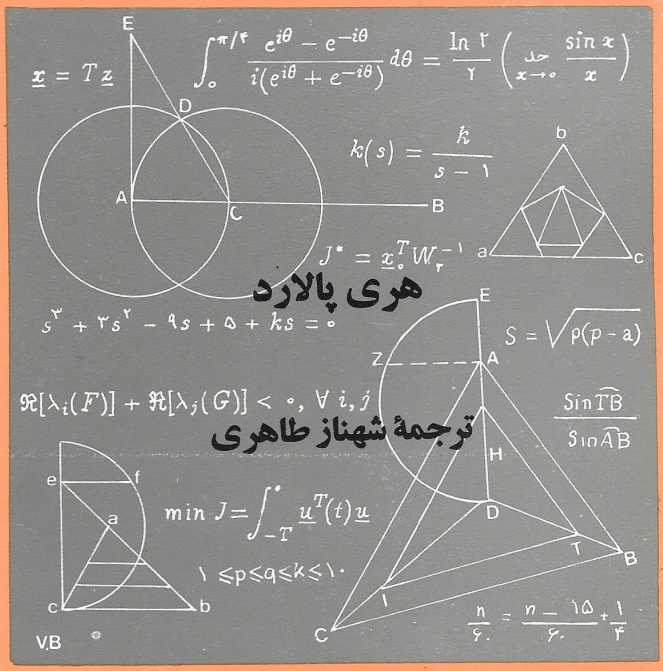
نظریه جبری اعداد



مجموعهٔ علوم ریاضی

هری پالارد

نظریهٔ جبری اعداد

ترجمهٔ شهناز طاهری

تهران ۱۳۷۶

فهرست مطالب

مقدمه

بشر همراه با شناخت اعداد به خواص آن نیز پی‌برده است. درواقع، نظریه اعداد را می‌توان علم مطالعه اعداد و روابط بین اعداد دانست.

مسائلی که در طی قرون به‌وسیله علاقه‌مندان مطالعهٔ خواص اعداد معرفی شده‌اند، پایه‌های اصلی نظریه اعداد مدرن را می‌سازند. این مسائل که به‌وسیله محققان و علاقه‌مندان مورد مطالعه قرار گرفته است، بتدریج به شکل‌گیری روش‌هایی که امروز در نظریه اعداد وجود دارند انجامیده است. از طرفی رشد علمی قرون هفدهم و هجدهم منجر به پیشایش شاخه‌های مختلف آنالیز، هندسه، و جبر گردید. این علوم جدید بنوبه خود بر تلاش‌هایی که برای حل مسائل نظریه اعداد صورت می‌گرفت تأثیر گذارد و باعث به‌وجود آمدن شاخه‌های مختلف نظریه اعداد ــ نظریه جبری اعداد، نظریه آنالتیک اعداد، و نظریه هندسی ــ اعداد گردید. از جهت دیگر با رشد سریع مهندسی، فیزیک، و ریاضیات در نیمه دوم قرن جاری شاهد پیشرفت سریع علوم محاسبات الکترونیکی و به‌کار گرفتن کامپیوتر در محاسبات با اعداد بزرگ هستیم. تمام این روش‌ها را می‌توان در خدمت حل مسائل کلاسیک قرار داد، که یا به حل

آنها دست می‌یابیم یا باعث کشف مسائل دیگری می‌شویم.

نوشتن یک عدد به حاصلضرب عوامل اولش مفهومی است که از یونان باستان به ارث برده‌ایم. با نگاهی مدرن این موضوع بدیهی را می‌توان در قالب نظریه جبری حلقه‌های جابجایی و ایده‌آل‌ها قرار داد. تجزیه یک عدد صحیح و مثبت به عوامل اول آن، معادل است با تجزیه یک ایده‌آل در حلقه اعداد صحیح به ایده‌آل‌های اولش. این تشابه را می‌توان سرآغاز نظریه جبری اعداد کلاسیک دانست. به‌طور کلی‌تر می‌توان گفت که روش‌های کلاسیک در نظریه جبری اعداد بر پایه خواص حلقه‌ها و ایده‌آل‌ها می‌باشد. این روش‌ها خصوصاً برای مطالعه معادله معروف فرما (Fermat) $x^n+y^n=z^n$، توسط کومر (Kummer) در قرن نوزدهم به‌کار گرفته شد. گرچه روش‌های فوق نتوانستند این مسأله معروف را حل کنند، ولی بنیان نظریه جبری اعداد را پایه‌گذاری کردند.

با در نظر گرفتن کمبود کتابهای فارسی در نظریه اعداد خصوصاً نظریه جبری اعداد و شاخه‌های دیگر نظریه اعداد، کتاب مختصر نظریه جبری اعداد نوشته شده به‌وسیله هری پالاردکه نسخه اول آن پیش از ۴ دهه قبل نوشته شد. می‌تواند شروع خوبی برای علاقه‌مندان به نظریه جبری اعداد باشد تا با روش‌های کلاسیک آشنا شوند.

صلاح‌الدین شکرانیان
دانشکده علوم ریاضی ـ دانشگاه صنعتی شریف
اسفند ۷۳ ـ تهران

فصل ۱

قابلیت تقسیم

۱. **یگانگی تجزیه.** موضوع بحث نظریهٔ اعداد مقدماتی، مطالعهٔ اعداد صحیح ۰ ، ۱± ، ۲± ، ... است. برخی از آنها، یعنی اعداد اول[1]، اهمیتی خاص دارند. آنها اعدادی غیر از ۰ و ۱±، در واقع، اعدادی چون m، هستند که عاملی غیر از ۱± و m± ندارند. به عنوان مثال، اعداد ۲، ۳، ۵- اول هستند، در صورتی که ۲×۳ = ۶ و $۳^۲$ = ۹ اول نیستند. اهمیت اعداد اول، در این است که آنها می‌توانند همراه ۰ و ۱±، همهٔ اعداد صحیح دیگر را بسازند. قضیهٔ اساسی حساب، بیانگر این موضوع است که *هر عدد صحیح بزرگتر از ۱ صرف نظر از ترتیب، تنها و تنها به یک طریق قابل تجزیه به حاصل‌ضرب اعداد اول مثبت است.* از این رو به عنوان مثال :

$$۱۲ = ۲^۳ \times ۳ = ۲ \times ۳ \times ۲ = ۳ \times ۲^۲$$

تنها صورتهای تجزیهٔ ۱۲ به عامل‌های اول مثبت هستند و همهٔ آنها دقیقاً عامل‌هایی یکسان ایجاد می‌کنند. در واقع، تنها تفاوت میان آنها ترتیب

---

1) *Prime*

قرار گرفتن عامل‌هاست.

در این فصل، ما اثباتی از قضیهٔ اساسی حساب را ارائه خواهیم کرد. در همین خصوص، دانستن این حقیقت نقشی مهم را ایفا می‌کند که هر مجموعهٔ متناهی یا نامتناهی از اعداد صحیح غیر منفی، شامل یک عضو به عنوان کوچکترین عضو است. در اینجا میزان اعتبار این فرض مورد بحث قرار نمی‌گیرد؛ زیرا این موضوع بدون اثبات واضح است، و خواننده می‌تواند آن را به عنوان یکی از خواص تعریف شدهٔ اعداد صحیح بپذیرد. به هر ترتیب، پیش از اثبات قضیهٔ اساسی حساب، لازم است ابتدا به اثبات چند قضیهٔ مقدماتی بپردازیم.

قضیهٔ ۱.۱. *اگر a و b اعداد صحیح هستند و $b > 0$، آنگاه اعداد صحیح q و r موجودند به طوری که*

$$a = bq + r,$$

که در آن $0 \le r < b$، و اعداد صحیح q و r منحصر به فرد هستند.

عدد گویای $\frac{a}{b}$ را در نظر گرفته و فرض می‌کنیم q بزرگترین عدد صحیح نابیشتر از آن است. پس $q \le \frac{a}{b}$، ولی $\frac{a}{b} < q + 1$ است. چون $b > 0$ و $\frac{r}{b} = \frac{a}{b} - q \ge 0$، در نتیجه $r \ge 0$. همچنین، از $\frac{a}{b} - q = \frac{a-bq}{b} = \frac{r}{b} < 1$ نتیجه می‌گیریم که $r < b$.

برای آنکه نشان دهیم q و r منحصر به فرد هستند، فرض می‌کنیم q' و r' هر جفت دلخواه از اعداد صحیح هستند، به طوری که

$$a = bq' + r', \quad 0 \le r' < b$$

اگر $q' < q$، آنگاه $q' \le q - 1$، بنابراین

$$r' = r - bq' \leq a - b\,(q + ۱) = r - b < ۰\,,$$

که با فرض $r' \geq ۰$ در تناقض است. اگر $q' < q$، آنگاه $q' \leq q - ۱$، بنابراین

$$r' = q - bq' \geq a - b(q - ۱) = r + b \geq b\,;$$

که با این واقعیت که $r' < b$ متناقض است.

پس هر دو امکان $q' > q$، $q' < q$ را کنار می‌گذاریم. در نتیجه $q' = q$، و از این رو $r = r'$؛ و این نتیجه اثبات قضیهٔ ۱.۱ را کامل می‌کند.

دو عدد صحیح a و b را نسبت به هم *اول*[۲] گوییم. اگر مقسوم‌علیه مشترکی به جز ± ۱ نداشته باشند. بنابراین، ۵ و ۹ نسبت به هم اولند، در صورتی که ۶ و ۹ نیستند.

قضیهٔ ۲.۱. *اگر a و b نسبت به هم اول هستند، آنگاه عدد صحیح s و t موجودند، به طوری که $as + bt = ۱$.*

باید در نظر داشت که ادعایی در مورد یکتایی s و t وجود ندارد. در واقع اگر $a = ۳$ و $b = ۵$، خواهیم داشت :

$$-۳ \times ۳ + ۲ \times ۵ = ۱ \qquad \text{و} \qquad ۲ \times ۳ - ۱ \times ۵ = ۱$$

برای اثبات قضیه، در ابتدا باید توجه داشت که a و b نمی‌توانند صفر باشند. مجموعهٔ تمام اعداد به صورت $ax + by$ را که در آنها x و y عدد صحیح هستند در نظر می‌گیریم. اگر $x = ۱$ و $y = ۰$ و سپس $x = -۱$ و $y = ۰$ را انتخاب کنیم، واضح است که a و a- هر دو در مجموعهٔ مورد بحث قرار

2) Relatively prime

دارند. چون $a \neq 0$ و یکی از دو عدد a و $-a$ مثبت هستند، بنابراین در این مجموعه اعداد مثبتی وجود دارند. فرض می‌کنیم d کوچکترین عدد مثبت موجود در مجموعهٔ مزبور است و بنویسیم $d = as + bt$

بنابر قضیهٔ ۱.۱، می‌توان اعداد q و r را چنان یافت که

$$b = dq + r, \qquad 0 \leq r < d$$

پس

$$r = b - dq = b - (as + bt)\, q = a(-sq) + b(1 - qt)$$

بنابراین r هم در این مجموعه است. حال، اینکه $0 < r < d$ غیر ممکن است؛ چون d کوچکترین عدد مثبت موجود در این مجموعه است. تنها حالت ممکن $r = 0$ است. از این رو $b = dq$.

بحثی مشابه با شروع از

$$a = dq' + r' \qquad 0 \leq r' < d$$

نشان می‌دهد که $r' = 0$ و $a = dq'$.

این موضوع، ثابت می‌کند d یک مقسوم علیه مشترک a و b است. امّا a و b نسبت به هم اول بودند و در نتیجه $d = \pm 1$، به علاوه، می‌دانیم که d مثبت است، پس باید ۱ باشد. از این رو $as + bt = 1$، و اثبات کامل است.

از این به بعد، علامت «$m \mid n$» به این معناست که "m، n را عاد می‌کند" یا "m یک عامل n است". اگر m یک عامل n نیست، می‌نویسیم $m \nmid n$. قضیهٔ زیر، کلید مهم یگانگی تجزیه است.

قضیهٔ ۳.۱. اگر p عدد اول است و $p \mid ab$، آنگاه $p \mid a$ یا $p \mid b$.

امکان اینکه $a|p$ و $b|p$ از این قضیه نتیجه نمی‌شود.

اگر $p|a$، چیزی برای اثبات نداریم. فرض کنیم $p \nmid a$ و نشان خواهیم داد که در این صورت p باید b را عاد کند. چون p و a نسبت به هم اولند، بنا بر قضیهٔ ۲.۱ اعداد صحیح l و m موجودند، به طوری که

$$lp + ma = ۱ \text{ و } lpb + mab = b .$$

این معنی از قضیهٔ قبل نتیجه می‌شود. چون $p|ab$، می‌توان نوشت $ab = pq$. پس می‌توان فرمول آخر را به این صورت بیان کرد که $p\,(lb + mq) = b$ ، بنابراین $P|b$ و اثبات کامل است.

نتیجهٔ ۴.۱. *اگر عدد اول p حاصل‌ضرب $a_۱ a_۲ \dots a_n$ از اعداد صحیح را عاد کند، حداقل یکی از a_i ها را عاد می‌کند.*

زیرا اگر p هیچ یک از a_i ها را عاد نکند، آنگاه طبق قضیهٔ ۳.۱ نمی‌تواند هیچ یک از حاصل‌ضربهای

$$a_۱ a_۲ \text{ و } (a_۱ a_۲) a_۳ \text{ و } \dots \text{ و } (a_۱ a_۲ \dots a_{n-۱}) a_n$$

را عاد کند.

حال به اثبات قضیهٔ اساسی حساب، که در اولین پاراگراف این فصل بیان شد، می‌پردازیم. فرض می‌کنیم m یک عدد صحیح مثبت غیر از ۱ است. اگر m عدد اول نیست، فرض می‌کنیم قابل تجزیه به‌صورت $m = m_۱ m_۲$ است که در آن $m_۱ > ۱$ و $m_۲ > ۱$. اگر $m_۱$ و $m_۲$ اول هستند، قضیه ثابت شده است. در غیر این صورت همین روش را برای هر یک از دو عدد $m_۱$ و $m_۲$ تکرار می‌کنیم و این کار را مجدداً برای عامل‌های جدیدی که پدید می‌آیند ادامه می‌دهیم. سرانجام باید به

مرحله‌ای برسیم که در آن هیچ یک از عامل‌ها دیگر قابل تجزیه نباشند؛ یعنی حالتی که در آن m-که یک عدد صحیح متناهی است، به حاصل‌ضرب تعدادی به دلخواه بزرگ از عامل‌های بزرگتر از ۱ تبدیل شود.

بنابراین، در این حالت به یک تجزیهٔ

$$m = p_1 p_2 \dots p_r$$

می‌رسیم که در آن هر p_i مثبت و اول است. فرض می‌کنیم

$$m = q_1 q_2 \dots q_s$$

هر تجزیهٔ دیگری از m به اعداد اول مثبت است. باید ثابت کنیم که این دو تجزیه تنها در ترتیب قرار گرفتن اعداد اول تفاوت دارند. از آنجایی که

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s \text{ و}$$

از نتیجهٔ ۴.۱ استنباط می‌شود که q_1 باید یکی از p_iها را عاد کند. در صورت لزوم، می‌توان p_i مورد بحث را با اندیس‌گذاری مجدد p_1 فرض کرد؛ پس $q_1 \mid p_1$. چون p_1 و q_1 مثبت و اول هستند، $p_1 = q_1$. از این رو با تقسیم طرفین بر $p_1 = q_1$ به دست می‌آوریم.

$$p_2 \dots p_r = q_2 \dots q_s$$

این روش را می‌توان برای q_2، ... تکرار کرد، تا تمام عامل‌های اول یک طرف تساوی به اتمام برسند. در این مرحله، تمام عامل‌های طرف دیگر نیز باید تمام شده باشند؛ زیرا در غیر این صورت باید حاصل‌ضربی از اعداد اول را در یک طرف، *برابر* ۱ در طرف دیگر، داشته باشیم. پس

$s = r$ و اثبات به پایان می‌رسد.

اگر سعی کنیم اصل یکتایی تجزیه را برای اعداد صحیح منفی به کار ببریم، در هنگام وجود علامت منفی در عامل‌ها با اشکال آشکاری روبرو می‌شویم. مثلاً

$$(-۲)(-۳)(-۲) = (-۳)\,۲^۲ = -۱۲$$

دو حالت متفاوت تجزیهٔ ۱۲- به اعداد اول هستند و صرفاً در ترتیب عامل‌ها متفاوت نیستند، بلکه در خود عامل‌ها نیز متفاوتند. عامل‌ها، در حالت اول ۲، ۲، ۳-، و در حالت دوم ۲-، ۳-، ۲- هستند. این اشکال را می‌توان با دادن تغییری جزئی در قضیهٔ اساسی اصلاح کرد، به طوری که شامل اعداد منفی هم باشد. فرض می‌کنیم ۱ و ۱- را یکه[3] بنامیم. در این حال، شکل جدید بیان قضیه بدین صورت خواهد بود.

قضیهٔ ۵.۱. *(قضیهٔ اساسی). هر عدد صحیح که صفر یا یکه نیست، قابل تجزیه به حاصل‌ضرب اعداد اول است؛ تجزیه‌ای که بدون در نظر گرفتن ترتیب عامل‌ها و ضرب در یکه‌ها برای هر عدد به طور منحصر به فرد تعیین می‌شود.*

انجام تغییرات جزئی در اثبات اولیه که در اینجا لازم هستند، به عهدهٔ خواننده گذاشته می‌شود.

۲. یک مسئلهٔ کلی. حال در موقعیتی هستیم که مسئلهٔ اساسی نظریهٔ اعداد جبری را بیان کنیم : اگر معنی «عدد صحیح» را به رده‌ای وسیعتر از اعداد شامل اعداد ۰، ۱±، ۲±، ...گسترش دهیم، آیا هنوز قضیهٔ ۵.۱

3) *Unit*

برقرار است؟ ماهیت این سؤال با مثالی روشنتر خواهد شد.

بدین منظور، ابتدا اعداد صحیح گاوسی[۴] را انتخاب می‌کنیم. به‌عنوان یک عدد صحیح، عددی به شکل $a + bi$ را در نظر می‌گیریم، که در آن a و b اعداد صحیح معمولی هستند و $i = \sqrt{-1}$. برای اجتناب از اشتباهات بعدی، از اعداد صحیح معمولی با عنوان «اعداد صحیح» گویا یاد می‌کنیم. فرض می‌کنیم G مجموعهٔ همه اعداد صحیح گاوسی و J مجموعهٔ همهٔ اعداد صحیح گویا است. باید توجه داشت که در هر یک از مجموعه‌ها، مجموع، تفاضل، و حاصل‌ضرب اعداد صحیح، اعدادی صحیح هستند.

اگر α و β اعدادی در مجموعهٔ G هستند، می‌گوییم α، β را عاد می‌کند و می‌نویسیم $\alpha | \beta$، اگر عددی مثل γ در G موجود باشد، چنانکه $\beta = \alpha\gamma$. یک عضو G یکه است، اگر عدد ۱ و بنابراین هر عضو G را عاد کند. عددی مثل π *اول* است، اگر یکه نیست و به علاوه در هر تجزیه $\pi = \alpha\beta$ یکی از اعداد α یا β یکه هستند. با این اصطلاحات، قضیهٔ ۵.۱ برای اعداد صحیح G معنا پیدا می‌کند.

امّا آیا آنچه گفته شد صحیح است؟ این همان چیزی است که بزودی نشان خواهیم داد. حقایقی که تا کنون بیان شده‌اند، ممکن است خواننده را تنها متوجه کند که بایستی چه انتظاراتی داشته باشد. ما با ارائهٔ کلاس سادهٔ دیگری از «اعداد صحیح» که برای آنها قضیهٔ ۵.۱ بامعنا ولی نادرست است، به طرح نقصهای موجود در مطالب پیشگفته خواهیم پرداخت.

اکنون، فرض می‌کنیم هر عدد به شکل $a + b\sqrt{-5}$ را که در آن a و b اعداد صحیح گویا هستند را به معنای «عدد صحیح» بگیریم. مشخص

---

4) *Gaussian*

است که مجموع، تفاضل، و حاصل‌ضرب چنین اعداد صحیحی به همین شکل خواهد بود. مجموعهٔ آنها را با H نشان خواهیم داد. یکه و عدد اول را درست همان طور که برای اعداد گاوسی داشتیم بسادگی با تغییر G به H تعریف می‌کنیم. چنانکه بعداً ثابت خواهیم کرد، ۱+ و ۱− تنها یکه‌های H هستند و اعداد ۳، ۷، $۱ + ۲\sqrt{-۵}$، و $۱ - ۲\sqrt{-۵}$ مانند اعداد اول در H عمل می‌کنند. ولی مشاهده می‌کنیم که

$$۲۱ = ۳ \times ۷ = (۱ + ۲\sqrt{-۵})\,(۱ - ۲\sqrt{-۵}),$$

بنابراین تجزیهٔ ۲۱ به عامل‌های اول بدون در نظر گرفتن ترتیب و ضرب در یکه‌ها، منحصر به فرد نیست.

پس معقول است که بپرسیم برای کدام یک از کلاس‌های «اعداد صحیح»، قضیهٔ اساسی برقرار است و برای کدام یک نیست. بخصوص، چطور با وجود یک تعبیر، اختلاف رفتار بین مجموعه‌های J و G از یک طرف و H از طرف دیگر قابل توجیه است؟ جواب این سؤالها را به بعد موکول می‌کنیم. فعلاً، به اثبات ادعاهایی در مورد مجموعه‌های G و H اکتفا می‌نماییم.

۳. اعداد صحیح گاوسی. اگر $\alpha = a + bi$ یک عضو G است، نورم[5] آن $N(\alpha)$، یا به طور ساده $N\alpha$، به صورت $\alpha\bar{\alpha} = |\alpha|^۲ = a^۲ + b^۲$ ($\bar{\alpha}$ مزدوج مختلط α است). لیست زیر، شامل خاصیتهای اساسی نورم است:

۱− اگر α همان طور که در G است در J هم هست، آنگاه $N\alpha = \alpha^۲$.

۲− $N(\alpha\beta) = N\alpha N\beta$.

۳− $N\alpha = ۱$، اگر و تنها اگر α یکه است.

---

5) *Norm*

۴- $N\alpha \begin{cases} = ۰ & \text{اگر } \alpha = ۰ \\ = ۱ & \text{اگر } \alpha = \pm ۱ \text{ یا } \pm i \\ > ۱ & \text{در سایر موارد} \end{cases}$

۵- اگر $N\alpha$ در J اول است، آنگاه α در G اول است.

اثبات خاصیت ۱ بدیهی است (چون $b = ۰$). برای اثبات خاصیت ۲، مشاهده می‌شود که اگر $\alpha = a + bi$ و $\beta = c + di$، آنگاه

$$(\alpha\beta)\ (\overline{\alpha\beta}) = (\alpha\bar{\alpha})\ (\beta\bar{\beta})$$

همچنین در خصوص خاصیت ۳، ابتدا فرض می‌کنیم که α یکه است. در نتیجه $\alpha \mid ۱$، و بنابراین به ازای بعضی مقادیر β، $\alpha\beta = ۱$. طبق خاصیت ۲، $N\alpha N\beta = N ۱ = ۱$ و $N\alpha \mid ۱$. چون $N\alpha$ باید یک عدد صحیح غیر منفی باشد، $N\alpha = ۱$. برعکس اگر $N\alpha = ۱$، $a^۲b^۲ = ۱$، و بنابراین $a = ۰$ یا $b = ۰$. در نتیجه، α مساوی است با ۱، ۱-، i- یا i، و این اعداد به وضوح یکه هستند. این بحث، همچنین بیشتر قسمتهای خاصیت ۴ را ثابت می‌کند، بقیه را به خواننده واگذار می‌کنیم.

سرانجام اینکه برای اثبات خاصیت ۵، فرض می‌کنیم $N\alpha$ اول است و $\alpha = \beta\gamma$. در نتیجه، $N\alpha = N\beta N\gamma$ در J اول است. بنابراین، یکی از دو عدد $N\beta$ یا $N\gamma$ برابر با ۱ بوده، و طبق خاصیت ۳، β، یا γ یکه است.

عکس خاصیت ۵ نادرست است. برای نشان دادن این موضوع، کافی است برای $N۳$ نشان دهیم که $N۳ = ۳^۲ = ۹$، ۳ در G اول است. فرض می‌کنیم $\alpha\beta = ۳$. در نتیجه $N\alpha\, N\beta = ۹$. اگر هیچ یک از دو عدد α یا β یکه نیستند، $N\alpha \neq ۱$ و $N\beta \neq ۱$؛ و بنابراین $N\alpha = N\beta = ۳$. امّا این به معنای آن است که اگر $\alpha = a + bi$، آنگاه $a^۲ + b^۲ = ۳$؛ و این برای هر

زوج عدد صحیح a و b موجود در J غیرممکن است (چرا؟).

برای اثبات اینکه قضیهٔ ۵.۱ برای اعداد صحیح گاوسی برقرار است، تا حد ممکن از اثباتی که قبلاً برای اعداد صحیح گویا ارائه شده پیروی خواهیم کرد.

قضیهٔ ۶.۱. *اگر α و β اعداد صحیح گاوسی هستند و $\beta \neq 0$، آنگاه دو عدد صحیح π و ρ موجودند، به طوری که*

$$\alpha = \pi\beta + \rho \quad \text{و} \quad N\rho < N\beta$$

عدد $\frac{\alpha}{\beta}$ مساوی با $A + Bi$ را که در آن A و B اعداد گویای معمولی هستند، در نظر می‌گیریم. اعداد صحیح گویای s و t را چنان انتخاب می‌کنیم که

$$|A - s| \leq \frac{1}{2} \quad \text{و} \quad |B - t| \leq \frac{1}{2}$$

ما همیشه می‌توانیم این کار را بوسیلهٔ انتخاب s و t، به ترتیب، به عنوان نزدیکترین اعداد صحیح گویا به A و B انجام دهیم. حال فرض می‌کنیم که $\pi = s + ti$ و $\rho = \alpha + \pi\beta$.

برای نشان دادن اینکه $N\rho < N\beta$، مشاهده می‌کنیم که

$$|\rho| = |\alpha - \pi\beta| = |\alpha - (s + ti)\beta| = |\beta| \left|\frac{\alpha}{\beta} - s - ti\right|$$

$$= |\beta| \, |(A - s) + (B - t)i| = |\beta| \, \{(A - S)^2 + (B - t)^2\}^{1/2}$$

$$\leq |\beta| \, \{\frac{1}{2^2} + \frac{1}{2^2}\}^{1/2} < |\beta| .$$

چون $N\beta = |\beta|^{۲} > |\rho|^{۲} = N\rho$، نامساوی اثبات شده است.

به عنوان مثال فرض می‌کنیم $\alpha = ۵ - i$ و $\beta = ۱ + ۲i$. در این حالت

$$\frac{\alpha}{\beta} = \frac{(۵ - i)(۱ - ۲i)}{(۱ + ۲i)(۱ - ۲i)} = \frac{۳}{۵} - \frac{۱۱}{۵} i,$$

بنابراین، $A = \frac{۳}{۵}$ و $B = -\frac{۱۱}{۵}$. اگر فرض کنیم، $s = ۱$، $t = -۲$، $\pi = ۱ - ۲i$، و $\rho = (۵ - i) - (۱ - ۲i)(۱ + ۲i) = ۵ - i - ۵ = -i$،

$$\text{آنگاه} \quad ۵ - i = (۱ - ۲i)(۱ + ۲i) - i$$
$$N(-i) < N(۱ + ۲i).$$

فرض می‌کنیم خواننده با یک مثال نشان دهد که بر خلاف آنچه قضیهٔ ۱.۱ بیان می‌کند، π و ρ به طور منحصر به فرد تعیین نمی‌شوند.

قضیهٔ ۷.۱. *اگر π یک عدد اول است و $\pi | \alpha\beta$، آنگاه $\pi | \alpha$ یا $\pi | \beta$.*

اگر $\pi | \alpha$، اثبات تمام است. بنابراین فرض می‌کنیم $\pi \nmid \alpha$ و ثابت خواهیم کرد که $\pi | \beta$.

طبق قضیهٔ ۶.۱، می‌توان دو عدد δ و ρ را چنان یافت که

$$\alpha = \delta\pi + \rho \quad , \quad N\rho < N\pi$$

به علاوه $N\rho \neq ۰$؛ زیرا در غیر این صورت $\rho = ۰$ و بنابراین $\pi | \alpha$، که این عکس فرض ماست. در نتیجه، $۰ < N\rho < N\pi$.

همهٔ اعداد صحیح غیر صفر G که به شکل $\alpha\xi + \pi\eta$ هستند را در نظر می‌گیریم و مجموعهٔ آنها را T می‌نامیم. $\rho = \alpha - \pi\delta$ یک عدد صحیح در T است. طبق خاصیت ۴ نورم در G، هر عضو T نورمی حداقل برابر با ۱

دارد. بنابراین، باید یکی از آنها به شکل $\gamma = \alpha\xi_0 + \pi\eta_0$ یافت شود که کوچکترین نورم مثبت است. حال عدد ρ که $\rho = \alpha - \pi\delta$، در T است و نورم کمتر از $N\pi$ دارد. چون γ حداقل نورم است، بنابراین $N\gamma < N\pi$. بعداً نشان خواهیم داد که γ واقعاً یکه است.

θ و ξ را چنان انتخاب می‌کنیم که

$$\pi = \theta\gamma + \xi \text{ و } N\xi < N\gamma$$

چون $\xi = \pi - \theta\gamma = \pi - \theta(\alpha\xi_0 + \pi\eta_0) = \alpha(-\theta\xi_0) + \pi(1 - \theta\eta_0)$، بنابراین $N\xi = 0$؛ چون در غیر این صورت ξ عضوی از T با نورم کوچکتر از γ است. بنابراین $\xi = 0$، $\pi = \theta\gamma$ و $N\pi = N\theta N\gamma$. چون π عددی اول است، از بین دو عدد θ و γ یکی از آنها یکه است. امّا اگر $N\theta = 1$، آنگاه $N\pi = N\gamma$، که این با $N\pi < N\gamma$ در تناقض است.

