انتشارات دانشگاه شهید چمران

۳۹۰

پنجاهمین سال تأسیس
دانشگاه شهید چمران (جندی شاپور)
را گرامی می داریم

مقدمه ای بر

جبر تعویض پذیر و نظریه اعداد

مولف: سوکمار داس آدهی کاری

$$A = \wp_1 \wp_2 \cdots \wp_n$$

مترجم: دکتر منصور معتمدی
عضو هیات علمی دانشکده علوم ریاضی و کامپیوتر
دانشگاه شهید چمران اهواز

ناشناخته‌ها زایندهٔ شناخته‌ها هستنند، اما همچنان ناشناخته باقی می‌مانند. همان طور که یک دانه بذر معرفِ بذرهای ناشماراست و صبوری و استواری جنگل‌هایِ بی‌شمار را دارد، ناشناخته‌ها نیز در بردارندهٔ تمام بودنی‌ها است، یا آنچه که می‌توانسته است باشد، یا همهٔ آنچه خواهد بود یا می‌تواند باشد.

سری‌نیسا گادادت مهاراجه

اگر چه امروزه نمی‌توانیم در جزئیات با کانت موافق باشیم، اما کلی‌ترین و بنیادی‌ترین تصورهایِ معرفت‌شناسیِ کانتی، همچنان با اهمیت هستند، از جمله محقّق بودنِ تقّدمِ وجه شهودیِ تفکر و لذا بررسی چگونگی امکانِ هرگونه معرفت،.... پیش از این چیزی در قوه تجسم به ما داده شده است: اشیایی معین و فرامنطقی که به طور شهودی به عنوان تجربه‌ای بی واسطه، قبل از استدلال وجود دارد.

داوود هیلبرت

مقدمه‌ای بر

جبر تعویض‌پذیر
و
نظریهٔ اعداد

مؤلف:

سوکمار داس آدهی‌کاری

مترجم:

دکتر منصور معتمدی

بهار ۱۳۸۲

پیشگفتار مترجم

یکی از زمینه‌های ظهور نظریهٔ حلقه‌های تعویض‌پذیر نظریهٔ جبری اعداد است. گرچه مسائل کلیدی در این مورد بر حسب اعداد صحیح بیان می‌شود، اما به تدریج مشخص شد که می‌توان این گونه مسائل را در حوزه‌هایی که حوزهٔ اعداد صحیح نامیده می‌شوند مطرح کرد و به آنها پرداخت.

نتیجهٔ اصلی در این مورد در کارهای تحقیقاتی ددکنید که در سال ۱۸۷۱ میلادی به صورت پیوست درس‌های نظریه اعداد دیریکله منتشر شد، متبلور گردید. ددکنید نشان داد که هر ایدال ناصفر در حوزهٔ صحیح اعداد در هر هیأت اعداد جبری، حاصلضربی یکتا از ایدآل‌های اول است. آشکار است که پیش از آن باید حوزهٔ اعداد صحیح، ایدآل و ایدآل اول تعریف می‌شدند. اعضای یک هیأت اعداد جبری ریشه‌های چند جمله‌ای‌هایی با ضرایب صحیح هستند. ددکنید حوزه اعداد صحیح را به صورت عناصری که ریشه های یک چندجمله‌ای تکین با ضرایب صحیح هستند تعریف کرد. وی نشان داد که این عناصر رفتاری شبیه اعداد صحیح دارند ، یعنی با جمع و ضرب معمولی یک حلقه تشکیل می‌دهند. مفهوم ایدآل به شکل امروزی آن، همان است که توسط ددکنید تعریف شده است.

کتابی که ترجمهٔ آن در اختیار شماست سعی در آشکار کردن حقایقی دارد که به آن اشاره شد. این کتاب می‌تواند به عنوان مقدمه‌ای برای درس نظریه جبری اعداد و نیز یک کتاب کمک درسی برای درس نظریه حلقه‌های تعویض‌پذیر مورد استفاده قرار گیرد.

نمادها و اصطلاح ها

در سراسر این کتاب، نمادهای $\mathbb{N}$، $\mathbb{Z}$، $\mathbb{Q}$،$\mathbb{R}$، $\mathbb{C}$ به ترتیب بر مجموعه‌های اعداد صحیح نامنفی ، مجموعهٔ اعداد صحیح، مجموعهٔ اعداد گویا، مجموعهٔ اعداد حقیقی و مجموعهٔ اعداد مختلط دلالت دارد. منظور از حلقه، همواره حلقهٔ تعویض‌پذیر با عنصر واحد است، تابع $f : A \to B$ یک به یک است، اگر $f(a_1) = f(a_2)$ ایجاب کند که $a_1 = a_2$. تابع f پوشا خوانده می شود هرگاه برای هر $b \in B$، $a \in A$ وجود داشته باشد که $f(a) = b$.

برای دو مجموعهٔ A و B نماد $A < B$ بر این دلالت دارد که A به طور اکید مشمول در B است. برای یک مجموعه S، $|S|$ تعداد عناصر S را نمایش می دهد.

برای هر حلقهٔ R، R^* نشان دهنده گروه عناصر وارون پذیر R است. برای هر عدد طبیعی q که توانی از یک عدد اوّل باشد، F_q هیات متناهی با q عنصر را نمایش می دهد. برای عدد حقیقی x، $[x]$ بخش صحیح x را نشان می دهد. از نماد $\Box$ برای نشان دادن پایان اثبات استفاده می کنیم.

فهرست مندرجات

فصل ۰

مقدمه:گروه‌ها

حلقه‌ها و هیات‌ها

۰.۱ گروه‌ها

تعریف. فرض کنیم G یک مجموعهٔ نا تهی است. یک قانون ترکیب بر G، یک تابع $f: G \times G \longrightarrow G$ است. نمادهایی نظیر $a.b$ ، $a+b$ یا به طور ساده، پهلوی هم گذاشتن ab برای $f((a,b))$ به کار برده می شود.

تعریف. فرض کنیم G مجموعه‌ای با قانون ترکیب $f: G \times G \longrightarrow G$ باشد. نماد ab را به جای $f((a,b))$ به کار می بریم. در این صورت زوج (G,f) یک گروه نامیده می شود، هر گاه سه شرطزیر بر قرار باشد:

یک) برای هر a,b,c در G، $a(bc)=(ab)c$. این واقعیت را چنین بیان می کنیم که قانون ترکیب، شرکتپذیر است.

دو)عنصرِ e در G وجود دارد به طوری که برای هر $a \in G$، $ae=ea=a$. به وضوح عنصرِ e یکتاست. آن را عنصرِ همانی G می نامیم.

سه) برای هر $a \in C$، عنصر $a^{-۱}$ در G وجود دارد به طوری که $aa^{-۱}=a^{-۱}a=e$.

بنابر قانون شرکتپذیری، برای هر a، چنین عنصری یکتاست و وارون a نامیده می شود.

تعریف. اگر زوج (G,f) در تعریف فوق، در شرط اضافیِ زیر نیز صدق کند آن را گروه آبلی می نامیم.
چهار) برای هر a,b در G، $ab=ba$. این امر چنین بیان می شود که قانون ترکیب تعویضپذیر است.

مثال‌ها. مجموعهٔ اعداد صحیح، $\mathbb{Z}$ با جمعِ معمولی، به عنوان قانون ترکیب، یک گروه آبلی است. مجموعهٔ اعداد گویای ناصفر، $\mathbb{Q}^*$ با ضرب به عنوانِ قانون ترکیب، نیز یک گروه آبلی است.

یادداشت. از این پس، با فرضِ داشتن تابع f، به جای گروه (G,f) می نویسیم G. به سبب شرکتپذیری قانون ترکیب، می توان به جای نماد $a(bc)=(ab)c$ از نماد abc استفاده کرد. در حالت کلی، برای دنباله ای از n عنصر، از نمادهایی نظیر $a_1a_2\cdots a_n$ استفاده می شود. اگر برای هر i، $i=1,2,\cdots n$، $a_i=a$، a^n دلالت بر $\underbrace{a\cdots a}_{n}$ دارد. اگر n صحیح و مثبت باشد، a^{-n} برابر با $\underbrace{a^{-1}\cdots a^{-1}}_{n}$ تعریف می شود. همچنین $a^\circ=a^{1-1}$ عنصر همانی e است. اگر به جای پهلوی هم گذاشتن، از نماد جمع استفاده شود به جای $\underbrace{a+a+\cdots+a}_{n}$ می نویسیم na.

تعریف. فرض کنیم H یک زیر مجموعهٔ G باشد، در این صورت H را یک زیر گروه G می نامیم، هر گاه سه شرطزیر برقرار باشد.
یک) برای هر $a,b\in H$، $ab\in H$.
دو) عنصر همانی e به H تعلق داشته باشد.
سه) اگر $a\in H$، آن گاه $a^{-1}\in H$.
پس اگر H یک زیر گروه G باشد، آن گاه، تحت قانون ترکیب القا شده از G، خود یک گروه است.

مثال. برای هر عدد صحیح a، زیر مجموعهٔ $a\mathbb{Z}:=\{ar|r\in\mathbb{Z}\}$ یک زیر گروه $(\mathbb{Z},+)$ است.

تعریف. فرض کنیم G یک گروه و a یک عضو G باشد. فرض کنیم $H:=\{a^n|n\in\mathbb{Z}\}$، در این صورت به سادگی دیده می شود که H یک زیر گروه G است. در واقع H کوچکترین زیر گروهِ شامل a می باشد، بدین معنی که هر زیر گروه G که شامل a باشد، شامل H نیز خواهد بود. زیر گروه H، زیر گروه دوری G، تولید شده با a نامیده می شود.

گروه G، دوری نامیده می شود، هر گاه عنصر $a \in G$ وجود داشته باشد به قسمی که زیر گروه دوری تولید شده با a تمام گروه G باشد. گوییم a، G را تولید می کند یا این که a مولد گروه دوری G است.

مرتبهٔ گروه G تعداد عناصر G است و مرتبهٔ عنصر a، مرتبهٔ زیر گروه دوری تولید شده با آن است. چنانچه مرتبهٔ گروه G متناهی باشد، آن را متناهی می نامیم. در غیر این صورت G نامتناهی خوانده می شود.

مثال. گروه $\mathbb{Z}$ تحت جمع دوری است. هر دو عنصرِ ۱ و ۱−، $\mathbb{Z}$ را تولید می کنند.

تعریف. یک همریختی از گروه G به توی گروه G' تابعی مانند $\phi : G \longrightarrow G'$ است به قسمی که برای هر $a, b \in G$، $\phi(ab) = \phi(a)\phi(b)$. همریختی ϕ از G به G' را یکریختی می نامیم هر گاه یک به یک و پوشا باشد. اگر یک یکریختی از G به G' موجود باشد، گروه G و G' را یکریخت می خوانیم.

تذکر ۱.۰ فرض کنیم G و G' دو گروه و e و e' به ترتیب عناصر همانی G و G' باشند. اگر $f : G \longrightarrow G'$ یک همریختی باشد، آن گاه $f(e) = f(ee) = f(e)f(e)$. با ضرب طرفین در $(f(e))^{-1}$ داریم $f(e) = e'$. همچنین برای هر $a \in G$، $f(aa^{-1}) = f(e) = e'$ و لذا $f(a^{-1}) = (f(a))^{-1}$.

مثال‌ها. فرض کنیم $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ با برابری $f(n) = 2n$، برای هر $n \in \mathbb{Z}$، تعریف شده باشد. در این صورت f یک همریختی است. در حالت کلی اگر b یک عنصر گروه G باشد، آن گاه $\phi : \mathbb{Z} \longrightarrow G$ که با $\phi(n) = b^n$ تعریف می شود، یک همریختی است.

فرض کنیم $\mathbb{Q}^*$ گروه عناصر نا صفر اعداد گویا تحت ضرب باشد، در این صورت تابع $f : \mathbb{Q}^* \longrightarrow \mathbb{Q}^*$ که برای هر $a \in \mathbb{Q}^*$ با $f(a) = a^{-1}$ تعریف می شود یک یکریختی است.

تعریف. فرض کنیم G و G' گروه و $f : G \longrightarrow G'$ یک همریختی باشد، در این صورت هستهٔ f برابر با مجموعهٔ تمام عناصر $a \in G$ تعریف می شود که به ازای آنها $f(a) = e'$، که در آن e' عنصر همانی G' است. از تذکر ۱.۰ فوق چنین نتیجه می شود که e به هسته f تعلق دارد. به سادگی دیده می شود که هسته f یک زیر گروه G است و f یک به یک است، اگر و تنها اگر هستهٔ f برابر با $\{e\}$ باشد.

تعریف. یک رابطهٔهم ارزی بر مجموعهٔ S، یک زیر مجموعهٔ $S \times S$، مانند R است که در سه شرط زیر صدق کند.

یک) بازتابی : برای هر $a \in S$، $(a, a) \in R$

دو) تقارنی : اگر $(a,b)\in R$، آن گاه $(b,a)\in R$
سه) ترایایی : اگر (a,b) و (b,c) هر دو در R باشند، آن گاه (a,c) هم در R است.

اگر $(a,b)\in R$، گوییم a با b هم ارز است و می نویسیم $a\sim b$. بدیهی است که اگر R یک رابطهٔ هم ارزی بر مجموعهٔ S باشد، آن گاه یک افرازِ S به مجموعه های مجزا حاصل خواهد شد، به نحوی که هر زیر مجموعه شامل عناصری است که با یکدیگر هم ارزند. بنابراین اگر a به یک زیر مجموعهٔ تعلق داشته باشد آن‌گاه هر b در آن زیرمجموعه در شرط $a\sim b$ صدق می کند. این زیر مجموعه که شامل تمام عناصر هم ارز با a هستند، ردهٔ هم ارزی a نامیده شده و با C_a نشان داده می شود. اگر $a\sim b$، آن گاه $C_a=C_b$. برای یک رابطهٔ هم ارزی R بر مجموعهٔ S، مجموعهٔ تمام رده ها، را خارج قسمتِ S توسط R می‌نامند و آن را با S/R یا $S/\sim$ نمایش می دهند.

در قسمت باقی‌ماندهٔ این بخش، تنها گروه‌های آبلی مورد نظر هستند.

تعریف. فرض کنیم G یک گروه آبلی و H یک زیر گروه آن باشد. فرض کنیم R یک زیر مجموعهٔ $G\times G$، شامل تمام عناصر (a,b) باشد به قسمی که $ab^{-1}\in H$. به سادگی دیده می شود که R یک رابطهٔ هم ارزی بر G است. در این جا، رده های هم ارزی، همدسته های G به پیمانه H نامیده می شوند. خارج قسمت، خارج قسمت H توسط G خوانده می شود و آن را با G/H نشان می دهند. به سهولت می توان تحقیق کرد که ردهٔ هم ارزی a برابر است با $aH:=\{ah|h\in H\}$. با تعریف ضرب در G/H به صورت $(aH)(bH)=(ab)H$، G/H به یک گروه تبدیل می شود که آن را گروه خارج قسمتی G توسط H می نامند.

تذکر ۲.۰ تعداد همدسته های زیر گروه H، شاخص H در G نامیده شده و با $[G:H]$ نمایش داده می شود. یک رابطهٔ هم ارزی بر یک مجموعه، آن رابه رده های دو به دو جدا از هم تجزیه می کند، بنابراین اگر G یک گروه متناهی باشد، با مشاهده این که هر همدستهٔ H به اندازه H عضو دارد، خواهیم داشت $|G|=|G:H||H|$. از این جا نتیجه می شود که مرتبهٔ H مرتبهٔ G را عاد می کند. (این گزاره که مرتبه یک زیر گروه یک گروه متناهی مرتبه گروه را عاد می کند حتی برای گروه‌هایی که آبلی نیستند نیز صادق است. این نتیجه به قضیه لاگرانژ موسوم است).

اگر تابع $\phi:G\longrightarrow G/H$ رابا $\phi(a)=aH$ تعریف کنیم، آن گاه ϕ یک همریختی پوشا با هستهٔ H است.

اکنون فرض کنیم G و G' گروه و f یک همریختی از G به توی G' باشد. فرض کنیم H هسته f باشد. در این صورت همریختی $\overline{f}$ از G/H به تصویر $f(G)$، که با

$\overline{f}(aH) = f(a)$ تعریف می شود را در نظر می گیریم، این همریختی یک تکریختی از G/H به روی $f(G)$ است. این واقعیت به نام اولین‌قضیهٔ یکریختی شناخته می شود.

۲.۰ حلقه‌ها و هیأت‌ها

تعریف. یک‌حلقهٔ تعویض‌پذیر R با عضو واحد مجموعهٔ ای است با دو قانون ترکیب با نام‌های جمع و ضرب که به ترتیب با $+$ و پهلوی هم گذاشتن، نشان داده می شود. این دو قانون ترکیب، در چهار شرط زیر صدق می کنند:
یک) R نسبت به جمع، گروهی آبلی است. عنصر همانیِ $(R,+)$، عنصرِ صفر حلقهٔ R نامیده شده و با 0 نشان داده می شود. برای $x \in R$، وارون جمعی x با $-x$ نشان داده می شود.
دو) ضرب شرکت‌پذیر و نسبت به جمع توزیع‌پذیراست. یعنی برای هر x، z, y در R، $(xy)z = x(yz)$ و $x(y+z) = xy + xz$ و $(y+z)x = yx + zx$.
سه) عنصر $1 \in R$ وجود دارد، به طوری که $x1 = 1x = x$. این عنصر که به وضوح یکتاست عنصر همانی R نامیده می شود.
چهار) برای هر y, x در R، $xy = yx$. این شرط، تعویض‌پذیری نامیده می شود.

تذکر ۳.۰ همان طور که قبلاً متذکر شدیم، مقصود از واژهٔ حلقه ، حلقهٔ تعویض‌پذیر واحددار است. یعنی آن حلقه هایی که علاوه بر شرط‌های اِستانده (یک) و (دو)، در شرط‌های (سه) و (چهار) نیز صدق می کنند. همچنین متذکر می شویم که به علت شرط تعویض‌پذیری (چهار) هر یک از دو قانون توزیع‌پذیری، دیگری را نتیجه خواهد داد.

تذکر ۴.۰ امکان برابریِ 0 با 1 را منتفی نمی دانیم. اگر چنین شود، برای هر x در R، داریم $x = x1 = x0 = 0$. لذا در آن حالت، R تنها از عنصر 0 تشکیل شده است. آن راحلقهٔ صفر می نامیم.

مثال‌ها. مجموعهٔ اعداد صحیح، $\mathbb{Z}$، تحت عمل جمع و ضرب یک حلقه است. همین وضعیت در مورد اعداد گویا $\mathbb{Q}$، مجموعهٔ اعداد حقیقی $\mathbb{R}$ و اعداد مختلط $\mathbb{C}$ برقرار است.

تعریف. یک‌زیر حلقهٔ Sِ حلقهٔ R، یک زیر گروه $(R,+)$ است به طوری که $1 \in S$ و برای هر $x, y \in S$، $xy \in S$.

تعریف. اگر R و S دو حلقه باشند، تابع $f : R \longrightarrow S$ یک همریختی حلقه‌ها یا به طور ساده یک همریختی نامیده می شود (زمانی که زمینه مشخص باشد)، هر گاه سه

شرط زیر برقرار باشد.
یک) $f(x+y) = f(x) + f(y)$
دو) $f(xy) = f(x)f(y)$
سه) $f(۱) = ۱$

تذکر ۵.۰ در این جا نماد ۱ را برای هر دو عنصر واحد R و S به کار برده ایم. به قرینه باید معلوم باشد که هر کدام در مکان ویژه خود به کدام حلقه معطوف است. به طور مشابه، در هر دو حلقهٔ R و S، نماد $+$ و پهلوی هم گذاشتن به ترتیب برای جمع و ضرب به کار برده شده اند.

تعریف. همانندِ حالت گروه‌ها، یک همریختی حلقه‌ها، $f : R \longrightarrow S$ یک یکریختی بین R و S نامیده می شود، هر گاه یک به یک و پوشا باشد. اگر یک یکریختی از حلقه R به حلقه S وجود داشته باشد، آن گاه این دو حلقه، یکریخت خوانده می شوند.

تعریف. یک ایدآل حلقهٔ R، یک زیرمجموعهٔ R است که یک زیر گروه $(R, +)$ بوده و علاوه بر آن اگر $a \in I$ و $r \in R$، آن گاه $ra \in I$.

برای هر x در R، مجموعهٔ $Rx := \{rx | r \in R\}$، به وضوح یک ایدآل است. این ایدآل را یک ایدآل اصلی تولید شده با x می نامند. آشکار است که Rx، کوچکترین ایدآل شامل x می باشد. هنگامی که حلقهٔ R در طی یک بحثِ مشخص، ثابت است، گاهی به جای Rx، می نویسیم (x). در حالت کلی، برای هر زیر مجموعهٔ Dی R، کوچکترین ایدآل شامل D، ایدآل تولید شده با D خوانده می شود. این ایدآل مجموعهٔ تمام مجموع‌های متناهی به شکل $r_۱d_۱ + r_۲d_۲ + \cdots + r_md_m$ است. که در آن برای هر $i = ۱, ۲, \cdots, m$، $r_i \in R$ و $d_i \in D$. در این‌جا m در مجموعهٔ اعداد طبیعی تغییر می کند.

مثال‌ها. برای حلقهٔ R، مجموعهٔ تک عضوی $\{۰\}$ و تمام حلقهٔ R به وضوح دو ایدآل R هستند. هر دو، ایدآل‌های اصلی اند که به ترتیب با ۰ و ۱ تولید شده اند.

تعریف. هر ایدآل R به جز $\{۰\}$ و R، متذکر در فوق یک‌ایدآل سرهٔ R خوانده می شود.

تعریف. اگر A یک ایدآل حلقهٔ R باشد، گروه خارج قسمتی R/A، یک ضرب از R می گیرد (یعنی $(x+A)(y+A) = xy + A$) که آن را به یک حلقه تبدیل می کند.این حلقه، حلقهٔ خارج قسمتی R بواسطه A نامیده می شود. به سادگی دیده می شود، تابع از A به R/A که x را به $x + A$ می نگارد، یک همریختی پوشا بر R/A است.

تذکر ۶.۰ فرض کنیم $f : R \longrightarrow S$ یک همریختی حلقه‌ها باشد. مجموعهٔ تمام عناصر R که به ۰ نگاشته می شوند، هستهٔ f نامیده می شود. آن را با $ker(f)$ نشان می دهیم. به سادگی دیده می‌شود که $ker(f)$ یک اید آل R است. همریختی f، یک،یکریختی حلقهٔ خارج قسمتی $R/kerf$ به تصویر f یعنی $f(R)$ القا می کند.

تعریف. عنصر x در حلقهٔ R، مقسوم علیه صفر نامیده می شود، هر گاه عنصر نا صفر y در R وجود داشته باشد بطوری که $xy = 0$.

حلقهٔ ناصفر R، یعنی حلقه ای که در آن $0 \neq 1$،یک حوزهٔ صحیح نامیده می شود، هر گاه شامل مقسوم علیه صفری به جز صفر نباشد.

عنصر یکه در R عنصری است مانند u، به طوری که به ازای یک $v \in R$، $uv = 1$. یکه های R، تحت ضرب، یک گروه آبلی تشکیل می دهند. به سادگی می توان مشاهده کرد که،عنصر u در حلقهٔ R یکه است، اگر و تنها اگر اید آل اصلی تولید شده با u، برابر با R باشد.

یک‌هیأت، حوزه صحیحی است، که در آن هر عنصر نا صفر وارون پذیر باشد.

یک زیر حلقهٔ Kی هیأت F یک زیر هیأت نامیده می شود، هرگاه K تحت اعمال القا شدهٔ F، یک هیأت باشد. اگر K یک زیر هیأت F باشد، آن گاه F یک توسیع K نامیده می شود.

تعریف. برای یک حلقهٔ R با عنصر واحدِ ۱، مقصود از یک $R-$مدول یک گروه آبلیِ $(V,+)$ همراه با ضربِ اسکالری $R \times V \longrightarrow V$ است به قسمی که برای تمام rها و sها در R و v,v'ها در V

آ) $1v = v$

ب) $(rs)v = r(sv)$

پ) $(r+s)v = rv + sv$

ت) $r(v+v') = rv + rv'$

مثال‌ها. $\mathbb{Z}$ یک حوزه صحیح است. حوزه های صحیحِ $\mathbb{Q}$، $\mathbb{C}, \mathbb{R}$ مثال‌هایی از هیأت هستند. هیأت‌های $\mathbb{Q}$ و $\mathbb{R}$ زیر هیأت‌های $\mathbb{C}$ هستند. گروه‌های آبلی همانِ $Z-$مدول‌ها هستند. هر حلقهٔ R، یک مدول روی خودش می باشد و اید آل‌ها دقیقاً، $R-$زیر مدول‌های R هستند. اگر F یک هیأت باشد، یک $F-$مدول، عیناً یک $F-$فضای برداری است. در این جافرض می کنیم که خواننده با فضاهای برداری آشناست. مطالعهٔ مدول‌ها را در فصل ۸ ادامه خواهیم داد.

تمرین ۱.۰ تنها اید آل های یک هیات، $\{0\}$ و F هستند. به عکس اگر حلقهٔ R، اید آل سره نداشته باشد، آن گاه یک هیأت است.

تمرین ۲.۰ نشان دهید که هر حوزهٔ صحیحِ متناهی، هیأت است.

تعریف. ایدآل Pی حلقه R، اول نامیده می شود، هرگاه $P \neq R$ و برای هر $x, y \in R$، اگر $xy \in R$، آن گاه $x \in R$ یا $y \in R$.

یک ایدآل M در حلقهٔ R، ماکسیمال نامیده می شود، هرگاه $M \neq R$ و ایدآل A که در شرط $M < A < R$ صدق کند وجود نداشته باشد.

تذکر ۷.۰ به سادگی می توان ملاحظه کرد که ایدآل Pی حلقهٔ R اول است، اگر و تنها اگر R/P یک حوزهٔ صحیح باشد. به طور مشابه ایدآل M ماکسیمال است اگر و تنها اگر R/M یک هیأت باشد. به وضوح، هر ایدآل ماکسیمال، اول است. عکس آن، در حالت کلی درست نیست.

تمرین ۳.۰ نشان دهید که هر حلقهٔ ناصفرِ R دست کم دارای یک ایدآل ماکسیمال است.

با طرح کلی اثباتی از یک قضیه مهم، این بخش را به پایان می بریم.

قضیه ۱.۰ با فرض این که D یک حوزه صحیح باشد، هیأتی مانند F وجود دارد که شامل یک تصویر یکریختِ D، به عنوان یک زیر حلقه است.

اثبات. فرض کنیم $S := \{(a,b)|a,b \in D, b \neq 0\}$. برای عناصر S، تعریف می‌کنیم $(a,b) \sim (c,d)$، اگر $ad = bc$. به وضوح $\sim$، به علت این که D شامل مقسوم علیه صفر نیست، یک رابطهٔ هم ارزی است. با فرض این که (a,b) یک عضو S باشد ردهٔ هم ارزی (a,b) را با a/b نشان می دهیم. پس از آن ملاحظه می کنیم که جمع و ضرب که با $a/b + c/d = ad + bc/bd$، $(a/b)(c/d) = ac/bd$ در $S/\sim$ تعریف می شود خوشترتیب است و آن را به یک حلقه تبدیل می کند.

این حلقه را با F نشان می دهیم. عنصر $1/1$، عنصر همانی F است. اینک اگر a/b یک عنصرِ ناصفرِ F باشد، آن گاه $a \neq 0$ و b/a وارون آن است. بنابراین F یک هیأت است. با مشاهده این نگاشت که $i : D \longrightarrow F$ که با $i(a) = a/1$ تعریف می شود یک همریختی یک به یک از D به توی F است، اثبات کامل می شود.□

تمرین ۴.۰ گیریم D یک حوزهٔ صحیح و F هیأت ساخته شده در اثبات فوق باشد. نشان دهید که هر همریختی یک به یک مفروض مانند $f : D \longrightarrow K$ که در آن K یک هیأت است می تواند به یک طریق، به یک یکریختی از F به K بسط داده شود.

تعریف. هیأت F در اثبات قضیه ۱.۰، هیأت خارج قسمت‌های D نامیده می شود. تمرین ۴.۰ نشان می دهد که F،« کوچکترین » هیأت شامل D است.

فصل ۱

اعداد صحیح

در این فصل، به اختصار درباره بخشپذیری و نتایجی که به همنهشتی‌ها در مجموعهٔ اعداد صحیح $\mathbb{Z}$ ارتباط دارد بحث خواهیم کرد. ساختِ اصل موضوعی اعداد صحیح، همچنین بعضی خواص اساسی مجموعهٔ اعداد صحیح، مانند اصل استقرای ریاضی و این که هر مجموعهٔ ناتهیِ اعداد صحیح مثبت دارای کوچکترین عضو است را دانسته فرض می کنیم. در واقع، در فصل قبل چندین بار به مجموعهٔ $\mathbb{Z}$ ارجاع داده شده است. ملاحظه کردیم که $\mathbb{Z}$ تحت اعمال جمع و ضرب معمولی اعداد، یک حلقه است.

۱.۱ بخشپذیری

تعریف. فرض کنیم a یک عدد صحیح ناصفر است. گوییم عدد صحیح b بر a بخشپذیر است، هر گاه عدد صحیح x وجود داشته باشد، به گونه ای که $b = ax$. این بخشپذیری با نوشتن $a \mid b$ بیان می شود. چنین حالتی را با b، a را عاد می کند، a مقسوم علیهٔ b است، یا این که b مضرب a است نیز بیان می کنیم.

در حالتی که b بر a بخشپذیر نباشد، می نویسیم $a \nmid b$. اگر $a \mid b$ و $|b| < |a| < ۱$، aیک مقسوم علیه سرهٔ b نامیده می شود. نماد $a^k||b$ بدین معنی است که $a^k \mid b$، اما $a^{k+۱} \nmid b$.

قضیه ۱.۱ (الگوریتم تقسیم)
با فرض این که a و b اعدادی صحیح باشند و $a > ۰$، اعداد صحیح یکتای q و r

وجود دارند به طوری که

$$b = qa + r \qquad\qquad \circ \leq r < a$$

(در این حالت گویند q خارج قسمت و r باقی‌ماندهٔ به دست آمده در تقسیم b بر a است. اگر $a \nmid b$، آن گاه، r در شرط نا برابریِ قویتر $\circ < r < a$ صدق می‌کند)

اثبات. از آنجا که $a \geq ۱$، داریم $\circ \leq |b| + b \leq |b|a + b$. بنابراین مجموعهٔ $\boldsymbol{S := \{b - xa | b - xa \geq \circ}$ و $\boldsymbol{x \in \mathbb{Z}\}}$ ناتهی است و بنابر اصل خوشترتیبی شامل کوچکترین عدد صحیح است. آن را r می نامیم. حال به علت این که r یک عضو S است. به شکل $b - qa$ خواهد بود. اگر $r \geq a$، آن گاه $r - a = b - (q + ۱)a$ نیز یک عضو S است که با این واقعیت که r کوچکترین عضو S است، تناقض دارد. بنابراین $r < a$. اکنون به اثبات یکتایی q و r می پردازیم. فرض کنیم اعداد صحیح دیگر q' و r' وجود داشته باشند. در این صورت خواهیم داشت $|r - r'| = a|q - q'|$ و همچنین $|r - r'| < a$. از این دو برابری چنین نتیجه می شود که $|q - q'| < ۱$. از آنجا که q و q' اعدادی صحیح اند، $q = q'$ و لذا $r = r'$.$\square$

یادداشت. فرض کرده ایم که $a > \circ$. در حالت کلی، الگوریتم تقسیم می گوید که برای اعداد صحیح a و b با شرط $a \neq \circ$، q و r وجود دارند به طوری که $\circ \leq r < |a|$.

تمرین ۱.۱

الف)زیر گروه‌های، گروه جمعی $(\mathbb{Z}, +)$، یعنی گروه اعداد صحیح را بیابید.

ب)نشان دهید که هر گروه دوری، یا با گروه جمعی اعداد صحیح، $\mathbb{Z}$ یا با گروه خارج قسمتی $\mathbb{Z}/m\mathbb{Z}$ برای یک $m > \circ$ یکریخت است.

پ) ثابت کنید که هر اید آل حلقهٔ $\mathbb{Z}$، یک اید آل اصلی است.

یادداشت. یاد آوری می کنیم که یک اید آل، اصلی نامیده می شود، هرگاه با یک عضوِ تنها تولید شود. حوزهٔ صحیحی که تمام اید آل‌های آن اصلی باشند یک حوزهٔ اید آلهای اصلی (ح ا ص) نامیده می شود. بنابراین قسمت (ب) تمرین فوق می گوید که $\mathbb{Z}$ یک ح ا ص است.

قضیه ۲.۱ فرض کنیم $a, b \in \mathbb{Z}$ تواماً صفر نباشند. در این صورت یک مقسوم علیه مشترک d ی a, b به شکل $d = ar + bs$، به ازای اعداد صحیح r و s وجود دارد به گونه ای که، هرگاه عدد صحیحی مانند e، a و b را عاد کند، d را نیز عاد خواهد کرد.

اثبات. مجموعهٔ

$$S=\{ax+by|ax+by>0, x,y\in\mathbb{Z}\}$$

را در نظر می گیریم.

از آنجا که a و b با هم صفر نیستند، به سادگی دیده می شود که S ناتهی است. بنابراین S شامل کوچکترین عضو است که آن را d می نامیم. چون $d\in S$، به ازای $r,s\in S$، $d=ar+bs$.

فرض کنیم m یک عضو S است. بنابر الگوریتم تقسیم $m=qd+c$ که در آن $0\leq c<d$. اگر $m=ar_1+bs_1$، که $r_1,s_1\in\mathbb{Z}$، آن گاه $c=m-qd=a(r_1-q_1)+b(s_1-qs)$ و لذا $c\in S$. بنابراین با توجه به انتخاب d نتیجه می‌شود $c=0$. از این رو $m=qd$، به عبارت دیگر d، m را عاد می کند.

در بند قبل ثابت کردیم، با فرض این که m یک عنصر S باشد، d، m را عاد می کند. اما اعداد صحیح $a=a.1+b.0$ و $b=a.0+b.1$ به S تعلق دارند، از این رو d، a و b را عاد می کند.

اگر عدد صحیح e، a و b را عاد کند، در این صورت e، $d=ar+bs$ را عاد خواهد کرد و اثبات کامل است.□

تعریف. به دلایلی آشکار، عدد صحیح d در قضیه ۲.۱ را بزرگترین مقسوم علیهٔ مشترک، (ب م م) a و b می‌نامند، آن را با (a,b) نشان می دهند. اگر $(a,b)=1$ گویند a و b نسبت به هم اولند.

برای عدد صحیح $n\geq 1$، تابع فیِ اویلر، $\phi(n)$، تعداد اعداد صحیح مثبتی تعریف می شود که بزرگتر از n نیستند و نسبت به n اولند.

عدد صحیح $p>1$ یک عدد اول (یا به اختصار اول) نامیده می شود هرگاه تنها مقسوم علیه های مثبت p، ۱ و p باشند. بنابراین برای عدد اول p، $\phi(p)=p-1$.

با فرض این که n عدد صحیح مثبتی باشد، دو عدد صحیح a و b را به پیمانه n همنهشت می نامند و می نویسند

$$a\equiv b \pmod n$$

هرگاه $n|b-a$، یعنی به ازای عدد صحیحی مانند k، $b-a=nk$. این شرط هم ارز با آن است که $b-a$ به ایدآل $n\mathbb{Z}$ تعلق داشته باشد. همان طور که در بخش قبل ملاحظه کردیم این رابطه، یک رابطهٔ هم ارزی است. در این جا، رده های هم ارزی (همدسته ها) ردهٔ همنهشتی یا رده های مانده ای به پیمانه n نامیده می شوند. ردهٔ همنهشتی عدد صحیح a با نشانه $\overline{a}$ نشان داده خواهد شد.

مجموعه‌ای، متشکل از n نماینده که هر کدام از یک ردهٔ مانده به پیمانه n انتخاب شده اند، یک دستگاه کامل مانده ها به پیمانه n نامیده می شود. مقصود از یک مجموعه کاهش یافته به پیمانه n مجموعه‌ای متشکل از $\phi(n)$ عدد صحیح است که از رده های مانده ای متمایز انتخاب شده و هر کدام نسبت به n اول هستند.

تذکر ۱.۱ به سادگی دیده می شود که شاخص $[\mathbb{Z} : n\mathbb{Z}]$ از زیر گروه $n\mathbb{Z}$ در $\mathbb{Z}$ برابر با n است. اکنون می دانیم که تابع $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ که هر a را به ردهٔ همنهشتی $\overline{a}$ می نگارد، با جمع و ضرب سازگار است.

قضیه ۳.۱ (لم اقلیدس) اگر $a|bc$ و $(a,b) = ۱$، آن گاه $a|c$.

اثبات. از آنجا که $(a,b) = ۱$ به ازای اعداد صحیحی مانند x و y داریم $ax + by = ۱$ بنابراین

$$\begin{aligned} c &= acx + bcy \\ &= acx + ary \\ &= a(cx + ry) \end{aligned}$$

که در آن $bc = ar$، زیرا که $a|bc$.$\square$

قضیه ۴.۱ اگر عدد اول p، ab را عاد کند، آن گاه $p|a$ یا $p|b$. در حالت کلی اگر عدد اول p، حاصلضرب $a_۱a_۲\cdots a_n$ را عاد کند، دست کم یکی از این عاملها را عاد خواهد کرد.

اثبات. فرض کنیم $p|ab$ و $p \nmid a$. اینک $(p,a) = ۱$، بنابراین به موجب لم اقلیدس، $p|b$. قسمت دوم به سادگی از استقرا نتیجه می شود.

۱.۲ قضیه بنیادی حساب

قضیه ۵.۱ (قضیه بنیادی حساب) هر عدد صحیحِ $a = ۰$ را می‌توان به صورت حاصلضربِ

$$a = cp_۱ \cdots p_k$$

نوشت که در آن $c = \pm ۱$ و $p > ۰$ اعدادی اول (نه لزوماً متمایز) هستند و $k \geq ۰$. این بیان با تقریب ترتیب اعداد اول یکتاست.

اثبات. ابتدا نشان می دهیم که تجزیهٔ به عامل‌های اول وجود دارد. کافی است حالت $a > ۱$ را در نظر بگیریم. به استقرا عمل می کنیم. برای $a = ۲$ نتیجه درست است. به موجب فرض استقرا تجزیه برای تمام bهایی که $b < a$ موجود است. اگر a

اول باشد چیزی برای اثبات وجود ندارد. اگر a اول نباشد، آن گاه $a = bb'$ که در آن $b, b' > ۱$. اینک به موجب آن که b و b' اکیداً از a کوچکترند. بنا به فرض استقرا می توان آنها را به اعداد اول تجزیه کرد. با قرار دادن دو تجزیه در کنار یکدیگر، تجزیه a حاصل می شود.

در ادامه باید نشان دهیم که تجزیه یکتاست.

فرض کنیم $\pm p_۱p_۲\cdots p_n =\pm q_۱q_۲\cdots q_n$ دو چنین تجزیه ای باشند. با به کار بردن قضیهٔ ۴.۱ با قرار دادن $p = p_۱$، به ازای یک $۱ \leq i \leq m$ داریم $p_۱|q_i$، چون q_i نیز اول است، $p_۱ = q_i$. اکنون $p_۱$ را حذف کرده و از استقرا استفاده می کنیم.□

تذکر ۲.۱ * تابع زتای ریمان. $\zeta(s)$ $(s = \sigma + it)$ که برای $\sigma > ۱$ با $\sum_{n=۱}^{\infty} \frac{۱}{n^s}$ تعریف می شود و به طور برخه ریخت در صفحه مختلط گسترده شده است، با توجه به اتحاد

$$\sum_{n=۱}^{\infty} \frac{۱}{n^s} = \prod_p (۱ - \frac{۱}{p^n})^{-۱}, \sigma > ۱$$

در درون خود حاوی اطلاعات ژرفی در بارهٔ ماهیت ضربی اعداد صحیح است.

این اتحاد هم ارز تحلیلی قضیه ۵.۱ فوق می باشد.

قضیه ٦.۱ (اقلیدس) بی نهایت عدد اول وجود دارد.

اثبات. فرض کنیم $p_۱p_۲\cdots p_n$ تعدادی متناهی عدد اول بوده و $۱ < p_۱ < p_۲ \cdots < p_n$. فرض کنیم $N = ۱ + p_۱p_۲\cdots p_n$. بنابر قضیه بنیادی حساب، عدد اول $p > ۱$ وجود دارد که N را عاد می کند. اگر به ازای یک $۱ \leq i \leq n$ داشته باشیم $p_i = p$، نتیجه خواهیم گرفت که $p_i|۱$ که ممکن نیست. بنابراین نشان دادیم که اگر تعدادی متناهی عدد اول داده شده باشند، همواره عدد اولی متمایز از همهٔ آنها وجود خواهد داشت. این امر قضیه را ثابت می کند.

تمرین ۲.۱ با تقلید از قضیه فوق نشان می دهید که بی نهایت عدد اول به شکل $۴k + ۳$ وجود دارد.

تذکر ۳.۱ * قضیه دیریکله در مورد اعداد اول درتصاعدهای حسابی می گوید که اگر $(a, m) = ۱$، تصاعد حسابی $mn + a$، $n = ۱, ۲, \cdots$ شامل بی نهایت عدد اول است. در تمرین‌های ٦.۱، ۷.۳ (ت ۴) با توجه به دانش پیشتر نظریه اعداد، مواردی از نوع استدلال اقلیدس که حالت‌های خاص تصاعد حسابی را به دست می دهد ملاحظه خواهیم کرد. با این حال اثبات اقلیدس را نمی توان در حالت کلی برای قضیه دیریکله به کار برد.

استدلال اصلی دیریکله که استدلالی تحلیلی است، ریشه در اثباتِ اویلر در نامتناهی بودن اعداد اول دارد. استدلال اویلر چنین است:
اگر $x \geq ۲$ و عدد صحیح m چنان باشد که $x \leq ۲^m$، آن گاه

$$\prod_{p \leq x}(۱ - \frac{۱}{p})^{-۱} > \prod(۱ + \frac{۱}{p} + \cdots + \frac{۱}{p^m}) \geq \sum_{n=۱}^{[x]} \frac{۱}{n}$$

که از آن نتیجه می شود $\prod_{p \leq x}(۱ - \frac{۱}{p})^{-۱}$ وقتی $x \longrightarrow \infty$، واگرا است.

تمرین ۳.۱
الف) اگر m و m' اعداد صحیح مثبتی باشند، به طوری که $(m, m') = ۱$ و a، a' به ترتیب در مجموعهٔ کامل مانده ها به پیمانه m و m' تغییر کنند، آن گاه نشان دهید که $a'm + am'$ در مجموعهٔ کامل مانده ها به پیمانه mm' تغییر می کند.
ب) چنانچه m و m' همان اعداد مذکور در (الف) باشند، نشان دهید که $\phi(mm') = \phi(m)\phi(m')$، که در آن ϕ تابعِ اویلر است. در این حالت گویند ϕ ضربی است.
پ) فرض کنید $n > ۱$ یک عدد صحیح باشد، اگر $n = p_۱^{a_۱} p_۲^{a_۲} \cdots p_k^{a_k}$، که در آن p_iها اعداد اول متمایزند، آن گاه

$$\phi(n) = n \prod_{i=۱}^{k}(۱ - \frac{۱}{p_i})$$

تمرین ۴.۱ اگر $(a, m) = ۱$، آن گاه همنهشتی $ax \equiv b \pmod m$ دقیقاً دارای یک جواب به پیمانه m است.

