ف. ج. هیگینز

نخستین درس در جبر مجرد

ترجمهٔ
محمدرضا رجب‌زاده مقدم

نخستین درس در جبر مجرد

تألیف: ف. ج. هیگینز

ترجمه: محمد رضا رجب‌زادهٔ مقدم

مرکز نشر دانشگاهی، تهران

A FIRST COURSE IN ABSTRACT ALGEBRA
P. J. Higgins, Van Nostrand Reinhold Company Limited, 1975.

نخستین درس در جبر مجرد
تألیف : ف. ج. هیگینز
ترجمهٔ محمدرضا رجب‌زادهٔ مقدم
ویراستاران : شادروان حمید کاظمی، همایون معین
مرکز نشر دانشگاهی، تهران
چاپ اول ۱۳۶۲
چاپ دوم ۱۳۷۶
تعداد ۳۰۰۰
چاپ و صحافی : معراج

فهرستنویسی پیش از انتشار کتابخانهٔ ملی جمهوری اسلامی ایران

هیگینز، فیلیپ، ۱۹۲۶ - Higgins, Philip J.
نخستین درس در جبر مجرد / تألیف ف. ج. هیگینز؛ ترجمهٔ محمدرضا رجب‌زاده مقدم؛ ویراستاران حمید کاظمی، همایون معین. ــ تهران : مرکز نشر دانشگاهی، ۱۳۷۶.
هشت، [۲۰۹] ص. ــ (مرکز نشر دانشگاهی؛ ۵۸. ریاضی و آمار و کامپیوتر؛ ۶)
ISBN 964-01-0058-7
فهرستنویسی براساس اطلاعات فیپا (فهرستنویسی پیش از انتشار).
عنوان اصلی : A first course in abstract algebra
این کتاب در سال ۱۳۶۲ توسط ستاد انقلاب فرهنگی، مرکز نشر دانشگاهی منتشر گردیده است.
واژه‌نامه.
کتابنامه : ص. [۲۰۹].
چاپ ۲؟
۱. جبر مجرد. الف. رجب‌زاده مقدم، محمدرضا، ۱۳۲۴ ــ ، مترجم. ب. مرکز نشر دانشگاهی. ج. عنوان.
۳ ن ۹ م / QA ۱۶۲ ۵۱۲/۰۲
۱۳۷۶
کتابخانهٔ ملی ایران ۷۶-۶۸۶۹م

فهرست مطالب

بسم الله الرحمن الرحیم

مقدمهٔ مترجم

این کتاب کـه متن اصلی آن چندسالـی است در دانشکده‌هـای ریاضی دانشگاه لندن به دانشجویان دورهٔ کارشناسی (دورهٔ لیسانس) ریاضی تدریس می‌شود، کتابی است جـامع که تقریباً تمام مطالب موردنیاز برای مطالعهٔ نخستین درس جبر را دربردارد، و بسیاری از صاحبنظران آن‌را برای تدریس دراین‌زمینه مناسب تشخیص داده و توصیه کرده‌انـد. نظر به‌اهمیت‌موضوع و همچنین نیاز به‌متون فارسی، درسال ۱۳۵۷ برآن‌شدم تاآن را به‌فارسی برگردانم واکنون خوشحالم که متن ترجمه پس‌از ویرایش‌چاپ‌شده ودر اختیار علاقه‌مندان قرار می‌گیرد.

هنگام‌ترجمه سعی‌شده است ازمیان واژه‌های موجود بهترین آنها انتخاب شود.هرجا (برای اولین‌بار) به‌نام دانشمندی برخورد شده املای لاتین آن درپاورقی آمده است. لازم به‌تذکر است که در اصل کتاب، هرجاکـه به‌منبعی اشاره شده، مشخصات کامـل‌آن در متن کتاب آمده است. لیکن درترجمه بهترآن دیدیم که همه این منابع‌را در آخـر کتاب تحت عنوان «منابع» و به‌ترتیب حروف الفبای نـام نویسندگان بیاوریم ودرمتن‌کتاب هریك از منابع فقط بایك‌شماره مشخص شده است. ضمناً اشتباهاتی درمتن اصلی کتاب وجود داشته که در ترجمه اصلاح شده است.

دراینجا لازم می‌دانم از تمام کسانی‌که به‌نحوی در چاپ این‌کتاب سهمی داشته‌اند تشکر وقدردانی‌نمایم. بخصوص ازآقایان دکتر نصرالله پورجوادی مدیرمرکز نشردانشگاهی و دکترعلی‌اکبر جعفریان مسئول گروه ریاضی آن‌مرکز، بخاطر تسهیلاتی‌که فراهم آورده‌اند کمال‌تشکر را دارم. یاد مرحـوم حمید کاظمی را که چندفصلی ازاین کتاب را ویـرایش نموده است‌گرامی می‌دارم. زحمات‌آقای همایون معین‌را جهت ویراستاری بقیه کتاب‌ارج می‌نهم. کارکنان واحدتولیدمرکز نشردانشگاهی‌وحروفچینان چاپخانهٔ مجتمع ادبیات و علوم انسانی‌که کارحروفچینی را بادقت‌انجام داده‌اند، قدردانی‌می‌کنم. بالاخره کارآقای احمد

برادران، مربی گروه ریاضی دانشگاه مشهد، را کـه فهرست راهنما و واژه‌های کتاب را به‌کمك کامپیوتر مرتب نموده است فراموش نمی‌کنم.

درخـاتمه، از خوانندگـان وعلاقه‌مندان تقاضا دارد چنانچه به‌لغزشهایـی درترجمه برخوردند، منتی براینجانب نهند ومرا آگاه کنند تابتوان در چاپهای بعدی، کتابی‌که حاوی نقایص کمتری بـاشد در اختیار علاقه‌مندان قـرار داد. قبلا ازابراز این‌مساعـدت نهایت سپاسگزاری را دارم.

والسلام ـ محمدرضا رجب‌زاده‌مقدم
خردادماه ۱۳۶۲
گروه ریاضی ـ دانشگاه مشهد

پیشگفتار مؤلف

به‌دنبال اولین برخورد دانشجو باهرمفهوم‌جدید ریاضی وباحداقل فاصله بایستی‌کاربردهایی ازآن مطالعه شود تاعلت معرفی‌آن را بیان‌کند. نیل به‌این هدف درمورد گروهها، حلقه‌ها و میدانهاکه موضوع اصلی این کتاب را تشکیل می‌دهند، مشکلاتی دارد. از یك طرف برای یك درس مقدماتی طرح‌کاربردهای واقعاً مهم درمسائلی مانند حل‌معادلات به‌وسیلهٔ رادیکالها یارده‌بندی سطوح، خیلی مشکل می‌نمایند. ازطرف دیگر،کاربردهایی که درمراحل مقدماتی قابل درك‌اند، عمدتاً مربوط به‌مسائلی هستندکه‌باروشهای دیگر به‌همان سادگی قابل‌حل‌اند. واز اینرو به‌عنوان تعلیل جبر مجرد متقاعدکننده نیستند. درنتیجه این‌موضوع اغلب به‌انفراد وبه‌عنوان یك‌نظام مجرد تعلیم داده می‌شود و دانشجو باید به‌آن اعتمادکند.

دراین‌کتاب،که براساس دروسی کـه درطی سالهای متمادی به‌دانشجویان سال اول کینگزکالج لندن ارائه شده، قراردارد، سعی کرده‌ام بحث دقیقی از مقدمات جبرمجرد را با مطالعهٔ مباحث مختلفی ترکیب‌کنم که درآنها، کاربرد جبرمجرد اگـرچه اساسی نیست ولی طبیعی و روشنگراست . نظریهٔ مقدماتی اعداد و تجـزیه چند جمله‌ایها دو مبحث اصلی از این نوع هستند وهمراه نظریهٔ مجردگسترش داده می‌شوند، تا به‌نتایجی برسیم ازقبیل قضیهٔ اویلر[1]، قضایای یکتـــایی تجـــزیه برای اعداد صحیح وچندجمله‌ایها، محك‌آیزنشتاین[2] ونظریهٔ کسرهای جزئی. امیدوارم این‌ترتیب ارائهٔ مطالب، به‌خواننده کمك‌کندکه‌سودمندی وهمچنین زیبایی ایده‌های مجرد را درك‌کند.

متن‌اصلی‌این‌کتاب به‌استثنای فصل‌آخر، که درآن قضیهٔ اساسی جبربدون اثبات به‌کار رفته، خودکفاست. معذالك مثالهای تشریحی‌ای کـه ازمطالب گوناگون ریاضی‌آورده شده،

---

1. Euler 2. Eisenstein

حاوی برخی‌ازمفاهیمی هستندکه درمتن‌تعریف نشده‌اند. به‌عنوان مثال، هیچ کوششی‌درجهت تعریف دقیق اعداد حقیقی ومختلط انجام‌نگرفته، اما آنهارا درمثالهاآزادانه به‌کار برده‌ایم، زیراکه برای بسیاری ازخوانندگان‌آشناترین چیزی هستندکه می‌توان درموردآنها ایده‌های جدید را به‌کارگرفت. این به‌هیچ‌وجه تأثیری دردقت درس، که مبتنی برمفاهیم شهودی‌نظریهٔ مجموعه‌ها ومفروضات صریح دربارهٔ اعداد صحیح است، نمی گذارد.

من مدیون بسیاری از دانشجویانم هستم که، ضمن سعی خود درفهم جبرمجـرد یاری نموده‌اند تادرس شکل حاضر خودرا بگیرد. همچنین از بحثهایی کـه با همکارانم درکینگز کالج درمورد برتری نسبی روشهای متعدد ارائـهٔ مطلب کرده‌ام، بسیار سود بـرده‌ام. مایلم قدردانی توأم باسپاس خودرا ازتمام کسانی کـه مرا درتهیهٔ کتاب یاری داده‌اند ابرازکنم، وبخصوص ازخانم د. وودز[1] به‌خاطرتایپ سریع وخوبش ازنسخهٔ خطی.

فیلیپ ج. هیگینز[2]
کینگز کالج ــ دانشگاه لندن
آوریل ۱۹۷۴

1. D. Woods 2. Philip J. Higgins

فصل ۱

جبر مجرد چیست؟

جبر عبارت است از بررسی اعمال وقوانین حاکم براین اعمال. درفصل ۲ معنی کلمهٔ «عمل» روشن‌خواهد شد ولی‌چندمثال‌آشنا، نوع‌اعمالی‌راکه‌درنظرداریم، نشان‌خواهند داد. موضوع مهمی که دراین مثالها بایستی به آن توجه‌کرد آن است‌که اعمال مختلف از قوانین‌مختلفی پیروی‌می‌کنند ومنجر به پیدایش انواع گوناگونی ازجبر می‌شوند. معهذا شباهتهایی وجود دارد‌که امکان بررسی مشترکی را به ذهن القاء می‌کنند.

مثال ۱.۱. جبراستانده. اغلب افراد نخست با این جبر مواجه می‌شوند. در سنین نوجوانی به افراد می‌آموزند‌که در جبر حروف نمایندهٔ اعداد هستند ومعادلات برای توصیف روابط بین آنها به‌کارمی‌روند. برخی از معادلات به ازاء تمام مقادیر ممکن حروفی‌که درآنها به‌کار رفته، برقرارند (اینها معمولا اتحاد نامیده می‌شوند). برخی دیگر فقط به ازاء بعضی از مقادیر ممکن حروف برقرار می‌باشند، و مسئلهٔ تعیین کلیهٔ این مقادیر، به «حل معادلات» مشهور است.

جمع، تفریق، ضرب و تقسیم، اعمال جبر استانده هستند. جمع وضرب برروی جفتی ازاعداد عمل می‌کنند وحاصلجمع، $x+y$، وحاصلضرب، $x\times y$، آنها را تولیدمی‌نمایند (که معمولا ضرب را به صورت xy می‌نویسیم). تفریق رابطهٔ نزدیکی باجمع دارد و با علامت منها نشان داده می‌شود. معمولا این علامت به دوطریق مختلف به‌کار می‌رود: (آ) به عنوان یك عمل دوتایی، که برروی جفتی ازاعداد x و y عمل می‌کند واختلاف‌آنها را می‌دهد، $x-y$، یا (ب) به‌عنوان یك‌عمل یکتایی، که برروی یك‌عدد x عمل‌می‌کند ومنفی آن، $-x$، را می‌دهد. این دو عمل با روابط $x-y=x+(-y)$ و $x-x=0$ $-x=0-x$ به‌هم‌مربوط‌اند، از اینرو یکی می‌تواندبرحسب دیگری بیان شود. ما عمل یکتایی را اساس

کارقرار خواهیم داد و $x-y$ را فقط به عنوان مخفف $x+(-y)$ به کار می‌بریم. به همین ترتیب بهتر آن‌است که راجع به تقسیم (که باضرب مرتبط است، به‌همان‌طریقی که تفریق باجمع ارتباط دارد) برحسب یك عمل یکتایی (که‌عکس نامیده‌می‌شود) فکر کنیم نه یك‌عمل دوتایی. این‌عمل‌یکتایی از عدد غیرصفر x، معکوسش x^{-1} را نتیجه می‌دهد وخارج قسمت $x \div y$ را می‌توان به صورت xy^{-1} نوشت. عملا، علامت تقسیم تقریباً هرگز توسط ریاضیدانان به‌کار نمی‌رود، وعلامت xy^{-1} (یادربعضی موارد x/y) به $x \div y$ ترجیح داده می‌شود.

علاوه براعمالی‌که درفوق مورد بحث قرارگرفت، قوانین جبر استانده متضمن‌اعداد ویژهٔ ۰ و ۱ هستند. این قوانین عبارت‌اند از:

(ج۱) به ازاء هر x، y، z، $(x+y)+z=x+(y+z)$؛

(ج۲) به ازاء هر x، $x+0=0+x=x$؛

(ج۳) به ازاء هر x، $x+(-x)=(-x)+x=0$؛

(ج۴) به ازاء هر x، y، $x+y=y+x$؛

(ض۱) به ازاء هر x، y، z، $(xy)z=x(yz)$؛

(ض۲) به ازاء هر x، $x1=1x=x$؛

(ض۳) به ازاء هر $x\neq 0$، $xx^{-1}=x^{-1}x=1$؛

(ض۴) به ازاء هر x، y، $xy=yx$؛

(ج‌ض۱) به ازاء هر x، y، z، $x(y+z)=xy+xz$ و $(x+y)z=xz+yz$؛

(ج‌ض۲) $1\neq 0$.

اگر به‌جای‌حروف مثلا اعداد گویا، حقیقی یامختلط گذاشته شود این‌قوانین برقرارخواهند بود. اینها، شاید به‌طور ناخودآگاه، در اعمال با معادلات و دستورات جبر مقدماتی به‌کار روند، و برای این منظور تقریباً کافی هستند به این معنی‌که می‌توان اغلب قوانین معتبر جبر مقدماتی را به‌طور منطقی ازآنها نتیجه گرفت. درفصل ۸ مجدداً به‌این مجموعهٔ ویژهٔ قوانین مراجعه خواهیم کرد.

مثال ۲.۱. جبر چند جمله‌ایها. مجموعهٔ تمام چند جمله‌ایهای با یك متغیر X و ضرایب، مثلاً، حقیقی‌رادر نظر گیرید، یعنی‌عباراتی به‌صورت $a_0+a_1X+a_2X^2+\cdots+a_nX^n$، که درآن a_i ها اعدادی حقیقی‌اند. دو چند جمله‌ای را می‌توان برطبق قوانین معمولی با هم جمع ویا در هم ضرب کردکه نتیجهٔ حاصل در هر حالت یك چند جمله‌ای است. هرچند جمله‌ای دارای یك قرینه است (علائم تمام ضرایب را تغییر دهید)، و دو چند جمله‌ای ویژهٔ ۰ و ۱ وجود دارند (یعنی‌آنهایی‌که درمورد‌آنها به‌ازاء $i>0$، $a_i=0$ و $a_0=0$ یا ۱). کلیهٔ قوانین جبراستانده بجز (ض۳) درمورد چند جمله‌ایها برقرارند. ولی (ض۳) برقرار

نیست زیرا همهٔ چند جمله‌ایهای غیرصفر، چند جمله‌ای معکوس ندارند. آن دسته‌ای که معکوس دارند با درجهٔ صفرند (آنهایی کـه برایشان $a_0 \neq 0$ و $a_i = 0$ ، به ازاء $i > 0$). قانون (ض۳) برای این چند جمله‌ایهای معکوس پذیر برقرار است؛ ولی اگر بخواهیم کـه این قانون به ازاء تمام چند جمله‌ایهای غیر صفر برقرار باشد آنگاه بایستی جبر چند جمله‌ایها را به جبر توابع گویا (خارج قسمت چند جمله‌ایها) تعمیم دهیم . این جبرها در فصل ۱۰ مورد بررسی قرار خواهند گرفت.

مثال ۳.۱. جبرماتریسی. برای سادگی توجه خودرا به‌ماتریسهای 2×2

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

با عناصرحقیقی معطوف می‌کنیم. مجموع و حاصلضرب دو ماتریس ازاین نوع را می‌توان طبق قواعد زیر به دست‌آورد:

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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

این اعمال بـه طور دلخواه انتخاب نشده‌اند بلکه از روش استعمال ماتریسها جهت نمایش تبدیلات خطی، به‌دست‌آمده‌اند. این ادعا که این اعمال «طبیعی»اند، یا به‌هرحال، ازنظر ریاضی جالب‌اند، با توجـه به‌اینـکه ازاکثر قوانین جبر استانده پیروی می‌کنند، تأییـد می‌شود. ماتریسهای ویژهٔ

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{و} \quad \mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

موجودندکه اگرآنها را به‌عنوان ۰ و ۱ وحروف‌را به‌عنوان ماتریس‌تعبیر کنیم، کلیهٔ قوانین استانده بجز (ض۳) و (ض۴) برقرارند. مانند چندجمله‌ایها، همهٔ ماتریسهای غیرصفردارای معکوس نیستند . در حقیقت

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

دارای معکوس است اگر و فقط اگر $\Delta = ad - bc \neq 0$ ، و درآن صورت معکوس‌آن

$$\begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix}$$

است . این ماتریسهای معکوس‌پذیر (یا غیرمنفرد) در (ض۳) صدق می‌کنند ، ولی برخلاف

چند جمله‌ایها دراینجا امکان ندارد که جبر ماتریسها را توسعه دهیم تا اینکه تمام ماتریسهای غیر صفر در (ض۳) صدق نمایند. (چرا نه؟ به رابطهٔ

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

توجه کنید.) این امر که ماتریسها در (ض۴) صدق نمی‌کنند با جستجوی یك مثال نقض ساده، بآسانی تحقیق می‌شود. برقراری (ض۱) مستقیماً به وسیلهٔ محاسبه می‌تواند ثابت گردد، اما هنگامی که در زمینهٔ تبدیلات خطی ثابت می‌شود کمتر اسرارآمیز جلوه می‌کند.

چون ممکن است تصور شود که هرجبری، راجع به اعمالی مانند جمع وضرب است که در برخی یا تمام قوانین استانده صدق می‌کنند، به دو مثال از انواع کاملاً متفاوت جبر می‌پردازیم :

مثال ۴.۱. جبر برداری. یك بردار حقیقی n بعدی عبارت است از سطری شامل n عدد حقیقی، $(u_۱ , u_۲ , \dots , u_n)$. اگر $\mathbf{u}=(u_۱ , u_۲ , \dots , u_n)$ و $\mathbf{v}=(v_۱ , v_۲ , \dots , v_n)$، آنگاه جمع بردارها به‌صورت $\mathbf{u}+\mathbf{v}=(u_۱+v_۱ , u_۲+v_۲ , \dots , u_n+v_n)$ تعریف می‌شود. این جمع همراه با بردار صفر $(۰ , ۰ , \dots , ۰)=۰$، در قوانین (ج۱) — (ج۴) صدق می‌کند. به جای ضرب دو بردار، عمل طبیعی‌ای که باید در نظر گیریم ضرب بردارها توسط اسکالرها (یعنی اعداد حقیقی) است. اگر λ یك عدد حقیقی باشد، آنگاه بردار $\lambda\mathbf{u}$ چنین تعریف می‌شود: $\lambda\mathbf{u}=(\lambda u_۱ , \lambda u_۲ , \dots , \lambda u_n)$ وقوانین زیر جایگزین سایر قوانین استانده می‌شوند :

$$\lambda(\mathbf{u}+\mathbf{v})=\lambda\mathbf{u}+\lambda\mathbf{v} ,$$

$$(\lambda_۱+\lambda_۲)\mathbf{u}=\lambda_۱\mathbf{u}+\lambda_۲\mathbf{u} ,$$

$$(\lambda_۱\lambda_۲)\mathbf{u}=\lambda_۱(\lambda_۲\mathbf{u}) ,$$

$$۱\,\mathbf{u}=\mathbf{u} ,$$

که همهٔ آنها وقتی که $\mathbf{u}$ و $\mathbf{v}$ بردارهای حقیقی n بعدی و λ ، $\lambda_۱$ ، $\lambda_۲$ اعداد حقیقی باشند، برقرارند. در آخرین معادله ، منظور از ۱،عدد حقیقی ۱ است. همچنین عمل مفید دیگری به‌نام ضرب اسکالر وجود دارد که روی جفتی از بردارهای $\mathbf{u}$ و $\mathbf{v}$ عمل نموده وحاصل آن عدد اسکالر $\mathbf{u}\cdot\mathbf{v}$ است. این ضرب اسکالر به صورت $\mathbf{u}\cdot\mathbf{v}=u_۱v_۱+u_۲v_۲+\dots+u_nv_n$ تعریف می‌شود وبرای توصیف زاویهٔ بین دو بردار به‌کار می‌رود.

چنانچه درجستجوی ضربهایی از نوع سه مثال اول باشیم، یعنی اعمالی روی جفتی از بردارها که حاصل نیز یك بردار باشد ، به مثالهای متعدد جالبی دست می‌یابیم. در مورد بردارهای دو بعدی می‌توانیم $\mathbf{uv}$ را به صورت زیر تعریف کنیم:

$$\mathbf{uv}=(u_۱v_۱-u_۲v_۲ , u_۱v_۲+u_۲v_۱) .$$

(با اقتباس از ضرب معمولی $(u_۱+iu_۲)$ در $(v_۱+iv_۲)$ ، که $i^۲=-۱$) و درمی‌یابیم

که کلیهٔ قوانین جبر استانده برقرارند، در صورتی که $\mathbf{u}\neq(0,0)$ آنگاه معکوس آن $(u_1/(u_1^2+u_2^2),\ -u_2/(u_1^2+u_2^2))$ است. حاصل، جبر اعداد مختلط است.

درمورد بردارهای سه‌بعدی ضرب‌برداری مشهور زیر وجود دارد که به‌صورت

$$\mathbf{u}\times\mathbf{v}=(u_2v_3-u_3v_2,\ u_3v_1-u_1v_3,\ u_1v_2-u_2v_1)$$

تعریف می‌شود. این‌ضرب به‌هیچ‌وجه درقوانین (ض۱) — (ض۴) صدق‌نمی‌کند ولی به‌ازاء تمام بردارهای سه‌بعدی $\mathbf{u}$ ، $\mathbf{v}$ و $\mathbf{w}$ دارای خواص

$$(\mathbf{u}\times\mathbf{v})\times\mathbf{w}+(\mathbf{v}\times\mathbf{w})\times\mathbf{u}+(\mathbf{w}\times\mathbf{u})\times\mathbf{v}=0 \quad\text{و}\quad \mathbf{u}\times\mathbf{v}=-\mathbf{v}\times\mathbf{u}$$

است؛ این ضرب دارای عضو «۱» و معکوس نیست. مثالهای جالب دیگری درفضاهای چهار بعدی (چهارگانهای هامیلتون[1] که در (ض۱)، (ض۲) و (ض۳) صدق می‌کنند) و هشت‌بعدی (هشت‌گانهای کیلی[2] که در (ض۲) و (ض۳) صدق می‌کنند) موجود است.

مثال ۵.۱. جبرمجموعه‌ها. فرض کنید S یك‌مجموعهٔ مشخص باشد و تمام زیرمجموعه‌های آن‌را به‌انضمام مجموعهٔ تهی $\varnothing$ وخود S درنظر بگیرید. اگر A و B دوزیرمجموعهٔ S باشند آنگاه $A\cup B$ و $A\cap B$ نیززیرمجموعه‌های S هستند، همین‌طور A'، متمم A در S، زیرمجموعهٔ S است. (چنانچه با این مفاهیم آشنایی ندارید برای تعریف آنها به‌اول فصل ۲ رجوع کنید.) سه‌عمل $\cup$ ، $\cap$ ، $'$ ، وزیرمجموعه‌های ویژهٔ $\varnothing$ و S درقوانین‌زیر، که به‌ازاء تمام زیرمجموعه‌های A ، B و C از S برقرارند، صادق می‌باشند.

$$A\cup B=B\cup A, \qquad A\cap B=B\cap A,$$
$$(A\cup B)\cup C=A\cup(B\cup C), \qquad (A\cap B)\cap C=A\cap(B\cap C),$$
$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C), \qquad A\cup(B\cap C)=(A\cup B)\cap(A\cup C),$$
$$A\cap(A\cup B)=A, \qquad A\cup(A\cap B)=A,$$
$$A\cup\varnothing=A, \qquad A\cap S=A,$$
$$A\cup S=S, \qquad A\cap\varnothing=\varnothing,$$
$$A\cup A'=S, \qquad A\cap A'=\varnothing,$$
$$(A')'=A,$$
$$(A\cup B)'=A'\cap B', \qquad (A\cap B)'=A'\cup B'.$$

اینها معروف‌اند به‌قوانین جبربول، که به‌افتخار جورج بول[3]، که روشهای جبری را درمطالعهٔ منطق و بررسی قیاسها[4] معرفی کرد، نامگذاری شده‌است. علائمی که بول به‌کار برده، متفاوت ولی

---

۱. W. R. Hamilton ، ۱۸۰۵–۱۸۶۵، جبردان، منجم وفیزیکدان بزرگ ایرلندی. م

۲. A. Cayley ، ۱۸۲۱–۱۸۹۵، جبردان، هندسه‌دان وآنالیزدان انگلیسی. م

۳. G. Boole ، ۱۸۱۵–۱۸۶۴، ریاضیدان انگلیسی و از علمای منطق. م

۴. قیاس، دراصطلاح منطق، استنتاجی است با دو مقدمه، وقضایای آن حملی هستند. م

معادل با آنچه درفوق آمده، هستند. اونه بامجموعه‌ها بلکه بادرستی گزاره‌ها سروکار داشت. ارتباط بین مجموعه‌ها ومنطق به‌صورت زیر بروزمی‌کند. فرض کنید $P(x)$ ، $Q(x)$ وغیره، نمایشگر گزاره‌هایی بایك متغیر x باشند، که مقادیر x روی مجموعهٔ S تغییر می‌کنند. یعنی، هنگامی که x عضو معینی از S را اختیارکند ، هرگزاره یا درست ویا نادرست است. اگر مجموعهٔ تمام xهایی از S راکه به‌ازاء آنها $P(x)$ درست است با $\Gamma(P)$ نشان دهیم، آنگاه داریم: $\Gamma(P \text{ یا } Q)=\Gamma(P)\cup\Gamma(Q)$ ، $\Gamma(P \text{و} Q)=\Gamma(P)\cap\Gamma(Q)$ ؛ $\Gamma(P)'=\Gamma(\text{چنین نیست که} P)$. بنابراین رابطهای منطقی «یا»، «و» و«چنین نیست که» با اعمال $\cup$ ، $\cap$ و $'$ روی مجموعه‌ها ارتباط نزدیك دارند. درحقیقت قوانین جبربول که درفوق آمده اساساً همان قوانین منطق است، ودلیل خوبی براین مدعا است که جبربول اساسی تراز جبراستانده می‌باشد. جبربول کاربردهای فراوانی ازجمله درطرح مدارهای قطع و وصل برای کامپیوتر دارد. کسانی که به‌روایت مقدماتی این کاربردعلاقمندند باید فصل آخر کتاب هیزل پرفکت[1] [۵] را بخوانند. مقالهٔ اصلی بول‌هم هنوز جالب وقابل فهم است که می‌توان به‌کتاب ایشان مراجعه نمود[۲].

ازهمهٔ این مثالها چنین به‌نظرمی‌رسدکه حیطهٔ وسیع ومتنوعی از اعمال هست که‌مستعد بررسی جبری‌اند واین‌اعمال ازقوانینی پیروی می‌کنندکه این‌قوانین‌هم تنوع قابل‌ملاحظه‌ای دارند . معهذا ظاهراً انواع خاصی از قوانین مرتباً ظاهرمی‌گردند، مثلا : قوانین جابجایی $x+y=y+x$ ، $xy=yx$ ، $A\cup B=B\cup A$ ، $A\cap B=B\cap A$ ، قوانین شرکت‌پذیری $(x+y)+z=x+(y+z)$ ، $(A\cup B)\cup C=A\cup(B\cup C)$ و غیره، وقوانین توزیع‌پذیری $x(y+z)=xy+xz$، $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$ و $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$. توجه کنیدکه این قوانین خودبخود برای همهٔ اعمال برقرار نیستند. مثلا، قانون شرکت‌پذیری درتفریق، $(a-b)-c=a-(b-c)$ ، و همین‌طور قانون توزیعی جمع نسبت به‌ضرب، $a+(bc)=(a+b)(a+c)$، درجبر استانده برقرارنیستند.

اکنون به‌یکی از وسیعترین ایده‌های ریاضی جدید بنام «تجرید» می‌پردازیم. دوطرز تفکرمتفاوت دربارهٔ اعمال وقوانین آنها وجود دارد: (آ) قوانین را می‌توانیم به‌عنوان گزاره‌های درست راجع به‌اعمال ویژه‌ای روی اشیاء بخصوص‌درنظر بگیریم، یا (ب) قوانین را می‌توانیم به‌عنوان قواعد یك‌بازی درنظربگیریم بدون توجه به‌ماهیت اشیایی که‌روی آنها عمل انجام‌می‌گیرد. ودراین‌مورد، هدف، دست‌یافتن به‌قوانین جدید به‌کمك قوانین‌مفروض باروشهای کاملا منطقی است. به‌عنوان مثال، چنانچه منظور ما به‌طور مشخص مطالعهٔ جبر اعداد حقیقی یا جبرماتریسهای حقیقی 2×2 باشد، روش (آ) را تعقیب‌می‌کنیم. ازطرف دیگر، چنانچه صرفاً مطالعهٔ نتایج منطقی قوانین جبر استانده موردنظرباشد، روش (ب) را دنبال می‌کنیم. اینکه درحقیقت این دو روش باهم متفاوت‌اند بسادگی می‌توانند با عبارت «معادلهٔ $x^2=2$ دارای جواب است» توصیف شود. این عبارت در جبر اعداد حقیقی

1. Hazel Perfect

درست، ولی درجبر اعداد گویا نادرست است. چون قوانین جبر استانده درجبر اعداد گویا معتبرند نتیجه می‌شود که وجود جواب برای $x^2 = 2$ نتیجه‌ای منطقی از این قوانین نیست؛ بنا براین گزاره‌های درستی دربارهٔ اعداد حقیقی موجودند که درجبر استانده قضیه نیستند[1].

جبرمجرد عبارت‌است ازمطالعهٔ اعمال‌وقوانین به‌وسیلهٔ روش(ب) ومثال خوبی است‌از روش اصل موضوعی، که مشخصهٔ بارز ریاضیات قرن‌بیستم می‌باشد. درروش اصل‌موضوعی عبارات معینی‌را (که به نامهای متعددی مانند اصول متعارفی، فرضیات یااصول موضوعه مشهورند)، در مورد اشیاء نامشخص فرض می‌کنیم ونتایج منطقی آنهارا موردبررسی قرار می‌دهیم. درحالت موردنظرما، اشیاء نامشخص عبارت‌اند از اعمال وچیزهایی که عمل روی آنها انجام می‌گیرد، واصول موضوعه قوانینی هستند که موردمطالعهٔ ما می‌باشند. این روش مزایای عدیده نسبت به روش مطالعهٔ اعمال مشخص دارد که بهره‌برداری ازآن مزایا دریك سطح مقدماتی، هدف کتاب حاضر است.

اولین مزیت جبر مجرد عمومیت آن است، یعنی هرعبارتی که بتواند ازیك مجموعهٔ قوانین‌مفروض نتیجه شود درهرمبحث جبری‌دیگری که این‌قوانین‌درآن صادق‌اند، نیز برقرار خواهدبود. این امرباعث اختصار زیادی دربرهان می‌شود به‌طوری که دربسیاری از زمینه‌ها، برای اثبات قضایای مشابه یك برهان به‌کار می‌رود. مزیت دیگری کـه عمومیت را تقویت می‌کند انعطاف‌پذیری است. شخص آزاد است که یك مجموعه از قوانین را انتخاب وتحت ملاحظهٔ خاص درآورد وقوانینی راکه نامناسب به‌نظرمی‌رسند، به‌کنار زند. به عنوان مثال، هرنتیجه ازقوانین استانده که بتواند بدون به‌کارگیری (ض۳) یا (ض۴) به‌دست‌آیـد نه‌فقط درمورد اعداد حقیقی، گویا و مختلط برقرار خـواهد بود بلکه برای اعداد صحیح، چند ـ جمله‌ایها وماتریسها نیزمعتبراست. این به‌ما می‌گوید که مجموعهٔ قـوانین استانده با حذف (ض۳) و (ض۴)، فی‌نفسه ارزش مطالعه دارد. همچنین می‌تـوان هریك از اعمال رابه‌طور جداگانه مورد مطالعه قرار داد، گرچه اینها دربـرخی زمینه‌ها به‌صورت دسته‌جمعی ظاهـر می‌شوند. سومین و مهمترین مزیت، وضوح است. پـدیدهٔ «دیده نشدن جنگل به‌علت دیـدن درختها» بخصوص در ریاضیات، حتی‌دربین متخصصان، خیلی معمول است. تاریخ ریاضیات بدفعات شاهد این بوده است که یك قضیهٔ مشکل و مبهم دربخش خاصی ازاین علم، بعدها به‌صورت حالت ویژه‌ای ازیك اصل‌کلی باسادگی اعجاب‌آور وکاربـرد فراوان ظاهر شده است. نکته این‌است که یك‌فرد باانباشته‌ای از دانستنیها دربارهٔ موضوعات مخصوص‌ریاضی رشد می‌کند و هنگامی که با مسئله‌ای مـواجه می‌گردد، تمایل دارد که اولین مطلب ریاضی راکه به‌فکرش خطور می‌کند و درمورد مسئله به‌نظرش می‌رسد، به‌کارگیرد. درصورتی کـه غالباً فقط هنگامی کـه بدون درنظرگرفتن برخی ازاین حقایق ریاضی (یا به‌سبب ضرورت در زمینه‌ای جدید یا به‌سبب‌کار منضبط فکری) اقدام به‌اثبات کند، به استدلال ساده‌تری کـه براصول اساسیتری متکی است دسترسی پیدا می‌کند. روش اصل موضوعی، به وسیلهٔ حذف فرضیات زائد، و مبنا قراردادن حـداقل اطلاعات، بـه‌ایضاح ارتباطهای منطقی بین مطالب

---

۱. دراصطلاح روش اصل‌موضوعی، «قضیه» به‌حکمی‌گفته می‌شودکه قابل استنتاج از اصول‌است .م

ریاضی درحدی کمك می کندکه باسایرروشها ممکن نیست.

برای خوانندگانی که درمورد ارزش پرداختن به‌جبرمجرد نیاز به‌متقاعد شدن دارند یا تصور می‌نمایندکه جبرمجرد ممکن است بغایت مشکل باشد، بایستی تذکرداده شودکه این روش را احتمالا درطول سالها به‌طورضمنی مورد استفاده قرارداده‌اند. آیاآنهاهنگامی که درجبرمقدماتی مشغول محاسبهٔ دستورات و معادلات بوده‌اند، درهرمرحله به‌یاد داشته‌اند که علائم، درنقش (مثلا) اعداد حقیقی‌اند واین امر را دراندیشه راجع به‌انجام مرحلهٔ بعدی به‌کار می گرفته‌اند؟ یا اینکه محاسبات به‌طورمکانیکی و بدون توجه به‌معنی حروف وفقط با به‌کارگیری دستورات معینی که به‌صورت طبیعت ثانویهٔ شخص درآمده بوده، انجام می‌شده است؟این‌امر که‌بعضی ازآنها قواعد غلط رابه‌کار می‌برده‌اند صرفاً گواه‌آن‌است که درواقع، درجبرمجردکار می کرده‌اند.

برای پایان بخشیدن به‌این فصل مقدماتی چندمثال ساده درمورد استنتاجات‌منطقی از قوانین جبری خواهیم‌آورد. قصدبراین است‌که این مثالها، ویژگی وکیفیت موضوع‌رانشان دهند؛ و بنابراین مثالها باتفصیل‌کامل نوشته شده‌اند ودرهرمرحله تصریح شده است‌که چه قانون یا قوانینی مورد استفاده قرارگرفته است. بتدریج که درکتاب پیش می‌رویم، به‌جای این نوع براهین تفصیلی، براهین‌مختصرتر وسهل‌القرائت‌ترمی‌آوریم که درآن فقط مراحل اصلی استدلال ارائه شده وبرخی جزئیات جهت تفکرباقی گذاشته شده‌اند. به‌خواننده‌اکیداً توصیه می‌شودکه سعی کندکلیهٔ جزئیات را انجام دهد تازمانی‌که از قدرت استدلال درست خویش مطمئن گردد ودریابدکه چه‌جزئیاتی می‌توانند بدون ایجاد ابهام حذف شوند.

حال به‌عنوان‌اصول، قوانین«جبراستانده» رابه‌صورتی که درمثال ۱.۱ فرموله‌شده‌اند، اخذ می کنیم وبه‌کمك‌آنها گزاره‌های زیررا نتیجه می گیریم:

(الف) اگر $a+b=a$ آنگاه $b=0$؛

(ب) اگر $a+b=0$ آنگاه $b=-a$ و $a=-b$؛

(پ) به‌ازاء هر a، $-(-a)=a$؛

(ت) به‌ازاء هر a، $a\cdot 0=0$؛

(ث) به‌ازاء هر a و b، $a(-b)=-(ab)$؛

(ج) $(-1)\cdot(-1)=1$.

البته به‌مجرد اینکه یکی‌ازاین عبارات را ازقوانین‌استانده نتیجه‌گرفتیم می‌توانیم‌آن‌رابرای به‌دست‌آوردن بقیه، مورد استفاده قرار دهیم، اما بایستی ازبراهین دوری اجتناب‌کنیم ومثلا نگوییم که از(الف) نتیجه‌می‌شود (ب)، از (ب) نتیجه‌می‌شود (پ) وسرانجام از (پ) نتیجه می‌شود (الف).

برهان (الف). فرض‌کنید $a+b=a$. دراین صورت بنابه (ج۳) داریم:

$$(-a)+(a+b)=-a+a=0.$$

ولی: بنا به (ج۱)، $(-a)+(a+b)=((-a)+a)+b$

بنا به (ج۳)، $=0+b$

بنا به (ج۲)، $=b$

در نتیجه $0=b$.

برهان (ب). فرض کنید $0=b+a$. در این صورت

بنا به (ج۲)، $-a=(-a)+0$

بنا به فرض، $=(-a)+(a+b)$

بنا به (ج۱)، $=((-a)+a)+b$

بنا به (ج۳)، $=0+b$

بنا به (ج۲)، $=b$

استدلال مشابهی (آن‌را بنویسید) نتیجه می‌دهد که $a=-b$.

برهان (پ). فرض کنید $a=-b$. در این صورت بنا به (ج۳)، داریم $0=b+a$. در نتیجه با استفاده از (ب)، $a=-b=-(-a)$.

برهان (ت). قانون توزیعپذیری (ج ض۱) را جهت ارتباط خواص جمعی و ضربی ۰ به کار می‌بریم. قرار می‌دهیم $b=a\cdot 0$. داریم:

$$b+b=a\cdot 0+a\cdot 0$$

بنا به (ج ض۱)، $=a\cdot(0+0)$

بنا به (ج۲)، $=a\cdot 0$

$=b$.

از (الف) نتیجه می‌شود که $b=0$.

برهان (ث). این قسمت شباهت زیادی با حالت قبل دارد. داریم:

بنا به (ج ض۱)، $a\cdot(-b)+a\cdot b=a\cdot((-b)+b)$

بنا به (ج۳)، $=a\cdot 0$

بنا به (ت)، $=0$

از اینرو با استفاده از (ب)، $a\cdot(-b)=-(a\cdot b)$.

برهان (ج) اگر در قسمت (ث)، $a=-1$ و $b=1$ قرار دهیم، آنگاه داریم:

$$(-۱)\cdot(-۱) = -((-۱)\cdot ۱)$$
$$= -(-۱) \quad \text{بنا به (ض۲)،}$$
$$= ۱ \quad \text{بنا به (پ)}$$

ملاحظه کنید که در این براهین قوانین (ج۴)، (ض۳)، (ض۴) یا (ج‌ض۲) را به‌کار نبرده‌ایم.

تمرینها

۱. از قوانین جبر استانده گزاره‌های زیر را نتیجه بگیرید:

(الف) به‌ازاء هر a، b و c، $(ab)c = (cb)a$؛

(ب) اگر $a+c = b+c$، آنگاه $a = b$؛

(پ) $a^۲ - b^۲ = (a-b)(a+b)$، (که در آن $a^۲$ یعنی $a\cdot a$)؛

(ت) اگر $ab = ۰$، آنگاه $a = ۰$ یا $b = ۰$.

۲. اعمال دوتایی $\vee$ و $\wedge$ که به ازاء هر a و b در قوانین $a \wedge (a \vee b) = a$ و $a \vee (a \wedge b) = a$ صدق می‌کنند، مفروض‌اند. ثابت کنید که به‌ازاء هر x، $x \vee x = x \wedge x = x$.

۳. عمل $*$ بادستور $a*b = a+b+ab$ روی اعداد حقیقی تعریف شده است، ثابت کنید این عمل دارای خواص جابجایی $(a*b = b*a)$ وشرکت‌پذیری

$$(a*b)*c = a*(b*c)$$

است. آیا عددی حقیقی مانند e وجود دارد به‌قسمی که به‌ازاء هر a، $a*e = e*a = a$؟ اگر $a*b = a*c$، آیا الزاماً $b = c$ درست است؟

۴. بااستفاده ازقوانین جبر بول نتیجه بگیرید که به‌ازاء هر A، B و C،

$$(A \cap B') \cup (A \cap (B \cup C)) = A.$$

(نبایستی A، B و C را مجموعه فرض کرد. اینها هرشیئی می‌توانند باشند و ما درمورد آنها فقط می‌دانیم که اعمال $\cup$، $\cap$ و $'$ وجود دارند، به‌طوری که این اشیاء واعمال درقوانین مثال ۵.۱ صدق می‌نمایند. ولی برای یافتن برهان، می‌توانید درآغاز کار آنهارا مجموعه فرض کنید.)

۵. به‌کمك قوانین جبر بول نشان دهید که اگر $A \cup B = A$، آنگاه $A \cap B = B$.

۶. فرض کنید که اشیاء A، B، C، ... نسبت به‌اعمال $\cup$، $\cap$ و $'$، درقوانین جبر بول صدق کنند. قرار دهید $A+B = (A \cup B) \cap (A' \cup B')$ و ۰ را به جای $\varnothing$ درنظر

بگیرید. ثابت کنید قوانین(ج۲)، (ج۳) و (ج۴) از جبراستانده برقرارند و $A-$ رامعین کنید. مجموع $A+B$ را (الف) درموردمجموعه‌ها و (ب) درمورد گزاره‌ها (که درآن $\cup$، $\cap$ و $'$، بترتیب به‌معنی «یا»، «و» و «چنین نیست که» می‌باشند.) تعبیر کنید.

۷. (مشکلتر). در ادامهٔ تمرین۶، ثابت کنید که قانون (ج۱) برقرار است. همچنین با فرض AB به‌جای $A \cap B$ و ۱ به‌جای S، نشان‌دهید قوانین (ض۱)، (ض۲)، (ض۴) و (ج‌ض۱) برقرارند.

۸. (مشکلتر). کدام‌یك ازعبارات زیر نتیجهٔ منطقی قوانین «جبراستانده» هستند؟

(الف) اگر $x^۲=y^۲$، آنگاه $x=y$ یا $x=-y$.

(ب) اگر $x^۲+y^۲=۰$، آنگاه $x=y=۰$.

(پ) اگر $x^۲+y^۲=a$، آنگاه bای وجود دارد به‌قسمی که $a=b^۲$.

(راهنمایی: برای نشان دادن اینکه یك گزاره نتیجه‌ای ازمجموعهٔ مفروضی‌از قوانین نیست، باید مثالی از دستگاهی ارائه دهیدکه درآن این قوانین برقرار است، اما گزارهٔ مذکور درموردآن نادرست است.)

فصل ۲

نظریهٔ مجموعه‌ها

در اثبات قضایای دستگاههای جبری به دو ابزار ریاضی، علاوه برمنطق محض،نیاز داریم. اولا خواص مقدماتی اعداد صحیح را لازم داریم ؛ مثلا وقتی علائم x^2 و x^n را به کار می‌بریم، فرض ضمنی ما این است که خواننده با اعداد صحیح ۲ و n آشناست؛ همچنین‌در تقریر قانون $x^m x^n = x^{m+n}$ ، پیش فرض ما آن است که شما جمع اعداد صحیح را می‌دانید. واضح است که بدون فرض چنین دانشی نمی‌توانیم ، حتی درجبر مجرد، به‌جای چشمگیری‌برسیم. ثانیاً، و به‌دلایل کمتر بدیهی، محتاج‌نظریهٔ مقدماتی مجموعه‌ها هستیم. زبان نظریهٔ مجموعه‌ها در اکثر شاخه‌های ریاضیات به عنوان وسیله‌ای برای تدقیق نحوهٔ بیان گزاره‌ها وتعریف روشن و غیر مبهم مفاهیم بنیادی به‌کارمی‌رود. مناسبت‌آن برای این‌منظور، بعدها دراین‌کتاب آشکار خواهد شد. بعلاوه ، گاهی مفهوم مجموعه در صورت قضایا ظاهر می‌شود؛ به عنوان مثال می‌توان ثابت کرد که اگر یك مجموعهٔ متناهی از اشیاء در تمام قوانین جبر استانده صدق کند آنگاه تعداد اشیاء آن بایستی توانی از یك عدد اول باشد. این‌خاصیتی ازمجموعهٔ اشیاء است، نه ازخود اشیاء بتنهایی؛ وبه‌همین‌دلیل‌است که‌نمی‌تواند فقط به‌کمك منطق ازقوانین جبر استانده نتیجه گردد.

آن قسمت از خواص اعداد صحیح راکه برای بسط جبر احتیاج داریم ، در فصل ۳ خواهیم گفت. در فصل حاضر به قسمتهای مورد لزوم از نظریهٔ مجموعه‌ها می‌پردازیم . این دومبحث رامی‌توان به‌روش اصول موضوعی بررسی کرد، ولی این‌روش باعث دشواریهایی می‌شودکه در یك درس مقدماتی مقتضی نیست. به جای این‌کار ، ما برخی از مطالب مشهور در مورد مجموعه‌ها واعداد را دانسته فرض می‌کنیم وسپس، با مجهز شدن به این اطلاعات بنیادی، با یك منطق دقیق اقدام به‌کار خواهیم کرد.

به‌خاطر دانشجویانی‌که نظریهٔ مجموعه‌ها را قبلا آموزش ندیده‌اند ، ما از مطالب

مقدماتی شروع کرده و تمام تعاریف را می‌آوریم. این عمل فصل حاضر را طولانی می‌کند و خوب است به خواننده توصیه کنیم که در وهلهٔ اول آن را نسبتاً سریع مطالعه کند، اما در جذب مفاهیم بنیادی تابع، عمل و رابطهٔ هم ارزی دقت کافی به عمل آورد. چنانچه این مفاهیم روشن هستند دانشجویان می‌توانند بدون مطالعهٔ این فصل ادامه دهند، و در مواقع لزوم و برای توضیح بیشتر به فصل ۲ مراجعه کنند.

دسته‌ای از اشیاء مجموعه است هر گاه کاملا به عنوان یك موجود بررسی شود. مثلا یك تیم فوتبال مجموعه‌ای از بازیکنان و یك کتابخانه مجموعه‌ای از کتب است. اشیائی که یك مجموعه را تشکیل می‌دهند اعضا یا عناصر آن نامیده می‌شوند. علامت $x\in S$ ، بدین معنی است که شئ x عضوی از مجموعهٔ S می‌باشد. همچنین گوییم x متعلق به S است. دو مجموعه را مساوی گوییم (یعنی به عنوان یك مجموعه می‌شناسیم) اگر و فقط اگر دارای اعضای یکسانی باشند. بنا براین وقتی می‌گوییم که یك کتابخانه مجموعه‌ای است از کتب، منظور آن است که از کیفیت ترتیب قرار گرفتن کتب در قفسه‌ها صرفنظر شده است. در آینده خواهیم دید که چنین کیفیات اضافی‌ای را که ممکن است یك مجموعه دارا باشد، چگونه در نظر خواهیم گرفت، اما در آغاز بایستی مجموعه‌های مجرد را که فقط به کمك اعضایشان معین می‌شوند بررسی کنیم.

مجموعه‌های خاص به دو طریق می‌توانند مشخص شوند. می‌توان اعضای آنها را فهرست کرد، که در این صورت اعضا را در داخل دو ابرو می‌نویسیم؛ به عنوان مثال $\{\pi\ ,\ 1\ ,\ 0\}$ مجموعهٔ سه‌عضوی ۰، ۱ و π را نشان می‌دهد. همچنین می‌توان اعضای مجموعه را به وسیلهٔ یك خاصیت مشخصهٔ P که در آنها مشترك است و هیچ چیز دیگری این خاصیت را ندارد، توصیف کرد. علامت مناسب برای این حالت $\{x\ ;\ P(x)\}$ می‌باشد که خوانده می‌شود «مجموعهٔ اشیایی مانند x که به ازاء آنها گزارهٔ $P(x)$ درست است».

مثال ۱.۲. بعضی مجموعه‌ها کراراً در ریاضیات ظاهر می‌شوند و به همین دلیل، علائم ویژه‌ای برای آنها وضع شده است. به عنوان مثال، ما همواره $\mathbf{N}$ را برای نمایش مجموعهٔ اعداد طبیعی به کار می‌بریم. اعضای این مجموعه اعداد ۰، ۱، ۲، ... هستند که در شمارش به کار می‌روند. مجموعهٔ تمام اعداد صحیح ۰، ± 1، ± 2، ... با $\mathbf{Z}$ نشان داده می‌شوند ($\mathbf{Z}$ از کلمهٔ آلمانی «Zahl» به معنی «عدد» گرفته شده است). مجموعه‌های دیگری که غالباً در مثالها مطرح خواهند بود عبارت‌اند از:

$\mathbf{Q}$، مجموعهٔ تمام اعداد گویا (خارج قسمتهای اعداد صحیح)؛

$\mathbf{R}$، مجموعهٔ تمام اعداد حقیقی؛

$\mathbf{C}$، مجموعهٔ تمام اعداد مختلط.

مجموعهٔ S مفروض است. می‌توانیم زیر مجموعه‌هایی از S را تشکیل دهیم، بدین ترتیب که برخی (یا تمام، یا هیچ کدام) از اعضای S را انتخاب کرده و آنها را اعضای یك مجموعهٔ جدید قرار دهیم. بنا براین مجموعهٔ T یك زیر مجموعهٔ S نامیده می‌شود هر گاه هر عضو T عضوی از S باشد. بخصوص، خود S یك زیر مجموعه از S است. در اینجا مفید

است که مجموعهٔ تهی را به عنوان یك مجموعهٔ بدون عضو، تعریف کنیم . چون دو مجموعهٔ تهی دقیقاً دارای اعضای مساوی‌اند، تمام مجموعه‌های تهی برابرند، ازاینرو می توانیم بگوییم مجموعهٔ تهی (نه مجموعه‌ای تهی) و علامت استاندهٔ $\varnothing$ را برای‌آن به‌کاربریم. این‌مجموعهٔ عجیب زیرمجموعهٔ‌هر مجموعه‌ای است. علامت $T \subset S$ یا $S \supset T$ را برای‌نشان دادن‌اینکه T زیرمجموعهٔ S است (خوانده می‌شود «T مشمول S است» یا «S شامل T است») به‌کار می بریم. توجه داشته باشیدکه اگر $S \subset T$ و $T \subset S$ آنگاه $S = T$. معمولا ، اگر منظور مشخص نمودن یك زیرمجموعهٔ ویژه از S باشد، این‌کار را با بیان خاصیتی‌که اعضای آن زیرمجموعه را از سایراعضای S متمایز می کند، انجام می‌دهیم. مثلا در مجموعهٔ همهٔ‌افراد بشر می‌توان زیرمجموعهٔ افراد یك پا را تشکیل داد. زیر مجموعه‌ای را که به این صورت وصف شده باشد، با علامت $\{x\,;\, x\in S\,,\, p(x)\}$ نشان می‌دهیم ، که در آن $p(x)$ حکمی راجع به x است. همچنین به طور ساده‌ترمی نویسیم $\{x\in S\,;\, p(x)\}$ ومی‌خوانیم «مجموعهٔ تمام x هایی در S به‌قسمی‌که گزارهٔ $p(x)$ درست‌است». البته، اگر $p(x)$ به‌ازاء هر$x\in S$ نادرست باشد ، آنگاه $\{x\in S\,;\, p(x)\} = \varnothing$.

مثال ۲.۲. تمام مجموعه‌هایی که در مثال ۱.۲ توصیف شده‌اند زیر مجموعه هایی از مجموعهٔ اعدادمختلط $\mathbf{C}$ هستند. در واقع، این مجموعه‌ها تشکیل زنجیره‌ای از زیرمجموعه‌ها را می‌دهند، به قسمی که هرکدام زیرمجموعه‌ای از مجموعهٔ بعدی است:

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}\,.$$

مثال ۳.۲. مجموعهٔ $\{x\in\mathbf{R}\,;\, ۲x^۲ - ۴x + ۱ = ۰\}$ فقط دارای دوعضو $۱ + \frac{۱}{۲}\sqrt[۱]{۲}$ و $\{x\in\mathbf{R}; x^۲ - x + ۱ = ۰\}$ و $\{x\in\mathbf{Q}; x^۲ = ۳\}$ و $\frac{۱}{۲}\sqrt[۱]{۲} - ۱$ است،درصورتی که‌مجموعه‌های هردو تهی هستند.

اگر A و B دو زیر مجموعه از S باشند ، اتحادشان $A \cup B$ زیر مجموعهٔ $\{x\,;\, x\in A$ یا $x\in B\}$ است. باید به‌این‌نکتهٔ مهم توجه کنید که‌در اینجا، به‌طورکلی‌در ریاضیات، «یا» همواره به معنی «شمول» به‌کار می‌رود یعنی $A \cup B$ شامل تمام عناصری از S است‌که یا به A یا به B یا به هردو متعلق‌باشند. بنابراین A و B هردو زیرمجموعه‌هایی از $A \cup B$ هستند و درحقیقت $A \cup B$ کوچکترین زیرمجموعهٔ S است‌که شامل A و B به عنوان زیر-مجموعه می‌باشد، به مفهوم اینکه اگر C زیر مجموعه‌ای از S باشد و $C \supset A$ و $C \supset B$ ، آنگاه $C \supset A \cup B$. به‌همین‌نحو،مقطع A و B زیرمجموعهٔ $A \cap B = \{x\,;\, x\in A$ و $x\in B\}$ است. این زیر مجموعه‌ای از A و B است‌که بزرگترین مجموعه‌ای است‌که زیر مجموعهٔ هردوست . البته ، اگر A و B دارای اعضای مشترکی نباشند، آنگاه $A \cap B = \varnothing$ ، و این به تنهایی توجیهی است کافی برای معرفی مجموعهٔ تهی ، چون در غیر این صورت مقطع همیشه تعریف نخواهد شد و در نتیجه قوانین نظریهٔ مجموعه‌ها پیچیده‌تر می‌شود . اتحاد و مقطع چند زیرمجموعهٔ $A_۱$ ، $A_۲$ ، ... ، A_n از S به همین نحو تعریف می‌شوند و علائم

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n \text{ ،}$$

و

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n \text{ ،}$$

را ، برای این منظور ، به‌کار می‌بریم. برای دسته‌های دلخواهی از زیر مجموعه‌ها (احتمالا تعدادی نامتناهی ازآنها) می‌توان اندیسهای تحتانی‌ای به کاربرد که اعداد صحیح نبوده بلکه ازیك مجموعهٔ I (که‌مجموعهٔ اندیس‌گذار نامیده‌می‌شود) باشند. درآن‌صورت علامت

$$\bigcup_{i \in I} A_i$$

را برای‌اتحاد مجموعه‌های A_i وعلامت

$$\bigcap_{i \in I} A_i$$

را برای مقطع‌آنها به‌کار می‌بریم. اگر $A \subset S$ ، مکمل A در S به صورت $\{x \in S \; ; \; x \notin A\}$ تعریف‌می‌شود که درآن $\notin$ به‌معنی «متعلق‌نیست به» است. این مکمل به صورت $S \setminus A$ ، یا A' اگر S مفروض ومشخص باشد، نشان‌داده‌می‌شود. قوانین‌حاکم براتحاد، مقطع‌ومکمل را قبلا درمثال ۵.۱ آورده‌ایم. خواننده باید خوب‌بفهمدکه مبنای‌منطقی قوانینی مانند $A \cup \varnothing = A$، $A \cap \varnothing = \varnothing$ و $\varnothing' = S$ چیست .

مشاهده‌کرده‌ایم که مقطع، اتحاد ومکمل زیرمجموعه‌های یك مجموعه نسبت نزدیکی با رابطهای منطقی «و» ، «یا» و «چنین نیست که» دارند. اکنون به معرفی نمادهای منطقی بیشتری می‌پردازیم و رابطهٔ آنها را با نظریهٔ مجموعه‌ها بیان می‌کنیم : سورهای $\forall$ و $\exists$ علامتهایی هستند به‌معنی «به ازاء هر» و «وجود دارد» که به‌طریق زیر به‌کار می‌روند. اگر $p(x)$ گزاره‌ای مشتمل بر (یا حکمی راجع به) شئ متغیر x باشد ، آنگاه $(\forall x)p(x)$ به معنی «$p(x)$ به ازاء تمام x ها درست است» و $(\exists x)p(x)$ به معنی «حداقل یك شئ x وجود داردکه به ازاء آن $p(x)$ درست است» هستند. عبارت «به ازاء هر x» بدون قید و شرط هیچ‌معنی روشنی‌ندارد، بلکه نیاز به توصیف‌نوع x ای‌که مورد بررسی قرارمی‌گیرد، داریم. این نارسایی را بامشخص‌کردن مجموعه‌ای مانند S، بنام حوزهٔ مقادیر x ، و محدود نمودن تغییر x به اعضای S ، برطرف می‌کنیم . گاهی S یکبار و برای همیشه معین می‌شود (ومجموعهٔ سخن‌نامیده می‌شود). دراین حالت معنی $(\forall x)p(x)$ و $(\exists x)p(x)$ روشن‌است. اگر گاه‌گاهی حوزهٔ مقادیر x دستخوش تغییراتی شد، بایستی صریحاً آن را متذکر شویم ، مثلا می‌نویسیم $(\forall x \in S)p(x)$ و $(\exists x \in S)p(x)$ که بترتیب به معانی «$p(x)$ به ازاء تمام اعضای x از S درست است» و «$p(x)$ برای حداقل یك x از S برقرار است» می‌باشند. توجه‌کنید که مفهوم $(\forall x \in S)p(x)$ با مفهوم $S = \{x \in S \; ; \; p(x)\}$ یکی است. همچنین $(\exists x \in S)p(x)$ به همان معنی $\{x \in S \; ; \; p(x)\} \neq \varnothing$ می‌باشد . اگر $\neg$ را برای «چنین نیست‌که» به‌کار بریم، یعنی‌اگر $\neg p(x)$ به‌معنی «$p(x)$ نادرست است» باشد، آنگاه گزارهٔ

$$\neg(\exists x\in S)\,p(x)$$

به‌معنی «xای در S وجود ندارد که به‌ازاء آن $p(x)$ درست باشد» خواهد بود. این بدین‌معنی است که «$p(x)$ به‌ازاء هر x از S نادرست است»، یا به‌زبان علائم:

$$(\forall x\in S)\neg p(x)\,.$$

به‌همین ترتیب، گزارهٔ

$$\neg(\forall x\in S)\,p(x)$$

معادل گزارهٔ

$$(\exists x\in S)\neg p(x)$$

است. بنابراین می‌توان نماد نفی را از یک سور عبور داد به‌شرط اینکه $\forall$ را به $\exists$ تغییر دهیم وبالعکس. مثالهای دیگری از کاربرد سورها را در روابط

$$\bigcup_{i\in I} A_i=\{x\in S\ ;\ (\exists i\in I)(x\in A_i)\}\ ,$$

$$\bigcap_{i\in I} A_i=\{x\in S\ ;\ (\forall i\in I)(x\in A_i)\}$$

می‌یابیم. اگر این روابط به‌زبان غیرسوری ترجمه شوند، معرف ـ به‌ترتیب ـ اتحاد و مقطع دسته‌ای از زیرمجموعه‌های S خواهند بود.

نماد $\Longrightarrow$ یعنی «نتیجه می‌دهد» واز لحاظ دستوری به‌عنوان یک فعل به‌کار می‌رود. اگر p و q دو گزاره باشند، آنگاه $p\Longrightarrow q$ (p نتیجه می‌دهد q) نیز یک گزاره است به‌معنی: «اگر p درست باشد آنگاه q هم درست است». واین از جنبهٔ منطقی با «یا p نادرست یا q درست است» معادل بوده واز اینرو $p\Longrightarrow q$ به‌معنی (q یا ($\neg p$)) می‌باشد. بیشترین استفادهٔ استلزام منطقی در بین گزاره‌هایی است با یک متغیر ومعنایش در این مورد طبیعی‌تر و جالب‌تر است. به‌عنوان مثال، مربع هر عدد زوج یک عدد زوج است واین عبارت می‌تواند به‌صورت (x^2 زوج است $\Longrightarrow x$ زوج است) $(\forall x\in\mathbf{Z})$ نوشته شود. به‌طور کلی، اگر $p(x)$ و $q(x)$ احکامی راجع به x باشند، گزارهٔ $(\forall x)(p(x)\Longrightarrow q(x))$ یعنی $q(x)$ درست است به‌ازاء هر مقدار از x که $p(x)$ را برقرار سازد. این عبارت نیز می‌تواند به‌زبان نظریهٔ مجموعه‌ها به‌صورت $\{x\ ;\ p(x)\}\subset\{x\ ;\ q(x)\}$ نوشته شود، که بیانگر ارتباط بین استلزام منطقی و مفهوم زیرمجموعه است. نماد $\Longleftarrow$ به‌معنی «نتیجه‌می‌شود به‌وسیلهٔ»، ونماد $\Longleftrightarrow$ به‌معنی «نتیجه می‌دهد و نتیجه می‌شود به‌وسیلهٔ» می‌باشند. اگر $p(x)$ و $q(x)$ دو گزاره باشند به‌قسمی که $(\forall x)(p(x)\Longleftrightarrow q(x))$ درست باشد، آنگاه آنهارا احکامی معادل راجع به x نامیم. در این حالت دو مجموعهٔ $\{x\ ;\ p(x)\}$ و $\{x\ ;\ q(x)\}$ مساوی‌اند.

اکنون به‌اولین ایدهٔ مهم در نظریهٔ مجموعه‌ها یعنی تابع می‌پردازیم. این ایده اساساً قدیمی است واز بررسی وابستگی یک کمیت فیزیکی به‌کمیت دیگر، ناشی شده است. معنی کلمهٔ «تابع» از توابع حقیقی با یک متغیر حقیقی (که خواننده حتماً آنهارا درحساب

دیفرانسیل و انتگرال مقدماتی به‌کار برده‌است) پس‌از گذشت سالها به‌توابع بامقدار مختلط، توابع چندمتغیره وتوابع بامقدار برداری (مثلا بردارموضعی یك ذره به‌عنوان‌تابعی از زمان) وغیره گسترش‌پیدا کرده است. معمولا یك‌تابع خاص به‌وسیلهٔ دستوری داده می‌شود که به‌کمك آن می‌توان مقادیرش را محاسبه کرد، ولی با توسعهٔ حساب دیفرانسیل وانتگرال لازم شد که از تابع دلخواه ونامشخصی‌صحبت شود. به‌همین دلیل بایستی محکی برای تصمیم‌گیری در مورد اینکه چه‌چیز تابع است وچه‌چیز تابع نیست، وجود می‌داشت. مهمترین‌خاصیت مشترك توابع مختلف‌فوق‌الذکرآن است‌که مقدار یك تابع به وسیلهٔ مقدار یك یاچند متغیر به‌طور یکتـــا معین می‌شود. امروزه این‌خاصیت‌به‌عنوان خاصیت‌مناسب‌برای به‌کار بردن درتعریف مفهوم«تابع» پذیرفته شده است. زبان نظریهٔ مجموعه‌ها بررسی انواع متغیرهای مختلف و مقادیرمختلفی‌راکه ممکن‌است یك‌تابع اختیارکند، ساده می‌کند. فقط لازم است دومجموعه مشخص‌گردد، اولا مجموعه‌ای‌که تمام مقادیرممکن متغیررا به‌عنوان اعضاء دربرداشته‌باشد، ثانیاً مجموعه‌ای‌که تمام مقادیر تابع را اختیارمی‌کند. تعریف نهایی به‌قرار زیراست:

تعریف. فرض‌کنید X و Y دومجموعه باشند. یك تابع از X به Y به‌کمك قاعـده‌ای داده می‌شودکه به‌ازاء هرعضو X عضو متناظری از Y را مشخص و معین مـی‌کند. مجموعهٔ X حوزهٔ تعریف ومجموعهٔ Y حوزهٔ مقادیر تابع نامیده می‌شوند.

اگر f نمایش تابعی‌از X به Y باشد و $x\in X$ ، آنگاه علامت $f(x)$ رابرای‌نمایش اثر تابع f بر x می‌نویسیم. پس $f(x)$ عضوی از Y است. این‌عضو، مقدار f در x نامیده می‌شود. توجه داشته‌باشیدکه شرایط تعریف‌یك‌تابع عبارت است‌از: (الف) f می‌تواند بر هر عضوی از X عمل نماید و (ب) به ازاء هر $x\in X$ ، مقدار $f(x)\in Y$ به طور یکتا معین می‌شود.

مثال۴.۲. تابع f از $\mathbf{R}$ به $\mathbf{R}$ را می‌توانیم بادستور $f(x)=x^2$ تعریف‌کنیم . این «تابع مجذور» است. ولی اگرسعی‌کنیم تابع «جذر» g از $\mathbf{R}$ به $\mathbf{R}$ را بادستور: «$g(x)$ یك عدد حقیقی است‌که مجذورش x می‌باشد» تعریف نماییم، آنگاه به‌دوعلت g تابع نخواهد بود. اولا، اگر x منفی باشد آنگاه هیچ عدد حقیقی وجود نداردکه مجذورش x گردد، لذا دستور نمی‌تواند برای این x عمل کند. ثانیاً اگر x مثبت باشد آنگاه دو عدد حقیقی وجود داردکه مجذورش x است. بنابراین $g(x)$ به‌طوریکتا معین‌نمی‌شود. معهذا می‌تـوانیم یك تابع جذر به‌دست‌آوریم به‌شرطی‌که اولا مقادیر x را با $x\geqslant 0$ محدودکنیم وسپس دستوری ارائه‌کنیم که به‌ازاء هر x فقط یکی از ریشه‌های x را اختیارکند. ساده‌ترین دستور، برگزیدن جـذر مثبت (یا ۰) است. جذر مثبت x به‌وسیلهٔ $\sqrt{x}$ نشان‌داده می‌شود ولذا تابعی‌مانند $\sqrt{}$ از X به $\mathbf{R}$ داریم، که‌درآن $X=\{x\in\mathbf{R}\ ;\ x\geqslant 0\}$. دستور مشابهی رامی‌توان‌برای تعریف‌تابعی از X به X به‌کاربرد.

مثال۵.۲. تابع f از $\mathbf{Z}$ به $\mathbf{Z}$ را می‌توانیم بادستور

$$f(n)=\begin{cases}-۱ & \text{اگر } n \text{ فرد باشد}\\ ۱ & \text{اگر } n \text{ زوج باشد}\end{cases}$$

تعریف کنیم. تعیین یك تـابع با روش تشخیص حالات گـوناگون، یك تدبیرعمومی است. افراطی‌ترین شکل این روش فهرست‌کردن مقادیر تابع به‌ازاء تمام مقادیرمتغیر است. مثلا اگر $X=\{۱ ، ۲ ، ۳\}$ ، آنگاه می‌توانیم تابعی مانند F از X به X رابادستور

$$\begin{cases}F(۱)=۳ ،\\ F(۲)=۲ ،\\ F(۳)=۲ ،\end{cases}$$

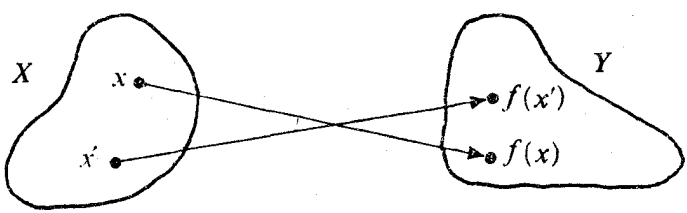
تعریف کنیم.

دودستور که توابع از X به Y را تعریف می کنند ممکن است اثـر یکسانی برروی هرعضو X داشته باشند. دراین حالت طبعاً مایلیم که آنهارا «یك‌تابع» بدانیم. اگر f و g توابعی از X به Y باشند آنگاه f و g را باهم مساوی‌گوییم اگروفقط اگر به‌ازاء هر $x\in X$، $f(x)=g(x)$. دراین حالت می‌نویسیم $f=g$.

مثال ۶.۲. توابع g و h از $\mathbf{Z}$ به $\mathbf{Z}$ که بادستورهای $g(n)=(-۱)^n$ ؛ $h(n)=\cos n\pi$ تعریف شده‌اند، باهم وباتابع f تعریف شده درمثال ۵.۲ فوق‌الذکرمساوی هستند.

مثال ۷.۲. اگر $X=\{۱ ، ۲ ، \dots ، m\}$ و $Y=\{۱ ، ۲ ، \dots ، n\}$ ، آنگاه تعداد تـوابع متمایز از X به Y برابر است با n^m ، زیرا هرتابع f به وسیلهٔ m مقدار $f(۱)$ ، $f(۲)$ ، ... ، $f(m)$ معین می‌شود وهرکدام از اینهارا می‌توان به‌طور دلخواه از n عضو Y انتخاب کرد.

تابع f از X به Y را می‌توان به‌عنوان «نگارندهٔ» هـرعضو x از X به‌عضو متناظر $f(x)$ از Y تصورکرد وآنرا یك«نگاشت» از X بتوی Y دانست.



به‌همین دلیل‌واژهٔ «نگاشت» غالباً به‌جای «تـابع» و دقیقاً به‌همان معنی به‌کار می‌رود و معنی نماد $f : X \longrightarrow Y$ این‌است که f نگاشتی است‌از X به Y . پیکانی ازنوع دیگر $\longmapsto$ ، برای نشان دادن اثریك نگاشت یا تابع برروی هریك ازعناصر X به‌کار می‌رود. مثلا نماد $x \longmapsto y$: f یعنی «fعضوxرا بهy می نگارد»، یعنی $f(x)=y$. این‌پیکان برای‌مشخص-

کردن توابع مناسب است؛ به‌عنوان مثال، تابع $f : \mathbf{R} \longrightarrow \mathbf{R}$ که با ضابطهٔ $f(x) = x^3 + x$ تعریف شده است را می‌توان به صورت $x \longmapsto x^3 + x (\mathbf{R} \longrightarrow \mathbf{R})$ بیان کرد. همچنین مقدار تابع $f(x)$ در x نقش x تحت نگاشت f نامیده می‌شود.

اگر دو نگاشت $f : X \longrightarrow Y$ و $g : Y \longrightarrow Z$ مفروض باشند، آنگاه می‌توانیم آنهارا ترکیب کرده و به‌طریق طبیعی نگاشتی از X به Z به‌دست‌آوریم. باعنصری مانند x از X شروع کرده اول آن را به‌نقشش $f(x)$ تحت f، می‌نگاریم، سپس نقش این عضو از Y، $g(f(x))$ را تحت g به دست می‌آوریم. نگاشت تعریف شده بدین طریق را ترکیب f و g می‌نامیم و با $g \circ f$ نشان می‌دهیم. این نگاشت با دستور، به ازاء هر $x \in X$، $(g \circ f)(x) = g(f(x))$ بیان می‌شود. احتمالاً خواننده قبلا با ترکیب توابع تحت نام «تابع تابع» آشنایی پیدا کرده است. ترکیب توابع همان جایگزینی یك تابع در تابع دیگری است. تابع مرکب $g \circ f$ فقط وقتی وجود دارد که حوزهٔ مقادیر f همان حوزهٔ متغیر g باشد.

مثال ۸۰۲. تابع $f : x \longmapsto \sin x (\mathbf{R} \longrightarrow \mathbf{R})$ و $g : y \longmapsto y^2$ (هردو تابع از $\mathbf{R}$ به $\mathbf{R}$ هستند) می‌باشد. توجه کنید که در این حالت خاص، توابع می‌توانند وارونه ترکیب شوند و تابع $f \circ g : \mathbf{R} \longrightarrow \mathbf{R}$ را نتیجه دهند. این تابع x را به $\sin(x^2)$ می‌نگارد و مساوی با تابع $g \circ f$ نیست.

قضیهٔ ۲آ. ترکیب توابع شرکت‌پذیر است. به‌عبارت دقیق‌تر، اگر $f : A \longrightarrow B$، $g : B \longrightarrow C$ و $h : C \longrightarrow D$ سه تابع باشند، آنگاه دو تابع $h \circ (g \circ f)$ و $(h \circ g) \circ f$ از A به D، مساوی هستند.

برهان. اگر k_1 و k_2 به‌ترتیب نمایش توابع $h \circ (g \circ f)$ و $(h \circ g) \circ f$ باشند، آنگاه از تعریف ترکیب توابع نتیجه می‌شود که به ازاء هر $a \in A$،

$$k_1(a) = h((g \circ f)(a)) = h(g(f(a)))$$

به همین نحو

$$k_2(a) = (h \circ g)(f(a)) = h(g(f(a))).$$

بنابراین به ازاء هر $a \in A$، $k_1(a) = k_2(a)$، یعنی $k_1 = k_2$.

برای هر مجموعهٔ A تابع ویژه‌ای از A به A موجود است که تابع همانی روی A نامیده می‌شود. این تابع هرعنصر A را به‌خودش تبدیل می‌کند و با i_A نمایش داده می‌شود. یعنی به ازاء هر $a \in A$، $i_A(a) = a$. واضح است که تابع همانی نسبت به ترکیب توابع نقش خاصی را ایفامی‌نماید؛ اگر $f : X \longrightarrow Y$ آنگاه $f \circ i_X = f$ و $i_Y \circ f = f$. توابع همانی رفتاری نسبتاً شبیه ۱ درجبر مقدماتی دارند، اما به‌صورت «یکطرفی» (قانون(ض۲) در مثال ۱۰۱ را ببینید). این امر ما را به تعریف توابع معکوس، به طریق زیر، راهنمایی می‌کند. فرض کنید $f : X \longrightarrow Y$ و $g : Y \longrightarrow X$ دوتابع باشند، آنگاه هردوتابع مرکب

$g\circ f : X\longrightarrow X$ و $f\circ g : Y\longrightarrow Y$ موجودند. اگر $g\circ f = i_X$ و $f\circ g = i_Y$، گوییم که توابع f و g معکوس یکدیگرند. به عبارت دیگر، f و g توابع معکوس هستند اگر به ازاء هر $x\in X$ و هر $y\in Y$ داشته باشیم: $f(g(y)) = y$ و $g(f(x)) = x$. همهٔ توابع دارای معکوس نیستند و به‌زودی محك ساده‌ای برای اینکه یك تابع دارای معکوس باشد، به دست خواهیم داد. مثالهای توابع معکوس را تا آن وقت به تعویق می‌اندازیم.

اگر تابع $f : X\longrightarrow Y$ دارای این خاصیت باشدکه هیچ دو عنصر متمایز X تحت f دارای یك نقش نباشند، آنگاه f یك به‌یك[1] نامیده می‌شود و گوییم که f مجموعهٔ X را در Y می‌نشاند. بنابراین f یك به‌یك است اگر وفقط اگر گزارهٔ

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

درست باشد. (در اینجا سورهای $\forall x_1\in X$ و $\forall x_2\in X$ را که درگزارهٔ فوق مستتر است، حذف کرده‌ایم. فقط هنگامی که خطر سوء تفاهم باشد، این چنین سورها را به گزاره‌های شرطی اضافه خواهیم کرد.)

مثال ۹.۲. تابع $x\longmapsto x^2 (\mathbf{R}\longrightarrow\mathbf{R})$ یك به‌یك‌نیست، زیرا $4\longmapsto 2$ و $4\longmapsto -2$. تابع $x\longmapsto x^3 (\mathbf{R}\longrightarrow\mathbf{R})$ یك به‌یك است، زیرا اگر x_1، x_2 حقیقی باشند، داریم: $x_1^3 = x_2^3 \Rightarrow x_1 = x_2$. ولی تابع $x\longmapsto x^3 (\mathbf{C}\longrightarrow\mathbf{C})$ یك به‌یك‌نیست، زیرا عدد ۱ در $\mathbf{C}$ دارای سه ریشهٔ سوم مختلف است.

مثال ۱۰.۲. اگر A زیرمجموعه‌ای از مجموعهٔ B باشد، آنگاه تابع $A\longrightarrow B$، که به ازاء هر $a\in A$، به وسیلهٔ $a\longmapsto a$ تعریف شده است، یك به یك است. این تابع، نگاشت شمول A در B نامیده می‌شود. (توجه: این تابع، با تابع همانی i_A فرق دارد چون‌حوزهٔ مقادیر تابع همانی، A است درصورتی‌که حوزهٔ مقادیر تابع شمول، B است.)

تابع $f : X\longrightarrow Y$ پروی نامیده می‌شود اگر هر عضو Y نقش لااقل یك عضو از X باشد، یعنی اگر $(\forall y\in Y)(\exists x\in X)(f(x) = y)$. نگاشتی که یك به‌یك و پروی باشد یك نگاشت دوسویی[2] یا یك تناظر یك به یك نامیده می‌شود.

برای ارائهٔ مثالها، مناسب است‌که نمادهای‌استانداردِ فاصله‌های محور حقیقی رامعرفی کنیم. اگر $a\leqslant b$ و $a, b\in\mathbf{R}$ آنگاه $[a, b]$ نمایش فاصلهٔ بستهٔ $\{x\in\mathbf{R} ; a\leqslant x\leqslant b\}$ می‌باشدکه حاوی نقاط انتهایی a و b است. اگر نقاط انتهایی را حذف‌کنیم فاصلهٔ باز $\{x\in\mathbf{R} ; a<x<b\}$ را به دست‌می‌آوریم که به وسیلهٔ (a, b) نشان‌داده‌می‌شود. همچنین نمادهای زیر را به‌کار می‌بریم:

$$[a, b) \quad \text{به‌جای} \quad \{x\in\mathbf{R} ; a\leqslant x<b\},$$

---

۱. مؤلف اصطلاح «injection» را به کار برده است کـه عده‌ای آن را «در نهاد» ترجمه کرده‌اند. البته دو اصطلاح «یك به یك» و «درنهاد» مترادف‌اند. ـم

۲. لغت «bijection» به «هم نهاد» هم ترجمه شده است. ـم

$[a, \infty)$ به‌جای $\{x \in \mathbf{R} ; x \geqslant a\}$،

$(-\infty, b)$ به‌جای $\{x \in \mathbf{R} ; x < b\}$.

قراردادهای مشابهی را برای $[a, b)$، (a, ∞)، $[a, \infty)$، $(-\infty, b]$ به‌کار می‌بریم.

مثال ۱۱.۲. نگاشت $x \longmapsto x^2$ از $\mathbf{R}$ به $[0, \infty)$، بروی‌است‌اما یك‌به‌یك‌نیست. نگاشت $x \longmapsto x^2$ از $[0, \infty)$ به $\mathbf{R}$ یك به یك است ولی بروی نیست. نگاشت $x \longmapsto x^2$ از $[0, \infty)$ به $[0, \infty)$ یك‌نگاشت دوسویی است. همچنین‌نگاشت $x \longmapsto x^3$ از $\mathbf{R}$ به $\mathbf{R}$ دوسویی است.

مثال ۱۲.۲. چنانچه‌سطوح را به‌عنوان مجموعه‌هایی ازنقاط درنظربگیریم آنگاه نقشه‌های جغرافیایی، به همان مفهوم ذکر شده در این‌کتاب، «نگاشت» هستند. به عنوان مثال، اگر X نمایش سطح زمین باشد (با فرض‌کروی بودن آن)، با حذف دو قطب آن، و اگر Y نمایش استوانه‌ای باشدکه منحنی هادی آن، خط استوا و مجور آن در امتداد محور قطبی باشد، آنگاه تصویر مرکاتور[1] (یعنی تصویر از مرکز زمین) تابعی مانند $f : X \longrightarrow Y$ را نتیجه می‌دهدکه در واقع دوسویی است.

قضیهٔ ۲ ب. فرض‌کنید $f : X \longrightarrow Y$ و $g : Y \longrightarrow Z$ دوتابع باشند، دراین‌صورت

(الف) اگر f و g هردویك به‌یك باشندآنگاه $g \circ f : X \longrightarrow Z$ یك‌به‌یك است؛

(ب) اگر f و g هردو بروی باشند آنگاه $g \circ f$ هم بروی است؛

(پ) اگر f و g هردو دوسویی باشند آنگاه $g \circ f$ نیز دوسویی است.

برهان. (الف) فرض کنید $x_1, x_2 \in X$ و $x_1 \neq x_2$. اگر f یك بـه یك باشد آنگاه $f(x_1) \neq f(x_2)$. چنانچه g نیز یك به یك باشد، از اینجا نتیجه می‌شود کـه $g(f(x_1)) \neq g(f(x_2))$. بنابراین اگر $x_1 \neq x_2$، آنگاه $(g \circ f)(x_1) \neq (g \circ f)(x_2)$؛ یعنی اینکه $g \circ f$ یك به یك است.

(ب) فرض‌کنید $z \in Z$. اگر g بروی باشد آنگاه عضوی مانند $y \in Y$ وجود داردکه $z = g(y)$. اگر f نیز بروی‌باشد، عنصر y را می‌توان، به‌ازاء یك عنصر $x \in X$، به‌صورت $y = f(x)$ نوشت. بنابراین به‌ازاء $x \in X$ داریم: $z = g(y) = g(f(x)) = (g \circ f)(x)$. چون این برای هر عنصر $z \in Z$ درست است، در نتیجه $g \circ f$ بروی می‌باشد.

(پ) این قسمت بلافاصله از (الف) و (ب) نتیجه می‌شود.

قضیهٔ ۲ پ. تابع $f : X \longrightarrow Y$ دارای‌معکوس $g : Y \longrightarrow X$ است‌اگروفقط‌اگر f دوسویی باشد. این تابع معکوس g، با فرض وجود، یکتاست وخود نیز دوسویی است.

---

1. Mercator's projection

برهان . اولا فرض کنید که f دارای معکوسی مانند g باشد . در این صورت به ازاء هر $x\in X$ ، $g(f(x))=x$ و به ازاء هر $y\in Y$ ، $f(g(y))=y$. اگر $x_1, x_2\in X$ و $f(x_1)=f(x_2)$ ، نتیجه می‌شود که

$$x_1=g(f(x_1))=g(f(x_2))=x_2,$$

بنابراین f یك به یك است. همچنین اگر $y\in Y$ ، آنگاه $y=f(g(y))$ که نقش عنصر $g(y)\in X$ تحت f است، لهذا f بروی است . این نشان می‌دهد که f یك تابع دو سویی است. همچنین، استدلال مشابهی نشان می‌دهد که g دوسویی است، زیرا g دارای معکوس (یعنی f) می‌باشد. یکتایی g بسادگی نتیجه می‌شود؛ زیرا فرض کنید g_1 و g_2 دو تابع معکوس f باشند. در این صورت به ازاء هر $y\in Y$ ، $f(g_1(y))=f(g_2(y))=y$. چون f یك به یك است، ازاینجا نتیجه می‌شود که به ازاء هر $y\in Y$ ، $g_1(y)=g_2(y)$ ، یعنی $g_1=g_2$.

