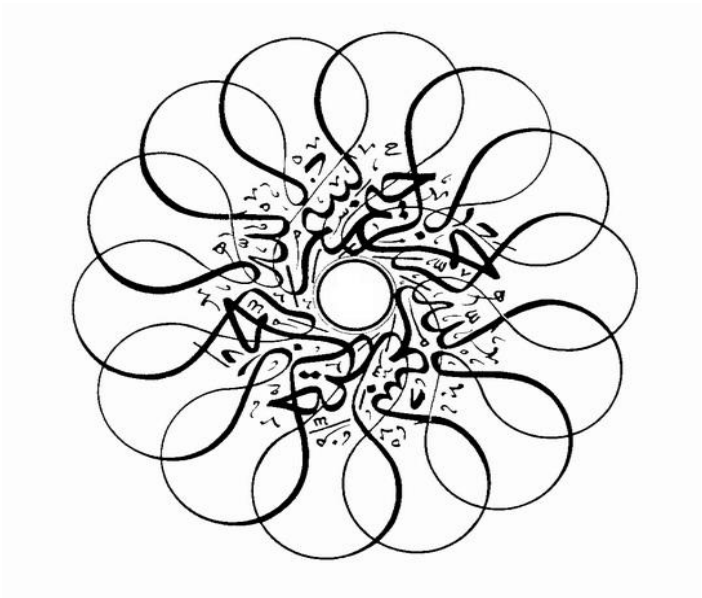


تقـــدیـــم به
همـــه‌ی اســـاتید و مدرســـین
جـــــبـــــر

به‌ویژه

مـــهـــدی مصبـــاح

سیـــامـــک یاســـمی

امیرهوشنگ یمینی

پیش گفتار

قلم‌ها قیام می‌کنند تا قیامت برپا کنند. دل‌ها را خورشیدی و چشم‌ها را بارانی کنند. طوفانی به راه اندازند و لیلی‌ها را مجنون کنند. هم از عشق می‌نویسند و هم از علم؛ و چه قلم ارزشمندی است قلم علم! اگر علم از قلم می‌چکد، بی‌شک لطف خداست، همین جاست که قلم مولانا می‌نویسد:

کار تو تبدیل اعیان و عطا
کار ما سهو است و نسیان و خطا
سهو و نسیان را مبدل کن به علم
من همه جهلم مرا ده صبر و حلم

درست همان جایی که خداوند به قلم قسم می‌خورد «ن و القلم و ما یسطرون» (سوره‌ی قلم، آیه‌ی۱). گرچه به قلم قسم می‌خورد اما در پس پرده به انسانی سوگند می‌خورد که قلم در دست

می‌گیرد و می‌نویسد. قلم به خودی خود ارزش ندارد؛ به دیگر بیان، اگر انسان ارزشمند باشد آن‌گاه قلم ارزشمند است و ارزشمند می‌نویسد.

باز در ادامه‌ی راه سطرها، قلم ردپای تازه‌ای از خود بر جای می‌گذارد که از چه بنویسد؟ ردپایش را دنبال کنید ... از هر کرانی بی‌کران، بی‌انتها چون آسمان، تا ناکجا آبادها، ناآشنایی آشنا ... بگذارید طبع شعر قلم را سرکوب کنیم، در یک کلام قلمرو ریاضیات! با دامنه‌ای به اندازه‌ی همه‌ی هستی و بردی که هر روز بزرگ‌تر می‌شود. مجموعه‌ای عظیم که هر کس عضوش باشد، علاقه‌اش تا بی‌نهایت میل خواهد کرد. کوته فکران در این قلمرو تعریف ناشدنی‌اند و تنها در اوج ابهام به پرگار شگفت انگیزی می‌نگرد که تمام جهان را با نقش‌های گوناگون رسم کرده است؛ جالب این جاست که خودشان هم ترسیم همین پرگارند، ولی نمی‌دانند و گیج می‌زنند!

در بین گروه‌ها، گروه ریاضیات حلقه‌ای در دست دارد که انگار جادو می‌کند؛ تمام علوم را خلق می‌کند، می‌رقصاند و در این میدان رقص ققنوس می‌آفریند. ققنوس شعله می‌کشد و از دل خاکسترش ققنوسی دیگر جان می‌گیرد. چیز مبهمی نیست. مسئله این جاست که همه‌ی حل ناشده‌ها نزد خود ماست. ما می‌توانیم ملکه‌ی علوم را، کلفت خویش سازیم، باور کنید! این قضیه‌ای است که اثباتش در عین سختی، بدیهی است. این قضیه را به اندازه‌ی تمام ریاضی‌دانان تاریخ، اثبات دارد. در حقیقت هر ریاضی‌دانی خود اثباتی برای این قضیه است.

جای بازی با کلمات بسیار است، اما فرصت ناچیز. اصل مطلب در این‌جا، انگیزه‌ی تدوین این کتاب است که اینک به رشته‌ی تحریر در خواهد آمد:

برای هر دانشجویی، دوره‌ی کارشناسی، دوره‌ی شیرینی است. لحظاتی که پای درس اساتید بزرگوارش می‌نشیند تا جرعه جرعه علم بنوشد. یکی از مهم‌ترین دروس دوره‌ی کارشناسی ریاضی، درس «جبر ۲» است؛ درسی دوست داشتنی. اما شاید در ابتدا، برای خیلی از دانشجویان جذاب نباشد! اگر چه استاد جبر، با سعه‌ی صدر، تعاریف و قضایا را یک‌به‌یک روی تابلو می‌نویسد، باز می‌کند و شرح می‌دهد، ولی هر کدام دیگری را پیچیده‌تر و ذهن‌ها را مغشوش‌تر می‌کند. انگار هیچ چیز آشنایی وجود ندارد که مطالب را برای شاگردان قابل درک کند. نگاه آن‌ها بی‌رمق می‌ماند و فکرشان پر از علامت سوال می‌شود. گاهی می‌پرسند. گاهی جرأت نمی‌کنند بپرسند. هر استاد ریاضی نیز شاید در گذشته‌ای نه چندان دور دوران کارشناسی، سر کلاس جبر ۲، همین احساس را تجربه کرده باشد.

ریشه‌ی این سوال‌ها و این نگاه‌ها از کجا آب می‌خورد؟ جواب معلـوم اسـت! و آن، ایـن‌کـه در هنگام تدریس یا مطالعه‌ی درس جبر ۲ (نظریه‌ی گـالوا) ، سـریع و مسـتقیم بـه اهـداف اساسـی نمی‌رسیم و دانشجو گیج و سردرگم می‌شود؛ دانشجویان ما معمولاً کم حوصله‌اند و مـی‌خواهنـد در کمترین فرصت به نتیجه برسند؛ از طرفی هم می‌خواهند موضوع درس را بـه راحتـی لمـس کننـد؛ البته حق دارند، حتی اگر دانشجوی رشته‌ی ریاضی محض باشند!

به‌عنوان مثال، اکثر کتب نظریه‌ی گالوا، ابتدا به بررسـی مفصـلی از مباحـث نظریـه‌ی میـدان، توسیع میدان، توسیع ساده، متناهی، نرمال، شکافنده، تفکیک پـذیر و ... مـی پردازنـد، مبـاحثی بـا قضایای کسل کننده و ملال آور و دانشجو متوجه اهداف پشت سر این مباحث نمـی‌شـود. انگیـزه‌ی اصلی نگارش این کتاب، فایق آمدن بر این مشکلات است.

ما تلاش کرده‌ایم، مطالب کتاب را، در حد امکان ساده بیان و از توضیحات اضافه پرهیز کنـیم. همین طور خواسته‌ایم به گونه‌ای عمل کنم که دانشجو با علاقه موضـوع درس را مطالعـه کنـد؛ بـه همین منظور، در ابتدای هر فصل پرسش‌ها و مسائل جذاب ریاضی مانند:

(۱) تثلیث زاویه، تضعیف مکعب وتربیع دایره (اهداف فصل۲)
(۲) ترسیم چند ضلعی‌های منتظم (اهداف فصل۲و۵)
(۳) یافتن فرمولی برای حل معادلات چند جمله‌ای (اهداف فصل۴)

که از دیرباز مورد توجه ریاضی‌دانان بوده اسـت، گنجانـده‌ایـم و آرام در طـی فصـل بـه پاسـخ ایـن پرسش‌ها می‌رسیم.

در فصل ۶ مباحث جذابی از قبیل اثبات قضیه‌ی اساسی جبـر، اثبـات متعـالی بـودن π و e، ترسیم ۱۷-ضلعی منتظم و ... آورده شده است که می‌توانند به‌عنوان سمینار و پروژه‌ی کلاس درسی مطرح گردند. در انتهای هر بخش سه نوع تمرین آورده شده است: هدف تمرین‌های سـطح ۱، فهـم بهتر درس بوده و کلیه دانشجویان باید از عهده‌ی حل این تمرین‌ها برآیند. تمـرین‌هـای سـطح ۲

مخصوص دانشجویان علاقمند و پرتلاش است و در نهایت تمرین‌های سطح ۳ که احتیاج به کار فکری بیشتری دارند، دانشجویان با هوش و مستعد را به مبارزه می‌طلبند.

دو پیوست در انتهای کتاب اضافه گردیده است. پیوست اول به مروری بر فضاهای برداری که زمینه‌ساز فصل ۲ است، اختصاص دارد. پیوست دوم به بیان مختصری از زندگی‌نامه‌ی ریاضی‌دانان سرشناسی که نقشی بسیار اساسی در این کتاب ایفا می‌کنند، می‌پردازد. این پیوست به خواننده کمک می‌کند که تصویری از مفاهیم داشته باشد.

در این‌جا لازم می‌دانیم به پاس تذکرات و راهنمایی های ارزنده سرکار خانم نجمه ربیعی ویراستار این اثر، تشکر و قدردانی کنیم. همچنین از دوست بسیار عزیزمان آقای دکتر احمد کاظمی فرد که نسخه‌ی ابتدایی این کتاب را تدریس نموده و با رهنمودهای خود ما را در بهتر شدن کتاب یاری داده‌اند، سپاسگزاری می‌گردد. از دوست عزیزمان جناب آقای جعفر اسماعیلی که طراحی جلد این کتاب را بر عهده داشتند، نیز کمال تشکر را داریم. در خاتمه از ریاست و کارکنان محترم انتشارات دانشگاه شهرکرد که موجبات چاپ این کتاب را فراهم کرده‌اند تشکر می‌نماییم. با آرزوی توفیق برای همه‌ی این عزیزان.

قطعاً، این کتاب عاری از عیب ونقص نیست امیدوارم همکاران و دانشجویان عزیز از راهنمائی‌های ارزشمند خود در جهت رفع نواقص موجود دریغ نفرمایند.

علیرضا نقی پور

جواد صدیقی

بام ایران- زمستان ۱۳۸۸

فهرست مطالب

فصل ۱

حلقه‌ها

باید به یاد داشته باشید که مفهوم‌های ریاضی نتیجه‌ای از کار آزاد ذهن نیستند؛ بلکه انعکاسی از جهان واقعی و عینی دوروبر ما هستند که البته اغلب به‌صورت کاملاً انتزاعی طرح می‌شود.

(د.یا. سترویک)

در این فصل می‌خوانیم:

مقدمه

در این فصل، ابتدا مرور مختصری بر مفهوم حلقه خواهیم داشت. در بخش دوم، به مطالعه‌ی حلقه‌های چندجمله‌ای خواهیم پرداخت. میدان کسرها و به‌دنبال آن تجزیه و یکتایی تجزیه، به‌ترتیب در بخش‌های سوم و چهارم بررسی می‌شوند. در بخش آخر محک‌هایی را برای تحویل‌ناپذیری ارائه خواهیم داد.

۱-۱ تعریف‌ها و خواص مقدماتی

در سراسر این کتاب، از نمادهای مرسوم زیر استفاده خواهیم کرد:

$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$؛ مجموعه‌ی اعداد صحیح،

$\mathbb{N} = \{1, 2, \ldots\}$؛ مجموعه‌ی اعداد طبیعی،

$\mathbb{N}_0 = \{0, 1, 2, \ldots\}$؛ مجموعه‌ی اعداد صحیح نامنفی،

$\mathbb{Q} = \{m / n \mid m, n \in \mathbb{Z}, n \neq 0\}$؛ مجموعه‌ی اعداد گویا،

$\mathbb{R}$؛ مجموعه‌ی اعداد حقیقی،

$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$؛ مجموعه‌ی اعداد مختلط،

$\mathbb{Z}_n$؛ مجموعه‌ی اعداد صحیح به پیمانه‌ی n.

تعریف ۱-۱

مجموعه‌ی ناتهی R، همراه با دو عمل دوتایی (که به صورت جمع و ضرب نوشته می‌شوند) یک **حلقه** است اگر شرایط زیر برقرار باشند:

(۱) $(R, +)$ یک **گروه آبلی** باشد،

(۲) (قانون **شرکت‌پذیری**): به ازای هر a و b و $c \in R$،

$$(ab)c = a(bc),$$

(۳) (قانون **توزیع‌پذیری**): به ازای هر a و b و $c \in R$،

$a(b + c) = ab + ac$ (توزیع‌پذیری چپ)،

$(a + b)c = ac + bc$ (توزیع‌پذیری راست).

تعریف۱-۲

حلقه‌ی R را **تعویض‌پذیر** گوییم اگر برای هر a و $b \in R$ داشته باشیم:

$$ab = ba.$$

اگر R تعویض‌پذیر نباشد، آن‌را **تعویض‌ناپذیر** گوییم.

تعریف ۱-۳

حلقه‌ی R را **یکدار** گوییم اگر عنصر $1_R \in R$ موجود باشد به‌طوری‌که برای هر $a \in R$،

$$1_R a = a 1_R = a.$$

❖ **تذکر:** درصورتی‌که جای هیچ ابهامی نباشد، برای راحتی به‌جای نماد 1_R از 1 استفاده می‌کنیم.

مثال ۱: هر یک از $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ همراه با جمع و ضرب معمولی اعداد، حلقه‌هایی تعویض‌پذیر و یکدار هستند.

□

مثال ۲: برای هر عدد طبیعی n، $\mathbb{Z}_n$ حلقه‌ای تعویض‌پذیر و یکدار است.

□

مثال ۳ (حلقه‌های ماتریسی): فرض کنید R یک حلقه باشد. مجموعه‌ی ماتریس‌های $n \times n$ روی حلقه‌ی R، یعنی $\mathbf{M}_n(R)$ همراه با جمع و ضرب ماتریس‌های $n \times n$ یک حلقه است. اگر R حلقه‌ای یکدار باشد، $\mathbf{M}_n(R)$ نیز چنین است.

□

❖ **تذکر:** اگر R حلقه‌ای باشد که $|R| > 1$ (یا به‌طور معادل $1_R \neq 0$)، آن‌گاه برای $n \geq 2$، $\mathbf{M}_n(R)$ حلقه‌ای تعویض‌ناپذیر است.

مثال ۸ : فرض کنیم

$$\mathbb{H}(\mathbb{R}) = \mathbb{H} = \left\{ a_0 + a_1 i + a_2 j + a_3 k \,\middle|\, a_i \in \mathbb{R} \right\}.$$

در این مجموعه، دو عنصر $a_0 + a_1 i + a_2 j + a_3 k$ و $b_0 + b_1 i + b_2 j + b_3 k$ را مساوی گوییم اگر و فقط اگر $a_i = b_i$ برای $i = 0,1,2,3$. جمع و ضرب روی $\mathbb{H}(\mathbb{R})$ را چنین تعریف می‌کنیم:

$$\begin{aligned}&\big(a_0 + a_1 i + a_2 j + a_3 k\big) + \big(b_0 + b_1 i + b_2 j + b_3 k\big) = \\ &\big(a_0 + b_0\big) + \big(a_1 + b_1\big) i + \big(a_2 + b_2\big) j + \big(a_3 + b_3\big) k,\end{aligned}$$

و

$$\begin{aligned}&\big(a_0 + a_1 i + a_2 j + a_3 k\big)\big(b_0 + b_1 i + b_2 j + b_3 k\big) = \\ &\big(a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3\big) + \big(a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2\big) i + \\ &\big(a_0 b_2 + a_2 b_0 + a_3 b_1 - a_1 b_3\big) j + \big(a_0 b_3 + a_3 b_0 + a_1 b_2 - a_2 b_1\big) k.\end{aligned}$$

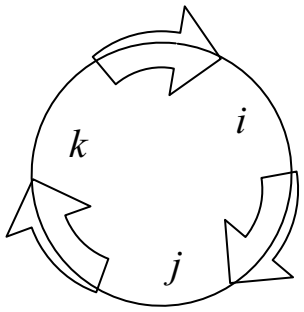
در این صورت $\mathbb{H}(\mathbb{R})$ همراه با جمع و ضرب اخیر یک حلقه است. این حلقه را **حلقه‌ی چهارگانی حقیقی** می‌نامند. به راحتی می‌توان بررسی کرد که فرمول‌های زیر برقرارند.

$$i^2 = j^2 = k^2 = ijk = -1. \qquad (*)$$

هم‌چنین با استفاده از (*) می‌توان نشان داد که تساوی‌های زیر نیز برقرارند.

$$ki = j = -ik\,, \quad jk = i = -kj, \quad ij = k = -ji$$

به سادگی می‌توان این تساوی‌ها را به خاطر سپرد. حاصل‌ضرب هر دو عنصر متوالی در جهت عقربه‌های ساعت، عنصر بعدی آن‌هاست، و حاصل‌ضرب هر دو عنصر متوالی در جهت خلاف عقربه‌های ساعت قرینه‌ی عنصر بعدی است. (شکل ۱-۱ ملاحظه شود).



شکل ۱-۱

□

در اوائل قرن نوزدهم، اهمیت اعداد مختلط روز به روز افزایش می‌یافت. **ویلیام رون هامیلتون**[1] (۱۸۰۵-۱۸۶۵) ریاضیدان معروف ایرلندی در سال ۱۸۳۳ اولین نمایش جدید از اعداد مختلط را مطرح نمود (مثال‌های ۷و۸ ملاحظه شوند). وی به‌دنبال توصیف مشابهی برای فضای سه بعدی، پس از ده سال تلاش فراوان، موفق به یافتن $\mathbb{H}(\mathbb{R})$ شد. هامیلتون این حلقه را حلقه‌ی **کواترنیون‌ها** نامید. اولین باری که معادلات (*) به‌ذهن هامیلتون رسید، در حال قدم زدن بود. اوبه‌قدری از یافتن این معادلات به‌وجد آمد که آن‌ها را با یک چاقو بر روی لبه‌ی پل بروقام[2] در دوبلین حک کرد. تاریخ این یادداشت ۶ اکتبر ۱۸۴۳ است.

مثال ۴: هرگاه $R_1, R_2, \dots, R_n$ حلقه باشند، با تعریف عمل‌های مؤلفه‌ای روی حاصل‌ضرب دکارتی آن‌ها؛ یعنی $R_1 \times R_2 \times \cdots \times R_n$، به‌صورت:

$$(r_1, r_2, \dots, r_n) + (s_1, s_2, \dots, s_n) = (r_1 + s_1, r_2 + s_2, \dots, r_n + s_n),$$
$$(r_1, r_2, \dots, r_n).(s_1, s_2, \dots, s_n) = (r_1 s_1, r_2 s_2, \dots, r_n s_n).$$

حلقه‌ای حاصل می‌شود که **حاصل‌ضرب مستقیم** حلقه‌های $R_1, R_2, \dots, R_n$ نام دارد.

□

قضیه ۱-۱

فرض کنیم R یک حلقه باشد. دراین‌صورت

(۱) برای هر $a \in R$، $0a = a0 = 0$،

(۲) برای هر $a, b \in R$، $a(-b) = (-a)b = -(ab)$،

(۳) برای هر $a, b \in R$، $(-a)(-b) = ab$،

(۴) برای هر $n \in \mathbb{Z}$ و هر $a, b \in R$، $(na)b = a(nb) = n(ab)$.

---

[1] William Rowan Hamilton
[2] Brougham

اثبات (۱): چون $0a = (0+0)a = 0a + 0a$، لذا طبق قانون حذف در گروه $(R,+)$ داریم $0a = 0$. به دلیل مشابه $a0 = 0$.

(۲): با توجه به(۱) داریم $0a = a(0) = a\big(b + (-b)\big) = ab + a(-b)$ و لذا $a(-b) = -(ab)$. به دلیل مشابه $(-a)b = -(ab)$.

(۳): با توجه به(۲) داریم $(-a)(-b) = -(-(a)b) = -(-(ab))$ و لذا $(-a)(-b) = ab$.

(۴): اگر $n = 0$، بنابر (۱) نتیجه حاصل است. فرض کنیم $k(ab) = (ka)b$ که $k > 0$. دراین‌صورت

$$(k+1)(ab) = k(ab) + ab = (ka)b + ab = (ka + a)b = \big[(k+1)a\big]b$$

و لذا طبق استقرا به ازای هر $n > 0$ مطلب ثابت شده است.
حال اگر $n < 0$، آن‌گاه

$$-\big((na)b\big) = (-na)b = -n(ab)$$

و لذا $(na)b = n(ab)$. بقیه‌ی اثبات مشابه است.

■■■

تعریف ۱-۴

زیر مجموعه‌ی S از حلقه‌ی R، یک **زیر حلقه** از R نامیده می‌شود، اگر با اعمال تعریف شده در R، خود یک حلقه باشد.

مثال ۵: فرض کنیم $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$. دراین‌صورت $\mathbb{Z}[i]$ زیر حلقه‌ای از $\mathbb{C}$ موسوم به حلقه‌ی **اعداد صحیح گاوسی**[1] است.

□

[1] Gaussian Integers

تعریف ۱-۵

فرض کنیم R و S دو حلقه باشند، تابع $\varphi : R \to S$ را یک **همریختی** (هممورفیسم) حلقه‌ای می‌نامیم اگر برای هر a و b در R:

(۱) $\varphi(a+b) = \varphi(a) + \varphi(b)$،

(۲) $\varphi(ab) = \varphi(a)\varphi(b)$.

همریختی $\varphi : R \to S$ را **تکریختی** (مونومورفیسم) حلقه‌ای گوییم، اگر φ یک‌به‌یک باشد.

همریختی $\varphi : R \to S$ را **برووریختی** (اپی‌مورفیسم) حلقه‌ای گوییم، اگر φ پوشا باشد.

همریختی $\varphi : R \to S$ را **یکریختی** (ایزومورفیسم) حلقه‌ای گوییم، اگر φ یک‌به‌یک و پوشا باشد.

یکریختی $\varphi : R \to R$ را یک **خودریختی** (اتومورفیسم) از R می‌نامیم.

R و S را **یکریخت** (ایزومورف) گوییم (و می‌نویسیم $R \cong S$)، هرگاه یک یکریختی مانند $\varphi : R \to S$ موجود باشد.

تعریف ۱-۶

فرض کنیم R و S دو حلقه باشند. گوییم R در S **قابل نشاندن** است اگر یک تکریختی $\varphi : R \to S$ موجود باشد؛ به عبارت دیگر، R با زیر حلقه‌ای از S یکریخت باشد.

مثال ۶: فرض کنیم n یک عدد طبیعی باشد. قرار می‌دهیم:

$$\gamma : \mathbb{Z} \to \mathbb{Z}_n$$
$$a \mapsto \overline{a}$$

جایی‌که $\overline{a}$ باقیمانده‌ی تقسیم عدد a به پیمانه‌ی n است. دراین‌صورت γ یک برووریختی است که به **برووریختی طبیعی** معروف است.

□

مثال ۷: فرض کنیم

$$R = \{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R}\}.$$

دراین‌صورت R یک زیر حلقه از $M_2(\mathbb{R})$ است و تابع

$$\varphi : \mathbb{C} \to R$$
$$a + bi \mapsto \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

یک یکریختی است؛ به‌عبارت دیگر $\mathbb{C}$ را می‌توان در $M_2(\mathbb{R})$ نشاند.

□

مثال ۸: فرض کنیم

$$R = \{\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \mid z, w \in \mathbb{C}\}.$$

دراین‌صورت R یک زیر حلقه از $M_2(\mathbb{C})$ است و تابع

$$\varphi : \mathbb{H} \to R$$
$$a + bi + cj + dk \mapsto \begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix}$$

یک یکریختی است؛ به‌عبارت دیگر $\mathbb{H}$ را می‌توان در $M_2(\mathbb{C})$ نشاند.

□

تعریف ۱-۷

فرض کنیم R حلقه‌ای یکدار باشد. گوییم عنصر $a \in R$ **معکوس چپ** دارد، اگر $b \in R$ چنان موجود باشد که $ba = 1$. همین‌طور، گوییم عنصر $a \in R$ **معکوس راست** دارد، اگر $c \in R$ چنان موجود باشد که $ac = 1$. عنصر $a \in R$ **معکوس‌پذیر (یکال)** گوییم اگر معکوس راست و چپ داشته باشد. مجموعه‌ی همه‌ی یکال‌های R که با R^* (یا $U(R)$) نمایش داده می‌شود، تحت عمل ضرب تشکیل یک گروه می‌دهد که به **گروه یکال‌های** R موسوم است.

❖ **تذکر:** اگر عنصر $a \in R$ معکوس‌پذیر باشد، آن‌گاه به آسانی می‌توان نشان داد که معکوس چپ و معکوس راست a با هم برابر است؛ بنابراین می‌توان گفت که عنصر $a \in R$ معکوس‌پذیر است اگر وفقط اگر عنصر $a^{-1} \in R$ چنان موجود باشد که $aa^{-1} = a^{-1}a = 1$. در این حالت عنصر a^{-1} را **معکوس** a گوییم.

مثال ۹: $\mathbb{Z}^* = \{-1,1\}$, $\mathbb{Z}_n^* = \{\overline{m} \in \mathbb{Z}_n \,|\, (m,n) = 1\}$.

□

مثال ۱۰: اگر $\mathbb{Z}[i] = \{a + bi | a,b \in \mathbb{Z}\}$ حلقه‌ی اعداد صحیح گاوسی باشد، آن‌گاه

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}.$$

برهان: فرض کنیم $u = a + bi$ یکالی از $\mathbb{Z}[i]$ باشد، چون $uu^{-1} = 1$، لذا:

$$| u |^2 \left|u^{-1}\right|^2 = \left|uu^{-1}\right|^2 = 1^2 = 1$$

اما $| u |^2 = a^2 + b^2$ یک عدد طبیعی است؛ بنابراین $| u |^2 = a^2 + b^2 = 1$. با توجه به این‌که a و b اعداد صحیح هستند، تنها جواب‌های ممکن عبارتند از:

$$(a,b)=(0,\pm1) \text{ یا } (a,b)=(\pm1,0)$$

بنابراین $\mathbb{Z}[i]^* = \{\pm1, \pm i\}$.

□

تعریف ۱-۸

فرض کنیم R حلقه‌ای یکدار باشد که $1_R \neq 0$. دراین‌صورت حلقه‌ی R را یک **حلقه‌ی بخشی (تقسیم)** گوییم هرگاه $R^* = R - \{0\}$؛ به‌عبارت دیگر هر عنصر غیر صفرش معکوس‌پذیر باشد. حلقه‌ی بخشی تعویض‌پذیر را **میدان** گوییم. زیر مجموعه‌ی F_1 از میدان F یک **زیر میدان** از F نامیده می‌شود، اگر با اعمال تعریف شده در F، خود یک میدان باشد.

مثال ۱۱: حلقه‌ی چهارگانی حقیقی، $\mathbb{H}(\mathbb{R})$، یک حلقه‌ی بخشی است.

حل: فرض کنیم $X = a_0 + a_1 i + a_2 j + a_3 k$ عنصر ناصفری از $\mathbb{H}(\mathbb{R})$ باشد. قرار می‌دهیم:

$$Y = (a_0 / b) - (a_1 / b)i - (a_2 / b)j - (a_3 / b)k,$$

که در این‌جا $b = a_0^2 + a_1^2 + a_2^2 + a_3^2$. به آسانی می‌توان ملاحظه نمود که $XY = 1 = YX$ و لذا $\mathbb{H}(\mathbb{R})$ یک حلقه‌ی بخشی است.

□

مثال ۱۲: $\mathbb{Q}$، $\mathbb{R}$، $\mathbb{C}$ و $\mathbb{Z}_p$ (p عددی اول) میدان هستند. در ضمن $\mathbb{Q}$ زیر میدانی از $\mathbb{R}$ و $\mathbb{R}$ زیرمیدانی از $\mathbb{C}$ است. □

قضیه‌ی معروفی به‌نام **قضیه ودربورن**[1] بیان می‌کند که هر حلقه‌ی بخشی متناهی لزوماً یک میدان است؛ به عبارت دیگر، حلقه‌ی بخشی متناهی تعویض‌ناپذیر وجود ندارد (بخش ۴ از فصل ۶ ملاحظه شود).

---

[1] Wedderburn's Theorem

قضیه ۱-۲

(۱) فرض کنیم $\{R_i\}_{i\in I}$ خانواده‌ای از زیرحلقه‌های حلقه‌ی R باشد. دراین‌صورت $\bigcap_{i\in I} R_i$ یک زیر حلقه‌ی R است.

(۲) فرض کنیم $\{F_i\}_{i\in I}$ خانواده‌ای از زیرمیدان‌های میدان F باشد. دراین‌صورت $\bigcap_{i\in I} F_i$ یک زیرمیدان F است.

اثبات: به‌عنوا ن‌تمرین به خواننده واگذار می‌شود.

■■■

تعریف ۱-۹

فرض کنیم R یک حلقه‌ی یکدار باشد. **مشخصه‌ی** حلقه‌ی R به‌صورت زیر تعریف می‌شود:

$$\mathrm{Char}R = \mathrm{Min}\{n \in \mathbb{N} \mid n1 = 0\},$$

و اگر برای هر $n \in \mathbb{N}$ داشته باشیم $n1 \neq 0$، قرار می‌دهیم $\mathrm{Char}R = 0$.

مثال ۳۰ : حلقه‌ی $\mathbb{Z}_n$ دارای مشخصه‌ی n بوده و حلقه‌های $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ دارای مشخصه‌ی 0 هستند.

□

تعریف ۱-۱۰

فرض کنیم R یک حلقه‌ی تعویض پذیر و یکدار باشد. عنصر $a \in R$ را یک **مقسوم‌علیه صفر** گوییم درصورتی‌که عنصر ناصفر $b \in R$ چنان موجود باشد که $ab = 0$. مجموعه‌ی همه‌ی عناصر مقسوم‌علیه صفر حلقه‌ی R را با نماد $Z(R)$ نمایش می‌دهیم.

تعریف ۱-۱۱

فرض کنیم R حلقه‌ای تعویض‌پذیر ویکدار باشد که $1_R \neq 0$. حلقه‌ی R را یک **دامنه‌ی صحیح** نامیم، اگر برای هر $a, b \in R$،

$$ab = 0 \text{ نتیجه دهد } a = 0 \text{ یا } b = 0$$

به‌عبارت دیگر، حلقه‌ی R یک دامنه‌ی صحیح است، اگر $Z(R) = \{0\}$.

مثال ۱۴ (الف): $\mathbb{Z}$ یک دامنه‌ی صحیح است،

(ب): هر میدان یک دامنه‌ی صحیح است.

□

قضیه ۱-۳

اگر R یک دامنه‌ی صحیح باشد، آن‌گاه مشخصه‌ی R یا صفر است یا عددی اول.

اثبات: به‌عنوان تمرین به خواننده واگذار می‌شود.

■■■

تعریف ۱-۱۲

فرض کنیم F یک میدان باشد. اشتراک همه‌ی زیرمیدان‌های F را **زیر میدان اول** F نامیم.

قضیه ۱-۴

فرض کنیم p یک عدداول، F یک میدان و P زیرمیدان اول F باشد.

(۱) اگر $\mathrm{Char}F = 0$، آن‌گاه $P \cong \mathbb{Q}$،

(۲) اگر $\mathrm{Char}F = p$، آن‌گاه $P \cong \mathbb{Z}_p$.

اثبات(۱): فرض کنیم $\mathrm{Char}F = 0$. دراین‌صورت به ازای هر عدد صحیح ناصفر n، داریم $n.1 = n.1_F \neq 0$ و لذا $(n.1)^{-1} \in F$. از این‌رو به آسانی می‌توان نشان داد که

$$P = \{(m.1)/(n.1) \mid m, n \in \mathbb{Z}, n \neq 0\}.$$

یک زیرمیدان از F است. از طرفی با توجه به تعریف زیرمیدان، هر زیر میدان از F باید شامل P باشد، پس P زیرمیدان اول F است. حال تعریف می‌کنیم:

$$\varphi : P \to \mathbb{Q}$$
$$(m.1)/(n.1) \mapsto m/n$$

به‌وضوح φ یک یکریختی است و لذا $P \cong \mathbb{Q}$.

(۲): فرض کنیم $\mathrm{Char}F = p$. دراین‌صورت به ازای هر عدد طبیعی $0 < n < p$، داریم $n.1 \neq 0$ و لذا $(n.1)^{-1} \in F$. ازاین‌رو به آسانی می‌توان نشان داد که

$$P = \{n.1 \mid 0 \leq n < p\}.$$

یک زیرمیدان از F است. از طرفی با توجه به تعریف زیرمیدان، هر زیر میدان از F باید شامل P باشد، پس P زیرمیدان اول F است. حال تعریف می‌کنیم:

$$\varphi : P \to \mathbb{Z}_p$$
$$(n.1) \mapsto \overline{n}$$

به‌سادگی دیده می‌شود که φ یکریختی است و لذا $P \cong \mathbb{Z}_p$.

■■■

تعریف ۱-۱۳

فرض کنیم R یک حلقه‌ی تعویض‌پذیر و یکدار بوده و $\mathbb{N}_0$ مجموعه‌ی اعداد صحیح نامنفی باشد. R را یک **حلقه‌ی اقلیدسی**[1] (به اختصار ER) نامیم اگر تابعی مانند $\upsilon : R - \{0\} \to \mathbb{N}_0$ موجود باشد به‌طوری‌که

(۱) به ازای هر $a, b \in R$، به‌قسمی که $ab \neq 0$، $\upsilon(a) \leq \upsilon(ab)$،

(۲) به ازای هر $a, b \in R$، به‌قسمی که $b \neq 0$، عناصر $q, r \in R$، وجود داشته باشند به‌طوری‌که، $a = bq + r$، که در این تساوی $r = 0$ یا $\upsilon(r) < \upsilon(b)$.

تابع υ را **تابع اقلیدسی**[2] در R می‌نامند. یک حلقه‌ی اقلیدسی که دامنه‌ی صحیح باشد را یک **دامنه‌ی اقلیدسی**[3] (به اختصار ED) نامیم.

[1] Euclidean Ring [2] Euclidean Function [3] Euclidean Domain

دلیل نام‌گذاری این حلقه‌ها به حلقه‌های اقلیدسی، کارآمد بودن الگوریتم اقلیدس، برای یافتن بزرگ‌ترین مقسوم‌علیه مشترک دو عنصر، بوده است(تمرین۷ از بخش۴).

مثال ۱۵: میدان F که در آن برای هر $x \in F$، $\upsilon(x) = 1$ یک دامنه‌ی اقلیدسی است.

□

مثال ۱۶: حلقه‌ی $\mathbb{Z}$ با $\upsilon(n) = \mid n \mid$، یک دامنه‌ی اقلیدسی است.

□

مثال ۱۷: حلقه‌ی اعداد صحیح گاوسی، $\mathbb{Z}[i]$ با $\upsilon(a+bi) = a^2 + b^2$ یک دامنه‌ی اقلیدسی است (تمرین۹).

تعریف ۱-۱۴

فرض کنیم I یک زیر حلقه از حلقه‌ی R باشد. I را یک **ایده‌آل** R گوییم اگر برای هر $r \in R$ و هر $a \in I$ داشته باشیم $ra \in I$ و $ar \in I$. ایده‌آل I از حلقه‌ی R را **ایده‌آل سره (حقیقی)** نامیم، اگر $I \neq R$.

مثال ۱۸: در حلقه‌ی R، $\{0\}$ و خود R ایده‌آل‌هایی از R هستند. ایده‌آل $\{0\}$را **ایده‌آل صفر** یا **ایده‌آل بدیهی** نامند.

□

مثال ۱۹: به ازای هر $n \in \mathbb{Z}$، $n\mathbb{Z}$ یک ایده‌آل $\mathbb{Z}$ است.

□

قضیه ۱-۵

فرض کنیم $\{I_\lambda \mid \lambda \in \Lambda\}$ خانواده ای از لیه‌آل‌های حلقه‌ی R باشد. دراین‌صورت $\bigcap_{\lambda\in\Lambda} I_\lambda$ یک لیه‌آل R است.

اثبات: به عنوا ن‌تمرین به خواننده واگذار می‌شود.

■■■

تعریف ۱-۱۵

فرض کنیم X زیر مجموعه‌ای از حلقه‌ی R باشد. در این صورت اشتراک تمام لیه‌آل‌های حلقه‌ی R که شامل X باشند را **ایده‌آل تولید شده** توسط X نامیده و آن را با $< X >$ نمایش می‌دهیم. اگر $X = \{x_1,...,x_n\}$، آن‌گاه $< X >$را با $< x_1,...,x_n >$ نمایش می‌دهیم.

عناصر X را **مولدهای** ایده‌آل $< X >$ نامیم. ایده‌آل Iاز R را **متناهی مولد** گوییم اگر زیر مجموعه‌ی متناهی $X = \{x_1,...,x_n\}$از R موجود باشد به‌طوری‌که $I =< x_1,...,x_n >$. اگر $X = \{x\}$ ، لیه‌آل $< x >$ را **ایده‌آل اصلی** تولید شده توسط x می‌نامیم. حلقه‌ی R را **حلقه‌ی ایده‌آل اصلی** (به اختصار PIR) گوییم اگر هر لیه‌آل آن اصلی باشد و حلقه‌ی R را **دامنه‌ی ایده‌آل اصلی** (به اختصار PID) گوییم اگر R یک دامنه‌ی صحیح و هر ایده‌آل آن اصلی باشد.

❖ **تذکر:** $< X >$ کوچک‌ترین ایده‌آل شامل X از حلقه‌ی R است.

قضیه ۱-۶

فرض کنیم R یک حلقه‌ی تعویض‌پذیر و یکدار بوده، $x \in R$ و $X \subseteq R$. دراین‌صورت

(۱) $< x >= Rx = \{rx | r \in R\}$،

(۲) $< X >= \{r_1x_1 + r_2x_2 + \cdots + r_mx_m \,|r_i \in R, x_i \in X, m \in \mathbb{N}\}$.

در حالت خاص، اگر $X = \{x_1, \ldots, x_n\}$، آن‌گاه

$$< X >= Rx_1 + Rx_2 + \cdots + Rx_n.$$

اثبات: قسمت (۲) را ثابت می‌کنیم. قسمت (۱) به‌راحتی از قسمت (۲) نتیجه می‌شود.

(۲): فرض کنیم $I = \{\sum_{i=1}^{m} r_ix_i \,|r_i \in R, x_i \in X, m \in \mathbb{N}\}$. به‌وضوح I ایده‌آلی شامل X است. بنابراین طبق تعریف $< X >$، داریم $< X > \subseteq I$. از طرفی هر ایده‌آل شامل X باید I را دربر داشته باشد. ازاین‌رو با استفاده‌ی مجدد از تعریف $< X >$، داریم $I \subseteq < X >$. درنتیجه $I =< X >$ و اثبات تمام است.

■■■

فرض کنیم $I_1, I_2, \ldots, I_n$ زیر مجموعه‌های غیر تهی از حلقه‌ی R باشند. تعریف می‌کنیم:

$$I_1 + I_2 + \cdots + I_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in I_n\}.$$

و اگر I و J دو زیر مجموعه‌ی غیر تهی از حلقه‌ی R باشند، قرار می دهیم:

$$IJ = \{a_1b_1 + \cdots + a_nb_n \,|a_i \in I, b_i \in J, n \in \mathbb{N}\},$$

و اگر $I = \{a\}$ به‌جای IJ می‌نویسیم aJ. همین‌طور اگر $J = \{b\}$، Ib را به‌جای IJ به‌کار می‌بریم.

توجه داشته باشیم که اگر J (یا I) نسبت به عمل جمع بسته باشد، آن‌گاه

$$\big(Ib = \{ab | a \in I\}\big) \quad aJ = \{ab | b \in J\}.$$

در حالت کلی، $I_1 I_2 \dots I_n$ را مجموعه‌ی تمام حاصل جمع‌های متناهی عباراتی به شکل

$$a_1 a_2 \dots a_n \qquad (a_i \in I, n \in \mathbb{N})$$

تعریف می‌کنیم. در حالت خاص که به ازای هر i، $1 \le i \le n$، $I_i = I$ را $I_1 I_2 \dots I_n$ با I^n نمایش می‌دهیم.

قضیه ۱-۷

فرض کنیم $I_1, I_2, \dots, I_n$ و I, J, K ایده‌آل‌هایی از حلقه‌ی R باشند. دراین‌صورت

(۱) $I_1 + I_2 + \cdots + I_n$ ، $I_1 I_2 \dots I_n$ لیه‌آل‌هایی از R هستند،

(۲) $(I + J) + K = I + (J + K)$،

(۳) $(IJ)K = I(JK)$،

(۴) $J\big(I_1 + I_2 + \cdots + I_n\big) = JI_1 + JI_2 + \cdots + JI_n$،

اثبات: به عنوا ن‌تمرین به خواننده واگذار می‌شود.

■■■

قضیه ۱-۸

(۱) هرحلقه‌ی اقلیدسی یک حلقه ی لیه‌آل اصلی است؛ به‌عبارت دیگر،

$$\mathrm{ER} \Rightarrow \mathrm{PIR}.$$

(۲) هر دامنه‌ی اقلیدسی یک دامنه ی لیه‌آل اصلی است؛ به‌عبارت دیگر،

$$\mathrm{ED} \Rightarrow \mathrm{PID}.$$

اثبات (۱): فرض کنیم I لیه‌آل ناصفری از حلقه‌ی R باشد. نشان می‌دهیم I یک لیه‌آل اصلی است. قرار می‌دهیم:

$$S = \{v(x) \mid x \neq 0, x \in I\}.$$

فرض کنیم $v(a)$ عنصر مینیمال S باشد. ادعا می‌کنیم $I =< a >$. به‌وضوح $< a >\subseteq I$. حال فرض کنیم $0 \neq b \in I$. در این صورت عناصر $q, r \in R$، وجود دارند به‌طوری‌که، $b = aq + r$. در این تساوی $r = 0$ یا $v(r) < v(a)$. با توجه به مینیمال بودن $v(a)$ و این‌که $r = b - aq \in I$، رابطه‌ی $v(r) < v(a)$ برقرار نیست. لذا $r = 0$ و $b = aq \in < a >$؛ یعنی $I =< a >$.

(۲): به آسانی از (۱) نتیجه می‌شود.

■■■

❖ **تذکر:** عکس قسمت‌های (۱) و (۲) قضیه‌ی اخیر برقرار نیست. برای دیدن این مطلب خواننده به بخش ۶ از فصل ۶ مراجعه نماید.

اینک، مفهوم گروه‌های خارج قسمتی را به حلقه‌های خارج قسمتی تعمیم می‌دهیم.

لم ۱-۱

فرض کنیم I یک زیر گروه جمعی حلقه‌ی R باشد. دراین‌صورت شرایط زیر معادلند.

(۱) عمل ضرب $(a + I)(b + I) = ab + I$ روی گروه خارج‌قسمتی جمعی R / I خوش تعریف است،

(۲) I لیه‌آلی از حلقه‌ی R است.

اثبات (۱) $\Leftarrow$ **(۲):** فرض کنیم $r \in R$ و $a \in I$. دراین‌صورت با توجه به (۱):

$$(ra + I) = (r + I)(a + I) = (r + I)(0 + I) = 0 + I = I$$

این نتیجه می‌دهد که $ra \in I$. به‌طریق مشابه ثابت می‌شود که $ar \in I$.

(۲) $\Leftarrow$ **(۱):** اگر $a + I = a' + I$ و $b + I = b' + I$، باید نشان دهیم $ab + I = a'b' + I$. داریم $a - a' \in I$ و $b - b' \in I$. ازاین‌رو

$$ab - a'b' = a\big(b - b'\big) + \big(a - a'\big)b' \in aI + Ib' \subseteq I + I = I.$$

بنابراین $ab + I = a'b' + I$.

■■■

قضیه ۱-۹

فرض کنیم I ایده‌آلی از حلقه‌ی R باشد. دراین‌صورت، گروه خارج قسمتی جمعی R/I همراه با $(a+I)(b+I)=ab+I$ یک حلقه است.

اثبات: با توجه به لم قبل، عمل ضرب خوش تعریف است. در مورد قانون شرکت‌پذیری داریم:

$$\begin{aligned}\big((a+I)(b+I)\big)(c+I) &= (ab+I)(c+I)\\ &= (ab)c+I\\ &= a(bc)+I\\ &= (a+I)(bc+I)\\ &= (a+I)\big((b+I)(c+I)\big)\end{aligned}$$

اثبات قانون توزیع‌پذیری را به خواننده واگذار می‌کنیم.

■■■

تعریف ۱-۱۶

لیه‌آل سره‌ی P از حلقه‌ی تعویض‌پذیر و یکدار R را یک **ایده‌آل اول** گوییم، اگر برای هر $a,b\in R$،

$$ab\in P \text{ نتیجه دهد } a\in P \text{ یا } b\in P$$

مجموعه ی لیه‌آل‌های اول حلقه‌ی تعویض‌پذیر و یکدار R را با نماد $\mathrm{Spect}(R)$ نمایش می‌دهیم.

مثال۲۰: $\mathrm{Spect}(\mathbb{Z})=\{<p>\mid p \text{ یک عدد اول باشد}\}$.

□

لیه‌آل‌های اول به صورت زیر شناسایی می‌شوند.

قضیه ۱-۱۰

ایده‌آل P از حلقه‌ی تعویض‌پذیر ویکدار R اول است اگر و فقط اگر R/P یک دامنه‌ی صحیح باشد.

اثبات: فرض کنیم P ایده‌آل اولی از حلقه‌ی R باشد. چون $P \neq R$، $1+P \neq 0+P$. فرض کنیم $(a+P)(b+P)=P$. بنابراین $ab+P=P$ و لذا $ab \in P$. چون P ایده‌آل اولی در حلقه‌ی تعویض‌پذیر R است، $a \in P$ یا $b \in P$. یعنی $a+P=P$ یا $b+P=P$. لذا R/P یک حوزه‌ی صحیح است. به عکس، اگر R/P دامنه صحیح باشد، آن‌گاه $1+P \neq 0+P$ و لذا $P \neq R$. حال اگر $ab \in P$ آن‌گاه $ab+P=P$ و درنتیجه $(a+P)(b+P)=P$. ازاین‌رو $a+P=P$ یا $b+P=P$؛ بنابراین $a \in P$ یا $b \in P$ و بنابر تعریف P اول است.

■■■

تعریف ۱-۱۷

ایده‌آل M از حلقه‌ی تعویض‌پذیر و یکدار R را یک **ایده‌آل ماکزیمال** گوییم هرگاه $M \neq R$ و به ازای هر ایده‌آل I از R، اگر $M \subsetneq I \subseteq R$، آن‌گاه $I=R$. مجموعه‌ی ایده‌آل‌های ماکزیمال حلقه‌ی R را با نماد $\mathrm{Max}(R)$ نمایش می‌دهیم.

اکنون یک شرط لازم و کافی را برای ماکزیمال بودن یک ایده‌آل در یک حلقه‌ی تعویض‌پذیر و یکدار ارائه می‌دهیم.

قضیه۱-۱۱

فرض کنیم R یک حلقه‌ی تعویض پذیر و یکدار و M ایده‌آلی از R باشد. دراین‌صورت M ماکزیمال است اگر و فقط اگر R/M یک میدان باشد.

اثبات: فرض کنیم M یک ایده‌آل ماکزیمال از حلقه‌ی R باشد. دراین‌صورت $1+M \neq 0+M$. اگر $a+M$ عنصر غیر صفری از R/M باشد، آن‌گاه $a \notin M$ و با توجه به ماکزیمال بودن M داریم $Ra+M=R$. ازاین‌رو $ra+m=1$ که در آن $m \in M, r \in R$. حال داریم:

$$1+M = ra+m+M = ra+M = (r+M)(a+M),$$

یعنی $r+M$ معکوس $a+M$ می‌باشد و در نتیجه R/M یک میدان است.

برعکس، فرض کنیم R/M یک میدان باشد. دراین‌صورت $1+M \neq 0+M$ و لذا $M \neq R$. حال فرض کنیم I ایده‌آلی از R باشد که $M \subsetneq I \subseteq R$. بنابراین $a \in I$ موجود است که $a \notin M$. چون $a+M$ عنصر غیر صفری از حلقه‌ی R/M است، پس عنصر $b+M \in R/M$ موجود است به‌طوری‌که $(a+M)(b+M)=1+M$. ازاین‌رو عنصری مانند $m \in M$ موجود است به‌گونه‌ای که $ab+m=1$. در نتیجه $1 \in I$؛ یعنی $I=R$.

■■■

نتیجه‌ی زیر به‌آسانی از قضیه‌ی ۱-۱۰ و قضیه‌ی ۱-۱۱ به‌دست می‌آید.

نتیجه ۱-۱

فرض کنیم R یک حلقه‌ی تعویض پذیر و یکدار باشد. دراین‌صورت

$$\mathrm{Max}(R) \subseteq \mathrm{Spec}(R).$$

◆ **تذکر:** عکس قضیه‌ی اخیر برقرار نیست. به‌عنوان مثال $\{0\}$ یک ایده‌آل اول حلقه‌ی $\mathbb{Z}$ است درصورتی‌که ماکزیمال نیست.

تعریف ۱-۱۸

گوییم R در شرط ACC (**شرط زنجیر صعودی**) روی ایده‌آل‌هایش صدق می کند اگر هر زنجیر صعودی از ایده‌آل‌های آن ایستا باشد؛ به عبارت دیگر، اگر

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

یک زنجیر صعودی از لیه‌آل‌های R باشد، آن‌گاه $k \in \mathbb{N}$ موجود باشد به‌طوری‌که

$$I_k = I_{k+1} = I_{k+2} = \cdots .$$

تذکر: حلقه‌ی R را **نوتری**[1] گوییم اگر در شرط ACC صدق کند.

قضیه ۱-۱۲

شرایط زیر روی حلقه‌ی R معادلند.

(۱) R در شرط ACC روی لیه‌آل‌هایش صدق می‌کند،

(۲) هر خانواده‌ی غیر تهی از ایده‌آل‌های R دارای عنصر ماکزیمال است،

(۳) هر لیه‌آل R متناهی مولد است.

اثبات (۲) $\Rightarrow$**(۱)**: فرض کنیم Ω یک خانواده‌ی غیر تهی از ایده‌آل‌های R باشد که دارای عنصر ماکزیمال نیست. فرض کنیم $I_1 \in \Omega$، چون Ω دارای عنصر ماکزیمال نیست، $I_2 \in \Omega$ وجود دارد که $I_1 \subsetneq I_2$. دوباره چون Ω دارای عنصر ماکزیمال نیست، $I_3 \in \Omega$ وجود دارد که $I_1 \subsetneq I_2 \subsetneq I_3$. با ادامه‌ی این روند زنجیر صعودی ناایستای

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subsetneq I_t \subsetneq \cdots,$$

را خواهیم داشت، که با (۱) در تناقض است.

(۳) $\Rightarrow$**(۲)**: فرض کنیم I لیه‌آلی از R باشد. قرار می‌دهیم:

$$\Omega = \{J \mid J \subseteq I \text{ و } R \text{ یک ایده‌آل متناهی مولد حلقه‌ی } J\}.$$

چون $< 0 > \in \Omega$، لذا $\Omega \neq \varnothing$. بنابراین طبق فرض Ω دارای عنصر ماکزیمال است. فرض کنید J عنصر ماکزیمال Ω باشد. اگر $x \in I$، آن‌گاه $J + < x > \in \Omega$ و لذا با توجه به ماکزیمال بودن J خواهیم داشت $J + < x > = J$. بنابراین $x \in J$ و در نتیجه $J = I$. ازاین‌رو I متناهی مولد است.

(۱) $\Rightarrow$**(۳)**: فرض کنیم $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ یک زنجیر صعودی از لیه‌آل‌های R باشد. قرار می‌دهیم $I = \bigcup_{k=1}^{\infty} I_k$. به‌وضوح I یک ایده‌آل R است. چون I متناهی مولد است،

---

[1] Noetherian

پس $I =< x_1, x_2, \ldots, x_n >$. اگر $(1 \le i \le n)\, x_i \in I_{k_i}$ و $k = \max\{k_i\}_{i=1}^{n}$، آن‌گاه با توجه به صعودی بودن زنجیر خواهیم داشت، $I \subseteq I_k$ و لذا

$$I = I_k = I_{k+1} = I_{k+2} = \cdots.$$

■■■

تمرین‌های سطح۱

۱- (الف) (آزمون زیر حلقه بودن) زیر مجموعه‌ی ناتهی S از حلقه‌ی R یک زیر حلقه است، هرگاه به ازای هر $a,b \in S$ داشته باشیم:

$$a-b,\ ab \in S$$

(ب)(آزمون زیر میدان بودن) زیر مجموعه‌ی ناتهی E از میدان F یک زیر میدان است، هرگاه به ازای هر $a,b \in E$ که $b \neq 0$، داشته باشیم:

$$a-b,\ ab^{-1} \in E$$

۲- فرض کنید $\varphi : R \to S$ را یک همریختی حلقه‌ای باشد. قرار می‌دهیم:

$$\mathrm{Im}\varphi = \varphi \textbf{ تصویر} = \{\varphi(x) \mid x \in R\},$$

$$\mathrm{Ker}\varphi = \varphi \textbf{ هسته} = \{x \in R \mid \varphi(x) = 0\}.$$

نشان دهید:

(الف) $\mathrm{Im}\varphi$ زیر حلقه‌ای از S است، **(ب)** $\mathrm{Ker}\varphi$ ایده‌آلی از R است.

۳- مشخصه‌ی هر یک از حلقه‌های زیر را بیابید.

(الف) $\mathbb{Z}_3 \times \mathbb{Z}_4$، **(ب)** $\mathbb{Z}_3 \times \mathbb{Z}$.

۴-مطلوب است تمامی عناصر یکال و مقسوم علیه صفر حلقه‌ی $\mathbb{Z}_5 \times \mathbb{Z}_{10}$.

۵-فرض کنید $R_1, \ldots, R_n$ حلقه‌هایی یکدار باشند. نشان دهید

$$U(R_1 \times \ldots \times R_n) = U(R_1) \times \ldots \times U(R_1).$$

۶- فرض کنید R یک حلقه باشد. عنصر $a \in R$ را **پوچ‌توان** گوییم اگر عدد طبیعی n چنان موجود باشد که $a^n = 0$. نشان دهید مجموعه‌ی همه‌ی عناصر پوچ‌توان حلقه‌ی تعویض‌پذیر R تشکیل یک ایده‌آل می‌دهند.

۷- فرض کنید R یک حلقه باشد. دراین‌صورت

(الف) فرض کنید $a \in R$ یک عنصر پوچ‌توان باشد. نشان دهید $1 + a$ یکال است،

(ب) نشان دهید مجموع یک عنصر یکال با یک عنصر پوچ‌توان از حلقه‌ی R، یک عنصر یکال از حلقه‌ی R است.

۸- عناصر a و b از حلقه‌ی تعویض‌پذیر R را بیابید چنان که $a, b \in Z(R)$ ولی $a + b \notin Z(R)$.

۹- نشان دهید $I = \{(n, 0) \mid n \in \mathbb{Z}\}$ ایده‌آل اولی از حلقه $\mathbb{Z} \times \mathbb{Z}$ است که ماکزیمال نیست.

۱۰- تابع ϕ اویلر[1] به ازای هر عدد طبیعی n به‌صورت زیر تعریف می شود:

$\phi(n) =$ تعداد اعداد طبیعی $1 \le m < n$، که نسبت به n اولند

(الف) نشان دهید $| \mathbb{Z}_n^* | = \phi(n)$، **(ب)** نشان دهید $n = \sum_{d \mid n} \phi(d)$.

۱۱- فرض کنید R یک حلقه‌ی تعویض‌پذیر و یکدار، با مشخصه‌ی عدد اول p باشد. تابع زیر را در نظر بگیرید.

$$\varphi : R \to R$$
$$a \mapsto a^p$$

نشان دهید:

(الف) φ یک همریختی حلقه‌ای است،

(ب) اگر R یک میدان باشد، φ یک تکریختی است،

---

[1] Euler ϕ Function

(ج) اگر $R \cong Z_p$، نشان دهید φ یک یکریختی است.

تمرین‌های سطح ۲

۱۲- نشان دهید حلقه‌ی اعداد صحیح گاوسی، $\mathbb{Z}[i]$ با $\upsilon(a+bi)=a^2+b^2$ یک دامنه‌ی اقلیدسی است.

۱۳- فرض کنید R یک حلقه‌ی تعویض‌پذیر و متناهی باشد که $Z(R)=\{0\}$. نشان دهید R یک میدان است.

۱۴- اگر R حلقه‌ای تعویض‌پذیر ویکدار باشدکه دامنه‌ی صحیح نیست، نشان دهید:

$$|Z(R)|<\infty \Leftrightarrow |R|<\infty.$$

۱۵- (قضیه‌ی ویلسون[1]**)** فرض کنیم $n \geq 2$ یک عدد صحیح باشد. نشان دهید $(n-1)!\overset{n}{\equiv}-1$ اگر و فقط اگر n یک عدد اول باشد.

تمرین‌های سطح ۳

۱۶- فرض کنید R حلقه‌ای تعویض‌پذیر و یکدار و $|R|=p_1p_2\dots p_n$، که p_iها اعداد اول متمایز هستند. نشان دهید R دقیقاً n ایده‌آل اول متمایز دارد. در مورد $|R|=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$ چه می‌توان گفت؟

۱۷- نشان دهید $\mathbb{Z}_n$ برای $n \geq 2$ دارای 2^d عنصر خودتوان است (d تعداد مقسوم علیه‌های اول n است).

۱۸- (الف) حلقه‌ای مانند R و عناصر $a,b \in R$ بیابید که $ab=0$ ولی $ba \neq 0$.

(ب) حلقه‌ای یکدار مانند R و عناصر $a,b \in R$ بیابید که $ab=1$ ولی $ba \neq 1$.

---

[1] Wilson's Theorem

۱-۲ حلقه‌ی چندجمله‌ای‌ها

در این بخش به تعریف دقیق حلقه‌ی چند جمله‌ای ها می‌پردازیم وسپس خواص اساسی این حلقه را مورد بررسی قرار می‌دهیم.

قضیه ۱-۱۳

فرض کنیم R یک حلقه‌ی تعویض‌پذیر و یکدار باشد. قرار می دهیم:

$P(R) = \{(a_0, a_1, a_2, \ldots) \mid a_n \in R$، فقط تعداد متناهی از a_nها غیر صفر باشند$\}$.

دراین‌صورت:

(۱) $P(R)$ همراه با اعمال زیر یک حلقه است.

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),$$
$$(a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots).$$

(۲) نگاشت زیر یک تکریختی است.

$$\varphi : R \to P(R)$$
$$a_0 \mapsto (a_0, 0, 0, \ldots)$$

(۳) اگر $x := (0,1,0,\ldots)$ و حلقه‌ی R را با تصویر تکریخت آن یعنی $\varphi(R)$ یکی بگیریم،آن‌گاه

$$P(R) = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R, n \geq 0\}.$$

اثبات: به‌عنوان تمرین به خواننده واگذار می‌شود.

■■■

تعریف ۱-۱۹

فرض کنیم R یک حلقه‌ی تعویض‌پذیر و یکدار باشد. حلقه‌ی $P(R)$ را **حلقه‌ی چند جمله‌ای‌ها** روی R گوییم و با نماد $R[x]$ نمایش می‌دهیم. عناصر $R[x]$ را **چند جمله‌ای** می‌نامیم. فرض کنیم

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x].$$

عناصر $a_0, a_1, \ldots, a_n$ را **ضرایب** چندجمله‌ای $f(x)$ می‌نامیم. اگر $a_n \neq 0$، a_n را **ضریب پیشروی** $f(x)$ می‌خوانیم و گوییم $f(x)$ از **درجه‌ی** n است و می‌نویسیم

$$\deg f(x) = n.$$

اگر $a_n = 1$، آن‌گاه $f(x)$ را یک **چند جمله‌ای تکین** می‌نامیم. برای راحتی درجه‌ی چند جمله‌ای صفر را $-\infty$ تعریف می‌کنیم.

قضیه ۱-۱۴

فرض کنیم R یک دامنه‌ی صحیح باشد.

(۱) اگر $f(x), g(x) \in R[x]$، آن‌گاه

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

(۲) $R[x]$ نیز یک دامنه‌ی صحیح است.

اثبات (۱): اگر $f(x)$ یا $g(x)$ چند جمله‌ای صفر باشند حکم به‌وضوح برقرار است. حال فرض کنید

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$
$$g(x) = a_0 + a_1x + \cdots + a_mx^m,$$

که در آن $a_n \neq 0$ و $a_m \neq 0$. دراین‌صورت

$$f(x)\,g(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + \cdots + a_nb_mx^{n+m}.$$

چون R دامنه‌ی صحیح است، لذا $a_n b_m \neq 0$ و در نتیجه
$$\deg f(x)g(x) = m + n = \deg f(x) + \deg g(x).$$

(۲): اگر $f(x), g(x) \in R[x]$ و $f(x)g(x) = 0$، آن‌گاه $\deg f(x)g(x) = -\infty$ و ازاین‌رو $f(x) = 0$ یا $g(x) = 0$. بدین‌ترتیب $R[x]$ یک دامنه‌ی صحیح است.

■■■

قضیه۱- ۱۵ (الگوریتم تقسیم)

فرض کنیم R یک حلقه‌ی تعویض پذیر و یکدار باشد. فرض کنیم $f(x), g(x) \in R[x]$ که $g(x) \neq 0$ و ضریب پیشروی $g(x)$ یکال است. دراین‌صورت چند جمله‌ای‌های یکتای $q(x), r(x) \in R[x]$ وجود دارند که

$$f(x) = g(x)q(x) + r(x) \text{ و } \deg r(x) < \deg g(x)$$

اثبات (وجود): فرض کنیم

$$S = \{f(x) - g(x)h(x) \mid h(x) \in R[x]\}.$$

به‌وضوح $S \neq \varnothing$، زیرا $f(x) \in S$. اگر $0 \in S$، آن‌گاه چندجمله‌ای $h(x) \in R[x]$ وجود دارد به‌طوری‌که $f(x) - g(x)h(x) = 0$ واز آن‌جا $f(x) = g(x)h(x)$. در نتیجه $q(x) = h(x)$ و $r(x) = 0$ در شرایط قضیه صدق می‌کند. حال فرض کنیم $0 \notin S$. دراین‌صورت عناصر S از درجه‌ی نامنفی بوده و لذا طبق اصل خوش ترتیبی، S دارای عنصری با کوچک‌ترین درجه، مانند $r(x)$ خواهد بود. بنابراین $q(x) \in R[x]$ موجود است به‌طوری‌که

$$f(x) - g(x)q(x) = r(x),$$

حال فرض کنیم $\deg r(x) \geq \deg g(x)$ (فرض خلف). اگر

$$g(x) = a_0 + a_1 x + \cdots + a_n x^n,$$
$$r(x) = b_0 + b_1 x + \cdots + b_m x^m,$$

که در آن $a_n, b_m \neq 0$، آن‌گاه با توجه به این‌که $m \geq n$ خواهیم داشت

$$\alpha(x) := r(x) - (b_m / a_n)x^{m-n}g(x) = f(x) - g(x)h(x) - (b_m / a_n)x^{m-n}g(x)$$
$$= f(x) - g(x)(h(x) - (b_m / a_n)x^{m-n}) \in S.$$

از طرف دیگر $\deg \alpha(x) < \deg r(x)$، که با انتخاب $r(x)$ در تناقض است. لذا $\deg r(x) < \deg g(x)$.