تمرین ۵.۱ اویلر—فرما اگر $(a, m) = ۱$، آن گاه $a^{\phi(m)} \equiv ۱ \pmod m$ که در آن ϕ تابع اویلر است.

تمرین ۶.۱ فرض کنید p یک عدد اول فرد است. اگر عدد طبیعی n چنان باشد که $n^۲ + ۱$ بر p بخشپذیر باشد، آن گاه p به شکل $۴m + ۱$ است (عکس این موضوع نیز صحیح است قضیه ۱.۳(پ) را ببینید). نتیجه بگیرید که بی نهایت عدد اول به شکل $۴m + ۱$ وجود دارد.

تمرین ۷.۱ آیا معادلهٔ $x^۲ + ۱ = ۳y^۵$ دارای جواب صحیح است؟

تذکر ۴.۱ معادله هایی که باید برای اعداد صحیح حل شوند به معادله های **دیوفانتی** موسومند (پس از دیوفانت اسکندرانی ۲۵۰ پس از میلاد). با این اصطلاح، تمرین فوق را می توان چنین بیان کرد که آیا معادلهٔ دیوفانتی $x^۲ + ۱ = ۳y^۵$ دارای جواب است؟

۱.۳ قضیهٔ باقی ماندهٔ چینی

قضیهٔ باقی ماندهٔ چینی که در صدد بحث در بارهٔ آن هستیم، ریشه در دوران باستان دارد. خواننده مشتاق می تواند به کتاب جدید، دینگ[۱]، پی[۲] و سالموا [۳]، [DPS۱۹۹۶] که به کاربرد های متنوع این قضیه پرداخته است مراجعه کند. حدود سدهٔ اول پس از میلاد، قضیهٔ باقی ماندهٔ چینی توسط سون شی در طی یک مسئله به ویژه عنوان شد. بعدها در ۱۹۵۳، چنگ داوی حلِ سون چی را با یک ترانه شرح داد. ذیلاً ترانه اصلی چینی را با ترجمهٔ آن می آوریم.

"*Sun ren tong xing qi shi xi,*
wu shu mei hua nian yi zhi,
qi zhi tuan yuan zheng ban yue,
chu bai lhng wu bian de zhi."

سه نفر، همگام، بعید است که یکی هفتاد باشد
پنج درخت با شکوفه های گیلاس
بیست و یک شاخه پر از میوه
هفت مرید برای نیمه ماه متحد شدند
صدوپنج از آن بردارید و خواهید دانست

از اثبات قضیهٔ باقی ماندهٔ چینی ملاخظه خواهیم کرد این ترانهٔ معما گونه، در واقع به حل همزمان x از همنهشتی‌های زیر دلالت می کند.

$$\begin{array}{lcll} x & \equiv & b_۱ & \pmod{۳} \\ x & \equiv & b_۲ & \pmod{۵} \\ x & \equiv & b_۳ & \pmod{۲} \end{array}$$

---

[۱] Ding
[۲] Pei
[۳] Salomaa

قضیه ۷.۱ (**قضیه باقی مانده چینی**) فرض کنیم $m_1, m_2, \cdots, m_r$ اعداد صحیح مثبت اند که دو به دو نسبت به یکدیگر اول هستند، یعنی اگر $i \neq k$، آن گاه $(m_i, m_k) = 1$. در این صورت برای اعداد صحیح دلخواه $b_1, b_2, \cdots, b_r$ دستگاه همنهشتی های

$$\begin{array}{cccc} x & \equiv & b_1 & \pmod{m_1} \\ x & \equiv & b_2 & \pmod{m_2} \\ \cdots & \cdots & \cdots & \cdots \\ x & \equiv & b_r & \pmod{m_r} \end{array}$$

به پیمانه $m_1 m_2 \cdots m_r$ دقیقاً دارای یک جواب است.

اثبات. فرض کنیم $M = m_1 m_2 \cdots m_r$ و $M_k = M/m_k$. اینک $(M_k, m_k) = 1$ و M_k دارای وارون یکتای M'_k به پیمانه m_k است.

فرض کنیم $x = b_1 M_1 M'_1 + b_2 M_2 M'_2 + \cdots + b_r M_r M'_r$. از آنجا که برای $i \neq k$ $M_i \equiv 0 \pmod{m_k}$، داریم $x \equiv b_k M_k M'_k \equiv b_k \pmod{m_k}$. بنابراین x در هر یک از معادله های همنهشتی صدق می کند. اگر x و y دو جواب دستگاه باشد، $x \equiv y \pmod{M}$.$\square$

تمرین ۸.۱ دستگاه معادله های همنهشتی زیر را حل کنید.

$$\begin{array}{cccc} x & \equiv & 2 & \pmod{3} \\ x & \equiv & 3 & \pmod{5} \\ x & \equiv & 2 & \pmod{7} \end{array}$$

تذکر ۵.۱ در این جا مناسب است که ترانه چینی را مجدداً بخوانیم. در هنگام حل تمرین فوق به همراه اثبات قضیهٔ ۷.۱ (با نماد گذاری قضیه) داریم $r = 3$ و $M = 105$. ترانه، اعداد $M_i M'_i$ را برای $i = 1, 2, 3, \cdots$ به دست می دهد. این مقادیر به ترتیب عبارتند از $70 = 2 \times 35$ و $21 = 1 \times 21$ و $15 = 1 \times 15$ (در این جا باید توجه کنیم که نیمه ماه به نصف تعداد روزهای یک ماه قمری یعنی ۱۵ معطوف است.) این اعداد به ترتیب باید در باقی مانده های ۲، ۳و۲ (b_iهای قضیه) که متناظر با اعداد اول ۳، ۵ و ۷ باشند ضرب شوند. پس از جمع اعدادی که بدین ترتیب حاصل می‌شوند باید ۱۰۵ را از آن برداریم، یعنی کم کنیم تا کوچکترین جواب به دست آید.

تمرین ۹.۱ فرض کنید $F(x)$ یک چند جمله ای با ضرایب صحیح باشد. (در صورت لزوم، برای تعریف چند جمله ای، فصل ۲ را ببینید). فرض کنید $m_1, m_2, \cdots, m_r$ اعداد صحیح مثبتی باشند که دو به دو نسبت بهم اولند. فرض

کنید $m = m_۱ m_۲ \cdots m_r$. ثابت کنید همنهشتی $F(x) \equiv ۰ \pmod{m}$ دارای جواب است، اگر و تنها اگر هر یک از همنهشتیهای $F(x) \equiv ۰ \pmod{m_i}$ برای $i = ۱, ۲, \cdots, r$ دارای جواب باشد.

تمرین ۱۰.۱

آ) اگر p عدد اول فرد باشد، نشان دهید که اعداد صحیح a و b وجود دارد به طوری که $a^۲ + b^۲ + ۱ \equiv ۰ \pmod{p}$

ب) نشان دهید که نتیجه فوق حتی اگر p^r به جای p جایگزین شود که در آن p عدد اول فرد است و $r \geq ۱$ نیز برقرار است.

پ) از (آ) و (ب) نتیجه بگیرید که برای هر عدد صحیح و مثبت فردِ m، اعداد صحیح a و b وجود دارد به طوری که $a^۲ + b^۲ + ۱ \equiv ۰ \pmod{m}$.

فصل ۲

حلقه‌های چند جمله‌ای

این فصل را با تعریفِ صوری حلقهٔ چند جمله‌ای‌ها با ضرایب در یک حلقه شروع می کنیم. با ساختن مجموعهٔ متشکل از چند جمله‌ای‌ها با ضرایب در یک حلقه، به حلقه های جدیدی که به نوبه خود بسیار با اهمیت به نظر می رسند، دسترسی پیدا خواهیم کرد. برخی از خواص حلقهٔ چند جمله‌ای‌ها روی یک هیأت را نیز به دست خواهیم آورد. این نتایج نقش مهمی در مطالعهٔ توسیع هیأت ها دارند.

۲.۱ حلقهٔ چند جمله ایها

تعریف. یک‌چند جمله ای با یک متغیر و با ضرایب در حلقهٔ R عبارتی است به شکل

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

که در آن برای هر i، $a_i \in R$.

به طور رسمی ، یک چند جمله ای، با ضرایب یا بردارهای $(a_0, a_1, \cdots, a_n, \cdots)$ که $a_i \in R$ و تمام a_iها، مگر تعدادی متناهی، صفر هستند، مشخص می شود. درجهٔ یک چند جمله ای نا صفرِ $f(x)$ که آن را با $degf(x)$ نشان می دهیم، بزرگترین عدد صحیح k است به قسمی که ضریب a_kی x^kصفر نیست. ضریب بزرگترین درجه یک چند جمله‌ای، که صفر نیست،ضریب پیشرو نامیده می شود. یک چند جمله‌ای تکین ، چند جمله ای است که ضریب‌پیشرو آن برابر با ۱، یعنی عضو همانی حلقهٔ R باشد.

جمع و ضرب چند جمله‌ای‌ها همانند جمع و ضرب معمولی توابع چند جمله ای حقیقی است. دقیق تر بگوییم، اگر $R[x]$ مجموعهٔ چند جمله‌ای ها با ضرایب در R را نشان دهد و جمع را با

$$(a_۰, a_۱, \cdots) + (b_۰, b_۱, \cdots) = (a_۰ + b_۰, a_۱ + b_۱, \cdots)$$

تعریف کنیم، آن گاه $(R[x], +)$ یک گروه آبلی است.
با ضربی که در $R[x]$ با

$$(a_۰, a_۱, \cdots).(b_۰, b_۱, \cdots) = (p_۰, p_۱, \cdots),$$

تعریف می شود، که در آن $p_i = \sum_{j+k=i} a_j b_k$، $(R[x], +, .)$ یک حلقهٔ تعویض‌پذیر می شود. عنصر $(۰, ۰, \cdots) = ۰$، به عنوان صفرِ این حلقهٔ و $(۱, ۰, ۰ \cdots) = ۱$ به عنوان عنصر همانی این حلقه عمل می کنند.

برای تعریف حلقهٔ چند جمله‌ای‌ها با دو متغیر x و y، خواننده می تواند ثابت کند که دو حلقهٔ $(R[x])[y]$ و $(R[y])[x]$ به طور طبیعی یکریخت هستند. با یکی گرفتن این دو حلقه و نوشتن $R[x, y]$ برای هر دوی آنها، حلقهٔ $R[x, y]$ را حلقهٔ چند جمله‌ای ها با دو متغیر x و y می نامند. به طور مشابه می توان حلقهٔ $R[x_۱, x_۲, \cdots, x_n]$ را با n متغیر تعریف کرد. برای عنصر

$$f = f(x_۱, x_۲, \cdots, x_n) = \sum_{a_{i_۱ \cdots i_n}} x_۱^{i_۱} \cdots x_n^{i_n} \in F[x_۱, \cdots x_n]$$

درجهٔ f، ماکسیمم مجموع $i_۱ + i_۲ + \cdots i_n$ است. که در تمام جمله ها حساب می شود.

تمرین ۱.۲ اگر R یک حوزهٔ صحیح باشد، نشان دهید که $R[x]$ نیز یک حوزه صحیح است.

تمرین ۲.۲ فرض کنیم $\phi : R \longrightarrow R'$ یک همریختی حلقه ها باشد. با فرض این که $\alpha \in R'$، نشان دهید که یک همریختی یکتایِ $\phi : R[x] \longrightarrow R'$ وجود دارد به طوری که x را به α می نگارد و تحدید آن به R برابر با ϕ است.

فرض کنیم R یک زیر حلقهٔ R' و $\alpha \in R$، اگر $i : R \longrightarrow R'$ نگاشت شمول باشد، همریختی یکتایِ مذکور در تمرین قبل، که i را به $R[x]$ بسط می دهد، تابع ارزیابی نامیده و آن را با I نشان می دهیم.

اگر $f \in R[x]$ و اگر $f(\alpha) := I(f) = ۰$، α یک ریشه یاصفر f در R' نامیده می شود.

فرض کنیم $i : \mathbb{Z} \longrightarrow \mathbb{C}$ تابع شمول باشد، برای هر عدد مختلط α تابع شمول یکتای $I : \mathbb{Z}[x] \longrightarrow \mathbb{C}$ را مانند فوق در نظر می گیریم. در این صورت، نگارهٔ حاصل که با $Z[\alpha]$ نشان داده می شود، کوچکترین زیر حلقهٔ $\mathbb{C}$ است که شامل α می باشد. مجموعهٔ $\mathbb{Z}[\alpha]$ شامل تمام عناصری به شکل $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0$ است که $a_i \in \mathbb{Z}$. اگر هستهٔ تابع I، صفر نباشد، α یک عدد جبری نامیده می شود. از طرفی اگر هیچ چند جمله ای با ضرایب صحیح وجود نداشته باشد که α ریشه آن باشد، α یک‌عدد متعالی نامیده می شود. از آنجا که مجموعهٔ اعداد جبری شماراست، چنین نتیجه می گیریم که اعداد متعالی وجود دارند. اگر α یک عدد متعالی باشد، آن گاه $\mathbb{Z}[x] \simeq \mathbb{Z}[\alpha]$. تابعی که این یکریختی را به وجود می آورد، $p(\alpha)$ را به $p(x)$ می نگارد.

۲.۲ تقسیم در حلقهٔ چند جمله‌ای‌ها

تقسیم با باقیمانده برای چند جمله‌ای‌ها عبارت است از:

قضیه ۱.۲ اگر $f(x), g(x) \in R[x]$ و ضریب پیشرو $f(x)$ در R یکه باشد، آن گاه، چند جمله‌ای‌های $q(x), r(x) \in R[x]$ وجود دارند به طوری که $g(x) = f(x)q(x) + r(x)$. به قسمی که $degr(x) < degf(x)$ یا این که $r(x) = 0$.
اثبات. اثبات با فرایندِ تقسیم طولانی است. اگر درجه $g(x)$ اکیداً از درجه $f(x)$ کوچکتر باشد، می توانیم قرار دهیم $q(x) = 0$ و $r(x) = g(x)$ تا برابریِ $g(x) = of(x) + g(x)$ که شرط مورد نظر را دارد. حاصل شود.

بنابراین فرض می کنیم درجه های $g(x)$ و $f(x)$ به ترتیب برابر با m و n است و علاوه بر آن $m \geq n$. فرض کنیم،
$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_n$ و $g(x) = b_ma^m + b_{m-1}x^{m-1} + \cdots + b_0$.
به موجب فرض a_n در R یکه است، پس a_n^{-1} در R وجود دارد که $a_na_n^{-1} = 1$.
چند جمله ای $g_1(x) = g(x) - b_ma_n^{-1}x^{m-n}f(x)$ را در نظر می گیریم. اگر $g_1(x) = c_kx^k + c_{k-1}x^{k-1} + \cdots + c_0$ و $c_k \neq 0$، در این صورت $k \leq m - 1$.
اگر $k \geq n$ فرآیند را ادامه می دهیم تا$g_2(x)$ و غیره و غیره به دست آید و $g_i(x)$ حاصل شود که درجهٔ آن اکیداً کوچکتر از n است. مشاهده می کنیم که $g(x) = (b_ma_n^{-1}x^{m-1} + c_ka_n^{-1}x^{k-n} + \cdots)f(x) + r(x)$ و $r(x) = g_0(x)$. $\square$

تذکر ۱.۲ از قضیهٔ بالا به سادگی نتیجه می شود که اگر $g(x)$ یک چند جمله ای در $R[x]$ و $\alpha \in R$، به طوری که $g(\alpha) = ۰$، آن گاه به ازای یک $q(x) \in R[x]$، $g(x) = (x-\alpha)q(x)$.

می توان اثبات این که هر ایدآل حلقهٔ اعداد صحیح، اصلی است را اقتباس کرده و تمرین زیر را اثبات کرد.(تمرین ۱.۱ قسمت پ را ببینید.)

تمرین ۳.۲ فرض کنید F یک هیأت باشد. نشان دهید که هر ایدآل حلقهٔ چند جمله‌ای های $F[x]$، اصلی است.

تمرین ۴.۲ فرض کنید F یک هیأت است و $f(x), g(x) \in R[x]$ که هر دو با هم صفر نیستند، در این صورت چند جمله‌ای تکین و یکتای $d(x)$ که بزرگترین مقسوم علیه مشترک f و g نامیده می شود وجود دارد به طوری که

آ) ایدآل تولید شده با f و g می تواند با d تولید شود.

ب) d، f, g را عاد می کند.

پ) اگر h مقسوم علیه f و g باشد، آن گاه h، d را عاد می کند.

ت) چندجمله ایهای $p, q \in R[x]$ وجود دارد به طوری که $d = pf + qg$.

تعریف. فرض کنیم F یک هیأت باشد. چند جمله ای $p(x) \in f[x]$ راتحویل ناپذیر می نامند، هر گاه، یک چند جمله ای ثابت نبوده و تنها مقسوم علیه های با درجه کمتر آن در $F[x]$، چند جمله‌ای های ثابت باشند.

معمولاً یک چند جمله ای تحویل ناپذیر را با عامل گیری ضریب پیشرو آن می توان به حالت نرمال در آورده تا به یک چند جمله ای تکین تبدیل شود.

مانندِ حالت اعداد صحیح، می توان نتیجه زیر را به دست آورد.

قضیه ۲.۲ فرض کنیم F یک هیأت و $F[x]$ حلقهٔ چند جمله‌ای ها با ضرایب در R باشد. در این صورت هر چندجمله ای ناصفر $f \in R[x]$ را می توان به صورت $f = cp_۱p_۲\cdots p_r$ نوشت که در آن $r \geq ۰$، $c \neq ۰$. یک عنصر F و p_iها چندجمله‌ای های تحویل ناپذیر در $F[x]$ هستند، نوشت این تجزیه، مگر برای ترتیب چند جمله‌ای‌ها یکتاست.

قضیه ۳.۲ فرض کنیم F یک هیأت و $f(x)$ یک چندجمله ای از درجهٔ n و ضرایب در F باشد. در این صورت f حداکثر n ریشه در F دارد.

اثبات. اگر f از درجه ۱ باشد، اثبات بدیهی است. فرض کنیم $\alpha \in F$ یک ریشه f باشد، در این صورت $f(x) = (x-\alpha)q(x)$ که $q(x)$ یک چندجمله ای از درجهٔ

$n - ۱$ است. اگر β یک ریشه دیگر باشد، آن گاه $(\beta - \alpha)q(\beta) = ۰$. اگر $\beta \neq \alpha$، پس $q(\beta) = ۰$. اما به موجب استقرا $q(x)$ حداکثر $n - ۱$ ریشه دارد.□

تذکر ۲.۲ این واقعیت که F یک هیأت است در قضیه بالا اساسی است. برای مثال اگر $R = \mathbb{Z}/۸\mathbb{Z}$، چند جمله ای $x^۲ - ۱ = (x + ۱)(x - ۱) = (x + ۳)(x - ۳)$ در $R[x]$ دارای چهار ریشه است.

مجموعه تمرین الف

آ . ۱ برای هر عدد صحیح $n \geq ۲$، نشان دهید که $\frac{۱}{۲}+\frac{۱}{۳}+\cdots+\frac{۱}{n}$ یک عدد صحیح نیست.

آ . ۲ فرض کنید اعداد صحیح a و b نسبت به هم اول باشند. ثابت کنید که اعداد صحیح m و n وجود دارند به طوری که $a^m+b^n \equiv ۱ mod ab$.

آ . ۳ یادآوری می کنیم که برای هر عدد صحیح و مثبت n، $\varphi(n)$ (تابع فی اویلر) ، برابر با تعداد اعداد صحیح بین ۱ و n است که نسبت به n اول هستند. ثابت کنید که $\sum_{d|n}\varphi(d)=n$.

آ . ۴ فرض کنید G یک گروه متناهی بامرتبه n و عضو همانی ۱ است. همچنین فرض کنید برای هر مقسوم علیه dی n، تعداد عناصر a در G که در برابری $a^d=۱$ صدق می کند از d بیشتر نیست. نشان دهید که G دوری است.

آ . ۵ نشان دهید که $۲^{\frac{۴}{۲}}+۷$ و $\sqrt{۳}+\sqrt{-۵}$ اعدادی جبری اند.

آ . ٦ فرض کنید $\mathbb{Q}[\alpha,\beta]$ کوچکترین زیر حلقه $\mathbb{C}$ است که شامل $\mathbb{Q}$، $\alpha=\sqrt{۲}$ و $\beta=\sqrt{۳}$ می باشد. همچنین فرض کنید $\gamma=\alpha+\beta$. نشان دهید که

$$\mathbb{Q}[\alpha,\beta]=\mathbb{Q}[\gamma].$$

آ . ۷ گروه یکه های حلقهٔ $\mathbb{Z}/۱۲\mathbb{Z}$ را توصیف کنید.

آ . ۸ اعدادصحیح گاوسی، یک زیر حلقهٔ اعداد مختلط است که با

$$\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$$

تعریف می شود. نشان دهید که $\mathbb{Z}[i]/(۱+۳i)$ با حلقهٔ $\mathbb{Z}/۱۰\mathbb{Z}$ یکریخت است.

آ . ۹ ثابت کنید که هر ایدآل ناصفر حلقهٔ اعداد گاوسی شامل یک عدد صحیح ناصفر است.

فصل ۳

باز شناخت حلقه‌ها و هیأت‌ها

در این فصل، تعریف ها و نتیجه های مقدماتی دیگری درباره حلقه ها و هیأت‌ها، که تا قبل از فصل اعداد صحیح و چند جمله‌ای‌ها امکان پرداختن به آنها وجود نداشت را مرور خواهیم کرد. برخی نتایج مهم نظریهٔ اعداد را نیز از طریق جبری به دست خواهیم آورد.

۳.۱ مشخصهٔ یک حلقه

تعریف. فرض کنیم R یک حلقه است. اگر عدد صحیح و مثبت n وجود داشته باشد به قسمی که $\underbrace{(۱ + ۱ + \cdots + ۱)}_{n} = n۱ = ۰$. در این صورت کوچکترین چنین عدد صحیح مثبتی مشخصهٔ R نامیده می شود. در این حالت گوییم مشخصهٔ حلقهٔ R متناهی است. اگر چنین عددی وجود نداشته باشد، به تناقض گویند R با مشخصهٔ صفر است.

تمرین ۱.۳ مشخصهٔ هر حوزهٔ صحیح، یا صفر یا این که یک عدد اول است.

تذکر ۱.۳ از تمرین ۴.۱ نتیجه می شود که اگر $(a, m) = ۱$، همنهشتی، $ax \equiv ۱ (modm)$ دارای جواب یکتا به پیمانه m است. بنابراین ملاحظه می کنیم که اگر p عددی اول باشد، آن گاه $\mathbb{Z}/p\mathbb{Z}$ یک هیأت است.(این هیأت با $\mathbb{F}_p$ نشان داده می شود).

مشخصهٔ $\mathbb{F}_p$ برابر با p است.مشخصهٔ حلقهٔ $\mathbb{Z}$ و هیأت $\mathbb{Q}$، هر کدام برابر با صفر است.

از آنجا که مشخصهٔ هر حلقه، همان عدد صحیح نا منفی است که هستهٔ همریختی تعریف شده از $\mathbb{Z}$ به $\mathbb{R}$ را، که ۱ را به عنصر همانی R می نگارد، تولید می کند، نتیجه می گیریم که R شامل یک زیر حلقهٔ یکریخت با $\mathbb{Z}$ یا یکریخت با $\mathbb{Z}/m\mathbb{Z}$ به ازای یک عدد صحیح m مثبت است. اگر R یک حوزهٔ صحیح باشد، شامل یک زیر حلقه یکریخت با $\mathbb{Z}$ یا $\mathbb{Z}/(p)$ است که p عددی اول است. بنابراین هر هیأت شامل یک زیر هیأت یکریخت با $\mathbb{Q}$ یا یک زیر هیأت یکریخت با $\mathbb{F}_p$ به ازای یک عدد اول p است.

تعریف. هیأت های $\mathbb{Q}$ و $\mathbb{F}_p$،هیأت های اول نامیده می شوند. هیأتی که شامل تعدادی متناهی عنصر باشد، هیأت متناهی نامیده می شود.

تذکر ۲.۳ هم اکنون هیأتهای $\mathbb{F}_p$، تعدادی نامتناهی، از هیأت‌های متناهی در اختیار ما قرار می دهند. خواهیم دید که هیأ تهای متناهی دیگری نیز وجود دارند. هر هیأت متناهی قطعاً مشخصهٔ متناهی خواهد داشت. حلقهٔ چند جمله‌ای‌های $\mathbb{F}_p[x]$ مثالی از یک حوزهٔ صحیح نامتناهی است که مشخصهٔ آن متناهی است.

تذکر ۳.۳ از تمرین آ.۴ و قضیهٔ ۲.۳ نتیجه می شود که یک زیر گروه متناهی زیر گروه ضربی عناصر ناصفر یک هیأت باید دوری باشد. به ویژه گروه ضربی عناصر نا صفرِ یک هیات متناهی، دوری است.

تمرین ۲.۳ اگر G یک گروه آبلی متناهی باشد، عنصر $x \in G$ وجود دارد که مرتبه آن کوچکترین مضرب مشترک مرتبه عناصر G است. بدین ترتیب اثبات دیگری از این واقعیت ارائه دهید که گروه ضربی عناصر نا صفر یک هیأت متناهی دوری است.

تمرین ۳.۳ فرض کنید R یک حوزه صحیح بامشخصهٔ p باشد، که p عددی اول است. ثابت کنید تابعی که از R به R با $x \longrightarrow x^p$ تعریف می شود یک همریختی حلقه ها است. (این همریختی، همریختی فروبنیوس نامیده می شود).

۳.۲ قضیه ویلسون

قضیه ۱.۳

یک) (**قضیه ویلسون**) برای هر عدد اول p

$$(p-1)! \equiv -1 (mod p).$$

دو) عکس قضیه ویلسون نیز درست است، یعنی اگر عدد صحیح مثبت $n > 1$، $(n-1)! + 1$ را عاد کند، آن گاه n عددی اول است.
سه) اگر p عددی اول به شکل $4k+1$ باشد، عدد طبیعی n وجود دارد به قسمی که p، n^2+1 را عاد می کند. **اثبات.** گروه ضربی عناصر وارونپذیر هیأت $\mathbb{F}_p$ را در نظر می گیریم. برای عدد صحیح a، $\overline{a}$ ردهٔ باقیمانده به پیمانه p را نشان می دهد. از آنجا که تنها ریشه های معادله $x^2-1=0$ در $\mathbb{F}_p$، ۱ و ۱− است، هیچ عنصر ناصفر دیگری که وارون ضربی خودش باشد وجود ندارد. بنابراین تمام عناصر نا صفر $\mathbb{F}_p$ را می توان به صورت (α,α^{-1}) جور کرد. پس $\overline{1}.\overline{2}\cdots\overline{p-1} = \overline{1}.\overline{(-1)} = \overline{(-1)}$ که اثبات قسمت (یک) را کامل می کند.

برای اثبات قسمت (دو) فرض کنیم به ازای $n > 1$، عدد صحیح مثبتی باشد که $(n-1)!+1$ را عاد می کند. پس به ازای عدد صحیحی مانند k، $nk = (n-1)!+1$ که نشان می دهد هیچ یک از اعداد $1, 2, \ldots, n-1$، n را عاد نمی کنند، بنابراین n یک عدد اول است.

اکنون فرض کنیم p یک عدد اول به شکل $4n+1$ است. از (یک) داریم

$$\begin{aligned}\overline{(-1)} &= \overline{1}.\overline{2}.\cdots\overline{(p-1)}\\ &= (\overline{1}.\overline{2}\cdots\overline{(p-1)/2})\overline{(-(p-1)/2)}\cdots\overline{(-2)(-1)}\end{aligned}$$

بنابراین p، $(-1)^{\frac{p-1}{2}}(1.2\cdots\frac{p-1}{2})^2+1$ را عاد می کند. از آنجا که p به شکل $4n+1$ است، $(-1)^{\frac{p-1}{2}} = 1$ و اثبات تمام است.□

تمرین ۴.۳ از قضیهٔ ۳.۲ نتیجه بگیرید که اگر p یک عدد اول باشد، هر ضریب چند جمله ایِ $f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$ بر p بخشپذیر است. بدین ترتیب ملاحظه کنید که اثبات دیگری از قضیه ویلسون به دست می آید.

۳.۳ نتیجه ای در مورد فضاهای برداری

این فصل را با نتیجه قابل توجه‌ای برای فضاهای برداری روی هیأت‌های نامتناهی به پایان می بریم. بعدها از این نتیجه استفاده خواهیم کرد.

قضیه ۲.۳ فرض کنیم V یک فضای برداری روی یک هیأت نامتناهی K باشد، در این صورت نمی توان V را به صورت اجتماعی متناهی از زیر فضاهای سرهٔ V نوشت. **اثبات.** اثبات با استفاده از استقرا روی n، تعداد زیر فضاهاست. اگر $n = 1$،

نتیجه بدیهی است. فرض کنیم نتیجه برای $n < m$ درست باشد. اکنون فرض کنیم m زیر فضای سرهٔ $V_1, V_2, \cdots, V_m$ موجود است. به موجب فرض استقرا، $e \in V$ وجود دارد که برای $i = 1, \cdots, m-1$، $e \notin V_i$. اگر $e \notin V_m$ چیزی برای اثبات باقی نمی ماند. فرض کنیم $e \in V_m$، عنصر $f \notin V_m$ را انتخاب می کنیم. در این صورت برای هر عنصر ناصفر $c \in K$، $e + cf \notin V_m$.

ادعا می کنیم که $c_0 \in K^*$ وجود دارد که برای هر i، $1 \leq i \leq m$، $e + c_0 f \notin V_i$، زیرا در غیر این صورت به علت این که K نامتناهی است، $c_1, c_2 \in K^*$ وجود دارند که $c_1 \neq c_2$، به طوری که برای یک $i < m$، $e + c_1 f, e + c_2 f \in V_i$. بنابراین $(c_1 - c_2) f \in V_i$، یعنی $f \in V_i$ و لذا $e \in V_i$ که یک تناقض است.□

فصل ۴

تجزیه به عامل‌ها

در این فصل تجزیه به عامل‌های اول را در یک حوزه صحیح مورد توجه قرار می دهیم. در فصل ۱، ملاحظه کردیم که در حلقهٔ اعداد صحیح، قضیهٔ بنیادی حساب تجزیه یکتای عناصر ناصفر به اعداد اول را با تقریب ترتیب و مضرب‌های ۱ و ۱− موجب می شود. می توان در جستجوی حلقه هایی با ویژگیهای مشابه بود. در حالت اعداد صحیح، الگوریتم تقسیم برای اثبات یکتایی تجزیه به عامل‌ها مورد استفاده قرار گرفت. این الگوریتم تقسیم را می توان به طریقی مناسب تعمیم داده و در پی یافتن حلقه هایی با چنین ویژگی‌ها باشیم. خواهیم دید که برای هیأت F، حلقهٔ چند جمله‌ای های $F[x]$، می تواند چنین حلقه ای باشد. مثال‌های دیگری را نیز ملاحظه خواهیم کرد.

۴.۱ بخشپذیری

این بخش را با تعمیمِ بخشپذیری، مطرح شده در حالت اعداد صحیح در فصل یک، شروع می کنیم.

تعریف . فرض کنیم R یک حوزه صحیح است. گویند عنصرِ نا صفرِ $a \in R$ عنصر b را عاد می کند، هر گاه به ازای یک $q \in R$، $b = aq$. در این صورت می نویسیم $a|b$.

عنصر a، مقسوم علیه سرهٔ b است هر گاه به ازای یک $q \in R$، $b = aq$ با این شرط که a و q یکه نباشند.

عنصر ناصفر a در R تحویل ناپذیر نامیده می شود هر گاه یکه نبوده و مقسوم علیه سره نداشته باشد.

دو عنصر a و a' وابسته نامیده می شوند، هر گاه هر کدام دیگری را عاد کند. به عبارت دیگر هر گاه یکهٔ u وجود داشته باشد که $a = ua'$.

گزاره‌های زیر بدیهی اند.

یک) u یکه است اگر و تنها اگر $(u) = (1)$

دو) a و a' وابسته هستند اگر و تنهااگر $(a) = (a')$.

سه) b, a را عاد می کند، اگر و تنها اگر $(b) \subset (a)$.

چهار) a مقسوم علیه سرهٔ b است اگر و تنها اگر $(1) > (a) > (b)$.

۴.۲ ح ت ی و ح ا ص

قضیه ۱.۴ فرض کنیم R یک حوزهٔ صحیح است. در این صورت شرط‌های زیر هم ارزند.

آ) برای هر $a \in R$ که نا صفر و نایکه است، رونډِ تجزیه به عامل‌ها پس از تعدادی متناهی مرحله پایان می پذیرد و به تجربهٔ $a = b_1 b_2 \cdots b_r$ به عناصر تحویل ناپذیر می انجامد.

ب) R شامل زنجیر نامتناهیِ افزایشی اید آل‌های اصلی $(a_1) < (a_2) \cdots (a_n) < \cdots$ نیست.

اثبات.

(آ) $\Longrightarrow$ (ب):

فرض کنیم (آ) برقرار باشد. در صورت امکان، فرض کنیم R شامل یک زنجیر نامتناهیِ افزایشی اید آل‌های اصلی $(a_1) < (a_2) \cdots < (a_n) < \cdots$ است. به وضوح هیچ یک از a_iها یکه نیستند. اینک $(a_n) < (a_{n+1})$، که ایجاب می کند a_{n+1} یک مقسوم علیه سرهٔ a_n است، مثلاً $a_n = a_{n+1} b_{n+1}$ که a_{n+1} و b_{n+1} یکه نیستند. بدین ترتیب روند بی پایان تجزیه a_1 حاصل می شود، یعنی

$$a_1 = a_2 b_2 = a_3 b_3 b_2 = \cdots = a_n b_n b_{n-1} \cdots b_2 = \cdots$$

که یک تناقض است.

(ب)$\Longrightarrow$ (آ):

آشکار است که یک دنباله بی پایان از روند تجزیه، وجود یک زنجیر نامتناهی افزایشی از اید آل‌های اصلی را موجب می شود.□

تعریف . حوزهٔ صحیح R یک حوزهٔ تجزیه نامیده می شود، هرگاه هر عنصر $r \in R$ دارای تجزیه ای به عناصر تحویل ناپذیر باشد.

مثال. فرض کنیم x_k، 2^kامین ریشهٔ x_1 در یک توسیع هیأت خارج‌قسمت‌های $F(x_1)$ حلقهٔ $F[x_1]$ باشد، که در آن F یک هیأت است.

فرض کنیم $R = [x_1, x_2, \cdots]$. اینک $x_1 = x_2^2 = (x_3^2)^2 = \cdots$ یک روند بی پایان تجزیهٔ x_1 را به دست می دهد. به عبارت دیگر R یک حوزهٔ تجزیه نیست.

تذکر ۱.۴ باید متذکر شد که غالباً با حالتی مانند حالت فوق مواجه نمی شویم. معمولاً تجزیه یک عنصر نا صفر به عناصر تحویل ناپذیر ممکن است، لیکن یکتا نیست.

برای مثال، حوزهٔ صحیح $R = \mathbb{Z}[\sqrt{-5}]$ را در نظر بگیرید. این حوزه صحیح متشکل از تمام اعداد مختلط به شکل $a + b\sqrt{-5}$ است که $a, b \in \mathbb{Z}$. این حلقه را با شرح بیشتر در فصل‌های بعد مطالعه خواهیم کرد. می توان ملاحظه کرد که یکه های این حلقه عبارتند از $+1$ و -1 و عنصر $6 \in R$ لزوماً دارای دو تجزیه اساساً متفاوت در R است، یعنی

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

تعریف. فرض کنیم R یک حوزهٔ صحیح است. عنصر $p \in R$، اول نامیده می شود، هرگاه p صفر و یکه نبوده و اگر p حاصلضرب عناصری در R را عاد کند، یکی از آنها را عاد کند.

حوزهٔ صحیح R یک حوزهٔ تجزیهٔ یکتا (ح ت ی) نامیده می شود هرگاه دارای خواص زیر باشد:

یک) روند تجزیه یک عنصر ناصفر و نایکه، پس از تعدادی متناهی مرحله پایان پذیرد و تجزیهٔ $a = p_1 p_2 \cdots p_m$ را که در آن p_iها عناصر تحویل ناپذیر R هستند به دست دهد،

دو) اگر a به دو طریق به عناصر تحویل ناپذیر تجزیه شود، مثلاً

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

آن گاه $m = n$ و q_1، q_2، $\cdots$، q_n را بتوان مجدداً به شکل q_{i_1}، q_{i_2}، $\cdots$، q_{i_m} مرتب کرد، به طوری که برای تمام jها، p_j با q_{i_j} وابسته باشد.

در اثبات قضیهٔ زیر استدلالی شبیه آنچه که در قضیه های ۱.۴ و ۱.۵ ملاحظه کردیم به کار برده می شود.

قضیه ۲.۴ فرض کنیم R یک حوزهٔ صحیح بوده و وجود تجزیه در R مسلم باشد. در این صورت R یک ح ت ی است اگر و تنها اگر هر عنصر تحویل ناپذیر اول باشد.

تمرین ۱.۴ مثالی از یک حلقه R ارائه دهید که شامل عنصر اول a باشد که تحویل ناپذیر نیست.

تمرین ۲.۴ نشان دهید که در یک حوزهٔ صحیح، عنصر اول عنصری است تحویل ناپذیر.

تمرین ۳.۴ مثالی از یک حوزهٔ صحیح D ارائه دهید که شامل عنصر تحویل ناپذیر a باشد که اول نیست.

تمرین ۴.۴ ثابت کنید در یک حوزهٔ ایدآل های اصلی، یک عنصر تحویل ناپذیر عنصری است اول.

تمرین ۵.۴ فرض کنید R یک حوزهٔ تجزیه یکتا است و فرض کنید، a و b عناصر Rاند که تواماً صفر نیستند. در این صورت یک بزرگترین مقسوم علیه مشترک a و b با خواص زیر وجود دارد:

(i) d، a و b را عاد می کند.

(ii) اگر عنصر $e \in R$، a و b را عاد کند، آن گاه e، d را عاد می‌کند.

قضیه ۳.۴ یک ح ا ص یک ح ت ی است.

اثبات. فرض کنیم R یک ح ا ص باشد، در این صورت بنابر تمرین ۵.۴ هر عنصر تحویل ناپذیر R اول است. بنابراین به موجب قضیه ۲.۴ کافی است وجود تجزیه برای R را ثابت کنیم که هم ارز با آن است که نشان داده شود R شامل زنجیر صعودی ایدآل های اصلی نیست.

در صورت امکان، فرض کنیم $(a_1) < (a_2) < \cdots < (a_n) < \cdots$ یک زنجیر نامتناهی صعودی از ایدآلهای اصلی در R باشد. اینک بنابر ملاحظهٔ فوق، اجتماع زنجیر فوق یک ایدآل R است. آن را I می نامیم. مجدداً از آنجا که R یک ح ا ص است. به ازای یک $b \in R$، $I = (b)$. به علت این که $b \in I$ به ازای یک n، $b \in (a_n)$ که ایجاب می کند $(b) \subset (a_n)$.

از طرف دیگر $(a_n) \subset (a_{n+1}) \subset (b)$. بنابراین داریم $(a_n) = (a_{n+1}) = (b)$ که متناقض با واقعیت $(a_n) < (a_{n+1})$ است. این تناقض اثبات را کامل می کند.$\square$

تمرین ۶.۴ فرض کنید R یک ح ا ص است که هیات نیست. در این صورت یک ایدآل سرهٔ Aی R ماکسیمال است اگر و تنها اگر با یک عنصر تحویل ناپذیر تولید شود.

قضیه ۴.۴ فرض کنیم R یک ح ا ص و p یک عنصر ناصفر R است. در این صورت $R/(p)$ یک هیات است اگر و تنها اگر p تحویل ناپذیر باشد. **اثبات.**فرض کنیم p تحویل ناپذیر است. در این صورت تنها ایدآل‌های اصلی که شامل ایدآل (p) هستند عبارتند از (p) و (۱). از این رو ایدآل (p) ماکسیمال است، که ایجاب می کند $R/(p)$ هیات باشد.□

به عکس، فرض کنیم $b \in R$ دارای تجزیهٔ سره $b = aq$ باشد که در آن a و q یکه نیستند. در این صورت $(۱) > (a) > (b)$ که نشان می‌دهد ایدآل (b) ماکسیمال نیست و لذا $R/(b)$ یک هیات نمی باشد.

۴.۳ حوزه های اقلیدسی

تعریف. یک تابع اندازه بر حوزهٔ صحیحِ R تابعی است مانندِ

$$\sigma : R \setminus \{0\} \longrightarrow \mathbb{N}$$

که در آن $\mathbb{N}$ مجموعه اعداد صحیح نا منفی است.

مثالها. توابع قدرمطلق و درجه که به ترتیب بر روی حلقه $\mathbb{Z}$ و $F[x]$ تعریف می شوند، هر کدام تابع اندازه هستند. در حلقه $\mathbb{Z}[i]$، حلقهٔ اعداد گاوسی، (معرفی شده در تمرین آ.۸) نیز تابع اندازه وجود دارد که با مربع قدرمطلق به دست می آید.

حوزه صحیح R حوزهٔ اقلیدسی نامیده می شود، هر گاه، یک تابع اندازه σ بر R تعریف شده باشد که در الگوریتم تقسیم صدق کند.

اگر $a, b \in R$ و $a \neq 0$، q و r در R وجود داشته باشند به طوری که $b = aq + r$ که در آن $r = 0$ یا این که $\sigma(r) < \sigma(a)$.

قضیه ۵.۴ حلقهٔ $\mathbb{Z}$، حلقه چند جمله‌ای های $F[x]$ روی هیأت F و حلقهٔ $Z[i]$، حلقه های اقلیدسی اند.

اثبات. در قضیهٔ ۱.۱ نتیجه را برای $\mathbb{Z}$ اثبات کردیم. همچنین به علت این که هر عنصر ناصفر یک هیات وارونپذیر است، به موجب قضیهٔ ۱.۲، نتیجه در حالت $F[x]$ هم به اثبات می رسد.

از این قرار، حلقهٔ $Z[i]$ را با تابع اندازهٔ σ تعریف شده با $\sigma(x) = |x|^۲$ در نظر می گیریم. فرض کنیم $a, b \in \mathbb{Z}[i]$ و $a \neq 0$. فرض کنیم $b = a\omega$، که در آن $\omega = x + iy$ یک عدد مختلط است. اکنون عدد گاوسی $m + in$ وجود دارد به طوری که

$x = m + x_\circ$ و $y = n + y_\circ$ که $-۱/۲ \leq x_\circ, y_\circ \leq ۱/۲$. اکنون

$$|b - (m + in)a|^۲ = |(x_\circ + iy_\circ)a|^۲ < ۱/۲|a|^۲$$

که اثبات را تمام می کند.□

اینک اثبات قضیه زیر سر راست است.

قضیه ٦.۴ هر حوزهٔ اقلیدسی یک ح ا ص و لذا یک ح ت ی است.

نتیجه ۱.۴ حلقه های $\mathbb{Z}$، $F[x]$ (که F یک هیات است) و $Z[i]$ حوزه ایدآل های اصلی اند.

