کتاب برگزیدهٔ سال

مؤسسهٔ انتشارات علمی
دانشگاه صنعتی شریف

جبر مجرد

آی.ان. هراشتاین

ترجمهٔ دکتر علی اکبر عالم‌زاده

جبر مجرد

آی. ان. هراشتاین

ترجمهٔ
دکتر علی اکبر عالم‌زاده

مؤسسهٔ انتشارات علمی دانشگاه صنعتی شریف

بسم‌الله الرحمن الرحیم

فهرست مطالب

پیشگفتار مترجم

آی. ان. هراشتاین با کتاب مباحثی در جبر در ایران شهرت یافت. کتاب عالی بود و به چاپهای متعدد رسید. همه جا حضور داشت و مطالب خود را تحمیل می‌کرد. سالها تنها کتاب درسی در مقاطع مختلف جبر بود و سؤالات امتحانی نیز از روی آن طرح می‌شد. هنوز نیز سلطهٔ خود را حفظ کرده و در بسیاری از موارد یکه‌تاز میدان است، بدیلی نمی‌شناسد و جبر دانشگاه را در اختیار خود دارد. مسائل ستاره‌دارش زبانزد عام‌اند و بهترین مغزها را از پا انداخته و عاجز ساخته‌اند. لکن برخی از متخصصان اشاره می‌کنند که کتاب برای شروع جبر در دانشگاه کمی سخت است و این نقص را تنها گردی می‌دانند که بر عارض یک الماس نشسته است. هراشتاین با تدوین کتاب حاضر این گرد را می‌زداید و نقص مذکور را مرتفع می‌سازد. در واقع این دو کتاب مکمل یکدیگرند و انتظار می‌رود که سالیان سال بر جبر دانشگاه سلطهٔ بی‌منازع داشته باشند.

علی‌اکبر عالم‌زاده

پیشگفتار چاپ دوم

وقتی از من خواسته شد که ویرایش دوم جبر مجرد هراشتاین را آماده سازم، احساس من این بود که هر تغییر کلی در این کتاب جذاب و کامل اشتباه محض است. این عقیدهٔ تمام افرادی بود که با آنها مشورت کرده‌ام. لذا در آن تغییری اساسی نداده و روش غیرقابل تقلید هراشتاین و مطالب کتاب را تقریباً حفظ نموده‌ام.

با این حال در ویرایش دوم تغییرات جزئی ولی مهمی صورت یافته است. برخی مربوط به غلطها و ناهمواریهای کتاب و بقیه مربوط به توضیح و ساده‌سازی مطالب و مثالهایند.

همچنین دو تغییر کوچک نیز در ساختار کتاب صورت گرفته است. اولاً فهرستی از علایم اضافه شده تا خواننده در برخورد با علامات فراموش شده از آن استفاده کند. ثانیاً (و مهمتر از اولاً) چند مسئله با علامت ستاره (*) مشخص شده‌اند. این مسائل مبنای معرفی چند مفهوم و استدلال ساده‌اند که بحث را به نحوی جالب پشتیبانی کرده و یا بدان مربوط می‌شوند. لذا باید این مسائل به‌دقت بررسی و حل شوند.

تنی چند با کمکهای شایان خود این ویرایش کتاب جذاب هراشتاین را جالبتر ساخته‌اند که از آنها سپاسگزارم. فرصت را مغتنم شمرده از جورجیا بِنکارت، باربارا کورتزن، و لین اسمال به خاطر پیشنهادهای سازنده و بسیار سودمندشان تشکر می‌کنم.

دیوید ج. وینتر
(David J. Winter)

پیشگفتار مؤلف بر چاپ اول

جبر مجرد در نیمهٔ دوم قرن اخیر نه فقط در ریاضیات بلکه در سایر نظامها نیز اهمیت بسیار یافته است. مثلاً نتایج و مفاهیم جبر مجرد نقش مهمی در فیزیک، شیمی، کامپیوتر، و غیره ایفا کرده‌اند.

جبر مجرد در خود ریاضیات نقشی دوگانه دارد. یکی آنکه بخشهای از هم جدای ریاضیات را متحد ساخته و دیگر آنکه مبحثی است تحقیقی که از جنب‌وجوش بسیار برخوردار است. این مبحث در ۱۰۰ سال اخیر در هر دو مورد پر بار و سودمند بوده است. برخی از کارهای بزرگ ریاضیات قرن بیستم در این مبحث رخ داده و نتایج هیجان‌انگیزی در نظریهٔ گروهها، نظریهٔ حلقه‌های تعویضپذیر و تعویض‌ناپذیر، جبرهای لی، جبرهای ژردان، ترکیبیات، و بخشهای دیگر که کلاً به جبر مجرد معروف‌اند به‌دست آمده است. این مبحث که زمانی سری تلقی می‌شد اینک درسی عام برای بسیاری از افراد می‌باشد.

این کتاب به دو منظور نگاشته شده است: کتاب برای خواننده‌ای که بخواهد در ریاضیات یا مبحثی مربوط به آن که از مفاهیم و روشهای جبر استفاده می‌کند تحقیق نماید مقدمات کار است، البته فقط مقدمه‌ای است بر این مبحث جذاب؛ و برای خوانندهٔ علاقه‌مند که بخواهد از یک بخش فعال در ریاضیات جدید سر درآورد کتابی مناسب بوده و می‌تواند ابزارهای لازم در زمینه‌های موردنظرش را فراهم سازد.

مطالب کتاب به منظور آشنا ساختن خواننده با چند دستگاه جبری اساسی که هم جالب بوده و هم استفادهٔ گسترده دارند انتخاب شده‌اند. به‌علاوه، در هر یک از این دستگاهها، هدف رسیدن به چند نتیجهٔ مهم می‌باشد. بررسی یک شیء مجرد بدون مشاهدهٔ نتایجی غیربدیهی کاری است بی‌ثمر. امیدواریم با ارائهٔ نتایجی جالب، عملی، و مهم در دستگاههای انتخاب شده به هدف مورد نظر رسیده باشیم.

همان‌طور که به‌زودی خواهید دید، کتاب [illegible] مسائل بسیار برخوردار است. این تمرینها اغلب

به سه بخش تقسیم شده‌اند: آسانتر، با سطح متوسط، و مشکلتر (و گاهی بسیار سخت). هدف از این مسائل آن است که شاگرد در شبیه‌سازی مطالب تمرین کرده، با آنها به مبارزه برخاسته، برای مطالب آتی مهیا شده، و بصیرت، توان شهودی، و تکنیکهای ریاضی خود را افزایش دهد. خواننده‌ای که از عهدهٔ حل تمام آنها بر نمی‌آید نباید مأیوس شود. بسیاری از مسائل به منظور سرگرم ساختن (نه مأیوس ساختن) خواننده و تلاش در آنها (نه حل آنها) تدوین شده‌اند. برخی از مسائل چندین بار درکتاب ظاهر می‌شوند. سعی در حل آنها بی‌شک بهترین راه برای آموزش این مبحث می‌باشد.

یک حل‌المسائل برای دانشجو تدوین شده که شامل حل مشروح بسیاری از مسائل است و می‌توان آن را از ناشر دریافت کرد. همچنین یک حل‌المسائل برای مدرس نیز در دسترس می‌باشد.

سعی شده است تا مطالب به‌صورت سخنرانی درکلاس عرضه شود. لذا ارائهٔ مطلب به نوعی محاوره‌ای می‌باشد. امید است این امر موجب تسهیل برای خواننده گردد. کوشیده‌ایم تا مثالها بسیار بوده و مفاهیم مورد بحث را توضیح دهند. برخی از این مثالها بیانگر پدیده‌هایی هستند که بعدها خواهند آمد. ما اغلب در ادامهٔ بحث به آنها ارجاع خواهیم داشت.

کتاب جز در یک بخش (بخش دوم از آخر) که در آن از این امر که یک چندجمله‌ای روی میدان مختلط ریشه‌های مختلط دارد (قضیهٔ معروف اساسی جبر که به گاوس منسوب است) تلویحاً استفاده می‌شود و آخرین بخش که در آن کمی حساب دیفرانسیل و انتگرال لازم می‌شود خودکفا می‌باشد.

افراد بی‌شماری انتقادات و پیشنهاداتی در دستنویس اولیهٔ کتاب داشته‌اند و بدین ترتیب مرا مدیون خود ساخته‌اند. کتاب با اعمال تغییرات پیشنهادی آنها خواندنی‌تر شده است. بجاست که از پروفسور مارتین ایساکز (Professor Martin Isaacs) نیز به‌خاطر نظرات بسیار سودمندش تشکر نمایم.

همچنین از فرد فلاورز (Fred Flowers) به خاطر تایپ بسیار عالی دستنویس و گاری دبلیو. اوستد (Gary W. Ostedt) از سازمان مک‌میلان به خاطر علاقه‌اش به این کتاب و چاپ آن سپاسگزارم.

در خاتمه برای تمام خوانندگان سفر ریاضی خوشی را به سرزمین جذاب و زیبای جبر مجرد آرزو دارم.

آی. ان. هراشتاین
(I. N. Herstein)

۱

نکاتی آشنا و نکاتی کمتر آشنا

۱. چند مطلب مقدماتی

این کتاب برای بسیاری از خوانندگان نخستین تماس با ریاضیات مجرد است. مبحثی که در این کتاب مطرح می‌شود معمولاً «جبر مجرد» نام دارد، اما مشکلی که خواننده با آن روبه‌روست بیشتر از ناحیهٔ «مجرد» است تا ناحیهٔ «جبر».

مبتدیان در برخورد اول با بخشهایی از ریاضیات مجرد از قبیل آنالیز، توپولوژی، و غیره واکنش مشترکی از خود نشان می‌دهند. این را می‌توان با احساس سرگشتگی (به خاطر نداشتن چیزی محسوس برای توسل بدان) به بهترین وجه توصیف کرد. این امر تعجب چندانی ندارد زیرا با آنکه بسیاری از ایده‌ها اساساً ساده‌اند ولی ظریف بوده و از چنگال شخص مبتدی می‌گریزند. یک راه فرو نشاندن این احساس ناخوشایند یا این سؤال که «نکتهٔ اساسی چیست؟» اختیار مفاهیم موجود و مشاهدهٔ معنی آنها در حالاتی خاص است. به‌عبارت دیگر، بهترین راه برای درک کامل مفاهیم ارائه شده توجه به مثالها می‌باشد. این امر در سراسر ریاضیات به‌ویژه در جبر مجرد صادق خواهد بود.

می‌پرسیم: آیا می‌توان به سرعت و با چند حرکت جوهر، هدف، و زمینهٔ مطالب مورد مطالعه را توصیف کرد؟ حال برای یافتن جواب این سؤال تلاش می‌کنیم.

بحث را با گردایه‌ای از اشیاء مانند S آغاز کرده و به این گردایه، با این فرض که به یک یا چند (معمولاً دو) طریق می‌توان عنصرهای S را باهم ترکیب کرده عناصری از S را به‌دست آورد،

ساختاری جبری می‌بخشیم. این طریق ترکیب عناصر S را اعمال بر S می‌نامیم. سپس سعی می‌کنیم، به‌وسیلهٔ چند قاعده در مورد رفتار این اعمال بر S، بر ماهیت S شرطی گذارده و یا در آن نظمی برقرار سازیم. این قواعد را معمولاً اصول موضوع معرف یک ساختار خاص بر S می‌نامند. تعریف این اصول با ماست، لیکن انتخاب آنها (از نظر تاریخ ریاضیات) از این امر ناشی می‌شود که دستگاههای ریاضی ملموس بسیاری وجود دارند که در این قواعد یا اصول موضوع صدق می‌کنند. ما در این کتاب برخی از دستگاههای جبری اصل موضوعی اساسی، یعنی گروهها، حلقه‌ها، و میدانها، را مطالعه خواهیم کرد.

البته با مجموعه‌های بسیاری از اصول موضوع می‌توان ساختارهای جدید تعریف کرد. ما از یک چنین ساختار چه انتظاری داریم؟ مسلماً می‌خواهیم که اصول موضوعش سازگار باشند؛ یعنی در چهارچوب اعمالی که اصول موضوع اجازه می‌دهند به محاسبه‌ای متناقض و بی‌معنی نرسیم. اما این امر کافی نیست. به آسانی می‌توان با اعمال مجموعه‌ای از قواعد بر مجموعهٔ S یک ساختار جبری ساخت و به دستگاهی بیمار و غیرعادی رسید. به‌علاوه، ممکن است موارد معدودی از قواعد ما پیروی نمایند.

تاریخ نشان داده است که بعضی از ساختارهای تعریف شده با «اصول موضوع» نقش مهمی در ریاضیات (و سایر مباحث) داشته و برخی دیگر اصلاً جالب نبوده‌اند. ساختارهایی که قبلاً ذکر شدند، یعنی گروهها، حلقه‌ها، و میدانها، از آزمون زمان سرافراز بیرون آمده‌اند.

یک نکته در باب استفاده از «اصول موضوع»: «اصل موضوع» در زبان عرف یعنی حقیقتی خود آشکار. ولی ما زبان عرف به‌کار نمی‌بریم؛ سروکار ما با ریاضیات است. یک اصل موضوع واقعیتی عام (با هر معنی ممکن) نیست بلکه یکی از چند قاعده‌ای است که ساختاری ریاضی برپا می‌سازند. اصل موضوع در دستگاه مورد مطالعهٔ ما درست است چرا که طبق فرض آن را درست گرفته‌ایم. یک اصل مجوزی است در یک ساختار خاص برای انجام برخی از کارها.

حال به نکته‌ای که قبلاً راجع به واکنش بسیاری از شاگردان در برخورد اول با این نوع جبر گفته شد، یعنی عدم احساس ملموس بودن مطلب، باز می‌گردیم. اگر اولین برخورد شما را در کمی ابهام فرو برد مأیوس نشوید. با آن باشید، سعی کنید آنچه را که یک مفهوم می‌گوید درک کنید و، از همه مهمتر، به مثالهای خاص و ملموس مفهوم مورد بحث بپردازید.

مسائل

۱. فرض کنید S مجموعه‌ای با عمل $*$ باشد که به هر دو عنصر $a, b \in S$ عنصر $a * b$ را

نسبت می‌دهد. همچنین دو قاعدهٔ زیر برقرار باشند:

۱. هرگاه a و b اشیائی در S باشند، آن‌گاه $a * b = a$؛

۲. هرگاه a و b اشیائی در S باشند، آن‌گاه $a * b = b * a$.

نشان دهید که S می‌تواند حداکثر یک شیء داشته باشد.

۲. فرض کنید S مجموعهٔ تمام اعداد صحیح $\ldots, \pm n, \ldots, \pm ۲, \pm ۱, ۰$ باشد. عمل $*$ را به ازای هر a و b در S با $a * b = a - b$ تعریف کرده و احکام زیر را تحقیق نمایید:

الف) $a * b \neq b * a$ مگر آنکه $a = b$؛

ب) به‌طور کلی، $(a * b) * c \neq a * (b * c)$. تحت چه شرایطی بر a و b و c خواهیم داشت $(a * b) * c = a * (b * c)$؟

پ) عدد صحیح ۰ واجد این خاصیت است که به ازای هر a در S، $a * ۰ = a$؛

ت) به ازای هر a در S، $a * a = ۰$.

۳. فرض کنید S از دو شیء $\square$ و $\triangle$ تشکیل شده باشد. عمل $*$ را بر S با گذاردن شروط زیر بر $\square$ و $\triangle$ تعریف می‌کنیم:

۱. $\square * \triangle = \triangle = \triangle * \square$؛

۲. $\square * \square = \square$؛

۳. $\triangle * \triangle = \square$.

با محاسبهٔ مستقیم تحقیق کنید که هرگاه a و b و c عناصر دلخواهی از S باشند (یعنی a و b و c مساوی $\square$ یا $\triangle$ باشند)، آن‌گاه

الف) $a * b$ در S است؛

ب) $(a * b) * c = a * (b * c)$؛

پ) $a * b = b * a$؛

ت) aای خاص در S هست به‌طوری که به ازای هر b در S، $a * b = b * a = b$؛

ث) هرگاه b در S باشد، آن‌گاه $b * b = a$ که در آن a عنصر خاص قسمت (ت) می‌باشد.

۲. نظریهٔ مجموعه‌ها

در پی تغییراتی که در برنامهٔ ریاضیات مدارس در ایالات متحده شد، بسیاری از شاگردان با نظریهٔ مجموعه‌ها آشنا شدند. این آشنایی در مدارس معمولاً مشتمل است بر مفاهیم و اعمال مقدماتی با مجموعه‌ها. با این فرض که بسیاری از خوانندگان آشنایی کمی با نظریهٔ مجموعه‌ها دارند، بخشهایی

از این نظریه را که بعداً به کارمان می‌آیند مرور سریعی می‌کنیم.

ابتدا به چند نماد نیاز داریم. برای احتراز از تکرار برخی از عبارات، برای آنها صورت فشرده معرفی می‌کنیم. فرض کنیم S گردایه‌ای از اشیاء باشد. اشیاء S را عنصرهای S می‌نامیم. برای آنکه a عنصری از S باشد می‌نویسیم $a \in S$ و می‌خوانیم: «a یک عنصر S است.» برای نشان دادن عکس آن، یعنی a یک عنصر S نیست، می‌نویسیم $a \notin S$. مثلاً، هرگاه S مجموعهٔ تمام اعداد صحیح مثبت $۱, ۲, ۳, \ldots, n, \ldots$ باشد، آن‌گاه $۱۶۵ \in S$ ولی $-۱۳ \notin S$.

ما اغلب می‌خواهیم بدانیم و یا ثابت کنیم که به ازای دو مجموعهٔ S و T، یکی از آنها بخشی از دیگری هست یا نه. گوییم S یک زیرمجموعهٔ T است و می‌نویسیم $S \subset T$ (بخوانید: «S مشمول T است») اگر هر عنصر S عنصری از T باشد. برحسب نمادها داریم: $S \subset T$ اگر $s \in S$ ایجاب کند که $s \in T$. این را می‌توان با $T \supset S$ نیز نشان داد و خواند: «T شامل S است». (این امر احتمال اینکه $S = T$، یعنی S و T عناصر یکسانی دارند، را نفی نمی‌کند.) مثلاً هرگاه T مجموعهٔ تمام اعداد صحیح مثبت بوده و S مجموعهٔ تمام اعداد صحیح زوج مثبت باشد، آن‌گاه $S \subset T$، و S زیرمجموعهٔ T می‌باشد. در تعریف فوق، به ازای هر مجموعهٔ S داریم $S \subset S$؛ یعنی S همیشه زیرمجموعهٔ خود می‌باشد.

ما اغلب با این مسئله که آیا دو مجموعهٔ S و T، که احتمالاً به طرق مختلفی تعریف شده‌اند، مساویند (یعنی از عناصر یکسانی تشکیل شده‌اند) مواجهیم. روش معمول برای اثبات آن نشان دادن هر دوی $S \subset T$ و $T \subset S$ است. مثلاً هرگاه S مجموعهٔ تمام اعداد صحیح مثبت با عامل ۶ بوده و T مجموعهٔ تمام اعداد صحیح مثبت با عوامل ۲ و ۳ باشند، آن‌گاه $S = T$. (ثابت کنید!)

همچنین به مجموعه‌ای بسیار خاص که اصلاً عضوی ندارد نیاز خواهیم داشت. این مجموعه را مجموعهٔ پوچ یا مجموعهٔ تهی نامیده و آن را با $\varnothing$ نشان می‌دهیم؛ $\varnothing$ واجد این خاصیت است که زیرمجموعهٔ هر مجموعهٔ S می‌باشد.

فرض کنیم A و B زیرمجموعه‌های S باشند. برای ساختن زیرمجموعه‌های دیگری از S به‌وسیلهٔ A و B روشهایی را معرفی می‌کنیم. اولین روش اجتماع A و B است که به‌صورت $A \cup B$ نوشته شده و این‌طور تعریف می‌شود: $A \cup B$ زیرمجموعه‌ای از S و مرکب از عناصری از S است که عنصر A یا عنصر B می‌باشند. لفظ «یا» که به‌کار برده‌ایم با معنی عادی‌اش اندکی متفاوت است. در اینجا مقصود آن است که عنصر c در $A \cup B$ است اگر در A یا در B یا در هر دو باشد. این «یا» احتمال درست بودن هر دو را نفی نمی‌کند. لذا، مثلاً، $A \cup A = A$.

هرگاه $A = \{۱, ۲, ۳\}$ و $B = \{۲, ۴, ۶, ۱۰\}$، آن‌گاه $A \cup B = \{۱, ۲, ۳, ۴, ۶, ۱۰\}$.

حال به روش دوم ساختن مجموعه‌های جدید از مجموعه‌های قدیم می‌پردازیم. مجدداً فرض

می‌کنیم A و B زیرمجموعه‌هایی از مجموعهٔ S باشند. منظور از اشتراک A و B، که به‌صورت $A\cap B$ نوشته می‌شود، یعنی زیرمجموعهٔ S مرکب از عناصری که هم در A و هم در B می‌باشند. لذا، در مثال فوق، $A\cap B = \{۲\}$. از تعاریف مربوطه واضح است که $A\cap B\subset A$ و $A\cap B\subset B$. چند مثال خاص از اشتراک که عموماً برقرارند عبارتند از

$$A\cap\varnothing=\varnothing \ ، \ A\cap S=A \ ، \ A\cap A=A$$

حال یک طرح نمادین را که گهگاه به‌کار می‌رود معرفی می‌کنیم. اغلب از ما می‌خواهند تا زیرمجموعهٔ A از مجموعهٔ S را که در خاصیت معینی چون P صدق می‌کند توصیف نماییم. ما این امر را به‌صورت $A=\{s\in S|$ در P صدق می‌کند $s\}$ می‌نویسیم. مثلاً هرگاه A و B زیرمجموعه‌هایی از S باشند، آن‌گاه $A\cup B=\{s\in S|s\in A$ یا $s\in B\}$ ولی $A\cap B=\{s\in S|s\in A$ و $s\in B\}$.

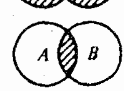
با آنکه مفاهیم اجتماع و اشتراک زیرمجموعه‌های S برای دو زیرمجموعه تعریف شده‌اند، واضح است که می‌توان آنها را برای هر تعداد زیرمجموعه تعریف کرد.

حال عمل سوم بر مجموعه‌ها، یعنی تفاضل دو مجموعه، را معرفی می‌کنیم. هرگاه A و B زیرمجموعه‌هایی از S باشند، تعریف می‌کنیم $A-B=\{a\in A|a\notin B\}$. لذا، اگر A مجموعهٔ تمام اعداد صحیح مثبت و B مجموعهٔ تمام اعداد صحیح زوج باشد، آن‌گاه $A-B$ مجموعهٔ تمام اعداد صحیح فرد مثبت است. در حالت خاص که A زیرمجموعهٔ S است، تفاضل $S-A$ را متمم A در S نامیده و آن را به‌صورت A' می‌نویسیم.

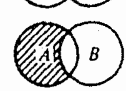
این سه عمل را با شکل نشان می‌دهیم. هرگاه A به شکل Ⓐ و B به شکل Ⓑ باشد، آن‌گاه

۱. 

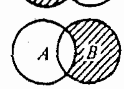
$A\cup B=$ سطح سایه‌دار است؛

۲. 

$A\cap B=$ سطح سایه‌دار است؛

۳. 

$A-B=$ سطح سایه‌دار است؛

۴. 

$B-A=$ سطح سایه‌دار است.

به رابطهٔ بین این سه عمل، یعنی $A\cup B=(A\cap B)\cup(A-B)\cup(B-A)$، توجه کنید. به‌عنوان توضیح اینکه چطور می‌توان تساوی مجموعه‌های حاصل از این اعمال نظریهٔ مجموعه‌ها

را ثابت کرد، تساوی فوق‌الذکر را ثابت می‌کنیم. ابتدا نشان می‌دهیم که

$$(A \cap B) \cup (A - B) \cup (B - A) \subset A \cup B$$

این بخش آسان است زیرا، طبق تعریف، $A \cap B \subset A$، $A - B \subset A$، و $B - A \subset B$؛ پس

$$(A \cap B) \cup (A - B) \cup (B - A) \subset A \cup A \cup B = A \cup B$$

حال، در جهت دیگر، یعنی اینکه $A \cup B \subset (A \cap B) \cup (A \cup B) \cup (B - A)$، گوییم به ازای $u \in A \cup B$، هرگاه $u \in A$ و $u \in B$، آن‌گاه $u \in A \cap B$؛ پس مسلماً در $(A \cap B) \cup (A - B) \cup (B - A)$ است. از آن سو، هرگاه $u \in A$ ولی $u \notin B$، آن‌گاه، بنابر تعریف $A - B$، $u \in A - B$؛ پس مجدداً در $(A \cap B) \cup (A - B) \cup (B - A)$ می‌باشد. بالاخره، هرگاه $u \in B$ ولی $u \notin A$، آن‌گاه $u \in B - A$؛ پس مجدداً در $(A \cap B) \cup (A - B) \cup (B - A)$ می‌باشد. لذا جمیع حالات مطرح شده و نشان داده‌ایم که $A \cup B \subset (A \cap B) \cup (A - B) \cup (B - A)$. حال با داشتن دو رابطهٔ شمول مخالف هم $A \cup B$ و $(A \cap B) \cup (A - B) \cup (B - A)$، تساوی مطلوب این دو مجموعه حاصل می‌شود.

این بحث کوتاه از نظریهٔ مجموعه‌ها را با ساختار دیگری بر مجموعه‌ها پایان می‌بخشیم. این ساختار ضرب دکارتی است که به ازای هر دو مجموعهٔ A و B با $A \times B = \{(a, b) | b \in B، a \in A\}$ تعریف می‌شود، که در آن گوییم جفت مرتب (a, b) مساوی جفت مرتب (a_1, b_1) است اگر و فقط اگر $a = a_1$ و $b = b_1$. در اینجا نیز نباید به دو مجموعه محدود شد؛ مثلاً می‌توان به ازای هر سه مجموعهٔ A و B و C حاصلضرب دکارتی آنها را مجموعه‌ای از سه‌تاییهای مرتب (a, b, c) تعریف کرد که $a \in A$، $b \in B$، و $c \in C$، و تساوی دو سه‌تایی مرتب را مؤلفه به مؤلفه تعریف می‌کنیم.

مسائل

مسائل آسانتر

۱. مجموعه‌های زیر را با الفاظ توصیف کنید:

الف) $S =$ {عطارد ,زهره ,زمین ... ,پلوتو}؛

ب) $S =$ {آلاباما ,آلاسکا... ,وایومینگ}.

۲. مجموعه‌های زیر را با الفاظ توصیف کنید:

الف) $S = \{۲, ۴, ۶, ۸, \ldots\}$؛

ب) $S = \{۲, ۴, ۸, ۱۶, ۳۲, \ldots\}$؛

پ) $S = \{۱, ۴, ۹, ۱۶, ۲۵, ۳۶, \ldots\}$.

۳. اگر A مجموعهٔ تمام ساکنین ایالات متحده، B مجموعهٔ تمام شهروندان کانادایی، و C مجموعهٔ تمام زنان جهان باشد، مجموعه‌های $A \cap B \cap C$، $A - B$، $A - C$، و $C - A$ را با الفاظ توصیف کنید.

۴. اگر $A = \{۱, ۴, ۷, a\}$ و $B = \{۳, ۴, ۹, ۱۱\}$ و بدانیم که $A \cap B = \{۴, ۹\}$، a چه خواهد بود؟

۵. اگر $A \subset B$ و $B \subset C$، ثابت کنید $A \subset C$.

۶. اگر $A \subset B$، ثابت کنید به ازای هر مجموعهٔ C، $A \cup C \subset B \cup C$.

۷. نشان دهید که $A \cup B = B \cup A$ و $A \cap B = B \cap A$.

۸. ثابت کنید $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$. این رابطه چه شکلی دارد؟

۹. ثابت کنید $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

۱۰. ثابت کنید $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

۱۱. تمام زیرمجموعه‌های $S = \{۱, ۲, ۳, ۴\}$ را بنویسید.

مسائل با سطح متوسط

۱۲*. اگر C زیرمجموعه‌ای از S باشد، C' را متمم C در S گرفته و قواعد دمورگان (De Morgan) را به ازای هر دو زیرمجموعهٔ A و B از S ثابت کنید:

الف) $(A \cap B)' = A' \cup B'$؛

ب) $(A \cup B)' = A' \cap B'$.

۱۳*. فرض کنید S یک مجموعه باشد. به ازای هر دو زیرمجموعه از S تعریف کنید

$$A \cdot B = A \cap B \quad \text{و} \quad A + B = (A - B) \cup (B - A)$$

و ثابت کنید

الف) $A + B = B + A$؛

ب) $A + \varnothing = A$؛

پ) $A \cdot A = A$؛

ت) $A + A = \varnothing$؛

ث) $A + (B + C) = (A + B) + C$؛

ج) هرگاه $A + B = A + C$، آن‌گاه $B = C$؛

چ) $A \cdot (B + C) = A \cdot B + A \cdot C$.

*۱۴. اگر C یک مجموعهٔ متناهی باشد، $m(C)$ را تعداد عناصر C بگیرید. اگر A و B مجموعه‌هایی متناهی باشند، ثابت کنید

$$m(A \cup B) = m(A) + m(B) - m(A \cap B)$$

۱۵. به ازای سه مجموعهٔ متناهی A و B و C، فرمولی برای $m(A \cup B \cup C)$ بیابید. (راهنمایی. ابتدا $D = B \cup C$ را در نظر گرفته و از مسئلهٔ ۱۴ استفاده کنید.)

۱۶. $m(A_1 \cup A_2 \cup \cdots \cup A_n)$ را به ازای n مجموعهٔ متناهی A_1، A_2، ...، A_n بیابید.

۱۷. با استفاده از مسئلهٔ ۱۴ نشان دهید که اگر ۸۰٪ تمام آمریکاییان به دبیرستان رفته و ۷۰٪ تمام آمریکاییان روزنامه بخوانند، دست‌کم ۵۰٪ آمریکاییان هم به دبیرستان رفته‌اند و هم روزنامه می‌خوانند.

۱۸. در یک رأی‌گیری ۹۳٪ مردم با اولین تصمیم، ۸۴٪ با دومین تصمیم، و ۷۴٪ با سومین تصمیم دولت موافق بوده‌اند. دست‌کم چه درصدی از مردم با هر سه تصمیم دولت توافق داشته‌اند؟ (راهنمایی. از مسئلهٔ ۱۵ استفاده کنید.)

۱۹. لوییس کارول (Lewis Carroll) در کتاب داستان بغرنج (A Tangled Tale) معمای زیر را در مورد گروهی جانباز مطرح می‌کند: ۷۰٪ یک چشم، ۷۵٪ یک گوش، ۸۰٪ یک دست، و ۸۵٪ یک پا از دست داده‌اند. دست‌کم چه درصدی از این گروه هر چهارعضو را از دست داده‌اند؟ معمای لوییس کارول را حل کنید.

*۲۰. نشان دهید که به ازای هر دو مجموعهٔ متناهی A و B، $m(A \times B) = m(A)m(B)$.

۲۱. اگر مجموعهٔ S دارای پنج عنصر باشد،

الف) S چند زیرمجموعه دارد؟

ب) S چند زیرمجموعهٔ چهار عنصری دارد؟

پ) S چند زیرمجموعهٔ دو عنصری دارد؟

مسائل مشکلتر

۲۲. الف) نشان دهید که هر مجموعهٔ n عنصری دارای 2^n زیرمجموعه است.

ب) اگر $0 < m < n$، چند زیرمجموعه درست m عنصر دارند؟

۳. نگاشتها

یکی از مفاهیم به‌واقع عام که تقریباً در همه جای ریاضیات حضور دارد تابع یا نگاشت از یک مجموعه به مجموعهٔ دیگر است. به جرأت می‌توان گفت که هیچ بخشی از ریاضیات نیست که این مفهوم در آن ظاهر نشده و یا نقشی اساسی نداشته باشد. تابع از یک مجموعه به مجموعهٔ دیگر را می‌توان به‌طور صوری و برحسب زیرمجموعه‌ای از حاصلضرب دکارتی این مجموعه‌ها تعریف کرد. ما به‌جای این کار تعریفی غیرصوری و نادقیق از نگاشت (تابع) از یک مجموعه به مجموعهٔ دیگر می‌آوریم.

فرض کنیم S و T دو مجموعه باشند. تابع یا نگاشت f از S به T قاعده‌ای است که به هر عنصر $s \in S$ عنصر منحصر به‌فردی چون $t \in T$ را نسبت می‌دهد. حال معنی این تعریف را کمی کاملتر توضیح می‌دهیم. هرگاه s عنصری از S باشد، آن‌گاه تنها یک عنصر مانند t در T هست که به‌وسیلهٔ این نگاشت به s منسوب می‌شود. وقتی s روی S تغییر کند، t روی T (به طریقی وابسته به s) تغییر می‌نماید. توجه کنید که، طبق تعریف، رابطهٔ زیر یک نگاشت نیست. فرض کنیم S مجموعهٔ تمام افراد جهان و T مجموعهٔ تمام کشورهای جهان باشد. همچنین f قاعده‌ای باشد که به هر شخص کشور یا شهروندیش را منتسب سازد. f یک نگاشت از S به T نیست. چرا نیست؟ زیرا افرادی در جهان هستند که شهروندی متعددی دارند. برای این افراد کشور یا شهروندی منحصر به‌فردی وجود ندارد. مثلاً، اگر مری جونز یک شهروند انگلیسی و فرانسوی باشد، f در اعمال بر مری جونز به‌عنوان یک نگاشت بی‌معنی است. از آن‌سو، قاعدهٔ $f : \mathbb{R} \to \mathbb{R}$ (که در آن $\mathbb{R}$ مجموعهٔ اعداد حقیقی است) با تعریف $f(a) = a^۲$ به ازای $a \in \mathbb{R}$ یک تابع کاملاً مناسب از $\mathbb{R}$ به $\mathbb{R}$ می‌باشد. باید توجه داشت که $f(-۲) = (-۲)^۲ = ۴ = f(۲)$ و، به ازای هر $a \in \mathbb{R}$، $f(-a) = f(a)$.

نگاشت بودن f از S به T را با $f : S \to T$ نشان داده و به ازای $t \in T$ مذکور در فوق می‌نویسیم $t = f(s)$؛ t را نقش s تحت f می‌نامیم.

این مفهوم برای هیچیک از ما تازگی ندارد. ما از دوران مدرسه مرتب با نگاشتها و تابعها (اغلب به شکل فرمول) برخورد داشته‌ایم. اما لازم نیست نگاشتها به مجموعه‌هایی از اعداد محدود باشند. همان‌طور که ذیلاً می‌بینیم، آنها می‌توانند در هر زمینه ظاهر شوند.

چند مثال

۱. فرض کنیم

$$S = \{\text{تمام مردانی که تا به حال زیسته‌اند}\}$$

و

$$T = \{\text{تمام زنانی که تا به حال زیسته‌اند}\}$$

$f : S \to T$ را با مادر s = $f(s)$ تعریف می‌کنیم. لذا، رزکندی = (جان اف.کندی)f و، بنابر تعریف ما، رزکندی نقش جان اف.کندی تحت f می‌باشد.

۲. فرض کنیم {تمام شهروندان ایالات متحده} = S و {تمام اعداد صحیح مثبت} = T. به ازای $s \in S$، $f(s)$ را با شمارهٔ شناسنامهٔ s = $f(s)$ تعریف می‌کنیم. این f معرف یک نگاشت از S به T می‌باشد.

۳. فرض کنیم S مجموعهٔ تمام اجناس فروشی در یک بقالی بوده و {تمام اعداد حقیقی} = T. $f : S \to T$ را با بهای s = $f(s)$ تعریف می‌کنیم. این f معرف یک نگاشت از S به T می‌باشد.

۴. فرض کنیم S مجموعهٔ تمام اعداد صحیح بوده و $S = T$. $f : S \to T$ را با $f(m) = ۲m$ به ازای هر عدد صحیح m تعریف می‌کنیم. لذا نقش ۶ تحت این نگاشت، یعنی $f(۶)$، عبارت است از $۱۲ = ۲ \cdot ۶ = f(۶)$، اما نقش ۳−، یعنی $f(-۳)$، عبارت است از $f(-۳) = ۲(-۳) = -۶$. اگر $s_۱, s_۲ \in S$ و $f(s_۱) = f(s_۲)$، راجع به $s_۱$ و $s_۲$ چه می‌شود گفت؟

۵. فرض کنید $S = T$ مجموعهٔ تمام اعداد حقیقی باشند. $f : S \to T$ را با $f(s) = s^۲$ تعریف می‌کنیم. آیا هر عنصر T نقش عنصری مانند $s \in S$ است؟ اگر نیست، مجموعهٔ تمام نقشهای $\{f(s) | s \in S\}$ را چطور توصیف می‌کنید؟ چه وقت $f(s_۱) = f(s_۲)$؟

۶. فرض کنیم $S = T$ مجموعهٔ تمام اعداد حقیقی باشند. $f : S \to T$ را با $f(s) = s^۳$ تعریف می‌کنیم. این یک تابع از S به T است. راجع به $\{f(s) | s \in S\}$ چه می‌شود گفت؟ چه وقت $f(s_۱) = f(s_۲)$؟

۷. فرض کنیم T یک مجموعهٔ ناتهی بوده و $S = T \times T$، یعنی حاصلضرب دکارتی T در خودش. $f : T \times T \to T$ را با $f(t_۱, t_۲) = t_۱$ تعریف می‌کنیم. این نگاشت از $T \times T$ به T را تصویر $T \times T$ به روی مؤلفهٔ اولش می‌نامند.

۸. فرض کنیم S مجموعهٔ تمام اعداد صحیح مثبت و T مجموعهٔ تمام اعداد گویای مثبت باشد. $f : S \times S \to T$ را با $f((m, n)) = m/n$ تعریف می‌کنیم. این یک نگاشت از $S \times S$

به T است. توجه کنید که $f((۱,۲)) = ۱/۲$ ولی، با آنکه $(۳,۶) \neq (۱,۲)$،

$$f((۳,۶)) = ۳/۶ = ۱/۲ = f((۱,۲))$$

زیرمجموعه‌ای از $S \times S$ را که در آن $f((a,b)) = ۱/۲$ توصیف نمایید.

نگاشتهای تعریف شده در مثالهای ۹ و ۱۰ برای مجموعه‌های ناتهی دلخواهند و نقشی خاص برعهده خواهند داشت.

۹. فرض کنیم S و T مجموعه‌هایی ناتهی بوده و t. عنصر ثابتی از T باشد. $f : S \to T$ را به ازای هر $s \in S$ با $f(s) = t$. تعریف می‌کنیم. f را یک تابع ثابت از S به T می‌نامیم.

۱۰. فرض کنیم S مجموعه‌ای ناتهی بوده و $i : S \to S$ را با $i(s) = s$ به ازای هر $s \in S$ تعریف می‌کنیم. ما این تابع از S به خود را تابع همانی (یا نگاشت همانی) بر S می‌نامیم. گاهی ممکن است آن را با i_S (و بعدها در این کتاب با e) نیز نشان دهیم.

حال که مفهوم نگاشت را داریم، باید راهی برای تشخیص تساوی دو نگاشت از یک مجموعه به مجموعهٔ دیگر بیابیم. این راه خدادادی نیست؛ اعلام اینکه $f = g$ که در آن $f : S \to T$ و $g : S \to T$ وظیفهٔ ماست. چه چیز طبیعی‌تر از اینکه این تساوی را از طریق اعمال f و g بر عناصر S تعریف کنیم؟ به‌طور دقیقتر، گوییم $f = g$ اگر و فقط اگر به ازای هر $s \in S$، $f(s) = g(s)$. هرگاه S مجموعهٔ تمام اعداد حقیقی بوده و f بر S با $f(s) = s^۲ + ۲s + ۱$ و g بر S با $g(s) = (s + ۱)^۲$ تعریف شده باشد، تعریف ما از تساوی f و g چیزی جز اتحاد آشنای $(s + ۱)^۲ = s^۲ + ۲s + ۱$ نیست.

حال که تساوی دو نگاشت تعریف شد، چند نوع نگاشت را به‌وسیلهٔ رفتارشان ممتاز می‌سازیم.

تعریف. نگاشت $f : S \to T$ برو یا سورژکتیو است اگر هر $t \in T$ نقش عنصری مانند $s \in S$ تحت f باشد؛ یعنی اگر و فقط اگر به ازای هر $t \in T$ عنصری مانند $s \in S$ باشد به‌طوری که $t = f(s)$.

در مثالهایی که قبلاً زده شد، نگاشت مثال ۱ برو نیست زیرا هر زنی که تا به حال زیسته مادر پسری نبوده است. نگاشت مثال ۲ نیز برو نیست، زیرا هر عدد صحیح مثبت شمارهٔ شناسنامهٔ یک شهروند آمریکایی نیست. نگاشت مثال ۴ نیز برو نیست، زیرا هر عدد صحیح زوج نیست؛ و نگاشت مثال ۵ نیز برو نیست، زیر مثلاً عدد -۱ مجذور هیچ عدد حقیقی نمی‌باشد. اما نگاشت

مثال ۶ بروست، زیرا هر عدد حقیقی دارای ریشهٔ سوم حقیقی منحصر به‌فرد می‌باشد. بر خواننده است که در سایر مثالها برو بودن یا نبودن نگاشتهای داده شده را تحقیق نماید.

اگر تعریف‌کنیم $f(S) = \{f(s) \in T | s \in S\}$، راه دیگر آنکه بگوییم نگاشت $f : S \to T$ بروست این است که بنویسیم $f(S) = T$.

در آنچه می‌آید، نوع خاص دیگری از نگاشتها نقش خاص و مهمی ایفا خواهد کرد.

تعریف. نگاشت $f : S \to T$ را یک‌به‌یک یا انژکتیو گوییم (و می‌نویسیم ۱-۱) اگر به ازای هر $s_1 \neq s_2$ در S، در T داشته باشیم $f(s_1) \neq f(s_2)$. به بیان معادل، f در صورتی ۱-۱ است که $f(s_1) = f(s_2)$ تساوی $s_1 = s_2$ را ایجاب نماید.

به‌عبارت دیگر، یک نگاشت در صورتی ۱-۱ است که اشیاء متمایز را به نقشهای متمایز ببرد. در مثالهای قبل از نگاشتها، نگاشت مثال ۱ یک‌به‌یک نیست، زیرا دو برادر می‌توانند یک مادر داشته باشند. ولی نگاشت مثال ۲ یک‌به‌یک است، زیرا شهروندان مختلف ایالات متحده شمارهٔ شناسنامهٔ مختلفی دارند (مشروط بر اینکه در واشنگتن اشتباه نشده باشد که بعید به نظر می‌رسد). تحقیق ۱-۱ بودن یا نبودن سایر نگاشتهای داده شده به خواننده محول می‌شود.

مجموعهٔ $B = \{s \in S | f(s) \in A\}$ را به ازای نگاشت $f : S \to T$ و زیرمجموعهٔ $A \subset T$ در نظر می‌گیریم. ما از نماد $f^{-1}(A)$ برای این B استفاده کرده و $f^{-1}(A)$ را نقش معکوس A تحت f می‌نامیم. مجموعهٔ مورد توجه $f^{-1}(t)$، یعنی نقش معکوس زیرمجموعهٔ $\{t\}$ از T مرکب از فقط عنصر $t \in T$، است. اگر نقش معکوس $\{t\}$ فقط از یک عنصر، مثلاً $s \in S$، تشکیل شده باشد، $f^{-1}(t)$ را با $f^{-1}(t) = s$ تعریف می‌کنیم. همان‌طور که خواهیم دید، این لازم نیست نگاشتی از T به S باشد، ولی در صورت یک‌به‌یک و برو بودن f چنین خواهد بود. ما از نماد واحد f^{-1} در هر دو حالت زیرمجموعه‌ها و عنصرها استفاده خواهیم کرد. f^{-1} در حالت کلی به چند دلیل معرف یک نگاشت از T به S نیست. اولاً، اگر f برو نباشد، tای در T هست که نقش هیچ عنصر s نیست؛ پس $f^{-1}(t) = \varnothing$. ثانیاً، اگر f یک‌به‌یک نباشد، به ازای $t \in T$ای دست‌کم دو عنصر مانند $s_1 \neq s_2$ در S هست که $f(s_1) = t = f(s_2)$. پس $f^{-1}(t)$ عنصر منحصر به‌فردی در S نیست، و این چیزی است که در تعریف نگاشت لازم است. با این حال، اگر f هم ۱-۱ و هم بروی T باشد، f^{-1} واقعاً معرف نگاشتی از T به روی S می‌باشد. (تحقیق کنید!) این امر ما را به ردهٔ بسیار مهمی از نگاشتها خواهد رسانید.

تعریف. گوییم نگاشت $f : S \to T$ یک تناظر ۱-۱ یا بیژکسیون است اگر f هم ۱-۱ و هم برو باشد.

حال که مفهوم نگاشت را داشته و انواع مختلفی از نگاشتها را مشخص کرده‌ایم، ممکن است بپرسیم: «با این نگاشتها چه می‌شود کرد؟» همان‌طور که لحظه‌ای بعد خواهید دید، می‌توان ترکیب نگاشتها را در بعضی از حالات معرفی کرد.

نگاشتهای $g : S \to T$ و $f : T \to U$ را در نظر می‌گیریم. g عنصر $s \in S$ را به عنصر $g(s)$ در T می‌برد؛ پس $g(s)$ آماده است که f بر آن عمل نماید. لذا عنصر $f(g(s)) \in U$ به‌دست می‌آید. حکم می‌کنیم که این روند نگاشتی از S به U به ما می‌دهد. (تحقیق کنید!) این مطلب را به نحوی صوریتر تعریف می‌کنیم:

تعریف. هرگاه $g : S \to T$ و $f : T \to U$، آن‌گاه ترکیب (یا حاصلضرب) آنها، که با $f \circ g$ نموده می‌شود، نگاشت $f \circ g : S \to U$ است که به ازای هر $s \in S$ با $(f \circ g)(s) = f(g(s))$ تعریف می‌شود.

توجه کنید که برای ترکیب دو نگاشت f و g، یعنی برای آنکه $f \circ g$ با معنی باشد، باید مجموعهٔ پایان T نگاشت g مجموعهٔ شروع نگاشت f باشد. یک حالت خاص که همیشه می‌توان دو نگاشت را با هم ترکیب کرد وقتی است که $S = T = U$؛ یعنی وقتی S را به توی خودش می‌نگاریم. این حالت، با وجود خاص بودن، نهایت اهمیت را خواهد داشت.

حال چند خاصیت از ترکیب نگاشتها را ثابت می‌کنیم.

لم ۱.۳.۱. هرگاه $h : S \to T$، $g : T \to U$، و $f : U \to V$، آن‌گاه $f \circ (g \circ h) = (f \circ g) \circ h$.

برهان. این لم را چگونه ثابت کنیم؟ برای اثبات تساوی دو نگاشت کافی است تحقیق کنیم که هر دو اثر یکسانی بر یک عنصر دارند. پیش از همه توجه می‌کنیم که چون هر دوی $f \circ (g \circ h)$ و $(f \circ g) \circ h$ نگاشتهایی از S به V اند، می‌توان راجع به تساوی آنها سخن گفت.

پس باید نشان دهیم که به ازای هر $s \in S$، $(f \circ (g \circ h))(s) = ((f \circ g) \circ h)(s)$. با استفاده از تعریف ترکیب معلوم می‌شود که

$$(f \circ (g \circ h))(s) = f((g \circ h)(s)) = f(g(h(s)))$$

همچنین

$$((f \circ g)) \circ h)(s) = (f \circ g)(h(s)) = f(g(h(s)))$$

لذا، به ازای هر $s \in S$،

$$(f \circ (g \circ h))(s) = ((f \circ g) \circ h)(s)$$

در نتیجه، طبق تعریف، $f \circ (g \circ h) = (f \circ g) \circ h$. ■

این تساوی با گفتن اینکه نگاشتها، تحت ترکیب، در قانون شرکتپذیری صدق می‌کنند توصیف می‌شود. به خاطر این تساوی نیازی به پرانتز نیست؛ در نتیجه $f \circ (g \circ h)$ را به‌صورت $f \circ g \circ h$ می‌نویسیم.

لم ۱.۳.۲. هرگاه $g : S \to T$ و $f : T \to U$ هر دو ۱-۱ باشند، آن‌گاه $f \circ g : S \to U$ نیز ۱-۱ می‌باشد.

برهان. فرض کنیم $(f \circ g)(s_۱) = (f \circ g)(s_۲)$. پس، طبق تعریف، $f(g(s_۱)) = f(g(s_۲))$. چون f یک‌به‌یک است، از این داریم $g(s_۱) = g(s_۲)$. اما g نیز ۱-۱ است. پس نتیجه می‌شود که $s_۱ = s_۲$. چون $(f \circ g)(s_۱) = (f \circ g)(s_۲)$ تساوی $s_۱ = s_۲$ را می‌دهد، نگاشت $f \circ g$ یک‌به‌یک می‌باشد. ■

اثبات تبصرهٔ بعد به خواننده واگذار می‌شود.

تبصره: هرگاه $g : S \to T$ و $f : T \to U$ هر دو برو باشند، آن‌گاه $f \circ g : S \to U$ نیز برو می‌باشد.

یک نتیجهٔ فوری از تبصرهٔ فوق و لم ۱.۳.۲ به قرار زیر است:

لم ۱.۳.۳. هرگاه $g : S \to T$ و $f : T \to U$ هر دو بیژکسیون باشند، آن‌گاه $f \circ g : S \to U$ نیز بیژکسیون است.

هرگاه f یک تناظر ۱-۱ از S به روی T باشد، آن‌گاه به آسانی می‌توان نشان داد که «تابع» $f^{-۱} : T \to S$ که قبلاً تعریف شد یک نگاشت ۱-۱ از T به روی S است. این تابع را معکوس f می‌نامیم. در این وضع داریم:

لم ۱.۳.۴. هرگاه $f : S \to T$ یک بیژکسیون باشد، آن‌گاه $f \circ f^{-۱} = i_T$ و $f^{-۱} \circ f = i_S$ که در آنها i_S و i_T به‌ترتیب نگاشتهای همانی S و T می‌باشند.

برهان. ما یکی از این روابط را تحقیق می‌کنیم. هرگاه $t \in T$، آنگاه

$$(f \circ f^{-1})(t) = f(f^{-1}(t))$$

اما $f^{-1}(t)$ چیست؟ طبق تعریف، $f^{-1}(t)$ آن عنصر $s_\circ \in S$ است که $t = f(s_\circ)$. پس $f(f^{-1}(t)) = f(s_\circ) = t$. به عبارت دیگر، به ازای هر $t \in T$، $(f \circ f^{-1})(t) = t$. لذا $f \circ f^{-1} = i_T$ یعنی نگاشت همانی بر T. ■

اثبات آخرین نتیجهٔ این بخش را به خواننده وا می‌گذاریم.

لم ۱.۳.۵. هرگاه $f : S \to T$ و i_T نگاشت همانی T به روی خرد و i_S نگاشت همانی S به روی خود باشد، آنگاه $i_T \circ f = f$ و $f \circ i_S = f$.

مسائل

مسائل آسانتر

۱. به ازای S و T داده شده، معین کنید که نگاشت $f : S \to T$ به وضوح و خالی از ابهام تعریف شده است یا نه؛ در صورت نشدن، دلیلش را بازگو نمایید.

الف) مجموعهٔ تمام زنان = S، مجموعهٔ تمام مردان = T، شوهر $s = f(s)$.

ب) مجموعهٔ تمام اعداد صحیح مثبت = S، $T = S$، $f(s) = s - ۱$.

پ) مجموعهٔ تمام اعداد صحیح مثبت = S، مجموعهٔ تمام اعداد صحیح نامنفی = T، $f(s) = s - ۱$.

ت) مجموعهٔ تمام اعداد صحیح نامنفی = S، $T = S$، $f(s) = s - ۱$.

ث) مجموعهٔ تمام اعداد صحیح = S، $T = S$، $f(s) = s - ۱$.

ج) مجموعهٔ تمام اعداد حقیقی = S، $T = S$، $f(s) = \sqrt{s}$.

چ) مجموعهٔ تمام اعداد حقیقی مثبت = S، $T = S$، $f(s) = \sqrt{s}$.

۲. در قسمتهایی از مسئلهٔ ۱ که f یک تابع است، ۱-۱، برو، یا هر دو بودن آن را مشخص سازید.

۳*. اگر f یک نگاشت ۱-۱ از S به روی T باشد، ثابت کنید f^{-1} یک نگاشت ۱-۱ از T به روی S می‌باشد.

۴*. اگر f یک نگاشت ۱-۱ از S به روی T باشد، ثابت کنید $f^{-1} \circ f = i_S$.

۵. تبصرهٔ بعد از لم ۱.۳.۲ را ثابت کنید.

۶*. اگر $f : S \to T$ برو بوده و $g : T \to U$ و $h : T \to U$ چنان باشند که $g \circ f = h \circ f$، ثابت کنید $g = h$.

۷*. فرض کنید $g : S \to T$، $h : S \to T$، و $f : T \to U$ یک‌به‌یک باشد. نشان دهید هرگاه $f \circ g = f \circ h$، آن‌گاه $g = h$.

۸. فرض کنید S مجموعهٔ تمام اعداد صحیح بوده و $T = \{۱, -۱\}$. $f : S \to T$ را با $f(s) = ۱$ اگر s زوج باشد و $f(s) = -۱$ اگر s فرد باشد تعریف می‌کنیم.

الف) آیا این f یک تابع از S به T است؟

ب) نشان دهید که $f(s_۱ + s_۲) = f(s_۱)f(s_۲)$. این رابطه چه چیز در باب اعداد صحیح می‌گوید؟

پ) آیا $f(s_۱ s_۲) = f(s_۱)f(s_۲)$ نیز صحیح است؟

۹. فرض کنید S مجموعهٔ تمام اعداد حقیقی باشد. $f : S \to S$ را با $f(s) = s^۲$ و $g : S \to S$ را با $g(s) = s + ۱$ تعریف کنید.

الف) $f \circ g$ را بیابید.

ب) $g \circ f$ را بیابید.

پ) آیا $f \circ g = g \circ f$؟

۱۰. فرض کنید S مجموعهٔ تمام اعداد حقیقی بوده و به ازای هر $a, b \in S$ که $a \neq ۰$، تعریف کنید $f_{a,b}(s) = as + b$.

الف) نشان دهید که به ازای اعدادی حقیقی مانند u و v، $f_{a,b} \circ f_{c,d} = f_{u,v}$. u و v را صریحاً برحسب a، b، c، و d بیابید.

ب) آیا همیشه $f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b}$؟

پ) تمام $f_{a,b}$هایی را بیابید که $f_{a,b} \circ f_{۱,۱} = f_{۱,۱} \circ f_{a,b}$.

ت) نشان دهید که $f_{a,b}^{-۱}$ موجود است و شکلش را بیابید.

۱۱. فرض کنید S مجموعهٔ تمام اعداد صحیح مثبت باشد. $f : S \to S$ را با $f(۱) = ۲$، $f(۲) = ۳$، $f(۳) = ۱$، و به ازای هر $s \in S$ دیگر، با $f(s) = s$ تعریف کرده و نشان دهید که $f \circ f \circ f = i_S$. در این حالت $f^{-۱}$ چیست؟

مسائل با سطح متوسط

۱۲. فرض کنید S مجموعهٔ تمام اعداد گویای نامنفی باشد؛ یعنی

$$S = \{m/n \mid n \neq ۰ \text{ و } m \text{ و } n \text{ اعداد صحیح نامنفی بوده}\}$$

و T مجموعهٔ تمام اعداد صحیح باشد.

الف) آیا $f : S \to T$ تعریف شده با $f(m/n) = 2^m 3^n$ معرف یک تابع از S به T است؟

ب) در غیر این صورت، چطور می‌توان تعریف f را اصلاح کرد تا تابع به‌دست آید؟

۱۳. فرض کنید S مجموعهٔ تمام اعداد صحیح مثبت به شکل $2^m 3^n$ باشد که در آن $m > 0$ و $n > 0$، و T مجموعهٔ تمام اعداد گویا باشد. $f : S \to T$ را با $f(2^m 3^n) = m/n$ تعریف می‌کنیم. ثابت کنید f معرف تابعی از S به T است. (این امر به چه خواصی از اعداد صحیح وابسته است؟)

۱۴. فرض کنید $f : S \to S$ (که در آن S مجموعهٔ تمام اعداد صحیح است) با $f(s) = as+b$ تعریف شده باشد که در آن a و b صحیح می‌باشند. شرایط لازم و کافی بر a و b جهت برقراری $f \circ f = i_S$ را بیابید.

۱۵. جمیع fها به شکل مسئلهٔ ۱۴ را که $f \circ f \circ f = i_S$ پیدا نمایید.

۱۶. اگر f یک نگاشت ۱-۱ از S به روی خود باشد، نشان دهید که $(f^{-1})^{-1} = f$.

۱۷. اگر S مجموعه‌ای متناهی و دارای $m > 0$ عنصر باشد، چند نگاشت از S به توی خود وجود دارد؟

۱۸. در مسئلهٔ ۱۷ چند نگاشت ۱-۱ از S به توی خود وجود دارد؟

۱۹. فرض کنید S مجموعهٔ تمام اعداد حقیقی بوده و $f : S \to S$ با $f(s) = s^2 + as + b$ تعریف شده باشد که در آن a و b اعداد حقیقی ثابتی می‌باشند. ثابت کنید f به ازای هیچ مقداری از a و b برو یا ۱-۱ نیست.

۲۰. فرض کنید S مجموعهٔ تمام اعداد حقیقی مثبت باشد. آیا ممکن است به ازای اعداد حقیقی a، b، c، d و c و d مثبت، «نگاشت» $f : S \to S$ تعریف شده با $f(s) = (as+b)/(cs+d)$ در رابطهٔ $f \circ f = i_S$ صدق کند؟ جمیع a و b و c و dهای صادق در این امر را بیابید. آیا f یک نگاشت از S به توی خود است؟

۲۱. فرض کنید S مجموعهٔ تمام اعداد گویا بوده و $f_{a,b} : S \to S$ با $f_{a,b}(s) = as + b$ تعریف شده باشد، که در آن $a \neq 0$ و b اعدادی گویا باشند. جمیع $f_{c,d}$ها به این شکل را بیابید که به ازای هر $f_{a,b}$،

$$f_{c,d} \circ f_{a,b} = f_{a,b} \circ f_{c,d}$$

۲۲. فرض کنید S مجموعهٔ تمام اعداد صحیح و a و b و c اعدادی گویا باشند. $f : S \to S$

را با $f(s) = as^2 + bs + c$ تعریف کرده و شرایط لازم و کافی بر a و b و c را طوری بیابید که f معرف یک نگاشت بر S باشد. [تذکر: لازم نیست a و b و c اعدادی صحیح باشند؛ مثلاً $f(s) = \frac{1}{2}s(s+1) = \frac{1}{2}s^2 + \frac{1}{2}s$ به ازای s صحیح همواره عددی صحیح به ما می‌دهد.]

مسائل مشکلتر

۲۳. فرض کنید S مجموعهٔ تمام اعداد صحیح به شکل $2^m 3^n$ باشد که در آن $m \geq 0$ و $n \geq 0$، و T مجموعهٔ تمام اعداد صحیح مثبت باشد. نشان دهید یک تناظر ۱-۱ از S به روی T موجود است.

۲۴. ثابت کنید یک تناظر ۱-۱ از مجموعهٔ تمام اعداد صحیح مثبت به روی مجموعهٔ تمام اعداد گویای مثبت وجود دارد.

۲۵. فرض کنید S مجموعهٔ تمام اعداد حقیقی و T مجموعهٔ تمام اعداد حقیقی مثبت باشد. نگاشت یک‌به‌یک f از S به روی T را چنان بیابید که به ازای هر $s_1, s_2 \in S$،

$$f(s_1 + s_2) = f(s_1)f(s_2)$$

۲۶. در مسئلهٔ ۲۵، f^{-1} را به‌طور صریح بیابید.

۲۷. هرگاه f و g نگاشتهایی از S به توی S بوده و $f \circ g$ یک تابع ثابت باشد، آن‌گاه

الف) اگر g برو باشد، راجع به f چه می‌شود گفت؟

ب) اگر f یک‌به‌یک باشد، راجع‌به g چه می‌شود گفت؟

۲۸. اگر S مجموعه‌ای متناهی و f نگاشتی از S به‌روی خود باشد، نشان دهید f باید ۱-۱ باشد.

۲۹. اگر S مجموعه‌ای متناهی و f نگاشتی ۱-۱ از S به توی خود باشد، نشان دهید f باید برو باشد.

۳۰. اگر S مجموعه‌ای متناهی و f نگاشتی ۱-۱ از S باشد، نشان دهید به ازای عدد صحیحی چون $n > 0$،

$$\underbrace{f \circ f \circ f \circ \cdots \circ f}_{n \text{ بار}} = i_S$$

۳۱. اگر S مسئلهٔ ۳۰ دارای m عنصر باشد، $n > 0$ ی (برحسب m) بیابید که به ازای جمیع نگاشتهای ۱-۱ از S به توی خود کارا باشد.

۴. $A(S)$ (مجموعهٔ نگاشتهای ۱-۱ از S به روی خود)

در این بخش توجه ما به نگاشتهایی خاص از مجموعهٔ ناتهی S به توی خود است؛ یعنی مجموعهٔ $A(S)$ مرکب از تمام نگاشتهای ۱-۱ از S به روی خود را در نظر می‌گیریم. با آنکه اغلب توجه ما در این کتاب به S متناهی است، در اینجا خود را به این حالت محدود نمی‌کنیم.

هرگاه S تعدادی متناهی (مثلاً n) عنصر داشته باشد، آن‌گاه $A(S)$ نامی خاص دارد. این نام عبارت است از گروه متقارن از درجهٔ n و اغلب با S_n نموده می‌شود. عناصر S_n جایگشتهای S نامیده می‌شوند. اگر به ساختار S_n علاقه‌مند باشیم، مجموعهٔ زمینهٔ S اهمیتی نخواهد داشت. لذا S را می‌توان مجموعهٔ $\{۱, \ldots, n\}$ انگاشت. فصل ۳ به مطالعهٔ نسبتاً عمیق S_n اختصاص یافته است. S_n در بررسی گروههای متناهی نقش اصلی را به‌عهده خواهد داشت.

مجموعهٔ $A(S)$ خواص بسیار دارد که می‌توان بدانها توجه کرد. ما در اینجا به جنبه‌هایی از آن می‌پردازیم که انگیزهٔ مفهوم گروه بوده و به خواننده تجربه و احساس کار در چهارچوب نظریهٔ گروهها را می‌بخشند. گروهها در فصل ۲ مطرح خواهند شد.

بحث را با نتیجه‌ای که در واقع فشردهٔ چند نتیجهٔ به‌دست آمده در بخش ۳ است آغاز می‌کنیم.

لم ۱.۴.۱. $A(S)$ از خواص زیر برخوردار است:

الف) $f, g \in A(S)$ ایجاب می‌کند که $f \circ g \in A(S)$؛

ب) $f, g, h \in A(S)$ ایجاب می‌کند که $(f \circ g) \circ h = f \circ (g \circ h)$؛

پ) عنصری (نگاشت همانی i) وجود دارد به‌طوری که به ازای هر $f \in A(S)$، $f \circ i = i \circ f = f$؛

ت) به ازای $f \in A(S)$ عنصری مانند $g \in A(S)$ $(g = f^{-۱})$ هست به‌طوری که $f \circ g = g \circ f = i$.

برهان. همهٔ این مطالب در بخش ۳ (در متن یا در مسائل) مطرح شده‌اند. بر خواننده است که اثبات احکام (الف) تا (ت) را در بخش ۳ پیدا نماید. ■

حال می‌خواهیم بدانیم اگر S مجموعه‌ای متناهی با n عنصر باشد، تعداد عناصر $A(S)$ چندتاست. برای این کار قدری از بحث منحرف می‌شویم.

فرض کنید بتوانیم کاری را به r طریق و کار دیگر را به s طریق انجام دهیم. به چند طریق می‌توان هر دو کار را با هم انجام داد؟ بهترین راه تجسم این امر در محدوده‌ای ملموس است. فرض کنیم از شیکاگو تا دیترویت r بزرگراه و از دیترویت تا آن آربر s بزرگراه موجود باشد. به چند طریق

می‌توان ابتدا به دیترویت و سپس به آن آربر رفت؟ واضح است که به ازای هر جاده که از شیکاگو به دیترویت اختیار شود، به s طریق می‌توان به آن آربر رفت. چون به r طریق می‌توان از شیکاگو حرکت کرد، پس به

$$\underbrace{s + s + s + \ldots + s}_{\text{بار } r} = rs$$

طریق می‌توان سفر را به پایان رسانید.

روشن است که این امر را می‌توان از دو کار مستقل به m کار مستقل، که m عدد صحیحی بزرگتر از ۲ است، تعمیم داد. هرگاه بتوان کار اول را به r_1 طریق، کار دوم را به r_2 طریق، ... ، و کار m م را به r_m طریق صورت داد، آن‌گاه همهٔ این کارها را می‌توان به $r_1 r_2 \cdots r_m$ طریق انجام داد.

حال نکته‌ای را یادآور می‌شویم که بسیاری از ما قبلاً آن را دیده‌ایم:

تعریف. هرگاه $n \geq 1$ یک عدد صحیح مثبت باشد، آن‌گاه $n!$ (بخوانید: «n فاکتوریل») با $n! = 1 \cdot 2 \cdot 3 \cdots n$ تعریف می‌شود.

لم ۲.۴.۱. هرگاه S دارای n عنصر باشد، آن‌گاه $A(S)$ دارای $n!$ عنصر است.

برهان. فرض کنیم $f \in A(S)$ که در آن $S = \{x_1, x_2, \ldots, x_n\}$. f به چند طریق می‌تواند x_1 را به جایی بفرستد؟ واضح است که به n طریق، زیرا می‌توان x_1 را تحت f به هر عنصر S فرستاد. ولی f دیگر مجاز نیست که x_2 را به هر جا بفرستد، زیرا چون f یک‌به‌یک است، باید داشته باشیم $f(x_1) \neq f(x_2)$. لذا می‌توان x_2 را به هر جا جز $f(x_1)$ فرستاد. پس f می‌تواند x_2 را به $n - 1$ نقش مختلف بفرستد. با ادامهٔ این وضع خواهیم دید که f می‌تواند x_i را به $n - (i - 1)$ نقش مختلف بفرستد. در نتیجه تعداد این fها مساوی است با $n(n-1)(n-2)\cdots 1 = n!$. ■

مثال. عدد $n!$ به سرعت بزرگ می‌شود. برای مشاهدهٔ کل کار، به حالت خاص $n = 3$، که هنوز $n!$ کوچک است، نظر می‌افکنیم.

$A(S) = S_3$ را در نظر می‌گیریم که در آن S از سه عنصر x_1، x_2، و x_3 تشکیل شده است. تمام عناصر S_3 را ذکر کرده و هر نگاشت را صریحاً با عملش بر هر x_1، x_2، و x_3 می‌نویسیم:

۱. $i : x_1 \to x_1, x_2 \to x_2, x_3 \to x_3$.

۲. $f: x_1 \to x_2, x_2 \to x_3, x_3 \to x_1$.

۳. $g: x_1 \to x_2, x_2 \to x_1, x_3 \to x_3$.

۴. $g \circ f: x_1 \to x_1, x_2 \to x_3, x_3 \to x_2$. (تحقیق کنید!)

۵. $f \circ g: x_1 \to x_3, x_2 \to x_2, x_3 \to x_1$. (تحقیق کنید!)

۶. $f \circ f: x_1 \to x_3, x_2 \to x_1, x_3 \to x_2$. (تحقیق کنید!)

چون شش عنصر متمایز S_3 را ذکر کرده‌ایم و S_3 فقط شش عنصر دارد، پس تمام عناصر S_3 لیست شده‌اند. این لیست به ما چه خواهد گفت؟ ابتدا توجه می‌کنیم که $f \circ g \neq g \circ f$؛ پس یکی از قواعد آشنای حساب نقض می‌شود. چون $g \in S_3$ و $g \in S_3$، باید $g \circ g$ نیز در S_3 باشد. این عنصر چیست؟ اگر $g \circ g$ را حساب کنیم، به آسانی معلوم می‌شود که $g \circ g = i$. به همین نحو به‌دست می‌آوریم

$$(f \circ g) \circ (f \circ g) = i = (g \circ f) \circ (g \circ f)$$

همچنین توجه کنید که $f \circ (f \circ f) = i$؛ پس $f \circ f = f^{-1}$. بالاخره، برخواننده است نشان دهد که $g \circ f = f^{-1} \circ g$.

نوشتن این ضرب در $A(S)$ با استفاده از $\circ$ کمی زحمت دارد. از حالا به بعد آن را حذف کرده و $f \circ g$ را فقط به‌صورت fg می‌نویسیم. همچنین نماییها را به‌صورت فشرده نوشته و از عباراتی چون $f \circ f \circ f \circ \ldots \circ f$ پرهیز می‌کنیم. به ازای $f \in A(S)$ تعریف می‌کنیم $f^0 = i$، $f^2 = f \circ f = ff$، و از این قبیل. به ازای نماهای منفی $-n$، f^{-n} را با $f^{-n} = (f^{-1})^n$ تعریف می‌کنیم که در آن n یک عدد صحیح مثبت است. قواعد معمول نماها، یعنی $f^r f^s = f^{r+s}$ و $(f^r)^s = f^{rs}$، برقرارند. اثبات این قواعد، که تا حدودی خسته‌کننده است، به خواننده واگذار می‌شود.

مثال. نباید نتیجه گرفت که جمیع خواص آشنای نماییها برقرارند. مثلاً، در مورد $f, g \in S_3$ تعریف شده در فوق، حکم می‌کنیم که $(fg)^2 \neq f^2 g^2$. برای مشاهدهٔ این امر توجه می‌کنیم که

$$fg: x_1 \to x_3, x_2 \to x_2, x_3 \to x_1;$$

در نتیجه $(fg)^2: x_1 \to x_1, x_2 \to x_2, x_3 \to x_3$؛ یعنی $(fg)^2 = i$. از آن سو، $f^2 \neq i$ و $g^2 = i$. پس $f^2 g^2 = f^2 \neq i$، که از آن در این حالت داریم $(fg)^2 \neq f^2 g^2$.

با این‌حال بعضی از خواص آشنا برقرارند. مثلاً، اگر f و g و h در $A(S)$ بوده و $fh = fg$، داریم $g = h$. چرا؟ چون‌که از $fg = fh$ داریم $f^{-1}(fg) = f^{-1}(fh)$. پس

$$g = ig = (f^{-1}f)g = f^{-1}(fg) = f^{-1}(fh) = (f^{-1}f)h = ih = h$$

به همین نحو $gf = hf$ ایجاب می‌کند که $g = h$. لذا در یک چنین معادله می‌توانیم عنصری را حذف کنیم مشروط بر اینکه طرفها را تغییر ندهیم. در S_3، f و g در $gf = f^{-1}g$ صدق می‌کنند، ولی چون $f \neq f^{-1}$، نمی‌توانیم g را حذف نماییم.

مسائل

به یاد آورید که fg یعنی $f \circ g$ و معنی f^m را نیز به خاطر بیاورید. S بدون زیرنویس یعنی یک مجموعهٔ ناتهی.

مسائل آسانتر

۱. اگر $s_1 \neq s_2$ در S باشند، نشان دهید که یک $f \in A(S)$ هست به‌طوری که $f(s_1) = s_2$.

۲. به ازای $s_1 \in S$ قرار دهید $H = \{f \in A(S) | f(s_1) = s_1\}$. نشان دهید که
الف) $i \in H$؛
ب) هرگاه $f, g \in H$، آن‌گاه $fg \in H$؛
پ) هرگاه $f \in H$، آن‌گاه $f^{-1} \in H$.

۳. فرض کنید $s_1 \neq s_2$ در S بوده و $f(s_1) = s_2$ که در آن $f \in A(S)$. در این صورت، اگر H همانند مسئلهٔ ۲ بوده و $K = \{g \in A(S) | g(s_2) = s_2\}$، نشان دهید
الف) هرگاه $g \in K$، آن‌گاه $f^{-1}gf \in H$؛
ب) هرگاه $h \in H$، آن‌گاه $g \in K$ای هست به طوری که $h = f^{-1}gf$.

۴. اگر $f, g, h \in A(S)$، نشان دهید که $(f^{-1}gf)(f^{-1}hf) = f^{-1}(gh)f$.
در باب $(f^{-1}gf)^n$ چه می‌شود گفت؟

۵. اگر $f, g \in A(S)$ و $fg = gf$، نشان دهید که
الف) $(fg)^2 = f^2g^2$؛
ب) $(fg)^{-1} = f^{-1}g^{-1}$.

۶. مسئلهٔ ۵ را پیش برده و به ازای همان f و g و جمیع اعداد صحیح m نشان دهید که $(fg)^m = f^m g^m$.

۷*. قواعد نماها، یعنی $f^r f^s = f^{r+s}$ و $(f^r)^s = f^{rs}$، را به ازای $f \in A(S)$ و اعداد صحیح مثبت r و s تحقیق نمایید.

۸. اگر $f, g \in A(S)$ و $(fg)^2 = f^2 g^2$، ثابت کنید $fg = gf$.

۹. اگر $S = \{x_1, x_2, x_3, x_4\}$، $f, g \in S_4$ را به‌صورت

$$f : x_1 \to x_2, x_2 \to x_3, x_3 \to x_4, x_4 \to x_1$$

و

$$g : x_1 \to x_2, x_2 \to x_1, x_3 \to x_3, x_4 \longrightarrow x_4$$

تعریف و عبارات زیر را حساب کنید:

الف) f^2, f^3, f^4؛

ب) g^2, g^3؛

پ) fg؛

ت) gf؛

ث) $(fg)^3, (gf)^3$.

ج) آیا fg و gf مساویند؟

۱۰. اگر $f \in S_3$، نشان دهید که $f^6 = i$.

۱۱. آیا می‌توان عدد صحیح مثبتی مانند m را چنان یافت که به ازای هر $f \in S_4$، $f^m = i$.

مسائل با سطح متوسط

۱۲*. اگر $f \in S_n$، نشان دهید که عدد صحیح مثبتی مانند k (تابع f) وجود دارد که $f^k = i$. (راهنمایی. توانهای مثبت f را در نظر بگیرید.)

۱۳*. نشان دهید که یک عدد صحیح مثبت مانند t هست به‌طوری که به ازای هر $f \in S_n$، $f^t = i$.

۱۴. اگر $m < n$، نشان دهید یک تابع ۱-۱ مانند $F : S_m \longrightarrow S_n$ هست به‌طوری که به ازای هر $f, g \in S_m$، $F(fg) = F(f)F(g)$.

۱۵. اگر S سه یا بیش از سه عنصر داشته باشد، نشان دهید که می‌توان $f, g \in A(S)$ را چنان یافت که $fg \neq gf$.

۱۶. فرض کنید S یک مجموعهٔ نامتناهی بوده و $M \subset A(S)$ مجموعهٔ تمام عناصری چون $f \in A(S)$ باشد که به ازای حداکثر تعدادی متناهی $s \in S$، $f(s) \neq s$. ثابت کنید

الف) $f, g \in M$ ایجاب می‌کنند که $fg \in M$؛

ب) $f \in M$ ایجاب می‌کند که $f^{-۱} \in M$.

۱۷. در مسئلهٔ ۱۶ نشان دهید که اگر $f \in A(S)$، $f^{-۱}Mf = \{f^{-۱}gf | g \in M\}$ باید مساوی M باشد.

۱۸. فرض کنید $T \subset S$ و زیرمجموعهٔ $U(T) = \{f \in A(S) | f(t) \in T$، به ازای هر $t \in T\}$ را در نظر بگیرید. نشان دهید که

الف) $i \in U(T)$؛

ب) $f, g \in U(T)$ ایجاب می‌کنند که $fg \in U(T)$.

۱۹. اگر S مسئلهٔ ۱۸ دارای n عنصر و T دارای m عنصر باشد، چند عنصر در $U(T)$ وجود دارد؟ نشان دهید که یک نگاشت مانند $F : U(T) \to S_m$ هست به‌طوری که به ازای $f, g \in U(T)$، $F(fg) = F(f)F(g)$ و F به روی S_m می‌باشد.

۲۰. اگر $m < n$، آیا F مسئلهٔ ۱۹ هیچگاه می‌تواند ۱-۱ باشد؟ اگر چنین است، چه وقت؟

۲۱. در S_n نشان دهید که نگاشت f تعریف شده با

$$f : x_۱ \to x_۲, x_۲ \to x_۳, x_۳ \to x_۴, \ldots, x_{n-۱} \to x_n, x_n \to x_۱$$

[یعنی $f(x_i) = x_{i+۱}$ اگر $i < n$، $f(x_n) = x_۱$] را می‌توان به‌صورت $f = g_۱g_۲ \ldots g_{n-۱}$ نوشت که در آن هر $g_i \in S_n$ درست دو عنصر از $S = \{x_۱, \ldots, x_n\}$ را با هم تعویض کرده سایر عناصر S را ثابت می‌گذارد.

مسائل مشکلتر

۲۲. اگر $f \in S_n$، نشان دهید که به ازای $h_j \in S_n$هایی که $h_j^۲ = i$، $f = h_۱h_۲ \ldots h_m$.

۲۳*. یک عنصر در S_n را ترانهش نامیم اگر دو عنصر را با هم تعویض کرده و سایرین را ثابت بگذارد. نشان دهید که هر عنصر در S_n حاصلضربی از ترانهشها می‌باشد (این امر مسئلهٔ ۲۲ را قویتر خواهد ساخت.)

۲۴. اگر n دست‌کم ۳ باشد، نشان دهید که به ازای fی در S_n، f را نمی‌توان به ازای هیچ gای در S_n به شکل $f = g^۳$ نوشت.

۲۵. اگر $f \in S_n$ چنان باشد که $f \neq i$ ولی $f^۳ = i$، نشان دهید که می‌توان عناصر S را طوری شماره‌گذاری کرد که $f(x_۱) = x_۲$، $f(x_۲) = x_۳$، $f(x_۳) = x_۱$، $f(x_۴) = x_۵$،

$f(x_5) = x_6$، $f(x_6) = x_4$، $\cdots$، $f(x_{3k+1}) = x_{3k+2}$، $f(x_{3k+2}) = x_{3k+3}$،
$f(x_{3k+3}) = x_{3k+1}$ به ازای kای، و به ازای سایر $x_t \in S$ها، $f(x_t) = x_t$.

۲۶. یک دسته کارت ۵۲ ورقی را پس از برزدن ثابت گرفته و آن را یک نگاشت ۱-۱ به روی خود در نظر بگیرید. نشان دهید که اگر آن را تعدادی متناهی (مثبت) بار بر بزنیم، دسته کارت به ترتیب اصلی‌اش باز خواهد گشت.

*۲۷. اگر $f \in A(S)$ و $s \in S$، مجموعهٔ $O(s) = \{f^j(s) | j$ تمام اعداد صحیح$\}$ را مدار s (نسبت به f) می‌نامیم. نشان دهید هرگاه $s, t \in S$، آن‌گاه $O(s) \cap O(t) = \varnothing$ یا $O(s) = O(t)$.

۲۸. هرگاه $S = \{x_1, x_2, \ldots, x_{12}\}$ و $f \in S_{12}$ با $f(x_i) = x_{i+1}$ اگر $i = 1, 2, \ldots, 11$ و $f(x_{12}) = x_1$ تعریف شده باشد، آن‌گاه مدارهای جمیع عناصر S (نسبت به f) را بیابید.

۲۹. اگر $f \in A(S)$ در رابطهٔ $f^3 = i$ صدق کند، نشان دهید که مدار هر عنصر S یک یا سه عنصر خواهد داشت.

*۳۰. به یاد آورید که عدد صحیح و مثبت $p > 1$ را یک عدد اول نامیم اگر p را نتوان به‌صورت حاصلضربی از اعداد صحیح مثبت کوچکتر تجزیه کرد. اگر $f \in A(S)$ در رابطهٔ $f^p = i$ صدق کند، راجع به اندازهٔ مدارهای عناصر S نسبت به f چه می‌شود گفت؟ برای رسیدن به جواب از چه خاصیتی از اعداد اول استفاده می‌کنید؟

۳۱. ثابت کنید هرگاه S بیش از دو عنصر داشته باشد، آن‌گاه تنها عناصر $f_\circ$ در $A(S)$ که به ازای هر $f \in A(S)$ رابطهٔ $f_\circ f = f f_\circ$ را برقرار می‌سازند باید در $f_\circ = i$ صدق نمایند.

*۳۲. گوییم $g \in A(S)$ با $f \in A(S)$ تعویض می‌شود اگر $fg = gf$. جمیع عناصری در $A(S)$ را بیابید که با $f : S \to S$ تعریف شده به‌وسیلهٔ $f(x_1) = x_2$، $f(x_2) = x_1$، و $f(s) = s$ اگر $s \neq x_1, x_2$ تعویض گردند.

۳۳. در S_n نشان دهید که تنها عناصری که با f تعریف شده به‌وسیلهٔ $f(x_i) = x_{i+1}$ اگر $i < n$ و $f(x_n) = x_1$ تعویض می‌شوند عبارتند از توانهای f یعنی $i = f^\circ, f, f^2, \ldots, f^{n-1}$.

۳۴. به فرض آنکه $C(f) = \{g \in A(S) | fg = gf\}$، ثابت کنید

الف) $g, h \in C(f)$ ایجاب می‌کنند که $gh \in C(f)$؛

ب) $g \in C(f)$ ایجاب می‌کند که $g^{-1} \in C(f)$؛

پ) $C(f)$ تهی نیست.

۵. اعداد صحیح

یک مجموعهٔ ریاضی که همه با آن آشنایی دارند مجموعهٔ اعداد صحیح مثبت ...,۲,۱ است که اغلب آن را N می‌نامیم. به همین اندازه آشنا مجموعهٔ تمام اعداد صحیح (مثبت، منفی، و صفر) $\mathbb{Z}$ می‌باشد. در اینجا (به خاطر این آشنایی با $\mathbb{Z}$) خواصی از آن را که اغلب در اثبات مطالب به کار خواهیم برد مرور می‌کنیم. اکثر این خواص بر همهٔ ما معلوم‌اند؛ فقط معدودی از آنها کمتر معلوم می‌باشند.

فرض اصلی ما راجع به مجموعهٔ اعداد صحیح به قرار زیر است:

اصل خوش ترتیبی. هر مجموعهٔ ناتهی از اعداد صحیح نامنفی کوچکترین عضو دارد.

این اصل به طور صوری می‌گوید که به ازای هر مجموعهٔ ناتهی V از اعداد صحیح نامنفی عنصری مانند $v_\circ \in V$ هست که به ازای هر $v \in V$، $v_\circ \leq v$. این اصل مبنای بحثی است که اینک راجع به اعداد صحیح مطرح می‌کنیم.

اولین کاربرد ما از این اصل اثبات مطلبی است که همهٔ ما بدان واقفیم؛ یعنی یک عدد صحیح را می‌توان بر دیگری بخش کرد و باقیماندهٔ کوچکتر به‌دست آورد. این امر به الگوریتم اقلیدس (Euclid) معروف است. این مطلب را به‌طور صوریتر بیان کرده و آن را بر اساس خوش ترتیبی به ثبوت می‌رسانیم.

قضیهٔ ۱.۵.۱(الگوریتم اقلیدس). هرگاه m و n اعدادی صحیح بوده و $n > \circ$، آن‌گاه اعداد صحیحی مانند q و r وجود دارند به‌طوری که $\circ \leq r < n$ و $m = qn+r$.

برهان. فرض کنیم W مجموعهٔ تمام $m - tn$هایی باشد که t همهٔ اعداد صحیح را می‌گیرد (یعنی $W = \{m - tn | t \in \mathbb{Z}\}$). حکم می‌کنیم که W شامل اعدادی صحیح و نامنفی است، چراکه اگر t به قدرکافی بزرگ و منفی باشد، $m - tn > \circ$. فرض کنیم $V = \{v \in W | v \geq \circ\}$. بنابر اصل خوش ترتیبی، V دارای کوچکترین عنصر مانند r است. چون $r \in V$، $r \geq \circ$، و به ازای qای، $r = m - qn$ (زیرا این شکل تمام عناصر $V \subset W$ است). حکم می‌کنیم که $r < n$. در غیر این صورت، $r = m - qn \geq n$؛ پس $m - (q + ۱)n \geq \circ$. ولی $m - (q + ۱)n$ در V بوده و $m - (q + ۱)n < r$ که با مینیمم بودن r در V در تضاد است. بدین ترتیب الگوریتم اقلیدس به اثبات می‌رسد. ■

الگوریتم اقلیدس نتایج بسیاردارد به‌خصوص در باب بخشپذیری. چون سخن راجع به اعداد

صحیح است، فرض می‌کنیم همهٔ حروف در این بخش اعداد صحیح باشند. این امر از تکرار برخی عبارات جلوگیری خواهد کرد.

تعریف. گوییم عدد صحیح $m \neq 0$ عدد صحیح n را عاد می‌کند، و می‌نویسیم $m|n$، اگر به ازای عدد صحیحی چون c، $n = cm$.

مثلاً ۱۴|۲، ۱۴|(۷−)، و (۱۶−)|۴. اگر $m|n$، m را یک مقسوم‌علیه یا عامل n و n را یک مضرب m می‌نامیم. اگر m یک مقسوم علیه n نباشد، می‌نویسیم $m \nmid n$، مثلاً ۳ ∤ ۵.

خواص مقدماتی و اصلی بخشپذیری در لم زیر آمده‌اند.

لم ۱.۵.۲. احکام زیر برقرارند:

الف) به ازای هر n، $1|n$؛

ب) هرگاه $m \neq 0$، آن‌گاه $m|0$؛

پ) هرگاه $m|n$ و $n|q$، آن‌گاه $m|q$؛

ت) هرگاه $m|n$ و $m|q$، آن‌گاه به ازای هر u و v، $m|(un + vq)$؛

ث) هرگاه $m|1$، آن‌گاه $m = 1$ یا $m = -1$؛

ج) هرگاه $m|n$ و $n|m$، آن‌گاه $m = \pm n$.

برهان. اثبات این احکام آسان بوده و فوراً از تعریف $m|n$ نتیجه می‌شوند. ما همهٔ قسمتها جز (ت) را به‌عنوان تمرین گذارده و قسمت (ت) را به‌صورت نمونه ثابت می‌کنیم.

فرض کنیم $m|n$ و $m|q$. پس به ازای c و dای $n = cm$ و $q = dm$. بنابراین $un + vq = u(cm) + v(dm) = (uc + vd)m$. لذا از تعریف خواهیم داشت $m|(un + vq)$.

■

حال، با داشتن مقسوم‌علیه یک عدد صحیح، بزرگترین مقسوم‌علیه مشترک دو (یا چند) عدد صحیح را معرفی می‌کنیم. این عدد بزرگترین عدد صحیحی است که مقسوم‌علیه هر دو عدد صحیح مربوطه می‌باشد. به دلایلی که بعدها دربحث حلقه‌ها معلوم می‌شوند، می‌خواهیم از به‌کارگیری اندازهٔ یک عدد صحیح پرهیز کنیم. لذا، تعریفی می‌آوریم که به نحوی عجیب می‌نماید.

تعریف. فرض کنیم a و b هر دو 0 نباشند. در این صورت بزرگترین مقسوم‌علیه مشترک آنها c این‌طور تعریف می‌شود:

الف) $c > 0$؛

ب) $c|a$ و $c|b$؛

پ) هرگاه $d|a$ و $d|b$، آن‌گاه $d|c$.

این c را به‌صورت $c = (a, b)$ می‌نویسیم.

به‌عبارت دیگر، بزرگترین مقسوم‌علیه مشترک a و b عدد مثبتی مانند c است که a و b را عاد کرده و بر هر d که a و b را عاد کند بخشپذیر است.

تعریف یک شیء وجود آن را تضمین نمی‌کند. لذا مجبوریم وجود (a, b) و یکتایی آن را ثابت کنیم. اثبات عملاً بیش از این را نشان می‌دهد، یعنی اینکه (a, b) ترکیب زیبایی از a و b است. این ترکیب منحصر به‌فرد نیست؛ مثلاً

$$(۲۴, ۹) = ۳ = ۳ \cdot ۹ + (-۱)۲۴ = (-۵)۹ + ۲ \cdot ۲۴$$

قضیهٔ ۳.۵.۱. هرگاه a و b هر دو ۰ نباشند، آن‌گاه بزرگترین مقسوم‌علیه مشترکشان $c = (a, b)$ موجود و منحصر به‌فرد است و، به‌علاوه، به ازای $m_\circ$ و $n_\circ$ مناسبی، $c = m_\circ a + n_\circ b$.

برهان. چون a و b هر دو ۰ نیستند، مجموعهٔ $A = \{ma + nb | m, n \in \mathbb{Z}\}$ عنصر ناصفر دارد. هرگاه $x \in A$ و $x < ۰$، آن‌گاه $-x$ نیز در A بوده و $-x > ۰$، زیرا هرگاه $x = m_۱ a + n_۱ b$، آن‌گاه $-x = (-m_۱)a + (-n_۱)b$ و در نتیجه در A می‌باشد. لذا A دارای عناصر مثبت است. پس، طبق اصل خوش‌ترتیبی، A کوچکترین عنصر مثبتی مانند c دارد. چون $c \in A$، بنابر شکل عنصرهای A، به ازای $m_\circ$ و $n_\circ$ی $c = m_\circ a + n_\circ b$.

حکم می‌کنیم که c بزرگترین مقسوم‌علیه مشترک مطلوب است. ابتدا توجه می‌کنیم که اگر $d|a$ و $d|b$، بنابر قسمت (ت) لم ۲.۵.۱، $d|(m_\circ a + n_\circ b)$؛ یعنی $d|c$. لذا c در صورتی عنصر مطلوب است که نشان دهیم $c|a$ و $c|b$.

بنابر الگوریتم اقلیدس، $a = qc + r$ که در آن $۰ \leq r < c$؛ یعنی $a = q(m_\circ a + n_\circ b) + r$. لذا $r = -qn_\circ b + (۱ - qm_\circ)a$. در نتیجه r در A است. ولی $r < c$ و در A است؛ پس، طبق انتخاب c، r نمی‌تواند مثبت باشد. بنابراین $r = ۰$. به‌عبارت دیگر، $a = qc$ و در نتیجه $c|a$. به همین ترتیب $c|b$.

برای یکتایی c گوییم اگر $t > ۰$ نیز در $t|a$، $t|b$، و $d|t$ به ازای هر d که $d|a$ و $d|b$ صدق کند، خواهیم داشت $t|c$ و $c|t$. پس، بنابر قسمت (ج) لم ۲.۵.۱، $c = t$ (زیرا هر دوی آنها مثبت‌اند).

■

حال به یک مثال صریح، یعنی $a = ۲۴$ و $b = ۹$، نگاه می‌کنیم. مستقیماً با امتحان معلوم می‌شود که $(۲۴, ۹) = ۳$. ملاحظه می‌کنیم که $(-۱)۲۴ + ۳ \cdot ۹ = ۳$. $(-۲۴, ۹)$ مساوی چیست؟

می‌پرسیم: این کار به ازای a و b مثبت و بزرگ چطور صورت می‌گیرد؟ اگر $a < b$، a و b را با هم تعویض می‌کنیم تا $a > b > ۰$. در این صورت (a, b) را می‌توان با

۱. توجه به $(a, b) = (b, r)$ که در آن $a = qb + r$ و $۰ \leq r < b$ (چرا؟)، و
۲. یافتن (b, r)، که به دلیل کوچکتر بودن اعداد فعلی از قبل، ساده‌تر است به‌دست آورد.

مثلاً، داریم

$$(۱۰۰, ۲۸) = (۲۸, ۱۶) \quad \text{زیرا} \quad ۱۰۰ = ۳(۲۸) + ۱۶$$
$$(۲۸, ۱۶) = (۱۶, ۱۲) \quad \text{زیرا} \quad ۲۸ = ۱(۱۶) + ۱۲$$
$$(۱۶, ۱۲) = (۱۶, ۴) \quad \text{زیرا} \quad ۱۶ = ۱(۱۲) + ۴$$

از روابط فوق داریم $(۱۰۰, ۲۸) = (۱۶, ۴) = ۴$. با برگشت در محاسباتی که برای یافتن ۴ شد، می‌توان $m.$ و $n.$ را طوری یافت که $۴ = m.۱۰۰ + n.۲۸$:

$$\text{چون} \quad ۱۶ = ۱(۱۲) + ۴ \text{، پس} \quad ۴ = ۱۶ + (-۱)۱۲$$
$$\text{چون} \quad ۲۸ = ۱(۱۶) + ۱۲ \text{، پس} \quad ۱۲ = ۲۸ + (-۱)۱۶$$
$$\text{چون} \quad ۱۰۰ = ۳(۲۸) + ۱۶ \text{، پس} \quad ۱۶ = ۱۰۰ + (-۳)۲۸$$

اما در این صورت

$$\begin{aligned} ۴ = ۱۶ + (-۱)۱۲ &= ۱۶ + (-۱)(۲۸ + (-۱)۱۶) \\ = (-۱)۲۸ + (۲)۱۶ &= (-۱)۲۸ + (۲)(۱۰۰ + (-۳)۲۸) \\ = (۲)۱۰۰ + (-۷)۲۸ & \end{aligned}$$

در نتیجه $m. = ۲$ و $n. = -۷$.

روش به‌کارگیری مکرر از مراحل ۱ و ۲ طرز استفاده از الگوریتم اقلیدس برای محاسبهٔ (a, b) به ازای هر دو عدد صحیح مثبت a و b را نشان می‌دهد.

در آخر این بخش چند تمرین راجع به خواص دیگر (a, b) گنجانده‌ایم.

حال به تعریف بسیار مهم زیر می‌رسیم.

تعریف. گوییم a و b نسبت به هم اول اند اگر $(a, b) = ۱$.

پس اعداد صحیح a و b در صورتی نسبت به هم اولند که عامل مشترک غیربدیهی نداشته باشند. یک نتیجهٔ فوری از قضیهٔ ۳.۵.۱ به قرار زیر است.

قضیهٔ ۴.۵.۱. اعداد صحیح a و b نسبت به هم اولند اگر و فقط اگر به ازای اعداد صحیح مناسبی چون m و n، $ma + nb = ۱$.

قضیهٔ ۴.۵.۱ نتیجهٔ فوری زیر را در بردارد.

قضیهٔ ۵.۵.۱. هرگاه a و b نسبت به هم اول بوده و $a|bc$، آن‌گاه $a|c$.

برهان. بنابر قضیهٔ ۴.۵.۱، به ازای m و n ی $ma + nb = ۱$؛ پس $c = (ma + nb)c$؛ یعنی $mac + nbc = c$. طبق فرض $a|bc$، و نیز $a|mac$؛ پس $a|(mac + nbc)$؛ و در نتیجه $a|c$. ■

نتیجه. هرگاه b و c نسبت به a اول باشند، آن‌گاه bc نیز نسبت به a اول است.

برهان. برهان قضیهٔ ۵.۵.۱ را از $mac + nbc = c$ به بعد به‌دست می‌گیریم. هرگاه $d = (a, bc)$، آن‌گاه $d|a$ و $d|bc$؛ پس $d|(mac + nbc) = c$. چون $d|a$ و $d|c$ و $(a, c) = ۱$، داریم $d = ۱$. و چون $(a, bc) = d = ۱$، bc نسبت به a اول می‌باشد. ■

حال ردهٔ بسیار مهمی از اعداد صحیح مثبت را که قبلاً در مسئلهٔ ۳۰ از بخش ۴ بدان برخوردیم ممتاز می‌سازیم.

تعریف. عدد صحیح $p > ۱$ یک عدد اول یا اول است اگر به ازای هر عدد صحیح a، $p|a$ یا p نسبت به a اول باشد.

این تعریف با تعریف معمول، یعنی اینکه p تجزیهٔ غیربدیهی ندارد، یکی است. زیرا هرگاه p با تعریف فوق اول بوده و $p = ab$ که در آن $۱ \leq a < b$، آن‌گاه $a = (a, p)$ (چرا؟) و p عدد a را عاد نمی‌کند زیرا $a < p$. پس $a = ۱$؛ در نتیجه $p = b$. از آن‌سو، هرگاه p به این معنی که

تجزیهٔ غیربدیهی ندارد اول بوده و عدد صحیح a نسبت به p اول نباشد، آن‌گاه (a,p) مساوی ۱ نبوده و a و p را عاد می‌کند. اما (a,p) طبق فرض مساوی p است. پس p، a را عاد خواهد کرد.

نتیجهٔ دیگر قضیهٔ ۵.۵.۱ به قرار زیر است.

قضیهٔ ۶.۵.۱. هرگاه p اول بوده و $p|(a_۱a_۲\cdots a_n)$، آن‌گاه به ازای iی که $۱ \leq i \leq n$، $p|a_i$.

برهان. اگر $p|a_۱$، چیزی برای اثبات نداریم. فرض کنیم $p \nmid a_۱$. پس p و $a_۱$ نسبت به هم اولند. اما $p|a_۱(a_۲\cdots a_n)$. پس طبق قضیهٔ ۵.۵.۱، $p|a_۲\cdots a_n$. برای $a_۲$ مانند فوق استدلال کرده و ادامه دهید. ■

اعداد اول نقش بسیار خاصی در مجموعهٔ اعداد صحیح بزرگتر از ۱ دارند به این نحو که هر عدد صحیح $n > ۱$ یا اول است یا حاصلضربی است از اعداد اول. این را در قضیهٔ زیر نشان خواهیم داد. در قضیهٔ بعد از آن یکتایی تجزیهٔ $n > ۱$ به عوامل اول به ثبوت می‌رسد. اثبات این دو امر قویاً به اصل خوش‌ترتیبی تکیه دارد.

قضیهٔ ۷.۵.۱. هرگاه $n > ۱$، آن‌گاه یا n اول است یا حاصلضربی است از اعداد اول.

برهان. فرض کنیم قضیه درست نباشد. پس باید عددی صحیح مانند $m > ۱$ باشد که قضیه به ازای آن برقرار نباشد. لذا مجموعهٔ M که قضیه به ازای اعضای آن درست نیست ناتهی است. پس، طبق اصل خوش‌ترتیبی، M دارای کوچکترین عنصر مانند m است. واضح است که چون $m \in M$، m نمی‌تواند اول باشد. لذا $m = ab$ که در آن $۱ < a < m$ و $۱ < b < m$. چون $a < m$ و $b < m$ و m کوچکترین عنصر در M است، $a \in M$ یا $b \in M$ را نخواهیم داشت. و چون $a \notin M$ و $b \notin M$، طبق تعریف M، قضیه باید به ازای هر دوی a و b درست باشد. لذا a و b اول بوده یا حاصلضربی از اعداد اول است. از $m = ab$ معلوم می‌شود که m حاصلضربی از اعداد اول است. این امر m را از M خارج می‌کند که با $m \in M$ در تضاد است. پس قضیه برقرار می‌باشد. ■

در بالا گفتیم که در تجزیهٔ یک عدد صحیح به عوامل اول یکتایی موجود است. حال این گفته را دقیق می‌سازیم. برای احتراز از بدیهیاتی چون $۶ = ۳ \cdot ۲ = ۲ \cdot ۳$ (در نتیجه ۶ دو تجزیه به اعداد اول ۲ و ۳ دارد)، قضیه را به نحوی خاص بیان می‌داریم.

قضیهٔ ۸.۵.۱. به ازای $n > 1$ یک و فقط یک راه برای نوشتن n به شکل $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ وجود دارد که در آن $p_1 < p_2 < \cdots < p_k$ اول بوده و نماهای a_1، a_2، $\cdots$، a_k همه مثبت می‌باشند.

برهان. همانند قضیهٔ قبل، یعنی با فرض نادرست بودن قضیه، شروع می‌کنیم. پس کوچکترین عدد صحیح مانند $m > 1$ وجود دارد که قضیه به ازای آن نادرست است. این m باید دو تجزیهٔ متمایز به‌صورت $m = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k} = q_1^{b_1}q_2^{b_2}\cdots q_\ell^{b_\ell}$ داشته باشد که در آنها $p_1 < p_2 < \cdots < p_k$ و $q_1 < q_2 < \cdots < q_\ell$ اول بوده و نماهای a_1، $\cdots$، a_k و b_1، $\cdots$، b_ℓ همه مثبت می‌باشند. چون $p_1|p_1^{a_1}\cdots p_k^{a_k} = q_1^{b_1}\cdots q_\ell^{b_\ell}$، بنابر قضیهٔ ۶.۵.۱، به ازای i ای $p_1|q_i^{b_i}$. لذا، مجدداً طبق قضیهٔ ۶.۵.۱، $p_1|q_i$؛ در نتیجه $p_1 = q_i$. به همین ترتیب، به ازای j ای، $q_1 = p_j$. لذا $p_1 \le p_j = q_1 \le q_i = p_1$. این نتیجه می‌دهد که $p_1 = q_1$. اما چون $m/p_1 < m$، m/p_1 دارای خاصیت یکتایی تجزیه است. ولی $m/p_1 = p_1^{a_1-1}p_2^{a_2}\cdots p_k^{a_k} = p_1^{b_1-1}q_2^{b_2}\cdots q_\ell^{b_\ell}$. چون m/p_1 را می‌توان به یک و تنها یک طریق به این شکل نوشت، به آسانی خواهیم داشت $k = \ell$، $p_2 = q_2$، $\cdots$، $p_k = q_k$، $a_1 - 1 = b_1 - 1$، $a_2 = b_2$، $\cdots$، $a_k = b_k$. پس معلوم می‌شود که اعداد اول و نماهایشان در تجزیهٔ m منحصر به فردند. این امر با عدم یکتایی تجزیهٔ m تناقض داشته، ولذا قضیه به اثبات خواهد رسید. ■

آنچه دو قضیهٔ اخیر به ما می‌گویند این است که اعداد صحیح را می‌توان از اعداد اول به نحوی بسیار دقیق و جا افتاده ساخت. از این انتظار می‌رود که باید بی‌نهایت عدد اول داشته باشیم. این نتیجه‌ای است قدیمی که به اقلیدس باز می‌گردد. در واقع استدلالی که می‌آوریم از آن اقلیدس است.

قضیهٔ ۹.۵.۱. تعدادی نامتناهی عدد اول وجود دارد.

برهان. اگر نتیجه نادرست می‌بود، می‌توانستیم همهٔ اعداد اول را به‌صورت p_1، p_2، $\cdots$، p_k شماره‌گذاری کنیم. حال عدد صحیح $q = 1 + p_1p_2\cdots p_k$ را در نظر می‌گیریم. چون به ازای هر $i = 1, 2, \ldots, k$، $q > p_i$، q نمی‌تواند اول باشد. و چون $p_i \nmid q$ (زیرا در تقسیم q بر p_i باقیماندهٔ ۱ داریم)، q بر هیچیک از p_1، $\ldots$، p_k بخشپذیر نیست. پس q نه اول است و نه بر عدد اولی بخشپذیر است. این امر قضیهٔ ۷.۵.۱ را نقض و قضیهٔ فوق را به اثبات می‌رساند. ■

در باب تعداد اعداد اول تا مرحله‌ای معلوم نتایج قویتری از قضیهٔ ۹.۵.۱ در دست است.

قضیهٔ مشهور اعداد اول می‌گوید که به ازای n بزرگ، تعداد اعداد اول نابیشتر از n «بیش و کم» مساوی $n/\log_e n$ است که در آن این «بیش و کم» دقیقاً توصیف شده است. اعداد اول مسائل حل نشدهٔ بسیار دارند.

مسائل

مسائل آسانتر

۱. به ازای

الف) $(116, -84)$؛

ب) $(85, 65)$؛

پ) $(72, 26)$؛

ت) $(72, 25)$.

(a, b) را یافته و (a, b) را به‌صورت $ma + nb$ بیان دارید.

۲. تمام قسمتهای لم ۲.۵.۱ را ثابت کنید.

۳. نشان دهید که اگر $m > 0$، $(ma, mb) = m(a, b)$.

۴. نشان دهید هرگاه $a|m$ و $b|m$ و $(a, b) = 1$، آن‌گاه $ab|m$.

۵. اعداد زیر را به اعداد اول تجزیه کنید:

الف) ۳۶؛

ب) ۱۲۰؛

پ) ۷۲۰؛

ت) ۵۰۴۰.

۶. هرگاه $m = p_1^{a_1} \cdots p_k^{a_k}$ و $n = p_1^{b_1} \cdots p_k^{b_k}$ که در آنها p_1، $\cdots$، p_k اعداد اول متمایزی بوده و a_1، $\cdots$، a_k و b_1، $\cdots$، b_k نامنفی باشند، آن‌گاه (m, n) را با توصیف cها برحسب aها و bها به‌صورت $p_1^{c_1} \cdots p_k^{c_k}$ بیان دارید.

*۷. کوچکترین مضرب مشترک اعداد صحیح مثبت m و n را کوچکترین عدد صحیح مثبت v تعریف کنید که $m|v$ و $n|v$.

الف) نشان دهید که $v = mn/(m, n)$.

ب) v برحسب تجزیهٔ m و n در مسئلهٔ ۶ چه صورتی دارد؟

۸. کوچکترین مضرب مشترک جفتهای مسئلهٔ ۱ را بیابید.

۹. اگر $m, n > 0$ دو عدد صحیح باشند، نشان دهید که می‌توان اعداد صحیح u و v را چنان یافت که $-n/2 \leq v \leq n/2$ و $m = un + v$.

۱۰. ثابت کنید برای امتحان اول بودن عدد صحیح $n > 1$ کافی است نشان دهیم n بر هیچ عدد اول p که $p \leq \sqrt{n}$ بخشپذیر نیست.

۱۱. اعداد زیر را از حیث اول بودن امتحان کنید:

الف) ۳۰۱؛

ب) ۱۰۰۱؛

پ) ۴۷۳.

۱۲. با شروع از ۲، ۳، ۵، ۷، ... اعداد صحیح مثبت ۲·۳ + ۱، ۲·۳·۵ + ۱، ۲·۳·۵·۷ + ۱، ... را بسازید. آیا همیشه یک عدد اول به‌دست می‌آید؟

مسائل با سطح متوسط

۱۳. اگر p عدد اول فردی باشد، نشان دهید p به شکل زیر است:

الف) $4n + 1$ یا $4n + 3$ به ازای nی؛

ب) $6n + 1$ یا $6n + 5$ به ازای nی.

۱۴. با تقلید از برهان قضیهٔ ۱.۵.۹ ثابت کنید

الف) بی‌نهایت عدد اول به شکل $4n + 3$ وجود دارد؛

ب) بی‌نهایت عدد اول به شکل $6n + 5$ وجود دارد.

۱۵. نشان دهید که هیچ عدد صحیح $u = 4n + 3$ را نمی‌توان به‌صورت $u = a^2 + b^2$ نوشت که در آن a و b صحیح باشند.

۱۶. اگر T زیرمجموعه‌ای نامتناهی از $\mathbb{N}$ (مجموعهٔ تمام اعداد صحیح مثبت) باشد، نشان دهید یک نگاشت ۱-۱ از T به روی $\mathbb{N}$ وجود دارد.

۱۷. اگر p اول باشد، ثابت کنید نمی‌توان اعداد صحیح ناصفری مانند a و b یافت به‌طوری که $a^2 = pb^2$. (این نشان می‌دهد که $\sqrt{p}$ گنگ است.)

۶. استقرای ریاضی

اگر به بخش ۵ بازگردیم خواهیم دید که در چند مورد (مثلاً در برهان قضیهٔ ۱.۵.۶) گفته‌ایم: «مانند فوق استدلال کرده و ادامه دهید.» این نوع استدلال چندان قانع کننده نیست. آنچه واضح

است این است که در اثبات حکمی راجع به تمام اعداد صحیح مثبت به روشی جهت پرهیز از این عبارات نیاز داریم. اصل استقرای ریاضی این روش را به ما می‌دهد؛ در واقع این همان روش معمول است که در اثبات قضایای مربوط به تمام اعداد صحیح مثبت به‌کار خواهیم برد.

قضیهٔ ۱.۶.۱. فرض کنیم $P(n)$ حکمی راجع به اعداد صحیح مثبت باشد به‌طوری که

الف) $P(1)$ درست باشد؛

ب) هرگاه $P(k)$ به ازای عدد صحیح $k \geq 1$ درست باشد، آن‌گاه $P(k+1)$ نیز درست باشد.