(یکتایی): فرض کنیم

$$f(x) = g(x)q(x) + r(x)\text{ ، }\deg r(x) < \deg g(x)$$

$$f(x) = g(x)q_1(x) + r_1(x)\text{ ، }\deg r_1(x) < \deg g(x)$$

دراین‌صورت $r(x) - r_1(x) = g(x)(q_1(x) - q(x))$. چون ضریب پیشروی $g(x)$ یکال است، داریم

$$\deg(q_1(x) - q(x)) = \deg(r(x) - r_1(x)) - \deg g(x) < 0.$$

ازاین‌رو $\deg(q_1(x) - q(x)) = -\infty$ و در نتیجه $q_1(x) - q(x) = 0$ و بنابراین $r_1(x) - r(x) = 0$. بدین ترتیب $q_1(x) = q(x)$ و لذا $r_1(x) = r(x)$.

■■■

تعریف ۱-۲۰

فرض کنیم R زیرحلقه‌ای از حلقه‌ی تعویض‌پذیر و یکدار S باشد. عنصر $u \in S$ را یک **ریشه** از چند جمله‌ای $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ گوییم، اگر

$$f(u) := a_0 + a_1u + \cdots + a_nu^n = 0.$$

نتیجه۱-۲

فرض کنیم R یک دامنه‌ی صحیح بوده و $f(x) \in R[x]$ و $a \in R$. دراین‌صورت

$f(a) = 0 \Leftrightarrow (x - a)$ عاملی از $f(x)$ باشد.

اثبات ($\Leftarrow$): اگر $f(a)=0$، طبق قضیه‌ی قبل چندجمله‌ای‌های $q(x), r(x) \in R[x]$ موجوداند که $f(x)=(x-a)q(x)+r(x)$، و $\deg r(x)=0$؛ یعنی $r(x)=b \in R$. از طرفی چون $r(a)=0$، پس $b=0$. در نتیجه $f(x)=(x-a)q(x)$.

($\Rightarrow$): حال فرض کنیم $(x-a)$عاملی از $f(x)$ باشد. دراین‌صورت چند جمله‌ای $q(x)$ موجود است چنان که $f(x)=(x-a)q(x)$؛ بنابراین $f(a)=0$.

■■■

نتیجه۱-۳

فرض کنیم R یک دامنه‌ی صحیح بوده و $f(x) \in R[x]$ و $\deg f(x)=n \geq 0$. دراین‌صورت $f(x)$دارای حداکثر n ریشه‌ی متمایز در R است.

اثبات: حکم را به‌وسیله استقرا روی n ثابت می‌کنیم. اگر $n=0$، آن‌گاه $f(x)=c \neq 0$و لذا $f(x)$ ریشه‌ای در Rندارد. حال فرض کنیم $n>0$. اگر $f(x)$ هیچ ریشه‌ای در R نداشته باشد، مطلب اثبات شده است. پس فرض کنیم $f(x)$ دارای ریشه‌ای مانند aدر R باشد. با توجه به نتیجه‌ی قبل چند جمله‌ای $q(x) \in R[x]$ به‌گونه‌ای موجود است که $f(x)=(x-a)q(x)$. اگر $b \in R$ریشه‌ای از $f(x)$ به‌جز a باشد، آن‌گاه

$$f(b)=(b-a)q(b)=0.$$

بنابراین با توجه به این‌که $b-a \neq 0$، خواهیم داشت $q(b)=0$، یعنی b ریشه‌ای از $q(x)$ است. بنابر فرض استقرا $q(x)$دارای حداکثر $n-1$ ریشه‌ی متمایز در R است. بنابراین نتیجه می‌شود که $f(x)$ دارای حداکثر n ریشه‌ی متمایز در R است.

■■■

تعریف ۱-۲۱

میدان Fرا **به‌طور جبری بسته** نامیم، اگر هر چندجمله‌ای غیرثابت از $F[x]$دارای ریشه‌ای در F است.

یکی از مهم‌ترین ویژگی‌های $\mathbb{C}$، میدان اعداد مختلط، که آن‌را بدون اثبات بیان خواهیم کرد، به‌طور جبری بسته بودن است.

قضیه۱- ۱۶(قضیه‌ی اساسی جبر)

میدان اعداد مختلط، $\mathbb{C}$، به‌طور جبری بسته $\mathbb{C}$ است.

اثبات این قضیه، برخلاف نامش، جبری نیست. همه‌ی اثبات‌های معروف با تکنیک‌های آنالیزی یا توپولوژیکی درگیر هستند. برای دیدن اثباتی از این قضیه، می‌توان صفحه‌ی ۲۲۲ منبع قابل دسترس زیر را ملاحظه نمود (در ضمن، چند اثبات ساده از این قضیه در بخش ۴ از فصل ۶ آورده شده است).

رودین، والتر. **اصول آنالیز ریاضی**. ترجمه‌ی عالم زاده، علی اکبر. انتشارات علمی و فنی (۱۳۶۲).

این بخش را با معرفی حلقه‌ی چند جمله‌ای‌های nمتغیره روی حلقه‌ی R به پایان می‌رسانیم.

تعریف ۱-۲۲

فرض کنیم R یک حلقه‌ی تعویض‌پذیر و یکدار باشد. حلقه‌ی nمتغیره روی Rبه استقرا به‌صورت زیر تعریف می‌شود.

$$R[x_1,\ldots,x_n] = (R[x_1,\ldots,x_{n-1}])[x_n].$$

تمرین‌های سطح۱

۱- فرض کنید R یک دامنه‌ی صحیح باشد. ثابت کنید $(R[x])^* = R^*$؛ به عبارت دیگر، عناصر معکوس‌پذیر حلقه‌های $R[x]$ و R برابرند.

۲- فرض کنید F یک میدان باشد. نشان دهید $F[x]$ یک دامنه‌ی اقلیدسی است.

۳- فرض کنید R یک دامنه‌ی صحیح باشد. ثابت کنید $R[x,y]$ یک دامنه‌ی ایده‌آل اصلی نیست.

۴- ثابت کنید $\mathbb{Z}[x]$ یک دامنه‌ی ایده‌آل اصلی نیست.

۵- فرض کنید R یک حلقه‌ی تعویض پذیر و یکدار باشد. ثابت کنید $(R[x])[y] \cong (R[y])[x]$. به‌عبارت‌دیگر

$$R[x,y] \cong R[y,x].$$

تمرین‌های سطح۲

۶- فرض کنید R یک حلقه‌ی تعویض‌پذیر و یکدار و $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. دراین‌صورت

(الف) f در $R[x]$ یکال است $\Leftrightarrow$ a_0 در R یکال بوده و $a_1, a_2, \ldots, a_n$ پوچ‌توان باشند.

(ب) f پوچ‌توان است $\Leftrightarrow$ $a_0, a_1, \ldots, a_n$ پوچ‌توان باشند.

(پ) f مقسوم علیه صفر است $\Leftrightarrow$ عنصر ناصفر $a \in R$ موجود باشد که $af = 0$.

۷-فرض کنیم p یک عدد اول باشد . نشان دهید در $\mathbb{Z}_p[x]$ رابطه‌ی زیر برقرار است.

$$x^p - 1 = (x-1)(x-2)\ldots(x-(p-1)).$$

تمرین‌های سطح ۳

۸-فرض کنید $\mathbb{C}$ میدان اعداد مختلط باشد. نشان دهید

$$\mathrm{Max}\mathbb{C}[x_1,\ldots,x_n] = \{(x_1 - a_1,\ldots,x_n - a_n) \mid a_i \in \mathbb{C}\}$$

آیا تمرین اخیر برای میدان اعداد حقیقی $\mathbb{R}$ برقرار است؟

۹- نشان دهید $R[x]$ یک حلقه‌ی ایده‌آل اصلی است اگر و فقط اگر $R \cong F_1 \times \cdots \times F_n$، که F_iها میدان هستند.

۱-۳ میدان کسرها

در این بخش، طرز ساخت اعداد گویا از طریق اعداد صحیح را تعمیم خواهیم داد.

قضیه ۱-۱۷

فرض کنیم R یک دامنه‌ی صحیح باشد و $S = R \setminus \{0\}$. در این صورت رابطه‌ی زیر یک رابطه‌ی هم ارزی روی $R \times S$ است:

$$(r,s) \sim (r',s') \Leftrightarrow rs' = sr'$$

اثبات: به عنوا ن‌تمرین به خواننده واگذار می‌شود.

■■■

نمادگذاری: فرض کنیم R یک دامنه‌ی صحیح باشد. کلاس هم ارزی $(r,s) \in R \times S$ را با r/s نمایش داده و قرار می‌دهیم:

$$F = \{r/s \mid r \in R, s \in S\}.$$

قضیه ۱-۱۸

فرض کنیم R یک دامنه‌ی صحیح باشد و $S = R \setminus \{0\}$. دراین‌صورت F همراه با اعمال جمع و ضرب زیر یک میدان است.

$$r/s + r'/s' = (rs' + sr')/ss',$$
$$(r/s)(r'/s') = (rr'/ss').$$

اثبات (۱): ابتدا نشان می‌دهیم که عمل جمع خوش تعریف است. فرض کنیم $r/s = r_1/s_1$ و $r'/s' = r_1'/s_1'$. دراین‌صورت

$$rs_1 = sr_1,$$
$$r's_1' = s'r_1'.$$

با ضرب معادله‌ی اول در $s's_1'$ و معادله‌ی دوم در ss_1 و جمع آن‌ها داریم:

$$\left(rs' + sr'\right)s_1s_1' = \left(r_1s_1' + s_1r_1'\right)ss'.$$

بنابراین $(rs' + r's)/ss' = (r_1s_1' + r_1's_1)/s_1s'$؛ یعنی عمل جمع خوش تعریف است. به طریق مشابه، می‌توان دید که عمل ضرب نیز خوش تعریف است. برای هر $s \in S$ عنصر $0/s = 0/1$ عنصر همانی جمعی F و $s/s = 1/1$ عنصر همانی عمل ضرب F است. تعویض‌پذیر بودن F به‌وضوح از تعویض‌پذیر بودن R نتیجه می‌شود. فرض کنیم r/s عنصر غیر صفری از F باشد، دراین‌صورت $r \neq 0$، لذا $r \in S$. بنابراین $s/r \in F$ و $(r/s)(s/r) = 1$؛ یعنی r/s معکوس‌پذیر است.
تکمیل بقیه‌ی اثبات به‌عنوان تمرین به خواننده واگذار می‌شود.

■■■

تعریف ۱-۲۳

اگر R یک دامنه‌ی صحیح باشد و $S = R \setminus \{0\}$، F را **میدان کسرهای** R می‌نامند.

مثال۲۱: میدان کسرهای حلقه‌ی اعداد صحیح $\mathbb{Z}$، دقیقاً میدان اعداد گویای $\mathbb{Q}$ است.

□

مثال۲۲: فرض کنیم R یک دامنه‌ی صحیح باشد. میدان کسرهای حلقه‌ی چند جمله‌ای‌های $R[x]$ را با $R(x)$ نمایش داده و آن‌را میدان **توابع گویا** از متغیر x روی حلقه‌ی R نامیم. در حقیقت

$$R(x) = \{f(x) / g(x) \mid f(x), g(x) \in R[x], g(x) \neq 0\}.$$

در حالت کلی میدان کسرهای حلقه‌ی چند جمله‌ای‌های $R[x_1,\ldots,x_n]$ را با $R(x_1,\ldots,x_n)$ نمایش داده و آن‌را میدان **توابع گویا** از متغیرهای $x_1,\ldots,x_n$ روی حلقه‌ی R می‌نامیم. در واقع

$$R(x_1,\ldots,x_n) = \{f(x_1,\ldots,x_n) / g(x_1,\ldots,x_n) \mid f(x), g(x) \in R[x_1,\ldots,x_n], g \neq 0\}.$$

□

قضیه ۱-۱۹

فرض کنیم R یک دامنه‌ی صحیح باشد و $S = R \setminus \{0\}$. دراین‌صورت نگاشت $\varphi : R \to F$ با ضابطه‌ی $\varphi(r) = r/1$ یک تکریختی است. به عبارت دیگر هر دامنه‌ی صحیح قابل نشاندن در میدا ن‌کسرهای خود است.

اثبات: به عنوا ن‌تمرین به خواننده واگذار می‌شود.

■■■

تمرین‌های سطح۱

۱- فرض کنید F یک میدان باشد. نشان دهید میدان کسرهای F یکریخت با F است.

تمرین‌های سطح۲

۲- دو دامنه‌ی صحیح غیریکریخت مثال بزنید که میدان کسرهایشان یکریخت باشد.

۳- فرض کنید R یک حلقه‌ی تعویض‌پذیر باشد (لزوماً یکدار نیست). نشان دهید R را می‌توان در یک حلقه‌ی تعویض‌پذیر و یکدار نشاند.

تمرین‌های سطح ۳

۴-نشان دهید زیرحلقه‌ی سره مانند A از $\mathbb{R}$ وجود دارد که میدان کسرهایش برابر $\mathbb{R}$ باشد.

۱-۴ دامنه‌ی تجزیه‌ی یکتا

تعریف ۱-۲۴

فرض کنیم R یک حلقه‌ی تعویض‌پذیر باشد.

(۱) فرض کنید $a,b \in R$. اگر $x \in R$ وجود داشته باشد به‌طوری‌که $ax = b$، گوییم a، b را **عاد می‌کند** و می‌نویسیم $a \mid b$.

علاوه بر این، فرض کنید R یکدار نیز باشد.

(۲) عنصر غیر یکال و غیر صفر $c \in R$ را **تحویل‌ناپذیر** (تجزیه‌ناپذیر) گوییم، اگر

$$c = ab \Rightarrow \text{یکال } b \text{ یا } a$$

(۳) عنصر غیر یکال و غیر صفر $p \in R$ را **اول** گوییم، اگر

$$p \mid ab \Rightarrow \ p \mid b \text{ یا } p \mid a$$

(۴) دو عنصر a و b از R را **شریک (وابسته)** گوییم واز نماد $a \sim b$ استفاده می‌کنیم، اگر عنصر یکال $u \in R$ موجود باشد به‌طوری‌که $a = bu$.

گزاره۱-۱

فرض کنیم R یک حلقه‌ی تعویض پذیر و یکدار باشد. دراین‌صورت

(۱) رابطه ی شکیبودن یک رابطه‌ی هم ارزی است،

(۲) اگر $a,b \in R$ شریک باشند، آن‌گاه $< a >=< b >$. هرگاه R یک دامنه‌ی صحیح باشد، عکس این مطلب نیز درست است.

اثبات: به‌عنوا ن‌تمرین به خواننده واگذار می‌شود.

■■■

گزاره۱-۲

فرض کنیم R یک دامنه‌ی صحیح باشد. دراین‌صورت

(۱) هر عنصر اول R تحویل‌ناپذیر است،

(۲) هرگاه R یک دامنه ی لیه‌آل اصلی باشد و $p \in R$، آن‌گاه

p اول است اگر و فقط اگر p تحویل‌ناپذیر باشد.

اثبات: به‌عنوا ن‌تمرین به عهده‌ی خواننده واگذار می‌شود.

■■■

❖ **تذکر:** عکس قسمت (۱) گزاره‌ی اخیر برقرار نیست. یعنی یک عنصر تحویل‌ناپذیر لزوماً اول نیست. تمرین ۲ را ملاحظه کنید.

تعریف ۱-۲۵

دامنه‌ی صحیح R را یک **دامنه‌ی تجزیه‌ی یکتا** (به اختصار UFD) می‌نامیم هرگاه:

(۱) (وجود تجزیه) هر عنصر غیر صفر و غیر یکال $a \in R$ را بتوان به‌صورت $a = a_1 a_2 \dots a_n$ نوشت که در آن a_iها عناصر تحویل‌ناپذیری از R هستند. به‌عبارت دیگر $a \in R$ را بتوان به‌صورت حاصل‌ضربی از عوامل تحویل‌ناپذیر تجزیه کرد.

(۲) (یکتایی تجزیه) اگر $a = b_1 b_2 \dots b_n = c_1 c_2 \dots c_m$، که b_iها و c_iها تحویل‌ناپذیرند، آن‌گاه $m = n$ و c_iها را بتوان طوری تجدید شماره‌گذاری کرد که هر b_i و c_i شریک باشند.

قضیه ۱-۲۰

هر دامنه ی ایده‌آل اصلی یک دامنه‌ی تجزیه‌ی یکتاست؛ به‌عبارت‌دیگر

$$PID \Rightarrow UFD.$$

اثبات: فرض کنیم R یک دامنه‌ی ایده‌آل اصلی باشد.

(وجود تجزیه): فرض کنیم Sمجموعه‌ی عناصر غیر صفر و غیر یکال از R باشد که نتوان آن‌ها را به‌صورت حاصل‌ضرب تعداد متناهی از عناصر تحویل‌ناپذیر نوشت. اگر $S = \varnothing$، مسئله حل است. حال فرض کنیم $S \neq \varnothing$. قرار می‌دهیم:

$$\Sigma = \{< x > | \, x \in S\}.$$

$\Sigma \neq \varnothing$، چون $S \neq \varnothing$. بنابراین طبق قضیه‌ی ۱۲، Σ دارای عنصر ماکزیمالی مانند $< a >$خواهد بود. چون $a \in S$، a تحویل‌ناپذیر نیست و ازاین‌رو $a = bc$، که در این‌جا b, cغیر یکال هستند. اگر $< a >=< b >$، آن‌گاه عنصر یکال $u \in R$ چنان موجود است که $a = bu$. ازاین‌رو $bc = bu$ و در نتیجه $c = u$، که تناقض است. بنابراین $< a > \subsetneq < b >$. به‌طریق مشابه می‌توان نشان داد که $< a > \subsetneq < c >$. درنتیجه با توجه به ماکزیمال بودن $a \in S$، داریم $b, c \notin S$. لذا عناصر تحویل‌ناپذیر $b_1, b_2, \ldots, b_m$ و $c_1, c_2, \ldots, c_m$ موجودند که $b = b_1 b_2 \ldots b_m$ و $c = c_1 c_2 \ldots c_n$. بنابراین

$$a = bc = b_1 b_2 \ldots b_m c_1 c_2 \ldots c_n.$$

یعنی a به‌صورت حاصل‌ضرب تعداد متناهی از عناصر تحویل‌ناپذیر نوشه شد، که متناقض با انتخاب a است. ازاین‌رو $S = \varnothing$ و قضیه اثبات است.

(یکتایی تجزیه): حال فرض کنیم $a = b_1 b_2 \ldots b_n = c_1 c_2 \ldots c_m$، که b_iها و c_iها تحویل ناپذیرند. بنابراین $b_1 \mid c_1 c_2 \ldots c_m$. با شماره‌گذاری مجدد c_iها (در صورت لزوم)، می‌توان فرض کرد $b_1 \mid c_1$. از آن‌جا که b_1و c_1 تحویل‌ناپذیر هستند، باید شریک باشند؛ یعنی $c_1 = b_1 u_1$ که u_1 یکالی از R است. بنابراین با توجه به ناصفر بودن b_1 خواهیم داشت

$$b_2 b_3 \ldots b_n = (u_1 c_2) c_3 \ldots c_m.$$

با ادامه‌ی این روند به تساوی زیر می‌رسیم

$$1 = u_1 \dots u_n c_{n+1} \dots c_m.$$

چون c_iها تحویل‌ناپذیرند، نتیجه می‌شود که $m = n$ و با شماره‌گذاری مجدد (در صورت لزوم) برای هر i، b_i شریک c_i است.

■■■

قضیه‌های ۸ و ۲۰ را می‌توان به‌صورت زیر که به‌خاطر سپردن آن آسان است خلاصه کرد.

$$\boxed{\text{ED} \Rightarrow \text{PID} \Rightarrow \text{UFD}}$$

تعریف ۱-۲۶

فرض کنیم R یک حلقه‌ی تعویض‌پذیر و $a_1, a_2, \dots, a_n \in R$. عنصر $d \in R$ را **بزرگ‌ترین مقسوم‌علیه مشترک** عناصر $a_1, a_2, \dots, a_n$ گوییم و با نماد $d = (a_1, a_2, \dots, a_n)$ نمایش می‌دهیم، اگر

(۱) به ازای هر i، $d \mid a_i$،

(۲) $c \mid a_i$ به ازای هر i نتیجه دهد $c \mid d$.

تعریف ۱-۲۷

عناصر $a_1, a_2, \dots, a_n$ از حلقه‌ی تعویض‌پذیر و یکدار R را **نسبت به هم اول** گوییم اگر 1 بزرگ‌ترین مقسوم‌علیه مشترک عناصر $a_1, a_2, \dots, a_n$ باشد.

◆ **تذکر:** بزرگ‌ترین مقسوم‌علیه مشترک همیشه موجود نیست. هم‌چنین بزرگ‌ترین مقسوم‌علیه مشترک ممکن است یکتا نباشد. اما می توان‌نشان داد که بزرگ‌ترین مقسوم‌علیه مشترک در حد شریک بودن یکتاست (تمرین۶).

گزاره‌ی زیر نشان می‌دهد که در یک حلقه‌ی ایده‌آل اصلی، بزرگ‌ترین مقسوم‌علیه مشترک موجود است. در تمرین ۳ از خواننده خواسته شده که نشان دهد در یک حلقه‌ی دامنه‌ی تجزیه‌ی یکتا نیز بزرگ‌ترین مقسوم‌علیه مشترک موجود است.

گزاره۱-۳

فرض کنیم R یک حلقه‌ی تعویض پذیر و یکدار بوده و $a_1,\ldots,a_n \in R$.

(۱) اگر $r_1,\ldots,r_n \in R$ و $d = r_1a_1 + \cdots + r_na_n$، آن‌گاه

$$< d >=< a_1 > + \cdots + < a_n > \Leftrightarrow d = (a_1,\ldots,a_n).$$

(۲) اگر R یک حلقه ی ایده‌آل اصلی باشد، آن‌گاه بزرگ‌ترین مقسوم علیه مشترک عناصر $a_1, a_2,\ldots,a_n$ موجود بوده و به‌صورت $d = r_1a_1 + \cdots + r_na_n$، که در آن $r_i \in R$، خواهد بود.

اثبات (۱) ($\Leftarrow$) : به‌وضوح $< a_1 > + \cdots + < a_n > \subseteq < d >$. حال فرض کنیم $s_1a_1 + \cdots s_na_n \in < a_1 > + \cdots + < a_n >$. دراین‌صورت با توجه به‌این‌که $a_i \mid d$، خواهیم داشت $d \mid s_1a_1 + \cdots s_na_n$ و لذا $s_1a_1 + \cdots + s_na_n \in < d >$.

($\Rightarrow$) : به‌وضوح $d \mid a_i$، به ازای هر i. حال فرض کنیم به ازای هر i، $c \mid a_i$. دراین‌صورت با توجه به این‌که $d = r_1a_1 + \cdots + r_na_n$، داریم $c \mid d$؛ بنابراین $d = (a_1,\ldots,a_n)$.

(۲): اگر R یک حلقه‌ی ایده‌آل اصلی باشد، آن‌گاه عنصر $d \in R$ موجود است به‌گونه‌ای که $< d >=< a_1 > + \cdots + < a_n >$. از این‌روطبق قسمت (۱)، $d = (a_1,\ldots,a_n)$.

■■■

تعریف ۱-۲۸

فرض کنیم R یک دامنه‌ی تجزیه‌ی یکتا باشد و $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$. **محتوای** f که با $C(f)$ نمایش داده می‌شود، بزرگ‌ترین مقسوم‌علیه مشترک ضرایب $a_1,a_2,\ldots,a_n$ تعریف می‌شود؛ به‌عبارت دیگر $C(f)=(a_1,a_2,\ldots,a_n)$. هم‌چنین f را یک **چند جمله‌ای اولیه** گوییم اگر $C(f)=1$.

لازم به ذکر است که $C(f)$ یکتا نیست، زیرا بزرگ‌ترین مقسوم‌علیه مشترک لزوماً یکتا نیست. ولی هر دو بزرگ‌ترین مقسوم‌علیه مشترک الزاماً شریک‌اند و هر شریک از یک محتوای f خود یک محتوا برای f است. پس $C(f)$ در حد یکه، یکتاست.

گزاره ۱-۴

فرض کنیم R یک دامنه‌ی تجزیه‌ی یکتا باشد و $f(x)\in R[x]$ و $a\in R$. دراین‌صورت

(۱) f را می‌توانیم به‌صورت $f=C(f)f_1$ بنویسیم که در آن f_1 یک چندجمله‌ای اولیه است.

(۲) $C(af)\sim aC(f)$.

اثبات: به‌عنوا ن‌تمرین به عهده‌ی خواننده واگذار می‌شود.

■■■

لم(گاوس) ۱-۲

فرض کنیم R یک دامنه‌ی تجزیه‌ی یکتا باشد و $f,g\in R[x]$. دراین‌صورت $C(fg)\sim C(f)C(g)$. به‌خصوص، اگر f,g دو چند جمله‌ای اولیه باشند، آن‌گاه fg نیز یک چندجمله‌ای اولیه است.

اثبات: فرض‌کنیم $f = C(f)f_1$ و $g = C(g)g_1$، که f_1 و g_1 اولیه‌اند. دراین‌صورت

$$C(fg) = C(C(f)f_1C(g)g_1) \sim C(f)C(g)C(f_1g_1)$$

ازاین‌رو کافی است ثابت شود که f_1g_1 اولیه است. اگر $f_1 = \sum_{i=0}^{m} a_i x^i$ و $g_1 = \sum_{g=0}^{n} b_j x^j$، آن‌گاه $f_1g_1 = \sum_{k=0}^{m+n} c_k x^k$ که در آن $c_k = \sum_{i+j=k} a_i b_j$. هرگاه f_1g_1 اولیه نباشد، آن‌گاه یک عنصر تحویل‌ناپذیر مانند $p \in R$ هست به‌طوری‌که به ازای هر $1 \le k \le m+n$، $p \mid c_k$. چون $C(f_1)$ یکه است، $p \nmid C(f_1)$، در نتیجه، کوچک‌ترین عدد صحیح مانند s موجود است به‌طوری‌که $p \mid a_i$ به ازای هر i، $i < s$ و $p \nmid a_s$. همین‌طور، کوچک‌ترین عدد صحیح t موجود است به‌طوری‌که $p \mid b_j$ برای هر j، $j < t$ و $p \nmid b_t$. چون

$$p \mid c_{s+t} = a_0b_{s+t} + \cdots + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + \cdots + a_{s+t}b_0$$

پس $p \mid a_sb_t$. چون هر عنصر تحویل‌ناپذیر در R اول است، $p \mid a_s$ یا $p \mid b_t$ که یک تناقض است؛ بنابراین f_1g_1 اولیه است.

■■■

لم۱-۳

فرض کنیم R یک دامنه‌ی تجزیه‌ی یکتا با میدان کسرهای F بوده و f و g چندجمله‌ای‌های اولیه در $R[x]$ باشند. دراین‌صورت

f و g در $R[x]$ شریک‌اند $\Leftrightarrow$ f و g در $F[x]$ شریک باشند.

اثبات ($\Leftarrow$): به‌وضوح برقرار است.

($\Rightarrow$) : فرض کنیم f و g در $F[x]$ شریک باشند. دراین‌صورت عنصر یکه‌ی $u \in F[x]$ موجود است چنان که $f = gu$. اما u باید یک یکه از F باشد ولذا $u = a/b$ که $a, b \in R$ و $b \neq 0$. بنابراین $bf = ag$ و در نتیجه با توجه به یکه بودن $C(f)$ و $C(g)$ در R، خواهیم داشت:

$$b \sim bC(f) \sim C(bf) = C(ag) \sim aC(g) \sim a.$$

بنابراین، به ازای یکه‌ای چون $v \in R$، $a = bv$ و $bf = ag = bvg$. در نتیجه $f = vg$ و لذا f و g در $R[x]$ شریک‌اند.

■■■

لم۱-۴

فرض کنیم R یک دامنه‌ی تجزیه‌ی یکتا با میدان کسرهای F بوده و f یک چندجمله‌ای غیر ثابت در $R[x]$ باشد. دراین‌صورت

f در $R[x]$ تحویل‌ناپذیر است $\Leftrightarrow$ f در $F[x]$ تحویل‌ناپذیر و در $R[x]$ اولیه باشد

اثبات ($\Rightarrow$): اگر $f = gh$، که در آن $g, h \in R[x]$، آن‌گاه چون f در $F[x]$ تحویل‌ناپذیر است، یکی از g یا h (مثلاً g) باید در $F[x]$ یکال باشد. ازاین‌رو $g(x)$ باید یک چندجمله‌ای ثابت باشد و لذا $g \in R$. چون f اولیه است و $C(f) = C(gh) \sim gC(h)$، پس g باید در R و در نتیجه در $R[x]$ یکه باشد. بنابراین f در $R[x]$ تحویل‌ناپذیر است.

($\Leftarrow$): فرض کنیم f در $R[x]$ تحویل‌ناپذیر است. چون $f = C(f)f_1$ که f_1 اولیه است، $C(f)$ باید در $R[x]$ و در نتیجه در R یکه باشد. بنابراین f اولیه است. حال فرض کنیم (فرض خلف) که f در $F[x]$ تحویل‌ناپذیر نباشد. ازاین‌رو $f = gh$ که $g, h \in F[x]$ و $\deg f \geq 1$، $\deg g \geq 1$. فرض‌کنیم $g = (a/b)g_1$ و $h = (c/d)h_1$، که $g_1, h_1 \in R[x]$ اولیه و $a, b, c, d \in R$. دراین‌صورت $gh = (ac/bd)g_1h_1$ و در نتیجه $bdgh = acg_1h_1$. با توجه به اولیه بودن g_1h_1، داریم

$$bd \sim bdC(f) \sim C(bdf) = C(bdgh) = C(acg_1h_1) \sim acC(g_1h_1) \sim ac.$$

ازاین‌رو bd و ac در R شریک‌اند، که نتیجه می‌دهد f و g_1h_1 در $R[x]$ شریک هستند. در نتیجه f در $R[x]$ تحویل‌ناپذیرنیست، که تناقض است؛ بنابراین f در $F[x]$ تحویل‌ناپذیر است.

■■■

به آسانی از لم ۴، خواهیم داشت:

نتیجه۱-۴

فرض کنیم $f(x) \in \mathbb{Z}[x]$ یک چندجمله‌ای غیر ثابت و اولیه باشد. دراین‌صورت

$f(x)$ در $\mathbb{Z}[x]$ تحویل‌ناپذیر است $\Leftrightarrow$ $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر باشد

اینک برای اثبات قضیه‌ی اصلی این بخش آماده هستیم:

قضیه ۱-۲۱

اگر R یک دامنه‌ی تجزیه‌ی یکتا باشد، آن‌گاه $R[x]$ نیز یک دامنه‌ی تجزیه‌ی یکتاست.

اثبات (وجود تجزیه): فرض کنیم $f(x)$ یک عنصر غیر صفر وغیر یکال از $R[x]$ باشد. اگر $\deg f(x) = 0$، مسئله حل است، زیرا R یک دامنه‌ی تجزیه‌ی یکتاست. فرض کنید $\deg f(x) > 0$ و F میدان کسرهای حلقه‌ی R باشد. چند جمله‌ای $f(x)$ را به‌عنوان عنصری از $F[x]$ در نظر بگیرید. چون $F[x]$ یک دامنه‌ی تجزیه‌ی یکتاست، می‌توان فرض کرد $f(x) = p_1(x)\dots p_m(x)$، که $p_i(x)$ها در $F[x]$ تحویل‌ناپذیرند. فرض کنیم $p_i(x) = (a_i / b_i)q_i(x)$ و $f(x) = C(f)f'(x)$، که در آن $a_i, b_i \in R$ و $q_i(x) \in R[x]$ و $f'(x) \in R[x]$ اولیه‌اند. دراین‌صورت

$$C(f)f' = (a / b)q_1(x)\dots q_m(x),$$

که در آن $a = a_1 \dots a_m$ و $b = b_1 \dots b_m$. بنابراین طبق لم۱-۲ و گزاره‌ی ۱-۴، عنصر یکال $u \in R$ موجود است به‌طوری‌که $bC(f)u = a$. ازاین‌رو

$$bf(x) = aq_1(x)\dots q_m(x) = bC(f)uq_1(x)\dots q_m(x),$$

و در نتیجه

$$f(x) = (C(f)u)q_1(x)\dots q_m(x).$$

چون هر $p_i(x)$ در $F[x]$ تحویل‌ناپذیر است، لذا $q_i(x)$، که عبارت است از حاصل‌ضرب $p_i(x)$ در یکالی از F، نیز در $F[x]$ تحویل‌ناپذیر است. از این‌رو $q_i(x)$ در $F[x]$ تحویل‌ناپذیر است و چون $q_i(x)$ در $R[x]$ اولیه است، لذا طبق لم۴، $q_i(x)$ در $R[x]$ تحویل‌ناپذیر است. از طرفی چون $C(f)u$ یا یکه از R است یا می‌توان آن‌را به حاصل‌ضربی از تحویل ناپذیرهای R تجزیه کرد، لذا نشان داده‌ایم که می‌توان $f(x)$ را به صورت حاصل‌ضربی ازتحویل‌ناپذیرها در $R[x]$ نوشت.

اثبات (یکتایی تجزیه): فرض کنیم

$$f(x) = a_1 \dots a_m p_1(x)\dots p_n(x) = b_1 \dots b_r q_1(x)\dots q_s(x),$$

که در آن a_i, b_i عناصری تحویل‌ناپذیر از R و $p_i(x), q_i(x)$ عناصری تحویل‌ناپذیر با درجه‌ی مثبت از $R[x]$ هستند.

با توجه به اولیه بودن $p_i(x), q_i(x)$ (طبق لم۴) و دامنه‌ی تجزیه‌ی یکتا بودن $F[x]$، $n = s$ و بعد از شماره گذاری مجدد (در صورت لزوم) هر $p_i(x)$ یک شریک $q_i(x)$ در $F[x]$ ودر نتیجه طبق لم۳ در $R[x]$ است. بنابرا ن عنصر یکه $u_i \in R$ موجود است چنان که $q_i(x) = u_i p_i(x)$. از این‌رو خواهیم داشت:

$$a_1 a_2 \dots a_m = (u_1 \dots u_n b_1) b_2 \dots b_r$$

چون R یک دامنه‌ی تجزیه‌ی یکتاست، پس $m = r$ و بعد از شماره گذاری مجدد (در صورت لزوم) هر a_i یک شریک b_i در R و در نتیجه در $R[x]$ خواهد بود. بدین ترتیب اثبات قضیه کامل است.

■■■

تمرین‌های سطح۱

۱-نشان دهید $\mathbb{Z}[\sqrt{2}]$ و $\mathbb{Z}[-\sqrt{2}]$ دامنه‌ی تجزیه‌ی یکتاست.

۲- فرض کنید $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$. نشان دهید عناصر 2 و $1 + \sqrt{-3}$ از حلقه‌ی $\mathbb{Z}[\sqrt{-3}]$ تحویل‌ناپذیر بوده ولی اول نیست.

۳-**(الف)** فرض کنید R یک دامنه‌ی تجزیه‌ی یکتا و $a_1, a_2 \in R$. فرض کنید $a_1 = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ و $a_2 = p_1^{\beta_1} \cdots p_n^{\beta_n}$، که در آن p_iها تحویل‌ناپذیرند. نشان دهید بزرگ‌ترین مقسوم‌علیه مشترک a_1 و a_2 برابر است با

$$p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_n^{\min\{\alpha_n, \beta_n\}}.$$

(ب) قسمت (الف) را برای n عنصر بیان واثبات کنید.

۴- نشان دهید $\mathbb{R}[x, y]$ یک دامنه‌ی تجزیه‌ی یکتاست درحالی‌که یک دامنه‌ی ایده‌آل اصلی نیست.

۵- فرض کنید R یک دامنه‌ی تجزیه‌ی یکتا و a عنصر غیر صفری از R باشد. نشان دهید تنها تعداد متناهی ایده‌آل اصلی شامل $< a >$ موجود است.

۶-**(الف)** فرض کنید R یک حلقه‌ی تعویض‌پذیر و یکدار و $d \in R$ بزرگ‌ترین مقسوم علیه مشترک عناصر $a_1, \ldots, a_n \in R$ باشد. اگر $d_1 \in R$ شریک d باشد، آن‌گاه نشان دهید d_1 نیز بزرگ‌ترین مقسوم علیه مشترک عناصر $a_1, \ldots, a_n$ خواهد بود.

(ب) فرض کنید R یک دامنه‌ی صحیح باشد. نشان دهید هر دو بزرگ‌ترین مقسوم علیه مشترک عناصر $a_1, a_2, \ldots, a_n \in R$ شریک هستند.

(پ) فرض کنید $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ و $a = 4$ و $b = 2 + 2\sqrt{-3}$. نشان دهید بزرگ‌ترین مقسوم علیه مشترک عناصر a, b موجود نیست.

۷- **(الگوریتم اقلیدس**[1]**)** فرض کنید R یک حلقه‌ی اقلیدسی با تابع اقلیدسی $\upsilon : R - \{0\} \to \mathbb{N}_0$ باشد. اگر $a, b \in R$ و $b \neq 0$، نشان دهید روش زیر بزرگ‌ترین مقسوم علیه a و b را به‌دست می‌آورد.

---

[1] Euclidean Algoritm

فرض کنید

$$a = bq_0 + r_1 \text{، که در آن } r_1 = 0 \text{ یا } v(r_1) < v(b)\text{،}$$

$$b = r_1q_1 + r_2 \text{، که در آن } r_2 = 0 \text{ یا } v(r_2) < v(r_1)\text{،}$$

$$r_1 = r_2q_2 + r_3 \text{، که در آن } r_3 = 0 \text{ یا } v(r_3) < v(r_2)\text{،}$$

$$\vdots$$

$$r_m = r_{m+1}q_{m+1} + r_{m+2} \text{، که در آن } r_{m+2} = 0 \text{ یا } v(r_{m+2}) < v(r_{m+1}).$$

اگر $r_0 = b$ و n کوچک‌ترین عدد صحیحی باشد که $r_{n+1} = 0$، آن‌گاه r_n بزرگ‌ترین مقسوم علیه a و b است.

۸- فرض کنید P, Q دو لیه‌آل اول غیر صفر از دامنه‌ی صحیح R باشند به‌طوری‌که $P \subseteq Q$. نشان دهید $P = Q$.

۹-نشان دهید $\dfrac{\mathbb{Z}_2[x]}{< x^2 + x + 1 >}$ یک میدان است درصورتی‌که $\dfrac{\mathbb{Z}_3[x]}{< x^2 + x + 1 >}$ میدان نیست.

۱۰- فرض کنیم F یک میدان و $f(x) = a_0 + a_1x + \cdots + a_nx^n$ یک چند جمله‌ای تحویل ناپذیر روی میدان F باشد. نشان دهید $L = F[x]/ < f(x) >$ یک میدان است.
(راهنمایی: نشان دهید $< f(x) >$ یک لیه‌آل ماکزیمال از حلقه‌ی $F[x]$ است).

تمرین‌های سطح ۲

۱۱- اگر R یک دامنه‌ی صحیح باشد، نشان دهید R یک دامنه‌ی تجزیه‌ی یکتاست، اگر وفقط اگر:

(۱) هر عنصر غیر صفر وغیر یکال به‌صورت حاصل‌ضربی از تحویل‌ناپذیرها نوشته شود

(۲) هر تحویل‌ناپذیری اول باشد.

تمرین‌های سطح ۳

۱۲- دامنه‌ی صحیح R دامنه‌ی تجزیه‌ی یکتاست اگر و فقط اگر هر لیه‌آل اول ناصفر در R شامل لیه‌آل اصلی ناصفری باشد که اول است.

۱۳- حلقه‌ی R یک دامنه‌ی لیه‌آل اصلی است اگر وفقط اگر R یک دامنه‌ی تجزیه‌ی یکتا باشد که هر لیه‌آل اول ناصفرش ماکزیمال است.

۱۴ - فرض‌کنید R زیر حلقه‌ی $\{a+b(1+\sqrt{19}i)/2 \mid a,b\in\mathbb{Z}\}$ از اعداد مختلط باشد. نشان دهید R یک دامنه‌ی لیه‌آل اصلی است، ولی یک دامنه‌ی اقلیدسی نیست.

۱-۵ آزمون‌های تحویل‌ناپذیری

قضیه ۱-۲۲: (محک آیزنشتاین)

فرض کنیم P یک ایده‌آل اول از دامنه‌ی صحیح R بوده و $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$ یک چند جمله‌ای اولیه باشد (در این‌جا $n\geq 1$). اگر $a_0,a_1,\ldots,a_{n-1}\in P$، $a_n\notin P$ و $a_0\notin P^2$، آن‌گاه $f(x)$ در $R[x]$ تحویل‌ناپذیر است.

اثبات: (برهان خلف) فرض کنیم f تحویل‌پذیر باشد. دراین‌صورت

$$f(x)=(b_0+b_1x+\cdots+b_mx^m)(c_0+c_1x+\cdots+c_kx^k),$$

که $b_i,c_i\in R$ و $m,k\geq 1$. چون $b_0c_0=a_0\in P$، $a_0\notin P^2$، پس P فقط شامل یکی از عناصر b_0,c_0 است. فرض کنیم $b_0\in P$ و $c_0\notin P$.

چون $a_n = b_m c_k$ و $a_n \notin P$، پس $b_m \notin P$. فرض کنیم i کوچک‌ترین عدد صحیح مثبتی باشد که $b_i \notin P$. دراین‌صورت $i \leq m < n$ و

$$a_i = b_i c_0 + (b_{i-1}c_1 + \cdots + b_0 c_i).$$

اما $a_i \in P$، $b_{i-1}c_1 + \cdots + b_0 c_i \in P$ و ازاین‌رو $b_i c_0 \in P$. چون P یک ایده‌آل اول است، پس $b_i \in P$ یا $c_0 \in P$، که یک تناقض است. بنابراین نتیجه می‌گیریم که f تحویل‌ناپذیر است. $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$

■■■

نتیجه ۱-۵ (محک آیزنشتاین برای $\mathbb{Z}[x]$)

فرض کنیم p یک عدد اول و $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ یک چندجمله‌ای اولیه باشد که $p \mid a_i$ برای هر $0 \leq i \leq n-1$ و $p^2 \nmid a_0$ و $p \nmid a_n$. دراین‌صورت f در $\mathbb{Z}[x]$ و $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

اثبات: به آسانی از محک آیزنشتاین به‌دست خواهد آمد.

■■■

قضیه ۱-۲۳

فرض کنیم R یک دامنه‌ی تجزیه‌ی یکتا و F میدان کسرهای R باشد. فرض کنیم $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ یک چند جمله‌ای درجه‌ی n باشد. اگر $r/s \in F$ ریشه‌ای از f باشد که در آن r و s نسبت به‌هم اولند، آن‌گاه $r \mid a_0$ و $s \mid a_n$.

اثبات: داریم:

$$f(r/s) = a_0 + a_1(r/s) + \cdots + a_n(r/s)^n = 0.$$

با ضرب در s^n خواهیم داشت:

$$a_0 s^n + a_1 r s^{n-1} + \cdots + a_{n-1} r^{n-1} s + a_n r^n = 0.$$

بنابراین $a_n r^n = s(-a_0 s^{n-1} - \cdots - a_{n-1} r^{n-1})$. ازاین‌رو $s \mid a_n r^n$. چون $(r,s) = 1$، پس $s \mid a_n$. به‌همین ترتیب، $a_0 s^n = r(-a_1 s^{n-1} - \cdots - a_n r^{n-1})$ و ازاین‌رو $r \mid a_0$.

■■■

قضیه‌ی زیر محک دیگری برای تحویل‌ناپذیری یک چند جمله‌ای در $\mathbb{Z}[x]$ ارائه می‌دهد.

قضیه ۱-۲۴

فرض کنیم $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ و p عدد اولی باشد که $p \nmid a_n$. فرض کنیم $\overline{f}(x) = \overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_n x^n \in \mathbb{Z}_p[x]$، که در آن $\overline{a}_i$ تصویر a_i تحت همریختی طبیعی $\mathbb{Z} \to \mathbb{Z}_p$ می‌باشد. دراین‌صورت اگر $\overline{f}$ در $\mathbb{Z}_p[x]$ تحویل‌ناپذیر باشد، آن‌گاه f در $\mathbb{Z}[x]$ و $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

اثبات: کافی است ثابت کنیم که f در $\mathbb{Z}[x]$ تحویل ناپذیر است. برهان خلف، فرض کنیم $f(x) = g(x)h(x)$ که، $\deg g(x) < \deg f(x)$ و $\deg h(x) < \deg f(x)$.

دراین‌صورت $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ و چون $\deg f(x) = \deg \overline{f}(x)$، لذا

$$\deg \overline{g}(x) \le \deg g(x) < \deg f(x) = \deg \overline{f}(x),$$
$$\deg \overline{h}(x) \le \deg h(x) < \deg f(x) = \deg \overline{f}(x),$$

که متناقض با تحویل‌ناپذیر بودن $\overline{f}$ در $\mathbb{Z}_p[x]$ است.

■■■

تفاوت یک کتاب بدون مسئله و یک کتاب با مسئله همانند تفاوت بین یادگیری خواندن به یک زبان است و یاد گیری صحبت کردن به آن زبان.

(فریمن دیسون)

تمرین‌های سطح۱

۱–نشان دهید چند جمله‌ای‌های زیر روی $\mathbb{Z}[x]$ تحویل‌ناپذیرند.

(۱) $f(x) = 2x^6 - 6x^5 + 9x + 15$،

(۲) $f(x) = 2x^5 - 10x + 5$،

(۳) $f(x) = x^4 + 4x^2 + 2$،

(۴) $f(x) = x^3 + x^2 - 2x - 1$،

(۵) $f(x) = 8x^3 - 6x - 1$،

(۶) $f(x) = x^3 - 3x + 1$.

تمرین‌های سطح۲

۲– نشان دهید چند جمله‌ای $f(x) = x^4 + 4x^3 + 6x^2 + 4x + 4$ روی $\mathbb{Z}[x]$ تحویل‌ناپذیر است.

۳– اگر p عددی اول و $f(x) = 1 + x + \cdots + x^{p-1}$، ثابت کنید $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

۴– اگر $n \in \mathbb{N}$ و $f(x) = (x-1)(x-2)\cdots(x-n) - 1$، ثابت کنید $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

۵– نشان دهید برای هر دو عدد صحیح m و n چند جمله‌ای $x^3 + (5m+1)x + 5n + 1$ روی $\mathbb{Z}$ تحویل‌ناپذیر است.

۶– چند جمله‌ای $x^{10} - 1$ را به عوامل تحویل‌ناپذیر در $\mathbb{Q}[x]$ تجزیه کنید.

۷- فرض کنید $f \in \mathbb{R}[x]$ و $\deg f \geq 3$. نشان دهید f در $\mathbb{R}$ تحویل‌پذیر است.

تمرین‌های سطح ۳

۸- فرض کنید p یک عدد اول و a, b دو ریشه‌ی متمایز معادله‌ی زیر باشند.

$$1 + x + x^2 / 2! + \cdots + x^p / p!$$

نشان دهیدکه $a \pm b$ و ab نمی‌توانند اعداد گویایی باشند.

منابعی برای مطالعه‌ی بیشتر

۱. طائری، بیژن. **مبانی جبرمجرد**. انتشارات دانشگاه صنعتی اصفهان (۱۳۸۲).

۲. نقی پور، علیرضا. **آشنایی با نظریه گروه‌ها و حلقه‌ها**. انتشارات دانشگاه شهرکرد (۱۳۸۷).

۳. هانگرفورد، تی. دبلیو. **مقدمه‌ای بر جبر مجرد**. ترجمه‌ی اعظم، سعید و انشائی، رضا. انتشارات دانشگاه اصفهان (۱۳۸۱).

4. Bhattacharya, P.B., Jain, S. K., Nagpaul, S. R. *Basic Abstract Algebra*. Cambridge University Press, 1994.

5. Fraleigh, J. B. *A First Course in Abstract Algebra*Add ison-esley, 1999.

6. Judson, T. W. *Abstract Algebra*. PWS Publishing Company, Boston, 1993.

7. L**a**g, S. *Introduction to Linear Algebra*. Springer-Verlag, New York, 1986.

8. Sharp, R. *Steps in Commutative Algebra*. Cambridge University Press, 2000.

فصل ۲

ترسیم به‌وسیله‌ی خط‌کش و پرگار

روش حلی خوب است که از همان آغاز بتوان پیش‌بینی کرد که با دنبال کردن این روش می‌توان به هدف رسید.

(لایب نیتس)

در این فصل می‌خوانیم:

مقدمه

چهار مسئله‌ی مشهور زیر از دیر باز (زمان یونان باستان) مورد توجه بوده است:

(۱) (تثلیث زاویه) آیا می‌توانیم با خط‌کش و پرگار یک زاویه‌ی دلخواه را به سه قسمت مساوی تقسیم کنیم؟

(۲) (تضعیف مکعب) آیا می‌توانیم با خط‌کش و پرگار مکعبی رسم کنیم که حجم آن دو برابر حجم یک مکعب مفروض باشد؟

(۳) (تربیع دایره) آیا می‌توانیم با خط‌کش و پرگار مربعی رسم کنیم که مساحت آن برابر مساحت یک دایره‌ی مفروض باشد؟

(۴) (ترسیم چند ضلعی منتظم) آیا با خط‌کش و پرگار می‌توانیم یک $n-$ضلعی منتظم ($n \geq 3$) ترسیم کنیم؟

در این فصل به سوال‌های۱و۲و۳ و تا حدودی به سوال ۴ پاسخ خواهیم داد (این سوال را به‌طور کامل در فصل ۵ پاسخ خواهیم داد). در این رهگذار، آشنایی مختصری با توسیع میدان‌ها لازم است.

۲-۱ توسیع میدان‌ها

در سراسر این بخش F، Kو L نشان‌دهنده‌ی میدان هستند.

تعریف ۲-۱

(الف): فرض کنیم Fو K دو میدان باشند. K را یک **توسیع** روی F نامیم درصورتی‌که F یک زیرمیدان K باشد.

(ب): فرض کنیم K یک توسیع از F باشد. میدان E را یک **میدان میانی** توسیع K روی F گوییم اگر $F \subseteq E \subseteq K$.

تعریف ۲-۲

فرض کنیم K یک توسیع از Fباشد. دراین‌صورت بعد فضای برداری K روی میدان F را با نماد $[K : F]$ نمایش می‌دهیم. اگر $[K : F] < \infty$، آن‌گاه Kرا یک **توسیع متناهی** از F گوییم.

قضیه‌ی زیر نقشی بسیار مهم در نظریه‌ی میدان و گالوا ایفا می‌کند.

قضیه ۲-۱ (قضیه‌ی برج)

فرض کنیم L یک توسیع از K و K یک توسیع از F باشد. دراین‌صورت

$$[L:F]=[L:K][K:F].$$

اثبات: اگر $[K:F]=\infty$، آن‌گاه K و در نتیجه L دارای یک زیر مجموعه‌ی نامتناهی مستقل خطی روی F خواهند بود و از این‌رو در این حالت $[L:F]=\infty$.

اگر $[L:K]=\infty$، آن‌گاه L دارای یک زیر مجموعه‌ی نامتناهی مستقل خطی روی K و در نتیجه روی F خواهد بود. بنابراین در این حالت نیز $[L:F]=\infty$.

اکنون فرض کنیم $m=[K:F]<\infty$ و $n=[L:K]<\infty$. فرض کنیم $\{x_1,\ldots,x_m\}$ یک پایه برای فضای برداری K روی F و $\{y_1,\ldots,y_n\}$ یک پایه برای فضای برداری L روی K باشد. قرار می‌دهیم:

$$\mathcal{B}=\{x_iy_j \mid 1\le i\le m, 1\le j\le n\}$$

کافی است نشان دهیم $\mathcal{B}$ یک پایه برای فضای برداری L روی F است. ابتدا نشان می‌دهیم $\mathcal{B}$ روی F مستقل خطی است. فرض کنیم $\sum_{i,j}a_{ij}(x_iy_j)=0$، که درآن $a_{ij}\in F$. دراین‌صورت

$$\sum_{j=1}^{n}(\sum_{i=1}^{m}a_{ij}x_i)y_j=0.$$

با توجه به مستقل خطی بودن $\{y_1,\ldots,y_n\}$ روی K، برای هر $1\le j\le n$ داریم $\sum_{i=1}^{m}a_{ij}x_i=0$. اما با توجه به رابطه‌ی $\sum_{i=1}^{m}a_{ij}x_i=0$ و مستقل خطی بودن $\{x_1,\ldots,x_m\}$ روی F، برای هر $1\le i\le m$ و هر $1\le j\le n$ خواهیم داشت $a_{ij}=0$. یعنی $\mathcal{B}$ روی F مستقل خطی است. در نهایت نشان می‌دهیم $\mathcal{B}$ فضای برداری L روی F را تولید می‌کند. فرض کنیم $z\in L$. چون $\{y_1,\ldots,y_n\}$ یک پایه برای فضای برداری L روی K است، پس عناصر $b_1,\ldots,b_n\in K$ موجودند به‌طوری‌که $z=\sum_{j=1}^{n}b_jy_j$.

چون $\{x_1,\dots,x_m\}$ یک پایه برای فضای برداری K روی F است، برای هر $1 \le j \le n$، عناصر $a_{j1},\dots,a_{jm} \in F$ موجودند به‌گونه‌ای که $b_j = \sum_{i=1}^{m} a_{ji}x_i$. دراین‌صورت

$$z = \sum_{j=1}^{n} b_j y_j = \sum_{j=1}^{n} (\sum_{i=1}^{m} a_{ij}x_i)y_j = \sum_{\substack{1\le i\le m\\ 1\le j\le n}} a_{ij}x_i y_j$$

ازاین‌رو $\mathcal{B}$ فضای برداری L روی F را تولید می‌کند.

■■■

از قضیه‌ی اخیر و استقرای ریاضی نتیجه‌ی زیر به‌آسانی به‌دست خواهد آمد.

نتیجه ۲-۱

فرض کنیم $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{\ell-1} \subseteq F_\ell$ یک توسیع از میدان‌ها باشد. دراین‌صورت
$$[F_\ell : F_0] = [F_\ell : F_{\ell-1}][F_{\ell-1} : F_{\ell-2}]\cdots[F_1 : F_0].$$

با توجه به قضیه‌ی ۱-۲، تعریف زیر را خواهیم داشت.

تعریف۲-۳

فرض کنیم K یک توسیع از F باشد و $X \subseteq K$. اشتراک همه‌ی زیر میدان‌های (زیرحلقه‌های) شامل $X \cup F$ از K **زیر میدان (زیر حلقه) تولید شده به‌وسیله** X روی F نام دارد و با نماد $F(X)$ $(F[X])$ نمایش داده می‌شود. اگر $X = \{u_1, u_2,\dots,u_n\}$، آن‌گاه زیرمیدان $F(X)$ (زیر حلقه $F[X]$) را با نماد $F(u_1, u_2,\dots,u_n)$ $(F[u_1, u_2,\dots,u_n])$ نمایش می‌دهیم. هرگاه $X = \{u\}$، آن‌گاه $F(u)$ را یک **توسیع ساده** از F گوییم.

❖ **تذکر:** $F(X)$ $(F[X])$ کوچک‌ترین زیرمیدان (زیر حلقه) از K است که شامل $X \cup F$ است.

غالباً مفید است که توصیفی درونی از $F(X)$ $(F[X])$ داشته باشیم. اکنون چنین توصیفی را ارائه می‌دهیم.

قضیه۲-۲

فرض کنیم K یک توسیع از F باشد و $X \subseteq K$ و $u, u_1, \ldots, u_n \in K$. دراین‌صورت

(۱) $F[u] = \{f(u) \mid f \in F[x]\}$،

(۲) $F[u_1, \ldots, u_n] = \{f(u_1, , \ldots, u_n) \mid f \in F[x_1, \ldots, x_n]\}$،

(۳) $F[X] = \{f(\alpha_1, \ldots, \alpha_n) \mid n \in \mathbb{N}_0, \alpha_i \in X, f \in F[x_1, \ldots, x_n]\}$،

(۴) $F(u) = \{f(u) / g(u) \mid f, g \in F[x], g(u) \neq 0\}$،

(۵)

$$F(u_1, \ldots, u_n) = \{f(u_1, \ldots, u_n) / g(u_1, \ldots, u_n) \mid f, g \in F[x_1, \ldots, x_n] \, , g(u_1, \ldots, u_n) \neq 0\},$$

(۶)

$$F(X) = \{f(\alpha_1, \ldots, \alpha_n) / g(\alpha_1, \ldots, \alpha_n) \mid n \in \mathbb{N}_0, \alpha_i \in X, f, g \in F[x_1, \ldots, x_n] \, , g(\alpha_1, \ldots, \alpha_n) \neq 0\}.$$

اثبات: با توجه به مشابه بودن اثبات فقط (۶) را ثابت می‌کنیم.

(۶): فرض کنیم

$$A = \{f(\alpha_1, \ldots, \alpha_n) / g(\alpha_1, \ldots, \alpha_n) \mid n \in \mathbb{N}_0, \alpha_i \in X, f, g \in F[x_1, \ldots, x_n] \, , g(\alpha_1, \ldots, \alpha_n) \neq 0\}.$$

به‌وضوح A میدانی شامل $X \cup F$ است. پس طبق تعریف $F(X)$، داریم $F(X) \subseteq A$. از طرفی هر میدان شامل $X \cup F$ باید A را در بر داشته باشد. ازاین‌رو با استفاده‌ی مجدد از تعریف $F(X)$، داریم $A \subseteq F(X)$. ازاین‌رو $A = F(X)$ و اثبات تمام است.

■■■

تعریف۲-۴

(۱) فرض کنیم K یک توسیع از F باشد و $a \in K$. گوییم a روی F **عنصری جبری** است اگر یک چندجمله‌ای ناصفر مانند $f(x) \in F[x]$ وجود داشته باشد به قسمی که $f(a) = 0$. اگر a ریشه‌ی هیچ چندجمله‌ای ناصفر $f(x) \in F[x]$ نباشد، گوییم a روی F **عنصری متعالی** است. K یک **توسیع جبری** F نام دارد اگر هر عنصر K روی F جبری باشد.

(۲) عدد $a \in \mathbb{C}$ را یک **عدد جبری** گوییم اگر a روی $\mathbb{Q}$ **جبری** باشد. اگر $a \in \mathbb{C}$ جبری نباشد، آن‌را یک **عدد متعالی** نامیم.

مثال۱: (۱) $1 + i\sqrt{2} \in \mathbb{C}$ یک عدد جبری است، زیرا ریشه‌ی $x^2 - 2x + 3 \in \mathbb{Q}[x]$ است.

(۲) $\alpha = \sum_{n=1}^{\infty} 10^{-n!}$ عددی متعالی است. α **عدد لیوویل**[1] نام دارد و اولین عدد متعالی شناخته شده است. (فصل ۶ ملاحظه شود). اعداد $\pi, e \in \mathbb{R}$ متعالی هستند. اثبات این مطالب پیچیده و درگیر مباحث آنالیزی است. برای دیدن اثبات خواننده می‌تواند به بخش‌های ۲و۳ از فصل ۶ مراجعه نماید.

□

تعریف۲-۵

فرض کنیم K یک توسیع از F و $u \in K$ روی F جبری باشد.
کوچک‌ترین (از نظر درجه) چند جمله‌ای تکین $p(x) \in F[x]$ که $p(u) = 0$ را **چندجمله‌ای مینیمال** u روی F گوییم. اگر درجه‌ی چند جمله‌ای مینیمال u روی F برابر n باشد، گوییم u **روی F جبری از درجه‌ی** n است.

[1] Liouville number

قضیه۲-۳

فرض کنیم K یک توسیع از F باشد. فرض کنیم $p(x)$ چندجمله‌ای مینیمال $u \in K$ روی F باشد. دراین‌صورت

(۱) اگر $0 \neq f(x) \in F[x]$ و $f(u) = 0$، آن‌گاه $\deg p(x) \leq \deg f(x)$

(۲) چند جمله‌ای مینیمال u روی F یکتاست،

(۳) چند جمله‌ای مینیمال u روی F تحویل‌ناپذیر است.

اثبات (۱): فرض کنیم c ضریب پیشروی $f(x)$ باشد. قرار می‌دهیم $f_*(x) = (1/c)f(x)$. دراین‌صورت $f_*(x)$ یک چندجمله‌ای تکین بوده و $f_*(u) = 0$. از این‌رو $\deg p(x) \leq \deg f_*(x) = \deg f(x)$.

(۲): فرض کنیم

$$p_1(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0,$$
$$p_2(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0,$$

دو چند جمله‌ای مینیمال u روی F باشند. دراین‌صورت با توجه به (۱)، داریم $m = n$. قرار می‌دهیم:

$$g(x) = p_1(x) - p_2(x) = (a_{n-1} - b_{n-1})x^{n-1} + \cdots + (a_1 - b_1)x + (a_0 - b_0).$$

چون $g(u) = 0$ و $\deg g(x) < n$، با توجه به (۱) باید داشته باشیم $g(x) = 0$. درنتیجه $p_1(x) = p_2(x)$.

(۳): فرض کنیم $p(x)$ چندجمله‌ای مینیمال u روی F باشد. فرض کنیم (برهان خلف) چندجمله‌ای‌های $f(x), g(x) \in F[x]$ موجود باشند به‌طوری‌که

$$p(x) = f(x)g(x),$$

که درآن، $\deg f(x) < \deg p(x)$ و $\deg g(x) < \deg p(x)$. چون K یک میدان است و $0 = p(u) = f(u)g(u)$، پس $f(u) = 0$ یا $g(u) = 0$، که با قسمت (۱) در تناقض است.

■■■

لم۲-۱

فرض کنیم K یک توسیع از F و $u \in K$ روی F جبری از درجه‌ی n باشد. دراین‌صورت

(۱) $F(u) = \{a_0 + a_1u + \cdots + a_{n-1}u^{n-1} \mid a_i \in F\}$،

(۲) $\mathcal{B} = \{1, u, \cdots, u^{n-1}\}$ یک پایه برای فضای برداری $F(u)$ روی F است.

اثبات(۱): کافی است نشان دهیم $A = \{a_0 + a_1u + \cdots + a_{n-1}u^{n-1} \mid a_i \in F\}$ یک زیرمیدان K است. به‌وضوح A نسبت به عمل جمع یک گروه آبلی است. فرض کنیم

$$p(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + x^n$$

چند جمله‌ای مینیمال u روی F باشد. دراین‌صورت

$u^n = -(b_0 + b_1u + \cdots + b_{n-1}u^{n-1})$. هم‌چنین

$$\begin{aligned} u^{n+1} &= uu^n \\ &= -(b_0u + b_1u^2 + \cdots + b_{n-2}u^{n-1} + b_{n-1}u^n) \\ &= -(b_0u + b_1u^2 + \cdots + b_{n-2}u^{n-1}) - b_{n-1}u^n \\ &= -(b_0u + b_1u^2 + \cdots + b_{n-2}u^{n-1}) + b_{n-1}(b_0 + b_1u + \cdots + b_{n-1}u^{n-1}) \end{aligned}$$

با ادامه‌ی این روند می‌توان مشاهده نمود که u^m برای $m \geq n$ یک ترکیب خطی از $u^{n-1}, \ldots, u, 1$ روی F است. بنابراین A نسبت به عمل ضرب بسته است. حال وجود معکوس ضربی را بررسی می‌کنیم. فرض کنیم $c = a_0 + a_1u + \cdots + a_{n-1}u^{n-1}$، که $a_i \in F$، یک عنصر غیرصفر از A می‌باشد. قرار می‌دهیم:

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}.$$

چون $c = f(u) \neq 0$، پس $p(x) \nmid f(x)$ و با توجه به تحویل‌ناپذیر بودن $p(x)$، داریم $(p(x), f(x)) = 1$. ازاین‌رو چندجمله‌ای‌های $r(x), s(x) \in F[x]$ موجودند به‌طوری‌که $r(x)p(x) + s(x)f(x) = 1$. بنابراین $r(u)p(u) + s(u)f(u) = 1$ و چون $p(u) = 0$ داریم $s(u)f(u) = 1$. از طرفی طبق آن‌چه گفته شد، $s(u) \in A$. یعنی $c = f(u)$ در A معکوس‌پذیر است؛ ازاین‌رو A یک میدان است.