تذکر ۲.۴ در اثبات قضیه ۱.۲، دربارهٔ وجود بزرگترین مقسوم علیه مشترک، خاصیت حلقه اعداد صحیح که نقشی اساسی داشت تابع قدرمطلق بود که یک تابع اندازه است و آن را به یک حوزه اقلیدسی تبدیل می کند. تمرین بعد دقیقاً در جهت تعمیم این مطلب است.

تمرین ۷.۴ در یک حوزه اقلیدسی R، هر دو عنصر a و b که یکی از آن دو مثلاً a، نا صفر است دارای بزرگترین مقسوم علیه مشترک d هستند. علاوه بر آن به ازای عناصری مانند $\lambda, \mu \in R$، $d = \lambda a + \mu b$.

فصل ۵

لم گاوس و معیار ایزنشتاین

در این فصل به طور عمده به برخی پرسش‌ها، مربوط به حلقهٔ چند جمله‌ای‌های $\mathbb{Z}[x]$ و $\mathbb{Q}[x]$ می پردازیم. بنابر قضیه ۵.۴ در فصل قبل، می دانیم که برای هیأت F، حلقه چند جمله ای های $F[x]$ یک حوزهٔ اقلیدسی و لذا یک حوزهٔ ایدآل های اصلی است. (قضیه ۶.۴ را ببینید). در این فصل خواهیم دید، برای این که $R[x]$ حوزهٔ تجزیه یکتا باشد، کافی است که R حوزهٔ تجزیه یکتا باشد.

۵.۱ لم گاوس

این بخش را با تعریف زیر شروع می کنیم.

تعریف. فرض کنیم $f(x) = a_n x^n + \cdots + a_\circ \in \mathbb{Z}[x]$. در این صورت $f(x)$ اولیه نامیده می شود، هر گاه ضریب پیشرو a_n مثبت بوده و ضرایب $a_n, \cdots a_\text{۱}$ عامل مشترکی به جز ۱ و ۱− نداشته باشند.

تمرین ۱.۵ هر چندجمله ای نا صفر $f(x) \in \mathbb{Q}[x]$ را می توان به صورت حاصلضرب $f(x) = cf_\circ(x)$ که در آن $c \in \mathbb{Q}$ و $f_\circ(x) \in \mathbb{Z}[x]$ اولیه است، نوشت. علاوه بر آن این طرز بیان یکتا است.

تذکر ۱.۵ بدیهی است که $f(x)$ دارای ضرایب صحیح است، اگر و تنها اگر c یک عدد صحیح باشد. در آن حالت $|c| > \circ$، بزرگترین مقسوم علیه مشترک ضرایب $f(x)$ است و علامت c، علامت ضریب پیشروِ $f(x)$ خواهد بود.

تعریف. عدد گویای c که در تمرین ۱.۵ ذکر شد، محتوای $f(x)$ نامیده می شود. اگر ضرایب $f(x)$ صحیح باشند، آن گاه محتوای $f(x)$، $f(x)$ را در $\mathbb{Z}[x]$ عاد می کند، $f(x)$ اولیه است اگر و تنها اگر محتوای آن برابر با ۱ باشد.

قضیه ۱.۵ **(لم گاوس)** حاصلضرب دو چند جمله ای اولیه در $\mathbb{Z}[x]$ یک چندجمله ای اولیه است.

اثبات. فرض کنیم $f(x), g(x)$ دو چند جمله ای اولیه در $Z[x]$ باشد. گیریم $h(x) = f(x)g(x)$. تنها چیزی که باید نشان دهیم، این است که هیچ عدد اولی تمام ضرایب $h(x)$ را عاد نمی کند.

همریختی $\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$ را که با

$$f(x) = a_m x^m + \cdots + a_\circ \longrightarrow \overline{f}(x) = \overline{a_m} x^m + \cdots + \overline{a_\circ}$$

تعریف شده و در آن ضرایب به پیمانهٔ p هستند، در نظر می گیریم. از آنجا که $f(x)$ و $g(x)$ اولیه هستند، $\overline{f} \neq \circ$ و $\overline{g} \neq \circ$. اگر به این حقیقت استناد کنیم که $\mathbb{F}_p[x]$ یک حوزهٔ صحیح است، نتیجه می گیریم که $\overline{h}(x) = \overline{f}(x)\overline{g}(x) \neq \circ$، لذا $h(x)$ اولیه است.$\square$

نتیجه ۱.۱.۵ حاصلضرب تعدادی متناهی چندجمله ای اولیه در $\mathbb{Z}[x]$، باز هم اولیه است.

قضیه ۲.۵ فرض کنیم $f(x), g(x) \in \mathbb{Z}[x]$ و $f(x)$ اولیه باشد. اگر $g(x) = f(x)q(x)$ و $q(x) \in \mathbb{Q}[x]$، آن گاه $q(x) \in \mathbb{Z}[x]$.

اثبات. فرض کنیم $q = cq_\circ$ که $q_\circ \in \mathbb{Z}[x]$ اولیه است و $c \in \mathbb{Q}$. بنابر لم گاوس، $fq_\circ$ اولیه است. اینک برابری $g = cfq_\circ$ نشان می دهد که $g_\circ = fq_\circ$ چند جمله ای اولیه وابسته به g است. از آنجا که $g \in \mathbb{Z}[x]$، نتیجه می گیریم که $c \in \mathbb{Z}$، به عبارت دیگر $q \in \mathbb{Z}[x]$.$\square$

نتیجه ۲.۲.۵ فرض کنیم $f(x), g(x) \in \mathbb{Q}[x]$ و $f_\circ(x), g_\circ(x)$ چندجمله‌ای های اولیه وابسته به آنها در $\mathbb{Z}[x]$ باشد. اگر $f(x)$، $g(x)$ را در $\mathbb{Q}[x]$ عاد کند، آن گاه $f_\circ(x)$، $g_\circ(x)$ را در $\mathbb{Z}[x]$ عاد می کند.

اثبات. اگر $f(x)$، $g(x)$ را در $\mathbb{Q}[x]$ عاد کند، به وضوح $f_\circ(x)$، $g_\circ(x)$ را در $\mathbb{Q}[x]$ عاد کند.

فرض کنیم $g_\circ(x) = q(x)f_\circ(x)$، که $f(x) \in \mathbb{Q}[x]$. به موجب قضیه ۲.۵، $q(x) \in \mathbb{Z}[x]$ و اثبات تمام است.$\square$

نتیجه ۳.۳.۵ فرض کنیم که $f(x), g(x) \in \mathbb{Z}[x]$ دارای یک عامل مشترک غیر ثابتِ $h(x)$ در $\mathbb{Q}[x]$ هستند. در این صورت این دوچند جمله‌ای دارای یک عامل مشترک غیر ثابت در $\mathbb{Z}[x]$ هستند.

اثبات. اگر $h_\circ(x)$ چندجمله ای اولیه وابسته به $h(x)$ باشد، آن گاه $h_\circ(x)$ نیز، $f(x)$ و $g(x)$ را در $\mathbb{Q}[x]$ عاد می کند. بنابر قضیه ۲.۵، $h_\circ(x)$، $f(x)$ و $g(x)$ را در $\mathbb{Z}[x]$ عاد می کند.

نتیجه ۴.۴.۵ اگر چندجمله ای غیر ثابت $f(x)$ در $\mathbb{Z}[x]$ تحویل ناپذیر باشد، در $\mathbb{Q}[x]$ تحویل ناپذیر است.

قضیه ۳.۵ فرض کنیم ضریب پیشرو چندجمله‌ای $f(x) \in \mathbb{Z}[x]$ مثبت باشد. در این صورت $f(x)$ در $\mathbb{Z}[x]$ تحویل ناپذیر است اگر و تنها اگر یکی از دو شرط زیر برقرار باشد.

(۱) $f(x)$ یک عدد صحیح اول است، یا

(۲) $f(x)$ یک چندجمله ای اولیه است که در $\mathbb{Q}[x]$ تحویل ناپذیر است **اثبات.** فرض کنیم $f(x)$ تحویل ناپذیر است. گیریم $f(x) = cf_\circ(x)$ که در آن $f_\circ(x)$ اولیه است چون $f(x)$ تحویل‌ناپذیر است c یا $f_\circ(x)$ برابر با یک است. اگر $f_\circ(x) = ۱$، آن گاه $f(x)$ ثابت و لذا یک عدد اول است. اگر $c = ۱$، در این صورت $f(x)$ اولیه است. همچنین به موجب نتیجهٔ ۳.۲.۵، $f(x)$ در $\mathbb{Q}[x]$ تحویل ناپذیر است. عکس قضیه بدیهی است.□

قضیه ۴.۵ در $\mathbb{Z}[x]$ هر چند جمله ای تحویل ناپذیر یک عنصر اول است.

اثبات. فرض کنیم $f(x) \in \mathbb{Z}[x]$ تحویل ناپذیر باشد، فرض کنیم $f(x)|g(x)h(x)$ که $g(x), h(x) \in \mathbb{Z}[x]$.

حالت (یک). ($f(x) = p$ یک عدد صحیح اول است)

فرض کنیم $g(x) = cg_\circ(x)$، $h(x) = dh_\circ(x)$ که در آن $g_\circ(x)$ و $h_\circ(x)$ به ترتیب چند جمله‌ای‌های وابسته به $g(x)$ و $h(x)$ هستند. بنابر لم گاوس $g_\circ(x)h_\circ(x)$ اولیه است و لذا یکی از ضرایب آن مثلاً a بر p بخشپذیر نیست. اما از آنجا که p، $g(x)h(x)$ را عاد می کند، $p|cda$ که از آن نتیجه می شود $p|c$ یا $c|d$. که آن هم موجب می شود $p|g(x)$ یا $p|h(x)$.

حالت (دو). ($f(x)$ یک چند جمله ای اولیه است که در $\mathbb{Q}[x]$ تحویل ناپذیر است)

همان طور که ملاحظه کردیم $\mathbb{Q}[x]$ یک حوزهٔ اقلیدسی و لذا یک ح ا ص است. بنابراین $f(x)$ یک عنصر تحویل ناپذیر $\mathbb{Q}[x]$ است و از این رو $f(x)$، $g(x)$ یا $h(x)$ را در $\mathbb{Q}[x]$ عاد می کند. بنابر قضیه ۲.۵، $f(x)$، $g(x)$ یا $h(x)$ را در $\mathbb{Z}[x]$ عاد می کند.□

قضیه ۵.۵ حلقهٔ چند جمله‌ای های $\mathbb{Z}[x]$ یک ح ت ی است.

اثبات. با فرض این که $f(x)$ در $\mathbb{Z}[x]$ ناصفر و نا یکه باشد، تجزیه آن در $\mathbb{Q}[x]$ را در نظر گرفته، با برداشتن مخرج‌ها، وجود تجزیه در $\mathbb{Z}[x]$ اثبات می شود. بنابراین به موجب قضیه های ۲.۴، ۴.۵ نتیجه حاصل است.□

با دنبال کردن روشی مشابه، می توان نتیجهٔ کلی تر زیر را ثابت کرد.

قضیه ۶.۵ اگر D یک ح ت ی باشد، آن گاه $D[x]$ یک ح ت ی است.

تذکر ۲.۵ از قضیهٔ فوق نتیجه می شود که حلقه های $\mathbb{Z}[x_1, x_2, \cdots, x_n]$ و $F[x_1, x_2, \cdots, x_n]$ که F یک هیأت است، ح ت ی هستند.

۵.۲ معیار ایزنشتاین

قضیه ۷.۵ (معیار ایزنشتاین) گیریم $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ یک چندجمله‌ای با ضرایب صحیح باشد. فرض کنیم p یک عدد صحیح اول باشد، به قسمی که $a_0, \cdots, a_{n-2}, a_{n-1}$ را عاد کند، $p \nmid a_n$ و $p^2 \nmid a_0$. در این صورت $f(x)$ در $\mathbb{Q}[x]$ تحویل ناپذیر است.

اثبات. فرض کنیم $f(x)$ در $\mathbb{Z}[x]$ به چند جمله‌ای‌هایی با درجهٔ مثبت تجزیه شود، مثلاً $f(x) = g(x)h(x)$. با تبدیل به پیمانه p، داریم $\overline{f}(x) = \overline{a_n} x^n$، که در آن $\overline{a}_n \neq 0$.

اینک $\overline{f}(x) \mid \overline{g}(x)$، $\overline{f}(x) \mid \overline{h}(x)$ و لذا $\overline{g}(x)$ و $\overline{h}(x)$ تک جمله ای اند.بنابراین تمام ضرایب $g(x)$ و $h(x)$ به جز ضریب پیشرو آنها بر p بخشپذیراند. فرض کنیم ضرایب ثابت $g(x)$ و $h(x)$ به ترتیب b_0 و c_0 باشند. از این جا نتیجه می گیریم که $a_0 = b_0 c_0$. اما $p \mid b_0$ و $p \mid c_0$ و لذا $p^2 \mid a_0$ که ممتنع است. بدین ترتیب $f(x)$ در $\mathbb{Z}[x]$ و لذا در $\mathbb{Q}[x]$ تحویل ناپذیر است.□

تمرین ۲.۵ نشان دهید که $f(x) = 8x^3 - 6x - 1$ در $\mathbb{Q}[x]$ تحویل ناپذیر است.

فصل ٦

توسیع‌های هیأت

در این فصل، به اختصار، بعضی ردهٔ های توسیع هیأت ها را بررسی کرده و نتیجه بسیار مفیدی (قضیه ۳.٦) راجع به توسیع‌های متناهی تفکیک پذیر، ثابت خواهیم کرد. در انتهای فصل، بعضی نتایج که ماهیتی حسابی دارند و به تعداد جوابهای چند جمله ایهای روی یک هیأت متناهی مربوط می شوند، ارائه خواهد شد.

٦.١ توسیع های جبری

تعریف. فرض کنیم K یک توسیع هیأت $\mathbb{F}$ است. فرض کنیم $\alpha_1, \alpha_2, \cdots, \alpha_r \in K$. در این صورت کوچکترین زیر هیأت K شاملِ F و α_iها را با $F(\alpha_1, \alpha_2 \cdots, \alpha_r)$ نشان داده و گوییم K با α_iها روی F تولید شده است. یک توسیع Kی F ساده نامیده میشود، هر گاه با یک عنصر روی F تولید شود، یعنی به ازای یک $\alpha \in K$، $K = F(\alpha)$.

فرض کنیم K یک توسیع هیأت F و $\alpha \in K$. تابع ارزیابی $I : F[x] \longrightarrow F[\alpha]$ با $g(x) = g(\alpha)$ تعریف می شود. همانندِ تعریف اعداد جبری و متعالی، اگر هسته I، $kerI$، صفر باشد، α روی F متعالی نامیده می شود. در غیر این صورت α روی F جبری نامیده می شود.

اگر α روی F جبری باشد، ایدآل ناصفر I در $F[x]$ یک ایدآل اصلی است که با یک چند جمله ای، مثلاً $f(x)$ تولید شده است. به سادگی می توان ملاحظه کرد که

$f(x)$ تحویل ناپذیر است. در صورت لزوم با تقسیم چند جمله ای $f(x)$ بر ضریب پیشرو، می توان فرض کرد که $f(x)$ تکین است. این چند جمله‌ای تحویل ناپذیر، چند جمله ای می نیمال α روی F نامیده می شود.

هر گاه K یک توسیع هیأت F باشد، آن گاه K یک فضای برداری روی F است. بُعد K به عنوان یک فضای برداریِ روی K، درجهٔ K روی F نامیده شده و با $[K:F]$ نشان داده می شود. اگر $[K:F]$ متناهی باشد، K را یک توسیع متناهی F می‌نامند. اگر هر عنصر K روی F جبری باشد، K توسیع جبری F نامیده می شود.

تمرین ۱.۶ نشان دهید که هر توسیع متناهی Kی هیأت F باید یک توسیع جبری باشد.

تمرین ۲.۶ فرض کنید K یک توسیع هیأت F و $\alpha \in K$ روی F جبری باشد. اگر n درجهٔ چند جمله ای می نیمال α روی F باشد، نشان دهید که $[K(\alpha):K]=n$. (در این حالت گوییم α روی F، جبری از درجهٔ n است.)

تمرین ۳.۶ فرض کنید K یک توسیع متناهی یک هیأت F و L یک توسیع متناهی K باشد. نشان دهید که $[L:F]=[L:K][K:F]$.

تذکر ۱.۶ فرض کنید K یک توسیع جبری F و L یک توسیع جبری K باشد. بنابر تمرین‌های ۱.۶، ۲.۶ و ۳.۶ ملاحظه می کنیم L یک توسیع جبری F است. برای اثبات این ادعا فرض کنیم α یک عنصر دلخواه L باشد، در این صورت چند جمله ای ناصفر $f(x)=a_nx^n+\cdots+a_0$ در $K[x]$ وجود دارد به طوری که $f(\alpha)=0$. فرض کنیم $K_1=F(a_n,\cdots,a_0)$، هیأت تولید شده با $\{a_n,\cdots,a_1\}$ روی F باشد. اینک به علت جبری بودن α روی K_1، بنابر تمرین ۲.۶، $K_1(\alpha)$ روی K_1 متناهی است. مجدداً بنابر تمرین‌های ۲.۶ و ۳.۶، K_1 یک توسیع متناهی F است. بنابراین $K_1(\alpha)$ روی F متناهی است و بنابر تمرینِ ۱.۶ α روی F جبری است.□

تعریف. فرض کنیم K یک توسیع هیأت F باشد. مجموعهٔ تمام عناصر K که روی F جبری هستند،بَستار جبری F در K نامیده می شود.

اگر α و β دو عنصر K و روی F جبری باشند، در این صورت $F(\alpha,\beta)$ کوچکترین زیر هیأت K است که شامل F، α و β است، لذا، بنابر تمرین ۱.۶ یک توسیع جبری F است. از آنجا که $\alpha\pm\beta, \alpha\beta \in F(\alpha,\beta)$، این عناصر روی F جبری اند. اگر $\alpha \neq 0$، همین امر در مورد α^{-1} صادق است. بنابراین بستارِ جبری F در K

یک زیر هیأت K است. اگر این بستار جبری برابر با F باشد، گوییم F به طور جبری در K بسته است.

تذکر ۲.۶ بستارِ جبری $\mathbb{Q}$ در $\mathbb{C}$ با $\overline{\mathbb{Q}}$ نشان داده می شود. ملاحظه می کنیم که $\overline{\mathbb{Q}}$ یک توسیع $\mathbb{Q}$ می باشد که جبری است، اما یک توسیع متناهی آن نیست، زیرا به ازای هر عدد صحیح مثبت n، چند جمله ای $x^n - 2$، به موجب معیار ایزنشتاین در $\mathbb{Q}[x]$ تحویل ناپذیر است (قضیه ۷.۵ را ببینید). پس اگر $\alpha \in \overline{\mathbb{Q}}$ یک ریشه آن باشد، $\mathbb{Q}(\alpha) \subset \overline{\mathbb{Q}}$ یک توسیع از درجهٔ n، F است.

۶.۲ توسیع های نرمال

قضیه ۱.۶ فرض کنیم F یک هیأت و $f(x) \in F[x]$ یک چند جمله ای تحویل ناپذیر با درجه n باشد. در این صورت یک توسیع برای F با $[K : F] = n$ وجود دارد به طوری که شامل یک ریشه $f(x)$ است.

اثبات. بنابر قضیه ۴.۴ $F[x]/(f(x))$ یک هیأت است. تابعِ $a \longrightarrow (f(x)) + a$ یک همریختی یک به یک از F به $F[x]/(f(x))$ است. بنابراین $F[x]/(f(x))$ شامل یک نخسه یکریخت با F است و می تواند به عنوان یک توسیع F در نظر گرفته شود. تابع طبیعی $g(x) \longrightarrow (f(x)) + g(x)$ از $F[x] \longrightarrow F[x]/(f(x))$ را در نظر می گیریم به وضوح تصویر aی x در $F[x]/(f(X))$، تحت این تابع در $f(a) = 0$ صدق می کند. بنابراین $K = F[x]/(f(x))$ توسیع مطلوب است. اثبات این که $[K : F] = n$ را به عهدهٔ خواننده می گذاریم.□

تعریف. توسیع متناهی Kی هیأت F، یک توسیع شکافنده برای $f(x) \in F[x]$ نامیده می شود، هرگاه $f(x)$ در $K[x]$ به حاصلضرب چند جمله‌ای‌های خطی تجزیه شود، لیکن به ازای هر زیرهیأت سره K مانند K_1، $f(x)$ در $K_1[x]$ چنین نباشد.

تمرین ۴.۶ فرض کنیم F یک هیأت و $f(x) \in F[x]$ با درجهٔ $n \geq 1$ باشد. نشان دهید که هیأت شکافنده $f(x)$ وجود دارد و درجهٔ آن حداکثر برابر با $n!$ است.

اثبات. فرض کنیم K_1 و K_2 دو توسیع هیأت F باشند. یک یکریختی از K_1 به توی K_2 که عناصر F را عنصر به عنصر، حفظ می کند یک F—یکریختی می نامیم و هیأت‌های K_1 و K_2 را F—یکریخت می‌گوییم. اگر $K_1 = K_2 = K$، آن گاه F—خودریختی‌های F، تحت ترکیب توابع تشکیل یک گروه می دهند. این گروه، گروه گالوای K روی F نامیده شده و با $Gal(K/F)$ نشان داده می شود.

فرض کنیم K یک توسیع جبری F باشد. دو عنصر α_1 و α_2 در K، روی F مزدوج خوانده می شوند، هرگاه یک $F-$یکریختی σ از $F(\alpha_1)$ به توی $F(\alpha_2)$ وجود داشته باشد به طوری که $\sigma(\alpha_1) = \alpha_2$.

تمرین ۵.۶ فرض کنید K یک توسیع جبری F و α_1 و α_2 دو عنصر K باشند. نشان دهید که α_1 و α_2 روی F مزدوج هستند، اگر و تنها اگر روی F، چند جمله‌ای‌های می نیمالِ یکسان داشته باشند.

فرض کنیم F_1 و F_2 دو هیأت و σ یک یکریختی از F_1 به روی F_2 باشد. برای $f(x) = a_nx^n + \cdots + a_0 \in F[x]$، تابع $f(x) \longrightarrow \sigma(a_n)x^n + \cdots + \sigma(a_0)$ همریختی یکتای $F_1[x] \longrightarrow F_2[x]$ است که توسیع σ می باشد. (تمرین ۲.۲ را ببینید) با به کار گیری نا به جای نماد، این توسیع را نیز با σ نشان خواهیم داد.

تمرین ۶.۶ با نماد گذاری فوق، اگر K_1 و K_2 به ترتیب هیات‌های شکافندهٔ $f(x)$ و $\sigma(f(x))$ روی F_1 و F_2 باشند، آن گاه نشان دهید که یک یکریختی از K_1 به روی K_2 وجود دارد که تحدید آن بر F_1، σ است.

تذکر ۳.۶ از تمرین فوق نتیجه می شود که هر دو هیأت شکافندهٔ یک چند جمله ای روی هیات F، $F-$ یکریخت هستند. بنابراین هنگام صحبت از یک هیأت شکافنده، می توان گفت، هیأت شکافنده.

تمرین ۷.۶ فرض کنید F یک هیأت و K هیأت شکافنده $f(x) \in F[x]$ باشد. فرض کنید L یک توسیع هیأت K باشد، نشان دهید که هر $F-$یکریختی $\sigma : K \longrightarrow L$، K را به روی خود می نگارد.

تعریف. فرض کنید F یک هیأت F است. یک توسیع نرمال F یک توسیع جبری Kی هیات F است به قسمی که هر چند جمله ای $f(x) \in F[x]$ که یک ریشه در K دارد، به حاصلضرب چند جمله‌ای های خطی در $K[x]$ تجزیه شود.

تمرین ۸.۶ نشان دهید که یک توسیع نرمال و متناهی یک هیأت F چیزی نیست مگر هیأت شکافنده یک چند جملای $f(x)$ روی F.

۳.۶ توسیع های تفکیک پذیر

تعریف. فرض کنیم F یک هیأت و $f(x) \in F[x]$. فرض کنیم K هیأت شکافنده $f(x)$ روی F باشد. اگر α یک ریشهٔ $f(x)$ در K باشد، چندگانگی α، بزرگترین عدد

صحیح n است، به قسمی که $(x-\alpha)^n$، $f(x)$ را در $K[x]$ عاد می کند. ریشه αی $f(x)$، ریشهٔ چندگانه خوانده می شود، هرگاه $n > 1$.

اگر $f(x)$، یک چند جمله ای تحویل ناپذیر در $F[x]$ باشد، آن گاه $f(x)$ تفکیک پذیر خوانده می شود، هرگاه ریشه چندگانه نداشته باشد.

فرض کنیم K یک توسیع هیأت F باشد. یک عنصر $\alpha \in K$، روی F تفکیک پذیر است، هرگاه چند جمله ای می نیمال $f(x)$ آن روی F تفکیک پذیر باشد. اگر تمام عناصر K روی F تفکیک پذیر باشند، آن گاه K توسیع تفکیک پذیر F نامیده می شود. اگر توسیع Kی F تفکیک پذیر نباشد، تفکیک ناپذیر خوانده می شود.

تمرین ۹.۶ فرض کنید $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$. می توان مشتق صوری $f(x)$ را برابر با $f'(x) = n a_n x^{n-1} + \cdots + a_1$ تعریف کرد. بررسی کنید که این مشتق صوری در خواص زیرِ مشتق که در ریاضیات عمومی دیده شده است، صدق می کند.

یک) اگر $f(x), g(x) \in F[x]$ و $F(x) = f(x)+g(x)$، آن گاه $F'(x) = f'(x)+g'(x)$.

دو) اگر $f(x), g(x) \in F[x]$ و $F(x) = f(x)g(x)$، آن گاه،

$$F'(x) = f'(x)g(x) + f(x)g'(x).$$

تمرین ۱۰.۶ فرض کنید K توسیع جبری F باشد. نشان دهید که عنصر $d \in K$ روی F تفکیک ناپذیر نیست، اگر و تنها اگر $f'(x)$ چندجمله ای صفر باشد. در این جا، $f(x)$ چند جمله ای می نیمال α روی F است. از این جا نتیجه بگیرید که اگر هیات F با مشخصه صفر باشد، آن گاه هر توسیع جبری Kی F تفکیک پذیر است. اگر به ازای عددی اول مانند p، F هیاتی با مشخصه p باشد، نشان دهید که چند جمله ای $f(x) \in F[x]$ می تواند ریشه چندگانه داشته باشد، تنهااگر به ازای یک $g(x) \in F[x]$، $f(x) = g(x^p)$.

قضیه ۲.۶ فرض کنیم K یک توسیع متناهی و تفکیک پذیر هیأت F باشد و $[K:F] = n$. فرض کنیم N یک توسیع K باشد، به قسمی که N توسیع نرمال F است. در این صورت دقیقاً n، $F-$یکریختی از K به توی N وجود دارد.

اثبات. از استقرای روی n استفاده می کنیم. اگر $n = 1$، چیزی برای اثبات باقی نمی ماند. پس فرض کنیم $n > 1$، گیریم $\alpha \in K$ و $\alpha \notin F$. اینک $[K:F(\alpha)] < n$ و K روی $F(\alpha)$ تفکیک پذیر است. بنابراین به موجب فرض استقرا، دقیقاً $s = [K:F(\alpha)]$، $F(\alpha)-$یکریختی σ_i، $i = 1, 2, \cdots, s$ از K به توی N وجود دارد. مجدداً، به علت این که α روی F تفکیک پذیر است، چند جمله ای می نیمال آن

روی F دارای ریشه های متمایز است، لذا به موجب تمرین ۵.۶ دقیقاً به اندازه $t = [F(\alpha) : F]$، F—یکریختی τ_j، $j = ۱,\cdots t$ از $F(\alpha)$ به توی N وجود دارد.

به دلیل این که N یک هیأت شکافنده است، F—یکریختی های τ_j را می توان به خود ریختی های N که تحدیدشان بر K یکریختی های K به توی N است بسط داد(تمرین ۶.۶ را ببینید). این یکریختی ها را نیز با τ_j نشان می دهیم. اکنون ترکیب های $\tau_j \circ \sigma_i$ یکریختی های K به توی N هستند. چنانچه برای هر $a \in K$، $\tau_j \circ \sigma_i(a) = \tau_u \circ \sigma_v(\alpha)$، آن گاه برای هر $a \in F(\alpha)$، داریم $\tau_j(a) = \tau_u(a)$ که ایجاب می کند $j = u$. از این رو برای هر $a \in K$، $\sigma_i(a) = \sigma_v(a)$ و لذا $i = v$. بنابراین نشان دادیم که $\tau_j \circ \sigma_i$ها $s.t$ یکریختی متمایز K به توی N هستند. اثبات این که F—یکریختی های K به توی N در بین همین $s.t$ یکریختی اند، چندان دشوار نیست. آن را به عنوان تمرین باقی می گذاریم. بنابراین تعداد F—یکریختی های متمایز K به توی N برابر است با

$$st = [K : F(\alpha)].[F(\alpha) : F] = [K : F] = n\square.$$

تذکر ۴.۶ عکس قضیه فوق نیز درست است. بدین معنی که اگر K توسیع متناهی هیأت K باشد و $[K : F] = n$، به قسمی که برای هر توسیع نرمال N از F، دقیقاً n، F—یکریختی متمایز از K به توی N وجود داشته باشد، آن گاه، K یک توسیع تفکیک پذیر F است.

قضیه ۳.۶ فرض کنیم K یک توسیع متناهی و تفکیک پذیر F باشد، در این صورت K یک توسیع ساده است. بدین معنی که $\alpha \in K$ وجود دارد که $K = F(\alpha)$.

اثبات. حالت (یک) (F یک هیأت متناهی است)

به علت این که یک توسیع متناهی یک هیأت متناهی است، خود یک هیأت متناهی است و لذا به موجب تذکر ۳.۳، K^* یک گروه دوری تولید شده با عنصری مثل α است. به وضوح $K = F(\alpha)$.

حالت (دو) (F یک هیأت نامتناهی است)

فرض کنیم $[K : F] = n$. فرض کنیم N/F یک توسیع متناهی و نرمال که شامل K به عنوان یک زیر هیأت است باشد. چنین توسیعی همواره وجود دارد، زیرا K که توسیع متناهی F است، با تعدادی متناهی عنصرِ $\alpha_r,\cdots,\alpha_۱$ روی F تولید شده است. اگر $f_i(x)$ چند جمله ای می نیمال α_i روی F باشد. آنگاه هیأت شکافندهٔ $\Pi_{i=۱}^{n} f_i(x)$ روی f چنین هیأتی خواهد بود. از آن جا که K/F متناهی و تفکیک پذیر است، بنابر قضیه ۲.۶ فوق، n، F—یکریختی متمایز، $\sigma_n \cdots,\sigma_۱$ از K به توی

N وجود دارد. برای هر $i \neq j$، فرض کنیم $Vij = \{x \in K : \sigma_i(x) = \sigma_j(x)\}$. در این صورت V_{ij} به وضوح یک زیر فضای F—فضای برداری K است و به دلیل این که σ_iها متمایزند، Vijها یک زیر فضای سرهٔ K است. بنابراین به موجب قضیه ۲.۳، $\bigcup_{i\neq j} Vij$ یک زیر فضای سرهٔ K است. این بدان معنی است که $\alpha \in K$ وجود دارد به طوری که برای $i \neq j$، $\sigma_i(\alpha) \neq \sigma_j(\alpha)$. بنابراین α دارای n مزدوج متمایز است و از این رو $K = F(\alpha)$.$\square$

۶.۴ هیأت های متناهی

پیش از به پایان بردن این فصل، به بحث کوتاهی دربارهٔ هیات‌های متناهی می پردازیم. در تذکر ۲.۳ ملاحظه کردیم که یک هیأت متناهی K به ازای یک عدد اول p، شامل هیأت $\mathbb{F}_p$ است. اگر $[K : \mathbb{F}_p] = r$، با در نظر گرفتن این که K یک فضای برداری است، K شامل p^r عنصر خواهد بود. می نویسیم $q = p^r$ و توجه می کنیم که عناصر ناصفر K با ضرب تشکیل یک زیر گروه دوری با $q - ۱$ عنصر می دهند، از آنجا که عناصر ناصفر در شرط $x^{q-۱} = x$ صدق می کنند، مشاهده می کنیم که تمام عناصر K در معادله $x^q = x$ صدق می کنند. بدین ترتیب چند جمله ای $x^q - x$ در $K[x]$ به شکل $x^q - x = \Pi_{a\in K}(x - a)$ تجزیه می شود. (تذکر ۱.۲ را ببینید). به وضوح K هیأت شکافندهٔ $x^q - x$ است.

از بحث فوق چنین نتیجه می گیریم که هر دو هیأت متناهی با تعدادی یکسان عنصر، هیأت شکافنده یک چند جمله‌ای یکسان هستند و لذا یکریخت اند.

اینک ادعا می کنیم که برای هر عدد اول مفروض p و عدد صحیح مثبت r هیأتی متناهی با $q = p^r$ عضو وجود دارد. زیرا K، هیأت $f(x) = x^q - x$ را در نظر می گیریم. بنابر تمرین ۱.۶ تعداد ریشه های $f(x)$ در K برابر با q است. دشوار نیست که تحقیق کنیم، این ریشه ها تشکیل یک زیر هیأت K را می دهند. در واقع باید برابر با K باشد.

قضیه ۴.۶ (قضیه وارنینگ [1]) فرض کنیم p عددی اول و به ازای یک عدد صحیح $r \geq ۱$، $q = p^r$. فرض کنیم $f(x_۱, x_۲, \cdots, x_n) = \mathbb{F}_q[x_۱, x_۲, \cdots, x_n]$ یک چندجمله ای با درجهٔ کمتر از n باشد. در این صورت تعداد جواب‌های معادلهٔ $f(x_۱, x_۲, \cdots, x_n) = ۰$ در $\mathbb{F}_q^n = \underbrace{\mathbb{F}_q \times \cdots \mathbb{F}_q}$ بر p بخشپذیر است.

[1] Warnning

اثبات. فرض کنیم $g(x_1,x_2,\cdots,x_n)=1-(f(x_1,x_2,\cdots,x_n))^{q-1}$. در این صورت درجه g از $n(q-1)$ کوچکتر است. برای $(\alpha_1,\alpha_2,\cdots,\alpha_n)\in\mathbb{F}_q^n$، $f(\alpha_1,\alpha_2,\cdots,\alpha_n)=0$ اگر و تنها اگر $g(\alpha_1,\alpha_2,\cdots,\alpha_n)=1$.

بنابراین تعداد جواب‌های $f(x_1,x_2,\cdots,x_n)=0$ در $\mathbb{F}_q^n$ برابر با $\sum g(\alpha_1,\alpha_2,\cdots,\alpha_n)$ است، که جمع روی تمام $(\alpha_1,\alpha_2,\cdots,\alpha_n)\in\mathbb{F}_q^n$ است.

ادعا می کنیم که این مجموع برابر با $0\in F_q$ است. اگر این ادعا ثابت شود، حکم قضیه ثابت شده است. اگر g تک جمله ای $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ باشد، آن گاه مجموع برابر است با $(\sum_{\alpha_1\in\mathbb{F}_q}\alpha_1^{i_1})\cdots(\sum_{\alpha_n\in\mathbb{F}_q}\alpha_1^{i_n})$. حداقل درجهٔ یکی از i_jها (مثلاً i_l) کمتر از $q-1$ است. اینک $a\in\mathbb{F}_q^*$ وجود دارد به طوری که $a^{i_l}\neq 1$. اکنون، $\sum_{\alpha_l\in\mathbb{F}_q}\alpha_l^{i_l}=\sum a^{i_l}\alpha_l^{i_l}$ و چون $a^{i_l}\neq 1$، $\sum_{\alpha_l\in\mathbb{F}_q}\alpha_l^{i_l}=0$. بنابراین، $(\sum_{\alpha_1\in\mathbb{F}_q})\alpha_1^{i_1}\cdots(\sum_{\alpha_n\in\mathbb{F}_q}\alpha_1^{i_n})=0$.

حالت کلی به طور بدیهی به دست می آید، زیرا آن حالت مجموع مضارب ثابت این مجموع‌ها است.□

قضیه ٥.٦ (**قضیهٔ شوالیه**[2]) فرض کنیم $f(x_1,x_2,\cdots,x_n)\in\mathbb{F}_q[x_1,x_2,\cdots,x_n]$ درجه ای کمتر از n داشته باشد و $f(0,0,\cdots,0)=0$. پس، $(\alpha_1,\alpha_2,\cdots,\alpha_n)\in\mathbb{F}_q^n$ وجود دارد که همهٔ α_iها صفر نیستند و $f(\alpha_1,\alpha_2,\cdots,\alpha_n)=0$.

اثبات. از آنجا که $f(0,0,\cdots,0)=0$، دست کم یک جواب وجود دارد. اکنون بنابر قضیه ۴.٦، تعداد جواب‌های $f(x_1,x_2,\cdots,x_n)=0$ در $\mathbb{F}_q^n$ ضریبی از p است و حداقل $p\geq 2$. قضیه اثبات شده است.□

تذکر ٥.٦ اگر جواب‌های همزمان تعدادی متناهی چند جمله ای را در نظر بگیریم، به شرط این که مجموع درجه های آنها از n کمتر باشد، با تعدیلِ ساختار چند جمله‌ای g در قضیه ۴.٦ می توان نتیجه ای مانند نتیجهٔ ٥.٦ به دست آورد.

تمرین ١١.٦ فرض کنید p عددی اول است. از تذکر بالا نتیجه بگیرید که اگر $\alpha_1,\alpha_2,\cdots,\alpha_{2p-1}$ دنباله‌ای از اعداد صحیح نه لزوماً متمایز باشد، آن گاه یک زیر دنباله p عضوی وجود دارد که مجموع آنها مضربی از p است.

تذکر ٦.٦ تمرین فوق حتی اگر به جای عدد اول p هر عدد صحیح مثبتی قرار دهیم نیز درست است. این بیان به قضیهٔ اردیش جیزبرگ—زیف[3] موسوم است. برای اطلاع بیشتر از این نوع نظریهٔ جمعی اعداد می توان به کتاب Nat١٩٩٦ مراجعه کرد.

---
[2] Chevalley
[3] Erdös-Gingburg-ziv

فصل ۷

قانون تقابل درجهٔ دوم

فرض کنیم $f(x)$ یک چندجمله ای با ضرایب صحیح باشد. مساله تعین جواب‌های همنهشتی چند جمله ای $f(x) \equiv 0 \pmod{n}$، در تمرین ۸.۱ خلاصه می شود: مسئله را باید با توان‌هایی اول که n را عاد می کنند حل کرد. در واقع می توان مسئله را به حل چندجمله‌ای‌ها به پیمانهٔ یک عدد اول با حل مجموعه ای از همنهشتی‌های خطی کاهش داد. یافتن روشی برای حل همنهشتی چندجمله ای به پیمانهٔ عددی اول، یکی از مهمترین مسائل حل نشده در نظریهٔ اعداد است. نخستین حالتِ نابدیهی، همنهشتی درجهٔ دومِ

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

است، که $a, b, c, \in \mathbb{Z}$ و $a \not\equiv 0 \pmod{p}$.

با تبدیل به مربعِ کامل، حل معادله فوق به حلِ معادله ای از نوعِ

$$x^2 \equiv d \pmod{p} \qquad (۱.۷)$$

که $d \in \mathbb{Z}$ و p یک عدد اول است، می‌انجامد.

۷.۱ قانون تقابل درجهٔ دوم

در این بخش، به روش جبری به قانون تقابل درجهٔ دوم، که یکی از مشهورترین نتایج در تمامی نظریهٔ اعداد است می پردازیم. این قانون به مسئلهٔ وجود جوابهای

همنهشتی (۱.۷) را در نظر دارد. یک طرح کلی از اثباتی مقدماتی به عنوان تمرین در انتهای فصل آمده است.

فرض کنیم $q = p^n$ و $\mathbb{F}_q$ هیأت اعداد با q عضو باشد. اگر $p = ۲$، از آنجا که $x \longrightarrow x^۲$ یک خودریختی $\mathbb{F}_q$ است، نتیجه می گیریم که تمام عناصر $\mathbb{F}_q$ مربع هستند.

اگر $p \neq ۲$، فرض کنیم Ω بستار جبری $\mathbb{F}_q$ باشد و برای $x \in \mathbb{F}_q^*$، فرض کنیم $y \in \Omega$ چنان باشد که $y^۲ = x$.

در این صورت $y^{q-۱} = x^{\frac{q-۱}{۲}} = \pm ۱$، زیرا که $x^{q-۱} = ۱$. برای این که x در $\mathbb{F}_q$ مربع کامل باشد، لازم و کافی است که y به $\mathbb{F}_q^*$ تعلق داشته باشد، یعنی $y^{q-۱} = ۱$. بنابراین اگر تابع $x \longrightarrow x^{(q-۱)/۲}$ از $\mathbb{F}_q$ به $\{-۱, +۱\}$ را در نظر بگیریم، آن گاه آشکارا این تابع یک همریختی است و $\mathbb{F}_q^{*۲}$ هستهٔ آن است. چندین روش وجود دارد که ملاحظه کنبم، این همریختی پوشا است. یک روش، توجه به این نکته است که برای عنصر $a \in \mathbb{F}_q^*$، هر دو عنصر a و $-a$ (این دو عنصر متمایزند، زیرا مشخصه برابر با ۱است) دارای یک مربع هستند و آن گاه استدلالی شمارشی به کار بریم. می توان مشاهده کرد که $\mathbb{F}_q^*$ یک گروه دوری از مرتبهٔ زوج است. بنابراین نتیجه می گیریم که شاخص $\mathbb{F}_q^{*۲}$ برابر با ۲ است.

تعریف. برای هر عدد اول غیر از ۲ و برای $x \in \mathbb{F}_q^*$، نماد لژاندر $(\frac{x}{p})$ را برابر با $x^{(p-۱)/۲}$ تعریف می کنیم.

با قرار دادن $(\frac{۰}{p}) = ۰$، تعریف $(\frac{x}{p})$ را به تمام $\mathbb{F}_q$ تعمیم می دهیم و آن را به طریقی بدیهی یک تابع بر $\mathbb{Z}$ در نظر می گیریم.

برای $x \equiv ۰ \pmod p *$، برحسب این که x، به پیمانهٔ p مربع باشد یا مربع نباشد، یعنی $y^۲ \equiv x \pmod p$ جواب داشته باشد یا نه، $(\frac{x}{p}) = ۱$ یا $(\frac{x}{p}) = -۱$. به ترتیب گویند x ماندهٔ درجهٔ دوم یانامانده‌ٔ درجهٔ دوم ، به پیمانه p است.

برای عدد اول p، غیراز ۲، از آنجا که شاخص $\mathbb{F}_p^{*۲}$ در $\mathbb{F}_p^*$برابر با ۲ است، همان تعداد ماندهٔ درجه دوم به پیمانهٔ درجهٔ دوم وجود دارد که ناماندهٔ درجه دوم. همچنین می دانیم که $(\frac{xy}{p}) = (\frac{x}{p})(\frac{y}{p})$، یعنی نماد لژاندر یک همریختی از $\mathbb{F}_q^*$ به توی گروه ضربی عناصر ناصفر اعداد مختلط است (هر همریختی از یک گروه آبلی به توی $\mathbb{C}^*$ یک مشخصهٔ گروه نامیده می شود.)

