری برای عموم معرفی می‌گردد، ولی عامل‌های اول p و q از n و اعداد d و k محرمانه نگهداشته می‌شوند. هر کسی با یک رایانه می‌تواند پیامها را با استفاده از e و n کُدگذاری نماید. ولی بدون آنکه ابتدا p و q را از تجزیه n پیدا کنند هیچ راه عملی برای دیگران وجود ندارد تا d را مشخص کنند (و از اینرو الگوریتم کُدگشا وجود ندارد) [۶]. همانگونه که در بخش ۴.۱ تشریح شد این کار با فن‌آوری موجود میلیون‌ها سال طول می‌کشد. بنابراین دستگاه RSA، تا زمانی که روش‌های جدید و خیلی سریع برای تجزیه توسعه نیافته است بنظر مطمئن می‌رسد.

حتی وقتی n به صورت فوق اختیار شود، بعضی از پیام‌ها ممکن است در شکل عددی بزرگتر از n باشند. در چنین حالت‌هایی پیام اصلی به چند قسمت شکسته می‌شود که هرکدام از آنها کمتر از n است. در اینجا مثالی آمده است که منسوب به ریوست ـ شامیر ـ ادلمان[۷] می‌باشد.

مثال ۱.۱۲. گیریم $p = ۴۷$ و $q = ۵۹$. آنگاه $n = pq = ۴۷ \times ۵۹ = ۲۷۷۳$

۶) به جای آن، یک فرد ممکن است تلاش کند تا k را پیدا نماید و آنگاه همنهشتی (پیمانه k) $ex \equiv ۱$ را حل کند تا d را بدست آورد. ولی می‌توان نشان داد که این کار از نظر محاسباتی هم‌ارز با تجزیه n است، بنابراین به هیچ وجه در زمان صرفه‌جویی نمی‌شود.

۷) Rivest-Shamir-Adleman

و $k = (p-1)(q-1) = ۴۶ \times ۵۸ = ۲۶۶۸$ [۸]. گیریم $d = ۱۵۷$ که به راحتی ثابت می‌شود که نسبت به ۲۶۶۸ اول است. تساوی $e = ۱۷$ از حل همنهشتی (پیمانه ۲۶۶۸) $۱۵۷x \equiv ۱$ به دست می‌آید (تمرین ۱۵ بخش ۱.۱۳ را ملاحظه کنید). می‌خواهیم پیام "IT'S All GREEK TO ME" را کُدگذاری کنیم. ما می‌توانیم فقط اعداد کمتر از $n = ۲۷۷۳$ را کدگذاری کنیم. بنابراین پیام را در بلوک‌های دو-حرفی می‌نویسیم (و جاهای خالی را با # نشان می‌دهیم):

I T	S#	A L	L#	G R
0920	1900	0112	1200	0718
E E	K #	T O	# M	E #
0505	1100	2015	0013	0500

در این صورت هر بلوک عددی کمتر از ۲۷۷۳ است. بلوک اول، 0920، با استفاده از $e = ۱۷$ و یک رایانه که کوچکترین باقیمانده $۹۲۰^{۱۷}$ به پیمانه ۲۷۷۳ را محاسبه می‌کند کدگذاری می‌شود:

$$۹۲۰^{۱۷} \equiv ۹۴۸ \quad (\text{پیمانه } ۲۷۷۳) \ .$$

بلوک‌های دیگر نیز به طور مشابه کدگذاری می‌شوند، بنابراین صورت کدشده پیام چنین است:

۰۹۴۸ ۲۳۴۲ ۱۰۸۴ ۱۴۴۴ ۲۶۶۳

۲۳۹۰ ۰۷۷۸ ۰۷۷۴ ۰۲۱۹ ۱۶۵۵

شخصی که این پیام را دریافت می‌کند از $d = ۱۵۷$ استفاده می‌کند تا هر بلوک را کدگشایی کند. برای مثال برای کدگشایی ۰۹۴۸، رایانه چنین محاسبه می‌کند:

$$۹۴۸^{۱۵۷} \equiv ۹۲۰ \quad (\text{پیمانه } ۲۷۷۳)$$

این همان اولین بلوک پیام است: $IT = ۰۹۲۰$.

برای اطلاع بیشتر درباره رمزنویسی و دستگاه RSA به De-Millo-Davida [۳۶]، Diffie-Hellman [۳۷]، Rivest-Shamir-Adleman [۳۸]، و Simmons [۳۹] رجوع کنید.

---

۸) این اعداد جهت ارائه مفاهیم انتخاب شده‌اند، ولی برای ارائه یک کُد مطمئن خیلی کوچکند زیرا ۲۷۷۳ به صورت دستی قابل تجزیه است.

تمرینها

A.۱. گیریم p عددی اول باشد و $k, a \in \mathbb{Z}$ طوری باشند که $p \nmid a$ و $0 < k < p$. ثابت کنید $ka \not\equiv 0 \pmod{p}$. [راهنمایی: قضیه ۸.۱.]

۲. اگر p و q اعداد اول متمایزی باشند که $q|c$ و $p|c$، ثابت کنید $pq|c$ [راهنمایی: اگر $c = pk$، آنگاه $q|pk$، قضیه ۸.۱ را بکار برید.]

۳. از یک ماشین‌حساب استفاده کنید و الگوریتم کدگذار RSA را با شرط $c = ۳$، $n = ۲۷۷۳$ بکار برید تا این پیام‌ها را کدگذاری نمایید.

(الف) GO HOME (ب) COME BACK (پ) DROP DEAD

[راهنمایی: از بلوک‌های دو حروفی استفاده کنید و جاهای خالی را حذف نکنید.]

۴. این شکل از قضیه کوچک فرما را ثابت کنید: اگر p عددی اول باشد و $a \in \mathbb{Z}$، آنگاه $a^p \equiv a \pmod{p}$. [راهنمایی: دو حالت $p|a$ و $p \nmid a$ را لحاظ کنید، در حالت دوم لم ۲.۱۲ را بکار برید.]

B.۵. الگوریتم کد گشایی را برای کد تمرین ۳ پیدا کنید.

۶. گیریم C صورت کد شده یک پیام باشد که با استفاده از الگوریتم RSA کد گذاری شده است. فرض کنید که شما کشف کرده‌اید که C و n، پیمانه کدگذاری، نسبت به هم اول نیستند. توضیح دهید که چگونه می‌توانید n را تجزیه کنید و بنابراین الگوریتم کدگذاری را پیدا کنید. [در صورتی که عوامل اول p و q در تجزیه n دارای بیش از ۱۰۰ رقم باشد، احتمال وقوع یک چنین C کمتر از $۱۰^{-۹۹}$ است.]

* * * * *

فصل سیزدهم

قضیه باقیمانده چینی[1]

پیشنیازها: بخش ۱.۲ و پیوست پ برای بخش ۱.۱۳؛ بخش ۱.۳ برای بخش ۲.۱۳؛ فصل ۶ برای بخش ۳.۱۳.

قضیه باقیمانده چینی (بخش ۱.۱۳) یک دستاورد مشهور در نظریه اعداد است، که برای ریاضیدانان چینی در قرن اول میلادی شناخته شده بود. این قضیه همچنین کاربردهای عملی در حساب رایانه (بخش ۲.۱۳) دارد. تعمیمی از این قضیه به حلقه‌های غیر از $\mathbb{Z}$، نتایج جالب توجهی در نظریه حلقه‌ها دارد (بخش ۳.۱۳). اگرچه به‌وضوح بخش ۳.۱۳ از بخش ۱.۱۳ نشأت گرفته‌است، این بخش از بقیه فصل مستقل است و می‌توان آن را تا پس از مطالعه فصل ۶ به تعویق انداخت.

---

۱) The Chinese Remainder Theorem

۱-۱۳ برهان قضیه باقیماندهٔ چینی

یک همنهشتی معادله‌ای است با ضرایب صحیح که در آن "=" با "(پیمانه n)$\equiv$ " جایگزین می‌شود. یک معادله می‌تواند موجب همنهشتی‌های متفاوت باشد، مانند

$$۶x + ۵ \equiv ۷ \text{ (پیمانه ۵)} \qquad \text{یا} \qquad ۶x + ۵ \equiv ۷ \text{ (پیمانه ۳)}.$$

فقط اعداد صحیح به عنوان جواب همنهشتی‌ها معنی دارند، بنابراین فنون حل معادلات همیشه برای همنهشتی‌ها قابل استفاده نمی‌باشد. برای مثال معادله $۶x + ۵ = ۷$ دارای جواب $x = \frac{۱}{۳}$ است، ولی (پیمانه ۳) $۶x + ۵ \equiv ۷$ هیچ جوابی ندارد(تمرین ۳)، و همنهشتی (پیمانه ۵) $۶x + ۵ \equiv ۷$ دارای بی‌نهایت جواب است (تمرین ۴).

تعدادی از مسئله‌های نظری و کاربردهای عملی، محتاج به حل دستگاهی از همنهشتی‌ها، مثل

$$x \equiv ۲ \quad \text{(پیمانه ۴)}$$
$$x \equiv ۵ \quad \text{(پیمانه ۷)}$$
$$x \equiv ۰ \quad \text{(پیمانه ۱۱)}$$
$$x \equiv ۸ \quad \text{(پیمانه ۱۵)}$$

می‌باشد. **یک جواب این دستگاه**، طبق تعریف عددی صحیح است که جواب هر همنهشتی در این دستگاه باشد. در ادامه چند حالت را که یک دستگاه همنهشتی‌های خطی حتماً باید دارای جواب داشته باشد را بررسی خواهیم کرد.

لم ۱.۱۳. اگر m و n اعداد صحیح مثبت نسبت بهم اول باشند و $a, b \in \mathbb{Z}$، آنگاه دستگاه

$$x \equiv a \quad \text{(پیمانه } m\text{)}$$
$$x \equiv b \quad \text{(پیمانه } n\text{)}$$

دارای یک جواب است.

برهان. چون $(m, n) = ۱$، (طبق قضیه ۳.۱) اعداد صحیح u و v وجود دارند به طوری که $mu + nv = ۱$. اگر دو طرف این معادله را در $b - a$ ضرب کنیم، داریم

$$mu(b-a) + nv(b-a) = b - a$$
$$a + mu(b-a) = b - nv(b-a). \qquad (*)$$

گیریم $t = a + mu(b-a)$. آنگاه t یک جواب همنهشتی اوّل این دستگاه است زیرا

$$t - a = (a + mu(b-a)) - a = mu(b-a) = m(ub - ua).$$

و بنابراین، طبق تعریف همنهشتی، (پیمانه m) $t \equiv a$. با استفاده از معادله $(*)$، می‌بینیم که

$$\begin{aligned} t - b &= (a + mu(b-a)) - b = (b - nv(b-a)) - b \\ &= n(va - vb). \end{aligned}$$

بنابراین (پیمانهn) $t \equiv b$، و t یک جواب این دستگاه است. ■

اثبات لم ۱.۱۳ الگوریتمی برای یافتن جواب صریح دستگاه‌هایی که دو همنهشتی دارند ارائه می‌کند:

۱. u و v ای پیدا کنید که $mu + nv = ۱$.[۲]

۲. آنگاه $x = a + mu(b-a)$ یک جواب دستگاه است.

مثال ۱.۱۳. برای حل دستگاه

$$\begin{aligned} x &\equiv ۲ \quad (\text{پیمانه } ۴) \\ x &\equiv ۵ \quad (\text{پیمانه } ۷) \end{aligned}$$

الگوریتم را با شرط $m = ۴$، $n = ۷$، $a = ۲$، $b = ۵$ بکار می‌بریم:

۱. به سادگی دیده می‌شود $u = ۲$ و $v = -۱$ در $۴u + ۷v = ۱$ صدق می‌کند،

۲. بنابراین یک جواب دستگاه برابر است با

$$x = a + mu(b-a) = ۲ + ۴ \times ۲(۵ - ۲) = ۲ + ۸ \times ۳ = ۲۶.$$

قضیه ۲.۱۳. (قضیه باقیمانده چینی) گیریم $m_۱, m_۲, \ldots, m_r$ اعداد صحیح مثبتی باشند که دوبدو نسبت بهم‌اولند (بدین معنا که برای $i \neq j$ $(m_i, m_j) = ۱$)، آنگاه برای هر $a_i \in \mathbb{Z}$،

۲) این کار همیشه با استفاده از الگوریتم اقلیدسی (قضیه ۶.۱) قابل انجام است، مثال بعد از قضیه ۶.۱ را ملاحظه کنید.

دستگاه

$$\begin{aligned} x &\equiv a_1 \quad (\text{پیمانه } m_1) \\ x &\equiv a_2 \quad (\text{پیمانه } m_2) \\ &\vdots \\ x &\equiv a_r \quad (\text{پیمانه } m_r) \end{aligned}$$

دارای یک جواب است. هر دو جواب این دستگاه در پیمانه $m_1 m_2 \cdots m_r$ همنهشت هستند. اگر t یک جواب دستگاه باشد، آنگاه z یک جواب است اگر و فقط اگر $z \equiv t$ (پیمانه $m_1 m_2 \cdots m_r$).

برهان. وجود یک جواب. برهان با استقراء روی r، تعداد همنهشتی‌های دستگاه‌انجام می‌شود. اگر $r = 2$، آنگاه طبق لم ۱.۱۳ یک جواب وجود دارد (با شرط $m = m_1$ و $n = m_2$ ، $a = a_1$ و $b = a_2$). به استقراء فرض کنید که برای $r = k$ یک جواب موجود باشد و دستگاه

$$\begin{aligned} x &\equiv a_1 \quad (\text{پیمانه } m_1) \\ x &\equiv a_2 \quad (\text{پیمانه } m_2) \\ &\vdots \\ x &\equiv a_k \quad (\text{پیمانه } m_k) \\ x &\equiv a_{k+1} \quad (\text{پیمانه } m_{k+1}) \end{aligned} \qquad (**)$$

را در نظر بگیرید. طبق فرض استقراء، دستگاه شامل اولین k معادله همنهشتی در (**) دارای یک جواب s است. به‌علاوه $m_1 m_2 \cdots m_k$ و m_{k+1} نسبت به هم اولند (تمرین ۵). در نتیجه، طبق لم ۱.۱۳، دستگاه

$$\begin{aligned} x &\equiv s \quad (\text{پیمانه } m_1 m_2 \cdots m_k) \\ x &\equiv a_{k+1} \quad (\text{پیمانه } m_{k+1}) \end{aligned} \qquad (***)$$

دارای یک جواب t است. این عدد t الزاماً در شرط

$$t \equiv s \quad (\text{پیمانه } m_1 m_2 \cdots m_k)$$

صدق می‌کند. در نتیجه، برای هر $i = ۱, ۲, \ldots, k$،

$$s \equiv a_i (\text{پیمانه } m_i) \quad \text{و} \quad t \equiv s (\text{پیمانه } m_i).$$

طبق شرط تعدّی (قضیه ۱.۲)،

$$t \equiv a_i \ (\text{پیمانه } m_i) \quad \text{برای } i = ۱, ۲, \ldots, k.$$

چون t یک جواب $(***)$ است باید در همنهشتی $t \equiv a_{k+۱} \ (\text{پیمانه } m_{k+۱})$ نیز صدق کند. پس t یک جواب دستگاه $(**)$ است و لذا برای $r = k + ۱$ یک جواب وجود دارد. بنابراین، طبق استقراء هر دستگاه از این نوع یک جواب دارد.

مجموعه کامل جواب‌ها. اگر z جوابی دیگر از این دستگاه باشد، آنگاه برای هر $i = ۱, ۲, \ldots, k$،

$$t \equiv a_i \ (\text{پیمانه } m_i) \quad \text{و} \quad z = a_i \ (\text{پیمانه } m_i).$$

طبق شرط تعدی (قضیه ۱.۲)، $z \equiv t \ (\text{پیمانه } m_i)$. پس

$$m_۱ | z - t, m_۲ | z - t, \ldots, m_r | z - t.$$

بنابراین طبق تمرین ۷، $m_۱ m_۲ \cdots m_r | z - t$. بدین دلیل $z \equiv t \ (\text{پیمانه } m_۱ m_۲ \cdots m_r)$.

بالعکس، اگر $z \equiv t \ (\text{پیمانه } m_۱ m_۲ \cdots m_r)$، آنگاه همانگونه که در بالا آمد، برای هر $i = ۱, ۲, \ldots, r$ $z \equiv t \ (\text{پیمانه } m_i)$. چون $t \equiv a_i \ (\text{پیمانه } m_i)$ شرط تعدی نشان می‌دهد که برای هر i $(\text{پیمانه } m_i)$، $z \equiv a_i$، بنابراین z یک جواب دستگاه است. ■

برهان قضیه ۲.۱۳ در واقع یک الگوریتم مفید برای حل دستگاههای بزرگ ارائه می‌کند. ابتدا دو معادله اول را طبق لم ۱.۱۳ حل کنید، آنگاه گام استقراء را تا آنجا که نیاز است تکرار کنید تا جوابی برای کل دستگاه مشخص شود.

مثال ۲.۱۳. برای حل دستگاه

$$x \equiv ۲ \ (\text{پیمانه } ۴)$$
$$x \equiv ۵ \ (\text{پیمانه } ۷)$$
$$x \equiv ۰ \ (\text{پیمانه } ۱۱)$$
$$x \equiv ۸ \ (\text{پیمانه } ۱۵)$$

با دو همنهشتی اول شروع کنید. مثال قبل نشان می‌دهد که $x = ۲۶$ یک جواب هر دو است. طبق گزاره آخر قضیه ۲.۱۳، هر عدد که همنهشت با ۲۶ به پیمانه $۲۸ = ۷ \times ۴$ باشد نیز یک جواب است، چون (پیمانه ۲۸) $۲۶ \equiv -۲$، -۲ جوابی از دو همنهشتی اول است[۳].

برهان قضیه ۲.۱۳ نشان می‌دهد که جواب‌های سه‌همنهشتی اول درست همان جواب‌های دستگاه زیر می‌باشد:

$$x \equiv -۲ \text{ (پیمانه ۲۸)} \qquad x \equiv -۲ \text{ (پیمانه } ۴ \times ۷\text{)}$$

یا به طور معادل

$$x \equiv ۰ \text{ (پیمانه ۱۱)} \qquad x \equiv ۰ \text{ (پیمانه ۱۱)}.$$

اینک از لم ۱.۱۳ با شرط $m = ۲۸$ و $n = ۱۱$ استفاده می‌کنیم. چنین درمی‌یابیم که $u = ۲$، $v = -۵$ در $۲۸u + ۱۱v = ۱$ صدق می‌کند، بدین دلیل

$$s = a + mu(b - a) = -۲ + ۲۸ \times ۲(۰ - (-۲)) = ۱۱۰$$

یک جواب سه‌همنهشتی اول است.

جواب دستگاه چهار همنهشتی، همان جواب دستگاه زیر می‌باشد:

$$x \equiv ۱۱۰ \text{ (پیمانه ۳۰۸)} \qquad x \equiv ۱۱۰ \text{ (پیمانه } ۴ \times ۷ \times ۱۱\text{)}$$

یا به طور معادل

$$x \equiv ۸ \text{ (پیمانه ۱۵)} \qquad x \equiv ۸ \text{ (پیمانه ۱۵)}.$$

با کمی محاسبه ثابت می‌شود که $۱ = ۱۵(-۴۱) + ۳۰۸(۲)$، پس $u = ۲$ و

$$t = a + mu(b - a) = ۱۱۰ + ۳۰۸ \times ۲(۸ - ۱۱۰) = -۶۲۷۲۲$$

یک جواب دستگاه چهارهمنهشتی می‌باشد. چون $۴۶۲۰ = ۱۵ \times ۱۱ \times ۷ \times ۴$ و $۱۹۵۸ \equiv -۶۲۷۲۲$ (پیمانه ۴۶۲۰)، لذا عدد ۱۹۵۸ نیز یک جواب دستگاه چهار همنهشتی است. بنابراین جواب‌های دستگاه همه اعدادی است که با ۱۹۵۸ به پیمانه ۴۶۲۰ همنهشت است.

---

۳) برای ساده‌کردن محاسبات، معمولاً چنین مرسوم است که از جوابهایی که حتی‌الامکان از نظر قدرمطلق کوچکند استفاده شود.

تمرینها

۱.A. اگر (پیمانه n) $u \equiv v$ و u جوابی از (پیمانه n) $۶x + ۵ \equiv ۷$ باشد، ثابت کنید v نیز یک جواب است. [راهنمایی: قضیه ۲.۲.]

۲. اگر (پیمانه n) $۶x+۵ \equiv ۷$ دارای یک جواب باشد، ثابت کنید که یکی از اعداد $۱, ۲, \ldots, n-۱$ نیز یک جواب است [راهنمایی: تمرین ۱ و نتیجه ۵.۲.]

۳. ثابت کنید که (پیمانه ۳) $۶x + ۵ \equiv ۷$ دارای جواب نیست.

۴. ثابت کنید که (پیمانه ۵) $۶x + ۵ \equiv ۷$ دارای بینهایت جواب است. [راهنمایی تمرینهای ۱ و ۲.]

۵. اگر $m_۱$، $m_۲$، ...، m_k، $m_{k+۱}$ اعداد صحیح مثبتی باشند که دوبدو نسبت به هم اول هستند (یعنی برای $i \neq j$، $(m_i, m_j) = ۱$)، ثابت کنید که $m_{k+۱}$ و $m_۱ m_۲ \ldots m_k$ نسبت بهم اولند. [راهنمایی: اگر چنین نباشد، عدد اول p ای هست که هر دوی آنها را می‌شمارد (چرا؟) از نتیجه ۹.۱ استفاده کنید تا به تناقض برسید.]

۶. اگر $(m, n) = ۱$ و $m|d$ و $n|d$، ثابت کنید که $mn|d$. [راهنمایی: اگر $d = mk$ آنگاه $n|mk$ ؛ از قضیه ۵.۱ استفاده کنید.]

۷. گیریم $m_۱$، $m_۲$، ...، m_k اعداد صحیح مثبتی باشند که دوبدو نسبت بهم اول هستند (یعنی برای $i \neq j$، $(m_i, m_j) = ۱$). فرض کنید برای هر i، $m_i|d$. ثابت کنید که $m_۱ m_۲ \cdots m_k|d$. [راهنمایی: تمرینهای ۵ و ۶ را مکرراً استفاده کنید.]

در تمرینهای ۱۳-۸، دستگاه همنهشتی را حل کنید.

۸. (پیمانه ۶) $x \equiv ۵$
(پیمانه ۱۱) $x \equiv ۷$

۹. (پیمانه ۱۱) $x \equiv ۳$
(پیمانه ۷) $x \equiv ۴$

۱۰. (پیمانه ۲) $x \equiv ۱$
(پیمانه ۳) $x \equiv ۲$
(پیمانه ۵) $x \equiv ۳$

۱۱. (پیمانه ۵) $x \equiv ۲$
(پیمانه ۶) $x \equiv ۰$
(پیمانه ۷) $x \equiv ۳$

۱۲. (پیمانه ۵) $x \equiv ۱$
(پیمانه ۶) $x \equiv ۲$
(پیمانه ۱۱) $x \equiv ۵$
(پیمانه ۱۳) $x \equiv ۱۰$

۱۳. (پیمانه ۷) $x \equiv ۱$
(پیمانه ۱۱) $x \equiv ۶$
(پیمانه ۱۲) $x \equiv ۰$
(پیمانه ۱۳) $x \equiv ۹$
(پیمانه ۱۷) $x \equiv ۰$

۱۴.B. (مسئله چین باستان) ۱۷ نفر دزد جعبه‌ای از سکه‌های طلا را می‌ربایند. وقتی سکه‌ها را به‌طور برابر بین یکدیگر تقسیم می‌کنند، سه سکه باقی می‌ماند. این امر باعث زدوخوردی می‌شود که یکی از دزدان کشته می‌شود. وقتی بقیه دزدان می‌کوشند که دوباره این سکه‌ها را بین هم تقسیم کنند ده سکه باقی می‌ماند. برخورد دیگری شروع می‌شود و پنج نفر از دزدان کشته می‌شوند. وقتی افراد زنده سکه‌ها را تقسیم می‌کنند چهار سکه می‌ماند. برخورد دیگری واقع می‌شود که در آن چهار دزد کشته می‌شوند. سپس بازماندگان سکه‌ها را به تساوی بین خود تقسیم می‌کنند و چیزی باقی نمی‌ماند. کمترین تعداد سکهٔ احتمالی داخل جعبه چقدر است؟

۱۵. اگر $(a,n) = d$ و $d|b$، ثابت کنید (پیمانه n) $ax \equiv b$ دارای یک جواب است. [راهنمایی: برای برخی c، $b = dc$ و اعداد v و u وجود دارند که $au + nv = d$ (چرا؟) معادلهٔ آخر را در c ضرب کنید، auc با چه عددی در پیمانه n همنهشت است؟]

۱۶. اگر $(a,n) = d$ و $d \nmid b$، ثابت کنید که (پیمانه n) $ax \equiv b$ دارای جواب نیست.

۱۷. اگر $(a,n) = ۱$ و s و t جواب‌هایی از (پیمانه n) $ax \equiv b$ باشند، ثابت کنید که (پیمانه n) $s \equiv t$. [راهنمایی: ثابت کنید $n|(as - at)$ و از قضیه ۵.۱ استفاده کنید.]

۱۸. اگر $(a,n) = d$ و s و t جواب‌هایی از (پیمانه n) $ax \equiv b$ باشند ثابت کنید که (پیمانه n/d) $s \equiv t$.

۱۹. اگر $(m,n) = d$، ثابت کنید که دستگاه

$$x \equiv a \quad (\text{پیمانه } m)$$
$$x \equiv b \quad (\text{پیمانه } n)$$

دارای جواب است اگر و فقط اگر (پیمانه d) $a \equiv b$.

۲۰. اگر s، t جواب‌هایی از دستگاه تمرین ۱۹ باشند، ثابت کنید (پیمانه r) $s \equiv t$، که در آن r کوچکترین مضرب مشترک m و n است.

۱۳-۲ کاربردهای قضیه باقیمانده چینی

هر رایانه در اندازه اعداد صحیحی که در حساب ماشین مورد استفاده قرار می‌گیرد دارای حدی می‌باشد که آن را **اندازه کلمه** می‌نامند. در یک رایانه بزرگ این اندازه می‌تواند 2^{35} باشد[۴]. حساب رایانه‌ای با اعداد بزرگتر از اندازه کلمه، به روش‌های وقت‌گیری نیازمند است که از دقت مضاعف برخوردار می‌باشد. در چنین وضعیت‌هایی روش جایگزین دیگری از جمع و ضرب که بر قضیه باقیمانده چینی مبتنی است اغلب سریعتر می‌باشد.

برای اعداد دلخواه r، s، t، n که کمتر از اندازه کلمه باشند، رایانه‌ای بزرگ می‌تواند بسرعت

- $r + s$ و $r \cdot s$ را (حتی وقتی جواب بزرگتر از اندازه کلمه باشد) حساب کند؛
- کوچکترین باقیمانده t به پیمانه n [۵] (از جمله حالتی که t از اندازه کلمه بیشتر باشد، به تمرین ۲ نگاه کنید) را حساب کند؛
- جمع و ضرب در $\mathbb{Z}_n$ را انجام دهد.

یک رایانه می‌تواند صورتی از الگوریتم جواب در قضیه باقیمانده چینی (قضیه ۲.۱۳) را، با اندک تغییری، بکار برد تا دستگاه‌های همنهشتی را حل نماید. ولی این فرآیند ممکن است شامل اعداد بزرگتر از اندازه کلمه باشد و بنابراین به شگردهای با دقت مضاعفی که بالطبع کندتر هستند نیاز است.

برای این‌که از چگونگی روش کار جایگزین ایده‌ای بدست آورید، تصور کنید که اندازه کلمهٔ رایانه ما عدد ۱۰۰ باشد، بنابراین روش‌های با دقت مضاعف را باید برای اعداد بزرگتر از ۱۰۰ بکار برد. مثال زیر نشان می‌دهد که در رایانه‌ای از این نوع و با استفاده از روش‌های با دقت مضاعف، چگونه دو عدد چهاررقمی در یکدیگر ضرب می‌شود.

---

۴) مترجم: توجه کنید که کلیه اعداد ارائه شده راجع به قابلیت‌های رایانه‌ها مربوط به سالهای قبل از چاپ کتاب می‌باشد (۱۹۹۰ میلادی).

۵) کوچکترین باقیمانده به پیمانه n برای عدد t باقیمانده r در تقسیم t بر n است. طبق الگوریتم تقسیم $t = nq + r$، بنابراین $t - r = nq$ و $t \equiv r$ (پیمانه n).

مثال ۳.۱۳. عدد ۳۴۵۶ را در عدد ۷۹۸۲ با لحاظ کردن دستگاه‌های همنهشتی گوناگون و استفاده از قضیه باقیمانده چینی ضرب می‌کنیم. اعداد گوناگونی را به عنوان پیمانه انتخاب می‌نماییم و کوچکترین باقیمانده اعداد ۳۴۵۶ و ۷۹۸۲ را برای هر پیمانه پیدا می‌کنیم: [۶]

	(پیمانه ۸۹) $۷۹۸۲ \equiv ۶۱$	(پیمانه ۸۹)	$۳۴۵۶ \equiv ۷۴$
	(پیمانه ۹۵) $۷۹۸۲ \equiv ۲$	(پیمانه ۹۵)	$۳۴۵۶ \equiv ۳۶$
(*)	(پیمانه ۹۷) $۷۹۸۲ \equiv ۲۸$	(پیمانه ۹۷)	$۳۴۵۶ \equiv ۶۱$
	(پیمانه ۹۸) $۷۹۸۲ \equiv ۴۴$	(پیمانه ۹۸)	$۳۴۵۶ \equiv ۲۶$
	(پیمانه ۹۹). $۷۹۸۲ \equiv ۶۲$	(پیمانه ۹۹)	$۳۴۵۶ \equiv ۹۰$

آنگاه طبق قضیه ۲.۲، می‌دانیم که (پیمانه ۸۹) $۳۴۵۶ \times ۷۹۸۲ \equiv ۷۴ \times ۶۱$. کوچکترین باقیماندهٔ ۷۴×۶۱ به پیمانه ۸۹ را حساب می‌کنیم و به‌طریق مشابه برای دیگر همنهشتی‌ها پیش می‌رویم، در این صورت داریم

	(پیمانه ۸۹)	$۳۴۵۶ \times ۷۹۸۲ \equiv ۷۴ \times ۶۱ \equiv ۶۴$
	(پیمانه ۹۵)	$۳۴۵۶ \times ۷۹۸۲ \equiv ۳۶ \times ۲ \equiv ۷۲$
(**)	(پیمانه ۹۷)	$۳۴۵۶ \times ۷۹۸۲ \equiv ۶۱ \times ۲۸ \equiv ۵۹$
	(پیمانه ۹۸)	$۳۴۵۶ \times ۷۹۸۲ \equiv ۲۶ \times ۴۴ \equiv ۶۶$
	(پیمانه ۹۹).	$۳۴۵۶ \times ۷۹۸۲ \equiv ۹۰ \times ۶۲ \equiv ۳۶$

بنابراین ۳۴۵۶×۷۹۸۲ جوابی از دستگاه زیر است

	(پیمانه ۸۹)	$x \equiv ۶۴$
	(پیمانه ۹۵)	$x \equiv ۷۲$
(***)	(پیمانه ۹۷)	$x \equiv ۵۹$
	(پیمانه ۹۸)	$x \equiv ۶۶$
	(پیمانه ۹۹).	$x \equiv ۳۶$

۶) دلیل این که چرا اعداد ۸۹، ۹۵، ۹۷، ۹۸ و ۹۹ انتخاب شده در ادامه شرح داده می‌شود.

قضیه باقیمانده چینی[۷] نشان می‌دهد که یک جواب $(***)$ عدد ۲۷۵۸۵۷۹۲ می‌باشد و این که هر جواب (از جمله ۷۹۸۲×۳۴۵۶) همنهشت با این عدد به پیمانه $۷۹۵۶۹۴۹۷۷۰ = ۹۹ \times ۹۸ \times ۹۷ \times ۹۵ \times ۸۹$ است (که از این به بعد آن را با M نشان می‌دهیم). چون هیچ دو عدد بین ۰ و M نمی‌توانند به پیمانه M همنهشت باشند، عدد ۲۷۵۸۵۷۹۲ تنها جواب بین ۰ و M است. می‌دانیم که $۰ < ۳۴۵۶ \times ۷۹۸۲ < ۱۰^۴ \times ۱۰^۴ = ۱۰^۸ < M$. چون عدد ۷۹۸۲×۳۴۵۶ یک جواب است باید داشته باشیم $۳۴۵۶ \times ۷۹۸۲ = ۲۷۵۸۵۷۹۲$.

اکنون از منظر دیگری به این مثال نگاه کنید. اگر کوچکترین باقیمانده یک عدد به پیمانه n را عضوی از $\mathbb{Z}_n$ در نظر بگیرید، آنگاه همنهشتی‌های در $(*)$ بیان می‌کند که عدد صحیح ۳۴۵۶ را می‌توان با عضو $(۷۴, ۳۶, ۶۱, ۲۶, ۹۰)$ در $\mathbb{Z}_{۹۹} \times \mathbb{Z}_{۹۸} \times \mathbb{Z}_{۹۷} \times \mathbb{Z}_{۹۵} \times \mathbb{Z}_{۸۹}$ نمایش داد. به طریق مشابه، عدد ۷۹۸۲ توسط $(۶۱, ۲, ۲۸, ۴۴, ۶۲)$ نمایش داده می‌شود. می‌دانیم که همنهشتی (پیمانه ۸۹) $۶۴ \equiv ۶۱ \times ۷۴$ در $(**)$ معادل تساوی $۶۴ = ۶۱ \times ۷۴$ در $\mathbb{Z}_{۸۹}$ است، بنابراین همنهشتی‌های در $(**)$ معادل با ضرب زیر در $\mathbb{Z}_{۹۹} \times \mathbb{Z}_{۹۸} \times \mathbb{Z}_{۹۷} \times \mathbb{Z}_{۹۵} \times \mathbb{Z}_{۸۹}$ می‌باشد:

$$(۷۴, ۳۶, ۶۱, ۲۶, ۹۰) \cdot (۶۱, ۲, ۲۸, ۴۴, ۶۲) =$$
$$= (۷۴ \times ۶۱, ۳۶ \times ۲, ۶۱ \times ۲۸, ۲۶ \times ۴۴, ۹۰ \times ۶۲)$$
$$= (۶۴, ۷۲, ۵۹, ۶۶, ۳۶).$$

جواب $(***)$ نشان می‌دهد که عنصر $(۶۴, ۷۲, ۵۹, ۶۶, ۳۶)$ از $\mathbb{Z}_{۹۹} \times \mathbb{Z}_{۹۸} \times \mathbb{Z}_{۹۶} \times \mathbb{Z}_{۹۵} \times \mathbb{Z}_{۸۹}$ عدد صحیح ۲۷۵۸۵۷۹۲ را نشان می‌دهد.

اینک شیوه کار برای یک اندازه کلمه واقعی روشن است. گیریم $m_۱, \ldots, m_r$ اعداد صحیح مثبتی باشند که دوبدو نسبت بهم اولند:

۱. هر عدد صحیح t را به صورت عضوی از $\mathbb{Z}_{m_۱} \times \cdots \times \mathbb{Z}_{m_r}$، با محاسبه کلاس همنهشتی t به پیمانه هر m_i نمایش دهید.

۲. محاسبه را در $\mathbb{Z}_{m_۱} \times \cdots \times \mathbb{Z}_{m_r}$ انجام دهید.

۳. از قضیه باقیمانده چینی استفاده کنید تا جواب را به صورت عدد صحیح برگردانید.

این اعداد m_i باید طوری انتخاب شوند که حاصل‌ضرب آنها که آن را با M نشان می‌دهیم از هر

۷) تا اینجا تمام محاسبات به‌سرعت با رایانه فرضی ما قابل انجام بوده است. این اولین جایی است که ممکن است به محاسباتی با دقت مضاعف و بالطبع کندتر نیاز باشد زیرا که اعداد از اندازه کلمه بزرگترند.

عددی که از محاسبات بدست می‌آید بزرگتر باشد. در غیر این صورت فرآیند برگشت در مرحله ۳ ممکن است به شکست بیانجامد (تمرینهای ۵-۳). این کار گاهی با بزرگ گرفتن m_iها تا حدی که از اندازه کلمه رایانه تجاوز نکند انجام می‌شود، همان‌طور که در مثال فوق انجام دادیم. اگر پیمانه‌های کوچکتری انتخاب شود، آنگاه تعداد بیشتری از آنها ممکن است لازم باشد تا مطمئن شویم که M به اندازه کافی بزرگ است.

فرآیند برگشت از اعداد صحیح به نمایش پیمانه‌ای و عکس آن (مراحل ۱ و ۳) مستلزم صرف زمانی است که در ضرب قراردادی اعداد صحیح مورد نیاز نیست (بویژه مرحله ۳، که ممکن است روش‌های با دقت مضاعف را شامل شود). ولی این کار برای هر عدد فقط یکبار بهنگام ورود و خروج لازم به انجام می‌باشد. نمایش پیمانه‌ای را می‌توان برای تمام محاسبات میانی بکار برد. این کار بسیار سریعتر از محاسبهٔ مستقیم با اعداد صحیح بزرگ است، بویژه در رایانه‌ای که ظرفیت پردازش موازی را دارد که می‌تواند همزمان در تمام $\mathbb{Z}_m$ها عمل کند. تحت شرایط مناسب مزیت سرعت حاصل از مرحله ۲ بیشتر از وقت غیرمفید مورد نیاز در مراحل ۱ و ۳ ارزش دارد. برای تفصیل بیشتر به ناث[۸] [۳۳] رجوع کنید.

گاهی یافتن جواب کامل (نه یک جواب اعشاری تقریبی) یک دستگاه از معادلات خطی ضروری می‌باشد. وقتی صدها معادله یا متغیر در دستگاه وجود دارد و ضرایب، اعداد صحیح بزرگ می‌باشند روش‌های معمول رایانه‌ای فقط جواب‌های تقریبی خواهند داشت زیرا رایانه اعداد خیلی بزرگ را به هنگام محاسبات میانی گِرد می‌کند. قضیه باقیمانده چینی اساس یک روش برای یافتن جواب‌های دقیق در چنین دستگاه‌هایی می‌باشد.

به اجمال، این مفهوم چنین است. گیریم m_1، ...، m_r اعداد اول متمایز (و بنابراین دوبدو نسبت به هم‌اول) باشند.[۹] برای هر m_i، دستگاه معادلات را به یک دستگاه روی $\mathbb{Z}_{m_i}$، با جایگزینی ضرایب صحیح با کلاس‌های هم‌ارزی آنها به پیمانه m_i، منتقل کنید. آنگاه هر یک از این دستگاه‌های جدید را با روش‌های معمول حل کنید (روش حذف جردن ـ گاوس[۱۰] بخوبی روی هر میدان $\mathbb{Z}_{m_i}$ عمل می‌کند، همانگونه که روی $\mathbb{R}$ عمل می‌کند، و گِردکردن برای اعداد کوچکتر واقع در $\mathbb{Z}_{m_i}$ مسئله مهمی نیست). بالاخره قضیه باقیمانده چینی و جبر ماتریس‌ها را بکار برید تا جواب‌های به پیمانه m_i را

---

۸) Knuth

۹) در نظر گرفتن اندازه کلمه مثل آنچه در بالا بحث شد در انتخاب m_i نقش دارد.

۱۰) Gauss-Jordan

به جواب‌های اصلی دستگاه برگردانید.[۱۱] یک توضیح خواندنی از این روش (که برای هر کسی که با یکدوره مقدماتی در جبر خطی آشناست قابل دسترسی باشد) در مک‌کیو[۱۲] [۳۵] عرضه شده است.

تمرینها

۱.A. فرض کنید که رایانه شما دارای اندازه کلمه ۱۰۰ باشد. از روشی که در کتاب طراحی شده استفاده کنید تا با بکار بردن $m_1 = ۹۵$، $m_2 = ۹۷$، $m_3 = ۹۸$، $m_4 = ۹۹$ مجموع $۴۱۳۴۵۳ + ۱۲۳۶۸۴$ را پیدا کنید.

۲. (الف) کوچکترین باقیمانده ۶۴۳۹۷ را به پیمانه ۱۲ فقط با استفاده از حساب در $\mathbb{Z}_{۱۲}$ پیدا کنید. [راهنمایی: قضیه‌های ۲.۲ و ۳.۲ و این واقعیت که

$$۶۴۳۹۷ = (((۶ \times ۱۰ + ۴)۱۰ + ۳)۱۰ + ۹)۱۰ + ۷$$

را بکار برید.]

(ب) گیریم عدد صحیح مثبت n کمتر از اندازه کلمه رایانه شما باشد و t عدد صحیح دلخواهی باشد (احتمالاً بزرگتر از اندازه کلمه). توضیح دهید که چگونه می‌توانید کوچکترین باقیمانده t به پیمانه n را پیدا کنید، در حالی که فقط از حساب $\mathbb{Z}_n$ استفاده می‌کنید (و بنابراین از نیاز به روش‌های دقت مضاعف اجتناب می‌کنید).

۳. روش طراحی شده در کتاب را بکار برید تا اعداد ۷ و ۸ را به عنوان عناصر $\mathbb{Z}_۳ \times \mathbb{Z}_۵$ نمایش دهید. ثابت کنید که حاصل‌ضرب این نمایشها در $\mathbb{Z}_۳ \times \mathbb{Z}_۵$ برابر (۱ و ۲) است. اگر قضیه باقیمانده چینی را آن طور که در کتاب آمده است بکار برید تا (۱ و ۲) را به صورت صحیح درآورید، آیا عدد حاصل ۵۶ است؟ چرا نه؟ این مثال نشان می‌دهد که چرا وقتی حاصل‌ضرب m_iها کمتر از جواب مسئله حساب مورد پرسش است این روش کار نمی‌کند. تمرین ۵ را نیز ملاحظه کنید.

---

۱۱) روش برگشت کمی ماهرانه‌تر از آن است که ممکن است در ابتدا بنظر برسد. برای مثال، دستگاه

$$\begin{matrix} ۸x + ۵y = ۱۲ \\ ۴x + ۵y = ۱۰ \end{matrix} \quad \text{روی } \mathbb{Z}_۷ \text{ به دستگاه} \quad \begin{matrix} x + ۵y = ۵ \\ ۴x + ۵y = ۱۰ \end{matrix}$$

تبدیل می‌شود. می‌توانید بررسی کنید که $x = ۴$ و $y = ۳$ یک جواب دستگاه در $\mathbb{Z}_۷$ است. با این حال معلوم نیست که چگونه از این جواب به جواب دستگاه اصلی که $x = \frac{۱}{۲}$، $y = \frac{۸}{۵}$ می‌باشد، برسیم.

۱۲) Mackiw

۴.B گیریم $f : \mathbb{Z} \to \mathbb{Z}_۳ \times \mathbb{Z}_۴ \times \mathbb{Z}_۵$ تابعی باشد که با ضابطه $f(t) = (|\, t \,|_۳, |\, t \,|_۴, |\, t \,|_۵)$ تعریف شده‌است، که در آن $|\, t \,|_n$ کلاس همنهشتی t در $\mathbb{Z}_n$ است. تابع f را می‌توان به عنوان نمایش t به صورت عضوی از $\mathbb{Z}_۳ \times \mathbb{Z}_۴ \times \mathbb{Z}_۵$ تصور کرد که با گرفتن کوچکترین باقیمانده‌ها حاصل می‌شود.

(الف) اگر $۰ \leq r, s \leq ۶۰$، ثابت کنید که $f(r) = f(s)$ اگر و تنها اگر $r = s$. [راهنمایی: قضیه ۲.۱۳.]

(ب) مثالی بزنید تا ثابت کنید که اگر r یا s بزرگتر از ۶۰ باشد، آنگاه قسمت (الف) ممکن است نادرست باشد.

۵. گیریم $m_۱$، $m_۲$، ...، m_r اعداد صحیح مثبت دوبدو نسبت بهم اول باشند و $f : \mathbb{Z} \to \mathbb{Z}_{m_۱} \times \mathbb{Z}_{m_۲} \times \cdots \times \mathbb{Z}_{m_r}$ تابعی باشد که با ضابطه $f(t) = (|\, t \,|_{m_۱}, |\, t \,|_{m_۲}, \ldots, |\, t \,|_{m_r})$ تعریف شده است که در آن $|\, t \,|_{m_i}$ کلاس همنهشتی t در $\mathbb{Z}_{m_i}$ است. گیریم $M = m_۱ m_۲ \cdots m_r$. اگر $۰ \leq r, s \leq M$، ثابت کنید $f(r) = f(s)$ اگر و فقط اگر $r = s$. [تمرین ۴ یک حالت خاص است.]

۶. تمرین ۷ (پ) را فرض شده بگیرید. اگر رایانه شما دارای اندازه کلمه $۲^{۳۵}$ باشد، با انتخاب چه m_iهایی می‌توانید حساب خود را با اعداد صحیحی به بزرگی $۲^{۱۸۴}$ (به طور تقریبی $۲/۴۵ \times ۱۰^{۵۵}$) انجام دهید؟

۷.C (الف) اگر a و b اعداد صحیح مثبت باشند، ثابت کنید که کمترین باقیمانده $۱ - ۲^a$ به پیمانه $۱ - ۲^b$ برابر $۱ - ۲^r$ است، که در آن r کوچکترین باقیمانده a به پیمانه b است.

(ب) اگر a و b اعداد صحیح مثبت باشند، ثابت کنید که بزرگترین شمارنده مشترک $۱ - ۲^a$ و $۱ - ۲^b$ برابر $۱ - ۲^t$ می‌باشد که در آن t بزرگترین شمارنده مشترک a و b است. [راهنمایی: از الگوریتم اقلیدسی و قسمت (الف) استفاده کنید.]

(پ) گیریم a و b اعداد صحیح مثبتی باشند. ثابت کنید که $۱ - ۲^a$ و $۱ - ۲^b$ نسبت بهم اولند اگر و تنها اگر a و b نسبت به هم اول باشند.

۱۳-۳ قضیه باقیمانده چینی برای حلقه‌ها

قضیه باقیمانده چینی برای دو همنهشتی را می‌توان با بیان آن به زبان ایده‌آل‌ها از $\mathbb{Z}$ به حلقه‌های دیگر تعمیم داد. کلید انجام این کار تعریف همنهشتی به پیمانه یک ایده‌آل (بخش ۱.۶) و این واقعیت است که: وقتی A و B ایده‌آل‌هایی در یک حلقه R باشند، مجموعهٔ مجموع‌های $\{a+b \mid a \in A, b \in B\}$ که با $A+B$ نشان داده می‌شود نیز یک ایده‌آل است (تمرین ۱۷ از بخش ۱.۶).

گیریم m و n اعداد صحیح باشند. گیریم I ایده‌آل مضارب m و J ایده‌آل مضارب n در $\mathbb{Z}$ باشند، *آنگاه همنهشتی به پیمانه m درست همان همنهشتی به پیمانه I می‌باشد.* اگر $(m,n)=1$، آنگاه برای برخی $u,v \in \mathbb{Z}$، $mu+nv=1$. از ضرب دو طرف این معادله در هر عدد صحیح r داریم $m(ur)+n(vr)=r$. پس هر عدد صحیح مجموع یک مضرب از m و یک مضرب از n است، یعنی مجموع یک عنصر از ایده‌آل I و یک عنصر از ایده‌آل J. پس $I+J$ تمام حلقه $\mathbb{Z}$ است. **بنابراین شرط $(m,n)=1$ معادل است با این که بگوییم $I+J=\mathbb{Z}$.**

وقتی $(m,n)=1$، اشتراک ایده‌آل‌های I و J ایده‌آلی است که تمام مضارب mn را شامل است. (تمرین ۶ از بخش ۱.۱۳). بنابراین **دو عدد صحیح در پیمانه mn همنهشت هستند دقیقاً وقتی که آنها در پیمانه ایده‌آل $I \cap J$ همنهشت باشند.**

گزاره‌هایی که در بندهای پیش با حروف پررنگ نوشته شده، چگونگی ترجمه قضیه باقیمانده چینی برای دو همنهشتی را به زبان ایده‌آل‌ها بیان می‌کند. با جایگزینی ایده‌آل‌های بحث فوق به هر ایده‌آل دلخواه R، خواهیم داشت:

قضیه ۳.۱۳. (قضیه باقیمانده چینی برای حلقه‌ها). گیریم I و J ایده‌آل‌هایی از حلقهٔ R باشند به طوری که $I+J=R$، آنگاه برای $a,b \in R$، دستگاه

$$x \equiv a \quad (\text{پیمانه } I)$$
$$x \equiv b \quad (\text{پیمانه } J)$$

دارای یک جواب است. هر دو جواب این دستگاه به پیمانه $I \cap J$ همنهشت هستند.

وقتی R عنصر همانی دارد، این قضیه را می‌توان به حالت r ایده‌آل I_1، I_2، I_3، ... و همنهشتی‌های (پیمانه I_k) $x \equiv a_k$ که در آن $I_i + I_j = R$ برای $i \neq j$ تعمیم داد (تمرین ۶ و

هانگرفورد [۱۳] [۷: ص ۱۳۱] را ملاحظه کنید).

برهان قضیه ۳.۱۳. چون $I+J=R$ و $b-a\in R$، لذا $i\in I$ و $j\in J$ وجود دارد به طوری که $i+j=b-a$. پس $a+i=b-j$. گیریم $t=a+i$؛ آنگاه

$$t-a=(a+i)-a=i\in I.$$

بنابراین $t\equiv a\ (I$ پیمانه$)$. به‌طریق مشابه، چون $a+i=b-j$ داریم

$$t-b=(a+i)-b=(b-j)-b=-j\in J.$$

پس $t\equiv b\ (J$ پیمانه$)$، و t یک جواب دستگاه است. اگر z نیز یک جواب باشد آنگاه طبق قضیه ۲.۶، $z\equiv a\ (I$ پیمانه$)$ و $t\equiv a\ (I$ پیمانه$)$ ایجاب می‌کند که $z\equiv t\ (I$ پیمانه$)$. به‌طریق مشابه، $z\equiv t\ (J$ پیمانه$)$. این بدین معنی است که $z-t\in I$ و $z-t\in J$. بنابراین $z-t\in I\cap J$ و $z\equiv t\ (I\cap J$ پیمانه$)$. ■

قضیه ۴.۱۳. اگر I و J ایده‌آل‌هایی از حلقه R باشند و $I+J=R$، آنگاه یک یکریختی حلقه‌ای وجود دارد:

$$R/(I\cap J)\cong(R/I)\times(R/J).$$

برهان. نگاشت $f:R\to R/I\times R/J$ را با ضابطه $f(r)=(r+I,r+J)$ تعریف کنید. آنگاه f یک همریختی است زیرا

$$\begin{aligned}f(r)+f(s)&=(r+I,r+J)+(s+I,s+J)\\&=((r+s)+I,(r+s)+J)=f(r+s),\\f(r)f(s)&=(r+I,r+J)(s+I,s+J)=(rs+I,rs+J)=f(rs).\end{aligned}$$

برای این که ثابت کنیم f پوشاست، گیریم $(a+I,b+J)\in R/I\times R/J$. باید عنصری از R پیدا کنیم که تصویرش تحت f، $(a+I,b+J)$ باشد. طبق قضیه ۳.۱۳ برای دستگاه:

$$\begin{aligned}x&\equiv a\ \ (I\text{ پیمانه})\\x&\equiv b\ \ (J\text{ پیمانه})\end{aligned}$$

---

۱۳) Hungerford

یک جواب $t \in R$ وجود دارد. ولی طبق قضیه ۴.۶، (پیمانه I) $t \equiv a$ نتیجه می‌دهد $t+I = a+I$. به‌طریق مشابه (پیمانه J) $t \equiv b$ نتیجه می‌دهد $t + J = b + J$. بنابراین

$$f(t) = (t + I, t + J) = (a + I, b + J).$$

پس f پوشاست.

گیریم K هسته f باشد. طبق قضیه اول یکریختی ۱۱.۶، R/K یکریخت با $R/I \times R/J$ است. حال K شامل تمام عناصر $r \in R$ است جایی که $f(r)$ عنصر صفر $R/I \times R/J$ است، یعنی تمام rهایی که

$$(r + I, r + J) = (0_R + I, 0_R + J),$$

یا به طور معادل

$$r + I = 0_R + I \quad \text{و} \quad r + J = 0_R + J.$$

ولی $r + I = 0_R + I$ یعنی این که (پیمانه I) $r \equiv 0_R$ و بنابراین $r \in I$. به طریق مشابه $r + J = 0_R + J$ نتیجه می‌دهد $r \in J$. بنابراین $r \in I \cap J$. پس $I \cap J$ هسته f است و $R/(I \cap J) = R/K \cong R/I \times R/J$. ■

نتیجه ۵.۱۳. اگر $(m, n) = 1$، آنگاه یک یکریختی حلقه‌ای $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ وجود دارد.

برهان. در حلقه $\mathbb{Z}$، ایده‌آل (m) شامل همه مضارب m و ایده‌آل (n) شامل تمام مضارب n است. از سه بند اول این بخش ثابت می‌شود که $(m) + (n) = \mathbb{Z}$ و این که ایده‌آل $(m) \cap (n)$ برابر ایده‌آل (mn) است. بنابراین طبق قضیه ۴.۱۳، (با شرط $R = \mathbb{Z}$، $I = (m)$ و $J = (n)$) یک یکریختی

$$\mathbb{Z}_{mn} = \mathbb{Z}/(mn) = \mathbb{Z}/(m) \cap (n) \cong \mathbb{Z}/(m) \times \mathbb{Z}/(n) = \mathbb{Z}_m \times \mathbb{Z}_n$$

وجود دارد. ■

نتیجه ۶.۱۳. اگر $n = p_1^{n_1} p_2^{n_2} \dots p_t^{n_t}$، که در آن p_iها اعداد اول متمایز مثبت و هر $n_i > 0$، آنگاه یک یکریختی حلقه‌ای $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_t^{n_t}}$ وجود دارد.

برهان. چون p_jها اعداد اول متمایزند برای هر i، $p_i^{n_1}$ و حاصل‌ضرب $p_{i+1}^{n_{i+1}} \dots p_t^{n_t}$ نسبت بهم اولند. بنابراین با استفاده مکرر از نتیجه ۵.۱۳ ثابت می‌شود که

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2} p_3^{n_3} \dots p_t^{n_t}} \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \mathbb{Z}_{p_3^{n_3} \dots p_t^{n_t}} \cong \cdots$$
$$\cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_t^{n_t}}.$$

به این ترتیب برهان کامل می‌شود. ■

تمرینها

۱.A. (الف) ثابت کنید که $\mathbb{Z}_{۵} \times \mathbb{Z}_{۱۲}$ یکریخت با $\mathbb{Z}_{۳} \times \mathbb{Z}_{۲۰}$ است.

(ب) آیا $\mathbb{Z}_{۴} \times \mathbb{Z}_{۳۵}$ با $\mathbb{Z}_{۵} \times \mathbb{Z}_{۲۸}$ یکریخت است؟

۲. اگر I و J ایده‌آل‌هایی از حلقه R باشند و $a \in I$ و $b \in J$، ثابت کنید که $ab \in I \cap J$.

۳.B. اگر $(m,n) \neq ۱$، ثابت کنید که $\mathbb{Z}_{mn}$ یکریخت با $\mathbb{Z}_m \times \mathbb{Z}_n$ نیست. [راهنمایی: اگر $(m,n) = d$، آنگاه mn/d عددی صحیح است (چرا؟). اگر یک یکریختی موجود باشد، آنگاه $۱ \in \mathbb{Z}_{mn}$ به $(۱,۱) \in \mathbb{Z}_m \times \mathbb{Z}_n$ تصویر می‌شود. با نشان دادن این‌که $\frac{mn}{d} \times ۱ \neq ۰$ در $\mathbb{Z}_{mn}$ ولی $\frac{mn}{d} \cdot (۱,۱) = (۰,۰)$ در $\mathbb{Z}_m \times \mathbb{Z}_n$ به یک تناقض برسید.]

۴. کدام یک از حلقه‌های زیر یکریختند: $\mathbb{Z}_{۷} \times \mathbb{Z}_{۶} \times \mathbb{Z}_{۲}$، $\mathbb{Z}_{۳} \times \mathbb{Z}_{۴} \times \mathbb{Z}_{۷}$، $\mathbb{Z}_{۸۴}$، $\mathbb{Z}_{۷} \times \mathbb{Z}_{۱۲}$، $\mathbb{Z}_{۴} \times \mathbb{Z}_{۲۱}$، $\mathbb{Z}_{۲} \times \mathbb{Z}_{۳} \times \mathbb{Z}_{۱۲}$؟

۵. اگر $I_۱$، $I_۲$، $I_۳$ ایده‌آل‌هایی از حلقه یکدار R باشند به طوری که $I_۱ + I_۲ = R$ و $I_۲ + I_۳ = R$، ثابت کنید که $(I_۱ \cap I_۲) + I_۳ = R$. [راهنمایی: اگر $r \in R$، در این صورت $r = i_۱ + i_۳$ و $۱_R = t_۲ + t_۳$ برای برخی $i_۱ \in I_۱$، $t_۲ \in I_۲$، $i_۳, t_۳ \in I_۳$. آنگاه $r = (i_۱ + i_۳)(t_۲ + t_۳)$، با انجام این ضرب ثابت کنید که r در $I_۳ + (I_۱ \cap I_۲)$ می‌باشد، تمرین ۲ می‌تواند مفید باشد.]

۶. گیریم $I_۱$، $I_۲$، $I_۳$ ایده‌آل‌هایی از حلقه یکدار R باشند به طوری که برای $i \neq j$، $I_i + J_j = R$. اگر $a_i \in R$، ثابت کنید که دستگاه

$$x \equiv a_۱ \pmod{I_۱} \quad \text{(پیمانه } I_۱\text{)}$$
$$x \equiv a_۲ \pmod{I_۲} \quad \text{(پیمانه } I_۲\text{)}$$
$$x \equiv a_۳ \pmod{I_۳} \quad \text{(پیمانه } I_۳\text{)}$$

دارای یک جواب است و هر دو جواب آن به پیمانه $I_1 \cap I_2 \cap I_3$ همنهشت هستند. [راهنمایی: اگر s جوابی از دو همنهشتی اول باشد از تمرین ۵ و قضیه ۳.۱۳ استفاده کنید تا ثابت کنید که دستگاه

$$x \equiv s \quad (\text{پیمانه } I_1 \cap I_2)$$
$$x \equiv a_3 \quad (\text{پیمانه } I_3)$$

دارای یک جواب است، و این جواب یک جواب دستگاه اصلی است.]

* * * * *

فصل چهاردهم

مشبکه‌ها و جبرهای بولی [1]

پیشنیازها: فصل ۳؛ به‌علاوه پیوست ب برای بخش‌های ۱.۱۴ و ۲.۱۴ و پیوست الف برای بخش ۳.۱۴؛ همچنین برای مثال‌ها و تمرین‌های اختیاری پیشنیازهای دیگری به این شرح لازم است: آنهایی که نمایه "حلقه" دارند بخش ۱.۶؛ آنهایی که نمایه "گروه" دارند بخش ۳.۷؛ و آنهایی که نمایه "میدان" دارند بخش ۲.۹.

مشبکه‌ها (بخش ۱.۱۴) تعمیمی از خواص رابطه ترتیب $\leq$ در دستگاه دیرآشنای اعداد و رابطه ترتیب $\subseteq$ بین مجموعه‌ها می‌باشند. جبرهای بولی (بخش ۲.۱۴) نمونه‌های خاصی از مشبکه‌ها می‌باشند. مشبکه‌ها در منطق، نظریه‌مدار، احتمال، مکانیک کلاسیک و کوانتم مکانیک کاربرد دارند، برخی از آنها در بخش ۳.۱۴ مطرح شده‌اند.

---

۱) Boolean

۱-۱۴ مشبکه‌ها

اگر S یک مجموعه باشد، آنگاه هر زیرمجموعه از $S \times S$ یک **رابطه** روی S نامیده می‌شود. یک رابطه T روی S یک **ترتیب جزیی** نامیده می‌شود هرگاه T در شرایط زیر صدق کند:

(i) **انعکاسی:** برای هر $a \in S$، $(a,a) \in T$.

(ii) **پاد متقارن:** اگر $(a,b) \in T$ و $(b,a) \in T$، آنگاه $a = b$.

(iii) **متعدی:** اگر $(a,b) \in T$ و $(b,c) \in T$، آنگاه $(a,c) \in T$.

یک مجموعه مجهز به یک رابطه ترتیب جزیی یک **مجموعه جزئاً مرتب** نامیده می‌شود.

نماد $\leq$ معمولاً برای نشان دادن یک ترتیب جزیی T بکار می‌رود:

$$a \leq b \quad \text{یعنی} \quad (a,b) \in T.$$

در این نمادگذاری شرایطی که یک ترتیب جزیی را تعریف می‌کنند چنین است:

(i) **انعکاسی:** برای هر $a \in S$، $a \leq a$.

(ii) **پاد متقارن:** اگر $a \leq b$ و $b \leq a$، آنگاه $a = b$.

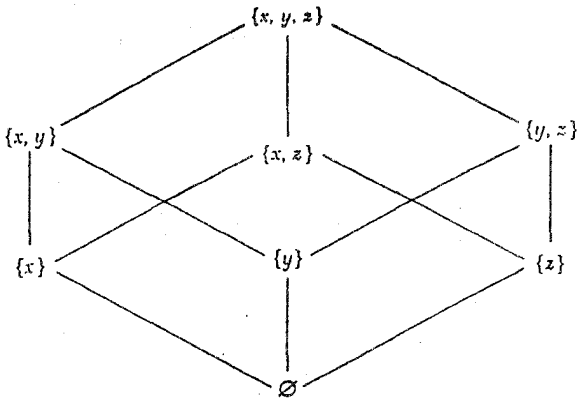
(iii) **متعدی:** اگر $a \leq b$ و $b \leq c$، آنگاه $a \leq c$.

وقتی از این نمادگذاری استفاده می‌شود، یک رابطه ترتیب جزیی روی S را معمولاً بدون آنکه اشاره صریحی به یک زیرمجموعه $S \times S$ شود، تعریف می‌کنند. ما از نماد معمول $\boldsymbol{b \leq a}$ به جای $\boldsymbol{a \geq b}$ نیز استفاده می‌کنیم.

مثال ۱.۱۴. مجموعه اعداد صحیح $\mathbb{Z}$ یک مجموعه جزئاً مرتب است که در آن $a \leq b$ همان معنی معمول را دارد. همین مطلب برای مجموعه اعداد گویای $\mathbb{Q}$ و مجموعه اعداد حقیقی $\mathbb{R}$ درست می‌باشد.

مثال ۲.۱۴. گیریم S مجموعه همه زیرمجموعه‌های $\{x,y,z\}$ باشد و $A \leq B$ را به معنی این که A زیرمجموعه B است تعریف کنید. رابطه " $\subseteq$ " انعکاسی، پاد متقارن و متعدی است (پیوست

ب را نگاه کنید). پس S یک مجموعه جزئاً مرتب است. این ترتیب را می‌توان به صورت طراحی شده با نمودار زیر نمایش داد، که در آن خطی که دو مجموعه را بهم وصل می‌کند چنین معنی می‌دهد که مجموعه پائین‌تر زیرمجموعهٔ مجموعه بالاتر است:



به دلیل خاصیت تعدی می‌توانیم از رسم پاره‌ای از خطوط صرف‌نظر کنیم. برای مثال از $\{x\}$ به $\{x,y,z\}$ خطی نمی‌کشیم، زیرا می‌توانیم از خاصیت تعدّی استفاده کنیم تا توسط خطوط از $\{x\}$ به $\{x,y\}$ و از $\{x,y\}$ به $\{x,y,z\}$ از $\{x\}$ به $\{x,y,z\}$ حرکت کنیم.

مثال ۳.۱۴. اگر X مجموعه‌ای دلخواه (احتمالاً بی‌پایان) باشد، آنگاه $P(X)$، مجموعه تمام زیرمجموعه‌های X، یک مجموعه جزئاً مرتب است که در آن $A \leq B$ به معنای $A \subseteq B$ می‌باشد.

مثال ۴.۱۴. یک رابطه روی مجموعه اعداد صحیح مثبت P توسط: $a \leq b$ به معنای $a|b$، تعریف کنید.[۲] آنگاه $|$ یک ترتیب جزیی روی P است:

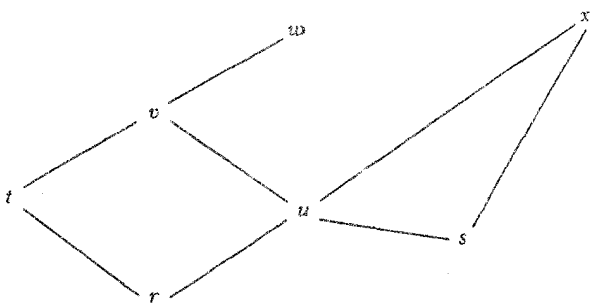
انعکاسی: برای هر $a \in P$، $a|a$ زیرا $a = a \cdot ۱$.

پاد متقارن: اگر $a|b$ و $b|a$، آنگاه $b = au$ و $a = bv$. پس $b = (bv)u$، که نتیجه می‌دهد $uv = ۱$. چون u و v اعداد صحیح مثبت هستند $v = ۱$ و بنابراین $a = bv = b$.

متعدی: اگر $a|b$ و $b|c$، آنگاه $b = av$ و $c = bs$. پس $c = (av)s = a(vs)$ و $a|c$.

۲) اگرچه در حالت کلی وقتی بحث مجموعه‌های جزئاً مرتب مطرح است از نماد $\leq$ استفاده می‌شود، با این حال در مجموعه اعداد صحیح نسبی ترتیب جزیی بخش‌پذیری را با نماد $|$ نشان می‌دهیم تا با مفهوم معمول $\leq$ در مجموعه اعداد صحیح اشتباه نشود.

مثال ۵.۱۴. مجموعه $\{r,s,t,u,v,w,x\}$ یک مجموعه جزئاً مرتب است که ترتیب جزیی آن توسط نمودار زیر ارائه شده است، که در آن $a \leq b$ به معنی آن است که یا $a = b$ و یا a پائین b قرار گرفته است و مسیری از پاره‌خط‌ها از a به b وجود دارد که هرگز به طرف پائین نمی‌آید:



بنابراین $r \leq u$ و $r \leq w$، ولی $r \leq s$ درست نیست. به طریق مشابه برای هر $a \in S$ بجز x، $a \leq w$.

گیریم B زیرمجموعه‌ای از مجموعه جزئاً مرتب S باشد. یک عضو u از S یک کران بالای B است اگر برای هر $b \in B$ داشته باشیم، $b \leq u$. مجموعه B می‌تواند کران‌های بالای متعدد داشته باشد که بعضی از آنها در خود B نیستند، البته ممکن است B هیچ کران بالایی نداشته باشد.

مثال ۶.۱۴. در مثال ۵.۱۴، تنها کرانهای بالای زیرمجموعه $B = \{t,u\}$، v و w می‌باشند. زیرمجموعه $\{r,u,s\}$ دارای چهار کران بالای u، v، w و x است. در مجموعه اعداد صحیح $\mathbb{Z}$ با ترتیب معمولی (مثال ۱.۱۴)، زیرمجموعه اعداد صحیح زوج دارای هیچ کران بالایی نیست.

اگر u یک کران بالای مجموعه B باشد به طوری که برای هر کران بالای دیگر v از B، $u \leq v$، آنگاه u را **کوچکترین کران بالای** (یا l.u.b. یا سوپریمم) B گویند.

مثال ۷.۱۴. در مثال ۵.۱۴، v کوچکترین کران بالای $\{t,u\}$ و u کوچکترین کران بالای $\{r,u,s\}$ است.

مثال ۸.۱۴. زیرمجموعه $\{۲,۳,۶\}$ از مجموعه اعداد صحیح مثبت P که با بخش‌پذیری مرتب شده است (مثال ۴.۱۴)، هر مضرب ۶ را به عنوان یک کران بالا دارد (زیرا ۲، ۳ و ۶ هر مضرب ۶ را می‌شمارد) و خود ۶ کوچکترین کران بالاست.

مثال ۹.۱۴. درمجموعه $\mathbb{Q}$ با ترتیب معمولی (مثال ۱.۱۴)، زیرمجموعه $B = \{b \in \mathbb{Q} \mid b^۲ < ۲\}$ کران‌های بالای متعدد دارد (هر عدد گویای بزرگتر از $\sqrt{۲}$) ولی کوچکترین کران بالا ندارد (تمرین ۹).

گیریم B زیرمجموعه‌ای از مجموعه جزئاً مرتب A باشد. یک عنصر w از A یک **کران پائین** B نامیده می‌شود اگر برای هر $b \in B$، $w \leq b$. اگر w یک کران پائین B باشد به‌طوری که برای هر کران پائین دیگر v از B داشته باشیم $v \leq w$، آنگاه w **بزرگترین کران پائین** (یا g.l.b. یا **اینفیمم**) B نامیده می‌شود.

مثال ۱۰.۱۴. در مجموعه $\mathbb{Z}$ با ترتیب معمولی (مثال ۱.۱۴)، مجموعه اعداد صحیح مثبت P دارای ۱, ۰ و هر عدد صحیح منفی به عنوان کران پائین و ۱ به عنوان یک بزرگترین کران پائین می‌باشد. مجموعه B متشکل از اعداد صحیح منفی دارای هیچ کران پائین و در نتیجه هیچ g.l.b. نیست.

ملاحظه بفرمائید که تعریف "کران پائین" و تعریف "کران بالا" یکسان می‌شود، مشروط بدانکه $\leq$ با $\geq$ جایگزین شود. در نتیجه، خواهیم داشت:

اصل دوگانی. *یک گزاره درست در مورد یک مجموعه جزئاً مرتب درست باقی می‌ماند وقتی $\leq$ با $\geq$ جایگزین شود و "(کوچکترین) کران بالا" با "(بزرگترین) کران پائین" جایگزین شود.*

مثال‌های فوق نشان می‌دهد که یک مجموعه B لازم نیست دارای یک کوچکترین کران بالا یا بزرگترین کران پائین باشد. ولی اگر B یک l.u.b. داشته باشد، این l.u.b. یکتاست و مشابه آن برای g.l.b. نیز درست است:

قضیه ۱.۱۴. گیریم B یک زیرمجموعه ناتهی یک مجموعه جزئاً مرتب S باشد. اگر B دارای یک کوچکترین کران بالا باشد، آنگاه این l.u.b. یکتاست، اگر B دارای یک بزرگترین کران پائین باشد، آنگاه این g.l.b. یکتاست.

برهان. فرض کنید $u_۱$ و $u_۲$ هردو، کوچکترین کرانهای بالای B باشند. طبق تعریف کوچکترین

کران بالا، برای هر کران بالای v از B، $u_1 \leq v$. به ویژه، چون u_2 یک کران بالای B است، $u_1 \leq u_2$. بالعکس، چون u_2 یک کوچکترین کران بالای B است، برای هر کران بالای v از B داریم $u_2 \leq v$. بویژه، $u_2 \leq u_1$. بنابراین طبق خاصیت پاد متقارن، $u_1 = u_2$. بنابراین B دارای یک کوچکترین کران بالاست.

گزاره متناظر برای بزرگترین کران پائین اکنون نتیجه‌ای فوری از اصل دوگانی است. (به بیان دیگر، با تکرار دلیل بالا و جایگزینی $\geq$ بجای $\leq$، "پائین" به جای "بالا" و "بزرگترین" بجای "کوچکترین" می‌توان آن را ثابت کرد.) ■

یک **مشبکه** یک مجموعه جزئاً مرتب L است که در آن هر زوج از عناصر دارای هم یک کوچکترین کران بالا و هم یک بزرگترین کران پائین باشد. اگر $a, b \in L$، آنگاه کوچکترین کران بالای a و b با $a \vee b$ نشان داده می‌شود و **وَست** (یا **پیوند**) a و b نامیده می‌شود. بزرگترین کران پائین a و b با $a \wedge b$ نشان داده می‌شود و **رَسَند** آنها نامیده می‌شود.

مثال ۱۱.۱۴. مجموعه اعداد صحیح مثبت که با بخش‌پذیری مرتب شده است (مثال ۴.۱۴) یک مشبکه است. l.u.b. اعداد صحیح b و c کوچکترین مضرب مشترک آنها و g.l.b.، b و c بزرگترین شمارنده مشترک آنهاست (تمرین ۱۰). مجموعه‌های جزئاً مرتب مثال‌های ۱.۱۴ و ۲.۱۴ نیز مشبکه هستند (تمرین ۴). مجموعه مثال ۵.۱۴ یک مشبکه نیست زیرا w و x دارای هیچ l.u.b. نیست.

مثال ۱۲.۱۴. مجموعه $P(X)$ متشکل از تمام زیرمجموعه‌های X (مثال ۳.۱۴)، یک مشبکه است. اگر A و B زیرمجموعه‌های X باشند، l.u.b. آنها، $A \cup B$ و g.l.b. آنها $A \cap B$ است (تمرین ۱۱).

مثال ۱۳.۱۴. (حلقه‌ها)[۳] اگر R یک حلقه باشد، آنگاه مجموعه S متشکل از تمام ایده‌آل‌های R، که با رابطه شمول ($\subseteq$) جزئاً مرتب شده است، یک مشبکه است (تمرین ۱۹). g.l.b. ایدالهای I و J ایده‌آل $I \cap J$ است. اجتماع دو ایده‌آل ممکن است یک ایده‌آل نباشد، بنابراین در این مشبکه

۳) مثال‌ها و تمرین‌هایی که با کلمات "حلقه‌ها"، "گروهها" یا "میدان‌ها" شروع شده‌اند، برای کسانی که فصول ۶، ۷ و ۹ را نخوانده‌اند اختیاری می‌باشد و خواننده می‌تواند از آن‌ها صرف‌نظر کند.

$I \cup J$ کوچکترین کران بالای I و J نیست. l.u.b. I و J ایده‌آل $I + J$ است (که در تمرین ۱۷ بخش ۱.۶ تعریف شده است).

مثال ۱۴.۱۴. **(گروهها)** اگر G یک گروه باشد، آنگاه مجموعه S متشکل از تمام زیرگروههای G، که توسط رابطه شمول جزئاً مرتب شده یک مشبکه است (تمرین ۲۰). g.l.b. زیرگروههای H و K زیرگروه $H \cap K$ می‌باشد. مجموعه $H \cup K$ ممکن است یک زیرگروه نباشد؛ l.u.b. H و K زیرگروه تولیدشده توسط مجموعه $H \cup K$ می‌باشد (قضیه ۱۲.۷ را نگاه کنید).

گیریم L یک مشبکه باشد. اگر $a, b \in L$، آنگاه $a \vee b$ نیز عضوی از L می‌باشد. بنابراین $\vee$ یک عمل دوتایی روی L است (همان‌طور که در پیوست ب تعریف شده است). به طور مشابه $\wedge$ نیز یک عمل دوتایی روی L است.

قضیه ۲.۱۴. اگر L یک مشبکه باشد، آنگاه برای هر $a, b, c \in L$ اعمال دوتایی $\vee$ و $\wedge$ در این شرایط صدق می‌کنند:

۱. **قوانین جابجایی:**

$$a \vee b = b \vee a \quad , \quad a \wedge b = b \wedge a$$

۲. **قوانین شرکت‌پذیری:**

$$a \vee (b \vee c) = (a \vee b) \vee c,$$
$$a \wedge (b \wedge c) = (a \wedge b) \wedge c.$$

۳. **قوانین جـذب:**

$$a \vee (a \wedge b) = a \quad , \quad a \wedge (a \vee b) = a$$

۴. **قوانین خودتوانی:**

$$a \vee a = a \quad , \quad a \wedge a = a$$

برهان. با توجه به اصل دوگانی، در هر قسمت فقط نیاز به اثبات گزاره اول داریم.

۱. طبق تعریف، $a \vee b$ کوچکترین کران بالای $\{a, b\}$ و $b \vee a$، کوچکترین کران بالای $\{b, a\}$ است. چون مجموعه $\{a, b\}$ همان مجموعه $\{b, a\}$ است، طبق قضیه ۱.۱۴، باشد داشته باشیم $a \vee b = b \vee a$.

۲. ابتدا ثابت می‌کنیم $(a \vee b) \vee c$ یک کران بالای مجموعه $\{a, b, c\}$ است. گیریم $d = a \vee b$. طبق تعریف کران بالا، $c \leq d \vee c = (a \vee b) \vee c$. به طور مشابه

$$a \leq a \vee b \quad \text{و} \quad a \vee b = d \leq d \vee c = (a \vee b) \vee c.$$

بدین دلیل طبق خاصیت تعدّی $a \leq (a \vee b) \vee c$. استدلالی مشابه نشان می‌دهد که $b \leq (a \vee b) \vee c$. بنابراین $(a \vee b) \vee c$ یک کران بالای $\{a, b, c\}$ است.

اینک نشان می‌دهیم $(a \vee b) \vee c$ یک کوچکترین کران بالای $\{a, b, c\}$ می‌باشد. اگر v هر کران بالای دیگری از $\{a, b, c\}$ باشد، $a \leq v$ و $b \leq v$. بنابراین چون $a \vee b$ کوچکترین کران بالا است، داریم $d = a \vee b \leq v$. چون $d \leq v$ و $c \leq v$ طبق تعریف **l.u.b.** دوباره $d \vee c \leq v$. بدین دلیل $(a \vee b) \vee c = d \vee c \leq v$ است. بنابراین $(a \vee b) \vee c$ کوچکترین کران بالای $\{a, b, c\}$ است. استدلال مشابهی نشان می‌دهد که $a \vee (b \vee c)$ نیز یک کوچکترین کران بالای $\{a, b, c\}$ است (تمرین ۱۳). بدین دلیل طبق قضیه ۱.۱۴ (با شرط $B = \{a, b, c\}$)، $a \vee (b \vee c) = (a \vee b) \vee c$.

۳. گیریم $t = a \wedge b$. آنگاه $a \vee t$ یک کران بالای $\{a, t\}$ است، بنابراین $a \leq a \vee t$. چون $a \wedge b$ یک کران پائین $\{a, b\}$ است داریم $t = a \wedge b \leq a$. چون $a \leq a$ باید طبق تعریف کوچکترین کران بالا داشته باشیم $a \vee t \leq a$. طبق خاصیت پادمتقارن، $a = a \vee t = a \vee (a \vee b)$.

۴. وَست $a \vee a$ کوچکترین کران بالای مجموعه $\{a\} = \{a, a\}$ است. ولی خود a به‌وضوح یک کوچکترین کران بالای مجموعه $\{a\}$ است. بنابراین طبق قضیه ۱.۱۴، $a \vee a = a$. ■

قضیه ۲.۱۴ بیان می‌کند که مشبکه دستگاهی است جبری با دو عمل دوتایی که در برخی شرایط صدق می‌کند. بالعکس، هر دستگاه جبری این چنین، یک مشبکه است:

قضیه ۳.۱۴. گیریم L یک مجموعه ناتهی مجهز به دو عمل دوتایی، $\vee$ و $\wedge$ باشد که تابع قوانین جابجایی، شرکت‌پذیری، جذب و خودتوانی است. یک رابطه $\leq$ روی L توسط $a \leq b$ اگر و تنها اگر $a \vee b = b$، تعریف کنید. آنگاه L نسبت به $\leq$ یک مشبکه است به طوری که برای هر $a, b \in L$،

$$\textbf{l.u.b.}\{a, b\} = a \vee b \quad , \quad \textbf{g.l.b.}\{a, b\} = a \wedge b.$$

اگرچه اعمال روی L را با همان نمادهایی که قبلاً برای l.u.b. و g.l.b. بکار رفته است نشان داده‌ایم، ما فرض نمی‌کنیم که L مجهز به یک ترتیب جزیی است. در واقع می‌توانستیم از نمادهای دیگری (برای مثال + و ۰) برای این دو عمل استفاده کنیم. نکته این قضیه آن است که دو عمل با خواص جبری بیان شده را می‌توان بکار برد تا یک ترتیب جزیی را ساخت که تحت آن L یک مشبکه گردد.

برهان قضیه ۳.۱۴. ابتدا ثابت می‌کنیم $\leq$ یک ترتیب جزیی روی L است.

انعکاسی: طبق قانون خودتوانی $a \vee a = a$. پس $a \leq a$.

پاد متقارن: اگر $a \leq b$ و $b \leq a$، آنگاه $a \vee b = b$ و $b \vee a = a$. بنابراین طبق خاصیت جابجایی $a = b \vee a = a \vee b = b$.

متعدی: اگر $a \leq b$ و $b \leq c$، آنگاه $a \vee b = b$ و $b \vee c = c$. بنابراین طبق خاصیت شرکت‌پذیری

$$a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c.$$

بنابراین $a \leq c$.

برای تکمیل اثبات، باید نشان دهیم که اگر $a, b \in L$ آنگاه $a \vee b$، کوچکترین کران بالا و $a \wedge b$، بزرگترین کران پائین $\{a, b\}$ می‌باشد. طبق قوانین جابجایی، شرکت‌پذیری و خودتوانی،

$$b \vee (a \vee b) = (a \vee b) \vee b = a \vee (b \vee b) = a \vee b.$$

پس $b \leq a \vee b$. به طور مشابه

$$a \vee (a \vee b) = (a \vee a) \vee b = a \vee b.$$

بنابراین $a \leq a \vee b$. بنابراین $a \vee b$ یک کران بالای $\{a, b\}$ است. اگر ω کران بالای دیگری از $\{a, b\}$ باشد، در این صورت $a \leq \omega$ و $b \leq \omega$، یعنی $a \vee \omega = \omega$ و $b \vee \omega = \omega$. بنابراین به موجب شرکت‌پذیری،

$$(a \vee b) \vee \omega = a \vee (b \vee \omega) = a \vee \omega = \omega.$$

بنابراین $a \vee b \leq \omega$، لذا $a \vee b$ کوچکترین کران بالای $\{a, b\}$ است. بالاخره در تمرین ۱۸ ثابت می‌شود که

$$a \vee b = b \qquad \text{اگر و تنها اگر} \qquad a \wedge b = a.$$

از این واقعیت استفاده کنید تا ثابت کنید که $a \wedge b$ بزرگترین کران پائین $\{a, b\}$ است (تمرین ۱۸). ■

قضیه ۳.۱۴ نشان می‌دهد که مشبکه‌ها را می‌توان به صورت دستگاههای صرفاً جبری تعریف کرد که اعمال آن در قوانین جابجایی، شرکت‌پذیری، جذب و خودتوانی صدق می‌کند. این امر بعضی وقتها مفیدتر از آن است که مشبکه‌ها را به عنوان نمونه‌های خاصی از مجموعه‌های جزئاً مرتب در نظر بگیریم.

تمرینها

۱.A. گیریم $S = \{۱, ۲, ۳, ۴, ۶, ۱۲\}$ مجموعه شمارنده‌های مثبت ۱۲ باشد.