(۲): با توجه به قسمت (۱)، کافی است ثابت کنیم که $\mathcal{B}$ مستقل خطی است. فرض کنیم (برهان خلف) $\mathcal{B}$ مستقل خطی نباشد. دراین‌صورت عناصر $c_i \in F$ که همگی صفر نیستند موجودند به‌طوری‌که $c_0 + c_1u + \cdots + c_{n-1}u^{n-1} = 0$. فرض کنیم

$$f(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$$

دراین‌صورت $0 \neq f(x) \in F[x]$، $\deg f(x) < n$ و $f(u) = 0$، که با قضیه‌ی۳(۱) در تناقض است.

■■■

قضیه۲-۴

فرض کنیم K یک توسیع از F و $u \in K$. دراین‌صورت

u روی F جبری از درجه‌ی n است $\Leftrightarrow [F(u) : F] = n$.

اثبات ($\Leftarrow$): از لم قبل نتیجه می‌شود.

($\Rightarrow$) : فرض کنیم $[F(u) : F] = n$. دراین‌صورت $\{1, u, \cdots, u^{n-1}, u^n\}$ یک مجموعه‌ی وابسته‌ی خطی روی F است. ازاین‌رو عناصر $c_i \in F$ که همگی صفر نیستند موجودند به‌گونه‌ای که $c_0 + c_1u + \cdots + c_{n-1}u^{n-1} + c_nu^n = 0$. بنابراین u ریشه‌ای از چند جمله‌ای غیر صفر $f(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + c_nx^n$ است و در نتیجه u روی F جبری است. حال فرض کنیم u روی F جبری از درجه‌ی m باشد. دراین‌صورت با توجه به قسمت اول، $[F(u) : F] = m$. در نتیجه $m = n$ و لذا u روی F جبری از درجه‌ی n است.

■■■

نتیجه۲-۲

فرض کنیم K یک توسیع از F باشد و $u \in K$. دراین‌صورت

(۱) u روی F جبری است $\Leftrightarrow [F(u) : F] < \infty$،

(۲) اگر K یک توسیع متناهی از F باشد ، آن‌گاه K یک توسیع جبری از F است.

اثبات: (۱) ($\Leftarrow$) :فرض کنیم u روی F جبری از درجه‌ی n باشد. دراین‌صورت با توجه به قضیه‌ی اخیر داریم $[F(u):F]=n<\infty$.

($\Rightarrow$) :حال فرض کنیم $n=[F(u):F]<\infty$. دراین‌صورت با استفاده‌ی مجدد از قضیه‌ی اخیر خواهیم داشت که u روی F جبری از درجه‌ی n است.

(۲): فرض کنیم $u\in K$. دراین‌صورت $[F(u):F]\leq[K:F]<\infty$و لذا طبق قسمت (۱)، u روی F جبری است؛ بنابراین K یک توسیع جبری از F است.

■■■

قضیه۲-۵

فرض کنیم K یک توسیع از F باشد. دراین‌صورت گزاره‌های زیر معادلند:

(۱) $[K:F]<\infty$،

(۲) عناصر جبری $u_1,\ldots,u_n$ از K روی F موجودند به‌گونه‌ای‌که

$$K=F(u_1,\ldots,u_n).$$

اثبات(۱) $\Leftarrow$ **(۲):** فرض کنیم $\{u_1,u_2,\cdots,u_n\}$ یک پایه برای فضای برداری K روی F باشد. دراین‌صورت $K=F(u_1,\ldots,u_n)$. از طرفی طبق قسمت (۲) نتیجه‌ی اخیر، u_iها روی F جبرینند.

(۲) $\Leftarrow$ **(۱):** u_iها برای هر $1\leq i\leq n$ روی $K=F(u_1,\ldots,u_{i-1})$ جبرینند و لذا بنابر قسمت (۱) نتیجه‌ی اخیر، $[F(u_1,\ldots,u_{i-1},u_i),F(u_1,\ldots,u_{i-1})]<\infty$. ازاین‌رو طبق نتیجه‌ی۱ داریم

$$[K:F]=$$
$$[F(u_1,\ldots,u_{n-1},u_n),F(u_1,\ldots,u_{n-1})]\cdots[F(u_1,u_2):F(u_1)][F(u_1):F]<\infty.$$

بدین ترتیب اثبات قضیه تمام است.

■■■

این بخش را با بیان دو نتیجه‌ی مهم زیر به پایان می‌بریم.

نتیجه۲-۳

فرض کنیم K یک توسیع از F باشد. دراین‌صورت مجموعه‌ی عناصر جبری روی F زیر میدانی از K خواهد بود.

اثبات: قرار می‌دهیم

$$A = \{u \in K \mid u \text{ روی } F \text{ جبری باشد}\}.$$

فرض کنیم $u, v \in A$. دراین‌صورت بنابر قضیه‌ی اخیر، $[F(u,v) : F] < \infty$. بنابراین طبق قسمت (۲) نتیجه‌ی۲، $F(u,v)$ یک توسیع جبری از F بوده و لذا $u - v$ و u / v ($v \neq 0$) روی F جبری هستند. در نتیجه A یک زیر میدان K است.

■■■

نتیجه۲-۴

فرض کنیم $F \subseteq L \subseteq K$ میدان باشند. دراین‌صورت K یک توسیع جبری از F است اگر وفقط اگر K یک توسیع جبری از L و L یک توسیع جبری از F باشد.

اثبات: اگر K یک توسیع جبری از F باشد، آن‌گاه به‌وضوح K یک توسیع جبری از L و L یک توسیع جبری از F است. به‌عکس، فرض کنیم K یک توسیع جبری از L و L یک توسیع جبری از F باشد. اگر $u \in K$ و $f(x) = a_0 + a_1x + \cdots + a_nx^n \in L[x]$ چندجمله‌ای مینیمال u روی L باشد، آن‌گاه u روی $F(a_0, a_1, \ldots, a_n)$ جبری بوده و لذا بنابر نتیجه‌ی۲:

$$[F(a_0, a_1, \ldots, a_n, u) : F(a_0, a_1, \ldots, a_n)] < \infty.$$

از طرفی بنا بر فرض a_i ها روی F جبری بوده و لذا طبق قضیه‌ی قبل $[F(a_0, a_1, \ldots, a_n) : F] < \infty$. ازاین‌رو طبق قضیه‌ی برج خواهیم داشت:

$$[F(u) : F] \leq [F(a_0, a_1, \ldots, a_n, u) : F]$$
$$= [F(a_0, a_1, \ldots, a_n, u) : F(a_0, a_1, \ldots, a_n)][F(a_0, a_1, \ldots, a_n) : F] < \infty.$$

بنابراین $u \in K$ روی F جبری است و در نتیجه K یک توسیع جبری از F خواهد بود.

■■■

تمرین‌های سطح۱

۱-(الف) نشان دهید $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. به‌عبارت‌دیگر $\mathbb{Q}(\sqrt{2},\sqrt{3})$ یک توسیع ساده از $\mathbb{Q}$ است.

(ب) فرض کنید $a,b \in \mathbb{Q}$ و $\sqrt{a}+\sqrt{b} \neq 0$. نشان دهید $\mathbb{Q}(\sqrt{a},\sqrt{b}) = \mathbb{Q}(\sqrt{a}+\sqrt{b})$.

۲- فرض کنید K یک توسیع از F باشد. فرض کنید $u \in K$ و $[F(u):F]$ عددی فرد باشد. نشان دهید $F(u) = F(u^2)$.

۳- فرض کنید K یک توسیع از F، $u,v \in K$، $m = [F(u):F]$ و $n = [F(v):F]$. نشان دهید $[F(u,v):F] \leq mn$. اگر $(m,n)=1$، آن‌گاه $[F(u,v):F] = mn$.

۴- فرض کنید K یک توسیع جبری از F و D دامنه‌ای صحیح باشد که $F \subseteq D \subseteq K$. نشان دهید D میدان است.

۵- فرض کنید K یک توسیع از F و $u \in K$ روی F متعالی باشد. نشان دهید $F(u) \cong F(x)$.

۶- ثابت یا رد کنید: $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{3})$.

۷- فرض کنید F یک میدان و $f(x) = a_0 + a_1x + \cdots + a_nx^n$ یک چندجمله‌ای تحویل‌ناپذیر روی میدان F باشد. نشان دهید $< f(x) >$ یک ایده‌آل ماکزیمال از حلقه‌ی $F[x]$ است.

تمرین‌های سطح۲

۸- فرض کنید $\alpha, \beta \in \mathbb{R}$ روی $\mathbb{Q}$ متعالی باشند. نشان دهید $\alpha\beta$ یا $\alpha+\beta$ روی $\mathbb{Q}$ متعالی‌اند.

۹- فرض کنید K یک توسیع از F و $u \in K$ روی F متعالی باشد. نشان دهید هر عنصر از $F(u)$ که در F نباشد، روی F متعالی است.

۱۰-فرض کنید $a, b \in \mathbb{Q}$ و $b \neq 0$. نشان دهید $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ اگر و فقط اگر عنصر $c \in \mathbb{Q}$ چنان موجود باشد که $a = bc^2$.

۱۱- فرض کنید K یک توسیع متناهی از F باشد. نشان دهید K یک توسیع ساده از F است اگر و فقط اگر تعداد میدان‌های میانی توسیع K روی F متناهی باشد.

تمرین‌های سطح ۳

۱۲- فرض کنید F میدانی با مشخصه‌ی صفر باشد. نشان دهید هر توسیع متناهی از F یک توسیع ساده از F است.

۱۳- توسیع K از میدان F را **بستار جبری** F نامیم، هرگاه K یک توسیع جبری از F بوده و K به‌طور جبری بسته باشد. نشان دهید:

(الف) هر میدان F دارای بستار جبری است،

(ب) اگر K_1 و K_2 دو بستار جبری از میدان F باشند، آن‌گاه یکریختی $\sigma : K_1 \to K_2$ موجود است به‌قسمی که $\sigma|_F = \mathrm{id}$.

۱۴-فرض کنید $p_n, \ldots, p_1$ اعداد اول متمایزی باشند. نشان دهید

$$[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n.$$

۲-۱ ترسیم به‌وسیله‌ی خط‌کش و پرگار

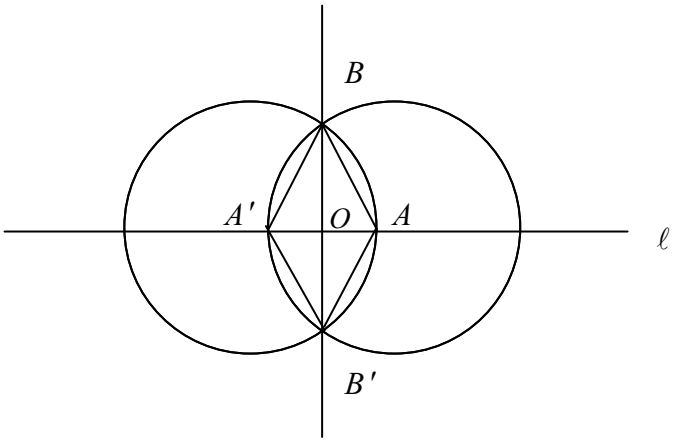
با برخی از ترسیمات به‌وسیله‌ی خط‌کش و پرگار در هندسه‌ی متوسطه آشنا هستید. به عنوان مثال به چند مسئله اشاره می‌کنیم:

مسئله۱

خط ℓ و نقطه‌ی O واقع بر آن داده شده است. با استفاده از خط‌کش و پرگار، خطی رسم می‌کنیم که از O گذشته و بر ℓ عمود باشد.

حل: نقطه‌ای دلخواه و متمایز با O مانند A را بر خط ℓ انتخاب می‌کنیم (شکل ۲-۱ ملاحظه شود). به مرکز O وشعاع OA یک دایره ترسیم کرده تا خط ℓ را در نقطه‌ی A' قطع کند. حال به مرکز A و A' وشعاع AA' دو دایره ترسیم می‌کنیم. محل تلاقی دو دایره را B و B' می‌نامیم. با توجه به لوزی بودن چهار ضلعی $ABA'B'$، خط گذرنده از B و B' که از O نیز می‌گذرد بر ℓ عمود است.

■■■



شکل ۲-۱

حل دو مسئله‌ی زیر را به خواننده واگذار می‌کنیم.

مسئله۲

خط ℓ ونقطه‌ی O خارج از آن داده شده است. با استفاده از خط‌کش و پرگار، خطی رسم کنید که از O گذشته و بر ℓ عمود باشد.

مسئله۳

خط ℓ ونقطه‌ی O خارج از آن داده شده است. با استفاده از خط‌کش و پرگار، خطی رسم کنید که از O گذشته و با ℓ موازی باشد.

صفحه‌ی اقلیدسی (یعنی $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$) را در نظر بگیرید. با استفاده از خط‌کش و پرگار دو خط عمود برهم مانند x و y ترسیم نمایید (این دو خط را محورهای مختصات می‌نامیم). محل تلاقی این دو خط را نقطه‌ی $(0,0)$ نام‌گذاری می‌کنیم (مبدا مختصات). نقطه‌ای دلخواه سمت راست $(0,0)$ انتخاب کرده و آن‌را $(1,0)$ می‌نامیم (واحد مختصات).

حال تعریف زیر را مطرح می‌کنیم:

تعریف ۲-۶

نقطه‌ی (a,b) از صفحه‌ی اقلیدسی را **ترسیم‌پذیر** گوییم، هرگاه بتوان آن‌را به‌وسیله‌ی خط‌کش و پرگار با شروع از نقاط $(0,0)$ و $(1,0)$ مشخص کرد.

به آسانی مشاهده می‌شود که نقاطی که مختصات آن‌ها صحیح است، ترسیم‌پذیر هستند. حال این سوال مطرح می‌شود:

سوال

دقیقاً چه نقاطی از صفحه‌ی اقلیدسی ترسیم‌پذیر هستند؟

اثبات گزاره‌ی زیر آسان و به عهده‌ی خواننده واگذار می‌شود.

گزاره۲-۱

(۱) نقطه‌ی $(a,b) \in \mathbb{R}^2$ ترسیم‌پذیراست اگر و فقط اگر نقاط $(a,0)$ و $(0,b)$ ترسیم‌پذیر باشند.

(۲) نقطه‌ی $(c,0) \in \mathbb{R}^2$ ترسیم‌پذیراست اگر و فقط اگر نقطه‌ی $(0,c)$ ترسیم‌پذیر باشد.

طبق گزاره‌ی بالا برای بررسی سوال مطرح شده، می‌توان توجه خود را به ترسیم‌پذیری نقطه‌ی $(c,0) \in \mathbb{R}^2$ معطوف کرد. از این رو تعریف زیر را مطرح می‌کنیم:

تعریف ۲-۷

عدد حقیقی $c \in \mathbb{R}$ را ترسیم‌پذیر گوییم، هرگاه نقطه‌ی $(c,0) \in \mathbb{R}^2$ ترسیم‌پذیر باشد.

قضیه۲-۶

فرض کنیم $\mathcal{C} = \{c \in \mathbb{R} \mid c$ ترسیم‌پذیر باشد$\}$. دراین‌صورت

(الف) $\mathcal{C}$ زیرمیدانی از $\mathbb{R}$ و حاوی $\mathbb{Q}$ است،

(ب) اگر $c \in \mathcal{C}$ و $c > 0$، آن‌گاه $\sqrt{c} \in \mathcal{C}$.

اثبات (الف): ابتدا متذکر می‌شویم که به‌وضوح $c \in \mathcal{C}$ اگر وفقط اگر $-c \in \mathcal{C}$.

فرض کنیم $a,b \in \mathcal{C}$. ابتدا نشان می‌دهیم $a-b \in \mathcal{C}$. اگر $a=0$ یا $b=0$ مطلب به‌وضوح برقرار است. اکنون حالات زیر را در نظر می‌گیریم:

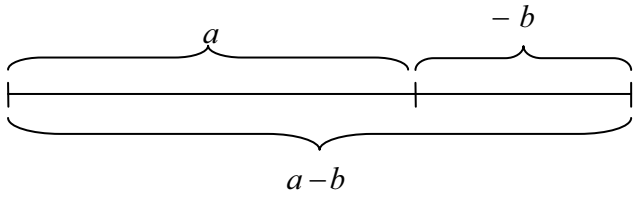
(۱) $a>0$ و $b<0$،

(۲) $a>0$ و $b>0$،

(۳) $a<0$ و $b>0$،

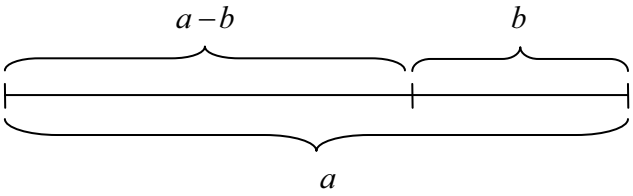
(۴) $a<0$ و $b<0$.

حالت (۱): در این حالت پاره‌خطی به‌طول a ترسیم کرده، با خط‌کش این پاره‌خط را ادامه می‌دهیم. با استفاده از پرگار پاره‌خطی به‌طول b $-$ در امتداد آن جدا می‌کنیم (شکل ۲-۲ ملاحظه شود). بدین ترتیب نشان داده‌ایم $a-b \in \mathcal{C}$.



شکل ۲-۲

حالت (۲): فرض کنیم $b \le a$. پاره‌خطی به‌طول a ترسیم کرده، با استفاده از پرگار پاره‌خطی به‌طول b از آن جدا می‌کنیم (شکل ۲-۳ ملاحظه شود). این کار پاره‌خطی به‌طول $a-b$ می‌سازد. اگر $b \ge a$، آن‌گاه به‌طریق مشابه $b-a$ قابل ترسیم بوده و در نتیجه طبق تذکر مطرح شده در ابتدای اثبات، $a-b \in \mathcal{C}$.



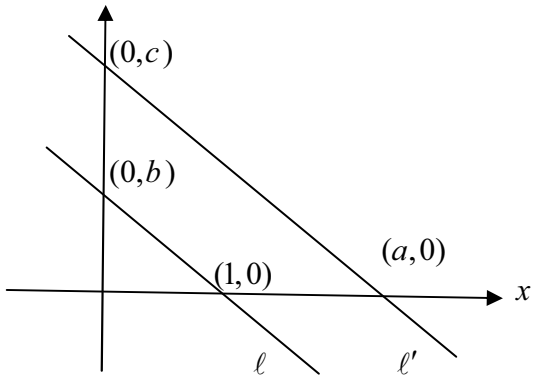
شکل ۲-۳

حالت‌های (۳) و (۴) با توجه به تذکر داده شده به حالت‌های (۱) و (۲) برمی‌گردند.

حال نشان می‌دهیم $ab \in \mathcal{C}$. خط گذرنده از نقاط $(1,0)$ و $(0,b)$ را ℓ می‌نامیم. از نقطه‌ی $(a,0)$ خط ℓ' را موازی خط ℓ ترسیم می‌کنیم تا محور yها را در نقطه‌ی $(0,c)$ قطع کند (شکل ۲-۴ ملاحظه شود). با استفاده از تشابه مثلث‌ها (یا قضیه‌ی تالس)، خواهیم داشت:

$$1/a = b/c.$$

بنابراین خط ℓ' محور y را در نقطه‌ی $c = ab$ قطع خواهد کرد و ازاین‌رو $ab \in \mathcal{C}$.

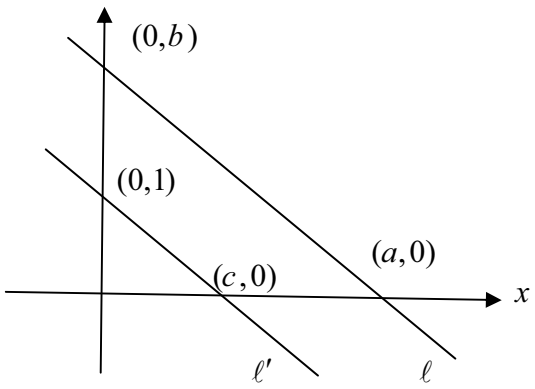


شکل ۲-۴

حال فرض کنیم $b \neq 0$. نشان می‌دهیم $a/b \in \mathcal{C}$. فرض کنیم ℓ خط گذرنده از نقـاط $(a,0)$ و $(0,b)$ باشد. خط ℓ' را از نقطه‌ی $(0,1)$ و موازی با ℓ ترسیم می‌کنیم تـا محـور xها را در نقطه‌ی $(c,0)$ قطع کند (شکل ۲-۵ ملاحظـه شـود). بـا بـه‌کـارگیری تشـابه مثلث‌ها (یا قضیه‌ی تالس)، خواهیم داشت

$$1/b = c/a.$$

بنابراین خط ℓ' محور x را در نقطه‌ی $c = a/b$ قطع خواهد کرد و از این‌رو $a/b \in \mathcal{C}$. بدین ترتیب نشان داده‌ایم که $\mathcal{C}$ یک میدان است.

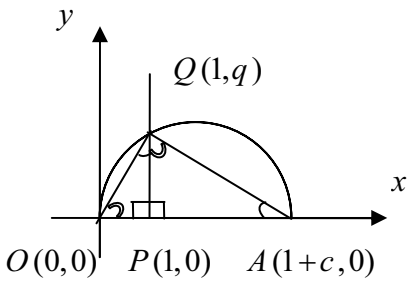


شکل ۲-۵

(ب): دایره‌ای با قطری برابر با قطعـه خـط واصـل نقـاط $O = (0,0)$ و $A = (1+c,0)$ روی محور xها ترسیم می‌کنیم (شکل ۲-۶ ملاحظه شود). اگـر از نقطـه‌ی $P = (1,0)$ عمودی بر محور xها ترسیم کنیم تا دایره را در نقطه‌ی $Q = (1,q)$ قطع کند، آن‌گاه بـا توجه به تشابه مثلث‌های OPQ و PQA خواهیم داشت:

$$q/c = 1/q.$$

بنابراین $q = \sqrt{c}$ و از این‌رو $\sqrt{c} \in \mathcal{C}$.



■■■

شکل ۲-۶

نتیجه۲-۵

فرض کنیم $F \leq K \leq \mathbb{R}$، $[K:F]=2$ و $F \leq \mathcal{C}$. دراین‌صورت $K \leq \mathcal{C}$.

اثبات: اگر $u \in K-F$، آن‌گاه با توجه بـه قضـیه‌ی بـرج $[F(u):F]=2$ و در نتیجـه طبق قضیه‌ی ۴ و لم۱ عناصر $a_1,a_2 \in F$ موجودند که $u^2=a_1u+a_2$. قـرار مـی‌دهـیم $c=\left|u-a_1/2\right|$. دراین‌صورت $K=F(c)$، $c>0$ و $c^2 \in F$. حال چون $c^2 \in \mathcal{C}$، پس با توجه به قضیه‌ی قبل، داریم $c \in \mathcal{C}$. ازاین‌رو با توجه به میدان بودن $\mathcal{C}$، خواهیم داشت $K=F(c) \leq \mathcal{C}$.

■■■

در انتهای فصل سوم به تعمیم این نتیجه خواهیم پرداخت (قضیه‌ی ۳-۹ ملاحظه شود).

تعریف ۲-۸

فرض کنیم F زیرمیدانی از $\mathbb{R}$ باشد.

(۱) منظور از صفحه‌ی F زیرمجموعه‌ی $F \times F$ از صفحه‌ی $\mathbb{R}^2$ است.

(۲) هر خط که از دو نقطه از صفحه‌ی F بگذرد یک خط در صفحه‌ی F نام دارد.

(۳) دایره‌ای که مرکزش عنصری از صفحه‌ی F و شعاعش عنصری از F باشد را دایره‌ای در صفحه‌ی F نامند.

فرض کنیم F زیرمیدانی از $\mathbb{R}$ باشد. تنها راه رسیدن به نقاط جدید با استفاده از صفحه و خط‌کش و پرگار تنها به یکی از طرق زیر است:

(۱) اشتراک دو خط از F.

(۲) اشتراک یک خط و یک دایره از F.

(۳) اشتراک دو دایره از F.

قضیه۲-۷

اگر F زیرمیدانی از $\mathbb{R}$ باشد، آن‌گاه موارد زیر برقرار است.

(۱) هر خط در صفحه‌ی F دارای معادله‌ای به‌صورت $ax + by = c$ است که در آن $a, b, c \in F$.

(۲) هر دایره در صفحه‌ی F دارای معادله‌ای به‌صورت $x^2 + y^2 + ax + by = c$ است که در آن $a, b, c \in F$.

اثبات(۱): خط گذرنده از نقاط (a_1, a_2) و (b_1, b_2) از صفحه‌ی F عبارت است از

$$(x - a_1)/(y - a_2) = (b_1 - a_1)/(b_2 - a_2).$$

بنابراین حکم با استفاده از میدان بودن F به‌دست می‌آید.

(۲): معادله‌ی دایره به شعاع $r \in F$ و مرکز $(a_1, a_2) \in F \times F$ عبارت است از

$$(x - a_1)^2 + (y - a_2)^2 = r^2.$$

ازاین‌رو حکم با استفاده از میدان بودن F به‌دست می‌آید.

■■■

قضیه۲-۸

فرض کنیم F زیرمیدانی از $\mathbb{R}$، و ℓ_1 و ℓ_2 دو خط نا موازی و C_1 و C_2 دو دایره‌ی متمایز در صفحه‌ی F باشند. دراین‌صورت

(۱) $\ell_1 \cap \ell_2$ عنصری از صفحه F است.

(۲) اگر $\ell_1 \cap C_1 \neq \varnothing$ ، آن‌گاه $\ell_1 \cap C_1$ متشکل از یک یا دو نقطه از صفحه‌ی $F(u)$ است که در آن $u \in \mathbb{R}$ و $u^2 \in F$.

(۳) اگر $C_1 \cap C_2 \neq \varnothing$ ، آن‌گاه $C_1 \cap C_2$ متشکل از یک یا دو نقطه از صفحه‌ی $F(u)$ است که در آن $u \in \mathbb{R}$ و $u^2 \in F$.

اثبات: فرض کنیم معادلات خطوط ℓ_1 و ℓ_2 و دوایر C_1 و C_2 داده شده باشند؛ یعنی

$$\ell_1 : a_1x + b_1y = c_1 \qquad \ell_2 : a_2x + b_2y = c_2$$

$$C_1 : x^2 + y^2 + d_1x + e_1y = f_1 \qquad C_2 : x^2 + y^2 + d_2x + e_2y = f_2$$

که در آن‌ها $a_i, b_i, c_i, d_i, e_i, f_i \in F$

(۱): فرض کنیم (x_0, y_0) نقطه‌ی اشتراک دو خط ℓ_1 و ℓ_2 باشد. دراین‌صورت طبق قاعده‌ی کرامر داریم:

$$y_0 = \begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix} / \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \text{ و } x_0 = \begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix} / \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$$

ازاین‌رو (x_0, y_0) نقطه‌ای از صفحه‌ی F است.

(۲): واضح هست که a_1, b_1 هر دو با هم صفر نیستند. بدون این‌که از کلیت مسئله کاسته شود می‌توانیم فرض کنیم $a_1 \neq 0$. فرض کنیم $(x_0, y_0) \in \ell_1 \cap C_1$. از معادله‌ی خط ℓ_1 داریم $x_0 = (-b_1 / a_1)y_0 + (c_1 / a_1)$. با جایگزین کردن این مقدار در معادله‌ی C_1، به معادله‌ی $ay_0^2 + by_0 + c = 0$، که در آن $a, b, c \in F$ و $a \neq 0$، می‌رسیم. بنابراین $y_0 = (-b \pm u) / 2a$، که در آن $u = \sqrt{b^2 - 4ac}$ و در نتیجه هر دوی x_0 و y_0 در F و یا در $F(u)$، که در آن $u \in \mathbb{R}$ و $u^2 \in F$، قرار می‌گیرند.

(۳): با کم کردن معادله‌ی C_1 از C_2 داریم

$$(d_1 - d_2)x + (e_1 - e_2)y = (f_1 - f_2),$$

که معادله‌ی خطی مانند ℓ در صفحه‌ی F است. پس $C_1 \cap C_2$ با $\ell \cap C_1$ برابر است و قسمت (۳) به قسمت (۲) تحویل می‌یابد.

■■■

قضیه۲-۹

فرض کنیم $c \in \mathcal{C}$ (یعنی c، عددی ترسیم پذیر است). دراین‌صورت $n \in \mathbb{N}_0$ موجود است به‌طوری‌که $[\mathbb{Q}(c) : \mathbb{Q}] = 2^n$.

اثبات: فرض کنیم با شروع از صفحه‌ی $\mathbb{Q}$ و پس از m ترسیم به نقطه‌ی c برسیم. اولین نقطه‌ی ترسیم شده با توجه به قضیه‌ی قبل در صفحه‌ی $\mathbb{Q}(u_1)$ که $u_1^2 \in \mathbb{Q}$، قرار دارد. دومین نقطه‌ی ترسیم شده با استفاده‌ی مجدد از قضیه‌ی قبل در صفحه‌ی $\mathbb{Q}(u_1)(u_2) = \mathbb{Q}(u_1, u_2)$، که $u_2^2 \in \mathbb{Q}(u_1)$، قرار دارد. با ادامه‌ی این روند، توسیع‌های زیر از $\mathbb{Q}$ را خواهیم داشت

$$\mathbb{Q} \subseteq \mathbb{Q}(u_1) \subseteq \mathbb{Q}(u_1, u_2) \subseteq \cdots \subseteq \mathbb{Q}(u_1, u_2, \cdots, u_m)$$

که در آن $u_i^2 \in \mathbb{Q}(u_1, u_2, \cdots, u_{i-1})$، برای هر $1 \leq i \leq m$ و $c \in \mathbb{Q}(u_1, u_2, \cdots, u_m)$. ازاین‌رو برای هر $1 \leq i \leq m$ داریم:

$$[\mathbb{Q}(u_1, u_2, \cdots, u_i) : \mathbb{Q}(u_1, u_2, \cdots, u_{i-1})] = 1 \text{ یا } 2$$

بنابراین طبق نتیجه‌ی۲-۱، عدد $t \in \mathbb{N}$ موجود است که به‌طوری‌که $[\mathbb{Q}(u_1, u_2, \cdots, u_m) : \mathbb{Q}] = 2^t$. چون $\mathbb{Q} \subseteq \mathbb{Q}(c) \subseteq \mathbb{Q}(u_1, u_2, \cdots, u_m)$، پس طبق قضیه‌ی برج، عدد طبیعی n موجود است به‌گونه‌ای که $[\mathbb{Q}(c) : \mathbb{Q}] = 2^n$. بدین ترتیب اثبات قضیه تمام است.

■■■

حال با توجه به قضیه‌ی بالا می‌توانیم به سوال‌های مطرح شده در ابتدای این فصل پاسخ دهیم.

قضیه۲-۱۰

تربیع دایره غیرممکن است؛ یعنی، به‌کمک خط‌کش و پرگار ترسیم مربعی که مساحتش با مساحت دایره‌ای مفروض، مساوی باشد، غیر ممکن است.

اثبات: فرض کنیم دایره‌ی مفروض با شعاع ۱ و لذا با مساحت π باشد. فرض کنیم (برهان خلف) مربعی با مساحت π ترسیم‌پذیر باشد. دراین‌صورت $\sqrt{\pi}$ (ضلع مربع) ترسیم‌پذیر بوده و در نتیجه $\pi = \sqrt{\pi}^2$ نیز ترسیم‌پذیر بوده و لذا با توجه به قضیه‌ی ۲-۹، $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2^n$ برای یک عدد طبیعی $n \in \mathbb{N}$، که یک تناقض است.

■■■

قضیه۲-۱۱

تضعیف مکعب غیرممکن است؛ یعنی، به‌کمک خط‌کش و پرگار ترسیم مکعبی که حجمش دو برابر حجم مکعبی مفروض باشد، غیرممکن است.

اثبات: فرض کنیم مکعب مفروض به ضلع۱ باشد. فرض کنیم (برهان خلف) مکعبی با حجم ۲ ترسیم‌پذیر باشد. در این صورت $\sqrt[3]{2}$ (ضلع مکعب) ترسیم‌پذیر بوده. اما $\sqrt[3]{2}$ ریشه‌ی چند جمله‌ای تحویل‌ناپذیر $f(x) = x^3 - 2$ روی $\mathbb{Q}$ است و لذا $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$، که تناقض است.

■■■

تعریف۲-۹

زاویه‌ی θرا **ترسیم‌پذیر** گوییم اگر بتوان نقاط ترسیم‌پذیر A و B را یافت به‌طوری‌که اندازه‌ی زاویه‌ی AOB (که Oمبدا است) برابر θ باشد.

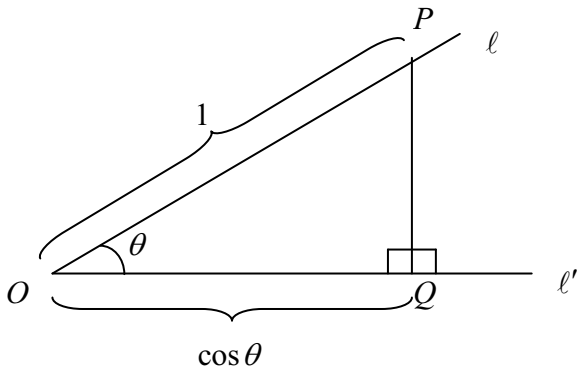
لم۲-۲

فرض کنیم $\theta \in \mathbb{R}$. دراین‌صورت گزاره‌های زیر معادلند.

(۱) زاویه‌ی θ ترسیم‌پذیر است،

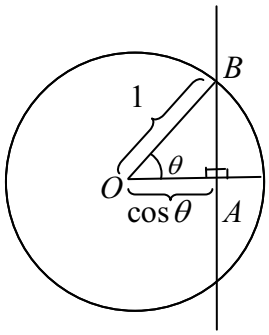
(۲) عدد $\cos\theta$ ترسیم‌پذیر است.

اثبات (۱) $\Leftarrow$ (۲): فرض کنیم نقاط ترسیم‌پذیر A و B به‌گونه‌ای باشند که اندازه‌ی زاویه‌ی AOB (که Oمبدا است) برابر θ باشد. فرض کنیم ℓ و ℓ' به‌ترتیب نیم‌خط‌های گذرنده از پاره‌خط‌های OAو OBباشند. نقطه‌ی P را برخط ℓ چنان انتخاب می‌کنیم که طول OP برابر ۱ باشد. از نقطه‌ی Pخطی عمود بر خط ℓ' رسیم می‌کنیم تا ℓ' را در نقطه‌ی Qقطع کند (شکل ۲-۷ ملاحظه شود). اندازه‌ی OQ برابر $\cos\theta$ بوده و لذا $\cos\theta$ ترسیم‌پذیر است.



شکل ۲-۷

(۲) $\Leftarrow$(۱): فرض کنیم طول پاره‌خط OA برابر $\cos\theta$ باشد. از نقطه‌ی A عمودی بر OA اخراج می‌کنیم تا دایره‌ی واحد به مرکز Oرا در نقطه‌ی B قطع کند(شکل ۲-۸ ملاحظه شود). اندازه‌ی زاویه‌ی AOB (که Oمبدا است) برابر θ بوده و لذا زاویه‌ی θ ترسیم‌پذیر است.



شکل ۲-۸

■■■

قضیه۲-۱۲

تثلیث زاویه 60° غیرممکن است؛ یعنی، زاویه‌ای وجود دارد که تنها به‌کمک خط‌کش و پرگار، نمی‌توان آن‌را به سه قسمت مساوی تقسیم کرد.

اثبات: فرض کنیم (برهان خلف) بتوانیم زاویه‌ی 60° را تثلیث کنیم. دراین‌صورت زاویه‌ی $\theta = 20^\circ$ ترسیم‌پذیر است و در نتیجه با توجه به لم قبل $\cos\theta$ نیز ترسیم‌پذیر است. با به‌کارگیری تساوی‌های مثلثاتی داریم

$$1/2 = \cos 60^\circ = 4\cos^3\theta - 3\cos\theta$$

از این‌رو $\cos\theta$ در چند جمله‌ای تحویل‌ناپذیر $f(x) = 8x^3 - 6x - 1$ روی $\mathbb{Q}$ صدق می‌کند. بنابراین $[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = 3$، که تناقض است.

■■■

یونانیان باستان به کمک خط‌کش و پرگار قادر به ترسیم برخی از چند ضلعی‌های منتظم بودند. برای مثال آن‌ها می‌توانستند ۵-ضلعی و۶-ضلعی منتظم را ترسیم کنند. اما از ترسیم بسیاری از چند ضلعی‌های منتظم عاجز بودند؛ به‌عنوان نمونه، راهی برای ترسیم۷-ضلعی منتظم در دست نداشتند. ترسیم ۱۷- ضلعی منتظم اولین بار توسط **کارل فریدریش گاوس**[1] انجام شد. گاوس چنان شیفته‌ی این ترسیم شد که وصیت کرد که بر سنگ قبرش۱۷-ضلعی منتظم حک شود.

[1]Carl Friedrich Gauss

گزاره۲-۲

فرض کنیم n یک عدد طبیعی بزرگ‌تر یا مساوی۳ باشد. n-ضلعی منتظم ترسیم‌پذیر است اگر و فقط اگر زاویه‌ی $2\pi / n$ ترسیم‌پذیر باشد.

اثبات: به‌عنوا ن‌تمرین به‌عهده‌ی خواننده واگذار می‌شود.

■■■

قضیه۲-۱۳

ترسیم ۷-ضلعی منتظم با به‌کارگیری تنها خط‌کش و پرگار غیرممکن است.

اثبات: فرض کنیم (برهان خلف) ۷-ضلعی منتظم ترسیم‌پذیر باشد. دراین‌صورت $\alpha = 2\cos(2\pi / 7)$ ترسیم‌پذیر است. اما α ریشه‌ی چندجمله‌ای تحویل‌ناپذیر $f(x) = x^3 + x^2 - 2x - 1$ روی $\mathbb{Q}$ است (تمرین ۱ از بخش ۱-۵ ملاحظه شود) و لذا $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$، که تناقض است.

■■■

گزاره۲-۳

فرض کنیم m و n دو عدد طبیعی بزرگ‌تر یا مساوی۳ باشد. دراین‌صورت

(۱) اگر n-ضلعی منتظم ترسیم‌پذیر و $m \mid n$، آن‌گاه m-ضلعی منتظم ترسیم‌پذیر است.

(۲) اگر m و n-ضلعی‌های منتظم ترسیم‌پذیر و اعداد m و n نسبت به‌هم اول باشند، آن‌گاه mn-ضلعی منتظم ترسیم‌پذیر است.

اثبات(۱): فرض کنیم $d = \frac{m}{n}$. با وصل کردن هر رأس dام یک n-ضلعی منتظم، می‌توانیم یک m-ضلعی منتظم ترسیم کنیم.

(۲): اعداد صحیح a و b موجودند به‌طوری‌که $am + bn = 1$. بنابراین

$$\frac{2\pi}{mn} = a.\frac{2\pi}{m} + b\frac{2\pi}{n}.$$

ازاین‌رو زاویه‌ی $\frac{2\pi}{mn}$ را می‌توان با استفاده از زاویه‌های $\frac{2\pi}{m}$ و $\frac{2\pi}{n}$ ترسیم کرد و لذا mn-ضلعی منتظم ترسیم‌پذیر است.

■■■

نتیجه‌ی بعدی به‌آسانی از گزاره‌ی قبل به‌دست می‌آید.

نتیجه ۲-۶

فرض کنیم $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ که در آن $p_1,\dots,p_r$ اعداد اول متمایزند. دراین‌صورت n-ضلعی منتظم ترسیم‌پذیر اگر و فقط اگر هر یک از $p_i^{\alpha_i}$-ضلعی‌های منتظم ترسیم‌پذیر باشند.

این بخش را با بیان قضیه‌ی زیر (قضیه‌ی گاوس) که به‌طور دقیق چند ضلعی‌های منتظم ترسیم‌پذیر را مشخص می‌کند به پایان می‌بریم (به‌دلیل نداشتن ابزار لازم، اثبات آن‌را به فصل ۵ موکول می‌کنیم). ابتدا اعداد اول فرما را معرفی می‌کنیم.

تعریف۲-۱۰

هر عدد اول به‌شکل $2^m + 1$ (که $m \in \mathbb{N}_0$) یک **عدد اول فرما**[1] نام دارد.

نخستین پنج عدد اول فرما عبارتند از:

۳، ۵، ۱۷، ۲۵۷ و ۶۵۵۳۷

قضیه۲- ۱۴ (قضیه‌ی گاوس)

فرض کنیم n یک عدد طبیعی بزرگ‌تر یا مساوی 3 باشد. n-ضلعی منتظم ترسیم‌پذیر است اگر و فقط اگر $n = 2^\alpha p_1 \dots p_\beta$ که در آن $\alpha \in \mathbb{N}_0$ و p_iها اعداد اول متمایز فرما هستند.

[1] Fermat Prime Number

هر راه حلی که برای مسئله‌ای پیدا می‌کنم به‌عنوان سرمشق به من کمک می‌کند تا مسئله‌های دیگری را هم به نتیجه برسانم.

(دکارت)

تمرین‌های سطح۱

۱- نشان دهید ۵-ضلعی و۶-ضلعی منتظم ترسیم‌پذیرهستند.

۲- ثابت کنید ۹-ضلعی منتظم ترسیم‌پذیر نیست.

۳- ثابت کنید برای هر عدد طبیعی $\alpha \geq 2$، 2^{α}-ضلعی منتظم ترسیم‌پذیر است.

تمرین‌های سطح۲

۴-ثابت کنید ۱۰-ضلعی منتظم ترسیم‌پذیر است.

۵-ثابت کنید زاویه‌ی 72° را می‌توان تثلیث نمود.

۶- نشان دهید $\cos 1^{\circ}$ روی $\mathbb{Q}$ جبری است اما ترسیم‌پذیر نیست.

تمرین‌های سطح۳

۷-ثابت کنید۱۷-ضلعی منتظم ترسیم‌پذیر است.

۸- فرض کنیم $S = \{\alpha \mid \alpha$ یک زاویه تثلیث‌پذیر باشد$\}$. نشان دهید S شماراست.

۹- یک شرط لازم و کافی برای عدد α بیابید به‌طوری‌که زاویه‌ی α تثلیث‌پذیر باشد.

منابعی برای مطالعه‌ی بیشتر

۱. محمدی حسن آبادی، علی اکبر. **جبر**. انتشارات دانشگاه اصفهان (۱۳۷۲).

۲. فنریک، مارین. اچ. **مقدمه‌ای بر تناظر گالوا**. ترجمه‌ی شریف، حبیب. انتشارات دانشگاه شیراز (۱۳۸۰).

3. Howie, J. M. *Fields and Galoies Theory*. Springer-Verlag, London, 2006.

4. Hungerford, T. *Algebra*. Springer-Verlag, New York, 1974.

5. Malik, D. S., Mordeson John M., Sen, M. K.Rotman, J. *Fundamentals of Abstract Algebra*McGraw- Hill Companies, Inc, 1996.

6. Rotman, J. *Galois Theory*. Springer-Verlag, 1998.

7. Stewart, I. *Galois Theory*. 3 nd ed., Chapam & Hall/CRC Press, 2004.

فصل ۳

نظریه‌ی گالوا

آثار گالوا که مجموعه‌ی آن‌ها فقط در یک شب نوشته شده است، صدها سال نسل‌های متعدد ریاضی‌دانان بزرگ را دچار تنگی نفس خواهد کرد.

(اریک تمپل بل)

در این فصل می‌خوانیم:

مقدمه

در این فصل ابتدا به معرفی میدان‌های شکافنده خواهیم پرداخت. سپس به‌عنوان کاربرد، نتایجی در باب میدان‌های متناهی ارائه می‌دهیم. در نهایت به بیان قضیه‌ی اساسی گالوا خواهیم پرداخت.

۳-۱ میدان‌های شکافنده

در سراسر این بخش F، K و L نشان‌دهنده‌ی میدان خواهند بود.

تعریف ۳-۱

فرض کنیم L یک توسیع میدان F و $f(x) \in F[x]$. گوییم $f(x)$ روی میدان L **شکافته** می‌شود اگر

$$f(x) = c(x - a_1)\dots(x - a_n),$$

که در آن $a_i \in L$ و $c \in F$.

کوچک‌ترین میدانی را که شامل F است و $f(x)$ روی آن شکافته می شود، **میدان شکافنده‌ی** $f(x)$ روی F نامیم.

❖ **تذکر:** در تمرین ۱۱ میدان شکافنده‌ی زیرمجموعه‌ی ناتهی $X \subseteq F[x]$، مورد بررسی قرار می‌گیرد.

مثال ۱: $\mathbb{Q}(\sqrt{2})$ میدان شکافنده چند جمله‌ای $x^2 - 2$ روی $\mathbb{Q}$ است. میدان اعداد مختلط میدان شکافنده‌ی چند جمله‌ای $x^2 + 1$ روی $\mathbb{R}$ است.

□

قضیه ۳-۱

فرض کنیم L یک توسیع میدان F و $f(x) = c(x - a_1)\dots(x - a_n)$، که در آن $a_i \in L$ و $c \in F$. دراین‌صورت $K = F(a_1, \dots, a_n)$ یک میدان شکافنده‌ی $f(x)$ روی F است.

اثبات: به وضوح $f(x)$ روی میدان K تجزیه می شود. حال فرض کنیم که K' میدانی دیگر باشد که $K' \subseteq K$ و $f(x)$ روی K' تجزیه شود:

$$f(x) = c'(x - a'_1)\dots(x - a'_n),$$

که در آن $a_i' \in K'$ و $c' \in F$. با توجه به یکتایی تجزیه‌ی L، $a_i' = a_i$ و لذا

$$K = F(a_1, \ldots, a_n) \subseteq K'.$$

ودر نتیجه $K = K'$.

■■■

قضیه۳-۲

فرض کنیم F یک میدان و $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ یک چند جمله‌ای تحویل ناپذیر روی میدان F باشد. دراین‌صورت توسیع ساده‌ی $L = F(u)$ از F موجود است به‌طوری‌که $f(u) = 0$.

اثبات: چون $f(x)$ تحویل ناپذیر است $L = F[x]/ < f(x) >$ یک میدان است (تمرین ۱۰ بخش ۱-۴ ملاحظه شود).

تعریف می‌کنیم:

$$\varphi : F \to L$$
$$a \mapsto a + < f(x) > .$$

فرض کنیم $\varphi(a_1) = \varphi(a_2)$. دراین‌صورت $a_1 - a_2 \in < f(x) >$. اگر $a_1 - a_2 \neq 0$، آن‌گاه $< f(x) >= F[x]$ و در نتیجه $f(x)$ یکال است، که تناقض است. بنابراین φ یک به یک است. ازاین‌رو F را می‌توان در میدان L نشاند، یعنی F را می‌توان با زیر میدان

$$\varphi(F) = \{a + < f(x) > | \, a \in F\}$$

از L یکی در نظر گرفت. حال نشان می‌دهیم $f(u) = 0$. قرار می‌دهیم $u = x + < f(x) >$. با توجه به یکسان سازی اخیر، در میدان L داریم:

$$\begin{aligned} f(u) &= \bar{a}_0 + \bar{a}_1 u + \cdots + \bar{a}_n u^n \\ &= (a_0 + a_1 x + \ldots + a_n x^n) + < f(x) > \\ &= < f(x) >= 0 \end{aligned}$$

بدین ترتیب قضیه ثابت است.

■■■

قضیه۳-۳

فرض کنیم F یک میدان و $f(x)$ یک چند جمله‌ای درجه‌ی n از $F[x]$ باشد. دراین‌صورت میدان شکافنده‌ی L از $f(x)$ موجود است به‌طوری‌که $[L : F] \leq n!$.

اثبات: قضیه را با استقرا روی $n = \deg f(x)$ اثبات می‌کنیم. دو حالت در نظر می‌گیریم:

حالت ۱ : فرض کنیم $f(x)$ به طور کامل روی F تجزیه شود به‌ویژه $n = 1$. دراین‌حالت F یک میدان شکافنده است و $[F : F] = 1$.

حالت ۲ : فرض کنیم $f(x)$ به طور کامل روی F تجزیه نشود و $f(x) = g(x)h(x)$ که $g(x)$ تحویل ناپذیر و $\deg g(x) > 1$. طبق قضیه‌ی قبل، توسیع ساده $K = F(u)$ موجود است به‌طوری‌که $g(u) = 0$. حال فرض کنیم $f(x) = (x-u)f_1$، تجزیه‌ای در $K[x]$ باشد. چون $\deg f_1(x) \le n-1$، لذا طبق فرض استقرا میدان شکافنده‌ی L از $f_1 \in K[x]$ روی $K[x]$ موجود است به‌طوری‌که $[L : K] \le (n-1)!$. بنابراین

$$[L : F] = [L : K][K : F] \le (n-1)!n = n!$$

برای اثبات این‌که L یک میدان شکافنده $f(x)$ است، فرض کنیم $L' \subseteq L$ و L' میدان شکافنده‌ی $f(x)$ باشد. چون $F(u) \subseteq L' \subseteq L$ و L' همه‌ی ریشه‌ی های $f_1(x)$ را داراست و با توجه به این‌که L میدان شکافنده‌ی $f_1(x)$ روی $F(u)$ است، داریم $L' = L$.

■■■

❖ **تذکر:** قضیه‌ی اخیر وجود میدان شکافنده را تضمین می‌کند. درضمن در مسئله‌ی۶، اثبات حالت کلی‌تری از این قضیه، خواسته شده است.

تعریف۳-۲

فرض کنیم $F \subseteq L$, $F' \subseteq L'$. یکریختی $\overline{\varphi} : L \to L'$ را یک توسیع از یکریختی $\varphi : F \to F'$ گوییم اگر $\overline{\varphi}|_F = \varphi$.

نمادگذاری: فرض کنیم $\varphi : F \to F'$ یک یکریختی باشد و $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$. قرار می‌دهیم:

$$\varphi(f) := \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n = \sum_{i=0}^{n} \varphi(a_i)x^i .$$

گزاره۳-۱

فرض کنیم $\varphi : F \to F'$ یک‌ریختی بوده و $f(x), g(x) \in F[x]$. دراین‌صورت

(۱) $\deg \varphi(f) = \deg f$،

(۲) $\varphi(f+g) = \varphi(f) + \varphi(g)$،

(۳) $\varphi(gf) = \varphi(f)\varphi(g)$.

اثبات: فرض کنیم $f(x) = a_0 + a_1x + \cdots + a_nx^n$ و $g(x) = b_0 + b_1x + \cdots + b_mx^m$.

(۱): اگر $\deg f = n$، آن‌گاه $a_n \neq 0$ و در نتیجه $\varphi(a_n) \neq 0$. بنابراین $\deg \varphi(f) = n$.

(۲): فرض کنیم $m \geq n$. (حالت $m \leq n$ مشابه است). دراین‌صورت

$$\begin{aligned}
\varphi(f+g) &= \varphi(a_0 + a_1x + \cdots + a_nx^n + b_0 + b_1x + \cdots + b_nx^n + \cdots + b_mx^m) \\
&= \varphi[(a_0+b_0) + (a_1+b_1)x + \cdots + (a_n+b_n)x^n + \cdots + b_mx^m] \\
&= \varphi(a_0) + \varphi(b_0) + (\varphi(a_1) + \varphi(b_1))x + \cdots \\
&+ (\varphi(a_n) + \varphi(b_n))x^n + \cdots + \varphi(b_m)x^m \\
&= \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n + \varphi(b_0) + \varphi(b_1)x \cdots + \varphi(b_m)x^m \\
&= \varphi(f) + \varphi(g).
\end{aligned}$$

(۳):

$$\begin{aligned}
\varphi(fg) &= \varphi((a_0b_0) + (a_0b_1 + a_1b_0)x + \cdots + (a_nb_m)x^{n+m}) \\
&= \varphi(a_0b_0) + \varphi(a_0b_1 + a_1b_0)x + \cdots + \varphi(a_nb_m)x^{n+m} \\
&= (\varphi(a_0)\varphi(b_0)) + (\varphi(a_0)\varphi(b_1) + \varphi(a_1)\varphi(b_0))x + \cdots + (\varphi(a_n)\varphi(b_m))x^{n+m} \\
&= (\varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n)(\varphi(b_0) + \varphi(b_1)x + \cdots + \varphi(b_m)x^m) \\
&= \varphi(f)\varphi(g).
\end{aligned}$$

■■■

گزاره۳-۲

فرض کنیم $\overline{\varphi}: L \to L'$ یک توسیع از $\varphi: F \to F'$ و $f(x) \in F[x]$.

(۱) اگر $u \in L$ ریشه‌ای برای $f(x)$ باشد، آن‌گاه $u' = \overline{\varphi}(u)$ یک ریشه برای $\varphi(f)$ است.

(۲) اگر $f(x)$ چند جمله‌ای مینیمال $u \in L$ روی F باشد، آن‌گاه $\varphi(f)$ چندجمله‌ای مینیمال $u' = \overline{\varphi}(u)$ روی میدان F' است.

اثبات (۱): فرض کنیم $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. دراین‌صورت

$$\begin{aligned}\varphi(f)(u') &= \sum_{i=0}^{n} \varphi(a_i)(u')^i = \sum_{i=0}^{n} \varphi(a_i)(\overline{\varphi}(u))^i \\ &= \sum_{i=0}^{n} \overline{\varphi}(a_i)(\overline{\varphi}(u))^i = \overline{\varphi}(\sum_{i=0}^{n} a_i u^i) \\ &= \overline{\varphi}(0) = 0\end{aligned}$$

(۲): فرض کنیم $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$ چند جمله‌ای مینیمال u روی میدان F و $g(x) = b_0 + b_1 x + \cdots + b_{m-1} x^{m-1} + x^m$ چند جمله‌ای مینیمال $u' = \overline{\varphi}(u)$ روی میدان F' باشد. دراین‌صورت

$$\begin{aligned}g(u') &= b_0 + b_1(u') + \cdots + b_{m-1}(u')^{m-1} + (u')^m \\ &= b_0 + b_1(\overline{\varphi}(u)) + \cdots + b_{m-1}(\overline{\varphi}(u))^{m-1} + (\overline{\varphi}(u))^m \\ &= 0,\end{aligned}$$

و لذا

$$\begin{aligned}\overline{\varphi}^{-1}(g(u')) &= \overline{\varphi}^{-1}(b_0) + \overline{\varphi}^{-1}(b_1)u + \ldots + \overline{\varphi}^{-1}(b_{m-1})u^{m-1} + u^m \\ &= \varphi^{-1}(b_0) + \varphi^{-1}(b_1)u + \ldots + \varphi^{-1}(b_{m-1})u^{m-1} + u^m \\ &= 0.\end{aligned}$$

با توجه به منحصربه‌فردی چندجمله‌ای مینیمال $f(x)$، داریم $m = n$ و $\varphi^{-1}(b_i) = a_i$، $0 \le i \le n-1$. ازاین‌رو

$$g(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_{m-1})x^{m-1} + x^m = \varphi(f).$$

بنابراین $\varphi(f)$ چندجمله‌ای مینیمال $u' = \overline{\varphi}(u)$ روی میدان F' است.

■■■

قضیه۳-۴ (ویژگی توسیعی توسیع‌های ساده)

فرض کنیم $\varphi: F \to F'$ یک‌ریختی بوده و $f(x) \in F[x]$. فرض کنیم u یک عنصر جبری روی F با چندجمله‌ای مینیمال f و u' یک عنصر جبری روی F' با چند جمله ای مینیمال $\varphi(f)$ باشد. دراین‌صورت φ را می‌توان به یک‌ریختی $\varphi^*: F(u) \to F'(u')$ توسیع داد.

اثبات: فرض کنیم u یک عنصر جبری از درجه‌ی n روی F باشد. دراین‌صورت هر عنصر $F(u)$ را می‌توان به‌صورت یکتایی به‌شکل $a_0 + a_1u + \cdots + a_{n-1}u^{n-1}$ نوشت. حال تعریف می‌کنیم:

$$\varphi^*: F(u) \to F'(u')$$
$$a_0 + a_1u + \cdots + a_{n-1}u^{n-1} \mapsto \varphi(a_0) + \varphi(a_1)u' + \cdots + \varphi(a_{n-1})u'^{n-1}$$

دراین‌صورت به‌آسانی می‌توان نشان داد که φ^* یک توسیع φ است. هم‌چنین داریم $\varphi^*(u) = u'$ و برای هر $a_0 \in F$، $\varphi^*(a_0) = \varphi(a_0)$.

■■■

قضیه۳-۵ (یکریخت بودن میدان‌های شکافنده)

فرض کنیم $\varphi: F \to F'$ یک‌ریختی بوده و $f(x) \in F[x]$. اگر L میدان شکافنده‌ی $f(x)$ روی F و L' میدان شکافنده‌ی $\varphi(f)$ روی F' باشد، آن‌گاه φ را می توان به‌یکریختی $\overline{\varphi}: L \to L'$ توسیع داد.

اثبات: قضیه را با استقرا روی $n = [L:F]$ ثابت می‌کنیم. اگر $f(x)$ به طور کامل روی F تجزیه شود یا $[L:F] = 1$، آن‌گاه $L = F$ و $L' = F'$. بنابراین در این حالت $\overline{\varphi} = \varphi$. حال فرض کنیم f به طور کامل روی F تجزیه نشود. دراین‌صورت $f(x) = g(x)h(x)$، که در این‌جا $h(x) \in F[x]$ و $g(x) \in F[x]$ یک چندجمله‌ای تحویل‌ناپذیر از درجه‌ی $m \geq 2$ است. فرض کنیم u ریشه‌ای از g و u' ریشه‌ای از $\varphi(g)$ باشد. طبق قضیه ۴، $\varphi: F \to F'$ را می‌توان به یکریختی

$\varphi^* : F(u) \to F'(u')$ توسیع داد. چون $n = [L:F] = [L:F(u)][F(u):F]$، پس $n > [L:F(u)] = (n/m)$؛ از طرفی L میدان شکافنده‌ی $f(x)$ روی $F(u)$ و L' میدان شکافنده‌ی $\varphi(f)$ روی $F'(u')$ است، لذا طبق فرض استقرا φ^* و به دنبال آن φ را می‌توان به یکریختی $\overline{\varphi} : L \to L'$ توسیع داد؛ بنابراین φ را می‌توان به از $\overline{\varphi}$ توسیع داد.

■■■

نتیجه ۳-۱

بین هر دو میدان شکافنده از یک چندجمله‌ای $f(x) \in F[x]$ یک یکریختی موجود است به‌طوری‌که تحدیدش به F، تابع همانی روی F خواهد بود.

اثبات: کافی است در قضیه‌ی قبل قرار دهیم $F = F'$ و $\varphi = 1_F$.

■■■

در ادامه نشان خواهیم داد که هر میدان متناهی یک میدان شکافنده روی زیر میدان اولش است.

تعریف ۳-۳

فرض کنیم R یک حلقه و $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. مشتق $f(x)$ را به‌صورت زیر تعریف می‌کنیم:

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

لم ۳-۱

فرض کنیم F یک میدان $a \in F$ و $f(x) \in F[x]$. در این‌صورت گزاره‌های زیر معادلند.

(۱) چندجمله‌ای $g(x) \in F[x]$ موجود است به‌قسمی که $f(x) = (x-a)^2 g(x)$،

(۲) $f(a) = f'(a) = 0$.

اثبات: به‌عنوا ن‌تمرین به‌عهده‌ی خواننده واگذار می‌شود.

■■■

❖ **تذکر:** لم اخیر را می‌توان بدین‌صورت بیان نمود که:

$f(x)\in F[x]$ دارای ریشه‌ی مکرر است اگر و فقط اگر f و f' دارای ریشه‌ی مشترک باشند.

لم۳-۲ (رویای دانشجوی تازه وارد)

فرض کنیم p یک عدد اول، F میدانی از مشخصه‌ی p و $a,b\in F$. دراین‌صورت برای هر عدد طبیعی n داریم

$$(a+b)^{p^n}=a^{p^n}+b^{p^n} \text{ و } (a-b)^{p^n}=a^{p^n}-b^{p^n}$$

اثبات: به‌عنوا ن‌تمرین به‌عهده‌ی خواننده واگذار می‌شود.

■■■

قضیه۳-۶

فرض کنیم F یک میدان متناهی و L یک توسیع متناهی از F باشد. دراین‌صورت عدد طبیعی n موجود است به‌قسمی که $|L|=|F|^n$.

اثبات: فرض کنیم $[L:F]=n$ و $B=\{x_1,\cdots,x_n\}$ یک پایه برای فضای برداری L روی F باشد. تعریف می‌کنیم:

$$\varphi: F\times\ldots\times F\to L$$
$$(c_1,c_2,\ldots,c_n)\mapsto c_1x_1+\ldots+c_nx_n$$

به‌وضوح φ یک به یک و پوشاست و لذا $|L|=|F|^n$.

■■■

نتیجه۳-۲

اگر F یک میدان متناهی باشد، آن‌گاه مرتبه‌ی F توانی از یک عدد اول است.

اثبات: فرض کنیم P زیرمیدان اول F باشد. دراین‌صورت عدد اول p موجود است که $P\cong\mathbb{Z}_p$. بنابراین با توجه قضیه‌ی قبل عدد طبیعی n موجود است به‌طوری‌که $|F|=|P|^n$. درنتیجه $|F|=p^n$.

■■■

گزاره۳-۳

فرض کنیم که G یک گروه متناهی است اگر معادله‌ی $x^n = e$ برای هرعدد طبیعی n حداکثر n ریشه در Gداشته باشد، آن‌گاه G دوری خواهد بود.

اثبات: فرض کنیم $n = |G|$. کافی است ثابت کنیم که G دارای عنصری از مرتبه‌ی n است. اگر d مقسوم علیهی از n باشد، قرار می‌دهیم:

$$\lambda(d) = \text{تعداد عناصری از } G \text{ که مرتبه‌ی آن‌ها برابر } d \text{ است}$$

(توضیح این‌که ممکن است $\lambda(d) = 0$). فرض کنیم $a \in G$عنصری از مرتبه‌ی d باشد. دراین‌صورت هر یک از اعضای مجموعه‌ی

$$A = \{e, a, \ldots, a^{d-1}\}$$

در معادله‌ی $x^d = e$ صدق می‌کند. چون این معادله، بنابر فرض، حداکثر d جواب دارد. G غیر از عناصر مجموعه‌ی A که دو به دو متمایزند هیچ عنصر دیگری که در معادله‌ی $x^d = e$ صدق کند، ندارد. ازاین‌رو عناصری از G که مرتبه‌ی آن‌ها dاست فقط عناصر A هستند. چون تعداد این قبیل عناصر $\phi(d)$است، نتیجه می‌گیریم:

$$\lambda(d) = \begin{cases} \phi(d) & \text{هرگاه } G \text{ عنصری از مرتبه‌ی } d \text{ داشته باشد} \\ 0 & \text{در غیر این‌صورت} \end{cases}$$

حال اگر به ازای مقسوم علیهی از n مانند m داشته باشیم $\lambda(m) = 0$، آن‌گاه

$$n = \sum_{d|n} \lambda(d) < \sum_{d|n} \phi(d) = n,$$

که یک تناقض است. بنابراین به ازای هر مقسوم علیه n مانند d داریم، $\lambda(d) \neq 0$ و بدین ترتیب اثبات تمام است.

■■■

نتیجه۳-۳

فرض کنیم F یک میدان، $F^* = F - \{0\}$ گروه ضربی میدان F و اگر G یک زیرگروه متناهی F^* باشد، آن‌گاه G دوری است.