حال فرض کنید که f دوسویی باشد. در این صورت به ازاء هر $y\in Y$ ، حداقل یك $x\in X$ به قسمی وجود دارد که $f(x)=y$ (زیرا f بروی است) . ولی برای y مفروض ، نمی‌تواند بیش از یك $x\in X$ موجود باشد به طوری که $f(x)=y$ (زیرا f یك به یك است). ازاین‌رو می‌توان $g(y)$ را همان عنصر یکتای $x\in X$ گرفت که $f(x)=y$ وبدین‌طریق یك تابع $g : Y\longrightarrow X$ به‌دست‌آورد. واضح است که g معکوس f است‌زیرا (الف) برطبق روش ساختن g ، به ازاء هر $y\in Y$ ، داریم : $f(g(y))=f(x)=y$ و (ب) اگر $x\in X$ وچنانچه y را برابر $f(x)$ بگیریم ، آنگاه ، بنا به ساختمان g ، $g(y)$ برابر است با x ، یعنی $g(f(x))=x$.

مثال ۱۳.۲. (الف) تابع $((0,\infty)\longrightarrow[0,\infty))\ x\longmapsto x^2$ دوسویی است و معکوس آن تابع $([0,\infty)\longrightarrow(0,\infty))\ y\longmapsto\sqrt{y}$ می‌باشد .

(ب) تابع $(\mathbf{R}\longrightarrow\mathbf{R})\ x\longmapsto 2x^3-1$ دوسویی است، زیرا ترکیب سه تابع دوسویی $x\longmapsto x^3$ ، $y\longmapsto 2y-1$ و $z\longmapsto z$ است. معکوس تابع $t\longmapsto\sqrt[3]{(t+1)/2}$ می‌باشد .

مثال ۱۴.۲. سری نمایی

$$\sum_{n=0}^{\infty}\frac{x^n}{n!}$$

به ازاء هرعدد حقیقی x متقارب است وحاصلجمع آن ، که به‌وسیلهٔ e^x نشان داده می‌شود، برابر یك عدد حقیقی است که با معلوم بودن x ، به‌طور یکتا معین می‌شود. بنابراین تابعی مانند $(\mathbf{R}\longrightarrow\mathbf{R})\ x\longmapsto e^x$ داریم که به‌تابع نمایی موسوم است. ازآنالیز مقدماتی به‌مطالب زیردر مورد تابع نمایی آشنایی داریم:

(الف) تابعی است اکیداً صعودی؛ (ب) مقادیرش همواره مثبت‌اند؛ (پ) پیوسته است؛ و

(ت) $\lim_{x\to-\infty} e^x = 0$ ، $\lim_{x\to+\infty} e^x = +\infty$.

از (الف) نتیجه می‌شود که تابع نمایی هیچگاه یك مقدار را دوبار اختیار نمی‌کند، یعنی $x \longmapsto e^x (\mathbf{R}\longrightarrow\mathbf{R})$ یك به‌یك‌است. بااستفاده از (ب)، واضح است‌که این تابع، بروی نیست. معهذا اگرتابع تحدیدی آن را $x\longmapsto e^x (\mathbf{R}\longrightarrow(0,\infty))$ درنظربگیریم، بروی بودن این تابع تحدیدی از (پ) و (ت) نتیجه می‌شود. استدلال بدین طریق است که بنابه (ت)، e^x مقادیرمثبت به‌دلخواه کوچك و به‌دلخواه بزرگ را اختیار می‌کند وچون پیوسته هم‌هست، تمام‌مقادیر فی مابین، وبالنتیجه تمام مقادیر مثبت‌را اختیارخواهدکرد. (به‌صفحات ۱۰۵ تا ۱۰۷ کتاب [۳] مراجعه شود.) بنابراین یك تابع دوسویی $x \longmapsto e^x$ از $\mathbf{R}$ به $(0,\infty)$ داریم‌که دارای‌یك‌تابع‌معکوس یکتا از $(0,\infty)$ به $\mathbf{R}$ است. این‌تابع معکوس تابع لگاریتمی نامیده می‌شود وبا $y\longmapsto \log y$ نشان داده می‌شود. این تابع به ازاء هر $y>0$ ، بدین صورت تعریف می‌شود: $\log y$ عدد حقیقی یکتای x است که $e^x = y$. چون تابع لگاریتمی معکوس تابع نمایی است، بنابراین در شرایط $e^{\log y} = y$ به ازاء هر $y>0$ و $\log(e^x) = x$ به ازاء هر $x\in\mathbf{R}$ ، صدق می‌کند.

مثال اخیرنشان می‌دهدکه توابع دوسویی ومعکوسشان در آنالیز مهم هستند. اهمیت آنها در نظریهٔ مجموعه‌ها از پدیدهٔ شمارش ناشی شده است. اینکه یك مجموعه از اشیاء را دقیقاً بشماریم و بعدبا اطمینان بفهمیم‌که n عضو دارد، معنی‌اش این است‌که می‌توان یك تناظر یك به‌یك (دوسویی) ازآن مجموعه به‌مجموعهٔ اعداد $\{1, 2, \dots, n\}$ برقرارکرد. مجموعهٔ Xرا مشابه مجموعهٔ Yگوییم اگریك‌تابع‌دوسویی‌از X به Y وجود داشته‌باشد ودر این حالت می‌نویسیم $X\simeq Y$. بنابه قضیهٔ ۲پ ، اگر $X\simeq Y$ ، آنگاه $Y\simeq X$. همچنین از قضیهٔ ۲ ب نتیجه‌می‌شودکه اگر $X\simeq Y$ و $Y\simeq Z$ آنگاه $X\simeq Z$. مجموعهٔ X متناهی‌است اگر $n\in\mathbf{N}$ وجود داشته باشد، به قسمی‌که Xمشابه‌مجموعهٔ $\{1, 2, \dots, n\}$ باشد. این‌عدد n عدد اصلی یا مرتبهٔ X نامیده می‌شود و با $|X|$ نشان داده می‌شود. این عدد به وسیلهٔ X به طوریکتا معین می‌گردد، زیرا به‌ازاء n های مختلف ، هیچ دو مجموعهٔ $\{1, 2, \dots, n\}$ مشابه هم نیستند. (این حکم اخیر را در فصل ۳ ثابت خواهیم‌کرد.) مجموعه‌ای که متناهی نیست نامتناهی نامیده می‌شود. مثلا، خود $\mathbf{N}$ نامتناهی است. مجموعه‌ای‌که مشابه با $\mathbf{N}$ یا زیرمجموعه‌ای از $\mathbf{N}$ باشد شمارش‌پذیر نامیده می‌شود.

مثال ۱۵۰۲. تمام مجموعه‌های متناهی شمارش‌پذیرهستند. مجموعهٔ تمام اعـــــدادصحیح شمارش‌پذیراست. برای اثبات این امرکافی است به تابع $f : \mathbf{Z}\longrightarrow\mathbf{N}$ توجه‌کنیم که با دستور زیر تعریف می‌شود:

$$\begin{cases} f(x) = 2x & \text{اگر } x \geqslant 0 \\ f(x) = -2x-1 & \text{اگر } x < 0 \end{cases}$$

این تابع اعداد صحیح را به‌ترتیب ۰ ، ۱ — ، ۱ ، ۲ — ، ۲ ، ۳ — ، ... می‌شمارد. حقیقت شگفتی که می‌توانند به چند طریق اثبات شود آن است که مجموعهٔ تمام اعداد گویا نیز شمارش‌پذیر است. یك راه اثبات این است: هر عدد گویای غیرصفر x به‌طور یکتا به صورت $x=(-1)^r p/q$ قابل بیان است، که در آن p و q اعداد صحیح مثبتی هستند با بزرگترین مقسوم‌علیه مشترك ۱ ، و r مساوی ۱ یا ۲ است. اگر x را به $2^r 3^p 5^q$ و ۰ را به ۰ بنگاریم، یك تابع یك‌به‌یك $\mathbf{N} \longrightarrow \mathbf{Q}$ به‌دست می‌آوریم که تشابه $\mathbf{Q}$ را با زیرمجموعه‌ای از $\mathbf{N}$ نتیجه می‌دهد. با کوشش بیشتر می‌توان یك تابع دوسویی از $\mathbf{Q}$ به $\mathbf{N}$ پیدا کرد.

مجموعهٔ اعداد حقیقی $\mathbf{R}$ شمارش‌پذیر نیست. بنابراین، این درست نیست که تمام مجموعه‌های نامتناهی مشابه‌اند، و همین حقیقت است که شخص را به مطالعهٔ اعداد اصلی نامتناهی هدایت می‌کند، موضوعی که خارج از بحث کتاب حاضر است (به‌عنوان مثال، صفحات ۹۰ تا ۹۸ کتاب هالموس[1] [۴] را ملاحظه کنید.) به‌نظر می‌رسد تعریف تابع که درفوق آمده است امکان تعریف توابع چندمتغیره را مقدور نسازد. لیکن روش سادهٔ زیر ما را قادر به بحث در توابع چند متغیره می‌نماید. دو مجموعهٔ A و B مفروض‌اند حاصلضرب‌شان $A \times B$ را برابر مجموعهٔ تمام جفتهای مرتب* (a , b) که $a \in A$ و $b \in B$ ، تعریف می‌کنیم. در اینجا جفت مرتب معنی خاصتری از یك مجموعهٔ دوعنصری دارد. ترتیب نوشتن عناصر در مجموعهٔ $\{a , b\}$ اهمیتی ندارد؛ یعنی $\{a , b\} = \{b , a\}$. لیکن برای جفتهای مرتب $(a , b) \neq (b , a)$ ، مگر اینکه $a = b$ ؛ درواقع $(a , b) = (c , d)$ اگر و فقط اگر $a = c$ و $b = d$. بنابراین اگر $|A| = m$ و $|B| = n$ ، آنگاه برای هر کدام از m عنصر ممکن $a \in A$ ، n جفت مختلف (a , b) وجود دارد در نتیجه $|A \times B| = mn$. حاصلضرب سه مجموعهٔ $A \times B \times C$ مساوی مجموعهٔ تمام سه‌تاییهای مرتب (a , b , c) می‌باشد، که در آن $a \in A$ ، $b \in B$ ، $c \in C$ وهیچ اشکالی در یکی دانستن این حاصلضرب با $(A \times B) \times C$ یا $A \times (B \times C)$ وجود ندارد، زیرا این حاصلضربهای مختلف به‌وسیلهٔ نگاشتهای بدیهی‌ای که عناصر (a , b , c) ، $((a , b) , c)$ و $(a , (b , c))$ را متناظر قرار می‌دهند، مشابه هستند. همین حکم برای هر حاصلضرب تعداد متناهی از مجموعه‌ها، $A_1 \times A_2 \times \cdots \times A_n$، برقرار است.

اکنون برای مجموعه‌های دلخواه X ، Y و Z تابع $f : X \times Y \longrightarrow Z$ را در نظر می‌گیریم. تابع f به هر عنصر $(x , y) \in X \times Y$ ، عنصری از Z را نسبت می‌دهد که با $f(x , y)$ نشان داده می‌شود. مقدار f به‌وسیلهٔ $x \in X$ و $y \in Y$ به‌طور یکتا معین می‌شود. این همان تابع دومتغیرهٔ مورد نظر ماست، و باید توجه شود که ممکن است دومتغیر آن، از نوع کاملا متفاوتی باشند، بدین معنی که از مجموعه‌های مختلف X و Y انتخاب شوند.

مثال ۱۶۰۲. مجموعهٔ $\mathbf{R} \times \mathbf{R}$ (که به‌صورت $\mathbf{R}^2$ نیز نوشته می‌شود) متشکل است از تمام

---

1. Halmos

* باعث تأسف است که نماد $(a \text{ و } b)$ برای فاصله‌های باز در $\mathbf{R}$ نیز به‌کار رفته‌است، ولی همواره متن نشان خواهد داد که کدام یك مورد نظر است.

جفتهای مرتب $(x\ ,\ y)$ از اعداد حقیقی. این مجموعه به‌عنوان صفحهٔ دکارتی یا صفحهٔ حقیقی شناخته شده است وموضوع هندسهٔ مختصاتی یا هندسهٔ تحلیلی مسطحه است. عناصر $(x\ ,\ y)$ نقاط، واعداد x و y مختصات نقطهٔ $(x\ ,\ y)$ نامیده می‌شوند. (روشهای دیگر هندسی‌تری برای تعریف صفحه وجود دارد، اما درآن تعاریف باید بعداً ثابت شود که صفحه رامی‌توان، به‌طریقی که گفتیم، مختصاتی کرد.) یك تابع $f : \mathbf{R}\times\mathbf{R}\longrightarrow\mathbf{R}$ که مثلا به‌وسیلهٔ $(x\ ,\ y)\longmapsto x^{۲}+y^{۲}$ تعریف شود، به‌مفهوم معمول کلمه، تابعی با مقدار حقیقی از دو متغیر حقیقی است، وازنظرگاه هندسی می‌تواند به‌عنوان نگاشتی ازصفحهٔ حقیقی به‌محور حقیقی تصور شود. ازطرف دیگر تابعی مانند $g : \mathbf{R}\longrightarrow\mathbf{R}\times\mathbf{R}$ که به‌وسیلهٔ $t\longmapsto(\cos t\ ,\ \sin t)$ تعریف می‌شود، به منحنی پارامتری موسوم است؛ این تابع خاص، محور حقیقی را بتوی صفحه می‌نگارد و درواقع تمام نقاط خط را به نقاط یك دایره می‌برد. توابع از صفحه به صفحه مانند $(x\ ,\ y)\longmapsto(x\cos y\ ,\ x\sin y)$ نیز همواره درآنالیز ظاهر می‌شوند. امروزه، همهٔ اینها حالات خاصی ازهمان تعریف تابع هستند.

تابع $f : A\times A\longrightarrow A$ یك عمل دوتایی روی A نامیده می‌شود. این تابع می‌تواند به‌هردو عنصر $a_{۱}\ ,\ a_{۲}\in A$ اثرنموده وعنصر سومی مانند $f(a_{۱}\ ,\ a_{۲})$ را به‌دست‌دهد. باهمین روش می‌توانیم اعمال سه‌تایی $A^{۳}=A\times A\times A\longrightarrow A$ و به‌طور کلی اعمال n تایی $A^{n}\longrightarrow A$ را تعریف کنیم. درحالت خاص، عمل یکتایی روی A به‌معنی تابعی است از A به A.

قسمت عمده‌ای از جبر صرف مطالعهٔ اعمال برروی مجموعه‌ها می‌شود واین کتاب عمدتاً به‌بررسی اعمال یکتایی و دوتایی‌ای که بیشتر ازبقیه به‌کار می‌آیند، اختصاص داده شده است. اعمال سه‌تایی وبالاتر، ازجنبهٔ علمی دارای اهمیت بیشتری هستند ودیگر ذکری ازآنها نخواهد رفت. اعمال دوتایی غالباً دارای علائم ویژه‌ای مانند $+$ ، $\times$ ، $\circ$ هستند که دربین متغیرها قرار می‌گیرند. برای اعمال یکتایی نمادهای مختلف زیادی به‌کار می‌رود.

مثال ۱۷۰۲. جمع روی $\mathbf{R}$ عملی دوتایی است که با $(x\ ,\ y)\longmapsto x+y$ ارائه می‌شود. همین دستور، عملی دوتایی روی $\mathbf{Z}$ تعریف می‌کند، چون مجموع دو عدد صحیح یك عدد صحیح است. به همین ترتیب $x\longmapsto -x$ عملی است یکتایی روی $\mathbf{R}$ یا $\mathbf{Z}$، ولی نه روی $\mathbf{N}$. توجه کنید که معکوس‌گیری $x\longmapsto x^{-۱}$ عملی روی $\mathbf{R}$ نیست زیرا در $x=۰$ نمی‌تواند به‌کار رود. لیکن $x\longmapsto x^{-۱}$ روی $(۰\ ,\ \infty)$ یك عمل یکتایی است.

مثال ۱۸۰۲. هنگام مشخص نمودن یك عمل، مهم است که مطمئن باشیم حوزهٔ تعریفش معین است و همچنین خودش به عنوان یك تابع، بدرستی تعریف شده است. با آوردن مثالی، یکی از اشتباهات بسیار رایج در این مورد را بیان می‌کنیم. هرعدد گویای q را می‌توان به صورت a/b نوشت، که در آن $a\ ,\ b\in\mathbf{Z}$ و $b\neq ۰$. بنابراین ظاهراً می‌توان عمل دوتایی $*$ را با دستور زیر روی $\mathbf{Q}$ تعریف کرد:

$$\frac{a}{b}*\frac{c}{d}=\frac{a+c}{bd}.$$

ولی عدد گویای q صورت و مخرجش، یعنی a و b، را به طور یکتا معین نمی‌کند، از اینرو دلیلی وجود ندارد که انتظار داشته باشیم $(a+c)/bd$ به‌کمك اعداد گویای a/b و c/d به طور یکتا معین می‌شـــود. در واقع، حاصل به طور یکتا معین نمی‌شود، زیرا بنا به تعریف داریم:

$$\frac{۱}{۲}*\frac{۱}{۳}=\frac{۲}{۶}=\frac{۱}{۳}$$

ولی:

$$\frac{۲}{۴}*\frac{۱}{۳}=\frac{۳}{۱۲}\neq\frac{۱}{۳}$$

گرچه:

$$\frac{۱}{۲}=\frac{۲}{۴}$$

از طرف دیگر دستور

$$\frac{a}{b}*\frac{c}{d}=\frac{ac}{bd}$$

یك عمل دوتایی روی **Q** تعریف می‌کند (ضرب اعداد گویا) زیرا اگر

$$\frac{c}{d}=\frac{c'}{d'}\ ,\ \frac{a}{b}=\frac{a'}{b'}$$

می‌توان نتیجه گرفت که:

$$\frac{ac}{bd}=\frac{a'c'}{b'd'}.$$

درفصول آینده به این نکته برخواهیم گشت ولی به خواننده توصیه می‌شود دربارهٔ اختلاف این دو دستور خوب فکر کند و تمرین ۱۶ را انجام دهد.

بررسی مقدماتی نظریهٔ مجموعه‌ها را با نگاهی کوتاه به تناظرها و رابطه‌ها به پایان می‌رسانیم. درآینده به طور قابل توجهی از رابطه‌های هم ارزی و، به مقیاس کمتری، از رابطه‌های ترتیبی استفاده خواهیم کرد.

نخست یك تناظر از مجموعـهٔ X به Y به وسیلهٔ قاعدهٔ کلیتر از قاعـــدهٔ تـابع داده می‌شود. این قاعـده مشخص می‌کند کـه عناصر معینی از X «متناظر» با عناصر معینی از Y هستند وفقط لازم است که قاعده، به ازاء هرجفت $(x\ ,\ y)\in X\times Y$، تعیین کند که آیا x

با y متناظر هست یا خیر. اگر γ نمایش چنین تناظری باشد، $x\,\gamma\,y$ را به معنی اینکه x متناظر با y است، می‌نویسیم. دراین نماد γ به‌عنوان یك فعل استفاده می‌شود و $x\,\gamma\,y$ یك گزاره است. مثالهایی از علائمی که بدین طریق برای تناظرها به‌کار گرفته می‌شوند عبارتند از: $=$ ، $>$ ، $\leqslant$ ، $\neq$ ، $\in$ ، $\subset$ ، $\supset$ ، $\perp$. یك تابع از X به Y حالت خاصی از یك تناظر γ از X به Y است که در شرایط زیر صدق کند:

(الف) به ازاء هر $x\in X$ حداقل یك $y\in Y$ به‌قسمی وجود دارد که $x\,\gamma\,y$ ، و

(ب) به‌ازاء هر $x\in X$ و هر $y_1\in Y$ ، $y_2\in Y$ ، اگر $x\gamma y_1$ و $x\,\gamma\,y_2$ آنگاه $y_1=y_2$.

مثال ۱۹۰۲. فرض کنید X مجموعهٔ تمام نقاط صفحه و Y مجموعهٔ تمام خطوط آن باشد. دراین‌صورت قرارداشتن نقاط برخطوط، یك تناظر γ از X به Y است که به‌وسیلهٔ $x\gamma y \iff$ نقطهٔ x برخط y قرار دارد. تعریف می‌شود. البته مشابهاً گزارهٔ «نقطهٔ x برخط y قرار ندارد» یك تناظر تعریف می‌کند، همچنانکه هر عبارت در مورد x و y که معنی‌دار بوده و به ازاء هرجفت ممکن $(x\,,\,y)$ یا درست یا نادرست باشد، یك تناظر تعریف می‌کند. دو تناظر γ ، γ' از X به Y مساوی در نظر گرفته می‌شوند اگر $x\,\gamma'\,y \iff x\,\gamma\,y$.

برای هرمجموعهٔ X ، یك تناظر از X به خودش یك رابطه روی X نامیده می‌شود. مثلا، اگر X مجموعهٔ افراد بشر باشد، آنگاه مفهوم «عمو» یك رابطهٔ ρ روی X تعریف می‌کند، بدین‌صورت: $a\,\rho\,b \iff a$ عموی b است، که در آن $a\,,\,b\in X$. به همین‌ترتیب تمام مفاهیم «برادر»، «پدر»، «جد»، «دوست»، «دشمن» رابطه‌هایی روی X تعریف می‌کنند. برای مثالهای ریاضی خیلی مجبور نیستیم نگران باشیم: $\geqslant$ روی $\mathbf{R}$ ؛ $=$ روی هرمجموعه ؛ $\subset$ روی مجموعهٔ زیرمجموعه‌های یك مجموعهٔ مفروض ؛ تقسیم‌پذیری روی $\mathbf{Z}$ ($m\,\rho\,n$ اگر n مضرب صحیحی از m باشد) رابطه می‌باشند. همچنین هرمعادلهٔ $f(x\,,\,y)=0$ یك رابطه روی $\mathbf{R}$ تعریف می‌کند که اگر f تابعی از $\mathbf{R}$ به $\mathbf{R}$ باشد؛ ρ دراین‌مورد به‌صورت $x\rho y \iff f(x\,,\,y)=0$ می‌باشد.

در ریاضیات به وفور با انواع مختلفی از رابطه‌ها با خواص ویژه مواجه می‌شویم. انواع زیر مورد توجه خاص‌اند:

(الف) رابطهٔ ρ روی X انعکاسی است اگر به ازاء هر $x\in X$ ، $x\rho x$ ؛

(ب) رابطهٔ ρ روی X متقارن است اگر به ازاء هر $x\,,\,y\in X$ ، $x\rho y \Rightarrow y\rho x$ ؛

(پ) رابطهٔ ρ روی X پادمتقارن است اگر به ازاء هر $x\,,\,y\in X$ ، $(x\rho y \text{ و } y\rho x) \Rightarrow x=y$ ؛

(ت) رابطهٔ ρ روی X متعدی است اگر به ازاء هر $x\,,\,y\,,\,z\in X$ ، $(x\rho y \text{ و } y\rho z) \Rightarrow x\rho z$.

مثال ۲۰۰۲. در مجموعهٔ تمام افراد بشر رابطهٔ «برادری» متقارن نیست؛ ولی رابطهٔ «همخونی»

متقارن است؛ رابطهٔ «والد» متعدی نیست ولی رابطهٔ «جد» متعدی است. رابطهٔ $\geqslant$ روی $\mathbf{R}$ انعکاسی، پاد متقارن و متعدی است. رابطهٔ $\neq$ روی $\mathbf{R}$ متقارن است (ولی متعدی نیست). رابطهٔ $=$ روی $\mathbf{R}$ انعکاسی، متقارن، پادمتقارن و متعدی است.

کاربردهای اصلی رابطه‌ها در ریاضیات برای مقایسه و رده‌بندی است. برای مقایسه یا مرتب نمودن عناصر یك مجموعهٔ X نیاز به معرفی رابطه‌ای مانند ρ روی X است، که درآن $x\rho y$ بدین معنی باشد که x از جهتی مقدم یا مسلط بر y است. چنین رابطه‌هایی غالباً متعدی و پادمتقارن خواهند بود و برای سهولت معمولا آنها را طوری تعریف‌می‌کنند که انعکاسی هم باشند. رابطه‌ای که دارای این سه خاصیت باشد رابطهٔ ترتیبی نامیده‌می‌شود، و مثالهای معروف این نوع رابطه عبارت‌اند از: $\geqslant$ روی $\mathbf{R}$؛ $\leqslant$ روی $\mathbf{R}$؛ $\subset$ روی مجموعهٔ زیر مجموعه‌های یك مجموعهٔ ثابت؛ تقسیم‌پذیری برروی مجموعهٔ اعداد صحیح مثبت (اما تقسیم‌پذیری روی $\mathbf{Z}$ به‌دلیل اینکه ۱ و ۱ — برهم قابل قسمت‌اند، رابطهٔ ترتیبی نیست). رابطهٔ $\geqslant$ روی $\mathbf{R}$ رابطهٔ ترتیبی جالبی است زیرا به کمك آن هردو عدد حقیقی می‌توانند با هم مقایسه شوند: همیشه یا $x\geqslant y$ یا $y\geqslant x$. چنین رابطه‌ای (یعنی یك رابطهٔ ترتیبی ρ روی X به قسمی که $(\forall x, y\in X)\ (x\rho y$ یا $y\rho x)$) رابطهٔ ترتیبی کلی یا رابطهٔ ترتیبی‌خطی نامیده می‌شود زیرا نظم کاملی از عناصر X را به‌دست‌می‌دهد. رابطه‌های $\subset$ روی مجموعهٔ زیرمجموعه‌های یك مجموعه و تقسیم‌پذیری روی مجموعهٔ اعداد صحیح مثبت روابط ترتیبی خطی نیستند.

برای اهداف رده‌بندی نوع نسبتاً متفاوتی‌از رابطه مورد نیاز است. رده‌بندی عناصر مجموعهٔ X، تقسیم آن به زیرمجموعه‌های جدا از هم است، یعنی تشکیل افرازی از X. به عبارت دقیقتر یك افرازاز X مجموعه‌ای از زیرمجموعه‌های X_i از X است، که i در یك‌مجموعهٔ اندیس‌گذار I تغییر می‌کند، به قسمی که

$$\text{(الف)}\qquad \bigcup_{i\in I} X_i = X \quad \text{و}$$

$$\text{(ب)}\qquad \text{اگر } i\neq j,\ X_i\cap X_j=\emptyset .$$

مجموعه‌های X_i رده‌های افرازنامیده می‌شوند. رابطهٔ ρ روی X مفروض است، می‌خواهیم عناصر X را طوری رده‌بندی‌کنیم که دو عنصر در یك رده قرارگیرند اگر و فقط اگر به وسیلهٔ ρ به هم مرتبط شوند. این امر گاهی‌امکان‌پذیر است و گاهی هم نیست. به عنوان‌مثال، اگر X مجموعهٔ افراد بشر باشد و $x\rho y$ بدین‌معنی باشدکه x و y تعدادمساوی مو برروی سرشان دارند، آنگاه رده‌بندی امکان‌پذیر است. از طرف دیگر، اگر $x\rho y$ بدین معنی‌باشد که x، y را می‌شناسدآنگاه چنین رده‌بندی‌ای امکان‌پذیرنیست. اینها مثالهای روشنی‌هستند، اما اگر ρ یك رابطهٔ ریاضی و، ازجمله، رابطه‌ای بر روی $\mathbf{Z}$ باشدکه درآن $x\rho y$ یعنی $x-y$ برعدد ۷ قابل قسمت است، ممکن است خیلی روشن نباشدکه آیا یك رده‌بندی امکان‌پذیراست یا نه. بنابراین نیاز به محکی برای تصمیم‌گیری دراین مورد داریم که آیا یك رابطهٔ مفروض برای رده‌بندی مناسب است یا خیر، واین به‌کمك تعریف و قضیهٔ زیر ارائه می‌شود.

تعریف. رابطهٔ ρ روی مجموعهٔ X یك رابطهٔ هم‌ارزی است اگر انعکاسی، متقارن و متعدی باشد.

قضیهٔ ۲ ت. (الف) یك افراز $X = \bigcup_{i \in I} X_i$ ازمجموعهٔ X مفروض‌است ، رابطهٔ σ روی X که به وسیلهٔ «$x \sigma y \Longleftrightarrow x$ و y در یك ردهٔ X_i از افراز قرار دارند» تعریف شده ، یك رابطهٔ هم‌ارزی است.

(ب) اگر ρ یك رابطهٔ هم‌ارزی روی X باشدآنگاه افرازی مانند $X = \bigcup_{i \in I} X_i$ از X به‌قسمی وجود داردکه عناصر x و y از X دریك ردهٔ X_i قرار می‌گیرند اگر و فقط اگر $x \rho y$.

برهان. (الف) ازتعریف افراز به‌روشنی پیداست که رابطهٔσ که به‌این‌طریق‌تعریف شده‌است یك‌رابطهٔ هم‌ارزی است.

(ب) فرض کنیدρ یك رابطهٔ هم‌ارزی رویX باشد. برای هر $x \in X$ ، قرار می‌دهیم:

$\{y \in X ; y \rho x\} = \langle x \rangle$. درآن‌صورت $x \in \langle x \rangle$ (زیرا $x \rho x$ برقرار است) و $\langle x \rangle$ را ردهٔ هم‌ارزی‌شامل x می‌نامیم. نشان می‌دهیم که

(آ) اگر $x \rho y$ آنگاه $\langle x \rangle = \langle y \rangle$ ، و

(ب) اگر $\neg x \rho y$ آنگاه $\langle x \rangle \cap \langle y \rangle = \varnothing$.

اولا ، اگر $x \rho y$ و t عضو دلخواهی از $\langle x \rangle$ باشد، آنگاه بنا به تعریف $t \rho x$ درست است و چون ρ متعدی است داریم $t \rho y$ ، یعنی $t \in \langle y \rangle$. بنابراین نشان داده‌ایم که‌اگر $x \rho y$ آنگاه $\langle x \rangle \subset \langle y \rangle$. امابه متقارن‌است‌لهذا اگر $x \rho y$آنگاه $y \rho x$، که‌همان استدلال نتیجه می‌دهد $\langle x \rangle \supset \langle y \rangle$ واین‌قسمت (آ) را ثابت‌می‌کند. ازطرف دیگر، اگر $\langle x \rangle$ و $\langle y \rangle$ دارای عنصری مشترك باشند ، یعنی $u \rho x$ و $u \rho y$ ، آنگاه بنا به خاصیت تقارن ، $x \rho u$ وازاینجا بنا به خاصیت تعدی داریم $x \rho y$ ، که در نتیجه قسمت (ب) اثبات می‌شود . عبارات (آ) و (ب) با هم نتیجه می‌دهند که رده‌های هم‌ارزی مختلف ، جدا ازهم هستند و دوعنصر x و y دریك رده قرار دارند اگر وفقط اگر $x \rho y$. اتحاد تمام رده‌های $\langle x \rangle$ مساوی X است (چون $x \in \langle x \rangle$) . بنابراین دستهٔ تمام مجموعه‌های متمایز به‌صورت $\langle x \rangle$ یك افراز از X را باخواص مذکور تشکیل می‌دهد.

مثال ۲۱.۲. رابطهٔ $\sim$ روی $\mathbf{R}^2$ که به‌وسیلهٔ $(x, y) \sim (x', y') \Longleftrightarrow y - y' = 2(x - x')$ تعریف شده است یك رابطهٔ هم‌ارزی است. رده‌های هم‌ارزی خطوط موازی $y = 2x + c$ هستند، به‌ازاء اعداد حقیقی مختلف c .

مثال ۲۲.۲. فرض کنید A مجموعهٔ $\mathbf{R}^2$ با حذف مبدأ $(0, 0)$ باشد . رابطهٔ $\sim$ که

روی A به‌وسیلهٔ

$$(x\ ,\ y)\sim(x'\ ,\ y')\Longleftrightarrow(\exists\lambda\in\mathbf{R})(\lambda x=x'\ \text{و}\ \lambda y=y')$$

تعریف شده است یك‌رابطهٔ هم‌ارزی است. یك ردهٔ هم‌ارزی نمونه‌ای، شامل تمام نقاط (به‌استثنای مبدأ) خطی است که ازمبدأ می‌گذرد.

مثال ۲۳.۲. فرض کنید $f:X\longrightarrow Y$ تابع دلخواهی باشد. آنگاه رابطهٔ $\sim$ که روی X به‌وسیلهٔ

$$x_1\sim x_2\Longleftrightarrow f(x_1)=f(x_2)$$

تعریف شده‌است یك‌رابطهٔ هم‌ارزی است‌ورده‌های هم‌ارزی‌آن بافتهای f نامیده‌می‌شوند. یك بافت نمونه‌ای، مجموعهٔ تمام $x\in X$ هایی است‌که به‌ازاء آنها $f(x)$ یك مقدار ثابت را اختیارمی‌کند.

مثال اخیر ازجهتی نمونه است. هر رابطهٔ هم‌ارزی را می‌توان به‌همین‌طریق باتابعی ارتباط داد. رابطهٔ هم‌ارزی ρ روی X مفروض است، مجموعهٔ جدید X/ρ را تشکیل می‌دهیم که اعضایش رده‌های هم‌ارزی ρ می‌باشند. بنابراین X/ρ مجموعه‌ای از زیر - مجموعه‌های X است ونباید باخود X اشتباه‌شود. اگر $x\in X$ ، آنگاه ردهٔ هم‌ارزی $\langle x\rangle$ که شامل x است، عضوی است از X/ρ ، ومی‌توانیم نگاشتی مانند f از X به X/ρ ، به‌ازاء هر $x\in X$ ، با قاعدهٔ $x\longmapsto\langle x\rangle$ تعریف کنیم. آنگاه

$$f(x_1)=f(x_2)\Longleftrightarrow\langle x_1\rangle=\langle x_2\rangle\Longleftrightarrow x_1\rho x_2\ .$$

ازاینرو بافتهای این‌نگاشت رده‌های هم‌ارزی ρ هستند. مجموعهٔ X/ρ مجموعهٔ‌خارج‌قسمت X به‌وسیلهٔ رابطهٔ هم‌ارزی ρ نامیده می‌شود، ونگاشت $x\longmapsto\langle x\rangle$ نگاشت متعارفی یا نگاشت خارج‌قسمت از X به X/ρ نامیده می‌شود. ساختن مجموعه‌های خارج‌قسمت روش بسیار مهمی برای ارائهٔ مفاهیم جدید ریاضی از روی مفاهیم قبلی است، وبعداً کاربردش را درچندین زمینه خواهیم دید.

مثال ۲۴.۲. درمثال ۲۱.۲ مجموعهٔ خارج‌قسمت $\mathbf{R}^2/\sim$ مجموعهٔ تمام خطوط باشیب ۲ درصفحهٔ $\mathbf{R}^2$ است، ونگاشت خارج‌قسمت‌هر نقطه را به‌خطی‌که ازآن‌نقطه باشیب۲می‌گذرد، می‌نگارد. درمثال ۲۲.۲ مجموعهٔ خارج‌قسمت $A/\sim$ مجموعهٔ تمام خطوط صفحهٔ $\mathbf{R}^2$ است که از مبدأ می‌گذرند ومبدأ درآنها محذوف است. برای هرشیب ممکن، یعنی بـــه‌ازاء هرعدد حقیقی؛ عنصری در $A/\sim$ وجود دارد ویك خط‌هم برای شیب بینهایت موجوداست. بنابراین $A/\sim$ مشابه است با $\mathbf{R}$ باضافهٔ عنصراضافی ∞ . $A/\sim$ خط تصویری‌حقیقی‌نامیده می‌شود و دارای اهمیت اساسی درمطالعهٔ هندسهٔ تصویری است. دراین هندسه نقاط یك‌خط به‌وسیلهٔ جفت $(x\ ,\ y)$ ، که هردوباهم صفر نیستند، از اعداد حقیقی نمایش داده می‌شوند، ولی درآن، $(x\ ,\ y)$ و $(\lambda x\ ,\ \lambda y)$ همواره نمایش یك نقطه‌اند.

قضیهٔ ۲ ث. فرض‌کنید ρ یك رابطهٔ هم‌ارزی روی مجموعهٔ A و $q : A \longrightarrow A/\rho$ نگاشت خارج قسمت باشد. اگر $f : A \longrightarrow B$ تابع مفروضی باشد. آنگاه دو شرط زیر معادل‌اند (یعنی، هرکدام دیگری را نتیجه می‌دهد):

(الف) تابعی مانند $g : A/\rho \longrightarrow B$ به‌قسمی وجود داردکه $g \circ q = f$؛

(ب) به‌ازاء هر $x, y \in A$، $x \rho y \Rightarrow f(x) = f(y)$.

برهان. (الف)$\Leftarrow$(ب): بنا به‌تعریف q، اگر $x \rho y$ آنگاه $q(x) = q(y)$ = ردهٔ هم‌ارزی شامل x و y. اگر تابعی مانند $g : A/\rho \longrightarrow B$ وجود داشته باشد که $f = g \circ q$، آنگاه نتیجه می‌شود که $f(x) = g(q(x)) = g(q(y)) = f(y)$.

(ب)$\Leftarrow$(الف) : فرض‌کنیدشرط (ب) برقرارباشد. دراین‌صورت اثر f روی هر ردهٔ هم‌ارزی ثابت است، یعنی مقدارآن به‌ازاء تمام اعضای هر ردهٔ هم‌ارزی مفروض، ثابت می‌باشد. ازاینرو، برای هر ردهٔ هم‌ارزی $X \in A/\rho$ می‌توانیم قرار دهیم: $g(X) = f(x)$، که درآن x عضو دلخواهی از X است. این $g(X)$، به‌علت ثابت بودن f روی X، به‌طور یکتا به‌وسیلهٔ X معین می‌شود. بدین‌ترتیب، تابعی مانند $g : A/\rho \longrightarrow B$ تعریف کرده‌ایم. چون به‌ازاء هر $x \in A$، $(g \circ q)(x) = g(\langle x \rangle) = f(x)$ داریم $g \circ q = f$.

خاصیت نگاشت خارج قسمت که درقضیهٔ فوق اثبات شده است اولین‌مثال ازخاصیت «جامع» می‌باشد. ازاین‌قضیه نتیجه می‌شودکه $q : A \longrightarrow A/\rho$ دربین توابع f باحوزهٔ تعریف A به‌قسمی‌که $x \rho y \Rightarrow f(x) = f(y)$، جامع است. این بدین‌معنی است‌که (آ) $x \rho y \Rightarrow q(x) = q(y)$ و (ب) هرتابع f که در $x \rho y \Rightarrow f(x) = f(y)$ صدق کند، می‌تواند از ترکیب q با تابع دیگری به‌دست آید. بعداً مثالهای دیگری از خواص جامع می‌آوریم.

تمرینها

۱. ثابت‌کنیدکه اگر A و B زیرمجموعه‌های یك‌مجموعهٔ S باشند، آنگاه

$$A \supset B \Longleftrightarrow A \cap B = B \Longleftrightarrow A \cup B = A.$$

۲. درستی قوانین توزیعی

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ و $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

وقوانین د مورگان[1] $(A \cup B)' = A' \cap B'$ و $(A \cap B)' = A' \cup B'$ را برای زیر-مجموعه‌های A، B و C از مجموعهٔ S، تحقیق کنید.

۳. کدامیك از دستورهای زیر تابعی بین دو مجموعهٔ داده شده، تعریف می‌کند؟ از

---

1. de Morgan

آنهایی که تابع هستند کدامیك یك‌به‌یك، برو وی و یادوسویی می‌باشند؟ توابع معکوس کلیهٔ توابع دوسویی را پیدا کنید.

(الف) $f(x)=1-x^2(\mathbf{R}\longrightarrow\mathbf{R})$؛

(ب) $f(x)=1-x^2([-1,1]\longrightarrow[0,1])$؛

(پ) $f(x)=\dfrac{(1-x)}{(1+x)}((-1,\infty)\longrightarrow(-1,\infty))$؛

(ت) $f(x)=x^n(\mathbf{R}\longrightarrow\mathbf{R})$، n عددی است صحیح و مثبت؛

(ث) $f(x)=\begin{cases}x+1 & \text{اگر } x \text{ زوج باشد}\\ x-1 & \text{اگر } x \text{ فرد باشد}\end{cases}(\mathbf{Z}\longrightarrow\mathbf{Z})$؛

(ج) $f(x)=\begin{cases}x^3 & \text{اگر } x \text{ گویا باشد}\\ x & \text{اگر } x \text{ اصم باشد}\end{cases}(\mathbf{R}\longrightarrow\mathbf{R})$؛

(چ) $f(x)=\tan x([0,\pi]\longrightarrow\mathbf{R})$؛

(ح) $f(x)=\tan x((-\dfrac{\pi}{2},\dfrac{\pi}{2})\longrightarrow\mathbf{R})$.

۴. اگر A و B دومجموعهٔ متناهی باشند به قسمی که $|A|=m$، $|B|=n$، چندتابع مختلف یك به یك از A به B وجود دارد؟

(مشکلتر) ثابت کنید که تعداد توابع بروی از A به B برابر است با

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)^m.$$

(در اینجا $\binom{n}{i}$ طبق معمول ضریب دوجمله‌ای نیوتن[1] $\dfrac{n!}{i!(n-i)!}$ می‌باشد. تعداد توابع بروی ارتباط نزدیکی با اعداد استرلینگ[2] دارد؛ (صفحهٔ ۹۱ کتاب ریوردان[3] [۶] را ببینید).

۵. ثابت کنید که اگر $f:A\longrightarrow B$ تابعی یك به یك باشد آنگاه به ازاء هر تابع $h:A\longrightarrow C$ تابعی مانند $g:B\longrightarrow C$ به قسمی وجود دارد که $g\circ f=h$. تحقیق کنید تابع $f:\mathbf{R}\longrightarrow\mathbf{R}^2$ که به‌وسیلهٔ $f(t)=((t+1)^2,(2t+1)^2)$ تعریف شده‌است، یك به‌یك است، و تابعی مانند $g:\mathbf{R}^2\longrightarrow\mathbf{R}$ طوری پیدا کنید که $g\circ f$، تابع همانی روی $\mathbf{R}$ باشد.

---

1. Newton 2. Stirling 3. Riordan

۶. فرض کنید $f : A \longrightarrow B$ و $h : A \longrightarrow C$ توابع مفروضی باشند. ثابت کنید که تابعی مانند $g : B \longrightarrow C$ به قسمی وجود دارد که $g \circ f = h$ اگر و فقط اگر h روی بافتهای f ثابت باشد (یعنی، $f(a_1) = f(a_2) \Rightarrow h(a_1) = h(a_2)$).

۷. فرض کنید $f : \mathbf{R} \longrightarrow \mathbf{R}$ تابعی باشد که به‌ازاء هر $x \in \mathbf{R}$، در $f(-x) = f(x)$ صدق کند. ثابت کنید که تابع یکتایی مانند $g : [0, \infty) \longrightarrow \mathbf{R}$ به قسمی وجود دارد که به ازاء هر $x \in \mathbf{R}$، $f(x) = g(x^2)$.

۸. فرض کنید $f : \mathbf{R} \longrightarrow \mathbf{R}^2$ تابعی باشد که به وسیلهٔ $f(x) = (\cos x, \sin x)$ تعریف شده است. بافتهای f چه هستند؟ ثابت کنید که اگر $g : \mathbf{R} \longrightarrow \mathbf{R}$ تابعی دوره‌ای بادورهٔ 2π باشد (یعنی به ازاء هر $x \in \mathbf{R}$، $g(x + 2\pi) = g(x)$) آنگاه g می‌تواند به صورت $g(x) = h(\cos x, \sin x)$ نوشته شود، که در آن h تابعی است دو متغیره از $\mathbf{R}^2$ به $\mathbf{R}$، که باید به‌طور مناسبی اختیار شود.

۹. فرض کنید $f : A \longrightarrow X$ و $g : A \longrightarrow Y$ توابع مفروضی باشند و h تابعی از A به $X \times Y$ باشد که به‌وسیلهٔ $h(a) = (f(a), g(a))$ تعریف شده است. ثابت کنید که h دوسویی است اگر وفقط اگر :

(الف) f و g هردو بروی باشند، و

(ب) هر بافت f با هر بافت g دقیقاً یك‌عضومشترك داشته‌باشد.

۱۰. کدامیك از رابطه‌های ρ در زیر، هم ارزی هستند؛ کدامیك رابطهٔ ترتیبی هستند؟ هنگامی که ρ یك رابطهٔ هم ارزی است، رده‌های هم ارزی آن را مشخص کنید.

(الف) در $\mathbf{Z}$؛ $x \rho y$ یعنی «x عاد می‌کند y را و y عاد می‌کند x را»؛

(ب) در $\mathbf{R}$؛ $x \rho y$ یعنی «$x - y$ گویاست»؛

(پ) در $\mathbf{R}$؛ $x \rho y$ یعنی «$xy \geqslant 0$»؛

(ت) در $\mathbf{Z} \times \mathbf{Z}$؛ $(a, b) \rho (c, d)$ یعنی «$ad = bc$»؛

(ث) در $\mathbf{Z} \times \mathbf{Z}'$، که در آن $\mathbf{Z}'$ مجموعهٔ اعداد صحیح غیر صفر است؛ ρ مانند حالت (ت)؛

(ج) در $\mathbf{R}$؛ $x \rho y$ یعنی «$(\forall n \in \mathbf{Z})(n < x \Leftrightarrow n < y)$»؛

(چ) در $\mathbf{R}^2$؛ $(x, y) \rho (x', y')$ یعنی
«$(\exists \lambda \in \mathbf{R})(\lambda > 0 \text{ و } x' = \lambda x, y' = \lambda y)$»؛

(ح) در $\mathbf{R}^2$؛ $(x, y) \rho (x', y')$ یعنی
«$(\exists \lambda \in \mathbf{R})(\lambda \geqslant 1 \text{ و } x' = \lambda x, y' = \lambda y)$».

۱۱. چند رابطهٔ هم ارزی مختلف روی مجموعه‌ای با چهار عنصر وجود دارد؟

۱۲. پارادکس زیر را تحلیل کنید.

گزاره . هر رابطهٔ متقارن ومتعدی ρ ، انعکاسی است .

برهان . فرض کنید $a\rho b$. در این صورت با استفاده از تقارن داریم $b\rho a$. اما به کمك تعدی $(a\rho b \text{ و } b\rho a)\Rightarrow a\rho a$. از اینرو به ازاء هر a ، $a\rho a$.

مثال نقض: در $\mathbf{R}$ ، فرض کنید $x\rho y$ به معنی $xy>0$ باشد.

۱۳. رابطهٔ ρ روی مجموعهٔ A را مستدیر می‌نامیم اگر

$$(\forall x, y, z\in A)(x\rho y \text{ و } y\rho z\Rightarrow z\rho x).$$

ثابت کنید که هر رابطهٔ مستدیر انعکاسی، یك‌رابطهٔ‌هم‌ارزی‌است.

۱۴. فرض کنید $A=A_1\times A_2$ و ρ_1 ، ρ_2 دو رابطهٔ هم ارزی - به‌ترتیب - روی A_1 ، A_2 باشند. فرض کنید ρ رابطه‌ای روی A باشد که به وسیلهٔ

$$(a_1, a_2)\rho(b_1, b_2)\Longleftrightarrow a_1\rho_1 b_1 \text{ و } a_2\rho_2 b_2$$

تعریف شده است. ثابت کنید که ρ یك رابطهٔ هم‌ارزی است و رده‌های هم ارزی آن را تعیین کنید . ثابت کنید که A/ρ مشابه $(A/\rho_1)\times(A/\rho_2)$ است.

۱۵. فرض کنید ρ رابطه‌ای انعکاسی و متعدی روی A باشد . فرض کنید $x\sigma y$ به معنی «$x\rho y$ و $y\rho x$» باشد. ثابت کنید که σ یك‌رابطهٔ هم‌ارزی است.

فرض کنید $B=A/\sigma$ و رابطهٔ $\overline{\rho}$ را روی B باقاعدهٔ

$$X\,\rho\,Y\Longleftrightarrow(\forall x\in X)(\forall y\in Y)(x\rho y)$$

تعریف کنید، که‌درآن X ، Y رده‌های هم ارزی σ هستند. ثابت کنید که $\overline{\rho}$ یك‌رابطهٔ ترتیبی روی B است.

[مثال: (الف) در $\mathbf{R}$ ، $x\rho y$ یعنی«$\sin x\leqslant\sin y$» ؛

(ب) در $\mathbf{Z}$ ، $x\rho y$ یعنی «x عاد می‌کند y را». در هریك از این مثالها σ ، B و $\overline{\rho}$ را تعیین کنید .]

۱۶. کدامیك از دستورهای زیریك‌عمل دوتایی* ، روی $\mathbf{Q}$ تعریف می‌کنند؟ درهرحالت n ، m ، n' و m' اعداد صحیح‌اند و $n\neq 0$ و $n'\neq 0$.

(الف) $$\frac{m}{n}*\frac{m'}{n'}=\frac{mn'+m'n}{nn'}\quad ;$$

(ب) $$\frac{m}{n}*\frac{m'}{n'}=\frac{mn'-m'n}{mn'+m'n}\quad ;$$

(پ) $$\frac{m}{n}*\frac{m'}{n'}=\frac{m^2n'+m'^2n}{(nn')^2}\quad ;$$

فصل ۳

اعداد صحیح

مجموعهٔ اعداد صحیح $\mathbf{Z}$ را می‌توان به‌طرق زیادی مشخص کرد. روشی که ما اختیار کرده‌ایم، مبتنی است بر اعمال $+$ ، $-$ ، $\cdot$ ، مقادیر ثابت 0 ، 1 و رابطهٔ $\leqslant$. این روش فقط ناظر است به‌رابطه‌های جبری موجود بین اعدادصحیح. روش مذکور هیچ‌چیز راجع به‌ماهیت خود اعدادصحیح به‌ما نمی‌گوید و درواقع این‌موضوع ماهیات جنبهٔ فلسفی‌اش بیشتر از جنبهٔ ریاضی آن است.

مفروضات اساسی ما درمورد $\mathbf{Z}$ عبارت‌انداز:

(۱) اعمال دوتایی $+$ ، $\cdot$ ، عمل یکتایی $-$ روی $\mathbf{Z}$ و ثابتهای $1 \in \mathbf{Z}$ ، 0 درکلیهٔ قوانین جبراستانده بجز (ض۳) صدق می‌کنند. (مثال ۱.۱ ازفصل ۱ را ببینید). اعدادصحیح در (ض۳) صدق نمی‌کنند درعوض قانون حذف درمورد آنها صادق است:

(ض'۳) اگر $xy = xz$ و $x \neq 0$ ، آنگاه $y = z$.

(۲) رابطهٔ $\leqslant$ روی $\mathbf{Z}$ یك رابطهٔ ترتیبی خطی‌است (ازفصل ۲ به‌خاطر داریم که این نوع رابطه، رابطه‌ای‌است انعکاسی، متعدی و پادمتقارن به‌قسمی‌که به‌ازاء هرعددصحیح x ، y داریم: $x \leqslant y$ یا $y \leqslant x$). این رابطه به‌وسیلهٔ قوانین زیر با اعمال روی $\mathbf{Z}$ ارتباط پیدا می‌کند:

(۰۱) در $\mathbf{Z}$ ، اگر $x \leqslant y$ آنگاه به‌ازاء هر $z \in \mathbf{Z}$ ، $x + z \leqslant y + z$ ؛

(۰۲) در $\mathbf{Z}$ ، اگر $x \leqslant y$ و $0 \leqslant z$ ، آنگاه $xz \leqslant yz$.

(توجه کنید که $a \geqslant b$ یعنی $b \leqslant a$. همچنین $a < b$ ، یا $b > a$ یعنی $a \leqslant b$ و $a \neq b$. عددصحیح a مثبت نامیده می‌شود اگر $0 < a$ و منفی خوانده می‌شود اگر $a < 0$.)

(۳) اصل خوش‌ترتیبی: هرمجموعهٔ غیرتهی ازاعداد صحیح ومثبت دارای کوچکترین عضو است. (کوچکترین عضویك‌مجموعهٔ S از اعدادصحیح، عددصحیحی است‌مانند $m\in S$، به‌قسمی که به‌ازاء هر $s\in S$ داشته باشیم $m\leqslant s$.)

خواننده درصورت‌تمایل‌می‌تواند گزاره‌های (۱)، (۲) و (۳) را به‌عنوان‌اصول‌موضوعه برای $\mathbf{Z}$ درنظر بگیرد؛ این مفروضات $\mathbf{Z}$ را تاحدی‌که به‌ساختمان جبری‌آن مربوط می‌شود کاملا مشخص می‌کنند. روشی دیگرولی طولانی، این است‌که از اصول موضوعهٔ پئانو[1] برای مجموعهٔ اعداد طبیعی $\mathbf{N}$ آغازکرده $\mathbf{Z}$ را به‌کمك‌آن بسازیم (به‌عنوان مثال صفحات ۴۶ تا ۵۳ کتاب هالموس[۴] را برای‌این‌منظور ببینید). قسمتهای (۱)، (۲) و (۳) رابدون بحث زیادتری می‌پذیریم و به‌کمك‌آنها خواص دیگری از $\mathbf{Z}$ را نتیجه می‌گیریم. نتایج‌سادهٔ زیر فقط به‌کمك دوقسمت (۱) و (۲) به‌دست می‌آیند، که درآنها a ، b و c اعداد صحیح دلخواه‌اند و سورهای عمومی مطابق قرارداد اتخاذ شده درفصل۲ حذف شده‌اند.

(الف) $ab=0\Rightarrow a=0$ یا $b=0$ ؛

(ب) $a<b \iff \neg(b\leqslant a)$ ؛

(پ) $a<b \iff a+c<b+c$ ؛

(ت) $a<b \iff b-a>0$ ؛

(ث) $a<b$ و $c>0\Rightarrow ac<bc$ ؛

(ج) $a^2\geqslant 0$ ؛

(چ) $1>0$.

اولین قسمت ازنتایج فوق صورت دیگری از قانون حذف (ض۳′) است. برای اثبات آن، فقط‌کافی است فرض‌کنیم $ab=0$ و $a\neq 0$ وسپس نتیجه بگیریم‌که $b=0$. این مستقیماً از (ض۳′) نتیجه می‌شود، زیرا داریم: $a.0=0=ab$. (فصل۱ را برای اثبات $a.0=0$ ببینید. دراثبات، قسمت(ض۳) به‌کار نمی‌رود.) برای اثبات(ب)، دقت‌کنیدکه اگر $a<b$، آنگاه حتماً $a\leqslant b$ و اگر $b\leqslant a$ نیز درست باشدآنگاه بنابه خاصیت پاد متقارن بودن $\leqslant$ خواهیم داشت $a=b$. اما $a\neq b$ ؛ بنابراین فرض $b\leqslant a$ بایستی نادرست باشد، و نتیجه می‌شود: $(b\leqslant a)\Rightarrow a<b$. بعکس، فرض کنید $\neg(b\leqslant a)$. دراین‌صورت‌داریم $a\leqslant b$ زیرا $\leqslant$ یك رابطهٔ ترتیبی خطی است. همچنین $b\neq a$ (زیرا اگر $b=a$ ، آنگاه $b\leqslant a$ برقراراست). بنابراین $a<b$ وثابت‌کرده‌ایم: $\neg(b\leqslant a)\Rightarrow a<b$. نیمهٔاول اثبات(ب) مثال خوبی از مورد استعمال برهان‌خلف است: برای اثبات اینکه P عبارت Q را نتیجه می‌دهد، کافی است فرض‌کنیم P درست و Q نادرست است وازاین فرض به‌یك تناقض یا گزارهٔ نادرست برسیم.

---

1. Peano

برای اثبات قسمت(پ) کافی است نشان دهیم که

$$\neg(a+c<b+c)\Rightarrow\neg(a<b).$$

(خواننده باید خودرا متقاعدکند که عبارات $P\Rightarrow Q$ و $\neg Q\Rightarrow\neg P$ دارای یك مفهوم هستند.) بااستفاده از (ب) کافی است ثابت کنیم، $a\geqslant b\Rightarrow a+c\geqslant b+c$، و این مطلب بسادگی از (۱۰) نتیجه می‌شود، زیرا

$$a+c\geqslant b+c\Rightarrow(a+c)+(-c)\geqslant(b+c)+(-c).$$

اثبات قسمتهای (ت) و (ث) را به‌عنوان تمرین بـه‌عهدهٔ دانشجویان مـی گذاریم و (ج) راثابت‌می کنیم. ازآنجاکه‌ترتیب‌خطی‌است به‌ازاء هرعدد مفروضa داریم: $a\geqslant 0$ یا $a\leqslant 0$. اگر $a\geqslant 0$ ، آنگاه بنابه (۲۰) ، $a.a\geqslant 0$. ازطرف دیگر، اگر $a\leqslant 0$ آنگاه بنابه (۱۰) ، $-a=(-a)+0\leqslant(-a)+(-a)$. بنابـراین $-a\geqslant 0$ و داریـم : $(-a)(-a)\geqslant 0$. ولی $a.a=(-a)(-a)$ (برای اثبات این مطلب به‌آخر فصل ۱ مراجعه‌شود). ازاینرو درهردوحالت $a^2=a.a\geqslant 0$ وچون $1^2=1\neq 0$ و $1>0$ بلافاصله نتیجه‌می‌شودکه .

عبارات‌مشابه زیادی درمورد اعداد صحیح موجود است‌که دانشجویان باآنهاآشنایی دارند ونتایج‌ساده‌ای از (۱) و (۲) هستند. ماکلیهٔ این‌عبارات‌را دانسته فرض‌می‌کنیم زیرا اثبات آنها تکراری وکسل‌کننده است وازطرف دیگر اغلب‌آنها ساده‌انـد واحتمال اشتباه درآنها خیلی‌کم است. ولی یك اشتباه عمومی وجود داردکه لازم به‌تذکرخاص است. این درست نیست‌که به‌ازاء هر $a,b,c\in\mathbf{Z}$ ، از $a\leqslant b$ نتیجه می‌شود $ac\leqslant bc$. ایـن نتیجه بنابه (۲۰)، برای $c\geqslant 0$ برقرار است ولی ضرب دراعـداد منفی درواقع ترتیب را عوض می‌کند. خواننده به‌عنوان یك‌تمرین الزامی(بااستفاده از (۱) و (۲)) بایستی ثابت‌کندکه

$$a\leqslant b\text{ و }c\leqslant 0\Rightarrow ac\geqslant bc$$

و

$$a<b\text{ و }c<0\Rightarrow ac>bc$$

واین روابط را خوب به‌خاطر بسپارد.

نتایجی‌که ازفرض (۳) به‌دست می‌آیند خیلی عمیق‌تراست وآنهارا باتفصیل بیشتری موردبحث قرار خواهیم‌داد. خواهیم‌دیدکه اصل خوش‌ترتیبی رابطهٔ نزدیکی بااصل استقراء داردکه یکی ازقوی‌ترین روشهای استدلال برای ریاضیدانان است.

اولا دوعبارت راکه شبیه اصل‌خوش‌ترتیبی‌بوده وبسادگی ازآن‌نتیجه می‌شوند تذکر می‌دهیم. زیر مجموعهٔ S از $\mathbf{Z}$ را از بالا کراندار گوییم اگر: $(\exists b\in\mathbf{Z})(\forall s\in S)(s\leqslant b)$، وازپایین کراندار گوییم اگر: $(\exists b'\in\mathbf{Z})(\forall s\in S)(s\geqslant b')$. عدد b که دراولین دستور صدق می کندیك کرانهٔ بالاییS، وبه‌همین‌ترتیب b' یك کرانهٔ پایینیS نامیده‌می‌شود. اکنون‌می‌توان بیان کردکه

(الف) هرزیرمجموعهٔ غیرتهیS از $\mathbf{Z}$ که ازپایین کراندارباشددارای کوچکترین‌عضواست؛

(ب) هرزیرمجموعهٔ غیرتهی S از $\mathbf{Z}$ که از بالاکراندار باشد دارای بزرگترین عضواست.

برهان (الف): عدد ثابت ومناسب n را طوری به‌تمام اعضای S اضافه می‌کنیم که همهٔ آنها مثبت شوند؛ این امکان‌پذیراست زیرا S ازپایین کراندار است. بااستفاده از (۳) ، مجموعهٔ به‌دست‌آمده دارای کوچکترین عضو m است و $m-n$ کوچکترین عضو S خواهدبود.

برهان (ب): دراین قسمت ترتیب را معکوس می‌کنیم، به‌عنوان مثال ، فرض کنید : $S'=\{-s\ ;\ s\in S\}$. دراین صورت S' از پایین کراندار و دارای کوچکترین عضو m است.عدد $-m$ بزرگترین‌عضو S خواهدبود. جزئیات‌راخودتان به‌عنوان‌تمرین انجام‌دهید.

عبارات (الف) و (ب) نبایستی با عبارات مشابهی که احتمالا دانشجویان درمورد اعدادحقیقی باآنها مواجه‌شده‌اند،اشتباه‌کرد. اگرمجموعهٔ اعدادصحیح $\mathbf{Z}$ با $\mathbf{R}$ تعویض‌شود آنگاه عبارات (الف) و (ب) نادرست خواهند بود؛ مثلا، مجموعهٔ اعدادحقیقی مثبت‌دارای کوچکترین عضونیست (گرچه دارای بزرگترین کرانهٔ پایینی باشد)، وحال‌آنکه مجموعهٔ اعداد صحیح مثبت دارای کوچکترین‌عضواست ومی‌توانیم ثابت‌کنیم که

(ج) عدد ۱ کوچکترین عدد صحیح مثبت است.

این گزاره مسلماً نمی‌تواند فقط از (۱) و (۲) نتیجه‌شود زیرا دستگاههای‌دیگری از اعداد موجودند (مانند $\mathbf{Q}$ و $\mathbf{R}$) که در (۱) و (۲) صدق‌می‌کنند ولی‌عدد ۱ درآنها کوچکترین‌عدد مثبت‌نیست. برای اثبات(ج) ، فرض‌کنید m کوچکترین عددصحیح مثبتی باشدکه بنا به (۳) موجود است. آنگاه $m\leqslant 1$ ، زیرا عدد ۱ صحیح ومثبت است. بنابراین‌کافی است فرض کنیم $m<1$ وبه‌تناقضی برسیم. اکنون اگر $m<1$ آنگاه داریم $m\cdot m<1\cdot m$ (چون $m>0$) ، یعنی $m^2<m$. همچنین $m^2>0$ زیرا $m>0$. بنابراین m^2 یك عدد صحیح مثبت کوچکتراز m می‌شود، که باتعریف m تناقض دارد.

قضیهٔ ۳آ. (اصل استقراء). فرض‌کنید $P(n)$ گزاره‌ای مشتمل برمتغیرصحیح n باشد وفرض‌کنید $P(1)$ درست‌باشدوبه‌ازاء هرعدد صحیح $n\geqslant 1$، $P(n)\Rightarrow P(n+1)$. آنگاه $P(n)$ برای‌تمام اعداد صحیح ومثبت n درست است.

برهان. به‌روش برهان خلف استدلال می‌کنیم. فرض‌کنید حکم نادرست باشد. آنگاه S ، مجموعهٔ تمام اعداد صحیح ومثبت n که به‌ازاء آنها گزارهٔ $P(n)$ نادرست است، غیرتهی بوده و از اینرو دارای کوچکترین عضو m است. واضح است که $m\neq 1$ زیرا $P(1)$ درست است. بنابراین $m>1$ ، چون ۱ کوچکترین عدد صحیح ومثبت است. درنتیجه $m-1$ ، مثبت وکوچکتراز m خواهدبود. از تعریف m نتیجه می‌شود که $P(m-1)$ بایستی درست باشد. همچنین چون $m-1\geqslant 1$ ، داریم $P(m-1)\Rightarrow P(m)$. بنابراین $P(m)$ درست

است و ما به یك تناقض رسیده‌ایم. درنتیجه حکم برقرار است.

البته‌شکلهای زیاد دیگری از اصل استقراء ریاضی وجود دارد. بـه‌عنوان مثال: اگر $P(0)$ درست‌باشد و به‌ازاء هر $n \geqslant 0$ ، $P(n) \Rightarrow P(n+1)$ ، آنگاه به‌ازاء هر $n \geqslant 0$، $P(n)$ درست است. نکتهٔ اصلی درروش استقراء آن‌است‌که بایستی یك نقطهٔ شروع وجود داشته باشد، یعنی، به‌ازاء عددی‌مانند a ، $P(a)$ درست باشد. وهمچنین‌درزنجیرهٔ‌استنتاجات $P(a) \Rightarrow P(a+1) \Rightarrow P(a+2) \Rightarrow \dots$ نبایدشکافی موجود باشد، یعنی‌بایستی به‌ازاء هـر $n \geqslant a$ ، استنتاج $P(n) \Rightarrow P(n+1)$ درست باشد. با این مفروضات می‌توان ثابت کردکه به‌ازاء هر $n \geqslant a$ ، $P(n)$ درست است، وبرهان‌آن مشابه برهان فوق است.

درعمل مهم‌است‌که نوشتن براهین‌استقرایی، به‌منظوراجتناب از استدلالهای‌ناصحیح، بادقت‌همراه‌باشد. روش‌عمل‌چنین‌است: (الف) $P(1)$ راثابت‌کنید؛ (ب) فرض‌کنید به‌ازاء یك $n \geqslant 1$ ، $P(n)$ برقرارباشد (این فرض، فرض استقراء نامیده‌می‌شود)؛ (پ) $P(n+1)$ را از فـرض استقراء نتیجه بگیرید؛ (ت) به‌استناد اصل‌استقراء نتیجه بگیریدکه به‌ازاء هر عدد صحیح $r \geqslant 1$ ، $P(r)$ درست است. گاهی مناسب‌تر است‌که فرض استقرایی قویتری راجایگزین(ب) کنیم، یعنی‌فرض‌کنیم به‌ازاء هرعددصحیح مثبت $r < n$ ، $P(r)$درست‌است، وسپس $P(n)$ رانتیجه بگیریم. مستند این روش قضیهٔ‌زیراست:

قضیهٔ ۳ب. (صورت‌دوم اصل‌استقراء). فرض‌کنید $P(n)$ مانند $P(n)$ درقضیهٔ۳آ و $Q(n)$گزارهٔ «به‌ازاء هر عدد صحیح $1 \leqslant r < n$ ، $P(r)$ درست است» باشد . همچنین فرض کنید $P(1)$ درست باشد وبه‌ازاء هر $n \geqslant 1$ ، $Q(n) \Rightarrow P(n)$. دراین‌صورت به‌ازاء هرعدد صحیح مثبت n ، $P(n)$ برقرار است.

برهان. S و m راهمان‌طورکه دراثبات قضیهٔ۳آ آمـد، اختیارکنید. درآن صورت $m \neq 1$ وبه‌ازاء تمام اعداد $1 \leqslant r \leqslant m$ ، $P(r)$ درست‌است. بنابراین $Q(m)$ درست‌بوده ودرنتیجه $P(m)$ درست‌است، که‌مانند قبل یك‌تناقض است.

مثال ۱۰۳. تساوی

$$\sum_{i=1}^{n} i^2 = \frac{1}{6} n(n+1)(2n+1)$$

رابرای تمام اعدادصحیح‌مثبت n ثابت می‌کنیم. اولا، گزاره، به‌ازاء $n = 1$ ، درست‌است، زیرا سمت‌چپ‌آن

$$\sum_{i=1}^{1} i^2 = 1^2 = 1$$

است وسمت راست‌آن

$$\frac{1}{6} \cdot 1 \cdot 2 \cdot 3 = 1$$

به‌عنوان‌فرض استقراء ، فرض‌کنیدکه‌گزاره ، به‌ازاء $n = r$ ، درست باشد، یعنی

$$\sum_{i=1}^{r} i^2 = \frac{1}{6} r(r+1)(2r+1)$$

دراین‌صورت

$$\sum_{i=1}^{r+1} i^2 = \frac{1}{6} r(r+1)(2r+1) + (r+1)^2$$

$$= \frac{1}{6}(r+1)[r(2r+1) + 6(r+1)]$$

$$= \frac{1}{6}(r+1)(2r^2 + 7r + 6)$$

$$= \frac{1}{6}(r+1)(r+2)(2r+3)$$

واین همان مقدار

$$\frac{1}{6} n(n+1)(2n+1)$$

است به‌ازاء $n = r+1$. بنابراین گزاره به‌ازاء $n = r+1$ درست است. استدلال به‌ازاء $r \geqslant 1$ معتبراست، از اینرو، بنابه اصل استقراء ، تساوی مزبور به‌ازاء هر $n \geqslant 1$ درست می‌باشد.

مثال ۳.۳. نشان می‌دهیم که هرعددصحیح $n \geqslant 2$ را می‌توان به‌صورت حاصلضربی (یکی یا بیشتر) از اعداد اول نوشت. (عدد اول را بدین‌ترتیب تعریف می‌کنیم که عدد صحیحی است بزرگتر یا مساوی ۲، کـه نتوان آن‌را به‌صورت حاصلضربی از دوعدد صحیح مثبت کوچکتراز خودش بیان‌کرد) این‌گزاره برای $n = 2$ درست می‌باشد زیرا ۲ خـودش یك عدد اول است. روش قضیهٔ ۳ب را به‌کار می‌بریم. به‌عنوان فرض استقراء ، فـرض‌کنید هر عدد $2 \leqslant r < n$ ، حاصلضربی از اعداد اول است وسپس n را بررسی کنید. یا n یك‌عدد اول است ویاحاصلضربی‌است به‌صورت $n = n_1 n_2$ که‌درآن، $2 \leqslant n_1 < n$ و $2 \leqslant n_2 < n$. درحالت اخیر، بااستفاده ازفرض استقراء هرکدام از n_1 و n_2 حاصلضربی از اعـداد اول هستند و درنتیجه $n = n_1 n_2$ نیز حاصلضربی از اعداد اول خواهد بود وبدین‌ترتیب حکم، بنابه اصل استقراء ، برقرار است.

مثال ۳.۳. همان‌طورکه درفصل۲ قول‌دادیم، دراینجا نشان می‌دهیم که اگر m و n اعدادی صحیح ومثبت باشند، دومجموعهٔ $M = \{1, 2, \ldots, m\}$ و $N = \{1, 2, \ldots, n\}$ فقط وقتی متشابه‌اند که $m = n$. فرض‌کنید نگاشت دوسویی $f : M \longrightarrow N$ مـوجود باشد؛ با به‌کاربردن عمل استقراء روی m ، نشان می‌دهیم که $m = n$. واضح است که اگر $m = 1$

آنگاه $n=1$. فرض می کنیم $m>1$ و $f(m)=r$. دراین صورت $r\in N$ و نگاشت $g: N\longrightarrow N$ که به‌صورت زیر تعریف می‌شود، یك نگاشت دوسویی است (زیرا g با معکوس خودش برابر است):

$$\begin{cases} g(r)=n \\ g(n)=r \\ g(x)=x \quad ، \quad \text{به‌ازاء همهٔ } x\text{های دیگر متعلق به } N \end{cases}$$

بنابراین $h=g\circ f$ یك نگاشت دوسویی از M به N خواهد بود. حال داریم : $h(m)=g(f(m))=g(r)=n$ از اینرو تحدید h نگاشتی دوسویی از $\{1,2,\ldots,m-1\}$ به $\{1,2,\ldots,n-1\}$ را به‌دست می‌دهد. بنابه فرض استقراء داریم: $m-1=n-1$ که ازآنجا $m=n$. بنابراین، حکم بنابه استقراء برقرار است.

روش استقراء نه‌فقط برای اثبات گزاره‌ها مفید است بلکه برای بیان تعریف تراجمی نیزمورد استفاده قرارمی گیرد. یك‌مثال‌نوعی دراین زمینه به‌ازاء عددصحیح مثبت دلخواه n، تعریف $n!$ است. این تابع به‌صورت تابعی مانند f باقواعد استقرایی روی مجموعهٔ‌اعداد صحیح مثبت تعریف می‌شود:

$$f(1)=1 \;;\; f(n+1)=(n+1)f(n) \;,\; n\geqslant 1 .$$

تعریف‌متداول‌آن به‌صورت $n!=1\cdot 2\cdot 3\cdots n$ خلاصهٔ مناسبی برای این‌تعریف‌استقرایی است. (دانشجویان بایستی توجه داشته باشندکه هرجا نقاط «...» ، یا عباراتی نظیر «و به همین‌نحو» ، «وغیره» به‌کار می‌رود، احتمالا یك روش‌استقرایی درآنجا مستتراست که‌ممکن است توجیه‌آن‌بسادگی امکان‌پذیرباشد یا نباشد.) اعتبار تعریف استقرایی $n!$ دراین‌حقیقت نهفته است‌که یك تابع وفقط یك تابع وجود داردکه روی اعداد صحیح مثبت تعریف شده و درشرایط مذکور صدق می کند. این را می‌توان به‌کمك اصل خوش‌ترتیبی وبا استدلالی بسیار مشابه قضیهٔ ۳آ ثابت‌کرد. معهذا ، طرح و اثبات قضیه‌ای‌که دربرگیرندهٔ همهٔ حالات تعاریف استقرایی باشد، قدری مشکلتراست وماهم متعرض آن نخواهیم شد. به علاقه‌مندان توصیه می‌شودکه دراین مورد به‌نظریهٔ توابع تراجمی مثلا به‌صفحهٔ ۴۳ کتاب هالموس[۴] مراجعه کنند.

مثال جالبی از یك برهان استقرایی‌که به‌جای استفاده ازقضیهٔ ۳آ یا ۳ب، مستقیماً به‌وسیلهٔ اصل خوش‌ترتیبی به‌بهترین وجهی انجام می گیرد، اثبات مطلب اساسی زیردرمورد فرآیند تقسیم در $\mathbf{Z}$ است.

قضیهٔ۳پ. (خاصیت‌اقلیدسی $\mathbf{Z}$).فرض‌کنید $a, b\in\mathbf{Z}$ و $b>0$. دراین‌صورت‌اعداد $q, r\in\mathbf{Z}$ به‌قسمی وجود دارندکه $a=bq+r$ و $0\leqslant r<b$. بعلاوه ، q و r ی صادق دراین روابط، یکتا هستند.

برهان. فرض کنید a و b دو عدد صحیح ثابت مفروض باشند و $T=\{a-bq\ ;\ q\in\mathbf{Z}\}$. واضح است که $T\neq\emptyset$. نشان می‌دهیم که T حداقل شامل یك عضو $t\geqslant 0$ می‌باشد. زیرا اگر $a\geqslant 0$، آنگاه $t=a=a-b.0$ چنین عضوی است. از طرف دیگر، اگر $a<0$، آنگاه چون $b\geqslant 1$، داریم $ba\leqslant a$؛ بنابراین $t=a-ba$ عضو مثبتی از T است. در نتیجه مجموعهٔ $S=\{t\in T\ ;\ t\geqslant 0\}$ یك مجموعهٔ غیرتهی از اعداد صحیح مثبت است و از اینرو دارای کوچکترین عضو است. فرض کنید r کوچکترین عضو S باشد، دراین‌صورت عددی مانند q وجود دارد به‌قسمی که $r=a-bq$ و $r\geqslant 0$. کافی است نشان دهیم $r<b$. اگر چنین نباشد، داریم $r\geqslant b$ و بنابراین $r-b\geqslant 0$. اما $r-b=a-bq-b=a-b(q+1)$ متعلق به T، وازاینرو، عضو S است. بعلاوه چون $r-b<r$ و $r-b>0$، بنابراین عضوی از S پیدا کرده‌ایم که کوچکتر از r است. این تناقض نشان می‌دهد $r<b$. وبالاخره برای اثبات یکتایی q و r فرض کنید داریم: $a=bq'+r'$ و $r'<b$ و $r'\geqslant 0$. نشان می‌دهیم که $q=q'$ و $r=r'$. حال اگر $q\neq q'$، آنگاه یا $q>q'$ ویا $q'>q$ ومی توانیم به‌دلیل تقارن، فرض کنیم که $q>q'$. چون $a=bq+r=bq'+r'$، داریم: $r'-r=b(q-q')\geqslant b$ زیرا $q-q'\geqslant 1$ و $b\geqslant 0$. ازاینجا نتیجه می‌شود: $r'\geqslant b+r\geqslant b$، که متناقض بامفروضات ماست؛ از اینرو بایستی داشته باشیم $q=q'$ ودرنتیجه $r=r'$.

درقضیهٔ ۳پ، عدد r به‌باقیماندهٔ تقسیم a بر b یا باقیماندهٔ a به‌پیمانهٔ b مشهور است. درصورتی که a و b مفروض باشند، عدد r به‌طور یکتا معین می‌شود ویکی ازمقادیر $0, 1, 2, \ldots, b-1$ را اختیارمی‌کند. حال اگر n عددصحیح مثبت وثابتی باشد و تقسیمات اعداد را برآن درنظر بگیریم، درآن‌صورت هرعدد دلخواه a دارای n باقیمانده ممکن $0, 1, 2, \ldots, n-1$ به‌پیمانهٔ n است. اعدادی که دارای یك باقیماندهٔ مفروض r به‌پیمانهٔ n باشند تشکیل زیرمجموعه‌ای از $\mathbf{Z}$ را می‌دهند که ردهٔ باقیمانده به‌پیمانهٔ n نامیده می‌شود. دقیقاً تعداد n رده (واضح است که همه‌غیرتهی هستند) موجود است و اینها یك افراز $\mathbf{Z}$ را تشکیل می‌دهند. اینها درواقع بافتهای تابعی‌هستند که به‌هرعدد، باقیماندهٔ آن‌را به پیمانهٔ n نسبت می‌دهد. (مثال ۲۳.۲ را ببینید)

ازآنجاکه رده‌های باقیمانده به‌پیمانهٔ n تشکیل افرازی از $\mathbf{Z}$ را می‌دهند، عبارت‌اند از رده‌های هم‌ارزی یك رابطهٔ هم‌ارزی مناسب روی $\mathbf{Z}$ (قضیهٔ ۲ت). اکنون این رابطهٔ هم‌ارزی را به‌زیباترین شکلش بیان می‌کنیم.

تعریف. گوییم عددصحیح t عددصحیح s را عاد می‌کند اگر عددصحیحی مانند u به‌قسمی وجود داشته باشد که $s=ut$. (درحالت خاص توجه کنید که هرعددصحیح، 0 را عاد می‌کند اما 0 هیچ عددصحیح دیگری غیراز خودش را عاد نمی‌کند).

بیان اینکه t عدد صحیح s را عاد می‌کند مانند آن است که بگوییم باقیماندهٔ s به پیمانهٔ t صفراست. علامتی که برای بیان «t عدد صحیح s را عاد می‌کند» به‌کار می‌رود

عبارت است از $t|s$. علامت $t+s$ یعنی «t عدد صحیح s را عاد نمی کند».

حال برای عدد صحیح مثبت و ثابت n، رابطه‌ای مانند $\equiv$ را روی $\mathbf{Z}$ تعریف می کنیم که همنهشتی به پیمانهٔ n نامیده می‌شود. به‌ازاء اعداد صحیح x ، y می نویسیم:

$$x \equiv y (n \text{ به پیمانهٔ})$$

و می‌خوانیم «x همنهشت y به پیمانهٔ n است» ، اگر n عدد صحیح $y-x$ را عاد کند.

قضیهٔ ۳ت. همنهشتی به پیمانهٔ n یک رابطهٔ هم‌ارزی است و n ردهٔ باقیمانده به پیمانهٔ n ، رده‌های هم‌ارزی آن هستند.

برهان. کافی است نشان دهیم ($x \equiv y (n$ به پیمانهٔ $)$ اگر و فقط اگر x و y باقیماندهٔ مساوی به پیمانهٔ n داشته باشند. فرض کنید x و y هردو دارای باقیماندهٔ r باشند. در این صورت q و q' متعلق به $\mathbf{Z}$ ، موجودند به‌قسمی که : $x=nq+r$ و $y=nq'+r$. در نتیجه $x-y=n(q-q')$ و از اینرو ($x \equiv y (n$ به پیمانهٔ $)$. بعکس، اگر $x \equiv y (n$ به پیمانهٔ $)$، آنگاه $t \in \mathbf{Z}$ به‌قسمی موجود است که $x=y+nt$. اگر r باقیماندهٔ y به پیمانهٔ n باشد، آنگاه به‌ازاء qای متعلق به $\mathbf{Z}$ ، $y=nq+r$ و بنابراین $x=n(q+t)+r$. ملاحظه می‌شود که r باقیماندهٔ x به پیمانهٔ n نیز هست، زیرا $0 \leqslant r < n$ (بنا به قسمت یکتایی قضیهٔ ۳پ).

از نظریهٔ همنهشتیها در این کتاب زیاد استفاده خواهد شد. فعلا فقط به علائم و اینکه همنهشتی به پیمانهٔ n یک رابطهٔ هم‌ارزی است، نیاز داریم. مجموعهٔ خارج قسمت $\mathbf{Z}$ متناظر با این رابطهٔ هم‌ارزی به‌وسیلهٔ $\mathbf{Z}_n$ نشان داده می‌شود. اعضای این مجموعه، رده‌های باقیماندهٔ به پیمانهٔ n هستند و بنابراین یک مجموعهٔ متناهی، بادقیقاً n عضو می باشد. معمولا ردهٔ هم‌ارزی شامل x را به‌وسیلهٔ $\langle x \rangle$ نشان می‌دهیم وچنانچه پیمانهٔ n معلوم نشده باشد، به‌صورت $\langle x \rangle_n$ می نویسیم.

تمرینها

۱. بدون استفاده از خاصیت اقلیدسی $\mathbf{Z}$ ، مستقیماً ثابت کنید که همنهشتی به پیمانهٔ n ، یک رابطهٔ هم‌ارزی است.

۲. ثابت کنید که به‌ازاء هرعدد صحیح x ، یا $x \geqslant 0$ یا $-x \geqslant 0$.

۳. برای اعداد صحیح x تعریف کنید:

$$|x| = \begin{cases} x \text{ ، } x \geqslant 0 \text{ اگر} \\ -x \text{ ، } x < 0 \text{ اگر} \end{cases}$$

ثابت کنید:

(الف) به‌ازاء هر $x\in\mathbf{Z}$ ، $|x|\geqslant 0$ ؛

(ب) به‌ازاء هر $x, y\in\mathbf{Z}$ ، $|xy|=|x|\,|y|$ ؛

(پ) به‌ازاء هر $x, y\in\mathbf{Z}$ ، $|x+y|\leqslant|x|+|y|$.

۴. به‌روش استقراء نشان‌دهید که عبارات زیر برای تمام اعداد صحیح ومثبت n برقرار هستند:

(الف) $\sum_{i=1}^{n}(-1)^i i^2=\frac{1}{2}(-1)^n n(n+1)$ ؛

(ب) $\sum_{i=1}^{n} i(i+1)=\frac{1}{3} i(i+1)(i+2)$ ؛

(پ) $n^2\leqslant 2^n$ ؛

(ت) تعداد زیرمجموعه‌های مختلف (همراه‌بازیرمجموعهٔتهی) یك‌مجموعهٔ n عضوی برابر 2^n است؛

(ث) $\sum_{i=1}^{n} i_1<(n+1)_1$

(توجه کنید که i_1 ، $(-1)^n$ ، 2^n و حتی $\sum_{i=1}^{n}$ به‌صورت‌استقرایی تعریف می‌شوند.)

۵. فرض کنید n یك‌عدد صحیح ومثبت باشد. نشان‌دهید که به‌ازاء هرعددصحیح $a\in\mathbf{Z}$ ، عددصحیحی مانند m به‌قسمی وجود دارد که $mn>a$. (این‌مطلب می‌تواند بسادگی از خاصیت اقلیدسی $\mathbf{Z}$ به‌دست‌آید ولی‌درواقع اساسیتر و بهتر است که مستقیماً به‌کمك مفروضات (۱) ، (۲) و (۳) ثابت گردد.)