قضیه ۱.۷ (**قانون تقابل درجهٔ دوم**) اگر p و l دو عددِ اول فرد باشند، آن گاه

یک) $(\frac{-۱}{p}) = (-۱)^{\frac{p-۱}{۲}}$

دو) $(\frac{۲}{p}) = (-۱)^{\frac{p^۲-۱}{۸}}$

سه) $(\frac{p}{l})(\frac{l}{p}) = (-۱)^{\frac{p-۱}{۲}\cdot\frac{l-۱}{۲}}$. **اثبات.** قسمت (یک) مستقیماً از تعریف نتیجه می

شود. متذکر می شویم که این نتیجه پیش از این در تمرین ۶.۱ و قسمت (سه) قضیهٔ ۱.۳ آمده است.

اینک فرض کنیم α یک ریشه هشتم واحد در یک بستار جبری Ωی F باشد (از آنجا که $p^{\phi(8)} \equiv 1 \pmod 8$، اگر هیات متناهی F با بعد $\phi(8)$ را روی $\mathbb{F}_p$ در نظر بگیریم، در این صورت خود F شامل یک ریشه هشتم واحد است. به همین دلیل، برای هر n با $(s,p) = 1$، Ω شامل ریشهٔ sام واحد است). پس

$$\alpha^4 = -1 \tag{۲.۷}$$

بنابراین $(\alpha^2 + \alpha^{-2})^2 = 0$ که نتیجه می دهد

$$\alpha^2 + \alpha^{-2} = 0 \tag{۳.۷}$$

اگر قرار دهیم،

$$y = \alpha + \alpha^{-1} \tag{۴.۷}$$

به موجب (۳.۷) داریم

$$y^2 = 2 \tag{۵.۷}$$

از (۴.۷) نتیجه می شود که $y^p = \alpha^p + \alpha^{-p}$.

بنابراین در حالت $p \equiv \pm 1 \pmod 8$، داریم $y^p = y$ (زیرا $\alpha^8 = 1$) که نتیجه می دهد $y^{p-1} = 1$ و لذا بنابر (۵.۷)،

$$(\frac{2}{p}) = 2^{\frac{p-1}{2}} = y^{p-1} = 1.$$

در حالت $p \equiv \pm 5 \pmod 8$ داریم $y^p = -y$. بنابراین، $y^{p-1} = -1$ که نتیجه می دهد $(\frac{2}{p}) = -1$، که بدین ترتیب (دو) ثابت شده است.

برای اثبات (سه) فرض کنیم ω یک ریشه l ام واحد در Ω باشد.

مجموع گاوسی $S = \sum_{x \in \mathbb{F}_l^*} (\frac{x}{l}) \omega^x$ را تشکیل می دهیم. توجه کنید که ω^x برای هر $x \in \mathbb{F}_l$ خوشتعریف است.

داریم

$$\begin{aligned} \boldsymbol{S}^2 &= \textstyle\sum_{x,y\in\mathbb{F}_l^*}(\frac{xy}{l})\boldsymbol{\omega}^{x+y} \\ &= \textstyle\sum_{y,z\in\mathbb{F}_l^*}(\frac{y^2x}{l})\boldsymbol{\omega}^{y(z+1)} \end{aligned}$$

(قرار داده ایم $x = yz$)

$$\begin{aligned} &= \textstyle\sum_{y,z\in\mathbb{F}_l^*}(\frac{z}{l})\boldsymbol{\omega}^{y(z+1)} \\ &= \textstyle\sum_{y\in\mathbb{F}_l^*}(\frac{-1}{l})\boldsymbol{\omega}^{0} + \sum_{z\neq -1}(\frac{z}{l})\sum_{y\in\mathbb{F}_l^*}\boldsymbol{\omega}^{y(z+1)} \\ &= (\tfrac{-1}{l}(\boldsymbol{l}-\mathbf{1}) + (-\mathbf{1})\textstyle\sum_{z\neq -1}(\frac{z}{l}) \end{aligned}$$

(زیرا $\sum_{y\in\mathbb{F}_l^*}\omega^{y(z+1)} + 1 = 1 + \omega + \cdots + \omega^{l-1} = 0$)،

$$S^2 = l(\frac{-1}{l}) - \sum_{x\in\mathbb{F}_l^*}(\frac{z}{l})$$

اینک همان تعداد مربع در $\mathbb{F}_l^*$ وجود دارد که نامربع وجود دارد، $\sum_{x\in\mathbb{F}_l^*}(\frac{z}{l}) = 0$ و لذا

$$S^2 = l(\tfrac{-1}{l}). \qquad (6.7)$$

از آنجا که Ω با مشخصهٔ p است، داریم

$$\begin{aligned} \boldsymbol{S}^p &= \textstyle\sum_{x\in\mathbb{F}_l^*}(\frac{x}{l})\boldsymbol{\omega}^{xp} \\ &= \textstyle\sum_{x\in\mathbb{F}_l^*}(\frac{zp^{-1}}{l})\boldsymbol{\omega}^{x} \end{aligned}$$

($\boldsymbol{p}^{-1}$ وارون $\boldsymbol{p}$ در $\mathbb{F}_l^*$ است و قرار داده ایم $\boldsymbol{xp} = \boldsymbol{z}$)

$$\begin{aligned} &= (\tfrac{p^{-1}}{l})\boldsymbol{S} \\ &= (\tfrac{p}{l})\boldsymbol{S}. \end{aligned}$$

از (۶.۷) آشکار است که $S \neq 0$ و بنابراین،

$$S^{p-1} = (\tfrac{p}{l}) \qquad (7.7)$$

از (۶.۷) و (۷.۷) نتیجه می گیریم که،

$$(\frac{p}{l}) = S^{p-1} = (l(\frac{-1}{l}))^{\frac{p-1}{2}} = (\frac{l}{p})(\frac{-1}{l})^{\frac{p-1}{2}} = (\frac{l}{p})(-1)^{\frac{p-1}{2}.\frac{l-1}{2}}$$

که برابری (سه) را به پیمانهٔ p نشان می‌دهد. از آنجا که p فرد است، نتیجه حاصل می شود.□

تذکر ۱.۷ در قضیه ۱.۷ در واقع (سه) قانون تقابل است، حال آن که (یک) و (دو) به ترتیب اولین و دومین قانونِ مکمل است.

نتیجه ۱.۷ هر توسیع درجهٔ دوم Kی $\mathbb{Q}$، به ازای یک ریشهٔ واحد ξ مشمول در $\mathbb{Q}(\xi)$ است.

اثبات. در اثبات (سه) فوق، اگر به جای ω، ریشهٔ l ام واحد در $\overline{\mathbb{Q}}$ را قرار داده و S را به همان روش تعریف کنیم، داریم $S^{۲} = \pm l$. بنابراین ریشهٔ دوم هر عدد اول فرد، به ازای یک ریشه ξ واحد در $\mathbb{Q}(\xi)$ مشمول است. با ملاحظه این که $\sqrt{۲} \in \mathbb{Q}(\xi)$، که ξ_n ریشهٔ هشتم واحد در $\mathbb{Q}$ است (زیرا $۲ = -i(۱+i)^{۲}$)، نتیجه حاصل می شود.

تذکر ۲.۷ * نتیجه فوق، حالت خاصی است از قضیه ای که توسط کرونکر[۱] حدس زده شده و توسط وبر[۲] اثبات شده است. در اینجا نتیجه را تنها بیان می کنیم.

هر توسیع آبلی Kی $\mathbb{Q}$ (یعنی یک توسیع گالوای K از $\mathbb{Q}$ به طوری که گروه گالوای، $Gal(K/\mathbb{Q})$ آبلی است) به ازای یک ریشهٔ ξ واحد مشمول در $\mathbb{Q}(\xi)$ است.

هنگامی که به جای هیات پایه $\mathbb{Q}$، یک هیات درجه دوم موهومی $K = \mathbb{Q}(\sqrt{d})$، $d < ۰$ قرار گیرد. در این صورت نقش ξ توسط مختصات نقاط با مرتبه متناهی، روی یک خم بیضویِ مشخص، القا می شود.

تمرین ۱.۷ معین کنید که آیا ۴۵ ماندهٔ درجه دوم به پیمانه ۱۰۰۹ است؟

تمرین ۲.۷ آیا معادلهٔ دیوفانتی $y^{۲} = x^{۳} + ۲۳$ دارای جواب است؟

تذکر ۳.۷ معادله تمرین فوق حالت خاصی است از معادله باشه[۳] به شکل $y^{۲} = x^{۳} + k$، که در سال ۱۶۲۱ توسط باشه بررسی شده است. موردل [۴] نشان داده است چنین معادله ای دارای تعدادی متناهی جواب است.

تمرین ۳.۷ نشان دهید که بی نهایت عدد اول به شکل $۸n - ۱$ وجود دارد.

۷.۲ نماد ژاکوبی

تعریف. اگر a عددی صحیح و b عدد صحیح مثبت و فردی باشد، نماد ژاکوبی $(\frac{a}{b})$ را چنان تعریف می کنیم که تعمیم دهندهٔ نماد لژاندر باشد.

---

[۱] Kronecker
[۲] Weber
[۳] Bachet
[۴] Mordel

فرض کنیم $b=\Pi_{i=1}^{1} P_i^{n_i}$، تجزیهٔ عدد صحیح مثبت و فردِ b باشد، در این صورت نماد ژاکوبی با

$$(\frac{a}{b})=\Pi_{i=1}^{r}(\frac{a}{p_i})^{n_i}$$

تعریف می شود.

تذکر ۴.۷ اگر a به پیمانه p مربع باشد، یعنی همنهشتی $x^2\equiv a \pmod b$ دارای جواب باشد، آن گاه برای هر i، $(\frac{a}{p_i})=1$. نتیجه این که $(\frac{a}{b})=1$، لیکن عکس آن درست نیست.

تمرین ۴.۷ برای اعداد صحیح a، a'، b و b' که b و b' مثبت و فردند نشان دهید که

یک) $(\frac{a}{b})(\frac{a'}{b})=(\frac{aa'}{b})$

دو) $(\frac{a}{b})(\frac{a}{b'})=(\frac{a}{bb'})$

سه) اگر $a\equiv a' \pmod b$، آنگاه $(\frac{a}{b})=(\frac{a'}{b})$.

تمرین ۵.۷ فرض کنید a و b اعداد صحیح و مثبت اند. نشان دهید که

یک) $(\frac{-1}{b})=(-1)^{\frac{b-1}{2}}$

دو) $(\frac{2}{b})=(-1)^{\frac{b^2-1}{8}}$

سه) $(\frac{a}{b})(\frac{b}{a})=(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$

۷.۳ کاربردها

نخست، کاربرد جالب توجه ای از قسمت (یک) قضیهٔ ۱.۷ در نظریهٔ جمعی اعداد را ملاحظه می کنیم.

با در نظر گرفتن پیمانه ۴، به سادگی دیده می شود که عدد صحیح

$$n\equiv 3 \pmod 4$$

را نمی توان به صورت مجموع دو مربع در $\mathbb{Z}$ نوشت.

از طرفی، اینک ثابت می کنیم:

قضیه ۲.۷ هر عدد اولِ p که به پیمانه ۴ با ۱ همنهشت باشد را می توان به صورت مجموع دو مربع در $\mathbb{Z}$ نوشت.

اثبات. فرض کنیم p یک عدد اول همنهشت با ۱ به پیمانهٔ ۴ باشد. ابتدا نشان می دهیم که اگر $x,y \in \mathbb{Z}$ وجود داشته باشند که برای عدد صحیح $k \geq 2$، $x^2+y^2=kp$، آن گاه $x_1, y_1 \in \mathbb{Z}$ وجود دارد به طوری که $x_1^2+y_1^2=k_1p$ و $1 \leq K_1 < k$.

اعداد صحیح x_0 و y_0 را چنان انتخاب می کنیم که

$$x_0 \equiv x \pmod{k}, y_0 \equiv y \pmod{k}$$

و

$$-\frac{k}{2} \leq x_0, y_0 < \frac{k}{2}$$

از این رو $x_0^2+y_0^2 \equiv x^2+y^2 \equiv 0 \pmod{k}$. قرار می دهیم $x_0^2+y_0^2=k_1k$. اکنون

$$(x_0x+y_0y)^2+(x_0y-y_0x)^2 \equiv (x_0^2+y_0^2)(x^2+y^2)=k_1k^2p \qquad (۸.۷)$$

اما

$$x_0x+y_0y \equiv x^2+y^2 \equiv 0 \pmod{k}$$

و

$$x_0y-y_0x \equiv xy_0-y_0x \equiv 0 \pmod{k}$$

و لذا از (۸.۷) داریم

$$(\frac{x_0x+y_0y}{k})^2+(\frac{x_0y-y_0k}{k})^2=k_1p.$$

که دو عدد صحیح x_1 و y_1 را که در $x_1^2+y_1^2=k_1p$ صدق می کنند به دست می دهد.

از آنجا که $k_1k=x_0^2+y_0^2 \leq \frac{k^2}{2}$ داریم $k_1 \geq \frac{k}{2}$. همچنین $k_1=0$ نتیجه می دهد $x_1=0$، $y_0=0$، از این رو $x \equiv 0 \pmod{k}$، $y \equiv 0 \pmod{k}$. بنابراین $pk \mid (x^2+y^2)=pk$، که از آن نتیجه می شود $k=p$ و این یک تناقض است. لذا $1 \leq k_1 < k$.

از آنجا که -1 ماندهٔ درجهٔ دوم به پیمانه p است، عدد صحیح u، $2 \leq u \leq p-1$ وجود دارد به طوری که $u^2+1=kp$ که $k \geq 1$. همچنین، به علت این که تفاضل

دو مربع نمی تواند برابر با ۱ باشد، داریم $k \neq p$. اگر $k = ۱$ اثبات تمام است. در غیر این صورت، به موجب نتیجه فوق، $x_۱, y_۱ \in \mathbb{Z}$ به دست خواهد آمد به طوری که برای $۱ < k_۱ < k$، $x_۱^۲ + y_۱^۲ = k_۱ p$ و در ادامه اعداد صحیح r و s به دست می آیند که $r^۲ + s^۲ = p$.□

قضیه ۳.۷ عدد صحیح $n \geq ۱$، مجموع دو مربع است اگر و تنها اگر هیچ عدد اول $p \equiv ۳ \pmod{۴}$، با توان فرد در تجزیه n به حاصلضرب اعداد اولِ متمایز وجود نداشته باشد.

اثبات. ابتدا فرض کنیم $n = x^۲ + y^۲$ و $p \equiv ۳ \pmod{۴}$، عدد اولی باشد که n را عاد می کند. گیریم p^r بزرگترین توانی از p باشد که n را عاد می‌کند.

در صورت امکان، فرض کنیم r فرد است. اگر $d = (x, y)$ بزرگترین مقسوم علیه مشترک x و y باشد، آن گاه $d^۲ \mid n$ و

$$n_۱ = x_۱^۲ + y_۱^۲ \qquad (۹.۷)$$

که در آن $x_۱ = x/d, y_۱ = y/d$ و $n_۱ = n/d^۲$، اینک $(x_۱, y_۱) = ۱$ و لذا p می تواند ، حداکثر یکی از اعداد صحیح $x_۱$، $y_۱$ و $n_۱$ را عاد کند. از آنجا که r، فرد است، $p \mid n_۱$. بنابراین p، نه $x_۱$ و نه $y_۱$ را عاد نمی کند. با در نظر گرفتن (۹.۷) به عنوان یک معادله روی $\mathbb{F}_p$، داریم $(x_۱/y_۱)^۲ = -۱$ که بدان معنی است که

$$(\frac{-۱}{p}) = ۱$$

به علت این که $p \equiv ۳ \pmod{۴}$، برابری فوق امکان پذیر نیست. لذا

$$(\frac{-۱}{p}) = (-۱)^{\frac{p-۱}{۲}} = -۱.$$

بنابراین r نمی تواند فرد باشد.

به عکس اگر، هیچ عدد اول $p \equiv ۳ \pmod{۴}$ باتوان فرد در تجزیهٔ n به توان‌های اعداد اولِ متمایز وجود نداشته باشد، آن گاه $n = m^۲ p_۱ \cdots p_l$ که در آن به ازای $j = ۱, \cdots, l$، $p_j \equiv ۱ \pmod{۴}$ از آن جا که بنابر (۸.۷) حاصلضرب مجموع مربعات دو عدد باز مجموع دو مربع است، بنابر قضیهٔ (۲.۷) n مجموع دو مربع است.□

فرض کنیم عدد صحیح n که مربع است، مفروض باشد. در این صورت بدیهی است n، برای هر عدد اول p ماندهٔ درجه دوم است. می توان سوأل کرد که آیا عکس این موضوع هم درست است. بدین معنی که اگر عدد صحیح n برای هر عدد اول p، ماندهٔ درجه دوم باشد آیا، n مربع کامل است؟

قضیهٔ بعد، بیانی قوی تر دارد. اثبات، همان است که در $[IR]$ آمده است.

قضیه ۴.۷ اگر عدد صحیحی برای تمام اعداد اول مگر تعداد متناهی، ماندهٔ درجه دوم باشد، آن گاه مربع است.

اثبات. ثابت می کنیم که اگر عدد صحیح و مثبت n، مربع نباشد، آن گاه تعدادی نامتناهی عدد اول p وجود دارد به طوری که a ماندهٔ درجه دوم به پیمانهٔ p نیست. از آنجا که برای عدد اول و فرد p، داریم $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$، نتیجه به دست خواهد آمد.

از آنجا که عدد صحیح مثبت و نامربع a را می توان به شکل n^2a' نوشت که $a' > 1$، بدون مربع است. از ابتدا می توان فرض کرد که a بدون مربع است. بنابراین فرض کنیم $a > 1$ بدون مربع باشد. گیریم $a = 2^s p_1 p_2 \cdots p_r$ که در آن $s = 0$ یا $s = 1$ و p_iها اعداد اول فرد متمایز هستند.

اثبات به دو حالت تقسیم می شود. حالتی که $r = 0$ (و لذا $s = 1$) و حالت دوم که $r > 0$.

حالت اول $(r = 0, s = 1)$

در اینجا $a = 2$. فرض کنیم $\{q_1, q_2, \cdots, q_m\}$ مجموعه متناهی اعداد اول فرد باشد که شامل ۳ نیست و برای $i = 1, 2, \cdots, m$، $(\frac{2}{q_i}) = -1$.

فرض کنیم $b = 8q_1q_2\cdots q_m + 3$. در این صورت بنابر تمرین ۵.۷ (۲). داریم $(\frac{2}{b}) = -1$ و لذا به ازای یک مقسوم علیه اول b مانند l، $(\frac{2}{l}) = -1$، اما l نمی تواند ۳ یا هیچکدام از اعداد اول q_i باشد. بنابراین تعداد نامتناهی عدد اول فرد وجود دارد که ۲ به پیمانهٔ آنها ناماندهٔ درجهٔ دوم است.

حالت دوم $(r > 0)$

فرض کنیم $\{q_1, q_2, \cdots, q_m\}$ مجموعه ای از اعداد اول فرد باشد که شامل هیچیک از p_iها نیست. فرض کنیم t عدد صحیحی باشد که $(\frac{t}{p_r}) = -1$.

بنابر قضیهٔ باقی ماندهٔ چینی، عدد صحیح مثبت N وجود دارد که در مجموعه همنهشتیهای زیر صدق می کند

$$\begin{aligned}
x &\equiv 1 \pmod{q_i} && \text{برای } i = 1, 2, \cdots, m\\
x &\equiv 1 \pmod{8} \\
x &\equiv 1 \pmod{p_i} && \text{برای } i = 1, 2, \cdots, r-1\\
x &\equiv t \pmod{p_r}
\end{aligned}$$

از آنجا که $N \equiv ۱ \pmod{۸}$، از تمرین ۴.۷، داریم $(\frac{۲}{N}) = ۱$ و برای $i = ۱, ۲, \cdots, r$، $(\frac{p_i}{N}) = (\frac{N}{p_i})$.
لذا

$$\begin{aligned}(\tfrac{a}{N}) &= (\tfrac{۲}{N})(\tfrac{p_۱}{N})\cdots(\tfrac{p_{r-۱}}{N})(\tfrac{p_r}{N})\\ &= (\tfrac{۲}{N})(\tfrac{N}{p_۱})\cdots(\tfrac{N}{p_{r-۱}})(\tfrac{N}{p_r})\\ &= -۱.\end{aligned}$$

بنابراین با توجه به تعریف نماد ژاکوبی، نتیجه می شود که به ازای یک عدد اول p، که N را عاد می کند، $(\frac{a}{p}) = -۱$. همچنین p عدد اول فردی است که $p \in \{q_۱, q_۲, \cdots, q_m\}$.

۷.۴ رهیافتی مقدماتی

در تمرین زیر، طرح کلیِ یک اثبات مقدماتیِ قانون تقابل درجهٔ دوم ارائه می شود.

تمرین ۶.۷ فرض کنید p یک عدد اول فرد و a یک عدد صحیح است، به قسمی که $a \not\equiv ۰ \pmod{p}$. کوچکترین مانده عدد صحیح مثبت t_i، $i = ۱, ۲, \cdots (p-۱)/۲$، به پیمانه p از $(p-۱)/۲$ مضربهای a را در نظر می گیریم:

$$a, ۲a, \cdots, \tfrac{p-۱}{۲}a \qquad (۱۰.۷)$$

یک)ملاحظه کنید که اعداد (۱۰.۷) به پیمانهٔ p ناهمنهشت هستند.

دو) فرض کنید $r_۱, r_۲, \cdots, r_m$ مانده هایی به پیمانهٔ p باشند که برابر با $(p-۱)/۲$ یا کوچکتر از آنند و $s_۱$،$s_۲$،$\cdots$،s_n، آنهایی باشند که از $(p-۱)/۲$ بزرگترند.
از این قرار $m + n = (p-۱)/۲$. نشان دهید که $(p-۱)/۲$ اعداد صحیح

$$r_۱, r_۲, \cdots, r_m, p-s_۱, \cdots, p-s_n$$

متمایزند. اکنون لم گاوس را نتیجه بگیرید:

$$(\frac{a}{p}) = (-۱)^n.$$

سه) نتیجه گاوس را به کاربرده، ثابت کنید

$$(\frac{۲}{p}) = (-۱)^{\frac{p^۲-۱}{۸}}.$$

چهار) اگر $k \in \{۱, ۲, \cdots, \frac{p-۱}{۲}\}$، داریم $ka = [ka/p]p + t_k$ که $[ka/p]$ قسمت صحیح (ka/p) است. مجموعهای زیر را در نظر بگیرید

$$\sum_{k=۱}^{(p-۱)/۲} ka$$

و

$$\sum_{k=۱}^{\frac{p-۱}{۲}} k = \sum_{k=۱}^{m} r_k + \sum_{k=۱}^{n} (p - s_k).$$

مجموع دوم را از مجموع اول تفریق کنید. ثابت کنید اگر a فرد باشد، آن گاه

$$(\frac{a}{p}) = (-۱)^M$$

که $M = \sum_{k=۱}^{(p-۱)/۲} [\frac{ka}{p}]$.

پنج) فرض کنید p و q دو عدد اول فرد باشد. مستطیلی را در صفحه XY که دارای رأسهای $(۰, ۰), (p/۲, ۰), (۰, q/۲), (p/۲, q/۲)$ است در نظر بگیرید. ملاحظه کنید که به تعداد $[kr/p]$ نقطه با مختصات مشبکه‌ای بالای نقطهٔ $(k, ۰)$، در پاره خط قائمی که $(k, ۰)$ و $(k, kq/p)$ را به یکدیگر وصل می کند، وجود دارد. با استدلالی مشابه برای پاره خطهای افقی، نشان دهید که شمارشِ نقاط مشبکه ای صحیح در داخلِ مستطیل به اثبات (سه) قضیه ۱.۷ می‌انجامد.

مجموعه تمرین ب

ب . ۱ فرض کنید R یک حوزه اقلیدسی است، نشان دهید که یک عنصر ناصفر نایکه u وجود دارد به طوری که برای هر $\alpha \in R$ عنصر $r \in R^* \cup \{0\}$ وجود دارد که $u \mid (\alpha - r)$.

ب . ۲ نشان دهید که حلقهٔ $R = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-13}}{2}$ یک حوزه اقلیدسی نیست.

ب . ۳ برای عدد اول p، ثابت کنید که چندجمله ای $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$ در $\mathbb{Q}[x]$ تحویل ناپذیر است.

ب . ۴ ثابت کنید که چند جمله‌ای های $x^2 + 1$ و $x^2 + x + 4$، عناصر تحویل ناپذیر $\mathbb{F}_{11}[x]$ هستند. نشان دهید که هیات‌های $\frac{\mathbb{F}_{11}[x]}{(x^2+1)}$ و $\frac{\mathbb{F}_{11}[x]}{(x^2+x+4)}$ یکریخت‌اند.

ب . ۵ فرض کنید $k = \mathbb{F}_2[x]/(1 + x + x^2)$، گروه گالوای $Gal(K : \mathbb{F}_2)$ چیست؟

ب . ٦ فرض کنید $q = p^2$، که p عددی اول است. نشان دهید که $Gal(\mathbb{F}_q/\mathbb{F}_p)$ یک گروه دوریِ مرتبه n است. مولد این گروه، خود ریختی فروبینیوس $a \longrightarrow a^p$ است.

ب . ۷ اگر تابع $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ مفروض باشد، نشان دهید که $g(x) \in \mathbb{F}_q[x]$ وجود دارد به طوری که برای هر $x \in \mathbb{F}_q$، $f(x) = g(x)$. به عکس اگر R یک حلقه باشد (مثل همیشه تعویضپذیر)، به قسمی که هر تابع از R به R با یک چندجمله ای $R[x]$ بیان شود، آن گاه R هیاتی متناهی است.

ب . ۸ آیا اعداد صحیح x و y وجود دارند که $7y = 2x^2 + 3x + 1$؟

ب . ۹ نشان دهید که معادله $y^2 = x^3 + 45$ در اعداد صحیح جواب ندارد.

فصل ۸

مدول‌ها

برای حلقه R، اصطلاح R−مدول‌ها پیش از این در فصل ۰، تعریف شده است. در این فصل بعضی تعریف‌ها و نتیجهٔ راجع به مدول‌ها را ملاحظه خواهیم کرد. خود را به جمع آوری آن مقدار اطلاعاتی که هنگام مطالعه هیأت های اعداد، در فصل‌های آینده مورد نیاز است، محدود خواهیم کرد.

۸.۱ تعریف های بنیادی

تعریف. فرض کنیم M یک R−مدول باشد. یک زیر مدول M، مانند M' یک زیر گروه M است که تحت ضربِ اسکالری، توسط عناصر R بسته باشد.

اگر M' یک زیر مدول M باشد، آن گاه گروه خارج قسمتیِ M/M' تحت ضرب اسکالری تعریف شده با $r(a+M') = ra+M'$، یک R−مدول می شود. این مدول، مدول خارج قسمتی M توسط M' نامیده می شود.

فرض کنیم M و N دو R−مدول باشند. یک تابع $f : M \longrightarrow N$ یک R−مدول همریختی نامیده می شود، هر گاه در شرایط زیر صدق کند

یک) برای هر $x, y \in M$، $f(x+y) = f(x) + f(y)$

دو) برای هر $r \in R$ و هر $x \in M$، $f(rx) = rf(x)$

یک مدول همریختی دو سویی، یک مدول یکریختی نامیده می شود. مانند حالت گروه‌ها و حلقه ها، اگر $f : M \longrightarrow N$ یک R−مدول همریختی باشد، آن گاه هستهٔ f که با $ker(f) = \{x \in M : f(x) = 0\}$ تعریف می شود یک زیر مدول M

است و مدول خارج قسمتی $M/ker(f)$ با تصویرِ $f(M)$ که با $Im(f)$ نشان داده می شود یکریخت است.

برای عنصر $r \in R$ و R–مدول M، rM با مجموعهٔ $\{rm : m \in M\}$ تعریف می شود. برای ایدآل Iی R، IM برابر با زیر مجموعهٔ M که شامل تمام مجموع های $\sum r_i a_i$ که $r_i \in I$، $a_i \in M$، تعریف می شود. بویژه حاصلضرب دو ایدآل R نیز تعریف می شود. به سادگی دیده می شود که rM و IM زیر مدولهای M هستند.

اگر N و N' دو زیر مدول R–مدول M باشند، آن گاه مجموعهٔ $\{r \in R : rN' \subset N\}$، به وضوح یک ایدآل R است. آن را با $(N : N')$ نشان می دهیم. در حالتِ ویژه، هنگامی که $N = \{\circ\}$، ایدآل $(N' : \{\circ\})$، پوچساز N' نامیده شده و با $Ann_R(N')$ نشان داده می شود. اگر پوچساز N'، $Ann_R(N')$، ایدآل صفر باشد، آن گاه N' صادق خوانده می شود.

فرض کنیم $\{M_i\}_{i\in I}$ یک خانوادهٔ R–مدول‌ها باشد. در این صورت، حاصلضرب مستقیم $\prod_{i\in I} M_i$، مجموعهٔ تمام خانواده های $(a_i)_{i\in I}$ است که با I اندیس دار شده و $a_i \in M_i$. جمع، و ضرب اسکالری به طریق معلومِ مولفه به مولفه تعریف می شود. حاصلجمع مستقیم این مدول‌ها، $\oplus M_i$ یک زیر مدول حاصلضرب مستقیم تعریف می شود که شامل تمام $(a_i)_{i\in I}$ است، به طوری که برای تمام، مگر تعدادی متناهی اندیسِ $i \in I$، $a_i = \circ$. اگر مجموعهٔ اندیس I متناهی باشد، آن گاه مجموع و حاصلضرب مستقیم یکی هستند.

یک مجموع مستقیمِ نسخه های R–مدول M، یک R–مدول آزاد نامیده می شود. از نماد R^n برای مجموع مستقیم n نسخهٔ R استفاده خواهیم کرد. به موجب قرار داد، R°، مدول $\{\circ\}$ را نشان می دهد.

اگر M یک R–مدول و S یک زیر مجموعهٔ M باشد، آن گاه کوچکترین زیر مدول M که شامل S است، زیر مدول تولید شده با S نامیده می شود. این زیر مدول اشتراک تمام زیر مدولهای M است که شامل S هستند. علاوه بر آن زیر مدول تولید شده با S را می توان به طور صریح توصیف کرد. این زیر مدول متشکل از تمام به شکل $\sum r_i s_i$ است که در آن، مجموع متناهی است و برای هر i، $r_i \in R$ و $s_i \in S$.

یک زیر مدول M که با یک مجموعهٔ متناهی تولید می شود متناهی–تولید شده نامیده می شود.

اگر خانوادهٔ $\{M_i\}_{i\in I}$ از زیرمدول‌های R–مدول M مفروض باشد، آن گاه کوچکترین زیر مدول M که شامل M_iها می باشد، مجموعِ زیرمدول‌های M_i بوده و با $\sum_{i\in I} M_i$ نشان داده می شود. اگر M متناهی باشد، مثلاً $I = \{۱, ۲, \cdots, r\}$ گاهی به

جای $\sum_{i=1}^{r} M_i$ می نویسیم $M_1 + M_2 + \cdots + M_r$. زیر مدول تولید شده توسط زیر مجموعهٔ S در M چیزی نیست مگر مجموع زیر مدول‌های Ra که $a \in S$.

یک زیر مجموعهٔ $R-$مدول M مانند S، مستقل خطی خوانده می شود، هرگاه برای هر زیر مجموعهٔ متناهی $\{a_1, \cdots, a_t\}$ از S، $\sum_{i=1}^{t} r_i a_i = 0$ نتیجه بدهد که برای هر i، $r_i = 0$. اگر یک زیر مجموعهٔ مستقلِ S در M وجود داشته باشد که M توسط S تولید شود، آن گاه S را پایهٔ M می نامند.

تذکر ۱.۸ یک فضای برداری یک $R-$مدول آزاد روی هیات F است. بر خلاف حالت فضای برداری، یک مجموعهٔ مستقل یک مدول آزاد لزوماً توسیع پذیر به یک پایه نیست. همچنین اگر زیر مجموعهٔ S، یک زیر مدول آزاد تولید کند، S لزوماً شامل یک پایه نیست.

تمرین ۱.۸ مثالی از یک مجموعهٔ مستقل یک مدول آزاد ارائه دهید که توسیع پذیر به یک پایه نباشد. همچنین یک زیر مجموعهٔ S از یک مدول M مثال بزنید که S، M را تولید کند، اما S شامل یک پایهٔ M نباشد.

تمرین ۲.۸ (آ) یک $R-$مدول M آزاد است، اگر و تنها اگر دارای یک پایه باشد.
(ب) برای یک $R-$مدول آزادM، عدد اصلی هر دو پایهٔ M روی R برابر است.

تعریف. در تمرین ۱.۸ (ب)، عدد اصلی پایه های مختلف R رتبهٔ $R-$مدول آزاد M نامیده شده و آن را با $ranK_R(M)$ نشان می دهند.

۲.۸ نتیجه‌ای دربارهٔ $R-$ مدول‌های متناهی تولید شده

قضیه ۱.۸ فرض کنیم M یک $R-$مدول متناهی—تولید شده با n عنصر است. فرض کنیم $\phi : M \longrightarrow M$ یک $R-$همریختی و I یک ایدآل R باشد به قسمی که $\phi(M) \subset IM$. در این صورت رابطه ای به شکل زیر برقرار است

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

اثبات. فرض کنیم $M = \sum_{i=1}^{n} Rw_i$. بنا بر فرض $a_{ij} \in I$ وجود دارد که برای هر $1 \le i \le n$، $\phi(w_i) = \sum_{j=1}^{n} a_{ij} w_j = 0$. برابری اخیر را می توان چنین نوشت

$$\sum_{j=1} (\phi\delta_{ij} - a_{ij})w_j = 0$$

که δ_{ij} نشانه کرونکر است و $1 \leq i \leq n$.
با ضرب طرف چپ در الحاقی ماتریسِ $(\delta_{ij}\phi - a_{ij})$ مشاهده می کنیم که دترمینانِ همریختی صفر است، زیرا برای هر i، $det((\delta_{ij} - a_{ij})a_{j\circ}) = \circ$. با بسط دترمینان نتیجه به دست می آید.□

نتیجهٔ زیر به کرول—آزومایا و ناکامایا منسوب است و در متون، به عنوان لم ناکامایا شناخته می شود.

قضیه ۲.۸ فرض کنیم M یک R–مدولِ متناهی—تولید شده و I یک ایدآل R باشد. اگر $IM = M$، آن گاه $r \in R$ وجود دارد که $r \equiv 1 \pmod{I}$ (یعنی $r - 1 \in I$) و $rM = \circ$. علاوه بر آن، اگر I مشمول در اشتراک تمام ایدآل‌های ماکسیمال باشد (که رادیکال جیکوبسن R نامیده می شود)، آن گاه $M = \circ$.

اثبات. تابع $\phi : M \longrightarrow M$ را تابع همانی اختیار می کنیم. از قضیه ۱.۸ مشاهده می شود که $r = 1 + a_1 + \cdots + a_n = \circ$ در شرطِ مطلوب صدق می کند.

اکنون فرض کنیم I مشمول در رادیکال جیکوبسن باشد. در این صورت r در R یکه است. زیرا r متعلق به یک ایدآل ماکسیمال است و از رابطه بالا، ۱ به آن تعلق خواهد داشت که ممتنع است. بنابراین $M = r^{-1}rM = \circ$.□

۸.۳ مدول‌های نویتری

تعریف. فرض کنیم M یک R–مدول باشد، گویند M نویتری است هر اگر زنجیر فزایندهٔ $M_1 \subset M_2 \subset \cdots$ از زیر مدولها ایستا باشد، یعنی عدد صحیح مثبت n وجود داشته باشد که $M_n = M_{n+1} = \cdots$.

حلقهٔ R یک حلقه نویتری خوانده می شود، هر گاه به عنوان R–مدول نویتری باشد.

مثال‌ها. اگر M یک R–مدول با تعدادی متناهی عنصر باشد، آن گاه، آشکارا، نویتری است. به ویژه یک گروه آبلی متناهی که به عنوان $\mathbb{Z}$ مدول در نظر گرفته می شود، نویتری است. از آنجا که ایدآل‌های $\mathbb{Z}$ به ازای یک عدد m به شکل $m\mathbb{Z}$ هستند. به سادگی دیده می شود که $\mathbb{Z}$، یک $\mathbb{Z}$–مدول نویتری است لذا $\mathbb{Z}$ مثالی از یک حلقهٔ نویتری است. حلقهٔ چندجمله‌ای‌های $R[x_1, x_2, \cdots]$ با تعداد نامتناهی متغیر نویتری نیست.

قضیه ۳.۸ فرض کنیم M یک R–مدول باشد. در این صورت شرط‌های زیر هم ارزند.

یک) M نویتری است.

دو) هر زیر مجموعهٔ ناتهیِ زیر مدول‌ها دارای عضو ماکسیمال است.

سه) هر زیر مدولِ M، متناهی تولید شده است.

اثبات. (یک) $\Longleftarrow$ (دو)

در صورت امکان فرض کنیم یک مجموعهٔ نا تهی $\mathcal{M}$ از زیر مدول‌ها وجود دارد که دارای عضو ماکسیمال نیست. فرض کنید $M_1 \subset \mathcal{M}$. از آنجا که M_1 ماکسیمال نیست، زیر مدول M_2 وجود دارد که $M_1 < M_2$. چون M_2 ماکسیمال نیست، زیر مدول M_3 وجود دارد که $M_2 < M_3$.با ادامهٔ این روند یک زنجیر فزایندهٔ زیر مدول‌ها به دست می آید که ایستا نیست، تناقض با این فرض که که M نویتری است.

(دو) $\Longleftarrow$ (سه)

فرض کنیم N یک زیر مدول دلخواه M است. فرض کنیم S مجموعهٔ تمام زیر مدول‌هایِ متناهی تولید شده است. از آنجا که $\{0\} \in S$ ملاحظه می کنیم که S تهی نیست. بنابراین S دارای عضو ماکسیمال، مثل N' است. فرض کنیم a یک عضو N باشد، زیر مدول $N' + Ra$ در N را در نظر می گیریم. این زیر مدول، متناهی–تولید شده است. از اینجا نتیجه می گیریم که $a \in N'$. به علت این که $a \in N$ دلخواه است. نتیجه می گیریم که $N = N'$، بنابراین N متناهی–تولید شده است.

(سه) $\Longleftarrow$ (یک).

فرض کنیم $M_1 \subset M_2 \subset \cdots$ یک زنجیر فزایندهٔ زیر مدول‌ها باشد. اینک $\cup_{i=1}^{\infty} M_i$ نیز یک زیر مدول M است و بنابرفرض، متناهی–تولید شده است. فرض کنیم $\{a_1, a_2, \cdots, a_m\}$ یک مجموعهٔ مولد برای M باشد. گیریم $a_i \in M_{t_i}$. فرض کنیم T در بین t_1، t_2 و $t_M, \cdots$ ، بزرگترین باشد. در این صورت $M_T = \cup_{i=1}^{T} M_i = \cup_{i=1}^{\infty} M_i$ و بنابراین $\cdots = M_{T+2} = M_{T+1} = M_T$.$\square$

تذکر ۲.۸ پیشتر مشاهده کردیم که $\mathbb{Z}$ نویتری است از قضیهٔ فوق (سه) نتیجه می شود که هر حوزهٔ ایدآل‌های اصلی نویتری است. به ویژه هر حوزهٔ اقلیدسی نویتری است.

اثبات. یک دنبالهٔ

$$\cdots \longrightarrow M_{r-1} \xrightarrow{f_r} M_r \xrightarrow{f_{r+1}} M_{r+1} \longrightarrow \cdots$$

از زیر مدول‌هایِ $\{M_i\}$ و R–همریختی‌هایِ $\{f_i\}$، در M_r کامل خوانده می شود،

هر گاه $Im(f_r) = ker(f_{r+1})$. این دنباله، دنبالهٔ کامل است، هرگاه در تمام M_rها کامل باشد.

دنبالهٔ کامل به شکل خاصِ

$$\{0\} \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow \{0\}$$

دنبالهٔ کامل کوتاه نامیده می شود. این بدان معنی است که f یک به یک، g پوشا است و $Im(f) = ker(g)$.

قضیه ۴.۸ فرض کنیم $\{0\} \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow \{0\}$ یک دنبالهٔ کاملِ کوتاه از R–مدول‌ها باشد. در این صورت M نویتری است، اگر و تنها اگر M' و M'' نویتری باشند.

اثبات. فرض کنیم M نویتری است و $M'_1 \subset M'_2 \subset \cdots$ یک زنجیر فزایندهٔ زیر مدول‌های M' است.

اینک $f(M'_1) \subset f(M') \subset \cdots$ یک زنجیرِ فزایندهٔ زیر مدول‌های M است. از آنجا که بنا بر فرض M نویتری است. این دنباله، ایستا است. به علت این که f یک به یک است. دنبالهٔ اصلیِ $M'_1 \subset M'_2 \subset \cdots$ ایستا می شود، بنابراین M' نویتری است. به طور مشابه زنجیرِ فزایندهٔ زیر مدول‌های M'' به یک زنجیرِ فزایندهٔ زیر مدول‌ها در M منجر می شود. با استدلالی مشابه در می یابیم که M'' نویتری است.

اکنون فرض کنیم که M' و M'' نویتری اند. فرض کنیم $M_1 \subset M_2 \subset \cdots$ یک زنجیر فزایندهٔ زیر مدول‌های M است. بنا بر فرض، زنجیرهای $f^{-1}(M_1) \subset f^{-1}(M_2) \subset \cdots$ و $g(M_1) \subset g(M_2) \subset \cdots$ ایستا می شوند، بنابراین عددِ صحیحِ مثبتِ N وجود دارد که برای هر $r \geq N$، $f^{-1}(M_1) \subset f^{-1}(M_2) \subset \cdots$ و $g(M_r) = g(M_N)$.

برای یک $r \geq N$، فرض کنیم $a \in M_r$، از آنجا که $g(m_r) = g(M_N)$، عنصرِ $b \in M_N$ وجود دارد که $g(a) = g(b)$. این برابری ایجاب می کند $a - b \in ker(g) = Im(f)$. فرض کنیم به ازای یک $c \in f^{-1}(M_r) = f^{-1}(M_N)$، داشته باشیم $f(c) = a - b$. بنابراین $a - b = f(c) \in M_N$ که نتیجه می دهد $a \in b + M_N = M_N$. پس ثابت کردیم که برای هر $r \geq N$، $M_r = M_N$. بنابراین M نویتری است. □

نتیجه ۱.۸ فرض کنیم M_1، M_2، $\cdots$، M_t، R–مدول‌های نویتری باشند، در این صورت $\oplus_{i=1}^{t} M_i$ نویتری است.

اثبات. از دنبالهٔ کوتاهِ کامل

$$\{\circ\} \longrightarrow M_{۲} \longrightarrow M_{۱} \oplus M_{۲} \longrightarrow M_{۱} \longrightarrow \{\circ\}$$

، به موجب قضیه فوق، $M_{۱} \oplus M_{۲}$ نویتری است. در حالت کلی از دنبالهٔ

$$\{\circ\} \longrightarrow M_{۱} \longrightarrow \oplus_{i=۱}^{t} M \longrightarrow \oplus_{i=۱}^{t-۱} M_i \longrightarrow \{\circ\}$$

و از استقرا نتیجه می گیریم که $\oplus_{i=۱}^{t} M_i$ نویتری است.□

نتیجه ۲.۸ فرض کنیم R یک حلقهٔ نویتری و M یک R–مدولِ متناهی—تولید شده باشد. در این صورت M نویتری است.