اثبات: معادله‌ی $x^n = 1$ برای هر عدد طبیعی n در میدان F و در نتیجه در G حداکثر n ریشه دارد. بنابراین طبق گزاره قبل G دوری است.

■■■

نتیجه۳-۴

فرض کنیم F یک میدان متناهی باشد. دراین‌صورت F^* یک گروه دوری است.

اثبات: در نتیجه‌ی قبل قرار دهید $G = F^*$.

■■■

❖ **تذکر :** عکس نتیجه‌ی اخیر نیز برقرار است (تمرین۹ ملاحظه شود).

اکنون نشان می‌دهیم که هر میدان متناهی یک توسیع ساده روی زیرمیدان اولش خواهد بود.

نتیجه۳-۵

فرض کنیم F یک میدان متناهی با زیر میدان اول $\mathbb{Z}_p$ باشد. دراین‌صورت عنصر $u \in F$ موجود است به‌طوری‌که $F = \mathbb{Z}_p(u)$.

اثبات: فرض کنیم u مولدی برای گروه دوری F^* باشد. دراین‌صورت برای هر عنصر ناصفر $v \in F$، عدد صحیح n موجود است به‌طوری‌که $v = u^n$؛ بنابراین $F = \mathbb{Z}_p(u)$.

■■■

حال نشان می‌دهیم که هر میدان متناهی یک میدان شکافنده روی زیر میدان اولش است.

قضیه۳-۷

فرض کنیم p یک عدد اول، F یک میدان و $n \in \mathbb{N}$. دراین‌صورت گزاره‌های زیر معادلند:

(۱) F میدانی با p^n عنصر است،

(۲) F میدان شکافنده‌ی چندجمله‌ای $f(x) = x^{p^n} - x$ روی $\mathbb{Z}_p$ است.

اثبات (۱) $\Rightarrow$(۲): فرض کنیم F دارای p^n عنصر باشد. چون $\left|F^*\right| = p^n - 1$، پس برای هر $u \in F^*$، $u^{p^n-1} = 1$. بنابراین هر عنصر F در چندجمله‌ای $f(x) = x^{p^n} - x$ صدق می‌کند. ازاین‌رو چون $\deg f = p^n$، پس f روی F شکافته می‌شود. درنتیجه F میدان شکافنده‌ی f روی $\mathbb{Z}_p$ است.

(۲) $\Rightarrow$(۱): فرض کنیم F میدان شکافنده‌ی چندجمله‌ای $f(x) = x^{p^n} - x$ روی $\mathbb{Z}_p$ باشد. قرار می‌دهیم:

$$E = \{u \in F \mid f(u) = 0\}.$$

با توجه به لم۲، E یک زیر میدان F است. از طرفی ریشه‌های f متمایزند زیرا اگر عنصر $u \in F$ یک ریشه‌ی چندگانه‌ی f باشد، آن‌گاه طبق لم۳، داریم $f'(u) = 0$ و در نتیجه $p^n u^{p^n-1} - 1 = 0$. چون F از مشخصه‌ی p است؛ ازاین‌رو $0 = -1$ ؛ که تناقض است. در نتیجه E دارای p^n عنصر است. حال چون F میدان شکافنده‌ی f روی $\mathbb{Z}_p$ است و E حاوی تمام ریشه‌های f است، $E = F$.

■■■

از قضیه‌ی قبل به‌وضوح داریم:

نتیجه۳-۶

(۱): فرض کنیم p یک عدد اول بوده و $n \in \mathbb{N}$. دراین‌صورت میدانی از مرتبه‌ی p^n موجود است،

(۲): هر دو میدان متناهی با تعداد عناصر یکسان، یکریخت‌اند.

تمرین‌های سطح۱

۱–فرض کنید K یک توسیع میدان F و $[K:F]=2$. نشان دهید K میدان شکافنده یک چند جمله‌ای $f(x)\in F[x]$ روی F است.

۲– فرض کنید $F\subseteq K\subseteq L$ و L میدان شکافنده‌ی f روی F باشد. ثابت کنید L میدان شکافنده‌ی f روی K نیز است.

۳– مطلوب است میدان شکافنده‌ی هر یک از چندجمله‌ای‌های f روی $\mathbb{Q}$.

(الف) $f(x)=(x^2-3)(x^2+1)$،

(ب) $f(x)=x^4+9$،

(پ) $f(x)=x^4+x^2+1$.

۴– فرض کنید F یک میدان و $f(x)\in F[x]$ یک چند جمله‌ای تحویل‌ناپذیر باشد. نشان دهید $f(x)$ دارای ریشه‌ی مکرر است اگر و تنها اگر $f'(x)=0$.

۵– فرض کنید F یک میدان و $f(x)\in F[x]$ یک چند جمله‌ای تحویل‌ناپذیر باشد. دراین‌صورت

(الف) اگر $\mathrm{Char}F=0$، نشان دهید $f(x)$ دارای ریشه‌ی مکرر نیست.

(ب) اگر $\mathrm{Char}F=p\neq 0$، نشان دهید $f(x)$ دارای ریشه‌ی مکرر است اگر و تنها اگر چند جمله‌ای $g(x)\in F[x]$ موجود باشد به‌قسمی که $f(x)=g(x^p)$.

تمرین‌های سطح۲

۶-فرض کنید F یک میدان و $f(x) \in F[x]$ یک چندجمله‌ای از درجه‌ی n باشد. اگر K میدان شکافنده‌ی f روی F باشد، ثابت کنید $n \mid [K : F]$.

۷- ثابت کنید اگر F یک میدان متناهی از مشخصه‌ی p باشد، آن‌گاه برای هر عنصر $a \in F$، عنصر یکتای $b \in F$ موجود است به‌طوری‌که $a = b^p$.

۸- میدانی با ۹ عنصر ساخته و جداول جمع و ضرب آن‌را بنویسید.

۹- فرض کنید F میدانی باشد که گروه ضربی آن، F^*، دوری است. ثابت کنید F متناهی است.

۱۰- فرض کنید F یک میدان و $f(x) \in F[x]$ یک چند جمله‌ای تحویل‌ناپذیر باشد. نشان دهید

$$f(x) = a[(x - u_1)(x - u_2)\cdots(x - u_n)]^m,$$

که $m \in \mathbb{N}$ و $a \in F$ و u_i ها ریشه‌های $f(x)$ در میدان شکافنده‌اش هستند.

۱۱- فرض کنید F یک میدان و $X \subseteq F[x]$ یک زیر مجموعه‌ی ناتهی باشد. کوچک‌ترین میدانی را که شامل F است و هر چندجمله‌ای از X روی آن شکافته شود، **میدان شکافنده‌ی** X روی F نامیم.

(الف) فرض کنید F یک میدان و $X = \{f_1, \ldots, f_n\}$ یک زیر مجموعه‌ی متناهی از $F[x]$ باشد. نشان دهید میدان شکافنده‌ی X روی F با میدان شکافنده‌ی چندجمله‌ای $f = f_1 \ldots f_n$ روی F یکی است.

(ب) اگر K یک توسیع میدان F باشد، نشان دهید شرایط زیر معادلند:

(۱) K یک بستار جبری F است،

(۲) K میدان شکافنده‌ی تمام چندجمله‌ای‌های $F[x]$ روی F است.

در تمرین بعدی توسیع‌های جدایی‌پذیر مورد بررسی قرار می‌گیرند.

۱۲–فرض کنید F یک میدان باشد. اگر $f(x) \in F[x]$ یک چند جمله‌ای تحویل ناپذیر باشد، آن‌گاه $f(x)$ را روی F **جدایی پذیر** نامیم، اگر $f(x)$ در میدان شکافنده‌اش دارای ریشه‌ی تکراری نباشد. فرض کنید K یک توسیع F باشد. اگر $u \in K$ روی F جبری باشد، آن‌گاه u را یک عنصر جدایی پذیر روی F نامیم، اگر چند جمله‌ای مینیمال u روی F جدایی پذیر باشد. توسیع K از F را یک **توسیع جدایی پذیر** گوییم، اگر هر $u \in K$ روی F جدایی پذیر باشد.

(الف) فرض کنید F یک میدان و $f(x) \in F[x]$ تحویل ناپذیر باشد. دراین‌صورت $f(x)$ روی F جدایی پذیر است اگر و فقط اگر $f'(x) \neq 0$.

(ب) فرض کنید K یک توسیع F و $u \in K$. نشان دهید u روی F جدایی پذیر است اگر و فقط اگر u یک ریشه‌ی غیر تکراری چند جمله‌ای مینیمال u روی F باشد.

(پ) فرض کنید K یک توسیع جدایی پذیر میدان F باشد. نشان دهید K یک توسیع جدایی پذیر از هر میدان میانی توسیع K روی F نیز هست.

۱۳–فرض کنیم F یک میدان باشد. دراین‌صورت F را یک میدان **کامل** نامیم اگر هر توسیع متناهی از F جدایی پذیر باشد.

۱۴–فرض کنید F یک میدان با مشخصه‌ی عدد اول p و $0 \neq a \in F$. دراین‌صورت یا $x^p - a$ روی F تحویل ناپذیر است و یا عنصر $b \in F$ موجود است به‌قسمی که $x^p - a = (x - b)^p$.

۱۵–فرض کنید F یک میدان با مشخصه‌ی غیر صفر p باشد. نشان دهید F یک میدان کامل است اگر و فقط اگر $F = \{a^p \mid a \in F\}$.

تمرین‌های سطح ۳

۱۶– هر عنصر یک میدان متناهی را می‌توان به‌صورت مجموع دو مربع نوشت.

۳-۲ تناظر گالوا

تعریف۳-۴

فرض کنیم K یک میدان باشد. قرار می‌دهیم:

$$\mathrm{Aut}K = \{f : K \to K \mid f \text{ یک خودریختی باشد}\}.$$

حال فرض کنیم K یک توسیع میدان F باشد. قرار می‌دهیم:

$$\mathrm{Aut}_F K = \{f \in \mathrm{Aut}K \mid f(x) = x,\ \forall x \in F\}$$

گزاره۳-۳

فرض کنیم K یک توسیع میدان F باشد. دراین‌صورت

(۱) $\mathrm{Aut}K$ با عمل ترکیب توابع یک گروه است،

(۲) $\mathrm{Aut}_F K$ یک زیرگروه از گروه $\mathrm{Aut}K$ است.

اثبات: به‌عنوان تمرین به‌عهده‌ی خواننده واگذار می‌شود.

■■■

تعریف۳-۵

$\mathrm{Aut}_F K$ را **گروه گالوایی**[1] **(توسیع)** K روی F می نامیم. اگر K میدان شکافنده‌ی چند جمله‌ای $f(x) \in F[x]$ باشد، آن‌گاه $\mathrm{Aut}_F K$ را **گروه گالوایی (چندجمله‌ای)** $f(x)$ روی F نامیده و با نماد G_f نمایش می‌دهیم.

❖ **تذکر:** گروه گالوایی $\mathrm{Aut}_F K$ را با نمادهای $\mathrm{Gal}_F K$ و $G(K,F)$ نیز نمایش می دهند.

نمادگذاری: فرض کنیم $F \subseteq E \subseteq K$ میدان باشند و $H \leq \mathrm{Aut}_F K$. دراین‌صورت

$$H' = \{x \in K \mid f(x) = x,\ \forall f \in H\},$$
$$E' = \{f \in \mathrm{Aut}_F K \mid f(x) = x,\ \forall x \in E\}.$$

---

[1] Galois Group

گزاره۳-۴

فرض کنیم $F \subseteq E \subseteq K$ میدان باشند و $H \leq \mathrm{Aut}_F K$. دراین‌صورت

(۱): $F \subseteq H' \subseteq K$،

(۲): $E' \leq \mathrm{Aut}_F K$.

اثبات: به‌عنوا ن‌تمرین به عهده‌ی خواننده واگذار می‌شود.

■■■

لم۳-۳

فرض کنیم $F \subseteq L \subseteq M \subseteq K$ میدان باشند و $H \leq J \leq \mathrm{Aut}_F K$. دراین‌صورت

(۱): $K' = \{1_K\}$ و $F' = \mathrm{Aut}_F K$،

(۲): $\{1_K\}' = K$،

(۳): $M' \leq L'$،

(۴): $J' \subseteq H'$،

(۶): $L \subseteq L''$ و $H \subseteq H''$،

(۷): $L' = L'''$ و $H' = H'''$.

اثبات: به‌عنوا ن‌تمرین به عهده‌ی خواننده واگذار می‌شود.

■■■

تعریف۳-۶

فرض کنیم $F \subseteq X \subseteq K$ یا $X \leq \mathrm{Aut}_F K$. دراین‌صورت X را **بسته** گوییم اگر $X'' = X$.

مثال۲: $\{1_K\}$طبق لم اخیر بسته است.

□

تعریف۳-۷

توسیع K از F را یک **توسیع نرمال (یا توسیع گالوا**[1]) از F گوییم، اگر F بسته باشد. به‌عبارت دیگر $(\mathrm{Aut}_F K)' = F$.

❖ **تذکر:** K یک توسیع گالوا از F است اگر و فقط اگر برای هر $u \in K - F$ عنصر $\sigma \in \mathrm{Aut}_F K$ موجود باشد به‌طوری‌که $\sigma(u) \neq u$.

مثال۳: فرض کنیم $K = \mathbb{C}$ و $F = \mathbb{R}$. اگر $f \in \mathrm{Aut}_{\mathbb{R}}\mathbb{C}$، آن‌گاه

$$f(a+bi) = f(a) + f(b)f(i) = a + bf(i).$$

از طرفی چون i ریشه‌ی چندجمله‌ای $g(x) = x^2 + 1$ است، پس $f(i)$ نیز ریشه‌ی $g(x)$ بوده و لذا $f(i) \in \{i, -i\}$. اگر $f(i) = i$، آن‌گاه $f = 1_{\mathbb{C}}$ و اگر $f(i) = -i$، آن‌گاه $f(a+bi) = a - bi$. بنابراین $\mathrm{Aut}_F K = \{1_K, \sigma\}$، که σ تزویج مختلط $(a+bi \mapsto a-bi)$ است. حال داریم

$$(\mathrm{Aut}_F K)' = \{a + bi \in \mathbb{C} \mid \sigma(a+bi) = a+bi\} = \{a \mid a \in \mathbb{R}\} = \mathbb{R} = F$$

یعنی $\mathbb{C}$ یک توسیع نرمال از $\mathbb{R}$ است.

□

مثال۴: فرض کنیم $K = \mathbb{Q}(\sqrt[3]{2})$ و $F = \mathbb{Q}$. اگر $f \in \mathrm{Aut}_F K$، آن‌گاه

$$f(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2^2}) = a_0 + a_1 f(\sqrt[3]{2}) + a_2 (f(\sqrt[3]{2}))^2$$

از طرفی $\sqrt[3]{2}$ چون ریشه‌ی چندجمله‌ای $g(x) = x^3 - 2$ است، پس $f(\sqrt[3]{2})$ نیز ریشه‌ی $g(x)$ بوده و لذا $f(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \alpha_1, \alpha_2\}$، که در این‌جا اعداد α_1, α_2 غیر حقیقی هستند. بنابراین $f(\sqrt[3]{2}) = \sqrt[3]{2}$ و در نتیجه $f = 1_K$. ازاین‌رو $\mathrm{Aut}_F K = \{1_K\}$ و درنتیجه $(\mathrm{Aut}_F K)' = \{1_K\}' = K$؛ یعنی K یک توسیع نرمال از F نیست.

□

[1] Galois Extension

تعریف۳-۸

فرض کنیم $F \subseteq E \subseteq K$ میدان باشند. گوییم E (نسبت به F و K) **پایا**ست اگر برای هر $\sigma \in \mathrm{Aut}_F K$ داشته باشیم $\sigma(E) \subseteq E$.

لم۳-۴

فرض کنیم K یک توسیع میدان F باشد.
(۱) اگر E (نسبت به F و K) پایا باشد، آن‌گاه $\mathrm{Aut}_E K \trianglelefteq \mathrm{Aut}_F K$،
(۲) اگر $H \trianglelefteq \mathrm{Aut}_F K$، آن‌گاه H' (نسبت به F و K) پایاست.

اثبات(۱): فرض کنیم $\sigma \in \mathrm{Aut}_F K$ و $\tau \in \mathrm{Aut}_E K$ نشان می‌دهیم $\sigma^{-1}\tau\sigma \in \mathrm{Aut}_E K$. اگر $u \in E$ آن‌گاه چون E پایاست $\sigma(u) \in E$ و لذا $\tau\sigma(u) = \sigma(u)$. پس $\sigma^{-1}\tau\sigma(u) = \sigma^{-1}\sigma(u) = u$ و درنتیجه $\sigma^{-1}\tau\sigma \in \mathrm{Aut}_E K$.

(۲): فرض کنیم $\sigma \in \mathrm{Aut}_F K$ و $u \in H'$. با توجه به نرمال بودن H، برای هر $\tau \in H$ داریم $\sigma^{-1}\tau\sigma \in H$. بنابراین $\sigma^{-1}\tau\sigma(u) = u$ و در نتیجه برای هر $\tau \in H$، $\tau\sigma(u) = \sigma(u)$. ازاین‌رو $\sigma(u) \in H'$ و در نتیجه H' (نسبت به F و K) پایاست.

■■■

لم۳-۵

فرض کنیم $F \subseteq E \subseteq K$ میدان باشند. اگر K یک توسیع نرمال از F و E پایا باشد، آن‌گاه E نیز یک توسیع نرمال از F است.

اثبات: فرض کنیم $u \in E - F$. دراین‌صورت $\sigma \in \mathrm{Aut}_F K$ موجود است به‌طوری‌که $\sigma(u) \neq u$. اما اگر $\tau = \sigma|_E$، آن‌گاه $\tau \in \mathrm{Aut}_F E$ و $\tau(u) \neq u$. بنابراین طبق تذکر اخیر E یک توسیع نرمال از F است.

■■■

لم۳-۶

فرض کنیم $F \subseteq E \subseteq K$. اگر E یک توسیع جبری نرمال از F باشد، آن‌گاه E (نسبت به F و K) پایاست.

اثبات: فرض کنیم $u \in E$ و $\sigma \in \mathrm{Aut}_F K$. باید نشان دهیم $\sigma(u) \in E$. فرض کنیم f چند جمله‌ای مینیمال $u \in E$ روی F باشد. اگر $u = u_1,\ldots,u_m$ همه‌ی ریشه‌های f در E باشند، قرار می‌دهیم:

$$g(x) = (x - u_1)\ldots(x - u_m)$$

فرض کنیم $\tau \in \mathrm{Aut}_F E$. چون τ هرریشه‌ی g را به یک ریشه‌ی g می‌برد، پس

$$\{\tau(u_1),\ldots,\tau(u_m)\} = \{u_1,\ldots,u_m\}$$

و لذا برای هر $\tau \in \mathrm{Aut}_F E$، $\tau g = g$. اگر $g(x) = a_0 + a_1 x + \ldots + a_m x^m$، آن‌گاه برای هر $\tau \in \mathrm{Aut}_F E$ داریم:

$$g(x) = a_0 + a_1 x + \cdots + a_m x^m = \tau(g) = \tau(a_0) + \tau(a_1)x + \cdots + \tau(a_m)x^m.$$

چون E یک توسیع نرمال روی F است، لذا ضرایب g در F هستند. از طرفی چون $g(u) = 0$، مینیمال بودن f ایجاب می‌کند که $f = g$. با توجه به این‌که $\sigma(u)$ یک ریشه از f است و $f = g$، پس $\sigma(u)$ یک ریشه از g نیز خواهد بود و در نتیجه $\sigma(u) \in E$.

■■■

لم ۳-۷

فرض کنیم $F \subseteq L \subseteq M \subseteq K$. اگر $[M : L] < \infty$، آن‌گاه $[L' : M'] \leq [M : L]$. به‌ویژه، اگر $[K : F] < \infty$ آن‌گاه $|\mathrm{Aut}_F K| \leq [K : F]$.

اثبات: به استقرا روی $n = [M : L]$ عمل می کنیم. اگر $n = 1$ آن‌گاه $M = L$ و در نتیجه $L' = M'$؛ پس حکم برقرار است. در حالت $[M : L] \neq 1$، فرض کنیم $u \in M - L$، $[L(u) : L] = m$ و $f(x) \in L[x]$ چندجمله‌ای مینیمال $u \in M$ روی L باشد.

حالت ۱: $m < n$.

طبق فرض استقرا

$$[L' : L(u)'] \leq [L(u) : L] \qquad (*)$$

$$[L(u)' : M'] \leq [M : L(u)] \qquad (**)$$

طبق (*)و (**) داریم:

$$[L':M']=[L':L(u)'][L(u)':M']\le[L(u):L][M:L(u)]=[M:L]$$

حالت ۲: $m=n$.

تعریف می‌کنیم:

$$\theta: S=\{\delta M' \mid \delta\in L'\}\to T=\{\alpha \mid f(\alpha)=0\}$$
$$\theta(\delta M')\mapsto \delta(u)$$

که u عضو میدان شکافنده است.

نشان می‌دهیم θ خوش تعریف و یک به یک است:

$$\delta M'=\tau M' \Leftrightarrow \tau^{-1}\delta\in M' \Leftrightarrow \tau^{-1}\delta(u)=u \Leftrightarrow \delta(u)=\tau(u)$$

بنابراین $|S|\le \deg f=n$ و لذا $[L':M']\le[M:L]$. قسمت دوم حکم با قرار دادن $L=F$ و $M=K$ به‌دست می‌آید.

■■■

لم۳-۸

فرض کنیم K یک توسیع میدان F و $H\le J\le \mathrm{Aut}_F K$. اگر $[J:H]<\infty$، آن‌گاه $[H':J']\le[J:H]$.

اثبات: فرض کنیم $[J:H]=n$ و $[H':J']>n$. دراین‌صورت هم‌دسته‌های متمایز چپ $\tau_1H,...,\tau_nH$ موجودند به‌طوری‌که $J=\tau_1H\cup...\cup\tau_nH$. چون $[H':J']\ge n+1$ لذا مجموعه‌ی $B=\{u_1,u_2,\dots,u_{n+1}\}$ که $B\subseteq H'$ موجود است به‌طوری‌که B روی J' مستقل خطی است. اکنون دستگاه n معادله و $n+1$ مجهول همگن زیر را در نظر می‌گیریم.

$$\begin{cases}\tau_1(u_1)x_1+\tau_1(u_2)x_2+\cdots+\tau_1(u_{n+1})x_{n+1}=0\\ \tau_2(u_1)x_1+\tau_2(u_2)x_2+\cdots+\tau_2(u_{n+1})x_{n+1}=0\\ \vdots\\ \tau_n(u_1)x_1+\tau_n(u_2)x_2+\cdots+\tau_n(u_{n+1})x_{n+1}=0\end{cases}$$

چون تعداد مجهولات بیشتر از تعداد معادلات است، دستگاه اخیر دارای یک جواب غیر بدیهی مانند، $(a_1,...,a_{n+1})\in K^{n+1}$است. بین تمام جواب های غیر بدیهی جوابی را

انتخاب می‌کنیم که تعداد عناصر غیر صفر آن کم‌ترین باشد. اگر r تعداد این عناصر غیر صفر باشد، با یک تجدید اندیس می‌توان فرض کرد که جواب مورد نظر به‌صورت زیر است:

$$X = (a_1,...,a_r,0,0,...,0) \qquad (a_i \neq 0;\ i = 1,2,\ldots,r)$$

دوباره می‌توان فرض کرد که $a_1 = 1$. حال باید با توجه به مستقل خطی بودن $B = \{u_1,u_2,...,u_{n+1}\}$ روی J' به تناقض با نحوه‌ی انتخاب r برسیم.

ادعا: $\delta \in J$ موجود است به‌قسمی که $\delta(a_k) \neq a_k$ برای یک $1 \leq k \leq r$ و

$$\delta_X := (\delta(a_1),\delta(a_2),...,\delta(a_r),0,0,...,0)$$

یک جواب دستگاه است.

با توجه به ادعای اخیر $X - \delta_X$ نیز یک جواب دستگاه است و داریم:

$$\begin{aligned} X - \delta_X &= (a_1 - \delta(a_1), a_2 - \delta(a_2),...,a_k - \delta(a_k),...,a_r - \delta(a_r),...) \\ &= (0, a_2 - \delta(a_2),...,a_k - \delta(a_k),...,a_r - \delta(a_r),0,0,...,0), \end{aligned}$$

که با انتخاب r در تناقض است. بنابراین $n \leq [H' : J']$. در نهایت به اثبات ادعا می‌پردازیم.

اثبات ادعا: $1 \leq i \leq n$ موجود است به‌طوری‌که $e \in \tau_i H$ و لذا $\tau_i \in H$. بنابراین $\tau_i(u_j) = u_j$ برای هر $j = 1,...,n+1$ و در نتیجه

$$\sum_{j=1}^{n+1} u_j a_j = \sum_{j=1}^{n+1} \tau_i(u_j) a_j = 0,$$

جایی‌که a_j همان مولفه‌های X هستند. چون a_j ناصفر و u_j ها روی J' مستقل هستند، پس $1 \leq k \leq n$، موجود است به‌طوری‌که $a_k \notin J'$. پس طبق تعریف $\delta \in J$ موجود است که $\delta(a_k) \neq a_k$. فرض کنیم $1 \leq t \leq n$ عدد دلخواهی باشد. چون $J = (\delta\tau_1)H \cup ... \cup (\delta\tau_n)H$، پس $1 \leq i \leq n$، موجود است به‌طوری‌که $\tau_t H = \delta\tau_i H$. از طرفی چون $u_j \in H'$، پس $\tau_t(u_j) = \delta\tau_i(u_j)$ و در نتیجه

$$\sum_{j=1}^{n+1} \tau_t(u_j)\delta(a_j) = \sum_{j=1}^{n+1} \delta\tau_i(u_j)\delta(a_j) = \delta\left(\sum_{j=1}^{n+1} \tau_i(u_j)a_j\right) = \delta(0) = 0,$$

یعنی δ_X یک جواب دستگاه است.

■■■

نتیجه۳-۷

(۱): فـرض کنـیم $F \subseteq L \subseteq M \subseteq K$ و L در K بسـته باشـد و $[M:L] < \infty$.
دراین‌صورت M نیز در K بسته است و $[M:L] = [L':M']$.
(۲): فرض کنـیم $H \leq J \leq G = \mathrm{Aut}_F K$ و H در G بسـته باشـد و $[J:H] < \infty$.
دراین‌صورت J نیز در G بسته است و $[J:H] = [H':J']$.

اثبات(۱): داریم

$$[M:L] = [M:L''] \leq [M'':L''] \leq [L':M'] \leq [M:L].$$

بنابراین $[M:L] = [L':M']$. از طرفی $[M:L] = [M'':L]$و در نتیجه $M = M''$.
(۲): اثبات مشابه (۱) است.

■■■

قضیه۳-۸ (قضیه‌ی اساسی نظریه گالوا)

فرض کنیم K یک توسیع متناهی و نرمال از F باشد. دراین‌صورت:
(۱): تمام میدان های میانی توسـیع K روی Fو تمـامی زیـر گـروه هـای $\mathrm{Aut}_F K$ بسته هستند و تابع

$$\theta : \mathbb{A} \to \mathbb{B}$$
$$\theta(E) = E' = \mathrm{Aut}_E K$$

که در آن

$$\mathbb{A} = \{F \text{ روی } K \text{ تمام میدان های میانی توسیع}\},$$
$$\mathbb{B} = \{\mathrm{Aut}_F K \text{ تمام زیر گروه‌های}\}.$$

یک دو سویی است.
(۲): اگر $F \subseteq L \subseteq M \subseteq K$، آن‌گاه $[M:L] = [L':M']$.
به‌ویژه $\left|\mathrm{Aut}_F K\right| = [K:F]$.

(۳): فرض کنیم E یک میدان میانی توسیع K روی F است. دراین‌صورت:

(الف): K روی E نرمال است.

(ب): E روی F نرمال است اگر و تنها اگر $\mathrm{Aut}_E K \trianglelefteq \mathrm{Aut}_F K$.

(ج): اگر E روی F نرمال باشد آن‌گاه $\mathrm{Aut}_F E \cong \dfrac{\mathrm{Aut}_F K}{\mathrm{Aut}_E K}$.

اثبات(۱): چون $[K:F] < \infty$ و F بسته است، لذا طبق نتیجه‌ی ۷(۱)،تمام میدان‌های میانی توسیع K روی F بسته‌اند و هم‌چنین

$$[K:F] = [F':K'] = |F'| = |\mathrm{Aut}_F K|.$$

حال چون $|\mathrm{Aut}_F K| < \infty$ و $\{1_K\}$ یک زیر گروه بسته است، لذا با توجه به نتیجه‌ی ۷ (۲) همه‌ی زیرگروه‌های $\mathrm{Aut}_F K$ بسته‌اند. فرض کنیم $\theta(E_1) = \theta(E_2)$. دراین‌صورت $E_1' = E_2'$ و لذا $E_1'' = E_2''$. بنابراین $E_1 = E_2$. در نتیجه θ یک به یک است. حال فرض کنیم $H \le \mathrm{Aut}_F K$. دراین‌صورت $\theta(H') = H'' = H$ و لذا θ پوشاست.

(۲) و (۳) (الف): به آسانی از نتیجه‌ی ۷(۱) به‌دست می‌آیند.

(۳) (ب): ($\Leftarrow$): فرض کنیم E روی F نرمال باشد. چون K یک توسیع متناهی روی F است، لذا E یک توسیع متناهی روی F بوده و در نتیجه E روی F جبری است. از این‌رو بنابر لم۶، E پایا بوده و بنابراین طبق لم ۴، $\mathrm{Aut}_E K \trianglelefteq \mathrm{Aut}_F K$.

($\Rightarrow$): فرض کنیم $\mathrm{Aut}_E K \trianglelefteq \mathrm{Aut}_F K$. دراین‌صورت E پایا بوده و لذا E روی F نرمال است.

(۳) (ج): تعریف می‌کنیم:

$$\varphi : \mathrm{Aut}_F K \to \mathrm{Aut}_F E$$
$$f \mapsto f|_E$$

چون $\mathrm{Ker}\varphi = \{f \in \mathrm{Aut}_F K : f|_E = 1_E\} = \mathrm{Aut}_E K$، پس طبق قضیه‌ی اول یکریختی داریم $\mathrm{Im}\,\varphi \cong \dfrac{\mathrm{Aut}_F K}{\mathrm{Aut}_E K}$. از طرفی طبق قضیه برج،

$$\left|\frac{\mathrm{Aut}_F K}{\mathrm{Aut}_E K}\right| = \frac{[K:E][E:F]}{[K:E]} = [E:F].$$

بنابراین φ پوشاست و لذا $\frac{\mathrm{Aut}_F K}{\mathrm{Aut}_E K} \cong \mathrm{Aut}_F E$.

■■■

❖ **تذکر:** برخی از قسمت‌های قضیه‌ی اساسی گالوا را می‌توان برای توسیع‌های جبری تعمیم داد (تمرین ۱۴ ملاحظه شود).

در نهایت به‌عنوان کاربردی از قضیه‌ی اساسی گالوا، نتیجه‌ی۲-۵ را تعمیم می‌دهیم:

قضیه۳-۹

فرض کنیم $F \leq K \leq \mathbb{R}$، $F \leq \mathcal{C}$، K یک توسیع نرمال از F باشد و $[K : F] = 2^n$ که $n \in \mathbb{N}$. دراین‌صورت $K \leq \mathcal{C}$.

اثبات: حکم را با استقرا روی n ثابت می‌کنیم. با توجه به نتیجه‌ی ۲-۵، حکم برای $n = 1$ برقرار است. حال فرض کنید $n \geq 2$ و حکم برای تمامی $m \in \mathbb{N}$ که $m < n$ برقرار باشد. چون K یک توسیع نرمال از F است، با فرض $G = \mathrm{Aut}_F K$، خواهیم داشت:

$$|G| = [K : F] = 2^n.$$

طبق قضیه‌ی اول سیلو (به بخش ۱ از فصل ۶ مراجعه شود)، G دارای زیرگروهی مانند H از مرتبه‌ی 2^{n-1} است. پس

$$[H' : F] = [G : H] = 2.$$

بنابراین طبق نتیجه‌ی۲-۵، $H' \leq \mathcal{C}$. حال چون K یک توسیع نرمال از F است و $F \leq H' \leq K$، پس K یک توسیع نرمال از H' نیز هست. از طرفی $[K : H'] = 2^{n-1}$ و $H' \leq \mathcal{C}$، لذا طبق فرض استقرا $K \leq \mathcal{C}$ و اثبات تمام است.

■■■

هر چه بیشتر تمرین یا اثبات کنیم، تمرین یا اثبات کردن برایمان ساده‌تر می‌شود.

(سیلوستر)

تمرین‌های سطح۱

۱-گروه گالوایی چند جمله‌ای‌های زیر را روی میدان‌های داده شده مشخص کنید.

(الف) x^4-3 روی $\mathbb{Q}$،

(ب) x^4-3 روی $\mathbb{Q}\sqrt{3}$،

(پ) x^3-2 روی $\mathbb{Q}$.

۲-تمام زیرگروه‌های گروه گالوایی و تمام میدان‌های میانی میدان شکافنده‌ی چندجمله‌ای $f(x)=(x^2-2)(x^2-3)$ روی $\mathbb{Q}$ را تعیین کنید.

تمرین‌های سطح۲

۳- فرض کنید F میدانی از مشخصه‌ی صفر و p عدد اولی باشد که برای هر توسیع سره K از F، $p\mid[K:F]$. نشان دهید، اگر K یک توسیع متناهی از F باشد، آن‌گاه عدد طبیعی n موجود است به‌قسمی که $[K:F]=p^n$.

۴-فرض کنید F زیرمیدانی از اعداد حقیقی باشد و $f(x)\in F[x]$ یک چند جمله‌ای تحویل‌ناپذیر درجه‌ی ۴باشد. نشان دهید اگر f دقیقاً دو ریشه‌ی حقیقی داشته باشد، آن‌گاه گروه گالوایی f یکریخت S_4 یا D_4 است.

۵–نشان دهید گروه گالوایی $f(x)=x^5-x-1\in\mathbb{Q}[x]$ با S_5 یکریخت است.

۶– اگر F یک میدان و $n\geq 1$ عددی صحیح باشد، نشان دهید یک ریشه‌ی n ام اولیه‌ی واحد w روی F وجود دارد اگر و تنها اگر $|F|$ عدد n را عاد نکند. هم‌چنین دراین‌صورت نشان دهید:

(الف) $F(w)$ میدان شکافنده‌ی x^n-1 روی F است،

(ب) $F(w)$ یک توسیع گالوای متناهی است و $\mathrm{Aut}_F F(w)$ با زیر گروهی از $\mathbb{Z}_n^*$ یکریخت است.

۷– عنصر $f(y_1,\ldots,y_n)$ از میدان $K=F(y_1,\ldots,y_n)$ را یک **تابع متقارن** نسبت به $y_1,\ldots,y_n$ روی F نامیم اگر برای هر $\sigma\in S_n$ داشته باشیم

$$f(y_1,\ldots,y_n)=f(y_{\sigma(1)},\ldots,y_{\sigma(n)}).$$

توابع متقارن مقدماتی نسبت به $y_1,\ldots,y_n$ روی F عبارتند از:

$$\begin{aligned}
s_1 &= y_1+y_2+\cdots+y_n,\\
s_2 &= y_1y_2+y_1y_3+\cdots+y_{n-1}y_n,\\
&\vdots\\
s_n &= y_1y_2\ldots y_n.
\end{aligned}$$

فرض کنید S مجموعه تمامی توابع متقارن نسبت به $y_1,\ldots,y_n$ روی F باشد. نشان دهید:

(۱) S زیر میدانی از K شامل F است،

(۲) $[K:S]=n!$،

(۳) K یک توسیع گالوا روی S است و $\mathrm{Aut}_S K\cong S_n$،

(۴) $S=F(s_1,\ldots,s_n)$،

(۵) K میدان شکافنده‌ی چندجمله‌ای

$$f(x)=\prod_{i=1}^{n}(x-y_i)=x^n-s_1x^{n-1}+s_2x^{n-2}-\cdots+(-1)^n s_n$$

روی S است.

۸- فرض کنید F یک میدان و $\sigma_1, \sigma_2, \dots, \sigma_n$ عناصر متمایزی از $\mathrm{Aut}F$ باشند. نشان دهید σ_iها روی F مستقل‌اند. به‌عبارت دیگر، اگر عناصر $c_1, c_2, \dots, c_n$ موجود باشند به‌طوری‌که برای هر $x \in F$ داشته باشیم $c_1\sigma_1(x) + c_2\sigma_2(x) + \cdots + c_n\sigma_n(x) = 0$، آن‌گاه نشان دهید $c_1 = c_2 = \cdots = c_n = 0$.

۹- فرض کنیم K یک توسیع متناهی و نرمال از میدان F و

$$\mathrm{Aut}_F K = \{\sigma_1, \sigma_2, \dots, \sigma_n\}.$$

نرم و اثر(رد) عنصر $a \in K$ به‌ترتیب عبارتند از:

$$N(a) = \sigma_1(a)\sigma_2(a)\cdots\sigma_n(a),$$
$$T(a) = \sigma_1(a) + \sigma_2(a) + \cdots + \sigma_n(a).$$

با فرض $u, v \in K$ نشان دهید:

(۱) $N(uv) = N(u)N(v)$ و $T(u+v) = T(u) + T(v)$،

(۲) $N(u) = ((-1)^n a_0)^{[K:F(u)]}$ و $T(u) = -[K : F(u)]a_{n-1}$،

که در آن $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ چندجمله‌ای مینیمال عنصر u روی میدان F است.

تمرین‌های سطح ۳

۱۰- اگر K یک توسیع میدان F باشد، نشان دهید شرایط زیر معادلند:

(۱) K روی F جبری و نرمال است،

(۲) K روی F جدایی‌پذیر و K میدان شکافنده‌ی زیر مجموعه‌ی مانند $X \subseteq F[x]$ روی F است،

(۳) K میدان شکافنده‌ی تمام چندجمله‌ای‌های جدایی‌پذیر از $F[x]$ روی F است.

۱۱- فرض کنید F یک میدان باشد. نشان دهید $\mathrm{Aut}_F F(x)$ دقیقاً از عناصری تشکیل شده که به‌وسیله‌ی

$$\sigma : F(x) \to F(x)$$
$$x \mapsto \frac{a+bx}{cx+d}$$

که در آن $a,b,c,d \in F$ و $ad-bc \neq 0$ القا می‌شود.

۱۲- (الف) اگر F یک میدان نامتناهی باشد، نشان دهید $F(x)$ روی F نرمال است.

(ب) اگر F یک میدان متناهی باشد، نشان دهید $F(x)$ روی F نرمال نیست.

۱۳- نشان دهید هر گروه متناهی با گروه گالوایی یک توسیع گالوای متناهی‌کریخت است.

۱۴- (تعمیم قضیه‌ی اساسی نظریه گالوا) فرض کنید K یک توسیع جبری و نرمال از F باشد. نشان دهید:

(۱): تابع

$$\theta : \mathbb{A} \to \mathbb{B}$$
$$\theta(E) = E' = \mathrm{Aut}_E K$$

که‌درآن

$$\mathbb{A} = \{F \text{ روی } K \text{ تمام میدان های میانی توسیع}\},$$
$$\mathbb{B} = \{\mathrm{Aut}_F K \text{ تمام زیر گروه‌های}\}.$$

یک دو سویی است.

(۲): فرض کنید E یک میدان میانی توسیع K روی F است. نشان دهید:

(الف): K روی E نرمال است.

(ب): E روی F نرمال است اگر و تنها اگر $\mathrm{Aut}_E K \trianglelefteq \mathrm{Aut}_F K$.

(ج): اگر E روی F نرمال باشد آن‌گاه $\dfrac{\mathrm{Aut}_F K}{\mathrm{Aut}_E K} \cong \mathrm{Aut}_F E$.

۱۵- فرض کنید K یک توسیع متناهی و نرمال از میدان F و $\mathrm{Aut}_F K$ یک گروه دوری با مولد σ باشد. اگر $a \in K$، نشان دهید:

(۱) $T(a) = 0$ اگر و فقط اگر به ازای عنصری مانند $b \in K$ داشته باشیم $a = b - \sigma(b)$،

(۲) **(قضیه‌ی ۹۰ هیلبرت**[1]**)** $N(a) = 1_F$ اگر و فقط اگر به ازای عنصری مانند $b \in K$ داشته باشیم $a = \dfrac{b}{\sigma(b)}$.

منابعی برای مطالعه‌ی بیشتر

۱. طائری، بیژن. **مبانی جبرمجرد**. انتشارات دانشگاه صنعتی اصفهان (۱۳۸۲).

۲. محمدی حسن آبادی، علی اکبر. **جبر**. انتشارات دانشگاه اصفهان (۱۳۷۲).

3. Garling, J. H. *A Course in Galois Theory*. Cambridge University Press, 1986.

4. Howie, J. M. *Fields and Galoies Theory*. Springer-Verlag, London, 2006.

5. Roman, S. *Field Theory*. Springer-Verlag, New York, 1995.

[1] Hilbert's Theorem 90

فصل ۴

حل‌پذیری با رادیکال‌ها

مشکل ما در برهان‌ها نیست، بلکه در این است که چه می‌خواهیم ثابت کنیم.

(امیل آرتین)

در این فصل می‌خوانیم:

۴-۱ گروه‌های حل‌پذیر

۴-۲ حل‌پذیری با رادیکال‌ها

مقدمه

پس از به دست آمدن فرمول‌های معادلات درجه سوم و چهارم در دوران رنسانس، ریاضیدان‌های قرن‌های هفدهم و هجدهم با سماجت بسیار به جستجوی فرمول‌های حل متناظری برای حل معادلات درجه‌ی ۵ و بالاتر پرداختند. در واقع، بعضی ریاضی‌دان‌ها، از جمله **چیر نهوس**[1] (۱۵۶۱-۸۰۷۱)، فکر می‌کردند که راهی برای حل این معادلات، به کمک رادیکال‌ها به دست آورده‌اند. اما کم کم معلوم شد که برای حل معادلات مذکور، روش مشخصی وجود ندارد. این مطلب را **لاگرانژ**[2] وگاوس بیان کردند. بعد از اثبات رخنه داری که **رافینی**[3] در سال ۱۷۹۹ در این زمینه مطرح کرد،

[1] Tschirnhaus
[2] Joseph-Louis Lagrange
[3] Paolo Ruffini

نیلس هنریک آبل[1] نابغه‌ی ریاضی، که در جوانی، بیماری سل، او را به کام مرگ کشید، موفق شد که اثبات کند معادله عمومی درجه‌ی ۵، و بالاتر را نمی‌توان با رادیکال‌ها حل کرد. البته، درک این موضوع در ابتدا مشکل بود؛ زیرا، بعضی از معادلات درجه‌ی ۵ به بالا، با رادیکال‌ها قابل حل بود که اثبات آبل نشان داد همه‌ی آن‌ها را نمی‌توان بدین شیوه حل نمود.

اواریست گالوا[2] (۱۸۱۱-۱۸۳۲) توانست همه‌ی معادلاتی را که با رادیکال‌ها قابل حل بودند، به‌طور دقیق و کامل بررسی کند. وی در نظریه‌اش، به هر معادله یک گروه اختصاص داد ویافته‌های مربوط به روش حل معادله‌ها را با کمک رادیکال‌ها به‌دست آورد.

۴-۱ گروه‌های حل‌پذیر

تعریف۴-۱

فرض کنیم G یک گروه و $G_0 = G$ و $G_n,...,G_1$ زیر گروه‌هایی از G باشند. اگر به ازای هر i، $0 \le i \le n-1$ ، $G_{i+1} \le G_i$، آن‌گاه زنجیر

$$G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = G$$

را یک **سری** از زیر گروه‌های G می‌نامند.

اگر برای هر i، $0 \le i \le n-1$، $G_{i+1} \trianglelefteq G_i \ (G_i \trianglelefteq G)$ آن‌گاه سری

$$G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = G$$

را یک **سری زیر نرمال (سری نرمال)** برای G گوییم. گروه‌های خارج قسمتی G_i / G_{i+1} را **عوامل** این سری زیر نرمال (سری نرمال) می‌نامیم.

---

[1] Niels Henrik Abel
[2] Evariste Galois

تعریف۴-۲

فرض کنیم G یک گروه باشد. سری زیر نرمال زیر را در نظر می‌گیریم.

$$\{e\} = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$$

(۱) سری بالا را یک سری **حل‌پذیر(آبلی)** برای G گوییم اگر عوامل G_i / G_{i+1} آبلی باشند.

(۲) سری بالا را یک سری **ترکیبی** برای G گوییم اگر عوامل G_i / G_{i+1} ساده باشند.

تعریف۴-۳

گروه G را **حل‌پذیر** گوییم اگر دارای یک سری حل‌پذیر (آبلی) باشد.

قضیه۴-۱

فرض کنیم G یک گروه متناهی باشد. دراین‌صورت گزاره‌های زیر معادلند.

(۱) G حل‌پذیر است،

(۲) عدد صحیح مثبت n موجود است به‌طوری‌که $G^{(n)} = \{e\}$،

(۳) G دارای یک سری ترکیبی است که عامل‌های آن گروه‌هایی دوری از مرتبه‌ی عددی اولند.

اثبات (۲) $\Rightarrow$ (۱): فرض کنیم G یک گروه حل‌پذیر و

$$\{e\} = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$$

یک سری حل‌پذیر (آبلی) برای G باشد. دراین‌صورت با استقرا روی $0 \leq i \leq n$ ثابت می‌کنیم که $G^{(i)} \leq G_i$:

به ازای $i = 0$, $G^{(0)} = G \leq G = G_0$. فرض کنیم $G^{(k)} \leq G_k$. دراین‌صورت بنابر فرض استقرا

$$G^{(k+1)} = \left(G^{(k)}\right)' \leq G_k' \leq G_{k+1},$$

زیرا بنابر فرض G_k / G_{k+1} آبلی است. در نتیجه بنابر استقرا به ازای هر i، $G^{(i)} \leq G_i$. لـذا $G^{(n)} \leq G_n = \{e\}$، که نتیجه حاصل است.

(۱) $\Rightarrow$ **(۲):** نتیجه با در نظر گرفتن سری زیر حاصل می‌شود.

$$\{e\} = G^{(n)} \leq G^{(n-1)} \leq \cdots \leq G^{(0)} = G.$$

(۱) $\Rightarrow$ **(۳):** واضح است.

(۳) $\Rightarrow$ **(۱):** فرض کنیم $\{e\} = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$ یک سری حل‌پـذیر (آبلی) برای G باشد. با استفاده از قضیه‌ی اساسی گروه‌های آبلی متناهی، سری ترکیبـی زیر، که در آن عامل‌ها از مرتبه‌ی عددی اولند، برای گروه آبلی G_i / G_{i+1} موجود است.

$$G_{i+1} / G_{i+1} \leq H_{in_i} / G_{i+1} \leq \cdots \leq H_{i1} / G_{i+1} \leq G_i / G_{i+1}.$$

با اضافه کردن $H_{in_i} \leq \cdots \leq H_{i1}$ بـین $G_{i+1} \leq G_i$، مـی‌تـوانیم بـه یـک سـری ترکیبـی برای G برسیم که در آن عامل‌ها گروه‌هایی دوری از مرتبه‌ی عددی اولند.

■■■

❖ **تذکر:** توجه داشته باشید که در گروه‌های نامتناهی تنها گزاره‌های (۱) و (۲) از قضیه‌ی اخیر معادلند (به تمرین‌های ۴ و ۵ مراجعه شود).

مثال۱: اگر G گروهی آبلی باشد، آن‌گاه چون $G' = \{e\}$، لذا G گروهی حل‌پذیر است.

□

اینک خواص دیگری از گروه‌های حل‌پذیر را مطرح می‌کنیم:

قضیه۴-۲

(۱) هر زیر گروه و هر تصویر همریخت از یک گروه حل‌پذیر، حل‌پذیر است،

(۲) اگر N زیر گروهی نرمال از گروه G باشد به‌طوری‌که N و G/N حل‌پذیر باشند، آن‌گاه G حل‌پذیر است،

(۳) حاصل‌ضرب مستقیم هر تعداد متناهی از گروه‌های حل‌پذیر، حل‌پذیر است.

اثبات (۱): فرض کنیم H زیر گروهی از گروه حل‌پذیر G باشد. دراین‌صورت n ای موجود است که $G^{(n)}=\{e\}$ چون $H^{(n)}\subseteq G^{(n)}$، لذا $H^{(n)}=\{e\}$؛ یعنی H حل‌پذیر است. برای تصویر همریخت، فرض کنیم $\varphi: G\to H$ یک برووریختی باشد (H تصویر همریخت گروه G است). دراین‌صورت به‌آسانی می‌توان نشان داد که برای هر i، $\varphi\left(G^{(i)}\right)=H^{(i)}$. حال چون G حل‌پذیر است، لذا nای موجود است که $G^{(n)}=\{e\}$. در این صورت

$$\{e\}=\varphi\left(G^{(n)}\right)=H^{(n)},$$

یعنی H حل‌پذیر است.

(۲): فرض کنیم $\gamma: G\to G/N$ همریختی طبیعی باشد. چون G/N حل‌پذیر است، لذا nای موجود است که

$$\gamma(G^{(n)})=\left(G/N\right)^{(n)}=\{N\}.$$

ازاین‌رو $G^{(n)}\leq \operatorname{Ker}\gamma=N$. چون N حل‌پذیر است. طبق قسمت (۱) عدد k موجود است به‌طوری‌که $(N)^{(k)}=\{e\}$ و لذا $G^{(n+k)}=\left(G^{(n)}\right)^{(k)}\subseteq (N)^{(k)}=\{e\}$. بنابراین G حل‌پذیر است.

(۳): فرض کنیم $G=H\times K$ که H و K حل‌پذیرند. به‌وضوح $H\times\{e\}\trianglelefteq H\times K=G$ و $K\cong G/(H\times\{e\})=(H\times K)/(H\times\{e\})$. بنابراین $G/(H\times\{e\})$ حل‌پذیر است. از طرفی چون $H\cong H\times\{e\}$، لذا $H\times\{e\}$ نیزحل‌پذیر است و درنتیجه طبق قسمت (۲)، G حل‌پذیر خواهد بود. حال با استقرا می‌توان نشان داد که حاصل‌ضرب هر تعداد متناهی از گروه‌های حل‌پذیر، حل‌پذیر است.

■■■

نتیجه‌ی زیر در بخش بعدی نقشی بسیار اساسی دارد.

نتیجه۴-۱

برای $n \geq 5$، گروه S_n حل‌پذیر نیست.

اثبات: فرض کنیم $n \geq 5$. اگر نشان دهیم A_n حل‌پذیر نیست، آن‌گاه طبق قضیه‌ی قبل S_n نیز حل‌پذیر نخواهد بود. چون A_n آبلی نیست، پس $A_n' \neq \{e\}$. از طرفی با توجه به این‌که $A_n' \trianglelefteq A_n$ و A_n ساده است (البته $n \geq 5$)، باید داشته باشیم $A_n' = A_n$؛ بنابراین برای هر $i \geq 1$, $A_n^{(i)} = A_n \neq \{e\}$ و لذا A_n حل‌پذیر نیست.

■■■

تمرین‌های سطح۱

۱- تمام سری‌های ترکیبی $S_3 \times \mathbb{Z}_3, A_4$ و S_4 را بنویسید.

۲-ثابت کنید هر گروه با مرتبه‌ی کوچک‌تر از 60 گروهی حل‌پذیر است.

۳- با یک مثال نقض نشان دهید که هر گروه نامتناهی الزاماً دارای یک سری ترکیبی نیست.

۴-با یک مثال نشان دهید که قضیه‌ی ۱ برای گروه‌های نامتناهی برقرار نیست.

۵- نشان دهید گزاره‌های (۱) و (۲) از قضیه‌ی ۱ برای گروه‌های نامتناهی معادلند.

تمرین‌های سطح۲

۶- فرض کنید p، q و r اعداد اول و n یک عدد طبیعی باشد. نشان دهید

(الف) هر گروه از مرتبه‌ی pqr حل‌پذیر است،

(ب) هر گروه از مرتبه‌ی p^2q^2 حل‌پذیر است،

(پ) هر گروه از مرتبه‌ی $p^n q$ حل‌پذیر است.

۷- ثابت کنید گروه آبلی G دارای سری ترکیبی است اگر و فقط اگر G متناهی باشد.

۸- اگر M یک زیر گروه ماکزیمال سره‌ای از گروه حل‌پذیر متناهی G باشد، ثابت کنید $[G : M]$ توانی از یک عدد اول است.

۹- اگر G یک گروه متناهی غیر ساده باشد به‌طوری‌که همه‌ی زیرگروه‌های سره‌ی آن آبلی باشند، ثابت کنید G حل‌پذیر است.

تمرین‌های سطح ۳

۱۰-فرض کنید G گروهی حل ناپذیر باشد به‌طوری‌که $|G| \leq 120$. ثابت کنید $G \cong A_5$.

۱۱- اگر اندیس هر زیرگروه ماکزیمال گروه متناهی G عددی اول یا مربع عددی اول باشد، نشان دهید G حل‌پذیر است.

۲-۴ حل‌پذیری با رادیکال‌ها

در این بخش به ارائه‌ی معروف‌ترین کاربرد نظریه‌ی گالوا، یعنی محکی برای حل معادلات چند جمله‌ای توسط رادیکال‌ها، می‌پردازیم. ابتدا مفهوم حل‌پذیری با رادیکال‌ها را معرفی می‌کنیم. فرض کنیم F میدانی با مشخصه‌ی صفر باشد. دستور آشنای زیر در مورد حل معادله‌ی درجه‌ی دوم $ax^2 + bx + c = 0$، که $a, b, c \in F$، را در نظر بگیرید:

$$x = \frac{-b \pm \sqrt{\Delta}}{2a},$$

جایی‌که $\Delta = b^2 - 4ac$. جواب‌های این معادله از انجام اعمال میدان (جمع وضرب) بر ضرایب وگرفتن ریشه از عنصر Δ به‌دست می‌آید؛ به‌عبارت دیگر، جواب‌های این معادله در توسیع $F(\sqrt{\Delta})$ قرار دارد. توجه داشته باشید که

$$\sqrt{\Delta}^2 \in F.$$

بـرای حـل معادلـه‌ی درجـه‌ی سـوم نیـز مـوقعیتی مشـابه داریـم. معادلـه‌ی $x^3 + rx^2 + sx + t = 0$، که $r,s,t \in F$، را در نظـر بگیریـد، فـرض کنـیم $p = s - \frac{r^2}{3}$، $q = \frac{2r^3}{27} - \frac{sr}{3}$. قرار می‌دهیم

$$u_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}} \quad \text{و} \quad u_2 = u_1\omega \quad \text{و} \quad u_3 = u_1\omega^2$$

$$v_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}} \quad \text{و} \quad v_2 = v_1\omega \quad \text{و} \quad v_3 = v_1\omega^2$$

که در آن‌ها $\omega \neq 1$ ریشه‌ی سوم واحد است. دراین‌صورت جواب‌های معادلـه داده شـده عبارتند از

$$y_1 = u_1 + v_1 \quad \text{و} \quad y_2 = u_2 + v_3 \quad \text{و} \quad y_3 = u_3 + v_2$$

با فرض $z = \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}$، جواب‌های این معادله در توسـیع $F(z,u_1,v_1,w)$ قـرار دارد. توجه داشته باشید که

$$\begin{aligned} &z^2 \in F, \\ &u_1{}^3 \in F(z), \\ &v_1{}^3 \in F(z) \subseteq F(z,u_1), \\ &w^3 \in F \subseteq F(z,u_1,v_1). \end{aligned}$$

حل معادله‌ی درجه‌ی چهارم نیـز بـا اسـتفاده از انجـام اعمـال میـدان (جمـع و ضـرب) برضرایب وگرفتن ریشه‌ی دوم، به حل یک معادله‌ی درجه‌ی سوم منجر می‌شـود و لـذا در این مورد نیز می‌توان فرمولی ارائه داد.

ریشه‌ی تاریخی نظریه‌ی گالوا در حل این مسأله است که آیا یک فرمول صریح (مسـتلزم فقط اعمال میدان و ریشه گیری) برای جواب‌های معادله‌ی چند جمله‌ای

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0,$$

که $a_i \in F$، وجود دارد.

اولین قدم بیان صورت دقیق مسأله با مفاهیم نظریه‌ی میدان است. وجـود یـک فرمـول برای حل یک معادله‌ی چند جمله‌ای؛ یعنی هر جواب را بتوان با تعـداد متنـاهی اعمـال جمع و ضرب و ریشه‌گیری روی میدان پایه‌ی F به‌دست آورد. انجام یـک عمـل میـدان، میدا ن‌پایه را تغییر نمی‌دهد؛ ولی ریشه گیری از عنصـر $c \in F$ منجـر بـه سـاختن یـک توسـیع ماننـد $F(u)$، کـه $u = \sqrt[m]{c}$، مـی‌شـود. ازایـن‌رو وجـود یـک فرمـول بـرای حـل معادله‌ی $f(x) = 0$ در واقع وجود یک زنجیر متناهی از میدان‌ها مانند

$$F = F_0 \subseteq F(u_1) \subseteq \cdots \subseteq F(u_1,,\ldots,u_n) = E$$

است که E شامل همه‌ی ریشه‌های $f(x)$ است و اعداد طبیعی $m_1,\ldots,m_n$ موجودند که

$$u_1^{m_1} \in F,$$

$$u_i^{m_i} \in F(u_1,\ldots,u_{i-1}),$$

برای $2 \leq i \leq n$. برعکس، فرض کنیم چنین زنجیری از میدان‌ها وجود داشته باشـد و E شامل تمام ریشه‌های $f(x)$ باشد. دراین‌صورت هر ریشه را مـی‌تـوان بـا تعـداد متنـاهی اعمال میدان، برحسب تعداد متناهی از عناصر $F \cup \{u_1,\ldots,u_n\}$ نوشت. اینـک انگیـزه‌ی لازم برای تعریف زیر فراهم است.

تعریف۴-۴

توسیع K از F را یک **توسیع رادیکالی** F گوییم اگر عناصر $u_1,\ldots,u_n \in K$ و اعداد طبیعی $m_1,\ldots,m_n$ موجود باشند به‌طوری‌که

(۱) $K = F(u_1,\ldots,u_n)$،

(۲) $u_1^{m_1} \in F$ و $u_i^{m_i} \in F(u_1,\ldots,u_{i-1})$ برای $2 \leq i \leq n$.

تعریف۴-۵

فرض کنیم F یک میدان و $f(x) \in F[x]$. دراین‌صورت گوییم $f(x)$ با رادیکال‌ها روی F **حل‌پذیر** است اگر یک توسیع رادیکالی مانند K از F شامل میدان شکافنده‌ی $f(x)$ روی F موجود باشد.

جهت رسیدن به محک حل‌پذیری با رادیکال‌ها نیاز داریم رابطه‌ی بین میدان‌های شکافنده و توسیع‌های نرمال را بیابیم و بدین منظور به گزاره‌های زیر احتیاج داریم.

گزاره۴-۱

فرض کنیم F یک میدان و $f(x) \in F[x]$ و K میدان شکافنده‌ی $f(x)$ روی F باشد. هم‌چنین فرض کنیم $p(x)$ عامل تحویل‌ناپذیر از $f(x)$ در $F[x]$ و $a_1, a_2, \ldots, a_r$ ریشه‌های $p(x)$ باشند. دراین‌صورت به ازای هر i، $1 \leq i \leq r$ عنصر $\sigma_i \in \mathrm{Aut}_F K$ موجود است به‌طوری‌که $\sigma_i(a_1) = a_i$.

اثبات: فرض کنیم $a_1, a_i \in K$ دو ریشه از $p(x)$ باشند. دراین‌صورت یکریختی $\tau : F(a_1) \to F(a_i)$ موجود است به‌نحوی که $\tau(a_1) \to a_i$ و به ازای هر $a \in F$، $\tau(a) = a$. چون K میدان شکافنده $f(x)$ روی $F(a_1)$ و نیز روی $F(a_i)$ است، لذا یکریختی $\sigma_i : K \to K$ موجود است به‌نحوی که $\sigma_i |_{F(a_1)} = \tau$. بنابراین، به ازای هر $a \in F(a_1)$، $\sigma_i(a_1) = \tau(a_1) = (a_i)$ و به‌ویژه به ازای هر $a \in F$، $\sigma(a) = a$؛ یعنی عنصر $\sigma_i \in \mathrm{Aut}_F K$ موجود است به‌طوری‌که $\sigma_i(a_1) = a_i$.

■■■

گزاره ۴-۲

اگر F میدانی با مشخصه‌ی صفر باشد، آن‌گاه هر توسیع متناهی از F توسیع ساده است.

اثبات: کافی است مطلب را در مورد $L = F(a,b)$ ثابت کرد. حالت کلی با استقرا به آسانی به دست می آید. فرض کنیم $f(x)$ و $g(x)$ به ترتیب چند جمله‌ای‌های مینیمال a و b روی F باشد و فرض کنیم $a = a_1, a_2, ..., a_m$ ریشه‌های $f(x)$ و $b = b_1, ..., b_n$ ریشه‌های $g(x)$ باشند. $\gamma \in F$ را طوری انتخاب می‌کنیم که با عناصر $\frac{a_i - a}{b - b_j}$، $j \neq 1$، متمایز باشد. با فرض $\theta = a + b\gamma$ نشان می‌دهیم $F(a,b) = F(\theta)$. به‌وضوح $F(\theta) \subseteq F(a,b)$. بنابراین کافی است نشان دهیم $a,b \in F(\theta)$. تعریف می‌کنیم:

$$h(x) := f(\theta - \gamma x) \in F(\theta)[x].$$

دراین‌صورت $h(b) = f(\theta - \gamma b) = f(a) = 0$ و برای هر $j \neq 1$، $h(b_j) = f(\theta - \gamma b_j) \neq 0$.

بنابراین در حلقه‌ی $F(\theta)[x]$ چند جمله‌ای‌های $g(x)$ و $h(x)$ دارای ریشه‌ی مشترک b هستند. فرض کنیم $p(x)$ چند جمله‌ای مینیمال b در حلقه $F(\theta)[x]$ باشد. ازاین‌رو $p(x) \mid g(x)$ و $p(x) \mid h(x)$. با توجه به این‌که b تنها ریشه مشترک $g(x)$ و $h(x)$ است، لذا $p(x) = x - b$ و در نتیجه $b \in F(\theta)$. بنابراین $a = \theta - b\gamma \in F(\theta)$ و اثبات تمام است.

■■■

قضیه۴-۳

فرض کنیم F میدانی با مشخصه‌ی صفر و K یک توسیع متناهی از F باشد. دراین صورت K یک توسیع نرمال از F است اگر و تنها اگر K میدان شکافنده‌ی یک چند جمله‌ای روی F باشد.

اثبات: فرض کنیم K یک توسیع نرمال از F باشد. چون K یک توسیع متناهی از F است، پس طبق گزاره‌ی ۲، K یک توسیع ساده F است ولذا عنصر $a \in K$ موجود است به‌طوری‌که $K = F(a)$. فرض کنیم $\mathrm{Aut}_F K = \{\sigma_1, ..., \sigma_n\}$. قرار می‌دهیم

$$f(x) = (x - \sigma_1(a)) \cdots (x - \sigma_n(a)) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$$

به‌آسانی می‌توان نشان داد که $c_i \in F$، و در نتیجه $f(x) \in F[x]$. از طرفی a ریشه‌ای از $f(x)$ بوده و $K = F(a)$ پس هر توسیع از F که شامل a باشد، باید شامل $K = F(a)$ نیز باشد، پس K میدان شکافنده‌ی $f(x)$ روی F است.