۶. ثابت کنید که اگر $n|m$ آنگاه تابعی مانند $f:\mathbf{Z}_m\longrightarrow\mathbf{Z}_n$ به‌قسمی وجود دارد که به‌ازاء هرعدد صحیح x ،

$$f(<x>_m)=<x>_n$$

فصل ۴

گروهها

اکنون آماده‌ایم تا مطالعهٔ جبر مجرد را شروع کنیم. خواننده توجه کرده است که قوانین جمع (ج ۱) — (ج ۴) در قوانین «جبر استانده» (مثال ۱.۱) شباهت زیادی به قوانین ضرب (ض۱) — (ض۴) دارند. برای رسیدن از یکی به دیگری فقط لازم است $+$ را با $\times$ ، ۰ را با ۱ و $x-$ را با x^{-1} تعویض کنیم. این امر ملقی این فکر است که شاید بررسی قوانین (ج۱) — (ج۴)، به‌تنهایی، مفید باشد. درواقع قانون‌جابجایی (ج۴) برای‌خیلی از اهداف ، بدرد نمی‌خورد (به عنوان مثال، هیچیك از (ج۴) و (ض۴) در براهین نمونه‌ای آخر فصل ۱ به‌کار نیامده‌اند) . لذا ، خوب است این قانون را عجالتاً کنار بگذاریم و تا آنجاکه ممکن است ، بدون آن پیش رویم. سه قانون باقیماندهٔ (ج۱) — (ج۳) ، در ۱۵۰ سال گذشته ، اهمیت دائم‌التزایدی در ریاضیات یافته‌اند . دستگاههایی که از این قوانین پیروی می‌کنند «گروه» نامیده می‌شوند و آنها نه فقط در زمینهٔ جبر استانده بلکه تقریباً در هر گوشه‌ای از ریاضیات ظاهر می‌شوند. به‌مجرد اینکه تعریف رسمی گروه را ارائه کردیم، مثالهای متنوعی خواهیم آورد .

یك گروه متشکل است از یك مجموعهٔ G ، یك عمل دوتایی $\circ$ روی G ، یك عمل یکتایی* روی G و عنصرخاصی مانند $e \in G$ ، که در قوانین زیرصدق می‌کنند:

(گ۱) به‌ازاء هر $x, y, z \in G$ ، $(x \circ y) \circ z = x \circ (y \circ z)$ ؛

(گ۲) به‌ازاء هر $x \in G$ ، $e \circ x = x \circ e = x$ ؛

(گ۳) به‌ازاء هر $x \in G$ ، $x \circ x^* = x^* \circ x = e$.

عنصر e ، به دلیل خاصیت (گ۲) ، عنصر خنثای G نامیده می‌شود. عنصر x^* ، به دلیل خاصیت (گ۳) ، معکوس x نسبت به‌عمل $\circ$ ، نامیده می‌شود. اگر گروهی در قانون دیگر

$$x \circ y = y \circ x \text{ ، } x, y \in G \quad \text{به ازاء هر} \quad (گ۴)$$

صدق کند آنگاه G یك‌گروه جابجایی ، یا گروه آبلی (به افتخار آبل[1] ، ریاضیدان نروژی که یکی از بنیانگذاران نظریهٔ گروههاست) نامیده می‌شود.

دراین تعریف علائم $\circ$ ، $*$ ، e را برای آن به‌کاربرده‌ایم که جمع وضرب معمولی، به ذهن خواننده ، متبادر نشود. البته هر علامت دیگری را به جای آنها می‌توان به کاربرد . درحالت خاص ، هنگامی که مناسب باشد، می‌توان نماد جمعی یا ضربی به‌کاربرد. در نماد جمعی، $+$ به‌جای عمل‌دوتایی $\circ$ ، $x - y$ به‌جای $x * y^{-1}$ و o را به‌جای e به‌کارمی بریم. در این صورت‌قوانین گروه به‌قوانین(ج۱) — (ج۳)درمثال ۱.۱ تبدیل‌می‌شوند. دراین‌نماد، مختصر- کردن $x+(-y)$ به $x-y$ معمول است و در این صورت «$-$» به عملی دوتایی‌تبدیل می‌گردد . گروهی که با این نماد نوشته شود گروه جمعی و عنصر خنثای آن عنصر صفر نامیده می‌شود. درنماد ضربی، $\times$ یا. را به‌جای $\circ$ و $^{-1}$ را به جای $*$ به‌کارمی‌بریم. عنصر خنثی، با توجه به سیاق متن ، به وسیلهٔ ۱ ، e ، I و غیره نشان داده می‌شود. این نماد غالباً با حذف علامت دوتایی ساده می‌شود و xy را برای «ضرب» x در y می‌نویسیم. گروهی که بدین‌طریق نوشته شود، گروه ضربی نامیده می‌شود وعنصرخنثای‌آن معمولا عنصرهمانی نامیده می‌شود .

یك‌گروه G متناهی یا نامتناهی نامیده می‌شود ، اگرمجموعهٔ G دارای تعداد متناهی یا نامتناهی عضو باشد. اگرگروه G متناهی باشد تعداد عناصرش مرتبهٔ گروه نامیده‌می‌شود. گویندگروه دارای مرتبهٔ نامتناهی است اگر نامتناهی باشد.

مثال ۱.۴. مجموعهٔ $\mathbf{Z}$ با اعمال $+$ ، $-$ و عنصرخنثای o یك‌گروه است. به‌همین ترتیب $\mathbf{Q}$ ، $\mathbf{R}$ و $\mathbf{C}$ (نسبت به‌مفاهیم معمولی $+$ ، $-$ ، o) گروههای‌جمعی می‌باشند.

مثال ۲.۴. مجموعهٔ اعداد صحیح زوج یك‌گروه جمعی است. همچنین مجموعهٔ تمام اعداد گویا به صورت $\frac{n}{۲}$ ، که $n \in \mathbf{Z}$ ، یك‌گروه جمعی است. دراین مثالها همواره بایستی‌تحقیق کردکه جمع وتفریق روی مجموعه‌های مفروض درواقع تعریف‌کنندهٔ عمل هستند (به‌عنوان مثال ، مجموع دو عدد زوج یك عدد زوج است) و o به مجموعه‌های مفروض، متعلق‌است.

مثال ۳.۴. مجموعهٔ تمام عناصر غیر صفر $\mathbf{Q}$ (به ترتیب $\mathbf{R}$ ، $\mathbf{C}$) به وسیلهٔ $\mathbf{Q}^*$ (به ترتیب $\mathbf{R}^*$ ، $\mathbf{C}^*$) نشان داده می‌شود. چون حاصلضربها و معکوسهای عناصر غیر صفر، غیرصفرند ، واضح است‌که $\mathbf{Q}^*$ ، $\mathbf{R}^*$ و $\mathbf{C}^*$ گروههای ضربی هستند . همچنین $\mathbf{Q}^+$ و $\mathbf{R}^+$ ، (به‌ترتیب) مجموعه‌های اعدادگویا و حقیقی مثبت ، تشکیل‌گروه ضربی می‌دهند.

---

1. Abel

مثال ۴.۴. همهٔ گروههای فوق‌الذکر نامتناهی‌اند، اما برخی گروههای متناهی ضربی که از اعداد مختلط ساخته شده‌اند، نیز موجود است. فرض کنید P_n نمایش مجموعهٔ تمام ریشه‌های nام عدد ۱ در $\mathbf{C}$ باشد. چون $x^n=1 \Rightarrow (x^{-1})^n=1$ و $x^n=y^n=1 \Rightarrow (xy)^n=1$، می‌بینیم که ضرب و معکوس‌گیری اعمالی روی P_n هستند. همچنین $1 \in P_n$ و قوانین گروه در P_n برقرارند، از اینرو P_n یک گروه ضربی است. چون تعداد ریشه‌های nام در $\mathbf{C}$ دقیقاً n تاست، بنابراین P_n گروهی از مرتبهٔ n است. به‌عنوان مثال، $P_1=\{1\}$، $P_2=\{1,-1\}$ و $P_4=\{1,-1,i,-i\}$ گروههای ضربی هستند.

مثال ۵.۴. مجموعهٔ T متشکل از کلیهٔ اعداد مختلط z با قدرمطلق ۱ گروهی ضربی است. (توجه کنید که اگر $|z|=|w|=1$ آنگاه $|zw|=|z|\,|w|=1$، از اینرو $z,w \in T \Rightarrow zw \in T$، و به همین ترتیب $z \in T \Rightarrow z^{-1} \in T$.) این گروه بنا به تعبیر هندسی آن در صفحهٔ آرگان[1] گروه دایره‌ای نامیده می‌شود. همهٔ گروههایی که تاکنون بحث شده‌اند آبلی هستند.

مثال ۶.۴. این مثال ما هیچ ارتباطی با اعداد ندارد و جامعیت تعریف مجرد گروهها را بخوبی نشان می‌دهد. با مجموعهٔ کاملا دلخواه A شروع می‌کنیم و $\mathcal{S}(A)$، یعنی مجموعهٔ همهٔ نگاشتهای دوسویی از A به A را مورد بررسی قرار می‌دهیم. این نگاشتهای دوسویی، جایگشتهای A نامیده می‌شوند، زیرا درحالتی که مجموعهٔ A متناهی باشد واعضایش مرتب به ترتیب خاصی باشند، هرعضو $\mathcal{S}(A)$، در واقع این را نشان می‌دهد که چگونه می‌توان بدون کم یا زیاد کردن اعضای A، ترتیب آنها را عوض کرد و آنها را «جابجا» نمود. حال (بنا به قضیهٔ ۲ب (پ)) ترکیب توابع، عملی دوتایی روی $\mathcal{S}(A)$ تعریف می‌کند. این عمل شرکت‌پذیر است (قضیهٔ ۲آ) و تابع همانی i_A عضو خنثای آن می‌باشد. بعلاوه، هر نگاشت دوسویی $f: A \longrightarrow A$ (بنا به قضیهٔ ۲پ) دارای معکوس $f^{-1}: A \longrightarrow A$ می‌باشد که خود نیز نگاشتی دوسویی است و در شرط $f \circ f^{-1} = f^{-1} \circ f = i_A$ صدق می‌کند. بنابراین $\mathcal{S}(A)$ نسبت به این اعمال یک گروه است، که گروه متقارن روی A نامیده می‌شود، اگر A مجموعه‌ای متناهی با n عنصر باشد، مثلا $A=\{1,2,\dots,n\}$، آنگاه گروه متقارن روی A با $\mathcal{S}_n$ نشان داده می‌شود، که گروهی متناهی و از مرتبهٔ $n!$ است (تعداد جایگشتهای متفاوت $\{1,2,\dots,n\}$). گروه $\mathcal{S}_n$ آبلی نیست مگر به ازاء $n=1,2$.

مثال ۷.۴. اگر در مثال اخیر مجموعهٔ A را صفحهٔ حقیقی $\mathbf{R}^2$ بگیریم آنگاه بعض انواع خاص جایگشتها از نظر هندسی قابل توجه‌اند. به عنوان مثال، حرکتهای صلب (یا تبدیلات اقلیدسی[2]) توابع دوسویی $\rho: \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ هستند که فواصل را حفظ می‌کنند، یعنی به‌ازاء هر دو نقطهٔ P و Q فاصلهٔ $\rho(P)$ تا $\rho(Q)$ برابر فاصلهٔ PQ می‌باشد. مجموعهٔ تمام حرکتهای صلب نسبت به ترکیب و معکوس‌گیری توابع یک گروه (غیرآبلی) است، و گروه اقلیدسی

---

1. Argand 2. Euclid

دو بعدی نامیده می‌شود.

مثال ۸.۴. حرکتهای صلب $\mathbf{R}^2$ که مبدأ را ثابت نگه‌می‌دارند تبدیلات متعامد نامیده می‌شوند. اینها شامل تمام دورانهای حول مبدأ وکلیهٔ انعکاسها[1] نسبت به خطوطی که ازمبدأ می‌گذرند، می‌باشند و نسبت به اعمال ترکیب و معکوس‌گیری توابع تشکیل یك گروه می‌دهند. این گروه را به وسیلهٔ O_2 نشان داده وگروه متعامد می‌نامند. دورانها به تنهایی نیز تشکیل یك گروه، O_2^+، می‌دهند (گروه متعامد خاص)؛ ولی انعکاسها به تنهایی تشکیل گروه نمی‌دهند، زیرا ترکیب دو انعکاس یك انعکاس نیست بلکه یك دوران است. گروه متعامد خاص O_2^+ آبلی است ولی گروه متعامد O_2 آبلی نیست.

مثال ۹.۴. شکل هندسی دلخواهی را در صفحه در نظربگیرید، مثلا دسته‌ای از نقاط و خطوط. آنگاه یك حرکت صلب در صفحه یك تقارن این شکل نامیده می‌شود اگر شکل‌را به خودش تبدیل‌کند. ضرورتی نداردکه ضمن‌این حرکت، نقاط وخطوط ثابت بمانند، بلکه تقارن‌می‌تواند نقاط راباهم وخطوطرا باهم جابجاکند. تقارنهای هرشکل (نسبت به‌ترکیب توابع) تشکیل‌یك‌گروه‌می‌دهند. همچنین ممکن است باانتخاب تقارنهایی‌ازشکل که به‌گروه متعامد یا گروه متعامد خاص متعلق‌اند، گروههای دیگری تشکیل داد. به عنوان مثال، مربعی به مرکز مبدأ دارای ۸ تقارن است که ۴ تای آنها دوران و ۴ تای دیگر انعکاس هستند[2]. این تقارنها تشکیل‌گروهی غیرآبلی می‌دهند. ۴ تقارن دورانی نیز تشکیل یك‌گروه می‌دهند، اما این‌گروه اخیرآبلی است.

مثال ۱۰.۴. مجموعهٔ تمام ماتریسهای حقیقی $n \times n$ نسبت به $+$ ، $-$ ، یك‌گروه است؛ عنصرصفراین‌گروه، ماتریسی‌است‌که‌همهٔ‌درایه‌هایش صفرباشند. ضرب ماتریسهاعملی‌دوتایی و شرکت‌پذیر است، و ماتریس همانی I_n (که درایه‌های قطری آن ۱ وسایر درایه‌های‌آن صفرند) عنصر خنثای ضرب است، اما این عمل تشکیل گروه نمی‌دهد زیرا اغلب ماتریسها دارای‌معکوس نیستند. ولی اگر توجه خودرا به‌مجموعهٔ ماتریسهای معکوس‌پذیر (غیرمنفرد) $n \times n$ معطوف‌نماییم،گروهی‌ضربی‌به نام گروه‌خطی‌عمومی، $\mathrm{GL}_n(\mathbf{R})$، به دست‌می‌آوریم. این‌گروه آبلی نیست مگر به ازاء $n = 1$. توجه‌کنید که مجموعهٔ ماتریسهای معکوس‌پذیر یك گروه جمعی نیست، زیرا مجموع دوماتریس معکوس‌پذیر الزاماً معکوس‌پذیر نیست.

مثالهای فوق نشان می‌دهندکه گروهها در زمینه‌های مختلف ریاضیات بوفور مطرح می‌شوند. کلیهٔ قضایایی که در موردگروهها ثابت می‌کنیم دراین مثالها، و مثالهای متعدد دیگر، کاربرد خواهند داشت. شگفت‌آورآن است‌که ازاین‌فرضیات معمولی و پیش‌پا افتاده، اینهمه نتایج گرانقدر حاصل می‌شود. دراثبات قضایا در موردگروههای دلخواه معمولا نماد

---

۱. در اینجا، منظور از انعکاس (reflection)، تقارن محوری است؛ یعنی عمل‌یافتن قرینهٔ یك شکل نسبت به یك محور. م

۲. البته‌لازم نیست مرکز مربع درمبدأ مختصات باشد؛ هرمربعی دارای ۸ تقارن است. م

ضربی گروه را به‌کار برده وعنصرخنثی را با e نشان می‌دهیم. قضایای متناظر برای گروههای جمعی را می‌توان با یك جایگزینی سادهٔ علامتی، به دست‌آورد (و ثابت‌کرد)؛ معنی قضایا به‌نماد خاص به‌کار رفته بستگی ندارد.

قضیهٔ ۴آ . فرض‌کنید G یك‌گروه باشد . دراین صورت

(الف) عنصر خنثی یکتاست؛

(ب) به‌ازاء هر $x\in G$ ، عنصر یکتای $y\in G$ به‌قسمی وجود داردکه $xy=yx=e$؛

(پ) به ازاء هر x ، $y\in G$ ، $xy=e\Rightarrow(x=y^{-1}$ و $y=x^{-1})$ ؛

(ت) به ازاء هر x ، $y\in G$ ، $(xy)^{-1}=y^{-1}x^{-1}$ ؛

(ث) به ازاء هر $x\in G$ ، $(x^{-1})^{-1}=x$ ؛

(ج) (قوانین حذف) به ازاء هر a ، x ، $y\in G$ ،

$$ax=ay\Rightarrow x=y$$

و

$$xa=ya\Rightarrow x=y\ ;$$

(چ) اگر x_1 ، x_2 ، ... ، $x_n\in G$ آنگاه حاصلضرب $x_1x_2\dots x_n$ مستقل از موقعیت پرانتزهاست ؛

(ح) اگر x_1 ، x_2 ، ... ، $x_n\in G$ و G آبلی باشد آنگاه حاصلضرب $x_1x_2\dots x_n$ مستقل از ترتیب عاملها وهمچنین نحوهٔ پرانتزگذاری می‌باشد.

برهان. (الف) اگر e و e' دو عنصر خنثی باشند، آنگاه $e=ee'=e'$.

(ب) اگر y و y' دو عنصر با خاصیت مفروض باشند آنگاه

$$y=ye=y(xy')=(yx)y'=ey'=y'\ .$$

اما به ازاء هر x ، عنصر x^{-1} دارای خاصیت $xx^{-1}=x^{-1}x=e$ می‌باشد ، بنابراین دقیقاً یك عنصر «معکوس» وجود دارد .

(پ) فرض کنید $xy=e$ ، در این صورت $x^{-1}(xy)=x^{-1}e=x^{-1}$ ولی $x^{-1}(xy)=(x^{-1}x)y=ey=y$ ، از اینرو $y=x^{-1}$. به همین ترتیب،

$$x=xe=x(yy^{-1})=(xy)y^{-1}=ey^{-1}=y^{-1}$$

(ت)
$$(xy)(y^{-1}x^{-1})=((xy)y^{-1})x^{-1}=(x(yy^{-1}))x^{-1}$$
$$=(xe)x^{-1}=xx^{-1}=e$$

ولی این رابطه ، بنابه (پ) ، نتیجه می‌دهد که هر یك از عناصر xy و $y^{-1}x^{-1}$ عکس‌یکدیگرند.وبخصوص $(xy)^{-1}=(y^{-1}x^{-1})$.

(ث) بنابه (گ۳)، داریم $xx^{-1}=e$. ولی این رابطه، به‌کمك (پ) نتیجه می‌دهد

که $x=(x^{-1})^{-1}$.

(ج) اگر $ax=ay$ آنگاه $a^{-1}(ax)=a^{-1}(ay)$. بنابراین $(a^{-1}a)x=(a^{-1}a)y$، یعنی، $x=y$. به همین ترتیب $xa=ya\Rightarrow x=y$.

(چ) این قسمت به کمك استقراء روی n ثابت می‌شود. حالت $n=1$ ، 2 واضح است. حالت $n=3$ ، همان قانون شرکت‌پذیری (گ ۱) می‌باشد. قسمتی از استدلال مربوط به حالت $n=4$ در (ت) آمده است؛ اثبات شامل کاربردهای متعددی از قانون شرکت‌پذیری است. اکنون استدلال را برای حالت کلی n می‌آوریم. فرض کنید P حاصلضرب پرانتزدار دلخواهی از x_1 ، x_2 ، ... ، x_n ، باهمین ترتیب، باشد. آنگاه $P=Q_1S_1$ ، که Q_1 ، S_1 حاصلضربهایی با طول کمتر از n هستند و این دو عامل به طور یکتا به وسیلهٔ پرانتزگذاری معین شده‌اند . اگر S_1 دارای طول ۲ یا بیشتر باشد، آنگاه خود حاصلضربی به صورت $S_1=R_2S_2$ است ، از اینرو $P=Q_1(R_2S_2)=(Q_1R_2)S_2=Q_2S_2$ ، که در آن $Q_2=Q_1R_2$. واضح است که S_2 کوتاه‌تر از S_1 است. اگر S_2 دارای طول ۲ یا بیشتر باشد می‌توان این‌روش را تکرار کرد تا طول عامل دوم برابر ۱ گردد. (استدلال استقرائی پنهان شدهٔ دیگری در اینجا موجود است.) بنابراین داریم $P=Qx_n$ ، که Q حاصلضرب پرانتزداری از x_1 ، x_2 ، ... ، x_{n-1} می‌باشد . به همین ترتیب اگر P' هر حاصلضرب پرانتزدار دیگری از x_1 ، x_2 ، ... ، x_n باشد، آنگاه $P'=Q'x_n$ ، که Q' حاصلضربی از x_1، x_2 ، ... ، x_{n-1} است. بنابه فرض استقراء $Q=Q'$ و بنابراین $P=Qx_n=Q'x_n=P'$. اکنون بنابه استقراء ، نتیجه برای همهٔ n ها برقرار است.

(ح) استدلال این حالت، مشابه حالت فوق است و درآن از قانون جابجایی برای مرتب نمودن مجدد حاصلضرب، بدون تغییر در مقدارش ، استفاده می‌شود . بنابه (چ) ، نیازی به گذاردن هیچ پرانتزی نداریم و این، نمادگذاری را ساده می‌کند. روشنترین‌روش اثبات آن است که نشان دهیم هر حاصلضربی از x_1 ، x_2 ، ... ، x_n برابر با حاصلضرب ویژهٔ $x_1x_2\dots x_n$ می‌باشد . این را می‌توان به صورت زیر انجام داد. نخست x_1 را با تعویضهای مکرر با عناصر ماقبلش به سمت جلو حرکت دهید ، هرتعویض ، بنابه قانون جابجایی، مجاز است . سپس می‌توان به همین نحو، به‌ترتیب با x_2 ، x_3 ، ... ، x_n عمل نمود، و هرکدام را به مکان مناسبش منتقل نمود. به‌طور خلاصه، می‌توان استقراء راروی n به‌کارگرفت. حکم به ازاء $n=1$ ، 2 واضح است. اگرهمانند فوق x_1 را به جلوحرکت دهیم، آنگاه برای مرتب نمودن x_2 ، x_3 ، ... ، x_n به ترتیب صحیح ، می‌توان از فرض استقراء استفاده کرد و بدین ترتیب حکم را ثابت نمود.

بایستی به برخی از پیامدهای‌فوری این‌نتایج مقدماتی توجه شود. اولا، بنابه (چ)، همواره می‌توانیم هنگام نوشتن‌حاصلضربها در یك گروه ، چنانچه مایل باشیم، پرانتزها را حذف کنیم ؛ نماد $x_1x_2\dots x_n$ (یا در یك گروه جمعی $x_1+x_2+\dots+x_n$) خالی از ابهام است. به همین ترتیب بنابه (ح)، به‌شرط اینکه گروه آبلی باشد: نیازی به مشخص

نمودن ترتیب عاملها در یك حاصلضرب نداریم. بنابراین اگر معلوم باشد که گروه آبلی است، نماد

$$\left(\sum_{i=1}^{n} x_i \text{ ، یا در یك گروه جمعی} \right) \prod_{i=1}^{n} x_i$$

مجاز است والا خیر.

ثانیاً، قسمتهای (الف) و (ب) قضیه‌نشان می‌دهند که‌وقتی بخواهیم ادعا کنیم که‌چیزی تشکیل یك‌گروه می‌دهد فقط نیاز داریم که مجموعه وعمل دوتایی روی آن را مشخص کنیم. اگر G یك‌گروه باشد، عنصر خنثی و معکوس هرعنصر زمانی که عمل دوتایی شناخته شده باشد، به طور یکتا معین می‌شوند. این امر، تعریف دیگر «گروه» را، که عموماً به‌کار گرفته می‌شود، تبیین می‌کند: یك‌گروه مجموعه‌ای‌مانند G است که یك‌عمل دوتایی $\circ$ روی آن تعریف‌شده است به‌قسمی که (الف) $\circ$ شرکت‌پذیر است، (ب)عنصری مانند $e \in G$ وجود دارد که به ازاء هر $x \in G$ در $e \circ x = x \circ e = x$ صدق می‌کند و (پ) به‌ازاء هر $x \in G$ عنصری‌مانند $y \in G$ به‌قسمی وجود دارد که $x \circ y = y \circ x = e$. من‌بعد، ما تعابیری ازقبیل «G نسبت‌به $+$ یك‌گروه‌است» و «$(G , +)$یك‌گروه‌است» را به‌کارخواهیم برد و دیدیم که‌این تعابیر خالی از ابهام‌اند.

ثالثاً، قسمت (ت) قضیه بااستقراء ساده‌ای نتیجه می‌دهد که برای هر حاصلضرب $x_1 x_2 \cdots x_n$ (که می‌توان آن را بدون پرانتز نوشت)

$$(x_1 x_2 \cdots x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \cdots x_1^{-1} .$$

اگر G یك‌گروه (ضربی) باشدمی‌توانیم توانهای یك‌عنصر $x \in G$ را به‌صورت‌زیر به استقراء تعریف کنیم: $x^0 = e$ ؛ $x^1 = x$ ؛ و به ازاء $n \geqslant 1$ ، $x^{n+1} = x^n x$. همچنین می‌توانیم توانهای‌منفی x را باقاعدهٔ $x^{-n} = (x^n)^{-1}$ ، به ازاء $n \geqslant 1$ ، تعریف کنیم. (دقت کنید که‌به ازاء $n = 1$ دومعنی ممکن x^{-1} توافق دارند.)

قضیهٔ ۴ب. فرض کنید G گروهی دلخواه باشد. دراین صورت

(الف) به‌ازاء هر $x \in G$ ، $m , n \in \mathbf{Z}$ ، $x^m x^n = x^{m+n}$ ؛

(ب) به‌ازاء هر $x \in G$ ، $m , n \in \mathbf{Z}$ ، $(x^m)^n = x^{mn}$ ؛

(پ) اگر G آبلی‌باشد، آنگاه به ازاء هر $x , y \in G$ ، $n \in \mathbf{Z}$ ، $(xy)^n = x^n y^n$.

برهان. اگر n عددی صحیح و مثبت باشد آنگاه، بنا به تعریف، x^n برابر یکی از حاصلضربهای ممکن n عامل است، که همهٔ عاملها مساوی x اند. برای اعداد صحیح مثبت m و n نتیجه می‌شود که (الف)، (ب) و(پ) حالتهای خاصی از قضیهٔ۴آ، (چ) و (ح) هستند. (این استدلال ارتباط بین اعداد صحیح مثبت و روشهای شمارش را به طور ضمنی به‌کار می‌برد. تنها راه برای اجتناب از این موضوع آن است که نظریهٔ اعداد طبیعی دقیقاً

روی اصول‌موضوعهٔ پئانو بنا شود. این‌کار پیچیدگی برهان را بسیار افزایش می‌دهد، بدون اینکه چیزی به فهم کسی اضافه کند.) اگر $m=0$ یا $n=0$ آنگاه عبارات به طور بدیهی درست‌هستند. برای‌مقادیردیگر m و n به تعریف $x^{-n}=(x^n)^{-1}$ رجوع‌می‌کنیم تاهرعبارت را به‌حالت‌مثبت‌برگردانیم. مثلا، فرض کنیم که در(الف)، $m>0$ ، $n<0$ و $m+n>0$.

قرارمی‌دهیم $p=-n>0$. آنگاه، بنا به‌حالت‌مثبت، $x^{m+n}x^p=x^{m+n+p}=x^m$. اما بنا به تعریف $x^n=x^{-p}=(x^p)^{-1}$ ، از اینرو $x^mx^n=x^{m+n}x^px^n=x^{m+n}$. حالات دیگر قسمت (الف) به‌همین‌ترتیب ثابت‌می‌شوند. برای‌اثبات (ب) وقتی $m<0$ ، $n>0$ ، قرار می‌دهیم $q=-m>0$ ، آنگاه بنا به دستور معکوس ضرب ، به ازاء هر $y\in G$ و $r>0$، $(y^r)^{-1}=(y^{-1})^r$. بنابراین

$$(x^m)^n=(x^{-q})^n=((x^q)^{-1})^n=((x^q)^n)^{-1}=(x^{qn})^{-1}=x^{-qn}=x^{mn}.$$

حالتهای دیگر را به‌عنوان تمرین به عهدهٔ خواننده می گذاریم.

نتیجه . درهرگروه ، توانهای متفاوت یك عنصر باهم جابجایی هستند .

برهان . چون جمع اعدادصحیح جابجایی‌است داریم: $x^mx^n=x^{m+n}=x^{n+m}=x^nx^m$

هنگامی‌که گروه G به صورت جمعی نوشته می‌شود «توانهای» یك عنصر x به‌جای x^n به صورت nx نـوشته‌می‌شوند (مثلا؛ $3x=x+x+x$ به جای $x^3=x\cdot x\cdot x$)و آنرا «مضارب صحیح x» یا «توانهای جمعی x» می‌نامیم. توجه‌کنید که تعریف $x^0=e$ به $0x=0$ تبدیل می‌شود، که در آن 0 نخست به جای عدد 0 و سپس به جای عنصر صفر G به‌کاررفته‌است.قوانین‌نمایی‌قضیهٔ ۴ب به $n(mx)=(nm)x$ ، $mx+nx=(m+n)x$ وبرای‌گروههای آبلی به $n(x+y)=nx+ny$ تبدیل‌می‌شوند. خواننده بایستی‌صورت جمعی قضیهٔ ۴آ را برای خود نوشته و آن را به خاطر بسپارد . ما این دو قضیه را فراوان به‌کار خواهیم برد و اغلب، بدون تصریح . اینها قـواعدی هستند کـه همهٔ محاسبات در گروهها رویشان بناشده است. شاید لازم به‌تذکر باشدکه نماد جمعی بندرت برای‌گروهی که آبلی نباشد ، به کار گرفته می‌شود (و در این کتاب هیچگاه بدین صورت بـه‌کار نرفته است) .

مثال ۱۱.۴. درگروه $GL_2(\mathbf{R})$ (مثال ۴ . ۱۰ را ببینید) ، عنصر

$$X=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$

دارای معکوس

$$X^{-1}=\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}$$

می‌باشد، به ازاء هر $n\in\mathbf{Z}$ ، توانهای X عبارت‌اند از :

$$X^n=\begin{pmatrix}۱ & n\\ ۰ & ۱\end{pmatrix}$$

این به ازاء $n>۰$ به وسیلهٔ استقراء و به‌ازاء $n<۰$ به روش معکوس‌گیری ثابت‌می‌شود.

مثال ۱۲.۴. در گروه $\mathscr{S}_n$ از جایگشتهای $\{n\ ,\ \dots\ ,\ ۲\ ,\ ۱\}$ ، نماد زیر را اتخاذ می‌کنیم : جایگشتی را که ۱ را به $r_۱$ ، ۲ را به $r_۲$ ، و به طور کلی i را به r_i بنگارد به وسیلهٔ

$$r=\begin{pmatrix}۱ & ۲ & \cdots & n\\ r_۱ & r_۲ & \cdots & r_n\end{pmatrix}$$

نشان می‌دهیم. این نماد به محاسبهٔ حاصلضربها کمك می‌کند؛ مثالهایی از $\mathscr{S}_۳$ می‌آوریم و تحقیق آنها را به‌عهده خواننده می‌گذاریم تا با هرروشی‌که صلاح می‌داند، درستی‌آنها را نشان دهد.

$$\begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۱ & ۳\end{pmatrix}\begin{pmatrix}۱ & ۲ & ۳\\ ۱ & ۳ & ۲\end{pmatrix}=\begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۳ & ۱\end{pmatrix},$$

$$\begin{pmatrix}۱ & ۲ & ۳\\ ۱ & ۳ & ۲\end{pmatrix}\begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۱ & ۳\end{pmatrix}=\begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۱ & ۲\end{pmatrix}.$$

به خاطر آورید که ضرب در $\mathscr{S}_n$ همان ترکیب توابع است، و $g\circ f$ تابعی است که نخست با اثر g و سپس f به دست آمده است. مثالها نشان می‌دهند که $\mathscr{S}_۳$ یك گروه آبلی نیست.

در $\mathscr{S}_۳$ شش عنصر وجود دارد، که به وسیلهٔ

$$e=\begin{pmatrix}۱ & ۲ & ۳\\ ۱ & ۲ & ۳\end{pmatrix},\quad a=\begin{pmatrix}۱ & ۲ & ۳\\ ۱ & ۳ & ۲\end{pmatrix},\quad b=\begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۲ & ۱\end{pmatrix},$$

$$c=\begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۱ & ۳\end{pmatrix},\quad p=\begin{pmatrix}۱ & ۲ & ۳\\ ۲ & ۳ & ۱\end{pmatrix},\quad q=\begin{pmatrix}۱ & ۲ & ۳\\ ۳ & ۱ & ۲\end{pmatrix}.$$

نشان می‌دهیم. هرکدام از سه توانهش a ، b ، c دو عدد را باهم تعویض می‌کنند وواضح است‌که هریك برابر معکوس خودش می‌باشد، یعنی $a^۲=b^۲=c^۲=e$. بنابراین اگر n فردباشد $a^n=a$ و اگر n زوج‌باشد $a^n=e$. جایگشتهای‌دوری p و q معکوس‌یکدیگرند، و $p^۲=q$ ، $p^۳=e$. از اینرو p^n همواره یکی ازعناصر e ، p ، q می‌باشد. در اینجا برای‌مراجعات‌آتی جدول ضرب کامل $\mathscr{S}_۳$ را درج‌می‌کنیم. یك درایهٔ نمونه‌ای، حاصلضرب xy است‌که x درسمت چپ سطر و y در بالای ستون جدول ظاهر می‌شود .

	e	a	b	c	p	q
e	e	a	b	c	p	q
a	a	e	p	q	b	c
b	b	q	e	p	c	a
c	c	p	q	e	a	b
p	p	c	a	b	q	e
q	q	b	c	a	e	p

اینکه هرعنصر $\mathcal{S}_3$ در هرسطر یا هرستون این جدول دقیقاً یکبار ظاهرمی‌شود، اتفاقی نیست؛ بلکه این مطلب در هر گروهی صادق است و نتیجه‌ای است از این امر مسلم که دریك گروه به ازاء عناصر مفروض s ، t ، معادلهٔ $sx=t$ (یا $xs=t$) دارای جوابی یکتاست.

گروه G دوری نامیده می‌شود اگرهمهٔ عناصرش توانی از یك عنصرخاص g باشند. این g ، مولد G نامیده می‌شود. برای مثال، گروه P_n از ریشه‌های n ام ۱ در $\mathbf{C}$ دوری است، زیرا همهٔ عناصرش توانی از $\zeta = e^{\frac{2\pi i}{n}}$ هستند. گروه جمعی $\mathbf{Z}$ نیز دوری است زیرا هرعدد صحیح توانی جمعی از ۱ می‌باشد. از طرف دیگر، گروه $\mathcal{S}_3$ دوری نیست زیراهیچ عنصرش بیشتر از ۳ توان متمایز ندارد (مثال ۱۱.۴ را ببینید) . هرگروه دوری آبلی است زیرا همهٔ توانهای مولدش با همدیگر جابجایی هستند (نتیجهٔ قضیهٔ ۴ب) . توجه کنید که مولد یك گروه دوری یکتا نیست؛ مثلا ۱ — یك مولدگروه جمعی $\mathbf{Z}$ است، و $e^{\frac{4\pi i}{5}}$ یك‌مولد P_5 می‌باشد. دراین باره بعداً مطالب بیشتری بـرای گفتن خواهیم داشت.

یك زیر گروه ازگروه G زیر مجموعه‌ای است مانند H از G به قسمی که

(الف) $e\in H$ ؛

(ب) $x, y\in H \Rightarrow xy\in H$ ؛

(پ) $x\in H \Rightarrow x^{-1}\in H$.

این شرایط برای آن‌گذاشته شده‌اندکه تضمین کنند که خود H نیز یك‌گروه باشد. این سه شرط می‌گویندکه H دارای عنصر خاص لازم e بوده وضرب و معکوس‌گیری در G ، وقتی که حوزهٔ تعریفشان محدود شده باشد، عملی دوتایی و یکتایی روی H القاء می‌کنند. چون قوانین (گ۱)، (گ۲) ، (گ۳) برای‌همهٔ عناصر G برقرارند، آنها خودبخود در H نیز برقرارخواهند بود. از اینرو H نسبت به‌اعمال القاء شده یك‌گروه است. بعکس، بسادگی دیده می‌شودکه اگر زیرمجموعهٔ H نسبت به‌ضرب تحدیدی یك‌گروه باشد، آنگاه بایستی درشرایط (الف) و(پ)فوق، وهمچنین(ب) ، صدق کند، لذا تعریف‌ما درواقع‌همهٔ گروههای

ضربی را که مشمول G هستند، دربرمی‌گیرد.

مثال ۱۳.۴. در هر گروه G زیرمجموعه‌های $\{e\}$ و G زیرگروه هستند.

مثال ۱۴.۴. اگر x عنصر ثابتی از یك گروه G باشد، آنگاه مجموعهٔ X که همهٔ اعضایش توانهایی از x اند یك زیرگروه است، که زیرگروه تولید شده به وسیلهٔ x نامیده می‌شود. دلایل ماعبارت‌اند از: (الف) $e=x^{0}$؛ (ب) $x^{m}x^{n}=x^{m+n}$؛ (پ) $(x^{n})^{-1}=x^{-n}$.

مثال ۱۵.۴. پیدا کردن تمام زیرگروههای $\mathcal{S}_3$ کار مشکلی نیست. برای جدول ضرب $\mathcal{S}_3$ به مثال ۱۲.۴ ارجاع می‌دهیم، و بی درنگ می‌توانیم زیرگروههای دوری $\mathcal{S}_3$ را بنویسیم. آنها عبارت‌اند از: $\{e\}$، $\{e, a\}$، $\{e, b\}$، $\{e, c\}$ و $\{e, p, q\}$. فرض کنید H زیر گروهی دلخواه باشد که در این فهرست نیست. اگر $H\supset\{e, p, q\}$، آنگاه H حداقل شامل یکی از عناصر a، b، c می‌باشد. به‌کمك تقارن می‌توانیم فرض کنیم که $a\in H$، و در آن صورت H شامل $ap=b$ و $aq=c$ خواهد بود و لذا $H=\mathcal{S}_3$. از طرف دیگر، اگر $H\not\supset\{e, p, q\}$. آنگاه $p\notin H$، $q\notin H$، پس H باید حداقل شامل دو عنصر از a، b، c باشد. اما این نتیجه می‌دهد که $p\in H$ زیرا $p=ab=bc=ca$. این تناقض نشان‌می‌دهد که به‌استثنای زیرگروههای دوری فهرست شدهٔ قبلی، $\mathcal{S}_3$ تنها زیرگروه است.

در یك گروه جمعی A زیرگروه دوری تولید شده به‌وسیلهٔ یك عنصر x شامل همهٔ توانهای جمعی nx از x می‌باشد. درحالت خاص، در گروه جمعی اعداد صحیح $\mathbf{Z}$، زیرگروه دوری تولید شده به‌وسیلهٔ عدد صحیح d مجموعهٔ $\mathbf{Z}d=\{nd\ ;\ n\in\mathbf{Z}\}$ می‌باشد. در اینجا مجموعهٔ $\mathbf{Z}$ نقش مضاعفی را ایفا می‌کند. از یك طرف به عنوان یك گروه تحت بررسی جانشین A شده است. از طرف دیگر اعداد صحیح $n\in\mathbf{Z}$، همان طور که می‌توان در هر گروه جمعی دیگر هم انجام داد، برای نشان دادن توانهای جمعی n ام عنصر d به‌کار رفته‌اند. تصادفاً برای این گروه خیلی‌خاص نماد nd قبلا به‌معنی حاصلضرب دوعدد صحیح به‌کار رفته‌است. خوشبختانه‌این دومعنی باهم متوافق‌اند، زیرا به‌ازاء عددصحیح‌مثبت n حاصلضربndبرابر است با $d+d+\cdots+d$ (n دفعه). هر دوتعبیر دربرهان قضیهٔ بعدی ما ظاهرمی‌شوند. این قضیه برای گسترش حساب درفصل ۵ اهمیت بنیادی دارد.

قضیهٔ ۴پ. هر زیرگروه H ازگروه جمعی $\mathbf{Z}$ دوری است، یعنی عددی چون $d\in\mathbf{Z}$ وجود دارد به قسمی‌که $H=\mathbf{Z}d$. مولد d می‌تواند چنان اختیار شودکه $d\geqslant 0$ ودراین صورت به طور یکتا به وسیلهٔ H معین می‌شود.

برهان. اگر $H=\{0\}$، می‌توان $d=0$ اختیارکرد و حکم به طور بدیهی برقرار است. بنابراین فرض کنیدکه $H\neq\{0\}$. پس H شامل عنصری مانند $h\neq 0$ می‌باشد، و ازآنجا که H یك زیرگروه است، بایستی شامل h — نیز باشد؛ لذا H باید حداقل شامل یك

عضو مثبت باشد. بنا به اصل خوش ترتیبی، H شامل کوچکترین عضو مثبت d است(صفحه ۳۸را ببینید). واضح است که همهٔ توانهای جمعی d در H قراردارند، زیرا H یك زیر گروه است، از این‌رو $\mathbf{Z}d \subset H$. حال فرض کنید که $n \in H$. بنابه خاصیت اقلیدسی $\mathbf{Z}$ (قضیهٔ ۳پ)، $n = qd + r$، که در آن $r \in \mathbf{Z}$، q و $0 \leqslant r < d$. چون H یك زیر گروه است، داریم $qd \in H$، و بنابراین $r = n - qd \in H$. ولی d کوچکترین عضو مثبت H است، و $0 \leqslant r < d$، لذا r مثبت نبوده وبایستی صفر باشد. بنابراین $n = qd \in \mathbf{Z}d$ و نتیجه‌می‌دهد که $H = \mathbf{Z}d$. نشان داده‌ایم که d می‌تواند مثبت یاصفراختیارشود. هنگامی که $H = \{0\}$، یکتایی d روشن است. اگر $H \neq \{0\}$، فرض کنیدکه $c > 0$ مولدی از H باشد. آنگاه همهٔ اعضای مثبت H به‌صورت nc با $n > 0$ هستند. اما این نتیجه‌می‌دهدکه $n \geqslant 1$ و ازاینرو $nc \geqslant c$. بنابراین c کوچکترین عضو مثبت H است و لذا به طور یکتا به وسیلهٔ H معین می‌گردد.

نتیجه. اگر G یك‌گروهٔ دوری باشد، آنگاه هر زیرگروه آن دوری است.

برهان. فرض کنید G به‌وسیلهٔ g تولیدشده‌باشد و K زیر گروه دلخواهی ازآن باشدوتعریف کنید: $H = \{n \in \mathbf{Z} \; ; \; g^n \in K\}$. آنگاه H زیر گروهی جمعی از $\mathbf{Z}$ است (سه شرط راتحقیق کنید!). بنابراین بنا به قضیه، به ازاء عددی چون d داریم $H = \mathbf{Z}d$. حال $k = g^d \in K$، زیرا $d \in H$، و واضح است که k زیر گروه K را تولید می‌کند. چون اگر $g^n \in K$ آنگاه $n \in H$ (بنابه تعریف)، از اینرو به ازاء عدد صحیحی چون r داریم $n = rd$، و $g^n = g^{rd} = k^r$.

در هر گروه، عنصر x از مرتبهٔ متناهی خوانده می‌شود اگر به ازاء عددی چون $n > 0$ داشته باشیم $x^n = e$؛ سپس کوچکترین‌این nها مرتبهٔ x نامیده می‌شود. اگر چنین n ای وجود نداشته باشدگوییم x دارای مرتبهٔ نامتناهی است. رابطهٔ بین مرتبهٔ عنصرها و مرتبهٔ گروهها (چنانکه قبلا تعریف شده است) در قضیهٔ بعدی‌آمده است.

قضیهٔ ۴ت: فرض‌کنید G یك گروه باشد و $x \in G$. دراین صورت مرتبهٔ x برابر است با مرتبهٔ زیرگروه دوری X تولید شده بوسیلهٔ x. اگر x دارای مرتبهٔ نامتناهی باشد، آنگاه همهٔ توانهایش متمایز هستند: $x^r = x^s \Longleftrightarrow r = s$. اگر x دارای مرتبهٔ متناهی nباشد، آنگاه

(الف) $x^r = x^s \Longleftrightarrow r \equiv s (n$ به‌پیمانهٔ $n)$ ؛ و(ب) $x^k = e \Longleftrightarrow n \mid k$.

برهان. نخست فرض‌کنیدکه x دارای مرتبهٔ‌نامتناهی باشد، یعنی به ازاءهر $k > 0$ داریم: $x^k \neq e$. حال اگر $x^r = x^s$ و اگر $r \geqslant s$ (این را می‌توان فرض‌کرد بی آنکه به‌کلیت مطلب خللی‌واردآید)، آنگاه $e = x^r (x^s)^{-1} = x^{r-s}$، و $r - s \geqslant 0$. درنتیجه $r - s = 0$ یعنی، $r = s$. بنابراین همهٔ توانهای x متمایزند و X گروهی نامتناهی است.

سپس فرض کنید که x دارای مرتبهٔ متناهی n باشد، یعنی، $x^n=e$ ، $n>0$ و به ازاء $0<k<n$ ، $x^k\neq e$. برای هرعدد صحیح k می‌توان نوشت: $k=qn+t$ ، که در آن q و t اعداد صحیح‌اند و $0\leqslant t<n$. چون $x^k=x^{qn+t}=(x^n)^q x^t=x^t$ ، بلافاصله نتیجه می‌شود که $x^k=e\Longleftrightarrow x^t=e\Longleftrightarrow t=0\Longleftrightarrow n|k$. ازاینرو داریم:

$$x^r=x^s\Longleftrightarrow x^{r-s}=e\Longleftrightarrow n|(r-s)\Longleftrightarrow r\equiv s(n \text{ به پیمانهٔ})$$

همچنین، $x^k=x^t$ نتیجه می‌دهد که هر توانی از x برابر یکی از عنصرهای e ، x ، x^2 ، ... ، x^{n-1} است ، و اینها متمایزند زیرا هیچ دو عدد صحیح از اعداد 0 ، 1 ، 2 ، ... ، $n-1$ همنهشت به پیمانهٔ n نیستند. پس $X=\{e, x, x^2, \ldots, x^{n-1}\}$ ، دقیقاً n عنصر دارد.

این قضیه نشانهٔ روشنی ازانواع گروههای دوری ممکن به دست می‌دهد. همهٔ آنهایی که نامتناهی‌اند شبیه هم هستند، یعنی عناصرشان به طور یکتا به وسیلهٔ اعداد صحیح قابل نامگذاری است. گروههای دوری متناهی ازمرتبهٔ مفروض n نیز شبیه هم‌اند. چون همهٔ آنها متشکل‌اند از عناصر e ، x ، x^2 ، ... ، x^{n-1} که درآن x مولد گروه است. حال به تدقیق عبارت «شبیه هم» می‌پردازیم. دو گروه A و B یکریخت نامیده می‌شوند (نوشته می‌شود : $A\cong B$) ، اگر نگاشت دوسویی $f: A\longrightarrow B$ وجود داشته باشد که ضرب گروه را حفظ کند، یعنی، به ازاء هر x ، $y\in A$ ، داشته باشیم $f(xy)=f(x)f(y)$. چنین نگاشت f یك یکریختی بین این گروهها نامیده می‌شود . از این شرط خودبخود نتیجه می‌شود که f عنصرخنثی ومعکوسها را نیزحفظ می‌کند، یعنی $f(e)=e$ (که درآن e به‌طور مسامحه‌آمیز برای نشان دادن عنصرهای خنثای A و B هر دو به‌کارگرفته شده است) و به ازاء هر $x\in A$ داریم $f(x^{-1})=(f(x))^{-1}$. برای اثبات این‌امر، قرار دهید $b=f(e)$ ، آنگاه $b^2=f(e)f(e)=f(e^2)=f(e)=b$ ، که از آن نتیجه‌می‌شود b عنصر خنثای B است. مجدداً قرار دهید $c=f(x^{-1})$ ، آنگاه در B داریم:

$$cf(x)=f(x^{-1})f(x)=f(x^{-1}x)=f(e)=e$$

واین نتیجه می‌دهد $c=(f(x))^{-1}$.

با استفاده ازتعریف واضح است که ترکیب دویکریختی یك یکریختی است. بعلاوه، معکوس یك‌یکریختی (یادآوری می کنیم که معکوس هر تابع دوسویی موجود است) نیزیك یکریختی‌می‌باشد. چون اگر $f: A\longrightarrow B$ یك‌یکریختی باتابع معکوس $g: B\longrightarrow A$ باشد واگر u ، $v\in B$ ، آنگاه $u=f(x)$ ، $v=f(y)$ که‌درآنها $x=g(u)$ ، $y=g(v)$. بنابراین $g(uv)=g(f(xy))=xy=g(u)g(v)$ ، و از اینرو $uv=f(x)f(y)=f(xy)$. این حقایق (همراه با این حقیقت بدیهی که نگاشت همانی روی یك گروه یك یکریختی است) نشان می‌دهند که رابطهٔ $A\cong B$ بین گروهها یك رابطهٔ هم ارزی است، یعنی برای همهٔ گروههای A ، B ، C داریم :

(الف) $A\cong A$ ،

(ب) $A\cong B\Longrightarrow B\cong A$ ،

(پ) $A \cong B$ و $B \cong C \Rightarrow A \cong C$.

بنابراین می‌توان گروهها را رده‌بندی کرد به طوری که دو گروه در یك رده قرارداشته باشند اگر و فقط اگر یکریخت باشند. (قضیهٔ ۲ت را ببینید.) این رده‌ها را «رده‌های یکریختی» یا «انواع یکریختی» نامیم.

چون ضرب، معکوس‌گیری و عنصرخنثی، که اجزای سازای همهٔ تساویها در گروهها هستند، به‌وسیلهٔ یکریختیها حفظ می‌شوند، نتیجه می‌شود که اگر $f : A \longrightarrow B$ یك‌یکریختی باشد، آنگاه هرتساوی درست در A دارای نظیری در B است. به عنوان مثال، اگر در A داشته باشیم: $a^5 = e$ واگر $b = f(a)$ ، آنگاه در B خواهیم داشت: $b^5 = e$ ، و بعکس زیرا f^{-1} یك یکریختی است. بنابراین دو گروه یکریخت از جنبهٔ نظریهٔ گروهها دارای خاصیتهای یکسانی هستند واز این‌نقطه نظر غیرقابل‌تشخیص‌اند. هنگامی که به‌نوع یکریختی یك‌گروه نظرمی‌کنیم، از طبیعت عناصر، به طور فردی، صرف‌نظرمی‌شود وتوجه معطوف به «ساخت جبری» می‌شـــود، یعنی ریخت حاصل از روابط جبری میان‌عنصرهامورد نظراست.

اگریکی از دو گروه A و B یا هردوی آنها با نماد دیگری‌نوشته شده باشند، تعریف را باید مطابق آن ارائه‌کرد. بنابراین یك یکریختی از گروهی جمعی به یك گروه ضربی نگاشتی‌است‌دوسویی‌مانند f که در $f(x+y) = f(x)f(y)$ صدق‌می‌کند. دراین‌صورت، f خودبخود در شرایط $f(0) = e$ و $f(-x) = (f(x))^{-1}$ صدق خواهدکرد و معکوس آن یعنی g در شرایـط $g(uv) = g(u) + g(v)$ ، $g(e) = 0$ و $g(u^{-1}) = -g(u)$ صدق خواهد نمود.

مثال ۱۶.۴. گروه جمعی $\mathbf{Z}$ باگروه جمعی همهٔ اعداد زوج به وسیلهٔ یکریختی $n \longrightarrow 2n$، یکریخت‌است .

مثال ۱۷.۴. مجموعهٔ G متشکل از همهٔ ماتریسهای

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

که درآن a و b دو عدد حقیقی‌اند و هردو صفر نیستند، نسبت به ضرب ماتریسها یك گروه است. این‌گروه G باگروه ضربی اعداد مختلط غیر صفر $\mathbf{C}^*$ یکریخت است . عدد مختلط متناظر با ماتریس

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

$a + bi$ است، و خواننده باید تحقیق‌کندکه در واقع این‌تناظر یك یکریختی است.

مثال ۱۸.۴. گروه جمعی $\mathbf{R}$ باگروه‌ضربی $\mathbf{R}^+$ ، مجموعهٔ اعدادحقیقی مثبت، بنابه‌نگاشت

نمایی $x \longrightarrow e^x$ ، یکریخت است. اینکه این نگاشت دوسویی است و نیز دستور معروف $e^{x+y}=e^x e^y$ که بیان می کنـــد نگاشت یکریختی است از بعضی قضایای آنالیز مقدماتی، نتیجه می‌شود. بنابراین $e^0=1$ و $e^{-x}=(e^x)^{-1}$. همچنین نتیجه می گیریم که تابع معکوس این تابع کـه تابع لگاریتمی نامیده می‌شود (و با log نشان داده می‌شود) ، در شرایط $\log(1)=0$ ، $\log(uv)=\log u+\log v$ و $\log(u^{-1})=-\log(u)$ صدق می کند. این یکریختی البته مبنایی است برای استفادهٔ لگاریتمها در ضرب اعداد مثبت . اینکـه دو گروه یکریخت‌اند به ما می گوید که علی‌رغم ظاهرشان ضرب اعـداد حقیقی مثبت اساساً همان عمل جبری جمع در اعداد حقیقی است. برای تعویض یکی به دیگری کافی است که به نحوی از این یکریختی استفاده کنیم مثلا، مجموعه‌ای از جداول لگاریتم، یا خط کش محاسبه .

قضیهٔ ۴ث. هر دو گروه دوری هم مرتبه یکریخت‌اند .

برهان. فرض کنید X و Y دو گروه دوری باشند که به‌ترتیب به وسیلهٔ x و y تولید شده‌اند. اگر هردو از مرتبهٔ نامتناهی باشند، آنگاه ، بنا به قضیهٔ ۴ت ، همهٔ توانهـای x وبـه همین ترتیب، همهٔ توانهای y ، متمایزند. این موضوع نتیجه می‌دهد که نگاشت $f : X \longrightarrow Y$ که به‌وسیلهٔ $f(x^r)=y^r$ تعریف‌شده ، نگاشتی دوسویی است. این نگاشت یکریختی است زیرا

$$f(x^r x^s)=f(x^{r+s})=y^{r+s}=y^r y^s=f(x^r)f(x^s).$$

حال فرض کنید که X و Y هردو ازمـرتبهٔ متناهی n باشند. آنگاه، بنا به قضیهٔ ۴ت ، داریم: $X=\{e, x, x^2, \dots, x^{n-1}\}$ و $Y=\{e, y, y^2, \dots, y^{n-1}\}$ ، از اینرو می‌توانیم نگاشتی دوسویی مانند $f : X \longrightarrow Y$ را به‌وسیلهٔ قاعدهٔ $f(x^r)=y^r$ ، به ازاء $0 \leqslant r < n$ ، تعریف کنیم. قاعدهٔ ضرب در X به‌صورت زیر است: اگر $0 \leqslant r < n$ ، $0 \leqslant s < n$ ، آنگاه $x^r \cdot x^s = x^{r+s} = x^t$ که در آن

$$\begin{cases} t=r+s & \text{اگر } r+s<n \text{ ،} \\ t=r+s-n & \text{اگر } r+s \geqslant n \text{ ،} \end{cases}$$

قاعدهٔ ضرب در Y شبیه حالت فوق است، ازاینرو واضح است که f ضرب را حفظ می کند و بنابراین یك یکریختی است.

نتیجه . (الف) هرگروه دوری نامتناهی با گروه جمعی $\mathbf{Z}$ یکریخت است.

(ب) هـر گروه دوری متناهی از مرتبهٔ n بـا گروه P_n از ریشه‌های n ام ۱ در $\mathbf{C}$ ، یکریخت است.

این فصل را با اثبات قضیهٔ مشهور لاگرانژ[1] به پایان می‌رسانیم که ادعا می کند که در

1. Lagrange

هر گروه متناهی از مرتبهٔ n، مرتبهٔ هرزیر گروه باید مقسوم‌علیهی از n باشد. این قضیه به وسیلهٔ افراز گروه به زیر مجموعه‌های هم اندازه ثابت می‌شود، و این افراز به طریق زیر حاصل می‌شود. فرض کنید H زیر گروهی از یك گروه G (که لزوماً متناهی نیست) باشد. به ازاء $x\in G$ ، $y\in G$ ، $x\sim y$ را به معنی $xy^{-1}\in H$ (یا درنماد جمعی $x-y\in H$) بگیرید. آنگاه $\sim$ یك رابطهٔ هم ارزی روی G است، سه شرط رابطهٔ هم ارزی به صورت جالبی با سه شرط برای یك زیر گروه متناظرند. ارتباط بین این دو مفهوم البته خیلی نزدیك است:

(الف) $\sim$ انعکاسی است زیرا $xx^{-1}=e\in H$ ، یعنی، $x\sim x$.

(ب) $\sim$ متقارن است زیرا اگر $x\sim y$ آنگاه $xy^{-1}\in H$، ازاینرو $(xy^{-1})^{-1}\in H$. اما $(xy^{-1})^{-1}=(y^{-1})^{-1}x^{-1}=yx^{-1}$، پس $y\sim x$.

(پ) $\sim$ متعدی است زیرا اگر $x\sim y$ و $y\sim z$ آنگاه $xy^{-1}\in H$ و $yz^{-1}\in H$ و بنابراین $xz^{-1}=(xy^{-1})(yz^{-1})\in H$ ، یعنی ، $x\sim z$.

رده‌های هم‌ارزی که ازاین رابطه ناشی می‌شوند همرده‌های راست H در G نامیده می‌شوند. همردهٔ راست $<x>$ حاوی عنصر x، شامل همهٔ عناصر $y\in G$ می‌باشد به‌قسمی که $yx^{-1}\in H$، یعنی به ازاء عنصری چون $h\in H$ داریم $y=hx$. بنابراین $<x>=Hx$ ، که در آن $Hx=\{hx\ ;\ h\in H\}$. همردهٔ راست شامل e برابر است با $He=H$.

استدلال مشابهی مارا به همرده‌های چپ H در G هدایت می‌کند. با رابطهٔ $x^{-1}y\in H$ آغاز می‌کنیم و درمی‌یابیم که رابطه‌ای هم‌ارزی است و رده‌هایش مجموعه‌های $xH=\{xh\ ;\ h\in H\}$ می‌باشند. البته چنانچه G گروهی آبلی باشد. آنگاه همرده‌های چپ و راست برهم منطبق‌اند. در نماد جمعی همرده‌های راست و چپ را به‌ترتیب به صورت $H+x$ و $x+H$ می‌نویسیم.

مثال ۱۹.۴. فرض کنید G گروه جمعی $\mathbf{C}$ و H زیر گروه $\mathbf{R}$ باشد. آنگاه همرده‌های راست (و چپ) H (در نمودار آرگان) خطوط موازی با محور حقیقی‌اند. به طور کلیتر اگر H زیر گروه شامل همهٔ مضارب حقیقی یك عدد مختلط ثابت z باشد، که در آن صورت، H برابر خطی مار بر مبدأ خواهد بود، آنگاه همرده‌های H خطوطی موازی با آن خط هستند. این خطوط صفحه را افراز می‌کنند.

مثال ۲۰.۴. فرض کنید G گروه ضربی $\mathbf{C}^*$ و H گروه دایره‌ای T باشد (مثال ۵.۴ را ببینید)، که زیر گروهی از $\mathbf{C}^*$ است. آنگاه همرده‌های راست (و چپ) T دایره‌هایی به مرکز o هستند. چون، اگر z_0 عدد مختلط ثابتی باشد آنگاه همردهٔ Tz_0 شامل همهٔ اعداد مختلط $z=tz_0$ می‌باشد که در آن $|t|=1$ ، و این اعداد دقیقاً آنهایی هستند که در

$|z|=|z_0|$ صدق می‌کنند.

مثال ۲۱.۴. فرض کنید $G=\mathbf{C}^*$ و H گروه ضربی $\mathbf{R}^+$ از اعداد حقیقی مثبت باشد. آنگاه همرده‌های H در G نیمخطهایی هستند که در نمودار آرگان همه ماربر مبدأ مختصات‌اند. (نیمخطی که حاوی یك عدد مختلط مفروض w است، شامل همهٔ مضارب حقیقی مثبت w نیز خواهد بود.)

مثال ۲۲.۴. اگر G گروه جمعی $\mathbf{R}$ و H زیر گروه $\mathbf{Z}$ باشد، آنگاه یك همردهٔ نمونه‌ای $x+\mathbf{Z}$ متشکل است ازهمهٔ نقاط $x+n$ $(n=0, \pm 1, \pm 2, \dots)$. این نقاط‌درامتداد محور حقیقی و به فاصلهٔ واحد از هم، قراردارند.

مثال ۲۳.۴. اگر G گروه جمعی $\mathbf{Z}$ و H زیر گروه $n\mathbf{Z}$ باشد، آنگاه یك همردهٔ $r+n\mathbf{Z}$، که $r\in\mathbf{Z}$، متشکل‌است ازهمهٔ اعداد صحیح $a=nq+r$، که درآن $q\in\mathbf{Z}$.به عبارت‌دیگر، همردهٔ $r+n\mathbf{Z}$، همان‌ردهٔ باقیماندهٔ به پیمانهٔ n ای است‌که شامل r می‌باشد. دراین‌حالت رابطهٔ هم‌ارزی‌که به وسیلهٔ $n\mathbf{Z}$ تعریف شده همان همنهشتی به‌پیمانهٔ n است، زیرا

$$a-b\in n\mathbf{Z} \Longleftrightarrow n|(a-b).$$

مثال ۲۴.۴. به منظور نشان دادن اینکه همرده‌های راست وچپ همیشه برهم منطبق نیستند، فرض می‌کنیم $G=\mathcal{S}_3$، گروه متقارن روی سه علامت، و $H=\{e, a\}$، که در آن a ترانهش

$$\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

است. با مراجعه به نمادگذاری وجدول ضرب درمثال ۱۲.۴، می‌بینیم که همرده‌های‌راست متمایز H عبارت‌انداز: $Hp=\{p, b\}$ و $Hq=\{q, c\}$، درصورتی که‌همرده‌های چپ آن H، $pH=\{p, c\}$ و $qH=\{q, b\}$ هستند.

قضیهٔ ۴ج. فرض‌کنید H زیر گروهی ازگروه G باشد. دراین صورت

(الف) همرده‌های‌راست Hx از H تشکیل‌یك افراز از G می‌دهند؛

(ب) $Hx=Hy \Longleftrightarrow x\in Hy \Longleftrightarrow y\in Hx$؛

(پ) یك نگاشت‌دوسویی بین هردو همردهٔ راست H وجود دارد.
نتیجهٔ مشابهی‌برای همرده‌های چپ برقرار است.

برهان. قبلا نشان داده‌ایم که نسبت به رابطهٔ هم‌ارزی $x\sim y \Longleftrightarrow xy^{-1}\in H$، مجموعهٔ

Hx همان ردهٔ هم ارزی شامل x است. از اینجا گزارهٔ (الف) فوراً نتیجه می‌شود. همچنین نتیجه می‌شود که $Hx=Hy \iff x\sim y \iff xy^{-1}\in H \iff x\in Hy$، و بنا به خاصیت تقارنی: $Hx=Hy \iff y\in Hx$. و سرانجام، برای اثبات (پ)، کافی است نشان دهیم که به‌ازاء هر $x\in G$، نگاشتی دوسویی از H به Hx وجود دارد. (سپس گزارهٔ (پ) از قضایای ۲ب و ۲پ نتیجه خواهد شد.) ولی بسادگی می‌توان دید که (به ازاء x ثابت) نگاشت $f: H \longrightarrow Hx$ که به وسیلهٔ $h \longmapsto hx$ تعریف شده، یك نگاشت دوسویی است. این نگاشت یك به‌یك است زیرا بنا به قانون حذف در گروهها داریم: $hx=h'x \Rightarrow h=h'$: بروی نیز می‌باشد زیرا، بنا به تعریف، هر عنصر Hx، به ازاء عنصری چون $h\in H$، به‌صورت hx است.

نتیجهٔ ۱. (قضیهٔ لاگرانژ) اگر گروه G متناهی از مرتبهٔ n باشد، آنگاه مرتبهٔ هر زیر گروه آن مقسوم‌علیهی از n است.

برهان. اگر H زیر گروهی از مرتبهٔ m باشد، آنگاه، بنا به قسمت (پ) قضیهٔ فوق، هر همردهٔ راست H دقیقاً شامل m عنصر است. چون همرده‌های راست تشکیل افرازی از G می‌دهند داریم $n=rm$، که در آن r تعداد همرده‌هاست.

نتیجهٔ ۲. اگر گروه G متناهی از مرتبهٔ n باشد، آنگاه به ازاء هر $x\in G$، $x^n=e$.

برهان. فرض کنید $x\in G$ و X زیر گروه دوری تولید شده به وسیلهٔ x باشد. اگر مرتبهٔ X برابر m باشد، آنگاه، بنا به قضیهٔ ۴ت، داریم $x^m=e$. اما، بنا به قضیهٔ لاگرانژ، به‌ازاء عدد صحیحی چون r داریم $n=rm$. بنابراین $x^n=x^{rm}=(x^m)^r=e^r=e$.

نتیجهٔ ۳. هر گروه از مرتبهٔ عدد اول، دوری است.

برهان. فرض کنید G گروهی ازمرتبهٔ عدداول p باشد. چون $p\geqslant 2$، عنصری مانند $x\neq e$ در G وجود دارد، و زیر گروه دوری، X، را بـاحداقل دو عنصر تولید می‌کند. بنا به‌قضیهٔ لاگرانژ، مرتبهٔ X یعنی m عدد p را عادمی‌کند، وچون $m\neq 1$ بایستی داشته‌باشیم $m=p$. بنابراین $X=G$ و G دوری است.

اخطار. عکس قضیهٔ لاگرانژ درست نیست؛ یعنی، اگریك گـروه G دارای مرتبهٔ متناهی n باشد و m مقسوم‌علیهی از n باشد، ممکن است هیچ زیر گروهی از مرتبهٔ m موجودنباشد. لیکن، دربرخی از موارد خاص وجود زیر گروهی از مرتبهٔ m را می‌توان ثابت کرد؛ مثلا، اگر G گروه دوری باشد، این مطلب برای همهٔ m هایی کـه n را عادکنند، درست است (قضیهٔ ۷ ج را ببینید). به‌طور کلیتر، اگر G آبلی باشد، برای هر m ی که n را عادکندمی‌توان

نشان داد که زیرگروههایی از مرتبهٔ m وجود دارند. همچنین قضیهٔ مشهور سیلو[1] می‌گوید که اگر m توان اولی باشد که n را عاد کند، آنگاه زیرگروهی از مرتبهٔ m وجود دارد. دو نتیجهٔ اخیر دراغلب کتابهای درسی استانداردِ نظریهٔ گروهها یافت‌می‌شوند ولی‌خارج ازبحث این کتاب مقدماتی‌هستند.

تمرینها

۱. کدامیك از مجموعه‌های زیر گروه هستند؟ در هرمورد دلیل بیاورید.

(الف) مجموعهٔ همهٔ اعداد صحیح فرد نسبت به جمع.

(ب) مجموعهٔ همهٔ اعداد گویا به‌صورت $m/2^n$ نسبت به(آ) جمع و (ب)ضرب.

(پ) مجموعهٔ همهٔ اعداد حقیقی بجز ۱ — نسبت به عمل $*$ که به وسیلهٔ $a*b=a+b+ab$ تعریف شده است.

(ت) مجموعهٔ همهٔ ماتریسهای 2×2 به صورت

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$$

که‌درآن $b\in\mathbf{Q}$ ، $c\in\mathbf{R}$ ، $a\neq 0$ ، $c\neq 0$، نسبت‌به‌عمل‌ضرب ماتریسها.

۲. کدامیك ازگروههای زیر دوری‌اند؟ در هرمورد دلایل خود را ذکر کنید.

(الف) گروه جمعی اعداد گویا، $\mathbf{Q}$.

(ب) گروه دایره‌ای $T=\{z\in\mathbf{C}\ ;\ |z|=1\}$ (مثال ۵.۴ را ببینید).

(پ) گروه متقارن $\mathcal{S}_3$ (مثال ۱۲.۴ را ببینید).

(ت) گروه تقارنهای دورانی وانعکاسی یك مربع مستطیل.

(ث) گروه خطی عمومی $\mathrm{GL}_n(\mathbf{R})$، برای هر $n\geqslant 1$ دلخواه (مثال ۱۰.۴ را ببینید).

۳. چهار تابع $\alpha,\beta,\gamma,\delta:\mathbf{R}^*\longrightarrow\mathbf{R}^*$ به وسیلهٔ $\alpha(x)=x$، $\beta(x)=-x$، $\gamma(x)=x^{-1}$ و $\delta(x)=-x^{-1}$ تعریف شده‌اند. ثابت‌کنیدکه این توابع تحت ترکیب توابع تشکیل یك‌گروه می‌دهند، واین گروه با گروه تقارنهای دورانی و انعکاسی یك مربع مستطیل (که مربع نباشد) یکریخت است.

۴. ثابت‌کنیدکه اگر به ازاء هرعنصر x از یك‌گروه G داشته باشیم $x^2=e$، آنگاه

---

1. Sylow

G آبلی است.

۵. ثابت کنید که هر گروه از مرتبهٔ کوچکتر یا مساوی ۵ آبلی است.

۶. جدول زیر قسمتی ازجدول‌ضرب گروهی ازمرتبهٔ ۶ است. جاهای خالی را پر کنید.

	p	q	r	s	t	u
p	r	·	·	t	·	·
q	·	t	·	·	r	·
r	p	·	·	·	·	·
s	·	·	·	r	·	·
t	·	·	·	p	·	·
u	·	s	·	·	·	r

۷. گروههای زیررا به‌رده‌های یکریختی قسمت کنید ودرستی رده‌بندی خودرا ثابت کنید.

(الف) گروه دایره‌ای $T=\{z\in\mathbf{C}\ ;\ |z|=1\}$.

(ب) گروه ضربی ریشه‌های ششم ۱ در $\mathbf{C}$.

(پ) گروه متقارن $\mathcal{S}_3$.

(ت) گروه جمعی $\mathbf{Z}$.

(ث) گروه تقارنهای دورانی یك شش ضلعی منتظم.

(ج) گروه تقارنهای دورانی وانعکاسی یك مثلث‌متساوی‌الاضلاع.

(چ) گروه توابع $f_n:\mathbf{Z}\longrightarrow\mathbf{Z}$ که به‌وسیلهٔ $f_n(x)=x+n$ تعریف شده‌اند، نسبت به عمل ترکیب توابع . (به ازاء هرعدد صحیح n یك تابع f_n موجود است .)

(ح) گروه ضربی همهٔ اعداد حقیقی به صورت $2^n\ (n\in\mathbf{Z})$.

(خ) گروه جمعی $\mathbf{R}$.

(د) گروه ضربی همهٔ ماتریسهای به صورت

$$\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}$$

که درآن $\theta\in\mathbf{R}$.

(ذ) گروه جمعی $\mathbf{Q}$.

(ر) گروه ضربی همهٔ ماتریسهای به صورت

$$\begin{pmatrix} ۱ & x \\ ۰ & ۱ \end{pmatrix}$$

که در آن $x \in \mathbf{R}$.

(ز) گروه متعامد خاص $O_۲^+$. (مثال ۸.۴ را ببینید)

۸. ثابت کنید که گروه ضربی $\mathbf{Q}^+$ با گروه جمعی $\mathbf{Q}$ یکریخت نیست.

۹. همهٔ زیر گروههای یك گروه دوری از مرتبهٔ ۱۲ را پیدا کنید.

۱۰. اگر A و B زیر گروههای یك گروه G باشند، نشان دهید که $A \cap B$ نیز یك زیر گروه است. آیا $A \cup B$ لزوماً یك زیر گروه است؟ (دلیل بیاورید.)

۱۱. فرض کنید G یك گروه و $g \in G$ عنصری ثابت باشد. ثابت کنید که

$$H = \{x \in G \; ; \; x^{-۱} g x = g\}$$

یك زیر گروه G است.

۱۲. ثابت کنید که در هر گروه آبلی G ، عناصر از مرتبهٔ متناهی تشکیل یك زیر گروه می‌دهند. این زیر گروه را در حالات خاص (الف) $G = O_۲^+$، (ب) (جمعی) $G = \mathbf{Q}$، (پ) (ضربی) $G = \mathbf{Q}^*$ ، (ت) (ضربی) $G = \mathbf{C}^*$ ، مشخص کنید .

۱۳. ثابت کنید اگر G گروهی باشد که تنها زیر گروههایش G و $\{e\}$ هستند، آنگاه G دوری و از مرتبهٔ اول است. (G را متناهی فرض نکنید، و به خاطر داشته باشید که عکس قضیهٔ لاگرانژ درست نیست .)

۱۴. (مشکلتر). ثابت کنید که اگر p و q اعداد اول متمایز باشند، آنگاه هر گروه از مرتبهٔ pq دوری است .

۱۵. (مشکلتر). همهٔ زیر گروههای $\mathcal{A}_۴$ را پیدا کنید.

۱۶. (مشکلتر). فرض کنید G گروهی متناهی از مرتبهٔ n باشد و A ، B دو زیر گروه آن با مرتبه‌های ، به ترتیب، a و b؛ ثابت کنید که مرتبهٔ $C = A \cap B$ (تمرین ۱۰ را ببینید) حداقل ab/n است. (راهنمایی : نشان دهید که هر همردهٔ راست C مشمول یك همردهٔ راست B است و آنهایی که مشمول A هستند همه در همرده‌های متفاوت B قرار دارند.)

۱۷. (مشکلتر) ثابت کنید که تعداد راههای پرانتز گذاری متفاوت برای یك حاصلضرب از n علامت برابر است با

$$\frac{۱}{n}\binom{۲n-۲}{n-۱}$$

فصل ۵

تجزیه در Z

اغلب اشخاص درمراحل اولیهٔ تعلیماتشان درحساب، می‌آموزندکه اگر عددی طبیعی را به‌طور مکرر تجزیه کنند بالاخره به‌تجزیه‌ای برحسب اعداد اول می‌رسند، وعوامل‌اولی که ظاهرمی‌شوند، مستقل از روش تجزیه هستند. این اصل مهم برای اعدادکوچك بسادگی تحقیق می‌شود ودراین مرحلهٔ مقدماتی طبیعی است فرض شودکه برای اعداد بزرگ درست باقی می‌ماند. بعد این اصل برای محاسبهٔ بزرگترین مقسوم‌علیه مشترك وکوچکترین مضرب مشترك دوعدد به‌کار می‌رود ــ بامقایسه وترکیب‌عوامل اول اعداد. البته‌ازکوچکترین مضرب مشترك برای ساده‌کردن محاسبات باکسرها استفاده می‌شود.

به‌این روش دوانتقاد وارد است‌که داتشجوی جدی در ریاضیات باید به‌آن توجه کند. اولا به‌هیچ‌وجه روشن‌نیست‌که عددی‌خیلی بزرگ که عوامل اول‌آن شناخته نشده‌اند (وحتی شاید باکامپیوترهای امروزه نیز قابل‌شناسایی نباشند) حتماً به‌طوریکتایی به‌صورت حاصلضرب اعداد اول قابل بیان باشد. چنین حکم کلی‌ای نیاز به برهان دارد ــ برهانی براساس احکام ساده‌تر وبدیهی‌تر. ثانیاً، تجزیهٔ یك عدد به‌عوامل اولش، ازنظرمحاسباتی، روش خیلی پیچیده‌ای است، وباید سؤال‌کرد آیا الگوریتم ساده‌تر وکوتاهتری‌برای‌محاسبهٔ بزرگترین مقسوم‌علیه‌های مشترك وجود دارد. درواقع اقلیدس در ۲۰۰۰ سال قبل، هم‌این برهان رامی‌دانست وهم‌این الگوریتم را وجای‌تأسف است‌که‌اینها امروزه‌به‌طورگسترده‌ای تدریس نمی‌شوند.

برهان اقلیدس درمورد یکتایی تجزیه به‌عوامل اول، که درسطور آتی به‌توصیف آن خواهیم‌پرداخت، مبتنی‌است بروجود وخواص بزرگترین‌مقسوم‌علیه مشترك، بنابراین‌بایستی اینها دروهلهٔ اول و بدون استفاده از عوامل اول ثابت‌گردند. روشی‌که دراولین پاراگراف فوق مختصراً شرح داده شده است، گرچه ممکن است بهترین روش برای تدریس موضوع

باشد، معهذا منطقی به‌نظر نمی‌رسد چون بقول معروف، ارابه را درجلوی اسب قرارمی‌دهد. وبعلاوه، به‌این حقیقت مهم نمی‌پردازدکه می‌گوید همواره می‌توان بزرگترین مقسوم‌علیه مشترك a و b را به‌صورت $ma+nb$، که درآن m و n اعداد صحیح‌اند، نوشت. ما این موضوع را به‌عنوان نتیجه‌ای از برهان وجود بزرگترین مقسوم‌علیه‌های مشترك، ثابت‌می‌کنیم، وبرهان را برروی نظریهٔ گروهها بنامی‌کنیم، زیرا این‌ساخت‌گروه است‌که به‌بهترین وجهی دلیل ظاهرشدن اعداد صحیح به‌صورت $ma+nb$ راتوضیح می‌دهد.

فرضیات اولیهٔ ما برای $\mathbf{Z}$ درفصل۳ شرح داده شده است. یادآوری می‌کنیم که به‌ازاء $x, y\in\mathbf{Z}$ ، $x|y$ یعنی «x عدد y را عاد می‌کند» ، یعنی ، $(\exists z\in\mathbf{Z})(y=xz)$ ، وبه‌برخی ازنتایج ساده توجه می‌کنیم:

(الف) به‌ازاء هر $x\in\mathbf{Z}$ ، $x|0$ ؛

(ب) اگر $a|0$ آنگاه $a=0$ ؛

(پ) اگر $a|1$ آنگاه $a=1$ یا $a=-1$ ؛

(ت) اگر $x|y$ و $y|x$ آنگاه $y=x$ یا $y=-x$

البته، قسمتهای (الف) و (ب) بلافاصله از تعریف نتیجه می‌شوند. برای اثبات(پ)، فرض کنیدکه $a|1$ ، یعنی به‌ازاء عدد صحیحی چون b داریم $ab=1$. واضح‌است‌که $a\neq 0$ و $b\neq 0$ ، ازاینرو یا a و b هردومثبت یاهردو منفی‌اند. اگر هردومثبت باشند، آنگاه $a\geqslant 1$ و $b\geqslant 1$ ، از اینرو $ab=1\geqslant a$ ونتیجه می‌گیریم که $a=1$ ؛ چون 1 کوچکترین عدد صحیح‌مثبت‌است. وبه‌همین‌ترتیب، اگرهردوی‌آنهامنفی باشندآنگاه $a\leqslant -1$ ، $b\leqslant -1$، از اینرو $a=-(-1)\geqslant 1=ab$ ، و نتیجه می‌شودکه $a=-1$. عبارت (ت) بسادگی نتیجه می‌شود زیرا اگر $x=my$ و $y=nx$ $(m, n\in\mathbf{Z})$ آنگاه $x=mnx$. از قانون‌حذف در $\mathbf{Z}$ ، نتیجه می‌شودکه یا $x=0$ یا $mn=1$. دراولین حالت $y=nx=0$، از اینرو $x=y$. در دومین حالت، بنابه قسمت (پ) ، داریم $n=\pm 1$ و از اینرو $y=nx=\pm x$.

بیان دیگر $a|1$ ، آن است‌که بگوییم a در $\mathbf{Z}$ معکوس‌پذیر است، یعنی دارای‌معکوسی مانند a^{-1} در $\mathbf{Z}$ است به‌قسمی‌که $aa^{-1}=1=a^{-1}a$. درآن‌صورت عبارت (پ) فوق می‌گوید‌که تنهاعنصرهای معکوس‌پذیر $\mathbf{Z}$ عبارت‌اند از: 1 و -1 . این عناصرمعکوس‌پذیر یکه‌های $\mathbf{Z}$ نیز نامیده می‌شوند.

دوعدد صحیح a و b مفروض‌است، گوییم که عدد صحیح d بزرگترین مقسوم‌علیه مشترك a و b است اگر

(الف) $d|a$ و $d|b$ ،

(ب) $(\forall c\in\mathbf{Z})((c|a, c|b)\Rightarrow c|d)$ ، و

(پ) $d\geqslant 0$.

شرایط (الف) و (ب) بیان می‌کنند که d مقسوم‌علیه مشترکی است که بر همهٔ مقسوم‌علیه‌های مشترک دیگر قابل قسمت است. شرط (پ) برای راحتی و به‌منظور یکتاساختن d اضافه شده است. توجه کنید که تعریف یک اصطلاح جدید به‌هیچ‌وجه وجود یا یکتایی آن‌را تضمین نمی‌کند؛ واصولا برای اینکه تعریف مفید فایده‌ای باشد، اینهارا باید قبلا ثابت کرد.

قضیهٔ ۵آ. هردوعدد صحیح a و b دارای بزرگترین مقسوم‌علیه مشترک یکتایی مانند d اند. بعلاوه، به‌ازاء اعداد مناسب $r, s\in\mathbf{Z}$، d می‌تواند به‌صورت $d=ra+sb$ نوشته شود.

برهان. اثبات یکتایی ساده‌است: اگر d و d' دو بزرگترین مقسوم‌علیه مشترک a و b باشند آنگاه، بنا به تعریف، $d|d'$ و $d'|d$. بنابراین $d'=\pm d$ وچون $d\geqslant 0$ و $d'\geqslant 0$، نتیجه می‌شود که $d=d'$. ازاینرو a و b دارای حداکثر یک بزرگترین مقسوم‌علیه مشترک هستند. برای اینکه نشان دهیم دارای حداقل یکی هستند، مجموعهٔ $H=\{ma+nb\ ;\ m, n\in\mathbf{Z}\}$ را درنظر می‌گیریم. (دراینجا a و b ثابت، m و n متغیرند). H زیرمجموعه‌ای از $\mathbf{Z}$ است واکنون تحقیق می‌کنیم که یک زیرگروه جمعی $\mathbf{Z}$ می‌باشد. سه‌شرط برای تحقیق وجود دارد، وهمهٔ آنها بسادگی از تعریف H نتیجه می‌شوند:

(الف) $0\in H$، زیرا $0=0a+0b$؛

(ب) اگر $x\in H$، آنگاه $x=ma+nb$، ازاینرو

$$-x=(-m)a+(-n)b\in H\ ;$$

(پ) اگر $x, x'\in H$، آنگاه $x=ma+nb$، $x'=m'a+n'b$. ازاینرو

$$x+x'=(m+m')a+(n+n')b\in H.$$

اما می‌دانیم زیرگروههای جمعی $\mathbf{Z}$ چه‌هستند: بنا به‌قضیهٔ ۴پ، H دوری است، یعنی، به‌ازاء عددصحیحی چون $d\geqslant 0$ داریم $H=\mathbf{Z}d=\{zd\ ;\ z\in\mathbf{Z}\}$. حال گوییم که این عددصحیح d، درواقع، بزرگترین مقسوم‌علیه مشترکی برای a و b است. در وهلهٔ اول، چون $H=\mathbf{Z}d$، هر عضو H، بر d قابل قسمت است. درحالت خاص، چون $a=1a+0b\in H$ و $b=0a+1b\in H$، داریم $d|a$ و $d|b$. دروهلهٔ دوم، چون $d\in H$، اعدادی مانند $r, s\in\mathbf{Z}$ موجودند به‌طوری که: $d=ra+sb$، وازاینرو اگر $c|a$ و $c|b$ آنگاه $c|d$ (زیرا، اگر $a=xc$ و $b=yc$ آنگاه $d=ra+sb=(rx+sy)c$). ازطرفی چون $d\geqslant 0$ پس d درهمهٔ شرایط بزرگترین مقسوم‌علیه مشترک صدق می‌کند. ضمناً آخرین قسمت حکم قضیه را نیز ثابت کرده‌ایم.