در این صورت $P(n)$ به ازای هر $n \geq 1$ درست خواهد بود.

برهان. استدلال ما در اینجا شبیه اثبات قضایای ۷.۵.۱ و ۸.۵.۱ است.

فرض کنیم قضیه درست نباشد. پس، طبق اصل خوش‌ترتیبی، کوچکترین عدد صحیح $m \geq 1$ وجود دارد به‌طوری که $P(m)$ درست نیست. چون $P(1)$ درست است، $m \neq 1$؛ در نتیجه $m > 1$. اما $1 \leq m - 1 < m$. پس، طبق انتخاب m، باید $P(m-1)$ برقرار باشد. ولی، در این صورت، طبق فرض استقرا [قسمت (ب)] $P(m)$ باید درست باشد. این با نادرست بودن $P(m)$ در تضاد است. لذا عدد صحیحی که به ازای آن P درست نباشد وجود ندارد، و در نتیجه قضیه ثابت می‌شود. ∎

حال طرز استفاده از استقرا را با مثالهایی نسبتاً متنوع توضیح می‌دهیم.

چند مثال

۱. فرض کنیم n توپ تنیس را به خط مستقیم و در تماس با هم قرار داده باشیم. حکم می‌کنیم که این توپها $n-1$ تماس با یکدیگر دارند.

برهان. اگر $n = 2$، مطلب واضح است. هرگاه به ازای k توپ $k-1$ تماس داشته باشیم، آن‌گاه با افزودن یک توپ (روی یک خط) یک تماس اضافه می‌شود. لذا $k+1$ توپ k تماس با هم خواهند داشت. پس اگر $P(n)$ حکم فوق راجع به توپهای تنیس باشد، می‌بینیم که با درست بودن $P(k)$، $P(k+1)$ درست است. لذا، طبق قضیهٔ فوق، $P(n)$ به ازای هر $n \geq 1$ درست می‌باشد. ∎

۲. هرگاه p اول بوده و $p|a_1a_2\cdots a_n$، آن‌گاه به ازای اندیسی چون $1 \leq i \leq n$، $p|a_i$.

برهان. فرض کنیم $P(n)$ حکم مثال ۲ باشد. پس $P(1)$ درست است چرا که اگر $p|a_1$،

به ازای اندیسی چون $۱ \leq i$، ۱، a_i را عاد می‌کند.

فرض کنیم $P(k)$ درست بوده و $p|a_۱a_۲\cdots a_ka_{k+۱}$. لذا، طبق قضیهٔ ۵.۵.۱، چون $p|(a_۱a_۲\cdots a_k)a_{k+۱}$، $p|a_{k+۱}$ (نتیجهٔ مطلوب) یا $p|a_۱\cdots a_k$. در حالت دوم، چون $P(k)$ درست است، به ازای اندیسی مانند $k \geq i \geq ۱$، $p|a_i$، از تلفیق دو حالت معلوم می‌شود که به ازای اندیسی مانند $k+۱ \geq j \geq ۱$، $p|a_j$. لذا قسمت (ب) قضیهٔ ۱.۶.۱ برقرار است؛ در نتیجه $P(n)$ به ازای هر $n \geq ۱$ درست می‌باشد. ■

۳. به ازای $n \geq ۱$، $۱ + ۲ + \cdots + n = \frac{۱}{۲}n(n+۱)$.

برهان. هرگاه $P(n)$ حکم $۱ + ۲ + \cdots + n = \frac{۱}{۲}n(n+۱)$ باشد، آن‌گاه $P(۱)$ مسلماً درست است، زیرا $\frac{۱}{۲}(۱+۱) = ۱$. اگر $P(k)$ درست باشد، داریم

$$۱ + ۲ + \cdots + k = \frac{۱}{۲}k(k+۱)$$

سؤال این است: آیا $P(k+۱)$ نیز درست است؛ یعنی آیا

$$۱ + ۲ + \cdots + k + (k+۱) = \frac{۱}{۲}(k+۱)((k+۱)+۱)?$$

داریم

$$\begin{aligned} ۱ + ۲ + \cdots + k + (k+۱) &= (۱ + ۲ + \cdots + k) + (k+۱) \\ &= \frac{۱}{۲}k(k+۱) + (k+۱) \end{aligned}$$

زیرا $P(k)$ برقرار است. ولی

$$\frac{۱}{۲}k(k+۱) + (k+۱) = \frac{۱}{۲}(k(k+۱) + ۲(k+۱)) = \frac{۱}{۲}(k+۱)(k+۲)$$

که درستی $P(k+۱)$ را تأیید می‌کند. لذا حکم $۱ + ۲ + \cdots + n = \frac{۱}{۲}n(n+۱)$ به ازای هر $n \geq ۱$ درست می‌باشد. ■

در اینجا نکته‌ای را مورد تأکید قرار می‌دهیم: استقرای ریاضی روشی برای یافتن نتایج مربوط به اعداد صحیح نیست بلکه روشی است برای تحقیق در یک نتیجه. فرمول فوق راجع به $۱ + ۲ + \cdots + n$ را می‌توان با ابزارهایی دیگر به‌دست آورد.

قسمت (ب) قضیهٔ ۱.۶.۱ را معمولاً مرحلهٔ استقرا می‌نامند.

در مسائل صورتهای دیگری از اصل استقرا را بیان خواهیم کرد.

مسائل

مسائل آسانتر

۱. به استقرا ثابت کنید که $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$.

۲. به استقرا ثابت کنید که $1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$.

۳. ثابت کنید هر مجموعه با $n \geq 2$ عنصر دارای $\frac{1}{2}n(n-1)$ زیرمجموعهٔ دو عنصری است.

۴. ثابت کنید هر مجموعه با $n \geq 3$ عنصر دارای $n(n-1)(n-2)/3!$ زیرمجموعهٔ سه عنصری است.

۵. اگر $n \geq 4$ و مجموعهٔ S دارای n عنصر باشد، از مسائل ۳ و ۴ حدس بزنید که S چند زیرمجموعهٔ ۴ عنصری دارد. سپس حدس خود را به استقرای ریاضی ثابت نمایید.

*۶. برهان قضیهٔ ۶.۵.۱ را به‌وسیلهٔ تعویض آخرین جمله با یک استدلال استقرایی کامل نمایید.

۷. اگر $a > 1$، به استقرا ثابت کنید که $1 + a + a^2 + \cdots + a^n = (a^{n+1} - 1)/(a-1)$.

۸. به استقرا نشان دهید که

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

۹. فرض کنید حکم $P(n)$ در باب اعداد صحیح چنان باشد که $P(n_0)$ برقرار بوده و اگر $P(k)$ درست باشد، $P(k+1)$ نیز باشد. راجع به $P(n)$ چه می‌شود گفت؟ گفتهٔ خود را ثابت نمایید.

۱۰. فرض کنید حکم $P(n)$ راجع به اعداد صحیح چنان باشد که $P(1)$ درست بوده و اگر $P(j)$ به ازای جمیع اعداد صحیح مثبت $j < k$ درست باشد، $P(k)$ نیز درست باشد. ثابت کنید $P(n)$ به ازای جمیع اعداد صحیح مثبت n درست است.

مسائل با سطح متوسط

۱۱. حکمی را مثال بزنید که به ازای هر عدد صحیح مثبت درست نباشد ولی فرض استقرا [قسمت (ب) قضیهٔ ۱.۶.۱] برایش برقرار باشد.

۱۲. به استقرا ثابت کنید که یک مجموعهٔ n عنصری درست 2^n زیرمجموعه دارد.

۱۳. به استقرا بر n ثابت کنید که $n^3 - n$ همیشه بر ۳ بخشپذیر است.

۱۴. مسئلهٔ ۱۳ را با استفاده از استقرا بر n به‌صورت زیر تعمیم دهید: هرگاه p یک عدد اول باشد، آن‌گاه $n^p - n$ همیشه بر p بخشپذیر است. (راهنمایی. قضیهٔ دوجمله‌ای.)

۱۵. به استقرا ثابت کنید که تعداد نگاشتهای ۱-۱ از یک مجموعهٔ n عنصری به خود مساوی $n!$ است.

۷. اعداد مختلط

همهٔ ما اعداد صحیح، اعداد گویا، و اعداد حقیقی را تا حدودی می‌شناسیم. این فرض در واقع برای بخشی از متن شده است و در بسیاری از مسائل نیز به این اعداد ارجاع می‌شود. متأسفانه شاگردان کالج اعداد مختلط و خواص آنها را کمتر می‌شناسند. زمانی اعداد مختلط بخشی از برنامهٔ دبیرستان و سالهای اول کالج بود. ولی اکنون چنین نیست. لذا ما این مجموعهٔ ریاضی بسیار مهم را به سرعت مرور می‌کنیم.

مجموعهٔ اعداد مختلط $\mathbb{C}$ عبارت است از مجموعهٔ تمام $a + bi$ که در آن a و b حقیقی‌اند، و حکم می‌کنیم که

۱. $a + bi = c + di$ (a و b و c و d حقیقی) اگر و فقط اگر $a = c$ و $b = d$؛
۲. $(a + bi) \pm (c + di) = (a \pm c) + (b \pm d)i$؛
۳. $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

آخرین خاصیت (یعنی ضرب) را می‌توان با استفاده از $i^۲ = -۱$ و ضرب صوری به بهترین وجه به خاطر آورد.

در عدد مختلط $z = a + bi$، a را قسمت حقیقی z و b را قسمت موهومی z می‌نامیم. اگر a مساوی ۰ باشد، z موهومی محض نامیده می‌شود.

ما عدد $۰ + ۰i$ را به‌صورت ۰ و عدد $a + ۰i$ را به‌صورت a می‌نویسیم. توجه کنید که به ازای هر عدد مختلط z، $z + ۰ = z$ و $z۱ = z$.

به ازای $z = a + bi$ عدد مختلطی در رابطه با z وجود دارد که به‌صورت $\bar{z}$ نوشته شده و با $\bar{z} = a - bi$ تعریف می‌شود. $\bar{z}$ را مزدوج مختلط z می‌نامیم. علامت «ـــ» نگاشتی از $\mathbb{C}$ به روی خود به‌دست می‌دهد. حکم می‌کنیم:

لم ۱.۷.۱. هرگاه $z, w \in \mathbb{C}$، آن‌گاه

الف) $\overline{(\bar{z})} = z$؛
ب) $\overline{(z + w)} = \bar{z} + \bar{w}$؛
پ) $\overline{(zw)} = \bar{z}\bar{w}$؛
ت) $z\bar{z}$ حقیقی و نامنفی است و، در واقع، اگر $z \neq ۰$ مثبت است؛

ث) $z + \bar{z}$ دو برابر قسمت حقیقی z است؛

ج) $z - \bar{z}$ دو برابر قسمت موهومی z ضربدر i است.

برهان. اغلب قسمتهای این لم سر راست بوده و فقط با استفاده از تعریف مزدوج مختلط ثابت می‌شوند. ما قسمتهای (پ) و (ت) را تحقیق می‌کنیم.

فرض کنیم $z = a + bi$ و $w = c + di$ که در آنها a و b و c و d حقیقی‌اند. پس $zw = (ac - bd) + (ad + bc)i$؛ در نتیجه

$$\overline{(zw)} = \overline{(ac - bd) + (ad + bc)i} = (ac - bd) - (ad + bc)i$$

ازآن سو، $\bar{z} = a - bi$ و $\bar{w} = c - di$؛ لذا، طبق تعریف در $\mathbb{C}$، $\bar{z}\bar{w} = (ac - bd) - (ad + bc)i$. از مقایسهٔ این با نتیجه‌ای که برای $\overline{(zw)}$ به‌دست آمد معلوم می‌شود که $\overline{(zw)} = \bar{z}\bar{w}$. این امر قسمت (پ) را ثابت می‌کند.

حال به اثبات قسمت (ت) می‌پردازیم. فرض کنیم $z = a + bi \neq 0$. پس $\bar{z} = a - bi$ و $z\bar{z} = a^2 + b^2$. چون a و b حقیقی بوده و هر دو 0 نیستند، همان‌طور که در قسمت (ت) حکم شده، $a^2 + b^2$ حقیقی و مثبت می‌باشد. ■

برهان قسمت (ت) لم ۱.۷.۱ نشان می‌دهد که اگر $z = a + bi \neq 0$، $z\bar{z} = a^2 + b^2 \neq 0$ و $z(\bar{z}/(a^2 + b^2)) = 1$. پس

$$\frac{\bar{z}}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \left(\frac{b}{a^2 + b^2}\right) i$$

مانند معکوس $1/z$ عدد z عمل می‌کند. این امر اجازهٔ تقسیم در $\mathbb{C}$ و بودن در $\mathbb{C}$ حین این عمل را خواهد داد.

حال چند خاصیت از $\mathbb{C}$ را ذکر می‌کنیم.

لم ۲.۷.۱. $\mathbb{C}$ تحت جمع و ضرب خود رفتاری به‌صورت زیر دارد: هرگاه $u, v, w \in \mathbb{C}$، آن‌گاه

الف) $u + v = v + u$؛

ب) $(u + v) + w = u + (v + w)$؛

پ) $uv = vu$؛

ت) $(uv)w = u(vw)$؛

ث) $u \neq 0$ وجود $u^{-1} = \frac{1}{u}$ را در $\mathbb{C}$ با خاصیت $uu^{-1} = 1$ ایجاب می‌کند.

برهان. اثبات قسمتهای فوق را به خواننده وا می‌گذاریم. ■

خواص فوق $\mathbb{C}$ را یک میدان می‌سازد که بعدها در کتاب به تفصیل مطالعه می‌شود. آنچه لم می‌گوید این است که در $\mathbb{C}$ می‌توان بیش و کم مانند اعداد حقیقی حساب کرد. ولی $\mathbb{C}$ ساختار قویتری از مجموعهٔ اعداد حقیقی دارد.

حال یک تابع «اندازه» بر $\mathbb{C}$ معرفی می‌کنیم.

تعریف. هرگاه $z = a + bi \in \mathbb{C}$، آن‌گاه قدرمطلق z به‌صورت $|z|$ نوشته شده و با $|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$ تعریف می‌شود.

لحظه‌ای دیگر تعبیر هندسی تعریف فوق را خواهیم دید. در این فاصله لم زیر را ثابت می‌کنیم.

لم ۳.۷.۱. هرگاه $u, v \in \mathbb{C}$، آن‌گاه $|uv| = |u||v|$.

برهان. طبق تعریف، $|u| = \sqrt{u\bar{u}}$ و $|v| = \sqrt{v\bar{v}}$. اما

$$\begin{aligned} |uv| &= \sqrt{(uv)\overline{(uv)}} = \sqrt{(uv)(\bar{u}\bar{v})} && \text{[بنابر قسمت (پ) لم ۱.۷.۱]} \\ &= \sqrt{(u\bar{u})(v\bar{v})} && \text{(بنابر لم ۲.۷.۱)} \\ &= \sqrt{u\bar{u}}\sqrt{v\bar{v}} = |u||v| \end{aligned}$$

راه دیگر اثبات این لم نوشتن $u = a + bi$، $v = c + di$، $uv = (ac - bd) + (ad + bc)i$ و توجه به اتحاد زیر است:

$$(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2)$$

■

به چند نکتهٔ کوچک راجع‌به مزدوجها توجه کنید. هرگاه $z \in \mathbb{C}$ ، آن‌گاه z حقیقی است اگر و فقط اگر $z = \bar{z}$، و z موهومی محض است اگر و فقط اگر $\bar{z} = -z$. هرگاه $z, w \in \mathbb{C}$، آن‌گاه

$$\overline{(z\bar{w} + \bar{z}w)} = \bar{z}\bar{\bar{w}} + \bar{\bar{z}}\bar{w} = \bar{z}w + z\bar{w}$$

پس $z\bar{w} + \bar{z}w$ حقیقی است. می‌خواهیم برای $|z\bar{w} + \bar{z}w|$ کران بالایی بیابیم. این امر در برهان قضیهٔ ۵.۷.۱ ظاهر می‌شود.

اما ابتدا کمی از بحث منحرف شده و حکمی راجع به عبارات درجهٔ دو عنوان می‌کنیم.

لم ۴.۷.۱. هرگاه a و b و c حقیقی و $a > 0$ چنان باشند که به ازای هر αی حقیقی $a\alpha^2 + b\alpha + c \geq 0$، آن‌گاه $b^2 - 4ac \leq 0$.

برهان. عبارت درجهٔ دو را به ازای $\alpha = -b/2a$ در نظر می‌گیریم. داریم

$$a(-b/2a)^2 + b(-b/2a) + c \geq 0$$

با ساده کردن این به‌دست می‌آوریم $(4ac - b^2)/4a \geq 0$، و چون $a > 0$، خواهیم داشت $4ac - b^2 \geq 0$؛ و در نتیجه $b^2 - 4ac \leq 0$. ■

ما از لم فوق برای اثبات قضیهٔ مهم زیر استفاده می‌کنیم.

قضیهٔ ۵.۷.۱(نامساوی مثلثی). به ازای $z, w \in \mathbb{C}$، $|z + w| \leq |z| + |w|$.

برهان. اگر $z = 0$، چیزی برای اثبات وجود ندارد. پس می‌توان فرض کرد $z \neq 0$. لذا $z\bar{z} > 0$. اما، به ازای αی حقیقی،

$$\begin{aligned} 0 \leq |\alpha z + w|^2 &= (\alpha z + w)(\overline{\alpha z + w}) = (\alpha z + w)(\alpha \bar{z} + \bar{w}) \\ &= \alpha^2 z\bar{z} + \alpha(z\bar{w} + \bar{z}w) + w\bar{w} \end{aligned}$$

هرگاه $a = z\bar{z} > 0$، $b = z\bar{w} + \bar{z}w$، و $c = w\bar{w}$، آن‌گاه لم ۴.۷.۱ می‌گوید که

$$b^2 - 4ac = (z\bar{w} + \bar{z}w)^2 - 4(z\bar{z})(w\bar{w}) \leq 0$$

پس

$$(z\bar{w} + \bar{z}w)^2 \leq 4(z\bar{z})(w\bar{w}) = 4|z|^2|w|^2$$

لذا، $z\bar{w} + \bar{z}w \leq 2|z||w|$.

از نتیجهٔ فوق به ازای $\alpha = 1$ داریم

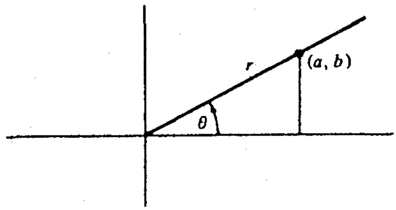
$$\begin{aligned} |z + w|^2 &= z\bar{z} + w\bar{w} + z\bar{w} + \bar{z}w = |z|^2 + |w|^2 + z\bar{w} + \bar{z}w \\ &\leq |z|^2 + |w|^2 + 2|z||w| \end{aligned}$$

به‌عبارت دیگر، $|z + w|^2 \leq (|z| + |w|)^2$. اگر جذر بگیریم نتیجهٔ مطلوب، یعنی

$$|z + w| \leq |z| + |w|$$

به‌دست می‌آید. ■

چرا این نتیجه را نامساوی مثلثی می‌نامند؟ دلیلش با توجه به تعبیر هندسی اعداد مختلط روشن است. عدد مختلط $z = a + bi$ را با نقطه به مختصات (a, b) در صفحهٔ x_y نمایش می‌دهیم. فاصلهٔ r این نقطه تا مبدأ مساوی $\sqrt{a^۲ + b^۲}$ یا $|z|$ است.

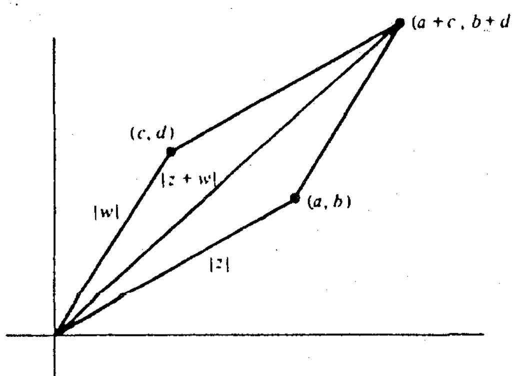


زاویهٔ θ را شناسهٔ z می‌نامند و، همان‌طور که می‌بینید، $\tan\theta = b/a$. همچنین $a = r\cos\theta$ و $b = r\sin\theta$. لذا $z = a + bi = r(\cos\theta + i\sin\theta)$. این نمایش z شکل قطبی آن نام دارد.

هرگاه $z = a + bi$ و $w = c + di$، آن‌گاه مجموعشان عبارت است از

$$z + w = (a + c) + (b + d)i$$

در این باب تصویر هندسی زیر را داریم.



نامساوی $|z + w| \leq |z| + |w|$ صرفاً مبین آن است که در مثلث T طول یک ضلع از مجموع طولهای دو ضلع دیگر کوچکتر است؛ اصطلاح نامساوی مثلثی از این امر ناشی شده است.

اعداد مختلط به شکل قطبی $\cos\theta + i\sin\theta$ اعداد جالبی هستند. ابتدا توجه می‌کنیم که

$$|\cos\theta + i\sin\theta| = \sqrt{\cos^۲\theta + \sin^۲\theta} = \sqrt{۱} = ۱$$

لذا اعداد مختلط بسیاری با قدرمطلق ۱ خواهیم داشت. اینها در واقع تمام اعداد مختلط با قدرمطلق ۱ می‌باشند. برای مشاهدهٔ این امر کافی است به شکل قطبی این اعداد نگاه کنیم.

حال دو اتحاد اصلی از مثلثات را یادآور می‌شویم:

$$\cos(\theta + \psi) = \cos\theta\cos\psi - \sin\theta\sin\psi$$

و

$$\sin(\theta + \psi) = \sin\theta\cos\psi + \cos\theta\sin\psi$$

لذا

$$\begin{aligned}(\cos\theta + i\sin\theta)(\cos\psi + i\sin\psi)\\ &= (\cos\theta\cos\psi - \sin\theta\sin\psi) + i(\sin\theta\cos\psi + \cos\theta\sin\psi)\\ &= \cos(\theta+\psi) + i\sin(\theta+\psi)\end{aligned}$$

لذا، در ضرب دو عدد مختلط، شناسهٔ حاصلضرب مساوی مجموع شناسه‌های عوامل می‌باشد. این امر نتیجهٔ بسیار جالب دیگری دارد.

قضیهٔ ۶.۷.۱ [**قضیهٔ دموآور (De Moivre)**]. به ازای هر عدد صحیح $n \geq ۱$،

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

برهان. به استقرا بر n عمل می‌کنیم. اگر $n = ۱$، حکم به وضوح درست است. حال فرض کنیم به ازای kای، $(\cos\theta + i\sin\theta)^k = \cos k\theta + i\sin k\theta$. لذا، طبق نتیجهٔ بند فوق،

$$\begin{aligned}(\cos\theta + i\sin\theta)^{k+۱} &= (\cos\theta + i\sin\theta)^k(\cos\theta + i\sin\theta)\\ &= (\cos k\theta + i\sin k\theta)(\cos\theta + i\sin\theta)\\ &= \cos(k+۱)\theta + i\sin(k+۱)\theta\end{aligned}$$

این امر استقرا را کامل می‌کند. پس نتیجه به ازای جمیع اعداد صحیح $n \geq ۱$ درست می‌باشد.

■

در مسائل خواهیم دید که قضیهٔ دموآور به ازای هر عدد صحیح m درست است؛ در واقع حتی وقتی m گویا باشد.

حالت خاص زیر را در نظر می‌گیریم.

$\theta_n = \cos ۲\pi/n + i \sin ۲\pi/n$ که در آن $n \geq ۱$ یک عدد صحیح است.

بنابر قضیهٔ دموآور،

$$\begin{aligned}\left(\cos\left(\frac{۲\pi}{n}\right) + i\sin\left(\frac{۲\pi}{n}\right)\right)^n \\ &= \cos\left(n\left(\frac{۲\pi}{n}\right)\right) + i\sin\left(n\left(\frac{۲\pi}{n}\right)\right) \\ &= \cos ۲\pi + i \sin ۲\pi = ۱\end{aligned}$$

پس $\theta_n^n = ۱$. می‌توان تحقیق کرد که اگر $۰ < m < n$، $\theta_n^m \neq ۱$. θ_n را یک ریشهٔ n ام اولیهٔ واحد می‌نامند.

مسائل

مسائل آسانتر

۱. ضربهای زیر را انجام دهید:

الف) $(۶ - ۷i)(۸ + i)$؛

ب) $(\frac{۲}{۳} + \frac{۳}{۲}i)(\frac{۲}{۳} - \frac{۳}{۲}i)$؛

پ) $(۶ + ۷i)(۸ - i)$.

۲. به ازای

الف) $z = ۶ + ۸i$؛

ب) $z = ۶ - ۸i$؛

پ) $z = \frac{۱}{\sqrt{۲}} + \frac{۱}{\sqrt{۲}}i$

$z^{-۱}$ را به شکل $z^{-۱} = a + bi$ بیان دارید.

۳*. نشان دهید که $(\bar{z})^{-۱} = \overline{(z^{-۱})}$.

۴. $(\cos\theta + i\sin\theta)^{-۱}$ را بیابید.

۵. تمام قسمتهای لم ۱.۷.۱ را ثابت کنید.

*۶. نشان دهید z حقیقی است اگر و فقط اگر $z = \bar{z}$، و موهومی محض است اگر و فقط اگر $\bar{z} = -z$.

۷. قانون تعویضپذیری ضرب $zw = wz$ در $\mathbb{C}$ را تحقیق کنید.

۸. نشان دهید که به ازای $z \neq ۰$، $|z^{-۱}| = ۱/|z|$.

۹. مقادیر زیر را بیابید:

الف) $|۶ - ۴i|$؛

ب) $|\frac{۱}{۲} + \frac{۲}{۴}i|$؛

پ) $|\frac{۱}{\sqrt{۲}} + \frac{۱}{\sqrt{۲}}i|$.

۱۰. نشان دهید که $|z| = |\bar{z}|$.

۱۱. شکل قطبی

الف) $z = \frac{\sqrt{۲}}{۲} - \frac{۱}{\sqrt{۲}}i$؛

ب) $z = ۴i$؛

پ) $z = \frac{۶}{\sqrt{۲}} + \frac{۶}{\sqrt{۲}}i$؛

ت) $z = -\frac{۱۳}{۲} + \frac{۳۹}{۲\sqrt{۳}}i$

را بیابید.

۱۲. ثابت کنید $\cos\theta + i\sin\theta = (\cos(\frac{۱}{۲}\theta) + i\sin(\frac{۱}{۲}\theta))^{۲}$.

۱۳. با محاسبهٔ مستقیم نشان دهید که $-۱ = (\frac{۱}{۲} + \frac{۱}{۲}\sqrt{۳}i)^{۳}$.

مسائل با سطح متوسط

۱۴. نشان دهید که به ازای جمیع اعداد صحیح m،

$$(\cos\theta + i\sin\theta)^m = \cos(m\theta) + i\sin(m\theta)$$

۱۵. نشان دهید که به ازای جمیع اعداد گویای r،

$$(\cos\theta + i\sin\theta)^r = \cos(r\theta) + i\sin(r\theta)$$

۱۶. اگر $z \in \mathbb{C}$ و $n \geq ۱$ عدد صحیح مثبت دلخواهی باشد، نشان دهید که n عدد مختلط متمایز مانند w هست به‌طوری که $z = w^n$.

۱۷. شرط لازم و کافی بر k را چنان بیابید که

الف) $\left(\cos\left(\frac{2\pi k}{n}\right)+i\sin\left(\frac{2\pi k}{n}\right)\right)^n = 1$؛

ب) اگر $0 < m < n$، $\left(\cos\left(\frac{2\pi k}{n}\right)+i\sin\left(\frac{2\pi k}{n}\right)\right)^m \neq 1$.

۱۸. صفحهٔ x-y را صفحهٔ تمام اعداد مختلط $x+iy$ گرفته، نشان دهید که ضرب در i یک دوران 90° خلاف عقربه‌های ساعت به صفحهٔ x-y می‌دهد.

۱۹. در مسئلهٔ ۱۸ اثر ضرب در عدد مختلط $a+bi$ بر صفحهٔ x-y را تعبیر هندسی نمایید.

۲۰. ثابت کنید $|z+w|^2+|z-w|^2 = 2(|z|^2+|w|^2)$.

*۲۱. مجموعهٔ $A=\{a+bi|a,b\in\mathbb{Z}\}$ را در نظر گرفته، ثابت کنید یک تناظر ۱-۱ از A به روی N وجود دارد. (A را مجموعهٔ اعداد گاوسی می‌نامند.)

۲۲. اگر a یک ریشهٔ (مختلط) چندجمله‌ای

$$x^n+\alpha_1 x^{n-1}+\cdots+\alpha_{n-1}x+\alpha_n$$

باشد که در آن α_iها حقیقی‌اند، نشان دهید که $\bar{a}$ نیز باید یک ریشه باشد. [r در صورتی ریشهٔ چندجمله‌ای $P(x)$ است که $P(r)=0$.]

مسائل مشکلتر

۲۳. شرایط لازم و کافی بر z و w را چنان بیابید که $|z+w|=|z|+|w|$.

۲۴. مسئلهٔ ۲۳ را برای $|z_1+\cdots+z_k|=|z_1|+\cdots+|z_k|$ حل کنید.

*۲۵. گوییم عدد مختلط θ از مرتبهٔ $n\geq 1$ است اگر $\theta^n=1$ و به ازای $0<m<n$، $\theta^m\neq 1$. نشان دهید هرگاه θ از مرتبهٔ n بوده و $\theta^k=1$ که در آن $k>0$، آن‌گاه $n|k$.

*۲۶. جمیع اعداد مختلط θ از مرتبهٔ n را بیابید. (اینها ریشه‌های nام اولیهٔ واحد می‌باشند.)

۲

گروهها

۱. چند تعریف و چند مثال از گروهها

در بخش ۴ از فصل ۱ دیدیم که به ازای هر مجموعهٔ ناتهی، مجموعهٔ $A(S)$ مرکب از تمام نگاشتهای S به روی خود تنها یک مجموعه نیست بلکه بافت قویتری دارد. امکان ترکیب دو عنصر $A(S)$ و یافتن عنصری دیگر از $A(S)$ به $A(S)$ ساختاری جبری می‌بخشد. ذیلاً طرز انجام این کار را یادآور می‌شویم: هرگاه $f, g \in A(S)$، آن‌گاه با ترکیب آنها نگاشت fg به‌دست می‌آید که به ازای هر $s \in S$ با $(fg)(s) = f(g(s))$ تعریف می‌شود. ما fg را حاصلضرب f و g نامیدیم و نشان دادیم که $fg \in A(S)$، و نیز دیدیم که این ضرب از چند قاعده پیروی می‌کند. از صدها امکان چهار قاعدهٔ خاص را که بر رفتار $A(S)$ نسبت به این ضرب حاکم بودند اختیار کردیم.

این چهار قاعده عبارت بودند از:

۱. بسته بودن، یعنی هرگاه $f, g \in A(S)$، آن‌گاه $fg \in A(S)$. گوییم $A(S)$ تحت این ضرب بسته است؛

۲. شرکتپذیری، یعنی هرگاه $f, g, h \in A(S)$، آن‌گاه $f(gh) = (fg)h$؛

۳. وجود عنصر یکه، یعنی عنصر خاصی مانند $i \in A(S)$ (نگاشت همانی) هست به‌طوری که به ازای هر $f \in A(S)$، $fi = if = f$؛

۴. وجود معکوسها، یعنی به ازای $f \in A(S)$ عنصری مانند f^{-1} در $A(S)$ هست به طوری که $ff^{-1} = f^{-1}f = i$.

تأیید و یا انگیزش اینکه چرا این چهار خاصیت $A(S)$ را بر خواص دیگر ترجیح داده‌ایم آسان نیست. در واقع در تاریخ این مبحث تشخیص اینکه این چهار خاصیت نقشی کلیدی دارند زمان زیادی برده است. ما این بصیرت تاریخی را مغتنم شمرده و با آن نه فقط این خواص را برای مطالعهٔ $A(S)$ اختیار می‌کنیم بلکه از آنها به‌عنوان راهنمای اصلی در تجرید محدوده‌ای بسیار وسیعتر استفاده خواهیم کرد.

دیدیم که چهار خاصیت فوق به ما توان محاسبه در $A(S)$ را می‌بخشند، اما تفاوتهایی میان این نوع محاسبه و محاسباتی که با آنها خو گرفته‌ایم وجود دارند. اگر S سه یا بیش از سه عنصر داشته باشد، در مسئلهٔ ۱۵ در فصل ۱، بخش ۴، دیدیم که ممکن است به ازای $f, g \in A(S)$، $fg \neq gf$. لیکن این امر مشکلات زیادی ایجاد نخواهد کرد.

بحث را پایان داده به تعریف زیر می‌پردازیم.

تعریف. گوییم مجموعهٔ ناتهی G یک گروه است اگر در G عملی مانند $*$ چنان تعریف شده باشد که

الف) $a, b \in G$ ایجاب کنند که $a * b \in G$ (این با گفتن اینکه G تحت $*$ بسته است توصیف می‌شود)؛

ب) هرگاه $a, b, c \in G$، آنگاه $a * (b * c) = (a * b) * c$ (این با گفتن اینکه قانون شرکتپذیری در G برقرار است توصیف می‌شود)؛

پ) عنصر خاصی مانند $e \in G$ هست به‌طوری که به ازای هر $a \in G$، $a*e = e*a = a$ (e را عنصر همانی یا عنصر یکهٔ G می‌نامیم)؛

ت) به ازای هر $a \in G$ عنصری مانند $b \in G$ هست به‌طوری که $a * b = b * a = e$ (این b را به‌صورت a^{-1} نوشته و آن را معکوس a در G می‌نامیم).

این چهار اصل (اصول موضوع گروه) از خواص برقرار در $A(S)$ گرفته شده‌اند. لذا گروه بودن $A(S)$ نسبت به عمل «ترکیب نگاشتها» تعجبی نخواهد داشت.

عمل $*$ در G را معمولاً ضرب می‌نامند ولی باید به یاد داشت که این با ضربی که ما در اعداد صحیح، گویا، حقیقی، و یا مختلط می‌شناسیم ارتباطی ندارد. در واقع ذیلاً خواهیم دید که در بسیاری از مثالهای آشنا از گروهها که از اعداد ناشی می‌شوند ضرب عملاً جمع اعداد است. ولی لازم نیست هر گروه رابطه‌ای با یک مجموعه از اعداد داشته باشد. مجدداً تکرار می‌کنیم: یک گروه مجموعه‌ای است صادق در چهار اصل موضوع گروه، نه بیشتر نه کمتر.

پیش از آنکه به بررسی ماهیت گروهها بپردازیم به چند مثال نظر می‌افکنیم.

چند مثال از گروهها

۱. فرض کنیم $\mathbb{Z}$ مجموعهٔ تمام اعداد صحیح و $*$ جمع معمولی $+$ در آن باشد. بسته و شرکتپذیر بودن $\mathbb{Z}$ تحت $*$ از خواص اصلی اعداد صحیح است. عنصر یکهٔ e از $\mathbb{Z}$ تحت $*$ چیست؟ واضح است که چون $a = a * e = a + e$، داریم $e = \circ$، و $\circ$ عنصر همانی مطلوب تحت جمع است. a^{-1} چیست؟ در اینجا نیز چون $e = \circ = a * a^{-1} = a + a^{-1}$، a^{-1} در این وضع $-a$ است، و به وضوح داریم $a * (-a) = a + (-a) = \circ$.

۲. فرض کنیم $\mathbb{Q}$ مجموعهٔ تمام اعداد گویا بوده و عمل $*$ بر $\mathbb{Q}$ جمع معمولی اعداد گویا باشد. مثل فوق به آسانی معلوم می‌شود که $\mathbb{Q}$ تحت $*$ یک گروه است. توجه کنید که $\mathbb{Z} \subset \mathbb{Q}$ و هر دوی $\mathbb{Z}$ و $\mathbb{Q}$ تحت عمل یکسان $*$ گروه می‌باشند.

۳. فرض کنیم $\mathbb{Q}'$ مجموعهٔ تمام اعداد گویای ناصفر بوده و عمل $*$ بر $\mathbb{Q}'$ ضرب معمولی اعداد گویا باشد. از خواص آشنای اعداد گویا معلوم می‌شود که $\mathbb{Q}'$ نسبت به $*$ یک گروه است.

۴. فرض کنیم $\mathbb{R}'$ مجموعهٔ تمام اعداد حقیقی مثبت بوده و عمل $*$ بر $\mathbb{R}'$ ضرب معمولی اعداد حقیقی باشد. مجدداً به آسانی معلوم می‌شود که $\mathbb{R}'$ تحت $*$ یک گروه است.

۵. فرض کنیم E_n توانهای θ_n^i، $i = \circ, ۱, ۲, \ldots, n - ۱$، باشد که در آن $\theta_n = \cos(۲\pi/n) + i\sin(۲\pi/n)$. همچنین $\theta_n^k * \theta_n^j = \theta_n^{k+j}$ ضرب معمولی توانهای θ به‌عنوان اعدادی مختلط است. از قضیهٔ دموآور دیدیم که $\theta_n^n = ۱$. تحقیق گروه بودن E_n تحت $*$ به خواننده محول می‌شود.

به تفاوت آشکار بین مثالهای ۱ تا ۴ و مثال ۵ توجه کنید؛ چهار گروه اول بی‌نهایت عنصر دارند ولی E_n تعدادی متناهی (n) عنصر دارد.

تعریف. گوییم گروه G یک گروه متناهی است اگر تعدادی متناهی عنصر داشته باشد. تعداد عناصر G را مرتبهٔ G نامیده و با $|G|$ نشان می‌دهیم.

مثلاً E_n یک گروه متناهی است و $|E_n| = n$.

تمام مثالهای فوق در خاصیت اضافی $a * b = b * a$ به ازای هر جفت از عناصر صدق می‌کنند. این خاصیت لازم نیست در یک گروه برقرار باشد. شاهد ما $A(S)$ است که در آن S سه یا بیش از سه عنصر داشته باشد. در این گروه دیدیم که می‌توان $f, g \in A(S)$ را چنان یافت

که $fg \neq gf$.

این ما را وا می‌دارد که گروههای G با خاصیت $a * b = b * a$ به ازای هر $a, b \in G$ را ممتاز سازیم.

تعریف. گوییم گروه G آبلی است اگر به ازای هر $a, b \in G$، $a * b = b * a$.

واژهٔ آبلی از نام ریاضیدان بزرگ نروژی، نیلزهنریک آبل (Niels Henrik Abel, 1802-1829) یکی از بزرگترین دانشمندانی که تاکنون نروژ به عالم علم هدیه کرده است، اخذ شده است.

گروهی که آبلی نباشد غیرآبلی نام دارد، نامی که چندان تعجب‌آور نیست.

حال چند مثال از گروههای غیرآبلی را ذکر می‌کنیم. البته $A(S)$ خانواده‌ای نامتناهی از این گروهها را به ما می‌دهد. حال چند مثال دیگر می‌آوریم که در آنها می‌توان نسبتاً سریع حساب کرد.

۶. فرض کنیم $\mathbb{R}$ مجموعهٔ تمام اعداد حقیقی بوده و G مجموعهٔ تمام نگاشتهای $T_{a,b} : \mathbb{R} \to \mathbb{R}$ با تعریف $T_{a;b}(r) = ar + b$ به ازای هر عدد حقیقی r باشد که در آن a و b اعدادی حقیقی بوده و $a \neq ۰$. مثلاً $T_{۵,-۶}$ چنان است که $T_{۵,-۶}(r) = ۵r - ۶$، $T_{۵,-۶}(۱۴) = ۵ \cdot ۱۴ - ۶ = ۶۴$، $T_{۵,-۶}(\pi) = ۵\pi - ۶$. $T_{a,b}$ها نگاشتهایی ۱-۱ از $\mathbb{R}$ به روی خوداند، و فرض کنیم $T_{a,b} * T_{c,d}$ حاصلضرب این نگاشتها باشد. بنابراین

$$\begin{aligned}(T_{a,b} * T_{c,d})(r) &= T_{a,b}(T_{c,d}(r)) = aT_{c,d}(r) + b = a(cr + d) + b \\ &= (ac)r + (ad + b) = T_{ac,ad+b}(r)\end{aligned}$$

لذا فرمول زیر را داریم

$$T_{a,b} * T_{c,d} = T_{ac,ad+b} \tag{۱}$$

این امر نشان می‌دهد که $T_{a,b} * T_{c,d}$ در G است زیرا در شرط عضویت G صدق می‌کند. لذا G تحت $*$ بسته است. چون راجع به حاصلضرب نگاشتها (یعنی ترکیب نگاشتها) صحبت می‌کنیم، $*$ شرکتپذیر می‌باشد. عنصر $i = T_{۱,۰}$ نگاشت همانی از $\mathbb{R}$ به روی خود است. بالاخره $T_{a,b}^{-۱}$ چیست؟ آیا می‌توان اعداد حقیقی $x \neq ۰$ و y را طوری یافت که

$$T_{a,b} * T_{x,y} = T_{x,y} * T_{a,b} = T_{۱,۰}?$$

حال به رابطهٔ (۱) باز می‌گردیم. می‌خواهیم $T_{ax,ay+b} = T_{1,0}$؛ یعنی $ax = 1$ و $ay + b = 0$. به یاد آورید که $a \neq 0$؛ پس اگر قرار دهیم $x = a^{-1}$ و $y = -a^{-1}b$، روابط مطلوب برقرارند. می‌توان فوراً تحقیق کرد که

$$T_{a,b} * T_{a^{-1},-a^{-1}b} = T_{a^{-1},-a^{-1}b} * T_{a,b} = T_{1,0}$$

پس G واقعاً گروه است.

$T_{c,d} * T_{a,b}$ چیست؟ بنابر فرمول (۱) که در آن a با c، c با a، b با d، و d با b عوض شده باشد، به‌دست می‌آوریم

$$T_{c,d} * T_{a,b} = T_{ca,cb+d} \tag{2}$$

لذا $T_{c,d} * T_{a,b} = T_{a,b} * T_{c,d}$ اگر و فقط اگر $bc + d = ad + b$. این مثلاً وقتی $a = 1$، $b = 1$، $c = 2$، و $d = 3$ برقرار نیست. لذا G غیرآبلی می‌باشد.

۷. فرض کنیم $G \supset H$، که در آن G گروه مثال ۶ است، با

$$H = \{T_{a,b} \in G | a \text{ و } b \text{ گویا}\}$$

تعریف شده باشد. گروه بودن H تحت عمل $*$ در G به خوانندهٔ محول می‌شود. H غیرآبلی می‌باشد.

۸. فرض کنیم $G \supset H \supset K$ که در آن H و G مانند فوق بوده و

$$K = \{T_{1,b} \in G | b \text{ حقیقی}\}$$

بر خواننده است تحقیق کند که K نسبت به عمل $*$ در G گروه است، ولی K آبلی می‌باشد.

۹. فرض کنیم S صفحه باشد، یعنی $S = \{(x, y) | x \text{ و } y \text{ حقیقی}\}$، و $f, g \in A(S)$ را با تعریف $f(x, y) = (-x, y)$ و $g(x, y) = (-y, x)$ در نظر می‌گیریم. f انعکاس نسبت به محور y و g دوران به اندازهٔ $90°$ خلاف عقربه‌های ساعت حول مبدأ است. حال تعریف می‌کنیم $G = \{f^i g^j | i = 0, 1;\ \ j = 0, 1, 2, 3\}$ و فرض می‌کنیم $*$ در G ضرب عناصر در $A(S)$ باشد. واضح است که نگاشت همانی $= g^4 = f^2$،

$$(f * g)(x, y) = (fg)(x, y) = f(g(x, y)) = f(-y, x) = (y, x)$$

و

$$(g * f)(x, y) = g(f(x, y)) = g(-x, y) = (-y, -x)$$

پس $g * f \neq f * g$. برخواننده است تحقیق کند که $g * f = f * g^{-1}$ و G یک گروه غیرآبلی از مرتبهٔ ۸ است. این گروه را گروه دو وجهی از مرتبهٔ ۸ می‌نامند. [سعی کنید برای $(f^i g^j) * (f^s g^t) = f^a g^b$ فرمولی بیابید که a و b را برحسب i، j، s، و t بیان دارد.]

۱۰. فرض کنیم S و f همانند مثال ۹ باشند. همچنین $n > 2$ و h دوران صفحه حول مبدأ به اندازهٔ زاویهٔ $2\pi/n$ در جهت خلاف عقربه‌های ساعت باشد. حال تعریف می‌کنیم $G = \{f^k h^j | k = 0, 1; j = 0, 1, 2, \ldots, n-1\}$ و ضرب $*$ در G را ضرب معمول نگاشتها می‌گیریم. می‌توان تحقیق کرد که نگاشت همانی $= f^2 = h^n$ و $fh = h^{-1} f$. با این روابط می‌توان (با کمی زحمت) نشان داد که G یک گروه غیرآبلی از مرتبهٔ $2n$ است. G گروه دووجهی از مرتبهٔ $2n$ می‌باشد.

۱۱. فرض کنیم $G = \{f \in A(S) | f(s) \neq s, s \in S$ به ازای فقط تعدادی متناهی $\}$ که در آن S یک مجموعهٔ نامتناهی است. حکم می‌کنیم که G تحت ضرب $*$ در $A(S)$ یک گروه است. شرکتپذیری در G خودبه‌خود برقرار است، زیرا قبلاً در $A(S)$ برقرار است. همچنین $i \in G$، زیرا به ازای هر $s \in S$، $i(s) = s$. لذا باید نشان دهیم که G تحت ضرب بسته است و هرگاه $f \in G$، آن‌گاه $f^{-1} \in G$.

ابتدا بسته بودن را نشان می‌دهیم. فرض کنیم $f, g \in G$. پس $f(s) = s$ جز مثلاً به ازای s_1، s_2، $\cdots$، s_n و $g(s) = s$ جز به ازای s'_1، s'_2، $\cdots$، s'_m. در این صورت، به ازای هر s غیر از s_1، s_2، $\cdots$، s_n، s'_1، $\cdots$، s'_m (و احتمالاً بعضی از اینها)، $(fg)(s) = f(g(s)) = s$. پس fg فقط تعدادی متناهی از عناصر S را حرکت می‌دهد؛ در نتیجه $fg \in G$.

بالاخره، هرگاه به ازای هر s غیر از s_1، s_2، $\cdots$، s_n، $f(s) = s$، آن‌گاه

$$f^{-1}(f(s)) = f^{-1}(s)$$

ولی $f^{-1}(s) = f^{-1}(f(s)) = (f^{-1} f)(s) = i(s) = s$. پس به ازای هر s جز s_1، $\cdots$، s_n، $f^{-1}(s) = s$. لذا $f^{-1} \in G$ و G در تمام اصول موضوع گروه صدق می‌کند؛ لذا G یک گروه می‌باشد.

۱۲. فرض کنیم G مجموعهٔ تمام نگاشتهای T_θ باشد که در آن T_θ دوران یک دایرهٔ مفروض حول مرکزش به اندازهٔ زاویهٔ θ در جهت عقربه‌های ساعت است. در G عمل $*$ را ترکیب نگاشتها

می‌گیریم. چون (به آسانی معلوم می‌شود) $T_\theta * T_\psi = T_{\theta+\psi}$، G تحت $*$ بسته است. اصول موضوع دیگر گروه را می‌توان به آسانی تحقیق کرد. توجه کنید که نگاشت همانی $= T_0 = T_{2\pi}$ و $T_\theta^{-1} = T_{-\theta} = T_{2\pi-\theta}$. G یک گروه آبلی می‌باشد.

همان‌طور که در مورد $A(S)$ شد، نماد فشردهٔ a^n را برای

$$\underbrace{a * a * a \cdots * a}_{n \text{ بار}}$$

معرفی کرده و به ازای هر عدد صحیح مثبت n تعریف می‌کنیم $a^{-n} = (a^{-1})^n$، و نیز قرار می‌دهیم $a^0 = e$. در این صورت قوانین معمول نماها برقرارند؛ یعنی به ازای هر دو عدد صحیح m و n، $(a^m)^n = a^{mn}$ و $a^m * a^n = a^{m+n}$.

توجه کنید که هرگاه G گروه اعداد صحیح تحت $+$ باشد، آن‌گاه a^n با نماد فوق مساوی na می‌باشد.

خواننده ممکن است از ۱۲ مثال فوق در مورد گروهها این ایده را بیابد که همهٔ (و یا تقریباً همهٔ) مجموعه‌ها با عملی مانند $*$ تشکیل گروه می‌دهند. این امر از واقعیت بدور است. حال چند مثال از ناگروهها را عرضه کرده و در هر حالت با امتحان چهار اصل موضوع گروه خواهیم دید که کدامها برقرار نیستند.

چند نامثال

۱. فرض کنیم G مجموعهٔ تمام اعداد صحیح بوده و $*$ ضرب معمولی اعداد صحیح در G باشد. چون به ازای $a, b \in G$، $a * b = ab$، G به وضوح نسبت به $*$ بسته و شرکتپذیر است. به‌علاوه عدد ۱ عنصریکه است، زیرا به ازای هر $a \in G$، $a * 1 = a1 = a = 1a = 1 * a$. لذا در سه‌چهارم راه اثبات گروه بودن Gایم. آنچه لازم داریم معکوس عناصر G نسبت $*$ است که در G باشند. ولی این امر برقرار نیست. واضح است که نمی‌توان عدد صحیح b را طوری یافت که $0 * b = 0b = 1$ زیرا به ازای هر b، $0 = 0b$. ولی حتی سایر اعداد صحیح نیز در G معکوس ندارند. به‌عنوان مثال نمی‌توان عدد صحیح b را چنان یافت که $3 * b = 1$ (زیرا این مستلزم آن است که $b = \frac{1}{3}$ و $\frac{1}{3}$ عددی صحیح نیست).

۲. فرض کنیم G مجموعهٔ تمام اعداد حقیقی ناصفر باشد و به ازای $a, b \in G$ تعریف می‌کنیم $a * b = a^2b$. مثلاً $4 * 5 = 4^2(5) = 80$. از اصول موضوع گروه کدامها تحت این عمل $*$ در G برقرارند و کدامها نیستند؟ واضح است که G تحت $*$ بسته است. آیا $*$ شرکتپذیر است؟ اگر چنین است، باید $(a * b) * c = a * (b * c)$ یعنی $(a * b)^2c = a^2(b * c)$؛ و در نتیجه $(a^2b)^2c = a^2(b^2c)$ که به‌صورت سادهٔ $a^2 = 1$ در می‌آید که فقط به ازای $a = \pm 1$

برقرار است. لذا قانون شرکتپذیری نسبت به * در حالت کلی در G برقرار نیست. به همین نحو می‌توان تحقیق کرد که G عنصر یکه ندارد. لذا بحث در باب معکوسها نسبت به * معنی نخواهد داشت.

۳. فرض کنیم G مجموعهٔ تمام اعداد صحیح مثبت تحت * باشد که $a * b = ab$ (ضرب معمولی اعداد صحیح). به آسانی می‌توان تحقیق کرد که G گروه نیست و این فقط به خاطر عدم وجود معکوس برای برخی (در واقع اغلب) عناصرش نسبت به * می‌باشد.

ما در تمرینات نیز چند نامثال دیگر از گروهها را خواهیم یافت.

مسائل

مسائل آسانتر

۱. معین کنید از مجموعه‌های G زیر با عمل ذکر شده کدامها گروهند. در صورت نبودن، اصول موضوعی را که برقرار نیستند مشخص نمایید:

الف) $G =$ مجموعهٔ تمام اعداد صحیح، $a * b = a - b$؛

ب) $G =$ مجموعهٔ تمام اعداد صحیح، $a * b = a + b + ab$؛

پ) $G =$ مجموعهٔ تمام اعداد صحیح نامنفی، $a * b = a + b$؛

ت) $G =$ مجموعهٔ تمام اعداد گویای مخالف -۱، $a * b = a + b + ab$؛

ث) $G =$ مجموعهٔ تمام اعداد گویای تحویل‌ناپذیر با مخرج بخشپذیر بر ۵، $a*b = a+b$؛

ج) G مجموعه‌ای است با بیش از یک عنصر و به ازای هر $a, b \in G$، $a * b = a$.

۲. درگروه G مثال ۶ نشان دهید که مجموعهٔ $H = \{T_{a,b} | a = \pm ۱, \text{حقیقی } b\}$ تحت عمل * در G یک گروه تشکیل می‌دهد.

۳. تحقیق کنید که مثال ۷ واقعاً یک گروه است.

۴. ثابت کنید Kی تعریف شده در مثال ۸ یک گروه آبلی است.

۵. در مثال ۹ ثابت کنید $g * f = f * g^{-۱}$، و نیز G گروهی است غیرآبلی و از مرتبهٔ ۸.

۶. فرض کنید H و G به‌ترتیب همانهای بوده در مثالهای ۶ و ۷ باشند. نشان دهید هرگاه $T_{a,b} \in G$، آن‌گاه به ازای $V \in H$، $T_{a,b} * V * T_{a,b}^{-۱} \in H$.

۷. مسئلهٔ ۶ را برای گروه $K \subset G$ مثال ۸ حل کنید.

۸. اگر G یک گروه آبلی باشد، ثابت کنید به ازای هر عدد صحیح n، $(a * b)^n = a^n * b^n$.

۹. اگر در گروه G به ازای هر $a \in G$ داشته باشیم $a^{2} = e$، نشان دهید که G آبلی است.

۱۰. اگر G گروه مثال ۶ باشد، جمیع $T_{a,b} \in G$ها را طوری بیابید که به ازای هر x حقیقی، $T_{a,b} * T_{1,x} = T_{1,x} * T_{a,b}$.

۱۱. در مثال ۱۰، به ازای $n = 3$ فرمولی برای $(f^{i}h^{j}) * (f^{s}h^{t})$ به‌صورت $f^{a}h^{b}$ بیابید. با این فرمول نشان دهید که G یک گروه غیرآبلی از مرتبهٔ ۶ است.

۱۲. مسئلهٔ ۱۱ را به ازای $n = 4$ حل کنید.

۱۳. نشان دهید که هر گروه از مرتبهٔ ۴ یا کمتر آبلی است.

۱۴. اگر G گروهی دلخواه بوده و $a, b, c \in G$، نشان دهید هرگاه $a * b = a * c$، آن‌گاه $b = c$، و هرگاه $b * a = c * a$، آن‌گاه $b = c$.

۱۵. $(a * b)^{-1}$ را برحسب a^{-1} و b^{-1} بیان دارید.

۱۶. با استفاده از مسئلهٔ ۱۵ ثابت کنید گروه G که در آن به ازای هر $a \in G$، $a = a^{-1}$ باید آبلی باشد.

۱۷. در هر گروه G ثابت کنید به ازای هر $a \in G$، $(a^{-1})^{-1} = a$.

۱۸. اگر G یک گروه متناهی از مرتبهٔ زوج باشد، نشان دهید که باید عنصری مانند $a \neq e$ موجود باشد به‌طوری که $a = a^{-1}$. (راهنمایی. از مسئلهٔ ۱۷ استفاده کنید.)

۱۹. نشان دهید که در S_3 چهار عنصر x صادق در $x^{2} = e$ و سه عنصر y صادق در $y^{3} = e$ وجود دارند.

۲۰. جمیع عناصر واقع در S_4 با خاصیت $x^{4} = e$ را بیابید.

مسائل با سطح متوسط

۲۱. نشان دهید که هر گروه از مرتبهٔ ۵ باید آبلی باشد.

۲۲. نشان دهید که مجموعهٔ تعریف شده در مثال ۱۰ یک گروه غیرآبلی از مرتبهٔ $2n$ است. این امر را با یافتن فرمولی برای بیان $(f^{i}h^{j}) * (f^{s}h^{t})$ به شکل $f^{a}h^{b}$ انجام دهید.

۲۳. در گروه G مثال ۶ جمیع عناصر $U \in G$ را بیابید که به ازای هر $T_{a,b} \in G$،

$$U * T_{a,b} = T_{a,b} * U$$

۲۴. اگر G گروه دووجهی از مرتبهٔ $2n$ تعریف شده در مثال ۱۰ باشد، ثابت کنید

الف) هرگاه n فرد بوده و $a \in G$ چنان باشد که به ازای هر $b \in G$، $a * b = b * a$، آن‌گاه $a = e$؛

ب) اگر n زوج باشد، نشان دهید که عنصری مانند $a \in G$، $a \neq e$، وجود دارد به‌طوری که به ازای هر $b \in G$، $a * b = b * a$؛

پ) اگر n زوج باشد، جمیع عناصر $a \in G$ را چنان بیابید که به ازای هر $b \in G$، $a * b = b * a$.

۲۵. اگر G یک گروه باشد، نشان دهید که

الف) e منحصر به‌فرد است (یعنی هرگاه $f \in G$ نیز یک عنصر یکهٔ G باشد، آن‌گاه $f = e$)؛

ب) هرگاه $a \in G$، آن‌گاه $a^{-1} \in G$ منحصر به‌فرد است.

۲۶. اگر G یک گروه متناهی باشد، ثابت کنید به ازای هر $a \in G$ عدد صحیح مثبتی مانند n (تابع a) هست به‌طوری که $a^n = e$.

۲۷. در مسئلهٔ ۲۶ نشان دهید که عدد صحیحی مانند $m > 0$ هست به طوری که به ازای هر $a \in G$، $a^m = e$.

مسائل مشکلتر

۲۸. فرض کنید مجموعهٔ G با عمل $*$ چنان باشد که

۱. G تحت $*$ بسته بوده؛

۲. $*$ شرکتپذیر باشد؛

۳. عنصری مانند $e \in G$ باشد به‌طوری که به ازای هر $x \in G$، $e * x = x$؛

۴. به ازای هر $x \in G$ عنصری مانند $y \in G$ باشد به‌طوری که $y * x = e$.

ثابت کنید G یک گروه است. (پس باید نشان دهید که به ازای e و y به‌صورت فوق، $x * e = x$ و $x * y = e$.)

۲۹. فرض کنید مجموعهٔ متناهی G با عمل $*$ چنان باشد که

۱. G تحت $*$ بسته بوده؛

۲. $*$ شرکتپذیر باشد؛

۳. هرگاه $a, b, c \in G$ و $a * b = a * c$، آن‌گاه $b = c$؛

۴. هرگاه $a, b, c \in G$ و $b * a = c * a$، آن‌گاه $b = c$.

ثابت کنید G باید تحت $*$ یک گروه باشد.

۳۰. با مثال نشان دهید که مسئلهٔ ۲۹ می‌تواند در صورت نامتناهی بودن مجموعهٔ G نادرست باشد.

۳۱. فرض کنید G گروه تمام اعداد حقیقی ناصفر تحت عمل $*$ (که ضرب معمولی اعداد حقیقی است) بوده و H گروه تمام اعداد حقیقی تحت عمل # (که جمع اعداد حقیقی است) باشد.

الف) نشان دهید یک نگاشت مانند $F : G \to H$ از G به روی H هست که در

$$F(a * b) = F(a)\#F(b)$$

به ازای هر $a, b \in G$ صدق می‌کند [یعنی $F(ab) = F(a) + F(b)$].

ب) نشان دهید که نگاشت F نمی‌تواند ۱-۱ باشد.

۲. چند تبصرهٔ ساده

در این بخش کوتاه نشان می‌دهیم که بعضی از خواص صوری ناشی از اصول موضوع گروه در هر گروه برقرارند. در واقع اغلب این نتایج قبلاً به‌صورت مسئله در آخر بخش پیش آمده‌اند.

چون نوشتن ضرب G به‌صورت $*$ کمی ناشیانه است، از حالا به بعد حاصلضرب $a * b$ به ازای هر $a, b \in G$ را فقط به‌صورت ab می‌نویسیم.

در لم زیر اولین نتایج صوری از این نوع ثابت شده‌اند.

لم ۲.۲.۱. هرگاه G یک گروه باشد، آن‌گاه

الف) عنصر همانی‌اش منحصر به‌فرد است؛

ب) هر $a \in G$ معکوس منحصر به‌فردی مانند $a^{-1} \in G$ دارد؛

پ) اگر $a \in G$، $(a^{-1})^{-1} = a$؛

ت) به ازای هر $a, b \in G$، $(ab)^{-1} = b^{-1}a^{-1}$.

برهان. با قسمت (الف) شروع می‌کنیم. در اثبات چه باید بکنیم؟ باید نشان دهیم هرگاه $e, f \in G$ و به ازای هر $a \in G$، $af = fa = a$ و به ازای هر $a \in G$، $ae = ea = a$، آن‌گاه $e = f$. این کار بسیار آسان است، زیرا داریم $e = ef$ و $f = ef$. پس، طبق حکم، $e = ef = f$.

به‌جای اثبات قسمت (ب) نتیجهٔ قویتری را (که ذیلاً به‌صورت لم ۲.۲.۲ درآمده) ثابت می‌کنیم. از این نتیجه قسمت (ب) فوراً به‌دست می‌آید. حکم می‌کنیم که در گروه G هرگاه $ab = ac$، آن‌گاه $b = c$؛ یعنی می‌توان از طرفین یک معادله عنصری را حذف کرد. برای مشاهدهٔ این امر، گوییم به ازای هر $a \in G$ عنصری مانند $u \in G$ هست به طوری که $ua = e$. لذا از $ab = ac$ داریم

$$u(ab) = u(ac)$$

پس، طبق قانون شرکتپذیری، $(ua)b = (ua)c$؛ یعنی $eb = ec$. لذا $b = eb = ec = c$ و نتیجه حاصل می‌باشد. استدلالی مشابه نشان می‌دهد که هرگاه $ba = ca$، آن‌گاه $b = c$. اما از $ab = ca$ نمی‌توان نتیجه گرفت که $b = c$؛ این در هر گروه آبلی درست است ولی در حالت کلی برقرار نیست.

حال برای به‌دست آوردن قسمت (ب) به‌عنوان نتیجه‌ای از خاصیت حذف، فرض کنیم $b, c \in G$ معکوسهای a باشند. در این صورت $ab = e = ac$. پس، بنابر خاصیت حذف، $b = c$ و معکوس a منحصر به‌فرد است. ما همواره آن را به‌صورت a^{-1} خواهیم نوشت.

برای اثبات قسمت (پ)، از تعریف داریم $a^{-1}(a^{-1})^{-1} = e$. ولی $a^{-1}a = e$. پس، بنابر خاصیت حذف در $a^{-1}(a^{-1})^{-1} = e = a^{-1}a$، به‌دست می‌آوریم $(a^{-1})^{-1} = a$.

بالاخره برای قسمت (ت) داریم

$$
\begin{aligned}
(ab)(b^{-1}a^{-1}) &= ((ab)b^{-1})a^{-1} && \text{(قانون شرکتپذیری)}\\
&= (a(bb^{-1}))a^{-1} && \text{(مجدداً قانون شرکتپذیری)}\\
&= (ae)a^{-1} = aa^{-1} = e
\end{aligned}
$$

به همین نحو $(b^{-1}a^{-1})(ab) = e$. لذا، طبق تعریف، $(ab)^{-1} = b^{-1}a^{-1}$. ■

ما قول داده‌ایم که بخشی از استدلال فوق را به‌صورت لمی جدا گانه ذکر کنیم. حال به این قول وفا کرده و می‌نویسیم:

لم ۲.۲.۲. در هر گروه G، هرگاه $a, b, c \in G$ و

الف) $ab = ac$، آن‌گاه $b = c$؛

ب) $ba = ca$، آن‌گاه $b = c$.

پیش از ترک این نتایج توجه می‌کنیم که اگر G گروه اعداد حقیقی تحت + باشد، قسمت (پ) لم ۱.۲.۲ به‌صورت آشنای $-(-a) = a$ در می‌آید.

در این بخش مقدار کمی ریاضیات وجود دارد. لذا به تعداد کمی مسئله قناعت می‌کنیم. همچنین به درجهٔ سختی مسائل اشاره‌ای نخواهیم کرد.

مسائل

۱. فرض کنید مجموعهٔ G تحت یک عمل شرکتپذیر بسته باشد به‌طوری که

۱. به ازای هر $a, y \in G$، $x \in G$ ی باشد که $ax = y$؛
۲. به ازای هر $a, w \in G$، $u \in G$ ای باشد که $ua = w$.
نشان دهید که G یک گروه است.

۲. اگر مجموعهٔ متناهی G تحت یک عمل شرکتپذیر بسته باشد به‌طوری که $ax = ay$ تساوی $x = y$ و $ua = wa$ تساوی $u = w$ را به ازای هر $a, x, y, u, w \in G$ ایجاب کند، ثابت کنید G یک گروه می‌باشد. (این تکرار مسئله‌ای است که قبلاً آمده است. از این مسئله بعدها در متن استفاده خواهد شد.)

۳. اگر در گروه G به ازای سه عدد صحیح متوالی i، $(ab)^i = a^i b^i$، ثابت کنید G آبلی است.

۴. نشان دهید که اگر در مسئلهٔ ۳ کلمهٔ «سه» با «دو» عوض شود، مسئله همیشه درست نیست. به‌عبارت دیگر، نشان دهید که گروهی چون G و اعدادی متوالی مانند i و $i + 1$ وجود دارند به‌طوری که G آبلی نبوده ولی دارای این خاصیت است که به ازای هر a و b در G، $(ab)^i = a^i b^i$ و $(ab)^{i+1} = a^{i+1} b^{i+1}$.

۵. فرض کنید در گروه G به ازای هر $a, b \in G$، $(ab)^3 = a^3 b^3$ و $(ab)^5 = a^5 b^5$. نشان دهید که G آبلی است.

۶. فرض کنید گروه G چنان باشد که به ازای عدد صحیح ثابتی چون $n > 1$ و هر $a, b \in G$، $(ab)^n = a^n b^n$. ثابت کنید به ازای هر $a, b \in G$،
الف) $(ab)^{n-1} = b^{n-1} a^{n-1}$؛
ب) $a^n b^{n-1} = b^{n-1} a^n$؛
پ) $(aba^{-1}b^{-1})^{n(n-1)} = e$.
[راهنمایی برای قسمت (پ). توجه کنید که به ازای جمیع اعداد صحیح r، $(aba^{-1})^r = ab^r a^{-1}$.]

۳. زیرگروهها

بررسی تمام گروه G برای کسب اطلاعات بیشتر راجع‌به آن ممکن است کار زیادی را طلب کند. ممکن است بخواهیم معطوف بخشهای مناسبی از G شویم که کوچکتر بوده و روی آنها کنترل بیشتری داریم و ضمناً چنانند که اطلاعات مربوط به آنها را می‌توان برای کسب اطلاعات و بصیرتی راجع‌به خود G به‌کار برد. بدین‌ترتیب سؤال زیر مطرح می‌شود: چه بخشهایی از G برای این نوع تشریح مناسب‌اند؟ واضح است که این بخشها هر چه باشند باید انعکاس‌دهندهٔ این واقعیت باشند

که G یک گروه است نه فقط یک مجموعهٔ قدیمی.

یک گروه با یک مجموعهٔ معمولی این فرق را دارد که دارای عملی خوشرفتار است. لذا طبیعی است که بخواهیم قسمتهای فوق‌الذکر نسبت به عمل G رفتار معقولی داشته باشند. با تضمین این امر، بی‌درنگ به مفهوم زیرگروه یک گروه خواهیم رسید.

تعریف. زیرمجموعهٔ ناتهی H از گروه G یک زیرگروه G نام دارد اگر H نسبت به ضرب در G خود یک گروه باشد.

ما بر عبارت «نسبت به ضرب در G» تأکید می‌کنیم. مثلاً زیرمجموعهٔ $A = \{۱, -۱\}$ در $\mathbb{Z}$ (مجموعهٔ اعداد صحیح) را اختیار می‌کنیم. A تحت ضرب اعداد صحیح یک گروه است. ولی A زیرگروه $\mathbb{Z}$ (به‌عنوان یک گروه نسبت به $+$) نیست.

هر گروه G خودبه‌خود دو زیرگروه واضح دارد که عبارتند از خود G و زیرگروه مرکب از فقط عنصر همانی e. ما این دو زیرگروه را زیرگروههای بدیهی می‌نامیم. توجه ما بیشتر به سایر زیرگروهها، یعنی زیرگروههای حقیقی، G می‌باشد.

پیش از آنکه نگاه نزدیکتری به ویژگی کلی زیرگروهها بیفکنیم، به زیرگروههایی از چند گروه خاص نظری می‌افکنیم. برخی از این گروهها همانهایی هستند که در مثالهای بخش ۱ عنوان شدند. ما شماره‌گذاری آنها را حفظ می‌کنیم. در بعضی از این مثالها تحقیق می‌کنیم که برخی از زیرمجموعه‌های آنها به واقع زیرگروهند. به خواننده قویاً توصیه می‌شود که این کار را برای زیرمجموعه‌های بسیار دیگر انجام داده و مثالهای دیگری برای خود بیابد.

ما در اثبات زیرگروه بودن زیرمجموعه‌ای از یک گروه یکی از اصول موضوع گروه (یعنی قانون شرکتپذیری) را امتحان نمی‌کنیم. چون قانون شرکتپذیری در گروه G برقرار است، این قانون به ازای هر سه عنصر از زیرمجموعهٔ A از G نیز چنین می‌باشد. لذا برای زیرمجموعهٔ A از G باید امتحان کرد که آیا A تحت عمل G بسته است، آیا e در A است، و بالاخره به ازای هر $a \in A$، آیا $a^{-۱}$ نیز در A است یا نه.

همچنین می‌توان یک محاسبهٔ دیگر را نیز انجام نداد. فرض کنیم $A \subset G$ ناتهی بوده و به ازای هر $a, b \in A$، $ab \in A$. همچنین هرگاه $a \in A$، آن‌گاه $a^{-۱} \in A$. در این صورت حکم می‌کنیم که $e \in A$. زیرا $a \in A$ را اختیار می‌کنیم. پس، طبق فرض، $a^{-۱} \in A$. لذا، مجدداً طبق فرض، $aa^{-۱} \in A$. چون $aa^{-۱} = e$، داریم $e \in A$. لذا A یک زیرگروه G است. به‌عبارت دیگر:

لم ۱.۳.۲. زیرمجموعهٔ ناتهی $A \subset G$ زیرگروه G است اگر و فقط اگر A نسبت به عمل G بسته بوده و هرگاه $a \in A$، آن‌گاه $a^{-۱} \in A$.

حال به چند مثال می‌پردازیم.

چند مثال

۱. فرض کنیم G گروه اعداد صحیح $\mathbb{Z}$ تحت $+$ و H مجموعهٔ اعداد صحیح زوج باشد. حکم می‌کنیم که H زیرگروه $\mathbb{Z}$ است. چرا؟ آیا H بسته است؛ یعنی به ازای هر $a, b \in H$، آیا $a + b \in H$؟ به عبارت دیگر، اگر a و b اعداد صحیح زوجی باشند، آیا $a + b$ یک عدد صحیح زوج است؟ جواب مثبت است. پس H تحت $+$ بسته است. حال در مورد معکوس. چون عمل $\mathbb{Z}$ به‌علاوه است، معکوس $a \in \mathbb{Z}$ نسبت به این عمل $-a$ است. هرگاه $a \in H$، یعنی a زوج باشد، آن‌گاه $-a$ نیز زوج است؛ پس $-a \in H$. به بیان کوتاه، H زیرگروه $\mathbb{Z}$ تحت $+$ می‌باشد.

۲. فرض کنیم G مجدداً گروه اعداد صحیح $\mathbb{Z}$ تحت $+$ باشد. در مثال ۱ مجموعهٔ اعداد صحیح زوج H را می‌توان به نحوی دیگر توصیف کرد؛ یعنی H عبارت است از تمام مضارب ۲. در مثال ۱ از خود ۲ استفاده‌ای نشد. فرض کنیم $m > ۱$ عددی صحیح بوده و H_m از تمام مضارب m در $\mathbb{Z}$ تشکیل شده باشد. بر خواننده است تحقیق کند که H_m زیرگروهی از $\mathbb{Z}$ تحت $+$ می‌باشد.

۳. فرض کنیم S زیرمجموعه‌ای ناتهی بوده و $G = A(S)$. اگر $a \in S$، قرار می‌دهیم $H(a) = \{f \in A(S) | f(a) = a\}$. حکم می‌کنیم که $H(a)$ زیرگروه G است. زیرا هرگاه $f, g \in H(a)$ آن‌گاه $(fg)(a) = f(g(a)) = f(a) = a$، زیرا $f(a) = g(a) = a$. لذا $fg \in H(a)$. همچنین هرگاه $f \in H(a)$، آن‌گاه $f(a) = a$؛ پس $f^{-۱}(f(a)) = f^{-۱}(a)$. اما $f^{-۱}(f(a)) = f^{-۱}(a) = i(a) = a$. لذا، چون $a = f^{-۱}(f(a)) = f^{-۱}(a)$، داریم $f^{-۱} \in H(a)$. در نتیجه $H(a)$ زیرگروه G است.

۴. فرض کنیم G همانند مثال ۶ و H همانند مثال ۷ در بخش ۱ باشد. H زیرگروه G است (ر.ک. مسئلهٔ ۳ در بخش ۱).

۵. فرض کنیم G همانند مثال ۶ و K همانند مثال ۸ در بخش ۱ باشد. در این صورت $K \subset H \subset G$ و K زیرگروه هر دوی H و G می‌باشد.

۶. فرض کنیم $\mathbb{C}'$ مجموعهٔ اعداد مختلط ناصفر به‌عنوان گروه تحت ضرب اعداد مختلط باشد. همچنین $V = \{a \in \mathbb{C}' | \text{گویاست} |a|\}$. در این صورت V زیرگروه $\mathbb{C}'$ است. زیرا هرگاه $|a|$ و $|b|$ گویا باشند، آن‌گاه $|ab| = |a||b|$ گویاست؛ پس $ab \in V$. همچنین $|a^{-۱}| = ۱/|a|$

گویاست؛ پس $a^{-1} \in V$. بنابراین، V زیرگروه $\mathbb{C}'$ می‌باشد.

۷. فرض کنیم $\mathbb{C}'$ و V مانند فوق بوده و قرار می‌دهیم

$$U = \{a \in \mathbb{C}' | a = \cos\theta + i\sin\theta \text{، } \theta \text{ عدد حقیقی دلخواه}\}$$

اگر $a = \cos\theta + i\sin\theta$ و $b = \cos\psi + i\sin\psi$، در فصل ۱ دیدیم که

$$ab = \cos(\theta+\psi) + i\sin(\theta+\psi)$$

پس $ab \in U$، و نیز $a^{-1} = \cos\theta - i\sin\theta = \cos(-\theta) + i\sin(-\theta) \in U$. همچنین $|a| = 1$، زیرا $|a| = \sqrt{\cos^2\theta + \sin^2\theta} = 1$. لذا $U \subset V \subset \mathbb{C}'$ و U زیرگروه هر دوی V و $\mathbb{C}'$ می‌باشد.

۸. فرض کنیم $\mathbb{C}'$ و U و V مانند فوق بوده و $n > 1$ عددی صحیح باشد. همچنین $\theta_n = \cos(2\pi/n) + i\sin(2\pi/n)$ و $B = \{1, \theta_n, \theta_n^2, \ldots, \theta_n^{n-1}\}$. چون (همان‌طور که از قضیهٔ دموآور دیدیم) $\theta^n = 1$، به آسانی معلوم می‌شود که B زیرگروه U و V و $\mathbb{C}'$ بوده و از مرتبهٔ n می‌باشد.

۹. فرض کنیم G یک گروه بوده و $a \in G$. مجموعهٔ $A = \{a^i | i \text{عدد صحیح دلخواه}\}$ زیرگروه G است. زیرا، طبق قواعد نماها، هرگاه $a^i \in A$ و $a^j \in A$، آن‌گاه $a^i a^j = a^{i+j}$؛ پس در A است. همچنین $(a^i)^{-1} = a^{-i}$؛ پس $(a^i)^{-1} \in A$. این امر A را زیرگروه G می‌سازد.

A زیرگروه دوری G تولید شده به‌وسیلهٔ a به مفهوم زیر می‌باشد.

تعریف. زیرگروه دوری G تولید شده به‌وسیلهٔ a مجموعهٔ $\{a^i | i \text{ عدد صحیح دلخواه}\}$ می‌باشد. این زیرگروه را با (a) نشان می‌دهیم.

توجه کنید که هرگاه e عنصر همانی G باشد، آن‌گاه $(e) = \{e\}$. گروه مثال ۸ عبارت است از گروه دوری (θ_n) از $\mathbb{C}$ که به وسیلهٔ θ_n تولید شده است.

۱۰. فرض کنیم G یک گروه باشد. به ازای $a \in G$ قرار می‌دهیم

$$C(a) = \{g \in G | ga = ag\}$$

حکم می‌کنیم که $C(a)$ زیرگروه G است. ابتدا به بسته بودن $C(a)$ می‌پردازیم. هرگاه $g, h \in C(a)$،

آن‌گاه $ga = ag$ و $ha = ah$. لذا، با استفادهٔ مکرر از قانون شرکتپذیری،

$$(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh).$$

در نتیجه، $gh \in C(a)$. همچنین هرگاه $g \in C(a)$، آن‌گاه از $ga = ag$ داریم

$$g^{-1}(ga)g^{-1} = g^{-1}(ag)g^{-1}$$

که به‌صورت $ag^{-1} = g^{-1}a$ ساده می‌شود، که از آنجا $g^{-1} \in C(a)$. پس $C(a)$ زیر گروه G می‌باشد.

زیرگروههای خاص $C(a)$ بعدها ظاهر خواهند شد و ما نامی خاص به آنها می‌دهیم. ما $C(a)$ را مرکز ساز a در G می‌نامیم. اگر در یک گروه $ab = ba$، گوییم a و b با هم تعویض می‌شوند. لذا $C(a)$ مجموعهٔ تمام عناصری در G است که با a تعویض می‌شوند.

۱۱. فرض کنیم G گروه بوده و $\mathbb{Z}(G) = \{z \in G | zx = xz$ ،$x \in G$ به ازای هر$\}$. برخواننده است تحقیق کند که $\mathbb{Z}(G)$ زیرگروه G است. این زیرگروه را مرکز G می‌نامیم.

۱۲. فرض کنیم G گروه و H زیرگروهی از آن باشد. به ازای $a \in G$ قرار می‌دهیم $a^{-1}Ha = \{a^{-1}ha | h \in H\}$. حکم می‌کنیم $a^{-1}Ha$ زیرگروه G است. اگر $x = a^{-1}h_1a$ و $y = a^{-1}h_2a$ که در آنها $h_1, h_2 \in H$، آن‌گاه

$$xy = (a^{-1}h_1a)(a^{-1}h_2a) = a^{-1}(h_1h_2)a \qquad (\text{قانون شرکتپذیری})$$

و چون H زیرگروه G است، $h_1h_2 \in H$. بنابراین، $a^{-1}(h_1h_2)a \in a^{-1}Ha$ بیانگر آن است که $xy \in a^{-1}Ha$. لذا $a^{-1}Ha$ بسته است. همچنین هرگاه $x = a^{-1}ha \in a^{-1}Ha$، آن‌گاه به‌آسانی معلوم می‌شود که

$$x^{-1} = (a^{-1}ha)^{-1} = a^{-1}h^{-1}a \in a^{-1}Ha$$

بنابراین، $a^{-1}Ha$ زیرگروه G است.

ظاهراً یک دوجین مثال از زیرگروهها باید برایمان کافی باشد. لذا به نکات دیگر می‌پردازیم. لم ۱.۳.۲ به موارد نیاز برای زیرگروه بودن یک زیرمجموعه از یک گروه اشاره دارد. در یک حالت خاص مهم می‌توان در امتحان زیرگروه G بودن زیرمجموعهٔ H زحمت زیادی را کم کرد و این در حالتی است که H متناهی می‌باشد.

لم ۲.۳.۲. فرض کنیم G گروه و H زیرمجموعه‌ای ناتهی و متناهی از G باشد که تحت ضرب در G بسته است. در این صورت H زیرگروه G می‌باشد.

برهان. بنابر لم ۱.۳.۲ باید نشان داد که $a \in H$ عضویت $a^{-1} \in H$ را ایجاب می‌کند. گوییم هرگاه $a = e$، آن‌گاه $a^{-1} = e$ و کار تمام است. حال فرض کنیم $a \neq e$. عنصرهای a، a^{2}، $\cdots$، a^{n+1} را در نظر می‌گیریم که در آنها $n = |H|$ (مرتبهٔ H). در اینجا $n+1$ عنصر نوشته شده است که همه در Hاند زیرا H با آنکه فقط n عنصر متمایز دارد بسته است. این امر چطور ممکن است؟ این فقط وقتی امکان دارد که دو عنصر لیست شده مساوی باشند. به بیان دیگر، فقط وقتی که به ازای i و jای با خاصیت $1 \leq i < j \leq n+1$، $a^{i} = a^{j}$. ولی، طبق خاصیت حذف در گروهها، $a^{j-i} = e$. چون $j - i \geq 1$، $a^{j-i} \in H$؛ در نتیجه $e \in H$. اما $j - i - 1 \geq 0$. پس $a^{j-i-1} \in H$ و $aa^{j-i-1} = a^{j-i} = e$ که از آنجا $a^{-1} = a^{j-i-1} \in H$. این لم ما را ثابت خواهد کرد. ■

یک نتیجهٔ فوری ولی مهم از لم ۲.۳.۲ به قرار زیر است.

نتیجه. هرگاه G یک گروه متناهی بوده و زیرمجموعهٔ ناتهی H از G تحت ضرب بسته باشد، آن‌گاه H زیرگروه G می‌باشد.

مسائل

مسائل آسانتر

۱. اگر A و B زیرگروههایی از G باشند، نشان دهید که $A \cap B$ نیز زیرگروهی است از G.

۲. زیرگروه دوری $\mathbb{Z}$ تولید شده به‌وسیلهٔ -1 تحت $+$ چیست؟

۳. فرض کنید S_3 گروه متقارن از درجهٔ ۳ باشد. تمام زیرگروههای S_3 را بیابید.

۴. تحقیق کنید که $\mathbb{Z}(G)$ (مرکز G) زیرگروه G است. (ر.ک. مثال ۱۱.)

۵. اگر $C(a)$ مرکزساز a در G باشد (مثال ۱۰)، ثابت کنید $Z(G) = \cap_{a\in G} C(a)$.

۶. نشان دهید $a \in Z(G)$ اگر و فقط اگر $C(a) = G$.

۷. $C(a)$ را به ازای هر $a \in S_3$ بیابید.

۸. اگر G یک گروه آبلی بوده و $H = \{a \in G | a^{2} = e\}$، نشان دهید که H زیرگروه G است.

۹. یک گروه غیر آبلی مثال بزنید که مجموعهٔ H مسئلهٔ ۸ زیرگروهش نباشد.

۱۰. اگر G یک گروه آبلی بوده و $n > 1$ عددی صحیح باشد، قرار دهید $A_n = \{a^n | a \in G\}$ و ثابت کنید A_n زیرگروه G است.

۱۱*. اگر G یک گروه آبلی بوده و $H = \{a \in G | a^{n(a)} = e$، به ازای $n(a) > 1$ای تابع $a\}$، ثابت کنید H زیرگروه G است.

گروه G دوری است اگر عنصری مانند $a \in G$ باشد به‌طوری که هر $x \in G$ توانی از a باشد؛ یعنی به ازای jای، $x = a^j$. a را مولد G می‌نامیم.

۱۲. ثابت کنید هر گروه دوری آبلی است.

۱۳. اگر G دوری باشد، نشان دهید که هر زیرگروه G دوری است.

۱۴. اگر G زیرگروه حقیقی نداشته باشد، ثابت کنید G دوری است.

۱۵. اگر G یک گروه بوده و H زیرمجموعه‌ای ناتهی از G باشد به‌طوری که به ازای هر $a, b \in H$، $ab^{-1} \in H$، ثابت کنید H زیرگروه G است.

مسائل با سطح متوسط

۱۶. اگر G زیرگروه حقیقی نداشته باشد، ثابت کنید G دوری از مرتبهٔ p است که در آن p اول می‌باشد. (این امر مسئلهٔ ۱۴ را قویتر می‌سازد.)

۱۷. اگر G یک گروه بوده و $a, x \in G$، ثابت کنید $C(x^{-1}ax) = x^{-1}C(a)x$. [برای تعاریف $C(b)$ و $x^{-1}C(a)x$، ر.ک. مثالهای ۱۰ و ۱۲.]

۱۸. اگر S یک مجموعهٔ ناتهی بوده و $X \subset S$، نشان دهید که

$$T(X) = \{f \in A(S) | f(X) \subset X\}$$

زیرگروه $A(S)$ است اگر X متناهی باشد.

۱۹. اگر A و B زیرگروههایی از گروه آبلی G باشند، قرار دهید $AB = \{ab | b \in B, a \in A\}$ و ثابت کنید AB زیرگروه G است.

۲۰. گروه G و دو زیرگروه A و B از آن را طوری مثال بزنید که AB زیرگروه G نباشد.

۲۱. اگر A و B زیرگروههایی از G باشند به‌طوری که به ازای هر $b \in B$، $b^{-1}Ab \subset A$، نشان دهید که AB زیرگروه G است.

۲۲*. اگر A و B زیرگروههایی متناهی و به‌ترتیب از مرتبهٔ m و n گروه آبلی G باشند، ثابت کنید AB زیرگروهی از mn است اگر m و n نسبت به هم اول باشند.

۲۳. اگر در مسئلهٔ ۲۲ m و n نسبت به هم اول نباشند، مرتبهٔ AB چیست؟

۲۴. اگر H زیرگروه G باشد، قرار دهید $N = \bigcap_{x\in G} x^{-1}Hx$ و ثابت کنید N زیرگروه G است به‌طوری که به ازای هر $y \in G$، $y^{-1}Ny = N$.

مسائل مشکلتر

۲۵. فرض کنید S، X، و $T(X)$ همانند مسئلهٔ ۱۸ باشند (ولی X متناهی نباشد). مجموعهٔ S و زیرمجموعهٔ نامتناهی X را چنان مثال بزنید که $T(X)$ زیرگروه $A(S)$ نباشد.

۲۶. فرض کنید G یک گروه و H زیرگروهی از آن باشد. قرار دهید $Hx = \{hx|h \in H\}$ و نشان دهید که به ازای هر $a, b \in G$، $Ha = Hb$ یا $Ha \cap Hb = \varnothing$.

۲۷. اگر در مسئلهٔ ۲۶ H زیرگروهی متناهی از G باشد، ثابت کنید تعداد عناصر Ha و Hb یکی است. این تعداد چندتاست؟

۲۸. فرض کنید M و N زیرگروههایی از G باشند به‌طوری که به ازای هر $x \in G$، $x^{-1}Mx \subset M$ و $x^{-1}Nx \subset N$. ثابت کنید MN زیرگروه G بوده و به ازای هر $x \in G$،

$$x^{-1}(MN)x \subset MN$$

*۲۹. اگر M زیرگروهی از G باشد به‌طوری که به ازای هر $x \in G$، $x^{-1}Mx \subset M$، ثابت کنید در واقع $x^{-1}Mx = M$.

۳۰. اگر M و N چنان باشند که به ازای هر $x \in G$، $x^{-1}Mx = M$ و $x^{-1}Nx = N$ و نیز $M \cap N = (e)$، ثابت کنید به ازای هر $m \in M$ و $n \in N$، $mn = nm$. (راهنمایی. عنصر $mnm^{-1}n^{-1}$ را در نظر بگیرید.)

۴. قضیهٔ لاگرانژ

حال اولین نتیجهٔ مهم و واقعی نظریهٔ گروهها را به‌دست می‌آوریم. این قضیه، با آنکه اثبات ساده‌ای دارد، الفبای گروههای متناهی بوده و کاربردهای جالبی در نظریهٔ اعداد خواهد داشت.

در واقع کسانی که مسائل ۲۶ و ۲۷ بخش ۳ را حل کرده‌اند برای اثبات این قضیه آمادگی تام دارند. این قضیه صرفاً می‌گوید که در یک گروه متناهی مرتبهٔ یک زیرگروه مرتبهٔ آن گروه را عاد می‌کند.

برای فراهم ساختن زمینهٔ اثبات این قضیه (که منسوب به لاگرانژ است) و استفادهٔ مکرر بعدی از آن، گردش کوتاهی در نظریهٔ مجموعه‌ها می‌کنیم.

مفهوم «رابطه» مانند مفهوم «تابع» در اغلب بخشهای ریاضی نفوذ دارد. یک رابطه عبارت است از حکمی مانند aRb راجع به عناصر $a, b \in S$. اگر S مجموعهٔ اعداد صحیح باشد، $a = b$ یک رابطه بر S است. به همین نحو $a < b$ رابطه‌ای است بر S؛ و همچنین است $a \leq b$.

تعریف. رابطهٔ $\sim$ بر مجموعهٔ S یک رابطهٔ هم‌ارزی است اگر به ازای هر $a, b, c \in S$،

الف) $a \sim a$ (انعکاس)؛

ب) $a \sim b$ ایجاب کند که $b \sim a$ (تقارن)؛

پ) $a \sim b$ و $b \sim c$ ایجاب کنند که $a \sim c$ (تعدی).

البته تساوی $(=)$ یک رابطهٔ هم‌ارزی است؛ در نتیجه مفهوم کلی رابطهٔ هم‌ارزی تعمیمی است از تساوی. به‌طور دقیقتر، یک رابطهٔ هم‌ارزی تساوی را از جهتی می‌سنجد. این نکتهٔ مبهم پس از چند مثال روشنتر خواهد شد.

چند مثال

۱. فرض کنیم S مجموعهٔ تمام اجناس فروشی در یک مغازهٔ بقالی باشد. گوییم به ازای $a, b \in S$، $a \sim b$ اگر بهای a مساوی بهای b باشد. واضح است که قواعد معرف رابطهٔ هم‌ارزی برای این $\sim$ برقرارند. توجه کنید که در سنجش این «تساوی تعمیم‌یافته» بر S از جمیع خواص عناصر S جز بهای آنها صرف‌نظر شده است. لذا $a \sim b$ اگر تا جایی که به بهای آنها مربوط می‌شود با هم مساوی باشند.

۲. فرض کنیم S مجموعهٔ اعداد صحیح بوده و $n > ۱$ عدد صحیح ثابتی باشد. به ازای $a, b \in S$ تعریف می‌کنیم $a \sim b$ اگر $n|(a-b)$. تحقیق می‌کنیم که این یک رابطهٔ هم‌ارزی است. چون $a - a = ۰|n$، داریم $a \sim a$. و چون $n|(a-b)$ ایجاب می‌کند که

$$n|(b-a) = -(a-b)$$

$a \sim b$ ایجاب می‌کند که $b \sim a$. بالاخره هرگاه $a \sim b$ و $b \sim c$، آن‌گاه $n|(a-b)$ و $n|(b-c)$. پس $n|((a-b)+(b-c))$؛ یعنی $n|(a-c)$. بنابراین $a \sim c$.

این رابطه بر اعداد صحیح در نظریهٔ اعداد اهمیت بسیار داشته و همنهشتی به پیمانهٔ n خوانده می‌شود. وقتی $a \sim b$، آن را به‌صورت $a \equiv b \mod (n)$ [یا گاهی به‌صورت $a \equiv b(n)$] نوشته و می‌خوانیم: «a همنهشت b به پیمانهٔ n است.» ما با این رابطه مکرر بر خواهیم خورد. همان‌طور که خواهید دید، این حالت خاصی است از یک پدیدهٔ بسیار وسیعتر در گروهها.

۳. مثال ۲ را تعمیم می‌دهیم. فرض کنیم G یک گروه و H زیرگروهی از آن باشد. به ازای $a, b \in G$ تعریف می‌کنیم $a \sim b$ اگر $ab^{-1} \in H$. چون $e \in H$ و $e = aa^{-1}$، داریم $a \sim a$. همچنین هرگاه $ab^{-1} \in H$، آن‌گاه چون H زیرگروه G است، $(ab^{-1})^{-1} \in H$. ولی $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$؛ پس $ba^{-1} \in H$؛ در نتیجه $b \sim a$. این به ما می‌گوید که $a \sim b$ رابطهٔ $b \sim a$ را ایجاب می‌کند. بالاخره هرگاه $a \sim b$ و $b \sim c$، آن‌گاه $ab^{-1} \in H$ و $bc^{-1} \in H$. ولی $(ab^{-1})(bc^{-1}) = ac^{-1}$ که از آنجا $ac^{-1} \in H$ و در نتیجه $a \sim c$. پس تعدی $\sim$ را نشان داده‌ایم. لذا $\sim$ یک رابطهٔ هم‌ارزی بر G می‌باشد.

توجه کنید که هرگاه $G = \mathbb{Z}$ گروه اعداد صحیح تحت $+$ بوده و H زیرگروه آن مرکب از تمام مضارب n (به ازای عدد صحیح ثابت $n > 1$) باشد، آن‌گاه $ab^{-1} \in H$ به‌صورت $a \equiv b(n)$ در می‌آید. لذا همنهشتی به پیمانهٔ n حالت بسیار خاصی از هم‌ارزی است که در مثال ۳ تعریف شد.

این رابطهٔ هم‌ارزی در اثبات قضیهٔ لاگرانژ به‌کار خواهد رفت.

۴. فرض کنیم G یک گروه باشد. به ازای $a, b \in G$ گوییم $a \sim b$ اگر عنصری مانند $x \in G$ باشد به‌طوری که $b = x^{-1}ax$. حکم می‌کنیم که این معرف یک رابطهٔ هم‌ارزی بر G است. اولاً $a \sim a$ زیرا $a = eae^{-1}$. ثانیاً هرگاه $a \sim b$، آن‌گاه $b = x^{-1}ax$؛ پس $a = (x^{-1})^{-1}b(x^{-1})$؛ در نتیجه $b \sim a$. بالاخره هرگاه $a \sim b$ و $b \sim c$، آن‌گاه به ازای $x, y \in G$ی، $b = x^{-1}ax$ و $c = y^{-1}by$. لذا $c = y^{-1}(x^{-1}ax)y = (xy)^{-1}a(xy)$؛ و در نتیجه $a \sim c$. پس این یک رابطهٔ هم ارزی بر G می‌باشد.

این رابطه نیز نقش مهمی در نظریهٔ گروهها دارد و نام خاص ترویج بدان اطلاق شده است. وقتی $a \sim b$، گوییم «a و b مزدوج یکدیگر در Gاند.» توجه کنید که هرگاه G آبلی باشد، آن‌گاه $a \sim b$ اگر و فقط اگر $a = b$.

می‌توان همین‌طور ادامه داد و مثالهای جالب متعددی از روابط هم‌ارزی ارائه کرد، ولی این کار ما را از هدف اصلی این بخش دور می‌سازد. در مسائل آخر این بخش مثال به حد وفور خواهیم داشت.

بحث را ادامه داده و تعریف زیر را می‌آوریم.

تعریف. هرگاه $\sim$ یک رابطهٔ هم‌ارزی بر S باشد، آن‌گاه $[a]$، یعنی ردهٔ a، با $[a] = \{b \in S | b \sim a\}$ تعریف می‌شود.

حال ردهٔ a را در مثالهای ۳ و ۴ که هم اکنون دیدیم مشخص می‌کنیم.

در مثال ۳، $a \sim b$ اگر $ab^{-1} \in H$؛ یعنی اگر به ازای $h \in H$، $ab^{-1} = h$. لذا $a \sim b$ ایجاب می‌کند که $a = hb$. از آن‌سو، هرگاه $a = kb$ که در آن $k \in H$، آن‌گاه $ab^{-1} = (kb)b^{-1} = k \in H$. پس $a \sim b$ اگر و فقط اگر $a \in Hb = \{hb|h \in H\}$. بنابراین $[b] = Hb$.

مجموعهٔ Hb یک هم‌مجموعهٔ راست H در G نام دارد. ما در مسئلهٔ ۲۶ از بخش ۳ به این مفهوم برخوردیم. توجه کنید که $b \in Hb$، زیرا $b = eb$ و $e \in H$ (و نیز زیرا $b \in [b] = Hb$). هم‌مجموعه‌های راست و همتاهای چپ آنها، یعنی هم‌مجموعه‌های چپ، نقشهای مهمی در آنچه می‌آیند خواهند داشت.

در مثال ۴ تعریف کردیم $a \sim b$ اگر به ازای $x \in G$ی، $b = x^{-1}ax$. لذا

$$[a] = \{x^{-1}ax|x \in G\}$$

در این حالت $[a]$ را با $\mathrm{cl}(a)$ نشان داده و آن را ردهٔ تزویج a در G می‌نامیم. هرگاه G آبلی باشد، آن‌گاه $\mathrm{cl}(a)$ فقط از a تشکیل شده است. در واقع هرگاه $a \in Z(G)$ (مرکز G)، آن‌گاه $\mathrm{cl}(a)$ فقط از a تشکیل شده است.

مفهوم تزویج و خواصش مجدداً، به‌ویژه در بخش ۱۱، ظاهر خواهد شد.

بررسی ردهٔ یک عنصر a در مثال ۲ را به بعد در این فصل موکول می‌کنیم.

اثر مهمی که یک رابطهٔ هم‌ارزی بر یک مجموعه دارد تجزیه و افراز آن به قطعات از هم جدای زیبایی می‌باشد.

قضیهٔ ۱.۴.۲. هرگاه $\sim$ یک رابطهٔ هم‌ارزی بر S باشد، آن‌گاه $S = \cup[a]$ که این اجتماع روی هر عنصر از هر رده گرفته شده و $[a] \neq [b]$ ایجاب می‌کند که $[a] \cap [b] = \varnothing$. یعنی $\sim$ مجموعهٔ S را به رده‌های هم‌ارزی افراز می‌کند.

برهان. چون $a \in [a]$، داریم $\cup_{a\in S}[a] = S$. برهان حکم دوم نیز آسان است. نشان می‌دهیم که هرگاه $[a] \neq [b]$، آن‌گاه $[a] \cap [b] = \varnothing$ یا، به بیان معادل، هرگاه $[a] \cap [b] \neq \varnothing$، آن‌گاه $[a] = [b]$.

پس فرض کنیم $[a] \cap [b] \neq \varnothing$. همچنین $c \in [a] \cap [b]$. بنابر تعریف رده، $a \sim c$ زیرا $c \in [a]$ و $c \sim b$ زیرا $c \in [b]$. لذا، طبق خاصیت ۲ از $\sim$، $c \sim a$؛ و در نتیجه، چون $a \sim c$ و $c \sim b$، داریم $a \sim b$. لذا $a \in [b]$. هرگاه $x \in [a]$، آن‌گاه $x \sim a$ و $a \sim b$ نتیجه می‌دهند که $x \sim b$؛ پس $x \in [b]$. لذا $[a] \subset [b]$. این استدلال به وضوح نسبت به a و b متقارن است. پس

داریم $[b] \subset [a]$ که از آنجا $[a] = [b]$ و حکم فوق ثابت است.

در اینجا قضیه به‌طور کامل ثابت می‌شود. ■

حال می‌توان نتیجهٔ مشهور لاگرانژ را اثبات کرد.

قضیهٔ ۲.۴.۲ (قضیهٔ لاگرانژ). هرگاه G یک گروه متناهی و H زیرگروهی از آن باشد، آن‌گاه مرتبهٔ H مرتبهٔ G را عاد می‌کند.

برهان. به مثال ۳ باز می‌گردیم. در آنجا ثابت شد که رابطهٔ $a \sim b$ اگر $ab^{-1} \in H$ یک رابطهٔ هم‌ارزی است و

$$[a] = Ha = \{ha | h \in H\}$$

فرض کنیم k تعداد رده‌های متمایز باشد. این رده‌ها را به‌صورت Ha_1، $\cdots$، Ha_k نشان می‌دهیم. بنابر قضیهٔ ۱.۴.۲، $G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$ و می‌دانیم که اگر $i \neq j$، $Ha_j \cap Ha_i = \varnothing$.

حکم می‌کنیم که هر Ha_i دارای مرتبهٔ (تعداد عناصر H) $= |H|$ است. نگاشت $H \to Ha_i$ را با $h \to ha_i$ تعریف می‌کنیم. حکم می‌کنیم که این نگاشت ۱-۱ است چرا که اگر $ha_i = h'a_i$، طبق خاصیت حذف در G داریم $h = h'$. لذا این نگاشت ۱-۱ است. این نگاشت طبق تعریف Ha_i برو نیز هست. لذا H و Ha_i یک تعداد عنصر (یعنی $|H|$) خواهند داشت.

چون $G = Ha_1 \cup \cdots \cup Ha_k$ و Ha_iها از هم جدا بوده و هر Ha_i دارای $|H|$ عنصر است، داریم $|G| = k|H|$. لذا $|H|$، $|G|$ را عاد کرده و قضیهٔ لاگرانژ ثابت می‌شود. ■

«لاگرانژ» به اسامی فرانسوی شباهت دارد، ولی ج. ال. لاگرانژ (J. L. Lagrange, 1736-1813) در واقع ایتالیایی بود که در تورین متولد و بزرگ شد. لیکن بخش اعظم عمرش را در فرانسه گذرانید. وی ریاضیدان عالیقدری بود که در تمام مباحث ریاضی زمان خود کارهایی اساسی کرده است.

اگر G متناهی باشد، تعداد هم‌مجموعه‌های راست H در G، یعنی $|G|/|H|$، اندیس H در G نام دارد و به‌صورت $i_G(H)$ نوشته می‌شود.

به یاد آورید که گروه G دوری است اگر به ازای عنصری مانند $a \in G$ هر عنصر G توانی از a باشد.

قضیهٔ ۳.۴.۲. هر گروه G از مرتبهٔ اول دوری است.

برهان. هرگاه H زیرگروه G باشد، آن‌گاه، بنابر قضیهٔ لاگرانژ، $|H|\,|\,|G| = p$ که در آن p اول است. پس ۱یا$p = |H|$. لذا، هرگاه $H \neq (e)$، آن‌گاه $H = G$. هرگاه $a \neq e \in G$، آن‌گاه مجموعهٔ توانهای a، یعنی $\{a^i\}$، زیرگروهی از G غیر از (e) است. لذا این زیرگروه تمام G می‌باشد. این امر می‌گوید که هر $x \in G$ به شکل $x = a^i$ است. پس G، طبق تعریف گروه دوری، دوری می‌باشد. ■

اگر G متناهی بوده و $a \in G$، قبلاً در برهان لم ۲.۳.۲ دیدیم که به ازای $n(a) \geq 1$ای تابع a، $a^{n(a)} = e$. پس تعریف زیر را می‌آوریم.

تعریف. هرگاه G متناهی باشد، آن‌گاه مرتبهٔ a، که به‌صورت $o(a)$ نوشته می‌شود، کوچکترین عدد صحیح مثبت m است که $a^m = e$.

فرض کنیم $a \in G$ از مرتبهٔ m باشد. مجموعهٔ $A = \{e, a, a^2, \ldots, a^{m-1}\}$ را در نظر می‌گیریم. حکم می‌کنیم که A زیرگروه G است (زیرا $a^m = e$) و m عنصر A متمایزند. اثبات این امور را به خواننده وا می‌گذاریم. لذا $o(a) = m = |A|$. چون $|A|\,|\,|G|$ ، داریم:

قضیهٔ ۴.۴.۲. هرگاه G متناهی بوده و $a \in G$، آن‌گاه $o(a)\,|\,|G|$.

اگر $a \in G$، که در آن G متناهی است، از قضیهٔ ۴.۴.۲ داریم $|G| = k \cdot o(a)$. لذا

$$a^{|G|} = a^{k \cdot o(a)} = (a^{o(a)})^k = e^k = e$$

پس قضیهٔ زیر ثابت شده است.

قضیهٔ ۵.۴.۲. هرگاه G یک گروه متناهی از مرتبهٔ $|G| = n$ باشد، آن‌گاه به ازای هر $a \in G$، $a^n = e$.

با اعمال قضیهٔ اخیر بر گروههایی خاص در نظریهٔ اعداد، به چند نتیجهٔ کلاسیک از این نظریه می‌رسیم که به فرما و اویلر منسوب‌اند.

فرض کنیم $\mathbb{Z}$ مجموعهٔ اعداد صحیح و $n > 1$ یک عدد صحیح ثابت باشد. به مثال ۲ در مورد روابط هم ارزی باز می‌گردیم. در آنجا تعریف شد که $a \equiv b(n)$ (a همنهشت b به پیمانهٔ n است) اگر $n|(a-b)$. ردهٔ a، یعنی $[a]$، از تمام $a + nk$هایی تشکیل شده است که در آنها k جمیع اعداد صحیح را می‌گیرد. ما آن را ردهٔ **همنهشتی** a می‌نامیم.

اگر b یک عدد صحیح باشد، از قضیهٔ ۱.۵.۱ داریم $b = qn + r$ که در آن $\circ \leq r < n$ لذا $[r] = [b]$. در نتیجه n ردهٔ $[\circ]$، $[۱]$، $\cdots$، $[n - ۱]$ تمام رده‌های همنهشتی می‌باشند. تحقیق متمایز بودن این رده‌ها به خواننده محول می‌شود.

فرض کنیم $\mathbb{Z}_n = \{[\circ], [۱], \ldots, [n - ۱]\}$. در $\mathbb{Z}_n$ دو عمل $+$ و $\cdot$ را معرفی می‌کنیم. $\mathbb{Z}_n$ تحت $+$ یک گروه آبلی تشکیل می‌دهد ولی تحت $\cdot$ گروهی نمی‌سازد. لیکن بخشی از آن یک گروه می‌باشد.

$[a] + [b]$ را چطور تعریف کنیم؟ طبیعی‌ترین راه عبارت است از

$$[a] + [b] = [a + b]$$

منتها مشکلی در پیش است. آیا عمل $+$ در $\mathbb{Z}_n$ تعریف شده است؟ معنی این امر چیست؟ $[a]$ را می‌توان با aهای بسیار نمایش داد. مثلاً اگر $n = ۳$، $\cdots = [-۲] = [۴] = [۱]$، در حالی که در تعریف جمع از aی خاصی استفاده می‌کنیم. آنچه باید نشان داد این است که هرگاه $[a] = [a']$ و $[b'] = [b]$، آن‌گاه $[a + b] = [a' + b']$، زیرا در این صورت خواهیم داشت $[a] + [b] = [a + b] = [a' + b'] = [a'] + [b']$.

فرض کنیم $[a'] = [a]$. پس $n|(a - a')$. همچنین از $[b'] = [b]$ داریم $n|(b - b')$. در نتیجه $n|((a - a') + (b - b')) = ((a + b) - (a' + b'))$. لذا $a + b \equiv a' + b'(n)$؛ و در نتیجه $[a + b] = [a' + b']$.

پس در $\mathbb{Z}_n$ یک جمع تعریف شده داریم. عنصر $[\circ]$ عنصر همانی و $[-a]$ عنصر $-[a]$، یعنی معکوس $[a]$، است. تحقیق گروه بودن $\mathbb{Z}_n$ تحت $+$ به خواننده محول می‌شود. این یک گروه دوری از مرتبهٔ n است که به‌وسیلهٔ $[۱]$ تولید می‌شود.

نکات فوق را در قضیهٔ زیر خلاصه می‌کنیم.

قضیهٔ ۶.۴.۲. $\mathbb{Z}_n$ تحت جمع $[a]+[b] = [a+b]$ یک گروه دوری تشکیل می‌دهد.

حال که از جمع در $\mathbb{Z}_n$ فارغ شدیم به معرفی ضرب می‌پردازیم. مجدداً طبیعی‌ترین راه عبارت است از

$$[a] \cdot [b] = [ab]?$$

مثلاً اگر $n = ۹$، $[۲][۷] = [۱۴] = [۵]$ و $[\circ] = [۱۸] = [۶][۳]$. بر خواننده است تحقیق کند که این ضرب تعریف شده است. $\mathbb{Z}_n$ تحت این ضرب یک گروه تشکیل نمی‌دهد. زیرا به ازای هر a، $[\circ][a] = [\circ]$ و چون عنصر یکه تحت ضرب $[۱]$ است، $[\circ]$ نمی‌تواند معکوس ضربی

داشته باشد. می‌پرسیم: چرا عناصر ناصفر $[a] \neq [۰]$ را تحت این ضرب در نظر نمی‌گیریم؟ در اینجا مجدداً اگر n اول نباشد مشکل داریم. مثلاً اگر $n = ۶$، $[۲] \neq [۰]$ و $[۳] \neq [۰]$ ولی $[۲][۳] = [۶] = [۰]$. پس عناصر ناصفر در حالت کلی گروهی به ما نمی‌دهند.