برعکس: فرض کنیم K میدان شکافنده‌ی چند جمله‌ای $f(x)$ روی F باشد. با توجه به این‌که $[K : F] < \infty$، با استقرا روی $[K : F]$ نشان می‌دهیم که K یک توسیع نرمالی از F است. اگر $[K : F] = 1$، به‌وضوح حکم برقرار است. حال فرض کنیم، حکم برای هر توسیع K_1 از میدان F_1 که $[K_1 : F_1] < [K : F]$ و K_1 که میدان شکافنده‌ی یک چند جمله‌ای روی F_1 است، برقرار باشد. اگر $f(x)$ به‌طور کامل روی F تجزیه شود، آن‌گاه $K = F$ و در نتیجه حکم برقرار است. پس فرض کنیم $f(x)$ دارای عامل تحویل‌ناپذیر $p(x) \in F[x]$ از درجه‌ی $m > 1$ باشد. $p(x)$ دارای ریشه‌های متمایز $a_1, \ldots, a_m$ است (تمرین۵(الف)از بخش۳-۱ ملاحظه شود). اگر K میدان شکافنده‌ی $f(x)$ روی $F(a_1)$ باشد، آن‌گاه

$$[K : F(a_1)] = \frac{[K : F]}{[F(a_1) : F]} = \frac{n}{m} < n.$$

بنابر فرض استقرا، K یک توسیع نرمال از $F(a_1)$ است. حال فرض کنیم، $a \in K$ عنصری باشد که برای هر $\sigma \in \mathrm{Aut}_F K$، $\sigma(a) = a$. برای اثبات نرمال بودن توسیع K روی F باید نشان دهیم که $a \in F$. چون $\mathrm{Aut}_{F(a_1)} K \leq \mathrm{Aut}_F K$، پس برای هر $\sigma \in \mathrm{Aut}_{F(a_1)} K$ ، $\sigma(a) = a$. با توجه به این‌که K یک توسیع نرمال از $F(a_1)$ است، خواهیم داشت $a \in F(a_1)$ و در نتیجه عناصر $c_0, \ldots, c_{m-1} \in F$ موجودند به‌طوری‌که

$$a = c_0 + c_1 a_1 + \cdots + c_{m-1} a_1^{m-1}.$$

با توجه به گزاره‌ی۱، برای هر i، $1 \leq i \leq m$، عنصر $\sigma_i \in \mathrm{Aut}_F K$ موجود است به‌طوری‌که $\sigma_i(a_1) = a_i$. از این‌رو با توجه به انتخاب a خواهیم داشت:

$$\begin{aligned} a = \sigma_i(a) &= \sigma_i(c_0 + c_1 a_1 + \cdots + c_{m-1} a_1^{m-1}) \\ &= c_0 + c_1 \sigma_i(a_1) + \cdots + c_{m-1} \sigma_i(a_1)^{m-1} \\ &= c_0 + c_1 a_i + \cdots + c_{m-1} a_i^{m-1}. \end{aligned}$$

بنابراین برای هر $1 \le i \le m$، a_i ریشه‌ی چندجمله‌ای زیر است.

$$q(x) = (c_0 - a) + c_1 x + \cdots + c_{m-1} x^{m-1}.$$

یعنی، $q(x)$ حداقل دارای m ریشه متمایز است. با توجه به این‌که $q(x)$ از درجه‌ی حداکثر $m-1$ است، باید داشته باشیم $q(x) = 0$. پس $c_0 - a = 0$ و در نتیجه $a = c_0 \in F$.

■■■

گزاره۴-۳

فرض کنیم F یک میدان با مشخصه‌ی صفر، n یک عدد صحیح مثبت، $0 \neq b \in F$ و K میدان شکافنده‌ی $g(x) = x^n - b$ روی F باشد. دراین صورت

(۱) گروه گالوایی $x^n - 1$ روی F آبلی است.

(۲)اگر F شامل تمامی ریشه‌های n ام واحد باشد، آن‌گاه گروه گالوایی $g(x)$ روی F آبلی است.

(۳) گروه گالوایی $g(x)$ روی F حل‌پذیر است.

اثبات(۱): فرض کنیم $f(x) = x^n - 1$ و E میدان شکافنده‌ی $f(x)$ روی F باشد. فرض کنیم $\Omega = \{w_1, \ldots, w_n\}$ مجموعه‌ی تمامی ریشه‌های $f(x)$ باشد (توجه داشته باشید که طبق لم ۳-۱ریشه‌های $f(x)$ متمایزند). دراین صورت Ω طبق نتیجه‌ی ۳-۳یک زیر گروه دوری از E^* است. اگر w یک مولد برای Ωباشد، آن‌گاه $E = F(w)$ و هر $\sigma \in \mathrm{Aut}_F E$ توسط $\sigma(w)$ به‌طور کامل مشخص می‌شود. به‌علاوه $\sigma(w)$ یک ریشه از $f(x)$ بوده و در نتیجه به ازای یک $1 \le i \le n$، $\sigma(w) = w^i$. اگر $\sigma, \tau \in \mathrm{Aut}_F E$، آن‌گاه عناصر $1 \le i, j \le n$ موجودند به‌طوری‌که $\sigma(w) = w^i$ و $\tau(w) = w^j$. بنابراین

$$\sigma\tau(w) = \sigma(\tau(w)) = \sigma(w^j) = (w^j)^i = w^{ji},$$
$$\tau\sigma(w) = (\sigma(w)) = \tau(w^i) = (w^i)^j = w^{ij}.$$

ازاین‌رو $\sigma\tau = \tau\sigma$، یعنی $\mathrm{Aut}_F E$ آبلی است.

(۲): فرض کنیم $\Omega = \{w_1, \ldots, w_n\} \subseteq F$ مجموعه‌ی تمامی ریشه‌های nام واحد باشد. اگر $a \in K$ ریشه‌ای از $g(x)$ باشد، آن‌گاه $A = \{w_1 a, \ldots, w_n a\}$ مجموعه تمامی ریشه‌های $g(x)$ است. از این‌رو $K = F(a)$ و هر $\sigma \in \mathrm{Aut}_F K$ توسط $\sigma(a)$ به‌طور کامل مشخص می‌شود. به‌علاوه $\sigma(a)$ یک ریشه از $g(x)$ بوده و در نتیجه به ازای یک $1 \leq i \leq n$، $\sigma(a) = w_i a$. اگر $\sigma, \tau \in \mathrm{Aut}_F K$، آن‌گاه عناصر $1 \leq i, j \leq n$ موجودند به‌طوری‌که $\sigma(a) = w_i a$ و $\tau(a) = w_j a$. بنابراین با توجه به این‌که $w_i, w_j \in F$، خواهیم داشت:

$$\sigma\tau(a) = \sigma(\tau(a)) = \sigma(w_j a) = \sigma(w_j)\sigma(a) = w_j(w_i a) = w_j w_i a,$$
$$\tau\sigma(a) = \tau(\sigma(a)) = \tau(w_i a) = \tau(w_i)\tau(a) = w_i(w_j a) = w_i w_j a.$$

ازاین‌رو $\sigma\tau = \tau\sigma$؛ یعنی $\mathrm{Aut}_F K$ آبلی است.

(۳): فرض کنیم w مولدی برای گروه دوری متشکل از ریشه‌های nام واحد باشد. فرض کنیم a ریشه‌ای از $g(x)$ باشد. درلین‌صورت wa نیز ریشه‌ای از $g(x)$ بوده و لذا $w = (wa)a^{-1} \in K$. حال فرض کنیم $E = F(w)$. دراین صورت E شامل تمامی ریشه‌های n ام واحد بوده و $F \subseteq E \subseteq K$. با توجه به (۱) و (۲) گروه‌های $\mathrm{Aut}_F E$ و $\mathrm{Aut}_E K$ آبلی‌اند. از طرفی با توجه به این‌که K یک توسیع نرمال از F بوده، لذا طبق قضیه‌ی اساسی نظریه‌ی گالوا، سری حل پذیر زیر را خواهیم داشت:

$$\{\mathrm{id}\} \leq \mathrm{Aut}_E K \leq \mathrm{Aut}_F K.$$

ازاین‌رو، طبق تعریف، $\mathrm{Aut}_F K$ حل‌پذیر است.

■■■

گزاره۴-۴

فرض کنیم F میدانی با مشخصه‌ی صفر و E یک توسیع رادیکالی از F باشد. دراین‌صورت یک توسیع رادیکالی نرمال K از F که شامل E است، موجود است.

اثبات: فرض کنیم $E = F(u_1,\dots,u_n)$، که $u_1^{m_1} \in F$ و $u_i^{m_i} \in F(u_1,\dots,u_{i-1})$ برای $2 \le i \le n$. فرض کنیم $f_i(x)$ چند جمله‌ای مینیمال u_i روی F و K میدان شکافنده چند جمله‌ای $f(x) = f_1(x)\dots f_n(x)$ روی F باشد. اگر $\mathrm{Aut}_F K = \{\sigma_1,\sigma_2,\dots,\sigma_k\}$، آن‌گاه با توجه به گزاره‌ی ۱ داریم:

$$K = F(\sigma_1(u_1),\dots,\sigma_k(u_1),\sigma_1(u_2),\dots,\sigma_k(u_2),\dots,\sigma_1(u_n),\dots,\sigma_k(u_n)).$$

کافی است نشان دهیم که K یک توسیع رادیکال روی F است. برای هر $1 \le j \le k$ داریم:

$$\begin{aligned}
[\sigma_j(u_1)]^{m_1} &= \sigma_j(u_1^{m_1}) \in \sigma_j(F) = F,\\
[\sigma_j(u_2)]^{m_2} &= \sigma_j(u_2^{m_2}) \in \sigma_j(F(u_1)) = F(\sigma_j(u_1)) \subseteq F(\sigma_1(u_1),\dots,\sigma_k(u_1)),\\
&\vdots\\
[\sigma_j(u_n)]^{m_n} &= \sigma_j(u_n^{m_n}) \in \sigma_j(F(u_1,\dots,u_{n-1})) = F(\sigma_j(u_1),\dots,\sigma_j(u_{n-1}))\\
&\subseteq F(\sigma_1(u_1),\dots,\sigma_k(u_1),\sigma_1(u_2),\dots,\sigma_k(u_2),\dots,\sigma_1(u_{n-1}),\dots,\sigma_k(u_{n-1})).
\end{aligned}$$

بنابراین طبق تعریف K یک توسیع رادیکال روی F است.

■■■

اکنون برای اثبات قضیه‌ی اساسی این بخش آماده هستیم.

قضیه ۴-۴

فرض کنیم F یک میدان با مشخصه‌ی صفر و $f(x) \in F[x]$. اگر $f(x)$ با رادیکال‌ها روی F حل‌پذیر باشد، آن‌گاه گروه گالوایی $f(x)$ روی F حل‌پذیر است.

اثبات: فرض کنیم L میدان شکافنده‌ی $f(x)$ روی F باشد. چون $f(x)$ با رادیکال‌ها روی F حل‌پذیر باشد، طبق تعریف، توسیع رادیکال E از F موجود است به‌طوری‌که $L \subseteq E$. طبق گزاره‌ی ۴ توسیع رادیکالی نرمال K از F موجود است به‌طوری‌که $E \subseteq K$. فرض کنیم $K = F(u_1,\dots,u_n)$، که $u_1^{m_1} \in F$ و $u_i^{m_i} \in F(u_1,\dots,u_{i-1})$ برای $2 \le i \le n$. قرار می‌دهیم $F_0 = F$ و $F_i = F(u_1,\dots,u_{i-1})$

برای $2 \leq i \leq n$. چون K یک توسیع نرمال از F_i است، بنابراین طبق قضیه‌ی اساسی گالوا $\mathrm{Aut}_{F_i}E$ یک زیرگروه نرمال از $\mathrm{Aut}_{F_{i-1}}K$ و در نتیجه سری زیرنرمال زیر را خواهیم داشت:

$$\{\mathrm{id}\} \subseteq \mathrm{Aut}_{F_{n-1}}K \subseteq \cdots \subseteq \mathrm{Aut}_{F}K.$$

با استفاده‌ی مجدد از قضیه‌ی اساسی گالوا داریم:

$$\frac{\mathrm{Aut}_{F_{i-1}}K}{\mathrm{Aut}_{F_i}K} \cong \mathrm{Aut}_{F_{i-1}}F_i.$$

با توجه به گزاره‌ی۳(۲) ، $\mathrm{Aut}_{F_{i-1}}F_i$ یک گروه آبلی است و در نتیجه بنابرتعریف، $\mathrm{Aut}_{F}K$ حل‌پذیر است. از طرفی طبق قضیه‌ی اساسی

$$\mathrm{Aut}_{F}L \cong \frac{\mathrm{Aut}_{F}K}{\mathrm{Aut}_{L}K}.$$

ازاین‌رو $\mathrm{Aut}_{F}L$ به‌عنوا ن‌گروه خارج قسمت یک گروه حل‌پذیر، حل‌پذیر است.

■■■

هدف بعدی این است که نشان دهیم عکس قضیه‌ی اخیر نیز برقرار است. یعنی محک بسیار مهم زیر را برای حل پذیری چندجمله‌ای‌ها با رادیکال‌ها، به‌دست خواهیم آورد.

محک حل‌پذیری چندجمله‌ای‌ها با رادیکال‌ها

اگر F یک میدا ن‌با مشخصه‌ی صفر و $f(x) \in F[x]$، آن‌گاه $f(x)$ با رادیکال‌ها روی F حل‌پذیر است اگر و تنها اگر گروه گالوایی $f(x)$ روی F حل‌پذیر باشد.

ابتدا لم زیر را بیان می‌کنیم.

لم۴-۱

فرض کنیم p عددی اول و F میدانی شامل همه‌ی ریشه‌های pام واحد باشد. فرض کنیم K توسیعی نرمال از F باشد به‌طوری‌که $[K:F]=p$ و $\mathrm{Aut}_F K$ دوری است. دراین‌صورت عنصر $u\in K$ موجود است به‌قسمی که $K=F(u)$ و $u^p\in F$.

اثبات: فرض کنیم $\Omega=\{w_1,\ldots,w_p\}$ مجموعه‌ی ریشه‌های pام واحد باشد و $\mathrm{Aut}_F K=<\sigma>$ و $c\in K-F$ عنصر ثابتی باشد (چون $[K:F]=p$ عددی اول است، پس $K=F(c)$). برای هر $1\le i\le p$ قرار می‌دهیم:

$$d_i=c+\sigma(c)w_i+\cdots+\sigma^{p-1}(c)w_i^{p-1}.$$

دراین‌صورت $d_i\in K$ و

$$\sigma(d_i)=\sigma(c)+\sigma^2(c)w_i+\cdots+\sigma^p(c)w_i^{p-1}=w_i^{-1}d_i,$$

بنابراین

$$\sigma(d_i^p)=(\sigma(d_i))^p=(w_i d_i)^p=d_i^p,$$

که با توجه به نرمال بودن K روی F، خواهیم داشت $d_i^p\in F$.

کافی است ثابت کنیم $1\le i\le p$موجود است که $d_i\notin F$. برای این منظور دستگاه زیر را در نظر می‌گیریم:

$$\begin{cases} c+\sigma(c)w_1+\cdots+\sigma^{p-1}(c)w_1^p=d_1\\ c+\sigma(c)w_2+\cdots+\sigma^{p-1}(c)w_2^p=d_2\\ \qquad\qquad\vdots\\ c+\sigma(c)w_p+\cdots+\sigma^{p-1}(c)w_p^p=d_p \end{cases}$$

ماتریس ضرایب این دستگاه که به **ماتریس واندرموند**[1] معروف است، عبارت است از:

[1] Vandermonde Matrix

$$M=\begin{bmatrix}1 & w_1 & \dots & w_1^{p-1}\\ 1 & w_2 & \dots & w_2^{p-1}\\ \vdots & \vdots & \vdots & \vdots\\ 1 & w_p & \dots & w_p^{p-1}\end{bmatrix}$$

بـه آسـانی مـی‌تـوان نشـان داد کـه $\det(M)=\prod_{i<j}(w_i-w_j)$ و لـذا مـاتریس M دارای معکوس M^{-1} است. ازاین‌رو

$$\begin{bmatrix}c\\ \sigma(c)\\ \vdots\\ \sigma^{p-1}(c)\end{bmatrix}=M^{-1}\begin{bmatrix}d_1\\ d_2\\ \vdots\\ d_p\end{bmatrix}$$

در نتیجه c ترکیب خطی از عناصر $d_1,\dots,d_p$ است و از آن‌جا که $K=F(c)$ و درایه‌هـای ماتریس M^{-1} در F است، خواهیم داشت:

$$K=F(d_1,\dots,d_p).$$

حـال اگـر بـه‌ازای هـر $1\le i\le p$، $d_i\in F$ آن‌گـاه $K=F$ کـه تنـاقض اسـت. بنابراین $1\le i\le p$ موجود اسـت بـه‌طـوری‌کـه $d_i\notin F$ و در نتیجـه $K=F(d_i)$. بـدین ترتیب اثبات تمام است.

■■■

قضیه۴-۵

فرض کنیم F یـک میـدان بـا مشخصـه‌ی صـفر و $f(x)\in F[x]$. اگـر گـروه گـالوایی $f(x)$روی F حل‌پذیر باشد، آن‌گاه $f(x)$ با رادیکال‌ها روی F حل‌پذیر است.

اثبات: فرض کنیم K میدان شکافنده‌ی $f(x)$ روی F، $G = \mathrm{Aut}_F K$ گروهی حل‌پذیر، $[K : F] = |G| = n$ و w مولدی برای گروه دوری متشکل از ریشه‌های nام واحد باشد. تعریف می‌کنیم:

$$\theta: \mathrm{Aut}_{F(w)} K(w) \to \mathrm{Aut}_F K$$
$$\tau \mapsto \tau\,|_K$$

به‌سادگی می‌توان تحقیق کرد که θ تکریختی است و لذا $\mathrm{Aut}_{F(w)} K(w)$ با زیرگروهی از $\mathrm{Aut}_F K$ یکریخت و در نتیجه حل‌پذیر است. بنابراین سری

$$\{1\} = H_m \subseteq H_{m-1} \subseteq \cdots \subseteq H_2 \subseteq H_1 = \mathrm{Aut}_{F(w)} K(w)$$

که در آن عوامل H_{i-1} / H_i دوری و از مرتبه‌ی عدد اول p_i می‌باشند، موجود است. قرار می‌دهیم $F_i = H_i'$. دراین‌صورت زنجیر

$$F = F_0 \subseteq F(w) = F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq F_m = K(w)$$

از زیرمیدان‌های $K(w)$ را خواهیم داشت. میدان $K(w)$ یک توسیع نرمال $F(w)$ است (زیرا $K(w)$ میدان شکافنده‌ی $x^n - 1$ روی $F(w)$ است)؛ همچنین به ازای هر $1 \le i \le m$، $\mathrm{Aut}_{F_{i+1}} K(w) \trianglelefteq \mathrm{Aut}_{F_i} K(w)$؛ لذا طبق قضیه‌ی اساسی، F_{i+1} یک توسیع نرمال F_i است. در ضمن

$$\frac{H_i}{H_{i+1}} \cong \frac{\mathrm{Aut}_{F_i} K(w)}{\mathrm{Aut}_{F_{i+1}} K(w)} \cong \mathrm{Aut}_{F_i} F_{i+1}$$

دوری و از مرتبه‌ی عدد اول p_i است. چون $p_i \mid |G| = n$ و به ازای هر $i > 1$، F_i شامل ریشه‌های nام واحد است، لذا F_i شامل تمامی ریشه‌های p_iام واحد است و بنابر لم اخیر، عنصر $d_i \in F_{i+1} \setminus F_i$ موجود است که $F_{i+1} = F_i(d_i)$ و $d_i^p \in F_i$. یعنی $K(w)$ یک توسیع رادیکالی از F است. از طرفی $K \subseteq K(w)$، پس بنابر تعریف، $f(x)$ با رادیکال‌ها روی F حل‌پذیر است.

■■■

این بخش را با ارائه‌ی مثالی از یک چند جمله‌ای که گروه گالوایی آن حل‌پذیر نیست به پایان می‌رسانیم. ابتدا گزاره‌های زیر را اثبات می‌کنیم.

گزاره۴-۵

فرض کنیم p یک عدد اول و H زیرگروهی از S_p باشد که شامل یک ترانهش مانند σ ویک دور به‌طول p مانند τ باشد. دراین صورت $H = S_p$.

اثبات: به‌عنوا ن‌تمرین به‌عهده خواننده واگذار می‌شود.

■■■

گزاره۴-۶

فرض کنیم F یک میدان با مشخصه‌ی صفر و $f(x) \in F[x]$ یک چند جمله‌ای تحویل‌ناپذیر از درجه‌ی n باشد. دراین صورت G_f با زیرگروهی از S_n یکریخت است.

اثبات: فرض کنیم $X = \{u_1,\dots,u_n\}$ مجموعه‌ی ریشه‌های متمایز f در میدان شکافنده K باشد. برای هر $u_i \in X$ قرار می‌دهیم، $I(u_i) := i$ (توجه داشته باشید که $I(u_i)$ نمایش‌گر اندیس u_i می‌باشد) و تعریف می‌کنیم:

$$\theta : G_f \to S_n$$
$$\sigma \mapsto \begin{pmatrix} 1 & 2 & \cdots & n \\ I(\sigma(u_1)) & I(\sigma(u_2)) & \cdots & I(\sigma(u_n)) \end{pmatrix}.$$

با توجه به این‌که $X = \{\sigma(u_1),\dots,\sigma(u_n)\}$، به آسانی می‌توان نشان داد که θ یک تکریختی است.

■■■

قضیه۴-۵

فرض کنیم $\mathbb{Q}$ میدان اعدادگویا و p یک عدد اول و $f(x) \in \mathbb{Q}[x]$ یک چند جمله‌ای تحویل‌ناپذیر از درجه‌ی p باشد. اگر $f(x)$ دارای دقیقاً دو ریشه‌ی غیر حقیقی باشد، آن‌گاه گروه گالوایی $f(x)$ روی $\mathbb{Q}$، برابر S_p است.

اثبات: فرض کنیم $X = \{u_1, u_2, ..., u_p\}$ مجموعه‌ی ریشه‌های متمایز $f(x)$ در میدان شکافنده‌ی K باشد به‌طوری‌که u_1, u_2 ریشه‌های غیر حقیقی هستند. برای هر $u_i \in X$ داریم:

$$| G_f | = [K : \mathbb{Q}] = [K : \mathbb{Q}(u_i)][\mathbb{Q}(u_i) : \mathbb{Q}] = [K : \mathbb{Q}(u_i)]p.$$

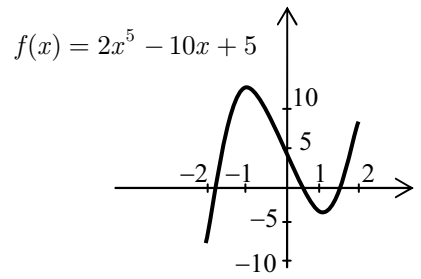
ازاین‌رو طبق قضیه‌ی کوشی (نتیجه ۶-۱)، G_f دارای عنصری مانند σ از مرتبه‌ی p است. تعریف می‌کنیم:

$$\tau : K \to K$$
$$x \mapsto \overline{x}$$

که در این‌جا $\overline{x}$ نشان‌دهنده‌ی مزدوج مختلط x است. با توجه به این‌که u_1 و u_2 مزدوج‌اند، $\tau(u_1) = u_2 \neq u_1$ و لذا τ عنصری مرتبه 2 از G_f است. با توجه به گزاره‌ی ۶، σ و τ را می‌توان به‌ترتیب به عنوان یک دور به‌طول p و یک ترانهش در نظر گرفت؛ بنابراین طبق گزاره‌ی ۵، $G_f = S_p$.

مثال۲: چند جمله‌ای $f(x) = 2x^5 - 10x + 5 \in \mathbb{Q}[x]$ با رادیکال‌ها روی $\mathbb{Q}$ حل‌پذیر نیست.

حل: با توجه به محک آیزنشتاین $f(x)$ روی $\mathbb{Q}$ تحویل ناپذیر است. اگر $f'(x) = 10(x^4 - 1) = 0$، آن‌گاه $x = \pm 1$. بنابراین نمودار $f(x)$ در نقاط $x = 1$ و $x = -1$ به‌ترتیب به مینیمم و ماکزیمم موضعی خود می‌رسد و با توجه به تعیین علامت $f(x)$ به نمودار زیر خواهیم رسید:



بنـابراین $f(x)$ دقیقـاً دارای دو ریشـه‌ی غیـر حقیقـی اسـت و لـذا طبـق قضـیه‌ی قبل $G_f = S_5$. ازاین‌رو طبق قضیه‌ی۴ و نتیجه‌ی۱، $f(x)$ با رادیکال‌ها روی $\mathbb{Q}$ حـل‌پـذیر نیست.

□

رمز موفقیت این است که چیزهایی را بدانی که دیگران نمی‌دانند.

(ارسطو اوناسیس)

تمرین‌های سطح۱

۱- نشان دهید چند جملـه‌ای $f(x) = 2x^5 - 5x^4 + 5 \in \mathbb{Q}[x]$ بـا رادیکـال‌هـا روی $\mathbb{Q}$ حل‌پذیر نیست.

۲- مثالی از یک چندجمله‌ای درجه‌ی ۷ از $\mathbb{Q}[x]$ بزنید که با رادیکال‌ها روی $\mathbb{Q}$ حل‌پذیر نباشد.

۳-فرض کنید F یک میدان و $f(x), g(x) \in F[x]$. نشان دهید که $f(x)g(x)$ با رادیکال‌ها روی F حل‌پذیر است اگر و تنها اگر هر دوی $f(x)$ و $g(x)$ با رادیکال‌ها روی F حل‌پذیر باشد.

تمرین‌های سطح۲

۴- میدان‌های $F \subseteq E \subseteq K$ را بیابید به‌طوری‌که K یک توسیع رادیکال F باشد، ولی E یک توسیع رادیکال F نباشد.

۵-زیرگروه H از S_n را یک گروه **جایگشتی انتقالی** گوییم اگر برای هر $i, j \in \{1, 2, \ldots, n\}$ عنصر $\sigma \in H$ موجود باشد به‌قسمی که $\sigma(i) = j$.

(الف) فرض کنید p یک عدد اول و زیرگروه H از S_p یک گروه جایگشتی انتقالی باشد. اگر H دارای یک ترانهش باشد، ثابت کنید $H = S_p$.

(ب) فرض کنید F یک میدان و $f(x) \in F[x]$ دارای ریشه مکرر نباشد. ثابت کنید $f(x)$ روی F تحویل نا پذیر است اگر و فقط اگر G_f یک گروه جایگشتی انتقالی باشد.

تمرین‌های سطح ۳

۶- اگر $n \geq 5$ باشد، نشان دهید یک چند جمله‌ای حل ناپذیر از درجه‌ی n وجود دارد.

منابعی برای مطالعه‌ی بیشتر

۱. طائری، بیژن. **مبانی جبرمجرد**. انتشارات دانشگاه صنعتی اصفهان (۱۳۸۲).

۲. محمدی حسن آبادی، علی اکبر. **جبر**. انتشارات دانشگاه اصفهان (۱۳۷۲).

۳. نقی پور، علیرضا. **آشنایی با نظریه گروه‌ها و حلقه‌ها**. انتشارات دانشگاه شهرکرد (۱۳۸۷).

4. Artin, E. *Galois Theory.* 2nd ed., Notre Dame Press, 1959.

5. Garling, J. H. *A Course in Galois Theory.* Cambridge University Press, 1986.

6. Howie, J. M. *Fields and Galoies Theory*. Springer-Verlag, London, 2006.

7. Morandi, P. *Fields and Galoies Theory*. Springer-Verlag, New York, 1996.

8. Swallow, J. *Exploratory Galoies Theory*. Cambridge University Press, 2004.

فصل ۵

ترسیم‌پذیری n–ضلعی‌های منتظم

پیش بروید که فهم موضوع در پی شما خواهد آمد.

(دالامبر)

در این فصل می‌خوانیم:

مقدمه

در این فصل ابتدا مروری بر تعریف ریشه‌های واحد خواهیم داشت و سپس چندجمله‌ای‌های دایره‌بر را معرفی می‌کنیم. هدف اصلی ما در این فصل ارائه‌ی یک شرط لازم وکافی در مورد ترسیم پذیری یک $n-$ضلعی منتظم است که این مطلب در بخش دوم و در قالب قضیه‌ی گاوس ارائه خواهد شد.

۵-۱ چندجمله‌ای‌های دایره‌بر

تعریف۵-۱

فرض کنیم K یک میدان دلخواه و n عدد صحیح مثبتی باشد و $\zeta \in K$. دراین‌صورت ζ را n**امین ریشه‌ی واحد اولیه** نامند هرگاه $\zeta^n = 1$ و به ازای هر m که $1 \leq m < n$، $\zeta^m \neq 1$.

فرض کنیم K یک میدان باشد، $m \in \mathbb{N}$ و مشخصه‌ی K عدد m را عاد نکند. دراین‌صورت اگر $f(x) = x^m - 1$ باشد، آن‌گاه f و f' (مشتق f) هیچ ریشه‌ی مشترکی ندارند (لم ۳-۱ ملاحظه شود)، پس f دارای mریشه‌ی متمایز در یک میدان شکافنده‌ی Fاز f روی Kاست.

واضح است که مجموعه‌ی E از ریشه‌های f یک زیر گروه متناهی از گروه ضربی Fاست و ازاین‌رو طبق نتیجه‌ی ۳-۳، E یک گروه دوری است. یک مولد ζ_m از E یک ریشه‌ی m ام اولیه‌ی واحد است، پس عناصر ${\zeta_m}^1, {\zeta_m}^2, \ldots, {\zeta_m}^m$ متمایز است و برای هر $j = 1, 2, \ldots, m$، $({\zeta_m}^j)^m = ({\zeta_m}^m)^j = 1$.

چون Eمجموعه‌ی ریشه‌های fاست،

$$E = \{\zeta_m^j : \quad 1 \leq j \leq m\}$$

ازاین‌رو، توسیع $K(\zeta_m)$ یک میدان شکافنده‌ی f روی Kاست وآن را یک **توسیع دایره‌بر** از K می نامند.

اصطلاح دایره‌بر به تقسیم دایره اشاره می کند، چون دلالت بر موقعیت ریشه های mام واحد روی میدان اعداد گویای $\mathbb{Q}$ به عنوان نقاط دایره‌ی واحد در صفحه‌ی مختلط دارد.

اگر چه ζ_m ریشه‌ای از چندجمله‌ای $f(x)=x^m-1$ است، f روی K تحویل ناپذیر نیست (در واقع، چندجمله‌ای $x-1$ در $K[x]$ عاملی از f است). می‌خواهیم چندجمله‌ای مینیمال ζ_m را روی K بیابیم.

چون ζ_m یک ریشه‌ی mام اولیه واحد است، و مجموعه‌ی E، مجموعه‌ی ریشه‌های f است،

$$f(x)=x^m-1=\prod_{j=1}^{m}(x-\zeta_m^j).$$

برای هر j که $1\le j\le m$، مرتبه‌ی عنصر ζ_m^j در گروه ضربی F با استفاده از فرمول

$$\circ(\zeta_m^j)=\frac{m}{(j,m)}$$

به‌دست می‌آید. ازاین‌رو هر ریشه‌ی mام واحد یک ریشه‌ی dام اولیه واحد برای مقسوم علیه منحصر به فرد d از m خواهد بود. حال مجموعه‌ی ریشه‌های mام واحد را با به‌کارگیری مجموعه‌ی مقسوم علیه‌های d از m به عنوان مجموعه‌ی اندیس‌ها، افراز می کنیم. برای هر مقسوم علیه d از m، اگر فرض کنیم

$$E_d=\{\zeta_m^j : \zeta_m^j \text{ یک ریشه‌ی } d \text{ ام اولیه واحد است }\}$$

آن‌گاه

$$f(x)=x^m-1=\prod_{d|m}\Big(\prod_{\zeta_m^j\in E_d}(x-\zeta_m^j)\Big).$$

تعریف ۵-۲

فرض کنیم K یک میدان باشد، $n\in\mathbb{N}$ و مشخصه‌ی K عدد n را عاد نکند.
چندجمله‌ای دایره‌بر nام، $\Phi_n(x)$، را به‌صورت

$$\Phi_n(x)=\prod_{\zeta\in E_n}(x-\zeta)$$

تعریف می‌کنیم که در آن

$$E_n=\{\zeta : \zeta \text{ یک ریشه‌ی } n \text{ ام اولیه واحد است }\}.$$

مشاهده کنید که اکنون تجزیه‌ی زیر از چندجمله‌ای $f(x)=x^m-1$ را داریم

$$f(x)=x^m-1=\prod_{d|m}\Phi_d(x).$$

نشان می دهیم که اگر چه چندجمله‌ای $\Phi_n(x)$ برحسب ریشه‌های nام اولیه واحد تعریف می شود و این‌ها به طور کلی عناصر K نیست، $\Phi_n(x)\in K[x]$ و در واقع ضریب‌های $\Phi_n(x)$ در زیر میدان اول K قرار دارند.

قضیه ۵-۱

فرض کنیم $n\in\mathbb{N}$، K میدانی که مشخصه‌ی آن عدد n را عاد نمی‌کند و $\Phi_n(x)$ چندجمله‌ای دایره‌بر nام روی K باشد. دراین‌صورت موارد زیر برقرار است:

(۱) ضرایب $\Phi_n(x)$ در زیر میدان اول P از K قرار دارد. به‌خصوص اگر $K=\mathbb{Q}$ باشد ،ضرایب $\Phi_n(x)$ اعداد صحیح است،

(۲) $\deg(\Phi_n(x))=\phi(n)$، که در آن ϕ تابع ϕ-اویلر است.

اثبات: (۱) با توجه به مطالب بالا می‌دانیم

$$f(x)=x^n-1=\prod_{d|n}\Phi_d(x) \qquad (*)$$

اینک، استقر روی nرا به کار خواهیم برد. چون $\Phi_1(x)=x-1\in P[x]$، نتیجه برای $n=1$ درست است.

فرض کنیم نتیجه برای تمام $m<n$ درست باشد. قرار می‌دهیم:

$$S=\{d:1\le d<n,\ d\mid n\}$$

و

$$g(x)=\prod_{d\in S}\Phi_d(x)$$

بنابر فرض استقرا، $g(x)\in P[x]$ و براساس (*) و با به‌کارگیری الگوریتم تقسیم در $P[x]$ داریم

$$x^n-1=g(x)h(x)+r(x)$$

که $h(x),\ r(x)\in P[x]$ و $\deg r(x)<\deg g(x)$. از آن‌جا که $P[x]\subseteq F[x]$ (که در آن $F=K(\zeta_n)$)، می‌توان از یکتایی خارج قسمت و باقی‌مانده (با به‌کار گرفتن الگوریتم تقسیم در $F[x]$) نتیجه گرفت که $r=0$ و $\Phi_n(x)=h(x)\in P[x]$. اگر $K=\mathbb{Q}$، آن‌گاه از بحث استقرایی بالا می‌توان استفاده کرد. بنا به تمرین ۱، چون $x^n-1=g(x)\Phi_n(x)$ یک چندجمله‌ای تکین در $\mathbb{Z}[x]$ است، $\Phi_n(x)\in\mathbb{Z}[x]$.

(۲) اگر ζ_n یک ریشه‌ی nام اولیه‌ی واحد باشد و $1\le j\le n$، آن‌گاه ζ_n^j یک ریشه‌ی nام اولیه‌ی واحد است اگر و فقط اگر $(j,n)=1$. ازاین‌رو تعداد ریشه‌های nام اولیه‌ی واحد برابر $\phi(n)$است، یعنی تعداد اعداد صحیح بین 1 و n که نسبت به n اول است.

■■■

توجه کنید که چندجمله‌ای $\Phi_n(x)\in K[x]$ لزوماً روی K تحویل ناپذیر نیست. برای مثال، $\Phi_4(x)$ روی $\mathbb{Z}_5$ به‌صورت $x^2+\bar{1}=(x+\bar{2})(x+\bar{3})$ تجزیه می شود. اما نشان خواهیم داد که $\Phi_n(x)$ برای تمام $n\in\mathbb{N}$ روی $\mathbb{Q}$ تحویل‌ناپذیر است.

پیش از ارائه‌ی اثباتی برای این مطلب، به بیا ن‌لم‌های زیر می‌پردازیم. اگر $a\in\mathbb{Z}$، از علامت $\bar{a}$ برای نمایش تصویر a تحت همریختی طبیعی $\mathbb{Z}\to\mathbb{Z}_p$ استفاده می‌کنیم.

یادآوری: برای تمام $\bar{a}\in\mathbb{Z}_p$، $\bar{a}^p=\bar{a}$. هم‌چنین اگر $f(x)=\sum_{i=0}^{n}a_ix^i\in\mathbb{Z}[x]$، آن‌گاه $\overline{f}(x)\in\mathbb{Z}_p[x]$ را چنین تعریف می‌کنیم:

$$\overline{f}(x)=\sum_{i=0}^{n}\overline{a}_i x^i.$$

لم ۵-۱

فرض کنیم $f,g\in\mathbb{Z}[x]$ و p یک عدد اول باشد. موارد زیر در حلقه‌ی چندجمله‌ای $\mathbb{Z}_p[x]$ برقرار است.

(۱) $\overline{fg}=\overline{f}\,\overline{g}$،

(۲) $\overline{f+g}=\overline{f}+\overline{g}$،

(۳) اگر در $\mathbb{Z}[x]$، $f\mid g$، آن‌گاه در $\mathbb{Z}_p[x]$، $\overline{f}\mid\overline{g}$،

(۴) اگر در $\mathbb{Z}[x]$، f_p را با ضابطه‌ی $f_p(x)=f(x^p)$ تعریف کنیم، آن‌گاه $\overline{f}_p=(\overline{f})^p$.

اثبات: (۱) و (۲) و (۳) ساده است و به خواننده واگذار می‌شود.

(۴): اگر f چندجمله‌ای ثابت $f(x)=a_0$ باشد، آن‌گاه $\overline{f}_p(x)=\overline{a}_0=(\overline{a}_0)^p=(\overline{f}(x))^p$. فرض کنیم که نتیجه برای تمام چندجمله‌ای‌های از درجه‌ی کم‌تر از n برقرار و f دارای درجه‌ی n باشد. دراین‌صورت $f(x)=\sum_{i=0}^{n}a_i x^i$، جایی‌که $a_i\in\mathbb{Z}$ برای $0\le i\le n$. داریم:

$$\begin{aligned}(\overline{f}(x))^p&=(\sum_{i=0}^{n}\overline{a}_i x^i)^p\\&=((\sum_{i=0}^{n-1}\overline{a}_i x^i)+\overline{a}_n x^n)^p\\&=\sum_{i=0}^{p}\binom{p}{i}(\sum_{i=0}^{n-1}\overline{a}_i x^i)^{p-i}(\overline{a}_n x^n)^i\end{aligned}$$

$$
\begin{aligned}
&=(\sum_{i=0}^{n-1}\overline{a}_i x^i)^p+\overline{a}_{n^p}x^{pn}\\
&=(\sum_{i=0}^{n-1}\overline{a}_i x^{pi})+\overline{a}_n x^{pn}\\
&=\sum_{i=0}^{n}\overline{a}_i\left(x^p\right)^i\\
&=\overline{f}_p(x).
\end{aligned}
$$

■■■

لم ۵- ۱

اگر ζ یک ریشه‌ی mام اولیه‌ی واحد، f چندجمله‌ای مینیمال ζ روی $\mathbb{Q}$ و p عدد اولی باشد که عدد m را عاد نمی‌کند، آن‌گاه $f(\zeta^p)=0$.

اثبات: برهان خلف، فرض کنیم $f(\zeta^p)\neq 0$ باشد. می‌توان فرض کرد که $f(x)\in\mathbb{Z}[x]$ (رجوع کنید به نتیجه‌ی۱-۴). فرض کنیم g چندجمله‌ای مینیمال ζ^p روی $\mathbb{Q}$ باشد؛ بنابراین باز هم می‌توان فرض کرد که $g\in\mathbb{Z}[x]$. از این مطلب که $g\neq f$ استفاده می کنیم و نشان می دهیم که چندجمله‌ای $\overline{\Phi}_m(x)\in\mathbb{Z}_p[x]$ دارای ریشه‌ی تکراری است و ازاین‌رو با این فرض که p عدد m را عاد نمی کند، به تناقض می رسیم.

$g_p(x)\in\mathbb{Z}[x]$ را به‌صورت $g_p(x)=g(x^p)$ تعریف می‌کنیم. چون $g_p(\zeta)=g(\zeta^p)=0$ و f چندجمله‌ای منیمال ζ روی $\mathbb{Q}$ است، در $\mathbb{Q}[x]$، $f\mid g_p$. بنابراین در $\mathbb{Z}[x]$، $f\mid g_p$ (رجوع کنید به تمرین۱).

حال به حلقه‌ی چندجمله‌ای $\mathbb{Z}_p[x]$ مراجعه می‌کنیم. چون در $\mathbb{Z}[x]$ ، $f\mid g_p$، بنابه لم قبل، در $\mathbb{Z}_p[x]$ داریم $\overline{f}\mid\overline{g}_p$. فرض کنیم $\overline{h}$ یک عامل تحویل ناپذیر $\overline{f}$ در $\mathbb{Z}_p$ باشد. بر اساس قسمت (۴) لم قبل، $\overline{g}_p=(\overline{g})^p$. حال چون $\overline{h}\mid(\overline{g})^p$ و $\overline{h}$ در $\mathbb{Z}_p[x]$ تحویل ناپذیر است، پس در $\mathbb{Z}_p[x]$ داریم $\overline{h}\mid\overline{g}$.

از آن‌جا که $\Phi_m(\zeta)=0=\Phi_m(\zeta^p)$، f و g هر دو در $\mathbb{Q}[x]$، Φ_m را می شمارند. حال چون f و g چندجمله‌ای‌های تحویل ناپذیر متمایزی در $\mathbb{Q}[x]$ هستند، fg در $\mathbb{Q}[x]$، و ازاین‌رو در $\mathbb{Z}[x]$، Φ_mرا می شمارد. اما دراین‌صورت در $\mathbb{Z}_p[x]$، $\overline{\Phi}_m$ بر $\overline{h}^2$ تقسیم پذیر است و در نتیجه $\overline{\Phi}_m$ در $\mathbb{Z}_p$ دارای ریشه‌ی تکراری است. اما چون $\mathbb{Z}_p$از مشخصه‌ی pاست و m بر عدد p بخش پذیر نیست، چندجمله‌ای $x^m-\bar{1}$ و مشتق آن هیچ ریشه‌ی مشترکی ندارند.

ازاین‌رو چندجمله‌ای $x^m-\bar{1}$ دارای ریشه‌ی تکراری نیست. بنابراین چون $\overline{\Phi}m$ در $\mathbb{Z}_p[x]$ چندجمله‌ای $x^m-\bar{1}$ را می شمارد، به تناقض مورد نظر رسیده‌ایم. پس نتیجه برقرار است.

■■■

حال اثبات تحویل ناپذیر بودن $\Phi_n(x)$ برای تمام $n\in\mathbb{N}$ روی $\mathbb{Q}$ را ارائه می‌دهیم. در اثبات از این مطلب استفاده می‌کنیم که $\mathbb{Q}$ میدان کسرهای حوزه‌ی صحیح $\mathbb{Z}$ است و اگر p عدد اولی باشد، آن‌گاه حلقه‌ی چندجمله‌ای $\mathbb{Z}_p[x]$ در مواردی که در لم‌های قبل بیان شد، صدق می‌کند.

قضیه ۵-۲

فرض کنیم $m\in\mathbb{N}$ و

$E_m=\{\zeta:\ \zeta$ یک ریشه‌ی mام اولیه واحد است $\}$.

دراین‌صورت، چندجمله‌ای دایره‌بر mام روی $\mathbb{Q}$، یعنی

$$\Phi_m(x)=\prod_{\zeta\in E_m}(x-\zeta)$$

روی $\mathbb{Q}$تحویل ناپذیر است.

اثبات: فرض کنیم ζ یک ریشه‌ی mام واحد اولیه باشد و fچندجمله‌ای مینیمال ζ روی $\mathbb{Q}$ باشد، بنابراین طبق نتیجه‌ی۱-۴ ، $f\in\mathbb{Z}[x]$. نشان می‌دهیم که

$f = \Phi_m$، دراین‌صورت همان گونه که ادعا شد، نتیجه می‌گیریم که Φ_mروی $\mathbb{Q}$ تحویل‌ناپذیر است. برای این منظور کافی است نشان دهیم که اگر δ یک ریشه‌ی mام اولیه‌ی واحد باشد، آن‌گاه $f(\delta) = 0$.

اگر δ یک ریشه‌ی mام اولیه‌ی واحد باشد، آن‌گاه $\delta = \zeta^r$ که r نسبت به m اول است. پس برای $k \in \mathbb{N}$، r را می‌توان به‌صورت حاصل‌ضرب k عدد اول که هر کدام نسبت به mاول است، نوشت. با استقراء روی k ثابت می‌کنیم که $f(\delta) = 0$.

اگر $k = 1$، نتیجه بر اساس لم قبل به‌دست می آید. فرض کنیم که نتیجه برای $k = j$ درست باشد و r را به‌توان به‌صورت حاصل‌ضرب $j+1$ عدد اول نوشت، پس $r = np$ که n حاصل ضربی از j عدد اول، که هر کدام نسبت به m اول است و p عدد اولی است که عدد n را نمی شمارد (و نسبت به mاول است). بنا بر فرض استقرا، چون ζ^n یک ریشه‌ی mام اولیه‌ی واحد است، $f(\zeta^n) = 0$. اگر f_1 چندجمله‌ای مینیمال ζ^n روی $\mathbb{Q}$ باشد، آن‌گاه $f_1 \mid f$ (در $\mathbb{Z}[x]$).

حال بنا به لم قبل، چون ζ^n یک ریشه‌ی mام اولیه‌ی واحد است و $p \nmid m$، $f_1(\delta) = f_1(\zeta^r) = f_1\left((\zeta^n)^p\right) = 0$ و نتیجه به‌دست می‌آید.

■■■

قضیه ۵-۳

فرض کنیم F یک میدان باشد، m یک عدد طبیعی که بر مشخصه‌ی میدان F بخش پذیر نیست، $K = F(\zeta_m)$ و $G = \mathrm{Aut}_F^K$. دراین‌صورت موارد زیر برقرار است.

(۱) G با زیر گروهی از $\mathbb{Z}_m^*$ یکریخت است،

(۲) G با $\mathbb{Z}_m^*$ یکریخت است اگر و فقط اگر، Φ_mروی F تحویل ناپذیر باشد.

اثبات (۱): فرض کنیم f_m چندجمله‌ای مینیمال ζ_m روی F باشد. چون $\Phi_m(\zeta_m) = 0$، در $F[x]$ داریم $f_m \mid \Phi_m$. در نتیجه اگر δ ریشه‌ای از f_m باشد، آن‌گاه $\delta = \zeta_m^j$، برای عدد منحصر به فرد j که $1 \le j \le m$.

اگر $\tau \in G$، آن‌گاه τ به وسیله‌ی عملش روی ζ_m به‌صورت منحصر به فردی تعیین می‌شود و باید ζ_m را به ریشه‌ای از f_m تصویر کند. تابع $\theta : G \to \mathbb{Z}^*_m$ را با ضابطه‌ی $\theta(\tau) = \overline{j}$ به شرط آن‌که $\tau(\zeta_m) = \zeta_m^j$ تعریف کنیم. به راحتی می‌توان نشان داد که θ یک تکریختی گروه‌هاست.

(۲): همان گونه که در اثبات (۱) بیان کردیم، چندجمله‌ای مینیمال f_m از ζ_m روی F چندجمله‌ای Φ_m را می شمارد. چون $K = F(\zeta_m)$ یک میدان شکافنده روی F است، در نتیجه بنا به قضیه‌ی ۴-۳ روی F نرمال است، پس

$$o(G) = [K : F] = \deg(f_m).$$

بنا به (۱)، G با زیر گروهی از گروه ضربی $\mathbb{Z}^*_m$ یکریخت است، در نتیجه چون

$$o(\mathbb{Z}^*_m) = \phi(m) = \deg(\Phi_m)$$

پس G با گروه ضربی $\mathbb{Z}^*_m$ یکریخت است، اگر و فقط اگر $\deg(f_m) = \deg(\Phi_m)$، یعنی اگر و فقط اگر $f = \Phi_m$.

■■■

نتیجه ۵-۱

فرض کنیم $m \in \mathbb{N}$، ζ_m یک ریشه‌ی mام اولیه‌ی واحد روی $\mathbb{Q}$ و $K = \mathbb{Q}(\zeta_m)$ باشد. دراین‌صورت $\mathrm{Aut}^K_{\mathbb{Q}} \cong \mathbb{Z}^*_m$.

اثبات: به عنوا ن‌تمرین به عهده دانشجو واگذار می‌گردد.

■■■

در پایان این بخش توضیحاتی در مورد ریشه‌های واحد و چندجمله‌ای‌های دایره‌بر بیان می‌کنیم و در بخش بعد نتایج آن را مورد استفاده قرار خواهیم داد.

فرض کنیم p عددی اول باشد و ζ یک ریشه‌ی p ام اولیه‌ی واحد روی $\mathbb{Q}$، یعنی p کوچک‌ترین عدد صحیح مثبت است که $\zeta^p = 1$. عدد ζ را می‌توان با استفاده از فرمول اعداد مختلط به‌صورت زیر تعریف کرد:

$$\zeta = e^{2\pi i/p} = \cos(\frac{2\pi}{p}) + i\sin(\frac{2\pi}{p}).$$

اگر چه ζ در چندجمله‌ای $f(x) = x^p - 1 \in \mathbb{Q}[x]$ صدق می کند، f چندجمله‌ای مینیمال ζ روی $\mathbb{Q}$ نیست، چون f روی $\mathbb{Q}$ تحویل ناپذیر نیست. در واقع، f روی $\mathbb{Q}[x]$ به‌صورت زیر تجزیه می شود،

$$f(x) = (x-1)g(x)$$

که $g(x) = (x^{p-1} + x^{p-2} + \cdots + x + 1)$. پس چون ζ در چندجمله‌ای $x-1$ صدق نمی‌کند باید در $g(x)$ صدق کند. همان طور که در زیر نشان خواهیم داد $g(x)$ روی $\mathbb{Q}$ تحویل ناپذیر است.

ابتدا مشاهده می کنیم که

$$g(x) = \frac{x^p - 1}{x-1}.$$

عنصر جدید $h \in \mathbb{Q}[x]$ را به‌صورت $h(x) = g(x+1)$ تعریف می‌کنیم. برای $j = 1,2,\ldots,p-1$، فرض کنیم b_jها ضرایب دوجمله‌ای، یعنی $\binom{p}{j}$ها باشد و توجه داشته باشید که $p \mid b_j$ برای $1 \le j < p$.

دراین‌صورت

$$\begin{aligned} h(x) = \frac{(x+1)^p - 1}{x} &= x^{-1}(x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x) \\ &= x^{-1}(x^p + b_{p-1}x^{p-1} + \cdots + b_j x^j + \cdots + b_1 x) \\ &= x^{p-1} + b_{p-1}x^{p-2} + \cdots + b_j x^{j-1} + \cdots + b_1. \end{aligned}$$

حال با به‌کارگیری محک آیزنشتاین نتیجه می‌گیریم که $h(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

سرانجام اگر عناصر $k(x), w(x) \in \mathbb{Q}[x]$ از درجه‌ی مثبت باشند که $g(x) = k(x)w(x)$، آن‌گاه $k(x+1)$ و $w(x+1)$ نیز از درجه‌ی مثبت‌اند و $h(x) = k(x+1)w(x+1)$، که با تحویل ناپذیر بودن $h(x)$ در تناقض است. پس $g(x)$ روی $\mathbb{Q}[x]$ تحویل ناپذیر است.

ازاین‌رو ζ روی $\mathbb{Q}$ جبری با چندجمله‌ای مینیمال $g(x)$ از درجه‌ی $p-1$ است. پس

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = p-1$$

و $\{1, \zeta, \ldots, \zeta^{p-2}\}$ یک پایه برای $\mathbb{Q}(\zeta)$ روی $\mathbb{Q}$ است.

تمرین‌های سطح ۱

۱- فرض کنید $h(x) \in \mathbb{Q}[x]$ و چندجمله‌ای های تکین $f(x), g(x) \in \mathbb{Z}[x]$ باشند به‌طوری‌که $f = gh$. دراین‌صورت نشان دهید $h(x) \in \mathbb{Z}[x]$.

۲- مقادیر $\Phi_n(x)$ را برای $1 \leq n \leq 5$ به دست آورید.

۴- فرض کنید n عدد طبیعی بزرگ‌تر از 2 باشد.

(الف) ثابت کنید $\zeta_n^{-1} = \zeta_n^{n-1}$.

(ب) ثابت کنید $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \dfrac{\phi(n)}{2}$.

(پ) میدان میانی از $\mathbb{Q}(\zeta_{11})$ را روی $\mathbb{Q}$ بیابید که $[E : \mathbb{Q}] = 5$.

۵- فرض کنید n یک عدد طبیعی بزرگ‌تر از 1 باشد. ثابت کنید اگر $E = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ آن‌گاه E یک میدان میانی $\mathbb{Q}$ و $\mathbb{R}$ است.

تمرین‌های سطح ۲

۶- ثابت کنید، اگر ζ یک ریشه‌ی nام اولیه‌ی واحد باشد، آن‌گاه مجموعه‌ی $\{1,\zeta,...,\zeta^{n-1}\}$ یک پایه برای $\mathbb{Q}(\zeta)$ روی $\mathbb{Q}$ تشکیل می دهد، اگر و تنها اگر n خالی از مربع باشد(یعنی nبر مربع هیچ عدد اولی تقسیم پذیر نباشد.).

۷- اگر pاول باشد، نشان دهید

$$\Phi_{p^n}(x) = 1 + x^q + x^{2q} + \cdots + x^{(p-1)q},$$

که در آن $q = p^{n-1}$ است.

۸- اگر $n \geq 3$فرد باشد، نشان دهید که $\Phi_{2n}(x) = \Phi_n(-x)$. (راهنمایی: $\Phi_2(x) = -\Phi_1(-x)$)

تمرین‌های سطح ۳

۹-تابع موبیوس[1] $\mu : \mathbb{Z}^+ \to \{0,1,-1\}$ به‌صورت زیر تعریف می‌شود:

$$\mu(n) = \begin{cases} 1 & \text{اگر } n = 1 \\ (-1)^k & \text{اگر } n \text{ حاصل‌ضرب } k \text{ عدد اول متمایزباشد} \\ 0 & \text{اگر به ازای عدد اولی مانند } p \text{، } p^2 \mid n \end{cases}$$

(الف) نشان دهید که

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{اگر } n = 1 \\ 0 & \text{اگر } n > 1 \end{cases}$$

[1] Moebius Function

(ب) نشان دهید $\phi(n)=\sum_{d|n} d\mu(n/d)$، که در آن ϕ تابع اویلر است.

۱۰- (الف) فرض کنید $\alpha:\mathbb{Z}^+\to\mathbb{Z}^+$ و $\beta:\mathbb{Z}^+\to\mathbb{Z}^+$ توابعی باشند که با $\alpha(n)=\sum_{d|n}\beta(d)$ به‌هم مربوط شده باشند. نشان دهید که β بر حسب α به‌صورت زیر داده می شود.

$$\beta(n)=\sum_{d|n}\mu[n/d]\alpha(d)=\sum_{d|n}\mu(d)\alpha[n/d]$$

که آن را فرمول انعکاس موبیوس می نامند. (راهنمایی:
$d\mid n \Leftrightarrow d\mid(n/c),\ c\mid(n/d),\ c\mid n$.)

(ب) ثابت کنید $\Phi_n(x)=\prod_{d|n}(x^d-1)^{\mu(n/d)}$، که در آن μ تابع موبیوس است.

۱۱- فرض کنید $n=p_1^{n_1}p_2^{n_2}...p_r^{n_r}$ که در آن p_iها اعداد اول متمایزی‌اند و $m=p_1p_2...p_r$. نشان دهید که $\Phi_n(x)=\Phi_m(x^{n/m})$.

۱۲- اگر p یک عدد اول فرد بوده و p، nرا عاد نکند، نشان دهید که

$$\Phi_{np}(x).\Phi_n(x)=\Phi_n(x^p).$$

۵-۲ قضیه‌ی گاوس

قبل از بیان قضیه‌ی گاوس، تعریف اعداد اول فرما را یادآوری می‌کنیم.

یادآوری: هر عدد اول به شکل 2^m+1 (که $m\in\mathbb{N}$) یک عدد اول فرما نام دارد.
نخستین پنج عدد اول فرما عبارتند از

۳، ۵، ۱۷، ۲۵۷ و ۶۵۵۳۷

❖ **تذکر:** در حقیقت اعداد اول فرما به‌صورت $2^{2^m}+1$ (که $m \in \mathbb{N}_0$) هستند. (تمرین۴ را ملاحظه کنید).

قضیه ۵-۵

فرض کنیم $n \in \mathbb{N}$، $n \geq 3$، و ζ_n یک ریشه‌ی nام اولیه‌ی واحد باشد. دراین‌صورت n-ضلعی منتظم ترسیم‌پذیر است، اگر و فقط اگر $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ توانی از 2 باشد.

اثبات: با توجه به مطالب بیان شده در بخش ۲-۲، n-ضلعی منتظم ترسیم‌پذیر است اگر و تنها اگر $\cos(2\pi/n) \in \mathcal{C}$.

یادآوری می‌کنیم چون میدان اعداد مختلط $\mathbb{C}$ مورد نظر است پس

$$\zeta_n = e^{(2\pi/n)i} = \cos(2\pi/n) + i\sin(2\pi/n)$$

و ازاین‌رو

$$(\zeta_n)^{-1} = e^{-(2\pi/n)i} = \cos(2\pi/n) - i\sin(2\pi/n)$$

پس

$$(\zeta_n)^{-1} + \zeta_n = 2\cos(2\pi/n) \qquad (*)$$

در نتیجه $\cos(2\pi/n) \in \mathbb{Q}(\zeta_n)$. حال با توجه به این‌که $\mathbb{Q}(\zeta_n)$ توسیعی از $\mathbb{Q}(\cos(2\pi/n))$ و $\mathbb{Q}(\cos(2\pi/n))$ توسیعی از $\mathbb{Q}$ است، داریم

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(2\pi/n))][\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}]$$

حال با ضرب کردن $(*)$ در ζ_n داریم $\zeta_n{}^2 + 1 = 2\cos(2\pi/n)\zeta_n$. ازاین‌رو ζ_n در چندجمله‌ای $f(x) = x^2 - 2\cos(2\pi/n)x + 1 \in \mathbb{Q}(\cos(2\pi/n))[x]$ صدق می‌کند و در نتیجه

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(2\pi/n))] = 1 \text{ یا } 2$$

حال یک بار دیگر توسیع $\mathbb{Q}(\zeta_n)$ از $\mathbb{Q}(\cos(2\pi/n))$ و توسیع $\mathbb{Q}(\cos(2\pi/n))$ از $\mathbb{Q}$ را در نظر می‌گیریم. اگر $\cos(2\pi/n)$ ترسیم پذیر باشد آن‌گاه $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}]$ توانی از 2 است و در نتیجه $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ باید توانی از 2 باشد.

بر عکس، اگر $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ توانی از 2 باشد، آن‌گاه چون $\mathbb{Q}(\zeta_n)$ یک توسیع نرمال از $\mathbb{Q}$ است براساس قضیه ۳-۹، نتیجه می‌گیریم که $\mathcal{C}$ میدانی حاوی $\mathbb{Q}(\zeta_n)$ است. ازاین‌رو چون $\cos(2\pi/n)\in\mathbb{Q}(\zeta_n)$، پس $\cos(2\pi/n)\in\mathcal{C}$.

■■■

نتیجه ۵ –۲

فرض کنیم p عدد اول فردی باشد. دراین‌صورت p -ضلعی منتظم ترسیم پذیر است اگر و فقط اگر، $p=2^m+1$ برای $m\in\mathbb{N}$.

اثبات: چون p اول است، $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=p-1$ (طبق آخرین مطلب بیان شده در بخش اول این فصل). بنابراین نتیجه از قضیه اخیر به‌دست می‌آید. ■

اکنون می‌توانیم بحث خود را با ترسیم‌پذیری یک چندضلعی منتظم با n ضلع پایان دهیم.
از تحویل ناپذیری چندجمله‌ای دایره‌بر $\Phi_n(x)$ روی $\mathbb{Q}$ استفاده می‌کنیم تا n هایی از $\mathbb{N}$ را که یک n -ضلعی منتظم ترسیم پذیر است به طور کامل مشخص کنیم.

قضیه ۵ – ۶

فرض کنیم p عددی اول باشد، $k\in\mathbb{N}$ و $n=p^k$، $n\geq 3$. دراین‌صورت n -ضلعی منتظم ترسیم‌پذیر است اگر و فقط اگر، یکی از دو شرط زیر برقرار باشد:

(۱) $p=2$ و k دلخواه باشد.

(۲) $p=2^m+1$ که $m\in\mathbb{N}$ و $k=1$ باشد (یعنی، n یک عدد اول فرماست)

اثبات: فرض کنیم ζ_n یک ریشه‌ی n ام اولیه‌ی واحد روی $\mathbb{Q}$ باشد. بنا به قضیه‌ی ۵، n -ضلعی منتظم ترسیم‌پذیر است اگر و تنها اگر، $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ توانی از 2 باشد. حال با توجه به قضیه‌ی۲ و این که $n=p^k$ است، فرمول زیر به‌دست می‌آید

$$[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\deg(\Phi_n(x))=\phi(n)=p^{k-1}(p-1)$$

اگر $p=2$، آن‌گاه $p^{k-1}(p-1)$ برای هر $k\in\mathbb{N}$، توانی از 2 است و ازاین‌رو یک چندضلعی منتظم با $n=2^k$ ضلع ترسیم پذیر است.
فرض کنیم $p\neq 2$. دراین‌صورت $p^{k-1}(p-1)$ توانی از 2 است اگر و تنها اگر $k=1$ و $p-1=2^m$ برای عنصر $m\in\mathbb{N}$، یعنی اگر و فقط اگر برای عنصری مثل $m\in\mathbb{N}$، $p=2^m+1$ باشد.

■■■

قضیه ۵ – ۷ (قضیه گاوس)

n –ضلعی منتظم ترسیم‌پذیر است اگر و فقط اگر $n=2^{\alpha}p_1p_2...p_{\beta}$ که در آن α,β اعداد صحیح نامنفی و p_i ها اعداد اول متمایز فرما باشند.

اثبات: از نتیجه‌ی ۲ – ۶ و قضیه‌ی قبل به راحتی به‌دست می آید.

■■■

من می‌خواهم مسئله‌ای را حل کنم، نه به این علت که نفعی برای بشریت خواهد داشت.

(دانیل گورنشتاین)

تمرین‌های سطح۱

۱– اولین 40 مقدار n، $n\geq 3$ به‌طوری‌که n – ضلعی منتظم ترسیم پذیر است را بیابید.

۲– فرض کنید n یک عدد طبیعی باشد. ثابت کنید که یک زاویه به اندازه‌ی $2\pi/n$ را می‌توان تثلیث نمود اگر و تنها اگر $\phi(3n)=2^k$ باشد، به ازای $k\in\mathbb{N}\cup\{0\}$.

۳-آیا با خط‌کش و پرگار می‌توان یک زاویه‌ی 60°را به پنج قسمت مساوی تقسیم کرد (تمرین ۵ ملاحظه شود).

تمرین‌های سطح۲

۴- فرض کنید $n = 2^m + 1$عددی اول باشد. ثابت کنید mتوانی از 2 است.

تمرین‌های سطح۳

۵- ثابت کنید که در حالت کلی تقسیم یک زاویه‌ی دلخواه به پنج قسمت مساوی با استفاده خط‌کش و پرگار غیر ممکن است.

۶- شرط لازم و کافی برای عدد گویای αبیابید به‌طوری‌که زاویه‌ی αترسیم‌پذیر باشد.