(الف) ثابت کنید که S یک مجموعه جزئاً مرتب تحت بخش‌پذیری است (یعنی، $a \leq b$ به‌معنی $a|b$ می‌باشد).

(ب) همچون مثال‌های ۲.۱۴ و ۵.۱۴، نموداری از ترتیب جزیی روی S را رسم کنید.

(پ) بررسی کنید که S مشبکه‌ای است که در آن $a \vee b$ کوچکترین مضرب مشترک a و b، و $a \wedge b$ بزرگترین شمارنده مشترک آنها است.

۲. تمرین ۱ را وقتی که S مجموعه تمام شمارنده‌های مثبت ۶۰ باشد حل کنید.

۳. توضیح دهید که بخش‌پذیری ($a \leq b$ یعنی $a|b$) یک رابطه ترتیب جزیی روی مجموعه اعداد صحیح ناصفر نمی‌باشد.

۴. ثابت کنید که $\mathbb{Z}$ با مفهوم معمول $\leq$ یک مشبکه است. [راهنمایی: اگر $a \leq b$، ثابت کنید a، بزرگترین کران پائین و b، کوچکترین کران بالای $\{a, b\}$ است.]

۵. تمرین ۴ را با جایگزینی $\mathbb{Q}$ بجای $\mathbb{Z}$ حل کنید؛ آن را با جایگزینی $\mathbb{R}$ بجای $\mathbb{Z}$ حل کنید.

۶. [گروهها] خطوط کلی ترتیب جزیی مشبکه تمام زیرگروههای $\mathbb{Z}_۶$ را طرح کنید (مانند مثال ۲.۱۴).

۷. [گروهها] تمرین ۶ را با جایگزینی $S_۳$ بجای $\mathbb{Z}_۶$ حل کنید.

۸. اگر S و T مجموعه‌های جزئاً مرتب باشند، یک رابطه ترتیب روی $S \times T$ به صورت $(s, t) \leq (u, v)$ اگر و تنها اگر $s \leq u$ در S و $t \leq v$ در T تعریف کنید.

(الف) ثابت کنید که این رابطه یک ترتیب جزیی روی $S \times T$ است.

(ب) اگر S و T مشبکه باشند، ثابت کنید $S \times T$ یک مشبکه است.

۹. فرض کنید که بین هر دو عدد حقیقی یک عدد گویا وجود داشته باشد و فرض کنید $\sqrt{۲}$ اصم باشد. در مجموعه $\mathbb{Q}$ با ترتیب معمولی ثابت کنید که مجموعه $B = \{b \in \mathbb{Q} \mid b^۲ < ۲\}$ دارای کوچکترین کران بالا نیست.

۱۰. ثابت کنید مجموعهٔ جزئاً مرتب P در مثال ۴.۱۴ یک مشبکه است؛ اثبات کنید که برای $a, b \in P$،

(الف) بزرگترین شمارنده مشترک a و b، بزرگترین کران پایین مجموعه $\{a, b\}$ است.

(ب) کوچکترین مضرب مشترک a و b کوچکترین کران بالای مجموعه $\{a, b\}$ است.

[راهنمایی: تمرین ۳۱ از بخش ۲.۱.]

۱۱. گیریم A یک مجموعه باشد. ثابت کنید که مجموعه $P(X)$ متشکل از تمام زیرمجموعه‌های X، که توسط رابطه $\subseteq$ مرتب شده‌است، یک مشبکه می‌باشد که در آن $A \cup B$، **l.u.b.** A و B، و $A \cap B$، **g.l.b.** آنها می‌باشد.

۱۲. گیریم L یک مشبکه باشد و $a, b \in L$. ثابت کنید گزاره‌های زیر هم‌ارزند.

(الف) $a \leq b$؛ (ب) $a \vee b = b$؛ (پ) $a \wedge b = a$.

۱۳. برهان قضیه ۲.۱۴ را با اثبات این که $a \vee (b \vee c)$ یک **l.u.b.** $\{a, b, c\}$ است تکمیل کنید.

۱۴. ثابت کنید هر زیرمجموعه متناهی از یک مشبکه L دارای هم یک **l.u.b.** و هم یک **g.l.b.** است. [راهنمایی: برهان قسمت ۲ قضیه ۲.۱۴ ثابت می‌کند $(a \vee b) \vee c$ کوچکترین کران بالایی $\{a, b, c\}$ است. این اثبات را پذیرفته از استقراء استفاده کنید تا ثابت کنید که $(a_۱ \vee \ldots \vee a_n) \vee a_{n+۱}$، کوچکترین کران بالای $\{a_۱, \ldots, a_{n+۱}\}$ می‌باشد. برای **g.l.b.** از اصل دوگانی استفاده کنید.]

۱۵. با ذکر مثال ثابت کنید که تمرین ۱۴ ممکن است نادرست باشد اگر در آن کلمه "متناهی" به "نامتناهی" تبدیل شود.

۱۶. اگر L یک مشبکه باشد و $a, b \in L$، و $a \leq b$، ثابت کنید که

(الف) $a \vee c \leq b \vee c$

(ب) $a \wedge c \leq b \wedge c$.

۱۷. اگر L یک مشبکه باشد و $a, b, c \in L$، ثابت کنید که

(الف) $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$.

(ب) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$.

۱۸. گیریم L مجموعه ناتهی مجهز به دو عمل دوتایی، $\vee$ و $\wedge$ باشد که در قوانین جابجایی، شرکت‌پذیری، جذب و خودتوانی صدق می‌کند. برهان قضیه ۳.۱۴ را تکمیل کنید، یعنی ثابت کنید که

(الف) $a \vee b = b$ اگر و تنها اگر $a \wedge b = a$.

(ب) اگر $a \leq b$ به‌معنی $a \vee b = b$ باشد، آنگاه $a \wedge b$، بزرگترین کران پائین $\{a, b\}$ است.

۱۹. [حلقه‌ها] گیریم S مجموعه تمام ایده‌آل‌های حلقهٔ R، جزئاً مرتب شده توسط $\subseteq$ باشد. ثابت کنید که S مشبکه‌ای است که در آن $I + J$، کوچکترین کران بالای I و Jاست و $I \cap J$ بزرگترین کران پائین آنها می‌باشد. [تمرین ۱۷ در بخش ۱.۶ را به بینید.]

۲۰. [گروهها] گیریم S مجموعه تمام زیرگروههای یک گروه G، جزئاً مرتب شده توسط $\subseteq$ باشد. ثابت کنید که S مشبکه‌ای است که در آن $H \cap K$، بزرگترین کران پائین H و K و زیرگروه تولیدشده توسط $H \cup K$ کوچکترین کران بالای آنهاست. [قضیه ۱۲.۷ را نگاه کنید.]

۲۱. (حلقه‌ها) مشبکه ایده‌آل‌های حلقه $\mathbb{Z}$ را توصیف کنید.

۲۲. [میدان‌ها] گیریم $\mathbb{K}$ یک توسیع میدان $\mathbb{F}$ باشد. ثابت کنید مجموعه تمام میدان‌های میانی تحت $\subseteq$ یک مشبکه است. [راهنمایی: ثابت کنید که بزرگترین کران پائین $\mathbb{E}_1$ و $\mathbb{E}_2$ برابر است با $\mathbb{E}_1 \cap \mathbb{E}_2$ وکوچکترین کران بالای آنها اشتراک تمام میدان‌های میانی می‌باشد که هر دو $\mathbb{E}_1$ و $\mathbb{E}_2$ را شامل است، تمرین ۱ در بخش ۲.۹ را ملاحظه کنید.]

۲۳. گیریم S یک مجموعهٔ جزئاً مرتب با این خاصیت باشد که:

اگر $a, b \in S$، آنگاه $a \leq b$ یا $b \leq a$. در این صورت S را یک **مجموعه کلاً مرتب** یا **زنجیر** نامند.

(الف) بررسی کنید که مجموعه‌های $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ در مثال ۱.۱۴ مجموعه‌های کلاً مرتب هستند.

(ب) با ارائه دو عدد صحیح a و b به طوری که $b \nmid a$ و $a \nmid b$ نشان دهید که مجموعه P در مثال ۴.۱۴ مجموعه کلاً مرتب نیست.

(ج) ثابت کنید که مجموعه S در مثال ۲.۱۴، مجموعه کلاً مرتب نیست.

۲۴. ثابت کنید یک مجموعه کلاً مرتب، [تمرین ۲۳] یک مشبکه است.

۲۵. یک عنصر c از یک مجموعه جزئاً مرتب S **بیشین** نامیده می‌شود اگر هیچ عضو b در B موجود نباشد که $c \neq b$ و $c \leq b$. یک عنصر d از S عنصر **کمین** نامیده می‌شود اگر هیچ $b \in S$ موجود نباشد به طوری که $b \neq d$ و $b \leq d$.

(الف) ثابت کنید که مجموعه P مثال ۴.۱۴ دارای یک عنصر کمین است و عنصر بیشین ندارد.

(ب) ثابت کنید که مجموعه S مثال ۵.۱۴ دارای دقیقاً دو عنصر بیشین و دو عنصر کمین است.

(پ) مثالی از یک مجموعه جزئاً مرتب بزنید که دقیقاً یک عنصر بیشین و یک عنصر کمین داشته باشد.

(ت) مثالی از یک مجموعه جزئاً مرتب ارائه کنید که هیچ عنصر بیشین یا عنصر کمین نداشته باشد.

۲۶. اگر L و M مجموعه‌های جزئاً مرتب باشند، آنگاه یک تابع $f : L \to M$ را **حافظ ـ ترتیب** گویند اگر $a \leq b$ در L ایجاب کند که $f(a) \leq f(b)$ در M. اگر L و M مشبکه باشند، آنگاه یک **همریختی مشبکه‌ای** یک تابع $f : L \to M$ است به طوری که برای هر $a, b \in L$، $f(a \vee b) = f(a) \vee f(b)$ و $f(a \wedge b) = f(a) \wedge f(b)$.

(الف) ثابت کنید هر همریختی مشبکه‌ای حافظ ترتیب است.

(ب) با ذکر یک مثال ثابت کنید یک نگاشت حافظ ـ ترتیب مشبکه‌ها لازم نیست یک همریختی مشبکه‌ای باشد.

۲-۱۴ جبرهای بـــولی

یک جبر بولی نوعی مشبکه خاص است. الگوی اصلی برای تعاریف زیر، مشبکه $P(X)$ متشکل از تمام زیرمجموعه‌های مجموعه X است.

بخاطر آورید که

$$A \in P(X) \qquad \text{یعنی} \qquad A \subseteq X$$

و برای $A, B \in P(X)$،

$$A \leq B \qquad \text{یعنی} \qquad A \subseteq B$$

در این مشبکه، $A \vee B = A \cup B$ و $A \wedge B = A \cap B$ (تمرین ۱۱ از بخش ۱.۱۴).

طبق تعریف $P(X)$، برای هر $A \in P(X)$، $A \subseteq X$. بنابراین X خودش بزرگترین عنصر در $P(X)$ است. چون $\emptyset \in P(X)$ و برای هر $A \in P(X)$، $\emptyset \subseteq A$، مجموعه تهی $\emptyset$ کوچکترین عضو $P(X)$ است. به‌علاوه، برای هر $A \in P(X)$،

$$A \cap X = A \qquad \text{و} \qquad A \cup \emptyset = A.$$

برای هر $A \in P(X)$، گیریم A' مکمل نسبی A در X را نشان دهد، یعنی

$$A' = X - A = \{x \mid x \in X, x \notin A\}.$$

فوراً نتیجه می‌شود که

$$A' \vee A = A' \cup A = X \quad (\text{بزرگترین عضو } P(X))$$

و

$$A' \wedge A = A' \cap A = \emptyset \quad (\text{کوچکترین عضو } P(X))$$

بالاخره این مطلب ساده است که تحقیق کنید برای $A, B, C \in P(X)$،

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

اگر $\cap$ را به عنوان ضرب و $\cup$ را به عنوان جمع بگیرید، این اتحاد همان قانون توزیع‌پذیری $A(B + C) = AB + AC$ است. تحقیق کنید که تعویض نقش اجتماع و اشتراک، قانون توزیع‌پذیری دیگری را در $P(X)$ ایجاد می‌کند:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

اکنون این مفاهیم را به مشبکه‌های دلخواه تعمیم می‌دهیم. یک عنصر I از یک مجموعه جزئاً مرتب S یک **بزرگترین عضو** است اگر برای هر $a \in S$، $a \leq I$. یک عنصر O از یک مجموعه جزئاً مرتب S یک **کوچکترین عضو** است اگر برای هر $a \in S$، $O \leq a$. یک مجموعه جزئاً مرتب ممکن است دارای بزرگترین عضو نباشد ولی اگر یک بزرگترین عضو داشته باشد، این عضو یکتاست (تمرین ۱). مشابه این نکات در مورد کوچکترین عضو برقرار است.

مثال ۱۵.۱۴. همان‌طور که در بالا شرح داده شد بزرگترین عضو $P(X)$، X و کوچکترین عضو آن $\emptyset$ است.

مثال ۱۶.۱۴. در مشبکه اعداد صحیح مثبت P، که با بخش‌پذیری مرتب شده است، بزرگترین عضو وجود ندارد (یعنی، هیچ عدد صحیح که بر هر عدد صحیح بخش‌پذیر باشد وجود ندارد). ولی ۱ کوچکترین عضو است چون برای هر $a \in P$، $1|a$.

گیریم L یک مشبکه با بزرگترین عضو I و کوچکترین عضو O باشد. اگر $a \in L$، آنگاه $O \leq a \leq I$. بنابراین طبق تمرین ۱۲ بخش ۱.۱۴،

$$a \vee O = a \qquad \text{و} \qquad a \wedge I = a.$$

یک مشبکه L با بزرگترین عضو I و کوچکترین عضو O را مشبکه **متممدار** گویند اگر برای هر $a \in L$، عضو $a' \in L$ موجود باشد به طوری که

$$a \wedge a' = O \qquad \text{و} \qquad a \vee a' = I.$$

این عضو a' را **متمم** a گویند.

مثال ۱۷.۱۴. مشبکه $P(X)$ همانگونه که در بالا شرح داده شد، یک مشبکه متممدار است.

مثال ۱۸.۱۴. مجموعه $L = \{1, 2, 3, 4, 6, 12\}$ متشکل از تمام شمارنده‌های مثبت ۱۲، مرتب شده با بخش‌پذیری مشبکه‌ای است که در آن $a \vee b$ کوچکترین مضرب مشترک a، b می‌باشد و $a \wedge b$ بزرگترین شمارنده مشترک a، b است (تمرین ۱ از بخش ۱.۱۴). به‌وضوح، ۱۲ بزرگترین

و ۱ کوچکترین عضو L است. ولی L یک مشبکه متممدار نیست زیرا ۶ دارای هیچ متمم نیست (تمرین ۴).

یک مشبکه L **توزیع‌پذیر** نامیده می‌شود اگر قانون توزیع‌پذیری زیر برقرار باشد:

$$\text{برای هر } a,b,c \in L,\quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

در بالا دیدیم که مشبکه $P(X)$ توزیع‌پذیر است. این واقعیت که قانون توزیع‌پذیری دیگری در $P(X)$ برقرار است (که در آن نقش $\wedge$ و $\vee$ عضو می‌شود) حالت خاصی از قضیه زیر است.

قضیه ۴.۱۴. یک مشبکه L توزیع‌پذیر است اگر و تنها اگر برای هر $a,b,c \in L$،

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

برهان. فرض کنید که L توزیع‌پذیر است. آنگاه

$$\begin{aligned}
a \vee (b \wedge c) &= [a \vee (a \wedge c)] \vee (b \wedge c) && \text{[قانون جذب]}\\
&= a \vee [(a \wedge c) \vee (b \wedge c)] && \text{[قانون شرکت‌پذیری]}\\
&= a \vee [(c \wedge a) \vee (c \wedge b)] && \text{[قانون جابجایی]}\\
&= a \vee [(c \wedge (a \vee b)] && \text{[قانون توزیع‌پذیری]}\\
&= a \vee [(a \vee b) \wedge c] && \text{[قانون جابجایی]}\\
&= [a \wedge (a \vee b)] \vee [(a \vee b) \wedge c] && \text{[قانون جذب]}\\
&= [(a \vee b) \wedge a] \vee [[a \vee b] \wedge c] && \text{[قانون جابجایی]}\\
&= (a \vee b) \wedge (a \vee c) && \text{[اعمال قانون توزیع‌پذیری برای } a \vee b \text{، } a \text{ و } c]
\end{aligned}$$

اصل دوگانی طرف عکس آن را به اثبات می‌رساند. ■

یک جبر بولی[۴] یک مشبکه با بزرگترین عضو I و کوچکترین عضو O است که هم متممدار و هم توزیع‌پذیر باشد.

مثال ۱۹.۱۴. مشبکه $P(X)$ یک جبر بولی است. مجموعه $\{۱, ۳, ۵, ۷, ۹, ۱۵, ۲۱, ۳۵, ۱۰۵\}$ از شمارنده‌های مثبت ۱۰۵، مرتب شده توسط بخش‌پذیری، نیز یک جبر بولی است (تمرین ۵). ولی مجموعه $\{۱, ۲, ۳, ۴, ۶, ۱۲\}$ متشکل از شمارنده‌های مثبت ۱۲ مرتب شده توسط بخش‌پذیری یک جبر بولی نیست، زیرا این مشبکه متممدار نیست (تمرین ۴).

در بخش ۱.۱۴ دیدیم که مشبکه‌ها می‌توانند به صورت جبری برحسب اعمال دوتایی $\vee$ و $\wedge$ توصیف شوند، بدون این‌که به یک رابطه ترتیب ارجاع شود. همین مطلب برای جبرهای بولی درست است:

قضیه ۵.۱۴. مجموعه غیرتهی B یک جبر بولی است اگر و تنها اگر اعمال دوتایی $\vee$ و $\wedge$ روی B موجود باشند به طوری که

۱. برای تمام $a, b, c \in B$ اعمال دوتایی $\vee$ و $\wedge$ در قوانین زیر صدق کنند:

قوانین جابجایی:

$$a \vee b = b \vee a \qquad \text{و} \qquad a \wedge b = b \wedge a.$$

قوانین شرکت‌پذیری:

$$a \vee (b \vee c) = (a \vee b) \vee c;$$
$$a \wedge (b \wedge c) = (a \wedge b) \wedge c.$$

قوانین توزیع‌پذیری

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c);$$
$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

---

۴) این نامگذاری به افتخار جورج بول (۱۸۶۴ـ۱۸۱۵) انجام گرفته است. جبرهای بولی اولین مشبکه‌هایی بودند که مورد مطالعه قرار گرفتند. جورج بول از آنها برای فرمول‌بندی منطق و حساب گزاره‌ها استفاده کرد. برای توضیح بیشتر بخش ۳.۱۴ را ملاحظه کنید.

۲. عضوهای $I, O \in B$ موجود باشند به طوری که برای هر $a \in B$

$$a \wedge I = a \qquad \text{و} \qquad a \vee O = a.$$

۳. برای هر $a \in B$، یک عضو $a' \in B$ موجود باشد به طوری که

$$a \wedge a' = O. \qquad \text{و} \qquad a \vee a' = I.$$

برهان. اگر B یک جبر بولی با بزرگترین عضو I وکوچکترین عضو O باشد، آنگاه تعاریف توزیع‌پذیری و متمم‌دار همراه با قضایای ۲.۱۴ و ۴.۱۴ با شرط $a \vee b$ به عنوان کوچکترین کران بالایی $\{a, b\}$، $a \wedge b$ به عنوان بزرگترین کران پایینی و a' به عنوان متمم a نشان می‌دهند که ۳-۱ درست است.

بالعکس، اگر B یک مجموعه با اعمال دوتایی باشد که در شرط ۱ صدق می‌کند، آنگاه طبق قضیه ۳.۱۴، B یک مشبکه توزیع‌پذیر خواهد بود مشروط به آن که در قوانین خودتوانی و جذب صدق کند. اولین قانون خودتوانی برقرار است زیرا

$$\begin{aligned} a = a \vee O &= a \vee (a' \wedge a) && \text{[۲، ۳ و قانون جابجایی]} \\ &= (a \vee a') \wedge (a \vee a) && \text{[قانون توزیع‌پذیری]} \\ &= I \wedge (a \vee a) && \text{[۳]} \\ &= a \vee a && \text{[۲ در مورد } a \vee a \text{ بکار رفته‌است]} \end{aligned}$$

قانون خودتوانی دیگر به طریق مشابه ثابت می‌شود. اولین قانون جذب نیز برقرار است:

$$\begin{aligned} a \vee (a \wedge b) &= (a \wedge I) \vee (a \wedge b) && \text{[۲]} \\ &= a \wedge (I \vee b) && \text{[قانون توزیع‌پذیری]} \end{aligned}$$

ولی در تمرین ۸ ثابت می‌شود که $I \vee b = I$. بنابراین طبق ۲،

$$a \vee (a \wedge b) = a \wedge (I \vee b) = a \wedge I = a.$$

به طور مشابه قانون جذب دیگر ثابت می‌شود. بنابراین طبق قضیه ۳.۱۴، B یک مشبکه توزیع‌پذیر است که در آن $a \leq b$ یعنی $a \vee b = b$.

اگر $a \in B$، آنگاه طبق ۲ و خاصیت جابجایی $O \vee a = a$. پس برای هر a، $O \leq a$. شرط $a \vee b = b$ طبق تمرین ۱۸ (الف) از بخش ۱.۱۴ هم‌ارز با $a \wedge b = a$ است. از اینرو نیمه دوم شرط ۲ $(a \wedge I = a)$ ایجاب می‌کند که برای هر $a \in B$، $a \leq I$. بنابراین I بزرگترین و O کوچکترین عضو در B است. طبق ۳، B یک مشبکه متممدار است و بدین دلیل یک جبر بولی است. ■

از قضیه ۵.۱۴ اغلب به عنوان یک تعریف جبرهای بولی استفاده می‌شود. در قضیه زیر واقعیت‌های مهم جبری دیگری درباره جبرهای بولی آمده است.

قضیه ۶.۱۴. اگر B یک جبر بولی باشد و $a, b, c \in B$، آنگاه

۱. $a \vee I = I$ و $a \wedge O = O$.

۲. قوانین حذف برقرار است:

اگر $a \vee b = a \vee c$ و $a \wedge b = a \wedge c$، آنگاه $b = c$.

۳. a دارای متمم یکتاست، یعنی

اگر $a \vee c = I$ و $a \wedge c = O$، آنگاه $c = a'$.

۴. $(a')' = a$

۵. $O' = I$ و $I' = O$

۶. قوانین دمورگان [۵] برقرار است:

$$(a \wedge b)' = a' \vee b' \quad \text{و} \quad (a \vee b)' = a' \wedge b'.$$

برهان ۱. تمرین ۸.

---

۵) De Morgan's laws

۲. اگر $a \vee b = a \vee c$ و $a \wedge b = a \wedge c$، آنگاه

$$
\begin{aligned}
b &= a \vee (b \wedge a) && \text{[قانون جذب]}\\
&= b \vee (a \wedge b) && \text{[قانون جابجایی]}\\
&= b \vee (a \wedge c) && [a \wedge b = a \wedge c]\\
&= (b \vee a) \wedge (b \vee c) && \text{[قانون توزیع‌پذیری]}\\
&= (a \vee b) \wedge (b \vee c) && \text{[قانون جابجایی]}\\
&= (a \vee c) \wedge (b \vee c) && [a \vee b = a \vee c]\\
&= (c \vee a) \wedge (c \vee b) && \text{[قانون جابجایی]}\\
&= c \vee (a \wedge b) && \text{[قانون توزیع‌پذیری]}\\
&= c \vee (a \wedge c) && [a \wedge b = a \wedge c]\\
&= c \vee (c \wedge a) && \text{[قانون جابجایی]}\\
&= c && \text{[قانون جذب]}
\end{aligned}
$$

۳. اگر $a \vee c = I$ و $a \wedge c = O$، آنگاه $a \vee c = a \vee a'$ و $a \wedge c = a \wedge a'$. بنابراین طبق قانون حذف $c = a'$.

۴. می‌دانیم $a' \vee a = I$ و $a' \wedge a = O$. با استفاده از ۳ (با جایگزینی a' بجای a و a بجای c)، داریم $a = (a')'$.

۵. تمرین ۹.

۶. طبق ۳ (با جایگزینی $a \vee b$ بجای a و $a' \wedge b'$ بجای c)، کافی است نشان دهیم که $(a \vee b) \vee (a' \wedge b') = I$ و $(a \vee b) \wedge (a' \wedge b') = O$ تا نتیجه بگیریم که $a' \wedge b' = (a \vee b)'$.

ولی

$$
\begin{aligned}
(a \vee b) \vee (a' \wedge b') &= a \vee (b \vee (a' \wedge b')) && \text{[قانون شرکت‌پذیری]}\\
&= a \vee ((b \vee a') \wedge (b \vee b')) && \text{[قانون توزیع‌پذیری]}\\
&= a \vee (b \vee a') \wedge I && [b' \text{ تعریف}]\\
&= a \vee (b \vee a') && [I \text{ تعریف}]\\
&= (a \vee b) \vee a' && \text{[قانون شرکت‌پذیری]}\\
&= a' \vee (a \vee b) && \text{[قانون جابجایی]}\\
&= (a' \vee a) \vee b && \text{[قانون شرکت‌پذیری]}\\
&= I \vee b && [a' \text{ تعریف}]\\
&= I && [۱]\\
(a \vee b) \wedge (a' \wedge b') &= (a' \wedge b') \wedge (a \vee b) && \text{[قانون جابجایی]}\\
&= ((a' \wedge b') \wedge a) \vee ((a' \wedge b') \wedge b) && \text{[قانون توزیع‌پذیری]}\\
&= ((a' \wedge a) \wedge b') \vee (a' \wedge (b' \wedge b)) && \text{[جابجایی و شرکت‌پذیری]}\\
&= (O \wedge b') \vee (a' \wedge O) && [b' \text{ و } a' \text{تعریف}]\\
&= (O \vee O) = O && [O \text{ تعریف و } ۱]
\end{aligned}
$$

اصل دوگانی اکنون دومین قانون دمورگان را ثابت می‌کند. ■

باقیمانده این بخش برای بخش ۳.۱۴ نیاز نیست و اگر بخواهید می‌توانید آن را حذف کنید. دو جبر بولی را **یکریخت** گویند، اگر یک تابع دوسویی $f : B \to C$ موجود باشد به طوری که برای هر $a, b \in B$، $f(a \wedge b) = f(a) \wedge f(b)$ و $f(a \vee b) = f(a) \vee f(b)$؛ تابع f یک **یکریختی** نامیده می‌شود. این تعریف، با تعریف یکریختی حلقه‌ها سازگار است ـ در هر دو حالت یک نگاشت دوسویی وجود دارد که اعمال دوتایی این دستگاه‌ها را حفظ می‌کند.

در اینجا دلیلی برای این که چرا جبر بولی $P(X)$ متشکل از تمام زیرمجموعه‌های یک مجموعه X، یک مثال اصلی برای جبرهای بولی است آورده‌شده‌است.

قضیه ۷.۱۴. اگر B یک جبر بولی متناهی باشد، آنگاه یک مجموعه متناهی X وجود دارد به طوری که B با $P(X)$ یکریخت است.

خطوط کلی برهان این قضیه در تمرین ۳۱ ارائه شده است. مثال ۱ پیوست **پ** نشان می‌دهد که اگر یک مجموعه X، n عضو داشته باشد، آنگاه مجموعه $P(X)$ دارای 2^n عضو است. بنابراین نتیجه زیر را داریم:

نتیجه ۸.۱۴. یک جبر بولی متناهی دارای 2^n عضو، برای برخی عدد صحیح n، می‌باشد.

قضیه ۷.۱۴ برای جبرهای بولی نامتناهی درست نیست. اگر B جبر بولی دلخواهی باشد، آنگاه یک مجموعه X وجود دارد به طوری که B با جبر بولی تشکیل شده توسط گردایه‌ای از زیرمجموعه‌های X (که احتمالاً تمام آنها نباشد) یکریخت است.

توصیف جبرهای بولی در قضیه ۵.۱۴ نشان می‌دهد که یک جبر بولی تقریباً یک حلقه جابجایی یکدار است. اگر $\vee$ به عنوان جمع و $\wedge$ به عنوان ضرب در نظر گرفته شود در این صورت O عنصر صفر و I عنصر همانی ضربی است. تنها اصلی از حلقه که برقرار نیست وجود منفی‌ها (معکوس‌های جمعی) است؛ به تمرین ۳۲ نگاه کنید. با این وجود، به هر جبر بولی می‌توان حلقه‌ای جابجایی نظیر کرد.

قضیه ۹.۱۴. گیریم B یک جبر بولی باشد و اعمال $+$ و $\cdot$ را روی B به صورت

$$a+b=(a\wedge b')\vee(a'\wedge b) \qquad \text{و} \qquad a\cdot b=a\wedge b$$

تعریف کنید. تحت این اعمال B یک حلقه جابجایی یکدار است به طوری که برای هر $a\in B$، $a\cdot a=a$.

تمرین‌های ۱۱ و ۳۶ در بخش ۱.۳ حالت‌های خاص این قضیه هستند (زیرا برای مجموعه‌ها، $A\cap B'=A-B$).

برهان قضیه ۹.۱۴. چون B تحت $\vee$ و $\wedge$ بسته است، B تحت $+$ و $\cdot$ بسته است. چون $\wedge$

و $\vee$ جابجایی هستند، $+$ نیز جابجایی است:

$$\begin{aligned} a+b = (a \wedge b') \vee (a' \wedge b) &= (a' \wedge b) \vee (a \wedge b') \\ &= (b \wedge a') \vee (b' \wedge a) \\ &= b + a. \end{aligned}$$

طبق تعریف $+$ داریم

$$(a+b)+c = [((a \wedge b') \vee (a' \wedge b)) \wedge c'] \vee [((a \wedge b') \vee (a' \wedge b))' \wedge c].$$

تمرین ۱۷ نشان می‌دهد که

$$((a \wedge b') \vee (a' \wedge b))' = (a \wedge b) \vee (a' \wedge b').$$

این واقعیت و قوانین توزیع‌پذیری، شرکت‌پذیری و جابجایی برای $\vee$ و $\wedge$ نشان می‌دهد که

$$\begin{aligned} (a+b)+c &= [((a \wedge b') \vee (a' \wedge b)) \wedge c'] \vee [((a \wedge b) \vee (a' \wedge b')) \wedge c] \\ &= [((a \wedge b') \wedge c') \vee ((a' \wedge b)) \wedge c'] \vee [((a \wedge b) \wedge c) \vee ((a' \wedge b') \wedge c)] \\ &= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a \wedge b \wedge c) \vee (a' \wedge b' \wedge c). \end{aligned}$$

خاصیت جابجایی $+$، واقعیت قبل (بکار رفته برای a، b، c بجای b، c، a)، و خاصیت جابجایی $\vee$ و $\wedge$ نشان می‌دهد که

$$\begin{aligned} a+(b+c) &= (b+c)+a \\ &= (b \wedge c' \wedge a') \vee (b' \wedge c \wedge a') \vee (b \wedge c \wedge a) \vee (b' \wedge c' \wedge a) \\ &= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a \wedge b \wedge c) \vee (a' \wedge b' \wedge c) \\ &= (a+b)+c. \end{aligned}$$

بنابراین جمع شرکت‌پذیر است. عنصر صفر، O است زیرا طبق قضایای ۵.۱۴ و ۶.۱۴

$$\begin{aligned} a+O &= (a \wedge O') \vee (a' \wedge O) \\ &= (a \wedge I) \vee (a' \wedge O) = a \vee O = a \end{aligned}$$

هر عنصر $a \in B$ منفی خودش می‌باشد زیرا طبق قضیه ۵.۱۴،

$$a + a = (a \wedge a') \vee (a' \wedge a) = O \vee O = O.$$

عمل ضرب $\cdot$ (یعنی همان $\wedge$) جابجایی و شرکت‌پذیر است و طبق قضیه ۵.۱۴، عنصر همانی آن I است. طبق خاصیت جذب و قضیه ۵.۱۴،

$$a \cdot a = a \wedge a = a \wedge (a \wedge O) = a.$$

اینک فقط لازم است قانون توزیع‌پذیری را تحقیق کنیم:

$$\begin{aligned}
ab + ac &= [(a \wedge b) \wedge (a \wedge c)'] \vee [(a \wedge b)' \wedge (a \wedge c)] \\
&= [(a \wedge b) \wedge (a' \vee c')] \vee [(a' \vee b') \wedge (a \wedge c)] \\
&= [((a \wedge b) \wedge a') \vee ((a \wedge b) \wedge c')] \vee [(a' \wedge (a \wedge c) \vee (b' \wedge (a \wedge c))] \\
&= ((a \wedge a') \wedge b) \vee (a \wedge (b \wedge c')) \vee ((a' \wedge a) \wedge c) \vee (b' \wedge (a \wedge c)) \\
&= ((O \wedge b) \vee (a \wedge (b \wedge c')) \vee (O \wedge c) \vee (a \wedge (b' \wedge c)) \\
&= O \vee (a \wedge (b \wedge c')) \vee O \vee (a \wedge (b' \wedge c)) \\
&= a \wedge (b \wedge c') \vee (a \wedge (b' \wedge c)) \\
&= a \wedge [(b \wedge c') \vee (b' \wedge c)] = a \cdot (b + c).
\end{aligned}$$

به این ترتیب برهان کامل می‌شود. ■

یک حلقه یکدار که در آن برای هر a، $a \cdot a = a$ یک **حلقه بولی** نامیده می‌شود. تمرین ۲۱ در بخش ۲.۳ نشان می‌دهد که هر حلقه بولی R جابجایی است و برای هر $a \in R$، $a + a = 0_R$. قضیه ۹.۱۴ می‌گوید که هر جبر بولی یک حلقه بولی تعریف می‌کند. عکس آن نیز درست است:

قضیه ۱۰.۱۴. گیریم R یک حلقه بولی باشد و اعمال دوتایی $\vee$ و $\wedge$ را روی R به صورت

$$a \vee b = a + b - ab \qquad \text{و} \qquad a \wedge b = ab$$

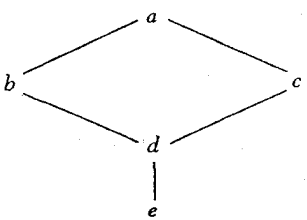
تعریف کنید. تحت این اعمال R یک جبر بولی است.

برهان. تمرین ۳۳. ■

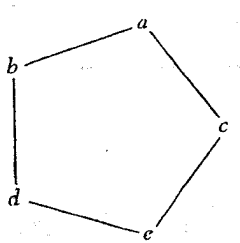
تمرینهـا

۱.A. ثابت کنید که یک مجموعه جزئاً مرتب دارای حداکثر یک بزرگترین عضو و یک کوچکترین عضو است.

۲. ثابت کنید که مشبکه پنج عضوی که ترتیب آنها با نمودار زیر مشخص شده است متمدار نیست.



۳. در مشبکه پنج عضوی که ترتیب آن با نمودار زیر نشان داده شده است یک عضو که دارای دو متمم است پیدا کنید.

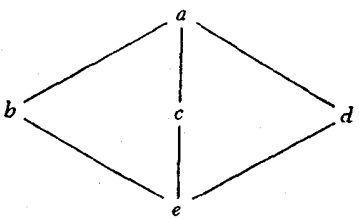


۴. ثابت کنید که عدد ۶ در مشبکه $\{1, 2, 3, 4, 6, 12\}$ که با بخش‌پذیری مرتب شده است دارای متمم نیست. [راهنمایی: یک متمم c برای عدد ۶ باید در شرط $\text{ک.م.م}\{6, c\} = 12$ و

۱ = {۶, c}ب.م.م. صدق کند.]

۵. ثابت کنید که مشبکه تمام شمارنده‌های مثبت ۱۰۵ که با بخش‌پذیری مرتب شده‌است، یک مشبکه متمدار است.

۶. ثابت کنید که مشبکه پنج عضوی که ترتیب آن با نمودار زیر داده شده است توزیع‌پذیر نیست.



۷. ثابت کنید که مشبکه تمام شمارنده‌های مثبت ۱۵، مرتب شده با بخش‌پذیری یک جبر بولی است.

۸. اگر B یک جبر بولی باشد، ثابت کنید که برای هر $a \in B$، $a \vee I = I$ و $a \wedge O = O$.

۹. اگر B یک جبر بولی باشد، ثابت کنید که $O' = I$ و $I' = O$.

۱۰.B. گیریم q، p دو عدد اول مثبت متمایز و L مشبکه تمام شمارنده‌های مثبت p^2q، مرتب شده توسط بخش‌پذیری باشد. ثابت کنید که pq دارای متمم نیست. [تمرین ۴ یک حالت خاص است.]

۱۱. گیریم p، q، r اعداد اول متمایز باشد و L مشبکه تمام شمارنده‌های مثبت pqr باشد، که با بخش‌پذیری مرتب شده است. ثابت کنید که L یک مشبکه متمدار است. [تمرین ۵ یک حالت خاص است.]

۱۲. یک مشبکه L **مشبکه مدولی** نامیده می‌شود اگر برای هر $a, b, c \in L$، $a \leq c$ ایجاب کند $a \vee (b \wedge c) = (a \vee b) \wedge c$. ثابت کنید که هر مشبکه توزیع‌پذیر مشبکه مدولی است. [عکس این مطلب نادرست است، به تمرین ۳۵ نگاه کنید.]

۱۳. ثابت کنید مشبکه اعداد صحیح مثبت P مرتب شده با بخش‌پذیری، توزیع‌پذیر است.

۱۴. گیریم S مجموعه‌ای ناتهی، D یک مشبکه توزیع‌پذیر و L مجموعه تمام توابع از S به D باشد. رابطه ترتیبی $f \leq g$ در L اگر و تنها اگر برای هر $x \in S$، $f(x) \leq g(x)$ را روی L تعریف کنید. ثابت کنید که L یک مشبکه توزیع‌پذیر است.

۱۵. اگر L یک مشبکه توزیع‌پذیر باشد، ثابت کنید که قانون حذف در L برقرار است (قضیه ۶.۱۴ را ببینید).

۱۶. ثابت کنید که در یک جبر بولی، $a \leq b$ اگر و تنها اگر $a' \leq b'$.

۱۷. گیریم B یک جبر بولی باشد. ثابت کنید که برای هر $a, b \in B$،

$$((a \wedge b') \vee (a' \wedge b))' = (a \wedge b) \vee (a' \wedge b').$$

۱۸. در یک جبر بولی ثابت کنید که $a = b$ اگر و تنها اگر $(a \wedge b') \vee (a' \wedge b) = O$.

۱۹. گیریم B یک جبر بولی باشد و $a, b, c \in B$. اگر $a \vee b = a \vee c$ و $a' \vee b = a' \vee c$، ثابت کنید که $b = c$.

۲۰. گیریم B مجموعه $\{۰, ۱\}$ با ترتیب داده شده توسط $۰ \leq ۱$ باشد. برای هر عدد صحیح مثبت n گیریم B^n حاصل‌ضرب دکارتی $B \times \cdots \times B$ از n نسخه B باشد. روی B^n یک عمل $\vee$ توسط

$$(a_۱, \ldots, a_n) \vee (b_۱, \ldots, b_n) = (c_۱, \ldots, c_n)$$

تعریف کنید که در آن برای هر i، c_i ماکسیمم a_i و b_i است. به طور مشابه تعریف کنید

$$(a_۱, \ldots, a_n) \wedge (b_۱, \ldots, b_n) = (d_۱, \ldots, d_n)$$

که در آن برای هر i، d_i مینیمم a_i، b_i است. بالاخره، تعریف کنید

$$(a_۱, \ldots, a_n)' = (a'_۱, \ldots a'_n)$$

جایی که $O' = ۱$ و $۱' = O$. ثابت کنید که B^n یک جبر بولی است که در آن $O = (۰, ۰, \ldots, ۰)$ و $I = (۱, ۱, \ldots, ۱)$.

تذکر: در تمرین‌های ۳۱-۲۱ از تعاریف زیر استفاده شده است. گیریم B یک جبر بولی

باشد. آنگاه $a < b$ معنی می‌دهد $a \leq b$ و $a \neq b$. یک عنصر $a \in B$ یک اتم است اگر $O < a$ و هیچ عنصر b موجود نباشد که $O < b < a$.

۲۱. ثابت کنید که a در جبر بولی B یک اتم می‌باشد اگر و تنها اگر $a \neq O$ و برای هر $b \in B$، یا $a \wedge b = a$ یا $a \wedge b = O$.

۲۲. گیریم B یک جبر بولی باشد و $a, b, c, d \in B$ و a اتم باشد. ثابت کنید

(الف) $d \leq b \wedge c$ اگر و تنها اگر $d \leq b$ و $d \leq c$.

(ب) $a \leq b \vee c$ اگر و تنها اگر $a \leq b$ یا $a \leq c$. [راهنمایی: اگر $a \leq b \vee c$، آنگاه $a = a \wedge (b \vee c)$. از توزیع‌پذیری و تمرین ۲۱ استفاده کنید تا ثابت کنید که یا $a \wedge b = a$ یا $a \wedge c = a$.]

۲۳. در جبر بولی $P(X)$ متشکل از تمام زیرمجموعه‌های X، ثابت کنید که A یک اتم است اگر و تنها اگر A یک زیرمجموعه تک عضوی X باشد.

۲۴. گیریم B یک جبر بولی متناهی باشد، $b \in B$ و $b \neq O$. ثابت کنید که یک اتم $a \in B$ وجود دارد که $a \leq b$. [راهنمایی: اگر b یک اتم باشد، قرار دهید $a = b$. اگر b اتم نباشد، عضو $a_1 \in B$ وجود دارد که $O < a_1 < b$ (چرا؟). اگر a_1 اتم نباشد، عضو $a_2 \in B$ وجود دارد که $O < a_2 < a_1 < b$. بدین طریق ادامه دهید، چرا این فرایند به یک اتم خاتمه می‌یابد؟]

۲۵. اگر a_1 و a_2 در یک جبر بولی اتم باشند و $a_1 \wedge a_2 \neq O$، ثابت کنید که $a_1 = a_2$. [راهنمایی: تمرین ۲۱.]

۲۶. گیریم B یک جبر بولی باشد و $b, c \in B$. ثابت کنید که شرایط زیر معادلند:

(الف) $b \leq c$، (ب) $b \wedge c' = O$، (پ) $b' \vee c = I$.

[راهنمایی: (الف) $\Leftarrow$ (ب) $b \leq c$ نتیجه می‌دهد $b \vee c = c$؛ از جایگزینی و قوانین دمورگان استفاده کنید. (ب) $\Leftarrow$ (پ) دمورگان. (پ) $\Leftarrow$ (الف) $b = b \wedge I = b \wedge (b' \wedge c)$؛ از توزیع‌پذیری استفاده کنید.]

۲۷. گیریم B یک جبر بولی متناهی باشد و $b, c \in B$، با $b \not\leq c$. ثابت کنید که یک اتم $a \in B$ وجود دارد که $a \leq b$ و $a \not\leq c$. [راهنمایی: تمرین‌های ۲۶ و ۲۴.]

۲۸. گیریم B یک جبر بولی متناهی باشد و $b \in B$. اگر a_1، a_2، ...، a_m تمامی اتم‌های B باشند که کوچکتر یا مساوی b هستند، ثابت کنید که $b = a_1 \vee a_2 \vee \cdots \vee a_m$. [راهنمایی: گیریم $c = a_1 \vee \cdots \vee a_m$ آنگاه $c \leq b$ (چرا؟) برای اثبات این که $b \leq c$، به خلاف فرض کنید که $b \not\leq c$ و از تمرین ۲۷ استفاده کنید تا به یک تناقض برسید.]

۲۹. گیریم B یک جبر بولی متناهی باشد و $b \in B$. اگر a و a_1، ...، a_m اتم‌هایی در B باشند به طوری که $a \leq b$ و $b = a_1 \vee a_2 \vee \cdots \vee a_m$، ثابت کنید که برای برخی i، $a = a_i$. [راهنمایی: $a = a \wedge b = a \wedge (a_1 \vee \cdots \vee a_m)$ (دلیل برابری دوم چیست؟). از توزیع‌پذیری و تمرین ۲۵ استفاده کنید.]

۳۰. گیریم B یک جبر بولی متناهی باشد و $b \in B$. اگر $b = a_1 \vee a_2 \vee \cdots \vee a_m$ و $b = c_1 \vee c_2 \vee \cdots \vee c_k$ با شرط این که a_iها اتم‌های متمایز و c_jها اتم‌های متمایزند، ثابت کنید که $m = k$ و (پس از ترتیب مجدد و نمایه‌گذاری مجدد، اگر لازم شد) برای هر i، $a_i = c_i$ [راهنمایی: تمرین ۲۹.]

۳۱. قضیه ۷.۱۴ را ثابت کنید: اگر B یک جبر بولی متناهی باشد، آنگاه یک مجموعه X وجود دارد به طوری که B با $P(X)$ یکریخت است. [راهنمایی: گیریم X مجموعه اتم‌های B باشد. طبق تمرین‌های ۲۸ و ۳۰ هر عضو B را می‌توان به صورت یکتایی به شکل $a_1 \vee a_2 \vee \cdots \vee a_m$ نوشت که در آن a_iها عناصر متمایز X می‌باشند. تابع $\theta : B \to P(X)$ را با ضابطه $\theta(a_1 \vee a_2 \vee \cdots \vee a_m) = \{a_1, a_2, \ldots, a_m\}$ تعریف کنید. چرا θ پوشاست؟ از تمرین ۲۷ استفاده کنید تا ثابت کنید که θ یک به یک است و از تمرین ۲۲ استفاده کنید تا ثابت کنید که $\theta(b \wedge c) = \theta(b) \wedge \theta(c)$ و $\theta(b \vee c) = \theta(b) \vee \theta(c)$.]

۳۲. اگر X یک مجموعه با بیشتر از دو عضو باشد، ثابت کنید جبر بولی $P(X)$ با اعمال $\cup$ به عنوان جمع و $\cap$ به عنوان ضرب، یک حلقه نیست.

۳۳. قضیه ۱۰.۱۴ را ثابت کنید: یک حلقه بولی R یک جبر بولی است با اعمال دوتایی $\vee$ و $\wedge$ که با ضابطه $a \vee b = a + b - ab$ و $a \wedge b = ab$ تعریف می‌شوند. [راهنمایی: گیریم $I = 1_R$ و $O = 0_R$ و $a' = 1_R - a$، از قضیه ۵.۱۴ استفاده کنید.]

۳۴. برای هر جبر بولی B مثل آنچه در قضیه ۹.۱۴ آمده است، گیریم $S(B)$ حلقه تعریف شده توسط B را نشان دهد. برای هر حلقه بولی R، مثل آنچه در قضیه ۱۴-۱۰ آمده است، گیریم

$T(R)$ جبر بولی تعریف شده توسط R باشد. با اثبات دو گزاره زیر نشان دهید که مفاهیم جبر بولی و حلقه بولی معادلند:

(الف) برای هر جبر بولی B، $T(S(B)) = B$.

(ب) برای هر حلقه بولی R، $S(T(R)) = R$.

۳۵.C. (گروهها) ثابت کنید که مجموعه تمامی زیرگروههای نرمال یک گروه، یک مشبکه مدولی است که ممکن است توزیع‌پذیر نباشد. [تمرین ۱۲ را نگاه کنید.]

۱۴-۳ کاربردهای جبرهای بولی

این بخش مشتمل بر دو زیربخش مستقل است که در ترتیب مطالعه آنها اولویتی وجود ندارد. بخش اول با منطق نمادین سروکار دارد که جبرهای بولی از آن نشأت گرفته است و هنوز کاربردهای مفیدی دارد. بخش دوم یکی از مهمترین کاربردهای عملی جبرهای بولی را که عبارت از مدل‌سازی، تجزیه و تحلیل و ساده‌سازی انتقالات یا تقویت کننده مدارها است را ارائه می‌کند.

منطق گزاره‌ها

اگر p و q گزاره باشند (همانطور که در پیوست **الف** تعریف شده است)، آنگاه گزاره " p یا q " با $p \vee q$ و گزاره " p و q " با $p \wedge q$ نشان داده می‌شود. نفی گزاره p با p' نمایش داده می‌شود. درستی یا نادرستی چنین گزاره‌های مرکبی به درستی یا نادرستی مولفه‌های p و q بستگی دارد. نمودارهای زیر (که **جداول ارزش** نامیده می‌شود) قواعد اساسی منطق را که در پیوست **الف** مورد بحث واقع شده است به طور خلاصه بیان می‌کند:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

p	p'
T	F
F	T

برای مثال نمودار اول نشان می‌دهد که " p و q " وقتی p و q هر دو درست باشند درست است و در غیر این صورت نادرست است.

گیریم p_1، p_2، ...، p_n گزاره باشند. دوگزارهٔ مرکب که با استفاده از p_iها، $\vee$، $\wedge$، $'$ و پرانتزها ساخته شده است **هم‌ارز** نامیده می‌شوند اگر ارزش راستی آن‌ها برای هر ترکیب ممکن از ارزشهای راستی p_1، p_2، ...، p_n یکسان باشد.

مثال ۲۰.۱۴. گزاره $p \wedge (q \vee r)$ هم‌ارز با گزاره $(p \wedge q) \vee (p \wedge r)$ است. برای اثبات این مطلب باید ارزش راستی هرگزاره را برای هرگزینه ممکن از ارزشهای راستی p، q و r مشخص کنیم. برای مثال وقتی p و q درست و r نادرست باشد، آنگاه $q \vee r$ درست است و بنابراین $p \wedge (q \vee r)$ نیز درست است. همچنین وقتی p و q درست و r نادرست باشد آنگاه $p \wedge q$ درست، $p \wedge r$ نادرست و به این دلیل $(p \wedge q) \vee (p \wedge r)$ درست است. بنابراین در این حالت دوگزاره دارای ارزش راستی یکسان می‌باشند. این استدلال در سطر ۲ جدول ارزش زیر، که مشتمل بر تمام حالات ممکن ارزش راستی p، q و r می‌باشد، خلاصه شده است:

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
T	T	T	T	**T**	T	T	**T**
T	T	F	T	**T**	T	F	**T**
T	F	T	T	**T**	F	T	**T**
T	F	F	F	**F**	F	F	**F**
F	T	T	T	**F**	F	F	**F**
F	T	F	T	**F**	F	F	**F**
F	F	T	F	**F**	F	F	**F**
F	F	F	F	**F**	F	F	**F**

این دوگزاره هم‌ارزند زیرا دارای ستون‌های پر رنگ یکسان هستند.

اگر p و q گزاره‌های هم‌ارز باشند، آنها را به عنوان یک گزاره در نظر می‌گیریم و می‌نویسیم $p = q$.[۶]

۶) این مشابه با در نظرگرفتن عناصر ۱ و ۴ به عنوان یک عضو در $\mathbb{Z}_3$ است و جای [۴] = [۱] می‌نویسیم ۴ = ۱. خوانندگانی که بحث رسمی را ترجیح می‌دهند می‌توانند این مبحث را به صورت زیر بپذیرند. رابطه هم‌ارزی روی یک مجموعه از گزاره‌ها همان‌طور که در پیوست ت تعریف شده است، یک رابطه هم‌ارزی است. وقتی p و q گزاره‌های هم‌ارز

با این نمادگذاری، مثال پیش بیان می‌کند که $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$. پس قانون توزیع‌پذیری برای گزاره‌ها برقرار است، در واقع داریم:

قضیه ۱۱.۱۴. گیریم p_1، p_2، ...، p_n گزاره باشند و B مجموعه تمام گزاره‌هایی باشد که بتوان با استفاده از p_iها، $\vee$، $\wedge$، $'$، و پرانتزها ساخت[۷]. آنگاه B تحت اعمال $\vee$ و $\wedge$ یک جبر بولی است.

برهان. اگر p و q گزاره‌هایی باشند که با استفاده از p_iها، $\vee$، $\wedge$، $'$، و پرانتزها ساخته شده‌اند، آنگاه همین مطلب برای $p \vee q$ و $p \wedge q$ درست است. بنابراین $\vee$ و $\wedge$ به واقع اعمال دوتایی روی B می‌باشند.

طبق قضیه ۵.۱۴، باید تحقیق کنیم که $\vee$ و $\wedge$ در قوانین جابجایی، شرکت‌پذیری و توزیع‌پذیری صدق می‌کنند. مثال قبل نشان می‌دهد که قانون اول توزیع‌پذیری برقرار است. قوانین دیگر با استفاده از جداول ارزشی مناسب به طور مشابه ثابت می‌شوند (تمرین ۵).

مجموعه B گزاره‌های همواره نادرست را شامل است (تمرین ۱)، و هر دو گزاره اینچنین لزوماً هم‌ارزند، گیریم O گزاره‌ای در B باشد که همواره نادرست است. اگر $p \in B$، آنگاه $p \vee O$ دقیقاً وقتی درست است که p درست باشد و نادرست است وقتی که p نادرست باشد. بنابراین $p \vee O$ هم‌ارز با p است؛ یعنی، برای هر $p \in B$، $p \vee O = p$. به‌علاوه، $p \wedge p' = O$ زیرا $p \wedge p'$ همواره نادرست است (زیرا یک مؤلفه آن همیشه نادرست است). به طریق مشابه، هر دو گزاره که همیشه درست هستند هم‌ارزند. I را گزاره‌ای در B بگیرید که همواره درست است و تحقیق کنید که برای هر $p \in B$، $p \wedge I = p$ و $p \vee p' = I$. بنابراین طبق ۵.۱۴، B یک جبر بولی است. ■

جبر بولی قضیهٔ ۱۱.۱۴ مدل ریاضی مفیدی از منطق گزاره‌های مرکب که در پیوست **الف** مورد بحث قرار گرفته‌است ارائه می‌کند. این مدل، گزاره‌های شرطی را نیز شامل می‌شود. برای دیدن چرایی این مطلب، گیریم $p, q \in B$ و جدول ارزش گزاره شرطی $p \Rightarrow q$ (همان‌طور که در پیوست **الف** طبق قوانین منطق معین شده است) و جدول گزاره $p' \vee q$ را مقایسه کنید:

باشند، کلاس‌های هم‌ارزی آنها برابرند $[q] = [p]$. عبارت $p = q$ بجای $[q] = [p]$، یک مختصرنویسی مناسب است. بنابراین "گزاره‌ها" در بحث زیر در واقع کلاس‌های هم‌ارزی گزاره‌ها هستند.

۷) در یک مبحث رسمی، عناصر B کلاس‌های هم‌ارزی گزاره‌هایی که بدین صورت ساخته می‌شوند می‌باشند. اعمال روی B با $[p \vee q] = [p] \vee [q]$ و $[p \wedge q] = [p] \wedge [q]$ تعریف می‌شوند. این تعاریف بستگی به انتخاب نمایندهٔ کلاس‌ها ندارد زیرا طبق تمرین ۱۱، اگر p هم‌ارز با p^* و q هم‌ارز با q^* باشد (یعنی $[p^*] = [p]$ و $[q^*] = [q]$)، آنگاه $p \vee q$ هم‌ارز با $p^* \vee q^*$ است (یعنی، $[p^* \vee q^*] = [p \vee q]$)، و به طور مشابه برای $\wedge$ چنین است.

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

p	q	p'	$p' \vee q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

چون ستون‌های آخر یکسان هستند، می‌بینیم که $p \Rightarrow q$ هم‌ارز با گزاره $p' \vee q$ در B است. جبر بولی B شامل گزاره‌های دوشرطی نیز می‌شود [" $p \Leftrightarrow q$ " به‌معنی " $p \Rightarrow q$ و $q \Rightarrow q$ " است و بنابراین هم‌ارز با $(p' \vee q) \wedge (q' \vee p)$ است].

خواص جبرهای بولی را می‌توان بکار برد تا هم‌ارزی‌های منطقی دیگر را تحقیق کرد. برای مثال گزاره شرطی $p \Rightarrow q$ هم‌ارز عکس نقیض آن $q' \Rightarrow p'$ است زیرا

$$(q' \Rightarrow p') = (q')' \vee p' = q \vee p' = p' \vee q = (p \Rightarrow q).$$

به طور مشابه، قوانین مربوط به گزاره‌های نفی، مشتمل بر رابط‌های "و" و "یا" عیناً قوانین دمورگان می‌باشند.

$$(p \vee q)' = p' \wedge q' \quad \text{و} \quad (p \wedge q)' = p' \vee q'.$$

مدارهای انتقالی

ما از کلیدها به عنوان وسیله‌ای مکانیکی برای کنترل جریان الکتریسته در یک مدار صحبت می‌کنیم. همانگونه که در شکل طراحی شده زیر نشان داده شده است، اگر کلید **بسته** باشد جریان می‌تواند از مدار عبور کند و اگر کلید باز باشد جریان نمی‌تواند عبور کند.

کلید بسته:
جریان عبور می‌کند

کلید باز:
جریان عبور نمی‌کند

ولی بحث فوق شامل انواع زیادی از ابزارهای دو وضعیتی، مثل مغناطیس‌های دوقطبی، ترانزیستورهای الکترونیکی، شیرهای کنترل مایعات، کلیدهای تقویت‌کننده، چراغ‌های راهنما و چشم‌های الکتریکی

می‌شود. مفهوم‌هایی نظیر عبور جریان یا عدم عبور آن، زیر باربودن ـ یا نبودن، به طور مثبت مغناطیس شدن یا به طور منفی مغناطیس شدن، پتانسیل بالا ـ پتانسیل پائین، حرکت ترافیک - یا توقف آن و غیره بستگی به موضوع مورد بحث دارد.

در نمودارهای طراحی شده زیر، کلیدها معمولاً با حروف کوچک (a، b، c، . . .) نشان داده می‌شوند. دو کلید متفاوت با یک حرف نمایه‌گذاری می‌شوند اگر طوری بهم مرتبط شوند که هر دو همواره یا با هم باز یا با هم بسته باشند. علامت پریم برای کلیدهایی که به صورت مخالف مرتبط شده‌اند بکار می‌رود، بدین معنی که کلید a' باز است وقتی که کلید a بسته است و a' بسته است وقتی a باز است.

گفته می‌شود که دو کلید به طور سری (یا رشته‌ای) بهم وصل شده‌اند اگر وقتی که دو کلید بسته‌اند جریان عبور کند و وقتی حداقل یک کلید باز است جریان عبور نکند.

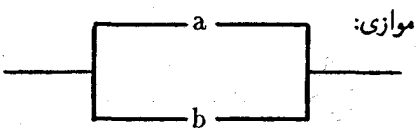
اتصال به طور سری: ——— a ——— b ———

اگر کلیدهای a و b به صورت سری بهم وصل شوند می‌نویسیم $a \cdot b$ (یا به طور ساده ab). اگر ۱ عبور جریان (کلید بسته است) و ۰ عدم آن را (کلید باز است) نشان دهد، آنگاه عبور جریان برای یک زوج کلید که به صورت سری بهم وصل شده‌اند با این جدول ارائه شده است:

a	b	a · b
0	0	0
۱	0	0
0	۱	0
۱	۱	۱

گفته می‌شود که دو کلید به طور موازی بهم وصل شده‌اند، به شرط آن که وقتی حداقل یک کلید بسته است جریان عبور کند و تنها وقتی هر دو کلید باز است جریان عبور نکند.

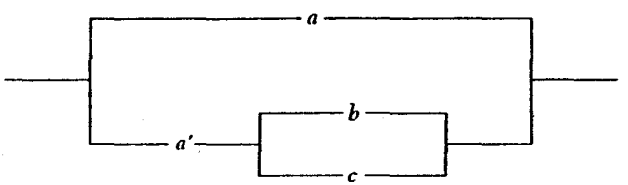
اتصال موازی:



اگر کلیدهای a و b به صورت موازی متصل باشند، می‌نویسیم $a + b$. در اینجا جدول عبور جریان برای یک زوج کلید که به صورت موازی بهم وصل شده‌اند آمده است:

a	b	a+b
0	0	0
۱	0	۱
0	۱	۱
۱	۱	۱

مثال ۲۱.۱۴. مداری که در نمودار زیر ارائه شده است به صورت جبری با $a + a'(b + c)$ نمایش داده می‌شود.

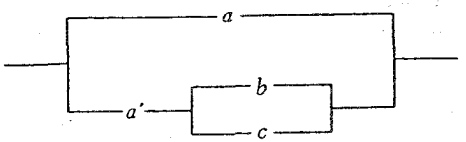


گیریم a_1، ...، a_n تعدادی کلید باشد و B مجموعه تمام مداراتی (که دو پایانه را بهم وصل می‌کند) باشد که می‌تواند از a_iها با استفاده از اتصال‌های سری و موازی و کلیدهایی که مجاز به اتصال موافق و مخالف باشند ساخته شود. مثال قبل یکی از چند مداری است که می‌تواند از کلیدهای a، b، c ساخته شود. دو مدار C و D در B هم‌ارز نامیده می‌شوند اگر برای هر انتخاب ممکن از وضعیت باز و بسته برای a_1، a_2، ...، a_n، جریان از C عبور کند اگر و تنها اگر جریان از D عبور کند. در این حالت می‌نویسیم $C = D$[۸].

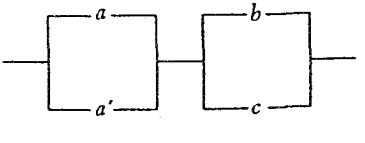
مثال ۲۲.۱۴. مدارهای شکل زیر هم‌ارز نیستند زیرا وقتی a بسته و b و c باز است جریان از مدار دست چپ عبور می‌کند، ولی از مدار دست راست عبور نمی‌کند:

---

۸) به بیان دقیق، رابطه هم‌ارزی مدارات، یک رابطه هم‌ارزی روی B است، و $C = D$ علامت اختصاری برای گزاره "کلاس هم‌ارزی C برابر با کلاس هم‌ارزی D است" می‌باشد. زیرنویس ۶ از فصل ۱۴ را ملاحظه کنید (با جایگزینی "مدار" بجای "گزاره"، + بجای ۷، و · بجای ۸).

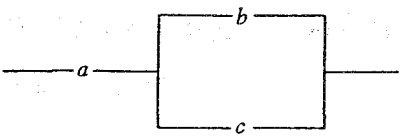


$a + a'(b + c)$

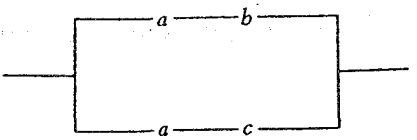


$(a + a')(b + c)$

مثال ۲۳.۱۴. این دو مدار هم‌ارزند:



$a(b + c)$



$ab + ac$

برای اثبات این حکم، باید تحقیق کنیم که جریان عبور برای هر ترکیب ممکن از حالات باز یا بسته برای a، b، c یکسان است:

a	b	c	$b+c$	$a(b+c)$	ab	ac	$ab+ac$
۰	۰	۰	۰	**۰**	۰	۰	**۰**
۰	۱	۰	۱	**۰**	۰	۰	**۰**
۰	۰	۱	۱	**۰**	۰	۰	**۰**
۰	۱	۱	۱	**۰**	۰	۰	**۰**
۱	۰	۰	۰	**۰**	۰	۰	**۰**
۱	۱	۰	۱	**۱**	۱	۰	**۱**
۱	۰	۱	۱	**۱**	۰	۱	**۱**
۱	۱	۱	۱	**۱**	۱	۱	**۱**

دو ستون پررنگ نشان می‌دهد که جریان از $a(b + c)$ عبور می‌کند اگر و فقط اگر جریان از $ab + ab$ عبور کند. بدین دلیل $a(b + c) = ab + ac$، و قانون توزیع‌پذیری برای مدارها برقرار است.

قضیه ۱۲.۱۴. گیریم a_1، a_2، ...، a_n کلیدهایی باشند و B مجموعه تمام مداراتی (که دو پایانه را بهم وصل می‌کنند) باشد که می‌تواند از a_iها با استفاده از اتصال‌های سری و موازی و کلیدهایی که

مجاز به اتصال موافق و مخالف باشند، ساخته شود. آنگاه B یک جبر بولی تحت اعمال $+$ و $\cdot$ است.

برهان. به سادگی می‌توان تحقیق کرد که $+$ و $\cdot$ اعمال دوتایی روی B می‌باشد. همچون مثال قبل، با استفاده از جدول عبور جریان، می‌توان تحقیق کرد که قوانین جابجایی، شرکت‌پذیری و توزیع‌پذیری برقرار است. مداراتی در B وجود دارند که همیشه جریان از آن عبور می‌کند (برای مثال $a + a'$، برای هر $a \in B$)، و هر دو مدار این‌چنین هم‌ارز هستند. I را مداری بگیرید که جریان همواره از آن عبور می‌کند و بررسی کنید که برای هر $a \in B$

$$a + a' = I \quad \text{و} \quad a \cdot I = a.$$

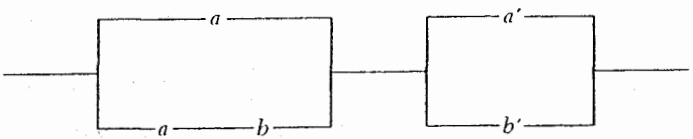
به طور مشابه، O را مداری بگیرید که جریان از آن عبور نمی‌کند و تحقیق کنید که

$$a \cdot a' = O \quad \text{و} \quad a + O = a.$$

بنابراین طبق قضیه ۵.۱۴، B یک جبر بولی (با فرض $+$ بجای $\vee$ و $\cdot$ بجای $\wedge$) می‌باشد. ■

اینک می‌توان خواص جبرهای بولی را برای ساده‌کردن انواع مدارها بکار برد.

مثال ۲۴.۱۴. برای ساده کردن مدار



آن را به صورت جبری بیان می‌کنیم و قضیه ۵.۱۴ را برای محاسبه زیر بکار می‌بریم:

$$\begin{aligned}(a + ab)(a' + b') &= a(a' + b') && \text{[قانون جذب]}\\ &= aa' + ab'\\ &= \circ + ab'\\ &= ab'\end{aligned}$$

بنابراین مدار اصلی را می‌توان با این مدار ساده‌تر هم‌ارز جایگزین کرد.

تمرینها

۱.A. گیریم p یک گزاره باشد.

(الف) یک گزاره مرکب شامل p بنویسید که همیشه نادرست باشد. [برهان قضیه ۱۱.۱۴ را ببینید.]

(ب) یک گزاره مرکب شامل p بنویسید که همیشه درست باشد.

۲. جداول راستی هر یک از این گزاره‌ها را بنویسید.

(الف) $(p \vee q) \Rightarrow q'$

(ب) $(p \wedge q') \Rightarrow (q \vee r)$

(پ) $(p \wedge q \wedge r) \Rightarrow (p \vee q) \wedge r)$

۳. یک گزاره مرکب که در هر حالت درست باشد یک **راستگو** نامیده می‌شود. از جداول راستی یا خواص جبرهای بولی استفاده کنید تا بررسی کنید که هر کدام از این گزاره‌ها یک راستگو می‌باشد.

(الف) $(p')' \iff p$

(ب) $(p \Rightarrow q)' \iff (p \wedge q')$

(پ) $((p \wedge (p \Rightarrow q)) \Rightarrow q$

(ت) $[p \Rightarrow (q \wedge r)] \iff [(p \Rightarrow q) \wedge (p \Rightarrow r)]$

(ث) $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$

۴. اگر a، b و c کلید باشند، هر یک از این مدارها را رسم کنید:

(الف) $ab + c$

(ب) $(a + b)(a + c)$

(پ) $a(b + c') + a'c$

(ت) $ac + ab' + bc(a + b')$

۵.B. با اثبات قوانین جابجایی، شرکت‌پذیری و توزیع‌پذیری برای جبر بولی گزاره‌ها، برهان قضیه ۱۱.۱۴ را تکمیل کنید.

۶. نمودار یک مدار (که دو پایانه را بهم وصل می‌کند) با کلیدهای a، b و c را رسم کنید که در شرط داده شده صدق کند:

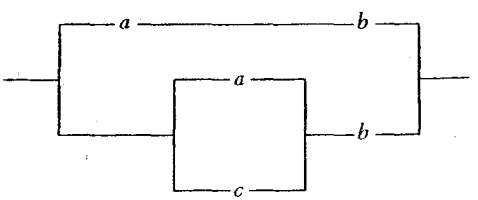
(الف) جریان از مدار عبور کند اگر و تنها اگر لااقل یکی از a، b، c بسته باشد.

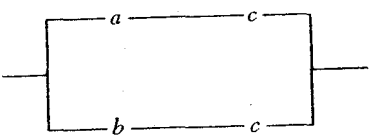
(ب) جریان از مدار عبور کند اگر و تنها اگر حداکثر یکی از a، b، c بسته باشد.

(پ) جریان از مدار عبور کند اگر و تنها اگر دقیقاً یکی از a، b، c بسته باشد.

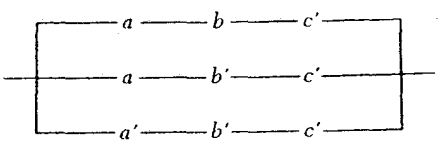
۷. آیا در هر قسمت دو مدار هم‌ارزند؟

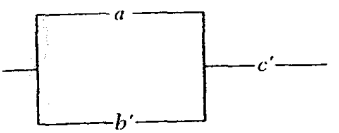
(الف)





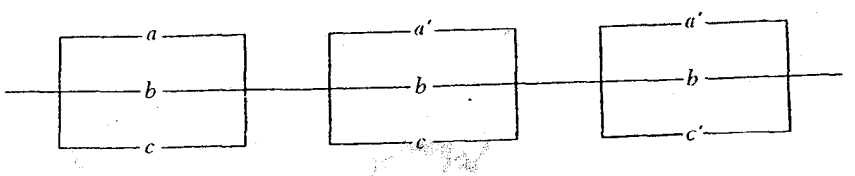
(ب)





۸. برهان قضیه ۱۲.۱۴ را تکمیل کنید.

۹. برای ساده کردن این مدار از خواص جبرهای بولی استفاده کنید؛ سپس مدار ساده شده را رسم کنید.



۱۰. گیریم p_1، ...، p_n گزاره باشند. گیریم p و p^* گزاره‌های مرکب حاصل از بکارگیری p_iها، ۷، ۸ و پرانتزها باشند، ثابت کنید که p و p^* هم‌ارزند اگر و تنها اگر گزاره $p^* \iff p$ همواره

درست باشد.

۱۱. گیریم p_1، ...، p_n گزاره باشند و p, p^*, q, q^* گزاره‌های مرکب حاصل از بکارگیری p_iها، ∨، ∧ و پرانتزها باشند. اگر p هم‌ارز p^* و q هم‌ارز q^* باشد، ثابت کنید که $p \vee q$ هم‌ارز $p^* \vee q^*$ و $p \wedge q$ هم‌ارز $p^* \wedge q^*$ است. [راهنمایی: تمرین ۱۰.]

* * * * *

فصل پانزدهم

ترسیم‌های هندسی

پیشنیازها: بخش‌های ۱.۴، ۴.۴ و ۵.۴.

از قرن ششم پیش از میلاد ریاضیدانان ترسیم‌های هندسی با چوب صاف (خط کش بی‌علامت) و پرگار را مطالعه کرده‌اند. یونانیان قدیم علیرغم مهارتشان در هندسه هرگز قادر به ایجاد بعضی از ترسیم‌ها مثل

دو برابر سازی مکعب (تضعیف مکعب): ترسیم ضلع مکعبی که حجم آن دو برابر حجم مکعب مفروض باشد.

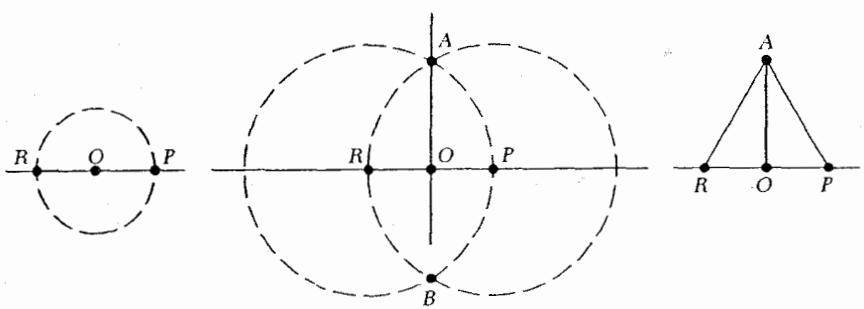
سه بخش کردن زاویه (تثلیث زاویه): ترسیم زاویه‌ای به اندازه یک سوم زاویه‌ای مفروض.

فقط با استفاده از چوب صاف و پرگار نبوده‌اند. سرانجام در قرن نوزدهم، ثابت شد که این ترسیم‌ها غیرممکن هستند. فصل حاضر برهانی مقدماتی از این مطلب را عرضه می‌کند.

این که گفته شود یک ترسیم ممکن نیست به معنی این نیست که برای مثال شما هرگز قادر به

سه‌بخش کردن یک زاویه نیستید. خیلی از زاویه‌ها، مثل ۹۰° به سادگی سه بخش شدنی توسط چوب صاف و پرگار می‌باشند (تمرین ۳). با قرار دادن حتی یک علامت روی یک چوب صاف می‌توان هر زاویه را سه بخش کرد. موضوع این است که آیا هر زاویه را می‌توان با یک خطکش بدون علامت و پرگار به سه بخش تقسیم کرد. بحث را با ارائه مثالی از یک ترسیم نمونه، با چوب صاف و پرگار آغاز می‌کنیم تا به شما احساسی از آنچه با آن سروکار داریم، بدهیم.

مثال ۱.۱۵. نقاط O و P مفروض است. از O خطی عمود بر OP به صورت زیر رسم کنید. دایره‌ای به مرکز O و شعاع OP رسم کنید. این دایره خط OP را در نقاط R و P قطع می‌کند، همان طورکه در طرف چپ شکل ۱ نشان داده شده است. قطعه خط‌های OR و OP شعاع‌های دایره هستند و بدین دلیل دارای یک اندازه می‌باشند. حال دایره‌ای به مرکز R و شعاع RP و دایره‌ای به مرکز P و شعاع RP رسم کنید. این دایره‌ها همان‌طور که در وسط شکل ۱ نشان داده شده است در نقاط A و B یکدیگر را قطع می‌کنند. قطعه خط‌های RP، RA و PA دارای یک اندازه هستند (چرا؟)



(شکل ۱)

خط AO را رسم کنید. در مثلث RAP که در طرف راست شکل ۱ نشان داده شده است، خط‌های RA و PA برابرند، همینطور OR و OP برابرند. ضلع OA با خودش برابر است. بنابراین مثلث‌های ORA و OPA به حالت سه‌ضلع برابرند. چون زاویه‌های ROA و POA مکمل و برابرند هرکدام

از آنها باید یک زاویه قائمه باشد. بنابراین خط AO بر خط OP در نقطه O عمود است.

اکنون یک توصیف رسمی ریاضی از ترسیم‌های خط‌کش و پرگار ارائه می‌کنیم. همچون مثال قبل که با دو نقطه شروع شد، گیریم S مجموعه $\{O, P\}$ باشد. خطی که توسط این دو نقطه S تعیین می‌شود را بکشید، دو دایره به مرکزهای O و P و شعاع OP رسم کنید. S_1 را مجموعه تمام نقاط تقاطع این خط و این دایره‌ها همراه با خود نقاط P و O از مجموعه S بگیرید. این فرآیند را با S_1 تکرار کنید. هر خطی که توسط زوج‌های نقاط S_1 تعیین می‌شود را رسم کنید. تمام دوایری که شعاع آنها برابر فاصله یک زوج از نقاط S_1 و مرکزش یک نقطه S_1 است را رسم کنید. S_2 را مجموعه تمام نقاط برخورد این خطوط و دوایر، همراه با نقاط S_1 بگیرید. این فرآیند را با S_2 تکرار کنید. با ادامه این روند یک دنباله

$$S \subseteq S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots$$

از مجموعه‌ها تولید می‌شود. یک نقطه **ساخت‌پذیر** نقطه‌ای است که در یکی از S_iها واقع است. یک خط **(ساخت‌پذیر)** خطی است که لااقل دو نقطه ساخت‌پذیر را شامل است. یک دایره **(ساخت‌پذیر)** دایره‌ای است که مرکزش یک نقطه ساخت‌پذیر و شعاعش برابر طول فاصله یک زوج نقاط ساخت‌پذیر باشد. برای مثال، تمام نقاط نمایه‌گذاری شده و تمام خطوط و دوایر شکل ۱ ساخت‌پذیر هستند. توجه کنید که نقاط برخورد خطوط و دوایر ساخت‌پذیر، نقاط ساخت‌پذیر هستند.

اکنون با گرفتن O به عنوان مبداء، فاصله از O تا P به عنوان طول واحد و خط OP به عنوان محور-xها، و با فرض این که P دارای مختصات $(1, 0)$ می‌باشد. صفحه را مختص‌دار می‌کنیم شکل ۱ نشان می‌دهد که محور-yها (خط AO) یک خط ساخت‌پذیراست. نقطه $(0, 1)$ ساخت‌پذیراست زیرا این نقطه تقاطع محور yها و دایره ساخت‌پذیر به مرکز O و شعاع OP می‌باشد. استدلالی مشابه نشان می‌دهد که

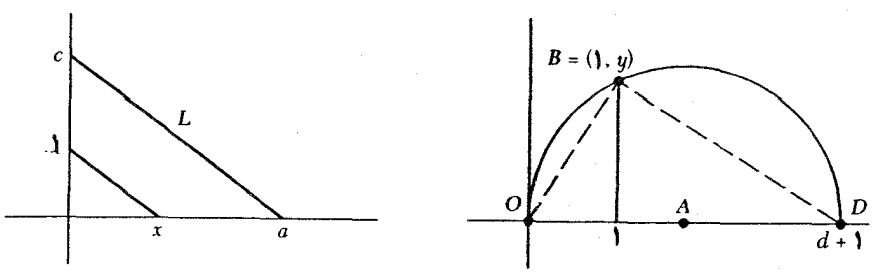
$(r, 0)$ ساخت‌پذیر است اگر و تنها اگر $(0, r)$ ساخت‌پذیر باشد.

یک عدد حقیقی r عدد **ساخت‌پذیر** نامیده می‌شود اگر نقطه $(r, 0)$ یک نقطه ساخت‌پذیر باشد. هر عدد صحیح یک عدد ساخت‌پذیراست (تمرین ۴). اگر r فاصله بین دو نقطه ساخت‌پذیر A و B باشد، آنگاه r یک عدد ساخت‌پذیر است زیرا $(r, 0)$ محل تقاطع محور ساخت‌پذیر xها و دایره ساخت‌پذیر به مرکز O و شعاع r می‌باشد. تمرین ۱۸ نشان می‌دهد که

یک نقطه ساخت‌پذیراست اگر و تنها اگر مختصاتش اعداد ساخت‌پذیر باشند.

قضیه ۱.۱۵. گیریم $a, b, , c, d$ اعداد ساخت‌پذیر باشند با شرط $c \neq 0$ و $d > 0$. آنگاه هر یک از $a+b$، $a-b$، ab، a/c و $\sqrt{d}$ یک عدد ساخت‌پذیراست.

برهان. ابتدا فرض می‌کنیم که a و c مثبت هستند و ثابت می‌کنیم که a/c یک عدد ساخت‌پذیر است. چون a و c اعداد ساخت‌پذیرند، نقاط $(a, 0)$ و $(0, c)$ ساخت‌پذیرهستند و همین‌طور خط L که توسط آنها تعیین می‌شود ساخت‌پذیراست. خطی که از نقطه ساخت‌پذیر$(0, 1)$ موازی L رسم می‌شود ساخت‌پذیر است (تمرین ۱۹). این خط محور-xها را در نقطه ساخت‌پذیر$(x, 0)$ قطع می‌کند، چنانچه در طرف چپ شکل ۲ در زیر نشان داده شده است. از این جهت x عدد ساخت‌پذیراست. از خواص مثلث‌های مشابه استفاده کنید تا نشان دهید که $1/c = x/a$ که ایجاب می‌کند $x = a/c$. تمرین ۱۳ نشان می‌دهد که وقتی $a = 0$ یا وقتی a یا c منفی باشد a/c ساخت‌پذیراست.



(شکل ۲)

اگر $b = 0$، در این صورت $ab = 0$ مسلماً ساخت‌پذیراست. اگر $b \neq 0$، آنگاه $1/b$ طبق بند قبل ساخت‌پذیراست، و از اینرو $a/(1/b) = ab$ نیز ساخت‌پذیراست. تمرین ۲ نشان می‌دهد که $a+b$ و $a-b$ ساخت‌پذیرهستند.

عدد $d+1$ طبق تمرین ۲ ساخت‌پذیراست. پس نقطه A وسط قطعه خطی که نقاط ساخت‌پذیر $(0, 0)$ و $(d+1, 0)$ را بهم وصل می‌کند ساخت‌پذیراست (تمرین ۲۰). بدین دلیل دایره به‌مرکز A و شعاع $(d+1)/2$ ساخت‌پذیر است. چنان‌که در شکل ۲ نشان داده شده است، خط ساخت‌پذیر که بر محور-xها در نقطه $(1, 0)$ عمود است این دایره را در نقطه ساخت‌پذیر$B = (1, y)$ قطع می‌کند. یک قضیهٔ هندسه مسطحه بیان می‌کند که زاویه‌ای که در یک نیمدایره محاط باشد (مثل OBD) یک زاویه قائمه است. از خواص مثلث‌های قائم‌الزاویه و قضیه فیثاغورث استفاده کنید تا ثابت کنید که

$y^۲ = d$ و بنابراین $y = \sqrt{d}$. پس نتیجه می‌شود که $y = \sqrt{۲}$ عدد ساخت‌پذیر است. ■

نتیجه ۲.۱۵. هر عدد گویا ساخت‌پذیراست.

برهان. هر عدد صحیح ساخت‌پذیراست (تمرین ۴). بنابراین طبق قضیه ۱.۱۵، هر خارج قسمت دو عدد صحیح (عدد گویا) ساخت‌پذیراست. ■

برای این‌که دقیقاً تعیین شود که کدام اعداد حقیقی ساخت‌پذیرمی‌باشند، باید معادلات خطوط و دوایر ساخت‌پذیررا بررسی کرد.

لم ۳.۱۵. گیریم $\mathbb{F}$ یک زیرمیدان از میدان اعداد حقیقی $\mathbb{R}$ باشد.

(۱) اگر خطی شامل دو نقطه باشد که مختصاتش در $\mathbb{F}$ است، آنگاه این خط معادله‌ای به صورت $ax + by + c = ۰$ دارد که در آن $a, b, c \in \mathbb{F}$.

(۲) اگر مرکز دایره‌ای نقطه‌ای باشد که مختصاتش در $\mathbb{F}$ است و شعاع دایره عددی باشد که مربعش در $\mathbb{F}$ است، آنگاه دایره معادله‌ای به صورت $x^۲ + y^۲ + rx + sy + t = ۰$ دارد که در آن $r, s, t \in \mathbb{F}$.