لذا می‌پرسیم: آیا می‌توان بخش مناسبی از $\mathbb{Z}_n$ را یافت که تحت ضرب تشکیل گروه دهد؟ جواب مثبت است! قرار می‌دهیم $U_n = \{[a] \in \mathbb{Z}_n | (a, n) = ۱\}$؛ به عبارت دیگر، $\{[a] |$ اول است n نسبت به $a\}$. بنا بر نتیجهٔ قضیهٔ ۵.۵.۱، هرگاه $(a, n) = ۱$ و $(b, n) = ۱$، آن‌گاه $(ab, n) = ۱$. لذا از $[a][b] = [ab]$ نتیجه می‌شود که اگر $[a], [b] \in U_n$، $[ab] \in U_n$. پس U_n بسته است. شرکتپذیری به آسانی تحقیق می‌شود و نتیجه‌ای است از شرکتپذیری اعداد صحیح تحت ضرب. عنصر همانی به آسانی به‌دست می‌آید که عبارت است از $[۱]$. ضرب در U_n تعویضپذیر نیز هست.

توجه کنید که هرگاه $[a][b] = [a][c]$ که در آن $[a] \in U_n$، آن‌گاه داریم $[ab] = [ac]$؛ و در نتیجه $[ab - ac] = [۰]$. این امر می‌گوید که $n | a(b - c) = ab - ac$. ولی a نسبت به n اول است. پس بنابر قضیهٔ ۵.۵.۱ باید داشته باشیم $n | (b - c)$؛ و در نتیجه $[b] = [c]$. به عبارت دیگر، در U_n خاصیت حذف را داریم. پس U_n طبق مسئلهٔ ۲ از بخش ۲ یک گروه می‌باشد.

مرتبهٔ U_n چیست؟ بنابر تعریف U_n،

$$|U_n| = \text{تعداد اعداد صحیح } ۱ \leq m < n \text{ که } (m, n) = ۱$$

این عدد مکرر ظاهر می‌شود و ما بدان نامی خاص می‌دهیم.

تعریف. تابع φی اویلر، یعنی $\varphi(n)$، با $\varphi(۱) = ۱$ و به ازای $n > ۱$ با

$$\varphi(n) = \text{تعداد اعداد صحیح مثبت } m \text{ که } ۱ \leq m < n \text{ و } (m, n) = ۱$$

تعریف می‌شود.

لذا $|U_n| = \varphi(n)$. اگر $n = p$ (اول)، داریم $\varphi(p) = p - ۱$. می‌بینیم که $\varphi(۸) = ۴$ زیرا فقط ۱، ۳، ۵، و ۷ از ۸ کوچکتر، مثبت، و نسبت به ۸ اولند. حال $\varphi(۱۵)$ را حساب می‌کنیم. تعداد اعداد $۱ \leq m < ۱۵$ نسبت به ۱۵ اول عبارتند از ۱، ۲، ۴، ۷، ۸، ۱۱، ۱۳، ۱۴. پس $\varphi(۱۵) = ۸$.

حال به چند مثال از U_n نگاه می‌کنیم.

۱. $U_{۸} = \{[۱],[۳],[۵],[۷]\}$. توجه کنید که $[۷] = [۱۵] = [۳][۵]$، $[۱] = [۲۵] = [۵]^{۲}$. $U_{۸}$ در واقع گروهی است از مرتبهٔ ۴ که در آن به ازای هر $a \in U_{۸}$، $a^{۲} = e$.

۲. $U_{۱۵} = \{[۱],[۲],[۴],[۷],[۸],[۱۱],[۱۳],[۱۴]\}$. توجه کنید که $[۸] = [۱۴۳] = [۱۱][۱۳]$، $[۱] = [۲]^{۴}$، و از این قبیل.

برخواننده است تحقیق کند که به ازای هر $a \in U_{۱۵}$، $a^{۴} = e = [۱]$.

۳. $U_{۹} = \{[۱],[۲],[۴],[۵],[۷],[۸]\}$. توجه کنید که $[۲] = [۲]^{۱}$، $۴ = [۲]^{۲}$، $[۸] = [۲]^{۳}$، $[۷] = [۱۶] = [۲]^{۴}$، $[۵] = [۳۲] = [۲]^{۵}$. همچنین

$$[۲]^{۶} = [۲][۲]^{۵} = [۲][۵] = [۱۰] = [۱]$$

لذا توانهای $[۲]$ همهٔ عناصر $U_{۹}$ را به ما می‌دهند. بنابراین $U_{۹}$ یک گروه دوری از مرتبهٔ ۶ است. چه عناصر دیگر از $U_{۹}$ این گروه را تولید می‌کنند؟

به موازات قضیهٔ ۶.۴.۲ داریم:

قضیهٔ ۷.۴.۲. U_n تحت ضرب $[a][b] = [ab]$ یک گروه آبلی از مرتبهٔ $\varphi(n)$ تشکیل می‌دهد که در آن $\varphi(n)$ تابع φی اویلر می‌باشد.

یک نتیجهٔ فوری از قضایای ۷.۴.۲ و ۵.۴.۲ قضیهٔ معروف زیر در نظریهٔ اعداد است.

قضیهٔ ۸.۴.۲(اویلر). هرگاه عدد صحیح a نسبت به n اول باشد، آن‌گاه

$$a^{\varphi(n)} \equiv ۱ \bmod n$$

برهان. U_n یک گروه از مرتبهٔ $\varphi(n)$ است. پس، بنابر قضیهٔ ۵.۴.۲، به ازای هر $g \in U_n$، $g^{\varphi(n)} = e$. این رابطه به‌صورت $[a^{\varphi(n)}] = [a]^{\varphi(n)} = [۱]$ در می‌آید که این خود صورت $n|(a^{\varphi(n)} - ۱)$ را خواهد داشت. این به‌طور دقیق می‌گوید که $a^{\varphi(n)} \equiv ۱(n)$. ■

یک حالت خاص، که در آن $n = p$ اول است، منسوب است به فرما.

نتیجه (فرما). هرگاه p اول بوده و $p \nmid a$، آن‌گاه

$$a^{p-۱} \equiv ۱(p)$$

به ازای هر عدد صحیح b، $b^p \equiv b \mod p$.

برهان. چون $\varphi(p) = p - ۱$، اگر $(a,p) = ۱$، از قضیهٔ ۸.۴.۲ داریم $a^{p-۱} \equiv ۱(p)$. پس $a^۱ \cdot a^{p-۱} \equiv a(p)$؛ در نتیجه $a^p \equiv a(p)$. هرگاه $p|b$، آن‌گاه $b \equiv ۰\,(p)$ و $b^p \equiv ۰\,(p)$؛ در نتیجه $b^p \equiv b(p)$. ■

لئونارد اویلر (Leonhard Euler , 1707-1785) احتمالاً بزرگترین دانشمندی است که کشور سوییس به جهان علم هدیه کرده است. وی پرکارترین ریاضیدان تمام اعصار بوده است.

پیرفرما (Pierre Fermat , 1601-1665) متخصص بزرگی در نظریهٔ اعداد بود. آخرین قضیهٔ فرما، که قضیه نبوده و بلکه یک حدس است، می‌گوید که $a^n + b^n = c^n$ به ازای $n > ۲$ فقط جواب بدیهی دارد که به ازای $a = ۰$ یا $b = ۰$ یا $c = ۰$ رخ می‌دهد.

آخرین نکته در باب قضیهٔ لاگرانژ. عکس این قضیه عموماً درست نیست. یعنی اگر G یک گروه متناهی از مرتبهٔ n باشد، لازم نیست به ازای هر مقسوم علیه m از n زیرگروهی از مرتبهٔ m موجود باشد. یک گروه با این خاصیت باید خیلی خاص بوده و ساختارش به‌خوبی و دقت قابل بیان باشد.

مسائل

مسائل آسانتر

۱. تحقیق کنید که رابطهٔ $\sim$ یک رابطهٔ هم‌ارزی بر مجموعهٔ S داده شده است:

الف) مجموعهٔ اعداد حقیقی $S = \mathbb{R}$، $a \sim b$ اگر $a - b$ گویا باشد؛

ب) مجموعهٔ اعداد مختلط $S = \mathbb{C}$، $a \sim b$ اگر $|a| = |b|$؛

پ) مجموعهٔ خطوط مستقیم در صفحه $= S$، $a \sim b$ اگر a و b موازی باشند؛

ت) مجموعهٔ تمام مردم $= S$، $a \sim b$ اگر هر دو چشمان همرنگ داشته باشند.

۲. رابطهٔ $\sim$ که بر مجموعهٔ اعداد حقیقی $\mathbb{R}$ با $a \sim b$ اگر هر دوی $a > b$ و $b > a$ برقرار باشند تعریف شده است یک رابطهٔ هم‌ارزی نیست. چرا نیست؟ این رابطه در چه خواصی از رابطهٔ هم‌ارزی صدق می‌کند؟

۳. فرض کنید رابطهٔ $\sim$ بر مجموعهٔ S در خواص زیر صدق کند: (۱) $a \sim b$ رابطهٔ $b \sim a$ را ایجاب کند و (۲) $a \sim b$ و $b \sim c$ رابطهٔ $a \sim c$ را ایجاب کنند. این خواص ظاهراً $a \sim a$ را

ایجاب می‌کنند. چرا که اگر $a \sim b$، بنابر (۱) $b \sim a$. پس $a \sim b$ و $b \sim a$. لذا، طبق (۲)، $a \sim a$. هرگاه این استدلال درست باشد، آن‌گاه رابطهٔ $\sim$ باید یک رابطهٔ هم‌ارزی باشد. مسئلهٔ ۲ نشان می‌دهد که این‌طور نیست. پس استدلال ما چه نقصی دارد؟

۴. فرض کنید S یک مجموعه بوده و $\{S_\alpha\}$ زیرمجموعه‌های ناتهی آن باشند به‌طوری که $S = \cup_\alpha S_\alpha$ و $S_\alpha \cap S_\beta = \varnothing$ اگر $\alpha \neq \beta$. یک رابطهٔ هم‌ارزی بر S چنان تعریف کنید که S_αها درست تمام رده‌های هم‌ارزی باشند.

۵. فرض کنید G یک گروه و H زیرگروهی از G باشد. به ازای $a, b \in G$، $a \sim b$ را با $a^{-1}b \in H$ تعریف و ثابت کنید این معرف یک رابطهٔ هم‌ارزی بر G است، و نشان دهید که $[a] = aH = \{ah | h \in H\}$. مجموعه‌های aH هم‌مجموعه‌های چپ H در G نام دارند.

۶. اگر G مساوی S_3 بوده و $H = \{i, f\}$، که در آن $f : S \to S$ با $f(x_1) = x_2$، $f(x_2) = x_1$، $f(x_3) = x_3$ تعریف شده است، تمام هم‌مجموعه‌های راست H در G و تمام هم‌مجموعه‌های چپ H در G را ذکر نمایید.

۷. در مسئلهٔ ۶ آیا هر هم‌مجموعهٔ راست H در G یک هم‌مجموعهٔ چپ H در G نیز هست؟

۸. اگر هر هم‌مجموعهٔ راست H در G یک هم‌مجموعهٔ چپ H در G باشد، ثابت کنید به ازای هر $a \in G$، $aHa^{-1} = H$.

۹. در $\mathbb{Z}_{16}$ تمام هم‌مجموعه‌های زیرگروه $H = \{[0], [4], [8], [12]\}$ را بنویسید. (چون عمل $\mathbb{Z}_n$ به‌علاوه است، هم‌مجموعه‌ها را به‌صورت $[a] + H$ بنویسید. و چون $\mathbb{Z}_n$ تحت $+$ آبلی است، لازم نیست بین هم‌مجموعه‌های راست و هم‌مجموعه‌های چپ تمیز بگذارید.)

۱۰. در مسئلهٔ ۹، $i_{\mathbb{Z}_{16}}(H)$ چیست؟ (به یاد آورید که ما اندیس $i_G(H)$ را تعداد هم‌مجموعه‌های راست در G تعریف کرده‌ایم.)

۱۱. نشان دهید که تعداد هم‌مجموعه‌های راست H در گروه متناهی G با تعداد هم‌مجموعه‌های چپ H در G یکی است.

۱۲. اگر aH و bH هم‌مجموعه‌های چپ متمایز H در G باشند، آیا Ha و Hb نیز هم‌مجموعه‌های راست متمایز H در Gاند؟ این امر را ثابت کنید یا مثال نقض بزنید.

۱۳. مرتبهٔ تمام عناصر U_{18} را بیابید. آیا U_{18} دوری است؟

۱۴. مرتبهٔ تمام عناصر U_{20} را بیابید. آیا U_{20} دوری است؟

۱۵. اگر p اول باشد، نشان دهید که تنها جوابهای $x^{2} \equiv 1(p)$ عبارتند از $x \equiv 1(p)$ یا $x \equiv -1(p)$.

۱۶. اگر G یک گروه آبلی متناهی بوده و a_{1}، $\cdots$، a_{n} همهٔ عناصر آن باشند، نشان دهید که $x = a_{1}a_{2}\cdots a_{n}$ باید در $x^{2} = e$ صدق کند.

۱۷. اگر G از مرتبهٔ فرد باشد، راجع به x مسئلهٔ ۱۶ چه می‌شود گفت؟

۱۸. با استفاده از مسائل ۱۵ و ۱۶ ثابت کنید هرگاه p یک عدد اول فرد باشد، آن‌گاه

$$(p-1)! \equiv -1(p)$$

(این مطلب به قضیهٔ ویلسون (Wilson) معروف است.) البته این قضیه به ازای $p = 2$ نیز درست است.

۱۹. مزدوجهای تمام عناصر S_{3} را بیابید.

۲۰. در گروه G مثال ۶ از بخش ۱ ردهٔ تزویج عنصر $T_{a,b}$ را یافته و آن را برحسب a و b توصیف کنید.

۲۱. فرض کنید G گروه دو وجهی از مرتبهٔ ۸ باشد (ر.ک. مثال ۱۰ در بخش ۱). رده‌های تزویج در G را بیابید.

۲۲. قضیهٔ اویلر را به ازای $n = 14$ و $a = 3$، و $a = 5$ تحقیق کنید.

۲۳. نشان دهید که در U_{41} عنصری مانند a هست به‌طوری که $[a]^{2} = [-1]$؛ یعنی عدد صحیحی مانند a هست به‌طوری که $a^{2} \equiv -1(41)$.

۲۴. اگر p عدد اولی به شکل $4n + 3$ باشد، نشان دهید که معادلهٔ

$$x^{2} \equiv -1(p)$$

را نمی‌توان حل کرد. (راهنمایی. قضیهٔ فرما را به‌کار برید که می‌گوید اگر $p \nmid a$، $a^{p-1} \equiv 1 \ (p)$.)

۲۵. نشان دهید که عناصر ناصفر $\mathbb{Z}_{n}$ تحت ضرب $[a][b] = [ab]$ یک گروه تشکیل می‌دهند اگر و فقط اگر n اول باشد.

مسائل با سطح متوسط

۲۶. فرض کنید G گروه، H زیرگروه G، S مجموعهٔ تمام هم‌مجموعه‌های راست متمایز H در G، و T مجموعهٔ تمام هم‌مجموعه‌های چپ H در G باشد. ثابت کنید یک نگاشت ۱-۱ از S به روی T وجود دارد. (تذکر: نگاشت واضحی که Ha را به توی aH می‌فرستد نگاشت مناسبی نیست. ر.ک. مسائل ۵ و ۱۲.)

۲۷. اگر $aH = bH$ در G ایجاب کند که $Ha = Hb$، نشان دهید که به ازای هر $a \in G$، $aHa^{-1} = H$.

۲۸. اگر G یک گروه دوری از مرتبهٔ n باشد، نشان دهید که $\varphi(n)$ مولد برای G وجود دارد. شکل آنها را صریحاً مشخص نمایید.

۲۹. اگر در گروه G داشته باشیم $aba^{-1} = b^{i}$، نشان دهید که به ازای جمیع اعداد صحیح مثبت r، $a^{r}ba^{-r} = b^{i^{r}}$.

۳۰. اگر در G داشته باشیم $a^{5} = e$ و $aba^{-1} = b^{2}$، $o(b)$ را در صورتی که $b \neq e$ بیابید.

۳۱. اگر $o(a) = m$ و $a^{s} = e$، ثابت کنید $m|s$.

۳۲. فرض کنید G یک گروه متناهی و H زیرگروهی از آن باشد. همچنین $f(a)$ کوچکترین m مثبتی باشد که $a^{m} \in H$. ثابت کنید $f(a)|o(a)$.

۳۳. اگر $i \neq f \in A(S)$ چنان باشد که $f^{p} = e$ (p اول است) و به ازای $s \in S$ی تساوی $f^{j}(s) = s$ به ازای عددی مانند $1 \leq j < p$ برقرار باشد، نشان دهید که $f(s) = s$.

۳۴. اگر $f \in A(S)$ از مرتبهٔ عدد اول p باشد، نشان دهید که به ازای هر $s \in S$، مدار s تحت f دارای یک یا p عنصر می‌باشد. [یادآوری: مدار s تحت f عبارت است از $\{f^{j}(s)|$ عدد صحیح دلخواه $j\}$.]

۳۵. اگر $f \in A(S)$ از مرتبهٔ عدد اول p بوده و S مجموعه‌ای متناهی با n عنصر باشد که $(n, p) = 1$، نشان دهید که به ازای $s \in S$ی، $f(s) = s$.

مسائل مشکلتر

۳۶. اگر $a > 1$ عددی صحیح باشد، نشان دهید که $n|\varphi(a^{n} - 1)$ که در آن φ تابع φی اویلر است. [راهنمایی. اعداد صحیح به پیمانهٔ $(a^{n} - 1)$ را در نظر بگیرید.]

۳۷. در یک گروه دوری از مرتبهٔ n نشان دهید که به ازای هر عدد صحیح m که n را عاد کند (به انضمام $m = 1$ و $m = n$) $\varphi(m)$ عنصر از مرتبهٔ m وجود دارد.

۳۸. با استفاده از مسئلهٔ ۳۷ نشان دهید که $n = \sum_{m|n} \varphi(m)$.

۳۹. فرض کنید G یک گروه آبلی متناهی از مرتبهٔ n باشد که در آن تعداد جوابهای $x^{m} = e$ به ازای هر mی که n را عاد کند حداکثر m است. ثابت کنید G باید دوری باشد. [راهنمایی. فرض کنید $\psi(m)$ تعداد عناصر G از مرتبهٔ m باشد. نشان دهید که $\psi(m) \leq \varphi(m)$ و از مسئلهٔ ۳۸ استفاده کنید.]

۴۰. با استفاده از مسئلهٔ ۳۹ نشان دهید که اگر p اول باشد، U_p دوری است. (این یک نتیجهٔ معروف در نظریهٔ اعداد است؛ این نتیجه وجود یک ریشهٔ اولیه به پیمانهٔ p را تأیید می‌کند.)

۴۱. با استفاده از مسئلهٔ ۴۰ نشان دهید که اگر p عدد اولی به شکل $p = ۴n + ۱$ باشد، معادلهٔ $x^۲ \equiv -۱(p)$ را می‌توان در اعداد صحیح حل کرد.

۴۲. با استفاده از قضیهٔ ویلسون (ر.ک. مسئلهٔ ۱۸) نشان دهید که اگر عدد اول p به شکل $p = ۴n + ۱$ بوده و

$$y = ۱ \cdot ۲ \cdot ۳ \cdots \frac{p-۱}{۲} = \left(\frac{p-۱}{۲}\right)!$$

داریم $y^۲ \equiv -۱(p)$. (این حل دیگری است از مسئلهٔ ۴۱.)

۴۳. فرض کنید G یک گروه آبلی از مرتبهٔ n بوده و $a_۱$، $\cdots$، a_n عنصرهای آن باشند. همچنین $x = a_۱a_۲\cdots a_n$. نشان دهید که

الف) هرگاه G درست یک عنصر $b \neq e$ داشته باشد که $b^۲ = e$، آنگاه $x = b$؛

ب) هرگاه G بیش از یک عنصر $b \neq e$ داشته باشد که $b^۲ = e$، آنگاه $x = e$؛

پ) هرگاه n فرد باشد، آنگاه $x = e$ (ر.ک. مسئلهٔ ۱۶).

۵. همریختیها و زیرگروههای نرمال

نظریهٔ گروهها به نوعی از سه مفهوم اصلی ساخته شده است که عبارتند از همریختی، زیرگروه نرمال، و گروه عاملی یا خارج قسمتی یک گروه بر یک زیرگروه نرمال. ما در این بخش دو مفهوم اول و در بخش ۶ مفهوم سوم را مورد بحث قرار می‌دهیم.

حال بی‌درنگ به اولین مفهوم می‌پردازیم.

تعریف. فرض کنیم G و G' دو گروه باشند. نگاشت $\varphi : G \to G'$ یک همریختی است اگر به ازای هر $a, b \in G$، $\varphi(ab) = \varphi(a)\varphi(b)$.

(تذکر: این φ ربطی به تابع φی اویلر ندارد.)

در این تعریف حاصلضرب سمت چپ (یعنی ab در $\varphi(ab)$) در G است ولی حاصلضرب $\varphi(a)\varphi(b)$ در G' می‌باشد. یک توصیف کوتاه از همریختی آن است که بگوییم عمل G را حفظ می‌کند. ما برو بودن φ را تأکید نمی‌کنیم چرا که اگر باشد، بودنش را ذکر خواهیم کرد. پیش از بررسی نکاتی راجع به همریختیها چند مثال ارائه می‌دهیم.

چند مثال

۱. فرض کنیم G گروه تمام اعداد حقیقی مثبت تحت ضرب اعداد حقیقی بوده و G' گروه تمام اعداد حقیقی تحت جمع باشد. همچنین $\varphi : G \to G'$ با $\varphi(x) = \log_{10} x$ به ازای $x \in G$ تعریف شده باشد. چون $\log_{10}(xy) = \log_{10} x + \log_{10} y$، داریم $\varphi(xy) = \varphi(x) + \varphi(y)$. پس φ یک همریختی است. این همریختی برو و ۱-۱ نیز می‌باشد.

۲. فرض کنیم G یک گروه آبلی بوده و $\varphi : G \to G$ با $\varphi(a) = a^2$ تعریف شده باشد. چون $\varphi(ab) = (ab)^2 = a^2b^2 = \varphi(a)\varphi(b)$، φ یک همریختی از G به توی خود است. این همریختی لزوماً برو نیست. خواننده می‌تواند امتحان کند که در U_8 (ر.ک. بخش ۴) به ازای هر $a \in U_8$، $a^2 = e$؛ پس $\{\varphi(a)\} = \{e\}$.

۳. مثال U_8 فوق همریختی بدیهی را پیشنهاد می‌کند. فرض کنیم G یک گروه و G' گروهی دیگر باشد. به ازای هر $x \in G$ تعریف می‌کنیم $\varphi(x) = e'$ (عنصر یکهٔ G'). φ بداهتاً یک همریختی از G به توی G' است. این همریختی مسلماً خیلی جالب نیست.

همریختی دیگری که همیشه ارائه می‌شود نگاشت همانی i از گروه دلخواه G به توی خود است. چون به ازای هر $x \in G$، $i(x) = x$، پس $i(xy) = xy = i(x)i(y)$. نگاشت i یک‌به‌یک و بروست ولی این همریختی نیز چندان جالب نخواهد بود.

۴. فرض کنیم G مجموعهٔ اعداد صحیح تحت $+$ بوده و $G' = \{1, -1\}$ زیرگروه اعداد حقیقی تحت ضرب باشد. تعریف می‌کنیم $\varphi(m) = 1$ اگر m زوج باشد و $\varphi(m) = -1$ اگر m فرد باشد. همریختی بودن φ صرفاً یعنی

$$\text{زوج} = \text{زوج} + \text{زوج}،\ \text{فرد} = \text{فرد} + \text{زوج}،\ \text{و}\ \text{زوج} = \text{فرد} + \text{فرد}$$

۵. فرض کنیم G گروه تمام اعداد مختلط ناصفر تحت ضرب و G' گروه اعداد حقیقی مثبت تحت ضرب باشد. $\varphi : G \to G'$ را با $\varphi(a) = |a|$ تعریف می‌کنیم. در این صورت، $\varphi(ab) = |ab| = |a||b| = \varphi(a)\varphi(b)$. پس φ یک همریختی از G به توی G' است. φ در واقع برو می‌باشد.

۶. فرض کنیم G گروه مثال ۶ از بخش ۱ بوده و G' گروه اعداد حقیقی ناصفر تحت ضرب باشد. $\varphi : G \to G'$ را با $\varphi(T_{a,b}) = a$ تعریف می‌کنیم. همریختی بودن φ از قاعدهٔ ضرب در G، یعنی $T_{a,b}T_{c,d} = T_{ac,ad+b}$، نتیجه خواهد شد.

۷. فرض کنیم $G = \mathbb{Z}$ گروه اعداد صحیح تحت + بوده و $G' = \mathbb{Z}_n$. $\varphi : G \to G'$ را با $\varphi(m) = [m]$ تعریف می‌کنیم. چون جمع در $\mathbb{Z}_n$ با $[m] + [r] = [m + r]$ تعریف می‌شود، می‌بینیم که $\varphi(m + r) = \varphi(m) + \varphi(r)$؛ پس φ در واقع یک همریختی از $\mathbb{Z}$ به روی $\mathbb{Z}_n$ است.

۸. ساختمان کلی زیر به قضیهٔ معروفی منجر می‌شود. فرض کنیم G یک گروه و $A(G)$ مجموعهٔ تمام نگاشتهای ۱-۱ از G به روی خود باشد؛ در اینجا G را فقط یک مجموعه دانسته و ضربش را نادیده می‌گیریم. نگاشت $T_a : G \to G$ را به ازای هر $x \in G$ با $T_a(x) = ax$ تعریف می‌کنیم. می‌پرسیم: حاصلضرب T_aT_b نگاشتهای T_a و T_b بر G چیست؟ داریم

$$(T_aT_b)(x) = T_a(T_b(x)) = T_a(bx) = a(bx) = (ab)x = T_{ab}(x)$$

(از قانون شرکتپذیری استفاده کرده‌ایم). پس خواهیم داشت $T_aT_b = T_{ab}$.

نگاشت $\varphi : G \to A(G)$ را به ازای هر $a \in G$ با $\varphi(a) = T_a$ تعریف می‌کنیم. قاعدهٔ ضرب در مورد Tها به‌صورت $\varphi(ab) = T_{ab} = T_aT_b = \varphi(a)\varphi(b)$ در می‌آید؛ در نتیجه φ یک همریختی از G به توی $A(G)$ می‌باشد. حکم می‌کنیم که φ یک‌به‌یک است. فرض کنیم $\varphi(a) = \varphi(b)$؛ یعنی $T_a = T_b$. لذا $a = T_a(e) = T_b(e) = b$؛ در نتیجه φ یک‌به‌یک است. φ در حالت کلی برو نیست زیرا مثلاً اگر G از مرتبهٔ $n > 2$ باشد، $A(G)$ از مرتبهٔ $n!$ است، و چون $n! > n$، φ کوچکترین شانسی برای برو بودن نخواهد داشت. به آسانی تحقیق می‌شود که نقش φ، یعنی $\varphi(G) = \{T_a | a \in G\}$، زیرگروهی است از $A(G)$.

یک‌به‌یک بودن φ این فکر را القا می‌کند که همریختیهای ۱-۱ باید نقشی خاص داشته باشند. ما ذیلاً این همریختیها را ممتاز می‌سازیم.

تعریف. همریختی $\varphi : G \to G'$ را تکریختی نامیم اگر φ یک‌به‌یک باشد. هر تکریختی که برو باشد یکریختی نام دارد. هر یکریختی از G به خود G یک خودریختی نامیده می‌شود.

حال تعریفی دیگر می‌آوریم.

تعریف. دو گروه G و G' را یکریخت نامیم اگر یک تکریختی از G به روی G' موجود باشد. یکریخت بودن G و G' را با $G \simeq G'$ نشان می‌دهیم.

این تعریف ظاهراً نامتقارن است ولی در واقع چنین نیست، چرا که اگر یک یکریختی از G به روی G' موجود باشد، یک یکریختی از G' به روی G نیز وجود دارد (رک. مسئلهٔ ۲).

یکریخت بودن دو گروه بعدها با تفصیل بیشتر مورد بحث قرار می‌گیرد. فعلاً مثال ۸ را به‌طور خلاصه بازگو می‌کنیم.

قضیهٔ ۱.۵.۲(قضیهٔ کیلی). هر گروه S با زیرگروهی از $A(S)$ به ازای Sی مناسب یکریخت است.

ما S مناسبی که به کار بردیم خود G بود. ولی ممکن است انتخابهای بهتری نیز داشته باشیم. در مسائلی که می‌آیند بعضی از آنها را خواهیم دید.

وقتی G متناهی است، می‌توان مجموعهٔ S قضیهٔ ۱.۵.۲ را متناهی گرفت که در این حالت $A(S)$ مساوی S_n بوده و عناصرش جایگشتها می‌باشند. در این حالت قضیهٔ کیلی معمولاً به‌صورت زیر بیان می‌شود:

هر گروه متناهی را می‌توان به‌صورت گروهی از جایگشتها نمایش داد.

آرتور کیلی (Arthur Cayley, 1821-1895) یک ریاضیدان انگلیسی است که در نظریهٔ ماتریسها، نظریهٔ پایایی، و بسیاری از بخشهای دیگر جبر کار کرده است.

اینجا جای مناسبی است برای بحث در اهمیت «یکریختی». فرض کنیم φ یک یکریختی از G به روی G' باشد. با استفاده از برچسب $\varphi(x)$ برای عنصر x می‌توان G' را برچسب زدهٔ مجدد G گرفت. آیا این برچسب زدن با ساختار G به‌عنوان یک گروه سازگار است؟ یعنی اگر x با $\varphi(x)$ و y با $\varphi(y)$ برچسب خورده باشد، برچسب xy چیست؟ گوییم چون $\varphi(xy) = \varphi(x)\varphi(y)$، xy به‌صورت $\varphi(x)\varphi(y)$ برچسب خورده است. پس این نامگذاری مجدد عناصر با ضرب در G سازگار است. لذا دو یکریخت که لزوماً مساوی نیستند به نوعی که در بالا توصیف شد مساوی می‌باشند. البته مطلوب آن است که یک گروه با گروه ملموسی که آن را می‌شناسیم یکریخت باشد.

حال به چند مثال دیگر می‌پردازیم.

۹. فرض کنیم G یک گروه بوده و $a \in G$ ثابت باشد. $\varphi : G \to G$ را با $\varphi(x) = a^{-1}xa$ به ازای هر $x \in G$ تعریف می‌کنیم. حکم می‌کنیم که φ یک یکریختی از G به روی خود است. گوییم اولاً

$$\varphi(xy) = a^{-1}(xy)a = a^{-1}xa \cdot a^{-1}ya = \varphi(x)\varphi(y)$$

پس φ لااقل یک همریختی از G به توی خود است. این نگاشت ۱-۱ است زیرا هرگاه $\varphi(x) = \varphi(y)$، آن‌گاه $a^{-1}xa = a^{-1}ya$. پس، بنابر خاصیت حذف در G، داریم $x = y$.

بالاخره φ بروست زیرا به ازای هر $x \in G$، $x = a^{-1}(axa^{-1})a = \varphi(axa^{-1})$.

این φ یک خودریختی داخلی G القا شده به‌وسیلهٔ a نامیده می‌شود. در مسائل مفهوم خودریختی و بعضی از خواصش مطرح خواهند شد.

آخرین مثال ما به قرار زیر است.

۱۰. فرض کنیم G گروه اعداد حقیقی تحت $+$ و G' گروه تمام اعداد مختلط ناصفر تحت ضرب باشد. $\varphi : G \to G'$ را با

$$\varphi(x) = \cos x + i \sin x$$

تعریف می‌کنیم. دیدیم که $(\cos x + i \sin x)(\cos y + i \sin y) = \cos(x+y) + i \sin(x+y)$. پس $\varphi(x+y) = \varphi(x)\varphi(y)$ و φ یک همریختی از G به توی G' است. φ یک‌به‌یک نیست زیرا، مثلاً $\varphi(2\pi) = \varphi(0) = 1$. φ برو نیز نیست.

حال که چند مثال در دست داریم به بررسی مختصری از همریختیها می‌پردازیم. بحث را با لم زیر آغاز می‌کنیم.

لم ۲.۵.۲. هرگاه φ یک همریختی از G به توی G' باشد، آن‌گاه

الف) $\varphi(e) = e'$ (عنصر یکهٔ G')؛

ب) به ازای هر $a \in G$، $\varphi(a^{-1}) = \varphi^{-1}(a)$.

برهان. چون $x = xe$، $\varphi(x) = \varphi(xe) = \varphi(x)\varphi(e)$. پس، طبق خاصیت حذف در G'، $\varphi(e) = e'$. همچنین $\varphi(aa^{-1}) = \varphi(e) = e'$. پس $e' = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$. ■

تعریف. نقش φ، یعنی $\varphi(G)$، عبارت است از $\varphi(G) = \{\varphi(a) | a \in G\}$.

اثبات لم زیر را به خواننده محول می‌کنیم.

لم ۳.۵.۲. هرگاه φ یک همریختی از G به توی G' باشد، آن‌گاه نقش φ زیرگروهی از G' می‌باشد.

ما همریختیهایی را ممتاز ساخته و آنها را تکریختی نامیدیم. خاصیت ویژهٔ آنها ۱-۱ بودنشان بود. حال می‌خواهیم میزان دوری یک همریختی را از تکریختی بودنش بسنجیم. این ما را به

تعریف زیر وامی‌دارد.

تعریف. هرگاه φ یک همریختی از G به توی G' باشد، آن‌گاه هستهٔ φ، یعنی $\mathrm{Ker}(\varphi)$، با $\mathrm{Ker}(\varphi) = \{a \in G | \varphi(a) = e'\}$ تعریف می‌شود.

$\mathrm{Ker}(\varphi)$ عدم یک‌به‌یک بودن در نقطهٔ e' را می‌سنجد. حکم می‌کنیم که این عدم نسبتاً یکنواخت است. می‌پرسیم: به ازای $w' \in G'$، $W = \{x \in G | \varphi(x) = w'\}$ چیست؟ واضح است که هرگاه $k \in \mathrm{Ker}(\varphi)$ و $\varphi(x) = w'$، آن‌گاه

$$\varphi(xk) = \varphi(x)\varphi(k) = \varphi(x)e' = w'$$

پس $xk \in W$. **همچنین هرگاه** $\varphi(x) = \varphi(y) = w'$، **آن‌گاه** $\varphi(x) = \varphi(y)$. لذا $\varphi(y)\varphi(x)^{-1} = e'$. ولی، طبق لم ۲.۵.۲، $\varphi(x)^{-1} = \varphi(x^{-1})$. پس

$$e' = \varphi(y)\varphi(x)^{-1} = \varphi(y)\varphi(x^{-1}) = \varphi(yx^{-1})$$

که از آنجا $yx^{-1} \in \mathrm{Ker}(\varphi)$؛ودرنتیجه $y \in \mathrm{Ker}(\varphi)x$. لذا نقش معکوس هر عنصر w' در $\varphi(G) \subset G'$ عبارت است از مجموعهٔ $\mathrm{Ker}(\varphi)x$ که در آن x عنصر دلخواهی در G است که $\varphi(x) = w'$.

ما این مطلب را به‌صورت لم زیر بیان می‌کنیم.

لم ۴.۵.۲. هرگاه $w' \in G'$ به شکل $\varphi(x) = w'$ باشد، آن‌گاه

$$\{y \in G | \varphi(y) = w'\} = \mathrm{Ker}(\varphi)x$$

حال به چند خاصیت اصلی هستهٔ همریختیها می‌پردازیم.

قضیهٔ ۵.۵.۲. هرگاه φ یک همریختی از G به توی G' باشد، آن‌گاه

الف) $\mathrm{Ker}(\varphi)$ زیرگروه G است؛

ب) به ازای هر $a \in G$، $a^{-1}\mathrm{Ker}(\varphi)a \subset \mathrm{Ker}(\varphi)$.

برهان. این قضیه با تمام اهمیتی که دارد برهانش ساده است. هرگاه $a, b \in \mathrm{Ker}(\varphi)$، آن‌گاه $\varphi(a) = \varphi(b) = e'$. پس $\varphi(ab) = \varphi(a)\varphi(b) = e'$ که از آنجا $ab \in \mathrm{Ker}(\varphi)$. پس $\mathrm{Ker}(\varphi)$ تحت ضرب بسته است. همچنین $\varphi(a) = e'$ ایجاب می‌کند که

$$\varphi(a^{-1}) = \varphi(a)^{-1} = e'$$

و در نتیجه $a^{-1} \in \text{Ker}(\varphi)$. لذا $\text{Ker}(\varphi)$ زیرگروه G است. هرگاه $k \in \text{Ker}(\varphi)$ و $a \in G$، آن‌گاه $\varphi(k) = e'$؛ در نتیجه

$$\begin{aligned}\varphi(a^{-1}ka) &= \varphi(a^{-1})\varphi(k)\varphi(a) = \varphi(a^{-1})e'\varphi(a) = \varphi(a^{-1})\varphi(a)\\ &= \varphi(a^{-1}a) = \varphi(e) = e'\end{aligned}$$

این به ما می‌گوید که $a^{-1}ka \in \text{Ker}(\varphi)$. پس $a^{-1}\text{Ker}(\varphi)a \subset \text{Ker}(\varphi)$ و قضیه به‌طور کامل ثابت می‌شود. ■

نتیجه. هرگاه φ یک همریختی از G به توی G' باشد، آن‌گاه φ یک تکریختی است اگر و فقط اگر $\text{Ker}(\varphi) = \{e\}$.

برهان. این امر در واقع نتیجه‌ای است از لم ۲.۵.۴. شرح مطلب را به خواننده وا می‌گذاریم. ■

خاصیت (ب) $\text{Ker}(\varphi)$ در قضیهٔ ۲.۵.۵ یک خاصیت جالب و اساسی زیرگروههاست. ما قبلاً در متن و مسائل چند بار به این خاصیت برخورده‌ایم. حال از آن برای تعریف ردهٔ بسیار مهمی از زیرگروههای یک گروه استفاده می‌کنیم.

تعریف. زیرگروه N از G را یک زیرگروه نرمال G نامیم اگر به ازای هر $a \in G$، $a^{-1}Na \subset N$.

البته $\text{Ker}(\varphi)$ هر همریختی یک زیرگروه نرمال G است. همان‌طور که در بخش بعد خواهیم دید، هر زیرگروه نرمال G هستهٔ همریختی مناسبی از G به توی گروه مناسبی چون G' است. لذا مفاهیم همریختی و زیرگروه نرمال به نوعی هم‌ارز یکدیگر می‌باشند.

با آنکه زیرگروه نرمال به‌وسیلهٔ $a^{-1}Na \subset N$ تعریف شد، ولی عملاً داریم $a^{-1}Na = N$، چرا که اگر به ازای هر $a \in G$، $a^{-1}Na \subset N$، آن‌گاه

$$N = a(a^{-1}Na)a^{-1} \subset aNa^{-1} = (a^{-1})^{-1}Na^{-1} \subset N$$

لذا به ازای هر $a \in G$، $N = aNa^{-1}$. با جابجایی داریم $Na = aN$؛ یعنی هر هم‌مجموعهٔ چپ N در G یک هم مجموعهٔ راست N در G است.

از آن‌سو، اگر هر هم‌مجموعهٔ چپ N در G یک هم‌مجموعهٔ راست باشد، به ازای هر $a \in G$ عنصری مانند $b \in G$ هست که $Na = bN$. ولی $a \in Na$. پس $a \in bN$. لذا $NN \subset N$)

زیرا N بسته است) $aN \subset (bN)N = b(NN) \subset bN$. پس $aN \subset bN = Na$؛ و در نتیجه $aNa^{-1} \subset N$ که به معنی نرمال بودن N در G می‌باشد.

اگر N زیرگروه نرمال G باشد، آن را با علامت اختصاری $N \lhd G$ نشان می‌دهیم.

توجه کنید که $a^{-1}Na = N$ به معنی $a^{-1}na = n$ به ازای هر $n \in N$ نیست. این صرفاً یعنی مجموعهٔ تمام $a^{-1}na$ها همان مجموعهٔ تمام nها می‌باشد.

پس قضیهٔ زیر ثابت شده است.

قضیهٔ ۶.۵.۲. $N \lhd G$ اگر و فقط اگر هر هم‌مجموعهٔ چپ N در G یک هم‌مجموعهٔ راست N در G باشد.

پیش از ادامهٔ بحث، لحظه‌ای مکث کرده به هستهٔ چند همریختی و زیرگروه نرمال نظر می‌افکنیم.

چند مثال

۱. هرگاه G آبلی باشد، آن‌گاه هر زیرگروه G نرمال است، زیرا به ازای هر $a, x \in G$، $a^{-1}xa = x$. عکس این مطلب درست نیست. گروههایی غیرآبلی وجود دارند که در آنها هر زیرگروه نرمال است. ببینید می‌توانید یک چنین گروه که از مرتبهٔ ۸ باشد بیابید. این گروههای غیرآبلی را به افتخار ریاضیدان ایرلندی، دبلیو.آر.هامیلتون (W.R. Hamilton, 1805-1865) هامیلتونی می‌نامند. گروه مطلوب از مرتبهٔ ۸ را می‌توان در چهارگانهای هامیلتون، که در فصل ۴، بخش ۱، معرفی می‌شوند، جستجو کرد.

در مثال ۱ ابتدای این بخش داریم $\varphi(x) = \log_{10} x$ و

$$\operatorname{Ker}(\varphi) = \{x \mid \log_{10} x = 0\} = \{1\}$$

در مثال ۲ که G آبلی است و $\varphi(x) = x^2$،

$$\operatorname{Ker}(\varphi) = \{x \in G \mid x^2 = e\}$$

هستهٔ همریختی بدیهی مثال ۳ تمام G است. در مثال ۴ $\operatorname{Ker}(\varphi)$ مجموعهٔ تمام اعداد صحیح زوج است. در مثال ۵ $\operatorname{Ker}(\varphi) = \{a \in \mathbb{C}' \mid \ |a| = 1\}$، که می‌توان آن را با استفاده از شکل قطبی یک عدد مختلط به‌صورت $\operatorname{Ker}(\varphi) = \{\cos x + i \sin x \mid \text{حقیقی } x\}$ نوشت. در مثال ۶ $\operatorname{Ker}(\varphi) = \{T_{1,b} \in G \mid \text{حقیقی } b\}$. در مثال ۷ $\operatorname{Ker}(\varphi)$ مجموعهٔ تمام مضارب n است.

در مثال ۸ و ۹ هسته‌ها فقط از e تشکیل شده‌اند، زیرا نگاشتها تکریختی می‌باشند. و در مثال ۱۰ ملاحظه می‌کنیم که $\mathrm{Ker}(\varphi) = \{2\pi m | m \text{ عدد صحیح}\}$.

البته تمام هسته‌های فوق زیرگروههای نرمال گروههای مربوط به خوداند. ما باید به چند زیرگروه نرمال که ذاتاً در خود Gاند بدون توسل به هسته‌های همریختی نیز توجه کنیم. برای این کار به مثالهای بخش ۱ باز می‌گردیم.

۱. در مثال ۷ $H = \{T_{a,b} \in G | a \text{ گویا}\}$. اگر $T_{x,y} \in G$، برخواننده است تحقیق کند که $T_{x,y}^{-1} H T_{x,y} \subset H$؛ و لذا $H \triangleleft G$.

۲. در مثال ۹ زیرگروه $G \triangleleft \{i, g, g^2, g^3\}$. در اینجا نیز تحقیق امر به خواننده محول می‌شود.

۳. در مثال ۱۰ زیرگروه $H = \{i, h, h^2, \ldots, h^{n-1}\}$ در G نرمال است. این امر را نیز به خواننده وامی‌گذاریم.

۴. اگر G یک گروه باشد، $Z(G)$، یعنی مرکز G، زیرگروه نرمالی از G است (ر.ک. مثال ۱۱ از بخش ۳).

۵. فرض کنیم $G = S_3$. G دارای عناصر i، f، g، g^2، fg، و gf است که $f(x_1) = x_2$، $f(x_2) = x_1$، $f(x_3) = x_3$، و $g(x_1) = x_2$، $g(x_2) = x_3$، $g(x_3) = x_1$. حکم می‌کنیم که $N = \{i, g, g^2\} \triangleleft S_3$. همان‌طور که قبلاً دیدیم (یا می‌توان حساب کرد)، $fgf^{-1} = g^{-1} = g^2$، $fg^2f^{-1} = g$، $(fg)g(fg)^{-1} = fggg^{-1}f^{-1} = fgf^{-1} = g^2$، و از این قبیل. لذا $N \triangleleft S_3$.

مطالب این بخش یک جیرهٔ غذایی نسبتاً قوی است. ممکن است ظاهراً چنین نباشد، ولی ایده‌های ارائه شده با همهٔ سادگی نسبتاً ظریف می‌باشند. به خواننده توصیه می‌شود که قبل از جلو رفتن مفاهیم و نتایج را کاملاً هضم نماید. یک راه برای درک میزان کامل بودن این هضم پرداختن به مسائل فراوانی است که ذیلاً می‌آیند. مطالب بخش بعد از این هم قویتر و هضمشان مشکلتر است. با هضم مطالب این بخش می‌توان از دل درد بعدی ریاضی پرهیز کرد.

مسائل

مسائل آسانتر

۱. در هر قسمت معین کنید که نگاشت داده شده همریختی است یا نه. در صورت بودن،

هسته‌اش را مشخص کرده و ۱-۱ یا برو بودن نگاشت را معین نمایید:

الف) $G = \mathbb{Z}$ تحت $+$، $G' = \mathbb{Z}_n$، $\varphi(a) = [a]$ به ازای $a \in \mathbb{Z}$؛

ب) G گروه، $\varphi : G \to G$ با تعریف $\varphi(a) = a^{-1}$ به ازای $a \in G$؛

پ) G گروه آبلی، $\varphi : G \to G$ با تعریف $\varphi(a) = a^{-1}$ به ازای $a \in G$؛

ت) G گروه تمام اعداد حقیقی ناصفر تحت ضرب، $G' = \{1, -1\}$، و $\varphi(r) = 1$ اگر r مثبت باشد، $\varphi(r) = -1$ اگر r منفی باشد؛

ث) G گروه آبلی، $n > 1$ یک عدد صحیح ثابت، و $\varphi : G \to G$ با تعریف $\varphi(a) = a^n$ به ازای $a \in G$.

۲. به یاد آورید که $G \simeq G'$ یعنی G با G' یکریخت است. ثابت کنید به ازای جمیع گروههای G_1، G_2، و G_3،

الف) $G_1 \simeq G_1$؛

ب) $G_1 \simeq G_2$ ایجاب می‌کند که $G_2 \simeq G_1$؛

پ) $G_1 \simeq G_2$ و $G_2 \simeq G_3$ ایجاب می‌کنند که $G_1 \simeq G_3$.

۳. فرض کنید G یک گروه و $A(G)$ مجموعهٔ تمام نگاشتهای ۱-۱ از G (به‌عنوان یک مجموعه) به روی خود باشد. $L_a : G \to G$ را با $L_a(x) = xa^{-1}$ تعریف و ثابت کنید

الف) $L_a \in A(G)$؛

ب) $L_a L_b = L_{ab}$؛

پ) نگاشت $\psi : G \to A(G)$ با تعریف $\psi(a) = L_a$ یک تکریختی از G به توی $A(G)$ است.

۴. در مسئلهٔ ۳ ثابت کنید به ازای هر $a, b \in G$، $T_a L_b = L_b T_a$ که در آن T_a همانند مثال ۸ تعریف می‌شود.

۵. در مسئلهٔ ۴ نشان دهید هرگاه $V \in A(G)$ چنان باشد که به ازای هر $a \in G$، $T_a V = V T_a$، آن‌گاه به ازای $b \in G$ای، $V = L_b$. (راهنمایی. با عمل بر $e \in G$ معین کنید که b چه باید باشد.)

۶. ثابت کنید هرگاه $\varphi : G \to G'$ یک همریختی باشد، آن‌گاه $\varphi(G)$، یعنی نقش G، زیرگروهی است از G'.

۷. نشان دهید که همریختی $\varphi : G \to G'$ یک تکریختی است اگر و فقط اگر $\mathrm{Ker}(\varphi) = \{e\}$.

۸. یک یکریختی از گروه تمام اعداد حقیقی G تحت $+$ به روی گروه تمام اعداد حقیقی مثبت G' تحت ضرب بیابید.

۹. تحقیق کنید که هرگاه G گروه مثال ۶ در بخش ۱ بوده و $H = \{T_{a,b} \in G | a \text{ گویا}\}$، آن‌گاه $H \lhd G$.

۱۰. تحقیق کنید که در مثال ۹ از بخش ۱، یعنی گروه دو وجهی از مرتبهٔ ۸، مجموعهٔ

$$H = \{i, g, g^2, g^3\}$$

یک زیرگروه نرمال G است.

۱۱. تحقیق کنید که در مثال ۱۰ از بخش ۱، زیرگروه $H = \{i, h, h^2, \ldots, h^{n-1}\}$ در G نرمال است.

۱۲. ثابت کنید هرگاه $Z(G)$ مرکز G باشد، آن‌گاه $Z(G) \lhd G$.

۱۳. اگر G یک گروه آبلی متناهی از مرتبهٔ n بوده و $\varphi : G \to G$ با $\varphi(a) = a^m$ به ازای هر $a \in G$ تعریف شده باشد، شرط لازم و کافی برای یکریختی بودن φ از G به روی خود را بیابید.

۱۴. اگر G آبلی بوده و $\varphi : G \to G'$ یک همریختی از G به روی G' باشد، ثابت کنید G' آبلی می‌باشد.

۱۵. اگر G یک گروه باشد، $N \lhd G$، و $\varphi : G \to G'$ یک همریختی از G به روی G' باشد، ثابت کنید نقش N، یعنی $\varphi(N)$، زیرگروه نرمال G' است.

۱۶. اگر $N \lhd G$ و $M \lhd G$ و $MN = \{mn | m \in M, n \in N\}$، ثابت کنید MN زیرگروه G بوده و $MN \lhd G$.

۱۷. اگر $M \lhd G$ و $N \lhd G$، ثابت کنید $M \cap N \lhd G$.

۱۸. اگر H زیرگروهی از G بوده و $N = \cap_{a \in G} a^{-1} H a$، ثابت کنید که $N \lhd G$.

۱۹. اگر H زیرگروهی از G باشد، $N(H)$ را به‌صورت $N(H) = \{a \in G | a^{-1} H a = H\}$ تعریف و ثابت کنید

الف) $N(H)$ زیرگروهی از G بوده و $N(H) \supset H$؛

ب) $H \lhd N(H)$؛

پ) هرگاه K زیرگروهی از G باشد به‌طوری که $H \lhd K$، آن‌گاه $K \subset N(H)$. [لذا $N(H)$ بزرگترین زیرگروهی از G است که در آن H نرمال است.]

۲۰. اگر $M \lhd G$، $N \lhd G$ و $M \cap N = (e)$، نشان دهید که به ازای هر $m \in M$ و $n \in N$، $mn = nm$.

۲۱. فرض کنید S مجموعه‌ای با بیش از دو عنصر بوده و $A(S)$ مجموعهٔ تمام نگاشتهای ۱-۱ از S به روی خود باشد. اگر $s \in S$، تعریف کنید $H(s) = \{f \in A(S) | f(s) = s\}$ و ثابت کنید $H(s)$ نمی‌تواند یک زیرگروه نرمال $A(S)$ باشد.

۲۲. فرض کنید $G = S_3$ گروه متقارن از درجهٔ ۳ بوده و $H = \{i, f\}$ که در آن $f(x_1) = x_2$، $f(x_2) = x_1$، $f(x_3) = x_3$.

الف) تمام هم‌مجموعه‌های چپ H در G را بنویسید.

ب) تمام هم‌مجموعه‌های راست H در G را بنویسید.

پ) آیا هر هم‌مجموعهٔ چپ H یک هم‌مجموعهٔ راست H است؟

۲۳. فرض کنید تمام زیرگروههای G در G نرمال باشند. ثابت کنید به ازای هر $a, b \in G$، jای هست به‌طوری که $ba = a^j b$.

۲۴. فرض کنید G_1 و G_2 دو گروه بوده و $G = G_1 \times G_2$ حاصلضرب دکارتی G_1 و G_2 باشد [یعنی G مجموعهٔ تمام جفتهای مرتب (a, b) باشد که $a \in G_1$ و $b \in G_2$]. ضرب در G را با

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$$

تعریف و

الف) ثابت کنید G یک گروه است؛

ب) نشان دهید که تکریختی φ_1 از G_1 به توی G با تعریف $\varphi_1(a_1) = (a_1, e_2)$، که در آن e_2 عنصر همانی G_2 است، چنان است که $\varphi_1(G_1) \triangleleft G$؛

پ) قسمت (ب) را برای G_2 نیز حل کنید؛

ت) با استفاده از نگاشتهای φ_1 و φ_2 قسمتهای (ب) و (پ)، ثابت کنید

$$\varphi_1(G_1)\varphi_2(G_2) = G$$

و $\varphi_1(G_1) \cap \varphi_2(G_2)$ عنصر همانی G است؛

ث) ثابت کنید $G_1 \times G_2 \simeq G_2 \times G_1$

۲۵. فرض کنید G یک گروه و $W = G \times G$ همانند مسئلهٔ ۲۴ تعریف شده باشد. ثابت کنید

الف) نگاشت $\varphi : G \to W$ با تعریف $\varphi(a) = (a, a)$ یک تکریختی از G به توی W است؛

ب) نقش $\varphi(G)$ در W [یعنی $\{(a, a) | a \in G\}$] در W نرمال است اگر و فقط اگر G آبلی باشد.

مسائل با سطح متوسط

*۲۶. اگر G یک گروه بوده و $a \in G$، $\sigma_a : G \to G$ را با $\sigma_a(g) = aga^{-1}$ تعریف کنید. در مثال ۹ این بخش دیدیم که σ_a یک یکریختی از G به روی خود است. پس $\sigma_a \in A(G)$ یعنی متعلق به گروه تمام نگاشتهای ۱-۱ از G (به‌عنوان مجموعه) به روی خود می‌باشد.
$\psi : G \to A(G)$ را به ازای هر $a \in G$ با $\psi(a) = \sigma_a$ تعریف و ثابت کنید

الف) ψ یک همریختی از G به توی $A(G)$ است؛

ب) (مرکز G) $\mathrm{Ker}(\psi) = Z(G)$.

۲۷. اگر θ یک خودریختی از G بوده و $N \triangleleft G$، ثابت کنید $\theta(N) \triangleleft G$.

۲۸. فرض کنید θ و ψ خودریختیهایی از G بوده و $\theta\psi$ حاصلضرب θ و ψ به‌عنوان نگاشتهایی بر G باشد. ثابت کنید $\theta\psi$ یک خودریختی G بوده و θ^{-1} یک خودریختی G است؛ در نتیجه مجموعهٔ تمام خودریختیهای G خود یک گروه می‌باشد.

*۲۹. زیرگروه T از گروه W را مشخص نامیم اگر به ازای هر خودریختی φ از W، $\varphi(T) \subset T$. ثابت کنید.

الف) مشخص بودن M در G ایجاب می‌کند که $M \triangleleft G$؛

ب) مشخص بودن M و N در G مشخص بودن MN در G را ایجاب می‌کنند؛

پ) لازم نیست هر زیرگروه نرمال یک گروه مشخص باشد. (اثبات این امر نسبتاً مشکل است؛ باید گروهی مانند G و یک زیرگروه نرمال غیرمشخص پیدا کنید.)

۳۰. فرض کنید $|G| = pm$ که در آن $p \nmid m$ و p اول است. اگر H یک زیرگروه نرمال از مرتبهٔ p در G باشد، ثابت کنید H مشخص است.

۳۱. فرض کنید G یک گروه آبلی از مرتبهٔ $p^n m$ باشد که $p \nmid m$ اول است. اگر H زیرگروهی از G از مرتبهٔ p^n باشد، ثابت کنید H یک زیرگروه مشخص از G است.

۳۲. اگر به طریقی بدانید که $H \triangleleft G$، مسئلهٔ ۳۱ را حتی اگر G آبلی نباشد حل کنید.

۳۳. فرض کنید $N \triangleleft G$ و $M \subset N$ یک زیرگروه مشخص N باشد. ثابت کنید $M \triangleleft G$. (این امر که هرگاه $M \triangleleft N$ و $N \triangleleft G$، آن‌گاه M باید در G نرمال باشد درست نیست. ر.ک. مسئلهٔ ۵۰.)

۳۴. فرض کنید G یک گروه و $A(G)$ گروه تمام خود ریختیهای G باشد. (ر.ک. مسئلهٔ ۲۸.) قرار دهید $I(G) = \{\sigma_a | a \in G\}$ که در آن σ_a همانند مسئلهٔ ۲۶ تعریف شده است. ثابت کنید $I(G) \triangleleft A(G)$.

۳۵. نشان دهید که $Z(G)$، یعنی مرکز Z، یک زیرگروه مشخص G است.

۳۶. اگر $G \triangleleft N$ و H زیرگروه G باشد، نشان دهید که $H \cap N \triangleleft H$.

مسائل مشکلتر

۳۷. اگر G یک گروه غیرآبلی از مرتبهٔ ۶ باشد، ثابت کنید $G \simeq S_3$.

۳۸. فرض کنید G گروه و H زیرگروهی از آن باشد. همچنین $S = \{Ha | a \in G\}$ مجموعهٔ تمام هم‌مجموعه‌های راست H در G باشد. به ازای $b \in G$، $T_b : S \to S$ را با $T_b(Ha) = Hab^{-1}$ تعریف کنید.

الف) ثابت کنید به ازای هر $b, c \in G$، $T_bT_c = T_{bc}$ [لذا نگاشت $\psi : G \to A(S)$ با تعریف $\psi(b) = T_b$ یک همریختی است].

ب) $\mathrm{Ker}(\psi)$، یعنی هستهٔ $\psi : G \to A(S)$، را توصیف کنید.

پ) نشان دهید که $\mathrm{Ker}(\psi)$ بزرگترین زیرگروه نرمال G واقع در H است [بزرگترین به این معنی که هرگاه $N \triangleleft G$ و $N \subset H$، آن‌گاه $N \subset \mathrm{Ker}(\psi)$].

۳۹. مسئلهٔ ۳۷ را با استفاده از مسئلهٔ ۳۸ حل کنید.

یادآور شویم که هرگاه H زیرگروه G باشد، آن‌گاه اندیس H در G، یعنی $i_G(H)$، تعداد هم‌مجموعه‌های راست متمایز H در G (در صورت متناهی بودن این عدد) می‌باشد.

۴۰. اگر G یک گروه متناهی بوده و زیرگروه H از G چنان باشد که $n \nmid i_G(H)!$ که در آن $n = |G|$، ثابت کنید یک زیرگروه نرمال مانند $N \neq (e)$ از G مشمول H وجود دارد.

۴۱. فرض کنید بدانیم که یک گروه G از مرتبهٔ ۲۱ شامل عنصری مانند a از مرتبهٔ ۷ است. ثابت کنید $A = (a)$، یعنی زیرگروه تولید شده به‌وسیلهٔ a، در G نرمال است. (راهنمایی. از مسئلهٔ ۴۰ استفاده کنید.)

۴۲. فرض کنید بدانیم که یک گروه G از مرتبهٔ ۳۶ زیرگروهی مانند H از مرتبهٔ ۹ دارد. ثابت کنید $H \triangleleft G$ یا زیرگروهی مانند N هست که $N \triangleleft G$، $N \subset H$، و $|N| = 3$.

۴۳. ثابت کنید یک گروه از مرتبهٔ ۹ باید آبلی باشد.

۴۴. ثابت کنید یک گروه از مرتبهٔ p^2، که p اول است، زیرگروه نرمالی از مرتبهٔ p دارد.

۴۵. با استفاده از مسئلهٔ ۴۴ ثابت کنید یک گروه از مرتبهٔ p^2، که p اول است، باید آبلی باشد.

۴۶. فرض کنید G گروهی از مرتبهٔ ۱۵ باشد. نشان دهید که عنصری مانند $a \neq e$ در G هست به‌طوری که $a^3 = e$ و عنصری مانند $b \neq e$ هست به‌طوری که $b^5 = e$.

۴۷. در مسئلهٔ ۴۶ نشان دهید که هر دو زیرگروه $A = \{e, a, a^2\}$ و $B = \{e, b, b^2, b^3, b^4\}$ در G نرمال‌اند.

۴۸. با استفاده از مسئلهٔ ۴۷ نشان دهید که هر گروه از مرتبهٔ ۱۵ دوری است.

مسائل بسیارمشکل

۴۹. فرض کنید G یک گروه و H زیرگروهی از آن باشد به‌طوری که $i_G(H)$ متناهی است. ثابت کنید زیرگروهی مانند $N \subset H$ هست که $N \triangleleft G$ و $i_G(N)$ متناهی است.

۵۰. گروه G را طوری بسازید که G زیرگروه نرمالی مانند N و N زیرگروه نرمالی مانند M داشته باشد (یعنی $N \triangleleft G$ و $M \triangleleft N$) ولی M در G نرمال نباشد.

۵۱. فرض کنید G گروهی متناهی و φ یک خودریختی از G باشد به‌طوری که φ^2 خودریختی همانی G است. همچنین $\varphi(x) = x$ تساوی $x = e$ را ایجاب کند. ثابت کنید G آبلی است و به ازای هر $a \in G$، $\varphi(a) = a^{-1}$.

۵۲. فرض کنید G گروهی متناهی بوده و خودریختی φ از G چنان باشد که به ازای بیش از سه‌چهارم عناصر G، $\varphi(x) = x^{-1}$. ثابت کنید به ازای هر $y \in G$، $\varphi(y) = y^{-1}$؛ و در نتیجه G آبلی می‌باشد.

۶. گروههای عاملی

فرض کنیم G یک گروه و N زیرگروه نرمالی از آن باشد. در اثبات قضیهٔ لاگرانژ، به ازای زیرگروه دلخواه H، از رابطهٔ هم‌ارزی $a \sim b$ اگر $ab^{-1} \in H$ استفاده شد. حال این رابطه را وقتی N نرمال است به کار می‌بریم تا ببینیم آیا می‌شود کمی بیش از یک زیرگروه عادی سخن گفت.

لذا قرار می‌دهیم $a \sim b$ اگر $ab^{-1} \in N$ و فرض می‌کنیم $[a] = \{x \in G | x \sim a\}$. همان‌طور که قبلاً دیدیم، $[a] = Na$ یعنی هم‌مجموعهٔ راست N در G شامل a. به یاد آورید که با یک نگاه به $\mathbb{Z}_n$ برایش رابطهٔ $+$ را به‌وسیلهٔ $[a] + [b] = [a + b]$ تعریف کردیم. چرا این کار را برای گروه دلخواه G و زیرگروه نرمال N از G نکنیم؟

لذا قرار می‌دهیم $M = \{[a] | a \in G\}$ که در آن $[a] = \{x \in G | xa^{-1} \in N\} = Na$. حال ضرب در M را با $[a][b] = [ab]$ تعریف می‌کنیم. به‌زودی نشان می‌دهیم که M تحت این ضرب یک گروه است. ولی قبل از هر چیز باید نشان دهیم که ضرب در M تعریف شده است. به عبارت دیگر، باید نشان دهیم که هرگاه $[a] = [a']$ و $[b] = [b']$، آن‌گاه $[ab] = [a'b']$ زیرا این

نشان می‌دهد که $[a][b] = [ab] = [a'b'] = [a'][b']$. به بیان معادل، این حاصلضرب رده‌ها به نماینده‌های خاصی که برای رده‌ها به‌کار می‌بریم بستگی ندارد.

لذا فرض می‌کنیم $[a] = [a']$ و $[b] = [b']$. از تعریف هم‌ارزی‌مان داریم $a' = na$ که در آن $n \in N$. به همین نحو $b' = mb$ که در آن $m \in N$. لذا $a'b' = namb = n(ama^{-1})ab$. چون $N \lhd G$، ama^{-1} در N است. پس $n(ama^{-1})$ نیز در N می‌باشد. لذا اگر قرار دهیم $n_1 = n(ama^{-1})$، داریم $n_1 \in N$ و $a'b' = n_1ab$. ولی این به ما می‌گوید که $a'b' \in Nab$. پس $a'b' \sim ab$ که از آن داریم $[a'b'] = [ab]$. این یعنی ضربمان در M تعریف شده است.

لذا M دارای ضرب تعریف شدهٔ $[a][b] = [ab]$ می‌باشد. حال اصول موضوع گروه را برای M تحقیق می‌کنیم. بسته بودن از تعریف این ضرب نتیجه می‌شود. هرگاه $[a]$ و $[b]$ و $[c]$ در M باشند، آن‌گاه

$$
\begin{aligned}
[a]([b][c]) = [a][bc] = [a(bc)] &= [(ab)c] \quad \text{(زیرا ضرب در } G \text{ شرکتپذیر است)} \\
&= [ab][c] = ([a][b])[c]
\end{aligned}
$$

لذا قانون شرکتپذیری برای ضرب در M برقرار است. و اما عنصر یکه چیست؟ چرا انتخاب واضح $[e]$ را امتحان نکنیم؟ بی‌درنگ مشاهده می‌شود که $[a][e] = [ae] = [a]$ و $[e][a] = [ea] = [a]$. پس $[e]$ به‌عنوان عنصر یکهٔ M عمل می‌کند. بالاخره معکوسها چیستند؟ در اینجا نیز انتخاب واضح انتخاب مناسبی است. هرگاه $a \in G$، آن‌گاه $[a][a^{-1}] = [aa^{-1}] = [e]$. پس $[a^{-1}]$ معکوس $[a]$ نسبت به ضرب تعریف شده در M می‌باشد.

مایلیم به M یک نام و بیش از آن علامتی بدهیم که وابستگی‌اش را به G و N نشان دهد. علامتی که برای M به‌کار می‌بریم G/N است (بخوانید: G روی N یا $G \bmod N$) و G/N را گروه عاملی یا گروه خارج‌قسمتی G بر N می‌نامیم.

آنچه به ثبوت رسیده است قضیهٔ بسیار معروف زیر است.

قضیهٔ ۱.۶.۲. هرگاه $N \lhd G$ و

$$G/N = \{[a] | a \in G\} = \{Na | a \in G\}$$

آن‌گاه G/N نسبت به عمل $[a][b] = [ab]$ یک گروه است.

بی‌درنگ معلوم می‌شود که:

قضیهٔ ۲.۶.۲. هرگاه $N \triangleleft G$، آن‌گاه یک همریختی مانند ψ از G به روی G/N هست به‌طوری که $\mathrm{Ker}(\psi)$، یعنی هستهٔ ψ، مساوی N است.

برهان. طبیعی‌ترین نگاشت از G به G/N حلال مشکلات است. $\psi : G \to G/N$ را با $\psi(a) = [a]$ تعریف می‌کنیم. ضرب ما در G/N نگاشت ψ را همریختی می‌سازد، زیرا $\psi(ab) = [ab] = [a][b] = \psi(a)\psi(b)$. چون هر عنصر $X \in G/N$ به ازای $b \in G$ای به شکل $X = [b] = \psi(b)$ است، پس ψ برو می‌باشد. بالاخره هستهٔ $\mathrm{Ker}(\psi)$ نگاشت ψ چیست؟ طبق تعریف، $\mathrm{Ker}(\psi) = \{a \in G | \psi(a) = E\}$ که در آن E عنصر یکهٔ G/N است. اما E چیست؟ این چیزی جز $E = [e] = Ne = N$ نیست، و $a \in \mathrm{Ker}(\psi)$ اگر و فقط اگر $E = N = \psi(a) = Na$. ولی $Na = N$ می‌گوید که $a = ea \in Na = N$. پس معلوم می‌شود که $\mathrm{Ker}(\psi) \subset N$. اثبات $N \subset \mathrm{Ker}(\psi)$ آسان است و به خواننده محول می‌شود. بنابراین $\mathrm{Ker}(\psi) = N$. ■

قضیهٔ ۲.۶.۲ نکتهٔ مذکور در بخش پیش که «هر زیرگروه نرمال N از G هستهٔ یک همریختی از G به روی یک گروه است» را تقویت می‌کند. «یک همریختی» عبارت است از ψ تعریف شده در بالا و «یک گروه» عبارت است از G/N.

ساختمان گروه عاملی G بر N احتمالاً مهمترین ساختمان در نظریهٔ گروههاست. همان‌طور که بعدها خواهیم دید، در سایر دستگاههای جبری نیز ساختمانهای مشابهی خواهیم داشت.

می‌پرسیم: در این مسئله نرمال بودن N در G کجا وارد شد؟ چرا این کار را برای هر زیرگروه H از G نکنیم؟ ببینیم با این کار چه رخ می‌دهد. مثل قبل تعریف می‌کنیم

$$W = \{[a] | a \in G\} = \{Ha | a \in G\}$$

که در آن هم‌ارزی $a \sim b$ با $ab^{-1} \in H$ تعریف می‌شود. حال ضربی در W مشابه ضرب G/N به‌صورت $[a][b] = [ab]$ تعریف می‌کنیم. آیا این ضرب تعریف شده است؟ هرگاه $h \in H$، آن‌گاه $[hb] = [b]$. پس برای آنکه این ضرب تعریف شده باشد باید $[a][b] = [a][hb]$؛ یعنی $[ab] = [ahb]$. از این داریم $Hab = Hahb$؛ و در نتیجه $Ha = Hah$. این ایجاب می‌کند که $H = Haha^{-1}$ که از آنجا $aha^{-1} \in H$. یعنی، به ازای هر $a \in G$ و هر $h \in H$، aha^{-1} باید در H باشد. به‌عبارت دیگر، H باید در G نرمال باشد. لذا، برای آنکه ضرب در W تعریف شده باشد، H باید زیرگروه نرمالی از G باشد.

مطلب فوق راجع به گروه خارج‌قسمتی را می‌توان به شیوه‌ای کمی متفاوت در نظر گرفت. اگر

A و B زیرمجموعه‌هایی از G باشند، قرار می‌دهیم $AB = \{ab|b \in B، a \in A\}$. هرگاه H زیرگروه G باشد، آن‌گاه $HH \subset H$ راه دیگر بیان بسته بودن H تحت ضرب G است.

فرض کنیم $G/N = \{Na|a \in G\}$ مجموعهٔ تمام هم‌مجموعه‌های راست زیرگروه نرمال N در G باشد. با استفاده از ضرب زیرمجموعه‌های G که در بالا تعریف شد، $(Na)(Nb)$ چیست؟ طبق تعریف، $(Na)(Nb)$ از تمام عناصر به شکل $(na)(mb)$ تشکیل شده است که در آن $n, m \in N$؛ و در نتیجه

$$(na)(mb) = (nama^{-1})(ab) = n_1ab$$

که در آن $n_1 = nama^{-1}$ در N است زیرا N نرمال می‌باشد. لذا $(Na)(Nb) \subset Nab$. از آن‌سو، هرگاه $n \in N$، آن‌گاه

$$n(ab) = (na)(eb) \in (Na)(Nb)$$

پس $Nab \subset (Na)(Nb)$. به‌طور خلاصه، نشان داده‌ایم که حاصلضرب Na و Nb به‌عنوان زیرمجموعه‌های G از فرمول $(Na)(Nb) = Nab$ به‌دست می‌آید. تمام اصول موضوع دیگر برای گروه بودن G/N از این فرمول ضرب به آسانی تحقیق می‌شوند.

راه دیگر مشاهدهٔ $(Na)(Nb) = Nab$ توجه به نرمال بودن N، یعنی $aN = Na$، است. داریم $(Na)(Nb) = N(aN)b = N(Na)b = NNab = Nab$، زیرا (به دلیل زیرگروه G بودن N) $NN = N$.

به هر حال با گرفتن G/N به‌عنوان رده‌های هم‌ارزی یا به‌عنوان مجموعه‌ای از زیرمجموعه‌های G گروهی به‌دست می‌آید که ساختارش با ساختار G از طریق همریختی طبیعی ψ از G به روی G/N ارتباط نزدیکی دارد.

به‌زودی خواهیم دید که چطور از تلفیق استقرا و ساختار G/N می‌توان اطلاعاتی راجع به G به‌دست آورد.

هرگاه G گروهی متناهی بوده و $N \triangleleft G$، آن‌گاه تعداد هم‌مجموعه‌های راست N در G، یعنی $i_G(N)$ (طبق قضیهٔ لاگرانژ) مساوی است با $i_G(N) = |G|/|N|$. اما این مرتبهٔ G/N است که مجموعهٔ تمام هم‌مجموعه‌های راست N در G می‌باشد. لذا $|G/V| = |G|/|N|$. این امر را به‌طور صوریتر بیان می‌کنیم:

قضیهٔ ۲.۶.۳. هرگاه G یک گروه متناهی بوده و $N \triangleleft G$، آن‌گاه

$$|G/N| = |G|/|N|$$

به‌عنوان کاربردی از آنچه فعلاً مورد بحث است، حالت خاصی از یک قضیه را ثابت می‌کنیم که اثبات وضع کلی آن بعدها خواهد آمد. برهان ما، که در حالت آبلی است، برهانی مناسب نیست ولی یک روش کلی را به‌طور کاملاً روشن توضیح می‌دهد و آن برگشت اطلاعات از G/N و دستیابی به اطلاعات مربوط به G می‌باشد.

قضیه‌ای که هم اکنون ثابت می‌کنیم منسوب است به ریاضیدان بزرگ فرانسوی، ا. ال. کشی (A.L. Cauchy, 1789-1857)، که اساسی‌ترین کارش در نظریهٔ متغیرهای مختلط است.

قضیهٔ ۴.۶.۲ (کشی). هرگاه G یک گروه آبلی متناهی از مرتبهٔ $|G|$ بوده و عدد اول p عدد $|G|$ را عاد کند، آن‌گاه G عنصری از مرتبهٔ p دارد.

برهان. پیش از پرداختن به برهان متذکر می‌شویم که این قضیه برای هر گروه متناهی درست است. ما بعدها حالت کلی آن را ثابت می‌کنیم البته با برهانی به‌مراتب زیباتر از برهان فعلی که برای حالت خاص آبلی داده می‌شود.

به استقرا بر $|G|$ عمل می‌کنیم. معنی دقیق این کار چیست؟ فرض می‌کنیم قضیه برای تمام گروههای آبلی از مرتبهٔ کوچکتر از $|G|$ درست باشد و نشان می‌دهیم که قضیه برای G نیز درست است. اگر $|G| = ۱$، چنین pای وجود ندارد و قضیه به انتفای مقدم درست است. لذا نقطهٔ شروع استقرا را داریم.

فرض کنیم زیرگروهی مانند $(e) \neq N \neq G$ موجود باشد. چون $|N| < |G|$، اگر $p \mid |N|$، بنا به فرض استقرا، عنصری از مرتبهٔ p در N، و لذا در G، هست و مطلب تمام. لذا می‌توان فرض کرد که $p \nmid |N|$. چون G آبلی است، هر زیرگروهش نرمال است. پس می‌توان G/N را تشکیل داد. و چون $p \mid |G|$ و $p \nmid |N|$ و نیز $|G/N| = |G|/|N|$، داریم $p \mid |G/N|$. گروه G/N آبلی است زیرا G چنین است (ثابت کنید!) و چون $N \neq (e)$، $|N| > ۱$. پس $|G/N| = |G|/|N| < |G|$. لذا، مجدداً طبق فرض استقرا، عنصری در G/N از مرتبهٔ p وجود دارد. این امر را می‌توان چنین بیان کرد: عنصری مانند $a \in G$ هست به‌طوری که $[a]^p = [e]$ ولی $[a] \neq [e]$. چون $[a^p] = [a]^p = [e]$، از هم‌ارزی تعریف شده با $\mod N$ داریم $a^p \in N$ و $a \notin N$. پس هرگاه $m = |N|$، آن‌گاه، بنابر قضیهٔ ۵.۴.۲، چون $a^p \in N$، $(a^p)^m = e$. پس $(a^m)^p = e$. هرگاه بتوان نشان داد که $b = a^m \neq e$، آن‌گاه b عنصر مطلوب از مرتبهٔ p در G است. ولی هرگاه $a^m = e$، آن‌گاه $[a]^m = [e]$، و چون $[a]$ از مرتبهٔ p است، $p|m$ (ر.ک. مسئلهٔ ۳۱ از بخش ۴). ولی، طبق فرض، $p \nmid m = |N|$. لذا اگر G زیرگروه غیربدیهی داشته باشد مطلب تمام است.

ولی اگر G زیرگروه غیربدیهی نداشته باشد، باید دوری از مرتبهٔ اول باشد (ر.ک. مسئلهٔ ۱۶ از بخش ۳ که اینک می‌توانید آن را ساده‌تر حل کنید.) این «مرتبهٔ اول» چیست؟ چون $p \mid |G|$، باید داشته باشیم $|G| = p$. ولی در این صورت هر عنصر $a \neq e \in G$ در $a^p = e$ صدق کرده و از مرتبهٔ p می‌باشد. این استقرا را کامل کرده و قضیه را به اثبات می‌رساند. ■

ما در مسائل کاربردهایی از این نوع استدلال که خاص نظریهٔ گروههاست خواهیم داشت.

مفهوم گروه عاملی مفهومی است بسیار ظریف و از بالاترین اهمیت برخوردار است. تشکیل مجموعه‌ای جدید از مجموعه‌ای قدیم با استفاده از عناصری که زیرمجموعه‌های مجموعهٔ قدیمی‌اند در نظر شخص مبتدی که این نوع ساختار را نخستین بار می‌بیند عجیب می‌نماید. لذا توجه به این امر از دیدگاههای مختلف با ارزش است. حال G/N را از زاویه‌ای دیگر در نظر می‌گیریم.

ما در تشکیل G/N چه کاری صورت می‌دهیم؟ مسلماً به رده‌های هم‌ارزی تعریف شده از طریق N نگاه می‌کنیم. حال به این امر از طریقی دیگر نظر می‌اندازیم. کاری که می‌کنیم این است که دو عنصر در G را که در رابطهٔ $ab^{-1} \in N$ صدق کنند با هم یکی می‌کنیم. ما N را به یک معنی حذف می‌کنیم. لذا، با آنکه G/N زیرگروه G نیست، می‌توان N را حذف و به آن مانند G نگاه کرد و دو عنصر را در صورتی مساوی گرفت که «با تقریب N» مساوی باشند.

مثلاً در تشکیل $\mathbb{Z}/N$، که در آن $\mathbb{Z}$ گروه اعداد صحیح و N مجموعهٔ تمام مضارب ۵ در $\mathbb{Z}$ است، ۱ با ۶، ۱۱، ۱۶، ۴−، ۹−، ... و تمام مضارب ۵ با ۰ یکی می‌شوند. نکتهٔ جالب آن است که وقتی به $\mathbb{Z}/N$ می‌رویم، این انطباق با جمع در $\mathbb{Z}$ سازگار می‌باشد.

حال از این دیدگاه به چند مثال نگاه می‌کنیم.

۱. فرض کنیم $G = \{T_{a,b} \mid \text{حقیقی } a \neq 0 \text{ و } b\}$ (مثال ۶ از بخش ۱). همچنین

$$N = \{T_{1,b} \mid \text{حقیقی } b\} \subset G$$

دیدیم که $N \triangleleft G$. پس صحبت راجع به G/N معنی دارد. اما $T_{a,b}$ و $T_{a,0}$ در هم مجموعه‌های راست یکسانی از N در Gاند. پس با یکی کردن $T_{a,b}$ و $T_{a,0}$ عنصری در G/N به‌دست می‌آید. این عنصر فقط تابع a است. به‌علاوه $T_{a,b}$ طبق زیرنویس اول a ضرب می‌شود زیرا $T_{a,b}T_{c,d} = T_{ac,ad+b}$ و اگر $T_{a,b}$ را با $T_{a,0}$ و $T_{c,d}$ را با $T_{c,0}$ یکی کنیم، حاصل ضربشان $T_{ac,ad+b}$ با $T_{ac,0}$ یکی می‌شود. لذا ضرب در G/N شبیه ضرب در گروه اعداد حقیقی ناصفر تحت ضرب است، و G/N را به یک معنی (که در بخش بعد دقیقتر خواهد شد) می‌توان با این گروه از اعداد حقیقی یکی کرد.

۲. فرض کنیم G گروه اعداد حقیقی تحت $+$ و $\mathbb{Z}$ گروه اعداد صحیح تحت $+$ باشد. چون G آبلی است، $\mathbb{Z} \triangleleft G$؛ و در نتیجه می‌توان راجع به $G/\mathbb{Z}$ سخن گفت. $G/\mathbb{Z}$ واقعاً چه شکلی است؟ در تشکیل $G/\mathbb{Z}$ هر دو عدد حقیقی که تفاضلشان صحیح باشد یکی می‌شوند. لذا، ۰ با ۱−، ۲−، ۳−، ... و ۱، ۲، ۳، ... یکی شده، و $\frac{3}{2}$ با $\frac{1}{2}$، $\frac{5}{2}$، $\frac{-1}{2}$، $\frac{-3}{2}$، ... یکی خواهد شد. لذا، هر عدد حقیقی a جفتی مانند $\bar{a}$ دارد که $0 \leq \bar{a} < 1$. پس در $G/\mathbb{Z}$ تمام خط حقیقی به بازهٔ یکهٔ $[0, 1]$ متراکم می‌شود. ولی مطلب کمی بیش از این است زیرا نقاط انتهایی این بازهٔ یکه نیز منطبق شده‌اند. یعنی بازهٔ یکه را خم و دو انتهایش را یکی کرده‌ایم. با این کار چه چیز به‌دست آورده‌ایم؟ البته یک دایره ! لذا، $G/\mathbb{Z}$ به یک معنی که می‌توان آن را دقیق ساخت شبیه یک دایره است، و این دایره یک گروه با ضربی مناسب می‌باشد.

۳. فرض کنیم G گروه اعداد مختلط ناصفر بوده و $N = \{a \in G | \ |a| = 1\}$ که دایره‌ای است به شعاع ۱ و مرکز ۰ در صفحهٔ مختلط. در این صورت N زیرگروهی است از G و نرمال است زیرا G آبلی می‌باشد. با رفتن به G/N حکم می‌کنیم که هر عدد مختلط با قدرمطلق ۱ با عدد حقیقی ۱ یکی است. اما هر $a \in G$ را می‌توان به شکل قطبی $a = r(\cos\theta + i\sin\theta)$ نوشت که در آن $r = |a|$ و $|\cos\theta + i\sin\theta| = 1$. اگر $\cos\theta + i\sin\theta$ را با ۱ یکی کنیم، a با r یکی می‌شود. لذا، با رفتن به G/N، هر عنصر با یک عدد حقیقی مثبت یکی می‌شود، و این انطباق با حاصل‌ضربها در G و در گروه اعداد حقیقی سازگار است زیرا $|ab| = |a|\ |b|$. لذا G/N به معنی واقعی (نه به معنی جناس) گروه اعداد حقیقی مثبت تحت ضرب می‌باشد.

مسائل

۱. اگر G گروه تمام اعداد حقیقی ناصفر تحت ضرب بوده و N زیرگروه تمام اعداد حقیقی مثبت باشد، G/N را با هم‌مجموعه‌های N در G نشان داده و ضرب در G/N را بسازید.

۲. اگر G گروه اعداد حقیقی ناصفر تحت ضرب بوده و $N = \{1, -1\}$، نشان دهید که چطور می‌توان G/N را با گروه تمام اعداد حقیقی مثبت تحت ضرب «یکی کرد». هم‌مجموعه‌های N در G چیستند؟

۳. اگر G گروه بوده و $N \triangleleft G$، نشان دهید هرگاه $\overline{M}$ زیرگروهی از G/N بوده و

$$M = \{a \in G | Na \in \overline{M}\}$$

آن‌گاه M زیرگروهی است از G و $M \supset N$.

۴. اگر در مسئلهٔ ۳ $\overline{M}$ در G/N نرمال باشد، نشان دهید که M تعریف شده در G نرمال می‌باشد.

۵. در مسئلهٔ ۳ نشان دهید که M/N باید با $\overline{M}$ مساوی باشد.

۶. در مثال ۲، $G/\mathbb{Z}$ را دایره گرفتیم که G گروه اعداد حقیقی تحت $+$ و $\mathbb{Z}$ اعداد صحیح بود. به همین ترتیب استدلال کرده و فرض کنید $G = \{(a,b)|$ حقیقی b و $a\}$ که در آن $+$ با $(a,b)+(c,d)=(a+c,b+d)$ تعریف می‌شود (پس G صفحه است) و قرار دهید $N = \{(a,b) \in G|$ صحیح b و $a\}$. نشان دهید که G/N را می‌توان با یک چنبره (نان روغنی) یکی کرد، و در نتیجه می‌توان ضرب برنان روغنی را طوری تعریف کرد که به‌صورت یک گروه در آید. در اینجا یک چنبره را می‌توانید حاصلضرب دکارتی دو دایره تصور کنید.

۷. اگر G یک گروه دوری و N زیرگروهی از آن باشد، نشان دهید که G/N یک گروه دوری است.

۸. اگر G یک گروه آبلی و N زیرگروهی از آن باشد، نشان دهید که G/N یک گروه آبلی است.

۹. مسائل ۷ و ۸ را با توجه به اینکه G/N نقش همریختی G است حل نمایید.

۱۰. فرض کنید G یک گروه آبلی از مرتبهٔ $p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ باشد که در آن p_1، p_2، $\cdots$، p_k اعداد اول متمایزی هستند. نشان دهید که G زیرگروههایی چون S_1، S_2، $\ldots$، S_k به‌ترتیب از مرتبهٔ $p_1^{a_1}$، $p_2^{a_2}$، $\ldots$، $p_k^{a_k}$ دارد. این مطلب، که در واقع برای تمام گروههای متناهی برقرار است، نتیجهٔ مشهوری است در نظریهٔ گروهها که به قضیهٔ سیلو (Sylow) معروف است. ما این قضیه را در بخش ۱۱ ثابت خواهیم کرد.

۱۱. اگر G گروه و $Z(G)$ مرکز آن باشد، نشان دهید هرگاه $G/Z(G)$ دوری باشد، آن‌گاه G آبلی می‌باشد.

۱۲. اگر G یک گروه و $N \triangleleft G$ چنان باشد که G/N آبلی است، ثابت کنید به ازای هر $a,b \in G$، $aba^{-1}b^{-1} \in N$.

۱۳. اگر G گروه و $N \triangleleft G$ چنان باشد که به ازای هر $a,b \in G$،

$$aba^{-1}b^{-1} \in N$$

ثابت کنید G/N آبلی است.

۱۴. اگر G یک گروه آبلی از مرتبهٔ $p_1p_2\cdots p_k$ باشد که در آن p_1، p_2، $\ldots$، p_k اعداد اول متمایزی‌اند، ثابت کنید G دوری است. (ر.ک. مسئلهٔ ۱۵.)

۱۵. اگر G یک گروه آبلی بوده و دارای عنصری از مرتبهٔ m و عنصری از مرتبهٔ n باشد که m و n نسبت به هم اولند، ثابت کنید G عنصری از مرتبهٔ mn دارد.

۱۶. فرض کنید G یک گروه آبلی از مرتبهٔ $p^n m$ باشد که در آن p اول بوده و $p \nmid m$. قرار دهید $P = \{a \in G | a^{p^k} = e$ ،a به ازای kای تابع$\}$. ثابت کنید

الف) P یک زیرگروه G است؛

ب) G/P عنصری از مرتبهٔ p ندارد؛

پ) $|P| = p^n$.

۱۷. فرض کنید G یک گروه آبلی از مرتبهٔ mn باشد که در آن m و n نسبت به هم اولند. قرار دهید $M = \{a \in G | a^m = e\}$ و ثابت کنید

الف) M یک زیرگروه G است؛

ب) G/M عنصری مانند x غیر از عنصر همانی ندارد که عنصر یکهٔ $G/N = x^m$.

۱۸. فرض کنید G یک گروه آبلی (احتمالاً نامتناهی) بوده و

$$T = \{a \in G | a \text{ تابع } m > ۱ \text{ ،} a^m = e\}$$

ثابت کنید

الف) T یک زیرگروه G است؛

ب) G/T عنصری غیر از عنصر همانی از مرتبهٔ متناهی ندارد.

۷. قضایای همریختی

فرض کنیم G و G' گروه و φ یک همریختی از G به روی G' باشد. هرگاه K هستهٔ φ باشد، آن‌گاه K یک زیرگروه نرمال G است. پس می‌توان G/K را تشکیل داد. طبعاً انتظار داریم که رابطهٔ بسیار نزدیکی بین G' و G/K موجود باشد. قضیهٔ اول همریختی، که لحظه‌ای دیگر ثابت می‌شود، این رابطه را با جزئیات دقیق بیان می‌سازد.

لیکن ابتدا به چند مثال از گروههای عاملی در بخش ۶ نگاه می‌کنیم تا شکل صریح رابطهٔ فوق‌الذکر را دریابیم.

۱. فرض کنیم $G = \{T_{a,b} |$ حقیقی b و $a \neq ۰\}$ و G' گروه اعداد حقیقی ناصفر تحت ضرب باشد. از قاعدهٔ ضرب این Tها، یعنی $T_{a,b}T_{c,d} = T_{ac,ad+b}$، معلوم شد که نگاشت $\varphi : G \to G'$ با تعریف $\varphi(T_{a,b}) = a$ یک همریختی از G به روی G' با هستهٔ $K = \{T_{۱,b} |$ حقیقی $b\}$

است. از آن‌سو، در مثال ۱ از بخش ۶ دیدیم که $G/K = \{KT_{a,\circ} | \text{حقیقی} \ a \neq \circ\}$. چون

$$(KT_{a,\circ})(KT_{x,\circ}) = KT_{ax,\circ}$$

به آسانی معلوم می‌شود که نگاشت از G/K به روی G' که هر $KT_{a,\circ}$ را به a می‌فرستد یک یکریختی از G/K به روی G' است. بنابراین $G/K \simeq G'$.

۲. در مثال ۳، G گروه اعداد مختلط ناصفر تحت ضرب و G' گروه اعداد حقیقی مثبت تحت ضرب بود. فرض کنیم $\varphi : G \to G'$ با تعریف $\varphi(a) = |a|$ به ازای $a \in G$ باشد. چون $|ab| = |a||b|$، φ یک همریختی از G به روی G' است (به چه دلیل بروست؟). لذا هستهٔ K از φ درست برابر $K = \{a \in G | \ |a| = ۱\}$ است. ولی قبلاً دیدیم که هرگاه $|a| = ۱$، آن‌گاه a به شکل $\cos\theta + i\sin\theta$ است. لذا قرار می‌دهیم $K = \{\cos\theta + i\sin\theta | \circ \leq \theta < ۲\pi\}$. هرگاه a یک عدد مختلط باشد، آن‌گاه $a = r(\cos\theta + i\sin\theta)$، که در آن $|a| = r$، شکل قطبی a می‌باشد. لذا

$$Ka = Kr(\cos\theta + i\sin\theta) = K(\cos\theta + i\sin\theta)r = Kr$$

زیرا به دلیل $\cos\theta + i\sin\theta \in K$ داریم $K(\cos\theta + i\sin\theta) = K$. در نتیجه همهٔ عناصر G/K که هم‌مجموعه‌های Kaاند به شکل Krاند که در آن $r > \circ$. پس نگاشت G/K به روی G' که Kr را به r می‌فرستد معرف یک یکریختی از G/K به روی G' می‌باشد. پس در اینجا نیز $G/K \simeq G'$.

حال با این تجربهٔ کم می‌توان تمام مطلب یعنی قضیهٔ زیر را نتیجه گرفت.

قضیهٔ ۱.۷.۲ (قضیهٔ اول همریختی). فرض کنیم φ یک همریختی از G به روی G' با هستهٔ K باشد. در این صورت $G' \simeq G/K$ و نگاشت

$$\psi : G/K \longrightarrow G'$$

با تعریف $\psi(Ka) = \varphi(a)$ یک یکریختی بین آنها می‌باشد.

برهان. بهترین راه برای اثبات یکریخت بودن G/K و G' نشان دادن یک یکریختی از G/K به روی G' است. صورت قضیه یک چنین یکریختی را پیشنهاد می‌کند.
لذا $\psi : G/K \to G'$ را با $\psi(Ka) = \varphi(a)$ به ازای $a \in G$ تعریف می‌کنیم. طبق معمول، اولین کار آن است که نشان دهیم ψ تعریف شده است؛ یعنی نشان دهیم هرگاه $Ka = Kb$،

آن‌گاه $\psi(Ka) = \psi(Kb)$. این یعنی هرگاه $Ka = Kb$، آن‌گاه $\varphi(a) = \varphi(b)$. ولی هرگاه $Ka = Kb$، آن‌گاه به ازای $k \in K$ای، $a = kb$. پس $\varphi(a) = \varphi(kb) = \varphi(k)\varphi(b)$. چون (هستهٔ φ) $k \in K$، داریم (عنصر همانی G') $\varphi(k) = e'$؛ در نتیجه داریم $\varphi(a) = \varphi(b)$. این نشان می‌دهد که نگاشت ψ تعریف شده است.

چون φ به روی G' است، به ازای هر $x \in G'$ عنصری مانند $a \in G$ هست که $x = \varphi(a)$. لذا $x = \varphi(a) = \psi(Ka)$. این نشان می‌دهد که ψ گروه G/K را به روی G' می‌نگارد.

می‌پرسیم: آیا ψ یک‌به‌یک است؟ فرض کنیم $\psi(Ka) = \psi(Kb)$. پس

$$\varphi(a) = \psi(Ka) = \psi(Kb) = \varphi(b)$$

لذا $e' = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$. چون ab^{-1} در هستهٔ φ یعنی K است، داریم $ab^{-1} \in K$. این ایجاب می‌کند که $Ka = Kb$. بدین‌ترتیب ψ یک‌به‌یک می‌باشد.

بالاخره آیا ψ یک همریختی از G/K به روی G' است؟ این امر را تحقیق می‌کنیم: با استفاده از همریختی بودن φ و $(Ka)(Kb) = Kab$ داریم

$$\psi((Ka)(Kb)) = \psi(Kab) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(Ka)\psi(Kb)\cdot$$

در نتیجه ψ یک همریختی از G/K به روی G' است و قضیهٔ ۱.۷.۲ به اثبات می‌رسد. ■

صحبت در باب قضیهٔ اول همریختی این فکر را القا می‌کند که باید قضایای دیگری نیز از این نوع داشته باشیم. ما قضیهٔ بعد را طبعاً قضیهٔ دوم همریختی می‌نامیم.

قضیهٔ ۲.۷.۲(قضیهٔ دوم همریختی). فرض کنیم نگاشت $\varphi : G \to G'$ یک همریختی از G به روی G' با هستهٔ K باشد. هرگاه H' زیرگروهی از G' بوده و

$$H = \{a \in G | \varphi(a) \in H'\}$$

آن‌گاه H زیرگروهی است از G، $K \subset H$، و $H/K \simeq H'$. بالاخره هرگاه $H' \lhd G'$، آن‌گاه $H \lhd G$.

برهان. ابتدا تحقیق می‌کنیم که H فوق زیرگروهی است از G. H تهی نیست زیرا $e \in H$. هرگاه $a, b \in H$، آن‌گاه $\varphi(a), \varphi(b) \in H'$. پس $\varphi(ab) = \varphi(a)\varphi(b) \in H'$، زیرا H' زیرگروهی از G' است. این امر ab را در H می‌گذارد. پس H بسته است. به‌علاوه، هرگاه $a \in H$،

آن‌گاه $\varphi(a) \in H'$؛ در نتیجه مجدداً به این دلیل که H' زیرگروه G' است، $\varphi(a^{-1}) = \varphi(a)^{-1}$ در H' است، که از آنجا $a^{-1} \in H$. بنابراین H زیرگروهی از G می‌باشد.

چون $\varphi(K) = \{e'\} \subset H'$ که در آن e' عنصر یکهٔ G' است، داریم $K \subset H$. و چون $K \triangleleft G$ و $K \subset H$، نتیجه می‌شود که $K \triangleleft H$. تحدید نگاشت φ به H یک همریختی از H به روی H' با هستهٔ K تعریف می‌کند. پس، بنابر قضیهٔ اول همریختی، $H/K \simeq H'$.

بالاخره هرگاه $H' \triangleleft G'$ و $a \in G$، آن‌گاه $\varphi(a)^{-1}H'\varphi(a) \subset H'$. پس

$$\varphi(a^{-1})H'\varphi(a) \subset H'$$

این به ما می‌گوید که $\varphi(a^{-1}Ha) \subset H'$. پس $a^{-1}Ha \subset H$ و این نرمال بودن H در G را به ثبوت می‌رساند. ■

بنابر این قضیه، یک تناظر ۱-۱ بین مجموعهٔ تمام زیرگروههای H از G که شامل Kاند و مجموعهٔ تمام زیرگروههای H' از G' وجود دارد. به‌علاوه، این تناظر نرمال بودن را حفظ می‌کند به این معنی که هرگاه H در G نرمال باشد، آن‌گاه H' در G' نرمال می‌باشد.

بالاخره به قضیهٔ سوم همریختی می‌پردازیم که راجع به رابطهٔ بین N و N' وقتی $N' \triangleleft G'$ اطلاعات بیشتری به ما می‌دهد.

قضیهٔ ۳.۷.۲ (قضیهٔ سوم همریختی). هرگاه نگاشت $\varphi : G \to G'$ یک همریختی از G به روی G' با هستهٔ K باشد، آن‌گاه اگر $N' \triangleleft G'$ و $N = \{a \in G | \varphi(a) \in N'\}$، نتیجه می‌شود که $G/N \simeq G'/N'$. به بیان معادل، $G/N \simeq (G/K)/(N/K)$.

برهان. نگاشت $\psi : G \to G'/N'$ را با $\psi(a) = N'\varphi(a)$ به ازای هر $a \in G$ تعریف می‌کنیم. چون φ به روی G' بوده و هر عنصر G'/N' هم‌مجموعه‌ای به شکل $N'x'$ است و به ازای $x \in G$ ی $x' = \varphi(x)$، نگاشت ψ گروه G را به روی G'/N' می‌نگارد.

به‌علاوه ψ یک همریختی از G به روی G'/N' است، زیرا

$$\psi(ab) = N'\varphi(ab) = N'\varphi(a)\varphi(b) = (N'\varphi(a))(N'\varphi(b)) = \psi(a)\psi(b)$$

زیرا $N' \triangleleft G'$. می‌پرسیم: هستهٔ M نگاشت ψ چیست؟ هرگاه $a \in M$، آن‌گاه $\psi(a)$ عنصر یکهٔ G'/N' است؛ یعنی $\psi(a) = N'$. از آن‌سو، طبق تعریف ψ، $\psi(a) = N'\varphi(a)$. چون $N'\varphi(a) = N'$، باید داشته باشیم $\varphi(a) \in N'$. ولی این، طبق تعریف N، a را در N می‌گذارد. لذا $M \subset N$. اثبات $N \subset M$ آسان است و به خواننده محول می‌شود. لذا $M = N$. پس ψ

یک همریختی از G به روی G'/N' با هستهٔ N است که از آنجا، طبق قضیهٔ اول همریختی، $G/N \simeq G'/N'$.

بالاخره، مجدداً طبق قضایای ۱.۷.۲ و ۲.۷.۲، $G' \simeq G/K$ و $N' \simeq N/K$ که ما را به $G/N \simeq G'/N' \simeq (G/K)/(N/K)$ می‌رساند. ■

تساوی اخیر بسیار الهام‌بخش است؛ ما در آن به نوعی K را از صورت و مخرج حذف می‌کنیم.

البته قضایای همریختی دیگری نیز وجود دارند. یکی از آنها که کلاسیک و مهم است در مسئلهٔ ۵ خواهد آمد.

مسائل

۱. در برهان قضیهٔ ۳.۷.۲ نشان دهید که $N \subset M$.

۲. فرض کنید G گروه تمام توابع حقیقی بر بازهٔ یکهٔ $[۰,۱]$ باشد که در آن جمع هر $f, g \in G$ با $(f+g)(x) = f(x) + g(x)$ به ازای هر $x \in [۰,۱]$ تعریف می‌شود. اگر

$$N = \{f \in G | f(\tfrac{1}{4}) = ۰\}$$

ثابت کنید مجموعهٔ اعداد حقیقی تحت $+ \simeq G/N$.

۳. فرض کنید G گروه اعداد حقیقی ناصفر تحت ضرب بوده و $N = \{۱, -۱\}$. ثابت کنید مجموعهٔ اعداد حقیقی مثبت تحت ضرب $\simeq G/N$.

۴. فرض کنید G_1 و G_2 دو گروه بوده و $G = G_1 \times G_2 = \{(a,b) | a \in G_1, b \in G_2\}$ که در آن تعریف می‌کنیم $(a,b)(c,d) = (ac, bd)$. نشان دهید

الف) $N = \{(a, e_2) | a \in G_1\}$، که در آن e_2 عنصر یکهٔ G_2 است، زیرگروه نرمال G می‌باشد؛

ب) $N \simeq G_1$؛

پ) $G/N \simeq G_2$.

۵. فرض کنید G یک گروه و H زیرگروهی از G بوده و نیز $N \triangleleft G$. همچنین

$$HN = \{hn | h \in H, n \in N\}$$

ثابت کنید.

الف) $H \cap N \triangleleft H$؛

ب) HN زیرگروه G است؛

پ) $N \subset HN$ و $N \triangleleft HN$؛

ت) $(HN)/N \simeq H/(H \cap N)$.

۶. فرض کنید G یک گروه بوده و $N \triangleleft G$. نشان دهید هرگاه $a \in G$ از مرتبهٔ متناهی $o(a)$ باشد، آن‌گاه Na در G/N از مرتبهٔ متناهی m است که $m|o(a)$. (این مطب را با استفاده از همریختی G به روی G/N ثابت کنید.)

۷. اگر φ یک همریختی از G به روی G' بوده و $N \triangleleft G$، نشان دهید که $\varphi(N) \triangleleft G'$.

۸. قضیهٔ کشی

در قضیهٔ ۲.۶.۴ (قضیهٔ کشی) ثابت شد که هرگاه عدد اول p مرتبهٔ گروه آبلی متناهی G را عاد کند، آن‌گاه G عنصری از مرتبهٔ p دارد. در آنجا خاطرنشان شد که قضیهٔ کشی حتی اگر گروه آبلی نباشد نیز درست است. حال اثبات بسیار زیبایی از آن را عرضه می‌کنیم. این برهان به مک‌کی (McKay) منسوب است.

ابتدا لحظه‌ای به نظریهٔ مجموعه‌ها بازگشته و آنچه راکه در مسائل بخش ۴ گفته‌ایم انجام می‌دهیم.

فرض کنیم S یک مجموعه بوده و $f \in A(S)$. بر S یک رابطه به‌صورت زیر تعریف می‌کنیم: $s \sim t$ اگر به ازای عدد صحیحی چون i، $t = f^i(s)$ (i می‌تواند مثبت، منفی، یا صفر باشد). برخواننده است تحقیق کند که این یک رابطهٔ هم‌ارزی بر S است. ردهٔ هم‌ارزی s، یعنی $[s]$، مدار s تحت f نام دارد. لذا S اجتماع از هم جدای مدارهای عناصرش می‌باشد.

وقتی f از مرتبهٔ عدد اول p باشد، می‌توان راجع به اندازهٔ مدارهای تحت f سخن گفت؛ خواننده‌ای که مسئلهٔ ۳۴ از بخش ۴ را حل کرده نتیجه را می‌داند. ما در اینجا برای آنکه آن را داشته باشیم ثابت می‌کنیم.

[البته اگر $f^k(s) = s$، به ازای هر عدد صحیح t، $f^{tk}(s) = s$. (ثابت کنید!)].

لم ۲.۸.۱. هرگاه $f \in A(S)$ از مرتبهٔ عدد اول p باشد، آن‌گاه مدار هر عنصر s تحت f دارای ۱ یا p عنصر می‌باشد.

برهان. فرض کنیم $s \in S$. هرگاه $f(s) = s$، آن‌گاه مدار s تحت f فقط از s تشکیل شده است. پس مدار دارای یک عنصر است. فرض کنیم $f(s) \neq s$. عنصرهای s، $f(s)$، $f^2(s)$، $\ldots$، $f^{p-1}(s)$ را در نظر می‌گیریم. حکم می‌کنیم که این p عنصر از هم متمایز بوده و مدار s تحت

f را می‌سازند. در غیر این صورت به ازای اعداد صحیحی چون $0 \le i < j \le p-1$ داریم $f^i(s) = f^j(s)$ ایجابگر آنکه $f^{j-i}(s) = s$. قرار می‌دهیم $m = j - i$. پس $0 < m \le p-1$ و $f^m(s) = s$. ولی $f^p(s) = s$ و چون $p \nmid m$، به ازای اعداد صحیحی چون a و b، $ap + bm = 1$. لذا $f^1(s) = f^{ap+bm}(s) = f^{ap}(f^{bm}(s)) = f^{ap}(s) = s$، زیرا $f^m(s) = f^p(s) = s$. این امر با $f(s) \neq s$ در تضاد است. پس مدار s تحت f از s، $f(s)$، $f^2(s)$، $\cdots$، $f^{p-1}(s)$ تشکیل شده است. لذا دارای p عنصر می‌باشد. ■

حال برهان مک‌کی از قضیهٔ کشی را ارائه می‌دهیم.

قضیهٔ ۲.۸.۲ (کشی). هرگاه عدد اول p مرتبهٔ G را عاد کند، آن‌گاه G عنصری از مرتبهٔ p دارد.

برهان. اگر $p = 2$، قضیه همان مسئلهٔ ۱۸ در بخش ۱ است. پس فرض کنیم $p \neq 2$. همچنین S مجموعهٔ تمام p تاییهای مرتب $(a_1, a_2, \ldots, a_{p-1}, a_p)$ باشد که در آن a_1، $\ldots$، a_p در G بوده و $a_1 a_2 \cdots a_{p-1} a_p = e$. حکم می‌کنیم که S دارای n^{p-1} عنصر است که $n = |G|$. چرا؟ می‌توان a_1، $\cdots$، a_{p-1} را در G دلخواه گرفته و قرار داد $a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$. در این صورت p تایی $(a_1, a_2, \ldots, a_{p-1}, a_p)$ در رابطهٔ زیر صدق می‌کند:

$$a_1 a_2 \cdots a_{p-1} a_p = a_1 a_2 \cdots a_{p-1} (a_1 a_2 \cdots a_{p-1})^{-1} = e$$

پس این حاصلضرب در S می‌باشد. لذا S دارای n^{p-1} عنصر می‌باشد.

توجه کنید که هرگاه $a_1 a_2 \cdots a_{p-1} a_p = e$، آن‌گاه $a_p a_1 a_2 \cdots a_{p-1} = e$ (چرا که اگر در یک گروه $xy = e$، داریم $yx = e$). پس نگاشت $f : S \to S$ با تعریف

$$f(a_1, \cdots, a_p) = (a_p, a_1, a_2, \cdots, a_{p-1})$$

در $A(S)$ است. توجه کنید که $f \neq i$ (نگاشت همانی بر S) و $f^p = i$. پس f از مرتبهٔ p می‌باشد.

هرگاه مدار s تحت f دارای یک عنصر باشد، آن‌گاه $f(s) = s$. از آن‌سو، اگر $f(s) \neq s$، حکم می‌کنیم که مدار s تحت f درست از p عنصر متمایز تشکیل شده است. این امر از لم ۱.۸.۲ نتیجه می‌شود. می‌پرسیم: چه وقت $f(s) \neq s$؟ حکم می‌کنیم که $f(s) \neq s$ اگر و فقط اگر وقتی $s = (a_1, a_2, \ldots, a_p)$، به ازای $i \neq j$ای، $a_i \neq a_j$. (اثبات این امر به خواننده محول می‌شود.) لذا $f(s) = s$ اگر و فقط اگر به ازای $a \in G$ای، $s = (a, a, \ldots, a)$.