اثبات. به علت این که M متناهی—تولید شده است. به ازای یک عدد صحیح مثبت n، M، خارج قسمت R^n است. بنابر نتیجه ۱.۴.۸، R^n نویتری است. بنابراین از قضیه ۴.۸ نتیجه می شود که M نویتری است.

تمرین ۳.۸ اگر حلقهٔ R نویتری باشد، نشان دهید که حلقهٔ چند جمله‌ای‌های $R[x_{۱}, x_{۲}, \cdots, x_n]$ نیز نویتری است. (این بیان به قضیهٔ پایهٔ هیلبرت موسوم است).

تمرین ۴.۸ فرض کنید R حلقه‌های است که هر ایدآل اول آن متناهی—تولید شده است. نشان دهید که R نویتری است.(این قضیه منسوب است به کاهن [۱]).

تمرین ۵.۸ فرض کنید $\{\circ\} \longrightarrow M' \longrightarrow M$ یک دنبالهٔ کوتاه باشد که M و M'، R–مدول اند. نشان دهید که برای هر همریختی مفروضِ $f : R \longrightarrow M$، یک همریختی h از R به توی M وجود دارد که $g \circ h = f$، نشان دهید که نتیجه فوق، در حالتی که به جای R یک R–مدول آزاد گذاشته شود نیز درست است. بنابراین نشان دهید که اگر دنبالهٔ

$$\{\circ\} \longrightarrow M_{۱} \xrightarrow{f} M \xrightarrow{g} P \longrightarrow \{\circ\}$$

مفروض باشد، که در آن P آزاد است، آن گاه $M_{۱} \oplus P = M$.

۸.۴ مدول‌های روی ح ا ص

اینک نتیجه مهمی را راجع به مدول‌های روی حوزه‌های ایدآل‌های اصلی ثابت می کنیم.

---

[۱] Cohen

قضیه ۵.۸ فرض کنیم R یک ح ا ص، M یک R−مدول آزاد است و $rank_R(M)=n$ که در آن n عدد صحیح مثبتی است و اگر N یک زیر مدول M باشد، آن گاه N نیز یک R−مدول آزاد است و $rank_R(N)\le m$.

اثبات. فرض کنیم $\{a_1,a_2,\cdots,a_m\}$ یک پایه برای M باشد. برای $1\le r\le m$ ، زیر مدولِ M را که با $\{a_1,a_2,\cdots,a_m\}$ تولید می شود با T_r نشان می دهیم. فرض کنیم $N_r=N\cap T_r$.

اکنون $\boldsymbol{N_1=\{a\in N : a=ra_1,}$ به ازای یک $\boldsymbol{r\in R}$ $\}$. مجموعهٔ $\{r\in R : ra_1\in N_1\}$ یک ایدآل R است و چون R یک ح ا ص است این ایدآل با عضوی مانند r_1 در R تولید شده است. $r_1=0$، آن گاه N_1، برابر با R−مدول آزادِ $R^0=\{0\}$ است که با مجموعه تهی تولید شده است. اگر $r_1\neq 0$، به وضوح N_1 با r_1a_1 تولید شده است.

فرض کنیم $2\le t\le m$. حال فرض کنیم که برای $i\le t-1$، N_i یک R−مدول آزاد و از رتبهٔ $rank_R(N_i)\le i$ است. ثابت می کنیم که N_t آزاد و با رتبه $rank_R(N_t)$ می باشد.

قرار می دهیم

$\boldsymbol{I=\{r\in R : ra_t+\sum_{j=1}^{t-1} r_ja_i\in N_t}$، برای بعضی $\boldsymbol{r'_j}$ها در $\boldsymbol{R}$ $\}$.

باز هم I یک ایدآل R است، لذا اصلی است و با عنصری مانند r_t تولید شده است. بدیهی است که $r_t=0$، اگر و تنها اگر $N_t=N_{t-1}$. اگر $r_t=0$، به موجب فرض استقرا، N_t آزاد و از رتبهٔ $rank_R(N_t)\le t-1<t$ است.

فرض کنیم $r_t\neq 0$، در این صورت $a'\in N_t$ وجود دارد به طوری که به ازای r_jهایی در R، $a'=r_ta_t+\sum_{j=1}^{t-1} r_ja_j\in N_t$. فرض کنیم a'' یک عضو N_t است، در این صورت به ازای s_jهایی در R، $a''=\sum_{j=1}^{t} s_ja_j$ که به ازای یک $r\in R$، $s_t=rr_t$. اکنون $ra'-a''\in N_{t-1}$. نتیجه می گیریم که $N_t=N_{t-1}\oplus Ra'$. بنابراین N_t آزاد با مرتبهٔ $rank_R(N_t)\le (t-1)+1=t$ است.

تذکر ۳.۸ بیان قضیهِ فوق، حتی اگر رتبه نامتناهی باشد، نیز درست است.

۸.۵ برخی نتایج ویژه

با در نظر گرفتن آنچه که در فصل‌های بعد به آن نیاز داریم، در قسمتِ باقی ماندهٔ این فصل، به نتیجه ای در مورد صورت‌های دو خطی روی فضاهای برداری توجه می کنیم. پس از آن نتیجه ای راجع به مشبکه ها در R^n خواهد آمد.

تعریف. فرض کنیم V یک فضای برداری روی هیأت K باشد. یک فرم دو خطیِ B بر V، یک تابعِ $V \times V \longrightarrow K$ است، به قسمی که برای هر $a, b \in V$، توابع $x \longrightarrow B(x,b)$ و $y \longrightarrow B(y,b)$ از V به K همریختی‌هایی از V به K باشند.

فرمِ دو خطیِ $B(x,y)$ بر V ناتبهگون خوانده می شود هرگاه برای عناصر ناصفر $a, b \in V$، همریختیهای $x \longrightarrow B(x,b)$ و $y \longrightarrow (B,y)$ نا صفر باشند.

تمرین ۶.۸ فرض کنید V یک فضای برداری با بعدِ n روی هیأت K و $B(x,y)$ یک فرم دوخطی ناتبهگون روی V باشد، در این صورت برای هر K–پایهٔ $w_1, w_2, \cdots, w_n$ در V یک پایهٔ متناظرِ $w_1, w_2, \cdots, w'_n$ وجود دارد که $B(w_{ij} w'_j) = \delta_{ij}$، $1 \leq i, j \leq n$.

تعریف. یک زیر گروه H از $\mathbb{R}^n$، گسسته نامیده می شود، اگر برای هر زیر مجموعهٔ فشرده $\mathbb{R}^n$ مانند S، اشتراک $H \cap S$، متناهی باشد.

مثال. $Z^n \subset R^n$ گسسته است.

قضیه ۶.۸ فرض کنیم H یک زیر گروه گسستهٔ R^n است. در این صورت H به عنوان یک $\mathbb{Z}$–مدول با $r \leq n$ بردار که روی R مستقل خطی هستند، تولید می شود.

اثبات. فرض کنیم $r(r \leq n)$ بزرگترین عدد صحیحی باشد که H دارای r عنصر باشد که روی $\mathbb{R}$ مستقل خطی اند. فرض کنیم $e_1, e_2, \cdots, e_r$ روی $\mathbb{R}$ مستقل خطی هستند.

فرض کنیم

$$P = \{x \in \mathbb{R}^n | x = \sum_{i=1}^{r} \alpha_i e_i, 0 \leq \alpha_i \leq 1\}$$

متوازی‌السطوح گونه ای باشد که با استفاده از مبدأ و e_iها به عنوان راس ساخته می شود.

به علت این که P فشرده است، $P \cap H$ متناهی است. فرض کنیم $x \in H$. از ماکسیمال بودن $(e_1, e_2, \cdots, e_r)$ نتیجه می گیریم که $\lambda_i \in \mathbb{R}, x = \sum_{i=1}^{r} \lambda_i e_i$.

برای هر عدد صحیح l قرار می دهیم،

$$x_l = lx - \sum_{i=1}^{r} [l\lambda_i] e_i = \sum_{i=1}^{r} (l\lambda_i - [l\lambda_i]) e_i \in P \cap H$$

از آنجا که $P \cap H$ متناهی است، $j \neq k$ وجود دارد که $x_j = x_k$.

از این رو برای $1 \leq i \leq r$ $(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i],$ ولذا ، به ازای یک $1 \leq i \leq r$، $\lambda_i \in \mathbb{Q}$.

بنابراین هر عضو H را می‌توان به صورت یک ترکیب خطی از e_iها با ضرایب گویا نوشت. همچنین به علت این که $x = x_1 + \sum_{i=1}^{r}[\lambda_i]e_i$ که $x_1 \in P \cap H$، H به عنوان یک $\mathbb{Z}-$مدول با $P \cap H$ تولید می شود.

اکنون، هرعنصر $P \cap H$، یک $\mathbb{Q}-$ ترکیب خطی e_iها می باشد.

فرض کنیم $d \in \mathbb{Z} - \{0\}$ مخرج مشترک این ضرایب باشد (بیاد آورید که $P \cap H$ متناهی است). پس $dH \subset \sum_{i=1}^{r}\mathbb{Z}e_i$. بنابراین به موجب قضیه ۵.۸، dH یک گروه آبلی آزاد با رتبه کوچکتر یا مساوی r است. همچنین به علت این که $H \supseteq \sum_{i=1}^{r}\mathbb{Z}e_i$، $rankH \geq r$، اما رتبهٔ H و dH برابر است، لذا $rankH = r$. از آنجا که H شامل r بردار است که روی $\mathbb{R}$ مستقل خطی اند، مولدهای H به عنوان یک $\mathbb{Z}-$مدول آزاد، باید روی R مستقل خطی باشند.□

تعریف. یک گروه گسستهٔ با رتبهٔ n در R^n یک مشبکه در R^n نامیده می شود.

تذکر ۴.۸ بنابر قضیهٔ ۶.۸ یک مشبکه روی $\mathbb{Z}$ با پایه ای از $\mathbb{R}^n$ روی $\mathbb{R}$ که یک $\mathbb{Z}$ پایه برای مشبکه مفروض است تولید می شود.

فصل ۹

اعداد صحیح گاوسی و حلقهٔ $\mathbb{Z}[\sqrt{-5}]$

ملاحظه کردیم که حوزهٔ اعداد صحیح گاوسی، یک حوزهٔ اقلیدسی است. در قسمتِ اول این فصل می کوشیم تا درکِ بیشتری از این حلقه به دست آوریم. در قسمتِ بعد، دربارهٔ حلقهٔ $Z[\sqrt{-۵}]$ که یک ح ت ی نیست بحث خواهیم کرد. مطالعهٔ این حلقه ها می تواند، به عنوان پیش درآمدی برای مطالعهٔ هیأت اعداد، که در فصلهای بعدی ادامه پیدا می کند، مفید باشد.

۹.۱ اعداد صحیح گاوسی

این بخش را با ملاحظاتی که خواهد آمد، شروع می کنیم. اگر یک عدد صحیح گاوسی به مجموعهٔ اعداد حقیقی تعلق داشته باشد، آن گاه یک عدد صحیح معمولی است، از طرف دیگر، یک عدد صحیح گاوسی عاد می کند، اگر و تنها اگر d هم a و b را عاد کند. پیشتر، در فصل ۴ ملاحظه کردیم که حلقهٔ اعداد صحیح گاوسی با تابع اندازه که با $\sigma(a+ib) = a^۲ + b^۲$ بر آن تعریف می شود، یک حوزهٔ اقلیدسی و لذا یک ح ا ص است. همچنین برای دو عنصرِ $a+bi_۱, c+di \in Z[i]$، $\sigma((a+bi)(c+di)) = \sigma(a+bi)\sigma(c+di)$. این برابری خاصیت معروفِ قدر مطلقِ اعداد مختلط است و به سادگی ثابت می شود.

اکنون فرض کنیم $\alpha = a + bi$ یک یکه در $Z[i]$ باشد. در این صورت $\alpha' \in \mathbb{Z}[i]$ وجود دارد که $\alpha\alpha' = ۱$ و لذا $\sigma(\alpha)\sigma(\alpha') = ۱$. این برابری ایجاب می کند که $a^۲ + b^۲ = \sigma(\alpha) = ۱$. به عکس اگر $\sigma(a + bi) = ۱$، آن گاه $a^۲ + b^۲ = (a + bi)(a - bi) = ۱$. که از آن نتیجه می گیریم $a + bi = ۱$. اینک تنها جوابهای معادله دیو فانتی $a^۲ + b^۲ = ۱$ عبارتند از $a = ۱, -۱$، $b = ۰$ یا $a = ۰$ و $b = +۱, -۱$. بنابراین یکه های $\mathbb{Z}[i]$ عبارتند از $+۱$، -۱، $+i$، $-i$.

تعریف. یک عنصر اول در حلقه اعداد صحیحِ گاوسی یک عدد اول گاوس نامیده می شود.

قضیه ۱.۹ اگر p یک عدد اول باشد، آن گاه یا p یک عدد صحیح گاوسی است، یا در غیر این صورت، حاصلضرب دو عددِ اولِ گاوس است، که مزدوج هستند.

اثبات. فرض کنیم p یک عدد صحیحِ اول باشد. ار آن جا که تنها یکه های حلقهٔ اعداد صحیح گاوسی عبارتند از $+۱$، -۱، $+i$ و $-i$. عدد صحیح اول p دارای مقسوم علیهٔ اول گاوس مانند $\Pi = a + bi$ است. از آن جا که p حقیقی است، با مزدوج خود برابر است. بنابراین $\overline{\Pi} = a - bi$ نیز، p را عاد می کند. از این جا نتیجه می گیریم که $\Pi\overline{\Pi} = a^۲ + b^۲$، $p^۲$ را در اعداد صحیح گاوسی عاد می کند. اینک $\Pi\overline{\Pi}$ یک مقسوم علیه $p^۲$ است، بنابراین، در حلقهٔ اعداد صحیح گاوسی یا Π مقسوم علیه سرهٔ p است یا این که Π وابستهٔ p می باشد. در حالت دوم p یک عدد اول گاوس است. در حالت اول $\Pi\overline{\Pi}$ یک مقسوم علیه سرهٔ $p^۲$ در حلقهٔ $\mathbb{Z}$ است، که از آن نتیجه می شود $\Pi\overline{\Pi} = p$.

قضیه ۲.۹ اگر Π یک عدد اول گاوس باشد، آن گاه $\Pi\overline{\Pi}$ یک عدد اول است یا مربع یک عدد اول است.

اثبات. فرض کنیم Π یک عدد اول گاوس باشد. اینک $\Pi\overline{\Pi} = n \in \mathbb{Z}$ و لذا در $Z[i]$ عدد اول گاوسِ Π. یکی از عوامل n مثلاً p را عاد می کند. حال $\Pi\overline{\Pi}$ مقسوم علیه صحیحِ $P^۲$ است. نتیجه حاصل می شود.□

قضیه ۳.۹ اگر p یک عدد اول باشد، آن گاه بیانهای زیر هم ارزند

یک) p حاصلضرب دو عدد مزدوج گاوس است.

دو) p مجموع دو مربع صحیح است.

سه) $p = ۲$ یا این که $p \equiv ۱ \pmod{۴}$.

اثبات. (یک)$\Longleftarrow$(دو)

فرض کنیم $p = \Pi\overline{\Pi}$ که $\Pi = a + bi$ عدد اول گاوس است نتیجه می گیریم که $p = a^۲ + b^۲$

(دو)$\Longleftarrow$(یک)

اگر $p = a^۲ + b^۲$، آن گاه $p = (a+bi)(a-bi)$، یک تجزیهٔ p را در حلقهٔ اعداد صحیحِ گاوسی به دست می دهد که بنابر قضیهٔ ۱.۹ یک تجزیه به عامل های اول است.

بنابراین نشان داده شده که (یک) و (دو) هم ارزند، از آن جا که بنابر قضیه ۲.۷، (دو) و (سه) هم ارزند. اثبات تمام است.□

تذکر ۱.۹ از قضیه ۱.۹ و همارزی (یک) و (سه) در قضیهٔ ۳.۹ نتیجه می شود، که اعداد صحیحِ اول که عدد اول گاوس اند، آنهایی هستند که به پیمانهٔ ۴ با ۳ همنهشت اند.

می توان ملاحظه کرد که اعداد صحیح گاوسی نقاط یک مربع مشبکه ای در صفحهٔ مختلط اند. به طور مشابه حلقهٔ $\mathbb{Z}[\sqrt{-۵}]$ شامل تمام اعداد مختلط که به شکل $a + b\sqrt{-۵}$ هستند، $a, b \in \mathbb{Z}$، نیز مثالی از یک مشبکه در صفحه مختلط است. آشکار است که ایدآل های نا صفرِ این حلقه هر کدام یک زیر مشبکه است.

۹.۲ حلقهٔ $\mathbb{Z}[\sqrt{-۵}]$

همان طور که پیشتر متذکر شدیم، حلقهٔ $\mathbb{Z}[\sqrt{-۵}]$ یک ح ت ی نیست. کارِ خود را با بحث دربارهٔ این حلقه ادامه می دهیم، با استدلالی مشابه حالتِ $\mathbb{Z}[i]$ با تابعِ نرم از $\mathbb{Z} \longrightarrow \mathbb{Z}[\sqrt{-۵}]$ که با $a + b\sqrt{-۵} \longrightarrow a^۲ + ۵b^۲$ تعریف می شود، می توان ملاحظه کرد که یکه های $\mathbb{Z}[\sqrt{-۵}]$، آنهایی هستند که دارای نرم ۱ هستند و لذا برابرند با ۱+ یا ۱−. از آن جا که نرم ضربی است، یک مقسوم علیه سرهٔ $۱ + \sqrt{-۵}$ یا $۱ - \sqrt{-۵}$ باید نرمی برابر با یک مقسوم علیه سرهٔ ٦ یعنی ۲ یا ۳ داشته باشد، از آن جا که $\mathbb{Z}[\sqrt{-۵}]$ فاقد چنین عنصری است، نتیجه می گیریم که $۱ + \sqrt{-۵}$ و $۱ - \sqrt{-۵}$ در $\mathbb{Z}[\sqrt{-۵}]$ تحویل ناپذیرند.

اکنون در موقعیتی هستیم که می توانیم نظری به تذکر ۱.۴ بیاندازیم و دریابیم که $(۱ - \sqrt{-۵})(۱ + \sqrt{-۵}) = ۳ \times ۲ = ٦$، در واقع دو تجزیهٔ، لزوماً متفاوتِ، یک عنصر $\mathbb{Z}[\sqrt{-۵}]$ را به دست می دهد.

بنابراین حلقهٔ $\mathbb{Z}[\sqrt{-۵}]$ یک ح ت ی نیست. قضیه ۲.۴ ایجاب می کند که $\mathbb{Z}[\sqrt{-۵}]$ یک ح ا ص نیست. قسمت باقیماندهٔ این فصل، به مشخص سازی ایدآل های غیر اصلیِ $\mathbb{Z}[\sqrt{-۵}]$ اختصاص داده شده است. برای انجام این کار، به دقت، طرز عمل (Ar ۱۹۹۴) را به کار می بریم.

قضیه ۴.۹ فرض کنیم r، می نیمم مقدارِ به دست آمدهٔ قدر مطلق عناصر نا صفر ایدآل A در حلقهٔ $\mathbb{Z}[\sqrt{-5}]$ باشد. فرض کنیم $\gamma \in A$ و D قُرصِ در صفحه مختلط با مرکز $\frac{1}{n}\gamma$ و شعاع $\frac{1}{n}r$، به ازای یک عدد صحیحِ مثبتِ n باشد. در این صورت درون D شامل هیچ نقطهٔ A مگر در صورت امکان، مرکز $\frac{1}{n}\gamma$ نیست.

اثبات. فرض کنیم β یک نقطه در درون D باشد. این بدان معنی است که $|n\beta - \gamma| < r$. اینک اگر $\beta \in A$، آن گاه، $n\beta - \gamma$ یک عنصرِ A با قدر مطلقِ کوچکتر از r است. از این جا لازم می آید که $n\beta - \gamma$ برابر با صفر باشد. بدین ترتیب قضیه ثابت شده است.□

اکنون فرض کنیم A یک ایدآل ناصفر $\mathbb{Z}[\sqrt{-5}]$ و α یک عنصر A با قدر مطلقِ می نیمال r باشد، ایدآل اصلی (α) شامل تمام اعدادِ مختلط $\alpha(a + b\sqrt{-5})$ است که $a, b \in \mathbb{Z}$. بنابراین ایدآل اصلی دارای پایهٔ مشبکهٔ $(\alpha, \alpha\sqrt{-5})$ است. اگر $(\alpha) < a$، فرض کنیم β یک عنصر A است که (α) نیست. عنصر β را می توان چنان انتخاب کرد که در مستطیل با رئوس 0 و α و $\alpha\sqrt{-5}$ و $\alpha + \alpha\sqrt{-5}$ قرار گیرد. چهار قرص، هرکدام با شعاع r و با مرکز چهار راسِ مستطیل در نظر می گیریم. سه قرص دیگر، هر کدام با شعاعهای $\frac{r}{2}$ و مراکز $(\alpha\sqrt{-5}/2)$، $(\alpha + \alpha\sqrt{-5})/2$ و $\alpha + (\alpha\sqrt{-5})/2$ را در نظر می گیریم. ملاحظه می کنیم که این هفت قرص، مستطیل را می پوشانند. بنابر قضیهٔ ۴.۹، تنها نقاط داخلی این قرص‌ها، که می تواند داخل A قرار گیرد مراکز این قرص‌ها هستند. بنابراین β باید یکی از نیم مشبکهٔ $\alpha(\sqrt{-5})/2$، $(\alpha + \alpha\sqrt{-5})/2$ و $\alpha + (\alpha\sqrt{-5})/2$ باشد. اگر $(\alpha\sqrt{-5})/2 \in A$، آن گاه با ضرب در $\sqrt{-5}$ نتیجه می گیریم که $5\alpha/2 \in A$. از آن جا که $\alpha \in A$، نتیجه می گیریم که $\alpha/2 \in A$ که با چگونگی انتخاب A متناقض است. به علت این که $(\alpha\sqrt{-5})/2 \notin A$، $\alpha + \alpha\sqrt{-5}/2$ هم نمی تواند به A تعلق داشته باشد. بنابراین $(\alpha + \alpha\sqrt{-5})/2 \in A$. خلاصه این که

قضیه ۵.۹ اگر A یک ایدآل نا صفرِ حلقه $\mathbb{Z}[\sqrt{-5}]$ و α یک عنصر نا صفر A با قدر مطلق می نیمال r باشد، آن گاه، یا A باایدآل اصلی (α) با پایهٔ مشبکه $(\alpha, \alpha\sqrt{-5})$ است، یا این که A یک ایدآل اصلی نیست و دارای پایهٔ مشبکهٔ $(\alpha, (\alpha + \alpha\sqrt{-5})/2)$ است.حالت دوم تنها در زمانی که $(\alpha + \alpha\sqrt{-5})/2$ عضو A نیست رخ می دهد.

تذکر ۲.۹ بنابر قضیهٔ ۵.۹ فوق، ایدآل $(2, 1 + \sqrt{-5})$ مثالی از یک ایدآل $\mathbb{Z}[\sqrt{-5}]$ است که اصلی نیست.

فصل ۱۰

هیأت های اعداد جبری (یک)

در این فصل ملاحظه خواهیم کرد که حلقه اعداد گاوسی و حلقهٔ $\mathbb{Z}[\sqrt{-5}]$، که در فصل قبل مورد بحث قرار گرفت، به ردهٔ ویژه ای از حلقه ها تعلق دارد. دقیق تر بگوییم، این دو حلقه، مثال‌هایی از حلقهٔ اعداد صحیح در هیأت اعداد جبری است، که اکنون مورد مطالعه ماست. این دو مثال نشان می دهد که تجزیهٔ یکتا می تواند در چنین حلقه هایی وجود داشته باشد یا این که وجود نداشته باشد. به هر حال، در بخش پایانی مشاهده خواهیم کرد که در سطحِ ایدآل ها، تجزیهٔ یکتا در چنین حلقه هایی وجود دارد.

۱۰.۱ وابستگی صحیح

این بخش را با بعضی تعریف‌ها و نتایج، که تا اندازه ای، موقعیتِ کلی تری را موجب می شود، شروع می کنیم.

تعریف. فرض کنیم B یک حلقه و A یک زیر حلقهٔ B است، گوییم عنصرِ $\alpha \in B$ روی A صحیح است، هرگاه α ریشهٔ یک چند جمله ای تکین در $A[x]$ باشد. اگر تمام عناصر A روی B صحیح باشند، گویند B روی A صحیح است. گوییم عدد مختلط α یک عدد صحیح جبری است، هرگاه α رویِ $\mathbb{Z}$ صحیح باشد.

تمرین ۱.۱۰ نشان دهید که مجموعهٔ اعداد جبریِ صحیح در $\mathbb{Q}$ برابر با $\mathbb{Z}$ است. در حالت کلی اگر A یک ح ت ی باشد، نشان دهید که عناصری که در هیأت

کسرهای A رویِ A صحیح اند، دقیقاً عناصر A هستند.

تمرین ۲.۱۰ فرض کنیم $n \in \mathbb{Z} \setminus \{۰, ۱\}$ یک عدد بدون مربع باشد، به طوری که $n \equiv ۱ \pmod{۴}$. نشان دهید که $\mathbb{Z} + \mathbb{Z}(\sqrt{n})$ یک ح ت ی نیست.

قضیه ۱.۱۰ فرض کنیم B یک حلقه و A یک زیر حلقهٔ B است. در این صورت بیان‌های زیر هم ارزند.
یک) عنصر $\alpha \in B$ روی A صحیح است.
دو) حلقهٔ $A[\alpha]$ یک A–مدول متناهی–تولید شده است.
سه) حلقهٔ $A[\alpha]$ مشمول در یک زیر حلقهٔ Cی B است، به قسمی که C یک A–مدول متناهی–تولید شده است.
چهار) یک $A[\alpha]$ مدول صادقِ M وجود دارد به قسمی که به عنوان یک A–مدول متناهی–تولید شده است.

اثبات.
(یک)$\Longleftarrow$ (دو)
عنصر α در معادلهٔ $\alpha^n + a_۱\alpha^{n-۱} + \cdots + a_n = ۰$ صدق می کند که در آن a_iها عناصر A هستند. به وضوح $A[\alpha]$ با۱، α، $\alpha^۲$،$\cdots$، و $\alpha^{n-۱}$ تولید شده است.
(دو)$\Longleftarrow$ (سه)
می توانیم $A[\alpha]$ را به عنوان C اختیار کنیم.
(سه) $\Longleftarrow$ (چهار)
زیر حلقهٔ C، یک $A[\alpha]$ مدول صادق است، زیرا $aC = ۰$ ایجاب می کند که $a.۱ = ۰$. بنابراین می توانیم قرار دهیم $M = C$.
(چهار) $\Longleftarrow$ (یک)
A– مدول متناهی–تولید شدهٔ M و A–مدول همریختیِ $\phi : M \longrightarrow M$ با تعریف $\phi(\beta) = \alpha\beta$ برای هر $\beta \in M$ را در نظر می گیریم. از آن جا که M یک $A[\alpha]$ مدول است، داریم $\alpha M \subset M$. بنابراین به موجب قضیهٔ ۱.۸ به ازای a_iهایی در A، $\alpha^n + a_۱\alpha^{n-۱} + \cdots + a_n \in Ann_A(M)$ از آن جا که M صادق است، $\alpha^n + a_۱\alpha^{n-۱} + \cdots a_n = ۰$. $\square$

نتیجه ۱.۱۰ اگر $b_۱$،$b_۲$،$\cdots$،b_r عناصر B و هر کدام روی A صحیح باشد، آن گاه $A[b_۱, b_۲, \cdots, b_r]$ یک A–مدولِ متناهی–تولید شده است.

اثبات. فرض کنیم B یک حلقه و A یک زیر حلقه B باشد، به طوری که B یک A–مدول متناهی–تولید شده با مولدهای $\beta_۱$، $\beta_۲$، $\cdots$، β_t باشد. اگر M یک

B-مدول متناهی تولید شده باشد، به قسمی که $\{m_1, m_2, \cdots, m_s\}$، M را روی B تولید کند، آن گاه به سادگی ملاحظه می شود که حاصلضربهای $\beta_i m_j$، $1 \leq j \leq s$، $1 \leq i \leq t$، M را به عنوان یک A-مدول تولید می کنند و لذا M یک A-مدول متناهی تولید شده است. بدین ترتیب نتیجه از استقرا روی r به دست می آید. □

نتیجه ۲.۱۰ مجموعهٔ C متشکل از عناصری در B که روی A صحیح هستند، یک زیر حلقه B می باشد.

اثبات. اگر c_1 و c_2 دو عنصر C باشند، ان گاه بنابر نتیجهٔ فوق ، $A[c_1, c_2]$ یک A- مدولِ متناهی تولید شده است. بنابراین به موجب قسمت (سهٔ) قضیه فوق $c_1 \pm c_2$ و $c_1 c_2$ روی A صحیح اند. □

نتیجه ۳.۱۰ اگر $A \subset B \subset C$ حلقه باشند، به قسمی که B روی A و C روی B صحیح باشد، آن گاه C روی A صحیح است.

اثبات. فرض کنیم $c \in C$، در این صورت $c^n + b_1 c^{n-1} + \cdots + b_n = 0$، که b_iها در B هستند. فرض کنیم $B_1 = A[b_1, b_2, \cdots, b_n]$. در این صورت بنابه نتیجه ۱.۱.۱۰ B_1 یک A-مدول متناهی تولید شده است. همچنین $B_1[c]$، به علت این که c روی B صحیح است، یک B_1-مدول متناهی—تولید شده است. بنابراین $B_1[c]$ یک A-مدول متناهی—تولید شده می باشد و از این رو c روی A صحیح است.□

تعریف. مجموعهٔ C متشکل از عناصری در B که روی A صحیح هستند بستار صحیح A در B نامیده می شود. از نتیجهٔ ۲.۱.۱۰ می دانیم که C یک حلقه است. اگر $C = A$ گویند A به طور صحیح در B بسته است اگر حوزه صحیح A به طور صحیح در هیأت خارج قسمت‌های خود، F، به طور صحیح بسته باشد، در این صورت فقط گویند A به طور صحیح بسته است.

تذکر ۱.۱۰ با اصطلاحات فوق، تمرین ۲.۱۰ مبین آن است که هر ح ت ی به طور صحیح بسته است.

۲.۱۰ اعداد صحیح در هیأت‌های اعداد

در اینجا قلمرو توسیع‌های صحیحِ حلقه های کلی را ترک کرده و بحث مربوط به حالت‌های خاص هیأت اعداد را ادامه می دهیم. این کار را با بعضی پیش نیازها برای هیأت اعداد شروع می کنیم.

تعریف. مقصود از یک هیأت جبری اعداد، یک زیر هیأت Kی $C*$ است به قسمی که K توسیع متناهیِ $\mathbb{Q}$ باشد. عدد صحیح $[K:Q]$ درجه K روی $\mathbb{Q}$ نامیده می شود.

تذکر ۲.۱۰ از تمرین ۱۰.٦ و قضیه ۳.٦ نتیجه می گیریم که برای هر هیأت اعداد جبریِ K، عنصر $\theta \in K$ وجود دارد که $K = \mathbb{Q}(\theta)$.

تذکر ۳.۱۰ فرض کنیم K یک هیأت اعداد جبری با درجهٔ n باشد. بنابر تذکر ۲.۱۰ و تمرین ۲.٦، به ازای یک $\theta \in K$، $K = \mathbb{Q}(\theta)$ و n درجهٔ f، چند جمله ای می نیمال θ، است. اگر $\theta = \theta_1$،θ_2،$\cdots$،θ_n تمامِ و بسته های f باشند، در این صورت، برای هر θ_i، $(i = 1, 2, \cdots, n)$ یک یکریختی σ_i از $K\mathbb{Q}(\theta)$ به توی $\mathbb{Q}(\theta_i) \subset C*$ وجود دارد که با $\sigma_i(\sum_{j=0}^{m} b_j(\theta^i) = \sum_{j=0}^{m} b_j(\theta_i^j)$. تعریف می شود، به وضوح σها متمایزند و تنها یکریختیهای K به توی $C*$ هستند.

تعریف. هیأت‌های $K^(i) = \sigma_i(K)$. $i = 1, 2, \cdots, n$، در تذکر فوق مزدوج‌های K نامیده می شوند. اگر $K(i) \subset \mathbb{R}$ آن را یک مزدوج حقیقی K می نامیم، در غیر این صورت یک مزدوج مختلط نامیده میشود. مزدوج‌های مختلط به حالت زوج زوج وجود دارند. r_1 و $2r_2$ به ترتیب تعدادِ مزدوج‌های حقیقی و مختلطِ K را نشان می دهد. همچنین $\sigma_i(\alpha)$ را با $\alpha^{(i)}$ نشان می دهیم.

قضیه ۲.۱۰ فرض کنیم K یک هیأت اعداد جبری و w_1،w_2،$\cdots$،w_n یک پایهٔ K روی $\mathbb{Q}$ باشد. با نماد گذاری فوق اگر Ω ماتریس $[w_j^{(i)}]_{i,j}$ را نشان دهد، آن گاه Ω ناتکین است.

اثبات. فرض کنیم $K = \mathbb{Q}(\theta)$ باشد که در تذکر ۳.۱۰ آمده است. فرض کنیم A ماتریس متناظرِ Ω برای پایهٔ ۱، θ،θ^2،$\cdots$،θ^{n-1} باشد. در این صورت دترمینان A، یک دترمینان واندرموند است و برابر است با $\prod_{1 \leq i<j \leq n}(\theta^{(i)} - \theta^{(j)})$. اگر B ماتریسی باشد که (w_i) را بر حسبِ پایهٔ $1, \theta, \cdots, \theta^{n-1}$ بیان می کند، آن گاه $\Omega = BA$. اینک به علت آن که B ماتریسی است که دارای وارون با درآیه ها در $\mathbb{Q}$ می باشد، نتیجه حاصل می شود.□

اکنون به مطالعهٔ حلقهٔ اعداد صحیح جبری در یک هیأت جبری اعداد می پردازیم. اگر K یک هیأت اعداد جبری باشد، حلقهٔ اعداد صحیح جبری در K با O_K نشان داده می شود.

تذکر ۴.۱۰ برای هر عدد جبری α، عدد صحیح $0 \neq m \in \mathbb{Z}$ وجود دارد که $m\alpha$ یک عدد صحیح جبری است زیرا اگر $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ که a_iها

در $\mathbb{Z}$ هستند، آن گاه $(a_n\alpha)^n + a_{n-۱}(a_n\alpha)^{n-۱} + \cdots + a_۰ a_n^{n-۱} = ۰$ که نتیجه می دهد $a_n\alpha$ یک عدد صحیح جبری است.

تعریف. فرض کنیم K یک هیأت اعداد جبری و $w_۱$،$w_۲$،$\cdots$،w_n یک پایهٔ K روی $\mathbb{Q}$ باشد. اگر K به عنوان یک فضای برداری روی $\mathbb{Q}$ در نظر گرفته شود. تابع $x \longrightarrow \alpha x$، برای هر $\alpha \in K$ یک تابع خطی است. اثر α که با $Tr(\alpha)$، $Tr_K(\alpha)$ یا $Tr_{K/Q}(\alpha)$ نشان داده می شود اثر این تابع خطی است. به طور مشابه نُرمِ α که با $N(\alpha)$،$N_K(\alpha)$ یا $N_{K/Q}(\alpha)$ نشان داده می شود، دترمینان این تابع خطی است. به وضوح، $Tr_K(\alpha)$ و $N_K(\alpha)$ در $\mathbb{Q}$ هستند.

تذکر ۵.۱۰ اگر $\alpha \in K$، برای $j = ۱, ۲, \cdots, n$، فرض کنیم $\alpha w_j = \sum_{i=۱}^n a_{ij} w_i$ و $A = [a_{ij}]$ با نمادهایی که پیش از قضیه ۲.۱۰ معرفی شد،

$$(\alpha w_j)^(k) = \alpha^{(k)} w_j^{(k)} = \sum_{i=۱}^n a_{ij} w_i^{(k)}$$

و بنابراین اگر ماتریس قطریِ $(\alpha^{(i)}\delta_{ij})$ را با $A_۰$ نشان دهیم، داریم $A_۰\Omega = \Omega A$. بنابر قضیهٔ ۲.۱۰، Ω دارای وارونِ $\Omega^{-۱}$ است و از این رو $A_۰ = \Omega A \Omega^{-۱}$. بنابراین $N_K(\alpha) = detA = det(\Omega A \Omega^{-۱}) = detA_۰ = \alpha^{(۱)} \cdots \alpha^{(n)}$ به طور مشابه $Tr_K(\alpha) = Tr_K(\alpha) = Tr(\Omega A \Omega^{-۱} = TrA_۰ = \alpha^(۱) + \cdots + \alpha^n$. بدین ترتیب تعریف دیگری از $Tr_K(\alpha)$ و $N_K(\alpha)$ به دست می آید.

تذکر ۶.۱۰ اگر A و B به ترتیب ماتریس‌هایی برای توابع خطی متناظر با $\alpha, \beta \in K$ ، آن گاه $A+B$ و AB، به ترتیب ماتریس‌های متناظر با $\alpha + \beta$ و $\alpha\beta$ هستند. بنابراین $A \longrightarrow \alpha$ یک همریختی K به توی فضای $n \times n$ ماتریسها روی $\mathbb{Q}$ است. این همریختی نمایش منظم K متناظر با پایهٔ $w_۱$،$w_۲$،$\cdots$،w_n است. همچنین نتیجه می گیریم که اثر مجموع دو عنصر K مجموع اثرهای آن عناصر است. همچنین نرم حاصلضرب دو عنصر K، حاصلضرب نرم آن عناصر است.

تذکر ۷.۱۰ فرض کنیم K یک هیأت اعداد جبری از درجهٔ n و α یک عدد صحیح جبری در K باشد اگر α از درجه m $(m \leq n)$ روی $\mathbb{Q}$ باشد، آن گاه $۱, \alpha, \cdots, \alpha^{m-۱}$ یک $\mathbb{Q}$–پایه برای $\mathbb{Q}(\alpha)$ است. فرض کنیم A ماتریس $m \times m$ با درآیه ها در $\mathbb{Q}$ باشد که متناظر است با نمایش منظم $\mathbb{Q}(\alpha)$ نسبت به پایهٔ ۱،α،$\cdots$،$\alpha^{m-۱}$. فرض کنیم $\beta_۱$،$\beta_۲$،$\cdots$،β_l پایه ای برای K به عنوان یک فضای برداری روی $\mathbb{Q}(\alpha)$ است. در این صورت $n = lm$ و

$$\beta_۱, \beta_۱\alpha, \cdots, \beta_۱\alpha^{m-۱}, \beta_۲, \beta_۲\alpha, \cdots, \beta_۲\alpha^{m-۱}, \cdots, \beta_l, \beta_l\alpha, \cdots, \beta_l\alpha^{m-۱}$$

یک پایه برای K روی هیأت $\mathbb{Q}$ تشکیل می دهند. فرض کنیم A ماتریسی باشد که متناظر با α در نمایش منظم K نسبت به این پایه است. در این صورت

$$A_1 = \begin{vmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ 0 & 0 & \cdots & A \end{vmatrix}$$

از اینجا نتیجه می گیریم که $TrA_1 = lTr(A)$. از آنجا که تمام عناصر A در $\mathbb{Z}$ هستند، اگر $x^m + a_{m-1}x^{m-1} + \cdots + a_0$ چند جمله‌ای می‌نیمال α باشد، نتیجه می گیریم که $Tr(A)$ و $Tr(A_1) = lTr(A) = -l - a_{m-1}$ اعدادی صحیح اند. به طور مشابه $N_K(\alpha) = detA_1 = (detA)^l \in \mathbb{Z}$.

قضیه ۳.۱۰ فرم دو خطی $B(x,y) := Tr_K(xy)$ برای $x, y \in K$ ناتبهگون است.

اثبات. فرض کنیم $x \neq 0$ در K باشد. در این صورت با ثابت نگه داشتن x، $Tr_K(xy)$ متحداً در y صفرنیست، زیرا برای $y = x^{-1}$، $Tr_K(xy) = Tr_K(1) = n$. به طور مشابه برای $y \neq 0$ در K، $Tr_K(xy)$ متحداً در x برابر با صفر نیست.

نتیجه زیر از تمرین ۶.۸ به دست می آید.

نتیجه ۴.۱۰ برای هر $\mathbb{Q}-$ پایهٔ w_1،w_2،$\cdots$،w_n در K، یک پایهٔ w'_1،w'_2،$\cdots$،w'_n وجود دارد به قسمی که $Tr_K(w_iw'_j) = \delta_{ij}$، $1 \leq i, j \leq n$.

قضیه ۴.۱۰ فرض کنیم K یک هیأت اعداد جبری از درجهٔ n و $\mathbf{O}_K$ حلقهٔ اعداد صحیح در K باشد. در این صورت یک $\mathbb{Q}$ پایه w_1،w_2،$\cdots$،w_n وجود دارد که w_iها در $\mathbf{O}_K$ هستند و $\mathbf{O}_K = Zw_1 + Zw_2 + \cdots + Zw_n$.

اثبات. از آنجا که برای هر عنصر α در K، $m \neq 0$ وجود دارد به طوری که $m\alpha \in \mathbf{O}_K$، یک $\mathbb{Q}$ پایه v_1،$\cdots$،v_n در K متشکل از عناصر $\mathbb{Q}_K$ وجود دارد. فرض کنیم v'_1،v'_2،$\cdots$،v'_n یک پایه برای K باشد به قسمی که

$$Tr_K(v_iv'_j) = \delta_{ij} \qquad , \ 1 \leq i, j < n \qquad\qquad (1.10)$$

برای هر $z \in \mathbf{O}_K$، $z = \sum_{i=1}^{n} a_iv'_i$ که a_iها به $\mathbb{Q}$ تعلق دارند. اینک برای $1 \leq i \leq n$، $zv_i \in \mathbb{Q}_K$. بنابراین $Tr_K(zv_i) \in \mathbb{Z}$. بنابر (۱.۱۰)، $Tr_K(zv_i) = a_i$ و لذا $\mathbb{Q}_K \subset \mathbb{Z}v'_1 + \cdots + \mathbb{Z}'v'_n$، بنابراین w_1،w_2،$\cdots$،$\cdots$،w_n $(m \leq n)$ وجود دارد به طوری که $\mathbf{O}_K = zw_1 + \cdots + zw_m$، لیکن اگر $m < n$، آن گاه $\mathbb{Q}-$ زیر فضای تولید شده یاw_1،w_2،$\cdots$،w_n همان K خواهد بودکه متناقض با این فرض است که بُعدِ K روی $\mathbb{Q}$ برابر با n است. بنابراین $m = n$، همچنین w_1،w_2،$\cdots$،w_n باید $\mathbb{Q}$ مستقل باشند و اثبات تمام است.□

تعریف. عناصر w_1،w_2،$\cdots$،w_n در قضیهٔ فوق یک پایه صحیحِ K نامیده می شود.