نتیجه. فرض کنید $a, b, c\in\mathbf{Z}$. دراینصورت معادلهٔ $ax+by=c$ دارای جواب صحیح است [یعنی، $(\exists x, y\in\mathbf{Z})(ax+by=c)$] اگر وفقط اگر بزرگترین مقسوم‌علیه مشترک a, b عدد c را بخش‌کند.

برهان. فرض کنید d بزرگترین مقسوم‌علیه مشترك a و b باشد. آنگاه همان‌طور که در برهان قضیه نشان‌داده شد، $H=\mathbf{Z}d$ دقیقاً مجموعهٔ همهٔ اعداد صحیح به‌صورت $ax+by$ است، به‌ازاء x، $y\in\mathbf{Z}$. بنابراین $c\in H \iff ax+by=c$ دارای جواب است $\iff d|c$. همچنین می‌توانیم به‌جای استفاده از برهان قضیهٔ قبل، حکم آن را به‌کار بریم: (الف) اگر به‌ازاء اعداد صحیح x، y داشته باشیم $ax+by=c$، آنگاه چون $d|a$ و $d|b$، داریم $d|c$؛ (ب) بنا به قضیهٔ فوق، به‌ازاء اعداد صحیحی چون r، $s\in\mathbf{Z}$ داریم $d=ar+bs$، از اینرو اگر $d|c$ آنگاه $c=dt=a(rt)+b(st)$ و از آنجا جواب صحیح $x=rt$، $y=st$ به‌دست می‌آید.

تبصره‌ها. (۱) خوب است زیرگروه $H=\{ma+nb\ ;\ m,n\in\mathbf{Z}\}$ با زیرگروههای دوری $A=\{ma\ ;\ m\in\mathbf{Z}\}$ و $B=\{nb\ ;\ n\in\mathbf{Z}\}$ مقایسه شود. H شامل هردو زیرگروه دوری A و B بوده ودرواقع کوچکترین زیرگروه $\mathbf{Z}$ است که شامل a و b می‌باشد.

(۲) بیان d به‌صورت $ma+nb$ یکتا نیست.

(۳) برهان قضیه نشان می‌دهد که بزرگترین مقسوم‌علیه مشترك a و b دقیقاً کوچکترین عدد نامنفی به‌صورت $ma+nb$ است.

(۴) اکنون وجه تسمیهٔ «بزرگترین مقسوم‌علیه مشترك» معلوم می‌شود (اگر a و b هردو صفر نباشند) زیرا d مثبت است و به همهٔ مقسوم‌علیه‌های مشترك قابل قسمت می‌باشد. بنابراین، درواقع، بزرگترین آنهاست.

(۵) اگر $a=0$ و b مثبت باشد آنگاه $d=b$. اگر $a=0$ و b منفی باشد آنگاه $d=-b$. «بزرگترین مقسوم‌علیه مشترك» ۰ و ۰ صفراست، امادراین حالت نام آن نامناسب است چون همهٔ اعداد صحیح مقسوم‌علیه‌های مشترك ۰ و ۰ هستند.

(۶) کوچکترین مضرب مشترك m از a و b می‌تواند به‌همین‌نحو باشرایط زیر تعریف شود:

(الف) $a|m$ ، $b|m$؛

(ب) $(a|m' \text{ و } b|m') \Rightarrow m|m'$؛

(پ) $m\geqslant 0$.

وجود m را می‌توان به‌کمك قضیهٔ ۵ آ نشان داد. به‌این‌ترتیب: اگر a و b هردوصفر نباشند و $a=da'$، $b=db'$، که درآنها d بزرگترین مقسوم‌علیه مشترکشان است، آنگاه عدد صحیح $ab/d=a'b'd$ دارای‌خواص (الف) و (ب) است. اثبات یکتایی m ساده است. به‌طریق دیگر می‌توانیم برهان قضیهٔ ۵ آ را تقلیدکنیم و به‌جای H زیرگروه $K=A\cap B$ را درنظربگیریم، که درآن A و B همانند تبصرهٔ(۱) تعریف می‌شوند.

نمادگذاری. بزرگترین مقسوم‌علیه مشترك a و b با $d=(a,b)$ نشان‌داده‌می‌شود. خواننده حتماً به‌یاد داردکه این نماد قبلا به‌کارگرفته شده، ولی چون سه‌معنای مختلف‌این علامت،

درزمینه‌های متفاوت استانده شده‌اند، وندرتاً باهم ظاهرمی‌شوند، بنابراین دلیل‌موجهی برای تغییردادن هیچکدام ازآنها نداریم.

تعریف. دوعدد صحیح a و b متباین (یانسبت بهم‌اول)هستند اگر $(a , b) = ۱$. این‌معادل آن‌است‌که بگوییم تنها مقسوم‌علیه‌های مشترك این دوعدد، یکه‌های ۱ و ۱ — هستند.

اکنون ما برای مراجعات‌آتی برخی ازخواص اصلی بزرگترین مقسوم‌علیه مشترك‌را فهرست می‌کنیم. دربرهان ازموضوع تجزیه به‌عوامل اول استفاده نمی‌شود بلکه‌کاملا مبتنی به‌تعاریف قبلی وتساوی $d = ma + nb$ هستند.

قضیهٔ۵ب. (الف) به‌ازاء هر $a , b , c \in \mathbf{Z}$ ، $(c \geqslant ۰)$ ، $(ac , bc) = (a , b)c$.

(ب) اگر $d = (a , b) \neq ۰$ ، آنگاه $a = da'$ ، $b = db'$ ، که درآن a' و b' متباین‌اند.

(پ) a و b متباین‌اند $\Longleftrightarrow (\exists m , n \in \mathbf{Z})(ma + nb = ۱)$.

(ت) اگر $a \mid bc$ و $(a , b) = ۱$ ، آنگاه $a \mid c$.

(ث) اگر $x \mid z$ ، $y \mid z$ و $(x , y) = ۱$ ، آنگاه $xy \mid z$.

(ج) اگر $a = bq + r$ ، آنگاه $(a , b) = (b , r)$.

برهان. (الف) فرض کنید $d = (a , b)$. دراین‌صورت $d \mid a$ و $d \mid b$ ، ازاینرو $dc \mid ac$ و $dc \mid bc$. ازطرفی d را می‌توان به‌صورت $d = ma + nb$ نوشت، ازاینرو $dc = m(ac) + n(bc)$ برهرمقسوم‌علیه مشترك ac و bc قابل قسمت است. چون $dc \geqslant ۰$ ، این نشان می‌دهد که $dc = (ac , bc)$:

(ب) اگر $d = (a , b) \neq ۰$ آنگاه، چون $d \mid a$ و $d \mid b$ ، می‌توانیم بنویسیم $a = da'$ ، $b = db'$ ، که درآن a' و b' به طور یکتا معین می‌شوند. بنابه قسمت (الف) ، داریم $d = (a , b) = (da' , db') = d(a' , b')$ و چون $d \neq ۰$ ، این نتیجه می‌دهد $(a' , b') = ۱$.

(پ) این قسمت حالت خاصی ازنتیجهٔ قضیهٔ۵آ است. معادلهٔ $ma + nb = ۱$ دارای جوابهای صحیح m ، n است اگروفقط اگر $(a , b) \mid ۱$ ، یعنی اگر وفقط اگر a و b متباین باشند.

(ت) فرض کنید $(a , b) = ۱$ ، دراین‌صورت $n \in \mathbf{Z}$ ، $\exists m$ به‌قسمی که $ma + nb = ۱$. بنابراین $c = mac + nbc$. واضح است که $a \mid mac$ ، حال اگر $a \mid bc$ ، آنگاه $a \mid nbc$ ، وبنابراین $a \mid (mac + nbc) = c$.

(ث) فرض کنید $z = ax$ و $z = by$. اگر $(x , y) = ۱$ آنگاه به‌ازاء اعدادمناسب $m , n \in \mathbf{Z}$ ، داریم $mx + ny = ۱$. بنابراین

$$z = zmx + zny = bymx + axny = (bm + an)xy.$$

(ج) هر مقسوم‌علیه مشترک a و b عدد $r=a-bq$ را عاد می‌کند و از اینرو یک مقسوم علیه مشترک b و r است. به‌همین ترتیب، هر مقسوم‌علیه مشترک b و r یک مقسوم‌علیه مشترک a و b است.

تعریف. عدد صحیح p اول است اگر (الف) هر مقسوم‌علیه p به‌صورت u یا up باشد که در آن u یک یکه است (یعنی $u=\pm 1$)، (ب) خود p یکه نباشد و (پ) $p>0$. این تعریف ممکن است غریب به‌نظر آید، ولی بسادگی دیده می‌شود که با اکثر تعاریف معمولی معادل است. علت بیان تعریف به‌این‌صورت خاص، بعداً، هنگامی که در فصل ۱۰ تجزیهٔ چندجمله‌ایها را مورد بحث قرار می‌دهیم، معلوم خواهد شد.

قضیهٔ ۵پ. (الف) اگر p، q دو عدد اول باشند و $p|q$ آنگاه $p=q$.

(ب) اگر a عددی صحیح و p اول باشد و $p\nmid a$ آنگاه $(p,a)=1$.

(پ) اگر $m>1$ اول نباشد آنگاه $\exists a,b\in\mathbf{Z}$، به‌قسمی که $m=ab$، $1<a<m$ و $1<b<m$.

(ت) اگر p اول باشد و $p|a_1a_2\cdots a_r$، آنگاه به‌ازاء حداقل یک i در حوزهٔ $1\leqslant i\leqslant r$ داریم $p|a_i$.

برهان. (الف) چون p یک مقسوم‌علیه عدد اول q است، بایستی به‌ازاء عدد یکه‌ای مانند u داشته باشیم $p=uq$ یا $p=u$. چون p اول است، حالت $p=u$، بنا به تعریف، درست نیست و چون p و q هر دو مثبت‌اند، نمی‌توانیم داشته باشیم $p=-q$. بنابراین $p=q$.

(ب) فرض کنید $d=(p,a)$. در این صورت $d|p$ و $d|a$. چون $p\nmid a$ نمی‌توانیم داشته باشیم $d=p$ یا $d=-p$. بنابراین d یک عدد یکه است و چون مثبت نیز هست، بایستی مساوی ۱ باشد.

(پ) اگر $m>0$ و اول نباشد آنگاه، بنا به تعریف، یا m یکه است یا m مقسوم‌علیهی دارد که برابر ± 1 یا $\pm m$ نیست. اگر $m>1$، اولین حالت نمی‌تواند برقرار باشد، از اینرو $m=ab$ که در آن $a\neq\pm 1$، $a\neq\pm m$. همچنین، چون داریم $m=(-a)(-b)$ می‌توان فرض کرد که $a>0$ و از اینرو $b>0$. بنابراین $a\geqslant 1$، $b\geqslant 1$ و در نتیجه $m=ab\geqslant b$ و $m=ab\geqslant a$. حال داریم $m=ab$، $1\leqslant a\leqslant m$، $1\leqslant b\leqslant m$. اما $a\neq 1$، $a\neq m$، پس $1<a<m$، و این نتیجه می‌دهد که $1<b<m$.

(ت) این قسمت مهمترین خاصیت اعداد اول است. استقراء را روی r به‌کار می‌بریم. اگر $r=1$، چیزی برای اثبات وجود ندارد. اگر $r>1$ آنگاه $p|aa_r$، که در آن $a=a_1a_2\cdots a_{r-1}$. چنانچه $p|a$، می‌توانیم فرض استقراء را به‌کار بریم و نتیجه بگیریم که به ازاء اندیسی مانند i در حوزهٔ $1\leqslant i\leqslant r-1$، $p|a_i$. از طرف دیگر، اگر $p\nmid a$، آنگاه، بنا به (ب)، $(p,a)=1$. چون $p|aa_r$ می‌توانیم نتیجه بگیریم که در این حالت $p|a_r$

(قضیهٔ۵ب، (ت)) . این مطلب پلهٔ استقراء از $r-1$ به r را کامل می کند، ونتیجه حاصل می‌شود.

اکنون کلیهٔ وسایل ضروری برای اثبات قضیهٔ اصلی این فصل راآماده داریم. این قضیه، گاهی «قضیهٔ اساسی حساب» نامیده می‌شود. اما نام اخباری‌تر آن «قضیهٔ یکتایی تجزیه در $\mathbf{Z}$» است.

قضیهٔ۵ت. (الف)هرعددصحیح غیرصفر n رامی‌توان به‌صورت $n=up_1p_2\cdots p_r$ تجزیه‌کرد، که‌درآن $u=\pm 1$ ، هر p_i یک‌عدد اول‌است، و $r\geqslant 0$.

(ب) اگر $n=vq_1q_2\cdots q_s$ تجزیهٔ دیگری از n باشد، که درآن $v=\pm 1$ ، q_j اول، و $s\geqslant 0$ ، آنگاه $u=v$ ، $r=s$ ، و اعداد اول q_1 ، q_2 ، ... ، q_s جایگشتی از p_1 ، p_2 ، ... ، p_s هستند.

برهان. (الف) چون $n=u|n|$ ، که درآن $u=\pm 1$ ، می‌توان فرض کرد که n مثبت‌است. (تمرین۳ از فصل۳ را برای تعریف وخواص $|n|$ ببینید.) اگر $n=1$، می‌توان $u=1$ و $r=0$ را اختیارکرد، ودراین حالت نتیجه درست است ازاینروکافی است $n>1$ بگیریم ونشان‌دهیم که n حاصلضربی از (یکی یا بیشتر) اعداد اول است. فرض کنیدکه به‌ازاء برخی از اعداد $n>1$ این‌حالت برقرار نباشد. دراین‌صورت به‌وسیلهٔ اصل خوش‌ترتیبی کوچکترین عدد صحیحی چون $m>1$ وجود دارد که نمی‌تواند به‌صورت حاصلضربی از اعداد اول نوشته شود. چون، بالاخص، m اول نیست می‌توانیم قضیهٔ۵پ (پ) را برای به‌دست‌آوردن تجزیه $m=ab$ ، که‌درآن $1<a<m$ ، $1<b<m$ ، به‌کار بریم. اما m کوچکترین‌عدد صحیحی‌است که غیرقابل‌تجزیه به‌عوامل اول است، ازاینرو a و b هردو می‌توانند به‌صورت حاصلضربهایی(یکی‌یا بیشتر) از اعدادا‌ول‌نوشته‌شوند، که‌درآن‌صورت $m=ab$ نیز چنین‌است. این تناقض، حکم را برقرارمی‌کند.

(ب) فرض کنید که $n=up_1p_2\cdots p_r=vq_1q_2\cdots q_s$. اگر $n>0$ آنگاه $u=v=1$ ، واگر $n<0$ آنگاه $u=v=-1$، زیرا همهٔ عوامل اول مثبت‌اند. بنابراین کافی است حالت $n>0$ را درنظر بگیریم. اگر $n=1$، آنگاه چون هیچ عدد اول را عاد نمی‌کند به‌وضوح داریم $r=s=0$. بنابراین می‌توان فرض کرد که $n>1$ و $n=p_1p_2\cdots p_r=q_1q_2\cdots q_s$ (با $r\geqslant 1$ ، $s\geqslant 1$). چون‌ضرب‌اعداد صحیح‌جابجایی و شرکت‌پذیراست می‌توان‌فرض کردکه عوامل اول به‌قسمی‌جابجا شده‌اندکه‌به‌ترتیب‌صعودی $p_1\leqslant p_2\leqslant\cdots\leqslant p_r$ و $q_1\leqslant q_2\leqslant\cdots\leqslant q_s$ مرتب شده‌اند. دراین‌صورت‌ثابت‌خواهیم کردکه $r=s$ وبه‌ازاء $i=1,2,\ldots,r$ ، $p_i=q_i$. زیرا، فرض کنید این حکم به‌ازاء عدد صحیحی چون $n>1$ درست نباشد؛ آنگاه کوچکترین عددصحیحی چون $n>1$ وجود داردکه دارای دوتجزیه به‌عوامل اول‌متفاوت است $n=p_1p_2\cdots p_r=q_1q_2\cdots q_s$ باشرط اینکه $p_1\leqslant p_2\leqslant\cdots\leqslant p_r$ و $q_1\leqslant q_2\leqslant\cdots\leqslant q_s$. کوچکترین‌عدداولی که‌دراین دوتجزیه

وجود دارد یا p_1 است یا q_1 ، ومی‌توان، بدون‌اینکه به‌کلیت خللی واردآید، فرض کرد که p_1 کوچکترین است. درآن صورت $p_1 | n = q_1 q_2 \cdots q_s$ ، از اینرو بنا به قضیهٔ ۵پ (ت)، به‌ازاء اندیسی‌چون i، داریم $p_1 | q_i$، وچون p_1 و q_i هردو اول‌اند نتیجه‌می‌شود که $p_1 = q_i$ (قضیهٔ۵پ (الف) را ببینید). اما p_1 کوچکترین عامل‌ازعوامل‌اول است، ازاینرو بایدداشته باشیم $p_1 = q_1$. حال بقیهٔ برهان ساده است . بایستی حداقل یك عامل دیگر در هر حاصلضرب داشته باشیم (زیرا تجزیه‌ها متفاوت‌اند) و با قانون حذف به‌دست می‌آوریم $p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s = n'$، بافرض $1 < n' < n$. دراین‌صورت‌عددصحیح کوچکتری بادوتجزیه متفاوت پیدا کرده‌ایم، که نحوهٔ انتخاب n را نقض می‌کند، وبرهان کامل می‌شود.

حال به‌مسئلهٔ محاسبهٔ بزرگترین مقسوم‌علیه مشترك برمی‌گردیم. براساس قضیهٔ یکتایی تجزیه، توجیه‌روش معمولی، که درآن تجزیه‌های عوامل اول‌اعداد به‌دست‌می‌آید وبالاترین توانها از عوامل اولی که هردو را عاد می‌کنند گردآوری می‌شود ، کار ساده‌ای است . به‌هرحال، مطمئناً این ساده‌ترین روش نیست، مگر درمورد اعدادکوچك‌که عوامل اولشان را بلافاصله می‌توان نوشت. الگوریتم اقلیدس خیلی ساده‌تر است وبنابراین ارزش مطالعهٔ دقیق را دارد.

فرض کنیم که‌می‌خواهیم (a, b) را برای‌دوعددصحیح‌مفروض a و b پیدا کنیم. چون

$$(a, b) = (b, a) \text{ ، } (a, a) = a \text{ ، } (a, 0) = 0$$

$$\text{و } (a, b) = (-a, b) = (a, -b) = (-a, -b) \text{ ،}$$

فقط نیاز داریم به‌حالت $a > b > 0$ بپردازیم. بنابه قضیهٔ۳پ، اعداد صحیح r, q به قسمی وجود دارندکه $a = bq + r$ $0 \leqslant r < b$؛ برای پیداکردن آنها a را بر b تقسیم کرده وبه خارج‌قسمت‌وباقیمانده توجه‌می‌کنیم. حال‌قضیهٔ۵ب (ج) به‌مامی‌گویدکه $(a, b) = (b, r)$، ازاینرو محاسبه را به‌پیدا کردن (b, r)، زوج کوچکتری از اعداد صحیح (غیرمنفی) تحویل کرده‌ایم. باتکرار این روش سرانجام جواب به‌دست خواهد آمد.

مثال۱۰۵. $(۱۳۲۰, ۷۱۴) = (۷۱۴, ۶۰۶) = (۶۰۶, ۱۰۸) = (۱۰۸, ۶۶)$

$$= (۶۶, ۴۲) = (۴۲, ۲۴) = (۲۴, ۱۸) = (۱۸, ۶) = ۶ .$$

برای‌توصیف دقیقتر الگوریتم، نمادهای زیررا معرفی می‌کنیم. فرض کنید $a = a_0$ ، $b = a_1$ وفرض کنید q_1 ، a_2 اعداد صحیح باشندکه به‌طور یکتایی معین شده‌اند به‌قسمی که $a_0 = a_1 q_1 + a_2$، و $0 \leqslant a_2 < a_1$. سپس q_n ، a_n را به‌طریق‌استقراء به‌صورت‌زیر تعریف می‌کنیم : اگر $a_n > 0$ آنگاه q_n و a_{n+1} اعداد صحیح یکتایی هستند به‌قسمی که $a_{n-1} = a_n q_n + a_{n+1}$ و $0 \leqslant a_{n+1} < a_n$؛ اگر $a_n = 0$، الگوریتم‌خاتمه می‌یابد. چون $a_1 > a_2 > a_3 > \cdots \geqslant 0$ ، نمی‌توانیم به‌ازاء همهٔ nها داشته باشیم $a_n > 0$ ، ازاینرو الگوریتم همواره متناهی است (باحداکثر b پله)، ومجموعه‌ای از تساویها، به‌صورت زیر به‌دست می‌آوریم:

$$a_0 = a_1 q_1 + a_2 ,$$
$$a_1 = a_2 q_2 + a_3 ,$$
$$\vdots$$
$$a_{r-3} = a_{r-2} q_{r-2} + a_{r-1} ,$$
$$a_{r-2} = a_{r-1} q_{r-1} + a_r ,$$
$$a_{r-1} = a_r q_r ,$$

که در آن a_{r+1} اولین aای است که مقدارش ۰ است. در این نماد، بزرگترین مقسوم‌علیه مشترک a و b آخرین باقیماندهٔ غیر صفر a_r است، زیرا

$$d = (a, b) = (a_0, a_1) = (a_1, a_2) = (a_2, a_3) = \cdots = (a_r, a_{r+1}) = (a_r, 0) = a_r .$$

خاصیت نوشتن تساویها به این طریق آن است که اکنون آنها می‌توانند برای بیان d به‌صورت $am + bn$ به کار گرفته شوند. از تساوی ماقبل آخر داریم $d = a_r = a_{r-2} - a_{r-1} q_{r-1}$. اگر در این تساوی مقدار $a_{r-1} = a_{r-3} - a_{r-2} q_{r-2}$ را، که از تساوی بعدی به سمت بالا به‌دست آمده است، جانشین کنیم، درمی‌یابیم که d به‌صورت $d = a_{r-3} s + a_{r-2} t$ بیان شده است. به‌این طریق عمل می‌کنیم تا به اولین تساوی برسیم، سرانجام تساوی‌ای به‌صورت $d = a_0 m + a_1 n = am + bn$ به‌دست می‌آوریم.

مثال ۲.۵. فرض کنید $a = ۹۷۵$ ، $b = ۶۱۶$. در این‌صورت محاسبات به‌صورت‌زیر است:

$$۹۷۵ = ۶۱۶ \times ۱ + ۳۵۹ ,$$
$$۶۱۶ = ۳۵۹ \times ۱ + ۲۵۷ ,$$
$$۳۵۹ = ۲۵۷ \times ۱ + ۱۰۲ ,$$
$$۲۵۷ = ۱۰۲ \times ۲ + ۵۳ ,$$
$$۱۰۲ = ۵۳ \times ۱ + ۴۹ ,$$
$$۵۳ = ۴۹ \times ۱ + ۴ ,$$
$$۴۹ = ۴ \times ۱۲ + ۱$$

بنابراین $(a, b) = ۱$ و ، با تعقیب روشی که درفوق توضیح داده شده، به‌دست می‌آوریم:

$$\begin{aligned} ۱ &= ۴۹ + ۴(-۱۲) \\ &= ۵۳(-۱۲) + ۴۹ \times ۱۳ \\ &= ۱۰۲ \times ۱۳ + ۵۳(-۲۵) \\ &= ۲۵۷(-۲۵) + ۱۰۲ \times ۶۳ \end{aligned}$$

$$= ۳۵۹ \times ۶۳ + ۲۵۷(-۸۸)$$
$$= ۶۱۶(-۸۸) + ۳۵۹ \times ۱۵۱$$
$$= ۹۷۵ \times ۱۵۱ + ۶۱۶(-۲۳۹).$$

مشکل بتوان بزرگترین مقسوم‌علیه مشترك a و b را با آزمایش و خطا تعیین کرد[1]؛ (البته ممکن است این روش راه‌حل کوتاهتری به‌دست دهد).

با قدری پیراستن قضیهٔ۳پ ، الگوریتم اقلیدس می‌تواند تسریع شود. اگر a و b مفروض باشند، به مضربی از b که اختلافش با a در مقدارقدر مطلق کوچکترین است، توجه می‌کنیم، تساوی $a = bq + r$ با $|r| \leqslant \frac{1}{2}b$ به‌دست می‌آید. چون $(a,b) = (b,r) = (b,|r|)$، این‌صورت دیگرحداقل به‌همان خوبی‌قبلی است و الگوریتم باید حداکثر پس‌ازn پله‌خاتمه یابد که دراینجا $b < 2^n$. این‌الگوریتم پیراسته‌نیز می‌تواند برای‌حل‌معادلهٔ $d = am + bn$ به‌کار رود.

مثال۳.۵. فرض کنید $a = ۱۳۲۰$ ، $b = ۷۱۴$ ، همانند مثال ۱.۵ باشند. دراین‌صورت

$$۱۳۲۰ = ۷۱۴ \times ۲ - ۱۰۸ ,$$
$$۷۱۴ = ۱۰۸ \times ۷ - ۴۲ ,$$
$$۱۰۸ = ۴۲ \times ۳ - ۱۸$$
$$۴۲ = ۱۸ \times ۲ + ۶ ,$$
$$۱۸ = ۶ \times ۳.$$

بنابراین بزرگترین مقسوم‌علیه مشترك a و b عدد ۶ است، و داریم

$$۶ = ۴۲ + ۱۸(-۲)$$
$$= ۱۰۸ \times ۲ + ۴۲(-۵)$$
$$= ۷۱۴ \times ۵ + ۱۰۸(-۳۳)$$
$$= ۱۳۲۰ \times ۳۳ + ۷۱۴(-۶۱).$$

---

۱. غیراز «روش» آزمایش و خطا و روش ارائه شده درفوق، راه دیگر یافتن ضرایب a و b ، استفاده از روش حل معادلهٔ سیالهٔ $ax + by = d$ است.ـم

مقایسهٔ این روش با کاربرد کاملا متفاوتی از الگوریتم اقلیدس درمورد اعداد حقیقی وتقریبشان به‌وسیلهٔ اعداد گویا، جالب است. (این مطلب، استطرادی است ودانشجویانی که مایل‌اند به موضوع اصلی برگردند، می‌توانند از آن بگذرند.) محتمل است که الگوریتم اقلیدس برای اولین‌مرتبه درزمینهٔ هندسه رخ داده‌باشد. هندسه‌دانان یونانی زمان‌قدیم، فرض می‌کردند که هردوقطعه خط متوافق‌اند، یعنی هردومضارب صحیح ازیك قطعه‌خط کوچکتری هستند، که می‌توان آن‌را به‌عنوان یك «مقسوم‌علیه‌مشترك» آنها تصور کرد. به‌منظور پیدا کردن چنین اندازهٔ مشترکی برای دوقطعه خط a و b که b کوتاهتر است، b را هرچند دفعه‌یی که ممکن باشد درامتداد a قرار دهید. اگر a به‌این‌ترتیب دقیقاً وکاملا پوشانده‌شد، آنگاه b یك‌اندازهٔ مشترك است. درغیراین‌صورت، قطعهٔ r_1 که از a «بیرون زده است» از b کوتاهتر خواهد بود، و روشن است که، هراندازهٔ مشترك r_1 و b قطعه خط a رانیز دقیقاً اندازه می‌گیرد، ازاینرو این‌فرایند را با b و r_1 تکرارکنید. اگر r_1 قطعه خط b را دقیقاً اندازه بگیرد، درآن‌صورت یك‌اندازهٔ مشترك a و b است. درصورتی که چنین نباشد قطعهٔ باقیماندهٔ r_2 از r_1 کوتاهتر است. بنابراین قطعات کوتاهتروکوتاهتر r_1، r_2، ...، به‌دست می‌آیند،واشتباهی که توسط هندسه‌دانان‌قدیم‌صورت‌می‌گرفت‌آن‌بودکه تصورمی‌کردند این فرایند بایستی پس‌از تعداد متناهی دفعه خاتمه‌یابد.

درنمادگذاری جدید طولهای قطعه خطها اعدادحقیقی a و b هستند و ، با قراردادن $a_0 = a$ ، $a_1 = b$ ، می‌توان a_n و q_n را به‌طور استقرائی به‌وسیلهٔ قاعدهٔ زیر تعریف کرد: اگر $a_n \neq 0$ آنگاه q_n بزرگترین عدد صحیح است به قسمی که $a_n q_n \leqslant a_{n-1}$ ، و $a_{n+1} = a_{n-1} - a_n q_n$. بنابراین همان رشته تساویهای قبلی را داریم

$$a_0 = a_1 q_1 + a_2 ,$$
$$a_1 = a_2 q_2 + a_3 ,$$
$$\vdots$$

باتفاوت‌اینکه $a_n \in \mathbf{R}$ ، $q_n \in \mathbf{Z}$ ، $a_{n+1} < a_n \geqslant 0$ و رشته‌تساویهاممکن‌است به‌طورنامتناهی وبدون اینکه a_n صفر گردد، ادامه پیداکند. درواقع الگوریتم پس‌از تعداد متناهی پله‌خاتمه می‌یابد اگروفقط‌اگر a و b متوافق باشند. (تمرین: این مطلب را ثابت‌کنید!). شگفت‌آور است‌که حتی وقتی الگوریتم‌خاتمه نمی‌یابد بی‌فایده نیست: این الگوریتم می‌خواهداندازهٔ مشترکی بین a و b پیداکند، وبنابراین عملا یك سری از اعداد گویا به‌ما می‌دهدکه مرتباً به a/b نزدیك ونزدیکترمی‌شوند. اگر برآوردی ازکارآیی الگوریتم انجام‌گیرد، می‌توان قضیهٔ زیر را درمورد تقریب‌زدن اعداد حقیقی به‌وسیلهٔ اعداد گویا ثابت‌کرد. برای هرعدد حقیقی مفروض x وهر $\varepsilon > 0$ مفروض، اعداد صحیح p ، q وجود دارند به‌قسمی‌که $q > 0$ و

$$\left| x - \frac{p}{q} \right| < \frac{\varepsilon}{q}$$

برای اثبات این قضیه، قرار می‌دهیم $a = x$ و $b = 1$ و الگوریتم اقلیدس را درآن حالت

کارآمدتر انجام می‌دهیم، یعنی حالتی که $a_{n-1}=a_nq_n+a_{n+1}$ و

$$|a_{n+1}|\leqslant\frac{1}{2}|a_n|$$

(کافی است نزدیکترین مضرب صحیح a_n به a_{n-1} را برگزینیم). آنگاه به وضوح داریم

$$|a_n|\leqslant\frac{1}{2^{n-1}}$$

وبنابراین می‌توان $n>1$ را به‌قسمی انتخاب کرد که $|a_n|<\varepsilon$. حال، دقیقاً همانند حالت صحیح ، a_n می‌تواند به‌صورت $a_n=a_0r+a_1s$ بیان‌شود که در آن r و s اعدادصحیح‌اند. بنابراین $a_n=xr+s$ ، و از اینرو $|xr+s|<\varepsilon$. می‌توانیم فرض کنیم که $r\neq0$ (چون اگر $r=0$، آنگاه a_n یك عددصحیح است وازاینرو بایستی‌صفر باشد؛ دراین‌حالت x عددی گویاست و قضیه به‌طور بدیهی برقرار است). ازتقسیم بر $|r|$ ، به‌دست می‌آوریم:

$$\left|x+\frac{s}{r}\right|<\frac{\varepsilon}{|r|}$$

وبرای اثبات‌قضیه، می‌توان قرارداد: $q=|r|$ و $p=\pm s$.

توجه. این قضیه‌نیزمی‌تواند بااستفاده ازنظریهٔ گروهها شبیه به‌آنچه‌که برای قضیهٔ ۵ آ به‌کار برده شد ثابت شود. (تمرین۱۴ زیررا ببینید.)

تمرینها

۱. بزرگترین‌مقسوم‌علیه‌مشترك ۱۸۰ و ۲۵۲ را پیدا کنید، وآن‌را به‌صورت $180x+252y$، که در آن $x\,,\,y\in\mathbf{Z}$ ، بیان کنید.

۲. یك جواب‌صحیح ازمعادلهٔ $686y=70$ $966x+$ را پیدا کنید.

۳. ثابت کنید که اگر $x\,,\,y\,,\,u\,,\,v\in\mathbf{Z}$ و $xy|uv$ ، آنگاه $(x\,,\,u)y|u(y\,,\,v)$. (سعی کنید که این‌را بدون استفاده ازقضیهٔ یکتایی تجزیه انجام دهید.)

۴. فرض کنید $a\,,\,b\,,\,c$ اعداد صحیحی باشند به‌قسمی که $ab=c^2$. ثابت کنید که اگر $(a\,,\,b)=1$، آنگاه هردوعدد a و b مربع‌کامل (از اعداد صحیح) هستند.

۵. ثابت کنید که به‌ازاء همهٔ‌اعداد صحیح $a\,,\,b\,,\,c$ داریم $((a\,,\,b)\,,\,c)=(a,(b\,,\,c))$.

۶. گزارهٔ $(\forall a\,,\,b\,,\,c\in\mathbf{Z})((ab\,,\,c)=(a\,,\,c)(b\,,\,c))$ درست‌است یا غلط؟

۷. ثابت کنید (بدون استفاده ازقضیهٔ یکتایی تجزیه) که اگر $a|bc$ ، آنگاه اعدادصحیح x و y وجود دارند به‌قسمی که $y|c$ ، $x|b$ و $a=xy$.

۸. فرض کنید m ، n_1 ، n_2 ، ... ، n_r اعداد صحیحی باشند به‌قسمی که به ازاء $i = 1, 2, \dots, r$ داشته باشیم $(m, n_i) = 1$. ثابت کنید که $(m, n) = 1$، که در آن $n = n_1 n_2 \cdots n_r$.

(راهنمایی: اگر $(a, b) \neq 1$ آنگاه a و b دارای یک مقسوم‌علیه مشترک اول‌اند.)

۹. ثابت کنید که اگر به‌ازاء عدد صحیحی چون $n > 0$، داشته باشیم $q \in \mathbf{Q}$ و $q^n \in \mathbf{Z}$، آنگاه $q \in \mathbf{Z}$. نتیجه بگیرید که اگر p عددی اول باشد، آنگاه به‌ازاء هر $n \geqslant 2$، عدد $p^{\frac{1}{n}}$ اصم است.

۱۰. فرض کنید $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$، $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$، که در آنها p_1 ، ... ، p_n اعداد اول متمایزند، $n \geqslant 1$، و $\alpha_i \geqslant 0$، $\beta_i \geqslant 0$ اعداد صحیح‌اند. ثابت کنید که $a \mid b$ اگر و فقط اگر به‌ازاء $i = 1, 2, \dots, n$، $\alpha_i \leqslant \beta_i$. دستوری برای تعداد مقسوم‌علیه‌های مثبت متمایز $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ پیدا کنید.

۱۱. فرض کنید n عدد صحیح مثبتی فاقد عامل مربع باشد (یعنی، n بر مربع هیچ عدد اولی قابل قسمت نباشد)، همچنین فرض کنید که، به‌ازاء همهٔ اعداد اول p، $p \mid n \iff (p-1) \mid n$. ثابت کنید که در این صورت $n = 1806$.

۱۲. (الف) آیا هر زیر گروه جمعی $\mathbf{Q}$ دوری است؟ (ب) آیا هر زیر گروه جمعی $\mathbf{Q}$، به‌ازاء عددی چون $d \in \mathbf{Q}$، به‌صورت $H = \mathbf{Q}d = \{qd \; ; \; q \in \mathbf{Q}\}$ هست؟

۱۳. ثابت کنید که $\mathbf{Z}$ شامل تعداد نامتناهی اعداد اول متمایز است. (راهنمایی: فرض کنید که p_1 ، p_2 ، ... ، p_n همهٔ اعداد اول متمایز باشند و با در نظر گرفتن تجزیه به‌عوامل اول عدد $p_1 p_2 \cdots p_n + 1$ به تناقض برسید.)

۱۴. (مشکلتر) فرض کنید G یک زیر گروه جمعی از $\mathbf{R}$ باشد. ثابت کنید که یا (الف) G دوری است، یا (ب) G شامل عناصر غیر صفر کوچک دلخواه می‌باشد. (راهنمایی: G یا شامل کوچکترین عضو مثبت است یا خیر.)

اگر x عددی حقیقی باشد، نشان دهید که $G = \{xm + n \; ; \; m, n \in \mathbf{Z}\}$ یک زیر-گروه جمعی $\mathbf{R}$ است. نشان دهید که G دوری است اگر و فقط اگر x گویا باشد. از اینجا نتیجه بگیرید که به‌ازاء هر عدد اصم x و هر $\varepsilon > 0$ اعداد صحیح p ، q وجود دارند به قسمی که $q > 0$ و

$$\left| x - \frac{p}{q} \right| < \frac{\varepsilon}{q}$$

۱۵. (مشکلتر) ثابت کنید احتمال اینکه دو عدد صحیح مثبت که به‌طور تصادفی انتخاب شده‌اند متباین باشند، برابر است با ... ۶۰۷۶ $= 6/\pi^2$.

(چند تبصره: احتمال بدین طریق تعریف می‌شود که اولا احتمال برای جفتی از اعداد صحیح که از N بزرگتر نیستند، محاسبه شود و سپس N به بینهایت میل داده شود.

اثبات دقیق این حکم مشکل است، اما با بررسی احتمال اینکه دوعـدد صحیح مثبت هردو برعدد اول مفروضی قابل‌قسمت باشند، استدلال نسبتاً متقاعدکننده‌ای می‌تواند به‌دست‌آید. دراین استدلال، لازم است بدانید که $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.)

فصل ۶

ساختن گروههای جدید به کمک گروههای مفروض

تاکنون، گروهها را فقط درنقش توصیفی به‌کار برده‌ایم، و صرفاً زبان جدیدی برای بحث دربارهٔ اوضاع آشنا معرفی کرده‌ایم، هدف عمدهٔ ما وحدت بخشیدن به‌ایده‌های متفرق بوده است. معهذا تبلور ایدهٔ مجرد گروه راه‌گشای امکان جدیدی است. درواقع، به‌جای اینکه دراطراف خود به‌اشیاء ریاضی نظر بیفکنیم و به‌امید یافتن گروههای بیشتری باشیم که روی آنها روشهای جدید را امتحان کنیم. قادریم گروههای جدیدی بسازیم که آنها را قبلا هرگز ندیده‌ایم. دراین فصل دوساختمان ازاین نوع را توضیح می‌دهیم (حاصلضرب گروهها و گروههای خارج قسمت) که درآنها، به‌وسیلهٔ عملیات کاملا مجرد، از گروه یا گروههای مفروض، گروه جدیدی به‌دست می‌آید. گاهی گروه ساخته شده با گروه معروفی یکریخت خواهد بود، ولی گاهی‌هم حقیقتاً جدید است. فایدهٔ ساختن چنین گروههایی آن است که می‌توانیم همهٔ قضایایی که درمورد گروهها ثابت کرده‌ایم بلافاصله برای آنها به‌کار گیریم، وچون گروههای جدید رابطهٔ نزدیکی با گروههایی دارند که از روی آنها ساخته شده‌اند، غالباً می‌توانیم حقایقی دربارهٔ گروههای اصلی نتیجه بگیریم که استنتاج آنها با روشهای دیگر مشکلتر است. اگر در وهلهٔ اول، ساختمانها خیلی مجرد وازنظر مفهوم مشکل به‌نظر آیند، بایستی دانشجو پشتکار داشته باشد تا به‌آنها تسلط پیدا کند. درفصلهای آتی خواهید دید که سعی شما کاملا ثمربخش است.

بین این دوساختمان، ضرب ساده‌تر است. یادآور می‌شویم که اگر A و B دومجموعه باشند آنگاه اعضای مجموعهٔ حاصلضرب $A \times B$ همهٔ جفتهای مرتب $(a\ ;\ b)$ هستند، که درآن $a \in A$ و $b \in B$. اگر A و B گروه باشند، آنگاه مجموعهٔ $A \times B$ به‌طریق طبیعی دارای ساخت گروهی است. هردوگروه را به‌طور ضربی می‌نویسیم وباقاعدهٔ زیر ضربی روی $A \times B$ تعریف می‌کنیم:

$$(a\,,\,b)\cdot(a'\,,\,b')=(aa'\,,\,bb').$$

چون $a\,,\,a'\in A$ و $b\,,\,b'\in B$ داریم $(aa'\,,\,bb')\in A\times B$، ازاینرو این ضرب عملی دوتایی روی $A\times B$ است و واضح است که شرکت‌پذیر می‌باشد، زیرا ضربهای گروه در A و B هردو شرکت‌پذیرند. (برهان کاملی ازقانون شرکت‌پذیری در $A\times B$ بنویسید.) اگر عناصر خنثای A و B را با e_A و e_B نشان دهیم، آنگاه $(e_A\,,\,e_B)\cdot(a\,,\,b)=(e_Aa\,,\,e_Bb)=(a\,,\,b)$، و به‌همین ترتیب $(a\,,\,b)\cdot(e_A\,,\,e_B)=(a\,,\,b)$، ازاینرو $(e_A\,,\,e_B)$ به‌عنوان عنصر خنثای $A\times B$ عمل می‌کند. بالاخره، اگر a^{-1} و b^{-1} به‌ترتیب معکوسهای a و b در A و B باشند، آنگاه

$$(a\,,\,b)\cdot(a^{-1}\,,\,b^{-1})=(a^{-1}\,,\,b^{-1})\cdot(a\,,\,b)=(e_A\,,\,e_B)\,,$$

که حاصل همان عنصر خنثای $A\times B$ است. بنابراین هرعنصر $(a\,,\,b)$ دارای معکوسی در $A\times B$ می‌باشد، وهمان‌طور که ادعا شد $A\times B$ یك گروه است. معمولا درنوشتن عنصر خنثی به‌صورت $(e\,,\,e)$ اشکالی به‌وجود نمی‌آید. اگر A و B به‌طورجمعی نوشته شده باشند، معمول است که $A\times B$ نیز به‌طور جمعی نوشته شود. دراین‌حالت

$$-(a\,,\,b)=(-a\,,\,-b)\,,\quad (a\,,\,b)+(a'\,,\,b')=(a+a'\,,\,b+b')$$

وعنصرخنثی $(0\,,\,0)$ است.

این ساختمان می‌تواند به‌هر تعداد از عوامل توسعه‌داده شود. اگر A_1، A_2، ...، A_n، گروههای ضربی باشند آنگاه اعضای مجموعهٔ $A_1\times A_2\times\cdots\times A_n$ همهٔ n تاییهای $(a_1\,,\,a_2\,,\,\ldots\,,\,a_n)$ هستند، که درآن $a_i\in A_i$ وضرب nتاییهارا بوسیلهٔ

$$(a_1\,,\,a_2\,,\,\ldots\,,\,a_n)\cdot(a'_1\,,\,a'_2\,,\,\ldots\,,\,a'_n)=(a_1a'_1\,,\,a_2a'_2\,,\,\ldots\,,\,a_na'_n)$$

تعریف می‌کنیم. استدلالهای مشابه نشان می‌دهد که $A_1\times A_2\times\cdots\times A_n$ یك گروه است. حاصلضربهای گروهها شرکت‌پذیرند، به مفهوم اینکه گروههای $A\times(B\times C)$، $(A\times B)\times C$ و $A\times B\times C$ جملگی به‌وسیلهٔ نگاشتهای بدیهی یکریخت‌اند، و بنابراین مابین آنها فرقی قائل نمی‌شویم.

مثال ۱.۶. فرض کنید $A=B=\mathbf{R}$، گروه جمعی اعداد حقیقی باشد. دراین صورت $\mathbf{R}^2=\mathbf{R}\times\mathbf{R}$ گروهی جمعی است که به‌ازاء اعداد حقیقی x، y، x' و y' داریم $(x\,,\,y)+(x'\,,\,y')=(x+x'\,,\,y+y')$. (این جمع گاهی به‌جمع برداری معروف است.) بدیهی است که این گروه با گروه جمعی $\mathbf{C}$ یکریخت است. در واقع یك روش تعریف $\mathbf{C}$ آن است که بگوییم $\mathbf{C}$ مجموعهٔ همهٔ جفتهای اعداد حقیقی است، باجمعی که درفوق تعریف شده است[1]. به‌همین ترتیب $\mathbf{R}^n=\mathbf{R}\times\mathbf{R}\times\cdots\times\mathbf{R}$ (n عامل) یك گروه جمعی است.

مثال ۲.۶. گروه ضربی $\mathbf{R}^*$ دارای دو زیرگروه $\mathbf{R}^+$ و $\{+1\,,\,-1\}$ است به‌طوری که هرعنصر

۱. وضربی که به‌گونه‌ای دیگر تعریف می‌شود.ـم.

$x \in \mathbf{R}^*$ به‌عنوان حاصلضرب عضوی از $\mathbf{R}^+$ و عضوی از $\{\pm 1\}$ به‌طور یکتایی قابل بیان است، یعنی

$$x = |x| \text{sign}(x) \text{ ، که در آن } \text{sign}(x) = \frac{x}{|x|} .$$

بنابراین نگاشتی دوسویی $\mathbf{R}^* \longrightarrow \mathbf{R}^+ \times \{\pm 1\}$ با ضابطهٔ $x \longmapsto (|x| \text{ ، } \text{sign}(x))$ داریم و بسادگی دیده می‌شود که این یك یکریختی گروههاست، به‌این‌دلیل که:

$$xx' \longmapsto (|xx'| \text{ ، } \text{sign}(xx')) = (|x|\,|x'| \text{ ، } \text{sign}(x)\,\text{sign}(x'))$$
$$= (|x| \text{ ، } \text{sign}(x)) \cdot (|x'| \text{ ، } \text{sign}(x')) .$$

مثال ۳.۶. استدلالی مشابه نشان می‌دهد

$$\mathbf{C}^* \cong \mathbf{R}^+ \times T ,$$

که در آن T گروه دایره‌ای است. یکریختی لازم، با در نظر گرفتن مختصات قطبی اعداد مختلط غیرصفر به‌دست می‌آید.

قضیهٔ ۶ آ. (الف) اگر A و B **گروههای** آبلی باشند، آنگاه $A \times B$ نیز آبلی است.

(ب) اگر A و B گروههای متناهی به‌ترتیب از مرتبهٔ m و n باشند، آنگاه $A \times B$ گروهی متناهی از مرتبهٔ mn است.

(پ) اگر A' و B' به‌ترتیب زیرگروههای A و B باشند، آنگاه $A' \times B'$ **زیرگروهی** از $A \times B$ است.

برهان. (الف) اگر A و B آبلی باشند آنگاه

$$(a \text{ ، } b) \cdot (a' \text{ ، } b') = (aa' \text{ ، } bb') = (a'a \text{ ، } b'b) = (a' \text{ ، } b') \cdot (a \text{ ، } b).$$

(ب) تعداد انتخابهای مختلف یك عنصر $a \in A$ و یك عنصر $b \in B$ برابر است با mn.

(پ) $A' \times B'$ زیرمجموعه‌ای از $A \times B$ است و شامل $(e \text{ ، } e)$ می‌باشد. اگر $(a_1, b_1) \text{ ، } (a_2, b_2) \in A' \times B'$ آنگاه $(a_1 a_2 \text{ ، } b_1 b_2) \in A' \times B'$ و $(a_1^{-1} \text{ ، } b_1^{-1}) \in A' \times B'$.

مثال ۴.۶. $\mathbf{Z}$ یك زیرگروه جمعی $\mathbf{R}$ است، بنابراین $\mathbf{Z}^2 = \mathbf{Z} \times \mathbf{Z}$ زیرگروهی از $\mathbf{R}^2$ است. این زیرگروه متشکل است از همهٔ نقاط درصفحه با مختصات صحیح. اگر آن را به‌عنوان زیرگروهی از $\mathbf{C} \cong \mathbf{R}^2$ در نظر بگیریم، شامل همهٔ اعداد مختلط $a + ib$ است که در آن $a \text{ ، } b \in \mathbf{Z}$. این اعداد مختلط به اعداد صحیح گاوسی[1] معروف‌اند.

1. Gaussian integers

قضیهٔ ۶ب. فرض‌کنید A ، B گروههای دوری به‌ترتیب از مرتبهٔ m ، n باشند ، که m و n متباین‌اند . دراین صورت گروه $C=A\times B$ دوری و از مرتبهٔ mn است. عنصر $c=(a\,,\,b)$ مولدی از C است اگر وفقط‌اگر a مولدی از A و b مولدی از B باشد.

برهان. یقیناً C دارای مرتبهٔ mnاست، ازاینرو به‌منظور نشان دادن اینکه C دوری است‌کافی است عنصری مانند $c=(a\,,\,b)$ از مرتبهٔ mn پیدا کنید. فرض کنید a ، b مولدهای A ، B باشند. دراین‌صورت a دارای مرتبهٔ m و b دارای مرتبهٔ n است. اگر $c=(a\,,\,b)$ دارای مرتبهٔ r باشد، آنگاه $(a\,,\,b)^r=(e\,,\,e)$ ، یعنی $a^r=e$ و $b^r=e$، ازاینرو $m|r$ و $n|r$ (قضیهٔ ۴ت‌را ببینید). اما m و n متباین‌اند، ازاینرو، بنا به‌قضیهٔ ۵ب(ث)، داریم $mn|r$. ولی r از mn نمی‌تواند تجاوز کند، پس $r=mn$ و بنابراین c گروه C را تولید می‌کند. بعکس، اگر $a\in A$ ، $b\in B$ و چنانچه $c=(a\,,\,b)$ گروه C را تولید کند، آنگاه هر عنصر $A\times B$ باید، به‌ازاء عددی چون $k\in\mathbf{Z}$، به‌صورت $c^k=(a^k\,,\,b^k)$ باشد، وازاینجا نتیجه‌می‌شود که a گروه A و b گروه B را تولید می‌کند.

مثال ۵.۶. درحالت کلی اینکه حاصلضرب گروههای دوری یك‌گروه دوری است، صحیح نمی‌باشد. به‌عنوان‌مثال، $\mathbf{Z}\times\mathbf{Z}$ دوری نیست، زیرا توانهای جمعی یك‌عنصرمفروض$(r\,,\,s)$ عناصر $(nr\,,\,ns)$ هستند وقتی که n متغیر باشد، واعداد صحیح nr و ns ، به‌ازاء همهٔ این توانها، دارای یك نسبت‌اند. $\mathbf{Z}\times\mathbf{Z}$ ازنظرهندسی، گروه‌نقاط درصفحه بامختصات صحیح است ومجموعه‌های نقاط با مختصات صحیح واقع برخطوط مستقیمی که ازمبدأ می گذرند، زیرگروههای دوری‌آن می‌باشند. درجای مناسب، خواننده نمونه‌هایی ازاین زیرگروهها را خواهد دید. مثال دیگر، حاصلضرب $A\times B$ ازدوگروه دوری ازمرتبهٔ ۲ است. دراین گروه $(a\,,\,b)^2=(a^2\,,\,b^2)=(e\,,\,e)$ ، ازاینروهرعنصر دارای‌مرتبهٔ ۱یا۲ است، وهیچ عنصری ازمرتبهٔ۴ وجود ندارد که گروه را تولیدکند. این گروه به ۴ـ گروه کلاین[1] معروف‌است.

ساختمان گروههای‌خارج‌قسمت دشوارتراست. با گروهی مانندG ویك مجموعهٔ‌خارج قسمت از G آغاز می‌کنیم. آنگاه سعی‌می‌کنیم ساخت‌گروه G را برای تعریف یك‌ساخت گروهی‌روی‌مجموعهٔ خارج‌قسمت به‌کار بریم. این‌کار راهمیشه نمی‌توان انجام‌داد، ازاینرو وبه‌منظور تحلیل این وضعیت، ابتدا به‌بررسی کلی اعمال روی مجموعه‌هـای خارج قسمت می‌پردازیم.

فرض‌کنیدS یك مجموعه و $\sim$ یك‌رابطهٔ هم‌ارزی رویS باشد. رده‌های هم‌ارزی$\sim$ عناصرمجموعهٔ خارج‌قسمت $S/\sim$ است، ونماد $\langle x\rangle$ را برای‌ردهٔ هم‌ارزی‌شاملx به‌کار می‌بریم. درآن‌صورت $x\sim y\iff\langle x\rangle=\langle y\rangle$. حال فرض‌کنید‌که عملی روی S مفروض باشد؛ به‌خاطر مشخص بودن‌مطالبی که فعلا می‌خواهیم بگوییم، فرض‌می‌کنیم که‌این‌عمل،

---

1. Klein

یک عمل دوتایی * است، ولی برای هر عمل، اصل مطلب تفاوتی نمی‌کند. برای تعریف عملی متناظر روی $S/\sim$، که آن‌را با همان * نشان می‌دهیم، تعریف باید به گونه‌ای باشد که به ازاء هر جفت از رده‌های هم‌ارزی $\langle x\rangle$ و $\langle y\rangle$، داشته باشیم $\langle x\rangle * \langle y\rangle \in S/\sim$ و هیچ چیز نمی‌تواند طبیعی‌تر از این باشد که آن‌را به‌وسیلهٔ تساوی

$$\langle x\rangle * \langle y\rangle = \langle x*y\rangle \qquad (\text{آ})$$

تعریف کنیم. طرف راست عضوی از $S/\sim$ است و با معلوم بودن x و y، به‌طور یکتا معین می‌شود. اما، آنچه که به‌ما داده‌شده x و y نیست، بلکه $\langle x\rangle$ و $\langle y\rangle$ است. چون $\langle x\rangle$ و $\langle y\rangle$ عناصر x و y را به‌طور یکتا معین نمی‌کنند، تساوی (آ) در حالت کلی عملی روی $S/\sim$ تعریف نخواهد کرد. چون طرف راست (آ) به‌وسیلهٔ $\langle x\rangle$ و $\langle y\rangle$ به‌طور یکتا معین می‌شود، شرط لازم و کافی برای آن که عملی بدین ترتیب تعریف شود آن است که $\langle x*y\rangle$ مستقل از نماینده‌های ویژهٔ x و y از دو ردهٔ $\langle x\rangle$ و $\langle y\rangle$ باشد. به‌عبارت دیگر، چنانچه نماینده‌های جدیدی از همان رده‌ها برگزینیم، یعنی $\langle x'\rangle = \langle x\rangle$ و $\langle y'\rangle = \langle y\rangle$، ردهٔ $\langle x'*y'\rangle$ باید با ستی همان ردهٔ $\langle x*y\rangle$ باشد.

به‌همین ترتیب، اگر † عملی یکتایی روی S باشد، تساوی

$$\langle x\rangle^{\dagger} = \langle x^{\dagger}\rangle$$

روی $S/\sim$ عملی یکتایی تعریف می‌کند اگر و فقط اگر به‌ازاء هر $x_1, x_2 \in S$، داشته باشیم $\langle x_1\rangle = \langle x_2\rangle \Rightarrow \langle x_1^{\dagger}\rangle = \langle x_2^{\dagger}\rangle$. این شرط می‌گوید که نگاشت $x \longmapsto x^{\dagger}$ از S به S هر ردهٔ هم‌ارزی را به یک ردهٔ هم‌ارزی تبدیل می‌کند، و واضح است که این شرط برای هر عمل و هر رابطهٔ هم‌ارزی دلخواه برقرار نیست.

شایسته است که این محکهای مهم را به‌صورت قضیه‌ای بیان کنیم. با به‌کاربردن این حقیقت که $x_1 \sim x_2 \iff \langle x_1\rangle = \langle x_2\rangle$ بیان آنها را کمی تغییر می‌دهیم.

قضیهٔ ۶پ. فرض کنید $\sim$ رابطه‌ای هم‌ارزی روی مجموعهٔ S، با رده‌های هم‌ارزی $\langle x\rangle$ باشد. فرض کنید † و * به‌ترتیب عملی یکتایی و دوتایی روی S باشند. در این صورت

(الف) شرط لازم و کافی برای اینکه تساوی $\langle x\rangle^{\dagger} = \langle x^{\dagger}\rangle$ عملی یکتایی روی $S/\sim$ تعریف کند آن است که به‌ازاء هر $x_1, x_2 \in S$، داشته باشیم $x_1 \sim x_2 \Rightarrow x_1^{\dagger} \sim x_2^{\dagger}$.

(ب) شرط لازم و کافی برای اینکه تساوی $\langle x\rangle * \langle y\rangle = \langle x*y\rangle$ عملی دوتایی روی $S/\sim$ تعریف کند آن است که به‌ازاء هر $x_1, x_2, y_1, y_2 \in S$ داشته باشیم

$$(x_1 \sim x_2 \ , \ y_1 \sim y_2) \Rightarrow (x_1 * y_1) \sim (x_2 * y_2).$$

مثال ۶.۶. فرض کنید $S = \mathbf{Z}$ و $\sim$ همنهشتی به پیمانهٔ ۳ باشد (قضیهٔ ۳ت را ببینید). در این صورت $S/\sim$ دارای سه عنصر $\langle 0\rangle$، $\langle 1\rangle$ و $\langle 2\rangle$ است. دو عمل دوتایی $+$ و $\cdot$ روی S داریم و بسادگی دیده می‌شود که اگر $x_1 \equiv x_2$ (به پیمانهٔ ۳) و $y_1 \equiv y_2$ (به پیمانهٔ ۳)

آنگاه(به‌پیمانهٔ ۳) $x_1+y_1\equiv x_2+y_2$ و (به‌پیمانهٔ ۳) $x_1\cdot y_1\equiv x_2\cdot y_2$. بنابراین $+$ و $\cdot$ اعمالی روی مجموعهٔ خارج‌قسمت $S/\sim$ القاء می‌کنند. ازطرف دیگر، عمل یکتایی $x\longmapsto|x|$ روی S عملی یکتایی روی $S/\sim$ القاء نمی‌کند زیرا، به‌عنوان مثال، ۱ — و ۲ در ردهٔ $<۲>$ قرار دارند، ولی مقادیر مطلق آنها ۱ و ۲ در رده‌های متفاوتی هستند.

مثال ۷.۶. مجدداً فرض کنید $S=\mathbf{Z}$ ولی این‌دفعه فرض کنید $x\sim y$، یعنی این که به‌ازاء عدد حقیقی مثبتی چون λ، داشته باشیم $x=\lambda y$. سه‌ردهٔ هم‌ارزی P، N، O وجود دارند که P و N به‌ترتیب متشکل‌اند ازهمهٔ اعداد صحیح مثبت ومنفی، و $O=\{0\}$. واضح است که اکنون عمل یکتایی $x\longmapsto|x|$، عملی یکتایی روی مجموعهٔ خارج‌قسمت القاء می‌کند؛ درواقع $|P|=P$، $|N|=P$ و $|O|=O$. به‌همین‌ترتیب، ضرب روی $\mathbf{Z}$، ضربی روی $\mathbf{Z}/\sim$ القاء می‌کند، دراین‌مورد داریم: $P\cdot P=P$، $N\cdot P=N$، $N\cdot N=P$، وغیره. اما جمع عملی روی $S/\sim$ القاء نمی‌کند. (بدون تردید جمع روی بعضی از جفتها تعریف می‌شود، مثلا $P+P=P$، $N+N=N$، $O+N=N$، $O+P=P$، ولی مجموع $N+P$ تعریف نشده است زیرا مجموع یك‌عددصحیح منفی ویك عدد صحیح‌مثبت، گاهی مثبت، گاهی منفی، وگاهی 0 است.)

حال فرض کنید که G گروهی آبلی و H زیرگروهی از G باشد. ازفصل ۴ می‌دانیم که همرده‌های H در G تشکیل افرازی از G می‌دهند که متناظر بارابطهٔ هم‌ارزی تعریف‌شده به‌وسیلهٔ $x\sim y\iff xy^{-1}\in H$ می‌باشد. مجموعهٔ خارج قسمت منتج، که اعضایش همهٔ همرده‌های Hx از H هستند، به‌جای $G/\sim$ به‌وسیلهٔ G/H نشان داده می‌شود. اگر محك فوق را به‌این مجموعهٔ خارج‌قسمت واعمال گروه روی G به‌کار ببریم، درمی‌یابیم که G/H دارای اعمال متناظراست و درواقع نسبت به‌آنها یك‌گروه است.

قضیهٔ ۶ت. فرض کنید H زیرگروهی ازگروه آبلی G باشد. دراین‌صورت تساوی

$$(Hx)(Hy)=H(xy)$$

عملی دوتایی روی‌مجموعهٔ G/H ازکلیهٔ همرده‌های H در G، تعریف می‌کند. G/Hنسبت به‌این عمل یك‌گروه آبلی است. $He=H$ عنصرخنثای آن است و $H(x^{-1})$ معکوس Hx می‌باشد.

برهان. برای ملاحظهٔ این‌که این تساوی‌یك‌عمل تعریف می‌کند، قضیهٔ ۶پ را به‌کارمی‌بریم. باید تحقیق کنیم که اگر $x_1\sim x_2$ و $y_1\sim y_2$ آنگاه $x_1y_1\sim x_2y_2$، که $x_1\sim x_2$ یعنی $x_1x_2^{-1}\in H$. اما اگر $x_1x_2^{-1}\in H$ و $y_1y_2^{-1}\in H$، آنگاه حاصلضربشان $x_1x_2^{-1}y_1y_2^{-1}$ در H قرار دارد. چون G آبلی است، ازاینجا نتیجه می‌گیریم که $x_1y_1y_2^{-1}x_2^{-1}\in H$، یعنی $x_1y_1(x_2y_2)^{-1}\in H$، واین می‌گوید که $x_1y_1\sim x_2y_2$. به‌طریق دیگر، می‌توانیم مستقیماً

باهمرده‌ها استدلال کنیم ونشان دهیم که حاصلضرب یك عنصر دلخواه از Hx وعنصر دلخواهی از Hy همواره در همردهٔ $H(xy)$ قرار دارد. برای اثبات این، فرض کنید $a\in Hx$، $b\in Hy$. دراین صورت $a=h_1x$، $b=h_2y$، که در آنها h_1، $h_2\in H$. بنابراین $ab=h_1xh_2y=h_1h_2xy$، زیرا G آبلی است. اما $h_1h_2=h\in H$، از اینرو $ab=hxy\in Hxy$. حال باقی می‌ماند که اصول موضوعهٔ گروه وقانون جابجایی را برای G/H تحقیق کنیم. اولا، واضح است که ضرب جابجایی است، زیرا

$$(Hx)(Hy)=H(xy)=H(yx)=(Hy)(Hx).$$

به‌همین ترتیب، قانون شرکت پذیری در G قانون شرکت‌پذیری در G/H را نتیجه می‌دهد (این را به‌تفصیل بنویسید!). همردهٔ $He=H$ به‌عنوان عنصر خنثی عمل می‌کند زیرا $(Hx)(He)=H(xe)=Hx$ و $(He)(Hx)=H(ex)=Hx$. بالاخره، $H(x^{-1})$ معکوس Hx است زیرا

$$(Hx)(H(x^{-1}))=H(xx^{-1})=He \quad \text{و} \quad (H(x^{-1}))(Hx)=H(x^{-1}x)=He.$$

بنابراین G/H یك گروه آبلی است، وآن‌را گروه خارج‌قسمت G می‌نامیم.

مثال ۸.۶. فرض کنید G گروه جمعی $\mathbf{Z}$ باشد و $H=n\mathbf{Z}$. دراین‌صورت عناصر $G/H=\mathbf{Z}/n\mathbf{Z}$ رده‌های باقیماندهٔ به‌پیمانهٔ n هستند. ازاینرو مجموعهٔ خارج‌قسمت $\mathbf{Z}/n\mathbf{Z}$ همان‌است که قبلا $\mathbf{Z}_n$ نامیده‌ایم. این‌مجموعه باعمل‌القائی تشکیل گروهی می‌دهد که به‌طورجمعی نوشته‌می‌شود. اگر x ردهٔ باقیماندهٔ شامل x باشد، آنگاه‌جمع‌رده‌های باقیمانده به‌وسیلهٔ $\langle x\rangle=nZ+x$ تعریف می‌شود. به‌عنوان مثال، عناصر $\mathbf{Z}/6\mathbf{Z}$ عبارت‌انداز: $\langle 0\rangle$، $\langle 1\rangle$، $\langle 2\rangle$، $\langle 3\rangle$، $\langle 4\rangle$، $\langle 5\rangle$ وجمع به‌وسیلهٔ $\langle x\rangle+\langle y\rangle=\langle x+y\rangle$ تعریف می‌شود؛ به‌این‌صورت:

«جمع به‌پیمانهٔ ۶»

$$\langle 2\rangle+\langle 3\rangle=\langle 1\rangle+\langle 4\rangle=\langle 5\rangle$$

$$\langle 2\rangle+\langle 4\rangle=\langle 0\rangle,\ \langle 3\rangle+\langle 4\rangle=\langle 1\rangle,\ \text{وغیره.}$$

توجه کنید که

$$\langle x\rangle+\langle y\rangle=\langle z\rangle \iff x+y\equiv z \ (\text{به‌پیمانهٔ } n),\ \text{و}$$

$$\langle x\rangle=-\langle y\rangle \iff x\equiv -y \ (\text{به‌پیمانهٔ } n)$$

ازاینرو همنهشتیها را همواره می‌توان به تساویهای مربوط به‌این گروه ترجمه کرد و بعکس. نتیجهٔ ساده‌ای ازاین مطلب آن است که جوابهای همنهشتی $p+x\equiv q\ (\text{به‌پیمانهٔ } n)$ همهٔ اعضای یك‌ردهٔ باقیمانده به‌پیمانهٔ n هستند، زیرا درهر گروه جمعی معادلهٔ $p+x=q$ دارای جوابی یکتاست.

مثال ۹.۶. فرض کنید G گروه ضربی $\mathbf{C}^*$ و H زیرگروه T (گروه دایره‌ای) باشد. همرده‌های T درنمودار آرگان عبارت‌اند ازهمهٔ دایره‌های به‌مرکز O، وبه‌هرعددحقیقی مثبت λ دقیقاً یکی متناظر است، یعنی دایرهٔ $T\lambda$ به شعاع λ. درگروه خارج‌قسمت $\mathbf{C}^*/T$ حاصلضرب دو دایرهٔ $T\lambda$، $T\mu$ به‌وسیلهٔ $(T\lambda)(T\mu)=T(\lambda\mu)$ تعریف می‌شود، یعنی دایره‌ای که شعاعش برابر

حاصلضرب دو شعاع است. بنابراین ضرب در $\mathbf{C}^*/T$ همان ضرب اعداد حقیقی مثبت را تقلید می کند ویك یکریختی از گروهها داریم، $\mathbf{C}^*/T \cong \mathbf{R}^+$.

مثال ۶.۱۰. فرض کنید G گروه ضربی $\mathbf{R}^*$ و H زیرگروه $\mathbf{R}^+$ باشد. در این صورت دو همرده از H وجود دارد: مجموعهٔ P از اعدادحقیقی مثبت ومجموعهٔ N از اعدادحقیقی منفی. گروه خارج‌قسمت، گروهی دوری ازمرتبهٔ ۲ باعنصرخنثای P می باشد و داریم: $N^2 = P$.

حال فرض کنید که G گروهی دلخواه و H زیرگروهی ازآن باشد. ما بایستی بین همرده‌های چپ و راست H تمایزی قائل شویم، ازاینرو برای معین بودن، G/H را برابر مجموعهٔ همرده‌های راست Hx از H در G تعریف می کنیم. درحالت کلی مجموعهٔ خارج‌قسمت G/H یك گروه نیست، وباید روی H شرطهایی منظور کنیم تا G/H به یك گروه تبدیل شود. نکته در این است که تساوی $(Hx)(Hy) = Hxy$ در حالت کلی یك عمل روی G/H تعریف نمی کند. اگر $a \in Hx$ و $b \in Hy$، آنگاه $a = h_1 x$، $b = h_2 y$ که درآن $h_1, h_2 \in H$، و $ab = h_1 x h_2 y$، که همیشه به Hxy متعلق نخواهد بود. حال می‌توانیم بنویسیم $ab = h_1 h_2 x^{-1} x y$. $h_1 x h_2 x^{-1} \in H$، واین به Hxy متعلق خواهد بود اگروفقط اگر $ab = h_1 x h_2 x^{-1} x y$. چون $h_1 \in H$، کافی خواهدبود که $x h_2 x^{-1} \in H$، اما این شرط لازم است که به‌ازاء هر $x \in G$ وهر $h_2 \in H$ برقرار باشد. این مطلب انگیزهٔ تعریف زیراست.

تعریف. یك زیرگروه H از G زیرگروه نرمال G (نوشته می‌شود $H \lhd G$) نامیده می‌شود اگر به‌ازاء هر $x \in G$ وهر $h \in H$، داشته باشیم $xhx^{-1} \in H$. به‌نتایج سادهٔ زیر ازاین تعریف توجه می کنیم:

(الف) درهر گروه آبلی، هرزیرگروه نرمال است.

(ب) اگر $H \lhd G$ آنگاه به‌ازاء هر $x \in G$ وهر $h \in H$، داریم $x^{-1}hx \in H$.

(پ) اگر $H \lhd G$ آنگاه همرده‌های چپ وراست H مساوی‌اند.

(چون اگر $a \in xH$ آنگاه به‌ازاء عنصری چون $h \in H$، داریم $a = xh$، از اینرو $ax^{-1} = xhx^{-1} \in H$، که نتیجه می‌دهد $a \in Hx$. بنابراین $xH \subset Hx$، وبه‌همین‌ترتیب $Hx \subset xH$.) بنابراین اگر H نرمال باشد، می‌توان G/H را، بدون تصریح بیشتر، «مجموعهٔ همرده‌های H» تعریف کرد.

قضیهٔ ۶.۱۱. فرض کنید G گروه دلخواهی باشد و H زیرگروهی نرمال از G. دراین‌صورت تساوی
$$(Hx)(Hy) = Hxy$$
عملی دوتایی روی G/H تعریف می‌کند، و G/H را به‌یك گروه تبدیل می‌کند. عنصر خنثای آن $He = H$ ومعکوس Hx همردهٔ Hx^{-1} است.

برهان. هم اکنون نشان دادیم، برای اثبات اینکه تساوی مذکور عملی تعریف کند، نرمال

بودن H دقیقاً همان فرضی است که محتاج آنیم. بقیهٔ برهان کاملا مانند برهان قضیهٔ ۶ع است، البته بجز اینکه نمی‌توانیم ثابت کنیم، و ادعا هم نمی‌کنیم، که G/H آبلی است.

مثال ۱۱.۶. فرض کنید $G=\mathcal{S}_3$ و با اخذ همان نمادهای مثالهای ۱۲.۴ و ۲۴.۴ قرار دهید: $H=\{e, a\}$. در این صورت H نرمال نیست، زیرا $pap^{-1}=cp^{-1}=cq=b\notin H$. همرده‌های چپ و راست آن، همان‌طوری که در ۲۴.۴ دیدیم، متفاوت‌اند. ولی زیر گروه $K=\{e, p, q\}$ نرمال است (این را تحقیق کنید!). همرده‌هایش عبارت‌اند از: K و $Ka=\{a, b, c\}$، و گروه خارج‌قسمت G/K، دوری و از مرتبهٔ دو است.

مثال ۱۲.۶. هر گروه G دارای دو زیر گروه نرمال G و $\{e\}$ است. خارج قسمتهای متناظر عبارت‌اند از: $G/G\cong\{e\}$ و $G/\{e\}\cong G$.

قضیهٔ ۶ج. فرض کنید H زیرگروهی نرمال از یک گروه G باشد. در این صورت

(الف) اگر G آبلی باشد، G/H نیز آبلی است؛

(ب) اگر G دوری باشد، G/H نیز دوری است؛

(پ) اگر G متناهی باشد، G/H نیز متناهی و مرتبه‌اش مرتبهٔ G را عاد می‌کند؛

(ت) $(Hx)^n$ عنصر خنثای G/H است $\Leftrightarrow x^n\in H$؛

(ث) همرده‌های Hx و Hy با همدیگر جابجایی‌اند اگر و فقط اگر $xyx^{-1}y^{-1}\in H$؛

(ج) G/H آبلی است $\Leftrightarrow$ به ازاء هر $x, y\in G$، داشته باشیم $xyx^{-1}y^{-1}\in H$.

برهان. (الف) از قضیهٔ ۶ع نتیجه می‌شود.

(ب) فرض کنید G به وسیلهٔ g تولید شده باشد. در این صورت هر عنصر x از G به صورت g^n است. بنابراین هر عنصر G/H به صورت $Hx=H(g^n)=(Hg)^n$ خواهد بود، و در نتیجه G/H دوری است، و به وسیلهٔ همردهٔ Hg تولید می‌شود.

(پ) این قسمت از قضیهٔ لاگرانژ نتیجه می‌شود. چنانچه G دارای مرتبهٔ n و H از مرتبهٔ m باشد، آنگاه $n=rm$، که r تعداد همرده‌های H است، یعنی r مرتبهٔ G/H می‌باشد.

(ت) چون $(Hx)^n=Hx^n$، داریم

$$(Hx)^n=He\Leftrightarrow Hx^n=He\Leftrightarrow x^n\in He=H.$$

(ث)
$$(Hx)(Hy)=(Hy)(Hx)\Leftrightarrow(Hx)(Hy)(Hx)^{-1}(Hy)^{-1}=He$$
$$\Leftrightarrow Hxyx^{-1}y^{-1}=He$$
$$\Leftrightarrow xyx^{-1}y^{-1}\in H.$$

(ج) این قسمت بلافاصله از (ث) نتیجه می‌شود.

نتیجه. $\mathbf{Z}/n\mathbf{Z}$ یک‌گروه دوری ازمرتبهٔ n است.

برهان. $\mathbf{Z}$ دوری است، و (به‌طورجمعی) به وسیلهٔ ۱ تولید می‌شود، ازاینرو $\mathbf{Z}/n\mathbf{Z}$ به‌وسیلهٔ ردهٔ باقیماندهٔ $1+n\mathbf{Z}=\langle 1\rangle$ تولیدمی‌شود. البته، این بسادگی دیده‌می‌شودچون‌توانهای جمعی $\langle 1\rangle$ عبارت‌اند از: $\langle 1\rangle$ ، $\langle 2\rangle$ ، $\langle 3\rangle$ ، ... ، $\langle n\rangle=\langle 0\rangle$ وبنابراین همهٔ عناصر $\mathbf{Z}/n\mathbf{Z}$ راتولید می‌کند.

ایدهٔ مهمی که به‌کمک آن می‌توان گروههای خارج‌قسمت را با گروههای دیگری ارتباط داد ایدهٔ همریختی گروههاست. این تعمیمی از یکریختی است و بـه‌صورت زیر تعریف می‌شود:

تعریف. اگر A و B دوگروه (که به‌طور ضربی نوشته شده‌اند) باشند، یك همریختی از A به B تابعی است مانند $f : A \longrightarrow B$ که ضرب را حفظ می‌کند، یعنی به‌قسمی است‌که به ازاءهر $a_1 , a_2 \in A$ ، داریم $f(a_1a_2)=f(a_1)f(a_2)$. بنابراین‌یك‌یکریختی،همریختی‌ای است‌که نگاشت دوسویی نیز باشد. همانند حالت یکریختی، گروهها می‌توانند جمعی، یا یکی جمعی ودیگری ضربی باشد، وغیره، که درآن حالت بایدتعریف رابطه مطابق‌ومناسب آن بیان شود. نکتهٔ اساسی این است‌که f باید عمل‌گروه A را به‌عمل‌گروه B انتقال دهد.

ممکن است تصور شود کـه درتعریف یك همریختی بایستی اصرار داشته باشیم کـه نگاشت باید معکوسها وعنصرخنثی را همانند ضرب حفظ کند. این فرض غیرضروری است زیرا تساویهای $f(e)=e$ و $f(x)^{-1}=f(x^{-1})$ ازتعریف ودقیقاً به‌وسیلهٔ همان‌استدلالهایی که (درصفحهٔ ۵۹) برای یکریختیها آوردیم، نتیجه‌می‌شود.

مثال ۱۳.۶. دراینجا برخی از همریختیهایی را کـه بعداً به آنها مراجعه می‌شود، فهرست می‌کنیم. درهرمورد، خواننده باید کاملا بفهمد چرانگاشت یك همریختی است.

(الف) فرض‌کنید $f_1 : \mathbf{R}^2 \longrightarrow \mathbf{R}$ به‌وسیلهٔ $(x , y) \longmapsto x$ داده‌شده باشد. دراین صورت f_1 یك همریختی گروههای جمعی‌است زیرا

$$(x_1 , y_1)+(x_2 , y_2)=(x_1+x_2 , y_1+y_2) \longrightarrow x_1+x_2 .$$

(ب) فرض‌کنید $f_2 : \mathbf{C} \longrightarrow \mathbf{C}$ به‌وسیلهٔ $z \longmapsto \bar{z}$ داده شده باشد ($\bar{z}$ مزدوج‌مختلط z است). دراین‌صورت f_2 یك همریختی جمعی است زیرا $\overline{z_1+z_2}=\bar{z}_1+\bar{z}_2$.

(پ) فرض‌کنید $f_3 : \mathbf{C}^* \longrightarrow \mathbf{R}^*$ به‌وسیلهٔ $z \longmapsto |z|$ داده شده‌باشد. دراین‌صورت f_3 یك همریختی ضربی است زیرا $|z_1z_2|=|z_1|\ |z_2|$.

(ت) فرض‌کنید $f_4 : \mathbf{R} \longrightarrow \mathbf{R}^*$ به‌وسیلهٔ $t \longmapsto e^t$ داده شده باشد . دراین صورت

$s+t \longmapsto e^{s+t}=e^s e^t$ ، ازاینرو f_4 یك همریختی از گروه جمعی $\mathbf{R}$ به گروه ضربی $\mathbf{R}^*$ است.

(ث) فرض کنید $f_5 : \mathbf{R} \longrightarrow \mathbf{C}^*$ به‌وسیلهٔ $t \longmapsto e^{2\pi i t}$ داده شده باشد، دراین‌صورت، مانندحالت (ت) ، f_5 یك همریختی ازگروه‌جمعی به‌گروه ضربی است.

(ج) فرض کنید $f_6 : \mathrm{GL}_n(\mathbf{R}) \longrightarrow \mathbf{R}^*$ به وسیلهٔ $M \longmapsto \det M$ داده شده باشد، که $\det M$ دترمینان‌ماتریس غیرمنفرد M را نشان می‌دهد. این یك همریختی ضربی است، زیرا $\det(M_1 M_2)=\det M_1 \cdot \det M_2$.

مثال ۱۴.۶. بین همریختیها وگروههای خارج قسمت بلافاصله می‌توانیم ارتباطی را نشان دهیم. فرض کنید $H \lhd G$ ونگاشت خارج‌قسمت $q : G \longrightarrow G/H$ را درنظر بگیرید. بنا به تعریف، به‌ازاء هر $x \in G$ ، $q(x)$ ردهٔ هم‌ارزی شامل x است ، یعنی $q(x)=Hx$. بنابراین $q(xy)=H(xy)=(Hx)(Hy)=q(x)q(y)$ وازاینرو q یك همریختی است، درواقع می‌توان گفت که تعریف‌ضرب در G/H دقیقاً به‌خاطرهمریختی ساختن نگاشت خارج‌قسمت انتخاب شده است.

اکنون یك‌همریختی‌دلخواه ازگروهها مانند $f : A \longrightarrow B$ رادرنظربگیرید. مجموعهٔ عناصر $a \in A$ به‌قسمی که $f(a)=e$ ، هستهٔ f نامیده می‌شود. این‌مجموعه برای‌یك یکریختی دقیقاً مساوی $\{e\}$ است،ولی‌درحالت کلی‌ممکن‌است‌شامل‌عناصردیگرنیز باشد. همچنین‌اصطلاح تصویر f را، به‌مفهوم‌معمول‌درنظریهٔ‌مجموعه‌ها، به‌کارخواهیم برد. $f(A)=\{f(a) \; ; \; a \in A\}$. قضیهٔ زیر یکی‌از اساسی‌ترین قضایای جبرمجرد است، که اولین قضیهٔ یکریختی گروهها نامیده می‌شود، و دارای حالت مشابه‌ای برای انواع دیگر ساختمانهای جبری می‌باشد. (قضایای‌دوم وسوم یکریختی نیز وجود دارند که‌دراین‌کتاب ازآنها صحبت نخواهیم کرد.)

قضیهٔ ۶چ. فرض‌کنید A و B دوگروه‌باشند و $f : A \longrightarrow B$ یك‌همریختی باشد. دراین‌صورت

(الف) هستهٔ K از f یك زیرگروه نرمال A است ؛

(ب) بافتهای f همرده‌های K هستند ؛

(پ) تصویر $C=f(A)$ از f یك زیرگروه B است؛

(ت) $C \cong A/K$

برهان. (الف) فرض کنید $k_1 , k_2 \in K$ و $a \in A$. دراین صورت $f(k_1)=f(k_2)=e$، از اینرو $f(k_1 k_2)=f(k_1)f(k_2)=e$ و $f(k_1^{-1})=f(k_1)^{-1}=e^{-1}=e$. این نشان می‌دهدکه $k_1 k_2 \in K$ و $k_1^{-1} \in K$. همچنین $e \in K$ چون $f(e)=e$ ، پس K زیرگروهی از A است، بالاخره

$f(ak_1a^{-1})=f(a)f(k_1)f(a^{-1})=f(a)ef(a)^{-1}=f(a)f(a)^{-1}=e$ ،
ازاینرو $ak_1a^{-1}\in K$ وبنابراین K نرمال است.

$$f(a_1)=f(a_2)\iff f(a_1)f(a_2)^{-1}=e \qquad (ب)$$
$$\iff f(a_1)f(a_2^{-1})=e$$
$$\iff f(a_1a_2^{-1})=e$$
$$\iff a_1a_2^{-1}\in K$$
$$\iff (a_1 \text{ و } a_2 \text{ دریك همرده از } K \text{ قرار دارند})$$

(پ) چون $f(e)=e$ ، داریم $e\in C$. همچنین، اگر c_1 ، $c_2\in C$ آنگاه به ازاء عناصری چون a_1 ، $a_2\in A$ ، داریم $c_1=f(a_1)$ ، $c_2=f(a_2)$؛ ازاینرو $c_1c_2=f(a_1a_2)$ و $c_1^{-1}=f(a_1^{-1})$ هردو در $f(A)=C$ قرار دارند.

(ت) بنا به‌قسمت (ب) ، f روی هر همرده از K ثابت است، از اینرو می‌توانیم نگاشتی مانند $f^*: A/K\longrightarrow C$ ، بامساوی قرار دادن $f^*(Ka)$ با مقدار f روی عضو دلخواهی از Ka ، تعریف کنیم. بنا به‌تعریف C ، واضح است که f^* بروی‌است، و ، بنا به قسمت(ب)، یك‌به‌یك می‌باشد. بالاخره، چون f یك همریختی است، داریم:

$$f^*((Ka_1)(Ka_2))=f^*(Ka_1a_2)=f(a_1a_2)=f(a_1)f(a_2)$$
$$=f^*(Ka_1)f^*(Ka_2)\ .$$

بنابراین f^* عمل گروه A/K را حفظ می‌کند ویك‌یکریختی گروههاست.

نتیجه. یك همریختی یك‌به‌یك است اگروفقط‌اگر هسته‌اش زیرگروه بدیهی $\{e\}$ باشد.

برهان. این بلافاصله ازقسمت(ب) قضیهٔ فوق به‌دست می‌آید، زیرا نگاشت یك‌به‌یك، بنا به تعریف، نگاشتی است که هریك از بافتهایش شامل فقط یك‌عنصر باشد.

مثال ۱۵.۶. به‌شش همریختی که‌درمثال ۱۳.۶ بیان شدند رجوع می‌کنیم وقضیهٔ ۶ج رابرای هریك‌ازآنها به‌کار می‌بریم.

(الف) $f_1:(x\ ,\ y)\longmapsto x$ از $\mathbf{R}^2$ به $\mathbf{R}$ دارای تصویر $\mathbf{R}$ است وهسته‌اش Kمجموعهٔ نقاطی از $\mathbf{R}^2$ است که وقتی برمحورxها تصویرشوند، برنقطهٔ ۰ قرارگیرند؛ به‌عبارت‌دیگر K محور yهاست، وبنا به‌قسمت (ت) قضیهٔ فوق: $\mathbf{R}^2/K\cong\mathbf{R}$.

(ب) $f_2: z\longmapsto\bar{z}$ از $\mathbf{C}$ به $\mathbf{C}$ دارای تصویر $\mathbf{C}$ و هستهٔ $\{0\}$ است، از اینرو قضیهٔ ۶ج فقط این‌حقیقت بدیهی را به‌ما می‌گوید که $\mathbf{C}/\{0\}\cong\mathbf{C}$.