فرض کنیم m تعداد $s \in S$هایی باشد که $f(s) = s$. چون به ازای $s = (e, e, \ldots, e)$، $f(s) = s$، پس داریم $m \geq 1$. از آن‌سو، اگر $f(s) \neq s$، مدار s از p عنصر تشکیل شده است و این مدارها به دلیل ردهٔ هم‌ارزی بودن از هم جدا می‌باشند. اگر این مدارها k تا باشند که $f(s) \neq s$، داریم $n^{p-1} = m + kp$ زیرا این امر برای هر عنصر S قابل بیان است.
ولی طبق فرض $p|n$ و $p|(kp)$. پس باید داشته باشیم $p|m$ زیرا $m = n^{p-1} - kp$. چون $m \neq 0$ و $p|m$، داریم $m > 1$. ولی این امر می‌گوید که یک

$$s = (a, a, \ldots, a) \neq (e, e, \ldots, e)$$

در S وجود دارد. این از تعریف S نتیجه می‌دهد که $a^p = e$. چون $a \neq e$، a عنصر مطلوب از مرتبهٔ p می‌باشد. ■

توجه کنید که این برهان به ما می‌گوید که تعداد جوابهای $x^p = e$ در G مضرب مثبتی از p می‌باشد.

از خواننده‌ای که برهان فوق را راحت نمی‌بیند قویاً می‌خواهیم که جزئیاتش را به ازای $p = 3$ تکرار کند. در این حالت عمل f بر S روشن بوده و احکام ما راجع به این عمل را می‌توان صریحاً امتحان کرد.

قضیهٔ کشی نتایج بسیار دارد. ما به‌زودی یکی از آنها را ارائه می‌دهیم که در آن ماهیت بعضی از گروهها از مرتبهٔ pq که p و q اعداد اول متمایزی‌اند کاملاً معین می‌شود. سایر نتایج را می‌توان در مجموعه مسائل زیر و مطالب بعدی راجع به گروهها یافت.

لم ۳.۸.۲. فرض کنیم G گروهی از مرتبهٔ pq باشد که در آن p و q اول بوده و $p > q$. هرگاه $a \in G$ از مرتبهٔ p و A زیرگروه G تولید شده به‌وسیلهٔ a باشد، آن‌گاه $A \triangleleft G$.

برهان. حکم می‌کنیم که A تنها زیرگروه G از مرتبهٔ p است. زیرا فرض کنیم B زیرگروه دیگری از مرتبهٔ p باشد. مجموعهٔ $AB = \{xy | x \in A، y \in B\}$ را در نظر می‌گیریم. حکم می‌کنیم که AB دارای p^2 عنصر متمایز است. زیرا فرض کنیم $xy = uv$ که در آن $x, u \in A$ و $y, v \in B$. پس $u^{-1}x = vy^{-1}$. ولی $u^{-1}x \in A$ و $vy^{-1} \in B$، و چون $u^{-1}x = vy^{-1}$، داریم $u^{-1}x \in A \cap B$. چون $B \neq A$ و $A \cap B$ زیرگروهی از A از مرتبهٔ اول است، نتیجه می‌شود که $A \cap B = (e)$؛ و لذا $u^{-1}x = e$؛ یعنی $u = x$. به همین نحو $v = y$. پس تعداد عناصر متمایز AB مساوی p^2 است. ولی همهٔ این عناصر در G اند که فقط $pq < p^2$ عنصر

دارد (زیرا $p > q$). با این تناقض معلوم می‌شود که $A = B$ و تنها زیرگروه از مرتبهٔ p در G است. ولی اگر $x \in G$، $B = x^{-1}Ax$ زیرگروهی از G از مرتبهٔ p است؛ در نتیجه $x^{-1}Ax = A$. بنابراین $A \lhd G$. ■

نتیجه. هرگاه G و a همانند لم ۳.۸.۲ بوده و $x \in G$، آن‌گاه $x^{-1}ax = a^i$ که در آن به ازای iی (وابسته به x) $0 < i < p$.

برهان. چون $e \neq a \in A$ و $x^{-1}Ax = A$، داریم $x^{-1}ax \in A$. ولی هر عنصر A به شکل a^i، $0 \leq i < p$، است و $x^{-1}ax \neq e$. در نتیجه $x^{-1}ax = a^i$ که در آن $0 < i < p$. ■

حال قضیه‌ای با رنگ و بوی متفاوت ثابت می‌کنیم.

لم ۴.۸.۲. فرض کنیم $a \in G$ از مرتبهٔ m و $b \in G$ از مرتبهٔ n باشد که در آن m و n نسبت به هم اولند. در این صورت، اگر $ab = ba$، $c = ab$ از مرتبهٔ mn می‌باشد.

برهان. فرض کنیم A زیرگروه تولید شده به‌وسیلهٔ a و B زیرگروه تولید شده به‌وسیلهٔ b باشد. چون $|A| = m$ و $|B| = n$ و $(m, n) = 1$، داریم $A \cap B = (e)$ زیرا طبق قضیهٔ لاگرانژ $|A \cap B| \,|n$ و $|A \cap B| \,|m$.

فرض کنیم $c^i = e$ که در آن $i > 0$. لذا $(ab)^i = e$. چون $ab = ba$، پس

$$e = (ab)^i = a^i b^i$$

این به ما می‌گوید که $a^i = b^{-i} \in A \cap B = (e)$. در نتیجه $a^i = e$ که از آنجا $m|i$، و $b^i = e$ که از آنجا $n|i$. چون $(m, n) = 1$ و m و n هر دو i را عاد می‌کنند، پس mn عدد i را عاد می‌نماید. لذا $i \geq mn$. و چون $(ab)^{mn} = a^{mn}b^{mn} = e$، معلوم می‌شود که mn کوچکترین عدد صحیح مثبت i است که $(ab)^i = e$. این امر می‌گوید که ab طبق حکم از مرتبهٔ mn می‌باشد. ■

پیش از توجه به حالت کلی‌تر گروهها از مرتبهٔ pq به حالت خاص گروه G از مرتبهٔ ۱۵ نگاه می‌کنیم. بنابر قضیهٔ کشی، G عنصری مانند b از مرتبهٔ ۳ و عنصری مانند a از مرتبهٔ ۵ دارد. بنابر نتیجهٔ لم ۳.۸.۲، $b^{-1}ab = a^i$ که در آن $0 < i < 5$. لذا

$$b^{-2}ab^2 = b^{-1}(b^{-1}ab)b = b^{-1}a^ib = (b^{-1}ab)^i = (a^i)^i = a^{i^2}$$

و به همین نحو $b^{-3}ab^3 = a^{i^3}$. ولی $b^3 = e$. پس داریم $a = a^{i^3}$ که از آنجا $a^{i^3-1} = e$. چون a از مرتبهٔ ۵ است، پس ۵ باید $i^3 - 1$ را عاد کند؛ یعنی $i^3 \equiv 1(5)$. ولی، طبق قضیهٔ فرما (نتیجهٔ قضیهٔ ۲.۴.۸)، $i^4 \equiv 1(5)$. این دو معادله نسبت به i به ما می‌گویند که $i \equiv 1(5)$. لذا، چون $0 < i < 5$، $i = 1$. به‌طور خلاصه $b^{-1}ab = a^i = a$ که به معنی $ab = ba$ است.
چون a از مرتبهٔ ۵ و b از مرتبهٔ ۳ است، بنا بر لم ۲.۸.۴، $c = ab$ از مرتبهٔ ۱۵ است. این یعنی ۱۵ توان $e = c^0, c, c^2, \ldots, c^{14}$ متمایزند. لذا باید تمام G را جارو کنند. در یک کلمه، G باید دوری باشد.

استدلال فوق در مورد ۱۵ را می‌توان کوتاهتر کرد ولی شکل آن نمونهٔ واقعی برهان در حالت کلی زیر می‌باشد.

قضیهٔ ۲.۸.۵. فرض کنیم G گروهی از مرتبهٔ pq باشد که در آن p و q اول بوده و $p > q$. در این صورت، اگر $q \nmid p - 1$، G باید دوری باشد.

برهان. بنا بر قضیهٔ کشی، G عنصری مانند a از مرتبهٔ p و عنصری مانند b از مرتبهٔ q دارد. و بنابر نتیجهٔ لم ۲.۸.۳، به ازای i ای که $0 < i < p$، $b^{-1}ab = a^i$. لذا، به ازای هر $r \geq 0$، $b^{-r}ab^r = a^{i^r}$ (ثابت کنید!)؛ و در نتیجه $b^{-q}ab^q = a^{i^q}$. ولی $b^q = e$. لذا $a^{i^q} = a$؛ و در نتیجه $a^{i^q-1} = e$. چون a از مرتبهٔ p است، نتیجه می‌شود که $p | i^q - 1$ که به معنی $i^q \equiv 1(p)$ است. ولی، طبق قضیهٔ فرما، $i^{p-1} \equiv 1(p)$. چون $q \nmid p - 1$، نتیجه می‌گیریم که $i \equiv 1(p)$، و چون $0 < i < p$، نتیجه می‌شود که $i = 1$. لذا $b^{-1}ab = a^i = a$. پس $ab = ba$ و، بنابر لم ۲.۸.۴، $c = ab$ از مرتبهٔ pq است. لذا توانهای c تمام G را جارو می‌کنند. بنابراین G دوری بوده و قضیه به اثبات می‌رسد. ■

مسائل

مسائل با سطح متوسط

۱. در برهان قضیهٔ ۲.۸.۲ نشان دهید هرگاه دو درایهٔ $s = (a_1, a_2, \ldots, a_p)$ متفاوت باشند، آن‌گاه $s \neq f(s)$ و مدار s تحت f دارای p عنصر می‌باشد.

۲. ثابت کنید هر گروه از مرتبهٔ ۳۵ دوری است.

۳. با استفاده از مسئلهٔ ۴۰ در بخش ۵، برهان دیگری از لم ۲.۸.۳ ارائه دهید (راهنمایی. به‌جای H یک زیرگروه از مرتبهٔ p به‌کار برید.)

۴. یک گروه غیرآبلی از مرتبهٔ ۲۱ بسازید. (راهنمایی. فرض کنید $a^3 = e$، $b^7 = e$، و i را طوری بیابید که $a^{-1}ba = a^i \neq a$، که با روابط $a^3 = b^7 = e$ سازگار است.)

۵. فرض کنید G گروهی از مرتبهٔ $p^n m$ باشد که در آن p اول بوده و $p \nmid m$. همچنین G زیرگروه نرمالی مانند P از مرتبهٔ p^n داشته باشد. ثابت کنید به ازای هر خودریختی θ از G، $\theta(P) = P$.

۶. فرض کنید G یک گروه متناهی بوده و زیرگروههای A و B از G چنان باشند که $|A| > \sqrt{|G|}$ و $|B| > \sqrt{|G|}$. ثابت کنید $A \cap B \neq (e)$.

۷. اگر G یک گروه و A و B گروههایی از مرتبهٔ m و n باشند که m و n نسبت به هم اولند، ثابت کنید زیرمجموعهٔ $AB = \{ab | b \in B، a \in A\}$ از G دارای mn عنصر متمایز می‌باشد.

۸. ثابت کنید هر گروه از مرتبهٔ ۹۹ زیرگروه نرمال غیربدیهی دارد.

۹. ثابت کنید هر گروه از مرتبهٔ ۴۲ زیرگروه نرمال غیربدیهی دارد.

۱۰. با استفاده از مسئلهٔ ۹ ثابت کنید هر گروه از مرتبهٔ ۴۲ زیرگروه نرمالی از مرتبهٔ ۲۱ دارد.

مسائل مشکلتر

۱۱. اگر G یک گروه و A و B زیرگروههایی متناهی از آن باشند، ثابت کنید مجموعهٔ

$$AB = \{ab | b \in B، a \in A\}$$

دارای $(|A||B|)/|A \cap B|$ عنصر متمایز است.

۱۲. ثابت کنید هر دو گروه غیرآبلی از مرتبهٔ ۲۱ یکریختند. (ر.ک. مسئلهٔ ۴.)

مسائل بسیارمشکل

۱۳. با استفاده از آبلی بودن هر گروه از مرتبهٔ ۹، ثابت کنید هر گروه از مرتبهٔ ۹۹ آبلی است.

۱۴. فرض کنید دو عدد اول $p > q$ چنان باشند که $q | p - 1$. ثابت کنید یک گروه غیرآبلی از مرتبهٔ pq وجود دارد. (راهنمایی. از مسئلهٔ ۴۰ در بخش ۴، یعنی دوری بودن U_p به ازای p اول، و ایدهٔ اثبات مسئلهٔ ۴ فوق استفاده کنید.)

۱۵. ثابت کنید هرگاه دو عدد اول $p > q$ چنان باشند که $q | p - 1$، آن‌گاه هر دو گروه غیرآبلی از مرتبهٔ pq یکریختند.

۹. ضربهای مستقیم

در چند مثال و مسئلهٔ پیش ساختمان زیر را به پا ساختیم: هرگاه $G_۱$ و $G_۲$ دو گروه باشند، آن‌گاه $G = G_۱ \times G_۲$ مجموعهٔ تمام جفتهای مرتب (a,b) است که $a \in G_۱$ و $b \in G_۲$ و ضرب مؤلفه به مؤلفه به‌وسیلهٔ $(a_۱, b_۱)(a_۲, b_۲) = (a_۱a_۲, b_۱b_۲)$ تعریف می‌شود که ضرب در هر مؤلفه درگروه مربوطهٔ $G_۱$ یا $G_۲$ صورت می‌گیرد. حال می‌خواهیم این امر را به‌طور صوری بیان کنیم.

تعریف. هرگاه $G_۱$، $G_۲$، ...، G_n، n گروه باشند، آن‌گاه حاصلضرب مستقیم (خارجی) $G_۱ \times G_۲ \times G_۳ \times \cdots \times G_n$ مجموعهٔ تمام n تاییهای مرتب $(a_۱, a_۲, \ldots, a_n)$ است که در آن به ازای $i = ۱, ۲, \ldots, n$، $a_i \in G_i$ و ضرب در $G_۱ \times G_۲ \times \cdots \times G_n$ مؤلفه به مؤلفه تعریف می‌شود؛ یعنی

$$(a_۱, a_۲, \ldots, a_n)(b_۱, b_۲, \ldots, b_n) = (a_۱b_۱, a_۲b_۲, \ldots, a_nb_n)$$

گروه بودن $G = G_۱ \times G_۲ \times \cdots \times G_n$ فوراً نتیجه می‌شود که درآن $(e_۱, e_۲, \ldots, e_n)$ عنصر یکه است که e_i عنصر یکهٔ G_i می‌باشد و

$$(a_۱, a_۲, \ldots, a_n)^{-۱} = (a_۱^{-۱}, a_۲^{-۱}, \ldots, a_n^{-۱})$$

G صرفاً حاصلضرب دکارتی گروههای $G_۱$، $G_۲$، ...، G_n است که در آن ضرب مؤلفه به مؤلفه صورت می‌گیرد. ما این ضرب را از آن‌رو خارجی می‌نامیم که گروههای $G_۱$، $G_۲$، ...، G_n دلخواه بوده و بینشان لزوماً رابطه‌ای برقرار نیست.

حال زیرمجموعه‌های $G = G_۱ \times G_۲ \times \cdots \times G_n \supset \bar{G}_i$ را در نظر می‌گیریم که

$$\bar{G}_i = \{(e_۱, \ldots, e_{i-۱}, a_i, e_{i+۱}, \ldots, e_n) | a_i \in G_i\}$$

به عبارت دیگر، $\bar{G}_i$ از تمام n تاییهایی تشکیل شده است که هر عنصر G_i می‌تواند در مؤلفهٔ iام بیاید و سایر مؤلفه‌ها عنصر همانی می‌باشند. واضح است که گروه $\bar{G}_i$ با G_i به‌وسیلهٔ یکریختی $\Pi_i : \bar{G}_i \to G_i$ با تعریف $\Pi_i(e_۱, e_۲, \ldots, a_i, \ldots, e_n) = a_i$ یکریخت است. به‌علاوه نه فقط $\bar{G}_i$ زیرگروه G است بلکه $\bar{G}_i \lhd G$. (ثابت کنید!)

به ازای هر عنصر $a = (a_۱, a_۲, \ldots, a_n) \in G$ داریم

$$a = (a_۱, e_۲, \ldots, e_n)(e_۱, a_۲, e_۳, \ldots, e_n) \cdots (e_۱, e_۲, \ldots, e_{n-۱}, a_n)$$

یعنی هر $a \in G$ را می‌توان به‌صورت $a = \bar{a}_1\bar{a}_2\cdots\bar{a}_n$ نوشت که در آن هر $\bar{a}_i \in \bar{G}_i$. به‌علاوه a را می‌توان به‌طور منحصر به فرد به این شکل نوشت؛ یعنی هرگاه $a = \bar{a}_1\bar{a}_2\cdots\bar{a}_n = \bar{b}_1\bar{b}_2\cdots\bar{b}_n$ که در آن $\bar{a}_i \in \bar{G}_i$ و $\bar{b}_i \in \bar{G}_i$، آن‌گاه $\bar{a}_1 = \bar{b}_1$، $\ldots$، $\bar{a}_n = \bar{b}_n$. لذا G از زیرگروههای نرمال $\bar{G}_i$ به‌صورت $G = \bar{G}_1\bar{G}_2\cdots\bar{G}_n$ و به نحوی ساخته شده که هر عنصر $a \in G$ نمایش منحصربه‌فردی به شکل $a = \bar{a}_1\bar{a}_2\cdots\bar{a}_n$ دارد که $\bar{a}_i \in \bar{G}_i$.

این امر انگیزه‌ای است برای تعریف زیر.

تعریف. گوییم گروه G حاصلضرب مستقیم (داخلی) زیرگروههای نرمال N_1، N_2، $\ldots$، N_n خود است اگر هر $a \in G$ نمایش منحصر به‌فردی به شکل $a = a_1a_2\cdots a_n$ داشته باشد که در آن به ازای $i = 1, 2, \ldots, n$، $a_i \in N_i$.

از بحث فوق لم زیر را خواهیم داشت.

لم ۱.۹.۲. هرگاه $G = G_1 \times G_2 \times \cdots \times G_n$ حاصلضرب مستقیم خارجی G_1، G_2، $\ldots$، G_n باشد، آن‌گاه G حاصلضرب مستقیم داخلی زیرگروههای نرمال $\bar{G}_1$، $\bar{G}_2$، $\ldots$، $\bar{G}_n$ تعریف شده در فوق می‌باشد.

حال به سویی دیگر رفته و ثابت می‌کنیم هرگاه G حاصلضرب مستقیم داخلی زیرگروههای نرمال N_1، N_2، $\ldots$، N_n خود باشد، آن‌گاه G با $N_1 \times N_2 \times \cdots \times N_n$ یکریخت است. برای این کار، ابتدا چند نتیجهٔ مقدماتی به‌دست می‌آوریم.

نتیجه‌ای که اینک به‌دست می‌آوریم قبلاً در مسئلهٔ ۲۰ از بخش ۵ آمده است. ما آن را برای کامل بودن بحث ثابت می‌کنیم.

لم ۲.۹.۲. فرض کنیم G یک گروه بوده و M و N زیرگروههای نرمالی از G باشند به‌طوری که $M \cap N = (e)$. در این‌صورت به ازای $m \in M$ و $n \in N$ داریم $mn = nm$.

برهان. عنصر $a = mnm^{-1}n^{-1}$ را در نظر می‌گیریم. a را به‌صورت $a = (mnm^{-1})n^{-1}$ می‌نویسیم. چون $N \lhd G$ و $n \in N$، داریم $mnm^{-1} \in N$؛ در نتیجه $a = (mnm^{-1})n^{-1}$ نیز در N است. حال a را به‌صورت $a = m(nm^{-1}n^{-1})$ در نظر می‌گیریم. چون $M \lhd G$ و $m^{-1} \in M$، داریم $nm^{-1}n^{-1} \in M$؛ و در نتیجه $a = m(nm^{-1}n^{-1}) \in M$. لذا $a \in M \cap N = (e)$ که به معنی $mnm^{-1}n^{-1} = e$ می‌باشد. از این داریم $mn = nm$ که

همان مطلوب ما می‌باشد. ■

اگر G حاصلضرب مستقیم داخلی زیرگروههای نرمال N_1، N_2، $\cdots$، N_n باشد، حکم می‌کنیم که به ازای $i \neq j$، $N_i \cap N_j = (e)$. زیرا فرض کنیم $a \in N_i \cap N_j$. پس $a = ee \cdots eae \cdots e$ که در آن a در موضع iام ظاهر شده است. این یک نمایش برای a در $G = N_1 N_2 \cdots N_n$ به‌دست می‌دهد. از آن‌سو، $a = ee \cdots eae \cdots e$ که در آن a در موضع jام آمده است. پس a نمایش دومی به‌صورت عنصری از $N_1 N_2 \cdots N_n$ خواهد داشت. بنابر یکتایی نمایش، $a = e$؛ و در نتیجه $N_i \cap N_j = (e)$.

شاید اگر بحث برای $n = 2$ مطرح شود مطالب واضح‌تر شوند. لذا فرض می‌کنیم $N_1 \triangleleft G$ و $N_2 \triangleleft G$ و هر عنصر $a \in G$ نمایش منحصر به‌فردی مانند $a = a_1 a_2$ داشته باشد که در آن $a_1 \in N_1$ و $a_2 \in N_2$. همچنین $a \in N_1 \cap N_2$. پس $a = a \cdot e$ نمایشی از $a = a_1 a_2$ است که در آن $a_1 = a \in N_1$ و $a_2 = e \in N_2$. ولی $a = ea$؛ در نتیجه $a = b_1 b_2$ که در آن $b_1 = e \in N_1$ و $b_2 = a \in N_2$. بنابر یکتایی نمایش باید داشته باشیم $a_1 = b_1$؛ یعنی $a = e$. لذا $N_1 \cap N_2 = (e)$.

استدلال فوق در مورد N_1، $\cdots$، N_n همان استدلال مربوط به $n = 2$ است ولی احتمالاً کمتر واضح. به‌هر حال لم زیر را ثابت کرده‌ایم.

لم ۳.۹.۲. هرگاه G حاصلضرب مستقیم داخلی زیرگروههای نرمال N_1، N_2، $\cdots$، N_n خود باشد، آن‌گاه به ازای هر $i \neq j$، $N_i \cap N_j = (e)$.

نتیجه. هرگاه G همانند لم ۳.۹.۲ باشد، آن‌گاه به ازای هر $a_i \in N_i$ و $a_j \in N_j$ که $i \neq j$، خواهیم داشت $a_i a_j = a_j a_i$.

برهان. بنابر لم ۳.۹.۲، به ازای هر $i \neq j$ داریم $N_i \cap N_j = (e)$. چون Nها در G نرمال‌اند، بنابر لم ۲.۹.۲ هر عنصر در N_i با هر عنصر در N_j تعویض می‌شود؛ یعنی به ازای هر $a_i \in N_i$ و $a_j \in N_j$ که $i \neq j$، $a_i a_j = a_j a_i$. ■

حال با این مقدمات می‌توان قضیهٔ زیر را اثبات کرد.

قضیهٔ ۴.۹.۲. هرگاه G حاصلضرب مستقیم داخلی زیرگروههای نرمال N_1، N_2، $\cdots$، N_n خود باشد، آن‌گاه G با $N_1 \times N_2 \times \cdots \times N_n$، یعنی حاصلضرب مستقیم خارجی N_1، N_2، $\cdots$، N_n، یکریخت است.

برهان. نگاشت ψ از $N_1 \times N_2 \times \cdots \times N_n$ به G را با

$$\psi((a_1, a_2, \ldots, a_n)) = a_1 a_2 \cdots a_n$$

تعریف می‌کنیم. چون هر عنصر a در G نمایشی به‌صورت $a = a_1 a_2 \cdots a_n$ دارد که در آن $a_i \in N_i$، نگاشت ψ برو می‌باشد. حکم می‌کنیم که این نگاشت ۱-۱ نیز هست، چرا که اگر $\psi((a_1, a_2, \ldots, a_n)) = \psi((b_1, b_2, \ldots, b_n))$، از تعریف ψ داریم

$$a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_n$$

و از یکتایی نمایش هر عنصر به این شکل خواهیم داشت $a_1 = b_1$، $a_2 = b_2$، $\ldots$، $a_n = b_n$. بنابراین ψ یک‌به‌یک می‌باشد.

تنها باقی است نشان دهیم که ψ یک همریختی است. لذا فرض می‌کنیم

$$\begin{aligned}\psi((a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)) &= \psi((a_1 b_1, a_2 b_2, \ldots, a_n b_n)) \\ &= (a_1 b_1)(a_2 b_2) \cdots (a_n b_n) \\ &= a_1 b_1 a_2 b_2 \cdots a_n b_n\end{aligned}$$

چون $b_1 \in N_1$، این عنصر طبق نتیجهٔ لم ۳.۹.۲ با هر a_i و b_i به ازای $i > 1$ تعویض می‌شود. پس می‌توان b_1 را به منتهی‌الیه راست کشانید و به‌دست آورد

$$a_1 b_1 a_2 b_2 \cdots a_n b_n = a_1 a_2 b_2 a_3 b_3 \cdots a_n b_n b_1$$

حال این روند را با b_2 و غیره تکرار کرده و به‌دست می‌آوریم

$$a_1 b_1 a_2 b_2 \cdots a_n b_n = (a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_n)$$

لذا

$$\begin{aligned}\psi((a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)) &= a_1 b_1 a_2 b_2 \cdots a_n b_n \\ &= (a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_n) \\ &= \psi((a_1, a_2, \ldots, a_n))\psi((b_1, b_2, \ldots, b_n))\end{aligned}$$

به عبارت دیگر، ψ یک همریختی می‌باشد.

با این امر برهان قضیهٔ ۴.۹.۲ به اتمام می‌رسد. ■

در پرتو قضیهٔ ۴.۹.۲ می‌توان صفت «داخلی» و «خارجی» را حذف کرده و راجع به «ضرب مستقیم» سخن گفت.

هدف اغلب نشان دادن این امر است که یک گروه حاصلضرب مستقیم زیرگروههایی نرمال می‌باشد. با این کار می‌توان ساختار گروه را در صورت دانستن آن زیرگروههای نرمال به‌طور کامل تعیین کرد.

مسائل

۱. اگر G_1 و G_2 گروه باشند، ثابت کنید $G_1 \times G_2 \simeq G_2 \times G_1$.

۲. اگر G_1 و G_2 گروههایی دوری از مرتبهٔ m و n باشند، ثابت کنید $G_1 \times G_2$ دوری است اگر و فقط اگر m و n نسبت به هم اول باشند.

۳. فرض کنید G یک گروه بوده و $A = G \times G$. در A قرار دهید $T = \{(g,g) | g \in G\}$ و ثابت کنید

الف) $T \simeq G$؛

ب) $T \triangleleft A$ اگر و فقط اگر G آبلی باشد.

۴. فرض کنید G یک گروه آبلی از مرتبهٔ $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ باشد که در آن اعداد اول p_1، p_2، $\cdots$، p_k متمایز بوده و $m_1 > 0$، $m_2 > 0$، $\cdots$، $m_k > 0$. بنابر مسئلهٔ ۱۰ از بخش ۶، G به ازای هر i زیرگروهی چون P_i از مرتبهٔ $p_i^{m_i}$ دارد. نشان دهید که $G \simeq P_1 \times P_2 \times \cdots \times P_k$.

۵. فرض کنید G یک گروه متناهی و N_1، N_2، $\cdots$، N_k زیرگروههای نرمالی از آن باشند به‌طوری که $G = N_1 N_2 \cdots N_k$ و $|G| = |N_1||N_2| \cdots |N_k|$. ثابت کنید G حاصلضرب مستقیم N_1، N_2، $\cdots$، N_k می‌باشد.

۶. فرض کنید G یک گروه و N_1، N_2، $\cdots$، N_k زیرگروههای نرمالی از آن باشند به‌طوری که

۱. $G = N_1 N_2 \cdots N_k$؛

۲. به ازای هر i، $N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_k) = (e)$.

ثابت کنید G حاصلضرب مستقیم N_1، N_2، $\cdots$، N_k است.

۱۰. گروههای آبلی متناهی (اختیاری)

لحظه‌ای قبل ضرب مستقیم گروهها به اتمام رسید. اگر این بحث همین جا رها شود، ممکن است این ساختار زیبا به نظر رسد ولی چه حاصلی برای ما دارد؟ برای آنکه بدان وزنی ببخشیم باید دست‌کم یک قضیه ثابت کنیم که بگوید هر گروه صادق در شرطی خاص حاصلضرب مستقیم چند گروه ساده است. خوشبختانه یک چنین رده از گروهها وجود دارند و آن گروههای آبلی متناهی

می‌باشند. آنچه ثابت می‌کنیم این است که هر گروه آبلی متناهی حاصلضرب مستقیم گروههایی دوری است. این امر اکثر مسائل مربوط به گروههای آبلی را به مسائل مربوط به گروههای دوری تحویل می‌کند و این تحویل اغلب ما را به جواب کامل این مسائل خواهد رسانید.

ساختار گروههای آبلی متناهی در واقع حالتی خاص از وضعیتی است با قضایای عامتر و عمیقتر. پرداختن به این گروهها ما را از بحث خیلی دور می‌سازد بخصوص اینکه داستان گروههای آبلی متناهی خود داستان بسیار مهمی می‌باشد. قضیه‌ای که ثابت می‌کنیم قضیهٔ اساسی گروههای آبلی متناهی نام دارد که به‌حق نام مناسبی برایش خواهد بود.

پیش از پرداختن به جزئیات برهان مایلیم طرح سریعی از آنچه در اثبات قضیه خواهیم گفت ارائه دهیم.

اولین گام تحویل مسئله از گروه آبلی متناهی به گروهی از مرتبهٔ p^n است که در آن p اول می‌باشد. این گام نسبتاً ساده است، و چون مرتبهٔ گروه مربوطه فقط شامل یک عدد اول است، جزئیات برهان با گروههایی که مرتبه‌شان به نوعی پیچیده‌اند مغشوش نخواهد شد.

لذا به گروههایی می‌پردازیم که مرتبه‌شان p^n است. فرض کنیم G یک گروه آبلی از مرتبهٔ p^n باشد. نشان می‌دهیم که زیرگروههایی دوری از G مانند A_1، A_2، $\cdots$، A_k وجود دارند به‌طوری که هر عنصر $x \in G$ را می‌توان به‌طور منحصر به‌فرد به‌صورت $x = b_1 b_2 \cdots b_k$ نوشت که در آن هر $b_i \in A_i$. به بیان دیگر، چون هر A_i دوری بوده و مثلاً به‌وسیلهٔ a_i تولید می‌شود، می‌خواهیم نشان دهیم که $x = a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}$ که در آن عناصر $a_i^{m_i}$ منحصر به‌فرد می‌باشند.

بلافاصله مشکلی پیش می‌آید چرا که انتخاب عناصر a_1، $\cdots$، a_k منحصر به فرد نیست. مثلاً هرگاه G یک گروه آبلی از مرتبهٔ ۴ با عناصر e، a، b، و ab باشد که $a^2 = b^2 = e$ و $ab = ba$، آن‌گاه می‌توان دید که اگر زیرگروههای A و B و C به‌ترتیب به‌وسیلهٔ a و b و ab تولید شده باشند، داریم $G = A \times B = A \times C = B \times C$. لذا انتخاب a_iها منحصر به‌فرد نیست. چطور می‌توان بر این مشکل فائق آمد؟

آنچه لازم است مکانیسمی است برای انتخاب a_1 و پس از آن انتخاب a_2، و غیره. می‌پرسیم: این مکانیسم چه باید باشد؟ کنترل ما بر عناصر G فقط تعیین مرتبهٔ آنهاست. این مرتبهٔ عنصر است که اگر به‌طور مناسب به‌کار رود ابزار لازم برای اثبات قضیه را به ما خواهد داد.

فرض کنیم $G = A_1 \times A_2 \times \cdots \times A_k$ که در آن $|G| = p^n$ و A_iها طوری شماره‌گذاری شده باشند که $|A_i| = p^{n_i}$ و $n_1 \geq n_2 \geq \cdots \geq n_k$ و هر A_i دوری بوده و به‌وسیلهٔ a_i تولید شده باشد. هرگاه چنین بوده و $x = a_1^{m_1} \cdots a_k^{m_k}$، آن‌گاه

$$x^{p^{n_1}} = (a_1^{m_1} \cdots a_k^{m_k})^{p^{n_1}} = a_1^{m_1 p^{n_1}} a_2^{m_2 p^{n_1}} \cdots a_k^{m_k p^{n_1}}$$

چون $n_1 \geq n_i$، $p^{n_i}|p^{n_1}$. لذا، چون هر $a_i^{m_i p^{n_i}} = e$، داریم $x^{p^{n_1}} = e$. به‌عبارت دیگر، a_1 باید عنصری از G باشد که مرتبه‌اش حتی‌الامکان بزرگ است. حال می‌توان a_1 را اختیار کرد. می‌پرسیم: برای a_2 چه کنیم؟ گوییم هرگاه $\bar{G} = G/A_1$، آن‌گاه برای به‌دست آوردن اولین عنصر لازم برای نمایش $\bar{G}$ به‌صورت حاصلضرب مستقیمی از گروههای دوری باید عنصری در $\bar{G}$ اختیار کنیم که مرتبه‌اش ماکزیمال باشد. این امر در خود G چه معنایی دارد؟ ما عنصری مانند a_2 می‌خواهیم دارای بالاترین توان ممکن که در A_1 قرار گیرد. لذا این راه انتخاب عنصر دوم می‌باشد. با این حال، اگر عنصر b_2 را با این خاصیت اختیار کنیم، ممکن است مشکل ما حل نشود. ممکن است برای رفع این معضل مجبور باشیم آن را تعدیل نماییم. همهٔ کار بخش فنی استدلال را تشکیل می‌دهد که انجام خواهد شد. سپس با تکرار مناسب این عمل عنصر a_3 را پیدا کرده و همین‌طور تا آخر ادامه می‌دهیم.

این روندی است که در اثبات قضیه به کار خواهیم برد. لیکن برای هموار ساختن این انتخابهای متوالی a_1، a_2، $\cdots$ از استقرا و چند نتیجهٔ کمکی مقدماتی استفاده خواهیم کرد.

امیدواریم برهان قضیه با این طرح به‌عنوان راهنما برای خواننده معنی داشته باشد. نباید ایدهٔ اصلی برهان (که کاملاً معقول است) با جزئیات فنی که ممکن است بحث را تیره سازند خلط شود. حال جزئیات طرح برهان مذکور در فوق را شرح می‌دهیم.

لم ۲.۱۰.۱. فرض کنیم G یک گروه آبلی متناهی از مرتبهٔ mn باشد که در آن m و n نسبت به هم اولند. هرگاه $M = \{x \in G | x^m = e\}$ و $N = \{x \in G | x^n = e\}$، آن‌گاه $G = M \times N$. به‌علاوه، هرگاه هیچیک از m و n مساوی ۱ نباشد، آن‌گاه $M \neq (e)$ و $N \neq (e)$.

برهان. به آسانی معلوم می‌شود که مجموعه‌های M و N تعریف شده در صورت لم زیرگروههایی از Gاند. به‌علاوه، هرگاه $m \neq 1$، آن‌گاه طبق قضیهٔ کشی (قضیهٔ ۴.۶.۲) داریم $M \neq (e)$، و به همین نحو اگر $n \neq 1$، خواهیم داشت $N \neq (e)$. به‌علاوه، چون $M \cap N$ زیرگروهی از هر دوی M و N است، بنابر قضیهٔ لاگرانژ $|M \cap N|$، $|M| = m$ و $|N| = n$ را عاد می‌کند. چون m و n نسبت به هم اولند، داریم $|M \cap N| = 1$. لذا $M \cap N = (e)$.

برای اتمام برهان باید نشان دهیم که $G = MN$ و $G = M \times N$. چون m و n نسبت به هم اولند، اعداد صحیحی چون r و s وجود دارند به‌طوری که $rm + sn = 1$. هرگاه $a \in G$، آن‌گاه $a = a^1 = a^{sn+rm} = a^{sn}a^{rm}$. چون $(a^{sn})^m = a^{snm} = e$، داریم $a^{sn} \in M$. به همین نحو $a^{rm} \in N$. لذا $a = a^{sn}a^{rm}$ در MN می‌باشد. بدین ترتیب $G = MN$. آخرین

مرحله، یعنی اثبات $G = M \times N$، را به خواننده وا می‌گذاریم. ■

یک نتیجهٔ فوری عبارت است از:

نتیجه. فرض کنیم G یک گروه آبلی متناهی بوده و عدد اول p چنان باشد که $p||G|$. در این صورت، به ازای زیرگروههایی چون P و T که $|P| = p^m$، $m > ۰$، و $|T|$ بر p بخشپذیر نیست، $G = P \times T$.

برهان. فرض کنیم $P = \{x \in G | x^{p^s} = e$، به ازای $s\}$ و
$$T = \{x \in G | x^t = e \text{، به ازای } t \text{ای نسبت به } p \text{ اول}\}$$
بنابر لم ۱.۱۰.۲، $G = P \times T$ و $P \neq (e)$. چون مرتبهٔ هر عنصر در P توانی از p است، با استمداد از قضیهٔ کشی به‌دست می‌آوریم $|P| = p^m$. ■

به آسانی و با استفاده از قضیهٔ لاگرانژ معلوم می‌شود که $p \nmid |T|$. لذا P در واقع فقط زیرگروه G نبوده و چیزی است که آن را زیرگروه p- سیلوی G می‌نامیم (ر.ک. بخش ۱۱).

حال به مرحلهٔ کلیدی برهان قضیه‌ای که در پی آنیم می‌رسیم. اثبات این قسمت کمی مشکل است، ولی با داشتن آن بقیهٔ کار آسان خواهد بود.

قضیهٔ ۲.۱۰.۲. فرض کنیم G یک گروه آبلی از مرتبه p^n بوده، p اول باشد، و $a \in G$ در بین تمام عناصر G از مرتبهٔ ماکزیمال باشد. در این صورت $G = A \times Q$ که در آن A زیرگروه دوری تولید شده به‌وسیلهٔ a می‌باشد.

برهان. بر n استقرا می‌کنیم. هرگاه $n = ۱$، آن‌گاه $|G| = p$ و G قبلاً یک گروه دوری تولید شده به‌وسیلهٔ هر $a \neq e$ در G می‌باشد.

فرض کنیم قضیه به ازای هر $m < n$ درست باشد. اگر عنصری مانند $b \in G$ چنان باشد که $b \notin A = (a)$ و $b^p = e$، نشان می‌دهیم که قضیه برقرار است. فرض کنیم $B = (b)$ یعنی زیرگروه Q تولید شده به‌وسیلهٔ b باشد. لذا $A \cap B = (e)$.

فرض کنیم $\bar{G} = G/B$. طبق فرض، $B \neq (e)$. پس $|\bar{G}| < |G|$. در $\bar{G}$ مرتبهٔ $\bar{a} = Ba$ چیست؟ حکم می‌کنیم که $o(\bar{a}) = o(a)$. در آغاز می‌دانیم که $o(\bar{a})|o(a)$ زیرا $a^{o(a)} = e$. لذا $\bar{a}^{o(a)} = (Ba)^{o(a)} = Ba^{o(a)} = B$. از آن‌سو، $\bar{a}^{o(\bar{a})} = \bar{e}$. پس $a^{o(\bar{a})} \in B$. چون $a^{o(\bar{a})} \in A$، می‌بینیم که $a^{o(\bar{a})} \in A \cap B = (e)$ که از آنجا $a^{o(\bar{a})} = e$. این به ما می‌گوید که $o(a)|o(\bar{a})$. لذا $o(a) = o(\bar{a})$.

چون $\bar{a}$ عنصری از مرتبهٔ ماکزیمال در $\bar{G}$ است، به استقرا معلوم می‌شود که به ازای زیرگروهی مانند T از $\bar{G}$، $\bar{G} = (\bar{a}) \times T$. همچنین از قضیهٔ دوم همریختی می‌دانیم که به ازای زیرگروهی مانند Q از G، $T = Q/B$. حکم می‌کنیم که $G = A \times Q$. در غیر این صورت $A \cap Q \neq (e)$. فرض کنیم $u \in A \cap Q$. پس $u = a^i \in Q$؛ در نتیجه $\bar{a}^i \in Q/B = T$، و چون $(\bar{a}) \cap T = (\bar{e})$، داریم $\bar{a}^i = \bar{e}$. پس $a^i \in B$. ولی $a^i \in A$ و $A \cap B = (e)$. لذا $a^i = e$ که به معنی $u = a^i = e$ می‌باشد. بنابراین $A \cap Q = (e)$ و خواهیم داشت $G = A \times Q$.

حال فرض کنیم عنصری مانند b در G و غیرواقع در A نیست که $b^p = e$. حکم می‌کنیم که $G = A = (a)$ که در این صورت G یک گروه دوری است. فرض کنیم $G \neq A$. همچنین $x \in G$ و $x \notin A$ کوچکترین مرتبهٔ ممکن را داشته باشد. چون $o(x^p) < o(x)$، بنابر انتخاب x داریم $x^p \in A$. پس $x^p = a^i$. حکم می‌کنیم که $p|i$. فرض کنیم چنین نباشد. قرار می‌دهیم $m = o(a) = p^s$. چون a در G از مرتبهٔ ماکزیمال است، پس به ازای هر $c \in G$، $o(c) = p^r \leq o(a) = p^s$. لذا $r \leq s$؛ و در نتیجه $o(c)|o(a) = m$. بنابراین $c^m = e$.

حال فرض کنیم $x^p = a^i$ و $p \nmid i$. پس $m \nmid im/p$؛ و در نتیجه $a^{im/p} \neq e$. ولی $x^m = (x^p)^{m/p} = (a^i)^{m/p} = a^{im/p} \neq e$ که با مطلب فوق که $x^m = e$ در تضاد است. لذا $p|i$؛ در نتیجه $i = jp$ و $x^p = a^i = a^{jp}$. فرض کنیم $y = a^{-j}x$. پس $y \notin A$ زیرا $x \notin A$ و $a^{-j} \in A$. به‌علاوه $y^p = (a^{-j}x)^p = a^{-jp}x^p = e$. ولی این ما را در وضع فوق قرار می‌دهد که در آن $x \in G$ی که $x \notin A$ هست به‌طوری که $x^p = e$. در این حالت دیدیم که قضیه درست است. لذا باید داشته باشیم $G = (a)$ و G یک گروه دوری می‌باشد. این امر استقرا را اتمام کرده و قضیه را به اثبات می‌رساند. ■

حال می‌توان قضیهٔ اساسی و مهم زیر را ثابت کرد.

قضیهٔ ۳.۱۰.۲ (قضیهٔ اساسی گروههای آبلی متناهی). هر گروه آبلی متناهی حاصلضرب مستقیم گروههایی دوری می‌باشد.

برهان. فرض کنیم G یک گروه آبلی متناهی بوده و عدد اول p عدد $|G|$ را عاد نماید. بنابر نتیجهٔ لم ۱.۱۰.۲، $G = P \times T$ که در آن $|P| = p^n$. و بنابر قضیهٔ ۲.۱۰.۲، $P = A_1 \times A_2 \times \cdots \times A_k$ که در آن A_iها زیرگروههای دوری P می‌باشند. لذا به استقرا بر $|G|$ می‌توان فرض کرد $T = T_1 \times T_2 \times \cdots \times T_q$ که در آن T_iها زیرگروههای دوری T

می‌باشند. بنابراین

$$G = (A_1 \times A_2 \times \cdots \times A_k) \times (T_1 \times T_2 \times \cdots \times T_q)$$
$$= A_1 \times A_2 \times \cdots \times A_k \times T_1 \times T_2 \times \cdots \times T_q$$

(ثابت کنید!) و قضیهٔ بسیار مهم فوق به اثبات می‌رسد. ■

حال به گروههای آبلی G از مرتبهٔ p^n باز می‌گردیم. آنچه داریم $G = A_1 \times A_2 \times \cdots \times A_k$ است که در آن A_iها گروههای دوری از مرتبهٔ p^{n_i} می‌باشند. گروهها را می‌توان طوری شماره‌گذاری کرد که $n_1 \geq n_2 \geq \cdots \geq n_k$. همچنین $|G| = |A_1 \times A_2 \times \cdots \times A_k| = |A_1||A_2|\cdots|A_k|$ که از آن داریم

$$p^n = p^{n_1}p^{n_2}\cdots p^{n_k} = p^{n_1+n_2+\cdots+n_k}$$

پس $n = n_1 + n_2 + \cdots + n_k$. لذا اعداد صحیح $n_i \geq 0$ افرازی از n را تشکیل می‌دهند. می‌توان نشان داد که این اعداد صحیح n_1، n_2، $\cdots$، n_k، که پایاهای G نام دارند، منحصر به‌فرداند. به عبارت دیگر، دو گروه آبلی از مرتبهٔ p^n یکریخت‌اند اگر و فقط اگر پایاهای یکسانی داشته باشند. با قبول این امر نتیجه می‌شود که تعداد گروههای آبلی غیریکریخت از مرتبهٔ p^n مساوی تعداد افرازهای n می‌باشد.

مثلاً اگر $n = 3$، سه افراز داریم: $3 = 3$، $2 + 1 = 3$، و $1 + 1 + 1 = 3$. پس سه گروه آبلی غیریکریخت از مرتبهٔ p^3 (مستقل از p) وجود دارند. گروههای نظیر این افرازها یک گروه دوری از مرتبهٔ p^3، حاصلضرب مستقیم یک گروه دوری از مرتبهٔ p^2 در یک گروه دوری از مرتبهٔ p، و حاصلضرب مستقیم سه گروه دوری از مرتبهٔ p می‌باشند.

به ازای $n = 4$ افرازهای زیر را داریم: $4 = 4$، $3 + 1 = 4$، $2 + 2 = 4$، $2 + 1 + 1 = 4$، و $1 + 1 + 1 + 1 = 4$ که تعدادشان پنج تاست. لذا پنج گروه غیریکریخت از مرتبهٔ p^4 وجود دارند. آیا می‌توانید آنها را با افرازهای ۴ توصیف کنید؟

هرگاه یک گروه آبلی از مرتبهٔ $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ باشد که در آن اعداد اول p_i متمایز بوده و a_iها همه مثبت باشند، آن‌گاه G حاصلضرب مستقیم زیرگروههای p_iـسیلوی خود است (مثلاً ر.ک. نتیجهٔ لم ۲.۱۰.۲). به ازای هر عدد اول p_i گروههای بسیاری از مرتبهٔ $p_i^{a_i}$ و افرازهایی از a_i در دست است. لذا تعداد گروههای آبلی غیریکریخت از مرتبهٔ $n = p_1^{a_1}\cdots p_k^{a_k}$ مساوی است با $f(a_1)f(a_2)\cdots f(a_k)$ که در آن $f(m)$ تعداد افرازهای m می‌باشد. لذا تعداد گروههای آبلی متناهی غیریکریخت را به ازای هر مرتبهٔ معلوم می‌دانیم.

مثلاً چند گروه آبلی غیریکریخت از مرتبهٔ ۱۴۴ وجود دارد؟ چون $2^4 3^2 = 144$ و پنج افراز از ۴ و دو افراز از ۲ داریم، پس ۱۰ گروه آبلی غیریکریخت از مرتبهٔ ۱۴۴ خواهیم داشت.

مطالب این بخش مشکل، مسیر بحث پرپیچ و خم، و تلاش برای درک نکات بسیار بود. لذا خواننده را بیش از این عذاب نداده و مسائلی به این بخش اختصاص نمی‌دهیم.

۱۱. تزویج و قضیهٔ سیلو (اختیاری)

در بحث روابط هم‌ارزی در بخش ۴ مفهوم تزویج به‌عنوان مثالی از این روابط در یک گروه G مطرح شد. به یاد آورید که عنصر b در G را مزدوج عنصر $a \in G$ نامیم اگر عنصری مانند $x \in G$ موجود باشد به‌طوری که $b = x^{-1}ax$. در بخش ۴ نشان دادیم که این معرف یک رابطهٔ هم‌ارزی بر G است. ردهٔ هم‌ارزی a، که با $\mathrm{cl}(a)$ نموده می‌شود، ردهٔ تزویج a نام دارد.

سؤال زیر بلافاصله در یک گروه متناهی مطرح می‌شود: $\mathrm{cl}(a)$ چقدر بزرگ است؟ این البته قویاً به عنصر a بستگی دارد. مثلاً هرگاه $a \in Z(G)$ (مرکز G)، آن‌گاه به ازای هر $x \in G$، $ax = xa$. لذا $x^{-1}ax = a$. به‌عبارت دیگر، ردهٔ تزویج a در این حالت فقط از a تشکیل شده است. از آن‌سو، هرگاه $\mathrm{cl}(a)$ فقط از a تشکیل شده باشد، آن‌گاه به ازای هر $x \in G$، $x^{-1}ax = a$. از این به ازای هر $x \in G$ داریم $xa = ax$. پس $a \in Z(G)$. لذا $Z(G)$ مجموعهٔ تمام aهایی در G است که ردهٔ تزویجشان فقط از یک عنصر، یعنی خود a، تشکیل شده است.

در گروه آبلی G، چون $G = Z(G)$، دو عنصر مزدوج‌اند اگر و فقط اگر مساوی باشند. لذا تزویج در گروههای آبلی رابطهٔ جالبی نیست. ولی این مفهوم در گروههای غیرآبلی بسیار جالب می‌باشد.

به ازای $a \in G$، $\mathrm{cl}(a)$ از تمام $x^{-1}ax$هایی که $x \in G$ تشکیل شده است. لذا در تعیین مزدوجهای متمایز a باید نشان دهیم چه وقت دو مزدوج a یکی است یا، به‌عبارت دیگر، چه وقت $x^{-1}ax = y^{-1}ay$؟ در این حالت با جابه‌جایی داریم $a(xy^{-1}) = (xy^{-1})a$. به بیان دیگر، xy^{-1} باید با a تعویض شود. این امر ما را به مفهوم آمده در مثال ۱۰ از بخش ۳، یعنی مرکز ساز a در G، می‌رساند. حال بخشی از مطالب آنجا را تکرار می‌کنیم.

تعریف. هرگاه $a \in G$، آن‌گاه $C(a)$، یعنی مرکزساز a در G، با $C(a) = \{x \in G | xa = ax\}$ تعریف می‌شود.

وقتی $C(a)$ در بخش ۳ ظاهر شد، نشان دادیم که زیرگروهی است از G. حال این امر را

به‌طور رسمی ثبت می‌کنیم.

لم ۱.۱۱.۲. $C(a)$ به ازای هر $a \in G$ زیرگروهی از G است.

همان‌طور که در بالا دیدیم، دو مزدوج $x^{-1}ax$ و $y^{-1}ay$ از a فقط وقتی مساویند که $xy^{-1} \in C(a)$؛ یعنی فقط وقتی x و y در یک هم‌مجموعهٔ راست $C(a)$ در G باشند. از آن‌سو، هرگاه x و y در یک هم‌مجموعهٔ راست $C(a)$ از G باشند، آن‌گاه $xy^{-1} \in C(a)$. پس $xy^{-1}a = axy^{-1}$. از این داریم $x^{-1}ax = y^{-1}ay$. لذا x و y مزدوج یکسانی از a را به‌دست می‌دهند اگر و فقط اگر x و y در هم‌مجموعهٔ راست یکسانی از $C(a)$ در G باشند. لذا تعداد مزدوجهای a در G به تعداد هم مجموعه‌های راست $C(a)$ در G است. این امر جالبترین وضع را زمانی دارد که G گروهی متناهی باشد، چرا که در این حالت تعداد هم‌مجموعه‌های راست $C(a)$ در G همان اندیس $i_G(C(a))$ از $C(a)$ در G است که مساوی $|G|/|C(a)|$ می‌باشد.
پس قضیهٔ زیر ثابت شده است.

قضیهٔ ۲.۱۱.۲. هرگاه G گروهی متناهی بوده و $a \in G$، آن‌گاه تعداد مزدوجهای متمایز a در G مساوی اندیس $C(a)$ در G می‌باشد.

به عبارت دیگر، تعداد عناصر $\mathrm{cl}(a)$ مساوی است با $i_G(C(a)) = |G|/|C(a)|$.
این قضیه با وجود داشتن برهانی نسبتاً ساده بسیار مهم بوده و نتایج زیادی دارد. ما چند تایی از آنها را در اینجا خواهیم دید.
یکی از این نتایج برای ثبت در اینجا مناسب است. چون تزویج یک رابطهٔ هم‌ارزی بر G است، G اجتماع رده‌های تزویج از هم‌جدا می‌باشد. به‌علاوه، طبق قضیهٔ ۲.۱۱.۲، تعداد عناصر هر رده را می‌دانیم. با جمع این اطلاعات به قضیهٔ زیر خواهیم رسید.

قضیهٔ ۳.۱۱.۲(معادلهٔ رده‌ای). هرگاه G یک گروه متناهی باشد، آن‌گاه

$$|G| = \sum_a i_G(C(a)) = \sum_a \frac{|G|}{|C(a)|}$$

که در آن مجموع روی یک a از هر ردهٔ تزویج گرفته می‌شود.

در بین ریاضیدانان تقریباً رسم است که به‌عنوان اولین کاربرد از معادلهٔ رده‌ای قضیهٔ خاصی راجع به گروهها از مرتبهٔ p^n، که در آن p اول است، ارائه می‌شود. ما این رسم را مراعات کرده و قضیهٔ زیبا و مهم زیر را ثابت می‌کنیم.

قضیهٔ ۴.۱۱.۲. هرگاه گروه G از مرتبهٔ p^n باشد که در آن p اول است، آن‌گاه $Z(G)$ (مرکز G) بدیهی نیست (یعنی عنصری مانند $a \neq e$ در G هست به‌طوری که به ازای هر $x \in G$، $ax = xa$)

برهان. ما در اثبات از معادلهٔ رده‌ای استفاده می‌کنیم. فرض کنیم $z = |Z(G)|$. همان‌طور که قبلاً گفتیم، z تعداد عناصری در G است که ردهٔ تزویجشان فقط یک عنصر دارد. چون $e \in Z(G)$، $z \geq ۱$. ردهٔ تزویج هر عنصر b خارج از $Z(G)$ بیش از یک عنصر دارد و $|C(b)| < |G|$. به‌علاوه، چون $|C(b)|$ طبق قضیهٔ لاگرانژ $|G|$ را عاد می‌کند، $|C(b)| = p^{n(b)}$ که در آن $n > n(b) \geq ۱$. حال معادلهٔ رده‌ای را به دو بخش تقسیم می‌کنیم: یک بخش از مرکز ناشی شده و دیگری بقیهٔ معادله می‌باشد. بدین ترتیب خواهیم داشت

$$p^n = |G| = \mathbf{z} + \sum_{b \notin Z(G)} \frac{|G|}{|C(b)|} = z + \sum_{n(b)<n} \frac{p^n}{p^{n(b)}} = z + \sum_{n(b)<n} p^{n-n(b)}$$

واضح است که p طرف چپ، یعنی p^n، و $\sum_{n(b)<n} p^{n-n(b)}$ را عاد می‌کند. پس $p|z$، و چون $z \geq ۱$، z دست‌کم p می‌باشد. لذا، چون $z = |Z(G)|$، باید عنصری مانند $a \neq e$ در $z(G)$ موجود باشد، و این قضیه را ثابت خواهد کرد. ■

قضیهٔ اخیر کاربرد جالبی دارد که ممکن است بعضی از خوانندگان آن را در حل مسئلهٔ ۴۵ از بخش ۵ دیده باشند. این کاربرد به قرار زیر است.

قضیهٔ ۵.۱۱.۲. هرگاه G گروهی از مرتبهٔ $p^۲$ باشد که در آن p اول است، آن‌گاه G آبلی می‌باشد.

برهان. بنابر قضیهٔ ۴.۱۱.۲، $Z(G) \neq (e)$. پس عنصری مانند a از مرتبهٔ p در $Z(G)$ وجود دارد. هرگاه $A = (a)$، یعنی زیرگروه تولید شده به‌وسیلهٔ a باشد، آن‌گاه $A \subset Z(G)$. پس به ازای هر $x \in G$، $A \subset C(x)$. به ازای $x \in G$ و $x \notin A$ داریم $C(x) \supset A$ و $x \in C(x)$. پس $|C(x)| > p$. ولی $|C(x)|$ باید $p^۲$ را عاد کند. در نتیجه $|C(x)| = p^۲$. لذا $C(x) = G$ که از آنجا $x \in Z(G)$. چون هر عنصر G در مرکز G است، G باید آبلی باشد. ■

در مسائلی که می‌آیند کاربردهای زیادی از خاصیت گروههای مرتبهٔ p^n به ازای pی اول ذکر خواهد شد. حمله به تمام این مسائل طبعاً به موازات استدلالی است که اینک خواهیم آورد. برای توضیح این روش، مجموعهٔ انتخابهای ما بیشترین وسعت ممکن را خواهد داشت.

قضیهٔ ۶.۱۱.۲. هرگاه G گروهی از مرتبهٔ p^n باشد که در آن p اول است، آن‌گاه G شامل یک زیرگروه نرمال از مرتبهٔ p^{n-1} می‌باشد.

برهان. به استقرا بر n عمل می‌کنیم. هرگاه $n = 1$، آن‌گاه G از مرتبهٔ p بوده و (e) زیرگروه نرمال مطلوب از مرتبهٔ $p^{1-1} = p^0 = 1$ است.

فرض کنیم به ازای kای هر گروه از مرتبهٔ p^k زیرگروه نرمالی از مرتبهٔ p^{k-1} داشته باشد. همچنین G از مرتبهٔ p^{k+1} باشد. بنابر قضیهٔ ۴.۱۱.۲ عنصری مانند a از مرتبهٔ p در $Z(G)$ (مرکز G) موجود است. لذا زیرگروه $A = (a)$ تولید شده به‌وسیلهٔ a از مرتبهٔ p و نرمال در G می‌باشد. $\Gamma = G/A$ را در نظر می‌گیریم. Γ طبق قضیهٔ ۳.۶.۲ یک گروه از مرتبه $|G|/|A| = p^{k+1}/p = p^k$ است. چون Γ از مرتبهٔ p^k است، Γ زیرگروه نرمالی از مرتبهٔ p^{k-1} مانند M دارد. و چون Γ نقش همریختی G است، بنابر قضیهٔ دوم همریختی (قضیهٔ ۲.۷.۲) زیرگروه نرمالی از G مانند N هست که $A \subset N$ و $M \simeq N/A$. اما در این صورت داریم

$$|M| = |N/A| = \frac{|N|}{|A|}$$

یعنی $p^{k-1} = |N|/p$ که ما را به $|N| = p^k$ می‌رساند. N زیرگروه نرمال مطلوب در G از مرتبهٔ p^k می‌باشد. این استقرا را تمام کرده و قضیه را به اثبات می‌رساند. ■

تاکنون مهمترین کاربرد ما از معادلهٔ رده‌ای برهان قضیهٔ سودمندی منسوب به سیلو، ریاضیدان نروژی، بوده است که آن را در ۱۸۷۱ به ثبوت رسانید. ما قبلاً صحت این قضیه را برای گروههای آبلی نشان داده‌ایم. حال آن را برای هر گروه متناهی ثابت می‌کنیم. راجع به اهمیت قضیهٔ سیلو در مطالعهٔ گروههای متناهی هر چه بگوییم کم است. این مبحث بدون قضیهٔ سیلو حتی نمی‌تواند آغاز شود.

قضیهٔ ۷.۱۱.۲ (قضیهٔ سیلو). فرض کنیم G گروهی از مرتبهٔ $p^n m$ باشد که در آن p اول بوده و $p \nmid m$. در این صورت G زیرگروهی از مرتبهٔ p^n دارد.

برهان. هرگاه $n = 0$، آن‌گاه $p \nmid |G|$ و چیزی برای اثبات وجود ندارد. لذا فرض می‌کنیم $n \geq 1$. در اینجا مجدداً بر $|G|$ استقرا کرده و فرض می‌کنیم نتیجه به ازای جمیع گروههای H که $|H| < |G|$ درست باشد.

فرض کنیم نتیجه برای G نادرست باشد. پس، طبق فرض استقرا، p^n نمی‌تواند $|H|$ را به ازای هر زیرگروه H از G که $H \neq G$ عاد کند. به‌خصوص، هرگاه $a \notin Z(G)$، آن‌گاه $C(a) \neq G$.

پس $p^n \nmid C(a)$. لذا، به ازای $a \notin Z(G)$، $p|\ |G|/|C(a)| = i_G(C(a))$.

معادلهٔ رده‌ای G را به موازات استدلال در قضیهٔ ۴.۱۱.۲ می‌نویسیم. هرگاه $z = |Z(G)|$، آن‌گاه $z \geq ۱$ و

$$p^n m = |G| = z + \sum_{a \notin Z(G)} i_G(C(a))$$

ولی اگر $a \notin Z(G)$، $p|i_G(C(a))$؛ در نتیجه $p|\sum_{a \notin Z(G)} i_G(C(a))$. چون $p|p^n m$، به‌دست می‌آوریم $p|z$. بنا بر قضیهٔ کشی، عنصری مانند a از مرتبهٔ p در $Z(G)$ وجود دارد زیرا $p|z = |Z(G)|$. هرگاه A زیرگروه تولید شده به‌وسیلهٔ a باشد، آن‌گاه $|A| = p$ و $A \triangleleft G$ زیرا $a \in Z(G)$. حال $\Gamma = G/A$ را در نظر می‌گیریم. $|\Gamma| = |G|/|A| = p^n m/p = p^{n-۱} m$. چون $|\Gamma| < |G|$، بنا بر فرض استقرا، Γ زیرگروهی مانند M از مرتبهٔ $p^{n-۱}$ دارد. ولی، بنا بر قضیهٔ دوم همریختی، زیرگروهی مانند P از G وجود دارد به‌طوری که $P \supset A$ و $M \simeq P/A$. لذا $|P| = |M||A| = p^{n-۱}p = p^n$. پس P زیرگروه مطلوب ما از G از مرتبهٔ p^n است که با فرض اینکه G چنین زیرگروهی ندارد در تضاد می‌باشد. این استقرا را کامل کرده و قضیهٔ سیلو را به ثبوت می‌رساند. ■

قضیهٔ سیلو در واقع از سه قسمت تشکیل شده است که ما فقط قسمت اولش را ثابت کرده‌ایم. دو قسمت دیگر (با فرض $|G| = p^n m$ که در آن $p \nmid m$) به شرح زیرند:

۱. هر دو زیرگروه از مرتبهٔ p^n در G مزدوج‌اند؛ یعنی هرگاه P و Q زیرگروه G بوده و $|P| = |Q| = p^n$، آن‌گاه به ازای $x \in G$ی، $Q = x^{-۱}Px$.

۲. تعداد زیرگروههای G از مرتبهٔ p^n به شکل $۱ + kp$ بوده و $|G|$ را عاد می‌نماید.

چون این زیرگروههای مرتبهٔ p^n همه‌جا ظاهر می‌شوند، آنها را زیرگروههای pـسیلوی G می‌نامیم. یک گروه آبلی به ازای هر عدد اول pای که مرتبه‌اش را عاد کند یک زیرگروه pـسیلو دارد. این در حالت کلی از واقعیت به‌دور است. مثلاً اگر $G = S_۳$ یعنی گروه متقارن از درجهٔ ۳ باشد، که از مرتبهٔ $۲ \cdot ۳ = ۶$ است، سه زیرگروه ۲ـسیلو (از مرتبهٔ ۲) و یک زیرگروه ۳ـسیلو (از مرتبهٔ ۳) خواهد داشت.

برای آنهایی که بخواهند چند برهان از بخشی از قضیهٔ سیلو که در بالا ثابت شد و نیز دو بخش دیگر را ببینند می‌توانند به بخش مربوطه درکتاب مباحثی در جبر اینجانب مراجعه نمایند.

مسائل

مسائل آسانتر

۱. در S_3، یعنی گروه متقارن از درجهٔ ۳، تمام رده‌های تزویج را یافته و صحت معادلهٔ رده‌ای را با تعیین مرتبهٔ مرکزسازهای عناصر S_3 امتحان کنید.

۲. مسئلهٔ ۱ را برای گروه دو وجهی G از مرتبهٔ ۸ حل نمایید.

۳. اگر $a \in G$، نشان دهید که $C(x^{-1}ax) = x^{-1}C(a)x$.

۴. اگر φ یک خودریختی از G باشد، نشان دهید که به ازای هر $a \in G$، $C(\varphi(a)) = \varphi(C(a))$.

۵. اگر $|G| = p^3$ و $|Z(G)| \geq p^2$، ثابت کنید G آبلی است.

۶. اگر P یک زیرگروه pـسیلوی G بوده و $P \triangleleft G$، ثابت کنید P تنها زیرگروه pـسیلوی G می‌باشد.

۷. اگر $P \triangleleft G$ و P یک زیرگروه pـسیلوی G باشد، ثابت کنید به ازای هر خودریختی φ از G، $\varphi(P) = P$.

۸. قضیهٔ کشی را با استفاده از معادلهٔ رده‌ای ثابت کنید.

اگر H زیرگروهی از G باشد، قرار دهید $N(H) = \{x \in G | x^{-1}Hx = H\}$. این بدان معنی نیست که اگر $x \in N(H)$ و $a \in H$، $xa = ax$. مثلاً هرگاه $H \triangleleft G$، آن‌گاه $N(H) = G$ ولی H لازم نیست در مرکز G باشد.

۹. ثابت کنید $N(H)$ زیرگروهی است از G، $H \subset N(H)$، و $H \triangleleft N(H)$.

۱۰. ثابت کنید $N(x^{-1}Hx) = x^{-1}N(H)x$.

۱۱. اگر P یک زیرگروه pـسیلوی G باشد، ثابت کنید P یک زیرگروه pـسیلوی $N(P)$ بوده و تنها زیرگروه pـسیلوی $N(P)$ می‌باشد.

۱۲. اگر P یک زیرگروه pـسیلوی G بوده و $a \in G$ از مرتبهٔ p^m به ازای mی باشد، نشان دهید هرگاه $a^{-1}Pa = P$، آن‌گاه $a \in P$.

۱۳. ثابت کنید هرگاه G یک گروه متناهی و H زیرگروهی از آن باشد، آن‌گاه تعداد زیرگروههای متمایز $x^{-1}Hx$ از G مساوی $i_G(N(H))$ می‌باشد.

۱۴. اگر P یک زیرگروه pـسیلوی G باشد، نشان دهید که تعداد $x^{-1}Px$های متمایز نمی‌تواند مضربی از p باشد.

۱۵. اگر $N \triangleleft G$، قرار دهید $B(N) = \{x \in G | xa = ax$، به ازای هر $a \in N\}$ و ثابت کنید $B(N) \triangleleft G$.

مسائل با سطح متوسط

۱۶. نشان دهید که هر گروه از مرتبهٔ ۳۶ زیرگروه نرمالی از مرتبهٔ ۳ یا ۹ دارد. (راهنمایی. ر.ک. مسئلهٔ ۴۰ از بخش ۵.)

۱۷. نشان دهید که هر گروه از مرتبهٔ ۱۰۸ زیرگروه نرمالی از مرتبهٔ ۹ یا ۲۷ دارد.

۱۸. اگر P یک زیرگروه pـسیلوی G باشد، نشان دهید که $N(N(P)) = N(P)$.

۱۹. اگر $|G| = p^n$، نشان دهید که G زیرگروهی از مرتبهٔ p^m به ازای هر $1 \leq m \leq n$ دارد.

۲۰. اگر $p^m \mid |G|$، نشان دهید G زیرگروهی از مرتبهٔ p^m دارد.

۲۱. اگر $|G| = p^n$ و $H \neq G$ زیرگروهی از H باشد، نشان دهید که $N(H) \supsetneq H$.

۲۲. نشان دهید که هر زیرگروه از مرتبهٔ p^{n-1} در گروه G از مرتبهٔ p^n در G نرمال است.

مسائل مشکلتر

۲۳. فرض کنید G یک گروه و H زیرگروهی از آن باشد. به ازای $a, b \in G$ تعریف کنید $a \sim b$ اگر به ازای $h \in H$ی، $b = h^{-1}ah$. ثابت کنید

الف) این معرف یک رابطهٔ هم‌ارزی بر G است؛

ب) اگر $[a]$ ردهٔ هم‌ارزی a باشد، نشان دهید هرگاه G یک گروه متناهی باشد، آن‌گاه $[a]$ دارای m عنصر است که m اندیس $H \cap C(a)$ در H می‌باشد.

۲۴. اگر G یک گروه و H زیرگروهی از آن باشد، به ازای زیرگروههای A و B تعریف کنید $A \sim B$ اگر به ازای $h \in H$ی، $B = h^{-1}Ah$.

الف) ثابت کنید این معرف یک رابطهٔ هم‌ارزی بر مجموعهٔ زیرگروههای G است.

ب) اگر G متناهی باشد، نشان دهید که تعداد زیرگروههای متمایز هم‌ارز با A مساوی اندیس $N(A) \cap H$ در H است.

۲۵. اگر P یک زیرگروه pـسیلوی G بوده و S مجموعهٔ تمام زیرگروههای pـسیلوی G باشد، به ازای $Q_1, Q_2 \in S$ تعریف کنید $Q_1 \sim Q_2$ اگر $Q_2 = a^{-1}Q_1a$ که در آن $a \in P$. با استفاده از این رابطه ثابت کنید هرگاه $Q \neq P$، آن‌گاه تعداد $a^{-1}Qa$های متمایز که $a \in P$ مضربی است از p.

۲۶. با استفاده از مسئلهٔ ۲۵ نشان دهید که تعداد زیرگروههای pـسیلوی G به شکل $1 + kp$ است. (این قسمت سوم قضیهٔ سیلو می‌باشد.)

۲۷. فرض کنید P یک زیرگروه pـسیلوی G و Q زیرگروه دیگری از این نوع باشد. همچنین به ازای هر $x \in G$، $Q \neq x^{-1}Px$. و نیز S مجموعهٔ تمام $y^{-1}Qy$هایی باشد که $y \in G$. به

ازای $Q_1, Q_2 \in S$ تعریف کنید $Q_1 \sim Q_2$ اگر $Q_2 = a^{-1}Q_1a$ که در آن $a \in P$.

الف) نشان دهید این ایجاب می‌کند که تعداد $y^{-1}Qy$های متمایز مضربی از p است.

ب) با استفاده از مسئلهٔ ۱۴ نشان دهید که قسمت (الف) نمی‌تواند برقرار باشد.

پ) با استفاده از این ثابت کنید هرگاه P و Q دو زیرگروه pـسیلوی G باشند، آن‌گاه به ازای $x \in G$ی، $Q = x^{-1}Px$. (این قسمت دوم قضیهٔ سیلو می‌باشد.)

۲۸. اگر H زیرگروهی از G از مرتبهٔ p^m باشد، نشان دهید که H مشمول زیرگروه pـسیلویی از G می‌باشد.

۲۹. اگر P یک زیرگروه pـسیلوی G بوده و $a, b \in Z(P)$ در G مزدوج باشند، ثابت کنید در $N(P)$ نیز مزدوج می‌باشند.

۳

گروه متقارن

۱. پیشنیازها

ابتدا قضیه‌ای را که در فصل ۲ برای گروههای مجرد ثابت شد یادآور می‌شویم. این نتیجه، که به قضیهٔ کیلی (قضیهٔ ۱.۵.۲) معروف است، حکم می‌کند که هر گروه G با زیرگروهی از $A(S)$ (مجموعهٔ نگاشتهای ۱-۱ از مجموعهٔ S به روی خود به ازای Sی مناسب) یکریخت است. در واقع در برهان این قضیه از خود گروه G به‌عنوان یک مجموعه برای S استفاده کرده‌ایم.

گروهها از نظر تاریخی خیلی پیش از آنکه مفهوم گروه مجرد تعریف شود ظاهر شده‌اند. ما در کارهای لاگرانژ، آبل (Abel)، گالوا (Galois)، و دیگران نتایجی راجع به گروه جایگشتها می‌بینیم که در اواخر قرن هجده و اوایل قرن نوزده ثابت شده‌اند. ولی در اواسط قرن نوزدهم بود که کیلی مفهوم مجرد گروه را تعریف کرد.

چون ساختار گروههای یکریخت یکسان است، قضیهٔ کیلی به ویژگی کلی گروههای $A(S)$ اشاره دارد. اگر ساختار تمام زیرگروههای $A(S)$ به ازای مجموعهٔ دلخواه S را می‌دانستیم، ساختار تمام گروهها معلوم بود. اما این انتظار بسیار زیاد است. با این‌حال می‌توان از نشاندن گروه دلخواه G در $A(S)$ به‌طور یکریخت سود جست. این امر دارای این مزیت است که دستگاه مجرد G به چیزی ملموستر، یعنی مجموعه‌ای از نگاشتهای زیبا از یک مجموعه به روی خود، تبدیل می‌شود.

ما به زیرگروههای $A(S)$ به ازای مجموعهٔ دلخواه S علاقمند نیستیم. اگر S نامتناهی باشد، $A(S)$ بسیار خودسر و پیچیده است. حتی اگر S متناهی باشد، تعیین ماهیت کامل $A(S)$ ناممکن

است.

در این فصل فقط $A(S)$هایی را در نظر می‌گیریم که در آنها S متناهی است. به یاد آورید که اگر S دارای n عنصر باشد، $A(S)$ گروه متقارن از درجهٔ n نام دارد و با S_n نموده می‌شود. عناصر S_n را جایگشت نامیده و آنها را با حروف کوچک یونانی نشان می‌دهیم.

چون ما $\sigma, \tau \in A(S)$ را با قاعدهٔ $(\sigma\tau)(s) = \sigma(\tau(s))$ در هم ضرب می‌کنیم، پس علایم نمایش عناصر S_n یا جایگشتها را از راست به چپ ضرب خواهیم کرد. خواننده در کتب دیگر جبر باید از طرز ضرب جایگشتها که از راست به چپ یا از چپ به راست است مطمئن شود. جبردانان اغلب جایگشتها را از چپ به راست در هم ضرب می‌کنند. ما، برای سازگاری با ترکیب عناصر در S_n، از راست به چپ ضرب خواهیم کرد.

از قضیهٔ کیلی می‌دانیم که هرگاه G یک گروه متناهی از مرتبهٔ n باشد، آن‌گاه G با زیرگروهی از S_n یکریخت بوده و S_n دارای $n!$ عنصر می‌باشد. ما معمولاً به بیان نادقیق می‌گوییم که G زیرگروه S_n است. چون n از $n!$ به ازای n نسبتاً بزرگ خیلی کوچکتر است، گروه ما فقط گوشه‌ای از S_n را اشغال می‌کند. مطلوب نشانیدن G در یک S_n به ازای n حتی‌الامکان کوچک است. این امر برای رده‌هایی از گروههای متناهی میسر می‌باشد.

فرض کنیم S مجموعه‌ای متناهی مرکب از n عنصر باشد. می‌توان قرار داد $S = \{x_1, x_2, \dots, x_n\}$. جایگشت $\sigma \in S_n = A(S)$ را در نظر می‌گیریم. به ازای $k = 1, 2, \dots, n$، $\sigma(x_k) \in S$. پس به ازای i_kای که $1 \leq i_k \leq n$، $\sigma(x_k) = x_{i_k}$. چون σ یک‌به‌یک است، هرگاه $j \neq k$، آن‌گاه $x_{i_j} = \sigma(x_j) \neq \sigma(x_k) = x_{i_k}$. لذا اعداد i_1، i_2، $\dots$، i_n همان اعداد ۱، ۲، $\dots$، nاند که ترتیبی دیگر یافته‌اند.

واضح است که عمل σ بر S با عملش بر زیرنویس j از x_j معین می‌شود. در نتیجه علامت «x» باری است اضافی و می‌توان آن را حذف کرد. به بیان کوتاه، می‌توان فرض کرد $S = \{1, 2, \dots, n\}$.

حال ضرب دو عنصر در $A(S)$ را به یاد می‌آوریم. اگر $\sigma, \tau \in A(S)$، $\sigma\tau$ را با $(\sigma\tau)(s) = \sigma(\tau(s))$ به ازای هر $s \in S$ تعریف کردیم. ما در بخش ۴ از فصل ۱ نشان دادیم که $A(S)$ در چهار خاصیت صدق می‌کند که بعداً از آنها به‌عنوان مدلی برای تعریف مفهوم گروه مجرد استفاده شد. لذا S_n به‌خصوص نسبت به ضرب نگاشتها یک گروه می‌باشد.

اولین نیاز راهی سودمند برای نمایش یک جایگشت، یعنی عنصری مانند σ در S_n، است. یک راه ساختن جدولی از اعمال σ بر هر عنصر S است. این جدول را می‌توان گراف σ نامید. ما این کار را قبلاً کرده و مثلاً $\sigma \in S_3$ را به‌صورت $\sigma : x_1 \to x_2, x_2 \to x_3, x_3 \to x_1$ نوشتیم. ولی

این عمل پر زحمت و جاگیر است. این امر را می‌توان با حذف xها و نوشتن $\sigma = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix}$ فشرده‌تر کرد. در این علامت عدد واقع در سطر دوم نقش عدد واقع در سطر اول و درست روی آن است. در اینجا ۳ عدد مقدسی نیست و می‌توان آن را با هر n عوض کرد.

اگر $\sigma \in S_n$ و $\sigma(۱) = i_۱$، $\sigma(۲) = i_۲$، $\cdots$، $\sigma(n) = i_n$، از علامت $\begin{pmatrix} ۱ & ۲ & \cdots & n \\ i_۱ & i_۲ & \cdots & i_n \end{pmatrix}$ برای نمایش σ استفاده کرده و می‌نویسیم $\sigma = \begin{pmatrix} ۱ & ۲ & \cdots & n \\ i_۱ & i_۲ & \cdots & i_n \end{pmatrix}$. لازم نیست سطر اول به‌ترتیب معمولی $n \quad \cdots \quad ۲ \quad ۱$ نوشته شود. سطر اول به هر طریق نوشته شود، به شرط آنکه i_jها در جای مناسب قرار گیرند، σ را خواهیم داشت. مثلاً در $S_۳$ داریم

$$\sigma = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix} = \begin{pmatrix} ۳ & ۱ & ۲ \\ ۱ & ۲ & ۳ \end{pmatrix} = \begin{pmatrix} ۲ & ۱ & ۳ \\ ۳ & ۲ & ۱ \end{pmatrix}$$

اگر $\sigma = \begin{pmatrix} ۱ & ۲ & \cdots & n \\ i_۱ & i_۲ & \cdots & i_n \end{pmatrix}$، $\sigma^{-۱}$ چیست؟ یافتن آن آسان است. کافی است در σ جای دو سطر با هم عوض شود تا $\sigma^{-۱} = \begin{pmatrix} i_۱ & i_۲ & \cdots & i_n \\ ۱ & ۲ & \cdots & n \end{pmatrix}$ به‌دست آید (ثابت کنید!). در مثال ما

$$\sigma = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix}, \quad \sigma^{-۱} = \begin{pmatrix} ۲ & ۳ & ۱ \\ ۱ & ۲ & ۳ \end{pmatrix} = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۱ & ۲ \end{pmatrix}$$

عنصر همانی، که آن را به‌صورت e می‌نویسیم، عبارت است از $e = \begin{pmatrix} ۱ & ۲ & \cdots & n \\ ۱ & ۲ & \cdots & n \end{pmatrix}$. می‌پرسیم:

ضرب در S_n چطور برحسب این علایم بیان می‌شود؟ چون $\sigma\tau$ به این معنی است که «ابتدا τ و سپس σ اعمال می‌شود»، پس برای ضرب علایم σ و τ به عدد k در سطر اول τ نگاه کرده می‌بینیم چه عدد i_k زیر k در سطر دوم τ آمده است. سپس در جای i_k در سطر اول σ نگاه کرده می‌بینیم زیر آن در سطر دوم σ چه عددی قید شده است. این عدد نقش k تحت $\sigma\tau$ می‌باشد. حال این کار را برای هر $k = ۱, ۲, \ldots, n$ انجام داده و علامت $\sigma\tau$ را به‌دست می‌آوریم. ما این عمل را با چشم انجام می‌دهیم.

حال عمل فوق‌الذکر را با دو جایگشت

$$\tau = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۳ & ۴ & ۵ & ۱ & ۲ \end{pmatrix} \quad \text{و} \quad \sigma = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۲ & ۳ & ۱ & ۵ & ۴ \end{pmatrix}$$

در $S_۵$ توضیح می‌دهیم. در این‌صورت، $\sigma\tau = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۱ & ۵ & ۴ & ۲ & ۳ \end{pmatrix}$.

اما این روش جای زیادی را اشغال می‌کند. سطر اول همیشه $n \; \cdots \; ۲ \; ۱$ است. پس می‌توان آن را حذف کرد و $\sigma = \begin{pmatrix} ۱ & ۲ & \cdots & n \\ i_۱ & i_۲ & \cdots & i_n \end{pmatrix}$ را به‌صورت $(i_۱, i_۲, \ldots, i_n)$ نوشت. این کار خوب است ولی در بخش بعد راهی بهتر و خلاصه‌تر برای نمایش جایگشتها خواهیم یافت.

مسائل

۱. حاصل‌ضربهای زیر را بیابید:

الف) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۶ & ۴ & ۵ & ۲ & ۱ & ۳ \end{pmatrix} \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۲ & ۳ & ۴ & ۵ & ۶ & ۱ \end{pmatrix}$؛

ب) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۲ & ۱ & ۳ & ۴ & ۵ \end{pmatrix} \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۳ & ۲ & ۱ & ۴ & ۵ \end{pmatrix}$؛

پ) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۴ & ۱ & ۳ & ۲ & ۵ \end{pmatrix}^{-۱} \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۲ & ۱ & ۳ & ۴ & ۵ \end{pmatrix} \times \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۴ & ۱ & ۳ & ۲ & ۵ \end{pmatrix}$.

۲. تمام توانهای هر یک از جایگشتهای زیر را حساب کنید (یعنی σ^k را به ازای هر k بیابید):

الف) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۲ & ۳ & ۴ & ۵ & ۶ & ۱ \end{pmatrix}$؛

ب) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۲ & ۱ & ۳ & ۴ & ۶ & ۵ & ۷ \end{pmatrix}$؛

پ) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۶ & ۴ & ۵ & ۲ & ۱ & ۳ \end{pmatrix}$.

۳. ثابت کنید $\begin{pmatrix} i_۱ & i_۲ & \cdots & i_n \\ ۱ & ۲ & \cdots & n \end{pmatrix} = \begin{pmatrix} ۱ & ۲ & \cdots & n \\ i_۱ & i_۲ & \cdots & i_n \end{pmatrix}^{-۱}$.

۴. در مسئلهٔ ۲ مرتبهٔ هر عنصر را بیابید.

۵. در مسئلهٔ ۱ مرتبهٔ هر حاصلضرب را بیابید.

۲. تجزیهٔ دوری

به ساده‌سازی نماد جایگشتها ادامه می‌دهیم. در این راه بیش از یک علامت جدید به‌دست می‌آوریم. ما برای تجزیهٔ هر جایگشت به‌صورت حاصلضرب چند جایگشت مناسب طرحی به‌دست خواهیم آورد.

تعریف. فرض کنیم $i_۱$، $i_۲$، $\cdots$، i_k، k عدد صحیح متمایز در $S = \{۱, ۲, \ldots, n\}$ باشند. علامت $(i_۱, i_۲ \cdots i_k)$ نمایش جایگشت $\sigma \in S_n$ است که $\sigma(i_۱) = i_۲$، $\sigma(i_۲) = i_۳$، $\cdots$، $\sigma(i_j) = i_{j+۱}$ به ازای $j < k$، $\sigma(i_k) = i_۱$، و $\sigma(s) = s$ به ازای هر $s \in S$ که $s \neq i_۱, i_۲, \ldots, i_k$.

مثلاً جایگشت $(۱ \ \ ۳ \ \ ۵ \ \ ۴)$ در $S_۷$ عبارت است از $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۳ & ۲ & ۵ & ۱ & ۴ & ۶ & ۷ \end{pmatrix}$. ما هر جایگشت به شکل $(i_۱, i_۲, \ldots, i_k)$ را یک kـدور می‌نامیم. در حالت خاص $k = ۲$، جایگشت $(i_۱, i_۲)$ یک ترانهش نام دارد. توجه کنید که هرگاه $\sigma = (i_۱ \ \ i_۲ \cdots i_k)$، آن‌گاه σ مساوی $(i_k \ \ i_۱ \ \ i_۲ \ \ \cdots \ \ i_{k-۱})$، $(i_{k-۱} \ \ i_k \ \ i_۱ \ \ i_۲ \ \ \cdots \ \ i_{k-۲})$، و غیره نیز هست. (ثابت کنید!) به‌عنوان مثال،

$$(۱ \ \ ۳ \ \ ۵ \ \ ۴) = (۴ \ \ ۱ \ \ ۳ \ \ ۵) = (۵ \ \ ۴ \ \ ۱ \ \ ۳) = (۳ \ \ ۵ \ \ ۴ \ \ ۱)$$

یک kـدور و یک mـدور را دورهای از هم‌جداگوییم اگر عدد صحیح مشترکی نداشته باشند. مثلاً $(۵ \ \ ۳ \ \ ۱)$ و $(۷ \ \ ۶ \ \ ۲ \ \ ۴)$ در $S_۷$ دورهایی از هم جدا می‌باشند.

هر دو دور از هم جدا در S_n با هم تعویض می‌شوند. اثبات این امر به خواننده محول می‌شود با این راهنمایی که اگر σ و τ دورهای از هم جدایی باشند، باید تحقیق کرد که به ازای هر $i \in S = \{۱, ۲, \ldots, n\}$، $(\sigma\tau)(i) = (\tau\sigma)(i)$. این نتیجه را به‌صورت لم زیر بیان می‌کنیم.

لم ۱.۲.۳. هرگاه $\sigma, \tau \in S_n$ دورهای از هم‌جدایی باشند، آن‌گاه $\sigma\tau = \tau\sigma$.

حال kـدور خاص $\sigma = (۱ \ \ ۲ \ \ \cdots \ \ k)$ را در S_n در نظر می‌گیریم. واضح است که طبق تعریف فوق، $\sigma(۱) = ۲$. ۳ چگونه با ۱ مرتبط است؟ چون $\sigma(۲) = ۳$، داریم

$\sigma^{۲}(۱) = \sigma(۲) = ۳$. با ادامهٔ این کار خواهیم دید که به ازای $j \le k - ۱$، $\sigma^j(۱) = j + ۱$ ولی $\sigma^k(۱) = ۱$. در واقع می‌بینیم که $\sigma^k = e$ که در آن e عنصر همانی S_n می‌باشد.

از بند فوق دو مطلب نتیجه می‌شود:

۱. مرتبهٔ یک kـدور به‌عنوان عنصری از S_n مساوی k است (ثابت کنید!)؛

۲. هرگاه $\sigma = (i_۱ \ \ i_۲ \ \ \cdots \ \ i_k)$ یک kـدور باشد، آن‌گاه مدار $i_۱$ تحت σ (ر.ک. مسئلهٔ ۲۷ در بخش ۴ از فصل ۱) عبارت است از $\{i_۱, i_۲, \ldots, i_k\}$.

لذا می‌توان دید که kـدور $\sigma = (i_۱ \ \ i_۲ \ \ \cdots \ \ i_k)$ عبارت است از

$$\sigma = (i_۱ \ \ \sigma(i_۱) \ \ \sigma^{۲}(i_۱) \ \ \cdots \ \ \sigma^{k-۱}(i_۱))$$

به ازای هر جایگشت τ در S_n که $i \in \{۱, ۲, \ldots, n\}$، مدار i تحت τ را در نظر می‌گیریم. این مدار عبارت است از $\{i, \tau(i), \tau^{۲}(i), \ldots, \tau^{s-۱}(i)\}$ که در آن $\tau^s(i) = i$ و s کوچکترین عدد صحیح مثبت با این خاصیت می‌باشد. sـدور $(i \ \ \tau(i) \ \ \tau^{۲}(i) \ \ \cdots \ \ \tau^{s-۱}(i))$ را در نظر می‌گیریم. ما آن را دور τ معین شده به‌وسیلهٔ i می‌نامیم.

حال مثال خاصی اختیار کرده و تمام دورهایش را می‌یابیم. فرض کنیم

$$\tau = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۳ & ۹ & ۴ & ۱ & ۵ & ۶ & ۲ & ۷ & ۸ \end{pmatrix}$$

دور معین شده به‌وسیلهٔ ۱ چیست؟ حکم می‌کنیم که این دور $(۱ \ \ ۳ \ \ ۴)$ است. می‌پرسیم چرا؟ گوییم τ عدد ۱ را به ۳، عدد ۳ را به ۴، و عدد ۴ را به ۱ می‌برد، و چون $\tau(۱) = ۳$، $\tau^{۲}(۱) = \tau(۳) = ۴$ و $\tau^{۳}(۱) = \tau(۴) = ۱$. این امر را می‌توان با چشم و تعقیب خطوط منقطع در

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۳ & ۹ & ۴ & ۱ & ۵ & ۶ & ۲ & ۷ & ۸ \end{pmatrix}$$

به‌دست آورد. دور τ معین شده به‌وسیلهٔ ۲ چیست؟ با تعقیب خطوط منقطع در

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۳ & ۹ & ۴ & ۱ & ۵ & ۶ & ۲ & ۷ & ۸ \end{pmatrix}$$

معلوم می‌شود که دور τ معین شده به‌وسیلهٔ ۲ مساوی است با $(۲ \ \ ۹ \ \ ۸ \ \ ۷)$. دور τ معین شده به‌وسیلهٔ ۵ و ۶ به‌ترتیب عبارتند از (۵) و (۶) زیرا ۵ و ۶ توسط τ ثابت می‌مانند. لذا دورهای τ عبارتند

از $(۱\ ۳\ ۴)$، $(۲\ ۹\ ۸\ ۷)$، (۵)، و (۶). بنابراین داریم $\tau = (۱\ ۳\ ۴)(۲\ ۹\ ۸\ ۷)(۵)(۶)$ که در آن این دورها (به‌صورت تعریف شده در فوق) جایگشتهایی در $S_۹$اند زیرا هر عدد صحیح در $S = \{۱, ۲, \dots, ۹\}$ در یک و فقط یک دور ظاهر شده و نقش هر i تحت τ از دوری که در آن ظاهر شده به‌دست می‌آید.

در استدلال فوق چیز خاصی راجع‌به جایگشت τ گفته نشد. پس این استدلال برای هر جایگشت در S_n به ازای هر n برقرار است. اثبات صوری این امر به خواننده محول می‌شود.

قضیهٔ ۲.۲.۳. هر جایگشت در S_n حاصلضرب دورهای از هم‌جدا می‌باشد.

ما در نوشتن جایگشت σ به‌صورت حاصلضربی از دورهای از هم جدا تمام ۱ـدورها را حذف می‌کنیم؛ یعنی iهایی را که $\sigma(i) = i$ نادیده می‌گیریم. مثلاً $\sigma = (۱\ ۲\ ۳)(۴\ ۵)$ در $S_۷$ طریقهٔ نوشتن ما از $\sigma = (۱\ ۲\ ۳)(۴\ ۵)(۶)(۷)$ است. به‌عبارت دیگر، با نوشتن σ به‌صورت حاصلضرب k- دورها به ازای $k > ۱$، فرض می‌کنیم σ هر عدد صحیح غایب در دورها را ثابت می‌گذارد. مثلاً، در گروه $S_{۱۱}$، جایگشت $\tau = (۱\ ۵\ ۶)(۲\ ۳\ ۹\ ۸\ ۷)$ اعداد ۴، ۱۰، و ۱۱ را ثابت می‌گذارد.

لم ۳.۲.۳. هرگاه τ در S_n یک kـ دور باشد، آن‌گاه مرتبهٔ τ مساوی k است؛ یعنی $\tau^k = e$ و به ازای $۰ < j < k$، $\tau^j \neq e$.

حال جایگشت $\tau = (۱\ ۲)(۳\ ۴\ ۵\ ۶)(۷\ ۸\ ۹)$ را در $S_۹$ در نظر می‌گیریم. مرتبهٔ این جایگشت چیست؟ چون دورهای از هم‌جدای $(۱\ ۲)$، $(۳\ ۴\ ۵\ ۶)$، و $(۷\ ۸\ ۹)$ تعویض می‌شوند، $\tau^m = (۱\ ۲)^m(۳\ ۴\ ۵\ ۶)^m(۷\ ۸\ ۹)^m$. برای برقراری $\tau^m = e$ باید $(۱\ ۲)^m = e$، $(۳\ ۴\ ۵\ ۶)^m = e$، و $(۷\ ۸\ ۹)^m = e$. (ثابت کنید!) برای برقراری $(۷\ ۸\ ۹)^m = e$ باید $۳|m$ زیرا $(۷\ ۸\ ۹)$ از مرتبهٔ ۳ است. برای برقراری $(۳\ ۴\ ۵\ ۶)^m = e$ باید $۴|m$ زیرا $(۳\ ۴\ ۵\ ۶)$ از مرتبهٔ ۴ است. و برای برقراری $(۱\ ۲)^m = e$ باید داشته باشیم $۲|m$ زیرا $(۱\ ۲)$ از مرتبهٔ ۲ می‌باشد. این به ما می‌گوید که m باید بر ۱۲ بخشپذیر باشد.

از آن‌سو،

$$\tau^{۱۲} = (۱\ ۲)^{۱۲}(۳\ ۴\ ۵\ ۶)^{۱۲}(۷\ ۸\ ۹)^{۱۲} = e$$

لذا τ از مرتبهٔ ۱۲ می‌باشد.

در اینجا مجدداً خواص ویژهٔ τ وارد کار نمی‌شوند. آنچه برای τ شد برای هر جایگشت قابل

انجام است. برای تنظیم کامل این امر به یاد آورید که کوچکترین مضرب مشترک m و n کوچکترین عدد صحیح مثبت v است که بر m و n بخشپذیر است. (ر.ک. مسئلهٔ ۷، فصل ۱، بخش ۵). در این صورت داریم:

قضیهٔ ۴.۲.۳. فرض کنیم $\sigma \in S_n$ دارای تجزیهٔ دوری به دورهای از هم جدا به طولهای m_1، m_2، $\cdots$، m_k باشد. در این صورت مرتبهٔ σ کوچکترین مضرب مشترک m_1، m_2، $\cdots$، m_k می‌باشد.

برهان. فرض کنیم $\sigma = \tau_1\tau_2\cdots\tau_k$ که در آن τ_iها دورهای از هم جدا به طولهای m_iاند. چون دورهای τ_i از هم‌جدایند، $\tau_i\tau_j = \tau_j\tau_i$. لذا هرگاه M کوچکترین مضرب مشترک m_1، m_2، $\cdots$، m_k باشد، آن‌گاه $\sigma^M = (\tau_1\tau_2\cdots\tau_k)^M = \tau_1^M\tau_2^M\cdots\tau_k^M = e$ (چون که $\tau_i^M = e$ زیرا τ_i از مرتبهٔ m_i است و $m_i|M$). بنابراین مرتبهٔ σ حداکثر M می‌باشد. از آن‌سو، هرگاه $\sigma^N = e$، آن‌گاه $\tau_1^N\tau_2^N\cdots\tau_k^N = e$. از این نتیجه می‌شود که هر $\tau_i^N = e$ (ثابت کنید!) زیرا τ_iها از هم جدایند؛ در نتیجه $m_i|N$ زیرا τ_i از مرتبهٔ m_i می‌باشد. لذا N بر کوچکترین مضرب مشترک m_1، m_2، $\cdots$، m_k بخشپذیر است. پس $M|N$. در نتیجه، همان‌طور که در قضیه حکم شده، σ از مرتبهٔ M می‌باشد. ■

توجه کنید که از هم جدایی دورها در قضیهٔ فوق لازم است. مثلاً (۱ ۲) و (۱ ۳)، که از هم جدا نیستند، هر یک از مرتبهٔ ۲ بوده ولی حاصل ضربشان (۱ ۳ ۲) = (۱ ۳)(۱ ۲) از مرتبهٔ ۳ می‌باشد.

حال قضیهٔ ۴.۲.۳ را در رابطه با بر زدن یک دسته کارت در نظر می‌گیریم. فرض کنید یک دسته مرکب از ۱۳ کارت را طوری بر بزنیم که کارت فوقانی در موضع سوم، کارت دوم در موضع چهارم، $\cdots$، و کارت i م در موضع $i + ۲$ م (با ۱۳ mod) قرار گیرد. σی مربوط به این بر، به‌عنوان یک جایگشت از اعداد ۱، ۲، $\cdots$، ۱۳، به‌صورت زیر در می‌آید:

$$\sigma = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ & ۱۰ & ۱۱ & ۱۲ & ۱۳ \\ ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ & ۱۰ & ۱۱ & ۱۲ & ۱۳ & ۱ & ۲ \end{pmatrix}$$

و σ چیزی جز ۱۳ـدور (۱ ۳ ۵ ۷ ۹ ۱۱ ۱۳ ۲ ۴ ۶ ۸ ۱۰ ۱۲) نیست. پس σ از مرتبهٔ ۱۳ می‌باشد. چند بار باید این بر تکرار شود تا دسته کارت به‌ترتیب اصلی باز گردد؟ جواب چیزی جز مرتبهٔ σ، یعنی عدد ۱۳، نیست. لذا باید ۱۳ بار بر بزنیم تا کارتها به‌ترتیب اصلی‌شان باز گردند.

حال بر فوق را پیچ می‌دهیم. فرض کنید کارتها را به‌صورت زیر بر بزنیم. ابتدا کارت فوقانی را در موضع دوم از آخر قرار داده و سپس بر زدن فوق را تعقیب می‌کنیم. چند تکرار لازم است تا کارتها به‌ترتیب اصلی بازگردند؟ اولین بر طبق جایگشت $\tau = (۱\ ۱۲\ ۱۱\ ۱۰\ ۹\ ۸\ ۷\ ۶\ ۵\ ۴\ ۳\ ۲)$ صورت می‌گیرد و سپس σی فوق اعمال می‌شود. لذا باید $\sigma\tau$ را حساب کرده و مرتبه‌اش را بیابیم. اما

$$\begin{aligned}\sigma\tau &= (۱\ ۳\ ۵\ ۷\ ۹\ ۱۱\ ۱۳\ ۲\ ۴\ ۶\ ۸\ ۱۰\ ۱۲)\\ &\times (۱\ ۱۲\ ۱۱\ ۱۰\ ۹\ ۸\ ۷\ ۶\ ۵\ ۴\ ۳\ ۲)\\ &= (۱)(۲\ ۳\ ۴\ ۵\ ۶\ ۷\ ۸\ ۹\ ۱۰\ ۱۱\ ۱۲\ ۱۳)\end{aligned}$$

پس مرتبه‌اش ۱۲ می‌باشد. لذا ۱۲ بار باید بر بزنیم تا به وضع اصلی بازگردیم.

آیا می‌توان ۱۳ کارت را طوری بر زد که ۴۲ تکرار یا ۲۰ تکرار لازم باشد؟ چه بری بیشترین تکرار را می‌خواهد و این عدد چند است؟

حال به بحث کلی باز می‌گردیم. جایگشت $(۱\ ۲\ ۳)$ را در نظر می‌گیریم. ملاحظه می‌کنیم که $(۱\ ۲\ ۳) = (۱\ ۳)(۱\ ۲)$. همچنین می‌بینیم که $(۱\ ۲\ ۳) = (۲\ ۳)(۱\ ۳)$. لذا دو مطلب واضح است. ابتدا می‌توان $(۱\ ۲\ ۳)$ را به‌صورت حاصلضرب دو ترانهش و دست‌کم به دو صورت متمایز نوشت. هرگاه $(i_۱, i_۲, \ldots, i_k)$ یک kـدور باشد، آن‌گاه

$$(i_۱\ i_۲\ \cdots\ i_k) = (i_۱\ i_k)(i_۱\ i_{k-۱})\cdots(i_۱\ i_۲).$$

لذا هر kـدور حاصلضرب $k - ۱$ ترانهش (اگر $k > ۱$) است و این امر را می‌توان به چند طریق (و نه فقط به یک طریق) انجام داد. از آنجا که هر جایگشت حاصلضرب دورهای از هم جدا و هر دور حاصلضربی از ترانهشهاست، خواهیم داشت:

قضیهٔ ۵.۲.۳. هر جایگشت در S_n حاصلضربی از ترانهشها می‌باشد.

این قضیه چندان تعجب‌آور نیست زیرا فقط می‌گوید که هر جایگشت عبارت است از یک سری از تعویضهای دو شیء در هر لحظه.

دیدیم که در نمایش یک جایگشت به‌صورت حاصلضربی از ترانهشها یکتایی وجود ندارد. ولی، همان‌طور که در بخش ۳ خواهیم دید، بعضی از جنبه‌های این تجزیه واقعاً منحصر به‌فرداند.

مسائل

مسائل آسانتر

۱. نشان دهید که اگر σ و τ دو دور از هم جدا باشند، $\sigma\tau = \tau\sigma$.

۲. تجزیهٔ دوری و مرتبه را در هر مورد بیابید:

الف) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۳ & ۱ & ۴ & ۲ & ۷ & ۶ & ۹ & ۸ & ۵ \end{pmatrix}$؛

ب) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۷ & ۶ & ۵ & ۴ & ۳ & ۲ & ۱ \end{pmatrix}$؛

پ) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۷ & ۶ & ۵ & ۳ & ۴ & ۲ & ۱ \end{pmatrix} \times \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۲ & ۳ & ۱ & ۵ & ۶ & ۷ & ۴ \end{pmatrix}$.

۳. هر مورد را به‌صورت حاصلضرب دورهای از هم جدا بیان کرده و مرتبه‌اش را بیابید:

الف) $(۱\ ۲\ ۳\ ۵\ ۷)(۲\ ۴\ ۷\ ۶)$؛

ب) $(۱\ ۲)(۱\ ۳)(۱\ ۴)$؛

پ) $(۱\ ۲\ ۳\ ۴\ ۵)(۱\ ۲\ ۳\ ۴\ ۶)(۱\ ۲\ ۳\ ۴\ ۷)$؛

ت) $(۱\ ۲\ ۳)(۱\ ۳\ ۲)$؛

ث) $(۱\ ۲\ ۳)(۳\ ۵\ ۷\ ۹)(۱\ ۲\ ۳)^{-۱}$؛

ج) $(۱\ ۲\ ۳\ ۴\ ۵)^{۳}$.

۴. قضیهٔ ۲.۲.۳ را به‌طور کامل ثابت کنید.

۵. نشان دهید که هر k-دور از مرتبهٔ k است.

۶. یک دسته کارت ۱۳ تایی را طوری بر بزنید که برای بازگشت به ترتیب اصلی ۴۲ تکرار لازم باشد.

۷. مسئلهٔ ۶ را در صورتی حل کنید که ۲۰ تکرار لازم باشد.

۸. جایگشتهای مسئلهٔ ۳ را به‌صورت حاصلضربی از ترانهشها بیان دارید.

۹. به ازای دو ترانهش $(۱\ ۲)$ و $(۱\ ۳)$، جایگشت σ را طوری بیابید که $\sigma(۱\ ۲)\sigma^{-۱} = (۱\ ۳)$.

۱۰. ثابت کنید جایگشتی مانند σ که $\sigma(۱\ ۲)\sigma^{-۱} = (۱\ ۲\ ۳)$ وجود ندارد.

۱۱. ثابت کنید جایگشتی مانند σ که $\sigma(۱\ ۲\ ۳)\sigma^{-۱} = (۴\ ۵\ ۶)$ وجود دارد.

۱۲. ثابت کنید جایگشتی مانند σ که $\sigma(۱\ ۲\ ۳)\sigma^{-۱} = (۱\ ۲\ ۴)(۵\ ۶\ ۷)$ وجود ندارد.

مسائل با سطح متوسط

۱۳. ثابت کنید $(1 \quad 2)$ را نمی‌توان به‌صورت حاصلضربی از ۳ـدورهای از هم جدا نوشت.

۱۴. ثابت کنید اگر τ یک ترانهش باشد، $\sigma\tau\sigma^{-1}$ نیز به ازای هر جایگشت σ یک ترانهش است.

۱۵. نشان دهید هرگاه τ یک kـدور باشد، آن‌گاه $\sigma\tau\sigma^{-1}$ نیز به ازای هر جایگشت σ یک kـدور است.

۱۶. به فرض آنکه φ یک خودریختی از S_3 باشد، نشان دهید که عنصری مانند $\sigma \in S_3$ هست به‌طوری که به ازای هر $\tau \in S_3$، $\varphi(\tau) = \sigma^{-1}\tau\sigma$.

۱۷. به فرض آنکه $(1 \quad 2)$ و $(1 \quad 2 \quad 3 \quad \cdots \quad n)$ در S_n باشند، نشان دهید که هر زیرگروه S_n شامل هر دوی اینها باید تمام S_n باشد (لذا این دو جایگشت S_n را تولید می‌کنند).

۱۸. اگر τ_1 و τ_2 ترانهش باشند، نشان دهید که $\tau_1\tau_2$ را می‌توان به‌صورت حاصلضربی از ۳ـدورهای نه لزوماً از هم جدا بیان کرد.

۱۹. ثابت کنید هرگاه τ_1، τ_2، و τ_3 ترانهش باشند، آن‌گاه $\tau_1\tau_2\tau_3 \neq e$ (عنصر همانی S_n).

۲۰. اگر τ_1 و τ_2 ترانهشهای متمایزی باشند، نشان دهید که $\tau_1\tau_2$ از مرتبهٔ ۲ یا ۳ است.

۲۱. اگر دو جایگشت σ و τ حرف مشترکی نداشته باشند و $\sigma\tau = e$، ثابت کنید $\sigma = \tau = e$.

۲۲. برای یافتن $\sigma\tau\sigma^{-1}$ به ازای جایگشتهای σ و τ از S_n یک الگوریتم بیابید.

۲۳. فرض کنید جایگشتهای σ و τ دارای تجزیه به دورهای از هم جدا به طولهای m_1، m_2، $\cdots$، m_k باشند. (گوییم این جایگشتها دارای تجزیه‌های مشابه به دورهای از هم جدایند.) ثابت کنید به ازای جایگشتی مانند ρ، $\tau = \rho\sigma\rho^{-1}$.

۲۴. ردهٔ تزویج $(1 \quad 2 \quad \cdots \quad n)$ در S_n را بیابید. مرتبهٔ مرکزساز $(1 \quad 2 \quad \cdots \quad n)$ در S_n چیست؟

۲۵. مسئلهٔ ۲۴ را برای $\sigma = (1 \quad 2)(3 \quad 4)$ حل کنید.

۳. جایگشتهای فرد و زوج

در بخش ۲ دیدیم که اگر چه هر جایگشت حاصلضربی از ترانهشهاست ولی این تجزیه منحصر به‌فرد نیست. با این حال گفتیم که بعضی از جنبه‌های این تجزیه منحصر به فردند. حال وارد این بحث می‌شویم.

حالت خاص S_3 را در نظر می‌گیریم که در آن بتوان همه‌چیز را به وضوح دید. فرض کنیم $f(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ عبارتی از سه متغیر x_1، x_2، x_3 باشد. همچنین S_3 بر $f(x) = f(x_1, x_2, x_3)$ به‌صورت زیر عمل کند. هرگاه $\sigma \in S_3$، آن‌گاه

$$\sigma^*(f(x)) = (x_{\sigma(1)} - x_{\sigma(2)})(x_{\sigma(1)} - x_{\sigma(3)})(x_{\sigma(2)} - x_{\sigma(3)})$$

حال عمل σ^* را بر $f(x)$ به ازای چند σ در S_3 در نظر می‌گیریم.

فرض کنیم $\sigma = (1\ \ 2)$. در این صورت $\sigma(1) = 2$، $\sigma(2) = 1$، و $\sigma(3) = 3$؛ در نتیجه

$$\begin{aligned}
\sigma^*(f(x)) &= (x_{\sigma(1)} - x_{\sigma(2)})(x_{\sigma(1)} - x_{\sigma(3)})(x_{\sigma(2)} - x_{\sigma(3)}) \\
&= (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) \\
&= -(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \\
&= -f(x)
\end{aligned}$$

لذا σ^* ناشی از $\sigma = (1\ \ 2)$ علامت $f(x)$ را تغییر می‌دهد. حال به عمل عنصر $\tau = (1\ \ 2\ \ 3)$ از S_3 بر $f(x)$ نگاه می‌کنیم. در این صورت

$$\begin{aligned}
\tau^*(f(x)) &= (x_{\tau(1)} - x_{\tau(2)})(x_{\tau(1)} - x_{\tau(3)})(x_{\tau(2)} - x_{\tau(3)}) \\
&= (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) \\
&= (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \\
&= f(x)
\end{aligned}$$

پس τ^* ناشی از $\tau = (1\ \ 2\ \ 3)$، $f(x)$ را ثابت می‌گذارد. سایر جایگشتهای S_3 چطور؛ آنها چه اثری بر $f(x)$ دارند؟ البته عنصر همانی e نگاشت e^* را بر $f(x)$ القا می‌کند که $f(x)$ را تغییر نمی‌دهد. τ^2 به ازای τ فوق چه اثری بر $f(x)$ دارد؟ چون $\tau^* f(x) = f(x)$، فوراً معلوم می‌شود که

$$\begin{aligned}
(\tau^2)^*(f(x)) &= (x_{\tau^2(1)} - x_{\tau^2(2)})(x_{\tau^2(1)} - x_{\tau^2(3)})(x_{\tau^2(2)} - x_{\tau^2(3)}) \\
&= f(x) \qquad \text{(ثابت کنید!)}
\end{aligned}$$

حال $\sigma\tau = (1\ \ 2)(1\ \ 2\ \ 3) = (2\ \ 3)$ را در نظر می‌گیریم. چون τ، $f(x)$ را راحت گذاشته و σ علامت $f(x)$ را تغییر می‌دهد، $\sigma\tau$ باید علامت $f(x)$ را تغییر دهد. به همین نحو $(1\ \ 3)$ علامت $f(x)$ را تغییر می‌دهد. پس عمل هر عنصر S_3 بر $f(x)$ مشخص است.