بنابراین θ یکه نیست؛ یعنی γ یکه است.

در نتیجه $\gamma = \alpha\xi_0 + \pi\eta_0$ یکه است. حال توجه می‌کنیم که

$$\alpha\beta\,\xi_0 + \pi\beta\eta_0 = \gamma\beta$$

چون طبق فرض $\alpha\beta \mid \pi$ و $\pi\beta\eta_0 \mid \pi$، پس $\gamma\beta \mid \pi$. بنابراین، یک عدد τ در مجموعهٔ G وجود دارد، به طوری که $\gamma\beta = \pi\tau$. در نتیجه، $\beta = \pi(\frac{\tau}{\gamma})$ و $\beta \mid \pi$؛ زیرا $\frac{\tau}{\gamma}$ در G است.

برای اثبات اینکه قضیهٔ ۵.۱ برای اعداد صحیح G برقرار است، همان طور عمل می‌کنیم که در مورد اعداد صحیح گویا عمل کردیم. اگر α یکه یا اول نیست، فرض می‌کنیم $\alpha = \alpha_1\alpha_2$، که در آن $N\alpha_1 > 1$ و $N\alpha_2 > 1$. همین روش را برای α_1 و α_2 تکرار کرده و این کار ادامه می‌دهیم. این عمل

در مرحله‌ای متوقف می‌گردد؛ زیرا در غیر این صورت $N\alpha$ حاصل‌ضرب تعداد به دلخواه بزرگی از عامل‌های همگی بزرگتر از ۱، است. بنابراین $\alpha = \pi_1 \dots \pi_r$، که در آن π_iها همگی اولند. اگر همچنین $\alpha = \sigma_1 \dots \sigma_t$ و σ_iها اول هستند، آنگاه طبق قضیهٔ ۷.۱، σ_1 باید یکی از π_iها، مثلاً π_1، را عاد کند. از این رو $\sigma_1 = \pi_1 \varepsilon_1$، که ε_1 یکه است. در نتیجه

$$\pi_2 \dots \pi_r = \varepsilon_1 \sigma_2 \dots \sigma_t$$

حال همان طور که در مورد J عمل کردیم، استدلال را کامل می‌کنیم.

با وجود تمام آنچه که گفته شد، هنوز اثبات گزاره‌ای که در مورد H در بخش قبل بیان شد، باقی می‌ماند؛ یعنی این گزاره که ± 1 تنها یکه‌ها و ۳، ۷، $2 + \sqrt{-5}$، و $2 - \sqrt{-5}$ اعداد اول موجود در H هستند.

اگر $\alpha = a + b\sqrt{-5}$، تعریف می‌کنیم $N\alpha = \alpha\bar{\alpha} = a^2 + 5b^2$. مانند گذشته $N(\alpha\beta) = N\alpha\, N\beta$. α یکه است، اگر و تنها اگر $N\alpha = 1$، اثبات مانند مورد اعداد صحیح گاوسی است. ولی تساوی $a^2 + 5b^2 = 1$؛ تنها وقتی $b = 0$ و $a = \pm 1$، برقرار است. بنابراین $\alpha = \pm 1$ تنها یکه‌های H هستند.

برای آنکه نشان دهیم ۳ اول است، فرض می‌کنیم $\alpha\beta = 3$، که α و β هیچ‌کدام یکه نیستند، یعنی $N\alpha \neq 1$ و $N\beta \neq 1$. چون $N3 = N\alpha \cdot N\beta = 9$، پس $N\alpha = N\beta = 3$، و بنابراین $a^2 + 5b^2 = 3$. اگر $b \neq 0$ آنگاه $a^2 + 5b^2 > 3$ و در نتیجه b باید صفر باشد. امّا در این صورت $a^2 = 3$، که چنین چیزی برای یک عدد صحیح a در J غیرممکن است. به طور مشابه، اگر $\alpha\beta = 7$، $N\alpha \neq 1$، و $N\beta \neq 1$ آنگاه $a^2 + 5b^2 = 7$. اگر $b^2 \neq 0$، $b^2 \neq 1$، آنگاه $a^2 + 5b^2 > 7$. بنابراین، باید $b = 0$ و یا $a^2 = 7$ که غیرممکن است، یا

$b = \pm 1$ و $a^2 = 2$ که این نیز غیرممکن است.

اعداد $1 \pm 2\sqrt{-5}$ اولند، زیرا اگر $\alpha\beta = 2\sqrt{-5} \pm 1$، آنگاه $N\alpha N\beta = 21$ $= N(1 \pm 2\sqrt{-5})$. $N\alpha$ یا $N\beta$ با ۳ برابر است، مگر آنکه یکی از دو عدد α یا β یکه باشد، که این امکان هم قبلاً مستثنیٰ شده است.

در این کتاب، مثالی اضافی از یک کلاس «اعداد صحیح» که یکتایی تجزیه برای آن درست است به وسیلهٔ مجموعهٔ اعداد $a + b\omega$ که در آنها $\omega = \frac{1}{2}(-1 + \sqrt{-3})$، ارائه شده است. خوانندگانی که به جزئیات علاقه‌مند هستند، می‌توانند این مثال را در فصل دوازدهم کتاب هاردی و رایت[6] که در فهرست منابع آمده است بیابند.

6) *Hardy and Wright*

فصل ۲

اعداد اول گاوسی

۱. اعداد اول گویا و گاوسی. اثبات اینکه اعداد اول گویا، یعنی همان اعداد اول موجود در J، به تعداد نامتناهی وجود دارند، مشکل نیست. ساده‌ترین اثبات که منسوب به اقلیدس است، به صورت ذکر شونده است. فرض می‌کنیم P_1، ...، P_n اعداد اول هستند. در این صورت، عدد $N = 1 + P_1 P_2 \ldots P_n$ نمی‌تواند هیچ یک از P_i ها را به عنوان یک عامل داشته باشد؛ چون در این صورت ۱ باید چنین عامل P_i را داشته باشد. پس هر عامل اول N غیر از P_1، ...، P_n است. این بدان معنی است که برای هر مجموعهٔ متناهی داده‌شده از اعداد اول، یک عدد اول غیر از همهٔ آنها وجود دارد. بنابراین، اگر حداقل یک عدد اول موجود است، تعدادی نامتناهی از آنها وجود خواهند داشت. امّا ۲ یک عدد اول است، و بدین ترتیب نتیجه حاصل می‌شود.

در صورتی که تنها بتوانیم یک عدد اول گاوسی بیابیم، دقیقاً اثباتی به همین شکل، برای اعداد اول گاوسی نیز صادق خواهد بود. امّا، چنانکه قبلاً نشان داده شد، ۳ یک عدد اول گاوسی است؛ بنابراین G شامل تعداد

نامتناهی عدد اول است. ما می‌توانیم مطلب را بیشتر توسعه بدهیم : به طور ضمنی، همهٔ اعداد اول در G را بر حسب اعداد اول J مشخص خواهیم کرد. برای رسیدن به این هدف، به دانستن مطالبی از نظریهٔ اعداد مقدماتی نیاز داریم. در واقع، ما چیزی بیشتر از آنچه در اینجا به آن نیاز داریم، اثبات خواهیم کرد. نتایج اضافی که به دست می‌آیند، در آینده مورد کاربردی پیدا خواهند کرد.

۲. همنهشتی‌ها. در این بخش، ما تنها دربارهٔ اعداد صحیح گویا بحث خواهیم کرد.

فرض می‌کنیم m یک عدد صحیح غیر صفر است..دو عدد صحیح a و b را همنهشت به سنج m[1] می‌نامیم و می‌نویسیم

$$a \equiv b \ (m \text{ سنج}) \quad \text{یا} \quad a \equiv b \ (m) \text{ و}$$

اگر $m \mid (a - b)$. اگر a و b همنهشت به سنج m نیستند، می‌نویسیم $a \not\equiv b (m)$.

طبق قضیهٔ ۱.۱، هر عدد صحیح a در تقسیم به $|m|$ یک باقیمانده، r، دارد. $0 \leq r < |m|$. نشان خواهیم داد که a و b به سنج m همنهشت هستند. اگر و تنها اگر در تقسیم به $|m|$ باقیماندهٔ یکسانی داشته باشند. ابتدا فرض می‌کنیم

$$a = q\,|m| + r \text{ و } b = q'\,|m| + r' \text{ و } 0 \leq r < |m|$$

در این صورت

$$a - b = (q - q')\,|m| \text{ و } \pm m \mid (a - b) \text{ و}$$

---

1) *Conguent modulo m*

در نتیجه $m \mid (a - b)$. برعکس، فرض می‌کنیم $a \equiv b(m)$. فرض می‌کنیم $a = q\,|m| + r$، $b = q'\,|m| + r'$، $0 \le r < |m|$ و $0 \le r' < |m|$. در این صورت

$$a - b = (q - q')\,|m| + (r - r')$$

چون $|m|$ عدد $a - b$ را عاد می‌کند، پس $r - r'$ را نیز عاد خواهد کرد. ولی $-|m| < r - r' < |m|$، بنابراین، $r - r'$ نمی‌تواند $|m|$ را بشمارد مگر اینکه $r = r'$.

در اینجا چند مورد از خواص همنهشتی بیان می‌شوند زیرا مکرراً استفاده خواهند شد:

۱- اگر $a \equiv b(m)$، آنگاه $b \equiv a(m)$.

۲- اگر $a \equiv b(m)$ و $b \equiv c(m)$، آنگاه $a \equiv c(m)$.

۳- اگر $a \equiv b(m)$، آنگاه به ازای هر عدد صحیح K، $Ka \equiv Kb(m)$.

۴- اگر $a_i \equiv b_i(m)$، برای $i = ۱، ۲، \ldots، n$، آنگاه

$$a_۱ + a_۲ + \ldots + a_n \equiv b_۱ + b_۲ + \ldots + b_n\ (m)$$

و

$$a_۱ a_۲ \ldots a_n \equiv b_۱ b_۲ \ldots b_n\ (m)$$

قسمت آخر، خاصیت ۴، تنها مورد از خواص همنهشتی است که کاملاً بدیهی نیست. این خاصیت را برای $n = ۲$ ثابت می‌کنیم؛ حالت کلی از به کار بردن مکرر این مورد نتیجه خواهد شد.

طبق خاصیت ۳

$$a_۱ a_۲ \equiv b_۱ a_۲\ (m) \quad \text{و} \quad b_۱ a_۲ \equiv b_۱ b_۲\ (m)$$

و

بنابراین طبق خاصیت ۲، $a_1 a_2 \equiv b_1 b_2 \ (m)$.

عکس خاصیت ۳ درست نیست؛ یعنی اگر $Ka \equiv Kb(m)$، نتیجه نمی‌شود که $a \equiv b(m)$. برای مثال (۳) $۱ \times ۳ \equiv ۲ \times ۳$، ولی (۳) $۱ \not\equiv ۲$. به منظور بیان یک خاصیت صحیح برای حالت عکس خاصیت ۳ نماد بزرگترین مقسوم علیه مشترک[2] دو عدد صحیح h و K را با نمایش $(K$ و $h)$ معرفی می‌کنیم که به بیان ساده بزرگترین عامل صحیح مشترک بین h و K است. باید توجه داشت که اگر c هر عامل مشترک h و K است، آنگاه $c \mid (K$ و $h)$؛ این حقیقت از قضیهٔ اساسی حساب نتیجه می‌شود. بدین ترتیب، به مورد دیگری از خواص همنهشتی می‌رسیم:

خاصیت ۵ـ اگر $Ka \equiv Kb(m)$، آنگاه (سنج $\frac{m}{d}$) $a \equiv b$، که در آن $d = (K, m)$. در حالت خاص، (سنج m) $a \equiv b$، اگر K و m نسبت به هم اول باشند (یعنی $d = ۱$).

حال فرض می‌کنیم که m یک عدد صحیح مثبت است. چون باقیماندهٔ تقسیم هر عدد صحیح بر m یکی از اعداد ۰، ۱، ...، $m - ۱$ خواهد بود، هر عدد صحیح دقیقاً با یکی از این اعداد به سنج m همنهشت است. هر مجموعه از اعداد صحیح را که هر عضو آن دقیقاً با یکی از این اعداد به سنج m همنهشت است یک دستگاه *کامل‌مانده* (یا *باقیمانده*) به سنج m[3] می‌نامیم. در نتیجه، یک مجموعه از اعداد صحیح، یک دستگاه کامل‌مانده به سنج m است، اگر و تنها اگر شامل دقیقاً m عدد صحیح است که هیچ دوتای آنها به سنج m همنهشت نیستند.

قضیهٔ ۱.۲. *اگر* a_1، ...، a_m *یک دستگاه کامل‌مانده به سنج* m *را تشکیل*

---

2) *The greatest common divisor*

3) *Complete residue (or remainder) system modulo m*

دهند و $(a , m) = ۱$، آنگاه $aa_۱$، ...، aa_m نیز یک دستگاه کامل‌مانده به سنج m را تشکیل می‌دهند.

زیرا اگر $aa_i \equiv aa_j \ (m)$، آنگاه طبق خاصیت پنجم از خواص همنهشتی $a_i \equiv a_j \ (m)$.

قضیهٔ ۲.۲. (قضیهٔ فرما[۴]). *اگر P عددی اول است و $(a , P) = ۱$، آنگاه* $a^{p-1} \equiv ۱ \ (p)$.

اعداد ۰، ۱، ۲، ...، و $p - ۱$ تشکیل یک دستگاه کامل‌مانده به سنج p را می‌دهند. از این رو ۰، a، $۲a$، ...، و $(p - ۱)a$ نیز طبق قضیهٔ قبل یک دستگاه کامل‌مانده است. حال هر کدام از اعداد متعلق به یک دستگاه دقیقاً با یکی از اعداد دستگاه دیگر همنهشت است. چون صفرها در دو دستگاه متناظر هستند، با حذف آنها از هر دستگاه طبق خاصیت ۴ خواهیم داشت

$$a \cdot ۲a \ \dots \ (p - ۱)a \equiv ۱ \times ۲ \ \dots \ (p - ۱) \qquad (\text{سنج } p)$$

یا

$$(p - ۱) \, ! \, a^{p-۱} \equiv (p - ۱) \, ! \qquad (\text{سنج } p)$$

طبق خاصیت ۵، با تقسیم طرفین بر $(p - ۱) \, !$ نتیجهٔ زیر به دست می‌آید.

نتیجهٔ ۳.۲. *اگر p یک عدد اول است، آنگاه به ازای هر عدد صحیح a،* $a^p \equiv a \ (p)$.

---

4) *Fermat*

قضیهٔ ۴.۲. (قضیهٔ ویلسون[5]). اگر p یک عدد اول است، آنگاه $(p)\ (p-1)! \equiv -1$.

اگر $p = ۲$ یا $p = ۳$، نتیجه واضح است، پس فرض می‌کنیم $p > ۳$.

فرض می‌کنیم a یکی از اعداد ۱، ۲، ...، $p-1$ است و معادلهٔ $(p)\ ax \equiv ۱$ را در نظر می‌گیریم. باید توجه داشته باشید که $(a, p) = ۱$. اگر x یکی از مقادیر ۱، ۲، ...، $p-1$ است، آنگاه طبق قضیهٔ ۱.۲، ax در یک دستگاه کامل‌مانده به سنج p است، به غیر از صفر. از این رو یک و تنها یک x موجود است که در همنهشتی فوق صدق می‌کند.

پس اعداد ۱، ۲، ...، $p-1$ به جفتهایی تقسیم می‌شوند که حاصل‌ضرب هر یک از آنها با ۱ به سنج p همنهشت است. اگر اعداد یک جفت مساوی باشند، مثلاً a با a، آنگاه $a^۲ \equiv ۱$، $a^۲ - ۱ \equiv ۰$، $(a+۱)(a-۱)$ P، و بنابراین $p \mid (a+۱)$ یا $p \mid (a-۱)$. p نمی‌تواند هم $(a+۱)$ و هم $(a-۱)$ را عاد کند، چون p تفاضل این اعداد یعنی ۲ را عاد می‌کند. از این رو $a \equiv ۱ \ (p)$ یا $a \equiv -۱ \ (p)$. چون $۱ \le a \le p-۱$، داریم $a = ۱$ یا $a = p-۱$.

با $p-۳$ عدد از مجموعهٔ ۲، ...، $p-۲$ می‌توان حاصل‌ضرب $\frac{p-۳}{۲}$ جفت از آنها را تشکیل داد که در نتیجه

$$۲ \times ۳ \times ۴ \dots (p-۲) \equiv ۱ \quad (p)$$

پس

$$(p-۱)! \equiv p-۱ \equiv -۱ \ (p)$$

نتیجهٔ ۵.۲. اگر p یک عدد اول به شکل $۴m+۱$ است، آنگاه $p \mid (n^۲ + ۱)$، و در آن $n = (۲m)!$.

---

5) *Wilson*

دو مجموعه از اعداد را بصورت زیر در نظر می‌گیریم :

$$-۲m \text{ و } \ldots \text{ و } -۲ \text{ و } -۱$$

$$۲m+۱ \text{ و } \ldots \text{ و } ۴m-۱ \text{ و } ۴m$$

هر عضو ردیف پایین دقیقاً با عضو بالایی در ردیف اول به سنج p همنهشت است، چون تفاضل آنها pاست. از این رو

$$۴m\,(۴m-۱)\ldots(۲m+۱) \equiv (-۱)(-۲)\ldots(-۲m) \quad (p)$$

همچنین چون $(۲m)! \equiv (۲m)!$، با ضرب این رابطه در طرفین، به دست می‌آوریم

$$(۴m)! \equiv \{(۲m)!\}^۲ \quad (p)$$

فرض می‌کنیم $n=(۲m)!$. چون $(۴m)! = (p-۱)! \equiv -۱$، با استفاده از قضیهٔ ویلسون نتیجه می‌شود که $n^۲ \equiv -۱ (p)$.

قضیهٔ ۲.۶. *اگر p یک عدد اول است و a و b اعداد صحیح هستند، آنگاه*

$$a^p + b^p \equiv (a+b)^p \quad (\text{سنج } p)$$

طبق نتیجهٔ ۳.۲ برای هر عدد صحیح c، $c^p \equiv c\ (p)$. فرض می‌کنیم $c = a+b$. آنگاه $(a+b)^p \equiv a+b$. امّا همچنین داریم $a^p \equiv a$، $b^p \equiv b$، و از اینجا نتیجه به دست می‌آید.

۳. تعیین اعداد اول گاوسی. حال در موقعیتی هستیم که اعداد اول گاوسی را دسته‌بندی کنیم. با توجه به این حقیقت که یک عدد اول گویا می‌تواند در G اول نباشد، وضعیت را قدری پیچیده‌تر می‌یابیم — برای

مثال $(۱ - ۲i)(۱ + ۲i) = ۵$؛ بخشی از مسئله ما این است که تصمیم بگیریم کدام اعداد اول گویا، اعداد اول گاوسی نیز هستند.

بهتر است در این دسته‌بندی دو عدد صحیح گاوسی را مرتبط[6] بنامیم، می‌نویسیم $\alpha \sim \beta$، اگر $\beta | \alpha$ و $\alpha | \beta$؛ یعنی اگر داشته باشیم $\alpha = \beta\varepsilon$، در این رابطه ε یک عدد یکه است.

قضیهٔ ۷.۲. *اعداد اول گاوسی به سه دستهٔ زیر تقسیم می‌شوند:*

۱. *همهٔ اعداد اول گویای مثبت به شکل* $۴m + ۳$ *و اعداد مرتبط با آنها در* G؛

۲. *عدد* $i + ۱$ *و اعداد مرتبط با آن*؛

۳. *همهٔ اعداد صحیح مرتبط با هر* $x + iy$ *یا* $x - iy$، *که در آنها* $x > ۰$، $y > ۰$، x *زوج است، و* $x^۲ + y^۲$ *یک عدد اول گویا به شکل* $۴m + ۱$ *است.*

قبل از اثبات این قضیه، کاربرد آن را در یافتن اعداد اول گاوسی شرح می‌دهیم. فرض کنیم $p = ۳$. این عدد در اولین دستهٔ مذکور در قضیه است ــ با مقدار m برابر با صفر. از این رو، ۳ یک عدد اول گاوسی است. فرض می‌کنیم $p = ۵$. این عدد به شکل $۴m + ۱$ است و $۵ = (۲ + i)(۲ - i)$. در نتیجه، $i + ۲$ و $i - ۲$ و اعداد مرتبط با آنها بنابر قسمت سوم قضیه، اعداد اول هستند.

برای اثبات قضیه، ابتدا نشان می‌دهیم که هر عدد اول π موجود در G دقیقاً یکی از اعدا اول مثبت p را عاد می‌کند. چون $N\pi = \pi\bar{\pi}$، بنابراین $\pi | N\pi$. فرض می‌کنیم $N\pi = p_۱ \dots p_r$ تجزیهٔ $N\pi$ به اعداد اول مثبت در J است. پس $\pi | p_۱ \dots p_r$. بنا بر قضیهٔ ۷.۱، π یکی از p_iها را عاد می‌کند.

---

6) *associates*

بنابراین، π عدد اول گویایی را عاد می‌کند. این عدد نمی‌تواند دو عدد p و q را عاد کند؛ زیرا طبق قضیهٔ ۲.۱ می‌توان اعداد صحیح گویای l و m را چنان یافت که $lp + mq = ۱$. اگر $\pi | p$ و $\pi | q$، آنگاه $\pi | ۱$؛ یعنی π یکه است و نه یک عدد اول که این موضوع با فرض در تناقض است.

از این رو، هر عدد اول در G را به یک و تنها یک صورت می‌توان بر حسب اعداد اول گویای مثبت، به عنوان اعضای G، تجزیه کرد.

حال، فرض می‌کنیم π یک عدد اول است و p عدد اول مثبتی است که $\pi | p$. پس $N\pi | Np$. امّا $Np = p^۲$؛ زیرا p یک عدد اول گویاست. از این‌رو $N\pi = p$ یا $N\pi = p^۲$. اگر $\pi = x + iy$، آنگاه $x^۲ + y^۲ = p$ یا $x^۲ + y^۲ = p^۲$.

p را بر ۴ تقسیم می‌کنیم. طبق قضیهٔ ۱.۱ باقیماندهٔ این تقسیم ۱، ۲، یا ۳ است. سه حالت مجزا را در نظر می‌گیریم.

حالت ۱: $P \equiv ۳ (۴)$. همان طور که در بالا گفته شد، $x^۲ + y^۲ = p$ یا $x^۲ + y^۲ = p^۲$. حال نشان خواهیم داد که حالت اول ممکن نیست اتفاق بیفتد. چون p فرد است، یکی از دو عدد x یا y، مثلاً x، باید زوج و دیگری فرد باشد. در غیر این صورت مجموع مجذورهای آنها زوج خواهد بود. فرض می‌کنیم $x = ۲a$ و $y = ۲b + ۱$. آنگاه اگر $x^۲ + y^۲ = p$،

$$p = x^۲ + y^۲ = ۴a^۲ + (۲b + ۱)^۲ = ۴(a^۲ + b^۲ + b) + ۱ \equiv ۱ (۴),$$

در صورتی که داشتیم $p \equiv ۳$.

بنابراین، در این حالت $x^۲ + y^۲ = p^۲$ و $N\pi = Np$. چون $\pi | P$، $p = \pi\nu$، که ν در G است. در نتیجه $NP = N\pi N\nu$، $\nu = ۱$، یکه است، و $P \sim \pi$

این اثبات قسمت اول قضیهٔ ۷.۲ بود.

حالت ۲ : $p = ۲$ (۴)۲ ≡ p. در این حالت $p = ۲$؛ چون ۲ تنها عدد اول زوج است. امّا $\pi | (۱ + i)(۱ - i) = ۲$ و $\pi | ۲$. بنابراین $\pi | (۱ + i)$ یا $\pi | (۱ - i)$. امّا $N(۱ + i) = N(۱ - i) = ۲$ یک عدد اول است. قبلاً نشان دادیم که اگر $N\alpha$ عدد اول است، برابر α است. پس $۱ + i$ و $۱ - i$ اول هستند. از این رو $\pi \sim ۱ + i$ یا $\pi \sim ۱ - i$. چون $\frac{۱ + i}{۱ - i} = i$، $۱ - i \sim ۱ + i$؛ و بدین ترتیب قسمت دوم قضیه اثبات می‌شود.

حالت ۳ : $p = ۴m + ۱$ (۴)۱ ≡ p. p به شکل $۴m + ۱$ است. بنابراین نتیجهٔ ۵.۲ قابل استفاده است و به ازای بعضی از اعداد n، $p | n^۲ + ۱$. امّا $(n + i)(n - i) = n^۲ + ۱$ و $p | \pi$؛ بنابراین $\pi | (n + i)$ یا $\pi | (n - i)$. ولی p نمی‌تواند $n + i$ یا $n - i$ را عاد کند؛ زیرا در غیر این صورت یکی از اعداد $\frac{۱}{p} \pm \frac{n}{p} i$ باید یک عدد صحیح گاوسی باشد که این موضوع غیرممکن است، چون $\frac{۱}{p}$ یک عدد صحیح گویا نیست. از این رو، π و p با هم مرتبط نیستند. در نتیجه $N\pi \neq NP$، و بنابراین $x^۲ + y^۲ \neq p^۲$. با استفاده از ملاحظات قبلی، تنها حالت باقیمانده این است که $x^۲ + y^۲ = p$.

پس $\pi\bar{\pi} = p$. به علاوه، $\pi = x + iy$ و $\bar{\pi} = x - iy$ اول هستند؛ زیرا $N\pi = N\bar{\pi} = p$. این دو عدد مرتبط نیستند؛ زیرا در غیر این صورت $x + iy = \varepsilon (x - iy)$، در جایی که $\varepsilon = ۱، -۱، i$ یا $-i$. اگر $\varepsilon = ۱$، $y = ۰$؛ و $p = x^۲$ پس p عدد اول نیست. اگر $\varepsilon = -۱$، $x = ۰$، و $p = y^۲$ و نتیجه‌ای مشابه به دست می‌آید. اگر $\varepsilon = \pm i$، $x = \pm y$، و p زوج خواهد بود. همهٔ این احتمالات غیرممکن هستند؛ بنابراین $x + iy$ و $x - iy$ ممکن نیست مرتبط باشند.

بالاخره، چون $p = x^۲ + y^۲$، یکی از اعداد x و y باید زوج باشد و دیگری فرد؛ که این معنی، اثبات را کامل می‌کند.

۴. قضیهٔ فرما برای اعداد اول گاوسی. حال منطقی است بپرسیم که آیا قضیهٔ مورد بحث برای اعداد اول گویا در قسمت دوم این فصل نظیری برای اعداد گاوسی دارد یا نه. این موضوعی است که ما می‌خواهیم به بررسی آن بپردازیم، و بررسی قضیهٔ همنهشتی و دستگاه کامل‌مانده را می‌توان به بعد موکول کرد. چون بعداً می‌خواهیم این موارد را پس از اعداد گاوسی برای دسته‌های بسیار کلی‌تر اعداد بررسی کنیم، تنها نوعی از آنها را که در اثبات قضیهٔ مشابه قضیهٔ فرما ۲.۲ به کار می‌روند شرح می‌دهیم.

می‌دانیم که منظور ما از نماد (سنج γ) $\alpha \equiv \beta$ (γ) یا $\alpha \equiv \beta$ آن است که $\gamma \mid (\alpha - \beta)$ در G. فرض می‌کنیم که π یک عدد اول گاوسی است.

قضیهٔ ۸.۲ (مشابه قضیهٔ فرما). *اگر α و π نسبت به هم اول هستند (یعنی عامل مشترکی به جز یکه‌ها ندارند)، آنگاه*

$$\alpha^{N\pi-1} \equiv 1 \ (\pi)$$

فرض می‌کنیم p تنها عدد اول p مثبت مذکور در اثبات قضیهٔ قبل است، به طوری که $\pi \mid p$. سه حالت در ارتباط با سه قسمت قضیهٔ ۷.۲ وجود خواهند داشت.

حالت ۱ : $p \equiv 3 \ (4)$. در این حالت، $N\pi = x^2 + y^2 = p^2$؛ پس باید نشان دهیم $\alpha^{p^2-1} \equiv 1 \ (\pi)$. ثابت خواهیم کرد که $\alpha^{p^2} \equiv \alpha \ (p)$. از این مطلب، نتیجهٔ مطلوب به دست خواهد آمد، زیرا

$$\pi \mid P \text{ و } P \mid \alpha^{p^2} - \alpha \text{ و } \pi \mid \alpha(\alpha^{p^2-1} - 1)$$

بنابراین $\pi \mid (\alpha^{p^2-1} - 1)$، چون $\pi \nmid \alpha$.

فرض می‌کنیم $\alpha = l + im$. آنگاه با توجه به بحثی که در اثبات قضیهٔ ۶.۲ به کار رفت، خواهیم داشت $\alpha^p \equiv l^p + i^p m^p \ (p)$. چون p به شکل $4n + 3$ است، $i^p = -i$. همچنین، طبق نتیجهٔ ۳.۲ $l^p \equiv l$ و $m^p \equiv m$. بنابراین

$$\alpha^p \equiv l - im \equiv \bar{\alpha} \ (p)$$

به طور مشابه

$$\bar{\alpha}^p \equiv \alpha \ (p) ,$$

بنابراین

$$\alpha^{p^2} \equiv \bar{\alpha}^p \equiv \alpha \ (p) ,$$

چنانکه ادعا شده بود.