در تمرین ۷.آ ۹ ملاحظه کردیم که هر ایدآل ناصفرِ حلقهٔ اعداد صحیحِ گاوسی شامل یک عدد صحیح ناصفر است. تذکر زیر، بیان کلیِ این نتیجه است.

تذکر ۸.۱۰ فرض کنیم K یک هیأت اعداد جبری و A یک ایدآل دلخواهِ $\mathbf{O}_K$ باشد، ادعا می کنیم که $A \cap \mathbb{Z} = \{0\}$. زیرا اگر $\alpha \neq 0$ یک عدد صحیح جبری در A باشد، آن گاه به ازای a_iها در $\mathbb{Z}$، $\alpha^r + a_{r-1}\alpha^{r-1} + \cdots + a_0 = 0$، به طوری که $a_0 \neq 0$، در این صورت به وضوح $a_0 = -\alpha(a_1 + \cdots + \alpha^{r-1}) \in A$. همچنین از تذکر ۴.۱۰ می دانیم که برای هر $\alpha \in K$، $m \neq 0$ در $\mathbb{Z}$ وجود دارد که $m\alpha \in \mathbf{O}_K$، از آنجا که A دارایِ عنصر $0 \neq m_1 \in \mathbb{Z}$ می باشد، $mm_1\alpha \in A$. بنابراین برای هر $\alpha \in K$، $l \neq 0$ در $\mathbb{Z}$ وجود دارد که $l\alpha \in A$.

تذکر ۹.۱۰ فرض کنیم A یک ایدآل ناصفر $\mathbf{O}_K$ است. اگر w_1،w_2،$\cdots$،w_n همان هایی باشند که در قضیهٔ ۴.۱۰ آمده است، آن گاه $A \subset \mathbf{O}_K = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n$، بنابراین به لحاظ این که حلقهٔ $\mathbb{Z}$ نویتری است، به موجب نتیجه ۲.۴.۸ و قضیه ۸. ۳عناصر v_1،v_2،$\cdots$،v_m $(m \leq n)$ در A وجود دارد که $A = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$. از تذکر ۸.۱۰ نتیجه می شود که v_1،v_2،$\cdots$،v_m، K را روی $\mathbb{Q}$ تولید می کنند و لذا باید داشته باشیم $m = n$. گوییم v_iها یک پایه صحیح برای A تشکیل می دهند. علاوه بر آن می توان v_iها را چنان انتخاب کرد که $v_i = \sum_{j \geq i} p_{ij} w_j$ ، $p_{ij} \in \mathbb{Z}$.

تذکر ۱۰.۱۰ اگر A یک ایدآل ناصفر $\mathbf{O}_K$ باشد، بنابر تذکر ۸.۱۰ ، $0 \neq a \in \mathbb{Z}$ وجود دارد که $\alpha\mathbf{O}_K \subset A \subset \mathbf{O}_K$، اینک اگر $\mathbb{O}_K = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n$، آن گاه $a\mathbb{Q}_K = \mathbb{Z}aw_1 + \cdots + \mathbb{Z}aw_n$، به طوری که تعداد عناصر $\mathbf{O}_K/a\mathbf{O}_k$ برابر با a^K است. بنابراین $\mathbf{O}_K/A$ نیز متناهی است. تعداد عناصر $\mathbf{O}_K/A$ نرم A نامیده شده و با $N(A)$ نمایش داده می شود. اگر $A = \{0\}$، قرار می دهیم $N(A) = 0$.

تذکر ۱۱.۱۰ اگر $\wp$ یک ایدآل اول $\mathbf{O}_K$ باشد، آن گاه از تذکر ۸.۱۰ نتیجه می‌گیریم که $\wp$ شامل یک عددِ اول $p > 0$ در $\mathbb{Z}$ است. اکنون اگر p و q دو عدد اول متمایز در $\wp$ باشند، می توانیم اعداد صحیح x و y در $\mathbb{Z}$ را چنان بیابیم که $xp + yq = 1$ که نتیجه می دهد $\wp = \mathbf{O}$، که یک تناقض است. بنابراین $\wp$ شامل دقیقاً یک عدد اول $p > 0$ در $\mathbb{Z}$ است. به خاطر تمیزِ بین ایدآل های اول در $\mathbf{O}_K$، عدد اول $p \in \mathbb{Z}$، عدد اولِ گویا نامیده می شود.

قضیه ۵.۱۰ حلقهٔ اعداد صحیحِ $\mathbf{O}_K$ در یک هیأت جبری اعداد K دارای ویژگی‌های زیر است.

یک) هر ایدآل ناصفر اول $\mathbf{O}_K$ ماکسیمال است.
دو) $\mathbf{O}_K$ به طور صحیح بسته است.
سه) $\mathbf{O}_K$ نویتری است.

اثبات. فرض کنیم K یک هیأت جبری اعداد با درجهٔ n روی $\mathbb{Q}$ و $\mathbf{O}_K$ حلقهٔ اعداد صحیح در K باشد. فرض کنیم p یک ایدآل اول $\mathbf{O}_K$است، در این صورت صورت $\mathbf{O}_K/\wp$ یک حوزهٔ صحیح متناهی و لذا یک هیأت است. این نشان می دهد که هر ایدآل ناصفرِ $\mathbf{O}_K$ ماکسیمال می باشد. از طرفی از نتیجه ۳.۱.۱۰ نتیجه می‌گیریم که بستار صحیح $\mathbf{O}_K$ در K همان $\mathbf{O}_K$ است. سرانجام ملاحظه می کنیم که اگر A و B ایدآلهای $\mathbf{O}_K$ باشند، $A \subset B$، و $A \neq B$ داریم $N(A) > N(B)$. بنابراین اگر $A_1 \subset A_2 \subset \cdots \subset A_n \subset \cdots$ یک دنبالهٔ افزایشی ایدآل هادر $\mathbf{O}_K$ باشد، به ازای یک عدد صحیح مثبت $m > m_0$ ، $A_m = A_{m+1}$، یعنی $\mathbf{O}_K$ نویتری است.□

مجموعه تمرینهای پ

پ . ۱ فرض کنید a، b و c اعداد صحیح معمولی هستند که دارای عامل مشترکی نیستند و $a^۲ = b^۲ + c^۲$. اگر Π یک عدد اول گاوسی باشد که $a+bi$ را در حلقه اعداد گاوسی عاد می کند، آن گاه نشان دهید، توان Π که در تجزیه یکتای $a+ib$ ظاهر می شود، زوج است.

پ . ۲ تمام جوابهای صحیح x، y و z در معادله $x^۲ + y^۲ = z^۲$ را که دارای عامل مشترک نیستند بیابید.

پ . ۳ تمام اعداد اول p را بیابید که معادلهٔ $x^۲ + ۲y^۲ = p$ دارای جواب صحیح باشد.

پ . ۴ فرض کنید w عدد $(\frac{-۱+\sqrt{-۳}}{۲})$ و حوزهٔ $\mathbb{Z}[w]$ رانشان دهد در این صورت نشان دهید:

(آ) D با تابعِ اندازهٔ $N(a+b(N)) = a^۲ + ab + b^۲$ یک حوزهٔ اقلیدسی است.

(ب) عنصر $\alpha \in D$ یکه است. اگر و تنها اگر $N(\alpha) = ۱$.این یکه‌ها عبارتند از ± ۱، $\pm w$، $\pm w^۲$.

(پ) اگر Π در D اول باشد، آن گاه عدد اول گویای p وجود دارد که $N(\Pi) = p$ یا $N(p) = ۲p^۲$. در حالت اول Π در D اول است.

(ت) اگر p یک عدد گویای اول باشد، به قسمی که $q \equiv ۲ \pmod{۳}$ آن گاه q در D اول است. اگر q عدد گویای اول باشد و $q \equiv ۱ \pmod{۳}$، آن گاه $q = \Pi\overline{\Pi}$ که Π در D اول است.

(ث) عنصر $۱ - w$ در D اول است و $۳ = -w^۲(۱-w)^۲$.

فصل ۱۱

حوزه های ددکنید

در این فصل، بعضی خواص بنیادیِ حوزه های ددکنید را خواهیم آموخت. گردآیه حوزه های ددکنید، برای مثال، شامل حوزه های ایدآل های اصلی است. حلقهٔ اعداد صحیح در یک هیأت اعداد، که موضوع اصلی موردِ علاقهٔ ماست، مثال هایِ نابدیهیِ حوزه های ددکنید را فراهم می آورد.

۱۱.۱ ایدآل های کسری

فرض کنیم R یک حوزه صحیح و K هیأت خارجِ قسمتهای آن باشد.

تعریف. مقصود از یک ایدآل کسری R، R–مدول ناصفر A است که مشمول در K باشد، به قسمی که به ازای یک $m \neq 0$ در R، $mA \subset R$.

تذکر ۱.۱۱ هر ایدآل R به طور بدیهی یک ایدآل کسری است. آن را یک ایدآل صحیح می نامیم همچنین هر ایدآل کسری A، به وضوح، به شکل $\alpha^{-1}B$ است، که در آن $0 \neq \alpha \in R$ و B یک ایدآل صحیح است.

تعریف. برای ایدآل کسری Aی R مجموعهٔ

$$\{x \in K : xA \subset R\}$$

را با A' نمایش می دهیم.

تمرین ۱.۱۱ نشان دهید که برای ایدآل کسری Aی R، مجموعهٔ A' تعریف شده در فوق نیز یک ایدآل کسری است.

اگر M یک R–مدول و A یک ایدآل R باشد، پیشتر AM را تعریف کردیم. حاصلضرب دو ایدآل کسری A و B نیز به همین روش تعریف می شود. یعنی مجموعهٔ تمام مجموعهای متناهیِ $a_1b_1 + a_2b_2 + \cdots + a_rb_r$ است، که $a_i \in A$ و $b_i \in B$ به سادگی دیده می شود که AB نیز یک ایدآل کسری R است.

اثبات. برای ایدآل کسری Aی R، به وضوح $AA' \subset R$. اگر برای ایدآل کسری A برابریِ $AA' = R$ برقرار باشد، آن گاه A وارونپذیر نامیده می شود و می نویسیم $A' = A^{-1}$.

برای $0 \neq a \in R$، aR به وضوح یک ایدآل کسری است. چنین ایدآل کسری را ایدآل کسری اصلی می نامیم.

تذکر ۲.۱۱ می توان ملاحظه کرد که هر ایدآل کسری اصلی، یک ایدآل وارونپذیر است.

تمرین ۲.۱۱ نشان دهید که مجموعهٔ تمام ایدآل های کسری و وارونپذیر R، با عمل ضرب تشکیل یک گروه می دهند.

تعریف. اگر R یک حوزه صحیح باشد، به قسمی که هر ایدآل کسری آن وارونپذیر باشد، آن را یک حوزه ددکنید می نامند.

تذکر ۳.۱۱ از تذکر ۳.۱۱ و ۲.۱۱ چنین نتیجه می شود که هر حوزهٔ ایدآل های اصلی یک حوزه ددکنید است.

۱۱.۲ خواص حوزه های دد کنید

در سه قضیه ای که خواهد آمد، برخی خواص با اهمیت حوزه های ددکنید را ثابت خواهیم کرد.

قضیه ۱.۱۱ هر حوزه ددکنید، نویتری است.

اثبات. فرض کنیم A یک ایدآل نا صفرِ حوزه ددکنید R باشد،از آنجا که A وارونپذیر است، عناصر $a_i \in A$ و $b_i \in A^{-1}$، $i = 1, 2, , \cdots, n$، وجود دارند که $a_1b_1 + a_2b_2 + \cdots + a_nb_n = 1$. اینک اگر α یک عنصر A باشد، داریم $\alpha = (\alpha b_1)a_1 + \cdots (\alpha b_n)a_n$. برای هر $i = 1, 2, \cdots, n$. $\alpha b_i \in R$ و لذا a_iها A را تولید می کنند. بنابراین R نویتری است.

قضیه ۲.۱۱ در هر حوزهٔ ددکنید، هر ایدآل نا صفرِ اول ماکسیمال است.

اثبات. فرض کنیم P یک ایدآل نا صفر و اولِ حوزهٔ ددکنید R باشد. فرض کنیم M یک ایدآل ماکسیمال شامل P است. اینک $PM^{-1} \subset MM^{-1} = R$. این برابری نشان می دهد که PM^{-1} یک ایدآل R است. از آنجا که، $(PM^{-1})M = P$ و P یک ایدآل اول است، داریم $PM^{-1} \subset P$، یا این که $M \subset P$. اگر $PM^{-1} \subset P$ ، آن گاه $M^{-1} \subset P^{-1}P = R$. به علت این که $R \subset M^{-1}$، بنابه تعریف $M^{-1} = R$ و لذا $M = R$، که یک تناقض است. بنابراین $M = P$ و این برابری قضیه را به اثبات می رساند.□

قضیه ۳.۱۱ هر حوزه ددکنید، به طور صحیح بسته است. **اثبات.** فرض کنیم R یک حوزهٔ ددکنید و K هیأت خارج قسمتهای آن باشد. فرض کنیم α یک عنصر K است، به قسمی که α روی K صحیح می باشد. در این صورت بنابر قضیهٔ ۱.۱۰، $R[\alpha]$، یک R–مدول متناهی–تولید شده است. فرض کنیم α_1،α_2،$\cdots$،α_n R–مدولِ $R[\alpha]$ را تولید کنند. به علت این که K هیأت خارج قسمتهای R است. برای $i = 1, 2, \cdots, n$، $0 \neq b \in R$ وجود دارد که $ba_i \in R$. از این جا معلوم می شود که $bR[\alpha] \subset R$. بنابراین $R[\alpha]$ یک ایدآل کسری است. اینک

$$R[\alpha] = RR[\alpha] = R[\alpha]^{-1}R[\alpha]R[\alpha] = R[\alpha]^{-1}R[\alpha] = R.$$

بنابراین $\alpha \in R$ و اثبات تمام است.□

چند قضیهٔ بعد. این واقعیت را بر ما معلوم می سازد، که خواص حوزه های ددکنید، بیان شده در قضیه های ۱.۱۱ ،۳.۱۱ ، در واقع مشخص کنندهٔ حوزه های ددکنید هستند.(تذکر ۴.۱۱ را ببینید).

قضیه ۴.۱۱ فرض کنیم R یک حوزهٔ نویتری است. در این صورت برای هر ایدآل نا صفرِ اولِ مفروضِ R مانند A می توان ایدآلهای اولِ P_1،P_2،$\cdots$،P_m را در R یافت به طوری که

$$P_1P_2\cdots P_m \subset A \subset P_1 \cap P_2 \cdots P_m$$

اثبات. در صورت امکان، فرض کنیم یک ایدآل نا صفرِ سرهٔ R وجود داشته باشد که دارای ویژگی بیان شده نباشد. فرض کنیم I در مجموعهٔ چنین ایدآل‌هایی عنصر ماکسیمال باشد. به وضوح I نمی تواند اول باشد، بنابراین عناصر a و b وجود دارند که

$ab \in I$، اما $a,b \notin I$. فرض کنیم $A = I + aR$ و $B = I + bR$. از آنجا که $AB \subset I$ ، برابریِ $A = R$ چنین نتیجه می دهد که $B = I$. این برابری به علت این که $b \notin I$ نمی تواند برقرار باشد، بنابراین $A \neq R$. به طورِ مشابه $B \neq R$. بنابراین A و B در خاصیت مذکور قضیه صدق می کنند. از آنجا که بنابر نوع ساخت، $AB \subset I \subset A \cap B$، I نیز دارای همان ویژگی است، که یک تناقض است.□

قضیه ۵.۱۱ فرض کنیم حوزهٔ صحیح R در شرطهای زیر صدق کند
یک) Rنویتری است.
دو)R به طور صحیح بسته است.
سه) هر ایدآل ناصفرِ اول R ماکسیمال است.
آن گاه هر ایدآل ناصفرِ اولِ R واروپذیر است.

اثبات. فرض کنیم P یک ایدآل نا صفرِ اول R و $\circ \neq \alpha \in P$. بنابر قضیهٔ ۴.۱۱، می توان کوچکترین عدد صحیح مثبت m را یافت به قسمی که ایدآل اصلی aR شامل حاصلضربِ m ایدآل اول $P_۱P_۲ \cdots P_m$ باشد. به علت این که P یک ایدآل اول است، بنابر شرط (سه) P برابر با یکی از ایدآلهای $P_۱$،$P_۲$،$\cdots$،P_m می باشد. بدون از دست دادن کلیت، فرض کنیم $P = P_۱$، بنابر فرض می نیمال بودن m، حاصلضرب $P_۲ \cdots P_m$ مشمول در aR نیست. فرض کنیم $b \in P_۲ \cdots P_m \setminus aR$، پس $ba^{-۱} \in R$. اینک $bP \subset PP_۲ \cdots P_m \subset aR$، که نتیجه می دهد $ba^{-۱}P \subset R$. لذا $ba^{-۱} \in P' \setminus R$. از این رو لازم است که $R < P'$.

فرض کنیم x یک عنصرِ ناصفرِ P است. با توجه به بند قبل، عنصرِ $y \in P' \setminus R$ وجود دارد. اینک $P = RP \subset P'P \subset R$. بنابر شرط (سه) یکی از دو برابریِ $P'P = P$ یا $P'P = R$ برقرار است. اگر $P'P = P$ آن گاه به ازای هر عدد صحیح مثبت n، $(P')^nP = P$، لذا برای تمامِ اعداد صحیح $n \geq ۱$، $xy^n \in P$، از این رو $xR[y] \subset R$ و $xR[y]$ یک ایدآل R است که بنابر شرط (یک) متناهی—تولید شده است. فرض کنیم $a_۱$،$a_۲$،$\cdots$،a_m، $xR[y]$ را به عنوان یک R−مدول تولید کند. در این صورت $a_۱x^{-۱}, \cdots, a_mx^{-۱}$، $R[y]$ را به عنوان R−مدول تولید می کند. بنابر قضیهٔ ۱.۱۰، y روی R صحیح است و بنابر شرط (دو) $y \in R$ که متناقض با فرض انتخاب y است. بنابراین $P'P = R$ و اثبات تمام است.

قضیه ۶.۱۱ فرض کنیم R یک حوزهٔ صحیح است که در شرطهای (یک)، (دو) و (سه) مذکور در قضیه قبل صدق می کند. در این صورت هر ایدآل سرهٔ R (یعنی ایدآلهایی غیر از (۰) یا R) را می توان به صورت حاصلضرب ایدآلهای اولی در R که صرف نظر از ترتیب، به طور یکتا مشخص می شوند نوشت.

اثبات. ابتدا وجود تجزیه را ثابت می کنیم. فرض کنیم S مجموعهٔ تمام ایدآلهای سرهٔ R باشد که نمی توان آنها را به ایدآلهای اول تجزیه کرد. در صورت امکان، فرض کنیم $S \neq \emptyset$. اینک هر عنصرِ S شامل حاصلضربی از ایدآلهای اول است. میتوانیم عنصرِ Aی S را به قسمی انتخاب کنیم که شامل حاصلضرب $P_1P_2\cdots P_m$ از ایدآلهای اول بوده و m می نیمال باشد. بنابر شرط (سه)، $m \neq 1$، زیرا A نمی تواند اول باشد. ایدآل اول $\wp$ $(\wp \neq A)$ وجود دارد به طوری که $A \supset \rho$. در این صورت $\wp$ باید برابر با یکی از P_iها، مثلاً P_1 باشد. به موجب قضیه قبل یک ایدآل کسری $\wp^{-1}$ وجود دارد به طوری که $R = \wp\wp^{-1}$. حال $P_2\cdots P_m \subset A\wp^{-1} \subset \wp\wp^{-1} = R$. به علت می نیمال بودن m، برای ایدآلهای اولِ $\wp_1،\wp_2،\cdots،\wp_r$ داریم $A\wp^{-1} = \wp_1\wp_2\cdots\wp_r$، که در این صورت $A = \wp_1\wp_2\cdots\wp_r$، که متناقض با فرض انتخاب A است.

اکنون به اثباتِ یکتایی تجزیه می پردازیم. اگر ممکن باشد، فرض کنیم ایدآل سرهٔ $A \subset R$ دارای دو تجزیهٔ

$$A = P_1P_2\cdots P_r = \wp_1\wp_2\cdots\wp_n \qquad (1.11)$$

باشد، که $P_1P_2,\cdots,P_r$، $\wp_1,\wp_2,\cdots,\wp_n$ ایدآلهای اولند. از آنجا که $\wp_1$ اول است، شامل یکی از ایدآلهای $P_1P_2,\cdots,P_i$ مثلاً P_1 است و علت آن که P_1 ماکسیمال است، $P_1 = \wp_1$، طرفین برابری (۱.۱۱) را در $P_1^{-1} = \wp_1^{-1}$ ضرب می کنیم، داریم $P_2\cdots P_r = \wp_2\cdots\wp_s$. استدلال راتکرار می کنیم، پس از تعدادی متناهی مرحله چنین نتیجه می شود که $r = s$ و تجزیه با تقریب مرتبه یکتاست.□

نتیجه ۱.۱۱ .۱ هر ایدآل نا صفر A را می توان به طور یکتا به شکل $P_1P_2\cdots P_r\wp_1^{-1}\wp_2^{-1}\cdots\wp_n^{-1}$ که در آن P_iها از $\wp_i$ها متمایزند نوشت.

اثبات. عنصرِ $0 \neq c \in R$ وجود دارد، به طوری که $cA = B \subset R$. به علت این که cR و B را می توان به صورت حاصلضرب ایدآلهای R که به طور یکتا مشخص می شوند نوشت، نتیجه حاصل می شود.□

تذکر ۴.۱۱ از قضیه های ۱.۱۱، ۲.۱۱،۳.۱۱،۵.۱۱ و نتیجهٔ ۶.۱۱ چنین نتیجه می گیریم که حوزه صحیح R یک حوزهٔ ددکنید است، اگر و تنها اگر در سه شرط قضیهٔ ۵.۱۱ صدق کند. بنابراین قضیه ۵.۱۰ مبین آن است که حلقهٔ اعداد صحیح در یک هیأت اعداد جبری یک حوزهٔ ددکنید است.

تذکر ۵.۱۱ بزرگترین مقسوم علیه مشترک (A,B)ی دو ایدآل A و B در حوزهٔ ددکنید R برابر با $\wp_1^{c_1}\cdots\wp_s^{c_s}$ تعریف می شود که $\wp_i$ها ایدآلهای ظاهر شده در تجزیهٔ

A یا B و $\wp_i^{e_i}$ها می نیمم توان $\wp_i$ $(C_i \geq \circ)$ که در تجزیه A و B ظاهر می شوند. اگر A و B دو ایدآل R باشند، آن گاه $A \subset B$، اگر و تنها اگر برای ایدآلی مانند C، $A = BC$. علت این است که اگر $A \subset B$، آن گاه $C = AB^{-1} \subset R$، به عکس اگر به ازای یک ایدآل C، $A = BC$، آن گاه $A \subset B$. بنابراین بزرگترین مقسوم علیه مشترک A و B، به وضوح کوچکترین ایدآلی است که شامل هم A و هم B است. این ایدآل همان $A + B$ است.

اگر برای دو ایدآل A و Bی حوزهٔ ددکنید R، بزرگترین مقسوم علیه مشترک A و B برابر با R باشد، یعنی اگر ایدآل اولی وجود نداشته باشد که هم A و هم B را عاد کند، گویند A و B نسبت به هم اولند.

اگر I یک ایدآل حلقهٔ R باشد، $a \equiv b \pmod I$، به معنی آن است که $a - b \in I$.

تمرین ۳.۱۱ فرض کنید R یک حوزهٔ ددکنید است. فرض کنید P یک ایدآل اول R باشد. در این صورت نشان دهید که برای هر $b \in R$، $a \in R \setminus P$ و هر عدد صحیح مثبت n، معادلهٔ همنهشتی $ax \equiv b \pmod{P^n}$ دارای یک جواب است.

تمرین بعد تعمیم طبیعی قضیهٔ باقیمانده چینی برای حوزه های دد کنید است.

تمرین ۴.۱۱ اگر $I_1, I_2, \cdots, I_n$ ایدآلهای دو به دو نسبت به هم اول یک حوزهٔ ددکنید بوده و $a_1, a_2, \cdots, a_n$ مفروض باشند، در این صورت یک حل مشترک برای همنهشت‌های $x \equiv a_i \pmod{I_i}$ ، $i = 1, 2, \cdots, n$، وجود دارد.

تمرین ۵.۱۱ قضیه باقیماندهٔ چینی را، همان طور که در تمرین قبل آمده است به کار برده نشان دهید که هر حوزهٔ ددکنید با تعدادی متناهی ایدآل یک ح ا ص است.

تمرین ٦.۱۱ نشان دهید که یک حوزه ددکنید یک ح ت ی است اگر و تنها اگر یک ح ا ص باشد.

تذکر ٦.۱۱ حلقه $\mathbb{Z}[\sqrt{-5}]$ که حلقهٔ اعداد صحیح در هیأت اعداد جبریِ $\mathbb{Q}[\sqrt{-5}]$ است (فصل ۱۲ را ببینید یک ح ا ص نیست. بنابراین دارای بی نهایت ایدآل اول است. از آنجا که هر یک از آنها شامل فقط یک عدد اولِ گویاست و هر عدد اول گویای p می تواند به تعدادی متناهی ایدآل تعلق داشته باشد (یعنی آنهایی که در تجزیهٔ ایدآل اصلی (p) ظاهر می شود) بدین ترتیب اثبات دیگری از نامتناهی بودن اعداد اول گویا به دست می آید.

ت. ۱ برای هر دو ایدآل صحیح A و B در هیأت اعداد جبری K عنصر $w \in \mathbf{O}_K$ وجود دارد به طوری که $(AB, (\omega))_s = A$.

ت. ۲ برای هر ایدآل صحیح A در هیأت اعداد جبری K، α, ω وجود دارد به طوری که $A = \omega\mathbf{O}_K + \alpha\mathbf{O}_K$. یعنی هر ایدآل صحیح روی $\mathbf{O}_K$ می‌تواند با دو عدد صحیح جبری تولید شود.

ت. ۳ برای عدد اول گویای $p > ۱$ فرض کنیم $\xi_p = e^{\frac{۲\pi i}{p}}$ و $\mathbf{O}_K$ حلقهٔ اعداد صحیح $K = \mathbf{Q}[\xi_p]$ باشد نشان دهید که

یک) $(۱ - \xi_p)\mathbf{O}_K \cap \mathbb{Z} = p\mathbb{Z}$.

دو) برای هر $y \in \mathbf{O}_K$، $T_r(y(۱ - \xi_p)) \in p \in \mathbb{Z}$.

سه) اگر $\alpha = a_۰ + a_۱\xi_p + \cdots + a_{p-۲}\xi^{p-۲}$ که a_iها در $\mathbf{Q}$ هستند به $\mathbf{O}_K$ تعلق داشته باشد، آن گاه نشان دهید که تمام a_iها به $\mathbb{Z}$ تعلق دارند، یعنی $\mathbf{O}_K = \mathbb{Z}[\xi_p]$.

ت. ۴ فرض کنیم m یک عدد صحیح $K = \mathbf{Q}[\xi_p]$ را نشان دهد، اگر $f(x) \in \mathbb{Z}[x]$ چند جمله‌ای تحویل‌ناپذیر ξ_m باشد، نشان دهید که

یک) برای عدد اول گویای $p > ۰$ به طوری که $p \nmid m$، ξ_m^p نیز یک ریشهٔ $f(x)$ است.

دو) $$f(x) = \prod_{\substack{(a,m) = ۱ \\ ۱ \leq a < m}} (x - \xi_m^a)$$

سه) برای عدد گویای اول $p > ۰$ به طوری که $p \nmid m$ و $a \in \mathbb{Z}$

$p \nmid f(a)$ اگر و تنها اگر مرتبهٔ ضربی a به پیمانهٔ p برابر m باشد.

چهار) برای عدد گویای اول $p > ۰$ به طوری که به ازای یک $a \in \mathbb{Z}$ و p که $p = ۱ \pmod{m}$ وجود دارد.

فصل ۱۲

هیأت های درجه دوم

پس از آگاهی به نظریهٔ عمومی هیأت های اعداد، در این فصل به یک ردهٔ مهم از این هیأت توجه بیشتری کرده، بعضی اطلاعات واضح تر در باره عناصر آن به دست خواهیم آورد.

۱۲.۱ پایه های صحیح و مبین ها

تعریف. اگر K یک هیأت اعداد باشد، به گونه ای که ۲ $= [K : Q]$، آن گاه K را یک هیأت درجه دوم می نامیم. از این جا معلوم می شود که هر هیأت درجه دوم به شکل $\mathbb{Q}[\sqrt{d}]$ است. (شامل اعداد مختلط $a + b\sqrt{d}$ که $a, b \in \mathbb{Q}$) که در آن d یک عدد صحیح ثابت، مثبت یا منفی است که مربع کامل نیست.

یک هیأت اعداد درجه دوم K، حقیقی یا یک هیأت اعداد موهومی است بر حسب این که $K \subset \mathbb{R}$ یا این که چنین نباشد.

یادآوری می کنیم که هیأت درجه دوم K حقیقی است اگر و تنها اگر $K = \mathbb{Q}(\sqrt{m})$ که در آن $m \in \mathbb{Z}$، بزرگتر از ۱ عدد بدون مربع است. اگر K یک هیأت درجه دوم موهومی باشد، آن گاه $K \cap \mathbb{R} = \mathbb{Q}$.

تذکر ۱.۱۲ فرض کنیم $K = (\sqrt{m})$ (m بدون مربع و به $\mathbb{Z}$ متعلق است) یک هیأت درجه دوم باشد. در این صورت، به ازای p و qای در $\mathbb{Q}$ $\alpha = p + q\sqrt{m}$. اینک

$Tr_K(\alpha) = ۲p$ و $N_K(\alpha) = p^۲ - q^۲m$ هر دو در $\mathbb{Z}$ هستند. اگر قرار دهیم $\alpha = ۲p$ و $b = p^۲ - q^۲m$، داریم $\frac{a^۲ - ۴q^۲m}{۴} = b \in \mathbb{Z}$. به عبارت دیگر

$$a^۲ - ۴q^۲m \equiv ۰ \pmod ۴ \qquad (۱.۱۳)$$

اینک از رابطه های $a^۲ - ۴q^۲m \in \mathbb{Z}$ و $a \in \mathbb{Z}$، چنین نتیجه می شود که $۴q^۲m \in \mathbb{Z}$. از آنجا که m بدون مربع است، اگر قرار دهیم $q = \frac{s}{l}$ که در آن $s, l \in \mathbb{Z}$ و $(s, l) = ۱$، آن گاه l می تواند یکی از دو مقدار ۱ یا ۲ را اختیار کند. به عبارت دیگر $q = \frac{f}{۲}$، که $f \in \mathbb{Z}$.

لذا

$$\alpha = \frac{a}{۲} + \frac{f}{۲}\sqrt{m} \quad a, f \in \mathbb{Z}$$

می خواهیم پایه ای برای $\mathbf{O}_K$ بیابیم. دو حالت در نظر می گیریم.

حالت یک ($m \equiv ۱ \pmod ۴$)

در این حالت از (۱.۱۳) چنین نتیجه می گیریم که $a^۲ \equiv f^۲ \pmod ۴$. بنابراین a و f هر دو زوج یا هر دو فردند. در هر حالت

$$a = u + v\frac{۱ + \sqrt{m}}{۲}, u, v \in \mathbb{Z}$$

حالت دو $m \equiv ۲, ۳ \pmod ۴$.

در این حالت (۱.۱۳) چنین نتیجه می دهد که

$$a = u' + v'\sqrt{m} \qquad u', v' \in \mathbb{Z}$$

خلاصه کنیم

$$O_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\frac{۱+\sqrt{m}}{۲} & m \equiv ۱ \pmod ۴ \\ \mathbb{Z} + \mathbb{Z}\sqrt{m} & m \equiv ۲, ۳ \pmod ۴ \end{cases}$$

ملاحظه می کنیم که به علتِ بدون مربع بودن m، حالت $m \equiv ۰ \pmod ۴$ نمی‌تواند رخ بدهد.

تذکر ۲.۱۲ فرض کنیم $K = \mathbb{Q}(\sqrt{m})$ یک هیأت درجه دوم باشد، که در آن $m \in \mathbb{Z}$ بدون مربع است. اینک به کمک، اطلاعاتی که در مورد پایهٔ صحیح که در

(۲.۱۳) به دست آمده است، می توانیم مبین $d(K)$ برای هیأت درجه دوم را بیابیم اگر $m \equiv ۱ \pmod{۴}$، آن گاه

$$d = d(\mathbb{Q}(\sqrt{m}) = \begin{vmatrix} ۱ & \frac{۱+\sqrt{m}}{۲} \\ ۱ & \frac{۱-\sqrt{m}}{۲} \end{vmatrix}^۲ = m$$

اگر $m \equiv ۲,۳ \pmod{۴}$ محاسبه ای مشابه، نشان می دهد که $d = ۴m$ از (۲.۱۳) و تذکر ۲.۱۳ چنین ملاحظه می کنیم که در تمام حالت‌ها

$$\mathbf{O}_K = \mathbb{Z} + \mathbb{Z}\frac{d+\sqrt{d}}{۲}$$

بنابراین قضیه زیر را خواهیم داشت.

قضیه ۱.۱۲ مبین به طور یکتا یک هیأت درجه دوم را مشخص می کند.

۱۲.۲ شکافیدن اعداد اولِ گویا

تعریف. فرض کنیم K یک هیأت درجه دوم و $\wp$ یک ایدآل دلخواه در $\mathbf{O}_K$ باشد. در این صورت ρ شاملِ یک عدد اول $p \in \mathbb{Z}$ است که $p > ۰$ همچنین $\wp$ در تجزیهٔ $p\mathbf{O}_K$ به ایدآلهای $\wp_۱ \cdots \wp_r$ ظاهر می شود. بنابراین $p^۲ = N_K(P) = N(p\mathbf{O}_K) = N(\wp_۱)\cdots N(p_r)$ که از آن نتیجه می گیریم $N(\wp) = p$ یا این که $N((\wp) = p^۲$.

از این قرار اگر $\wp'$ تصویر $\wp$ تحت خود ریختی نابدیهی K باشد، یکی از حالتهای زیر برقرار خواهد بود.

یک) $\wp \neq \wp', \wp\mathbf{O}_K = \wp\wp'$

دو) $P\mathbf{O}_K = \wp = \wp'$

سه) $\wp = \wp', P\mathbf{O}_K = P^۲$

در حالت (یک) گوییم p در K شکافته می شود. در حالت (دو) گوییم p در K اول باقی می ماند. سرانجام اگر (سه) برقرار شود گوییم p در K منشعب می شود.

قضیه ۲.۱۲ فرض کنیم K یک هیأت درجه دوم با مبین d، معرفی شده در فوق باشد آن گاه برای عدد اول فرد $p \in Z$ داریم

یک) p در K شکافته می شود اگر و تنها اگر $(\frac{d}{p}) = ۱$

دو) p در K منشعب میشود اگر و تنها اگر $(\frac{d}{p}) = 0$

سه) p در K اول باقی می ماند اگر و تنها اگر $(\frac{d}{p}) = -1$

اثبات.

یک) اگر $(\frac{d}{p}) = 1$، در این صورت $y \in \mathbb{Z}$ وجود دارد، به گونه ای که

$$y^2 \equiv d \pmod p \qquad (3.13)$$

فرض کنیم $\wp$ ایدآل تولید شده با p و $y+\sqrt{d}$ باشد، در این صورت

$$\wp\wp' = (p^2, p(y+\sqrt{d}), p(y-\sqrt{d}), y^2-d)\mathbf{O}_K \qquad (4.13)$$

بنابر (۳.۱۳)، $p|y^2-d$ و بنابر (۴.۱۳)

$$\wp\wp' \subset p\mathbf{O}_K$$

اینک از این واقعیت که $p(y+\sqrt{d})$ و $p(y-\sqrt{d})$ عناصر $\wp\wp'$ هستند چنین نتیجه می شود که $2py \in \wp\wp'$. بنابراین با مشاهدهٔ این که به ازای اعداد صحیح l_1 و l_2، $p = (p^2, 2py) = l_1p^2 + l_2 2py$ مبینیم که $p \in \wp\wp'$ و لذا $p\mathbf{O}_K \subset \wp\wp'$. از این جا و همچنین (۵.۱۳) چنین نتیجه می شود که $p\mathbf{O}_K = \wp\wp'$. چون حداکثر دو ایدآل اول $\mathbf{O}_K$ می توانند $p\mathbf{O}_K$ را عاد کنند و p و p' ایدآلهای اول هستند، همچنین $p \in \wp$ و $2d = \sqrt{d}((y+\sqrt{d})-(y-\sqrt{d})) \in \wp+\wp'$ در این صورت، $1 = (p, 2d) \in \wp+\wp'$ که نتیجه می دهد $\wp \neq \wp'$.

به عکس فرض کنیم $p\mathbf{O}_K = \wp\wp'$ که در آن $\wp$ یک ایدآل اول است و $\wp \neq \wp'$. در این صورت $N(\wp) = N(\wp') = p$. عنصر $\alpha \in \wp$ وجود دارد که $\alpha \notin p\mathbf{O}_K = \wp\wp'$. از این جا معلوم می شود که

$$\alpha = k + l\tfrac{d+\sqrt{d}}{2} \qquad (6.13)$$

که در آن $k, l \in \mathbb{Z}$ به گونه ای هستند که $p \nmid (k, l)$.

از آنجا که $\alpha \in \wp$، به ازای ایدآلی مانند $\wp''$، $\alpha\mathbf{O}_K = \wp\wp''$. از این رو نتیجه می شود که $p = N(\wp)$، $\frac{d}{4}|(k+l\frac{d}{2})^2 - l^2| = |N_K(\alpha)| = N(\alpha o_K)$ را عاد می کند. لذا

$$(2k+dl)^2 \equiv l^2d \pmod p \qquad (7.13)$$

اگر $p|l$، آن گاه $p|(2k+dl)^2$ که علاوه بر آن ایجاب می کند که $p|l$. از آنجا که فرد است، داریم $p|k$. بنابراین $p|(k,l)$ که با (۶.۱۳) در تناقض است. بنابراین p، l را عاد نمی کند. اینک از (۷.۱۳) نتیجه می گیریم که به ازای sای، در $\mathbb{Z}$، $s^2 \equiv d \pmod p$، یعنی $(\frac{d}{p}) = 1$.

دو) فرض کنیم $(\frac{d}{p}) = 0$. ایدآل $\wp = p\mathbf{O}_K + \sqrt{d}\mathbf{O}_K$ را در نظر می گیریم در این صورت $\wp^2 = (p^2, p\sqrt{d}, d)\mathbf{O}_K = p\mathbf{O}_K$، زیرا $p = (d, p^2)$. همچنین $\wp$لزوماً

یک ایدآل اول است.

به عکس اگر $p\mathbf{O}_K = \wp^{۲}$ که در آن $\wp$ یک ایدآل اولِ $\mathbf{O}_K$ است. آن گاه $\theta = k + l\frac{d+\sqrt{d}}{۲} \in \wp$ وجود دارد که $k, l \in \mathbb{Z}$ و به گونه ای که $\theta \in p\mathbf{O}_K$. از آنجا که $\theta^{۲} \in p\mathbf{O}_K$ با ملاحظه این که

$$\theta^{۲} = \frac{۱}{۴}((۲k+ld)(۲k-ld)+l^{۲}d)+l(۲k+ld)\frac{d+\sqrt{d}}{۲}$$

چنین بدست می آوریم که

$$p|((۲k+ld))(۲k-ld)+l^{۲}d \qquad (۸.۱۳)$$

و

$$p|l(۲k+ld) \qquad (۹.۱۳)$$

اگر p، l را عاد کند، از (۸.۱۳) نتیجه می گیریم که p، $(۲k+ld)$ یا $(۲k-ld)$ را عاد می کند. از آنجا که p فرد است، $p|k$، اما $p|l$ و $p|k$ ایجاب می کند که $\theta \in p\mathbf{O}_K$ که یک تناقض است.

بنابراین p، l را عاد نمی کند و از (۹.۱۳) نتیجه می گیریم که p، $۲k+ld$ را عاد می کند، اما در این صورت (۸.۱۳) نتیجه خواهد داد که $p|l^{۲}d$ و لذا $p|d$ $(\frac{d}{p}) = ۰$.□

سه) درستی (سه) نتیجهٔ (یک) و (دو) است.

با در نظر گرفتن اشعاب عدد ۲، شرط در قضیه زیر توضیح داده شده است که بدون اثبات آن را بیان می کنیم

قضیه ۳.۱۲ فرض کنیم K یک هیأت درجه دوم با مبین d باشد. آن گاه

یک) ۲ در K شکافته می شود اگر و تنها اگر $d \equiv ۱ \pmod{۸}$.

دو) ۲ در K منشعب می شود اگر و تنها اگر $d \equiv ۰ \pmod{۴}$.

سه) ۲ در K اول باقی می ماند اگر و تنها اگر $d \equiv ۵ \pmod{۸}$.

۱۲.۳ گروه یکه ها

اکنون کار خود را با مطالعهٔ گروه یکه ها در هیأت های درجه دوم ادامه می دهیم. ابتدا حالت هیأت های موهومی را در نظر می گیریم.

قضیه ۴.۱۲ فرض کنیم $K = \mathbb{Q}[\sqrt{-m}]$ یک هیأت درجه دوم موهومی باشد. در این صورت گروه یکه ها، در K به شرح زیر است.

یک) اگر $m=-1$، آن گاه $\mathbb{Q}_k^*=\{1,-1,i,-i\}$، یعنی $\mathbf{Q}_k^*$ گروه ریشه های چهارم واحد است.

دو) اگر $m=3$ آن گاه Q_k^* گروه ریشه های ششم واحد است.

سه) اگر m هر عدد صحیح مثبتی به جز ۱ یا ۳ باشد، آن گاه $\mathbf{Q}_k^*=\{-1,+1\}$.

اثبات. با نمادهای قضیهٔ ۱۱.۱۲ برای هیأت درجه دوم داریم $r_1=0, r_2=1$ و بنابراین $r=r_1+r_2-1=0$. از این رو به موجب قضیه ۱۱.۱۲ گروه Q_k^*، یعنی گروه یکه های K برابر با G_K است که در آن G_K یک گروه متناهیِ دوری شامل ریشه های واحد در K است.

برای دستیابی به اطلاعات دقیق تر چنین عمل می کنیم. از ۲.۱۳ داریم

$$O_K=\begin{cases}\mathbb{Z}+\mathbb{Z}\frac{1+\sqrt{m}}{2} & -m\equiv 1 \pmod 4\\ \mathbb{Z}+\mathbb{Z}\sqrt{m} & -m\equiv 2,3 \pmod 4\end{cases}$$

برای $-m=2,3 \pmod 4$ یک عنصر $\alpha=a+b\sqrt{-m}$ از $\mathbf{O}_K$ را در نظر می‌گیریم. برای این که α یکه باشد، به موجب تمرین ۶.۱۲ باید داشته باشیم $a^2+mb^2=1$. اگر $m>1$، b باید صفر باشد و $a=\pm$، اگر $m=1$، جوابها عبارتند از $a=0$، $b=\pm 1$ و $b=0$ و $a=\pm 1$.