فرض کنیم $\rho \in S_3$ حاصلضرب $\rho = \tau_1\tau_2\cdots\tau_k$ از ترانهشهای τ_1، $\cdots$، τ_k باشد. ρ در عمل بر $f(x)$ علامت $f(x)$ را k بار تغییر می‌دهد زیرا هر τ_i علامت $f(x)$ را تغییر می‌دهد. لذا $\rho^*(f(x)) = (-1)^k f(x)$. اگر $\rho = \sigma_1\sigma_2\cdots\sigma_t$ که در آن σ_1، $\cdots$، σ_t ترانهش باشند، طبق همین استدلال، $\rho^*(f(x)) = (-1)^t f(x)$. لذا $(-1)^t f(x) = (-1)^k f(x)$ که از آنجا

$(-۱)^k = (-۱)^t$. این به ما می‌گوید که t و k جفتی یکسان دارند؛ یعنی اگر t فرد باشد، k باید فرد باشد، و اگر t زوج باشد، k باید زوج باشد.

این امر به ما می‌گوید که اگر تجزیهٔ جایگشت σ به‌صورت حاصلضربی از ترانهشها منحصر به‌فرد نیست، جفتی تعداد ترانهشها در این تجزیهٔ σ ممکن است منحصر به‌فرد باشد.

حال، در تلاش به سوی این هدف، به خواننده پیشنهاد می‌کنیم که استدلال مذکور در حالت خاص $n = ۳$ را برای n دلخواه بیان دارد.

همان‌طور که در بالا ذکر شد، $f(x) = f(x_۱, \ldots, x_n)$ را به‌صورت زیر تعریف می‌کنیم:

$$\begin{aligned} f(x) &= (x_۱ - x_۲)(x_۱ - x_۳)\cdots(x_۱ - x_n)(x_۲ - x_۳)(x_۲ - x_۴) \\ &\quad \times \cdots(x_۲ - x_n)\cdots(x_{n-۱} - x_n) \\ &= \prod_{i<j}(x_i - x_j) \end{aligned}$$

که در آن i تمام مقادیر از ۱ تا $n - ۱$ و j تمام مقادیر از ۲ تا n را می‌گیرد. اگر $\sigma \in S_n$، σ^* را بر $f(x)$ به‌صورت زیر تعریف می‌کنیم:

$$\sigma^*(f(x)) = \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)})$$

هرگاه $\sigma, \tau \in S_n$، آن‌گاه

$$\begin{aligned} (\sigma\tau)^*(f(x)) &= \prod_{i<j}(x_{(\sigma\tau)(i)} - x_{(\sigma\tau)(j)}) = \sigma^*\left(\prod_{i<j}(x_{\tau(i)} - x_{\tau(j)})\right) \\ &= \sigma^*(\tau^*(\prod_{i<j}(x_i - x_j)) = \sigma^*(\tau^* f(x)) = (\sigma^*\tau^*)(f(x)) \end{aligned}$$

لذا در عمل بر $f(x)$ داریم $(\sigma\tau)^* = \sigma^*\tau^*$.

ترانهش τ بر $f(x)$ چه می‌کند؟ حکم می‌کنیم که $\tau^*(f(x)) = -f(x)$. برای اثبات این امر فرض کنیم $\tau = (i \quad j)$ که در آن $i < j$ و تعداد $(x_u - x_v)$ها با $u < v$ را که به یک $(x_a - x_b)$ با $a > b$ تبدیل شده‌اند حساب می‌کنیم. این برای $(x_u - x_j)$ اگر $i < u < j$، برای $(x_i - x_v)$ اگر $i < v < j$، و بالاخره برای $(x_i - x_j)$ رخ می‌دهد. هر یک از اینها به تغییر علامتی برای $f(x)$ منجر می‌شود و چون از اینها $۲(j - i - ۱) + ۱$ تا وجود دارد، که تعدادی فرد است، وقتی τ^* بر $f(x)$ عمل کند، تعدادی فرد تغییر علامت حاصل می‌شود. لذا $\tau^*(f(x)) = -f(x)$. بنابراین حکم ما که به ازای هر ترانهش τ، $\tau^*(f(x)) = -f(x)$ تأیید می‌گردد.

هرگاه σ جایگشتی در S_n بوده و $\sigma = \tau_1\tau_2\cdots\tau_k$ که در آن τ_1، τ_2، $\cdots$، τ_k ترانهش باشند، آن‌گاه در عمل بر $f(x)$ داریم $\sigma^* = (\tau_1\tau_2\cdots\tau_k)^* = \tau_1^*\tau_2^*\cdots\tau_k^*$، و چون هر $\tau_i^*(f(x)) = -f(x)$، معلوم می‌شود که $\sigma^*(f(x)) = (-1)^k f(x)$. به همین نحو، هرگاه $\sigma = \xi_1\xi_2\cdots\xi_t$ که در آن ξ_1، ξ_2، $\cdots$، ξ_t ترانهش‌اند، آن‌گاه $\sigma^*(f(x)) = (-1)^t f(x)$. از مقایسهٔ این دو مقدار برای $\sigma^*(f(x))$ نتیجه می‌گیریم که $(-1)^t = (-1)^k$. لذا این دو تجزیهٔ σ به حاصلضرب ترانهشها دارای جفتی یکسان می‌باشند. بنابراین هر جایگشت یا حاصلضرب تعدادی فرد از ترانهشهاست یا حاصلضرب تعدادی زوج از ترانهشها، و هیچ حاصلضرب تعدادی زوج ترانهش نمی‌تواند مساوی حاصلضرب تعدادی فرد ترانهش باشد.

این امر تعریف زیر را پیشنهاد می‌کند.

تعریف. جایگشت $\sigma \in S_n$ یک جایگشت فرد است اگر σ حاصلضرب تعدادی فرد ترانهش باشد، و یک جایگشت زوج است اگر σ حاصلضرب تعدادی زوج ترانهش باشد.

آنچه در فوق ثابت شد به قرار زیر می‌باشد.

قضیهٔ ۱.۳.۳. هر جایگشت در S_n یا فرد است یا زوج ولی نه هر دو.

به کمک قضیهٔ ۱.۳.۳ می‌توان چند نتیجه گرفت.

فرض کنیم A_n مجموعهٔ تمام جایگشتهای زوج باشد. هرگاه $\sigma, \tau \in A_n$، آن‌گاه فوراً داریم $\sigma\tau \in A_n$. چون A_n یک زیرمجموعهٔ بستهٔ متناهی از گروه (متناهی) S_n است، طبق لم ۲.۳.۲ زیرگروهی از S_n می‌باشد. A_n را گروه متناوب از درجهٔ n می‌نامیم.

به طریقی دیگر می‌توان نشان داد که A_n زیرگروه S_n است. دیدیم که A_n تحت ضرب بسته است. پس برای آنکه A_n زیرگروه S_n باشد کافی است نشان دهیم که $\sigma \in S_n$ رابطهٔ $\sigma^{-1} \in S_n$ را ایجاب می‌کند. به ازای هر جایگشت σ حکم می‌کنیم که σ و σ^{-1} جفتی یکسان دارند. چرا؟ چون که هرگاه $\sigma = \tau_1\tau_2\cdots\tau_k$ که در آن τ_iها ترانهش‌اند، آن‌گاه

$$\sigma^{-1} = (\tau_1\tau_2\cdots\tau_k)^{-1} = \tau_k^{-1}\tau_{k-1}^{-1}\cdots\tau_2^{-1}\tau_1^{-1} = \tau_k\tau_{k-1}\cdots\tau_2\tau_1$$

زیرا $\tau_i^{-1} = \tau_i$. لذا جفتی σ و σ^{-1} مساوی $(-1)^k$ است؛ در نتیجه جفتی مساوی خواهند داشت. این امر نشان می‌دهد که $\sigma \in A_n$ رابطهٔ $\sigma^{-1} \in A_n$ را ایجاب می‌کند که از آنجا A_n زیرگروه S_n می‌باشد.

ولی این امر بیش از این را نشان می‌دهد و آن این است که A_n زیرگروه نرمال S_n می‌باشد.

زیرا فرض کنیم $\sigma \in A_n$ و $\rho \in S_n$. جفتی $\rho^{-1}\sigma\rho$ چیست؟ طبق استدلال فوق، ρ و ρ^{-1} جفتی یکسان دارند و σ یک جایگشت زوج است. پس $\rho^{-1}\sigma\rho$ جایگشت زوجی است و لذا در A_n می‌باشد. بنابراین A_n زیرگروه نرمالی از S_n می‌باشد.

حال مطلب فوق را در قضیهٔ زیر خلاصه می‌کنیم.

قضیهٔ ۲.۳.۳. A_n، یعنی گروه متناوب از درجهٔ n، یک زیرگروه نرمال S_n است.

حال به این امر از طریقی دیگر نگاه می‌کنیم. از تعاریف مربوطه می‌توان قواعد سادهٔ زیر را برای ضرب جایگشتها وضع کرد:

۱. حاصلضرب دو جایگشت زوج زوج است؛

۲. حاصلضرب دو جایگشت فرد زوج است؛

۳. حاصلضرب یک جایگشت زوج در یک جایگشت فرد (یا یک جایگشت فرد در یک جایگشت زوج) فرد است.

اگر σ یک جایگشت زوج باشد، قرار می‌دهیم $\theta(\sigma) = ۱$، و اگر σ یک جایگشت فرد باشد، قرار می‌دهیم $\theta(\sigma) = -۱$. قواعد فوق راجع‌به ضرب به‌صورت $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$ در می‌آیند. پس θ یک همریختی از S_n به روی گروه $E = \{۱, -۱\}$ از مرتبهٔ ۲ تحت ضرب است. هستهٔ N همریختی θ چیست؟ از تعریف A_n معلوم می‌شود که $N = A_n$. لذا، طبق قضیهٔ اول همریختی، $S_n/A_n \approx E$. لذا، اگر $n > ۱$، $۲ = |E| = |S_n/A_n| = |S_n|/|A_n|$. از این داریم $|A_n| = \frac{۱}{۲}|S_n| = \frac{۱}{۲}n!$.

بنابراین،

قضیهٔ ۳.۳.۳. A_n، به ازای $n > ۱$، یک زیرگروه نرمال S_n از مرتبهٔ $\frac{۱}{۲}n!$ است.

نتیجه. به ازای $n > ۱$، تعداد جایگشتهای زوج در S_n مساوی $\frac{۱}{۲}n!$ و تعداد جایگشتهای فرد در آن برابر $\frac{۱}{۲}n!$ می‌باشد.

پیش از اتمام این بخش چند کلمه راجع‌به برهان قضیهٔ ۱.۳.۳ بیان می‌کنیم. برای قضیهٔ ۱.۳.۳ برهانهای متفاوتی در دست است. بی‌پرده بگوییم که ما هیچیک از آنها را نمی‌پسندیم. برخی درگیر چیزی هستند که ما آن را یک «فرایند گردایه‌ای» می‌نامیم که در آن شخص می‌کوشد نشان دهد که ρ را نمی‌توان به‌صورت حاصلضرب تعداد فردی ترانهش نوشت با این فرض که یک

چنین حاصلضرب کوتاهترین حاصلضرب است و سپس با ترفندهای مناسب این حاصلضرب را کوتاهتر کرده و تناقضی به‌دست آورد. سایر برهانها از طرحهایی دیگر استفاده می‌کنند. در برهان ما از تابع $f(x)$ استفاده می‌شود که به نوعی نسبت به کل ماجرا بیگانه است. ولی این برهان احتمالاً از سایر برهانها ملموستر است و به همین دلیل آن را اختیار کرده‌ایم.

بالاخره گروه A_n به ازای $n \geq ۵$ گروه بسیار جالبی است. در فصل ۶ نشان می‌دهیم که تنها زیرگروههای نرمال A_n، به ازای $n \geq ۵$، عبارتند از (e) و خود A_n. هر گروه غیرآبلی واجد این خاصیت یک گروه ساده نام دارد (با یک گروه آسان اشتباه نشود). لذا A_n به ازای $n \geq ۵$ خانواده‌ای نامتناهی از گروههای ساده به ما می‌دهد. خانواده‌های نامتناهی دیگری نیز از گروههای سادهٔ متناهی وجود دارند. در ۲۰ سال گذشته گروهی جبردان با تلاش فوق‌العادهٔ خود تمام گروههای سادهٔ متناهی را معین کرده‌اند. تعیین این گروههای ساده تقریباً ۱۰۰۰۰ صفحهٔ چاپی را اشغال کرده است. جالب آنکه هر گروه سادهٔ متناهی باید مرتبهٔ زوج داشته باشد.

مسائل

مسائل آسانتر

۱. جفتی هر جایگشت زیر را بیابید:

الف) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۲ & ۴ & ۵ & ۱ & ۳ & ۷ & ۸ & ۹ & ۶ \end{pmatrix}$؛

ب) $(۱\ ۲\ ۳\ ۴\ ۵\ ۶)(۷\ ۸\ ۹)$؛

پ) $(۱\ ۲\ ۳\ ۴\ ۵\ ۶)(۱\ ۲\ ۳\ ۴\ ۵\ ۷)$؛

ت) $(۱\ ۲)(۱\ ۲\ ۳)(۴\ ۵)(۵\ ۶\ ۸)(۱\ ۷\ ۹)$.

۲. اگر σ یک kـدور باشد، نشان دهید که σ به ازای kی زوج جایگشتی فرد و به ازای kی فرد جایگشتی زوج می‌باشد.

۳. ثابت کنید به ازای هر $\sigma, \tau \in S_n$، σ و $\tau^{-۱}\sigma\tau$ جفتی یکسان دارند.

۴. اگر $m < n$، $S_m \subset S_n$ را می‌توان با توجه به عمل $\sigma \in S_m$ بر ۱، ۲، ...، m، ...، n به صورتی که بر ۱، ۲، ...، m کرده است و σ، $j > m$ را ثابت می‌گذارد در نظر گرفت. ثابت کنید جفتی یک جایگشت در S_m وقتی به این صورت عنصری از S_n ملحوظ شود تغییری نمی‌کند.

۵. فرض کنید جایگشت

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۳ & ۱ & ۲ & & & ۷ & ۸ & ۹ & ۶ \end{pmatrix}$$

در $S_۹$، که در آن نقشهای ۴ و ۵ گم شده‌اند، یک جایگشت زوج باشد. نقشهای ۴ و ۵ چه باید باشند؟

مسائل با سطح متوسط

۶. اگر $n \geq ۳$، نشان دهید که هر عنصر در A_n حاصلضربی از ۳ـدورهاست.

۷. نشان دهید که هر عنصر در A_n حاصلضربی از nـدورهاست.

۸. یک زیرگروه نرمال در $A_۴$ از مرتبهٔ ۴ بیابید.

مسائل مشکلتر (در واقع بسیار مشکل)

۹. اگر $n \geq ۵$ و $(e) \neq N \subset A_n$ زیرگروه نرمالی از A_n باشد، نشان دهید که N باید شامل یک ۳ـ دور باشد.

۱۰. با استفاده از مسئلهٔ ۹ نشان دهید که اگر $n \geq ۵$، تنها زیرگروههای نرمال A_n عبارتند از (e) و خود A_n. (لذا گروههای A_n به ازای $n \geq ۵$ یک خانوادهٔ نامتناهی از گروههای ساده تشکیل می‌دهند.)

۴

نظریهٔ حلقه‌ها

۱. چند تعریف و چند مثال

تا به حال در مطالعهٔ جبر مجرد با نوعی از دستگاه مجرد آشنا شده‌ایم که در جبر امروز نقش اصلی را دارد. این دستگاه عبارت بود از گروه. هر گروه دستگاهی جبری با فقط یک عمل است و لازم نیست در قاعدهٔ $ab = ba$ صدق کند که با تجربهٔ قبلی ما در جبر تعارض دارد. ما با دستگاههایی خوکرده‌ایم که در آنها می‌توان عناصر را جمع و ضرب کرد و عنصرها در قانون تعویضپذیری ضرب $ab = ba$ صدق می‌کنند. به‌علاوه، این دستگاههای آشنا معمولاً از مجموعه‌های اعداد (صحیح، گویا، حقیقی، و گاهی مختلط) ناشی شده‌اند.

مفهوم جبری دیگری که در نظر می‌گیریم حلقه است. این دستگاه از بسیاری جهات بیش از گروهها یادآور اطلاعات قبلی ما می‌باشد. حلقه‌ها از یک‌سو صاحب جمع و ضرب بوده و این اعمال تحت بسیاری از قواعد آشنایی که از حساب می‌دانیم قرار دارند. از سوی دیگر لازم نیست حلقه‌ها از دستگاههای اعداد معمولی ناشی شوند و، در واقع، با این موارد آشنا سروکار کمی دارد. با آنکه بسیاری از قواعد صوری حساب برقرارند، پدیده‌های عجیب (یا به ظاهر عجیب) زیادی رخ می‌دهند. همان‌طور که پیش رفته و مثالهایی از حلقه‌ها را می‌بینیم، به بعضی از آنها برخواهیم خورد.

حال با این مقدمات آمادهٔ شروع بحث می‌باشیم. طبعاً اولین کار باید تعریف چیزی باشد که راجع به آن سخن خواهیم گفت.

تعریف. گوییم مجموعهٔ ناتهی R یک حلقه است اگر در R دو عمل $+$ و $\cdot$ موجود باشند به‌طوری که

الف) $a, b \in R$ ایجاب کنند که $a + b \in R$؛

ب) به ازای $a, b \in R$، $a + b = b + a$؛

پ) به ازای $a, b, c \in R$، $(a + b) + c = a + (b + c)$؛

ت) عنصری مانند $0 \in R$ موجود باشد به‌طوری که به ازای هر $a \in R$، $a + 0 = a$؛

ث) به ازای هر $a \in R$ عنصری مانند $b \in R$ موجود باشد به‌طوری که $a + b = 0$. (ما b را به‌صورت $-a$ خواهیم نوشت.)

ما تاکنون گفته‌ایم که R تحت $+$ یک گروه آبلی است. حال قواعد ضرب در R را بیان می‌کنیم.

ج) $a, b \in R$ ایجاب کنند که $a \cdot b \in R$؛

چ) به ازای $a, b, c \in R$، $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

این تا جایی که به ضرب مربوط است کل مطلب ما می‌باشد. ولی $+$ و $\cdot$ مجاز نیستند که در انزوا بمانند. ما آنها را با دو قانون پخشپذیری به هم خواهیم بافت:

ح) به ازای $a, b, c \in R$،

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

و

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

اصول موضوع فوق آشنا به نظر می‌رسند. باید این‌طور باشد چرا که مفهوم حلقه تعمیمی است از خواص اعداد صحیح. به خاطر اصل موضوع (چ)، یعنی قانون شرکتپذیری ضرب، حلقه‌هایی که ما تعریف کرده‌ایم معمولاً حلقه‌های شرکتپذیر نام دارند. حلقه‌های شرکت‌ناپذیر نیز وجود دارند و برخی از آنها نقش مهمی در ریاضیات ایفا می‌کنند. ولی ما در اینجا به آنها توجهی نداریم. لذا، هر جا از واژهٔ «حلقه» استفاده کنیم، منظورمان «حلقهٔ شرکتپذیر» می‌باشد.

با آنکه اصول موضوع (آ) تا (ح) آشنایند، نکاتی هست که توسط آنها بازگو نمی‌شود. حال به چند قاعدهٔ آشنا نگاه می‌کنیم که در یک حلقهٔ کلی رویشان تأکید نمی‌شود.

اولاً وجود عنصری مانند $1 \in R$ که به ازای هر $a \in R$، $a \cdot 1 = 1 \cdot a = a$ اصل موضوع نشده است. بسیاری از مثالهایی که با آنها مواجه می‌شویم این عنصر را دارند و در این صورت گوییم R یک حلقهٔ یکدار است. بسیاری از جبردانان شرط می‌کنند که هر حلقه عنصر یکه دارد. ما تأکید می‌کنیم که $0 \neq 1$؛ یعنی حلقهٔ مرکب از فقط 0 یک حلقهٔ یکدار نیست.

ثانیاً، در تجربیات قبلی ما از این نوع اشیاء، هر وقت $a \cdot b = 0$ نتیجه می‌گرفتیم که $a = 0$ یا $b = 0$. این در یک حلقهٔ کلی لزوماً درست نیست. وقتی این برقرار باشد، حلقه حلقه‌ای مناسب بوده و نامی خاص خواهد داشت. ما این نوع حلقه را یک قلمرو می‌نامیم.

ثالثاً در یک حلقه اصول موضوعی که قانون تعویضپذیری $a \cdot b = b \cdot a$ ضرب را ایجاب کنند ذکر نشده است. حلقه‌هایی تعویض‌ناپذیر وجود دارند که در آنها این قانون برقرار نیست. ما به‌زودی به بعضی از آنها بر خواهیم خورد. در این فصل توجه اصلی ما به حلقه‌های تعویضپذیر است ولی، در بسیاری از نتایج اولیه، تعویضپذیری در حلقه‌ها فرض نخواهد شد.

همان‌طور که در بالا گفتیم، بعضی چیزها حلقه‌ها را جالبتر می‌سازند و لذا شایسته است نامی خاص به این حلقه‌ها بدهیم. ما به سرعت تعاریف مربوط به بعضی از این حلقه‌های جالب را ذکر خواهیم کرد.

تعریف. حلقهٔ تعویضپذیر R یک قلمرو صحیح است اگر $a \cdot b = 0$ در R ایجاب کند که $a = 0$ یا $b = 0$.

در بعضی از کتب جبر قید می‌کنند که هر قلمرو صحیح شامل عنصر یکه است. لذا خواننده باید در خواندن کتب دیگر مواظب این امر باشد. مجموعهٔ اعداد صحیح $\mathbb{Z}$ مثال آشکاری است از یک قلمرو صحیح. ما مثالهای کمتر آشنای دیگر را نیز خواهیم دید.

تعریف. حلقهٔ یکدار R را یک حلقهٔ بخشی گوییم اگر به ازای هر $a \neq 0$ در R عنصری مانند $b \in R$ (که معمولاً به‌صورت a^{-1} نوشته می‌شود) موجود باشد به‌طوری که $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

دلیل حلقهٔ بخشی نامیدن این حلقه کاملاً واضح است زیرا در آنها می‌توان (دست‌کم با رعایت طرفهای چپ و راست) بخش کرد. با آنکه حلقه‌های بخشی تعویض‌ناپذیر وجود دارند و نقش مهمی در جبر تعویض‌ناپذیر ایفا می‌کنند، ولی نسبتاً پیچیده بوده و ما فقط یک مثال از آنها را ذکر خواهیم کرد. این حلقهٔ بخشی مثالی است بسیار کلاسیک که در سال ۱۸۴۳ توسط هامیلتون معرفی شد و به حلقهٔ چهارگانها معروف است. (ر.ک. مثال ۱۳ زیر.)

بالاخره به جالبترین رده از حلقه‌ها، یعنی میدانها، می‌رسیم.

تعریف. گوییم حلقهٔ R یک میدان است اگر R یک حلقهٔ بخشی تعویضپذیر باشد.

به‌عبارت دیگر، هر میدان یک حلقهٔ تعویضپذیر است که در آن می‌توان آزادانه بر عناصر ناصفر تقسیم کرد. به دیگر سخن، R درصورتی یک میدان است که عناصر ناصفر R تحت $\cdot$ (یعنی

ضرب در R) یک گروه آبلی تشکیل دهند.

برای میدانها چند مثال آماده داریم: اعداد گویا، اعداد حقیقی، و اعداد مختلط. ولی مثالهایی دیگر که شاید کمتر آشنایند را نیز خواهیم دید. فصل ۵ به بررسی میدانها اختصاص یافته است.

ما تا آخر این بخش به چند مثال از حلقه‌ها می‌پردازیم. همچنین علامت $\cdot$ برای ضرب را حذف کرده، و $a \cdot b$ را فقط به‌صورت ab می‌نویسیم.

چند مثال

۱. اولین مثال ما از حلقه‌ها حلقهٔ اعداد صحیح $\mathbb{Z}$ تحت جمع و ضرب معمولی این اعداد است. $\mathbb{Z}$ طبعاً یک قلمرو صحیح می‌باشد.

۲. دومین مثال نیز همین‌قدر واضح است. فرض کنیم $\mathbb{Q}$ مجموعهٔ اعداد گویا باشد. همان‌طور که می‌دانید، $\mathbb{Q}$ در تمام قواعد لازم برای یک میدان صدق می‌کند؛ در نتیجه $\mathbb{Q}$ یک میدان می‌باشد.

۳. مجموعهٔ اعداد حقیقی $\mathbb{R}$ نیز مثالی از یک میدان است.

۴. مجموعهٔ اعداد مختلط $\mathbb{C}$ نیز یک میدان می‌باشد.

توجه کنید که $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. این امر را با گفتن اینکه $\mathbb{Q}$ زیرمیدان $\mathbb{R}$ (و $\mathbb{C}$) و $\mathbb{R}$ زیر میدان $\mathbb{C}$ است توصیف می‌کنیم.

۵. فرض کنیم $R = \mathbb{Z}_۶$ یعنی مجموعهٔ اعداد صحیح $\bmod ۶$ با جمع و ضرب زیر باشد:

$$[a][b] = [ab] \text{ و } [a] + [b] = [a + b]$$

توجه کنید که $[۰]$ صفر لازم در اصول موضوع یک حلقه بوده و $[۱]$ عنصر یکهٔ R می‌باشد. همچنین $\mathbb{Z}_۶$ یک قلمرو صحیح نیست زیرا $[۰] = [۶] = [۳][۲]$ ولی $[۰] \neq [۲]$ و $[۰] \neq [۳]$. R یک حلقهٔ یکدار تعویضپذیر می‌باشد.

مثال اخیر تعریف زیر را پیشنهاد خواهد کرد.

تعریف. عنصر $a \neq ۰$ در حلقهٔ R یک مقسوم‌علیه صفر در R است اگر به ازای عنصری مانند $b \neq ۰$ در R، $ab = ۰$.

آنچه در بالا تعریف شد در واقع عنصر صفر چپ است. چون بحث ما عمدتاً راجع به حلقه‌های تعویضپذیر است، برای مقسوم‌علیه‌های صفر تمایز بین چپ و راست لازم نیست.

توجه کنید که $[۲]$ و $[۳]$ هر دو در $\mathbb{Z}_۶$ مقسوم‌علیه صفرند. البته هر قلمرو صحیح یک حلقهٔ

تعویضپذیر بدون مقسوم‌علیه صفر می‌باشد.

۶. فرض کنیم $R = \mathbb{Z}_5$ یعنی حلقهٔ اعداد صحیح $\bmod 5$ باشد. R البته یک حلقهٔ تعویضپذیر یکدار است. ولی چیزی است بیش از این و در واقع یک میدان می‌باشد. عناصر ناصفرش عبارتند از $[1]$، $[2]$، $[3]$، $[4]$ و توجه کنید که $[1] = [6] = [2][3]$ و $[1]$ و $[4]$ معکوسهای خود می‌باشند. لذا هر عنصر ناصفر در $\mathbb{Z}_5$ دارای معکوسی در $\mathbb{Z}_5$ می‌باشد.

حال مثال (۶) را به ازای هر عدد اول p تعمیم می‌دهیم:

۷. فرض کنیم $\mathbb{Z}_p$ مجموعهٔ اعداد صحیح $\bmod p$ باشد که در آن p اول است. مجدداً $\mathbb{Z}_p$ یک حلقهٔ تعویضپذیر یکدار می‌باشد. حکم می‌کنیم که $\mathbb{Z}_p$ میدان است. برای مشاهدهٔ این امر گوییم هرگاه $[a] \neq [0]$، آن‌گاه $p \nmid a$. لذا، طبق قضیهٔ فرما (نتیجهٔ قضیهٔ ۸.۴.۲)، $a^{p-1} \equiv 1(p)$. این در مورد رده‌های $[\cdot]$ می‌گوید که $[a^{p-1}] = [1]$. ولی $[a^{p-1}] = [a]^{p-1}$؛ در نتیجه $[a]^{p-1} = [1]$. بنابراین $[a]^{p-2}$ معکوس لازم برای $[a]$ در $\mathbb{Z}_p$ است. لذا $\mathbb{Z}_p$ یک میدان می‌باشد.

چون $\mathbb{Z}_p$ فقط تعدادی متناهی عنصر دارد، آن را یک میدان متناهی می‌نامند. بعدها میدانهایی متناهی خواهیم ساخت که با $\mathbb{Z}_p$ها متفاوت می‌باشند.

۸. فرض کنیم $\mathbb{Q}$ مجموعهٔ اعداد گویا باشد. اگر $a \in \mathbb{Q}$، می‌توان نوشت $a = m/n$ که در آن اعداد صحیح m و n نسبت به هم اولند. ما این شکل را شکل تحویل یافتهٔ a می‌نامیم. فرض کنیم R مجموعهٔ تمام $a \in \mathbb{Q}$هایی باشد که مخرج شکل تحویل شده‌شان فرد است. مجموعهٔ R تحت جمع و ضرب در $\mathbb{Q}$ یک حلقه است. این حلقه یک قلمرو صحیح یکدار است ولی میدان نیست زیرا $\frac{1}{2}$، یعنی معکوس لازم برای ۲، در R نیست. چه عناصری از R دارای معکوس در Rاند؟

۹. فرض کنیم R مجموعهٔ تمام $a \in \mathbb{Q}$هایی باشد که مخرج شکل تحویل شده‌شان بر عدد اول ثابت p بخشپذیر نیست. R، همانند مثال ۸، تحت جمع و ضرب معمولی $\mathbb{Q}$ یک حلقه است، یک قلمرو صحیح است، ولی یک میدان نمی‌باشد. چه عناصری از R دارای معکوس در Rاند؟

تعریف. مثالهای ۸ و ۹ زیرحلقهٔ $\mathbb{Q}$اند به مفهوم زیر. فرض کنیم R یک حلقه باشد. یک زیرحلقهٔ R زیرمجموعه‌ای است مانند S از R که یک حلقه است اگر اعمال ab و $a+b$ $(a, b \in S)$ همان عملهای R باشند که بر عناصر $a, b \in S$ اعمال می‌شوند.

برای زیرحلقه بودن S لازم و کافی است که S ناتهی بوده و به ازای هر $a, b \in S$،

$ab, a \pm b \in S$. (ثابت کنید!)

حال مثال تعویضپذیر دیگری می‌زنیم. این مثال از حساب دیفرانسیل و انتگرال می‌باشد.

۱۰. فرض کنیم R مجموعهٔ تمام توابع پیوستهٔ حقیقی بر بازهٔ یکهٔ بستهٔ $[۰, ۱]$ باشد. به ازای $f, g \in R$ و $x \in [۰, ۱]$ تعریف می‌کنیم $(f + g)(x) = f(x) + g(x)$ و $(f \cdot g)(x) = f(x)g(x)$. از حساب دیفرانسیل و انتگرال می‌دانیم که $f + g$ و $f \cdot g$ توابع پیوسته‌ای بر $[۰, ۱]$اند. R با این اعمال یک حلقهٔ تعویضپذیر است. R یک قلمرو صحیح نیست. مثلاً هرگاه به ازای $۰ \leq x \leq \frac{۱}{۲}$، $f(x) = -x + \frac{۱}{۲}$ و به ازای $\frac{۱}{۲} < x \leq ۱$، $f(x) = ۰$ و نیز به ازای $۰ \leq x \leq \frac{۱}{۲}$، $g(x) = ۰$ و به ازای $\frac{۱}{۲} < x \leq ۱$، $g(x) = ۲x - ۱$، آن‌گاه $f, g \in R$ و به آسانی معلوم می‌شود که $f \cdot g = ۰$. R دارای عنصر یکه است؛ یعنی تابع e با تعریف $e(x) = ۱$ به ازای هر $x \in [۰, ۱]$. چه عناصری از R دارای معکوس در Rاند؟

حال می‌خواهیم چند مثال تعویض‌ناپذیر ببینیم. حلقه‌های تعویض‌ناپذیر بسیارند، ولی چون خواننده را مطلع از جبر خطی نپنداشته‌ایم، این مثالها آسان به‌دست نمی‌آیند. ساده‌ترین و طبیعی‌ترین منبع اولیهٔ ما از آنها مجموعهٔ ماتریسها روی یک میدان است. لذا، در اولین مثال تعویض‌ناپذیر ما، ماتریسهای ۲×۲ با درایه‌های حقیقی ایجاد می‌شوند.

۱۱. فرض کنیم F میدان اعداد حقیقی و R مجموعهٔ تمام آرایه‌های مربعی صوری

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

باشد که در آن a، b، c، و d اعداد حقیقی دلخواهی می‌باشند. جمع در این آرایه‌های مربعی طبعاً به‌صورت زیر تعریف می‌شود:

$$\begin{pmatrix} a_۱ & b_۱ \\ c_۱ & d_۱ \end{pmatrix} + \begin{pmatrix} a_۲ & b_۲ \\ c_۲ & d_۲ \end{pmatrix} = \begin{pmatrix} a_۱ + a_۲ & b_۱ + b_۲ \\ c_۱ + c_۲ & d_۱ + d_۲ \end{pmatrix}$$

به آسانی معلوم می‌شود که R تحت این $+$ یک گروه آبلی است که در آن $\begin{pmatrix} ۰ & ۰ \\ ۰ & ۰ \end{pmatrix}$ عنصر صفر و $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ قرینهٔ $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ می‌باشد. برای حلقه ساختن R نیاز به یک ضرب داریم. این

ضرب را به‌صورت ظاهراً غیرطبیعی زیر تعریف می‌کنیم:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} ar+bt & as+bu \\ cr+dt & cs+du \end{pmatrix}$$

با کمی زحمت می‌توان تحقیق کرد که R با این اعمال یک حلقهٔ تعویض‌ناپذیر با عنصر یکهٔ ضربی $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ است. توجه کنید که

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

ولی

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

پس

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

توجه کنید که $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ و $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ مقسوم‌علیه‌های صفرند؛ در واقع

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$ ؛ در نتیجه $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

یک عنصر ناصفر است که مجذورش عنصر ۰ در R می‌باشد. R را حلقهٔ تمام ماتریسهای ۲ × ۲ روی F (میدان حقیقی) می‌نامیم.

ما، به خاطر افراد ناآشنا با این ماتریسها و کسانی که ضرب تعریف شده در آنها را بی‌معنی می‌بینند، طرز محاسبهٔ این ضرب را از نظر می‌گذرانیم. برای به‌دست آوردن درایهٔ چپ فوقانی حاصلضرب AB که $A, B \in R$، سطر اول A را در ستون اول B «ضرب می‌کنیم». برای به‌دست آوردن درایهٔ راست فوقانی، سطر اول A در ستون دوم B ضرب می‌شود. درایهٔ چپ تحتانی از ضرب سطر دوم A در ستون اول B، و بالاخره درایهٔ راست تحتانی از ضرب سطر دوم A در ستون دوم B به‌دست می‌آید.

مطلب را با یک مثال توضیح می‌دهیم: فرض کنیم

$$B = \begin{pmatrix} \frac{۱}{۲} & \frac{۲}{۵} \\ \pi & -\pi \end{pmatrix} \quad \text{و} \quad A = \begin{pmatrix} ۱ & \frac{۱}{۲} \\ -۳ & ۲ \end{pmatrix}$$

در این صورت سطر اول A مساوی $\frac{۱}{۲}$ ۱ و ستون اول B برابر π $\frac{۱}{۲}$ است. ما این دو را «درهم ضرب کرده» به‌دست می‌آوریم $\frac{\pi}{۲} + \frac{۱}{۲} = \pi \cdot \frac{۱}{۲} + \frac{۱}{۲} \cdot ۱$، و به همین ترتیب تا آخر. لذا داریم

$$AB = \begin{pmatrix} \frac{۱}{۲} + \frac{\pi}{۲} & \frac{۲}{۵} - \frac{\pi}{۲} \\ -۱ + ۲\pi & -\frac{۶}{۵} - ۲\pi \end{pmatrix}$$

ما در مسائل ضرب ماتریسی زیادی را خواهیم دید؛ در نتیجه خواننده می‌تواند با این مثال عجیب ولی مهم آشنایی بیشتری کسب نماید.

۱۲. فرض کنیم R یک حلقه بوده و

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in R \right\}$$

که در آن + و · همانند مثال ۱۱ تعریف شده‌اند. می‌توان تحقیق کرد که S نیز تحت این اعمال یک حلقه است. این حلقه را حلقهٔ ماتریسهای ۲ × ۲ روی R می‌نامند.

آخرین مثال ما یکی از مثالهای مهم کلاسیک است و آن عبارت است از چهارگانهای حقیقی که توسط هامیلتون (به عنوان اشیایی غیرتعویضپذیر به موازات اعداد مختلط) معرفی شده است.

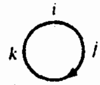
۱۳. چهارگانها. فرض کنیم F میدان اعداد حقیقی باشد. مجموعهٔ تمام علایم صوری $\alpha_۰ + \alpha_۱ i + \alpha_۲ j + \alpha_۳ k$ را که در آنها $\alpha_۰, \alpha_۱, \alpha_۲, \alpha_۳ \in F$ در نظر می‌گیریم. تساوی و جمع این علایم آسان و به‌صورت واضح زیر می‌باشند:

$$\alpha_۰ + \alpha_۱ i + \alpha_۲ j + \alpha_۳ k = \beta_۰ + \beta_۱ i + \beta_۲ j + \beta_۳ k$$

اگر و فقط اگر $\alpha_۰ = \beta_۰$، $\alpha_۱ = \beta_۱$، $\alpha_۲ = \beta_۲$، $\alpha_۳ = \beta_۳$، و

$$\begin{aligned}(\alpha_۰ + \alpha_۱ i + \alpha_۲ j + \alpha_۳ k) &+ (\beta_۰ + \beta_۱ i + \beta_۲ j + \beta_۳ k) \\ &= (\alpha_۰ + \beta_۰) + (\alpha_۱ + \beta_۱) i + (\alpha_۲ + \beta_۲) j + (\alpha_۳ + \beta_۳) k\end{aligned}$$

حال به قسمت مشکل کار، یعنی ضرب، می‌رسیم. وقتی هامیلتون در ۶ اکتبر ۱۸۴۳ این ضرب را کشف کرد، قواعد اصلی‌اش را با نیش چاقو روی پل بروهام (Brougham Bridge) در دوبلین حک نمود. این ضرب مبتنی است بر $i^2 = j^2 = k^2 = -1$، $ij = k$، $jk = i$، $ki = j$، $ji = -k$، $kj = -i$، $ik = -j$. اگر روی دایره در جهت عقربه‌های ساعت حرکت کنیم، حاصلضرب



هر دو عنصر متوالی عنصر بعدی است، و اگر خلاف عقربه‌های ساعت حرکت کنیم قرینه‌ها به‌دست می‌آیند.

حال می‌توان ضرب هر دو چهارگان را طبق قواعد فوق تعریف کرد:

$$(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k) = \gamma_0 + \gamma_1 i + \gamma_2 j + \gamma_3 k$$

که در آن

$$\begin{aligned} \gamma_0 &= \alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 \\ \gamma_1 &= \alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2 \\ \gamma_2 &= \alpha_0\beta_2 - \alpha_1\beta_3 + \alpha_2\beta_0 + \alpha_3\beta_1 \\ \gamma_3 &= \alpha_0\beta_3 + \alpha_1\beta_2 - \alpha_2\beta_1 + \alpha_3\beta_0 \end{aligned} \tag{1}$$

این ضرب ظاهر هولناکی دارد؛ این‌طور نیست؟ ولی به آن بدیی که فکر می‌کنید نخواهد بود. با استفاده از قوانین پخشپذیری و قواعد ضرب فوق برای i، j، و k می‌توان به‌طور صوری ضرب کرد.

اگر α_iی در $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ مساوی ۰ باشد، می‌توان آن را از عبارت x حذف کرد. مثلاً $0 + 0i + 0j + 0k$ را به‌صورت ۰، $1 + 0i + 0j + 0k$ را به‌صورت ۱، $0 + 3i + 4j + 0k$ را به‌صورت $3i + 4j$، و غیره نوشت.

با محاسبه معلوم می‌شود که

$$(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \tag{2}$$

این رابطه نتیجهٔ بسیار مهمی دارد، زیرا فرض کنیم $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \neq 0$ (پس $\alpha_i \neq 0$ی). چون αها حقیقی‌اند، $\beta = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \neq 0$. در این صورت از

(۲) به آسانی به‌دست می‌آوریم

$$(\alpha_۰ + \alpha_۱ i + \alpha_۲ j + \alpha_۳ k)\left(\frac{\alpha_۰}{\beta} - \frac{\alpha_۱}{\beta}i - \frac{\alpha_۲}{\beta}j - \frac{\alpha_۳}{\beta}k\right) = ۱$$

لذا، هرگاه $x \neq ۰$، آن‌گاه x در مجموعهٔ چهارگانها دارای معکوس است. لذا چهارگانها یک حلقهٔ بخشی تعویض‌ناپذیر تشکیل می‌دهند.

همان‌طورکه قبلاً گفتیم، با آنکه حلقه‌های بخشی تعویض‌ناپذیرکم نیستند، ولی چهارگانهای فوق (یا بخشی از آنها) اغلب تنها حلقه‌های بخشی تعویض‌ناپذیری‌اند که حتی بسیاری از ریاضیدانان حرفه‌ای آنها را دیده‌اند.

راجع به دو مثال ماتریسهای ۲×۲ و چهارگانها مسائل بسیار (بعضی آسان و برخی کمی سختتر) خواهیم داشت. بدین ترتیب خواننده می‌تواند در حلقه‌های تعویض‌ناپذیر مهارتی کسب نماید.

آخرین سخن ما در این بخش: هرگاه $\gamma_۰$، $\gamma_۱$، $\gamma_۲$، و $\gamma_۳$ همانند در (۱) باشند، آن‌گاه

$$(\alpha_۰^۲ + \alpha_۱^۲ + \alpha_۲^۲ + \alpha_۳^۲)(\beta_۰^۲ + \beta_۱^۲ + \beta_۲^۲ + \beta_۳^۲) = \gamma_۰^۲ + \gamma_۱^۲ + \gamma_۲^۲ + \gamma_۳^۲ \quad (۳)$$

این تساوی را اتحاد لاگرانژ می‌نامند. این تساوی حاصلضرب دو مجموع از چهار مجذور را مجدداً به‌صورت مجموعی از چهار مجذور بیان می‌دارد. تحقیق آن یکی از تمرینات خواهد بود.

مسائل

مسائل آسانتر

*۱. تمام عناصر $\mathbb{Z}_{۲۴}$ را که در آن معکوسپذیر اند (یعنی دارای معکوس ضربی‌اند) بیابید.

۲. نشان دهید که هر میدان یک قلمرو صحیح است.

۳. نشان دهید که $\mathbb{Z}_n$ یک میدان است اگر و فقط اگر n اول باشد.

۴. تحقیق کنید که مثال ۸ یک حلقه است. تمام عناصر معکوسپذیر آن را بیابید.

۵. مسئلهٔ ۴ را در مورد مثال ۹ حل کنید.

۶. در مثال ۱۱، یعنی ماتریسهای ۲×۲ روی اعداد حقیقی، قانون شرکتپذیری ضرب را تحقیق کنید.

۷. اعمال زیر را انجام دهید:

الف) $\begin{pmatrix} \frac{۱}{۵} & \frac{۲}{۳} \\ ۰ & ۱ \end{pmatrix} \cdot \begin{pmatrix} ۱ & ۲ \\ ۴ & -۷ \end{pmatrix}$؛

ب) $\begin{pmatrix} ۱ & ۱ \\ ۱ & ۱ \end{pmatrix}^{۲}$؛

پ) $\begin{pmatrix} \frac{۱}{۲} & \frac{۱}{۲} \\ ۰ & ۰ \end{pmatrix}^{۳}$؛

ت) $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} ۱ & ۰ \\ ۰ & ۰ \end{pmatrix} - \begin{pmatrix} ۱ & ۰ \\ ۰ & ۰ \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

۸. تمام ماتریسهای $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ با خاصیت $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} ۱ & ۰ \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} ۱ & ۰ \\ ۰ & ۰ \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ را بیابید.

۹. تمام ماتریسهای ۲ × ۲ی $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ راکه با تمام ماتریسهای ۲ × ۲ تعویض می‌شوند بیابید.

۱۰. فرض کنید R یک حلقهٔ یکدار و S حلقهٔ ماتریسهای ۲ × ۲ روی R باشد (ر.ک. مثال ۱۲.)

الف) قانون شرکتپذیری ضرب در S را تحقیق کنید. (یادآوری: R لازم نیست تعویضپذیر باشد.)

ب) نشان دهید که $\left\{ \begin{pmatrix} a & b \\ ۰ & c \end{pmatrix} \middle| a, b, c \in R \right\}$ یک زیرحلقهٔ S است.

پ) نشان دهید که $\begin{pmatrix} a & b \\ ۰ & c \end{pmatrix}$ در S دارای معکوس است اگر و فقط اگر a و c در R معکوس داشته باشند. در این صورت $\begin{pmatrix} a & b \\ ۰ & c \end{pmatrix}^{-۱}$ را به‌طور صریح بنویسید.

۱۱. فرض کنید $F : \mathbb{C} \to \mathbb{C}$ با $F(a + bi) = a - bi$ تعریف شده باشد. نشان دهید که

الف) به ازای $x, y \in \mathbb{C}$، $F(xy) = F(x)F(y)$؛

ب) $F(x\bar{x}) = |x|^{۲}$؛

پ) با استفاده از قسمتهای (الف) و (ب) نشان دهید که

$$(a^{۲} + b^{۲})(c^{۲} + d^{۲}) = (ac - bd)^{۲} + (ad + bc)^{۲}$$

[تذکر: $F(x)$ عبارت است از $\bar{x}$.]

۱۲. اتحاد قسمت (پ) مسئلهٔ ۱۱ را مستقیماً تحقیق کنید.

۱۳. حاصلضربهای زیر از چهارگانها را بیابید:

الف) $(i + j)(i - j)$؛

ب) $(۱ + ۲i - ۴j + ۶k)(۱ - i + ۲j - ۲k)$؛

پ) $(۲i - ۳j + ۴k)^{۲}$؛

ت) $i(\alpha_{۰} + \alpha_{۱}i + \alpha_{۲}j + \alpha_{۳}k) - (\alpha_{۰} + \alpha_{۱}i + \alpha_{۲}j + \alpha_{۳}k)i$.

۱۴. نشان دهید که تنها چهارگانهایی که با i تعویض می‌شوند به شکل $\alpha + \beta i$ می‌باشند.

۱۵. چهارگانهایی را که با هر دوی i و j تعویض می‌شوند بیابید.

۱۶. تحقیق کنید که

$$(\alpha_{۰} + \alpha_{۱}i + \alpha_{۲}j + \alpha_{۳}k)(\alpha_{۰} - \alpha_{۱}i - \alpha_{۲}j - \alpha_{۳}k) = \alpha_{۰}^{۲} + \alpha_{۱}^{۲} + \alpha_{۲}^{۲} + \alpha_{۳}^{۲}$$

۱۷. اتحاد لاگرانژ را با محاسبهٔ مستقیم تحقیق نمایید.

مسائل با سطح متوسط

۱۸. در چهارگانها تعریف کنید

$$|\alpha_{۰} + \alpha_{۱}i + \alpha_{۲}j + \alpha_{۳}k| = \sqrt{\alpha_{۰}^{۲} + \alpha_{۱}^{۲} + \alpha_{۲}^{۲} + \alpha_{۳}^{۲}}$$

و نشان دهید که به ازای هر دو چهارگان x و y، $|xy| = |x||y|$.

۱۹. نشان دهید که معادلهٔ $x^{۲} = -۱$ در چهارگانها بی‌نهایت جواب دارد.

۲۰. مجموعهٔ هشت عنصری $G = \{\pm ۱, \pm i, \pm j, \pm k\}$ را در چهارگانها در نظر بگیرید.

الف) ثابت کنید G (تحت ضرب) یک گروه است؛

ب) تمام زیرگروههای G را بنویسید؛

پ) مرکز G چیست؟

ت) نشان دهید که G یک گروه غیرآبلی است که تمام زیرگروههایش نرمال‌اند.

۲۱. نشان دهید که هر حلقهٔ بخشی یک قلمرو است.

۲۲. در چهارگانها یک قلمرو تعویض‌ناپذیر مثال بزنید که حلقهٔ بخشی نباشد.

۲۳. نگاشت * را در چهارگانها به‌صورت زیر تعریف کنید:

$$(\alpha_{۰} + \alpha_{۱}i + \alpha_{۲}j + \alpha_{۳}k)^{*} = (\alpha_{۰} - \alpha_{۱}i - \alpha_{۲}j - \alpha_{۳}k)$$

و نشان دهید که

الف) $x^{**} = (x^{*})^{*} = x$؛

ب) $(x + y)^{*} = x^{*} + y^{*}$؛

پ) $xx^* = x^*x$ حقیقی و نامنفی است؛

ت) $(xy)^* = y^*x^*$.

[در قسمت (ت) به ترتیب عکس توجه کنید.]

۲۴. با استفاده از * تعریف کنید $|x| = \sqrt{xx^*}$ و به کمک قسمتهای (پ) و (ت) مسئلهٔ ۲۳ نشان دهید که به ازای هر دو چهارگان x و y، $|xy| = |x||y|$.

۲۵. اتحاد لاگرانژ را با استفاده از مسئلهٔ ۲۴ ثابت نمایید.

در مسائل ۲۶ تا ۳۰ فرض کنید R مجموعهٔ تمام ماتریسهای ۲ × ۲ روی اعداد حقیقی باشد.

۲۶. اگر $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R$، نشان دهید که $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ در R معکوسپذیر است اگر و فقط اگر $ad - bc \neq ۰$. در این صورت $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-۱}$ را پیدا کنید.

۲۷. تعریف کنید $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$ و به ازای $x, y \in R$ نشان دهید که

$$\det(xy) = (\det x)(\det y)$$

۲۸. نشان دهید که $\{x \in R | \det x \neq ۰\}$ تحت ضرب ماتریسها گروهی مانند G تشکیل می‌دهد و $N = \{x \in R | \det x = ۱\}$ یک زیرگروه نرمال آن است.

۲۹. اگر $x \in R$ یک مقسوم‌علیه صفر باشد، نشان دهید که $\det x = ۰$ و، به عکس، هرگاه $x \neq ۰$ چنان باشد که $\det x = ۰$، آن‌گاه x یک مقسوم‌علیه صفر در R است.

۳۰. در R نشان دهید که $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a \text{ و } b \text{ حقیقی} \right\}$ یک میدان است.

مسائل مشکلتر

۳۱. فرض کنید R حلقهٔ تمام ماتریسهای ۲ × ۲ روی $\mathbb{Z}_p$ باشد که در آن p یک عدد اول است. نشان دهید هرگاه $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \neq ۰$، آن‌گاه $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ در R معکوسپذیر است.

۳۲. فرض کنید R همانند مسئلهٔ ۳۱ باشد و نشان دهید که به ازای هر $x, y \in R$،

$$\det(xy) = \det(x)\det(y)$$

۳۳. فرض کنید G مجموعهٔ عناصری از R مسئلهٔ ۳۱ باشد که $\det(x) \neq 0$.

الف) ثابت کنید G یک گروه است؛

ب) مرتبهٔ G را بیابید؛ (نسبتاً مشکل.)

پ) مرکز G را بیابید؛

ت) یک زیرگروه p-سیلوی G را بیابید.

۳۴. فرض کنید T گروه تمام ماتریسهای A با درایه‌های واقع در میدان $\mathbb{Z}_2$ باشد که $\det A$ مساوی ۰ نیست. ثابت کنید T با گروه متقارن از درجهٔ ۳ی S_3 یکریخت است.

۳۵. نشان دهید که حلقهٔ R مثال ۱۰ (توابع پیوسته بر $[0, 1]$) یک قلمرو صحیح نیست.

فرض کنید $H(F)$ حلقهٔ چهارگانها روی میدان F باشد؛ یعنی مجموعهٔ تمام $\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ها که در آنها $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in F$ و تساوی، جمع، و ضرب همانند چهارگانهای حقیقی تعریف می‌شوند.

۳۶. اگر $F = \mathbb{C}$، یعنی مجموعهٔ اعداد مختلط باشد، نشان دهید که $H(\mathbb{C})$ یک حلقهٔ بخشی نیست.

۳۷. در $H(\mathbb{C})$ عنصری مانند $x \neq 0$ را چنان بیابید که $x^2 = 0$.

۳۸. نشان دهید که $H(F)$ یک حلقهٔ بخشی است اگر و فقط اگر $\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 0$ به ازای α_1، α_2، α_3، α_4 در F ایجاب کند که $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 0$.

۳۹. اگر Q میدان اعداد گویا باشد، نشان دهید که $H(Q)$ یک حلقهٔ بخشی است.

۴۰. ثابت کنید هر قلمرو متناهی یک حلقهٔ بخشی است.

۴۱. با استفاده از مسئلهٔ ۴۰ نشان دهید که اگر p اول باشد، $\mathbb{Z}_p$ یک میدان است.

۲. چند نتیجهٔ ساده

حال که چند حلقه را دیده و در بازی با آنها تجربه‌ای اندوخته‌ایم شایسته است که چند قاعدهٔ محاسباتی به‌دست آوریم. با این قواعد می‌توان از بدیهیاتی که محاسبات را به ستوه می‌آورند پرهیز نماییم.

نتایجی که در این بخش ثابت می‌شوند نه تعجب‌آورند نه جالب و لذا هیجان‌انگیز نیستند. همچنین الفبای کار نیز نبوده و بلکه چیزی هستند که باید پیش از مطالب مبسوط‌تر و بهتر حاصل شوند. این امر در مورد نتایجی که هم‌اکنون ثابت شوند نیز صادق است.

چون حلقهٔ R دست‌کم یک گروه آبلی تحت $+$ است، نکاتی از نظریهٔ گروهها برقرارند. مثلاً $-(-a) = a$، $-(a+b) = (-a)+(-b)$؛ هرگاه $a+b = a+c$، آن‌گاه $b = c$، و از این قبیل.

بحث را با لم زیر آغاز می‌کنیم.

لم ۴.۲.۱. فرض کنیم R یک حلقه بوده و $a, b \in R$. در این‌صورت،

الف) $a\circ = \circ a = \circ$؛

ب) $a(-b) = (-a)b = -(ab)$؛

پ) $(-a)(-b) = ab$؛

ت) هرگاه $\text{۱} \in R$، آن‌گاه $(-\text{۱})a = -a$.

برهان. این احکام را به نوبت ثابت می‌کنیم.

الف) چون $\circ + \circ = \circ$، داریم $a\circ = a(\circ + \circ) = a\circ + a\circ$. در نتیجه $a\circ = \circ$. ما در این برهان از قانون پخشپذیری از چپ استفاده کرده‌ایم. قانون پخشپذیری از راست نتیجه می‌دهد که $\circ a = \circ$.

ب) از قسمت (الف) داریم $ab + a(-b) = a(b+(-b)) = a\circ = \circ$. لذا $a(-b) = -(ab)$. به همین نحو $(-a)b = -(ab)$.

پ) بنابر قسمت (ب)، $(-a)(-b) = -((-a)b) = -(-(ab)) = ab$ زیرا در یک گروه آبلی هستیم.

ت) هرگاه $\text{۱} \in R$، آن‌گاه $(-\text{۱})a + a = (-\text{۱})a + (\text{۱})a = (-\text{۱}+\text{۱})a = \circ a = \circ$. پس، طبق تعریف $-a$، $(-\text{۱})a = -a$. ■

نتیجهٔ محاسباتی دیگر به قرار زیر است.

لم ۴.۲.۲. در هر حلقهٔ R به ازای هر $a, b \in R$، $(a+b)^{\text{۲}} = a^{\text{۲}} + b^{\text{۲}} + ab + ba$.

برهان. این به وضوح شبیه $(\alpha + \beta)^{\text{۲}} = \alpha^{\text{۲}} + \text{۲}\alpha\beta + \beta^{\text{۲}}$ مثلاً در اعداد صحیح است، ولی به یاد داشته باشید که R ممکن است تعویض‌ناپذیر باشد. طبق قانون پخشپذیری از راست،

$$(a+b)^{\text{۲}} = (a+b)(a+b) = (a+b)a + (a+b)b = a^{\text{۲}} + ba + ab + b^{\text{۲}}$$

که همان حکم ما می‌باشد. ■

آیا صورت تعویض‌ناپذیری قضیهٔ دو جمله‌ای را می‌توانید ببینید؟ آن را در مورد $(a+b)^3$ ثابت کنید.

وقتی R یکدار است، از دو قانون پخشپذیری نکتهٔ جالبی حاصل می‌شود و آن نتیجه شدن قانون تعویضپذیری جمع از سایر قوانین است.

لم ۳.۲.۴. هرگاه R دستگاهی یکدار و صادق در تمام اصول موضوع حلقه جز احتمالاً $a+b=b+a$ به ازای هر $a,b \in R$ باشد، آن‌گاه R یک حلقه می‌باشد.

برهان. باید نشان دهیم که به ازای هر $a,b \in R$، $a+b=b+a$. بنابر قانون پخشپذیری از راست،

$$(a+b)(1+1)=(a+b)1+(a+b)1=a+b+a+b$$

از آن‌سو، طبق قانون پخشپذیری از چپ،

$$(a+b)(1+1)=a(1+1)+b(1+1)=a+a+b+b$$

پس داریم $a+b+a+b=a+a+b+b$. چون در یک گروه تحت +ایم، می‌توانیم a را از چپ و b را از راست حذف کرده و $b+a=a+b$، یعنی مطلوب خود، را به‌دست آوریم. لذا R یک حلقه می‌باشد. ■

این بخش کوتاه را با نتیجه‌ای کمی جالبتر خاتمه می‌دهیم. گوییم حلقهٔ R یک حلقهٔ بولی [به افتخار ریاضیدان انگلیسی، جرج بول (George Boole, 1815-1864)] است اگر به ازای هر $x \in R$، $x^2=x$.

در این باب لم زیبای زیر را ثابت می‌کنیم.

لم ۴.۲.۴. هر حلقهٔ بولی تعویضپذیر است.

برهان. فرض کنیم x و y در حلقهٔ بولی R باشند. لذا $x^2=x$، $y^2=y$، و $(x+y)^2=x+y$. اما، طبق لم ۲.۲.۴،

$$(x+y)^2=x^2+xy+yx+y^2=x+xy+yx+y$$

پس $x+xy+yx+y=(x+y)^2=(x+y)$ که از آن داریم $xy+yx=0$.

لذا $xy + xyx = xy + xyx = x^2y + xyx = x(xy+yx) = 0$، حال آنکه

$$0 = (xy+yx)x = xyx + yx^2 = xyx + yx$$

از این نتیجه می‌شود که $xy + xyx = xyx + yx$؛ و در نتیجه $xy = yx$. لذا R تعویضپذیر می‌باشد. ■

مسائل

۱. فرض کنید R یک حلقه باشد. چون R تحت $+$ یک گروه آبلی است، na به ازای $n \in \mathbb{Z}$ و $a \in R$ معنی دارد. نشان دهید که اگر n و m صحیح بوده و $a, b \in R$، $(na)(mb) = (nm)(ab)$.

۲. اگر R یک قلمرو بوده و به ازای $b, c \in R$, $a \neq 0$، $ab = ac$، نشان دهید که $b = c$.

۳. اگر R یک قلمرو صحیح متناهی باشد، نشان دهید که R یک میدان است.

۴. اگر R یک حلقه بوده و $e \in R$ چنان باشد که $e^2 = e$، نشان دهید که به ازای هر $x \in R$، $(xe - exe)^2 = (ex - exe)^2 = 0$.

۵. فرض کنید حلقهٔ R چنان باشد که در آن به ازای هر $x \in R$، $x^3 = x$. ثابت کنید R تعویضپذیر است.

۶. اگر در R داشته باشیم $a^2 = 0$، نشان دهید که $ax + xa$ با a تعویض می‌شود.

۷. فرض کنید حلقهٔ R چنان باشد که به ازای هر $x \in R$، $x^4 = x$. ثابت کنید R تعویضپذیر است.

۸. اگر F یک میدان متناهی باشد، نشان دهید که

الف) عدد اولی مانند p هست به‌طوری که به ازای هر $a \in F$، $pa = 0$؛

ب) هرگاه F دارای q عنصر باشد، آن‌گاه به ازای عدد صحیحی چون n، $q = p^n$.

(راهنمایی. قضیهٔ کشی.)

۹. فرض کنید p یک عدد اول فرد بوده و $1 + \frac{1}{2} + \cdots + 1/(p-1) = a/b$ که در آن a و b صحیح‌اند. نشان دهید که $p|a$. (راهنمایی. وقتی a در $\mathbb{Z}_p$ تغییر کند، a^{-1} نیز چنین می‌کند.)

۱۰. اگر p یک عدد اول بوده و $p > 3$، نشان دهید هرگاه $1 + \frac{1}{2} + \cdots + 1/(p-1) = a/b$ که در آن a و b صحیح‌اند، آن‌گاه $p^2|a$. (راهنمایی. $1/a^2$ را وقتی a در $\mathbb{Z}_p$ تغییر کند در نظر بگیرید.)

۳. ایده‌آلها، همریختیها، و حلقه‌های خارج‌قسمتی

در مطالعهٔ گروهها دیدیم که همریختیها و هسته‌هایشان، یعنی زیرگروههای نرمال، نقش اصلی را دارند. دلیلی ندارد که این امر در حلقه‌ها برقرار نباشد. در واقع، در حلقه‌ها، مشابه همریختی و زیرگروه نرمال نقشی کلیدی بر عهده خواهند داشت.

با زمینه‌ای که از این اشیاء در نظریهٔ گروهها به‌دست آمد، مطالب موازی در حلقه‌ها باید آسان و سریع باشند، که در واقع چنین است! بدون بحث بیشتر، تعریف زیر را می‌آوریم.

تعریف. نگاشت $\varphi : R \to R'$ از حلقهٔ R به توی حلقهٔ R' یک همریختی است اگر به ازای هر $a, b \in R$،

الف) $\varphi(a+b) = \varphi(a) + \varphi(b)$ و

ب) $\varphi(ab) = \varphi(a)\varphi(b)$.

چون هر حلقه دو عمل دارد، طبیعی است که هر دو تحت همریختی حلقه‌ها حفظ شوند که ما آن را در تعریف خواسته‌ایم. به‌علاوه خاصیت (الف) در تعریف به ما می‌گوید که φ یک همریختی از R است که فقط یک گروه آبلی تحت $+$ در نظر گرفته شود به توی R' (که تحت جمع خود یک گروه آبلی به حساب آید). لذا از این امر می‌توان نتایجی را انتظار داشت.

همان‌طور که در فصل ۲، بخش ۵ در مورد گروهها دیدیم، نقش R تحت همریختی از R به R' یک زیرحلقهٔ R' به‌صورت تعریف شده در فصل ۴، بخش ۱ است (ثابت کنید!)

فرض کنیم $\varphi : R \to R'$ یک همریختی حلقه‌ها بوده و $\mathrm{Ker}\varphi = \{x \in R | \varphi(x) = 0\}$ که در آن 0 متعلق به R' است. $\mathrm{Ker}\varphi$ چه خواصی دارد؟ واضح است که، طبق نظریهٔ گروهها، $\mathrm{Ker}\varphi$ یک زیرگروه جمعی R است. ولی بیش از این برقرار است. هرگاه $k \in \mathrm{Ker}\varphi$ و $r \in R$، آن‌گاه $\varphi(k) = 0$؛ در نتیجه $\varphi(kr) = \varphi(k)\varphi(r) = 0\varphi(r) = 0$. و به همین نحو $\varphi(rk) = 0$. لذا $\mathrm{Ker}\varphi$ ضرب از چپ و راست در عناصر دلخواه حلقه را می‌بلعد.

حال این خاصیت $\mathrm{Ker}\varphi$ را مجرد ساخته و مشابه مهم زیرگروه نرمال در نظریهٔ گروهها را در نظریهٔ حلقه‌ها تعریف می‌کنیم.

تعریف. فرض کنیم R یک حلقه باشد. زیرمجموعهٔ ناتهی I از R را یک ایده‌آل R نامیم اگر

الف) I یک زیرگروه جمعی R بوده و

ب) هرگاه $r \in R$ و $a \in I$، آن‌گاه $ra \in I$ و $ar \in I$.

به‌زودی چند مثال از همریختیها و ایده‌آلها را خواهیم دید. ولی ابتدا ملاحظه می‌کنیم که قسمت

(ب) تعریف ایده‌آل در واقع قسمت چپ و قسمت راست دارد. می‌توان آن را تجزیه کرد و مجموعهٔ L از R را یک ایده‌آل چپ R نامید اگر L یک زیرگروه جمعی R بوده و به ازای $r \in R$ و $a \in L$، $ra \in L$. لذا در یک ایده‌آل چپ فقط بلعیدن از چپ را شرط می‌کنیم. به همین نحو می‌توان ایده‌آلهای راست را تعریف کرد. یک ایده‌آل به‌صورتی که تعریف شد هم ایده‌آل چپ R است هم ایده‌آل راست R. پس یک ایده‌آل را می‌توان با حفظ حقوق یک ایده‌آل دوطرفهٔ R نامید. در واقع وقتی در نظریهٔ حلقه‌های تعویض‌ناپذیر کار می‌کنیم از این نام استفاده خواهیم کرد. در اینجا منظور از «ایده‌آل» همواره یعنی یک ایده‌آل دوطرفه. ما در این فصل از ایده‌آلهای یکطرفه جز در چند مسئله استفاده نخواهیم کرد.

پیش از ادامهٔ بحث، آنچه را که در بالا برای $\mathrm{Ker}\varphi$ اثبات شد به ثبت می‌رسانیم:

لم ۱.۳.۴. هرگاه $\varphi : R \to R'$ یک همریختی باشد، آن‌گاه $\mathrm{Ker}\varphi$ یک ایده‌آل R است.

به‌زودی خواهیم دید که هر ایده‌آل را می‌توان هستهٔ یک همریختی دانست، شبیه آنچه برای زیرگروههای نرمال گروهها رخ داد!

بالاخره فرض کنیم K یک ایده‌آل R باشد. چون K یک زیرگروه جمعی R است، گروه خارج قسمتی R/K وجود دارد. این صرفاً مجموعهٔ تمام هم‌مجموعه‌های $a + K$ است که a در R تغییر می‌کند. ولی R فقط یک گروه نیست بلکه یک حلقه می‌باشد. K نیز صرفاً یک زیرگروه جمعی R نبوده و بیش از آن یعنی یک ایده‌آل R می‌باشد. باید بتوان همهٔ این امور را کنار هم گذارد و R/K را یک حلقه ساخت.

چطور می‌توان در R/K به‌طور طبیعی ضرب تعریف کرد؟ می‌خواهیم $(a+K)(b+K)$ چه باشد؟ تنها کار معقول $(a+K)(b+K) = ab + K$ است که ما انجام می‌دهیم. طبق معمول، اولین گام نشان دادن آن است که این ضرب تعریف شده است. آیا چنین است؟ باید نشان دهیم که هرگاه $a + K = a' + K$ و $b + K = b' + K$، آن‌گاه

$$(a+K)(b+K) = ab + K = a'b' + K = (a'+K)(b'+K)$$

اما هرگاه $a + K = a' + K$، آن‌گاه $a - a' \in K$؛ در نتیجه $(a - a')b \in K$ زیرا K یک ایده‌آل R می‌باشد (در واقع چون K ایده‌آل راست R است). چون $b + K = b' + K$، داریم $b - b' \in K$؛ در نتیجه $a'(b - b') \in K$ زیرا K یک ایده‌آل R است (در واقع چون K یک

ایده‌آل چپ R است). لذا هر دوی

$$(a-a')b = ab - a'b \quad \text{و} \quad a'(b-b') = a'b - a'b'$$

در Kاند. بنابراین

$$(ab - a'b) + (a'b - a'b') = ab - a'b' \in K$$

ولی این (فقط از نظریهٔ گروهها) به ما می‌گوید که $ab + K = a'b' + K$ یعنی همان چیزی که برای تعریف شدن ضرب لازم است.

لذا R/K دارای جمع و ضرب است. به‌علاوه نگاشت $\varphi : R \to R/K$ با تعریف $\varphi(a) = a + K$ به ازای $a \in R$ یک همریختی از R به روی R/K با هستهٔ K است. (ثابت کنید!) این بی‌درنگ به ما می‌گوید که R/K یک حلقه است زیرا نقش همریختی حلقهٔ R می‌باشد.

همهٔ مطالب فوق را در قضیهٔ زیر خلاصه می‌کنیم.

قضیهٔ ۲.۳.۴. فرض کنیم K ایده‌آلی از R باشد. در این صورت گروه خارج قسمتی R/K به عنوان یک گروه جمعی تحت ضرب $(a+K)(b+K) = ab + K$ یک حلقه می‌باشد. به‌علاوه نگاشت $\varphi : R \to R/K$ با تعریف $\varphi(a) = a + K$ به ازای $a \in R$ یک همریختی از R به روی R/K با هستهٔ K می‌باشد. لذا R/K نقش همریختی R خواهد بود.

تنها از نظریهٔ گروهها و گروه جمعی بودن R معلوم می‌شود که هرگاه φ یک همریختی از R به توی R' باشد، آن‌گاه φ یک‌به‌یک است اگر و فقط اگر $\mathrm{Ker}\varphi = (۰)$. همانند گروهها، یک همریختی در صورتی تکریختی است که ۱-۱ باشد. هر تکریختی که برو نیز باشد یکریختی نام دارد. R و R' را یکریخت گوییم اگر یک یکریختی از R به روی R' موجود باشد.

هر یکریختی از حلقهٔ R به روی خود یک خودریختی R نام دارد. مثلاً هرگاه R میدان اعداد مختلط $\mathbb{C}$ باشد، آن‌گاه نگاشت از R به R که هر عنصر R را به مزدوج مختلط خود بفرستد یک خودریختی $\mathbb{C}$ نام دارد. (ثابت کنید!)

باید خیلی بدبین باشیم که انتظار عدم برقراری قضایای ثابت شده در بخشهای ۵ و ۶ از فصل ۲ را داشته باشیم. در واقع این قضایا با اصلاحاتی جزئی برقرارند. ما قضایای همریختی را بدون بحث بیشتر بیان کرده و اثبات آنها را به خواننده وامی‌گذاریم.

قضیهٔ ۳.۳.۴(قضیهٔ اول همریختی). فرض کنیم نگاشت $\varphi : R \to R'$ یک همریختی از R به روی R' با هستهٔ K باشد. در این صورت $R' \simeq R/K$. در واقع نگاشت $\psi : R/K \to R'$ با تعریف $\psi(a+K) = \varphi(a)$ یک یکریختی از R/K به روی R' می‌باشد.

حال به قضیهٔ همریختی بعدی می‌پردازیم.

قضیهٔ ۴.۳.۴(قضیهٔ دوم همریختی). فرض کنیم نگاشت $\varphi : R \to R'$ یک همریختی از R به روی R' با هستهٔ K باشد. اگر I' یک ایده‌آل R' باشد، قرار می‌دهیم $I = \{a \in R | \varphi(a) \in I'\}$. در این صورت I ایده‌آلی است از R، $K \subset I$، و $I/K \simeq I'$. این امر تناظری ۱-۱ بین تمام ایده‌آلهای R' و ایده‌آلهایی از R که شامل Kاند ایجاد می‌نماید.

بالاخره به آخرین قضیهٔ همریختی که مایلیم بیان کنیم می‌رسیم. البته قضایای همریختی دیگری نیز وجود دارند. ما آنها را در مسائل خواهیم آورد.

قضیهٔ ۵.۳.۴(قضیهٔ سوم همریختی). فرض کنیم نگاشت $\varphi : R \to R'$ یک همریختی از R به روی R' با هستهٔ K باشد. هرگاه I' ایده‌آلی از R' بوده و $I = \{a \in R | \varphi(a) \in I'\}$، آنگاه $R/I \simeq R'/I'$. به‌عبارت دیگر، هرگاه K ایده‌آلی از R بوده و $K \subset I$ ایده‌آلی از R باشد، آنگاه $R/I \simeq (R/K)/(I/K)$.

این بخش را با بررسی نکاتی طی چند مثال به پایان می‌بریم.

چند مثال

۱. طبق معمول، مثال اول را حلقهٔ اعداد صحیح $\mathbb{Z}$ می‌گیریم. فرض کنیم $n > ۱$ یک عدد صحیح ثابت و I_n مجموعهٔ تمام مضارب n باشد. I_n یک ایده‌آل R است. اگر $\mathbb{Z}_n$ اعداد صحیح با $\bmod n$ باشد، $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ را با $\varphi(a) = [a]$ تعریف می‌کنیم. به آسانی معلوم می‌شود که φ یک همریختی از $\mathbb{Z}$ به روی $\mathbb{Z}_n$ با هستهٔ I_n است. لذا، طبق قضیهٔ ۳.۳.۴، $\mathbb{Z}_n \simeq \mathbb{Z}/I_n$. (این امر تعجب‌آور نیست، زیرا $\mathbb{Z}_n$ اساساً به این طریق معرفی شده است.)

۲. فرض کنیم F یک میدان باشد. ایده‌آلهای F چه می‌توانند باشند؟ فرض کنیم $I \neq (۰)$ ایده‌آلی از F باشد. همچنین $a \neq ۰ \in I$. چون I ایده‌آل F است، $۱ = a^{-۱}a \in I$. ولی چون $۱ \in I$، به ازای هر $r \in F$، $r۱ = r \in I$. به‌طور خلاصه، $I = F$. لذا ایده‌آلهای F منحصر

است به ایده‌آل بدیهی $(\circ)$ و خود F.

۳. فرض کنیم R حلقهٔ اعداد گویایی باشد که مخرج شکل تحویل شده‌شان فرد است. همچنین I مجموعهٔ عناصری از R باشد که صورت شکل تحویل شده‌شان زوج است. به آسانی معلوم می‌شود که I یک ایده‌آل R است. (اعداد صحیح ۲ mod) $\varphi : R \to \mathbb{Z}_۲$ را با $\varphi(a/b) = \circ$ اگر a زوج باشد (a و b عامل مشترک ندارند) و $\varphi(a/b) = ۱$ اگر a فرد باشد تعریف می‌کنیم. بر خواننده است تحقیق کند که φ یک همریختی از R به روی $\mathbb{Z}_۲$ با هستهٔ I است. لذا $R/I \simeq \mathbb{Z}_۲$. یک یکریختی صریح از R/I به روی $\mathbb{Z}_۲$ مثال بزنید.

۴. فرض کنیم R حلقهٔ تمام اعداد گویایی باشد که مخرج شکل تحویل شده‌شان بر عدد اول ثابت p بخشپذیر نیست. همچنین I مجموعهٔ عناصری در R باشد که صورتشان بر p بخشپذیر است. I یک ایده‌آل R است و (اعداد صحیح p mod) $R/I \simeq \mathbb{Z}_p$. (ثابت کنید!)

۵. فرض کنیم R حلقهٔ تمام توابع پیوستهٔ حقیقی بر بازهٔ یکهٔ بسته باشد که در آن به ازای هر $f, g \in R$ و $x \in [\circ, ۱]$، $(f+g)(x) = f(x) + g(x)$ و $(fg)(x) = f(x)g(x)$. همچنین $I = \{f \in R | f(\frac{۱}{۲}) = \circ\}$. حکم می‌کنیم که I یک ایده‌آل R است. واضح است که I یک زیرگروه جمعی است. به‌علاوه، هرگاه $f \in I$ و $g \in R$، آن‌گاه $f(\frac{۱}{۲}) = \circ$؛ در نتیجه $(fg)(\frac{۱}{۲}) = f(\frac{۱}{۲})g(\frac{۱}{۲}) = \circ g(\frac{۱}{۲}) = \circ$. لذا $fg \in I$. چون I تعویضپذیر است، gf نیز در I می‌باشد. لذا I یک ایده‌آل R می‌باشد.

R/I چیست؟ هرگاه $f \in R$، آن‌گاه

$$f(x) = \left(f(x) - f\left(\frac{۱}{۲}\right)\right) + f\left(\frac{۱}{۲}\right) = g(x) + f\left(\frac{۱}{۲}\right)$$

که در آن $g(x) = f(x) - f(\frac{۱}{۲})$. چون $g(\frac{۱}{۲}) = f(\frac{۱}{۲}) - f(\frac{۱}{۲}) = \circ$، g در I است. پس $g + I = I$. لذا $f + I = (f(\frac{۱}{۲}) + g) + I = f(\frac{۱}{۲}) + I$. چون $f(\frac{۱}{۲})$ عددی حقیقی است، R/I از هم‌مجموعه‌های $\alpha + I$ به ازای αی حقیقی تشکیل شده است. حکم می‌کنیم که هر عدد حقیقی α ظاهر می‌شود. زیرا هرگاه $f(\frac{۱}{۲}) = \beta \neq \circ$، آن‌گاه

$$\alpha\beta^{-۱}f + I = (\alpha\beta^{-۱} + I)(f + I) = (\alpha\beta^{-۱} + I)\left(f\left(\frac{۱}{۲}\right) + I\right)$$
$$= (\alpha\beta^{-۱} + I)(\beta + I) = \alpha\beta^{-۱}\beta + I = \alpha + I$$

در نتیجه R/I از تمام $\alpha + I$هایی تشکیل شده است که در آنها α حقیقی است. لذا می‌توان نشان داد که R/I با میدان حقیقی یکریخت است.

حال با استفاده از قضیهٔ ۳.۳.۴ نشان می‌دهیم که میدان حقیقی $\simeq R/I$. فرض کنیم $\varphi : R \to \mathbb{R}$ با $\varphi(f) = f(\frac{1}{2})$ تعریف شده باشد. در این صورت φ (مثل فوق) بروست است و $\mathrm{Ker}\varphi = \{f \in R | f(\frac{1}{2}) = 0\}$. به بیان دیگر، $\mathrm{Ker}\varphi = I$. در نتیجه $\mathbb{R} =$ نقش $\varphi \simeq R/I$.

۶. فرض کنیم R مجموعهٔ چهارگانهای صحیح باشد؛ یعنی

$$R = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k | \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}\}$$

و

$$I_p = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in R | \ p | \alpha_i \quad \text{به ازای } i = 0, 1, 2, 3 \text{ و عدد اول ثابت } p\}$$

بر خواننده است تحقیق کند که I_p یک ایده‌آل R است و $R/I_p \simeq H(\mathbb{Z}_p)$ (ر.ک. مسئلهٔ ۳۸ از بخش ۱ و بند پیش از آن).

۷. فرض کنیم $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$؛ R یک زیر حلقهٔ ماتریسهای 2×2 روی اعداد حقیقی است. قرار می‌دهیم $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| b \in \mathbb{R} \right\}$. به آسانی معلوم می‌شود که I یک زیرگروه جمعی R است. آیا I یک ایده‌آل R است؟ می‌نویسیم

$$\begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & xb \\ 0 & 0 \end{pmatrix}$$

که در I است. به همین نحو

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} = \begin{pmatrix} 0 & bx \\ 0 & 0 \end{pmatrix}$$

که این نیز در I است. لذا I یک ایده‌آل R می‌باشد. R/I چیست؟ ما از دو سو به آن نزدیک می‌شویم.

هرگاه $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R$، آن‌گاه

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$

پس

$$\begin{pmatrix} a & b \\ \circ & a \end{pmatrix} + I = \left(\begin{pmatrix} a & \circ \\ \circ & a \end{pmatrix} + \begin{pmatrix} \circ & b \\ \circ & \circ \end{pmatrix} \right) + I = \begin{pmatrix} a & \circ \\ \circ & a \end{pmatrix} + I$$

زیرا $\begin{pmatrix} \circ & b \\ \circ & \circ \end{pmatrix}$ در I است. لذا تمام هم مجموعه‌های I در R به شکل $\begin{pmatrix} a & \circ \\ \circ & a \end{pmatrix} + I$ می‌باشند.

اگر این را به روی a بنگاریم، یعنی $\psi \left\{ \begin{pmatrix} a & \circ \\ \circ & a \end{pmatrix} + I \right\} = a$، می‌توان تحقیق کرد که ψ یک یکریختی به روی میدان حقیقی است. در نتیجه $R/I \simeq \mathbb{R}$.

حال به روشی دیگر نشان می‌دهیم که $R/I \simeq \mathbb{R}$. $\varphi : R \to \mathbb{R}$ را با $\varphi \begin{pmatrix} a & b \\ \circ & a \end{pmatrix} = a$ تعریف می‌کنیم. حکم می‌کنیم که φ یک همریختی است. زیرا به ازای $\begin{pmatrix} a & b \\ \circ & a \end{pmatrix}$ و $\begin{pmatrix} c & d \\ \circ & c \end{pmatrix}$ داریم

$$\varphi \begin{pmatrix} c & d \\ \circ & c \end{pmatrix} = c \quad \text{و} \quad \varphi \begin{pmatrix} a & b \\ \circ & a \end{pmatrix} = a$$

چون

$$\begin{pmatrix} a & b \\ \circ & a \end{pmatrix} \begin{pmatrix} c & d \\ \circ & c \end{pmatrix} = \begin{pmatrix} ac & ad + bc \\ \circ & ac \end{pmatrix} \quad \text{و} \quad \begin{pmatrix} a & b \\ \circ & a \end{pmatrix} + \begin{pmatrix} c & d \\ \circ & c \end{pmatrix} = \begin{pmatrix} a + c & b + d \\ \circ & a + c \end{pmatrix}$$

لذا

$$\begin{aligned} \varphi \left(\begin{pmatrix} a & b \\ \circ & a \end{pmatrix} + \begin{pmatrix} c & d \\ \circ & c \end{pmatrix} \right) &= \varphi \begin{pmatrix} a + c & b + d \\ \circ & a + c \end{pmatrix} \\ &= a + c = \varphi \begin{pmatrix} a & b \\ \circ & a \end{pmatrix} + \varphi \begin{pmatrix} c & d \\ \circ & c \end{pmatrix} \end{aligned}$$

و

$$\begin{aligned} \varphi \left(\begin{pmatrix} a & b \\ \circ & a \end{pmatrix} \begin{pmatrix} c & d \\ \circ & c \end{pmatrix} \right) &= \varphi \begin{pmatrix} ac & ad + bc \\ \circ & ac \end{pmatrix} \\ &= ac = \varphi \begin{pmatrix} a & b \\ \circ & a \end{pmatrix} \varphi \begin{pmatrix} c & d \\ \circ & c \end{pmatrix} \end{aligned}$$

لذا φ واقعاً یک همریختی از R به روی $\mathbb{R}$ است. $\mathrm{Ker}\varphi$ چیست؟ هرگاه $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathrm{Ker}\varphi$، آن‌گاه $a = \varphi\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$. از آن‌سو، طبق تعریف φ و اینکه $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathrm{Ker}\varphi$، $\varphi\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = 0$. لذا $a = 0$. از این معلوم می‌شود که $I = \mathrm{Ker}\varphi$ پس، طبق قضیهٔ ۳.۳.۴، $\mathbb{R} = $ نقش $\varphi \simeq R/I$.

۸. فرض کنیم $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$ و $\mathbb{C}$ میدان اعداد مختلط باشد. نگاشت $\psi : R \to \mathbb{C}$ را با $\psi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi$ تعریف می‌کنیم. بر خواننده است تحقیق کند که ψ یک یکریختی از R به روی $\mathbb{C}$ است. لذا R با میدان اعداد مختلط یکریخت می‌باشد.

۹. فرض کنیم R یک حلقهٔ تعویضپذیر یکدار باشد. اگر $a \in R$، قرار می‌دهیم $(a) = \{xa | x \in R\}$ و حکم می‌کنیم که (a) یک ایده‌آل R است. برای مشاهدهٔ این امر فرض می‌کنیم $u, v \in (a)$. پس به ازای $x, y \in R$ی، $u = xa$ و $v = ya$ که از آنجا

$$u \pm v = xa \pm ya = (x \pm y)a \in (a)$$

همچنین هرگاه $u \in (a)$ و $r \in R$، آن‌گاه $u = xa$. پس $ru = r(xa) = (rx)a$؛ در نتیجه در (a) است. لذا (a) یک ایده‌آل R می‌باشد.

توجه کنید که اگر R تعویضپذیر نباشد، (a) لزوماً یک ایده‌آل نیست ولی مسلماً یک ایده‌آل چپ R می‌باشد.

مسائل

مسائل آسانتر

۱. اگر R یک حلقهٔ تعویضپذیر بوده و $a \in R$، قرار دهید $L(a) = \{x \in R | xa = 0\}$ و ثابت کنید $L(a)$ یک ایده‌آل R است.

۲. اگر R یک حلقهٔ تعویضپذیر یکدار بوده و R ایده‌آلی جز (0) و خود نداشته باشد، ثابت کنید R یک میدان است. (راهنمایی. به مثال ۹ نگاه کنید.)

۳*. اگر $\varphi : R \to R'$ یک همریختی از R به روی R' بوده و R دارای عنصر یکهٔ ۱ باشد، نشان دهید که $\varphi(1)$ عنصر یکهٔ R' است.

۴. اگر I و J ایده‌آلهایی از R باشند، $I+J$ را با $I+J=\{i+j|j\in J\ ،\ i\in I\}$ تعریف و ثابت کنید $I+J$ یک ایده‌آل R است.

۵. اگر I ایده‌آلی از R و A زیرحلقه‌ای از R باشد، نشان دهید که $I\cap A$ ایده‌آلی از A می‌باشد.

۶. اگر I و J ایده‌آلهایی از R باشند، نشان دهید که $I\cap J$ ایده‌آلی از R است.

۷. قضیهٔ ۲.۳.۴ را به‌طور کامل ثابت کنید.

۸. قضیهٔ ۴.۳.۴ را به‌طور کامل ثابت کنید.

۹. فرض کنید $\varphi : R\to R'$ یک همریختی از R به روی R' با هستهٔ K باشد. اگر A' زیرحلقهٔ R' بوده و $A=\{a\in R|\varphi(a)\in A'\}$، نشان دهید که

الف) A زیرحلقهٔ R بوده و $A\supset K$؛

ب) $A/K\simeq A'$؛

پ) هرگاه A' یک ایده‌آل چپ R' باشد، آن‌گاه A یک ایده‌آل چپ R است.

۱۰. قضیهٔ ۵.۳.۴ را ثابت کنید.

۱۱. در مثال ۳ یک یکریختی از R/I به روی $\mathbb{Z}_2$ نشان دهید.

۱۲. در مثال ۴ نشان دهید که $R/I\simeq\mathbb{Z}_p$.

۱۳. در مثال ۶ نشان دهید که $R/I_p\simeq H(\mathbb{Z}_p)$.

۱۴. در مثال ۸ تحقیق کنید که نگاشت ψ داده شده یک یکریختی از R به روی $\mathbb{C}$ است.

۱۵. اگر I و J ایده‌آلهایی از R باشند، IJ را مجموعهٔ تمام مجموعها از عناصر به شکل ij بگیرید که در آن $i\in I$ و $j\in J$. ثابت کنید IJ یک ایده‌آل R است.

۱۶. نشان دهید که حلقهٔ ماتریسهای 2×2 روی اعداد حقیقی دارای ایده‌آلهای چپ غیربدیهی (و نیز ایده‌آلهای راست غیربدیهی) است.

۱۷. اگر A زیرحلقه‌ای از R و I ایده‌آلی از R باشد، قرار دهید

$$A+I=\{a+i|i\in I\ ،\ a\in A\}$$

و ثابت کنید.

الف) $A+I$ زیرحلقهٔ R است و $A+I\supset I$؛

ب) $(A+I)/I\simeq A/(A\cap I)$.

مجموع مستقیم $R\oplus S$ دو حلقهٔ R و S را به‌صورت $R\oplus S=\{(r,s)|s\in S،r\in R\}$

تعریف می‌کنیم که در آن $(r,s) = (r_1, s_1)$ اگر و فقط اگر $r = r_1$ و $s = s_1$، و

$$(r,s)(t,u) = (rt, su) \quad ، \quad (r,s) + (t,u) = (r+t, s+u)$$

۱۸. نشان دهید که $R \oplus S$ یک حلقه است و زیرحلقه‌های $\{(r, 0) | r \in R\}$ و $\{(0, s) | s \in S\}$ ایده‌آلهایی از $R \oplus S$اند که به ترتیب با R و S یکریخت می‌باشند.

۱۹. اگر $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \, a \text{ و } b \text{ و } c \text{ حقیقی} \right\}$ و $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| \, b \text{ حقیقی} \right\}$، نشان دهید که

الف) R یک حلقه است؛

ب) I ایده‌آلی است از R؛

پ) $R/I \simeq F \oplus F$ که در آن F میدان اعداد حقیقی است.

۲۰. اگر I و J ایده‌آلهایی از R بوده و $R_1 = R/I$ و $R_2 = R/J$، نشان دهید که $\varphi : R \to R_1 \oplus R_2$ با تعریف $\varphi(r) = (r + I, r + J)$ یک همریختی از R به توی $R_1 \oplus R_2$ است به‌طوری که $\text{Ker}\varphi = I \cap J$.

۲۱. فرض کنید $\mathbb{Z}_{15}$ حلقهٔ اعداد صحیح $\bmod 15$ باشد. نشان دهید که $\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

مسائل با سطح متوسط

۲۲. فرض کنید $\mathbb{Z}$ حلقهٔ اعداد صحیح بوده و m و n دو عدد صحیح نسبت به هم اول باشند. I_m را مجموعهٔ مضارب m در $\mathbb{Z}$ و I_n را مجموعهٔ مضارب n در $\mathbb{Z}$ بگیرید.

الف) $I_m \cap I_n$ چیست؟

ب) با استفاده از مسئلهٔ ۲۰ نشان دهید که یک یکریختی از $\mathbb{Z}/I_{mn}$ به توی $\mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$ وجود دارد.

پ) با شمارش عناصر دو طرف نشان دهید که

$$\mathbb{Z}/I_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$$

۲۳. اگر m و n نسبت به هم اول باشند، ثابت کنید $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$. (راهنمایی. مسئلهٔ ۲۲.)

*۲۴. قضیهٔ باقیماندهٔ چینی را با استفاده از مسئلهٔ ۲۲ یا مسئلهٔ ۲۳ ثابت کنید. این قضیه می‌گوید که اگر اعداد صحیح m و n نسبت به هم اول باشند، می‌توان عدد صحیح x را چنان یافت که همزمان داشته باشیم $x = a \bmod m$ و $x \equiv b \bmod n$.

۲۵. فرض کنید R حلقهٔ ماتریسهای ۲×۲ روی اعداد حقیقی بوده و I ایده‌آلی از R باشد. نشان دهید که $I = (\circ)$ یا $I = R$. (این نتیجه را با مسئلهٔ ۱۶ مقایسه کنید.)

مسائل مشکلتر

۲۶. فرض کنید R حلقه‌ای یکدار و S حلقهٔ ماتریسهای ۲×۲ روی R باشد. اگر I ایده‌آلی از S باشد، نشان دهید که ایده‌آلی از R مانند J هست به‌طوری که I عبارت است از مجموعهٔ تمام ماتریسهای ۲×۲ روی J.

۲۷. اگر $p_۱$، $p_۲$، $\cdots$، p_n اعداد اول متمایزی باشند، نشان دهید که معادلهٔ

$$x^۲ \equiv x \mod (p_۱ \quad \cdots \quad p_n)$$

که در آن $\circ \leq x < p_۱ \quad \cdots \quad p_n$ درست ۲^n جواب دارد.

۲۸. فرض کنید R حلقه‌ای باشد که تنها ایده‌آلهای چپش عبارتند از $(\circ)$ و R. ثابت کنید R یک حلقهٔ بخشی است یا R دارای p عنصر است، p اول بوده، و به ازای هر $a, b \in R$، $ab = \circ$.

۲۹. فرض کنید R یک حلقهٔ یکدار باشد. گوییم عنصر $a \in R$ دارای معکوس چپ است اگر به ازای $b \in R$ای، $ba = ۱$. نشان دهید هرگاه معکوس چپ b از a منحصر به‌فرد باشد، آن‌گاه $ab = ۱$ (پس b نیز یک معکوس راست a است).

۴. ایده‌آلهای ماکزیمال

این بخش حاوی قضیه‌ای مهم است. اهمیت این قضیه زمانی کاملاً ظاهر می‌شود که میدانها را در فصل ۵ مطرح کنیم. با این حال این نتیجه‌ای است که بر دو پای خود استوار است. اثباتش مشکل نیست، ولی در ریاضیات ارتباط بین مشکل و مهم همیشه زیاد نیست. نتایج مشکل بسیاری در دست‌اند که اصلاً جالب نبوده و حتی اهمیتی ندارند و نتایج آسانی وجود دارند که مهم می‌باشند. البته نتایج بسیار زیادی هستند که بی‌نهایت مشکل و مهم می‌باشند.

لم ۱.۴.۴. فرض کنیم R یک حلقهٔ تعویض‌پذیر یکدار باشد که ایده‌آلهایش فقط $(\circ)$ و خودش‌اند. در این صورت R یک میدان می‌باشد.

برهان. فرض کنیم $a \neq \circ$ در R باشد. همان‌طور که در مثال ۹ بخش قبل تحقیق شد، $(a) = \{xa | x \in R\}$ یک ایده‌آل R است. چون $a = ۱a \in (a)$، پس $(a) \neq \circ$. لذا، طبق فرض ما بر R، $R = (a)$. ولی در این صورت، طبق تعریف (a)، هر عنصر $i \in R$ مضربی از

a مانند xa به ازای $x \in R$ ای می‌باشد. به‌خصوص، چون $1 \in R$، به ازای $b \in R$ای، $ba = 1$.
این نشان می‌دهد که a دارای معکوس b در R است. در نتیجه R یک میدان می‌باشد. ■

در قضیهٔ ۴.۳.۴ (قضیهٔ دوم همریختی) دیدیم که هرگاه $\varphi : R \to R'$ یک همریختی از R به روی R' با هستهٔ K باشد، آن‌گاه یک تناظر ۱-۱ بین ایده‌آلهای R' و ایده‌آلهای R که شامل Kاند وجود دارد. فرض کنیم ایده‌آلی جز خود K و R که شامل Kاند موجود نباشد. از این چه چیز راجع به R' نتیجه می‌شود؟ چون (0) در R' نظیر K در R بوده و R نظیر R' در این تناظر حاصل از قضیهٔ دوم همریختی است، باید در این حالت نتیجه بگیریم که R' ایده‌آلی جز (0) و خودش ندارد. لذا اگر R' تعویضپذیر بوده و دارای عنصر یکه باشد، R' طبق لم ۱.۴.۴ باید یک میدان باشد.

این امر تعریف زیر را پیش می‌آورد.

تعریف. ایده‌آل حقیقی M از R در صورتی یک ایده‌آل ماکزیمال R است که تنها ایده‌آلهای R شامل M خود M و R باشند.

در بحث پیش از این تعریف تقریباً قضیهٔ زیر اثبات شده است.

قضیهٔ ۲.۴.۴. فرض کنیم R یک حلقهٔ تعویضپذیر یکدار بوده و M یک ایده‌آل ماکزیمال R باشد. در این صورت R/M یک میدان است.

برهان. یک همریختی از R به روی $R' = R/M$ وجود دارد، و چون $1 \in R$، R' دارای عنصر یکهٔ $1 + M$ می‌باشد. (ر.ک. مسئلهٔ ۳ در بخش ۳). چون M یک ایده‌آل ماکزیمال R است، در بحث فوق دیدیم که R' ایده‌آل غیربدیهی ندارد. لذا، طبق لم ۱.۴.۴، $R' = R/M$ یک میدان است. ■

این قضیه دروازهٔ ورود به میدانهاست زیرا به ما توان ساختن میدانهای مطلوب خاصی را در موقع لزوم می‌دهد.

قضیهٔ ۲.۴.۴ دارای عکس است به قرار زیر:

قضیهٔ ۳.۴.۴. هرگاه R یک حلقهٔ تعویضپذیر یکدار بوده و M ایده‌آلی از R باشد به‌طوری که R/M یک میدان است، آن‌گاه M یک ایده‌آل ماکزیمال R می‌باشد.

برهان. در مثال ۲ از بخش ۳ دیدیم که تنها ایده‌آلهای میدان F عبارتند از (0) و خود F. چون R/M میدان است، فقط (0) و خودش را به‌عنوان ایده‌آل دارد. ولی، طبق تناظر ناشی

از قضیهٔ ۴.۳.۴، ایده‌آلی از R حقیقتاً بین M و R نیست. لذا M یک ایده‌آل ماکزیمال R می‌باشد. ■

حال در حلقه‌های تعویضپذیر چند ایده‌آل ماکزیمال مثال می‌زنیم.

چند مثال

۱. فرض کنیم $\mathbb{Z}$ مجموعهٔ اعداد صحیح و M ایده‌آلی از آن باشد. M به‌عنوان ایده‌آلی از $\mathbb{Z}$ یک زیرگروه جمعی $\mathbb{Z}$ است. پس باید از تمام مضارب عدد صحیح ثابتی چون n تشکیل شده باشد. لذا، چون $R/M \simeq \mathbb{Z}_n$ و $\mathbb{Z}_n$ میدان است اگر و فقط اگر n اول باشد، پس M یک ایده‌آل ماکزیمال $\mathbb{Z}$ است اگر و فقط اگر M از تمام مضارب عدد اولی چون p تشکیل شده باشد. لذا مجموعهٔ ایده‌آلهای ماکزیمال در $\mathbb{Z}$ نظیر اعداد اول می‌باشد.

۲. فرض کنیم $\mathbb{Z}$ مجموعهٔ اعداد صحیح بوده و $R = \{a+bi|a,b \in \mathbb{Z}\}$ یک زیرحلقهٔ $\mathbb{C}$ باشد $(i^۲ = -۱)$. در R فرض می‌کنیم M مجموعهٔ تمام $a+bi$هایی در R باشد که $۳|a$ و $۳|b$. بر خواننده است تحقیق کند که M یک ایده‌آل R است.

حکم می‌کنیم که M یک ایده‌آل ماکزیمال R است. زیرا فرض کنیم $N \supset M$ و $N \neq M$ ایده‌آلی از R باشد. پس عنصری مانند $r+si \in N$ هست که ۳ نه r را عاد می‌کند نه s را. لذا $۳ \nmid (r^۲+s^۲)$. (ثابت کنید!) ولی $t = r^۲+s^۲ = (r+si)(r-si)$؛ در نتیجه در N است زیرا $r+si \in N$ و N یک ایده‌آل R است. لذا N دارای عدد صحیحی مانند $t = r^۲+s^۲$ است که بر ۳ بخشپذیر نیست. بنابراین، به ازای اعداد صحیحی چون u و v، $ut+۳v = ۱$. ولی $t \in N$. پس $ut \in N$ و $۳ \in M \subset N$؛ در نتیجه $۳v \in N$. بنابراین $۱ = ut+۳v \in N$. پس به‌ازای هر $a+bi \in R$، $(a+bi)۱ \in N$ زیرا N یک ایده‌آل R می‌باشد. این به ما می‌گوید که $N = R$. پس تنها ایده‌آل R بالای M خود R می‌باشد. در نتیجه M یک ایده‌آل ماکزیمال R می‌باشد.

از قضیهٔ ۲.۴.۴ می‌دانیم که R/M یک میدان است. می‌توان نشان داد (ر.ک. مسئلهٔ ۲) که R/M میدانی با نه عنصر می‌باشد.

۳. فرض کنیم R همانند مثال ۲ بوده و $I = \{a+bi| \ ۵|a \text{ و } ۵|b\}$. حکم می‌کنیم که I یک ایده‌آل ماکزیمال R نیست.

در R می‌توان تجزیه کرد: $۵ = (۲+i)(۲-i)$. فرض کنیم $M = \{x(۲+i)|x \in R\}$. M یک ایده‌آل R است، و چون $۵ = (۲+i)(۲-i)$ در M است، معلوم می‌شود که $I \subset M$. واضح است که $I \neq M$ زیرا $۲+i \in M$ و در I نیست زیرا $۲ \nmid ۵$. پس $I \neq M$. آیا

$M = R$؛ اگر چنین باشد، به ازای a و bای $(۲+i)(a+bi) = ۱$. از این داریم $۲a - b = ۱$ و $۲b + a = ۰$. این دو معادله ایجاب می‌کنند که $۵a = ۲$؛ پس $a = \frac{۲}{۵}$ و $b = -\frac{۱}{۵}$. ولی $\frac{۲}{۵} \not\in \mathbb{Z}$ و $-\frac{۱}{۵} \not\in \mathbb{Z}$. لذا عنصر $a + bi = \frac{۲}{۵} - \frac{۱}{۵}i$ در R نیست. بنابراین $M \neq R$.

ولی می‌توان نشان داد که M یک ایده‌آل ماکزیمال R است. (ر.ک. مسئلهٔ ۳.)

۴. فرض کنیم $R = \{a + b\sqrt{۲} |$ صحیح b و $a\}$ که یک زیر حلقهٔ میدان حقیقی تحت جمع و ضرب اعداد حقیقی است. حلقه بودن R از روابط

$$(a + b\sqrt{۲}) + (c + d\sqrt{۲}) = (a + c) + (b + d)\sqrt{۲}$$

و

$$(a + b\sqrt{۲})(c + d\sqrt{۲}) = (ac + ۲bd) + (ad + bc)\sqrt{۲}$$

نتیجه می‌شود. فرض کنیم $M = \{a + b\sqrt{۲} \in R | \ ۵|a$ و $۵|b\}$. به آسانی معلوم می‌شود که M یک ایده‌آل R است. بر خواننده است نشان دهد که M یک ایده‌آل ماکزیمال R است و R/M میدانی با ۲۵ عنصر می‌باشد.

۵. فرض کنیم R حلقهٔ تمام توابع پیوستهٔ حقیقی بر بازهٔ یکهٔ بستهٔ $[۰, ۱]$ باشد. در مثال ۵ از بخش ۳ نشان دادیم که $M = \{f \in R | f(\frac{۱}{۲}) = ۰\}$ یک ایده‌آل R بوده و R/M با میدان حقیقی یکریخت است. لذا، طبق قضیهٔ ۳.۴.۴، M یک ایده‌آل ماکزیمال R می‌باشد.

البته اگر قرار دهیم $M_\gamma = \{f \in R | f(\gamma) = ۰\}$ که در آن $\gamma \in [۰, ۱]$، M_γ نیز یک ایده‌آل ماکزیمال است. می‌توان نشان داد که هر ایده‌آل ماکزیمال در R به ازای $\gamma \in [۰, ۱]$ای به شکل M_γ است، ولی برای اثبات آن نیاز به نتایجی از نظریهٔ متغیرهای حقیقی داریم.

آنچه این مثال می‌گوید آن است که ایده‌آلهای ماکزیمال R نظیر نقاط $[۰, ۱]$ می‌باشند.

مسائل

۱. اگر a و b اعداد صحیحی بوده و $۳ \nmid a$ و $۳ \nmid b$، نشان دهید که $۳ \nmid (a^۲ + b^۲)$.

۲. نشان دهید که در مثال ۲، R/M میدانی است با نه عنصر.

۳. در مثال ۳ نشان دهید که $M = \{x(۲ + i) | x \in R\}$ یک ایده‌آل ماکزیمال R است.

۴. در مثال ۳ نشان دهید که $R/M \simeq \mathbb{Z}_۵$.

۵. در مثال ۳ نشان دهید که $R/I \simeq \mathbb{Z}_۵ \oplus \mathbb{Z}_۵$.

۶. در مثال ۴ نشان دهید که M یک ایده‌آل ماکزیمال R است.

۷. در مثال ۴ نشان دهید که R/M میدانی است با ۲۵ عنصر.

۸. با استفاده از مثال ۲ به عنوان مدل، میدانی با ۴۹ عنصر بسازید.

حال لحظه‌ای کوتاه به همنهشتیها $\bmod p$ ، که در آن p یک عدد اول فرد است، باز می‌گردیم. اگر عدد صحیح a چنان باشد که $p \nmid a$ و $x^2 \equiv a \bmod p$ جوابی برای x در $\mathbb{Z}$ داشته باشد، گوییم a یک ماندهٔ مربعی $\bmod p$ است. در غیر این صورت گوییم a یک غیرماندهٔ مربعی $\bmod p$ می‌باشد.

۹. نشان دهید که $(p-1)/2$ تا از اعداد ۱، ۲، ... ، $p-1$ ماندهٔ مربعی و $(p-1)/2$ تا غیرماندهٔ مربعی $\bmod p$ می‌باشند. (راهنمایی. نشان دهید که $\{x^2 | x \neq 0 \in Z_p\}$ یک گروه از مرتبهٔ $(p-1)/2$ می‌باشد.)

۱۰. فرض کنید $m > 0$ در $\mathbb{Z}$ بوده و m یک مجذور در $\mathbb{Z}$ نباشد. همچنین

$$R = \{a + \sqrt{m}b | a, b \in \mathbb{Z}\}$$

ثابت کنید R تحت اعمال جمع و ضرب اعداد حقیقی یک حلقه است.

۱۱. اگر p یک عدد اول فرد باشد، قرار دهید $I_p = \{a + \sqrt{m}b | \ p|a \text{ و } p|b\}$ که در آن (حلقهٔ مسئلهٔ ۱۰) $a + \sqrt{m}b \in R$. نشان دهید که I_p یک ایده‌آل R است.

۱۲. اگر m یک غیر ماندهٔ مربعی $\bmod p$ باشد، نشان دهید که ایده‌آل I_p مسئلهٔ ۱۱ یک ایده‌آل ماکزیمال R است.

۱۳. در مسئلهٔ ۱۲ نشان دهید که R/I_p میدانی با p^2 عنصر است.

۵. حلقه‌های چندجمله‌ای

مطالب این بخش راجع به چندجمله‌ای و مجموعهٔ تمام چندجمله‌ایها روی یک میدان است. امیدواریم اغلب خوانندگان با مفهوم چندجمله‌ای در دبیرستان آشنا شده و اعمالی مانند تجزیه، یافتن ریشه‌ها، تقسیم یک چندجمله‌ای بر دیگری و به‌دست آوردن باقیمانده، و غیره را دیده باشند. تأکیدی که ما بر این مفهوم و مفهوم جبری حلقهٔ چندجمله‌ای خواهیم داشت در جهتی کاملاً مخالف جهت دبیرستان است.

به هر حال آنچه در اینجا انجام می‌دهیم معرفی حلقهٔ چندجمله‌ایها روی یک میدان و بحث دقیقی راجع‌به این حلقه است که ساختار درونی‌اش را آشکار می‌سازد. همان‌طور که خواهید دید،

این حلقه بسیار خوشرفتار است. بحث ما یادآور عملی است که در مورد حلقهٔ اعداد صحیح در بخش ۵ از فصل ۱ شد. لذا به مشابهٔ الگوریتم اقلیدسی، بزرگترین مقسوم علیه مشترک، بخشپذیری، و احتمالاً مهمترین آنها یعنی مشابه عدد اول می‌رسیم. این امر ما را به یکتایی تجزیهٔ یک چندجمله‌ای به «چندجمله‌ایهای اول» و ماهیت ایده‌آلها و ایده‌آلهای ماکزیمال در این محدودهٔ جدید می‌رساند.