حالت ۲ : $p \equiv 2 \ (4)$. در این حالت $p = 2$؛ بنابراین $\pi \sim 1 + i$. می‌توان فرض کرد $\pi = 1 + i$. چون $N\pi = 2$، آنچه باید ثابت کنیم این است که $\alpha^{N\pi - 1} = \alpha \equiv 1 \ (\pi)$، یا به طور ساده‌تر وقتی $1 + i$ و α نسبت به هم اول هستند، $1 + i$ ، $\alpha - 1$ را عاد می‌کند. چون $1 + i$ اول است، کافی است نشان دهیم اگر α یک عدد صحیح گاوسی است.

$$\beta = \frac{\alpha \ (\alpha - 1)}{1 + i} = \frac{\alpha \ (\alpha - 1)(1 - i)}{2}$$

نیز هست. فرض می‌کنیم $\alpha = a + bi$. آنگاه

$$\beta = \frac{1}{2} \{(a^2 - a - b^2 - b + 2ab) + (-a^2 + a + b^2 - b + 2ab) \ i\}$$

ولی

$$a^2 - a - b^2 - b + 2ab = a(a-1) - b(b+1) + 2ab$$

$$-a^2 + a + b^2 - b + 2ab = -a(a-1) + b(b-1) + 2ab$$

هر دو زوج هستند. از این رو، β یک عدد صحیح گاوسی است.

حالت ۳. $p \equiv 1 \pmod 4$. حال $N\pi = x^2 + y^2 = p$، پس باید نشان دهیم که $\alpha^{P-1} \equiv 1 \pmod \pi$. چون $\pi | p$ و α و π نسبت به هم اولند، اگر بتوانیم ثابت کنیم $\alpha^P \equiv \alpha \pmod p$، حکم ثابت خواهد شد.

فرض می‌کنیم $\alpha = l + mi$. مانند حالت ۱، $\alpha^p \equiv l^p + i^p m^p \pmod p$.

ولی p به شکل $4n + 1$ است؛ بنابراین $i^p = i$ و $\alpha^p \equiv l + im = \alpha$.

فصل ۳

چند جمله‌ای‌ها روی یک هیأت

۱. **خاصیت بخش‌پذیری چند جمله‌ای‌ها.** یک هیأت *اعداد* F[1] به معنای مجموعه‌ای از اعداد حقیقی یا مختلط با این خاصیت است که : اگر α و β در F هستند، $\alpha+\beta$، $\alpha-\beta$، $\alpha\beta$، و $\frac{\alpha}{\beta}$، وقتی $\beta \neq 0$، نیز در F هستند. هر هیأت اعداد F شامل همهٔ اعداد گویاست. زیرا اگر $\alpha \neq 0$ در F است، $\frac{\alpha}{\alpha}=1$ نیز در F است. بنابراین $1+1=2$، $2+1=3$، ...، و همهٔ اعداد صحیح گویای مثبت نیز در F هستند. ولی $1-1=0$ و در نتیجه $0-r$، r که یک عدد صحیح گویاست، باید در F موجود باشد. بنابراین، همهٔ اعداد صحیح گویا در F قرار می‌گیرند. چون همهٔ خارج‌قسمتهای اعداد صحیح گویای غیر صفر نیز در F هستند، ادعای ما ثابت شده است.

خواننده می‌تواند ثابت کند که مجموعه‌های ذکرشونده از اعداد تشکیل هیأت می‌دهند : مجموعهٔ R از همهٔ اعداد گویا، مجموعهٔ همه اعداد به شکل $a+b\sqrt{2}$ با a و $b \in R$، مجموعهٔ همهٔ اعداد حقیقی و مجموعهٔ همهٔ اعداد مختلط. از طرف دیگر، باید توجه داشت که هیچ یک

---

1) *number field F*

از مجموعه‌های J، G، یا H که در فصل قبل در نظر گرفتیم، تشکیل یک هیأت را نمی‌دهند، زیرا شامل اعداد گویا نیستند.

در جبر وجود انواع کلی‌تری از هیأت تعریف شده است؛ ولی در این کتاب، یک «هیأت» به معنای همان «هیأت اعداد» وجود دارد.

یک چند جمله‌ای *مرتبهٔ n ام*[1] که در آن $n \geq 0$ روی یک هیأت F، عبارتی به صورت

$$p(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + a_n x^n$$

است که در آن همهٔ ضرایب در F هستند و $a_n \neq 0$ است. حاصل ضرب دو چند جمله‌ای $p(x)$ و $q(x)$ که

$$q(x) = b_0 + b_1 x + \ldots + b_m x^m,$$

به‌صورت

$$p(x)\, q(x) = c_0 + c_1 x + \ldots + c_k x^k,$$

وقتی که

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + a_1 b_0$$

$$c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_{i-1} b_1 + a_i b_0$$

و $k = m + n$.

در آنالیز نشان داده شده که یک چندجمله‌ای مرتبهٔ *n ام*[2] که در آن

---

2) *polynomial of degree n*

$n \geq ۱$ به طور یگانه قابل تجزیه به صورت

$$p(x) = a_۰ (x - r_۱) (x - r_۲) \dots (x - r_n)$$ و

است که در آن r_i لزوماً در هیأت F که شامل ضرایب $p(x)$ است نیست. به عنوان مثال، $p(x) = x^۲ + ۲x + ۳$ یک چندجمله‌ای روی هیأت R از اعداد گویاست، ولی در این حالت $r_۱ = -۱ + \sqrt{-۲}$ و $r_۲ = -۱ - \sqrt{-۲}$، و این دو یقیناً در R نیستند.

اعداد $r_۱$، ...، r_n، ریشه‌ها یا صفرها[3]ی چند جمله‌ای نامیده می‌شوند. از یگانگی تجزیه، آنچنان که ذکر شد نتیجه می‌شود که یک چند جمله‌ای مرتبهٔ nام که در آن $n \geq ۱$، حداکثر n ریشهٔ مجزا از هم دارد. البته ممکن است همه یا تعدادی از ریشه‌ها مساوی باشند. به‌عنوان مثال

$$x^۳ - ۳x^۲ + ۳x - ۱ = (x - ۱) (x - ۱) (x - ۱)$$

یک چند جمله‌ای روی F، *اول* یا *تحویل ناپذیر*[4] روی F نامیده می‌شود، اگر نتوان آن را به حاصل‌ضرب دو یا تعداد بیشتری چند جمله‌ای

$$p(x) = p_۱(x)\, p_۲(x) \dots p_k(x)\,,$$

تجزیه کرد که هر $p_i(x)$ از مرتبهٔ کمتر از $p(x)$ بوده و خود یک چند جمله‌ای روی F باشد. مثلاً $x^۲ + ۲x + ۳$ روی R تحویل‌ناپذیر است، هر چند روی هیأت اعداد مختلط تحویل‌پذیر است.

ثابت خواهیم کرد که هر چند جمله‌ای روی F قابل تجزیه به حاصل‌ضرب عوامل تحویل‌ناپذیر روی F بوده و این تجزیه صرف نظر از

---

3) *roots or zeros* 4) *irreducible*

ترتیب و ضرب در یکه‌ها، یکتاست. در این حالت، هر یکه به طور ساده یک ثابت، یعنی یک عدد در F، است. چند جمله‌ای‌ها نسبت به هم اولند، اگر تنها عوامل مشترک آنها یکه باشند.

اثبات این موضوع، بی‌شباهت به اثبات قضیهٔ اساسی حساب نیست؛ و ما کار خود را با اثبات نتایجی به موازات قضایای مذکور در فصل اول شروع می‌کنیم.

لم ۱.۳. *فرض می‌کنیم $f(x)$ و $g(x)$ چند جمله‌ای‌هایی به ترتیب از مرتبهٔ n و m روی یک هیأت F هستند و فرض می‌کنیم $n \geq m$. در این صورت به ازای یک عدد مناسب C موجود در F، عبارت*

$$f(x) - C x^{n-m} g(x)$$

برابر صفر یا یک چند جمله‌ای از مرتبهٔ کمتر از n است.

فرض می‌کنیم $f(x)$ و $g(x)$ به ترتیب به صورت

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$
$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0,$$

تعریف شده باشند که در آنها $a_n \neq 0$ و $b_m \neq 0$. $C = \dfrac{a_n}{b_m}$ را در نظر می‌گیریم. در این صورت

$$f(x) - Cx^{n-m} g(x) = (a_n x^n + \ldots) - \frac{a_n}{b_m} x^{n-m} (b_m x^m + \ldots),$$

و بنابراین جمله x^n حذف می‌شود. ممکن است همهٔ جمله‌ها حذف شوند؛ ولی در هر حالت تنها جمله‌های با مرتبهٔ کمتر از x^n می‌توانند باقی بمانند.

از این پس بهتر است ۰ را هم به عنوان یک چند جمله‌ای در نظر بگیریم؛ گرچه هیچ مرتبه‌ای را به آن نسبت نمی‌دهیم. نماد $f(x) \equiv 0$، بدین معنی است که $f(x)$ چند جمله‌ای، صفر است. یک ثابت غیر صفر، طبق تعریف قبلی ما یک چند جمله‌ای مرتبهٔ nام است که در آن $n = 0$.

قضیهٔ ۲.۳. *فرض می‌کنیم $f(x)$ و $g(x)$ که $g(x) \neq 0$ است چند جمله‌ای‌هایی روی F هستند. آنگاه، چند جمله‌ای‌های $q(x)$ و $r(x)$ روی F وجود دارند، به طوری که*

$$f(x) = q(x)\, g(x) + r(x)\,,$$

که در آن $r(x) \equiv 0$ و یا $r(x)$ از مرتبهٔ کمتر از $g(x)$ است.

اگر $f(x)$ صفر یا دارای مرتبهٔ کمتر از $g(x)$ است، می‌توان این طور در نظر گرفت که $q(x) \equiv 0$ و $r(x)$ خود $f(x)$ است.

حال $g(x)$ را ثابت و از مرتبهٔ m در نظر می‌گیریم. می‌خواهیم با استقراء قضیه، را برای هر $f(x)$ از مرتبهٔ $n \leq m$ ثابت کنیم. فرض می‌کنیم که نتیجهٔ قضیه برای هر $f(x)$ از مرتبهٔ ۰ تا $n - 1$ برقرار است. طبق لم پیشگفته

$$f(x) - C\, x^{n-m}\, g(x) = f_1(x)$$

صفر یا از مرتبهٔ حداکثر $n - 1$ است. طبق قسمت اول اثبات، اگر $f_1(x) \equiv 0$، یا طبق فرض استقراء اگر $f_1(x) \neq 0$ باشد، خواهیم داشت

$$f_1(x) = q_1(x)\, g(x) + r(x)\,,$$

که در آن $r(x) \equiv 0$ یا $r(x)$ از مرتبهٔ کمتر از $g(x)$ است. در این صورت

$$f(x) = f_1(x) + C\, x^{n-m}\, g(x)$$

$$= [C\,x^{n-m} + q_1(x)]\,g(x) + r(x)$$
$$= q(x)\,g(x) + r(x),$$

و استقراء کامل شده است.

قضیهٔ ۳.۳. *اگر $f(x)$ و $g(x)$ چند جمله‌ای‌های غیر صفر روی F بوده و بر روی F نسبت به هم اول باشند، آنگاه چند جمله‌ای‌های $S_0(x)$ و $t_0(x)$ روی F موجودند، به طوری که*

$$1 = S_0(x)\,f(x) + t_0(x)\,g(x)$$

مجموعهٔ T از همهٔ چند جمله‌ای‌های به شکل $S(x)\,f(x) + t(x)\,g(x) \neq 0$ را در نظر می‌گیریم، که در آن $S(x)$ و $t(x)$ ضرایبی در F دارند. در T، یک عضو $d(x)$ را با کمترین مرتبه انتخاب می‌کنیم. $d(x)$، البته ممکن است یک ثابت غیر صفر باشد؛ و ما نشان خواهیم داد که واقعاً چنین است.

طبق قضیهٔ ۲.۳، می‌توان $q(x)$ و $r(x)$ را چنان یافت که

$$r(x) = f(x) - q(x)\,d(x),$$

در حالی که $r(x) \equiv 0$، و یا آنکه این چند جمله‌ای از مرتبهٔ کمتر از $d(x)$ است. امکان دوم منتفی است؛ زیرا $r(x)$ به وضوح در T بوده و هیچ چندجمله‌ای در T با مرتبهٔ کمتر از $d(x)$ موجود نیست. بنابراین، $r(x) \equiv 0$. از این رو، $f(x) = q(x)\,d(x)$. به طور مشابه، به ازای بعضی از چند جمله‌ای‌های $q_1(x)$ خواهیم داشت، $g(x) = q_1(x)\,d(x)$. چون $f(x)$ و $g(x)$ نسبت به هم اولند، $d(x)$ باید یک ثابت $d \neq 0$ باشد. چون d در T است، نمایشی به صورت زیر دارد.

$$d = S_0(x) f(x) + t_0(x) g(x)$$

با تقسیم بر d، قضیه اثبات شده است.

یک چند جمله‌ای تکین[5] است، اگر ضریب پیشرو a_n در آن ۱ باشد. با استفاده از قضیهٔ ۳.۳، دو قضیهٔ زیر که به ترتیب مشابه قضایای ۳.۱ و ۵.۱ هستند، به راحتی ثابت می‌شوند. انجام و تکمیل جزئیات این اثباتها، تمرین خوبی برای خواننده خواهد بود.

قضیهٔ ۴.۳. *اگر $p(x)$، $f(x)$؛ و $g(x)$ چند جمله‌ای‌هایی روی F هستند، $p(x)$ تحویل‌ناپذیر است و $p(x)$ حاصل‌ضرب $g(x)$ و $f(x)$ را روی F عاد می‌کند، آنگاه $p(x)$ یا $f(x)$ را عاد می‌کند یا $g(x)$ را.*

قضیهٔ ۵.۳. *هر چندجمله‌ای $p(x) = a_n x^n + \dots + a_0$ روی F که غیر صفر و غیرثابت است، قابل تجزیه به حاصل‌ضرب*

$$p(x) = a_n p_1(x) \dots p_r(x)$$

که در آن $p_i(x)$ چندجمله‌ای‌های تکین تحویل‌ناپذیر روی F هستند؛ چندجمله‌ای‌هایی که صرف نظر از ترتیب، به طور یگانه تعیین می‌شوند.

۰۲ محک تحویل‌ناپذیری آیزنشتاین.[6] در این بخش، یک تست مفید و ساده را برای تحویل‌ناپذیری یک چندجمله‌ای روی هیأت R از اعداد گویا ارائه می‌کنیم.

یک چندجمله‌ای با ضرایب صحیح گویا *ابتدایی*[7] است، اگر ضرایب آن

---

5) *monic* 6) *Eisenstein*
7) *prinitive*

عامل مشترکی به غیر از ± 1 نداشته باشد. در همین رابطه، قضیهٔ زیر خیلی مهم است.

قضیهٔ ۶.۳ (لم گوس). *حاصل‌ضرب چندجمله‌ای‌های ابتدایی، ابتدایی است.*

فرض می‌کنیم $a_0 + a_1 x + \ldots + a_n x^n$ و $b_0 + b_1 x + \ldots + b_m x^m$ ابتدایی بوده و حاصل‌ضرب آنها $c_0 + c_1 x + \ldots + c_k x^k$ غیرابتدایی است. در این صورت، همهٔ c_i ها توسط بعضی اعداد اول مثل P عاد می‌شوند. فرض می‌کنیم a_i و b_j اولین ضرایب در دو چندجمله‌ای، اول هستند (به ترتیب نوشتن این جملات توجه کنید) و توسط p عاد نشوند. اینها باید وجود داشته باشند چون چندجمله‌ای‌ها ابتدایی هستند و بنابراین همهٔ ضرایب آنها نمی‌توانند توسط p عاد شوند.

حال، طبق فرمول حاصل‌ضرب دو چندجمله‌ای،

$$C_{i+j} = (a_0 b_{i+j} + \ldots + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + \ldots + a_{i+j} b_0)$$

امّا a_0، a_1، $\ldots$، a_{i-1} و b_0، b_1، $\ldots$، b_{j-1}، و C_{i+j} همه توسط P عاد می‌شوند. بنابراین، $a_i b_j$ نیز باید توسط p عاد شوند.

چون p اول است، $P \mid a_i$ یا $P \mid b_j$. ولی این معنی با انتخاب a_i و b_j به عنوان ضرایبی که توسط P عاد نمی‌شوند در تناقض است. بنابراین، این فرض که C_i ها یک عامل مشترک P دارند نادرست است و $C_0 + C_1 x + \ldots + C_k x^k$ باید ابتدایی باشد.

به عنوان مثال چندجمله‌ای‌های ابتدایی $x^2 + 3$ و $3x^2 + 7x - 11$ را در نظر می‌گیریم. حاصل‌ضرب آنها

$$۳x^۴ + ۷x^۳ - ۲x^۲ + ۲۱x - ۳۳$$

نیز یقیناً ابتدایی است.

قضیهٔ ۷.۳. *اگر یک چندجمله‌ای با ضرایب صحیح گویا روی R قابل تجزیه است، می‌توان آن را به چندجمله‌ای‌هایی با ضرایب صحیح گویا تجزیه کرد.*

به عنوان مثال

$$۲x^۲ + ۱۹x + ۳۵ = (۲x + ۱۴)(x + \frac{۵}{۲}),$$

ولی همچنین

$$۲x^۲ + ۱۹x + ۳۵ = (x + ۷)(۲x + ۵)$$

اثبات این قضیه دو قسمت دارد. قبل از شروع اثبات، باید توجه داشت که هر چندجمله‌ای $f(x) \neq$ روی R را می‌توان به طور یگانه‌ای به صورت

$$f(x) = C_f f^*(x),$$

نوشت که در آن $f^*(x)$ ابتدایی بوده و C_f یک عدد گویای مثبت است؛ زیرا فرض می‌کنیم

$$f(x) = a_n x^n + a_{n-۱} x^{n-۱} + \ldots + a_۰,$$

که در آن a_i ها گویا هستند. می‌توانیم بنویسیم $a_i = \frac{bi}{c}$ که C بزرگترین مخرج مشترک همهٔ a_i هاست. در نتیجه

$$f(x) = \frac{۱}{c}(b_n x^n + b_{n-۱} x^{n-۱} + \ldots + b_۰)$$

حال، عامل خارج پرانتز، بزرگترین عامل مشترک مثبت همهٔ b_i هاست. در این شرایط، آنچه داخل پرانتز باقی مانده را $f^*(x)$ و آنچه خارج مانده را c_f می‌نامیم. واضح است که $C_f >$ و $f^*(x)$ با روشی که بیان کردیم ابتدایی است. در خصوص یگانگی، باید گفت که اگر

$$f(x) = C_f f^*(x) = cp(x) ,$$

که در آن C_f و C مثبت بوده و $f^*(x)$ و $p(x)$ ابتدایی هستند، آنگاه $p(x) | f^*(x)$ و $f^*(x) | p(x)$؛ و بنابراین $f^*(x) = \pm p(x)$، که علامت + مورد قبول است.

حال به اثبات قضیه می‌پردازیم. فرض می‌کنیم $f(x) = g(x)h(x)$ روی R ، و $f(x)$ ضرایب صحیح دارد. در این صورت

$$c_f f^*(x) = c_g g^*(x) \cdot c_h h^*(x) ,$$

که در آن $f(x)$، $g(x)$ $h(x)$ به صورت مورد بحث نوشته شده‌اند. بنابراین

$$f(x) = c_f f^*(x) = (c_g c_h) g^*(x) h^*(x)$$

امّا طبق قضیهٔ ۶.۳، $g^*(x)$ $h^*(x)$ ابتدایی است. به علاوه، تجزیهٔ $f(x)$ به این صورت یکتاست، بنابراین $f^*(x) = g^*(x) h^*(x)$ و

$$f(x) = c_f g^*(x) h^*(n)$$

ولی $f(x)$ و $f^*(x)$ ضرایب صحیح دارند و $f^*(x)$ ابتدایی است. بنابراین، c_f باید یک عدد صحیح مثبت باشد؛ و این موضوع قضیه را ثابت می‌کند.

قضیهٔ ۸.۳. (محک تحویل‌ناپذیری آیزنشتاین). فرض می‌کنیم p یک

عدد اول و $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ یک چندجمله‌ای با ضرایب صحیح است، به طوری که

$$p \nmid a_n \quad \text{و} \quad p^2 + a_0 ; \qquad p \mid a_i \quad \text{و} \quad i = 0, 1, \ldots, n-1$$

در این صورت، $f(x)$ روی R تحویل‌ناپذیر است.

اگر $f(x)$ روی R تجزیه شود، آنگاه طبق قضیهٔ ۷.۳ عواملی با ضرایب صحیح خواهد داشت. فرض می‌کنیم

$$f(x) = (b_m x^m + \ldots + b_0)(c_k x^k + \ldots + c_0),$$

که در آن b_i و c_i صحیح هستند و $m + k = n$ مرتبهٔ $f(x)$ است. چون $a_0 = b_0 c_0$ و $p^2 \nmid a_0$، b_0 و c_0 هیچکدام توسط p عاد نمی‌شوند. امّا $P \mid a_0$ و بنابراین $P \mid b_0$ یا $P \mid c_0$. فرض می‌کنیم $P \mid c_0$ و $P \nmid b_0$.

حال، مشاهده می‌شود که $a_n = b_m c_k$ توسط p عاد نمی‌شود. بنابراین، c_k هم توسط آن عاد نمی‌شود. لیست ضرایب c_0، c_1، ...، c_k را در نظر می‌گیریم. باید کوچکترین مقدار r که $r \leq k$ چنان موجود باشد که c_r توسط p عاد نشود، امّا c_0، c_1، ...، c_{r-1} عاد می‌شوند. طبق فرمول حاصل‌ضرب چندجمله‌ای‌ها

$$a_r = b_0 c_r + b_1 c_{r-1} + \ldots + b_r c_0$$

همهٔ جملات سمت راست بجز $b_0 c_r$ توسط p عاد می‌شوند. بنابراین، a_r هم نمی‌تواند توسط p عاد شود. امّا طبق فرض، تنها یکی از ضرایب a_i توسط p عاد نمی‌شود و آن هم a_n است؛ پس $r = n$. چون $r \leq k$، $n \leq k$. امّا $k + m = n$؛ بنابراین $n \geq k$. دو نامساوی مذکور تنها وقتی هر دو

برقرارند که داشته باشیم $n = k$.

از این رو، یکی از عوامل در نظر گرفته شدهٔ $f(x)$ لزوماً همان مرتبهٔ $f(x)$ را دارد. پس $f(x)$ باید تحویل‌ناپذیر باشد.

به عنوان کاربردی از محک آیزنشتاین، تحویل‌ناپذیری روی R را برای چندجمله‌ای مهم ثابت خواهیم کرد. ابتدا باید توجه داشت که چندجمله‌ای $f(x)$ تحویل‌ناپذیر است، اگر و تنها اگر $f(x + ۱)$ تحویل‌ناپذیر باشد؛ زیرا $f(x + ۱) = g(x)\ h(x)$ و اگر و تنها اگر $f(x) = g(x - ۱)\ h(x - ۱)$.

فرض می‌کنیم p یک عدد اول است و چندجمله‌ای زیر که چندجمله‌ای تقسیم *دایره*[۸] نامیده می‌شود را در نظر می‌گیریم،

$$\frac{x^p - ۱}{x - ۱} = x^{p-۱} + x^{p-۲} + \ldots + ۱ .$$

این چندجمله‌ای روی R تحویل‌ناپذیر است، اگر

$$\frac{(x + ۱)^p - ۱}{(x + ۱) - ۱} = \frac{(x + ۱)^p - ۱}{x}$$

نیز تحویل‌ناپذیر باشد. امّا این عبارت به صورت زیر است (چرا؟)

$$x^{p-۱} + p\ (x^{p-۲} + \ldots) + p ,$$

و تحویل‌ناپذیزی آن از قضیهٔ ۸.۳ نتیجه می‌شود.

به عنوان یک مثال مهم دیگر، چندجمله‌ای زیر را در نظر می‌گیریم

$$\frac{x^{p^۲-۱}}{x^p - ۱} = x^{p(p-۱)} + x^{p(p-۲)} + \ldots x^p + ۱$$

با جایگزینی x به وسیلهٔ $x + ۱$ رابطهٔ بالا به صورت زیر درمی‌آید

$$x^{p(p-1)} + p\,q(x)$$ و

که در آن $q(x)$ ضرایب صحیح دارد و جملهٔ آخر آن ۱ است. دوباره محک آیزنشتاین نشان می‌دهد که چندجمله‌ای روی R تحویل‌ناپذیر است.

قضیهٔ ۹.۳. *اگر p یک عدد اول است، آنگاه چندجمله‌ای‌های*

$$x^{p-1} + x^{p-2} + \ldots + x + 1$$

و

$$x^{p(p-1)} + x^{p(p-2)} + \ldots + x^{p} + 1$$

روی R تحویل‌ناپذیرند.

۳. چندجمله‌ای‌های متقارن. فرض می‌کنیم x_1، ... ، x_n متغیرهایی مستقل هستند. یک چندجمله‌ای از x_1، ... ، x_n روی F را مجموعی متناهی به صورت

$$g(x_1, \ldots, x_n) = \sum_{i_1, i_2, \ldots, i_n} a_{i_1, i_2, \ldots, in}\; x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$ و

تعریف می‌کنیم، که در آن aها عناصر F بوده و توان‌ها اعداد صحیح غیر منفی هستند. به عنوان مثال، $x_1 x_3 + \frac{1}{5} x_3^2 x_2 + 6x_1 + x_2 x_3$ یک چندجمله‌ای از x_1، x_2، x_3 است.

یک چندجمله‌ای $g(x_1, \ldots, x_n)$ متقارن[8] است اگر با هر یک از $n!$ جایگشت متغیرهای $x_1, \ldots, x_n$ تغییر نکند. مثلاً وقتی $n = 3$،

8) *Symmetric*

چندجمله‌ای‌های $x_1 + x_2 + x_3$ و $x_1 x_2 + x_2 x_3 + x_3 x_1$ متقارن هستند.

حال، با فرض اینکه Z متغیر دیگری است، تعریف می‌کنیم

$$f(z) = (z - x_1)(z - x_2) \dots (z - x_n)$$
$$= z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \dots (-1)^n \sigma_n$$

بسادگی ثابت می‌شود که

$$\sigma_1 = x_1 + x_2 + \dots + x_n$$
$$\sigma_2 = x_1 x_2 + x_1 x_3 + \dots + x_2 x_3 + \dots + x_{n-1} x_n$$
$$\dots\dots$$
$\sigma_i =$ مجموع همهٔ حاصل‌ضربهای i تایی مختلف x_j
$$\sigma_n = x_1 x_2 \dots x_n .$$

در چنین شرایطی، σ_i ها توابع متقارن *ابتدایی*[9] از x_1، ...، x_n نامیده می‌شوند.

قضیهٔ استاندارد زیر را در ارتباط با چندجمله‌ای‌های متقارن بدون اثبات می‌پذیریم. تفصیل این قضیه را در اکثر کتابهای تئوری معادلات، برای مثال کتاب توماس[10] که در فهرست منابع آمده، می‌توان یافت.

قضیهٔ ۳.۱۰. *هر چند جمله‌ای متقارن از x_1، ...، x_n روی یک هیأت F را می‌توان به صورت یک چندجمله‌ای روی F از توابع متقارن ابتدایی σ_1، ...، σ_n نوشت. اگر ضرایب چندجمله‌ای اول اعداد صحیح گویا هستند، چندجمله‌ای دوم نیز چنین خواهند بود.*

برای مثال، اگر $n = 3$، آنگاه

9) *elementary symmetric functions* 10) *Thomas*

$$x_1^2 + x_2^2 + x_3^2$$
$$= (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1) = \sigma_1^2 - 2\sigma_2$$

ما مکرراً از نتیجهٔ قضیهٔ ۳.۱۰ به جای خود قضیه استفاده خواهیم کرد.

قضیهٔ ۳.۱۱. *اگر $f(x)$ یک چند جمله‌ای مرتبهٔ nام روی F با ریشه‌های $r_1, r_2, \ldots, r_n$ بوده و $P(x_1, \ldots, x_n)$ یک چندجمله‌ای متقارن روی F است، آنگاه $p(r_1, \ldots, r_n)$ یک عضو F است.*

به‌عنوان مثال اگر $f(x) = 2x^2 - 7x + 7$، $F = R$، و $P(x_1, x_2) = x_1^2 + x_2^2$. آنگاه ریشه‌های $f(x)$، $\frac{7 \pm \sqrt{7}i}{4}$ هستند و

$$P(r_1, r_2) = \left(\frac{7+\sqrt{7}i}{4}\right)^2 + \left(\frac{7-\sqrt{7}i}{4}\right)^2 = \frac{21}{4},$$

که $\frac{21}{4}$، همان طور که با استفاده از قضیه پیش‌بینی می‌شد، یک عدد گویاست.

نشان دادن اینکه قضیهٔ ۳.۱۱ نتیجه‌ای از قضیهٔ ۳.۱۰ است، مشکل نیست. طبق قضیهٔ ۳.۱۰، $p(x_1, \ldots, x_n)$ یک چندجمله‌ای روی F از $\sigma_1, \ldots, \sigma_n$ است. این به معنای آن است که یک $p(r_1, \ldots, r_n)$ یک چندجمله‌ای از $r_1 + r_2 + \ldots$، $r_1r_2 + r_1r_3 + \ldots$، و $r_1r_2 \ldots r_n$ است. امّا این عبارات ضرایب $\frac{f(x)}{a_n}$ هستند، اگر بنویسیم

$$f(x) = a_n (x^n - b_{n-1}x^{n-1} + b_{n-2}x^{n-2} - \ldots \pm b_0)$$

همهٔ b_i ها در F قرار دارند.

یک نتیجهٔ مهم قضیهٔ ۳.۱۱ نتیجهٔ زیر است.

نتیجهٔ ۳.۱۲. *اگر $f(x)$ و $g(x)$ چندجمله‌ای‌هایی روی یک هیأت F بوده و*

α_1، ...، α_n، β_1، ...، β_k به ترتیب ریشه‌های آنها هستند، آنگاه حاصل‌ضربهای

$$h_1(x) = \prod_{j=1}^{k} \prod_{i=1}^{n} (x - \alpha_i - \beta_j)$$

$$h_2(x) = \prod_{j=1}^{k} \prod_{i=1}^{n} (x - \alpha_i \beta_j)$$

چندجمله‌ای‌هایی از x هستند که ضرایب آنها در F قرار دارند.