منابعی برای مطالعه‌ی بیشتر

۱. فنریک، مارین. اچ. **مقدمه‌ای بر تناظر گالوا**. ترجمه‌ی شریف، حبیب. انتشارات دانشگاه شیراز (۱۳۸۰).

2. Bhattacharya, P.B., Jain, S. K., Nagpaul, S. R. *Basic Abstract Algebra* Cambridge University Press, 1994.

3. Herstein, I. N. *Topics in Algebra*. New York, Blaisdell, 1984.

4. Howie, J. M. *Fields and Galoies Theory*. Springer-Verlag, London, 2006.

فصل ۶

مباحث ویژه

جبر، یک ابزار ذهنی است که خلق شده تا مفاهیم کمّی جهان را بـه‌وضـوح ارائه کند.

(آلفرد نورث وایتهد)

در این قسمت می‌خوانیم:

مقدمه

در این فصل، ابتدا به اثبات قضیه‌ی اول سیلو می‌پردازیم. در بخش دوم، چند اثبات متنوع از قضیه‌ی اساسی جبر مطرح می‌کنیم. در بخش سوم، اثبات‌های بسیار ساده‌ای برای متعالی بودن عدد لیوویل و اعداد e و π بیان می‌کنیم. در بخش چهارم، به حل معادلات درجه‌ی پایین؛ یعنی درجه‌ی ۲و۳و۴، خواهیم پرداخت. در بخش پنجم، اثبات

قضیه‌ی معروف ودربورن مطرح می‌گردد. در بخش ششم، حلقه‌ای مثال می‌زنیم که دامنه‌ی ایده‌آل اصلی بوده، ولی دامنه‌ی اقلیدسی نیست. در نهایت، با ترسیم ۱۷-ضلعی منتظم، این فصل را به پایان می‌رسانیم.

۶-۱ اثبات ساده‌ای از قضیه‌ی اول سیلو

در این بخش به ارائه‌ی اثبات ساده‌ای از **قضیه‌ی اول سیلو**[1] که به مهم‌ترین قضیه‌ی گروه‌های متناهی مشهور است، می‌پردازیم.

قضیه۶-۱ (قضیه اول سیلو)

فرض کنیم p عددی اول و G گروهی از مرتبه‌ی $p^\alpha m$ باشد. دراین‌صورت G دارای زیرگروهی از مرتبه‌ی p^α است.

اثبات: فرض کنیم p^r بزرگ‌ترین توانی از p باشد که $p^r \mid m$. فرض کنیم Ω خانواده‌ی همه‌ی زیرمجموعه‌های p^α عنصری از G باشد. دراین‌صورت $|\Omega| = \binom{p^\alpha m}{p^\alpha}$. با توجه به انتخاب r داریم $p^{r+1} \nmid m$ و در نتیجه به‌وضوح $p^{r+1} \nmid |\Omega|$. با فرض $A, B \in \Omega$، تعریف می‌کنیم:

$$A \sim B \Leftrightarrow \text{عنصر } g \in G \text{ موجود باشد به‌طوری‌که } A = gB$$

به‌آسانی می‌توان نشان داد که "$\sim$" یک رابطه‌ی هم‌ارزی روی Ω بوده و اگر این رابطه‌ی هم‌ارزی Ω را به دسته‌های هم‌ارزی $\overline{M}_1, \ldots, \overline{M}_n$ افراز کند (شکل۶-۱)، آن‌گاه برای هر $1 \le i \le n$ خواهیم داشت

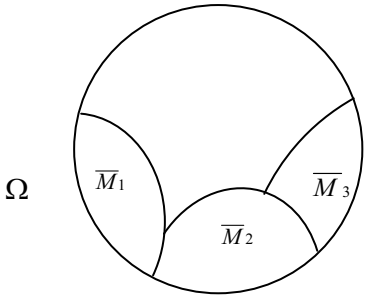
$$\left|\overline{M}_i\right|\left|H_i\right| = |G| = p^\alpha m, \qquad (*)$$

[1] First Sylow Theorem

جایی‌که $H_i = \{g \in G \mid gM_i = M_i\}$ زیرگروهی از G است. چون اجتماع عناصر هر دسته‌ی هم‌ارزی برابر G است، پس برای هر $1 \le i \le n$، $\left|\overline{M}_i\right| \ge m$. حال اگر برای هر $1 \le i \le n$، $\left|\overline{M}_i\right| > m$، آن‌گاه $p^{r+1} \mid \left|\overline{M}_i\right|$ (زیرا با فرض $p^{r+1} \nmid |\overline{M}_i|$، داریم $p^{\alpha} \mid \left|H_i\right|$ و در نتیجه $p^{\alpha} \le \left|H_i\right|$. ازاین‌رو با توجه به (*)، $\left|\overline{M}_i\right| \le m$، که تناقض است). بنابراین

$$p^{r+1} \mid \left|\overline{M}_1\right| + \cdots + \left|\overline{M}_n\right| = |\Omega|,$$

که متناقض با فرض است. پس $1 \le i \le n$ موجود است به‌طوری‌که $\left|\overline{M}_i\right| = m$ و لذا طبق (*) خواهیم داشت $\left|H_i\right| = p^{\alpha}$؛ یعنی H_i همان زیرگروه مورد نظر است. بدین ترتیب اثبات قضیه تمام است.



شکل ۶-۱

■■■

از قضیه‌ی اول سیلو به آسانی نتیجه‌ی زیر که به **قضیه‌ی کوشی**[1] معروف است، به‌دست می‌آید.

نتیجه۶-۱ (قضیه‌ی کوشی)

فرض کنیم G یک گروه متناهی و p عددی اول باشد که $p \mid |G|$. دراین‌صورت G داری عنصری از مرتبه‌ی p است.

[1] Cauchy's Theorem

۶-۲ اثبات قضیه‌ی اساسی جبر

قضیه‌ی اساسی جبر تاکنون به کمک روش‌های متنوعی به اثبات رسیده است. گاوس اولین کسی بود که این قضیه را به ۵ روش مختلف اثبات نمود. در این بخش این قضیه را به سه روش مختلف ثابت می‌کنیم.

قضیه ۶-۲(قضیه‌ی اساسی جبر)

هر چند جمله‌ای غیر ثابت با ضرایب مختلط، ریشه دارد.

اثبات اول (قضیه‌ی اساسی جبر): فرض کنیم

$$P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$$

یک چند جمله‌ای با ضرایب مختلط باشد که $n \geq 1$ و P دارای هیچ ریشه‌ای نباشد. تعریف می‌کنیم:

$$f(t,x) = \frac{1}{P(te^{ix})} \qquad (۱)$$

با توجه به این‌که مخرج صفر نمی شود، $f(t,x)$ روی $\mathbb{R}\times\mathbb{R}$ به‌طور پیوسته مشتق پذیر است. تعریف می‌کنیم

$$F(t) = \int_0^{2\pi} f(t,x)dx \qquad (۲)$$

دراین‌صورت خواهیم داشت

$$F'(t) = \int_0^{2\pi} \partial_t f(t,x)dx$$

ادعا می کنیم $F' = 0$ که نشان می‌دهد F ثابت است. داریم

$$\partial_t f(t,x) = -\frac{nt^{n-1}e^{inx} + \cdots + a_1 e^{ix}}{(t^n e^{inx} + \cdots + a_1 te^{ix} + a_0)^2},$$

$$\partial_x f(t,x) = -\frac{t^n e^{inx}.in + \cdots + a_1 t e^{ix}.i}{\left(t^n e^{inx} + \cdots + a_1 t e^{ix} + a_0\right)^2} = it\partial_t f(t,x).$$

بنابراین

$$F'(t) = \frac{1}{it}\int_0^{2\pi} \partial_x f(t,x)dx = \frac{1}{it} f(t,x)\,|_{x=0}^{x=2\pi} = \frac{1}{it}\left[\frac{1}{P(te^{i2\pi})} - \frac{1}{P(te^{i0})}\right] = 0,$$

لذا F ثابت است. با قرار دادن $t=0$ در رابطه‌ی (۲) داریم

$$F(0) = \int_0^{2\pi} f(0,x)dx = \int_0^{2\pi} \frac{1}{P(0)}\,dx = \frac{2\pi}{P(0)}.$$

بنابراین F یک ثابت غیر صفر است. اما رابطه‌ی (۱) نشان می‌دهد که $\lim_{t\to\infty} F(t) = 0$. این نشان می‌دهد که F بایستی ثابت صفر باشد، که یک تناقض است؛ ازاین‌رو، فرض ریشه دار نبودن P خلاف است.

■■■

یک اثبات برای قضیه اساسی جبر به کار بردن قضیه‌ی لیوویل (در توابع مختلط) است که از قضیه‌ی کوشی نتیجه می شود، که با تغییر می تواند از قضیه‌ی گرین سرچشمه گیرد. برای مثال، کتاب زیبای

Fine, B and Rosenberger, G. *The Fundamental Theorem of Algebra*, Springer-Verlag, New York, 1997.

را ببینید. اکنون اثباتی از مرجع

Loya, P. Green's theorem and the fundamental theorem of algebra. Amer. Math. Monthly 110(2003), no. 10, 944-946.

برای قضیه‌ی اساسی جبر مطرح می‌کنیم که در آن فقط از قضیه‌ی گرین (در حساب دیفرانسیل و انتگرال) استفاده شده است. در حقیقت این اثبات از توپولوژی و نظریه‌ی توابع تحلیلی استفاده نمی‌کند.

اثبات دوم (قضیه‌ی اساسی جبر به کمک قضیه گرین):

فرض کنیم $p(w)$ یک چندجمله‌ای از $w = x + iy$ و از درجه‌ی $n \geq 1$ با ضرایب مختلط باشد. نشان می‌دهیم که $p(w)$ باید یک صفر داشته باشد. به طور معمول برهان خلف را به‌کار می بریم. فرض کنیم که $p(w)$ به ازای هیچ w ای صفر نشود، بنابراین $f(x,y) = \ln|p(x+iy)|$ یک تابع هموار از (x,y) در $\mathbb{R}^2$ است. برای $r > 0$، D_r را قرص به شعاع r و مرکز مبداء می‌گیریم و فرض کنیم C_r مرز D_r در جهت خلاف عقربه‌های ساعت باشد. دو طرف فرمول گرین؛ یعنی

$$\int_{C_r} P dx + Q dy = \iint_{D_r} (\partial_x Q - \partial_y P) dx dy, \qquad (1)$$

با $P = -\partial_y f$ و $Q = \partial_x f$ را بررسی می‌کنیم. ابتدا سمت راست، را می‌یابیم.

در حقیقت، نشان می‌دهیم که سمت راست برابر صفر است. توجه کنید که $\partial_x Q - \partial_y P = \partial_x^2 f + \partial_y^2 f$. ازآن‌جایی‌که $f(x,y) = (1/2)\ln|p(x+iy)|^2$، داریم:

$$\begin{cases} \partial_x f = \dfrac{1}{2} \dfrac{\partial_x |p(x+iy)|^2}{|p(x+iy)|^2} \\ \partial_y f = \dfrac{1}{2} \dfrac{\partial_y |p(x+iy)|^2}{|p(x+iy)|^2} \end{cases} \qquad (2)$$

بنابراین

$$\begin{cases} \partial_x^2 f = \dfrac{1}{2}\dfrac{\partial_x^2 |p|^2}{|p|^2} - \dfrac{1}{2}\dfrac{(\partial_x |p|^2)^2}{|p|^4} \\ \partial_y^2 f = \dfrac{1}{2}\dfrac{\partial_y^2 |p|^2}{|p|^2} - \dfrac{1}{2}\dfrac{(\partial_y |p|^2)^2}{|p|^4} \end{cases} \qquad (3)$$

حکم می‌کنیم کـه $\partial_y p = i\partial_x p$ و $\partial_y \overline{p} = -i\partial_x \overline{p}$. در واقـع، بـا اسـتفاده از خاصـیت خطی مشتق‌ها، اثبات این تساوی‌ها برای $q = (x+iy)^k$ کفایت می‌کند. در ایـن حالـت بـا اسـتفاده از قضـیه‌ی بسـط دو جملـه‌ای، $q = \sum_{l=0}^{k} \binom{k}{l} x^{k-l} i^l y^l$. ازایـن‌رو $\partial_y q = \sum_{l=1}^{k} \binom{k}{l} l x^{k-1} i^l y^{l-1}$. قرار می‌دهیم $l = j+1$، با توجه به اینکه

$$\binom{k}{j+1}(j+1) = \binom{k}{j}(k-j)$$

به‌دست می‌آوریم

$$\partial_y q = \sum_{j=0}^{k-1} \binom{k}{j}(k-j) x^{k-j-1} i^{j+1} y^j ,$$

که دقیقاً $i\partial_x q$ است. دومین برابری به طریق مشـابه و یـا بـا قـرار دادن مـزدوج اعـداد مختلط در برابری اول، اثبات مـی‌شـود. حـال ایـن برابـری هـا و قاعـده لایبنیـز را روی $|p|^2 = p\overline{p}$ به کار می‌بریم، خواننده می‌تواند با یـک محاسـبه‌ی مسـتقیم معـادلات بـه دسـت آمـده‌ی $\partial_x^2 f$, $\partial_y^2 f$ در (3) را بـه کـار بـرده و ثابـت کنـد $\partial_x^2 f = \partial_y^2 f$. پـس $\partial_x Q - \partial_y P = 0$ و بنابراین سمت راست (1) برابر صفر است.

حال سمت چپ (1) را محاسبه می کنیم. بدون کاسته شدن از کلیت، فـرض مـی کنـیم ضریب پیشرو $p(w)$ برابر 1باشد. بنابراین $p(x+iy)$ به‌صـورت $(x+iy)^n$بـه اضـافه‌ی یک چندجمله‌ای از $(x+iy)$ حداکثر از درجه‌ی $n-1$ است. ازاین‌رو می‌نویسیم

$$|p(x+iy)|^2 = p(x+iy)\overline{p(x+iy)} = (x^2+y^2)^n + \tilde{p}(x,y), \qquad (4)$$

جایی‌که $\tilde{p}(x,y)$ یک چندجمله‌ای با متغیرهای x,y و حداکثر از درجه‌ی $2n-1$ است. با گرفتن مشتقات جزئی از $|p(x+iy)|^2=(x^2+y^2)^n+\tilde{p}(x,y)$ نسبت به x,y و قرار دادن نتایج در (2) به دست می‌آوریم

$$P=-\partial_y f=-\frac{ny}{x^2+y^2}+\tilde{P},\quad Q=\partial_x f=\frac{nx}{x^2+y^2}+\tilde{Q}$$

جایی‌که

$$\tilde{P}=-\frac{(x^2+y^2)\partial_y\tilde{p}(x,y)-2ny\tilde{p}(x,y)}{2|p(x+iy)|^2(x^2+y^2)},$$
$$\tilde{Q}=\frac{(x^2+y^2)\partial_x\tilde{p}(x,y)-2nx\tilde{p}(x,y)}{2|p(x+iy)|^2(x^2+y^2)}.$$

با به کار بردن منحنی $c_r(t)=(r\cos t,r\sin t)$ ، که C_r را برای $0\le t\le 2\pi$ طی می‌کند، یک محاسبه مستقیم به‌دست می‌دهد

$$\int_{C_r}\frac{-ny}{x^2+y^2}dx+\frac{nx}{x^2+y^2}dy=2\pi n.$$

بنابراین

$$\int_{C_r}Pdx+Qdy=2\pi n+g(r),\qquad(5)$$

جایی‌که

$$g(r)=\int_{C_r}\tilde{P}dx+\tilde{Q}dy.$$

$g(r)$ را به صورت زیر بررسی می‌کنیم.

ازآن‌جایی که $\tilde{p}(x,y)$ یک چندجمله‌ای از x,y و حداکثر از درجه‌ی $2n-1$ است، $\partial_x\tilde{p}(x,y),\ \partial_y\tilde{p}(x,y)$ چندجمله‌ای‌هایی از x,y و حداکثر از درجه‌ی $2n-2$ هستند. ازاین‌رو صورت‌های $\tilde{P},\tilde{Q}$ چندجمله‌ای‌هایی از x,y و حداکثر از درجه‌ی $2n$

هستند. به‌عنوان یک نتیجه، قدرمطلق این صورت‌ها به حاصل‌ضرب یک ثابت در $(x^2+y^2)^n$ کراندار هستند. ازآن‌جایی که $\tilde{Q},\tilde{P}$ در مخرج هایشان شامل $|p(x+iy)|^2\ (x^2+y^2)$ هستند، با توجه به (4) نتیجه می‌شود که $|\tilde{P}|,|\tilde{Q}|$ هر یک به حاصل‌ضرب یک ثابت در $(x^2+y^2)^{-1}$ کراندارند. این تخمین‌ها روی $|\tilde{P}|,|\tilde{Q}|$ نتیجه می‌دهد که $|g(r)|$ به حاصل‌ضرب یک ثابت در r^{-1} کراندار است. ازآن‌جایی که نشان داده شد، سمت راست (1) برابر صفر است، با میل دادن $r\to\infty$ در (5)، تناقض $2\pi n=0$ به‌دست می‌آید. بنابراین فرض این‌که $p(w)$ دارای صفر نیست، باطل می‌شود.

■■■

همان‌طوری که دیدیم، قضیه‌ی اساسی جبر، یک قضیه‌ی جبری نیست و اثبات آن احتیاج به مباحث آنالیزی دارد. این بخش را با ارائه‌ی برهانی از این قضیه که در آن مباحث آنالیزی به حداقل رسیده و در حقیقت کاربردی از نظریه‌ی گالواست به پایان می‌رسانیم.

ابتدا لم زیر را بیان می‌کنیم (متذکر می‌شویم که در اثبات این لم فقط از قضیه‌ی مقدار میانی استفاده شده است).

لم۶-۱

(الف) فرض کنیم $f(x)\in\mathbb{R}[x]$ از درجه‌ی فرد باشد. دراین‌صورت $f(x)$ دارای ریشه‌ای در $\mathbb{R}$ است،

(ب) هر عدد حقیقی مثبت دارای ریشه‌ی دوم حقیقی است،

(ج) هر عدد مختلط دارای ریشه‌ی دوم مختلط است.

اثبات (الف): فرض کنیم $f(x) = a_0 + a_1 + \cdots + a_n x^n$، که $a_n \neq 0$ و n یک عدد طبیعی فرد است. بدون این‌که از کلیت کاسته شود می‌توان فرض کرد $a_n > 0$ (زیرا ریشه‌های $f(x)$ و $-f(x)$ یکسانند). دراین‌صورت، داریم

$$\lim_{x\to\pm\infty} f(x) = \lim_{x\to\pm\infty} x^n(\frac{a_0}{x^n} + \cdots + \frac{a_{n-1}}{x} + a_n) = \lim_{x\to\pm\infty} x^n a_n = \pm\infty.$$

بنابراین طبق تعریف حد، عدد حقیقی مثبت $a \in \mathbb{R}$ موجود است به‌طوری‌که برای هر $x > a$، $f(x) > 0$ و برای هر $x < a$، $f(x) < 0$.

در نتیجه طبق قضیه‌ی مقدار میانی نقطه‌ی $c \in \mathbb{R}$ موجود است به‌قسمی که $f(c) = 0$.

(ب): فرض کنیم $a > 0$. دراین‌صورت، چندجمله‌ای $f(x) = x^2 - a$ به ازای مقادیر بزرگ x، مثبت است و به ازای $x = 0$، منفی است. در نتیجه طبق قضیه‌ی مقدار میانی نقطه‌ی $c \in \mathbb{R}$ موجود است به‌قسمی که $c^2 = a$.

(ج): فرض کنیم $z = a + bi$ که در آن $a, b \in \mathbb{R}$، عدد مختلط ناصفری باشد. با توجه به قسمت (ب) اعداد حقیقی c, d موجودند که

$$c^2 = \left|\frac{\sqrt{a^2+b^2} + a}{2}\right|,$$

$$d^2 = \left|\frac{\sqrt{a^2+b^2} - a}{2}\right|.$$

به‌آسانی می‌توان نشان داد که با انتخاب علامت‌های مناسب $z = (\pm c \pm d)^2$.

■■■

نتیجه۶-۲

اگر K میدانی باشد که $\mathbb{C} \leq K$، آن‌گاه $[K : \mathbb{C}] \neq 2$.

اثبات: فرض کنیم $[K:\mathbb{C}]=2$. دراین‌صورت به‌ازای $u\in K-\mathbb{C}$ داریم $K=\mathbb{C}(u)$. بنابراین u ریشه‌ی چندجمله‌ای تکین $f(x)=x^2+bx+c\in\mathbb{C}[x]$ است. طبق لم۱(ج)، عنصر $b^2-4c\in\mathbb{C}$ دارای ریشه‌ی دوم $s\in\mathbb{C}$ است. ازاین‌رو عناصر $(-b\pm s)/2\in\mathbb{C}$ ریشه‌های $f(x)$ هستند و در نتیجه $f(x)$ روی $\mathbb{C}$ شکافته می‌شود، که تناقض است.
■■■

اثبات سوم (قضیه‌ی اساسی جبر به کمک قضیه‌ی اساسی گالوا):

فرض کنیم $f(x)\in\mathbb{C}[x]$ و K میدان شکافنده‌ی $f(x)$ روی $\mathbb{C}$ باشد. کافی است نشان دهیم که $K=\mathbb{C}$. فرض کنیم $G=\mathrm{Aut}_{\mathbb{R}}K$ و $|G|=2^n m$ که $n\in\mathbb{N}_0$، $(2,m)=1$. طبق قضیه‌ی اول سیلو G دارای زیرگروهی مانند H از مرتبه‌ی 2^n است. دراین‌صورت

$$\big[H':\mathbb{R}\big]=[G:H]=m.$$

چون $\mathrm{Char}\mathbb{R}=0$، لذا عنصر تحویل‌ناپذیر $u\in H'$ از درجه‌ی فرد m موجود است به‌قسمی‌که $H'=\mathbb{R}(u)$. طبق لم۱(الف) این درجه باید یک باشد. ازاین‌رو $u\in\mathbb{R}$ و $\big[H':\mathbb{R}\big]=1$. بنابراین $G=H$ و $|G|=2^n$. درنتیجه زیرگروه $\mathrm{Aut}_{\mathbb{C}}K$ از $\mathrm{Aut}_{\mathbb{R}}K$، به ازای $0\le t\le n$ از مرتبه‌ی 2^t است. فرض کنیم $t>0$. دراین‌صورت طبق قضیه‌ی اول سیلو دارای زیر گروهی مانند J از مرتبه‌ی 2^{t-1} است. با توجه به قضیه‌ی اساسی گالوا داریم:

$$\big[J':\mathbb{C}\big]=\big[\mathrm{Aut}_{\mathbb{C}}K:J\big]=2,$$

که با نتیجه۲ در تناقض است. ازاین‌رو $t=0$ و $\mathrm{Aut}_{\mathbb{C}}K=1$. لذا با استفاده‌ی مجدد از قضیه‌ی اساسی گالوا داریم:

$$[K:\mathbb{C}]=\big[\mathrm{Aut}_{\mathbb{C}}K:\{1\}\big]=\big|\mathrm{Aut}_{\mathbb{C}}K\big|=1.$$

پس $K = \mathbb{C}$ و بدین ترتیب قضیه اثبات می‌شود.

■■■

۶-۳ اعداد متعالی

اولین عدد متعالی توسط **لیوویل**[1] در سال ۱۸۴۴ به‌دست آمد. لیوویل لمی (لم۲) برای اعداد جبری مطرح نمود و سپس عددی ارائه داد که در این لم صادق نبود و بدین ترتیب عددی متعالی به‌دست آورد. متعالی بودن‌عدد e برای اولین بار توسط **هرمیت**[2] در سال ۱۸۷۳ ثابت شده است. متعالی بودن عدد π توسط **لیندمان**[3] به کمک همان روش هرمیت در سال ۱۸۸۲، یعنی ۹ سال بعد از اثبات متعالی بودن e، ثابت شد. در این‌جا اثبات ساده‌ای از متعالی بودن اعداد π و e که از کتاب

Stewart, I. *Galois Theory.* 3 nd ed., Chapam & Hall/CRC Press, 2004.

اقتباس شده است، می‌آوریم.

یادآوری: عدد حقیقی

$$\alpha = 0.11000100000000000000000001000... = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

عدد لیوویل نام دارد (توجه کنید که عدد 1 در موقعیت‌های $1!, 2!, 3!, \ldots$ ظاهر می‌شود).

---

[1] Joseph Liouville
[2] Charles Hermite
[3] Lindemann

لم۶-۲

فرض کنیم α یک عدد جبری از درجه‌ی $n > 1$ باشد. دراین‌صورت عدد حقیقی $A > 0$ موجود است به‌طوری‌که برای اعداد صحیح p,q، $q > 0$ داریم:

$$|\alpha - \frac{p}{q}| > \frac{A}{q^n}.$$

اثبات: فرض کنیم $f(x)$ چند جمله‌ای مینیمال α باشد (با ضرب $f(x)$ در کوچک‌ترین مضرب مشترک مخرج‌های همه‌ی ضرایبش، می‌توان فرض کرد که همه‌ی ضرایب $f(x)$ اعداد صحیح‌اند).

فرض کنیم

$$M = \max\{f'(x) \mid \alpha - 1 \le x \le \alpha + 1\}.$$

عدد حقیقی $A > 0$ را طوری انتخاب می‌کنیم که

$$A < \min\{1, \frac{1}{M}\}.$$

(فرض خلف) فرض کنیم اعداد صحیح p,q، $q > 0$ موجود باشند به‌قسمی که

$$|\alpha - \frac{p}{q}| \le \frac{A}{q^n} \le A < \min\{1, \frac{1}{M}\}.$$

با توجه به قضیه‌ی مقدار میانگین، عدد c بین $\frac{p}{q}$ و α هست که

$$f(\alpha) - f(\frac{p}{q}) = (\alpha - \frac{p}{q}) f'(c)$$

اما $f(\alpha) = 0$ (طبق فرض) و $f(\frac{p}{q}) \neq 0$، زیرا $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر و از درجه‌ی بزرگ‌تر از یک است. بنابراین $f(x)$ نمی‌تواند ریشه‌ای در $\mathbb{Q}$ داشته باشد و لذا $f'(c) \neq 0$.

پس خواهیم داشت

$$|\alpha - \frac{p}{q}| = \frac{|f(\alpha) - f(\frac{p}{q})|}{|f'(c)|} = \frac{|f(\frac{p}{q})|}{|f'(c)|}.$$

حال فرض کنیم که $f(x)=\sum_{i=0}^{n} a_i x^i$ که $a_i \in \mathbb{Z}$. دراین‌صورت با توجه به این‌که $f(\frac{p}{q}) \neq 0$، داریم

$$|f(\frac{p}{q})| = |\sum_{i=0}^{n} a_i p^i q^{-i}| = \frac{|\sum_{i=0}^{n} a_i p^i q^{n-i}|}{q^n} \geq \frac{1}{q^n}.$$

چون $f'(c) \leq M$ و $\frac{1}{M} > A$، پس

$$|\alpha - \frac{p}{q}| = \frac{|f(\frac{p}{q})|}{|f'(c)|} \geq \frac{1}{Mq^n} > \frac{A}{q^n} \geq |\alpha - \frac{p}{q}|,$$

که تناقض است. بدین ترتیب لم اثبات می‌شود.

■■■

قضیه۶-۳ (متعالی بودن عدد لیوویل)

عدد α متعالی است.

اثبات: فرض کنیم $p_m = \sum_{i=1}^{m} \frac{1}{10^{m!+i!}}$ و $q_m = \frac{1}{10^{m!}}$. دراین‌صورت

$$|\alpha - \frac{p_m}{q_m}| \leq \sum_{i=m+1}^{\infty} \frac{1}{10^{i!}} \leq \frac{2}{10^{(m+1)!}}.$$

بنابراین به‌ازای هر عدد صحیح $n > 1$ و هر عدد حقیقی $A > 0$، نامساوی

$$|\alpha - \frac{p_m}{q_m}| > \frac{A}{q_m^n}$$

به‌ازای همه‌ی mهای به‌قدر کافی بزرگ، برقرار است. ازاین‌رو بنابر لم اخیر، عدد α متعالی است.

■■■

قضیه ۶-۴ (متعالی بودن عدد e)

عدد e متعالی است.

اثبات: فرض کنیم $a_{\mathrm{m}}e^{m}+\cdots+a_{1}e+a_{0}=0,\ (a_{i}\in\mathbb{Z})$. بدون کاسته شدن از کلیت مسئله فرض می‌کنیم $a_{0}\neq 0$. تعریف می‌کنیم

$$f(x)=\frac{x^{p-1}(x-1)^{p}(x-2)^{p}\ldots(x-m)^{p}}{(p-1)!}$$

جایی‌که p یک عدد اول دلخواه است. سپس تعریف می‌کنیم:

$$F(x)=f(x)+f'(x)+\cdots+f^{(mp+p-1)}(x).$$

حال اگر $0<x<m$ باشد، آن‌گاه

$$|f(x)|\leq\frac{m^{p-1}m^{mp}}{(p-1)!}=\frac{m^{mp+p-1}}{(p-1)!}.$$

هم‌چنین

$$\frac{d}{dx}(e^{-x}F(x))=e^{-x}[F'(x)-F(x)]=-e^{-x}f(x).$$

بنابراین

$$a_{j}\int_{0}^{j}e^{-x}f(x)dx=a_{j}[-e^{-x}F(x)]_{0}^{j}=a_{j}F(0)-a_{j}e^{-j}F(j).$$

با ضرب در e^{j} و مجموع گرفتن روی $j=0,1,\ldots,m$، به‌دست می‌آوریم

$$\sum_{j=0}^{m}a_{j}e^{j}\int_{0}^{j}e^{-x}f(x)dx=F(0).0-\sum_{j=0}^{m}a_{j}F(j)$$
$$=-\sum_{j=0}^{m}\sum_{i=0}^{mp+p-1}a_{j}f^{(i)}(j).$$

ادعا می‌کنیم که هر $f^{(i)}(j)$ یک عدد صحیح قابل تقسیم بر p است، به‌جز زمانی که $j=0$ و $i=p-1$ است. برای قسمت های ناصفر به دست آمده از قسمت هایی که عامل

$(x-j)^p$ دارای p بار مشتق است، $p!$ با $(p-1)!$ ساده می شود و فقط p باقی می‌ماند به‌جز در حالت استثنا شده ($j=0$ و $i=p-1$).

نشان می دهیم که حالت استثنا بر p قابل قسمت نیست. به‌وضوح $f^{(p-1)}(0)=(-1)^p\ldots(-m)^p$. عدد اول p را بزرگ‌تر از m انتخاب می‌کنیم، در این صورت این حاصل ضرب دارای عامل اول p نیست. ازاین‌رو سمت راست معادله‌ی اخیر یک عدد صحیح مخالف صفر است. اما با استفاده از نامساوی بالا برای $|f(x)|$ هرگاه p به سمت بی نهایت میل کند، سمت چپ به سمت صفر میل می کند که این یک تناقض است.

■■■

قضیه۶-۵ (متعالی بودن عدد π)

عدد π متعالی است.

اثبات: اگر π در یک معادله‌ی جبری با ضرایب در $\mathbb{Q}$ صدق کند، $i\pi$ نیز چنین است. فرض کنیم این معادله‌ی $\theta_1(x)=0$ با ریشه‌های $i\pi=\alpha_1,\ldots,\alpha_n$ باشد. حال می‌دانیم $e^{i\pi}+1=0$، بنابراین

$$(e^{\alpha_1}+1)\ldots(e^{\alpha_n}+1)=0.$$

حال یک معادله‌ی جبری با ضرایب صحیح می سازیم که ریشه‌های آن توان‌های e در بسط حاصل‌ضرب فوق باشد. برای مثال توان‌ها در جفت‌ها، $\alpha_1+\alpha_2,\alpha_1+\alpha_3,\ldots,\alpha_{n-1}+\alpha_n$ است. به‌وضوح این جفت‌ها ریشه‌های معادله‌ای مانند $\theta_2(x)=0$ با ضرایب گویا هستند. به طور مشابه حاصل جمع‌های سه تایی αها ریشه‌های $\theta_3(x)=0$ هستند و غیره. بنابراین معادله‌ی

$$\theta_1(x)\theta_2(x)\ldots\theta_n(x)=0$$

یک معادله‌ی چندجمله‌ای روی $\mathbb{Q}$است که ریشه‌هایش تمام حاصل‌جمع‌های αهاست. با حذف ریشه‌های صفر، در صورت وجود، چند جمله‌ای زیر را از آن به‌دست می‌آوریم

$$\theta(x)=0,$$
$$\theta(x)=cx^r+c_1x^{r-1}+\cdots+c_r$$

که $c_r \neq 0$، زیرا ریشه‌های صفر را حذف کرده بودیم. ریشه‌های این معادله توان‌های غیر صفر e در بسط حاصل‌ضرب بالا هستند، آن‌ها را $\beta_1,...,\beta_r$ می‌نامیم. معادله‌ی اصلی به صورت زیر در می‌آید

$$e^{\beta_1}+...+e^{\beta_r}+e^0+...+e^0=0$$

یعنی

$$\sum e^{\beta^i}+k=0$$

جایی‌که k یک عدد صحیح بزرگ‌تر از صفر است. حال تعریف می‌کنیم

$$f(x)=c^s x^{p-1}\frac{[\theta(x)]^p}{(p-1)!}$$

جایی‌که $s=rp-1$ و p بعداً مشخص می‌شود.

اکنون تعریف می‌کنیم:

$$F(x)=f(x)+f'(x)+...+f^{(s+p)}(x).$$

و به‌دست می‌آوریم

$$\frac{d}{dx}[e^{-x}F(x)]=-e^{-x}f(x).$$

ازاین‌رو داریم

$$e^{-x}F(x)-F(0)=-\int_0^x e^{-y}f(y)dy$$

با قرار دادن $y=\lambda x$، به‌دست می‌آوریم

$$F(x)-e^x F(0)=-x\int_0^1 e^{(1-\lambda)x}f(\lambda x)d\lambda.$$

به‌جای x قرار می‌دهیم β_j و روی آن مجموع می‌گیریم. با توجه به این که $\sum e^{\beta^i}+k=0$، به‌دست می آوریم

$$\sum_{j=1}^r F(\beta_j)+kF(0)=-\sum_{j=1}^r \beta_j\int_0^1 e^{(1-\lambda)\beta_j}f(\lambda\beta_j)d\lambda.$$

ادعا: برای pهای به اندازه کافی بزرگ، سمت چپ یک عدد صحیح مخالف صفر است.

با استفاده از تعریف f، $\sum_{j=1}^{r} f^{(t)}(\beta_j) = 0$ $(0 < t < p)$. هر مشتق از مرتبه‌ی p یا بیشتر، دارای یک عامل p و یک عامل c^s است. $f^{(t)}(\beta_j)$ یک چندجمله‌ای از β_j و از درجه‌ی بیشتر از s است. بنابراین مجموع، یک عدد صحیح است به شرط آنکه هر ضریب بر c^s قابل قسمت باشد، که این چنین است. بنابراین داریم

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = pk_t \qquad t = p, \ldots, p+s.$$

پس

$$\text{سمت چپ} = (\text{عدد صحیح}) + kF(0)$$

$F(0)$ چیست؟ محاسبه نشان می‌دهد که

$$f^{(t)}(0) = \begin{cases} 0 & (0 \le t \le p-2) \\ c^s c_r^p & (t = p-1) \\ \ell_t p & (t \ge p) \end{cases}$$

برای عدد مناسب $\ell_t \in \mathbb{Z}$. پس سمت چپ یک ضریب صحیح از $p + c^s c_r^p k$ است. این بر p قابل قسمت نیست مگر $p > k, c, c_r$. بنابراین یک عدد صحیح مخالف صفر است. اما هرگاه p به سمت بی‌نهایت میل کند، سمت راست به صفر میل می‌کند و تناقض معمول به‌دست می‌آید.

■■■

۶-۴ هر حلقه‌ی تقسیم متناهی، میدان است

مشهورترین حلقه‌ی تقسیم غیرتعویض‌پذیر، حلقه‌ی کواترنیون‌هاست که در فصل اول مطالعه شد. همان‌طوری که از عنوان این فصل استنباط می شود،چنین حلقه‌ی تقسیمی الزاماً نامتناهی است. این واقعیت که امروزه از احکام معروف و قدیمی به

حساب می‌آید، توجه بسیاری از ریاضی‌دانان را بـه خـود جلـب کـرده اسـت؛ چنـان‌کـه **هرشتاین**[1] می‌نویسد:

" این قضیه به طرز بسیار نامنتظره‌ای دو چیز ظاهراً نامرتبط، تعداد عناصر یـک دستگاه جبری معین و ضرب در آن دستگاه را به هم مرتبط می‌سازد."

این قضیه‌ی زیبا که به **ودربورن**[2] نسبت داده می‌شود (البته در این انتساب تردید وجود دارد) به‌وسیله‌ی افراد زیادی با راه‌حل‌های متنوعی به اثبات رسیده است. خود ودربـورن سه اثبات در سال ۱۹۰۵ ارائـه داد. لئونوردیکسـن هـم در همـان سـال اثبـات دیگـری به‌دست آورد. بعدها امیـل آرتـین، هـانس تسانسـهاوس، نیکـولاس بورباکی و بسـیاری ریاضی‌دانان دیگر اثبات‌هایی ارائه دادند.

قضیه۶-۶ (قضیه‌ی ودربورن)

اگر D یک حلقه‌ی تقسیم متناهی باشد، آن‌گاه D یک میدان است.

اثبات: فرض کنیم F مرکز D و $q = |F|$. کافی است نشـان دهـیم $n := \dim_F D = 1$.
(فرض خلف) فرض کنیم $n > 1$. معادله‌ی رده‌ای را برای گروه متناهی D^* می‌نویسیم:

$$| D^* | = q^n - 1 = q - 1 + \sum [D^* : C(a)^*].$$

اگر $r(a) = \dim_F C(a)$، آن‌گاه معادله‌ی بالا به شکل زیر خواهد شد:

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^{r(a)} - 1}. \qquad (*)$$

چون $r(a) \mid n$، خواهیم داشت:

$$x^n - 1 = \Phi_n(x)(x^{r(a)} - 1)f(x)$$

---

[1] I. N. Herstein
[2] J. H. M. Wedderburn

که در این‌جا $f(x) \in \mathbb{Z}[x]$ و $\Phi_n(x)$، nامین چند جمله‌ای دایره‌بر است. این معادله نشان می‌دهد که $\Phi_n(q) \mid \frac{q^n-1}{q^{r(a)}-1}$ و لذا طبق $(*)$، $\Phi_n(x) \mid q-1$. به‌خصوص

$$q-1 \geq \mid \Phi_n(q) \mid = \prod \mid q-\varepsilon \mid,$$

که εروی تمام ریشه‌های nام واحد اولیه تغییر می‌کند. رابطه‌ی اخیر با توجه به این‌که برای هر ε، $\mid q-\varepsilon \mid > q-1 \geq 1$ ، یک تناقض است.

■■■

۶-۵ حل معادلات درجه‌ی ۲، ۳ و ۴

بزرگترین ریاضی‌دان عصرخود، و اگر همه شرایط را در نظرآوریم، یکی از بزرگترین ریاضی‌دانان همه اعصار خوارزمی است.

(جورج سارتون)

تصویر خوارزمی بنیان گذار جبر[۱]

حل معادلات درجه ۲

با توجه به این‌که از دوره‌ی دبیرستان با فرمول حل معادله‌ی درجه دوم

$$ax^2 + bx + c = 0$$

یعنی

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

آشنا هستیم در این‌جا فقط به بیان توضیحاتی تاریخی راجع به حل معادله‌ی درجـه دوم اکتفا می‌کنیم.

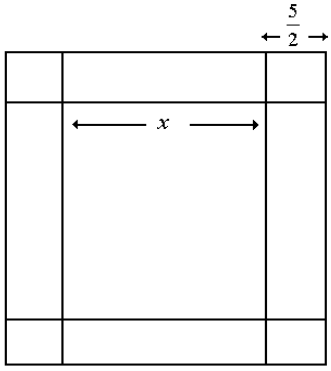
---

[۱] تصویر بالا (و همچنین تصاویر موجود در این کتاب) از سایت زیر گرفته شده است:

http://www-groups.dcs.st-and.ac.uk/~history/index.html

کتاب جبر خوارزمی (مرجع [۲] ملاحظه شود)، نقشی بسیار اساسی در ریاضیات دارد. وقتی این کتاب به زبان لاتین ترجمه شد، مدت‌ها تنها کتاب درسی ریاضی، در تمام اروپای غربی بود. خوارزمی در این کتاب راه حل معادله‌های درجه اول و دوم را شرح داده است. خوارزمی برای حل معادله‌ی $x^2+10x=39$ دو روش کلی به‌کار برد، که ما در این‌جا یکی از این روش‌ها را می‌آوریم.

مربعی به ضلع x می‌سازیم و سپس روی ضلع‌های آن، مستطیل‌هایی به ضلع‌های مساوی x و $5/2$ اضافه می‌کنیم. بعد، تمام شکل را به‌صورت یک مربع کامل در می‌آوریم (شکل۶-۲ را ببینید). از روی شکل دیده می‌شود که مساحت مربع بزرگ برابر است با مساحت مربع به ضلع x به‌اضافه‌ی مساحت چهار مستطیل به ضلع‌های x و $5/2$ و نیز مساحت چهار مربع به ضلع $5/2$. بنابراین، مساحت مربع بزرگ برابر است با $x^2+10x+25$ و چون x^2+10x برابر 39 است، لذا مساحت مربع بزرگ برابر $39+25$؛ یعنی 64 می‌شود. به‌این‌ترتیب، ضلع این مربع برابر $5-8$؛ یعنی 3 می‌شود.



شکل ۶-۲

حل معادلات درجه ۳

حالت کلی معادله‌ی درجه سوم، در برابر همه کوشش‌های ریاضی‌دانان باستانی، تسلیم ناپذیر باقی ماند. این معادله، تنها در آغاز سال‌های ۱۵۰۰ و در دوره‌ی بازسازی در

ایتالیا و توسط **فه‌رو**[1]، ریاضی‌دان ایتالیایی حل شد. بنابر عادت زمان، فه‌رو کشف خود را منتشر نکرد، ولی آن را به یکی از شاگردان خود اطلاع داد. بعد از مرگ فه‌رو، این شاگرد، یکی از بزرگ‌ترین ریاضیدانان ایتالیا؛ یعنی **تارتاگلیا**[2]، را برای حل چند معادله‌ی درجه سوم به مسابقه دعوت کرد. تارتاگلیا دعوت را پذیرفت و ۸ روز پیش از پایان مسابقه، روش حل هر معادله‌ی درجه سوم به‌صورت $x^3 + px + q = 0$ را پیدا کرد.

او در ۲ ساعت همه‌ی مسئله‌های رقیب خود را حل کرد. **کاردان**[3] پروفسور ریاضیات و فیزیک در میلان، از کشف تارتاگلیا آگاهی پیدا کرد و از او خواهش کرد، کشف خود را برای او فاش کند. تارتاگلیا سرانجام موافقت کرد، ولی با این شرط که کاردان، روش او را پنهان نگه دارد. کاردان پیمان خود را شکست و دستور تارتاگلیا را در کتاب خود به‌نام "Ars Magna" «هنر بزرگ» منتشر کرد.

از این زمان، دستور حل معادله‌ی درجه سوم را دستور کاردان می‌نامند.

صورت عمومی معادله‌ی درجه سوم به‌صورت:

$$Ax^3 + Bx^2 + Cx + D = 0$$

است که در آن x متغیری است که $\mathbb{C}$، مجموعه‌ی اعداد مختلط، به عنوان حوزه‌ی اصلی آن در نظر گرفته شده است. A، B، Cو Dضرایب حقیقی‌اند. Ax^3 جمله‌ی درجه‌ی سوم، Bx^2 جمله‌ی درجه‌ی دوم، Cx جمله‌ی خطی و Dجمله‌ی مطلق نامیده می‌شود.

با تقسیم دو طرف معادله بر $A \neq 0$ و قرار دادن $B/A = r$و $C/A = s$ و $D/A = t$ صورت نرمال $x^3 + rx^2 + sx + t = 0$ را به‌دست می‌آوریم.

---

[1] Scipione del Ferro
[2] Nicolo Fontana Tartaglia
[3] Girolamo Cardano

با جانشینی $x = y - (r/3)$ صورت نرمال $x^3 + rx^2 + sx + t = 0$ را به‌صورت تحویل‌یافته‌ی $y^3 + py + q = 0$ تبدیل می‌کنیم. در این فرمول از اختصارات $p = s - (r^2/3)$، $q = (2r^3/27) - (sr/3)$ استفاده کرده‌ایم.

قرار می‌دهیم $y = u + v$ و ازاین‌رو $(u+v)^3 + p(u+v) + q = 0$ یا

$(u^3 + v^3 + q + 9u + v)(3uv + p) = 0$ را به‌دست می‌آوریم. اکنون معادله‌ای با دو متغیر u و v داریم. بنابراین در استفاده از شرطی اضافی در ارتباط بین u و v آزادیم. این شرط را چنان اختیار می‌کنیم که عامل $3uv + p = 0$، و در نتیجه آخرین جمعوند، صفر می‌شود. این کار دستگاه معادلاتی بر حسب متغیرهای u و v به‌صورت زیر می‌دهد:

$$\begin{cases} u^3 + v^3 = -q \\ uv = -\dfrac{p}{3} \end{cases}$$

با حل دستگاه بالا داریم:

$$u^3 = -\frac{q}{2} \pm \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3} \qquad \text{و} \qquad v^3 = -\frac{q}{2} \mp \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}$$

با تعویض علامت‌های بالا به علامت‌های پایین، u^3 به v^3 تبدیل می‌شود، اما، اگر u و v با هم عوض شوند، معادله‌های $u^3 + v^3 = q = 0$ و $uv = -\frac{p}{3}$ بی‌تغییر باقی می‌مانند. بنابراین کافی‌است تنها یکی از این علامت‌ها، مثلاً بالایی را در نظر بگیریم.

هر ریشه‌ی سوم یک عدد مختلط دارای سه مقدار است، در این‌صورت غیر از جواب x_1 دو جواب دیگر ωx_1 و $\omega^2 x_1$، که $\omega \neq 1$ ریشه‌ی سوم واحد است، موجودند. در نتیجه مقادیر زیر را برای u و v به‌دست می‌آوریم.

$$u_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}} \quad \text{و} \quad u_2 = u_1\omega \quad \text{و} \quad u_3 = u_1\omega^2$$

$$v_3 = v_1\omega^2 \quad \text{و} \quad v_2 = v_1\omega \quad \text{و} \quad v_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}}$$

به ازای $y = u_i + v_j$ نه جواب $(i = 1,2,3;\ j = 1,2,3)$ معادله‌ی درجه‌ی سوم مورد بحث را به‌دست می‌آوریم. اما تعدادجواب‌ها به سه جواب زیر تحویل می‌شود و

$$y_1 = u_1 + v_1 \quad \text{و} \quad y_2 = u_2 + v_3 \quad \text{و} \quad y_3 = u_3 + v_2$$

زیرا، ازآن‌جا که $\omega\omega^2 = \omega^3 = 1$، شرط اضافی $u_i v_j = -p/3$ تنها به ازای u_1v_1، u_2v_3، u_3v_2 برقرار است.

بنابراین داریم:

$$y_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

$$y_2 = u_1\omega + v_1\omega^2 = \frac{-(u_1 + v_1)}{2} + \left[\frac{(u_1 - v_1)}{2}\right] i\sqrt{3},$$

$$y_3 = u_1\omega^2 + v_1\omega = \frac{-(u_1 + v_1)}{2} - \left[\frac{(u_1 - v_1)}{2}\right] i\sqrt{3}.$$

حل معادلات درجه ۴

بلافاصله بعد از حل معادله‌ی درجه‌ی سوم، حالت کلی معادله‌ی درجه‌ی چهارم توسط **فراری**[1] (۱۵۲۲-۱۵۶۵)، شاگرد و همکار کاردان، کشف شد. این فرمول نیز توسط کاردان در کتاب "Ars Magna" آورده شده است.

روش فراری چنین است:

معادله‌ی درجه‌ی چهارم کلی زیر را در نظر می‌گیریم:

---

[1] Lodovico Ferrari

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

و آن‌را به این‌صورت می‌نویسیم

$$x^4 + ax^3 = -bx^2 - cx - d$$

و به هر دو طرف برابری $\frac{a^2x^2}{4}$ را اضافه می‌کنیم، سمت چپ معادله به صورت مجذور کامل در می‌آید و معادله چنین می‌شود:

$$(x^2 + \frac{ax}{2})^2 = (\frac{a^2}{4} - b)x^2 - cx - d$$

دوباره به دو طرف برابری این جمله‌ها را اضافه می‌کنیم

$$(x^2 + \frac{ax}{2})y + \frac{y^2}{4}$$

که در آن، y یک مجهول تازه است که بعد، شرطی درباره‌ی آن پیدا خواهیم کرد. در این‌صورت باز هم سمت چپ معادله به‌صورت مجذور کامل در می‌آید و خواهیم داشت:

$$(x^2 + \frac{ax}{2} + \frac{y}{2})^2 = (\frac{a^2}{4} - b + y)x^2 + (\frac{ay}{2} - c)x + (\frac{y^2}{4} - d) \qquad (*)$$

به این‌ترتیب به معادله‌ای با دو مجهول می‌رسیم.

سمت راست برابری (*)، یک سه جمله‌ای درجه دوم نسبت به x است که ضریب‌های آن به y بستگی دارد. yرا طوری انتخاب می‌کنیم که این سه جمله‌ای برابر مجذور یک دو جمله‌ای درجه اول $\alpha x + \beta$ باشد.

برای آن‌که یک سه جمله‌ای درجه دوم $Ax^2 + Bx + C$ برابر مجذور دو جمله‌ای $\alpha x + \beta$ باشد، کافی است داشته باشیم

$$B^2 - 4AC = 0,$$

زیرا دراین‌صورت خواهیم داشت

$$Ax^2 + Bx + C = (\sqrt{A}x + \sqrt{C})^2.$$

یعنی

$$Ax^2 + Bx + C = (\alpha x + \beta)^2,$$

که در آن داریم $\beta = \sqrt{C}$ و $\alpha = \sqrt{A}$. بنابراین، اگر y را طوری انتخاب کنیم که داشته باشیم

$$(\frac{ay}{2} - c)^2 - 4(\frac{a^2}{4} - b + y)(\frac{y^2}{4} - d) = 0.$$

سمت راست معادله‌ی (*) برابر مجذور کاملی به‌صورت $(\alpha x + \beta)^2$ خواهد بود. اگر پرانتزها را باز کنیم، به معادله‌ی درجه‌ی سومی نسبت به y می‌رسیم

$$y^3 - by^2 + (ac - bd)y - [d(a^2 - 4b) + c^2] = 0.$$

با حل این معادله‌ی کمکی درجه‌ی سوم (مثلاً به کمک دستور کاردان)، می‌توانیم α و β را بر حسب ریشه‌ی آن، y_0، پیدا کنیم و به‌دست می‌آید

$$(x^2 + \frac{ax}{2} + \frac{y_0}{2})^2 = (\alpha x + \beta)^2$$

و از آن‌جا $x^2 + \frac{ax}{2} + \frac{y_0}{2} = \alpha x + \beta$ یا $x^2 + \frac{ax}{2} + \frac{y_0}{2} = -\alpha x - \beta$.

از این دو معادله‌ی درجه دوم، هر چهار ریشه‌ی معادله‌ی درجه چهارم به‌دست می‌آید.

PID⇏ED ۶-۶

در اکثر کتاب‌های جبر (به‌ویژه نظریه‌ی میدان) نشان داده شده که هر دامنه‌ی اقلیدسی یک دامنه ی ایده‌آل اصلی است. و متذکر می‌شوند که عکس این مطلب برقرار نیست و تنها به ذکر این نکته که زیر حلقه‌ی

$$A = \mathbb{Z}[\theta] = \{a + b\theta \mid a, b \in \mathbb{Z}, \theta = (1 + \sqrt{-19})/2\}$$

از اعداد مختلط یک دامنه ی ایده‌آل اصلی است که دامنه‌ی اقلیدسی نیست، اکتفا می‌کنند. در این بخش با ارائه‌ی اثبات ساده‌ای از

Campoli, O. A. *A principal ideal domain that is not a Euclidean domain*. Amer. Math. Monthly 95 (1988), no. 9, 868-871.

نشان می‌دهیم که A یک دامنه ی ایده‌آل اصلی بوده در حالی که دامنه‌ی اقلیدسی نیست.

قضیه۶-۷

حلقه‌ی A یک دامنه‌ی اقلیدسی نیست.

اثبات: برای این‌که نشان دهیم A یک دامنه‌ی اقلیدسی نیست، باید نشان دهیم هیچ تابع اقلیدسی برای حلقه‌ی A یافت نمی‌شود. (برهان خلف) فرض کنیم v یک تابع اقلیدسی برای حلقه‌ی A باشد. قرار می‌دهیم:

$$\ell = \mathrm{Min}\{v(a) \mid a \in A - \{0\}\},$$
$$U = \{a \in A - \{0\} \mid v(a) = \ell\}.$$

چون هر عنصر یکال A، عناصر ناصفر A را عاد می‌کند، خاصیت اول تابع اقلیدسی ایجاب می‌کند که هر یکالی در U است. از طرفی خاصیت دوم تابع اقلیدسی ایجاب می‌کند که هر عنصر U، بر هر عنصر ناصفری از A بخش‌پذیر است؛ بنابراین U دقیقاً عناصر یکال A است. در ادامه نشان خواهیم داد که $U = \{1, -1\}$. برای این منظور قدری محاسبه در A لازم است.

اتحادهای زیر با توجه به تعریف $\theta = (1 + \sqrt{-19})/2$، به‌آسانی به‌دست می‌آیند. برای هر $a \in A$، $\overline{a}$ نمایش‌دهنده‌ی مزدوج مختلط عدد a است.

(۱) $\overline{\theta} = 1 - \theta$

(۲) $\theta\overline{\theta} = 5$

(۳) $\theta^2 = \theta - 1$

(۴) اگر $x = a + b\theta \in A$ ، آن‌گاه $\theta x = -5b + (a + b)\theta$.

اتحاد (۱) بسته بودن A تحت مزدوج مختلط را ایجاب می‌کند. اتحاد (۲) نتیجه می‌دهد که عنصر 5 در حلقه‌ی A اول نیست. به‌وضوح خواهیم دید که θ عنصر یکالی از A نیست و این ایجاب می‌کند که 5 عنصری تحویل‌پذیر از A است. از (۳) به‌دست می‌آید که $\theta^2 \in A$ و در نتیجه A تحت ضرب مختلط بسته است (واقعیتی که با توجه به تعریف A، واضح نیست)

اگر $\|z\| = z\bar{z}$ همان نرم مختلط معمول باشد، آن‌گاه اتحادهای اخیر ایجاب می‌کنند که:

$$\|a+b\theta\| = (a+b\theta)(\overline{a+b\theta}) = a^2+ab+5b^2 \quad (۴)$$

ازاین‌رو اگر عنصر $a+b\theta \in A$ یکال باشد، آن‌گاه

$$a^2+ab+5b^2 = \|a+b\theta\| = 1,$$

و در نتیجه اگر $ab \geq 0$، آن‌گاه $b=0$ و $a=\pm 1$. هم‌چنین، چون

$$1 = \|a+b\theta\| = (a+b)^2 - ab + 4b^2,$$

نتیجه می‌گیریم که هرگاه $ab \leq 0$، آن‌گاه دوباره $b=0$ و $a=\pm 1$.

حال فرض کنیم $m \in A$ عنصری غیر از عناصر $0,1,-1$ بوده به‌قسمی که $\upsilon(m)$ مینیمم باشد. طبق تعریف تابع اقلیدسی عناصر $q,r \in A$ موجودند به‌قسمی که $2 = qm + r$ و $\upsilon(r) < \upsilon(m)$. بنابراین r باید یکی از اعداد $0,1,-1$ باشد. ازاین‌رو m بر 2 یا 3 بخش‌پذیر است. ادعا می‌کنیم که m باید یکی از اعداد $\pm 2, \pm 3$ باشد. این ادعا از اول بودن 2 و 3 در حلقه‌ی A که در زیر نشان می‌دهیم، نتیجه می‌شود. فرض کنیم $2 = (a+b\theta)(c+d\theta)$. دراین‌صورت $\|2\| = \|a+b\theta\|\|c+d\theta\|$ و 4 فرض غیر یکال بودن عناصر $a+b\theta, c+d\theta$ در A ایجاب می‌کند که

$$2 = \|a+b\theta\| = a^2+ab+5b^2 = \left\|a+b\bar{\theta}\right\| = (a+b)^2 - ab + 4b^2.$$

بنابراین با در نظر گرفتن حالت‌های $ab \geq 0$ و $ab < 0$، نتیجه خواهیم گرفت که $b=d=0$. پس $2 = (a+b\theta)(c+d\theta) = ac$ یک تجزیه در $\mathbb{Z}$ است. چون 2 در $\mathbb{Z}$ اول است، پس 2 در A اول است. به‌طریق مشابه می‌توان نشان داد که 3 نیز در A اول است.

با به‌کارگیری مجدد تعریف تابع اقلیدسی، داریم که θ به‌پیمانه‌ی ± 2 یا ± 3 با $0,1$ یا -1 همنهشت است. درنتیجه θ یا $\theta-1$ یا $\theta+1$ بر 2 یا 3 بخش پذیر است. اما این غیر ممکن است، زیرا $\|\theta-1\| = \|5\| = \|\theta\|$ و $\|\theta+1\| = 7$، در حالی که $\|2\| = 4$ و $\|3\| = 9$.

■■■

قضیه۶-۸

حلقه‌ی A یک دامنه‌ی ایده‌آل اصلی است.

اثبات: برای این‌که ثابت کنیم که A یک دامنه ی ایده‌آل اصلی است، کافی است نشان دهیم که A تقریباً یک دامنه‌ی اقلیدسی است. به‌عبارت دیگر، نشان می‌دهیم که برای هر $\alpha, \beta \in A$، $\beta \neq 0$، اگر β بر α بخش‌پذیر نباشد و $\|\beta\| \geq \|\alpha\|$، آن‌گاه عناصر $\gamma, \delta \in A$ موجودند به‌طوری‌که

$$0 < \|\alpha\gamma - \beta\delta\| < \|\beta\|. \qquad (۱)$$

همانند اثبات معمولی که نشان می‌دهد $\mathbb{Z}$ یک PID است، می‌توان PID بودن A را به‌دست آورد. فرض کنیم $I \neq 0$ یک ایده‌آل A باشد. فرض کنیم که $\beta \in I$ عنصری باشد که $\|\beta\|$ در بین عناصر غیر صفر I مینیمم باشد. دراین‌صورت $\beta A = I$. در حقیقت، به‌وضوح $\beta A \subseteq I$؛ حال فرض کنیم که $\alpha \in I$ عنصری باشد که β بر α بخش‌پذیر نباشد. ازاین‌رو $\alpha \neq 0$ و در نتیجه $\|\beta\| \geq \|\alpha\|$. حال وجود عنصر $\alpha\gamma - \beta\delta$ از I با مینیمال بودن $\|\beta\|$ در تناقض است.

برای نشان دادن (۱)، فرض کنیم $\alpha, \beta \in A$، $\beta \neq 0$. اگر β بر α بخش‌پذیر نباشد $\|\beta\| \geq \|\alpha\|$، می‌نویسیم

$$\frac{\alpha}{\beta} = a + b\theta,$$

جایی‌که a و bاعداد گویایی بوده که دست کم یکی از آن‌ها صحیح نیست. این ممکن است زیرا معکوس β به‌عنوان یک عدد مختلط در $\mathbb{Q}[\theta]$،که زیر میدانی از $\mathbb{C}$ است، خواهد بود.

با در نظر گرفتن حالت به حالت می‌توان عناصر $\gamma, \delta \in A$ را یافت به‌طوری‌که

$$0 < \left\| \frac{\alpha}{\beta}\gamma - \delta \right\| < 1,$$

یا

$$\|\alpha\gamma - \delta\beta\| < \|\beta\|.$$

هفت حالت ممکن است.

حالت ۱: $b \in \mathbb{Z}$. دراین‌صورت $a \notin \mathbb{Z}$ و می‌توان قرار داد $\gamma = 1$ و $\delta = \{a\} + b\theta$(جایی‌که $\{x\}$دلالت بر نزدیک‌ترین عدد صحیح به x است که $\{n + \frac{1}{2}\} = n$). حال داریم

$$0 < \left\| \frac{\alpha}{\beta}\gamma - \delta \right\| \leq \frac{1}{4} < 1.$$

حالت۲ (الف): $a \in \mathbb{Z}$ و $5b \notin \mathbb{Z}$. دراین‌صورت $\frac{\alpha}{\beta}\overline{\theta} = a + 5b - a\theta$ و می‌توان قرار داد $\gamma = \overline{\theta}$ و $\delta = \{a + 5b\} - a\theta$.

حالت۲ (ب): $a \in \mathbb{Z}$ و $5b \in \mathbb{Z}$. قرار می‌دهیم $\gamma = 1$ و $\delta = a + \{b\}\theta$.

حالت۳ (الف): $a, b \notin \mathbb{Z}$ و $2a, 2b \in \mathbb{Z}$. دراین‌صورت، رابطه‌ی (۴) در اثبات قضیه‌ی اخیر، برای $a, b \in \mathbb{Z}$برقرار است؛ اما به‌وضوح این رابطه برای عناصر گویای a, b نیز صادق است و درنتیجه $\theta(\alpha / \beta) = -5b + (a + b)\theta$ و $b \in \mathbb{Z}$. بنابراین، می‌توان قرار داد $\gamma = \theta$ و $\delta = \{-5b\} + \{a + b\}\theta$.

حالت۳ (ب): $a, b \notin \mathbb{Z}$ و $2a, 2b \notin \mathbb{Z}$. دراین‌صورت یا $| b - \{b\} | \leq 1 / 3$ و یا $| 2b - \{2b\} | \leq 1 / 3$. در حالت اول قرار می‌دهیم $\gamma = 1$ و $\delta = \{a\} + \{b\}\theta$ و داریم

$$0 < \left\| \frac{\alpha}{\beta}\gamma - \delta \right\| \leq \frac{35}{36} < 1.$$

در حالت دوم قرار می‌دهیم $\gamma = 2$ و $\delta = \{2a\} + \{2b\}\theta$ و همان نتیجه‌ی حالت اول برقرار است.

حالت۳ (ج): $a, b \notin \mathbb{Z}$ و $2a \in \mathbb{Z}$ و $2b \notin \mathbb{Z}$. اگر $5b \in \mathbb{Z}$ قرار می‌دهیم $\gamma = 5$ و $\delta = \{5a\} + 5b\theta$ و اگر $5b \notin \mathbb{Z}$ قرار می‌دهیم $\gamma = 2\overline{\theta}$ و $\delta = \{2a + 10b\} - 2a\theta$.

حالت۳ (د): $a, b \notin \mathbb{Z}$ و $2b \in \mathbb{Z}$ و $2a \notin \mathbb{Z}$. قرار می‌دهیم $\gamma = 2$ و $\delta = \{2a\} + 2b\theta$.

■■■

۶-۷ ترسیم پذیری ۱۷- ضلعی منتظم

ساختارهای بسیاری برای 17-ضلعی منتظم مطرح شده است که نخستین ساختار توسط **هاگانین**[1] در۱۸۰۳ به چاپ رسید. به منبع زیر مراجعه کنید.

Klein, F. *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*, Kegan Paul, London, 1913.

یک روش ساختن 17-ضلعی منتظم این است که از قضیه‌ی گاوس استفاده کنیم، که در حقیقت بعد از کمی محاسبات اضافی یک ساختار کاملاً معین را نتیجه می‌دهد.