اما حلقهٔ چندجمله‌ای خاصیتی دارد که حلقهٔ اعداد صحیح از آن بی‌بهره است. این خاصیت ریشهٔ چندجمله‌ای می‌باشد. بررسی ماهیت این ریشه‌ها، که تا حدودی در فصل بعد انجام می‌شود، بخش وسیع و مهم تاریخچهٔ جبری گذشته را تشکیل می‌دهد. این بخش تحت عنوان نظریهٔ معادلات بوده و در گذشتهٔ پرافتخارش نتایج مهمی به چشم می‌خورد. ما چند تا از آنها را حین بحث خواهیم دید.

حال که خلاصهٔ کار ذکر شد به شرح آن می‌پردازیم.

فرض کنیم F یک میدان باشد. منظور از حلقهٔ چندجمله‌ایها از x روی F، که اغلب به‌صورت $F[x]$ نوشته می‌شود، یعنی مجموعهٔ تمام عبارات صوری

$$p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \qquad (n \geq 0)$$

که در آن a_iها، یعنی ضرایب چندجمله‌ای $p(x)$، در Fاند. در $F[x]$ تساوی، مجموع، و حاصلضرب دو چندجمله‌ای را چنان تعریف می‌کنیم که $F[x]$ یک حلقهٔ تعویضپذیر به‌صورت زیر گردد:

۱. تساوی. حکم می‌کنیم که $p(x) = a_0 + a_1x + \cdots + a_nx^n$ و

$$q(x) = b_0 + b_1x + \cdots + b_nx^n$$

مساوی‌اند اگر و فقط اگر ضرایب نظیرشان مساوی باشند؛ یعنی اگر و فقط اگر به‌ازای هر $i \geq 0$، $a_i = b_i$.

تعریف تساوی چندجمله‌ایهای $p(x)$ و $q(x)$ را با این قرار مزین می‌کنیم که اگر

$$q(x) = b_0 + b_1x + \cdots + b_nx^n$$

و $b_{m+1} = \cdots = b_n = 0$، می‌توان $n-m$ جملهٔ آخر را حذف کرده و $q(x)$ را به‌صورت زیر نوشت:

$$q(x) = b_0 + b_1x + \cdots + b_mx^m$$

این قرار در تعریف جمع که ذیلاً می‌آید نیز رعایت می‌شود. در این تعریف s ماکزیمم m و n بوده و ضرایب $a_{n+1} = \cdots = a_s = 0$ اگر $s > n$ یا $b_{m+1} = \cdots = b_s = 0$ اگر $s > m$ با هم جمع می‌شوند.

۲. جمع. اگر $p(x) = a_0 + a_1x + \cdots + a_nx^n$ و $q(x) = b_0 + b_1x + \cdots + b_mx^m$، حکم می‌کنیم که $p(x)+q(x) = c_0 + c_1x + \cdots + c_sx^s$ که در آن به ازای هر i، $c_i = a_i + b_i$.
لذا جمع چندجمله‌ایها با افزودن ضرایب نظیرشان به هم صورت می‌گیرد.

تعریف ضرب کمی پیچیده‌تر است. ابتدا آن را به‌طور نادقیق تعریف کرده و بعداً آن را دقیقتر می‌سازیم.

۳. ضرب. اگر $p(x) = a_0 + a_1x + \cdots + a_nx^n$ و $q(x) = b_0 + b_1x + \cdots + b_mx^m$، حکم می‌کنیم که $p(x)q(x) = c_0 + c_1x + \cdots + c_tx^t$ که در آن c_iها با ضرب صوری عبارات و استفاده از قوانین پخشپذیری و قاعدهٔ نماهای $x^ux^v = x^{u+v}$ و دسته‌بندی جملات به‌دست می‌آیند. به‌طور صوری،

$$\text{به ازای هر } i\text{،}\quad c_i = a_ib_0 + a_{i-1}b_1 + \cdots + a_1b_{i-1} + a_0b_i$$

این اعمال را با یک مثال ساده توضیح می‌دهیم، ولی ابتدا قرار می‌گذاریم که اگر ضریبی ۰ باشد جملهٔ نظیر را حذف کنیم. مثلاً $9 + 0x + 7x^2 + 0x^3 - 14x^4$ را به‌صورت $9 + 7x^2 - 14x^4$ می‌نویسیم.

حال فرض کنیم $p(x) = 1 + 3x^2$ و $q(x) = 4 - 5x + 7x^2 - x^3$. در این صورت $p(x) + q(x) = 5 - 5x + 10x^2 - x^3$ ولی

$$\begin{aligned} p(x)q(x) &= (1 + 3x^2)(4 - 5x + 7x^2 - x^3) \\ &= 4 - 5x + 7x^2 - x^3 + 3x^2(4 - 5x + 7x^2 - x^3) \\ &= 4 - 5x + 7x^2 - x^3 + 12x^2 - 15x^3 + 21x^4 - 3x^5 \\ &= 4 - 5x + 19x^2 - 16x^3 + 21x^4 - 3x^5 \end{aligned}$$

این ضرب را با استفاده از c_iها به‌صورت مذکور در فوق امتحان کنید.

تعریف ما از $F[x]$ به یک معنی تعریف نیست چرا که در آن دستکاری شده است. ولی کار ما را انجام می‌دهد. برای تعریف دقیقتر $F[x]$ می‌توان از دنباله‌ها استفاده کرد، ولی این امر دید اغلب خوانندگان را تیره خواهد ساخت.

اولین نکته‌ای که متذکر می‌شویم (ولی آن را ثابت نمی‌کنیم) حلقهٔ تعویضپذیر بودن $F[x]$ است. امتحان اصول موضوع یک حلقهٔ تعویضپذیر سر راست است ولی زحمت بسیار دارد. لیکن توجه به لم زیر مهم خواهد بود.

لم ۱.۵.۴. $F[x]$ یک حلقهٔ تعویضپذیر یکدار است.

تعریف. هرگاه $p(x) = a_\circ + a_1 x + \cdots + a_n x^n$ و $a_n \neq \circ$، آن‌گاه درجهٔ $p(x)$، که با $\deg p(x)$ نموده می‌شود، n می‌باشد.

لذا درجهٔ چندجمله‌ای $p(x)$ بالاترین توان x است که با ضریب ناصفر در $p(x)$ آمده است. مثلاً $\deg(x - x^2 + x^4) = 4$، $\deg(x) = 1$، و $\deg 7 = \circ$. (توجه کنید که این تعریف به چندجمله‌ای $\circ$ درجه‌ای منتسب نمی‌کند. ولی شایسته است که درجهٔ $\circ$ را $-\infty$ بگیریم. در این صورت بسیاری از نتایج مربوط به درجه در این محدوده برقرارند.) چندجمله‌ایها از درجهٔ $\circ$ را ثابتها می‌نامند. لذا مجموعهٔ ثابتها را می‌توان با F یکی کرد.

تابع درجه بر $F[x]$ نقشی مشابه نقش اندازهٔ اعداد صحیح در $\mathbb{Z}$ دارد والگوریتم اقلیدس را برای $F[x]$ به‌دست می‌دهد.

یک خاصیت فوری و مهم تابع درجه خوشرفتار بودن آن در حاصلضربهاست.

لم ۲.۵.۴. هرگاه $p(x)$ و $q(x)$ عناصر ناصفری از $F[x]$ باشند، آن‌گاه $\deg(p(x)q(x)) = \deg p(x) + \deg q(x)$.

برهان. فرض کنیم $m = \deg p(x)$ و $n = \deg q(x)$. لذا

$$p(x) = a_\circ + a_1 x + \cdots + a_m x^m$$

که در آن $a_m \neq \circ$ و $q(x) = b_\circ + b_1 x + \cdots + b_n x^n$ که در آن $b_n \neq \circ$. از تعریف حاصلضرب معلوم می‌شود که بالاترین توان x در $p(x)q(x)$ عبارت است از x^{m+n}. ضریب x^{m+n} چیست؟ تنها راهی که x^{m+n} می‌تواند ظاهر شود از $(a_m x^m)(b_n x^n) = a_m b_n x^{m+n}$ است. لذا ضریب x^{m+n} در $p(x)q(x)$ عبارت است از $a_m b_n$ که $\circ$ نیست زیرا $a_m \neq \circ$ و $b_n \neq \circ$. لذا، همان‌طور که حکم شده،

$$\deg(p(x)q(x)) = m + n = \deg p(x) + \deg q(x)$$

■

راجع به $\deg(p(x)+q(x))$ نیز نکته‌ای قابل ذکر است که در لم زیر آمده است.

لم ۳.۵.۴. هرگاه $p(x)\,,\ q(x) \in F[x]$ و $p(x)+q(x) \neq 0$، آن‌گاه $\deg(p(x)+q(x)) \leq \max(\deg p(x), \deg q(x))$.

اثبات لم ۳.۵.۴ را به خواننده محول می‌کنیم. این لم در آنچه می‌آید نقشی ندارد ولی لم ۲.۵.۴ مهم خواهد بود. ذکر آن از این جهت بود که جمع در برابر ضرب احساس حقارت نکند.

یک نتیجهٔ فوری لم ۲.۵.۴ به قرار زیر است:

لم ۴.۵.۴. $F[x]$ یک قلمرو صحیح است.

برهان. هرگاه $p(x) \neq 0$ و $q(x) \neq 0$، آن‌گاه $\deg p(x) \geq 0$ و $\deg q(x) \geq 0$. پس $\deg(p(x)q(x)) = \deg p(x) + \deg q(x) \geq 0$. لذا $p(x)q(x)$ دارای درجه است؛ در نتیجه نمی‌تواند 0 (که دارای درجه نیست) باشد. بنابراین $F[x]$ یک قلمرو صحیح می‌باشد. ■

یکی از چیزهایی که درگذشته به اجبار یاد گرفته‌ایم تقسیم یک چندجمله‌ای بر دیگری است. این کار را چطور انجام می‌دادیم؟ این فرایند تقسیم طولانی نام داشت. طرز کار را با یک مثال توضیح می‌دهیم، زیرا آنچه در یک مدل انجام گیرد در حالت کلی نیز صورت خواهد گرفت.

می‌خواهیم $x^4 - 7x + 1$ را بر $2x^2 + 1$ تقسیم کنیم. این کار به‌صورت زیر انجام می‌شود:

$$
\begin{array}{ll}
x^4 - 7x + 1 & \quad \underline{\big|\ 2x^2 + 1\ } \\
x^4 + \frac{1}{2}x^2 & \quad \frac{1}{2}x^2 - \frac{1}{4} \\
\hline
-\frac{1}{2}x^2 - 7x + 1 & \\
-\frac{1}{2}x^2 \qquad\ \ - \frac{1}{4} & \\
\hline
\qquad -7x + 1\frac{1}{4} &
\end{array}
$$

و این را به شکل زیر تعبیر می‌کنیم:

$$x^4 - 7x + 1 = (2x^2 + 1)\left(\frac{1}{2}x^2 - \frac{1}{4}\right) + \left(-7x + \frac{5}{4}\right)$$

و $-7x + \frac{5}{4}$ را باقیمانده در این تقسیم می‌نامیم.

ما دقیقاً چکار کرده‌ایم؟ اولاً $\frac{1}{2}x^2$ از کجا آمد؟ این جمله از آنجا ناشی شد که در ضرب $2x^2 + 1$ در $\frac{1}{2}x^2$ جملهٔ x^4، یعنی بالاترین توان در $x^4 - 7x + 1$، به‌دست می‌آید. لذا با تفریق $\frac{1}{2}x^2(2x^2 + 1)$ از $x^4 - 7x + 1$ جملهٔ x^4 حذف می‌شود و ما فرایند را با آنچه باقیمانده ادامه می‌دهیم.

این «تکرار روند» استقرا را طلب می‌کند و این نحوهٔ اثبات خواهد بود. ولی به یاد داشته باشید که آنچه انجام خواهیم داد همانی است که در مثال فوق کرده‌ایم.

آنچه به‌دست می‌آید چیزی شبیه الگوریتم اقلیدس در اعداد صحیح است. ولی ما آن را در اینجا الگوریتم تقسیم می‌نامیم.

قضیهٔ ۵.۵.۴(الگوریتم تقسیم). به ازای چندجمله‌ایهای $f(x), g(x) \in F[x]$ که $g(x) \neq 0$ داریم

$$f(x) = q(x)g(x) + r(x)$$

که در آن $q(x), r(x) \in F[x]$ و $r(x) = 0$ یا $\deg r(x) < \deg g(x)$.

برهان. روی $\deg f(x)$ استقرا می‌کنیم. هرگاه $f(x) = 0$ یا $\deg f(x) < \deg g(x)$، آن‌گاه $f(x) = 0g(x) + f(x)$ که در قضیه صدق می‌کند.

لذا فرض کنیم $\deg f(x) \geq \deg g(x)$. پس $f(x) = a_0 + a_1x + \cdots + a_mx^m$ که در آن $a_m \neq 0$ و $g(x) = b_0 + b_1x + \cdots + b_nx^n$ که در آن $b_n \neq 0$ و $m \geq n$. می‌نویسیم

$$\begin{aligned}\frac{a_m}{b_n}x^{m-n}g(x) &= \frac{a_m}{b_n}x^{m-n}(b_0 + b_1x + \cdots + b_nx^n)\\ &= \frac{a_mb_0}{b_n}x^{m-n} + \cdots + a_mx^m\end{aligned}$$

لذا $(a_m/b_n)x^{m-n}g(x)$ همان درجه و بزرگترین ضریب $f(x)$ را دارد؛ در نتیجه $f(x) - (a_m/b_n)x^{m-n}g(x) = h(x)$ چنان است که رابطهٔ $\deg h(x) < \deg f(x)$ برقرار می‌باشد. لذا، طبق فرض استقرا،

$$h(x) = q_1(x)g(x) + r(x) \quad \text{که در آن} \quad q_1(x), r(x) \in F[x]$$

و $r(x) = 0$ یا $\deg r(x) < \deg g(x)$. با توجه به $h(x)$ داریم

$$h(x) = f(x) - \frac{a_m}{b_n}x^{m-n}g(x) = q_1(x)g(x) + r(x)$$

در نتیجه

$$f(x) = \left(\frac{a_m}{b_n}x^{m-n} + q_1(x)\right)g(x) + r(x)$$

اگر $q(x) = (a_m/b_n)x^{m-n} + q_1(x)$، شکل مذکور در صورت قضیه به‌دست می‌آید. ■

الگوریتم تقسیم کاربردی فوری دارد: این الگوریتم به ما اجازهٔ تعیین سرشت تمام ایده‌آلهای $F[x]$ را می‌دهد. همان‌طور که در قضیهٔ بعد می‌بینیم، هر ایده‌آل $F[x]$ چیزی جز تمام مضارب یک چندجمله‌ای ثابت در عناصر $F[x]$ نیست.

قضیهٔ ۶.۵.۴. هرگاه $I \neq (0)$ یک ایده‌آل $F[x]$ باشد، آن‌گاه $I = \{f(x)g(x) | f(x) \in F[x]\}$؛ یعنی I از تمام مضارب چندجمله‌ای ثابت $g(x)$ در عناصر $F[x]$ تشکیل شده است.

برهان. برای اثبات قضیه باید چندجمله‌ای ثابت $g(x)$ را بیابیم. کجا باید آن را جستجو کنیم؟ تنها کنترل عددی ما بر یک چندجمله‌ای درجه‌اش می‌باشد. لذا چرا از تابع درجه به‌عنوان مکانیسمی در یافتن $q(x)$ استفاده نکنیم.

چون $I \neq (0)$، عناصری در I با درجهٔ نامنفی وجود دارند. لذا یک چندجمله‌ای مانند $g(x) \neq 0$ در I با درجهٔ مینیمم وجود دارد؛ یعنی $g(x) \neq 0$ در I است و هرگاه $t(x) \in I$ $\neq 0$، آن‌گاه $\deg g(x) \geq \deg t(x)$. لذا، طبق الگوریتم تقسیم، $t(x) = q(x)g(x) + r(x)$ که در آن $r(x) = 0$ یا $\deg r(x) < \deg g(x)$. ولی چون $g(x) \in I$ و I یک ایده‌آل $F[x]$ است، داریم $q(x)g(x) \in I$. طبق فرض، $t(x) \in I$. لذا $t(x) - q(x)g(x)$ در I است. پس $r(x) = t(x) - q(x)g(x)$ در I می‌باشد. چون $g(x)$ در میان عناصر I درجهٔ مینیمم دارد و $r(x) \in I$، پس $\deg r(x)$ نمی‌تواند از $\deg g(x)$ کمتر باشد. لذا تنها باید $r(x) = 0$. ولی این می‌گوید که $t(x) = q(x)g(x)$. لذا هر عنصر I مضربی از $g(x)$ است. از آن‌سو، چون $g(x) \in I$ و I ایده‌آلی از $F[x]$ است، به ازای هر $f(x) \in F[x]$، $f(x)g(x) \in I$. خلاصه آنکه $I = \{f(x)g(x) | f(x) \in F[x]\}$. ■

تعریف. قلمرو صحیح R را یک قلمرو ایده‌آل اصلی گویند اگر هر ایده‌آل I در R به ازای $a \in R$ای به شکل $I = \{xa | x \in R\}$ باشد.

قضیهٔ ۶.۵.۴ را می‌توان چنین بیان کرد: $F[x]$ یک قلمرو ایده‌آل اصلی است.

ما ایده‌آل تولید شده به‌وسیلهٔ چندجمله‌ای $g(x)$، یعنی $\{f(x)g(x) | f(x) \in F[x]\}$، را

به‌صورت $(g(x))$ می‌نویسیم.

برهان فوق نشان می‌دهد که اگر I یک ایده‌آل R باشد، $I = (g(x))$ که در آن $g(x)$ یک چندجمله‌ای با کمترین درجه در I است. ولی $g(x)$ منحصر به‌فرد نیست، زیرا هرگاه $a \neq 0 \in F$، آن‌گاه $ag(x)$ در I است و همان درجهٔ $g(x)$ را دارد؛ در نتیجه $I = (ag(x))$.

برای به‌دست آوردن نوعی یکتایی، یک رده از چندجمله‌ایها را ممتاز می‌سازیم.

تعریف. $f(x) \in F[x]$ یک چندجمله‌ای تکین است اگر ضریب بزرگترین توانش ۱ باشد.

لذا تکین بودن $f(x)$ یعنی

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a.$$

بر خواننده است نشان دهد که اگر I یک ایده‌آل $F[x]$ باشد، تنها یک چندجمله‌ای از پایین‌ترین درجه در I موجود است. با ممتازکردن این به‌عنوان مولد I، یکتایی «تکین» برای مولد I به‌دست می‌آید.

گام بعدی در این بحث که به موازات بحث اعداد صحیح پیش می‌رود تقسیم یک چندجمله‌ای بر دیگری است.

تعریف. هرگاه $f(x)$ و $g(x) \neq 0$ در $F[x]$ باشند، آن‌گاه $g(x)$ چندجمله‌ای $f(x)$ را عاد می‌کند، که به‌صورت $g(x)|f(x)$ نوشته می‌شود، اگر به ازای $a(x) \in F[x]$ی، $f(x) = a(x)g(x)$.

توجه کنید که هرگاه $g(x)|f(x)$، آن‌گاه بنابر لم ۲.۵.۴، $\deg g(x) \leq \deg f(x)$. همچنین توجه کنید که هرگاه $g(x)|f(x)$، آن‌گاه ایده‌آلهای $(f(x))$ و $(g(x))$ از $F[x]$ که به ترتیب با $f(x)$ و $g(x)$ تولید می‌شوند در رابطهٔ شمول $(f(x)) \subset (g(x))$ صدق می‌کنند. (ثابت کنید!)

مجدداً بر توازی بین مجموعهٔ اعداد صحیح $\mathbb{Z}$ و $F[x]$ در رابطه با مفهوم بزرگترین مقسوم‌علیه مشترک تأکید می‌کنیم. برای به دست آوردن نوعی یکتایی قید می‌کنیم که بزرگترین مقسوم‌علیه مشترک همواره یک چندجمله‌ای تکین است.

تعریف. به ازای هر دو چندجمله‌ای $f(x)$ و $g(x)$ در $F[x]$ (که هر دو ۰ نباشند)، چندجمله‌ای $d(x) \in F[x]$ بزرگترین مقسوم‌علیه مشترک $f(x)$ و $g(x)$ است اگر $d(x)$ یک چندجمله‌ای تکین باشد به‌طوری که

الف) $d(x)|f(x)$ و $d(x)|g(x)$؛

ب) هرگاه $h(x)|f(x)$ و $h(x)|g(x)$، آن‌گاه $h(x)|d(x)$.

با آنکه بزرگترین مقسوم‌علیه مشترک دو چندجمله‌ای را تعریف کرده‌ایم، ولی نه وجودش را می‌دانیم و نه شکلش را. می‌توان آن را به طریق معادل دیگر به‌عنوان چندجمله‌ای تکین از بالاترین درجه که هر دوی $f(x)$ و $g(x)$ را عاد می‌کند تعریف کرد. اگر چنین کنیم، وجودش خودبه‌خود ثابت می‌شود ولی شکلش معلوم نیست.

قضیهٔ ۷.۵.۴. هرگاه $f(x)$ و $g(x) \neq ۰$ در $F[x]$ باشند، آن‌گاه بزرگترین مقسوم‌علیه مشترکشان $d(x) \in F[x]$ موجود است. به‌علاوه، به ازای $a(x), b(x) \in F[x]$ی، $d(x) = a(x)f(x) + b(x)g(x)$.

برهان. فرض کنیم I مجموعهٔ تمام $r(x)f(x) + s(x)g(x)$هایی باشد که $r(x)$ و $s(x)$ در $F[x]$ تغییر می‌کنند. I یک ایده‌آل R است زیرا

$$\begin{aligned}(r_۱(x)f(x) + s_۱(x)g(x)) + (r_۲(x)f(x) + s_۲(x)g(x))\\ = (r_۱(x) + r_۲(x))f(x) + (s_۱(x) + s_۲(x))g(x)\end{aligned}$$

در نتیجه در I است، و به ازای $t(x) \in F[x]$ داریم

$$t(x)(r(x)f(x) + s(x)g(x)) = (t(x)r(x))f(x) + (t(x)s(x))g(x)$$

لذا این نیز در I است. پس I یک ایده‌آل $F[x]$ می‌باشد. چون $g(x) \neq ۰$، پس $I \neq ۰$ زیرا هر دوی $f(x)$ و $g(x)$ در I می‌باشند.

چون $I \neq ۰$ یک ایده‌آل $F[x]$ است، به‌وسیلهٔ یک چندجمله‌ای تکین منحصر به‌فرد مانند $d(x)$ تولید می‌شود (قضیهٔ ۶.۵.۴). و چون $f(x)$ و $g(x)$ در Iاند، باید حاصلضرب $d(x)$ در عناصری از $F[x]$ باشند. این تضمین می‌کند که $d(x)|f(x)$ و $d(x)|g(x)$.

از آنجا که $d(x) \in I$ و I مجموعهٔ تمام $r(x)f(x) + s(x)g(x)$هاست، به ازای $a(x)\ ,\ b(x) \in F[x]$ی داریم $d(x) = a(x)f(x) + b(x)g(x)$. لذا هرگاه $h(x)|f(x)$ و $h(x)|g(x)$، آن‌گاه $h(x)|a(x)f(x) + b(x)g(x) = d(x)$. پس $d(x)$ بزرگترین مقسوم‌علیه مشترک $f(x)$ و $g(x)$ می‌باشد.

این امر قضیه را ثابت می‌کند. یکتایی $d(x)$ با این قرار که بزرگترین مقسوم‌علیه مشترک باید تکین باشد تضمین خواهد شد. ■

لم زیر یکتایی $d(x)$ را به طریقی دیگر ثابت می‌کند.

لم ۸.۵.۴. هرگاه $f(x) \neq ۰$ و $g(x) \neq ۰$ در $F[x]$ بوده و $f(x)|g(x)$ و $g(x)|f(x)$، آن‌گاه $f(x) = ag(x)$ که در آن $a \in F$.

برهان. بنابر شرط بخشپذیری متقابل بر $f(x)$ و $g(x)$، از لم ۲.۵.۴ داریم

$$\deg f(x) \leq \deg g(x) \leq \deg f(x)$$

در نتیجه $\deg f(x) = \deg g(x)$. ولی $f(x) = a(x)g(x)$. پس

$$\deg f(x) = \deg a(x) + \deg g(x) = \deg a(x) + \deg f(x)$$

در نتیجه $\deg a(x) = ۰$. لذا $a(x) = a$ عنصری از F می‌باشد. ■

اثبات یکتایی بزرگترین مقسوم‌علیه مشترک به‌وسیلهٔ لم ۸.۵.۴ را به خواننده محول می‌کنیم.

تعریف. چندجمله‌ایهای $f(x)$ و $g(x)$ در $F[x]$ را نسبت به هم اول گوییم اگر بزرگترین مقسوم‌علیه مشترکشان ۱ باشد.

قضیهٔ زیر حالت بسیار خاصی از قضیهٔ ۷.۵.۴ است و صرفاً جهت تأکید و ارجاع ذکر می‌شود.

قضیهٔ ۹.۵.۴. هرگاه $f(x), g(x) \in F[x]$ نسبت به هم اول باشند، آن‌گاه به ازای $a(x), b(x) \in F[x]$ی، $a(x)f(x) + b(x)g(x) = ۱$. به‌عکس، هرگاه به ازای $a(x), b(x) \in F[x]$ی، $a(x)f(x) + b(x)g(x) = ۱$، آن‌گاه $f(x)$ و $g(x)$ نسبت به هم اول می‌باشند.

برهان. اثبات قسمت «عکس» را به‌عنوان تمرین می‌گذاریم. ■

همانند اعداد صحیح داریم:

قضیهٔ ۱۰.۵.۴. هرگاه $q(x)$ و $f(x)$ نسبت به هم اول بوده و $q(x)|f(x)g(x)$، آن‌گاه $q(x)|g(x)$.

برهان. بنابر قضیهٔ ۹.۵.۴، به ازای $a(x), b(x) \in F[x]$ی، $a(x)f(x) + b(x)q(x) = ۱$. بنابراین

$$a(x)f(x)g(x) + b(x)q(x)g(x) = g(x) \qquad (۱)$$

چون طبق فرض $q(x)|b(x)g(x)q(x)$ و $q(x)|f(x)g(x)$، $q(x)$ طرف چپ رابطهٔ (۱) را عاد می‌کند. لذا $q(x)$ طرف راست (۱) را نیز عاد می‌کند؛ یعنی $q(x)|g(x)$ که همان نتیجهٔ مطلوب است. ■

حال آماده‌ایم تا ردهٔ مهمی از چندجمله‌ایها را که نقششان در $F[x]$ مانند نقش اعداد اول در $\mathbb{Z}$ است ممتاز سازیم.

تعریف. چندجمله‌ای $p(x) \in F[x]$ از درجهٔ مثبت در $F[x]$ تحویل‌ناپذیر است اگر به ازای هر چندجمله‌ای $f(x)$ در $F[x]$، $p(x)|f(x)$ یا $p(x)$ نسبت به $f(x)$ اول باشد.

از تعریف فوق نتیجه می‌شود که $p(x)$ در $F[x]$ تحویل‌ناپذیر است اگر و فقط اگر $p(x)$ را نتوان به‌صورت حاصلضربی از دو چندجمله‌ای از درجهٔ مثبت تجزیه کرد. (ثابت کنید!) یعنی، به بیان دیگر، هرگاه $p(x) = a(x)b(x)$ که در آن $a(x)$ و $b(x)$ در $F[x]$اند، آن‌گاه $a(x)$ یا $b(x)$ ثابت است (عنصری از F = ثابت).

توجه کنید که تحویل‌ناپذیری یک چندجمله‌ای تابع میدان F است. مثلاً چندجمله‌ای $x^۲ - ۲$ در $\mathbb{Q}[x]$، که در آن $\mathbb{Q}$ میدان اعداد گویاست، تحویل‌ناپذیر است ولی $x^۲ - ۲$ در $\mathbb{R}[x]$، که در آن $\mathbb{R}$ میدان اعداد حقیقی است، تحویل‌ناپذیر نیست، زیرا در $\mathbb{R}[x]$

$$x^۲ - ۲ = (x - \sqrt{۲})(x + \sqrt{۲})$$

نتیجهٔ قضیهٔ ۱۰.۵.۴. هرگاه $p(x)$ در $F[x]$ تحویل‌ناپذیر بوده و $p(x)|a_۱(x)a_۲(x)\cdots a_k(x)$ که در آن $a_۱(x)$، $\cdots$، $a_k(x)$ در $F[x]$اند، آن‌گاه به ازای iای، $p(x)|a_i(x)$.

برهان. اثبات به خواننده محول می‌شود. (ر.ک. قضیهٔ ۶.۵.۱.) ■

چندجمله‌ای تحویل‌ناپذیر $p(x)$ در $F[x]$ علاوه بر خواص دیگر دارای این ویژگی است که $(p(x))$، یعنی ایده‌آل تولید شده به‌وسیلهٔ $p(x)$ در $F[x]$، یک ایده‌آل ماکزیمال $F[x]$ است. این مطلب ذیلاً به ثبوت می‌رسد.

قضیهٔ ۱۱.۵.۴. هرگاه $p(x) \in F[x]$، آن‌گاه ایده‌آل $(p(x))$ تولید شده به‌وسیلهٔ $p(x)$ در $F[x]$ یک ایده‌آل ماکزیمال $F[x]$ است اگر و فقط اگر $p(x)$ در $F[x]$ تحویل‌ناپذیر باشد.

برهان. ابتدا ثابت می‌کنیم هرگاه $p(x)$ در $F[x]$ تحویل‌ناپذیر باشد، آن‌گاه ایده‌آل $M = (p(x))$

یک ایده‌آل ماکزیمال $F[x]$ است. زیرا فرض کنیم N ایده‌آلی از $F[x]$ باشد و $N \supset M$. بنابر قضیهٔ ۶.۵.۴،

$$N = (f(x)) \quad \text{به ازای } f(x) \in F[x]\text{ی،}$$

چون $p(x) \in M \subset N$، $p(x) = a(x)f(x)$ زیرا هر عنصر در N به این شکل است. ولی $p(x)$ در $F[x]$ تحویل‌ناپذیر است؛ در نتیجه $a(x)$ یا $f(x)$ ثابت است. هرگاه $a(x) = a \in F$، آن‌گاه $p(x) = af(x)$؛ در نتیجه $f(x) = a^{-1}p(x)$. پس $f(x) \in M$ مبین آنکه $N \subset M$. لذا $N = M$. از آن‌سو، هرگاه $f(x) = b \in F$، آن‌گاه $1 = b^{-1}b \in N$ زیرا N یک ایده‌آل $F[x]$ است. لذا به ازای هر $g(x) \in F[x]$، $g(x)1 \in N$. این مبین آن است که $N = F[x]$. بنابراین نشان داده‌ایم که M یک ایده‌آل ماکزیمال $F[x]$ باشد.

از آن‌سو، فرض کنیم $M = (p(x))$ یک ایده‌آل ماکزیمال $F[x]$ باشد، هرگاه $p(x)$ تحویل‌ناپذیر نباشد، آن‌گاه $p(x) = a(x)b(x)$ که در آن $\deg a(x) \geq 1$ و $\deg b(x) \geq 1$. قرار می‌دهیم $N = (a(x))$. چون $p(x) = a(x)b(x)$، داریم $p(x) \in N$. لذا $M \subset N$. و چون $\deg a(x) \geq 1$، $N = (a(x)) \neq F[x]$ زیرا هر عنصر در $(a(x))$ درجه‌ای دست‌کم برابر درجهٔ $a(x)$ دارد. از ماکزیمالی M نتیجه می‌گیریم که $M = N$. ولی در این صورت $a(x) \in N = M$ که به ما می‌گوید که $a(x) = f(x)p(x)$. از تلفیق این با $p(x) = a(x)b(x) = b(x)f(x)p(x)$ به‌دست می‌آوریم $b(x)f(x) = 1$. چون

$$\deg 1 = 0 < \deg b(x) \leq \deg(b(x)f(x)) = \deg 1 = 0$$

به تناقض می‌رسیم. لذا $p(x)$ تحویل‌ناپذیر می‌باشد. ■

این قضیه از آنجهت مهم است که دقیقاً ایده‌آلهای ماکزیمال $F[x]$، یعنی ایده‌آلهای تولید شده به‌وسیلهٔ چندجمله‌ای تحویل‌ناپذیر، را مشخص می‌کند. اگر M یک ایده‌آل ماکزیمال $F[x]$ باشد، $F[x]/M$ یک میدان است و این میدان شامل F (یا، به‌طور دقیقتر، میدان $\{a + M | a \in F\}$ که با F یکریخت است) می‌باشد. این امر به ما اجازهٔ ساختن میدانهای ظریفی چون $K \supset F$ را می‌دهد که ظرافتشان در این است که $p(x)$ در K یک ریشه دارد. بیان و توضیح دقیق این امر را به فصل ۵ موکول می‌کنیم.

آخرین مطلب در این راستا تجزیهٔ یک چندجمله‌ای به حاصلضرب چندجمله‌ایهای تحویل‌ناپذیر است. توجه کنید که هرگاه $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ $(a_0 \neq 0)$ در $F[x]$ تحویل‌ناپذیر باشد، آن‌گاه $a_0^{-1}p(x)$ نیز در $F[x]$ چنین است. ولی $a_0^{-1}p(x)$ این مزیت

را دارد که تکین است. لذا این چندجمله‌ای تحویل‌ناپذیر تکین را داریم که بداهتاً از خود $p(x)$ حاصل می‌شود. با این امر می‌توان بخش یکتایی قضیهٔ بعد را دقیقتر ساخت.

قضیهٔ ۱۲.۵.۴. فرض کنیم $f(x) \in F[x]$ از درجهٔ مثبت باشد. در این صورت $f(x)$ در $F[x]$ تحویل‌ناپذیر است یا $f(x)$ حاصلضرب چندجمله‌ایهای تحویل‌ناپذیر در $F[x]$ می‌باشد. در واقع

$$f(x) = ap_1(x)^{m_1}p_2(x)^{m_2}\cdots p_k(x)^{m_k}$$

که در آن a بالاترین ضریب $f(x)$ بوده، $p_1(x)$، $\cdots$، $p_k(x)$ در $F[x]$ تکین و تحویل‌ناپذیرند، $m_1 > 0$، $\cdots$، $m_k > 0$، و این تجزیه صرف‌نظر از ترتیب $p_i(x)$ها منحصر به‌فرد می‌باشد.

برهان. ابتدا نیمهٔ اول قضیه را نشان می‌دهیم؛ یعنی $f(x)$ تحویل‌ناپذیر یا حاصلضربی از تحویل‌ناپذیرهاست. برهان همان برهان قضیهٔ ۷.۵.۱ است منتها با کمی تغییر.

روی $\deg f(x)$ استقرا می‌کنیم. هرگاه $\deg f(x) = 1$، آن‌گاه $f(x) = ax + b$ که در آن $a \neq 0$ و به وضوح در $F[x]$ تحویل‌ناپذیر است. لذا مطلب در این حالت درست است.

حال فرض کنیم قضیه برای هر $a(x) \in F[x]$ که $\deg a(x) < \deg f(x)$ درست باشد. هرگاه $f(x)$ تحویل‌ناپذیر باشد، آن‌گاه چیزی برای اثبات نداریم. در غیر این‌صورت

$$f(x) = a(x)b(x)$$

که در آن $a(x)$ و $b(x)$ در $F[x]$اند و $\deg a(x) < \deg f(x)$ و $\deg b(x) < \deg f(x)$. بنا به فرض استقرا، $a(x)$ [و $b(x)$] تحویل‌ناپذیر است یا حاصلضربی است از تحویل‌ناپذیرها. در این صورت $f(x)$ حاصلضربی از چندجمله‌ایهای تحویل‌ناپذیر در $F[x]$ می‌باشد. این استقرا را کامل کرده و نیمهٔ اول قضیه را به ثبوت می‌رساند.

حال به قسمت یکتایی می‌پردازیم. مجدداً روی $\deg f(x)$ استقرا می‌کنیم. اگر $\deg f(x) = 1$، آن‌گاه $f(x)$ تحویل‌ناپذیر بوده و یکتایی واضح است.

فرض کنیم نتیجه برای چندجمله‌ایها از درجهٔ کمتر از $\deg f(x)$ درست باشد. همچنین

$$f(x) = ap_1(x)^{m_1}p_2(x)^{m_2}\cdots p_k(x)^{m_k} = aq_1(x)^{n_1}\cdots q_r(x)^{n_r}$$

که در آن $p_i(x)$ها و $q_i(x)$ها چندجمله‌ایهای تحویل‌ناپذیر تکین بوده و m_iها و n_iها همه مثبت‌اند و a بالاترین ضریب $f(x)$ می‌باشد. چون $p_1(x)|f(x)$، داریم $p_1(x)|q_1(x)^{n_1}\cdots q_r(x)^{n_r}$.

پس، بنابر نتیجهٔ قضیهٔ ۱۰.۵.۴، به ازای iی، $p_1(x)|q_i(x)$. چون $q_i(x)$ مانند $p_1(x)$ تکین و تحویل‌ناپذیر است، داریم $p_1(x) = q_i(x)$. می‌توان (با اندیسگذاری مجدد) فرض کرد که $p_1(x) = q_1(x)$. لذا

$$\begin{aligned}\frac{f(x)}{p_1(x)} &= ap_1(x)^{m_1-1}p_2(x)^{m_2}\cdots p_k(x)^{m_k}\\ &= ap_1(x)^{n_1-1}q_2(x)^{n_2}\cdots q_r(x)^{n_r}\end{aligned}$$

بنا به فرض استقرا، برای $f(x)/p_1(x)$ (که درجه‌اش از $\deg f(x)$ کمتر است) تجزیهٔ منحصربه‌فردی به شکل مطلوب وجود دارد. لذا، با اندیسگذاری مجدد qها، به‌دست می‌آوریم $m_1 - 1 = n_1 - 1$ (در نتیجه $m_1 = n_1$)، $m_2 = n_2$، $\cdots$، $m_k = n_k$، $r = k$، و $p_2(x) = q_2(x)$، $\cdots$، $p_k(x) = q_k(x)$. ■

ما قبلاً به تشابه بین مجموعهٔ اعداد صحیح $\mathbb{Z}$ و حلقهٔ چندجمله‌ایهای $F[x]$ اشاره کردیم. این امر القاگر آن است که باید ردهٔ وسیعتری از حلقه‌ها (که $\mathbb{Z}$ و $F[x]$ حالات خاصی در آنند) موجود باشد که در آن بیشتر مطالب ما برقرار باشند. این مطالب از آنجهت برای $\mathbb{Z}$ و $F[x]$ برقرار بودند که در آنها یک اندازه (اندازهٔ یک عدد صحیح یا درجهٔ یک چندجمله‌ای) داشتیم. این اندازه چنان بود که یک الگوریتم اقلیدس گونه را برقرار می‌ساخت.

این امر ما را به تعریف رده‌ای از حلقه‌ها، یعنی حلقه‌های اقلیدسی، می‌کشاند.

تعریف. قلمرو صحیح R یک حلقهٔ اقلیدسی است اگر تابعی مانند d از عناصر ناصفر R به اعداد صحیح نامنفی موجود باشد به‌طوری که

الف) به ازای $a \neq 0, b \neq 0 \in R$، $d(a) \leq d(ab)$؛

ب) به ازای $a \neq 0$ و $b \neq 0$ عناصری مانند q و r در R باشند که $b = qa + r$ که در آن $r = 0$ یا $d(r) < d(a)$.

شاگرد علاقمند می‌تواند نتایج ثابت شده در حلقه‌های چندجمله‌ای (و اعداد صحیح) را در حلقهٔ اقلیدسی کلی امتحان کند. ما، جز در چند مسئلهٔ مربوط به حلقه‌های اقلیدسی، در این ردهٔ جالب از حلقه‌ها بیش از این پیش نخواهیم رفت.

آخرین تذکار ما در اینجا آن است که سعی می‌کنیم آنچه برای چندجمله‌ایها روی یک میدان شد برای چندجمله‌ایها روی یک حلقهٔ دلخواه انجام دهیم. یعنی اگر R یک حلقه (تعویضپذیر یا تعویض‌ناپذیر) باشد، می‌توان حلقهٔ چندجمله‌ای $R[x]$ از x روی R را با تعریف تساوی، جمع، و

و ضرب درست مثل $F[x]$، که در آن F یک میدان است، تعریف کرد. حلقه‌ای که به این نحو ساخته می‌شود، یعنی $R[x]$، حلقه‌ای است بسیار جالب که ساختارش با ساختار خود R ارتباط نزدیکی دارد. این انتظار که تمام (یا حتی بخشی از) قضایای ثابت شده در این بخش در $R[x]$ به ازای حلقهٔ کلی R برقرار باشد انتظاری است بیش از حد.

مسائل

در مسائل زیر F همواره یک میدان است.

مسائل آسانتر

۱. اگر F یک میدان باشد، نشان دهید که تنها عناصر معکوسپذیر $F[x]$ عنصرهای ناصفر F می‌باشند.

۲. اگر R یک حلقه باشد، حلقهٔ $R[x]$ چندجمله‌ایها از x روی R را درست مثل $F[x]$ و $\deg f(x)$ را برای $f(x) \in R[x]$ مثل $F[x]$ تعریف کرده و نشان دهید که

الف) اگر $f(x)g(x) \neq ۰$، $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$؛

ب) یک حلقهٔ تعویضپذیر مانند R هست به‌طوری که بتوان $f(x)$ و $g(x)$ را در $R[x]$ یافت که $\deg(f(x)g(x)) < \deg f(x) + \deg g(x)$.

۳. بزرگترین مقسوم‌علیه مشترک چندجمله‌ایهای زیر روی $\mathbb{Q}$ (میدان اعداد گویا) را بیابید:

الف) $x^۳ - ۶x + ۷$ و $x + ۴$؛

ب) $x^۲ - ۱$ و $۲x^۷ - ۴x^۵ + ۲$؛

پ) $۳x^۲ + ۱$ و $x^۶ + x^۴ + x + ۱$؛

ت) $x^۳ - ۱$ و $x^۷ - x^۴ + x^۳ - ۱$.

۴. لم ۳.۵.۴ را ثابت کنید.

۵. در مسئلهٔ ۳ فرض کنید $I = \{f(x)a(x) + g(x)b(x)\}$ که در آن $f(x)$ و $g(x)$ روی $\mathbb{Q}[x]$ تغییر کرده و $a(x)$ اولین و $b(x)$ دومین چندجمله‌ای در هر قسمت از مسئله باشند. $d(x)$ را طوری بیابید که در هر یک از قسمتهای (آ)، (ب)، (پ)، و (ت) داشته باشیم $I = (d(x))$.

۶. اگر $f(x), g(x) \in F[x]$ و $g(x)|f(x)$، نشان دهید که $(f(x)) \subset (g(x))$.

۷. یکتایی بزرگترین مقسوم‌علیه مشترک دو چندجمله‌ای در $F[x]$ را با استفاده از لم ۸.۵.۴ ثابت کنید.

۸. اگر $f(x), g(x) \in F[x]$ نسبت به هم اول بوده و $f(x)|h(x)$ و $g(x)|h(x)$، نشان دهید که $f(x)g(x)|h(x)$.

۹. نتیجهٔ قضیهٔ ۱۰.۵.۴ را ثابت کنید.

۱۰. نشان دهید که چندجمله‌ایهای زیر روی میدان F ذکر شده تحویل‌ناپذیرند:

الف) $x^2 + 7$ روی $\mathbb{R}$ = میدان حقیقی = F؛

ب) $x^3 - 3x + 3$ روی $\mathbb{Q}$ = میدان گویا = F؛

پ) $x^2 + x + 1$ روی $F = \mathbb{Z}_2$؛

ت) $x^2 + 1$ روی $F = \mathbb{Z}_{19}$؛

ث) $x^3 - 9$ روی $F = \mathbb{Z}_{13}$؛

ج) $x^4 + 2x^2 + 2$ روی $F = \mathbb{Q}$.

۱۱. اگر $p(x) \in F(x)$ از درجهٔ ۳ بوده و $p(x) = a_0x^3 + a_1x^2 + a_2x + a_3$، نشان دهید که $p(x)$ در صورتی روی F تحویل‌ناپذیر است که عنصری مانند $r \in F$ با خاصیت $p(r) = a_0r^3 + a_1r^2 + a_2r + a_3 = 0$ موجود نباشد.

۱۲. اگر $F \subset K$ دو میدان بوده و $f(x), g(x) \in F[x]$ در $F[x]$ نسبت به هم اول باشند، نشان دهید که اینها در $K[x]$ نیز نسبت به هم اولند.

مسائل با سطح متوسط

۱۳. فرض کنید $\mathbb{R}$ میدان اعداد حقیقی و $\mathbb{C}$ میدان اعداد مختلط باشد. نشان دهید که $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$. [راهنمایی. اگر $A = \mathbb{R}[x]/(x^2 + 1)$، u را نقش x در A گرفته و نشان دهید که هر عنصر در A به شکل $a + bu$ است که در آن $a, b \in \mathbb{R}$ و $u^2 = -1$.]

۱۴. فرض کنید $F = \mathbb{Z}_{11}$ یعنی مجموعهٔ اعداد صحیح $\bmod 11$ باشد.

الف) اگر $p(x) = x^2 + 1$، نشان دهید که $p(x)$ در $F[x]$ تحویل‌ناپذیر است و $F[x]/(p(x))$ میدانی با ۱۲۱ عنصر می‌باشد.

ب) اگر $p(x) = x^3 + x + 4 \in F[x]$، نشان دهید که $p(x)$ در $F[x]$ تحویل‌ناپذیر بوده و $F[x]/(p(x))$ میدانی با 11^3 عنصر می‌باشد.

۱۵. فرض کنید $F = \mathbb{Z}_p$ میدان اعداد صحیح $\bmod p$ باشد که در آن p اول است و $q(x) \in F[x]$ تحویل‌ناپذیر از درجهٔ n باشد. نشان دهید که $F[x]/(q(x))$ میدانی است با حداکثر p^n عنصر. (برای حکم دقیقتر، ر.ک. مسئلهٔ ۱۶.)

۱۶. اگر F و $q(x)$ همانند مسئلهٔ ۱۵ باشند، نشان دهید که $F[x]/(q(x))$ درست p^n عنصر

دارد.

۱۷. اگر $p_1(x), p_2(x), \dots, p_k(x) \in F[x]$ چندجمله‌ایهای تحویل‌ناپذیر متمایزی بوده و $q(x) = p_1(x)p_2(x)\cdots p_k(x)$، نشان دهید که

$$\frac{F[x]}{(q(x))} \simeq \frac{F[x]}{(p_1(x))} \oplus \frac{F[x]}{(p_2(x))} \oplus \cdots \oplus \frac{F[x]}{(p_k(x))}$$

۱۸. اگر F یک میدان متناهی باشد، نشان دهید که $F[x]$ شامل چندجمله‌ایهای تحویل‌ناپذیر از درجهٔ بالای دلخواه است. (راهنمایی. از برهان اقلیدس در مورد وجود بی‌نهایت عدد اول تقلید کنید.)

۱۹. به ازای هر عدد اول فرد p، میدانی با p^2 عنصر بسازید.

۲۰. اگر R یک حلقهٔ اقلیدسی باشد، نشان دهید که هر ایده‌آل R اصلی است.

۲۱. اگر R یک حلقهٔ اقلیدسی باشد، نشان دهید که R دارای عنصر یکه است.

۲۲. اگر R حلقهٔ اعداد صحیح زوج باشد، با یافتن دو عدد صحیح زوج که الگوریتم اقلیدس برایشان برقرار نباشد، نشان دهید که این الگوریتم در R درست نیست.

مسائل مشکلتر

۲۳. اگر $F = \mathbb{Z}_7$ و $p(x) = x^3 - 2$ و $q(x) = x^3 + 2$ در $F[x]$ باشند، نشان دهید که $p(x)$ و $q(x)$ در $F[x]$ تحویل‌ناپذیر بوده و میدانهای $F[x]/(p(x))$ و $F[x]/(q(x))$ یکریخت‌اند.

۲۴. فرض کنید $\mathbb{Q}$ میدان اعداد گویا بوده و $q(x) = x^2 + x + 1$ در $\mathbb{Q}[x]$ باشد. اگر عدد مختلط α چنان باشد که $\alpha^2 + \alpha + 1 = 0$، به دو طریق نشان دهید که مجموعهٔ $\{a + b\alpha | a, b \in \mathbb{Q}\}$ یک میدان است: ابتدا با نشان دادن اینکه با میدانی که می‌شناسید یکریخت است، بعد با نشان دادن اینکه اگر $a + b\alpha \neq 0$، معکوسش به همین شکل می‌باشد.

۲۵. اگر p اول باشد، نشان دهید که $q(x) = 1 + x + x^2 + \cdots + x^{p-1}$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

۲۶. فرض کنید R یک حلقهٔ تعویضپذیر باشد که در آن $a^2 = 0$ فقط اگر $a = 0$. نشان دهید هرگاه $q(x) \in R[x]$ در $R[x]$ مقسوم‌علیه صفر باشد، آنگاه چنانچه

$$q(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

عنصری مانند $b \neq 0$ در R هست به‌طوری که $ba_0 = ba_1 = \cdots = ba_n = 0$.

۲۷. فرض کنید R یک حلقه و I ایده‌آلی از آن باشد. اگر $R[x]$ و $I[x]$ حلقه‌های چندجمله‌ای از x به ترتیب روی R و I باشند، نشان دهید که
الف) $I[x]$ یک ایده‌آل $R[x]$ است؛
ب) $R[x]/I[x] \simeq (R/I)[x]$.

مسائل بسیارمشکل

*۲۸. مسئلهٔ ۲۶ راحتی اگر شرط «$a^2 = 0$ فقط اگر $a = 0$» در R برقرار نباشد حل نمایید.

۲۹. به فرض آنکه $R = \{a + bi | \text{صحیح } b \text{ و } a\} \subset \mathbb{C}$ و $d(a+bi) = a^2 + b^2$، نشان دهید که R با این d به‌عنوان تابع اقلیدسی یک حلقهٔ اقلیدسی است. (R به حلقهٔ اعداد صحیح گاوسی معروف است و نقش مهمی در نظریهٔ اعداد دارد.)

۶. چندجمله‌ایها روی اعداد گویا

در بحث حلقهٔ چندجمله‌ای $F[x]$ روی میدان F سرشت خاص F هرگز وارد کار نشد. همهٔ نتایج ما در میدانهای دلخواه برقرارند. اما نتایجی هستند که از ویژگی صریح بعضی از میدانها استفاده می‌کنند. یکی از این میدانها میدان اعداد گویا می‌باشد.

ما برای $\mathbb{Q}[x]$، یعنی حلقهٔ چندجمله‌ای روی میدان گویای $\mathbb{Q}$، دو قضیهٔ مهم ارائه می‌دهیم. این نتایج قویاً به این امر که با اعداد گویا کار می‌کنیم بستگی دارند. اولین آنها، یعنی لم گاوس، تجزیه روی اعداد گویا را به تجزیه روی اعداد صحیح ربط می‌دهد. دومین قضیه، که به محک آیزن اشتاین معروف است، روشی برای ساختن چندجمله‌ایهای تحویل‌ناپذیر از درجهٔ دلخواه در $\mathbb{Q}[x]$ به‌دست می‌دهد. در این قضیه $\mathbb{Q}$ بسیار خاص می‌باشد. مثلاً برای یافتن چندجمله‌ایهای تحویل‌ناپذیر از درجهٔ دلخواه n روی میدان $\mathbb{Z}_p$ اعداد صحیح $\bmod p$ ، که در آن p اول است، الگوریتم خاصی وجود ندارد. حتی این الگوریتم روی $\mathbb{Z}_2$ نیز موجود نیست. اگر می‌بود خیلی (به‌خصوص در نظریهٔ رمز) مفید بود. ولی تاکنون این الگوریتم به‌دست نیامده است.

بحث را با دو نتیجهٔ ساده آغاز می‌کنیم.

لم ۱.۶.۴. هرگاه $f(x) \in \mathbb{Q}[x]$، آن‌گاه

$$f(x) = \frac{u}{m}(a_0 x^n + a_1 x^{n-1} + \cdots + a_n)$$

که در آن u، m، a_0، $\cdots$، a_n صحیح بوده و a_0، a_1، $\cdots$، a_n عامل مشترک بزرگتر از ۱ ندارند (یعنی نسبت به هم اولند) و $(u, m) = 1$.

برهان. چون $f(x) \in \mathbb{Q}[x]$، $f(x) = q_\circ x^n + q_1 x^{n-1} + \cdots + q_n$ که در آن q_iها اعدادی گویا می‌باشند. پس به ازای هر $i = \circ, 1, 2, \ldots, n$، $q_i = b_i/c_i$ که در آن b_iها و c_iها صحیح‌اند. لذا

$$f(x) = \frac{b_\circ}{c_\circ}x^n + \frac{b_1}{c_1}x^{n-1} + \cdots + \frac{b_n}{c_n}$$

اگر مخرجها را از بین ببریم، داریم

$$f(x) = \frac{1}{c_\circ c_1 \cdots c_n}(u_\circ x^n + u_1 x^{n-1} + \cdots + u_n)$$

که در آن u_iها صحیح‌اند. هرگاه w بزرگترین مقسوم‌علیه مشترک $u_\circ$، u_1، $\cdots$، u_n باشد، آن‌گاه هر $u_i = wa_i$ که در آن اعداد صحیح $a_\circ$، a_1، $\cdots$، a_n نسبت به هم اولند. در این صورت

$$f(x) = \frac{w}{c_\circ c_1 c_2 \cdots c_n}(a_\circ x^n + a_1 x^{n-1} + \cdots + a_n)$$

با حذف بزرگترین عامل مشترک w و $c_\circ c_1 \cdots c_n$ نتیجه می‌شود که

$$f(x) = \frac{u}{m}(a_\circ x^n + \cdots + a_n)$$

که در آن، همان‌طور که در لم حکم شده، u و m نسبت به هم اولند. ■

لم بعد نتیجه‌ای است راجع‌به نقش همریختی خاص $R[x]$ به ازای هر حلقهٔ R.

لم ۲.۶.۴. هرگاه R یک حلقه و I ایده‌آلی از آن باشد، آن‌گاه $I[x]$، یعنی حلقهٔ چندجمله‌ای از x روی I، یک ایده‌آل $R[x]$ است. به‌علاوه

$$R[x]/I[x] \simeq (R/I)[x] \quad (\text{حلقهٔ چندجمله‌ای از } x \text{ روی } R/I)$$

برهان. فرض کنیم $\bar{R} = R/I$. پس یک همریختی مانند $\varphi : R \to \bar{R}$ با تعریف $\varphi(a) = a + I$ وجود دارد که هسته‌اش I است. $\Phi : R[x] \to \bar{R}[x]$ را به‌صورت زیر تعریف می‌کنیم: هرگاه

$$f(x) = a_\circ x^n + a_1 x^{n-1} + \cdots + a_n$$

آن‌گاه

$$\Phi(f(x)) = \varphi(a_\circ)x^n + \varphi(a_1)x^{n-1} + \cdots + \varphi(a_n)$$

بر خواننده است ثابت کند که Φ یک همریختی از $R[x]$ به روی $\bar{R}[x]$ است. هستهٔ $K(\Phi)$ همریختی Φ چیست؟ هرگاه $f(x) = a_. x^n + \cdots + a_n$ در $K(\Phi)$ باشد، آن‌گاه $\Phi(f(x)) = \circ$ (عنصر ۰ حلقهٔ $\bar{R}[x]$). چون

$$\Phi(f(x)) = \varphi(a_.)x^n + \varphi(a_۱)x^{n-۱} + \cdots + \varphi(a_n) = \circ$$

از تعریف چندجمله‌ای ۰ در یک حلقهٔ چندجمله‌ای نتیجه می‌شود که $\varphi(a_.) = \circ$، $\varphi(a_۱) = \circ$، ...، $\varphi(a_n) = \circ$. لذا هر a_i در هستهٔ φ است که I می‌باشد. چون $a_.$، $a_۱$، ...، a_n در Iاند، $f(x) = a_.x^n + a_۱x^{n-۱} + \cdots + a_n$ در $I[x]$ می‌باشد. در نتیجه $K(\Phi) \subset I[x]$. رابطهٔ $I[x] \subset K[\Phi]$ فوراً از تعریف نگاشت Φ نتیجه می‌شود. لذا $K(\Phi) = I[x]$. پس، بنابر قضیهٔ اول همریختی (قضیهٔ ۳.۳.۴)، حلقهٔ $I[x]$ یک ایده‌آل $R[x]$ بوده و

$$\bar{R}[x] \simeq R[x]/K(\Phi) = R[x]/I[x]$$

این امر با توجه به $\bar{R} = R/I$ لم را ثابت خواهد کرد. ■

به‌عنوان حالت بسیار خاصی از لم فوق داریم:

نتیجه. فرض کنیم $\mathbb{Z}$ حلقهٔ اعداد صحیح، p عدد اولی در $\mathbb{Z}$، و $I = (p)$ ایده‌آل تولید شده به‌وسیلهٔ p از $\mathbb{Z}$ باشد. در این صورت $\mathbb{Z}[x]/I[x] \simeq \mathbb{Z}_p[x]$.

برهان. چون $\mathbb{Z}/I \simeq \mathbb{Z}_p$، نتیجه با اعمال لم فوق بر $R = \mathbb{Z}$ حاصل خواهد شد. ■

حال برای اثبات اولین نتیجه از دو نتیجهٔ مهم این بخش حاضر و آماده‌ایم.

قضیهٔ ۳.۶.۴ (لم گاوس). هرگاه $f(x) \in \mathbb{Z}[x]$ یک چندجمله‌ای تکین بوده و $f(x) = a(x)b(x)$ که در آن $a(x)$ و $b(x)$ در $\mathbb{Q}[x]$اند، آن‌گاه

$$f(x) = a_۱(x)b_۱(x)$$

که در آن $a_۱(x)$ و $b_۱(x)$ چندجمله‌ایهایی تکین در $\mathbb{Z}[x]$ بوده و $\deg a_۱(x) = \deg a(x)$ و $\deg b_۱(x) = \deg b(x)$.

برهان. فرض کنیم $f(x) = x^n + u_۱x^{n-۱} + \cdots + u_n$ که در آن $u_i \in \mathbb{Z}$ها صحیح‌اند. چون $a(x)$ و $b(x)$ در $\mathbb{Q}[x]$اند، $a(x) = a_.x^s + a_۱x^{s-۱} + \cdots + a_s$ و

$b(x) = b_\circ x^r + b_1 x^{r-1} + \cdots + b_r$ که در آن a_iها و b_iها اعدادی گویایند. بنابر لم ۱.۶.۴،

$$a(x) = \frac{u_1}{m_1}(a'_\circ x^s + a'_1 x^{s-1} + \cdots + a'_s) = \frac{u_1}{m_1} a_1(x)$$

که در آن $a'_\circ$، a'_1، $\cdots$، a'_s صحیح و نسبت به هم اول بوده و

$$b(x) = \frac{u_2}{m_2}(b'_\circ x^r + b'_1 x^{r-1} + \cdots + b'_r) = \frac{u_2}{m_2} b_1(x)$$

که در آن $b'_\circ$، b'_1، $\cdots$، b'_r صحیح و نسبت به هم اولند. لذا

$$f(x) = a(x)b(x) = \frac{u_1 u_2}{m_1 m_2} a_1(x) b_1(x) = \frac{v}{w} a_1(x) b_1(x)$$

که در آن، با حذف عامل مشترک $u_1 u_2$ و $m_1 m_2$، v و w نسبت به هم اولند. لذا

$$w f(x) = v a_1(x) b_1(x)$$

و $f(x)$، $a_1(x)$، و $b_1(x)$ همه در $\mathbb{Z}[x]$ می‌باشند.

هرگاه $w = 1$، آن‌گاه چون $f(x)$ تکین است، به‌دست می‌آوریم $v a'_\circ b'_\circ = 1$ و این به آسانی به $v = 1$ و $a'_\circ = b'_\circ = 1$[1] منجر می‌شود؛ و در نتیجه $f(x) = a_1(x) b_1(x)$ که در آن هر دوی $a_1(x)$ و $b_1(x)$ تکین با ضرایب صحیح می‌باشند. این همان حکم قضیه است زیرا $\deg a_1(x) = \deg a(x)$ و $\deg b_1(x) = \deg b(x)$.

حال فرض کنیم $w \neq 1$. لذا عدد اولی مانند p هست به‌طوری که $p|w$، و چون $(v, w) = 1$، $p \nmid v$. همچنین از اینکه ضرایب $a'_\circ$، a'_1، $\cdots$، a'_s از $a_1(x)$ نسبت به هم اولند نتیجه می‌شود که iای هست به‌طوری که $p \nmid a'_i$. به همین نحو jای هست به‌طوری که $p \nmid b'_j$. فرض کنیم $I = (p)$ ایده‌آل تولید شده به‌وسیلهٔ p در $\mathbb{Z}$ باشد. پس $\mathbb{Z}/I \simeq \mathbb{Z}_p$ و، بنا بر نتیجهٔ لم ۲.۶.۴، $\mathbb{Z}[x]/I[x] \simeq \mathbb{Z}_p[x]$؛ در نتیجه یک قلمرو صحیح است. اما چون $p|w$، $\bar{w}$، یعنی نقش w در $\mathbb{Z}[x]/I[x]$، مساوی ۰ است، و چون $p \nmid v$، $\bar{v}$، یعنی نقش v در $\mathbb{Z}[x]/I[x]$، مساوی ۰ نیست. لذا $\bar{v}\bar{a}_1(x)\bar{b}_1(x) = f(x)$ ۰ که در آن $\bar{v} \neq 0$ و $\bar{a}_1(x) \neq 0$ و $\bar{b}_1(x) \neq 0$ زیرا به ازای i و j داده شده در فوق، $p \nmid a'_i$ و $p \nmid b'_j$. این امر با قلمرو صحیح بودن $\mathbb{Z}[x]/I[x]$ در تضاد است. پس $w \neq 1$ ممکن نیست و قضیه به اثبات می‌رسد. ■

خواننده می‌تواند مستقیماً نشان دهد که اگر $x^3 + 6x - 7$ حاصلضرب دو چندجمله‌ای با ضرایب گویا باشد، قبلاً حاصلضرب دو چندجمله‌ای تکین با ضرایب صحیح است.

---

۱. $a'_\circ = b'_\circ = -1$ نیز امکان دارد که در این حالت $-a_1(x)$ و $-b_1(x)$ تکین بوده و $f(x) = (-a_1(x))(-b_1(x))$.

لازم است چندکلمه‌ای راجع به سی.اف.گاوس (C. F. Gauss, 1777-1855) صحبت کنیم. بسیاری وی را بزرگترین ریاضیدان تمام قرون می‌دانند. آثارش در نظریهٔ اعداد، جبر، هندسه، و غیره عظیم است. کارهایش در فیزیک و نجوم آنچنان زیاد است که فیزیکدانان وی را یکی از بزرگان خود و منجمان وی را یکی از منجمان مهم به حساب می‌آورند.

همان‌طور که در ابتدای این بخش گفتیم، ساختن چندجمله‌ایهای تحویل‌ناپذیر از درجهٔ n روی میدان F ممکن است بسیار مشکل باشد. ولی، به‌خاطر قضیهٔ زیر، این چندجمله‌ایها روی اعداد گویا فراوان بوده و به آسانی ساخته می‌شوند.

قضیهٔ ۴.۶.۴ (محک آیزن اشتاین). فرض کنیم $f(x) = x^n+a_1x^{n-1}+\cdots+a_n$ یک چندجمله‌ای با ضرایب صحیح باشد. همچنین عدد اولی مانند p باشد به‌طوری که $p|a_1$، $p|a_2$، $\cdots$، $p|a_n$ ولی $p^2 \nmid a_n$. در این صورت $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

برهان. فرض کنیم $f(x) = u(x)v(x)$ که در آن $u(x)$ و $v(x)$ از درجهٔ مثبت بوده و چندجمله‌ایهایی در $\mathbb{Q}[x]$ باشند. بنابر لم گاوس، می‌توان فرض کرد که هر دوی $u(x)$ و $v(x)$ چندجمله‌ایهایی تکین با ضرایب صحیح باشند. فرض کنیم $I = (p)$ ایده‌آل تولید شده به‌وسیلهٔ p در $\mathbb{Z}$ باشد، و $\mathbb{Z}[x]/I[x]$ را در نظر می‌گیریم که یک قلمرو صحیح است زیرا از نتیجهٔ لم ۲.۶.۴ می‌دانیم که $\mathbb{Z}[x]/I[x] \simeq (\mathbb{Z}/I)[x] \simeq \mathbb{Z}_p[x]$. نقش $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ در $\mathbb{Z}[x]/I[x]$ مساوی x^n است زیرا $p|a_1$، $\cdots$، $p|a_n$. در نتیجه هرگاه $\bar{u}(x)$ نقش $u(x)$ و $\bar{v}(x)$ نقش $v(x)$ در $\mathbb{Z}[x]/I[x]$ باشد، آن‌گاه $\bar{u}(x)\bar{v}(x) = x^n$. چون در $\mathbb{Z}[x]/I[x]$ داریم $\bar{u}(x)|x^n$ و $\bar{v}(x)|x^n$، باید به ازای rی که $1 < r < n$ داشته باشیم $\bar{u}(x) = x^r$ و $\bar{v}(x) = x^{n-r}$. ولی در این صورت $u(x) = x^r + pg(x)$ و $v(x) = x^{n-r} + ph(x)$ که در آنها $g(x)$ و $h(x)$ چندجمله‌ایهایی با ضرایب صحیح‌اند. چون

$$u(x)v(x) = x^n + px^rh(x) + px^{n-r}g(x) + p^2g(x)h(x)$$

و $1 < r < n$، جملهٔ ثابت $u(x)v(x)$ مساوی p^2st است که در آن s جملهٔ ثابت $g(x)$ و t جملهٔ ثابت $h(x)$ می‌باشد. چون $f(x) = u(x)v(x)$، جملات ثابتشان مساویند. پس $a_n = p^2st$. و چون s و t صحیح‌اند، به‌دست می‌آوریم $p^2|a_n$ که تناقض است. بدین‌ترتیب معلوم می‌شود که $f(x)$ تحویل‌ناپذیر می‌باشد. ■

حال به چند مثال از طرز به کارگیری محک آیزن اشتاین اشاره می‌کنیم.

۱. فرض کنیم $f(x) = x^{۰n} - p$ که در آن p عددی اول است. با یک نگاه معلوم می‌شود که $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است زیرا محک آیزن اشتاین قابل اعمال است.

۲. فرض کنیم $f(x) = x^{۵} - ۴x + ۲۲$. چون $۲|-۴$، $۲|۲۲$، و $۲^{۲} \nmid ۲۲$، محک آیزن اشتاین به ما می‌گوید که $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

۳. فرض کنیم $f(x) = x^{۱۱} - ۶x^{۴} + ۱۲x^{۳} + ۳۶x - ۶$. با امتحان شرایط محک آیزن اشتاین به‌وسیلهٔ ۲ یا ۳ معلوم می‌شود که $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

۴. فرض کنیم $f(x) = ۵x^{۴} - ۷x + ۷$. $f(x)$ تکین نیست ولی می‌توان آن را با کمی تعدیل به‌صورتی درآورد که محک آیزن اشتاین به‌کار رود. فرض کنیم

$$g(x) = ۵^{۳}f(x) = ۵^{۴}x^{۴} - ۷\cdot ۵^{۳}x + ۷\cdot ۵^{۳} = (۵x)^{۴} - ۱۷۵(۵x) + ۸۷۵$$

هرگاه قرار دهیم $y = ۵x$، آن‌گاه $g(x) = h(y) = y^{۴} - ۱۷۵y + ۸۷۵$. با استفاده از عدد اول ۷ و اعمال محک آیزن اشتاین معلوم می‌شود که چندجمله‌ای $h(y)$ در $\mathbb{Q}[y]$ تحویل‌ناپذیر است. تحویل‌ناپذیری $h(y)$ ایجاب می‌کند که $g(x)$ و در نتیجه $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر باشد.

این امر تعمیم مختصر محک آیزن اشتاین به چندجمله‌ایهای ناتکین را پیشنهاد می‌کند. (ر.ک. مسئلهٔ ۴.)

۵. فرض کنیم $f(x) = x^{۴} + x^{۳} + x^{۲} + x + ۱$. محک آیزن اشتاین بر این $f(x)$ قابل اعمال نیست. ما به چندجمله‌ای $g(x)$ که به $f(x)$ بسیار نزدیک است می‌رویم که تحویل‌ناپذیری‌اش در $\mathbb{Q}[x]$ تحویل‌ناپذیری $f(x)$ را تضمین می‌کند. فرض کنیم

$$\begin{aligned} g(x) = f(x+۱) &= (x+۱)^{۴} + (x+۱)^{۳} + (x+۱)^{۲} + (x+۱) + ۱ \\ &= x^{۴} + ۵x^{۳} + ۱۰x^{۲} + ۱۰x + ۵ \end{aligned}$$

با استفاده از عدد اول ۵ می‌توان محک آیزن اشتاین را بر $g(x)$ اعمال کرد. لذا $g(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. این ایجاب می‌کند که $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر باشد. (ر.ک.مسئلهٔ ۱.)

گاتهولد آیزن اشتاین (Gotthold Eisenstein, 1833-1852) درحیات کوتاه خود کارهایی اساسی در جبر و آنالیز کرده است.

مسائل

۱. در مثال ۵ نشان دهید که $f(x)$ به خاطر تحویل‌ناپذیری $g(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

۲. ثابت کنید $f(x) = x^{3} + 3x + 2$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

۳. نشان دهید بی‌نهایت عدد صحیح مانند a هست به‌طوری‌که $f(x) = x^{7}+15x^{2}-30x+a$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. چه aهایی را پیشنهاد می‌کنید؟

۴. تعمیم زیر از محک آیزن اشتاین را ثابت کنید: فرض کنید

$$f(x) = a_0x^{n} + a_1x^{n-1} + \cdots + a_n$$

دارای ضرایب صحیح بوده و عدد اولی مانند p باشد به‌طوری که $p \nmid a_0$، $p|a_1$، $p|a_2$، $\cdots$، $p|a_{n-1}$، $p|a_n$ ولی $p^{2} \nmid a_n$. در این صورت $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

۵. اگر p اول باشد، نشان دهید که $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ در $Q[x]$ تحویل‌ناپذیر است.

۶. فرض کنید F یک میدان و φ یک خودریختی از $F[x]$ باشد به‌طوری که به ازای هر $a \in F$، $\varphi(a) = a$. اگر $f(x) \in F[x]$، ثابت کنید $f(x)$ در $F[x]$ تحویل‌ناپذیر است اگر و فقط اگر $g(x) = \varphi(f(x))$ چنین باشد.

۷. فرض کنید F یک میدان باشد. نگاشت $\varphi : F[x] \to F[x]$ را با $\varphi(f(x)) = f(x+1)$ به ازای هر $f(x) \in F[x]$ تعریف و ثابت کنید φ یک خودریختی از $F[x]$ است به‌طوری که به ازای هر $a \in F$، $\varphi(a) = a$.

۸. فرض کنید F یک میدان و $b \neq 0$ عنصری از آن باشد. نگاشت $\varphi : F[x] \to F[x]$ را با $\varphi(f(x)) = f(bx)$ به ازای هر $f(x) \in F[x]$ تعریف و ثابت کنید φ یک خودریختی از $F[x]$ است به‌طوری که به ازای هر $a \in F$، $\varphi(a) = a$.

۹. فرض کنید F یک میدان و $b \neq 0$ و c عناصری از آن باشند. نگاشت $\varphi : F[x] \to F[x]$ را با $\varphi(f(x)) = f(bx + c)$ به ازای هر $f(x) \in F[x]$ تعریف و ثابت کنید φ یک خودریختی از $F[x]$ است به‌طوری که به ازای هر $a \in F$، $\varphi(a) = a$.

۱۰. فرض کنید φ یک خودریختی از $F[x]$، که در آن F میدان است، باشد به‌طوری که به ازای هر $a \in F$، $\varphi(a) = a$. ثابت کنید هرگاه $f(x) \in F[x]$، آن‌گاه $\deg \varphi(f(x)) = \deg f(x)$.

۱۱. فرض کنید φ یک خودریختی از $F[x]$، که در آن F میدان است، باشد به‌طوری که به ازای هر $a \in F$، $\varphi(a) = a$. ثابت کنید $b \neq 0$ و cای در F موجودند به‌طوری که به ازای هر $f(x) \in F[x]$، $\varphi(f(x)) = f(bx + c)$.

۱۲. یک خودریختی غیرهمانی مانند φ از $\mathbb{Q}[x]$ چنان بیابید که $\varphi^{۲}$ خودریختی همانی $\mathbb{Q}[x]$ باشد.

۱۳. نشان دهید که در مسئلهٔ ۱۲ فرض $\varphi(a) = a$ به ازای هر $a \in \mathbb{Q}$ لازم نیست زیرا هر خودریختی $\mathbb{Q}[x]$ خودبه‌خود در $\varphi(a) = a$ به ازای هر $a \in \mathbb{Q}$ صادق خواهد بود.

۱۴. فرض کنید $\mathbb{C}$ میدان اعداد مختلط باشد. به ازای هر عدد صحیح $n > ۰$ یک خودریختی مانند φ از $\mathbb{C}[x]$ از مرتبهٔ n پیدا نمایید.

۷. میدان خارج‌قسمتهای یک قلمرو صحیح

حلقهٔ اعداد صحیح $\mathbb{Z}$ را که قلمروی است صحیح در نظر می‌گیریم. میدان اعداد گویای Q مرکب از تمام کسرهای صحیح، یعنی تمام کسرهای m/n که در آنها $m, n \neq ۰$ در $\mathbb{Z}$اند، رابطهٔ نزدیکی با $\mathbb{Z}$ دارد. توجه کنید که راه منحصر به‌فردی برای نمایش مثلاً $\frac{۱}{۲}$ در Q وجود ندارد زیرا $\cdots = (-۱۴)/(-۷) = \frac{۲}{۴} = \frac{۱}{۲}$. به‌عبارت دیگر، ما $\frac{۱}{۲}$ را با $\frac{۲}{۴}$، $(-۱۴)/(-۷)$، و غیره یکی می‌کنیم. این امر می‌گوید که آنچه در ساختن اعداد گویا از اعداد صحیح رخ می‌دهد چیزی جز یک رابطهٔ هم‌ارزی بر مجموعه‌ای مبتنی بر اعداد صحیح نیست.

رابطهٔ Q با $\mathbb{Z}$ را می‌توان به هر قلمرو صحیح D کشانید. به ازای قلمرو صحیح D میدان $F \supset D$ را طوری می‌سازیم که عناصرش خارج‌قسمتهای a/b با $a, b \neq ۰ \in D$ باشند. این ساختن را به‌طور صوری شرح می‌دهیم.

فرض کنیم D یک قلمرو صحیح بوده و $S = \{(a,b) | b \neq ۰ \text{ و } a, b \in D\}$. S زیرمجموعه‌ای است از $D \times D$ (حاصلضرب دکارتی D در خودش) که در آن مؤلفهٔ دوم ۰ نیست. (a,b) را یک لحظه به‌صورت a/b تصور می‌کنیم. در این صورت چه وقت $(a,b) = (c,d)$؟ واضح است که می‌خواهیم $a/b = c/d$ که در D به شکل $ad = bc$ در می‌آید. حال، با این بحث به عنوان راهنما، رابطهٔ $\sim$ را بر S به‌صورت زیر تعریف می‌کنیم: به ازای (a,b) و (c,d) در S، $(a,b) \sim (c,d)$ اگر و فقط اگر $ad = bc$.

ابتدا حکم می‌کنیم که این یک رابطهٔ هم‌ارزی بر S است. سه شرط رابطهٔ هم‌ارزی را تحقیق می‌کنیم.

۱. $(a,b) \sim (a,b)$ زیرا به وضوح $ab = ba$ (چون D تعویض‌پذیر است). لذا $\sim$ منعکس است.

۲. $(a,b) \sim (c,d)$ ایجاب می‌کند که $(c,d) \sim (a,b)$، زیرا $(a,b) \sim (c,d)$ به معنی

$ad = bc$ است. برای برقراری $(c,d) \sim (a,b)$ باید $cb = da$. ولی این درست است زیرا $cb = bc = ad = da$ پس $\sim$ متقارن می‌باشد.

۳. $(c,d) \sim (a,b)$ و $(c,d) \sim (e,f)$ ایجاب می‌کنند که $ad = bc$ و $cf = de$. پس $adf = bcf = bde$. ولی $d \neq 0$ و ما در یک قلمرو صحیح هستیم. در نتیجه $af = be$. این می‌گوید که $(a,b) \sim (e,f)$. لذا رابطه متعدی می‌باشد.

پس نشان داده‌ایم که $\sim$ یک رابطهٔ هم‌ارزی بر S است. فرض کنیم F مجموعهٔ تمام رده‌های هم‌ارزی $[a,b]$ از عناصر $(a,b) \in S$ باشد. F میدان مطلوب ما می‌باشد.

برای اثبات میدان بودن F باید به آن جمع و ضرب ببخشیم. ابتدا جمع: جمع چه باید باشد؟ ما، صرف‌نظر از تمام تخیلات راجع به رابطهٔ هم‌ارزی، می‌خواهیم $[a,b]$ مساوی a/b باشد. در این صورت $[a,b]+[c,d]$ نباید جز به شکل

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

محاسبه شود. این امر انگیزهٔ تعریف زیر است:

$$[a,b]+[c,d]=[ad+bc,bd] \qquad (۱)$$

از آنجا که $b \neq 0$ و $d \neq 0$ و D یک قلمرو است، پس $bd \neq 0$. لذا $[ad+bc,bd]$ عنصری از F می‌باشد.

طبق معمول باید نشان داد که این جمع در F تعریف شده است. به عبارت دیگر، باید نشان داد که هرگاه $[a,b]=[a',b']$ و $[c,d]=[c',d']$، آنگاه $[a,b]+[c,d]=[a',b']+[c',d']$. لذا، طبق (۱)، باید نشان داد که $[ad+bc,bd]=[a'd'+b'c',b'd']$ که به معنی

$$(ad+bc)b'd'=bd(a'd'+b'c')$$

است. چون $[a,b]=[a',b']$ و $[c,d]=[c',d']$، $ab'=ba'$ و $cd'=dc'$. لذا، همان‌طور که حکم شده،

$$(ad+bc)b'd'=ab'dd'+bb'cd'=ba'dd'+bb'dc'=(a'd'+b'c')bd$$

بنابراین «+» در F تعریف شده است.

ردهٔ $[0,b]$ $(b \neq 0)$ عنصر 0 تحت «+» است. ما آن را فقط با 0 نشان می‌دهیم. ردهٔ $[-a,b]$ نیز قرینهٔ $[a,b]$ می‌باشد. اثبات گروه آبلی بودن F آسان ولی پرزحمت است زیرا باید قانون شرکتپذیری تحقیق شود.

حال به ضرب در F می‌پردازیم. مجدداً $[a,b]$ را به‌صورت a/b گرفته و تعریف می‌کنیم

$$[a,b][c,d]=[ac,bd] \qquad (۲)$$

مجدداً چون $b\neq 0$ و $d\neq 0$، داریم $bd\neq 0$. پس عنصر $[ac,bd]$ نیز در F است.

همانند «+» باید نشان داد که این ضرب تعریف شده است؛ یعنی هرگاه $[a,b]=[a',b']$ و $[c,d]=[c',d']$، آن‌گاه

$$[a,b][c,d]=[ac,bd]=[a'c',b'd']=[a',b'][c',d']$$

می‌دانیم که $ab'=ba'$ و $cd'=dc'$. پس $acb'd'=ab'cd'=ba'dc'=bda'c'$ که همان مطلب مورد نیاز برای $[ac,bd]=[a'c',b'd']$ است. لذا ضرب در F تعریف شده است.

چه عنصری در F به عنوان ۱ عمل می‌کند؟ حکم می‌کنیم که به ازای هر $a\neq 0$ و $b\neq 0$ در D، $[a,a]=[b,b]$ (زیرا $ab=ab$) و $[c,d][a,a]=[ca,da]=[c,d]$ زیرا $(ca)d=(da)c$. پس $[a,a]$ به‌عنوان ۱ عمل می‌کند، و ما آن را به‌صورت سادهٔ $[a,a]=1$ (به‌ازای هر $a\neq 0$ در D) می‌نویسیم. هرگاه $[a,b]\neq 0$، آن‌گاه $a\neq 0$؛ در نتیجه $[b,a]$ در F است. لذا، چون $[a,b][b,a]=[ab,ba]=[ab,ab]=1$، $[a,b]$ در F معکوس دارد. آنچه از اثبات گروه آبلی بودن عناصر ناصفر F تحت این ضرب باقی است قوانین شرکتپذیری و تعویضپذیری می‌باشد. ما اثبات این دو را به خواننده وا می‌گذاریم.

برای اثبات میدان بودن F کافی است قانون پخشپذیری را نشان دهیم. داریم

$$[ad+bc,bd][e,f]=[(ad+bc)e,bdf]$$

در نتیجه

$$([a,b]+[c,d])[e,f]=[ade+bce,bdf]$$

حال آنکه

$$\begin{aligned}
&[a,b][e,f]+[c,d][e,f]\\
&\qquad=[ae,bf]+[ce,df]=[aedf+bfce,bdf^2]\\
&\qquad=[(ade+bce)f,bdf^2]=[ade+bce,bdf][f,f]\\
&\qquad=[ade+bce,bdf]
\end{aligned}$$

که مساوی $[e,f]([a,b]+[c,d])$ است. پس قانون پخشپذیری برقرار بوده و F یک میدان می‌باشد.

فرض کنیم $a \neq 0$ عنصر ثابتی در D باشد و $[da,a]$ را به ازای هر $d \in D$ در نظر می‌گیریم. نگاشت $\varphi : d \to [da,a]$ یک تکریختی از D به توی F است. ۱-۱ بودن این نگاشت واضح است زیرا هرگاه $\varphi(d) = [da,a] = 0$، آن‌گاه $da = 0$. پس $d = 0$ زیرا D یک قلمرو صحیح است. همچنین $\varphi(d_1 d_2) = [d_1 d_2 a, a]$ ولی

$$\begin{aligned}\varphi(d_1)\varphi(d_2) &= [d_1 a, a][d_2 a, a] = [d_1 d_2 a^2, a^2] = [d_1 d_2 a, a][a,a] \\ &= [d_1 d_2 a, a] = \varphi(d_1 d_2)\end{aligned}$$

به‌علاوه

$$\begin{aligned}([d_1 a, a] + [d_2 a, a]) &= ([d_1 a^2 + a^2 d_2, a^2]) \\ &= [d_1 a + d_2 a, a][a,a] \\ &= ([(d_1 + d_2)a, a])\end{aligned}$$

در نتیجه

$$\varphi(d_1 + d_2) = [(d_1 + d_2)a, a] = [d_1 a, a] + [d_2 a, a] = \varphi(d_1) + \varphi(d_2)$$

لذا φ، D را به‌طور تکریختی به توی F می‌نگارد. پس D با زیرحلقه‌ای از F یکریخت است و در نتیجه می‌توان D را در F «نشانید». ما هر عنصر $[a,b]$ از F را به‌صورت کسر a/b در نظر می‌گیریم.

آنچه ثابت کرده‌ایم به قرار زیر است:

قضیهٔ ۱.۷.۴. فرض کنیم D یک قلمرو صحیح باشد. در این صورت میدانی مانند $F \supset D$ هست که از تمام کسرهای a/b از عناصر D به‌صورت تعریف شده در فوق تشکیل شده است.

میدان F را میدان خارج‌قسمتهای D می‌نامیم. وقتی $D = \mathbb{Z}$، F با میدان اعداد گویای $\mathbb{Q}$ یکریخت است. همچنین اگر D قلمرو اعداد صحیح زوج باشد، F تمام میدان $\mathbb{Q}$ می‌باشد.

آنچه در ساختن میدان خارج‌قسمتهای D شد راهی طویل، صوری، و احتمالاً خسته‌کننده در انجام کاری است که ماهیت بسیار ساده‌ای دارد. ما کاری جز تشکیل تمام کسرهای صوری a/b،

که $a, b \neq 0$ در Dاند، و جمع و ضرب آنها به‌صورت معمول نکرده‌ایم. ولی گاهی لازم است که یک کار، ولو پر رنج، تا آخر به تفصیل انجام شود. اغلب ما ساختن صوری و دقیق اعداد گویا از اعداد صحیح را هرگز ندیده‌ایم. حال که F از D به این روش صوری ساخته شد، از جزئیات صرف‌نظر کرده و F را مجموعهٔ تمام کسرها از عناصر D می‌گیریم.

مسائل

۱. قانون شرکتپذیری جمع در F را ثابت کنید.

۲. قانون تعویضپذیری جمع در F را ثابت کنید.

۳. ثابت کنید ضرب در F تعویضپذیر و شرکتپذیر است.

۴. اگر K میدانی شامل D باشد، نشان دهید که $F \subset K$. (در نتیجه F کوچکترین میدان شامل D می‌باشد.)

۵

میدانها

مفهوم حلقه برای اغلب ما نامأنوس بود ولی میدان به تجربیات ما نزدیکتر است. ما در آموزش اولیهٔ خود تنها حلقهٔ غیرمیدانی که دیده‌ایم حلقهٔ اعداد صحیح است، ولی تجربهٔ ما در اعداد گویا، اعداد حقیقی و برای برخی از ما اعداد مختلط در حل معادلات خطی و درجهٔ دو بیشتر بوده است. امکان تقسیم بر عناصر ناصفر (که در اعداد صحیح آن را نداشتیم) در حل مسائل مختلف به ما قدرت می‌بخشید.

لذا، در اولین نگاه، وقتی با میدانها شروع می‌کنیم احساس امنیت داریم. همین‌طور که پیش می‌رویم، به ایده‌ها و نتایج جدیدی می‌رسیم. بار دیگر در سرزمینی ناآشنا خواهیم بود. ولی خوشبختانه، پس از آشنایی با مطالب، مفاهیم به‌صورت طبیعی در خواهند آمد.

میدانها نقش مهمی در هندسه، نظریهٔ معادلات، و بعضی از بخشهای بسیار مهم نظریهٔ اعداد دارند. همین‌طور که پیش می‌رویم با هر یک از این جنبه‌ها تماس خواهیم یافت. متأسفانه، به خاطر ابزار تکنیکی لازم، به نظریهٔ گالوا که بخش زیبایی از مبحث است نمی‌پردازیم. امیدواریم بسیاری از خوانندگان در آموزش ریاضی خود با نظریهٔ گالوا تماس حاصل نمایند.

۱. چند مثال از میدانها

به یاد آورید که میدان F حلقه‌ای است تعویضپذیر با عنصر یکهٔ ۱ به‌طوری که به ازای هر عنصر ناصفر $a \in F$ عنصری مانند $a^{-1} \in F$ هست که $aa^{-1} = 1$. به‌عبارت دیگر، میدانها «چیزی

شبیه» اعداد گویای $\mathbb{Q}$ می‌باشند. ولی آیا واقعاً چنین است؟ اعداد صحیح $\mod p$ یعنی $\mathbb{Z}_p$ که در آن p اول است یک میدان تشکیل می‌دهند. در $\mathbb{Z}_p$ داریم

$$p۱ = \underbrace{۱ + ۱ + \cdots + ۱}_{(p \text{ بار})} = ۰$$

هیچ چیز شبیه این در $\mathbb{Q}$ رخ نمی‌دهد. حتی تفاوتهای فاحش‌تری از این بین میدانها وجود دارند: چطور چندجمله‌ایها روی آنها تجزیه می‌شوند، خواص ویژه‌ای که چند مثالی از آنها را خواهیم دید، و غیره.

بحث را با چند مثال آشنا آغاز می‌کنیم.

چند مثال

۱. $\mathbb{Q}$ میدان اعداد گویا.

۲. $\mathbb{R}$ میدان اعداد حقیقی.

۳. $\mathbb{C}$ میدان اعداد مختلط.

۴. فرض کنیم $F = \{a + bi | a, b \in \mathbb{Q}\} \subset \mathbb{C}$. اثبات میدان بودن F نسبتاً آسان است. تنها تحقیق می‌کنیم که هرگاه $a + bi \neq ۰$ در F باشد، آن‌گاه $(a + bi)^{-۱}$ نیز در F است. ولی $(a + bi)^{-۱}$ چیست؟ این صرفاً عبارت است از

$$\frac{a}{(a^۲ + b^۲)} - \frac{ib}{(a^۲ + b^۲)} \quad \text{(تحقیق کنید!)}$$

و چون $a^۲ + b^۲ \neq ۰$ و گویاست، $a/(a^۲ + b^۲)$ و $b/(a^۲ + b^۲)$ گویایند؛ در نتیجه $(a + bi)^{-۱}$ در F می‌باشد.

۵. فرض کنیم $F = \{a + b\sqrt{۲} | a, b \in \mathbb{Q}\} \subset \mathbb{R}$. مجدداً تحقیق میدان بودن F خیلی سخت نیست. در اینجا نیز کافی است وجود معکوسهای عناصر ناصفر F را در F ثابت کنیم. فرض کنیم $a + b\sqrt{۲} \neq ۰$ در F باشد. چون $\sqrt{۲}$ گنگ است، $a^۲ - ۲b^۲ \neq ۰$. و چون

$$(a + b\sqrt{۲})(a - b\sqrt{۲}) = a^۲ - ۲b^۲$$

معلوم می‌شود که $(a + b\sqrt{۲})(a/c - \sqrt{۲}b/c) = ۱$ که در آن $c = a^۲ - ۲b^۲$. معکوس مطلوب برای $a + b\sqrt{۲}$ عبارت است از $a/c - \sqrt{۲}b/c$ که مسلماً عنصری از F است زیرا a/c و b/c گویا می‌باشند.

۶. فرض کنیم F یک میدان و $F[x]$ حلقهٔ چندجمله‌ایها از x روی F باشد. چون $F[x]$ یک قلمرو صحیح است، بنابر قضیهٔ ۱.۷.۴ دارای میدان خارج‌قسمتها می‌باشد که عبارت است از جمیع خارج‌قسمتهای $f(x)/g(x)$ که $f(x)$ و $g(x)$ در $F[x]$ بوده و $g(x) \neq 0$. این میدان خارج‌قسمتهای $F[x]$ را با $F(x)$ نموده و میدان توابع گویا از x روی F می‌نامیم.

۷. $\mathbb{Z}_p$، یعنی اعداد صحیح به پیمانهٔ عدد اول p، یک میدان (متناهی) است.

۸. در مثال ۲ از بخش ۴ در فصل ۴ طرز ساختن یک میدان دارای نه عنصر را دیدیم.

این هشت مثال نمونه‌هایی خاص‌اند. با استفاده از قضایایی که قبلاً دیده‌ایم می‌توان میدانهای کلی دیگری را ساخت.

۹. هرگاه D یک قلمرو صحیح باشد، آن‌گاه، طبق قضیهٔ ۱.۷.۴، دارای میدان خارج‌قسمتهاست که عبارت است از جمیع کسرهای a/b که در آن a و b در D بوده و $b \neq 0$.

۱۰. هرگاه R حلقه‌ای تعویضپذیر با عنصر یکهٔ ۱ بوده و M ایده‌آل ماکزیمالی از R باشد، آن‌گاه قضیهٔ ۲.۴.۴ به ما می‌گوید که R/M یک میدان است.

مثال اخیر به ازای Rهای خاص نقش مهمی در این فصل خواهد داشت.

می‌توان با حالات خاصی از مثالهای ۹ و ۱۰ جلو رفت و چند مثال دیگر را دید. مثال ۱۰ فوق میدانهای مختلفی را به ما نشان می‌دهد و می‌بینیم که گردش در میدانها چندان مشکل نیست.

در مثالهای ۷ و ۸ میدانها متناهی‌اند. اگر F یک میدان متناهی با q عنصر بوده و F را فقط گروهی آبلی تحت جمع «$+$» در نظر بگیریم، از قضیهٔ ۵.۴.۲ معلوم می‌شود که به ازای هر $x \in F$، $qx = 0$. این رفتار با آنچه در میدانهای آشنا مانند اعداد گویا و اعداد حقیقی رخ می‌دهد کاملاً متفاوت است.

حال این نوع رفتار را ممتاز می‌سازیم.

تعریف. گوییم میدان F دارای (یا از) مشخص $p \neq 0$ است اگر عدد صحیح مثبتی مانند p باشد به‌طوری که به ازای هر $x \in F$، $px = 0$ و هیچ عدد صحیح مثبت کوچکتر از p این خاصیت را نداشته باشد.

اگر F به ازای هیچ عدد صحیح مثبت p از مشخص p نباشد، گوییم F از مشخص ۰ است. مثلاً میدانهای $\mathbb{Q}$، $\mathbb{R}$، و $\mathbb{C}$ از مشخص ۰اند ولی $\mathbb{Z}_3$ از مشخص ۳ می‌باشد.

در تعریف فوق استفاده از حرف p برای مشخص بسیار غریب است زیرا p همواره عددی اول است. در واقع، همان‌طور که در قضیهٔ زیر می‌بینیم، این مورد استعمال سازگار می‌باشد.

قضیهٔ ۱.۱.۵. مشخص یک میدان یا ۰ است یا عددی اول.

برهان. اگر میدان F دارای مشخص ۰ باشد، چیزی برای گفتن نداریم. پس فرض کنیم به ازای هر $x \in F$، $mx = 0$ که در آن m یک عدد صحیح مثبت است. همچنین p کوچکترین عدد صحیح مثبتی باشد که به ازای هر $x \in F$، $px = 0$. حکم می‌کنیم که p اول است. چرا که اگر $p = uv$ که در آن $u > 1$ و $v > 1$ صحیح‌اند، در F داریم $(uv)1 = 0 = (u1)(v1)$ که در آن ۱ عنصر یکهٔ F است. ولی F به‌دلیل میدان بودن یک قلمرو صحیح است. پس $u1 = 0$ یا $v1 = 0$. در هر حالت به ازای هر x در F داریم $ux = (u1)(x) = 0$ (یا، به نحو مشابه، $vx = (v1)x = 0$). ولی این امر انتخاب p را به‌عنوان کوچکترین عدد صحیح با این خاصیت نقض می‌کند. لذا p اول می‌باشد. ■

توجه کنید که ما از فرض میدان بودن F استفادهٔ کامل نکردیم. تنها لازم بود که F یک قلمرو صحیح (دارای ۱) باشد. لذا اگر مشخص یک قلمرو صحیح را ۰ یا کوچکترین عدد صحیح مثبت p که به ازای هر $x \in F$، $px = 0$ تعریف کنیم، همان نتیجه به‌دست می‌آید. لذا داریم:

نتیجه. هرگاه D یک قلمرو صحیح باشد، آن‌گاه مشخص آن ۰ یا عددی اول است.

مسائل

۱. نشان دهید که هر میدان یک قلمرو صحیح است.

۲. نتیجهٔ فوق‌الذکر را حتی اگر D عنصر یکه نداشته باشد ثابت کنید.

۳. فرض کنید R یک حلقه، $S = R[x]$ حلقهٔ چندجمله‌ایها از x روی R، و $T = S[y]$ حلقهٔ چندجمله‌ایها از y روی S باشد. نشان دهید که

الف) هر عنصر $f(x, y)$ در T به شکل $\sum\sum a_{ij}x^iy^j$ است که در آن a_{ij}ها در Rاند؛

ب) شرط تساوی دو عنصر $f(x, y)$ و $g(x, y)$ در T را برحسب شکل $f(x, y)$ در T که در قسمت (الف) داده شده بیان دارید؛

پ) برای $f(x, y) + g(x, y)$ به ازای $f(x, y)$ و $g(x, y)$ در T فرمولی برحسب شکل $f(x, y)$ مذکور در قسمت (الف) بیابید؛

ت) اگر $f(x,y)$ و $g(x,y)$ در T باشند، حاصلضرب $f(x,y)$ در $g(x,y)$ را به‌دست آورید. (T را حلقهٔ چندجمله‌ایها از دو متغیر روی R نامیده و آن را با $R[x,y]$ نشان می‌دهیم.)

۴. اگر D قلمرو صحیح باشد، نشان دهید که $D[x,y]$ نیز قلمرو صحیح است.

۵. اگر F یک میدان بوده و $D = F[x,y]$، میدان خارج‌قسمتهای D میدان توابع گویا از دو متغیر روی F نام دارد و معمولاً با $F(x,y)$ نموده می‌شود. عنصر نوعی $F(x,y)$ را بیابید.

۶. ثابت کنید $F(x,y)$ با $F(y,x)$ یکریخت است.

۷. اگر F میدانی از مشخص $p \neq 0$ باشد، نشان دهید که به ازای هر $a, b \in F$،

$$(a+b)^p = a^p + b^p$$

(راهنمایی. از قضیهٔ دو جمله‌ای و اول بودن p استفاده کنید.)

۸. اگر F میدانی از مشخص $p \neq 0$ باشد، نشان دهید که به ازای هر a و b در F و هر عدد صحیح مثبت n، $(a+b)^m = a^m + b^m$ که در آن $m = p^n$.

۹. فرض کنید F میدانی از مشخص $p \neq 0$ بوده و $\varphi : F \to F$ با $\varphi(a) = a^p$ به ازای هر $a \in F$ تعریف شده باشد.

الف) نشان دهید که φ یک تکریختی از F به توی خود است.

ب) میدان F را طوری مثال بزنید که در آن φ برو نباشد (بسیار مشکل).

۱۰. اگر F یک میدان متناهی از مشخص p باشد، نشان دهید که نگاشت φ تعریف شده در فوق برو و در نتیجه یک خودریختی F است.

۲. گردشی کوتاه در فضاهای برداری

برای بحث در نظریهٔ میدان به ابزاری تکنیکی نیاز داریم که هنوز در دسترس ما نیست. این ابزار در رابطه با دو میدان $K \supset F$ است و چیزی که ما می‌خواهیم اندازهٔ K در رابطه با اندازهٔ F می‌باشد. این اندازه چیزی است که ما بعد یا درجهٔ K روی F می‌نامیم.

در این مورد K می‌تواند خیلی کمتر از یک میدان باشد. اگر نتایج فقط در محدودهٔ خاص دو میدان $K \supset F$ ثابت شوند کوتاهی شده است، زیرا همین ایده‌ها، برهانها، و جوهر کار در وضعیت وسیعتری برقرارند. ما به مفهوم فضای برداری روی میدان F نیاز داریم. آنچه در فضاهای برداری می‌گوییم نه تنها در میدانها مهم است بلکه ایده‌های مربوطه در تمام بخشهای ریاضی نیز ظاهر می‌شوند. شاگردان جبر باید این چیزها را در مرحله‌ای از تعلیم خود ببینند و موقع مناسب برای این کار همین جا می‌باشد.

تعریف. فضای برداری V روی میدان F یک گروه آبلی تحت «$+$» است به‌طوری که به ازای هر $\alpha \in F$ و هر $v \in V$ عنصری مانند $\alpha v \in V$ باشد به‌طوری که

۱. به ازای $\alpha \in F$ و $v_1, v_2 \in V$، $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$؛

۲. به ازای $\alpha, \beta \in F$ و $v \in V$، $(\alpha + \beta)v = \alpha v + \beta v$؛

۳. به ازای $\alpha, \beta \in F$ و $v \in V$، $\alpha(\beta v) = (\alpha\beta)v$؛

۴. به ازای هر $v \in V$، $1v = v$ که در آن ۱ عنصر یکهٔ F است.

در بحث فضاهای برداری، که ما به اختصار به آن می‌پردازیم، عنصرهای V را با حروف لاتینی کوچک و عناصر F را با حروف یونانی کوچک نشان می‌دهیم.

در اینجا توجه اصلی ما به یک جنبه از نظریهٔ فضاهای برداری است و آن مفهوم بعد V روی F می‌باشد. ما این مفهوم را به‌طور سریع و نه لزوماً به بهترین و زیباترین وجه عرضه می‌کنیم. به خواننده قویاً توصیه می‌شود که جنبه‌های دیگر فضاهای برداری را در سایر کتب جبر یا جبر خطی (مثلاً کتابهای

A Primer on Linear Algebra

و

Matrix Theory and Linear Algebra

اینجانب) ببیند.

پیش از به‌دست آوردن چند نتیجه به چند مثال توجه می‌کنیم. تحقیق در فضای برداری بودن آنها به خواننده محول می‌شود.

چند مثال

۱. فرض کنیم F یک میدان بوده و $V = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) | \alpha_i \in F$، به ازای هر $i\}$ مجموعهٔ تمام n تاییها روی F با تساوی و جمع مؤلفه به مؤلفه باشد. به ازای $v = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ و $\beta \in F$، βv را با $\beta v = (\beta\alpha_1, \beta\alpha_2, \ldots, \beta\alpha_n)$ تعریف می‌کنیم. در این صورت V یک فضای برداری روی F می‌باشد.

۲. فرض کنیم F یک میدان و $V = F[x]$ حلقهٔ چندجمله‌ایها از x روی F باشد. با چشم‌پوشی از ضرب عناصر دلخواه $F[x]$ و فقط استفاده از ضرب یک چندجمله‌ای در یک ثابت، مثلاً

$$\beta(\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n) = \beta\alpha_0 + \beta\alpha_1 x + \cdots + \beta\alpha_n x^n$$

V فضایی برداری روی F خواهد شد.

۳. فرض کنیم V همانند مثال ۲ بوده و $W = \{f(x) \in V | \deg(f(x)) \leq n\}$. در این صورت W یک فضای برداری روی F است، و $W \subset V$ یک زیرفضای V به معنی زیر می‌باشد.

تعریف. یک زیرفضای فضای برداری V زیرمجموعه‌ای است ناتهی مانند W از V به‌طوری که به ازای هر α در F و $w, w_1, w_2 \in W$، $\alpha w \in W$ و $w_1 + w_2 \in W$.

از تعریف زیرفضای W از V نتیجه می‌شود که W یک فضای برداری است که اعمالش همان اعمال Vاند که به عناصر W محدود شده‌اند.

۴. فرض کنیم V مجموعهٔ تمام توابع مشتق‌پذیر حقیقی بر بازهٔ یکهٔ بستهٔ $[0, 1]$ با جمع و ضرب معمولی یک تابع در یک عدد حقیقی باشد. در این صورت V یک فضای برداری روی $\mathbb{R}$ می‌باشد.

۵. فرض کنیم W مجموعهٔ تمام توابع حقیقی پیوسته بر $[0, 1]$ با جمع و ضرب معمولی یک تابع در یک عدد حقیقی باشد. W نیز یک فضای برداری روی $\mathbb{R}$ است و V مثال ۴ زیرفضایی از W است.

۶. فرض کنیم F یک میدان و $F[x]$ حلقهٔ چندجمله‌ایها از x روی F باشد. همچنین $f(x)$ در $F[x]$ بوده و $J = (f(x))$ ایده‌آل $F[x]$ تولید شده به‌وسیلهٔ $f(x)$ باشد. و نیز $V = F[x]/J$ که در آن تعریف می‌کنیم $\alpha(g(x) + J) = \alpha g(x) + J$. در این صورت V یک فضای برداری روی F است.

۷. فرض کنیم $\mathbb{R}$ میدان حقیقی بوده و V مجموعهٔ تمام جوابهای معادلهٔ دیفرانسیل $d^2y/dx^2 + y = 0$ باشد. V یک فضای برداری روی $\mathbb{R}$ می‌باشد.

۸. فرض کنیم V یک فضای برداری روی میدان F بوده و v_1، v_2، ...، v_n عنصرهای V باشند. همچنین

$$< v_1, v_2, \dots, v_n >= \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n | \alpha_1, \alpha_2, \dots, \alpha_n \in F\}$$

در این صورت $< v_1, v_2, \dots, v_n >$ یک فضای برداری روی F و زیرفضایی از V است.

این زیرفضای $< v_1, v_2, \dots, v_n >$ را زیرفضای V تولید شده یا پیموده شده به‌وسیلهٔ v_1، ...، v_n روی F و عنصرهایش را ترکیبات خطی v_1، ...، v_n می‌نامیم. به‌زودی راجع به $< v_1, v_2, \dots, v_n >$ صحبت بسیار خواهیم داشت.

۹. فرض کنیم V و W فضاهایی برداری روی میدان F بوده و

$$V \oplus W = \{(v, w) | w \in W \text{ ، } v \in V\}$$

که در آن تساوی و جمع مؤلفه به مؤلفه تعریف شده است و $\alpha(v, w) = (\alpha v, \alpha w)$. به آسانی معلوم می‌شود که $V \oplus W$ یک فضای برداری روی F است. این فضا را مجموع مستقیم V و W می‌نامند.

۱۰. فرض کنیم $F \subset K$ دو میدان با جمع «+» K بوده و αv به ازای $\alpha \in F$ و $v \in K$ حاصلضرب به‌عنوان عناصر K باشد. شرایط ۱ و ۲ تعریف فضای برداری حالات خاص قوانین پخشپذیری در K و شرط ۳ نتیجه‌ای از شرکتپذیری ضرب در K است. بالاخره شرط ۴ بیان مجدد این امر است که ۱ عنصر یکهٔ K می‌باشد. لذا K یک فضای برداری روی F خواهد بود.

این مثالها تفاوت فاحشی با یکدیگر دارند. این تفاوت را با بررسی چند تا از آنها توضیح می‌دهیم.

۱. در مثال ۱ هرگاه

$$v_n = (0, 0, \dots, 1) \text{، } \cdots \text{، } v_2 = (0, 1, 0, \dots, 0) \text{، } v_1 = (1, 0, \dots, 0)$$

آن‌گاه هر عنصر v در V نمایش منحصر به فردی به شکل $v = \alpha v_1 + \cdots + \alpha_n v_n$ دارد که در آن α_1، ...، α_n در Fاند.

۲. در مثال ۳ هرگاه $v_1 = 1$، $v_2 = x$، ...، $v_i = x^{i-1}$، ...، $v_{n+1} = x^n$، آن‌گاه هر $v \in V$ نمایش منحصر به فردی به‌صورت $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ دارد که در آن α_iها در Fاند.

۳. در مثال ۷ جواب $d^2y/dx^2 + y = 0$ به شکل منحصر به‌فرد $y = \alpha \cos x + \beta \sin x$ است که در آن α و β حقیقی می‌باشند.

۴. در مثال ۸ هر $v \in < v_1, \dots, v_n >$ نمایش (البته نه لزوماً منحصر به‌فرد) به‌صورت

است. یکتایی این $v = \alpha_۱ v_۱ + \cdots + \alpha_n v_n$ دارد که ناشی از تعریف $< v_۱, \ldots, v_n >$ نمایش قویاً به عناصر $v_۱$، $\cdots$، v_n وابسته است.

۵. در حالت خاصی از مثال ۱۰ که در آن $K = \mathbb{C}$ میدان اعداد مختلط و $F = \mathbb{R}$ میدان اعداد حقیقی است، هر $v \in \mathbb{C}$ به شکل منحصر به‌فرد $v = \alpha + \beta i$ با $\alpha, \beta \in \mathbb{R}$ می‌باشد.

۶. فرض کنیم $K = F(x) \supset F$ میدان توابع گویا از x روی F باشد. حکم می‌کنیم (و به خواننده وامی‌گذاریم) که نمی‌توان مجموعه‌ای متناهی از عناصر K را یافت که K را روی F بپیماید. این امر در بعضی از فضاهای برداریی که مثال زده‌ایم نیز برقرار است.

در اینجا همهٔ توجه ما به فضای برداریی است که زیرمجموعه‌ای متناهی آن را روی میدان پایه بپیماید.

پیش از ورود به این بحث، ابتدا باید لیستی از خواص صوری برقرار در یک فضای برداری را ارائه دهیم. شما خوانندهٔ عزیز در پرداختن به این مفاهیم صوری و مجرد آنقدر استاد شده‌اید که از عهدهٔ لم زیر برآیید.

لم ۱.۲.۵. هرگاه V یک فضای برداری روی میدان F باشد، آنگاه به ازای هر $\alpha \in F$ و هر $v \in V$،

الف) $\alpha ۰ = ۰$ که در آن ۰ عنصر صفر V است؛

ب) $۰ v = ۰$ که در آن ۰ عنصر صفر F است؛

پ) $\alpha v = ۰$ ایجاب می‌کند که $\alpha = ۰$ یا $v = ۰$؛

ت) $(-\alpha)v = -(\alpha v)$.

در پرتو این لم می‌توان علامت ۰ را بدون ابهام برای صفر F و صفر V به‌کار برد.