می‌توان نوشت

$$f(x) = a_n (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$ و

که a_n ضریب پیشرو $f(x)$ است. در این صورت

$$f(x - \beta_j) = a_n (x - \alpha_1 - \beta_j)(x - \alpha_2 - \beta_j) \dots (x - \alpha_n - \beta_j)$$

$$= a_n \prod_{i=1}^{n} (x - \alpha_i - \beta_j)$$

از این رو

$$a_n^k h_1(x) = \prod_{j=1}^{k} f(x - \beta_j) .$$

این حاصل‌ضرب یک چندجمله‌ای از x است که ضرایب آن عبارات متقارنی از β_1، ...، β_k هستند و بنابراین طبق قضیهٔ ۱۱.۳ ضرایب مزبور در F قرار دارند. اگر طرفین را بر a_n^k تقسیم کنیم، نتیجه می‌شود که ضرایب $h_1(x)$ در F هستند؛ چون F یک هیأت است.

برای اثبات نتیجهٔ مورد بحث در خصوص $h_2(x)$، باید توجه داشت که

$$f\left(\frac{x}{\beta_j}\right) = a_n \left(\frac{x}{\beta_j} - \alpha_1\right) \ldots \left(\frac{x}{\beta_j} - \alpha_n\right)$$ و

پس

$$\beta_j^n f\left(\frac{x}{\beta_j}\right) = a_n (x - \alpha_1 \beta_j) \ldots (x - \alpha_n \beta_j)$$ و

و بنابراین

$$a_n^k h_2(x) = \prod_{j=1}^{k} \beta_j^n f\left(\frac{x}{\beta_j}\right).$$

بقیهٔ اثبات مثل حالت قبل است.

فصل ۴

هیأت‌های اعداد جبری

۱. اعداد جبری روی یک هیأت. فرض می‌کنیم F یک هیأت اعداد است. عدد θ روی F جبری[1] نامیده می‌شود، اگر در یک معادلهٔ چندجمله‌ای

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0$$

با ضرایب موجود در F صدق کند. θ لزوماً در F نیست. برای مثال، گرچه $\sqrt{2}$ در $x^2 - 2 = 0$ روی R صدق می‌کند، ولی این عدد در R نیست.

حال تصور می‌کنیم θ روی F جبری است، و همهٔ چندجمله‌ای‌های روی F را که θ ریشهٔ آنهاست در نظر می‌گیریم. فرض می‌کنیم $p(x)$ یکی از آنها با کمترین درجه است. چون همیشه می‌توان چندجمله‌ای را بر ضریب پیشرو تقسیم کرد، فرض می‌کنیم $p(x)$ تکین است. در این صورت، $p(x)$ را یک چندجمله‌ای *مینیمال برای* θ[2] روی F می‌نامیم. $p(x)$ به وضوح تحویل‌ناپذیر است، در غیر این صورت θ باید در یک چندجمله‌ای با درجهٔ کمتر صدق کند.

---

1) *algebric*

2) *minimal polynomial for* θ

قضیهٔ ۱.۴. *اگر θ روی F جبری است، یک چندجمله‌ای مینیمال یکتا دارد.*

فرض می‌کنیم $p(x)$ یک چندجمله‌ای مینیمال و $q(x)$ چندجمله‌ای دیگری روی F است که θ در آن صدق کند. در این صورت

$$q(x) = g(x)\,p(x) + h(x)$$ و

که درآن $h(x) \equiv 0$ یا $h(x)$ با درجهٔ کمتر از $p(x)$ است. فرض می‌کنیم $x = \theta$. چون $p(\theta) = q(\theta) = 0$، پس $h(\theta) = 0$. در این صورت $h(x) \equiv 0$، وگرنه $p(x)$ مینیمال نخواهد بود. بنابراین $p(x) \mid q(x)$.

حال اگر $q(x)$ هر چندجمله‌ای مینیمال دیگر θ روی F است، با بحثی مشابه می‌توان نشان داد که $q(x) \mid p(x)$. از این رو $p(x) = \pm q(x)$ و چون $p(x)$ و $q(x)$ هر دو تکین هستند با هم برابرند، چنانکه ادعا شده بود.

ما به طور ضمنی نتیجهٔ زیر را هم ثابت کرده‌ایم:

نتیجهٔ ۲.۴. *هر چندجمله‌ای روی F که θ در آن صدق کند شامل چندجمله‌ای مینیمال θ به عنوان یک عامل است.*

نتیجهٔ ۳.۴. *اگر $f(x)$ و $g(x)$ روی F نسبت به هم اول باشند آنگاه ریشهٔ مشترک ندارند.*

زیرا اگر θ یک ریشهٔ مشترک است، آنگاه طبق نتیجهٔ ۲.۴ چندجمله‌ای مینیمال θ روی F، $f(x)$ و $g(x)$ را عاد می‌کند، که با فرض اینکه آنها عامل مشترک ندارند در تناقض است.

نتیجهٔ ۴.۴. *هر چندجمله‌ای تحویل‌ناپذیر درجهٔ n روی F، n ریشهٔ مجزا دارد.*

زیرا اگر فرض کنیم چندجمله‌ای تحویل‌ناپذیر $f(x)$ دو ریشهٔ یکسان دارد، می‌توانیم بنویسیم

$$f(x) = a_n (x - r)^2 g(x)$$

در این صورت، با مشتق گرفتن از طرفین خواهیم داشت

$$f'(x) = a_n (x - r)^2 g'(x) + 2a_n (x - r) g(x) \quad \text{و}$$

بنابراین، $f(x)$ و $f'(x)$ یک ریشهٔ مشترک r دارند. طبق نتیجهٔ قبل، چندجمله‌ای‌های $f(x)$ و $f'(x)$ باید یک عامل مشترک داشته باشند. چون $f(x)$ تحویل‌ناپذیر است، خود عامل مشترک است و $f(x) \mid f'(x)$. امّا این ممکن نیست؛ چون $f'(x)$ از مرتبهٔ کمتر از $f(x)$ است.

فرض می‌کنیم θ روی F جبری بوده و $p(x)$ چندجمله‌ای مینیمال آن، مثلاً از درجهٔ n است. آنگاه، θ روی F از درجهٔ n[3] گفته می‌شود. فرض می‌کنیم θ_1، ...، θ_n ریشه‌های $p(x)$ هستند که $\theta_1 = \theta$. طبق نتیجهٔ ۴.۴، این n عدد مجزا هستند. آنها را مزدوج‌های θ روی F[4] می‌نامیم.

به عنوان مثال، فرض می‌کنیم $F = R$. طبق محک آیزنشتاین، $x^3 - 2$ روی R تحویل‌ناپذیر است. اگر $2^{1/3}$ ریشهٔ مثبت چندجمله‌ای است. آنگاه

$$2^{1/3}\omega^2 \quad ، \quad 2^{1/3}\omega \quad ، \quad 2^{1/3}$$

مزدوج‌های آن هستند، که در آنها $\omega = -1/2 + (\sqrt{-3}/2)$؛ زیرا 1 و ω و ω^2 ریشه‌های $x^3 - 1$ هستند.

قضیهٔ ۵.۴. *کلیهٔ اعداد جبری روی یک هیأت F، تشکیل یک هیأت*

---

3) *degree* 4) *Conjugates of θ over F*

می‌دهد.

فرض کنیم α و β ($\beta \neq 0$) روی F جبری هستند. باید نشان دهیم که $\alpha + \beta$، $\alpha - \beta$، $\alpha\beta$، و $\frac{\alpha}{\beta}$ همه روی F جبری هستند؛ یعنی در چندجمله‌ای‌های روی F صدق می‌کنند. فرض می‌کنیم $f(x)$ و $g(x)$ به ترتیب چندجمله‌ای‌های مینیمال α و β روی F هستند. چندجمله‌ای‌های $h_1(x)$ و $h_2(x)$ را چنانکه در نتیجهٔ ۱۲.۳ شرح داده شد تشکیل می‌دهیم. این چندجمله‌ای‌ها، روی F هستند و $\alpha + \beta = \alpha_1 + \beta_1$ و $\alpha\beta = \alpha_1\beta_1$ در آنها صدق می‌کنند. از این رو، مجموع $\alpha + \beta$ و حاصل‌ضرب $\alpha\beta$ جبری هستند. چون β در $g(-x)$ صدق می‌کند، $-\beta$ جبری است. در نتیجه، مجموع $\alpha - \beta = \alpha + (-\beta)$ نیز جبری است. بالاخره، اگر m درجهٔ $g(x)$ است، آنگاه $\frac{1}{\beta}$ در $x^m g(\frac{1}{x})$ صدق می‌کند و بنابراین $\frac{1}{\beta}$ جبری است؛ پس با نتیجه‌ای که در مورد حاصل‌ضرب داشتیم، $\frac{1}{\beta} \cdot \alpha$ نیز روی F جبری است.

بعداً اثبات دیگری را از این قضیه ارائه خواهیم کرد که از بحث توابع متقارن مستقل است.

۲. توسیع‌های یک هیأت. فرض می‌کنیم F یک هیأت است. در این صورت هر هیأت K شامل F یک توسیع[5] F نامیده می‌شود. به عنوان مثال، هر هیأت عددی یک توسیع هیأت R از اعداد گویاست.

اگر θ روی F جبری است، آنگاه $K = F(\theta)$ کوچکترین هیأت شامل F و θ تعریف می‌شود. K، توسیع جبری ساده[6] F نامیده می‌شود. روشن است که K شامل همهٔ خارج‌قسمت‌های $\frac{f(\theta)}{g(\theta)}$ است که در آنها $f(x)$ و $g(x)$ چندجمله‌ای‌هایی روی F هستند و $g(\theta) \neq 0$. در قضیهٔ بعدی، نشان خواهیم داد که هر عضو $F(\theta)$ را می‌توان به طور خیلی ساده به صورت

---

5) *extention* 6) *Simple algebric extention*

یک چندجمله‌ای بر حسب θ نوشت.

قضیهٔ ۶.۴. *هر عضو α از $F(\theta)$ را می‌توان به طور یگانه‌ای به صورت*

$$\alpha = a_0 + a_1\,\theta + \ldots + a_{n-1}\,\theta^{n-1} = r(\theta)$$

و نوشت که در آن a_iها در F هستند و n درجهٔ θ روی F است.

فرض می‌کنیم $\alpha = \dfrac{f(\theta)}{g(\theta)}$، که در آن $g(\theta) \neq 0$، و $p(x)$ چندجمله‌ای مینیمال θ روی F است. در این صورت، $P(x)$ تحویل‌ناپذیر است و $p(x) \nmid g(x)$ چون در غیر این صورت $g(\theta) = 0$، و بنابراین $p(x)$ و $g(x)$ نسبت به هم اولند. طبق قضیهٔ ۳.۳، چند جمله‌ای‌های $S(x)$ و $t(x)$ وجود دارند، چنانکه $S(x)\,p(x) + t(x)\,g(x) = 1$. فرض می‌کنیم $x = \theta$. چون $p(\theta) = 0$، داریم $t(\theta) = \dfrac{1}{g(\theta)}$، و بنابراین چندجمله‌ای

$$\alpha = \frac{f(\theta)}{g(\theta)} = f(\theta)\,t(\theta)$$

یک چندجمله‌ای بر حسب θ است ــ برای سادگی می‌نویسیم $\alpha = h(\theta)$.

اکنون مشاهده می‌شود که $h(x) = q(x)\,p(x) + r(x)$؛ که $r(x) \equiv 0$ یا درجهٔ $r(x)$ کمتر از $p(x)$ است. چون $p(\theta) = 0$، نتیجه می‌شود که

$$\alpha = h(\theta) = r(\theta)$$

از این رو، α یک چندجمله‌ای بر حسب θ از درجهٔ حداکثر $n-1$ است.

حال، تنها باید نشان دهیم $r(x)$ یگانه است. فرض می‌کنیم α برابر با $r_1(\theta)$ هم هست ــ که $r_1(x)$ از درجهٔ حداکثر $n-1$ است. پس $r(\theta) - r_1(\theta) = 0$ و θ در چندجمله‌ای $r(x) - r_1(x)$ صدق می‌کند. ولی θ در هیچ چندجمله‌ای با درجهٔ کمتر از n صدق نمی‌کند؛ و این نتیجه می‌دهد که $r_1(x)$ و $r(x)$ یکی هستند.

فرض می‌کنیم α_1، ...، α_n اعداد جبری روی F هستند. اگر $n > 1$، کوچکترین هیأت $K = F(\alpha_1, \ldots, \alpha_n)$ شامل F و α_iها یک توسیع جبری چندگانه[۷] از F نامیده می‌شود.

قضیهٔ ۷.۴. *یک توسیع جبری چندگانه F یک توسیع جبری ساده است.*

برای اثبات این قضیه، کافی است ثابت کنیم که وقتی α و β روی F جبری هستند، $F(\alpha, \beta)$ ساده است ــ یعنی برای بعضی θ های جبری روی F، $F(\alpha, \beta) = F(\theta)$ ــ زیرا اگر داشته باشیم $K = F(\alpha_1, \alpha_2, \alpha_3)$، می‌توان نوشت $K = F(\alpha_1, \alpha_2)(\alpha_3)$ و نتیجهٔ مربوط به دو عدد جبری را به کار بست، و به همین ترتیب برای $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

فرض می‌کنیم α_1، ...، α_n و β_1، ...، β_m به ترتیب مزدوج‌های α و β روی F هستند آنها را طوری شماره‌گذاری می‌کنیم که $\alpha_1 = \alpha$ و $\beta_1 = \beta$. اگر $K \neq 1$، آنگاه $\beta_k \neq \beta$؛ چون مزدوج‌ها روی F مجزا هستند. از این رو، به ازای هر i و هر K که $K \neq 1$، معادلهٔ

$$\alpha_i + x\,\beta_k = a_1 + x\,\beta_1$$

حداکثر یک جواب برای x در F دارد. چون از این معادلات و در نتیجه از جوابهای x به تعدادی متناهی موجود است، می‌توان یک عدد c که $c \neq 0$ را در F چنان انتخاب کرد که متفاوت از همهٔ جوابهای x باشد. در این صورت

$$\alpha_i + c\beta_k \neq \alpha + c\beta$$

به ازای هر i و هر k که $k \neq 1$. حال فرض می‌کنیم $\theta = \alpha + c\beta$. نشان خواهیم داد که $F(\theta) = F(\alpha, \beta)$ و این قضیه را ثابت خواهد کرد.

اولاً باید دانست که هر عضو $F(\theta)$ در $F(\alpha$ و $\beta)$ وجود دارد؛ چرا که طبق قضیهٔ ۶.۴، هر عضو $F(\theta)$ را می‌توان به صورت

$$a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1} = a_0 + a_1(x + c\beta) + \ldots + a_{n-1}(\alpha + c\beta)^{n-1},$$

نوشت؛ که سمت راست رابطهٔ مزبور یقیناً عضوی از $F(\alpha$ و $\beta)$ است.

حال باید نشان دهیم که هر عضو $F(\alpha$ و $\beta)$ در $F(\theta)$ است. اگر بتوانیم ثابت کنیم که β و α در $F(\theta)$ هستند، به نتیجه خواهیم رسید؛ زیرا اگر چنین باشد، آنها به صورت $\alpha = r(\theta)$ و $\beta = s(\theta)$ خواهند بود. در این صورت، هر عضو $F(\alpha$ و $\beta)$ به شکل

$$\frac{u(\alpha, \beta)}{v(\alpha, \beta)} = \frac{u(r(\theta), s(\theta))}{v(r(\theta), s(\theta))}$$

که یقیناً در $F(\theta)$ قرار دارد. ما برای منظور خود کافی است نشان دهیم که β در $F(\theta)$ است؛ زیرا در این صورت $\alpha = \theta - c\beta$ نیز در $F(\theta)$ خواهد بود.

فرض می‌کنیم $f(x)$ و $g(x)$ به ترتیب چند جمله‌ای‌های مینیمال α و β هستند. چون $f(\theta - c\beta) = f(\alpha) = 0$، عدد β در معادلهٔ $g(x) = 0$ و $f(\theta - cx) = 0$ صدق می‌کند. $g(x)$ و $f(\theta - cx)$، تنها ریشهٔ β را مشترکاً دارند؛ زیرا ریشه‌های $g(x)$ عبارتند از β_1، ...، β_m و اگر به ازای بعضی از مقادیر i $(i \neq 1)$ داشته باشیم $f(\theta - c\beta_i) = 0$، آنگاه $\theta - c\beta_i$ یکی از α_i هاست، که با انتخاب c در تناقض است.

حال، مشاهده می‌شود که $g(x)$ و $f(\theta - cx)$ چند جمله‌ای‌هایی بر حسب x هستند که ضرایب آنها در $F(\theta)$ بوده و دقیقاً دارای ریشهٔ مشترک β هستند. فرض می‌کنیم $h(x)$ چند جمله‌ای مینیمال β روی $F(\theta)$ است. طبق نتیجهٔ ۲.۴، $h(x) \mid g(x)$ و $h(x) \mid f(\theta - cx)$ در $F(\theta)$. $h(x)$ نمی‌تواند درجهٔ بیشتر از یک داشته باشد، زیرا در غیر این صورت $g(x)$ و $f(\theta - cx)$ بیش از

یک ریشهٔ مشترک خواهند داشت. از این رو $h(x) = \gamma x + \delta$، که γ و δ در $F(\theta)$ هستند. این در حالی است که $h(\beta) = ۰$، پس $\beta = \frac{-\delta}{\gamma}$ در $F(\theta)$ است؛ و بدین ترتیب حکم ثابت می‌شود.

به عنوان مثال، فرض می‌کنیم لازم است R ($\sqrt[3]{۲}$ و $\sqrt{۳}$) را به عنوان یک توسیع سادهٔ $R(\theta)$ بنویسیم. مزدوج‌های $\sqrt{۳}$ اعداد $\sqrt{۳}$ و $-\sqrt{۳}$ بوده و مزدوج‌های $\sqrt[3]{۲}$ اعداد $\sqrt[3]{۲}$ و $\sqrt[3]{۲}\omega$ و $\sqrt[3]{۲}\omega^{۲}$ هستند. در این حالت، می‌توان c را انتخاب کرد و بدین ترتیب $\theta = \sqrt{۳} + \sqrt[3]{۲}$. پس $R(\sqrt[3]{۲}) = R(\sqrt{۳} + \sqrt[3]{۲})$، $R(\sqrt{۳})$

حال دو اثبات از این واقعیت مهم که هر عضو یک توسیع جبری ساده، و در نتیجه هر عضو یک توسیع جبری چندگانه F، روی F جبری است را ارائه خواهیم داد. برای یکی از اثباتها، از نظریهٔ توابع متقارن استفاده خواهیم کرد. برای دیگری، از لم زیر، که در جبر مقدماتی است، استفاده خواهیم کرد ــ اثبات آن را می‌توان در پاراگراف ۲۷ کتاب تامس پیدا کرد (به فهرست منابع مراجعه شود).

لم ۸.۴. *اگر* $m > n$ *و اگر* a_{ij} *ها در یک هیأت* F *باشند، آنگاه دستگاه معادلات*

$$\sum_{j=۱}^{m} a_{ij}\, x_j = ۰ \quad \text{و} \quad i = ۱, ۲, , \ldots , n$$

برای $x_۱$، ...، x_n *دارای یک جواب، در* F *است که همهٔ* x_j *ها صفر نیستند.*

قضیهٔ ۹.۴. *اگر* θ *روی* F *جبری است، هر عضو* $F(\theta)$ *نیز چنین است.*

اثبات اول: فرض می‌کنیم α در $F(\theta)$ است و θ روی F از درجهٔ n است. طبق قضیهٔ ۶.۴، هر یک از توان‌های α^i ($i = ۰, ۱, \ldots, n$) از α را می‌توان به صورت

$$\alpha^j = \sum_{j=0}^{n-1} a_{ij}\,\theta^j ,$$

نوشت، که a_{ij} ها در F هستند. طبق لم پیشگفته، می‌توان مجموعه‌ای از اعداد d_i، که همگی صفر نیستند، را در F چنان یافت که

$$\sum_{i=0}^{n} a_{ij}\,d_i = 0 \qquad j = 0, 1, \ldots, n-1 ,$$

زیرا تعداد مجهولات d_i یکی بیشتر از تعداد معادلات است. پس

$$\sum_{i=0}^{n} d_i\,\alpha_i = \sum_{i=0}^{n} d_i \sum_{j=0}^{n-1} a_{ij}\,\theta^j = \sum_{j=1}^{n-1} \theta^j \sum_{i=0}^{n} a_{ij}\,d_i = 0$$

بنابراین α در چندجمله‌ای $d_n x^n + d_{n-1} x^{n-1} + \ldots + d_0$ روی F صدق می‌کند.

اثبات دوم: طبق قضیهٔ ۶.۴، $\alpha = r(\theta)$. فرض می‌کنیم

$$f(x) = \prod_{i=1}^{n} (x - r(\theta_i)) ,$$

که θ_1 و θ_2، ...، θ_n مزدوج‌های θ روی F هستند. طبق قضیهٔ ۱۱.۳، ضرایب $f(x)$ به صورت یک چندجمله‌ای بر حسب x در F هستند. به علاوه $f(\alpha) = 0$؛ و بدین صورت اثبات کامل می‌شود.

حال، امکان آن هست که ــ چنانکه قبلاً وعده داده بودیم ــ اثبات جدیدی از قضیهٔ ۵.۴ را مستقل از نظریهٔ توابع متقارن ارائه کنیم. برای این کار، باید نشان دهیم که وقتی α و β جبری هستند، $\alpha + \beta$، $\alpha - \beta$، $\alpha\beta$، و $\frac{\alpha}{\beta}$ $(\beta \neq 0)$ روی F نیز جبری هستند. هیأت $F(\alpha, \beta)$ را در نظر می‌گیریم، که در حالت خاص شامل این چهار عنصر است. بنابر قضیهٔ ۷.۴، این هیأت یک توسیع جبری ساده است، و بنابراین، طبق قضیهٔ ۹.۴ هر عضو

آن روی F جبری است.

۳. اعداد جبری و متعالی (غیرجبری). عدد θ یک عدد جبری نامیده می‌شود، اگر روی هیأت R از اعداد گویا، جبری باشد. طبق قضیهٔ ۵.۴، کلیهٔ اعداد جبری روی R تشکیل یک هیأت می‌دهند. منطقی است که بپرسیم آیا این هیأت بر هیأت همهٔ اعداد مختلط منطبق است و به عبارت دیگر آیا همهٔ اعداد، اعداد جبری هستند یا نه؟ با ارائه اعدادی که جبری نیستند، به این سؤال جواب منفی خواهیم داد، چنین اعدادی، *متعالی*[8] نامیده می‌شوند.

لم ۴.۱۰. *اگر θ یک عدد جبری حقیقی از مرتبهٔ $n > 1$ روی R است، آنگاه یک عدد مثبت M وجود دارد، به طوری که هر عدد گویای $\frac{p}{q}$، $q > 0$ داریم*

$$| \theta - \frac{p}{q} | \geq \frac{M}{q^n}$$

فرض می‌کنیم $f(x)$ یک چندجمله‌ای ابتدایی با کمترین درجه است که θ در آن صدق می‌کند. این چندجمله‌ای، حداکثر در یک مضرب ثابت با چندجمله‌ای مینیمال θ اختلاف دارد و بنابراین از درجهٔ n است. فرض می‌کنیم M' ماکزیمم $|f'(x)|$ در روی فاصلهٔ $\theta - 1 \leq x \leq \theta + 1$ بوده و M کوچکترین مقدار میان ۱ و $\frac{1}{M'}$ است. به ازای چنین مقداری از M، نامساوی مذکور صادق است. حال با توجه به آنچه گفته شد، اثبات دو قسمت دارد.

ابتدا، فرض می‌کنیم $| \theta - \frac{p}{q} | \geq 1$. در چنین شرایطی، به ازای هر دو عدد گویای p و q $(q \neq 0)$

8) *transcendental*

$$| \theta - \frac{p}{q} | \geq M \geq \frac{M}{q^n}$$

و بنابراین حکم برقرار می‌شود.

اگر $| \theta - \frac{p}{q} | < ۱$، اثبات مشکل‌تر است، طبق قانون میانگین

$$|F(\theta) - f(\frac{p}{q})| = | \theta - \frac{p}{q}| \ |f'(\xi)| \leq M' | \theta - \frac{p}{q}| ,$$

که در آن ξ بین θ و $\frac{p}{q}$ و در نتیجه در فاصلهٔ $(۱ + \theta$ و $۱ - \theta)$ قرار دارد. به علاوه $f(\theta) = ۰$؛ پس

$$|f(\frac{p}{q})| \leq M' | \theta - \frac{p}{q} |$$

حال مشاهده می‌شود که $f(\frac{p}{q}) \neq ۰$ زیرا در غیر این صورت $f(x)$ نمی‌تواند روی R تحویل‌ناپذیر باشد. چون $f(x)$ ضرایب صحیح دارد و از مرتبهٔ n است، $|f(\frac{p}{q})| = \frac{m}{q^n}$، که m یک عدد صحیح است. امّا $m \geq ۱$، به طوری که

$$\frac{۱}{q^n} \leq |f(\frac{p}{q})| \leq M' | \theta - \frac{p}{q} |$$

و از این رو با انتخاب M داریم

$$|\theta - \frac{p}{q} | \geq \frac{۱}{M'} \frac{۱}{q^n} \geq \frac{M}{q^n}$$

قضیهٔ ۱۱.۴. (*قضیهٔ لیوویل*[۹]). *اعداد متعالی وجود دارند.*

فرض می‌کنیم $\xi = \sum_{m=۱}^{\infty} (-۱)^m ۲^{-m!}$، و مجموع K جملهٔ اول سری ξ را با

$$\xi_k = \frac{p_k}{q_k} = \frac{p_k}{۲^{k!}}$$

نشان می‌دهیم. در این صورت

---

۹) *Liouville*

$$|\xi - \frac{p_k}{q_k}| = ۲^{-(k+۱)!} - ۲^{-(k+۲)!} + \ldots < ۲^{-(k+۱)!} < ۲^{-k.k!} = q_k^{-k}$$

فرض می‌کنیم ξ روی R جبری از مرتبهٔ $n > ۱$ است. طبق نامساوی قبل

$$q_k^n \mid \xi - \frac{p_k}{q_k} \mid \leq q_k^{n-k}$$

حال اگر $k \to \infty$، آنگاه

$$\lim q_k^n \mid \xi - \frac{p_k}{q_k} \mid = ۰$$

در اینجا یک تناقض به وجود می‌آید. زیرا، طبق لم پیشگفته، عددی مثل $M > ۰$ وجود دارد، به طوری که

$$|\xi - \frac{p_k}{q_k}| \geq \frac{M}{q^n{}_k} \quad ,$$

بنابراین برای هر k، $|q^n{}_k| \xi - \frac{p_k}{q_k} \geq M > ۰$، که با حد صفر به‌دست آمده متناقض است. پس ξ نمی‌تواند عددی جبری از مرتبهٔ $n > ۱$ باشد.

این موضوع، نتیجه می‌دهد که ξ یا یک عدد گویا ــ یعنی یک عدد جبری از مرتبهٔ ۱ ــ و یا یک عدد متعالی است. ما اولین امکان را رد می‌کنیم. فرض می‌کنیم $\xi = \frac{p}{q}$، که p و q اعداد گویا هستند و $q > ۰$. عدد فرد K را چنان انتخاب می‌کنیم که $۲^{k.k!} > q$. پس عدد η که به صورت زیر تعریف شده،

$$\eta = ۲^{k!}\,\xi q - ۲^{k!} q \sum_{m=۱}^{k} (-۱)^m ۲^{-m!} = ۲^{k!} q \sum_{m=k+۱}^{\infty} (-۱)^m ۲^{-m!}$$

تعریف شده، یک عدد صحیح گویای مثبت است. امّا با انتخاب K داریم

$$\eta < ۲^{k!} q \frac{۱}{۲^{(k+۱)!}} = \frac{q}{۲^{k!}} < ۱ \quad ۰$$

با این تناقض فقط حالتی باقی می‌ماند که ξ متعالی است.

عدد $\xi_i + \xi$ نیز متعالی است. زیرا اگر جبری، و در نتیجه، ریشهٔ یک چندجمله‌ای با ضرایب حقیقی باشد، مزدوج آن $\xi_i - \xi$ نیز یک ریشه است. بنابراین، مجموع $2\xi = (\xi_i - \xi) + (\xi + \xi_i)$ یک عدد جبری خواهد بود که می‌دانیم این غیرممکن است، چون ξ یک عدد جبری نیست.

برای خوانندهٔ آشنا با نظریهٔ شمارش‌پذیری، برای قضیهٔ ۱۱.۴ یک اثبات ساده‌تر نیز موجود است، هرچند هیچ مثال روشنی را از اعداد متعالی به دست نمی‌دهد. این اثبات، به اختصار به صورت زیر دنبال می‌شود : مجموعهٔ چندجمله‌ای‌های با ضرایب گویا شمارش‌پذیراست. هر یک از چندجمله‌ای‌های مزبور، تعدادی متناهی ریشه‌دارند. بنابراین، مجموعهٔ اعداد جبری شمارش‌پذیر است. این در حالی است که مجموعهٔ اعداد مختلط شمارش‌ناپذیر است؛ و در نتیجه، باید بعضی از آنها جبری نباشند.

تعیین متعالی بودن اعداد خاص، مسئلهٔ بسیار مشکلی است. در قرن اخیر، اعداد e و π به عنوان اعداد متعالی شناخته شده‌اند (در این خصوص، می‌توان در جلد ۳ کتاب وورلسونگن نوشتهٔ لانداو اثبات ساده‌ای را پیدا کرد، نگاه کنید به فهرست منابع). به هر ترتیب، اخیراً فقط اعدای چون e^{π} و $2^{\sqrt{2}}$ به عنوان اعداد متعالی نشان داده شده‌اند. این موضوع، نتیجه‌ای از قضیهٔ گلفوند و اشنایدر[10] است که ما در اینجا آن را بدون اثبات بیان می‌کنیم. یک اثبات آن توسط ای.هیل[11] در *ماهنامهٔ ریاضی آمریکا*، جلد ۴۹ (۱۹۴۲)، صفحات ۶۵۴ تا ۶۶۱ ارائه شده است.