برهان. (۱) فرض کنید $(x_۱, y_۱)$ و $(x_۲, y_۲)$ نقاطی روی خط باشند به طوری که $x_i, y_i \in \mathbb{F}$. اگر $x_۲ \neq x_۱$، آنگاه فرمول معادله یک خط نشان می‌دهد که این خط دارای معادله زیر است:

$$y - y_۱ = \frac{y_۲ - y_۱}{x_۲ - x_۱}(x - x_۱)$$

$$\underbrace{(\frac{y_۲ - y_۱}{x_۲ - x_۱})}_{\downarrow\ ax} x \; - \; ۱y \; + \; \underbrace{[-x_۱(\frac{y_۲ - y_۱}{x_۲ - x_۱}) + y_۱)]}_{\downarrow\ c} = ۰$$

$$ax \quad + \; by \; + \quad c \quad = ۰$$

چون $\mathbb{F}$ میدان است و $x_i, y_i \in \mathbb{F}$، هر سه عدد a، b و c در $\mathbb{F}$ قراردارد. حالتی که $x_۱ = x_۲$ به خواننده واگذار می‌شود.

(۲) اگر $(x_۱, y_۱)$ مرکز و k شعاع باشد، که در آن شرط $x_۱, y_۱, k^۲ \in \mathbb{F}$، آنگاه معادله دایره

چنین است:

$$(x-x_1)^2+(y-y_1)^2=k^2$$
$$x^2+y^2+(-2x_1)x+(-2y_1)y+[x_1^2+y_1^2-k^2]=0.$$

جایی که ضرایب در $\mathbb{F}$ قرار دارند. ■

لم ۴.۱۵. گیریم $\mathbb{F}$ زیرمیدانی از $\mathbb{R}$ و k یک عضو مثبت $\mathbb{F}$ باشد به طوری که $\sqrt{k}\notin\mathbb{F}$. گیریم $\mathbb{F}(\sqrt{k})$ مجموعه $\{a+b\sqrt{k}\mid a,b\in\mathbb{F}\}$ باشد. آنگاه

(۱) $\mathbb{F}(\sqrt{k})$ زیرمیدانی از $\mathbb{R}$ است که $\mathbb{F}$ را شامل است.

(۲) هر عضو $\mathbb{F}(\sqrt{k})$ را می‌توان به طور یکتایی به صورت $a+b\sqrt{k}$ نوشت که در آن $a,b\in\mathbb{F}$.

برهان. (۱) تمرین ۱۵. (۲) اگر $a+b\sqrt{k}=a_1+b_1\sqrt{k}$، که در آن $a,b,a_1,b_1\in\mathbb{F}$، آنگاه $a-a_1=(b_1-b)\sqrt{k}$. اگر $b_1-b\neq 0$، آنگاه $\sqrt{k}=(a-a_1)(b_1-b)^{-1}$، که عضوی از $\mathbb{F}$ می‌باشد. این متناقض با این واقعیت است که $\sqrt{k}\notin\mathbb{F}$. از اینرو $b_1-b=0$ و بنابراین $a-a_1=0\sqrt{k}=0$. بدین دلیل $a=a_1$ و $b=b_1$. ■

میدان $\mathbb{F}(\sqrt{k})$ یک **توسیع درجه دوم میدان** $\mathbb{F}$ نامیده می‌شود. توسیع‌های درجه دوم نقش مهمی در تعیین این که کدام اعداد ساخت‌پذیر هستند، دارد.

لم ۵.۱۵. گیریم $\mathbb{F}$ زیرمیدانی از $\mathbb{R}$ باشد. فرض کنید L_1 و L_2 خط‌هایی باشند که معادله‌های آن‌ها دارای ضرایب در $\mathbb{F}$ است. فرض کنید C_1 و C_2 دوایری باشند که معادله‌های آن‌ها دارای ضرایب در $\mathbb{F}$ است. در این صورت

(۱) اگر L_1، L_2 را قطع کند، آنگاه مختصات نقطه برخورد آن‌ها در $\mathbb{F}$ است.

(۲) اگر C_1، C_2 را قطع کند، آنگاه مختصات نقاط برخورد در $\mathbb{F}$ یا در یک توسیع میدان درجه دوم $\mathbb{F}(\sqrt{k})$ می‌باشد.

(۳) اگر L_1، C_1 را قطع کند. آنگاه مختصات نقاط برخورد آن‌ها در $\mathbb{F}$ یا در یک توسیع میدان درجه دوم $\mathbb{F}(\sqrt{k})$ می‌باشد.

برهان. (۱) فرض کنید L_1 و L_2 دارای معادلات

$$L_1 : a_1x + b_1y = c_1$$
$$L_2 : a_2x + b_2y = c_2$$

باشند که در آن $a_i, b_i, c_i \in \mathbb{F}$. چون L_1، L_2 را قطع می‌کند این معادلات یک جواب مشترک دارند. از حل دستگاه فوق با استفاده از روش حذف یا دترمینان‌ها می‌بینیم که این جواب عبارت است از:

$$x = \frac{b_2c_1 - b_1c_2}{a_1b_2 - a_2b_1} \quad \text{و} \quad y = \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1}.$$

چون $a_i, b_i, c_i \in \mathbb{F}$ مختصات نقطه برخورد (x, y) در میدان $\mathbb{F}$ می‌باشد.

(۲) فرض کنید C_1 و C_2 دارای معادلات

$$C_1 : x^2 + y^2 + r_1x + s_1y + t_1 = 0$$
$$C_2 : x^2 + y^2 + r_2x + s_2y + t_2 = 0$$

باشند که در آن $r_i, s_i, t_i \in \mathbb{F}$. مختصات نقاط برخورد در هر دو معادله صدق می‌کند و از اینرو باید در معادله حاصل از تفریق معادله دوم از اول نیز صدق کند:

$$(r_1 - r_2)x + (s_1 - s_2)y + (t_1 - t_2) = 0.$$

این معادله یک خط است، و ضرایبش در $\mathbb{F}$ می‌باشد. چون نقاط برخورد C_1 و C_2 روی این خط و دایره C_1 قرار دارد، فقط نیاز به اثبات (۳) است تا اثبات قضیه تمام شود.

(۳) گیریم L_1 و C_1 دارای معادلات مفروض فوق باشند. لااقل یکی از a_1 یا b_1 باید ناصفر باشد، گیریم $b_1 \neq 0$. معادله L_1 را نسبت به y حل کنید و نتیجه را در معادله C_1 جایگزین کنید. تحقیق کنید که این امر منجر به یک معادله به صورت $ax^2 + bx + c = 0$ می‌شود، جایی که $a, b, c \in \mathbb{F}$. جواب‌های این معادله عبارتند از

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = A \pm B\sqrt{k},$$

است که در آن $A = -b/2a$، $B = 1/2a$، و $k = b^2 - 4ac$ عضوهای $\mathbb{F}$ هستند. چون L_1 و C_1 یکدیگر را قطع می‌کنند می‌دانیم $k \geq 0$. با استفاده از معادلهٔ L_1 می‌بینیم که مختصات نقاط

برخورد L_1 و C_1 عبارتند از:

$$x = A + B\sqrt{k} \quad \text{و} \quad y = \frac{c_1 a_1 A}{b_1} - \frac{a_1 B}{b_1}\sqrt{k}$$
$$x = A - B\sqrt{k} \quad \text{و} \quad y = \frac{c_1 a_1 A}{b_1} - \frac{a_1 B}{b_1}\sqrt{k}.$$

اگر $k = 0$، این معادلات به یک نقطه برخورد کاهش می‌یابد. چون $b_1 \neq 0$، تمام این مختصات یا در $\mathbb{F}$ قرار می‌گیرد (اگر $\sqrt{k} \in \mathbb{F}$) یا در توسیع درجه دوم $\mathbb{F}(\sqrt{k})$ قرار می‌گیرد (اگر $\sqrt{k} \notin \mathbb{F}$). ■

قضیه ۶.۱۵. اگر عدد حقیقی r ساخت‌پذیر باشد، آنگاه یک زنجیر متناهی از میدان‌ها $\mathbb{Q} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n \subseteq \mathbb{R}$ وجود دارد به طوری که $r \in \mathbb{F}_n$ و هر $\mathbb{F}_i$ یک توسیع درجه دوم از میدان ماقبل است، یعنی؛

$$\mathbb{F}_1 = \mathbb{F}_0(\sqrt{c_0}), \quad \mathbb{F}_2 = \mathbb{F}_1(\sqrt{c_1}), \quad \mathbb{F}_3 = \mathbb{F}_2(\sqrt{c_2}), \ldots, \mathbb{F}_n = \mathbb{F}_{n-1}(\sqrt{c_{n-1}}) \ ,$$

جایی که برای هر $i = 0, 1, 2, \ldots, n-1$، $c_i \in \mathbb{F}_i$ ولی $\sqrt{c_i} \notin \mathbb{F}_i$.

زنجیری متناهی از میدان‌ها، به صورتی که در قضیه آمده است را **یک زنجیر توسیع درجه دوم** می‌نامند.

برهان قضیه ۶.۱۵. گیریم r یک عدد ساخت‌پذیر باشد آنگاه نقطه $(r, 0)$ از نقاط $O = (0, 0)$ و $P = (0, 1)$ با دنباله‌ای متناهی از اعمال به صورت‌های زیر می‌تواند ترسیم شود:

(i) خط تعیین شده توسط A و B را رسم کنید، که در آن A و B نقاطی هستند که قبلاً ترسیم شده‌اند یا عضوهای $\{O, P\}$ می‌باشند:

(ii) دایره‌ای به مرکز A و شعاع فاصله B تا C که در آن A، B، C نقاطی هستند که قبلاً ترسیم شده یا عضو $\{O, P\}$ می‌باشند، بکشید؛

(iii) نقاط برخورد خطوط و دوایر تشکیل شده در (i) و (ii) را تعیین کنید.

این فرآیند از نقاط O و P که مختصاتشان در $\mathbb{Q}$ است، شروع می‌شود. طبق لم ۳.۱۵، معادله‌های خطوط یا دوایری که به وسیله آن‌ها تعیین می‌شود، دارای ضرایب گویا خواهدبود. نقاط برخورد چنین خطوط و دوایری نقاطی خواهند بود که مختصات آنها یا در $\mathbb{Q}$ است یا طبق لم ۵.۱۵ در یک توسیع درجه دوم $\mathbb{Q}(\sqrt{c_0})$ می‌باشد. خطوط و دوایر تعیین شده توسط این نقاط طبق لم ۳.۱۵ معادلاتی با ضرایب در میدان $\mathbb{F}_1 = \mathbb{Q}(\sqrt{c_0})$ خواهند داشت. مختصات نقاط برخورد این خطوط و دوایر

طبق لم ۵.۱۵ یا در $\mathbb{F}$ یا در یک توسیع درجه دوم $\mathbb{F}_1(\sqrt{c_1})$ قرار خواهد داشت. با ادامه این روند می‌بینم که در هر مرحله از ترسیم (r, s)، مختصات نقاط مورد سوال در یک میدان $\mathbb{F}_i$ و در مرحله بعد مختصات نقاط جدیداً پدیدآمده در $\mathbb{F}_i$ یا در یک توسیع درجه دوم $\mathbb{F}_i(\sqrt{c_i})$ قرار خواهد داشت. پس از تکرار تعدادی متناهی از چنین مراحلی به نقطه (r, s) می‌رسیم، که لزوماً مختصاتی در آخرین میدان زنجیر توسیع درجه دوم $\mathbb{Q} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n$ خواهد داشت. ■

دو راه برای اثبات این که بعضی اعداد حقیقی ساخت‌پذیر نیستند وجود دارد. روشی که در اینجا عرضه شد مقدماتی است و فقط به فصل ۴ بستگی دارد. ولی اگر بخش‌های ۱.۹ و ۲.۹ را خوانده‌اید، این پاورقی را ملاحظه کنید و مطالب کتاب را از بعد از قضیه ۹.۱۵ پی بگیرید. [۱].

قضیه ۷.۱۵. گیریم $\mathbb{F}$ یک زیرمیدان $\mathbb{R}$ باشد و $f(x) \in \mathbb{F}[x]$. فرض کنید $k \in \mathbb{F}$ ولی $\sqrt{k} \notin \mathbb{F}$. اگر $a + b\sqrt{k}$ یک ریشه $f(x)$ باشد، آنگاه $a - b\sqrt{k}$ نیز یک ریشه $f(x)$ است.

برهان. اگر $u = r + s\sqrt{k} \in \mathbb{F}(\sqrt{k})$، گیریم $\bar{u}$، $r - s\sqrt{k}$ را نشان دهد. این عمل خوش‌تعریف است زیرا طبق لم ۴.۱۵، هر عضو $\mathbb{F}(\sqrt{k})$ را می‌توان به طور یکتا به صورت $r + s\sqrt{k}$ نوشت $(r, s \in \mathbb{F})$. تحقیق کنید که برای هر $u, v \in \mathbb{F}(\sqrt{k})$، $\overline{(u+v)} = \bar{u} + \bar{v}$ و $\overline{uv} = \bar{u} \cdot \bar{v}$. همچنین توجه داشته باشید که $u = \bar{u}$ اگر و تنها اگر $s = 0$، یعنی اگر و تنها اگر $u \in \mathbb{F}$. بقیه برهان، با برهان لم ۲۴.۴، که حالت خاص $\mathbb{F} = \mathbb{R}$، $k = -1$ و $\sqrt{k} = i$ است، یکی است. ■

قضیه ۸.۱۵. گیریم $\mathbb{F}$ زیرمیدانی از یک میدان $\mathbb{K}$ باشد. گیریم $f(x), g(x) \in \mathbb{F}[x]$ و $h(x) \in \mathbb{K}[x]$. اگر $f(x) = g(x)h(x)$، آنگاه $h(x)$ نیز در $\mathbb{F}[x]$ است.

برهان. طبق قانون تقسیم در $\mathbb{F}[x]$، چندجمله‌ایهای $k(x)$ و $r(x)$ در $\mathbb{F}[x]$ وجود دارند که $f(x) = g(x)k(x) + r(x)$، که در آن $r(x) = 0$ یا $\deg r(x) < \deg g(x)$. چون $\mathbb{F} \subseteq \mathbb{K}$،

---

۱) اگر $k \in \mathbb{F}$ و $\sqrt{k} \notin \mathbb{F}$، آنگاه $x^2 - k \in \mathbb{F}[x]$ چندجمله‌ای مینیمال $\sqrt{k}$ روی $\mathbb{F}$ است و بنابراین طبق قضیه ۷.۹، $[\mathbb{F}(\sqrt{k}) : \mathbb{F}] = 2$. اگر $\mathbb{Q} \subseteq \cdots \subseteq \mathbb{F}_n$ یک زنجیر توسیع درجه دوم باشد، آنگاه $[\mathbb{F}_n : \mathbb{Q}]$ باید طبق قضیه ۴.۹ توانی از ۲ باشد. بنابراین چندجمله‌ای مینیمال یک عدد ساخت‌پذیر u دارای درجه 2^k برای برخی k است (چون این درجه برابر بعد $[\mathbb{Q}(u) : \mathbb{Q}]$ است که باید $[\mathbb{F}_n : \mathbb{Q}]$ را بشمارد). در نتیجه هیچ عدد ساخت‌پذیرنمی‌تواند ریشه یک چندجمله‌ای درجه سوم تحویل‌ناپذیر در $\mathbb{Q}[x]$ باشد. چون یک چندجمله‌ای درجه سوم که ریشه گویا نداشته باشد طبق نتیجه ۱۴.۴ تحویل‌ناپذیر است، هیچ چندجمله‌ای این چنین دارای عددی ساخت‌پذیر به‌عنوان ریشه نیست.

تمام این چندجمله‌ایها در $\mathbb{K}[x]$ هستند. اکنون قانون تقسیم را در $\mathbb{K}[x]$ در نظر بگیرید، که اظهار می‌کند یک خارج قسمت و باقیمانده یکتا وجود دارد. داریم $f(x) = g(x)k(x) + r(x)$، و طبق فرض نیز داریم $f(x) = g(x)h(x) + ۰$. طبق یکتایی باید داشته باشیم $r(x) = ۰$ و $h(x) = k(x)$. چون $k(x) \in \mathbb{F}[x]$، لم ثابت شده است. ■

قضیه ۹.۱۵. گیریم $f(x)$ یک چندجمله‌ای درجه سوم در $\mathbb{Q}[x]$ باشد. اگر $f(x)$ دارای ریشه در $\mathbb{Q}$ نباشد، آنگاه $f(x)$ دارای ریشه ساخت‌پذیر نیست.

از این قضیه، برای مثال، نتیجه می‌شود که $\sqrt[۳]{۲}$ یک عدد ساخت‌پذیر نیست زیرا ریشه $x^۳ - ۲$ است، که طبق آزمون ریشه گویا (قضیه ۱۶.۴) دارای ریشه ساخت‌پذیر نیست.

برهان قضیه ۹.۱۵. به خلاف، فرض کنید که $f(x)$ دارای ریشه‌های حقیقی باشد که ساخت‌پذیر هستند، هر یک از این ریشه‌ها بنابر قضیه ۶.۱۵ در یک زنجیر توسیع درجه دوم $\mathbb{Q}$ قرار دارد. در بین تمام زنجیرهای توسیع درجه دوم یک ریشه $f(x)$، یکی که کمترین طول ممکن را دارد مثلاً $\mathbb{Q} = \mathbb{F}_۰ \subseteq \mathbb{F}_۱ \subseteq \cdots \subseteq \mathbb{F}_n$ را انتخاب کنید. بنابراین $f(x)$ دارای یک ریشه r در $\mathbb{F}_n$ است و هیچ زنجیر توسیع درجه دوم به طول $n - ۱$ یا کمتر دارای یک ریشه $f(x)$ نیست. توجه کنید که چون $f(x)$ دارای هیچ ریشه گویا نیست، $\mathbb{F}_n \neq \mathbb{Q}$. طبق قضیه عامل ۱۲.۴، $f(x) = (x - r)t(x)$ برای برخی $t(x) \in \mathbb{F}_n[x]$. اکنون $r \in \mathbb{F}_n$ و طبق تعریف یک زنجیر توسیع درجه دوم داریم، $\mathbb{F}_n = \mathbb{F}_{n-۱}(\sqrt{k})$ برای برخی $k \in \mathbb{F}_{n-۱}$ با $\sqrt{k} \notin \mathbb{F}_{n-۱}$. بنابراین $r = a + b\sqrt{k}$ که در آن $a, b \in \mathbb{F}_{n-۱}$. باید داشته باشیم $b \neq ۰$، زیرا در غیر این صورت r در زنجیر $\mathbb{F}_{n-۱} \subseteq \cdots \subseteq \mathbb{F}_۰$ خواهد بود، که متناقض با این واقعیت است که $f(x)$ در یک زنجیر به طول $n - ۱$ دارای ریشه نیست. طبق لم ۷.۱۵، $\bar{r} = a - b\sqrt{k}$ نیز یک ریشه $f(x) = (x - r)t(x)$ است. چون $\bar{r} \neq r$ (زیرا $b \neq ۰$)، $\bar{r}$ باید یک ریشه $t(x)$ باشد. طبق قضیه عامل $f(x) = (x - r)(x - \bar{r})h(x)$ برای یک $h(x) \in \mathbb{F}_n[x]$. فرض کنید $g(x) = (x - r)(x - \bar{r})$ و مشاهده کنید که ضرایب $g(x)$ در $\mathbb{F}_{n-۱}$ هستند:

$$g(x) = (x - (a + b\sqrt{k}))(x - (a - b\sqrt{k})) = x^۲ - ۲ax + (a^۲ - kb^۲).$$

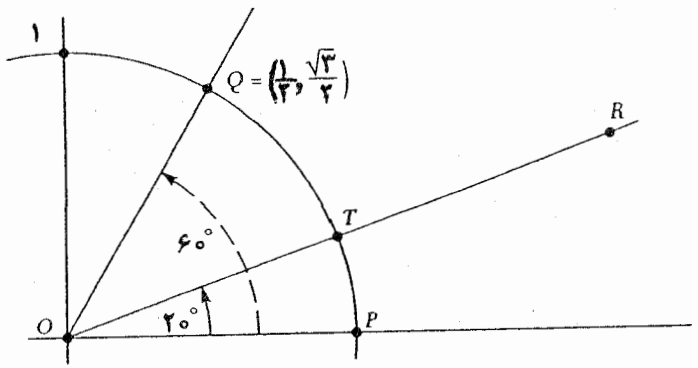
بنابراین $f(x) = g(x)h(x)$ که در آن $f(x), g(x) \in \mathbb{F}_{n-۱}[x]$. در نتیجه طبق لم ۸.۱۵، $h(x) \in \mathbb{F}_{n-۱}[x]$. حال $f(x)$ دارای درجه ۳ و $g(x)$ دارای درجه ۲ است، بنابراین طبق قضیه

۱.۴، $h(x)$ دارای درجه ۱ است. چون هرچندجمله‌ای درجه یک روی یک میدان دارای یک ریشه در همان میدان است، $h(x)$ و بدین دلیل $f(x)$ دارای یک ریشه در $\mathbb{F}_{n-1}$ است. این متناقض با انتخاب $\mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n$ به عنوان یک زنجیر توسیع درجه دوم متناهی به طول مینیمم که یک ریشه $f(x)$ را شامل است، می‌باشد. بنابراین $f(x)$ دارای هیچ ریشه ساخت‌پذیر نیست. ■

سرانجام، ما در جایگاهی هستیم که عدم امکان ترسیم‌هایی که در ابتدای فصل مورد بحث قرار دادیم را ثابت کنیم. از اینجا به بعد، فرض بر این است که وقتی یک نقطه، خط، شعاع، و غیر آن را به دلخواه بتوان انتخاب کرد، این نقطه، خط، شعاع و غیر آن را ساخت‌پذیر انتخاب کنیم. این کار تضمین می‌کند که همه نقاط، خطوط و غیر آن که در فرآیند ساختار ظاهر می‌شوند هرکدام ساخت‌پذیر باشند.

تضعیف مکعب. نقاط انتهایی یک ضلع یک مکعب مفروض را با O و P نمایه‌گذاری کنید و ضلع OP را به عنوان واحد اندازه برای مختص‌گذاری صفحه استفاده کنید. چون مکعب مفروض دارای ضلع ۱ است، حجم آن نیز ۱ است. اگر راهی برای ترسیم ضلع مکعبی به حجم ۲ با خطکش و پرگار بود، آنگاه طول c این ضلع عددی ساخت‌پذیر است به طوری که $c^3 = 2$. پس c یک ریشه $x^3 - 2$ است. ولی طبق آزمون ریشه گویا این چندجمله‌ای دارای ریشه گویا نیست، و بدین دلیل طبق قضیه ۹.۱۵، هیچ ریشه ساخت‌پذیرندارد. این تناقض نشان می‌دهد که دوبرابرسازی مکعب با خطکش و پرگار ممکن نیست.

تثلیث زاویه. کافی است ثابت کنیم یک زاویه 60° نمی‌تواند به وسیله خطکش و پرگار به سه قسمت مساوی تقسیم شود. دو نقطه O و P را انتخاب کنید و صفحه را با O به عنوان مبداء و $P = (1, 0)$ مختص‌گذاری کنید. نقطه $Q = (1/2, \sqrt{3}/2)$ ساخت‌پذیر است زیرا مختصات آن طبق قضیه ۱.۱۵ و نتیجه ۲.۱۵، ساخت‌پذیرند. به‌علاوه Q روی دایره یکه $x^2 + y^2 = 1$ قرار دارد. بنابراین کسینوس زاویه POQ برابر $\frac{1}{2}$ است (مختص اول Q) و بنابراین اندازه این زاویه 60° است. اگر تثلیث زاویه با خطکش و پرگار ممکن باشد، یک دنباله متناهی از نقاط ساخت‌پذیر وجود خواهد داشت که به یک نقطه ساخت‌پذیر R منتهی می‌شود به طوری که اندازه زاویه ROP برابر 20° است، همان‌طورکه در شکل ۳ نشان داده شده است.



(شکل ۳)

چون نقطه T نقطه برخورد خط ساخت‌پذیر OR با دایره واحد است یک نقطه ساخت‌پذیراست. از اینرو مختص اول آن که $\cos ۲۰^\circ$ است یک عدد ساخت‌پذیر است. بنابراین طبق قضیه ۱.۱۵، $۲\cos ۲۰^\circ$ یک عدد ساخت‌پذیر است. ولی برای هر زاویه t درجه، مثلثات مقدماتی (تمرین ۵) نشان می‌دهد که

$$\cos ۳t = ۴\cos^۳ t - ۳\cos t.$$

اگر $t = ۲۰^\circ$، آنگاه این اتحاد به صورت زیر در می‌آید:

$$\cos ۶۰^\circ = ۴\cos^۳ ۲۰^\circ - ۳\cos ۲۰^\circ$$

$$\frac{۱}{۲} = ۴\cos^۳ ۲۰^\circ - ۳\cos ۲۰^\circ.$$

از ضرب در ۲ و مرتب‌کردن مجدد، خواهیم داشت:

$$(۲\cos ۲۰^\circ)^۳ - ۳(۲\cos ۲۰^\circ) - ۱ = ۰.$$

بنابراین عدد ساخت‌پذیر مفروض $۲\cos ۲۰^\circ$ یک ریشه $x^۳ - ۳x - ۱$ می‌باشد. آزمون ریشه گویا نشان می‌دهد که این چندجمله‌ای ریشه گویا ندارد، و لذا طبق قضیه ۹.۱۵، ریشه ساخت‌پذیرندارد. این یک تناقض است. بنابراین زاویه ۶۰° قابل تثلیث به وسیله خط‌کش و پرگار نیست.

تمرینها

A.۱. ثابت کنید r یک عدد ساخت‌پذیراست اگر و تنها اگر $-r$ ساخت‌پذیر باشد.

۲. گیریم a و b اعداد ساخت‌پذیر باشند. ثابت کنید $a+b$ و $a-b$ ساخت‌پذیر می‌باشند.

۳. از خط‌کش و پرگار استفاده کنید تا هر یک از زاویه‌های زیر را بسازید:

(الف) ۳۰° (ب) ۴۵°

(پ) ثابت کنید که زاویه ۹۰° و زاویه ۴۵° را می‌توان با خط‌کش و پرگار تثلیث کرد.

۴. ثابت کنید که هر عدد صحیح یک عدد ساخت‌پذیراست. [راهنمایی: ۱ ساخت‌پذیر است (چرا؟) دایره‌ای به مرکز $(۱,۰)$ و شعاع ۱ رسم کنید تا ثابت کنید ۲ ساخت‌پذیراست.]

۵. ثابت کنید $\cos ۳t = ۴\cos^۳ t - ۳\cos t$. [راهنمایی: این اتحادها می‌تواند مفید باشد:

(۱) $\cos(t_۱ + t_۲) = \cos t_۱ \cos t_۲ - \sin t_۱ \sin t_۲$ ؛

(۲) $\cos ۲t = ۲\cos^۲ t - ۱$ و $\sin ۲t = ۲\sin t \cos t$ ؛

(۳) $\sin^۲ t + \cos^۲ t = ۱$.]

۶. اگر $\cos ۳t = ۱$، آیا ممکن است زاویه $۳t$ درجه را تثلیث کرد؟ اگر $\cos ۳t = ۱۱/۱۶$ باشد چه می‌شود؟

B.۷. جعبه‌ای مکعب مستطیل شکل که قاعده‌اش مربعی به ضلع x و ارتفاعش y است در نظر بگیرید. فرض کنید حجم این جعبه ۳ واحد مکعب و سطح آن ۷ واحد مربع باشد. آیا می‌توان اضلاع این جعبه را با خط‌کش و پرگار ترسیم کرد؟

۸. از قطعه خط واحد شروع نموده، با استفاده از خط‌کش و پرگار پاره‌خطی به طول $۱ + \sqrt{۳}$ ترسیم کنید.

۹. آیا ممکن است با خط‌کش و پرگار یک مثلث متساوی‌الساقین به محیط ۸ و مساحت واحد رسم نمود؟

۱۰. (الف) ثابت کنید که مجموع دو زاویه ساخت‌پذیر، ساخت‌پذیر است. [یک زاویه ساخت‌پذیر زاویه‌ای است که ضلع‌هایش خطوط ساخت‌پذیر باشد.]

(ب) از قطعه خط واحد شروع نموده، ثابت کنید که ممکن نیست یک زاویه 1° با خط‌کش و پرگار ترسیم نمود. [راهنمایی: اگر این کار ممکن بود، در مورد زاویهٔ 20° چه می‌توان گفت؟]

۱۱. ثابت کنید که زاویهٔ t درجه ساخت‌پذیراست اگر و تنها اگر $\cos t$ عددی ساخت‌پذیر باشد.

۱۲. ثابت کنید که r عددی ساخت‌پذیراست اگر و تنها اگر یک قطعه خط به طول $|r|$ را بتوان با خط کش و پرگار، با شروع از قطعه‌ای به طول واحد، ترسیم کرد.

۱۳. گیریم a و c اعداد ساخت‌پذیر باشند و $c \neq 0$. ثابت کنید که a/c ساخت‌پذیراست. [حالتی که $a > 0$، $c > 0$ در برهان قضیه ۱.۱۵ انجام شده است.]

۱۴. ثابت کنید که مجموعه تمام اعداد ساخت‌پذیر یک میدان است.

۱۵. گیریم $\mathbb{F}$ یک زیرمیدان $\mathbb{R}$ باشد و $k \in \mathbb{F}$. ثابت کنید که $\mathbb{F}(\sqrt{k}) = \{a+b\sqrt{k} \mid a, b \in \mathbb{F}\}$ زیرمیدانی از $\mathbb{C}$ است که $\mathbb{F}$ را شامل است. اگر $k > 0$، ثابت کنید که $\mathbb{F}(\sqrt{k})$ یک زیرمیدان $\mathbb{R}$ است. [راهنمایی: با راهنمایی تمرین ۲۸ در بخش ۱.۳ تطبیق کنید.]

۱۶. عکس قضیه ۶.۱۵ را ثابت کنید: اگر r در یک زنجیر توسیع درجه دوم باشد، آنگاه r یک عدد ساخت‌پذیر است. [راهنمایی: قضیه ۱.۱۵ و نتیجه ۲.۱۵.]

۱۷. گیریم C یک نقطه ساخت‌پذیر و L یک خط ساخت‌پذیر باشد. ثابت کنید که خطی که از C بر L عمود است ساخت‌پذیراست. [راهنمایی: حالتی که C روی خط L است در مثال ۱.۱۵ انجام شد. اگر C روی L نباشد و D یک نقطه ساخت‌پذیر روی L باشد، دایره به مرکز C و شعاع CD ساخت‌پذیر است و خط L را در نقاط ساخت‌پذیر D و E قطع می‌کند. دوایر به مرکز D و شعاع CD، و به مرکز E و شعاع CE در نقاط ساخت‌پذیر C و Q یکدیگر را قطع می‌کنند. ثابت کنید که خط CQ بر L عمود است.]

۱۸. ثابت کنید که (r, s) یک نقطه ساخت‌پذیراست اگر و فقط اگر r و s اعداد ساخت‌پذیر باشند. [راهنمایی: طبق تمرین ۱۷ خطوط قائم بر محورهای مختصات از نقطه (r, s) ساخت‌پذیرهستند.]

۱۹. گیریم A یک نقطه ساخت‌پذیر باشد که روی خط ساخت‌پذیر L نیست. ثابت کنید که خطی که به موازات L از A بگذرد ساخت‌پذیراست. [راهنمایی: از تمرین ۱۷ استفاده کنید تا یک خط ساخت‌پذیر M که از A می‌گذرد و قائم بر L است پیدا کنید. آنگاه یک خط که از A

می‌گذرد و بر M عمود است ترسیم کنید.]

۲۰. ثابت کنید که نقطه میانی پاره‌خط بین دو نقطه ساخت‌پذیر یک نقطه ساخت‌پذیر است. [راهنمایی: با راهنمایی تمرین ۱۷ تطبیق کنید.]

۲۱.C مربع کردن دایره. دایره‌ای به شعاع r مفروض است، ثابت کنید که غیرممکن است که با خط‌کش و پرگار ضلع مربعی که مساحتش برابر مساحت دایره مفروض است را رسم کرد. می‌توانید این واقعیت نابدیهی که π ریشه هیچ چند جمله‌ای غیرصفر در $\mathbb{Q}[x]$ نیست را پذیرفته قلمداد کنید.

* * * * *

فصل شانزدهم

نظریه کدگذاری جبری

پیشنیازها: بخش ۴.۷ و پیوست ج برای بخش ۱.۱۶، بخش ۸.۷ (تا قضیهٔ لاگرانژ) برای بخش ۲.۱۶، بخش ۶.۹ برای بخش ۳.۱۶.

نظریه کدگذاری با انتقال سریع و دقیق پیامها روی یک "کانال" الکترونیک (تلفن، تلگراف، رادیو، تلویزیون، ماهواره، کامپیوتر و مانند آن) که در معرض "پارازیت" (شرایط جوی، تداخل امواج حاصل از وسایل الکترونیک نزدیک، تجهیزات و مانند آن) است سروکار دارد. این پارازیت، ممکن است موجب خطاهایی شود که پیام‌های رسیده درست همان پیام ارسال شده نباشد. هدف نظریه کدگذاری آن است که گیرنده را به کشف چنین خطاهایی قادر ساخته و در صورت امکان آنها را اصلاح کند[1].

ریچارد هامینگ[2] که نامش به دفعات در این فصل ظاهر می‌شود پیشگام استفاده از جبر مجرد

---

۱) بنابراین نظریه کدگذاری اساساً هیچ ارتباطی با کدهای محرمانه که در فصل ۱۲ بحث شد ندارد. در فصل ۱۲، هدف مخفی کردن پیام بود، در صورتی که در اینجا منظور تضمین شفافیت آن است.

۲) Richard W. Hamming

برای حل مسائل کدگذاری می‌باشد. در سال ۱۹۵۰ او به بسط رده بزرگی از کدهای اصلاح ـ خطا که بعضی از آنها در اینجا عرضه شده‌اند، اقدام کرد.

۱-۱۶ کدهای خطی

پیام‌های شفاهی معمولاً برای انتقال الکترونیک به صورت عددی تبدیل می‌شوند. وقتی از رایانه‌ها استفاده شود، این امر معمولاً به وسیله یک کد دوتایی انجام می‌گیرد، که در آن پیام‌ها به صورت رشته‌هایی از ۰ و ۱ بیان می‌گردد. چنین پیام‌هایی به سادگی بکار می‌روند زیرا واحدهای پردازش داخلی بیشتر کامپیوترها، حروف، اعداد و نمادها را بدین طریق نمایش می‌دهند. موضوع مورد بحث در اینجا فقط با چنین کدهای دوتایی سروکار دارد [۳].

در سراسر این فصل، فرض می‌کنیم که یک **کانال دوتایی متقارن** داشته باشیم بدین معنا که:

۱. احتمال این که ۰ به اشتباه بجای ۱ دریافت شود برابر است با احتمال این که ۱ به اشتباه بجای ۰ دریافت شود؛

۲. احتمال خطای انتقال در یک تک رقم تنها کمتر از ۰/۵ است؛ و

۳. خطاهای انتقالی چندگانه مستقلاً پیش می‌آید.[۴]

در اینجا مثال ساده‌ای آمده است که گوشه‌ای از این موضوع را عرضه می‌کند.

مثال ۱.۱۶. فرض کنید پیامی که باید فرستاده شود یک تک رقم، ۰ یا ۱ باشد. این پیام می‌تواند برای مثال، علامتی باشد که به یک ماهواره بگوید که آیا دور یک سیاره در فواصل دور گردش کند یا نه. با یک پیام تک رقمی، گیرنده راهی برای این که بگوید آیا خطایی اتفاق افتاده است ندارد. ولی اگر بجای آن یک پیام چهاررقمی ارسال شود: ۱۱۱۱ برای ۱ یا ۰۰۰۰ برای ۰، آنگاه این کد می‌تواند خطاهای یگانه (تک خطا) را اصلاح کند. برای مثال، اگر ۱۱۰۱ دریافت شده باشد، آنگاه محتمل است که خطایی یگانه صورت گرفته باشد و پیام صحیح ۱۱۱۱ باشد. البته ممکن است سه خطا صورت گرفته باشد و پیام صحیح ۰۰۰۰ باشد، ولی این احتمال بسیار کمتر از یک خطای یگانه

۳) "دوتایی" به این واقعیت برمی‌گردد که این کدها در مبنای $\mathbb{Z}_2$ می‌باشند. اگرچه کدهای دوتایی متداول‌ترین کدها هستند، کدهای دیگری نیز می‌تواند با استفاده از هر میدان متناهی بجای $\mathbb{Z}_2$ ساخته شود.

۴) میزان دقت انتقال پیام بستگی به این احتمالات دارد. چون احتمال مقدماتی از پیشنیازهای این کتاب نمی‌باشد، بحث پیرامون چنین مسائلی را به حداقل می‌رسانیم، تمرین‌های ۳۱ـ۲۷ را ملاحظه کنید.

می‌باشد[۵]. این کد می‌تواند خطاهای دوگانه را کشف کند ولی نمی‌تواند آنها را اصلاح کند. برای مثال اگر ۱۱۰۰ دریافت شود، آنگاه احتمال وقوع دو خطا وجود دارد، ولی پیام مورد نظر روشن نیست.

این مثال به صورت ساده‌ای مؤلفه‌های اصلی نظریه کدگذاری را شرح می‌دهد. کلمات عددی پیام (۰,۱) به صورت کلمه کدها (۰۰۰۰ و ۱۱۱۱) ترجمه شده‌اند. گرچه که فقط کلمه کدها منتقل شده‌اند، ولی در این مثال هر رشته چهارقمی از ۰ و ۱ها می‌تواند یک کلمه احتمالی دریافت شده‌باشد. از مقایسه کلمات رسیده با کلمات کد و تصمیم‌گیری در مورد بیشترین خطای ممکن، یک کدگشا خطاها را کشف و در صورت امکان آنها را اصلاح می‌کند[۶]. بالاخره، کلمه کدهای اصلاح‌شده به کلمه‌های پیام برگردانده می‌شوند و یا برای کلمه‌های رسیده که قابل اصلاح نیستند یک خطا اعلام می‌شود.

هر نوع روش انتساب یک کلمه پیام به یک کلمه کد منحصربفرد را می‌توان برای ترجمه فی‌مابین پیام‌ها و کلمه کدها بکار برد. اگر تصمیم گرفته‌بودیم، برای مثال، که ۱۱۱۱ کلمه کد برای ۰ و ۰۰۰۰ کلمه کد برای ۱ باشد، فرآیند کشف و تصحیح خطاهای انتقالی عیناً مثل قبل می‌بود زیرا این فرایند فقط به کلمه کدها بستگی دارد و نه به این که آنها چه معنی دارند. از دیدگاه انتقال و کدگشایی، این عیناً همان کد قبلی است اگرچه کلمه کدها معانی مختلف دارند.

با ملاحظه مثال قبل از دیدگاهی دیگر، می‌توانیم به بسط و توسعه تعریفی قابل استفاده از "کد" در حالت کلی بپردازیم. اگر کلمه‌های پیام ۰ و ۱ را به عنوان عناصری از $\mathbb{Z}_2$ در نظر بگیریم آنگاه کلمات رسیده را می‌توانیم با قراردادن مثلاً (۱,۰,۱,۱) به جای ۱۰۱۱ و (۰,۰,۰,۰) به جای ۰۰۰۰، به عنوان عناصری از گروه جمعی $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ در نظر بگیریم. در این گروه عمل جمع، مولفه به مولفه صورت می‌گیرد و برای مثال ۰۰۰۱ = ۱۰۱۱ + ۱۰۱۰ (بخاطر آورید که در $\mathbb{Z}_2$، ۰ = ۱ + ۱). مجموعه کلمه کدهای $C = \{0000, 1111\}$ تحت جمع بسته است، بنابراین طبق قضیه ۸.۷، زیرگروهی از $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ است.

برای هر عدد صحیح مثبت n، ضرب دکارتی $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ از n نسخهٔ $\mathbb{Z}_2$ را با $B(n)$ نشان می‌دهیم. با جمع مولفه به مولفه، $B(n)$ یک گروه جمعی از مرتبه 2^n می‌باشد (تمرین ۱۵). عناصر $B(n)$ به صورت رشته‌هایی از ۰ و ۱ به طول n نوشته می‌شوند. اگر $0 < k < n$، آنگاه یک **(n, k) کد خطی دوتایی** عبارت از یک زیرگروه C از $B(n)$ از مرتبه 2^k است. برای

---

۵) اگر احتمال دریافت یک رقم اشتباه ۰٫۰۱ باشد، آنگاه وقوع سه یا چهار خطا در یک کلمه کمتر از ۰٫۰۰۰۴% بارخواهد بود (یعنی یکبار خطا در هر ۲۵۰۰۰۰ انتقال پیام)؛ تمرین ۲۷ را ملاحظه کنید.

۶) این موضوع بعضی وقتها **کدگشایی احتمال ـ ماکسیمم** نامیده می‌شود.

راحتی، اغلب C را یک (n,k) کد، یک کد خطی یا فقط یک کد می‌نامند[۷]. **عناصر C را کلمه کدها** نامگذاری کرده‌اند. تنها کلمه‌های کد هستند که انتقال می‌یابند، ولی هر یک از عناصر $B(n)$ می‌تواند یک **کلمه دریافت شده** باشد.

در مثال قبل $C = \{۰۰۰۰, ۱۱۱۱\}$ یک $(۴,۱)$ کد است زیرا C زیرگروهی از مرتبه ۲ از گروه $B(۴) = \mathbb{Z}_۲ \times \mathbb{Z}_۲ \times \mathbb{Z}_۲ \times \mathbb{Z}_۲$ از مرتبه $۲^۴$ است. در این حالت مجموعه کلمه‌های پیام درست برابر $\mathbb{Z}_۲$ است. به طریق مشابه وقتی با یک (n,k) کد دلخواه سروکار داریم گروه $B(k) = \mathbb{Z}_۲ \times \mathbb{Z}_۲ \times \cdots \times \mathbb{Z}_۲$ (k نسخهٔ $\mathbb{Z}_۲$) که دارای مرتبه ۲^k است را، به عنوان مجموعه کلمه‌های پیام درنظر می‌گیریم.

مثال ۲.۱۶. در $(۶,۵)$ **کد توازن سنج**، کلمه پیام‌ها عناصر $B(۵)$، یعنی تمام رشته‌های ۵-رقمی از ۰ و ۱ می‌باشند. کلمه پیام‌ها را با اضافه کردن یک رقم اضافی در انتهای رشته به کلمه کدها (عناصر $B(۶)$) تبدیل می‌کنیم؛ این رقم اضافی از مجموع ارقام کلمه پیام (در $\mathbb{Z}_۲$) بدست می‌آید. برای مثال، $۱۱۰۱۱۰ \in B(۶)$ کلمه کد برای ۱۱۰۱۱ است زیرا در $\mathbb{Z}_۲$، $۰ = ۱+۱+۰+۱+۱$. به طور مشابه، $۱۰۱۰۱ \in B(۵)$ به کلمه کد $۱۰۱۰۱۱ \in B(۶)$ تبدیل می‌شود.

یک عضو $B(۶)$ یک کلمه کد است اگر و تنها اگر مجموع ارقامش صفر باشد. [دلیل: اگر مجموع ارقام کلمه پیام ۰ باشد، یک صفر اضافه می‌شود تا کلمه کد ساخته شود. اگر مجموع ارقام کلمه پیام یک شود یک، ۱ به کلمه کد اضافه می‌شود و $۰ = ۱ + ۱$؛ برای عکس آن به تمرین ۱۲ نگاه کنید.] با استفاده از این ویژگی به سادگی می‌توان ثابت کرد که مجموعه C متشکل از کلمه کدها زیرگروهی از $B(۶)$ است (تمرین ۱۳).

این کد می‌تواند خطاهای انتقالی یگانه (که ۱ بجای ۰ یا ۰ بجای ۱ دریافت شده است) را کشف کند. زیرا به جای ۰، مجموع ارقام کلمه دریافت شده ۱ است. همین مطلب برای هر تعداد فردی از خطاها درست است. ولی این کد نه می‌تواند تعداد زوجی از خطاها را کشف کند و نه قادر است هیچ خطایی را اصلاح کند. برای هر $n \geq ۲$، یک $(n, n-۱)$ کد توازن‌سنج به همین طریق ساخته می‌شود[۸].

وقتی انتقال مجدد پیام‌ها ساده باشد، یک کد توازن‌سنج می‌تواند خیلی مفید باشد. چنین کدهایی اغلب در بانکداری و حساب داخلی رایانه مورد استفاده واقع می‌شوند. ولی وقتی انتقال مجدد

۷) کدهای خطی را کدهای بلوکی یا کدهای گروهی نیز می‌نامند.

۸) مترجمان: این مثال در حقیقت تعریفی از کد توازن سنج ارائه می‌دهد.

گران‌قیمت، مشکل یا نشدنی است، یک کد اصلاح- خطا مطلوبتر است. ما اکنون به توسعه ابزارهای ریاضی برای تعیین تعداد خطاهایی که یک کد می‌تواند کشف و اصلاح کند می‌پردازیم.

تعریف. **وزن هامینگ**[۹] یک عضو u از $B(n)$، تعداد مولفه‌های ناصفر u است که آن را با $Wt(u)$ نمایش می‌دهند.

مثال ۳.۱۶. اگر $u = ۱۱۰۱۱$ در $B(۵)$ باشد، آنگاه $Wt(u) = ۴$. بطور مشابه $v = ۱۰۱۰۰۱۰ \in B(۷)$ دارای وزن ۳ و ۰۰۰۰۰۰۰ دارای وزن ۰ می‌باشد.

تعریف. گیریم $u, v \in B(n)$. **فاصله هامینگ** بین u و v که با $d(u,v)$ نمایش داده می‌شود، تعداد مولفه‌هایی است که u و v در آنها برابر نیستند[۱۰].

مثال ۴.۱۶. اگر در $B(۵)$، $u = ۰۰۱۰۱$ و $v = ۱۰۱۱۱$، آنگاه $d(u,v) = ۲$ زیرا u و v در مولفه‌های اول و چهارم با هم فرق دارند. در $B(۴)$ فاصله بین ۰۰۰۰ و ۱۱۱۱، چهار است.

لم ۱.۱۶. اگر $u, v, w \in B(n)$، آنگاه

(۱) $d(u,v) = Wt(u-v)$ ؛

(۲) $d(u,v) \leq d(u,w) + d(w,v)$.

برهان. (۱) یک مولفه از $u - v$ ناصفر است اگر و تنها اگر در آن مولفه، u و v با هم متفاوت باشند. بنابراین تعداد مولفه‌های ناصفر در $u - v$، یعنی $Wt(u-v)$، درست برابر تعداد مولفه‌هایی است که در آنها u و v با هم فرق دارند، یعنی $d(u,v)$.

(۲) کافی است طبق (۱) ثابت کنیم $Wt(u-v) \leq Wt(u-w) + Wt(w-v)$. طرف چپ این نامساوی، تعداد مولفه‌های ناصفر $u - v$ و طرف راست تعداد کل مولفه‌های ناصفر در $u - w$ و $w - v$ است. پس فقط لازم است تحقیق کنیم که وقتی $u - v$، مولفه i ام ناصفر دارد، لااقل یکی از $u - w$ و $w - v$ نیز دارای مولفه i ام ناصفر است. با استفاده از زیرنویس i برای نشان

---

۹) Hamming weight

۱۰) به بیان دیگر، اگر $u = u_۱u_۲\cdots u_n$ و $v = v_۱v_۲\cdots v_n$ (به شرطی که هر یک از u_i، v_iها، ۱ یا ۰ باشد) آنگاه $d(u,v)$ تعداد نمایه‌های i است که $u_i \neq v_i$.

دادن i امین مولفه، فرض کنید $u_i - v_i$، مولفه i ام $u - v$، ناصفر باشد. اگر $u_i - w_i$ مولفه i ام $u - w$ ناصفر باشد. آنگاه چیزی برای اثبات وجود ندارد. اگر $u_i - w_i = 0$، آنگاه $u_i = w_i$. بدین دلیل $w_i - v_i = u_i - v_i \neq 0$. بنابراین $w_i - v_i$ مؤلفه i ام $w - v$ ناصفر است. ■

اگر یک کلمه کد u انتقال یافت و کلمه w دریافت شد، آنگاه تعداد خطاهای واقع در این انتقال برابر تعداد مولفه‌هایی است که در آنها u و w باهم متفاوتند، یعنی، فاصله هامینگ از u تا w است. چون وقوع تعداد زیادی از خطاهای انتقال احتمالاً کمتر از یک عدد کوچک است (تمرین ۲۷)، نزدیکترین کلمه کد به یک کلمه دریافتی به احتمال زیاد کلمه کد ارسال شده‌است. بنابراین، یک کلمه دریافتی به عنوان آن کلمه کدی که نزدیکترین فاصله را با آن در فاصله هامینگ دارد کُدگشایی می‌شود. اگر بیشتر از یک کلمه کد به آن نزدیکتر باشد کدگشا یک خطا را علامت می‌دهد[۱۱]. این فرآیند، **کدگشایی نزدیکترین ـ همسایه** نامیده، می‌شود[۱۲].

گفته می‌شود که یک کد خطی، t **خطا را اصلاح می‌کند** اگر هر کلمه کدی که با تعداد t یا کمتر خطا انتقال یافته است توسط کدگشایی نزدیکترین ـ همسایه بدرستی کدگشایی شود.

قضیه ۲.۱۶. یک کد خطی t خطا را اصلاح می‌کند اگر و تنها اگر فاصله هامینگ بین هر دو کلمه کد لااقل $2t + 1$ باشد.

برهان. فرض کنید که فاصله بین هر دو کلمه کد لااقل $2t + 1$ باشد. اگر کلمه کد u با خطای t یا کمتر منتقل گردد و به صورت w دریافت شود، آنگاه $d(u, w) \leq t$. اگر v کلمه کد دیگری باشد، آنگاه طبق فرض $d(u, v) \geq 2t + 1$. از اینرو طبق لم ۱.۱۶،

$$2t + 1 \leq d(u, v) \leq d(u, w) + d(w, v) \leq t + d(w, v).$$

تفریق t از طرفین رابطه $2t + 1 \leq t + d(w, v)$ نشان می‌دهد که $d(w, v) \geq t + 1$. چون $d(u, w) \leq t$، u نزدیکترین کد کلمه به w است، بنابراین کدگشایی نزدیکترین ـ همسایه w را به درستی به عنوان u کدگشایی می‌کند. بنابراین، این کد t خطا را اصلاح می‌کند. تمرین ۱۵ را برای برهان عکس این قضیه ملاحظه کنید. ■

۱۱) گزینه دیگر این است که کدگشا را طوری برنامه‌ریزی کرد که یکی از نزدیکترین کلمه کدها را به دلخواه انتخاب کند. این کار معمولاً وقتی انتقال مجدد مشکل یا ناممکن باشد انجام می‌گیرد.

۱۲) طبق مفروضات ما در این فصل، کدگشایی نزدیکترین ـ همسایه بر کدگشایی احتمال ماکسیمم منطبق است.

چون فقط کلمه کدها انتقال می‌یابند وقتی یک کلمه دریافتی کلمه کد نباشد خطاها کشف می‌شوند. گویند یک کد خطی، t **خطا کشف می‌کند** اگر کلمه دریافتی در هر انتقالی که همراه با حداقل یک و حداکثر t خطا باشد، یک کلمه کد نباشد.

قضیه ۳.۱۶. یک کد خطی t خطا کشف می‌کند اگر و تنها اگر فاصله هامینگ بین هر دو کلمه کد لااقل $t+1$ باشد.

برهان. فرض کنید که فاصله بین هر دو کلمه کد لااقل $t+1$ باشد. اگر کلمه کد u با لااقل یک و حداکثر t خطا انتقال یابد و به عنوان w دریافت شود، آنگاه

$$0 < d(u,w) \leq t \qquad \text{و بنابراین} \qquad d(u,w) < t+1.$$

پس w نمی‌تواند یک کلمه کد باشد. بنابراین، این کد t خطا را کشف می‌کند. برای دیدن برهان طرف عکس قضیه، تمرین ۱۶ را ملاحظه کنید. ■

اگر u و v کلمه کدهای متمایز باشند آنگاه طبق لم ۱.۱۶، $d(u,v)$ وزن کلمه کد ناصفر $u-v$ است. برعکس، وزن هر کلمه کد ناصفر w فاصله بین کلمه کدهای متمایز w و $B(n) \ni 00\cdots0 = 0$ است، زیرا $Wt(w) = Wt(w-0) = d(w,0)$. بنابراین فاصله هامینگ مینیمم بین هر دو کلمه کد درست برابر با کمترین وزن هامینگ تمام کلمه کدهای ناصفر می‌باشد. از ترکیب این واقعیت با قضایای ۲.۱۶ و ۳.۱۶ نتیجه می‌شود:

نتیجه ۴.۱۶. یک کد خطی $2t$ خطا را کشف و t خطا را اصلاح می‌کند اگر و تنها اگر وزن هامینگ هر کلمه کد ناصفر لااقل $2t+1$ باشد.

مثال ۵.۱۶. گیریم $B(2) \ni 11, 01, 10, 00$، کلمه‌های پیام باشند و به هر کلمه پیام، کلمه کد (عنصر $B(10)$) حاصل از پنج بار تکرار کلمه پیام را نظیر کنید تا یک $(10,2)$ کد بسازید:

$$0000000000, \quad 1010101010, \quad 0101010101, \quad 1111111111.$$

مجموعه C متشکل از کلمه کدها تحت جمع بسته است و از این جهت یک زیرگروه از مرتبه 2^2 می‌باشد (قضیه ۸.۷). بنابراین C یک $(10,2)$ کد است. هر کد ناصفر دارای وزن هامینگ لااقل

$۱ + ۲ \times ۲ = ۵$ می‌باشد. طبق قضیه ۴.۱۶ (با شرط این که $t = ۲$)، این کد C دو خطا را اصلاح و چهار خطا را کشف می‌کند.

با ساختن کدهایی که کلمه‌های پیام را به تعداد زیادی بار تکرار می‌کنند (۵ بار در مثال قبل)، همیشه یک درجه کشف و اصلاح بالا را می‌توانید تضمین کنید. اشکال چنین کدهای تکراری، ناکارآیی آنها در هنگامی است که پیام‌های طولانی باید ارسال شود. انتقال تعداد زیادی رقم برای هر کلمه پیام، وقت‌گیر و گران است. بنابراین هدف این است که کدهایی بسازیم که به میزان دقت قابل قبولی برسد بدون آن که میزان انتقال به طور غیر ضرور کاهش یابد.

یک فن کارآمد برای ساختن کدهای خطی براساس ضرب ماتریسی بنا شده است. کدهایی که بدین طریق ساخته می‌شوند به طور خودکار مجهز به یک الگوریتم کدگذار هستند که هر کلمه پیام را به یک کلمه کد یکتا متناظر می‌کنند.

مثال ۶.۱۶. می‌خواهیم یک $(۷, ۴)$ کد بسازیم. کلمه‌های پیام عناصر $B(۴)$ خواهند بود، و کلمه کدها عناصر $B(۷)$. کلمه‌های پیام به عنوان بردارهای سطری در نظر گرفته می‌شوند و با ضرب از طرف راست در ماتریس زیر که درایه‌هایش در $\mathbb{Z}_۲$ است به کلمه کدها تبدیل می‌شوند:

$$G = \begin{pmatrix} ۱ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ \end{pmatrix}$$

برای مثال، کلمه پیام ۱۱۰۱ به کلمه کد ۱۱۰۱۰۰۱ تبدیل می‌شود زیرا

$$(۱۱۰۱) \begin{pmatrix} ۱ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ \end{pmatrix} = (۱۱۰۱۰۰۱).$$

تمام عناصر مجموعه C متشکل از کلمه کدها را می‌توان به طور مشابه پیدا کرد:

کلمه کد	کلمه پیام	کلمه کد	کلمه پیام
۱۰۰۰۰۱۱	۱۰۰۰	۰۰۰۰۰۰۰	۰۰۰۰
۱۰۰۱۱۰۰	۱۰۰۱	۰۰۰۱۱۱۱	۰۰۰۱
۱۰۱۰۱۰۱	۱۰۱۰	۰۰۱۰۱۱۰	۰۰۱۰
۱۰۱۱۰۱۰	۱۰۱۱	۰۰۱۱۰۰۱	۰۰۱۱
۱۱۰۰۱۱۰	۱۱۰۰	۰۱۰۰۱۰۱	۰۱۰۰
۱۱۰۱۰۰۱	۱۱۰۱	۰۱۰۱۰۱۰	۰۱۰۱
۱۱۱۰۰۰۰	۱۱۱۰	۰۱۱۰۰۱۱	۰۱۱۰
۱۱۱۱۱۱۱	۱۱۱۱	۰۱۱۱۱۰۰	۰۱۱۱

قضیه ۶.۱۶ در زیر نشان می‌دهد که C در واقع یک زیرگروه $B(۷)$ است. بنابراین C یک $(۷,۴)$ کد است که **$(۷,۴)$ کد هامینگ** نامیده می‌شود. جدول فوق نشان می‌دهد که هر کلمه کد ناصفر دارای وزن هامینگ لااقل $۱+۱\times ۲=۳$ می‌باشد. بنابراین طبق نتیجه ۴.۱۶ (با $t=۱$) این کد خطاهای یگانه را اصلاح و دوگانه را کشف می‌کند.

جدول فوق نشان می‌دهد که کلمه کدها در $(۷,۴)$ کدِ هامینگ دارای شکل خاصی هستند: چهار رقم اول هر کلمه کد کلمه پیام متناظر را تشکیل می‌دهد. برای مثال ۱۱۰۱۰۰۱ کلمه کد برای ۱۱۰۱ است[۱۳]. یک (n,k) کد که در آن اولین k رقم هر کلمه کد تشکیل کلمه پیام متناظر را می‌دهد یک کد **روش‌مند** نامیده می‌شود. تمام مثال‌های فوق کدهای **روش‌مند** می‌باشند. کدهای روش‌مند راحت می‌باشند زیرا کلمه کدها به سادگی به کلمه‌های پیام برگردانده می‌شود: عیناً k رقم اول را بگیرید.

می‌توانیم با دنبال کردن روشی مشابه مثال آخر، کدهای روش‌مند دیگری بسازیم. یک **ماتریس مولد استاندارد** عبارت است از یک ماتریس $k\times n$ با درایه‌های در $\mathbb{Z}_۲$ به‌صورت

$$G=\begin{pmatrix} ۱ & ۰ & \cdots & ۰ & ۰ & a_{۱۱} & \cdots & a_{۱n-k} \\ ۰ & ۱ & & ۰ & ۰ & a_{۲۱} & \cdots & a_{۲n-k} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ ۰ & ۰ & & ۱ & ۰ & a_{(k-۱)۱} & \cdots & a_{k-۱n-k} \\ ۰ & ۰ & & ۰ & ۱ & a_{k۱} & \cdots & a_{kn-k} \end{pmatrix} = (I_k \mid A)$$

۱۳) سه رقم آخر هر کلمه کد **ارقام کنترل** هستند که می‌تواند برای تعیین این که آیا یک کلمه دریافتی یک کلمه کد است مورد استفاده قرار گیرد، تمرین ۲۲ را ملاحظه کنید.

که در آن I_k ماتریس همانی $k \times k$ و A یک ماتریس $k \times (n-k)$ است. برای مثال، ماتریس مثال قبل یک ماتریس مولد استاندارد ۷×۴ است. این ماتریس به شکل $(I_۴ \mid A)$ است که در آن A یک ماتریس ۳×۴ می‌باشد.

یک ماتریس مولد استاندارد می‌تواند با ضرب از طرف راست به عنوان الگوریتم کدگذاری برای تبدیل عناصر $B(k)$ به کلمه کدها (عناصر $B(n)$) مورد استفاده قرارگیرد. هر $u \in B(k)$ به عنوان یک بردار سطری به طول k در نظرگرفته می‌شود. در این صورت ضرب ماتریسی uG یک بردار سطری به طول n یعنی یک عضو $B(n)$ می‌باشد. چون اولین k ستون G ماتریس همانی را تشکیل می‌دهد، **k ستون اول کلمه کد uG کلمه پیام متناظر $u \in B(k)$ را تشکیل می‌دهد** (تمرین ۲۳). برای این که درستی نامگذاری کلمه کد برای uG را ثابت کنیم باید نشان دهیم که مجموعه تمام چنین عضوهایی یک زیرگروه $B(n)$ است.

لم ۵.۱۶. اگر $f : B(k) \to B(n)$ یک همریختی گروهی یک به یک باشد آنگاه تصویر f یک (n,k) کد است.

برهان. طبق قضیه ۱۴.۷، Imf زیرگروهی از $B(n)$ است که با $B(k)$ یکریخت است. بنابراین Imf دارای مرتبه ۲^k است و به این دلیل یک (n,k) کد است. ■

قضیه ۶.۱۶. اگر G یک ماتریس مولد استاندارد $k \times n$ باشد، آنگاه $\{uG \mid u \in B(k)\}$ یک (n,k) کد روش‌مند است.

برهان. تابع $f : B(k) \to B(n)$ را با ضابطه $f(u) = uG$ تعریف کنید. تصویر f برابر $\{f(u) \mid u \in B(k)\} = \{uG \mid u \in B(k)\}$ است. طبق لم ۵.۱۶ و تذکرات قبل از آن که با خط پررنگ نوشته شده‌است، فقط لازم است ثابت کنیم که f یک همریختی گروهی یک به یک است. چون ضرب ماتریسی توزیع‌پذیر است

$$f(u+v) = (u+v)G = uG + vG = f(u) + f(v).$$

پس f یک همریختی گروهی است.

اگر $u = u_۱u_۲\cdots u_k \in B(k)$، آنگاه چون G یک ماتریس مولد استاندارد است k مولفه اول uG، $u_۱, \cdots, u_k$ می‌باشند، و به طور مشابه برای $v = v_۱v_۲\ldots v_k \in B(k)$ چنین است. از

این واقعیت استفاده می‌کنیم تا ثابت کنیم f یک به یک است. اگر $f(u) = f(v)$، آنگاه در $B(n)$:

$$u_1u_2\cdots u_k * ** = uG = f(u) = f(v) = vG = v_1v_2\cdots v_k * **,$$

که در آن *ها مولفه‌های باقیمانده uG و vG را نمایش می‌دهند. چون این عضوها در $B(n)$ برابرند مولفه‌های آنها باید برابر باشند. بویژه $u_1 = v_1$، $u_2 = v_2$، ...، $u_k = v_k$. بنابراین در $B(k)$، $u = v$ و f یک به یک است. ■

مثال ۷.۱۶. طبق قضیه ۶.۱۶، ماتریس مولد استاندارد

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$(6,3)$ کد $\{uG \mid u \in B(3)\}$ را تولید می‌کند. تحقیق کنید که الگوریتم کدگذاری $u \to uG$، کلمه کدهای زیر را تولید می‌کند:

کلمه کد	کلمه پیام	کلمه کد	کلمه پیام
۱۰۰۰۱۱	۱۰۰	۰۰۰۰۰۰	۰۰۰
۱۰۱۱۰۱	۱۰۱	۰۰۱۱۱۰	۰۰۱
۱۱۰۱۱۰	۱۱۰	۰۱۰۱۰۱	۰۱۰
۱۱۱۰۰۰	۱۱۱	۰۱۱۰۱۱	۰۱۱

چون وزن هامینگ هر کلمه کد ناصفر لااقل ۳ است، طبق نتیجه ۴.۱۶، (با $t = 1$) این کد خطاهای یگانه را اصلاح و خطاهای دوگانه را کشف می‌کند.

توصیف یک کد بزرگ به وسیله ماتریس مولد استاندارد کارآیی بسیار بیشتری از نوشتن تمام کلمه کدها دارد. برای مثال، در یک $(۵۰, ۳۰)$ کد فقط ۱۵۰۰ درآیه در ماتریس مولد ۵۰×۳۰ موجود است ولی بیش از یک میلیارد کلمه کد وجود دارد.

از جبر خطی می‌توان استفاده کرد تا نشان داد که هر کد خطی روش‌مند توسط یک ماتریس مولد استاندارد حاصل می‌شود. ماتریس‌های مولد استاندارد برای کدهای مثال‌های فوق در تمرین‌های ۹ـ۷ آمده است.

تمرینها

A.۱. نشان دهید که $C = \{۰۰۰۰, ۰۱۰۱, ۱۰۱۰, ۱۱۱۱\}$ یک $(۴, ۲)$ کد است.

۲. وزن هامینگ این کدها را پیدا کنید.

(الف) $۰۱۱۰۱۱۰ \in B(۷)$ (ب) $۱۱۱۱۰۰۱۱ \in B(۸)$

(پ) $۰۰۰۰۰۱ \in B(۶)$ (ت) $۱۰۱۱۰۱۱۰۱۱۰۱ \in B(۱۲)$

۳. فاصله هامینگ بین این کدها را پیدا کنید.

(الف) ۱۰۱۰۱۰۱ و ۰۰۱۰۱۰۱ (ب) ۱۰۱۰۱۰۱۰۱ و ۱۰۰۱۱۰۰۱۰

(پ) ۱۱۱۱۱۱ و ۰۰۰۰۱۱ (ت) ۱۰۰۰۱۰۰۰ و ۰۰۰۰۱۰۰۰

۴. در $(۴, ۷)$ کد هامینگ، از کُدگشایی نزدیکترین همسایه استفاده کنید تا خطاها را کشف کنید و در صورت امکان، این کلمه‌های دریافت شده را کدگشایی کنید.

(الف) ۰۱۱۱۰۰۰ (ب) ۱۱۰۱۰۰۱

(پ) ۱۰۱۱۱۰۰ (ت) ۰۰۱۰۰۱۰

۵. تمام کلمه کدهای پدیدآمده توسط هر یک از ماتریس‌های مولد استاندارد زیر را بنویسید.

(الف) $\begin{pmatrix} ۱ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۱ \end{pmatrix}$ (ب) $\begin{pmatrix} ۱ & ۰ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۱ & ۰ \end{pmatrix}$

(پ) $\begin{pmatrix} ۱ & ۰ & ۰ & ۱ \\ ۰ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۰ \end{pmatrix}$ (ت) $\begin{pmatrix} ۱ & ۰ & ۰ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۱ & ۱ & ۰ \end{pmatrix}$

۶. تعداد خطاهایی که هر یک از کدهای تمرین ۵ کشف و اصلاح می‌کند را تعیین کنید.

۷. ثابت کنید که ماتریس مولد استاندارد

$$G = \begin{pmatrix} ۱ & ۰ & ۰ & ۰ & ۰ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۱ \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۰ & ۰ & ۱ & ۱ \end{pmatrix}$$

$(۶,۵)$ کد توازن سنج واقع در مثال ۲.۱۶ را تولید می‌کند. [راهنمایی: تمام کلمه کدهای پدیدآمده توسط G را بنویسید؛ آنگاه تمام کلمه کدهای کد توازن‌سنج را نوشته؛ این دو فهرست را با هم مقایسه کنید.]

۸. نشان دهید که ماتریس مولد استاندارد

$$G = \begin{pmatrix} ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ \\ ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \end{pmatrix}$$

$(۱۰,۲)$ کد تکرار واقع در مثال ۵.۱۶ را پدید می‌آورد. [راهنمایی، تمرین ۷ را ملاحظه کنید.]

۹. نشان دهید که ماتریس ۴×۱ مولد استاندارد (۱۱۱۱)، کد مثال ۱.۱۶ را پدید می‌آورد.

۱۰. ثابت کنید که $B(n) = \mathbb{Z}_۲ \times \mathbb{Z}_۲ \times \cdots \times \mathbb{Z}_۲$ با جمع مولفه به مولفه یک گروه آبلی از مرتبه ۲^n است.

B ۱۱. ثابت کنید که برای $u, v, w \in B(n)$،

(الف) $d(u,v) = d(v,u)$.

(ب) $d(u,v) = ۰$ اگر و تنها اگر $u = v$.

(پ) $d(u,v) = d(u+w, v+w)$.

۱۲. ثابت کنید که یک عضو $B(۶)$ در $(۶,۵)$ کد توان‌سنج یک کلمه کد است اگر مجموع ارقامش صفر باشد [راهنمایی: مجموع ۵ رقم اول را با رقم ششم مقایسه کنید.]

۱۳. ثابت کنید که مجموع تمام کلمه کدهای واقع در $(۶,۵)$ کد توازن‌سنج یک زیرگروه $B(۶)$ است. [راهنمایی: تمرین ۱۲ را بکار برید.]

۱۴. اگر v و u کلمه کدهای متمایز یک کد باشند که t خطا را اصلاح می‌کند توضیح دهید که چرا $d(u,v) \geq t$.

۱۵. با اثبات این که اگر یک کد t خطا را اصلاح کند، آنگاه فاصله هامینگ بین هر دو کلمه کد لااقل $۲t + ۱$ است، برهان قضیه ۲.۱۶ را تکمیل کنید. [راهنمایی: اگر u، v کلمه کدهایی باشند که $d(u,v) \leq ۲t$، با ساختن یک کلمه w که با u دقیقاً در t مولفه تفاوت دارد و با v در t مولفه یا کمتر متفاوت است یک تناقض بدست آورید؛ تمرین ۱۴ را ملاحظه کنید.]

۱۶. با اثبات این که اگر یک کد t خطا را کشف کند، آنگاه فاصله هامینگ بین هر دو کلمه کد لااقل $t+1$ است برهان قضیه ۳.۱۶ را تکمیل کنید.

۱۷. یک $(۵,۲)$ کد که خطاهای یگانه را اصلاح کند بسازید.

۱۸. نشان دهید که هیچ $(۶,۳)$ کد خطاهای دوگانه را اصلاح نمی‌کند.

۱۹. یک $(۷,۳)$ کد بسازید که در آن هر کلمه کد ناصفر دارای وزن هامینگ لااقل ۴ باشد.

۲۰. آیا یک $(۶,۲)$ کد وجود دارد که در آن هر کلمه کد ناصفر دارای وزن هامینگ لااقل ۴ باشد؟

۲۱. فرض کنید تنها سه پیام لازم است (برای مثال "برو"، "آهسته‌برو"، "توقف کن"). کوچکترین n ممکن را پیدا کنید به طوری که این سه پیام را در یک (n,k) کد که خطاهای یگانه را اصلاح می‌کند، بتوان انتقال داد.

۲۲. گیریم G ماتریس مولد استاندارد برای $(۷,۴)$ کد هامینگ واقع در مثال ۶.۱۶ باشد.

(الف) اگر $u=(u_۱,u_۲,u_۳,u_۴)$ یک کلمه پیام باشد، نشان دهید که کلمه کد متناظر uG برابر است با

$$(u_۱,u_۲,u_۳,u_۴,u_۲+u_۳+u_۴,u_۱+u_۳+u_۴,u_۱+u_۲+u_۴).$$

(ب) اگر $v=(v_۱,v_۲,v_۳,v_۴,v_۵,v_۶,v_۷)\in B(۷)$، نشان دهید که v یک کلمه کد است اگر و تنها اگر سه مولفه آخر آن (ارقام کنترل) در این معادلات صدق کند.

$$v_۵=v_۲+v_۳+v_۴$$
$$v_۶=v_۱+v_۳+v_۴$$
$$v_۷=v_۱+v_۲+v_۴.$$

۲۳. اگر G یک ماتریس مولد استاندارد $k\times n$ و $u=u_۱u_۲\cdots u_k$ یک کلمه پیام باشد نشان دهید که k رقم اول کلمه کد uG ارقام $u_۱$، $u_۲$، ...، u_k می‌باشد.

۲۴. اگر C یک کد خطی باشد، ثابت کنید که یا هر کلمه کد دارای وزن هامینگ زوج است یا دقیقاً نیمی از این کلمه کدها وزن هامینگ زوج دارند.

۲۵. ثابت کنید که عناصر با وزن هامینگ زوج در $B(n)$ تشکیل یک $(n, n-1)$ کد می‌دهند.

۲۶. اگر $k < n$ و $f : B(k) \to B(n)$ یک همریختی گروهی باشد، آیا $\mathrm{Im} f$ یک کد خطی است؟ آیا $\mathrm{Im} f$ یک (n, k) کد خطی است؟

توجه: برای تمرین‌های ۳۱ – ۲۷ اطلاع از نظریه احتمال مقدماتی و استفاده از ماشین حساب ضرورت دارد.

۲۷. فرض کنید که احتمال انتقال ناصحیح یک رقم یگانه ۰٫۰۱ باشد و این که یک کلمه کد چهار رقمی انتقال یافته است، یک درخت احتمال مناسب بسازید و احتمال آن که کلمه کد به یکی از حالات زیر انتقال یابد را حساب کنید

(الف) بدون خطا؛ (ب) خطای یگانه ؛

(پ) دو خطا ؛ (ت) سه خطا ؛

(ث) چهار خطا ؛ (ج) لااقل سه خطا.

۲۸. تمرین ۲۷ را برای یک کلمه کد پنج ـ رقمی انجام دهید.

۲۹. فرض کنید که احتمال انتقال ناصحیح یک رقم یگانه بیشتر از ۰٫۵ باشد. توضیح دهید که چرا "کدگشایی معکوس" (کدگشایی ۱ بجای ۰ و ۰ بجای ۱) بایستی بکار رود.

۳۰. فرض کنید که احتمال انتقال ناصحیح یک رقم یگانه برابر ۰٫۰۱ باشد و این که M یک پیام ۵۰۰ ـ رقمی باشد.

(الف) احتمال این که M بدون هیچ خطایی منتقل شود چقدر است؟

(ب) فرض کنید که هر رقم سه بار انتقال یابد (۱۱۱ برای هر ۱، ۰۰۰ برای هر ۰) و هر رقم دریافت شده طبق "قانون اکثریت" کدگشایی شود (۱۱۱، ۱۱۰، ۱۰۱، ۰۱۱ به صورت ۱ کدگشایی می‌شوند و ۰۰۰، ۰۰۱، ۰۱۰، ۱۰۰ به صورت ۰). احتمال این که پیام دریافت شده وقتی که M انتقال یافته است به درستی کدگشایی شود چیست؟ [راهنمایی: احتمال این که یک رقم یگانه به درستی بعد از انتقال کدگشایی شود را پیدا کنید.]

۳۱. (الف) نشان دهید که تعداد حالاتی که k خطا می‌تواند در یک پیام n- رقمی پیشامد کند برابر $\binom{n}{k}$ است، که در آن $\binom{n}{k}$ ضریب دوجمله‌ای است.

(ب) اگر p، احتمال انتقال ناصحیح یک رقم یگانه و q احتمال انتقال آن به صورت صحیح

باشد، نشان دهید که احتمال وقوع k خطا در یک پیام $n-$ رقمی برابر $\binom{n}{k}p^k q^{n-k}$ است.

۲-۱۶ فنون کدگشایی

کدگشایی نزدیکترین ـ همسایه برای یک (n,k) کد با مقایسه هر کلمه دریافت شده، با تمامی 2^k کلمه کدها به منظور کدگشایی آن، در بخش ۱.۱۶ انجام گردید. ولی وقتی k خیلی بزرگ باشد، این روشِ بی‌روح مبتنی بر مقایسه صرف، ممکن است غیرعملی یا غیرممکن باشد. بنابراین اکنون به بسط و توسعه فنون کدگشایی که بعضاً مؤثرترند می‌پردازیم. یکی از اینها مبتنی بر دو مفهوم گروه و هم‌مجموعه می‌باشد.

مثال ۸.۱۶. گیریم C، $(5,2)$کدِ $\{00000, 10110, 01101, 11011\}$ باشد. از عضوهایی که در $B(5)$ و در C نیستند یکی که کمترین وزن را دارد انتخاب کنید (که در این حالت این وزن ۱ است)، مثلاً $e_1 = 10000$. هم‌مجموعه $e_1 + C$ را با اضافه نمودن e_1 به طور متوالی به عناصر C بسازید و عضوهای این هم‌مجموعه را بنویسید به طوری که برای هر $c \in C$، $e_1 + c$ مستقیماً زیر $c \in C$ قرار گیرد:

C:	00000	10110 01101 11011
$e_1 + C$:	10000	00110 11101 01011

پس، برای مثال، $11101 \in C$ مستقیماً زیر $01101 \in C$ است زیرا $11101 = 01101 + 10000 = 01101 + e_1$. در بین عناصری که در بالا فهرست نشده است، یکی را که کمترین وزن را دارد انتخاب کنید، مثلاً $e_2 = 01000$ و هم‌مجموعه‌های آن را به همان طریق (به طوری که $e_2 + c$ زیر $c \in C$ باشد) فهرست کنید:

C:	00000	10110 01101 11011
$e_1 + C$:	10000	00110 11101 01011
$e_2 + C$:	01000	11110 00101 10011

بین عناصری که هنوز فهرست نشده است، یکی که کوچکترین وزن را دارد انتخاب و هم‌مجموعه‌های آن را فهرست کنید و به این طریق ادامه دهید تا این که هر یک از عناصر $B(5)$ در جدول ظاهر شود. تحقیق کنید که این یک جدول کامل است:

کلمه کدها	۱۱۰۱۱	۰۱۱۰۱	۱۰۱۱۰	۰۰۰۰۰
	۰۱۰۱۱	۱۱۱۰۱	۰۰۱۱۰	۱۰۰۰۰
	۱۰۰۱۱	۰۰۱۰۱	۱۱۱۱۰	۰۱۰۰۰
کلمه‌های دریافتی	۱۱۱۱۱	۰۱۰۰۱	۱۰۰۱۰	۰۰۱۰۰
	۱۱۰۰۱	۰۱۱۱۱	۱۰۱۰۰	۰۰۰۱۰
	۱۱۰۱۰	۰۱۱۰۰	۱۰۱۱۱	۰۰۰۰۱
	۰۰۰۱۱	۱۰۱۰۱	۰۱۱۱۰	۱۱۰۰۰
	۰۱۰۱۰	۱۱۱۰۰	۰۰۱۱۱	۱۰۰۰۱

قانون کدگشایی (که ذیلاً درستی آن بررسی می‌شود) چنین است: یک کلمه دریافت شده w را به عنوان آن کلمه کدی کدگشایی کنید که در بالای ستونی که w درآن ظاهر می‌شود قرار دارد. برای مثال، ۰۱۰۰۱ (چهارمین سطر) به عنوان ۰۱۱۰۱ کدگشایی شده است ؛ و ۰۱۰۱۰ (سطر آخر) به عنوان ۱۱۰۱۱ کدگشایی شده است. به طور مشابه، ۱۱۰۰۰ (سطر هفتم) به عنوان ۰۰۰۰۰ کدگشایی شده است.

جدول کدگشایی این مثال یک **آرایه استاندارد** نامیده می‌شود، و آن را قانون کدگشایی **آرایه ـ استاندارد** یا **کدگشایی هم‌مجموعه** می‌نامند. همین روش را می‌توان بکار برد تا آرایه استانداردی برای یک کد دلخواه C ساخت. سطرهای این آرایه هم‌مجموعه‌های C هستند که البته خود C در اولین سطر آن قراردارد. هر سطر به صورت $e+C$ است که در آن e **پیشرو هم‌مجموعه** (یک عنصر از کمترین وزن در هم‌مجموعه و به عنوان اولین کلمه در سطر فهرست می‌شود) است. عنصر $e+c$ (با $c \in C$) در ستون زیر c فهرست می‌شود و به عنوان c کدگشایی می‌شود.

قضیه ۷.۱۶. گیریم C یک (n,k) کد باشد. کدگشایی آرایه‌ـ استاندارد برای C کدگشایی نزدیکترین ـ همسایه می‌باشد.

برهان. اگر $w \in B(n)$، آنگاه $w = e + v \in e + C$، که در آن e یک پیشرو هم‌مجموعه است و v آن کلمه کدی است که در بالای ستون شامل w است. کدگشایی آرایه استاندارد w را به عنوان v کدگشایی می‌کند. باید ثابت کنیم که v نزدیکترین کلمه کد نسبت به w است. اگر $u \in C$ کلمه کد دیگری باشد، آنگاه $w - u$ عنصری از $w + C$ است. ولی $w + C$، هم‌مجموعه e است (زیرا $e = w - v \in w + C$). طبق ساختار، پیشرو هم‌مجموعه e دارای کمترین وزن در هم‌مجموعه خودش می‌باشد، پس $Wt(w - u) \geq Wt(e)$. بنابراین، طبق لم ۱.۱۶،

$$d(w, u) = Wt(w - u) \geq Wt(e) = Wt(w - v) = d(w, v).$$

بدین دلیل v نزدیکترین کلمه کد به w است. ■

وقتی کدگشایی نزدیکترین ـ همسایه توسط یک آرایه استاندارد صورت عمل بخود گرفت، در صورتی که بیشتر از یک کلمه کد نزدیکترین فاصله را با یک کلمه دریافتی w داشته باشد، سیستم (به جای اعلام خطا) یکی از آنها را به طور خودکار انتخاب می‌کند. بنابراین در چنین حالت‌هایی ممکن است کدگشایی ناصحیح واقع شود. کد ارائه شده در آخرین مثال، خطاهای یگانه را اصلاح می‌کند (هر کلمه حداقل دارای وزن ۳ می‌باشد؛ نتیجه ۴.۱۶ را ملاحظه کنید). چون دو خطا یا بیشتر بسیار کمتر از یک خطای یگانه احتمال وقوع دارد، کد گشایی آرایه ـ استاندارد برای این کد دارای میزان دقت بالا است (تمرین ۱۸).

وقتی یک آرایه استاندارد ساخته شد، این آرایه برای کدگشایی خیلی بیشتر از روش بی‌روح مبتنی بر مقایسه صرف با تمام کلمه کدها مؤثر خواهد بود. متأسفانه، ساختن یک آرایه استاندارد برای یک کد بزرگ ممکن است به همان زیادی روش مبتنی بر مقایسه صرف، از رایانه حافظه و زمان ببرد. ولی وقتی یک کد توسط یک ماتریس مولد عرضه می‌شود، یک آرایه کدگشایی بسیار کوتاهتر امکان وقوع دارد، چنان که اکنون می‌بینیم.

یک (n, k) کد با ماتریس مولد $k \times n$، $G = (I_k \mid A)$ را در نظر بگیرید. **ماتریس توازن سنج** این کد، ماتریس $n \times (n - k)$، $H = \left(\frac{A}{I_{n-k}}\right)$[۱۴] است.