فضاهای برداری را لحظه‌ای فراموش کرده و به جوابهای برخی از دستگاههای معادلات خطی در میدانها نگاه می‌کنیم. مثلاً دو معادلهٔ خطی همگن با ضرایب حقیقی $x_۱ + x_۲ + x_۳ = ۰$ و $۳x_۱ - x_۲ + x_۳ = ۰$ را اختیار می‌کنیم. به آسانی معلوم می‌شود که به ازای هر $x_۱$ و $x_۳$ که $۴x_۱ + ۲x_۳ = ۰$ و $x_۲ = -(x_۱ + x_۳)$ جوابی از این دستگاه به‌دست می‌آید. در واقع این دستگاه علاوه بر جواب بدیهی $x_۱ = ۰$، $x_۲ = ۰$، $x_۳ = ۰$ بی‌نهایت جواب دارد. با توجه به این مثال از خود می‌پرسیم: چرا این دستگاه معادلات خطی بی‌نهایت جواب دارد؟ به سرعت نتیجه می‌شود که دلیلش بیشتر بودن تعداد متغیرها از تعداد معادلات است و ما جا برای مانور و تولید

جواب داریم. همان‌طور که ذیلاً می‌بینید، این وضع درست در حالت کلی برقرار است.

تعریف. فرض کنیم F یک میدان باشد. در این صورت nتایی $(\beta_1, \ldots, \beta_n)$، که در آن β_iها در Fاند و همهٔ آنها 0 نیستند، یک جواب غیربدیهی دستگاه معادلات همگن خطی

$$(*) \qquad \begin{aligned} \alpha_{11}x_1+\alpha_{12}x_2+\cdots+\alpha_{1n}x_n &= 0 \\ \alpha_{21}x_1+\alpha_{22}x_2+\cdots+\alpha_{2n}x_n &= 0 \\ \cdot \qquad \cdot \qquad \cdots \quad \cdot \quad &= 0 \\ \cdot \qquad \cdot \qquad \cdots \quad \cdot \quad &= 0 \\ \alpha_{i1}x_1+\alpha_{i2}x_2+\cdots+\alpha_{in}x_n &= 0 \\ \cdot \qquad \cdot \qquad \cdots \quad \cdot \quad &= 0 \\ \alpha_{r1}x_1+\alpha_{r2}x_2+\cdots+\alpha_{rn}x_n &= 0 \end{aligned}$$

که در آن α_{ij}ها همه در Fاند، نام دارد اگر با جانشانی $x_1 = \beta_1$، $\ldots$، $x_n = \beta_n$ همهٔ معادلات $(*)$ برقرار شوند.

برای دستگاه $(*)$ قضیهٔ زیر را خواهیم داشت.

قضیهٔ ۲.۲.۵. هرگاه $n > r$، یعنی تعداد متغیرها (مجهولات) از تعداد معادلات $(*)$ بیشتر باشد، آن‌گاه دستگاه $(*)$ یک جواب غیربدیهی در F دارد.

برهان. روش همانی است که در دبیرستان آموخته‌ایم و آن حل معادلات همزمان به‌وسیلهٔ حذف یکی از مجهولات و یکی از معادلات است.

ما به استقرا روی r، یعنی تعداد معادلات، عمل می‌کنیم. اگر $r = 1$، دستگاه $(*)$ به $\alpha_{11}x_1 + \cdots + \alpha_{1n}x_n = 0$ تحویل می‌شود که در آن $n > 1$. هرگاه تمام $\alpha_{1i} = 0$ها، آن‌گاه $x_1 = x_2 = \cdots = x_n = 1$ یک جواب غیربدیهی $(*)$ است. لذا، با اندیسگذاری مجدد، می‌توان فرض کرد که $\alpha_{11} \neq 0$. در این صورت برای $(*)$ جواب غیربدیهی $x_2 = \cdots = x_n = 1$ و $x_1 = -(1/\alpha_{11})(\alpha_{12} + \cdots + \alpha_{1n})$ را داریم.

فرض کنیم نتیجه برای $r = k$ به ازای kای درست بوده و $(*)$ دستگاهی از $k + 1$ معادلهٔ همگن خطی از $n > k + 1$ متغیر باشد. همانند فوق می‌توان فرض کرد که $\alpha_{ij} \neq 0$ای و، بی‌آنکه به کلیت خللی وارد آید، $\alpha_{11} \neq 0$.

دستگاه مرتبط (**) را مرکب از k معادلهٔ همگن خطی از $n-۱$ متغیر می‌سازیم. چون $n > k+۱$، داریم $n-۱ > k$. پس می‌توان استقرا را بر این دستگاه جدید (**) اعمال کرد. این دستگاه جدید چطور به‌دست می‌آید؟ می‌خواهیم $x_۱$ را از این معادلات حذف کنیم. این کار را با تفریق $\alpha_{i۱}/\alpha_{۱۱}$ برابر اولین معادله از معادلهٔ iام به ازای هر $i = ۲, ۳, \ldots, k+۱$ انجام می‌دهیم. با این کار به دستگاه جدیدی از k معادلهٔ همگن خطی از $n-۱$ متغیر زیر می‌رسیم:

$$\begin{array}{ll} \beta_{۲۲}x_۲ + \cdots + \beta_{۲n}x_n = ۰ & \\ \beta_{۳۲}x_۲ + \cdots + \beta_{۳n}x_n = ۰ & \\ \cdot \quad \cdots \quad \cdot & (**) \\ \cdot \quad \cdots \quad \cdot & \\ \beta_{k+۱,۲}x_۲ + \cdots + \beta_{k+۱,n}x_n = ۰ & \end{array}$$

که در آن به ازای $i = ۲, ۳, \ldots, k+۱$ و $j = ۲, ۳, \ldots, n$، $\beta_{ij} = \alpha_{ij} - (\alpha_{i۱}/\alpha_{۱۱})\alpha_{۱j}$.

چون (**) دستگاهی از k معادلهٔ همگن خطی از $n-۱$ متغیر است و $k < n-۱$، بنابه فرض استقرا، (**) یک جواب غیربدیهی مانند $(\gamma_۲, \ldots, \gamma_n)$ در F دارد. فرض کنیم $\gamma_۱ = -(\alpha_{۱۲}\gamma_۲ + \cdots + \alpha_{۱n}\gamma_n)/\alpha_{۱۱}$. بر خواننده است تحقیق کند که $(\gamma_۱, \gamma_۲, \ldots, \gamma_n)$ جواب غیربدیهی مطلوب (*) می‌باشد. این امر استقرا را کامل کرده و قضیه را به ثبوت می‌رساند.

■

حال که این نتیجه اثبات شد آن را در بررسی فضاهای برداری به‌کار خواهیم برد. اینک به این فضاها می‌پردازیم. برای تأکید، چیزی را که قبلاً در مثال ۸ تعریف شد تکرار می‌کنیم.

تعریف. فرض کنیم V یک فضای برداری روی F بوده و $v_۱$، $v_۲$، ...، v_n در V باشند. گوییم عنصر $v \in V$ یک ترکیب خطی از $v_۱$، $v_۲$، ...، v_n است اگر به ازای $\alpha_۱$، ...، α_nی در F داشته باشیم $v = \alpha_۱ v_۱ + \cdots + \alpha_n v_n$.

همان‌طور که در مثال ۸ گفتیم، مجموعهٔ $< v_۱, v_۲, \ldots, v_n >$ جمیع ترکیبات خطی $v_۱$، $v_۲$، ...، v_n یک فضای برداری روی F است و، به‌خاطر بودن در V، زیرفضایی از V می‌باشد. چرا این یک فضای برداری است؟ هرگاه $\alpha_۱ v_۱ + \cdots + \alpha_n v_n$ و $\beta_۱ v_۱ + \cdots + \beta_n v_n$ دو

ترکیب خطی از v_1، $\cdots$، v_n باشند، آن‌گاه، بنابر اصول موضوع فضای برداری،

$$(\alpha_1 v_1 + \cdots + \alpha_n v_n) + (\beta_1 v_1 + \cdots + \beta_n v_n)$$
$$= (\alpha_1 + \beta_1)v_1 + \cdots + (\alpha_n + \beta_n)v_n$$

و در نتیجه در $< v_1, \ldots , v_n >$ است. هرگاه $\gamma \in F$ و

$$\alpha_1 v_1 + \cdots + \alpha_n v_n \in < v_1, \ldots , v_n >$$

آن‌گاه

$$\gamma(\alpha_1 v_1 + \cdots + \alpha_n v_n) = \gamma\alpha_1 v_1 + \cdots + \gamma\alpha_n v_n$$

در نتیجه در $< v_1, \ldots , v_n >$ است. لذا $< v_1, \ldots , v_n >$ یک فضای برداری می‌باشد. همان‌طور که قبلاً نامیدیم، این زیرفضای V پیموده شده روی F به‌وسیلهٔ v_1، $\cdots$، v_n می‌باشد.

این امر ما را به تعریف بسیار مهم زیر می‌رساند.

تعریف. فضای برداری V روی F با بعد متناهی روی F است اگر به ازای v_1، $\cdots$، v_nی در V، $V =< v_1, \ldots , v_n >$؛ یعنی V به‌وسیلهٔ مجموعه‌ای متناهی از عناصر روی F پیموده شود.

اگر V با بعد متناهی روی F نباشد، گوییم V با بعد نامتناهی روی F است. ما با آنکه فضای برداری با بعد متناهی را تعریف کرده‌ایم ولی هنوز بعدش را تعریف نکرده‌ایم. این امر در جای خود انجام خواهد شد.

فرض کنیم V یک فضای برداری روی F بوده و v_1، $\cdots$، v_n در V باشند به‌طوری که هر v در $< v_1, \ldots , v_n >$ نمایش منحصر به‌فردی به شکل $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ داشته باشد که در آن $\alpha_1, \ldots , \alpha_n \in F$. چون

$$0 = 0v_1 + \cdots + 0v_n \quad \text{و} \quad 0 \in < v_1, \ldots , v_n >$$

از یکتایی فرض شده نتیجه می‌شود که اگر $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$،

$$\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$$

این امر تعریف بسیار مهم دیگر زیر را موجب می‌شود.

تعریف. فرض کنیم V یک فضای برداری روی F باشد. در این صورت عناصر v_1، $\cdots$، v_n در V را مستقل خطی روی F گوییم هرگاه $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$، که در آن α_1، $\cdots$، α_n در F اند، ایجاب کند که $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

هرگاه عناصر v_1، $\cdots$، v_n در V مستقل خطی روی F نباشند، آن‌گاه گوییم وابستهٔ خطی روی Fاند. مثلاً هرگاه $\mathbb{R}$ میدان اعداد حقیقی بوده و V مجموعهٔ ۳ تاییهایی روی $\mathbb{R}$ باشد که در مثال ۱ تعریف شد، آن‌گاه $(1,0,0)$، $(0,1,0)$، و $(0,0,1)$ مستقل خطی روی $\mathbb{R}$اند (ثابت کنید!) ولی $(1,-2,7)$، $(0,1,0)$، و $(1,-3,7)$ وابستهٔ خطی روی $\mathbb{R}$اند زیرا

$$1(1,-2,7) + (-1)(0,1,0) + (-1)(1,-3,7) = (0,0,0)$$

یک ترکیب خطی غیربدیهی از این عناصر روی $\mathbb{R}$ است و بردار 0 نیز می‌باشد.

توجه کنید که استقلال خطی تابع میدان F است. هرگاه $\mathbb{C} \supset \mathbb{R}$ میدانهای مختلط و حقیقی باشند، آن‌گاه $\mathbb{C}$ یک فضای برداری روی $\mathbb{R}$ است ولی یک فضای برداری روی خود $\mathbb{C}$ نیز هست. عناصر ۱ و i در $\mathbb{C}$ مستقل خطی روی $\mathbb{R}$اند ولی روی $\mathbb{C}$ چنین نیستند زیرا $i1 + (-1)i = 0$ یک ترکیب خطی غیربدیهی از ۱ و i روی $\mathbb{C}$ می‌باشد.

حال لم زیر را ثابت می‌کنیم.

لم ۳.۲.۵. هرگاه V یک فضای برداری روی F بوده و v_1، $\cdots$، v_n در V مستقل خطی روی F باشند، آن‌گاه هر عنصر $v \in < v_1, \ldots, v_n >$ نمایش منحصر به‌فردی به‌صورت

$$v = \alpha_1 v_1 + \cdots + \alpha_n v_n$$

دارد که در آن α_1، $\cdots$، α_n در F می‌باشند.

برهان. فرض کنیم $v \in < v_1, \ldots, v_n >$ دو نمایش به‌صورت

$$v = \alpha_1 v_1 + \cdots + \alpha_n v_n = \beta_1 v_1 + \cdots + \beta_n v_n$$

با αها و βهای در F داشته باشد. از این داریم $(\alpha_1 - \beta_1)v_1 + \cdots + (\alpha_n - \beta_n)v_n = 0$. چون v_1، $\cdots$، v_n مستقل خطی روی Fاند، نتیجه می‌گیریم که $\alpha_1 - \beta_1 = 0$، $\cdots$، $\alpha_n - \beta_n = 0$ که یکتایی نمایش را به‌دست می‌دهد. ■

یک فضای برداری با بعد متناهی چقدر متناهی است؟ برای سنجش این امر، زیرمجموعهٔ $\{v_1, \ldots, v_n\}$ از V را یک مجموعهٔ مولد مینیمال برای V روی F نامیم اگر $V = < v_1, \ldots, v_n >$ و هیچ مجموعه‌ای با تعداد عناصر کمتر از n فضای V را روی F نپیماید.

حال به سومین تعریف بسیار مهم خود می‌رسیم.

تعریف. هرگاه V یک فضای برداری با بعد متناهی روی F باشد، آن‌گاه بعد V روی F، که به‌صورت $\dim_F(V)$ نوشته می‌شود، مساوی n یعنی تعداد عناصر یک مجموعهٔ مولد مینیمال برای V روی F می‌باشد.

در مثالهای داده شده $\dim_{\mathbb{R}}(\mathbb{C}) = 2$ زیرا $\{1, i\}$ یک مجموعهٔ مولد مینیمال برای $\mathbb{C}$ در $\mathbb{R}$ است. ولی $\dim_{\mathbb{C}}(\mathbb{C}) = 1$. در مثال ۱ داریم $\dim_F(V) = n$ و در مثال ۳ خواهیم داشت $\dim_F(V) = n + 1$. در مثال ۷ بعد V روی F مساوی ۲ می‌باشد. بالاخره هرگاه $V \supset < v_1, \ldots, v_n >$، آن‌گاه $\dim_F < v_1, \ldots, v_n >$ حداکثر n می‌باشد.

حال لم زیر را ثابت می‌کنیم.

لم ۴.۲.۵. هرگاه V با بعد متناهی روی F از بعد n بوده و عناصر v_1، $\cdots$، v_n از V فضای V را روی F تولید کنند، آن‌گاه v_1، $\cdots$، v_n مستقل خطی روی Fاند.

برهان. فرض کنیم v_1، $\cdots$، v_n وابستهٔ خطی روی F باشند. لذا یک ترکیب خطی مانند $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ وجود دارد که همهٔ α_iها 0 نیستند. بی‌آنکه به کلیت خللی وارد شود می‌توان فرض کرد $\alpha_1 \neq 0$. پس $v_1 = (-1/\alpha_1)(\alpha_2 v_2 + \cdots + \alpha_n v_n)$. اگر $v \in V$، چون v_1، $\cdots$، v_n یک مجموعهٔ مولد برای V روی F است،

$$v = \beta_1 v_1 + \cdots + \beta_n v_n = \left(\frac{-\beta_1}{\alpha_1}\right)(\alpha_2 v_2 + \cdots + \alpha_n v_n) + \beta_2 v_2 + \cdots + \beta_n v_n$$

لذا v_2، $\cdots$، v_n فضای V را روی F می‌پیمایند که با مجموعهٔ مولد مینیمال بودن $\{v_1, v_2, \ldots, v_n\}$ از V روی F در تضاد است. ■

حال به تعریف مهم دیگری می‌رسیم:

تعریف. فرض کنیم V یک فضای برداری با بعد متناهی روی F باشد. در این صورت v_1، $\cdots$، v_n یک پایه از V روی F است اگر عناصر v_1، $\cdots$، v_n فضای V را روی F پیموده و

مستقل خطی روی F باشند.

لم ۴.۲.۵ ، هر مجموعهٔ مولد مینیمال از V روی F یک پایهٔ V روی F است. لذا برداری با بعد متناهی دارای پایه می‌باشند. حال به اثبات قضیهٔ زیر می‌پردازیم.

قضیهٔ ۵.۲.۵. فرض کنیم V با بعد متناهی روی F باشد. در این صورت هر دو پایه از V روی F یک تعداد عنصر دارند و این عدد درست برابر $\dim_F(V)$ است.

برهان. فرض کنیم v_1، $\cdots$، v_n و w_1، $\cdots$، w_m دو پایه از V روی F باشند. می‌خواهیم نشان دهیم که $m = n$. فرض کنیم $m > n$. چون v_1، $\cdots$، v_n یک پایه از V روی F است، هر عنصر در V ترکیبی خطی از v_iها روی F می‌باشد. به‌خصوص هر یک از w_1، $\cdots$، w_m ترکیبی خطی از v_1، $\cdots$، v_n روی F است. لذا داریم

$$\begin{aligned}
w_1 &= \alpha_{11}v_1 + \alpha_{12}v_2 + \cdots + \alpha_{1n}v_n \\
w_2 &= \alpha_{21}v_1 + \alpha_{22}v_2 + \cdots + \alpha_{2n}v_n \\
&\vdots \qquad\qquad\qquad\qquad \vdots \\
w_m &= \alpha_{m1}v_1 + \alpha_{m2}v_2 + \cdots + \alpha_{mn}v_n
\end{aligned}$$

که در آن α_{ij}ها در Fاند.

حال

$$\begin{aligned}
\beta_1 w_1 + \cdots + \beta_m w_m =& (\alpha_{11}\beta_1 + \alpha_{21}\beta_2 + \cdots + \alpha_{m1}\beta_m)v_1 \\
&+ \cdots + (\alpha_{1n}\beta_1 + \alpha_{2n}\beta_2 + \cdots + \alpha_{mn}\beta_m)v_n
\end{aligned}$$

را در نظر می‌گیریم. طبق قضیهٔ ۲.۲.۵، دستگاه معادلات همگن خطی

$$\alpha_{1i}\beta_1 + \alpha_{2i}\beta_2 + \cdots + \alpha_{mi}\beta_m = 0, i = 1, 2, \ldots, n$$

یک جواب غیربدیهی در F دارد زیرا تعداد متغیرها یعنی m از تعداد معادلات یعنی n بیشتر است. هرگاه β_1، $\cdots$، β_m یک چنین جواب در F باشد، آن‌گاه، طبق فوق، $\beta_1 w_1 + \cdots + \beta_m w_m = 0$ ولی همهٔ β_iها 0 نیستند. این امر استقلال خطی w_1، $\cdots$، w_m روی F را نقض می‌کند. بنابراین $m \leq n$. به همین نحو $n \leq m$. لذا $m = n$. پس قضیه ثابت است زیرا هر مجموعهٔ مولد مینیمال از V روی F یک پایه از V روی F بوده و تعداد عناصر این مجموعهٔ مولد مینیمال طبق

تعریف مساوی $\dim_F(V)$ می‌باشد. بنابراین، طبق فوق، $n = \dim_F(V)$ و برهان تمام خواهد بود. ■

نتیجه‌ای دیگر که در نظریهٔ میدان به‌کار خواهیم برد و سرشت مشابهی با کارهای فعلی ما دارد عبارت است از:

قضیهٔ ۶.۲.۵. فرض کنیم V یک فضای برداری روی F باشد به‌طوری که $\dim_F(V) = n$. هرگاه $m > n$، آن‌گاه هر m عنصر از V وابستهٔ خطی روی Fاند.

برهان. فرض کنیم $w_1, \ldots, w_m \in V$ و v_1، ...، v_n پایه‌ای از V روی F باشد. در اینجا طبق قضیهٔ ۵.۲.۵ $n = \dim_F(V)$. بنابراین

$$w_m = \alpha_{m1}v_1 + \cdots + \alpha_{mn}v_n, \ldots, w_1 = \alpha_{11}v_1 + \cdots + \alpha_{1n}v_n$$

در اینجا برهانی که در قضیهٔ ۵.۲.۵ داده شد که اگر $m > n$، می‌توان β_1، ...، β_m را در F که همه ۰ نیستند چنان یافت که $\beta_1 w_1 + \cdots + \beta_m w_m = 0$ کلمه به کلمه برقرار است. ولی این ثابت می‌کند که w_1، ...، w_m وابستهٔ خطی روی F می‌باشند. ■

این بخش را با آخرین قضیه که رنگ و بوی قضایای قبلی را دارد پایان می‌بخشیم.

قضیهٔ ۷.۲.۵. فرض کنیم V یک فضای برداری روی F بوده و $\dim_F(V) = n$. در این صورت هر n عنصر مستقل خطی از V یک پایه از V روی F تشکیل می‌دهند.

برهان. می‌خواهیم نشان دهیم که اگر $v_1, \ldots, v_n \in V$ مستقل خطی روی F باشند، V را روی F می‌پیمایند. فرض کنیم $v \in V$. پس v، v_1، ...، v_n، $n+1$ عنصرند. لذا، طبق قضیهٔ ۶.۲.۵، وابستهٔ خطی روی F می‌باشند. پس عناصری چون α، α_1، ...، α_n در F که همه ۰ نیستند وجود دارند به‌طوری که $\alpha v + \alpha_1 v_1 + \cdots + \alpha_n v_n = 0$. عنصر α نمی‌تواند ۰ باشد، در غیر این صورت $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ و همهٔ α_iها ۰ نیستند. این امر استقلال خطی عناصر v_1، ...، v_n روی F را نقض می‌کند. لذا $\alpha \neq 0$؛ و در نتیجه $v = (-1/\alpha)(\alpha_1 v_1 + \cdots + \alpha_n v_n) = \beta_1 v_1 + \cdots + \beta_n v_n$ که در آن $\beta_i = -\alpha_i/\alpha_1$. بنابراین v_1، ...، v_n فضای V روی F را می‌پیمایند و لذا باید یک پایه از V روی F را تشکیل دهند. ■

مسائل

مسائل آسانتر

۱. معین کنید که عناصر زیر در فضای برداری V مرکب از ۳ تاییها روی $\mathbb{R}$ مستقل خطی روی $\mathbb{R}$اند یا خیر:

الف) $(۱,۲,۳)$، $(۴,۵,۶)$، $(۷,۸,۹)$؛

ب) $(۱,۰,۱)$، $(۰,۱,۲)$، $(۰,۰,۱)$؛

پ) $(۱,۲,۳)$، $(۰,۴,۵)$، $(\frac{۱}{۲},۳,\frac{۲۱}{۴})$.

۲. یک جواب غیربدیهی دستگاه معادلات همگن خطی

$$\begin{aligned} x_۱ + x_۲ \;\; + x_۳ \;\; &= ۰ \\ x_۱ + ۲x_۲ + ۳x_۳ &= ۰ \\ ۳x_۱ + ۴x_۲ + ۲x_۳ &= ۰ \end{aligned}$$

را در $\mathbb{Z}_۵$ بیابید.

۳. اگر V یک فضای برداری با بعد n روی $\mathbb{Z}_p$ باشد که در آن p اول است، نشان دهید که V دارای p^n عنصر می‌باشد.

۴. لم ۱.۲.۵ را به‌طور کامل ثابت کنید.

۵. فرض کنید F یک میدان بوده و $V = F[x]$ حلقهٔ چندجمله‌ای از x روی F باشد. با گرفتن V به‌عنوان یک فضای برداری روی F، ثابت کنید V با بعد متناهی روی F نیست.

۶. اگر V یک فضای برداری با بعد متناهی روی F و W زیرفضایی از آن باشد، ثابت کنید

الف) W با بعد متناهی روی F بوده و $\dim_F(W) \leq \dim_F(V)$؛

ب) هرگاه $\dim_F(W) = \dim_F(V)$، آن‌گاه $V = W$.

۷*. همریختی فضاهای برداری ψ از V به W را، که V و W فضاهایی برداری روی Fاند، طبق نظر خود تعریف کنید. راجع به هستهٔ Kی ψ یعنی $K = \{v \in V | \psi(v) = ۰\}$ چه می‌شود گفت؟ یکریختی فضاهای برداری چیست؟

۸. اگر V یک فضای برداری روی F و W زیرفضایی از آن باشد، اعمال لازم در V/W را طوری تعریف کنید که V/W یک فضای برداری روی F گردد.

۹. نشان دهید که اگر $\dim_F(V) = n$ و W زیرفضایی از V باشد که $\dim_F(W) = m$، داریم $\dim_F(V/W) = n - m$.

۱۰. اگر $\psi : V \to V'$ یک همریختی از V به روی V' با هستهٔ K باشد، نشان دهید که (به‌عنوان فضاهای برداری روی F) $V' \simeq V/K$. (ر.ک. مسئلهٔ ۷.)

۱۱. اگر V یک فضای برداری با بعد متناهی روی F بوده و v_1، $\cdots$، v_m در V مستقل خطی روی F باشند، نشان دهید که می‌توان w_1، $\cdots$، w_r در V را چنان یافت که $m+r = \dim_F(V)$ و v_1، $\cdots$، v_m، w_1، $\cdots$، w_r یک پایه از V روی F تشکیل دهند.

۱۲. اگر V یک فضای برداری با بعد n روی F باشد، ثابت کنید V با فضای برداری n تاییها روی F یکریخت است (مثال ۱). (ر.ک.مسئلهٔ ۷).

مسائل با سطح متوسط

۱۳. فرض کنید $K \supset F$ دو میدان باشند. همچنین K، به عنوان یک فضای برداری روی F، دارای بعد متناهی n باشد. نشان دهید هرگاه $a \in K$، آن‌گاه α_0، α_1، $\cdots$، α_nی در F وجود دارند که همه ۰ نبوده و

$$\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_n a^n = 0$$

۱۴. فرض کنید F یک میدان و $F[x]$ حلقهٔ چندجمله‌ای از x روی F بوده و در $F[x]$ داشته باشیم $f(x) \neq 0$. $V = F[x]/J$ را به‌عنوان یک فضای برداری روی F در نظر بگیرید که در آن J ایده‌آل $F[x]$ تولید شده به وسیلهٔ $f(x)$ باشد. ثابت کنید

$$\dim_F(V) = \deg f(x)$$

۱۵. اگر V و W دو فضای برداری با بعد متناهی روی F باشند، ثابت کنید $V \oplus W$ با بعد متناهی روی F بوده و $\dim_F(V \oplus W) = \dim_F(V) + \dim_F(W)$.

۱۶. فرض کنید V یک فضای برداری روی F بوده و U و W زیرفضاهایی از V باشند. با تعریف $U + W = \{u + w | w \in W ، u \in U\}$ ثابت کنید

الف) $U + W$ زیرفضای V است؛

ب) اگر U و W با بعد متناهی روی F باشند، $U + W$ نیز چنین است؛

پ) $U \cap W$ زیرفضای V است؛

ت) $U + W$ نقش همریخت $U \oplus W$ است؛

ث) هرگاه U و W با بعد متناهی روی F باشند، آن‌گاه

$$\dim_F(U + W) = \dim_F(U) + \dim_F(W) - \dim_F(U \cap W)$$

مسائل مشکلتر

۱۷. فرض کنید $F \subset K$ دو میدان باشند به‌طوری که $\dim_F(K) = m$. همچنین V یک فضای برداری روی K باشد. ثابت کنید

الف) V یک فضای برداری روی F است؛

ب) هرگاه V با بعد متناهی روی K باشد، آن‌گاه با بعد متناهی روی F است؛

پ) هرگاه $\dim_K(V) = n$، آن‌گاه

$$\dim_F(V) = mn$$

[یعنی $\dim_F(V) = \dim_K(V)\dim_F(K)$].

۱۸. فرض کنید $F \subset K$ دو میدان بوده و V یک فضای برداری روی K باشد به‌طوری که $\dim_F(V)$ متناهی است. اگر $\dim_F(K)$ متناهی باشد، نشان دهید که $\dim_K(V)$ متناهی است و مقدارش را برحسب $\dim_F(V)$ و $\dim_F(K)$ معین کنید.

۱۹. فرض کنید D یک قلمرو صحیح دارای ۱ بوده و یک فضای برداری با بعد متناهی روی میدان F باشد. ثابت کنید D یک میدان است. (تذکر. چون $F1$، که قابل انطباق با F است، در D می‌باشد، ساختار حلقهٔ D و ساختار فضای برداری D روی F با هم توافق دارند.)

۲۰. فرض کنید V یک فضای برداری روی میدان نامتناهی F باشد. نشان دهید که V نمی‌تواند اجتماع تعدادی متناهی زیرفضای حقیقی V باشد. (بسیار مشکل.)

۳. توسیعهای میدان

حال به رابطهٔ بین دو میدان K و F که $F \subset K$ رو می‌آوریم. K را یک توسیع (یا توسیع میدان) F و F را یک زیرمیدان K می‌نامیم. اعمال F همان اعمال Kاند که به عناصر F محدود شده‌اند. در این بخش فرض است که $F \subset K$.

گوییم K یک توسیع متناهی F است اگر، به‌عنوان یک فضای برداری روی F، $\dim_F(K)$ متناهی باشد. ما $\dim_F(K)$ را به‌صورت $[K : F]$ نوشته و آن را درجهٔ K روی F می‌نامیم.

بحث را با اولین نتیجه‌ای که معمولاً در توسیعهای متناهی مطرح می‌شود آغاز می‌کنیم.

قضیهٔ ۱.۳.۵. فرض کنیم $F \subset K \subset L$ سه میدان باشند به‌طوری که هر دوی $[L : K]$ و $[K : F]$ متناهی‌اند. در این صورت L یک توسیع متناهی F بوده و $[L : F] = [L : K][K : F]$.

برهان. با نمایش یک پایهٔ متناهی از L روی F ثابت می‌کنیم L یک توسیع متناهی F است. برای این کار نتیجهٔ قویتری را ثابت می‌کنیم؛ یعنی ثابت می‌کنیم $[L:F]=[L:K][K:F]$.

فرض کنیم $[L:K]=m$ و $[K:F]=n$. پس L دارای پایهٔ $v_۱$، $v_۲$، $\cdots$، v_m روی K است و K دارای پایهٔ $w_۱$، $w_۲$، $\cdots$، w_n روی F است. ثابت می‌کنیم mn عنصر v_iw_j، که $i=۱,۲,\ldots,m$ و $j=۱,۲,\ldots,n$، یک پایه از L روی F می‌باشد.

ابتدا نشان می‌دهیم که این عنصرها L را روی F می‌پیمایند. این البته نشان می‌دهد که L یک توسیع متناهی F است. فرض کنیم $a\in L$. چون عنصرهای $v_۱$، $\cdots$، v_m یک پایه از L روی K را تشکیل می‌دهند، داریم $a=k_۱v_۱+\cdots+k_mv_m$ که در آن $k_۱$، $k_۲$، $\cdots$، k_m در Kاند. و چون $w_۱$، $\cdots$، w_n یک پایه از K روی F است، هر k_i را می‌توان به‌صورت زیر بیان کرد:

$$k_i=f_{i۱}w_۱+f_{i۲}w_۲+\cdots+f_{in}w_n$$

که در آن f_{ij}ها در Fاند. باگذاردن این عبارات به‌جای k_i در عبارت مربوط به a به‌دست می‌آوریم

$$\begin{aligned}a&=(f_{۱۱}w_۱+f_{۱۲}w_۲+\cdots+f_{۱n}w_n)v_۱\\&\quad+\cdots+(f_{m۱}v_۱+f_{m۲}v_۲+\cdots+f_{mn}v_n)v_m\end{aligned}$$

لذا این مجموع به‌طور صریح خواهد بود

$$a=f_{۱۱}w_۱v_۱+f_{۱۲}w_۲v_۱+\cdots+f_{ij}w_jv_i+\cdots+f_{mn}w_nv_m$$

پس mn عنصر v_iw_j در L میدان L را روی F می‌پیمایند. بنابراین $[L:F]$ متناهی است و در واقع $[L:F]\leq mn$.

برای اثبات $[L:F]=mn$ کافی است نشان دهیم که mn عنصر v_iw_j فوق مستقل خطی روی Fاند زیرا در این صورت، همراه با این امر که آنها L را روی F می‌پیمایند، این عناصر یک پایه از L روی F را تشکیل می‌دهند. لذا، طبق قضیهٔ ۵.۲.۵، نتیجهٔ مطلوب $[L:F]=mn=[L:K][K:F]$ به‌دست می‌آید.

پس فرض کنیم به ازای b_{ij}هایی در F رابطهٔ زیر را داشته باشیم:

$$\begin{aligned}۰&=b_{۱۱}v_۱w_۱+b_{۱۲}v_۱w_۲+\cdots+b_{۱n}v_۱w_n+b_{۲۱}v_۲w_۱\\&\quad+\cdots+b_{۲n}v_۲w_n+\cdots+b_{m۱}v_mw_۱+\cdots+b_{mn}v_mw_n\end{aligned}$$

با جمع‌وجور کردن این مجموع به‌دست می‌آوریم $c_1v_1 + c_2v_2 + \cdots + c_mv_m = 0$ که در آن $c_1 = b_{11}w_1 + \cdots + b_{1n}w_n$، $\cdots$، $c_m = b_{m1}w_1 + \cdots + b_{mn}w_n$. چون c_iها عناصر K بوده و v_1، $\cdots$، v_n در L مستقل خطی روی Kاند، به‌دست می‌آوریم $c_1 = c_2 = \cdots = c_m = 0$.

با توجه به اینکه $c_i = b_{i1}w_1 + \cdots + b_{in}w_n$ که در آن b_{ij}ها در Fاند و w_1، $\cdots$، w_n در K مستقل خطی روی Fاند، از $c_1 = c_2 = \cdots = c_m = 0$ نتیجه می‌شود که هر $b_{ij} = 0$. لذا فقط ترکیب خطی بدیهی عناصر v_iw_j با هر ضریب 0 می‌تواند روی F مساوی 0 باشد. بنابراین v_iw_jها مستقل خطی روی F می‌باشند. در بالا دیدیم که این برای اثبات قضیه کافی است. ■

از خواننده می‌خواهیم قضیهٔ ۱.۳.۵ را با نتیجهٔ کلیتر مذکور در مسئلهٔ ۱۷ از بخش ۲ مقایسه نماید. حال می‌توانید مسئلهٔ ۱۷ را به راحتی حل نمایید.

به‌عنوان نتیجه‌ای از قضیهٔ فوق داریم:

نتیجه. هرگاه $L \supset K \supset F$ سه میدان باشند به‌طوری که $[L : F]$ متناهی باشد، آن‌گاه $[K : F]$ متناهی بوده و $[L : F]$ را عاد می‌کند.

برهان. چون $L \supset K$، K نمی‌تواند عناصر مستقل خطی بیشتری از L روی F داشته باشد. و چون، به خاطر قضیهٔ ۶.۲.۵، $[L : F]$ اندازهٔ بزرگترین مجموعه از عناصر مستقل خطی در L روی F است، داریم $[K : F] \leq [L : F]$. در نتیجه باید متناهی باشد. چون L با بعد متناهی روی F بوده و K شامل F است، L باید با بعد متناهی روی K باشد. لذا تمام شرایط قضیهٔ ۱.۳.۵ برقرارند که از آنجا $[L : F] = [L : K][K : F]$. پس، همان‌طور که در نتیجه حکم شده، $[K : F]$ عدد $[L : F]$ را عاد می‌نماید. ■

اگر K یک توسیع متناهی F باشد، می‌توان راجع به رفتار عناصر K در مقابل F صحبت کرد.

قضیهٔ ۲.۳.۵. فرض کنیم K یک توسیع متناهی F از درجهٔ n باشد. در این صورت، به ازای هر عنصر u در K، عناصری مانند α_0، α_1، $\cdots$، α_n در F وجود دارند که همه صفر نیستند به‌طوری که

$$\alpha_0 + \alpha_1 u + \cdots + \alpha_n u^n = 0$$

برهان. چون $[K : F] = \dim_F(K) = n$ و عنصرهای 1، u، u^2، $\cdots$، u^n، $n + 1$

تا هستند، بنابر قضیهٔ ۶.۲.۵ باید وابستهٔ خطی روی F باشند. لذا می‌توان α_0، α_1، ...، α_n را در F چنان یافت که همه ۰ نبوده و $\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \cdots + \alpha_n u^n = 0$ که قضیه را به ثبوت می‌رساند. ■

قضیهٔ فوق پیشنهاد می‌کند که عناصر یک توسیع میدان و صادق در یک چندجمله‌ای غیربدیهی را ممتاز سازیم.

تعریف. هرگاه $F \subset K$ دو میدان باشند، آنگاه گوییم $a \in K$ روی F جبری است اگر یک چندجمله‌ای مانند $p(x) \neq 0$ در $F[x]$ باشد که $p(a) = 0$.

منظور از $p(a)$ یعنی عنصر $\alpha_0 a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n$ در K که در آن

$$p(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n$$

اگر K یک توسیع F باشد به‌طوری که هر عنصرش روی F جبری باشد، K را یک توسیع جبری F می‌نامیم. قضیهٔ ۲.۳.۵ را می‌توان با این اصطلاحات به‌صورت زیر بیان کرد: هرگاه K یک توسیع متناهی F باشد، آنگاه K یک توسیع جبری F می‌باشد.

عکس این مطلب درست نیست؛ یعنی یک توسیع جبری F لزوماً از درجهٔ متناهی روی F نمی‌باشد. آیا می‌توانید در این مورد مثال بزنید؟

هر عنصر K که روی F جبری نباشد روی F متعالی نام دارد.

حال چند عنصر جبری را در محدوده‌ای ملموس مثال می‌زنیم. $\mathbb{C} \supset \mathbb{Q}$، یعنی میدان مختلط به‌عنوان توسیعی از میدان گویا، را در نظر می‌گیریم. عدد مختلط $a = 1 + i$ روی $\mathbb{Q}$ جبری است زیرا در $a^2 - 2a + 2 = 0$ روی $\mathbb{Q}$ صدق می‌کند. به همین نحو عدد حقیقی $b = \sqrt{1 + \sqrt[3]{1 + \sqrt{2}}}$ روی $\mathbb{Q}$ جبری است زیرا $b^2 = 1 + \sqrt[3]{1 + \sqrt{2}}$؛ در نتیجه $(b^2 - 1)^3 = 1 + \sqrt{2}$ و لذا $((b^2 - 1)^3 - 1)^2 = 2$. با بسط این رابطه به یک عبارت چندجمله‌ای غیربدیهی از b با ضرایب گویا می‌رسیم که مساوی ۰ است. لذا b روی $\mathbb{Q}$ جبری می‌باشد.

به آسانی می‌توان اعدادی حقیقی ساخت که روی $\mathbb{Q}$ متعالی باشند (رک. بخش ۶ از فصل ۶). ولی اثبات متعالی بودن برخی از اعداد آشنا واقعاً زحمت دارد. می‌توان نشان داد که دو عدد آشنای e و π روی $\mathbb{Q}$ متعالی‌اند. متعالی بودن e در سال ۱۸۷۳ توسط هرمیت (Hermite) و متعالی بودن π روی $\mathbb{Q}$، که بسیار مشکلتر است، اول بار توسط لیندمان (Lindemann) در ۱۸۸۲ ثابت شد. ما در اینجا متعالی بودن هیچ عددی را روی $\mathbb{Q}$ ثابت نمی‌کنیم. ولی در بخش ۷

از فصل ۶ لااقل گنگ بودن π را نشان می‌دهیم. با این کار می‌توان آن را به‌عنوان یک عدد متعالی روی $\mathbb{Q}$ نامزد کرد زیرا هر عدد گویای b به وضوح روی $\mathbb{Q}$ جبری است چون که در چندجمله‌ای $p(x) = x - b$، که دارای ضرایب گویاست، صدق می‌کند.

تعریف. گوییم یک عدد مختلط عدد جبری است اگر روی $\mathbb{Q}$ جبری باشد.

همان‌طور که به‌زودی خواهید دید، اعداد جبری یک میدان تشکیل می‌دهند که زیر میدانی است از $\mathbb{C}$.

حال به بحث کلی نظریهٔ میدانها باز می‌گردیم. ما در قضیهٔ ۲.۳.۵ دیدیم که اگر K یک توسیع متناهی F باشد، هر عنصر K روی F جبری است. می‌پرسیم: اگر K توسیعی از F بوده و $a \in K$ روی F جبری باشد، آیا می‌توان با استفاده از a یک توسیع متناهی F را ساخت؟ جواب مثبت است. این امر نتیجه‌ای است از قضیهٔ زیر که ما آن را در محدوده‌ای کمی کلیتر از آنچه واقعاً لازم داریم ثابت خواهیم کرد.

قضیهٔ ۳.۳.۵. فرض کنیم D یک قلمرو صحیح یکدار بوده و یک فضای برداری با بعد متناهی روی میدان F نیز باشد. در این صورت D یک میدان می‌باشد.

برهان. برای اثبات این قضیه باید برای $a \neq 0$ در D معکوس a^{-1} در D را بیابیم: $aa^{-1} = 1$.

همانند برهان قضیهٔ ۲.۳.۵، هرگاه $\dim_F(D) = n$، آنگاه 1، a، a^2، $\cdots$، a^n در D وابستهٔ خطی روی Fاند. لذا، به ازای α_0، α_1، $\cdots$، α_n مناسبی در F که همه 0 نیستند،

$$\alpha_0 a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$$

فرض کنیم $p(x) = \beta_0 x^r + \beta_1 x^{r-1} + \cdots + \beta_r \neq 0$ یک چندجمله‌ای در $F[x]$ ازکوچکترین درجه باشد به‌طوری که $p(a) = 0$. حکم می‌کنیم که $\beta_r \neq 0$. چرا که اگر $\beta_r = 0$،

$$\begin{aligned} 0 &= \beta_0 a^r + \beta_1 a^{r-1} + \cdots + \beta_{r-1} a \\ &= (\beta_0 a^{r-1} + \beta_1 a^{r-2} + \cdots + \beta_{r-1}) a \end{aligned}$$

چون D قلمرو صحیح بوده و $a \neq 0$، نتیجه می‌شود که $\beta_0 a^{r-1} + \beta_1 a^{r-2} + \cdots + \beta_{r-1} = 0$. لذا $q(a) = 0$ که در آن $q(x) = \beta_0 x^{r-1} + \beta_1 x^{r-2} + \cdots + \beta_{r-1}$ در $F[x]$ از درجهٔ

کوچکتر از درجهٔ $p(x)$ است که یک تناقض می‌باشد. لذا $\beta_r \neq ۰$؛ در نتیجه $\beta_r^{-۱}$ در F بوده و

$$\frac{a(\beta_۰ a^{r-۱} + \cdots + \beta_{r-۱})}{\beta_r} = -۱$$

که $-(\beta_۰ a^{r-۱} + \cdots + \beta_{r-۱})/\beta_r$ را در D به‌دست می‌دهد که $a^{-۱}$ مطلوب a در D می‌باشد. این امر قضیه را ثابت خواهد کرد. ■

حال که قضیهٔ ۳.۳.۵ در دست است می‌خواهیم آن را به‌کار بریم. می‌پرسیم: چگونه می‌توان زیرحلقه‌هایی از میدان K را ساخت که شامل F بوده و با بعد متناهی روی F باشند؟ این زیرحلقه‌ها، به‌عنوان زیرحلقه‌های یک میدان، خودبه‌خود قلمرو صحیح‌اند، و در فرض قضیهٔ ۳.۳.۵ صدق می‌کنند. ابزارها عناصری در K اند که روی F جبری می‌باشند.

ولی ابتدا یک تعریف می‌آوریم.

تعریف. عنصر a در توسیع K از F را جبری از درجهٔ n گوییم اگر یک چندجمله‌ای مانند $p(x)$ در $F[x]$ از درجهٔ n باشد به‌طوری که $p(a) = ۰$ و هیچ چندجمله‌ای ناصفر از درجهٔ کمتر در $F[x]$ این خاصیت را نداشته باشد.

می‌توان فرض کرد که چندجمله‌ای $p(x)$ در این تعریف تکین است، زیرا می‌توان این چندجمله‌ای را بر بالاترین ضریبش تقسیم و چندجمله‌ای تکینی مانند $q(x)$ در $F[x]$ با همان درجهٔ $p(x)$ یافت که $q(a) = ۰$. لذا از این پس فرض می‌کنیم این چندجمله‌ای $p(x)$ تکین باشد. ما آن را چندجمله‌ای مینیمال برای a روی F می‌نامیم.

لم ۴.۳.۵. فرض کنیم $a \in K$ روی F جبری با چندجمله‌ای مینیمال $p(x)$ در $F[x]$ باشد. در این صورت $p(x)$ در $F[x]$ تحویل‌ناپذیر است.

برهان. فرض کنیم $p(x)$ در $F[x]$ تحویل‌ناپذیر نباشد. در این صورت $p(x) = f(x)g(x)$ که در آن $f(x)$ و $g(x)$ در $F[x]$ بوده و درجهٔ هر یک مثبت است. چون $۰ = p(a) = f(a)g(a)$ و $f(a)$ و $g(a)$ در میدان Kاند، نتیجه می‌شود که $f(a) = ۰$ یا $g(a) = ۰$ که هر دو ناممکن است زیرا هر دوی $f(x)$ و $g(x)$ از درجهٔ کمتر از درجهٔ $f(x)$اند. لذا $p(x)$ در $F[x]$ تحویل‌ناپذیر می‌باشد. ■

فرض کنیم $a \in K$ روی F جبری از درجهٔ n بوده و $p(x) \in F[x]$ چندجمله‌ای مینیمال آن روی F باشد. بنابر الگوریتم تقسیم، به ازای $f(x) \in F[x]$ داریم $f(x) = q(x)p(x) + r(x)$

که در آن $q(x)$ و $r(x)$ در $F[x]$ بوده و $r(x) = 0$ یا $\deg r(x) < \deg p(x)$. لذا $f(x) = q(a)p(a) + r(a) = r(a)$ زیرا $p(a) = 0$. به‌طور خلاصه، هر عبارت چندجمله‌ای از a روی F را می‌توان به‌صورت یک عبارت چندجمله‌ای از a از درجهٔ حداکثر $n-1$ بیان کرد.

فرض کنیم $F[a] = \{f(a) | f(x) \in F[x]\}$. حکم می‌کنیم که $F[a]$ زیر میدانی از K است که شامل هر دوی F و a می‌باشد و $[F(a) : F] = n$. بنابر مطلب فوق، $F[a]$ به وسیلهٔ ۱، a، a^2، $\cdots$، a^{n-1} روی F پیموده می‌شود؛ در نتیجه با بعد متناهی روی F است. به‌علاوه به آسانی معلوم می‌شود که $F[a]$ یک زیرحلقهٔ K است. $F[a]$ به‌عنوان زیرحلقه‌ای از K یک قلمرو صحیح است. لذا، طبق قضیهٔ ۳.۳.۵، $F[a]$ یک میدان می‌باشد. چون به‌وسیلهٔ ۱، a، a^2، $\cdots$، a^{n-1} روی F پیموده می‌شود، داریم $[F[a] : F] \leq n$. برای اثبات $[F[a] : F] = n$ کافی است نشان دهیم که ۱، a، a^2، $\cdots$، a^{n-1} مستقل خطی روی Fاند. ولی اگر $\alpha_0 + \alpha_1 a + \cdots + \alpha_{n-1}a^{n-1} = 0$ که در آن α_iها در Fاند، $q(a) = 0$ که در آن $q(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1}$ در $F[x]$ است. چون $q(x)$ از درجهٔ کمتر از درجهٔ $p(x)$ است، که چندجمله‌ای مینیمال a در $F[x]$ است، نتیجه می‌شود که $q(x) = 0$. این ایجاب می‌کند که $\alpha_0 = \alpha_1 = \cdots = \alpha_{n-1} = 0$. لذا ۱، a، a^2، $\cdots$، a^{n-1} مستقل خطی روی F بوده و یک پایه از $F[a]$ روی F را تشکیل می‌دهند. لذا $[F[a] : F] = n$. چون $F[a]$ یک میدان است نه فقط مجموعه‌ای از عبارات چندجمله‌ای از a، $F[a]$ را با $F(a)$ نشان خواهیم داد. همچنین توجه کنید که اگر M میدانی شامل هر دوی F و a باشد، شامل تمام عبارات چندجمله‌ای از a روی F است؛ در نتیجهٔ $F(a) \subset M$. لذا $F(a)$ کوچکترین زیرمیدان K شامل هر دوی F و a می‌باشد.

تعریف. $F(a)$ میدان یا توسیع حاصل از الحاق a به F نام دارد.

حال مطالب فوق را در قضیهٔ زیر خلاصه می‌کنیم.

قضیهٔ ۵.۳.۵. فرض کنیم $F \subset K$ و a در K جبری روی F از درجهٔ n باشد. در این صورت $F(a)$، یعنی میدان حاصل از الحاق a به F، یک توسیع متناهی F بوده و

$$[F(a) : F] = n$$

پیش از ترک قضیهٔ ۵.۳.۵ از دیدگاهی کمی متفاوت بدان نگاه می‌کنیم. فرض کنیم $F[x]$ حلقهٔ چندجمله‌ای از x روی F بوده و $M = (p(x))$ ایده‌آل تولید شده به‌وسیلهٔ $p(x)$ (چندجمله‌ای مینیمال a در K روی F) از $F[x]$ باشد. بنابر لم ۴.۳.۵، $p(x)$ در $F[x]$ تحویل‌ناپذیر است.

لذا، طبق قضیهٔ ۱۱.۵.۴، M یک ایده‌آل ماکزیمال $F[x]$ می‌باشد. بنابراین، طبق قضیهٔ ۲.۴.۴، $F[x]/(p(x))$ یک میدان می‌باشد.

نگاشت $\psi : F[x] \to K$ را با $\psi(f(x)) = f(a)$ تعریف می‌کنیم. نگاشت ψ یک همریختی از $F[x]$ به توی K بوده و، طبق تعریف $F(a)$، نقش $F[x]$ در K چیزی جز $F(a)$ نیست. هستهٔ ψ چیست؟ طبق تعریف، $J = \{f(x) \in F[x] | \psi(f(x)) = ۰\}$، و چون $\psi(f(x)) = f(a)$، $J = \{f(x) \in F[x] | f(a) = ۰\}$. چون $p(x)$ در J بوده و $p(x)$ چندجمله‌ای مینیمال a روی F است، $p(x)$ در بین عناصر J از پایین‌ترین درجه می‌باشد. لذا، طبق برهان قضیهٔ ۶.۵.۴، $J = (p(x))$؛ و در نتیجه $J = M$. بنابر قضیهٔ اول همریختی برای حلقه‌ها، $F(a) =$ نقش $F[x]$ تحت $\psi \simeq F[x]/M$، و چون $F[x]/M$ میدان است، $F(a)$ میدان می‌باشد. اثبات رابطهٔ $[F(a) : F] = \deg p(x)$ از این دیدگاه را به خواننده وامی‌گذاریم.

مسائل

۱. نشان دهید که اعداد زیر در $\mathbb{C}$ اعدادی جبری‌اند:

الف) $\sqrt{۲} + \sqrt{۳}$؛

ب) $\sqrt{۷} + \sqrt[۳]{۱۲}$؛

پ) $۲ + i\sqrt{۳}$؛

ت) $\cos(۲\pi/k) + i\sin(۲\pi/k)$ که در آن k یک عدد صحیح مثبت است.

۲. درجهٔ اعداد قسمتهای (الف) و (پ) مسئلهٔ ۱ را روی $\mathbb{Q}$ تعیین کنید.

۳. درجهٔ $\cos(۲\pi/۳) + i\sin(۲\pi/۳)$ روی $\mathbb{Q}$ چیست؟

۴. درجهٔ $\cos(۲\pi/۸) + i\sin(۲\pi/۸)$ روی $\mathbb{Q}$ چیست؟

۵. اگر p یک عدد اول باشد، ثابت کنید درجهٔ $\cos(۲\pi/p) + i\sin(۲\pi/p)$ روی $\mathbb{Q}$ مساوی $p - ۱$ بوده و

$$f(x) = ۱ + x + x^۲ + \cdots + x^{p-۱}$$

چندجمله‌ای مینیمال آن روی $\mathbb{Q}$ است.

۶. (برای شاگردانی که درس حساب دیفرانسیل و انتگرال را گذرانیده‌اند) نشان دهید که

$$e = ۱ + \frac{۱}{۱!} + \frac{۱}{۲!} + \cdots + \frac{۱}{n!} + \cdots$$

گنگ است.

۷. اگر a در K چنان باشد که $a^{۲}$ روی زیر میدان F از K جبری باشد، نشان دهید که a روی F جبری است.

۸. اگر $F \subset K$ و $f(a)$ روی F جبری باشد که در آن $f(x)$ از درجهٔ مثبت در $F[x]$ بوده و $a \in K$، ثابت کنید a روی F جبری است.

۹. در بحث بعد از قضیهٔ ۵.۳.۵ نشان دهید که $F[x]/M$ از درجهٔ $n = \deg p(x)$ روی F است؛ و در نتیجه $[F(a) : F] = n = \deg p(x)$.

۱۰. ثابت کنید $\cos ۱^{\circ}$ روی $\mathbb{Q}$ جبری است. (یک درجه $= ۱^{\circ}$.)

۱۱. اگر $a \in K$ روی F متعالی باشد، قرار دهید

$$F(a) = \{f(a)/g(a) | f(x), g(x) \neq \circ \in F[x]\}$$

و نشان دهید که $F(a)$ یک میدان و کوچکترین زیرمیدان K شامل هر دوی F و a است.

۱۲. اگر a همانند مسئلهٔ ۱۱ باشد، نشان دهید $F(a) \simeq F(x)$ که در آن $F(x)$ میدان توابع گویا از x روی F است.

۱۳. فرض کنید K یک میدان متناهی و F زیرمیدانی از آن باشد. اگر $[K : F] = n$ و F دارای q عنصر باشد، نشان دهید که K دارای q^n عنصر است.

۱۴. با استفاده از مسئلهٔ ۱۳ نشان دهید که هر میدان متناهی دارای p^n عنصر است که در آن p عددی اول و n عدد صحیح مثبتی می‌باشد.

۱۵. دو میدان K و F را چنان بسازید که K یک توسیع جبری F بوده ولی یک توسیع متناهی F نباشد.

۴. توسیعهای متناهی

بخش قبل را ادامه می‌دهیم. مجدداً $F \subset K$ دو میدان بوده و حروف رومی عناصر K و حروف یونانی عنصرهای F می‌باشند.

فرض کنیم $E(K)$ مجموعهٔ تمام عناصری در K باشد که روی F جبری‌اند. مسلماً $F \subset E(K)$. هدف ما اثبات میدان بودن $E(K)$ است. پس از این کار، به‌طرز جاگرفتن $E(K)$ در K خواهیم پرداخت.

بدون بحث بیشتر، قضیهٔ زیر را ثابت می‌کنیم.

قضیهٔ ۱.۴.۵. $E(K)$ زیرمیدان K است.

برهان. آنچه باید نشان دهیم این است که هرگاه $a, b \in K$ روی F جبری باشند، آنگاه $a \pm b$، ab، و a/b (اگر $b \neq 0$) همه روی F جبری‌اند. این متضمن آن است که $E(K)$ زیرمیدانی از K باشد. جبری بودن $a \pm b$، ab، و a/b را یکجا ثابت می‌کنیم.

فرض کنیم $K_0 = F(a)$ زیرمیدانی از K باشد که با الحاق a به F به‌دست می‌آید. چون a روی F جبری مثلاً از درجهٔ m است، بنابر قضیهٔ ۵.۳.۵، $[K_0 : F] = m$. و چون b روی F جبری بوده و K_0 شامل F است، b روی K_0 جبری می‌باشد. هرگاه b روی F جبری از درجهٔ n باشد، آنگاه روی K_0 جبری از درجهٔ حداکثر n می‌باشد. لذا $K_1 = K_0(b)$، یعنی زیرمیدان حاصل از K با الحاق b به K_0، یک توسیع متناهی K_0 بوده و $[K_1 : K_0] \leq n$.

لذا، طبق قضیهٔ ۱.۳.۵، $[K_1 : F] = [K_1 : K_0][K_0 : F] \leq mn$؛ یعنی K_1 یک توسیع متناهی F است. لذا، طبق قضیهٔ ۲.۳.۵، K_1 یک توسیع جبری F است؛ و در نتیجه تمام عناصرش روی F جبری‌اند. چون $a \in K_0 \subset K_1$ و $b \in K_1$، پس تمام عناصر $a \pm b$، ab، و a/b در K_1اند. لذا روی F جبری می‌باشند. این درست همان چیزی است که می‌خواستیم و قضیه به ثبوت می‌رسد. ■

اگر به برهان فوق کمی دقیقتر نگاه کنیم می‌بینیم که مطلب بیشتری ثابت شده است؛ یعنی:

نتیجه. هرگاه a و b در K روی F جبری و به‌ترتیب از درجات m و n باشند، آنگاه $a \pm b$، ab، و a/b (اگر $b \neq 0$) روی F جبری از درجهٔ حداکثر mn می‌باشند.

حالتی خاص، ولی مهم و شایستهٔ ذکر، حالت $K = \mathbb{C}$ و $F = \mathbb{Q}$ است. در این حالت عناصر جبری در $\mathbb{C}$ روی $\mathbb{Q}$ را اعداد جبری نامیدیم. لذا قضیهٔ ۱.۴.۵ در این حالت به‌صورت زیر درمی‌آید.

قضیهٔ ۲.۴.۵. اعداد جبری زیرمیدانی از $\mathbb{C}$ را تشکیل می‌دهند.

ممکن است حدس بزنید که مجموعهٔ اعداد جبری تمام $\mathbb{C}$ است. این حدس درست نیست زیرا اعداد متعالی وجود دارند. این مطلب را در بخش ۶ از فصل ۶ نشان می‌دهیم.

حال به میدان کلی K باز می‌گردیم. زیرمیدانش $K(E)$ ویژگی بسیار خاصی دارد که ذیلاً ثابت می‌شود. این خاصیت می‌گوید که هر عنصر در K که روی $E(K)$ جبری است باید در $E(K)$ باشد.

برای آنکه در برهان زیر انحراف مطلب نیابیم نماد زیر را معرفی می‌کنیم. هرگاه a_1،

a_2، $\cdots$، a_n در K باشند، آن‌گاه $F(a_1, \ldots, a_n)$ میدانی است که به طریق زیر به‌دست می‌آید: $K_1 = F(a_1)$، $K_2 = K_1(a_2) = F(a_1, a_2)$، $K_3 = K_2(a_3) = F(a_1, a_2, a_3)$، $\cdots$، $K_n = K_{n-1}(a_n) = F(a_1, a_2, \ldots, a_n)$.

حال قضیهٔ زیر را ثابت می‌کنیم.

قضیهٔ ۳.۴.۵. هرگاه u در K روی $E(K)$ جبری باشد، آن‌گاه u در $E(K)$ می‌باشد.

برهان. برای اثبات قضیه کافی است نشان دهیم که u روی F جبری است. این امر u را در $E(K)$ قرار داده و مطلب را تمام خواهد کرد.

چون u روی $E(K)$ جبری است، یک چندجمله‌ای غیربدیهی مانند

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n$$

هست که در آن a_1، a_2، $\cdots$، a_n در $E(K)$ بوده و $f(u) = 0$. چون a_1، a_2، $\cdots$، a_n در $E(K)$اند، روی F جبری از درجهٔ مثلاً m_1، m_2، $\cdots$، m_n می‌باشند. حکم می‌کنیم که $[F(a_1, \ldots, a_n) : F]$ حداکثر $m_1 m_2 \cdots m_n$ است. برای مشاهدهٔ این امر، قضیهٔ ۱.۳.۵ را n بار بر دنبالهٔ K_1، K_2، $\cdots$، K_n از میدانهای تعریف شده در فوق اعمال می‌کنیم. برهانش به خواننده واگذار می‌شود. لذا، چون u روی میدان $K_n = F(a_1, a_2, \ldots, a_n)$ جبری است [چندجمله‌ای برقرار به‌وسیلهٔ u عبارت است از $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ که جمیع ضرایبش در $F(a_1, a_2, \ldots, a_n)$ می‌باشند]، میدان $K_n(u)$ یک توسیع متناهی K_n است، و چون K_n یک توسیع متناهی F است، مجدداً، طبق قضیهٔ ۱.۳.۵، $K_n(u)$ یک توسیع متناهی F است. از آنجا که $u \in K_n(u)$، از قضیهٔ ۲.۳.۵ معلوم می‌شود که u روی F جبری است. این امر u را طبق تعریف $E(K)$ در $E(K)$ می‌گذارد و بدین ترتیب قضیه به ثبوت می‌رسد. ■

قضیهٔ معروفی از گاوس وجود دارد که اغلب قضیهٔ اساسی جبر نامیده می‌شود. این قضیه (برحسب توسیع) می‌گوید که تنها توسیع متناهی میدان اعداد مختلط $\mathbb{C}$ خود $\mathbb{C}$ است. این نتیجه در واقع یک نتیجهٔ صرفاً جبری نیست و اعتبارش اتکای سنگینی به خواص توپولوژیک میدان اعداد حقیقی دارد. این قضیه هرچه باشد قضیهٔ بسیار مهمی در جبر و بسیاری از بخشهای دیگر ریاضیات است.

تنظیم قضیهٔ اساسی جبر برحسب عدم وجود توسیعهای متناهی $\mathbb{C}$ با صورت معمول آن کمی فرق دارد. متداولترین شکلش مستلزم ریشهٔ یک چندجمله‌ای است، مفهومی که بعدها به تفصیل

مطرح خواهد شد. قضیهٔ اساسی جبر برحسب این مفهوم به‌صورت زیر درمی‌آید: یک چندجمله‌ای از درجهٔ مثبت با ضرایب در $\mathbb{C}$ دست‌کم یک ریشه در $\mathbb{C}$ دارد. بعدها، پس از ذکر مطالبی راجع به ریشه‌ها، معنی دقیق این حکم و هم‌ارزی‌اش با شکل دیگر قضیه که در بالا ذکر شد روشن خواهد شد.

میدان L با خاصیت $\mathbb{C}$ مذکور در بند فوق را به‌طور جبری بسته می‌نامیم. هرگاه بپذیریم که $\mathbb{C}$ به‌طور جبری بسته است (قضیهٔ گاوس)، آن‌گاه، بنابر قضیهٔ ۳.۴.۵ نیز داریم:

میدان اعداد جبری به‌طوری جبری بسته است.

مسائل

۱. با ارائهٔ یک چندجمله‌ای مانند $f(x)$ از درجهٔ ۴ روی $\mathbb{Q}$ که $f(a) = ۰$، نشان دهید که $a = \sqrt{۲} - \sqrt{۳}$ روی $\mathbb{Q}$ جبری از درجهٔ حداکثر ۴ است.

۲. اگر a و b در K روی F جبری از درجات m و n بوده و m و n نسبت به هم اول باشند، نشان دهید که $[F(a,b) : F] = mn$.

۳. اگر $a \in \mathbb{C}$ چنان باشد که $p(a) = ۰$ و

$$p(x) = x^{۵} + \sqrt{۲}x^{۳} + \sqrt{۵}x^{۲} + \sqrt{۷}x + \sqrt{۱۱}$$

نشان دهید که a روی Q جبری از درجهٔ حداکثر ۸۰ است.

۴. اگر $F \subset K$ چنان باشد که $[K : F] = p$ که در آن p اول است، نشان دهید که به ازای هر a در K که در F نباشد، $K = F(a)$.

۵. اگر $[K : F] = ۲^n$ و T زیرمیدانی از K باشد، نشان دهید که به‌ازای $m \leq n$ی، $[T : F] = ۲^m$.

۶. دو عدد جبری a و b از درجات به‌ترتیب ۲ و ۳ مثال بزنید که ab از درجهٔ کمتر از ۶ روی $\mathbb{Q}$ باشد.

۷. اگر $F \subset K$ دو میدان و $a_۱$، $\cdots$، a_n در K باشند،نشان دهید که به ازای هر جایگشت σ از ۱، ۲، ...، n، $F(a_۱, \ldots, a_n)$ مساوی $F(a_{\sigma(۱)}, \ldots, a_{\sigma(n)})$ است.

۵. ترسیم‌پذیری

یونانیان باستان، به‌خلاف سایر تمدنهای همعصر خود، به ریاضیات به‌جای انبانی از ترفندها برای محاسبه و سنجش به‌صورت یک نظام مجرد توجه داشته‌اند. آنها نتایجی قوی در نظریهٔ اعداد و به‌خصوص در هندسه به‌دست آوردند و مسائل جالبی در این زمینه طرح کردند. مسائل طرح شده توسط آنها در هندسه (که دوتای آنها مبحث فعلی ما را تشکیل می‌دهند) هنوز مورد توجه بوده و دارای وزن می‌باشند. جی. اچ. هاردی، ریاضیدان انگلیسی، درکتاب کوچک غم‌انگیز ولی جذاب خود به نام *A Mathematician's Apology* ریاضیدانان یونانی را «همکاران خود درکالجی دیگر» توصیف می‌کند.

در این بخش دو سؤال از یونان باستان مورد توجه ماست. ولی در واقع جواب هر دو نتیجه‌ای است از محک ترسیم‌پذیری که به‌دست خواهیم آورد. حال این دو سؤال را بیان کرده و کمی بعد نتایج حاصل از آنها را توضیح خواهیم داد.

سؤال ۱. آیا با استفاده از ستاره و پرگار می‌توان یک مکعب را تضعیف کرد؟ (تضعیف یک مکعب یعنی دو برابر کردن حجم آن.)

سؤال ۲. آیا با استفاده از ستاره و پرگار می‌توان یک زاویه را به سه قسمت مساوی تقسیم کرد؟

علی‌رغم تعداد زیادی تثلیث‌گر که هر سال ظهور می‌کنند، جواب هر دو سؤال فوق «منفی» است. همان‌طور که خواهید دید، تثلیث 60° فقط با استفاده از ستاره و پرگار ناممکن است. البته بعضی از زوایا مثلاً 0°، 90°، 145°، 180°، $\cdots$ قابل تثلیث‌اند ولی اغلب زوایا این خاصیت را ندارند.

پیش از پرداختن به معنی دقیق این سؤالات، قواعد بازی را به‌طور صریح بیان می‌کنیم. منظور از ستاره خط‌کش، یعنی وسیله‌ای برای سنجش طولهای دلخواه، نیست. یک ستاره فقط یک خط راست است بدون خواص کتی یا متری. ما یک پاره‌خط داریم که به آن طول ۱ نسبت می‌دهیم و هر طول دیگری که به‌دست می‌آوریم فقط باید با استفاده از ستاره و پرگار باشد.

عدد حقیقی نامنفی b را یک طول ترسیم‌پذیر نامیم اگر با تعدادی متناهی بار اعمال ستاره و پرگار و نقاط اشتراک حاصل بین خطوط و دوایر رسم شده به این طریق بتوان پاره‌خطی به طول b را با شروع از پاره‌خطی که طول ۱ بدان داده‌ایم رسم کرد.

از هندسهٔ دبیرستان نکاتی به یاد می‌آیند که در این چهارچوب قابل انجام‌اند.

۱. هر طولی که روی یک خط ترسیم‌پذیر باشد با استفاده از پرگار به‌عنوان عامل انتقال بر هر

خط دیگر نیز ترسیم‌پذیر است.

۲. از یک نقطه می‌توان خطی به موازات خطی مفروض رسم کرد.

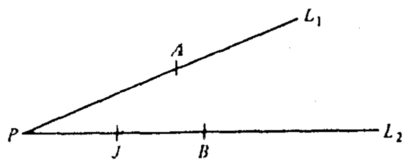
۳. به ازای هر عدد صحیح نامنفی n می‌توان طول n را رسم کرد.

با استفاده از اینها و نتایج مربوط به تشابه مثلثها می‌توان هر طول گویای نامنفی را رسم کرد. ما در اینجا این کار را نمی‌کنیم زیرا این امر حالت خاص چیزی است که اینک می‌خواهیم انجام دهیم.

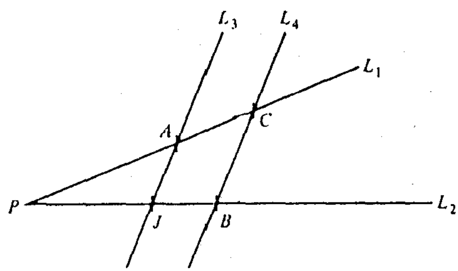
حال حکم به خواص زیر می‌دهیم:

۱. هرگاه a و b دو طول ترسیم‌پذیر باشند، آن‌گاه $a + b$ نیز چنین است. چرا که اگر AB پاره‌خطی به طول a و CD پاره‌خطی به طول b باشد، می‌توان پاره‌خط CD را به‌وسیلهٔ پرگار منتقل کرده و خط ABE را یافت که در آن AB به طول a و BE به طول b باشد. لذا پاره‌خط AE به طول $a + b$ می‌باشد. اگر $b > a$، $b - a$ چطور رسم می‌شود؟

۲. هرگاه a و b طولهایی ترسیم‌پذیر باشند، آن‌گاه ab نیز چنین است. می‌توان فرض کرد $a \neq 0$ و $b \neq 0$ چه در غیر این صورت حکم بدیهی است. نمودار زیر را در نظر می‌گیریم:



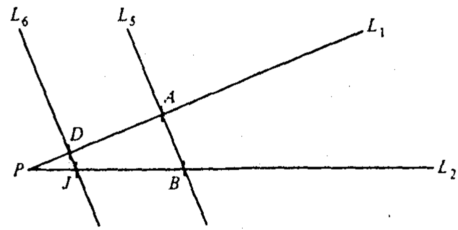
که در آن دو خط متمایز L_1 و L_2 در P متقاطع بوده و PA به طول a، PB به طول b، و PJ به طول ۱ می‌باشد. فرض کنیم L_3 خط ماربر J و A و L_4 خط موازی L_3 ماربر B باشد. اگر C نقطهٔ اشتراک L_1 و L_4 باشد، نمودار زیر را خواهیم داشت:



همهٔ این ترسیمات را می‌توان با ستاره و پرگار انجام داد. از هندسهٔ مقدماتی می‌دانیم که طول PC

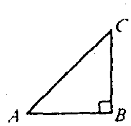
مساوی ab است. لذا ab ترسیم‌پذیر می‌باشد.

۳. هرگاه a و b ترسیم‌پذیر بوده و $b \neq 0$، آن‌گاه a/b ترسیم‌پذیر است. نمودار زیر را در نظر می‌گیریم:



که در آن P، A، B، J، L_1، و L_2 همانهای بوده در خاصیت ۲ فوقند. فرض کنیم L_5 خط ماربر A و B و L_6 خط ماربر J موازی L_5 باشد. هرگاه D نقطهٔ اشتراک L_1 و L_6 باشد، آن‌گاه مجدداً، طبق هندسهٔ مقدماتی، طول PD مساوی a/b می‌باشد. مجدداً تأکید می‌کنیم که همهٔ این ترسیمات را می‌توان با ستاره و پرگار انجام داد.

این البته نشان می‌دهد که اعداد گویای نامنفی طولهایی ترسیم‌پذیرند زیرا خارج‌قسمتهای اعداد صحیح نامنفی‌اند که می‌دانیم طولهایی ترسیم‌پذیر می‌باشند. اما طولهای ترسیم‌پذیر دیگری مثلاً عدد گنگ $\sqrt{2}$ نیز وجود دارند. چون مثلث قائم‌الزاویهٔ



به اضلاع AB و BC به طول ۱ را می‌توان با ستاره و پرگار رسم کرد، از قضیهٔ فیثاغورس معلوم می‌شود که AC به طول $\sqrt{2}$ است. لذا $\sqrt{2}$ طولی ترسیم‌پذیر می‌باشد.

در خواص ۱ تا ۳ نشان دادیم که طولهای ترسیم‌پذیر تقریباً یک میدان تشکیل می‌دهند. آنچه غایب است وجود قرینه‌هاست. برای رفع این مشکل تعریف زیر را می‌آوریم.

تعریف. گوییم عدد حقیقی a یک عدد ترسیم‌پذیر است اگر $|a|$، یعنی قدرمطلق a، طولی ترسیم‌پذیر باشد.

ممکن است حدس بزنید که هر عدد حقیقی ترسیم‌پذیر است. به‌زودی محکی به‌دست می‌آوریم که به ما می‌گوید که بعضی از اعداد حقیقی ترسیم‌پذیر نیستند. مثلاً از این محک می‌توان نتیجه

گرفت که $\sqrt[3]{2}$ و $\cos 20^\circ$ ترسیم‌پذیر نیستند. این به نوبهٔ خود به ما اجازه می‌دهد که به هر دو سؤال ۱ و ۲ فوق جواب «منفی» بدهیم.

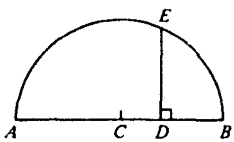
ابتدا قضیهٔ زیر را ثابت می‌کنیم.

قضیهٔ ۱.۵.۵. اعداد ترسیم‌پذیر زیرمیدانی از میدان اعداد حقیقی را تشکیل می‌دهند.

برهان. خواص ۱ تا ۳ تقریباً همهٔ کار را انجام می‌دهند. خاصیت ۱ باید کمی تعدیل شود تا قرینه‌ها نیز مجاز باشند. ذکر جزئیات را به خواننده محول می‌کنیم. ■

هدف بعدی نشان دادن این است که هر عدد ترسیم‌پذیر باید یک عدد جبری باشد، نه یک عدد جبری قدیم بلکه عددی که در یک شرط نسبتاً سخت صدق می‌کند.

ابتدا توجه می‌کنیم که هرگاه $a \geq 0$ یک عدد ترسیم‌پذیر باشد، آن‌گاه $\sqrt{a}$ نیز چنین است. نمودار زیر را در نظر می‌گیریم:



این نمودار نیمدایره‌ای به شعاع $(a+1)/2$ و مرکز C بوده و AD به طول a، DB به طول ۱، و DE عمود بر AB در D است که دایره را در E قطع می‌کند. همهٔ اینها به‌وسیلهٔ ستاره و پرگار ترسیم‌پذیرند. از هندسهٔ مقدماتی می‌دانیم که DE به طول $\sqrt{a}$ است. لذا $\sqrt{a}$ ترسیم‌پذیر می‌باشد.

حال به یافتن شرط لازم برای آنکه یک عدد حقیقی ترسیم‌پذیر باشد می‌پردازیم. فرض کنیم K میدان اعداد ترسیم‌پذیر بوده و $K_\circ$ زیرمیدانی از K باشد. منظور از صفحهٔ $K_\circ$ یعنی مجموعهٔ تمام نقاط (a,b) در صفحهٔ اقلیدسی حقیقی که مختصات a و bشان در $K_\circ$اند. هرگاه (a,b) و (c,d) در صفحهٔ $K_\circ$ باشند، آن‌گاه خط مستقیم واصل بین آنها به معادلهٔ $(y-b)/(x-a)=(b-d)/(a-c)$ است؛ در نتیجه به شکل $ux+vy+w=0$ است که در آن u، v، و w در $K_\circ$اند. دو خط $u_1x+v_1y+w_1=0$ و $u_2x+v_2y+w_2=0$، که در آنها u_1، v_1، w_1 و u_2، v_2، w_2 همه در $K_\circ$اند، یا با هم موازیند یا نقطهٔ اشتراکشان در $K_\circ$ است. (ثابت کنید!)

هرگاه شعاع r دایره‌ای در $K_\circ$ بوده و مرکزش (a,b) در صفحهٔ $K_\circ$ باشد، آن‌گاه معادله‌اش عبارت است از $(x-a)^2+(y-b)^2=r^2$ که با بسط به شکل $x^2+y^2+dx+ey+f=0$

درمی‌آید که در آن d، e، و f در $K_\circ$اند. برای آنکه ببینیم این دایره خط $ux+vy+w=\circ$ راکجا در صفحهٔ $K_\circ$ قطع می‌کند، معادلات خط و دایره را همزمان حل می‌کنیم. مثلاً هرگاه $v\neq\circ$، آن‌گاه $y=-(ux+w)/v$. باگذاردن این به‌جای y در معادلهٔ $x^۲+y^۲+dx+ey+f=\circ$ دایره به معادلهٔ درجهٔ دو نسبت به مختص x (یعنی c) این نقطهٔ اشتراک به شکل $c^۲+s_۱c+s_۲=\circ$ با $s_۱$ و $s_۲$ در $K_\circ$ می‌رسیم. بنابر فرمول درجهٔ دو، $c=(-s_۱\pm\sqrt{s_۱^۲-۴s_۲})/۲$، و اگر خط و دایره در صفحهٔ حقیقی متقاطع باشند، $s_۱^۲-۴s_۲\geq\circ$. هرگاه $s=s_۱^۲-۴s_۲\geq\circ$ و $K_۱=K_\circ(\sqrt{s})$، آن‌گاه می‌بینیم که مختص x نقطهٔ اشتراک، یعنی c، در $K_۱$ قرار دارد. هرگاه $\sqrt{s}\in K_\circ$، آن‌گاه $K_۱=K_\circ$. در غیر این صورت $[K_۱:K_\circ]=۲$. چون مختص y نقطهٔ اشتراک $d=-(uc+w)/v$ است، d نیز در $K_۱$ می‌باشد. لذا نقطهٔ اشتراک (c,d) در صفحهٔ $K_۱$ است که $[K_۱:K_\circ]=۱$ یا ۲. داستان در صورتی که $v=\circ$ و $u\neq\circ$ به همین نحو می‌باشد.

بالاخره برای به‌دست آوردن اشتراک دو دایرهٔ $x^۲+y^۲+dx+ey+f=\circ$ و $x^۲+y^۲+gx+hy+k=\circ$ در صفحهٔ $K_\circ$، با تفریق یکی از این معادلات از دیگری به معادلهٔ خط $(d-g)x+(e-h)y+(f-k)=\circ$ در صفحهٔ $K_\circ$ می‌رسیم. لذا یافتن نقاط دو دایره در صفحهٔ $K_\circ$ همان یافتن نقاط اشتراک یک خط در صفحهٔ $K_\circ$ با یک دایره در همان صفحه است. این درست همان وضعیت فوق می‌باشد. لذا اگر دو دایره در صفحهٔ حقیقی متقاطع باشند، نقاط اشتراکشان در صفحهٔ توسیعی از $K_\circ$ از درجهٔ ۱ یا ۲ قرار دارد.

برای رسم طول ترسیم‌پذیر a، از صفحهٔ اعداد گویای $\mathbb{Q}$ شروع می‌کنیم. ستاره خطوط در صفحهٔ $\mathbb{Q}$ و پرگار دوایر در صفحهٔ $\mathbb{Q}$ را به‌دست می‌دهد. بنابر بحث فوق، اینها در نقطه‌ای در صفحهٔ یک توسیع درجهٔ ۱ یا ۲ از $\mathbb{Q}$ متقاطع‌اند. برای به‌دست آوردن a، با این روند از صفحهٔ $\mathbb{Q}$ به صفحهٔ $L_۱$ می‌رویم که مثلاً $[L_۱:\mathbb{Q}]=۱$ یا ۲. سپس به صفحهٔ $L_۲$ که $[L_۲:L_۱]=۱$ یا ۲ می‌رویم، و این کار را چندین بار تکرار می‌کنیم. بدین ترتیب دنباله‌ای متناهی از میدانها مانند $\mathbb{Q}=L_\circ\subset L_۱\subset\cdots\subset L_n$ به‌دست می‌آید که هر $[L_i:L_{i-۱}]=۱$ یا ۲ و a در L_n می‌باشد.

بنابر قضیهٔ ۵.۳.۱، $[L_n:\mathbb{Q}]=[L_n:L_{n-۱}][L_{n-۱}:L_{n-۲}]\cdots[L_۱:\mathbb{Q}]$ و چون هر $[L_i:L_{i-۱}]=۱$ یا ۲، می‌بینیم که $[L_n:\mathbb{Q}]$ توانی از ۲ است. چون $a\in L_n$، $\mathbb{Q}(a)$ زیرمیدانی از L_n است. لذا، طبق نتیجهٔ قضیهٔ ۵.۳.۱، $[\mathbb{Q}(a):\mathbb{Q}]$ باید توانی از ۲ را عاد کند. در نتیجه، به ازای عدد صحیح نامنفیی چون m، $[\mathbb{Q}(a):\mathbb{Q}]=۲^m$. به بیان معادل، بنابر قضیهٔ ۵.۳.۵، درجهٔ چندجمله‌ای مینیمال a روی $\mathbb{Q}$ باید توانی از ۲ باشد. این امر شرط لازم برای

ترسیم‌پذیری a می‌باشد. لذا محک مهمی برای ترسیم‌پذیری ثابت کرده‌ایم؛ یعنی:

قضیهٔ ۲.۵.۵. برای آنکه عدد حقیقی a ترسیم‌پذیر باشد، باید $[\mathbb{Q}(a):\mathbb{Q}]$ توانی از ۲ باشد. به بیان معادل، باید درجهٔ چندجمله‌ای مینیمال a روی $\mathbb{Q}$ توانی از ۲ باشد.

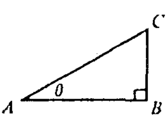
برای تضعیف مکعبی به ضلع ۱ (و در نتیجه به حجم ۱) به‌وسیلهٔ ستاره و پرگار باید مکعبی به طول ضلع b بسازیم که حجمش ۲ باشد. ولی حجم این مکعب $b^۳$ است؛ در نتیجه باید بتوان عدد ترسیم‌پذیر b را چنان یافت که $b^۳ = ۲$.

هرگاه b عددی حقیقی باشد که $b^۳ = ۲$، آن‌گاه چندجمله‌ای مینیمالش روی $\mathbb{Q}$ عبارت است از $p(x) = x^۳ - ۲$، زیرا این چندجمله‌ای تکین و تحویل‌ناپذیر روی $\mathbb{Q}$ است (اگر بخواهید، طبق محک آیزن اشتاین)، و $p(b) = ۰$. همچنین $p(x)$ از درجهٔ ۳ می‌باشد. چون ۳ توانی از ۲ نیست، بنابر قضیهٔ ۲.۵.۵، یک چنین b ترسیم‌پذیر وجود ندارد. لذا تضعیف مکعب به‌وسیلهٔ ستاره و پرگار جوابی منفی دارد. حال این امر را در قضیهٔ زیر خلاصه می‌کنیم.

قضیهٔ ۳.۵.۵. تضعیف یک مکعب به حجم ۱ به‌وسیلهٔ ستاره و پرگار ناممکن است.

حال که سؤال کلاسیک ۱ پاسخ یافته است به سؤال ۲، یعنی تثلیث یک زاویه به‌وسیلهٔ ستاره و پرگار، می‌پردازیم.

اگر بتوان زاویهٔ خاص ۶۰° را تثلیث کرد، می‌توان مثلث ABC نمودار زیر را، که در آن $\theta = ۲۰^\circ$ و AC به طول ۱ است، با ستاره و پرگار رسم نمود:



چون AB به طول $\cos ۲۰^\circ$ است، $b = \cos ۲۰^\circ$ یک عدد ترسیم‌پذیر می‌باشد.

حال نشان می‌دهیم که $b = \cos ۲۰^\circ$ یک عدد ترسیم‌پذیر نیست. این کار را با یافتن چندجمله‌ای مینیمال آن روی $\mathbb{Q}$ و نشان دادن آنکه این چندجمله‌ای از درجهٔ ۳ است انجام می‌دهیم. برای این کار فرمول سه برابر زاویه را از مثلثات به یاد می‌آوریم: $\cos ۳\phi = ۴\cos^۳\phi - ۳\cos\phi$. هرگاه $b = \cos ۲۰^\circ$، آن‌گاه چون $\frac{۱}{۲} = \cos ۶۰^\circ = \cos(۳\cdot ۲۰^\circ)$، این فرمول مثلثاتی به‌صورت

$\frac{1}{2} = 3b - 4b^3$ در می‌آید؛ و در نتیجه $8b^3 - 6b - 1 = 0$. اگر $c = 2b$، این رابطه به شکل $c^3 - 3c - 1 = 0$ در می‌آید. هرگاه b ترسیم‌پذیر باشد، آن‌گاه c نیز چنین است. ولی $p(c) = 0$ که در آن $p(x) = x^3 - 3x - 1$، و این چندجمله‌ای روی $\mathbb{Q}$ تحویل‌ناپذیر است. (ثابت کنید!) لذا $p(x)$ چندجمله‌ای مینیمال c روی $\mathbb{Q}$ می‌باشد. از آنجا که $p(x)$ از درجهٔ ۳ بوده و ۳ توانی از ۲ نیست، بنابر قضیهٔ ۲.۵.۵، c ترسیم‌پذیر نمی‌باشد. لذا $60°$ را نمی‌توان با ستاره و پرگار تثلیث نمود. این امر به سؤال ۲ جواب منفی خواهد داد.

قضیهٔ ۴.۵.۵. $60°$ را نمی‌توان با ستاره و پرگار تثلیث نمود.

امیدواریم این قضیه خواننده را از الحاق به گروه تثلیث‌گر باز دارد. برای صرف وقت راههای سودمندتر و جالبتری وجود دارد.

مسئلهٔ کلاسیک دیگری از این نوع وجود دارد که جواب آن نیز «منفی» است. این مسئله تربیع دایره می‌باشد. این مسئله چنین است: آیا می‌توان با ستاره و پرگار مربعی رسم کرد که مساحتش مساوی مساحت دایره‌ای به شعاع ۱ باشد؟ این سؤال هم‌ارز آن است که بپرسیم: آیا $\sqrt{\pi}$ یک عدد ترسیم‌پذیر است؟ هرگاه چنین باشد، آن‌گاه چون $(\sqrt{\pi})^2 = \pi$، عدد π نیز ترسیم‌پذیر است. ولی لیندمان در سال ۱۸۸۲ ثابت کرد که π متعالی است. پس π مسلماً جبری نیست؛ و در نتیجه ترسیم‌پذیر نمی‌باشد. لذا تربیع دایره به شعاع ۱ با ستاره و پرگار ممکن نیست.

البته آنچه در بالا شد برهانی از عدم امکان تربیع دایره نیست چرا که نتیجهٔ لیندمان بدون اثبات پذیرفته شده است. اثبات متعالی بودن π ما را از بحث دور می‌سازد. می‌توان انتظار داشت که اثبات ترسیم‌ناپذیری π از اثبات جبری نبودنش آسانتر باشد. این امر ظاهراً چنین نیست زیرا تا به حال تمام برهانها برای ترسیم‌ناپذیری π از راه متعالی بودن π بوده است.

مسائل

۱. برهان قضیهٔ ۱.۵.۵ را کامل کنید.

۲. ثابت کنید $x^3 - 3x - 1$ روی $\mathbb{Q}$ تحویل‌ناپذیر است.

۳. نشان دهید که ترسیم داده شده برای $\sqrt{a}(a \geq 0)$ $\sqrt{a}$ را به‌دست می‌دهد.

۴. ثابت کنید هفت ضلعی منتظم (چندضلعی با هفت ضلع به طول مساوی) با ستاره و پرگار ترسیم‌پذیر نیست.

۶. ریشه‌های چندجمله‌ایها

فرض کنیم $F[x]$ طبق معمول حلقهٔ چندجمله‌ای از x روی میدان F بوده و K یک توسیع میدان F باشد. اگر $a \in K$ و

$$f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$$

منظور از $f(a)$ یعنی عنصر

$$f(a) = \alpha_0 + \alpha_1 a + \cdots + \alpha_n a^n$$

در K. این نماد در سراسر این فصل به‌کار رفته است. حال به aهایی در K توجه داریم که $f(a) = 0$.

تعریف. عنصر $a \in K$ یک ریشهٔ چندجمله‌ای $f(x) \in F[x]$ است اگر $f(a) = 0$.

تا به حال همواره توسیع میدان K از F داده شده است و ما عناصری در K را در نظر گرفته‌ایم که روی F جبری‌اند؛ یعنی عنصرهایی از K که ریشه‌های چندجمله‌ایهای ناصفر در $F[x]$ می‌باشند. دیدیم که هرگاه $a \in K$ روی F جبری از درجهٔ n باشد، یعنی چندجمله‌ای مینیمال a روی F از درجهٔ n باشد، آن‌گاه $[F(a) : F] = n$ که در آن $F(a)$ زیرمیدانی از K است که با الحاق a به F حاصل می‌شود.

حال مسئله را عکس می‌کنیم. ما دیگر توسیع K از F را نداریم. در واقع کار اصلی ما تولید آن است. با چندجمله‌ایی مانند $f(x)$ از درجهٔ مثبت در $F[x]$ به‌عنوان تنها داده شروع می‌کنیم. هدف ترسیم توسیع میدان K از F است که در آن $f(x)$ دارای ریشه باشد. به محض داشتن این K، طبق معمول یک سری نتایج جالب به‌دست می‌آوریم.

پیش از یافتن Kی مناسب باید اطلاعاتی از رابطهٔ ریشه‌های یک چندجمله‌ای و تجزیهٔ آن چندجمله‌ای به‌دست آوریم.

لم ۵.۶.۱. هرگاه $a \in L$ یک ریشهٔ چندجمله‌ای $f(x) \in F[x]$ از درجهٔ n باشد که در آن L توسیع میدان F است، آن‌گاه $f(x)$ در $L(x)$ به‌صورت $f(x) = (x-a)q(x)$ تجزیه می‌شود که در آن $q(x)$ از درجهٔ $n - 1$ در $L[x]$ می‌باشد. به عکس، هرگاه $f(x) = (x-a)q(x)$ که در آن $f(x)$، $q(x)$، و a مثل فوق‌اند، آن‌گاه a یک ریشهٔ $f(x)$ در L می‌باشد.

برهان. چون $F \subset L$، $F[x]$ مشمول $L[x]$ است. و چون $a \in L$، $x-a$ در $L[x]$ است. بنابر الگوریتم تقسیم (قضیهٔ ۵.۵.۴)، برای چندجمله‌ایها در $L[x]$ داریم $f(x) = (x-a)q(x)+r(x)$ که در آن $q(x)$ و $r(x)$ در $L[x]$ بوده و $r(x) = \circ$ یا $\deg r(x) < \deg(x-a) = 1$. از این داریم $r(x) = b$ یعنی عنصری از L. با گذاردن a به‌جای x در رابطهٔ فوق و استفاده از $f(a) = \circ$ به‌دست می‌آوریم $\circ = (a-a)q(a) + b = \circ + b = b$. لذا $b = \circ$. و چون $r(x) = b = \circ$، آنچه می‌خواهیم به‌دست می‌آید؛ یعنی $f(x) = (x-a)q(x)$.

برای حکم $\deg q(x) = n - 1$ توجه می‌کنیم که چون $f(x) = (x-a)q(x)$، بنابر لم ۲.۵.۴، $n = \deg f(x) = \deg(x-a) + \deg q(x) = 1 + \deg q(x)$. از این نتیجهٔ مطلوب، یعنی $\deg q(x) = n - 1$، به‌دست می‌آید.

عکس مطلب کاملاً بدیهی می‌باشد. ■

یک نتیجهٔ فوری از لم ۱.۶.۵ به قرار زیر است.

قضیهٔ ۲.۶.۵. فرض کنیم $f(x)$ در $F[x]$ از درجهٔ n باشد. در این صورت $f(x)$ در هر توسیع K از F می‌تواند حداکثر n ریشه داشته باشد.

برهان. به استقرا بر n عمل می‌کنیم. هرگاه $n = 1$، آن‌گاه $f(x) = ax + b$ که در آن a و b در F بوده و $a \neq \circ$. لذا تنها ریشهٔ $f(x)$ عبارت است از $-b/a$ که عنصری از F است.

فرض کنیم قضیه برای تمام چندجمله‌ایها از درجهٔ $k - 1$ روی هر میدان درست باشد. همچنین $f(x)$ در $F[x]$ از درجهٔ k باشد. هرگاه $f(x)$ ریشه‌ای در K نداشته باشد، آن‌گاه قضیه مسلماً درست است. پس فرض کنیم $a \in K$ ریشه‌ای از $f(x)$ باشد. بنابر لم ۱.۶.۵، $f(x) = (x-a)q(x)$ که در آن $q(x)$ از درجهٔ $k - 1$ در $K[x]$ است. هر ریشهٔ b در K از $f(x)$ یا a است یا ریشه‌ای از $q(x)$ زیرا $\circ = f(b) = (b-a)q(b)$. بنا به فرض استقرا، $q(x)$ حداکثر $k - 1$ ریشه در K دارد. پس $f(x)$ حداکثر k ریشه در K خواهد داشت. این امر استقرا را تمام کرده و قضیه را به ثبوت می‌رساند. ■

برهان فوق در واقع مطلب بیشتری را ثابت می‌کند. برای توضیح این «بیشتر» به مفهوم بستایی یک ریشه نیاز داریم.

تعریف. هرگاه K یک توسیع F باشد، آن‌گاه عنصر a در K یک ریشه با بستایی $k > \circ$ از $f(x)$ است (که $f(x)$ در $F[x]$ است) اگر به ازای $q(x)$ی در $K[x]$، $f(x) = (x-a)^k q(x)$

و $x - a$، $q(x)$ را عاد نکند (یا، معادلاً، $q(a) \neq 0$).

برهانی شبیه برهان قضیهٔ ۲.۶.۵ صورت قویتری از آن را به‌دست می‌دهد:

فرض کنیم $f(x)$ یک چندجمله‌ای از درجهٔ n در $F[x]$ باشد. در این صورت، با احتساب یک ریشه با بستایی k به‌عنوان k ریشه، $f(x)$ می‌تواند حداکثر n ریشه در توسیع میدان K از F داشته باشد.

قضیهٔ ۳.۶.۵. فرض کنیم $f(x)$ در $F[x]$ تکین از درجهٔ n بوده و K توسیعی از F باشد که در آن $f(x)$، با احتساب یک ریشه با بستایی k به‌عنوان k ریشه، دارای n ریشه است. هرگاه این ریشه‌ها در K به‌صورت a_1، a_2، $\cdots$، a_m و هر یک به‌ترتیب با بستایی k_1، k_2، $\cdots$، k_m باشند، آن‌گاه $f(x)$ در $K[x]$ به‌صورت $f(x) = (x-a_1)^{k_1}(x-a_2)^{k_2}\cdots(x-a_m)^{k_m}$ تجزیه می‌شود.

برهان. برهان با استفاده از لم ۱.۶.۵ و استقرا روی n آسان است. بیان کامل آن را به خواننده وامی‌گذاریم. ■

تعریف. گوییم $f(x)$ در $F[x]$ به عوامل خطی روی (یا در) K تجزیه می‌شود اگر $f(x)$ در $K[x]$ تجزیهٔ مذکور در قضیهٔ ۳.۶.۵ را داشته باشد.

قضیهٔ ۳.۶.۵ کاربرد زیبایی در میدانهای متناهی دارد. فرض کنیم میدان متناهی F دارای q عنصر بوده و a_1، a_2، $\cdots$، a_{q-1} عناصر ناصفر آن باشند. چون این عنصرها تحت ضرب در F یک گروه از مرتبهٔ $q-1$ تشکیل می‌دهند، بنابر قضیهٔ ۵.۴.۲ (که خیلی وقت پیش ثابت شد) به ازای هر $a \neq 0$ در F، $a^{q-1} = 1$. لذا چندجمله‌ای $x^{q-1} - 1$ در $F[x]$ دارای $q-1$ ریشهٔ متمایز در F است. بنابر قضیهٔ ۳.۶.۵، $x^{q-1} - 1 = (x-a_1)(x-a_2)\cdots(x-a_{q-1})$. هرگاه 0 را نیز در نظر بگیریم، آن‌گاه هر عنصر a در F در $a^q = a$ صدق می‌کند؛ در نتیجه چندجمله‌ای $x^q - x$، q عنصر F را به‌عنوان ریشه‌های متمایز خود دارد. پس از قضیهٔ ۳.۶.۵ داریم:

قضیهٔ ۴.۶.۵. فرض کنیم F یک میدان متناهی با q عنصر باشد. در این صورت $x^q - x$ در $F[x]$ به‌صورت زیر تجزیه می‌شود:

$$x^q - x = x(x-a_1)(x-a_2)\cdots(x-a_{q-1})$$

که در آن a_1، a_2، $\cdots$، a_{q-1} عناصر ناصفر Fاند، و

$$x^{q-1} - 1 = (x - a_1)(x - a_2) \cdots (x - a_{q-1})$$

در یک حالت بسیار خاص داریم $F = \mathbb{Z}_p$ یعنی اعداد صحیح به پیمانهٔ عدد اول p. در اینجا $q = p$ و a_1، a_2، $\cdots$، a_{p-1} همان ۱، ۲، $\cdots$، $p-1$اند با ترتیبی خاص. لذا خواهیم داشت:

نتیجه. $x^{p-1} - 1$ در $\mathbb{Z}_p[x]$ به‌صورت زیر تجزیه می‌شود:

$$x^{p-1} - 1 = (x - 1)(x - 2) \cdots (x - (p-1))$$

این مطلب را به ازای p مساوی ۵، ۷، و ۱۱ توضیح دهید.

به‌عنوان نتیجه‌ای از مطلب فوق، نتیجه‌ای در نظریهٔ اعداد به‌دست می‌آوریم به نام قضیهٔ ویلسون که در مسئلهٔ ۱۸ در بخش ۴ از فصل ۲ ذکر شده است.

نتیجه. هرگاه p اول باشد، آن‌گاه $(p-1)! \equiv -1 \mod p$.

برهان. بنابر نتیجهٔ فوق،

$$x^{p-1} - 1 = (x - 1)(x - 2) \cdots (x - (p-1))$$

با گذاردن $x = 0$ در این رابطه داریم

$$\begin{aligned} -1 &= (-1)(-2) \cdots (-(p-1)) = (-1)^{p-1} 1 \cdot 2 \cdots (p-1) \\ &= (-1)^{p-1}(p-1)! \end{aligned}$$

در $\mathbb{Z}_p$. این در اعداد صحیح $\mod p$ به‌صورت زیر در می‌آید:

$$(-1)^{p-1}(p-1)! \equiv -1 \mod p$$

و در نتیجه $(p-1)! \equiv (-1)^p \mod p$. ولی $(-1)^p \equiv -1 \mod p$. پس قضیهٔ ویلسون به ثبوت خواهد رسید. ■

حال جهت بحث را عوض کرده و مسئلهٔ مذکور در آغاز این بخش را در نظر می‌گیریم: به ازای $f(x) \in F[x]$ توسیع متناهی K از F را طوری می‌سازیم که در آن $f(x)$ ریشه داشته

باشد. همان‌طور که لحظه‌ای بعد خواهید دید، اگر نتایج مربوط به حلقه‌های چندجمله‌ای را که در فصل ۴ ثابت شده‌اند وارد کار کنیم، ساختن K ساده خواهد شد. با این حال اثبات امکان‌پذیر بودن این کار کمی زحمت دارد.

قضیهٔ ۵.۶.۵. فرض کنیم F یک میدان بوده و $f(x)$ یک چندجمله‌ای از درجهٔ مثبت n در $F[x]$ باشد. در این صورت یک توسیع متناهی مانند K از F وجود دارد که $[K:F] \le n$ و در آن $f(x)$ دارای ریشه می‌باشد.

برهان. بنابر قضیهٔ ۱۲.۵.۴، $f(x)$ در $F[x]$ بر یک چندجمله‌ای تحویل‌ناپذیر مانند $p(x)$ در $F[x]$ بخشپذیر است. چون $p(x)$، $f(x)$ را عاد می‌کند، به ازای یک چندجمله‌ای مانند $q(x)$ در $F[x]$، $\deg p(x) \le \deg f(x) = n$ و $f(x) = p(x)q(x)$. هرگاه b ریشه‌ای از $p(x)$ در یک توسیع میدان باشد، آن‌گاه b خودبه‌خود یک ریشهٔ $f(x)$ است زیرا $f(b) = p(b)q(b) = \circ q(b) = \circ$. لذا برای اثبات قضیه کافی است یک توسیع از F بیابیم که در آن $p(x)$ ریشه داشته باشد.

چون $p(x)$ در $F[x]$ تحویل‌ناپذیر است، بنابر قضیهٔ ۱۱.۵.۴ ایده‌آل $M = (p(x))$ تولید شده به‌وسیلهٔ $p(x)$ در $F[x]$ یک ایده‌آل ماکزیمال $F[x]$ است. لذا، طبق قضیهٔ ۲.۴.۴، $K = F[x]/M$ یک میدان می‌باشد. حکم می‌کنیم که این میدان مطلوب ما می‌باشد.

به بیان دقیق، K شامل F نیست. ولی، همان‌طور که اینک نشان می‌دهیم، K شامل میدانی یکریخت با F است. چون هر عنصر در M مضربی از $p(x)$ در $F[x]$ است، هر چنین عنصر ناصفر باید درجه‌ای دست‌کم از درجهٔ $p(x)$ داشته باشد. لذا $M \cap F = (\circ)$. بنابراین همریختی $\psi : F[x] \to K$ با تعریف $\psi(g(x)) = g(x) + M$ به ازای هر $g(x)$ در $F[x]$ در تحدید به F بر F یک به یک است. بنابراین نقش $\bar{\mathbf{F}}$ از F در K میدانی یکریخت با F می‌باشد. $\bar{\mathbf{F}}$ را می‌توان به‌وسیلهٔ ψ با F یکی کرد و در نتیجه، بدین‌طریق، K را توسیعی از F گرفت.

$x + M \in K$ را با a نشان می‌دهیم؛ در نتیجه به ازای $a \in K$، $\psi(x) = a$. بر خواننده است نشان دهد که چون ψ یک همریختی از $F[x]$ به روی K با هستهٔ M است، به ازای هر $g(x)$ در $F[x]$، $\psi(g(x)) = g(a)$. $\psi(p(x))$ چیست؟ از یک‌سو، چون $p(x)$ در $F[x]$ است، $\psi(p(x)) = p(a)$. و از سوی دیگر، چون $p(x)$ در M، یعنی هستهٔ ψ، است، $\psi(p(x)) = \circ$. با متحد گرفتن این دو مقدار برای $\psi(p(x))$ به‌دست می‌آوریم $p(a) = \circ$. به عبارت دیگر، عنصر $a = \psi(x)$ در K ریشهٔ $p(x)$ می‌باشد.

برای اتمام برهان کافی است نشان دهیم که $[K:F] = \deg p(x) \le n$. این امر قبلاً در

برهان دیگری که برای قضیهٔ ۵.۳.۵ داده شد آمده است. در آنجا اثبات این مطلب به خواننده محول شد. ما در اینجا سخاوت به خرج داده و آن را به تفصیل ثابت می‌کنیم.

هرگاه $h(x)$ در $F[x]$ باشد، آن‌گاه، بنابر الگوریتم تقسیم، $h(x) = p(x)q(x) + r(x)$ که در آن $q(x)$ و $r(x)$ در $F[x]$اند و $r(x) = 0$ یا $\deg r(x) < \deg p(x)$. با استفاده از پیمانهٔ M داریم

$$\begin{aligned}\psi(h(x)) = \psi(p(x)q(x) + r(x)) &= \psi(p(x)q(x)) + \psi(r(x))\\ &= \psi(p(x))\psi(q(x)) + \psi(r(x))\\ &= \psi(r(x)) = r(a)\end{aligned}$$

[زیرا $\psi(p(x)) = p(a) = 0$].

لذا چون هر عنصر در $K = F[x]/M$ مساوی $\psi(h(x))$ به ازای $h(x)$ی در $F[x]$ است و $\psi(h(x)) = r(a)$، معلوم می‌شود که هر عنصر از K به شکل $r(a)$ است که در آن $r(x)$ در $F[x]$ بوده و $\deg r(x) < \deg p(x)$. اگر $\deg p(x) = m$، بحثی که هم‌اکنون شد به ما می‌گوید که ۱، a، a^2، …، a^{m-1}، K را روی F می‌پیمایند. به‌علاوه این عناصر مستقل خطی روی Fاند زیرا هر رابطه به شکل $\alpha_0 + \alpha_1 a + \cdots + \alpha_{m-1}a^{m-1} = 0$ ایجاب می‌کند که $g(a) = 0$ که در آن $g(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{m-1}x^{m-1}$ در $F[x]$ است. این امر $g(x)$ را در M می‌گذارد که ناممکن است زیرا $g(x)$ از درجهٔ کمتر از درجهٔ $p(x)$ می‌باشد مگر آنکه $g(x) = 0$. به عبارت دیگر، تناقض داریم مگر آنکه $\alpha_0 = \alpha_1 = \cdots = \alpha_{m-1} = 0$.

لذا عناصر ۱، a، a^2، …، a^{m-1} مستقل خطی روی Fاند. چون این عناصر K را روی F می‌پیمایند، یک پایه از K روی F تشکیل می‌دهند. در نتیجه

$$\dim_F K = [K : F] = m = \deg p(x) \le n = \deg f(x)$$

و قضیه به ثبوت می‌رسد. ■

استدلال به‌کار رفته در برهان اخیر را تکرار کرده و قضیهٔ مهم زیر را ثابت می‌کنیم.

قضیهٔ ۶.۶.۵. فرض کنیم $f(x) \in F[x]$ از درجهٔ n باشد. در این صورت توسیعی مانند K از F از درجهٔ حداکثر $n!$ روی F هست به‌طوری که $f(x)$ دارای n ریشه (با احتساب بستاییها) در K است. به بیان معادل، $f(x)$ به عوامل خطی روی K تجزیه می‌شود.

برهان. به استقرا روی n عمل می‌کنیم. هرگاه $n = ۱$، آن‌گاه $f(x) = \alpha + \beta x$ که در آن $\alpha, \beta \in F$ و $\beta \neq ۰$. تنها ریشهٔ $f(x)$ عبارت است از $-\alpha/\beta$ که در F است. لذا $K = F$ و $[K : F] = ۱$.

فرض کنیم نتیجه در تمام میدانها برای چندجمله‌ایها از درجهٔ k درست باشد و $f(x) \in F[x]$ از درجهٔ $k + ۱$ باشد. بنابر قضیهٔ ۵.۶.۵، توسیعی مانند $K_۱$ از F هست که $[K_۱ : F] \leq k + ۱$ و در آن $f(x)$ دارای ریشهٔ $a_۱$ است. لذا، در $K_۱[x]$، $f(x)$ به‌صورت $f(x) = (x - a_۱)q(x)$ تجزیه می‌شود که در آن $q(x) \in K_۱[x]$ از درجهٔ k است. بنابه فرض استقرا، توسیعی مانند K از $K_۱$ از درجهٔ حداکثر $k!$ روی $K_۱$ هست که $q(x)$ در آن به عوامل خطی تجزیه می‌شود. ولی در این صورت $f(x)$ به عوامل خطی روی K تجزیه می‌شود. چون

$$[K : F] = [K : K_۱][K_۱ : K] \leq (k + ۱)k! = (k + ۱)!$$

استقرا کامل شده و قضیه به ثبوت می‌رسد. ■

در اینجا توسیع میدانها را ترک می‌کنیم. ما درست در آغاز نظریهٔ گالوا هستیم. با داشتن توسیع K از F از درجهٔ متناهی که رویش چندجمله‌ای $f(x)$ به عوامل خطی تجزیه می‌شود، توسیعی با کمترین درجه و واجد این خاصیت وجود دارد. این نوع توسیع را میدان تجزیه‌گر $f(x)$ روی F می‌نامند. می‌توان ثابت کرد که میدان تجزیه‌گر با تقریب یکریختی منحصر به فرد است. با داشتن این نتیجه، نظریهٔ گالوا چرخش کامل یافته و رابطهٔ بین گروه خودریختیهای این میدان تجزیه‌گر و ساختار زیرمیدانی‌اش را مطالعه خواهد کرد. این امر مالاً به آنجا می‌رسد که از جمله چیزهای دیگر نشان دهیم که چندجمله‌ایهایی روی اعداد گویا از درجهٔ ۵ یا بیشتر وجود دارند که ریشه‌هایشان را نمی‌توان برحسب ضرایب این چندجمله‌ایها به طرزی زیبا بیان کرد.

این توصیفی است کوتاه و بسیار خام از کاری که می‌توان در نظریهٔ میدانها ادامه داد. ولی شتابی در کار نیست. خواننده بهتر است مطالبی را که ارائه شد تحلیل نماید. این امر وی را برای آموختن نظریهٔ گالوا در صورت داشتن تمایل مهیا می‌سازد.

مسائل

۱. قضیهٔ ۳.۶.۵ را ثابت کنید.