هدف یافتن عبارت‌های رادیکالی برای صفرهای چندجمله‌ای

$$\frac{t^{17} - 1}{t - 1} = t^{16} + \cdots + t + 1 \qquad (1)$$

روی $\mathbb{C}$ است. فرض کنیم

$$\theta = 2\pi / 17,$$
$$\zeta_k = e^{ki\theta} = \cos(k\theta) + i \sin(k\theta).$$

پس صفرهای (1) در $\mathbb{C}$ عبارتند از $\zeta_1, \zeta_2, \ldots, \zeta_{16}$.

---

[1] Huguenin

توان‌ها ی طبیعی 3 به پیمانه 17 به‌صورت زیر هستند:

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	…
3^m	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	…

تعریف می‌کنیم

$$\begin{aligned}
x_1 &= \zeta_1 + \zeta_9 + \zeta_{13} + \zeta_{15} + \zeta_{16} + \zeta_8 + \zeta_4 + \zeta_2,\\
x_2 &= \zeta_3 + \zeta_{10} + \zeta_5 + \zeta_{11} + \zeta_{14} + \zeta_7 + \zeta_{12} + \zeta_6,\\
y_1 &= \zeta_1 + \zeta_{13} + \zeta_{16} + \zeta_4,\\
y_2 &= \zeta_9 + \zeta_{15} + \zeta_8 + \zeta_2,\\
y_3 &= \zeta_3 + \zeta_5 + \zeta_{14} + \zeta_{12},\\
y_4 &= \zeta_{10} + \zeta_{11} + \zeta_7 + \zeta_6.
\end{aligned}$$

حال به ازای $k = 1,2,\ldots,16$ داریم

$$\zeta_k + \zeta_{17-k} = 2\cos k\theta \qquad (2)$$

که نتیجه می‌دهد

$$\begin{aligned}
x_1 &= 2(\cos\theta + \cos 8\theta + \cos 4\theta + \cos 2\theta),\\
x_2 &= 2(\cos 3\theta + \cos 7\theta + \cos 5\theta + \cos 6\theta),\\
y_1 &= 2(\cos\theta + \cos 4\theta),\\
y_2 &= 2(\cos 8\theta + \cos 2\theta),\\
y_3 &= 2(\cos 3\theta + \cos 5\theta),\\
y_4 &= 2(\cos 7\theta + \cos 6\theta).
\end{aligned} \qquad (3)$$

از (1) نتیجه می‌شود که

$$x_1 + x_2 = -1.$$

با استفاده از (2)و (3)و معادله‌ی

$$2\cos m\theta \cos n\theta = \cos(m+n)\theta + \cos(m-n)\theta$$

به‌دست می‌آوریم

$$\begin{aligned}x_1x_2 = 2(&\cos 4\theta + \cos 2\theta + \cos 8\theta + \cos 6\theta + \cos 4\theta + \cos 6\theta + \cos 5\theta\\ &+ \cos 7\theta + \cos 11\theta + \cos 5\theta + \cos 15\theta + \cos\theta + \cos 13\theta + \cos 3\theta\\ &+ \cos 14\theta + \cos 2\theta + \cos 7\theta + \cos\theta + \cos 3\theta + \cos 11\theta + \cos\theta\\ &+ \cos 9\theta + \cos 2\theta + \cos 10\theta + \cos 5\theta + \cos\theta + \cos 9\theta + \cos 5\theta\\ &+ \cos 7\theta + \cos 3\theta + \cos 4\theta + \cos 8\theta) = -4.\end{aligned}$$

بنابراین x_1 و x_2 صفرهای چندجمله‌ای درجه‌ی دوم

$$t^2 + t - 4 \tag{4}$$

هستند. به‌علاوه $x_1 > 0$، نتیجه می‌دهد $x_1 > x_2$. با استفاده از روابط مثلثاتی، شبیه آن‌چه که در بالا آورده شد، به‌دست می‌آوریم

$$\begin{aligned}y_1 + y_2 &= x_1,\\ y_1y_2 &= -1\end{aligned}$$

و y_1 و y_2 صفرهای

$$t^2 - x_1t - 1 \tag{5}$$

هستند و $y_1 > y_2$. به‌همین طریق y_3 و y_4 صفرهای

$$t^2 - x_2t - 1 \tag{6}$$

هستند و $y_3 > y_4$. حال از

$$\begin{aligned}2\cos\theta + 2\cos 4\theta &= y_1,\\ 4\cos\theta\cos 4\theta = 2(\cos 5\theta + \cos 3\theta) &= y_3\end{aligned}$$

نتیجه می‌شود

$$\begin{aligned}z_1 &= 2\cos\theta,\\ z_2 &= 2\cos 4\theta\end{aligned}$$

صفرهای

$$t^2 - y_1t + y_3 \tag{7}$$

هستند و $z_1 > z_2$.

با استفاده از حل دسته معادلات درجه‌ی دوم (4)، (5)، (6)، (7) و نامعادلات برای تشخیص این‌که این صفرها کدامند، معادله

$$\begin{aligned}\cos\theta = \frac{1}{16}(&-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}\\ &+ \sqrt{68 + 12\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}} - 2(1 - \sqrt{17})\sqrt{34 - 2\sqrt{17}}}\,)\end{aligned}$$

را به‌دست می‌آوریم که در آن ریشه‌های دوم مثبت هستند.

ازاین‌رو می‌توانیم با ساختن ریشه‌های دوم مربوط، یک ساخت هندسی برای 17-ضلعی به‌دست آوریم.

روش زیر برگرفته از منابع

1. Richmond, H. W. *A construction for a regular polygon of seventeen sides*. Quart. J. Pure Appl. Math. 26(1893), 206-207.

2. Richmond, H. W. *To construct a regular polygon of* 17 *sides*. Math. Ann. 67(1909), no. 4, 459-461.

است.

فرض کنیم α کوچک‌ترین زاویه‌ی حاده مثبت باشد به‌طوری‌که $\tan 4\alpha=4$. لذا α، 2α و 4α همگی حاده هستند. عبارت (4) در بالا را می‌توان به‌صورت

$$t^2+4t\cot 4\alpha - 4$$

نوشت که صفرهای آن عبارتند از

$$2\tan 2\alpha, \qquad -2\cot 2\alpha.$$

ازاین‌رو

$$x_1 = 2\tan 2\alpha,$$
$$x_2 = -2\cot 2\alpha.$$

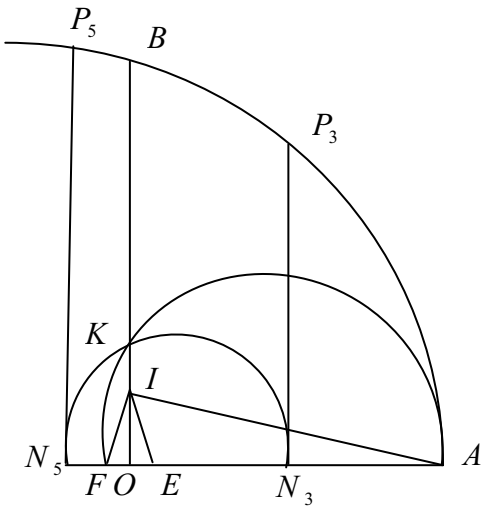
از این نتیجه می‌شود که

$$y_1 = \tan(\alpha + \frac{\pi}{4}),$$
$$y_2 = \tan(\alpha - \frac{\pi}{4}),$$
$$y_3 = \tan\alpha,$$
$$y_4 = -\cot\alpha.$$

پس

$$2(\cos 3\theta + \cos 5\theta) = \tan\alpha,$$
$$4\cos 3\theta \cos 5\theta = \tan(\alpha - \frac{\pi}{4}). \qquad (8)$$

حال مانند شکل زیر، فرض کنیم OA و OB دو شعاع عمود بـر هـم یـک دایـره باشـند. فرض کنیم $OI = \frac{1}{4}OB$ و $\angle OIE = \frac{1}{4}\angle OIA$. نقطه F را روی AO به‌گونـه‌ای بیابیـد که $\angle EIF = \frac{\pi}{4}$. دایره‌ای به قطر AF



شکل ۶-۳

رسم می‌کنیم، محل تقاطع این دایره را با OB، K می‌نامیم. دایره‌ای به مرکز E و بـه شعاع EK قطر AF را در N_3 و N_5 قطع می‌کند. N_3P_3 و N_5P_5 را عمـود بـر OA رسـم می‌کنیم، دراین‌صورت

$$\angle OIE = \alpha,$$
$$\angle OIA = 4\alpha.$$

هم‌چنین

$$\begin{aligned}2(\cos\angle AOP_3+\cos\angle AOP_5) &= 2\frac{ON_3-ON_5}{OA}\\ &= 4\frac{OE}{OA}\\ &= \frac{OE}{OI}\\ &= \tan\alpha,\end{aligned}$$

و

$$\begin{aligned}4\cos\angle AOP_3\cos\angle AOP_5 &= -4\frac{ON_3\cdot ON_5}{OA\cdot OA}\\ &= -4\frac{OK^2}{OA^2}\\ &= -4\frac{OF}{OA}\\ &= -\frac{OF}{OI}\\ &= \tan(\alpha-\frac{\pi}{4}).\end{aligned}$$

از مقایسه با (8) می‌بینیم که

$$\angle AOP_3 = 3\theta,$$
$$\angle AOP_5 = 5\theta.$$

ازاین‌رو A، P_3 و P_5 رئوس 0-ام، 3-ام و 5-ام یک 17-ضلعی منتظم محاط در دایره مفروض هستند. حال رئوس دیگر به سادگی پیدا می‌شوند.

منابعی برای مطالعه‌ی بیشتر

۱. آیگینز، مارتین. تسیگلر، گونتر. **کتاب اثبات**. ترجمه‌ی کاظمی، سیامک. انتشارات پژوهشگاه دانش‌های بنیادین (۱۳۷۹).

۲. خوارزمی، محمد بن موسی. **جبر و مقابله**. ترجمه‌ی خدیوجم، حسین. انتشارات یونسکو در ایران (۱۳۶۲).

۳. گروه مولفین انستیتوی ریاضی استکلووای شوروی. جوهر، **روش و کارایی ریاضیات۱**. ترجمه‌ی شهریاری، پرویز. انتشارات فنی ایران (۱۳۷۹).

۴. مدقالچی، علیرضا. **گزیده‌ای از مقاله‌های ریاضی**. انتشارات مرکز نشر دانشگاهی تهران (۱۳۸۲).

5. Arnold, B. H. A topological proof of the fundamental theorem of algebra. Amer. Math. Monthly 56, (1949). 465-466.

6. Derksen, H. The fundamental theorem of algebra and linear algebra. Amer. Math. Monthly 110 (2003), no. 7, 620-623.

7. Herstein, I. N. *Topics in Algebra*. New York, Blaisdell, 1984.

8. Lam, T. Y. *A first Course in Noncommutative Rings*. Springer-Verlag, New York, 1991.

9. Leibman, G. A nonstandard proof of the fundamental theorem of algebra. Amer. Math. Monthly 112 (2005), no. 8, 705-712.

10. Rotman, J. *Galois Theory*. 2 nd ed., Springer-Verlag, New York, 1998.

11. Stewart, I. *Galois Theory*. 3 nd ed., Chapam & Hall/CRC Press, 2004.

12. Suzuki, J. Lagrange's proof of the fundamental theorem of algebra. Amer. Math. Monthly 113 (2006), no. 8, 705-714.

13. Velleman, D. J. Another proof of the fundamental theorem of algebra. Math. Mag. 70 (1997), no. 3, 216-217.

14. Wielandf, H. Ein Bewise Für die Existenz der Sylowgruppen, Arc. Math. 10(1959), 401-402.

پیوست الف

مروری بر فضاهای برداری

توان حرکت ابداع ریاضی استدلال نیست بلکه تخیل است.

(اگوستوس دمورگان)

در این فصل می‌خوانیم:

مقدمه

برای مطالعه‌ی این کتاب، به‌ویژه قسمت توسیع میدان‌ها، آشنا بودن با مفاهیم فضای برداری، استقلال خطی و پایه بسیار اساسی است. ازاین‌رو به منظور خودکفا بودن کتاب این مفاهیم را در این بخش مورد بررسی قرار می‌دهیم.

الف-۱ فضاهای برداری

تعریف الف- ۱ (فضای برداری)

فرض کنیم F یک میدان باشد. گروه آبلی $(V,+)$ همراه با ضرب اسکالر

$$F \times V \to V$$

$$(a,x) \mapsto ax$$

یک **فضای برداری** روی میدان F نامیم اگر برای هر $x,y \in V$ و $a,b \in F$ داشته باشیم:

(۱) $a(x+y) = ax + ay$،

(۲) $(a+b)x = ax + bx$،

(۳) $a(bx) = (ab)x$،

(۴) $1_F x = x$.

مثال۱: فرض کنیم $F \subseteq K$ دو میدان باشند. دراین‌صورت K یک فضای برداری روی میدان F است.

□

مثال۲: فرض کنیم F یک میدان و n یک عدد طبیعی باشد. دراین‌صورت

$$F^n = \{(a_1, a_2, ..., a_n) \mid a_i \in F\}$$

همراه جمع و ضرب اسکالر زیر

$$(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n) = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n),$$
$$c(a_1, a_2, ..., a_n) = (ca_1, ca_2, ..., ca_n).$$

یک فضای برداری روی میدان F است.

□

مثال۳: فرض کنیم F یک میدان باشد. مجموعه‌ی ماتریس‌های $m \times n$ روی میدان F، $M_{m\times n}(F)$، تحت اعمال جمع و ضرب اسکالری که برای $A,B \in M_{m\times n}(F)$ و $c \in F$ به ازای هر $1 \le i \le m$ و $1 \le j \le n$ به‌صورت

$$(A+B)_{ij} = A_{ij} + B_{ij} \quad \text{و} \quad (cA)_{ij} = cA_{ij}$$

تعریف می‌شوند، یک فضای برداری روی میدان F است.

□

مثـال ۴: فـرض کنیـد X یـک مجموعـه و F یـک میـدان باشـد. فـرض کنیـد کـه $\mathrm{Map}(X,F)$، مجموعه‌ی توابع از X به F را نشـان دهـد. مجموعـه‌ی $\mathrm{Map}(X,F)$، تحت اعمال جمع و ضرب اسکالری که برای هر $f,g \in \mathrm{Map}(X,F)$ و $c \in F$، به‌صورت

$$(f+g)(x) = f(x) + g(x),$$
$$(cf)(x) = cf(x),$$

تعریف می‌شوند، یک فضای برداری روی میدان F است.

این اعمال همان اعمال جمع و ضرب اسکالر توابع هسـتند کـه در حسـاب دیفرانسـیل مورد استفاده قرار می‌گیرند.

□

مثال۵: فرض کنیم F یک میدان و $F[x]$ مجموعـه‌ی چنـدجملـه‌ای‌هـا بـا ضـرایبی از میدان F باشد. فرض کنیم $c \in F$ و $f(x), g(x)$ دو عنصر دلخـواه از $F[x]$ باشـند. بـدون این‌که از کلیت کاسته شود می‌توان فرض کرد $n \geq m$ و

$$f(x) = a_0 + \cdots + a_m x^m + \cdots + a_n x^n,$$
$$g(x) = b_0 + \cdots + b_m x^m,$$

دراین‌صورت $F[x]$ تحت اعمال جمع و ضرب اسکالر

$$f(x) + g(x) = (a_0 + b_0) + \cdots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_n x^n,$$
$$cf(x) = ca_0 + \cdots + ca_{n-1}x^{n-1} + ca_n x^n,$$

یک فضای برداری روی میدان F است.

□

قضیه الف- ۱

فرض کنید V یک فضای برداری روی میدان F، $x \in V$ و $c \in F$. در این‌صورت:

(1) $c0 = 0$،

(۲) $0x = 0$،

(۳) $(-1)x = -x$،

(۴) اگر $cx = 0$ در این صورت $c = 0$ یا $x = 0$.

اثبات: تنها قسمت (۱) را ثابت می‌کنیم بقیه‌ی قسمت‌ها را به‌عهده خواننده واگذار می‌کنیم. داریم:

$$c0 + c0 = c(0 + 0) = c0$$

لذا طبق قانون حذف در گروه آبلی $(V,+)$، داریم $c0 = 0$.

■■■

تعریف الف- ۲

زیر مجموعه‌ی W از فضای برداری V(روی میدان F) را یک زیر فضای V می‌نامیم اگر W همراه با اعمال جمع و ضرب اسکالر V، خود یک فضای برداری باشد.

برای این‌که W یک زیرفضای Vباشد، کافی است نشان دهیم که نسبت به اعمال جمع و ضرب اسکالر بسته است، زیرا سایر شرایط از V به W به ارث می‌رسند. برقراری بسته بودن دو عمل را می‌توان در یک شرط خلاصه کرد.

قضیه الف- ۲

زیر مجموعه‌ی ناتهی W از فضای برداری V(روی میدان F)، زیر فضاست اگر و تنها اگر برای هر $x_1, x_2 \in W$ و هر $c_1, c_2 \in F$ داشته باشیم:

$$c_1x_1 + c_2x_2 \in W.$$

اثبات: اگر W زیر فضا باشد برقراری این شرط بدیهی است. به‌عکس فرض کنید برای هر $x_1, x_2 \in W$ و هر $c_1, c_2 \in F$ داشته باشیم، $c_1x_1 + c_2x_2 \in W$. اگر $c_2 = 0$، آن‌گاه برای هر $x_1 \in W$ و هر $c_1 \in F$ داریم $c_1x_1 \in W$. یعنی W نسبت به عمل ضرب اسکالر بسته است. هم‌چنین اگر $c_1 = c_2 = 1$، آن‌گاه برای هر $x_1, x_2 \in W$ داریم $x_1 + x_2 \in W$. یعنی W نسبت به عمل جمع بسته است. بنابراین W یک زیر فضای V است.

■■■

مثال۶: در هر فضای برداری V, V و $\{0\}$ زیر فضا هستند.

□

مثال ۷: در فضای برداری $\mathbb{R}^3$ هر صفحه‌ی گذرنده از مبدأ یک زیر فضای $\mathbb{R}^3$ است.

حل: فرض کنیم W یک صفحه‌ی گذرنده از مبدأ باشد. دراین‌صورت عناصر $a,b,c \in \mathbb{R}$ موجودند که

$$W = \{(x,y,z) : ax + by + cz = 0\}$$

حال اگر $X_1 = (x_1,y_1,z_1) \in W$ و $X_2 = (x_2,y_2,z_2) \in W$ و $c_1,c_2 \in \mathbb{R}$، آن‌گاه

$$a(c_1x_1 + c_2x_2) + b(c_1y_1 + c_2y_2) + c(c_1z_1 + c_2z_2) =$$
$$c_1(ax_1 + by_1 + cz_1) + c_2(ax_2 + by_2 + cz_2) = 0 + 0 = 0$$

لذا $c_1X_1 + c_2X_2 = (c_1x_1 + c_2x_2, c_1y_1 + c_2y_2, c_1z_1 + c_2z_2) \in W$ و در نتیجه W زیر فضاست.

□

مثال ۸: مجموعه‌ی جواب‌های این دستگاه m معادله، n مجهولی، همگن $Ax = 0$ زیر فضایی از $\mathbb{R}^n$ است. مجموعه‌ی جواب‌های دستگاه به‌صورت $W = \{x \in \mathbb{R}^n : Ax = 0\}$ است. W ناتهی است، چون $0 \in W$. اگر $x_1,x_2 \in W$ و $c_1,c_2 \in \mathbb{R}$، آن‌گاه

$$A(c_1x_1 + c_2x_2) = c_1Ax_1 + c_2Ax_2 = 0 + 0 = 0.$$

□

گزاره الف- ۱

فرض کنیم U و W دو زیر فضا از فضای برداری V (روی میدان F) باشند. دراین‌صورت

(۱) $U \cap W$ یک زیر فضای V است،

(۲) $U + W := \{x + y \mid x \in U, y \in W\}$ یک زیر فضای V است.

اثبات (۱): چون $0 \in U \cap W$، پس $U \cap W \neq \varnothing$. حال فرض کنیم $x_1,x_2 \in U \cap W$ و $c_1,c_2 \in F$. دراین‌صورت $c_1x_1 + c_2x_2 \in U$ و $c_1x_1 + c_2x_2 \in W$. بنابراین $c_1x_1 + c_2x_2 \in U \cap W$. ازاین‌رو $U \cap W$ زیر فضای V است.

(۲) چون $0 = 0 + 0 \in U + W$، پس $U + W \neq \varnothing$. حال فرض کنیم $x, y \in U + W$ و $a, b \in F$. دراین‌صورت عناصر $u_1, u_2 \in U$ و $w_1, w_2 \in W$ موجودند به‌طوری‌که $x = u_1 + w_1$ و $y = u_2 + w_2$. بنابراین

$$ax + by = a(u_1 + w_1) + b(u_2 + w_2) = (au_1 + bu_2) + (aw_1 + bw_2) \in U + W.$$

ازاین‌رو $U + W$ زیر فضای V است.

■■■

نمادگذاری: اگر U و W دو زیر فضا از فضای برداری V باشند که $U \cap W = \{0\}$، آن‌گاه $U + W$ را با نماد $U \oplus W$ نمایش داده و آن‌را **جمع مستقیم** دو زیر فضای U و W می‌نامیم.

الف-۲ پایه

تعریف الف- ۳

فرض کنید V فضایی برداری و X یک زیرمجموعه‌ی ناتهی از V باشد. بردار $v \in V$ را **ترکیبی خطی** از اعضای X نامند، هرگاه تعدادی متناهی عضو از X مانند $x_n, \ldots, x_2, x_1$ و تعداد متناهی اسکالر در F، مانند $a_n, \ldots, a_2, a_1$ موجود باشد که $v = a_1x_1 + a_2x_2 + \cdots + a_nx_n$. در این حالت می‌گوییم که v ترکیبی خطی از $x_n, \ldots, x_2, x_1$ است و $a_n, \ldots, a_2, a_1$ را **ضرایب ترکیب خطی** می‌نامیم.

مثال ۹: فرض کنیم $x = (1,2,-1)$ و $y = (3,2,1)$ بردارهایی در $\mathbb{R}^3$ باشند. نشان می‌دهیم $z = (9,2,7)$ ترکیبی خطی از x, y است و هم‌چنین $z' = (4,-1,8)$ ترکیبی خطی از x و y نیست.

برای این‌که نشان دهیم z ترکیب خطی x و y است، باید اسکالرهای c_1 و c_2 را طوری بیابیم که

$$z = c_1x + c_2y.$$

بنابراین

$$(9,2,7) = c_1(1,2,-1) + c_2(3,2,1) = \left(c_1 + 3c_2, 2c_1 + 2c_2, -c_1 + 1c_2\right)$$

با مساوی قرار دادن مؤلفه‌ها به دستگاه زیر می‌رسیم

$$\begin{cases} c_1 + 3c_2 = 9 \\ 2c_1 + 2c_2 = 2 \\ -c_1 + c_2 = 7 \end{cases}$$

که جواب آن $c_1 = -3$ و $c_2 = 4$ است. در واقع

$$z = -3x + 2y$$

به طور مشابه اگر z' بخواهد ترکیب خطی x و y باشد، باید c_1 و c_2ای موجود باشد که $z' = c_1x + c_2y$. این رابطه دستگاه زیر را نتیجه می‌دهد

$$\begin{cases} c_1 + 6c_2 = 4 \\ 2c_1 + 4c_2 = -1 \\ -c_1 + 2c_2 = 8 \end{cases}$$

که این دستگاه دارای جواب نیست، ازاین‌رو z' ترکیب خطی x و y نیست.

□

تعریف الف- ۴

فرض کنیم X یک زیر مجموعه ناتهی از فضای برداری V باشد. منظور از **زیر فضای تولید شده** از X که با $< X >$ نشان داده می‌شود، مجموعه‌ی تمام ترکیبات خطی اعضای X است. اگر $X = \{v_1, \ldots, v_n\}$، $< X >$را با نماد $< v_1, \ldots, v_n >$ نمایش می‌دهیم. هم‌چنین $< \varnothing >$ را $\{0\}$ تعریف می‌کنیم.

قضیه الف- ۳

فرض کنیم X یک زیر مجموعه‌ی ناتهی از فضای برداری Vباشد. دراین‌صورت

(۱): $< X >$، زیر فضایی از V است.

(۲): $< X >$ کوچک‌ترین زیر فضای V شامل X است.

اثبات: مجموعه‌ی X ناتهی است، لذا عنصری مانند x دارد. پس $0x = 0$ عنصری از $< X >$است. فرض کنیم $x, y \in < X >$، دراین‌صورت، عناصر $x_1, x_2, ..., x_m$ و $y_1, y_2, ..., y_n$ در X و اسکالرهای $a_1, a_2, ..., a_m$ و $b_1, b_2, ..., b_n$ موجودند که:

$$x = a_1x_1 + a_2x_2 + \cdots + a_mx_m,$$
$$v = b_1y_1 + b_2y_2 + \cdots + b_ny_n.$$

بنابراین، به ازای اسکالرهای $c_1, c_2 \in F$ عنصر

$$c_1x + c_2y = (c_1a_1)x_1 + \cdots + (c_1a_m)x_m + (c_2b_1)y_1 + \cdots + (c_2b_n)y_n.$$

متعلق به $< X >$ هستند. لذا $< X >$ زیر فضایی از V است.

اکنون فرض کنیم W زیر فضای دلخواهی از V باشد که $X \subseteq W$. اگر $w \in < X >$، آن‌گاه به ازای عناصری از X مانند $w_1, w_2, ..., w_k$ و اسکالرهایی چون $c_1, c_2, ..., c_k$، داریم $w = c_1w_1 + \cdots + c_kw_k$. چون $X \subseteq W$، پس $w_1, w_2, ..., w_k \in W$. و چون W زیرفضا است لذا $w \in W$. بنابراین $< X > \subseteq W$. ازاین‌رو $< X >$ کوچک‌ترین زیر فضای V شامل X است.

■■■

تعریف الف- ۵

فرض کنیم X یک زیر مجموعه‌ی ناتهی از فضای برداری V باشد که $< X > = V$. دراین‌صورت X را **مولد فضای** V می‌نامیم و می‌گوییم X، V را **تولید می‌کند.**

تعریف الف- ۶

زیر مجموعه‌ی X از فضای برداری V(روی میدان F) را یک زیر مجموعه‌ی **مستقل خطی** نامیم اگر برای هر $x_1, x_2, ..., x_n \in X$ و هر $c_1, c_2, ..., c_n \in F$ داشته باشیم:

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n = 0 \Rightarrow c_1 = c_2 = \cdots = c_n = 0.$$

تعریف الف- ۷

فرض کنیم V یک فضای برداری روی میدان F باشد. زیر مجموعه‌ی $\mathcal{B}$ از V را یک **پایه** برای V گوییم اگر $\mathcal{B}$ مستقل خطی بوده و $\mathcal{B}$ مولدی برای V باشد.

مثال۱۰: فرض کنیم $\mathbb{C}$ فضای برداری میدان اعداد مختلط روی میدان اعداد حقیقی $\mathbb{R}$ باشد. فرض کنید $(a,b) \in \mathbb{C}$. دراین صورت داریم

$$(a,b) = a + bi$$

این رابطه نشان می‌دهد که $\mathbb{C} = < 1, i >$ لذا مجموعه‌ی $\mathcal{B} = \{1, i\}$ مولد $\mathbb{C}$ است. حال فرض کنیم عناصر $c_1, c_2 \in \mathbb{R}$ موجود باشند به‌قسمی که $c_1 1 + c_2 i = 0$. ازاین‌رو

$$c_1 1 + c_2 i = (c_1, c_2) = (0,0)$$

لذا $c_1 = c_2 = 0$؛ یعنی $\mathcal{B}$ یک مجموعه‌ی مستقل خطی است و درنتیجه $\mathcal{B}$ یک پایه $\mathbb{C}$ است.

□

مثال۱۱: فرض کنیم $e_i \in F^n$ نشان دهنده برداری باشد که i امین مختص یک است و سایر مختصاتش صفرند. فرض کنید $(a_1, a_2, ..., a_n) \in F^n$ در این صورت داریم

$$\begin{aligned}(a_1, a_2, ..., a_n) &= (a_1, 0, 0, ..., 0) + (0, a_2, 0, ..., 0) + ... + (0, ..., 0, a_n) \\ &= a_1 e_1 + a_2 e_2 + ... + a_n e_n\end{aligned}$$

این رابطه نشان می‌دهد که $F^n = < e_1, e_2, ..., e_n >$ لذا مجموعه‌ی $\mathcal{B} = \{e_1, e_2, ..., e_n\}$ مولد F^n است. حال فرض کنیم عناصر $c_1, c_2, ..., c_n \in F$ موجود باشند به‌قسمی که $c_1 e_1 + c_2 e_2 + \cdots + c_n e_n = 0$. ازاین‌رو

$$c_1 e_1 + c_2 e_2 + \cdots + c_n e_n = (c_1, c_2, ..., c_n) = (0, 0, ..., 0)$$

لذا $c_1 = c_2 = \cdots = c_n = 0$؛ یعنی $\mathcal{B}$ یک مجموعه‌ی مستقل خطی است و درنتیجه $\mathcal{B}$ یک پایه F^n است.

□

مثال۱۲: فرض کنیم F یک میدان و $E_{ij} \in M_{m\times n}(F)$ ماتریسی $m \times n$ باشد که در درایه (i,j) ام 1 و در بقیه‌ی درایه‌ها صفر است. اگر $A = [a_{ij}]_{m\times n}$ دراین‌صورت رابطه‌ی زیر را داریم:

$$A = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}E_{ij}$$

از این نتیجه می‌شود مجموعه‌ی $\mathcal{B}=\{E_{ij} | 1 \le i \le m, 1 \le j \le n\}$ مولد فضای $M_{m\times n}(F)$ است. حال فرض کنیم عناصر $c_{ij} \in F$ که $1 \le i \le m, 1 \le j \le n$، موجود باشند به‌قسمی که $\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}E_{ij} = 0$. ازاین‌رو

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}E_{ij} = (c_{ij}) = 0$$

لذا برای هر $1 \le i \le m, 1 \le j \le n$، داریم $c_{ij} = 0$؛ یعنی $\mathcal{B}$ یک مجموعه‌ی مستقل خطی است و در نتیجه $\mathcal{B}$ یک پایه $M_{m\times n}(F)$ است.

□

اکنون نشان می‌دهیم که هر فضای برداری دارای یک پایه است.

قضیه الف- ۴

فرض کنیم V یک فضای برداری روی میدان F باشد. اگر $C \subseteq D$ زیر مجموعه‌هایی از V باشند که C مستقل خطی و D فضای V را تولید کند، آن‌گاه پایه $\mathcal{B}$ موجود است به‌طوری‌که $C \subseteq \mathcal{B} \subseteq D$.

اثبات: قرار می‌دهیم:

$$\Omega = \{E \mid C \subseteq E \subseteq D, E \text{ مستقل خطی است}\}.$$

Ω ناتهی است، زیرا $C \in \Omega$، و با رابطه‌ی شمول یک مجموعه‌ی جزئی مرتب است. حال نشان می‌دهیم که شرایط لم زرن برقرار است.

فرض کنیم

$$E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n \subseteq \cdots$$

یک زنجیر صعودی از عناصر Ω باشد. اگر $A=\bigcup_i E_i$، آن‌گاه به‌وضوح $A\in\Omega$ و A یک کران بالا برای عناصر این زنجیر است. بنابراین طبق لم زرن Ω دارای عنصری ماکزیمال مانند B است. نشان می‌دهیم که $\mathcal{B}$ یک پایه برای V است. چون $\mathcal{B}\in\Omega$، پس $\mathcal{B}$ مستقل خطی است. ثابت می‌کنیم $D\subseteq<\mathcal{B}>$. (فرض خلف) فرض کنیم عنصر $v\in D$ موجود باشد به‌طوری‌که $v\notin<\mathcal{B}>$. دراین‌صورت v ترکیب خطی عناصر $\mathcal{B}$ نبوده و لذا $\mathcal{B}\cup\{v\}$ مستقل خطی است. علاوه بر این $\mathcal{B}\cup\{v\}\subseteq D$، که تناقض با ماکزیمال بودن $\mathcal{B}$ است. ازاین‌رو $D\subseteq<\mathcal{B}>$. درنتیجه $V=<D>=<\mathcal{B}>$ و بدین ترتیب قضیه اثبات است.

■■■

در ادامه نشان خواهیم داد که تعداد عناصر هر دو پایه از یک فضای برداری، برابرند. ابتدا لم زیر را مطرح می‌کنیم.

لم الف- ۱

فرض کنیم $m>n$ و $\{u_1,u_2,...,u_n\}$ و $\{v_1,v_2,...,v_m\}$ زیر مجموعه‌هایی از فضای برداری V باشند. اگر $\{v_1,v_2,...,v_m\}\subseteq<u_1,u_2,...,u_n>$، آن‌گاه $\{v_1,v_2,...,v_m\}$ وابسته‌ی خطی است.

اثبات: مطلب را با استقرا روی $n\geq 1$ ثابت می‌کنیم. فرض کنیم $n=1$ و $\{v_1,v_2,...,v_m\}\subseteq<u_1>$. دراین‌صورت $m\geq 2$ و درنتیجه عناصر $c_1,c_2\in F$ موجودند که $v_1=c_1u_1$ و $v_2=c_2u_1$. اگر $c_1=0$، آن‌گاه $v_1=0$ و حکم برقرار است. بنابراین فرض کنیم $c_1\neq 0$. دراین‌صورت $v_2-c_2c_1^{-1}v_1=0$؛ یعنی $\{v_1,v_2,...,v_m\}$ وابسته‌ی خطی است. حال فرض کنیم $\{v_1,v_2,...,v_m\}\subseteq<u_1,u_2,...,u_n>$. داریم

$$\begin{aligned}
v_1 &= c_{11}u_1+\cdots+c_{1n}u_n\\
v_2 &= c_{21}u_1+\cdots+c_{2n}u_n\\
&\vdots\\
v_m &= c_{m1}u_1+\cdots+c_{mn}u_n
\end{aligned}$$

اگر برای هر $1 \leq i \leq m$، $c_{i1} = 0$ آن‌گاه $\{v_1, v_2, ..., v_m\} \subseteq < u_2, ..., u_n >$ و لذا طبق فرض استقرا حکم برقرار است. ازاین‌رو فرض کنیم $1 \leq i \leq m$ موجود است که $c_{i1} \neq 0$. بدون این‌که از کلیت کاسته شود می‌توان فرض کرد $c_{11} \neq 0$. برای هر $i \geq 2$، تعریف می‌کنیم:

$$w_i = v_i - c_{i1}c_{11}^{-1}v_1 \in < u_2, ..., u_n >$$

(ضریب u_1 در w_i برابر $c_{i1} - (c_{i1}c_{11}^{-1})c_{11}u_1 = 0$ است). چون $m - 1 > n - 1$، طبق فرض استقرا، عناصر $d_2, ..., d_m \in F$ که همگی صفر نیستند موجودند که

$$d_2w_2 + \cdots + d_mw_m = 0,$$

ودر نتیجه با جایگذاری w_i، داریم:

$$(-\sum_{i\geq 2} d_ic_{i1}c_{11}^{-1})v_1 + d_2v_2 + \cdots + d_mv_m = 0,$$

یعنی $\{v_1, v_2, ..., v_m\}$ وابسته‌ی خطی است. بدین ترتیب قضیه اثبات است.

■■■

نتیجه الف- ۱

فرض کنیم $\mathcal{B} = \{u_1, u_2, ..., u_n\}$ یک پایه‌ی متناهی برای فضای برداری V روی میدان F باشند. اگر $\mathcal{C}$ یک پایه دیگری برای V باشد، آن‌گاه $\mathcal{C}$ متناهی است و $|\mathcal{C}| = |\mathcal{B}|$.

اثبات: ابتدا نشان می‌دهیم که $\mathcal{C}$ متناهی است. (برهان خلف) فرض کنیم $\mathcal{C}$ متناهی نباشد. فرض کنیم $m > n$ و $\{v_1, v_2, ..., v_m\} \subseteq \mathcal{C}$. دراین‌صورت، طبق لم اخیر $\{v_1, v_2, ..., v_m\}$ وابسته‌ی خطی است که تناقض است. بنابراین $\mathcal{C}$ متناهی است. چون $\mathcal{B} \subseteq < \mathcal{C} >$ پس طبق قضیه‌ی اخیر $|\mathcal{C}| \leq |\mathcal{B}|$. به‌طریق مشابه $|\mathcal{C}| \geq |\mathcal{B}|$. درنتیجه $|\mathcal{C}| = |\mathcal{B}|$.

■■■

قضیه الف- ۵

فرض کنیم $\mathcal{B}$ و $\mathcal{C}$ دو پایه‌ی برای فضای برداری V روی میدان F باشند. دراین‌صورت $|\mathcal{B}|=|\mathcal{C}|$.

اثبات: اگر یکی از $\mathcal{B}$ و $\mathcal{C}$ متناهی باشد، آن‌گاه طبق نتیجه‌ی اخیر حکم برقرار است. بنابراین فرض می‌کنیم $\mathcal{B}$ و $\mathcal{C}$ هر دو نامتناهی باشند. برای هر $y_i \in \mathcal{C}$ داریم، $y_i = \sum_j c_{ij}x_j$ که $x_j \in \mathcal{B}$. فرض کنیم

$$\mathcal{B}_i = \{x_j \mid c_{ij} \neq 0\}$$

چون هر عنصر $\mathcal{C}$ ترکیب خطی عناصر $\bigcup_i \mathcal{B}_i$ است، $< \bigcup_i \mathcal{B}_i >= V$. از طرفی $\bigcup_i \mathcal{B}_i \subseteq \mathcal{B}$ و $\mathcal{B}$ پایه‌ای برای V است، پس $\bigcup_i \mathcal{B}_i = \mathcal{B}$.

چون $\mathcal{B}_i$ متناهی است، پس $|\mathcal{B}_i| \leq \aleph_0$ و در نتیجه با اجتماع گرفتن روی عناصر $\mathcal{C}$، و با توجه به نامتناهی بودن $\mathcal{C}$ داریم

$$|\mathcal{B}| = |\bigcup_i \mathcal{B}_i| \leq \aleph_0 |\mathcal{C}| = |\mathcal{C}|$$

با تعویض $\mathcal{B}$ و $\mathcal{C}$، خواهیم داشت $|\mathcal{C}| \leq |\mathcal{B}|$. در نتیجه $|\mathcal{B}| = |\mathcal{C}|$.

■■■

تعریف الف- ۸

تعداد بردارهای یک پایه از فضای برداری V روی میدان F را **بعد فضای** V تعریف می‌کنیم و آن را با $\dim_F V$ نشان می‌دهیم. فضای برداری صفر را صفر بعدی می‌نامیم.

◆ **تذکر:** در صورتی که جای هیچ‌گونه ابهامی نباشد، برای راحتی کار، از نوشتن اندیس F در $\dim_F V$ صرف‌نظر می‌کنیم.

مثال۱۳ : با توجه به مثال‌های ۱۰و۱۱و۱۲ خواهیم داشت:

$$\dim_{\mathbb{R}} \mathbb{C} = 2,$$
$$\dim_F F^n = n,$$
$$\dim_F M_{m\times n}(F) = mn.$$

□

من در حل مسئله شکست نخورده‌ام، فقط ده هزار روش پیدا کرده‌ام که هیچ کدام کارایی ندارند.

(ادیسون)

تمرین‌های سطح۱

۱- فرض کنید $f_1 = (1,0,...,0)$ ، $f_2 = (1,1,0,...,0)$ و $f_n = (1,1,...,1)$. نشان دهید که مجموعه‌ی $B = \{f_1,...,f_n\}$ یک پایه برای فضای برداری F^n روی میدان F است.

۲- فرض کنید F یک میدان و $P_n[x] = \{f \in F[x] \mid \deg f(x) \le n\}$.

(الف) نشان دهید $P_n[x]$ یک زیر فضا از $F[x]$ است،

(ب) نشان دهید $B = \{1, x, ..., x^n\}$ یک پایه برای $P_n[x]$ است،

(ج) اگر $B = \{f_0, f_1, ..., f_n\}$ که $\deg f_i = i$، نشان دهید B یک پایه برای $P_n[x]$ است.

۳- فرض کنید W_1 و W_2 دو زیر فضا از فضای برداری V باشند. نشان دهید $W_1 \cup W_2$ یک زیر فضای V است اگر و فقط اگر $W_1 \subseteq W_2$ یا $W_2 \subseteq W_1$.

۴- فرض کنید V و W دو فضای برداری روی میدان F باشند. تابع $T : V \to W$ یک **تبدیل خطی** نام دارد اگر برای هر $x, y \in V$ و هر $c \in F$ داشته باشیم:

$$T(cx + y) = cT(x) + T(y).$$

فرض کنید $T : V \to W$ یک تبدیل خطی باشد و

$$\mathrm{Im}\,T = T \textbf{ تصویر} = \{T(x) \mid x \in V\},$$

$$\mathrm{Ker}\,T = T \textbf{ هسته} = \{x \in V \mid T(x) = 0\}.$$

(الف) نشان $\mathrm{Im}\,T$ دهید یک زیر فضا از W است،

(ب) نشان دهید $\mathrm{Ker}\,T$ یک زیر فضا از V است،

۵- فرض کنید $T : V \to W$ یک تبدیل خطی باشد. نشان دهید T یک‌به‌یک است اگر و فقط اگر $\mathrm{Ker}\,T = \{0\}$.

۶- فرض کنید V یک فضای برداری و $T : V \to V$ یک تبدیل خطی باشد که $T^2 = T$. نشان دهید

$$\mathrm{V} = \mathrm{Im}\,T \oplus \mathrm{Ker}\,T.$$

۷- فرض کنید V یک فضای برداری با بعد متناهی باشد. اگر W یک زیر فضای سره از V باشد، نشان دهید $\dim W < \dim V$.

تمرین‌های سطح ۲

۸- فرض کنید V و W دو فضای برداری و $T : V \to V$ یک تبدیل خطی باشد. نشان دهید:

$$\mathrm{dimV} = \mathrm{dim}\,\mathrm{Im}\,T + \mathrm{dimKer}\,T.$$

۹- فرض کنید W_1 و W_2 دو زیر فضا با بعد متناهی از فضای برداری V باشند. نشان دهید:

$$\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2).$$

۱۰-فرض کنید V یک فضای برداری با بعد متناهی و $T : V \to V$ یک تبدیل خطی باشد. نشان دهید عدد طبیعی n موجود است که

$$\mathrm{V}=\mathrm{Im}\,T^n \oplus \mathrm{Ker}\,T^n.$$

۱۱- فرض کنید F یک میدان و n عددی طبیعی باشد. تابع Tr **(اثر)** به‌صورت زیر تعریف می‌شود:

$$\mathrm{Tr} : M_n(F) \to F_n$$
$$(a_{ij}) \mapsto a_{11} + \cdots + a_{nn}$$

یعنی $\mathrm{Tr}(A)$ جمع عناصر قطر اصلی ماتریس A است.

(الف) نشان دهید برای هر دو عنصر $A, B \in M_n(F)$ داریم $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

(ب) فرض کنید $T : M_n(F) \to F_n$ یک تبدیل خطی باشد که به ازای هر $A, B \in M_n(F)$ داشته باشیم $T(AB) = T(BA)$. نشان دهید T مضرب اسکالری از تابع Tr است. بعلاوه اگر $T(I) = n$، نشان دهید $T = \mathrm{Tr}$.

۱۲- فرض کنید F یک میدان و n عددی طبیعی باشد. قرار می‌دهیم:

$$W = \{A \in M_n(F) : \mathrm{Tr}(A) = 0\}.$$

(الف) نشان دهید W یک زیر فضا از $M_n(F)$ است،

(ب) نشان دهید $\dim W = n^2 - 1$.

۱۳- فرض کنید V یک فضای برداری روی میدان نامتناهی F و $W, W_1, \ldots, W_n$ زیر فضاهایی از V باشند که $W \subseteq W_1 \cup \ldots \cup W_n$، نشان دهید $1 \le i \le n$ موجود است که $W \subseteq W_i$.

تمرین‌های سطح ۳

۱۴- فرض کنید W_1 و W_2 دو زیر فضا از فضای برداری V که $\dim(W_1) = \dim(W_2)$ باشند. نشان دهید زیر فضای U از V موجود است به‌طوری‌که

$$U \oplus W_1 = U \oplus W_2.$$

۱۵- فرض کنید V یک فضای برداری با بعد متناهی روی میدان F باشد. اگر $\{V_i\}_{i\in I}$ مجموعه‌ای از زیرفضاهای سرهٔ V باشد به‌طوریکه $\dim V_i = \dim V_j$ به ازای هر $i,j \in I$ و اگر $|I| < |F|$، ثابت کنید یک زیرفضای سره چون U وجود دارد به‌قسمی‌که

$$\forall i \in I: \quad V = V_i \oplus U.$$

۱۶- فرض کنید $A_n,...,A_2,A_1$ ماتریس‌هایی $m\times m$ و دو به دو تعویض‌پذیر باشند به‌طوری‌که $A_i^2 = 0$ برای هر i. اگر $m < 2^n$، ثابت کنید $A_1A_2...A_n = 0$.

۱۷- نشان دهید برای هر ماتریس $n\times n$ مانند A، ماتریس $n\times n$ای مانند B وجود دارد به‌طوریکه AB خودتوان است.

۱۸- فرض کنید A یک ماتریس $m\times n$ و B یک ماتریس $n\times m$ باشند که $n \neq m$. نشان دهید حداقل یکی از دو ماتریس AB و BA وارون‌پذیر نیست.

۱۹- فرض کنید V یک فضای برداری روی میدان F باشد. قرار می‌دهیم:

$$\mathrm{GL}(V) := \{T \mid T: V \to V \text{ یک تبدیل خطی دوسوئی باشد}\}.$$

$\mathrm{GL}(V)$ با عمل ترکیب توابع تشکیل یک گروه می‌دهد که به **گروه خطی عام** V معروف است. اگر $|F| = q$ و V یک فضای برداری n بعدی باشد، نشان دهید:

$$|\mathrm{GL}(V)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}).$$

منابعی برای مطالعه‌ی بیشتر

۱. اونان، م. **جبر خطی**. ترجمه محمدی حسن آبادی، علی اکبر. مرکز نشر دانشگاهی تهران (۱۳۷۰).

۲. هافمن، ک.، کنز، ر. **جبر خطی**. ترجمه فرشیدی، جمشید. مرکز نشر دانشگاهی تهران (۱۳۶۵).

3. Baker, R. *Linear Algebra*, Rinton Press, 2001.

4. Lang, S. *Introduction to Linear Algebra*, 2nd ed., New York: Springer-Verlag, 1986.

5. Proskuryakov, I. V. *Problems in Linear Algebra*, Moscow: Mir Publishers, 1978.

6. Shores, T. S. *Applied Linear Algebra and Matrix Analysis*. Springer-Verlag, New York, 2007.

پیوست ب

زندگی‌نامه

در این قسمت می‌خوانیم:

مقدمه

براین باوریم که هر انسان، معجزه‌ای است که خود می‌تواند، معجزه بیافریند. هنگامی که انسان، بر خویشتن خویش، ایمان بیاورد و هر چیز مقدسی را که در وجودش نهفته است، متبلور نماید، معجزه آفریده است.
دانش ریاضی، از مقدس چیزهایی است که انسان‌های زیادی را به آفرینش معجزه بر انگیخته است. **گاوس، آبل** و **گالوا**، از جمله معجزاتی هستند که در این دانش مقدس، اعجازهای جاودانه‌ای خلق کردند و قلب همه انسان‌های معجزه شناس عاشق ریاضیات را، تا ابدیت تسخیر نمودند.

ب-۱ زندگی نامه گاوس

شاه‌زاده‌ی ریاضی‌دانان

شاه‌زاده‌ی همه‌ی ریاضی‌دانان تاریخ، **کارل فردریش گاوس** است؛ فاخرترین ریاضی‌دانی که با نبوغش، ریاضیات را به مرحله‌ی جدیدی وارد کرد. او کسی است که با شکوه‌ترین تاج را برسر حساب عالی نهاد و آن را «ملکه‌ی ریاضیات» نامید، تا خود نیز «شاه‌زاده‌ی ریاضی‌دانان» باشد. گرچه او به شاه‌زاده ریاضی‌دانان شهره است؛ لیکن، در

یک خانواده‌ی فقیر، در خانه‌ای محقر، در شهر برونسویک،از شهرهای آلمـان، بـه تـاریخ ۳۰ آوریل ۱۷۷۷ میلادی، خورشید زندگی‌اش طلوع کرد و تابیدن گرفت.

پدرش **گرهارت دیدریش**، مردی بود کـه در راسـتی و شـرافت، بـه درجـه‌ی وسـواس رسیده بود؛ اما، شگفت آن‌که بر گاوس به شدت سخت‌گیری می‌کرد و با تمام وجـود، بـا درس خواندن پسر نابغه‌اش مخـالف بـود! جـای نیـک‌بختـی بـود کـه در مقابـل پـدری این‌چنین، که مانع بزرگی بر سر راه درس خواندن گاوس بود، **دوروته بنز**، مادرش قـرار داشت که علاوه بر پاکی و نجابت، بسیار روشن فکر بود. دوروته همواره پشتیبان پسـرش بود و برای این‌که او درس بخواند، شجاعانه رو در روی شوهرش ایستاد.

گاوس، اولین نشانه‌های نبوغ خود را، قبل از سه سالگی بـروز داد؛ روزی پـدرش درحـال تنظیم اوراق پرداخت حقوق کارگران زیر دستش بود؛ بی آن‌که متوجه باشد پسـرش بـا دقت زیاد محاسباتش را تعقیب می‌کند، هنگام پایان کار دید، پسر خردسالش می‌گویـد: «پدر، حساب تو درست نیست و باید بنویسی ... ». پدر با بررسی دوباره‌ی محاسـبات، در نهایت بهت و حیرت دریافت، عددی که گاوس به‌دست آورده، صحیح است !!

گاوس، هفت ساله بود که راهی مدرسه شد. جایی کـه بـا شـیوه‌هـای وحشـتناک قـرون وسطا اداره می‌شد. دو سال گذشت تا این‌که به کلاس حساب وارد شد. معلم کلاس، آدم بسیار خشنی بود و با دادن مسئله‌های سخت و طولانی به شاگردانش، تفـریح مـی‌کـرد! روزی از آن‌ها محاسبه‌ی مجموع

$$۱۰۰۸۹۹ + ... + ۸۱۶۹۳ + ۸۱۴۹۵ + ۸۱۲۹۷$$

را می‌خواست که در آن، اختلاف هر دو جمله‌ی متوالی ۱۹۸ و تعداد جملـه‌هـایش صـد تاست. هنوز معلم، صورت مسئله را تمام نکرده بود که گـاوس بـر لـوح خـود یـک عـدد نوشت و آن را به معلم نشان داد. معلم شگفت زده، به او خیره مانـد؛ زیـرا عـدد گـاوس، جواب صحیح مسئله بود! این اتفاق نقطه‌ی آغاز جاودانه شدن نام گاوس بود.

از آن پس، گاوس، با علاقه‌ی فراوان، مطالعه‌ی ریاضی را آغاز کرد و در همان ابتـدا، بـه نتایج جالبی دست پیدا کرد. یکی از آن نتایج، حل قاطع قضیه دوجمله‌ای

$$(1+x)^n = 1 + \frac{n}{1}x + \frac{n(n-1)}{1\times 2}x^2 + \frac{n(n-1)(n-2)}{1\times 2\times 3}x^3 + \ldots$$

است که در آن n ، لزوماً عدد صحیح و مثبتی نیست و می‌تواند هر عدد دلخواهی باشد.

اگر nعدد صحیح و مثبت نباشد، سمت راست تساوی ،پایان نمی‌یابد. برای این که معلوم شود، چه وقت این مجموع با $(1+x)^n$ برابر است، باید بر x و nشرایط لازم اعمال شود تا مجموع بالا به حدی معین میل نماید.

تا آن زمان، ریاضی‌دانانی که پیش از گاوس، به آنالیز ریاضی پرداخته بودند، سعی نکرده بودند تا بفهمند که چه شرایطی لازم است تا مجموع‌هایی از این نوع، به حدی معین میل نمایند و چه موقع است که نتیجه‌ی نامعقول حاصل می‌شود. تا این که، گاوس در ابتدای نوجوانی توانست، قضیه‌ی دو جمله‌ای را اثبات کند و همین امر، او را در آنالیز ریاضی، متبحر ساخت.

استعداد خیره‌کننده‌ی گاوس در محاسبات ذهنی، همه را شیفته‌اش کرده بود. یکی از معلمانش، با تلاش زیاد، **کارل ویلهلم فردیناند**، یکی از اشراف زادگان ثروتمند شهر برونسویک را با گاوس آشنا ساخت. فردیناند، جوانمردانه قول داد که همه‌ی مخارج تحصیل گاوس را بپردازد. پشتیبانی مالی این مرد بزرگ منش سبب شد که گاوس، بدون دغدغه و با تمرکز به یافته‌های علمی خویش ادامه دهد. گاوس به پاس قدردانی از فردیناند، اولین کتابش را به این انسان سخاوتمند تقدیم کرد.

گاوس در پانزده سالگی به زبان‌های لاتین و یونانی مسلط بود و به طور عمیق به جستجو در مهم‌ترین آثار **نیوتن**، **اویلر** و **لاگرانژ**، پرداخت. در همین دوره بود که قضیه اعداد اول را کشف کرد. قضیه‌ای که در سال ۱۸۹۶، با تلاش ریاضی‌دانان زیادی، سرانجام اثبات شد. سپس مطالعات خود را در حساب عالی آغاز کرد و در این زمینه، نام خویش را ابدی ساخت. او با کوششی وصف ناپذیر، توانست «جواهر ریاضیات» یا «قضیه طلایی» را کشف کند.

نقطه‌ی شروع کشف قضیه‌ی طلایی که به قانون تقابل مربعی معروف است، این سوال ساده است: «در دوره هر یک از کسرهای متناوب، چند رقم وجود دارد؟». گاوس برای

پاسخ به این سوال، شکل اعشاری تمام کسرهای متعارفی $\frac{1}{n}$ را برای n از یک تا هزار حساب کرد. نتیجه‌ای که به‌دست آورد همین قانون تقابل مربعی است که برای او از صدها گنج، ارزشمندتر بود.

به دلیل ساده بودن این قانون، در ادامه به شرح آن می پردازیم. در ابتدا، مفهومی را معرفی می کنیم که گاوس را به نام گذاری و اصطلاحات حساب وارد کرد و آن مفهوم همنهشنی است.

اگر b,a و m عدد صحیح باشند و تفاضل $a-b$ یا $b-a$ بر m بخش پذیر باشد، می‌گوییم دو عدد a و b پیمانه‌ی m همنهشت هستند و می‌نویسیم $a \equiv b \pmod{m}$.

فلیه این شکل نام گذاری این است که هم، شباهت کامل با طرز نوشتن معادلات جبری دارد و هم، مفهوم بخش پذیری را به صورت دقیق، بیان می کند.

اکنون فرض کنیم، x عدد مجهول و r و m اعدادی معلوم باشند که r بر m بخش پذیر نباشد. دراین‌صورت، r غیر باقی‌مانده‌ی مربعی، به پیمانه‌ی m گوییم، در واقع، اگر r باقی‌مانده‌ی مربعی به پیمانه‌ی m باشد، حداقل باید بتوان عدد x را پیدا کرد چنان که وقتی مربع آن را بر m تقسیم می‌کنیم، باقی‌مانده برابر با r شود.

حال، این سوال مطرح می شود که باقی‌مانده‌ها وغیر باقی‌مانده‌های تربیعی عدد معلوم m کدامند؟ یعنی، اگر در هم نهشتی $x^2 \equiv r \pmod{m}$ عدد m معلوم باشد و مقادیر ۱ ، ۲ ، ۳ ، ... را به جای x بگذاریم، چه عددهایی در r قرار می‌گیرند و چه اعدادی در r قرار نمی‌گیرند؟

کافی است این مسئله را هنگامی که m و r اولند، بررسی کنیم؛ زیرا حالات دیگر، به همین شکل خواهد بود. پس باز می‌پرسیم، اگر p عدد اول معلومی باشد، دراین‌صورت، اعداد اولی چون q که در همنهشتی $x^2 \equiv q \pmod{\text{p}}$ صدق کند، کدام است؟

بین دو همنهشتی $x^2 \equiv q \pmod{\text{p}}$ و $x^2 \equiv p \pmod{\text{q}}$ که p و q اولند، خاصیت متقابل جالبی وجود دارد؛ یا هر دو جواب دارد یا هر دو جواب ندارد. مگر حالتی که

تقسیم دو عدد p و q بر ۴ برابر با ۳ شود. دراین‌صورت، یکی جواب دارد و دیگری ندارد؛ و این، همان قانون تقابل مربعی است.

اثبات این قضیه، آسان نیست؛ اما گاوس، اولین اثبات آن را در نوزده سالگی به دست آورد. خود او بعدها نوشت: «یک سال تمام، این قضیه ذهنم را مشغول کرد تا سرانجام اثباتش نمودم.» به‌دلیل اهمیت زیادی که این قضیه، در حساب عالی و بسیاری از قسمت‌های جبر داشت، مدت‌ها در ذهن گاوس ماند و او توانست شش اثبات متمایز دیگر را برایش پیدا کند. یکی از این اثبات‌ها، به ترسیم هندسی چند ضلعی‌های منتظم، به کمک خط کش و پرگار، مرتبط است.

گاوس، وقتی در هجده سالگی کالج کارولین را ترک کرد تا به دانشگاه گوتینکن، قدم بگذارد، به درستی نمی‌دانست که ریاضیات را دنبال کند یا در زبان‌های گوناگون به مطالعه بپردازد؛ چون علاوه بر این‌که، عاشق ریاضیات بود، به زبان‌های کلاسیک نیز علاقه داشت.

نقطه‌ی عطف نمودار زندگی‌اش، لحظه‌ای به‌دست آمد که توانست با جادوی نبوغش، طلسم ۱۷- ضلعی منتظم را بشکند. شکسته شدن این طلسم باعث شد که گاوس، در روز ۳۰ مارس ۱۷۹۶، غول ریاضیات را به آغوش بکشد و پری زبان‌های کلاسیک را، برای همیشه رها سازد. همان روز دفتری برای یاداشت یافته‌های علمی‌اش برگزید که به یکی از با ارزش ترین اسناد تاریخ ریاضیات بدل گردید.

اولین چیزی که در دفترش ثبت نمود، ترسیم ۱۷− ضلعی منتظم بود. این موضوع، به اندازه‌ای برایش با ارزش بود که وصیت کرد، روی سنگ قبرش، ۱۷− ضلعی منتظم را ترسیم کنند! گر چه، یونانیان باستان با روش ترسیم چند ضلعی های منتظم با ۳، ۴، ۵ و ۱۵ ضلع و همه چند ضلعی‌هایی که با نصف کردن زوایای این اشکال، به‌کمک خط‌کش و پرگار، به‌دست می‌آید، آشنا بودند، اما، روش کلی برایش نیافته بودند. حدود دو هزار سال راکد ماند تا سر انجام، گاوس آن‌را به طور کامل، پاسخ داد و به‌صورت قضیه‌ی دوسویی زیر بیان و اثبات کرد:

هر n–ضلعی منـتظم ترسـیم پـذیر اسـت، اگـر و تنهـا اگـر، $n = 2^{\alpha} p_1 \dots p_k$، کـه در آن α یک عدد صحیح نامتناهی و p_iها $(i = 1,\dots,k)$ عـدد اول فرمـا هسـتند؛ یعنـی: $p_i = 2^{2^i} + 1$.

گاوس، در سال ۱۷۹۸ راهی دانشگاه هلمشتدت شد تا تحصیلات خود را در آن‌جـا تکمیل نماید. ازآن‌جا که شهرت او به این دانشگاه رسیده بود، مورد استقبال گرم اسـتاد ریاضیات دانشگاه قرار گرفت. یک سال بعد، یعنی در ۱۷۹۹ موفق به اخذ درجه‌ی دکتـرا در علوم، از همین دانشگاه شد.

دراین‌جا خوب است، نگاهی اجمالی به رساله‌ی دکترای او بیندازیم:

عنوان:

«راه اثبات جدیدی از این قضیه که هر معادله‌ی جبری یک مجهولی، حداقل یک ریشه دارد.»

در این عنوان، عبارت «راه اثبات جدید»، این توهم را ایجاد می‌کند که گاوس، تنها یـک راه جدید برای این قضیه یافته که بر اثبات‌هایی که از قبل وجود داشت، اضافه شده بود. اما، کسانی که قبل از گاوس، برای این قضـیه اثبـاتی منتشـر کـرده بودنـد، در حقیقـت اثباتشان واقعی نبود؛ به‌عبارت‌دیگر، گاوس اولین کسی بود که توانست، آن‌را واقعاً اثبـات نماید و ما، با اجازه‌ی گاوس، عنوان رساله را این گونه باز نویسی می‌کنیم:

«اولین راه اثبات از این قضیه که هر معادله‌ی جبری یک مجهولی، حداقل یک ریشه دارد.»

گره کور این قضیه وقتی باز می شود که بفهمیم، مقصود از ریشـه چیسـت؟ گـاوس، بـا توجه به همین علامت سوال ثابت کرد که ریشه‌های هر معادله جبری عدد $a+bi$ است که a,b دو عدد حقیقی و i، جذر عدد ۱- اسـت. در حقیقـت عـدد $a+bi$نـوعی عـدد جدید بود که عدد مختلط نام گرفت. این قضیه، آن‌قدر برای گاوس اهمیـت داشـت کـه چهار راه اثبات متمایز دیگر، برایش پیدا کرد که آخرین اثبـات را در هفتـاد سـالگی بـه دست آورد.

اینک، به سراغ اولین کتاب گاوس، یعنی «تجسسات حسابی» گاوس می رویم. اثری که عده‌ای آن را بزرگ ترین شاهکار او می‌دانند. در ابتدای مقدمه کتابش، نوشته است: «تجسساتی که در این کتاب مندرج است، به بخشی از ریاضیات تعلق دارد که از اعداد صحیح و کسرها، سخن می‌گوید و اعداد اصم در تمام حالات کنار گذاشته شده است.»

سه بخش نخست این کتاب، درباره‌ی تئوری همنهشتی است. به ویژه، از همنهشتی دو جمله‌ای $x^n \equiv A \pmod{p}$ بحث عمیقی وجود دارد که در آن A و n اعداد صحیح معلوم و اختیاری هستند و p عدد اول و x عدد صحیح نامعلوم است. این قضیه در حساب، شباهت زیادی به قضیه‌ی معادله‌ی دوجمله‌ای $x^n = A$ در جبر دارد.

در بخش چهارم، گاوس، تئوری باقی‌مانده‌ها را مورد مطالعه قرار می دهد و در همین بخش، برای اولین بار، یک استدلال واقعی از «قانون تقابل مربعی» بیان می‌کند. بخش پنجم، از تئوری «فرم‌های تربیعی دو مجهولی» در حساب، بحث می‌کند و بعد به مطالعه «فرم‌های تربیعی سه مجهولی» می پردازد. در بخش ششم هم، تمام تئوری های بخش‌های پیشین را در شکل‌های خاص به‌کار برده است؛ مثلاً معادله‌ی مبهم $mx^2 + ny^2 = A$ را که m و n و A اعداد صحیح اند ،حل کرده است.

در بخش هفتم و آخرین بخش، گاوس برای بحث در معادله‌ی جبری $x^n = 1$، که در آن n عدد صحیح است، تئوری همنهشتی‌های دو جمله‌ای را، به کار می‌برد. حل معادله $x^n = 1$، همان صورت جبری مسئله هندسی است که موضوع آن ساخت $n-$ضلعی منتظم یا تقسیم محیط دایره به n بخش مساوی است.