---

۱۴) چون ماتریس مولد را همواره می‌توان از ماتریس توازن‌سنج بدست آورد، بسیاری از کتاب‌های نظریه کدگذاری، یک کد را بر حسب ماتریس توازن‌سنج بجای ماتریس مولد آن تعریف می‌کنند. در اغلب کتاب‌ها ماتریس توازن‌سنج را ترانهاده ماتریس H تعریف کرده‌اند، یعنی ماتریس $n \times (k - n)$ ای که i امین سطر آن، i امین ستون H است. کار با

مثال ۹.۱۶. تحقیق کنید که ماتریس مولد استاندارد برای $(۵,۲)$ کد $\{۰۰۰۰۰, ۱۰۱۱۰, ۰۱۱۰۱, ۱۱۰۱۱\}$ مثال قبل عبارت است از

$$G = \begin{pmatrix} ۱ & ۰ & ۱ & ۱ & ۰ \\ ۰ & ۱ & ۱ & ۰ & ۱ \end{pmatrix} = (I_۲ \mid A).$$

در اینجا $k = ۲$، $n = ۵$، $n - k = ۳$ و A یک ماتریس ۳×۲ است. بنابراین ماتریس توازن‌سنج عبارت است از ماتریس ۳×۵ زیر

$$H = \begin{pmatrix} ۱ & ۱ & ۰ \\ ۱ & ۰ & ۱ \\ ۱ & ۰ & ۰ \\ ۰ & ۱ & ۰ \\ ۰ & ۰ & ۱ \end{pmatrix} = \begin{pmatrix} A \\ \overline{I_۳} \end{pmatrix}.$$

تحقیق کنید که ماتریس حاصل‌ضرب GH ماتریس ۳×۲ صفر است. این پدیده در حالت کلی نیز برقرار است:

لم ۸.۱۶. اگر $G = (I_k \mid A)$ ماتریس مولد استاندارد برای یک کد خطی باشد و $H = \begin{pmatrix} A \\ \overline{I_{n-k}} \end{pmatrix}$ ماتریس توازن‌سنج آن باشد، آنگاه GH ماتریس صفر است.

برهان. درایه سطر i–ام و ستون j–ام GH حاصل‌ضرب سطر i–ام G (بندهای بعد از مثال

ماتریس H در اینجا مناسب‌تر است، و در هر حال، تمام نتایج را می‌توان به سادگی از این نماد به نماد دیگر انتقال داد.

۶.۱۶ را ملاحظه کنید) و ستون j–ام H است[۱۵]:

$$(\delta_{i_1}\delta_{i_2}\cdots\delta_{ij}\cdots\delta_{ik}a_{i_1}a_{i_2}\cdots a_{ij}\cdots a_{in-k})\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{ij} \\ \vdots \\ a_{kj} \\ \delta_{1j} \\ \delta_{2j} \\ \vdots \\ \delta_{ij} \\ \vdots \\ \delta_{n-kj} \end{pmatrix}$$

$$= \delta_{i_1}a_{1j} + \delta_{i_2}a_{2j} + \cdots + \delta_{ii}a_{ij} + \cdots + \delta_{ik}a_{kj}$$
$$+a_{i_1}\delta_{1j} + a_{i_2}\delta_{2j} + \cdots + a_{ij}\delta_{jj} + \cdots + a_{i(n-k)}\delta_{(n-k)j}.$$

چون وقتی $r \neq s$، $\delta_{rs} = 0$ و چون جمع در $\mathbb{Z}_2$ است، این مجموع به مجموع

$$\delta_{ii}a_{ij} + a_{ij}\delta_{jj} = 1a_{ij} + a_{ij}1 = a_{ij} + a_{ij} = 0$$

کاهش می‌یابد. ■

در یک (n,k) کد با ماتریس مولد استاندارد G با ابعاد $k \times n$، کلمه دریافت‌شده $w \in B(n)$ یک بردار سطری به طول n است. چون ماتریس توازن‌سنج H، $n \times (n-k)$ است، حاصل‌ضرب wH یک بردار سطری به طول $n-k$، یعنی یک عضو $B(n-k)$ است. کلمه $000\ldots0 \in B(n-k)$ را با 0 نمایش می‌دهیم.

۱۵) نماد دلتای کرونکر δ_{rs} در پیوست ج تشریح شده است.

مثال ۱۰.۱۶. گیریم H ماتریس توازن‌سنج برای (۵,۲) کد مثال قبل باشد. آنگاه $H = ۰۱۱$ ۱۱۰۰۰ و $H = ۰$ ۱۰۱۱۰:

$$(۱۱۰۰۰)\begin{pmatrix} ۱ & ۱ & ۰ \\ ۱ & ۰ & ۱ \\ ۱ & ۰ & ۰ \\ ۰ & ۱ & ۰ \\ ۰ & ۰ & ۱ \end{pmatrix} = (۰۱۱)$$

و

$$(۱۰۱۱۰)\begin{pmatrix} ۱ & ۱ & ۰ \\ ۱ & ۰ & ۱ \\ ۱ & ۰ & ۰ \\ ۰ & ۱ & ۰ \\ ۰ & ۰ & ۱ \end{pmatrix} = (۰۰۰)$$

این واقعیت که ۱۰۱۱۰ یک کلمه کد در این کد است و $H = ۰$ ۱۰۰۱۰ مصداقی از قضیه زیر است.

قضیه ۹.۱۶. گیریم C یک (n,k) کد با ماتریس مولد استاندارد G و ماتریس توازن‌سنج H باشد. آنگاه یک عنصر $w \in B(n)$ یک کلمه کد است اگر و تنها اگر $wH = ۰$.

برهان. تابع $f : B(n) \to B(n-k)$ با ضابطه $f(w) = wH$ را تعریف کنید. آنگاه f یک همریختی گروهی است (همان استدلال قضیه ۶.۱۶). حال w یک کلمه کد است اگر و تنها اگر $w \in C$. همچنین، $w \in K$ (هسته $f = K$) اگر و تنها اگر $wH = ۰$. بنابراین باید ثابت کنیم که $w \in C$ اگر و تنها اگر $w \in K$، یعنی این که $C = K$. طبق تعریف ماتریس مولد، هر عنصر C به صورت uG برای برخی $u \in B(k)$ می‌باشد. ولی $(uG)H = u(GH) = ۰$ زیرا GH ماتریس صفر است (لم ۸.۱۶). بنابراین $K \subseteq C$. چون C یک زیرگروه از مرتبه ۲^k است، برای این که نتیجه بگیریم $C = K$ کافی است ثابت کنیم K دارای مرتبه ۲^k است.

تمرین ۱۴ نشان می‌دهد که f پوشاست. طبق اولین قضیه یکریختی ۲۹.۷،

$B(n-k) \cong B(n)/K$، و طبق قضیه لاگرانژ ۳۳.۷،

$$\begin{aligned} ۲^n &= |\, B(n)\,| = |\, K\,|\,[B(n):K] \\ &= |\, K\,| \cdot |\, B(n)/K\,| = |\, K\,|\,|\, B(n-k)\,| = |\, K\,| \cdot ۲^{n-k} \end{aligned}$$

تقسیم اولین و آخر جمله این معادله بر ۲^{n-k} نشان می‌دهد که $|\, K\,| = ۲^k$. ■

نتیجه ۱۰.۱۶. گیریم C یک کد خطی با ماتریس توازن‌سنج H باشد و گیریم $u, v \in B(n)$. آنگاه u و v در یک هم‌مجموعه C هستند اگر و تنها اگر $uH = vH$.

برهان. گفتن این که u و v در یک هم مجموعه هستند به معنی $u + C = v + C$ است. قضیه ۱۸.۷ در نمادگذاری جمعی نشان می‌دهد که

$$u + C = v + C \quad \text{اگر و تنها اگر} \quad u - v \in C.$$

طبق قضیه ۹.۱۶،

$$u - v \in C \quad \text{اگر و تنها اگر} \quad (u-v)H = ۰.$$

چون ضرب ماتریسی توزیع‌پذیر است، $(u-v)H = uH - vH$. همچنین $uH - vH = ۰$ هم‌ارز $uH = vH$ است. از این جهت

$$(u-v)H = ۰ \quad \text{اگر و تنها اگر} \quad uH = vH.$$

از ترکیب سه گزاره بالا (که در وسط سطر قرارگرفته‌اند) این قضیه ثابت می‌شود. ■

اگر $w \in B(n)$ و H ماتریس توازن‌سنج باشد، آنگاه wH **علامت مشخصه** w نامیده می‌شود. طبق نتیجه ۱۰.۱۶، w و پیشرو هم‌مجموعه‌اش e دارای یک علامت مشخصه می‌باشند. اگر $w = e + v$ که در آن $v \in C$، آرایه استاندارد، w را به عنوان $v = w - e$ کدگشایی می‌کند. بنابراین کدگشایی آرایه ـ استاندارد (نزدیکترین ـ همسایه) می‌تواند به صورت زیر به اجراء گذاشته شود:

۱. اگر w یک کلمه دریافت‌شده باشد، علامت مشخصه w (یعنی wH) را محاسبه کنید.

۲. پیشرو هم‌مجموعه e که علامت مشخصه آن با w یکی است (یعنی $eH = wH$) را پیدا کنید.

۳. w را به عنوان $w - e$ کدگشایی کنید.

چون این فرآیند (که **کدگشایی علامت مشخصه** نامیده می‌شود) تنها مستلزم دانستن علامت مشخصه

پیشروهای هم‌مجموعه می‌باشد، آرایه استاندارد می‌تواند با یک جدول بسیار کوتاهتر جایگزین شود.

مثال ۱۱.۱۶. پیشروهای هم‌مجموعه برای $(۵, ۲)$ کد $\{۰۰۰۰۰, ۱۰۱۱۰, ۰۱۱۰۱, ۱۱۰۱۱\}$ که در مثال‌های پیشین ارائه شد، عبارتند از

$$۰۰۰۰۰, ۱۰۰۰۰, ۰۱۰۰۰, ۰۰۱۰۰, ۰۰۰۱۰, ۰۰۰۰۱, ۱۱۰۰۰, ۱۰۰۰۱$$

از ضرب هر یک از آن‌ها در ماتریس توازن‌سنج H که در مثال قبل عرضه شد، علامت مشخصه آن‌ها بدست می‌آید:

علامت مشخصه	۰۰۰	۱۱۰	۱۰۱	۱۰۰	۰۱۰	۰۰۱	۰۱۱	۱۱۱
پیشرو هم‌مجموعه	۰۰۰۰۰	۱۰۰۰۰	۰۱۰۰۰	۰۰۱۰۰	۰۰۰۱۰	۰۰۰۰۱	۱۱۰۰۰	۱۰۰۰۱

برای مثال، برای کدگشایی $w = ۰۱۰۰۱$، محاسبه می‌کنیم: $H = ۱۰۰$ ۰۱۰۰۱. جدول نشان می‌دهد که پیشرو هم‌مجموعه با این علامت مشخصه، $e = ۰۰۱۰۰$ است. بنابراین ما w را به عنوان $w - e = ۰۱۰۰۱ - ۰۰۱۰۰ = ۰۱۱۰۱$ کدگشایی می‌کنیم.

بسته به اندازه کد و این که پیشروهای هم‌مجموعه را بتوان بدون ساختن تمام آرایه استاندارد تعیین کرد یا نه، کدگشایی علامت مشخصه می‌تواند مفیدتر از کدگشایی نزدیکترین ـ همسایه باشد. برای مثال، یک (۴۸ و ۵۶) کد دارای $۲^{۴۸}$ (تقریباً $۲٫۸ \times ۱۰^{۱۴}$) کلمه کد است ولی فقط دارای $۲۵۶ = ۲^{۸}$ هم‌مجموعه است.

آرایه استاندارد و کدگشایی علامت مشخصه طرح‌های کدگشای **کامل** می‌باشند، بدین معنی که آنها همواره یک نزدیکترین کلمه کد را برای هر کلمه دریافت شده پیدا می‌کنند. وقتی انتقال مجدد پیام غیرعملی باشد، کدگشایی کامل یک ضرورت است، ولی وقتی انتقال مجدد امکان‌پذیر باشد ممکن است استفاده از یک طرح کدگشایی غیرکامل بهتر باشد که، t خطا را اصلاح کند و در صورت کشف بیشتر از t خطا درخواست انتقال مجدد نماید.

گیریم $e_i \in B(n)$ بردار سطری باشد که در مؤلفه i ام آن ۱ و در مولفه‌های دیگر ۰ باشد. در $B(۳)$، برای مثال، $e_۱ = ۱۰۰$، $e_۲ = ۰۱۰$ و $e_۳ = ۰۰۱$. هر e_i دارای وزن ۱ است؛ در حقیقت $e_۱$، $e_۲$، ...، e_n عضوهای به وزن ۱ در $B(n)$ می‌باشند.

حاصل‌ضرب $e_2 \in B(3)$ و ماتریس H زیر را در نظر بگیرید:

$$e_2H = (010)\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = (011) = (\text{سطر دوم } H)$$

تمرین ۱۰ نشان می‌دهد که این امر در حالت کلی نیز اتفاق می‌افتد. اگر $e_i \in B(n)$ و H یک ماتریس n سطری باشد، آنگاه

e_iH سطر i ام ماتریس H است.

اکنون فرض کنید C یک کد خطی با ماتریس توازن‌سنج H باشد و این که سطرهای H ناصفر و هیچ دوتای آنها برابر نباشد. آنگاه e_iH سطر $i-$ ام H است که طبق فرض مخالف ۰ است؛ از این جهت طبق قضیه ۹.۱۶،

e_i کلمه کد نیست.

به‌علاوه، اگر $i \neq j$، آنگاه e_i و e_j نمی‌توانند در یک هم‌مجموعهٔ C باشند (در غیر این صورت طبق نتیجه ۱۰.۱۶، e_iH، سطر $i-$ام H با e_jH که سطر $j-$ ام H است برابر می‌باشد). بدین دلیل

e_i تنها عنصر به وزن ۱ در هم‌مجموعه‌اش می‌باشد.

بنابراین هر عنصر دیگر در هم‌مجموعه e_i دارای وزن حداقل ۲ می‌باشد[۱۶]. در نتیجه

e_i همواره پیشرو هم‌مجموعه در هم‌مجموعهٔ خودش می‌باشد.

بالاخره، اگر علامت مشخصه یک کلمه دریافت‌شده w، سطر i ام H باشد، آنگاه $wH = e_iH$، بنابراین w و e_i طبق نتیجه ۱۰.۱۶، در یک هم‌مجموعه هستند.

بند قبل راه مناسبی را برای انجام کدگشایی علامت مشخصه (احتمالاً غیرکامل)، وقتی که سطرهای H ناصفر و متمایز باشند پیشنهاد می‌کند:

۱. اگر w دریافت شود، علامت مشخصه wH آن را محاسبه کنید.

۲. اگر $wH = 0$، w را به عنوان w کدگشایی کنید (زیرا طبق قضیه ۹.۱۶، w یک کلمه کد است).

---

۱۶) تنها عنصر از وزن ۰، $000\ldots000$ می‌باشد، که هم‌مجموعه آن C است. C هم‌مجموعه e_i نیست زیرا e_i یک کلمه کد نیست.

۳. اگر $wH \neq ۰$ و wH سطر i ام H باشد، w را با تغییر i امین مولفه‌اش کدگشایی کنید (یعنی، w را به عنوان $w - e_i$ کدگشایی کنید زیرا e_i پیشرو هم‌مجموعهٔ w است).

۴. اگر $wH \neq ۰$ و wH سطری از H نباشد، کدگشایی نکنید و یک انتقال مجدد درخواست کنید.

این طرح (که **کدگشایی ماتریس توازن‌سنج** نامیده می‌شود) به سادگی می‌تواند با کدهای بزرگ اجرا شود زیرا احتیاجی به محاسبه هم‌مجموعه‌ها یا پیشرو هم‌مجموعه‌ها نیست. به‌علاوه، قضیه زیر را داریم:

قضیه ۱۱.۱۶. گیریم C یک کد خطی با ماتریس توازن‌سنج H باشد. اگر هر سطر H ناصفر و هیچ دوسطری برابر نباشند، آنگاه کدگشایی ماتریس توازن‌سنج تمام خطاهای یگانه را اصلاح می‌کند.

برهان. وقتی یک کلمه کد u با دقیقاً یک خطا در مولفه i-ام آن منتقل شود و به صورت w دریافت شود، آنگاه $w - u = e_i$. از این جهت $e_i = w - u \in w + C$، بنابراین e_i باید پیشرو هم‌مجموعه w باشد. بنابراین w به درستی به‌عنوان $w - e_i = u$ کدگشایی می‌شود. ■

مثال ۱۲.۱۶. گیریم C، $(۵, ۲)$ کدی باشد که ماتریس توازن‌سنج آن در مثال ۹.۱۶ عرضه شد. اگر ۱۰۰۱۱ دریافت شود، علامت مشخصه آن سطر دوم H است:

$$(۱۰۰۱۱)H = (۱۰۰۱۱)\begin{pmatrix} ۱ & ۱ & ۰ \\ ۱ & ۰ & ۱ \\ ۱ & ۰ & ۰ \\ ۰ & ۱ & ۱ \\ ۰ & ۰ & ۱ \end{pmatrix}$$

$$= (۱۰۱) = (H \text{ سطر دوم})$$

بنابراین ۱۰۰۱۱ به صورت ۱۱۰۱۱ = ۰۱۰۰۰ − ۱۰۰۱۱ = ۱۰۰۱۱ − $e_۲$ کدگشایی می‌شود.

اگر ۱۱۰۰۰ دریافت شود، تحقیق کنید که علامت مشخصه آن ۰۱۱ است، که یک سطر H نیست. بنابراین ۱۱۰۰۰ کدگشایی نمی‌شود، و یک انتقال مجدد درخواست می‌گردد.

در یک رده مهم ازکدها، کدگشایی توازن‌سنج در واقع کدگشایی علامت مشخصه کامل (نزدیکترین ـ همسایه) است.

مثال ۱۳.۱۶. ماتریس مولد استاندارد برای $(۷,۴)$ کد هامینگ در مثال ۶.۱۶ عرضه شد. ماتریس توازن‌سنج آن دارای سطرهای ناصفر متمایز می‌باشد:

$$H = \begin{pmatrix} ۰ & ۱ & ۱ \\ ۱ & ۰ & ۱ \\ ۱ & ۱ & ۰ \\ ۱ & ۱ & ۱ \\ ۱ & ۰ & ۰ \\ ۰ & ۱ & ۰ \\ ۰ & ۰ & ۱ \end{pmatrix}$$

علامت‌های مشخصه ممکن یک کلمه دریافت شده w در این کد عنصر ۰۰۰ و هفت عنصر ناصفر $B(۳)$ می‌باشد. ولی تمام عناصر ناصفر $B(۳)$ به صورت سطرهای H ظاهر می‌شوند. بنابراین هر علامت مشخصه یا ۰۰۰ (w را به عنوان خودش کدگشایی کنید) یا سطر iام H برای یک i است (w را با تغییر i امین مولفه آن کدگشایی کنید). بنابراین هر کلمه دریافت شده کدگشایی می‌شود.

این مثالی است از رده نامتناهی کدهایی که می‌توانند با استفاده از این واقعیت که یک کد خطی به طور کامل توسط ماتریس توازن‌سنج آن (که برای آن یک ماتریس مولد استاندارد به سادگی می‌توان پیدا کرد) تعیین می‌شود، توصیف گردد. گیریم $r \geq ۲$ یک عدد صحیح باشد و گیریم $n = ۲^r - ۱$ و $k = ۲^r - ۱ - r$. آنگاه $n - k = r$. مثال قبل حالت $r = ۳$ است. گیریم H آن ماتریس $n \times (n-k)$ باشد که r سطر آخرش ماتریس همانی I_r و n سطر اول آن شامل عناصر ناصفر $B(r)$ باشد. چون تعداد عناصر ناصفر $B(r)$، $n = ۲^r - ۱$ است، هر عنصر ناصفر دقیقاً یکبار به صورت یک سطر H ظاهر می‌شود. بنابراین سطرهای H متمایز و ناصفرند. کدی که ماتریس توازن‌سنج آن این ماتریس باشد **کد هامینگ** نامیده می‌شود.

در هر کد هامینگ تمام علامت‌های مشخصه ممکن، سطرهای H می‌باشند. بنابراین کدگشایی ماتریس توازن‌سنج، کدگشایی علامت مشخصه کاملی است که خطاهای یگانه را اصلاح می‌کند.

تمرینها

۱.A. ماتریس توازن‌سنج هر ماتریس مولد استاندارد تمرین ۵ از بخش ۱.۱۶ را پیدا کنید.

۲. ماتریس توازن‌سنج برای کد مثال آخر بخش ۱.۱۶ را پیدا کنید.

۳. ماتریس توازن‌سنج برای کد توازن‌سنج واقع در مثال ۲.۱۶ را پیدا کنید. [تمرین ۷ در بخش ۱.۱۶ را ملاحظه کنید.]

۴. ماتریس توازن‌سنج برای $(۱۰, ۲)$ کد تکرار در مثال ۵.۱۶ را پیدا کنید. [تمرین ۸ در بخش ۱.۱۶ را ملاحظه کنید.]

۵. یک ماتریس توازن‌سنج برای $(۱۵, ۱۱)$ کد هامینگ پیدا کنید.

۶. نشان دهید که کد خطی C با ماتریس توازن‌سنج $\begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \\ ۱ & ۰ \\ ۰ & ۱ \\ ۱ & ۰ \\ ۰ & ۱ \end{pmatrix}$ قادر به اصلاح همهٔ خطاهای یگانه نیست.

۷. گیریم C، $(۴, ۲)$ کد با ماتریس مولد استاندارد $G = \begin{pmatrix} ۱ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۱ \end{pmatrix}$ باشد. یک آرایه استاندارد برای C بسازید و علامت مشخصه هر پیشرو هم مجموعه را پیدا کنید.

۸. یک آرایه استاندارد برای $(۶, ۳)$ کد مثال آخر بخش ۱.۱۶ بسازید و علامت مشخصه هر پیشرو هم‌مجموعه را پیدا کنید.

۹. برای $(۵, ۲)$ کد واقع در مثال ۸.۱۶ یک پیشرو هم‌مجموعه (در صورت امکان) انتخاب کنید و از آنها استفاده کنید تا یک آرایه استاندارد بسازید. این آرایه چگونه با آرایه‌های واقع در مثال ۸.۱۶ مقایسه می‌شود.

۱۰. گیریم $e_i = ۰۰\ldots۰۱۰\ldots۰۰ \in B(n)$، که در آن ۱ در مکان i- ام و ۰ در بقیه جاها قرار دارد. اگر H یک ماتریس با n سطر باشد، ثابت کنید که e_iH سطر i ام H است.

۱۱.B. فرض کنید یک کلمه کد u ارسال شده است و w دریافت گردیده‌است. ثابت کنید که کدگشایی آرایه ـ استاندارد، w را به صورت u کدگشایی می‌کند اگر و تنها اگر $w - u$ یک پیشرو هم‌مجموعه باشد.

۱۲. اگر هر عنصر به وزن t یک پیشرو هم‌مجموعه در یک آرایه استاندارد برای یک کد C باشد، نشان دهید که C، t خطا را اصلاح می‌کند.

۱۳. اگر یک کلمه کد u منتقل شود و w دریافت شود، آنگاه $e = w - u$ **الگوی خطا** نامیده می‌شود. ثابت کنید که یک خطا کشف می‌شود اگر و تنها اگر الگوی خطای متناظر آن یک کلمه کد نباشد.

۱۴. ثابت کنید که تابع $f : B(n) \to B(n-k)$ در اثبات قضیه ۹.۱۶ پوشاست. [راهنمایی: اگر $v = v_1 \cdots v_{n-k} \in B(n-k)$، نشان دهید که $v = f(u)$، که در آن $u = 00 \cdots 0 v_1 v_2 \cdots v_{n-k} \in B(n)$.]

۱۵. گیریم C یک کد خطی با ماتریس توازن‌سنج H باشد. ثابت کنید که C خطاهای یگانه را اصلاح می‌کند اگر و تنها اگر سطرهای H متمایز و ناصفر باشند.

۱۶. با مثال نشان دهید که ماتریس کدگشای توازن‌سنج با (۷, ۴) کد هامینگ نمی‌تواند خطاهای چندگانه، دو یا بیشتر، را کشف کند.

۱۷. نشان دهید در هر کد هامینگ، هر کلمه کد ناصفر دارای وزن حداقل ۳ است.

۱۸. [برای حل این تمرین به دانش احتمال نیاز است] در (۵،۲) کد واقع در مثال ۸.۱۶، فرض کنید که احتمال انتقال خطا در یک تک رقم برابر ۰٫۰۱ باشد.

(الف) نشان دهید که احتمال انتقال یک تک کلمه کد بدون خطا ۰٫۹۵۰۹۹ است.

(ب) نشان دهید که احتمال انتقال یک ۱۰۰-کلمه پیام بدون خطا کمتر از ۰٫۰۱ است.

(پ) نشان دهید که احتمال انتقال یک تک کلمه کد با دقیقاً یک خطا ۰٫۴۸۰۳ است.

(ت) نشان دهید که احتمال این که یک کلمه کد توسط آرایه استاندارد واقع در مثال ۸.۱۶ کدگشایی شود لااقل ۰٫۹۹۹۲ است.

(ث) نشان دهید که احتمال این که یک ۱۰۰-کلمه پیام توسط آرایه استاندارد به درستی کدگشایی شود حداقل ۰٫۹۲ است. [با قسمت (ب) مقایسه کنید.]

۱۶-۳ کدهـای BCH [۱۷]

کدهای هامینگ که در بخش قبل ارائه شد دارای الگوریتم‌های کدگشای کارآمدی هستند که تمام خطاهای یگانه را اصلاح می‌کنند. همین مطلب برای BCH کدها که در اینجا ارائه می‌شود درست است، البته این کدها مفیدترند زیرا خطاهای چندگانه را هم اصلاح می‌کنند.

در ساختار یک BCH کد، از یک حلقهٔ متناهی استفاده می‌شود که گروه جمعی آن (یکریخت با) یک $B(n)$ است. هر ایده‌ال در چنین حلقه‌ای یک کد خطی است زیرا گروه جمعی آن (یکریخت با) یک زیرگروه جمعی $B(n)$ است. ساختار جبری دیگر (عمل ضرب) این حلقه الگوریتم‌های اصلاح ـ خطای کارآمدی برای این کد ارائه می‌کند.

این حلقه‌های مورد بحث به صورت زیر ساخته می‌شوند. گیریم n یک عدد صحیح مثبت باشد و $(x^n - ۱)$ ایده‌ال اصلی $\mathbb{Z}_۲[x]$ شامل تمام مضارب $x^n - ۱$ باشد. عناصر حلقه خارج قسمت $\mathbb{Z}_۲[x]/(x^n - ۱)$ کلاس‌های همنهشتی (هم‌مجموعه‌های) به پیمانه $(x^n - ۱)$ می‌باشند. طبق نتیجه ۵.۵، کلاس‌های همنهشتی متمایز $\mathbb{Z}_۲[x]/(x^n - ۱)$ در تناظر یک به یک با چندجمله‌ای‌هایی به صورت زیر است

$$a_۰ + a_۱x + a_۲x^۲ + \cdots + a_{n-۱}x^{n-۱} \qquad (*)$$

که در آن $a_i \in \mathbb{Z}_۲$.

هرچنین چندجمله‌ای دارای n ضریب است و دو امکان برای هر ضریب وجود دارد. بنابراین $\mathbb{Z}_۲[x]/(x^n - ۱)$ یک حلقه با ۲^n عضو است. به‌علاوه، n ضریب $(a_۰, a_۱, \ldots, a_{n-۱})$ از چندجمله‌ای $(*)$ می‌تواند به عنوان عنصری از گروه $B(n) = \mathbb{Z}_۲ \times \cdots \times \mathbb{Z}_۲$ در نظر گرفته شود.

قضیه ۱۲.۱۶. تابع $f : \mathbb{Z}_۲[x]/(x^n - ۱) \to B(n)$ که با

$$f([a_۰ + a_۱x + \cdots + a_{n-۱}x^{n-۱}]) = (a_۰, a_۱, \ldots, a_{n-۱})$$

داده شده است یک یکریختی گروههای جمعی است.

برهان. تمرین ۷. ■

---

۱۷) سه حرف BCH از حروف نخستین نام‌های Bose، Chaudhuri و Hocquenghem که این کدها را در سال‌های ۶۰-۱۹۵۹ ابداع کردند تشکیل شده است.

قضیه ۱۲.۱۶ نشان می‌دهد که هر ایده‌ال در $\mathbb{Z}_2[x]/(x^n-1)$ را می‌توان به عنوان یک کد خطی در نظر گرفت زیرا (تا حد یکریختی) یک زیرگروه $B(n)$ است. به ویژه، اگر $g(x) \in \mathbb{Z}_2[x]$، آنگاه کلاس همنهشتی (هم‌مجموعه) $g(x)$ یک ایده‌ال اصلی I در $\mathbb{Z}_2[x]/(x^n-1)$ را پدید می‌آورد. ایده‌ال I شامل تمام کلاس‌های همنهشتی به صورت $[h(x)g(x)]$ است که در آن $h(x) \in \mathbb{Z}_2[x]$. کدهای BCH از این نمونه می‌باشند.

برای تعریف یک BCH کد که t خطا را اصلاح کند یک عدد صحیح مثبت r انتخاب کنید به طوری که $t < 2^{r-1}$. گیریم $n = 2^r - 1$. آنگاه $g(x)$ با در نظر گرفتن یک میدان متناهی از مرتبه 2^r تعیین می‌شود، چنانکه در زیر شرح داده شده است.

مثال ۱۴.۱۶. قرارمی‌دهیم $t = 2$ و $r = 4$، پس $n = 2^4 - 1 = 15$. با پیدا کردن یک $g(x)$ مناسب، کدی در $\mathbb{Z}_2[x]/(x^{15}-1)$ می‌سازیم که تمام خطاهای دوگانه را اصلاح کند. برای انجام این امر به یک میدان از مرتبه $2^4 = 16$ نیاز می‌باشد.

چندجمله‌ای $1 + x + x^4$ در $\mathbb{Z}_2[x]$ تحویل‌ناپذیر است (تمرین ۳). بدین دلیل طبق قضیه ۹.۵ (و تذکرات بعد از آن) $\mathbb{K} = \mathbb{Z}_2[x]/(1 + x + x^4)$ میدانی از مرتبه ۱۶ است. طبق قضیه ۱۰.۵، $\mathbb{K}$ یک ریشه α از $1 + x + x^4$ را دارد. با استفاده از این واقعیت که

$$1 + \alpha + \alpha^4 = 0 \quad \text{و در نتیجه} \quad \alpha^{18} = 1 + \alpha,$$

می‌توانیم توان‌های α را محاسبه کنیم. برای مثال، $\alpha^6 = \alpha^4 \cdot \alpha^2 = (1+\alpha)\alpha^2 = \alpha^2 + \alpha^3$ به‌طریق مشابه، بدست می‌آوریم

$\alpha^1 = \alpha$	$\alpha^6 = \alpha^2 + \alpha^3$	$\alpha^{11} = \alpha + \alpha^2 + \alpha^3$
$\alpha^2 = \alpha^2$	$\alpha^7 = 1 + \alpha + \alpha^3$	$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3$
$\alpha^3 = \alpha^3$	$\alpha^8 = 1 + \alpha^2$	$\alpha^{13} = 1 + \alpha^2 + \alpha^3$
$\alpha^4 = 1 + \alpha$	$\alpha^9 = \alpha + \alpha^3$	$\alpha^{14} = 1 + \alpha^3$
$\alpha^5 = \alpha + \alpha^2$	$\alpha^{10} = 1 + \alpha + \alpha^2$	$\alpha^{15} = 1$

طبق قضیه ۷.۹ این عناصر متمایز و ناصفرند. بنابراین همه آنها عناصر ناصفر $\mathbb{K}$ می‌باشند و α یک مولد گروه ضربی $\mathbb{K}$ است.

۱۸) بخاطر آورید که در $\mathbb{Z}_2$، $-1 = 1$.

برای ساختن چندجمله‌ای $g(x)$، ابتدا چندجمله‌ای‌های کمین α، $\alpha^۲$، $\alpha^۳$، $\alpha^۴$ روی $\mathbb{Z}_۲$ را پیدا می‌کنیم. طبق ساختار $\mathbb{K}$، چندجمله‌ای کمین α، $m_۱(x) = ۱ + x + x^۴$ است. چندجمله‌ای $m_۱(x)$ چندجمله‌ای کمین $\alpha^۲$ و $\alpha^۴$ نیز هست، برای مثال طبق رویای سال‌اولی‌ها (لم ۲۴.۹)،

$$\begin{aligned} m_۱(\alpha^۲) &= ۱ + \alpha^۲ + (\alpha^۲)^۴ \\ &= ۱ + \alpha^۲ + (\alpha^۴)^۲ = (۱ + \alpha + \alpha^۴)^۲ = ۰^۲ = ۰. \end{aligned}$$

تحقیق کنید که چندجمله‌ای کمین $\alpha^۳$، $m_۳(x) = ۱ + x + x^۲ + x^۳ + x^۴$ است (تمرین۵). چندجمله‌ای $g(x)$ به صورت حاصل‌ضرب $m_۱(x)m_۳(x)$ تعریف می‌شود، بنابراین

$$\begin{aligned} g(x) &= (۱ + x + x^۴)(۱ + x + x^۲ + x^۳ + x^۴) \\ &= ۱ + x^۴ + x^۶ + x^۷ + x^۸ \in \mathbb{Z}_۲[x]. \end{aligned}$$

گیریم C ایده‌ال پدیدآمده توسط $[g(x)]$ در $\mathbb{Z}_۲[x]/(x^{۱۵} - ۱)$ باشد. آنگاه طبق قضیه ۱۲.۱۶، C یک کد می‌باشد. در زیر خواهیم دید که C یک $(۱۵, ۷)$ کد است که خطاهای یگانه و دوگانه را اصلاح می‌کند.

دقیقاً کلمه کدهای C چگونه بنظر می‌رسند؟ طبق نتیجه ۵.۵ هر رده همنهشتی در $\mathbb{Z}_۲[x]/(x^{۱۵} - ۱)$ رده یک چندجمله‌ای یکتا به صورت

$$a_۰ + a_۱x + a_۲x^۲ + \cdots + a_{۱۳}x^{۱۳} + a_{۱۴}x^{۱۴} \qquad (**)$$

است که در آن $a_i \in \mathbb{Z}_۲$. بنابراین، این رده را با این چندجمله‌ای نشان می‌دهیم[۱۹]. وقتی مناسب باشد، این چندجمله‌ای را (همچون قضیه ۱۲.۱۶) با عنصر $(a_۰, a_۱, \ldots, a_{۱۴}) = a_۰a_۱a_۲\cdots a_{۱۴}$ از $B(۱۵)$ یکی می‌گیریم. کلمه کدها، شامل رده‌های مضارب چندجمله‌ای $g(x)$ می‌باشد. برای مثال،

---

۱۹) این مشابه همان چیزی است که در بند قبل از مثال ۸.۲ فصل ۲ انجام گرفت، جایی که قرار شد یک عنصر (رده) $[k]$ از $\mathbb{Z}_n$ را با k نشان دهیم.

کلمه کد به صورت چندجمله‌ای	کلمه کد به صورت عضوی در $B(۱۵)$
$g(x) = ۱ + x^۴ + x^۶ + x^۷ + x^۸$	۱۰۰۰۱۰۱۱۱۰۰۰۰۰
$xg(x) = x(۱ + x^۴ + x^۶ + x^۷ + x^۸)$	
$= x + x^۵ + x^۷ + x^۸ + x^۹$	۰۱۰۰۰۱۰۱۱۱۰۰۰۰
$(۱ + x^۶)g(x) = ۱ + x^۴ + x^۷ + x^۸ + x^{۱۰}$	
$+ x^{۱۲} + x^{۱۳} + x^{۱۴}$	۱۰۰۰۱۰۰۱۱۰۱۰۱۱۱

اگر $g(x)$ در یک چندجمله‌ای $h(x)$ از درجه ≤ ۷ ضرب شود، آنگاه کلمه کد $h(x)g(x)$ درجه ≤ ۱۵ دارد و به صورت (**) نیست. برای مثال اگر $h(x) = x^۸$، آنگاه

$$h(x)g(x) = x^۸g(x) = x^۸(۱ + x^۴ + x^۶ + x^۷ + x^۸)$$
$$= x^۸ + x^{۱۲} + x^{۱۴} + x^{۱۵} + x^{۱۶}.$$

یک چندجمله‌ای به صورت (**) که رده آن برابر با ردهٔ $h(x)g(x)$ است، باقیمانده تقسیم $h(x)g(x)$ بر $x^{۱۵} - ۱$ می‌باشد (نتیجه ۵.۵ را ملاحظه کنید). تحقیق کنید که

$$h(x)g(x) = (۱ + x)(x^{۱۵} - ۱) + (۱ + x + x^۸ + x^{۱۲} + x^{۱۴}).$$

از اینرو $[h(x)g(x)]$ کلمه کد $۱ + x + x^۸ + x^{۱۲} + x^{۱۴}$ یا به طور معادل ۱۱۰۰۰۰۰۰۱۰۰۰۱۰۱ می‌باشد.

شیوه عمل این مثال به سادگی تعمیم می‌یابد. اگر t تعداد خطاهایی باشد که کد باید اصلاح کند، گیریم $n = ۲^r - ۱$، که در آن r طوری انتخاب شده است که $t < ۲^{r-۱}$ (در مثال بالا $t = ۲$، $r = ۴$). طبق نتیجه ۲۶.۹، یک میدان متناهی $\mathbb{K}$ از مرتبه ۲^r وجود دارد. طبق قضیه ۲۸.۹، $\mathbb{K} = \mathbb{Z}_۲(\alpha)$ که در آن α یک مولد گروه ضربی عناصر ناصفر $\mathbb{K}$ است (و بنابراین دارای مرتبه ضربی $n = ۲^r - ۱$ است). گیریم

$$m_۱(x), m_۲(x), m_۳(x), \ldots, m_{۲^r}(x) \in \mathbb{Z}_۲[x]$$

چندجمله‌ای‌های کمین عناصر

$$\alpha, \alpha^۲, \alpha^۳, \ldots, \alpha^{۲^r} \in \mathbb{K}$$

باشد. گیریم $g(x)$ حاصل‌ضرب چندجمله‌ای‌های متمایز در فهرست $m_1(x)$، $m_2(x)$، ...، $m_{24}(x)$ باشد.

ایده‌ال C پدیدآمده توسط $[g(x)]$ در $\mathbb{Z}_2[x]/(x^n - 1)$ را **کد BCH به طول n و فاصله طرح شده $2t + 1$** با **چندجمله‌ای مولد $g(x)$** گویند. بنابراین کد مثال اخیر یک BCH کد به طول ۱۵ و فاصله طرح شده ۵($= 1 + 2 \times 2$) می‌باشد. اگر $g(x)$ دارای درجه m باشد آنگاه تمرین ۱۴ نشان می‌دهد که کد C یک (n, k) کد است که در آن $k = n - m$.

قضیه ۱۳.۱۶. یک BCH کد به طول n و فاصله طرح شده $2t + 1$، t خطا را اصلاح می‌کند.

برهان. برهان این قضیه نیازمند آگاهی از دترمینان‌ها است؛ لیدل ـ پیلز[20] [۳۴؛ صفحه ۲۳۰] یا ماکیو[21] [۳۵؛ صفحه ۶۰] را ملاحظه کنید. ■

قضیه ۱۳.۱۶ نشان می‌دهد که BCH کدهایی وجود دارند که هر تعداد دلخواهی از خطاها را اصلاح می‌کنند. مهمتر این که از دیدگاه عملی، الگوریتم‌های مفیدی برای کدگشایی BCH کدهای بزرگ وجود دارد[22]. توصیف کامل این الگوریتم‌ها ما را از موضوع اصلی خیلی دور می‌کند. ولی در اینجا به صورت ساده ایده زیربنایی کارکرد اصلاح ـ خطا آمده است.

گیریم C یک BCH کد با فاصله طرح شدهٔ $2t + 1$ و چندجمله‌ای مولد $g(x)$ باشد. طبق تعریف $g(x)$، هرچندجمله‌ای کمین $m_i(x)$، $g(x)$ را می‌شمارد. از این جهت برای هر $i = 1, \ldots, 2t$، $g(\alpha^i) = 0$. اگر $[f(x)]$ یک کلمه کد در C باشد، آنگاه برای برخی $h(x)$، $f(x) = h(x)g(x)$ و بنابراین

$$f(\alpha^i) = h(\alpha^i)g(\alpha^i) = h(\alpha^i) \cdot 0 = 0.$$

برعکس، اگر $f(x) \in \mathbb{Z}_2[x]$ هر α^i را به عنوان یک ریشه داشته باشد، آنگاه طبق قضیه ۶.۹ هر $m_i(x)$، $f(x)$ را می‌شمارد. این ایجاب می‌کند که $g(x) \mid f(x)$ (تمرین ۸). بنابراین

(*) **$[f(x)]$ یک کلمه کد است اگر و تنها اگر برای هر $1 \leq i \leq 2t$، $f(\alpha^i) = 0$.**

۲۰) Lidl-Pilz

۲۱) Mackiw

۲۲) این یک دلیل کاربرد زیاد BCH کدهاست. برای مثال دستگاه ارتباطی بین اروپا و آن سوی اقیانوس اطلس از یک BCH کد با شرط $t = 6$ و $r = 8$ استفاده می‌کند. این کد یک $(255, 231)$ کد است که شش خطا را اصلاح می‌کند که در آن احتمال شکست ۱ در ۱۶ میلیون است.

کد گشا کلمه $a_0a_1\cdots a_k$ را دریافت می‌کند که (ردهٔ) چندجمله‌ای

$$r(x) = a_0 + a_1x + \cdots + a_kx^k$$

را نمایش می‌دهد. کد گشا این عضوهای میدان $\mathbb{K} = \mathbb{Z}_2(\alpha)$ را محاسبه می‌کند:

$$r(\alpha), r(\alpha^2), r(\alpha^3), \ldots, r(\alpha^{2t}).$$

اگر همه آنها صفر باشند، آنگاه طبق تذکرات بالا $r(x)$ یک کلمه کد است. اگر تعدادی از آن‌ها ناصفر باشند کدگشا (طبق روش مشخصی) از آنها استفاده می‌کند تا یک چندجمله‌ای $D(x) \in \mathbb{K}[x]$ بسازد، که چندجمله‌ای **مکان‌یاب-خطا** نامیده می‌شود. چون $\mathbb{K}$ متناهی است، ریشه‌های ناصفر $D(x)$ در $\mathbb{K}$ را با جایگذاری هر $\alpha^i \in \mathbb{K}$ در $D[x]$ می‌توان یافت.

اگر بیشتر از t خطا ایجاد نشود، ریشه‌های ناصفر $D(x)$ مکان‌های خطاهای انتقالی را بدست می‌دهد. برای مثال، اگر α^7 یک ریشه باشد آنگاه a_7 درکلمه دریافت شده $r(x)$ ناصحیح است، به طور مشابه اگر $\alpha^0 = 1$ یک ریشه باشد یک خطا در انتقال a_0 پیش آمده است.

اگر $D(x)$ در $\mathbb{K}$ ریشه نداشته باشد یا اگر تعداد معینی از $r(\alpha^i)$ها صفر باشند، به طوری که $D(x)$ را نتوان ساخت، آنگاه بیش از t خطا ایجاد شده است. بنابراین کد گشا فرآیندهای مجموعه‌ای (که وارد بحث آن نمی‌شویم) را دنبال می‌کند تا به دلخواه نزدیکترین کلمه کد به $r(x)$ را انتخاب کند.

مثال ۱۵.۱۶. در BCH-$(15,7)$ کد مثال قبل، فرض کنید این کلمه دریافت شده است،

$$r(x) = x + x^7 + x^8 = 010000011000000.$$

با استفاده از جدول واقع در مثال ۱۴.۱۶ و این واقعیت که برای هر $u \in \mathbb{K}$، $u + u = 0$ (تمرین ۱)، داریم

$$\begin{aligned} r(\alpha) &= \alpha + \alpha^7 + \alpha^8 = \alpha + (1 + \alpha + \alpha^3) + (1 + \alpha^2) \\ &= \alpha^2 + \alpha^3 = \alpha^6. \end{aligned}$$

$$\begin{aligned} r(\alpha^3) &= \alpha^3 + (\alpha^3)^7 + (\alpha^3)^8 \\ &= \alpha^3 + \alpha^{21} + \alpha^{24} = \alpha^3 + \alpha^6 + \alpha^9 \\ &= \alpha^3 + (\alpha^2 + \alpha^3) + (\alpha + \alpha^3) = \alpha + \alpha^2 + \alpha^3 = \alpha^{11}. \end{aligned}$$

تمرین ۶ نشان می‌دهد که

$$r(\alpha^{2}) = (r(\alpha))^{2} = (\alpha^{6})^{2} = \alpha^{12};$$
$$r(\alpha^{4}) = (r(\alpha))^{4} = (\alpha^{6})^{4} = \alpha^{24} = \alpha^{9}.$$

چندجمله‌ای مکان‌یاب ـ خطا با این فرمول (که در تمرین ۱۵ توجیه آن ارائه شده است) عرضه می‌شود:

$$D(x) = x^{2} + r(\alpha)x + \left(r(\alpha^{2}) + \frac{r(\alpha^{3})}{r(\alpha)}\right).$$

با استفاده از جدول واقع در مثال ۱۴.۱۶ می‌بینیم که

$$D(x) = x^{2} + \alpha^{6}x + (\alpha^{12} + \frac{\alpha^{11}}{\alpha^{6}}) = x^{2} + \alpha^{6}x + (\alpha^{12} + \alpha^{5})$$
$$= x^{2} + \alpha^{6}x + \alpha^{14}.$$

با جایگذاری هر یک از عناصر ناصفر $\mathbb{K}$ در $D(x)$، در می‌یابیم که

$$D(\alpha^{5}) = (\alpha^{5})^{2} + \alpha^{6}\alpha^{5} + \alpha^{14} = \alpha^{10} + \alpha^{11} + \alpha^{14}$$
$$= (1 + \alpha + \alpha^{2}) + (\alpha + \alpha^{2} + \alpha^{3}) + (1 + \alpha^{3}) = 0;$$
$$D(\alpha^{9}) = (\alpha^{9})^{2} + \alpha^{6}\alpha^{9} + \alpha^{14} = \alpha^{18} + \alpha^{15} + \alpha^{14} = \alpha^{3} + 1 + \alpha^{14}$$
$$= \alpha^{3} + 1 + (1 + \alpha^{3}) = 0.$$

بنابراین α^{5} و α^{9} ریشه‌های $D(x)$ می‌باشند، پس خطاها در ضرایب x^{5} و x^{9} پیش آمده‌است. کلمه دریافت شده

$$r(x) = x + x^{7} + x^{8} = 0100\underline{0}0\underline{1}1\underline{0}00000$$

به صورت زیر اصلاح می‌شود

$$c(x) = x + x^{5} + x^{7} + x^{8} + x^{9} = 0100\underline{1}0\underline{1}1\underline{1}00000,$$

که یک کلمه کد است (مثال ۱۴.۱۶ را ملاحظه کنید).

به طور مشابه، اگر $r(x) = x^۲ + x^۶ + x^۹ + x^{۱۰} = ۰۰۱۰۰۰۱۰۰۱۱۰۰۰۰$ دریافت شود، آنگاه $r(\alpha) = \alpha$، $r(\alpha^۲) = \alpha^۴$، $r(\alpha^۳) = \alpha^۹$ و

$$D(x) = x^۲ + r(\alpha)x + [r(\alpha^۲) + \frac{r(\alpha^۳)}{r(\alpha)}] = x^۲ + \alpha^۸x + (\alpha + \frac{\alpha^۹}{\alpha^۸})$$
$$= x^۲ + \alpha^۸x + (\alpha + \alpha) = x^۲ + \alpha^۸x = x(x + \alpha^۸)$$

تنها ریشه ناصفر $D(x)$، $\alpha^۸$ است، پس یک خطای یگانه در ضریب $x^۸$ پیش آمده است و کلمه صحیح

$$c(x) = x^۲ + x^۶ + x^۸ + x^۹ + x^{۱۰} = ۰۰۱۰۰۰۱۰۱۱۱۰۰۰۰$$

است. بالاخره، اگر $x + x^۴ + ۱$ دریافت شود، آنگاه

$$r(\alpha) = ۱ + \alpha + \alpha^۴ = ۰ \quad \text{و} \quad r(\alpha^۳) = ۱ + \alpha^۳ + \alpha^{۱۲} = \alpha^۵.$$

بنابراین $D(x)$ نمی‌تواند ساخته شود و نتیجه می‌گیریم که بیش از دو خطا پیش آمده است. به طور مشابه، اگر $x + x^۳ + ۱$ دریافت شود، آنگاه تحقیق کنید که $D(x) = x^۲ + \alpha^۷x + \alpha^۵$ و این که $D(x)$ در $\mathbb{K}$ هیچ ریشه‌ای ندارد. پس یکبار دیگر بیش از دو خطا پیش آمده است.

تمرینها

توجه. همواره (مگر خلاف آن ذکر شود) $\mathbb{K}$ میدان $\mathbb{Z}_۲[x]/(۱ + x + x^۴)$ از مرتبه ۱۶ است و α یک ریشه $x + x^۴ + ۱$ می‌باشد، همان‌طور که در مثال ۱۴.۱۶ آمده‌است.

A.۱. (الف) ثابت کنید که برای هر $f(x) \in \mathbb{Z}_۲[x]$، $f(x) + f(x) = ۰$.

(ب) ثابت کنید که برای هر u در میدان $\mathbb{K}$، $u + u = ۰$.

۲. نشان دهید که تنها چندجمله‌ای درجه دوم تحویل‌ناپذیر در $\mathbb{Z}_۲[x]$، $x^۲ + x + ۱$ است. [راهنمایی: تمام چندجمله‌ایهای درجه دوم را فهرست کنید و از نتیجه ۱۴.۴ استفاده کنید.]

۳. ثابت کنید که $x + x^۴ + ۱$ در $\mathbb{Z}_۲[x]$ تحویل‌ناپذیر است. [راهنمایی: تمرین ۲ و نتیجه ۱۴.۴.]

۴. ثابت کنید که چندجمله‌ای کمین $\alpha^{۵}$ روی $\mathbb{Z}_۲$، $۱ + x + x^۲$ است [از جدول واقع در مثال ۱۴.۱۶ استفاده کنید.]

۵. (الف) ثابت کنید چندجمله‌ای کمین $\alpha^{۳}$ روی $\mathbb{Z}_۲$، $۱ + x + x^۲ + x^۳ + x^۴$ است. [راهنمایی: تمرین ۲، نتیجه ۱۴.۴، و جدول واقع در مثال ۱۴.۱۶.]

(ب) ثابت کنید که $\alpha^{۴}$ نیز یک ریشه $۱ + x + x^۴$ است.

۶.B. اگر $f(x) \in \mathbb{Z}_۲[x]$ و α یک عضو در یک توسیع میدان $\mathbb{Z}_۲$ باشد، ثابت کنید که برای هر $k \geq ۱$، $f(\alpha^{۲k}) = f(\alpha^k)^۲$. [راهنمایی: لم ۲۴.۹.]

۷. (الف) نشان دهید که تابع $f : \mathbb{Z}_۲[x]/(x^n - ۱) \to B(n)$ با ضابطه

$$f([a_۰ + a_۱x + \cdots + a_{n-۱}x^{n-۱}]) = (a_۰, a_۱, \ldots, a_{n-۱})$$

پوشاست.

(ب) ثابت کنید که f یک همریختی از گروههای جمعی است.

(پ) ثابت کنید که f یک به یک است [راهنمایی: قضیه ۲۷.۷ با نماد جمعی.]

۸. (الف) گیریم $\mathbb{F}$ یک میدان باشد و $f(x) \in \mathbb{F}[x]$. اگر $p(x)$ و $q(x)$ تحویل‌ناپذیرهای تکین در $\mathbb{F}[x]$ باشند به طوری که $p(x)|f(x)$ و $q(x)|f(x)$، ثابت کنید که $p(x)q(x)|f(x)$. [راهنمایی: اگر $f(x) = q(x)h(x)$ آنگاه $p(x)|q(x)h(x)$؛ از قسمت ۲ قضیه ۸.۴ استفاده کنید.]

(ب) اگر $m_۱(x), m_۲(x), \ldots, m_k(x)$ تحویل‌ناپذیرهای تکین در $\mathbb{F}[x]$ باشند به طوری که $m_i(x)$، $f(x)$ را بشمارد، ثابت کنید که $g(x) = m_۱(x)m_۲(x)\cdots m_k(x)$، $f(x)$ را می‌شمارد.

۹. گیریم C، BCH-$(۱۵, ۷)$ کد مثال ۱۴.۱۶ باشد. از فن اصلاح ـ خطای ارائه شده در آنجا استفاده کنید تا این کلمه‌های دریافت‌شده را اصلاح و یا تعیین کنید که سه خطا یا بیشتر ایجاد شده است.

(الف) $۱ + x =$ ۱۱۰۰۰۰۰۰۰۰۰۰۰۰۰

(ب) $۱ + x^۳ + x^۴ + x^۵ =$ ۱۰۰۱۱۱۰۰۰۰۰۰۰۰۰

(پ) $1 + x^2 + x^4 + x^7 = 10101001000000$

(ت) $1 + x^6 + x^7 + x^8 + x^9 = 1000001111100000$.

۱۰. نشان دهید که چندجمله‌ای‌مولد برای BCH کد با شرط $t = 3$، $r = 4$، $n = 15$، چندجمله‌ای $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$ است. [تمرین‌های ۵-۳ می‌تواند مفید باشد.]

۱۱. گیریم $\mathbb{K} = \mathbb{Z}_2(\alpha)$ یک میدان متناهی از مرتبه 2^r باشد که گروه ضربی آن توسط α پدید آمده است. برای هر i، گیریم $m_i(x)$ چندجمله‌ای کمین α^i روی $\mathbb{Z}_2$ باشد. اگر $n = 2^r - 1$، ثابت کنید که هر $m_i(x)$، $x^n - 1$ را می‌شمارد. [راهنمایی: $\alpha^n = 1$ (چرا؟)؛ از قضیه ۶.۹ استفاده کنید.]

۱۲. اگر $g(x)$ چندجمله‌ای مولد یک BCH کد در $\mathbb{Z}_2[x]/(x^n - 1)$ باشد، ثابت کنید که $g(x)$، $x^n - 1$ را می‌شمارد. [راهنمایی: تمرینهای ۱۱ و ۸ (ب).]

۱۳. گیریم $g(x) \in \mathbb{Z}_2[x]$ یک شمارنده $x^n - 1$ باشد و گیریم C ایده‌آل اصلی پدیدآمده توسط $[g(x)]$ در $\mathbb{Z}_2[x]/(x^n - 1)$ باشد. آنگاه C یک کد است. ثابت کنید C دوری است، بدین معنی که C (با کلمه کدهایی که به صورت عضوهای $B(n)$ نوشته شده) دارای این خاصیت است: اگر $(c_0, c_1, \ldots, c_{n-1}) \in C$ آنگاه $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. [راهنمایی: $c_{n-1} + c_0 x + \cdots + c_{n-2}x^{n-1} = x(c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}) - c_{n-1}(x^n - 1)$.]

۱۴.C. گیریم C کد تمرین ۱۳ باشد. فرض کنید $g(x)$ دارای درجه m باشد و قرار دهید $k = n - m$. گیریم J مجموعه تمام چندجمله‌ای‌های $\mathbb{Z}_2[x]$ به صورت $a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1}x^{k-1}$ باشد.

(الف) ثابت کنید هر عضو C به صورت $[s(x)g(x)]$ است که در آن $s(x) \in J$. [راهنمایی: گیریم $h(x)g(x)] \in C$. طبق الگوریتم تقسیم، $h(x)g(x) = e(x)(x^n - 1) + r(x)$ که در آن $\deg r(x) < n$ و $[h(x)g(x)] = [r(x)]$. نشان دهید که $r(x) = s(x)g(x)$، که در آن $s(x) = h(x) - e(x)f(x)$ و $g(x)f(x) = x^n - 1$. از قضیه ۱.۴ استفاده کنید تا نشان دهید $s(x) \in J$.]

(ب) ثابت کنید C دارای مرتبهٔ 2^k است و بنابراین یک (n, k) کد است. [راهنمایی: نتیجه ۵.۵ را بکار برید تا نشان دهید که اگر $s(x) \neq t(x)$ در J، آنگاه $[s(x)g(x)] \neq [t(x)g(x)]$

در C. تعداد عناصر J چندتاست؟]

۱۵. گیریم C، BCH-$(۱۵,۷)$ کد مثال ۱۴.۱۶ باشد، که در آن کلمه کدها به صورت چندجمله‌ای‌هایی از درجه ≥ ۱۴ نوشته می‌شوند. فرض کنید کلمه کد $c(x)$ با خطاهای واقع در ضرایب x^i و x^j منتقل شده‌است و $r(x)$ دریافت شده است. آنگاه $D(x) = (x+\alpha^i)(x+\alpha^j) \in \mathbb{K}[x]$، که ریشه‌هایش α^i و α^j هستند، چندجمله‌ای مکان‌یاب ـ خطا می‌باشد. ضرایب $D(x)$ را بر حسب $r(\alpha)$، $r(\alpha^۲)$، $r(\alpha^۳)$ به صورت زیر بیان کنید.

(الف) نشان دهید که $r(x) - c(x) = x^i + x^j$.

(ب) نشان دهید که برای $k = ۱, ۲, ۳$، $r(\alpha^k) = \alpha^{ki} + \alpha^{kj}$. [گزارهٔ $(*)$ را در قضیه ۱۳.۱۶ ملاحظه کنید.]

(پ) نشان دهید که $D(x) = x^۲ + (\alpha^i + \alpha^j)x + \alpha^{i+j} = x^۲ + r(\alpha)x + \alpha^{i+j}$.

(ت) نشان دهید که $\alpha^{i+j} = r(\alpha^۲) + \frac{r(\alpha^۳)}{r(\alpha)}$. [راهنمایی: نشان دهید که

$$r(\alpha)^۳ = (\alpha^i + \alpha^j)^۳ = \alpha^{۳i} + \alpha^{۳j} + \alpha^{i+j}(\alpha^i + \alpha^j) = r(\alpha^۳) + r(\alpha)\alpha^{i+j}$$

و نسبت به α^{i+j} حل کنید، توجه کنید که $r(\alpha)^۲ = r(\alpha^۲)$.]

۱۶. نشان دهید که یک BCH کد با شرط $t = ۱$ در واقع یک کد هامینگ است. (بند بعد از مثال ۱۳.۱۶ را ملاحظه کنید).

* * * * *

پیوست الف
منطق و برهان

در اینجا خلاصه‌ای از حقایق اساسی در مورد منطق و برهان که برای مطالعه کتاب نیاز می‌باشد، آمده است. برای بحثی کامل از این موضوعات لوکاس[۲۳] [۱۰]، موراش[۲۴] [۱۱]، اسمیت ـ اِگن ـ سنت‌آندره[۲۵] [۱۲]، یا سولو[۲۶] [۱۳] را ملاحظه کنید.

یک **گزاره** جمله‌ای خبری است که می‌تواند درست و یا نادرست باشد. برای مثال هر کدام از این جملات یک گزاره است:

π یک عدد حقیقی است.

هر مثلث متساوی‌الساقین است.

---

۲۳) Lucas

۲۴) Morash

۲۵) Smith-Eggen-St. Andre

۲۶) Solow

سال گذشته ۱۰۳ عقاب سرسفید در ایالات متحده بدنیا آمده است.

توجه کنید که جمله آخر یک گزاره است اگرچه ممکن است قادر به تحقیق درستی یا نادرستی آن نباشیم. هیچ‌یک از جملات زیر یک گزاره نیست.

چه وقت است؟ آه!

گزاره‌های مرکب

ما اغلب با گزاره‌های مرکبی سروکار داریم که از گزاره‌های دیگر و با استفاده از رابط‌های "و" و "یا" تشکیل می‌شوند. ارزش راستی گزاره‌های مرکب بستگی به ارزش راستی مولفه‌های آن دارد. اگر P و Q گزاره باشند، آنگاه

"P و Q" یک گزاره درست است وقتی که P و Q هر دو درست باشند و در غیر این صورت نادرست است.

برای مثال،

π یک عدد حقیقی است و $۹ < ۱۰$

یک گزاره درست است زیرا هر دو مؤلفه‌اش درست است ولی

π یک عدد حقیقی است و $۱۸ = ۵ - ۷$

یک گزاره نادرست است زیرا یکی از مولفه‌هایش نادرست است.

در زبان انگلیسی رایج، کلمه "یا" اغلب به طور انحصاری، به معنی "یکی یا دیگری و نه هر دو" بکار می‌رود، مثل

او دست کم ۲۱ سال دارد یا او کمتر از ۲۱ سال دارد.

ولی "یا" می‌تواند به طور جامع، بدین معنی که "یکی یا دیگری یا احتمالاً هر دو" نیز بکار رود. مثل جمله

آنها، بازی اوّل یا بازی دوم را خواهند برد.

پس "یای" جامع دارای درست همان معنی "و / یا" در محاوره روزمره است. در *ریاضیات "یا" همواره در مفهوم جامع آن بکار می‌رود*، که احتمال این که هر دو مؤلفه درست باشند را مجاز می‌سازد، گرچه الزامی به آن نیست. در نتیجه، اگر P و Q گزاره باشند، آنگاه

P یا Q یک گزاره درست است وقتی که لااقل یکی از P یا Q درست باشد و نادرست است اگر هر دو P و Q نادرست باشند.

برای مثال

$$۵ < ۷ \quad \text{یا} \quad ۳ + ۸ = ۱$$

و

$$۵ < ۷ \quad \text{یا} \quad ۳ + ۸ = ۲۳$$

هر دو، گزاره‌های درست می‌باشند زیرا لااقل یک مؤلفه در هر حالت درست است، ولی

$$۲ > ۴ \quad \text{یا} \quad ۵ + ۳ = ۱۲$$

درست نیست، زیرا هر دو مؤلفه آن نادرست است.

نفی

نفی یک گزارهٔ P، گزاره "چنین نیست که P " می‌باشد که می‌توانیم به سادگی آن را به صورت " نفی‌P " خلاصه کنیم. بنابراین نفی گزاره

۷ یک عدد صحیح مثبت است،

گزاره "چنین نیست که ۷ یک عدد صحیح مثبت است" می‌باشد، که به صورت عادی به شکل ساده " ۷ یک عدد صحیح مثبت نیست" نوشته می‌شود. پس

نفی–P درست است دقیقاً وقتی که P نادرست باشد، و
نفی–P نادرست است دقیقاً وقتی که P درست باشد.

نفی گزاره "P و Q" گزاره "چنین نیست که P و Q " می‌باشد. حال "P و Q" درست است دقیقاً وقتی که P و Q هر دو درست باشد، پس گفتن، "چنین نیست که" به معنی این است که لااقل یکی از P یا Q نادرست است، ولی این دقیقاً وقتی اتفاق می‌افتد که لااقل نفی‌P یا نفی‌Q درست باشد. به این دلیل

نفی گزاره " P و Q " گزارهٔ "نفی‌P یا نفی‌Q" می‌باشد.

برای مثال، نفی

f پیوسته است و f در $x = ۵$ مشتق‌پذیر است،

گزاره زیر می‌باشد:

f پیوسته نیست یا f در $x = ۵$ مشتق‌پذیر نیست،

نفی گزاره " P یا Q " گزارهٔ "چنین نیست که P یا Q " می‌باشد. حال " P یا Q " درست است دقیقاً وقتی که لااقل یکی از P یا Q درست باشد. گفتن "چنین نیست که" به معنی آن است که P و Q هر دو نادرست می‌باشند. ولی P و Q هر دو نادرست هستند دقیقاً وقتی که نفی‌P و نفی‌Q هر دو درست باشند. بدین دلیل

نفی گزاره " P یا Q" گزاره "نفی‌P و نفی‌Q" می‌باشد.

برای مثال، نفی

۱۱۹ اول است یا $\sqrt{۳}$ یک عدد گویا است،

گزاره

۱۱۹ اول نیست و $\sqrt{۳}$ یک عدد گویا نیست

می‌باشد.

سـورهـا

بسیاری از گزاره‌های ریاضی شامل سورها می‌باشد. **سور عمومی** بیان می‌کند که یک خاصیت برای تمام اقلام مورد بحث درست می‌باشد. از نظر قواعد دستوری، سور عمومی را می‌توان به طرق مختلف بیان کرد، مثلاً

برای تمام اعداد حقیقی c، $c^۲ \neq -۱$.

هر عدد صحیح یک عدد حقیقی است.

همه اعداد صحیح گویا هستند

برای هر عدد حقیقی a، عدد $a^۲ + ۱$ مثبت است.

سور وجودی اظهار می‌دارد که لااقل یک شی با برخی خواص معین وجود دارد. برای مثال اعداد گویای مثبت وجود دارند.

یک عدد x وجود دارد به طوری که $x^۲ - ۵x + ۶ = ۰$.

یک عدد اول زوج وجود دارد.

در ریاضیات، کلمه "برخی" به معنای "لااقل یک" می‌باشد و در اصل یک سور وجودی است. برای مثال

برخی اعداد صحیح اول هستند

معادل است با این که بگوییم "لااقل یک عدد صحیح، اول می‌باشد" یعنی

یک عدد صحیح اول وجود دارد.

وقتی نفی گزاره‌های مشتمل بر سورها را تشکیل می‌دهیم باید احتیاط کنیم. برای مثال، نفی گزاره

تمام اعداد حقیقی گویا هستند

گزاره "چنین نیست که تمام اعداد حقیقی گویا هستند" می‌باشد، که به معنای آن است که لااقل یک عدد حقیقی وجود دارد که اصم (= غیرگویا) است. بنابراین نفی گزاره فوق عبارت است از

یک عدد حقیقی اصم وجود دارد.

بویژه، هیچ یک از گزاره‌های "تمام اعداد حقیقی گویا نیستند" و "تمام اعداد حقیقی اصم هستند" نفی گزاره "تمام اعداد حقیقی گویا هستند" نمی‌باشد. این مثال یک اصل کلی را طرح می‌کند:

نفی یک گـزاره با یک سـور عمومی
یک گزاره با یک سور وجودی می‌باشد.

نفی گزاره

یک عدد صحیح مثبت وجود دارد،

گزاره "چنین نیست که یک عدد صحیح مثبت وجود دارد" می‌باشد که به معنی "هر عدد صحیح نامثبت است" و یا به طور معادل "هیچ عدد صحیحی مثبت نیست" می‌باشد. بدین دلیل

نفی یک گزاره با یک سور وجودی
یک گزارهٔ با سور عمومی می‌باشد.

گزاره‌های شرطی و دوشرطی

در برهان‌های ریاضی اصولاً ما با **گزاره‌های شرطی** به صورت

اگر P، آنگاه Q

که به صورت نمادین $P \Rightarrow Q$ نوشته می‌شود، سروکار داریم. گزاره P را **فرض** یا **مقدمه** و Q را **حکم** می‌نامند. در اینجا چند مثال آمده است:

اگر c و d اعداد صحیح باشند، آنگاه cd یک عدد صحیح است.

اگر f در $x = ۳$ پیوسته باشد، آنگاه f در این نقطه مشتق‌پذیر است.

$a \neq ۰ \Rightarrow a^۲ > ۰$

چند قاعده دستوری متنوع وجود دارد که همهٔ آنها همان معنی "اگر P، آنگاه Q " را می‌دهند:

P نتیجه می‌دهد Q.

P برای Q کافی است.

Q مشروط به آنکه P.

Q وقتی که P.

در عرف معمول، گزاره "اگر P، آنگاه Q " بدین معنی است که درستی P، درستی Q را تضمین می‌کند، در نتیجه،

$P \Rightarrow Q$ یک گزاره درست است وقتی که P و Q هر دو درست باشند و نادرست است وقتی P درست و Q نادرست باشد.

یکی از مواردی که به‌ندرت پیش می‌آید این است که با گزاره‌ای به صورت $P \Rightarrow Q$ برخورد کنیم که در آن P نادرست باشد. برای مثال، این وعدهٔ انتخاباتی را ملاحظه کنید: "اگر من انتخاب شوم، آنگاه مالیات‌ها کاهش می‌یابد." اگر این نامزد انتخاب شود (P درست است)، درستی یا نادرستی این جمله وابسته به این است که آیا مالیات‌ها کاهش می‌یابند یا نه. ولی اگر او انتخاب نشود (P نادرست باشد) چه می‌شود؟ صرف‌نظر از این که برای مالیات‌ها چه اتفاقی خواهد افتاد، انصاف این است که به این وعدهٔ انتخاباتی نسبت دروغ ندهید. در نتیجه، چنین مرسوم است که در منطق نمادین این قاعده را بپذیریم:

وقتی P نادرست است، گزاره " $P \Rightarrow Q$ " درست می‌باشد.

عکس نقیض گزارهٔ شرطی " $P \Rightarrow Q$ " گزاره "نفی-P $\Rightarrow$ نفی-Q " است. برای مثال عکس نقیض گزاره زیر در مورد اعداد صحیح،

اگر c مضربی از ۶ باشد، آنگاه c زوج است

عبارت است از گزاره

اگر c زوج نباشد آنگاه c مضربی از ۶ نیست.

توجه داشته باشید که گزاره اصلی و عکس نقیض آن هر دو درست می‌باشند. دو گزاره را **هم‌ارز** گویند اگر درستی یکی معادل درستی دیگری باشد. ادعا می‌کنیم که

گزاره شرطی "$P \Rightarrow Q$" هم ارز با
عکس نقیض آن "نفی-P ⇒ نفی-Q " می‌باشد.

برای اثبات این هم‌ارزی، فرض کنید $P \Rightarrow Q$ درست باشد و گزاره نفی-$P \Rightarrow$ نفی-Q را در نظر بگیرید. فرض کنید نفی-Q درست باشد. آنگاه Q نادرست است. حال اگر P درست می‌بود لزوماً Q باید درست باشد، که چنین چیزی نیست. بنابراین P باید نادرست باشد، و از اینرو نفی-P درست می‌باشد. بدین دلیل نفی-$P \Rightarrow$ نفی-Q درست است. دلیلی مشابه نشان می‌دهد که وقتی نفی-$P \Rightarrow$ نفی-Q درست باشد، آنگاه $P \Rightarrow Q$ نیز درست است.

عکس گزاره شرطی " $P \Rightarrow Q$ " گزاره " $Q \Rightarrow P$ " می‌باشد. برای مثال عکس گزارهٔ

اگر b عدد حقیقی مثبت باشد، آنگاه b^2 عدد حقیقی مثبت است،

عبارت است از گزاره

اگر b^2 عدد حقیقی مثبت باشد آنگاه b عدد حقیقی مثبت است.

این گزاره اخیر نادرست است زیرا، برای مثال $(-3)^2$ عدد مثبت ۹ است، ولی ۳- مثبت نیست. بنابراین

عکس یک گزاره درست ممکن است نادرست باشد.

در برخی موارد یک گزاره شرطی و عکس آن هر دو درست می‌باشند برای مثال، گزاره

اگر عدد صحیح k فرد باشد، آنگاه عدد صحیح $k+1$ زوج است

درست است، همان‌طور که عکس آن

اگر عدد صحیح $k+1$ زوج باشد، آنگاه عدد صحیح k فرد است

درست می‌باشد. این واقعیت را می‌توانیم به اجمال با گفتن " k فرد است اگر و تنها اگر $k+1$ زوج باشد" بیان کنیم. به صورت کلی‌تر، گزاره

"P اگر و تنها اگر Q"

که به صورت "$P \iff Q$" خلاصه می‌شود، به معنی

$$P \Rightarrow Q \quad \text{و} \quad Q \Rightarrow P$$

می‌باشد. گزاره، "P اگر و تنها اگر Q" **گزاره دو شرطی** نامیده می‌شود. قوانین گزاره‌های مرکب نشان می‌دهد که " P اگر و تنها اگر Q " درست است دقیقاً وقتی که $P \Rightarrow Q$ و $Q \Rightarrow P$ درست باشند. در این حالت، درستی P درستی Q را نتیجه می‌دهد و بالعکس. بنابراین P درست است دقیقاً وقتی که Q درست باشد. به بیان دیگر "P اگر و تنها اگر Q" به معنی این است که P و Q گزاره‌های هم‌ارز می‌باشند.

قضیه و برهان

توسعه رسمی یک مبحث ریاضی با معرفی برخی اصطلاحات تعریف نشده و برخی **اصول** (گزاره‌هایی در مورد اصطلاحات تعریف نشده که فرض می‌شود درست باشند) حاکم بر آنها آغاز می‌گردد. با بکار بردن این اصطلاحات تعریف نشده و اصول حاکم بر آنها اصطلاحات جدید و قضایا (گزاره‌های درست در مورد اشیاء) ساخته می‌شوند. **برهان** یک قضیه بررسی کاملی از درستی گزاره آن است.

بیشتر قضایا گزاره‌های شرطی می‌باشند. قضیه‌ای که به صورت شرطی بیان نشده است اغلب هم‌ارز یک گزاره شرطی است. برای مثال، گزاره

هر عدد صحیح بزرگتر از ۱ حاصل‌ضربی از اعداد اول است،

هم‌ارز با گزاره زیر می‌باشد:

اگر n یک عدد صحیح و $n > 1$، آنگاه n حاصل‌ضربی از اعداد اول است.

اولین مرحله در اثبات قضیه‌ای که می‌توان آن را به صورت شرطی بیان کرد مشخص کردن فرض P و حکم Q می‌باشد. برای اثبات قضیه "$P \Rightarrow Q$" فرض P را درست قلمداد می‌کنیم و آنگاه با

استفاده از آن به همراه اصول، تعاریف و قضایایی که قبلاً ثابت شده‌اند استدلال می‌کنیم که حکم Q لزوماً درست است.

روشهای برهان

چند شگرد معمول در برهان قضایا در زیر توصیف شده است. گرچه که دانستن چنین شگردهایی مفید می‌باشد، امّا هیچ دستورالعمل متقن و سریعی وجود ندارد که فرآیندی دقیق برای اثبات هر گزاره ممکن ریاضی را عرضه کند. روشهایی که در اینجا بحث می‌شود در اصل نقشه‌هایی هستند که ما را در تجزیه و تحلیل قضیه و ساختن برهان آن راهنمایی می‌کند. داشتن یک نقشه نمی‌تواند همه مشکلات سفر را معلوم کند ولی معمولاً خط سیر را روشن‌تر و مسافرت را ساده‌تر می‌نماید.

روش مستقیم این روش برهان بر قاعده اساسی منطق که آن را *قیاس استثنایی* می‌نامند مبتنی است: اگر R گزاره‌ای درست و "$R \Rightarrow S$" یک گزاره شرطی درست باشد، آنگاه S گزاره‌ای درست است. برای اثبات قضیه "$P \Rightarrow Q$" با روش مستقیم، دنباله‌ای از گزاره‌های P_1، P_2، ...، P_n را پیدا می‌کنیم و درستی هر یک از *استلزام‌های* $P \Rightarrow P_1$، $P_1 \Rightarrow P_2$، $P_2 \Rightarrow P_3$، ...، $P_{n-1} \Rightarrow P_n$ و $P_n \Rightarrow Q$ را بررسی می‌نماییم. آنگاه فرض این که P درست است و استفاده مکرر از قیاس استثنایی نشان می‌دهد که Q درست است.

روش مستقیم رایج‌ترین روش برهان است. در عمل، ممکن است یافتن گزاره‌های متعدد میانی که پیشروی از P به Q را ممکن می‌سازد کار کاملاً مشکلی باشد. برای یافتن آنها بیشتر ریاضیدانان فرآیندی از تفکر را بکار می‌برند که بعضاً شگرد **جلو - عقب** نامیده می‌شود. ابتدا کار را با جلو رفتن آغاز می‌کنید و از خود می‌پرسید که من درباره فرض P چه می‌دانم؟ چه واقعیت‌هایی را نتیجه می‌دهد؟ از این واقعیتها چه گزاره‌هایی نتیجه می‌شود؟ و همین‌طور الی آخر. در این جا ممکن است فهرستی از گزاره‌های استنتاج شده توسط P داشته باشید که ارتباط آنها، در صورت وجود، با حکم Q هنوز روشن نباشد.

اکنون با پرسیدن این که چه واقعیت‌هایی درستی Q را تضمین می‌کنند، از Q به عقب برمی‌گردیم. چه گزاره‌هایی این واقعیت‌ها را نتیجه می‌دهند؟ و همین‌طور ادامه می‌دهیم. حال یک فهرست از گزاره‌هایی دارید که Q را نتیجه می‌دهند. این فهرست را با فهرست اول مقایسه کنید. اگر خوش‌شانس باشید گزاره‌ای خواهید یافت که متعلق به هر دو فهرست می‌باشد، و محتمل‌تر آنکه یک گزاره S در فهرست اول و یک گزاره T در فهرست دوم بیابید طوری که قادر باشید نشان دهید $S \Rightarrow T$. آنگاه

خواهید داشت $P \Rightarrow S$ و $S \Rightarrow T$ و $T \Rightarrow Q$، بنابراین $P \Rightarrow Q$.

وقتی شگرد جلو ـ عقب را با موفقیت برای یافتن برهانی برای $P \Rightarrow Q$ بکار بردید، باید برهان را به صورت پایان‌یافته‌اش بنویسید. این شکل پایان‌یافته ممکن است کاملاً از فرآیند تفکری که شما را به برهان هدایت کرد متفاوت باشد. فرآیند تفکر شما به جلو و عقب پرش داشت، ولی برهان نهایی معمولاً باید از P شروع شده و با ترتیب منطقی مرحله به مرحله از P به S بعد به T و نهایتاً به Q پیش رود. برهان پایان‌یافته باید فقط شامل آن واقعیت‌هایی که در برهان مورد نیاز است باشد. بسیاری از گزاره‌هایی که در فرآیند جلو ـ عقب ظاهر می‌گردد به استدلال نهایی بی‌ارتباط می‌باشد و نباید آنها را در برهان نهایی آورد. همان‌طورکه در بیشتر برهان‌های این کتاب نشان داده شده‌است، برهان نهایی به جای این که به شکل دنباله‌ای از گزاره‌های شرطی نوشته شود معمولاً به صورت داستان‌وار نوشته می‌شود.

روش عکس نقیض چون هرگزاره شرطی هم‌ارز عکس نقیضش می‌باشد، شما مجازید درستی "$P \Rightarrow Q$" را با اثبات نفی‌ـ $P \Rightarrow$ نفی‌ـQ نتیجه گیری کنید. "$P \Rightarrow Q$" درست است. برای مثال، بجای اثبات این که برای یک تابع معین f،

$$\text{اگر } a \neq b \text{ ، آنگاه } f(a) \neq f(b)$$

می‌توانید عکس نقیض آن یعنی

$$\text{اگر } f(a) = f(b) \text{ ، آنگاه } a = b$$

را ثابت کنید.

برهان خلف فرض کنید که درستی یک گزاره R را پذیرفته‌اید و استدلال معتبری ارائه دهید که $R \Rightarrow S$ (یعنی $R \Rightarrow S$ یک گزاره درست است). اگر گزاره S در واقع یک گزاره نادرست باشد، تنها یک نتیجه‌گیری ممکن وجود دارد: گزاره اصلی Rباید نادرست باشد، زیرا درستی مقدمه R و درستی گزاره $R \Rightarrow S$ طبق قیاس استثنایی منجر به درستی S می‌شود.

برای این که این واقعیت را برای اثبات قضیه "$P \Rightarrow Q$" بکار برید، طبق معمول فرض کنید که P یک گزاره درست باشد. آنگاه بحث بند قبل را با شرط "نفی‌ـ$Q = R$ " بکار برید. به بیان دیگر، فرض کنید که نفی‌ـQ درست است و استدلالی ارائه دهید (احتمالاً با استفاده از P و نتایجی که قبلاً ثابت شده است) که نشان دهد $S \Rightarrow$ نفی‌ـQ، که در آن S گزاره‌ای است که می‌دانیم نادرست است. نتیجه می‌گیریم که نفی‌ـQ باید نادرست باشد. ولی نفی‌ـQ نادرست است دقیقاً وقتی که

Q درست باشد. بنابراین Q درست است و ما ثابت کرده‌ایم که $P \Rightarrow Q$. باز هم، معمولاً قسمت مشکل یافتن گزاره S خواهد بود و ثابت کردن این که نفی‌ـQ، S را نتیجه می‌دهد.

مثال ۱. بخاطر آورید که یک عدد صحیح زوج است اگر مضربی از ۲ باشد و بخاطر آورید که عددی که زوج نباشد را فرد گویند. برهان خلف را بکار می‌بریم تا گزاره زیر را ثابت کنیم:

اگر m^2 زوج باشد، آنگاه m زوج است.

در اینجا P گزاره "m^2 زوج است" و Q گزاره "m زوج است" می‌باشد. به خلاف فرض می‌کنیم "m زوج نیست" یا به طور معادل "m فرد است" (گزاره نفی‌ـQ). ولی هر عدد فرد یک واحد بیشتر از یک عدد زوج است. چون هر عدد صحیح زوج مضربی از ۲ است، باید برای برخی k داشته باشیم $m = 2k + 1$. آنگاه قوانین اساسی حساب نشان می‌دهد که

$$m^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

این گزاره اخیر می‌گوید که m^2 یک واحد بیشتر از مضربی از ۲ است، یعنی m^2 فرد است. ولی فرض ما این بود که m^2 زوج است (گزاره P)، و بدین دلیل "m^2 تواماً زوج و فرد می‌باشد" (گزاره S). این گزاره نادرست است زیرا هیچ عدد صحیحی تواماً زوج و فرد نیست. بنابراین فرض اصلی ما (نفی‌ـQ) به یک تناقض منجر شده است (گزاره نادرست S) در نتیجه نفی‌ـQ باید نادرست باشد، و از اینرو گزاره "m زوج است" (گزارهٔ Q) درست است.

در مثال قبل گزاره‌های مختلف با حروف نمایه‌گذاری شده‌اند در نتیجه شما به سادگی این مثال را با مبحث کلی ربط می‌دهید. این امر در استدلال‌های با برهان خلف معمولاً چنین نیست و چنین برهانهایی مانند مثال فوق مشروحاً عرضه نمی‌شوند.

انتخاب یک روش برهان تا حدّی سلیقه‌ای و تا حدی مربوط به کارآمد بودن آن می‌باشد. اگرچه هر یک از روش‌هایی که در بالا فهرست شد را می‌توان بکار برد، اما بسته به شرایط، یک روش ممکن است برای حصول نتیجه به راه خیلی کوتاهتر یا ساده‌تر از دیگری منجر شود. به علاوه روش‌های برهانی مشخصی وجود دارد که قابل بکار بردن برای نمونه‌های معینی از گزاره‌ها هستند.

برهان با استقراء این روش به تفصیل در پیوست پ مورد بحث قرارگرفته است.

روش ساختاری این روش برای قضایایی مناسب است که متضمن گزاره‌ای به صورت "وجود دارد یک ـ چنین و ـ چنان با خاصیت چنین و چنان" می‌باشد. برای مثال

یک عدد صحیح d وجود دارد به قسمی که $d^2 - 4d - 5 = 0$.

اگر r و s اعداد گویای متمایز باشند، آنگاه یک عدد گویا بین r و s وجود دارد.

اگر r یک عدد حقیقی مثبت باشد،

آنگاه یک عدد صحیح مثبت m وجود دارد به طوری که $\frac{1}{m} < r$.