(پ) $f_3: z\longmapsto|z|$ از $\mathbf{C}^*$ به $\mathbf{R}^*$ دارای تصویر $\mathbf{R}^+$ و هسته‌اش مجموعهٔ

$T=\{z\in\mathbf{C}^*\ ;\ |z|=1\}$ یعنی همان گروه دایره‌ای می‌باشد. حال قضیهٔ ۶ ج می گوید که $\mathbf{C}^*/T\cong\mathbf{R}^+$ (مثال ۹.۶ را ببینید).

(ت) $f_4 : t\longrightarrow e^t$ از $\mathbf{R}$ به $\mathbf{R}^*$ دارای تصویر $\mathbf{R}^+$ و هستهٔ $\{0\}$ می‌باشد. بنابراین یك‌به‌یك بوده و یك یکریختی از $\mathbf{R}$ به $\mathbf{R}^+$ القاء می‌کند که قبلا درمثال ۱۸.۴ با آن برخورد کرده‌ایم.

(ث) $f_5 : t\longrightarrow e^{2\pi it}$ از $\mathbf{R}$ به $\mathbf{C}^*$ جالبتراست. هسته‌اش مجموعهٔ اعداد حقیقی t است به‌قسمی که $e^{2\pi it}=1$، به‌عبارت دیگر برابر است با $\mathbf{Z}$. تصویرش مجموعهٔ همهٔ اعداد مختلط به‌صورت $\cos t+i\sin t$، به‌ازاء عددحقیقی t، می‌باشد، واین همان گروه دایره‌ای T است. بنابراین، قضیهٔ ۶ ج این حقیقت‌جالب را به‌ما می گوید که $\mathbf{R}/\mathbf{Z}\cong T$. این حقیقت کمتر شگفت‌آور خواهد بود چنانچه تصور شود که محورحقیقی را به دور دایره‌ای به‌محیط واحد پیچانده‌ایم به‌قسمی که همهٔ اعداد صحیح برهم منطبق شده‌اند. دراین صورت هرهمردهٔ $\mathbf{Z}$ به‌یك‌نقطه از دایره تبدیل می گردد و، پس‌از توسعهٔ دایره‌به‌دایرهٔ به‌شعاع‌واحد، جمع در $\mathbf{R}$ به‌ضرب در T مبدل می‌شود.

(ج) $f_6 : M\longmapsto\det M$ از $\mathrm{GL}_n(\mathbf{R})$ به $\mathbf{R}^*$ برومی‌باشد، زیرا به‌ازاء $\alpha\in\mathbf{R}^*$ مفروض، ماتریس‌قطری با درایه‌های قطراصلی α، 1، 1، ...، 1 غیرمنفرد بوده ودارای دترمینان α است. هستهٔ f_6، بنابه تعریف، گروه خطی ویژهٔ $\mathrm{SL}_n(\mathbf{R})$ است، ازاینرو داریم $\mathrm{SL}_n(\mathbf{R})\lhd\mathrm{GL}_n(\mathbf{R})$ و $\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R})\cong\mathbf{R}^*$.

مثال ۱۶.۶. فرض کنید G گروه دوری دلخواهی باشدکه به‌وسیلهٔ عنصر g تولید شده است. فرض کنید $f : \mathbf{Z}\longrightarrow G$ نگاشتی باشدکه به‌وسیلهٔ $r\longrightarrow g^r$ تعریف شده است. f یك همریختی از گروه جمعی $\mathbf{Z}$ به G است، زیرا $g^{r+s}=g^rg^s$. وتصویرش G است چون G به‌وسیلهٔ g تولید شده است. بنابراین $G\cong\mathbf{Z}/K$، که درآن K هستهٔ f است. هستهٔ f برابر است با $\{0\}$، اگر g دارای مرتبهٔ نامتناهی باشد، وبرابراست با $n\mathbf{Z}$، اگر g دارای مرتبهٔ متناهی n باشد. بنابراین هر گروه‌دوری با $\mathbf{Z}$ یا، به‌ازاء عددی‌چون $n\geqslant 1$، با $\mathbf{Z}/n\mathbf{Z}$ یکریخت است. وبدین‌ترتیب برهان دیگری ازقضیهٔ ۴ث ونتیجهٔ آن به‌دست می‌آید.

خاصیت جامع مجموعه‌های خارج قسمت که درقضیهٔ ۲ث بیان شد، دارای نظیری در گروههای خارج‌قسمت است که اکنون آن‌را ثابت می کنیم. این‌قضیه اساساً بیان دیگری از قضیهٔ ۶ ج است به‌صورت کمی‌قویتر.

قضیهٔ ۶ ح. فرض کنید A یك‌گروه باشد، $N\lhd A$ و $q : A\longrightarrow A/N$ همریختی خارج قسمت باشد. اگر $f : A\longrightarrow B$ همریختی دلخواهی بین‌گروههای A و B باشد به‌قسمی‌که $f(N)=\{e\}$، آنگاه همریختی یکتایی مانند $f^* : A/N\longrightarrow B$ به‌قسمی وجود دارد که $f=f^*\circ q$.

برهان. استدلالها خیلی شبیه قضیهٔ۶چ هستند. اگر a_1 ، a_2 دریك‌همرده از N در A باشند آنگاه $a_1a_2^{-1}\in N$، ازاینرو $f(a_1a_2^{-1})=e$، که‌نتیجه می‌دهد $f(a_1)=f(a_2)$. بنابراین f روی همرده‌های N ثابت است ومی‌توانیم نگاشتی مانند $f^*: A/N\longrightarrow B$ با دستور $f^*(Na)=f(a)$ تعریف کنیم. (این‌را باقضیهٔ۲ث مقایسه کنید.) واضح است که $f=f^*\circ q$ زیرا $f^*(q(a))=f^*(Na)=f(a)$. اینکه f^* یك همریختی است ازتعریف ضرب در A/N به‌دست می‌آید: زیرا

$$f^*((Na_1)(Na_2))=f^*(Na_1a_2)=f(a_1a_2)=f(a_1)f(a_2)$$
$$=f^*(Na_1)f^*(Na_2).$$

اینکه f^* یکتاست ازتساوی $f=f^*\circ q$ به‌دست‌می‌آید؛ چون اگر $f=g\circ q$ آنگاه‌به‌ازاء هر $a\in A$، داریم $g(q(a))=f(a)$ ، ازاینرو $g(Na)=f(a)$ و $g=f^*$. البته، عکس این‌قضیه بدیهی است، یعنی اگر f^* یك‌همریختی‌از A/N به B باشد واگر $f=f^*\circ q$، آنگاه $f(N)=\{e\}$.

مثال ۱۷.۶. فرض کنید $q: \mathbf{Z}\longrightarrow \mathbf{Z}/n\mathbf{Z}$ همریختی خارج‌قسمت باشد که هرعدد صحیح را به‌ردهٔ باقیمانده‌اش به‌پیمانهٔ n می‌فرستد. ردهٔ x را با $\langle x\rangle_n$ نشان می‌دهیم. حال فرض کنید $f: \mathbf{Z}\longrightarrow B$ همریختی گروهی دلخواهی باشد به‌قسمی که $f(n)=e$. دراین‌صورت هستهٔ f باید شامل‌زیرگروه تولیدشده به‌وسیلهٔ n، یعنی $n\mathbf{Z}$ باشد، ازاینرو می‌توانیم قضیهٔ۶ح را برای به‌دست‌آوردن یك همریختی $f^*: \mathbf{Z}/n\mathbf{Z}\longrightarrow B$ به‌قسمی که ، به‌ازاء هر $x\in\mathbf{Z}$ ، $f^*(\langle x\rangle_n)=f(x)$ به‌کاربریم. بخصوص، اگر f نیز یك‌همریختی خارج‌قسمت، مثلا، از $\mathbf{Z}$ به $\mathbf{Z}/m\mathbf{Z}$ باشد، آنگاه $f(n)=\langle n\rangle_m=0$ اگر وفقط‌اگر $m|n$. بنابراین، اگر $m|n$ ، آنگاه یك همریختی گروهی $\mathbf{Z}/n\mathbf{Z}\longrightarrow\mathbf{Z}/m\mathbf{Z}$ داریم که، به‌ازاء هرعدد صحیح x ، $\langle x\rangle_n$ رابه $\langle x\rangle_m$ می‌فرستد. اگر $m\nmid n$، چنین‌نگاشتی نمی‌تواند وجود داشته‌باشد، وخوب است خواننده این‌را ثابت‌کند.

تمرینها

۱. فرض کنید A و B دو گروه باشند. فرض کنید $a\in A$ ، $b\in B$ به‌ترتیب عناصری از مرتبه‌های m و n باشند. ثابت کنید که‌عنصر $(a\,,b)$ از $A\times B$، دارای مرتبهٔ N است، که N کوچکترین مضرب‌مشترك m و n است.

۲. عکس‌قضیهٔ۶ب راثابت کنید، یعنی اگر A و B گروههای دوری باشند، وچنانچه $A\times B$ نیز دوری باشد، آنگاه A و B متناهی هستند ومرتبه‌هایشان متباین‌اند.

۳. فرض کنید $f: A\longrightarrow B$ یك‌همریختی گروهی و بروی باشد. ثابت کنید:
(الف) اگر A آبلی باشد، B نیز آبلی‌است؛

(ب) اگر A دوری باشد، B نیز دوری است؛

(پ) اگر B بدون تاب باشد، A نیز بدون تاب است. (یك گروه بدون تاب است اگر e تنها عنصر از مرتبهٔ متناهی در آن باشد.)

۴. ثابت کنید که اگر G یك گروه از مرتبهٔ $2n$ و H زیر گروهی از مرتبهٔ n باشد آنگاه H نرمال است.

۵. ثابت کنید که $(\mathbf{R}\times\mathbf{R})/(\mathbf{Z}\times\mathbf{Z})\cong T\times T$.

۶. ثابت کنید که $T/\{\pm 1\}\cong T$. دربارهٔ T/P_n چه می‌توان گفت، که در آن P_n گروه ریشه‌های nام ۱ در $\mathbf{C}$ است.

۷. ثابت کنید که $\mathbf{C}^*/\mathbf{R}^+\cong T$. (راهنمایی: یك همریختی از $\mathbf{C}^*$ به T پیدا کنید که $\mathbf{R}^+$ را به ۱ بفرستد.)

۸. فرض کنید G گروه دلخواهی باشد و H مجموعهٔ همهٔ عناصری از G باشد که می‌توانند به صورت حاصلضربی از مجذورات عناصر G بیان شوند. ثابت کنید که H زیر گروه نرمال G است و G/H آبلی می‌باشد.

۹. فرض کنید A و B دو گروه باشند و $G=A\times B$. نشان دهید که مجموعهٔ $H=\{(a\,,e)\;;\;a\in A\}$ یك زیر گروه نرمال G است و یکریختیهای $H\cong A$ و $G/H\cong B$ را ثابت کنید.

۱۰. ثابت کنید که گروه $\mathbf{R}/\mathbf{Q}$ بدون تاب است. (برای تعریف، تمرین ۳ در فوق را ببینید.)

۱۱. ثابت کنید که مجموعهٔ همهٔ ریشه‌های ۱ در $\mathbf{C}$، یعنی

$$\mathrm{P}=\bigcup_{n=1}^{\infty}\mathrm{P}_n$$

یك زیر گروه از گروه دایره‌ای است. ثابت کنید که $\mathbf{Q}/\mathbf{Z}\cong\mathrm{P}$.

۱۲. ثابت کنید که هر گروه از مرتبهٔ ۴ یا دوری است یا با حاصلضرب دو گروه دوری از مرتبهٔ ۲ یکریخت می‌باشد.

فصل ۷

همنهشتیهای خطی در z

به ازاء هرعدد صحیح مثبت n ، همنهشتی به پیمانهٔ n یك رابطهٔ هم‌ارزی روی $\mathbf{Z}$ است که رده‌های هم‌ارزی آن رده‌های باقیمانده به پیمانهٔ n هستند. این رده‌ها عناصر گروه خارج‌قسمت $\mathbf{Z}/n\mathbf{Z}$ ، که دوری واز مرتبهٔ n است، هستند؛ وعمل گروهی «جمع به پیمانهٔ n»است. قبلا خاطر نشان کرده‌ایم که عبارات همنهشتی بین اعداد صحیح همواره می‌توانند به‌عبارات تساوی میان رده‌های باقیمانده در گروه $\mathbf{Z}/n\mathbf{Z}$ برگردانده شوند، از اینرو شگفت‌آور نیست که اکثر قوانین مربوط به حل معادلات، برای همنهشتیها نیز معتبرهستند. اکنون این مطلب‌را دقیقتر نموده و اشکالاتش را خاطرنشان می‌کنیم ــ بعضی از روشهای استانده برای حل معادلات درمورد همنهشتیها قابل اعمال نیستند.

اولا یك پیمانهٔ ثابت n برمی‌گزینیم وهمنهشتیهای‌دلخواه به‌صورت $a\equiv b(n$ به پیمانهٔ$)$ را در نظرمی‌گیریم ، که a و b می‌توانند نشانگر عبارات پیچیده‌یی متشکل از متغیرهای صحیح باشند، البته مقادیر a و b همیشه اعداد صحیح‌اند . همانند معادلات، قوانین زیر را داریم :

(الف) $a\equiv b(n$ به پیمانهٔ$)\iff a-b\equiv 0(n$ به پیمانهٔ$)$ ؛

(ب) $a\equiv b+c(n$ به پیمانهٔ$)\iff a-c\equiv b(n$ به پیمانهٔ$)$ ؛

(پ) $a\equiv b(n$ به پیمانهٔ$)\iff -a\equiv -b(n$ به پیمانهٔ$)$.

هرسه عبارت از قوانین متناظر برای معادلات در $\mathbf{Z}/n\mathbf{Z}$ نتیجه می‌شوند، و نیز می‌توان آنها را مستقیماً به کمك تعریف ثابت کرد .

(ت) به‌ازاء هرعددصحیح r ، داریم $a\equiv b(n$ به پیمانهٔ$)\Rightarrow ra\equiv rb(n$ به پیمانهٔ$)$.

برهان. اگر $n|(a-b)$ آنگاه $n|(ra-rb)=r(a-b)$. به بیان دیگر، در $\mathbf{Z}/n\mathbf{Z}$، اگر $<b>=<a>$ آنگاه توانهای جمعی r ام $<a>$ و $<b>$ باهم مساویند، یعنی $r<b>=r<a>$. چون $r<a>=<ra>$، درنتیجه $<rb>=<ra>$.

اخطار. این استلزام فقط یکطرفه کار می‌کند. اگر معادلات در $\mathbf{Z}$ مورد بحث ما می‌بود آنگاه $ra=rb$ نتیجه می‌داد (قانون حذف) $a=b$ بشرطی که $r\neq 0$. ولی اگر (به پیمانهٔ n) $ra\equiv rb$ نمی‌توانیم نتیجه بگیریم که (به پیمانهٔ n) $a\equiv b$ حتی اگر (به پیمانهٔ n) $r\not\equiv 0$. به عنوان مثال، (به پیمانهٔ ۶) $۲\times ۲\equiv ۴\times ۲$ و (به پیمانهٔ ۶) $۲\not\equiv ۰$، اما ۲ را نمی‌توانیم حذف کنیم و نتیجه بگیریم که (به پیمانهٔ ۶) $۱\equiv ۴$. آنچه در اینجا می‌گوییم، به زبان نظریهٔ گروهها، آن است که در $\mathbf{Z}/n\mathbf{Z}$، $r<a>=r<b>\Leftrightarrow<a>=<b>$. اگر این را به نماد ضربی برای یک گروه G برگردانیم، بیان می‌کند که اگر x و y در G، $x^r=y^r$، آنگاه لزومی ندارد که x مساوی با y باشد، حتی در یک گروه دوری.

البته گاهی r می‌تواند از یک همنهشتی مانند (به پیمانهٔ n) $ra\equiv rb$ حذف شود و داشتن محکی قابل استفاده در این مورد، از اهمیت خاصی برخوردار است. همچنین، در اینجا پدیده‌ای نو ظاهر می‌گردد: گاهی اوقات می‌توان r را حذف کرد، به شرط آنکه مقدار پیمانه نیز عوض شود. سؤالات اصلی در این زمینه به وسیلهٔ قضیهٔ زیر جواب داده می‌شود.

قضیهٔ ۷آ. فرض کنید n عددی صحیح و مثبت و a، b، r اعداد صحیح باشند.

(الف) اگر $(r, n)=۱$، آنگاه (به پیمانهٔ n) $a\equiv b\Longleftrightarrow$ (به پیمانهٔ n) $ra\equiv rb$.

(ب) اگر $r|n$، مثلاً $n=rn'$، آنگاه (به پیمانهٔ n') $a\equiv b\Longleftrightarrow$ (به پیمانهٔ n) $ra\equiv rb$.

(پ) در حالت کلی، اگر $r\neq 0$ فرض کنید $(r, n)=d$. آنگاه (به پیمانهٔ $n_۱$) $a\equiv b\Longleftrightarrow$ (به پیمانهٔ n) $ra\equiv rb$، که در آن $n=n_۱d$.

برهان. (الف) اگر (به پیمانهٔ n) $ra\equiv rb$ آنگاه $n|r(a-b)$. چنانچه $(r, n)=۱$ می‌توان، بنا به قضیهٔ ۵ب، نتیجه گرفت که $n|(a-b)$، یعنی، (به پیمانهٔ n) $a\equiv b$. قبلا استلزام عکس آن ثابت شده است و به ازاء هر r درست است.

(ب) فرض کنید $n=rn'$. اگر (به پیمانهٔ n') $a\equiv b$، آنگاه $n'|(a-b)$، از اینرو واضح است که $rn'|(ra-rb)$، یعنی، (به پیمانهٔ n) $ra\equiv rb$. بعکس، اگر (به پیمانهٔ n) $ra\equiv rb$، آنگاه $rn'|(ra-rb)$، از اینرو به ازاء عدد صحیحی چون k، داریم $r(a-b)=rn'k$. اکنون می‌توان قانون حذف در $\mathbf{Z}$ را برای استنتاج $a-b=n'k$ به کار برد. (توجه کنید که $r\neq 0$، زیرا $n=rn'$ مثبت است.) بنابراین (به پیمانهٔ n') $a\equiv b$.

(پ) فرض کنید $r\neq 0$ و $(r, n)=d$. در این صورت $d\neq 0$، $r=r_۱d$، $n=n_۱d$، که در آن $(r_۱, n_۱)=۱$ (قضیهٔ ۵ب). اگر (به پیمانهٔ n) $ra\equiv rb$ آنگاه (به پیمانهٔ $n_۱$) $dr_۱a\equiv dr_۱b$ و، با به کار بردن قسمت (ب) که r با d جایگزین شده‌است،

نتیجه می گیریم که ($r_1 a \equiv r_1 b (n_1)$ به پیمانهٔ n_1). بنا به قسمت (الف)، چون $(r_1, n_1) = 1$، نتیجه می‌شود که $a \equiv b (n_1)$ (به پیمانهٔ n_1).

مثال ۱۰۷. قسمت (پ) از قضیهٔ فوق ازجنبهٔ نظری مهم است و دو قسمت دیگر را به عنوان حالتهای ویژه در بردارد. درعمل، اگر اعداد به کار رفته کوچك باشند، به‌کاربردن قسمت (ب) ساده‌تر است ومعمولا به‌چیزی بیش از آن نیازنداریم. به عنوان مثال، برای حل همنهشتی $198x \equiv 132 (110)$ (به پیمانهٔ ۱۱۰) (یعنی، پیدا کردن همهٔ اعدادصحیح x که به ازاء آنها همنهشتی درست است) اولا مقسوم‌علیه‌های مشترك ۱۹۸، ۱۳۲ و ۱۱۰ را جستجو می کنیم، وسپس قسمت (ب) را به کار می بریم. بدست می آوریم

$$198x \equiv 132 (110) \text{ (به پیمانهٔ ۱۱۰)} \iff 99x \equiv 66 (55) \text{ (به پیمانهٔ ۵۵)}$$

$$\iff 9x \equiv 6 (5) \text{ (به پیمانهٔ ۵)}.$$

اکنون با استفاده از قسمت (الف) و با $r = 3$، می‌توانیم بیشتر ساده کنیم. چون ۳ و ۵ متباین‌اند داریم: $9x \equiv 6$ (به پیمانهٔ ۵) $\iff 3x \equiv 2$ (به پیمانهٔ ۵)، که بهتر به‌نظر می‌آید ولی‌حل‌آن ساده‌تر نیست. روشهای گوناگون دیگری برای تحویل وجود دارد وممکن است‌عملی‌تر ازاین روش‌اخیر باشند. برای‌مثال، چون

$$1 \equiv -4 \text{ (به پیمانهٔ ۵)} \text{ و } 1 \equiv 6 \text{ (به پیمانهٔ ۵)}$$

می بینیم که

$$9x \equiv 6 \text{ (به پیمانهٔ ۵)} \iff -x \equiv 1 \text{ (به پیمانهٔ ۵)} \iff x \equiv -1 \text{ (به پیمانهٔ ۵)}$$

و این همنهشتی را به طورکامل حل می‌کند: همهٔ جوابها اعداد صحیح به صورت $x = 5m - 1$ هستند. البته، اگرمشاهده کنیم که $6 \equiv -4 (5)$ می‌توانیم به‌جای‌آن بدین‌طریق‌استدلال کنیم که $9x \equiv -4 (5) \iff 9x \equiv -1 (5)$ وسپس‌قسمت (الف) قضیه را به‌کار می‌بریم ونتیجه می گیریم که

$$x \equiv -1 \text{ (به پیمانهٔ ۵)} \iff 9x \equiv -1 (5) \text{ (به پیمانهٔ ۵)},$$

زیرا $(5, 9) = 1$. روشی‌سیستماتیك موردنیاز است تادرحالتی‌که اعدادکمتر قابل‌بررسی و رام هستند جانشین این روشهای مربوط به‌حالت خاص شود. هدف بعدی ما یافتن چنین روشی است.

همنهشتی خطی $px \equiv q (n)$ (به پیمانهٔ n) ممکن است هیچ جوابی‌نداشته باشد؛ به‌عنوان مثال $2x \equiv 3 (4)$ (به پیمانهٔ ۴) هیچگاه نمی‌تواند برقرارباشد، چون $3 - 2x$ همیشه فرد است. ازطرف‌دیگر، اگر $px \equiv q (n)$ (به پیمانهٔ n) دارای‌یك جواب باشد، بینهایت جواب دارد. چون اگر به ازاء x خاصی $px \equiv q (n)$ (به‌پیمانهٔ n) درست باشد، آشکارا به ازاء هرعدد صحیح همنهشت با x (به‌پیمانهٔ n) نیز درست است. در واقع این نشان می‌دهد که جوابهای $px \equiv q (n)$ (به‌پیمانهٔ n)، درصورت وجود، تشکیل اتحادی از رده‌های باقیمانده به پیمانهٔ n می‌دهند. با در نظرگرفتن این حقیقت، گوییم که همنهشتی خطی $px \equiv q (n)$ (به پیمانهٔ n) دارای k جواب به پیمانهٔ n است اگر جوابهایش دقیقاً شامل k ردهٔ باقیماندهٔ کامل به پیمانهٔ n

باشند. اینکه ممکن است k بیش از ۱ باشد می‌تواند از همنهشتی (به‌پیمانهٔ ۴) $2x \equiv 2$ دیده شود که نه تنها به ازاء همهٔ (به‌پیمانهٔ ۴) $x \equiv 1$ صدق می‌کند بلکه به وسیلهٔ همهٔ (به‌پیمانهٔ ۴) $x \equiv 3$ صادق است. این همنهشتی دوجواب به پیمانهٔ ۴ دارد.

قضیهٔ ۷ب. (الف) p و n مفروض‌اند. همنهشتی (به‌پیمانهٔ n) $px \equiv 1$ دارای جواب است اگر وفقط اگر $(p, n) = 1$. اگر $(p, n) = 1$، جوابی یکتا به پیمانهٔ n وجود دارد.

(ب) p ، q و n مفروض‌اند. همنهشتی (به‌پیمانهٔ n) $px \equiv q$ دارای جواب است اگر و فقط اگر $d \mid q$، که در آن $d = (p, n)$. اگر $d \mid q$ آنگاه دقیقاً d جواب به‌پیمانهٔ n وجود دارد.

برهان. (الف) این قسمت حالت خاصی از (ب) می‌باشد، ولی شایسته است که در این حالت استدلال ساده‌ای ارائه شود. همنهشتی (به‌پیمانهٔ n) $px \equiv 1$ دارای جواب است اگر وفقط اگر اعداد صحیح x و y به قسمی وجود داشته باشند که $px + ny = 1$. اما، بنا به قضیهٔ ۵ ب (پ)، چنین اعداد صحیح وقتی وفقط وقتی وجود دارند که $(p, n) = 1$. فرض کنید که $(p, n) = 1$ بسادگی دیده می‌شود که جواب به پیمانهٔ n یکتاست، چون اگر (به‌پیمانهٔ n) $px \equiv 1$ و (به‌پیمانهٔ n) $px' \equiv 1$ آنگاه (به‌پیمانهٔ n) $px \equiv px'$ و بنابراین، بنا به قضیهٔ ۷آ (الف)، (به‌پیمانهٔ n) $x \equiv x'$.

(ب) استدلال مشابه فوق بوده ولی کمی مشکلتر است. همنهشتی (به‌پیمانهٔ n) $px \equiv q$ دارای جواب است $\Leftrightarrow (\exists x, y \in \mathbf{Z})(px + ny = q) \Leftrightarrow (p, n) \mid q$، بنابه نتیجهٔ قضیهٔ ۵آ. فرض کنید که $d \mid q$، $d = (p, n)$، بنابراین می‌توان نوشت: $p = dp_1$، $n = dn_1$، $q = dq_1$ و در این صورت بنا به قضیهٔ ۷آ (ب)، داریم

$$px \equiv q \text{ (به‌پیمانهٔ } n) \iff p_1 x \equiv q_1 \text{ (به‌پیمانهٔ } n_1)$$

ولی (بنا به قضیهٔ ۵ب (ب)) $(p_1, n_1) = 1$ از اینرو اگر x و x' دو جواب باشند آنگاه (به‌پیمانهٔ n_1) $p_1 x \equiv p_1 x'$ و بنابراین، بنا به قضیهٔ ۷آ (الف)، (به‌پیمانهٔ n_1) $x \equiv x'$. بنابراین در این حالت همنهشتی دارای جوابی یکتا به پیمانهٔ n_1 است. باقی می‌ماند که نشان دهیم هر ردهٔ باقیمانده به‌پیمانهٔ n_1 شامل d ردهٔ باقیمانده به‌پیمانهٔ $n = dn_1$ می‌باشد. از اینرو فرض کنید R یک ردهٔ باقیمانده به‌پیمانهٔ n_1 باشد. واضح است که R اتحادی از رده‌های باقیمانده به پیمانهٔ n است، زیرا (به‌پیمانهٔ n_1) $x \equiv y \Rightarrow$ (به‌پیمانهٔ n) $x \equiv y$. ازاینرو بایدفقط تعداد اعدادصحیحی ازمجموعهٔ مقادیر $0, 1, 2, \ldots, n-1$ را که در R قراردارند، بشماریم. فرض کنید r عضویکتایی از R درمجموعهٔ مقادیر $0 \leqslant r < n_1$ باشد. دراین‌صورت اعدادصحیح مورد نظر عبارت‌اند از: r ، $r + n_1$ ، $r + 2n_1$ ، ... ، $r + (d-1)n_1$ ، و دقیقاً تعداد آنها d است. (عدد بعدی $r + dn_1 = r + n$ «خیلی» بزرگ است.)

اکنون می‌توانیم هر همنهشتی خطی (به‌پیمانهٔ n) $px \equiv q$ را حل کنیم. نخست $(p, n) = d$ را به وسیلهٔ الگوریتم اقلیدس محاسبه کنید. اگر $d + q$ هیچ جوابی وجود ندارد. چنانچه $d \mid q$، الگوریتم را برای بیان q به‌صورت $q = px + ny$ به‌کار ببرید. این یک جواب x

را به دست می‌دهد، و مجموعهٔ کامل جوابها شامل همهٔ اعداد صحیح همنهشت با این x به پیمانهٔ n_1 است، که $n=dn_1$. برای مقادیر کوچك p ، q و n راههای کوتاهتری همانند مثال ۱.۷ ممکن است وجود داشته باشد .

مثال ۲.۷. برای حل $27x\equiv 13 \pmod{60}$، ملاحظه کنید که $3=(60,27)$ و $3\nmid 13$، ازاینرو هیچ‌جوابی وجود ندارد. برای حل $27x\equiv 15 \pmod{60}$ ، چون حالا $3\mid 15$، چنین استدلال می‌کنیم:

$$27x\equiv 15 \pmod{60} \iff 9x\equiv 5 \pmod{20}$$
$$\iff 9x\equiv 45 \pmod{20}$$
$$\iff x\equiv 5 \pmod{20}$$

از اینرو جوابها به‌پیمانهٔ ۶۰ عبارت‌اند از : $x\equiv 5, 25, 45 \pmod{60}$.

مثال ۳.۷. برای حل $224x\equiv 154 \pmod{385}$ ، الگوریتم اقلیدس را به‌کار می‌بریم:

$$385=224\times 2-63$$
$$224=63\times 4-28$$
$$63=28\times 2+7$$

بنابراین $7=(224,385)$ و $7\times 22=154$، لذا جواب موجوداست. همچنین، به‌کمك الگوریتم داریم،

$$7=63-28\times 2=224\times 2-63\times 7=385\times 7-224\times 12,$$

از اینرو $154=385\times 7\times 22-224\times 12\times 22$. این یك جواب

$$x=-12\times 22=-264\equiv 121 \pmod{385}$$

به‌دست می‌دهد. بنابه قضیهٔ ۷ب، تعداد ۷ جواب به پیمانهٔ ۳۸۵ وجود دارد و در فواصل مساوی $\frac{385}{7}=55$ ازهم قرار گرفته‌اند. بنابراین جوابها عبارت‌اند از :

$$x\equiv 11, 66, 121, 176, 231, 286, 341 \pmod{385}$$

حل دستگاه همنهشتیهای خطی بمراتب مشکلتر است. به‌عنوان مثال ، یك جفت از همنهشتیها با دو مجهول را درنظر بگیرید ،

$$\begin{cases} ax+by\equiv c & (\text{به پیمانهٔ } n) \qquad (1)\\ a'x+b'y\equiv c' & (\text{به پیمانهٔ } n) \qquad (2)\end{cases}$$

در مورد معادلات روش بدین ترتیب است که با به‌کاربردن (۱) x را از (۲) حذف کرده ، معادله را برای y حل‌می‌کنیم وسپس (۱) را برای‌پیدا کردن x به‌کار می‌بریم. اگر $a\neq 0$ این روش را می‌توان توجیه کرد، ولی در مورد همنهشتیها موانعی وجود دارد . نمی‌توانیم

طرفین را بر a تقسیم کنیم چون فقط بایستی با اعداد صحیح کار کنیم. از اینرو بهترین کاری که می‌توانیم انجام دهیم آن است که (۱) و (۲) را در اعداد صحیح مناسب ضرب کنیم تا ضرایب x مساوی گردند. ولی، اگر همنهشتیها را در اعداد صحیح کـه با n متباین نیستند ضرب کنیم ممکن است جوابهای همنهشتیها را به‌طور فردی وشاید هم جوابهای کل دستگاه را تغییردهیم. از اینرو ممکن‌است حذف امکان‌پذیر نباشد. اگر اتفاقاً n اول باشد این‌وضع پیش نمی‌آید (همان‌طور که بعداً خواهیم دید) و همین روش معمولی، قابل اعمال است. در غیراین صورت باید با احتیاط زیادی گام برداشت. بسط رسمی نظریهٔ چنین همنهشتیهایی، برای ما نافع نیست و به جای آن خود را به‌دومثال قانع می‌کنیم.

مثال ۴.۷. برای حل دستگاه

$$\left\{\begin{array}{l} 3x-4y\equiv 2 \ (\text{به‌پیمانهٔ } 7) \\ 5x+6y\equiv 3 \ (\text{به‌پیمانهٔ } 7) \end{array}\right\} \qquad (3)$$

می‌توانیم ، بدون تغییر جوابهایشان ، اولین همنهشتی را در ۵ و دومی را در ۳ ضرب کنیم. از اینرو داریم

$$(3) \longleftrightarrow \left\{\begin{array}{l} 15x-20y\equiv 10 \ (\text{به‌پیمانهٔ } 7) \\ 15x+18y\equiv 9 \ (\text{به‌پیمانهٔ } 7) \end{array}\right\}$$

$$\longleftrightarrow \left\{\begin{array}{l} 15x-20y\equiv 10 \ (\text{به‌پیمانهٔ } 7) \\ 38y\equiv -1 \ (\text{به‌پیمانهٔ } 7) \end{array}\right\}$$

حال داریم

$38y\equiv -1$ (به‌پیمانهٔ ۷) $\longleftrightarrow 3y\equiv -1\equiv 6$ (به‌پیمانهٔ ۷) $\longleftrightarrow y\equiv 2$ (به‌پیمانهٔ ۷)

از اینرو جوابهای (۳) به‌وسیلهٔ $y\equiv 2$ (به‌پیمانهٔ ۷) و $15x-20\equiv 10$ (به‌پیمانهٔ ۷) داده می‌شوند. بنابراین جواب یکتای $x\equiv 1$ ، $y\equiv 2$ (به‌پیمانهٔ ۷) وجود دارد.

مثال ۵.۷. برای حل دستگاه

$$\left\{\begin{array}{l} 4x-6y\equiv 2 \ (\text{به‌پیمانهٔ } 30) \\ 5x+22y\equiv 7 \ (\text{به‌پیمانهٔ } 30) \end{array}\right\}$$

نمی‌توانیم بدون تغییر جوابها x را حذف کنیم. ولی چون $2=(30,22)$ ، می‌توانیم یك ضریب ۲ برای y در معادلهٔ دوم ساخته و سپس y را حذف کنیم. برای انجام این امر لازم است $22k\equiv 2$ (به‌پیمانهٔ ۳۰) را حل کنیم و ، هنگامی که دانستیم $k\equiv 11$ یك جواب است ، با توجه به اینکه $1=(30,11)$ ، معادلهٔ دوم را در ۱۱ ضرب می‌کنیم. بنابراین

$$\left\{\begin{array}{l}4x-6y\equiv 2\ (\text{به پیمانهٔ }30)\\ 5x+22y\equiv 7\ (\text{به پیمانهٔ }30)\end{array}\right\}\Longleftrightarrow\left\{\begin{array}{l}4x-6y\equiv 2\ (\text{به پیمانهٔ }30)\\ 25x+2y\equiv 17\ (\text{به پیمانهٔ }30)\end{array}\right\}$$

$$\Longleftrightarrow\left\{\begin{array}{l}25x+2y\equiv 17\ (\text{به پیمانهٔ }30)\\ 19x\equiv 23\ (\text{به پیمانهٔ }30)\end{array}\right\}$$

توجه کنید که در آخرین مرحله نباید اولین همنهشتی $4x-6y\equiv 2$ را به جای $25x+2y\equiv 17$ نگه‌داریم، زیرا درآن صورت پس از ضرب آن در ۳ قادر نخواهیم بود که $25x+2y\equiv 17$ را مجدداً به‌دست آوریم. از اینجا به بعد دیگر بسادگی می‌توان جواب یکتای (به پیمانهٔ ۳۰) $x\equiv -13$ را برای همنهشتی (به پیمانهٔ ۳۰) $19x\equiv 23$ به‌دست آورد و از آنجا دو دستگاه جواب به پیمانهٔ ۳۰ از جفت همنهشتی اصلی را یافت:

$$y=6\ ,\ x=-13\ ;\quad y=-9\ ,\ x=-13\ .$$

روش دیگر ما حذف به‌وسیلهٔ روشهای استانده برای معادلات خطی می‌باشد با کسب اطمینان از اینکه حداقل درهر مرحله، همنهشتیهای جدید ازقبلی‌ها نتیجه می‌شوند گرچه عکس آن صادق نباشد. درپایان استدلال، مجموعه‌ای ازهمنهشتیها خواهیم داشت که جوابهایشان نه فقط شامل همهٔ جوابهای اصلی هستند، بلکه ممکن است تعدادی جوابهای اضافی نیز داشته باشند. دراین مرحله بایستی جایگزینی برگشتی انجام داد، تا دریابیم کدام‌یك ازجوابها حقیقی‌اند. مثلا برای همان دستگاه همنهشتی می‌توان بدین طریق استدلال کرد.

$$\left\{\begin{array}{l}4x-6y\equiv 2\ (\text{به پیمانهٔ }30)\\ 5x+22y\equiv 7\ (\text{به پیمانهٔ }30)\end{array}\right\}\Rightarrow\left\{\begin{array}{l}20x-30y\equiv 10\ (\text{به پیمانهٔ }30)\\ 20x+88y\equiv 28\ (\text{به پیمانهٔ }30)\end{array}\right\}$$

$$\Rightarrow\left\{\begin{array}{l}20x\equiv 10\ (\text{به پیمانهٔ }30)\\ 28y\equiv 18\ (\text{به پیمانهٔ }30)\end{array}\right\}$$

این دستگاه اخیر نتیجه می‌دهد (به پیمانهٔ ۳۰) $y\equiv -9$ یا $y\equiv 6$ ولی، متأسفانه، ده مقدار ممکن برای x (به پیمانهٔ ۳۰) به دست می‌دهد، که در واقع نه تای آنها جوابهای همنهشتیهای اصلی را نمی‌دهند. البته، با مشاهدهٔ اینکه همنهشتیهای اصلی نیز (به وسیلهٔ تفریق) نتیجه می‌دهند که $x+28y\equiv 5$، می‌توان بلافاصله همهٔ جوابها بغیر از دو تا را حذف کرد، و بنابراین $x\equiv 5-28\times 9$ یا $x\equiv 5+28\times 6$. هردوی اینها (به پیمانهٔ ۳۰) $x\equiv -13$ را به‌دست می‌دهند و نهایتاً همان جوابهای فوق را به‌دست می‌آوریم.

اکنون به‌دستگاه همنهشتیهای خطی ازنوع متفاوتی می‌پردازیم ــ چندین همنهشتی با یك مجهول ولی با پیمانه‌های متفاوت. در اینجا هیچ شباهتی با دستگاه معادلات جهت راهنمایی خود نداریم، ولی حالت خاص مهمی وجود دارد که بدون زحمت زیادمی‌توانیم مسئله را به‌طور کامل حل کنیم. این حالتی که پیمانه‌های متفاوت دو به‌دو متباین‌اند. قضیهٔ معروف به باقیماندهٔ چینی اطلاعات لازم را به ما می‌دهد.

قضیهٔ ۷پ. فرض کنید m ، n اعداد صحیح مثبت باشند با $(m, n) = ۱$. همچنین فرض کنید a و b اعداد صحیح دلخواه باشند. در این صورت همنهشتیهای

$$\left\{\begin{array}{l} x \equiv a \ (m \text{ به پیمانهٔ}) \\ x \equiv b \ (n \text{ به پیمانهٔ}) \end{array}\right\}$$

دارای جوابی مشترك است، و مجموعهٔ جوابهای مشترك ردهٔ واحدی از باقیماندهها به پیمانهٔ mn می‌باشد.

برهان. واضح است که، اگر x جواب مشترکی باشد وچنانچه ($x' \equiv x (mn$ به پیمانهٔ x'، آنگاه x' نیز یك جواب مشترك است. بعکس، اگر x و x' دو جواب مشترك باشند آنگاه $m|(x - x')$ و $n|(x - x')$، از اینرو، بنا به قضیهٔ ۵ب (ث)، $mn|(x - x')$، چون $(m, n) = ۱$). بنابراین، اگر جوابهای مشترکی وجود داشته باشند، تشکیل یك ردهٔ واحد از باقیماندهها به پیمانهٔ mn می‌دهند، و تنها مسئله وجود جوابهاست. دو برهان می‌آوریم. در اولین برهان از گروههای $A = \mathbf{Z}/m\mathbf{Z}$ و $B = \mathbf{Z}/n\mathbf{Z}$ که دوری و بترتیب از مرتبه‌های m و n هستند، استفاده می‌شود. چون $(m, n) = ۱$، قضیهٔ غ‌ب به ما می‌گوید که گروه حاصلضرب $A \times B$، دوری و از مرتبهٔ mn است و (به‌طور جمعی) به‌وسیلهٔ عنصر $g = (\langle ۱ \rangle_m, \langle ۱ \rangle_n)$ تولید می‌شود. در اینجا $\langle ۱ \rangle_m$ ردهٔ باقیماندهٔ (m به پیمانهٔ) شامل ۱ بوده و مولدی از A است؛ به‌همین نحو $\langle ۱ \rangle_n$ گروه B را تولید می‌کند.

توانهای (جمعی) g عبارت‌اند از :

$$rg = (r\langle ۱ \rangle_m, r\langle ۱ \rangle_n) = (\langle r \rangle_m, \langle r \rangle_n)$$

و اینها $A \times B$ را کاملا می‌سازند. بنابراین، به ازاء اعداد صحیح دلخواه a ، b ، عدد صحیحی مانند r به قسمی وجود دارد که

$$(\langle r \rangle_m, \langle r \rangle_n) = (\langle a \rangle_m, \langle b \rangle_n)$$

و این r همان جواب مورد نظر است.

بهرحال، این استدلال زیبا به پیدا کردن جواب کمك نمی‌کند، از اینرو برهان سودمندتری نیز می‌آوریم. چون $(m, n) = ۱$ ، (به وسیلهٔ الگوریتم اقلیدس) اعداد صحیح p و q را به قسمی می‌توانیم پیدا کنیم که $mp + nq = ۱$. جوابی از همنهشتیها را در حالت ویژهٔ $a = ۱$ ، $b = ۰$ جستجو می‌کنیم، یعنی $x_۱$ ای را جستجو می‌کنیم به قسمی که $x_۱ \equiv ۱ (m$ به پیمانهٔ) و $x_۱ \equiv ۰ (n$ به پیمانهٔ). واضح است که $x_۱ = nq$ چنین جوابی است. به همین نحو، $x_۲ = mp$ جوابی از $x_۲ \equiv ۰ (m$ به پیمانهٔ) و $x_۲ \equiv ۱ (n$ به پیمانهٔ) می‌باشد. باحل این دو حالت می‌توانیم آنها را برای به دست آوردن جوابی در حالت کلی ترکیب کنیم، زیرا آشکار است که اگر قراردهیم $x = ax_۱ + bx_۲$ ، داریم

$$x \equiv a \times ۰ + b \times ۱ (n \text{ به پیمانهٔ}) \text{ و } x \equiv a \times ۱ + b \times ۰ (m \text{ به پیمانهٔ})$$

وحکم برقرار است.

نتیجهٔ ۱. فرض کنید n_1 ، n_2 ، ... ، n_r اعداد صحیح مثبت دوبه‌دو متباین باشند. فرض کنید a_1 ، a_2 ، ... ، a_r اعداد صحیح دلخواه باشند. دراین‌صورت همنهشتیهای (به‌پیمانهٔ n_i) $x \equiv a_i$، $i = 1, 2, \ldots, r$ ، دارای جواب مشترکی هستند و جوابهای مشترک تشکیل یك ردهٔ واحد از باقیمانده‌ها به‌پیمانهٔ n می‌دهند ، که $n = n_1 n_2 \cdots n_r$.

برهان. از استقراء روی r استفاده می‌کنیم. اگر $r = 1$ ، چیزی برای اثبات وجود ندارد . چنانچه $r = 2$ ، ادعا همانند قضیهٔ فوق است. به ازاء $r > 2$ ، می‌توان فرض استقراء را برای به دست‌آوردن جوابی مانند $x = a_0$ از اولین $r - 1$ همنهشتی به‌کاربریم. مجموعهٔ همهٔ چنین‌جوابهایی یك‌ردهٔ باقیمانده به‌پیمانهٔ $n_0 = n_1 n_2 \cdots n_{r-1}$ است. بنابراین‌جوابهای مشترك همهٔ r همنهشتی دقیقاً جوابهای مشترك (به‌پیمانهٔ n_0) $x \equiv a_0$ و (به‌پیمانهٔ n_r) $x \equiv a_r$ هستند. به شرطی که بدانیم $n_0 = n_1 n_2 \cdots n_{r-1}$ و n_r متباین‌اند ،نتیجه به وسیلهٔ کاربرد دیگری از قضیه به دست می‌آید. قبلا این به عنوان تمرینی آمده است (تمرین ۸، فصل۵) ولی برای کامل بودن بحث ، برهانی ازآن را در اینجا می‌آوریم . اگر $(n_0, n_r) \neq 1$ آنگاه عامل‌مشترکی مانند d از n_0 و n_r وجود دارد‌که یکه‌نیست، این d برعدد اولی مانند p قابل قسمت است ، و داریم $p | n_r$ و $p | n_0 = n_1 n_2 \cdots n_{r-1}$. بنابه قضیهٔ ۵پ (ت) ، به ازاء اندیسی چون i درمجموعهٔ $1 \leqslant i \leqslant r - 1$ ، $p | n_i$ و بنابراین n_i و n_r متباین نیستند ، که متناقض با فرض است. این تناقض ثابت می‌کند‌که $(n_0, n_r) = 1$.

نتیجهٔ ۲. (قضیهٔ عمومی‌باقیماندهٔ‌چینی). فرض کنید n_1 ، n_2 ، ... ، n_r اعداد صحیح مثبت دوبه‌دو متباین باشند. فرض کنید b_i ، c_i $(i = 1, 2, \ldots, r)$ اعداد صحیح دلخواه باشند. دراین‌صورت همنهشتیهای (به‌پیمانهٔ n_i) $b_i x \equiv c_i$ $(i = 1, 2, \ldots, r)$ دارای‌جوابی‌مشترك‌اند اگر و فقط اگر هرکدام ازآنها دارای جواب باشد.

برهان. اگر همنهشتی i ام دارای جوابی مانند a_i باشد آنگاه هر (به‌پیمانهٔ n_i) $x \equiv a_i$ نیز یك جواب است. چنانچه به ازاء هر i ، جواب a_i وجود داشته باشد، آنگاه نتیجهٔ۱ وجود x ای راکه در همهٔ همنهشتیها صدق نماید، تضمین می‌کند .

مثال ۶.۷. برای حل دستگاه همنهشتیهای (به‌پیمانهٔ ۱۰) $x \equiv 3$ ، (به‌پیمانهٔ ۷) $2x \equiv 5$ و (به‌پیمانهٔ ۹) $6x \equiv 3$ اولا تحقیق می‌کنیم کـه هریك ازآنها جوابهایی دارند و آنها را به همنهشتیهای معادل تحویل می‌کنیم :

(به‌پیمانهٔ ۳) $x \equiv 2$ ، (به‌پیمانهٔ ۷) $x \equiv -1$ ، (به‌پیمانهٔ ۱۰) $x \equiv 3$.

پیمانه‌ها دوبه‌دو متباین‌اند، از اینرو جوابهای مشترك تشکیل ردهٔ واحدی از باقیمانده‌ها به پیمانهٔ ۲۱۰ می‌دهند ، وفقط لازم است‌که یك جواب به دست‌آید. واضح است‌کـه آخرین دو همنهشتی جوابهای مشترك (به‌پیمانهٔ ۲۱) $x \equiv -1$ دارند، از اینرو جواب مشترکـی از این‌همنهشتی و(به‌پیمانهٔ ۱۰) $x \equiv 3$ رامی‌خواهیم. اکنون $1 = 2 \times 10 - 1 \times 21$ ازاینرو

$x_1 = -۲۰$ و $x_2 = ۲۱$ جوابهای (به پیمانهٔ ۲۱) $x_1 \equiv ۱$ ، (به پیمانهٔ ۱۰) $x_1 \equiv ۰$ ، (به پیمانهٔ ۲۱) $x_2 \equiv ۰$ ، (به پیمانهٔ ۱۰) $x_2 \equiv ۱$ هستند. بنابراین

$$x = (-۲۰) \times (-۱) + ۲۱ \times ۳ = ۸۳$$

جواب موردنظرماست. جوابهای همنهشتیهای اصلی عبارت‌انداز : (به پیمانهٔ ۲۱۰) $x \equiv ۸۳$.

قبلا ارتباط بین همنهشتیها و گروههای دوری روشن‌شده است. از این ارتباط می‌توان در دوجهت بهره‌برداری کرد واکنون به‌مطالعهٔ بیشتری درساخت گروههای دوری می‌پردازیم ــ مولدهایشان، زیرگروههایشان ومرتبه‌های عناصرشان ــ که در آن نظریهٔ همنهشتیها نقش مهمی را ایفا می‌کند. قضایای مجرد منتج را می‌توان برای به دست آوردن اطلاعاتی در مورد طبیعت اعداد صحیح از جنبهٔ نظریهٔ اعداد، به‌کارگرفت.

قضیهٔ ۷ ت. فرض کنید G یك گروه دوری از مرتبهٔ n باشد ، که به وسیلهٔ عنصر g تولید شده است. دراین صورت g^s گروه G را تولید می‌کند اگر وفقط اگر $(s, n) = ۱$.

برهان. فرض کنید $h = g^s$. اگر h گروه G را تولیدکند ، آنگاه g بایستی توانی از h باشد. بعکس ، اگر g توانی از h باشد، آنگاه هرعنصر G که توانی از g است ، توانی از h نیزهست. بنابراین h گروه G را تولیدمی‌کند اگروفقط اگر عددصحیحی مانند x به‌قسمی وجود داشته باشدکه $g = h^x = g^{sx} \iff sx \equiv ۱ \ (n)$. اما (به پیمانهٔ n) $g^{sx} = g$ ، زیرا g دارای مرتبهٔ n است (قضیهٔ ۴ ت را ببینید). این همنهشتی دارای جواب x است اگر وفقط اگر $(s, n) = ۱$ (قضیهٔ ۷ ب).

تعریف. تابع اویلر[1] φ روی مجموعهٔ اعداد صحیح مثبت به وسیلهٔ قانون زیر تعریف می‌شود : $\varphi(n)$ برابر است با تعداد اعداد صحیح r در مجموعهٔ $۱ \leqslant r \leqslant n$ که با n متباین . بنابراین،مثلا، $\varphi(۱) = ۱$ ، $\varphi(۲) = ۱$ ، $\varphi(۳) = ۲$ ، $\varphi(۴) = ۲$ ، $\varphi(۵) = ۴$ و $\varphi(۶) = ۲$. ازاین به بعد علامت φ را برای این تابع به‌کار خواهیم برد.

نتیجه . در یك گروه دوری G از مرتبهٔ n ، تعداد عناصری که (بتنهایی) G را تولید می‌کنند $\varphi(n)$ است.

برهان. عناصر G را می‌توان ، به‌ازاء $s = ۱ ، ۲ ، \ldots ، n$ ، به صورت g^s نوشت و ، بنابه قضیهٔ فوق ، آن عده از این عناصرکه G را تولید می‌کنند، آنهایی هستندکه در مورد آنها $(s, n) = ۱$.

مثال ۷.۷. یك ریشهٔ n ام ۱ در $\mathbf{C}$ یك ریشهٔ n ام اولیهٔ ۱ نامیده می‌شود اگر ، به ازاء هر

1. Euler

$k<n$ ، یك ریشهٔ k ام ۱ نباشد ، به عبارت دیگر ، اگر مرتبه‌اش دقیقاً برابر n باشد. ولی این مثل آن است که بگوییم آن ریشه ، گروه دوری P_n از همهٔ ریشه‌های n ام ۱ را تولید می‌کند. گروه P_n دارای مرتبهٔ n است، ازاینرو تعداد ریشه‌های n ام اولیهٔ ۱ مساوی $\varphi(n)$ است. ریشه‌های اولیه عبارت‌اند از $e^{\frac{2\pi is}{n}}$ ، که در آن $1\leqslant s\leqslant n$ و $(s,n)=1$.

قضیهٔ ۷ ث. اگر $(m,n)=1$ ، آنگاه $\varphi(mn)=\varphi(m)\varphi(n)$.

برهان. برای این قضیه برهانهای زیادی وجود دارد، ولی شاید زیباترین آنها برهانی باشد که مشخصهٔ $\varphi(n)$ را به‌عنوان تعداد مولدها در یك گروه دوری به‌کار می‌برد. فرض کنیم گروههای دوری A و B بترتیب از مرتبه‌های m و n باشند. بنا به قضیهٔ ۶ ب ، چون $(m,n)=1$ ، گروه $A\times B$ دوری و از مرتبهٔ mn است . مولدهای $A\times B$ عناصری مانند (a,b) هستند، که a و b بترتیب مولدهای A و B باشند . بنا به قضیهٔ ۷ ت ، چون $\varphi(m)$ امکان انتخاب برای a و $\varphi(n)$ امکان انتخاب برای b وجود دارد، تعداد مولدهای متفاوت $A\times B$ برابر $\varphi(m)\varphi(n)$ است. اما، مجدداً بنا به قضیهٔ ۷ ت ، این عدد برابر است با $\varphi(mn)$.

نتیجهٔ ۱. اگر n_1 ، n_2 ، ... ، n_r اعداد صحیح مثبت دو به دو متباین باشند، آنگاه

$$\varphi(n_1n_2\cdots n_r)=\varphi(n_1)\varphi(n_2)\cdots\varphi(n_r)$$

برهان. اثبات، استقراء ساده‌ای روی r است، که با به‌کاربردن قضیهٔ فوق و اینکه $n_1n_2\cdots n_{r-1}$ با n_r متباین است، انجام می‌شود. (برهان قضیهٔ ۷ پ و نتیجهٔ ۱ را ببینید.)

نتیجهٔ ۲. به ازاء هر $n>0$ ،

$$\varphi(n)=n\prod_{p\mid n}\left(1-\frac{1}{p}\right)$$

که در آن حاصلضرب برروی همهٔ مقسوم‌علیه‌های اول متمایز p از n گرفته شده است.

برهان . فرض کنید p_1 ، p_2 ، ... ، p_r مقسوم علیه‌های اول متمایز n باشند و فرض کنید $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ $(\alpha_i\geqslant 1)$. در این صورت $p_i^{\alpha_i}$ و $p_j^{\alpha_j}$ متباین‌اند اگر $i\neq j$ (تمرین) از اینرو بنا به نتیجهٔ ۱ ،

$$\varphi(n)=\sum_{i=1}^{r}\varphi(p_i^{\alpha_i})\ .$$

حال اگر p اول باشد آنگاه $\varphi(p^\alpha)$ $(\alpha\geqslant 1)$ برابر تعداد اعداد صحیح s در مجموعهٔ $1\leqslant s\leqslant p^\alpha$ می‌باشد که بر p قابل قسمت نیستند. بوضوح دیده می‌شود تعدادی که بر p

قابل قسمت‌اند برابر است با p^α . $\frac{1}{p}$ ، از اینرو

$$\varphi(p^\alpha) = p^\alpha\left(1-\frac{1}{p}\right).$$

بنابراین

$$\varphi(n) = \prod_{i=1}^{r}\varphi(p_i^{\alpha_i}) = \prod_{i=1}^{r}p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right) = n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right).$$

قضیهٔ ۷ ج. فرض‌کنید G یك گروه دوری از مرتبهٔ n باشد ، که به وسیلهٔ عنصر g تولید شده است. در این صورت

(الف) هر زیرگروه G دوری است و مرتبه‌اش مقسوم‌علیهی از n است.

(ب) عنصر g^r دارای مرتبهٔ $\frac{n}{(n,r)}$ است.

(پ) تعداد جوابهای معادلهٔ $x^m = e$ در G برابر است با (m,n).

(ت) به ازاء هر مقسوم‌علیه d از n دقیقاً یك زیرگروه ازمرتبهٔ d وجود دارد.

(ث) تعداد عناصر G که دقیقاً از مرتبهٔ d باشند عبارت است از :

$$\begin{cases}\varphi(d) \text{ ، } d|n & \text{اگر}\\ 0 \text{ ، } d\nmid n & \text{اگر}\end{cases}$$

برهان. (الف) قبلا این قسمت‌ثابت شده است. قضیهٔ ۴ پ ، نتیجه ، و قضیهٔ ۴ ج ، نتیجه۱ را ملاحظه کنید.

(ب) فرض کنید $h = g^r$. در این صورت $h^s = g^{rs} = e \iff n|rs$. اگر $(n,r) = d$ آنگاه $r = dr_1$ ، $n = dn_1$ ، با $(n_1, r_1) = 1$. بنابراین

$$n|rs \iff dn_1|dr_1s \iff n_1|r_1s \iff n_1|s \text{ ،}$$

و نتیجه می‌شود که مرتبه h برابر است با $n_1 = \frac{n}{d}$.

(پ) فرض کنید $(m,n) = c$ و c را به‌صورت $c = ma + nb$ بنویسید، که درآن a و b اعداد صحیح‌اند. چون ، به ازاء هر $x \in G$ ، $x^n = e$ ، داریم ، هرجواب $x^m = e$ در معادلهٔ $x^c = x^{ma+nb} = e^ae^b = e$ صدق می کند . بعکس ، اگر $x^c = e$ ، آنگاه ، چون $c|m$ ، داریم $x^m = e$. بنابراین فقط نیاز داریم که جوابهای $x^c = e$ را بشماریم ، وچون $c|n$ واضح است که دقیقاً c تا جواب موجود است، یعنی همهٔ g^r ها به ازاء

$$r=\frac{n}{c},\ \frac{2n}{c},\ldots,\frac{cn}{c}.$$

(ت) فرض کنید $d|n$. در این صورت عنصر $h=g^{\frac{n}{d}}$ دقیقاً دارای مرتبهٔ d است واز اینرو زیرگروهی دوری مانند H ازمرتبهٔ d تولید می‌کند. باید نشان دهیم که زیرگروه دیگری وجودندارد. حال گوییم هرعنصر H در $x^d=e$ صدق می‌کند، وبنابه قسمت (پ) تعدادکل جوابهای $x^d=e$ در G برابراست با $(n,d)=d$. بنابراین همهٔ جوابها در H هستند. بالاخص هرعنصر ازمرتبهٔ d در H قرار دارد و ازاینرو همهٔ عناصر از مرتبهٔ d همان زیرگروه H را تولید می‌کنند.

(ث) این قسمت بلافاصله نتیجه می‌شود. اگر $d|n$، همهٔ عناصر ازمرتبهٔ d مولد های زیرگروه یکتای H از مرتبهٔ d هستند، از اینرو، بنابه قضیهٔ ۷ ت، دقیقاً $\varphi(d)$ تا از آنها وجود دارد. اگر $d\nmid n$، بنابه قسمت (الف) یا (ب)، هیچ عنصری از مرتبهٔ d وجود ندارد.

نتیجه. به ازاء هر عددصحیح مثبت n، $\sum_{d|n}\varphi(d)=n$.

برهان. جمع‌یابی بر روی همهٔ مقسوم‌علیه‌های متمایز d از n می‌باشد. بنابه قسمت (ث) قضیهٔ فوق، به ازاء هرچنین d، تعداد عناصر در G دقیقاً از مرتبهٔ d برابر است با $\varphi(d)$. بنابراین جمع فوق تعدادکل عناصر G است، زیرا هر عنصر دارای مرتبه‌ای است که n را عاد می‌کند.

مثال ۸.۷. فرض کنید $G=P_n$ گروه ریشه‌های n ام ۱ در $\mathbf{C}$ باشد. دراین صورت به ازاء هر $d|n$، P_d زیرگروه مرتبهٔ d است. به همین نحو، جوابهای $x^m=1$ در G آن عده از ریشه‌های m ام ۱ اندکه ریشه‌های n ام ۱ نیزهستند. بنابراین آنهاعنصر $P_m\cap P_n$ می‌باشند، که زیرگروهی از هریك از P_n و P_m است. بنابه قسمت (پ) از قضیهٔ فوق، این گروه دارای‌مرتبهٔ (m,n) است‌ازاینرو به‌ازاء هر m و n باید داشته‌باشیم $P_n\cap P_m=P_{(m,n)}$. این نتیجه را می‌توان مستقیماً در $\mathbf{C}$ ثابت‌کرد وآن را برای ارائهٔ برهان دیگری از قضیهٔ‌فوق که به نظر ساده‌تر از برهان داده شده می‌رسد، به‌کارگرفت. به‌همین نحو، می‌توان نتیجهٔ فوق را به وسیلهٔ شمارش همهٔ ریشه‌های n ام ۱ در $\mathbf{C}$ برطبق مرتبه‌هایشان «ثابت»کرد که هرکدام ریشهٔ d ام اولیه‌یی برای $d|n$ یکتاست، و $\varphi(d)$ ریشهٔ d ام اولیه در $\mathbf{C}$ وجوددارد، که تمامی آنها در میان ریشه‌های n ام قراردارند. اما واقعاً این روش درست نیست زیرا فرض می‌کندکه همهٔ گروههای دوری متناهی از هر مرتبه‌ای زیرگروه یك‌گروه بزرگ T هستند و برای ساختن این T، لازم است‌که از دستگاه اعداد حقیقی یا مختلط استفاده‌کنیم. این مطلب، موضوعی عمیق‌تر و پیچیده‌تر از ساخت گروههای دوری است. روش طبیعی

بررسی توأم گروههای دوری متناهی آن است که آنها را به‌عنوان گروههای خارج قسمت از یك گروه بزرگ، یعنی $\mathbf{Z}$، در نظر بگیریم.

تمرینها

۱. همنهشتیهای زیر را حل کنید:

(الف) $11x \equiv 18 \pmod{25}$ (به پیمانهٔ ۲۵)؛

(ب) $36x \equiv 168 \pmod{192}$ (به پیمانهٔ ۱۹۲).

۲. کوچکترین مضرب مثبت ۸۴ را که آخرین سه‌رقمش (در نماد دهدهی) ۸۳۲ است پیدا کنید.

۳. دستگاه همنهشتیهای زیر را حل کنید،

$$\begin{cases} x \equiv 3 & \text{(به پیمانهٔ ۱۸)} \\ 3x \equiv 19 \pmod{35} & \text{(به پیمانهٔ ۳۵)} \end{cases}.$$

۴. دستگاه همنهشتیهای زیر را حل کنید،

$$\begin{cases} 5x \equiv 21 & \text{(به پیمانهٔ ۴۸)} \\ 6x \equiv 10 & \text{(به پیمانهٔ ۷۰)} \\ 7x \equiv 35 & \text{(به پیمانهٔ ۱۰۰۱)} \end{cases}.$$

۵. حوادث A و B به طور منظم، بترتیب در فواصل ۴ روز و ۵ روز رخ می‌دهند. در یك سال معین، حادثهٔ A در روز یکشنبهٔ اول ژانویه و حادثهٔ B در روز دوشنبهٔ دوم ژانویه رخ داده‌است. درطول سال چندبار دوحادثه باهم در یك روز پنجشنبه رخ می‌دهند؟ آخرین این پنجشنبه‌ها کی بوده‌است؟ (این را به‌صورت «روز n ام سال» جواب دهید.)

۶. ثابت کنید که دستگاه همنهشتیهای

$$\begin{cases} x \equiv a & (\text{به پیمانهٔ } m) \\ x \equiv b & (\text{به پیمانهٔ } n) \end{cases}$$

دارای جواب است اگر وفقط اگر (m, n) عدد $a - b$ را عاد کند.

۷. ثابت کنید یك عدد صحیح که به‌مبنای دهدهی نوشته شده باشد بر ۹ قابل قسمت است اگر وفقط اگر مجموع رقمهایش بر ۹ قابل قسمت باشد. قانون مشابهی برای تقسیم‌پذیری بر ۱۱ بیان وثابت کنید.

۸. دستگاه همنهشتیهای

$$\begin{cases} 3x-5y\equiv 7 & \text{(به پیمانهٔ ۴۵)} \\ 10x-36y\equiv 12 & \text{(به پیمانهٔ ۴۵)} \end{cases}$$

را حل کنید.

۹. ثابت کنید که، به ازاء هر $n>2$، $\varphi(n)$ زوج است.

۱۰. ثابت کنید که، به‌ازاء همهٔ اعدادصحیح مثبت m و n، $\varphi(mn)\geqslant\varphi(m)\varphi(n)$.

۱۱. ثابت کنید که اگر $n\geqslant 3$، حاصلضرب همهٔ ریشه‌های n ام اولیهٔ ۱ در $\mathbf{C}$ برابر است با ۱.

۱۲. ثابت کنید که ریشه‌های دوازدهم اولیهٔ ۱ در $\mathbf{C}$ عبارت‌اند از ریشه‌های معادلهٔ

$$z^4-z^2+1=0$$

معادلهٔ متناظری برای ریشه‌های دهم اولیهٔ ۱ پیدا کنید.

۱۳. ثابت کنید که اگر G گروهی متناهی از مرتبهٔ فرد باشد آنگاه هرعنصر G دارای یك «ریشهٔ دوم» است، یعنی، $(\forall g\in G)(\exists h\in G)(h^2=g)$. آیا الزاماً هر عنصر دارای یك ریشهٔ دوم یکتاست؟ (راهنمایی: دربارهٔ زیرگروههای دوری G بیندیشید.)

۱۴. ثابت کنید که اگر n یك عدد اول فرد باشد، همنهشتی (به پیمانهٔ n) $x^2\equiv 1$ دقیقاً دارای دو جواب به پیمانهٔ n است. ثابت کنید که همنهشتی دقیقاً دارای چهار جواب به پیمانهٔ n است اگر $n=pq$، که در آن p و q اعداد اول فرد متمایزند.

۱۵. نشان دهید که اگر n عددصحیح مثبتی باشد و $d|n$، آنگاه تعداد اعدادصحیح x به‌قسمی که $1\leqslant x\leqslant n$ و $(x,n)=d$ دقیقاً برابر است با $\varphi\left(\frac{n}{d}\right)$.

۱۶. نشان دهید که اگر a و b اعداد صحیح باشند و (به پیمانهٔ ۴) $ab\equiv 3$، آنگاه یا (به پیمانهٔ ۴) $a\equiv 3$ یا (به پیمانهٔ ۴) $b\equiv 3$.

یك دنباله از اعداد صحیح a_1، a_2، a_3، ... به وسیلهٔ $a_1=1$؛ $a_{n+1}=4a_1a_2\cdots a_n+3$ تعریف شده‌اند. ثابت کنید اگر $i\neq j$، آنگاه $(a_i,a_j)=1$ ونتیجه بگیرید که بینهایت عدد اول به صورت $4k+3$ وجود دارد.

فصل ۸

حلقه‌ها و میدانها

تاکنون مطالعات خودرا دربارهٔ دستگاههای مجرد جبری به‌گروهها منحصر کرده‌ایم. مثلا، درموردکاربردها به‌اعداد صحیح، توجه خود را روی ساخت جمعی گروه متمرکز نموده‌ایم وگرچه می‌توانستیم حقایقی دربارهٔ ساخت ضربی، مانند قضیهٔ یکتایی تجزیه، نتیجه بگیریم، این تنها امکان بود زیرا ضرب اعداد صحیح برحسب جمع قابل تعریف است. مانمی‌توانیم انتظار داشته باشیم که روش مشابهی درسایرموقعیتها کارگر باشد؛ مثلا، بـرای پیشرفت مشابه باچندجمله‌ایها، یااثبات نتایج عمیق‌تر دربارهٔ اعداد صحیح، نیاز به‌مطالعهٔ نـزدیکتری بین فعل وانفعالات ساختهای جمعی و ضربی داریم. برای این منظور، مفهوم اساسی، مفهوم یك حلقه‌است.

تعریف. یك حلقه عبارت است ازمجموعه‌ای مانند R بادوعمل دوتایی $+$ ، $\cdot$ ، ویك‌عمل یکتایی $-$ ، روی‌آن، که شامل عناصر ویژهٔ ۰ و ۱ بوده، وبرای‌آن اصول موضوعهٔ زیر برقرار باشد.

(ج۱) به‌ازاء هر $x, y, z \in R$ ، $(x+y)+z = x+(y+z)$ ؛

(ج۲) به‌ازاء هر $x \in R$ ، $x+0 = 0+x = x$ ؛

(ج۳) به‌ازاء هر $x \in R$ ، $x+(-x) = (-x)+x = 0$ ؛

(ج۴) به‌ازاء هر $x, y \in R$ ، $x+y = y+x$ ؛

(ض۱) به‌ازاء هر $x, y, z \in R$ ، $(xy)z = x(yz)$ ؛

(ض۲) به‌ازاء هر $x \in R$ ، $x1 = 1x = x$ ؛

$$\begin{cases} x(y+z)=xy+xz \\ (x+y)z=xz+yz \end{cases}$$ و (ج‌ض۱) به‌ازاء هر $x, y, z \in R$،

این قوانین، زیرمجموعه‌ای از «قوانین استانده» فصل ۱ هستند ومی‌توانند گویای این‌باشد که R یك‌گروه آبلی جمعی است با ضربی شرکت‌پذیر و توزیعی‌که شامل عنصر همانی ۱ برای ضرب می‌باشد.

قبلاچندین‌مثال ازحلقه‌هارا دیده‌ایم. آشکارترین‌آنها $\mathbf{Z}$ ، $\mathbf{Q}$ ، $\mathbf{R}$ و $\mathbf{C}$ هستند. همچنین، جبرتمام چندجمله‌ایهای $p(X)$ باضرایب‌حقیقی یك‌حلقه است (مثال ۲.۱ را ببینید). همهٔ‌این حلقه‌ها دراصل موضوعهٔ دیگر

$$xy=yx$$ (ض۴) به‌ازاء هر $x, y \in R$،

صدق‌می‌کنند و درنتیجه حلقه‌های‌جابجایی نامیده می‌شوند. مثالی ازحلقه‌ای‌که جابجایی نیست حلقهٔ تمام ماتریسهای 2×2 با درایه‌های حقیقی می‌باشد (مثال ۳.۱ را ببینید). به‌طورکلیتر، اگر $n \geqslant 2$ ، مجموعهٔ همهٔ ماتریسهای $n \times n$ بادرایه‌های حقیقی یك‌حلقهٔ غیر جابجایی است.

بابعضی ازنتایج مقدماتی اصول موضوعه‌آغاز می‌کنیم.

قضیهٔ ۸ آ. فرض‌کنید R یك حلقه باشد. دراین‌صورت

(الف) به‌ازاء هر $a \in R$ ، $a \cdot 0 = 0 \cdot a = 0$ ؛

(ب) به‌ازاء هر $a, b \in R$ ، $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ ؛

(پ) به‌ازاء هر $a, b \in R$ ، $(-a) \cdot (-b) = ab$ ؛

(ت) هر حاصلضرب $a_1 a_2 \cdots a_n$ در R مستقل از نحوهٔ پرانتزگذاری عوامل ضرب است؛

(ث) به‌ازاء هر $a \in R$ وهر $m, n \in \mathbf{N}$ ، $a^m a^n = a^n a^m = a^{m+n}$ و $(a^m)^n = a^{mn}$،

که a^n به‌طور استقرایی به‌وسیلهٔ $a^0 = 1$ ، $a^{n+1} = a^n a$ تعریف‌شده است ؛

(ج) به ازاء هر $a_i, b_j \in R$ ، $\left(\sum_{i=1}^{n} a_i\right) \cdot \left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n} \sum_{j=1}^{m} (a_i b_j)$.

برهان. درپایان‌فصل ۱ قسمتهای (الف) و (ب) فقط با به‌کاربردن اصول موضوعهٔ حلقه ثابت شده‌اند. (پ) نتیجهٔ فوری از قسمت (ب) است. اثبات (ت) مشابه برهان قضیهٔ ۴ آ (ج) می‌باشد. همانند قضیهٔ ۴ ب، قسمت (ث) از (ت) به‌آسانی نتیجه می‌شود. بالاخره، (ج) به‌طریق زیر اثبات می‌شود. نخست استقراء را روی n به‌کار برید ونشان دهیدکه به‌ازاء هر $a_i, b \in R$ ،

$$(a_1+a_2+\cdots+a_n)b=a_1b+a_2b+\cdots+a_nb\,.$$

در پلهٔ استقراء از قانون توزیعی (ج‌ض۱) یکبار استفاده می‌شود. حال برای تکمیل برهان، این نتیجه را همراه با $b=b_1+b_2+\cdots+b_m$ واستقراء روی m، به‌کار ببرید. این مطلب را به‌عنوان یك تمرین به‌عهدهٔ خواننده می گذاریم.

دراینجا دواخطار لازم به‌تذکر است. اولا درحالت کلی a^n برای اعدادصحیح منفی n تعریف نشده است؛ این به‌آن علت است که فرض نکرده‌ایم عناصر نسبت به‌ضرب دارای معکوس‌اند. ثانیاً، قانون حذف وجود ندارد: $ab=ac$ نتیجه نمی‌دهد $b=c$، حتی‌وقتی که $a\neq 0$. درواقع ممکن‌است $ab=0$ ، درست‌باشد درصورتی که نه a ونه b هیچکدام‌صفر نباشند، به‌عنوان مثال، درحلقهٔ ماتریسهای 2×2 ، حاصلضرب

$$\begin{pmatrix}0&0\\0&1\end{pmatrix}\quad\text{و}\quad\begin{pmatrix}1&0\\0&0\end{pmatrix}$$

ماتریس صفراست.

هرحلقه شامل عناصرویژهٔ معینی است که دراغلب موارد نقش اعداد صحیح را ایفا می کنند. اگر x عنصردلخواهی ازحلقهٔ R باشد واگر $n\in\mathbf{Z}$ آنگاه، طبق‌معمول، nx توان جمعی n ام x را در گروه جمعی R نشان می‌دهد. بنابراین $x+x+x=3x$ و $-x-x=(-2)x$. اگر R خودحلقهٔ اعداد صحیح باشدآنگاه دیده‌ایم که nxمی‌تواند به‌عنوان حاصلضرب n و x در R نیز تعبیرشود. این‌را درحالت‌کلی نمی‌توانیم انجام‌دهیم، زیرا ممکن است n عضو R نباشد. به‌هرحال، اگربنویسیم $\bar{n}=n1$ ، که درآن 1 عنصر همانی R است، بسادگی‌ثابت می‌شود که $\bar{n}x=nx$ ، که درآن حالا سمت چپ رابطه حاصلضربی در R است. این‌مطلب به‌ازاء n های مثبت ازقانون توزیعی نتیجه‌می‌شود، زیرا $x+\cdots+x=(1+\cdots+1)x=(1+\cdots+1)x$ (با nجمله‌درهرطرف). برای $n=-m<0$، بآسانی ملاحظه می‌شود که

$$\bar{n}=(\overline{-m})=(-m)1=-(m1)=-\bar{m}\,,$$

وبنابراین

$$nx=(-m)x=-(mx)=-(\bar{m}x)=(-\bar{m})x=\bar{n}x\,.$$

علی‌رغم تمایز روشن موجود بین $n\in\mathbf{Z}$ و $\bar{n}\in R$ ، حذف علامت «بار» (خطهای بالای m و n) ، در اکثرمواردکاری رایج است و طوری صحبت می‌شود که گویی اعداد صحیح واقعاً اعضای R هستند. این مطلب هیچ مسئلهٔ جدی را موجب نمی گردد به‌شرطی که به‌خاطر داشته باشیم که ممکن است حالت $\bar{n}=\bar{m}$ اتفاق بیفتد حتی هنگامی که $m\neq n$. بنابراین، اگربارها حذف شوند ممکن‌است تساوی $2=0$ دریك حلقه درست باشد. بعداً به‌این نکته

مراجعه خواهیم کرد.

محاسبات گوناگونی دریك حلقهٔ جابجایی می‌تواند انجام گیرد که درحلقه‌های دلخواه معتبر نیستند. قضیهٔ دوجمله‌ای مثال مناسبی است که اکنون آن را درهر حلقهٔ جابجایی ثابت می‌کنیم. به‌عنوان مثال، این قضیه درحلقهٔ ماتریسها درست نیست؛ زیرا برای دوماتریس $n\times n$ ، B و A ازقوانین توزیعی نتیجه می‌شود که

$$(A+B)^2=A^2+AB+BA+B^2\ ,$$

ولی نمی‌توان نوشت $AB+BA=2AB$، زیرا درحالت کلی $AB\neq BA$.

قضیهٔ ۸ ب. فرض کنید R یك حلقهٔ جابجایی باشد. دراین‌صورت

(الف) به‌ازاء هر a ، $b\in R$ وهر $n\in\mathbf{N}$ ، $(ab)^n=a^nb^n$ ؛

(ب) به‌ازاء هر a ، $b\in R$ وهمهٔ اعداد صحیح $n>0$ ،

$$(a+b)^n=a^n+na^{n-1}b+\binom{n}{2}a^{n-2}b^2+\cdots+\binom{n}{r}a^{n-r}b^r+\cdots+b^n$$

که درآن $\binom{n}{r}$ ، طبق معمول، عدد صحیح $\dfrac{n!}{r!\,(n-r)!}$ را نشان می‌دهد.

برهان . (الف) دقیقاً همانند گروههای آبلی ثابت می‌شود (ولی به‌ازاء $n<0$ برقرار نیست).

(ب) این‌قسمت به‌کمك استقراء روی n مشابه اعداد حقیقی ثابت می‌شود. اگر $n=1$ نتیجه بدیهی است. بنابراین فرض می‌کنیم که دستور مفروض به‌ازاء یك مقدار ثابت n برقرار باشد (وبه‌ازاء هر a ، $b\in R$) ونتیجه بگیریم که

$$\begin{aligned}(a+b)^{n+1}&=(a+b)^n(a+b)\\&=(a^n+na^{n-1}b+\cdots+\binom{n}{r}a^{n-r}b^r+\cdots+b^n)(a+b)\\&=(a^{n+1}+na^nb+\cdots+\binom{n}{r}a^{n-r+1}b^r+\cdots+ab^n)\\&\quad+(a^nb+na^{n-1}b^2+\cdots+\binom{n}{r}a^{n-r}b^{r+1}+\cdots+b^{n+1}).\end{aligned}$$

همهٔ جمله‌های این عبارت به‌صورت ka^pb^q هستند، که در آن k عددی است صحیح و $p+q=n+1$. ضریب $a^{n+1-r}b^r$ برابر است با

$$\binom{n}{r}+\binom{n}{r-1},$$

که در آن $\binom{n}{0}$ و $\binom{n}{n}$ را، طبق معمول، مساوی ۱ و $\binom{n}{n+1}$ را برابر صفر تعبیر می‌کنیم.

محاسبهٔ ساده‌ای نشان می‌دهد که

$$\binom{n}{r}+\binom{n}{r-1}=\binom{n+1}{r},$$

و بنابراین

$$(a+b)^{n+1}=a^{n+1}+(n+1)a^nb+\cdots+\binom{n+1}{r}a^{n+1-r}b^r+\cdots+b^{n+1}.$$

این مطلب پلهٔ استقراء را کامل می‌کند و در نتیجه قضیه اثبات می‌شود.

قبلا یکه‌های $\mathbf{Z}$ را دیده‌ایم. در حالت کلی، عنصر x از حلقهٔ R یك یکه از R نامیده می‌شود اگر دارای معکوس ضربی باشد، یعنی، اگر $y\in R$ وجود داشته باشد به‌قسمی که $xy=yx=1$. مجموعهٔ یکه‌های حلقهٔ R به‌وسیلهٔ $U(R)$ نشان داده می‌شود.

مثال ۱۰۸. $U(\mathbf{Z})=\{\pm 1\}$.

مثال ۲۰۸. در هریك از حلقه‌های $\mathbf{Q}$، $\mathbf{R}$ و $\mathbf{C}$ همهٔ عناصر غیرصفر یکه هستند، به‌عبارت‌دیگر:

$$U(\mathbf{Q})=\mathbf{Q}^*,\ U(\mathbf{R})=\mathbf{R}^*\text{ و }U(\mathbf{C})=\mathbf{C}^*.$$

مثال ۳۰۸. یکه‌های حلقهٔ $\mathbf{R}^{n\times n}$ از ماتریسهای حقیقی $n\times n$، ماتریسهای معکوس‌پذیر (یا غیرمنفرد) هستند. به‌عبارت دیگر: $U(\mathbf{R}^{n\times n})=\mathrm{GL}_n(\mathbf{R})$ (مثال ۱۰۰۴ را ببینید).

خواننده احتمالاً توجه کرده است که در هریك از این مثالها مجموعهٔ یکه‌ها، گروه آشنایی است. این مطلب اتفاقی نیست، بلکه قضیه‌ای ساده است.

قضیهٔ ۸ پ. مجموعهٔ یکه‌های $U(R)$ از هر حلقهٔ R نسبت به ضرب حلقه، یك گروه است.

برهان. قرار دهید $U=U(R)$. اگر x و $y\in U$ آنگاه هریك دارای معکوسی مانند x'، y'،

هستند به‌قسمی که $xx'=x'x=yy'=y'y=1$. ازاین نتیجه می‌شود که حاصلضرب xy در R نیز دارای معکوسی مانند $y'x'$ است؛ زیرا

$$(xy)(y'x')=x(yy')x'=x1x'=xx'=1$$

و به‌همین‌ترتیب $(y'x')(xy)=1$. بنابراین $xy\in U$ وضرب عملی دوتایی روی U القاء می‌کند. این‌عمل‌شرکت‌پذیراست‌زیرا ضرب‌در R شرکت‌پذیرمی‌باشد. حال $1\in U$ (معکوس آن ۱ است) و ۱ به‌عنوان عنصرخنثای ضرب عمل می‌کند. باقی می‌ماند نشان دهیم که معکوسها در U وجود دارند. این تقریباً، ولی نه‌کاملا، تعریف U است. می‌دانیم که هر $x\in U$ دارای معکوس x' در R است، وکافی است نشان دهیم که این x' در U قرار دارد، یعنی‌اینکه معکوس عنصر یکه عنصری است یکه. اما این واضح است، زیرا x' دارای معکوس x در R است.

توجه. مهمترین خاصیت یکه‌ها این است که می‌توانند حذف شوند: اگر در R ، $ua=ub$، که درآن u یکه است، آنگاه $a=b$ ، زیرا می‌توان سمت چپ را درمعکوس u یعنی u^{-1} ضرب کرد و $u^{-1}ua=u^{-1}ub$ را به‌دست‌آوریم، که ازآنجا $1a=1b$ ، یعنی $a=b$. به‌همین‌نحو، اگر u یکه باشد، $au=bu$ نتیجه می‌دهد $a=b$.

یك زیرحلقه ازحلقهٔ R به‌طریق روشنی، ومانند زیرگروههای یك‌گروه تعریف‌می‌شود. زیرمجموعهٔ S از R یك زیرحلقه است به‌شرط‌آنکه $1\in S$ ، و اگر a ، $b\in S$ آنگاه همهٔ عناصر $a+b$ ، $a-$ و ab در S قرار داشته باشند. بسادگی نتیجه می‌شود که خود S نسبت به‌اعمال تحدیدی یك‌حلقه است.

مثال ۴.۸. مجموعهٔ همهٔ «اعدادصحیح» $n1=\overline{n}$ ازحلقهٔ R یك‌زیرحلقه‌است. خواننده‌باید خود تمام جزئیات راتحقیق‌کند وبرای‌کلیهٔ مثالهای زیرنیز همین‌عمل را انجام‌دهد.

مثال ۵.۸. در زنجیرهٔ‌مجموعه‌های $\mathbf{Z}\subset\mathbf{Q}\subset\mathbf{R}\subset\mathbf{C}$ ، هرکدام زیرحلقهٔ بعدی است. ولی $\mathbf{N}$ زیرحلقهٔ $\mathbf{Z}$ نیست.

مثال ۶.۸. درحلقهٔ ماتریسهای حقیقی 2×2، مجموعهٔ همهٔ ماتریسهای به‌صورت

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$$

یك زیرحلقه است، ولی مجموعهٔ ماتریسهای به‌صورت

$$\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$$

زیرحلقه نیست.

مثال ۷.۸. مجموعهٔ تمام اعداد صحیح زوج زیرحلقهٔ $\mathbf{Z}$ نیست، درواقع درهمهٔ شرطها صادق است بجزیکی: این مجموعه شامل عنصر همانی ۱ نیست. (وقه دارای عنصری همانی از خودش می‌باشد.) دراینجا باید یادآورشد که دربعضی کتابها داشتن عناصر همانی را برای حلقه‌ها ضروری نمی‌دانند، واگر حلقه‌ای شامل عنصر همانی باشد، آن‌را «حلقهٔ یکدار» می‌نامند. چنانچه این قرارداد اتخاذ گردد آنگاه بایدمجموعهٔ اعداد صحیح زوج را به‌عنوان زیرحلقه‌ای از $\mathbf{Z}$ درنظر گرفت.