به طریقی مشابه، در حالت $-m\equiv 1 \pmod 4$ به جز $m=3$، یکه ها عبارتند از $\{-1,+1\}$ و برای $m=3$ محاسبه نشان می دهد که یکه ها همان هایی هستند که در حالت (دو) قضیه بیان شده‌اند.□

اگر K هیأت درجه دوم حقیقی باشد، آن گاه r_1، $r_2=0$ بنابراین $r_1+r_2-1=1$. همچنین در این حالت $G_K=\{\pm 1\}$، از قضیه ۱۱.۱۲ داریم.

قضیه ۵.۱۲ گروه یکه های یک هیأت درجه دوم حقیقی با $\mathbb{Z}\times\{1,-1\}$ یکریخت است.

تعریف. از قضیه ۵.۱۳ در می یابیم که در حالت هیأت درجه دوم حقیقی K هر یکهٔ ϵ در K را می توان به شکل $\pm\epsilon_1^n$، به ازای یک $n\in\mathbb{Z}$ و یک یکه ثابت ϵ_1 در K نوشت. همچنین $\epsilon_1 \neq \pm 1$. در این جا نقش ϵ_1 می تواند با $-\epsilon_1$ یا $-\epsilon_1^{-1}$ نیز ایفا شود. اما در بین ϵ_1، $-\epsilon_1$، $-\epsilon_1^{-1}$ تنها یکی از ۱ بزرگتر است. آن را یکهٔ بنیادی K می‌نامیم.

اکنون معادله دیو فانتی موسوم به معادله پل[1] را در نظر می گیریم

[1] Pell

$$a^۲ - mb^۲ = \pm ۱ \qquad (۱۰.۱۳)$$

که در آن $m \neq ۰$ یک عدد صحیح بدون مربع است.

در جستجوی جوابهای صحیح (۱۰.۱۳) هستیم.اگر $m < ۰$، جوابها برای $m < -۱$ عبارتند از $(\pm ۱, ۰)$ و اگر $m = -۱$ جوابها عبارت خواهند بود از $(\pm ۱, ۰)$ و $(۰, \pm ۱)$.

در حالتی که $m > ۱$ یک واقعیت نابدیهی این است که (۱۰.۱۳) دارای بی نهایت جواب صحیح است. از دانش خود دربارهٔ یکه ها در هیأت های درجه دوم حقیقی سود جسته و نتیجهٔ دقیقی در این باره به دست خواهیم آورد.

فرض کنیم $K = \mathbb{Q}(\sqrt{m})$، که در آن $m > ۱$ یک عدد صحیح بدون مربع است. باز هم تجزیه و تحلیل خود را به دو حالت تقسیم می کنیم.

حالت یک $(m \equiv ۲, ۳ \pmod{۴})$

در این حالت

$$Q_K = \mathbb{Z} + \mathbb{Z}\sqrt{m}$$

از آنجا که یکه های K اعداد صحیح با نرم $\pm$هستند، یکه های K که بزرگتر از ۱ هستند، اعدادی به شکل $\alpha = a + b\sqrt{m}$، هستند، به گونه ای که $a, b \in \mathbb{Z}$، $a, b > ۰$ و

$$N(\alpha) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^۲ - mb^۲ = \pm ۱$$

بنابراین اگر یکهٔ بنیادی $a_۱ + b_۱\sqrt{m}$ در K را اختیار کرد و قرار دهیم

$$a_n + b_n\sqrt{m} = (a_۱ + b_۱\sqrt{m})^n \qquad n \geq ۱$$

آن گاه دنبالهٔ (a_n, b_n) تمام جوابهای (۱۰.۱۳) را فهرست می کند. اگر نرم یکهٔ بنیادی برابر با ۱ باشد، دنباله (a_n, b_n) تنها جوابهای $a^۲ - mb^۲ = ۱$ را به دست خواهد داد. در این حالت معادله $a^۲ - mb^۲ = -۱$ دارای جوابی در اعداد طبیعی نیست. اگر نرم یکهٔ بنیادی برابر با ۱− باشد، جوابهای $a^۲ \pm mb^۲ = ۱$ از طریق دنبالهٔ $(a_۲n, b_۲n)$ به دست می آید. برای مثال، حالت اول برای $m = ۳$ و حالت دوم برای $m = ۲$ رخ می دهد.

حالت دو $m \equiv ۱ \pmod{۴}$

در این حالت $\mathbf{O}_K = \{\frac{۱}{۲}(a + b\sqrt{m})$ که در آن $a, b \in \mathbb{Z}$ دارای یک زوجیت هستند. اگر $\frac{۱}{۲}(a + b\sqrt{m})$ در K یکه باشد. باید داشته باشیم $a^۲ - mb^۲ = \pm ۴$. در

این حالت نیز جوابها مانند حالت قبل به دست می آیند. همچنین در این حالت جوابهای (۱۰.۱۳) متناظر با یکه های $a+b\sqrt{m}$ متعلق به حلقهٔ $\mathbb{Z}[\sqrt{m}]$ است.

۱۲.۴ هیأت های اقلیدسی نرم

تعریف. هیأت درجه دوم K را اقلیدسی—نرم می نامیم هر گاه حلقه اعداد صحیح آن با تابع اندازه $\phi(x)=|N_{K/\mathbb{Q}}(x)|$، اقلیدسی باشد.

تمرین ۱.۱۲ نشان دهید که هیأت درجه دوم K، اقلیدسی نرم است اگر و تنها اگر برای هر عنصر $\alpha\in K$، عدد صحیح b در همان هیأت وجود داشته باشد که $|N_{K/\mathbb{Q}}(a-b)|<۱$

تمرین ۲.۱۲ ییأت درجه دوم موهومی $K=\mathbf{Q}(\sqrt{-m})$ اقلیدسی نرم است اگر وتنها اگر m برابر با ۱،۲،۳،۷ یا ۱۱ باشد.

تذکر ۳.۱۲ با در نظر گرفتن یکتایی تجزیه در هیأت های درجه دوم موهومی، گاوس که اگر m یکی از مقادیر ۱−، ۲−، ۳−، ۷−، ۱۱−، ۱۹−، ۴۳−، ۶۷−، ۱۶۳− را اختیار کند، آن گاه $\mathbb{Q}(\sqrt{m})$ یک ح ت ی است. وی همچنین حدس زد که مقادیر دیگری وجود ندارد. پس از ۱۵۰ سال از این حدس، در سال ۱۹۶۶ بیکر[۲] و استارک [۳] این حدس را ثابت کردند. باید متذکر شد تعبیری از اثبات پیشتر توسط هینجر [۴] ارائه شده بود.

تذکر ۴.۱۲ حدس متناظری در مورد هیات های درجه دوم حقیقی، که حاکی است تعدادی نامتناهی m وجود دارد که $\mathbb{Q}(\sqrt{m})$ دارای عدد رده ۱ است هنوز مفتوح است.

تذکر ۵.۱۲ در حالت هیأت درجه دوم حقیقی، معلوم شده است که $\mathbb{Q}(\sqrt{m})$ اقلیدسی—نرم است اگر و تنها اگر m یکی از مقادیر ۲، ۳، ۵، ۶، ۷، ۱۱، ۱۳، ۱۷، ۱۹، ۲۱، ۲۹، ۳۳، ۳۷، ۴۱، ۵۷، ۷۳ را اختیار کند.

تذکر ۶.۱۲ در حالت موهومی، معلوم شده است که حالتهای دیگری به جز آن که در تمرین ۱۳. ۲آمده است و احتمالاً می تواند یا هر تابع اندازه گیری دیگری

---

[۲] Baker
[۳] Stark
[۴] Heegner

اقلیدسی باشد وجود ندارد با در نظر گرفتن تذکر ۳.۱۳ مثال‌هایی از هیأت های $\mathbb{Q}(\sqrt{-19})$، $\mathbb{Q}(\sqrt{-43})$، $\mathbb{Q}(\sqrt{-67})$، $\mathbb{Q}(\sqrt{-163})$ که حلقه اعداد صحیح آن حوزهٔ ایدآلهای اصلی است اما حوزه اقلیدسی نیستند، فراهم می آید.

تذکر ۷.۱۲ * با پذیرفتن صورت تعمیم یافتهٔ فرض ریمان، وینبرگر [5] [We۱۹۷۳] نشان داده است که هر گاه هیأت اعداد جبری تعدادی نامتناهی یکه داشته باشد، حلقهٔ اعداد صحیح آن حوزه اقلیدسی است اگر و تنها اگر یک حوزه ایدآل‌های اصلی باشد. اخیراً کلارک[6] [C۱۹۹۴] ثابت کرده است که $\mathbb{Q}(\sqrt{69})$ همان طور که از نتیجه وینبرگر انتظار می رود، با یک تابع اندازه اقلیدسی است در این مورد می توان به مقاله‌های [GMM۱۹۸۷] و [Le۱۹۹۵] مراجعه کرد.

---

[5] Weinberger

[6] Clark

ضمیمه

آزمون لوکا—لهمر

در این جا، کاربردی از دانشِ خود دربارهٔ هیائت اعداد را در آزمون اوّل بودن ملاحظه خواهیم کرد. به سادگی می توان مشاهده کرد که برای اعداد صحیح $n > ۱$ و $a > ۱$، اگر $a^n - ۱$ اوّل باشد، آن گاه $a = ۲$ و n یک عدد اوّل است. مرسن بیان کرده است که برای اعداد اوّلِ کمتر از ۲۵۷ یا برابر آن، عدد صحیح $M_p := ۲^{p-۱}$، دقیقاً برای ۱۱ تا از این اعداد اوّل است. این یازده عدد توسط وی فهرست شده‌اند. بعدها معلوم شد که بیان مرسن دارای چندین اشتباه است. برای مثال اولین اشتباه کشف شده این است که $M_{۶۱}$ اوّل است، امّا در فهرست مرسن وجود ندارد.

قضیهٔ شایان توجه زیر یک شرط لازم و کافی برای اوّل بودن M_p، که p عددی اوّل و فرد است، به دست می دهد. این آزمون به راحتی می تواند در رایانه انجام شود. اثبات ما اثبات روزن [Ro ۱۹۸۸] است که توسط بروس [Br ۱۹۹۳] ساده شده است.

قضیه ۶.۱۲ آ—۱ (لوکا—لومهر) برای اعداد اوّل، p، $M_p = ۲^p - ۱$ اوّل است، اگر و تنها اگر M_p، $S_{p-۱}$ را عاد کند، که در آن $S_{p-۱}$ با $S_۱ = ۴$ و برای $n \geq ۲$، یا $S_n = S_{n-۱} - ۲$ تعریف می شود.

پیش از اثبات، به اثبات دو لم می پردازیم.

فرض کنیم: $\tau = \frac{۱+\sqrt{۳}}{\sqrt{۲}}$، $\bar{\tau} = \frac{۱-\sqrt{۳}}{\sqrt{۲}}$ و $\omega = \tau^۲ = ۲ + \sqrt{۳}$ و $\bar{\omega} = ۲ - \sqrt{۳}$.
توجه می کنیم که $\tau\bar{\tau} = -۱$ و $\omega\bar{\omega} = ۱$.

برای اعداد صحیح $m \geq ۱$، $S_m = \omega^{۲^{m-۱}} + \bar{\omega}^{۲^{m-۱}}$. **اثبات** برای $m \geq ۱$، می نویسیم $T_m = \omega^{۲^{m-۱}} + \bar{\omega}^{۲^{m-۱}}$. در این صورت داریم $T_۱ = \omega + \bar{\omega} = ۴ = S_۱$. اینک از آنجا که $T_۱ = S_۱$. درستیِ لم از تعریف n نتیجه می شود.

اگر M_p اوّل باشد، آن گاه در حلقهٔ اعداد صحیح، O داریم $\tau^{M_p+۱} \equiv -۱$ $(\mathrm{mod}\ M)_p$. **اثبات** در طول اثبات قرار می دهیم $M = M_p$. از آنجا که $\sqrt{۲}\tau = ۱ + \sqrt{p}$ همنهشتی زیر در O به دست می آید

$$\tau^M ۲^{\frac{M-۱}{۲}} \equiv ۱_+ ۳^{\frac{M-۱}{۲}} \sqrt{۳} (modM)$$

از آنجا که $M \equiv -۱(mod۸)$ و همچنین $M \equiv ۱(mod۳)$ همنهشتی های زیر در $Z \subset O$ به دست می آید.

$$۲^{\frac{M-۱}{۲}} \equiv (\frac{۲}{M} = ۱(modM)$$

$$۳^{\frac{M-۱}{۲}} \equiv (\frac{۳}{M} = -۱(modM)$$

اکنون از(۲.٪)، (۳.٪) و (۴.٪) داریم

$$\tau^M\sqrt{۲} \equiv ۱ - \sqrt{۳}(modM)$$

به عبارت دیگر، به ازای یک $\theta \in O$،

$$\sqrt{۲}(\tau^M - \bar{\tau} = M\theta$$

از آنجا که $M = M_p + ۲^{p-۱}$، با ضرب برابری فوق در $۲^{\frac{۲p-۱}{۲}}$، داریم:

$$\tau^M \equiv \bar{\tau}(modM).$$

ولذا

$$\tau^{M+۱} \equiv \tau\bar{\tau} \equiv -۱(modM$$

اثبات قضیه آ.۱: فرض کنیم M_p به ازای عدد اوّل p، اوّل باشد، در این صورت بنابر لم آ.۲، همنهشتی زیر را در o داریم

$$\tau^{۲^p} + ۱ \equiv ۰(modM_p)$$

که از آن نتیجه می شود

$$\omega^{۲^{p-۱}} + ۱ \equiv))modM_p)$$

و لذا بنابر (۱.٪)،

$$\omega^{۲^p-۲} + \bar{\omega}^{۲^{p-۲}} \equiv ۰(modM_p)$$

بنابر این به موجب لم آ.۱، داریم$S_p - ۱ = M_p\delta$، که در آن $\delta \in O$. از آنجا که δ به $\mathbb{Q}$ نیز تعلق دارد، داریم $\delta \in \mathbb{Z}$.

برعکس فرض کنیم p یک عدد اوّل فرد است و M_p، S_{p-1} را عاد می کند. در صورت امکان، فرض کنیم q عدد اوّلی است که یک مقسوم علیه M_p است و $q^2 \leq M_p$. از آنجا که M_p، S_{p-1} را در حلقهٔ اعداد صحیح Q_k که $K = \mathbb{Q}(\sqrt{3})$ عاد می کند داریم :

$$\omega^{2^{p-1}+1} \equiv 0 (mod q)$$

این همنهشتی نشان می دهد که مرتبهٔ ω در گروه $(\frac{O_k}{qO_k})^*$ برابر با 2^p می باشد. از آنجا که مرتبه گروه $(\frac{O_k}{M-pO_k})^*$ از $q^2 - 1$ بیشتر نیست داریم

$$2^p \leq q^2 - 1 \leq M_p - 1 = 2^p - 2$$

که غیر ممکن است. بنابراین M_p اوّل است.

فصل ۱۳

حل مسائل برگزیده

۱.۰ از آنجا که در یک هیأت تمام عناصر ناصفر یکه هستند، بیان اول بدیهی است. اینک فرض کنیم R حلقه ای است که ایدآل سره ندارد. فرض کنیم r یک عنصر ناصفر R باشد، از آنجا که (r) یعنی ایدآل اصلی تولید شده با r ناصفر است، به موجب فرض باید بابر با R باشد. این بدان معنی است که ۱ به (r) تعلق دارد. بنابراین $r' \in R$ وجود دارد که $rr' = ۱$، یعنی r' وارون r است. از این رو هر عنصر ناصفر r یکه و R یک هیأت است.

۲.۰ فرض کنیم D یک حوزه صحیح و $d_۱$،$d_۲$،$\cdots$،d_n عناصر متمایز آن باشند. فرض کنیم d یک عنصر ناصفر R است، عناصر، $dd_۱$، $dd_۲$،$\cdots$،dd_n را در نظر می گیریم. از آنجا که D دارای مقسوم علیه صفر نیست، به ازای $i \neq j$، $dd_i \neq dd_j$. بنابراین، $\{dd_۱, dd_۲, \cdots, dd_n\}$ که یک زیر مجموعهٔ D است، به اندازهٔ D عضو دارد لذا برابر با D است. پس به ازای یک $i \in \{۱, ۲, \cdots, n\}$ ، $dd_i = ۱$. بنابراین هر عنصر ناصفر R دارای وارون است و اثبات تمام می شود.

۳.۰ فرض کنیم $\mathcal{S}$ مجموعهٔ تمام ایدآل های حلقه ناصفر R به جز R است. از آنجا که ایدآل صفر به $\mathcal{S}$ تعلق دارد $\mathcal{S}$ تهی نیست. خانواده $\mathcal{S}$ را که با رابطه شمول مرتب شده است در نظر می گیریم. عنصر ماکسیمالِ $\mathcal{S}$ در این رابطهٔ ترتیب، به موجب تعریف، یک ایدآل ماکسیمال است. از لم تسورن استفاده کرده، نشان می دهیم $\mathcal{S}$ دارای عضو ماکسیمال است. اگر $\mathcal{F}$ یک مجموعهٔ کاملاً مرتب $\mathcal{S}$ باشد، ملاحظه می کنیم که اجتماع تمام عناصر $\mathcal{F}$ یک عنصر $\mathcal{S}$ است و به وضوح یک کران بالای $\mathcal{F}$ می باشد. به موجب لم تسورن $\mathcal{S}$ دارای عضو ماکسیمال M می باشد.

۱.۱ (آ) پیشتر ملاحظه کردیم که برای هر عدد صحیح n، مجموعهٔ $n\mathbb{Z} = \{nr | r \in \mathbb{Z}\}$ یک زیر گروه $(\mathbb{Z}, +)$ است.

فرض کنیم H یک زیر گروه $(\mathbb{Z}, +)$ باشد، اگر H شامل هیچ عنصر ناصفری نباشد، در این صورت $H = \circ\mathbb{Z}$. اگر H شامل عنصر ناصفر a باشد، آن گاه H شامل یک عدد صحیح مثبت است (زیرا یا a یا $-a$ به H تعلق دارد). فرض کنیم m کوچکترین عدد صحیح مثبت در H باشد. از آنجا که H یک زیر گروه است، برای اثبات $m\mathbb{Z} \subseteq H$ گوییم اگر k یک عدد صحیح مثبت باشد، $mk = \underbrace{m + \cdots + m}$ (n بار) $\in H$. از طرفی $m(-k) = -mk \in H$ و $m\circ = \circ \in H$. اگر ممکن باشد، فرض کنیم $b \in H \setminus m\mathbb{Z}$. اینک به موجب الگوریتم تقسیم، $b = mq + r$ که $\circ \leq r < m$، به لحاظ این که b به $m\mathbb{Z}$ تعلق ندارد، $r \neq \circ$ که در این صورت $r = b - qm \in H$، که با مینیمال بودن m تناقض دارد. از این رو $H = m\mathbb{Z}$، بنابراین زیر گروههای $(\mathbb{Z}, +)$ دقیقاً زیر مجموعه های $n\mathbb{Z}$ به ازای یک $n \in \mathbb{Z}$ هستند.

(ب) فرض کنیم G یک گروه دوری و a یک مولد آن باشد. فرض کنیم $f : \mathbb{Z} \longrightarrow G$ تابعی باشد که با $f(a) = a^n$ تعریف شده است. به وضوح این تابع، یک همریختی پوشا است. هستهٔ f یک زیر گروه $\mathbb{Z}$ و لذا به ازای mای، $m \geq \circ$ برابر با $m\mathbb{Z}$ است. اگر $m = \circ$، آن گاه G با $\mathbb{Z}$ یکریخت است.

اگر $m > \circ$ بنابر قضیه اول یکریختی G با $\mathbb{Z} \setminus m\mathbb{Z}$ یکریخت است.

(پ) از قسمت (آ) نتیجه می شود.

۲.۱ اگر $p_1 = ۳$، $p_2 = ۷$، $\cdots$، p_r اعداد اول به شکل $۴n + ۳$ به ترتیب افزایشی باشد، آن گاه عدد $m = ۴p_2p_3 \cdots p_r + ۳$ را در نظر می گیریم. اعداد اولی که عدد فرد m را عاد می کنند، نمی توانند همگی به شکل $۴n + ۱$ باشند، از این رو m باید مقسوم علیه ای به شکل $۴n + ۳$ داشته باشد. به وضوح این عدد اول نمی تواند هیچ یک از p_iها باشد، $i = ۱, ۲, \cdots, r$.

۳.۱ (آ) به تعداد mm'، عدد به شکل $a'm + am'$ وجود دارد که a، a' به ترتیب در مجموعه کامل مانده ها به پیمانه m و m' تغییر می کنند، اگر $a'm + am' \equiv b'm + bm' \pmod{mm'}$، آن گاه $a'm \equiv b'm \pmod{m'}$ و $am' \equiv bm' \pmod{m}$. چون $(m, m') = ۱$. نتیجه می شود که $a' \equiv b' \pmod{m'}$ و $a \equiv b \pmod{m}$.

(ب) اگر a در یک دستگاه تحویل یافته مانده ها به پیمانه m و a' در یک دستگاه تحویل یافته به پیمانه m' تغییر کند، نشان می دهیم که $a'm + am'$ در یک دستگاه تحویل یافته مانده ها به پیمانه mm' تغییر می کند.

در قسمت (آ) نشان دادیم که اعداد $a'm + am'$ نا همنهشت اند. فرض کنیم p عدد اولی باشد که $(mm', am' + am')$ را عاد می کند. در این صورت p، m یا m' را عاد می کند، اگر $p|m$، آن گاه p همچنین am' را عاد می کند. از آنجا که $(m, m') = ۱$، چنین نتیجه می شود که $p|a$. بنابراین $p|(a, m)$. این رابطه بخشپذیری، با این فرض که a در مجموعهٔ دستگاه تحویل یافتهٔ مانده ها به پیمانه m تغییر می کند متناقض است، بنابراین $(mm', a'm + am') = ۱$.

فرض کنیم d عدد صحیحی باشد که $(d, mm') = ۱$، به موجب قسمت (آ)، اعداد صحیح a و a' وجود دارند که $d = a'm + am'$. اینک $(a, m) = (am', m) = (a'm + am', m) = (d, m) = ۱$، به طور مشابه $(a', m') = ۱$ بدین ترتیب اثبات (ب) کامل می شود.

(پ) بنابر قسمت (ب) کافیست نشان دهیم که $\phi(p^a) = p^a(۱ - \frac{۱}{p})$، که در آن p یک عدد اول و a یک عدد صحیح مثبت است. اینک در بین p^a عدد ۱ و ۲ و $\cdots$ و p^a، دقیقاً $p^{a-۱}$ عدد وجود دارد که مضرب p است، بنابراین $\phi(p^a) = p^a - p^{a-۱} = p^a(۱ - \frac{۱}{p})$

۱.۴ مجموعهٔ $\{۱, ۲, \cdots, m\}$ را که یک دستگاه کامل مانده ها به پیمانه m است در نظر می گیریم. ملاحظه می کنیم که مجموعهٔ $\{a, ۲a, \cdots, ma\}$ نیز یک دستگاه کامل مانده ها به پیمانه m است. زیرا به علت این که $(a, m) = ۱$، $ia \equiv ja \pmod m$ نتیجه می‌دهد که $i \equiv j \pmod m$. بنابراین تنها یکی از اعداد a، $\cdots$، ma به پیمانه m با b همنهشت است.

۵.۱ مانند تمرین ۴.۱ ملاحظه می کنیم که اگر یک دستگاه تحویل یافته مانده‌های، $\{a_۱, a_۲, \cdots, a_{\phi(m)}\}$ به پیمانه m مفروض باشد، مجموعهٔ $\{aa_۱, \cdots, aa_{\phi(m)}\}$ نیز یک دستگاه تحویل یافته مانده ها به پیمانه m است.

بنابراین $a_۱a_۲ \cdots a_{\phi(m)} \equiv aa_۱ \cdots aa_{\phi(m)} \pmod m$. از آنجا که هر a_i نسبت به m اول است، داریم $a^{\phi(m)} \equiv ۱ \pmod m$.

۶.۱ به علت این که p، $n^۲ + ۱$ را عاد می کند، نتیجه می گیریم که $(p, n) = ۱$. بنابراین به موجب قضیه ۱.۵ که در p_iها اعداد اول متمایز هستند،

$$n^{p-۱} \equiv ۱ \pmod p \qquad (۱.۱۴)$$

بنابر فرض

$$n^۲ \equiv -۱ \pmod p \qquad (۲.۱۴)$$

در صورت امکان، فرض کنیم p به شکل $۴n + ۳$ است، در این صورت $\frac{p-۱}{۲}$ عددی است فرد و لذا از (۲.۱۴) نتیجه می شود که

$$n^{p-1} \equiv -1 \pmod p \qquad (۳.۱۴)$$

از (۱.۱۴) و (۳.۱۴) چنین نتیجه می شود که $1 \equiv -1 \pmod p$ که ممتنع است، زیرا p یک عدد فرد است. بنابراین هر عدد اول فرد که عددی به شکل n^2+1 را عاد کند به شکل $4m+1$ است. اینک، در صورت امکان، فرض می‌کنیم تنهاا عداد اول به شکل $4m+1$ عبارت باشند از

$$p_1 = 5, p_2 = 13, \cdots, p_r$$

اکنون عدد $d = (2P_1p_2\cdots p_r)^2 + 1$ را در نظر می گیریم. به وضوح هر مقسوم علیه d فرد است. بنابر قسمت اول این تمرین، هر مقسوم علیه اول d باید به شکل $4m+1$ باشد. این واقعیت ما را به تناقض می کشاند، زیرا هیچ یک از اعداد p_1 ، p_2، $\cdots$، p_r نمی توانند d را عاد کنند. بنابراین باید تعداد نامتناهی عدد اول به شکل $4m+1$ وجود داشته باشد.

۷.۱ برای هر عدد صحیح ملاحظه می کنیم n^2 به پیمانه ۳ همنهشت با ۰ یا ۱ است. بنابراین n^2+1 به پیمانه ۳ همنهشت با ۱ یا ۲ میشود. از این رو همنهشتی $x^2+1-3y^5 \equiv 0 \pmod 3$ دارای هیچ جوابی نیست، لذا معادلهٔ مفروض نیز دارای جواب صحیح نیست.

۱۰.۱ می توان مشاهده کرد که $\frac{p+1}{2}$ عنصر مجموعهٔ $\{a^2, 0 \le a \le \frac{p-1}{2}\}$ و همچنین عناصر مجموعهٔ $\{-a^2-1, 0 \le a \le \frac{p-1}{2}\}$ به پیمانه p متمایزند. بنابر اصل لانه کبوتری عنصری در مجموعهٔ اول وجود دارد، که به پیمانه p، برابر با عنصری در مجموعه دوم است. بدین ترتیب قسمت (آ) ثابت شده است. ملاحظه می کنیم که اگر دو عدد صحیح a و b چنان باشند که $a^2+b^2+1 \equiv 0 \pmod{p^k}$ آن گاه حداقل یکی از عناصر a و b مثلاً a بر p بخشپذیر نیست. اینک به ازای عدد صحیحی مانند q، $a^2 = -b^2 - 1 + qp^k$، به علت این که a بر عدد اول p بخشپذیر نیست، داریم $(2a,p) = 1$ و لذا به ازای اعداد صحیحی مانند x و y، $q = 2ax + yp$. اینک به سادگی مشاهده می شود که $(a-xp^k) \equiv -b^2 - 1 \pmod{p^{k+1}}$ و قسمت (ب)، با استقرا از قسمت (آ) نتیجه می شود. سر انجام اگر تجزیه m به حاصلضرب اعداد اول به شکل $m = \Pi_{i=1}^{l} p_i^{r_i}$ باشد که در آن p_iها اعداد اول متمایز هستند، بنابر قسمت (ب) برای هر i، a_i و b_i وجود دارد که $a_i^2 + b_i^2 + 1 \equiv 0 \pmod{p_i^{r_i}}$. اکنون بنا بر قضیه باقی ماندهٔ چینی a و b وجود دارند که $a \equiv a_i \pmod{P_i^{r_i}}$ و $b \equiv b_i \pmod{p_i^{r_i}}$ و داریم $a^2+b^2+1 \equiv 0 \pmod n$.

(۱.آ) فرض کنیم $n > 1$ یک عدد صحیح است، فرض کنیم $m = \frac{1}{n} + \cdots + \frac{1}{2}$ یک عدد صحیح باشد و $2^r \le n < 2^{r+1}$. اگر قرار دهیم $d = 2^r$، داریم

$$\sum_{۲\leq i\leq n} \frac{۱}{i} = m - \frac{۱}{d} \qquad (۴.۱۴)$$

اگر L کوچکترین مضرب مشترک مخرج های سمت چپ باشد، آن گاه $L = ۲^{r-۱} \times L_۱$ که در آن، L فرد است. پس از جمع کسرهای سمت چپ به ازای عدد صحیحی مانند N داریم $\frac{N}{L} = \frac{md-۱}{d}$. اینک $Nd = (md - ۱)L$ که بزرگترین توان ۲ که سمت راست را عاد می کند $۲^{r-۱}$ است(زیرا $md - ۱$ فرد است)، حال آن که بزرگترین توان ۲ی سمت راست، $d = ۲^r$ می باشد، که متناقض با تجزیه یکتای اعداد صحیح است.

(۲.آ) از آنجا که $(a,b) = ۱$، نتیجه می گیریم که $(a+b, ab) = ۱$، بنابراین $(a+b)^{\phi(ab)} \equiv ۱ \pmod{ab}$. با بسط سمت چپ، داریم $a^{\phi(ab)} + b^{\phi(ab)} \equiv ۱$ $\pmod{ab}$.

(۳.آ) کسرهای

$$\frac{۱}{n}, \frac{۲}{n}, \ldots, \frac{n-۱}{n}, \frac{n}{n}$$

را در نظر می گیریم. اگر این کسرها را ساده کنیم فقط $\phi(n)$ تا از آنها مخرجشان برابر با n خواهد بود. مشاهده می کنیم که این امر در مورد تمام مقسوم علیه های n درست است. فرض کنیم d یک مقسوم علیه n و $n = dd'$، در بین کسرهای مفروض تنها آنهایی که صورتشان مضرب d' است مقسوم علیه های d را، پس از ساده کردن، در مخرج خود دارند، آنها عبارتند از

$$\frac{d'}{n}, \frac{۲d'}{n}, \ldots, \frac{dd'}{n}$$

و تعداد آنها برابر با d است و می توان آنها را به شکل

$$\frac{۱}{n}\frac{۲}{n}, \ldots, \frac{d}{d}$$

نوشت. بنابراین در بین کسرهای ساده شده، دقیقاً $\phi(d)$ کسر وجود دارد که مخرج آنها برابر با d است، از آنجا که n کسر وجود دارد، داریم $n = \sum_{d|n} \phi(d)$.

(۴.آ) فرض کنیم d مقسوم علیه n است. اگر یک عنصر aی G با مرتبهٔ d وجود داشته باشد، آن گاه G دارای یک زیر گروه دوری با مرتبه G است که با a تولید می شود. اینک هر عضو bی H در معادلهٔ $b^d = ۱$ صدق می کند. از آنجا که H، d عضو دارد ، به موجب شرط داده شده، عنصری با مرتبه d که خارج H نباشد، وجود ندارد. مشاهده می کنیم که تعداد مولدهای H برابر با $\phi(d')$ است و لذا اگر برای یک مقسوم علیه dی n، عنصری با مرتبه d در G وجود داشته باشد، تعداد آنها برابر با $\phi(d)$ است.

اینک هر عضو G یک گروه دوری از مرتبه d تولید می کند، به گونه ای که $d|n$. بنابر این تعداد عناصر G برابر است با $\sum_{d|n}\phi(d)$، که درآن مجموع طوری حساب می‌شود که G دارای یک عنصر از مرتبهٔ d باشد. از آنجا که به موجب تمرین آ.۳ داریم $n=\sum_{d|n}\phi(d)$. اگر به ازای dای، عنصری از مرتبهٔ d وجود نداشته باشد، نتیجه می گیریم که تعداد عناصر G اکیداً کوچکتر از n می باشد که یک تناقض است. بنابر این G برای هر مقسوم علیه dی n عنصری از مرتبه d دارد. اما n یک مقسوم علیه n است و عنصری با مرتبه n در G وجود دارد. این نشان می دهد که G دوری است.

۲.۳ فرض کنیم a عنصری با مرتبه ماکسیمم در G است. فرض کنیم n مرتبهٔ a باشد. ادعا می کنیم که مرتبهٔ هر عضو G، n را عاد می کند. اگر ممکن باشد، فرض کنیم b در G باشد که مرتبهٔ m آن، n را عاد نکند، از اینجا چنین نتیجه می شود که عدد اول p وجود دارد که توان ماکسیمم p که m را عاد می کند اکیداً از توان ماکسیمم p که n را عاد می کند بزرگتر است. از این قرار عدد اول با شرط $p^i||m$، $p^j||n$ و $i>j$ وجود دارد. اینک مرتبه $b^{m/p'}$ برابر با p^i و مرتبهٔ a^{p^j} برابر باn/p^j است. از آنجا که $(n/p^j,p^i)=۱$ مرتبهٔ $b^{m/p'}a^{p^j}$ برابر با $(n/p^j)p^i>n$ می باشد که با ماکسیمال بودن n در تناقض است. به این ترتیب قسمت اول تمرین ثابت شده است. فرض کنیم F یک هیأت متناهی باشد، فرض کنیم α یک عنصر $F^*=F\setminus\{۰\}$ با مرتبهٔ ماکسیمال مثلاً n باشد. در این صورت به موجب قسمت اولِ تمرین برای هر $\beta\in F^*$، $\beta^n=۱$. از آنجا که چند جمله ای $x^n-۱$ حداکثرز دارای n ریشه است، چنین نتیجه می گیریم که مرتبه F^* حداکثر برابر n است، لیکن $۱,\alpha,\cdots,\alpha^{n-۱}$ در F^* هستند. بنابر این F^* با α تولید شده است.

۴.۳ تعداد جواب های متمایز همنهشتی $f(x)\equiv ۰ \pmod{p}$ به پیمانهٔ p همان تعداد جواب های معادلهٔ

$$((x-\bar{۱})(x-\bar{۲})\cdots(x-\overline{(p-۱)}))-x^{p-۱}+\bar{۱}=\bar{۰} \qquad (۵.۱۴)$$

در هیأت $F_p=\frac{\mathbb{Z}}{p\mathbb{Z}}$ است، که در آن $\bar{a}$ رده باقی‌مانده به پیمانه p است. به موجب تمرین (۵.۱) (اویلر—فرما) چنین نتیجه می گیریم که تمام عناصر ناصفرِ $\frac{\mathbb{Z}}{p\mathbb{Z}}$ جواب های $x^{p-۱}-\bar{۱}=\bar{۰}$ هستند. از طرفی تمام عناصرِ ناصفر $\frac{\mathbb{Z}}{p\mathbb{Z}}$ جواب های $(x-\bar{۱})(x-\bar{۲})\cdots(x-\overline{(p-۱)})=\bar{۰}$ می باشند بنابر این تمام عناصر ناصفر $\frac{\mathbb{Z}}{p\mathbb{Z}}$ جواب های معادلهٔ (۵.۱۴) هستند. اما درجه این معادله کمتر از $p-۱$ است، زیرا جملهٔ $x^{p-۱}$ حذف می شود. بنابر این چند جمله ای سمت چپ (۵.۱۴) چند جمله ای صفر است. بدین ترتیب قسمت اول تمرین ثابت شده است. برای قسمت دوم باید به جملهٔ ثابت چند جمله ای $f(x)$ که همان $(p-۱)!+۱$ است توجه کنیم. از قسمت

اول تمرین نتیجه می گیریم که این عبارت بر p بخشپذیر است. این واقعیت همان بیان قضیه ویلسون است.

۱.۴ عنصر ۲ را در حلقهٔ $R = \frac{\mathbb{Z}}{6\mathbb{Z}}$ در نظر می گیریم، اگر در R، $\bar{2}|\bar{a}\bar{b}$ آن گاه به سادگی دیده میشود که $\bar{a}|2$ یا $\bar{b}|2$. اما به این لحاظ این که $\bar{2}.\bar{4} = \bar{2}$ که در آن نه $\bar{2}$ و نه $\bar{4}$ یکه نیستند (یکه های R عبارتند از $\bar{1}$ و $\bar{5}$) چنین نتیجه می گیریم که $\bar{2}$ در R تحویل‌ناپذیر نیست.

۲.۴ فرض کنیم R یک حوزهٔ صحیح و p در R اول است، فرض کنیم $p = ab$ که در آن $a, b \in R$. از آنجا که p اول است، $p|a$ یا $p|b$. اگر $p|a$ آن گاه به ازای عنصری مانند $r \in R$، $p = ab = (rp)b$. از این جا نتیجه می شود که $p(1 - rb) = 0$ و چون R یک حوزهٔ صحیح و p ناصفر است ، نتیجه می گیریم که $rb = 1$، یعنی b یکه است. به طور مشابه اگر $p|b$ نتیجه خواهد داد که a یکه است. بنابر این p تحویل ناپذیر است

۴.۴ فرض کنیم R یک ح ا ص و α یک عنصر تحویل ناپذیر R باشد. باید نشان دهیم که اگر α حاصلضرب دو عنصر R را عاد کند، آن گاه α یکی یا هر دوی آنها را عاد می کند. فرض کنیم $\alpha|ab$ که $a, b \in R$. اگر $\alpha \nmid a$ ، هر ایدآل R به ویژه ایدآلی که با α و b تولید می شود اصلی است. فرض کنیم این ایدآل با β تولید شود. اینک به ازای rی در R، $\alpha = \beta r$. چون α تحویل‌ناپذیر است، β یا r یکه هستند. اگر β یکه باشد، آن گاه ۱ به ایدآل تولید شده با α و b تعلق دارد این بدان معنی است که به ازای $x, y \in R$، $x\alpha + y\beta = 1$، بنابر این $ax\alpha + ayb = a$. از آنجا که $\alpha|ab$ نتیجه می گیریم که $\alpha|a$ که با فرض تناقض دارد. بنابر این r یکه است و لذا $(\beta) = (\alpha)$ اینک $b \in (\beta) = (\alpha)$ که نتیجه می دهد $\alpha|b$ و اثبات تمام است.

۵.۲ ملاحظه می کنیم که $f(x - 1) = 8x^3 - 24x^2 + 18x - 3$. با قرار دادن $p = 3$ به موجب معیار ایزنشتاین (قضیهٔ ۷.۵) ملاحظه می کنیم که $f(x - 1)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. بنابر این $f(x)$ نیز تحویل‌ناپذیر است.

۱.۶ فرض کنیم K یک توسیعِ هیأت F و $\alpha \in K$. دنبالهٔ عناصر $1, \alpha, \alpha^2, \cdots$ نمی‌تواند روی F مستقل خطی باشد. در واقع اگر $[K : F] = n$، آن گاه مجموعه $\{1, \alpha, \alpha^2, \cdots, \alpha^n\}$ متشکل از $n + 1$ عنصر، در F وابسته خطی خواهد بود. اگر $a_0 + a_1\alpha + \cdots + a_n\alpha^n$، $a_i \in F$ یک ترکیب نابدیهی باشد، آن گاه α در چند جمله ای ناصفرِ $a_0 + a_1x + \cdots + a_nx^n$ که $a_i \in F$ صدق می کند و لذا روی F جبری است.

۱۱.۶ چند جمله ای های $f(x_1, x_2, \cdots, x_{2p-1})$ و $g(x_1, x_2, \cdots, x_{2p-1}$ در

$F_p[x_1, x_2, \cdots, x_{2p-1}]$ را که با

$$f(x_1, x_2, \cdots, x_{2p-1}) \sum_{i=1}^{2p-1} x_i^{p-1}$$

و

$$g(x_1, x_2, \cdots, x_{2p-1}) = \sum_{i=1}^{2p-1} a_i x_i^{p-1}$$

تعریف می شوند در نظر می گیریم. مجموع درجه های چند جمله‌ای‌های f و g، $2p-2$ برابر $2p-1 < 2p-2$ است. به لحاظ این که $f(0,0,\cdots,0) = g(0,0,\cdots,o) = 0$، بنا به تذکر ۵.٦، عنصر $(\alpha_1, \cdots, \alpha_n) \in F_p^n$ وجود دارد که تمام α_i صفر نیستند و

$$\sum_{i=1}^{2p-1} \alpha_i^{p-1} = 0 \qquad (٦.۱۴)$$

و

$$\sum_{i=1}^{2p-1} a_i \alpha_i^{p-1} = 0 \qquad (۷.۱۴)$$

برای هر $\alpha \in F_p$، $\alpha^{p-1} = 1$، اگر و تنها اگر $\alpha \neq 1$. بنابر این از (٦.۱۴) چنین نتیجه می شود که دقیقاً p تا از α_i ها مثلاً $\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_p}$ ناصفر هستند و بنابر این از (۷.۱۴) داریم $a_{i_1} + a_{i_2} + \cdots + a_{i_p} = 0$.

۱.۷

$$\begin{aligned}
\left(\frac{45}{1009}\right) &= \left(\frac{3^2}{1009}\right)\left(\frac{5}{1009}\right) \\
&= \left(\frac{5}{1009}\right) \\
&= \left(\frac{1009}{5}\right)(-1)^{\frac{1009-1}{2}\frac{5-1}{2}} \\
&= \left(\frac{1009}{5}\right) \\
&= \left(\frac{9}{5}\right) = 1.
\end{aligned}$$

بنابر این ۴۵ به پیمانه عدد اول ۱۰۰۹ یک مربع است.

۲.۷ فرض کنید اعداد صحیح x, y در معادلهٔ $y^2 = x^3 + 23$ صدق کنند. اینک y^2 به پیمانه ۴ با ۰ یا ۱ همنهشت است و $23 \equiv 3 \pmod 4$. از آنجا که x^3 به پیمانه ۴ با یکی از اعداد ۰ یا ۱ یا ۳ همنهشت است، تنها امکان این است که $x \equiv 1 \pmod 4$. معادلهٔ داده شده را به شکل $y^2 + 4 = x^3 + 27$ می‌نویسیم. اما $x^3 + 27 = (x+3)(x^3 - 3x + 29)$ و $(x^3 - 3x + 9) \equiv -1 \pmod 4$ بنابر این عدد اول $p \equiv -1 \pmod 4$ وجود دارد به طوری که $p | x^2 - 3x + 9$ و لذا

$p|y^۲ + ۴$، به عبارت دیگر $y^۲ \equiv -۴ \pmod p$ که به معنی آن است که $\left(\frac{-۴}{p}\right) = ۱$ که آنهم نتیجه می دهد $\left(\frac{-۱}{p}\right) = ۱$ که یک تناقض است. بنابراین معادلهٔ دیوفانتی داده شده دارای جواب نیست.

۳.۷ فرض کنید $p_۱, p_۲, \cdots, p_r$ مجموعه متناهی اعداد اول به شکل $۸n - ۱$ باشد. عدد صحیح $N = (۴p_۱p_۲\cdots p_r)^۲ - ۲$ را در نظر می گیریم. اگر p یک عدد اول فرد و مقسوم علیه N باشد، آن گاه $(۲/p) = ۱$. بنابر این بنابر قسمت (دو) قضیهٔ ۱.۷ ، $p \equiv \pm ۱ \pmod ۸$. اگر قرار دهیم $N = ۲M$، ملاحظه می کنیم که M به شکل $۸n - ۱$ است. از این رو تمام مقسوم علیه های اول N نمی توانند به شکل $۸n + ۱$ باشند. بنابر این N باید یک مقسوم علیه اول مانند q به شکل $۸n - ۱$ داشته باشد. از آنجا که q نمی تواند در بین اعداد اولِ $p_۱, p_۲, \cdots, p_r$ باشد، ادعا درست است.