برای اثبات چنین گزاره‌هایی، باید یک شی با خاصیت مورد نظر را ساخت (پیدا کرد، بوجود آورد، حدس زند و امثال آن). وقتی برهان چنین گزاره‌ای را مطالعه می‌کنید، فقط لازم است تحقیق کنید که شئ ارائه شده در برهان در واقع دارای خاصیت اظهار شده می‌باشد. یک برهان وجودی ممکن است به چیزی بیشتر از عرضه یک مثال نیانجامد (برای مثال، ارائه عدد صحیح ۲ برهانی برای گزاره "یک عدد صحیح مثبت وجود دارد"، عرضه می‌کند). ولی اغلب به استدلالی غیربدیهی برای ایجاد شئ مورد سوال نیاز می‌باشد.

هشدار اگرچه ارائه یک مثال برای اثبات یک گزاره وجودی کافی است، ولی ارائه چند مثال هرگز گزاره‌ای که به طور مستقیم یا غیرمستقیم شامل یک سور عمومی است را ثابت نمی‌کند. برای مثال، اگر حتی یک میلیون عدد صحیح داشته باشید که در گزاره

اگر c عدد صحیح باشد، آنگاه $c^2 - c + 11$ عددی اول است

صدق کند، باز هم این را اثبات نکرده‌اید. زیرا این گزاره، در اصل، اظهار می‌کند که برای هر عدد صحیح c، یک عدد صحیح معین دیگر اول است. وقتی که $c = 12$ این موضوع درست نیست زیرا $11 \times 13 = 143 = 11 + 12 - 12^2$. بنابراین گزاره نادرست است. این مثال به وضوح نشان می‌دهد که

یک مثال نقض برای رد یک گزاره کافی است.

اصل مطلب این است که وقتی مطمئن نیستید که یک گزاره درست است، سعی کنید مثال‌هایی در تأیید و یا رد آن پیدا کنید. اگر تنها یک مثال پیدا کنید که گزاره برقرار نباشد، آن را رد کرده‌اید. با این حال اگر فقط مثال‌هایی در تأیید درستی گزاره پیدا کنید شما آن را ثابت نکرده‌اید، ولی قرینه دلگرم کننده‌ای مبنی بر درستی آن در اختیار دارید.

برهان گزاره‌های چندشرطی

برای این که گزارهٔ دوشرطی " P اگر و تنها اگر Q " را ثابت کنید، باید هر دو گزاره "$P \Rightarrow Q$" و "$Q \Rightarrow P$" را ثابت کنید. اثبات یکی از این گزاره‌ها و عدم اثبات دیگری یک اشتباه رایج در بین دانشجویان است. برای مثال گزاره

مثلثی به اضلاع a، b، c مثلثی قائم‌الزاویه
به وتر c است اگر و تنها اگر $c^2 = a^2 + b^2$

دارای دو قسمت مجزا است. اول باید فرض کنید که یک مثلث قائم‌الزاویه به اضلاع a و b و وتر c دارید و ثابت کنید که $c^2 = a^2 + b^2$. آنگاه باید دلیل دیگری عرضه کنید: فرض کنید که اضلاع مثلثی در رابطه $c^2 = a^2 + b^2$ صدق می‌کند و ثابت کنید که این مثلث یک مثلث قائم‌الزاویه به وتر c است.

گزاره‌ای به صورت

شرایط زیر هم‌ارزند: $\boldsymbol{P}$، $\boldsymbol{Q}$، $\boldsymbol{R}$، $\boldsymbol{S}$، $\boldsymbol{T}$

یک **گزارهٔ چند شرطی** نامیده می‌شود و بدین معنی است که هر یک از گزاره‌های P، Q، R، S، یا T هر یک از گزاره‌های دیگر را نتیجه می‌دهد. بنابراین یک گزاره چندشرطی دقیقاً خلاصه‌ای برای یک فهرست از گزاره‌های دو شرطی؛ $P \iff Q$ و $P \iff R$ و $P \iff S$ و $P \iff T$ و $R \iff Q$ و $S \iff Q$ و امثال آن می‌باشد. برای اثبات این گزارهٔ چندشرطی فقط لازم است ثابت کنید که

$$P \Rightarrow Q, \quad Q \Rightarrow R, \quad R \Rightarrow S, \quad S \Rightarrow T, \quad T \Rightarrow P.$$

آنگاه تمام استلزام‌های مورد نیاز دیگر سریعاً نتیجه می‌شود. برای مثال از $T \Rightarrow P$ و $P \Rightarrow Q$ می‌دانیم که $T \Rightarrow Q$، و همین‌طور حالت‌های دیگر نتیجه می‌شود.

مثال ۲. می‌خواهیم قضیه زیر را در مورد اعداد صحیح ثابت کنیم:

شرایط زیر درباره یک عدد صحیح p هم‌ارزند:

(۱) p اول است.

(۲) اگر p یک عامل ab باشد، آنگاه p یک عامل a یا یک عامل b است.

(۳) اگر $p = rs$، آنگاه $r = \pm ۱$ یا $s = \pm ۱$.

باید سه دلیل جداگانه اقامه کنید. اول (۱) را فرض کنید و (۲) را ثابت کنید، بنابراین (۱) $\Leftarrow$ (۲) درست است. دوم (۲) را فرض کنید و (۳) را ثابت کنید، پس (۲) $\Leftarrow$ (۳) درست است. بالاخره، (۳) را باید فرض کنید و (۱) را ثابت کنید، بنابراین (۳) $\Leftarrow$ (۱) درست است. **دقت کنید:** در هر مرحله فقط یکی از سه گزاره را فرض می‌کنید و از آن استفاده می‌کنید تا دیگری را ثابت کنید، گزاره سوم در این قسمت استدلال نقشی ندارد.

* * * * *

پیوست ب

مجموعه‌ها و توابع

برای اهداف مورد نظر ما، یک **مجموعه** گردایه‌ای دلخواه از اشیاء است؛ برای مثال،

مجموعه $\mathbb{Z}$ از اعداد صحیح.

مجموعه مثلث‌های قائم‌الزاویه به مساحت ۲۴.

مجموعه تمام اعداد اصم مثبت.

اشیاء واقع در یک مجموعه **عناصر یا اعضاء** مجموعه نامیده می‌شوند. اگر B یک مجموعه باشد، گزاره "b عضوی از B است" را به طور اختصار با "$b \in B$" نشان می‌دهند و به طور مشابه گزاره "b عضوی از B نیست" به اختصار به صورت "$b \notin B$" نوشته می‌شود. برای مثال، اگر $\mathbb{Z}$ مجموعه اعداد صحیح باشد[۲۷]، آنگاه

$$۲ \in \mathbb{Z} \quad \text{و} \quad \pi \notin \mathbb{Z}.$$

۲۷) در سرتاسر این کتاب نماد $\mathbb{Z}$ همیشه مجموعه اعداد صحیح را نشان می‌دهد.

روشهای گوناگونی برای توصیف مجموعه‌ها وجود دارد. یک مجموعه را همچون مثال‌های فوق می‌توان توصیف لفظی کرد. یک مجموعه متناهی (باپایان) کوچک را می‌توان با فهرست کردن عناصرش توصیف کرد. چنین فهرستی معمولاً بین دو آکولاد قرار می‌گیرد، برای مثال

$$\{۳, ۷, -۴, ۹\} \quad \text{یا} \quad \{a, b, c, r, s, t\}.$$

مجموعه‌های نامتناهی (بی‌پایان) را نیز می‌توان با فهرست کردن عناصرشان نشان داد. برای مثال $\{۲, ۴, ۶, ۸, \ldots\}$ مجموعه تمام اعداد صحیح مثبت زوج را نشان می‌دهد. البته این طرز نمایش یک مجموعه نامتناهی مبهم است زیرا به این بستگی دارد که آیا همه الگوی واحدی را از آن برداشت می‌کنند، و این که آیا این مجموعه برای همیشه ادامه دارد. البته وقتی سیاق عبارت روشن باشد هیچ ابهامی پیش نخواهد آمد.

بالاخره، یک مجموعه را می‌توان برحسب خواصی که منحصر به عناصر آن است توصیف کرد. این معمولاً با نماد **مجموعه‌ـ ساز** انجام می‌گیرد. برای مثال،

$$\{x \mid x \text{ یک عدد صحیح است و } x > ۹\}$$

مجموعه تمام عضوهای x ای که x یک عدد صحیح بزرگتر از ۹ می‌باشد را نشان می‌دهد. در حالت کلی نماد خط قائم " | " را می‌خوانیم "به طوری که" و نماد "$\{y \mid P\}$" را می‌خوانیم "مجموعه تمام عضوهای y به طوری که P ". بدین دلیل هر یک از مجموعه‌های زیر مجموعه اعداد صحیح زوج می‌باشد:

$\{x \mid x$ یک عدد صحیح زوج است $\}$.

$\{t \mid t \in \mathbb{Z}$، t زوج است$\}$.

$\{r \mid r \in \mathbb{Z}$، r مضربی از ۲ است$\}$.

$\{y \mid y \in \mathbb{Z}$، $y = ۲k$ برای یک عدد صحیح زوج $k\}$.

مجموعه تهی

در بعضی موارد نماد مجموعه ـ ساز به ایجاد مجموعه‌ای غیرعادی می‌انجامد. برای مثال، مجموعه

$$\{x \mid x \text{ عددی صحیح است و } ۰ < x < ۱\}$$

هیچ عضوی ندارد زیرا هیچ عدد صحیحی بین ۰ و ۱ وجود ندارد. مجموعه‌ای که دارای هیچ عضوی نیست را **مجموعه تهی** یا **پوچ** می‌نامند و با $\emptyset$ نمایش می‌دهند. برای هر عضو c،

$$c \in \emptyset \text{ نادرست است و } c \notin \emptyset \text{ درست است.}$$

در اختیار داشتن مفهومی به نام مجموعه تهی بسیار مناسب است، لکن زمانی که با قضیه‌هایی سروکار داریم که فقط برای مجموعه‌های ناتهی (یعنی مجموعه‌هایی که حداقل یک عضو دارند) درستند باید کمی دقت بخرج دهیم.

زیرمجموعه‌ها

یک مجموعه B **زیرمجموعهٔ** یک مجموعه C گفته می‌شود (نوشته می‌شود $B \subseteq C$) مشروط به آن که هر عضو B عضو C نیز باشد. به بیان دیگر $B \subseteq C$ دقیقاً وقتی که این گزاره درست باشد:

$$x \in B \Rightarrow x \in C.$$

برای مثال، مجموعه اعداد صحیح زوج یک زیرمجموعه از تمام اعداد صحیح $\mathbb{Z}$ می‌باشد، و مجموعه اعداد گویا زیرمجموعه‌ای از مجموعهٔ اعداد حقیقی است.

تعریف "$B \subseteq C$" امکان $B = C$ را مجاز می‌سازد (زیرا مسلماً در این حالت هر عضو B عضو C نیز می‌باشد). به بیان دیگر،

$B \subseteq B$ برای هر مجموعه B.

اگر B یک زیرمجموعه C و $B \neq C$ باشد، گوییم **B یک زیرمجموعه سره C** است و می‌نویسیم $B \subsetneq C$.

به سادگی می‌توان دید که رابطه زیر مجموعه بودن متعدی است، یعنی

اگر $B \subseteq C$ و $C \subseteq D$ ، آنگاه $B \subseteq D$.

دو مجموعه B و C **برابر** می‌باشند وقتی که دقیقاً دارای عناصر یکسانی باشند. در این حالت هر عضو B عضوی از C می‌باشد و هر عضو C عضوی از B است. از این جهت

$B = C$ اگر و تنها اگر $B \subseteq C$ و $C \subseteq B$.

این واقعیت عمومی‌ترین روش مورد استفاده برای اثبات تساوی دو مجموعه می‌باشد، یعنی اثبات این که هر کدام زیرمجموعه دیگری است.

استلزام‌های منطقی، به واقعیت اعجاب‌انگیزی در مورد مجموعه تهی می‌انجامد. چون گزاره $x \in \emptyset$ همواره نادرست است، استلزام

$$x \in \emptyset \Rightarrow x \in C$$

همواره درست است (**پیوست الف** را ملاحظه کنید). ولی این دقیقاً تعریف "$\emptyset$ زیرمجموعه C است" می‌باشد. بنابراین

مجموعه $\emptyset$ زیرمجموعه هر مجموعه می‌باشد.

اَعمال روی مجموعه‌ها

اکنون طرق متعارف ساختن مجموعه‌های جدید از مجموعه‌های مفروض را مطالعه می‌کنیم. اگر B و C مجموعه باشند، آنگاه **مکمل نسبی** C در B با $B - C$ نمایش داده می‌شود وشامل تمام عناصری از B است که در C نمی‌باشد. از اینرو

$$B - C = \{x \mid x \in B, x \notin C\}.$$

برای مثال، اگر E مجموعه اعداد صحیح زوج باشد، آنگاه $\mathbb{Z} - E$ مجموعه اعداد صحیح فرد است.

اشتراک مجموعه‌های B و C شامل تمام عناصری است که در هر دو B و C باشد و با $B \cap C$ نمایش داده می‌شود. بدین دلیل

$$B \cap C = \{x \mid x \in B \quad و \quad x \in C\}.$$

برای مثال اگر $B = \{-۲, ۱, \sqrt{۲}, ۵, \pi\}$ و C مجموعه اعداد گویای مثبت باشد، آنگاه $B \cap C = \{۱, ۵\}$، زیرا ۱ و ۵ تنها عناصری هستند که در هر دو مجموعه می‌باشند. اگر B مجموعه اعداد صحیح مثبت و C مجموعه اعداد صحیح منفی باشد آنگاه $B \cap C = \emptyset$، چون هیچ عضوی در هر دو مجموعه نمی‌باشد. وقتی B و C مجموعه‌هایی باشند که $B \cap C = \emptyset$، گوییم B و C **متمایزند**.

اجتماع مجموعه‌های B و C تمام عناصری را شامل است که لااقل در یکی از B یا C باشد و با $B \cup C$ نشان داده می‌شود. از این جهت

$$B \cup C = \{x \mid x \in B \quad یا \quad x \in C\}.$$

مثلاً، اجتماع $B = \{1,3,5,7\}$ و $C = \{-1,1,4,9\}$، $B \cup C = \{-1,1,3,4,5,7,9\}$ می‌باشد. اگر B مجموعه اعداد گویا و C مجموعه اعداد غیرگویا باشد، آنگاه $B \cup C$ مجموعه تمام اعداد حقیقی است. تحقیق کنید که اجتماع و اشتراک دارای خواص زیر می‌باشد. برای مجموعه‌های دلخواه B، C و D:

$$
\begin{aligned}
&B \cap B = B && B \cup B = B \\
&B \cup \emptyset = B && B \cap \emptyset = \emptyset \\
&B \cup C = C \cup B && B \cap C = C \cap B \\
&B \subseteq B \cup C && B \cap C \subseteq B \\
&B \subseteq C \quad \text{اگر و تنها اگر} && B \cup C = C \qquad (*) \\
&B \subseteq C \quad \text{اگر و تنها اگر} && B \cap C = B
\end{aligned}
$$

$$
\begin{aligned}
&B \cup (C \cup D) = (B \cup C) \cup D \\
&B \cap (C \cap D) = (B \cap C) \cap D \\
&B \cap (C \cup D) = (B \cap C) \cup (B \cap D) \\
&B \cup (C \cap D) = (B \cup C) \cap (B \cup D).
\end{aligned}
$$

مفاهیم اجتماع و اشتراک به سادگی به گردایه‌های بزرگ، احتمالاً نامتناهی، تعمیم می‌یابد. فرض کنید I یک مجموعه ناتهی (که مجموعه **نمایه‌گذار** نامیده می‌شود) باشد و فرض کنید که برای هر $i \in I$ مجموعه A_i داده شده باشد. آنگاه اشتراک این خانواده از مجموعه‌ها (که با $\bigcap_{i \in I} A_i$ نمایش داده می‌شود) مجموعه آن عناصری است که در همه مجموعه‌های A_i می‌باشد، یعنی،

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \quad \text{برای هر } i \in I\}.$$

به طور مشابه اجتماع این خانواده (که با $\bigcup_{i \in I} A_i$ نمایش داده می‌شود) مجموعه آن عناصری است که لااقل در یکی از مجموعه‌های A_i می‌باشد، یعنی،

$$\bigcup_{i \in I} A_i = \{x \in A \mid x \in A_i \quad \text{برای برخی } i \in I\}.$$

ضرب دکارتی مجموعه‌های B و C با $B \times C$ نمایش داده می‌شود و شامل تمام زوجهای مرتب (x, y) با شرط $x \in B$ و $y \in C$ می‌باشد. تساوی زوجهای مرتب با قانون:

$$(x, y) = (u, v) \quad \text{اگر و تنها اگر} \quad x = u, \quad y = v,$$

تعریف می‌شود. برای مثال اگر $B = \{r, s, t\}$ و $C = \{۵, ۷\}$، آنگاه $B \times C$ مجموعه

$$\{(r, ۵), (r, ۷), (s, ۵), (s, ۷), (t, ۵), (t, ۷)\}$$

می‌باشد. گاهی مجموعه اعداد حقیقی $\mathbb{R}$ را با محور حقیقی در دستگاه مختصات یکی می‌گیریم. وقتی این کار انجام شود، ضرب دکارتی $\mathbb{R} \times \mathbb{R}$ همان صفحه مختصات معمولی، مجموعه همه نقاط با مختصات (x, y) که در آن $x, y \in \mathbb{R}$، می‌باشد.

ضرب دکارتی هر تعدادی متناهی مجموعه‌های $B_۱$، $B_۲$، ...، B_n به طریق مشابه تعریف می‌شود. $B_۱ \times B_۲ \times \cdots \times B_n$ مجموعه تمام n–تایی‌های مرتب $(x_۱, x_۲, \ldots, x_n)$ است که در آن برای هر $i = ۱, \ldots, n$، $x_i \in B_i$. برای مثال، اگر $B = \{۰, ۱\}$، $\mathbb{Z}$ مجموعه اعداد صحیح باشد، و $\mathbb{R}$ مجموعه اعداد حقیقی باشد، آنگاه $B \times \mathbb{Z} \times \mathbb{R}$ مجموعه تمام سه‌تایی‌های مرتب به صورت $(۰, k, r)$ و $(۱, k, r)$ است که در آن $k \in \mathbb{Z}$ و $r \in \mathbb{R}$. حاصلضرب $B \times \mathbb{Z} \times \mathbb{R}$ یک مجموعه نامتناهی می‌باشد، سه تایی‌های $(۳, -۵, ۰)$، $(\pi, ۲۴, ۱)$، و $(-\sqrt{۳}, ۱, ۱)$ از جمله عضوهای آن می‌باشند.

توابع

یک **تابع** (یا **نگاشت**) f از یک مجموعه B به یک مجموعه C (که با $f : B \to C$ نشان داده می‌شود) ضابطه یا دستوری است که به هر عضو b از B دقیقاً یک عضو c از C را متناظر می‌کند: عضو c **تصویر** b یا **مقدار** تابع f در b نامیده می‌شود و معمولاً با $f(b)$ نشان داده می‌شود. مجموعه B **دامنه** و مجموعه C **برد** تابع f نامیده می‌شود.

درس‌های ریاضی قبلی شما با گونه‌های وسیعی از توابع سروکار داشته است. برای مثال، اگر $\mathbb{R}$ مجموعه اعداد حقیقی باشد، آنگاه هر یک از ضابطه‌های زیر تابعی از $\mathbb{R}$ به $\mathbb{R}$ تعریف می‌کند:

$$f(x) = \cos x \quad ،g(x) = x^۲ + ۱ \quad ،h(x) = x^۳ - ۵x + ۲.$$

ضابطه یک تابع لازم نیست با یک فرمول جبری ارائه شود، برای مثال تابع $f : \mathbb{Z} \to \{0, 1\}$ با ضابطه

$$f(x) = 0 \text{ اگر } x \text{ زوج باشد و } f(x) = 1 \text{ اگر } x \text{ فرد باشد،}$$

را در نظر بگیرید. اگر B یک مجموعه باشد، آنگاه تابعی از B به B را که هر عضو B را به خود آن عضو می‌نگارد، **نگاشت همانی** روی B می‌نامند و با ι_B نشان می‌دهند. بنابراین $\iota_B : B \to B$ توسط

$$\iota_B(x) = x \quad \text{برای هر } x \in B$$

تعریف می‌شود.

ترکیب توابع

گیریم f و g توابعی باشند به طوری که برد f با دامنه g یکسان باشد، مثلاً $f : B \to C$ و $g : C \to D$. آنگاه ترکیب f و g تابع $h : B \to D$ است با ضابطه:

$$h(x) = g(f(x)).$$

به بیان دیگر، تابع مرکب ابتدا با بکار بردن f و سپس با بکار بردن g حاصل می‌شود،

$$B \xrightarrow{f} C \xrightarrow{g} D$$

$$x \longmapsto f(x) \longmapsto g(f(x)).$$

نماد معمول برای تابع مرکب f و g، $g \circ f$ می‌باشد (به ترتیب نوشتن آنها دقت کنید). بنابراین $(g \circ f)(x) = g(f(x))$.

مثال ۱. گیریم E مجموعه اعداد صحیح زوج و $\mathbb{N}$ مجموعه اعداد صحیح نامنفی باشد. گیریم $f : E \to \mathbb{Z}$ با $f(x) = x/2$ تعریف شود (چون x زوج است $x/2$ یک عدد صحیح می‌باشد). گیریم $g : \mathbb{Z} \to \mathbb{Z}$ با $g(n) = n^2$ تعریف شده باشد. آنگاه تابع مرکب $g \circ f : E \to \mathbb{N}$ دارای ضابطه زیر است:

$$(g \circ f)(x) = g(f(x)) = g(x/2) = (x/2)^2 = x^2/4.$$

در این مثال، تابع مرکب $f \circ g$ (ابتدا g را، سپس f را بکار برید)، تعریف نشده است زیرا برد g با دامنه f یکسان نیست. برای مثال $g(3) = 9$، ولی دامنه f مجموعه اعداد صحیح زوج است؛ اگرچه

قاعده f برای اعداد صحیح فرد نیز معنی دارد امّا $f(g(۳)) = f(۹) = ۹/۲$، که در $\mathbb{Z}$ نمی‌باشد.

مثال ۲. گیریم $f : \mathbb{Z} \to \mathbb{Z}$ و $g : \mathbb{Z} \to \mathbb{Z}$ با $f(x) = x - ۱$ و $g(x) = x^۲$ تعریف شوند. آنگاه تابع مرکب $f \circ g$ با ضابطه

$$(f \circ g)(x) = f(g(x)) = f(x^۲) = x^۲ - ۱$$

تعریف می‌شود. در این مثال تابع مرکب $g \circ f$، که ترتیب آن مخالف $f \circ g$ است، نیز تعریف شده است؛ قاعده آن عبارت است از:

$$(g \circ f)(x) = g(f(x)) = g(x - ۱) = (x - ۱)^۲ = x^۲ - ۲x + ۱.$$

پس برای مثال، داریم

$$(f \circ g)(۳) = ۳^۲ - ۱ = ۸ \quad \text{ولی} \quad (g \circ f)(۳) = ۹ - ۶ + ۱ = ۴.$$

بنابراین اگرچه هر دو $f \circ g$ و $g \circ f$ تعریف شده‌اند امّا توابع یکسانی نیستند.

دو تابع $h : B \to C$ و $k : B \to C$ را **برابر** گویند مشروط به آن که برای هر $b \in B$، $h(b) = k(b)$.

مثال ۳. گیریم $f : B \to C$ تابعی دلخواه و $\iota_C : C \to C$ تابع همانی روی C باشد آنگاه $\iota_C \circ f : B \to C$ و برای هر $b \in B$،

$$(\iota_C \circ f)(b) = \iota_C(f(b)) = f(b).$$

بنابراین $\iota_C \circ f = f$. به طور مشابه اگر ι_B تابع همانی روی B باشد، آنگاه $f \circ \iota_B : B \to C$، و برای هر $b \in B$،

$$(f \circ \iota_B)(b) = f(\iota_B(b)) = f(b).$$

در نتیجه

اگر $f : B \to C$، آنگاه $\iota_C \circ f = f$ و $f \circ \iota_B = f$.

اگر $f : B \to C$، $g : C \to D$، و $h : D \to E$ تابع باشند، آنگاه هر یک از توابع مرکب $(f \circ g) \circ h$ و $f \circ (g \circ h)$ تابعی از B به E می‌باشد. ادعا می‌کنیم که

$$(f \circ g) \circ h = f \circ (g \circ h).$$

اثبات این گزاره تمرین ساده‌ای در بکارگیری تعریف تابع مرکب می‌باشد. برای هر $b \in B$،

$$[(f \circ g) \circ h](b) = (f \circ g)(h(b)) = f[(g(h(b))]$$

و

$$[f \circ (g \circ h](b) = f[(g \circ h)(b)] = f[(g(h(b))].$$

چون طرف راست دو تساوی برابر است، توابع مرکب $(f \circ g) \circ h$ و $f \circ (g \circ h)$ دارای اثر یکسان روی هر $b \in B$ می‌باشند، که ادعای ما را ثابت می‌کند.

اعمال دوتایی

به طور غیررسمی می‌توانیم یک عمل دوتایی روی اعداد صحیح را برای مثال، به عنوان قانونی برای ایجاد یک عدد صحیح از دو عدد صحیح مفروض در نظر بگیریم. جمع و ضرب معمولی اعمالی به این مفهوم می‌باشد: با مفروض بودن a و b به $a + b$ و ab می‌رسیم. ایجاد یک عدد صحیح جدید از دو عدد مفروض، مفهوم یک تابع را پیشنهاد می‌کند. جمع اعداد صحیح را می‌توان به عنوان یک تابع f از $\mathbb{Z} \times \mathbb{Z}$ به $\mathbb{Z}$ که ضابطه آن

$$f(a, b) = a + b$$

است در نظر گرفت. به طور مشابه عمل ضرب را می‌توان به عنوان یک تابع $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ با ضابطه $g(a, b) = ab$ در نظر گرفت.

مثال ۴. همان‌طورکه در بالا دیدیم، جمع و ضرب معمولی اعمالی دوتایی روی $\mathbb{Z}$ می‌باشند. تابع $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ با ضابطهٔ $f(a, b) = ab - ۱$ عمل دوتایی دیگری را روی $\mathbb{Z}$ تعریف می‌کند. اگر این عمل با $*$ نشان داده شود، آنگاه $۱۴ = ۱ - ۱۵ = ۵ * ۳$، و به طور مشابه

$$۱۲ * ۴ = ۴۷ \quad \text{و} \quad -۷ * ۴ = -۲۹ \quad \text{و} \quad ۰ * ۸ = -۱.$$

توجه کنید که $a * b = ab - ۱ = ba - ۱ = b * a$، بنابراین، مثل حالت جمع و ضرب معمولی به هنگام کاربرد $*$ ترتیب عناصر مهم نیست (این خاصیت در اصطلاح علمی، خاصیت جابجایی نامیده می‌شود). از جهت دیگر

$$(۱ * ۲) * ۳ = ۱ * ۳ = ۲ \qquad \text{ولی} \qquad ۱ * (۲ * ۳) = ۱ * ۵ = ۴.$$

پس در حالت کلی $a * (b * c) \neq (a * b) * c$. بنابراین $*$ برخلاف جمع و ضرب که شرکت‌پذیرند (به این معنی که همواره $(a + b) + c = a + (b + c)$ و $(ab)c = a(bc)$) شرکت‌پذیر نمی‌باشد.

مثال ۵. گیریم S یک مجموعه ناتهی باشد. اگر $f : S \to S$ و $g : S \to S$ تابع باشند، آنگاه $f \circ g$ ترکیب آنها نیز یک تابع از S به S می‌باشد. بنابراین اگر B مجموعه تمام توابع از S به S باشد، آنگاه ترکیب توابع یک عمل روی B است. به بیان دیگر، تابعی که (f, g) را به $f \circ g$ می‌فرستد یک تابع از $B \times B$ به B است. بحث توابع مرکب در فوق نشان می‌دهد که عمل ترکیب روی B شرکت‌پذیر (یعنی همواره $(f \circ g) \circ h = f \circ (g \circ h)$) است ولی جابجایی نیست ($f \circ g$ لازم نیست با $g \circ f$ برابر باشد).

گیریم $*$ یک عمل روی یک مجموعه B باشد و $C \subseteq B$. زیرمجموعه C را تحت عمل $*$ **بسته** گویند مشروط به آن که

$$\text{وقتی } a, b \in C \text{، آنگاه } a * b \in C.$$

برای مثال، فرض کنید B مجموعه اعداد حقیقی مثبت باشد و عمل ضرب معمولی را روی آن در نظر بگیرید. C را زیرمجموعه اعداد صحیح مثبت بگیرید. آنگاه C تحت این عمل بسته است زیرا وقتی a و b اعداد صحیح مثبت باشند ab مثبت است. امّا وقتی عمل روی B تقسیم معمولی باشد، C بسته نیست: اگر a و b اعداد صحیح باشند، $a : b$ لزوماً یک عدد صحیح نیست (برای مثال $۳ : ۷ = ۳/۷ \notin C$).

اگر $*$ یک عمل روی یک مجموعه B باشد، آنگاه B (به عنوان زیرمجموعه‌ای از خودش) تحت عمل $*$ بسته است. با این وجود بسیاری از کتاب‌های درسی از جمله این کتاب بسته بودن B تحت عمل $*$ را به عنوان یکی از خواص عمل فهرست می‌کنند. البته این امر منطقاً ضرورت ندارد، امّا توجه به آن نظر خواننده را به اهمیت خاصیت بسته‌بودن جلب می‌کند و خاطرنشان می‌سازد که این

خاصیت را نباید برای زیرمجموعه‌های دلخواه B، تضمین شده فرض کرد.

توابع یک به یک و پوشا

یک تابع $f : B \to C$ **یک به یک** نامیده می‌شود مشروط به این که f عناصر متمایز B را به عناصر متمایز C بنگارد، یا در نماد تابعی: اگر در B، $a \neq b$، آنگاه در C، $f(a) \neq f(b)$. این گزاره نسبتاً ناهنجار، هم‌ارز عکس نقیضش می‌باشد، که توصیف مؤثرتری را بدست می‌دهد:

$f : B \to C$ یک به یک است مشروط به این که
وقتی در C، $f(a) = f(b)$ آنگاه در B، $a = b$.

مثال ۶. گیریم $\mathbb{R}$ مجموعه تمام اعداد حقیقی باشد. برای این که نشان دهیم تابع $f : \mathbb{R} \to \mathbb{R}$ که با ضابطه $f(x) = ۲x + ۳$ تعریف شده است یک به یک می‌باشد، فرض می‌کنیم $f(a) = f(b)$، یعنی

$$۲a + ۳ = ۲b + ۳.$$

با تفریق ۳ از طرفین بدست می‌آید $۲a = ۲b$؛ با تقسیم طرفین بر ۲ بدست می‌آید $a = b$. بنابراین f یک به یک می‌باشد.

مثال ۷. نگاشت $f : \mathbb{Z} \to \mathbb{Z}$ که با ضابطه $f(x) = x^۲$ تعریف شده است یک به یک نیست زیرا $f(۳) = ۹ = f(-۳)$، ولی $۳ \neq -۳$. به بیان دیگر، عضوهای متمایز ۳ و -۳ تصویر یکسان دارند.

یک تابع $f : B \to C$ **پوشا (برو)** نامیده می‌شود مشروط به آن که هر عضو C تصویر لااقل یک عضو B، تحت تابع f باشد، به بیان دیگر

اگر $c \in C$، آنگاه عضو $b \in B$ وجود داشته باشد به طوری که $f(b) = c$.

مثال ۸. گیریم $\mathbb{N}$ مجموعه اعداد صحیح نامنفی و $f : \mathbb{Z} \to \mathbb{N}$ تابع تعریف شده توسط $f(x) = |x|$ باشد. f پوشاست زیرا هر عضو $\mathbb{N}$ تصویر تحت f لااقل یک عضو $\mathbb{Z}$ (یعنی خود آن عضو) می‌باشد. البته توجه کنید که f یک به یک نمی‌باشد، زیرا برای مثال $f(۱) = f(-۱)$.

مثال ۹. گیریم E مجموعه اعداد صحیح زوج باشد و تابع $g : \mathbb{Z} \to E$ تعریف شده با $g(x) = 4x$ را در نظر بگیرید. ادعا می‌کنیم که عضو ۲ در E تصویر تحت g هیچ عضوی از $\mathbb{Z}$ نیست. اگر برای برخی $b \in \mathbb{Z}$، $g(b) = 2$، آنگاه $4b = 2$، و بنابراین $2b = 1$. این غیر ممکن است زیرا ۱ مضرب صحیح ۲ نمی‌باشد. بنابراین g پوشا نیست. با این حال، توجه داشته باشید که g یک به یک است زیرا $4b = 4a$ (یعنی $g(a) = g(b)$) ایجاب می‌کند که $a = b$.

مثال ۱۰. گیریم $\mathbb{R}$ مجموعه اعداد حقیقی و $f : \mathbb{R} \to \mathbb{R}$ تابع تعریف شده توسط $f(x) = 2x + 3$ باشد. برای این که ثابت کنیم f پوشاست، گیریم $c \in \mathbb{R}$؛ باید $b \in \mathbb{R}$ را چنان پیدا کنیم که $f(b) = c$. به بیان دیگر، باید یک عدد b پیدا کنیم به طوری که $2b + 3 = c$. برای انجام این کار این معادله آخر را برای b حل می‌کنیم و بدست می‌آوریم $b = (c - 3)/2$، آنگاه

$$f(b) = 2(\frac{c-3}{2}) + 3 = c - 3 + 3 = c.$$

بنابراین f پوشا است. همچنین تابع f یک به یک نیز هست (مثال ۶ را ملاحظه کنید).

مثال‌های پیشین پیشنهاد می‌کند که یک به یک بودن و پوشا بودن مفاهیم مستقل می‌باشند. یکی دیگری را نتیجه نخواهد داد، و یک تابع خاص می‌تواند یک، هر دو، یا هیچ‌یک از این خواص را نداشته باشد.

اگر $f : B \to C$ یک تابع باشد، آنگاه **تصویر f** زیرمجموعه

$$\mathrm{Im} f = \{c \mid c = f(b) \text{ برای برخی } b \in B\} = \{f(b) \mid b \in B\}$$

از C می‌باشد. برای مثال، اگر $f : \mathbb{Z} \to \mathbb{Z}$ با ضابطه $f(x) = 2x$ تعریف شود، آنگاه $\mathrm{Im} f$ مجموعه اعداد صحیح زوج می‌باشد زیرا $\mathrm{Im} f = \{f(x) \mid x \in \mathbb{Z}\} = \{2x \mid x \in \mathbb{Z}\}$. به طور مشابه، اگر $g : \mathbb{Z} \to \mathbb{Z}$ با $g(x) = |x|$ تعریف شود، آنگاه $\mathrm{Im} g$ مجموعه اعداد صحیح نامنفی می‌باشد. یک تابع $f : B \to C$ پوشا می‌باشد هرگاه هر عضو C تصویر حداقل یک عضو B باشد. بنابراین

$$f : B \to C \text{ پوشاست اگر و تنها اگر } \mathrm{Im} f = C.$$

اگر $f : B \to C$ یک تابع باشد و S یک زیرمجموعه B باشد، آنگاه تصویر S، زیرمجموعه

$$f(S) = \{c \mid c = f(b), b \in S \text{ برای برخی}\} = \{f(b) \mid b \in S\}$$

می‌باشد. اگر برای مثال، $f : \mathbb{Z} \to \mathbb{Z}$ با ضابطه $f(x) = ۲x$ تعریف شود، و S زیرمجموعه اعداد صحیح فرد باشد، آنگاه $f(S) = \{۲x \mid x$ فرد است$\}$ مجموعه اعداد صحیح زوجی هستند که مضرب ۴ نمی‌باشند. اگر زیرمجموعه S خود مجموعه B باشد، آنگاه $f(B)$ دقیقاً $\mathrm{Im} f$ می‌باشد.

توابع دوسویی

یک تابع $f : B \to C$ را **دوسویی** (یا **تناظر یک به یک**) گویند مشروط به آن که f هم یک به یک و هم پوشا باشد.

مثال ۱۱. مثال ۱۰ نشان می‌دهد که نگاشت $f : \mathbb{R} \to \mathbb{R}$ که توسط $f(x) = ۲x + ۳$ تعریف می‌شود دوسویی است.

مثال ۱۲. نگاشت f از مجموعه $\{۱, ۲, ۳, ۴, ۵\}$ به مجموعه $\{v, w, x, y, z\}$ که با $f(۱) = v$، $f(۲) = w$، $f(۳) = x$، $f(۴) = y$ و $f(۵) = z$ تعریف می‌شود به وضوح یک دوسویی می‌باشد.

مثال آخر مبین این واقعیت است که برای مجموعه‌های دلخواه B و C، یک دوسویی از B به C موجود می‌باشد اگر و تنها اگر B و C تعداد عضوهای برابر داشته باشند. به ویژه، اگر B متناهی باشد و $C \subsetneq B$ آنگاه بین B و C نمی‌تواند یک دوسویی وجود داشته باشد. ولی این وضعیت درباره مجموعه‌های نامتناهی متفاوت می‌باشد.

مثال ۱۳. گیریم E مجموعه اعداد صحیح زوج باشد و نگاشت $f : \mathbb{Z} \to E$ که با ضابطه $f(x) = ۲x$ تعریف می‌شود را در نظر بگیرید. طبق تعریف هر عدد صحیح زوج مضرب صحیحی از عدد ۲ است، پس f پوشا می‌باشد. به علاوه، $۲a = ۲b$ ایجاب می‌کند که $a = b$، پس f یک به یک است. بنابراین، f یک دوسویی می‌باشد. در واقع کمی بیشتر از این درست است. یک نگاشت $g : E \to \mathbb{Z}$ با ضابطه $g(u) = u/۲$ تعریف کنید؛ این مطلب معنی‌دار است زیرا $u/۲$ وقتی u زوج است یک عدد صحیح می‌باشد. تابع مرکب $g \circ f : \mathbb{Z} \to \mathbb{Z}$ را در نظر بگیرید:

$$(g \circ f)(x) = g(f(x)) = g(۲x) = ۲x/۲ = x.$$

بدین دلیل برای هر x، $(g \circ f)(x) = x = \iota(x)$، یعنی تابع مرکب $g \circ f$ تابع همانی $\iota_{\mathbb{Z}}$ روی $\mathbb{Z}$

می‌باشد. اکنون به ترکیب $f \circ g : E \to E$ نگاه کنید،

$$(f \circ g)(u) = f(g(u)) = f(u/۲) = ۲(u/۲) = u.$$

بنابراین تابع مرکب $f \circ g$ تابع همانی ι_E می‌باشد.

مثال پیش خاصیتی را مطرح می‌کند که همه نگاشت‌های دوسویی دارند و اینک به اثبات آن می‌پردازیم.

قضیه ب.۱ تابع $f : B \to C$ دوسویی است اگر و تنها اگر یک تابع $g : C \to B$ وجود داشته باشد به طوری که

$$g \circ f = \iota_B \qquad \text{و} \qquad f \circ g = \iota_C.$$

برهان. ابتدا فرض کنید که f دوسویی باشد. تابع $g : C \to B$ را به شرح زیر تعریف کنید. اگر $c \in C$، آنگاه $b \in B$ وجود دارد به طوری که $f(b) = c$، زیرا f پوشا است. به علاوه، چون f یک به یک نیز می‌باشد، تنها یک عضو b وجود دارد به طوری که $f(b) = c$ (برای این که اگر $f(b') = c$، آنگاه $f(b) = f(b')$ ایجاب می‌کند که $b = b'$). پس می‌توانیم تابع $g : B \to C$ را با این ضابطه تعریف کنیم:

$g(c) = b$، که در آن b عضو یکتایی از B است که $f(b) = c$.

بنابراین $g(c) = b$ دقیقاً وقتی که $f(b) = c$. از این جهت برای هر $c \in C$،

$$(f \circ g)(c) = f(g(c)) = f(b) = c,$$

که از آن نتیجه می‌گیریم $f \circ g = \iota_C$. به طور مشابه، برای هر $u \in B$، $f(u)$ یک عضو C می‌باشد، مثلاً $f(u) = v$، و از اینرو طبق تعریف g داریم $g(v) = u$. بنابراین

$$(g \circ f)(u) = g(f(u)) = g(v) = u,$$

و لذا $g \circ f = \iota_B$. این مطلب نیمه‌اول قضیه دو شرطی ما را ثابت می‌کند.

برای اثبات نیمه دیگر، فرض کنید که یک نگاشت $g : C \to B$ با خواص بیان شده وجود داشته

باشد. باید نشان دهیم که f دوسویی است. فرض کنید $f(a) = f(b)$. آنگاه

$$g(f(a)) = g(f(b))$$
$$(g \circ f)(a) = (g \circ f)(b)$$
$$\iota_B(a) = \iota_B(b)$$
$$a = b.$$

بنابراین $f(a) = f(b)$ ایجاب می‌کند که $a = b$، و f یک به یک است. برای نشان دادن این که f پوشاست، گیریم c عضوی دلخواه از C باشد. آنگاه $g(c) \in B$ و

$$f(g(c)) = (f \circ g)(c) = \iota_C(c) = c.$$

بنابراین یک عضو از B یافته‌ایم (یعنی $g(c)$) که تحت f به c نگاشته می‌شود، لذا f پوشا می‌باشد. بنابراین f دوسویی است، و قضیه ثابت می‌شود. ■

اگر $f : B \to C$ یک دوسویی باشد آنگاه نگاشت g در قضیه ب.۱ **معکوس (یا وارون)** f نامیده می‌شود و معمولاً با f^{-1} نشان داده می‌شود. تعویض نقش f و g در قضیه ب.۱ نشان می‌دهد که نگاشت معکوس یک دوسویی خودش یک دوسویی است.

تمرینها

توجه: $\mathbb{Z}$ مجموعه اعداد صحیح، $\mathbb{Q}$ مجموعه اعداد گویا و $\mathbb{R}$ مجموعه اعداد حقیقی می‌باشد.

A.۱. هر مجموعه را با فهرست کردن عضوهای آن توصیف کنید:

(الف) اعداد صحیح اکیداً بین ۳- و ۹.

(ب) اعداد صحیح منفی بزرگتر از ۱۰-.

(پ) اعداد صحیحی که ریشه دوم آنها کمتر یا مساوی ۴ می‌باشد.

۲. هر مجموعه را با نماد مجموعه ـ ساز توصیف کنید:

(الف) تمام اعداد حقیقی مثبت.

(ب) تمام اعداد اصم منفی.

(پ) تمام نقاط صفحه مختصات با مؤلفه اول گویا.

(ت) تمام اعداد صحیح منفی زوج بزرگتر از -۵۰.

۳. کدام یک از مجموعه‌های زیر ناتهی می‌باشند؟

(الف) $\{r \in \mathbb{Q} \mid r^۲ = ۲\}$.

(ب) $\{r \in \mathbb{R} \mid r^۲ + ۵r - r = ۰\}$.

(پ) $\{t \in \mathbb{Z} \mid ۶t^۲ - t - ۱ = ۰\}$.

۴. آیا B زیرمجموعه C می‌باشد وقتی

(الف) $B = \mathbb{Z}$ و $C = \mathbb{Q}$ ؟

(ب) B، مجموعه تمام جوابهای $x^۲ + ۲x - ۵ = ۰$ و $C = \mathbb{Z}$ ؟

(پ) $B = \{a, b, ۷, ۹, ۱۱, -۶\}$ و $C = \mathbb{Q}$ ؟

۵. اگر $A \subseteq B$ و $B \subseteq C$، ثابت کنید $A \subseteq C$.

۶. در هر قسمت $B - C$، $B \cap C$ و $B \cup C$ را پیدا کنید:

(الف) $B = \mathbb{Z}$، $C = \mathbb{Q}$ ، (ب) $B = \mathbb{R}$، $C = \mathbb{Q}$

(پ) $B = \{a, b, c, ۱, ۲, ۳, ۴, ۵\}$ ، $C = \{a, c, e, ۲, ۴, ۶, ۸\}$.

۷. عضوهای $B \times C$ را فهرست کنید وقتی $B = \{a, b, c\}$ و $C = \{۰, ۱, c\}$.

۸. عضوهای $A \times B \times C$ را فهرست کنید وقتی $A = \{۰, ۱\}$ و C, B مانند تمرین ۷ باشند.

۹. گیریم $A = \{۱, ۲, ۳, ۴\}$. توابع f و g از A به A را چنان ارائه کنید که $f \circ g \neq g \circ f$.

۱۰. وقتی $A = \mathbb{Z}$ تمرین ۹ را انجام دهید.

۱۱. آیا زیرمجموعه B تحت عمل داده‌شده بسته است؟

(الف) B، مجموعه اعداد صحیح زوج ؛ عمل: ضرب در $\mathbb{Z}$.

(ب) B، مجموعه اعداد صحیح فرد؛ عمل: جمع در $\mathbb{Z}$.

(پ) B، مجموعه اعداد گویای ناصفر؛ عمل: تقسیم در مجموعه اعداد حقیقی ناصفر.

(ت) B، مجموعه اعداد صحیح فرد؛ عمل $*$ روی $\mathbb{Z}$، که در آن $a * b$ توسط $ab - (a + b) + ۲$ تعریف می‌شود.

۱۲. تصویر تابع f را پیدا کنید وقتی

(الف) $f : \mathbb{R} \to \mathbb{R}$ ؛ $f(x) = x^۲$.

(ب) $f : \mathbb{Z} \to \mathbb{Q}$ ؛ $f(x) = x - ۱$.

(پ) $f : \mathbb{R} \to \mathbb{R}$ ؛ $f(x) = -x^۲ + ۱$.

۱۳. گیریم $B = \{۱, ۲, ۳, ۴\}$ و $C = \{a, b, c\}$.

(الف) چهار تابع متفاوت پوشا از B به C فهرست کنید.

(ب) چهار تابع متفاوت یک به یک از C به B فهرست کنید.

(پ) تمام توابع دوسویی از C به C را فهرست کنید.

۱۴. (الف) مثالی از یک تابع یک به یک ارائه کنید که پوشا نباشد.

(ب) مثالی از یک تابع پوشا ارائه کنید که یک به یک نباشد.

۱۵. گیریم B و C مجموعه‌های ناتهی باشند. ثابت کنید که تابع $f : B \times C \to C \times B$ که با ضابطه $f(x, y) = (y, x)$ تعریف می‌شود یک دوسویی است.

۱۶.B. تمام زیرمجموعه‌های $\{۱, ۲\}$ را فهرست کنید. همین کار را برای $\{۱, ۲, ۳\}$ و $\{۱, ۲, ۳, ۴\}$ انجام دهید. تعداد زیرمجموعه‌های یک مجموعه $n-$ عضوی را حدس بزنید. [مجموعه تهی را فراموش نکنید.]

۱۷. درستی هر یک از خواص مجموعه‌های فهرست شده در (⋆) (در مبحث اعمال روی مجموعه‌ها) را تحقیق کنید.

۱۸. اگر $a, b \in \mathbb{R}$ و $a < b$، آنگاه مجموعه $\{r \in \mathbb{R} \mid a \le r < b\}$ با $[a, b)$ نمایش داده می‌شود. گیریم $\mathbb{N}$ مجموعه اعداد صحیح نامنفی را نشان دهد و P مجموعه اعداد صحیح مثبت باشد. این اجتماع‌ها و اشتراک‌ها را پیدا کنید:

(الف) $\bigcup_{n \in \mathbb{N}} [n, n + ۱)$ (ب) $\bigcap_{n \in P} [-۱/n, ۰)$

(پ) $\bigcup_{n \in P} [\frac{۱}{n}, ۲ + \frac{۱}{n})$ (ت) $\bigcap_{n \in P} [\frac{۱}{n}, ۲ + \frac{۱}{n})$

۱۹. ثابت کنید که برای هر سه مجموعه دلخواه A، B، C:

$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

۲۰. گیریم A، B زیرمجموعه‌های U باشند. قوانین دمورگان را ثابت کنید:

(الف) $U - (A \cap B) = (U - A) \cup (U - B)$

(ب) $U - (A \cup B) = (U - A) \cap (U - B)$

۲۱. ثابت کنید که برای مجموعه‌های دلخواه A، B، C:

$$(A - B) \cup (B - A) = (A \cup B) - (A \cap B).$$

۲۲. اگر C مجموعه‌ای متناهی باشد، $|\ C\ |$ تعداد عضوهای C را نشان می‌دهد. اگر A و B مجموعه‌هایی متناهی باشند، آیا تساوی $|\ A \cup B\ | = |\ A\ | + |\ B\ |$ درست است؟

۲۳. گیریم R^{**} مبین مجموعه اعداد حقیقی مثبت باشد. آیا قاعده زیر یک تابع از $\mathbb{R}^{**}$ به $\mathbb{R}$ تعریف می‌کند: به هر عدد حقیقی مثبت c عدد حقیقی‌ای که مربع آن c باشد را نسبت دهید.

۲۴. تعیین کنید که کدام یک از عمل‌های داده شده روی $\mathbb{R}$ جابجایی (یعنی برای هر a، b، $a * b = b * a$) یا شرکت‌پذیر (یعنی برای هر a، b، c، $(a * (b * c) = (a * b) * c$) می‌باشد.

(الف) $a * b = ۲^{ab}$

(ب) $a * b = ab^{۲}$

(پ) $c * b = ۰$

(ت) $a * b = (a + b)/۲$

(ث) $a * b = ۱$

(ج) $a * b = b$

(چ) $a * b = a^{۲} + b^{۲}$

۲۵. ثابت کنید که هر یک از توابع زیر یک به یک می‌باشد.

(الف) $f : \mathbb{Z} \to \mathbb{Z}$ ؛ $f(x) = ۲x$

(ب) $f : \mathbb{R} \to \mathbb{R}$ ؛ $f(x) = x^{۳}$

(پ) $f : \mathbb{Z} \to \mathbb{Q}$ ؛ $f(x) = x/۷$

(ت) $f : \mathbb{R} \to \mathbb{R}$ ؛ $f(x) = -۳x + ۵$.

۲۶. ثابت کنید که هر یک از توابع زیر پوشا می‌باشد.

(الف) $f : \mathbb{R} \to \mathbb{R}$ ؛ $f(x) = x^{۳}$.

(ب) $f : \mathbb{Z} \to \mathbb{Z}$ ؛ $f(x) = x - ۴$.

(پ) $f : \mathbb{R} \to \mathbb{R}$ ؛ $f(x) = -3x + 5$.

(ت) $f : \mathbb{Z} \to \mathbb{Q}$ ؛ $f(a,b) = a/b$ وقتی که $b \neq 0$ و $f(a,b) = 0$ وقتی که $b = 0$.

۲۷. گیریم $f : B \to C$ و $g : C \to D$ تابع باشند. ثابت کنید که:

(الف) اگر f و g یک به یک باشند، آنگاه $g \circ f : B \to D$ یک به یک می‌باشد.

(ب) اگر f و g پوشا باشند، آنگاه $g \circ f$ پوشا می‌باشد.

۲۸. (الف) گیریم $f : B \to C$ و $g : C \to D$ دو تابع باشند و $g \circ f$ یک به یک باشد. ثابت کنید که f یک به یک است.

(ب) مثالی از موقعیت قسمت (الف) ارائه کنید که در آن g یک به یک نباشد.

۲۹. (الف) گیریم $f : B \to C$ و $g : C \to D$ دو تابع باشند و $g \circ f$ پوشا باشد. ثابت کنید که g پوشا است.

(ب) مثالی از موقعیت قسمت (الف) ارائه کنید که در آن f پوشا نباشد.

۳۰. گیریم $g : B \times C \to C$ (که در آن $B \neq \emptyset$) تابع تعریف شده توسط $g(x,y) = y$ باشد.

(الف) ثابت کنید که g پوشا می‌باشد.

(ب) آیا هیچ شرطی وجود دارد که تحت آن g یک به یک باشد؟

۳۱. اگر $f : B \to C$ یک تابع باشد، آنگاه f را می‌توان به عنوان یک نگاشت از B به $\mathrm{Im} f$ در نظر گرفت زیرا برای هر $b \in B$، $f(b) \in \mathrm{Im} f$. نشان دهید که نگاشت $f : B \to \mathrm{Im} f$ پوشا می‌باشد.

۳۲. گیریم B یک مجموعه متناهی باشد و $f : B \to B$ یک تابع باشد. ثابت کنید که f یک به یک است اگر و تنها اگر f پوشا باشد.

۳۳. گیریم $f : B \to C$ یک تابع باشد وگیریم S و T زیرمجموعه‌های B باشند.

(الف) ثابت کنید که $f(S \cup T) = f(S) \cup f(T)$.

(ب) ثابت کنید که $f(S \cap T) \subseteq f(S) \cap f(T)$.

(ج) مثالی بزنید که در آن $f(S \cap T) \neq f(S) \cap f(T)$.

۳۴. ثابت کنید که $f : B \to C$ یک به یک است اگر و تنها اگر برای هر زوج از زیرمجموعه‌های S و T از B، $f(S \cap T) = f(S) \cap f(T)$.

۳۵. گیریم $f : B \to C$ و $g : C \to D$ توابع دوسویی باشند. آنگاه طبق تمرین ۲۷، تابع مرکب $g \circ f : B \to D$ دوسویی می‌باشد. ثابت کنید که $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

* * * * *

پیوست پ

خوش‌ترتیبی و استقراء

فرض می‌کنیم که شما با حساب معمولی در مجموعه اعداد صحیح $\mathbb{Z}$ و با رابطه ترتیب معمولی $(<)$ روی $\mathbb{Z}$ آشنایی دارید. مجموعه اعداد صحیح نامنفی با $\mathbb{N}$ نشان داده می‌شود، پس

$$\mathbb{N} = \{۰, ۱, ۲, ۳, \ldots\}.$$

اصل اساسی زیر را در مورد زیرمجموعه‌های $\mathbb{N}$ می‌پذیریم:

اصل خوش‌ترتیبی هر زیرمجموعه ناتهی $\mathbb{N}$ یک کوچکترین عضو دارد.

اگرچه بیشتر مردم این اصل را کاملاً قابل قبول می‌یابند، ولی مهم است به این نکته توجه داشته باشید که اگر $\mathbb{N}$ با مجموعه‌ای دیگر از اعداد جایگزین شود ممکن است این اصل برقرار نباشد، برای مثال بخش ۱-۱ کتاب را ملاحظه کنید.

یک نتیجه مهم اصل خوش‌ترتیبی روش برهان معروف به استقراء ریاضی می‌باشد. استقراء ریاضی را می‌توان بکار برد تا گزاره‌هایی مثل

یک مجموعه n عضوی دارای 2^n عضو می‌باشد

را ثابت کرد. این گزاره را با نماد $P(n)$ نشان دهید و مشاهده کنید که برای هر مقدار ممکن n، یک گزاره بدست می‌آورید، یعنی در حقیقت بی‌نهایت گزاره بدست می‌آورید:

$P(0)$: یک مجموعه ۰ عضوی دارای $2^0 = 1$ زیرمجموعه می‌باشد،

$P(1)$: یک مجموعه ۱ عضوی دارای $2^1 = 2$ زیرمجموعه می‌باشد،

$P(2)$: یک مجموعه ۲ عضوی دارای $2^2 = 4$ زیرمجموعه می‌باشد،

$P(3)$: یک مجموعه ۳ عضوی دارای $2^3 = 8$ زیرمجموعه می‌باشد،

و همین طور الی آخر. برای اثبات گزارهٔ اصلی باید ثابت کرد که

$P(n)$ برای هر $n \in \mathbb{N}$ گزاره‌ای درست می‌باشد.

در قضیه زیر روش انجام این کار آمده است:

قضیه پ.۱. (اصل استقراء ریاضی) فرض کنید که برای هر عدد صحیح نامنفی n، یک گزاره $P(n)$ مفروض باشد اگر

(i) $P(0)$ یک گزاره درست باشد؛ و

(ii) وقتی $P(k)$ یک گزاره درست باشد آنگاه $P(k+1)$ نیز درست می‌باشد آنگاه برای هر $n \in \mathbb{N}$، $P(n)$ یک گزاره درست است.

بعد از برهان این قضیه، مثال مربوط به تعداد زیرمجموعه‌های یک مجموعه n عضوی را ادامه می‌دهیم. اگر مایل باشید می‌توانید ابتدا این مثال را بخوانید تا ببینید که چگونه بکار بردن قضیه از روش اثبات آن کاملاً متفاوت است.

برهان قضیه پ.۱. گیریم S زیرمجموعه‌ای از $\mathbb{N}$ مشتمل بر اعداد صحیح j ای باشد که برای آن $P(j)$ نادرست است. برای اثبات قضیه لازم است ثابت کنیم که S تهی است. برای انجام این کار از برهان خلف استفاده می‌کنیم. فرض کنید S ناتهی باشد. آنگاه طبق اصل خوش‌ترتیبی S دارای کوچکترین عضوی مثل d می‌باشد. چون طبق تعریف S، $P(d)$ نادرست است و $P(0)$

طبق خاصیت (i) درست می‌باشد باید داشته باشیم $d \neq 0$. در نتیجه $d \geq 1$ (زیرا d یک عدد صحیح نامنفی است)، و از این جهت $d - 1 \geq 0$، یعنی، $d - 1 \in \mathbb{N}$. چون $d - 1 < d$ و d کوچکترین عضو در S است، $d - 1$ نمی‌تواند در S باشد بنابراین $P(d-1)$ باید درست باشد (در غیر این صورت $d - 1$ در S خواهد بود). خاصیت (ii) (با شرط $k = d - 1$) ایجاب می‌کند که $P((d-1)+1) = P(d)$ نیز باید یک گزارهٔ درست باشد. این یک تناقض است زیرا $d \in S$. بنابراین S مجموعه تهی است، و قضیه ثابت می‌شود. ■

برای این که اصل استقراء ریاضی را برای یک رشته از گزاره‌ها بکار بریم، باید تحقیق کنیم که این گزاره‌ها در هر دو خاصیت (i) و (ii) صدق می‌کنند. توجه کنید که خاصیت (ii) بیان نمی‌کند که هر $P(k)$ در واقع درست می‌باشد، بلکه حکم می‌کند که یک رابطه شرطی برقرار است: اگر $P(k)$ درست باشد، آنگاه $P(k+1)$ نیز باید درست باشد. بنابراین برای بررسی خاصیت (ii)، درستی $P(k)$ را فرض می‌کنید و این فرض را بکار می‌برید تا ثابت کنید که $P(k+1)$ درست می‌باشد. همان طور که در مثال‌های زیر خواهید دید، اثبات این گزارهٔ شرطی در بیشتر موارد امکان‌پذیر است اگرچه ممکن است قادر به اثبات مستقیم این که برای یک j خاص، $P(j)$ درست است نباشیم. فرض این که $P(k)$ درست است **فرض استقراء** نامیده می‌شود.

احتمالاً دیده‌اید که برای اثبات گزاره‌ای مثل "مجموع اولین n عدد صحیح نامنفی $n(n+1)/2$ می‌باشد" استقراء بکار می‌رود؛ در اینجا $P(n)$ گزاره: "$0+1+2+\cdots+n = n(n+1)/2$" می‌باشد. اگرچه چنین مثال‌هایی برای افراد مبتدی تمرین‌هایی قشنگ است امّا نمونه مناسبی برای چگونگی کاربرد روش استقراء در ریاضیات پیشرفته نیست. مثال‌های زیر تصویر جامع‌تری از برهان استقرایی عرضه می‌کند. این مثال‌ها کمی پیچیده‌تر از مثال‌های مقدماتی معمولی می‌باشند، ولی قابل فهم برای خوانندگان می‌باشد.

مثال ۱. اصل استقراء ریاضی را بکار می‌بریم تا ثابت کنیم که برای هر $n \geq 0$،

یک مجموعه n عضوی دارای 2^n زیرمجموعه می‌باشد.

اگر $n = 0$ آنگاه این مجموعه باید تهی (تنها مجموعه با هیچ عضو) باشد که تنها و تنها زیرمجموعه آن، خودش می‌باشد (زیرا $\emptyset$ زیرمجموعهٔ هر مجموعه می‌باشد). پس گزاره

$P(0)$: یک مجموعه 0 عضوی دارای $2^0 = 1$ زیرمجموعه می‌باشد،

درست است (خاصیت (i) برقرار است).

برای این که خاصیت (ii) قضیه پ.۱ را بررسی کنیم، درستی گزاره
$P(k)$: یک مجموعه k عضوی دارای ۲^k عضو می‌باشد،

را می‌پذیریم و این فرض استقراء را بکار می‌بریم تا درستی گزاره
$P(k+۱)$: یک زیرمجموعه $k+۱$ عضوی دارای $۲^{k+۱}$ می‌باشد،

را ثابت کنیم. برای انجام این کار، گیریم T مجموعه دلخواهی با $k+۱$ عضو باشد و یک عضو c از T را انتخاب کنید. هر زیرمجموعه T یا c را شامل است و یا نیست. زیرمجموعه‌هایی از T که c را شامل نیستند دقیقاً زیرمجموعه‌های $T-\{c\}$ می‌باشند. چون مجموعه $T-\{c\}$ یک عضو کمتر از T دارد، این مجموعه یک زیرمجموعه k عضوی می‌باشد و بنابراین دقیقاً ۲^k زیرمجموعه دارد (زیرا درستی فرض استقراء $P(k)$ را پذیرفته‌ایم). اکنون هر زیرمجموعه T که c را شامل است باید به صورت $D\cup\{c\}$ باشد، جایی که D زیرمجموعه $T-\{c\}$ است. چون ۲^k انتخاب ممکن برای D وجود دارد، لذا T دارای ۲^k زیرمجموعه است که c را شامل می‌باشد. در نتیجه، تعداد کل زیرمجموعه‌های T برابر است با:

$$\begin{aligned}
&= ۲^k + ۲^k \quad \text{(تعداد زیرمجموعه‌های فاقد } c\text{)} + \text{(تعداد زیرمجموعه‌های شامل } c\text{)}\\
&= ۲(۲^k)\\
&= ۲^{k+۱}.
\end{aligned}$$

بدین دلیل هر مجموعه $k+۱$ عضوی T دارای $۲^{k+۱}$ زیرمجموعه می‌باشد، یعنی $P(k+۱)$ یک گزاره درست می‌باشد. اکنون خاصیت (ii) را تحقیق کرده‌ایم و بنابراین می‌توان قضیه پ.۱ را بکار برد تا نتیجه بگیریم که برای هر $n\in\mathbb{N}$، $P(n)$، درست می‌باشد؛ یعنی هر مجموعه n عضوی دارای ۲^n زیرمجموعه می‌باشد.

در برخی قضایا، اگرچه بنظر می‌رسد شیوه مناسب اثبات، استقراء ریاضی باشد امّا در عمل این کار براحتی قابل انجام نیست. در چنین مواردی نوعی از تغییر در فرآیند کار لازم است:

قضیه پ.۲. (اصل استقراء کامل) فرض کنید که برای هر عدد صحیح نامنفی n، یک گزاره $P(n)$ داده شده باشد. اگر

(i) $P(۰)$ یک گزاره درست باشد؛ و

(ii) وقتی $P(j)$ یک گزاره درست برای تمام jهایی که $۰\le j<t$ باشد، آنگاه $P(t)$ نیز درست باشد،

در این صورت $P(n)$ برای هر $n \in \mathbf{N}$ یک گزاره درست است.

اگرچه استعمال عنوان "استقراء کامل" متداول است امّا این عنوان چندان بامسمّی نیست زیرا هم‌چنان که در زیر خواهیم دید، این شکل استقراء هم‌ارز شکل قبلی آن می‌باشد.

برهان قضیه پ.۲. برای هر $n \in \mathbf{N}$، گیریم $Q(n)$ گزاره زیر باشد:

$$P(j) \text{ برای هر } j \text{ که } ۰ \leq j \leq n \text{ درست می‌باشد.}$$

به دقت توجه کنید که در این گزاره، $P(j)$ برای $j = n$ نیز درست است. اصل استقراء ریاضی (قضیه پ.۱) را بکار می‌بریم تا نشان دهیم که $Q(n)$ برای هر $n \in \mathbf{N}$ درست می‌باشد. اینک $Q(۰)$ گزاره

$$P(j) \text{ برای هر } j \text{ که } ۰ \leq j \leq ۰ \text{ درست است،}$$

می‌باشد. طبق فرض (ii) (با شرط $t = k + ۱$)، نتیجه می‌گیریم که $P(k + ۱)$ نیز درست می‌باشد. بنابراین $P(j)$ برای تمام jهایی که $۰ \leq j \leq k + ۱$ درست می‌باشد، یعنی $Q(k + ۱)$ یک گزاره درست است. بنابراین نشان داده‌ایم که وقتی $Q(k)$ درست است، آنگاه $Q(k + ۱)$ نیز درست می‌باشد. طبق اصل استقراء ریاضی $Q(n)$ برای هر $n \in \mathbf{N}$ درست است، و برهان کامل می‌شود. ■

گرچه که استفاده از نماد $P(n)$ در توصیف رسمی اصول استقراء کاملاً مناسب است، ولی این نماد به ندرت در برهان‌های واقعی مورد استفاده قرار می‌گیرد. مثال بعد، نمونه واقعی‌تری از روش‌های برهان استقرایی را که معمولاً مورد استفاده قرار می‌گیرد، نشان می‌دهد. البته در این مثال نیز ما جزئیات بیشتری از آنچه معمول است را گنجانده‌ایم.

مثال ۲. اصل استقراء کامل را به کار می‌بریم تا ثابت کنیم

$$\text{اگر } n, b \in \mathbf{N} \text{ و } ۰ < b، \text{ آنگاه } q, r \in \mathbf{N} \text{ وجود دارد به طوری که}$$

$$n = bq + r, \qquad ۰ \leq r < b. \qquad (\star)$$

این گزاره (که **الگوریتم تقسیم** برای اعداد صحیح نامنفی نامیده می‌شود) فرمول‌بندی همان تقسیم معمولی دوره ابتدایی است؛ وقتی n بر b تقسیم شود، یک خارج قسمت q و باقیمانده r (کمتر از

مقسوم‌علیه b) وجود دارد به طوری که $n = bq + r$ ؛ بحث ارائه شده در بخش ۱-۱ کتاب را ملاحظه کنید.

گزاره (*) برای $n = ۰$ و هر عدد مثبت b درست است (قرار دهید $q = ۰$ و $r = ۰$). بنابراین خاصیت (i) قضیه پ.۲ برقرار می‌باشد. فرض کنید که (*) برای تمام nهایی که $۰ \leq n < t$ درست باشد (این فرض استقراء است). باید نشان دهیم (*) برای $n = t$ درست است. اگر $t < b$، آنگاه $t = b \cdot ۰ + t$، بنابراین (*) با شرط $q = ۰$ و $r = t$ درست می‌باشد. اگر $b \leq t$، آنگاه $۰ \leq t - b < t$، و طبق فرض استقراء، (*) برای $n = t - b$ درست است. بنابراین اعداد صحیح $q_۱$ و $r_۱$ وجود دارد به طوری که

$$t - b = q_۱ b + r_۱ \qquad \text{و} \qquad ۰ \leq r_۱ < b .$$

در نتیجه

$$t = b + q_۱ b + r = (۱ + q_۱)b + r_۱ \qquad \text{و} \qquad ۰ \leq r_۱ < b .$$

بنابراین (*) برای $n = t$ درست می‌باشد (با شرط $q = ۱ + q_۱$ و $r = r_۱$). بدین دلیل خاصیت (ii) قضیه پ.۲ برقرار است. طبق اصل استقراء کامل، (*) برای هر $n \in \mathbb{N}$ درست می‌باشد.

بعضی گزاره‌های ریاضی برای $n = ۰$ یا دیگر مقادیر کوچک n نادرست می‌باشد (یا تعریف نشده است) اما برای $n = r$ و تمام اعداد صحیح بعدی درست می‌باشند. برای مثال، می‌توان نشان داد که

برای هر $n \geq ۱$، $۳n > n + ۱$ ؛
برای هر $n \geq ۵$، $۲^n > n^۲ + ۲$.

چنین گزاره‌هایی را اغلب می‌توان توسط نوعی از استقراء ریاضی اثبات کرد:

برای این که ثابت کنیم گزاره $P(n)$ برای $n \geq r$ درست می‌باشد، همان شیوه اساسی را مثل قبل دنبال کنید، تنها به جای $P(۰)$ از $P(r)$ شروع کنید.

اعتبار این شیوه عمل نتیجه‌ای از قضیه زیر است.

قضیه پ.۳. گیریم r یک عدد صحیح مثبت باشد و فرض کنید که برای هر $n \geq r$ یک گزاره $P(n)$ مفروض باشد. اگر

(i) $P(r)$ یک گزاره درست باشد؛

و یکی از گزاره‌های زیر نیز برقرار باشد:

(ii) وقتی $k \geq r$ و $P(k)$ درست است، آنگاه $P(k+1)$ درست باشد؛

یا

(ii′) وقتی $r \leq j < t$ و $P(j)$ درست است، آنگاه $P(t)$ درست باشد،

آنگاه $P(n)$ برای هر $n \geq r$ درست می‌باشد.

برهان. شرایط (i) و (ii) مشابه قضیه پ.۱ می‌باشند. بررسی کنید که برهان قضیه پ.۱ کلمه به کلمه به وضع حاضر منتقل می‌شود اگر ۰ با r و ۱ با $r+1$ و $\mathbb{N}$ با مجموعه $\mathbb{N}_r = \{n \mid n \in \mathbb{N}, n \geq r\}$ جایگزین گردد. شرط‌های (i) و (ii′) مشابه قضیه پ.۲ می‌باشند: برهان آن به طور مشابه انجام می‌شود. ■

قضیه بعد برای مطالعه بقیه کتاب ضروری نیست، ولی دستاوردی است که هر دانشجوی علاقه‌مند ریاضی باید بداند. همچنین مثال خوبی از این واقعیت است که درک شهودی می‌تواند بعضی وقت‌ها گمراه‌کننده باشد. بیشتر مردم احساس می‌کنند که اصل خوش‌ترتیبی واضح است، و این که اصل استقراء کامل به نظر عمیق‌تر می‌آید و محتاج به برهان است. ولی همان‌طور که اکنون می‌بینیم، این دو اصل در واقع هم‌ارزند. این هم‌ارزی از جمله نشان می‌دهد که اصل خوش‌ترتیبی خیلی عمیق‌تر از آن است که ابتدا بنظر می‌رسد.

قضیه پ.۴ گزاره‌های زیر هم‌ارزند:

(۱) اصل خوش‌ترتیبی.

(۲) اصل استقراء ریاضی.

(۳) اصل استقراء کامل.

برهان. برهان قضیه پ.۱ نشان می‌دهد که (۱) $\Leftarrow$ (۲)، و برهان قضیه پ.۲ نشان می‌دهد که (۲) $\Leftarrow$ (۳). برای اثبات (۳) $\Leftarrow$ (۱)، اصل استقراء کامل را می‌پذیریم و S را زیرمجموعه دلخواهی از $\mathbb{N}$ می‌گیریم. برای اثبات‌این که اصل خوش‌ترتیبی درست است باید نشان دهیم

اگر S ناتهی باشد، آنگاه S دارای یک کوچکترین عضو است.

برای انجام این امر، گزاره عکس نقیض هم‌ارز آن را ثابت خواهیم کرد:

اگر S دارای کوچکترین عضو نباشد، آنگاه S تهی است.

فرض کنید که S کوچکترین عضو ندارد؛ برای این که ثابت کنیم S تهی است لازم است فقط ثابت کنیم گزارهٔ زیر برای هر $n \in \mathbb{N}$ درست است:

(**) n عضو S نمی‌باشد.

چون ۰ کوچکترین عضو $\mathbb{N}$ است، کوچکترین عضو هر زیرمجموعه $\mathbb{N}$ که ۰ را شامل است نیز می‌باشد. چون S دارای هیچ کوچکترین عضوی نیست، ۰ نمی‌تواند در S باشد، و بدین دلیل (**) برای $n = 0$ درست است (خاصیت (i) قضیه پ.۲ برقرار است). فرض کنید (**) برای همه jهایی که $0 \leq j < t$ درست است. آنگاه هیچ یک از اعداد صحیح ۰، ۱، ۲، ...، $t-1$ در S نمی‌باشد، یا به طور معادل هر عضو S باید بزرگتر یا مساوی t باشد. اگر t در S باشد، آنگاه t کوچکترین عضو S خواهد بود زیرا برای هر $s \in S$، $s \geq t$. چون S دارای کوچکترین عضو نیست، t در S نمی‌باشد. به بیان دیگر، (**) برای $n = t$ درست است. از اینرو درستی (**) برای $j < t$ درستی آن را برای t ایجاب می‌کند (خاصیت (ii) قضیه پ.۲ برقرار است). طبق اصل استقراء ریاضی کامل، (**) برای هر $n \in \mathbb{N}$ درست می‌باشد. بنابراین S تهی است و اثبات تمام است. ■

تمرینها

A.۱. ثابت کنید که مجموع اولین n عدد صحیح نامنفی $n(n+1)/2$ می‌باشد. [راهنمایی: گیریم $P(k)$ گزاره:

$$0 + 1 + 2 + \cdots + k = k(k+1)/2$$

باشد.]

۲. ثابت کنید که برای عدد صحیح نامنفی n، $2^n > n$.

۳. ثابت کنید که برای هر عدد صحیح نامنفی n، $2^{n-1} \leq n!$ [بخاطر آورید که $0! = 1$ و برای $n > 0$، $n! = 1 \times 2 \times 3 \times \cdots \times (n-1) \times n$.]

۴. گیریم r یک عدد حقیقی باشد و $r \neq 1$. ثابت کنید که برای هر $n \geq 1$،

$$1 + r + r^2 + \cdots + r^{n-1} = \frac{r^n - 1}{r - 1}.$$

۵.B. ثابت کنید که برای هر عدد صحیح مثبت n، ۴ یک عامل $۷^n - ۳^n$ می‌باشد. [راهنمایی:
$۷^{k+۱} - ۳^{k+۱} = ۷^{k+۱} - ۷ \times ۳^k + ۷ \times ۳^k - ۳^{k+۱} = ۷(۷^k - ۳^k) + (۷ - ۳)۳^k$.]

۶. ثابت کنید که برای هر عدد صحیح مثبت n، ۳ یک عامل $۴^n - ۱$ می‌باشد.

۷. ثابت کنید که برای هر عدد صحیح مثبت n، ۳ یک عامل $۲^{۲n+۱} + ۱$ می‌باشد.

۸. ثابت کنید که برای هر عدد صحیح مثبت n، ۵ یک عامل $۲^{۴n-۲} + ۱$ می‌باشد.

۹. ثابت کنید که برای هر عدد صحیح نامنفی n، ۶۴ یک عامل $۹^n - ۸n - ۱$ می‌باشد.

۱۰. از اصل استقراء کامل استفاده کنید تا نشان دهید که هر عدد صحیح بزرگتر از ۱ حاصلضربی از عوامل اول می‌باشد. [بخاطر آورید که عدد صحیح p اول است مشروط به آن که $p > ۱$ و تنها عامل‌های مثبت p، ۱ و p باشند.]

۱۱. گیریم B یک مجموعه n عضوی باشد. ثابت کنید که تعداد $n!$ تابع یک به یک متفاوت از B به B وجود دارد. [$n!$ در تمرین ۳ تعریف شده است.]

۱۲. درست یا نادرست است: $n^۲ - n + ۱$ برای هر عدد صحیح نامنفی n عددی اول می‌باشد. جواب خود را توجیه کنید. [عدد اول در تمرین ۱۰ تعریف شده است.]

۱۳. گیریم B یک مجموعه n عضوی باشد.

(الف) اگر $n \geq ۲$، ثابت کنید که تعداد زیرمجموعه‌های دوعضوی B، برابر با $n(n-۱)/۲$ می‌باشد.

(ب) اگر $n \geq ۳$، ثابت کنید که تعداد زیرمجموعه‌های سه عضوی B برابر با $n(n-۱)(n-۲)/۳!$ می‌باشد.

(ج) حدسی برای تعداد زیرمجموعه‌های $k-$ عضوی B وقتی $n \geq k$ بزنید. حدس خود را ثابت کنید.

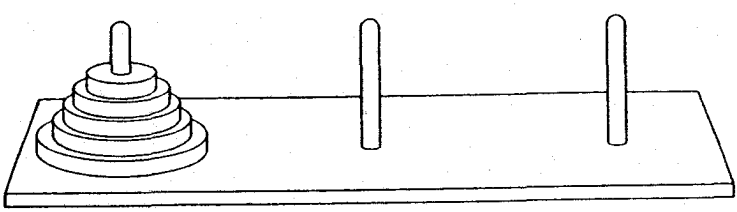
۱۴. در یک مسابقه سرگرمی بین زوج‌های جوان هر زوج درست یکبار با هر زوج دیگر مسابقه می‌دهد. فرض کنید که در این مسابقه تساوی وجود ندارد.

(الف) اگر شرکت‌کنندگان n زوج باشند، ثابت کنید که یک "زوج شایسته" به مفهوم زیر وجود دارد: زوج u یک زوج "شایسته" است به شرط آن که برای هر زوج v، u بر v پیروز شود یا u زوجی را شکست دهد که بر زوج v غلبه کرده است.

(ب) بامثال نشان دهید که ممکن است بیشتر از یک زوج شایسته وجود داشته باشد.

۱۵. در "برهان" زیر، راجع به هم‌رنگ بودن همه گلهای رز، چه چیز نادرست است. کافی است که این گزاره را ثابت کنید: در هر مجموعه از n گل رز تمام گلهای رز هم رنگ هستند. اگر $n = ۱$، این گزاره بدون تردید درست است. فرض کنید این گزاره برای $n = k$ درست باشد. گیریم S مجموعه‌ای از $k + ۱$ گل رز باشد، یک گل رز از S بردارید (آن را گل رز A بنامید)، k گل رز باقی می‌ماند، و طبق فرض استقراء باید همه آنها هم‌رنگ باشند. گل رز A را جایگزین کنید و گل رز دیگری بردارید (آن را گل رز B بنامید). باز هم k گل رز باقی می‌ماند که طبق فرض استقراء باید همه آنها هم‌رنگ باشند. چون گلهای رز باقیمانده شامل گل رز A است، تمام گلهای رز مجموعه S هم‌رنگ می‌باشند. این مطلب ثابت می‌کند که گزاره برای $n = k + ۱$ درست است. بنابراین گزاره برای تمام nها، طبق استقراء درست است.

۱۶. گیریم n یک عدد صحیح مثبت باشد. فرض کنید که سه عدد پایه چوبی وجود دارد و روی یکی از آنها، n حلقه گذاشته‌اند به طوری که قطر هر حلقه از قطر حلقه زیر آن کمتر است، همان‌طور که در شکل زیر نشان داده شده است:



می‌خواهیم تمام این حلقه‌ها را به پایه دیگر، بر طبق این دستورالعمل انتقال دهیم: (i) در هر بار فقط یک حلقه را می‌توان منتقل کرد؛ (ii) یک حلقه را می‌توان به هر یک از پایه‌ها منتقل کرد ولی نمی‌توان آن را بالای یک حلقه کوچکتر قرار داد؛ (iii) ترتیب نهایی حلقه‌ها روی حلقه جدید باید درست مانند ترتیب اصلی آنها روی پایه اول باشد. ثابت کنید که این بازی را می‌توان در $۲^n - ۱$ انتقال تمام کرد و نمی‌توان آن را با انتقال‌های کمتری به پایان برد.

۱۷. گیریم x یک عدد حقیقی بزرگتر از -۱ باشد. ثابت کنید که برای هر عدد صحیح مثبت n،

$.(1+x)^n > 1+nx$

۱۸.C. نقشه‌هایی در صفحه را، که از رسم تعداد متناهی خط مستقیم (خط، نه پاره‌خط) بدست آمده است، در نظر بگیرید. با استفاده از استقراء ثابت کنید که هر نقشه این‌چنین را می‌توان با دقیقاً دو رنگ طوری نقاشی کرد که هر دو ناحیه که در یک پاره خط مرز مشترک دارند، دارای رنگهای متفاوت باشند. دو ناحیه که فقط در یک نقطه دارای مرز مشترک هستند می‌توانند یک رنگ داشته باشند. [این مسئله حالتی خاص از قضیه معروف به چهار ـ رنگ می‌باشد، که اظهار می‌کند که هر نقشه واقع در صفحه (با هر چند منحنی پیوسته یا قطعات منحنی به عنوان مرز) می‌تواند با حداکثر چهار رنگ، نقاشی شود به طوری که هر دو ناحیه که بیشتر از یک نقطه در مرز مشترکشان دارند رنگهای متفاوت داشته باشند.]

* * * * *

پیوست ت
روابط هم‌ارزی

این پیوست می‌تواند پس از اتمام پیوست ب مطالعه گردد، ولی در متن کتاب تا بخش ۴.۸ بدان نیازی نیست. اگر این پیوست را قبل از بخش ۴.۸ مطالعه کنید، با مثال‌های ۱ تا ۳ مشکلی نخواهید داشت ولی احتمالاً باید بعضی از مثال‌های دیگر را رها کنید. فصل ۲ برای مثال‌هایی که با عبارت "اعداد صحیح" شروع شده‌است پیشنیاز می‌باشد، فصل ۶ برای مثال‌هایی که با عبارت "حلقه‌ها" شروع شده‌است و فصل ۷ برای مثال‌هایی که با عبارت "گروهها" شروع شده‌است پیشنیاز می‌باشد.

اگر A یک مجموعه باشد، آنگاه هر زیرمجموعه از $A \times A$ یک **رابطه** روی A نامیده می‌شود. یک رابطه T روی A یک **رابطه هم‌ارزی** نامیده می‌شود مشروط به آن که زیرمجموعه T در شرایط زیر صدق کند:

(i) **انعکاسی:** برای هر $a \in A$، $(a,a) \in T$.

(ii) **متقارن:** اگر $(a,b) \in T$، آنگاه $(b,a) \in T$.

(iii) **متعدی:** اگر $(a,b) \in T$ و $(b,c) \in T$، آنگاه $(a,c) \in T$.

اگر T یک رابطه هم‌ارزی روی A باشد و $(a,b) \in T$، گوییم **a** هم‌ارز **b** است و به‌جای $(a,b) \in T$ می‌نویسیم $a \sim b$. با این نماد جدید، شرایطی که رابطه هم‌ارزی را تعریف می‌کنند به‌صورت زیر در می‌آید:

(i) **انعکاسی:** برای هر $a \in A$، $a \sim a$.

(ii) **متقارن:** اگر $a \sim b$، آنگاه $b \sim a$.

(iii) **متعدی:** اگر $a \sim b$ و $b \sim c$ آنگاه $a \sim c$.

وقتی از این نماد استفاده می‌شود، مفهوم رابطه معمولاً بدون ارجاع صریح به یک زیرمجموعه از $A \times A$ تعریف می‌شود.

مثال ۱. گیریم A یک مجموعه باشد و $a \sim b$ را به‌معنی $a = b$ تعریف کنیم. به بیان دیگر، رابطه هم‌ارزی روی A زیرمجموعه $T = \{(a,b) \mid a = b\}$ از $A \times A$ می‌باشد. آنگاه به آسانی دیده می‌شود که " $=$ " یک رابطه هم‌ارزی است.