توجه کنید که درحالت خاص هرزیرحلقه ازیك حلقهٔ R زیرگروهی جمعی از R است. بنابراین ازاین جهت تمام قضایایی که درمورد زیرگروهها ثابت کرده‌ایم به‌زیرحلقه‌های یك حلقه به‌کار می‌روند. به‌عنوان مثال، درحلقه‌ای متناهی با n عنصر، تعداد عناصر هر زیرحلقه مقسوم‌علیهی از n است. همچنین، همرده‌های جمعی یك زیرحلقه تشکیل افرازی ازحلقه را می‌دهند.

کاوش شباهت بین گروهها و حلقه‌ها را ادامه می‌دهیم ومفاهیمی ازقبیل ضرب حلقه‌ها، یکریختیها و همریختیهای حلقه‌ها، وحلقه‌های خارج‌قسمت را تعریف خواهیم کرد. یکی‌دو اشکال که به‌وسیلهٔ وجود عمل اضافی موجب می‌شود، وجود دارد، ولی براهین به‌طور خیلی مشابهی جریان می‌یابند. قضایای منتج، در دوفصل آینده، درمورد حلقهٔ اعداد صحیح وحلقه‌های چندجمله‌ایها به‌کار می‌روند.

اگر R و S دوحلقه باشند آنگاه چون، درحالت خاص، نسبت به‌جمع گروه آبلی هستند، حاصلضربشان $R\times S$، به‌مفهوم نظریهٔ مجموعه‌ها، نسبت به‌جمع نیز یك گروه آبلی است که عمل جمع به‌وسیلهٔ $(r_1, s_1)+(r_2, s_2)=(r_1+r_2, s_1+s_2)$ تعریف شده است. حال اگرعمل ضرب را در $R\times S$ به‌وسیلهٔ $(r_1, s_1)(r_2, s_2)=(r_1r_2, s_1s_2)$ تعریف کنیم درآن‌صورت بسادگی تحقیق می‌شود $R\times S$ یك حلقه است، که حاصلضرب حلقه‌های R و S نامیده می‌شود. عنصرصفرآن $(0, 0)$ وعنصرهمانی آن برابراست با $(1, 1)$. تحقیق اینها را به‌عنوان تمرین به‌عهدهٔ خواننده می‌گذاریم. اگر R و S حلقه‌های جابجایی باشند آنگاه واضح است که $R\times S$ نیزجابجایی است.

قضیهٔ ۸ ت. فرض کنید R و S دوحلقه باشند. دراین‌صورت

$$U(R\times S)=U(R)\times U(S)$$

برهان. عنصر $(r, s)\in R\times S$ یکه است اگر وفقط اگر عنصری مانند $(r', s')\in R\times S$ وجود داشته باشد به‌قسمی که $(r, s)(r', s')=(r', s')(r, s)=(1, 1)$. ولی بنابه تعریف $(r, s)(r', s')=(rr', ss')$؛ ازاینرو (r, s) یکه‌است اگروفقط اگر $r'\in R$، $s'\in S$ وجود داشته باشند به‌قسمی که $rr'=r'r=1$ و $ss'=s's=1$، یعنی اگروفقط اگر r و s

هردو یکه باشند ، واین مطلب قضیه را اثبات می‌کند . توجه کنید که تساوی $U(R\times S)=U(R)\times U(S)$ نه‌فقط تساوی مجموعه‌هاست، بلکه تساوی گروهها نیز هست: ضرب در $U(R\times S)$ همانند ضرب در گروه حاصلضرب $U(R)\times U(S)$ است.

دقیقاً همان‌طور که همریختی گروهها نگاشتی است که اعمال گروه را حفظ می‌کند، همریختی حلقه‌ها نیز نگاشتی است مانند $f : R\longrightarrow S$ ، بین دوحلقهٔ R و S ، که اعمال حلقه‌ها را حفظ می‌کند. بخصوص، شرایط اینکه f یک همریختی بین حلقه‌ها باشد عبارت‌اند از:

(الف) به‌ازاء هر $x, y\in R$ ، $f(x+y)=f(x)+f(y)$ ؛

(ب) به‌ازاء هر $x, y\in R$ ، $f(xy)=f(x)f(y)$ ؛

(پ) $f(1)=1$.

قبلادیده‌ایم که(الف) نتیجه می‌دهد $f(-x)=-f(x)$ و $f(0)=0$، زیرا R و S گروههای‌جمعی‌هستند (خواننده بایداستدلالی راکه‌برای‌یکریختی گروهها درصفحهٔ۱۵۹ارائه شده است به‌خاطر آورد). متأسفانه(ب) نتیجه نمی‌دهد $f(1)=1$ ، از اینرو بایستی این‌را به‌عنوان فرض جداگانه‌ای قرار دهیم. (مثال: نگاشتی از اعداد حقیقی به ماتریسها که x را به

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

تبدیل می‌کند، درشرایط (الف) و (ب) صدق‌کرده، ولی در (پ) صدق نمی‌کند.) لیکن ، (ب) و (پ) با همدیگر نتیجه می‌دهند که اگر x یک در R باشد ، آنگاه $f(x^{-1})=f(x)^{-1}$ ، زیرا $f(x^{-1})f(x)=f(x^{-1}x)=f(1)=1$، وبه‌همین‌ترتیب $f(x)f(x^{-1})=1$. این مطلب قضیهٔ زیر را اثبات می‌کند:

قضیهٔ ۸ ث. اگر $f : R\longrightarrow S$ همریختی حلقه‌هاباشدآنگاه f یکه‌های R را به‌یکه‌های S تبدیل‌کرده ومعکوسها را حفظ می‌کند. بنابراین f یك همریختی‌گروههای ضربی از $U(R)$ به $U(S)$را، القاء می‌کند.

البته، یکریختی‌حلقه‌ها یك همریختی دوسویی بین‌حلقه‌هاست. دوحلقه که یکریخت‌اند اساساً دارای یك ساخت حلقه‌ای هستند.

مثال ۸.۸. اگر R حلقهٔ دلخواهی باشد ونگاشت $f : \mathbf{Z}\longrightarrow R$ باضابطهٔ $f(n)=n1=\overline{n}$ داده شده باشد، آنگاه f یك همریختی حلقه‌هاست. اگر، مثلا، R حلقهٔ اعداد حقیقی یاحلقهٔ

ماتریسهای حقیقی ۲×۲ باشد، درآن‌صورت همریختی f یك‌به‌یك است ولی بروی نیست.

مثال ۹.۸. نگاشت $f : \mathbf{C} \longrightarrow \mathbf{R}^{۲\times ۲}$ که به‌ازاء همهٔ اعداد حقیقی x و y به‌وسیلهٔ

$$f(x+iy)=\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

تعریف شده‌است یك‌همریختی حلقه‌ها ویك‌به‌یك است. خواننده باید تمام جزئیات‌این مثال را تحقیق کند.

اکنون به‌ساختمان حلقه‌های خارج‌قسمت می‌پردازیم، وهمان طرح گروهها را دنبال می‌کنیم. افرازی از حلقهٔ R را جستجو می‌کنیم که درآن خود همرده‌ها بتوانند جمع‌وضرب شوند تااینکه ساختی ازحلقه روی مجموعهٔ خارج قسمت به‌دست‌آید. قبلا می‌دانیم بدلیل آنکه جمع به‌طور صحیح‌کارکند بایستی باانتخاب همرده‌های یك‌زیر گروه جمعی A از R شروع کنیم. دراینجا ما فقط این‌را که R یك گروه آبلی جمعی است، به‌کار می‌بریم. قضیهٔ ۶ت نشان می‌دهدکه برای هر زیر گروه جمعی A از R مجموعهٔ R/A ازتمام همرده‌های جمعی $x+A=\langle x\rangle$ نسبت به‌جمعی که به‌وسیلهٔ $\langle x\rangle+\langle y\rangle=\langle x+y\rangle$ تعریف شده، یك گروه آبلی است. ولی اگر حالا سعی‌کنیم ضرب را با ضابطهٔ $\langle x\rangle\langle y\rangle=\langle xy\rangle$ تعریف کنیم، اشکال کوچکی بوجود می‌آید، زیرا سمت راست الزاماً مستقل‌ازنماینده‌های‌انتخاب شده برای‌همرده‌های $\langle x\rangle$ و $\langle y\rangle$ نیست. درواقع ما نیاز داریم که شرط زیر از قضیهٔ۶پ را تحقیق کنیم:

$$\langle x\rangle=\langle x'\rangle \;\&\; \langle y\rangle=\langle y'\rangle \Rightarrow \langle xy\rangle=\langle x'y'\rangle ,$$

که به‌ازاء تمام زیر گروهها درست نیست. (مثلا، اگر $R=\mathbf{Q}$ و $A=\mathbf{Z}$، آنگاه

$$\langle ۱\rangle=\langle ۲\rangle \text{ و } \langle \tfrac{۱}{۲}\rangle=\langle -\tfrac{۱}{۲}\rangle \text{، ولی}$$

$$(\cdot \langle ۱\times \tfrac{۱}{۲}\rangle \neq \langle ۲\times(-\tfrac{۱}{۲})\rangle)$$

حالت‌خاصی ازاین‌شرط، این‌را می‌گوید که‌اگر $\langle ۰\rangle=\langle x\rangle$ آنگاه، به‌ازاء هر y؛ $\langle ۰\rangle=\langle ۰y\rangle=\langle xy\rangle$؛ به‌عبارت دیگر، اگر $x\in A$آنگاه، به‌ازاء هر $y\in R$، $xy\in A$، و به‌همین نحو $yx\in A$. هر زیر گروه جمعی A که دراین شرط اخیر (یعنی، $x\in A \;\&\; y\in R \Rightarrow xy\in A \;\&\; yx\in A$) صدق کند یك ایده‌آل از R نامیده می‌شود. درواقع خواهیم دیدکه این شرط، تمام چیزی‌است‌که برای خوب‌کارکردن خارج‌قسمتها لازم‌است. توجه کنیدکه هرایده‌آلی تحت ضرب بسته است، ولی همیشه یك زیرحلقه نیست زیرا $۱\in A$ را جزء شرایط محسوب نمی‌کنیم. درواقع اگر A ایده‌آلی از R باشدو $۱\in A$ آنگاه‌باید داشته باشیم $A=R$.

از اینرو حال فرض می‌کنیم A ایده‌آل دلخواهی از R باشد، و همچنین

$<x>=<x'>$ و $<y>=<y'>$. این به‌آن معنی است که $x-x'\in A$ و $y-y'\in A$ ، ومایلیم بدانیم که آیا $<xy>=<x'y'>$ ، یعنی‌آیا $xy-x'y'\in A$؟ درهرحلقه می‌توانیم بنویسیم $xy-x'y'=x(y-y')+(x-x')y'$. چون $y-y'\in A$ و A یك ایده‌آل است، داریم $x(y-y')\in A$. به‌همین‌ترتیب $(x-x')y'\in A$ و نتیجه می‌شود که $xy-x'y'\in A$ ، یعنی $<xy>=<x'y'>$. این نشان می‌دهد که ضرب می‌تواند، بدون‌هیچ ابهامی، روی R/A ، باضابطهٔ $<x><y>=<xy>$ ، تعریف شود. حال‌بسادگی‌می‌توانیم نتیجه بگیریم که R/A حلقه‌ای باعنصرهمانی $<1>=A+1$ است. واضح است که به‌ازاء هر $x\in R$ ،

$$<1><x>=<x><1>=<x>\ ,$$

و

$$(<x><y>)<z>=<xy><z>=<(xy)z>=<x(yz)>$$
$$=<x><yz>=<x>(<y><z>)\ .$$

قوانین توزیعی به‌وسیلهٔ استدلال عادی مشابهی ثابت می‌شوند. همچنین، اگر در R ، $xy=yx$، آنگاه $<x><y>=<y><x>$ در R/A برقراراست. بدین‌ترتیب قضیهٔ زیراثبات می‌شود.

قضیهٔ ۸ ج. اگر A ایده‌آل دلخواهی ازحلقهٔ R باشدآنگاه مجموعهٔ R/A ازهمرده‌های‌جمعی A در R نسبت به‌اعمالی‌که به‌وسیلهٔ

$$<x>+<y>=<x+y>$$
$$<x>\cdot<y>=<xy>$$

تعریف‌شده یك‌حلقه است، که‌دراینجا $<x>$ همردهٔ $A+x$ رانشان‌می‌دهد. $A=<0>$ عنصر صفر R/A است وعنصرهمانی‌آن $A+1=<1>$ می‌باشد. اگر R حلقه‌ای‌جابجایی باشد R/A نیز جابجایی است.

همانند حالت گروهها، واضح است که نگاشت خارج قسمت $q: R\longrightarrow R/A$ یك همریختی سقف است؛ این صرفاً انعکاسی است از نحوهٔ تعریف اعمال حلقه در R/A . اکنون کم‌وبیش می‌توانیم قضیهٔ اول یکریختی گروهها را (قضیهٔ۶ج) باتغییرات مناسبی به اصطلاحات حلقه، رونویسی کنیم. هستهٔ یك‌همریختی حلقه‌ها، $f: R\longrightarrow S$، مجموعهٔ‌عناصر $x\in R$ است به‌قسمی که $f(x)=0$. تصویر f درست همان‌نظریهٔ مجموعه‌ای‌آن، یعنی $f(R)$ می‌باشد.

قضیهٔ ۸ چ. فرض‌کنید R و S حلقه و $f: R\longrightarrow S$ همریختی حلقه‌ها باشد. دراین‌صورت

(الف) هستهٔ K از f یك ایده‌آل R است ؛

(ب) بافتهای f همرده‌های جمعی K هستند ؛

(پ) تصویر $T=f(R)$ از f یك زیرحلقهٔ S است ؛

(ت) $T\cong R/K$ (یکریختی حلقه‌ها) .

برهان. چون f یك همریختی گروههای جمعی است، K زیرگروهی جمعی از R است و بافتهای f همرده‌های جمعی K هستند. همچنین T یك زیرگروه جمعی S است، و به‌عنوان گروه $T\cong R/K$ ، همهٔ اینها مشمول قضیهٔ ع‌ج هستند. حال اگر $k\in K$ و $r\in R$ ، آنگاه $f(k)=0$ ، پس $f(kr)=f(k)f(r)=0\times f(r)=0$ و به‌همین نحو $f(rk)=0$ ؛ بنابراین $kr\in K$ و $rk\in K$ ، ازاینرو K یك ایده‌آل R است. به‌همین ترتیب، اگر x ، $y\in T$، آنگاه به‌ازاء عناصری چون a ، $b\in R$ ، داریم $x=f(a)$ و $y=f(b)$ ، از اینرو $xy=f(a)f(b)=f(ab)\in T$. همچنین $1=f(1)\in T$ ، و این نشان می‌دهد که T زیرحلقهٔ S است. بالاخره، یکریختی گروهی $f^*: R/K\longrightarrow T$ که یادآور می‌شویم به‌وسیلهٔ $f^*(<r>)=f(r)$ تعریف شده است، درواقع یکریختی حلقه‌ای است زیرا

$$f^*(<r_1><r_2>)=f^*(<r_1r_2>)=f(r_1r_2)=f(r_1)f(r_2)$$
$$=f^*(<r_1>)f^*(<r_2>)$$

والبته $1=f(1)=f^*(<1>)$. بدین‌ترتیب برهان کامل می‌شود.

قبل‌از اینکه نظری به‌کاربرد این نتایج بیفکنیم بعضی از مفاهیم جدید درنظریهٔ حلقه‌ها را معرفی خواهیم کرد که هیچ‌صورت مشابهی درنظریهٔ گروهها ندارند . آنها به‌ساختمان کسرها مربوط می‌شوند و برای درك درستی از اعدادگویا و توابع گویا حائز اهمیت‌اند.

بامفهوم مقسوم‌علیه صفر دریك‌حلقهٔ جابجایی R آغاز می‌کنیم. واضح است که هر عنصر x از R صفررا عاد می‌کند بدین‌معنی که به‌ازاء y مناسبی (یعنی ، $y=0$) ، $xy=0$. بنابراین برای اجتناب ازاین حالت بدیهی، مقسوم‌علیه صفررا در R عنصر $x\in R$ تعریف می‌کنیم که دراین شرط صدق کند: $y\in R$ وجود داشته باشد به‌قسمی که $xy=0$ و $y\neq 0$. (دریك حلقهٔ غیرجابجایی بایستی بین مقسوم‌علیه‌های صفرچپ‌وراست فرق قائل شویم، ولی این حالت‌را درنظرنمی‌گیریم.)

عنصر x که مقسوم‌علیه صفر نباشد درشرط $xy=0\Rightarrow y=0$ ، صدق می‌کند. چنین عنصر x ای می‌تواند ازمعادلات به‌صورت $xa=xb$ حذف شود، زیرا

$$xa=xb\Rightarrow x(a-b)=0\Rightarrow a-b=0\Rightarrow a=b\,.$$

ازطرف دیگر، مطمئناً یك مقسوم‌علیه‌صفر x همیشه نمی‌تواند حذف‌شود، زیرا $y \neq 0$ به‌قسمی وجود دارد که $xy = 0 = x0$. بنابراین هرحلقهٔ جابجایی به‌دونوع ازعناصر افرازمی‌شود: مقسوم‌علیه‌های صفروعناصر قابل حذف. درمیان‌مقسوم‌علیه‌های صفر، مقسوم علیه‌های صفر سره را تمیز می‌دهیم، یعنی آنهایی که برابر ۰ نیستند.

قضیهٔ ۸ ح. فرض‌کنید R یك حلقهٔ جابجایی باشد. دراین‌صورت سه‌شرط زیر معادل‌اند:

(الف) R شامل هیچ مقسوم‌علیه صفر سره‌نیست ؛

(ب) در R ، $xy = 0$ نتیجه می‌دهد $x = 0$ یا $y = 0$ ؛

(پ) R درقانون حذف صدق می‌کند: اگر در R ، $xa = xb$ و $x \neq 0$ آنگاه $a = b$.

برهان. به‌طورساده(ب) بیان‌دوباره‌ای از (الف) به‌صورتی‌متقارن‌تراست، و به‌وضوح‌معادل‌آن می‌باشد. همچنین، درفوق نشان دادیم که یك‌عنصرقابل حذف است اگر وفقط‌اگر مقسوم‌علیه صفرنباشد. بنابراین(الف) دقیقاً بیان‌می‌کندکه همهٔ‌عناصرغیرصفر قابل حذف‌اند: که همان عبارت (پ) است.

تعریف. حوزهٔ‌صحیح یك حلقهٔ جابجایی است‌که دریکی‌از (وبنابراین درتمام) شرایط قضیهٔ ۸ح صدق‌کندکه‌درآن عناصر ۰ و ۱ متمایزند. (قبلا فرض نکرده‌ایم‌که $0 \neq 1$ ، وبسادگی تحقیق می‌شودکه دقیقاً یك حلقه، حلقه‌های‌یکریخت را یکی‌فرض‌می‌کنیم، وجود دارد که‌درآن $0 = 1$. این حلقه فقط یك عنصر دارد. نکته‌ای مطرح است‌که آیا این حلقه درشرایط‌قضیه صدق‌می‌کند، ولی تحلیلی‌دقیق ومنطقی بایستی خواننده را متقاعدکندکه جواب مثبت است. حال مایلیم وقتی‌که حوزه‌های صحیح را بررسی می‌کنیم این حلقهٔ بدیهی را مستثنی کنیم، گرچه باید اجازه دهیم‌که واقعاً یك حلقه باشد، اگردرحالت‌کلی فرض $0 \neq 1$ را به‌عنوان اصلی برای حلقه‌ها قرار دهیم آنگاه قضیهٔ ۸ح نادرست خواهد بود، زیرا یقیناً تمام‌حلقهٔ R ایده‌آلی از R بوده وخارج‌قسمت مربوطه ، R/R ، فقط دارای یك‌عنصر است!) بامراجعه به‌تعریف، حوزهٔ صحیح حلقه‌ای است جابجایی باحداقل دوعنصر، که درآن قانون حذف برقراراست. مثالهایی‌که به‌ذهن خطورمی‌کنند عبارت‌اند از: $\mathbf{Z}$ ، $\mathbf{Q}$ ، $\mathbf{R}$ و $\mathbf{C}$. درفصل ۱۰ خواهیم دیدکه حلقه‌های معینی ازچندجمله‌ایها نیزحوزهٔ صحیح‌اند.

دلیل اینکه $\mathbf{Q}$ ، $\mathbf{R}$ و $\mathbf{C}$ حوزهٔ صحیح‌اند آن است‌که درهریك ازآنها، هرعنصر غیر صفر یکه است. قبلا نشان داده‌ایم‌که عناصر یکه همیشه قابل حذف‌اند («توجه»صفحهٔ ۱۲۰را ببینید) از اینرو قانون حذف بلافاصله نتیجه می‌شود. چنین حلقه‌هایی ارزش نام خاصی دارند و میدان نامیده می‌شوند. بنابراین‌میدان یك‌حلقهٔ R است‌که، علاوه‌براصول موضوعهٔ

حلقه که در اول فصل آمده‌اند، در قوانین زیر نیز صدق کند:

(ض۳) هر $x\neq 0$ در R دارای معکوسی چون $x^{-1}\in R$ است به قسمی که $xx^{-1}=x^{-1}x=1$ ؛

(ض۴) به‌ازاء هر $x, y\in R$ ، $xy=yx$ ؛

(ج‌ض۲) $1\neq 0$.

این ما را به‌نقطهٔ شروع می‌رساند، زیرا این سه‌قانون، همراه با اصول موضوعهٔ حلقه ، شامل مجموعهٔ کامل قوانین «جبر استانده» است که در فصل ۱ فهرست شده‌اند. حال اگر فهرست کامل، مجدداً مورد مطالعه قرار گیرد ملاحظه می‌شود که یك میدان را می‌توان به‌اختصار به زبان دوساخت گروهی، یعنی ساخت جمعی وضربی، شرح داد. به‌منظور دقیق بودن تعریف میدان‌را دوباره به‌صورت زیر بیان‌می کنیم. میدان F مجموعه‌ای است که دوعمل دوتایی $+$ و $\cdot$ روی آن تعریف شده‌اند به‌قسمی که :

(الف) F نسبت به‌جمع یك گروه آبلی است ؛

(ب) اگر از عنصر صفر این گروه آبلی صرف‌نظر کنیم، آنگاه بقیهٔ عناصر نسبت به‌ضرب تشکیل یك گروه آبلی می‌دهند؛

(پ) ضرب نسبت به‌جمع توزیعی است.

توجه کنید که این سه شرط نتیجه می‌دهند $1\neq 0$ زیرا گروه ضربی که درقسمت(ب)مشخص شده شامل صفر نیست، ولی شامل ۱ هست.

ازمیان انواع فراوان جبر مجرد که امروزه تحت مطالعه وبررسی قرار دارند محتملا میدانها ــ پس‌از گروهها ــ مهمترین‌اند. آنها حوزه‌هایی هستند که درآنجا می‌توان همهٔ اعمال وقواعد جبر استانده را به‌کاربرد. آنها کراراً به‌عنوان منبع ضرایب چندجمله‌ایها ومعادلات خطی ومکان‌مناسبی برای جستجوی حل چنین معادلاتی به‌کار می‌روند. میدان درنظریهٔ اعداد به‌عنوان‌مجموعه‌ای باساخت زیبا از اعداد جبری ودرهندسه به‌عنوان مجموعه‌ای‌ازمختصات ممکنهٔ نقاط به‌کار می‌رود. درتمام این زمینه‌ها، غنای‌ساخت وسادگی‌محاسبات‌جبری‌درمیدان است که آن‌را سودمند ساخته.

همهٔ عناصر غیرصفر میدان قابل حذف‌اند، واین خاصیت درهرزیرحلقهٔ آن‌نیز برقرار است. بنابراین‌همهٔ زیرحلقه‌های‌میدانها حوزهٔ صحیح‌هستند. بایستی از به‌کاربردن نیندیشیدهٔ استدلالهایی نظیر این برحذر بود. مثلا، همهٔ عناصر غیرصفر میدان یکه هستند، اما این خاصیت دریك زیرحلقه‌درست باقی نمی‌ماند زیرا زیرحلقه ممکن است شامل‌عنصرمفروضی

باشد بدون اینکه حاوی معکوس‌آن باشد. ساده‌ترین مثال، زیرحلقهٔ $\mathbf{Z}$ ازمیدان $\mathbf{Q}$ است؛ این زیرحلقه حوزهٔ صحیح‌است (درواقع نخستین نمونه!) ولـی فقط دارای دو عنصر یکه ۱ و ۱— است.

مثال ۱۰۰۸. درمیدان $\mathbf{C}$ ، مجموعهٔ همهٔ‌اعداد صحیح گاوسی $m+in$، که‌در‌آن $m, n \in \mathbf{Z}$ ، یك‌زیرحلقه است و بنا بر این یك‌حوزهٔ صحیح می‌باشد.

مثال ۱۰۰۸. درمیدان $\mathbf{R}$ ، مجموعهٔ S ازهمهٔ اعداد به‌صورت $a+b\sqrt{۲}$ ، که در‌آن a و b اعدادگویا هستند، یك‌زیرحلقه است زیرا ۱ و ۰ به‌این‌صورت هستند ومجموع وحاصلضرب هردوعدد به‌صورت مذکور نیز دارای همین‌صورت است. (توجه کنید که

$$(a+b\sqrt{۲})(a'+b'\sqrt{۲}) = (aa'+۲bb')+(ab'+ba')\sqrt{۲}$$

واعداد $aa'+۲bb'$ و $ab'+ba'$ گویا هستند اگر a ، b ، a' ، b' گویا باشند.) درواقع این زیرحلقهٔ S از $\mathbf{R}$ یك زیرمیدان است. این به‌آن دلیل است‌که اگر a و b اعداد گـویا وهردو باهم صفرنباشند آنگاه معکوس $a+b\sqrt{۲}$ در $\mathbf{R}$ می‌تواند به‌صورت

$$\frac{a-b\sqrt{۲}}{a^۲-۲b^۲} = \frac{a}{a^۲-۲b^۲} + \frac{-b}{a^۲-۲b^۲}\sqrt{۲}$$

نوشته شود و ازاینرو عضوی از S است. بنابراین هرعنصرغیرصفر S یکه است، ودرنتیجه S یك میدان است.

ارتباط بین حوزه‌های صحیح ومیدانها حتی نزدیکتر ازآن است‌که ما تاکنون مطرح کرده‌ایم. نه‌فقط هرزیرحلقه میدان حوزهٔ صحیح است، بلکه هرحوزهٔ صحیح زیرحلقه‌ای‌از یك میدان مناسب است. فصل حاضررا باانبات ایـن نتیجهٔ مهم به‌پایان می‌رسانیم. حـوزهٔ صحیحی مانند D مفروض است می‌خواهیم میدانی مانند F بسازیم به‌قسمی‌کـه D به‌مثابهٔ زیرحلقه‌ای در F باشد. درواقع کاری را که قدری راحتتر است انجام می‌دهیم، بدین‌معنی که میدان F را به‌قسمی‌می‌سازیم که D بازیرحلقه‌ای از F یکریخت باشد؛ یعنی، به‌طوری‌که همریختی یك‌به‌یکی از D به F وجود داشته باشد. بهرحال، پس‌از انجام این امر، می‌توانیم F را به‌قسمی‌پیرایش کنیم (تااندازه‌ای به‌طور مصنوعی) کـه واقعاً D را به‌عنوان زیرحلقه دربرداشته باشد؛ به‌طور ساده نسخهٔ D' یکریخت بـا D را از F بـرداشته و آن‌را با D جایگزین می‌کنیم. سپس مجموعهٔ جدید F' می‌تواند به‌وسیلهٔ فـرایند بهم‌پیوستن و به‌طریقی روشن به‌یك میدان تبدیل‌شود به‌طوری‌که D یك‌زیرحلقهٔ آن باشد. این فرایند «همانندنمودن D باتصویرش در F» نامیده می‌شود و جزئیات صوری آن‌را نمی‌نویسیم.

قضیهٔ ۸.خ. فرض‌کنید D یك‌حوزهٔ صحیح‌باشد. دراین‌صورت میدانی مانند F که D را به‌عنوان

زیرحلقه دربر دارد وجود دارد به‌قسمی‌که هرعنصر F به‌صورت xy^{-1} است، که x ، $y\in D$. میدان F تاحد یکریختی یکتا و دارای خاصیت جامع زیر است: اگر $\theta : D\longrightarrow F'$ جادهی دلخواهی از D دریك میدان باشد (یعنی، همریختی حلقه‌ای یك‌به‌یك به‌توی یك میدان) آنگاه θ می‌تواند به‌طور یکتا به‌یك جادهی F در F' توسعه داده شود.

برهان. مفتاح پی‌بردن به‌ساختمان F، صورت عناصرآن، یعنی xy^{-1} است. Fرا به‌صورت مجموعه‌ای از«کسرها»ی x/y، که درآن $y\in D$ ، x ، تعریف‌خواهیم کرد، ولی‌تعریف‌اینها نیاز به‌دقت بیشتری دارد. قواعدآشنای محاسبات‌کسرها به‌ما می‌گوید‌که مخرج‌کسر نباید هرگز صفرباشد واینکه x/y و x'/y' یك‌کسرند هرگاه $xy'=yx'$. بنابراین تجربهٔ‌خود از روابط هم‌ارزی را به‌کارگرفته‌کسرها را به‌مثابهٔ رده‌های هم‌ارزی جفتهای $(x\ ,\ y)$ تعریف می‌کنیم. جزئیات امر به‌صورت زیر است. فرض‌کنید $S\subset D\times D$ مجموعهٔ همهٔ جفتهای $(x\ ,\ y)$ باشد، که $y\in D$ ، x و $y\neq 0$. رابطهٔ $\sim$ روی S رابا قاعدهٔ زیرتعریف کنید:

$$(x\ ,\ y)\sim(x'\ ,\ y') \quad \text{اگر در } D\ ،\ xy'=yx' .$$

نخست‌محقق می‌سازیم‌که $\sim$ رابطه‌ای هم‌ارزی است. واضح است‌که انعکاسی هست، زیرا $xy=yx$. همچنین، متقارن است، زیرا با به‌کار بردن مجدد قانون جابجایی در D ، اگر $xy'=yx'$ آنگاه $x'y=y'x$. اثبات قانون تعدی کمی مشکل‌تر است، فرض کنید که در S داریم : $(x\ ,\ y)\sim(x'\ ,\ y')\sim(x''\ ,\ y'')$. دراین صورت $xy'=yx'$ و $x'y''=y'x''$ ، که ازآنجا $xy'y''=yx'y''=yy'x''$. چون D حوزهٔ صحیح است و، بنابه‌تعریف، $y'\neq 0$ ، می‌توان y' را از طرفین تساوی اخیر حذف‌کرد و به‌دست آورد: $xy''=yx''$ ؛ یعنی $(x\ ,\ y)\sim(x''\ ,\ y'')$. رده‌های هم‌ارزی $\sim$ روی S کسر نامیده می‌شوند و x/y را برای ردهٔ هم‌ارزی شامل $(x\ ,\ y)$ می‌نویسیم. فرض می‌کنیم Fمجموعهٔ همهٔ این‌کسرها باشد، یعنی $F=S/\sim$. باید F را به‌وسیلهٔ تعریف اعمال مناسبی روی کسرها به‌یك‌میدان تبدیل‌کنیم. ابتدا جمع‌را به‌صورت زیر تعریف می‌کنیم

$$\frac{x}{y}+\frac{x'}{y'}=\frac{xy'+yx'}{yy'} \qquad (1)$$

چون این عملی است‌روی مجموعهٔ خارج قسمت دیگربار بااین سؤال مواجه هستیم که آیا این عمل خوش تعریف است. خواننده را به‌قضیهٔ‌عوپ رجوع می‌دهیم و استدلال لازم را عرضه می‌کنیم . فرض کنید که در S ، داریم $(x_1\ ,\ y_1)\sim(x_2\ ,\ y_2)$ و $(x'_1\ ,\ y'_1)\sim(x'_2\ ,\ y'_2)$. باید نشان دهیم‌که در S ،

$$(x_1y_1'+y_1x_1'\ ,\ y_1y_1')\sim(x_2y_2'+y_2x_2'\ ,\ y_2y_2') .$$

حال D یك حلقه است، ازاینرو هردوی این‌جفتها در $D\times D$ قرار دارند؛ همچنین چونD حوزهٔ صحیح است و y_1 ، y_2 ، y_1' و y_2' همگی غیر صفرند، داریم $y_1y_1'\neq 0$ و

$y_۲y_۲' \neq ۰$ ، پس جفتهای مذکور در S قرار دارند. باقی می‌ماند که در D نشان دهیم:

$$(x_۱y_۱' + y_۱x_۱')(y_۲y_۲') = (y_۱y_۱')(x_۲y_۲' + y_۲x_۲') .$$

این تساوی از روابط مفروض $x_۱y_۲ = y_۱x_۲$ و $x_۱'y_۲' = y_۱'x_۲'$ به‌دست می‌آید زیرا

$$\begin{aligned}(x_۱y_۱' + y_۱x_۱')(y_۲y_۲') &= x_۱y_۲y_۱'y_۲' + y_۱y_۲x_۱'y_۲' \\ &= y_۱x_۲y_۱'y_۲' + y_۱y_۲y_۱'x_۲' \\ &= (y_۱y_۱')(x_۲y_۲' + y_۲x_۲') .\end{aligned}$$

پس‌از اینکه به‌وسیلهٔ معادلهٔ (۱) خوش تعریفی جمع روی F را ثابت‌کردیم، تحقیق‌می‌کنیم که جمع مزبور F را یك‌گروه آبلی می‌سازد. واضح است کـه ۰/۱ به‌عنوان عنصر صفر عمل می‌کند وجمع جابجایی است. قانون شرکت‌پذیری به‌وسیلهٔ بررسی اینکه هردو روش پرانتزگذاری عبارت زیر

$$\frac{x}{y} + \frac{x'}{y'} + \frac{x''}{y''}$$

مارا به‌کسر

$$\frac{xy'y'' + yx'y'' + yy'x''}{yy'y''}$$

می‌رساند، اثبات می‌شود. همانند معکوسهای جمعی، ملاحظه می‌شود که

$$\frac{۰}{yy} = \frac{۰}{۱} \quad \text{و} \quad \frac{x}{y} + \frac{-x}{y} = \frac{۰}{yy}$$

زیرا $۰ \times yy = ۱ \times ۰$. بنابراین $-x/y$ معکوس جمعی x/y است.

ضرب در F را باضابطهٔ

$$\frac{x}{y} \cdot \frac{x'}{y'} = \frac{xx'}{yy'} \qquad (۲)$$

به‌ازاء هر $y, y' \in D$ ، x, x' با $y' \neq ۰$ ، y ، تعریف مـی‌کنیم. اثبات ایـن‌راکه (۲) نامبهم است وعملی روی F تعریف می‌کند به‌عهدهٔ خواننده می‌گذاریم. واضح است که‌عمل جابجایـی وشرکت‌پذیر است ودارای عنصرخنثای ۱/۱ است تحقیق قانـون توزیعی ساده است:

$$\left(\frac{x}{y} + \frac{x'}{y'}\right)\frac{x''}{y''} = \frac{(xy' + yx')x''}{yy'y''}$$

$$= \frac{(xy' + yx')x''}{yy'y''}$$

$$= \frac{xx''}{yy''} + \frac{x'x''}{y'y''}.$$

بنابراین F یك حلقهٔ جابجایی است وباقی می‌ماند نشان دهیم که هرعنصرغیرصفر x/y یکه است. ولی اگر $(x/y) \neq (۰/۱)$ آنگاه $x \neq ۰$ ، از اینرو $(y/x) \in F$ و واضح است که

$$\frac{x}{y} \cdot \frac{y}{x} = \frac{xy}{yx} = \frac{۱}{۱}.$$

این نشان می‌دهد که F یك میدان است.

حال F شامل D نیست، اما نگاشت واضحی مانند $\sigma : x \longrightarrow x/۱$ از D به F وجود دارد که یك همریختی یك به‌یك حلقه‌هاست (این را تحقیق کنید!). بنابراین همان‌طور که در فوق توضیح داده شد D را با تصویرش در F همانند می‌گیریم، پس از این x را به‌جای $x/۱$ می‌نویسیم. دراین نمادگذاری، به‌ازاء هر $y \neq ۰$ در D داریم

$$y^{-۱} = \left(\frac{y}{۱}\right)^{-۱} = \frac{۱}{y},$$

وبنابراین همان‌طور که ادعا شده است داریم

$$\frac{x}{y} = xy^{-۱}.$$

حال خاصیت جامع F را ثابت می‌کنیم. اگر $\theta : D \longrightarrow F'$ یك جادهی D درمیدان دیگری باشد، ملاحظه می‌کنیم که ، به‌ازاء $y \neq ۰$ در D ، $\theta(y) \neq ۰$ ، ازاینرو $\theta(y)$ دارای معکوسی در F' است. اگر قرار است که θ به‌یك جادهی $\theta^* : F \longrightarrow F'$ توسعه‌داده شود، θ^* باید معکوسها را حفظ کند، ازاینرو $\theta^*(y^{-۱}) = \theta(y)^{-۱}$ وباید داشته‌باشیم

$$\theta^*(xy^{-۱}) = \theta(x)\theta(y)^{-۱} \qquad (۳)$$

این نشان می‌دهد که θ^*، درصورت وجود، یکتاست. برای اثبات وجود بایستی نشان دهیم که (۳) نامبهم است، یعنی اگر در F ،

$$\frac{x}{y} = \frac{x'}{y'}$$

آنگاه بایدنشان دهیم که در F' ، $\theta(x)\theta(y)^{-۱} = \theta(x')\theta(y')^{-۱}$. این را به‌عهدهٔ خواننده می‌گذاریم که بعلاوه باید تحقیق کند نگاشت θ^* که به‌وسیلهٔ (۳) تعریف شده است درواقع جمع وضرب را حفظ می‌کند و ۱ را به ۱ می‌فرستد. اینکه θ^* یك‌به‌یك است ازاین‌مطلب به‌دست می‌آید که اگر $\theta^*(xy^{-۱}) = ۰$ آنگاه در F' ، $\theta(x)\theta(y)^{-۱} = ۰$ و از اینرو

$\theta(x)=0$ ، ولی این نتیجه می‌دهد $x=0$ ، زیرا θ یك‌به‌یك است. بنابراین $\operatorname{Ker}\theta^*=0$ وبنابه قضیهٔ عرج ونتیجه‌اش، θ^* یك‌به‌یك است. اکنون یکتایی F به‌آسانی نتیجه می‌شود؛ اگر D به‌وسیلهٔ نگاشتی مانند θ درمیدان F' جا داده شود، به‌طریقی که هرعنصر F' بتواند به‌ازاء x ، $y\in D$ مناسبی، به‌صورت $\theta(x)\theta(y)^{-1}$ نوشته‌شود، آنگاه نگاشت $\theta^*: F\longrightarrow F'$ بروی و بنابراین یکریختی است.

میدان F که از D ساخته‌شده‌است میدان‌کسرهای D نامیده می‌شود. این‌میدان‌علی‌رغم طولانی‌بودن‌برهان وجودش، از اهمیت فراوانی برخوردار است و اساساً ساختمان روشن و ساده‌ای‌می‌باشد. دومثال‌اصلی(اعداد گویا وتوابع گویا) در دوفصل‌آینده به‌تفصیل‌موردبحث قرار خواهند گرفت.

تمرینها

۱. ثابت‌کنیدکه حلقهٔ R جابجایی است اگروفقط‌اگر، به‌ازاء هر x ، $y\in R$ ، رابطهٔ $(x+y)(x-y)=x^2-y^2$ درست باشد.

۲. ثابت‌کنیدکه گروه یکه‌های حلقهٔ اعداد صحیح گاوسی(مثال۱۰.۸) گروهی دوری از مرتبهٔ ۴ است.

۳. ثابت‌کنیدکه مجموعهٔ همهٔ‌اعدادحقیقی به‌صورت $m+n\sqrt{2}$ ، که درآن m ، $n\in\mathbf{Z}$، یك‌حوزهٔ صحیح است. نشان دهید که دراین حلقه $m+n\sqrt{2}$ عنصری‌یکه است اگر وفقط‌اگر $m^2-2n^2=\pm 1$.

۴. دستوری مشابه قضیهٔ‌عرج برای حلقه‌ها تنظیم‌کرده آن‌راثابت‌کنید.

۵. ثابت‌کنیدکه تنها ایده‌آلهای یك میدان F ، $\{0\}$ وخود F هستند. بنابراین نشان‌دهید که هرهمریختی حلقه‌ای بین دومیدان یك‌به‌یك است.

۶. ثابت‌کنیدکه حلقهٔ M متشکل ازتمام ماتریسهای حقیقی $n\times n$ فقط دارای دوایده‌آل $\{0\}$ و خود M است. (راهنمایی: اثر ضرب‌عناصر یك ایده‌آل را در (الف) ماتریسهای مبنای E_{ij} با عدد ۱ درمکان $(i\ ,\ j)$ ام و صفر دربقیهٔ مکانها و (ب) ماتریسهای اسکالر λI ، بررسی‌کنید.)

۷. نشان دهیدکه اگر D یك‌حوزهٔ صحیح و $d\in D$ عنصری ثابت وغیرصفر باشد، آنگاه نگاشت $x\longmapsto dx$ از D به D یك‌به‌یك است. درمورد D متناهی نتیجه بگیریدکه این نگاشت دوسویی است و بنابراین ثابت کنیدکه هرحوزهٔ صحیح متناهی یك میدان است.

۸. فرض کنید R حلقه‌ای دلخواه و $\sigma:\mathbf{Z}\longrightarrow R$ همریختی متعارف باشد، که به‌وسیلهٔ $\sigma(n)=\overline{n}=n1$ داده شده است. بادرنظرگرفتن‌هستهٔ σ ، نشان‌دهیدکه‌عدد

صحیح یکتای $k \geqslant 0$ (که مشخصهٔ R نامیده می‌شود) وجود دارد به‌قسمی که (الف) به‌ازاء هر $x \in R$ ، $kx = 0$ ، و (ب) اگر به‌ازاء هر $x \in R$ ، $mx = 0$ آنگاه $k|m$. ثابت کنید که اگر R حوزهٔ صحیح باشد آنگاه مشخصهٔ آن، ۰ یا یك عدد اول است. نتیجه بگیرید که تمام عناصر غیر صفر یك حوزهٔ صحیح دارای مرتبهٔ جمعی برابرند.

۹. ثابت کنید که اگر R و S دوحلقهٔ جابجایی و هریك حداقل دارای دوعنصر باشند، آنگاه $R \times S$ نمی‌تواند یك‌حوزهٔ صحیح باشد.

فصل ۹

حلقه‌های $\mathbf{Z}_n$ و میدان $\mathbf{Q}$

ساده‌ترین حلقه‌ای که دراختیار داریم حلقهٔ اعداد صحیح $\mathbf{Z}$ است، و اکنون حلقه‌هایی را مورد مطالعه قرار می‌دهیم که با به کاربردن ساختمانهای مجرد فصل ۸ از $\mathbf{Z}$ به دست می‌آیند.

نخست، تعیین‌زیرحلقه‌های $\mathbf{Z}$ کاری ساده است. هرزیر حلقه شامل ۱ است و ازاینرو بایستی شامل زیرگروه جمعی تولید شده به‌وسیلهٔ ۱، که همان $\mathbf{Z}$ است، باشد. بنابراین $\mathbf{Z}$ تنها زیرحلقه است.

اما ایده‌آلهای $\mathbf{Z}$ را نیز از پیش می‌شناسیم. هرایده‌آل یك زیرگروه جمعی است، ازاینرو بایستی به ازاء عدد صحیحی چون $n \geqslant 0$، به صورت $n\mathbf{Z}$ باشد (قضیهٔ ۴ پ). بعکس، هرزیرگروه $n\mathbf{Z}$، ایده‌آلی از $\mathbf{Z}$ است، زیرا اگر $m \in n\mathbf{Z}$ آنگاه $n|m$، از اینرو به ازاء هرعدد صحیح r، $n|mr$، که از آنجا $mr \in n\mathbf{Z}$. این استدلال اخیر در هرحلقهٔ جابجایی R درست است: اگر $a \in R$-آنگاه مجموعهٔ $aR = \{ar\ ;\ r \in R\}$ ایده‌آلی از R است. ایده‌آلهایی که بدین طریق تشکیل می‌شوند ایده‌آلهای اصلی و عنصر a یك مولد ایده‌آل aR نامیده می‌شود. بنابراین قضیهٔ ۴ پ بیان می‌کندکه هرایده‌آل $\mathbf{Z}$ یك ایده‌آل اصلی، $n\mathbf{Z}$، است که به وسیلهٔ عددی چون $n \geqslant 0$ تولید می‌شود.

حال، نسبت به‌هریك‌ازاین ایده‌آلهای $n\mathbf{Z}$، به‌ازاء $n \geqslant 1$، می‌توانیم حلقهٔ‌خارج‌قسمت $\mathbf{Z}/n\mathbf{Z}$ راتشکیل‌دهیم، که‌به‌وسیلهٔ $\mathbf{Z}_n$ نشان‌داده‌می‌شود. (حالت $n = 0$ را از بررسی‌استثنامی کنیم زیرا $\mathbf{Z} \cong \mathbf{Z}/\{0\} = \mathbf{Z}/0\mathbf{Z}$ حلقهٔ‌جدیدی‌نیست). قبلا $\mathbf{Z}_n$ را به‌عنوان گروهی‌جمعی‌دیده‌ایم. این گروه رده‌های‌باقیماندهٔ به‌پیمانهٔ n است‌و گروهی‌است دوری‌ازمرتبهٔ n که به‌وسیلهٔ ردهٔ‌باقیماندهٔ $\langle 1 \rangle$ شامل ۱، تولیدمی‌شود. این‌حقیقت‌جدید که‌ازقضیهٔ ۸ ج ناشی شده‌این است که به‌دلیل

ایده‌آل بودن $n\mathbf{Z}$ ، ضرب رده‌های باقیمانده نیز برطبق قاعدهٔ $\langle x\rangle\langle y\rangle=\langle xy\rangle$ امکان‌پذیر است واز این جهت گروه رده‌های باقیمانده تشکیل یك حلقه می‌دهد. این حلقهٔ $\mathbf{Z}_n$ جابجایی است زیرا $\mathbf{Z}$ جابجایی است ، عنصر همانی آن $\langle 1\rangle$ و «اعدادصحیح» آن $\langle r\rangle=\langle r\rangle\langle 1\rangle=\bar{r}r$ هستند. بنابراین پس ازاین $\bar{r}$ را برای ردهٔ باقیماندهٔ $\langle r\rangle$ در $\mathbf{Z}_n$ خواهیم نوشت. توجه کنید که $\bar{r}$ تصویر r تحت‌نگاشت خارج قسمت $\mathbf{Z}\longrightarrow\mathbf{Z}_n$ بوده که هسته‌اش $n\mathbf{Z}$ است .

مثال ۱۰.۹. حلقهٔ $\mathbf{Z}_4$ دارای جدولهای جمع و ضرب زیر است:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

اثبات برقراری‌اصول موضوعهٔ حلقه به‌کمك این جدولها کار بسیار کسل‌کننده‌ای است؛ ولی این ضرورتی ندارد زیرا تحلیل‌ما ازحلقه‌های خارج قسمت پیشاپیش آن را تضمین می‌کند. اعمال ابتدا به‌وسیلهٔ انجامشان در $\mathbf{Z}$ وسپس تحویلشان به پیمانهٔ ۴ ، صورت گرفته‌اند. البته، به‌ازاء هر n ، به‌همین ترتیب انجام می‌شود. توجه کنید که $\mathbf{Z}_4$ یك حوزهٔ صحیح نیست‌زیرا $\bar{0}=\bar{2}\cdot\bar{2}$.عناصریکه‌آن $\bar{1}$ و $\bar{3}$ هستند، که تشکیل یك گروه دوری از مرتبهٔ ۲ می‌دهند.

واضح است که هیچ دو حلقهٔ $\mathbf{Z}_n$ ($n=1,2,3,\dots$) یکریخت نیستند زیرا هیچ دوتایی از آنها دارای تعداد عناصر مساوی نمی‌باشند. بنابراین تعداد بینهایت حلقهٔ متناهی واقعاً متفاوت ساخته‌ایم. به محاسبه دراین حلقه‌ها غالباً به‌عنوان «حساب پیمانه‌ای» اشاره می‌شود و به‌طور مشروع می‌توان‌همهٔ قوانین‌حلقه‌های‌جابجایی را به‌کاربرد ــ به‌استثنای‌قانون (ض ۳) وقانون حذف، البته بجز درحالتهای خاص. برای تعیین اینکه‌کدام یك ازحلقه‌های $\mathbf{Z}_n$ از این قوانین اضافی پیروی می‌کنند بایستی یکه‌های $\mathbf{Z}_n$ را پیداکنیم.

قضیهٔ ۹.۲. عنصر $\bar{r}$ از حلقهٔ $\mathbf{Z}_n$ یکه است اگر و فقط اگر r و n متباین باشند.

برهان. چون $\mathbf{Z}_n$ یك حلقهٔ جابجایی است،

$\bar{r}$ عنصریکهٔ $\mathbf{Z}_n$ است $\Leftrightarrow$ در $\mathbf{Z}_n$ بـه ازاء عددی چون $s\in\mathbf{Z}$ ، $\bar{r}\cdot\bar{s}=\bar{1}$

$\Leftrightarrow$ در $\mathbf{Z}_n$ به ازاء عـددی چون $s\in\mathbf{Z}$ ، $\overline{rs}=\bar{1}$

$\Leftrightarrow$ به‌ازاء عددی‌چون $s\in\mathbf{Z}$ ، (به پیمانهٔ n) $rs\equiv 1$

$\Leftrightarrow$ بنا به قضیهٔ ۷ب ، $(r,n)=1$.

نتیجه. حلقهٔ $\mathbf{Z}_n$ میدان است اگر وفقط اگر n عددی اول باشد.

برهان. اگر n یك‌عدد اول‌باشد آنگاه به‌ازاء هر rکه برn قابل قسمت‌نیست، $(r,n)=1$؛ بنابراین در $\mathbf{Z}_n$ ، هر $\bar{r}\neq\bar{0}$ یك یکه است، از اینرو $\mathbf{Z}_n$ میدان است. از طرف دیگر، اگر $n>1$ اول نباشد، آنگاه به ازاء اعداد صحیح مناسب r_1 ، r_2 که در شرایط $1<r_1<n$ ، $1<r_2<n$ صادق‌اند، $n=r_1r_2$. در این حالت در $\mathbf{Z}_n$ داریم $\bar{r}_1\bar{r}_2=\bar{n}=\bar{0}$ ، ولـی $\bar{r}_1\neq\bar{0}$ و $\bar{r}_2\neq\bar{0}$ ، از اینرو $\mathbf{Z}_n$ نه فقط یك میدان نمی‌باشد ، بلکـه یك حوزهٔ صحیح هم نیست .

اکنون‌دسته‌ای نامتناهی ازمیدانهای‌متناهی $\mathbf{Z}_2$ ، $\mathbf{Z}_3$ ، $\mathbf{Z}_5$ ، $\mathbf{Z}_7$ ، $\mathbf{Z}_{11}$ ، ... ساخته‌ایم (این دسته به موجب تمرین ۱۳ از فصل ۵ نامتناهی است.) حساب به پیمانهٔ یك عدد اول از تمام قوانین جبر استانده پیروی می‌کند ، و این مطلب تبصره‌هـای فصل ۷ دربارهٔ حل دستگاه همنهشتیهای چندمجهولی را نسبت به‌یك پیمانهٔ تك توضیح‌می‌دهد. اگر اتفاقاً پیمانه عددی اول باشد آنگاه همهٔ قـواعد معمولی حـذف مجازند و جـوابها می‌توانند به وسیلهٔ آلگوریتمهای استانده برای معادلات خطی پیدا شوند. اشاره می‌کنیم که به‌ازاء اعداد اول p ، میدانهای $\mathbf{Z}_p$ تنها میدانهای متناهی نیستند. در واقـع میدانی بـا q عنصر وجود دارد وقتی که q توانی از یك عدد اول باشد ، ولی ساختن آن هنگامی کـه q اول نباشد کمی مشکلتر است .

مثال ۲.۹. عناصر ۰ ، ۱ ، a ، b با جمع وضربی که به وسیلهٔ جدولهای

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

×	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

تعریف شده‌اند تشکیل یك میدان می‌دهند. درفصل آینده روشی ازاثبات این مطلب بدون تحقیق مستقیم همهٔ قوانین به‌دست‌خواهیم داد.

گروه ضربی یکه‌های $\mathbf{Z}_n$ را با U_n نشان می‌دهیم. بنابه قضیهٔ ۹ آ ، عناصر U_n رده‌های باقیماندهٔ $\bar{r}$ هستند، که $1 \leqslant r \leqslant n$ و $(r, n) = 1$. بنابراین تعداد عناصر U_n برابر است با $\varphi(n)$ ، که درآن φ تابع اویلر است (صفحهٔ۱۵۸را ببینید). (توجه کنیدکه یکه‌های $\mathbf{Z}_n$ همان عناصر مولدگروه جمعی $\mathbf{Z}_n$ هستند. برای ملاحظهٔ عبارت مشابه در مورد حلقه‌های عام، تمرین ۱۲ آخر همین فصل را ببینید.) حال دریك گروه متناهی از مرتبهٔ m هرعنصر دارای مرتبه‌ای است که m را عاد می‌کند و بنابراین توان m ام آن ، عنصر همانی است (نتیجهٔ۲ از قضیهٔ ۴ ج). چنانچه این را به‌گروه U_n از مرتبهٔ $\varphi(n)$ به‌کار ببریم، می‌بینیم که در $\mathbf{Z}_n$ به ازاء هر یکهٔ $\bar{r}$ ، $\bar{r}^{\varphi(n)} = \bar{1}$. اگراین عبارت را به‌زبان همنهشتیها برگردانیم، قضیهٔ زیر به‌دست می‌آید.

قضیهٔ ۹ ب. (قضیهٔ اویلر) . فرض کنید n عددی صحیح و مثبت باشد. دراین صورت به ازاء همهٔ اعداد صحیح r متباین با n :

$$r^{\varphi(n)} \equiv 1 \quad (\text{به پیمانهٔ } n) .$$

برهان. اگر $(r, n) = 1$ آنگاه بنابه قضیهٔ ۹ آ ، در $\mathbf{Z}_n$ ، $\bar{r}$ یکه است. بنابراین به‌موجب استدلال فوق ، در $\mathbf{Z}_n$ ، $\bar{r}^{\varphi(n)} = \bar{1}$ ، یعنی $r^{\varphi(n)} \equiv 1$ (به پیمانهٔ n) .

نتیجهٔ ۱. (قضیهٔ فرما[1]). فرض کنید p عددی اول باشد، در این صورت به‌ازاء همهٔ اعداد صحیح r که بر p قابل قسمت نیستند:

$$r^{p-1} \equiv 1 \quad (\text{به پیمانهٔ } p) .$$

برهان. وقتی که p اول باشد ، $\varphi(p) = p - 1$. همچنین ، هنگامی که p اول باشد ، $(r, p) = 1 \iff p \nmid r$.

نتیجهٔ ۲. (صورت دیگر قضیهٔ فرما .) فرض کنید p عددی اول باشد ، در این صورت به ازاء همهٔ اعداد صحیح n ،

$$n^p \equiv n \quad (\text{به پیمانهٔ } p) .$$

---

1. Fermat .

برهان. به عنوان تمرین می گذاریم .

دو نتیجهٔ اخیر شامل اطلاعاتی غنی از حساب است، من بـاب مثال این به هیچ وجه روشن‌نیست که $۱ - ۵^۶$ بر ۷ و $۱ - ۱۷^۴$ بر ۱۲ قابل قسمت‌است. برهانی که ارائه‌داده‌ایم بیشترین بصیرت را دراین امر به دست می‌دهد که چرا چنین همنهشتیهایی درست هستند. در اصل این نتایج با روشهای کاملا متفاوتی اثبات شده‌اند و شاید بیارزدکه برهان مقدماتیتری ازقضیهٔ فرما داده شود. فرض کنید p عددی اول و r عددی صحیح باشدکه بر p قابل‌قسمت نیست. درآن صورت اعداد صحیح r ، $۲r$ ، $۳r$ ، ... ، $(p-۱)r$ در رده‌هـای باقیماندهٔ متمایز به‌پیمانهٔ p قراردارند (زیرا اگر $rx \equiv ry (p$ به‌پیمانهٔ $p)$ آنگاه $x \equiv y (p$ به‌پیمانهٔ $p)$؛ به ازاء r و p متباین). بنابراین هریك ازاین اعداد دریك ردهٔ باقیماندهٔ غیرصفر قرار دارد و ازاینرو حاصلضربشان به‌ردهٔ باقیماندهٔ $(p-۱)$ ... ۳ . ۲ . ۱ متعلق‌است. به‌عبارت‌دیگر،

$$r^{p-۱} \cdot ۱ \cdot ۲ \cdot ۳ \cdots (p-۱) \equiv ۱ \cdot ۲ \cdot ۳ \cdots (p-۱) \quad (\text{به پیمانهٔ } p)$$

ونتیجه‌می گیریم که $r^{p-۱} \equiv ۱ (p$ به‌پیمانهٔ $p)$ زیرا می توانیم‌هریك‌از ۱ ، ۲ ، ۳ ، ... ، $p-۱$ را از طرفین حذف کنیم . (خوانندهٔ فکور تشخیص می‌دهدکه اساس این برهان را می‌توان درهرگروه آبلی G به‌کاربرد: ضرب به‌وسیلهٔ $r \in G$ عناصر G را جایگشت می‌دهد، ازاینرو حاصلضربشان را تغییر نمی‌دهد،واین‌مطلب نتیجهٔ ۲ازقضیهٔ ۴ج را درحالت آبلی اثبات‌می کند. بنابراین دو برهان چندان باهم تفاوت ندارند !).

مثال ۳.۹. ازقضایای فرما و اویلر می‌توان همنهشتیهای بیشتری استنتاج کرد. مثلا ، به ازاء همهٔ اعداد صحیح n ، (به‌پیمانهٔ $n^{۱۳} \equiv n (۲۷۳۰$. برای اثبات آن ، ملاحظه می کنیم کـه $۱۳ \times ۷ \times ۵ \times ۳ \times ۲ = ۲۷۳۰$ حاصلضربی از اعداد اول متمایز است ، از اینرو کافی است‌نشان‌دهیم که به‌ازاء $p = ۲ ، ۳ ، ۵ ، ۷ ، ۱۳$ و به‌ازاء هر n، (به پیمانهٔ p) $n^{۱۳} = n$. اگر $p = ۱۳$ ، قضیهٔ فرما به ما می گوید که (به‌پیمانهٔ p) $n^{۱۳} \equiv n$. برای $p = ۷$ ، داریم (به‌پیمانهٔ ۷) $n^۷ \equiv n$ ، که ازآنجا (به‌پیمانهٔ ۷) $n^{۱۳} = n^۷ \cdot n^۶ \equiv n \cdot n^۶ \equiv n^۷ \equiv n$. برای $p = ۵$ چنین استدلال می کنیم که

$$n^{۱۳} = n^۵ \cdot n^۸ \equiv n \cdot n^۸ = n^۵ \cdot n^۴ \equiv n \cdot n^۴ = n^۵ \equiv n \quad (\text{به‌پیمانهٔ } ۵)$$

واستدلالهای مشابه‌همنهشتیهای‌عمومی(به‌پیمانهٔ p) $n^{۱۳} \equiv n$ را به ازاء $p = ۲ ، ۳$ به دست می‌دهد .

پس ازاین ، خطهای روی عناصر $\mathbf{Z}_n$ را حذف خواهیم کرد بجز در مواردی‌که‌برای روشنی امور لازم باشند. بنابـراین ، به عنوان مثال ، در $\mathbf{Z}_n$ می‌نـویسیم $r = s$ ، به معنی (به‌پیمانهٔ n) $r \equiv s$ وگوییم که r یکه‌ای در $\mathbf{Z}_{۱۲}$ است، با عنصرمعکوس $۲ - = ۱۱$.

یکه‌های $\mathbf{Z}_n$ می‌توانند به‌طریقی دیگر ، یعنی به عنوان ریشه‌هـای ۱ در $\mathbf{Z}_n$ توصیف شوند؛ زیرا اگردر $\mathbf{Z}_n$ ، $x^k = ۱$ آنگاه واضح‌است‌که x یکه‌ای با معکوس $x^{k-۱}$ است و، ازطرف دیگر، بنابه قضیهٔ اویلر، هریکه از $\mathbf{Z}_n$ ریشهٔ $\varphi(n)$ ام ۱ است. بنابراین هریکهٔ $\mathbf{Z}_n$

به‌ازاء عددی چون $k \geqslant 1$ ، یك ریشهٔ k ام اولیهٔ ۱ است؛ این عدد k ، مرتبهٔ ضربی عنصر یکه در گروه U_n است.

مثال ۴.۹. یکه‌های $\mathbf{Z}_8$ عبارت‌اند از: ۱ ، ۳ ، ۵ و ۷ . از میان اینها ، ۱ دارای مرتبهٔ ۱ و بقیه دارای مرتبهٔ ۲ هستند. از اینرو $\mathbf{Z}_8$ دارای سه ریشهٔ دوم اولیهٔ ۱ است و دارای هیچ ریشهٔ چهارم اولیهٔ ۱ نیست. بنابراین گروه یکه‌های U_8 دوری نیست بلکه همان ۴-گروه کلاین است (مثال ۵.۶ و تمرین ۱۲ از فصل ۶ را ببینید).

مثال ۵.۹. یکه‌های $\mathbf{Z}_7$ عبارت‌اند از: ۱ ، ۲ ، ۳ ، ۴ ، ۵ و ۶. توانهای ۳ به پیمانهٔ ۷ عبارت‌اند از : $۳^۱ = ۳$ ، $۳^۲ = ۲$ ، $۳^۳ = -۱$ ، $۳^۴ = -۳$ ، $۳^۵ = -۲$ و $۳^۶ = ۱$ ، از اینرو ۳ یك ریشهٔ ششم اولیهٔ ۱ در $\mathbf{Z}_7$ است و U_7 گروهی دوری از مرتبهٔ ۶ است.

این سؤال که آیا گروه U_n دوری است یا خیر بسادگی می‌تواند در مورد یك مقدار خاص n به وسیلهٔ محاسبهٔ مستقیم توانهای همهٔ یکه‌ها جواب داده شود. درحالتی که p اول باشد می‌توان ثابت کرد که U_p دوری است، یعنی به‌ازاء هرعدد اول p ، یك ریشهٔ $(p-1)$ ام اولیه به پیمانهٔ p وجود دارد. این مطلب خیلی مشکل است، ارائهٔ پاسخ کلی به‌سؤال «چه‌وقت U_n دوری است؟» ازآن هم مشکلتر است، اما با به‌کاربردن قضیهٔ زیر برخی ازحالات می‌تواند حل وفصل شود.

قضیهٔ ۹پ. اگر m و n دوعدد صحیح مثبت‌باشند و $(m , n) = ۱$ ، آنگاه

$$\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn} ,$$

که یکریختی حلقه‌هاست.

برهان. دراینجا نماد $\bar{r}$ مبهم است زیرا با سه حلقهٔ متفاوت $\mathbf{Z}_m$ ، $\mathbf{Z}_n$ ، $\mathbf{Z}_{mn}$ سروکار داریم . بنابراین برای رده‌های باقیماندهٔ r درحلقه‌های $\mathbf{Z}_m$ و $\mathbf{Z}_n$ به‌ترتیب $\bar{r}_{(m)}$ و $\bar{r}_{(n)}$ می‌نویسیم . نگاشتهای $r \longrightarrow \bar{r}_{(m)}$ و $r \longrightarrow \bar{r}_{(n)}$ ، از $\mathbf{Z}$ به $\mathbf{Z}_m$ و $\mathbf{Z}_n$، همریختیهای‌حلقه‌ای‌هستند. بنابه تعریف‌اعمال‌حلقه‌ای در $\mathbf{Z}_m \times \mathbf{Z}_n$ بلافاصله نتیجه‌می‌شود که نگاشت $\theta : r \longrightarrow (\bar{r}_{(m)} , \bar{r}_{(n)})$ از $\mathbf{Z}$ به $\mathbf{Z}_m \times \mathbf{Z}_n$ یك همریختی حلقه‌ای است. (به عنوان مثال،

$$\begin{aligned} r+s \longrightarrow (\overline{(r+s)}_{(m)} , \overline{(r+s)}_{(n)}) &= (\bar{r}_{(m)} + \bar{s}_{(m)} , \bar{r}_{(n)} + \bar{s}_{(n)}) \\ &= (\bar{r}_{(m)} , \bar{r}_{(n)}) + (\bar{s}_{(m)} , \bar{s}_{(n)}) , \end{aligned}$$

ازاینرو θ حافظ عمل‌جمع است.) تااین اندازه برای m و n دلخواه درست است. هستهٔ θ مجموعهٔ اعداد صحیح r است به قسمی که $\bar{r}_{(m)} = \bar{0}_{(m)}$ و $\bar{r}_{(n)} = \bar{0}_{(n)}$ ، یعنی به‌طوری که

$m|r$ و $n|r$. اگر n و m متباین باشند، نتیجه می‌شود که هستهٔ θ مجموعهٔ تمام مضارب mn است (قضیهٔ ۵ ب (ث) را ببینید.)، یعنی $\mathrm{Ker}\theta = mn\mathbf{Z}$. حال قضیهٔ اول یکریختی برای حلقه‌ها (قضیهٔ ۸ ج) را به‌کار می‌بریم تا استنتاج کنیم که تصویر θ با $\mathbf{Z}/\mathrm{Ker}\theta = \mathbf{Z}/mn\mathbf{Z} = \mathbf{Z}_{mn}$ یکریخت است. اما $\mathbf{Z}_{mn}$ دارای mn عنصر است، یعنی به همان تعداد عناصر $\mathbf{Z}_m \times \mathbf{Z}_n$ که شامل تصویر θ است. بنابراین تصویر بایستی تمامی $\mathbf{Z}_m \times \mathbf{Z}_n$ باشد ، و برهان قضیه کامل است .

نتیجه. اگر $(m , n) = ۱$ آنگاه $U_m \times U_n \cong U_{mn}$ که ، یکریختی گروههاست.

برهان. قضیهٔ ۸ ت را به‌کار گیرید تا به‌دست آورید

$$U_{mn} = U(\mathbf{Z}_{mn}) \cong U(\mathbf{Z}_m \times \mathbf{Z}_n) \cong U(\mathbf{Z}_m) \times U(\mathbf{Z}_n) = U_m \times U_n \ .$$

مثال ۶.۹. از این نتیجه مستقیماً می‌توانیم استنتاج کنیم که اگر n دارای تجزیهٔ به عوامل اول $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ باشد ، آنگاه $U_n \cong U_{q_1} \times U_{q_2} \times \dots \times U_{q_r}$ ، که q_i همان $p_i^{a_i}$ است. برای اینکه این گروه ، دوری باشد لازم وکافی است که هریك از عوامل دوری بوده ومرتبه‌هایشان دوبه‌دو متباین باشند. (تمرینهای ۱ و ۲ از فصل ۶ را ببینید.) پس، به عنوان مثال ، $U_{۷۲} \cong U_۹ \times U_۸$ دوری نیست زیرا $U_۸$ ، همان‌طور که درمثال ۴.۹ نشان دادیم ، دوری نمی‌باشد. همچنین $U_{۳۶} \cong U_۹ \times U_۴$ دوری نیست زیرا مرتبه‌های دو عامل عبارت‌اند از: $\varphi(۹) = ۶$ و $\varphi(۴) = ۲$ که متباین نیستند.

دراینجا مشاهده می‌کنیم که قضیهٔ ۹ پ وبرهانش به‌طور نزدیك باقضیهٔ باقیماندهٔ چینی (قضیهٔ ۷ پ) مربوط است . در هردو حالت برهان یکی است و نشان می‌دهد که وقتی $(m , n) = ۱$ همریختی طبیعی $\mathbf{Z} \longrightarrow \mathbf{Z}_m \times \mathbf{Z}_n$ بروی است ، یعنی به ازاء اعداد صحیح دلخواه a ، b عددی‌مانند r وجوددارد که درشرایط $r \equiv a (m$ به پیمانهٔ $)$ و $r \equiv b (n$ به پیمانهٔ $)$ صدق می‌کند.

اکنون نظر خود را به‌ساختمان میدانهای کسرها معطوف می‌کنیم . نمی‌توانیم آن را به‌طور ثمربخشی برای حلقه‌های متناهی $\mathbf{Z}_n$ به‌کار بریم زیرا آنهایی که حوزهٔ صحیح‌اند مسلماً میدان نیزهستند. لیکن ، چون $\mathbf{Z}$ حوزهٔ صحیح است ساختمان مذکور می‌تواند برای آن به‌کار رود ومیدان کسرهای حاصل میدان اعداد گویا ، $\mathbf{Q}$ ، است. بدفعات این میدان قبلا در مثالهای ما ظاهرشده است، ولی این اولین باری است که به‌صورت منطقی ظاهرمی‌شود. براستی توجیه به‌کارگیری اعداد گویا محتوای قضیهٔ ۸ د است ، که وجود میدانی را که اعضایش کسرهای m/n هستند، با $m , n \in \mathbf{Z}$ ، $n \neq ۰$ ، نشان می‌دهد .(استفاده ازمیدانهای $\mathbf{R}$ و $\mathbf{C}$ باید به‌همین ترتیب توجیه گردد ، ولی بهتر است ساختمانشان دریك درس آنالیز مطالعه شود.)

هرعدد گویای x را می‌توان به‌صورت

$$x=\frac{a}{b}$$

نوشت، با $b>0$ (زیرا $\frac{a}{b}=\frac{-a}{-b}$).

به موجب خاصیت اقلیدسی $\mathbf{Z}$، به‌طور یکتا داریم $a=bq+r$، که در آن $0\leqslant r<b$. بنابراین به‌طور یکتا

$$x=q+\frac{r}{b},$$

که در آن $q\in\mathbf{Z}$، $0\leqslant r<b$. q و r/b را به ترتیب قسمتهای صحیح و کسری x می‌نامیم. اکنون به شرح و بسط نظریهٔ کسرهای جزئی می‌پردازیم که هدف از آن بیان x به صورت مجموع کسرهایی از نوع بویژه ساده است، یعنی کسرهایی با مخرجهایی از توانهای اول.

لم. اگر $b=b_1b_2$، که در آن b_1، b_2 اعداد صحیح متباین‌اند، آنگاه به ازاء اعداد صحیح مناسب r_1 و r_2 رابطهٔ

$$\frac{1}{b}=\frac{r_1}{b_1}+\frac{r_2}{b_2}.$$

در $\mathbf{Q}$ برقرار است.

برهان. رابطهٔ مفروض در $\mathbf{Q}$ با رابطهٔ $r_1b_2+r_2b_1=1$ در $\mathbf{Z}$ معادل‌است (دو طرف رابطه را در b ضرب کنید). این رابطه به ازاء اعداد مناسب r_1 و r_2 برقرار است زیرا b_1 و b_2 متباین‌اند (قضیهٔ ۵ب (پ)).

قضیهٔ ۹ ت. هر عدد گویای

$$x=\frac{a}{b}$$

می‌تواند به‌طوریکتایی به‌صورت

$$x=x_0+\frac{a_1}{b_1}+\frac{a_2}{b_2}+\cdots+\frac{a_s}{b_s} \qquad (1)$$

بیان شود، که در آن a_i، $b_i\in\mathbf{Z}$، x_0، b_1، b_2، ...، b_s توانهایی از اعداد اول متمایزند، و به ازاء هر i، $0<a_i<b_i$ و $b_i|b$.

برهان. اثبات وجود، نتیجهٔ ساده‌ای از لم فوق است. می‌نویسیم

$$x=\frac{a}{b}$$

با $b>0$. اگر $b=1$ آنگاه x عددی‌است‌صحیح و x_0 را برابر x اتخاذ می‌کنیم. چنانچه $b>1$ آنگاه $b=b_1b_2\dots b_s$، که در آن b_1، b_2، ...، b_s توانهایی از اعداد اول متمایزند. چون b_1، b_2، ...، b_s دوبه‌دو متباین‌اند، استقراء ساده‌ای با استفاده از لم فوق، به ازاء اعداد صحیح مناسب r_1، r_2، ...، r_s، به‌دست می‌دهد:

$$\frac{1}{b}=\frac{r_1}{b_1}+\frac{r_2}{b_2}+\dots+\frac{r_s}{b_s}.$$

بنابراین

$$\frac{a}{b}=\frac{ar_1}{b_1}+\frac{ar_2}{b_2}+\dots+\frac{ar_s}{b_s},$$

و چنانچه حالا تمام قسمتهای صحیح جمله‌های

$$\frac{ar_i}{b_i}$$

را با هم دسته‌بندی‌کنیم عبارتی به صورت مطلوب، با $0\leqslant a_i<b_i$، به دست می‌آوریم. اگر هریك از این a_i ها صفر باشد، بسادگی آن را حذف می‌کنیم تا جمله‌های ما درشرط $0<a_i<b_i$ صدق کند.

اثبات یکتایی کمی‌دشوارتراست. فرض کنید x دارای عبارت‌دیگری به‌صورت‌زیر باشد

$$x=y_0+\frac{c_1}{d_1}+\dots+\frac{c_t}{d_t}.$$

دراین صورت

$$\frac{a_1}{b_1}+\frac{a_2}{b_2}+\dots+\frac{a_s}{b_s}-\frac{c_1}{d_1}-\dots-\frac{c_t}{d_t}\in\mathbf{Z},$$

و چنانچه هرجفت از جملاتی‌راکه مخرجشان توانی از یك عدد اول یکسان‌اند باهم جمع کنیم دستوری به‌صورت

$$\frac{u_1}{v_1}+\frac{u_2}{v_2}+\dots+\frac{u_r}{v_r}\in\mathbf{Z} \qquad (2)$$

به‌دست می‌آوریم، که درآن v_1، v_2، ...، v_r توانهایی از اعداد اول متمایزند، وبسادگی دیده می‌شود که به ازاء هر i، $|u_i|<v_i$. (این مطلب اخیردرصورتی که

$$\frac{u_i}{v_i}$$

یکی از جمله‌های

$$\frac{a_j}{b_j} \quad \text{یا} \quad -\frac{c_j}{d_j}$$

باشد واضح است و در غیر این صورت u_i/v_i به صورت

$$\frac{g}{p^m} - \frac{h}{p^n}$$

است، که در آن $0 < g < p^m$ و $0 < h < p^n$. با فرض ، مثلا ، $m \leqslant n$ ، داریم

$$\frac{u_i}{v_i} = \frac{gp^{n-m} - h}{p^n}$$

و به‌وضوح $|gp^{n-m} - h| < p^n$ ($gp^{n-m} - h \neq 0$) حال (۲) را در $v_2 \cdots v_r$ ضـــرب می کنیم. آنگاه همهٔ کسرها بجز اولی به‌اعداد صحیح تبدیل می‌شوند، ازاینرو داریم

$$\frac{u_1 v_2 v_3 \cdots v_r}{v_1} \in \mathbf{Z} \text{ ، یعنی } v_1 | u_1 v_2 v_3 \cdots v_r .$$

اما v_1 با $v_2 v_3 \cdots v_r$ متباین است ، پس نتیجه می‌شود کـه $v_1 | u_1$. چون $|u_1| < v_1$ ، این نتیجه می‌دهد $u_1 = 0$. به همین نحو ، می‌توانیم ثابت کنیم کـه به ازاء هر i ، $u_i = 0$. بنابراین جمله‌های کسری دو عبارت x بایستی دقیقاً برابر باشند ولذا جمله‌هـای صحیح نیز باهم برابرند.

فرایند کسرهای جزئی را می‌توانیم با تفکیك جملاتی از نوع q/p^m ، که در آن p اول است، کمی بیشتر بررسی کنیم.

قضیهٔ ۹ث. فرض کنید p عدد اول ثابتی باشد. دراین‌صورت هرعدد صحیح مثبت q می‌تواند به‌طور یکتایی به‌صورت $q_0 + q_1 p + q_2 p^2 + \cdots + q_n p^n$ نوشته شود، که‌درآن $0 \leqslant q_i < p$ و $q_n \neq 0$.

برهان . اگـر $q < p$ آنگاه $n = 0$ و $q = q_0$ اختیار می کنیم . چنانچه $q \geqslant p$ داریـم $q = q'p + q_0$ ، که درآن $0 \leqslant q_0 < p$ ، $q' > 0$. با استفاده از استقراء روی q می بینیم که q' ، که از q کوچکتر است ، می‌تواند به صورت $q' = q_1 + q_2 p + \cdots + q_n p^{n-1}$ نوشته شود و لذا $q = q_0 + q_1 p + \cdots + q_n p^n$. یکتایی این عبارت به طریق‌زیر ثابت می‌شود. فرض کنید که

$$q_0+q_1p+q_2p^2+\cdots+q_np^n=r_0+r_1p+r_2p^2+\cdots+r_mp^m,$$

با $0\leqslant q_i<p$ و $0\leqslant r_i<p$. با تحویل به پیمانهٔ p درمی‌یابیم (به پیمانهٔ p) $q_0\equiv r_0$، که از آنجا، به‌موجب مجموعهٔ مقادیر تحدید شدهٔ آنها، $q_0=r_0$. باتفریق $q_0=r_0$ وحذف p به دست می‌آوریم

$$q_1+q_2p+\cdots+q_np^{n-1}=r_1+r_2p+\cdots+r_np^{n-1},$$

و استقراء ساده‌ای برهان را کامل می‌کند.

قضیهٔ ۹ ج. هرعدد گویای

$$x=\frac{a}{b}$$

می‌تواند به طور یکتا به‌صورت

$$x=x_0+\frac{r_1}{p_1^{\alpha_1}}+\frac{r_2}{p_2^{\alpha_2}}+\cdots+\frac{r_k}{p_k^{\alpha_k}} \qquad (۳)$$

بیان‌شود، که درآن x_0 ، r_i ، p_i و α_i اعداد صحیح و p_1 ، p_2 ، ... ، p_k اعداد اول‌هستند (الزاماً متمایز نیستند) ، به ازاء هر i ، $0<r_i<p_i$ و $0<\alpha_i$ ، و همهٔ توانهای اول $p_1^{\alpha_1}$ ، $p_2^{\alpha_2}$ ، ... ، $p_k^{\alpha_k}$ متمایزند و b، مخرج‌کسر x، را عاد می‌کنند.

برهان. در تجزیهٔ x به‌کسرهای جزئی که در قضیهٔ ۹ت آمده است، هرجمله بغیر از x_0 ، به ازاء عدداولی چون p به صورت a/p^n است، که درآن $0<a<p^n$ و $p^n|b$. بنابه‌قضیهٔ ۹ ث ، a می‌تواند به صورت $a=q_0+q_1p+\cdots+q_rp^r$ نوشته شود، که در آن $0\leqslant q_i<p$ و $q_r\neq 0$. واضح است که $r<n$ ، از اینرو از تقسیم طرفین بر p^n به دست می‌آوریم

$$\frac{a}{p^n}=\frac{q_0}{p^n}+\frac{q_1}{p^{n-1}}+\cdots+\frac{q_r}{p^{n-r}}, \qquad (۴)$$

که به صورت مطلوب است. چنانچه این را برای هرجمله انجام دهیم ونتایج حاصل را با هم جمع کنیم، می‌توانیم x را به صورت مطلوب (۳) بیان کنیم. این بیان یکتاست، زیرا اگر تمام جملاتی که مخرجشان توان یك عدد اول یکسان‌اند دسته‌بندی و با هم جمع کنیم، تجزیه‌ای به‌صورت

$$x=x_0+\frac{a_1}{b_1}+\cdots+\frac{a_s}{b_s}$$

به‌دست می‌آوریم که از نوع ارائه شده در قضیهٔ ۹ ث است. این تجزیه یکتاست، از اینرو

a_i/b_i ها به‌طور یکتا معین می‌شوند. اما هریك ازاینها دارای تجزیهٔ یکتایی به‌صورت (۴) می‌باشد ، لذا جمله‌های (۳) به‌طور یکتا معین‌می‌شوند.

مثال ۷.۹. عدد گویای

$$\frac{۱۴}{۱۳۵}=\frac{۱۴}{۳^{۳}\times ۵}$$

بنا به قضیهٔ ۹ ج ، می‌تواند به‌صورت

$$a+\frac{b}{۵}+\frac{c}{۳}+\frac{d}{۳^{۲}}+\frac{e}{۳^{۳}}$$

نوشته شود، که در آن a ، b ، c ، d و e اعداد صحیح‌اند و $۰\leqslant b<۵$ ، $۰\leqslant c<۳$ ، $۰\leqslant d<۳$ و $۰\leqslant e<۳$. برای یافتن صورتها طرفین‌را در ۵×۳^{۳} ضرب کرده به‌دست می‌آوریم $۱۴=۳^{۳}\times ۵a+۳^{۳}b+۳^{۲}\times ۵c+۳\times ۵d+۵e$. این رابطه به پیمانهٔ ۵ به‌دست می‌دهد (به‌پیمانهٔ ۵) $۲۷b\equiv ۱۴$ ، یعنی (به پیمانهٔ ۵) $۲b\equiv ۴$ ، که ازآنجا $b=۲$ (زیرا $۰\leqslant b<۵$) . باجایگزین‌کردن این مقدار به‌دست‌می‌آوریم

$$-۴۰=۳^{۳}\times ۵a+۳^{۲}\times ۵c+۳\times ۵d+۵e$$

که‌ازآنجا $۲۷a+۹c+۳d+e=-۸$ ، که c ، d و e درمجموعهٔ‌مقادیر $\{۰،۱،۲\}$ هستند. این به‌پیمانهٔ ۳ به‌دست‌می‌دهد $e\equiv -۸\equiv ۱$ ، ازاینرو $e=۱$. بنابراین $۹a+۳c+d=-۳$ ، که به‌دست می‌دهد $d=۰$. با ادامهٔ این‌طریق به‌دست می‌آوریم $c=۲$ و $a=-۱$ و از اینرو می‌توان نتیجه گرفت که

$$\frac{۱۴}{۱۳۵}=-۱+\frac{۲}{۵}+\frac{۲}{۳}+\frac{۱}{۲۷}\cdot \qquad (۵)$$

به‌منطق این ادعا توجه‌کنید: به موجب قضیهٔ فوق می‌دانیم که تجزیه‌ای به صورت مطلوب وجود دارد؛ بافرض اینکه ۱۴/۱۳۵ به‌صورت مزبوربیان شود، ثابت‌کرده‌ایم که تنهامقادیر ممکن صورتها آنهایی هستندکه به‌دست آورده‌ایم ؛ بنابراین (۵) درست است. تنها دلیل برای تحقیق درستی نتیجه آن است که مطمئن شویم هیچ خطای محاسباتی در عملیات رخ نداده است. لیکن ، آزمودن و به‌کاربردن همان استدلال برای تجزیهٔ یك عدد به صورتی که در واقع امکان‌پذیر نیست اشتباه متداولی است. مثلا ، اگر کسی قضایا را درست درنیابد ، ممکن است تصورکندکه ، چون ۷/۴۵ دارای قسمت صحیح ۰ است، می‌تواند به‌صورت

$$\frac{۷}{۴۵}=\frac{a}{۳}+\frac{b}{۹}+\frac{c}{۵}$$

نوشته شود با $۰\leqslant a<۳$ ، $۰\leqslant b<۳$ ، $۰\leqslant c<۵$. چنانچه این را فرض‌کنیم وطرفین را در ۴۵ ضرب‌کنیم ، به‌دست می‌آوریم $۱۵a+۵b+۹c=۷$ که به پیمانهٔ ۳ به‌دست

می‌دهد (به پیمانهٔ ۳) $5b \equiv 7$ وازآن نتیجه می‌شود $b = 2$ و $15a + 9c = -3$. این به پیمانهٔ ۵ بـه دست می‌دهد (به پیمانهٔ ۵) $9c \equiv -3$ ، و به پیمانـهٔ ۹ بـه دست می‌دهد (به پیمانهٔ ۹) $15a \equiv -3$. اینها نتیجه می‌دهند $c = 3$ و $a = 1$. بنابراین ممکن است استنتاج کرد که

$$\frac{7}{45} = \frac{1}{3} + \frac{2}{9} + \frac{3}{5}$$

که نادرست است. نکته دراینجاست که ۷/۴۵ نمی‌تواند به‌صورت مورد نظر نوشته شود، از اینرو هر اطلاعی که بتوان درمورد a ، b و c استنتاج کرد فاقد ارزش است.