---

10) *Gelfond and Schneider* 11) *E. Hille*

قضیهٔ ۱۲.۴. *فرض می‌کنیم α و β اعداد متعالی غیر از ۰ و ۱ هستند. اگر عدد*

$$\eta = \frac{log\ \alpha}{log\beta}$$

غیرگویا است، آنگاه متعالی نیز هست.

این قضیه را با اثبات اینکه $۲^{\sqrt{۲}}$ متعالی است شرح خواهیم داد. اگرچنین نیست، $۲^{\sqrt{۲}} = \alpha$ باید عدد جبری باشد. β را مساوی با ۲ می‌گیریم. چون

$$\eta = \frac{log\ ۲^{\sqrt{۲}}}{log\ ۲} = \sqrt{۲}$$

غیرگویاست، پس η باید متعالی باشد، این مطلب به وضوح نادرست است؛ بنابراین α نمی‌تواند جبری باشد.

بحثی مشابه ثابت می‌کند که e^{π} متعالی است، به شرط آنکه ابتدا نشان دهیم e^{π} را می‌توان به صورت $i^{-۲i}$ نوشت. انجام و تکمیل جزئیات این اثبات به عهدهٔ خواننده گذاشته می‌شود.

فصل ۵

پایه‌ها

۱. پایه‌ها و توسیع‌های متناهی. فرض می‌کنیم F یک هیأت اعداد و K یک توسیع آن است. مجموعهٔ اعداد α_1، α_2، ... ، α_r در K (روی F) *وابستهٔ خطی*[1] خوانده می‌شود، اگر بتوان در F مجموعه‌ای از اعداد c_1، c_2، ... ، c_r، که همگی صفر نیستند، را یافت به طوری که

$$c_1 \alpha_1 + c_2 \alpha_2 + \ldots + c_r \alpha_r = 0$$

در غیر این صورت، اعداد α_1، α_2، ... ، α_r *مستقل خطی*[2] نامیده می‌شوند.

مجموعهٔ اعداد β_1، β_2، ... ، β_s در K تشکیل یک *پایه*[3] را روی F برای K می‌دهند. اگر برای هر عضو β در K مجموعهٔ یگانه‌ای از اعداد d_1، d_2، ... ، d_s در F موجود باشد، به طوری که

---

1) *Linearly dependent* 2) *Linearly independent*

۳) Base ، در متون قدیمی‌تر یک دستگاه اساسی *fundamental system* نیز نامیده شده است.

$$\beta = d_1 \beta_1 + d_2 \beta_2 + \ldots + d_s \beta_s .$$

باید توجه داشت که β_iها مستقل خطی هستند؛ زیرا در غیر این صورت o نمایشی به صورت زیر دارد

$$o = e_1 \beta_1 + e_2 \beta_2 + \ldots + e_s \beta_s ,$$

که همهٔ e_iها صفر نیستند، و همچنین نمایشی به صورت

$$o = o \cdot \beta_1 + o \cdot \beta_2 + \ldots + o \cdot \beta_s ,$$

که با لزوم یگانگی در تناقض است.

لم ۱.۵. *اگر K یک پایه از S عنصر روی F داشته باشد، آنگاه در K هر t عدد $(t>s)$ روی F وابستگی خطی دارند.*

فرض می‌کنیم β_1، ...، β_s یک پایه برای K، و α_1، ...، α_t، t عدد در K هستند. طبق تعریف یک پایه، می‌توان در F اعداد a_{ij} را چنان یافت که

$$\alpha_i = \sum_{j=1}^{s} a_{ij} \beta_j , \qquad i = 1 ، \ldots ، t$$

چون $t > s$، می‌توان با استناد به لم ۸.۴ نتیجه گرفت که اعداد c_i، که همگی صفر نیستند، در F موجودند به طوری که

$$\sum_{j=1}^{t} a_{ij} \cdot c_i = o \qquad j = 1 ، \ldots ، s$$

که نتیجه می‌دهد

$$\sum_{i=1}^{t} c_i \alpha_i = \sum_{i=1}^{t} c_i \sum_{j=1}^{s} a_{ij} \beta_j = \sum_{j=1}^{s} \beta_j \sum_{i=1}^{t} a_{ij} c_i = o ,$$

بنابراین، α_iها وابستهٔ خطی هستند.

قضیهٔ ۲.۵. *اگر $\alpha_1, \ldots, \alpha_t$ و $\beta_1, \ldots, \beta_s$ هر دو پایه‌هایی برای K روی F هستند، آنگاه $s = t$.*

اگر $s \neq t$، می‌توان فرض کرد که $t > s$. طبق لم پیشگفته، α_i ها باید وابستهٔ خطی باشند. این غیرممکن است؛ چون آنها تشکیل یک پایه را می‌دهند.

ملاحظه کردیم که اگر K یک پایه روی F داشته باشد، تمامی پایه‌ها n عضو دارند. n مرتبهٔ k روی F و K یک توسیع متناهی[۴] مرتبهٔ n روی F نامیده می‌شود (می‌نویسیم $n = (\frac{K}{F})$).

لم ۳.۵. *اگر K یک توسیع متناهی مرتبهٔ n روی F است، آنگاه هر n عضو مستقل خطی در K تشکیل یک پایه را می‌دهد.*

فرض می‌کنیم $\beta_1, \ldots, \beta_n$ یک پایه برای K روی F بوده و $\alpha_1, \ldots, \alpha_n$ یک مجموعهٔ n عضوی مستقل خطی از K است. می‌خواهیم نشان دهیم که هر عضو α قابل نمایش به صورت زیر است،

$$\alpha = d_1 \alpha_1 + d_2 \alpha_2 + \ldots + d_n \alpha_n$$

که مستقیماً از استقلال خطی α_i ها نتیجه می‌شود چنین نمایشی یکتاست.

چون β_i ها تشکیل یک پایه را می‌دهند، می‌توان نوشت

$$\alpha_i = \sum_{j=1}^{n} a_{ij} \beta_j \qquad i = 1, \ldots, n$$

$$\alpha = \sum_{j=1}^{n} a_{\cdot j} \beta_j$$

طبق لم ۸.۴، می‌توان c_i هایی، که همگی صفر نیستند، را در F چنان

یافت که

$$\sum_{i=0}^{n} a_{ij}\, c_i = 0\,, \qquad j = 1, \ldots, n$$

پس

$$c_0\alpha + c_1\,\alpha_1 + c_2\,\alpha_2 + \ldots + c_n\,\alpha_n = \sum_{i=0}^{n} c_i \sum_{j=1}^{n} a_{ij}\,\beta_j = \sum_{j=1}^{n} \beta_j \sum_{i=0}^{n} c_i\, a_{ij} = 0$$

حال $c_0 \neq 0$، چون در غیر این صورت $c_1\,\alpha_1 + \ldots + c_n\,\alpha_n = 0$، و بنا بر استقلال خطی α_iها، همهٔ c_iها صفر خواهند بود. از این رو

$$\alpha = -\frac{c_1}{c_0}\,\alpha_1 - \frac{c_2}{c_0}\,\alpha_2 - \ldots - \frac{c_n}{c_0}\,\alpha_n\,,$$

و این همان چیزی است که می‌خواستیم نشان دهیم.

قضیهٔ ۴.۵. *اگر $\alpha_1, \ldots, \alpha_n$ یک پایه برای K روی F بوده و*

$$\beta_j = \sum_{i=1}^{n} a_{ij}\,\alpha_i \qquad \text{و} \quad j = 1, 2, \ldots, n$$

a_{ij}ها در F هستند، آنگاه $\beta_1, \ldots, \beta_n$ نیز یک پایه است، اگر و فقط اگر دترمینان $|a_{ij}|$ غیر صفر باشد.

ابتدا فرض می‌کنیم $|a_{ij}| \neq 0$. طبق نتایج قبلی، کافی است نشان دهیم β_jها مستقل خطی هستند. فرض می‌کنیم $\sum_{j=1}^{n} c_j\,\beta_j = 0$، و c_jها در F هستند. در نتیجهٔ این موضوع

$$0 = \sum_{j=1}^{n} c_j \sum_{i=1}^{n} a_{ij}\,\alpha_i = \sum_{i=1}^{n} \alpha_i \sum_{j=1}^{n} c_j\, a_{ij}$$

امّا چون α_iها مستقل خطی هستند:

$$\sum_{j=1}^{n} c_j a_{ij} = 0, \qquad i = 1, \ldots, n$$

دترمینان $|a_{ij}|$ مخالف صفر است. بنابراین، همهٔ c_jها باید صفر باشند.

برعکس، فرض می‌کنیم $|a_{ij}| = 0$. در این صورت، معادلات پیشگفته، یک جواب با c_jهایی که همگی صفر نیستند دارد با طی کردن مراحل قبلی، در جهت عکس، به دست می‌آید

$$\sum_{j=1}^{n} c_j \beta_j = 0,$$

و بنابراین β_jها مستقل خطی نیستند.

۲. خواص توسیع‌های متناهی. در این قسمت، قصد داریم نشان دهیم که توسیع‌های متناهی و توسیع‌های سادهٔ جبری یک هیأت، یکی هستند.

لم ۵.۵. *اگر K یک توسیع متناهی F است، آنگاه هر عضو α از K روی F جبری است.* فرض می‌کنیم $n = (\frac{K}{F})$. طبق لم ۱.۵، $n+1$ عدد $1, \alpha, \alpha^2, \ldots, \alpha^n$ وابستهٔ خطی هستند، بنابراین $c_0, c_1, \ldots, c_n$ که همگی صفر نیستند در F موجودند، به طوری که

$$c_0 + c_1 \alpha + \ldots + c_n \alpha^n = 0$$

این موضوع، نتیجه می‌دهد که α در یک چندجمله‌ای روی F صدق می‌کند.

قضیهٔ ۶.۵. *یک توسیع K از F متناهی است، اگر و تنها اگر یک توسیع سادهٔ جبری باشد.*

ابتدا فرض می‌کنیم که K یک توسیع متناهی F و α_1، ...، α_n یک پایه است. در این صورت، $K = F(\alpha_1, \ldots, \alpha_n)$. طبق لم پیشگفته هر α_i روی F جبری است. از قضیهٔ ۷.۴ نیز نتیجه می‌شود که K یک توسیع جبری سادهٔ F است.

برعکس فرض می‌کنیم $K = F(\theta)$، که θ روی F از مرتبهٔ n است. طبق قضیهٔ ۶.۴، اعداد 1، θ، ...، θ^{n-1} تشکیل یک پایه برای K روی F می‌دهند. این معنی، اثبات را کامل می‌کند (باید توجه داشت که (K/F) همان مرتبهٔ θ روی F است).

قضیهٔ ۷.۵. *اگر K روی F و E روی K متناهی است، آنگاه E روی F متناهی است؛ علاوه بر اینکه*

$$(E/F) = (E/K) \cdot (K/F)$$

فرض می‌کنیم α_1، ...، α_n پایهٔ K روی F و β_1، ...، β_m پایهٔ E روی K است. به راحتی ثابت می‌شود که mn حاصل‌ضرب $\alpha_i \beta_j$ مستقل خطی هستند. حال، نشان خواهیم داد که آنها روی F تشکیل یک پایه را برای E می‌دهند.

اگر α عددی در E است، می‌توان آن را به صورت $\alpha = \sum_{i=1}^{m} \gamma_i \beta_i$ نوشت، که γ_iها در K هستند، زیرا β_iها روی F تشکیل یک پایه را برای E می‌دهند. به طور مشابه، هر γ_i را می‌توان به صورت $\sum_{j=1}^{n} a_{ij} \alpha_j$ نوشت، که a_{ij}ها در F هستند، زیرا α_iها برای K تشکیل یک پایه را روی F می‌دهند. پس

$$\alpha = \sum_{i=1}^{m} \beta_i \sum_{j=1}^{n} a_{ij} \alpha_j = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \alpha_j \beta_i ,$$

و این همان چیزی است که می‌خواستیم. فرمول داده شده در قضیه نیز،

بلافاصله نتیجه می‌شود.

حال می‌توان شکل بهبود یافتهٔ لم ۵.۵ را ثابت کرد.

نتیجهٔ ۸.۵. *اگر K روی F از مرتبهٔ n است، آنگاه هر عضو α از K روی F جبری است و مرتبهٔ آن n را عاد می‌کند.*

فرض می‌کنیم $E = F(\alpha)$. در این صورت

$$n = (K/F) = (K/E)\,(E/F)$$

از این رو (E/F) ، n را عاد می‌کند؛ و این در حالی است که با ملاحظهٔ قسمت آخر اثبات قضیهٔ ۶.۵ نتیجه می‌شود که مرتبهٔ E روی F همان مرتبهٔ α روی F است.

قضیهٔ ۹.۵. *اگر α در معادلهٔ*

$$\alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_0 = 0$$

صدق کند، که α_i ها روی F جبری هستند، آنگاه α روی F جبری است.

فرض می‌کنیم $E = F(\alpha_1, \ldots, \alpha_n)$. این رابطه، می‌تواند به صورت یک توسیع جبری سادهٔ F نوشته شود. طبق قضیهٔ ۶.۵، E یک توسیع متناهی F است. به علاوه $E(\alpha)$ یک توسیع متناهی E و از این رو، طبق قضیهٔ ۷.۵، یک توسیع متناهی F است. پس α در یک توسیع متناهی F قرار دارد؛ و در این حال می‌توان گفت که طبق نتیجهٔ قبل α روی F جبری است.

در بیشتر مواردی که در این کتاب بدانها برخورد خواهیم کرد، هیأت F هیأت R از اعداد گویا خواهد بود. یک هیأت *اعداد جبری*[5] ، هر توسیع

---

5) *algebric number field*

متناهی (و از این رو سادهٔ) R است. کلیهٔ اعداد جبری تشکیل یک هیأت اعداد جبری را نمی‌دهند، و حال آنکه تشکیل یک هیأت را می‌دهند (قضیهٔ ۵.۴). در توجیه آنچه گفته شد، فرض می‌کنیم این هیأت روی R از مرتبهٔ n است. در این حالت، وجود یک عضو از مرتبهٔ بزرگتر از n با نتیجهٔ ۸.۵ در تناقض است. امّا بسادگی می‌توان یک عدد جبری از مرتبهٔ $n+1$ ساخت. چندجمله‌ای $x^{n+1}-2$ ـ طبق محک آیزنشتاین ـ روی R تحویل‌ناپذیر است. بنابراین، $2^{1/n+1}$ از مرتبهٔ $n+1$ است.

۳. مزدوج‌ها و مبین‌ها. خواننده به یاد می‌آورد که مزدوج‌های روی F یک عدد جبری α روی F، ریشه‌های چندجمله‌ای مینیمال α روی F هستند. ما این موضوع را برای تعریف یک مفهوم جدید از مزدوج بودن و بررسی رابطهٔ آن با مفهوم قبلی مفید می‌دانیم.

فرض می‌کنیم $K = F(\theta)$ یک توسیع متناهی مرتبهٔ n روی F بوده و α یک عدد در K است. طبق نتیجهٔ ۸.۵ m، مرتبهٔ α روی F، n را عاد می‌کند. طبق قضیهٔ ۶.۴، α را می‌توان به صورتی یگانه به شکل زیر نوشت

$$\alpha = \sum_{i=0}^{n-1} c_i \theta^i = r(\theta) .$$

فرض می‌کنیم $\theta_1, \ldots, \theta_n$ مزدوج‌های θ روی F هستند. در این صورت، اعداد

$$\alpha_i = r(\theta_i) \quad , \qquad i = 1, \ldots, n$$

مزدوج‌های α در $F(\theta)$ نامیده می‌شوند. بنابراین α، n مزدوج در حالت جدید، و m مزدوج در حالت قبلی دارد، که $m \mid n$.

بسادگی ثابت می‌شود که مزدوج‌های $\alpha\beta$ و $\alpha+\beta$ برای $F(\theta)$ به ترتیب $\alpha_1\beta_1, \ldots, \alpha_n\beta_n$ و $\alpha_1+\beta_1, \ldots, \alpha_n+\beta_n$ هستند.

قضیهٔ بعدی، رابطهٔ بین مزدوج‌های جدید و قدیم را برقرار می‌کند.

قضیهٔ ۵.۱۰. *(۱) مزدوج‌های α برای $F(\theta)$ همان مزدوج‌های روی F هستند که هرکدام $\frac{n}{m}$ بار تکرار شده‌اند. (۲) α در F است، اگر و تنها اگر همهٔ مزدوج‌ها برای $F(\theta)$ یکسان باشند. (۳) $F(\alpha) = F(\theta)$، اگر همهٔ مزدوج‌های $F(\alpha)$ برای $F(\theta)$ مجزا باشند.*

چنانکه در اثبات دوم قضیهٔ ۹.۴ نشان دادیم، چندجمله‌ای

$$f(x) = \prod_{1}^{n} (x - r(\theta_i))$$

یک چندجمله‌ای روی F است و $f(\alpha) = 0$. چندجمله‌ای $f(x)$ چندجمله‌ای هیأت α نامیده می‌شود. فرض می‌کنیم $g(x)$ چندجمله‌ای مینیمال α روی F است. طبق نتیجهٔ ۲.۴، $f(x) \mid g(x)$ و بنابراین می‌توان نوشت

$$f(x) = [g(x)]^s h(x) \ ,$$

که $g(x)$ و $h(x)$ نسبت به هم اولند. ثابت می‌کنیم که $h(x) \equiv 1$. باید توجه داشت که اگر $h(x)$ همه جا یک ثابت است، باید آن را ۱ در نظر گرفت؛ چون $g(x)$ و $f(x)$ تکین هستند.

اگر $h(x)$ ثابت نیست، ریشه‌ای مثل $r(\theta_i)$ دارد. پس $h(r(x))$ وقتی x برابر یکی از مقادیر θ_i است صفر می‌شود. فرض می‌کنیم $p(x)$ چندجمله‌ای مینیمال برای θ، و از این رو برای θ_i، است. در این صورت، $p(x) \mid h(r(x))$. این موضوع، نتیجه می‌دهد که $h(r(x))$ به ازای همهٔ θ_i ها و بخصوص به ازای θ صفر است. بنابراین، $h(r(\theta)) = h(\alpha) = 0$. چنین چیزی طبق نتیجهٔ ۳.۴ غیرممکن است؛ چون $g(\alpha) = 0$، $g(x)$ و $h(x)$ نسبت به هم اولند.

از این رو $f(x) = [g(x)]^s$. چون m مرتبهٔ α روی F است، $S = \frac{n}{m}$ و

چندجمله‌ای هیأت توانی از چندجمله‌ای مینیمال است. این مطلب، قسمت (۱) قضیه را ثابت می‌کند.

در خصوص قسمت (۲)، باید گفت که اگر α در F است، آنگاه $g(x) = x - \alpha$، $m = ۱$، $S = \frac{n}{m} = n$، $f(x) = (x - \alpha)^n$ و بنابراین همهٔ مزدوج‌ها یکی هستند. نتیجه‌گیری مزبور، در جهت عکس نیز می‌تواند عمل شود؛ بدین معنی که اگر همهٔ مزدوج‌ها یکسان باشند، $f(x) = (x - \alpha)^n$ و بنابراین $S = n$، $m = ۱$، و α در F است.

بالاخره، قسمت (۳) را اثبات می‌کنیم. قابل توجه است که

$$(\frac{F(\theta)}{F}) = (\frac{F(\theta)}{F(\alpha)}) \cdot (\frac{F(\alpha)}{F}) ,$$

پس $F(\theta) = F(\alpha)$، اگر و تنها اگر $m = n$ و $S = ۱$. در این حالت $f(x) = g(x)$ و همهٔ مزدوج‌ها مجزا هستند، $s = ۱$، $m = n$ و نتیجهٔ دلخواه به دست می‌آید. بدین ترتیب، آخرین قسمت قضیه نیز ثابت می‌شود.

حال، فرض می‌کنیم $K = F(\theta)$ از مرتبهٔ n روی F و $\alpha_۱$، ...، α_n یک پایه است. مزدوج‌های α_j در K را به صورت $\alpha_j^{(i)}$ و n، ...، $i = ۱$، نشان می‌دهیم. مبین مجموعهٔ $\alpha_۱$، ...، α_n به صورت زیر تعریف می‌شود،

$$\Delta [\alpha_۱ ، \dots ، \alpha_n] = |\alpha_j^{(i)}|^۲ ,$$

که $|\alpha_j^{(i)}|$ دترمینان زیر است :

$$\begin{vmatrix} \alpha_۱^{(۱)} & \alpha_۲^{(۱)} & \dots & \alpha_n^{(۱)} \\ \dots & \dots & \dots & \dots \\ \alpha_۱^{(n)} & \alpha_۲^{(n)} & \dots & \alpha_n^{(n)} \end{vmatrix}$$

حال، اگر

$$\beta_k = \sum_{j=1}^{n} c_{jk}\,\alpha_j \quad \text{و} \qquad K = 1, \ldots, n$$

پایه دیگری است، آنگاه طبق قضیهٔ ۴.۵، $|c_{jk}| \neq 0$. با ضرب کردن دترمینان‌ها در یکدیگر، به این فرمول مهم می‌رسیم که

$$\Delta\,[\beta_1, \ldots, \beta_n] = |c_{jk}|^2\,\Delta\,[\alpha_1, \ldots, \alpha_n]\,. \qquad (5.1)$$

بنابر قضیهٔ ۶.۴، یک پایهٔ خاص $F(\theta)$ به صورت $1, \theta, \theta^2, \ldots, \theta^{n-1}$ است. اگر این حقیقت را در نظر بگیریم که $(\theta^{i})^{(j)}$ (مزدوج jام، θ^{i}) همان $(\theta^{(j)})^{i}$ (توان iام $\theta^{(j)}$) است، به دست می‌آوریم که

$$D(\theta) = \Delta\,[1, \theta, \ldots, \theta^{n-1}] = \begin{vmatrix} 1 & \theta^{(1)} & (\theta^{(1)})^2 & \ldots & (\theta^{(1)})^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \theta^{(n)} & (\theta^{(n)})^2 & \ldots & (\theta^{(n)})^{n-1} \end{vmatrix}^2$$

و این دترمینان که به عنوان دترمینان *واندرموند*[7] شناخته می‌شود، مقدار زیر را دارد[8] :

$$D\,(\theta) = \prod_{1 \leq i < j \leq n} (\theta^{(i)} - \theta^{(j)})^2 \qquad (5.2)$$

$D\,(\theta) \neq 0$، چون مزدوج‌های θ برای $F\,(\theta)$ الزاماً مجزا هستند. چون $D\,(\theta)$ بر حسب $\theta^{(i)}$ متقارن است، یک عضو F است. به وضوح می‌توان دید که این مقدار مثبت است، اگر همهٔ $\theta^{(i)}$ ها حقیقی باشند. در رابطهٔ (۵.۱)، در

---

7) Vandermonde determinant

8) Uspensky, *Theory of Equations, P. 214.*

نظر می‌گیریم که $\alpha_i = \theta^{i-1}$، $i = ۱، \ldots، n$. پس

$$\Delta[\beta_۱, \ldots, \beta_n] = |c_{j\,k}|^۲ D(\theta)$$

عضوی از F است. بدین ترتیب، قضیهٔ بعدی هم اثبات می‌شود:

قضیهٔ ۱۱.۵. *مبین هر پایه برای (θ) F عضوی از F است و هرگز صفر نمی‌شود. اگر F، θ و مزدوج‌های θ همه حقیقی باشند، آنگاه مبین هر پایه مثبت است.*

۴. هیأت تقسیم دایره. حال دربارهٔ نوعی خاص از هیأت که بسیار مهم است بحث می‌کنیم. این موضوع به عنوان شرحی از نظریهٔ قبلی سودمند و در زمینهٔ کارهای بعدی مفید خواهد بود.

فرض می‌کنیم P یک عدد اول فرد است. طبق قضیهٔ ۹.۳، چندجمله‌ای تقسیم دایره $x^{P-۱} + x^{P-۲} + \ldots + ۱$ روی R تحویل‌ناپذیر است. از این رو، هر ریشهٔ ξ آن یک هیأت $R(\xi)$ از مرتبهٔ $P-۱$ روی R تولید می‌کند، که $R(\xi)$ یک *هیأت تقسیم دایره*[9] نامیده می‌شود.

اگر ξ یک ریشهٔ چندجمله‌ای مذکور است، آنگاه ξ، $\xi^۲$، $\ldots$، $\xi^{P-۱}$ همه، ریشه‌های دیگر آن هستند؛ زیرا:

۱ـ هیچ یک از ξ^s ها، ۱ نیستند؛ چون در غیر این صورت ξ در یک چندجمله‌ای $x^s - ۱$ با مرتبهٔ کمتر از $P-۱$ صدق خواهد کرد؛

۲ـ به دلیلی مشابه، همهٔ آنها مجزا هستند؛ و

۳ـ همهٔ آنها در $x^P - ۱ = ۰$ صدق می‌کنند؛ چون $(\xi^P)^s - ۱ = ۰$ $(\xi^s)^P - ۱$. ریشه‌های مورد بحث $(\xi، \ldots، \xi^{P-۱})$، ریشه‌های P ام ابتدایی

9) *Cyclotomic field*

واحد[10] نامیده می‌شوند؛ چون آنها روی یک دایره با شعاع واحد قرار داشته و هیچ یک ۱ ± نیستند، همهٔ آنها موهومی هستند. پس مزدوج‌های ξ برای $R(\xi)$، عبارتند از ξ^2، ...، ξ^{p-1}. از این رو، می‌توان نوشت $\xi^{(i)} = \xi^i$. ما از این مطلب برای محاسبهٔ $D(\xi)$ استفاده خواهیم کرد.

بنابر قضیهٔ ۶.۴ با داشتن مقدار $n = p - ۱$، یک پایه برای $R(\xi)$ عبارت است از: ۱، ξ، ...، ξ^{p-2}. طبق رابطهٔ (۵.۲)

$$D(\xi) = \prod_{0 \le i < j \le p-2} (\xi^i - \xi^j)^2$$

و امّا پایهٔ دیگر ξ، ξ^2، ...، ξ^{p-1} است؛ زیرا این مجموعه از اعداد روی R مستقل خطی هستند. رابطهٔ بین این دو پایه چنین داده شده است:

$$\begin{aligned}
\xi &= 0 + \xi \\
\xi^2 &= 0 + 0 + \xi^2 \\
&\cdots \\
\xi^{p-2} &= 0 + 0 + \ldots + \xi^{p-2} \\
\xi^{p-1} &= 1 - \xi - \xi^2 - \ldots - \xi^{p-2} \quad ,
\end{aligned}$$

بنابراین، مجذور دترمینان $|c_{jk}|$ برابر با ۱ است. از این رو، طبق روابط (۵.۱)، (۵.۲) و (۵.۳)، $D(\xi) = \Delta[\xi, \xi^2, \ldots, \xi^{p-1}] = \prod_{1 \le i < j \le p-1} (\xi^i - \xi^j)^2$.

قضیهٔ ۱۲.۵. *اگر ξ یکی از ریشه‌های Pام ابتدایی واحد و P یک عدد فرد است، آنگاه*

$$D(\xi) = (-1)^{\frac{(p-1)}{2}} p^{p-2}$$

---

10) *primitive P^{th} roots of unity.*

چون ξ، ...، ξ^{p-1} همه ریشه‌های ابتدایی هستند، داریم

$$\frac{x^p - 1}{x - 1} = x^{p-1} + \ldots + 1 = \prod_{i=1}^{p-1} (x - \xi^i) \qquad (5.4)$$

از طرفین مشتق می‌گیریم و چنین قرار می‌گذاریم که $x = \xi^j$. چون $\xi^p = 1$، به دست می‌آوریم

$$-\frac{P\xi^{p-j}}{1 - \xi^j} = \prod_{\substack{i=1 \\ i \neq j}}^{p-1} (\xi^j - \xi^i) \qquad (5.5)$$

طبق رابطهٔ (۵.۴)، با در نظر گرفتن اینکه $x = 0$ و $x = 1$، به ترتیب نتیجه می‌شود

$$\prod_{j=1}^{p-1} \xi^{p-j} = \xi \cdot \xi^2 \ldots \xi^{p-1} = (-1)^{p-1}$$

$$\prod_{j=1}^{p-1} (1 - \xi^j) = P$$

از این رو، طبق رابطهٔ ۵

$$P^{p-2} = \prod_{j=1}^{p-1} \prod_{\substack{i=1 \\ i \neq j}}^{p-1} (\xi^j - \xi^i)$$

در حاصل‌ضرب آخر، برای نیمی از عامل‌ها $i<j$ و برای نیمی دیگر $j<i$. مجموعاً $(P-2)(P-1)$ عامل وجود دارند. در نتیجه حاصل‌ضرب اخیر به

صورت زیر است.

$$P^{p-2} = (-1)^{(p-1)(p-2)/2} \prod_{1 \le i < j \le p-1} (\zeta^i - \zeta^j)^2$$

امّا P فرد است؛ پس

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

اگر این حقایق را با رابطهٔ (۵.۳) ادغام کنیم، اثبات قضیه کامل خواهد شد.

فصل ۶

اعداد صحیح جبری و پایه‌های صحیح

۱. **اعداد صحیح جبری.** فرض می‌کنیم $R(0)$ یک هیأت اعداد جبری است. منظور از یک عدد صحیح در این هیأت چیست؟ با مثالی از اعداد صحیح گاوسی به عنوان «اعداد صحیح» در $R(i)$، شرایط زیر برای طرح تعریف قابل قبول به نظر می‌رسند:

۱ـ اگر α و β در $R(\theta)$ عدد صحیح هستند، $\alpha+\beta$، $\alpha-\beta$ و $\alpha\beta$ نیز چنین هستند؛

۲ـ اگر α عدد صحیحی در $R(0)$ و همچنین عددی گویا است، آنگاه یک عدد صحیح گویاست؛

۳ـ اگر α عددی صحیح است، مزدوج‌های آن نیز صحیح هستند (این معنی در خصوص هر دو مفهوم «مزدوج» بودن صدق می‌کند).