مثال ۲. به‌سادگی می‌توانید بررسی کنید که روی مجموعه اعداد حقیقی $\mathbb{R}$ رابطه تعریف شده با

$$r \sim s \quad \text{به معنی} \quad |r| = |s|$$

یک رابطه هم‌ارزی است.

مثال ۳.[۲۸] یک رابطه روی مجموعه اعداد صحیح $\mathbb{Z}$ به صورت زیر تعریف کنید:

$a \sim b$ به معنی $a - b$ مضربی از ۳ است.

برای مثال $۵ \sim ۱۷$ زیرا $۱۲ = ۵ - ۱۷$، مضربی از ۳ می‌باشد. به‌وضوح برای هر a، $a \sim a$ زیرا $a - a = ۰ = ۳ \times ۰$. برای اثبات خاصیت (ii) فرض کنید $a \sim b$. آنگاه $a - b$ مضربی از ۳ است. در نتیجه $-(a-b) = b - a$ نیز مضربی از ۳ است. ولی $b \sim a$، بنابراین $b \sim a$. برای اثبات (iii) فرض کنید $a \sim b$ و $b \sim c$ آنگاه $a - b$ و $b - c$ مضرب ۳ هستند و بنابراین

۲۸) اگر شما قبلاً بخش ۱.۲ را مطالعه کرده‌اید، مثال ۳ را رها کنید، این مثال همان همنهشتی به پیمانه n است وقتی که $n = ۳$.

تفاضل آنها $(a-b)-(b-c)=a-c$ مضربی از ۳ است، پس $a \sim c$. از اینرو $\sim$ یک رابطه هم‌ارزی است (این رابطه معمولاً همنهشتی به پیمانه ۳ نامیده می‌شود و با (پیمانه ۳) $a \equiv b$ نشان داده می‌شود).

مثال ۴. **(اعداد صحیح)** اگر n یک عدد صحیح مثبت ثابت باشد، رابطه هم‌ارزی به پیمانه n روی مجموعه $\mathbb{Z}$، که به‌صورت زیر تعریف می‌شود:

$$a \equiv b \ (\text{پیمانه } n) \quad \text{اگر و تنها اگر} \quad a-b \text{ مضربی از } n \text{ باشد،}$$

طبق قضیه ۱.۲ یک رابطه هم‌ارزی است.

مثال ۵. **(حلقه‌ها)** اگر I یک ایده‌ال در حلقه R باشد، آنگاه رابطه همنهشتی به پیمانه I که به صورت زیر تعریف می‌شود:

$$a \equiv b \ (I \text{ پیمانه}) \quad \text{اگر و تنها اگر} \quad a-b \in I \text{،}$$

طبق قضیه ۲.۷ یک رابطه هم‌ارزی روی R است.

مثال ۶. **(گروهها)** اگر K یک زیرگروه از گروه G باشد آنگاه رابطه تعریف شده با

$$a \equiv b \ (K \text{ پیمانه}) \quad \text{اگر و تنها اگر} \quad ab^{-1} \in K \text{،}$$

طبق قضیه ۱۷.۸ یک رابطه هم‌ارزی روی G است.

هشدار. احتمال دارد که یک رابطه روی یک مجموعه داشته باشیم که در یک یا دو خاصیت رابطه هم‌ارزی صدق کند ولی همزمان هر سه خاصیت برای آن رابطه برقرار نباشد. برای مثال رابطه ترتیب $\leq$ روی مجموعه اعداد حقیقی $\mathbb{R}$ انعکاسی و متعدی است و متقارن نیست؛ برای مثال‌های دیگر تمرین‌های ۸ و ۹ را ببینید. بنابراین شما باید هر سه خاصیت را برای این که یک رابطه خاص در واقع یک رابطه هم‌ارزی باشد بررسی کنید.

گیریم $\sim$ یک رابطه هم‌ارزی روی مجموعه A باشد. اگر $a \in A$، آنگاه **کلاس هم‌ارزی** a (که با $[a]$ نشان داده می‌شود) مجموعه تمام عضوهایی از A است که هم‌ارز با a است، یعنی،

$$[a] = \{b \mid b \in A, b \sim a\}.$$

برای نمونه، در مثال ۲ کلاس [۹] شامل تمام اعداد حقیقی b است که $b \sim ۹$، یعنی تمام اعداد b که $|b| = |۹|$. از اینرو $[۹] = \{۹, -۹\}$.

مثال ۷. **(حلقه‌ها ـ گروهها)** اگر I یک ایده‌آل حلقه R باشد، آنگاه یک کلاس هم‌ارزی تحت رابطه همنهشتی به پیمانه I یک هم‌مجموعه $a + I = \{a + i \mid i \in I\}$ می‌باشد. به طور مشابه اگر K یک زیرگروه از گروه G باشد، آنگاه یک کلاس هم‌ارزی رابطه هم‌ارزی به پیمانه K یک هم‌مجموعه راست $Ka = \{ka : k \in K\}$ می‌باشد.

مثال ۸. (ادامه مثال ۳) کلاس هم‌ارزی عدد صحیح ۲ شامل تمام اعداد صحیح b است که $b \sim ۲$، یعنی تمام bهایی که $b - ۲$ مضربی از ۳ است، ولی $b - ۲$ مضربی از ۳ است درست وقتی که b برای یک عدد صحیح k به صورت $b = ۲ + ۳k$ باشد. بنابراین

$$[۲] = \{۲ + ۳k \mid k \in \mathbb{Z}\} = \{۲ + ۰, ۲ \pm ۳, ۲ \pm ۶, ۲ \pm ۹, \dots\}$$
$$= \{\dots, -۷, -۴, -۱, ۲, ۵, ۸, ۱۱, \dots\}.$$

استدلالی مشابه نشان می‌دهد که کلاس هم‌ارزی [۸] شامل تمام اعداد صحیح به صورت $۸ + ۳k$، $(k \in \mathbb{Z})$، می‌باشد؛ به طور معادل

$$[۸] = \{\dots, -۷, -۴, -۱, ۲, ۵, ۸, ۱۱, ۱۴, ۱۷, \dots\}.$$

از اینرو [۲] و [۸] مساوی می‌باشند. توجه کنید که $۸ \sim ۲$. این مصداقی از قضیه زیر است.

قضیه ت.۱. گیریم $\sim$ یک رابطه هم‌ارزی روی مجموعه A باشد و $a, c \in A$. آنگاه

$$a \sim c \qquad \text{اگر و تنها اگر} \qquad [a] = [c].$$

برهان[۲۹]. فرض کنید $a \sim c$. برای این که ثابت کنیم $[a] = [c]$ ابتدا نشان می‌دهیم $[c] \subseteq [a]$. برای انجام این کار، گیریم $b \in [a]$. آنگاه طبق تعریف $a \sim b$. چون $a \sim c$، طبق خاصیت تعدی $c \sim b$. بنابراین $b \in [c]$ ولذا $[c] \subseteq [a]$. با تعویض نقش a و c در این استدلال و استفاده از این

۲۹) اگر بخش ۱.۲ را مطالعه کرده‌اید، توجه داشته باشید که این برهان و برهان نتیجه ت.۲ زیر اساساً با برهان‌های قضیه ۳.۲ و نتیجه ۴.۲ یکی هستند: کافی است $\equiv$ را با $\sim$ جایگزین کنید.

واقعیت که طبق خاصیت تقارن $a \sim c$، نشان دهید که $[a] \subseteq [c]$. بنابراین $[a] = [c]$. بالعکس، فرض کنید که $[a] = [c]$. چون طبق خاصیت انعکاسی $a \sim a$، داریم $a \in [a]$، و در نتیجه $a \in [c]$. تعریف $[c]$ نشان می‌دهد که $a \sim c$. ■

به طور کلی برای دو مجموعه، سه حالت محتمل است: یا دو مجموعه مساویند یا دو مجموعه مجزا هستند و یا دو مجموعه در بعضی (ولی نه تمام) عناصر مشترکند. در کلاس‌های هم‌ارزی، احتمال سوم نمی‌تواند رخ دهد.

نتیجه ت.۲. گیریم $\sim$ یک رابطه هم‌ارزی روی مجموعهٔ A باشد. آنگاه هر دو کلاس هم‌ارزی یا مجزا هستند و یا برابر می‌باشند.

برهان. گیریم $[a]$ و $[c]$ کلاس‌های هم‌ارزی باشند. اگر این دو کلاس مجزا باشند چیزی برای اثبات نمی‌ماند. اگر مجزا نباشند، آنگاه $[a] \cap [c]$ ناتهی است، و طبق تعریف عضو b وجود دارد بطوری که $b \in [a]$ و $b \in [c]$. طبق تعریف کلاس هم‌ارزی، $a \sim b$ و $b \sim c$. در نتیجه طبق خاصیت تعدی و تقارن، $a \sim c$. بنابراین طبق قضیه ت.۱، $[a] = [c]$. ■

یک افراز مجموعه A یک خانواده از زیرمجموعه‌های ناتهی و دوبدو مجزای[۳۰] A است که اجتماعشان برابر A می‌باشد. هر رابطه هم‌ارزی $\sim$ روی A منجر به یک افراز می‌شود، که اینک به توضیح آن می‌پردازیم. چون برای هر $a \in A$، $a \in [a]$، هر کلاس هم‌ارزی ناتهی است و هر عضو A در یک کلاس است. کلاس‌های هم‌ارزی متمایز طبق نتیجه ت.۲ مجزا هستند. بنابراین

کلاس‌های هم‌ارزی متمایز یک رابطه هم‌ارزی روی یک مجموعه A یک افراز از A بوجود می‌آورد.

بالعکس، هر افراز از مجموعه A منجر به یک رابطه هم‌ارزی می‌شود که کلاس‌های هم‌ارزی آن دقیقاً زیرمجموعه‌های این افراز می‌باشد (تمرین ۲۱).

تمرینها

A.۱. گیریم P یک صفحه باشد. اگر p و q نقاطی در P باشند، رابطه $p \sim q$ را به معنای این که p و q به فاصله یکسانی از مبداء می‌باشند تعریف می‌کنیم. ثابت کنید که $\sim$ یک رابطه هم‌ارزی روی P است.

۳۰) یعنی هر دو تا از این زیرمجموعه‌ها مجزا می‌باشند.

۲. روی مجموعه اعداد گویای $\mathbb{Q}$ یک رابطه تعریف کنید: $r \sim s$ اگر و تنها اگر $r - s \in \mathbb{Z}$. ثابت کنید که $\sim$ یک رابطه هم‌ارزی است.

۳. (الف) ثابت کنید که رابطه زیر روی مجموعه اعداد حقیقی $\mathbb{R}$ یک رابطه هم‌ارزی است: $a \sim b$ اگر و تنها اگر $\cos a = \cos b$.

(ب) کلاس هم‌ارزی 0 و کلاس هم‌ارزی $\pi/2$ را توصیف کنید.

۴. اگر m و n خطوطی در یک صفحه P باشند، رابطه $m \sim n$ را به معنی آن که m و n موازیند تعریف کنید. آیا $\sim$ یک رابطه هم‌ارزی روی P است؟

۵. (الف) رابطه $\sim$ را روی صفحه مختصات معمولی توسط $(x, y) \sim (u, v)$ اگر و تنها اگر $x = u$ تعریف کنید. ثابت کند که $\sim$ یک رابطه هم‌ارزی است.

(ب) کلاس‌های هم‌ارزی این رابطه را تعریف کنید.

۶. ثابت کنید که رابطه زیر روی صفحه مختصات یک رابطه هم‌ارزی است: $(x, y) \sim (u, v)$ اگر و تنها اگر $x - u$ یک عدد صحیح باشد.

۷. گیریم $f : A \to B$ یک تابع باشد. ثابت کنید رابطه زیر یک رابطه هم‌ارزی روی A است: $u \sim v$ اگر و تنها اگر $f(u) = f(v)$.

۸. گیریم $A = \{1, 2, 3\}$. از تعریف رابطه به صورت زوج مرتب استفاده کنید تا یک رابطه روی A با خواص بیان شده ارائه کنید:

(الف) انعکاسی، نامتقارن، نامتعدی.

(ب) متقارن، ناانعکاسی، نامتعدی.

(پ) متعدی، ناانعکاسی، نامتقارن.

(ت) انعکاسی و متقارن، نامتعدی.

(ث) انعکاسی و متعدی، نامتقارن.

(ج) متقارن و متعدی، ناانعکاسی.

۹. در هر یک از روابط زیر کدامیک از خواص (انعکاسی، متقارن و متعدی) برقرار است؟

(الف) $a < b$ روی مجموعه اعداد حقیقی $\mathbb{R}$.

(ب) $A \subseteq B$ روی مجموعه تمام زیرمجموعه‌های یک مجموعه S.

(پ) $a \neq b$ روی مجموعه تمام اعداد حقیقی $\mathbb{R}$.

(ت) $(-1)^a = (-1)^b$ روی مجموعه اعداد صحیح $\mathbb{Z}$.

B۱۰. اگر r یک عدد حقیقی باشد، آنگاه $[\![r]\!]$، بزرگترین عدد صحیح نابیشتر از r را نشان می‌دهد، برای مثال $[\![\pi]\!] = ۳$، $[\![۷]\!] = ۷$ و $[\![-۱/۵]\!] = -۲$. ثابت کنید که رابطه زیر روی $\mathbb{R}$ یک رابطه هم‌ارزی است: $r \sim s$ اگر و تنها اگر $[\![r]\!] = [\![s]\!]$.

۱۱. گیریم $\sim$ روی مجموعه اعداد حقیقی ناصفر $\mathbb{R}^*$ به صورت زیر تعریف شده باشد، $a \sim b$ اگر و تنها اگر $a/b \in \mathbb{Q}$. ثابت کنید که $\sim$ یک رابطه هم‌ارزی است.

۱۲. آیا رابطه زیر یک رابطه هم‌ارزی روی $\mathbb{R}$ است: $a \sim b$ اگر و تنها اگر $k \in \mathbb{Z}$ موجود باشد به طوری که $a = ۱۰^k b$.

۱۳. در مجموعه چندجمله‌ایهای با ضرایب حقیقی $\mathbb{R}[x]$، تعریف کنید: $f(x) \sim g(x)$ اگر و تنها اگر $f'(x) = g'(x)$، که در آن " $'$ " مشتق را نشان می‌دهد. ثابت کنید که $\sim$ یک رابطه هم‌ارزی روی $\mathbb{R}[x]$ است.

۱۴. گیریم T مجموعهٔ تمام توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$ باشد و تعریف کنید $f \sim g$ اگر و تنها اگر $f(۲) = g(۲)$. ثابت کنید که $\sim$ یک رابطه هم‌ارزی است.

۱۵. ثابت کنید که رابطه تعریف شده زیر روی $\mathbb{Z}$ یک رابطه هم‌ارزی است: $a \sim b$ اگر و تنها اگر (پیمانه ۶) $a^۲ \equiv b^۲$.

۱۶. گیریم $S = \{(a,b) \mid a,b \in \mathbb{Z}, b \neq ۰\}$ و تعریف کنید $(a,b) \sim (c,d)$ اگر و تنها اگر $ad = bc$. ثابت کنید که $\sim$ یک رابطه هم‌ارزی روی S است.

۱۷. گیریم $\sim$ یک رابطه متقارن و متعدی روی یک مجموعه A باشد. در برهان زیر برای اثبات این که $\sim$ انعکاسی است چه چیز غلط است: طبق تقارن $a \sim b$ ایجاب می‌کند که $b \sim a$، آنگاه طبق تعدی $a \sim b$ و $b \sim a$ ایجاب می‌کند $a \sim a$. [تمرین ۸ (ج) را نیز ملاحظه کنید.]

۱۸. گیریم G یک گروه باشد و تعریف کنید $a \sim b$ اگر و تنها اگر $c \in G$ موجود باشد به طوری که $b = c^{-۱}ac$. ثابت کنید که $\sim$ روی G یک رابطه هم‌ارزی است.

۱۹. (الف) گیریم K زیرگروهی از G باشد و تعریف کنید $a \sim b$ اگر و تنها اگر $a^{-1}b \in K$. ثابت کنید که $\sim$ یک رابطه هم‌ارزی روی G است.

۲۰. گیریم G زیرگروهی از S_n باشد. یک رابطه روی مجموعه $\{1, 2, \ldots, n\}$ به صورت زیر تعریف کنید: $a \sim b$ اگر و تنها اگر برای برخی σ در G، $a = \sigma(b)$. ثابت کنید که $\sim$ یک رابطه هم‌ارزی است.

۲۱. گیریم A یک مجموعه و $\{A_i \mid i \in I\}$ یک افراز از A باشد. یک رابطه روی A به صورت زیر تعریف کنید: $a \sim b$ اگر و تنها اگر a و b در یک زیرمجموعه از این افراز باشد (یعنی، $k \in I$ وجود دارد به طوری که $a \in A_k$ و $b \in A_k$).

(الف) ثابت کنید که $\sim$ یک رابطه هم‌ارزی روی A است.

(ب) ثابت کنید که کلاس‌های هم‌ارزی $\sim$ دقیقاً زیرمجموعه‌های A_i این افراز می‌باشند.

* * * * *

پیوست ث

قضیه دوجمله‌ای

پیوست پ و بخش ۲.۳ پیشنیازهای این پیوست می‌باشد. مطالب این پیوست در بخش ۶.۹ و تمرینهای موردی در جاهای دیگر مورد استفاده قرارگرفته است.

همان‌طورکه در مثال ۱۸.۳ دیدیم برای هر a، b در یک حلقه جابجایی R

$$(a+b)^2 = a^2 + 2ab + b^2.$$

با استفاده از توزیع‌پذیری و جابجایی ضرب، محاسبات مشابه نشان می‌دهد که

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

این مثال‌ها الگویی را ظاهر می‌کند که ممکن است چندان واضح بنظر نرسد، مگر آن که ابتدا حقایقی چند مورد توجه قرارگیرد.

بخاطر آورید که $0! = 1$ برابر با ۱ تعریف شده است و این که برای هر عدد صحیح مثبت n نماد $n!$ عدد $1 \times 2 \times 3 \times \cdots \times (n-2)(n-1)n$ را نشان می‌دهد. برای هر k، که $0 \leq k \leq n$ ضریب دوجمله‌ای $\binom{n}{k}$ به‌صورت $n!/k!(n-k)!$ تعریف می‌شود. این عدد در نگاه اول ممکن است یک کسر به نظر آید ولی هر ضریب دوجمله‌ای در واقع عددی صحیح است (تمرین ۶). برای مثال،

$$\binom{4}{1} = \frac{4!}{1!(4-1)!} = \frac{4 \times 3 \times 2 \times 1}{1 \times 3 \times 2 \times 1} = 4$$

و به طور مشابه، $\frac{4!}{2!2!} = \binom{4}{2} = 6$. توجه کنید که این اعداد به عنوان ضرایب عبارت $(a+b)^4$ در فوق ظاهر شده‌اند، در واقع می‌توانید بررسی کنید که

$$(a+b)^4 = a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + b^4.$$

این مصداقی از قضیه زیر است:

قضیه ث.۱. (قضیه دو جمله‌ای) گیریم R یک حلقه جابجایی باشد و $a, b \in R$. آنگاه برای هر عدد صحیح مثبت n،

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + b^n.$$

برهان. برهان با استقراء روی n انجام می‌شود. اگر $n = 1$، قضیه بیان می‌کند که، $(a+b)^1 = a^1 + b^1$، که مسلماً درست است. فرض کنید که قضیه برای $n = k$ درست است، یعنی این که

$$(a+b)^k = a^k + \binom{k}{1}a^{k-1}b + \cdots + \binom{k}{r}a^{k-r}b^r + \cdots + \binom{k}{k-1}ab^{k-1} + b^k.$$

باید از این فرض استفاده کنیم تا درستی قضیه را برای $n = k+1$ ثابت کنیم. طبق تعریف توان داریم $(a+b)^{k+1} = (a+b)(a+b)^k$. با بکارگیری فرض استقراء برای $(a+b)^k$ و با استفاده

از توزیع‌پذیری و جابجایی ضرب داریم،

$$(a+b)^{k+1} = (a+b)(a+b)^k$$
$$= (a+b)[a^k + \binom{k}{1}a^{k-1}b + \cdots + \binom{k}{r}a^{k-r}b^r + \cdots + \binom{k}{k-1}ab^{k-1} + b^k]$$
$$= a[a^k + \binom{k}{1}a^{k-1}b + \cdots + \binom{k}{r}a^{k-r}b^r + \cdots + \binom{k}{k-1}ab^{k-1} + b^k]$$
$$+ b[a^k + \binom{k}{1}a^{k-1}b + \cdots + \binom{k}{r}a^{k-r}b^r + \cdots + \binom{k}{k-1}ab^{k-1} + b^k]$$
$$= [a^{k+1} + \binom{k}{1}a^k b + \cdots + \binom{k}{r}a^{k-r+1}b^r + \cdots + \binom{k}{k-1}a^2 b^{k-1} + ab^k]$$
$$+ [a^k b + \binom{k}{1}a^{k-1}b^2 + \cdots + \binom{k}{r}a^{k-r}b^{r+1} + \cdots + \binom{k}{k-1}ab^k + b^{k+1}]$$
$$= a^{k+1} + [\binom{k}{1} + 1]a^k b + [\binom{k}{2} + \binom{k}{1}]a^{k-1}b^2 + \cdots$$
$$+ [\binom{k}{k+1} + \binom{k}{r}]a^{k-r}b^{r+1} + \cdots + [1 + \binom{k}{k-1}]ab^k + b^{k+1}.$$

تمرین ۵ (که شما باید آن را حل کنید) نشان می‌دهد که برای $r = 0, 1, \ldots, k$

$$\binom{k}{r+1} + \binom{k}{r} = \binom{k+1}{r+1}.$$

این حقیقت را برای هر یک از ضرایب در آخرین معادله فوق بکار برید. برای مثال، $\binom{k+1}{1} = \binom{k}{0} + \binom{k}{1} = 1 + \binom{k}{1}$، و $\binom{k+1}{2} = \binom{k}{1} + \binom{k}{2}$، و همین‌طور الی آخر. آنگاه از قسمتهای اول و آخر معادله فوق داریم

$$(a+b)^{k+1} = a^{k+1} + \binom{k+1}{1}a^k b + \binom{k+1}{2}a^{k-1}b^2 + \cdots$$
$$+ \binom{k+1}{r+1}a^{k-r}b^{r+1} + \cdots + \binom{k+1}{k}ab^k + b^{k+1}.$$

بنابراین قضیه برای $n = k+1$ درست است و بدین جهت طبق استقراء برای هر عدد صحیح مثبت n درست است. ■

تمرینها

A.۱. گیریم x و y اعداد حقیقی باشند. ضریب $x^۵y^۸$ را در عبارت $(۲x - y^۲)^۹$ پیدا کنید. [راهنمایی. قضیه ث.۱ را با شرط $a = ۲x$، $b = -y^۲$ بکار برید.]

۲. اگر x و y اعداد حقیقی باشند، ضریب $x^{۱۲}y^۶$ در عبارت $(x^۳ - ۳y)^{۱۰}$ چیست؟

B.۳. گیریم r و n اعداد صحیح باشند و $۰ < r < n$. ثابت کنید که $\binom{n}{r} = \binom{n}{n-r}$.

۴. ثابت کنید که برای عدد صحیح مثبت n، $\binom{n}{۰} + \binom{n}{۱} + \binom{n}{۲} + \cdots + \binom{n}{n} = ۲^n$. [راهنمایی: $(۱ + ۱)^n = ۲^n$.]

۵. گیریم r و k اعداد صحیحی باشند به طوری که $۰ \le r \le k - ۱$. ثابت کنید که $\binom{k}{r} + \binom{k}{r+۱} = \binom{k+۱}{r+۱}$. [راهنمایی: از این واقعیت که

$$(k - r)(k - (r + ۱))! = (k - r)! = ((k + ۱) - (r + ۱))!$$

استفاده کنید تا هر جمله طرف چپ را به صورت کسری با مخرج $(k - r)!(k + ۱)!$ بیان کنید. این کسرها را جمع کنید، صورت را ساده کنید و نتیجه بدست آمده را با $\binom{k+۱}{r+۱}$ مقایسه کنید.]

۶. گیریم n عدد صحیح مثبتی باشد. استقراء ریاضی را بکار برید تا این گزاره را ثابت کنید: برای هر عدد صحیح r به طوری که $۰ \le r \le n$، $\binom{n}{r}$ یک عدد صحیح است. [راهنمایی: برای $n = ۱$ خیلی ساده است که حساب کنیم $\binom{۱}{۰} = ۱ = \binom{۱}{۱}$؛ فرض کنید این جمله برای $n = k$ درست باشد و از تمرین ۵ استفاده کنید تا نشان دهید این جمله برای $n = k + ۱$ درست است.]

۷. در اینجا پنج سطر اول **مثلث خیام-پاسکال** آمده است:

سطر ۰:			۱		
سطر ۱:			۱	۱	
سطر ۲:		۱	۲	۱	
سطر ۳:		۱	۳	۳	۱
سطر ۴:	۱	۴	۶	۴	۱

توجه کنید که هر درایه در یک سطر مفروض (بجز ۱های انتهایی) مجموع دو عدد بالای آن در سطر پیش است. برای مثال اولین ۴ در سطر ۴ مجموع ۱ و ۳ در سطر ۳ می‌باشد؛ به طور مشابه، ۶ در سطر ۴ مجموع ۳ و ۳ در سطر ۳ می‌باشد.

(الف) سه سطر بعدی مثلث خیام-پاسکال را بنویسید.

(ب) ثابت کنید که درایه‌های سطر n ام مثلث خیام-پاسکال دقیقاً ضرایب عبارت $(a+b)^n$، یعنی $\binom{n}{0}$، $\binom{n}{1}$، $\binom{n}{2}$،...، $\binom{n}{n}$ می‌باشد. [تمرین ۵ می‌تواند مفید باشد.]

* * * * *

پیوست ج
جبر ماتریسی

این پیوست را می‌توان در زمانی دلخواه بعد از بخش ۱.۳ مطالعه نمود ولی فقط در فصل شانزدهم مورد نیاز است. در سراسر این پیوست، R حلقه‌ای با عضو همانی ضربی است.

حلقهٔ ماتریس‌های ۲×۲ با درایه‌های در $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ در بخش ۱.۳ معرفی شدند. این ماتریس‌ها حالت‌های خاص این تعریف است: یک ماتریس $n \times m$ روی R یک آرایه از n سطر افقی و m ستون عمودی به صورت زیر است؛

$$\begin{pmatrix} r_{۱۱} & r_{۱۲} & r_{۱۳} & \cdots & r_{۱m} \\ r_{۲۱} & r_{۲۲} & r_{۲۳} & \cdots & r_{۲m} \\ r_{۳۱} & r_{۳۲} & r_{۳۳} & \cdots & r_{۳m} \\ \vdots & \vdots & \vdots & & \vdots \\ r_{n۱} & r_{n۲} & r_{n۳} & \cdots & r_{nm} \end{pmatrix}$$

که در آن هر $r_{ij} \in R$. برای مثال

$$A = \begin{pmatrix} ۷ & -۶ & ۴ & ۱۰ & ۰ \\ ۱ & ۰ & ۵ & -۲ & ۱ \\ ۳ & ۳ & ۴ & ۱۲ & ۹ \\ ۰ & ۵ & ۲ & ۰ & -۸ \end{pmatrix} \qquad B = \begin{pmatrix} ۱ & ۴ & ۰ \\ ۲ & ۱ & ۳ \\ ۳ & ۲ & ۰ \end{pmatrix} \qquad C = \begin{pmatrix} ۱ & ۰ & ۱ & ۰ \\ ۰ & ۱ & ۱ & ۱ \end{pmatrix}$$

۴×۵ روی $\mathbb{Z}$ $\qquad$ ۳×۳ روی $\mathbb{Z}_۵$ $\qquad$ ۲×۴ روی $\mathbb{Z}_۲$

ماتریس‌ها معمولاً با حروف بزرگ نشان داده می‌شوند و درایه‌های آنها با حروف کوچک، با زیرنمایه‌های دوگانه که سطر و ستونی را که درایه در آن ظاهر می‌شود نشان می‌دهند. برای مثال، در ماتریس $A = (a_{ij})$ فوق، درایهٔ سطر ۴ و ستون ۲ برابر است با $a_{۴۲} = ۵$. در ماتریس C فوق داریم، $c_{۱۲} = ۰$ و $c_{۲۳} = ۱$. بدین دلیل برای مثال سطر i–ام از ماتریس (r_{ij}) برابر است با

$$r_{i۱} \quad r_{i۲} \quad r_{i۳} \quad r_{i۴} \cdots \quad r_{im}.$$

ماتریس $n \times m$ صفر، ماتریسی $n \times m$ای است که تمام درایه‌های آن ۰_R است. ماتریس همانی I_n ماتریسی $n \times n$ است که درایه‌های ۱-۱، ۲-۲، ۳-۳، ...، $n-n$ آن ۱_R است و بقیه درایه‌ها ۰_R می‌باشد. برای مثال، روی حلقه $\mathbb{Z}$:

$$I_۳ = \begin{pmatrix} ۱ & ۰ & ۰ \\ ۰ & ۱ & ۰ \\ ۰ & ۰ & ۱ \end{pmatrix} \qquad I_۴ = \begin{pmatrix} ۱ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۱ \end{pmatrix} \qquad I_۵ = \begin{pmatrix} ۱ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۱ \end{pmatrix}$$

ماتریس همانی I_n را می‌توان مختصراً به صورت $I_n = (\delta_{ij})$ نمایش داد که در آن δ_{ij} نماد **دلتای کرونکر** است که با ضابطه زیر تعریف می‌شود:

$$\delta_{ij} = \begin{cases} ۱_R & \text{اگر } i = j \\ ۰_R & \text{اگر } i \neq j \end{cases}$$

گاهی اوقات مناسب است که یک ماتریس بزرگ را ماتریسی که از دو ماتریس کوچکتر ساخته شده است در نظر بگیریم. برای مثال، اگر A ماتریس ۲×۳

$$\begin{pmatrix} ۴ & ۲ \\ ۱ & ۰ \\ ۳ & ۵ \end{pmatrix}$$

روی $\mathbb{Z}$ باشد، آنگاه $(A \mid I_۳)$ ماتریس ۵×۳

$$\begin{pmatrix} ۱ & ۰ & ۰ & ۴ & ۲ \\ ۰ & ۱ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۱ & ۳ & ۵ \end{pmatrix}$$

را نشان می‌دهد. به طور مشابه اگر $A = \begin{pmatrix} ۲ & ۳ \\ ۴ & ۶ \end{pmatrix}$، آنگاه $\frac{A}{I_۲}$ ماتریس $\begin{pmatrix} ۲ & ۳ \\ ۴ & ۶ \\ ۱ & ۰ \\ ۰ & ۱ \end{pmatrix}$ را نشان می‌دهد.

اگر $A = (a_{ij})$ و $B = (b_{ij})$ ماتریس‌های $n \times m$ باشند، آنگاه مجموع ماتریسی $A + B$ ماتریسی $n \times m$ است که درایه $ij-$ ام آن $a_{ij} + b_{ij}$ می‌باشد. به بیان دیگر، نظیر به نظیر درایه‌های دو ماتریس را جمع کنید، همان‌طور که در این مثال روی $\mathbb{Z}_۵$ دیده می‌شود:

$$\begin{pmatrix} ۱ & ۳ & ۴ \\ ۰ & ۲ & ۱ \end{pmatrix} + \begin{pmatrix} ۳ & ۲ & ۰ \\ ۱ & ۴ & ۲ \end{pmatrix} = \begin{pmatrix} ۴ & ۰ & ۴ \\ ۱ & ۱ & ۳ \end{pmatrix}.$$

اگر A و B دارای اندازه‌های متفاوت باشند، مجموع آنها تعریف نشده است. اگر A، B، C ماتریس‌های $n \times m$ باشند، آنگاه تمرین ۳ نشان می‌دهد که جمع ماتریسی خاصیت جابجایی دارد $[A + B = B + A]$ و شرکت‌پذیر است $[A + (B + C) = (A + B) + C]$. ماتریس $n \times m$ صفر به عنوان همانی جمع عمل می‌کند (تمرین ۴).

به دلایلی که در درس جبر خطی آورده می‌شود، حاصل‌ضرب ماتریس‌های A و B فقط وقتی تعریف می‌شود که تعداد ستون‌های A درست برابر تعداد سطرهای B باشد. ساده‌ترین حالت، حاصل‌ضرب یک ماتریس $m \times ۱$، A شامل تنها یک سطر $(a_۱ a_۲ \cdots a_m)$ و یک ماتریس $۱ \times m$،

B شامل تنها یک ستون $\begin{pmatrix} b_۱ \\ b_۲ \\ \vdots \\ b_m \end{pmatrix}$ می‌باشد[۳۱]. این حاصل‌ضرب بنا به تعریف، ماتریسی است ۱×۱ که تنها درایه‌اش عضو

$$a_۱b_۱ + a_۲b_۲ + a_۳b_۳ + a_۴b_۴ + \cdots + a_mb_m$$

می‌باشد. برای مثال، روی $\mathbb{Z}$

$$\begin{pmatrix} ۲ & ۳ & ۱ \end{pmatrix} \begin{pmatrix} ۴ \\ ۰ \\ ۲ \end{pmatrix} = ۲ \times ۴ + ۳ \times ۰ + ۱ \times ۲ = ۱۰ \qquad (*)$$

اگر A یک ماتریس $n \times m$ و B یک ماتریس $m \times k$ باشد، آنگاه **حاصل‌ضرب ماتریسی** AB ماتریس $n \times k$، (c_{ij}) است، که درایه واقع در جای i-j آن حاصل‌ضرب سطر i-ام A و ستون j-ام B می‌باشد:

$$c_{ij} = a_{i۱}b_{۱j} + a_{i۲}b_{۲j} + a_{i۳}b_{۳j} + a_{i۴}b_{۴j} + \cdots + a_{im}b_{mj} = \sum_{r=۱}^{m} a_{ir}b_{rj}$$

مثال ۱. حاصل‌ضرب

$$A = \begin{pmatrix} ۲ & ۳ & ۱ \\ ۱ & ۵ & ۰ \end{pmatrix} \quad \text{و} \quad B = \begin{pmatrix} ۴ & ۲ & ۶ & ۳ \\ ۰ & ۱ & ۲ & ۱ \\ ۲ & ۶ & ۰ & ۲ \end{pmatrix}$$

یک ماتریس ۴×۲ است که درایه ۱-۱ آن برابر ۱۰ (حاصل‌ضرب سطر ۱ از A و ستون ۱ از B همان‌طور که در $(*)$ بالا نشان داده شده است) می‌باشد. درایه واقع درجای ۳-۲ ماتریس AB حاصل‌ضرب سطر ۲ از A و ستون ۳ از B است:

$$۱ \times ۶ + ۵ \times ۲ + ۰ \times ۰ = ۱۶.$$

---

۳۱) یک ماتریس با تنها یک سطر یک **بردار سطری** نامیده می‌شود و یک ماتریس با تنها یک ستون **بردار ستونی** نامیده می‌شود. استفاده از زیرنمایه‌های یگانه برای نمایش درایه‌های بردارهای سطری و ستونی کافی است.

محاسبات مشابه نشان می‌دهد که

$$AB = \begin{pmatrix} ۲ & ۳ & ۱ \\ ۱ & ۵ & ۰ \end{pmatrix} \begin{pmatrix} ۴ & ۲ & ۶ & ۳ \\ ۰ & ۱ & ۲ & ۱ \\ ۲ & ۶ & ۰ & ۲ \end{pmatrix} = \begin{pmatrix} ۱۰ & ۱۳ & ۱۸ & ۱۱ \\ ۴ & ۷ & ۱۶ & ۸ \end{pmatrix}.$$

حاصل‌ضرب BA تعریف نشده است زیرا B چهارستون دارد ولی A فقط دو سطر دارد.

مثال ۲. حاصل‌ضرب بردار سطری $\begin{pmatrix} ۲ & ۰ & ۱ \end{pmatrix}$ و ماتریس ۳×۴، B ارائه شده در آخرین مثال، بردار سطری $\begin{pmatrix} ۷ & ۶ & ۱۴ & ۸ \end{pmatrix}$ می‌باشد زیرا

$$\begin{pmatrix} ۱ & ۰ & ۲ \end{pmatrix} \begin{pmatrix} ۴ & ۲ & ۶ & ۳ \\ ۰ & ۱ & ۲ & ۱ \\ ۲ & ۶ & ۰ & ۲ \end{pmatrix} = \begin{pmatrix} ۸ & ۱۴ & ۶ & ۷ \end{pmatrix}.$$

اگر A، B، C ماتریس‌های با اندازه‌های مناسب باشند به طوری که هر یک از حاصل‌ضرب‌های AB و BC تعریف شده باشد، آنگاه ضرب ماتریسی شرکت‌پذیر است: $A(BC) = (AB)C$ (تمرین ۷). به طور مشابه، اگر E، F، G ماتریس‌هایی باشند به طوری که EG و FG تعریف شوند، آنگاه قانون توزیع‌پذیری برقرار است: $(E+F)G = EG + FG$ (تمرین ۵). ماتریس‌های همانی مانند عناصر همانی برای ضرب عمل می‌کنند، بدین معنی که: اگر A یک ماتریس $n \times m$ باشد، آنگاه $I_n \cdot A = A$ و $A \cdot I_m = A$ (تمرین ۶). حتی وقتی هر دو حاصل‌ضرب AB و BA تعریف شده‌اند، ضرب ماتریسی ممکن است جابجایی نباشد (مثال ۶.۳ را ملاحظه کنید).

مجموعه $M_n(R)$، مجموعه تمام ماتریس‌های $n \times n$ روی حلقه R را نشان می‌دهد. چون تمام ماتریس‌های واقع در $M_n(R)$ دارای تعداد سطر و ستون برابر می‌باشند برای هر $A, B \in M_n(R)$ ماتریس‌های $A+B$ و AB و BA تعریف شده‌اند. خواص جمع و ضرب ماتریسی فهرست شده در بالا برهان قضیه زیر را فراهم می‌کند:

قضیه ج.۱. اگر R یک حلقه یکدار باشد، آنگاه $M_n(R)$، مجموعه تمام ماتریس‌های $n \times n$ روی R، یک حلقه (غیرجابجایی) با عضو همانی I_n می‌باشد.

تمرینها

توجه. تمام ماتریس‌ها روی یک حلقه یکدار R تعریف شده‌اند، مگر خلاف آن ذکر شود.

۱.A. فرض کنید A و B ماتریس‌هایی روی $\mathbb{Z}$ باشند. $A+B$ را پیدا کنید:

(الف) $A=\begin{pmatrix} ۱ & ۲ & -۲ & ۰ \\ ۳ & ۵ & ۷ & ۱۱ \end{pmatrix}$ $\quad B=\begin{pmatrix} ۰ & -۸ & ۲ & ۴ \\ ۶ & ۰ & ۴ & ۱ \end{pmatrix}$

(ب) $A=\begin{pmatrix} ۱ & -۲ & ۰ \\ ۳ & ۰ & ۴ \\ ۰ & ۷ & -۶ \\ ۱ & ۶ & ۰ \end{pmatrix}$ $\quad B=\begin{pmatrix} ۳ & ۰ & ۲ \\ ۴ & ۱ & ۶ \\ ۰ & ۱ & ۰ \\ ۲ & -۵ & ۷ \end{pmatrix}$

۲. فرض کنید A و B ماتریس‌هایی روی $\mathbb{Z}_۶$ باشند. وقتی که حاصل‌ضرب تعریف شده باشد AB و BA را پیدا کنید:

(الف) $A=\begin{pmatrix} ۲ & ۴ \\ ۱ & ۵ \\ ۳ & ۰ \end{pmatrix}$ $\quad B=\begin{pmatrix} ۱ & ۰ & ۱ \\ ۲ & ۳ & ۲ \end{pmatrix}$

(ب) $A=\begin{pmatrix} ۱ & ۴ \\ ۵ & ۲ \end{pmatrix}$ $\quad B=\begin{pmatrix} ۰ & ۵ & ۳ \\ ۱ & ۰ & ۲ \end{pmatrix}$

(پ) $A=\begin{pmatrix} ۳ & ۲ & ۱ & ۰ \end{pmatrix}$ $\quad B=\begin{pmatrix} ۱ & ۰ & ۰ \\ ۰ & ۱ & ۰ \\ ۰ & ۰ & ۱ \\ ۱ & ۱ & ۱ \end{pmatrix}$

۳.B. گیریم $A=(a_{ij})$، $B=(b_{ij})$، و $C=(c_{ij})$ ماتریس‌های $n\times m$ باشند. ثابت کنید که

(الف) $A+B=B+A$ $\qquad$ (ب) $A+(B+C)=(A+B)+C$

۴. اگر $A=(a_{ij})$ یک ماتریس $n\times m$ و Z ماتریس $n\times m$ صفر باشد، ثابت کنید که $A+Z=A$.

۵. (الف) گیریم E و F بردارهای سطری $1 \times m$ و $G = (g_{ij})$ یک ماتریس $m \times k$ باشد، ثابت کنید که $(E+F)G = EG + FG$.

(ب) گیریم $E = (e_{ij})$ و $F = (f_{ij})$ ماتریس‌های $n \times m$ و $G = (g_{ij})$ یک ماتریس $m \times k$ باشد. ثابت کنید که $(E+F)G = EG + FG$.

۶. اگر A یک ماتریس $n \times m$ باشد، ثابت کنید که $I_n \cdot A = A$ و $A \cdot I_m = A$.

۷. گیریم $A = (a_{ij})$ یک ماتریس $n \times m$، $B = (b_{ij})$ یک ماتریس $m \times k$ و $C = (c_{ij})$ یک ماتریس $k \times p$ باشد. ثابت کنید که $A(BC) = (AB)C$ [راهنمایی: $BC = (d_{ij})$ که در آن، $d_{ij} = \sum_{r=1}^{k} b_{ir}c_{rj}$، $AB = (e_{ir})$، که در آن $e_{ir} = \sum_{t=1}^{m} a_{it}b_{tr}$. درایه ij-ام $A(BC)$ برابر است

$$\sum_{t=1}^{m} a_{it}d_{tj} = \sum_{t=1}^{m} a_{it}(\sum_{r=1}^{k} b_{tr}c_{rj}) = \sum_{t=1}^{m}\sum_{r=1}^{k} a_{it}b_{tr}c_{rj}.$$

نشان دهید که درایه ij-ام $(AB)C$ نیز برابر همین مجموع دوگانه است.]

* * * * *

پیوست چ
چندجمله‌ایها

درباره نماد "x" که در چندجمله‌ایها ظاهر می‌شود در ریاضیات دبیرستانی ابهامی وجود دارد، بدین معنی که x گاهی نماینده یک عدد مشخص است (مانند آنچه در معادله $۲x - ۶ = ۱۷$ آمده است) و زمانی x بنظر نمی‌رسد که نماینده عددی باشد بلکه عیناً نمادی است که به صورت جبری با آن کار می‌شود (مانند تمرینهایی همچون $(x+۳)(x-۵) = x^۲ - ۲x - ۱۵$)[۳۲]. هدف ما در اینجا آن است که یک تعریف دقیق از "چندجمله‌ای" ارائه دهیم که این ابهام را برطرف کند. پیشنیازهای این مبحث، جبر دبیرستانی و فصل ۳ می‌باشد.

به عنوان پیش‌درآمدی از بحث رسمی، توجه داشته باشید که چندجمله‌ایهای دبیرستانی را می‌توان بدون هیچگونه ذکری از x بیان کرد. برای مثال، $۲x^۳ - ۶x + ۵$ به طور کامل توسط ضرایبش $(۲, ۰, -۶, ۵)$

---

۳۲) گاهی اوقات هم، x به عنوان متغیری که می‌تواند بینهایت مقدار بگیرد بکار می‌رود (همان‌طور که در تابع $f(x) = x^۳ - x$ دیده می‌شود). این کاربرد در بخش ۴.۴ مورد مطالعه قرار گرفته است.

تعیین می‌گردد[۳۳]. ولی آن را می‌توان به صورت $۵ + ۶x + ۰x^۲ - ۲x^۳ + ۰x^۴ + ۰x^۵ + ۰x^۶$ هم نوشت. برای این که این جمله‌های صفر را تجویز نماییم ضرایب را به صورت یک دنباله نامتناهی $(۵, ۶, ۰, -۲, ۰, ۰, ۰, \dots)$ که به صفر ختم می‌شود فهرست می‌کنیم.

جمع چندجمله‌ایها در این نماد جدید به نسبت زیادی مانند قبل می‌باشد: جمع ضرایب توانهای متناظر x یعنی، جمع مولفه به مولفه دنباله‌ها:

$$\begin{array}{ll} ۵ + ۶x \quad - ۲x^۳ & (۵,\ ۶,\ ۰, -۲, ۰, ۰, ۰, \dots) \\ \underline{۳ - ۲x + ۵x^۲ - ۴x^۳} & \underline{(۳, -۲, ۵, -۴, ۰, ۰, ۰, \dots)} \\ ۸ + ۴x + ۵x^۲ - ۶x^۳ & (۸,\ ۴,\ ۵, -۶, ۰, ۰, ۰, \dots) \end{array}$$

ضرب چندجمله‌ای‌ها را نیز می‌توان برحسب دنباله‌ها بیان کرد، همان‌طورکه در ذیل خواهیم دید. اگر این الگو را در ذهن خود نگهدارید به وضوح خواهید دید که قضایا و تعاریف رسمی از کجا آمده‌اند.

سراسر باقیماندهٔ این پیوست، R یک حلقه یکدار (که لزوماً جابجایی نیست) می‌باشد. **یک چندجمله‌ای با ضرایب در حلقه R** به صورت یک دنباله نامتناهی

$$(a_۰, a_۱, a_۲, a_۳, \dots)$$

تعریف می‌شود به طوری که هر $a_i \in R$ و فقط تعداد باپایانی از a_iها ناصفرند، یعنی k ای وجود دارد که برای هر $i > k$، $a_i = ۰$. عضوهای $a_i \in R$ **ضرایب** این چندجمله‌ای نامیده می‌شوند.

چندجمله‌ایهای $(a_۰, a_۱, a_۲, \dots)$ و $(b_۰, b_۱, b_۲, \dots)$ **برابرند** اگر به عنوان دنباله‌ها برابر باشند، یعنی، اگر $a_۰ = b_۰$ و $a_۱ = b_۱$ و به‌طورکلی برای هر $i \geq ۰$، $a_i = b_i$. **جمع چندجمله‌ایها** با $\oplus$ نشان داده می‌شود و با این قاعده تعریف می‌شود:

$$(a_۰, a_۱, a_۲, \dots) \oplus (b_۰, b_۱, b_۲, \dots) = (a_۰ + b_۰, a_۱ + b_۱, a_۲ + b_۲, \dots)$$

بررسی کنید که دنباله طرف راست در واقع یک چندجمله‌ای است، یعنی از مرحله‌ای به بعد، همهٔ مؤلفه‌ها صفر هستند (تمرین ۲).

ضرب چندجمله‌ای‌ها با نماد $\odot$ نشان داده می‌شود و با این قاعده تعریف می‌شود:

$$(a_۰, a_۱, a_۲, \dots) \odot (b_۰, b_۱, b_۲, \dots) = (c_۰, c_۱, c_۲, \dots)$$

۳۳) ۰ ضریب $x^۲$ است.

که در آن

$$
\begin{aligned}
c_0 &= a_0 b_0 \\
c_1 &= a_0 b_1 + a_1 b_0 \\
c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 \\
&\vdots \\
c_n &= a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + a_3 b_{n-3} + \cdots + a_{n-1} b_1 + a_n b_0 \\
&= \sum_{i=0}^{n} a_i b_{n-i}
\end{aligned}
$$

برای این که نشان دهید که حاصل‌ضربی که در اینجا تعریف شده است در واقع یک چندجمله‌ای است باید تحقیق کنید که از مرحله‌ای به بعد تمام مولفه‌های $(c_0, c_1, \dots)$ صفر می‌باشد (تمرین ۲).

قضیه چ.۱. گیریم R یک حلقه یکدار و P مجموعه تمام چندجمله‌ایهای با ضرایب در R باشد. آنگاه P یک حلقه یکدار است. اگر R جابجایی باشد، آنگاه P نیز چنین است.

برهان. تمرین ۲ نشان می‌دهد که P تحت جمع و ضرب بسته است. برای آن که نشان دهیم جمع در P جابجایی است، توجه می‌کنیم که چون R یک حلقه است برای تمام $a_i, b_i \in R$ داریم $a_i + b_i = b_i + a_i$ ؛ بنابراین در P

$$
\begin{aligned}
(a_0, a_1, a_2, \dots) \oplus (b_0, b_1, b_2, \dots) &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) \\
&= (b_0 + a_0, b_1 + a_1, b_2 + a_2 \dots) \\
&= (b_0, b_1, b_2, \dots) \oplus (a_0, a_1, a_2, \dots).
\end{aligned}
$$

شرکت‌پذیری جمع و قوانین توزیع‌پذیری به طور مشابه ثابت می‌شوند. به سادگی می‌توانید بررسی کنید که عضو همانی ضرب در P چندجمله‌ای $(1_R, 0_R, 0_R, 0_R, \dots)$ است، عضو صفر، چندجمله‌ای $(0_R, 0_R, 0_R, \dots)$ می‌باشد و جواب معادله $(a_0, a_1, a_2, \dots) + X = (0_R, 0_R, 0_R, \dots)$ برابر با $X = (-a_0, -a_1, -a_2, \dots)$ است.

برای تکمیل برهان این که P یک حلقه یکدار است باید نشان دهیم که ضرب شرکت‌پذیر است.

گیریم $A, B, C \in P$، که در آن

$$A = (a_0, a_1, a_2, \dots) \quad B = (b_0, b_1, b_2, \dots) \quad \text{و} \quad C = (c_0, c_1, c_2, \dots).$$

آنگاه n-امین مولفه $(A \odot B) \odot C$ برابر است با

$$\sum_{i=0}^{n} (ab)_i c_{n-i} = \sum_{i=0}^{n} [\sum_{j=0}^{i} a_j b_{i-j}] c_{n-i} = \sum_{i=0}^{n} \sum_{j=0}^{i} a_j b_{i-j} c_{n-i}. \qquad (*)$$

تمرین ۶ نشان می‌دهد که آخرین مجموع طرف راست دقیقاً برابر

$$\sum a_u b_v c_w \qquad (**)$$

می‌باشد که در آن مجموع روی تمام اعداد صحیح u، v، w محاسبه می‌شود که $u + v + w = n$ و $u \geq 0$، $v \geq 0$، $w \geq 0$. از طرف دیگر، n-امین مولفه $A \odot (B \odot C)$ برابر است با

$$\sum_{r=0}^{n} a_r (bc)_{n-r} = \sum_{r=0}^{n} a_r [\sum_{s=0}^{n-r} b_s c_{n-r-s}] = \sum_{r=0}^{n} \sum_{s=0}^{n-r} a_r b_s c_{n-r-s}.$$

تمرین ۶ نشان می‌دهد که آخرین مجموع طرف راست در برابری فوق نیز با مجموع (**) برابر است. چون n-امین مؤلفه $(A \odot B) \odot C$ و $A \odot (B \odot C)$ برای هر $n \geq 0$، برابر است، لذا $(A \odot B) \odot C = A \odot (B \odot C)$. برهان جمله آخر قضیه به خواننده واگذار می‌شود (تمرین ۳). ■

در نمادگذاری قبلی، چندجمله‌ایهای ثابت مثل اعداد معمولی هستند. در حالی که در نمادگذاری جدید، چندجمله‌ایهای ثابت در P به صورت $(r, 0_R, 0_R, 0_R, \dots)$ می‌باشند که اساساً همان حلقه R است، همانگونه که در قضیه زیر می‌بینیم:

قضیه چ.۲. گیریم P حلقه چندجمله‌ایهای با ضرایب در حلقه R باشد. گیریم R^* مجموعه تمام چندجمله‌ایها در P به صورت $(r, 0_R, 0_R, 0_R, \dots)$ باشد، که در آن $r \in R$. آنگاه R^* زیرحلقه P است و یکریخت با R می‌باشد.

برهان. تابع $f : R \to R^*$ تعریف شده با

$$f(r) = (r, 0_R, 0_R, 0_R, \dots)$$

را در نظر بگیرید. به سادگی می‌توانید بررسی کنید که f دوسویی است. به‌علاوه،

$$f(r+s) = (r+s, {}^\circ_R, {}^\circ_R, {}^\circ_R, \dots)$$
$$= (r, {}^\circ_R, {}^\circ_R, {}^\circ_R, \dots) \oplus (s, {}^\circ_R, {}^\circ_R, {}^\circ_R, \dots)$$

و

$$f(rs) = (rs, {}^\circ_R, {}^\circ_R, {}^\circ_R, \dots) = (r, {}^\circ_R, {}^\circ_R, {}^\circ_R, \dots) \odot (s, {}^\circ_R, {}^\circ_R, {}^\circ_R, \dots)$$
$$= f(r) \odot f(s)$$

بنابراین f یک یکریختی است و بدین جهت R^* یک زیرحلقه است. ■

اکنون که حقایق اساسی را ثابت کرده‌ایم، وقت آن رسیده است که نماد "قدیمی" چندجمله‌ای را احیاء کنیم. ابتدا می‌خواهیم چندجمله‌ایهای واقع در R^* بیشتر شبیه "ثابتها" (عناصر R) باشد، بنابراین

$(a, {}^\circ_R, {}^\circ_R, {}^\circ_R, \dots)$ با حرف پررنگ $\boldsymbol{a}$ نشان داده می‌شود.

سپس با بازگشت به مبداء اصلی نماد دنباله‌ای خودمان،

دنباله $({}^\circ_R, {}^1_R, {}^\circ_R, {}^\circ_R, {}^\circ_R, \dots)$ با x نشان داده می‌شود.

هیچگونه ابهامی در مورد این که x در اینجا چیست وجود ندارد ـ x یک دنباله مشخص در P است، یک عضو R یا R^* نیست، و "نماینده" هیچ عضو R یا R^* نمی‌باشد.

این نماد باعث می‌شود که محاسبات آشناتر بنظر رسند. برای مثال،

$$(a, {}^\circ_R, {}^\circ_R, {}^\circ_R, \dots) \oplus (b, {}^\circ_R, {}^\circ_R, {}^\circ_R, \dots) \odot ({}^\circ_R, {}^1_R, {}^\circ_R, {}^\circ_R, \dots),$$

$\boldsymbol{a} + \boldsymbol{bx}$ می‌شود. به طور مشابه، انتظار داریم که $\boldsymbol{cx}^3$ (ثابت $\boldsymbol{c}$ ضربدر x^3) دنباله $({}^\circ_R, {}^\circ_R, {}^\circ_R, c, {}^\circ_R, {}^\circ_R, \dots)$ شود که در آن c در مکان ۳-ام است [۳۴]. البته نمی‌توانیم به‌سادگی فرض کنیم که همه چیز مثل آنچه در نماد قدیم انجام می‌گرفت، کارکند. با این حال، آنچه احتیاج داریم در دو نتیجه زیر اثبات شده است:

۳۴) بخاطر آورید که در چندجمله‌ای $(r, s, t, \dots)$، عضو r در مکان ۰-ام، s در مکان ۱-ام، t در مکان ۲-ام و غیره است.

لم چ.۳. گیریم P حلقه چندجمله‌ایهای با ضرایب در حلقه R و x چندجمله‌ای $(\circ_R, 1_R, \circ_R, \circ_R, \circ_R, \dots)$ باشد. آنگاه برای هر عضو $\boldsymbol{a}=(a, \circ_R, \circ_R, \circ_R, \dots)$ از R^* و هر عدد صحیح $n \geq 1$

(۱) $x^n = (\circ_R, \circ_R, \dots, \circ_R, 1_R, \circ_R, \dots)$، که در آن 1_R در مکان n-ام می‌باشد.

(۲) $\boldsymbol{a}x^n = (\circ_R, \circ_R, \dots, \circ_R, a, \circ_R, \dots)$، که در آن a در مکان n-ام می‌باشد.

برهان. چندجمله‌ای x می‌تواند به این صورت بیان شود:

$$x = (e_0, e_1, e_2, \dots)$$ که در آن $e_1 = 1_R$ و برای هر $i \neq 1$، $e_i = \circ_R$.

گزاره (۱) را با استقراء روی n ثابت می‌کنیم[۳۵]. طبق تعریف $x^1 = x$ و لذا این گزاره برای $n = 1$ درست است. فرض کنید که مطلب برای $n = k$ درست باشد، یعنی، فرض کنید که

$$x^k = (d_0, d_1, d_2, \dots)$$ که در آن $d_k = 1_R$ و برای هر $i \neq k$، $d_i = \circ_R$.

آنگاه

$$x^{k+1} = x^k x = (d_0, d_1, d_2, \dots)(e_0, e_1, e_2, \dots) = (r_0, r_1, r_2, \dots)$$

که در آن برای هر $j \geq 0$،

$$r_j = \sum_{i=0}^{j} d_i e_{j-i}.$$

چون برای $i \neq 1$، $e_i = \circ_R$ و برای $i \neq k$، $d_i = \circ_R$، داریم

$$r_{k+1} = \underbrace{d_0 e_{k+1} + \cdots + d_{k-1} e_2}_{\circ} + d_k e_1 + \underbrace{d_{k+1} e_0}_{\circ} = d_k e_1 = 1_R \cdot 1_R = 1_R$$

و برای $j \neq k+1$

$$r_j = \underbrace{d_0 e_j + d_1 e_{j-1} + \cdots + d_{j-2} e_2}_{\circ} + d_{j-1} e_1 + \underbrace{d_j e_0}_{\circ}$$

$$= d_{j-1} e_1 = d_{j-1} 1_R = d_{j-1}.$$

ولی $j - 1 \neq k$ چون $j \neq k+1$. بنابراین برای تمام $j \neq k+1$، $r_j = d_{j-1} = \circ_R$. بدین دلیل

$$x^{k+1} = (r_0, r_1, r_2, \dots) = (\circ_R, \circ_R, \dots, \circ_R, 1_R, \circ_R, \dots)$$

۳۵) پیوست پ را ملاحظه کنید.

که در آن 1_R در جای $(k+1)$-ام می‌باشد. در نتیجه (۱) برای $n = k+1$ درست است و بنابراین طبق استقراء برای هر n درست است.

یک استدلال مشابه استقرایی (۲) را ثابت می‌کند؛ تمرین ۷ را ملاحظه کنید. ■

قضیه چ.۴. گیریم P حلقه چندجمله‌ایهای با ضرایب در حلقه R باشد. آنگاه P شامل یک نسخه R^* از R و یک عضو x است به طوری که

(۱) برای هر $\boldsymbol{a} \in R^*$، $\boldsymbol{ax} = \boldsymbol{xa}$.

(۲) هر عضو P را می‌توان به صورت $\boldsymbol{a}_0 + \boldsymbol{a}_1 x + \boldsymbol{a}_2 x^2 + \cdots + \boldsymbol{a}_n x^n$ نوشت.

(۳) اگر $\boldsymbol{a}_0 + \boldsymbol{a}_1 x + \cdots + \boldsymbol{a}_n x^n = \boldsymbol{b}_0 + \boldsymbol{b}_1 x + \cdots + \boldsymbol{b}_m x^m$ که در آن $n \le m$، آنگاه برای $i \le n$، $\boldsymbol{a}_i = \boldsymbol{b}_i$ و برای $i > n$، $\mathbf{b}_i = 0$؛ به ویژه

(۴) $\boldsymbol{a}_0 + \boldsymbol{a}_1 x + \boldsymbol{a}_2 x^2 + \cdots + \boldsymbol{a}_n x^n = 0_R$ اگر و تنها اگر برای هر $i \ge 0$، $\boldsymbol{a}_i = 0_R$.

برهان. گیریم x مثل آنچه در لم چ.۳ آمده است باشد. برهان (۱) به خواننده واگذار می‌شود (تمرین ۵).

(۲) اگر $(a_0, a_1, a_2, \ldots) \in P$، آنگاه نمایه n وجود دارد به طوری که برای هر $i > n$، $a_i = 0$. طبق لم چ.۳

$$
\begin{aligned}
&(a_0, a_1, a_2, \ldots, a_n, 0_R, 0_R, \ldots)\\
&= (a_0, 0_R, 0_R, \ldots) + (0_R, a_1, 0_R, \ldots) + (0_R, 0_R, a_2, 0_R, \ldots) + \ldots\\
&+ (0_R, \ldots, 0_R, a_n, 0_R, \ldots)\\
&= \boldsymbol{a}_0 + \boldsymbol{a}_1 x + \boldsymbol{a}_2 x^2 + \cdots + \boldsymbol{a}_n x^n.
\end{aligned}
$$

(۳) با معکوس کردن استدلال ارائه شده در (۲) ثابت می‌شود که $\boldsymbol{a}_0 + \boldsymbol{a}_1 x + \cdots + \boldsymbol{a}_n x^n$ دنبالهٔ $(a_1, a_2, \ldots, a_n, 0_R, 0_R, \ldots)$ است و این که

$$\boldsymbol{b}_0 + \boldsymbol{b}_1 x + \cdots + \boldsymbol{b}_m x^m = (b_0, b_1, b_2, \ldots, b_m, 0_R, 0_R, \ldots).$$

اگر این دو دنباله برابر باشند، آنگاه برای هر $i \le n$، $a_i = b_i$ و برای $n < i \le m$، باید $b_i = 0_R$.

(۴) حالت خاصی از (۳) است: کافی است قرار دهید $b_i = 0_R$. ■

وقتی چندجمله‌ایها به شکل $\boldsymbol{a}_0 + \boldsymbol{a}_1 x + \cdots + \boldsymbol{a}_n x^n$ نوشته می‌شوند، جمع و ضرب آنها شبیه جمع و ضربی است که در دبیرستان انجام می‌دادیم، با این تفاوت که در اینجا ما برخی از نمادها را با حروف پررنگ نشان می‌دهیم.

مثال ۱. در حلقه چندجمله‌ایهای با ضرایب حقیقی، قوانین توزیع‌پذیری و قضایای چ.۲ و چ.۴ نشان می‌دهد که

$$\begin{aligned}(3x+1)(2x+5) &= (3x+1)2x + (3x+1)5 \\ &= 3x \times 2x + 1 \times 2x + 3x \times 5 + 1 \times 5 \\ &= 3 \times 2 \times x \times x + 2x + 3 \times 5 \times x + 5 \\ &= 6x^2 + 17x + 5\end{aligned}$$

توجه کنید که تمایز بین تایپ پررنگ و تایپ عادی عناصر مهم است زیرا حرف پررنگ $\boldsymbol{a}$ معرف یک دنباله است در صورتی که حرف a یک عضو R را نشان می‌دهد. با این حال از نظر ساختار جبری نیازی به این تمایز نیست زیرا R^* (متشکل از تمام $\boldsymbol{a}$های پررنگ) یکریخت با R (متشکل از تمام aها) است. در نتیجه هیچ مشکلی در یکی‌گیری R با نسخه یکریختش R^* و نوشتن عضوهای $R \cong R^*$ با حروف تایپ معمولی پیش نمی‌آید [۳۶]. در این حالت، چندجمله‌ای‌ها چه از نظر شکل و چه از نظر رفتار مشابه قبل بنظر می‌رسند. به این دلیل، از این به بعد به جای P، نماد استاندارد $R[x]$ را برای حلقه چندجمله‌ای‌ها بکار می‌بریم.

اینک پس از یک چرخش کامل در بکارگیری نمادها، به نماد اوّل برگشته‌ایم، البته با این تفاوت که در حال حاضر توجیه دقیقی از عملیاتی که قبلاً با چندجمله‌ای‌ها انجام می‌دادیم بدست آورده‌ایم، به‌علاوه، مفاهیم را به حلقه‌های دلخواه تعمیم داده‌ایم و به دیدگاه جدیدی دست یافته‌ایم. با شروع از یک حلقه یکدار R **حلقه توسیع** $R[x]$ (یعنی حلقه‌ای که R یک زیرحلقه آن است) را ساختیم.

۳۶) در واقع این یکی‌گیری را برای سالها انجام می‌داده‌اید، مثلاً آن هنگام که چندجمله‌ای ۴ را به عنوان عدد حقیقی ۴ در نظر می‌گرفتید. از مسئله یکی‌گیری می‌توان به طورکلی دوری جست، به این طریق که یک چندجمله‌ای را یا یک عضو R تعریف کنیم و یا یک دنباله به صورت $(a_0, a_1, \ldots)$ که در آن حداقل یکی از a_iها مخالف صفر است و از مرحله‌ای به بعد همه a_iها صفر هستند. در این صورت چندجمله‌ای‌ها، R را به‌عنوان یک زیرمجموعه شامل هستند. البته با این تعریف، هنگام جمع و ضرب چندجمله‌ای‌ها و برهان قضایا باید حالت گوناگونی را در نظر گرفت. سپس روال عادی را طی کرده (البته با مشقت) تا این که قضیه چ.۴ را دوباره ثابت کنید.

این حلقه توسیع شامل یک عضو x است که با هر عضو R جابجا می‌شود. عضو x در R نیست و نماینده هیچ عضو R هم نمی‌باشد، هر عضو این حلقه توسیع را می‌توان به صورت یکتایی (اساساً یکتا) برحسب عناصر R و توان‌های x نوشت. چون x دارای این خاصیت است که

$$a_0 + a_1x + \cdots + a_nx^n = 0_R \quad \text{اگر و تنها اگر برای هر } i،\ a_i = 0_R.$$ برای هر i.

x را یک عضو **متعالی** یا **مجهول** روی R می‌نامند.

سرانجام، در مورد چندجمله‌ای‌های با ضرایب در یک حلقه R که دارای عضو همانی نیست چه می‌توان گفت؟ در این حالت کافی است حلقه یکدار S را چنان بیابیم که R را به‌عنوان یک زیرحلقه شامل باشد. برای مثال حلقه اعداد صحیح زوج دارای عضو همانی نیست و در حلقه همه اعداد صحیح $\mathbb{Z}$ قرار دارد که دارای عضو همانی است، برای حالت کلی، تمرین ۳۲ بخش ۳.۳ را ملاحظه کنید. سپس حلقه $S[x]$ را به صورت بالا تشکیل دهید. چندجمله‌ایهایی در $S[x]$ که ضرایبشان در R است یک زیرحلقه $S[x]$ را تشکیل می‌دهند؛ این همان حلقه مورد نظر $R[x]$ است. توجه کنید که وقتی R عنصر همانی نداشته باشد، خود چندجمله‌ای x در $R[x]$ نیست.

تمرینها

۱.A. هر چندجمله‌ای را به صورت یک دنباله و هر دنباله را به صورت یک چندجمله‌ای بیان کنید.

(الف) $(0, 1, 0, 1, 0, 1, 0, 0, 0, \ldots)$

(ب) $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 0, 0, \ldots)$

(پ) $3x^6 - 5x^4 + 12x^3 - 3x^2 + 7/5x - 11$

(ت) $(x - 1)(x^3 - x^2 + 1)$

۲. (الف) اگر $(a_1, a_2, \ldots)$ و $(b_1, b_2, \ldots)$ دو چندجمله‌ای باشند، نشان دهید که مجموع آنها یک چندجمله‌ای است (یعنی، از مرحله‌ای به بعد تمام مولفه‌های مجموع صفر می‌باشد).

(ب) نشان دهید که $(a_1, a_2, \ldots) \odot (b_1, b_2, \ldots)$ یک چندجمله‌ای است [راهنمایی: اگر برای $i > k$، $a_i = 0$ و برای $i > t$، $b_i = 0$، مولفه i ام حاصلضرب را برای $i > k + t$ امتحان کنید.]

۳. قسمت‌های زیر از قضیه چ.۱ را ثابت کنید:

(الف) جمع در P شرکت‌پذیر است؛

(ب) هر دو قانون توزیع‌پذیری در P برقرار است؛

(پ) اگر R جابجایی باشد P جابجایی است.

۴. برهان قضیه چ.۲ را با اثبات گزاره‌های زیر کامل کنید:

(الف) f یک به یک است. (ب) f پوشا است.

۵. قسمت (۱) قضیه چ.۴ را ثابت کنید.

B.۶. (الف) در برهان قضیه چ.۱ (شرکت‌پذیری ضرب در P) نشان دهید که

$$\sum_{i=0}^{n}\sum_{j=0}^{i} a_j b_{i-j} c_{n-i} = \sum a_u b_v c_w$$

که در آن مجموع آخر روی تمام اعداد صحیح نامنفی u، v، w با شرط $u+v+w=n$ محاسبه می‌شود. [راهنمایی: این دو مجموع را جمله به جمله مقایسه کنید، مجموع زیرنمایه‌ها در جمله $a_j b_{i-j} c_{n-i}$ برابر n است، برای این که نشان دهید $a_u b_v c_w$ در مجموع دیگر قرار دارد، قرار دهید $j=u$ و $i=u+v$ و تحقیق کنید که $n-i=w$.]

(ب) نشان دهید که

$$\sum_{r=0}^{n}\sum_{s=0}^{n-r} a_r b_s c_{n-r-s} = \sum a_u b_v c_w$$

(آخرین مجموع مانند قسمت (الف) می‌باشد).

۷. قسمت (۲) لم چ.۳ را ثابت کنید [راهنمایی: $\boldsymbol{a}=(a_0,a_1,a_2,\dots)$، که در آن برای $i>1$، $a_i = 0_R$ و طبق (۱) داریم $x^n=(d_0,d_1,d_2,\dots)$، که در آن $d_n = 1_R$ و برای $i\neq n$، $d_i = 0$؛ از استقراء روی n استفاده کنید.]

۸. گیریم R یک دامنه صحیح باشد. با استفاده از نماد دنباله‌ای، ثابت کنید که حلقه چندجمله‌ای‌های $R[x]$ نیز یک دامنه صحیح است.

۹. گیریم R یک میدان باشد. با استفاده از نماد دنباله‌ای ثابت کنید که حلقه چندجمله‌ای‌های $R[x]$ یک میدان نمی‌باشد. [راهنمایی: آیا $(0_R, 1_R, 0_R, 0_R, \dots)$ یکه است؟]

C.۱۰. (الف) گیریم $\mathbb{Q}[\pi]$ مجموعه تمام اعداد حقیقی به صورت $r_0 + r_1\pi + r_2\pi^2 + \cdots + r_n\pi^n$ باشد، که در آن $n \geq 0$ و هر $r_i \in \mathbb{Q}$، نشان دهید که $\mathbb{Q}[\pi]$ یک زیرحلقهٔ $\mathbb{R}$ است.

(ب) فرض کنید بدانیم که $r_0 + r_1\pi + \cdots + r_n\pi^n = 0$ اگر و تنها اگر $r_i = 0$. (این واقعیت برای اولین بار در سال ۱۸۸۲ ثابت شد؛ برهان آن خارج از حوزه این کتاب است.) ثابت کنید که $\mathbb{Q}[\pi]$ یکریخت با حلقه چندجمله‌ای‌های $\mathbb{Q}[x]$ است.

* * * * *

پاسخ و پیشنهادهایی برای حل تمرین‌های منتخب فرد

در این بخش، جهت کمک به دانشجویان راهنمایی‌هایی ارائه می‌شود. در تمرین‌هایی که اثبات مطلبی از شما خواسته شده‌است، ممکن است چهارچوب اثبات ارائه شده باشد (که شما جزئیات آن را کامل می‌کنید). در مواردی، تنها یک قسمت کلیدی اثبات ارائه شده که بقیه آن را کامل می‌کنید، در مورد تعدادی از تمرین‌ها نیز، تنها یک راهنمایی ارائه شده که شما را قادر به یافتن راه حل می‌نماید.

بخش ۱.۱، صفحه ??

۱. (الف) خارج قسمت ۱۵؛ باقیمانده ۱۷ (پ) خارج قسمت ۰؛ باقیمانده ۰
(ث) خارج قسمت ۱۱۷؛ باقیمانده ۱۲.

۵. (الف) خارج قسمت ۶؛ باقیمانده ۱۹ (پ) خارج قسمت ۶۲۷۲۰ ؛ باقیمانده ۹۲
(ث) خارج قسمت ۱۴۹۴۰- ؛ باقیمانده ۳۳۵.

۷. اگر $a = 3q + 1$، در این صورت $a^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$ که به‌صورت $3k + 1$ با $k = 3q^2 + 2q$ می‌باشد. استدلال مشابهی را وقتی که $a = 3q$ یا $a = 3q + 2$ بکار برید.

۹. بر طبق الگوریتم تقسیم، هر عدد صحیح a به‌صورت $3q$، $3q + 1$ یا $3q + 2$ می‌باشد. در هر یک از این حالات، a^3 را محاسبه کنید و مانند تمرین ۷ پیش روید.

بخش ۲.۱، صفحه ۱۴

۱. (الف) ۸ (پ) ۱ (ث) ۹ (چ) ۵۹۲

۳. $a|b$ یعنی برای برخی عدد صحیح u، $b = au$. به‌طور مشابه، $b|c$ یعنی برای برخی عدد صحیح v، $c = bv$. با ترکیب این دو نشان دهید که c مضرب صحیحی از a است و لذا $a|c$.

۵. $a|b$ یعنی برای برخی عدد صحیح u، $b = au$ و $b|a$ یعنی برای برخی عدد صحیح v، $a = bv$. این دو معادله را ترکیب کنید تا نشان دهید $a = auv$، که نتیجه می‌دهد $uv = 1$. با توجه به عدد صحیح بودن u و v، تنها احتمالات ممکن چیست؟

۱۱. (الف) ۱ یا ۲.

۱۳. اگر $d|k$ و $d|a$، در این صورت $k = du$ و $a = dv$، لذا $du = k = abc + 1 = dvbc + 1$. اولین و آخرین قسمت این برابری‌ها را بکار برید تا نشان دهید که $d|1$.

۱۵. جوابهای ممکن بسیاری وجود دارد، از جمله: (الف) $8 = 56 \times 4 + 72(-3)$

(پ) $1 = 143 \times 1943 + 227(-1224)$ (ث) $5092 = 4144 \times 2 + 7696(-1)$.

۱۷. برای برخی $u \in \mathbb{Z}$، $c = au$ (چرا؟) چون $b|c$، داریم $b = au$. قضیه ۵.۱ را بکار برید.

۱۹. فرض کنید $d|a$ و $d|b$، لذا $a = du$ و $b = dv$. چون $a|(b+c)$، $b + c = aw$. بنابراین $c = aw - b = adu - dv = d(au - v)$، لذا $d|c$. با توجه به این که $(b,c) = 1$، درباره d و (a,b) چه نتیجه‌گیری می‌توانید بکنید؟

۲۳. هر شمارنده مشترک a و (b,c) یک شمارنده مشترک (a,b) و c نیز هست. [اثبات: اگر $d|(b,c)$، در این صورت طبق تعریف (b,c)، $d|b$ و $d|c$. اگر به‌علاوه $d|a$، در این صورت

d یک شمارنده مشترک a و b است و بنابراین طبق نتیجه ۴.۱، $d|(a,b)$.] استدلالی مشابه نشان می‌دهد که هر شمارنده مشترک (a,b) و c یک شمارنده مشترک a و (b,c) نیز هست.

۲۹. برای برخی u و v، $d = cu + av$ (چرا؟). بنابراین $db = cbu + abv$. با بکار بردن این حقیقت که برای برخی w، $ab = cw$ (چرا؟)، نشان دهید $c|db$.

۳۳. ابتدا نشان دهید که هر عدد صحیح n را می‌توان به صورت مضربی از ۹ به اضافه مجموع ارقام آن نوشت. [مثلاً:

$$\begin{aligned}
۷۸۴۲ &= ۷ \times ۱۰۰۰ + ۸ \times ۱۰۰ + ۴ \times ۱۰ + ۲ \\
&= ۷(۹۹۹ + ۱) + ۸(۹۹ + ۱) + ۴(۹ + ۱) + ۲ \\
&= (۷ \times ۹۹۹ + ۸ \times ۹۹ + ۴ \times ۹) + (۷ + ۸ + ۴ + ۲) \\
&= ۹(۶ \times ۱۱۱ + ۸ \times ۱۱ + ۴) + (۷ + ۸ + ۴ + ۲)].
\end{aligned}$$

فرض کنید r باقیمنده تقسیم مجموع ارقام n بر ۹ باشد. نشان دهید که برای برخی k، $n = ۹k + r$. بنابراین n بر ۹ قابل قسمت است اگر و تنها اگر $r = ۰$، یعنی اگر و تنها اگر ۹ مجموع ارقام n را بشمارد.

بخش ۳.۱، صفحه ۲۱

۱. (الف) $۷ \times ۵ \times ۳^۲ \times ۲^۴ = ۵۰۴۰$ (پ) $۴۵۶۷۰ = ۲ \times ۵ \times ۴۵۶۷$

۳. ($\Rightarrow$) فرض کنید p دارای خاصیت مفروض باشد. فرض کنید d یک شمارنده p باشد، مثلاً $p = dt$. بنابه این خاصیت، $d = \pm ۱$ یا $t = \pm ۱$ (و بنابراین $d = \pm p$). پس تنها شمارنده‌های p، ± ۱ و $\pm p$ هستند، و p اول است.

۷. (الف) ۳، $۳^۲$، $۳^۳$، ...، ۳^s؛ ۵×۳، ۵×۳^۲، ۵×۳^۳، ...، ۵×۳^s؛ $۵^۲ \times ۳$، $۵^۲ \times ۳^۲$، $۵^۲ \times ۳^۳$، ...، $۵^۲ \times ۳^s$؛ $۵^۳ \times ۳$، ...، $۵^t \times ۳$؛ $۵^t \times ۳^۲$، $۵^t \times ۳^۳$، ...، $۵^t \times ۳^s$.

۹. بر طبق قضیه ۸.۱، هر شمارنده اول $a^۲$، یک شمارنده a نیز هست و همین برای $b^۲$ نیز برقرار است.

۱۳. اگر $p_1p_2\dots p_k$، تجزیه c به اعداد اول باشد، در این صورت $ab = c^2 = p_1p_1p_2p_2\dots p_kp_k$. حال بنا به قضیه ۸.۱، p_1 باید a یا b، مثلاً a، را بشمارد. چون $(a,b) = 1$، p_1 نمی‌تواند b را بشمارد. بنابراین $(p_1)^2|a$. با تغییر نمایه‌ها، در صورت لزوم، نشان دهید که $a = p_1p_1p_2p_2\dots p_jp_j = (p_1p_2\dots p_j)^2$ و

$$b = p_{j+1}p_{j+1}\dots p_kp_k = (p_{j+1}p_{j+2}\dots p_k)^2.$$

۱۵. طبق نتیجه ۹.۱، هر شمارنده اوّل a^3 باید a را نیز بشمارد. همین برای b نیز برقرار است.

۱۷. اگر $p = 6k+1$، در این صورت

$$p^2 + 2 = (6k+1)^2 + 2 = 36k^2 + 12k + 3 = 3(12k^2 + 4k + 1).$$

حالت‌های دیگر به‌طور مشابه انجام می‌شود.

بخش ۴.۱، صفحه ۲۷

۱. همه آنها

۵. هر عدد صحیح سه رقمی، کمتر از ۱۰۰۰ است و $\sqrt{1000} \approx 31{,}62$. قضیه ۱۳.۱ را بکار برید.

۷. بررسی کنید که

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \dots + x^2 + x + 1).$$

نتیجه‌گیری کنید که $y^m - 1$ یک شمارنده $(y^m)^n - 1 = y^{mn} - 1$ است. با بکار بردن این حقیقت برای $y = 2$ و $p = mn$، نشان دهید که هرگاه p مرکب باشد، $2^p - 1$ نیز مرکب است.

۱۳. تمرین ۶ پیوست چ نشان می‌دهد که $\binom{p}{k}$ یک عدد صحیح است. $p = \binom{p}{1}$، و برای $k > 1$، مخرج $\binom{p}{k}$ حاصل‌ضربی از اعداد صحیحی است که هر کدام اکیداً از p کوچکتر است.

بخش ۱.۲، صفحه ۳۵

۱. (⇒) طبق الگوریتم تقسیم، $a = qn + r$ و $b = pn + s$ با باقیمانده‌های r و s ای که در نابرابریهای $0 \leq r < n$ و $0 \leq s < n$ صدق می‌کنند. اگر (پیمانه n) $a \equiv b$، در این صورت $a - b = kn$ (چرا؟)، و بنابراین $kn = (qn + r) - (pn + s)$، که نتیجه می‌دهد $r - s = (k - q + p)n$، یعنی $n|(r - s)$. امّا این محال است مگر این که $r - s = 0$، زیرا r و s اکیداً از n کوچکترند. برای اثبات طرف عکس، فرض کنید $r = s$ و نشان دهید که $n|(a - b)$.

۵. طبق نتیجه ۵.۲، در پیمانه ۴ داریم $a \equiv 0$ یا $a \equiv 1$ یا $a \equiv 2$ یا $a \equiv 3$. بنابراین طبق قضیه ۲.۲، در پیمانه ۴، a^2 همنهشت با 0^2 یا 1^2 یا 2^2 یا 3^2 است.

۹. (الف) $(n - a)^2 = n^2 - 2na + a^2$. بنابراین $(n - a)^2 - a^2$ بر n بخش‌پذیر است.

۱۱. (الف) هر عدد صحیح که همنهشت با ۴ به پیمانه ۵ باشد.

(پ) هر عدد صحیح که به پیمانه ۱۵ همنهشت با ۴ یا ۹ یا ۱۴ باشد.

۱۳. (الف) اگر (پیمانه $2n$) $a \equiv b$، در این صورت برای برخی k، $b = a + 2nk$ (چرا؟). بنابراین $b^2 = (a + 2nk)^2 = a^2 + 4nka + 4n^2k^2$، لذا $b^2 - a^2 = 4n(ka + nk^2)$.

۱۵. فرض کنید c و d اعداد صحیح دلخواهی باشند. طبق نتیجه ۵.۲، هر یک از اینها همنشهت (به پیمانه ۴) با دقیقاً یکی از اعداد ۰، ۱، ۲، ۳ است. اگر $c \equiv 2$ و $d \equiv 3$، در این صورت طبق قضیه ۲.۲، (پیمانه ۴) $c^2 + d^2 \equiv 2^2 + 3^2 \equiv 1$. چون (پیمانه ۴) $a \equiv 3$، در این حالت برابری $a = c^2 + d^2$ نمی‌تواند برقرار باشد. حالات دیگر به‌طور مشابه انجام می‌شود.

۲۱. برای برخی k، $a - b = nk$ (چرا؟). نشان دهید که هر شمارنده مشترک a و n یک شمارنده b نیز هست، و این که هر شمارنده مشترک b و n یک شمارنده a نیز هست. این مطلب درباره (a, n) و (b, n) چه می‌گوید؟

۲۳. (الف) تجزیه $x^n - 1$ در جواب ارائه شده به تمرین ۷ بخش ۴.۱ را وقتی $x = 10$ بکار برید.

۲۵. توجه کنید که (پیمانه ۱۱) $-1 \equiv 10$ و قضیه ۲.۲ را بکار برید.