ب ۱ فرض کنید σ تابع اندازه باشد که R را به یک حوزهٔ اقلیدسی تبدیل می کند. فرض کنید u یک عنصر ناصفر و نا یکه از R باشد به قسمی که $\sigma(u)$ می‌نیمال است، یعنی برای هر عنصر ناصفر و نایکه u، $\sigma(u) \leq \sigma(u')$. اگر $\alpha \in K$ مفروض باشد می توان نوشت $\alpha = qu + r$ که $q, r \in R$ و $\sigma(r) \leq \sigma(u)$. می نیمال بودن $\sigma(u)$ نشان می دهد که r نمی تواند یک عنصر نایکه R باشد.

ب۲ در صورت امکان فرض کنیم R یک حوزه اقلیدسی باشد. بنابر تمرین ب ۱، عنصر ناصفر و نایکهٔ u در R وجود دارد به طوری که برای هر $\alpha \in R$، $r \in R^* \cup \{۰\}$ وجود دارد که $u|(\alpha - r)$. با در نظر گرفتن توان دوم قدر مطلق عناصر R به سادگی در می یابیم که تنها عناصر یکهٔ R عبارتند از ۱+ و ۱−. بنابر این‌برای هر $\alpha \in R$، u یکی از عناصر α، $\alpha - ۱$ یا $\alpha + ۱$ را عاد می کند. از آنجا که u نا یکه است، اگر قرار دهیم $\alpha = ۲$ داریم $u|۲$ یا $u|۳$. به عبارت دیگر $v \in R$ وجود دارد که $uv = ۲$ یا $uv = ۳$ ادعا می کنیم که $u \in \mathbb{Z}$، زیرا که اگر $u \notin \mathbb{Z}$، آن گاه $v \notin \mathbb{Z}$. اینک برای هر $r \in R$ با شرط $r \notin \mathbb{Z}$، مقدار قدر مطلق r بزرگتر از ۳ خواهد بود. با توجه به این موضوع برای u, v صادق است، مربع uv بزرگتر از ۹ خواهد بود که با واقعیت برابری های $uv = ۲$ و $uv = ۳$ تناقض دارد. این تناقض ادعا را ثابت می کند. بنابراین $u = \pm ۲$ یا $u = \pm ۳$. اینک قرار می دهیم $\alpha = \frac{۱+\sqrt{-۱۳}}{۲}$، به طوری که مربع قدر مطلق هیچیک از اعداد α، $\alpha - ۱$ و $\alpha + ۱$ بر ۴ یا ۹ بخشپذیر نیست، u هیچیک از سه عنصر α، $\alpha - ۱$ یا $\alpha + ۱$ را عاد نمی کند که یک تناقض است.

(ب ٦) فرض کنیم αمولد گروه دوری F_q^* باشد، از آنجا که $F_q = F_p(\alpha)$، چند جمله‌ای می نیمال α روی F_p از درجهٔ $r = [F_q : F_p]$ است (در ضمن ملاحظه

می‌کنیم این واقعیت را ثابت کرده ایم که روی F_p و به طور مشابه روی هرهیأت متناهی چند جمله ای تحویل ناپذیر با درجهٔ دلخواه وجود دارد) اینک، هر عنصر $Gal(F_q : F_p)$ با مقدار آن در α مشخص می شود . اما برای هر $\sigma \in Gal(F_q : F_p)$، $\sigma(\alpha)$ باید مزدوج α باشد. بنابر این $Gal(F_q : F_p)$ خود ریختی فربینیوس از مرتبهٔ r است و این به علت آن است که $\alpha^{p^r} = \alpha$ و برای $s < r$ برابری $\alpha^{p^s} = \alpha$ وجود p^r ریشه برای معادلهٔ $x^{p^s} = x$ را در F_q ایجاب خواهد کرد که ممکن نیست.

(ب ۷) دو چند جمله ای متمایز با ضرایب در F_q و با در جه کمتر از q، دو تابع یکسان را نمایش نخواهند داد. زیرا در غیر این صورت تفاوت آن ها یک چند جمله ای ناصفر با درجه ای کمتر است، q ریشه در F_q خواهد داشت که ممکن نیست، اما تعداد چند جمله ای های متمایز در $F_q[x]$ و با درجهٔ کمتر از q بربر با q^q است. از طرف دیگر q^q تعداد توابع از F_q به F_q است. این ادعا، قسمت اول تمرین را ثابت می کند. اینک فرض کنیم R حلقه ای است که هر تابع $f : R \to R$ با یک چند جمله ای در $R[x]$ به دست می آید. ابتدا ملاحظه می کنیم کهR باید متناهی باشد، زیرا حتی اگر R شمارا متناهی باشد، مجموعه تمام توابع از R به خودش شمارا نیست. حال آن که مجموعه تمام چند جمله ای ها روی R شمارا است. در حالت کلی اگرعدد اصلی R را با $|R|$ نشان دهیم، مجموعه تمام توابع از R به R داری عدد اصلی $|R|^{|R|}$ و مجموعهٔ دوم دارای عدداصلی $\mathcal{N}_0|R|$ است و این دو عدد اصلی تنها هنگامی که R متناهی باشد می توانند برابر باشند. ادعا می کنیم که برای هر عنصر ناصفر $r \in R$، تابع $f_r : R \to R$ که با $x \to rx$ به دست می آید پوشا است. فرض کنیم $y \in R$. تابع

$$g_{r,y}(x) = \begin{cases} y & x = r \\ 0 & x \neq r \end{cases}$$

را در نظر می گیریم. بنابر این چند جمله ای $a_n x^n + \cdots + a_0 \in R[x]$ وجود دارد که $g_{r,y}$ با این چند جمله ای به دست می آید. به عبارت دیگر

$$a_n x^n + \cdots + a_0 = 0 \qquad , x \neq r \tag{۸.۱۴}$$

و

$$a_n r^n + \cdots + a_1 r + a_0 = 0 \tag{۱۹.۱۴}$$

اگر در (۸.۱۴) قرار دهیم $x = 0$ خواهیم داشت $a_0 = 0$. بنابر این از (۹.۱۴) داریم $r(a_n r^{n-1} + \cdots + a_1 = y$. این برابری ، ادعای ما را ثابت می کند. از آنجا که R متناهی است، نتیجه می گیریم که f_r یک به یک است. این بدان معنی است که $rx = 0$ اگر و تنها اگر $x = 0$. بنابر این R یک حوزهٔ صحیح متناهی و لذا یک هیأت است.(بنابر تمرین ۲.۰)

ب ۸ معادلهٔ داده شده را با ضرایب در F_7 در نظر می گیریم. این پرسش معادل این پرسش است که آیا معادلهٔ $\bar{2}x^2 + \bar{3}x + \bar{1} = 0$ در $\mathbb{F}_7$ دارای جواب است. اگر طرفین معادله را در $\bar{4}$ که وارون $\bar{2}$ در $\mathbb{F}_7$ است ضرب کرده آن را مربع کنیم به معادلهٔ $(x+\bar{6})^2 = \bar{4}$ دست می یابیم و چون $(\frac{4}{7}) = 1$ نتیجه می گیریم که x, y وجود دارند که در معادله صدق می کنند.

ب ۹ فرض کنیم معدلهٔ دیوفانتی داده شده دارای جواب (x, y) باشد، در صورت امکان، فرض کنیم $x \equiv 0 \pmod 2$، از این جا نتیجه می شود که $x^3 \equiv 0 \pmod 8$. بنابر این $y^2 \equiv 5 \pmod 8$. این همنهشتی نمی تواند برقرار باشد زیرا به سادگی ملاحظه می کنیم که مربع هر عدد صحیح باید بایکی از اعداد ۰ ، ۱ یا ۴ همنهشت باشد. بنابراین x فرد است. اگر $x \equiv 1 \pmod 4$، آن گاه $y^2 \equiv 2 \pmod 4$ که باز هم ممکن نیست. بنابر این x، به پیمانهٔ ۸، باید با یکی از اعداد ۳ یا ۷ همنهشت باشد، فرض کنیم $x \equiv 3 \pmod 8$، می توانیم بنویسیم $y^2 = x^3 + 45$ زیرا، $y^2 - 2.6^2 = x^3 - 27 = (x-3)(x^2+3x+9)$. اینک ملاحظه می کنیم که $x^2 + 3x + 9 \equiv 3 \pmod 8$ و لذا درای مقسوم علیه اولی به شکل $p \equiv \pm 3 \pmod 8$ است. این عدد اول، $y^2 - 2.6^2$ را عاد می کند و از این جا نتیجه می شود که $(2.6^2/p) = 1$ و لذا $(2/p) = 1$ که ممکن نیست، زیرا $p \equiv \pm 3 \pmod p$. آخرین امکان این است که $x \equiv 7 \pmod 8$. اینک $y^2 - 2.3^2 = x^3 + 27 = (x+3)(x^2-3x+9)$ و لذا دارای مقسوم علیه اولی به شکل $p \equiv \pm 3 \pmod 8$. بنابراین چنین نتیجه می گیریم که معادله دیوفانتی داده شده دارای جواب نیست.

۱.۸ حلقهٔ $\mathbb{Z}$ را به عنوان یک مدول روی خودش در نظر می گیریم. برای هر عدد صحیح n، مجموعهٔ تک عضوی $\{n\}$ به وضوح مستقل خطی است، اما اگر $n > 1$، $\{n\}$ نه پایه است ونه می توان آن را به یک پایه بسط داد. از طرفی p, q دو عدد اول متمایز در $\mathbb{Z}$ باشند، اعدادصحیح a, b وجود دارند به طوری که $ap + bq = 1$ و لذا ملاحظه می کنیم که مجموعهٔ $\{p, q\}$، $\mathbb{Z}$ را به عنوان یک مدول روی خودش تولید می‌کند. اما q, p مستقل خطی نیستند. بنابر این $\{p, q\}$ شامل هیچ پایه‌ای نیست.

۲.۸ (آ) فرض کنید M شامل یک پایهٔ S است، اگر S تهی باشد بنابر قرار داد M مدول آزاد $\{0\}$ است. پس فرض کنیم S ناتهی باشد. برای $s \in S$ ساده است که ملاحظه کنیم Rs یک R−مدول با R یکریخت است و M مجموع مستقیم دسته زیر مدول های $\{Rs\}_{s \in S}$ است. به عکس فرض کنیم $M = \oplus_{s \in S} R$. برای هر عضو $s \in S$ فرض کنیم α_s عنصر $\{r_i\}$ از $\oplus_{s \in S} R$ باشد که در آن $r_i = 0$. اگر $i \neq s$ و

$r_s = ۱$. در این صورت به سادگی مشاهده می کنیم که $\{\alpha_s : s \in S\}$ یک پایه برای M است .

(ب) فرض کنیم M یک ایدآل ماکسیمال R است. اینک M/AM یک فضای برداری روی هیأت $F = R/A$ است. اگر S یک پایه برای M باشد، آن گاه $\{s + AM : s \in S\}$ یک پایه برای M/AM است.

۳.۸ نتیجه را برای یک متغیر ثابت می کنیم. نتیجه کلی به طور بدیهی از استقرا نتیجه می شود. فرض کنیم R نویتری و A یک ایدآل در $R[x]$ است. آشکار است که دسته تمام ضرایب پیشرو تمام چند جمله ای ها در A یک ایدآل R است. این ایدآل را I می نامیم. از آنجا که R نویتری است، I با یک مجموعه متناهی مثلاً $\{r_۱, r_۲, \cdots, r_m\}$ تولید می شود. برای هر i، $۱ \leq i \leq n$ یک چند جمله ای مثلاً $f_i(x)$ با ضرایب پیشرو r_i انتخاب می کنیم. اگر d ماکسیمم درجه های f_i ها باشد، به سادگی دیده میشود که $A = B \cap A + A'$ که در آن B، $R-$ مدول تولید شده با $۱, x, \cdots, x^{d-۱}$ است و $A' \subset A$ ایدآل تولید شده با $\{f_۱(x), \cdots, f_m(x)\}$ می باشد. اینک به علت نویتری بودن $R-$مدول B، زیر مدول $B \cap A$ متناهی تولید شده است و لذا A نیز متناهی تولید شده می باشد.

۴.۸ اگر ممکن باشد، فرض کنیم R نویتری نیست. در این صورت اگر S مجموعه تمام ایدآل‌های متناهی تولید نشده R را نشان دهد، $S \neq \emptyset$. با بکار گیری لم تسورن عنصر ماکسیمال Tی S به دست می آید. این ایدآل نمی تواند اول باشد، بنابر این $a, b \in R$ وجود دارد که $ab \in T$، اما نه a و نه b در T نیستند. اینک $T + bR > T$ و به موجب ماکسیمال بودن T، $T + bR$ متناهی تولید شده است. فرض کنیم $T + bR$ با $\{b_۱, b_۲, \cdots, b_s\}$ تولید می شود. فرض کنیم برای $۱ \leq i \leq s$، $b_i = t_i + a_i b$ که در آن $t_i \in T$ و $a_i \in R$. اینک ایدآل $(T : bR) = \{e \in R : rb \in T\}$ در نظر می گیریم. به وضوح $t \subset (T : bR)$ همچنین $a \in (T : bR)$، بنابر این $T < (T : bR)$. باز هم به علت ماکسیمال بودن T، $(T : bR)$ متناهی تولید شده است. اگر مجموعهٔ $\{c_۱, c_۲, \cdots, c_l\}$، $(T : bR)$ را تولید کند و قرار دهیم $d_i = c_i b \in T$، آن گاه T با مجموعهٔ $\{t_۱, t_۲, \cdots, t_s, d_۱, d_۲, \cdots, d_l\}$ تولید شده است که متناقض با فرض $T \in S$ است. بنابر این $S = \emptyset$.

۶.۸ فرض کنیم V^* فضای دوگان V، شامل تمام شکل های خطی بر V باشد. به سادگی می توان مشاهده کرد که V^* هم یک فضای برداری با بعد n روی K است. در واقع اگر $v_n, \cdots, v_۲, v_۱$ یک پایه برای فضای V باشد عناصر f_j، $j = ۱, ۲, \cdots, n$ در V^* که در آن $f_j(v_i) = \delta_{ij}$ تشکیل یک پایه می دهند (که

فضای دوگان پایه $v_1, v_2, \cdots, v_n$ از V^* است.) تابع $\phi : V \to V^*$ که در آن $b \in V$ و $\phi(b)$ در V^* همریختی تعریف شده با $x \to B(x,b)$ است را در نظر می گیریم. به وضوح ϕ یک همریختی است. از آنجا که B ناتبهگون است، ϕ یک به یک است. بادر نظر گفتن بعد، ملاحظه می کنیم که ϕ باید پوشا باشد. اگر $w_1, w_2, \cdots, w_n$ یک پایه برای V باشد، فرض کنیم f_j دوگان توصیف شدهٔ فوق باشد. برای هر j، $w'_j \in V$ وجود دارد که $\phi(w'_j) = f_j$. اکنون $B(w_i, w'_j) = f_j(w_i) = \delta_{ij}$.

۲.۱۰) فرض کنیم $n = ۴k + ۱$. حال $\alpha = \frac{۱+\sqrt{n}+n}{۲}$ یک عنصر در هیأت خارج قسمتهای حلقهٔ مفروض است. داریم

$$\alpha^۲ = \frac{۱ + ۲\sqrt{n} + n}{۴} = \frac{۲\sqrt{n} + ۴k + ۲}{۴} = k + \alpha$$

لذا $\alpha^۲ - \alpha - k = ۰$. از این رو عنصر α در هیأت خارج قسمتهای حلقهٔ داده شده $R = \mathbb{Z} + \mathbb{Z}\sqrt{n}$ وجود دارد به طوری که α روی R صحیح است. و $\alpha \notin R$ بنابر تمرین ۱.۱۰ R یک ح ت ی نیست.

(**پ ۱**) فرض کنیم π یک عدد اول گاوسی است که $a + ib$ را در حلقهٔ اعداد گاوسیِ $\mathbb{Z}[i]$ عاد می کند. اکنون π، $c = a^۲ + b^۲ = (a+ib)(a-ib)$ را به تعدادی زوج مرتب عاد می کند. اگر π هم $a + ib$ و هم $a - ib$ را در $\mathbb{Z}[i]$ عاد کند، آن گاه π، $۲a$ را در $\mathbb{Z}[i]$ عاد می کند. از آنجا که c, b, a، هیچ عامل مشترکی ندارند، c باید به ازای اعداد صحیحی مانند n, m برابر با $m(۲a) + nc = (۲a, c) = ۱$ باشد. بنابر این π، $m(۲a) + nc = ۱$ را در $\mathbb{Z}[i]$ عاد می کند. که بافرض این که π یک عدد اول گاوسی است تناقض دارد.

پ۲) فرض کنیم $x^۲ + y^۲ = z^۲$ و z, y, x دو به دو نسبت به هم اول باشند. (اگر تمام چنین جوابهایی که جواب اولیه نامیده می شوند، یافت شوند، سایر جواب ها به شکل tz, ty, tx هستند که $t \in \mathbb{Z}$) در $\mathbb{Z}[i]$ داریم $(x+iy)(x-iy) = Z^۲$. از آنجاکه $\mathbb{Z}[i]$ یک ح ت ی است به موجب تمرین پ۱، $x + iy$ به شکل $u(c+id)^۲$ است که u یک یکه در $\mathbb{Z}[i]$ و d, c اعدادصحیح اند. از آنجا که تنها یکه های $\mathbb{Z}[i]$ عبارتند از ۱، ۱−، i، -i ، داریم

$$x = +(c^۲ - d^۲) \ , \ y = +۲cd \ , \ z = \pm(c^۲ + d^۲) \qquad (۱۰.۱۴)$$

شرط های موجود بر z, y, x ایجاب می کند که d, c نسبت به هم اول و d, c هر دو با هم فرد نیستند. به عکس با چنین انتخابی از d, c جوابهای $x^۲ + y^۲ = z^۲$ در (۱۰.۱۴) به دست می آیند.

پ۴) از آنجا که $N(a+bw) = a^{۲} - ab + b = (a+bw)(\overline{a+bw})$، ملاحظه می کنیم که برای دو عنصر θ, δدر $\mathbb{Z}[w]$، $N(\delta\theta) = N(\delta)N(\theta)$. بافرض این که $\alpha, \beta \in \mathbb{Z}[w]$ و $\alpha \neq ۰$ و ملاحظه این که $\alpha\bar{\alpha} \in \mathbb{Z}$، داریم $\beta/\alpha = (\beta\bar{\alpha})/(\alpha\bar{\alpha}) = r_{۱} + r_{۲}w$ که در آن r_iها در Q اند. اعداد صحیح $m_{۲}, m_{۱}$ وجود دارند به طوری که برای هر $i = ۱, ۲$، $|r_i - m_i| \leq ۱/۲$. اینک اگر بنویسیم $k = m_{۱} + m_{۲}w$، داریم

$$N(\beta/\alpha - k) = (r_{۱} - m_{۱})^{۲} - (r_{۱} - m_{۱})(r_{۲} - m_{۲}) + (r_{۲} - m_{۲})^{۲} < ۱.$$

بنابر این با نوشتن $\rho = \beta - k\alpha$، اگر $\rho \neq ۰$، آن گاه

$$N(\rho) = N(\alpha.(\beta/\alpha - k)) = N(\alpha)N(\beta/\alpha - k) < N(\alpha)$$

(ت) قسمت دوم را انجام می دهیم، فرض کنیم q عدد اول گویایی باشد به طوری که $q \equiv ۱ \pmod{۳}$ داریم

$$(-۳/q) = (-۱)^{\frac{q-۱}{۲}}(q/۳)(-۱)^{\frac{q-۱}{۲}\frac{۳-۱}{۲}} = ۱$$

بنابر این $n \in \mathbb{Z}$ وجود دارد به طوری که $n^{۲} \equiv -۳ (modq)$. این به آن معنی است که q، $(n + \sqrt{-۳})(n - \sqrt{-۳}) = (n + ۱ + ۲w)(n - ۱ - ۲w)$ را عاد می‌کند. از آنجا که $۲/q \notin \mathbb{Z}$ چنین نتیجه می گیریم q هچیک از عامل های $(n + ۱ + ۲w)$ و $(n - ۱ - ۲w)$ را عاد نمی کند. بنابر این q در $\mathbb{Z}[w]$ اول نیست. فرض کنیم α یک نا یکه باشد که q را در $\mathbb{Z}[w]$ عاد میکند در این صورت $N(\alpha)$، $q^{۲}$ را در $\mathbb{Z}$ عاد می کند. اگر $N(\alpha) = q^{۲}$، α یک وابستهٔ q است. بنابر این اگر $q = \alpha\alpha'$، که در آن نه α و نه α' یکه نیستند، آن گاه تنها امکان این است که $q = N(\alpha) = \alpha\bar{\alpha}$.

(ث) در اتحاد $x^{۲} + x + ۱ = (x - w)(x - w^{۲})$ قرار دهید $x = ۱$. داریم $(۱ - w)^{۲} = -w^{۲}(۱ - w)^{۲} = ۳$. از این جا نتیجه می شودکه $N(۱ - w^{۲}) = ۹$ و لذا $(۱ - w)$ اول است.

۱.۱۱ به سادگی دیده می شود که A' یک R–مدول است. از آنجا که A یک ایدآل کسری است، A' ناصفر است. همچنین $r \in R$ وجود دارد که $rA \subset R$. بنابر این اگر عنصر ناصفر x در A را انتخاب کنیم rx یک عنصر ناصفر R است. ازآنجا که R یک R–مدول است، rx هم به A تعلق دارد و بنابر این برای هر $y \in A'$، $rxy \in R$. بنابر این عنصر ناصفر rx در R را یافتیم که $rxA' \subset R$. بنابر این A' یک ایدآل کسری است.

۳.۱۱ ملاحظه می کنیم که P^n+aR یک اید آل است که شامل P^n بوده و در P مشمول نیست و باید برابر با R باشد

۵.۱۱ فرض کنیم $\wp_1,\wp_2,\cdots,\wp_n$ تمام اید آل های متمایز حوزهٔ ددکیند R باشد. عنصر $x_j\in\wp_j\setminus\wp_j^2$ را برای $1\leq j\leq n$ انتخاب می کنیم بنابر قضیه باقی مانده چینی برای $1\leq j\leq m$، $y_j\in R$ وجود دارد که

$$y_j\equiv x_j(mod\wp_j^2)$$

و برای

$$y_j\equiv 1(mod\wp_i)\ \ ,\ \ i\neq j.$$

پس برای هر $1\leq j\leq n$، داریم $y_jR=\wp_j$. از آنجا که تمام ایدال های اول اصلی اند، هر اید آل نیز یک اید آل اصلی و R یک ح ت ی است.

۶.۱۱ از قضیه ۳.۴ می دانیم که هر ح ا ص یک ح ت ی است. برای حوزه ددکیند R این نتیجه از این واقعیت به دست می آید که در سطح اید آل ها یک تجزیه یکتا وجود دارد. بنابر این اگر ممکن باشد، فرض کنیم R یک حوزهٔ ددکیند باشد که یک ح ت ی است اما ح اص نیست. حال، تمام ایدال های R نمی توانند اصلی باشند، فرض کنیم P یک اید آل اول و نا اصلی R است. قرار می دهیم

$S=\{I$ یک اید آل ناصفر R است به طوری که PI اصلی نیست $:I\}$

فرض کنیم $0\neq\alpha\in P$. در این صورت $\alpha R\subset P$ و در این صورت اید آل ناصفر I وجود دارد به طوری که $\alpha R=PI_1$. بنابر این S ناتهی است و لذا شامل یک عنصر ماکسیمال مانند M است. فرض کنیم $PM=\beta R$. ادعا می کنیم که β تحویل ناپذیر است. اگر $\beta=\gamma\delta$، آن گاه $\beta R=(\gamma R)(\delta R)$. بنابر این P، γR یا δR را عاد می کند. اگر P، γR را عاد کند، آن گاه به ازای یک اید آل J که M را عاد می کند، $\gamma R=PJ$. ماکسیمال بودن M نتیجه می دهد که $M=J$. بنابر این $\gamma R=R$ و لذا δ یکه است. به طور مشابه اگر P، δR را عاد کند، آن گاه γ یکه است. این استدلال ادعادرا ثابت می کند. عناصر $\theta_1\in R\setminus\beta R$ و $\theta_2\in M\setminus\beta R$ را انتخاب می کنیم. در این صورت $\theta_1\theta_2\in\beta R$ اما $\theta_1\notin\beta R$ و $\theta_2\notin\beta R$ که به آن معنی است که $\beta|\theta_1\theta_2$، اما $\beta\nmid\theta_1$و $\beta\nmid\theta_2$. که یک تناقض است، زیراح ت ی بودنِ R نتیجه می دهد که هر عنصر تحویل ناپذیر باید اول باشد.

۱.۱۲ کافی نشان دهیم که $N(AP_1)=N(A)N(P)$ که در آن P یک اید آل ماکسیمال O_k است. اگر S یک مجموعهٔ متناهی باشد، تعداد عناصر آن را با $|S|$

نشان می دهیم. داریم

$$|\mathbf{O}_K/AP| = |\mathbf{O}_K/A|.|A/AP|$$

اینک A/AP یک $\mathbf{O}_K$– مدول است که با P پوچ می شود و لذا یک فضای برداری رویِ $\mathbf{O}_K/P$ است. یک فضای سرهٔ این فضای برداری به شکل A'/AP است که در آن A' یک ایدآل $\mathbf{O}_K$ است به قسمی که $AP < A' < A$. از تذکر ۵.۱۱ به ازای یک ایدآل $B \neq \mathbf{O}_K$ داریم $A' = AB$. از آنجا که $AP < A'$ چنین ایدآل B وجود ندارد. بنابراین A/AP یک فضای برداری با بعدِ ۱ روی $\mathbf{O}_K/P$ است و این نتیجه می دهد که $|A/AP| = |\mathbf{O}_K/P|$. بنابراین از ۱۱.۱۴ نتیجه می شود که $|\mathbf{O}_K/AP| = |\mathbf{O}_K/A|.|\mathbf{O}_K/P|$.

۲.۱۲ فرض کنیم A یک ایدآل $\mathbf{O}_K$ است به قسمی که $N(A) \leq m$. فرض کنیم $A = P_1^{r_1}P_2^{r_2}\cdots P_r^{r_l}$ تجزیهٔ A به حاصلضرب ایدآل های اولِ $\mathbf{O}_K$ باشد. از آنجا که $N(P_1) \geq 2$، به موجب تمرین ۱.۱۲ شرط $N(A) \leq m$ نتیجه می دهد که r_iها از بالا کران دار هستند. حال ملاحظه می کنیم که ایدآل اول P_i که در تجزیهٔ A ظاهر می شود شامل عدد اول $p_i < m$ است. این بدان علت است که نرم یک ایدآل اول شامل عدد اول گویای p، به ازای یک $1 \leq d \leq n$ برابر با p^d است که در آن n درجهٔ k است. از طرفی ایدآل اولی به جز n ایدآل اول $\mathbf{O}_K$ که شامل $\mathbf{O}_K$ باشد وجود ندارد. بنابراین با شرط $N(A) \leq m$، در تجزیهٔ ایدآل Aیِ $\mathbf{O}_K$، تنها تعداد متناهی ایدآل اول، با کران یکنواخت، می تواند وجود داشته باشدو نتیجه محقق است.

۳.۱۲ بردار v متعلق به مشبکه H به شکل زیر است

$$r_1v_1 + r_2v_2 + r_3v_3 + r_4v_4 = (r_1m + r_3a + r_4b, r_2m + r_3b - r_4a, r_3, r_4)$$

که در آن r_iها در $\mathbb{Z}$ هستند.

از آنجا که $a^2 + b^2 + 1 \equiv 0 \pmod m$، به سادگی ملاحظه می کنیم که عدد صحیح $|v|^2$ مضربی از m است.

اینک $\mathcal{B}$ یک جسم محدب متقارن، دورِ مرکز است و حجم آن برابر است با $2\pi^2m^2 > 2^4m^2 = 2^4\nu(H)$. بنابراین بنابر نتیجه ۱.۸.۱۲ $\mathcal{B}$ شامل یک نقطه ناصفر، مانند $u = (l_1, l_2, l_3, l_4)$ است.

اکنون $2m > |u| > 0$ و $|u|^2$ یک مضرب m است، که از آنجا لازم می آید $|u|^2 = m$، یعنی $l_1^2 + l_2^2 + l_3^2 + l_4^2 = m$. سرانجام از آنجا که $l_1^2 + l_2^2 + l_3^2 + l_4^2$ نتیجه می دهد که $2m = (l_1 + l_2)^2 + (l_1 - l_2)^2 + (l_3 + l_4)^2 + (l_3 + l_4)^2$ و نتیجه محقق است.

۵.۱۲ در اینجا با نمادهای قضیه ۱۰.۱۲ داریم $r_۲ = ۱$ و $n = ۲$ و از تذکر ۲.۱۳ داریم $|d(K)| = ۲۰$. بنابراین

$$(\frac{۴}{n})^{r_۲}\frac{n!}{n^n}|d(K)|^{۱/۲} = \frac{۴\sqrt{۵}}{\pi} < ۳۰$$

بنابراین کافی است مقسوم علیه های اولِ $۲\mathbf{O}_K$ را بیابیم، حال، $۲\mathbf{O}_K = (۲, ۱ + \sqrt{۵})^۲$. به موجب تذکر ۲.۹، ایدآل $(۲, ۱ + \sqrt{۵})$ اصلی نیست. مستقیماً نیز می توان این ادعا را ثابت کرد. اگر $(۲, ۱ + \sqrt{-۵})$ اصلی و مثلاً برابر با (α) باشد، می نویسیم $\alpha = a + b\sqrt{-۵}$ و خواهیم داشت $(N_K(\alpha)) = N((\alpha)) = ۲$ که از آن نتیجه می شود $a^۲ + ۵b^۲ =^+_- ۲$ که ممکن نیست. بنابراین عدد ردهٔ $\mathbb{Q}(\sqrt{-۵})$ برابر با ۲ است.

ت۱ فرض کنیم $A = \rho_۱^{m_۱}\rho_۲^{m_۲}\cdots\rho_r^{m_r}$ و $B = \rho_۱^{n_۱}\rho_۲^{n_۲}\cdots\rho_r^{n_r}$ که در آن ρ_iها ایدآل های اول و m_i، n_iها اعداد صحیح نامنفی اند. برای هر $۱ \leq i \leq r$،

$$\alpha_i \in (\rho_۱^{m_۱+۱}\cdots\rho_{i-۱}^{m_{i-۱}+۱}\rho_i^{m_i+۱}\rho_{i+۱}^{m_{i+۱}+۱}\cdots\rho_r^{m_r+۱})$$

را چنان انتخاب می کنیم که

$$\alpha_i \notin (\rho_۱^{m_۱+۱}\cdots\rho_{i-۱}^{m_{i-۱}+۱}\rho_i^{m_i+۱}\rho_{i+۱}^{m_{i+۱}+۱}\cdots\rho_r^{m_r+۱})$$

اگر قرار دهیم $w = \alpha_۱ + \cdots + \alpha_r$، نتیجه می گیریم که $A = (AB, (w))$.

ت۲ فرض کنیم A یک ایدآل $\mathbf{O}_K$ است. اینک $A^{-۱}$ یک ایدآل کسری $\mathbf{O}_K$ است و لذا $\alpha \in \mathbf{O}_K \neq \alpha$ ۰ وجود دارد که $\alpha A^{-۱} \subset \mathbf{O}_K$ اگر قرار دهیم $B = \alpha A^{-۱}$، داریم $AB = \alpha\mathbf{O}_K$ بنابراین به موجب تمرین ت۱، $w \in \mathbf{O}_K$ وجود دارد که بزرگترین مقسوم علیه مشترک AB و w برابر با A شود. به عبارت دیگر (تذکر(۵.۱۱) را ببینید) $A = AB + w\mathbf{O}_K = \alpha\mathbf{O}_K + w\mathbf{O}_K$.

ت۳ چند جمله ای می نیمال ξ_p روی $\mathbb{Q}$ برابر با $x^{p-۱} + x^{p-۲} + \cdots + ۱$ است، بنابراین براي $j = ۱, ۲, \cdots, p-۱$، $(Tr(\xi_p^j) = Tr_{K/\mathbb{Q}}(\xi_p) = -۱)$ از طرفی $Tr(۱) = p - ۱$ بنابراین

$$Tr(۱-\xi_p) = Tr(۱-\xi_p^۲) = \cdots = Tr(۱-\xi_p^{p-۱)=p} \qquad (۱۲.۱۴)$$

اگر قرار دهیم $x = y + ۱$،

$$\frac{x^{p-۱}}{x-۱} = \frac{(y+۱)^p - ۱}{y} = y^{p-۱} + py^{p-۲} + \cdots + p \qquad (۱۳.۱۴)$$

و لذا

$$N(\xi_p - ۱) = (-۱)^{p-۱}p$$

که نتیجه می دهد

$$N(\text{۱}-\xi_p)=p$$

از این قرار

$$(\text{۱}-\xi_p)(\text{۱}-\xi_p^{\text{۲}})\cdots(\text{۱}-\xi_p^{p-\text{۱}})=p \qquad (\text{۱۴.۱۴})$$

اکنون (۱۴.۱۴) نتیجه می دهد که p به ایدآل اصلیِ $(\text{۱}-\xi_p)\mathbf{O}_K$ تعلق دارد و لذا

$$p\mathbb{Z}\subset(\text{۱}-\xi_p)\mathbf{O}_K\cap\mathbb{Z}$$

اگر $p\mathbb{Z}\neq(\text{۱}-\xi_P)\mathbf{O}_K\cap\mathbb{Z}$، آن گاه به علت این که $p\mathbb{Z}$ یک ایدآل ماکسیمال $\mathbb{Z}$ است، داریم

$$\mathbb{Z}=(\text{۱}-\xi_p)\mathbf{O}_K\cap\mathbb{Z}$$

و لذا

$$\text{۱}\in(\text{۱}-\xi_p)\mathbf{O}_K$$

بنابراین $\xi_p-\text{۱}$ یک یکهٔ $\mathbf{O}_K$ است. بنابراین $N(\text{۱}-\xi_p)=\pm\text{۱}$. این برابری با (۱۴.۱۴) در تناقض است. بنابراین

$$p\mathbb{Z}=(\text{۱}-\xi_p)\mathbf{O}_K\cap\mathbb{Z} \qquad (\text{۱۵.۱۴})$$

این برابری، قسمت (آ) را ثابت می کند.

فرض کنیم y یک عنصر $\mathbf{O}_K$ است. یک زوج مزدوج $y(\text{۱}-\xi_p)$ به ازای یک $\text{۱}\leq j\leq p-\text{۱}$ به شکل $y_j(\text{۱}-\xi_p^j)$ است که در آن y_j مزدوج y می باشد. از آنجا که $\text{۱}-\xi_p^j=(\text{۱}-\xi_p)(\text{۱}+\xi_p)(\text{۱}+\xi_p+\cdots+\xi_p^{j-\text{۱}})$، نتیجه می گیریم که

$$Tr(y(\text{۱}-\xi_p))\in p\mathbb{Z} \qquad (\text{۱۶.۱۴})$$

اکنون به اثبات قسمت (پ) می پردازیم. داریم

$$\alpha(\text{۱}-\xi_p)=a_\circ(\text{۱}-\xi_p)+a_\text{۱}(\xi_p-\xi_p^{\text{۲}})+\cdots+a_{p-\text{۲}}(\xi_p^{p-\text{۲}}-\xi_p^{p-\text{۱}})$$

بنابراین به موجب (۱۲.۱۴)، $Tr(\alpha(\text{۱}-\xi_p))=a_\circ Tr(\text{۱}-\xi_p)=a_\circ p$. از این رو بنابر قسمت (۱۶.۱۴) داریم $a_\circ p\in p\mathbb{Z}$ که آن هم نتیجه می دهد $a_\circ\in\mathbb{Z}$. اینک $a_\text{۱}\xi_p+\cdots+a_{p-\text{۲}}\xi_p^{p-\text{۲}}\in\mathbf{O}_K$. با ضرب طرفین در $\xi_p^{p-\text{۱}}=\xi_p^{-\text{۱}}$ نتیجه می گیریم که $a_\text{۱}+\cdots+a_{p-\text{۲}}\xi_p^{p-\text{۳}}\in\mathbf{O}_K$. با ادامهٔ این کار نتیجه می گیریم که $a_\text{۱}\in\mathbb{Z}$. با تکرار این استدلال نتیجه می گیریم که برای هر i، $a_i\in\mathbb{Z}$.

ت۴ فقط به حل قسمت (چهار) می پردازیم. فرض کنیم $p|f(a)$، بنابر قسمت (سه) $a^m \equiv ۱ \pmod p$ و برای هر مقسوم علیه سرهٔ m، $a^r \equiv ۱ \pmod{}$. با در نظر گرفتن a بع عنوان یک عضو F_p^* نتیجه می گیریم $m|(p-۱)$.

به عکس، اگر $p \equiv ۱ \pmod m$، از آنجا که F_p^* دوریِ از مرتبهٔ $p-۱$ است یک عنصرa که مرتبهٔ ضربی آن به پیمانه p برابر با m باشد وجود دارد. بنابر این بنابر قسمت (سه) $p|f(a)$.

اینک فرض کنیم که یک مجموعهٔ (احتمالاً تهی) از تعدادی متناهی عدد اولِ $S = \{p_۱, p_۲, \cdots, p_r\}$ در تصاعد حسابی $m, ۱+۲m, \cdots$ وجود داشته باشد.می نویسیم $s = mp_۱p_۲\cdots p_r$ (اگر S تهی باشد،داریم $s = m$). فرض کنیم t یک عدد صحیح دلخواه است. در این صورت $f(st) \equiv \pm ۱ \pmod s$. این همنهشتی نتیجه می دهد که برای هر $i = ۱, ۲, \cdots, r$، $f(s) = \pm ۱ \pmod p)_i$ و $f(st) = \pm ۱$ $(\bmod m)$. اگر $t \to \infty$، داریم $f(st) \to \infty$. بنابر این می توان t را چنان انتخاب کرد که $f(st) \neq \pm ۱$، اینک فرض کنیم P عدد اول گویایی است که $f(st)$ را عاد می کند. در این صورت بنابر قسمت اول، $P \equiv ۱ \pmod m$. هم اکنون ملاحظه کردیم که هیچ یک از p_i ها، $f(st)$ را عاد نمی کنند بنابر این P عدد اولی به جز p_i هاست که $P \equiv ۱ \pmod m$.

۱.۱۳ K اقلیدسی نرم است اگر به ازای $a, b \in \mathbf{O}_K$ و b ناصفر باشد، $q \in \mathbf{O}_K$ وجود داشته باشد که

$$|N_{K/Q}(a - qp)| < |N_{K/Q}(b)|$$

از آنجا که نرم ضربی است شرط فوق را می توان به شکل زیر نوشت

$$|N_{K/Q}(ab^{-۱} - q)| < ۱.$$

کتابنامه

AM 1969. M F. Atiyah and I. G. Macdonald, *Introduction ton Commutatiiv Algebra,* Addison-Wesley.

Ar 1994. Michael Artin, *Algebra,* Preintic Hall.

Br 1993.J. W. Bruce, *A Really Trivial proof of the Lucas-Lehmer Test,* Amer. Math. Monthly, Vol. 100, 370-371.

Cl 1994. D. A Clark, *A quadratic field which is Educlidean but not norm-Euclidean,* Manuscripta math., Vol. 83, 327-330.

DPS 1996. C. Ding, D.Pei, A. Salomaa, *Chinese Reminder Theorem-Applications In Computing, Coding, Cryptography,*World Scientific.

Du 1969. U. Dudley, *Elementry Number Thery,* W. H. Freeman and Comapny, San Francisco.

EM 1999. Jody Esmonde and M. Ram Murty, *Problems in Algebaric Number theory,* Springer-Verlage.

GMM 1987. R. Gupta, M. Murty, V. Murty,, *The Euclidean Algorithm for S-integers,* canada. Math. Soc. Conference Proce., Vol. 7, 189-201.

HW 1981. g.H Hadly & E. M. wright, *An introduction to the theory of numbers, 5th edition,* Oxford University Press.

He 1975. I. N. Herstein, *Topics in Algebra, 2nd edition,* Wiley,New York.

Hu 1982. L. K. Hua, *Introduction to Number Theory,* Springer-Verlage.

IR 1982. Kenneth Ireland and Michael Rosen, *An Introduction to Modern Number Theory,* Springer-Verlage.

La 1993. Serge Lange, *Algebra,* 3rd edition, Addison-Wesley.

Le 1995. Franz Lemmermeyer, *The Euclidean algorithm in algebraic number field,* Expo. Math. Vol. 13, 385-416.

LN 1983. R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of mathematics and its aoolications,* Vol. 20., Addison-Wesley.

Ma 1977. Daniel A. Marcus, *Number Fieldes* Springer-Verlage.

Na 1990. W. narkiewicz, *elementary and Analytic theory of Algebraic Numbers,* 2ed edition, Springer-Verlage.

NRRL 1966. raghavan narasimhan, S. Raghavan, S.S. rangachari and Sunder Lal, *Algebraic Number Theory,* Tata Institute.

Ro 1988. M¿ I. rosen, *A Proof of the Lucas-Lehmer Test,* Amer. Math. Monthly, Vol. 95, 855-856.

Sa 1967. P. Samuel, *theorie Algebraique des Nombers,* Hermann & Cie.

Sa 1968. P. Samuel, *Unique Factorization,* amer. Math. Monthly, Vol. 75, 947-952.

Sp 1994. Karlheinz Spindler, *abstract Algebra with applications, Vol. II,Marcel Dekker.*

Wa 1982. *Lawrence C. Washington,* Introduction to Cyclotomic Fields, *Springer-Verlage.*

We 1973. *P. J. Weinberger,* on Eucliden rings of algebraic integers, *Proc. Symp. Pure Math., Vol. 24, 321-332.*

Wy 1972. *B. F. Wyman,* What is a reciprocity law?, *Amer. Math. Monthly, Vol. 79, 571-587.*

نمایه

واژه‌نامهٔ انگلیسی به فارسی

اثر .... trace
اعداد اول گاوسی .... Gaussian primes
ایدآل .... ideal
ایدآل صحیح .... integral ideal
ایدآل کسری .... fractional ideal
باقی مانده درجه دوم .... quadratic residue
بستار جبری .... algebraic clouser
بستار صحیح .... integral clouser
تابع زتای ریمان .... Riemann zeta function
تحویل‌ناپذیر .... irreduable
توسیع جبری .... algebraic extention
چند جمله ای تکین .... monic polynomial
حلقه نوتری .... Noetherian ring
حوزه ددکیند .... Dedekind domainm
دنباله دقیق .... exact sequenc
رادیکال جیکوبسن .... Jacobson radical
شاخص اویلر .... Euler totient
ضربی .... muliplicative
قانون تقابل درجه دوم .... quadratic reciproaty low
قضیه باقی مانده چینی .... Chaines remainder theorem
قضیه پایه هیلبرت .... Hilbert's theorem
گروه رده .... class group
مبین .... discriminant
مدول وفادار .... faithful modul
مشبکه .... lattic
معیار ایزنشتاین .... eisenstin criterion
منشعب شده .... ramified
نامانده درجه دوم .... quadratic nonresidues