تعریف ذکرشونده، تمام شرایط مورد نیازی که به آنها اشاره شد را برآورده می‌کند: یک عدد جبری، یک عدد صحیح جبری است، اگر ضرایب چندجمله‌ای مینیمال آن تنها اعداد صحیح گویا باشند. حال، چون یک چندجمله‌ای مینیمال تکین است، α باید در یک

معادله

$$P(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0 = 0 \quad ,$$

صدق کند، که در آن a_i ها اعداد صحیح گویا هستند. در نتیجه، شرط ۳ خودبه‌خود برقرار می‌شود. باید توجه داشت که شرط ۲ نیز به راحتی برقرار می‌شود؛ زیرا اگر α در $P(x)$ صدق می‌کند و گویا است، آنگاه مرتبهٔ آن روی R، ۱ است، پس $n = 1$، و بنابراین چندجمله‌ای مینیمال به طور ساده $x + a_0 = 0$ است.

اثبات برقراری شرط ۱ تا اندازه‌ای پیچیده‌تر است. برای این منظور، توجه به آنچه در ادامه ذکر خواهد شد ضروری است.

لم ۱.۶. *اگر α در هر چندجمله‌ای تکین $f(x)$ با ضرایب صحیح گویا صدق کند آنگاه α یک عدد صحیح جبری است.*

فرض می‌کنیم $p(x)$ چندجمله‌ای مینیمال α روی R است که تکین است. می‌خواهیم ثابت کنیم همهٔ ضرایب آن، عدد صحیح هستند. این موضوع، نتیجه خواهد داد که α یک عدد صحیح جبری است.

طبق نتیجهٔ ۲.۴، $f(x) = p(x)\,q(x)$، که در آن $q(x)$ یک چندجمله‌ای روی R است. اثبات قضیهٔ ۷.۳ نشان می‌دهد که $f(x) = c_f\,p^*(x)\,q^*(x)$، که در آن $p(x) = c_p\,p^*(x)$ و $p^*(x)$ و $q^*(x)$ ابتدایی هستند. $f(x)$، به علت تکین بودن ابتدایی است، و $p^*(x).c_f = 1$ و $q^*(x)$ به خاطر داشتن ضرایب صحیح باید تکین باشند؛ زیرا حاصل‌ضرب آنها $f(x)$ تکین است. امّا $p(x)$ نیز تکین است. از این رو، $c_p = 1$، و $p(x) = p^*(x)$ ضرایب صحیح دارد.

قضیهٔ ۲.۶. *اگر $R(\theta)$ یک هیأت اعداد جبری است، آنگاه اعداد صحیح آن خواص ۱، ۲ و ۳ مذکور در ابتدای فصل، را دارند.*

می‌ماند. فرض می‌کنیم α_1، ...، α_n و β_1، ...، β_k به ترتیب مزدوج‌های اعداد صحیح جبری $\alpha = \alpha_1$ و $\beta = \beta_1$ روی R هستند.

توابع متقارن ابتدایی از β_1، ...، β_k اعداد صحیح گویا هستند، چون آنها، بجز در علامت، ضرایب چندجمله‌ای مینیمال عدد صحیح جبری β هستند. این موضوع از قسمت دوم قضیهٔ ۱۰.۳ نتیجه می‌شود که *هر چندجمله‌ای متقارن از* β_1، ...، β_k *که ضرایب آن، اعداد صحیح گویا هستند، یک عدد صحیح گویاست.*

حال فرض می‌کنیم $f(x)$ چندجمله‌ای مینیمال عدد صحیح α است و تعریف می‌کنیم

$$h(x) = \prod_{j=1}^{k} f(x - \beta_j)$$

عبارت فوق، یک چندجمله‌ای بر حسب x است. چون $f(x)$ ضرایب صحیح دارد، ضرایب $h(x)$ چندجمله‌ای‌های متقارن از β_j با ضرایب صحیح گویا هستند. طبق قسمت دوم قضیهٔ ۱۰.۳ که در بالا یادآوری شد، $h(x)$ ضرایب صحیح گویا دارد. چون $f(x)$ تکین است، $h(x)$ نیز تکین است. سرانجام اینکه چون $f(\alpha_1) = 0$

$$h(\alpha + \beta) = h(\alpha_1 + \beta_1) = f(\alpha_1 + \beta_1 - \beta_1) \prod_{j=2}^{k} f(\alpha_1 + \beta_1 - \beta_j) = 0,$$

پس بنابر لم ۱.۶، $\alpha + \beta$ یک عدد صحیح جبری بوده و متعلق به $R(\theta)$ است؛ چرا که α و β در $R(\theta)$ هستند. اثبات در مورد $\alpha - \beta$ و $\alpha\beta$ مشابه است و به آن نمی‌پردازیم (به اثبات اول قضیهٔ ۵.۴ رجوع کنید).

در ضمن، باید توجه داشت که این اثبات نشان می‌دهد که وقتی α و β عدد صحیح جبری هستند، $\alpha + \beta$، $\alpha - \beta$ و $\alpha\beta$ نیز اعداد صحیح جبری هستند؛ حتی اگر فرض نکنیم که α و β در هیأت داده شده $R(\theta)$ هستند.

حال، یک حلقه[1] را به صورت مجموعه‌ای از اعداد تعریف می‌کنیم که وقتی شامل α و β است، $\alpha + \beta$، $\alpha - \beta$ و $\alpha\beta$ را نیز شامل شود. در این صورت، خواهیم داشت:

نتیجهٔ ۳.۶. *کلیهٔ اعداد صحیح جبری تشکیل یک حلقه را می‌دهند. همچنین، کلیهٔ اعداد صحیح جبری واقع در هر هیأت اعداد جبری نیز تشکیل یک حلقه را می‌دهند.*

قضیهٔ ۴.۶. *اگر α در معادلهٔ*

$$f(x) = x^n + \gamma_{n-1} x^{n-1} + \gamma_{n-2} x^{n-2} + \ldots + \gamma_0 = 0$$

صدق کند (که در آن γ_iها اعداد صحیح جبری هستند)، آنگاه α یک عدد صحیح جبری است.

فرض می‌کنیم اعداد به شکل $\gamma_j^{(i)}$ مزدوج‌های γ_j روی R هستند. حاصل‌ضرب

$$h(x) = \Pi\,(x^n + \gamma_{n-1}{}^{(i1)} x^{n-1} + \gamma_{n-2}{}^{(i2)} x^{n-2} + \ldots + \gamma_0{}^{(in)}),$$

را روی تمام این مزدوج‌ها تشکیل می‌دهیم. حال، با توجه به بحث آشنای توابع متقارن، ضرایب $h(x)$ در R قرار دارند. امّا آنها اعداد صحیح جبری نیز هستند؛ زیرا شامل مجموعه‌هایی از حاصل‌ضربهای $\gamma_j^{(i)}$ها هستند. طبق خاصیت ۲، آنها اعداد صحیح گویا هستند. چون $f(x) \mid h(x)$، $h(\alpha) = 0$. سرانجام اینکه $h(x)$ تکین است؛ پس برای تکمیل اثبات می‌توان لم ۱.۶ را به کار برد.

این بخش را با ذکر یک خاصیت ساده ولی خیلی مفید اعداد صحیح به

---

1) *ring*

پایان می‌رسانیم.

قضیهٔ ۵.۶. *اگر θ یک عدد جبری است، عدد صحیح گویای r چنان وجود دارد که $r\theta$ یک عدد صحیح جبری باشد.*

θ در یک معادلهٔ

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0 ,$$

صدق می‌کند، که در آن a_i ها اعداد صحیح گویا هستند. از این موضوع نتیجه می‌گیریم که $a_n \theta$ در معادلهٔ

$$x^n + a_{n-1} x^{n-1} + a_n a_{n-2} x^{n-2} + a_n^2 a_{n-3} x^{n-3} + \ldots + a_n^{n-1} a_0 = 0$$

صدق می‌کند؛ پس $a_n \theta$ یک عدد صحیح جبری است.

یک تعبیر زیبا از خواص ابتدایی اعداد صحیح جبری بدون استفاده از توابع متقارن را می‌توان در دو کتاب از لانداو که در فهرست منابع ذکر شده‌اند، پیدا کرد.

۲. اعداد صحیح در یک هیأت درجهٔ دوم. یک هیأت درجهٔ دوم[2] هیأتی از مرتبهٔ ۲ روی اعداد گویاست. چنین هیأتی الزاماً به شکل $R(\theta)$ است ــ که θ ریشه‌ای از یک چندجمله‌ای درجهٔ دوم تحویل‌ناپذیر روی اعداد گویاست. طبق قضیهٔ ۵.۶، می‌توان فرض کرد که θ یک عدد صحیح جبری است. فرض می‌کنیم که θ در معادلهٔ $x^2 + 2ax + b = 0$ صدق کند که در آن a و b اعداد گویا هستند. در این صورت، $\theta = -a \pm \sqrt{a^2 - b}$. از $a^2 - b$ همهٔ عوامل مجذور آن را بیرون می‌کشیم، بنابراین $a^2 - b = S^2 D$، که در آن D هیچ عامل با توان بیش از یک ندارد. واضح است که

2) *quadratic*

$R(\theta) = R(\sqrt{D})$. به طور خلاصه، هر هیأت درجهٔ دوم به شکل $R(\sqrt{D})$ است که D یک عدد صحیح گویای خالی از مربع است.

طبق قضیهٔ ۶.۴، اعداد ۱ و $\sqrt{D}$ تشکیل یک پایه برای هیأت $R(\sqrt{D})$ را می‌دهند. بنابراین، هر عضو آن را می‌توان به شکل $\frac{l + m\sqrt{D}}{n}$ نوشت، که l و m و n اعداد صحیح گویا هستند. در صورت لزوم، با ساده کردن می‌توان فرض کرد که l و m و n نسبت به هم اولند و n مثبت است. ما این فرض را خواهیم ساخت.

چطور اعداد جبری در میان اعضای $R(\sqrt{D})$ شناخته می‌شوند؟ جواب به ماهیت عدد صحیح D بستگی دارد. $\frac{l + m\sqrt{D}}{n}$ یک عدد صحیح است، تنها اگر در یک معادلهٔ درجهٔ دوم $x^2 + bx + c = 0$ صدق کند، که b و c اعداد صحیح گویا هستند. در نتیجه، می‌توان نوشت

$$(l + m\sqrt{D})^2 + bn\,(l + m\sqrt{D}) + cn^2 = 0 \qquad (۶.۱)$$

پس

$$l^2 + m^2 D + bnl + cn^2 = 0 \qquad (۶.۲)$$

و

$$m\,(2l + bn) = 0$$

اگر $m = 0$، آنگاه $\frac{l + m\sqrt{D}}{n}$ یک عدد صحیح است، اگر و تنها اگر $n \mid l$، بنابراین، فرض می‌کنیم $m \neq 0$. در این حالت $2l = -bn$، پس معادلهٔ (۶.۲) به صورت زیر درمی‌آید:

$$m^2 D - l^2 + cn^2 = 0$$

فرض می‌کنیم $d = (l, n)$. در این صورت، $d^2 \mid m^2 D$. چون D خالی از

مربع است، پس $d|m^2$. امّا l و m و n طبق فرض هیچ عامل مشترکی به جز ۱ ندارند. از این رو $d = 1$ و l و n نسبت به هم اولند. امّا $bn = 2l$، پس $l|b$. در نتیجه، $n = 1$ یا $n = 2$.

اگر $n = 1$، آنگاه $\frac{l + m\sqrt{D}}{n}$ لزوماً یک عدد صحیح است. این موضوع، از معادلهٔ (۶.۱) نتیجه می‌شود. امکان اینکه $n = 2$ باید دقیق‌تر مورد بررسی قرار گیرد. عدد $\frac{l + m\sqrt{D}}{2}$ در معادلهٔ درجهٔ دوم زیر صدق می‌کند:

$$x^2 - lx + \frac{l^2 - m^2 D}{4} = 0$$

در نتیجه، این عدد یک عدد صحیح است، اگر و تنها اگر $\frac{l^2 - m^2 D}{4}$ یک عدد صحیح گویا باشد، یعنی

$$l^2 \equiv m^2 D \ (4)$$

چون $1 = (2 \text{ و } l) = (n \text{ و } l)$، l باید فرد باشد. فرض می‌کنیم $l = 2t + 1$. در این صورت $l^2 = 4t^2 + 4t + 1$، و شرط برقرار می‌شود، اگر

$$1 \equiv m^2 D \ (4) \qquad (۶.۳)$$

حال، چون D خالی از مربع است، D همنهشت ۱، ۲ یا ۳ به سنج ۴ است. هر یک از این سه امکان را جداگانه در نظر می‌گیریم. اگر $D \equiv 1$ (۴)، آنگاه (۶.۳) به صورت رابطهٔ $m^2 \equiv 1$ (۴) درمی‌آید. این رابطه برقرار است، اگر m فرد باشد، و برقرار نیست اگر m زوج باشد. از این رو، اگر $D \equiv 1$ (۴)، همهٔ اعداد به شکل $\frac{l + m\sqrt{D}}{2}$، که در آن l و m هر دو فرد هستند، صحیح هستند. اگر $D \equiv 2$ (۴)، آنگاه D زوج است، پس (۶.۳) برای هیچ انتخابی از m نمی‌تواند برقرار شود. بالاخره، اگر $D \equiv 3$ (۴)، معادلهٔ (۶.۳) به صورت $3m^2 \equiv 1$ (۴) در خواهد آمد.

برقراری این رابطه ، اگر m زوج باشد، غیرممکن است. همچنین، اگر $m = 2s + 1$ فرد باشد، (۶.۳) به تناقض (۴) $3 \equiv 1$ منجر می‌شود. در نتیجه $n = 2$ عدد صحیحی تولید نمی‌کند، مگر اینکه داشته باشیم (۴) $D \equiv 1$. با توجه به آنچه گفته شد، ما قضیهٔ زیر را اثبات کرده‌ایم:

قضیهٔ ۶.۶. *هر هیأت درجهٔ دوم به شکل $R(\sqrt{D})$ وجود دارد، که در آن D یک عدد صحیح گویای خالی از مربع است. اعداد صحیح جبری شامل این کلاس‌ها هستند:*

۱ـ همهٔ اعداد به شکل $l + m\sqrt{D}$، که l و m اعداد صحیح گویا هستند، و

۲ـ اگر (۴) $D \equiv 1$، همهٔ اعداد به شکل $\frac{l + m\sqrt{D}}{2}$، که l و m فرد هستند.

۳. پایه‌های صحیح. فرض می‌کنیم $K = R(\theta)$ یک هیأت اعداد جبری از مرتبهٔ n است. طبق قضیهٔ ۵.۶، می‌توان فرض کرد θ یک عدد صحیح است، و همین کار را خواهیم کرد. طبق قضیهٔ ۶.۴، هر عضو K را می‌توان به طور یگانه‌ای به صورت $\sum_{i=0}^{n-1} a_i \theta^i$ نوشت، که در آن a_i ها در R هستند.

یک مجموعه اعداد صحیح α_1، ...، α_s یک پایهٔ صحیح[3] K نامیده می‌شود، اگر هر عدد صحیح α در K را بتوان به طور یگانه‌ای به صورت

$$\alpha = b_1 \alpha_1 + \ldots + b_s \alpha_s \quad ,$$

نوشت، که در آن b_i ها اعداد صحیح گویا هستند. ما در ادامهٔ مطلب نشان

---

3) *integral basis*

خواهیم داد که یک پایهٔ صحیح، لزوماً یک پایه است.

فرض می‌کنیم β یک عضو K است. طبق قضیهٔ ۵.۶، با انتخاب مناسب عدد صحیح گویای r، $r\beta$ یک عدد صحیح است. در نتیجه، می‌توان نوشت

$$r\beta = b_1\,\alpha_1 + \ldots + b_s\,\alpha_s$$
$$\beta = \frac{b_1}{r}\,\alpha_1 + \ldots + \frac{b_s}{r}\,\alpha_s$$

تنها باید نشان دهیم که α_iها روی R مستقل خطی هستند. فرض می‌کنیم

$$c_1\,\alpha_1 + \ldots + c_s\,\alpha_s = 0 \quad \text{و}$$

که در آن c_iها اعداد گویا هستند. با ضرب کردن معادله در بزرگترین مخرج مشترک رابطهٔ زیر

$$d_1\,\alpha_1 + \ldots + d_s\,\alpha_s = 0 \quad \text{و}$$

به دست می‌آید، که در آن d_iها اعداد صحیح گویا هستند. طبق تعریف یک پایهٔ صحیح، d_iها همگی صفرند. در نتیجه، c_iها نیز همگی صفر بوده و α_iها مستقل خطی هستند.

لم ۷.۶ *یک پایهٔ صحیح، یک پایه است.*

از این معنی، استنباط می‌شود که $S = n$؛ یعنی تعداد اعضای یک پایهٔ صحیح برابر مرتبهٔ هیأت است.

لم ۸.۶. *اگر α_1، ...، α_n هر پایهٔ K شامل فقط اعداد صحیح است. آنگاه، $\Delta[\alpha_1, \ldots, \alpha_n]$ یک عدد صحیح گویاست.*

مزدوج‌های α_i اعداد صحیح جبری هستند. در نتیجه

$$\Delta = \Delta[\alpha_1, \ldots, \alpha_n] = \begin{vmatrix} \alpha_1^{(1)} & \ldots & \alpha_n^{(1)} \\ \ldots\ldots\ldots\ldots\ldots \\ \alpha_1^{(n)} & \ldots & \alpha_n^{(n)} \end{vmatrix}^2$$

یک عدد صحیح جبری است. طبق قضیهٔ ۱۱.۵، با فرض کردن اینکه $F = R$، نتیجه می‌شود که Δ یک عدد گویا نیز هست. بنابراین، Δ یک عدد صحیح گویا است.

قضیهٔ ۹.۶. *هر هیأت اعداد جبری حداقل یک پایهٔ صحیح دارد.*

$K = R(\theta)$ را یک هیأت اعداد جبری در نظر می‌گیریم که در آن θ صحیح فرض شده است. همهٔ پایه‌های K که اعضای آن اعداد صحیح جبری هستند را در نظر می‌گیریم؛ به عنوان مثال ۱، θ، ...، θ^{n-1}[۴]. چون طبق لم ۸.۶ مبین چنین پایه‌ای یک عدد صحیح گویاست، پایه‌ای مثل ω_1، ...، ω_n موجود است که برای آن $|\Delta(\omega_1, \ldots, \omega_n)|$ یک مقدار مینیمم d دارد. طبق قضیهٔ ۱۱.۵، d غیر صفر است.

ثابت خواهیم کرد که ω_1، ...، ω_n یک پایهٔ صحیح است. فرض می‌کنیم چنین نیست. چون پایهٔ مورد بحث به هر حال یک پایه است، بنابراین استنباط می‌شود که یک عدد صحیح ω وجود دارد، به طوری که

$$\omega = a_1\omega_1 + \ldots + a_n\omega_n \quad \text{و}$$

که در آن a_iها اعداد گویا هستند، ولی لزوماً همه صحیح نیستند. می‌توان فرض کرد که a_1 غیر صحیح است. آن را به صورت $a_1 = a + r$ می‌نویسیم که a یک عدد صحیح گویاست و $0 < r < 1$. تعریف می‌کنیم

---

۴) ما ثابت نمی‌کنیم که ۱، θ، ...، θ^{n-1} یک پایهٔ صحیح است. بعداً« در این فصل خواهیم

$$\omega_1^* = \omega - a\omega_1 = (a_1 - a)\,\omega_1 + a_2\,\omega_2 + \ldots + a_n\,\omega_n \quad \text{و}$$

$$i = 2, \ldots, n \qquad \omega_i^* = \omega_i \quad \text{و}$$

دترمینان

$$\begin{vmatrix} a_1 - a & a_2 & a_3 & \ldots \\ 0 & 1 & 0 & \ldots \\ 0 & 0 & 1 & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & 1 \end{vmatrix} = a_1 - a = r$$

غیرصفر است. طبق قضیهٔ ۴.۵، ω_1^*، ...، ω_n^* یک پایه بوده و علاوه بر آن کلاً شامل اعداد صحیح است. همچنین

$$\Delta[\omega_1^*, \ldots, \omega_n^*] = r^2\,\Delta[\omega_1, \ldots, \omega_n] \quad \text{و}$$

$$|\Delta[\omega_1^*, \ldots, \omega_n^*]| < |\Delta[\omega_1, \ldots, \omega_n]|$$

که با انتخاب $|\Delta[\omega_1, \ldots, \omega_n]|$ به عنوان مینیمم در تضاد است. با توجه به نتیجه‌ای که هم اکنون گرفتیم، یک پایهٔ صحیح را یک پایهٔ مینیمال[5] نیز می‌نامند.

قضیهٔ ۱۰.۶. *همهٔ پایه‌های صحیح یک هیأت $K = R(\theta)$ مبین یکسانی دارند.*

فرض می‌کنیم α_1، ...، α_n و β_1، ...، β_n دو پایهٔ صحیح هستند. در این صورت

5) *minimal basis*

$$\alpha_j = \sum_{i=1}^{n} c_{ij}\,\beta_i \quad \text{و} \quad j = 1, \ldots, n \text{ و}$$

که در آن c_{ij} ها اعداد صحیح گویا هستند. امّا

$$\Delta[\alpha_1, \ldots, \alpha_n] = |c_{ij}|^2\,\Delta[\beta_1, \ldots, \beta_n] \quad \text{و} \quad (۶.۴)$$

و $|c_{ij}|^2$ یک عدد صحیح گویای غیر صفر است. بنابراین

$$\Delta[\beta_1, \ldots, \beta_n] \mid \Delta[\alpha_1, \ldots, \alpha_n]$$

با تعویض نقش α_j و β_i می‌بینیم که

$$\Delta[\alpha_1, \ldots, \alpha_n] \mid \Delta[\beta_1, \ldots, \beta_n]$$

امّا مبین‌ها اعداد صحیح گویا هستند. بنابراین، $\Delta[\beta_1, \ldots, \beta_n] = \pm\,\Delta[\alpha_1, \ldots, \alpha_n]$. طبق رابطهٔ (۶.۴)، علامت مثبت درست است و بدین ترتیب اثبات کامل است.

مبین d مشترک بین همهٔ پایه‌های صحیح، مبین هیأت K نامیده می‌شود. واضح است که $d \neq 0$. چون d یک عدد صحیح گویاست، $|d| \geq 1$. بعداً نشان خواهیم داد که اگر $K \neq R$، آنگاه $|d| > 1$.

۴. مثالهایی برای پایه‌های صحیح. در این بخش با یافتن پایه‌های صحیح برای هیأت‌های درجهٔ دوم $R(\sqrt{D})$ مذکور در بخش ۲ این فصل، شروع می‌کنیم.

نخستین چیزی که در نظر می‌گیریم، این است که اگر $D \not\equiv 1 \pmod 4$، آنگاه هر عدد صحیح به شکل $l + m\sqrt{D}$ است (قضیهٔ ۶.۶). در نتیجه، یک پایهٔ صحیح عبارت است از 1 و $\sqrt{D}$. قابل توجه است که در این حالت، مبین هیأت مقدار زیر است:

$$d = \begin{vmatrix} ۱ & \sqrt{D} \\ ۱ & -\sqrt{D} \end{vmatrix}^{۲} = ۴D$$

در مرحلهٔ بعد، فرض می‌کنیم $D \equiv ۱ \ (۴)$. در این صورت، هر عدد صحیح به شکل $\frac{l + m\sqrt{D}}{۲}$ است، که l و m هر دو زوج یا هر دو فرد هستند. در حالت خاص، $\frac{۱ + \sqrt{D}}{۲}$ یک عدد صحیح است؛ که در نتیجه در چنین حالتی هر عدد صحیح را می‌توان به صورت زیر نوشت:

$$a + b\,\frac{۱ + \sqrt{D}}{۲} \quad \text{و}$$

که در آن a و b اعداد صحیح گویا هستند. بنابراین، یک پایهٔ صحیح، ۱ و $\frac{۱ + \sqrt{D}}{۲}$ است. بعلاوه

$$d = \begin{vmatrix} ۱ & \frac{۱ + \sqrt{D}}{۲} \\ ۱ & \frac{۱ - \sqrt{D}}{۲} \end{vmatrix}^{۲} = D$$

قضیهٔ ۱۱.۶. *یک پایهٔ صحیح برای $R(\sqrt{D})$، ۱ و $\sqrt{D}$ است، اگر $D \equiv ۱ \ (۴)$، و ۱، $\frac{۱ + \sqrt{D}}{۲}$ است، اگر $D \equiv ۱ \ (۴)$. در حالت اول $d = ۴D$، و در حالت دوم $d = D$.*

یک مسئلهٔ پیچیده‌تر، مشتق‌گیری از یک پایهٔ صحیح برای هیأت تقسیم دایره $R(\xi)$ است، که ξ یک pامین ریشهٔ ابتدایی واحد است. در بخش ۴ از فصل ۵ نشان داده شد که مجموعهٔ ۱، ξ، ...، $\xi^{p-۲}$ یک پایه برای $R(\xi)$ است. حال نشان خواهیم داد که این پایه در حقیقت یک پایهٔ صحیح است.

لم ۱۲.۶. *اگر $\xi - ۱ = \lambda$، آنگاه ۱، λ، ...، $\lambda^{p-۲}$ یک پایهٔ صحیح برای $R(\xi)$ است.*

فرض می‌کنیم ω_1 ، ... ، ω_{p-1} پایهٔ صحیحی برای $R(\zeta)$ است. در این صورت

$$\lambda^j = \sum_{i=1}^{p-1} c_{ij}\,\omega_i \quad \text{و} \quad j = 0 ، \ldots ، p-2 \text{ و} \qquad (۶.۵)$$

که هر c_{ij} یک عدد صحیح گویاست. طبق رابطهٔ (۵.۱)

$$\Delta\,[1, \lambda, \ldots, \lambda^{p-2}] = |c_{ij}|^2\,\Delta\,[\omega_1, \ldots, \omega_{p-1}] \qquad (۶.۶)$$

حال داریم

$$\begin{aligned} \lambda &= 1 - \zeta \\ \lambda^2 &= 1 - 2\zeta + \zeta^2 \\ \lambda^3 &= 1 - 3\zeta + 3\zeta^2 - \zeta^3 \\ &\ldots \end{aligned} \qquad (۶.۷)$$

و همچنین

$$\begin{aligned} \zeta &= 1 - \lambda \\ \zeta^2 &= 1 - 2\lambda + \lambda^2 \\ \zeta^3 &= 1 - 3\lambda + 3\lambda^2 - \lambda^3 \\ &\text{و } \ldots \end{aligned}$$

به طوری که

$$\Delta\,[1, \lambda, \ldots, \lambda^{p-2}] = |a_{ij}|^2\,\Delta\,[1, \zeta, \ldots, \zeta^{p-2}]$$

و

$$\Delta\,[1, \zeta, \ldots, \zeta^{p-2}] = |a_{ij}|^2\,\Delta\,[1, \lambda, \ldots, \lambda^{p-2}] \quad \text{و}$$

که در آن a_{ij}ها ضرایب دوجمله‌ای هستند که در رابطهٔ (۶.۷) ظاهر شدند. از این رو $|a_{ij}|^{۲} = ۱$، و بنابراین طبق رابطهٔ (۶.۶)

$$\Delta [۱, \xi, \ldots, \xi^{p-۲}] = |c_{ij}|^{۲} \Delta [\omega_۱, \ldots, \omega_{p-۱}]$$

چون $|c_{ij}|^{۲}$ و $\Delta [\omega_۱, \ldots, \omega_{p-۱}]$ اعداد صحیح گویا هستند، از قضیهٔ ۱۲.۵ نتیجه می‌شود که به ازای برخی اعداد صحیح $j \geq ۰$، $|c_{ij}| = \pm p^{j}$.

اگر دستگاه (۶.۵) را برای ω_i حل کنیم، ثابت می‌شود که می‌توان آنها را به صورت

$$\frac{a_۰ + a_۱ \lambda + \ldots + a_{p-۲} \lambda^{p-۲}}{p^{j}}$$ و

بیان کرد، که در آن a_iها اعداد صحیح گویا هستند. چون $\omega_۱$، ...، $\omega_{p-۱}$ یک پایهٔ صحیح است، در نتیجه هر عدد صحیح در $R(\xi)$را می‌توان به این شکل بیان کرد.

اگر ۱، λ، ...، $\lambda^{p-۲}$ یک پایهٔ صحیح نیستند، باید بتوانیم یک عدد صحیح در $R(\xi)$به شکل

$$\frac{a_۰ + a_۱ \lambda + \ldots + a_{p-۲} \lambda^{p-۲}}{p}$$ و

پیدا کنیم که در آن p مقدار $a_۰ + a_۱ \lambda + \ldots + a_{p-۲} \lambda^{p-۲}$ را عاد نکند. فرض می‌کنیم a_m یکی از a_iها با کوچکترین اندیس است، به طوری که $p \nmid a_m$. در این صورت

$$\frac{a_m \lambda^{m} + \ldots + a_{p-۲} \lambda^{p-۲}}{p}$$

یک عدد صحیح جبری است، که $m \leq p - ۲$.

همان طور که در بخش ۴ از فصل ۵ نشان دادیم

$$p = (۱ - \xi)(۱ - \xi^{۲}) \ldots (۱ - \xi^{p-۱})$$

$$= (۱ - \xi)\ (۱ - \xi)\ \dots\ (۱ - \xi)\ K$$
$$= \lambda^{p-۱} K = \lambda^{m+۱} K' \quad \text{و}$$

که در آن K و K' اعداد صحیح جبری هستند. از این رو

$$\frac{a_m \lambda^m + \dots + a_{p-۲} \lambda^{p-۲}}{\lambda^{m+۱}}$$

یک عدد صحیح جبری است. $\lambda^{m+۱}$ از همهٔ جملات به جز جملهٔ اول حذف می‌شود، و بنابراین می‌توان با حذف آن نتیجه گرفت که $\frac{a_m}{\lambda}$ یک عدد صحیح جبری است، برای سهولت کار، می‌نویسیم $a_m = a$.