تمرینها

۱. ثابت کنید که گروه یکه‌های $\mathbf{Z}_n$ به‌ازاء $n = 2, 3, 4, 5, 6, 7$ ، دوری است . نشان دهید که به‌ازاء $n = 15$ ، دوری نیست.

۲. مولدی برای گروه ضربی میدان $\mathbf{Z}_{23}$ پیدا کنید.

۳. کوچکترین عدد صحیح مثبت n را به‌قسمی پیدا کنید که (به پیمانهٔ ۷۷) $27^n \equiv 1$.

۴. ثابت کنید که به ازاء هر $n \in \mathbf{Z}$ ، (به‌پیمانهٔ ۲۵) $n^{21} \equiv n^5$.

۵. ثابت کنید که به‌ازاء هر $n \in \mathbf{Z}$ ، (به‌پیمانهٔ ۱۰۰۱) $n^{61} \equiv n$.

۶. ثابت کنید که به ازاء هر $n \in \mathbf{Z}$ ، (به‌پیمانهٔ ۲۵۲) $n^8 \equiv n^2$.

۷. ثابت کنید که به‌ازاء همهٔ اعدادصحیح فرد، (به‌پیمانهٔ ۸۱۶۰) $n^{17} \equiv n$ ، این‌همنهشتی به ازاء کدام یك از اعداد صحیح زوج n درست است؟ بزرگترین عددصحیح Nرا به‌قسمی پیدا کنید که ، به‌ازاء هر $n \in \mathbf{Z}$ ، (به‌پیمانهٔ N) $n^{17} \equiv n$.

۸. نشان دهید که اعداد ۲ ، ۴ ، ۶ و ۸ تحت عمل ضرب به پیمانهٔ ۱۰ تشکیل یك گروه می‌دهند. عنصرهمانی آن چیست؟ آیا یك گروه دوری است؟

۹. فرض کنید p یك عدد اول فرد باشد و فرض کنید کـه (به پیمانهٔ p) $a^p + b^p \equiv 0$. نتیجه بگیرید که (به پیمانهٔ p^2) $a^p + b^p \equiv 0$.

۱۰. $\frac{۳۷۹}{۱۲۰۰}$ را به‌صورت‌مجموع کسرهایی که مخرج آنها توان‌یك‌عدد اول است‌بیان کنید.

۱۱. تجزیهٔ‌کامل $\frac{۲۹}{۱۸۰}$ را به‌کسرهای جزئی ، همانند قضیهٔ ۹ ج ، پیدا کنید.

۱۲. فرض کنید R حلقه‌ای جابجایی باشد و $x \in R$. ثابت کنید کـه x عنصر یکه‌ای از R

است اگروفقط اگرایده‌آل اصلی xR که به‌وسیلهٔ x تولیدمی‌شود تمامی R باشد.

۱۳. ثابت کنید که هرایده‌آل $\mathbf{Z}_n$ یك ایده‌آل اصلی به‌صورت $d\mathbf{Z}_n$ است، که درآن $d|n$. نشان دهید حلقهٔ خارج قسمت مربوطه، با $\mathbf{Z}_d$ یکریخت است.

۱۴. ثابت کنید که اگر R زیرحلقه‌ای از $\mathbf{Q}$ باشدآنگاه میدان کسرهای R با $\mathbf{Q}$ یکریخت است. (راهنمایی: خاصیت‌جامع میدان کسرهاواین‌حقیقت راکه $R \supset \mathbf{Z}$ به‌کاربرید.)

۱۵. فرض کنید p عدد اول ثابتی باشد و L_p زیرمجموعهٔ $\mathbf{Q}$ شامل همهٔ کسرهای a/p^r، به ازاء $a, r \in \mathbf{Z}$، $r \geqslant 0$. ثابت کنید که L_p زیرحلقه‌ای از $\mathbf{Q}$ است و هرایده‌آل غیرصفر از L_p به‌صورت dL_p می‌باشد، که درآن d عدد صحیح مثبتی است که بر p قابل‌قسمت نیست.

۱۶. فرض کنید P مجموعه‌ای از اعداد اول باشد، و همچنین L_p مجموعهٔ تمام اعداد گویایی رانشان‌دهد که مخرجهایشان حاصلضربی از توانهای اعداد اول در Pباشند. نشان دهیدکه L_p زیرحلقه‌ای از $\mathbf{Q}$ است. بعکس، نشان دهیدکه هر زیرحلقهٔ $\mathbf{Q}$، به ازاء مجموعه‌ای‌ازاعداد اولP، برابر است با L_p. (راهنمایی: برای‌اثبات‌عکس‌مطلب، نشان دهیدکه اگرزیرحلقهٔ R از $\mathbf{Q}$ شامل عددگویایی باشدکه مخرجش برعدد اول مفروضی مانند p قابل قسمت باشد ولی صورت‌آن بر p قابل قسمت نباشد، آنگاه $\frac{1}{p} \in R$ وبنابراین $R \supset L_p$.)

۱۷. ثابت کنیدکه هرعددگویای r، با خاصیت $0 < r < 1$، می‌تواند به‌صورت

$$r = \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}$$

نوشته شود، که درآن n_1، n_2، ...، n_kاعدادصحیح‌اند و $n_1 < n_2 < \cdots < n_k$. آیا این‌کاربرای هرعدد مثبت‌گویایی می‌تواند انجام شود؟ (اشتباه نکنید! این هیچ ارتباطی با کسرهای‌جزئی‌ندارد وصرفاً برای‌ازدیاد اطلاعات‌شما آمده است.)

فصل ۱۰

حلقهٔ چندجمله‌ایها

اساساً یك چندجمله‌ای عبارتی به‌صورت

$$a_0+a_1X+a_2X^2+\cdots+a_nX^n \qquad (1)$$

است، ولی تعریف‌دقیق مستلزم کمی دقت‌است. بایستی روشن کنیم کـه ضرایب a_i چه‌هستند (مثلا ، آیا می‌توانیم X را بـه‌عنوان ضرایب به‌کار ببریم ؟) همچنین بـا استفاده از تعریف باید قادر باشیم که تعیین کنیم آیا $0X^2$ همان چندجمله‌ای $0X^4$ است ویا $2X+X^2$ همان چندجمله‌ای $2X+X^2$ است؟

با تعیین یك حلقهٔ جابجایی R که ضرایب از آن اختیار می‌شوند و علامت X ، که عضوی از R نیست، آغازمی‌کنیم. یك چندجمله‌ای از X باضرایب در R را عبارتی‌صوری مانند زیرتعریف می‌کنیم.

$$\sum_{i=0}^{\infty} a_iX^i \quad (\text{یا برای اختصار} \ , \ \sum a_iX^i) \ ,$$

که ضرایب a_0 ، a_1 ، a_2 ، ... اعضای R هستند وهمه بجز تعداد متناهی ازآنها صفرنـد. دراین‌تعریف (هنوز) $\sum$ جمع را اعلام نمی‌کند. X هم به‌جای عنصر متغیری ازRمحسوب نمی‌شود؛ به‌طور ساده منظور ازآن نشان‌کردن جمله‌های گوناگون به‌طریقی مناسب بـرای محاسبات آینده است. دو چندجمله‌ای $\sum a_iX^i$ و $\sum b_iX^i$ باهم مساوی‌اند اگر وفقط اگر به‌ازاء هر $i\in\mathbf{N}$ ، $a_i=b_i$. مجموعهٔ همهٔ چندجمله‌ایها ازایـن نـوع به‌وسیلهٔ $R[X]$ نشان داده می‌شود، وکار بعدی ما آن است که این مجموعه را به‌یك ساخت حلقه‌ای مجهز کنیم.

مجموع دوچندجمله‌ای $\sum a_iX^i$ و $\sum b_iX^i$ برابر $\sum c_iX^i$ تعریف‌می‌شود، که درآن به‌ازاء هر $i\in N$ ، $c_i=a_i+b_i\in R$ ؛ این مجموع نیز یك چندجمله‌ای است زیـرا به‌ازاء هر i ، $c_i=a_i+b_i\in R$ وفقط تعداد متناهی از c_i ها مخالف صفرند. بنابرایـن یك عمل دوتایی $+$ داریم که روی $R[X]$ تعریف‌شده است و به‌وضوح $R[X]$ را به‌یك گروه‌آبلی

تبدیل می‌کند. عنصر صفر آن چندجمله‌ای است که همهٔ ضرایبش صفرند (این چندجمله‌ای را نیز به‌وسیلهٔ ۰ نشان می‌دهیم). قرینهٔ چندجمله‌ای $\sum a_iX^i$ چندجمله‌ای $\sum(-a_i)X^i$ است، که آن‌را به‌صورت $-\sum a_iX^i$ نیز می‌نویسیم. قوانین شرکت‌پذیری وجابجایی برای جمع چند جمله‌ایها مستقیماً ازهمان قوانین در R به‌دست می‌آیند.

حاصلضرب دوچندجمله‌ای $\sum a_iX^i$ و $\sum b_iX^i$ چندجمله‌ای $\sum d_iX^i$ تعریف می‌شود، که در آن

$$d_n=a_0b_n+a_1b_{n-1}+\cdots+a_ib_{n-i}+\cdots+a_nb_0.$$

نخست مشاهده می‌کنیم که به‌ازاء هر n، $d_n\in R$، و همچنین همه بجز تعداد متناهی از d_n ها صفرند (زیرا Nای وجود دارد به‌قسمی که به‌ازاء $i>N$، $a_i=b_i=0$، و واضح است که به‌ازاء $n>2N$، $d_n=0$). بنابراین یك عمل دوتایی خوش تعریف ضرب‌روی $R[X]$ داریم وحال ادعا می‌کنیم که $R[X]$، همراه باعمل‌جمعی که قبلا تعریف کردیم، یك حلقهٔ جابجایی‌است.هنوز تعدادی قوانین هست که باید تحقیق شوند، وآنهایی که واضح‌اند عبارت‌اند از (الف) قانون‌جابجایی ضرب، که از رابطهٔ

$$d_n=a_0b_n+a_1b_{n-1}+\cdots+a_nb_0=b_0a_n+b_1a_{n-1}+\cdots+b_na_0$$

نتیجه‌می‌شود و(ب) $R[X]$ دارای عنصر همانی ۱ است که برابر چندجمله‌ای $\sum a_iX^i$ می‌باشد، که در آن $a_0=1$ وتمامی a_iهای دیگرصفرند. قانون‌شرکت‌پذیری ضرب وقانون توزیعی باقی می‌مانند، که هیچکدام بلافاصله واضح نیستند. برای قانون شرکت‌پذیری، می‌نویسیم $a(X)=\sum a_iX^i$، $b(X)=\sum b_iX^i$ و $c(X)=\sum c_iX^i$، وقرارمی‌دهیم: $d(X)=a(X)b(X)$، $e(X)=b(X)c(X)$ باید نشان دهیم که

$$d(X)c(X)=a(X)e(X).$$

حال $d(X)=\sum d_iX^i$، که‌در آن

$$d_n=a_0b_n+a_1b_{n-1}+\cdots+a_nb_0=\sum_{i+j=n}a_ib_j.$$

بنابراین، بنابه‌تعریف، $d(X)c(X)=\sum g_iX^i$، که در آن

$$\begin{aligned}g_m&=d_0c_m+d_1c_{m-1}+\cdots+d_mc_0\\&=\sum_{n+k=m}d_nc_k\\&=\sum_{n+k=m}\Big(\sum_{i+j=n}a_ib_j\Big)c_k\\&=\sum_{i+j+k=m}a_ib_jc_k.\end{aligned}$$

تقارن این دستور نتیجه می‌دهدکه اگرضرایب $a(X)e(X)$ را محاسبه‌کنیم همان نتیجه را به‌دست خواهیم‌آورد و ازاینرو قانون شرکت‌پذیری در $R[X]$ درست است. درستی آن

عمدتاً مبتنی است برقوانین شرکت‌پذیری و توزیعی در R . قانون توزیعی به‌وسیلهٔ محاسبهٔ مشابهی از ضرایب $a(X)b(X)+a(X)c(X)$ و $a(X)\{b(X)+c(X)\}$ با به‌کار بردن تعاریف جمع و ضرب در $R[X]$ اثبات می‌شود: این‌را به‌عنوان تمرین می‌گذاریم واصرار داریم که خواننده آن‌را به‌طورکامل بنویسد، زیرا قوانین‌حلقه برای چندجمله‌ایها بدون‌سؤال بیشتری به‌کار برده می‌شود واو باید درمورد درستی همهٔ‌آنها متقاعد شده‌باشد.

خاصیتهای حلقهٔ‌جابجایی $R[X]$ به‌طور اصولی بررسی خواهد شد، ولی ابتدابرخی از نمادهای مختصرکننده را معرفی می‌کنیم. چندجمله‌ای $\sum a_iX^i$ که درآن به‌ازاء هر $i\geqslant 1$ ، $a_i=0$ ، به‌طور ساده به‌وسیلهٔ a_0 نشان داده می‌شود. این ممکن است نسنجیده به‌نظرآید زیرا a_0 عنصری از R را نیز نشان می‌دهد. لیکن، مجموع و حاصلضرب a_0 و b_0 به‌عنوان چندجمله‌ایها، همان مجموع و حاصلضربشان در R است (این‌را به‌کمك تعاریف تحقیق کنید!). بنابراین‌می‌توان R را بامجموعهٔ تمام‌چندجمله‌ایها ازاین‌نوع ساده همانندکرد وازاینرو با R به‌عنوان زیرحلقه‌ای از $R[X]$ رفتارکرد.

هرچندجمله‌ای غیرصفر $\sum a_iX^i$ دارای حداقل یك‌ضریب غیرصفرمی‌باشد وبنابراین دارای‌آخرین ضریب غیر صفر است، یعنی ضریب $a_n\neq 0$ به‌قسمی که به‌ازاء هر $i>n$ ، $a_i=0$. این‌ضریب، ضریب پیشرو نامیده می‌شود (اگرچه درنمادگذاری ما ضریب دنباله‌روست) ، جملهٔ a_nX^n جملهٔ پیشرو وعدد صحیح n درجهٔ چندجمله‌ای نامیده می‌شود. چندجمله‌ای ۰ دارای درجه‌ای به‌این مفهوم نیست وبایستی درمقابل کسی که فرض کند درجه‌اش صفر است جبهه‌گرفت. چندجمله‌ایهای درجهٔ صفر چندجمله‌ایهایی هستند بااین خاصیت که $a_0\neq 0$ وبه‌ازاء $i>0$ ، $a_i=0$. بنابراین زیرحلقهٔ R از $R[X]$ متشکل‌است از چندجمله‌ایهای درجهٔ صفر همراه باچندجمله‌ای صفر . $\deg(a(X))$ را برای نمایش درجهٔ چندجمله‌ای $a(X)$ می‌نویسیم و ، به دلایلی که بعداً آشکار می‌شوند، به‌طور قراردادی‌درجهٔ $-\infty$ را به‌چندجمله‌ای صفرنسبت می‌دهیم.

چندجمله‌ای‌درجهٔ‌یکی که‌ضرایبش عبارت‌اند از: $a_0=0$ ، $a_1=1$ وبه‌ازاء $i>1$ ، $a_i=0$ ، به‌طور ساده به‌وسیلهٔ X نشان داده خواهد شد. با به‌کار بردن تعریف ضرب برای این‌چندجمله‌ای درمی‌یابیم که $X^m=XX\dots X$ (عامل m) چندجمله‌ای باضرایب $a_m=1$ ، $a_i=0$ به‌ازاء $i\neq m$ ، می‌باشد. به‌همین‌نحو به‌ازاء $a\neq 0$ در R چندجمله‌ای aX^m دارای ضرایب $a_m=a$ و $a_i=0$ به‌ازاء $i\neq m$، است. بنابراین، اگرچندجمله‌ای $\sum a_iX^i$ دارای درجهٔ n باشد درواقع مجموع چندجمله‌ایهای a_0 ، a_1X ، a_2X^2 ، ... ، a_nX^n در $R[X]$ است و از اینرو می‌توانند به‌صورت(۱) نوشته شود. اکنون علامت جمع درتعریف چندجمله‌ایها وهمچنین نماد a_iX^i برای جمعوندهایش درجنبهٔ درست خود ظاهر می‌شوند. البته، چون‌جمع در $R[X]$ جابجایی است چندجمله‌ای $\sum a_iX^i$ از درجهٔ n می‌تواندبه‌صورت $a_nX^n+a_{n-1}X^{n-1}+\dots+a_1X+a_0$ یا به روشهای دیگرنیز نوشته شود.

قضیهٔ ۱۰ آ. فرض‌کنید $a(X)$ ، $b(X)$ چندجمله‌ایهای غیرصفر در $R[X]$ باشند. دراین صورت

(الف) $\deg(a(X)+b(X)) \leqslant \max\{\deg(a(X)), \deg(b(X))\}$ ؛

(ب) $\deg(a(X)b(X)) \leqslant \deg(a(X))+\deg(b(X))$.

اگر R حوزهٔ صحیح باشد آنگاه

$$\deg(a(X)b(X))=\deg(a(X))+\deg(b(X))$$

وبنابراین $R[X]$ نیز یك حوزهٔ صحیح است.

برهان . فرض کنید $m=\deg(a(X))$ ، $n=\deg(b(X))$ که ، طبق معمول ، $a(X)=\sum a_iX^i$ و $b(X)=\sum b_iX^i$. دراین‌صورت به‌ازاء $i>m$ ، $a_i=0$ ، وبه‌ازاء $i>n$ ، $b_i=0$. بنابراین به‌ازاء $i>\max\{m, n\}$ ، $a_i+b_i=0$ ، ولذا (الف) نتیجه می‌شود. به‌همین ترتیب اگر $a(X)b(X)=\sum d_iX^i$ آنگاه درصورتی که $r>m+n$ داریم:

$$d_r=\sum_{i+j=r} a_ib_j=0 .$$

ولذا (ب) نتیجه می‌گردد . لیکن، اگر R حوزهٔ صحیحی باشد، آنگاه ضریب پیشروی حاصلضرب برابر است با

$$d_{m+n}=a_0b_{m+n}+\cdots+a_mb_n+\cdots+a_{m+n}b_0=a_mb_n$$

واین صفر نیست زیرا $a_m\neq 0$ ، $b_n\neq 0$. بنابراین $a(X)b(X)$ چندجمله‌ای صفر نیست و $R[X]$ یك‌حوزه‌صحیح‌است. (دستورفوق‌وقتی‌که $a(X)$ یا $b(X)$ برابرصفرباشد نیزصادق است، هرگاه، عباراتی مانند $n+(-\infty)$ به‌طریق واضحی تعبیر گردند.)

به‌دلیل این قضیه، ازاین به‌بعد، توجه خودرا تقریباً به‌تمامه منحصر به‌چندجمله‌ایهایی می‌کنیم که ضرایبشان دریك حوزهٔ صحیح قرار دارند. برای برخی‌از نتایج حتی خواهان این فرضیم که حوزهٔ ضرایب یك میدان باشد ودراین‌صورت آن‌را به‌وسیلهٔ F نشان‌می‌دهیم. لیکن توجه کنید که اگر F یك میدان‌باشد نمی‌توانیم نتیجه بگیریم که $F[X]$ یك میدان‌است. درواقع این‌مطلب به‌دلیل قضیهٔ زیرهرگز درست‌نیست.

قضیهٔ ۱۰ ب. اگر D حوزهٔ صحیح باشدآنگاه یکه‌های حلقهٔ چندجمله‌ای $D[X]$ همان یکه‌های D هستند. بالاخص، اگر F یك‌میدان باشد، یکه‌های $F[X]$ دقیقاً چندجمله‌ایهای درجهٔ صفرند.

برهان. واضح است که یکه‌های D هنگامی که به‌عنوان اعضای $D[X]$ درنظر گرفته شوند یکه باقی‌می‌مانند. بعکس، فرض کنید که $a(X)$ یکه‌ای از $D[X]$ باشد. دراین‌صورت به‌ازاء چندجمله‌ایی چون $b(X)\in D[X]$ ، داریم $a(X)b(X)=1$. بنابراین بنابه‌قضیهٔ ۱۰ آ ،

$\deg(a(X))+\deg(b(X))=0$ زیرا D حوزهٔ صحیح است . ایـن نتیجه می‌دهد که $a(X)$ و $b(X)$ هردو دارای درجهٔ صفرند و بنابراین عنصرهای زیرحلقهٔ D هستند. چـون حاصلضربشان برابراست با ۱ ، هردوی آنها یکه‌های D می‌باشند. هنگامی که $D=F$ یك میدان باشد، این یکه‌ها همهٔ عناصرغیرصفر F هستند، یعنی تمام چندجمله‌ایهای‌درجهٔ صفرند.

درمورد حلقه‌های‌چندجمله‌ای $F[X]$ روی میدان F شباهت‌زیادی با حلقهٔ $\mathbf{Z}$ مبتنی بر «خاصیت‌اقلیدسی» زیر وجود دارد، که بایستی باقضیهٔ ۳پ مقایسه شود.

قضیهٔ۱۰ پ. فرض کنید F یك میدان و $a(X)$ ، $b(X)$ چندجمله‌ایهایی در $F[X]$ باشند با $b(X)\neq 0$. دراین صورت‌چندجمله‌ایهای $q(X)$ ، $r(X)$ در $F[X]$ به‌قسمی‌وجود دارندکه $a(X)=b(X)q(X)+r(X)$ و $\deg(r(X))<\deg(b(X))$. بعلاوه ، $q(X)$ و $r(X)$ بااین خاصیت، یکتاهستند.

برهان. فرض کنید $r(X)$ درمیان همهٔ چندجمله‌ایهای به‌صورت $a(X)-b(X)q(X)$، به‌ازاء $q(X)$ دلخواه، دارای کوچکترین درجهٔ ممکن باشد. قراردادمان را یادآور می‌شویم کـه چندجمله‌ای صفر دارای درجه $-\infty$ است، کـه به‌عنوان کوچکترین عدد طبیعی تعبیر شده است ، $r(X)$ چندجمله‌ای صفر خواهد بود اگر 0 بین چندجمله‌ایهای بـا صورت مفروض باشد؛ درغیراین صورت مجموعهٔ تمام درجه‌های این چندجمله‌ایها مجموعـه‌ای غیرتهی از اعداد طبیعی است وازاینرو دارای کوچکترین عضواست، که‌وجود $r(X)$ را ضمانت‌می‌کند. حال نشان می‌دهیم که $\deg(r(X))<\deg(b(X))$. زیرا اگرچنین نباشد، فرض‌می‌کنیم جمله‌های پیشروی $r(X)$ و $b(X)$ به‌ترتیب r_nX^n و b_mX^m باشند، با $n\geqslant m$. چون $b_m\neq 0$ و F یـك میدان است ، چندجملـه‌ای $s(X)=b_m^{-1}r_nX^{n-m}$ در $F[X]$ قـرار دارد ، و $b(X)s(X)$ دارای‌جملهٔ پیشروی r_nX^n است که‌همان جملهٔ پیشروی $r(X)$ می‌باشد. بنابراین چندجمله‌ای $t(X)=r(X)-b(X)s(X)$ دارای درجهٔ کوچکتراز درجهٔ $r(X)$ است. اما به‌ازاء چندجمله‌ایی چون $q(X)$ ، $r(X)=a(X)-b(X)q(X)$ ، ازاینرو

$$t(X)=a(X)-b(X)\{q(X)+s(X)\}$$

نیز به‌همان صورت‌است ودارای درجهٔ کوچکتراز درجهٔ $r(X)$ است؛ که یك تناقض‌می‌باشد. این‌ثابت می‌کندکه $\deg(r(X))<\deg(b(X))$. اکنون‌یکتایی $q(X)$ و $r(X)$ بآسانی نتیجه‌می‌شود: اگر $a(X)=b(X)q_1(X)+r_1(X)$ با $\deg(r_1(X))<\deg(b(X))$، آنگاه

$$b(X)\{q(X)-q_1(X)\}=r_1(X)-r(X)\ .$$

بنابه‌قضیهٔ۱۰ آ ، طرف‌راست رابطهٔ‌فوق‌دارای درجهٔ‌کمتراز $\deg(b(X))$ است، درصورتی که طرف‌چپ حداقل‌دارای درجهٔ $\deg(b(X))$ است مگراینکه $q(X)-q_1(X)\}=0$. استنتاج می‌کنیم که $q(X)=q_1(X)$ وازآنجا $r(X)=r_1(X)$.

حال مشابه قضیهٔ ۴پ درمورد زیرگروههای $\mathbf{Z}$ را ثابت می‌کنیم، که مبنای نظریهٔ تجزیه در $\mathbf{Z}$ بود. یك چندجمله‌ای را تکین نامیم اگر ضریب پیشروی آن برابر ۱ باشد، و ملاحظه کنید که هرچندجمله‌ای غیرصفر روی یك میدان می‌تواند به‌وسیلهٔ ضرب دریك یکه، یعنی معکوس‌ضریب پیشرواش، تکین گردد.

قضیهٔ ۱۰ت. (قضیهٔ ایده‌آل اصلی.) فرض‌کنید F یك میدان باشد. دراین‌صورت هرایده‌آل $F[X]$ ایده‌آلی اصلی مانند $d(X)F[X]$ است، به‌ازاء یك $d(X)\in F[X]$. مولد $d(X)$ می‌تواند یا ۰ یاچندجمله‌ایی تکین انتخاب شود ودرآن‌صورت یکتاست.

برهان. فرض کنید I ایده‌آل دلخواهی از $F[X]$ باشد. اگر $I=\{0\}$ آنگاه می‌توان $d(X)=0$ برگزید واین به‌وضوح یکتاست. درغیراین‌صورت، I شامل چندجمله‌ایهایی غیر صفر است وازآن میان چندجمله‌ای باکوچکترین درجهٔ ممکن را انتخاب می‌کنیم. چنانچه این چندجمله‌ای را دریك یکه ضرب کنیم در I باقی می‌ماند و درجه‌اش تغییر نمی‌کند، ازاینرو می‌توان آن‌را به‌قسمی انتخاب کرد که‌تکین باشد. این‌چندجمله‌ای را $d(X)$ می‌نامیم. واضح است که $d(X)F[X]\subset I$ و باقی می‌ماند نشان دهیم که هر $a(X)\in I$، به‌ازاء چندجمله‌ایی چون $q(X)$، به‌صورت $a(X)=d(X)q(X)$ است. بنابه قضیهٔ ۱۰پ، می‌دانیم $a(X)=d(X)q(X)+r(X)$، که‌درآن $\deg r(X)<\deg(d(X))$. ولی $r(X)=a(X)-d(X)q(X)\in I$، ازاینرو به‌یك تناقض می‌رسیم مگراینکه $r(X)=0$. (یادآورمی‌شویم که $d(X)$ عنصر غیرصفری باکوچکترین درجه در I بود.) بنابراین‌همان‌طور که می‌خواستیم بایستی داشته‌باشیم $r(X)=0$ و $a(X)=d(X)q(X)$. یکتایی $d(X)$ واضح است‌زیرا اگر $d_1(X)$ مولدتکین‌دیگری از I باشد، آنگاه $d_1(X)=d(X)q(X)$ و $d(X)=d_1(X)q_1(X)$، پس $d(X)=d(X)q(X)q_1(X)$. طبق‌دستور درجه، ملاحظه می‌کنیم که $q(X)q_1(X)$ دارای درجهٔ صفراست وبنابراین $q(X)$ و $q_1(X)$ هردو یکه‌اند. ولی چون $d_1(X)$ و $d(X)$ هردو تکین‌اند، ازاینرو نتیجه می‌شود $q(X)=q_1(X)=1$، که‌ازآنجا $d_1(X)=d(X)$.

اکنون روش اثبات مشابه تمام قضیه‌های فصل ۵ روشن است. براستی می‌توانیم به‌طور همزمان قضیه‌های متناظر را برای $\mathbf{Z}$ و $F[X]$ به‌وسیلهٔ معرفی ایدهٔ «حوزهٔ اقلیدسی»، که حوزهٔ صحیح باخاصیت اقلیدسی مناسبی است، ثابت کنیم. لیکن، چون مافقط با این دو مثال ازچنین ساختهایی ارتباط خواهیم داشت، طرح‌اصل موضوعه‌ای خیلی ثمربخش‌نیست. به‌جای‌آن، تعاریف وقضایا را برای حلقه‌های چندجمله‌ای بیان می‌کنیم واشارات کافی از براهین می‌آوریم تا خواننده قادر باشد آنهارا تکمیل کند. به‌منظور صرفه‌جویی علامت X را معمولا از چندجمله‌ایها حذف می‌کنیم و می‌نویسیم $a, b, \ldots \in F[X]$ به‌معنی $a(X), b(X), \ldots \in F[X]$.

تقسیم‌پذیری‌دریك‌حلقهٔ چندجمله‌ای $D[X]$ طبق‌معمول تعریف‌می‌شود: $a|b$ یعنی‌اینکه

$\exists c\in D[X]$ به‌قسمی که $b=ac$. خواننده بسادگی خاصیتهای مقدماتی زیر را محقق‌خواهد کرد، دوقسمت‌آخر به‌حوزهٔ صحیح بودن D بستگی دارند.

(الف) به‌ازاء هر $a\in D[X]$ ، $a|0$ ؛

(ب) $a=0 \iff 0|a$ ؛

(پ) $a|b \ \&\ b|c \Rightarrow a|c$ ؛

(ت) به‌ازاء هر $p, q\in D[X]$ ، $a|b \ \&\ a|c \Rightarrow a|bp+cq$ ؛

(ث) در $D[X]$ ، $a \iff a|1$ یکه‌ای از D است.

(ج) به‌ازاء یکه‌ای مانند u از D ، $a|b \ \&\ b|a \iff a=bu$.

برای چندجمله‌ایهای $a, b\in D[X]$ که در آن D یك حوزهٔ صحیح است و a ، b هردو صفر نیستند، گوییم که $d\in D[X]$ بزرگترین مقسوم‌علیه مشترك a و b است اگر

(الف) $d|a$ و $d|b$ ؛

(ب) $c|a \ \&\ c|b \Rightarrow c|d$ ؛

(پ) d تکین باشد.

مانند حالت اعداد صحیح، شرط سوم بدین سبب اضافه شده است که مطمئن شویم d ، درصورت وجود، یکتاست. زیرا اگر d و d_1 هردو درسه شرط صدق کنند آنگاه $d|d_1$ و $d_1|d$. که ازآنجا به‌ازاء یکه‌ای چون u از D ، $d=d_1u$. چون d و d_1 تکین‌اند ، بایستی داشته باشیم $d=d_1$. لیکن، نمی‌توانیم وجود بزرگترین مقسوم‌علیه‌های مشترك را بااین کلیت ثابت کنیم، درحال حاضر ما فقط حالتی را که D میدان است مورد بررسی قرار می‌دهیم.

قضیهٔ ۵ ث. فرض کنید F یك میدان باشد و $a, b\in F[X]$ که هردو صفر نیستند. دراین‌صورت a و b دارای بزرگترین مقسوم‌علیه مشترك یکتای d در $F[X]$ هستند و d می‌تواند به‌ازاء چندجمله‌ایهای مناسب $p, q\in F[X]$ ، به‌صورت $d=ap+bq$ نوشته شود.

برهان. فرض کنید I مجموعهٔ همهٔ چندجمله‌ایهای به‌صورت $ap+bq$ باشد، که در آن a و b چندجمله‌ایهای ثابت مفروض‌اند و p ، q چندجمله‌ایهای دلخواه هستند. درآن‌صورت I ایده‌آلی از $F[X]$ است. (تحقیق‌این‌را به‌عهدهٔ خواننده می گذاریم.) بنا به‌قضیهٔ ۵ ت، این ایده‌آل اصلی‌است و به‌وسیلهٔ یك‌چندجمله‌ای‌تکین، چون $d\in I$، تولید می‌شود. (توجه کنید که $I\neq\{0\}$ زیرا $a\in I$ و $b\in I$.) به‌ازاء چندجمله‌ایهای مناسب $p, q\in F[X]$ ، داریم $d=ap+bq$. بنابراین، اگر $c|a$ و $c|b$ ، داریم $c|d$. بالاخره ، چون $I=dF[X]$ و $a, b\in I$ ، داریم $d|a$ و $d|b$. یکتایی d قبلا اثبات شده است.

همانند حلقهٔ $\mathbf{Z}$ ، دراین مورد نیز $d=(a,b)$ را بـرای بزرگترین‌مقسوم‌علیه مشترك می‌نویسیم، وگوییم که a و b متباین‌اند اگر $(a,b)=1$. همچنین‌قراردادی‌اتخاذ می‌کنیم که $(0,0)=0$ (گرچه این یك‌چندجمله‌ای تکین نیست).

قضیهٔ ۱۰ ج. فرض‌کنید F یك‌میدان‌باشد. دراین‌صورت

(الف) به‌ازاء هر $a,b,c\in F[X]$ ، بافرض تکین‌بودن c ، $(ac,bc)=(a,b)c$؛

(ب) اگر در $F[X]$ ، $d=(a,b)\neq 0$ ، آنگاه $a=da_1$ ، $b=db_1$ که‌درآن a_1 و b_1 متباین‌اند؛

(پ) a و b در $F[X]$ متباین‌اند $\Longleftrightarrow (\exists p,q\in F[X])(ap+bq=1)$ ؛

(ت) اگر در $F[X]$ ، $(a,b)=1$ و $a|bc$ ، آنگاه $a|c$ ؛

(ث) اگر در $F[X]$ ، $a|c$ و $b|c$ ، $(a,b)=1$ ، آنگاه $ab|c$ ؛

(ج) اگر در $F[X]$ ، $a=bq+r$ آنگاه $(a,b)=(b,r)$.

برهان. خواننده باید تحقیق کند که بـرهان قضیهٔ ۵ب در زمینهٔ چندجمله‌ایها باکمی تغییر برقرار است وقتی که شرطی مانند $c>0$ به‌وسیلهٔ شرط «c تکین است» تعویض شود.

آخرین عبارت (ج) از قضیهٔ فوق، درحالت $\mathbf{Z}$ ، مبنایی برای الگوریتم اقلیدس‌است، وبه‌کمك همان استدلال می‌توانیم ثابت‌کنیم که الگوریتم اقلیدس می‌تواند بـرای محاسبهٔ بزرگترین مقسوم‌علیه‌های مشترك‌چندجمله‌ایها (روی‌یك‌میدان)استفاده‌شود. البته، انجام‌عمل تقسیم چندجمله‌ایها مشکلتر‌ازتقسیم اعدادصحیح‌است؛ از اینرو الگوریتم پرزحمت‌تر است، ولی اساس‌کار‌کاملا یکی است. هرگاه چندجمله‌ایهای a_0 ، $a_1\in F[X]$ با $a_1\neq 0$ مفروض باشند، می‌نویسیم

$$\begin{aligned}
a_0&=a_1q_1+a_2\\
a_1&=a_2q_2+a_3\\
&\vdots\\
a_{n-2}&=a_{n-1}q_{n-1}+a_n\\
a_{n-1}&=a_nq_n
\end{aligned}$$

که، درهرمرحله، $\deg(a_i)<\deg(a_{i-1})$. سرانجام باید داشته باشیم $a_{n+1}=0$ زیرا درجه‌ها نمی‌توانند به‌طور نامحدود تنزل‌کنند. اگر $a_n\neq 0$ ، آنگاه a_n ، پس‌ازاینکه بـا ضرب در یکه‌ای تکین شد، بزرگترین مقسوم‌علیه مشترك است، زیرا

$$(a_0,a_1)=(a_1,a_2)=\cdots=(a_{n-1},a_n)=(a_n,0)=a_nu\ ,$$

که‌در آن u معکوس ضریب پیشروی a_n است.

مثال ۱۰. ۱۰. فرض کنید $F=\mathbf{Q}$ و

$$a_0(X)=12X^4-9X^3-14X^2+15X-10$$

و

$$a_1(X)=4X^4+9X^3-7X^2+6X.$$

برای محاسبهٔ ب. م. م. a_0 و a_1 تقسیمات طولانی لازم را درمراحل ساده انجام می‌دهیم، باقیمانده نیز همیشه ازکوچکترین درجهٔ ممکن نیست. همچنین برای اجتناب ازکسرها همه را در یکه‌های مناسب (درواقع اعداد صحیح‌غیرصفر) ضرب می‌کنیم. هیچیك ازاین‌تغییرات الگوریتم درنتیجهٔ حاصله تأثیر نمی‌گذارد.

$$a_0=3a_1+a_2 \text{ ، که‌در آن } a_2=-36X^3+7X^2-3X-10 ;$$

$$9a_1=(-X)a_2+a_3 \text{ ، که‌در آن } a_3=88X^3-66X^2+44X$$

$$=22(4X^3-3X^2+2X)$$

$$a_2=-\frac{9}{22}a_3+a_4 \text{، که‌در آن } a_4=-20X^2+15X-10$$

$$=5(-4X^2+3X-2)$$

$$a_3=(-\frac{22}{5}X)a_4.$$

بنابراین

$$(a_0, a_1)=(a_1, a_2)=(9a_1, a_2)=(a_2, a_3)=(a_3, a_4)=(a_4, 0)$$

$$=X^2-\frac{3}{4}X+\frac{1}{2}.$$

برای بیان این عبارت به‌صورت a_0p+a_1q محاسبه را به‌طریق عکس محاسبات‌فوق‌انجام می‌دهیم:

$$a_4=a_2+\frac{9}{22}a_3=a_2+\frac{9}{22}(9a_1+Xa_2)=\frac{81}{22}a_1+(1+\frac{9}{22}X)a_2$$

$$=\frac{81}{22}a_1+(1+\frac{9}{22}X)(a_0-3a_1)$$

$$=(1+\frac{9}{22}X)a_0+(\frac{15}{22}-\frac{27}{22}X)a_1.$$

دراین‌صورت ب. م. م. تکین به‌وسیلهٔ تقسیم بر ۲۰ — به‌دست می‌آید.

مثال ۱۰. ۲. فرض کنید $F=\mathbf{Z}_5$ و

$$a_0=2X^3+4X+1 \quad \text{و} \quad a_1=3X^3+2X^2+3X+2 .$$

دراینجا خطهای روی ضرایب را، که اعداد صحیح نیستند بلکه رده‌های باقیمانده به پیمانهٔ ۵ هستند، حذف می‌کنیم. لیکن می‌توانیم با اعداد صحیح محاسبه کنیم به‌شرطی که بخاطر داشته باشیم که $7=3-=2$ وغیره. چون معکوسهای ۱ ، ۲ ، ۳ و ۴ عبارت‌اند از : ۱ ، ۳ ، ۲ و ۴ ، کار با اینها خیلی ساده است، البته، الگوریتم به‌وسیلهٔ این‌حقیقت که $\mathbf{Z}_5$ میدان است توجیه می‌شود.

$$a_0=4a_1+a_2 \text{ ، که درآن } a_2=2X^2+2X+3 ;$$
$$a_1=4Xa_2+a_3 \text{ ، که درآن } a_3=4X^2+X+2 ;$$
$$a_2=3a_3+a_4 \text{ ، که درآن } a_4=4X+2 ;$$
$$a_3=Xa_4+a_5 \text{ ، که درآن } a_5=4X+2 ;$$
$$a_4=a_5$$

بنابراین $d=4a_5=X+3$ ب. م. م. است. اگر مرحله‌به‌مرحله به‌عقب برگردیم، به‌دست می‌آوریم

$$d=4a_4=4a_2+3a_3=4a_2+3(a_1+Xa_2)=(4+3X)a_2+3a_1$$
$$=(4+3X)(a_0+a_1)+3a_1=(4+3X)a_0+(7+3X)a_1 .$$

مشابه «عدد اول» برای حلقهٔ $F[X]$ ، «چندجمله‌ای تکین تحویل‌ناپذیر» است که درزیر تعریف شده است. چندجمله‌ای $p\in F[X]$ تحویل‌ناپذیر است اگر

(الف) $p\neq 0$ ،

(ب) p چندجمله‌ای یکه نباشد ، و

(پ) هرمقسوم‌علیه p در $F[X]$ به‌صورت u یا up باشد، که u یك یکه است.

چون یکه‌های $F[X]$ دقیقاً چند جمله‌ایهای درجهٔ صفرند، بسادگی‌دیده می‌شود که یك چند-جمله‌ای تحویل‌ناپذیر است اگروفقط اگر حداقل دارای درجهٔ ۱ باشد ونتواند به‌صورت حاصلضرب‌دو چندجمله‌ای از درجهٔ بزرگتریا مساوی۱ نوشته‌شود. دوچندجمله‌ای‌تحویل‌ناپذیر وابسته‌هستند اگریکی برابرمضرب یکه‌ای از دیگری‌باشد.درهر رده ازچندجمله‌ایهای‌تحویل-ناپذیر وابسته یك‌چندجمله‌ای تکین تحویل‌ناپذیر یکتا وجود دارد (که همان نقش عدد اول مثبت nرا که از جفت $\pm n$ اختیار شده، ایفامی‌کند). با به‌کاربردن‌خواص‌بزرگترین مقسوم-علیه مشترك، همانند قضیهٔ ۵پ ، خواننده نباید دراثبات قضیهٔ زیر بااشکالی مواجه گردد.

قضیهٔ۱۰ چ. فرض‌کنید F یك میدان باشد. دراین‌صورت

(الف) اگر p و q چندجمله‌ایهای تکین تحویل‌ناپذیر در $F[X]$ باشند و $p|q$ ، آنگاه $p=q$ ؛

(ب) اگر $p\in F[X]$ ، a ، و چنانچه p تحویل‌ناپذیر باشد و $p\nmid a$ ، آنگاه $(p,a)=1$ ؛

(پ) اگر چندجمله‌ای $a\in F[X]$ صفر، یکه و تحویل‌ناپذیر نباشد، آنگاه b ، $c\in F[X]$ وجود دارد به‌قسمی که

$$a=bc\ ,\quad 0<\deg(b)<\deg(a)\ ,\quad 0<\deg(c)<\deg(a)\ ;$$

(ت) اگر p یك چندجمله‌ای تحویل‌ناپذیر باشد و $p|a_1a_2\cdots a_n$ در $F[X]$ برقرار باشد، آنگاه به‌ازاء حداقل یك مقدار i ، $p|a_i$.

بامجهز شدن به این اطلاعات می‌توانیم قضیهٔ یکتایی تجزیه برای چندجمله‌ایها را ثابت کنیم.

قضیهٔ ۱۰ ح. فرض کنید F یك میدان باشد. دراین صورت

(الف) هر چندجمله‌ای غیر صفر $a\in F[X]$ می‌تواند به‌صورت $a=up_1p_2\cdots p_r$ تجزیه شود، که u یك یکه است، وهر p_i یك چندجمله‌ای تکین تحویل‌ناپذیر است، و $r\geqslant 0$ ؛

(ب) اگر $a=vq_1q_2\cdots q_s$ تجزیهٔ دیگری باشدکه v یکه وهر q_j چندجمله‌ای تکین تحویل‌ناپذیر است، آنگاه $u=v$ ، $r=s$ و q_1 ، q_2 ، ... ، q_s جایگشتی از p_1 ، p_2 ، ... ، p_r است.

برهان. (الف) چون هر چندجمله‌ای غیرصفر مضرب یکه‌ای از یك چندجمله‌ای تکین است، می‌توانیم فرض کنیم که a تکین است. اگر a یکه باشد، می‌توان اختیار کرد، $u=a$ ، $r=0$. اگر a تحویل‌ناپذیر باشد، می‌توان اختیار کرد: $u=1$ ، $r=1$ ، $p_1=a$. درغیراین‌صورت، بنا به‌قضیهٔ ۱۰ ج، $a=bc$ که در آن $0<\deg(b)<\deg(a)$ و $0<\deg(c)<\deg(a)$. چون a تکین است می‌توانیم هردوی b و c را تکین اختیار کنیم. حال عمل استقراء روی $\deg(a)$ وجود تجزیهٔ مطلوب مانند حالت $\mathbf{Z}$ را به‌دست می‌دهد. (قضیهٔ ۵ ت را ببینید.)

(ب) فرض کنیم که $a=up_1p_2\cdots p_r=vq_1q_2\cdots q_s$. واضح است که $u=v$ ضریب پیشروی a است، از اینرو می‌توان فرض کرد که a تکین است و $u=v=1$. اگر a دارای درجهٔ صفر باشد آنگاه $a=1$ و واضح است که $r=s=0$. بنابراین می‌توان فرض کرد که $a=p_1p_2\cdots p_r=q_1q_2\cdots q_s$ با $r\geqslant 1$ ، $s\geqslant 1$. چندجمله‌ایهای تحویل‌ناپذیر را نمی‌توانیم به ترتیب صعودی مرتبه‌هایشان مرتب کنیم، چنانکه برای اعداد صحیح انجام دادیم، ولی اساساً استدلال یکی است. ازاستقراء روی درجهٔ a استفاده می‌کنیم، حالت $\deg(a)=0$ قبلا مورد رسیدگی قرار گرفته است. داریم $p_1|q_1q_2\cdots q_s$ ، از اینرو به‌ازاء اندیسی

چون j، $p_1 | q_j$ ، و بنابراین، بنا به قضیهٔ ۱۰ ج، $p_1 = q_j$. چون $F[X]$ یك حوزهٔ صحیح است (قضیهٔ ۱۰ ت ۲) می‌توان p_1 و q_j را حذف نمود و $b = p_2 p_3 \cdots p_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s$ را به دست آورد. ولی $\deg(b) < \deg(a)$ ، از اینرو بنا به فرض استقراء ، q_1 ، ... ، q_{j-1} ، q_{j+1} ، ... ، q_s جایگشتی از p_2 ، p_3 ، ... ، p_r است، وچون $p_1 = q_j$ نتیجه می‌شود که q_1 ، q_2 ، ... ، q_s جایگشتی از p_1 ، p_2 ، ... ، p_r است.

مثال ۳.۱۰. تجزیهٔ یك چندجمله‌ای به عوامل تحویل‌ناپذیر بستگی زیادی به میدانی دارد که ضرایب می‌باید از آنجا انتخاب شوند. مثلا ، چندجمله‌ای $X^4 - 4$ می‌تواند به‌عنوان عضوی از $\mathbf{C}[X]$ ، $\mathbf{R}[X]$ یا $\mathbf{Q}[X]$ بررسی گردد. تجزیهٔ آن در $\mathbf{C}[X]$ ، به صورت $(X - \sqrt{2})(X + \sqrt{2})(X - i\sqrt{2})(X + i\sqrt{2})$ است؛ این عاملها الزاماً تحویل‌ناپذیرند زیرا آنها از درجهٔ ۱ هستند. در $\mathbf{R}[X]$ داریم $X^4 - 4 = (X - \sqrt{2})(X + \sqrt{2})(X^2 + 2)$ وهمهٔ این عاملها در $\mathbf{R}[X]$ تحویل‌ناپذیرند. در $\mathbf{Q}[X]$ نمی‌توانیم تجزیه‌ای بهتر از $X^4 - 4 = (X^2 - 2)(X^2 + 2)$ انجام دهیم. در آینده توجیه این ادعاها ساده‌تر خواهد شد. لیکن، هم‌اکنون می‌توانیم مطمئن باشیم که در هریك از این حلقه‌های چندجمله‌ای، تجزیه به‌عوامل تحویل‌ناپذیر یکتاست.

یك جنبه از چندجمله‌ایها که حلقهٔ اعداد صحیح بکلی فاقد آن است ، این است که چندجمله‌ایها می‌توانند برای تعریف توابع به‌کار روند. اگر R حلقهٔ جابجایی دلخواهی باشد و چنانچه $a(X) \in R[X]$ ، آنگاه به ازاء عنصرهایی چون $a_i \in R$ ، $a(X) = a_0 + a_1 X + \cdots + a_n X^n$. اگر دراین دستور به‌جای X عضو x از R را جایگزین کنیم، عبارتی به‌صورت $a_0 + a_1 x + \cdots + a_n x^n$ به‌دست می‌آوریم که با به‌کار بردن اعمال حلقهٔ R می‌توانند محاسبه شوند، ونتیجه عضوی از R است که به‌وسیلهٔ $a(x)$ نشان‌داده می‌شود. بنابراین چندجمله‌ای $a(X)$ تابعی مانند $\alpha : x \longmapsto a(x)$ از R به R را معین می‌کند . و این‌را تابع چندجمله‌ای می‌نامیم . نمادگذاری، ما را ملزم می‌کند که این تابع‌را به وسیلهٔ a نشان دهیم زیرا مقدارش در x برابر است با $a(x)$. لیکن، از این نماد بایستی اجتناب‌شود زیرا ممکن است که چندجمله‌ایهای متفاوت تنها یك تابع چندجمله‌ای را معین‌کنند.

مثال ۴.۱۰. فرض کنید $R = \mathbf{Z}_p$ ، که در آن p یك عدد اول است. در حلقهٔ چندجمله‌ای $\mathbf{Z}_p[X]$ ، X^p و X چندجمله‌ایهای متفاوت‌اند زیرا دارای درجات مختلف‌اند: اما توابع از $\mathbf{Z}_p$ به $\mathbf{Z}_p$ که به‌وسیلهٔ آنها معین می‌شوند عبارت‌اند از: $x^p \longmapsto x$ و $x \longmapsto x$ ، و هر دوی اینها یك تابع هستند زیرا، بنا به نتیجهٔ ۲ قضیهٔ ۹ ب ، به‌ازاء هر $x \in \mathbf{Z}_p$ ، $x^p = x$.

به‌عبارت دیگر، این اخطار می‌گوید که چندجمله‌ای $a[X] \in R[X]$ ممکن است بدون اینکه چندجمله‌ای صفر باشد، به‌ازاء هر $x \in R$ در «اتحاد» $a(X) = 0$ صدق کند (مثلا، چندجمله‌ای $a(X) = X^p - X$ وقتی که $R = \mathbf{Z}_p$). بنابراین استدلالی که غالباً به‌کار می‌رود «به‌ازاء هر x ، $a(x) = b(x)$ ، پس می‌توان ضرایب $a(X)$ و $b(X)$ را برابر گرفت»

درحالت عمومی معتبر نیست. همان‌طور که مثال ۴.۱۰ نشان می‌دهد، این مطلب حتی‌وقتی که R یك میدان است معتبر نیست. لیکن بزودی نشان خواهیم داد که این‌مطلب هنگامی که R میدانی نامتناهی است، معتبر است.

قضیهٔ ۱۰ خ. (خاصیت‌جامع حلقه‌های‌چندجمله‌ای.) فرض‌کنید R ، S حلقه‌های‌جابجایی و $f : R \longrightarrow S$ یك همریختی حلقه‌ها باشد ، و $x \in S$. دراین صورت همریختی یکتایی ازحلقه‌های $R[X] \longrightarrow S$ وجود دارد به‌قسمی‌که(الف) به‌ازاء هر $r \in R$ ، $r \longmapsto f(r)$ و (ب) $X \longmapsto x$. این همریختی به ازاء هر چندجمله‌ای $a(X) \in R[X]$ ، به‌وسیلهٔ $a(X) \longmapsto a^*(X)$ داده می‌شود، که‌درآن چندجمله‌ای $a^*(X) \in S[X]$ از $a(X)$ باائر f به‌همهٔ ضرایبش به‌دست می‌آید.

برهان. فرض‌کنید یك همریختی F از $R[X]$ به S وجود داشته باشدکه در (الف) و (ب) صدق کند. با نوشتن r^* به‌جای $f(r)$ می‌بینیم که چون F ضرب را حفظ می‌کند، rX^n را به r^*x^n می‌فرستد. بنابراین F بایستی $\sum a_i X^i$ را به $\sum a_i^* x^i$ بفرستد، زیرا جمع را نیز حفظ می‌کند. این نشان‌می‌دهد که F یکتاست و به‌وسیلهٔ $a(X) \longrightarrow a^*(x)$ داده‌شده‌است. برای اثبات وجوداین‌همریختی، فرض‌می‌کنیم F نگاشتی از $R[X]$ به S باشد که به‌وسیلهٔ $a(X) \longmapsto a^*(x)$ داده‌شده‌است. این نگاشت‌خوش تعریف است و درشرایط (الف)و(ب) صدق می‌کند؛ جمع وضرب‌را نیز حفظ‌می‌کند زیرا اعمال‌روی $R[X]$ دقیقاً بادرنظرگرفتن‌این‌موضوع‌تعریف‌شده‌اند. برای اثبات آن، فرض‌کنید $a(X) = \sum a_i X^i$ ، $b(X) = \sum b_j X^j$. دراین‌صورت، بنابه تعریف ، $a(X)+b(X)$ چندجمله‌ای $\sum (a_i+b_i)X^i$ است که به‌وسیلهٔ F به $\sum (a_i+b_i)^* x^i = \sum (a_i^*+b_i^*)x^i$ نگاشته‌می‌شود. قوانین‌حلقه در S نتیجه‌می‌دهندکه‌این برابر است با $a^*(x)+b^*(x)$. بنابراین F جمع راحفظ‌می‌کند. به‌همین‌ترتیب، $a(X)b(X) = c(X)$ ، که درآن $c(X) = \sum c_n X^n$ و

$$c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 .$$

این چند جمله‌ای به‌وسیلهٔ F به $c^*(x) = \sum c_n^* x^n \in S$ نگاشته می‌شود . ولی $c_n^* = a_0^* b_n^* + a_1^* b_{n-1}^* + \cdots + a_n^* b_0^*$، زیرا f یك همریختی حلقه‌ای است. نتیجه‌می‌شود که

$$\begin{aligned} a^*(x)b^*(x) &= (\sum a_i^* x^i)(\sum b_j^* x^j) \\ &= \sum c_n^* x^n \\ &= c^*(x) \end{aligned}$$

(قوانین S را برای دسته‌بندی همهٔ جمله‌هایی که حاوی x^*اند، به‌کار برده‌ایم). بنابراین F ضرب را حفظ می‌کند ویك همریختی حلقه‌هاست. بدین‌ترتیب قضیه اثبات می‌شود.

نتیجهٔ ۱. به‌ازاء حلقهٔ جابجایی دلخواه R وهرعنصر $x \in R$ ، نگاشت از $R[X]$ به R که باضابطهٔ

$a(X)\longmapsto a(x)$ داده شده، یك همریختی حلقه‌هاست.

برهان. این حالت خاص قضیه است که در آن $R=S$ و f نگاشت همانی باشد.

نتیجهٔ ۲. (قضیهٔ باقیمانده.) فرض کنید F یك میدان باشد، $t\in F$ و $a(X)\in F[X]$. دراین صورت r، باقیماندهٔ تقسیم $a(X)$ بر $X-t$ برابر است با $a(t)$.

برهان. بنا به قضیهٔ ۱۰پ، داریم

$$a(X)=(X-t)q(t)+r, \qquad (1)$$

که در آن $\deg(r)<1$، یعنی $r\in F$. بنا به نتیجهٔ ۱، نگاشتی که هرچندجمله‌ای $b(X)$ را به $b(t)\in F$ بفرستد یك همریختی حلقه‌هاست و بنا بر این رابطهٔ (۱) را بین چندجمله‌ایها حفظ می‌کند. پس در F داریم

$$a(t)=(t-1)q(t)+r,$$

و از اینرو $r=a(t)$.

نتیجهٔ ۳. (قضیهٔ عامل). فرض کنید F یك میدان باشد، $t\in F$ و $a(X)\in F[X]$. دراین صورت در $F[X]$، $(X-t)$ چندجمله‌ای $a(X)$ را عاد می‌کند اگر و فقط اگر در F، $a(t)=0$.

برهان. $(X-t)\mid a(X)$ $\Longleftrightarrow$ در نتیجهٔ ۲، $r=0$.

هرعنصر $t\in F$ به‌قسمی که $a(t)=0$ یك ریشهٔ $a(X)$ در F نامیده می‌شود. چندجمله‌ای مفروض $a(X)\in F[X]$ ممکن است دارای هیچ ریشه‌ای در F نباشد. مثلا، X^2+2 هیچ ریشه‌ای در $\mathbf{R}$ ندارد زیرا به‌ازاء هر $t\in\mathbf{R}$، $t^2+2\geqslant 2$، ازاینرو نمی‌توانیم داشته باشیم $t^2+2=0$.

قضیهٔ ۱۰د. فرض کنید F یك میدان باشد و $a(X)\in F[X]$ دارای درجهٔ بزرگتر یا مساوی صفر n. دراین صورت $a(X)$ حداکثر دارای n ریشهٔ متمایز در F است.

برهان. از استقراء روی n استفاده می‌کنیم. اگر $n=0$ آنگاه $a(X)$ عنصری غیرصفر از F است وهیچ ریشه‌ای ندارد. اگر $n>0$ و $a(X)$ هیچ ریشه‌ای نداشته باشد، قضیه درست است. چنانچه دارای یك ریشهٔ t باشد، آنگاه بنا به قضیهٔ عامل $a(X)=(X-t)b(X)$، که درآن $b(X)$ دارای درجهٔ $n-1$ است. اگر s ریشهٔ دیگری از $a(X)$ در F باشد به‌قسمی که $s\neq t$، آنگاه $0=a(s)=(s-t)b(s)$، که از آنجا $b(s)=0$ زیرا $s-t\neq 0$

و F یك میدان است. اما، بنا به فرض استقراء، $b(X)$ حداکثر دارای $n-1$ ریشهٔ متمایز است، پس $a(X)$ حداکثر دارای $n-1$ ریشهٔ متمایز بجز t است، ازاینرو روی‌هم‌رفته حداکثر n ریشه دارد. بدین‌ترتیب قضیه به‌ازاء همهٔ n ها درست‌است.

نتیجهٔ ۱. اگرچندجمله‌ای $a(X)\in F[X]$ دارای درجهٔ‌کمتراز m باشد و m ریشهٔ متمایز در F داشته باشد، آنگاه یك چندجمله‌ای صفراست.

برهان. اگر $a(X)\neq 0$ آنگاه دارای‌درجهٔ بزرگتر یا مساوی‌صفر n است وازاینرو نمی‌تواند بیش‌از n ریشهٔ متمایز داشته باشد.

نتیجهٔ ۲. اگر $a(X)$ ، $b(X)\in F[X]$ هردو بادرجهٔ‌کمتراز m باشند وچنانچه به‌ازاء m مقدار متمایز t در F ، $a(t)=b(t)$ ، آنگاه $a(X)=b(X)$.

برهان. نتیجهٔ ۱ را برای چندجمله‌ای $a(X)-b(X)$ ، که درجه‌اش کمتراز m است ، به‌کار ببرید.

نتیجهٔ ۳. فرض کنید F میدانی نامتناهی باشد و $a(X)$ ، $b(X)\in F[X]$. اگر به ازاء هر $t\in F$ ، $a(t)=b(t)$ ، آنگاه $a(X)=b(X)$. بنابراین دراین‌حالت چندجمله‌ایهای‌متمایز، توابع چندجمله‌ای‌متمایزی‌راهعین می‌کنند.

برهان. فرض کنید n از درجهٔ $a(X)$ و $b(X)$ بزرگتر باشد. دراین صورت به‌ازاء $n+1$ مقدار متمایز t در F ، $a(t)=b(t)$ ، ازاینرو نتیجهٔ۲ به‌دست می‌دهد که $a(X)=b(X)$.

نتیجهٔ ۴. فرض‌کنید F میدان دلخواهی باشد و $a(X)\in F[X]$ دارای درجهٔ بزرگتر از صفر n. اگر $a(X)$ دارای n ریشهٔ متمایز t_1 ، t_2 ، ... ، t_n در F باشدآنگاه

$$a(X)=u(X-t_1)(X-t_2)\cdots(X-t_n),$$

که‌درآن u ضریب‌پیشروی $a(X)$ است.

برهان. چندجمله‌ای

$$b(X)=a(X)-u(X-t_1)(X-t_2)\cdots(X-t_n)$$

را درنظر بگیرید. درجه‌اش‌کمتراز n است زیرا ضریب X^n برابراست با $u-u=0$. اما $b(X)$ دارای n ریشهٔ متمایز t_1 ، t_2 ، ... ، t_n است، از اینرو بایستی چندجمله‌ای صفر باشد.

مثال ۵.۱۰. فرض کنید $F=\mathbf{Z}_p$ ، که p یک‌عدد اول است. دراین‌صورت F میدان است و همهٔ نتایج فوق برای حلقهٔ چندجمله‌ای $\mathbf{Z}_p[X]$ درست هستند. حال چندجمله‌ای X^p-X دارای p ریشهٔ متمایز در $\mathbf{Z}_p$ است، یعنی، بنا به قضیهٔ فرما، همهٔ عناصر $\mathbf{Z}_p$ ریشه‌اند. دراین صورت می‌توانیم نتیجهٔ ۴ فوق‌را به‌کار ببریم واستنتاج کنیم که در $\mathbf{Z}_p[X]$

$$X^p-X=X(X-۱)(X-۲)\cdots(X-p+۱)\ .$$

به‌عنوان مثال، اگر $p=۳$ داریم

$$X(X-۱)(X-۲)=X(X^۲-۳X+۲)=X(X^۲-۱)=X^۳-X\ .$$

البته، می‌توانیم X را از دوطرف حذف کنیم تا در $\mathbf{Z}_p[X]$ به‌دست‌آوریم:

$$X^{p-۱}-۱=(X-۱)(X-۲)\cdots(X-p+۱)\ .$$

دراین رابطه علامتهای ۱ ، ۲ ، ... عناصر $\mathbf{Z}_p$ هستند. اکنون تساوی چندجمله‌ایها به‌معنی تساوی ضرایب توانهای متناظر X است، ازاینرو می‌توان «ضرایب را مساوی گرفت». جمله‌های بادرجهٔ صفر در $\mathbf{Z}_p$ به‌دست می‌دهند

$$-۱=(-۱)(-۲)\cdots(-p+۱)\ .$$

به‌عبارت‌دیگر، باتحویل به‌اعداد صحیح واقعی، داریم

$$-۱\equiv(-۱)(-۲)\cdots(-p+۱)\quad(\text{به‌پیمانهٔ } p)\ ,$$

که به (به پیمانهٔ p) $(-۱)^p\equiv(-۱)^{p-۱}$ تبدیل می‌شود. از آنجاکه اگر p فرد باشد $-۱=(-۱)^p$ ، و (به‌پیمانهٔ ۲) $-۱\equiv(-۱)^۲$ ، می‌توانیم بنویسیم

$$-۱\equiv(-۱)!\ (p-۱)\quad(\text{به‌پیمانهٔ } p)\ ،\ \text{به‌ازاء هرعدد اول } p$$

نتیجه‌ای‌که به‌نام قضیهٔ ویلسون[1] مشهور است.

شباهت میان اعداد صحیح و چندجمله‌ایها روی میدان F می‌تواند بیش‌ازآنچه که ما تاکنون انجام داده‌ایم دنبال شود. ما به تعدادی از نتایجی که می‌توانند به‌این‌طریق به‌دست آیند اشاره‌خواهیم کرد. همنهشتیها می‌توانند به‌وسیلهٔ نوشتن (به‌پیمانهٔ $p(X)$) $a(X)\equiv b(X)$ اگر $p(X)\mid\{a(X)-b(X)\}$ ، درحلقهٔ چندجمله‌ای $F[X]$ تعریف شوند. این معادل آن است که بگوییم $a(X)$ و $b(X)$ دریک‌همردهٔ جمعی از ایده‌آل $I=p(X)F[X]$ متشکل‌از تمام مضارب $p(X)$ ، قرار دارند. بنابراین، درست مانند اعداد صحیح، رده‌های باقیماندهٔ چندجمله‌ایها به‌پیمانهٔ $p(X)$ تشکیل یک‌حلقهٔ جابجایی می‌دهند. یعنی حلقهٔ خارج قسمت $F[X]/I$.

قضیهٔ ۱۰ذ. فرض کنید F یک‌میدان باشد، $p(X)\in F[X]$ و I ایده‌آل اصلی که به‌وسیلهٔ $p(X)$ تولیدشده‌است، دراین‌صورت $F[X]/I$ میدان‌است اگر و فقط اگر $p(X)$ تحویل‌ناپذیر باشد.

1-Wilson

برهان. فرض کنید $p(X)$ تحویل‌ناپذیر باشد. می‌دانیم که $R=F[X]/I$ یک‌حلقهٔ‌جابجایی است و باید نشان دهیم که عناصر غیر صفر آن دارای معکوس‌اند. به‌عبارت دیگر، اگر $a(X)\in F[X]$ و $p(X)\nmid a(X)$ باید نشان دهیم که چندجمله‌ای $b(X)$ به‌قسمی وجود دارد که (به‌پیمانهٔ $p(X)$) $a(X)b(X)\equiv 1$. اما مانند اعداد صحیح و بنابه‌قضیهٔ ۱۰ ج، داریم $1=(a(X),p(X))$، ازاینرو می‌توانیم $r(X)$ و $s(X)$ را به‌قسمی پیدا کنیم که $p(X)r(X)+a(X)s(X)=1$. دراین صورت چند جمله‌ای $s(X)$ در خاصیت (به‌پیمانهٔ $p(X)$) $a(X)s(X)\equiv 1$ صدق‌می‌کند. ازطرف‌دیگر، اگر $p(X)$ تحویل‌ناپذیر نباشد آنگاه یا (الف) $p(X)$ برابر صفر است، یا (ب) یك یکه است، یا (پ) $p(X)=a(X)b(X)$، که‌درآن $a(X)$، $b(X)$ غیرصفر و بادرجهٔ کوچکتراز درجهٔ $p(X)$ اند. درحالت (الف) $F[X]/I\cong F[X]$ که میدان نیست. درحالت (ب) $I=F[X]$، ازاینرو $F[X]/I$ حلقهٔ تك عنصری است ومیدان نیست، درحالت(پ) رده‌های باقیماندهٔ شامل $a(X)$ و $b(X)$ غیرصفرند ولی حاصلضربشان صفر است، پس $F[X]/I$ حتی حوزهٔ صحیح‌هم نیست.

مثال ۶.۱۰. فرض کنید $F=\mathbf{R}$ و $p(X)=X^2+1$. دراین‌صورت چندجمله‌ای $p(X)$ در $\mathbf{R}[X]$ تحویل‌ناپذیر است (درغیر این‌صورت $p(X)$ حاصلضرب دوعامل با درجهٔ ۱ بوده، دارای ریشه‌ای در $\mathbf{R}$ است). بنابراین رده‌های باقیمانده به‌پیمانهٔ X^2+1 تشکیل‌یك میدان می‌دهند. برای‌انجام‌محاسبات دراین میدان، چندجمله‌ایهای باضرایب حقیقی را به‌کار می‌بریم‌اما باقراردادن $X^2=-1$ هرجاکه X^2ظاهرشود، آنهارا به‌پیمانهٔ X^2+1تحویل می‌کنیم. دراین‌صورت‌هرچندجمله‌ای‌بایك‌چندجمله‌ای‌به‌صورت $a+bX$ $(a,b\in\mathbf{R})$همنهشت است وهیچ دوچندجمله‌ای از این نوع همنهشت نیستند. اینهارا مانند چندجمله‌ایها جمع و ضرب می‌کنیم باقرار دادن $X^2=-1$ وخواننده متوجه خواهد شدکه میدان جدیددرست همان‌میدان اعداد مختلط است؛ زیرا اگر درهمه‌جا علامت X را با i جایگزین کنیم‌محاسبات درست همانند محاسبات درمیدان $\mathbf{C}$ است.

مثال ۷.۱۰. فرض کنید $F=\mathbf{Z}_2$ و $p(X)=X^2+X+1$. آنگاه $p(X)$ در $\mathbf{Z}_2[X]$ تحویل‌ناپذیراست‌زیرا درغیراین‌صورت‌حاصلضربی‌ازعوامل بادرجهٔ ۱ بوده‌ودرنتیجه‌دارای ریشه‌ای در $\mathbf{Z}_2$ است واین درست نیست چون $p(0)=1=p(1)$. بنابراین رده‌های باقیماندهٔ چندجمله‌ایهای به‌پیمانهٔ X^2+X+1 تشکیل میدان می‌دهند. هرچندجمله‌ای با یك‌چندجمله‌ای به‌صورت $a+bX$ $(a,b\in\mathbf{Z}_2)$ همنهشت است ومحاسبه باآنهارا همچون چندجمله‌ایها انجام می‌دهیم ولی جواب را با قراردادن $X+1=-(X+1)=X^2$ هرجاکه X^2 ظاهرشود، به‌صورت $a+bX$ تبدیل می‌کنیم. فقط چهارچندجمله‌ای به‌صورت $a+bX$ وجود دارد: یعنی ۰، ۱، X، $X+1$. جدولهای جمع‌وضرب عبارت‌اند از:

$+$	0	1	X	$1+X$
0	0	1	X	$1+X$
1	1	0	$1+X$	X
X	X	$1+X$	0	1
$1+X$	$1+X$	X	1	0

$\times$	0	1	X	$1+X$
0	0	0	0	0
1	0	1	X	$1+X$
X	0	X	$1+X$	1
$1+X$	0	$1+X$	1	X

این جدولها شبیه‌جدولهای مثال۲.۹ هستند (باتغییری درنماد)، ازاینرو اکنون نشان‌داده‌ایم که این مثال میدانی با چهار عنصر است. این‌روش می‌تواند برای ساختن میدان متناهی از مرتبهٔ q به‌کار رود، که q هرتوانی ازیك‌عدد اول است.

قضیهٔ۱۰ ر. (قضیهٔ باقیماندهٔ چینی برای چندجمله‌ایها.) فرض‌کنید F یـك میدان باشد و $p_1(X)$ ، $p_2(X)$ ، ... ، $p_n(X)$ چـند جمله‌ایـهای دو بـدو متبایـن در $F[X]$. هرگاه $c_1(X)$ ، $c_2(X)$ ، ... ، $c_n(X)$ چندجمله‌ایهای دلخواهـی در $F[X]$ باشند، دراین‌صورت یك چندجمله‌ای $a(X)$ در $F[X]$ به‌قسمی وجـود دارد کـه بـه‌ازاء n ، ... ، ۲ ، ۱ $=i$ ، $a(X)\equiv c_i(X)$ $(p_i(X)$ به‌پیمانهٔ$)$، و $a(X)$ به‌پیمانهٔ $p(X)=p_1(X)p_2(X)\cdots p_n(X)$ یکتاست.

برهان. برهان دقیقاً همانند حالت اعداد صحیح است. ابتدا، قرار دهید،

$$q_1(X)=p_2(X)p_3(X)\cdots p_n(X).$$

دراین‌صورت $p_1(X)$ با $q_1(X)$ متباین است وبنابراین می‌توانیم بنویسیم

$$1=p_1(X)r_1(X)+q_1(X)s_1(X).$$

حال چندجمله‌ای $a_1(X)=q_1(X)s_1(X)$ درشرایط زیرصدق می‌کند،

$$a_1(X)\equiv 1 \ (p_1(X) \text{ به‌پیمانهٔ})$$

$$a_1(X)\equiv 0 \ (p_i(X) \text{ به پیمانهٔ}) \qquad \text{و به ازاء } i=2,3,\dots,n,$$

به همین ترتیب می‌توانیم به ازاء $j=1,2,\dots,n$ ، $a_j(X)$ را طوری پیدا کنیم که

$$a_j(X)\equiv 1 \quad (p_j(X) \text{ به پیمانهٔ})$$

$$a_j(X)\equiv 0 \ (p_i(X) \text{ به پیمانهٔ}) \qquad \text{و به ازاء } i\neq j,$$

حال چندجمله‌ای $a(X)=\sum a_i(X)c_i(X)$ در تمام همنهشتیهای

$$a(X)\equiv c_i(X) \ (p_i(X) \text{ به پیمانهٔ})$$

صدق می‌کند. اگر $b(X)$ جواب دیگری باشد آنگاه به ازاء $i=1,2,\dots,n$ ، $a(X)\equiv b(X)$ ($p_i(X)$ به پیمانهٔ) و نتیجه می‌شود که $a(X)\equiv b(X)$ ($p(X)$ به پیمانهٔ) . همچنین واضح است که هر چندجمله‌ای همنهشت با $a(X)$ ($p(X)$ به پیمانهٔ) یك جواب است.

مثال ۸.۱۰. حالت خاص جالبی از قضیهٔ باقیماندهٔ چینی به صورت زیر است. فرض کنید $t_1, t_2, \dots, t_n$ عناصر متمایزی از F باشند. در این صورت چندجمله‌ایهای تکین $X-t_1$ ، $X-t_2$ ، ... ، $X-t_n$ متمایز و تحویل‌ناپذیرند و از اینرو دو به دو متباین‌اند. اگر قرار دهیم $p_i(X)=X-t_i$ و $c_i(X)$ را عنصری مانند c_i از F اختیار کنیم، آنگاه قضیه بیان می‌کند که یك چندجمله‌ای $a(X)$ وجود دارد که به ازاء $i=1,2,\dots,n$ در شرط $a(X)\equiv c_i$ ($(X-t_i)$ به پیمانهٔ) صدق می‌کند. حال قضیهٔ باقیمانده (غیرچینی!) می‌گوید که $a(t_i)=c_i \iff a(X)\equiv c_i$ ($(X-t_i)$ به پیمانهٔ) . بنابراین چندجمله‌ای $a(X)$ وجود دارد که مقادیر مفروض $c_1, c_2, \dots, c_n$ را در نقاط (متمایز) مفروض $t_1, t_2, \dots, t_n$ اختیار می‌کند. بعلاوه، مجموعهٔ تمام چنین چندجمله‌ایهایی یك ردهٔ باقیمانده به پیمانهٔ $(X-t_1)(X-t_2)\cdots(X-t_n)$ است. چون $p(X)=(X-t_1)(X-t_2)\cdots(X-t_n)$ دارای درجهٔ n است، چندجمله‌ای یکتایی مانند $a(X)$ با درجهٔ کمتر از n وجود دارد که به ازاء $i=1,2,\dots,n$، درشرط $a(t_i)=c_i$ صدق می‌کند (یعنی، باقیماندهٔ تقسیم هرچنین چندجمله‌ای بر $p(X)$) . درواقع برای نوشتن این چندجمله‌ای می‌توانیم روش ارائه شده در برهان قضیه را به کار گیریم. ابتدا، بایستی چندجمله‌ای $a_i(X)$ را پیدا کنیم که در $a_i(t_i)=1$ و $a_i(t_j)=0$ به ازاء $j\neq i$ صدق کند. چندجمله‌ای

$$b_i(X)=\prod_{j\neq i}(X-t_j)$$

تقریباً درست است. این چندجمله‌ای دارای خاصیتهای $b_i(t_j)=0$ ، به ازاء $j\neq i$ و

$$b_i(t_i)=(t_1-t_i)(t_2-t_i)\cdots(t_{i-1}-t_i)(t_{i+1}-t_i)\cdots(t_n-t_i)=s_i$$

است. بنابراین $a_i(X)$ را به صورت زیر اختیار می‌کنیم

$$a_i(X)=s_i^{-1}\prod_{j\neq i}(X-t_j)$$

اکنون چندجمله‌ای مطلوب به صورت زیر است

$$a(X)=\sum_{i=1}^{n} c_i a_i(X)=\sum_{i=1}^{n} c_i s_i^{-1}\prod_{j\neq i}(X-t_j)\ ,$$

این دستوری است که اولین‌بار توسط لاگرانژ پیدا شده است. این دستور به‌نام دستور درونیابی لاگرانژ مشهور است زیرا وقتی که $F=\mathbf{R}$ این دستور شخص را قادر می‌سازد که مقادیر یك تابع بین مقادیرمفروض c_i درنقاط t_i را درونیابی کند. واضح است که چندجمله‌ای $a(X)$ حداکثر دارای درجهٔ $n-1$ است و بنابراین تنها چندجمله‌ای با این خاصیت است.

توسیع $\mathbf{Z}$ به‌میدان کسرهایش $\mathbf{Q}$ ساختمانی است که برای هرحوزهٔ صحیح به‌کارمی‌آید (قضیهٔ ۸خ) . درحالت خاص، اگر D یك حوزهٔ صحیح باشد، بنابه‌قضیهٔ ۱۰آ، $D[X]$ هم‌یك حوزهٔ صحیح است، و بنابراین $D[X]$ دارای یك میدان کسرهاست. جالبترین حالت وقتی است که $D=F$ میدان باشد، و ما میدان کسرهای $F[X]$ را با $F(X)$ نشان می‌دهیم . عضوهایش کسرهای $a(X)/b(X)$ هستند ، که درآن $a(X)$ و $b(X)$ چندجمله‌ای هستند و $b(X)\neq 0$. چنین کسرهایی توابع گویا نامیده می‌شوند، نام خیلی بی‌مسمایی است زیرا آنها ابداً تابع نیستند، گرچه می‌توانند مانند حالت‌چندجمله‌ایها برای تعیین توابع به‌کار روند. «صورتهای گویا» نام بهتری خواهد بود. دوکسر

$$\frac{a_1(X)}{b_1(X)} \quad \text{و} \quad \frac{a_2(X)}{b_2(X)}$$

در $F(X)$ باهم برابرند اگروفقط اگر در $F[X]$ داشته باشیم $a_1(X)b_2(X)=b_1(X)a_2(X)$. به‌این دلیل عوامل مشترك صورت ومخرج می‌توانند حذف شوند. چنانچه هردوی صورت و مخرج را به‌صورت حاصلضربی از یکه‌ها و چندجمله‌ایهای تکین تحویل‌ناپذیر بیان‌کنیم، ودرصورت ممکن‌حذف‌نماییم، می‌بینیم که هرعنصر $F[X]$ می‌تواند به‌طوریکتایی به‌صورت $up_1(X)^{\alpha_1}p_2(X)^{\alpha_2}\dots p_n(X)^{\alpha_n}$ بیان‌شود، که‌درآن u یك یکه و $p_1(X)$، $p_2(X)$، ...، $p_n(X)$ چندجمله‌ایهای تکین‌تحویل‌ناپذیرند و $\alpha_i\in\mathbf{Z}$ ، $\alpha_i\neq 0$. البته، دراینجا به‌لحاظ‌مخرج، α_i می‌تواند منفی باشد. تمرین خوبی است که یکتایی این تجزیه در $F(X)$ از قضیهٔ یکتایی تجزیه معروف در $F[X]$ استنتاج شود.

احکام‌مربوط به‌کسرهای‌جزئی که برای $\mathbf{Q}$ درفصل۹ شرح‌داده شد در $F(X)$ هم برقرار است. (براستی شاید دراین زمینه، به‌سبب کاربردش درانتگرالگیری توابع گویا بایك‌متغیر حقیقی برایمان‌آشناتر باشد.) اکنون مرور مجدد همان استدلال بی‌موردخواهد بود، از اینرو بسادگی نتیجهٔ اصلی را بیان می‌کنیم وبه‌خواننده توصیه می‌کنیم که برهان‌آن‌را بیاورد (درصورت امکان بدون مراجعه به‌فصل۹) .

قضیهٔ ۱۰ز. فرض‌کنید F یك میدان باشد. دراین‌صورت هرعنصر غیر صفر ازمیدان توابع گویای $F(X)$ می‌تواندبه‌طور یکتا به‌صورت زیر بیان شود

$$a(X)+\frac{b_1(X)}{p_1(X)^{\alpha_1}}+\frac{b_2(X)}{p_2(X)^{\alpha_2}}+\cdots+\frac{b_n(X)}{p_n(X)^{\alpha_n}},$$

که در آن $a(X)$ ، $b_i(X)$ ، $p_i(X)$ چند جمله‌ایهایی در $F[X]$ هستند، $p_1(X)$ ، $p_2(X)$ ، ... ، $p_n(X)$ چند جمله‌ایهای تکین تحویل‌ناپذیرند (الزاماً متمایز نیستند) ، α_1 ، α_2 ، ... ، α_n اعداد صحیح مثبت‌اند ، $p_1(X)^{\alpha_1}$ ، $p_2(X)^{\alpha_2}$ ، ... ، $p_n(X)^{\alpha_n}$ متمایزند ، و به‌ازاء n ، ... ، ۲ ، ۱ $= i$ ، $\deg(b_i(X))<\deg(p_i(X))$.

تمرینها

۱. الگوریتم اقلیدس را برای پیدا کردن بزرگترین مقسوم‌علیه مشترک

$$X^5-2X^3+X^2-3X+1$$

و

$$X^4-2X^3-3X^2+7X-2$$

در $\mathbf{R}[X]$ به‌کار ببرید.

۲. بزرگترین مقسوم‌علیه مشترک $X^{12}+1$ و X^9+1 را در $\mathbf{Z}_3[X]$ و در $\mathbf{Z}_7[X]$ پیدا کنید.

۳. بزرگترین مقسوم‌علیه مشترک $X^{72}-1$ و $X^{45}-1$ را در $\mathbf{Q}[X]$ پیدا کنید، و آن‌را به‌صورت $p(X)(X^{72}-1)+q(X)(X^{45}-1)$ بیان کنید.

۴. ثابت کنید که اگر چندجمله‌ای $f(X)\in F[X]$ بادرجهٔ ۳ دارای هیچ ریشه‌ای در F نباشد آنگاه تحویل‌ناپذیر است. مثالی بیاورید و نشان دهید که این مطلب برای چندجمله‌ایهای درجهٔ ۴ درست نیست. (F یك میدان است.)

۵. ثابت کنید که اگر $a(X)$ ، $b(X)\in F[X]$ وچنانچه F زیرمیدانی ازیك میدان F' باشد، آنگاه بزرگترین مقسوم‌علیه مشترک $a(X)$ و $b(X)$ در $F[X]$ برابر است با بزرگترین مقسوم‌علیه مشترکشان در $F'[X]$. (توجه کنید: این مطلب جوابهای تمرین ۲ فوق را نقض نمی‌کند زیرا نه $\mathbf{Z}_2$ زیر میدانی است از $\mathbf{Z}_3$ و نه $\mathbf{Z}_3$ زیر میدانی از $\mathbf{Z}_2$.)

۶. فرض کنید F یك میدان باشد و J مجموعهٔ همهٔ چند جمله‌ایهای $a(X)\in F[X]$ به‌قسمی که به‌ازاء هر $x\in F$ ، $a(x)=0$. ثابت کنید که J ایده‌آلی از $F[X]$ است و مولدی برای آن پیدا کنید (الف) درصورتی که $F=\mathbf{R}$ ، (ب) درصورتی که $F=\mathbf{Z}_3$. (توجه کنید که بنا به قضیهٔ ۱۰ت ، J یك ایده‌آل اصلی است.)

۷. چندجمله‌ای $a(X)\in F[X]$ با درجهٔ کوچکتر یا مساوی ۳ به‌قسمی پیدا کنید که $a(0)=3$ ، $a(-1)=0$ ، $a(1)=-2$ ، $a(2)=1$ وقتی که (الف) $F=\mathbf{Q}$ و (ب) $F=\mathbf{Z}_7$.

۸. نشان دهید که چندجمله‌ایهای X^3+2 و X^2-X در $\mathbf{R}[X]$ متباین‌اند، و یك

چندجمله‌ای حقیقی $p(X)$ به‌قسمی پیدا کنید که

$$p(X)\equiv X-1 \qquad (X^3+2 \text{ به پیمانهٔ})$$

$$p(X)\equiv 2X \qquad (X^2-X \text{ به پیمانهٔ}) .$$

اگر چندجمله‌ایهای X^3+2 و X^2-X به‌عنوان عناصر $\mathbf{Z}_2[X]$ درنظر گرفته‌شوند، آیا درآن‌صورت متباین‌اند؟ آیا یك‌چندجمله‌ای $p(X)\in\mathbf{Z}_2[X]$ وجود دارد که در دستگاه همنهشتیهای مفروض‌صدق کند؟

۹. فرض کنید F یك میدان باشد و $q(X)\in F[X]$ ، $p(X)$ ، که

$$\deg(q(X))<\deg(p(X)) .$$

ثابت کنید که‌چندجمله‌ایهای $p_0(X)$ ، $p_1(X)$ ، ... ، $p_k(X)$ هریك‌بادرجهٔ کمتر از $\deg(q(X))$ به‌قسمی وجود دارند که

$$p(X)=p_0(X)+p_1(X)q(X)+p_2(X)(q(X))^2+\cdots+p_k(X)(q(X))^k$$

نشان‌دهید که چندجمله‌ایهای $p_i(X)$ یکتا هستند.