۲. اگر F یک میدان متناهی با $q - ۱$ عنصر ناصفر $a_۱$، $a_۲$، $\cdots$، $a_{q-۱}$ باشد، ثابت کنید $a_۱ a_۲ \cdots a_{q-۱} = (-۱)^q$.

۳. فرض کنید $\mathbb{Q}$ میدان گویا بوده و $p(x) = x^4 + x^3 + x^2 + x + 1$. نشان دهید که توسیعی از $\mathbb{Q}$ مانند K هست که $[K : \mathbb{Q}] = 4$ و $p(x)$ رویش به عوامل خطی تجزیه می‌شود. [راهنمایی. ریشه‌های $p(x)$ را بیابید.]

۴. اگر $q(x) = x^n + a_1x^{n-1} + \cdots + a_n$، $(a_n \neq 0)$ یک چندجمله‌ای با ضرایب صحیح بوده و عدد گویای r ریشهٔ $q(x)$ باشد، ثابت کنید r یک عدد صحیح بوده و $r | a_n$.

۵. نشان دهید که $q(x) = x^3 - 7x + 11$ روی $\mathbb{Q}(x)$ تحویل‌ناپذیر است.

۶. اگر F میدانی از مشخص $p \neq 0$ باشد، نشان دهید که به ازای هر a و b در F، $(a + b)^p = a^p + b^p$.

۷. مسئلهٔ ۶ را با نشان دادن اینکه $(a + b)^m = a^m + b^m$ که در آن $m = p^n$ تعمیم دهید.

۸. فرض کنید $F = \mathbb{Z}_p$ که در آن p اول است و چندجمله‌ای $x^m - x$ را در $\mathbb{Z}_p[x]$ در نظر بگیرید که در آن $m = p^n$. همچنین K یک توسیع متناهی از $\mathbb{Z}_p$ باشد که $x^m - x$ رویش به عوامل خطی تجزیه می‌شود. در K فرض کنید $K.$ مجموعهٔ تمام ریشه‌های $x^m - x$ باشد و نشان دهید که $K.$ میدانی با حداکثر p^n عنصر می‌باشد.

۹. در مسئلهٔ ۸ نشان دهید که $K.$ درست p^n عنصر دارد. (راهنمایی. ر.ک. مسئلهٔ ۱۴.)

۱۰. توسیع میدان K_n از $\mathbb{Q}$ را چنان بسازید که به ازای هر $n \geq 1$، $[K_n : \mathbb{Q}] = n$.

۱۱. نگاشت $\delta : F[x] \to F[x]$ را با

$$\delta(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)$$
$$= a_1 + 2a_2x + \cdots + ia_ix^{i-1} + \cdots + na_nx^{n-1}$$

تعریف و ثابت کنید که به ازای هر $f(x)$ و $g(x)$ در $F[x]$،

الف) $\delta(f(x) + g(x)) = \delta(f(x)) + \delta(g(x))$؛

ب) $\delta(f(x)g(x)) = f(x)\delta(g(x)) + \delta(f(x))g(x)$.

۱۲. اگر F از مشخص $p \neq 0$ باشد، تمام $f(x)$هایی را در $F[x]$ توصیف کنید که $\delta(f(x)) = 0$.

۱۳. نشان دهید هرگاه $f(x)$ در $F[x]$ ریشه‌ای با بستایی بزرگتر از ۱ در توسیع میدانی از F داشته باشد، آن‌گاه $f(x)$ و $\delta(f(x))$ در $F[x]$ نسبت به هم اول نیستند.

۱۴. اگر F از مشخص $p \neq 0$ باشد، نشان دهید که جمیع ریشه‌های $x^m - x$ که در آن $m = p^n$ متمایزند.

۱۵. اگر $f(x)$ در $F[x]$ تحویل‌ناپذیر بوده و در توسیعی از F ریشه‌ای با بستایی بزرگتر از ۱ داشته باشد، نشان دهید که

الف) F باید به ازای عدد اولی چون p از مشخص p باشد؛

ب) به ازای چندجمله‌ایی مانند $g(x)$ در $F[x]$، $f(x) = g(x^p)$.

۶

مباحث ویژه (اختیاری)

در این فصل نهایی به چند مطلب جدا از هم می‌پردازیم. یکی از آنها از نظریهٔ گروهها و بقیه از نظریهٔ میدانها می‌باشند. در این مباحث ویژه از بسیاری نتایج و ایده‌هایی که قبلاً در کتاب آمده استفاده می‌کنیم. با آنکه این مباحث به نوعی خاص‌اند، هر یک از نتایجی برخوردارند که در خطهٔ خود واقعاً اهمیت دارند.

خواننده‌ای که تا به‌حال طاقت آورده است باید چند روش، کمی تجربه، و اطلاعاتی جبری به‌دست آورده باشد تا بتواند مطالب را به سادگی تعقیب نماید. ما اکنون در بررسی مطالب به‌طور خلاصه‌تر از سابق و سپردن جزئیات به خواننده احساس آزادی بیشتری داریم.

مطالبی که مطرح می‌کنیم به آسانی تسلیم مسائل، دست‌کم آنهایی که خیلی مشکل باشند، نمی‌شوند. لذا تعداد نسبتاً کمی تمرین خواهیم آورد. این امر به افرادی که بخواهند مطالب این فصل را تحلیل کنند آرامش خواهد بخشید.

۱. ساده بودن A_n

در فصل ۳ که S_n، یعنی گروه متقارن از درجهٔ n، را مطرح ساختیم نشان دادیم که اگر $n \geq ۲$، S_n زیرگروه نرمالی مانند A_n به نام گروه متناوب از درجهٔ n دارد که گروهی است از مرتبهٔ $n!/۲$. A_n در واقع مجموعهٔ تمام جایگشتهای زوج در S_n است.

در بحث A_n گفتیم که A_n به ازای $n \geq ۵$ یک گروه ساده است؛ یعنی A_n زیرگروه نرمالی

جز (e) و خود ندارد. در آنجا قول دادیم که این امر را در فصل ۶ ثابت خواهیم کرد. حال به این قول وفا می‌کنیم.

برای توضیح مطلبی که می‌خواهیم ثابت کنیم باید آنچه را که در بالا گفتیم تکرار کرده و گروه ساده را به‌طور صوری تعریف نماییم.

تعریف. گوییم یک گروه غیرآبلی ساده است اگر تنها زیرگروههای نرمالش (e) و خودش باشد.

ما شرط غیرآبلی را بر G به این دلیل می‌گذاریم که حالات بدیهی گروههای دوری از مرتبهٔ عددی اول را از «ساده بودن» خارج کنیم. گروههای دوری از مرتبهٔ عددی اول زیرگروه غیربدیهی ندارند. لذا، به ناچار، زیرگروه نرمال حقیقی نخواهند داشت. به آسانی معلوم می‌شود که یک گروه آبلی بدون زیرگروه حقیقی دوری از مرتبهٔ عددی اول می‌باشد.

بحث را با لم بسیار سادهٔ زیر شروع می‌کنیم.

لم ۶.۱.۱. هرگاه $n \geq ۳$ و $\tau_۱$ و $\tau_۲$ دو ترانهش در S_n باشند، آن‌گاه $\tau_۱\tau_۲$ یک ۳ـدور یا حاصلضربی از دو ۳ـدور می‌باشد.

برهان. هرگاه $\tau_۱ = \tau_۲$، آن‌گاه $\tau_۱\tau_۲ = \tau_۱^۲ = e$ و e مسلماً حاصلضربی از دو ۳ـدور است، مثلاً به‌صورت $e = (۱۲۳)(۱۳۲)$.

هرگاه $\tau_۱ \neq \tau_۲$، آن‌گاه یا حرف مشترکی دارند یا ندارند. اگر یک حرف مشترک داشته باشند، می‌توان با شماره‌گذاری مناسب فرض کرد که $\tau_۱ = (۱۲)$ و $\tau_۲ = (۱۳)$. ولی در این صورت $\tau_۱\tau_۲ = (۱۲)(۱۳) = (۱۳۲)$ یک ۳ـدور است.

بالاخره اگر $\tau_۱$ و $\tau_۲$ حرف مشترک نداشته باشند، می‌توان بدون ضایع ساختن کلیت فرض کرد $\tau_۱ = (۱۲)$ و $\tau_۲ = (۳۴)$، که در این حالت $\tau_۱\tau_۲ = (۱۲)(۳۴) = (۱۴۲)(۱۴۳)$ که در واقع حاصلضرب دو ۳ـدور است و لم ثابت می‌شود. ■

یک نتیجهٔ فوری از لم ۶.۱.۱ این است که به ازای $n \geq ۳$، ۳ـدورها A_n، یعنی گروه متناوب از درجهٔ n، را تولید می‌کنند.

قضیهٔ ۶.۱.۲. هرگاه σ یک جایگشت زوج در S_n باشد که $n \geq ۳$، آن‌گاه σ حاصلضرب ۳ـدورهاست. به عبارت دیگر، ۳ـدورها در S_n، A_n را تولید می‌کنند.

برهان. فرض کنیم $\sigma \in S_n$ یک جایگشت زوج باشد. بنا بر تعریف جفتی یک جایگشت، σ حاصلضرب تعدادی زوج ترانهش است. لذا $\sigma = \tau_۱\tau_۲\cdots\tau_{۲i-۱}\tau_{۲i}\cdots\tau_{۲m-۱}\tau_{۲m}$ حاصلضرب

$2m$ ترانهش $\tau_1, \tau_2, \cdots, \tau_{2m}$ است. بنا بر لم ۶.۱.۱، هر $\tau_{2i-1}\tau_{2i}$ یک ۳ـدور است یا حاصلضربی از دو ۳ـدور. لذا σ یا یک ۳ـدور است یا حاصلضرب حداکثر $2m$ تا ۳ـدور. این امر قضیه را به ثبوت می‌رساند. ■

حال برای محاسبهٔ مزدوج یک جایگشت در S_n الگوریتمی ارائه می‌دهیم. فرض کنیم $\sigma \in S_n$ و $\sigma(i) = j$. اگر $\tau \in S_n$، $\tau\sigma\tau^{-1}$ چه شکلی است؟ فرض کنیم $\tau(i) = s$ و $\tau(j) = t$. پس $\tau\sigma\tau^{-1}(s) = \tau\sigma(\tau^{-1}(s)) = \tau\sigma(i) = \tau(j) = t$. به عبارت دیگر، برای محاسبهٔ $\tau\sigma\tau^{-1}$ هر علامت در σ را با نقشش تحت τ عوض می‌کنیم.

مثلاً هرگاه $\sigma = (۱۲۳)$ و $\tau = (۱۴۳)$، آن‌گاه، چون $\tau(۱) = ۴$، $\tau(۲) = ۲$، $\tau(۳) = ۱$، و $\tau(۴) = ۳$، می‌بینیم که $\tau\sigma\tau^{-1} = (۴۲۱) = (۱۴۲)$.

هر دو kـدور $(۱\ ۲ \cdots k)$ و $(i_1\ i_2 \cdots i_k)$ در S_n مزدوج‌اند زیرا هرگاه جایگشت τ عدد ۱ را به i_1، ۲ را به i_2، $\cdots$، k را به i_k بفرستد، آن‌گاه $\tau(۱\ ۲ \cdots k)\tau^{-1} = (i_1 i_2 \cdots i_k)$. چون هر جایگشت حاصلضربی از دورهای از هم جداست و تزویج یک خودریختی است، از نتیجهٔ مربوط به kـدورها معلوم می‌شود که برای محاسبهٔ $\tau\sigma\tau^{-1}$ به ازای هر جایگشت σ، هر علامت در σ را با نقشش تحت τ عوض می‌کنیم. پس به آسانی می‌توان مزدوج یک جایگشت را حساب کرد.

هرگاه σ_1 و σ_2 دو جایگشت در S_n باشند، آن‌گاه، با استفاده از ملاحظات فوق، این دو جایگشت مزدوج‌اند اگر در تجزیه‌شان به حاصلضربهای دورهای از هم‌جدا دارای طولهای دوری مساوی بوده و همهٔ طولهای دوری بستایی یکسانی داشته باشند. مثلاً $(۵۶۷)(۳۴)(۱۲)$ و $(۵۶۸)(۲۴)(۳۷)$ در S_8 مزدوج‌اند ولی $(۵۶۷)(۳۴)(۱۲)$ و $(۵۶۸)(۳۷)$ چنین نیستند.

به یاد آورید که یک افراز عدد صحیح مثبت n یعنی تجزیهٔ n به‌صورت $n = n_1 + n_2 + \cdots + n_k$ که در آن $0 \le n_1 \le n_2 \le \cdots \le n_k$. هرگاه σ در S_n حاصلضرب از هم‌جدای یک n_1ـدور، یک n_2ـدور، $\cdots$، یک n_kـدور باشد، آن‌گاه $n = n_1 + n_2 + \cdots + n_k$ و جایگشت τ مزدوج σ است اگر و فقط اگر τ حاصلضرب از هم‌جدای دورها به همین نحو باشد. لذا تعداد رده‌های تزویج در S_n مساوی تعداد افرازهای n می‌باشد.

مثلاً هرگاه $n = ۴$، آن‌گاه افرازهای ۴ عبارتند از $۴ = ۴$، $۴ = ۱ + ۳$، $۴ = ۱ + ۱ + ۲$، $۴ = ۱ + ۱ + ۱ + ۱$، و $۴ = ۲ + ۲$ که پنج تایند. لذا S_4 دارای پنج ردهٔ تزویج است که عبارتند از رده‌های (۱۲۳۴)، (۱۲۳)، (۱۲)، e، و $(۳۴)(۱۲)$.

ما مطالب مذکور در فوق را در سه حکم مختلف بیان می‌کنیم.

لم ۳.۱.۶. برای یافتن $\tau\sigma\tau^{-۱}$ در S_n هر علامت در σ را با نقشش تحت τ عوض می‌کنیم.

لم ۴.۱.۶. دو عنصر در S_n مزدوج‌اند اگر در حاصلضرب به‌صورت دورهای از هم‌جدا تجزیه‌های مشابهی داشته باشند.

لم ۵.۱.۶. تعداد رده‌های تزویج در S_n مساوی تعداد افرازهای n می‌باشد.

از نتایج فوق واضح است که هر دو ۳ـدور در S_n در S_n مزدوج‌اند. هر ۳ـدور یک جایگشت زوج است؛ پس در A_n است. ممکن است بپرسیم که آیا هر دو ۳ـدور در گروه کوچکتر A_n مزدوج‌اند یا نه. جواب به ازای $n \geq ۵$ «مثبت» بوده و به آسانی ثابت می‌شود:

لم ۶.۱.۶. هرگاه $n \geq ۵$، آن‌گاه هر دو ۳ـدور در S_n در A_n مزدوج می‌باشند.

برهان. فرض کنیم $\sigma_۱$ و $\sigma_۲$ دو ۳ـدور در S_n باشند. بنا بر لم ۴.۱.۶، این دورها در S_n مزدوج‌اند. با شماره‌گذاری مجدد می‌توان فرض کرد که به ازای $\tau \in S_n$ای، $\sigma_۱ = (۱۲۳)$ و $\sigma_۲ = \tau(۱۲۳)\tau^{-۱}$. هرگاه τ زوج باشد، آن‌گاه کار تمام است. هرگاه τ فرد باشد، آن‌گاه $\rho = \tau(۴۵)$ زوج است و

$$\rho(۱۲۳)\rho^{-۱} = \tau(۴۵)(۱۲۳)(۴۵)^{-۱}\tau^{-۱} = \tau(۱۲۳)\tau^{-۱} = \sigma_۲$$

لذا $\sigma_۱$ و $\sigma_۲$ در A_n مزدوج می‌باشند. پس لم درست خواهد بود. ■

در $S_۳$ دو ۳ـدور (۱۲۳) و (۱۳۲) در $S_۳$ مزدوج‌اند ولی در $A_۳$، که گروه دوری از مرتبهٔ ۳ است، مزدوج نیستند.

حال نتیجه‌ای را ثابت می‌کنیم که نه فقط در نظریهٔ گروهها مهم است بلکه در نظریهٔ میدانها و نظریهٔ معادلات نیز نقشی کلیدی دارد.

قضیهٔ ۷.۱.۶. هرگاه $n \geq ۵$، آن‌گاه تنها زیرگروه نرمال حقیقی غیربدیهی از S_n عبارت است از A_n.

برهان. فرض کنیم N یک زیرگروه نرمال S_n بوده و N نه (e) باشد نه S_n. فرض کنیم $\sigma \neq e$ در N باشد. چون مرکز S_n مساوی (e) است (ر.ک. مسئلهٔ ۱) و ترانهشها S_n را تولید

می‌کنند، یک ترانهش مانند τ هست که $\sigma\tau \neq \tau\sigma$. بنا بر لم ۴.۱.۶، $\tau_۱ = \sigma\tau\sigma^{-۱}$ یک ترانهش است؛ در نتیجه $\tau\tau_۱ = \tau\sigma\tau\sigma^{-۱} \neq e$ در N است زیرا $\sigma \in N$ و $\tau\sigma\tau = \tau\sigma\tau^{-۱} \in N$ چون که N در S_n نرمال است. لذا N شامل عنصری است که حاصلضرب دو ترانهش یعنی $\tau\tau_۱$ می‌باشد.

هرگاه τ و $\tau_۱$ یک حرف مشترک داشته باشند، آن‌گاه، همان‌طور که در برهان لم ۱.۱.۶ دیدیم، $\tau\tau_۱$ یک ۳ـدور است. لذا N شامل یک ۳ـدور می‌باشد. بنا بر لم ۴.۱.۶، تمام ۳ـدورها در S_n مزدوج $\tau\tau_۱$اند. پس بنا بر نرمال بودن N در S_n، باید در N باشند. لذا زیرگروه S_n تولید شده به‌وسیلهٔ ۳ـدورها، که بنا بر قضیهٔ ۲.۱.۶ تمام A_n است، در N قرار دارد. توجه کنید که تا اینجا از $n \geq ۵$ استفاده نکرده‌ایم.

لذا می‌توان فرض کرد که τ و $\tau_۱$ حرف مشترکی ندارند. بی‌آنکه به کلیت خللی وارد شود می‌توان فرض کرد که $\tau = (۱۲)$ و $\tau_۱ = (۳۴)$. لذا $(۱۲)(۳۴)$ در N است. چون $n \geq ۵$، (۱۵) در S_n است. پس $(۱۵)(۱۲)(۳۴)(۱۵)^{-۱} = (۳۴)(۲۵)$ نیز در N است. لذا $(۱۲)(۳۴)(۲۵)(۳۴) = (۱۲۵)$ در N می‌باشد. پس در این حالت نیز N باید شامل یک ۳ـدور باشد. لذا استدلال فوق نشان می‌دهد که $N \supset A_n$.

پس در هر دو حالت نشان داده‌ایم که N باید شامل A_n باشد. چون بین A_n و S_n اکیداً زیرگروهی نیست و $N \neq S_n$، نتیجهٔ مطلوب $N = A_n$ به‌دست می‌آید. ■

نتیجه به ازای $n = ۴$ درست نیست؛ زیرگروه

$$N = \{e, (۱۲)(۳۴), (۱۳)(۲۴), (۱۴)(۲۳)\}$$

یک زیرگروه نرمال حقیقی $S_۴$ است و مساوی $A_۴$ نیست.

حال تمام زیرگروههای نرمال S_n را وقتی $n \geq ۵$ می‌دانیم. آیا با استفاده از این می‌توان تمام زیرگروههای نرمال A_n را به ازای $n \geq ۵$ تعیین کرد؟ پاسخ «مثبت» است و به‌زودی خواهیم دید که اگر $n \geq ۵$، A_n یک گروه ساده می‌باشد. برهان ممکن است به نظر بسیاری عجیب باشد، زیرا بر این مبتنی است که ۶۰، یعنی مرتبهٔ $A_۵$، مجذور کامل نمی‌باشد.

قضیهٔ ۸.۱.۶. گروه $A_۵$ یک گروه ساده از مرتبهٔ ۶۰ است.

برهان. فرض کنیم $A_۵$ ساده نباشد. پس دارای زیرگروه نرمال حقیقی N است که مرتبه‌اش حتی‌الامکان کوچک است. فرض کنیم $T = \{\sigma \in S_۵ | \sigma N \sigma^{-۱} \subset N\}$ که نرمال‌ساز N در $S_۵$ است. چون N در $A_۵$ نرمال است، $T \supset A_۵$. T زیرگروه $S_۵$ است. پس اگر $T \neq A_۵$،

داریم $T = S_5$. ولی این به ما می‌گوید که N در S_5 نرمال است که، بنا بر قضیهٔ ۷.۱.۶، ایجاب می‌کند که $A_5 \supset N$ که به ما $N = A_5$ را می‌دهد که با این فرض که N زیرگروه حقیقی A_5 است در تضاد می‌باشد. لذا باید داشته باشیم $T = A_5$. چون (۱۲) فرد است، در A_5 نیست؛ لذا در T نمی‌باشد. بنا براین $M = (12)N(12)^{-1} \neq N$.

چون $N \triangleleft A_5$، نیز داریم $M \triangleleft A_5$ (ثابت کنید!). لذا $M \cap N$ و $MN = \{mn | n \in N ، m \in M\}$ هر دو در A_5 نرمال‌اند. (ر.ک. مسئلهٔ ۹.) چون $M \neq N$، داریم $M \cap N \neq N$، و چون N زیرگروه نرمال حقیقی مینیمال A_5 است، پس $M \cap N = (e)$. از آن‌سو، بنا بر نرمال بودن M و N در A_5،

$$(12)MN(12)^{-1} = (12)M(12)^{-1}(12)N(12)^{-1} = NM$$

$= MN$ (چون $M = (12)N(12)^{-1}$ و $N = (12)M(12)^{-1}$).

لذا عنصر (۱۲) در نرمال‌ساز MN در S_5 است، و چون MN در A_5 نرمال است، همانند فوق معلوم می‌شود که MN در S_5 نرمال است و در نتیجه، بنا بر قضیهٔ ۷.۱.۶، $MN = A_5$.

حال به آنچه داریم توجه می‌کنیم. M و N زیرگروههای نرمالی از A_5اند، هر یک از مرتبهٔ $|N|$ بوده و $MN = A_5$ و $M \cap N = (e)$. حکم می‌کنیم و به خواننده وامی‌گذاریم که MN باید از مرتبهٔ $|N|^2$ باشد. چون $MN = A_5$، داریم $|N|^2 = |MN| = |A_5| = 60$. ولی این امری است محال زیرا ۶۰ مجذور هیچ عدد صحیح نیست. این مطلب قضیهٔ ۸.۱.۶ را ثابت خواهد کرد. ■

استنتاج ساده بودن A_n به ازای $n \geq 5$ از ساده بودن A_5 خیلی سخت نیست. توجه کنید که استدلال مذکور برای A_n تا جایی که گفتیم «۶۰ مجذور هیچ عدد صحیح نیست» تابع ۵ نبود. در واقع استدلال تا جایی که بدانیم $n!/2$ مجذور کامل نیست معتبر است. مثلاً هرگاه $n = 6$، آن‌گاه $6!/2 = 360$ مجذور کامل نیست. پس A_6 یک گروه ساده می‌باشد. چون این امر در آینده لازم می‌شود، پیش از ادامهٔ بحث آن را ثبت می‌کنیم.

نتیجهٔ برهان قضیهٔ ۸.۱.۶. A_6 یک گروه ساده می‌باشد.

حال به این مسئله که $n!/2$ مجذور است یا نه باز می‌گردیم. در واقع اگر $n > 2$، چنین نیست. این را می‌توان به‌عنوان نتیجه‌ای از یک قضیهٔ زیبا در نظریهٔ اعداد [به نام اصل برتران (Bertrand)] نشان داد که می‌گوید اگر $m > 1$، همواره عدد اولی بین m و $2m$ وجود دارد.

چون این نتیجه در اختیار ما نیست، ساده بودن A_n به ازای هر $n \geq 5$ را از راهی دیگر نشان می‌دهیم.

حال این قضیهٔ مهم را به ثبوت می‌رسانیم.

قضیهٔ ۹.۱.۶. گروه A_n به ازای هر $n \geq 5$ ساده است.

برهان. بنا بر قضیهٔ ۸.۱.۶ می‌توان فرض کرد $n \geq 6$. مرکز A_n به ازای $n > 3$ چیزی جز (e) نیست. (ثابت کنید!) چون A_n به‌وسیلهٔ ۳ـدورها تولید می‌شود، هرگاه $\sigma \neq e$ در A_n باشد، آن‌گاه به ازای یک ۳ـدور مانند τ، $\sigma\tau \neq \tau\sigma$.

فرض کنیم $N \neq (e)$ زیرگروه نرمالی از A_n بوده و $\sigma \neq e$ در N باشد. لذا، به ازای یک ۳ـدور مانند τ، $\sigma\tau \neq \tau\sigma$؛ یعنی $\sigma\tau\sigma^{-1}\tau^{-1} \neq e$. چون N در A_n نرمال است، عنصر $\tau\sigma^{-1}\tau^{-1}$ در N است. پس $\sigma\tau\sigma^{-1}\tau^{-1}$ نیز در N می‌باشد. چون τ یک ۳ـدور است، $\sigma\tau\sigma^{-1}$ نیز باید یک ۳ـدور باشد. لذا N شامل حاصلضرب دو ۳ـدور است، و این حاصلضرب مساوی e نیست. این دو ۳ـدور مستلزم حداکثر شش حرف‌اند. پس می‌توان آنها را نشسته در A_6 گرفت که، چون $n \geq 6$، می‌توان به‌طور یکریخت نشانیده در A_n در نظر گرفت. (ثابت کنید!) ولی در این صورت $N \cap A_6 \neq (e)$ یک زیرگروه نرمال A_6 است. پس، طبق نتیجهٔ فوق، $N \cap A_6 = A_6$. لذا N باید شامل یک ۳ـدور باشد، و چون تمام ۳ـدورها در A_n مزدوج‌اند (لم ۶.۱.۶)، N باید شامل تمام ۳ـدورها در S_n باشد. چون این ۳ـدورها A_n را تولید می‌کنند، پس N تمام A_n است و قضیه به ثبوت می‌رسد. ■

قضیهٔ ۹.۱.۶ برهانهای متفاوت بسیار دارد (که معمولاً نشان می‌دهند که یک زیرگروه نرمال A_n باید شامل یک ۳ـدور باشد) که از برهان ما کوتاهتر و احتمالاً آسانترند. ولی ما برهان خود و اینکه تمام ماجرا به این امر منجر می‌شود که ۶۰ مجذور کامل نیست را ترجیح می‌دهیم. به خواننده توصیه می‌شود که به چند برهان دیگر از این قضیهٔ بسیار مهم به‌خصوص در کتابهای نظریهٔ گروهها نگاه کند.

A_n خانواده‌ای نامتناهی از گروههای سادهٔ متناهی است. خانواده‌های نامتناهی دیگری از گروههای سادهٔ متناهی و نیز ۲۶ گروه خاص که به هیچ خانوادهٔ نامتناهی تعلق ندارند موجودند. این یعنی تعیین تمام گروههای سادهٔ متناهی که در دههٔ ۱۹۶۰ و دههٔ ۱۹۷۰ توسط تعداد کثیری از متخصصان نظریهٔ گروهها به‌دست آمدند، و این یکی از مهمترین کارهایی است که در ریاضیات قرن بیستم صورت یافته است.

مسائل

۱. ثابت کنید که اگر $n \geq 3$، مرکز S_n مساوی (e) است.

۲. ثابت کنید که اگر $n \geq 4$، مرکز A_n مساوی (e) است.

۳. راجع به ساختارهای دوری حاصل‌ضرب دو ۳-دور چه می‌شود گفت؟

۴. اگر $m \leq n$، نشان دهید که یک زیرگروه از S_n وجود دارد که با S_m یکریخت است.

۵. نشان دهید که هر گروه آبلی که زیرگروه حقیقی نداشته باشد دوری از مرتبهٔ اول است.

۶. چند ردهٔ تزویج در S_4 وجود دارد؟

۷. اگر عناصر a_1، a_2، ...، a_n گروه G را تولید کرده و b یک عنصر غیرمرکزی از G باشد، ثابت کنید به ازای iی، $a_i b \neq b a_i$.

۸. اگر $N \lhd G$ و $M \lhd N$، نشان دهید که به ازای هر $a \in G$، aMa^{-1} در N نرمال است.

۹. اگر $M \lhd G$ و $N \lhd G$، نشان دهید که MN یک زیرگروه نرمال G است.

۱۰. اگر $n \geq 5$ فرد باشد، نشان دهید که n-دورها A_n را تولید می‌کنند.

۱۱. نشان دهید که مرکزساز $(1\,2\,\cdots\,k)$ در S_n، از مرتبهٔ $k(n-k)!$ و مرکزساز $(1\,2\,\cdots\,k)$ از مرتبهٔ $n!/(k(n-k)!)$ در S_n، مزدوج‌اند.

۱۲. در برهان قضیهٔ ۸.۱۱.۶ نشان دهید که $|MN| = |N|^2$.

۳. میدانهای متناهی (قسمت یک)

هدف ما در این بخش و دو بخش بعد توصیف کامل تمام میدانهای متناهی است. چیزی که ما نشان می‌دهیم این است، که گروه ضربی عناصر ناصفر یک میدان گروهی دوری است. این امر در این بخش صورت می‌گیرد. در دو بخش بعد، هدف اثبات وجود و یکتایی میدانهای متناهی با p^n عنصر به ازای هر pی اول و هر عدد صحیح مثبت n است.

بعضی از کارهایی که انجام می‌دهیم قبلاً در مجموعه مسائل نظریهٔ گروهها و نظریهٔ میدانها بعنوان مسائل مشکل آمده‌اند، و روشهای ما از نظریهٔ گروهها و نظریهٔ میدانها، همراه با کمی نظریهٔ اعداد، می‌باشند.

تابع φی اویلر را یادآور می‌شویم. ما تابع φی اویلر را با $\varphi(1) = 1$ و به ازای $n > 1$، $\varphi(n)$ تعداد اعداد صحیح مثبت کمتر از n و نسبت به n اول تعریف می‌کنیم.

بحث را با نتیجه‌ای از نظریهٔ اعداد که در اثباتش از نظریهٔ گروهها استفاده می‌شود آغاز می‌کنیم. پیش از پرداختن به حالت کلی یک مثال می‌زنیم.

فرض کنیم $m = 12$. پس $\varphi(12) = 4$ زیرا فقط ۱، ۵، ۷، و ۱۱ از ۱۲ کمتر و نسبت به ۱۲ اولند. $\varphi(d)$ را به ازای جمیع مقسوم‌علیه‌های ۱۲ حساب می‌کنیم. داریم $\varphi(1) = 1$، $\varphi(2) = 1$، $\varphi(3) = 2$، $\varphi(4) = 2$، $\varphi(6) = 2$، و $\varphi(12) = 4$. توجه کنید که مجموع تمام $\varphi(d)$ها روی تمام مقسوم‌علیه‌های ۱۲ مساوی ۱۲ است. این امر تصادفی نبوده و حالت خاصی از قضیهٔ زیر می‌باشد.

قضیهٔ ۶.۳.۱۱. هرگاه $m \geq 1$، آنگاه $m = \sum \varphi(d)$ که در آن مجموع روی تمام مقسوم‌علیه‌های d از m گرفته می‌شود.

برهان. فرض کنیم G یک گروه دوری از مرتبهٔ m باشد که به‌وسیلهٔ عنصر a تولید می‌شود. اگر $d|m$، چند عنصر G از مرتبهٔ dاند؟ هرگاه $b = a^{m/d}$، آنگاه تمام جوابهای $x^d = e$ در G توانهای e، b، b^2، ……، b^{d-1} از b می‌باشند. چند تا از اینها از مرتبهٔ dاند؟ حکم می‌کنیم و به خواننده وامی‌گذاریم که b^r از مرتبهٔ d است اگر و فقط اگر r نسبت به d اول باشد. لذا تعداد عنصرهای از مرتبهٔ d در G به ازای هر مقسوم‌علیه d از m مساوی $\varphi(d)$ می‌باشد. مرتبهٔ هر عنصر در G مقسوم‌علیهی از m است؛ در نتیجه اگر تعداد عناصر از مرتبهٔ d یعنی $\varphi(d)$ را روی تمام dهایی که m را عاد می‌کنند جمع‌بندی کنیم، هر عنصر G یک و فقط یکبار به حساب می‌آید. لذا اگر روی تمام مقسوم‌علیه‌های d از m جمع‌بندی کنیم، $m = \sum \varphi(d)$. این امر قضیه را به ثبوت می‌رساند. ■

در یک گروه دوری متناهی از مرتبهٔ m تعداد جوابهای (عنصر یکهٔ G) $x^d = e$ به ازای هر dای که m را عاد کند درست، مساوی d است. ما از این امر در برهان قضیهٔ ۶.۳.۱۱ استفاده کردیم. حال عکس این مطلب را ثابت کرده و محکی برای دوری بودن یک گروه متناهی به دست می‌آوریم.

قضیهٔ ۶.۳.۱۲. فرض کنیم G یک گروه متناهی از مرتبهٔ m با این خاصیت باشد که به ازای هر dای که m را عاد کند حداکثر d جواب برای $x^d = e$ در G موجود باشد. در این صورت G یک گروه دوری می‌باشد.

برهان. فرض کنیم $\psi(d)$ تعداد عناصری از G باشند که از مرتبهٔ dاند. طبق فرض، هرگاه $a \in G$ از مرتبهٔ d باشد، آنگاه تمام جوابهای $x^d = e$ توانهای متمایز e، a، a^2، ……، a^{d-1}اند که از آنها $\varphi(d)$ تا از مرتبهٔ d می‌باشند. لذا هرگاه عنصری از مرتبهٔ d در G موجود باشد، آنگاه

$\psi(d) = \varphi(d)$. از آن‌سو، هرگاه عنصری در G از مرتبهٔ d نباشد، آن‌گاه $\psi(d) = 0$. لذا به ازای هر $d|n$ داریم $\psi(d) \leq \varphi(d)$. ولی چون هر عنصر G مرتبه‌ای چون d دارد که n را عاد می‌کند، $\sum \psi(d) = n$ که در آن مجموع روی تمام مقسوم‌علیه‌های d از n گرفته می‌شود. اما

$$n = \sum \psi(d) \leq \sum \varphi(d) = n$$

زیرا هر $\psi(d) \leq \varphi(d)$. از این داریم $\sum \psi(d) = \sum \varphi(d)$ که همراه با $\psi(d) \leq \varphi(d)$ معلوم می‌شود که به ازای هر dای که n را عاد کند، $\psi(d) = \varphi(d)$. لذا، به‌خصوص، $\psi(n) = \varphi(n) \geq 1$. این رابطه به ما چه می‌گوید؟ بالاخره $\psi(n)$ تعداد عناصر G از مرتبهٔ n است و چون $\psi(n) \geq 1$، باید عنصری مانند a در G از مرتبهٔ n موجود باشد. بنا براین عناصر e، a، a^2، $\dots$، a^{n-1} متمایز بوده و تعدادشان n است؛ در نتیجه باید تمام G را به ما بدهند. لذا G دوری با مولد a بوده و قضیه به ثبوت می‌رسد. ∎

آیا حالتی هست که در آن معادلهٔ $x^d = e$ حداکثر d جواب در یک گروه مفروض داشته باشد؟ مسلماً وجود دارد. هرگاه K^* گروه عناصر ناصفر یک میدان تحت ضرب باشد، آن‌گاه، بنا بر قضیهٔ ۲.۶.۵، چندجمله‌ای $x^n - 1$ حداکثر n ریشه در K^* دارد. لذا هرگاه $G \subset K^*$ یک زیرگروه ضربی متناهی K^* باشد، آن‌گاه تعداد جوابهای $x^d = 1$ در G به ازای هر عدد صحیح مثبت d، و در نتیجه به ازای هر d که مرتبهٔ G را عاد کند، حداکثر d است. بنا بر قضیهٔ ۲.۲.۶، G باید یک گروه دوری باشد. لذا قضیهٔ زیر ثابت شده است.

قضیهٔ ۳.۲.۶. هرگاه K یک میدان و K^* گروه عناصر ناصفر K تحت ضرب باشد، آن‌گاه هر زیرگروه متناهی K^* دوری است.

یک حالت بسیار خاص از قضیهٔ ۳.۲.۶، ولی فعلاً مهمترین حالت برای ما، قضیهٔ زیر است.

قضیهٔ ۴.۲.۶. هرگاه K یک گروه متناهی باشد، آن‌گاه K^* یک گروه دوری است.

برهان. K^* یک زیرگروه متناهی خود است. پس، طبق قضیهٔ ۳.۲.۶، K^* دوری می‌باشد. ∎

حالت خاصی از قضیهٔ ۴.۲.۶ اهمیت زیادی در نظریهٔ اعداد دارد و به وجود ریشه‌های اولیه $\bmod p$ به ازای pی اول معروف است.

قضیهٔ ۵.۲.۶. هرگاه p اول باشد، آن‌گاه $\mathbb{Z}_p$ یک گروه دوری است.

مسائل

۱. اگر $a \in G$ از مرتبهٔ d باشد، ثابت کنید a^r نیز از مرتبهٔ d است اگر و فقط اگر r و d نسبت به هم اول باشند.

۲. برای $\mathbb{Z}_{11}^*$ یک مولد دوری (ریشهٔ اولیه) بیابید.

۳. مسئلهٔ ۲ را برای $\mathbb{Z}_{17}^*$ حل کنید.

۴. میدان K را با نه عنصر ساخته و برای گروه K^* یک مولد دوری بیابید.

۵. هرگاه p اول بوده و $m = p^2$، آنگاه $\mathbb{Z}_m$ میدان نیست ولی مجموعهٔ $\{[a] | (a, p) = 1\}$ تحت ضرب در $\mathbb{Z}_m$ یک گروه تشکیل می‌دهد. ثابت کنید این گروه دوری از مرتبهٔ $p(p-1)$ است.

۶. تمام زیرگروههای متناهی $\mathbb{C}^*$ را، که در آن $\mathbb{C}$ میدان اعداد مختلط است، تعیین نمایید.

در مسائل زیر φ تابع φی اویلر است.

۷. اگر p اول باشد، نشان دهید که $\varphi(p^n) = p^{n-1}(p-1)$.

۸. اگر اعداد صحیح مثبت m و n نسبت به هم اول باشند، ثابت کنید

$$\varphi(mn) = \varphi(m)\varphi(n)$$

۹. با استفاده از مسائل ۷ و ۸، $\varphi(n)$ را برحسب تجزیهٔ n به عوامل با توانهای اعداد اول بنویسید.

۱۰. ثابت کنید $\lim_{n\to\infty} \varphi(n) = +\infty$.

۳. میدانهای متناهی (قسمت دو): وجود

فرض کنیم K یک میدان متناهی باشد. در این صورت K باید از مشخص عدد اول p بوده و شامل ۰، ۱، ۲، ...، $p-1$، یعنی p مضرب عنصر یکهٔ ۱ از K، باشد. در نتیجه $K \supset \mathbb{Z}_p$ یا، به‌طور دقیقتر، K شامل میدانی یکریخت با $\mathbb{Z}_p$ است. چون K یک فضای برداری روی $\mathbb{Z}_p$ بوده و به وضوح با بعد متناهی روی $\mathbb{Z}_p$ است، اگر $[K : \mathbb{Z}_p] = n$، K دارای p^n عنصر می‌باشد. این امر درست است زیرا هرگاه v_1، v_2، ...، v_n پایه‌ای از K روی $\mathbb{Z}_p$ باشد، آن‌گاه به ازای هر انتخاب متمایز $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ که در آن α_iها در $\mathbb{Z}_p$اند، عنصرهای

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

متمایزند. لذا چون می‌توان $(a_1, a_2, \dots, a_n)$ را به p^n راه اختیار کرد، K دارای p^n عنصر می‌باشد.

چون K^*، یعنی گروه ضربی عناصر ناصفر K، گروهی از مرتبهٔ $p^n - 1$ است، به ازای هر a در K داریم $a^{m-1} = 1$ که در آن $m = p^n$. لذا $a^m = a$. چون این به ازای $a = 0$ نیز درست است، به ازای هر a در K داریم $a^m = a$. لذا چندجمله‌ای $x^m - x$ در $\mathbb{Z}_p[x]$ دارای $m = p^n$ ریشهٔ متمایز در K است یعنی تمام عناصر K. لذا $x^m - x$ در $K[x]$ به صورت زیر تجزیه می‌شود:

$$x^m - x = (x - a_1)(x - a_2)\cdots(x - a_m)$$

که در آن a_1، a_2، ...، a_m عناصر K می‌باشند.

آنچه هم اکنون ذکر شد قبلاً بیش و کم در بخش ۶ از فصل ۵ گفته بودیم. چون می‌خواستیم مطالب برای شما تازه باشد، آنها را در اینجا تکرار نمودیم.

آنچه را که هم اکنون گفته شد در قضیهٔ زیر خلاصه می‌کنیم.

قضیهٔ ۶.۳.۱. فرض کنیم K یک میدان متناهی از مشخصه عدد اول p باشد. در این صورت K شامل $m = p^n$ عنصر است که در آن $[K : \mathbb{Z}_p] = n$ و چندجمله‌ای $x^m - x$ در $\mathbb{Z}_p[x]$ به عوامل خطی در $K[x]$ به صورت زیر تجزیه می‌شود:

$$x^m - x = (x - a_1)(x - a_2)\cdots(x - a_m)$$

که در آن a_1، a_2، ...، a_m عناصری از K می‌باشند.

در اینجا دو سؤال مطرح می‌شود:

۱. به ازای چه pهای اول و چه اعداد صحیح n میدانی با p^n عنصر وجود دارد؟
۲. چند میدان غیر یکریخت با p^n عنصر وجود دارد؟

ما در این بخش و بخش بعد به هر دو سؤال پاسخ می‌دهیم. جوابها به قرار زیرند:

۱. به ازای هر pی اول و هر عدد صحیح مثبت n یک میدان متناهی با p^n عنصر وجود دارد.
۲. هر دو میدان متناهی با تعداد عناصر یکسان یکریخت می‌باشند.

حال به این دو نتیجه می‌پردازیم. نخست مسئلهٔ وجود میدانهای متناهی را ثابت می‌بخشیم. بحث را با نکته‌ای کلی در باب چندجمله‌ایهای تحویل‌ناپذیر شروع می‌کنیم.

لم ۶.۳.۲. فرض کنیم F یک میدان و $p(x)$ یک چندجمله‌ای تحویل‌ناپذیر در $F[x]$ باشد. همچنین $q(x)$ در $F[x]$ چنان باشد که $p(x)$ و $q(x)$ در توسیع میدانی از F ریشهٔ مشترک داشته باشند. در این صورت $p(x)$، $q(x)$ را در $F[x]$ عاد می‌کند.

برهان. فرض کنیم $p(x)$، $q(x)$ را عاد نکند. چون $p(x)$ در $F[x]$ تحویل‌ناپذیر است، $p(x)$ و $q(x)$ باید در $F[x]$ نسبت به هم اول باشند. لذا چندجمله‌ایهایی مانند $u(x)$ و $v(x)$ در $F[x]$ وجود دارند بطوری که

$$u(x)p(x)+v(x)q(x)=1$$

فرض کنیم عنصر a در توسیعی از F مانند K ریشهٔ مشترک $p(x)$ و $q(x)$ باشد. لذا $p(a)=q(a)=0$. ولی در این صورت $0=u(a)p(a)+v(a)q(a)=1$ که یک تناقض است. در نتیجه $p(x)$، $q(x)$ را در $F[x]$ عاد می‌کند. ■

توجه کنید که عملاً می‌توان مطلب بیشتری را ثابت کرد؛ یعنی:

نتیجه. هرگاه $f(x)$ و $g(x)$ در $F[x]$ نسبت به هم در $K[x]$ اول نباشند که K یک توسیع F است، آنگاه نسبت به هم در $F[x]$ نیز اول نیستند.

فرض کنیم F میدانی از مشخص $p\neq 0$ باشد. حکم می‌کنیم که چندجمله‌ای $f(x)=x^m-x$ که در آن $m=p^n$ نمی‌تواند ریشهٔ چندگانه‌ای در هیچ توسیع میدانی K از F داشته باشد. آیا به یاد می‌آورید که ریشهٔ چندگانهٔ یک چندجمله‌ای چیست؟ ما خاطرات شما را تازه می‌کنیم. هرگاه $g(x)$ در $F[x]$ بوده و K یک توسیع میدانی F باشد، آنگاه a در K یک ریشهٔ چندگانهٔ $g(x)$ است اگر به ازای $q(x)$ای در $K[x]$ داشته باشیم $g(x)=(x-a)^2q(x)$.

حال به چندجمله‌ای $f(x)=x^m-x$ فوق باز می‌گردیم. چون $f(x)=x(x^{m-1}-1)$ و 0 ریشهٔ $x^{m-1}-1$ نیست، 0 یک ریشهٔ سادهٔ $f(x)$ است (یعنی چندگانه نیست). فرض کنیم $a\in K$ $(K\supset F)$ ریشهٔ $f(x)$ باشد. لذا $a^m=a$. هرگاه $y=x-a$، آنگاه

$$f(y)=y^m-y=(x-a)^m-(x-a)=x^m-a^m-(x-a)$$

(زیرا مشخص $p\neq 0$ و $m=p^n$)

$$=x^m-x\quad(\text{زیرا } a^m=a)=f(x)$$

لذا

$$f(x)=f(y)=y^m-y=(x-\alpha)^m-(x-\alpha)$$
$$=(x-\alpha)((x-\alpha)^{m-1}-1)$$

و واضح است که این بر $x-\alpha$ فقط با توان یک بخشپذیر است زیرا $x-\alpha$ عبارت $(x-\alpha)^{m-1}-1$ را عاد نمی‌کند. لذا α یک ریشهٔ چندگانهٔ $f(x)$ نیست.

لذا قضیهٔ زیر ثابت شده است.

قضیهٔ ۳.۳.۶. هرگاه $n>0$، آنگاه $f(x)=x^m-x$ که در آن $m=p^n$ ریشهٔ چندگانه‌ای در یک میدان از مشخص p ندارد.

لازم است با افزودن نکته‌ای به برهان فوق، قضیهٔ ۳.۳.۶ را به‌صورتی که داده‌ایم تثبیت نماییم. هر میدان از مشخص $p\neq 0$ یک توسیع $\mathbb{Z}_p$ است، و چندجمله‌ای $f(x)$ در $\mathbb{Z}_p[x]$ می‌باشد. لذا استدلال فوق که در آن K میدانی از مشخص p بوده و $F=\mathbb{Z}_p$ قضیه را به شکل داده شده‌اش ثابت می‌کند.

حال ابزارهای لازم برای اثبات قضیهٔ مهم ۴.۳.۶ در اختیار ماست.

قضیهٔ ۴.۳.۶. به ازای هر عدد اول p و هر عدد صحیح مثبت n یک میدان متناهی با p^n عنصر وجود دارد.

برهان. چندجمله‌ای x^m-x در $\mathbb{Z}_p[x]$ را در نظر می‌گیریم که در آن $m=p^n$. بنا بر قضیهٔ ۶.۶.۵، یک میدان متناهی مانند K از $\mathbb{Z}_p$ هست به‌طوری که چندجمله‌ای x^m-x در $K[x]$ به‌صورت زیر تجزیه می‌شود:

$$x^m-x=(x-a_1)(x-a_2)\cdots(x-a_m)$$

که در آن a_1، a_2، $\cdots$، a_m در Kاند. بنا بر قضیهٔ ۳.۳.۶، x^m-x ریشهٔ چندگانه‌ای در K ندارد. پس عنصرهای a_1، a_2، $\cdots$، a_m، $m=p^n$ عنصر متمایز می‌باشند. همچنین می‌دانیم که a_1، a_2، $\cdots$، a_m همهٔ ریشه‌های x^m-x در Kاند زیرا x^m-x از درجهٔ m می‌باشد.

فرض کنیم $A=\{a\in K|a^m=a\}$. همان‌طور که اینک دیدیم، A دارای m عنصر متمایز است. حکم می‌کنیم که A یک میدان است. گوییم هرگاه $a,b\in A$، آنگاه $a^m=a$ و $b^m=b$؛ در نتیجه $(ab)^m=a^mb^m=ab$. لذا $ab\in A$. چون ما در میدانی از مشخص $p\neq 0$ بوده و $m=p^n$، $(a+b)^m=a^m+b^m=a+b$؛ در نتیجه $a+b$ در A می‌باشد.

چون A زیرمجموعه‌ای متناهی از یک میدان بوده و نسبت به جمع و ضرب بسته است، A باید زیرمیدانی از K باشد. و چون A دارای $m = p^n$ عنصر است، A میدانی است که وجودش در صورت قضیه تصریح شده است. با این امر قضیه ثابت خواهد شد. ■

مسائل

*۱. نتیجهٔ لم ۲.۳.۶ را به‌طور کامل ثابت کنید.

دو مسئلهٔ بعدی تکرار مسائلی است که قبلاً در کتاب آمده‌اند.

۲. اگر $f(x) = a_{\circ}x^n + a_{1}x^{n-1} + \cdots + a_n$ در $F[x]$ بوده و $f'(x)$ مشتق صوری $f(x)$ تعریف شده با معادلهٔ زیر باشد:

$$f'(x) = na_{\circ}x^{n-1} + (n-1)a_{1}x^{n-2} + \cdots + (n-i)a_{i}x^{n-i-1} + \cdots + a_{n-1}$$

ثابت کنید

الف) $(f(x) + g(x))' = f'(x) + g'(x)$؛

ب) به ازای هر $f(x)$ و $g(x)$ در $F[x]$، $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

*۳. ثابت کنید $f(x)$ از $F[x]$ در توسیعی از F ریشهٔ چندگانه دارد اگر و فقط اگر $f(x)$ و $f'(x)$ نسبت به هم اول نباشند.

۴. اگر $f(x) = x^n - x$ در $F[x]$ باشد، ثابت کنید $f(x)$ در هیچ توسیع F ریشهٔ چندگانه ندارد اگر F از مشخص $\circ$ باشد یا مشخص $p \neq \circ$ و p، $n - 1$ را عاد نکند.

۵. قضیهٔ ۳.۳.۶ را با استفاده از مسئلهٔ ۴ به صورتی دیگر ثابت کنید.

۶. اگر F میدانی از مشخص $p \neq \circ$ باشد، یک چندجمله‌ای با ریشه‌های چندگانه به شکل $x^n - x$ بسازید که $p|(n-1)$.

۷. اگر میدان K دارای p^n عنصر باشد، نشان دهید که به ازای هر mی که n را عاد کند زیرمیدانی از K با p^m عنصر وجود دارد.

۴. میدانهای متناهی (قسمت سه): یکتایی

حال که می‌دانیم به ازای هر pی اول و هر عدد صحیح مثبت n میدانهای متناهی با p^n عنصر وجود دارند، می‌پرسیم: چند میدان متناهی با p^n عنصر وجود دارد؟ برای آنکه سؤال با معنی

باشند می پرسیم: چند میدان غیریکریخت متمایز با p^n عنصر وجود دارد؟ جواب این سوال کوتاه و دل‌چسب است: فقط یکی. ما در این جا نشان می‌دهیم که هر دو میدان متناهی با تعداد عناصر یکسان یکریخت‌اند.

فرض می‌کنیم K و L، دو میدان متناهی با p^n عنصر باشند. لذا L و K میدان‌های برداری n بعدی روی Z_p اند. L و K به عنوان فضای برداری یکریخت می‌باشند. از آن سو، طبق ۴.۲.۶ K^* و L^* هر دو گروههای دوری از مرتبه‌ی $p^n - 1$ می‌باشند. لذا K^* و L^* به عنوان گروههای ضربی یکریخت می‌باشند. ممکن است تصور شود که با کنار هم گذاردن این دو یکریختی می‌توان ثابت کرد که L و K به عنوان میدان یکریخت‌اند. ولی این طور نیست. برهان در این جهت پیش نخواهد رفت. اما متناهی بودن L و K همراه با این دو یکریختی (در ساختار K و L) پیشنهاد می‌کند که L و K احتمالاً میدان‌های یکریخت‌اند. این در واقع درست است و ما اینک آن را نشان می‌دهیم.

بحث را با لم زیر آغاز می‌کنیم:

لم ۱.۴.۶ هرگاه $q(x)$ در $Z_p[x]$ تحویل‌ناپذیر از درجه‌ی n باشد، آنگاه $q(x) \mid (x^m - x)$ که در آن $m = p^n$

برهان. بنابر قضیه‌ی ۱.۵.۴ ایده‌آل $(q(x))$ تولیدشده به وسیله‌ی $q(x)$ از $Z_p[x]$ یک ایده‌آل ماکزیمال از $Z_p[x]$ است. زیرا $q(x)$ در $Z_p[x]$ تحویل‌ناپذیر است. فرض می‌کنیم $A = Z_p[x]/(q(x))$. بنابر قضیه‌ی ۲.۴.۴، A میدانی از درجه‌ی n روی Z_p است پس دارای p^n عنصر می‌باشد. لذا به ازای هر عنصر u در A، $u^m = u$.

فرض می‌کنیم $a = x + (q(x))$ هم‌مجموعه‌ی x در $A = Z_p[x]/(q(x))$ باشد لذا $q(a) = 0$، $q(x)$ چندجمله‌ای مینیمال a روی Z_p است. چون a در A است، $a^m = a$ در نتیجه a ریشه‌ی چندجمله‌ای $x^m - x$ است که در آن $m = p^n$. لذا $x^m - x$ و $q(x)$ ریشه‌ی مشترکی در A دارند. بنابر لم ۲.۳.۶ $q(x) \mid (x^m - x)$. □

حال در وضعیتی هستیم که می‌توانیم نتیجه‌ی اصلی این بخش را ثابت کنیم.

قضیه ۲.۴.۶. هرگاه K و L میدان‌های متناهی با تعداد عناصر یکسان باشند آن‌گاه K و L میدان‌های یکریخت‌اند.

برهان: فرض می‌کنیم K و L دارای p^n عنصر باشند. بنابر قضیه‌ی ۲.۴.۶ L^* یک گروه دوری

است که مثلاً بوسیلهٔ عنصر b در L تولید می‌شود. در این صورت $\mathbb{Z}_p(b)$، یعنی میدان حاصل از الحاق b به $\mathbb{Z}_p$، مسلماً تمام L است. چون $m = [L : \mathbb{Z}_p]$، بنا بر قضیهٔ ۵.۳.۲، b روی $\mathbb{Z}_p$ جبری از درجهٔ m است که $m = \deg(q(x))$ و در آن $q(x)$ چندجمله‌ای مینیمال در $\mathbb{Z}_p[x]$ عنصر b بوده و در $\mathbb{Z}_p[x]$ تحویل‌ناپذیر می‌باشد.

نگاشت $\psi : \mathbb{Z}_p[x] \to L = \mathbb{Z}_p(b)$ با تعریف $\psi(f(x)) = f(b)$ یک همریختی از $\mathbb{Z}_p[x]$ به روی L با هستهٔ $(q(x))$ (ایدآل تولید شده بوسیلهٔ $q(x)$ از $\mathbb{Z}_p[x]$) می‌باشد. لذا $L \simeq \mathbb{Z}_p[x]/(q(x))$.

چون $q(x)$ در $\mathbb{Z}_p[x]$ تحویل‌ناپذیر از درجهٔ m است، بنا بر لم ۱۱.۴.۶، $q(x)$ باید $x^m - x$ را که در آن $m = p^n$ عاد کند. ولی، طبق لم ۱۱.۳.۶، چندجمله‌ای $x^m - x$ در $K[x]$ بصورت زیر تجزیه می‌شود:

$$x^m - x = (x - a_1)(x - a_2) \cdots (x - a_m)$$

که در آن $a_1, a_2, \ldots, a_m$ همهٔ عناصر Kاند. لذا $q(x)$ عبارت $(x-a_1)(x-a_2)\cdots(x-a_m)$ را عاد می‌کند. بنا بر نتیجهٔ قضیهٔ ۱۰.۵.۴، $q(x)$ نمی‌تواند نسبت به همهٔ a_iها $x - a_i$ها در $K[x]$ اول باشند. لذا، به ازای jای، $q(x)$ و $x - a_j$ عامل مشترکی از درجهٔ دست‌کم ۱ دارند. بطور خلاصه، $x - a_j$ باید $q(x)$ را در $K[x]$ عاد کند؛ در نتیجه به ازای $h(x)$ای در $K[x]$، $q(x) = (x - a_j)h(x)$. لذا $q(a_j) = 0$.

چون $q(x)$ در $\mathbb{Z}_p[x]$ تحویل‌ناپذیر بوده و a_j ریشه‌ای از $q(x)$ است، $q(x)$ باید چندجمله‌ای مینیمال a_j در $\mathbb{Z}_p[x]$ باشد. لذا $L \simeq \mathbb{Z}_p[x]/(q(x)) \simeq \mathbb{Z}_p(a_j)$. این همراه با چیزهای دیگر به ما می‌گویند که $m = [\mathbb{Z}_p(a_j) : \mathbb{Z}_p]$؛ و چون $\mathbb{Z}_p(a_j) \subset K$ و $m = [K : \mathbb{Z}_p]$، نتیجه می‌شود که $\mathbb{Z}_p(a_j) = K$. لذا $K = \mathbb{Z}_p(a_j) \simeq L$. پس نتیجهٔ مطلوب بدست می‌آید؛ یعنی K و L میدانهایی یکریخت می‌باشند. این امر قضیه را به ثبوت می‌رساند. ■

از تلفیق قضایای ۴.۳.۶ و ۲.۴.۶ خواهیم داشت:

قضیهٔ ۳.۴.۶. به ازای هر عدد اول p و هر عدد صحیح مثبت m یک و فقط یک میدان (با تقریب یکریختی) دارای p^m عنصر وجود دارد.

۵. چندجمله‌ای دایره بر

فرض کنیم $\mathbb{C}$ میدان اعداد مختلط باشد. بعنوان نتیجه‌ای از قضیهٔ دموآور عدد مختلط $\theta_n = \cos 2\pi/n + i \sin 2\pi/n$ در روابط $\theta_n^n = 1$ و $\theta_n^m \neq 1$ اگر $0 < m < n$ صدق

می‌کند. ما θ_n را یک ریشهٔ nم اولیهٔ واحد می‌نامیم. سایر ریشه‌های nم اولیهٔ واحد عبارتند از

$$\theta_n^k = \cos\left(\frac{۲\pi k}{n}\right) + i\sin\left(\frac{۲\pi k}{n}\right)$$

که در آن $(k,n) = ۱$ و $۱ \leq k < n$.

واضح است که θ_n در چندجمله‌ای $x^n - ۱$ در $\mathbb{Q}[x]$، که در آن $\mathbb{Q}$ میدان اعداد گویاست، صدق می‌کند. می‌خواهیم چندجمله‌ای مینیمال (تکین) θ_n روی $\mathbb{Q}$ را بیابیم.

ما دنباله‌ای از چندجمله‌ایها را به استقرا تعریف می‌کنیم. در نگاه اول ممکن است این چندجمله‌ایها ارتباطی با یافتن چندجمله‌ای مینیمال θ_n روی $\mathbb{Q}$ نداشته باشند. ولی خواهیم دید که آنها به سؤال فوق بسیار مربوط بوده و، همان‌طور که بعداً ثابت خواهد شد، چندجمله‌ای $\phi_n(x)$ که اینک معرفی می‌شود یک چندجمله‌ای تکین با ضرایب صحیح بوده، روی $\mathbb{Q}$ تحویل‌ناپذیر است و، علاوه بر این، $\phi_n(\theta_n) = ۰$. این به ما خواهد گفت که $\phi_n(x)$ چندجمله‌ای مینیمال تکین مطلوب θ_n روی $\mathbb{Q}$ می‌باشد.

حال به تعریف این چندجمله‌ایها می‌پردازیم.

تعریف. چندجمله‌ایهای $\phi_n(x)$ به استقرا چنین تعریف می‌شوند:

الف) $\phi_۱(x) = x - ۱$؛

ب) هرگاه $n > ۱$، آن‌گاه $\phi_n(x) = (x^n - ۱)/\Pi\phi_d(x)$ که در حاصلضرب آمده در مخرج d روی تمام مقسوم‌علیه‌های n جز خود n تغییر می‌کند.

این چندجمله‌ایها را چندجمله‌ایهای دایره بر و $\phi_n(x)$ را چندجمله‌ای دایره بر nم می‌نامند.

فعلاً معلوم نیست که $\phi_n(x)$ها حتی چندجمله‌ای‌اند و هیچ اطلاعی از سرشت ضرایب آنها نداریم. این امور به موقع روشن خواهند شد. ابتدا به چند مثال نگاه می‌کنیم.

چند مثال

۱. $\phi_۲(x) = (x^۲ - ۱)/\phi_۱(x) = (x^۲ - ۱)/(x - ۱) = x + ۱$

۲. $\phi_۳(x) = (x^۳ - ۱)/\phi_۱(x) = (x^۳ - ۱)/(x - ۱) = x^۲ + x + ۱$

۳. $$\begin{aligned}\phi_۴(x) &= (x^۴ - ۱)/(\phi_۱(x)\phi_۲(x)) = (x^۴ - ۱)/(x - ۱)(x + ۱)\\ &= (x^۴ - ۱)/(x^۲ - ۱) = x^۲ + ۱\end{aligned}$$

۴.
$$\phi_5(x) = (x^5 - 1)/\phi_1(x) = (x^5 - 1)/(x - 1)$$
$$= x^4 + x^3 + x^2 + x + 1$$

۵.
$$\phi_6(x) = \frac{x^6 - 1}{\phi_1(x)\phi_2(x)\phi_3(x)}$$
$$= \frac{x^6 - 1}{(x - 1)(x + 1)(x^2 + x + 1)}$$
$$= \frac{x^3 + 1}{x + 1} = x^2 - x + 1$$

حال به چند مطلب در باب چندجمله‌ایهای فوق اشاره می‌کنیم:

۱. همهٔ آنها چندجمله‌ایهای تکین با ضرایب صحیح‌اند؛

۲. به ازای $1 \leq n \leq 6$، درجهٔ $\phi_n(x)$ مساوی $\varphi(n)$ است که در آن φ تابع φی اویلر می‌باشد (امتحان کنید)؛

۳. $\phi_n(x)$ به ازای $1 \leq n \leq 6$ در $\mathbb{Q}(x)$ تحویل‌ناپذیر است (تحقیق کنید!)؛

۴. به ازای $1 \leq n \leq 6$، θ_n ریشهٔ $\phi_n(x)$ می‌باشد (تحقیق کنید!).

این چند حالت به وضع کلی تمام $\phi_n(x)$ها اشاره دارند. به‌عنوان اشاره بلی ولی فقط اشاره. اثبات این خواص برای $\phi_n(x)$ کمی کار خواهد داشت.

برای کسب اطلاعات بیشتر از این چندجمله‌ایها، حالت خاصی را در نظر می‌گیریم که در آن $n = p^m$ و p اول است. برای احتراز از زیرنویسهای مزاحم، $\phi_n(x)$ را با $\psi^{(m)}(x)$ نشان می‌دهیم که در آن $n = p^m$. عدد اول p را در طول بحث ثابت می‌گیریم. ما برای $\psi^{(m)}(x)$ها فرمولهایی صریح یافته و خواص اساسی‌شان را تعیین می‌کنیم. ولی روشی که به‌کار می‌بریم در حالت کلی $\phi_n(x)$ قابل اعمال نیست. بررسی وضعیت کلی نیاز به روشهایی وسیعتر و عمیقتر از روشهای لازم برای $\psi^{(m)}(x)$ خواهد داشت.

حال یک مثال ساده می‌زنیم. اگر p اول باشد، تنها مقسوم‌علیه p که خود p نباشد ۱ است. از تعریف $\phi_p(x) = \psi^{(1)}(x)$ داریم

$$\psi^{(1)}(x) = \phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$$

توجه کنید که در بررسی محک آیزن اشتاین نشان دادیم که این چندجمله‌ای در $\mathbb{Q}(x)$ تحویل‌ناپذیر است.

راجع به $\psi^{(m)}(x)$های بالاتر چه می‌شود گفت؟

لم ۶.۵۵.۱۱. به ازای هر $m \geq 1$،

$$\psi^{(m)}(x)=\frac{x^{p^m}-1}{x^{p^{m-1}}-1}=1+x^{p^{m-1}}+x^{2p^{m-1}}+\cdots+x^{(p-1)p^{m-1}}$$

برهان. روی m استقرا می‌کنیم.

اگر $m=1$، در بالا نشان دادیم که

$$\psi^{(1)}(x)=(x^p-1)/(x-1)=1+x+x^2+\cdots+x^{p-1}$$

در نتیجه لم در این حالت درست است.

فرض کنیم به ازای هر $r<m$، $\psi^{(r)}=(x^{p^r}-1)/(x^{p^{r-1}}-1)$. $\psi^{(m)}(x)$ را در نظر می‌گیریم. چون تنها مقسوم‌علیه‌های حقیقی p^m عبارتند از ۱، p، p^2، ...، p^{m-1}، از تعریف $\psi^{(m)}(x)$ داریم

$$\psi^{(m)}(x)=\frac{x^{p^m}-1}{(x-1)\psi^{(1)}(x)\cdots\psi^{(m-1)}(x)}$$

بنابه فرض استقرا، به ازای $r<m$، $\psi^{(r)}(x)=(x^{p^r}-1)/(x^{p^{r-1}}-1)$؛ در نتیجه

$$(x-1)\psi^{(1)}(x)\cdots\psi^{(m-1)}(x)=(x-1)\frac{x^p-1}{x-1}\frac{x^{p^2}-1}{x^p-1}\cdots\frac{x^{p^{m-1}}-1}{x^{p^{m-2}}-1}=x^{p^{m-1}}-1$$

ولی در این صورت

$$\psi^{(m)}(x)=\frac{x^{p^m}-1}{x^{p^{m-1}}-1}$$

استقرا را تمام کرده و لم را ثابت می‌نماید. ■

در اینجا توجه می‌کنیم که

$$\psi^{(m)}(x)=\frac{x^{p^m}-1}{x^{p^{m-1}}-1}=1+x^{p^{m-1}}+\cdots+x^{(p-1)p^{m-1}}$$

یک چندجمله‌ای تکین با ضرایب صحیح است. درجه‌اش به وضوح مساوی $(p-1)p^{m-1}$ است که در واقع $\varphi(p^m)$ می‌باشد. بالاخره هرگاه θ یک ریشهٔ اولیهٔ p^mام واحد باشد، آنگاه $\theta^{p^m}=1$

ولی $\theta^{p^{m-1}} \neq 1$. درنتیجه $\psi^{(m)}(\theta)=0$. لذا θ ریشه‌ی $\psi^{(m)}(x)$ می باشد. آخرین چیزی که می‌خواهیم بدانیم این است که آیا $\psi^{(m)}(x)$ تحویل ناپذیر است؟

توجه کنید که

$$\psi^{(m)}(x)=1+x^{p^{m-1}}+\dots+x^{(p-1)p^{m-1}}=\phi^{(1)}(x^{p^{m-1}})$$

و می دانیم که $\psi^{(1)}(x)$ در $Q[x]$ تحویل ناپذیر است. با استفاده از محک آیزنشتاین ثابت می‌کنیم که $\psi^{(m)}(x)$ در $Q[x]$ تحویل ناپذیر می باشد.

حال یک لحظه، از بحث منحرف می‌شویم اگر $f(x)$ و $g(x)$ دو چندجمله‌ای با ضرایب صحیح باشند تعریف می‌کنیم $f(x)\equiv g(x) \mod p$ اگر $f(x)=g(x)+r(x)$ که در آن $r(x)$ یک چندجمله‌ای با ضرایب صحیح است. این هم از آن است که، بگوییم ضرایب نظیر $f(x)$ و $g(x)$ همنهشت $\mod p$ اند. با بسط $(f(x)+g(x))^p$ طبق قضیه‌ی دوجمله‌ای و استفاده از این که تمام ضرایب دوجمله ای، بر p بخشپذیرند (زیرا p اول است) به رابطه‌ی

$$(f(x)+g(x))^p = f(x)^p+g(x)^p \mod p$$

می رسیم.

هرگاه $f(x)=a_0x^n+a_1x^{n-1}+\dots+a_n$ که در آن a_i ها صحیح اند، آن‌گاه طبق فوق،

$$f(x)^p=(a_0x^n+a_1x^{n-1}+\dots+a_n)^p\equiv a_0^p x^{np}+a_1^p x^{(n-1)p}+\dots+a_n^p$$

$$\equiv a_0x^{np}+a_1x^{(n-1)p}+\dots+a_n \mod p$$

همنهشتی اخیر نتیجه‌ی از قضیه‌ی فرما (نتیجه قضیه‌ی ۸.۴.۲) چون

$$f(x^p)=a_0x^{np}+a_1^{(n-1)p}+\dots+a_n$$

داریم

$$f(x^p)\equiv f(x)^p \mod p$$

با تکرار آن چه هم اکنون کردیم به $f(x^{p^k})=f(x)^{p^k} \mod p$ به ازای k نامنفی می‌رسیم.

حال به $\psi^{(m)}(x)$ باز می‌گردیم. چون $\psi^{(m)}(x) = \psi^{(1)}(x^{p^{m-1}})$، از بحث فوق داریم $\psi^{(m)}(x) \equiv \psi^{(1)}(x^{p^{m-1}}) \bmod p$. لذا

$$\begin{aligned}\psi^{(1)}(x+1)^{p^{m-1}} &= \left(\frac{(x+1)^p - 1}{(x+1)-1}\right)^{p^{m-1}} = \left(\frac{(x+1)^p - 1}{x}\right)^{p^{m-1}}\\ &= \left(x^{p-1} + px^{p-2} + \frac{p(p-1)}{2}x^{p-3} + \cdots + \frac{p(p-1)}{2}x + p\right)^{p^{m-1}}\\ &\equiv \psi^{(1)}(x)^{p^{m-1}(p-1)} \bmod p \equiv \psi^{(m)}(x+1) \bmod p\end{aligned}$$

این به ما می‌گوید که

$$\psi^{(m)}(x+1) = x^{p^{m-1}(p-1)} + pr(x)$$

که در آن $r(x)$ یک چندجمله‌ای با ضرایب صحیح می‌باشد. لذا تمام ضرایب $\psi^{(m)}(x+1)$، جز ضریب پیشرو ۱، بر p بخشپذیرند. اگر به نحوی می‌دانستیم که جملهٔ ثابت $h(x) = \psi^{(m)}(x+1)$ بر p^2 بخشپذیر نیست، می‌توانستیم محک آیزن اشتاین را به‌کار برده و نشان دهیم که $h(x)$ تحویل‌ناپذیر است. ولی جملهٔ ثابت $h(x) = \psi^{(m)}(x+1)$ چیست؟ این جمله چیزی جز $h(0) = \psi^{(m)}(1)$ نیست که، بنا بر شکل صریح $\psi^{(m)}(x+1)$ که در چهار بند قبل به‌دست آمد، درست مساوی p است. لذا $h(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است؛ یعنی $\psi^{(m)}(x+1)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. ولی این بی‌درنگ ایجاب می‌کند که $\psi^{(m)}(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر می‌باشد.

حال آنچه را که ثابت شده خلاصه می‌کنیم.

قضیهٔ ۲.۵.۶. چندجمله‌ای $\phi_n(x)$ به ازای $n = p^m$ که در آن p اول بوده و m یک عدد صحیح نامنفی است در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

همان‌طور که قبلاً گفتیم، این حالتی بسیار خاص از قضیه‌ای است که به‌زودی ثابت می‌شود؛ یعنی اینکه $\phi_n(x)$ به ازای جمیع اعداد صحیح مثبت n تحویل‌ناپذیر است. به‌علاوه، نتیجه و برهان قضیهٔ ۲.۵.۶ نقشی در برهان این حکم کلی که $\phi_n(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است ندارد. ولی، به‌خاطر قضیهٔ ۲.۵.۶ و شکل صریح $\phi_n(x)$ وقتی $n = p^m$، ایدهٔ خوبی از آنچه در حالت کلی برقرار است به‌دست می‌آید. حال به تحویل‌ناپذیری $\phi_n(x)$ به ازای n کلی می‌پردازیم.

قضیهٔ ۳.۵.۶. به ازای هر عدد صحیح $n \geq 1$،

$$\phi_n(x) = (x - \theta^{(1)}) \cdots (x - \theta^{(\varphi(n))})$$

که در آن $\theta^{(1)}$، $\theta^{(2)}$، ...، $\theta^{(\phi(n))}$، $\varphi(n)$ ریشهٔ nم اولیهٔ واحد متمایز می‌باشند.

برهان. به استقرا روی n عمل می‌کنیم.

هرگاه $n = 1$، آن‌گاه $\phi_1(x) = x - 1$، و چون ۱ تنها ریشهٔ اول واحد است، نتیجه در این حالت مسلماً برقرار است.

فرض کنیم نتیجه به ازای هر $m < n$ درست باشد. لذا هرگاه $d|n$ و $d \neq n$، آن‌گاه، طبق فرض استقرا، $\phi_d(x) = (x - \theta_d^{(1)})\cdots(x - \theta_d^{(\varphi(d))})$ که در آن $\theta_d^{(i)}$ها ریشه‌های dم اولیهٔ واحد می‌باشند. اما

$$x^n - 1 = (x - \zeta_1)(n - \zeta_2)\cdots(x - \zeta_n)$$

که در آن ζ_i روی تمام ریشه‌های nم واحد تغییر می‌کند. با جدا کردن ریشه‌های nم اولیهٔ واحد در این حاصلضرب داریم

$$x^n - 1 = (x - \theta^{(1)})\cdots(x - \theta^{(\varphi(n))})v(x)$$

که در آن $v(x)$ حاصلضرب $x - \zeta_i$های دیگر می‌باشد. لذا، طبق فرض استقرا، $v(x)$ حاصلضرب $\phi_d(x)$ها روی تمام مقسوم‌علیه‌های d از n بجز $d = n$ گرفته می‌شود. لذا چون

$$\phi_n(x) = \frac{(x^n - 1)}{v(x)} = \frac{(x - \theta^{(1)})\cdots(x - \theta^{(\varphi(n))})v(x)}{v(x)}$$
$$= (x - \theta^{(1)})(x - \theta^{(2)})\cdots(x - \theta^{(\varphi(n))})$$

قضیه به اثبات خواهد رسید. ■

از شکل $\phi_n(x)$ در قضیهٔ ۳.۵.۶ فوراً معلوم می‌شود که $\phi_n(x)$ یک چندجمله‌ای تکین در $\mathbb{C}[x]$ از درجهٔ $\varphi(n)$ است. با دانستن این، در واقع ثابت می‌کنیم که ضرایب $\phi_n(x)$ صحیح‌اند. چرا اینها صحیح‌اند؟ به استقرا بر n عمل کرده و فرض می‌کنیم اگر $d|n$ و $d \neq n$، این امر درست باشد. لذا هرگاه $v(x)$ چندجمله‌ای به‌کار رفته در برهان قضیهٔ ۳.۵.۶ باشد، آن‌گاه $(x^n - 1)/v(x) = \phi_n(x) \in \mathbb{C}[x]$؛ در نتیجه $v(x)|x^n - 1$ در $\mathbb{C}[x]$. ولی، طبق فرایند تقسیم طولانی، با تقسیم چندجمله‌ای تکین $x^n - 1$ با ضرایب صحیح بر $v(x)$ به یک چندجمله‌ای تکین با ضرایب صحیح (و بدون باقیمانده زیرا در $\mathbb{C}[x]$، $(v(x))|(x^n - 1)$) می‌رسیم. لذا $(x^n - 1)/v(x) = \phi_n(x)$ یک چندجمله‌ای تکین با ضرایب صحیح است. همان‌طور که دیدیم، درجه‌اش $\varphi(n)$ می‌باشد. لذا خواهیم داشت:

قضیهٔ ۴.۵.۶. چندجمله‌ای $\phi_n(x)$ به ازای هر عدد صحیح مثبت n یک چندجمله‌ای تکین با ضرایب صحیح از درجهٔ $\varphi(n)$ است که در آن φ تابع φی اویلر می‌باشد.

با دانستن اینکه $\phi_n(x)$ چندجمله‌ای است، به طریقی دیگر می‌توان دید که درجه‌اش $\varphi(n)$ است. از رابطهٔ $\phi_n(x) = (x^n - ۱)/v(x)$ با استفاده از استقرا بر n و شکل $v(x)$ معلوم می‌شود که $\deg(\phi_n(x)) = n - \deg(v(x)) = n - \sum\varphi(d)$ که در آن مجموع روی تمام مقسوم‌علیه‌های d از n غیر از $d = n$ گرفته شده است. با استمداد از قضیهٔ ۱.۲.۶ داریم $n - \sum\varphi(d) = \varphi(n)$ که این مجموع نیز روی تمام $d|n$ها که $d \neq n$ گرفته می‌شود. لذا خواهیم داشت $\deg(\phi_n(x)) = \varphi(n)$.

نتیجه‌ای که اینک به‌دست می‌آوریم بی‌شک یکی از اساسی‌ترین نتایج راجع به چندجمله‌ایهای دایره بر است.

قضیهٔ ۵.۵.۶. چندجمله‌ای $\phi_n(x)$ به ازای هر عدد صحیح مثبت n در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

برهان. فرض کنیم $f(x)$ یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{Q}[x]$ باشد به‌طوری که $f(x)|\phi_n(x)$. لذا، به ازای $g(x)$ی در $\mathbb{Q}[x]$، $\phi_n(x) = f(x)g(x)$. بنا بر لم گاوس، می‌توان فرض کرد که هر دوی $f(x)$ و $g(x)$ چندجمله‌ایهایی تکین با ضرایب صحیح‌اند؛ لذا در $\mathbb{Z}[x]$ می‌باشند. هدف ما نشان دادن $\phi_n(x) = f(x)$ می‌باشد. هرگاه چنین باشد، آن‌گاه، چون $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است، $\phi_n(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر می‌باشد.

چون $\phi_n(x)$ ریشهٔ چندگانه ندارد، $f(x)$ و $g(x)$ باید نسبت به هم اول باشند. فرض کنیم عدد اول p چنان باشد که p، n را عاد نکند. اگر θ ریشه‌ای از $f(x)$ باشد، ریشه‌ای از $\phi_n(x)$ نیز هست. پس، طبق قضیهٔ ۳.۵.۶، θ یک ریشهٔ nم اولیهٔ واحد می‌باشد. چون p نسبت به n اول است، θ^p نیز یک ریشهٔ nم اولیهٔ واحد می‌باشد. لذا، طبق قضیهٔ ۳.۵.۶، θ^p ریشهٔ $\phi_n(x)$ می‌باشد. بنا براین داریم $\phi_n(\theta^p) = f(\theta^p)g(\theta^p) = ۰$، که از آن $f(\theta^p) = ۰$ یا $g(\theta^p) = ۰$ نتیجه می‌شود.

هدف ما نشان دادن $f(\theta^p) = ۰$ است. فرض کنیم چنین نباشد. پس داریم $g(\theta^p) = ۰$. لذا θ یک ریشهٔ $g(x^p)$ است. چون θ ریشهٔ چندجمله‌ای تحویل‌ناپذیر $f(x)$ نیز هست، از لم ۲.۳.۶ داریم $f(x)|g(x^p)$. همان‌طور که در جریان اثبات قضیهٔ ۲.۵.۶ دیدیم،

$$g(x^p) \equiv g(x)^p \bmod p$$

فرض کنیم J ایده‌آل تولید شده به‌وسیلهٔ p در $\mathbb{Z}$ باشد. بنا بر نتیجهٔ لم ۲.۶.۴،

$$\mathbb{Z}[x]/J[x] \simeq \mathbb{Z}_p[x]$$

بدین معنی که تحویل ضرایب هر چندجمله‌ای $\bmod p$ یک همریختی از $\mathbb{Z}[x]$ به روی $\mathbb{Z}_p[x]$ می‌باشد.

از آنجا که تمام چندجمله‌ایهای $\phi_n(x)$، $v(x)$، $f(x)$، و $g(x)$ در $\mathbb{Z}[x]$اند، اگر $\bar{\phi}_n(x)$، $\bar{v}(x)$، $\bar{f}(x)$، و $\bar{g}(x)$ نقشهای آنها در $\mathbb{Z}_p[x]$ باشند، با رفتن به $\bmod p$ تمام روابط بین آنها حفظ می‌شود. لذا روابط $x^n - ۱ = \phi_n(x)\bar{v}(x)$، $\bar{\phi}_n(x) = \bar{f}(x)\bar{g}(x)$، و $\bar{f}(x)|\bar{g}(x^p) = \bar{g}(x)^p$ را خواهیم داشت.

بنابراین $\bar{f}(x)$ و $\bar{g}(x)$ در توسیعی مانند K از $\mathbb{Z}_p$ ریشهٔ مشترکی مانند a دارند. اما $\bar{f}(x)\bar{g}(x) = \bar{\phi}_n(x)\bar{v}(x) = x^n - ۱$. لذا a به‌عنوان ریشه‌ای از هر دوی $\bar{f}(x)$ و $\bar{g}(x)$ یک ریشهٔ چندگانهٔ $x^n - ۱$ است. ولی مشتق صوری $(x^n - ۱)'$ از $x^n - ۱$ مساوی $nx^{n-۱} \neq ۰$ است زیرا p عدد n را عاد نمی‌کند. لذا $(x^n - ۱)'$ نسبت به $x^n - ۱$ اول می‌باشد. بنا بر مسئلهٔ ۳ از بخش ۳، چندجمله‌ای $x^n - ۱$ نمی‌تواند ریشهٔ چندگانه داشته باشد. پس فرض اینکه θ^p ریشهٔ $f(x)$ نیست به این تناقض می‌خورد و نتیجه می‌شود که هرگاه θ یک ریشهٔ $f(x)$ باشد، آن‌گاه به ازای هر pی اولی که n را عاد نکند، θ^p باید یک ریشه باشد.

با تکرار این استدلال به این نتیجه می‌رسیم که به ازای هر عدد صحیح r که نسبت به n اول باشد، θ^r یک ریشهٔ $f(x)$ می‌باشد. اما، به‌عنوان یک ریشهٔ $f(x)$، ریشه‌ای از $\phi_n(x)$ است؛ در نتیجه یک ریشهٔ nم اولیهٔ واحد می‌باشد. لذا θ^r نیز به ازای هر r نسبت به n اول ریشهٔ nم اولیهٔ واحد می‌باشد. با تغییر تمام rهای نسبت به n اول، هر ریشهٔ nم اولیهٔ واحد را به‌عنوان یک چنین θ^r اختیار می‌کنیم. لذا تمام ریشه‌های nم اولیهٔ واحد ریشه‌های $f(x)$ می‌باشند. پس از قضیهٔ ۳.۵.۶ معلوم می‌شود که $\phi_n(x) = f(x)$؛ در نتیجه $\phi_n(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر می‌باشد. ■

ممکن است به نظر خواننده استفاده از $\bmod p$ برای اثبات تحویل‌ناپذیری یک چندجمله‌ای با ضرایب گویا غیرطبیعی باشد. در واقع ممکن است چنین باشد. ولی تا جایی که می‌دانیم برهانی از تحویل‌ناپذیری $\phi_n(x)$ که کاملاً در $\mathbb{Q}[x]$ بوده و به $\bmod p$ پناه نبرده باشد وجود ندارد. داشتن یک چنین برهان حس زیباشناسی ما را اقناع می‌سازد. از آن‌سو، این تنها موردی که یک نتیجه با توسل به یک دستگاه کمکی مرتبط به‌دست می‌آید نیست. بسیاری از قضایا در نظریهٔ اعداد (راجع به اعداد صحیح معمولی) در برهانهایشان از اعداد صحیح $\bmod p$ استفاده می‌کنند.

از آنجا که $\phi_n(x)$ یک چندجمله‌ای تکین با ضرایب صحیح بوده و در $\mathbb{Q}[x]$ تحویل‌ناپذیر است و نیز θ_n، یعنی ریشهٔ nم اولیهٔ واحد، ریشهٔ $\phi_n(x)$ می‌باشد، خواهیم داشت:

قضیهٔ ۶.۵.۶. $\phi_n(x)$ چندجمله‌ای مینیمال ریشه‌های nم اولیهٔ واحد در $\mathbb{Q}[x]$ می‌باشد.

مسائل

۱. مستقیماً تحقیق کنید که شش چندجمله‌ای دایره بر اول در $\mathbb{Q}[x]$ تحویل‌ناپذیرند.

۲. شکلهای صریح
الف) $\phi_{10}(x)$،
ب) $\phi_{15}(x)$،
پ) $\phi_{20}(x)$
را بنویسید.

۳. اگر $(x^m - 1)|(x^n - 1)$، ثابت کنید $m|n$.

۴. اگر $a > 1$ یک عدد صحیح بوده و $(a^m - 1)|(a^n - 1)$، ثابت کنید $m|n$.

۵. اگر K یک توسیع متناهی میدان اعداد گویای $\mathbb{Q}$ باشد، ثابت کنید تنها تعدادی متناهی ریشهٔ واحد در K وجود دارند. (راهنمایی. از مسئلهٔ ۱۰ در بخش ۲ همراه با قضیهٔ ۶.۵.۶ استفاده کنید.)

۶. محک لیوویل

به یاد آورید که یک عدد مختلط را جبری از درجهٔ n گوییم اگر ریشهٔ یک چندجمله‌ای از درجهٔ n روی میدان اعداد گویای $\mathbb{Q}$ بوده و ریشهٔ هیچ چندجمله‌ای از این نوع و از درجهٔ کمتر از n نباشد. با اصطلاحات فصل ۵، یک عدد جبری عددی مختلط و جبری روی $\mathbb{Q}$ می‌باشد.

هر عدد مختلط که جبری نباشد متعالی نام دارد. بعضی از اعداد آشنا مانند e، π، e^π، و بسیاری دیگر متعالی‌اند. حدس می‌زنند که اعداد آشنای دیگر مانند $e+\pi$، $e\pi$، و π^e متعالی‌اند. ولی این امر تا به حال ثابت نشده است.

ژوزف لیوویل (Joseph Liouville, 1809-1882)، ریاضیدان فرانسوی، محکی ارائه داد که هر عدد جبری از درجهٔ n باید در آن صدق کند. این محک شرطی دارد که میزان تقریب یک

عدد جبری حقیقی از درجهٔ n به اعداد گویا را محدود می‌سازد و از چنان سرشتی برخوردار است که به آسانی می‌توان اعدادی ساخت که محک را به ازای هر $n > 0$ ناکام سازد. در این صورت هر چنین عددی متعالی خواهد بود. بدین ترتیب می‌توان اعداد متعالی را به‌دلخواه تولید کرد. با این‌حال تعالی هیچیک از اعداد آشنا را نمی‌توان با محک لیوویل اثبات نمود.

در این بخش محک لیوویل را ارائه می‌دهیم. اثبات این نتیجه به طرز تعجب‌آوری ساده و مقدماتی است. اما این چیزی از ارزشش نکاسته و بلکه آن را بالا خواهد برد.

قضیهٔ ۱.۶.۶ (لیوویل). فرض کنیم a یک عدد جبری از درجهٔ $n \geq 2$ باشد (یعنی a جبری است ولی گویا نیست). در این صورت یک ثابت مثبت مانند c (که فقط تابع a است) وجود دارد به‌طوری که به ازای هر دو عدد صحیح u و v که $v > 0$، $|a - u/v| > c/v^n$.

برهان. فرض کنیم a ریشهٔ چندجمله‌ای $f(x)$ از درجهٔ n در $\mathbb{Q}[x]$ باشد که در آن $\mathbb{Q}$ میدان اعداد گویا می‌باشد. با از بین بردن مخرجها در ضرایب $f(x)$ می‌توان فرض کرد $f(x) = r_0x^n + r_1x^{n-1} + \cdots + r_n$ که در آن تمام r_iها صحیح بوده و $r_0 > 0$.

چون چندجمله‌ای $f(x)$ تحویل‌ناپذیر و از درجهٔ n است، n ریشهٔ متمایز مانند $a = a_1$، a_2، $\cdots$، a_n در میدان اعداد مختلط $\mathbb{C}$ دارد. لذا $f(x)$ روی $\mathbb{C}$ به‌صورت

$$f(x) = r_0(x - a)(x - a_2)\cdots(x - a_n)$$

تجزیه می‌شود. فرض کنیم u و v صحیح بوده و $v > 0$، پس داریم

$$f\left(\frac{u}{v}\right) = \frac{r_0u^n}{v^n} + \frac{r_1u^{n-1}}{v^{n-1}} + \cdots + \frac{r_{n-1}u}{v} + r_n$$

در نتیجه

$$v^nf\left(\frac{u}{v}\right) = r_0u^n + r_1u^{n-1}v + \cdots + r_{n-1}uv^{n-1} + r_nv^n$$

صحیح است. به‌علاوه، چون $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر از درجهٔ $n \geq 2$ است، $f(x)$ ریشهٔ گویا ندارد؛ در نتیجه $v^nf(u/v)$ یک عدد صحیح ناصفر است که از آنجا $|v^nf(u/v)| \geq 1$. با استفاده از شکل تجزیهٔ $f(x)$ داریم

$$f\left(\frac{u}{v}\right) = r_0\left(\left(\frac{u}{v}\right) - a\right)\left(\left(\frac{u}{v}\right) - a_2\right)\cdots\left(\left(\frac{u}{v}\right) - a_n\right)$$

در نتیجه

$$\left|\left(\frac{u}{v}\right)-a\right|=\frac{|f(u/v)|}{r.|(u/v)-a_۲|\cdots|(u/v)-a_n|}$$
$$=\frac{v^n|f(u/v)|}{r.v^n|(u/v)-a_۲|\cdots|(u/v)-a_n|}$$
$$\geq\frac{۱}{r.v^n|(u/v)-a_۲|\cdots|(u/v)-a_n|}$$

فرض کنیم s ماکزیمم $|a|$، $|a_۲|$، $\cdots$، $|a_n|$ باشد. دو حالت در نظر می‌گیریم: $|u/v|>۲s$ یا $|u/v|\leq ۲s$. هرگاه $|u/v|>۲s$، آن‌گاه، بنا بر نامساوی مثلثی،

$$|a-(u/v)|\geq|u/v|-|a|>۲s-s=s$$

و، چون $v\geq ۱$، $|a-(u/v)|>s/v^n$.

از آن‌سو، هرگاه $|u/v|\leq ۲s$، آن‌گاه، مجدداً طبق نامساوی مثلثی،

$$|a_i-(u/v)|\leq|a_i|+|u/v|\leq s+۲s=۳s$$

بنابراین،

$$t=\left|a_۲-\left(\frac{u}{v}\right)\right|\cdots\left|a_n-\left(\frac{u}{v}\right)\right|\leq(۳s)^{n-۱}$$

در نتیجه $۱/t\geq ۱/(۳s)^{n-۱}=۱/(۳^{n-۱}s^{n-۱})$. با مراجعه به نامساوی فوق که

$$|a-(u/v)|\geq ۱/[r.v^n|a_۲-(u/v)|\cdots|a_n-(u/v)|]$$

داریم $|a-(u/v)|\geq ۱/(r.۳^{n-۱}s^{n-۱}v^n)$. اعداد r، $۳^{n-۱}$، $s^{n-۱}$ یک بار و برای همیشه به‌وسیلهٔ a و چندجمله‌ای مینیمالش $f(x)$ معین می‌شوند و تابع u یا v نیستند. هرگاه قرار دهیم $b=۱/(r.۳^{n-۱}s^{n-۱})$، آن‌گاه $b>۰$ و $|a-(u/v)|>b/v^n$. این حالت دوم را که $(u/v)\leq ۲s$ سامان خواهد داد.

اگر c عدد مثبتی کوچکتر از هر دوی b و s باشد، از بحث فوق نتیجه می‌شود که به ازای هر دو عدد صحیح u و v که $v>۰$، $|a-u/v|>c/v^n$ و بدین‌ترتیب قضیه به ثبوت می‌رسد. ■

اکنون به حالت خاص $a=\sqrt{۲}$ در برهان می‌پردازیم. چندجمله‌ای مینیمال a در $\mathbb{Q}[x]$ عبارت است از $f(x)=(x-a)(x+a)$؛ در نتیجه $a=a_۱$ و $a_۲=-a$. لذا هرگاه u و v

صحیح بوده و $v > 0$، آن‌گاه

$$v^2 f\left(\frac{u}{v}\right) = v^2\left(\left(\frac{u}{v}\right)^2 - a^2\right) = v^2\left(\left(\frac{u}{v}\right)^2 - 2\right) = u^2 - 2v^2 \neq 0$$

یک عدد صحیح است. در نتیجه $|u^2 f(u/v)| \geq 1 \geq 1/v^2$. s فوق ماکزیمم $|\sqrt{2}|$ و $|-\sqrt{2}|$ است؛ یعنی $s = \sqrt{2}$. همچنین bی فوق مساوی است با $1/(3^{2-1}(\sqrt{2})^{2-1}) = 1/(3\sqrt{2})$؛ در نتیجه هرگاه c عدد مثبتی کوچکتر از $1/(3\sqrt{2})$ باشد، آن‌گاه $|\sqrt{2} - u/v| > c/v^2$.

آنچه قضیه می‌گوید به قرار زیر است: هر عدد حقیقی جبری اعدادی گویا به قدرکافی نزدیک به خود دارد (این امر برای تمام اعداد حقیقی درست است)، ولی اگر این عدد حقیقی جبری a از درجهٔ $n \geq 2$ باشد، برای تقریب a به اعداد گویا محدودیتهایی موجود است. این شروط همانهایی است که قضیهٔ لیوویل اعمال می‌کند.

چگونه می‌توان با این نتیجه اعداد متعالی تولید کرد؟ کافی است مثلاً عدد حقیقی τ را چنان تولید کنیم که به ازای عدد صحیح مثبت دلخواه n و عدد صحیح مثبت دلخواه c بتوان اعداد صحیح u و v را با $v > 0$ چنان یافت که $|\tau - u/v| < c/v^n$. این τ را می‌توان با نوشتن بسط اعشاری نامتناهی مستلزم ۰ و ۱ که در آن ۰ها بین ۱ها به سرعت پخش می‌شوند به آسانی یافت. مثلاً $\tau = 0/1010010000000010\ldots010\ldots$ که در آن ۰ها بین ۱های متوالی به‌صورت $m!$ قرار دارند عددی است که محک لیوویل را به ازای هر $n > 0$ نقض می‌کند. (رک. مسئلهٔ ۳ در بخش ۳). لذا τ متعالی می‌باشد.

البته می‌توان توزیعهای دیگری از ۰ها بین ۱ها، مثلاً m^m، $(m!)^2$، و غیره، را نیز به‌کار برد و اعداد متعالی به‌دست آورد. همچنین به‌جای استفاده از ۱ می‌توان هر یک از نه رقم ناصفر را برای به‌دست آوردن اعداد متعالی دیگر به‌کار برد. اثبات عدم صادق بودن این اعداد در محک لیوویل به ازای هر عدد صحیح مثبت n و هر عدد مثبت c به خواننده واگذار می‌شود.

با استفاده از عدد متعالی τ و صورتهای توصیف شده‌اش می‌توان نتیجهٔ مشهوری از کانتور (Cantor) را به‌دست آورد. این نتیجه می‌گوید که تناظر یک‌به‌یکی بین جمیع اعداد حقیقی و مجموعهٔ اعداد متعالی حقیقی وجود دارد. به بیان دیگر، به تعداد اعداد حقیقی اعداد متعالی خواهیم داشت. ما طرح اثبات این امر را بازگو کرده و جزئیات را به خواننده وا می‌گذاریم.

اولاً ساختن یک نگاشت ۱-۱ از اعداد حقیقی به روی اعداد حقیقی که اکیداً بین ۰ و ۱ اند آسان است (سعی کنید این نگاشت را بیابید). این امر برای اعداد متعالی حقیقی و اعداد متعالیی که اکیداً بین ۰ و ۱ اند نیز درست است. فرض کنیم مجموعهٔ اول A و مجموعهٔ دوم B باشد. حال یک نگاشت ۱-۱ از A به توی B می‌سازیم. این برای تمام کردن کار کافی خواهد بود.

هر عدد در A را می‌توان به‌صورت بسط اعشاری نامتناهی $\circ/a_1a_2\cdots a_n\cdots$ نوشت که در آن a_iها بین ۰ و ۹ قرار دارند. (ما در اینجا کمی نادقیق عمل می‌کنیم. بر خواننده است که استدلال را دقیقتر جلو ببرد.) نگاشت f از A به B را با $f(\circ/a_1a_2\cdots a_n\cdots)=\circ/a_1\circ a_2\circ\circ a_3\circ\circ\circ\circ\circ\circ a_4\cdots$ تعریف می‌کنیم. بنا بر محک لیوویل، جز در مورد مجموعهٔ کوچکی از a_1، a_2، $\cdots$، a_n، $\cdots$، اعداد $\circ/a_1\circ a_2\circ\circ a_3\circ\circ\circ\circ\circ\circ a_4\cdots$ متعالی‌اند. در این صورت f فوق نگاشت مطلوب خواهد بود.

آخرین کلام در باب نوع تقریب اعداد جبری به‌وسیلهٔ اعداد گویا که در قضیهٔ ۱.۶.۶ بیان شده است. در آنجا هرگاه a یک عدد جبری حقیقی از درجهٔ $n \geq 2$ باشد، آن‌گاه به ازای cی مثبت مناسبی، $|a-u/v|>c/v^n$. اگر بتوان n را تا $m<n$ به ازای $|a-u/v|>c/v^m$ و cی مناسبی (تابع a و m) کاهش داد، می‌توان نتیجهٔ قویتری به‌دست آورد. در سال ۱۹۵۵، کا. اف. روت (K.F. Roth)، ریاضیدان جوان انگلیسی، نتیجهٔ توانایی را ثابت کرد که با آن می‌توان n را تا ۲ تقلیل داد. نتیجهٔ دقیق وی به قرار زیر است: هرگاه a جبری از درجهٔ $n \geq 2$ باشد، آن‌گاه به ازای هر عدد حقیقی $r>2$ ثابت مثبتی مانند c تابع a و r هست به‌طوری که به ازای همه جز تعدادی متناهی کسر u/v، $|a-u/v|>c/v^r$.

۷. گنگ بودن π

همان‌طور که قبلاً گفتیم، در سال ۱۸۸۲ لیندمان ثابت کرد که π یک عدد متعالی است. به‌خصوص از این نتیجه می‌شود که π گنگ است. ما در اینجا متعالی بودن π را ثابت نمی‌کنیم (اثباتش ما را خیلی از بحث دور می‌سازد) ولی لااقل ثابت می‌کنیم که π گنگ است. برهان زیبایی که از این امر می‌آوریم به آی.نیون (I. Niven) منسوب است که در مقاله‌اش

"*A Simple Proof That π Is Irrational*"

آمده است. این مقاله در

Bulletin of the American Mathematical Society, Vol. 53(1947), p.509

به چاپ رسیده است. برای درک برهان نیون فقط به چند مطلب از درس حساب دیفرانسیل و انتگرال متعارف در سال اول نیاز خواهد بود.

بحث را با لم زیر آغاز می‌کنیم.

لم ۱.۷.۶. هرگاه u یک عدد حقیقی باشد، آن‌گاه $\lim_{n\to\infty} u^n/n! = \circ$.

برهان. هرگاه u یک عدد حقیقی باشد، آن‌گاه e^u یک عدد حقیقی تعریف شده بوده و

$$e^u = 1 + u + u^2/2! + u^3/3! + \cdots + u^n/n! + \cdots$$

سری $1 + u + u^2/2! + \cdots + u^n/n! + \cdots$ به e^u همگراست. چون این سری همگراست، جملهٔ nمش باید به ۰ برود. لذا $\lim_{n\to\infty} u^n/n! = 0$. ■

حال برهان نیون راجع به گنگ بودن π را ارائه می‌دهیم.

قضیهٔ ۲.۷.۶. π یک عدد گنگ است.

برهان. فرض کنیم π گویا باشد. پس $\pi = a/b$ که در آن a و b صحیح و مثبت می‌باشند. به ازای هر عدد صحیح $n > 0$ یک چندجمله‌ای بر مبنای فرض $\pi = a/b$ معرفی می‌کنیم که خواصش ما را به نتیجهٔ مطلوب می‌رسانند. خواص اصلی این چندجمله‌ای به ازای جمیع nهای مثبت برقرار است. روش اثبات انتخاب مناسب n در جای مناسبی از برهان است.

فرض کنیم $f(x) = x^n(a - bx)^n/n!$ که در آن $\pi = a/b$. این یک چندجمله‌ای از درجهٔ $2n$ با ضرایب گویاست. آن را بسط می‌دهیم:

$$f(x) = \frac{a_0x^n + a_1x^{n+1} + \cdots + a_nx^{2n}}{n!}$$

که در آن

$$a_n = (-1)^n b^n ، \cdots ، a_i = \frac{(-1)^i n!}{i!(n-i)!}a^{n-i}b^i ، \cdots ، a_1 = -na^{n-1}b ،a_0 = a^n$$

صحیح می‌باشند.

ما مشتق iم $f(x)$ نسبت به x را با نماد متداول $f^{(i)}(x)$ نشان داده و $f^{(0)}(x)$ را به معنی خود $f(x)$ می‌گیریم.

ابتدا به خاصیت تقارن $f(x)$ توجه می‌کنیم؛ یعنی $f(x) = f(\pi - x)$. برای مشاهدهٔ این امر توجه می‌کنیم که $f(x) = (b^n/n!)x^n(\pi - x)^n$ که از شکل آن واضح است که $f(x) = f(\pi - x)$. چون این امر برای $f(x)$ برقرار است، از قاعدهٔ زنجیره‌ای برای مشتقگیری به آسانی معلوم می‌شود که $f^{(i)}(x) = (-1)^i f^{(i)}(\pi - x)$.

از این امر راجع به $f(x)$ و تمام مشتقاتش نتیجه می‌شود که به ازای احکامی که راجع به سرشت تمام $f^{(i)}(0)$ ها بیان شود، احکام مناسبی راجع به تمام $f^{(i)}(\pi)$ها وجود دارند.

ما به $f^{(i)}(\circ)$ و $f^{(i)}(\pi)$ به ازای جمیع iهای نامنفی علاقمندیم. توجه کنید که از شکل بسط یافتهٔ $f(x)$ مذکور در فوق به آسانی معلوم می‌شود که $f^{(i)}(\circ)$ چیزی جز $i!$ برابر ضریب x^i در چندجمله‌ای $f(x)$ نیست. این فوراً ایجاب می‌کند که، چون پایین‌ترین توان x در $f(x)$ مساوی n است، پس اگر $i < n$، $f^{(i)}(\circ) = \circ$. به ازای $i \geq n$ داریم $f^{(i)}(\circ) = i!a_{i-n}/n!$. چون $i \geq n$، $i!/n!$ یک عدد صحیح است و، همان‌طور که در بالا گفتیم، a_{i-n} نیز صحیح می‌باشد. لذا $f^{(i)}(\circ)$ به ازای هر عدد صحیح نامنفی i صحیح می‌باشد. چون $f(\circ)^i(-\backslash)^i f(\circ)$... $f^{(i)}(\pi) = (-\text{۱})^i f^{(i)}(\circ)$، $f^{(i)}(\pi)$ به ازای جمیع اعداد صحیح نامنفی i صحیح می‌باشد.

حال تابع کمکی زیر را معرفی می‌کنیم:

$$F(x) = f(x) - f^{(\text{۲})}(x) + \cdots + (-\text{۱})^n f^{(\text{۲}n)}(x)$$

چون به ازای $m > \text{۲}n$ داریم $f^{(m)}(x) = \circ$، معلوم می‌شود که

$$\begin{aligned}\frac{d^{\text{۲}}F}{dx^{\text{۲}}} &= F''(x) = f^{(\text{۲})}(x) - f^{(\text{۴})}(x) + \cdots + (-\text{۱})^n f^{(\text{۲}n)}(x)\\ &= -F(x) + f(x)\end{aligned}$$

بنابراین

$$\begin{aligned}\frac{d}{dx}(F'(x)\sin x - F(x)\cos x) &= F''(x)\sin x + F'(x)\cos x\\ &\quad - F'(x)\cos x + F(x)\sin x\\ &= (F''(x) + F(x))\sin x = f(x)\sin x\end{aligned}$$

از این نتیجه می‌گیریم که

$$\begin{aligned}\int_\circ^\pi f(x)\sin x\,dx &= [F'(x)\sin x - F(x)\cos x]_\circ^\pi\\ &= (F'(\pi)\sin\pi - F(\pi)\cos\pi) - (F'(\circ)\sin\circ - F(\circ)\cos\circ)\\ &= F(\pi) + F(\circ)\end{aligned}$$

ولی از شکل $F(x)$ در فوق و اینکه تمام $f^{(i)}(\circ)$ها و $f^{(i)}(\pi)$ها صحیح‌اند نتیجه می‌گیریم که $F(\pi) + F(\circ)$ صحیح می‌باشد. لذا $\int_\circ^\pi f(x)\sin x\,dx$ صحیح می‌باشد. این حکم راجع به $\int_\circ^\pi f(x)\sin x\,dx$ به ازای هر عدد صحیح $n > \circ$ برقرار است. حال می‌خواهیم n را زیرکانه طوری اختیار کنیم که حکم «$\int_\circ^\pi f(x)\sin x\,dx$ یک عدد صحیح است» نتواند درست باشد.

حال $\int_0^\pi f(x)\sin x dx$ را تخمین می‌زنیم. به ازای $0 < x < \pi$ داریم

$$f(x) = x^n(a-bx)^n/n! \le \pi^n a^n/n!$$

(زیرا $a > 0$)، و نیز $0 < \sin x \le 1$. لذا

$$0 < \int_0^\pi f(x)\sin x dx < \int_0^\pi \pi^n a^n/n! dx = \pi^{n+1}a^n/n!$$

فرض کنیم $u = \pi a$. پس، طبق لم ۶.۷.۱، $\lim_{n\to\infty} u^n/n! = 0$؛ در نتیجه اگر n را به قدر کافی بزرگ اختیار کنیم، می‌توان مطمئن بود که $u^n/n! < 1/\pi$. لذا $\pi^{n+1}a^n/n! = \pi u^n/n! < 1$. ولی در این صورت $\int_0^\pi f(x)\sin x dx$ اکیداً بین ۰ و ۱ می‌باشد. ولی، بنا بر آنچه نشان داده‌ایم، $\int_0^\pi f(x)\sin x dx$ یک عدد صحیح است. چون عدد صحیحی اکیداً بین ۰ و ۱ نیست، پس به تناقض رسیده‌ایم. لذا فرض گویا بودن π نادرست است و π گنگ می‌باشد. این امر برهان قضیه را تمام خواهد کرد. ∎

واژه‌نامه انگلیسی-فارسی

automorphism	خودریختی
bijection	بیژکسیون
centralizer	مرکزساز
characteristic	مشخص
chinese remainder	باقیماندهٔ چینی
commuting	تعویض
composition	ترکیب
conjugacy	تزویج
constructibility	ترسیم‌پذیری
constructible	ترسیم‌پذیر
coset	هم‌مجموعه
cyclotomic	دایره‌بر
extension	توسیع
homomorphism	همریختی

identity	همانی (اتحاد)
injective	انژکتیو
irreducible	تحویل‌ناپذیر
isomorphic	یکریخت
isomorphism	یکریختی
kernel	هسته
mapping	نگاشت
maximal	ماکزیمال
minimal	مینیمال
monic	تکین
multiplicity	بستایی
nonresidue	غیرمانده
onto	برو
permutation	جایگشت
quaternion	چهارگان
residue	مانده
surjective	سورژکتیو
transitivity	تعدی
transposition	ترانهش

واژه‌نامه فارسی-انگلیسی

انژکتیو	injective
باقیماندهٔ چینی	chinese remainder
برو	onto
بستایی	multiplicity
بیژکسیون	bijection
تحویل‌ناپذیر	irreducible
ترانهش	transposition
ترسیم‌پذیر	constructible
ترسیم‌پذیری	constructibility
ترکیب	composition
تزویج	conjugacy
تعدی	transitivity
تعویض	commuting
تکین	monic
توسیع	extension

جایگشت	permutation
چهارگان	quaternion
خودریختی	automorphism
دایره‌بر	cyclotomic
سورژکتیو	surjective
غیرمانده	nonresidue
ماکزیمال	maximal
مانده	residue
مرکزساز	centralizer
مشخص	characteristic
مینیمال	minimal
نگاشت	mapping
هسته	kernel
همانی	identity
همریختی	homomorphism
هم‌مجموعه	coset
یکریخت	isomorphic
یکریختی	isomorphism

فهرست راهنما

فهرست علایم