بخش ۲.۲، صفحه ۴۴

۱. (الف)

+	۰	۱
۰	۰	۱
۱	۱	۰

۰	۰	۱
۰	۰	۰
۱	۰	۱

(پ)

+	۰	۱	۲	۳	۴	۵	۶
۰	۰	۱	۲	۳	۴	۵	۶
۱	۱	۲	۳	۴	۵	۶	۰
۲	۲	۳	۴	۵	۶	۰	۱
۳	۳	۴	۵	۶	۰	۱	۲
۴	۴	۵	۶	۰	۱	۲	۳
۵	۵	۶	۰	۱	۲	۳	۴
۶	۶	۰	۱	۲	۳	۴	۵

·	۰	۱	۲	۳	۴	۵	۶
۰	۰	۰	۰	۰	۰	۰	۰
۱	۰	۱	۲	۳	۴	۵	۶
۲	۰	۲	۴	۶	۱	۳	۵
۳	۰	۳	۶	۲	۵	۱	۴
۴	۰	۴	۱	۵	۲	۶	۳
۵	۰	۵	۳	۱	۶	۴	۲
۶	۰	۶	۵	۴	۳	۲	۱

۳. (الف) $a = ۳$ یا $a = ۵$.

۵. (الف) $x = ۰, ۱, ۲, ۳, ۴, ۵$

(پ) $x = ۰, ۱, ۲, ۳, ۴$

۹. (الف) $a^5 + b^5$ (پ) $a^2 + b^2$.

بخش ۳.۲، صفحه ۴۷

۱. (الف) $a = ۱, ۲, ۳, ۴, ۵, ۶$ (پ) $a = ۱, ۲, ۴, ۵, ۷, ۸$

۳. $ab = ۰$ در $\mathbb{Z}_p$ یعنی $p|ab$ در $\mathbb{Z}$. قضیه ۸.۱ را بکار برید و نتیجه را به $\mathbb{Z}_p$ انتقال دهید.

۵. $a \neq ۰$ در $\mathbb{Z}_p$ بدین معنی است که (پیمانه p) $a \not\equiv ۰$، یعنی $p \nmid a$، لذا $(p, a) = ۱$ (چرا؟). طبق نتیجه ۹.۲، (پیمانه p) $ax \equiv ۱$ دارای یک جواب است. با بکار بردن این، جوابی برای (پیمانه p) $ax \equiv b$ بیابید.

بخش ۱.۳، صفحه ۶۰

۱. (الف) بسته بودن برای جمع.

۷. (الف) زیرحلقه بدون همانی ضربی (حاصل‌ضرب هر دو ماتریس، ماتریس صفر است).
(پ) زیرحلقه بدون همانی ضربی. (ث) زیرحلقه جابجایی یکدار.

۱۱.

+	۰	S	A	B	C	D	E	F
۰	۰	S	A	B	C	D	E	F
S	S	۰	F	E	D	C	B	A
A	A	F	۰	D	E	B	C	S
B	B	E	D	۰	F	A	S	C
C	C	D	E	F	۰	S	A	B
D	D	C	B	A	S	۰	F	E
E	E	B	C	S	A	F	۰	D
F	F	A	S	C	B	E	D	۰

$\cdot$	$\circ$	S	A	B	C	D	E	F
$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$
$\circ$	$\circ$	S	A	B	C	D	E	F
A	$\circ$	A	A	$\circ$	$\circ$	A	A	$\circ$
B	$\circ$	B	$\circ$	B	$\circ$	B	$\circ$	B
C	$\circ$	C	$\circ$	$\circ$	C	$\circ$	C	C
D	$\circ$	D	A	B	$\circ$	D	A	B
E	$\circ$	E	A	$\circ$	C	A	E	C
F	$\circ$	F	$\circ$	B	C	B	C	F

۱۵. (الف)

$+$	$(\circ,\circ)$	$(1,1)$	$(\circ,2)$	$(1,\circ)$	$(\circ,1)$	$(1,2)$
$(\circ,\circ)$	$(\circ,\circ)$	$(1,1)$	$(\circ,2)$	$(1,\circ)$	$(\circ,1)$	$(1,2)$
$(1,1)$	$(1,1)$	$(\circ,2)$	$(1,\circ)$	$(\circ,1)$	$(1,2)$	$(\circ,\circ)$
$(\circ,2)$	$(\circ,2)$	$(1,\circ)$	$(\circ,1)$	$(1,2)$	$(\circ,\circ)$	$(1,1)$
$(1,\circ)$	$(1,\circ)$	$(\circ,1)$	$(1,2)$	$(\circ,\circ)$	$(1,1)$	$(\circ,2)$
$(\circ,1)$	$(\circ,1)$	$(1,2)$	$(\circ,\circ)$	$(1,1)$	$(\circ,2)$	$(1,\circ)$
$(1,2)$	$(1,2)$	$(\circ,\circ)$	$(1,1)$	$(\circ,2)$	$(1,\circ)$	$(\circ,1)$

$\circ$	$(\circ,\circ)$	$(1,1)$	$(\circ,2)$	$(1,\circ)$	$(\circ,1)$	$(1,2)$
$(\circ,\circ)$	$(\circ,\circ)$	$(\circ,\circ)$	$(\circ,\circ)$	$(\circ,\circ)$	$(\circ,\circ)$	$(\circ,\circ)$
$(1,1)$	$(\circ,\circ)$	$(1,1)$	$(\circ,2)$	$(1,\circ)$	$(\circ,1)$	$(1,2)$
$(\circ,2)$	$(\circ,\circ)$	$(\circ,2)$	$(\circ,1)$	$(\circ,\circ)$	$(\circ,2)$	$(\circ,1)$
$(1,\circ)$	$(\circ,\circ)$	$(1,\circ)$	$(\circ,\circ)$	$(1,\circ)$	$(\circ,\circ)$	$(1,\circ)$
$(\circ,1)$	$(\circ,\circ)$	$(\circ,1)$	$(\circ,2)$	$(\circ,\circ)$	$(\circ,1)$	$(\circ,2)$
$(1,2)$	$(\circ,\circ)$	$(1,2)$	$(\circ,1)$	$(1,\circ)$	$(\circ,2)$	$(1,1)$

۱۷. برای اثبات بسته بودن E تحت $*$، باید بررسی کنید که وقتی a و b اعداد صحیح زوج هستند، $a*b=ab/2$ نیز زوج است. برای اثبات شرکت‌پذیری $*$، برابری $(a*b)*c=a*(b*c)$

را به صورت آنچه در پی می‌آید بررسی کنید. طبق تعریف، $(a*b)*c = (ab/۲)*c = (ab/۲)c/۲$. اینک $a*(b*c)$ را برحسب ضرب در $\mathbb{Z}$ بیان کنید و بررسی کنید که دو عبارت برابرند. جابجایی $*$ به‌صورت مشابه اثبات می‌شود. برای اثبات قانون توزیع‌پذیری، باید بررسی کنید که $a*(b+c) = a*b + a*c$، یعنی این که $a(b+c)/۲ = ab/۲ + ab/۲$. در صورت وجود یک همانی ضربی e، باید برای هر $a \in E$، $e*a = a$، که معادل برابری $ea/۲ = a$ در $\mathbb{Z}$ است. امّا $ea/۲ = a$ نتیجه می‌دهد که $e = ۲$.

۲۱. همانیِ ضربی، ۶ است.

۳۱. (ب) چون H مشمول در حلقه $M(\mathbb{C})$ است، جمع آن جابجایی و شرکت‌پذیر است، ضرب آن شرکت‌پذیر است، و قانون توزیع‌پذیری برقرار است. بنابراین تنها لازم است بررسی شود که H تحت عمل جمع و ضرب بسته است، این که ماتریس صفر و ماتریس همانی در H قرار دارد، و این که قرینه هر ماتریس در H در H است.

۳۳. جدول جواب تمرین ۱۵ (الف) بالا را برای $R = \mathbb{Z}_۲$ و $S = \mathbb{Z}_۳$ امتحان کنید.

بخش ۲.۳، صفحه ۷۴

۱. (الف) $a^۲ - ab + ba - b^۲$.

۳. اگر e یک عنصر غیرصفر خودتوان باشد، قضیه ۷.۳ را برای معادله $e^۲ = e \cdot ۱_R$ بکار برید.

۹. اگر $ub = ۰_R$ و u یکه با وارون v باشد، دو طرف را در v ضرب کنید. تعریف یک مقسوم‌علیه صفر چیست؟

۱۱. یکه‌ها: $(۱,e)$، $(۱,b)$، $(۵,e)$، $(۵,b)$؛ مقسوم‌علیه‌های صفر: $(۰,c)$، $(۲,۰)$، $(۲,c)$، $(۳,۰)$، $(۳,c)$، $(۴,۰)$، $(۴,c)$.

۱۵. $ab = ac$ معادل $a(b-c) = ۰$ است.

۱۷. ($\Rightarrow$) اگر S تحت عمل تفریق بسته باشد و $a \in S$، در این صورت $a - a \in S$، لذا $۰_R \in S$. بنابراین برای هر $b \in S$، $۰_R - b \in S$. با استفاده از این نشان دهید که S تحت عمل جمع بسته است، یعنی برای $a, b \in S$، $a + b \in S$.

۲۱. (الف) $(a+a)^2 = a+a$ زیرا برای هر x، $x^2 = x$. از طرفی

$$(a+a)^2 = (a+a)(a+a) = a^2+a^2+a^2+a^2 = a+a+a+a.$$

۲۵. (الف) با توجه به تمرین ۹، کافی است نشان دهید که هر عنصر غیر یکه در $\mathbb{Z}_n$ یک مقسوم‌علیه صفر است. اگر a در $\mathbb{Z}_n$ یکه نباشد، در این صورت طبق نتیجه ۹.۲، در $\mathbb{Z}$ داریم $(a,n) = d > 1$. بنابراین n/d یک عدد صحیح است. آیا n/d در $\mathbb{Z}_n$ غیرصفر است؟ حاصل‌ضرب آن با a در $\mathbb{Z}_n$ چیست؟

۲۷. مثال: اگر $R = \mathbb{Z}_{10}$ و $a = 5$، در این صورت

$$S = \{r \in \mathbb{Z}_{10} \mid 5r = 0\} = \{0, 2, 4, 6, 8\}.$$

بویژه، عنصر a لزوماً در S نیست، تنها عناصری در S هستند که a را تحت عمل ضرب صفر می‌کنند. برای نشان دادن این که S تحت عمل جمع و ضرب بسته است، باید بررسی کنید که $ra = 0_R$ و $sa = 0_R$ نتیجه می‌دهد که $(r+s)a = 0_R$ و $(rs)a = 0_R$.

بخش ۳.۳، صفحه ۸۸

۱. جداول $\mathbb{Z}_2 \times \mathbb{Z}_2$ در جواب تمرین ۱۵ (الف) بخش ۱.۳، ارائه شده است.

۳. اگر $f(a) = f(b)$، در این صورت $(a,a) = (b,b)$، و بنابراین بر طبق قوانین برابری برای زوجهای مرتب، $a = b$. پس f یک به یک است. به‌علاوه داریم

$$f(a+b) = (a+b, a+b) = (a,a) + (b,b) = f(a) + f(b).$$

اثبات را با نشان دادن این که $f(ab) = f(a)f(b)$ و این که f پوشا است، کامل کنید.

۷. برای اثبات یک به یک بودن f از این حقیقت استفاده کنید که، اگر $a - b\sqrt{2} = c - d\sqrt{2}$ (با $a, b, c, d \in \mathbb{Q}$)، در این صورت $b = d$، که نتیجه می‌دهد $a = c$. [اثبات: اگر $b \neq d$، در این صورت $\sqrt{2} = (c-a)/(d-b)$، که متناقض با اصم‌بودن عدد حقیقی $\sqrt{2}$ است.]

۹. اگر $f(a) = f(b)$، در این صورت $[a] = [b]$ در $\mathbb{Z}_n$، که نتیجه می‌دهد (پیمانه n) $a \equiv b$ در $\mathbb{Z}$. امّا این در حالت $a \neq b$ نیز می‌تواند رخ دهد، بنابراین f یک به یک نیست و در نتیجه یکریختی نمی‌باشد.

۱۳. از همان استدلال به‌کار رفته در جواب تمرین ۷، با i به جای $\sqrt{۲}$ استفاده کنید.

۱۷. همانی ضربی در $\mathbb{Z}^*$، عنصر ۰ است. اگر یک یکریختی $f : \mathbb{Z} \to \mathbb{Z}^*$ موجود باشد، قضیه ۱۰.۳ نشان می‌دهد که f باید در شرط $f(۱) = ۰$ صدق کند. بنابراین

$$f(۲) = f(۱ + ۱) = f(۱) \oplus f(۱) = ۰ \oplus ۰ = ۰ + ۰ - ۱ = -۱.$$

به طور مشابه،

$$f(۳) = f(۱ + ۲) = f(۱) \oplus f(۲) = ۰ \oplus (-۱) = ۰ + (-۱) - ۱ = -۲.$$

$f(۴)$، $f(۵)$، $f(-۱)$ چیست؟ فرمولی برای f بیابید. با استفاده از این فرمول نشان دهید، f یک به یک، پوشا و یک همریختی است.

۲۳. (الف) چون f و g همریختی هستند،

$$\begin{aligned}(f \circ g)(a + b) = f(g(a + b)) = f(g(a) + g(b)) &= f(g(a)) + f(g(b)) \\ &= (f \circ g)(a) + (f \circ g)(b).\end{aligned}$$

استدلالی مشابه نشان می‌دهد که

$$(f \circ g)(ab) = (f \circ g)(a) \cdot (f \circ g)(b).$$

(ب) باید دو چیز را نشان دهید: (۱) در صورت یک به یک بودن f و g، $f \circ g$ نیز یک به یک است؛ و (۲) اگر f و g پوشا باشند، $f \circ g$ نیز پوشا است. برای اثبات (۱)، فرض کنید $(f \circ g)(a) = (f \circ g)(b)$، یعنی $f(g(a)) = f(g(b))$. سپس از یک بودن f و g استفاده کنید تا نشان دهید که $a = b$.

۲۵. (الف) نشان دهید، برای هر $s \in S$، $f(۱_R)s = s = sf(۱_R)$. [راهنمایی: با توجه به پوشا بودن f، در مورد هر $s \in S$، چه می‌توان گفت؟]

۲۷. (الف) $\mathbb{Z}$ دارای یک عضو همانی است و E دارای چنین عضوی نیست. (پ) تعداد عناصر $\mathbb{Z}_{۱۶} \times \mathbb{Z}_{۴}$ بیشتر از $\mathbb{Z}_{۱۶}$ است و بنابراین هیچ تابع یک به یکی وجود ندارد. (ث) معادله $x + x = x$ در $\mathbb{Z} \times \mathbb{Z}_{۲}$ دارای یک جواب غیرصفر است (این جواب چیست؟) امّا در $\mathbb{Z}$ دارای جواب نیست.

بخش ۱.۴، صفحه ۱۰۱

۱. (الف) $۳x^{۴} + x^{۳} + ۲x^{۲} + ۲$ (پ) $x^{۵} - ۱$.

۵. (الف) $x^{۳}$؛ $x^{۳} + x^{۲}$؛ $x^{۳} + x^{۲} + x$؛ $x^{۳} + x^{۲} + ۱$؛ $x^{۳} + x + ۱$؛ $x^{۳} + x^{۲} + x + ۱$؛ $x^{۳} + x^{۲} + x + ۱$.

۷. (الف) $q(x) = ۳x^{۲} - ۵x + ۸$؛ $r(x) = -۴x - ۶$.

(پ) $q(x) = x^{۳} + ۳x^{۲} + ۲x + ۳$؛ $r(x) = ۴$.

۹. بله (تعریف یک مقسوم‌علیه صفر را بخوانید و به خاطر داشته باشید که R یک زیرمجموعه $R[x]$ است).

۱۵. اگر $b \in R \neq ۰$، در این صورت $b \in R[x]$ و $۱_R = bq(x) + r(x)$. با استفاده از این حقیقت که $\deg b = ۰$، نشان دهید که $r(x) = ۰$ و $q(x) \in R$. بنابراین هر عضو غیرصفر R دارای یک وارون است.

بخش ۲.۴، صفحه ۱۰۸

۱. اگر $c \in \mathbb{F} \neq ۰_{\mathbb{F}}$، در این صورت c دارای یک وارون است؛ بنابراین $f(x) = c(c^{-۱}f(x))$.

۵. (الف) $x - ۱$ (پ) $x^{۲} - ۱$ (ث) $x - i$.

۷. چون $f(x)$ هر چندجمله‌ای درجه اول را می‌شمارد، $f(x)$ باید دارای درجه ۱ یا ۰ باشد. اگر $f(x) = cx + d$ با $c \neq ۰_{\mathbb{F}}$، در این صورت $f(x) = c(x + dc^{-۱})$، و بنابراین $x + dc^{-۱}$ نیز هر چندجمله‌ای غیر ثابت را می‌شمارد. تمرین ۳ را بکار برید تا به یک تناقض برسید. نتیجه‌گیری کنید که $\deg f(x) = ۰$.

۱۵. هر شمارنده $h(x)$ یک شمارنده $f(x)$ نیز هست.

بخش ۳.۴، صفحه ۱۱۴

۱. (الف) $x^۳ + \frac{۲}{۳}x^۲ + \frac{۱}{۳}x + \frac{۵}{۳}$ (پ) $x^۳ - ix + i$.

۳. (الف) $x^۲ + x + ۱$؛ $۲x^۲ + ۲x + ۲$؛ $۳x^۲ + ۳x + ۳$؛ $۴x^۲ + ۴x + ۴$.

۷. (⇐) فرض کنید $f(x)$ تحویل‌ناپذیر باشد و $g(x) = cf(x)$، با $c \in \mathbb{F}$ و $c \neq ۰_{\mathbb{F}}$. اگر $g(x) = r(x)s(x)$، در این صورت $f(x) = (c^{-۱}r(x))s(x)$، و بنابراین بر طبق قضیه ۸.۴، حداقل یکی از $c^{-۱}r(x)$ یا $s(x)$ ثابت و غیرصفر است. اگر $c^{-۱}r(x)$ ثابت باشد، نشان دهید که $r(x)$ نیز ثابت است. بنابراین بر طبق قضیه ۸.۴، $g(x)$ تحویل‌ناپذیر است.

۹. (الف) $x^۲ + x + ۱$ (پ) $x^۲ + ۱$؛ $x^۲ + x + ۲$؛ $x^۲ + ۲x + ۲$؛ $۲x^۲ + ۲$؛ $۲x^۲ + x + ۱$؛ $۲x^۲ + ۲x + ۱$.

۱۱. اگر تحویل‌ناپذیر باشد، باید یک عامل تکین از درجه ۱ داشته باشد (چرا؟)، یعنی یک عامل به صورت $x + a$ با $a \in \mathbb{Z}_۷$. بررسی کنید که هیچ یک از هفت مورد $x + a$، یک عامل نیست.

۱۳. $(x - ۳)(x - ۴)^۳$.

۲۱. (الف) اگر $f(x) \in \mathbb{Z}_p$ یک چندجمله‌ای درجه دوم تکین باشد، در این صورت برای برخی $c, d, e \in \mathbb{Z}$، $f(x)$ باید به صورت $(cx + d)(c^{-۱}x + e)$ تجزیه شود (چرا؟). بنابراین $f(x) = c(x + dc^{-۱})c^{-۱}(x + ec) = (x + a)(x + b)$ با $a = dc^{-۱}$ و $b = ec$. هنگامی که عوامل ممکن را جفت‌جفت می‌شمارید، توجه کنید که، برای مثال، دو تجزیه $(x + ۲)(x + ۳)$ و $(x + ۳)(x + ۲)$ یکسان هستند. همچنین تجزیه‌هایی به صورت $(x + ۲)(x + ۲)$ را در نظر بگیرید.

۲۳. (الف) همانند روش ارائه شده در تمرین ۱۱، با $\mathbb{Z}_۵$ به جای $\mathbb{Z}_۷$، عمل کنید.

بخش ۴.۴، صفحه ۱۲۱

۱. (الف) جواب‌های صحیح زیادی وجود دارد، از جمله $f(x) = x^۲ + x$.

۳. (الف) خیر؛ $f(-۲) \neq ۰$. (پ) بله.

۹. در $\mathbb{Z}_۳[x]$: $x^۲+۱$؛ $x^۲+x+۲$؛ $x^۲+۲x+۲$.

۱۳. (الف) اگر $f(x)=cg(x)$ با $c \neq ۰_{\mathbb{F}}$، در این صورت $g(x)=c^{-۱}f(x)$. بنابراین $g(u)=۰_{\mathbb{F}}$ نتیجه می‌دهد $f(u)=۰_{\mathbb{F}}$ و بالعکس.

۱۵. اگر $x^۲+۱$ تحویل‌پذیر باشد، در این صورت برای برخی $a,b \in \mathbb{Z}_p$، $x^۲+۱=(x+a)(x+b)$ (جواب تمرین ۲۱ (الف) بخش ۳.۴ را ملاحظه کنید). طرف راست را بسط دهید.

۱۹. (الف) اگر $f(x)=(x-a)^k g(x)$ با $g(a) \neq ۰$، در این صورت

$$f'(x)=k(x-a)^{k-۱}g(x)+(x-a)^k g'(x).$$

اگر a یک ریشه چندگانه $f(x)$ باشد، در این صورت $k \geq ۲$ و $k-۱ \geq ۱$. اگر a یک ریشه هر دو $f(x)$ و $f'(x)$ باشد، نشان دهید $k \geq ۲$.

بخش ۵.۴، صفحه ۱۳۳

۱. (الف) $(-۱)(x+۱)(x-۲)(x^۲+۱)$ (پ) $xx(x+۲)(x-۱)(۳x-۱)$
(ث) $(x+۳)(۲x+۱)(x^۲+۱)$.

۳. آزمون ریشه گویا را بکار برید.

۵. (الف) فرض کنید $p=۲$. (پ) فرض کنید $p=۲$ یا $p=۳$.

۷. (الف) فرض کنید $p=۵$ و نتیجه ۱۴.۴ را به کار برید.

۱۱. ۹۱ را فاکتور بگیرید؛ محک آیزنشتاین و نتیجه ۱۴.۴ را به کار برید.

۱۷. یک چندجمله‌ای از درجه k دارای $k+۱$ ضریب است. بجز ضریب a_k از x^k، برای هر ضریب دیگر، n انتخاب وجود دارد. چه تعداد انتخاب برای a_k وجود دارد؟

بخش ۶.۴، صفحه ۱۳۹

۱. (الف) $-۱ - ۲i$؛ $۱ + ۲i$؛ ۳؛ ۲-، (پ) $۳ + ۲i$؛ $۳ - ۲i$؛ $-۱ + i$؛ $-۱ - i$.

۳. (الف) $x^۲ - ۲$ در $\mathbb{Q}[x]$؛ $(x^۲ + \sqrt{۲})(x + \sqrt[۴]{۲})(x - \sqrt[۴]{۲})$ در $\mathbb{R}[x]$؛
$(x - \sqrt[۴]{۲}i)(x + \sqrt[۴]{۲}i)(x + \sqrt[۴]{۲})(x - \sqrt[۴]{۲})$ در $\mathbb{C}[x]$.

(پ) $(x - ۱)(x^۲ - ۵)$ در $\mathbb{Q}[x]$؛ $(x - ۱)(x + \sqrt{۵})(x - \sqrt{۵})$ در $\mathbb{R}[x]$ و $\mathbb{C}[x]$.

۵. طبق لم ۲۴.۴، ریشه‌های غیر حقیقی $f(x)$ جفت‌جفت رخ می‌دهد.

بخش ۱.۵، صفحه ۱۴۵

۱. جواب تمرین ۱ بخش ۱.۲ با $f(x)$ و $g(x)$ به جای a و b را ملاحظه کنید.

۳. به موجب فرض $p(x)|k(x)(f(x) - g(x))$؛ از قضیه ۱۶.۴ استفاده کنید.

۹. هشت کلاس همنهشتی وجود دارد.

۱۱. نشان دهید که اگر $a \neq b$، در این صورت (پیمانه $x^۲ - ۲$) $x + a \not\equiv x + b$. بنابراین کلاس‌های هم‌ارزی $x + a$ و $x + b$ متمایز هستند.

بخش ۲.۵، صفحه ۱۵۱

۱. برای پرهیز از بزرگی بیش از اندازه جداول زیر $x^۲ + x + ۱$ با نماد A نشان داده شده است.

$+$	$[۰]$	$[۱]$	$[x]$	$[x+۱]$	$[x^۲]$	$[x^۲+۱]$	$[x^۲+x]$	$[A]$
$[۰]$	$[۰]$	$[۱]$	$[x]$	$[x+۱]$	$[x^۲]$	$[x^۲+۱]$	$[x^۲+x]$	$[A]$
$[۱]$	$[۱]$	$[۰]$	$[x+۱]$	$[x]$	$[x^۲+۱]$	$[x^۲]$	$[A]$	$[x^۲+x]$
$[x]$	$[x]$	$[x+۱]$	$[۰]$	$[۱]$	$[x^۲+x]$	$[A]$	$[x^۲]$	$[x^۲+۱]$
$[x+۱]$	$[x+۱]$	$[x]$	$[۱]$	$[۰]$	$[A]$	$[x^۲+x]$	$[x^۲+۱]$	$[x^۲]$
$[x^۲]$	$[x^۲]$	$[x^۲+۱]$	$[x^۲+x]$	$[A]$	$[۰]$	$[۱]$	$[x]$	$[x+۱]$
$[x^۲+۱]$	$[x^۲+۱]$	$[x^۲]$	$[A]$	$[x^۲+x]$	$[۱]$	$[۰]$	$[x+۱]$	$[x]$
$[x^۲+x]$	$[x^۲+x]$	$[A]$	$[x^۲]$	$[x^۲+۱]$	$[x]$	$[x+۱]$	$[۰]$	$[۱]$
$[A]$	$[A]$	$[x^۲+x]$	$[x^۲+۱]$	$[x^۲]$	$[x+۱]$	$[x]$	$[۱]$	$[۰]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[A]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[A]$
$[x]$	$[0]$	$[x]$	$[x^2]$	$[x^2+x]$	$[x+1]$	$[1]$	$[A]$	$[x^2+1]$
$[x+1]$	$[0]$	$[x+1]$	$[x^2+x]$	$[x^2+1]$	$[A]$	$[x^2]$	$[1]$	$[x]$
$[x^2]$	$[0]$	$[x^2]$	$[x+1]$	$[A]$	$[x^2+x]$	$[x]$	$[x^2+1]$	$[1]$
$[x^2+1]$	$[0]$	$[x^2+1]$	$[1]$	$[x^2]$	$[x]$	$[A]$	$[x+1]$	$[x^2+x]$
$[x^2+x]$	$[0]$	$[x^2+x]$	$[A]$	$[1]$	$[x^2+1]$	$[x+1]$	$[x]$	$[x^2]$
$[A]$	$[0]$	$[A]$	$[x^2+1]$	$[x]$	$[1]$	$[x^2+x]$	$[x^2]$	$[x+1]$

۳.

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[1]$	$[x+1]$
$[x+1]$	$[0]$	$[x+1]$	$[x+1]$	$[0]$

۷. $[a+bx]+[c+dx]=[(a+c)+(b+d)x]$؛
$[a+bx][c+dx]=[(ac+3bd)+(ad+bc)x]$.

۱۱. حاصل‌ضرب $[x]$ در خودش را در نظر بگیرید.

بخش ۳.۵، صفحه ۱۵۷

۱. بنابه نتیجه ۵.۵، عناصر متمایز $\mathbb{F}[x]/(x-a)$، کلاس‌هایی به صورت $[c]$ هستند با $c \in \mathbb{F}$. با استفاده از این، نشان دهید $\mathbb{F}[x]/(x-a)$ با $\mathbb{F}$ یکریخت است.

۳. (الف) بررسی کنید که وارون ضربی $r+s\sqrt{۳}$ به صورت $\frac{r}{t}-\frac{s}{t}\sqrt{۳}$ است، جایی که $t=r^۲-۳s^۲$.

۷. بنابه نتیجه ۱۱.۵، یک توسیع میدان $\mathbb{K}$ از $\mathbb{F}$ وجود دارد که ریشه‌ای مانند $c_۱$ از $f(x)$ را شامل است. بنابراین $f(x)=(x-c_۱)g(x)$ در $\mathbb{K}[x]$. با استفاده مجدد از نتیجه ۱۱.۵، توسیع میدان $\mathbb{L}$ از $\mathbb{K}$ را چنان بیابید که ریشه‌ای مانند $c_۲$ از $g(x)$ را شامل باشد. این روند را ادامه دهید.

بخش ۱.۶، صفحه ۱۶۷

۱. I غیرتهی است زیرا $۰_R=۰_Rc\in I$. اگر $r,s\in R$ با $rc,sc\in I$، در این صورت $rc-sc=(r-s)c\in I$. برای هر $t\in R$، $(rc)t=t(rc)=(tr)c\in I$. بنابراین طبق قضیه ۱.۶، I یک ایده‌آل است.

۳. برای دیدن این که K یک ایده‌آل نیست، ملاحظه کنید چه رخ می‌دهد وقتی یک چندجمله‌ای ثابت را در یک چندجمله‌ای با درجه مثبت ضرب می‌کنید.

۵. (الف) $(۱)=(۲)=(۳)=(۴)=\mathbb{Z}_۵$ و $(۰)=\{۰\}$

(پ) $(۱)=(۵)=(۷)=(۱۱)=\mathbb{Z}_{۱۲}$؛ $(۰)=\{۰\}$؛

$(۲)=(۶)=(۱۰)=\{۰,۲,۴,۶,۸,۱۰\}$؛ $(۴)=(۸)=\{۰,۴,۸\}$؛

$(۳)=(۹)=\{۰,۳,۶,۹\}$.

۱۱. (الف) اگر $r\in R$ و $۱_R\in I$، در این صورت $r=r\cdot ۱_R\in I$. بنابراین $R\subseteq I$ و لذا $R=I$.

۱۳. تمرین ۱۱ و تذکرات بعد از قضیه ۵.۳ را بکار برید.

۲۱. هر عضو $(n)\cap(m)$ بر هر دو عدد m و n بخش‌پذیر است؛ بنابراین بنا به تمرین ۱۷ بخش ۱.۲ در (mn) قرار دارد.

۲۵. ($\Leftarrow$) اگر $(a)=(b)=(۰_R)$، نشان دهید که $a=۰_R=b$ و بنابراین $a=bu$ با $u=۱_R$.

اگر $(a)=(b)\neq(۰_R)$، در این صورت هر دو a و b غیر صفرند و $a=a\cdot ۱_R\in(a)$.

بنابراین $a\in(b)$ و در نتیجه برای برخی $u\in R$، $a=bu$. به‌طور مشابه برای برخی $v\in R$،

$b = av$. بنابراین $a = bu = avu$ که نتیجه می‌دهد $uv = 1_R$ (قضیه ۷.۳)، پس u یک یکه است.

۲۹. از قضیه ۱.۶ استفاده کنید. K غیرتهی است زیرا طبق قضیه ۱۰.۳، $f(0_R) = 0_S$ و بنابراین $0_R \in K$. اگر $a, b \in K$، در این صورت بنا به تعریف K، $f(a) = 0_S$ و $f(b) = 0_S$. برای نشان دادن این که $a - b \in K$، باید ثابت کنید که $f(a - b) = 0_S$. اگر $r \in R$، به منظور نشان دادن $ra \in K$، باید ثابت کنید $f(ra) = 0_S$.

۳۳. اگر $I \neq (3)$، نشان دهید که I شامل یک عنصر b است به قسمی که $(3, b) = 1$. از قضیه ۱.۳ استفاده کنید تا نشان دهید که $1 \in I$ و بنابراین، طبق تمرین ۱۱ (الف)، $I = \mathbb{Z}$.

۳۷. (ب) اگر $f(x) \in \mathbb{Z}[x]$ دارای جمله ثابت c باشد، در این صورت $f(x) - c$، x را می‌شمارد، پس طبق (الف) (پیمانه J) $f(x) \equiv c$. بنابراین بنا به قضیه ۴.۶، $f(x) + J = c + J$. اگر b و c اعداد صحیح متمایز باشند، در این صورت $c - b$ نمی‌تواند بر x بخش‌پذیر باشد (چرا؟). بنابراین طبق قضیه ۴.۶، $b + J \neq c + J$.

بخش ۲.۶، صفحه ۱۷۹

۳. طبق تمرین ۱۳ بخش ۱.۶، هسته f یا $(0_{\mathbb{F}})$ یا $\mathbb{F}$ است. توضیح دهید چرا نمی‌تواند $\mathbb{F}$ باشد. طبق قضیه ۹.۶، f یک به یک است و بنابراین یک یکریختی است.

۵. حالتی را که در آن $R = \mathbb{Z}$ و I ایده‌ال اصلی (n) است در نظر بگیرید. در این صورت $\mathbb{Z}/I$ همان $\mathbb{Z}_n$ است. آیا $\mathbb{Z}_n$ همیشه یک دامنه صحیح است؟

۹. قضیه اول یکریختی را برای نگاشت همانی از R به R بکار برید.

۱۳. $g(x)$ در هسته φ است اگر و تنها اگر $g(1) = 0$. امّا طبق قضیه عامل ۱۲.۴، $g(1) = 0$ اگر و تنها اگر $(x - 1)$، $g(x)$ را بشمارد.

۱۹. طبق قضیه اول یکریختی، هر تصویر همریختی $\mathbb{Z}$ یکریخت با حلقه‌ای به صورت $\mathbb{Z}/K$ است که در آن K یک ایده‌آل $\mathbb{Z}$ است. بنا به تمرین ۴۱ بخش ۱.۶، هر ایده‌آل K اصلی است، مثلاً $K = (n)$. بنابراین هم‌مجموعه‌های به پیمانه K همان کلاس‌های هم‌ارزی به پیمانه n

هستند و $\mathbb{Z}/K$ برابر $\mathbb{Z}$ است (اگر $n = 0$)، برابر 0 است (اگر $n = 1$)، و برابر $\mathbb{Z}_n$ است (اگر $n > 1$).

۲۷. اگر $r + J$ عنصر پوچ‌توانی از R/J باشد، در این صورت برای برخی n، داریم $0_R + J = (r + J)^n = r^n + J$. بنابراین $r^n \in J$ (چرا؟) که بدین معنی است که r^n در R پوچ‌توان است. بنابراین برای برخی m، $0_R = (r^n)^m$. امّا این بیان می‌کند که $r \in J$ و لذا $r + J$ هم مجموعه صفر $0_R + J$ است.

بخش ۳.۶، صفحه ۱۸۷

۱. بنا به تعریف مرکب بودن، $n = cd$ با $|n| > |c| > 1$ و $|n| > |d| > 1$. پس c و d نمی‌توانند مضاربی از n باشند. حال $cd = n \in (n)$، و $c \notin (n)$ و $d \notin (n)$. بنابراین (n) یک ایده‌آل اوّل نیست.

۳. (الف) با استفاده از قضیه ۸.۲، نشان دهید p اول است اگر و تنها اگر $\mathbb{Z}_p$ یک میدان باشد. امّا $\mathbb{Z}_p = \mathbb{Z}/(p)$؛ قضیه ۱۳.۶ را بکار برید.

۵. ایده‌آلهای بیشین $\mathbb{Z}_6$، عبارتند از $\{0, 3\}$ و $\{0, 2, 4\}$.

۷. اگر R یک میدان باشد، از تمرین ۱۳ بخش ۱.۶ استفاده کنید. اگر (0_R) یک ایده‌آل بیشین باشد، از قضیه ۱۳.۶ و تمرین ۹ بخش ۲.۶ استفاده کنید.

۹. اگر $p = cd$، در این صورت $cd \in (p)$. چون (p) اوّل است، یا $c \in (p)$ یا $d \in (p)$، مثلاً فرض کنید $c \in (p)$. بنابراین برای برخی $v \in R$، $c = pv$. با استفاده از این و این حقیقت که $p = cd$، نشان دهید d یک یکه است.

۱۵. (ب) M اول نیست زیرا برای مثال، $0 = 7 \times 3 \in M$، امّا $3 \notin M$ و $7 \notin M$.

۱۷. بنا به تمرین ۲۴ بخش ۲.۶، I یک ایده‌آل است. با استفاده از این حقیقت که $J \neq S$ (چرا؟) و پوشا بودن f، نشان دهید که $I \neq R$. اگر $rs \in I$، در این صورت $f(rs) \in J$، بنابراین $f(r)f(s) \in J$ (چرا؟)، پس بنا به اوّل بودن، $f(r) \in J$ یا $f(s) \in J$، بنابراین $r \in I$ یا $s \in I$، و لذا I اوّل است.

۱۹. (⇐) فرض کنید R دارای یک ایده‌آل بیشین یکتای M باشد. بنابه تعریف، $M \neq R$ و بنابراین طبق تمرین ۱۱ بخش ۱.۶، M مشمول در مجموعه عناصر غیریکه R است. اگر c غیریکه باشد، در این صورت $(c) \neq R$ (چرا؟). بنابراین طبق فرض، (c) مشمول در یک ایده‌آل بیشین است. امّا M تنها ایده‌آل بیشین R است. پس $c \in (c) \subseteq M$. چون هر عنصر یکه در M قرار دارد، ایده‌آل M، مجموعهٔ غیریکه‌های R است.

بخش ۱.۷، صفحه ۲۰۳

۱. $\begin{pmatrix}۱&۲&۳\\۳&۱&۲\end{pmatrix} = \begin{pmatrix}۱&۲&۳\\۲&۳&۱\end{pmatrix}^{-۱}$ و $\begin{pmatrix}۱&۲&۳\\۲&۳&۱\end{pmatrix}^{-۱} = \begin{pmatrix}۱&۲&۳\\۳&۱&۲\end{pmatrix}$. هریک از جایگشت‌های دیگر وارون خودش است.

۳. (الف) ۱۸ (پ) ۲۴ (ث) ۶.

۵.

∘	$r_۰$	$r_۱$	$r_۲$	s	t	u
$r_۰$	$r_۰$	$r_۱$	$r_۲$	s	t	u
$r_۱$	$r_۱$	$r_۲$	$r_۰$	t	u	s
$r_۲$	$r_۲$	$r_۰$	$r_۱$	u	s	t
s	s	u	t	$r_۰$	$r_۲$	$r_۱$
t	t	s	u	$r_۱$	$r_۰$	$r_۲$
u	u	t	s	$r_۲$	$r_۱$	$r_۰$

۱۱. (الف) $S_۳ \times \mathbb{Z}_۲$ غیرآبلی از مرتبه ۱۲ و $D_۴ \times \mathbb{Z}_۳$ غیرآبلی از مرتبه ۱۶ است.

۱۵. (الف) G یک گروه است. بسته‌بودن: اگر $a, b \in \mathbb{Q}$، در این صورت $a*b = a+b+۳ \in \mathbb{Q}$.

شرکت‌پذیری:

$$\begin{aligned}(a*b)*c=(a+b+3)*c&=(a+b+3)+c+3\\&=a+b+c+6\\&=a+(b+c+3)+3\\&=a*(b+c+3)\\&=a*(b*c).\end{aligned}$$

بررسی کنید که ۳− عنصر همانی است و اینکه $a-6$− وارون a است زیرا $(-6-a)*a=a+(-6-a)+3=-3$، و به طور مشابه $a*(-6-a)$.

(پ) G یک گروه با عضو همانی ۰ است. وارون a عبارت است از $-a/(1+a)$.

۱۷. خیر؛ هیچ عضو همانی e وجود ندارد که برای هر عد حقیقی غیرصفر a در هر دو رابطه $a*e=a$ و $e*a=a$ صدق کند.

۲۵. اگر $ab=ac$، آنگاه $eb=(a^{-1}a)b=a^{-1}(ab)=a^{-1}(ac)=(a^{-1}a)c=ec$. پس $b=eb=ec=c$.

۲۹. فرض کنید a، b و c عناصر متمایزی از T باشند. گیریم $\sigma\in A(T)$ توسط $\sigma(a)=b$، $\sigma(b)=a$، و $\sigma(t)=t$ برای هر عنصر دیگر t از T تعریف شده‌باشد. فرض کنید $\tau\in A(T)$ توسط $\tau(a)=b$، $\tau(b)=c$، $\tau(c)=a$، و $\tau(t)=t$ برای هر عنصر دیگر T، تعریف شده باشد. بررسی کنید که $(\sigma\circ\tau)(a)=a$ و $(\tau\circ\sigma)(a)=c$؛ بنابراین $\sigma\circ\tau\neq\tau\circ\sigma$.

بخش ۲.۷، صفحه ۲۱۲

۱. $e=c^{-1}c=c^{-1}c^{2}=(c^{-1}c)c=ec=c$.

۵. اگر $f(a)=f(b)$، در این صورت $a^{-1}=b^{-1}$. پس $(a^{-1})^{-1}=(b^{-1})^{-1}$. بنابراین طبق نتیجه ۳.۷، $a=(a^{-1})^{-1}=(b^{-1})^{-1}=b$. پس f یک به یک است. با استفاده از نتیجه ۳.۷ همچنین می‌توان نشان داد که f پوشا است.

۷. جدول مثال ۹.۷ نشان می‌دهد که ۶ عضو از گروه D_4 در معادلهٔ $x^2 = e$ صدق می‌کنند.

۱۱. (الف) U_{10} دارای مرتبه ۴ است؛ U_{24} دارای مرتبه ۸ است.

۱۳. اگر G یک گروه متناهی باشد و $a \in G$، در این صورت همه عناصر a، a^2، a^3، ... نمی‌توانند متمایز باشند. بنابراین برای برخی $i > j$، $a^i = a^j$. نتیجه ۶.۷ نشان می‌دهد که a دارای مرتبه متناهی است.

۱۵. (الف) $x = a^{-1}b$ یک جواب $ax = b$ است زیرا $a(a^{-1}b) = (aa^{-1})b = eb = b$. اگر c نیز یک جواب باشد، در این صورت $ac = b = a(a^{-1}b)$. بنابراین طبق قسمت ۲ قضیه ۲.۷، $c = a^{-1}b$.

۲۱. اگر $a, b \in G$، در این صورت بنا به فرض $aa = e$، $bb = e$ و $abab = e$. دو طرف معادله آخر را از سمت چپ در ba ضرب کنید و ساده نمایید.

۲۳. فرض کنید $x = a^{-1}cb^{-1}$ و نشان دهید که $axb = c$. برای اثبات یکتایی، فرض کنید $ayb = c$ و نشان دهید که $y = a^{-1}cb^{-1}$.

۲۷. (ب) در S_3، فرض کنید $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ و $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. بررسی کنید که $|a| = 2$، $|b| = 2$، $ab = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$، و $(ab)^2 = ab$.

۲۹. فرض کنید $|a| = m$ و $|b| = n$، با $(m, n) = 1$. اگر $(ab)^k = e$ و $ab = ba$، در این صورت $a^k b^k = (ab)^k = e$، پس $a^k = b^{-k}$. بنابراین $a^{kn} = (b^{-k})^n = (b^n)^{-k} = e$. لذا طبق قضیه ۵.۷، $m|kn$ و در نتیجه طبق قضیه ۵.۱، $m|k$. به طور مشابه $n|k$. بنابراین طبق تمرین ۱۷ بخش ۲.۱، $mn|k$.

۳۱.

$$\begin{aligned} ab = b^2a \Rightarrow aba^{-1} = b^2 &\Rightarrow (aba^{-1})^3 = (b^2)^3 \\ &\Rightarrow (aba^{-1})(aba^{-1})(aba^{-1}) = b^{12} \\ &\Rightarrow ab^3a^{-1} = e \quad (b^6 = e \text{ زیرا}) \\ &\Rightarrow ab^3 = a \Rightarrow b^3 = e. \end{aligned}$$

بنابراین $ab = b^4a = b^3ba = eba = ba$.

بخش ۳.۷، صفحه ۲۲۱

۱. چون e_H عضو همانی H است، $e_He_H = e_H$. تمرین ۱ بخش ۲.۷ را با $c = e_H$ به کار برید.

۳. (الف) اگر $a, b \in H \cap K$، در این صورت $a, b \in H$ و $a, b \in K$. چون H یک زیرگروه است، $ab \in H$ و $a^{-1} \in H$. به طور مشابه، $ab \in K$ و $a^{-1} \in K$. پس $ab \in H \cap K$ و $a^{-1} \in H \cap K$. بنابراین طبق قضیه ۷.۷، $H \cap K$ یک زیرگروه است.

۷. $\langle 1 \rangle = \{1\}$؛ $\langle 2 \rangle = \langle 8 \rangle = \{1, 2, 4, 8\}$؛ $\langle 4 \rangle = \{1, 4\}$؛
$\langle 7 \rangle = \langle 13 \rangle = \{1, 4, 7, 13\}$؛
$\langle 11 \rangle = \{1, 11\}$؛ $\langle 14 \rangle = \{1, 14\}$.

۱۱. $2^4 = 1$؛ $2^1 = 2$؛ $2^2 = 4$؛ $13^3 = 7$؛ $2^3 = 8$؛ $2013 = 11$؛ $13^1 = 13$؛
$13^{2013} = 14$.

۱۵. (الف) با بکاربردن نماد جمعی می‌بینیم که $\mathbb{Z}_2 \times \mathbb{Z}_3$ دوری با مولد $(1, 1)$ است:
$1(1, 1) = (1, 1)$؛ $2(1, 1) = (0, 2)$؛ $3(1, 1) = (1, 0)$؛ $4(1, 1) = (0, 1)$؛
$5(1, 1) = (1, 2)$؛ $6(1, 1) = (0, 0)$.

۱۷. چون H غیرتهی است، عنصری مثل c در H وجود دارد. بنابه فرض، $e = cc^{-1} \in H$. اگر $d \in H$، چون $e \in H$ داریم $d^{-1} = ed^{-1} \in H$. با استفاده از این و این حقیقت که $d = (d^{-1})^{-1}$، نشان دهید که $c, d \in H$ نتیجه می‌دهد $cd \in H$. قضیه ۷.۷ را به کار برید.

۱۹. از قضیه ۷.۷ استفاده کنید. اگر $a, b \in \mathcal{Z}(G)$، باید نشان دهید که $ab \in \mathcal{Z}(G)$ و $a^{-1} \in \mathcal{Z}(G)$، یعنی این که برای هر $g \in G$، $abg = gab$ و $ga^{-1} = a^{-1}g$.

۲۳. ($\Leftarrow$) اگر a در مرکز G باشد، در این صورت برای هر $g \in G$، $ag = ga$. بنابراین $C(a) = \{a \in G \mid ag = ga\} = G$.

۲۷. اگر $a, b \in H$ و $x^{-1}ax$ و $x^{-1}bx$ در $x^{-1}Hx$ قرار داشته باشند، در این صورت

$ab \in H$، و بنابراین $(x^{-1}ax)(x^{-1}bx) = x^{-1}(ab)x \in x^{-1}Hx$. نشان دهید که $(x^{-1}ax)^{-1} = x^{-1}a^{-1}x \in x^{-1}Hx$؛ قضیه ۷.۷ را بکار برید.

۳۱. اگر $a^n, b^n \in H$، در این صورت چون G آبلی است، $a^n b^n = (ab)^n \in H$. همچنین $(a^n)^{-1} = a^{-n} = (a^{-1})^n \in H$. قضیه ۷.۷ را به کار برید.

۳۳. زیرگروههای $\mathbb{Z}_{12}$ عبارتند از $\{0\}$، $\{0,6\}$، $\{0,3,6,9\}$، $\{0,4,8\}$، $\{0,2,4,6,8,10\}$ و $\mathbb{Z}_{12}$.

۳۷. تمرین ۲۹ بخش ۲.۷ را ملاحظه کنید.

۴۱. اگر $(m,n) = d > 1$، در این صورت $m = dr$، $n = ds$ و $drs < mn$. اگر $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$، در این صورت

$$drs(a,b) = (drsa, drsb) = (sma, rnb) = (0,0).$$

بنابراین مرتبهٔ (a,b) یک شمارندهٔ drs است (طبق قضیه ۵.۷، در نماد جمعی) و لذا اکیداً کوچکتر از mn است. طبق قضیه ۱۰.۷، (a,b) یک مولد $\mathbb{Z}_m \times \mathbb{Z}_n$ (گروهی از مرتبه mn) نیست.

۴۵. (الف) نشان دهید که $U_{18} = \{1,5,7,11,13,17\}$ توسط ۵ تولید شده است.

بخش ۴.۷، صفحه ۲۳۲

۱. (الف) همریختی: $f(x+y) = 3(x+y) = 3x+3y = f(x)+f(y)$. پوشا بودن: اگر $t \in \mathbb{R}$، در این صورت $f(t/3) = 3(t/3) = t$. یک به یک بودن: اگر $f(x) = f(y)$، در این صورت $3x = 3y$ و بنابراین $x = y$.

۳. (الف) $\begin{pmatrix}1&0\\0&1\end{pmatrix}$، $\begin{pmatrix}1&1\\0&1\end{pmatrix}$، $\begin{pmatrix}1&0\\1&0\end{pmatrix}$، $\begin{pmatrix}0&1\\1&1\end{pmatrix}$، $\begin{pmatrix}1&1\\1&0\end{pmatrix}$، $\begin{pmatrix}0&1\\1&0\end{pmatrix}$.

(ب) ساده‌تر این است که جداول دو گروه را مقاسیه کنید، وقتی که ترتیب عناصر متناظر در دو گروه یکسان در نظر گرفته شود. برای تعیین یک تناظر، به خاطر آورید که تحت یکریختی، عناصر متناظر باید دارای مرتبه یکسان باشند.

۵. نشان دهید که هر دو گروه دوری از مرتبه ۴ هستند و قضیه ۱۳.۷ را به کار برید.

۹. $f(a^0) = f(e_G) = e_H = f(a)^0$. برای اعداد صحیح مثبت، استقراء بکار برید: $f(a^1) = f(a) = f(a)^1$. اگر $f(a^k) = f(a)^k$، در این صورت

$$f(a^{k+1}) = f(a^k a^1) = f(a^k)f(a) = f(a)^k f(a) = f(a)^{k+1}.$$

بنابراین برای هر $n \geq 0$، $f(a^n) = f(a)^n$. در مورد اعداد صحیح منفی چه می‌توان گفت؟

۱۳. ($\Leftarrow$) اگر G آبلی باشد، در این صورت f یک همریختی است زیرا، $f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b)$. در این حالت، طبق تمرین ۵ بخش ۲.۷، f یک یکریختی است.

۱۹. اگر $a^n = e_G$، آنگاه طبق تمرین ۹ و قضیه ۱۴.۷، $f(a)^n = f(a^n) = f(e_G) = e_H$. به طور مشابه، اگر $f(a)^n = e_H$ در این صورت $f(a^n) = f(a)^n = e_H = f(e_G)$. از یک به یک بودن f بدست می‌آوریم $a^n = e_G$. پس $a^n = e_G$ اگر و تنها اگر $f(a)^n = e_H$.

۲۳. اگر $f, g \in \mathrm{Inn}G$، در این صورت برای برخی c و d، $f(a) = c^{-1}ac$ و $g(a) = d^{-1}ad$. نشان دهید که $(f \circ g)(a) = (dc)^{-1}a(dc)$ و بنابراین $f \circ g \in \mathrm{Inn}G$. نشان دهید وارون تابع f، تابع $h \in \mathrm{Inn}G$ با ضابطه $h(a) = cac^{-1} = (c^{-1})^{-1}ac^{-1}$ است. قضیه ۷.۷ را به کار برید.

۲۷. (الف) بررسی کنید که هر عضو غیر همانی U_8 دارای مرتبهٔ ۲ است اما این در مورد U_{10} درست نیست. بنابراین طبق تمرین ۱۹، هیچ یکریختی f ای وجود ندارد.
(ب) بله. آن را با مقایسه جداول اَعمال اثبات کنید.

۳۳. (الف) اگر $\theta_c(x) = \theta_c(y)$، در این صورت $xc^{-1} = yc^{-1}$. بنا به قضیه ۲.۷، $x = y$. پس θ_c یک به یک است. اگر $x \in G$، در این صورت $xc \in G$ و $\theta_c(xc) = (xc)^{-1}c = x$. بنابراین θ_c پوشاست.

۳۹. (الف) نشان دهید که h و v هر دو خودریختی داخلی یکسانی را القاء می‌کنند (یعنی، برای هر $a \in D_4$، $h^{-1}ah = v^{-1}av$. همین کار را برای r_0 و r_2، r_1 و r_3 و برای d و t نیز انجام دهید. سپس نشان دهید که خودریختی‌های القایی توسط h، r_0، r_1 و d متمایزند (یعنی

هیچ دوتای آنها دارای اثر یکسان روی تمام عناصر D_4 نیست).

بخش ۵.۷، صفحه ۲۴۳

۱. ($\Leftarrow$) اگر $Ka = K$، در این صورت $a = ea \in Ka = K$. بنابراین $a \in K$.

۵. (ب) اگر $N \ni \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ و $G \ni \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$، در این صورت

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1/a & -b/ad \\ 0 & 1/d \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$
$$= \begin{pmatrix} 1/a & -b/ad \\ 0 & 1/d \end{pmatrix} \begin{pmatrix} a & b+cd \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & cd/a \\ 0 & 1 \end{pmatrix} \in N.$$

۷. طبق تمرین ۵ بخش ۳.۷، $G^\# = G \times < e > = G^\#$ یک زیرگروه است. طبق قضیه ۲۱.۷، $G^\#$ نرمال است زیرا برای هر $(c,d) \in G \times H$ و $(a,e) \in G^\#$، داریم

$$(c,d)^{-1}(a,e)(c,d) = (c^{-1}, d^{-1})(a,e)(c,d)$$
$$= (c^{-1}ac, d^{-1}ed) = (c^{-1}ac, e) \in G^\#.$$

۱۱. اگر $c \in G$، فرض کنید f خودریختی داخلی تعریف شده توسط $f(x) = c^{-1}xc$ (مثال ۳۱.۷ را ملاحظه کنید) باشد. چون N مشخصه است، $f(N) \subseteq N$، یعنی $c^{-1}Nc \subseteq N$. بنابراین طبق قضیه ۲۱.۷، N نرمال است.

۱۷. تمرین ۳ بخش ۳.۷ را به کار برید تا نشان دهید $N \cap K$ یک زیرگروه K است. اگر $g \in K$ و $n \in N \cap K$، در این صورت $g \in G$، $n \in N$ و بنابراین بدلیل نرمال بودن N در G، $g^{-1}ng \in N$. امّا $n \in N \cap K$ نتیجه می‌دهد $n \in K$ و چون K بسته است، $g^{-1}ng \in K$. پس $g^{-1}ng \in N \cap K$، لذا $g^{-1}(N \cap K)g \subseteq N \cap K$. بنابراین طبق قضیه ۲۱.۷، $N \cap K$ در K نرمال است.

۱۹. اگر $n \in N$ و $k \in K$، با استفاده از نرمال بودن نشان دهید که $k^{-1}(n^{-1}kn) = (k^{-1}n^{-1}k)n$ در $K \cap N = \langle e \rangle$ قرار دارد.

۲۷. فرض کنید $N = \langle a \rangle$. طبق قضیه ۱۱.۷، برای برخی k، $H = \langle a^k \rangle$. اگر $g \in G$، طبق نرمال بودن، $g^{-1}ag \in N$؛ بنابراین برای برخی t، $g^{-1}ag = a^t$. در نتیجه برای هر $a^{ki} \in H$، $g^{-1}a^{ki}g = (g^{-1}ag)^{ki} = (a^k)^{ti} \in H$.

۳۳. طبق تمرین ۳ و ۲۷ بخش ۳.۷، N یک زیرگروه است. نشان دهید که N در G نرمال است.

۳۵. طبق فرض، گروه دوری $\langle a \rangle$ نرمال است. بنابراین $b^{-1}ab \in \langle a \rangle$، یعنی برای برخی k، $b^{-1}ab = a^k$.

بخش ۶.۷، صفحه ۲۵۱

۳. نشان دهید که $\mathbb{Z}_{18}/M$ دوری با مولد $M + 1$ است؛ سپس نشان دهید که $M + 1$ دارای مرتبه ۶ در $\mathbb{Z}_{18}/M$ است.

۵. $G/N \cong \mathbb{Z}_2$.

۹. چون $ab = ba$ در G، $NaNb = Nab = Nba = NbNa$ در G/N.

۱۳. $\mathbb{R}^*/\mathbb{R}^{**} \cong \mathbb{Z}_2$.

۱۵. (الف) اگر $m, n \in \mathbb{Z}$، در این صورت $n(\frac{m}{n} + \mathbb{Z}) = m + \mathbb{Z} = 0 + \mathbb{Z}$ در $\mathbb{Q}/\mathbb{Z}$.

بخش ۷.۷، صفحه ۲۵۸

۱. (الف) همریختی: $f(x + y) = 3(x + y) = 3x + 3y = f(x) + f(y)$. هسته f عبارت است از $\{0, 4, 8\}$.

(پ) هسته g عبارت است از $\{0, 2, 4, 6\}$. (ث) همریختی:

$$h([x]_{18} + [y]_{18}) = h([x + y]_{18}) = [2(x + y)]_3 = [2x]_3 + [2y]_3 = h([x]_{18}) + h([y]_{18}).$$

۵. (الف) $\mathbb{Z}_2$، $\mathbb{Z}_3$، $\mathbb{Z}_4$، $\mathbb{Z}_6$، $\mathbb{Z}_{12}$.

۷. هسته f یک زیرگروه نرمال G است، پس چه می‌تواند باشد؟

۹. هسته، زیرگروه همه مضارب ۳ $-$ x در $\mathbb{Z}[x]$ است.

۱۱. نشان دهید نگاشت $f : \mathbb{R}^* \to \mathbb{R}^{**}$ که توسط $f(r) = | r |$ تعریف می‌شود یک همریختی پوشاست. هسته آن چیست؟

۱۹. چون طبق قضیه اول یکریختی $H \cong G/K$، کافی است یک دوسویی بین مجموعه S متشکل از همه زیرگروههای G که K را شامل هستند و مجموعه T متشکل از همه زیرگروههای G/K تعریف کنید. اگر B یک زیرگروه G باشد که K را شامل است، در این صورت B/K زیرگروهی از G/K است، سپس $\theta : S \to T$ را توسط $\theta(B) = B/K$ تعریف کنید. طبق قضیه ۳۱.۷، θ پوشاست. نشان دهید که θ یک به یک است.

بخش ۸.۷، صفحه ۲۷۳

۱. (الف) ۴ (ب) ۱ (پ) ۶.

۳. (الف) ۱، ۲، ۳، ۴، ۶، ۸، ۱۲، ۲۷ (پ) ۱، ۲، ۴، ۵، ۸، ۱۰، ۱۶، ۲۰، ۴۰، ۸۰.

۵. ۲۷، ۷۲۰.

۷. $H \cap K$ یک زیرگروه H و K است و لذا طبق قضیه لاگرانژ مرتبه آن باید p را بشمارد. بنابراین $|H \cap K|$ یا ۱ است (که در این حالت $H \cap K =< e >$) یا p است (که در این حالت $H = H \cap K = K$).

۹. (الف) ۳ یا ۵.

۱۱. (الف) اگر $e \neq a \in G$، در این صورت $\langle a \rangle$ زیرگروهی غیرهمانی از G است. بنابراین $G = \langle a \rangle$. اگر $| G | = | a |$ یک عدد مرکب باشد، مثلاً $| a | = td$، در این صورت طبق قضیه ۵.۷، $\langle a^t \rangle$ زیرگروهی از مرتبه d است. قضیه ۳۵.۷ را بکار برید.

۱۳. ۲.

۱۷. اگر $a^n = e_G$، در این صورت $f(a)^n = f(a^n) = f(e_G) = e_H$. پس طبق قضیه ۵.۷، $| f(a) |$، n را می‌شمارد.

۱۹. یک زیرگروه سره دارای مرتبه n است، با $1 < n < pq$ و n یک شمارندهٔ pq است. قضیه ۳۵.۷ را به کار برید.

۲۳. اگر مرکز $\mathcal{Z}(G)$ دارای مرتبهٔ p باشد، در این صورت $G/\mathcal{Z}(G)$ دارای مرتبهٔ q است. بنابراین طبق قضایای ۳۵.۷ و ۲۵.۷، G دوری است.

۲۷. طبق قضیه لاگرانژ، $\mathcal{Z}(G)$ باید دارای مرتبه p یا p^2 باشد. اگر دارای مرتبه p^2 باشد، در این صورت $G = \mathcal{Z}(G)$، پس G آبلی است. اگر $\mathcal{Z}(G)$ دارای مرتبه p باشد، در این صورت $G/\mathcal{Z}(G)$ دارای مرتبه p است و بنابراین طبق قضایای ۳۵.۷ و ۲۵.۷، G آبلی است.

۳۱. اگر $a^p = e$ و $b^p = e$، در این صورت $(ab)^p = a^p b^p = e$. بنابراین طبق قضایای ۵.۷ و ۸.۷، H یک زیرگروه است. اگر $|H|$ توسط یک عدد اول q که مخالف p است شمرده شود، در این صورت طبق قضیه کشی ۳۵.۷، H باید عنصری از مرتبهٔ q را شامل باشد. بنابراین $|H|$ باید توانی از p باشد.

بخش ۹.۷، صفحه ۲۸۴

۱. (الف) $(۱\ ۷\ ۳)$ (پ) $(۱\ ۴\ ۷\ ۶\ ۲\ ۸\ ۳)$.

۳. (الف) $(۱\ ۲)(۴\ ۵)(۶\ ۷\ ۹)$ (پ) $(۱\ ۳)(۲\ ۵\ ۴)(۶\ ۹)(۷\ ۸)$.

۵. (الف) فرد (پ) زوج.

۷. (الف) ۳ (پ) ۶۰.

۱۱. $(a_1 a_2 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2)$. تعداد $k-1$ ترانهش (یکی برای هر یک از $a_2, a_3, \ldots, a_k$) وجود دارد. $k-1$ زوج است اگر و تنها اگر k فرد باشد.

۱۵. σ را به r_1 و σ^2 را به $(r_1)^2$ نظیر کنید، و غیره. τ را به d، $\sigma\tau$ را به $r_1 d$، $\sigma^2\tau$ را به $(r_1)^2 d$ نظیر کنید و غیره.

۲۳. فرض کنید $\tau = (ab)$ و σ را به صورت حاصل‌ضربی از دورهای مجزا بیان کنید. چون طبق تمرین ۱۲، دورهای مجزا جابجا می‌شوند و چون هر دور وارون خودش است، همه دورهایی در

$\sigma\tau\sigma^{-1}$ که a یا b را شامل نیستند حذف خواهند شد و $\sigma\tau\sigma^{-1}$، به یکی از موارد زیر کاهش می‌یابد (جایی که a، b، x، y نمادهای متمایز هستند): $(ab)(ab)(ab)$؛ $(by)(ab)(by)$؛ $(ax)(ab)(ax)$؛ $(ax)(by)(ab)(ax)(by)$. بررسی کنید که هر یک، یک ترانهش است.

۲۵. اثبات قضیه ۴۸.۷ را با G به جای S_n سازگار کنید.

۲۹. سه حالت ممکن وجود دارد (جایی که a، b، c و d نمادهایی متمایز هستند): $(ab)(ab)$، $(ab)(ac)$ و $(ab)(cd)$. ولی $(abc)^3 = (1) = (ab)(ab)$؛ $(ab)(ac) = (acb)$؛ و $(ab)(cd) = (acb)(acd)$.

بخش ۱.۸، صفحه ۲۹۷

۳. (الف) درست است. برهان: $a|b$ یعنی $b = au$ و $c|d$ یعنی $d = cv$. بنابراین $bd = aucv = ac(uv)$.

۵. اگر a یک وابسته b باشد، در این صورت برای برخی یکه u، $a = bu$. بنابراین $bu = a = bc$، و لذا $u = c$، که یک تناقض است.

۷. (الف) فرض کنید $q = pu$، جایی که p تحویل‌ناپذیر و u یکه است. فرض کنید $q = rs$؛ آنگاه $rs = pu$، و بنابراین $p = (pu)u^{-1} = (rs)u^{-1} = r(su^{-1})$. چون p تحویل‌ناپذیر است از قضیه ۱.۸ نتیجه می‌شود، یا r یا su^{-1} یکه است. اگر su^{-1} یکه باشد، مثلاً $su^{-1}w = 1$، در این صورت s یکه است. بنابراین طبق قضیه ۱.۸، q تحویل‌ناپذیر است.

۱۱. مثال بعد از نتیجه ۴.۸ را ملاحظه کنید.

۱۳. $\Leftarrow$) هر شمارنده یک عنصر یکه u خود یکه است (چرا؟) و بنابراین طبق تمرین ۷ (ب) یک وابسته u است. پس u هیچ شمارنده سره‌ای ندارد.

۱۵. اگر $a \in R \neq 0_R$، قضیه ۱.۸ را بکار برید تا نشان دهید که a^2 نمی‌تواند تحویل‌ناپذیر باشد و لذا باید یکه باشد. بنابراین a یکه است.

۱۷. فرض کنید $p = rs$. آنگاه $p|r$ یا $p|s$. نشان دهید که r یا s باید یکه باشد و قضیه ۱.۸ را بکار برید.

۲۳. برای برخی d، $bc = ad$. اگر $a = r_1 r_2 \cdots r_k$، $d = z_1 z_2 \cdots z_n$، $b = p_1 p_2 \cdots p_s$ و $c = q_1 q_2 \cdots q_t$ که در آن همه p_i، q_i، r_i و z_iها تحویل‌ناپذیرند، در این صورت $p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t = r_1 r_2 \cdots r_k z_1 z_2 \cdots z_n$. پس هر r_i یک وابسته p_j یا q_j است. اما r_i نمی‌تواند یک وابسته هیچ یک از p_jها باشد (در غیر این صورت، باید 1_R را که ب‌م‌م a و b است بشمارد، امّا این نتیجه می‌دهد که تحویل‌ناپذیر r_i یکه است).

بخش ۸.۲، صفحه ۳۰۷

۳. $(ab) \subseteq (b)$ زیرا $b|ab$. اگر $(ab) = (b)$، در این صورت $ab|b$، یعنی $abu = b$. بنابراین $au = 1_R$، که غیریکه بودن a را نقض می‌کند.

۵.

$$\begin{aligned}\delta(ab) &= \delta((su - tv) + (sv + tu)i) = (su - tv)^2 + (sv + tu)^2 \\ &= s^2u^2 - 2stuv + t^2v^2 + s^2v^2 + 2stuv + t^2u^2 \\ &= s^2u^2 + t^2v^2 + s^2v^2 + t^2u^2 = (s^2 + t^2)(u^2 + v^2) \\ &= \delta(a)\delta(b).\end{aligned}$$

۱۱. اگر (a) یک ایده‌آل سره R باشد، در این صورت a یکه نیست (چرا؟) و لذا باید توسط یک عنصر تحویل‌ناپذیر p شمرده شود (قضیه ۱۰.۸). بنابراین $(p) \subseteq (a)$، جایی که طبق تمرین ۱۰، (p) بیشین است.

۱۳. (ب) بررسی کنید تابع $f : \mathbb{Z} \to \mathbb{Z}_6$ که توسط $f(a) = [a]$ تعریف می‌شود، یک همریختی پوشاست.

۱۹. طبق تمرین ۱۷، برای برخی $u, v \in R$، $d = au + bv$. اگر $e \in S$ یک شمارنده مشترک a و b باشد، آنگاه e الزاماً d را می‌شمارد. بنابراین d یک بزرگترین مقسوم‌علیه مشترک a و b در S است.

۲۵. فرض کنید برای هر عضو غیرصفر $a \in R$، $\delta(a) = k$. اگر $b \neq 0_R$، آنگاه q و r چنان وجود دارند که $1_R = bq + r$، با $r = 0_R$ یا $\delta(r) < \delta(b)$. شرط آخری ناممکن است زیرا $\delta(r) = k = \delta(b)$. پس $r = 0_R$ و بنابراین q یک وارون ضربی b است.

۲۷. طبق قضیه ۱۱.۸، $I=(b)$ که در آن b غیرصفر است. اگر $a\in\mathbb{Z}[i]$، آنگاه $a=bq+r$ با $r=0$ یا $\delta(r)<\delta(b)$، و بنابراین (پیمانه I) $a\equiv r$. طبق قضیه ۴.۶، تعداد هم‌مجموعه‌های متمایز I (کلاس‌های همنشهتی به پیمانه I) حداکثر برابر تعداد rهای ممکن تحت تقسیم عناصر $\mathbb{Z}[i]$ بر b است. نشان دهید تنها تعداد متناهی چنین rهایی وجود دارد.

بخش ۳.۸، صفحه ۳۲۰

۱. اگر $x=a$، $y=b$، $z=c$ یک جواب $x^n+y^n=z^n$ باشد و $n=kt$، نشان دهید که $x=a^t$، $y=b^t$ و $z=c^t$، یک جواب $x^k+y^k=z^k$ است، که فرض را نقض می‌کند.

۳.

$$\begin{aligned}N(ab)&=N((rm+snd)+(rn+sm)\sqrt{d})=(rm+snd)^2-d(rn+sm)^2\\&=r^2m^2+2mnrsd+s^2n^2d^2-dr^2n^2-2mnrsd-ds^2m^2\\&=r^2m^2+s^2n^2d^2-dr^2n^2-ds^2m^2\\&=(r^2-ds^2)(m^2-dn^2)=N(a)N(b).\end{aligned}$$

۹. (الف) نتیجه ۱۶.۸ را بکار برید.

۱۷. ($\Leftarrow$) فرض کنید $a=u+v\sqrt{-5}$ و $b=w+z\sqrt{-5}$. اگر $r+s\sqrt{-5}\in P$، در این صورت

$$\begin{aligned}r+s\sqrt{-5}=2a+(1+\sqrt{-5})b&=2(u+v\sqrt{-5})+(1+\sqrt{-5})(w+z\sqrt{-5})\\&=(2u+w-5z)+(2v+w+z)\sqrt{-5}.\end{aligned}$$

بنابراین $r-s=(2u+w-5z)-(2v+w+z)=2(u-v-3z)$، و لذا $r\equiv s$ (پیمانه ۲).

بخش ۴.۸، صفحه ۳۳۰

۱. (۲) $[a,b]=[ak,bk]$ زیرا $a(bk)=b(ak)$.

۳. چون $[a,1_R]+[b,1_R]=[a1_R+1_Rb,1_R1_R]=[a+b,1_R]\in R^*$ پس R^* تحت جمع بسته است، و چون $[a,1_R][b,1_R]=[ab,1_R1_R]=[ab,1_R]\in R^*$ پس R^* تحت ضرب بسته است. عضو صفر $\mathbb{F}$ یعنی $[0_R,1_R]$ در R^* قرار دارد. قرینهٔ $[a,1_R]$، $[-a,1_R]\in R^*$ است.

۵. بررسی کنید که تابع $f:R\to\{r+si\mid r,s\in\mathbb{Q}\}$ که به صورت

$$f([a+bi,c+di])=\left(\frac{ac+bd}{c^2+d^2}\right)+\left(\frac{bc-ad}{c^2+d^2}\right)$$

تعریف می‌شود، یک یکریختی است.

۱۱. طبق قضیه ۳.۱، اعداد صحیح u و v وجود دارند به قسمی که $mu+nv=1$ ؛ u و v ممکن است منفی نیز باشند. توان‌های منفی a در $\mathbb{F}$ تعریف شده‌اند و بنابراین در $\mathbb{F}$ داریم

$$a=a^1=a^{mu+nv}=a^{mu}a^{nv}=(a^m)^u(a^n)^v=(b^m)^u(b^n)^v$$
$$=b^{mu+nv}=b^1=b.$$

بخش ۵.۸، صفحه ۳۳۸

۱. ($\Leftarrow$) اگر $f(x)$ در $R[x]$ یکه باشد، در این صورت برای برخی $g(x)$، $f(x)g(x)=1_R$. طبق قضیه ۱.۴، $\deg f(x)+\deg g(x)=\deg 1_R=0$. بنابراین $\deg f(x)=0=\deg g(x)$، لذا $f(x),g(x)\in R$. بنابراین $f(x)$ در R یکه است.

۳. ($\Rightarrow$) فرض کنید p در $R[x]$ تحویل‌ناپذیر باشد. اگر در R، $p=rs$، آنگاه یا r یا s در $R[x]$ یکه است. پس طبق تمرین ۱، r یا s در R یکه است. بنابراین طبق قضیه ۱.۸، p در R تحویل‌ناپذیر است.

۵. چون $c_1c_2\cdots c_mf(x)=g(x)$، هر c_i، $g(x)$ را می‌شمارد. بنابراین هر c_i در R یکه است زیرا $g(x)$ اولیه است.

۹. ابتدا به کمک خاصیت **دی‌ت** $R[x]$ نشان دهید که R یک دامنه صحیح است. اگر c عضو غیرصفر غیریکه‌ای از R باشد، در این صورت طبق تمرین ۱، c غیرصفر و غیریکه در $R[x]$

است. بنابراین $c = p_1 p_2 \cdots p_k$، که در آن هر p_i در $R[x]$ تحویل‌ناپذیر است. قضیه ۱.۴ نشان می‌دهد که هر p_i در R قرار دارد. طبق تمرین ۳، p_i در R تحویل‌ناپذیر است. از این که $R[x]$ یک دی‌ت است استفاده کنید تا نشان دهید که این تجزیه تا حد ترتیب و وابسته‌های در R یکتاست.

بخش ۱.۹، صفحه ۳۴۹

۱. $a + bi = (b - ۲a)i + a(۱ + ۲i) + ۰(۱ + ۳i)$. همچنین

$$a + bi = (-۲a)i + (a - b)(۱ + ۲i) + b(۱ + ۳i).$$

۳. تحقیق کنید که $(\frac{-۲}{\sqrt{۲}} - \sqrt{۳})\sqrt{۲} + \sqrt{۳}(\sqrt{۲} + i) + \sqrt{۳}(\sqrt{۳} - i) = ۰$.

۵. اگر این زیرمجموعه، مجموعه $\{۰_{\mathbb{F}}, u_۲, u_۳, \ldots, u_n\}$ باشد آنگاه

$$۱_{\mathbb{F}} ۰_{\mathbb{F}} + ۰_{\mathbb{F}} u_۲ + ۰_{\mathbb{F}} u_۳ + \cdots + ۰_{\mathbb{F}} u_n = ۰_{\mathbb{F}}$$

که اولین ضریب آن ناصفر است.

۷. چون v_iها وابسته خطی‌اند، عناصر $c_i \in \mathbb{F}$ وجود دارند به طوری که همگی صفر نیستند و $c_۱ v_۱ + \cdots + c_k v_k = ۰_{\mathbb{F}}$. مجموعه $\{v_۱, \ldots, v_k, w_۱, \ldots, w_t\}$ وابسته خطی است زیرا $c_۱ v_۱ + \cdots + c_k v_k + ۰_{\mathbb{F}} w_۱ + \cdots + ۰_{\mathbb{F}} w_t = ۰_{\mathbb{F}}$ و همه ضرایب صفر نیستند.

۹. برای هر $r + si \in \mathbb{C}$، $r + si = (\frac{r}{b} - \frac{cs}{bd})b + \frac{s}{d}(c + di)$. از اینرو $\{b, c + di\}$ را $\mathbb{C}$، روی $\mathbb{R}$ پدید می‌آورد. ثابت کنید که این مجموعه نیز روی $\mathbb{R}$ مستقل خطی است.

۱۵. (الف) اگر $a + b\sqrt{۲} + c\sqrt{۳} = ۰$، آنگاه $a + b\sqrt{۲} = -c\sqrt{۳}$. طرفین را به توان ۲ برسانید و پس از مرتب‌کردن نشان دهید که:

$$۲ab\sqrt{۲} = ۳c^۲ - a^۲ - ۲b^۲.$$

اگر $ab \neq ۰$، آنگاه $\sqrt{۲} = (۳c^۲ - a^۲ - ۲b^۲)/۲ab \in \mathbb{Q}$ که متناقض با این واقعیت است که $\sqrt{۲}$ اصم است. پس $a = ۰$ یا $b = ۰$. اگر $a = ۰$، در این صورت $b\sqrt{۲} + c\sqrt{۳} = ۰$.

دو طرف را مربع کنید و استدلالی مشابه بکار برید تا نشان دهید که $bc = 0$. پس $b = 0$ یا $c = 0$. ولی $a = 0$ و $b = 0$ ایجاب می‌کند که $c\sqrt{3} = 0$، در نتیجه $c = 0$. به طور مشابه $a = 0$ و $c = 0$ ایجاب می‌کند که $b = 0$.

۲۱. فرض کنید که $c_1u_1 + \cdots + c_tu_t + dw = 0_{\mathbb{F}}$. اگر $d \neq 0_{\mathbb{F}}$ آنگاه $w = -d^{-1}c_1u_1 - d^{-1}c_2u_2 - \cdots - d^{-1}c_tu_t$، که تناقض است. بنابراین $d = 0_{\mathbb{F}}$. در نتیجه همه c_iها صفراند زیرا $\{u_1, \ldots, u_t\}$ مستقل خطی است.

۲۵. (i) $\Leftarrow$ (iii) فرض کنید که $S = \{v_1, \ldots, v_n\}$، $\mathbb{K}$ را روی $\mathbb{F}$ پدید آورد. آنگاه طبق تمرین ۲۲، S یک پایه T از $\mathbb{K}$ را شامل می‌باشد. چون $[\mathbb{K} : \mathbb{F}] = n$، T باید n عضو داشته باشد و بدین دلیل $T = S$. از تمرین ۲۴ استفاده کنید تا نشان دهید که (ii) $\Leftarrow$ (iii) و (i).

بخش ۲.۹، صفحه ۳۵۸

۳. طبق تعریف، دو میدان $\mathbb{F}(u+c)$ و $\mathbb{F}(u)$ میدان $\mathbb{F}$ را شامل هستند. چون $c \in \mathbb{F}$ و $u \in \mathbb{F}(u)$، $u + c \in \mathbb{F}(u)$. چون $\mathbb{F}(u + c)$ کوچکترین میدانی است که $\mathbb{F}$ و $u + c$ را شامل است بنابراین $\mathbb{F}(u) \supseteq \mathbb{F}(u + c)$. برعکس، $u = (u + c) - c \in \mathbb{F}(u + c)$. چون $\mathbb{F}(u)$ کوچکترین میدانی است که شامل $\mathbb{F}$ و u می‌باشد، داریم $\mathbb{F}(u) \subseteq \mathbb{F}(u + c)$. پس $\mathbb{F}(u + c) = \mathbb{F}(u)$.

۵. (الف) تحقیق کنید که $5i + 3$ یک ریشه $x^2 - 6x + 34$ است. (پ) تحقیق کنید که $\sqrt{2} + 1$ یک ریشه $x^3 - 3x^2 + 3x - 3$ است.

۷. طبق فرض، u ریشهٔ یک چندجمله‌ای $p(x)$ در $\mathbb{F}[x]$ است. ولی $\mathbb{F}[x] \subseteq \mathbb{K}[x]$، بنابراین u ریشه چندجمله‌ای $p(x)$ در $\mathbb{K}[x]$ است.

۹. $\sqrt{\pi}$ یک ریشه $x^2 - \pi$ در $\mathbb{Q}(\pi)[x]$ است.

۱۱. ۶.

۱۵. طبق لم ۲۴.۴ و قضیه عامل، $a + bi$ یک ریشه $f(x) = (x - (a + bi))(x - (a - bi))$ است. تحقیق کنید که $f(x)$ ضرایب حقیقی دارد.

۱۷. (الف) $x^4 - 2x^2 - 4$.

۲۱. π یک ریشه $x^۴ - \pi^۴$ در $\mathbb{Q}(\pi^۴)[x]$ است و از اینرو روی $\mathbb{Q}(\pi^۴)$ جبری است. بنابراین طبق قضیه ۷.۹، $\{۱, \pi, \pi^۲, \pi^۳\}$ یک پایه است.

بخش ۳.۹، صفحه ۳۶۵

۳. جوابهای صحیح زیادی وجود دارد، از جمله:
(الف) $\{۱, \sqrt{۵}, i, \sqrt{۵}i\}$، (پ) $\{۱, \sqrt{۲}, \sqrt{۳}, \sqrt{۵}, \sqrt{۶}, \sqrt{۱۰}, \sqrt{۱۵}, \sqrt{۳۰}\}$.

۵. از نتیجه ۱۴.۴ استفاده کنید تا نشان دهید که $x^۲ + ۱$ روی $\mathbb{Q}(\sqrt{۳})$ تحویل‌ناپذیر است و بنابراین چندجمله‌ای کمین i روی $\mathbb{Q}(\sqrt{۳})$ است. از اینرو $[\mathbb{Q}(\sqrt{۳}, i) : \mathbb{Q}(\sqrt{۳})] = ۲$ و

$$[\mathbb{Q}(\sqrt{۳}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{۳}, i) : \mathbb{Q}(\sqrt{۳})][\mathbb{Q}(\sqrt{۳}) : \mathbb{Q}] = ۲ \times ۲ = ۴.$$

۷. طبق قضیه‌های ۷.۹ و ۴.۹، $[\mathbb{K}(u) : \mathbb{F}]$ متناهی است. بدین دلیل طبق قضیه ۹.۹، u روی $\mathbb{F}$ جبری است. اگر $p(x) \in \mathbb{F}[x]$ چندجمله‌ای کمین u روی $\mathbb{F}$ و $q(x) \in \mathbb{F}[x]$ چندجمله‌ای کمین u روی $\mathbb{K}$ باشد، آنگاه طبق قضیه ۶.۹، $q(x)|p(x)$، بنابراین طبق قضیه ۷.۹، $[\mathbb{K}(u) : \mathbb{K}] = \deg q(x) \leq \deg p(x) = [\mathbb{F}(u) : \mathbb{F}]$.

۹. طبق قضایای ۴.۹، ۷.۹ و ۹.۹ و تمرین ۸، $[\mathbb{F}(u) : \mathbb{F}]$ و $[\mathbb{K}(u) : \mathbb{F}(u)]$ متناهی هستند، قضیه ۴.۹ را برای دنباله $\mathbb{F} \subseteq \mathbb{F}(u) \subseteq \mathbb{K}(u)$ بکار برید.

۱۱. (الف) بکارگیری قضیه ۴.۹ برای دنباله $\mathbb{F} \subseteq \mathbb{F}(u) \subseteq \mathbb{F}(u, v)$ نشان می‌دهد که $m = \deg p(x) = [\mathbb{F}(u) : \mathbb{E}]$، $[\mathbb{F}(u, v) : \mathbb{F}]$ را می‌شمارد. به‌طور مشابه، $n|[\mathbb{F}(u, v) : \mathbb{F}]$. از اینرو طبق تمرین ۱۷ از بخش ۳.۱، $mn|[\mathbb{F}(u, v) : \mathbb{F}]$. قضیه ۴.۹ و تمرین ۷ را بکار گیرید تا نشان دهید که $[\mathbb{F}(u, v) : \mathbb{F}] \leq mn$. بنابراین $[\mathbb{F}(u, v) : \mathbb{F}] = mn$.