ثابت خواهیم کرد که a/λ نمی‌تواند یک عدد صحیح جبری باشد، و بدین ترتیب به یک تناقض می‌رسیم. از این موضوع، نتیجه خواهد شد که $x = \frac{a}{\lambda} = \frac{a}{۱ - \xi}$. در $۱, \lambda, \dots, \lambda^{p-۲}$ یک پایهٔ صحیح است. فرض می‌کنیم این صورت $\frac{a}{x} = ۱ - \xi$، و بنابراین $(۱ - \frac{a}{x})^p = ۱$ و از $x^p = (x - a)^p$ این رو، $\frac{a}{\lambda}$ در یک معادلهٔ

$$g(x) = p\, x^{p-۱} + p(\dots) + a^{p-۱} = ۰ \quad \text{و}$$

صدق می‌کند که در آن a p. چون $p \nmid a$، چندجمله‌ای $p + p(\dots) + a^{p-۱} x^{p-۱} g(\frac{۱}{x}) = x^{p-۱}$ طبق محک آیزنشتاین تحویل‌ناپذیر است. بنابراین $g(x)$ روی R تحویل‌ناپذیر است. چون $g(x)$ ابتدایی بوده و ضریب پیشرو آن ۱ نیست، ریشهٔ آن a/λ یک عدد صحیح جبری نیست. این معنی، اثبات لم را کامل می‌کند.

چون $۱, \lambda, \dots, \lambda^{p-۲}$ یک پایهٔ صحیح است، بنابراین $۱, \xi, \dots, \xi^{p-۲}$ نظر به رابطهٔ (۶.۷)، یک پایه صحیح است. با ترکیب این حقیقت با قضیهٔ ۱۲.۵، به قضیهٔ زیر می‌رسیم:

قضیهٔ ۱۳.۶. مجموعهٔ $1, \zeta, \ldots, \zeta^{p-2}$ یک پایهٔ صحیح برای $R(\zeta)$ است. این هیأت، دارای مبین $p^{p-2}(-1)^{(p-1)/2}$ است.

فصل ۷

محاسبه در هیأت‌های اعداد جبری

۱. یکه‌هاو اعداد اول. حلقهٔ همهٔ اعداد صحیح جبری را در نظر گرفته و قصد داریم پس از الگوی فصل ۱، یک نظریهٔ تجزیه در این حلقه را مدل‌سازی کنیم. می‌گوییم α، βرا *عاد* می‌کند. و می‌نویسیم $\alpha|\beta$، اگر β/α یک عدد صحیح جبری است. ε یک یکه است، اگر عدد ۱ را عاد کند. α یک عدد *اول* است، اگر یکه و صفر نیست و اگر در هر تجزیهٔ آن به اعداد صحیح به صورت $\alpha = \beta\gamma$، نتیجه بگیریم که βیا γ یکه است.

متأسفانه این تلاش، همانند کار قبلی ما، محکوم به شکست است؛ چرا که هیچ عدد اولی در حلقهٔ همهٔ اعداد صحیح جبری وجود ندارد! زیرا فرض می‌کنیم α یک عدد صحیح غیر صفر و غیر یکه است. در این صورت، همیشه می‌توان نوشت $\alpha = \sqrt{\alpha}\,\sqrt{\alpha}$. اگر α در $p(x) = 0$ صدق کند، آنگاه $\sqrt{\alpha}$در $p(x^2) = 0$صدق نموده و بنابراین یک عدد صحیح است. این حقیقت، ما را وادار می‌سازد که از تعاریفی که ارائه کرده‌ایم صرف‌نظر کنیم.

در عوض، بهتر است توجه خود را به حلقهٔ همهٔ اعداد صحیح در یک هیأت اعداد جبری ثابت $K = R(\theta)$ معطوف کنیم. در حقیقت، این همان کاری است که در فصل ۱ انجام دادیم. تعریفی که در بالا ارائه شد، اکنون باید تغییر کند. α، β را عاد می‌کند، $\alpha | \beta$، اگر β/α یک عدد صحیح در K است. ε یکه است، اگر $1 | \varepsilon$. α یک عدد *اول* است، اگر صفر و یکه نیست و در هر تجزیهٔ $\alpha = \beta\gamma$ به اعداد صحیح در K نتیجه شود که β یا δ یکه است.

با چنین تعاریفی، تجزیهٔ اعداد صحیح در K به حاصل‌ضرب اعداد اول همواره ممکن است. این مطلب بتدریج ثابت خواهد شد. از طرف دیگر، چنانکه در فصل ۱ دیدیم، حلقهٔ H از همهٔ اعداد صحیح[1] در $R(\sqrt{-5})$ خاصیت یگانگی تجزیه را ندارد. قبل از تحقیق علت این پدیده و روش اصلاح آن، ثابت خواهیم کرد تجزیه به اعداد اول خواه یگانه باشد یا نباشد، در K امکانپذیر است.

اگر α یک عدد صحیح در K و K روی R از مرتبهٔ n است، آنگاه α، n مزدوج α_1، ...، α_n در K دارد. با توجه به آنچه گفته شد، نورم α، که به صورت $N(\alpha)$ یا $N\alpha$ نوشته می‌شود، را چنین تعریف می‌کنیم:

$$N\alpha = \alpha_1 \dots \alpha_n .$$

لم ۱.۷. $N\alpha$ *یک عدد صحیح گویاست.*

فرض می‌کنیم $f(x)$ (چنانکه در اثبات قضیهٔ ۱۰.۵ تعریف شد) چندجمله‌ای هیأت α است. چون $f(x)$ توانی از چندجمله‌ای مینیمال

---

۱) که در واقع طبق قضیهٔ ۶.۶، H تشکیل حلقهٔ همهٔ اعداد صحیح در $R(\sqrt{-5})$ را می‌دهد؛ چون $1(4) \equiv 5 \equiv -5$.

است، ضرایب صحیح دارد. از این رو

$$f(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_0 = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)$$ و

که در آن a_0 یک عدد صحیح گویاست. در این صورت

$$N\alpha = \alpha_1 \ldots \alpha_n = (-1)^n a_0$$

لم ۲.۷. $N(\alpha\beta) = N\alpha \cdot N\beta$.

اگر α_1 و α_2، ...، α_n و β_1، β_2، ...، β_n به ترتیب مزدوج‌های α و β در K هستند، آنگاه $\alpha_1\beta_1$ و $\alpha_2\beta_2$، ...، $\alpha_n\beta_n$ مزدوج‌های $\alpha\beta$ در K هستند. این موضوع، لم را ثابت می‌کند.

لم ۳.۷. *α یک یکه در K است، اگر و تنها اگر $N\alpha = \pm 1$.*

زیرا α یک یکه است، اگر و تنها اگر $\alpha \mid 1$. اگر $\alpha \mid 1$ آنگاه، $N\alpha \mid 1$ و $N\alpha = \pm 1$. اگر $N\alpha = \pm 1$، آنگاه $\alpha_1, \ldots, \alpha_n$، و بنابراین $\alpha \mid 1$.

قضیهٔ ۴.۷. *اگر $N\alpha$ یک عدد اول گویا است، α در K اول است.*

زیرا اگر $\alpha = \beta\gamma$، $N\alpha = N\beta N\gamma$. چون $N\alpha$ اول است، یکی از دو عدد $N\beta$ یا $N\gamma$ برابر با ± 1 است. از این رو با توجه به لم قبل، یکی از دو عدد β یا γ یکه است.

قضیهٔ ۵.۷. *هر عدد صحیح غیرصفر و غیریکه در K، قابل تجزیه به حاصل‌ضرب اعداد اول است.*

اگر α اول است، می‌نویسیم $\alpha = \beta\gamma$، که β و γ هیچ کدام یکه نیستند. این روش را برای β و γ تکرار کرده و ادامه می‌دهیم. این عمل باید متوقف شود، زیرا در غیر این صورت $\alpha = \gamma_1 \ldots \gamma_n$، که در آن n به دلخواه بزرگ

است و در نتیجه $|N\gamma_1| \dots |N\gamma_n| = |N\alpha|$ را می‌توان به اندازهٔ دلخواه بزرگ کرد، چون هر عامل $|N\gamma_i|$ از یک بیشتر است.

نتیجهٔ ۶.۷. تعداد اعداد اول در یک هیأت جبری نامتناهی است.

بحثی مشابه آنچه در بخش ۱ از فصل ۲ انجام شد، نشان می‌دهد که اگر حداقل یک عدد اول در K وجود داشته باشد، تعدادی نامتناهی از اعداد اول در K موجود است. این در حالی است که ما حداقل در مورد وجود یکی از این اعداد مطمئنیم؛ زیرا عدد ۲ یقیناً در K است و بنابر قضیهٔ ۵.۷ یک عامل اول دارد.

ما سؤال یگانگی تجزیه را دوباره در بخش ۳ مطرح خواهیم کرد.

۲. یکه‌ها در هیأت درجهٔ دوم. برای روشن شدن برخی از مطالب بخش قبل، می‌خواهیم مسئلهٔ تعیین یکه‌ها در یک هیأت درجهٔ دوم $R(\sqrt{D})$ را بررسی کنیم. اگر عدد $\alpha = a + b\sqrt{D}$ که α یک عدد صحیح در $R(\sqrt{D})$ است، آنگاه

$$N\alpha = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$$

این موضوع، مسئلهٔ تعیین یکه‌ها را به حل معادلهٔ $a^2 - Db^2 = \pm 1$ خلاصه می‌کند.

اگر $D \not\equiv 1 \pmod 4$، اعداد صحیح همگی اعدادی به شکل $l + m\sqrt{D}$ خواهند بود، که در آن l و m اعداد صحیح گویا هستند. پس برای تعیین یکه‌ها باید معادلهٔ

$$l^2 - Dm^2 = \pm 1 \qquad (۷.۱)$$

را برای اعداد صحیح و گویای l و m حل کنیم.

به علاوه، اگر $D \equiv ۱ \pmod{۴}$، اعداد صحیح $\frac{l + m\sqrt{D}}{۲}$ نیز موجودند که در آن l و m هر دو فرد هستند. پس همهٔ یکه‌های دیگر از حل معادلهٔ

$$l^۲ - Dm^۲ = \pm ۴ \qquad (۷.۲)$$

به دست می‌آیند، که در آن l و m اعداد صحیح فرد هستند.

ابتدا فرض می‌کنیم $D > ۰$. در این حالت، هیأت $R(\sqrt{D})$ موهومی نامیده می‌شود. باید توجه داشت که اعضای سمت چپ روابط ۷.۱ و ۷.۲ هر دو مثبت هستند؛ بنابراین علامتهای منفی اعضای سمت راست باید حذف شوند. در نتیجه، یکه‌ها از معادلهٔ $l^۲ - Dm^۲ = ۱$ به دست می‌آیند، و اگر $D \equiv ۱ \pmod{۴}$، از معادلهٔ $l^۲ - Dm^۲ = ۴$ نیز حاصل می‌شوند. چون $D > ۰$، هر یک از این معادلات حداکثر تعداد متناهی جواب را می‌توانند داشته باشند که می‌خواهیم آنها را صریحاً تعیین کنیم. ابتدا به خواننده یادآور می‌شویم که D خالی از مربع است.

اگر $D < -۱$، آنگاه $l^۲ - Dm^۲ = ۱$ تنها جوابهای $l = \pm ۱$ و $m = ۰$ را دارد، اگر $D < -۴$، $l^۲ - Dm^۲ = ۴$ نیز تنها همین جوابها را دارد. از این رو، اگر $D < -۴$، تنها یکه‌ها، ± ۱ هستند. بررسی حالات $D = -۳$ و -۲ و -۱ باقی می‌ماند. اولین حالت این اعداد، متناظر با هیأت $R(i)$ است و قبلاً در فصل ۱ ثابت کردیم که یکه‌ها در این هیأت ± ۱ و $\pm i$ هستند. در مرحلهٔ دوم، چون $D = -۲ \not\equiv ۱ \pmod{۴}$، با توجه به مطلب مذکور در ابتدای این پاراگراف تنها یکه‌های $R(\sqrt{-۲})$، ± ۱ هستند.

حال توجه خود را به $R(\sqrt{-۳})$ معطوف می‌داریم. چون $-۳ \equiv ۱ \pmod{۴}$، علاوه بر ± ۱ می‌توان انتظار به دست آمدن یکه‌های دیگری را نیز از

جواب معادلهٔ $l^2 + 3m^2 = 4$ داشت. جوابهای این معادله، جوابهای (۱ و ۱)، (۱ ـ و ۱)، (۱ و ۱ ـ) و (۱ ـ و ۱ ـ) هستند. بنابراین، یکه‌های $R(\sqrt{-3})$ عبارتند از ± 1، $\frac{1 \pm \sqrt{-3}}{2}$ و $\frac{-1 \pm \sqrt{-3}}{2}$. باید توجه داشت که اینها ریشه‌های $x^2 \pm x + 1$ و $x \pm 1$ هستند.

قضیهٔ ۷.۷. *هیأت درجهٔ دوم $R(\sqrt{D})$ که در آن D منفی و خالی از مربع است، تنها یکه‌های ± 1 دارد؛ مگر اینکه داشته باشیم $D = -1$، که در این حالت $\pm i$ نیز یکه هستند، یا اینکه داشته باشیم $D = -3$، که در این حالت،*

$$\frac{-1 \pm \sqrt{-3}}{2} \quad \text{و} \quad \frac{1 \pm \sqrt{-3}}{2}$$

نیز یکه هستند.

امّا اگر $D < 0$، آیا هیأت حقیقی است؟ این حالت از حالت موهومی پیچیده‌تر است و ما فعلاً به یک جواب برای حالت $D = 2$ اکتفا می‌کنیم. چون $1 \neq \pm 2$ (۴)، تنها جوابهای معادلهٔ $l^2 - 2m^2 = \pm 1$، رابطهٔ ۷.۱، مورد نظر هستند.

لم ۸.۷. *$R(\sqrt{2})$، یکه‌ای بین ۱ و $1 + \sqrt{2}$ ندارد.*

فرض می‌کنیم داشته باشیم $\varepsilon = x + y\sqrt{2}$، در حالی که $x^2 - 2y^2 = \pm 1$ بوده و ε بین ۱ و $1 + \sqrt{2}$ قرار دارد در نتیجه $1 < \varepsilon < 1 + \sqrt{2}$ و چون $\pm \frac{1}{x + y\sqrt{2}} = x - y\sqrt{2}$، پس $-1 < x - y\sqrt{2} < 1$. با جمع کردن این نامساوی‌ها با هم، داریم $0 < 2x < 2 + \sqrt{2}$ و $0 < x < 1/8$.

چون x یک عدد صحیح است، پس برابر با ۱ است. امّا برقراری رابطه $1 < 1 + y\sqrt{2} < \sqrt{2}$، برای هیچ عدد صحیح y، ممکن نیست.

مشاهده می‌شود که یک جواب $l^2 - 2m^2 = \pm 1$، (۱ و ۱) است؛

بنابراین $\lambda = ۱ + \sqrt{۲}$ یک یکه است.

قضیهٔ ۹.۷. *$R(\sqrt{۲})$ تعدادی نامتناهی یکه به صورت $\pm\lambda^n$ دارد* $(n = ۰, \pm۱, \pm۲, \ldots)$.

برای اثبات، ابتدا توجه می‌کنیم که همهٔ اعضای $R(\sqrt{۲})$ حقیقی هستند. از این رو، اگر ε یک یکه در $R(\sqrt{۲})$ است، یا مثبت است و یا منفی.

فرض می‌کنیم $\varepsilon > ۰$. چون $\lambda = ۱ + \sqrt{۲}$ بیشتر از ۱ است، می‌توان عدد صحیح n را چنان یافت که $\lambda^n \le \varepsilon < \lambda^{n+۱}$. اگر $\lambda^n < \varepsilon < \lambda^{n+۱}$، آنگاه $۱ < \varepsilon\lambda^{-n} < ۱ + \sqrt{۲}$. امّا $N(\varepsilon\lambda^{-n}) = N(\varepsilon) / N(\lambda)^n = ۱$، چون ε و λ یکه هستند. در نتیجه $\varepsilon\lambda^{-n}$ یکه‌ای بین ۱ و $۱ + \sqrt{۲}$ است، که این موضوع با لم ۸.۷ در تناقض است. تنها حالت باقیمانده، حالت $\varepsilon = \lambda^n$ است. چون $۱/\varepsilon$ و ε ـ هم یکه هستند، اثبات کامل می‌شود.

در یکی از فصلهای بعدی در خصوص یکه‌ها نشان خواهیم داد که هر هیأت اعداد جبری به جز R و هیأت‌های قضیهٔ ۷.۷ تعدادی نامتناهی یکه دارند، بنابراین، $R(\sqrt{۲})$ نمونه‌ای از حالت عمومی‌تر هیأت‌های درجهٔ دوم موهومی است. چون اثبات در این مرحله مشکل است، باید آن را به تعویق انداخت.

۳. یگانگی تجزیه[۲]. قبلاً مشاهده کردیم که قضیهٔ ۵.۷ دربارهٔ یگانگی تجزیه به اعداد اول (بدون در نظر گرفتن ترتیب و یکه‌ها) هیچ چیز نمی‌گوید. برای آنکه بفهمیم عدم یگانگی چگونه پدید می‌آید، بهتر است

---

۲) موضوع این بخش از فصل ۵ کتاب هکه (Hecke) که در فهرست منابع آمده اقتباس شده است.

بدقت اعداد صحیح $R(\sqrt{-5})$ را بررسی کنیم. چنانکه در فصل ۱ دیدیم

$$۲۱ = ۳ \times ۷ = (۱ + ۲\sqrt{-5})(۱ - ۲\sqrt{-5})$$ و

که در آن همهٔ عوامل ظاهرشده اول هستند. در این حالت، وضعیتی که به وجود می‌آید این است که عدد ۳، یک عدد اول است، $(۲\sqrt{-5} - ۱)$ $(۲\sqrt{-5} + ۱)$ را عاد می‌کند، امّا از عادکردن هر عاملی در $R(\sqrt{-5})$ ناتوان است. این وضعیت، چنانکه قبلاً در فصل ۱ ثابت شد، ممکن نیست در مورد R یا $R(i)$ رخ دهد.

برای توضیح این وضعیت، موقتاً به تعریف عادکردن که در شروع بخش ۱ داده شد، ولی بعداً آنرا رها کردیم، برمی‌گردیم. فرض می‌کنیم $\alpha = ۱ + ۲\sqrt{-5}$ و $\lambda = ۲ + \sqrt{-5}$ در این صورت

$$\frac{\alpha^۲}{\lambda} = -۲ + ۳\sqrt{-5} \quad \text{و} \quad \frac{۹}{\lambda} = ۲ - \sqrt{-5}$$

در $R(\sqrt{-5})$ عدد صحیح بوده و در نتیجه ریشه‌های دوم آنها $\frac{۳}{\sqrt{\lambda}}$ و $\frac{\alpha}{\sqrt{\lambda}}$ نیز اعداد صحیح هستند. امّا این اعداد صحیح در $R(\sqrt{-5})$ نیستند (چرا؟). به عبارت دیگر، ۳ و $۲\sqrt{-5} + ۱$ هر دو (طبق تعریف بسط‌یافتهٔ «عادکردن») توسط عدد صحیح $\sqrt{\lambda}$ که در $R(\sqrt{-5})$ نیست قابل شمارش هستند. به علاوه، چون

$$\sqrt{\lambda} = (\frac{-۲\alpha}{\sqrt{\lambda}})\alpha - (\frac{۱۲ - ۳\sqrt{-5}}{\sqrt{\lambda}})۳ \quad \text{و}$$

هر عامل مشترک دیگر ۳ و $۲\sqrt{-5} + ۱ = \alpha$، $\sqrt{\lambda}$ را عاد می‌کند.

به‌طور مشابه، ۷ و $۲\sqrt{-5} - ۱$ نیز «بزرگترین عامل مشترک» $\sqrt{K}$ را دارند، که $K = ۲ + ۳\sqrt{-5}$.

یک محاسبهٔ ساده نشان می‌دهد که

$$۱ + ۲\sqrt{-۵} = \sqrt{\lambda}\sqrt{-K} \qquad ۳ = \sqrt{\lambda}\sqrt{\lambda}$$
$$۱ - ۲\sqrt{-۵} = \sqrt{\lambda}\sqrt{-K}\sqrt{} = \sqrt{K}\sqrt{K}$$

که در آن علامت «ـ» (بار)، علامت مزدوج ـ مختلط است. پس ۲۱ قابل تجزیه است ــ امّا نه در $R(\sqrt{-۵})$ ــ به‌طوری که

$$۲۱ = \sqrt{\lambda}\sqrt{\lambda} \cdot \sqrt{-K}\sqrt{-K}$$

و تجزیه‌های مختلف به دست آمده در $R(\sqrt{-۵})$ از جفت کردن این چهار عامل به روشهای مختلف حاصل می‌شوند.

به‌طور خلاصه :

۱ ـ اعداد اول موجود در $R(\sqrt{-۵})$ که مرتبط نیستند (یعنی نسبت آنها یک عدد یکه نیست) می‌توانند یک عامل مشترک داشته باشند که در $R(\sqrt{-۵})$ نیست.

۲ ـ کلیهٔ اعداد صحیح موجود در $R(\sqrt{-۵})$ که توسط یک عدد اول α در $R(\sqrt{-۵})$ عاد می‌شوند، لازم نیست بر مجموعهٔ اعداد صحیح موجود در $R(\sqrt{-۵})$ که توسط یک عامل α ــ که در $R(\sqrt{-۵})$ نبود و یکه هم نیست ــ عاد می‌شوند، منطبق باشد ($\alpha = ۱ + ۲\sqrt{-۵}$ اول است و $\sqrt{\lambda}$ هم α و هم ۳ را عاد می‌کند، ولی ۳ بر α بخش‌پذیر نیست).

پس به‌نظر می‌رسد که در یک هیأت اعداد جبری K اعداد اول لزوماً عناصری نیستند که همهٔ اعداد صحیح توسط آنها ساخته شده باشند. برای مثال در $R(\sqrt{-۵})$، به‌نظر می‌رسد لازم است حلقهٔ اعداد صحیح را چنان بسط دهیم که شامل اعداد «*ایده‌آل*»[۳] چون $\sqrt{\lambda}$ و $\sqrt{K}$ شود، که در

---

3) *Ideal*

ابتدا در حلقه نبودند. امّا این اعداد را که باید به K افزوده شوند، چطور مشخص خواهیم کرد؟

فرض می‌کنیم یک عدد صحیح ξ، انتخابی برای افزوده شدن به K است، به واسطهٔ اینکه یک عامل مشترک دو عدد صحیحی است که نسبت به هم در K اول هستند. مجموعهٔ A *از همهٔ اعداد صحیح در* K *که توسط* ξ (در حالت توسعه‌یافته) عاد می‌شوند *را در نظر می‌گیریم*. چنین مجموعه‌ای، این خاصیت را دارد که اگر α و β اعداد صحیحی در A هستند، در این صورت همهٔ اعداد صحیح در K به شکل $\lambda\alpha + \mu\beta$ است، که در آن λ و μ نیز اعداد صحیحی در K هستند. هر مجموعه از اعداد صحیح در K با خاصیت اخیر را یک ایده‌آل می‌نامیم.

این مطلب، روش ذکرشونده را برای جواب دادن به سؤال طرح شده در خصوص اعدادی که باید به K افزوده شوند ارائه می‌کند. بدین منظور، ایده‌آلی را در K در نظر گرفته و سعی می‌کنیم ثابت نماییم که ایده‌آل مزبور همان مجموعهٔ اعداد صحیح موجود در K است که توسط بعضی اعداد ثابت صحیح ξ که لزوماً در K نیستند، عاد می‌شوند. اگر بتوانیم این مطلب و همچنین یگانه بودن ξ را در برخی حالات نشان بدهیم، آنگاه اعداد صحیح جامانده را با استفاده از ایده‌آل‌ها مشخص کرده‌ایم، این همان کاری است که ما در فصل بعدی انجام خواهیم داد.

امّا اینجا مسئلهٔ دیگری مطرح است. اگر بخواهیم ایده‌آل‌هایی را برای جانشینی اعداد صحیح بسازیم، آنگاه مسئلهٔ تجزیهٔ اعداد صحیح، به تجزیهٔ ایده‌آل‌ها تبدیل خواهد شد. چنانکه خواهیم دید، برای ایده‌آل‌ها

یک محاسبهٔ کاملاً قانع‌کننده وجود دارد، که سرانجام به وسیلهٔ آن مسئلهٔ یگانگی تجزیه را به انجام خواهیم رساند.

۴. ایده‌آل‌ها در یک هیأت اعداد جبری. فرض می‌کنیم K یک هیأت اعداد جبری است. مجموعهٔ A از اعداد صحیح موجود در K یک *ایده‌آل* است، اگر، همراه با هر جفت از اعداد صحیح α و β در A، این مجموعه به ازای اعداد صحیح λ و μ موجود در K، $\lambda\alpha + \mu\beta$ را نیز شامل شود. یک مجموعه از اعداد صحیح ω_1، ...، ωr در A، یک پایه برای A نامیده می‌شود، اگر هر عضو α در A را بتوان به‌طور یگانه‌ای به صورت

$$\alpha = c_1\,\omega_1 + \ldots + c_r\,\omega_r \qquad (۷.۳)$$

نمایش داد، که در آن c_iها اعداد صحیح گویا هستند.

از این پس ایده‌آلی را که تنها شامل ۰ است را با (۰) نمایش می‌دهیم. نشان خواهیم داد که اگر یک ایده‌آل A که مخالف صفر است در یک هیأت K یک پایهٔ ω_1، ...، ω_r داشته باشد، آنگاه r باید برابر n، مرتبه هیأت باشد. طبق خاصیت یگانگی نمایش (۷.۳)، مجموعهٔ ω_1، ...، ω_r باید روی R مستقل خطی باشد. از این رو، بنابر لم ۵.۱، $r \le n$. برای نشان دادن اینکه $r < n$ غیرممکن است، فرض می‌کنیم β_1، ...، β_n یک پایهٔ صحیح K روی R است. اگر α یک عضو غیرصفر A است، آنگاه $\alpha\beta_1$، ...، $\alpha\beta_n$ مستقل خطی و در A هستند. آنها به علت استقلال خطی تشکیل یک پایه را روی K می‌دهند. به علاوه

$$\alpha\beta_j = \sum_{i=1}^{n} a_{ij}\,\omega_i \qquad j = 1, \ldots, n,$$

که ω_i را برای i که $r < i \leq n$، صفر تعریف می‌کنیم. پس

$$\Delta [\alpha\beta_1 , \dots , \alpha\beta_n] = |a_{ij}|^2 \Delta [\omega_1 , \dots , \omega_n] .$$

امّا $\Delta [\omega_1 , \dots , \omega_n] = \Delta [\omega_1 , \dots , \omega_r , 0 , \dots] = 0$. از این رو $\Delta [\alpha\beta_1 , \dots , \alpha\beta_n] = 0$، که این معنی با این حقیقت که مبین یک پایه هرگز صفر نمی‌شود در تناقض است، در نتیجه $r = n$.

برای اثبات اینکه یک ایده‌آل A که مخالف صفر است لزوماً یک پایه دارد، می‌توان از اثبات قضیهٔ ۹.۶ پیروی کرد. همهٔ مجموعه‌های $\alpha_1 , \dots , \alpha_n$ از اعداد صحیح در A را در نظر می‌گیریم که تشکیل یک پایه روی K را می‌دهند. با اعداد $\alpha\beta_1 , \dots , \alpha\beta_n$ که در بالا به آنها اشاره شد یک مثال را در این خصوص ارائه می‌دهیم. بنابر لم ۸.۶ $\Delta [\alpha_1 , \dots , \alpha_n]$ همیشه یک عدد صحیح گویای غیرصفر است. بنابراین، می‌توان یک چنین مجموعهٔ $\omega_1 , \dots , \omega_n$، را از A انتخاب کرد که برای آن $|\Delta[\omega_1 , \dots , \omega_n]|$ یک مینیمم است. دقیقاً با بحثی مشابه آنچه که در اثبات قضیهٔ ۹.۶ به کار رفت، می‌توان نتیجه گرفت که این یک پایه برای ایده‌آل A است.

برعکس، هر عدد صحیح موجود در K که به شکل (۷.۳) باشد، در A است. این یک نتیجه از تعریف یک ایده‌آل و این حقیقت است که همهٔ اعداد گویا در K صحیح هستند. بدین ترتیب، قضیه زیر اثبات می‌شود :

قضیهٔ ۱۰.۷. *اگر K روی R از مرتبهٔ n و $A \neq (0)$ یک ایده‌آل در K است، آنگاه اعداد صحیح $\omega_1 , \dots , \omega_n$ در A وجود دارند، به‌طوری که A مجموعهٔ اعداد صحیح به شکل $\sum_{i=1}^{n} c_i \omega_i$ است که در آن c_i ها اعداد صحیح گویا هستند.*

یک ایده‌آل A را تولیدشده توسط $\alpha_1 , \dots , \alpha_t$ می‌گوییم و می‌نویسیم

$A = (\alpha_1, \ldots, \alpha_t)$، اگر A شامل همهٔ مجموع‌های به صورت $\sum_{i=1}^{t} \lambda_i \alpha_i$ است، که در آن λ_iها اعداد صحیح و نه لزوماً گویا در K هستند. بدیهی است که اگر $\omega_1, \ldots, \omega_n$ یک پایه برای A است، آنگاه $A = (\omega_1, \ldots, \omega_n)$، امّا اگر داشته باشیم $A = (\alpha_1, \ldots, \alpha_t)$، α_iها لزوماً تشکیل یک پایه را برای A نمی‌دهند. به عنوان مثال، ایده‌آل (۲) را در $R(i)$ در نظر می‌گیریم. این ایده‌آل، شامل همهٔ اعداد صحیح به شکل $2bi + 2a$ است، که در آن a و b اعداد صحیح گویا هستند، و بنابراین ۲ و $2i$ یک پایه برای (۲) است. عدد ۲ به تنهایی یک پایه برای (۲) نیست.