۱۰. فرض کنید $r(X)=p(X)/[a(X)b(X)]$ درمیدان‌توابع گویای $F(X)$ باشد، که F یك میدان است . فرض کنید $a(X)$ و $b(X)$ چندجمله‌ایهای متباین باشند و $\deg(p(X))<\deg(a(X))+\deg(b(X))$. ثابت کنید که $r(X)$ می‌تواند به‌صورت زیر نوشته شود

$$r(X)=\frac{c(X)}{a(X)}+\frac{d(X)}{b(X)} ,$$

که درآن $c(X)$ و $d(X)$ چندجمله‌ایهایی‌هستند با $\deg(c(X))<\deg(a(X))$ و $\deg(d(X))<\deg(b(X))$.

۱۱. فرض کنید $p(X)=p_0+p_1X+\cdots+p_nX^n$ که درآن $p_i\in\mathbf{Z}$ و $p_n\neq 0$. ثابت کنید که اگر $p(t)=0$ ، که درآن $t\in\mathbf{Q}$ ، آنگاه $t=r/s$ ، که $s\in\mathbf{Z}$ ، r و $r|p_0$ ، $s|p_n$.

۱۲. فرض کنید p یك عدد اول باشد. ثابت کنید که در $\mathbf{Z}_p[X]$ ، $(1+X)^p=1+X^p$ و استنتاج کنید که

$$(1+X)^{p-1}=1-X+X^2-\cdots+(-1)^{p-1}X^{p-1} .$$

بنابراین نشان‌دهید که به‌ازاء $i=1,2,\ldots,p-1$ ،

$$p\left|\binom{p}{i}\right.$$

و به‌ازاء $i=0,1,2,\ldots,p-1$ ،

$$\binom{p-1}{i}\equiv(-1)^i \qquad (p \text{ به پیمانهٔ}).$$

۱۳. ثابت کنید که حاصلضرب همهٔ عناصر یك گروه آبلی ضربی برابر است با حاصلضرب تمام عناصر بامرتبهٔ ۲. نشان دهید که گروه ضربی میدان $\mathbf{Z}_p$ (p یك عدد اول فرد) دقیقاً دارای یك عنصر بامرتبهٔ ۲ است وقضیهٔ ویلسون را نتیجه بگیرید:

$$(p-1)! \equiv -1 \qquad (\text{به پیمانهٔ } p).$$

۱۴. ثابت کنید که اگر p یك عدد اول بزرگتر یا مساوی ۳ باشد، آنگاه

$$\sum_{k=1}^{p-1} k^3 \equiv 0 \qquad (\text{به پیمانهٔ } p).$$

(راهنمایی: مجموع مکعبات ریشه‌های یك چندجمله‌ای می‌توانند برحسب ضرایب بیان شوند.)

۱۵. ثابت کنید که به‌ازاء هرعددصحیح n وهرعدد اول p ،

$$\sum_{k=1}^{p-1} n^k \equiv 0 \text{ یا } -1 \qquad (\text{به پیمانهٔ } p).$$

۱۶. ثابت کنید که اگر 2^n+1 عددی اول باشد آنگاه n توانی از ۲ است. (راهنمایی: تجزیه‌های چندجمله‌ای X^n+1 را درنظر بگیرید.)

۱۷. ثابت کنید که اگر p عدد اول فردی باشد آنگاه در $\mathbf{Z}_p$ دقیقاً $(p-1)/2$ عنصر وجود دارد که هریك مجذور عنصر غیرصفری از $\mathbf{Z}_p$ هستند. نشان دهید که این مجذورها، ریشه‌های چندجمله‌ای $X^{(p-1)/2}-1$ در $\mathbf{Z}_p$ هستندوعناصرغیرمجذور در $\mathbf{Z}_p$ ریشه‌های $X^{(p-1)/2}+1$ می‌باشند. نتیجه بگیرید که همنهشتی

$$x^2 \equiv -1 \qquad (\text{به پیمانهٔ } p),$$

که درآن p اول است، دارای جواب است اگر و فقط اگر (به پیمانهٔ ۴) $p \equiv 1$ یا $p=2$.

فصل ۱۱

چندجمله‌ایها روی Z و Q ، R ، C

تجزیهٔ یك چند جمله‌ای $a(X)\in F[X]$ به عوامل تحویل ناپذیر در صورتی کـه به میدان بزرگتری مانند F' برویم وعوامل تحویل‌ناپذیـر در $F'[X]$ را جستجوکنیم ممکن است تغییر نماید. ارتباط بین این دوتجزیه بسادگی توصیف می‌شود.

قضیهٔ ۱۱ آ. فرض‌کنید F زیر میدانی از میدان F' باشد.

(الف) اگرچندجمله‌ای $p(X)\in F[X]$ در $F'[X]$ تحویل‌ناپذیرباشد آنگاه در $F[X]$ نیز تحویل‌نـاپذیر است.

(ب) اگر چندجمله‌ای $a(X)\in F[X]$ دارای تجزیهٔ تحویل‌ناپذیر

$$a(X)=up_1(X)p_2(X)\cdots p_n(X)$$

در $F'[X]$ باشد و اگر ضرایب هر $p_i(X)$ در F باشند آنگاه این تجزیهٔ $a(X)$ ، در $F[X]$ نیز تحویل ناپذیراست.

(پ) (حالتِ عمومی) . فـرض کنید $a(X)\in F[X]$ دارای تجزیهٔ تحـویل ناپذیر $a(X)=vq_1(X)q_2(X)\cdots q_m(X)$ در $F[X]$ باشد. در ایـن صورت تجزیهٔ تحویل‌ناپذیر $a(X)$ در $F'[X]$ می‌تواند به‌وسیلهٔ تجزیهٔ هر $q_i(X)$ به‌صورت حاصلضربی ازچندجمله‌ایهای تحویل‌ناپذیـر در $F'[X]$ به دست آید. بعکس ، اگـر $a(X)$ دارای تجزیهٔ تحویل ناپذیر $a(X)=up_1(X)p_2(X)\cdots p_n(X)$ در $F'[X]$ باشد وچنانچه هر $p_i(X)$ تکین باشد ، آنگاه‌تجزیهٔ تحویل ناپذیر $a(X)$ در $F[X]$ به‌صورت $uq_1(X)q_2(X)\cdots q_m(X)$ است، که پس‌از نام‌گذاری مناسب مجدد p_1 ، p_2 ، ... ، p_n، داریم:

$$q_1(X)=p_1(X)p_2(X)\cdots p_i(X)\,,$$
$$q_2(X)=p_{i+1}(X)p_{i+2}(X)\cdots p_j(X)\,,$$
$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$
$$q_m(X)=p_{k+1}(X)p_{k+2}(X)\cdots p_n(X)\,.$$

برهان. (الف) واضح است، و (ب) بسادگی نتیجه می‌شود زیرا اگر ضرایب p_i در F باشند در $F[X]$ تحویل‌ناپذیرند، و یکهٔ u نیز بایستی در F باشد. (پ) واضح است که، اگرهر q_i را به‌صورت حاصلضربی از عوامل تحویل‌ناپذیر در $F'[X]$ بیان کنیم آنگاه تجزیهٔ مطلوب در $F'[X]$ را به‌دست می‌آوریم زیرا یکهٔ v از $F[X]$ در $F'[X]$ یکه باقی می‌ماند. برای اثبات عکس این حالت، فرض کنید $a(X)=up_1(X)\cdots p_n(X)$ در $F'[X]$ باشد، که در آن $p_i(X)$ ها تکین و تحویل‌ناپذیرند. در این صورت یکهٔ u و p_i به طور یکتا معین می‌شوند (صرف‌نظر از جایگشتی از عاملها). واضح است که $u\in F$، زیرا ضریب پیشروی $a(X)$ است. اگر اکنون این تجزیه را با تجزیهٔ تحویل‌ناپذیر

$$a(X)=vq_1(X)\cdots q_m(X)$$

در $F[X]$ که در آن q_jها تکین‌اند، مقایسه کنیم، آنگاه بلافاصله درمی‌یابیم که $v=u$. بعلاوه، اگرهر q_j را به‌صورت حاصلضربی از چندجمله‌ایهای تکین تحویل‌ناپذیر در $F'[X]$ بیان کنیم (که این امر امکان‌پذیر است زیرا q_j تکین است)، می‌بایستی به‌موجب یکتایی تجزیه در $F'[X]$، دقیقاً عوامل $p_1(X)$، ...، $p_n(X)$ را ــ باترتیبی ــ به‌دست آوریم. بنابراین q_jها همان‌طور که ذکر شد با دسته‌بندی p_i ها به‌دست می‌آیند.

قضیهٔ ۱۱ ب. فرض کنید F زیر میدانی از F' باشد و $a(X)$، $b(X)\in F[X]$. اگر در $F'[X]$، $a(X)|b(X)$، آنگاه $a(X)|b(X)$ در $F[X]$.

برهان. اگر $a(X)=0$، نتیجه بدیهی است. در غیر این صورت، طبق خاصیت اقلیدسی $F[X]$، داریم $b(X)=a(X)q(X)+r(X)$، که در آن $q(X)$، $r(X)\in F[X]$ و $\deg(r(X))<\deg(a(X))$. همهٔ این چندجمله‌ایها در $F'[X]$ قرار دارند، و در $F'[X]$، $a(X)|b(X)$. نتیجه می‌شود که در $F'[X]$، $a(X)|r(X)$. اما $\deg(r(X))<\deg(a(X))$، ازاینرو $r(X)$، بنابه قضیهٔ ۱۰ آ، باید چند جمله‌ای صفر باشد. بنابراین همان‌طور که ادعا شده است، $b(X)=a(X)q(X)$، که در آن $q(X)\in F[X]$.

این قضیه‌ها را برای مقایسهٔ تجزیه‌ها در $\mathbf{R}[X]$ و $\mathbf{C}[X]$ به کار می‌بریم. به‌وضوح با عدم تعریفی دقیق از $\mathbf{R}$ و $\mathbf{C}$ مطالب زیادی در مورد آنها نمی‌توانیم ثابت کنیم، ازاینرو فرض می‌کنیم (الف) که $\mathbf{C}$ میدانی است بازیر میدانهای $\mathbf{Q}\subset\mathbf{R}$ و (ب) هرعنصر $\mathbf{C}$ به‌طور یکتا به‌صورت $a+bi$ است، با a، $b\in\mathbf{R}$، که در آن i عنصر ثابتی از $\mathbf{C}$ است به قسمی که $i^2=-1$.

شرح کاملی از این میدانها را می‌توان در کتاب بیرکف[1] و مك‌لین[2] [۱] پیدا کرد. همچنین حقیقت‌خیلی عمیقتر زیر دربارهٔ C را که مبنای تجزیه در $C[X]$ است، دانسته فرض می‌کنیم.

قضیهٔ اساسی جبر. هرچندجمله‌ای در $C[X]$ که درجه‌اش حداقل یك باشد دارای یك ریشه در C است.

برای اثبات این قضیه دومشی اصلی موجود است. اولین مشی نظریهٔ توابع تحلیلی یك متغیرهٔ مختلط را به‌کار می‌برد. این، نظریهٔ فوق‌العاده زیبایی است که، در مرحله‌ای، کلیهٔ دانشجویان ریاضی باید آن را مطالعه نمایند، ولی پرداختن به چنین برهانی بتنهایی قابل استفاده نخواهد بود. صورت ساده شدهٔ چنین برهانی را، بدون جزئیات تحلیلی، می‌توان در کتاب قابل تحسین بیرکف و مك‌لین [۱] پیدا کرد. دومین مشی به‌کاربردن این حقیقت است که چندجمله‌ایهای با درجهٔ فرد در $R[X]$ همیشه دارای حداقل یك ریشه در R هستند. این حقیقت به‌طور شهودی روشنتر است و می‌توان آن‌را فقط با به‌کاربردن مقدار کمی آنالیز حقیقی ثابت کرد. آنگاه مرحلهٔ R به C را می‌توان به‌طریق جبری محض انجام داد. (برای مثال، کتاب واندر واردن[3] جلد ۱ [۷] را ببینید).

قضیهٔ ۱۱ پ. هرچندجمله‌ای تحویل‌ناپذیر در $C[X]$ دارای درجهٔ ۱ است. بنابراین هر چندجمله‌ای غیرصفر $a(X)\in C[X]$ دارای تجزیه‌ای به صورت

$$a(X)=u(X-t_1)(X-t_2)\cdots(X-t_n)\,,$$

است که در آن $t_n\in C$ ، $\ldots$ ، t_2 ، t_1 ، u ، $u\neq 0$ و $n\geqslant 0$.

برهان. فرض کنید $p(X)\in C[X]$ تحویل‌ناپذیر باشد. بنا به تعریف، $\deg(p(X))\geqslant 1$، از اینرو بنا به قضیهٔ اساسی، $p(X)$ دارای یك ریشه در C است، مثلا t . $p(t)=0$. بنا به قضیهٔ عامل (نتیجهٔ ۳ قضیهٔ ۱۰خ) ، $(X-t)\mid p(X)$ ، و چون $p(X)$ تحویل‌ناپذیر است نتیجه‌می‌شود که به‌ازاء یکه‌ای‌چون u ، $p(X)=u(X-t)$. بنابراین $\deg(p(X))=1$. اکنون بقیهٔ اثبات ازقضیهٔ یکتایی تجزیه (قضیهٔ ۱۰ ح) نتیجه می‌شود.

متأسفانه، دانستن اینکه یك چند جمله‌ای دارای تجزیه‌ای باعوامل خطی است کمکی به پیدا نمودن عاملها نمی‌کند. در واقع، در حالت کلی هیچ امکانی برای پیدا کردن آنها با روشی دقیق وجود ندارد. بهترین امیدی که می‌توان داشت الگوریتمی است که تقریبهای نزدیك ونزدیکتر به‌ریشه‌های یك‌چندجمله‌ای مفروض را به‌دست‌می‌دهد. چنین‌الگوریتمهایی موجودند ولی انجام‌آنها بادست، کار پرزحمتی است. بهرحال، دانش‌نظری وجودتجزیه‌ای خطی بتنهایی با اهمیت است واکنون نتایجش را برای چندجمله‌ایهای حقیقی موردبررسی قرار می‌دهیم.

---

1. G. Birkhoff 2. S. MacLane 3. B. L. Vander Waerden

اگر $c=a+bi$ عددی مختلط باشد $(a\,,\,b\in\mathbf{R})$ آنگاه مزدوج مختلط c عددمختلط $\overline{c}=a-bi$ است. مزدوجها در قوانین زیر که بسادگی اثبات می‌شوند، صدق می کنند:

(الف) به ازاء هر $c_1\,,\,c_2\in\mathbf{C}$ ، $\overline{c_1+c_2}=\overline{c}_1+\overline{c}_2$ ،

(ب) به‌ازاء هر $c_1\,,\,c_2\in\mathbf{C}$ ، $\overline{c_1c_2}=\overline{c}_1\overline{c}_2$ ،

(پ) $\overline{c}=c\Longleftrightarrow c\in\mathbf{R}$ ،

(ت) به ازاء هر $c\in\mathbf{C}$ ، $\overline{\overline{c}}=c$.

عبارتهای (الف) و (ب) ، همراه با این حقیقت که $\overline{1}=1$ ، بیان‌می کنند که نگاشت $c\longmapsto\overline{c}$ از $\mathbf{C}$ به $\mathbf{C}$ یك‌همریختی‌حلقه‌هاست. این‌نگاشت، بنا به‌قسمت (ت) نگاشتی‌دوسویی است (در واقع ، معکوس خودش است). بنا براین یك یکریختی از $\mathbf{C}$ به خودش می‌باشد. (چنین یکریختی یك خود ریختی $\mathbf{C}$ نامیده می‌شود .)

قضیهٔ ۱۱ ت. فرض کنید $a(X)\in\mathbf{R}[X]$ و x یك ریشهٔ $a(X)$ در $\mathbf{C}$ باشد . در این صورت $\overline{x}$ نیز یك ریشهٔ $a(X)$ در $\mathbf{C}$ است.

برهان . برای هرچند جمله‌ای $p(X)\in\mathbf{C}[X]$ ، مثلا $p(X)=\sum p_iX^i$ ، می‌نویسیم $\overline{p}(X)=\sum\overline{p}_iX^i$. چون $c\longmapsto\overline{c}$ یك خودریختی است، به ازاء هرعدد مختلط x، داریم $\overline{(x^i)}=(\overline{x})^i$ ، $\overline{p_ix^i}=\overline{p}_i\overline{x}^i$ ، و از اینرو $\overline{p(x)}=\overline{p}(\overline{x})$. بخصوص،اگر $a(X)\in\mathbf{R}[X]$ داریم $a(\overline{X})=a(\overline{x})$. بنابراین اگر $a(x)=0$ نتیجه می‌شود که $a(\overline{x})=0$.

نتیجهٔ ۱. هر چند جمله‌ای تحویل‌ناپذیر در $\mathbf{R}[X]$ یا با درجهٔ ۱ است یا به صورت aX^2+bX+c است، که در آن $a\,,\,b\,,\,c\in\mathbf{R}$ ، و $b^2<4ac$. بعکس ، همهٔ چنین چند‌جمله‌ایها تحویل ناپذیرند.

برهان. فرض کنید $p(X)\in\mathbf{R}[X]$ تحویل‌ناپذیر باشد، دراین صورت $\deg(p(X))\geqslant 1$، ازاینرو $x\in\mathbf{C}$ وجود دارد به قسمی که $p(x)=0$ (به‌موجب قضیهٔ اساسی) . اگر $x\in\mathbf{R}$ ، آنگاه، بنا به‌قضیهٔ‌عامل، در $\mathbf{R}[X]$ داریم $(X-x)\,|\,p(X)$، ازاینرو $p(X)=u\cdot(X-x)$ که درآن u یکه‌ای در $\mathbf{R}[X]$ است (زیرا $p(X)$ تحویل‌ناپذیر است) . بنابراین در این حالت ، $p(X)$ دارای درجهٔ ۱ است . از طرف دیگر ، اگر $x\notin\mathbf{R}$ ، آنگاه $\overline{x}\neq x$ و $p(\overline{x})=0$. ازقضیهٔ‌عامل نتیجه‌می‌شود که $(X-x)\,|\,p(X)$ و در $\mathbf{C}[X]$، $(X-\overline{x})\,|\,p(X)$. بنابراین در $\mathbf{C}[X]$ ، داریم $(X-x)(X-\overline{x})\,|\,p(X)$ ، زیرا $(X-x)$ و $(X-\overline{x})$ متباین‌اند. حال داریم

$$(X-x)(X-\bar{x})=X^{2}-(x+\bar{x})X+x\bar{x},$$

و اگر $x=s+ti$ آنگاه $x+\bar{x}=2s$ و $x\bar{x}=s^{2}+t^{2}$ هردو حقیقی‌اند. از اینرو در $\mathbf{C}[X]$ چند جمله‌ای $p(X)$ بریك چند جمله‌ای با درجهٔ ۲ و ضرایب حقیقی قابل قسمت است. بنابه قضیهٔ ۱۱ ب ، $p(X)$ هنوز در $\mathbf{R}[X]$ براین چند جمله‌ای قابل قسمت است و بنابراین دارای درجهٔ ۲ است زیرا در $\mathbf{R}[X]$ تحویل‌ناپذیر است. پس

$$p(X)=a(X^{2}-2sX+(s^{2}+t^{2})),$$

که درآن $t\in\mathbf{R}$ ، s ، a و $a\neq 0$. اگر برای ضرایب X^{1} و X^{0} بنویسیم : $b=-2as$ و $c=a(s^{2}+t^{2})$، داریم

$$b^{2}-4ac=4a^{2}s^{2}-4a^{2}(s^{2}+t^{2})=-4a^{2}t^{2}<0.$$

بعکس ، همهٔ چند جمله‌ایها با درجهٔ ۱ به‌طور روشن تحویل ناپذیرند. اگر

$$p(X)=aX^{2}+bX+c \text{ و } b^{2}<4ac,$$

آنگاه $p(X)$ نیز تحویل‌ناپذیر است ، زیرا درغیراین‌صورت حاصلضربی از دوعامل درجهٔ ۱ خواهد بود وبنابراین دارای یك ریشهٔ $t\in\mathbf{R}$ است؛ ولی $at^{2}+bt+c=0$ نتیجه می‌دهد

$$b^{2}-4ac=b^{2}+4a(at^{2}+bt)=(2at+b)^{2}\geqslant 0,$$

که یك تناقض است.

نتیجهٔ ۲. هرچندجمله‌ای بادرجهٔ‌بزرگتریامساوی ۱ وضرایب حقیقی، دارای تجزیه‌ای به‌صورت حاصلضرب چند جمله‌ایهای درجهٔ ۱ یا ۲ با ضرایب حقیقی است .

برهان. این مطلب از نتیجهٔ ۱ و قضیهٔ یکتایی تجزیه به‌دست می‌آید .

مثال ۱۰۱۱. چندجمله‌ای $a(X)=X^{n}-1$ در $\mathbf{R}[X]$ را درنظر بگیرید. می‌دانیم که $a(X)$ دارای n ریشهٔ متمایز در $\mathbf{C}$ است، یعنی ۱ ، ζ ، ζ^{2} ، ... ، ζ^{n-1} ، که $\zeta=e^{2\pi i/n}$. همهٔ اینها متمایزند، وبنابراین بـه‌موجب نتیجهٔ ۴ قضیهٔ ۱۰د ، داریم

$$X^{n}-1=(X-1)(X-\zeta)(X-\zeta^{2})\cdots(X-\zeta^{n-1}),$$

ریشهٔ ۱ حقیقی است ، وهمچنین اگر n زوج باشد ریشهٔ $\zeta^{n/2}=-1$ نیز حقیقی است. به موجب قضیهٔ ۱۱ ت ، ریشه‌های دیگر به‌صورت جفتهای مزدوج ظاهر می‌شوند که هرجفت یك چند جمله‌ای تحویل‌ناپذیر در $\mathbf{R}[X]$ به دست می‌دهد. اگر $n=2m$ زوج باشد ، جفتهای‌مزدوج عبارت‌اند از : ζ^{r} و $\zeta^{n-r}=\zeta^{-r}$ به‌ازاء $r=1,2,\ldots,m-1$. عوامل درجهٔ دوم متناظر عبارت‌اند از $(X-\zeta^{r})(X-\zeta^{-r})=X^{2}-(2\cos 2\pi r/n)X+1$ ، از اینرو تجزیهٔ تحویل‌ناپذیر $(X^{n}-1)$ در $\mathbf{R}[X]$ عبارت است از:

$$X^n-1=(X-1)(X+1)\prod_{r=1}^{m-1}\left(X^2-\left(2\cos\frac{2\pi r}{n}\right)X+1\right).$$

به همین‌نحو، اگر $n=2m-1$ فرد باشد، داریم

$$X^n-1=(X-1)\prod_{r=1}^{m-1}\left(X^2-\left(2\cos\frac{2\pi r}{n}\right)X+1\right).$$

تجزیه در $\mathbf{Q}[X]$ مشکلتر است. البته، گاهی اتفاق می‌افتد که عوامل تحویل‌ناپذیر یك چندجمله‌ای $a(X)\in\mathbf{Q}[X]$ در $\mathbf{R}[X]$ همه دارای ضرایبی در $\mathbf{Q}$ باشند، که در این حالت آنها عوامل تحویل‌ناپذیر در $\mathbf{Q}[X]$ نیز هستند (قضیهٔ ۱۱ آ). درغیراین صورت به‌سختی می‌توان گفت که آیا یك چند جمله‌ای در $\mathbf{Q}[X]$ تحویل‌ناپذیر است یا خیر. ممکن است امتحان کرد که آیا $a(X)\in\mathbf{Q}[X]$ دارای ریشه‌ای در $\mathbf{Q}$ هست یا نه و همهٔ این چنین ریشه‌ها را پیدا کرد؛ اما این فقط مسئلهٔ تحویل‌ناپذیری چند جمله‌ایها را تا درجهٔ ۳ فیصله می‌دهد، ولی همان‌طور که در آینده خواهیم دید، $\mathbf{Q}[X]$ شامل چندجمله‌ایهای تحویل‌ناپذیر از هردرجهٔ دلخواهی هست. بهترین روش پرداختن به حل مسئله تحویل آن به مسئلهٔ تجزیه در $\mathbf{Z}[X]$ است، وچون $\mathbf{Z}$ میدان نیست مجبوریم با احتیاط عمل کنیم.

تحویل‌ناپذیری در $\mathbf{Z}[X]$ دقیقاً همانند قبل تعریف می‌شود: $p(X)\neq 0$ تحویل‌ناپذیر است چنانکه یکه‌ای در $\mathbf{Z}[X]$ نباشد و تنها مقسوم علیه‌هایش به صورت u یا $up(X)$ باشند که u یك یکه است. اما یکه‌ها در $\mathbf{Z}[X]$ درست همان یکه‌های $\mathbf{Z}$ هستند، یعنی ۱ و ۱ —، ازاینرو اکنون پدیدهٔ جدیدی داریم — هرعدد اول در $\mathbf{Z}$ چند جمله‌ای تحویل‌ناپذیری با درجهٔ صفر در $\mathbf{Z}[X]$ است. مشکل دیگر در $\mathbf{Z}[X]$ آن است که، هر چند جمله‌ای حاصلضرب یك یکه ویك چند جمله‌ای تکین نیست. بنابراین باید هنگام مقایسهٔ تجزیه‌ها در $\mathbf{Z}[X]$ و $\mathbf{Q}[X]$ دقت کرد.

در بررسی تجزیه در $\mathbf{Z}[X]$ «تحویل به‌پیمانهٔ p» تدبیر کاملا مفیدی است. عدد اول p را ثابت‌اختیار می‌کنیم و نگاشت خارج قسمت $\sigma:\mathbf{Z}\longrightarrow\mathbf{Z}_p$ را درنظر می‌گیریم. این σ همریختی حلقه‌هاست، ازاینرو به‌طور یکتایی به یك همریختی از $\mathbf{Z}[X]$ به $\mathbf{Z}_p[X]$ که X را به X می‌برد، توسعه می‌یابد (به موجب قضیهٔ ۱۰ خ). این همریختی با ضابطهٔ $\sum a_iX^i\longrightarrow\sum\sigma(a_i)X^i$ داده می‌شود و به‌وضوح بروی است. دراین صورت داریم:

قضیهٔ ۱۱ث. فرض کنید $p\in\mathbf{Z}$ اول باشد و، به‌ازاء هر $a(X)\in\mathbf{Z}[X]$، فرض کنید $a^*(X)$ چند جمله‌ای باشد که ضرایبش رده‌های باقیماندهٔ به‌پیمانهٔ p ضرایب متناظر $a(X)$ باشد. در این صورت نگاشت $a(X)\longrightarrow a^*(X)$ یك همریختی حلقه‌ای از $\mathbf{Z}[X]$ بروی $\mathbf{Z}_p[X]$ است.

چندجمله‌ای $a(X)=\sum a_iX^i$ در $\mathbf{Z}[X]$ مفروض است، بزرگترین مقسوم‌علیه مشترك همهٔ ضرایب $a(X)$ در $\mathbf{Z}$ را محتوای $a(X)$ تعریف می‌کنیم. ب. م. م. a_1، a_2، ...، a_n به طریق استقرایی به صورت

$$d=(\dots((a_1,a_2),a_3),\dots,a_n)$$

تعریف می‌شود. بسادگی دیده می‌شود که d به وسیلهٔ خاصیتهای زیر مشخص می‌گردد:

(الف) در $\mathbf{Z}$ به ازاء $i=0,1,2,\dots,n$ ، $d|a_i$ ؛

(ب) اگر در $\mathbf{Z}$ به‌ازاء $i=0,1,2,\dots,n$ ، $c|a_i$ آنگاه در $\mathbf{Z}$ $c|d$ ؛

(پ) $d\geqslant 0$.

محتوای $a(X)$ را با $\gamma(a(X))$ نشان می‌دهیم، و ملاحظه می‌کنیم که اگر $\gamma(a(X))=d$، آنگاه $a(X)=d\cdot b(X)$، که در آن $b(X)\in\mathbf{Z}[X]$ و $\gamma(b(X))=1$ (زیرا اگر c، $\gamma(b(X))$، آنگاه تمام ضرایب $a(X)$ بر dc قابل قسمت‌اند). اکنون حکم قاطعی را برای تجزیه در $\mathbf{Z}[X]$ ثابت می کنیم.

قضیهٔ ۱۱ ج. (لم گاوس). فرض کنید $a(X)$ ، $b(X)\in\mathbf{Z}[X]$. در این صورت

$$\gamma\{a(X)b(X)\}=\gamma(a(X))\gamma(b(X)).$$

برهان. اگر یکی از چندجمله‌ایها صفر باشد، محتوایش صفر است، و قضیه به طور بدیهی درست است. ازاینرو فرض کنید $\gamma(a(X))=r>0$ ، $\gamma(b(X))=s>0$. دراین‌صورت $a(X)=r\cdot a_1(X)$ و $b(X)=s\cdot b_1(X)$ ، که $a_1(X)$ و $b_1(X)$ هریك‌دارای‌محتوای ۱ است. بنابراین تمام ضرایب $a(X)b(X)=rs\cdot a_1(X)b_1(X)$ بر rs قابل قسمت‌اند، و کافی است نشان دهیم که $\gamma\{a_1(X)b_1(X)\}=1$. فرض کنید که این درست نباشد؛ در آن صورت عدد اولی مانند p وجود دارد که تمام ضرایب $a_1(X)b_1(X)=c(X)$ را عاد می‌کند. حال اگر ضرایب را (به پیمانهٔ p) برای این عدد اول تحویل کنیم، قضیهٔ ۱۱ ث نتیجه می‌دهد که در $\mathbf{Z}_p[X]$:

$$a_1^*(X)b_1^*(X)=c^*(X)=0 .$$

اما $\mathbf{Z}_p[X]$ حوزهٔ صحیح‌است (قضیهٔ ۱۰ آ) زیرا $\mathbf{Z}_p$ میدان است، ازاینرو نتیجه می گیریم که در $\mathbf{Z}_p[X]$ ، یا $a_1^*(X)=0$ یا $b_1^*(X)=0$. بدین ترتیب در $\mathbf{Z}[X]$ همهٔ ضرایب $a_1(X)$ یا $b_1(X)$ بر p قابل‌قسمت‌اند، که متناقض با این‌حقیقت است که هردوی این‌چندجمله‌ایها دارای محتوای ۱ هستند.

این استدلال مثال خیلی‌خوبی ازسودمندی روش مجرد است. عبارت قضیه فقط اعداد صحیح و چند جمله‌ایها را دربر می گیرد و می‌تواند مستقیماً در $\mathbf{Z}[X]$ اثبات شود، ولی تنها به وسیلهٔ بعضی محاسبات نسبتاً پیچیده برای تحلیل مقتضیاتی که تحت آنها همهٔ‌ضرایب حاصلضرب دوچند جمله‌ای بر عدد اولی قابل قسمت‌اند. لیکن تحویل به پیمانهٔ p ، با استفاده ازاین استدلال که $\mathbf{Z}_p$ میدان است پس $\mathbf{Z}_p[X]$ یك حوزهٔ صحیح است، ما را از این پیچیدگی رها می‌سازد. دراثبات این حقیقت اخیر، که مجدداً مطرح خواهد شد، فقط

از ضرایب پیشروی چندجمله‌ایها استفاده می‌شود، و این همانجایی است که تسهیل مطالب نهفته است. حتی مثال بهتری ازاین فرایند تسهیل به وسیلهٔ تحویل (به پیمانهٔ p)، برهان محك آیزنشتاین است که ذیلا آمده است (قضیهٔ ۱۱ خ).

نتیجه. فرض کنید $a(X), b(X)\in\mathbf{Z}[X]$ و اگر در $\mathbf{Q}[X]$، $a(X)|b(X)$، وچنانچه محتوای $a(X)$ برابر ۱ باشد، آنگاه در $\mathbf{Z}[X]$، $a(X)|b(X)$.

برهان. مطابق فرض داریم: $b(X)=a(X)q(X)$، که در آن $q(X)$ دارای ضرایب گویاست. عددی صحیح و مخالف صفری مانند n به قسمی وجود دارد که $q_1(X)=nq(X)$ دارای ضرایب صحیح است (مثلا، فرض کنید n حاصلضرب مخرجهای ضرایب غیرصفر $q(X)$ باشد). بنابراین در $\mathbf{Z}[X]$، داریم $nb(X)=a(X)q_1(X)$. بنا به لم گاوس،

$$n\gamma(b(X))=\gamma(q_1(X)),\quad \text{زیرا}\quad \gamma(a(X))=1.$$

بنابراین n محتوای $q_1(X)$ را عاد می‌کند و از اینرو

$$q(X)=\frac{1}{n}q_1(X)$$

دارای ضرایب صحیح است. پس در $\mathbf{Z}[X]$، $a(X)|b(X)$.

مثال ۳.۱۱. فرض کنید $b(X)\in\mathbf{Z}[X]$ و $b(X)=b_0+b_1X+\cdots+b_nX^n$. فرض کنید $b(X)$ دارای یك ریشهٔ $t=r/s$ در $\mathbf{Q}$ باشد. در این صورت در $\mathbf{Q}[X]$، $(X-t)|b(X)$، ازاینرو در $\mathbf{Q}[X]$، $(sX-r)|b(X)$. r و s را می‌توانیم طوری انتخاب کنیم که اعداد صحیح متباین باشند که در نتیجه $\gamma(sX-r)=1$. بنا به نتیجهٔ فوق، در $\mathbf{Z}[X]$ داریم $(sX-r)|b(X)$، یعنی

$$b_0+b_1X+\cdots+b_nX^n=(-r+sX)(c_0+c_1X+\cdots+c_{n-1}X^{n-1}),$$

که در آن $c_0, c_1, \ldots, c_{n-1}\in\mathbf{Z}$. با مساوی قراردادن ضرایب X^0 و X^n درمی‌یابیم که $b_0=-rc_0$ و $b_n=sc_{n-1}$ بنابراین در $\mathbf{Z}$، $r|b_0$ و $s|b_n$. چون b_0 و b_n فقط دارای تعداد متناهی مقسوم‌علیه هستند می‌توانیم همهٔ اعداد گویای r/s را که $r|b_0$ و $s|b_n$، امتحان کنیم و ملاحظه کنیم آیا ریشه هستند یا نه ولذا معین کنیم که آیا $b(X)$ هیچ ریشه‌ای در $\mathbf{Q}$ دارد یا خیر. به عنوان مثال، اگر $b(X)=X^2-2$، تنها ریشه‌های ممکن در $\mathbf{Q}$ عبارتند از $t=\pm1, \pm2$. ولی چون هیچکدام ازاینها ریشه نیست، درنتیجه X^2-2 دارای ریشهٔ گویا نمی‌باشد. این برهان که «$\sqrt{2}$ اصم است» ساده‌تر از برهان معمول به نظر می‌آید، ولی این فقط بدان علت است که قبلا کار در اثبات لم گاوس و نتیجه‌اش انجام شده است.

مثال ۳.۱۱. اگر $b(X)=3X^3-2X^2+X-4$، ریشه‌های ممکن $b(X)$ در $\mathbf{Q}$ عبارتند از:

$$t=\pm 1\ ,\ \pm 2\ ,\ \pm 4\ ,\ \pm\frac{1}{3}\ ,\ \pm\frac{2}{3}\ ,\ \pm\frac{4}{3}\ .$$

در واقع هیچ کدام ازاینها در شرط $b(t)=0$ صدق نمی کند ، از اینرو $b(X)$ هیچ ریشه‌ای در $\mathbf{Q}$ ندارد. بنابراین $b(X)$ در $\mathbf{Q}[X]$ تحویل‌ناپذیر است‌زیرا درغیراین‌صورت‌حاصلضرب دو چند جمله‌ای از درجه‌های ۱ و ۲ می‌باشد و لذا یك ریشه در $\mathbf{Q}$ خواهد داشت . $b(X)$ در $\mathbf{Z}[X]$ نیز تحویل‌ناپذیر است زیرا هیچ مقسوم‌علیه $sX-r$ در $\mathbf{Z}[X]$ ندارد و هیچ مقسوم‌علیه از درجهٔ صفر بجز ± 1 ندارد چون محتوایش برابر است با ۱.

قضیهٔ ۱۱ چ. فرض کنید $a(X)\in\mathbf{Z}[X]$ دارای محتوای ۱ باشد. در این صورت $a(X)$ در $\mathbf{Z}[X]$ تحویل‌ناپذیر است اگر وفقط اگر در $\mathbf{Q}[X]$ تحویل ناپذیر باشد.

برهان. ابتدافرض کنید$a(X)$ در$\mathbf{Q}[X]$تحویل ناپذیر باشد.دراین‌صورت$\deg(a(X))\geqslant 1$، ازاینرو $a(X)$ در $\mathbf{Z}[X]$ یکه نیست. اگر $a(X)=b(X)c(X)$ تجزیه‌ای در $\mathbf{Z}[X]$ باشد، آنگاه یك تجزیه در $\mathbf{Q}[X]$ نیزهست ، از اینرو یکی از عاملها ، مثلا $b(X)$ ، در $\mathbf{Q}[X]$ یکه است. چون $b(X)$ دارای ضرایب صحیح است پس عددی است صحیح و بایستی ± 1 باشد زیرا $a(X)$ دارای محتوای ۱ است. بنابراین $a(X)$ در $\mathbf{Z}[X]$ تحویل‌ناپذیر است.

بعکس، فرض کنید $a(X)$ در $\mathbf{Z}[X]$ تحویل‌ناپذیر باشد. $a(X)$ برابر باصفر و ± 1 نیست‌پس‌بایستی‌دارای درجهٔ بزرگتریامساوی۱ باشد، زیرا محتوایش ۱ است. فرض کنیدکه در$\mathbf{Q}[X]$ ، $a(X)=b(X)c(X)$. عددگویایی مانند $r\neq 0$ به قسمی وجود دارد که $b_1(X)=rb(X)$ دارای ضرایب صحیح ومحتوای۱باشد (مضرب صحیحی از $b(X)$ پیدا کنیدکه دارای ضرایب صحیح باشد و سپس برمحتوایش تقسیم کنید). بوضوح در $\mathbf{Q}[X]$ $b_1(X)|a(X)$ وبنابراین، بنابه نتیجهٔ قضیهٔ ۱۱ ج، در $\mathbf{Z}[X]$ داریم $b_1(X)|a(X)$. چون $a(X)$ در$\mathbf{Z}[X]$تحویل‌ناپذیراست،نتیجه‌می‌شودکه$b_1(X)=\pm 1$ یا $b_1(X)=\pm a(X)$. بنابراین $b(X)$ برابر است با $\pm r^{-1}$ یا $\pm r^{-1}a(X)$ و از اینرو $a(X)$ در $\mathbf{Q}[X]$ تحویل ناپذیر است.

نتیجه. فرض‌کنید $a(X)\in\mathbf{Z}[X]$ دارای محتوای n باشد. در این صورت $a(X)$ در $\mathbf{Q}[X]$ تحویل‌ناپذیر است اگر و فقط اگر $n^{-1}a(X)$ در $\mathbf{Z}[X]$ تحویل‌ناپذیر باشد.

قضیهٔ ۱۱ ح . هرچند جمله‌ای غیر صفر $a(X)\in\mathbf{Z}[X]$ دارای تجزیه‌ای به صورت زیر است

$$a(X)=np_1(X)p_2(X)\cdots p_r(X)\ ,$$

که در آن $n\in\mathbf{Z}$ و $p_i(X)$ ها چندجمله‌ایهای تحویل‌ناپذیر در $\mathbf{Z}[X]$ با محتوای ۱ وضرایب پیشروی مثبت هستند. صرفنظر از ترتیب عاملها ، تجزیه یکتاست.

برهان. قضیهٔ ۱۰ ح یك تجزیهٔ $a(X)=u\cdot q_1(X)q_2(X)\cdots q_r(X)$ را در$\mathbf{Q}[X]$ تضمین

می‌کند، که درآن u یک‌عدد گویای غیرصفر است وهـر $q_i(X)$ در $\mathbf{Q}[X]$ تحویل‌ناپذیـر است. به‌ازاء اعداد گویای غیرصفر مناسب r_i ، چندجمله‌ایهای $p_i(X)=r_iq_i(X)$ دارای ضرایب‌صحیح ومحتوای ۱ هستند. درصورت لزوم با تغییر r_i به $-r_i$ ، می‌توان فرض کرد که ضریب پیشروی $p_i(X)$ مثبت است. حال در $\mathbf{Q}[X]$ داریم

$$a(X)=v\cdot p_1(X)p_2(X)\cdots p_r(X)$$

ومی‌خواهیم نشان‌دهیم که عدد گویای v صحیح است. این مطلب ازنتیجهٔ قضیهٔ ۱۱ج به‌دست می‌آید، زیرا $p_1(X)p_2(X)\cdots p_r(X)$ دارای محتوای ۱ است.

یکتایی تجزیه‌بسادگی اثبات می‌شود. ابتدا، n یکتاست زیرا بنابه لم گاوس، برابر است با $\pm\gamma(a(X))$ و علامتش علامت‌ضریب پیشروی $a(X)$ است. سپس‌بنا به‌قضیهٔ ۱۱ج، هر $p_i(X)$ در $\mathbf{Q}[X]$ تحویل‌ناپذیر است. بنابراین، اگر

$$a(X)=np_1'(X)p_2'(X)\cdots p_s'(X)$$

تجزیهٔ دیگری ازنوع مفروض‌باشدآنگاه ، بنابه‌قضیهٔ یکتایی‌تجزیه برای $\mathbf{Q}[X]$ ، $r=s$ و (درصـورت لـزوم پس از انـدیس‌گـذاری مجـدد) در $\mathbf{Q}[X]$ ، $p_i(X)\mid p_i'(X)$ و $p_i'(X)\mid p_i(X)$. چون $p_i(X)$ و $p_i'(X)$ هردو دارای محتوای ۱ اند ، کاربـرد دیگری از نتیجهٔ قضیهٔ ۱۱ج نشان می‌دهد که هـر کدام دیگری را در $\mathbf{Z}[X]$ عاد می‌کند و بنابـراین $p_i(X)=\pm p_i'(X)$. اما هـردو چندجمله‌ای دارای ضریب پیشروی مثبت‌انـد، لذا باهم برابرند، وتجزیه‌یکتاست.

مثال ۴.۱۱. چندجمله‌ای $X^6+1\in\mathbf{Z}[X]$ دارای‌سه‌جفت ریشهٔ مزدوج $\zeta^{\pm1}$ ، $\zeta^{\pm3}$ ، $\zeta^{\pm5}$ در $\mathbf{C}$ است، که $\zeta=e^{2\pi i/12}$. بنابراین‌عوامل‌تحویل‌ناپذیر X^6+1 در $\mathbf{R}[X]$ عبارت‌اند از:

$$(X-\zeta)(X-\zeta^{-1})=X^2-2\cos\frac{\pi}{6}+1\ ,$$

$$(X-\zeta^3)(X-\zeta^{-3})=X^2+1\ ,$$

و

$$(X-\zeta^5)(X-\zeta^{-5})=X^2-2\cos\frac{5\pi}{6}+1\ .$$

بنابه‌قضیهٔ ۱۱آ ، عوامل تحویل‌ناپذیر X^6+1 در $\mathbf{Q}[X]$ به‌وسیلهٔ ترکیب مناسب‌عوامل فوق به‌دست‌می‌آیند.پس‌در $\mathbf{Q}[X]$، $X^6+1=(X^2+1)(X^4-X^2+1)$، ودر $\mathbf{R}[X]$

$$X^4-X^2+1=(X^2-2\cos\frac{\pi}{6}+1)(X^2-2\cos\frac{5\pi}{6}+1)$$

و از اینرو تنها سؤال این‌است‌که آیا $\cos\frac{\pi}{6}$ گویاست یا خیر. اما

$$\cos\frac{\pi}{6}=\frac{\sqrt{3}}{2}$$

یك ریشهٔ چندجمله‌ای $۳ - ۴X^۲$ است که بنا به استدلالی که درمثالهای ۲.۱۱ و ۳.۱۱ به‌کار رفته است، هیچ‌ریشهٔ گویایی ندارد. بنابراین عوامل تحویل‌ناپذیر $۱ + X^۶$ در $\mathbf{Q}[X]$ عبارت‌اند از: $۱ + X^۲$ و $۱ + X^۲ - X^۴$. هردوی اینها در $\mathbf{Z}[X]$ هستند ودارای‌محتوای ۱ اند، ازاینرو آنها عوامل تحویل‌ناپذیر $۱ + X^۶$ در $\mathbf{Z}[X]$ نیز هستند.

اکنون یکی از معدود محکهای شناخته شده برای تحویل‌ناپذیری یك‌چندجمله‌ای را در $\mathbf{Z}[X]$ ثابت می‌کنیم. این شرط کافی، ولی نه‌لازم، برای تحویل‌ناپذیری است، لذامحل به‌اندازهٔ کافی توانا نیست که توسط‌آن‌بتوان درحالت‌کلی تعیین کردکه آیا یك چندجمله‌ای مفروض‌تحویل‌ناپذیر است یاخیر. لیکن، دربرخی ازحالات ویژه‌خیلی‌مفیداست وبخصوص نشان‌می‌دهدکه‌در $\mathbf{Z}[X]$ چندجمله‌ایهای‌تحویل‌ناپذیر ازهردرجهٔ‌بالای‌دلخواهی وجود دارد.

قضیهٔ ۱۱ خ. (محك آیزنشتاین.) فرض‌کنید

$$a(X) = a_۰ + a_۱X + \cdots + a_nX^n$$

یك‌چندجمله‌ای بادرجهٔ بزرگتریامساوی یك n وضرایب صحیح بامحتوای ۱ باشد. فرض‌کنیدکه عدد اولی مانند p به‌قسمی وجود داشته‌باشدکه

(الف) به‌ازاء $i = ۰ ، ۱ ، \ldots ، n - ۱$ ، $p \mid a_i$ ،

(ب) $p^۲ \nmid a_۰$.

دراین‌صورت $a(X)$ در $\mathbf{Z}[X]$ تحویل‌ناپذیر است وبنابراین در $\mathbf{Q}[X]$ نیز تحویل‌ناپذیر است.

برهان. فرض‌می‌کنیم که $a(X)$ در $\mathbf{Z}[X]$ تحویل‌ناپذیر باشد وبه‌جستجوی‌تناقضی می‌پردازیم. چون محتوای $a(X)$ برابراست با ۱ ، دارای هیچ‌عامل تحویل‌ناپذیر بادرجهٔ صفر نیست، ازاینرو باید دارای تجزیهٔ زیر باشد

$$a(X) = b(X)c(X) ،$$

که‌درآن $b(X) ، c(X) \in \mathbf{Z}[X]$ به‌ترتیب دارای درجه‌های $r ، s$ هستند ودرشرایط $r \geqslant ۱$ ، $s \geqslant ۱$ ، $r + s = n$ صدق می‌کنند. حال ضرایب را به‌پیمانهٔ p (عدد اول مفروض)تحویل می‌کنیم ومعادلهٔ $a^*(X) = b^*(X)c^*(X)$ را در $\mathbf{Z}_p[X]$ به‌دست‌می‌آوریم (قضیهٔ ۱۱ث را ببینید). بنا به‌شرط (الف) داریم $a^*(X) = uX^n$ ، که درآن u ردهٔ باقیماندهٔ a_n به‌پیمانهٔ p است، بـه‌وضوح در $\mathbf{Z}_p$ ، $u \neq ۰$ زیرا در غیـراین صورت p همهٔ ضرایب $a(X)$ را عاد می‌کند.

حال $\mathbf{Z}_p$ میدان‌است (نتیجهٔ‌قضیهٔ ۹ آ) وبنابراین‌قضیهٔ یکتایی‌تجزیه در $\mathbf{Z}_p[X]$ برقرار است (قضیهٔ ۱۰ ح). چندجمله‌ای X تحویل‌ناپذیر است ونتیجه می‌شودکه تنهامقسوم‌علیه‌های uX^n به‌صورت tX^m هستند، کـه درآن t عنصر غیرصفری از $\mathbf{Z}_p$ است و $m \leqslant n$. چـون $b^*(X)c^*(X)$ به‌ترتیب‌حداکثردارای‌درجه‌های s و r هستند، تجزیهٔ $uX^n = b^*(X)c^*(X)$ بایستی به‌صورت $uX^n = (vX^r)(wX^s)$ باشد. حال اگربه $\mathbf{Z}[X]$ رجوع کنیم می‌بینیم کـه

«جمله‌های ثابت» $b(X)$ و $c(X)$ ، یعنی جمله‌های b_0 و c_0 بادرجهٔ صفر، هردو بر p قابل قسمت‌اند، زیرا آنهادر $b^*(X)$ و $c^*(X)$ به‌ه تبدیل‌می‌شوند (توجه‌کنیدکه $r \geqslant 1$، $s \geqslant 1$). بنابراین $a_0 = b_0 c_0$ بر p^2 قابل قسمت‌است، که‌شرط(ب) رانقض می کند. این‌تناقض‌قضیه را اثبات می کند. (تحویل‌ناپذیری در $\mathbf{Q}[X]$ ازقضیهٔ ۱۱ ج نتیجه می‌شود.)

مثال ۵.۱۱. به‌ازاء هرعدد اول p و هر $n \geqslant 1$ چندجمله‌ای $X^n - p$ دارای محتوای ۱ است ودرمحك آیزنشتاین‌صدق‌می کند؛ بنابراین در$\mathbf{Z}[X]$ و $\mathbf{Q}[X]$ تحویل‌ناپذیراست.این بخصوص نشان می‌دهدکه ریشهٔ مثبتnام p در $\mathbf{R}$ گویا نیست، واقعیتی که بسادگی‌می‌تواند ازقضیهٔ یکتایی تجزیه برای$\mathbf{Z}$ نیز به‌دست‌آید.

مثال ۶.۱۱. فرض‌کنید p یك‌عدد اول باشد وچندجمله‌ای

$$a(X) = \frac{1}{X}\{(X+1)^p - 1\}$$

$$= X^{p-1} + pX^{p-2} + \cdots + \binom{p}{i} X^{p-i-1} + \cdots + p$$

را در $\mathbf{Z}[X]$ درنظر بگیرید. این چندجمله‌ای دارای محتوای ۱ است، زیرا تکین است، و همهٔ ضرایب

$$\binom{p}{i}$$

به‌ازاء $i = 1, 2, \ldots, p-1$ بر p قابل قسمت‌اند. این مطلب را از دستور زیر نیز می‌توان دریافت:

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!},$$

که درآن صورت بر p قابل قسمت‌است درحالی‌که مخرج نیست. [به‌طریق دیگر (تمرین ۱۲ از فصل ۱۰ را ببینید) می‌توان در $\mathbf{Z}_p[X]$ چنین استدلال کرد که چندجمله‌ای $(X+1)^p - X^p - 1$ دارای درجهٔ $p-1$ است، ودارای p ریشهٔ متمایز در $\mathbf{Z}_p$ می‌باشد زیرا به‌ازاء هر $x \in \mathbf{Z}_p$ ،

$$(x+1)^p = x + 1 = x^p + 1.$$

پس این چندجمله‌ای، چندجمله‌ای صفراست. نتیجه می‌شودکه در $\mathbf{Z}[X]$ همهٔ ضرایب $(X+1)^p - X^p - 1$ بر p قابل قسمت‌اند.] اگر به $a(X)$ درفوق رجوع کنیم، ملاحظه می‌کنیم که جملهٔ ثابتش p بر p^2 قابل قسمت نیست و بنابراین به‌موجب محك آیزنشتاین $a(X)$ در $\mathbf{Z}[X]$ و در $\mathbf{Q}[X]$ تحویل‌ناپذیراست.

با مقایسهٔ تجزیه‌های چندجمله‌ای X^n-1 در $\mathbf{C}[X]$ ، $\mathbf{R}[X]$ و $\mathbf{Q}[X]$ مطلب را به‌پایان می‌رسانیم. در $\mathbf{C}[X]$ داریم

$$X^n-1=\prod_{r=1}^{n}(X-\zeta^r)\ ,$$

که در آن $\zeta=e^{2\pi i/n}$. باجدا کردن ریشه‌های مزدوج ζ^r و $\zeta^{-r}=\zeta^{n-r}$ (مثال ۱۰.۱۱ را ببینید) عوامل تحویل‌ناپذیر در $\mathbf{R}[X]$ را به‌دست می‌آوریم. برای به‌دست‌آوردن عاملی از X^n-1 در $\mathbf{Q}[X]$ بایستی مجموعه‌ای از ریشه‌های nام ۱ را به‌قسمی پیدا کنیم که حاصلضرب عاملهای مربوطه $X-\zeta^r$ دارای ضرایب گویا باشد. امتحانی درمورد مقادیر کوچك n جواب این مسئله‌را به‌دست می‌دهد. به‌عنوان مثال

$$\begin{aligned}X^6-1&=(X^3-1)(X^3+1)\\&=(X-1)(X+1)(X^2+X+1)(X^2-X+1).\end{aligned}$$

ریشه‌های این‌چهارعامل، به‌حسب $\zeta=e^{\pi i/3}$ ، عبارت‌اند از: $\{\zeta^6\}$ ، $\{\zeta^3\}$ ، $\{\zeta^4,\zeta^2\}$ و $\{\zeta^5,\zeta^1\}$. اینها به‌ترتیب ریشه‌های یکم اولیه، ریشه‌های دوم اولیه، ریشه‌های سوم اولیه و ریشه‌های ششم اولیه ۱ هستند. خواننده بایستی تحقیق کند که طرح‌مشابهی برای‌مقادیر کوچك دیگر n وجود دارد. این طرح تعریف زیر را القاء می‌کند. به‌ازاء هر عددصحیح مثبت m، چندجمله‌ای تکین $\Phi_m(X)$ راکه‌ریشه‌هایش در $\mathbf{C}$ ، ریشه‌های mام اولیه ۱ اند چندجمله‌ای دایره بر mام تعریف می‌کنیم . بنابراین

$$\Phi_m(X)=\prod_{\rho\in S_m}(X-\rho)\ ,$$

که در آن S_m مجموعهٔ تمام ریشه‌های mام اولیهٔ ۱ است. عضوهای S_m به‌صورت ζ^r هستند، که $\zeta=e^{2\pi i/m}$ و r همهٔ اعدادصحیح درمجموعهٔ مقادیر $1\leqslant r\leqslant m$ راکه با m متباین‌اند، اختیار می‌کند (مثال ۷.۷ را ببینید). بنابراین S_m دارای $\varphi(m)$ عضواست و لذا درجهٔ $\Phi_m(X)$ برابر است با $\varphi(m)$.

حال ، به‌ازاء هر $n\geqslant 1$ ، مجموعهٔ همهٔ ریشه‌های n ام ۱ برابر اتحاد مجزای مجموعه‌های S_m است، به‌ازاء همهٔ مقسوم‌علیه‌های m از n . ازاین‌نتیجه می‌شود که در $\mathbf{C}[X]$،

$$X^n-1=\prod_{m|n}\Phi_m(X)\ .$$

(به‌طور ساده عوامل خطی $X-\rho$ از X^n-1 را برطبق مرتبهٔ ریشه‌های ρ دسته‌بندی کرده‌ایم.)

قضیهٔ ۱۱ د. چندجمله‌ایهای دایره‌بر $\Phi_m(X)$ دارای ضرایب صحیح‌اند.

برهان. از استقراء روی m استفاده می‌کنیم. مسلماً چندجمله‌ای $\Phi_1(X)=X-1$ دارای ضرایب‌صحیح است، ازاینرو فرض‌می‌کنیم که به‌ازاء هرعددصحیح r کوچکتراز m ، $\Phi_r(X)$

دارای ضرایب صحیح باشد و $\Phi_m(X)$ را درنظر می‌گیریم. داریم $X^m-1=\Phi_m(X)\Psi(X)$، که $\Psi(X)$ حاصلضرب همهٔ $\Phi_r(X)$ هایی است که $r|m$ و $r\neq m$. بنابه‌فرض استقراء، همهٔ این $\Phi_r(X)$ها دارای ضرایب صحیح‌اند و بنابراین $\Psi(X)$ نیز دارای ضرایب صحیح است. چون در $\mathbf{C}[X]$، $\Psi(X)|X^m-1$، قضیهٔ ۱۱ ب نشان می‌دهد که در $\mathbf{Q}[X]$، $\Psi(X)|X^m-1$، و بنابراین خارج‌قسمت $\Phi_m(X)$ دارای ضرایب گویاست، بعلاوه، $\Psi(X)$ و X^m-1 هردو در $\mathbf{Z}[X]$ قرار دارند و دارای محتوای ۱ هستند زیرا آنها تکین‌اند؛ بنابراین، به‌موجب نتیجهٔ قضیهٔ ۱۱ ج، در $\mathbf{Z}[X]$ داریم $\Psi(X)|X^m-1$. لذاخارج‌قسمت $\Phi_m(X)$ دارای ضرایب صحیح است، و بدین‌ترتیب استقراء کامل می‌شود.

اکنون تجزیه‌ای استانده از X^n-1 در $\mathbf{Z}[X]$ داریم، یعنی

$$X^n-1=\prod_{d|n}\Phi_d(X).$$

توجه داشته باشید که دستور درجهٔ یك حاصلضرب، رابطهٔ آشنای

$$n=\sum_{d|n}\varphi(d),$$

را به‌دست می‌دهد. این حقیقتی است که همهٔ چندجمله‌ایهای دایره‌بر در $\mathbf{Z}[X]$ ودر $\mathbf{Q}[X]$ تحویل‌ناپذیرند (اثبات آن دراینجا خیلی مشکل است)، به‌طوری که درواقع تجزیهٔ کامل X^n-1 را درتمام حالتها داریم. خوانندهٔ علاقه‌مند برهانی ازاین حقیقت را درکتاب وان در واردن [۷] پیدا خواهدکرد. لیکن ما حالت خاص زیررا می‌توانیم ثابت کنیم.

مثال ۷.۱۱. اگر p عددی اول باشد آنگاه ریشه‌های pام اولیهٔ ۱، بجز خود ۱، همان ریشه‌های pام ۱ هستند. بنابراین

$$\Phi_p(X)=\frac{X^p-1}{X-1}=X^{p-1}+X^{p-2}+\cdots+X+1.$$

برای مشاهدهٔ اینکه این چندجمله‌ای در $\mathbf{Z}[X]$ تحویل‌ناپذیر است علامت جدیدی مانند Y اختیار می‌کنیم وچندجمله‌ای

$$a(Y)=\Phi_p(Y+1)=Y^{-1}\{(Y+1)^p-1\}\in\mathbf{Z}[Y]$$

را درنظرمی‌گیریم. درمثال ۶.۱۱ به‌به‌کار بردن محك آیزنشتاین ثابت کردیم که $a(Y)$ در $\mathbf{Z}[Y]$ تحویل‌ناپذیر است. بابررسی نگاشتی از $\mathbf{Z}[X]$ به $\mathbf{Z}[Y]$ که هرچندجمله‌ای $c(X)$ را به $c(Y+1)$ می‌فرستد می‌توانیم نتیجه بگیریم که $\Phi_p(X)$ در $\mathbf{Z}[X]$ تحویل‌ناپذیر است. بنابه قضیهٔ ۱۰خ، این نگاشت یك همریختی حلقه‌هاست، و هر عدد صحیح را به‌خودش می‌فرستد. بنابراین هرتجزیهٔ $\Phi_p(X)=f(X)g(X)$ در $\mathbf{Z}[X]$ تجزیهٔ $a(Y)=f(Y+1)g(Y+1)$ در $\mathbf{Z}[Y]$ را نتیجه می‌دهد. یکی از عاملهای تجزیهٔ اخیر بایستی برابر ±1 باشد، ازاینرو این مطلب برای عاملهای $f(X)$ و $g(X)$ در $\mathbf{Z}[X]$ نیز

درست است. این نشان می‌دهد که ، وقتی p اول باشد، $\Phi_p(X)$ تحویل‌ناپذیر است.

تمرینها

۱. عوامل تحویل‌ناپذیر X^n+1 را در $\mathbf{R}[X]$ پیدا کنید.

۲. عوامل تحویل‌ناپذیر $X^{2n}+X^n+1$ را در $\mathbf{R}[X]$ پیدا کنید.

۳. $X^{12}-1$ را به‌صورت حاصلضربی از چندجمله‌ایهای تحویل‌ناپذیر در (الف) $\mathbf{R}[X]$، (ب) $\mathbf{Q}[X]$ ، (پ) $\mathbf{Z}_2[X]$ و (ت) $\mathbf{Z}_7[X]$ بیان کنید. جوابهای خودرا توجیه کنید.

۴. ثابت کنید که بزرگترین مقسوم‌علیه مشترک X^m-1 و X^n-1 در $\mathbf{Q}[X]$ برابر است با X^d-1 ، که در آن d بزرگترین مقسوم‌علیه مشترک m و n در $\mathbf{Z}$ است.

۵. ضرایب $\Phi_9(X)$ ، $\Phi_{10}(X)$ و $\Phi_{36}(X)$ را پیدا کنید.

۶. ثابت کنید که به‌ازاء $n \geqslant 2$ ، $\Phi_n(0)=1$.

۷. با فرض تحویل‌ناپذیری چندجمله‌ایهای دایره‌بر ، عوامل تحویل‌ناپذیر X^n+1 و $X^{2n}+1$ را در $\mathbf{Z}[X]$ پیدا کنید.

واژه‌نامهٔ فارسی به‌انگلیسی

آبل	Abel
آبلی	abelian
گروه‌ـ	ـgroup
اتحاد، اجتماع	union
آرگان	Argand
آزمایش و خطا	trial and error
استانده	standard
جبرـ	ـalgebra
استقرا	induction
استقرایی	inductive
اسکالر	scalar
استرلینگ	Stirling
استلزام منطقی	implication
استنتاج کردن	deduce
استنتاج	deduction
استوانه	cylinder
اصل پئانو	Peano'saxiom
اصل خوش‌ترتیبی	well-ordering principle
اصل متعارفی	postulate
اصل موضوع	axiom
اصل موضوعی	axiomatic
اصول موضوعه	axioms

اعشاری	decimal
نمادـ	ـnotation
آغازی	initial
افراز	partition
اقلیدس	Euclid
الگوریتمـ	ـ's algorithm
اقلیدسی	euclidean
تبدیلـ	ـtransformation
حوزهـ	ـdomain
خاصیتـ	ـproperty
گروهـ	ـgroup
اکیداً صعودی	strictly increasing
اگر وفقط اگر	if and only if
الگوریتم	algorithm
آنالیز	analysis
nتایی	n-ary
انتگرالگیری	integrating
اندیس	index
انعکاس	reflection
انعکاسی	reflexive
اول (عدداول)	prime
اولیه	primitive
ریشهـ	ـroot

Euler	اویلر
ideal	ایده‌آل
principal—	ـ اصلی
Eisenstein	آیزنشتاین
—criterion	محك ـ
open	باز
—interval	بازهٔ (فاصلهٔ) ـ
remainder	باقیمانده
residue	باقیمانده
—class	ردهٔ ـ
fibre	بافت
bounded above	بالاکراندار
into	بتوی
torsion-free	بدون‌تاب
trivial	بدیهی
vector	بردار
—algebra	جبر ـ ی
—product	ضرب ـ ی
onto	برو
greatest common divisor	بزرگترین مقسوم‌علیه مشترك
dimension	بعد
vice versa	بعکس
block	بلوك
Bool	بول
boolean	بولی
—algebra	جبر ـ
modulo n	به پیمانهٔ n
uniquely	به‌طور یکتا
Birkhoff	بیرکف
infinite	بینهایت
antisymmetric	پادمتقارن
paradox	پارادکس
Peano	پئانو
leading	پیشرو
—coefficient	ضریب ـ
—term	جملهٔ ـ
modulus	پیمانه
modular	پیمانه‌ای
function	تابع
Euler's—	ـ اویلر
rational—	ـ گویا
exponential—	ـ نمائی
surjection	تابع برو
injection	تابع یك به‌یك
transformation	تبدیل
euclidean—	ـ اقلیدسی
orthogonal—	ـ متعامد
decomposition (factorization)	تجزیه
restrict	تحدید کردن
reducible	تحویل‌پذیر
irreducible	تحویل‌ناپذیر
recursive	تراجعی
transposition	ترانهش
rearrangement	ترتیب‌مجدد
similarity	تشابه
Mercator's projection	تصویر مرکاتور
projective	تصویری
definition	تعریف
subtraction	تفریق
symmetry	تقارن
division	تقسیم
correspondence	تناظر
one-one—	ـ یك به‌یك
period	تناوب
power	توان

at least	حداقل
at most	حداکثر
elimination	حذف
eliminate	حذف کردن
arithmetic	حساب
real	حقیقی
–number	عدد–
–line	محور–
solution	حل
solve	حل کردن
ring	حلقه
commutative–	–جابجایی
quotient–	–خارج‌قسمت
non-commutative–	–غیرجابجایی
finite–	–متناهی
euclidean domain	حوزهٔ اقلیدسی
domain	حوزهٔ تعریف
integral domain	حوزهٔ صحیح
range	حوزهٔ مقادیر (مجموعهٔ مقادیر)
terminate	خاتمه یافتن
quotient	خارج‌قسمت
property	خاصیت
euclidean–	–اقلیدسی
universal–	–جامع
line	خط
linear	خطی
equator	خط استوا
automorphism	خودریختی
well-ordered	خوش‌ترتیب
well-ordering	خوش‌ترتیبی
well-defined	خوش‌تعریف
cyclotomic	دایره‌بر
determinant	دترمینان
prime–	–اول
distributive	توزیعی
–law	قانون–
empty	تهی
–set	مجموعهٔ–
embed	جادادن
embedding	جادهی
universal	جامع
algebra	جبر
standard–	–استانده
vector–	–برداری
boolean–	–بولی
abstract–	–مجرد
elementary–	–مقدماتی
modern–	–نو
algebraic	جبری
–structure	ساخت–
–law	قانون–
disjoint	جدا ازهم
pair	جفت
ordered–	–مرتب
term	جمله
leading–	–پیشرو
summation	جمع‌یابی
summand	جمعوند
additive	جمعی
polynomial	چندجمله‌ای
monic–	–تکین
cyclotomic–	–دایره‌بر
product	حاصلضرب
direct–	– مستقیم
limit	حد

entry	درایه
degree	درجه
quadratic	درجهٔدوم
validity	درستی
false	دروغ
interpolation	درون‌یابی
Lagrange's—	ـ لاگرانژ
equations	دستگاه‌معادلات
simultaneous congruences	دستگاه همنهشتیها
formulae	دستور، فرمول
collection	دسته
cartesian	دکارتی
arbitrary	دلخواه
Demorgan	دمورگان
pairwise	دوبدو
binary	دوتایی
—operation	عمل—
rotation	دوران
period	دوره
bijection	دوسویی
relation	رابطه
ordered—	ـ ترتیبی
equivalence—	ـ هم ارزی
true	راست
class	رده
residue—	ـ باقیمانده
equivalence—	ـ هم ارزی
digit	رقم
axiomatic method	روش اصل موضوعی
mathematical	ریاضی
mathematics	ریاضیات
root	ریشه
primitive—	ـ اولیه
Riordan	ریوردان
even	زوج (عدد)
subring	زیر حلقه
subspace	زیرفضا
subgroup	زیرگروه
normal—	ـ نرمال
subset	زیر مجموعه
subfield	زیرمیدان
algebraic structure	ساخت جبری
simplify	ساده کردن
column	ستون
proper	سره
surface	سطح
row	سطر
quantifier	سور
Sylow	سیلو
—'s theorem	قضیهٔ ـ
sine	سینوس
include	شامل بودن
condition	شرط
associative	شرکت‌پذیری
hexagon	شش ضلعی
radius	شعاع
renumbering	شماره گذاری‌مجدد
include	شمول
slope	شیب
satisfy	صدق کردن
plane	صفحه
zero	صفر
increasing	صعودی

numerator	صورت کسر
rational form	صورت گویا
formal	صوری
multiplication	ضرب
vector product	ضرب برداری
multiplicative	ضربی
coefficient	ضریب
_number	عدد ـ
factor	عامل
statement	عبارت
number	عدد
cardinal_	ـ اصلی
irrational_	ـ اصم
real_	ـ حقیقی
even_	ـ زوج
natural	ـطبیعی
odd_	ـ فرد
rational_	ـ گویا
complex_	ـ مختلط
gaussian integer	عدد صحیح گاوسی
member	عضو
sign	علامت
operation	عمل
unary_	= یکتایی
general	عمومی
element	عنصر
non-chinese	غیرچینی
non-square	غیرمربع
non-singular	غیرمنفرد
interval	فاصله
closed_	ـ بسته

square-free	فاقد عامل مربع
process	فرایند
odd	فرد
individual	فردی
hypothesis	فرض
Fermat	فرما
_'s Theorem	قضیهٔ ـ
divisible	قابل تقسیم، تقسیم پذیر
rule	قاعده
theorem	قضیه
fundamental_	ـ اساسی
Euler's_	ـ اویلر
chinese remainder_	ـ باقیماندهٔ چینی
Wilson's_	ـ ویلسون
polar	قطبی
diagonal	قطری
segment	قطعه خط
sufficient	کافی
complete	کامل
bound	کران
upper_	ـ بالا
lower_	ـ پائین
fraction	کسر
cosine	کسینوس
Klein	کلاین
_'s 4-group	ـ ۴-گروه
total	کلی
completeness	کمال
minimum	کمینه
least common multiple	کوچکترین مضرب مشترك
Cayley	کیلی
_'s octanious	ـ هشتگانهای

گاوس	Gauss	متناوب	alternative
گروه	group	متناهی	finite
ـ اقلیدسی	euclidean—	مثال نقض	counter-example
ـ خارج‌قسمت	quotient (factor)—	مثبت	positive
ـ خطی عمومی	general linear—	مثلث	triangle
ـ خطی‌ویژه	special linear—	مجموع	sum
ـ دایره‌ای	circle—	مجموعه	set
ـ دوری	cyclic—	ـ تهی	empty—
ـ متعامد	orthogonal—	ـ خارج قسمت	quotient—
ـ متقارن	symmetric—	ـ شمارش‌پذیر	countable—
ـ متناهی	finite—	ـ متناهی	finite—
گزاره	proposition	مجهول	unknown
گویا	rational	محتوا	content
تابع ـ	—function	محض	pure
صورت ـ	—form	محك	criterion
عدد ـ	—number	محور حقیقی	real line
		محور	axis
لاگرانژ	Lagrange	ـxها	x—
لگاریتم	logarithm	ـyها	y—
لم	lemma	محیط	circumference
		مختصات	coordinates
ماتریس	matrix	ـقطبی	polar—
مبدأ	origin	مختلط	complex
متباین	coprime	عدد ـ	—number
متساوی‌الاضلاع	equilateral	مزدوج ـ	—conjugate
متصل	continuous	مخرج کسر	denomerator
متعارف	canonical	مربع	square
متعامد	orthogonal	مرتبه	order
تبدیل ـ	—transformation	مرکاتور	Mercator
گروه ـ	—group	تصویر ـ	—'s projection
متعدی	transitive	مزدوج	conjugate
متغیر	variable	مستدیر	circular
متقابل	opposite	مستطیل	rectangle
متقارن	symmetric	مستطیلی	rectangular
گروه ـ	—group	مستقل	independent

point	نقطه
mapping	نگاشت
quotient—	ـ خارج‌قسمت
canonical —	ـ متعارف
geographical —	ـ جغرافیایی
surjection	نگاشت برو
bijection	نگاشت دوسوئی
injection	نگاشت یك‌به‌یك
exponent	نما
representative	نماینده، نمودار
type	نوع
typical	نوعی
Newton	نیوتن
associated	وابسته
Van der Waerden	وان در وردن
existence	وجود
Wilson	ویلسون
Halmos	هالموس
Hamilton	هامیلتون
Hamiltonian	هامیلتونی
kernel	هسته
Cayley octanions	هشتگانهای کیلی
equivalence	هم‌ارزی
—class	ردهٔ‌ـ
coset	همردهٔ
right—	ـراست
homomorphic	همریخت
homomorphism	همریختی
quotient—	ـخارج‌قسمت
congruence	همنهشتی
geometry	هندسه
geometrical	هندسی

characteristic	مشخصه
contained	مشمول
multiple	مضرب
equation	معادله
inverse	معکوس
invertable	معکوس‌پذیر
inversion	معکوس‌گیری
definite	معین
value	مقدار
divisor	مقسوم علیه
zero—	ـ صفر
common—	ـ مشترك
intersection	مقطع
complement	مکمل
Maclane	مکلین
logic	منطق
logical	منطقی
regular	منظم
singular	منفرد
negative	منفی
parallel	موازی
generator	مولد
field	میدان
infinite	نامتناهی
indefinite	نامعین
consequence, corollary	نتیجه
imply	نتیجه دادن
normal	نرمال
ratio	نسبت
relatively prime	نسبت به هم اول
theory	نظریه
negation	نفی
end-points	نقاط انتهایی
image	نقش

isomorphic	یکریخت	one-to-one	یك‌به‌یك
isomorphism	یکریختی	unique	یکتا
identical	یکسان	unary	یکتایی
unit	یکه	—operation	عمل—
identify	یکی گرفتن	uniqueness	یکتایی

واژه‌نامهٔ انگلیسی به‌فارسی

Abel	آبل
abelian group	گروه آبلی
absolute value	قدر مطلق
abstract algebra	جبر مجرد
abstraction	تجرید
additive power	توان جمعی
algebra	جبر
algebraic	جبری
—law	قانون—
—structure	ساخت—
algorithm	الگوریتم
alternative	متناوب
analysis	آنالیز
analytic	تحلیلی
antisymmetric	پادمتقارن
approximation	تقریب
Argand	آرگان
arithmetic	حساب
associative	شرکت‌پذیری
assumption	فرض
automorphism	خودریختی
axiomatic method	روش اصل موضوعی
axiom	اصل موضوع
axioms	اصول موضوعه
axis	محور
belong	متعلق بودن
bijection	تابع‌دوسویی
binary operation	عمل‌دوتایی
Birkhoff	بیرکف
block	بلوك
Bool	بول
boolean algebra	جبر بولی
bounded above	بالاکراندار
cancellation law	قانون حذف
canonical map	نگاشت متعارف
cardinal number	عدد اصلی
cartesian	دکارتی
Cayley	کیلی
—octanions	هشتگانهای—
characteristic	مشخصه
chinese remainder theorem	قضیهٔ باقیماندهٔچینی
circle group	گروه دایره‌ای

circular	مستدیر
circumference	محیط
class	رده
closed interval	فاصلهٔ (بازهٔ) بسته
coefficient	ضریب
collection	دسته
column	ستون
common divisor	مقسوم‌علیه مشترك
commutative ring	حلقهٔ جابجایی
complement	مکمل
complete	کامل
complex	مختلط
ـconjugate	مزدوج ـ
ـnumber	عدد ـ
composite function	تابع مرکب
composition	ترکیب
congruence	همنهشتی
conjugate	مزدوج
contained	مشمول
content	محتوا
continuous	متصل
contradiction	تناقض
coordinates	مختصات
coprime	متباین
corollary	نتیجه
correspondence	تناظر
coset	همرده
cosine	کسینوس
countable set	مجموعهٔ شمارش‌پذیر
counter-example	مثال نقض
criterion	محك
cyclic group	گروه دوری
cyclotomic	دایره‌بر
ـpolynomial	چندجمله‌ای ـ
cylinder	استوانه
decimal notation	نمادعشاری
decomposition	تجزیه
deduction	استنتاج
definite	معین
definition	تعریف
degree	درجه
Demorgan	دمورگان
denomerator	مخرج کسر
determinant	دترمینان
diagonal	قطری
diagram	نمودار
digit	رقم
dimension	بعد
direct product	حاصلضرب مستقیم
disjoint	جدا ازهم
distributive law	قانون توزیعی
division	تقسیم
divisor	مقسوم علیه
domain	حوزهٔ تعریف
Eisenstein	آیزنشتاین
ـcriterion	محك ـ
element	عنصر
elementary algebra	جبرمقدماتی
elimination law	قانون حذف
embeding	جادهی
empty set	مجموعهٔ تهی
end-points	نقاط انتهایی
entry	درایه
equator	خط استوا
equilateral	متساوی‌الاضلاع
equivalence	هم‌ارزی

ردهٔ—	—class
رابطهٔ—	—relation
اقلیدس	Euclid
الگوریتم—	—'s algorithm
اقلیدسی	euclidean
حوزهٔ—	—domain
گروه—	—group
خاصیت—	—property
تبدیل—	—transformation
اویلر	Euler
الگوریتم—	—'s algorithm
تابع—	—'sfunction
قضیه—	—'stheorem
عدد زوج	even number
نما	exponent
تابع نمائی	exponential function
عامل	factor
گروه خارج‌قسمت	factor group
تجزیه	factorization
فرما	Fermat
قضیهٔ —	—'s Theorem
بافت	fibre
میدان	field
متناهی	finite
میدان—	—field
گروه —	—group
حلقه—	—ring
مجموعه—	—set
دستور	formulae
قضیهٔ اساسی جبر	fundamental theorem of algebra
گاوس	Gauss
عدد صحیح گاوسی	gaussian integer
گروه خطی عمومی	general linear gorup
مولد	generator
نگاشت‌جغرافیایی	geographical map
بزرگترین‌مقسوم‌علیه‌مشترك	greatest common divisor
گروه	group
هالموس	Halmos
هامیلتون	Hamilton
هامیلتونی	hamiltonian
شش ضلعی	hexagon
همریخت	homomorphic
فرض	hypothesis
ایده‌آل	ideal
یکسان	identical
عنصر همانی	identity element
اگر وفقط اگر	if and only if
نقش	image
شامل بودن	implication
شمول	include
استلزام منطقی	inclusion
صعودی	increasing
مستقل	independent
اندیس	index
فردی	individual
استقرا	induction
نامتناهی	infinite
آغازی	initial
تابع یك به‌یك	injection
عددصحیح	integer

integral domain	میدان صحیح
integrating	انتگرالگیری
interpolation	درون‌یابی
intersection	مقطع
interval	فاصله (بازه)
into	بتوی
inverse	معکوس
inversion	معکوس‌گیری
invertable	معکوس‌پذیر
irrational number	عدد اصم
irreducible	تحویل‌ناپذیر
isomorphic	یکریخت
isomorphism	یکریختی
kernel	هسته
Klein	کلاین
—'s 4-group	۴-گروه‌ـ
Lagrange	لاگرانژ
leading	پیشرو
—coefficient	ضریب‌ـ
—term	جملهٔ‌ـ
least common multiple	کوچکترین مضرب مشترك
lemma	لم
limit	حد
line	خط
linear	خطی
logarithm	لگاریتم
logic	منطق
lower bound	کران پائین
Maclane	مکلین
mapping	نگاشت
mathematical	ریاضی
matrix	ماتریس
member	عضو
Mercator	مرکاتور
—'s projection	تصویر ـ
minimum	کمینه
modern algebra	جبر نو
modular	پیمانه‌ای
modulo n	به پیمانهٔ n
modulus	پیمانه
monic polynomial	چندجمله‌ای تکین
multiple	مضرب
multiplication	ضرب
multiplicative	ضربی
n-ary	nتایی
natural number	عددطبیعی
negation	نفی
negative	منفی
neutral elemet	عنصر خنثی
Newton	نیوتن
non-chinese	غیرچینی
non-commutative ring	حلقهٔ غیرجابجایی
non-singular	غیرمنفرد
non-square	غیرمربع
normal subgroup	زیرگروه نرمال
numerator	صورت کسر
odd	فرد
one-one correspondence	تناظر یك‌به‌یك
one-to-one	یك‌به‌یك
onto	برو

باز	open
عمل	operation
متقابل	opposite
مرتبه	order
رابطهٔ ترتیبی	order relation
جفت‌مرتب	ordered pair
مبدأ	origin
متعامد	orthogonal
گروه‌ـ	ـgroup
تبدیل ـ	ـtransformation
جفت	pair
دوبدو	pairwise
پارادکس	paradox
موازی	parallel
کسرجزئی	partial fraction
افراز	partition
پئانو	Peano
اصل ـ	ـ's axiom
تناوب	period
دوره‌ای	periodic
جایگشت	permutation
صفحه	plane
نقطه	point
مختصات‌قطبی	polar coordinates
چندجمله ای	polynomial
مثبت	positive
اصل متعارفی	postulate
ماقبل	predecessor
اول	prime
توان اول	prime-power
ریشهٔ‌اولیه	primitive root
ایده‌آل اصلی	principal ideal
اصل	principle
احتمال	probability
فرایند	process
حاصلضرب	product
تصویر	projection
تصویری	projective
برهان	proof
سره	proper
گزاره	proposition
محض	pure
درجهٔ‌دوم	quadratic
سور	quantifier
خارج‌قسمت	quotient
گروه‌ـ	ـgroup
همریختی‌ـ	ـhomomorphism
نگاشت‌ـ	ـmapping
حلقه‌ـ	ـring
مجموعهٔ‌ـ	ـset
شعاع	radius
حوزهٔ مقادیر	range
نسبت	ratio
گویا	rational
عدد ـ	ـnumber
صورت ـ	ـform
تابع ـ	ـfunction
حقیقی	real
خط‌ـ	ـline
عدد‌ـ	ـnumber
ترتیب‌مجدد	rearrangement
مستطیل	rectangle
مستطیلی	rectangular
تراجعی	recursive
انعکاس	reflection

انعکاسی	reflexive
منظم	regular
نسبت به هم اول	relatively prime
باقیمانده	remainder
شماره گذاری مجدد	renumbering
ردهٔ باقیمانده	residue class
تحدید کردن	restrict
همرده راست	right coset
حلقه	ring
ریوردان	Riordan
ریشه	root
دوران	rotation
سطر	row
قاعده	rule
اسکالر	scalar
قطعه خط	segment
سری	series
مجموعه	set
علامت	sign
تشابه	similarity
دستگاه همنهشتیها	simultaneous congruences
دستگاه معادلات	simultaneous equations
منفرد	singular
شیب	slope
گروه خطی ویژه	special linear group
کره	sphere
فاقد عامل مربع	square-free
جبر استانده	standard algebra
استرلینگ	Stirling
اکیداً صعودی	strictly increasing
زیرمیدان	subfield
زیرگروه	subgroup
زیرحلقه	subring
زیرمجموعه	subset
زیرفضا	subspace
جمعوند	summand
جمع یابی	summation
سطح	surface
تابع برو	surjection
سیلو	Sylow
قضیهٔ ـ	ـ's theorem
گروه متقارن	symmetric group
تقارن	symmetry
جمله	term
خاتمه یافتن	terminate
قضیه	theorem
نظریه	theory
بدون تاب	torsion-free
تبدیل	transformation
متعدی	transitive
ترانهش	transposition
آزمایش و خطا	trial and error
مثلث	triangle
بدیهی	trivial
عمل یکتایی	unary operation
اتحاد (اجتماع)	union
یکتا	unique
یکه	unit
خاصیت جامع	universal property
مجهول	unknown
کران بالا	upper bound
وان در وردن	Van der Waerden

theorem	قضیهٔ ـ	variable	متغیر
		vector	بردار
x–axis	محور xها	–algebra	جبر ـ ی
		–product	ضرب ـ ی
y–axis	محور yها	vice versa	بعکس
zero	صفر	well-defined	خوش‌تعریف
–element	عنصر ـ	well-ordering	خوش‌ترتیبی
–divisor	مقسوم‌علیه ـ	–principle	اصل ـ
		Wilson	ویلسون

فهرست راهنما

منابع

[1] Birkhoff, G. and MacLane, S. *A Survey of Modern Algebra*, Macmillan, (1953).

[2] Boole, G. *The Mathematical Analysis of Logic*, Cambridge, (1847). Reprinted by Blackwell, Oxford, (1948).

[3] Burkhill, J.C. *A First Course in Mathematical Analysis*, Cambridge University Press, (1962).

[4] Halmos, P. *Naive Set Theory*, Van Nostrand, (1960).

[5] Perfect, H. *Topics in Algebra*, Pergamon (1967).

[6] Riordan, J. *Introduction to Combinatorial Analysis*, Wiley, (1958).

[7] Van der Waerden, B. L. *Modern Algebra*, Vol. I, Ungar, (1950).