۱۳. گیریم $h(x) \in \mathbb{F}(u)[x]$ چندجمله‌ای کمین v روی $\mathbb{F}[u]$ باشد، آنگاه $h(x)|q(x)$. طبق تمرین ۱۱ (الف) و قضایای ۴.۹ و ۷.۹،

$$\begin{aligned}(\deg p(x))(\deg q(x)) = [\mathbb{F}(u, v) : \mathbb{F}] &= [\mathbb{F}(u, v) : \mathbb{F}(u)][\mathbb{F}(u) : \mathbb{F}] \\ &= (\deg h(x))(\deg p(x)).\end{aligned}$$

بنابراین $\deg h(x) = \deg q(x)$ و از اینرو برای برخی $k \in \mathbb{K}$، $q(x) = kh(x)$. چون $h(x)$ روی $\mathbb{F}(u)$ تحویل‌ناپذیر است، $q(x)$ نیز تحویل‌ناپذیر است.

۱۵. اگر u روی $\mathbb{E}$ جبری باشد آنگاه طبق قضیه ۱۰.۹ و نتیجه ۱۱.۹ روی $\mathbb{F}$ جبری است.

بخش ۴.۹، صفحه ۳۷۳

۳. $\mathbb{Q}(\sqrt{5}, i)$ یک میدان شکافنده است. طبق تمرین ۳ از بخش ۳.۹، ۸۹۸۹بُعد ۴ دارد.

۷. چندجمله‌ای کمین $p(x)$ از u در $\mathbb{F}[x]$ تحویل‌ناپذیر است و یک ریشه در $\mathbb{K}$ دارد. بنابراین $p(x)$ روی $\mathbb{K} = \mathbb{F}(u)$ شکافته می‌شود.

۱۱. ریشه‌های چهارم ۱−، عبارتند از i، $(\pm\sqrt{2}/2) \pm (\sqrt{2}/2)i$، لذا $\mathbb{Q}(\sqrt{2}, i)$ یک میدان شکافنده است.

۱۵. طبق نتیجه ۱۴.۴، $x^2 + 1$ در $\mathbb{Z}_3[x]$ تحویل‌ناپذیر است. از اینرو طبق قضیه ۱۰.۵، $\mathbb{Z}_3[x]/(x^2+1)$ یک میدان ۹ عضوی است که ریشه‌های $[x]$ و $[2x]$ از چندجمله‌ای $x^2 + 1$ را شامل است.

۲۱. اگر $p(x) \in \mathbb{K}[x]$ و u یک ریشه $p(x)$ باشد، آنگاه طبق قضیه ۱۰.۹، $\mathbb{K}(u)$ روی $\mathbb{K}$ جبری است. بنابراین طبق نتیجه ۱۱.۹، u روی $\mathbb{F}$ جبری است. اگر $q(x)$ چندجمله‌ای کمین u روی $\mathbb{F}$ باشد آنگاه $q(x)$ روی $\mathbb{K}$ شکافته می‌شود و طبق قضیه ۶.۹ چندجمله‌ای تحویل‌ناپذیر $p(x)$ در $\mathbb{K}[x]$ را می‌شمارد. نشان دهید که $p(x)$ درجه ۱ دارد و تمرین ۱۹ را بکار برید.

بخش ۶.۹، صفحه ۳۸۸

۳.

$$na = a + a + \cdots + a = 1_R a + 1_R a + \cdots + 1_R a = (1_R + \cdots + 1_R)a$$
$$= (n1_R)a = 0_R a = 0_R.$$

۵. گیریم $\mathbb{F}$ و $\mathbb{K}$ دارای مشخصه یکسان p باشند. $\mathbb{F}$ مرتبه p^m دارد، که در آن طبق قضیه ۲۳.۹، $m = [\mathbb{F} : \mathbb{Z}_p]$، و بنابراین $q = p^m$. چون $[\mathbb{K} : \mathbb{Z}_p] = [\mathbb{K} : \mathbb{F}][\mathbb{F} : \mathbb{Z}_p] = nm$، قضیه ۲۳.۹ نشان می‌دهد که $\mathbb{K}$ مرتبه $p^{mn} = q^n$ دارد.

۱۳. طبق برهان قضیه ۲۵.۹، هر عضو a از $\mathbb{Z}_p$ یک ریشه $x^p - x$ است. بنابراین در $\mathbb{Z}_p$، $a^p = a$ که به معنی آن است که در $\mathbb{Z}$، (پیمانه p) $a^p \equiv a$. اگر در $\mathbb{Z}$، a نسبت به p اول باشد، آنگاه a یک عضو ناصفر میدان $\mathbb{Z}_p$ است و از اینرو وارون دارد.

۱۷. طبق قضیه ۲۵.۹، $\mathbb{E} = \mathbb{Z}_p(u_1, \ldots, u_t) = \mathbb{F}$، که در آن u_iها، تمام ریشه‌های $x^{p^n} - x$ در $\mathbb{K}$ می‌باشند.

بخش ۱.۱۰، صفحه ۳۹۷

۳. (الف) $\{(0,0)\}$؛ $\{(0,0),(1,0)\}$؛ $\{(0,0),(0,1)\}$؛ $\{(0,0),(1,1)\}$؛ $\mathbb{Z}_2 \times \mathbb{Z}_2$.

۵. $\mathbb{Z}_2 \times \mathbb{Z}_2$.

۹. خیر.

۱۳. (ب) اگر D نرمال باشد، آنگاه برای هر $a, b \in G$، $(a,e,e)(b,b,b)(a,e,e)^{-1} \in D$. ولی $(a,e,e)(b,b,b)(a,e,e)^{-1} = (aba^{-1}, b, b)$. چون این عضو در D است، باید داشته باشیم $aba^{-1} = b$ که ایجاب می‌کند $ab = ba$.

۲۳. (الف) زیرگروههای $M = \langle (123) \rangle$ و $N = \langle (12) \rangle$ را در S_3 در نظر بگیرید.

۲۵. همریختی f در برهان قضیه ۱.۱۰ را بکار برید. اگر $f(a_1, \cdots, a_k) = e$، آنگاه $a_i = (a_1 \cdots a_{i-1})^{-1} e (a_{i+1} \cdots a_k)^{-1}$. از لم ۲.۱۰ و نتیجه ۳.۷ مکرراً استفاده کنید تا نشان دهید که $a_i \in N_i \cap N_1 \cdots N_{i-1} N_{i+1} \cdots N_k =< e >$. از اینرو طبق قضیه ۲۷.۷، f یک به یک است.

۲۷. (الف) زیرگروههای نرمال S_3 چه هستند؟

بخش ۲.۱۰، صفحه ۴۱۲

۱. اگر $p^n a = 0$ و $p^m b = 0$، آنگاه $p^n(-a) = -(p^n a) = 0$ و

$$p^{m+n}(a+b) = p^n p^m (a+b) = p^m(p^n a) + p^n(p^m b) = 0.$$

از اینرو $a + b \in G(p)$ و $-a \in G(p)$. از قضیه ۷.۷ استفاده کنید.

۳. (الف) $\mathbb{Z}_۴ \oplus \mathbb{Z}_۳$؛ $\mathbb{Z}_۲ \oplus \mathbb{Z}_۲ \oplus \mathbb{Z}_۳$ (پ) $\mathbb{Z}_۲ \oplus \mathbb{Z}_۳ \oplus \mathbb{Z}_۵$ (ث) $\mathbb{Z}_۲ \oplus \mathbb{Z}_۳ \oplus \mathbb{Z}_۳ \oplus \mathbb{Z}_۵$؛
(چ) $\mathbb{Z}_۲ \oplus \mathbb{Z}_۹ \oplus \mathbb{Z}_۵$؛ $\mathbb{Z}_۲ \oplus \mathbb{Z}_۲ \oplus \mathbb{Z}_۲ \oplus \mathbb{Z}_۳ \oplus \mathbb{Z}_۵ \oplus \mathbb{Z}_۵$؛
$\mathbb{Z}_۲ \oplus \mathbb{Z}_۴ \oplus \mathbb{Z}_۳ \oplus \mathbb{Z}_۵ \oplus \mathbb{Z}_۵$؛ $\mathbb{Z}_۲ \oplus \mathbb{Z}_۲ \oplus \mathbb{Z}_۲ \oplus \mathbb{Z}_۳ \oplus \mathbb{Z}_{۲۵}$؛ $\mathbb{Z}_۸ \oplus \mathbb{Z}_۳ \oplus \mathbb{Z}_۵ \oplus \mathbb{Z}_۵$؛
$\mathbb{Z}_۸ \oplus \mathbb{Z}_۳ \oplus \mathbb{Z}_{۲۵}$؛

۵. (الف) ۲، $۵^۳$ (پ) ۲، ۲، $۲^۲$، $۲^۳$، ۳، ۵، ۵، ۵، ۵.

۷. (الف) ۲، ۲ و ۲، ۲ (پ) ۲، $۲^۲$ و ۲، $۲^۲$.

۹. (الف) G باید یک عضو از مرتبه p داشته باشد (چرا؟). اگر a مرتبه p داشته باشد، آنگاه $pa = ۰$.

۱۳. اگر q عدد اولی غیر از p باشد و اگر q، $|G|$ را بشمارد، از قضیهٔ کشی ۳۸.۷ استفاده کنید تا به یک تناقض برسید.

۱۹. (الف) تمرین ۱ یک حالت خاص این تمرین است که در آن هر عضو از مرتبه متناهی دارای مرتبه‌ای از توان p است. اساساً همان برهان در اینجا نیز کار می‌کند.

بخش ۳.۱۰، صفحه ۴۲۰

۳. $\{(۱), (۲۳)(۱۴), (۲۴)(۱۳), (۳۴)(۱۲)\}$ تنها ۲ـ زیرگروه سیلو است. ۳ـ زیرگروههای سیلو عبارتند از $\langle(۱۲۳)\rangle$، $\langle(۱۲۴)\rangle$ و $\langle(۲۳۴)\rangle$.

۵. (الف) ۱ یا ۴.

۷. (الف) نشان دهید که G یک ۷–زیرگروه سیلوی نرمال دارد. (پ) نشان دهید که G یک ۱۱–زیرگروه سیلوی نرمال دارد.

۹. اگر $a \in G$، آنگاه در G/N داریم $(Na)^{p^n} = N$)، در نتیجه $a^{p^n} \in N$.

۱۳. اگر $N_۱$، ...، N_k، p–زیرگروههای سیلو باشند، از همریختی یک به یک f ارائه شده در تمرین ۲۵ از بخش ۱.۱۰ استفاده کنید. تحقیق کنید که $|N_۱ \times \cdots \times N_k| = |G|$ و نتیجه بگیرید که f پوشا نیز هست.

۱۹. نشان دهید که یک ۳–زیرگروه سیلوی نرمال وجود دارد. توجه فرمایید که اگر شش ۵- زیرگروه نرمال وجود داشته باشد، G دارای ۲۴ عضو متمایز از مرتبه ۵ می‌باشد (چرا؟). به طور مشابه،

اگر تعداد ده ۳- زیرگروه سیلو وجود داشته باشد، G دارای ۲۰ عضو متمایز از مرتبه ۳ است.

بخش ۴.۱۰، صفحه ۴۲۹

۱. (الف) $\{r_0\}$، $\{r_2\}$، $\{r_1, r_3\}$، $\{h, v\}$، $\{d, t\}$.

۳. در D_4 به $\{r_0, r_1, r_2, r_3\}$ نگاه کنید.

۵. $\langle(123)\rangle$، $\langle(124)\rangle$، $\langle(134)\rangle$، $\langle(234)\rangle$.

۹. اگر C رده مزدوجی $a \in G$ باشد، نشان دهید که $f(C)$ رده مزدوجی $f(a)$ است.

۱۵. در معادله تمرین ۱۴ (پ)، تحقیق کنید که $|C_i|$ یا ۱ است یا توانی مثبت از p است. دست کم یک $|C_i|$ برابر ۱ می‌باشد زیرا $\{e\}$ یک رده مزدوجی است. چون $|N|$ بر p بخش‌پذیر است، باید بیشتر از یک C_i وجود داشته باشد که $|C_i| = 1$ و از اینرو یک عنصر غیرهمانی N در $Z(G)$ است.

۱۹. اگر $b \in N(N(K))$، آنگاه $b^{-1}N(K)b = N(K)$. از اینرو $b^{-1}Kb \subseteq N(K)$، زیرا $K \subseteq N(K)$. تحقیق کنید که هر دو K و $b^{-1}Kb$، $p-$زیرگروههای سیلوی $N(K)$ هستند و از اینرو در $N(K)$ مزدوج هستند. ولی K در $N(K)$ نرمال است، و بنابراین $b^{-1}Kb = K$. بدین دلیل $b \in N(K)$.

۲۱. اگر S یک $p-$زیرگروه سیلو شامل H باشد (تمرین ۲۵)، آنگاه هر $p-$زیرگروه سیلو، برای برخی $a \in G$ به صورت $a^{-1}Sa$ است و بنابراین شامل $a^{-1}Ha$ است.

بخش ۵.۱۰، صفحه ۴۳۶

۱. (الف) (۳ ۲ ۱)، (۲ ۳ ۱)، (۴ ۲ ۱)، (۲ ۴ ۱)، (۴ ۳ ۱)، (۳ ۴ ۱)، (۴ ۳ ۲)، (۳ ۴ ۲).

۳. (۱)

۵. طبق تمرین ۱۲ از بخش ۹.۷ ترانهش‌های مجزا، جابجا می‌شوند.

۷. وارون یک $k-$دور یک $k-$دور است، و دورهای متمایز طبق تمرینهای ۱۰ و ۱۲ از بخش ۹.۷ جابجا می‌شوند. چون هر $\sigma \in N$ در رابطه $\sigma^2 = (1)$ صدق می‌کند، تحقیق کنید که یک

عضو غیرهمانی در N باید یا یک ترانهش باشد یا حاصل‌ضرب ترانهش‌های متمایز باشد.

بخش ۱.۱۱، صفحه ۴۴۷

۱. اگر برای هر $c \in \mathbb{F}$، $\sigma(c) = c$، آنگاه $\sigma^{-1}(c) = \sigma^{-1}(\sigma(c)) = c$.

۳. از قضیه ۷.۹ استفاده کنید تا نشان دهید که برای هر $c \in \mathbb{F}(u)$، $\sigma(c) = c$.

۵. از نتیجه ۵.۱۱ و قضیهٔ لاگرانژ ۳۳.۷ استفاده کنید.

۹. (الف) $p(x) = x^2 + x + 1$ (ب) $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(w) \cong \mathbb{Z}_2$.

۱۱. $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, i) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

بخش ۲.۱۱، صفحه ۴۵۶

۱. تعداد میدان‌های میانی درست برابر با تعداد زیرگروههای $\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$ است، که طبق قضیه ۱۱.۱۱ متناهی است.

۵. دارای چهار میدان میانی به ابعاد ۱۰، ۵، ۲ و ۱ می‌باشد.

۹. (الف) هر زیرگروه $\mathrm{Gal}_{\mathbb{F}}\mathbb{K} \cong \mathbb{Z}_n$ (بویژه، $\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$) طبق قضیه ۱۱.۷ دوری و نرمال است. طبق قضیه ۱۱.۱۱، $\mathrm{Gal}_{\mathbb{F}}\mathbb{E} \cong \mathrm{Gal}_{\mathbb{F}}\mathbb{K}/\mathrm{Gal}_{\mathbb{E}}\mathbb{K}$؛ از تمرین ۱۴ بخش ۶.۷ استفاده کنید.
(ب) چون طبق محک ایزنشتاین، $x^4 - 2$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است، $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. طبق نتیجه ۱۴.۴ چندجمله‌ای کمین i روی $\mathbb{Q}(\sqrt[4]{2})$، $x^2 + 1$ است.

بخش ۳.۱۱، صفحه ۴۶۹

۱. (الف) جواب‌های صحیح زیادی وجود دارند، از جمله

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{5}, \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt[4]{2 + \sqrt{5}})$$
$$\subseteq \mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt[4]{2 + \sqrt{5}}, \sqrt[4]{1 + \sqrt{7}})$$

۵. $A_۴$ شامل زیرگروه H و هشت تا ۳ـ دور (۳ ۲ ۱)، (۲ ۳ ۱)، (۴ ۲ ۱)، (۲ ۴ ۱)، (۴ ۳ ۱)، (۳ ۴ ۱)، (۴ ۳ ۲)، (۳ ۴ ۲) است. نشان دهید که H در $A_۴$ نرمال است. از این واقعیت که تمام گروههای از مرتبه ≥ ۴ آبلی هستند استفاده کنید تا نشان دهید که سری $S_۴ \supseteq A_۴ \supseteq H \supseteq (۱)$ در تعریف حلپذیری صدق می‌کند.

۷. (الف) ± ۱ (ب) $\pm ۱, \pm i$. (ث) $\pm ۱, \frac{۱}{۲} \pm i\frac{\sqrt{۳}}{۲}, -\frac{۱}{۲} \pm i\frac{\sqrt{۳}}{۲}$.

۱۳. اگر $\mathbb{K}$ میدان شکافنده یک چندجمله‌ای درجه ۳ باشد، آنگاه $[\mathbb{K} : \mathbb{F}]$ بر ۳ بخش‌پذیر است (چرا؟) و طبق قضیه ۱۳.۹، کوچکتر یا مساوی ۶ است. پس این گروه گالوا، یک زیرگروه $S_۳$ (نتیجه ۵.۱۱) از مرتبه ۳ یا ۶ است.

۱۷. (الف) $x^۶ - ۴x^۳ + ۴ = (x^۳ - ۲)^۲$. $\mathbb{Q}(\sqrt[۳]{۲}, w)$ یک میدان شکافنده است، که در آن w یک ریشه سوم مختلط ۱ است، $G \cong S_۳$.

(پ) $x^۵ + ۶x^۳ + ۹x = x(x^۲ + ۳)^۲$. $\mathbb{Q}(i\sqrt{۳})$ یک میدان شکافنده است. $G \cong \mathbb{Z}_۲$

(ث) $G \cong S_۵$.

فصل ۱۲، صفحه ۴۸۰

۱. اگر (پیمانه p) $ka \equiv ۰$، آنگاه $p|ka$ ولی $(p, k) = ۱$ (چرا؟). پس طبق قضیه ۸.۱، $p|a$ که یک تناقض است.

۳. (الف) ۰۱۰۷ ۰۵۱۲ ۲۴۲۱ ۱۴۷۹.

بخش ۱.۱۳، صفحه ۴۸۷

۳. اگر یک جواب وجود داشته باشد، آنگاه طبق تمرین ۲، اعداد ۰، ۱ و ۲ نیز جواب هستند. تحقیق کنید که این طور نیست.

۹. (پیمانه ۱۸۷) $x \equiv -۳۰$.

۱۱. (پیمانه ۲۱۰) $x \equiv -۱۸$.

۱۳. (پیمانه ۲۰۴۲۰۴) $x \equiv ۲۰۴$.

۱۹. (⇒) اگر $b-a=dk$ و $mu+nv=d$، آنگاه $muk+nvk=b-a$. مانند برهان لم ۱.۱۳ ادامه دهید.

بخش ۲.۱۳، صفحه ۴۹۳

۳. در $\mathbb{Z}_۲ \times \mathbb{Z}_۵$، ۷، $(۱,۲)$ است و ۸، $(۲,۳)$ می‌باشد. بنابراین حاصل‌ضرب عبارت است از $(۲,۱)=(۱۰۲,۲۰۳)$.

۵. (⇐) اگر $f(r)=f(s)$، آنگاه r و s هر دو جواب‌های دستگاه $x \equiv r \ (m_۱)$ (پیمانه $m_۱$)، $x \equiv r \ (m_۲)$ (پیمانه $m_۲$)، ...، $x \equiv r \ (m_r)$ (پیمانه m_r) می‌باشد.

بخش ۳.۱۳، صفحه ۴۹۸

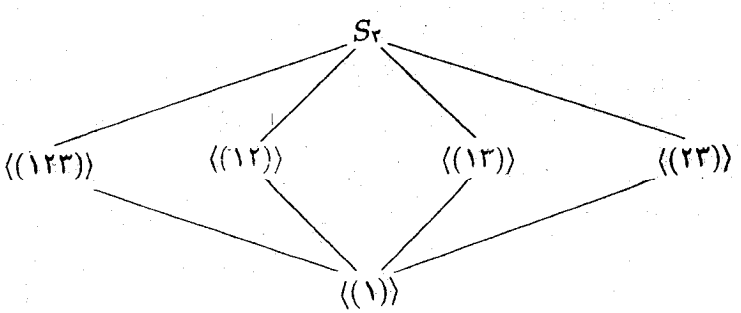
۱. (الف) استفاده مکرر از نتیجه ۶.۱۳ نشان می‌دهد که هر دو یکریختند با $\mathbb{Z}_۲ \times \mathbb{Z}_۴ \times \mathbb{Z}_۵$ و از اینرو با یکدیگر یکریختند.

بخش ۱.۱۴، صفحه ۵۱۰

۱. (الف) برهان داده شده در مثال ۴.۱۴ نیز در اینجا بکار می‌آید.

۳. پاد متقارن نیست (۳ و ۳− را در نظر بگیرید).

۷.



۱۵. در مجموعه P از اعداد صحیح مثبت که با بخش‌پذیری مرتب شده است، طبق تمرینهای ۱۰ و ۱۴، کوچکترین کران بالای یک مجموعه کوچکترین مضرب مشترک اعداد صحیح این مجموعه است. زیرمجموعه اعداد اول را در نظر بگیرید.

۱۷. (الف) طبق تعریف g.l.b. و l.u.b. داریم $a \wedge b \leq a$ و $a \wedge b \leq b \leq b \vee c$ و بنابراین $a \wedge b \leq a \wedge (b \vee c)$. به طور مشابه $a \wedge c \leq a \wedge (b \vee c)$. بنابراین $a \wedge (b \vee c)$ یک کران بالای $a \wedge b$ و $a \wedge c$ است، و لذا $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$.

۲۱. $\mathbb{Z}$ یک دامنه ایده‌آل اصلی است و $(c) \subseteq (a)$ اگر و تنها اگر $c|a$ (بخش ۲.۸ را نگاه کنید).

۲۵. (الف) ۱ تنها عضو مینیمال P است. هیچ عضو ماکسیمال وجود ندارد زیرا هیچ عدد صحیح مثبت وجود ندارد که بر تمام اعداد صحیح مثبت بخش‌پذیر باشد. (پ) جواب‌های صحیح زیادی وجود دارد، مجموعه S تمرین ۱ را بحساب آورید.

بخش ۲.۱۴، صفحه ۵۲۵

۱. اگر I و J هر دو بزرگترین عضو باشند، آنگاه $I \leq J$ زیرا J بزرگترین عضو است و $J \leq I$ زیرا I بزرگترین عضو است. پس $I = J$.

۳. c.

۵. نشان دهید که اگر $mn = ۱۰۵$، آنگاه n مکمل m است (یعنی، $[m,n] = ۱۰۵$ و $(m,n) = ۱$). توجه کنید که $۱۰۵ = ۳ \times ۵ \times ۷$.

۹. چون برای هر a، $a = O \vee a$ و طبق تعریف $O \vee O' = I$، لذا $O' = O \vee O' = I$.

۱۳. باید نشان دهید که برای هر عدد صحیح a، b، c، $[a,(b,c)] = ([a,b],[a,c])$. طبق تمرین ۱۱ بخش ۳.۱ کافی است حالتی را در نظر بگیریم که p عددی اول است و $a = p^r$، $b = p^s$، $c = p^t$. شش حالت پیش می‌آید ($r \leq s \leq t$، $s \leq t \leq r$ و غیره). مثلاً، در حالت اول $[a,(b,c)] = \max(r, \min(s,t)) = s$ و $([a,b],[a,c]) = \min(\max(r,s), \max(r,t)) = s$.

۱۷. با استفاده مکرر از قوانین دمورگان و قوانین توزیع‌پذیری داریم،

$((a \wedge b') \vee (a' \wedge b))' = (a \wedge b')' \wedge (a' \wedge b)' = (a' \vee b'') \wedge (a'' \vee b') =$
$\wedge a) \vee ((a' \vee b)(a' \vee b) \wedge (a \vee b') = ((a' \vee b) \wedge b') =$
$((a' \wedge a) \vee (b \wedge a) \vee (a' \wedge b') \vee (b \wedge b') = (o \vee (b \wedge a)) \vee ((a' \wedge b') \vee o) =$
$(b \wedge a) \vee (a' \wedge b') = (a \wedge b) \vee (a' \wedge b')$.

۲۱. (⇒) چون $O \leq a \wedge b \leq a$ و O یک اتم است، باید داشته باشیم $a \wedge b = O$ یا $a \wedge b = a$.

۲۳. (⇐) اگر $A = \{c\}$، آنگاه تنها زیرمجموعه‌های آن $\emptyset$ و A می‌باشد. از اینرو $\emptyset \subsetneqq B \subsetneqq A$ ناممکن است و A یک اتم است.

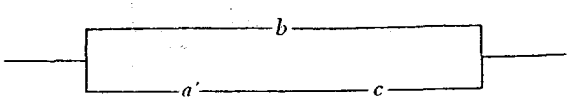
بخش ۳.۱۴، صفحه ۵۳۸

۱. (الف) $p \wedge p'$.

۳. (الف) از قضیه ۶.۱۴ استفاده کنید.
(پ)

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

۹.



فصل ۱۵، صفحه ۵۵۳

۳. (الف) مثل آنچه در ترسیم صفحه مختصات آمده‌است شروع کنید. سوزن پرگار را روی $(۱,۰)$ بگذارید و دایره‌ای رسم کنید که شعاعش برابر طول پاره خط بین $(۱,۰)$ و $(۳,۰)$ باشد. این دایره محور قائم را در Q قطع می‌کند. مثلث قائم‌الزاویه‌ای که رأس‌های آن $(۰,۰)$، Q و $(۱,۰)$ است دارای وتر به طول ۲ و یک ضلع ۱ است. پس طبق یک قضیه معروف هندسه زاویه Q (مقابل ضلع ۱) یک زاویه ۳۰° است. (پ) قسمت (الف) نشان می‌دهد که یک زاویه ۹۰° را می‌توان به سه قسمت تقسیم کرد. چون یک زاویه ۳۰° را می‌توان به دو قسمت تقسیم کرد، یک زاویه ۴۵° را می‌توان به سه قسمت تقسیم کرد.

۵.

$$\cos ۳t = \cos(t + ۲t) = \cos t \cos ۲t - \sin t \sin ۲t$$
$$= \cos t(۲\cos^۲ t - ۱) - \sin t(۲ \sin t \cos t) = ۲\cos^۳ t - \cos t - ۲\sin^۲ t \cos t$$
$$= ۲\cos^۳ t - \cos t - ۲(۱ - \cos^۲ t)\cos t = ۳\cos^۳ t - ۳\cos t.$$

۷. خیر. برای اثبات این مطلب نشان دهید که x باید ریشه یک چندجمله‌ای درجه سوم در $\mathbb{Q}[x]$ باشد که ریشه گویا ندارد.

۱۵. اگر $\sqrt{k} \in \mathbb{F}$، آنگاه $\mathbb{F}(\sqrt{k}) = \mathbb{F}$. اگر $\sqrt{k} \notin \mathbb{F}$، آنگاه وارون ضربی یک عضو ناصفر $a + b\sqrt{k}$ از $\mathbb{F}(\sqrt{k})$ برابر است با $c + d\sqrt{k}$ که در آن $c = a/(a^۲ - kb^۲)$ و $d = -b/(a^۲ - kb^۲)$.

بخش ۱.۱۶، صفحه ۵۶۸

۱. تحقیق کنید که C تحت جمع بسته است و طبق قضیه ۸.۷ یک زیرگروه است.

۳. (الف) ۱ (پ) ۴.

۵. (الف) ۰۰۰۰، ۱۰۰۰، ۰۱۱۱، ۱۱۱۱ (پ) ۰۰۰۰، ۰۰۱۰، ۰۱۰۱، ۰۱۱۱، ۱۰۰۱، ۱۰۱۱، ۱۱۰۰، ۱۱۱۰.

۱۱. (پ) اگر مولفه i ام با یک زیرنویس نشان داده شود، آنگاه $(u + w)_i = u_i + w_i$ و $(v + w)_i = v_i + w_i$.

۱۷. پاسخ‌های صحیح زیادی وجود دارد، از جمله ۰۰۰۰۰، ۱۱۱۰۰، ۰۰۱۱۱، ۱۱۰۱۱.

۲۱. $n = 5$.

۲۵. تحقیق کنید که یک عنصر $B(n)$ دارای وزن هامینگ زوج است اگر و تنها اگر این عنصر مجموع تعداد زوجی از عناصر به وزن هامینگ ۱ باشد. (برای مثال، ۱۰۰ + ۰۱۰ = ۱۱۰). از این مطلب استفاده کنید تا نشان دهید که مجموعه عناصر به وزن هامینگ زوج تحت جمع بسته است.

۲۷. (الف) ۰٫۹۶۰۵۹۶۰۱ (پ) ۰٫۰۰۰۵۸۸۰۶ (ث) ۰٫۰۰۰۰۰۰۰۱.

بخش ۲.۱۶، صفحه ۵۸۲

۱. (الف) $\begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$ (پ) $\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$

۳. $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$

۵. جوابهای ممکن گوناگون وجود دارد، از جمله

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

۱۳. یک خطا کشف می‌شود اگر و تنها اگر w یک کلمه کد نباشد. توجه کنید که $w = u + e$ و این که مجموعه کلمه کدها تحت جمع بسته است.

بخش ۳.۱۶، صفحه ۵۹۲

۱. (الف) اگر $f(x) = a_n x^n + \cdots + a_i x^i + \cdots + a_0$، آنگاه

$$f(x) + f(x) = (a_n + a_n)x^n + \cdots + (a_i + a_i)x^i + \cdots + (a_0 + a_0)$$
$$= 0x^n + \cdots + 0x^i + \cdots + 0$$

زیرا برای هر $a_i \in \mathbb{Z}_2$، $a_i + a_i = 0$.

۳. تحقیق کنید که $1 + x + x^4$ در $\mathbb{Z}_2$ هیچ ریشه‌ای ندارد و بنابراین دارای هیچ عامل درجه اول یا سوم نمی‌باشد. اگر یک عامل درجه دوم داشته باشد، این عامل یا حاصل‌ضرب دو عامل خطی است یا تحویل‌ناپذیر است. از تقسیم استفاده کنید تا نشان دهید که تنها چندجمله‌ای درجه دوم تحویل‌ناپذیر (تمرین ۲) یک عامل نیست.

۵. (الف) از جدول استفاده کنید تا نشان دهید که α^3 یک ریشه $f(x) = 1 + x + x^2 + x^3 + x^4$ است. پس در این صورت کافی است نشان دهیم که $f(x)$ تحویل‌ناپذیر است. از روش تمرین ۳ استفاده کنید.

۷. (پ) اگر $f([a_0 + a_1x + \cdots + a_{n-1}x^{n-1}]) = (0, 0, \ldots, 0)$، آنگاه

$$[a_0 + a_1x + \cdots + a_{n-1}x^{n-1}] = [0]$$

لذا، هستهٔ f زیرگروه همانی است، از قضیه ۲۷.۷ استفاده کنید.

۹. (الف) چندجمله‌ای $D(x) = x^2 + \alpha^4x + \alpha$ دارای ریشه‌های $\alpha = \alpha^1$ و $1 = \alpha^0$ است، بنابراین ۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰ کلمه صحیح می‌باشد. (پ) $D(x) = x^2 + \alpha^{13}x + \alpha^4$ دارای ریشه‌های α^9 و α^{10} است از اینرو ۱۰۱۰۱۰۰۱۰۱۱۰۰۰۰ کلمه صحیح می‌باشد.

پیوست ب، صفحه ۶۲۵

۱. (الف) $\{-2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$ (پ) $\{1, 2\}$.

۲. (الف) چون $\sqrt{2}$ اصم است تهی می‌باشد. (پ) تهی است.

۷. $(a, 0)$، $(a, 1)$، $(b, 0)$، $(b, 1)$، (b, c)، $(c, 0)$، $(c, 1)$، (c, c).

۱۱. (الف) بلی (پ) بلی

۱۳. (الف) جوابهای صحیح متعددی وجود دارد، از آن جمله توابع f، g، h که به صورت زیر داده شده‌اند $f(1) = a$، $f(2) = b$، $f(3) = c$، $f(4) = a$؛ $g(1) = c$، $g(2) = b$، $g(3) = a$، $g(4) = b$؛ $h(1) = b$، $h(2) = a$، $h(3) = c$، $h(4) = c$؛ $k(1) = c$، $k(2) = a$، $k(3) = a$، $k(4) = b$.

(پ) شش نگاشت دوسویی از C به C وجود دارد.

۱۹. اگر $(a, d) \in A \times (B \cup C)$، آنگاه $a \in A$ و $d \in B$ یا $d \in C$. بنابراین $(a, d) A \times B$ یا $(a, d) \in A \times C$ و بدین دلیل $(a, d) \in (A \times B) \cup (A \times C)$. پس $A \times (B \cup C) \subseteq$ $(A \times B) \cup (A \times c)$. برعکس، فرض کنید $(r, s) \in (A \times B) \cup (A \times C)$. آنگاه $(r, s) \in A \times B$ یا $(r, s) \in A \times C$. اگر $(r, s) \in A \times B$، آنگاه $r \in A$ و $s \in B$ (و لذا $s \in B \cup C$)، در نتیجه $(r, s) \in A \times (B \cup C)$. به طور مشابه، اگر $(r, s) \in A \times C$، آنگاه $(r, s) \in A \times (B \cup C)$. بنابراین $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$، و لذا دو مجموعه برابرند.

۲۳. خیر؛ چرا نه؟

۲۵. (الف) اگر $f(a) = f(b)$، آنگاه $2a = 2b$، از تقسیم طرفین بر ۲ ثابت می‌شود که $a = b$. بنابراین f یک به یک است.

(پ) اگر $f(a) = f(b)$، آنگاه $a/v = b/v$، که ایجاب می‌کند $a = b$.

۲۷. (الف) اگر $(g \circ f)(a) = (g \circ f)(b)$، آنگاه $g(f(a)) = g(f(b))$. چون g یک به یک است، $f(a) = f(b)$. این ایجاب می‌کند که $a = b$ زیرا f یک به یک است. بنابراین $g \circ f$ یک به یک است.

۲۹. (الف) گیریم $d \in D$. چون $g \circ f$ پوشاست، $b \in B$ وجود دارد به طوری که $(g \circ f)(b) = d$. گیریم $c = f(b) \in C$ آنگاه $g(f(b)) = (g \circ f)(b) = d$. از اینرو g پوشاست.

پیوست پ، صفحه ۶۳۸

۱. $P(0)$ درست است زیرا $0(0+1)/2 = 0$. اگر $P(k)$ درست باشد، آنگاه $1 + 2 + \cdots + k = k(k+1)/2$. این مطلب درستی $P(k+1)$ را بیان می‌کند.

۳. گیریم $P(n)$ گزاره $n! \leq 2^{n-1}$ باشد. تحقیق کنید که $P(0)$ و $P(1)$ درست است اگر $P(k)$ درست باشد و $k \geq 1$، آنگاه $k! \leq 2^{k-1}$ و $2 \leq k+1$. لذا $(k+1)!2^{k-1} \times 2 \leq 2^{k-1}$. یعنی $(k+1)! \leq 2^k$ پس $P(k+1)$ درست است.

۷. فرض کنید که گزاره برای k درست باشد، یعنی، این که ۳ عاملی از $2^{2k+1} + 1$ است. در این صورت $2^{2k+1} + 1 = 3t$، و از اینرو $2^{2k+1} = 3t - 1$. برای این که نشان دهیم گزاره برای $k+1$ درست است، توجه کنید که

$$2^{2(k+1)+1} - 1 = 2^{2k+2+1} - 1 = 2^{2k+1} \times 2^2 - 1 = (3t-1)4 - 1 = 12t - 4 - 1 = 3(4t-1)$$

و لذا $2^{2(k+1)+1} + 1 = 3(4t-1)$.

۱۱. گیریم $B = \{b_1, b_2, \ldots, b_n\}$. برای تعریف یک تابع یک به یک از B به B، برای تصویر b_1، n انتخاب ممکن وجود دارد، $n-1$ انتخاب ممکن برای تصویر b_2 وجود دارد (زیرا b_2 نمی‌تواند همان تصویر b_1 را داشته باشد)، $n-2$ انتخاب برای تصویر b_3، و همین‌طور الی آخر.

۱۳. (الف) فرض کنید که هر مجموعه k عضوی دارای $k(k-1)/2$ زیرمجموعه دو عضوی است و این که B دارای $k+1$ عضو است. $b \in B$ را انتخاب کنید و بگیرید $C = B - \{b\}$. هر زیرمجموعه دوعضوی B یا شامل دو عضو از C است یا شامل b و یک عضو از C است. طبق فرض استقراء، تعداد $k(k-1)/2$ زیرمجموعه از نمونه اول وجود دارد.

پیوست ت، صفحه ۶۴۷

۳. (الف) $a \sim a$ زیرا $\cos a = \cos a$. اگر $a \sim b$، آنگا $\cos a = \cos b$. طبق خاصیت تقارنی $\cos b = \cos a$؛ لذا $b \sim a$. اگر $a \sim b$ و $b \sim c$، آنگاه $\cos a = \cos b$ و $\cos b = \cos c$. لذا $\cos a = \cos c$، و بنابراین $a \sim c$.

۵. (ب) رده هم‌ارزی (r,s) خط قائم گذرنده از (r,s) است.

۹. (الف) متعدی (پ) متقارن.

۱۹. (ب) زیرگروه $K = \{r_0, v\}$ از D_4 را در نظر بگیرید.

پیوست ث، صفحه ۶۵۴

۱. ۴۰۳۲

۳.

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n!}{(n-(n-r))!(n-r)!} = \binom{n}{n-r}$$

پیوست ج، صفحه ۶۶۲

۱. (الف) $$A + B = \begin{pmatrix} ۱ & -۶ & ۰ & ۴ \\ ۹ & ۵ & ۱۱ & ۱۲ \end{pmatrix}$$

۳. (الف) درایه ij–ام ماتریس $A+B$ برابر $a_{ij}+b_{ij}$ است. ولی $a_{ij}+b_{ij} = b_{ij}+a_{ij}$، که درایه ij–ام ماتریس $B+A$ است. لذا $A+B = B+A$.

پیوست چ، صفحه ۶۷۳

۱. (الف) $x + x^۳ + x^۵$ (پ) $(\ldots, ۰, ۰, ۰, ۳, ۰, -۵, ۱۲, -۳, ۵, ۷, -۱۱)$.

۳. (الف)

$$\begin{aligned}
&[(a_۰, a_۱, \ldots) \oplus (b_۰, b_۱, \ldots)] \oplus (c_۰, c_۱, \ldots)\\
=&(a_۰ + b_۰, a_۱ + b_۱, \ldots) \oplus (c_۰, c_۱, \ldots)\\
=&(a_۰ + b_۰) + c_۰, (a_۱ + b_۱) + c_۱, \ldots)\\
=&(a_۰ + (b_۰ + c_۰), a_۱ + (b_۱ + c_۱), \ldots)\\
=&(a_۰, a_۱, \ldots) \oplus [(b_۰, b_۱, \ldots) \oplus (c_۰, c_۱, \ldots)].
\end{aligned}$$

* * * * *

کتاب نامه

فهرست زیر مشتمل بر کلیه کتابها و مقالاتی است که در متن کتاب به آنها ارجاع داده شده است. به‌علاوه تعدادی مراجع دیگر نیز، که برای مطالعه جانبی و بررسی عمیق‌تر پاره‌ای مباحث لازم می‌باشد، آمده است. دلیل عمده انتخاب این مراجع سهل الوصول بودن مطالب آن برای دانشجویان می‌باشد. البته این فهرست به هیچ وجه کامل نیست.

برای هر کس که بتواند این کتاب را شروع کند هفده مرجع اول کتاب‌نامه (به استثنای مراجع [7]، [8] و [16]) قابل فهم است. برای خواندن بقیه مراجع دانستن قسمتهایی از این کتاب ضرورت دارد.

جبرد مجرد، به طور عام (در سطح کارشناسی) **Abstract Algebra in General (Undergraduate Level)**

منابع ارائه شده در این قسمت، تقریباً همان مطالب فصل‌های ۱ تا ۱۱ کتاب را شامل می‌شود، گر چه که هر یک از آنها از دیدگاه خاص خود به موضوعات پرداخته است. تنها مراجع [1] و [4] همپوشانی نسبتاً زیادی با فصلهای ۱۲ تا ۱۶ دارد. اغلب این مراجع موضوعاتی مانند جبر خطی و برخی مباحث دیگر را شامل می‌باشد که در این کتاب به آن پرداخته نشده است.

[1] Birkhoff, G., and S. Mac Lane, A Survey of Modern Algebra, 4th edition, New York: Macmillan, 1977.

[2] Burton, D. M., Abstract Algebra, Dbuque, Iowa:Wm. C. Brown, 1988.

[3] Fraleigh, J., A First Course in Abstract Algebra, 4th edition, Reading, Mass.: Addison-Wesley, 1989.

[4] Gallian, J., Contemporary Abstract Algebra, Lexington, Mass: Heath, 1986.

[5] Herstein, I. N., Topics in Algebra, 2nd edition. Lexington, Mass: Xerox publishing, 1975.

[6] McCoy, N., and T. Berger, Algebra: Groups, Rings, and Other Topics, Boston: Allyn and Bacon, 1977.

Abstract Algebra in General (جبر مجرد بطور عام)

(Graduate Level) (در سطح کارشناسی‌ارشد)

مراجع این قسمت، موضوعات فصل‌های ۱ تا ۱۱ را به صورت خیلی عمیق‌تری ازکتاب پوشش می‌دهد، بعلاوه موضوعات زیاد دیگری را هم که این کتاب به آن نپرداخته است شامل می شود.

[7] Hungerford, T. W., Algebra, New York: Springer-Verlag, 1974.

[8] Jacobson, N., Basic Algebra I, 2nd edition, and Basic Algebra II, San Francisco: Freeman, 1985 and 1980.

Logic, Proof, and Set Theory منطق، برهان، و نظریهٔ مجموعه‌ها

[9] Halmos, P., Naive Set Theory, New York: Springer-Verlag, 1974.

[10] Lucas, J., Introduction to Abstract Mathematics, New York: Ardsley, 1986.

[11] Morash, R., Bridge to Abstract Mathematics, New York: Random House, 1987.

[12] Smith, D., M. Eggen, and R. St. Andre, A Transition to Advanced Mathematics, 2nd edition. Monterey, Cal.: Brooks/Cole, 1986.

[13] Solow, D., How To Read and Do Proofs, 2nd edition. New York: Wiley, 1990.

Number Theory نظریه‌اعداد

[14] Burton, D. M., Elementary Number Theory, Boston: Allyn and Bacon, 1980.

[15] Dudley, U., Elementary Number Theory, 2nd edition. San Francisco: Freeman, 1978.

[16] Ireland, K., and M. Rosen, A Classical Introduction to Modern Number Theory, New York: Springer-Verlag, 1982.

[17] Rosen, K. H., Elementary Number Theory and Its Applications, 2nd edition Reading, Mass: Addison-Wesley, 1988.

Rings حلقه‌ها

[18] Herstein, I. N., Noncommutative Rings, Carus Monograph 15. Washington, D.C.: Mathematical Association of America, 1968.

[19] Kaplansky, I., Commutative Rings, revised edition. Chicago: University of Chicago Press, 1974.

[20] McCoy, N., Rings and Ideals, Carus Monograph 8. Washington, D.C.: Mathematical Association of America, 1948.

[21] Robinson, A., Numbers and Ideals, San Francisco: Holden-Day, 1965.

[22] Stark, H., "A Complete Determination of Complex Quadratic Fields of Class Number One," Michigan Mathamtical Journal, 14(1967), pp. 1-27.

[23] Wilson, J. C., "A Principal Ideal Domain That Is Not a Euclidean Ring," Mathematics Magazine, 46(1973), pp. 74–78.

Groups **گروهها**

[24] Gallian, J., "The Search for Finite Simple Groups," Mathematics Magazine, 49(1976), pp. 163-179.

[25] Kaplansky, I., Infinite Abelian Groups, 2nd edition. Ann Arbor, Mich: University of Michigan Press, 1969.

[26] Rotman, J., An Introduction to the Theory of Groups, 3rd edition. Boston: Allyn and Bacon, 1984.

[27] Steen, L. A., "A Monstrous Piece of Research," Science News, 118(1980) pp. 204-206.

Fields and Galois Theory **میدانها و نظریه گالوا**

[28] Gaal, L., Classical Galois Theory with Examples, 4th edition. New York: Chelsea, 1988.

[29] Hadlock, C. R., Field Theory and Its Classical Problems, Carus Monograph 19. Washington, D.C.: Mathematical Association of America, 1978.

[30] Kaplansky, I., Fields and Rings, revised 2nd edition. Chicago: University of Chicago Press, 1972.

[31] Niven, I., Irrational Numbers, Carus Monograph 11. Washington, D.C.: Mathematical Association of America, 1956.

Applied Algebra and Computer Science جبر کاربردی و علم کامپیوتر

[32] Childs, L., A Concrete Introduction to Higher Algebra, New York: Springer-Verlag., 1979.

[33] Knuth, D.E., The Art of Computer Programming: Seminumerical Algorithms, Vol. 2, 2nd edition. Reading, Mass.: Addison-Wesley, 1981.

[34] Lidl. R., and G. Pilz, Applied Abstract Algebra, New York: Springer-Verlag., 1984.

[35] Mackiw, G., Applications of Abstract Algebra, New York: Wiley, 1985.

Cryptography رمزنویسی

[36] DeMillo, R. A., G. Davida, et al., Applied Cryptology, Cryptographic Protocols, and Computer Security Models, Proceedings of Symposia in Applied Mathematics, Vol. 29, Providence, R. I.: American Mathematical Society, 1983.

[37] Diffie, W., and M. Hellman, "Privacy and Authentication: An Introduction to Cryptography," Proc. of the IEEE, 67(1979), pp. 297-427.

[38] Rivest, R. L., A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the A.C.M., 21 (1978), pp. 120-126.

[39] Simmons, G. J., "Cryptology: The Mathematics of Secure Communication," Mathematical Intelligencer, 1(1979), pp. 233-246.

Lattices and Boolean Algrbra مشبکه‌ها و جبرهای بولی

[40] Abbott, J. C., Sets, Lattices, and Boolean Algebras, Boston: Allyn and Bacon, 1969.

[41] Birkhoff, G., Lattice Theory, Providence, R. I.: American Mathematical Society, 1967.

[42] Hohn, F. E., Applied Boolean Algebra, 2nd edition. New York: Macmillan, 1966.

[43] — , "Some Mathamtical Aspects of Switching," American Mathematical Monthly, 62(1955), pp. 75-90.

[44] Stone, M. H., "The Theory of Representations of Boolean Algebras," Transactions of the American Mathematical Society, 40(1936), pp.37-111.

Algebraic Coding Theory نظریه کدگذاری جبری

[45] Berlekamp, E., Algebraic Coding Theory, New York: McGraw-Hill, 1968.

[46] MacWilliams, F. J., and N. J. A. Sloane, The Theory of Error-Correcting Codes, Amsterdam: North-Holland, 1977.

[47] Peterson, W. W., and E. J. Weldon, Jr., Error-Correcting Codes, 2nd edition. Cambridge, Mass.: MIT Press, 1972.

History تاریخ ریاضیات

[48] Boyer, C., A History of Mathematics, Princeton, N.J.: Princeton University Press, 1985.

[49] Burton, D., The History of Mathematics: An Introduction, Boston: Allyn and Bacon, 1985.

[50] Eves, H., An Introduction to the History of Mathematics, 5th edition. Philadelphia: Saunders College Publishing, 1983.

[51] Van der Waerden, B. L., A History of Algebra: From Al-Khowarizmi to Emmy Noether, New York: Springer-Verlag, 1985.

❋ ❋ ❋ ❋ ❋

واژه‌نامه انگلیسی به فارسی

Abel	آبل
Abelian group	گروه آبلی
absorption	جـذب
absorption law	قانون جذب
abstract algebra	جبر مجرد
abstraction	مجردسازی، تجرید
additive	جمعی
adjoining an element	اتصال (الحاق) یک عنصر
algebra	جبر
algebraic	جبری
algbraic closure	بستار جبری
algbraic element	عنصر جبری
algebraically closed	بسته جبری

algorithm	الگوریتم
alternating group	گروه تناوبی
antisymmetric	پادمتقارن
arithmetic	حساب
ascending chain	زنجیر صعودی (فزآینده)
ascending chain condition	شرط زنجیر صعودی
associate	وابسته
associative law	قانون شرکت‌پذیری
associativity	شرکت‌پذیری
atom	اتم
automorphism	خودریختی
axiom	اصل موضوع
base=basis	پایه، مبنا
biconditional statement	گزاره دو شرطی
bijection	دوسویی
bijective function	تابع دوسویی
binary	دوتایی
binomial	دوجمله‌ای
binomial theorem	قضیه دوجمله‌ای
block	بلوک
Boole	بـول
Boolean algebra	جبر بولی
Boolean ring	حلقه بولی
bound	کران
cancelation law (=rule)	قانون (قاعده) حذف
Cartesian product	حاصل‌ضرب دکارتی
Cauchy's Theorem	قضیه کشی

Cayley's Theorem	قضیه کیلی
center	مرکز
centralizer	مرکزساز
chain	زنجیر
characteristic	مشخصه
characteristic subgorup	زیرگروه مشخصه
check digits	ارقام کنترل
Chinese Remainder Theorem	قضیه باقیمانده چینی
circle	دایره
circuit	مدار
class	کلاس ـ رده
class equation	معادله رده‌ای
classification of finite groups	رده‌بندی گروههای متناهی
closed	بسته
closure	بستار
code	کد ـ رمز
codeword	کلمه کد
coding theory	نظریه کدگذاری
coefficient	ضریب
column vector	بردار ستونی
combination	ترکیب
combinatorial mathematics=combinatorics	ریاضیات ترکیبیاتی، ترکیبیات
common divisor	شمارنده مشترک
commutative	جابجایی ـ تعویض‌پذیر
commutator subgroup	زیرگروه جابجاگر
compass	پرگار
complement	مکمل ـ متمم

complementary modular lattice	مشبکه مدولی متممدار
complete lattice	مشبکه کامل
complete induction	استقراء کامل
complex	مختلط
composite function	تابع ترکیب
composition factor	عامل ترکیب
compound statment	گزاره مرکب
computer arithmetic	حساب رایانه
conditional statement	گزاره شرطی
congruence	همنهشتی
congruent modulo n	همنهشت به پیمانه n
conjugacy	مزدوجی
canjugate	مزدوج
constant polynomial	چندجمله‌ای ثابت
constructible	ترسیم شدنی ـ ساخت‌پذیر
construction	ساختار
converse	وارون ـ معکوس
converse of a theorem	عکس یک قضیه
contradiction	تناقض
contrapositive	عکس نقیض
corollary	نتیجه
correspondence	تناظر
coset	هم‌مجموعه
counter example	مثال نقض
cryptography	رمزنگاری
cube duplication	دوبرابرسازی مکعب
cubic equation	معادلهٔ درجهٔ سه

cycle(s)	دور(ها)
cyclic group	گروه دوری
cyclic permutation	جایگشت دوری
decoding	کدگشایی
decompsition	تجزیه
Dedekind	ددکیند
degree	درجه
De Moiver formula	فرمول دمواور
De Morgan's laws	قوانین دمورگان
dependent	وابسته
derivative	مشتق
designed distance	فاصله طراحی شده
determinant	دترمینان
diagonal matrix	ماتریس قطری
dihedral group	گروه دو وجهی
dimension	بعد
direct product	ضرب مستقیم
direct proof	برهان مستقیم
direct sum	جمع مستقیم
disjoint	مجزا
distance	فاصله
distributive law	قانون توزیع‌پذیری
divides	می‌شمارد
division algorithm	الگوریتم تقسیم
division ring	حلقه تقسیمی
divisor	شمارنده
domain	دامنه

duality	دوگانی
duplication of the cube	دوبرابرسازی مکعب
Eisenstein's Criterion	معیار ایزنشتاین
element	عنصر ـ عضو
elementary divisor	شمارنده مقدماتی
empty set	مجموعه تهی
epimorphism	برووریختی
equality	برابری، تساوی
equation	معادله، برابری
equivalence	هم‌ارزی
equivalent statements	گزاره‌های هم‌ارز
Euclidean algorithm	الگوریتم اقلیدسی
Euler ϕ – function	تابع ϕ–اویلر
Euler's Theorem	قضیه اویلر
evaluation homomorphism	همریختی ارزشی
even	زوج
existential quantifier	سور وجودی
exponent notation	نماد نمایی
extension	توسیع
external direct product	حاصل‌ضرب مستقیم خارجی
factor	عامل ـ سازه
factorization	تجزیه (به عامل‌ها)، عاملگیری
Fermat	فرما
field(s)	میدان(ها)
finite	متناهی ـ با پایان
finite field	میدان متناهی
finite group	گروه متناهی

finitely generated	با مولد متناهی
First Isomorphism Theorem	قضیه اول یکریختی
First Sylow Theorem	قضیه اول سیلو
fixed field	میدان ثابت
formal logic	منطق صوری
formula	فرمول، دستور
formulation	فرمولبندی
forward-backward technieque	شگرد جلو ـ عقب
Four-Color Theorem	قضیه چهار ـ رنگ
four-group=(Klein) four-group	چهار ـ گروه (کلاین)
fraction	کسر
Freshman's Dream	رویای سال‌اولی‌ها
function	تابع
Fundamental Theorem	قضیه اساسی
Galois	گالوا
Galois extension	توسیع گالوا
Galois group	گروه گالوا
Golois theory	نظریه گالوا
Gauss	گاوس
Gaussian integers=complex integers	اعداد گاوسی
general linear group	گروه خطی عام
generalization	تعمیم
generator	مولد
generators and relations	مولدها و روابط
greatest	بزرگترین
greatest common divisor=greatest common factor	بزرگترین مقسوم‌علیه مشترک، بزرگترین عامل مشترک

group automorphisms	گروه خودریختی‌ها
group of motions	گروه حرکتها
group(s)	گروه(ها)
Hamming weight	وزن هامینگ
homomorphic image	تصویر همریختی
homomorphism	همریختی
hypothesis	فرض
ideal=two-sided ideal	ایده‌ال(ها)
idempotent	خودتوان
identity	همانی
identity function=identity mapping	تابع همانی، نگاشت همانی
if and only if	اگر و تنها اگر، اگر و فقط اگر
implication	استلزام
inclusion	شمول، جزئیت
inclusion mapping	نگاشت شمول
inclusion relation	رابطه شمول
inclusive or	یای منطقی
image	تصویر
indecomposable group	گروه تجزیه‌ناپذیر
independent	مستقل
indeterminate	مجهول ـ متغیر
index	نمایه ـ اندیس ـ شاخص
index of a subgroup	شاخص یک زیرگروه
induction	استقراء
inequality	نامعادله، نابرابری
infimum	اینفیمم
infinite	نامتناهی ـ بی‌پایان

infinite set	مجموعه نامتناهی
information theory	نظریه اطلاعات
injective function	تابع یک به یک
injective mapping=injection=one-to -one mapping	نگاشت یک به یک
injective	یک به یک
inner automorphism	خودریختی داخلی
inner product	(حاصل) ضرب داخلی
integer	عدد صحیح
integral domain	دامنه صحیح
intermediate field	میدان میانی
internal direct product	حاصل‌ضرب مستقیم‌داخلی
intersection	اشتراک، مقطع
invariant factor	عامل پایا ـ سازه پایا
inverse	وارون ـ معکوس
invertible matrix	ماتریس وارون‌پذیر
irreducibility	تحویل‌ناپذیری
irreducible	تحویل‌ناپذیر
isolated set	مجموعه تنها
isomorphic	یکریخت
isomorphism	یکریختی
join	وَست ـ پیوند
join of elements in a lattice	وست عنصرها در یک مشبکه
Kernel	هسته
kernel of a homomorphism	هستهٔ همریختی
Kronecker delta	دلتای کرونکر
label	نشان
Lagrange's Theorem	قضیه لاگرانژ

lattice	مشبکه
leading coefficient	ضریب پیشرو
least common multiple	کوچکترین مضرب مشترک
least residue	کوچکترین باقیمانده
least upper bound	کوچکترین کران بالا
left	چپ
left coset	هم‌مجموعهٔ چپ
Lemma	لم
length of cycle	طول یک دور
line (, constructible)	خط (ساخت‌پذیر)
linear	خطی
linearly dependent	وابسته خطی
linearly independent	مستقل خطی
linked switches	کلیدهای متصل
logic	منطق
logical equivalence	هم‌ارزی منطقی
logical inference	استنتاج منطقی
lower bound	کران پایین
l.u.b	ک‌ک‌ب (کوچکترین کران بالا)
map	نگاشت
mapping	نگاشت
mathematical induction	استقراء ریاضی
matrices	ماتریس‌ها
matrix	ماتریس.
maximal	بیشین ـ ماکسیمال
maximal element=maximal member	عنصر ماکسیمال، عضو ماکسیمال
maximum likelihood decoding	کدگشایی احتمال بیشین

meet	رسند ـ تلاقی
meet of elements in a lattice	رسند عنصرها در یک مشبکه
message word	کلمه پیام
metabelian group	گروه متاآبلی
minimal	مینیمال
minimal element=minimal member	عنصر مینیمال، عضو مینیمال
minimal polynomial	چندجمله‌ای مینیمال
minimum	مینیمم ـ کمینه
modulo	پیمانه
modular	مدولی
modus ponens	قیاس استثنایی
monic polynomial	چندجمله‌ای تکین
monomorphism	تکریختی
multiconditional statement	گزاره چندشرطی
multiplication	ضرب
multiplicative	ضربی
natural homomorphism	همریختی طبیعی
nearest-neighbor decoding	کدگشایی نزدیکترین همسایه
necessity	لزوم
negation	نفی
negative	منفی
nilpotent	پوچتوان
norm	نرم ـ اندازه
normal	نرمال
normalizer	نرمالساز
notation	نماد، نمادگذاری
null set	مجموعه تهی

number	عدد
number theory	نظریهٔ اعداد
object	شئ
odd permutation	جایگشت فرد
one-to-one	یک به یک
one-to-one correspondence	تناظر یک به یک
onto function	تابع پوشا(برو)
open circuit	مدار باز
oppositely linked switches	کلیدهای به طور مخالف مرتبط
orbit	مدار
order	مرتبه
ordering	ترتیب
pair	جفت
pairwise disjoint	دوبدو مجزا
$p-$ (sub)group	$p-$(زیر)گروه
parallel switches	کلیدهای موازی
parity-check	توازن سنج
partial order=partial ordering	ترتیب جزیی
partially ordered set	مجموعهٔ جزئاً مرتب
partition	افراز
Pascal's triangle	مثلث خیام-پاسکال
permutation	جایگشت
permutation group	گروه جایگشتها
phi-function	تابع $\phi-$
polynomials	چندجمله‌ای(ها)
polynomial equation	معادله چندجمله‌ای
polynomial function	تابع چندجمله‌ای

polynomial ring	حلقه چندجمله‌ای
positive integer	عدد صحیح مثبت
premise	مقدمه
primality testing	آزمون اول بودن
prime	اول
prime element of a ring	عنصر اول حلقه
prime field	میدان اول
prime number	عدد اول
primitive	اولیه
primitive polynomial	چندجمله‌ای اولیه
prinicpal ideal	ایده‌ال اصلی
principle	اصل
product	حاصل‌ضرب
process	فرآیند
proof	برهان
proper	سره
proper subgroup	زیرگروه سره
proposition	گزاره، قضیه
propositional calculus	حساب گزاره‌ها
public-key cryptography system	دستگاه رمزنگاری ـ کلید ـ عمومی
quadratic	درجه دوم
quadratic congruence	همنهشتی درجهٔ دوم
quantifier	سور
quaternion(s)	چهارگانی (چهارگانها)
quotient(s)	خارج‌قسمت (ها)
quotient group	گروه خارج قسمتی
quotient ring	حلقه خارج قسمتی

radius	شعاع
radius of a circle	شعاع دایره
radical	رادیکال
range of a function	برد یک تابع
rational	گویا
rational function	تابع گویا
rational number	عدد گویا
real	حقیقی
real number field	میدان اعداد حقیقی
reduced fraction	کسر ساده شده
received word	کلمه دریافتی
reducible polynomial	چندجمله‌ای تحویل‌پذیر
reflexive	انعکاسی
relation	رابطه
relaive complement	مکمل نسبی
relatively prime	نسبت به هم اول
remainder	باقیمانده
Remainder Theorem	قضیه باقیمانده
representation	نمایش
residue class	کلاس باقیمانده
right	راست
right angle	زاویه قائمه
right coset	هم‌مجموعه راست
ring(s)	حلقه(ها)
ring homomorphism	همریختی حلقه‌ای
ring isomorphism	یکریختی حلقه‌ای
ring theory	نظریه حلقه‌ها

root	ریشه
row vector	بردار سطری
RSA system	دستگاه RSA
rule	قاعده
ruler and compass constructions	ترسیم‌های با خطکش و پرگار
scheme	طـرح
second	دوم، دومین
section	بخش، مقطع
segment	قطعه
semicircle	نیمدایره
semidirect prodcut	حاصل‌ضرب نیمه‌مستقیم
separability	تفکیک‌پذیری
separable	تفکیک‌پذیر
separable extension	توسیع تفکیک‌پذیر
sequence	دنباله
series switches	کلیدهای سری
set(s)	مجموعه(ها)
set theory	نظریه مجموعه‌ها
side	ضلع، طرف
sieve of Erathosthenes	غربال اراتستن
simple	ساده
simple gorup	گروه ساده
size	اندازه
smallest element	کوچکترین عضو
solution	حل، جواب
solution of an equation	حل یک معادله، جواب یک معادله
solvable	حلپذیر

solvable group	گروه حل‌پذیر
span	پدیدآوردن
special linear group	گروه خطی خاص
splits	شکافته می‌شود
splitting field	میدان شکافنده
square	مربع، توان دوم
square root	ریشه دوم، جذر
square-free integer	عدد صحیح مربع ـ آزاد
squaring the circle	تربیع دایره ـ مربع‌سازی دایره
standard	استاندارد
straightedge	خط کش
statement	حکم، گزاره
statement caculus	حساب گزاره‌ها
subfield	زیرمیدان
subgroup	زیرگروه
subring	زیرحلقه
subset	زیرمجموعه
subtraction	تفریق
sum	جمع
supremum	سوپریمم
surjective	پوشا
Sylow theorems	قضایای سیلو
symmetric	متقارن
symmetric group	گروه متقارن
symmetries of the square	تقارن‌های مربع
syndrome decoding	کدگشائی مشخصه
system of linear congruences	دستگاه همنهشتی‌های خطی

systematic code	کد روش‌مند
switch	کلید
table	جدول
tautology	راستگو
technique	فن، تکنیک
term	جمله
thematic table of contents	جدول فهرست موضوعی
theorem	قضیه
torsion (sub)group	(زیر) گروه تابدار
totally ordered set	مجموعه کلاً مرتب
trial and error	آزمون و خطا
triangle	مثلث
transcendental element	عنصر متعالی
transposition	ترانهش
trisection of an angle	تثلیث زاویه
truth table	جدول راستی
union	اجتماع
union of sets	اجتماع مجموعه‌ها
unique factorization	یکتایی تجزیه
unique factorization domain	دامنه یکتایی تجزیه
unit	یکه
unity	واحد
universal quantifier	سور عمومی
upper bound	کران بالا
vector	بردار
weight (of a code)	وزن (یک کد)
Well-Ordering Axiom	اصل خوش‌ترتیبی

word size	اندازه کلمه
zero	صفر
zero divisor	مقسوم‌علیه‌صفر
zero element	عضو (عنصر) صفر
zero ideal	ایده‌ال صفر
zero matrix	ماتریس صفر
zero vector	بردار صفر

واژه‌نامه فارسی به انگلیسی

آبل	Abel
اتصال	adjoining
اتم	atom
اجتماع	union
اجتماع مجموعه‌ها	union of sets
ارقام کنترل	check digits
آزمون و خطا	trial and error
استقراء	induction
استقراء ریاضی	logical induction
استقراء کامل	complete induction
استلزام	implication
استنتاج ریاضی	logical infrence
استاندارد	standard

اشتراک	intersection
اصل	principal
اصل موضوع	axiom
اعداد گوسی	Gaussian integers=complex integers
اگر و تنها اگر، اگر و فقط اگر	if and only if
افراز	partition
الگوریتم	algorithm
الگوریتم اقلیدسی	Euclidean algorithm
الگوریتم تقسیم	division algorithm
اندازه	size
اندازه	norm
اندازه کلمه	word size
اندیس	index
انعکاسی	reflexive
اول	prime
اولیه	primitive
ایده‌ال(ها)	ideal(s)
ایده‌ال اصلی	principal ideal
اینفیمم	infimum
با پایان	finite
با مولد متناهی	finitely generated
برابری	equality
بردار	vector
بردار ستونی	column vector
بردار سطری	row vector
بردار صفر	zero vector
برد یک تابع	range of a function

greatest	بزرگترین
greatest common divisor	بزرگترین عامل مشترک
greatest common factor	بزرگترین مقسوم‌علیه مشترک
proof	برهان
direct proof	برهان مستقیم
epimorphism	بروریختی
section	بخش
closure	بستار
algebraic closure	بستار جبری
closed	بسته
algebraically closed	بسته جبری
dimension	بعد
block	بلوک
Boole	بول
maximal	بیشین
antisymmetric	پاد متقارن
base=basis	پایه
compass	پرکار
span	پدید آوردن
p-(sub) group	پی ـ (زیر) گروه
modulo	پیمانه
join	پیوند
nilpotent	پوچتوان
surjective	پوشا
function	تابع
onto function	تابع پوشا
composite function	تابع ترکیب

polynomial function	تابع چندجمله‌ای
bijective function	تابع دوسویی
rational function	تابع گویا
phi-function	تابع ـ فی (ϕ)
identity function	تابع همانی
one to one function=injective function	تابع یک به یک
transposition	ترانهش
squaring the circle	تربیع دایره
partial order=partial ordering	ترتیب جزیی
decomposition	تجزیه
factorization	تجزیه (به عامل‌ها)
irreducible	تحویل‌ناپذیر
irreduciblity	تحویل‌ناپذیری
constructible	ترسیم‌شدنی
ruler and compass construction	ترسیم‌های با خطکش و پرگار
combination	ترکیب
combinatorices	ترکیبیات
image	تصویر
homomorphic image	تصویر همریختی
generalization	تعمیم
commutative	تعویض‌پذیر
subtraction	تفریق
separable	تفکیک‌پذیر
separability	تفکیک‌پذیری
symmetries of square	تقارنهای مربع
monomorphism	تکریختی
technique	تکنیک

meet	تلاقی
correspondecne	تناظر
one-to-one correspondence	تناظر یک به یک
contradiction	تناقض
parity-check	توازن سنجی
extension	توسیع
separable extension	توسیع تفکیک‌پذیر
Galois extension	توسیع گالوا
commutative	جابجایی
permutation	جایگشت
cyclic permutation	جایگشت دوری
odd permutation	جایگشت فرد
algebra	جبر
Boolean algebra	جبر بولی
algebraic	جبری
abstract algebra	جبر مجرد
table	جدول
truth table	جدول راستی
thematic table of contents	جدول فهرست موضوعی
absorption	جذب
square root	جذر
pair	جفت
sum	جمع
direct sum	جمع مستقیم
additive	جمعی
term	جمله
solution	جواب

جواب یک معادله	solution of an equation
چپ	left
چندجمله‌ای (ها)	polynomial(s)
چندجمله‌ای اولیه	primitive polynomial
چندجمله‌ای تحویل‌پذیر	reducible polynomial
چندجمله‌ای تحویل‌ناپذیر	irreducible polynomial
چندجمله‌ای تکین	monic polynomial
چندجمله‌ای ثابت	constant polynomial
چندجمله‌ای مینیمال	minimal polynomial
چهارگانی (چهارگانها)	quaternion(s)
چهار ـ گروه (کلاین)	(Klien) four-gorup
حاصل‌ضرب	product
حاصل‌ضرب داخلی	inner product
حاصل‌ضرب دکارتی	Cartesian product
حاصل‌ضرب مستقیم داخلی	internal direct product
حاصل‌ضربی مستقیم خارجی	external direct product
حاصل‌ضرب نیمه مستقیم	semi direct product
حساب	arithmetic
حساب رایانه	computer arithmetic
حساب گزاره‌ها	propositional calculus=statement calculus
حقیقی	real
حکم	statement
حل	solution
حل‌پذیر	solvable
حل یک معادله	solution of an equation
حلقه (ها)	ring(s)
حلقه بولی	Boolean ring

division ring	حلقه تقسیمی
polynomial ring	حلقه چندجمله‌ای
quotient ring	حلقه خارج قسمتی
line	خط
straightedge	خط کش
linear	خطی
idempotent	خودتوان
automorphism	خودریختی
inner automorphism	خودریختی داخلی
circle	دایره
determinant	دترمینان
domain	دامنه
integral domain	دامنه صحیح
unique factorization domain	دامنه یکتایی تجزیه
Dedekind	ددکیند
degree	درجه
quadratic	درجه دوم
RSA system	دستگاه RSA
public-key cryptography system	دستگاه رمزنگاری ـ کلید ـ عمومی
system of linear congruences	دستگاه همنهشتی‌های خطی
formula	دستور
Kronecker delta	دلتای کرونکر
sequence	دنباله
pairwise disjoint	دوبدو مجزا
duplication of the cube	دوبرابرسازی مکعب
binary	دوتایی
cycle(s)	دور(ها)

دوجمله‌ای	binomial
دوسویی	bijection
دوگانی	duality
دوم، دومین	second
رابطه	relation
رابطه شمول	inclusion relation
رادیکال	radical
راست	right
راستگو	tautolegy
رده	class
رده‌بندی گروه‌های متناهی	classification of finite groups
رسند	meet
رسند عنصرها در یک شبکه	meet of elements in a lattice
رمز	code
رمزنگاری	cryptography
رویای سال‌اولی‌ها	Fershman's Dream
ریاضیات ترکیبیاتی	combinatorial mathematics
ریشه	root
ریشه دوم	square root
زاویه قائمه	right angle
زنجیر	chain
زنجیر صعودی = زنجیر فزاینده	ascending chain
زوج	even
زیرحلقه	subring
زیرگروه	subgroup
زیرگروه تابدار	torsion subgroup
زیرگروه جابجاگر	commutator subgroup

proper subgroup	زیرگروه سره
characteristic subgroup	زیرگروه مشخصه
subset	زیرمجموعه
subfield	زیرمیدان
construction	ساختار
simple	ساده
factor	سازه
invariant factor	سازه پایا
proper	سره
supremum	سوپریمم
quantifier	سور
universal quantifier	سور عمومی
existential quantifier	سور وجودی
index	شاخص
index of a subgroup	شاخص یک زیرگروه
ascending chain condition	شرط زنجیر صعودی
associativity	شرکت پذیری
radius	شعاع
radius of a circle	شعاع یک دایره
splits	شکافته می‌شود
forward-backward technieque	شگرد جلو ـ عقب
divisor	شمارنده
common divisor	شمارنده مشترک
elementary divisor	شمارنده‌های مقدماتی
inclusion	شمول
object	شی
zero	صفر

ضرب	multiplication
ضرب مستقیم	direct product
ضربی	multiplicative
ضریب	coefficient
ضریب پیشبرد	leading coefficient
ضلع	side
طرح	schem
طرف	side
عامل	factor
عامل پایا	invariant factor
عامل ترکیب	composition factor
عدد	number
عدد اول	prime number
عدد صحیح	integer
عدد صحیح مثبت	positive integer
عدد صحیح مربع ـ آزاد	square-free integer
عدد گویا	rational number
عضو	element = member
عضو ماکسیمال	maximal element=maximal member
عکس نقیض	contrapositive
عکس یک قضیه	converse of a theorem
عنصر	element
عنصر اول یک حلقه	prime element of a ring
عنصر جبری	algebraic element
عنصر (عضو) صفر	zero element
عنصر ماکسیمال	maximal element
عنصر متعالی	transendental element

sieve of Erathosthenes	غربال ارتستن
distance	فاصله
designed distance	فاصله طراحی شده
process	فرآیند
hypothesis	فرض
Fermat	فرما
formula	فرمول
formulation	فرمول‌بندی
De Moivar Formla	فرمول دمواور
technique	فن
rule	قاعده
law	قانون
distributive law	قانون توزیع‌پذیری
absorption law	قانون جذب
cancelation law	قانون حذف
associative law	قانون شرکت‌پذیری
Sylow theorems	قضایای سیلو
theorem	قضیه
fundament theorem	قضیه اساسی
First Sylow Theorem	قضیه اول سیلو
First Isomorphism Theorem	قضیه اول یکریختی
Euler's Theorem	قضیه اویلر
Remainder Theorem	قضیه باقیمانده
Chinese Remainder Theorem	قضیه باقیمانده چینی
Four- Color Theorem	قضیه چهار ـ رنگ
binomial Theorem	قضیه دوجمله‌ای
Cauchy Theorem	قضیه کشی

Cayley Theorem	قضیه کیلی
Lagrange Theorem	قضیه لاگرانژ
segment	قطعه
De Morgan's laws	قوانین دمورگان
modus ponens	قیاس استثنایی
code	کد
systematic code	کد روش‌مند
decoding	کدگشائی
maximum likelihood decoding	کدگشائی احتمال بیشین
syndrome decoding	کدگشائی مشخصه
nearest-neighbor decoding	کدگشائی نزدیکترین همسایه
bound	کران
upper bound	کران بالا
lower bound	کران پائین
fraction	کسر
reduced frection	کسر ساده شده
l.u.b.	ک‌ک‌ب (کوچکترین کران بالا)
class	کلاس
residue class	کلاس باقیمانده
massage word	کلمه پیام
received word	کلمه دریافتی
codeword	کلمه کد
switch	کلید
oppositely linked swiches	کلیدهای به طور مخالف مرتبط
series switches	کلیدهای سری
linked switches	کلیدهای متصل
parallel switches	کلیدهای موازی

minimum	کمینه
least residue	کوچکترین باقیمانده
least element	کوچکترین عضو (عنصر)
least upper bound	کوچکترین کران بالا
least common multiple	کوچکترین مضرب مشترک
Galois	گالوا
Gauss	گاوس
Abelean group	گروه آبلی
torsion group	گروه تابدار
alternating group	گروه تناوبی
indecomposable gourp	گروه تجزیه‌ناپذیر
permutation group	گروه جایگشتها
group of motions	گروه حرکتها
slovable group	گروه حل‌پذیر
quotient group	گروه خارج قسمتی
special linear group	گروه خطی خاص
general linear group	گروه خطی عام
group automorphisms	گروه خودریختی‌ها
cyclic group	گروه دوری
dihedral group	گروه دو وجهی
simple group	گروه ساده
Galois group	گروه گالوا
metablean group	گروه متاآبلی
symmetric group	گروه متقارن
finite group	گروه متناهی
group(s)	گروه(ها)
proposition=statement	گزاره

biconditional statement	گزاره دوشرطی
multiconditional statement	گزاره چندشرطی
conditional statement	گزاره شرطی
compound statement	گزاره مرکب
equivalent statements	گزاره‌های هم‌ارز
rational	گویا
necessity	لزوم
lemma	لم
matrix	ماتریس
matrices	ماتریس‌ها
zero matrix	ماتریس صفر
invertible matrix	ماتریس وارون‌پذیر
maximal	ماکسیمال
indeterminate	متغیر
symmetric	متقارن
complement	متمم
finite	متناهی
counter example	مثال نقض
triangle	مثلث
Pascal's triangle	مثلث خیام-پاسکال
abstraction	مجردسازی
disjoint	مجزا
isolated set	مجموعه تنها
empty set	مجموعه تهی
partially ordered set	مجموعه جزئاً مرتب
tatally ordered set	مجموعه کلاً مرتب
infinite set	مجموعه نامتناهی

set(s)	مجموعه(ها)
indeterminate	مجهول
complex	مختلط
circuit=orbit	مدار
open circuit	مدار باز
modular	مدولی
square	مربع
squaring the circle	مربع‌سازی دایره
order	مرتبه
center	مرکز
centralizer	مرکزساز
conjugate	مزدوج
conjugacy	مزدوجی
independent	مستقل
linearly independent	مستقل خطی
lattice	مشبکه
complete lattice	مشبکه کامل
complementary modular lattice	مشبکه مدولی متمدار
derivative	مشتق
characteristic	مشخصه
equation	معادله
cubic equation	معادله درجه سه
class equation	معادله رده‌ای
converse	معکوس
inverse	معکوس
Eisenstein Criterion	معیار ایزنشتاین
primise	مقدمه

zero divisor	مقسوم‌علیه صفر
intersection=section	مقطع
complement	مکمل
relative complement	مکمل نسبی
logic	منطق
formal logic	منطق سوری
negative	منفی
generators and relations	مولدها و روابط
field	میدان
real number field	میدان اعداد حقیقی
prime field	میدان اول
fixed field	میدان ثابت
splitting field	میدان شکافنده
finite field	میدان متناهی
infinite field	میدان نامتناهی
minimal	مینیمال
minimum	مینیمم
inequality	نابرابری، نامعادله
infinite	نامتناهی
corollary	نتیجه
norm	نرم
normal	نرمال
normalizer	نرمال‌ساز
relatively prime	نسبت به هم اول
label	نشان
number theory	نظریه اعداد
information theory	نظریه اطلاعات

ring theory	نظریه حلقه‌ها
coding theory	نظریه کدگذاری
set theory	نظریه مجموعه‌ها
map=mapping	نگاشت
inclusion mapping	نگاشت شمول
injective mapping=one-to-one mapping	نگاشت یک به یک
notation	نماد ـ نمادگذاری
representation	نمایش
index	نمایه
semicircle	نیمدایره
dependent	وابسته
associate	وابسته
linearly dependent	وابسته خطی
unity	واحد
converse	وارون
inverse	وارون
weight (of a code)	وزن (یک کد)
Hamming weight	وزن هامینگ
join	وست
join of elements in a lattice	وست عنصرها در یک مشبکه
kernel	هسته
kernel of a homomorphism	هسته یک همریختی
equivalence	هم‌ارزی
logical equivalence	هم‌ارزی منطقی
identity	همانی
homomorphism	همریختی
evaluation homomorphism	همریختی ارزشی

همریختی حلقه‌ای	ring homomorphism
هم‌مجموعه	coset
هم‌مجموعه چپ	left coset
هم‌مجموعه راست	right coset
همنهشت به پیمانه n	congruence modulo n
همنهشتی	congruence
همنهشتی درجه دوم	quadratic congruence
یای منطقی	inclusive or
یک به یک	injective=one-to-one
یکریخت	isomorphic
یکریختی حلقه‌ای	ring isomorphism
یکه	unit

فهرست نمادها

نماد	مفهوم	اولین صفحهٔ مراجعه
$\mathbb{Q}$	مجموعهٔ (میدان) اعداد گویا	۵۵
$\mathbb{Q}_{\mathbb{Z}}[x]$	چندجمله‌ایهای روی $\mathbb{Q}$ با جمله ثابت صحیح	۲۹۵
$\mathbb{R}$	مجموعهٔ (میدان) اعداد حقیقی	۵۵
$\mathbb{C}$	مجموعهٔ (میدان) اعداد مختلط	۵۵
$P \Rightarrow Q$	P نتیجه می‌دهد Q (یا اگر P آنگاه Q)	۶۰۲
$P \Longleftrightarrow Q$	P اگر و فقط اگر Q	۶۰۴
$a \in S$	a متعلّق به مجموعهٔ S است	۴
$a \notin S$	a متعلّق به مجموعهٔ S نیست	۱۹
$\{a \mid P(a)\}$	مجموعهٔ عناصر a که دارای خاصیت P هستند	۹
$\mathbf{N}$	مجموعهٔ اعداد صحیح نامنفی	۶۱۷

$a \not\equiv b \pmod{m}$	a همنهشت با b به پیمانهٔ m نیست	۳۴
$\mathbb{Z}_n$	مجموعهٔ کوچکترین باقیمانده‌های غیرمنفی به پیمانهٔ n	۲۹
U_n	گروه ضربی یکه‌های $\mathbb{Z}_n$	۱۹۶
φ	تابع ـ فی اویلر	۲۷۲
$A(T)$	مجموعهٔ جایگشتهای مجموعهٔ T	۲۰۴
S_n	مجموعهٔ جایگشتهای یک مجموعهٔ n عنصری	۱۹۷
$\begin{pmatrix} ۱ & ۲ & \cdots & n \\ T(۱) & T(۲) & \cdots & T(n) \end{pmatrix}$	جایگشت T از مجموعهٔ $\{۱, ۲, \ldots, n\}$	۱۹۳
$(x\ T(x) \cdots T^{r-۱}(x))$	دور T به طول r	۲۷۸
A_n	مجموعهٔ جایگشتهای زوج روی n عنصر	۲۸۱
$P(X)$	مجموعه زیرمجموعه‌های مجموعه X	۵۰۳
$\mid G \mid$	مرتبهٔ یک گروه G	۱۹۵
$D_۴$	گروه دو وجهی ازدرجهٔ ۴	۲۰۱
D_n	گروه دو وجهی از درجهٔ n	۲۰۱
$GL(n, \mathbb{F})$	گروه خطی عام از درجهٔ n روی میدان $\mathbb{F}$	۱۹۷
$SL(n, \mathbb{F})$	گروه خطی خاص از درجهٔ n روی میدان $\mathbb{F}$	۲۰۵
e (و یا ۱)	عنصر همانی یک گروه	۱۹۵
$\langle a \rangle$	گروه دوری تولیدشده توسط a	۲۱۸
$\mid a \mid$	مرتبهٔ عنصر a از یک گروه	۲۱۰
AB	حاصلضرب ایده‌آل‌های A و B از یک حلقه	۱۶۹
$a + I$	هم‌مجموعهٔ چپ I با نمایندهٔ a در یک حلقه	۱۶۵
aK	هم‌مجموعهٔ چپ K با نمایندهٔ a در یک گروه	۲۳۹
Ka	هم‌مجموعهٔ راست K با نمایندهٔ a در یک گروه	۲۳۸
$[G : H]$	شاخص زیرگروه H در گروه G	۲۶۳
R/I	حلقه خارج قسمت R بر I	۱۶۶
l.u.b.	کوچکترین کران بالا	۵۰۵
g.l.b.	بزرگترین کران پائین	۵۰۴

$[\mathbb{K} : \mathbb{F}]$	بعد $\mathbb{K}$ روی میدان $\mathbb{F}$	۳۴۶
$\mathbb{F}(u)$	زیرمیدان حاصل از الحاق u به $\mathbb{F}$	۳۵۵
$\mathrm{Gal}_{\mathbb{F}}\mathbb{K}$	گروه خودریختی‌های توسیع $\mathbb{K}$ از میدان $\mathbb{F}$	۴۴۰
$\mathbb{K}(x)$	میدان توابع گویای یک متغیره	۳۳۰

فهرست راهنما