با انتشار این اثر، دنیای جدیدی در حساب عالی رخ نمود و در خاک مزارع مجزایی از ریاضیات؛ مثل جبر، آنالیز و هندسه، ریشه دوانید. گاوس در دوران کهن سالی‌اش در این‌باره گفته است: «کتاب تجسسات حسابی، وارد تاریخ شده است.» گاوس، بعد از انتشار این کتاب، بیش‌تر به نجوم و فیزیک پرداخت و این علوم را، چه از جنبه‌ی نظری و چه از لحاظ تجربی، مورد کنکاش قرار داد. گاوس در نهم اکتبر ۱۸۰۵، در بیست و هشت سالگی، با دختر مورد علاقه‌اش، **یوهانا اشتهوف**، از اهالی زادگاهش، ازدواج کرد. حاصل ازدواجش با یوهانا، **یوزف**، **مینا** و **لودویش** بود.

در آن زمان، کشمکش‌های سیاسی و نظامی، کشورهای اروپایی از جمله آلمان را، دچار شرایط بحرانی کرده بود. در سال ۱۸۰۶، سردار ارتش آلمان، در درگیری نظامی بین آلمان و فرانسه، جانش را از دست داد. این سردار، کسی نبود جز ویلهلم فردیناند؛ مرد سخاوتمندی که سال‌ها، پدرانه، پشتیبان مالی گاوس بود و با تشویق‌هایش به او قوت قلب می‌داد. نه تنها مرگ فردیناند، ضربه‌ی سختی را به گاوس وارد کرد، بلکه شکست کشورش در مقابل فرانسه، برای وطن پرستی چون او، غیر قابل تحمل بود. در سال ۱۸۰۸، گاوس پدرش را نیز از دست داد. با وجود آن‌که خاطره‌ی خوشی از پدرش در ذهن نداشت، اما این دلیل نمی‌شد که او پدرش را دوست نداشته باشد و از مرگش متأثر نباشد.

یازدهم اکتبر ۱۸۰۹، دو روز بعد از چهارمین سالگرد ازدواجش، حادثه‌ی شوم دیگری برایش رقم خورد. او در لحظه‌ی به‌دنیا آمدن لودویش، سومین فرزندش، یوهانا را برای همیشه از دست داد تا بهار زندگیش، از خزان هم بگذرد و به زمستان بدل شود. همه‌ی این اتفاقات تلخ، کافی است تا سرسخت ترین انسان‌ها را، از لحاظ روحی ویران کند و گاوس را که آن لحظه، بیش از سی سال داشت، افسرده و منزوی سازد. مثلاً، در یادداشتی از او که راجع به توابع بیضوی است، ناگهان متن علمی قطع می شود و این جمله با دست خط ریزش آشکار می شود: «مرگ برای من، از چنین زندگی‌ای شایسته‌تر است.» گاوس یک سال بعد، درچهارم اوت ۱۸۱۰، به‌خاطر بچه‌های خردسالش، تن به ازدواج دوم داد. زن دومش، **مینا والدک**، دوست صمیمی یوهانا بود. گاوس از مینا نیز، صاحب دو پسر و یک دختر شد.

سال ۱۸۱۱، دوره‌ی جدیدی در تاریخ ریاضیات بود که با سال ۱۸۰۱، یعنی زمان انتشار کتاب تجسسات حسابی گاوس، قابل مقایسه است. در این زمان، گاوس با درک عمیقی که از اعداد مختلط و شیوی نمایش آن‌ها پیدا کرده بود، بر آن شد که مسئله‌ای را حل کند که امروزه آن را با نام «توابع تحلیلی یا متغیر مختلط» می‌شناسند. این مسئله یکی از بزرگ‌ترین یافته‌های ریاضی قرن نوزده است. گاوس در نامه‌ای به **بسل** موضوعاتی که با شکل اصلی این تئوری ارتباط داشت، مورد بحث قرار داد. اما هیچ گاه یافته‌هایش را منتشر نکرد تا این که **کوشی** و بعد، **وایرشتراس** آن را دوباره کشف کنند.

سال ۱۸۱۲ نیز، زمان انتشار یکی دیگر از آثار بزرگ اوست کـه بـه نوبـه‌ی خـود، باعـث پیشرفت ریاضیات بود. نام این اثر «رشته فوق هندسی» است. این رشته بـه‌صـورت زیـر است:

$$1+\frac{ab}{c}\cdot\frac{x}{1}+\frac{a(a+1)b(b+1)}{c(c+1)}\cdot\frac{x^2}{1\times 2}+\frac{a(a+1)(a+2)b(b+1)(b+2)}{c(c+1)(c+2)}\cdot\frac{x^3}{1\times 2\times 3}$$

گاوس شرایطی را برای a,b,c,x در نظر گرفت که مجموع بالا، متقارب باشد. او بـا دادن مقادیر خاص به یک یا چند تا از a,b,c,x، مجموع‌های مربوط به هر مقدار داده شـده را که در آنالیز ریاضی کاربرد دارد، به‌دست آورد؛ مثل مجموع محاسبه‌ی لگاریتم، مجمـوع توابع مثلثاتی و مجموع‌هایی که در نجوم و فیزیـک اسـتفاده مـی‌شـوند. حتـی قضـیه‌ی دوجمله‌ای هم، یکی از حالت‌های خاص مجموع بالاست.

از کارهای دیگر گاوس، یافته‌های او درباره » قانون تقابل درجه‌ی چهار» است. وقتی کـه گاوس قانون تقابل مربعی با درجـه‌ی دو را اثبـات کـرد، توجـه خـود را بـه شـکل کلـی همنهشتی‌های دوجمله‌ای معطوف ساخت؛ یعنـی همنهشـتی $x^n \equiv m \pmod{p}$ کـه n عدد صحیح مثبت و m عددی صحیح است که بر عدد اول مفروض p، بخـش پـذیر نیست. اگر بتوانیم، عدد صحیح چون x را در همنهشتی صـدق دهـیم، مـی‌گـوییم m باقی‌مانده‌ی nام برای p است. وقتی $n=4$ باشد، m باقی‌مانده چهارم برای p اسـت. در هندسه نیز، توفیقات مهمی، حاصل کرد و درباره‌ی مسئله‌ی انطباق سطوح، فهمیـد کـه چه رویه‌هایی را می‌توان، بدون کشش و پارگی، بر رویه‌ای معین، تطبیق داد.

سال‌های پرکار و درخشان زندگی گاوس گذشت و گرد پیری بر چهره‌اش نشست. اینـک دستانش می‌لرزد، چشمانش آب آورده، قلبش درست کار نمی کند، ولـی تسـلیم نشـده است و هنوز می خواهد مثل دوران جوانی‌اش کار کند. روز شانزدهم ژوئن ۱۸۵۴ اسـت، می‌خواهد برای اولین بار بعد از بیست سال، شهر گوتینگن را ترک کند تا بـه بازدیـد راه آهن گوتینگن-کاسل برود. وقتی به آن‌جا رسید، بر روی کالسکه‌اش ایستاد تـا منظـره‌ی راه آهن را تا دور دست‌ها تماشا کند. برایش جالب بود. ناگهان اسب کالسـکه رمیـد و او بر زمین افتاد. خوش‌بختانه، با وجود ضربه‌ی سختی که خورد، جان سـالم بـه‌در بـرد. در

روز سی ویکم ژوئن ۱۸۵۴، باز در محل راه آهن حاضر شد، تا در لحظات افتتاح راه آهن سهیم باشد؛ چیزی که می‌توانست، او را بعد از مدت‌ها راضی نماید!

و بعد از یک سال، سرانجام گرفتگی عضلات قلب، او را در بستر مرگ انداخت، و در سپیده دم ۲۳ فوریه‌ی۱۸۵۵، در هفتاد و هشت سالگی، بدرود حیات گفت، اما در قلمرو ریاضیات تا ابدیت، یاد و خاطره‌اش زنده خواهد ماند! روحش شاد ... و راهش پر رهرو باد!

ب-۲ زندگی نامه آبل

" هابیل ریاضیات ، قابیل فقر"

در آسمان ریاضیات، ستاره‌های دنباله‌داری ظهور کرده است که تا چشم‌های ستاره پرست خواستند، آن‌ها را محو تماشا شوند، برای همیشه ناپدید شدند، ولی آن‌چنان درخشان بودند که تا پایان هستی، آسمان ریاضیات را نور باران کرده‌اند. یکی از این ستاره‌های دنباله دار، **آبل** است. ستاره‌ای در ادامه نسل حضرت آدم که ... **هابیل** ریاضیات بود و قاتلش ... **قابیل فقر** !!!

با آغاز قرن نوزدهم میلادی، بازهم جهان منتظر نابغه‌ی دیگری در اروپا بود. این بار در نروژ؛ در دهکده‌ای به نام **فیندو** از توابع کریستیانساند در روز پنجم اوت ۱۸۰۲ م. پسری در خانه‌ی کشیش دهکده به‌دنیا آمد که دومین فرزند کشیش بود و کسی نبود جز، **نیل هنریک آبل**. زمان با آرامش می‌گذشت. تنها سرمایه‌ی خانواده‌ی آبل، محبت بود که در جان یخ زده از فقرشان شعله می‌کشید. بی پول بودند، اما با غرور زندگی می‌کردند. مدرسه‌اش شکنجه گاه بود، با هیولایی که نقش معلم را بازی می‌کرد. یک روز آن قدر یکی از بچه‌ها را کتک زد که طفل معصوم زیر دست و پایش تلف شد!! مردم برآشفتند و این هیولا را از مدرسه راهی دادگاه کردند. معلم دیگری آمد؛ ریاضی‌دانی لایق ولی نه چندان مطرح به اسم برندت میکائیل هولمبوئه.

در این هنگام، آبل پانزده سالش بود. هولمبوئه که حالا معلمش شده بود، درک عمیقی داشت. حس کرد که **آبل** در ریاضی استعداد دارد. هولمبوئه خالق اثر بزرگی نبود، ولی آن‌ها را می‌شناخت وستایش می‌کرد؛ آبل را تشویق کرد که کتاب‌های مهم ریاضی بخواند تا سرانجام آبل احساس کرد عاشق ریاضیات شده است. هولمبوئه هر بار می‌دید نابغه‌ی کلاسش ستاره‌ای در ریاضیات کشف می‌کند، به وجد می‌آمد. این معلم دلسوز، بعدها آثار شاگردش را در ۱۸۳۹ م. به چاپ رساند. آبل پسر خنده رویی بود. معیشت خانواده‌اش هرروز بدتر می‌شد، اما صبور و قانع بود. شب در بسترخواب، خودش را استاد دانشگاه می‌دید که بر تخته سیاه با گچ سفید، مسائل شیرین ریاضیات را نقاشی می‌کند و چشمان حیرت زده‌ی شاگردانش او را به شوق می‌آورد ... و با همین آرزوی قشنگ مست خواب می‌شد.

آبل از نخستین ریاضی‌دانانی بود که حفره‌های استدلال قدما را لمس کرد و تصمیم گرفت آن‌ها را پر کند. از آثاری که نتیجه‌ی این طرز فکر بود، استدلال دقیق قضیه‌ی قوای دو جمله‌ای عمومی بود که حالات خاص آن را نیوتن و اویلر اثبات کرده بودند. آن دوره معادله‌ی درجه‌ی پنجم، مد شده بود و تقریبا همه‌ی ریاضی‌دانان را به مبارزه می‌طلبید. آبل هم جسورانه به دل مسئله حمله برد ... به خیالش حلش کرد؛ اما فهمید اشتباه کرده است. خوب ... شکست اولین گام پیروزی است! **شمعی** در ذهنش روشن شد: « **آیا اصلاً ، راه جبری برای حل این مسئله وجود دارد؟**»

خوب است، چند خط از اثر آبل، به نام «**درباره‌ی حل معادلات جبری**» را بیان کنیم تا هم به اهمیت مسئله پی‌ببریم و هم طرز فکر یک ریاضی‌دان بزرگ را نشان دهیم:

« یکی از جالب‌ترین مسائل در جبر عبارت است از حل جبری معادلات که تقریبا همه‌ی ریاضی‌دانان در این عرصه کوشیده‌اند. معادلات جبری تا درجه‌ی چهار، به سادگی حل می‌شوند و برای تعیین ریشه‌های آن‌ها، دستورهای روشنی وجود دارد. این دستورهای کلی این تصور را ایجاد می‌کند که بقیه معادلات نیز قابل حل‌اند. اما با وجود تلاش های ریاضی‌دانانی چون لاگرانژ، هیچ راه حلی پیدا نشد. به نظر می‌رسد، معادلات جبری از درجه‌ی بالاتر از چهار، به صورت جبری قابل حل نیستند. ولی برای اثبات این فرض هم موفقیتی به دست نیامده است؛ به‌عبارت‌دیگر، ابتدا باید دید که حل کردن این معادلات، ممکن است یا خیر. بدیهی است، کسی موفق می‌شود معادله‌ای را حل کند که معادله حل شدنی باشد. هستند افرادی که عمری را صرف حل مسئله‌ای کرده‌اند که اصلاً حل کردنش غیر ممکن است و طبیعی است که به نتیجه نرسند؛ بنابراین، برای این که بیش تر سرگردان نمانیم، باید روش فکری دیگری در پیش گرفت و ... موضوع را این گونه مطرح کنیم که آیا وجود چنین رابطه‌ای

امکان دارد یا نه ؟ ... . طرح مسئله به این صورت، نطفه‌ی راه حل را شامل می‌شود و روشی که باید در پیش گرفت، آشکار می‌سازد ...» .

کمی بعد، دو مسئله‌ی کلی را که با هم در ارتباط هستند، به صورت زیر بیان می‌کند:

۱- تعیین تمام معادلات از درجه‌ی معین و اختیاری که از روش جبری قابل حل باشند.

۲- تعیین این که معادله‌ی معلومی را می توان به صورت جبری حل کرد یا نه.

سپس می‌گوید که این دو مسئله در واقع یکی‌اند و با این که مدعی نیست آن‌ها را به طور کامل حل کرده است، اما « **وسائل مطمئنی به دست آورده است** » که می‌توان مسئله‌ها را به طور کامل با آن‌ها بررسی نمود. او قبل از این که فرصت کند تا مسئله های بالا را حل کند، به مسائل مهم‌تری کشیده شد؛ در اصل حل کامل این مسئله، یعنی بیان صریح شرایط لازم و کافی برای آن که معادله‌ی جبری حل شود، کاری است که گالوا انجام داد. لژاندر در ستایش این اثر آبل گفته است: «**بنای عظیمی است که گذشت زمان را به جنگ می طلبد**».

آبل آن روزها، هرگز تصور نمی‌کرد که پدرش هنوز چهل وهشت سالش تمام نشده، پیمانه‌ی عمرش لبریز می‌شود. بعد از مرگ پدر مسئولیت خانواده بر دوش آبل افتاد. شاگرد خصوصی پذیرفت و هر کاری می‌توانست، انجام می‌داد. درآمدش خوب بود؛ ولی کفاف هفت نفر را نمی‌داد؛ سر وکله زدن با ریاضیات، تنها زنگ تفریحش بود. هولمبوئه وقتی می‌دید شاگرد نابغه‌اش هر روز لاغرتر می شود، زجر می‌کشید. سعی می‌کرد، کار بهتری برایش دست و پا کند؛ حتی گاهی از جیبش مایه می‌گذاشت؛ با این که خودش هم زیاد پول دارتر از آبل نبود!

آبل هیجده سالش بود و هم چنان کار می‌کرد؛ با همه‌ی سختی‌ها و به یاری دوستانی چون هولمبوئه ،راهی دانشگاه کریستیانیا شد. تا قبل از بیست سالگی هر کاری که باید دراین مرکز علمی انجام بدهد، به پایان رساند. دیگر چیزی که برایش جذاب باشد، وجود نداشت. درحسرت آرزویی می‌سوخت؛ می‌خواست فرانسه را ببیند؛ ملکه‌ی

دنیای ریاضیات را ... برود آلمان؛ گاوس را ببیند؛ شاه‌زاده‌ی ریاضی‌دانان را ... اما ... با کدام پول؟! دوستانش تصمیم گرفتند برای آبل کاری کنند؛ افتادند به جان دانشگاه ... دانشگاه هم افتاد به جان حکومت تا شاید به این جوان با استعداد، کمک مالی کند و او را به آرزویش برساند.

آبل برای این که نشان دهد، شایستگی دریافت این کمک مالی را دارد، اثری را به دانشگاه ارائه داد. خدا می‌داند که انتشار این اثر چه قدر باعث افتخار دانشگاه و کشورش می‌شد. اما دانشگاه به دلیل مشکلات مالی آن را منتشر نکرد و دست آخرهم گم شد! سرانجام، بعد از مدت‌ها چانه زنی، حکومت با اعطای کمک مالی به آبل موافقت کرد، به این شرط که یک سال و نیم در دانشگاه کریستیانیا بماند و زبان آلمانی و فرانسه بخواند. آبل به خوبی می‌دانست که حکومت با وجود همه‌ی مشکلات مالی، برای او چنین امتیازی در نظر گرفته است ؛به همین خاطر نسبت به آن قدر شناس بود و تصمیم گرفت، زبان آلمانی و فرانسه بخواند. حالا علاوه بر خواندن زبان، باید به شدت کار می‌کرد تا هزینه‌ی زندگی خانواده را برای زمانی که می‌رفت سفر، تامین کند. جالب است که حتی در این موقعیت فرصت عاشق شدن را هم داشت و با دختری به‌نام کرلی کامپ نامزد کرد. چند ماه گذشت؛ هنوز یک سال ونیم نشده بود که از طرف پادشاه مبلغی برای سفری یک ساله در اختیار آبل قرار گرفت. چه قدر منتظر این لحظه بود. شب آخری که در فیندو بود، دریک مهمانی که هولمبوئه ترتیب داده بود، از همه‌ی دوستانش خداحافظی کرد. وقتی راهی سفر شد، سبتامبر۱۸۲۵م. بود.

اول سری به ریاضی‌دانان نروژ و دانمارک زد. بعد عازم برلین شد؛ شهری که خاطرات شیرینی را درصفحات ذهنش پر کرد؛ توانست با اوگوست لئوپولد کرل آشنا شود که برای او هولمبوئه‌ی دیگری شد؛ آبل، انگار کرل را جادو کرده بود؛ کرل بد جوری مسحور آبل شد؛ هر جا می رفت او را با خود می‌برد و به عنوان بزرگ‌ترین کشفی که در ریاضیات کرده است، معرفی می‌کرد؛ کرل همان سال، یعنی ۱۸۲۶ م. مجله‌ای را راه اندازی کرد، به اسم «**ریاضیات محض و کاربردی**» که بعدها به مجله‌ی «**کرل**» معروف شد.

مجله‌ی کرل، اولین مجله‌ای بود که درجهان تنها به ریاضیات اختصاص داشت و مطالب جدید و به روز را هرسه ماه یک بار منتشر می‌کرد؛ حتی هنوز هم به عنوان یکی از معتبرترین مجلات تخصصی ریاضی جهان مشغول فعالیت است و همیشه خوشه‌های رسیده، آب‌دار و شیرین را به علاقمندان تقدیم می‌کند. سه جلد اولش شامل بیست و دو تا خوشه از آثار آبل بود که هم باعث شهرت آبل شد و هم شهرت مجله را درپی‌داشت. بیش تر خوانندگان دلیل موفقیت آبل را در ریاضیات جویا می‌شدند. او پاسخ می‌داد: «**معلم فوق العاده ام هولمبوئه، دوستانم و کتاب های خوب و البته علاقه و پشتکار زیاد**» .

کرل با تمام قدرت و نفوذش، سعی می‌کرد تا برای آبل یک کرسی استادی در دانشگاه برلین به دست آورد؛ اما این کار آسانی نبود و احتیاج به زمان داشت. روزی به آبل گفت: « **می خواهم ترتیب ملاقات تو را با گاوس بدهم**» ... آبل از موضوع استقبال نکرد!! کرل دلیلش را خواست ... آبل از جواب دادن طفره رفت ... کرل این قدر سماجت کرد که آبل به اکراه لب به سخن گشود:

« **نروژ که بودم، مدتی قبل از سفرم تصمیم گرفتم، اثری از خودم که درباره‌ی معادلات درجه‌ی پنجم بود و به تو هم نشان داده‌ام، برای گاوس بفرستم، تا مثلا شاه‌زاده‌ی ریاضی‌دانان ارزش اثرم را درک و مرا به قصر شاه زاده‌های ریاضی دعوت کند. با هزار بدبختی، پول چاپ آن را دادم و نسخه‌ای برای او فرستادم. اما بعد از یک منبع موثق فهمیدم که او وقتی آن را دریافت کرده است، با عصبانیت گفته است: « باز هم یکی دیگر از عجایب فرستاده‌اند!» بعد مچاله‌اش می‌کند و دور می‌اندازد ! ... بی انصاف! حتی نگاهش نمی‌کند! این کارش هم قلب مرا و هم بتی که از او ساخته بودم، شکست؛ فکر نمی‌کردم تا این حد از خود متشکر باشد؛ اگر آن را می‌خواند و بعد مچاله می‌کرد دلم نمی سوخت ... حاضر نیستم ببینمش ...! اگر قرار است من هم روزی به خاطر علم و سواد مغرور شوم، کاش خدا علم و سواد را از من بگیرد! ... ببخشد! نمی‌خواستم**

چیزی بگویم، اما خودت باعث شدی؛ امیدوارم از این که این جوری از هم وطن دانشمندت بد گویی کردم، ناراحت نشوی » .

کرل درحالی که محو تماشای آبل بود، آهی کشید و گفت: «**اتفاقا خیلی هم ناراحت شدم ... اما نه از تو ... بلکه از گاوس!!! نمی دانم چرا این کار را کرده است؟! امیدوارم برای این کارش دلیل قانع کننده‌ای داشته باشد و این اتفاق در نهایت به نفع تو تمام شود. به هر حال تو حالا به عنوان یک ریاضی‌دان واقعی مشهور شده‌ای؛ به زودی گاوس تو را خواهد شناخت و وقتی بفهمد که قبلاً با تو چه کرده است، حتما شرمنده خواهد شد. تو تنها جانشین شایسته‌ی گاوس هستی، من به این ایمان دارم. قول می‌دهم کاری کنم که تو استاد بزرگ دانشگاه برلین شوی و همه در برابرت زانو بزنند؛ حتی شاه زاده! قول می‌دهم».** در این لحظه کرل نمی‌دانست که آبل خیال دارد به زودی برلین را ترک کند؛ وقتی جریان را فهمید، خیلی ناراحت شد و هر کاری کرد تا مانع رفتن آبل شود.

کرل که دید نمی‌تواند جلوی آبل را بگیرد، تصمیم گرفت با او راهی شود؛ اما به دلیل موانع سر راهش نتوانست برود. سر انجام لحظه‌ی خداحافظی فرا رسید؛ آبل از آن جا رفت سوئیس؛ شهر فریبورگ؛ جای دنجی بود؛ طوری که توانست به دور از هیاهو، اساس آن چه را که امروز « **قضیه‌ی آبل**» نام دارد، بنا کند. اما زیاد ماندگار نشد؛ شور دیدار با ریاضی‌دانان بزرگ فرانسوی، مثل کوشی، لژاندر و ... او را رهسپار پاریس کرد؛ به پاریس رسید؛ آن طور که شنیده بود، جذاب و تماشایی نبود! دلش خوش بود که بالاخره با کسانی که تنها اسمشان را شنیده و آثارشان را دیده است، می‌تواند ملاقات کند؛ پیش خود آرزو می کرد: «**کاش آن‌ها به اندازه‌ی گاوس مغرور نباشند!!**»

برای مدتی که آن جا می‌ماند، باید جایی را اجاره می‌کرد؛ پاریس شهر گرانی بود وپولش آن قدر نبود که بتواند اتاقی مناسب کرایه کند. برای اجاره‌ای که قادر بود بپردازد تنها یک اتاق کوچک وکثیف، پیدا شد. چند روز بعد، به دیدن ریاضی‌دانان فرانسوی رفت؛ اما آن ها آبل را نمی‌شناختند؛ نمی‌دانستند که او چه گوهری است و در طی مدتی هم که او آن‌جا بود، کسی نتوانست این گوهر نایاب را کشف کند؛ درحالی که

جلوی چشمشان بود !!!! ... آبل هم آدمی نبود که از خودش تعریف کند؛ تا مـی‌خواسـت لب تر کند و درباره‌ی موضوعی از ریاضی حـرف بزنـد، فـوری نطـق بلیغـی از اهمیـت و ارزش شخص شخیص خویش ایراد می‌فرمودند !!! تنها پذیرایی ریاضی‌دانان فرانسـه از او برخوردی مودبانه بود !

بی تفاوت تر از همه لژاندر بود؛ یک روز در حـالی کـه سـوار کالسـکه‌اش مـی شـد، صدایی شنید: « **معذرت می‌خواهم**». سرش را برگرداند؛ پسر جوانی را دید کـه گهگـاه او را دیده بود. نگاه سردی به صورت پسر جوان انداخت و بعـد از کمـی مکـث پرسـید: «**کاری داری جوان؟**» جوان که همان آبل خودمان بود، از رفتار خشک لژاندر وا رفـت. خجالت کشید، عرق سردی بر پیشانی اش نشست و گفت: «**ببخشید ... نمی‌خواسـتم مزاحم شوم ... راستش ... می خواستم درباره‌ی موضوئی با شما صحبت کـنم ...** ». لژاندر گفت: « **فعلا کار دارم. با اجازه!!**» و کالسکه‌اش به راه افتاد!!!

آبل به راه افتاد ؛ آهسته به جلو قدم می‌زد؛ فرش زیر پایش برگ‌هـای پـائیزی بـود؛ در آرزوهایش غوطه ور بود؛ ناگاه خود را جلوی در اتاقش یافت ... در را بـاز کـرد و رفـت تو ... قاب پنجره پر از غروب خورشید بود؛ سرفه‌اش گرفت؛ مدت‌ها بود که این سـرفه‌هـا گاه و بی گاه به جانش می‌افتاد و هر روز هم بدتر می‌شد؛ نیمه‌های شب از فرط سـرفه از خواب پرید؛ با این که چیزی رویش نکشیده بود، خیس عرق بود. دیگر خوابش نمی‌برد؛ بلند شد یک برگ کاغذ سفید پیدا کرد تا برای هولمبوئه نامه بنویسد.

در قسمتی از نامه این‌گونه می‌خوانیم: «**حقیقت را به تـو بگـویم؛ پـاریس؛ پـر هیاهوترین شهر اروپا برایم صحراست! هیچ کس را نمی‌شناسم ... فقط کوشی، ژاکوبی، لژاندر، هاشت و چند نفر دیگر را دیده‌ام ... بـرای یـک تـازه وارد کـار دشواری است که خود را مطرح کند ... تازگی‌ها مطلبی درباره‌ی طبقه خاصی از توابع متعالی به اتمام رسانده‌ام؛ آن را به آکادمی علوم تحویـل دادم؛ آن را بـه کوشی هم نشان دادم؛ اما بدون خودستایی می‌گویم اثرمهم و زیبایی از کـار در آمده است. کنجکاوم بدانم نظر دانشکده درباره‌ی آن چیست ... کارهای زیادی باقی مانده است که باید انجام دهم؛ ولی در سفر جریان امور در دستم نیست ...**

اگر من هم یک کرسی استادی داشتم چه می‌شد؟ باز هم صبر می‌کنم، شاید سر نوشت به زودی به من لبخند بزند ! ...»

سرفه‌اش گرفت؛ این بار خیلی شدیدتر؛ آن قدر سرفه کرد که چشمانش سیاهی رفت و بر زمین افتاد. در قفسه‌ی سینه احساس فشار می‌کرد. احساس ضعف شدیدی کرد؛ کمی دراز کشید ... صبح، تصمیم گرفت که به دکتر برود؛ دکترسوالاتی از او پرسید و او را به دقت معاینه کرد ... بعد از معاینه با اضطراب به صورت رنگ پریده‌ی آبل نگاه کرد و با کمی مقدمه چینی به آبل گفت که به سل مبتلا شده است. آبل باور نکرد و به دکتر دیگری مراجعه کرد؛ اما این دکتر هم، همان حرف‌های دکتر قبلی را تکرار کرد. انگار آب یخ بر سرش ریختند. بدون این که بفهمد دکتر هنوز در حال صحبت است، ازآن جا بیرون رفت ...همین طور راه می‌رفت، در خود فرو رفت؛ گویی در این عالم نبود.

گوشه‌ی خلوتی را پیدا کرد ... ساعت‌ها با خود اندیشید؛ به آرزوهایش؛ به کسانی که دوستشان داشت؛ به خانواده‌اش، به نامزدش کرلی، به دوستانش کرل و هولمبوئه، به ریاضی، استاد شدن ... آهی کشید ... چشمانش پر از اشک شد. خودش به خودش دلداری می‌داد. برخاست و به اقامت گاهش برگشت؛ همان دخمه‌ای که به احتمال قوی مسبب بیماری اش بود. بار و بندیلش را بست؛ ازکسانی که می‌شناخت، خداحافظی کرد و از پاریس رفت؛ با یادگاری بیماری سل و سوغاتی از خاطرات تلخ؛ به هر کجا که ریاضی‌دانی در آن زندگی کند؛ حتی مدتی هم برای دلش سفرکرد و از زیبایی‌های طبیعت لذت برد تا حال وهوایش عوض شود و اندکی غم وغصه‌هایش را فراموش کند. بعد هم به نروژ باز گشت. وقتی به کریستیا نساند رسید، رمقی نداشت؛ آن زمان روزهای پایانی بهار سال ۱۸۲۷ م. بود.

اما، کار اثری که آبل قبل از ترک پاریس به دانشکده‌ی علوم داده بود، به کجا کشید؟ روز دهم اوکتبر ۱۸۲۶ م. اثر آبل با عنوان «**درباره‌ی خاصیت عمومی طبقه‌ی وسیعی از توابع متعالی**» برای مطالعه و اعلام نتیجه به کوشی و لژاندر محول شد. لژاندر پیر حوصله‌اش را نداشت و کوشی میان سال هم فقط به فکر خودش بود! بالاخره

آقای لژاندر در گزارشش نوشت: «**این نسخه‌ی خطی را نمی‌شود به درستی خواند، مرکبی که با آن نوشته‌اند، خیلی بی رنگ است، از مولف بخواهید یکی پررنگ تر و خواناتر بفرستد ...**»؛ عجب هنرمندی !!! ... خوب، آقای کوشی چه کرد؟ هیچ او هم هنرمندتر!!! اثر را به خانه برد و به گوشه‌ای انداخت؛ بعد هم به کلی آن را فراموش کرد تا معجزه‌ی آبل خاک بخورد !!!

آبل از لحظه‌ای که اثرش را به دانشکده سپرد منتظر اعلام نتیجه‌ی آن ها بود. حالا ماه ها از این موضوع گذشته و او در کریستیانساند است؛ اما هیچ خبری نشده است! همه نزدیکانش از بیماری اش با خبر شده بودند ؛ برای همه عجیب بود که او با وجود این بیماری لا علاج، از زندگی‌اش لذت می‌برد و به شدت کار می‌کند؛ با این که خیلی راحت می‌توانست، پول‌هایش را نگه دارد وسکه‌ای هم برای خانواده‌اش خرج نکند، اما هم چنان خرج خانواده‌اش را می‌داد. حالا دیگر اروپا، کم کم فهمیده بود که آبل یک ریاضی‌دان نابغه است. هولمبوئه هم بیش از پیش درکنار شاگرد قدیمی‌اش بود و هوایش را داشت. دوستش کرل هم از برلین نامه می‌نوشت و خبرهای امیدوار کننده‌ای به او می‌داد.

با این که آبل، نا امیدی را، نا امید کرده بود، اما روز به روز ضعیف‌تر می‌شد. بیماری در اول بهار ۱۸۲۹ م. به اوج رسید؛ سرفه‌های وحشتناک و خونریزی شدید به او فهماند، فرصت چندانی باقی نیست. روز آخر همه دورش حلقه زده بودند؛ سمت راستش مادرش بود که به شدت اشک می‌ریخت؛ رو به رویش هولمبوئه ایستاده بود و نامزدش کرلی کامپ هم دست چپش نشسته بود. به آن‌ها دلداری داد و از همه طلب بخشش کرد. آن‌گاه لبخندی زد وچشمانش را بست ... برای همیشه!!! دو روز بعد نامه‌ای از کرل برای آبل رسید که: «**... آبل عزیزم، بالاخره تو به عنوان استاد دانشگاه برلین انتخاب شدی، تبریک می‌گویم ...**». هولمبوئه اشک می‌ریخت و نامه را برای آبل می خواند؛ بر سر قبرش!!

حالا باید به وصیت شاگردش عمل می‌کرد تا بفهمد چه به سر اثر آبل، در دانشکده‌ی علوم فرانسه آمده است. حکومت نروژ را در جریان امر قرار داد و حکومت هم از طریق

سفارت نروژ در پاریس، از حکومت فرانسه توضیح خواست. جنجال سیاسی به پاشد. موضوع در دبیرخانه‌ی دانشکده مطرح شد. دبیر دانشکده از کوشی خواست که هرچه زودتر این مسئله را روشن کند. کوشی همه جا را زیر و رو کرد تا سرانجام آن را در خانه‌اش پیدا کرد. تازه یادش آمد که زمانی قرار بود آن را بخواند ولی ...

آن را به آکادمی برد تا اعضا هیئت علمی آن‌را بررسی کنند. موضوع اثر آبل، به موضوع اثری از ژاکوبی شباهت داشت. به ژاکوبی سپردند که آن‌را بخواند و نتیجه را گزارش دهد. ژاکوبی به مطالعه‌ی اثر پرداخت؛ ما هم با ژاکوبی همراه می‌شویم؛

عنوان: **«درباره‌ی خاصیت عمومی طبقه‌ی وسیعی از توابع متعالی»**

« توابع متعالی (غیرجبری)، توسط ریاضی‌دانان به آنالیز وارد شده است که بسیار معدود هستند. تقریبا همه تئوری توابع متعالی به توابع لگاریتمی، مجهول القوه و توابع مثلثاتی منحصر می شود. این توابع در واقع صور مختلف یک تابع‌اند. فقط در سال‌های اخیر است که برخی توابع دیگر را مورد مطالعه قرار داده اند؛ ازجمله آقای لژاندر که توانسته است بسیاری از خواص زیبا و مهم توابع بیضوی را به دست آورد ... من در اثری که اکنون افتخار تقدیم آن را به دانشکده دارم، طبقه بزرگی از توابع را مطالعه کرده‌ام که عبارتند از: توابعی که مشتق آن‌ها در یک معادله‌ی جبری صدق می‌کند که همه‌ی ضرایب آن، منطق یک متغیر هستند. بنده توانسته‌ام برای مجموعه‌ی این توابع خواصی مشابه با خواص توابع لگاریتمی و توابع بیضوی کشف کنم ...

... این مطالعات، در نهایت به بیان قضیه زیر منجر شد:

اگر توابعی داشتیم که مشتق آن‌ها بتواند، ریشه‌های معادله‌ی جبری واحدی باشند و همه‌ی ضرایب این توابع، منطق یک متغیر باشند، دراین‌صورت، همواره می‌توانیم مجموع تعداد غیر مشخصی از این توابع را به‌صورت یک تابع جبری و لگاریتمی نمایش داد؛ به شرطی که میان متغیرهای توابع مذکور، یک رابطه‌ی

جبری موجود باشد. تعداد این روابط جبری به تعداد توابعی کـه بـا هـم جمـع می‌شود، بستگی ندارد، بلکه به ماهیت توابع وابسته است ...»

قضیه‌ی بالا که به « **قضیه‌ی آبل**» مشهور شده است، کاری خارق العاده در حساب انتگرال است. آبل برای اثبات این قضیه نهایت دقت، کوتاهی و ظرافت را مانند اثبات های دیگرش در قضایای دیگر، به کار برده است. آن قدر اثبات قضیه را آسان بیان کرده که دانش آموز دبیرستانی هم آن‌را می‌فهمد.

ژاکوبی بعد از خواندن این اثر در گزارشش می‌نویسـد: « **کشف آبل، فوق العـاده است! چه طور کشف بزرگی مثل این که یکـی از آثـار بـزرگ ریاضـی اسـت و تاریخش مال دو سال پیش است مورد توجه ما قرار نگرفته** ؟ !!! ... ». لژانـدر هـم مثل این که دیگر مرکب برایش کم رنگ نبود! چون درباره‌ی آن گفـت: « **این اثر بنایی محکم تر از آهن است**». بعضی از اعضای دانشکده هنوز آبـل را بـه خـاطر داشـتند؛ از این که با او رفتاری شایسته مقامش نکرده بودند عذاب وجدان‌داشتند؛ از جملـه همـین لژاندر، به خصوص آن روز که سوار کالسکه‌اش می‌شد را خوب یـادش بـود؛ آبـل کـارش داشت ولی او ... !! اما اینک، پشیمانی چه سودی برای آبل نابغه داشت ؟

در سال ۱۸۳۰ م. اعضای دانشکده صادقانه به خطای خـود اعتـراف کردنـد؛ از روح آبل بخشـش خواسـتند ومراتـب عـذر خـواهی را بـه دولـت نـروژ ابـلاغ کردنـد؛ آن‌هـا درمراسمی، جایزه‌ی بزرگ آکادمی علوم فرانسه را به آبل اعطا نمودند؛ افسوس کـه او در این لحظه با شکوه زنده نبود؛ اما تا ابد در کتاب‌هـای مقـدس ریاضـیات، **معجـزه‌هـای هابیل ریاضیات**، یادگاری خواهد ماند.

ب-۳ زندگی نامه گا لوا

نابغه‌ی ریاضی در دوئل عشق

تصویر گالوا[1]

بازهم ستاره‌ای دنباله دار می‌گذرد. نام این ستاره **گالوا**ست. زندگی گـالوا، یـک تـراژدی واقعی است که بی‌شک، هر کس آن را بخواند، ناخود آگاه خواهـد گریسـت. او بـا وجـود عمر کوتاهش، هم‌چون قهرمان یک سریال خیالی، ایفای نقش کرد!

گالوا، در ۲۵ اکتبر ۱۸۱۱ میلادی، در بورلان، شهری در نزدیکی پاریس، دیده به جهان گشود. پدرش، **نیکلا گابریل گالوا**، شهردار شـهر بـورلان و مـادرش، **آدلاییـد مـاری**

[1] این تصویر به کمک حافظه‌ی برادر گالوا در سال ۱۸۴۸م. کشیده شده است.

دمانت، زنی از خانواده‌ای که طی چند نسل، حقوق‌دانان برجسته‌ای بودند. هم نیکلا و هم آدلایید، هواخواه پر حرارت آزادی و مخالف سر سخت استبداد بودند و گالوا را نیز با این اعتقاد، تربیت نمودند. گالوا مانند پدرش، شعر می سرود و گاه در محافل آزادی خواهان، شعرهایش را می‌خواند. پسری مهربان و اخمو که بیش‌تر، شبیه مادرش بود. تا دوازده سالگی جز مادرش، معلم دیگری نداشت. نه در اجداد پدری و نه در نیاکان مادری، کسی به ریاضیات نپرداخته بود و اگر هم، کسی از آن‌ها، استعداد ریاضی داشت، هرگز بروز نکرده بود. گالوا، اولین فرد از این خانواده بود که ناگهان، نبوغ ریاضی در وجودش، متبلور شد.

گالوا، بعد از دوازده سالگی، به مدرسه لوئی لوگران پاریس رهسپار شد؛ زندانی واقعی که مدیرش نیز، به یک زندان‌بان شباهت بیش‌تری داشت. گالوا در پایان سال اول، در همه‌ی دروس، شاگرد اول شد. با توجه به این‌که ادبیات و زبان لاتین را، نزد مادرش به خوبی فراگرفته بود، از مسئولان مدرسه خواست که به کلاس ادبیات و زبان لاتین نرود. اما کسی خواسته‌اش را اجابت نکرد و مجبور شد، یک سال در کلاسی حاضر شود که همه چیزش تکراری بود. این اتفاق، علاقه‌اش را به ادبیات و زبان لاتین، به نفرت تبدیل کرد و تکالیف کسل کننده‌اش را، خیلی سطحی انجام می‌داد. و در پایان، نمره‌ی قبولی نگرفت و یک سال دیگر، او را سر این کلاس، نشاندند!

در اثنای همین سال‌ها، به طور منظم، به خواندن ریاضی مشغول شد و چون لذت این کار را احساس کرد، با شور و اشتیاق، به مطالعه‌ی کتاب زیبای هندسه لژاندر پرداخت. هندسه را دوست داشت و جالب این‌که از جبر متنفر بود! از آن‌جا که علاقه‌اش را به هندسه، مدیون اثر بزرگی چون هندسه‌ی لژاندر بود، تصمیم گرفت به‌جای این‌که، هم چنان از جبر متنفر باشد، سری هم به آثار بزرگ جبر بزند. برای همین، به سراغ آثار جبری لاگرانژ رفت و بعد هم به آثار جبری آبل روی آورد. او که این زمان، چهارده ساله بود، شاه کارهای جبری؛ مثل حل معادلات عددی، تئوری توابع تحلیلی و حساب دیفرانسیل را، مثل یک داستان مرور می کرد. کارش در مدرسه تعریفی نداشت؛ چون حاضر نبود وقتش را برای درس‌های عادی، تلف کند. با این وجود، در مسابقه‌ی عمومی اول شد و همه را حیرت زده کرد!

گالوا وقتی فهمید، در ریاضیات استعداد خارق العاده‌ای دارد، احساس کرد، مانند استادان بزرگ ریاضی حرفی برای گفتن دارد و با غرور تمام، به مطالعه‌ی مسائلی پرداخت که حتی بزرگان ریاضی، جرئت آن را نداشتند. همه از رفتارش تعجب می‌کردند، گاهی هم وحشت! وقتی معلمانش در برابر سوال‌هایش کم می‌آوردند، سعی می‌کرد با آن‌ها مدارا کند، اما از نظر او، آنان انسان‌هایی کوته فکر بودند که برایش، گناهی نابخشودنی به حساب می‌آمد و او را عصبی می‌کرد.

وقتی گالوا، به شانزده سالگی رسید، تصور کرد، معادله‌ی کلی درجه‌ی پنجم را حل کرده است و این دقیقاً اشتباهی بود که قبل از او، آبل نیز مرتکب شده بود. رفته رفته، با رسیدن به سال پایانی مدرسه، او باید خود را برای آزمون ورودی پلی‌تکنیک؛ یعنی جایی که مادر همه ریاضی‌دانان فرانسه بود، آماده می کرد. اما چون حوصله‌ی درس خواندن نداشت، در آزمون قبول نشد. برای نابغه‌ای چون او، ناراحت کننده بود؛ به‌خصوص وقتی دید، افرادی بی‌استعداد، فقط به صرف حفظ کردن طوطی وار مطالب درسی، راهی پلی‌تکنیک شده‌اند. در سال ۱۸۲۸، به کالج اکول نرمان راه یافت. معلم ریاضی کالج، **لوئی پول امی ریچارد**، اولین کسی بود که فهمید، گالوا یک نابغه است. ریچارد، معتقد بود نابغه‌ای چون گالوا، باید بدون آزمون به پلی‌تکنیک راه یابد. اما، متأسفانه، همه عقیده‌ی او را نداشتند. جایزه‌ی اول کلاس ریچارد، نصیب گالوا شد. ریچارد درباره‌ی گالوا می‌نویسد: «گالوا، آشکارا، ما فوق دیگران است و فقط دوست دارد در سخت‌ترین قسمت‌های ریاضی، مشغول باشد.»

با تشویق‌های ریچارد، در اوایل مارس ۱۸۲۹، گالوا اولین مقاله‌اش را با نام «درباره‌ی کسرهای مسلسل» منتشر کرد. حالا تصمیم گرفته بود، یافته‌های خود را درباره‌ی نظریه‌ی معادلات چند جمله‌ای، به‌صورت مقاله، به دانشکده‌ی علوم فرانسه بفرستد تا با تائید آن‌جا، آن را منتشر نماید. گالوا، یکی از اعضای دانشکده، به نام **کوشی** را می‌شناخت که بزرگ‌ترین ریاضی‌دان فرانسه بود. او به کوشی گفت که مقاله‌ای به دانشکده فرستاده است و کوشی به او اطمینان داد که مقاله‌اش را بررسی خواهد کرد. اما، کوشی موضوع را به‌کلی فراموش کرد و سهل انگاری اعضای دانشکده، باعث شد که نوشته‌ی گالوا، مفقود شود. وقتی گالوا، نتیجه بررسی را جویا شد، به او گفتند، مقاله‌اش

به تائید دانشکده نریسده و گالوای بیچاره، نمی‌دانست که این مسخره‌ترین دروغی است که در عمرش، شنیده است !!!

سرنوشت، در حال رقم زدن تلخ‌ترین حادثه زندگی گالوا بود!؟ «وطن پرستان»یا همان دوستاران نظام سلطنتی، دشمنان سیاسی «جمهوری خواهان» یا همان هواداران آزادی بودند. در زمره‌ی وطن پرستان، کشیشان بودند که منفعت خود را، در گرو ادامه حیات سلطنت می‌دیدند و هر کس که طرفدار آزادی بود، از سر راه بر می‌داشتند. بعد از انتخابات محلی، وقتی پدر گالوا، دوباره به عنوان شهردار، رأی اعتماد گرفت، از آن‌جاکه جمهوری خواه بود، کشیشی درصدد برآمد که او را از میان بردارد. با ساختن اسناد جعلی و طرح اتهامات بی اساس، برطبل رسوایی شهردار کوبید. پدر گالوا نجیب و شرافتمند بود. در برابر این بی‌آبرویی، طاقت نیاورد و در دوم ژوئیه ۱۸۲۹، خودکشی کرد.

مدت کمی از این حادثه‌ی سوزناک گذشته بود. گالوا مجبور بود با قلبی سرشار از غم پدر، دوباره در آزمون پلی‌تکنیک شرکت کند. اصلاً، حوصله‌ی ایرادهای بنی اسرائیلی مأمور امتحان را نداشت و در پی درگیری لفظی، کنترلش را از دست داد و مداد پاکنش را به صورت مأمور، پرتاب کرد. همین کافی بود تا در آزمون مردود شود. وقتی راهی به پلی‌تکنیک، به رویش باز نشد، به دانشسرای عالی رفت تا خود را برای تعلیم آماده کند.

مدرسین دانشسرا، با او سرسازگاری نداشتند و عذابش می‌دادند. منت آن‌ها را نکشید و به تنهایی خود را برای امتحانات آخر سال، آماده کرد و نمرات خوبی آورد. دراین زمان، با تنظیم اثری درباره‌ی معادلات جبری، آن را به دانشکده‌ی علوم فرستاد تا شاید، بزرگ‌ترین جایزه‌ی ریاضی دانشکده را تصاحب کند؛ تاج شکوهمندی که فقط بزرگ‌ترین ریاضی‌دانان، مدعی آن بودند! دست نوشته‌ی گالوا به دبیرخانه دانشکده رسید و **فوریه**، ریاضی‌دان سرشناسی که دبیر دانشکده بود، آن را برای بررسی به خانه برد و درست قبل از مطالعه‌ی دست نوشته، دار فانی را وداع گفت! در این گیرو دار، کسی از اعضای دانشکده نفهمید که اثرگالوا درخانه‌ی فوریه است و عاقبت ناپدید شد، تا گالوا هم‌چنان ناشناخته بماند.

آتش انقلاب، هر لحظه در وجود گالوا شعله می‌کشید. از بی‌عدالتی به ستوه آمده بود. روح آزادی خواهش، او را وادار می‌کرد که از دوستانش، در دانشسرای عالی بخواهد، که برای خلق حماسه‌ای بزرگ، در تظاهرات شرکت کنند. دوستانش گرچه با او هم عقیده بودند، اما چیزی که در وجودشان نبود، شجاعت بود. درست در همان ایام، دانشجویان پلی‌تکنیک به خیابان‌ها ریختند تا با تظاهرات پر شورشان، تاریخ را با دست‌های خود، بنا کنند. رئیس دانشسرای عالی، با بستن درها، از رفتن دانشجویان دانشسرای عالی، به تظاهرات، جلوگیری کرد، این اتفاق، خشم گالوا را برانگیخت و در نامه‌ای جنون آمیز به «روزنامه‌ی مدارس» رئیس دانشسرا و دانشجویانش را به باد کوبنده‌ترین انتقادها گرفت. این نامه رئیس دانشسرا را برآشفت و گالوا را اخراج کرد.

اینک چه باید می‌کرد؟ برکدام زخمش مرهم بگذارد؟ کاری هم نیافته بود، تنها راه نجات جیب‌هایش را از بی‌پولی، تدریس خصوصی یافت. اما برای تدریس خصوصی، شاگردی پیدا نکرد. حالا مجبور است، به توپخانه‌ی گارد ملی وارد شود. «دوستان ملت» نام گردان آزادی خواهان بود. و او به دوستان ملت ملحق شد. نابود شده بود، اما هنوز امیدوار بود. یافته‌های قبلی‌اش را جمع کرد و این بار به **پوآسون**، یکی دیگر از اعضای دانشکده داد تا شاید، ستاره‌ای در افق تاریک زندگی‌اش، سوسو کند. اما باز هم کسی به آن اهمیتی نداد تا تندیس ترک خورده‌ی آرزوهای قشنگش، برای همیشه فرو بریزد. سرنوشت برایش نوشت که تو حق نداری برای خودت زندگی کنی! پس از این لحظه، خودش را وقف مردم کرد و تنها هدفش، رسیدن به آزادی حقیقی بود. در بیانیه‌ای گفت: « اگر جسدی لازم است تا مردم را به قیام وادارد، من حاضرم، خویش را تقدیم کنم.»

نهم ماه مه ۱۸۳۱، نقطه‌ی آغاز سراشیبی‌ای بود که به خط پایان زندگی‌اش می‌رسید! او و جمعی از جمهوری خواهان، در ضیافتی گرد هم آمدند تا به تصمیم پادشاه، مبنی بر انحلال واحدهای توپخانه‌ای جمهوری خواهان اعتراض کنند. فردا او را دستگیر و روانه زندان سیاسی کردند. در دادگاه، با ترفندهای زیرکانه‌ی وکیل مدافعش، تبرئه شد. گرچه آزاد شد، اما، یک ماه بعد برای جلوگیری از اقدامات ضد حکومتی، دوباره دستگیر شد و این بار به شش ماه حبس محکوم شد.

در محیط کثیف زندان، مرض وبا شیوع پیدا کرده بود. گالوا هم به بیماری وبا مبتلا شد. او را برای درمان، به مریض‌خانه منتقل کردند. مرض وبا خوب شد، اما چه خوب شدنی!؟ چون، دختری زیبا، قلبش را به مرض عشق مبتلا کرد. بالاخره، از زندان آزاد شد، با چهره‌ای که از رنج این شش ماه، شصت سال شکسته بود و با قلبی که اینک، زندانی عشق شده بود. تصمیم گرفت به ییلاق برود تا اندکی به دور از هیاهو، به آینده‌ی مبهم خویش، بیندیشد. یکی از وطن پرستان، اسیر عشق دختری شده بود که گالوا را نیز در مریض‌خانه، به مرض عشق مبتلا کرده بود. برای همین موضوع، از گالوا خواست که در دوئل حاضر شود. گالوا باید بهای گزافی برای عشق می‌پرداخت.

سخت‌ترین شب زندگی گالوا، شب ۲۹ مه ۱۸۳۲ بود. می‌دانست که به خط پایان عمرش، نزدیک شده است. دوباره اراده کرد و در آن لحظات، ذره‌ای از نبوغش را بر کاغذ نقاشی کرد، تا به این دل‌خوش باشد که اگر جسمش می‌میرد، با قلمش بر صفحه‌ی زمان زنده است. گاه گاه در حاشیه، با خط ناخوانا می‌نوشت: «وقت ندارم، وقت ندارم.» و باز ادامه می‌داد. آن شب توانست، یک‌بار برای همیشه راه حل واقعی مشکلی را بیابد که قرن‌ها، ریاضی‌دانان را در اندیشه و اضطراب نگاه داشته بود و آن این‌که، در چه شرایطی می‌توان معادله‌ای را حل کرد.

کاغذ دیگری برداشت تا وصیت‌نامه‌اش را بنویسد. خطاب به همه‌ی جمهوری خواهان و حتی وطن پرستان، از آنان خواست که او را به‌خاطر این‌که در راهی غیر از وطن می‌میرد، ملامت نکنند و در ادامه می‌آورد: «اکنون وجدانی را با خود به گور می‌برم که منزه از دروغ است» و در پایان می‌نویسد: «یادگار مرا حفظ کنید، زیرا سرنوشت آن قدر به من مهلت نداد که وطن، نام مرا بداند. من می‌میرم، در حالی که دوست شما هستم. صمیمانه همه شما را می‌بوسم»

گالوا صبح روز سی‌ام مه۱۸۳۲، برای دوئل رودر روی حریفش ایستاد. ناگهان صدای شلیک طپانچه‌ای برخاست و این گالوا بود که به زمین افتاد. حریفش او را همان جا، رها کرد. نزدیک ساعت۹، کشاورزی با دیدن پیکر نیمه جانش او را به درمانگاه برد. برادرکوچکش از ماجرا آگاه شد و با چشم گریان به بالین او آمد. گالوا، اشک از گونه برادرش می‌زدود و می‌گفت: «گریه نکن، من برای مردن در بیست سالگی، به شجاعت

احتیاج دارم.» و سرانجام سحرگاه روز سی و یکم مه ۱۸۳۲ با طلوع خورشید از شرق، خورشید زندگی گالوا در غرب جهان غروب کرد. او رفت اما از خود چیزی فنا ناپذیر به یادگار گذاشت. چیزی که شامل شصت صفحه بود. **اوگوست شوالیه**، دست نوشته‌های علمی گالوا را نزد خود نگاه داشت، و دنیا باید برای حفظ این آثار ارزشمند،مدیون این دوست صمیمی گالوا باشد تا این که ...

چهارده سال بعد در سال۱۸۴۶، **ژوسف لیوویل**، این دست نوشته‌ها را در مجله‌ی «ریاضیات محض و کاربردی» منتشر کرد و درباره‌ی این‌که چه جواهری کشف کرده است، می‌گوید: «تلاش من برای مطالعه‌ی این آثار، ثمر داد و بعد از اصلاح جزئیات، وقتی دیدم روش او صحیح است، هیجان زده شدم، مخصوصاً، وقتی به این قضیه‌ی زیبا رسیدم: «شرط لازم و کافی برای این که معادله‌ای تجزیه ناپذیر با درجه‌ی عددی اول، به کمک رادیکال‌ها قابل حل باشد، این است که تمام ریشه‌های آن توابع منطقی از دو ریشه‌ی اختیاری آن باشد»

و گالوا در سرزمینی از ریاضیات به نام جبر، متولد شد... .

منابعی برای مطالعه‌ی بیشتر

۱. استرویک، درک. ج. **تاریخ فشرده‌ی ریاضیات**. ترجمه‌ی برادران خسرو شاهی، غلامرضا و کامرانی، حشمت الله. نشر نو(۱۳۶۶).

۲. ایوز، هاورد ویتلی. **آشنایی با تاریخ ریاضیات**. ترجمه‌ی وحیدی اصل، محمد قاسم. مرکز نشر دانشگاهی تهران(۱۳۶۸).

۳. بل، اریک تمپل. **ریاضیدانان نامی**. ترجمه‌ی صفاری، حسن. چاپ اول، تهران، انتشارات امیرکبیر(۱۳۶۳).

فهرست نمادها

نماد	مفهوم	اولین صفحهٔ مراجعه
$\mathbb{N}$	مجموعه‌ی اعداد طبیعی	۲
$\mathbb{N}_0$	مجموعه‌ی اعداد صحیح نامنفی	۲
$\mathbb{Z}$	مجموعه‌ی اعداد صحیح	۲
$\mathbb{Q}$	مجموعه‌ی اعداد گویا	۲
$\mathbb{R}$	مجموعه‌ی اعداد حقیقی	۲
$\mathbb{C}$	مجموعه‌ی اعداد مختلط	۲
$\mathbb{Z}_n$	مجموعه‌ی اعداد صحیح به پیمانه n	۲
1_R	عنصر همانی حلقه R	۳
$\mathrm{M}_n(R)$	مجموعه‌ی ماتریس‌های $n\times n$ با درایه‌های از R	۳
$\mathbb{H}(\mathbb{R})$	حلقه چهارگانی حقیقی	۳
$R_1\times\cdots\times R_n$	حاصل‌ضرب مستقیم حلقه‌های $R_1,\cdots,R_n$	۵
$\mathbb{Z}[i]$	حلقه‌ی اعداد صحیح گوسی	۶
$\cong$	یکریخت بودن	۷
$U(R)$ یا R^*	گروه یکال‌های R	۹
$\mathrm{Char}R$	مشخصه‌ی حلقه R	۱۱
$Z(R)$	مجموعه‌ی عناصر مقسوم‌علیه صفر حلقه R	۱۱
ER	حلقه‌ی اقلیدسی	۱۳

$F(u_1,\ldots,u_n)$	زیر میدان تولید شده به وسیله‌ی $u_1,\ldots,u_n$ روی F	۵۹
$F[X]$	زیر حلقه‌ی تولید شده به وسیله‌ی X روی F	۵۹
$F(X)$	زیر میدان تولید شده به وسیله‌ی X روی F	۵۹
π	عدد پی	۶۰
e	عدد نپر	۶۰
$\mathcal{C}$	مجموعه‌ی اعداد ترسیم‌پذیر $\mathbb{R}$	۷۰
$f'(x)$	مشتق $f(x)$	۹۲
$\mathrm{Aut}K$	گروه یکریختی‌های میدان K	۱۰۰
$\mathrm{Aut}_F K$	گروه گالوایی K روی F	۱۰۰
$\mathrm{Gal}_F K$ ($G(K,F)$)	گروه گالوایی K روی F	۱۰۰
G_f	گروه گالوایی چندجمله‌ای $f(x)$	۱۰۰
$\Phi_n(x)$	n امین چندجمله‌ای دایره‌بر	۱۴۱
μ	تابع موبیوس	۱۵۱
$\mathrm{Map}(X,F)$	مجموعه‌ی توابع از X به F	۱۹۹
$U \oplus W$	جمع مستقیم زیر فضاهای Uو W	۲۰۲
$\langle X \rangle$	زیر فضای تولید شده توسط X	۲۰۳
$< v_1,\ldots,v_n >$	زیر فضای تولید شده توسط $v_1,\ldots,v_n$	۲۰۳
$\dim_F V$	بعد فضای برداری V روی میدان F	۲۰۹
$\mathrm{GL}(V)$	گروه خطی عام فضای برداری V	۲۱۳

واژه‌نامه فارسی به انگلیسی و فهرست راهنما

آ–ا

اثر(رد)،۱۱۲،۲۱۲	trace
استقلال خطی،۲۰۴	linearly independent
الگوریتم-	-algorithm
- اقلیدس،۴۶	Euclidean
- تقسیم،۲۸	division
ایده‌آل،۱۴	ideal
-اصلی،۱۵	principle-
-اول،۱۹	prime-
-تولید شده توسط مجموعه X،۱۵	X -generated by the set
-سره،۱۴	proper-
-ماکزیمال،۲۰	maximal-
ایزومورفیسم،۷	isomorphism

ب–پ–ت

بروریختی۷	epimorphism
-طبیعی۸	canonical-

بزرگ‌ترین مقسوم علیه مشترک،۳۹	greatest common divisor
بستار جبری،۶۷	algebraic closure
بسته،۱۰۱	closed
بعد،۲۰۹	dimension
به طور جبری بسته،۳۰	algebraically closed
پایه،۱۳۹	basis
پوچ‌توان،۲۴	nilpotent
تابع متقارن،۱۱۱	symmetric function
-مقدماتی،۱۱۱	elementary-
تثلیث زاویه،۵۳	trisecting the angle
تحویل‌ناپذیر۵۳،	irreducible
تربیع دایره،۴۳	squaring the circle
ترسیم‌پذیر،۴۳	constructible
ترکیب خطی،۴۳	linearly combination
تصویر،۲۳،۲۱۱	image
تضعیف مکعب،۴۳	doubling the cube
تکریختی،۷	monomorphism
توزیع‌پذیری،۲	distributive
توسیع،۵۶	extension
-جبری،۶۰	algebraic-
-جدایی‌پذیر۸	separable-
-دایره‌بر۸	cyclotomic-
-رادیکال،۱۲۳	radical-
-ساده،۵۸	simple-

-متناهی،۵۶	finite-
-نرمال (گالوا)۸	normal(Galois)-

ج-چ

جبری،۶۰	algebraic
جدایی‌پذیر،۱۸۰	separable
جمع مستقیم،۲۰۲	direct sum
چند جمله‌ای،۲۷	polynomial
-اولیه،۴۱	primitive-
-تکین،۲۷	monic-
-دایره‌بر،۱۴۱	cyclotomic-
-مینیمال۸	minimal-

ح-خ

حل‌پذیر با رادیکال‌ها،۹	solvable by radicals
حلقه،۲	ring
-اقلیدسی،۱۳	Euclidean-
- ایده‌آل اصلی،۱۵	principal ideal-
-بخشی (تقسیم)،۱۰	division-
-تعویض‌پذیر،۲	commutative-
-چند جمله‌ای،۲۷	polynomial-

د–ر–ز

س-ش

سری،۱۱۶	series
-ترکیبی،۱۱۷	composition-
-حل‌پذیر،۱۱۷	solvable-
-زیرنرمال،۱۱۶	subnormal-
-نرمال،۱۱۶	normal-
شرط زنجیر صعودی،۲۱	ascending chain condition (ACC)
شرکت‌پذیر،۲	associative
شریک (وابسته)، ۳۶	associate

ض- ع

ضریب پیشرو،۲۷	leading coefficient
عدد-	-number
اول فرما،۸۲،۱۵۲	Fermat prime
جبری،۶۰	algebraic
لیوویل،۶۰، ۱۶۸	Liouville
متعالی،۶۰	transcendental
عنصر-	-element
اول،۳۶	prime
تحویل‌ناپذیر،۳۶	irreducible
جبری،۶۰	algebraic
متعالی،۶۰	transcendental

عوامل،۱۱۶	factors

ف–ق

فضای برداری،۱۴۵	vector space
قابل نشاندن،۷	embeddable
قضیه‌ی اساسی جبر،۳۱،۱۶۰	fundamental theorem of algebra
قضیه‌ی اساسی نظریه‌ی گالوا ،۱۰۷	fundamental theorem of Galois theory
قضیه‌ی-	-Theorem
اول سیلو،۱۶۲	First Sylow
برج،۱۷۰	Tower
کوشی،۱۳۵،۱۵۹	Cauchy’s
گاوس،۸۲	Guass’s
ودربورن،۱۰	Wedderburn’s
ویلسون،۲۵	Wilson’s
قضیه‌ی۹۰هیلبرت ،۱۱۴	Hilbert’s theorem 90

ک–گ

کواترنیون،۱۵	quaternion
گروه،۱۰	group
-جایگشتی انتقالی،۱۳۷	transitive permutation-
-حل‌پذیر،۱۱۷	solvable-
-خطی عام،۲۱۳	general linear-
-گالوایی،۱۰۰	Galois-

-یکال‌ها،۹	units-

م

ماتریس واندرموند،۱۳۱	Vandermonde matrix
متعالی،۱۶۸،۶۰	transcendental
محتوا،۴۱	content
محک آیزنشتاین،۴۸	Eisenstein’s criterion
مشتق،۹۲	derivative
مشخصه،۱۱	characteristic
معکوس ،۹	inverse
معکوس پذیر،۹	invertible
-چپ،۹	left-
-راست،۹	right-
مقسوم علیه صفر،۱۱	zero divisor
مولد،۱۵،۱۹۵	generator
مونومورفیسم،۷	monomorphism
میدان،۱۰	field
-شکافنده،۸۶	splitting-
-کامل،۹۹	perfect-
-کسرها،۳۴	quotients-
-میانی،۵۶	interminate-

ن- ه-ی

نرم،۱۱۲	norm
نسبت به‌هم اول ،۳۹	relatively prime
نوتری،۲۲	Noetherian
هسته،۲۱۱،۲۳	kernel
همریختی(هم‌مورفیسم)،۷	homomorphism
یکال،۹	unit
یکریخت،۷	isomorphic
یکریختی،۷	isomorphism