یک ایده‌آل A، *اصلی*[۴] است، اگر به وسیلهٔ یک عدد صحیح منفرد تولید شده باشد ــ یعنی $A = (\alpha)$.

قضیه ۱۱.۷. *هر ایده‌آل در R یا در $R(i)$ اصلی است. در $R(\sqrt{-5})$ یک ایده‌آل وجود دارد که اصلی نیست.*

ابتدا فرض می‌کنیم A یک ایده‌آل در R است. A کلاً شامل اعداد صحیح گویاست. فرض می‌کنیم $A \neq (0)$، در این صورت، A شامل یک عنصر $a \neq 0$ است؛ به علاوه شامل $a - a = 0$ و $-a + a = 0$ نیز هست. بنابراین، α+ و α- هر دو در A هستند، و یکی از آنها باید مثبت باشد. از این رو، A شامل اعداد صحیح مثبت است. m را کوچکترین عدد صحیح مثبت موجود در A درنظر می‌گیریم. اگر n هر عدد دیگری در A است، می‌توان q و r را چنان یافت که

$$n = mq + r \quad \text{و} \quad 0 \leq r < m .$$

---

4) *principal*

امّا هر عدد به شکل $ns + mt$ در A است و بخصوص $r = n - mq$. پس اینکه $0 < r < m$ با انتخاب m به عنوان کوچکترین عدد صحیح مثبت در A غیرممکن است. از این رو $r = 0$ و $n = mq$. به عبارت دیگر، هر عضو a مضربی از m است. به علاوه، هر مضرب m در A است، و بنابراین $A = (m)$. این همان چیزی بود که می‌خواستیم.

بحثی مشابه، برای ایده‌آل‌های A در $R(i)$ نیز به کار می‌رود، با این تفاوت که در آن به جای انتخاب کوچکترین عدد مثبت در A، عضوی با حداقل نورم مثبت را درنظر گرفته و قضیهٔ ۶.۱ را به کار می‌بریم.

از طرف دیگر ایده‌آل B که $B = (3, 1 + 2\sqrt{-5})$ در $R(\sqrt{-5})$ اصلی نیست؛ زیرا اگر $B = (\beta)$ آنگاه $\beta \mid 3$ و $\beta \mid (1 + 2\sqrt{-5})$. چون 3 و $1 + 2\sqrt{-5}$ هر دو در $R(\sqrt{-5})$ اول هستند و از این رو نسبت به هم اولند، β باید یک یکه باشد. تنها یکه‌های موجود در $R(\sqrt{-5})$، ± 1 هستند؛ بنابراین $B = (1)$. با توجه به نتایج بخش قبلی، هر عضو B بر $\sqrt{\lambda}$ (در حالت بسط‌یافتهٔ عاد کردن) بخش‌پذیر است، چون 3 و $1 + 2\sqrt{-5}$ نیز بخش‌پذیر هستند. از این رو $\frac{1}{\sqrt{\lambda}}$ یک عدد صحیح است، و بنابراین

$$\frac{1}{\lambda} = \frac{1}{2 + \sqrt{-5}} = \frac{2 - \sqrt{-5}}{9}$$

یک عدد صحیح است که این با قضیهٔ ۶.۶ در تناقض قرار می‌گیرد. در نتیجه، B در $R(\sqrt{-5})$ نمی‌تواند اصلی باشد.

خواننده شاید از قضیهٔ اخیر نتیجه بگیرد که یگانگی تجزیهٔ اعداد صحیح در یک هیأت اعداد جبری، با اصلی بودن همه ایده‌آل‌ها در آن معادل است. این نتیجه‌گیری، در فصل ۹ تأیید خواهد شد.

فصل ۸

قضیهٔ اساسی نظریهٔ ایده‌آل‌ها

۱. **خواص اساسی ایده‌آل‌ها.** طبق فصل قبل، هر ایده‌آل در هیأت اعداد جبری K را می‌توان به صورت $A = (\alpha_1, \ldots, \alpha_s)$ نوشت. امّا این سؤال مطرح است که تحت چه شرایطی می‌توان گفت که A و $B = (\beta_1, \ldots, \beta_t)$ ایده‌آل‌های یکسانی هستند؟ به این سؤال، جوابی ساده به صورت زیر داده شده است :

قضیهٔ ۸.۱. *ایده‌آل‌های A و B یکسان هستند، اگر و تنها اگر بتوان هر α_i به صورت*

$$\alpha_i = \sum_j \gamma_{i\,j}\, \beta_j$$

و هر β_j را به صورت

$$\beta_j = \sum_i \delta_{j\,i}\, \alpha_i \,,$$

نوشت، که $\gamma_{i\,j}$ و $\delta_{j\,i}$ اعداد صحیحی در K هستند.

لزوم شرط مذکور بدیهی است. برای اثبات کفایت آن، فرض می‌کنیم $\beta = \sum_j \lambda_j \beta_j$ هر عضوی از B است. در این صورت، $\alpha_i = \sum_j (\sum_i \lambda_j \delta_{j\,i})$ $= \sum_j \lambda_j \sum_i \delta_{j\,i}\, \alpha_i$؛ و بنابراین β در A است. به‌طور مشابه، هر عضو A نیز در B است؛ و از این رو $A = B$.

دو عدد صحیح α و β در K مرتبط هستند، اگر $\frac{\alpha}{\beta}$ یک یکه در K است.

نتیجهٔ ۲.۸. *دو ایده‌آل اصلی (α) و (β) یکسان هستند، اگر و تنها اگر α و β مرتبط باشند.*

اگر α و β مرتبط باشند، $\alpha = \beta\varepsilon$، که ε یک یکه است، و $\beta = \alpha(\frac{1}{\varepsilon})$، که $\frac{1}{\varepsilon}$ یکه است. طبق قضیهٔ قبل، $(\beta) = (\alpha)$. برعکس، اگر $(\beta) = (\alpha)$، آنگاه $\alpha = \beta\gamma$ و $\beta = \alpha\delta$، که γ و δ اعداد صحیح در K هستند. از این رو $\alpha = (\alpha\delta)\gamma$، و $\delta\gamma = ۱$. بنابراین $N\gamma \mid ۱$ و $\frac{\alpha}{\beta} = \gamma$ یکه است.

با تشکیل حاصل‌ضرب AB از ایده‌آل‌های $A = (\alpha_۱, \ldots, \alpha_s)$ و $(\beta_۱, \ldots, \beta_t)$، $B = (\beta_۱, \ldots$ در K، ایده‌آل

$$AB = (\alpha_۱ \beta_۱, \ldots, \alpha_i \beta_j, \ldots, \alpha_s \beta_t)$$

را ایده‌آل تولیدشده توسط همهٔ حاصل‌ضربهای $\alpha_i \beta_j$ در K درنظر می‌گیریم. با در نظر گرفتن قضیهٔ ۱.۸، به راحتی ثابت می‌شود که حاصل‌ضرب AB مستقل از مجموعه‌های خاص مولدهایی است که برای ایده‌آل‌های A و B انتخاب شده‌اند. این یک نتیجهٔ مستقیم تعریف حاصل‌ضرب است که برای ایده‌آل‌های A و B و C داریم

$$AB = BA$$

$$(AB)\, C = A\, (BC)\,.$$

می‌گوییم A، B را عاد می‌کند، می‌نویسیم $A|B$، اگر یک ایده‌آل C موجود است، به‌طوری که $B=AC$. در این صورت، A یک عامل[1] B نامیده می‌شود. می‌گوییم A شامل[2] B است و می‌نویسیم $A\supset B$، اگر هر عضو B در A نیز هست. در این صورت، A یک مقسوم‌علیه[3] B نامیده می‌شود. باید به این تفاوت که بین یک عامل و یک مقسوم‌علیه قائل می‌شویم، بدقت توجه شود.

لم ۸.۳. *اگر* $A|B$، *آنگاه* $A\supset B$.

به عبارت دیگر، می‌توان گفت که یک عامل، یک مقسوم‌علیه است. فرض می‌کنیم که $B=AC$، که $C=(\gamma_1, \ldots, \gamma_v)$. در این صورت، $(\beta_1, \ldots, \beta_t) = (\alpha_1\gamma_1, \ldots, \alpha_j\delta_i, \ldots, \alpha_s\delta_s)$، پس هر β_k به شکل $\sum_{i,j}\lambda_{ij}\alpha_i\gamma_j = \sum_i(\sum_j \lambda_{ij}\gamma_j)\alpha_i$ بوده و در A است. از این رو، A شامل B است.

لم ۸.۴. *یک عدد صحیح گویای غیرصفر، حداکثر در تعدادی متناهی از ایده‌آل‌های* K *وجود دارد.*

فرض می‌کنیم $\omega_1, \ldots, \omega_n$ یک پایهٔ صحیح برای K است. در این صورت، هر عدد صحیح هیأت به شکل $\alpha=\sum_{i=1}^{n} c_i\omega_i$ است که در آن c_i ها اعداد صحیح گویا هستند.

فرض می‌کنیم a یک عدد صحیح گویای غیرصفر و A یک ایده‌آل شامل آن است. چون $\pm a$ هر دو در A هستند، می‌توان فرض کرد که $a>0$. هر c_i را می‌توان به صورت زیر نوشت،

---

1) *Factor* 2) *includes*
3) *divisor*

$$c_i = q_i a + r_i \qquad 0 \le r_i < a \quad و \quad 1 \le i \le n$$

در این صورت

$$\alpha = \sum (q_i a + r_i)\, \omega_i = a \sum q_i\, \omega_i + \sum r_i\, \omega_i = a\gamma + \beta \quad و$$

که در آن γ یک عدد صحیح است و β فقط می‌تواند تعدادی متناهی مقدار متفاوت را اختیار کند (چون $0 \le r_i < a$).

فرض می‌کنیم $A = (\alpha_1, \ldots, \alpha_s)$. چون $a \in A$، $A = (\alpha_1, \ldots, \alpha_s, a)$ با توجه به ملاحظات ذکر شده، هر α_i به شکل $a\gamma_i + \beta_i$ است؛ بنابراین $A = (\beta_1, \ldots, \beta_s, a)$. طبق قضیهٔ ۱.۸، $A = (a\gamma_1 + \beta_1, \ldots, a\gamma_s + \beta_s, a)$. امّا β_i به ازای هر i متعلق به مجموعهٔ اعداد از ۱ تا S می‌تواند فقط تعدادی متناهی از مقادیر متفاوت را اختیار کند. بنابراین، A می‌تواند یکی از این تعداد متناهی از ایده‌آل‌ها باشد.

قضیهٔ ۵.۸. *یک ایده‌آل $A \neq (0)$ تنها تعدادی متناهی مقسوم‌علیه دارد.*

فرض می‌کنیم α یک عضو A است. آنگاه $N\alpha = \alpha\,(\alpha_2 \ldots \alpha_n)$ در A است. اگر $B \supset A$، آنگاه $N\alpha$ در B است. امّا طبق لم پیشگفته، $N\alpha$ تنها می‌تواند در تعدادی متناهی از ایده‌آل‌های B باشد.

از لم ۳.۸ همچنین، نتیجهٔ زیر به دست می‌آید:

نتیجهٔ ۶.۸. *یک ایده‌آل $A \neq (0)$ تنها تعدادی متناهی عامل دارد.*

هدف ما برقرارکردن یک نظریهٔ یگانگی تجزیه برای ایده‌آل‌ها ــ مشابه آنچه در فصل ۱ برای اعداد صحیح گویا به دست آوردیم ــ است. نقش یکه‌ها در نظریهٔ اخیر، به وسیلهٔ ایده‌آل (۱) ــ یعنی حلقهٔ همهٔ اعداد

صحیح در K ــ درنظر گرفته خواهد شد. ایده‌آل‌هایی که وظیفهٔ اعداد صحیح گویای اول را بر عهده می‌گیرند، طبیعتاً آن ایده‌آل‌های P هستند که هیچ عاملی به غیر از P و (۱) ندارند. در متون کلاسیک، مرسوم است که چنین ایده‌آل‌هایی را «اول» می‌نامند؛ امّا در نظریهٔ حلقهٔ جدید کلمهٔ «اول» برای خاصیت دیگری از ایده‌آل‌ها که بعداً ذکر خواهد شد در نظر گرفته شده و بنابراین در حال حاضر، به جای آن، کلمهٔ «تحویل‌ناپذیر» را به کار خواهیم برد. پس یک ایده‌آل P تحویل‌ناپذیر است، اگر هیچ عاملی به غیر از P و (۱) نداشته باشد. آنچه که سرانجام اثبات خواهیم کرد، این است که هر ایده‌آل غیر از (۰) و (۱) را می‌توان ــ صرف نظر از ترتیب و ضرب در (۱) ــ به‌طور یگانه‌ای به صورت حاصل‌ضرب ایده‌آل‌هایی تحویل‌ناپذیر نشان داد.

ما دو اثبات از این قضیهٔ مهم را ارائه خواهیم کرد. یکی از آنها حالت اصلاح شدهٔ اثبات کلاسیک این قضیه بر اساس نظرات ای.هرویتس[۴] بوده، و دیگری اثبات جدید آن است که توسط ای. نوتر و دبلیو[۵]. کرول انجام گرفته است. این دو اثبات، در دو بخش آیندهٔ کتاب ارائه خواهد شد. می‌توانید آنها را مستقل از یکدیگر مطالعه کنید.

معرفی دو نوع دیگر از ایده‌آل‌ها که سرانجام به معادل بودن آنها با یکدیگر و به موضوع ایده‌آل‌های تحویل‌ناپذیر منجر خواهد شد، مفید به‌نظر می‌رسد. یک ایده‌آل A *ماکزیمال*[۶] است، اگر هیچ مقسوم‌علیهی به غیر از (۱) و A نداشته باشد ــ یعنی اگر به جز (۱) در هیچ ایده‌آل بزرگتر قرار نداشته باشد. یک ایده‌آل P غیر از (۰) یا (۱) اول است، اگر این

---

4) *A. Hurwitz*
5) *E. Noether and W. Krull*
6) *maximal*

خاصیت را داشته باشد که در صورت وجود حاصل‌ضرب اعداد صحیح $\gamma\delta$ در P، γ یا δ نیز در P باشد.

قضیهٔ ۷.۸. *یک ایده‌آل P غیر از (۰) یا (۱) ماکزیمال است، اگر و تنها اگر اول باشد.*

ابتدا فرض می‌کنیم $P = (\alpha_1, \ldots, \alpha_s)$ ماکزیمال بوده و شامل $\gamma\delta$ است. این ایده‌آل اگر شامل γ است، اثبات تمام است. پس فرض می‌کنیم شامل γ نیست، و نشان خواهیم داد که شامل δ است. فرض می‌کنیم $P' = (\alpha_1, \ldots, \alpha_s, \gamma)$. در این صورت $P' \supset P$. امّا P ماکزیمال است؛ پس $P' = P$ یا $P' = (1)$. اینکه $P' = P$ غیرممکن است؛ زیرا در این صورت γ در P است. از این رو $P' = (1)$ و بنابراین ۱ در P' است. پس ۱ را می‌توان به صورت زیر نوشت

$$1 = \lambda_1 \alpha_1 + \ldots + \lambda_s \alpha_s + \lambda\gamma \ ,$$

بنابراین

$$\delta = (\lambda_1\delta)\, \alpha_1 + \ldots + (\lambda_s\delta)\, \alpha_s + \lambda\, (\gamma\delta)$$

چون $\alpha_1, \ldots, \alpha_s$ و $\gamma\delta$ در P هستند، پس δ نیز در P قرار دارد و از این رو P اول است.

برعکس، فرض می‌کنیم $P = (\alpha_1, \ldots, \alpha_s)$ یک ایده‌آل اول است و همچنین $P' \supset P$ و $P' \neq P$. باید نشان دهیم که $P' = (1)$. فرض می‌کنیم α یک عدد صحیح در P' است که در P نیست. توانهای α^j را تشکیل می‌دهیم که همگی در P' هستند.

فرض می‌کنیم $\omega_1, \ldots, \omega_n$ یک پایهٔ صحیح برای K بوده و $\beta \neq 0$ یک عدد صحیح دلخواه در P است. در این صورت، $\pm N\beta$ در P

هستند؛ بنابراین P شامل یک عدد صحیح گویای مثبت a است. بنابر اثبات لم ۴.۸، هر عدد صحیح موجود در K را می‌توان به صورت $a\gamma + \sum_{i=1}^{n} \omega_i r_i$ نوشت، که در آن هر یک از r_iها تنها می‌توانند تعدادی متناهی از مقادیر متفاوت را اختیار کنند. در حالت خاص، هر α^j به شکل زیر است،

$$\alpha^j = a\gamma_j + \sum_{i=1}^{n} r_{ij}\,\omega_i$$

پس $\alpha^j - a\gamma_j$ تنها می‌تواند تعدادی متناهی از مقادیر متفاوت را اختیار کند. بنابراین، یک جفت از اعداد صحیح k و l $(k > l)$ وجود دارد، به‌طوری که

$$\alpha^k - a\gamma_k = \alpha^l - a\gamma_l$$

با انتخاب مناسب a ، $\alpha^k - \alpha^l = a(\gamma_k - \gamma_l)$ در P است. بنابراین α^l $(\alpha^{k-l} - 1)$ در P قرار دارد. چون P یک ایده‌آل است، یکی از دو عامل α^l و $\alpha^{k-l} - 1$ باید در P باشد.

حال، $\alpha^l = \alpha \cdot \alpha \ldots \alpha$ ممکن نیست که در P باشد؛ زیرا در غیر این صورت یکی از عامل‌های α در P خواهد بود و این در حالی است که α یک عدد صحیح غیرواقع در P انتخاب شده بود. از این رو، $\alpha^{k-l} - 1$ در P است. چون $P' \supset P$، $\alpha^{k-l} - 1$ نیز در P' است. امّا هر توانی از α، و در حالت خاص α^{k-l}، در P' است. در نتیجه ۱ـ در P' است، و بنابراین $P' = (1)$. این موضوع، نتیجه می‌دهد که P ماکزیمال است.

نتیجهٔ ۸.۸. *اگر P یک ایده‌آل ماکزیمال بوده و $P \supset AB$، آنگاه $P \supset A$ یا*

$P \supset B$.

اگر $P \supset A$، به نتیجه رسیده‌ایم. فرض می‌کنیم α در A است، ولی در P نیست. اگر β در B است، آنگاه $\alpha\beta$ در P است؛ زیرا $P \supset AB$. امّا P اول است، بنابراین طبق قضیهٔ ۷.۸، شامل β می‌شود. از این رو، هر عضو B در P است، یعنی $P \supset B$.

۲. اثبات کلاسیک قضیهٔ یگانگی تجزیه.

این بخش را با لم زیر شروع می‌کنیم:

لم ۹.۸. *هر ایده‌آل A غیر از (۰) و (۱) یک مقسوم‌علیه ماکزیمال دارد.*

بنابر قضیهٔ ۵.۸، ایده‌آل A تنها تعدادی متناهی مقسوم‌علیه دارد. هر مقسوم‌علیه B از A ($B \neq A$) مقسوم‌علیه‌هایی کمتر از A دارد؛ زیرا هر مقسوم‌علیه B یک مقسوم‌علیه A است، چون $B \supset A$، و به علاوه A یک مقسوم‌علیه دارد که B ندارد، یعنی خود A.

در میان مقسوم‌علیه‌های A یکی را متفاوت از (۱) با کمترین تعداد مقسوم‌علیه انتخاب می‌کنیم. این کار، بنابر قضیهٔ ۵.۸ ممکن است، این مقسوم‌علیه را P می‌نامیم. پس P ماکزیمال است. اگر چنین نبود، یک ایده‌آل $P' \neq (1)$ وجود داشت، به‌طوری که $P' \supset P$، $P' \neq P$. امّا در این صورت P' مقسوم‌علیه‌های کمتر از P دارد و $P' \supset A$ که این با انتخاب P در تناقض است.

لم زیر برای اثبات عکس لم ۳.۸ استفاده خواهد شد.

لم ۱۰.۸. *اگر*

$$f(x) = \delta_m x^m + \delta_{m-1} x^{m-1} + \ldots + \delta_0 \quad (\delta m \neq 0)$$

را یک چندجمله‌ای در نظر بگیریم که همهٔ ضرایب آن اعداد صحیح بوده و ρ یکی از ریشه‌های آن است، آنگاه همهٔ ضرایب چندجمله‌ای $\frac{f(x)}{x - \rho}$ اعداد صحیح جبری هستند.

بنابر قضیهٔ ۲.۶، $\delta_m \rho$ یک عدد صحیح جبری است، زیرا در معادلهٔ

$$x^m + \delta_{m-1} x^{m-1} + \ldots + \delta_m{}^{m-1} \delta_0 = 0$$

صدق می‌کند. برای اثبات لم، از استقراء استفاده می‌کنیم. این لم، یقیناً برای $m = 1$ درست است. فرض می‌کنیم که این لم برای همهٔ چندجمله‌ای‌های از درجهٔ کوچکتر یا مساوی $m - 1$ برقرار است، چون

$$\phi(x) = f(x) - \delta_m x^{m-1} (x - \rho)$$

از درجهٔ کوچکتر یا مساوی $m - 1$ است و چون $\phi(\rho) = 0$، چندجمله‌ای

$$\frac{\phi(x)}{x - \rho} = \frac{f(x)}{x - \rho} - \delta_m x^{m-1}$$

ضرایب صحیح دارد. پس $\frac{f(x)}{x - \rho}$ نیز چنین است. این معنی، استقراء را کامل می‌کند.

لم ۱۱.۸. اگر $f(x)$ همان چندجمله‌ای لم ۸. ۱۰ است و

$$f(x) = \delta_m (x - \rho_1) \ldots (x - \rho_m),$$

آنگاه $\delta_m \rho_1 \ldots \rho_k$ برای m، ...، ۲، $K = 1$ یک عدد صحیح جبری است.

زیرا با به کار بردن متوالی لم پیشگفته،

$$\frac{f(x)}{(x - \rho_{k+1}) \dots (x - \rho_m)} = \delta_m (x - \rho_1) \dots (x - \rho_k)$$

تنها ضرایب صحیح دارد.

لم بعد، تعمیمی از لم گاوس (قضیهٔ ۶.۳) است.

لم ۱۲.۸. فرض می‌کنیم

$$p(x) = \alpha_p x^p + \alpha_{p-1} x^{p-1} + \dots + \alpha_0$$

$$q(x) = \beta_r x^r + \beta_{r-1} x^{r-1} + \dots + \beta_0$$

و

چندجمله‌ای‌هایی با ضرایب صحیح هستند و $\alpha_p \beta_r \neq 0$. همچنین، فرض می‌کنیم

$$r(x) = p(x)\, q(x) = \gamma_s x^s + \gamma_{s-1} x^{s-1} + \dots + \gamma_0$$

اگر δ یک عدد صحیح است، به‌طوری که همهٔ δ / γ_kها نیز اعداد صحیح هستند، آنگاه تمام $\alpha_i \beta_j / \delta$ها نیز عدد صحیح خواهند بود.

زیرا فرض می‌کنیم

$$p(x) = \alpha_p (x - \rho_1) \dots (x - \rho_p) \quad ,$$

و ؛ $$q(x) = \beta_r (x - \delta_1) \dots (x - \delta_r)$$

آنگاه

$$\frac{r(x)}{\delta} = \frac{\alpha_p \beta_r}{\delta} (x - \rho_1) \dots (x - \rho_p) (x - \delta_{p1}) \dots (x - \delta_r)$$

ضرایب صحیح دارد. طبق لم ۱۱.۸، هر حاصل‌ضرب

$$\frac{\alpha_p \beta_r}{\delta} \rho_{n1} \rho_{n2} \dots \rho_{ni} \delta_{m1} \delta_{m2} \dots \delta_{mk} \qquad (8.1)$$

یک عدد صحیح است. امّا α_i/α_p و β_j/β_r توابع متقارن ابتدایی، به ترتیب بر حسب ρ_i و δ_i هستند. بنابراین

$$\frac{\alpha_i \beta_j}{\delta} = \frac{\gamma_s}{\delta} \frac{\alpha_i}{\alpha_p} \frac{\beta_j}{\beta_r}$$

مجموعی از جمله‌های به شکل (۸.۱) است. از این رو، $\frac{\alpha_i \beta_j}{\delta}$ یک عدد صحیح جبری است.

قضیهٔ ۱۳.۸. *برای هر ایده‌آل* $A \neq (0)$ *یک ایده‌آل* $B \neq (0)$ *وجود دارد، به‌طوری که* AB *اصلی است. در حقیقت، می‌توان* B *را چنان یافت که* $AB = (a)$ *و* a *یک عدد صحیح گویاست.*

فرض می‌کنیم $A = (\alpha_1, \ldots, \alpha_r)$ و تعریف می‌کنیم

$$g_i(x) = \alpha_1^{(i)} x + \alpha_2^{(i)} x^2 + \ldots + \alpha_r^{(i)} x^r, \qquad i = 1, \ldots, n$$

که در آن اعداد به فورم $\alpha_j^{(i)}$، $i = 1, \ldots, n$ مزدوج‌های α_j در K هستند. حال، با استفاده از بحثی که با آن آشنا هستیم، می‌توان گفت که حاصل‌ضرب

$$F(x) = g_1(x) \ldots g_n(x) = \sum c_p x^p$$

یک چندجمله‌ای با ضرایب صحیح گویاست. به علاوه $g_1(x) \mid F(x)$، که در آن $g_1(x)$ را یک چندجمله‌ای می‌گیریم که α_i های اصلی را به عنوان ضرایب داراست. خارج قسمت

$$h(x) = \frac{F(x)}{g_1(x)} = g_2(x) \ldots g_n(x) = \beta_1 x + \ldots + \beta_m x^m$$

ضرایبی دارد که اعداد صحیحی در K هستند.

فرض می‌کنیم a بزرگترین مقسوم‌علیه مشترک c_p ها است. بنابراین

حقیقت، $\frac{F(x)}{a}$ ابتدایی است. تعریف می‌کنیم $B = (\beta_1, \ldots, \beta_m)$. نشان خواهیم داد که $AB = (a)$.

طبق لم ۱۲.۸، a همهٔ $\alpha_i \beta_j$ها را عاد می‌کند. این در حالی است که AB با همهٔ حاصل‌ضربهای $\alpha_i \beta_j$ تولید شده است. از این رو، $AB \supset (a)$. از طرف دیگر، چون a بزرگترین عامل مشترک c_p هاست، اعداد صحیح گویای c_k/a نسبت به هم اولند. پس اعداد صحیح به فورم x_kوجود دارند، به‌طوری که[۷]

$$a = \sum x_k c_k \quad \text{و} \quad 1 = \sum x_k \frac{c_k}{a}$$

امّا هر c_k، طبق تعریف به شکل $\sum \lambda_{ijk} \alpha_i \beta_j$ است. در نتیجه، a به شکل $\sum_{i,j} (\sum_k \lambda_{ijk} x_k) \alpha_i \beta_j$ است؛ و بنابراین a در ABاست و $AB \supset (a)$. پس سرانجام نتیجه می‌گیریم که $AB = (a)$.

نتیجهٔ ۱۴.۸. *اگر* $AB = AC$، $A \neq (0)$ *آنگاه* $B = C$.

زیرا فرض می‌کنیم $AD = (\delta)$، یک ایده‌آل اصلی است. در این صورت، $ABD = ACD$و $B = (\delta)C$. پس δ برابر هر عدد صحیح در B، مساوی است با δ برابر بعضی اعداد صحیح در C. بنابراین، هر عدد صحیح موجود در B در C نیز هست و $C \supset B$. به‌طور مشابه، می‌توان نتیجه گرفت که $B \supset C$، بنابراین، $B = C$.

نتیجهٔ ۱۵.۸. (عکس لم ۳.۸). *اگر* $A \supset B$، *آنگاه* $A|B$. به عبارت دیگر، یک مقسوم‌علیه، یک عامل است.

D را چنان انتخاب می‌کنیم که داشته باشیم $AD = (\delta)$. چون $A \supset B$،

---

۷) این مطلب، به روش مشابه قضیهٔ ۲.۱ قابل اثبات است.

$AD \supset BD$؛ این موضوع از تعریف حاصل‌ضرب ایده‌آل‌ها نتیجه می‌شود. می‌نویسیم $BD = (\rho_1, \ldots, \rho_m)$. هر ρ_i در $AD = (\delta)$ بوده و بنابراین به شکل $\delta\ \lambda_i$ است. از این رو

$$BD = (\delta)\ (\lambda_1, \lambda_2, \ldots, \lambda_m) = AD\ (\lambda_1, \lambda_2, \ldots, \lambda_m)$$

بنابر نتیجهٔ ۱۴.۸، $B = A\ (\lambda_1, \lambda_2, \ldots, \lambda_m)$. بنابراین، $A \mid B$.

نتیجهٔ ۱۶.۸. *یک ایده‌آل ماکزیمال است، اگر و تنها اگر تحویل‌ناپذیر باشد.*

زیرا هم اکنون ثابت شد که عامل‌ها و مقسوم‌علیه‌ها یکسان هستند؛ بنابراین ایده‌آلی که یکی را ندارد، دیگری را هم ندارد.

لم ۱۷.۸. *اگر $A \mid B$ و $B \neq A$، آنگاه B عامل‌های کمتری از A دارد.*

این مطلب در بخشی از اثبات لم ۹.۸ ثابت شده است؛ چون اکنون می‌دانیم که مقسوم‌علیه‌ها و عامل‌ها یکی هستند.

لم ۱۸.۸. *هر ایده‌آل غیر از (۰) یا (۱) قابل تجزیه به حاصل‌ضرب ایده‌آل‌های تحویل‌ناپذیر است.*

طبق لم ۹.۸، ایده‌آل A یک مقسوم‌علیه ماکزیمال P_1 دارد، که به موجب نتیجهٔ ۱۵.۸ یک عامل نیز هست. پس $A = P_1 A_1$. اگر A_1 ایده‌آل (۱) یا ماکزیمال است، کار تمام است. در غیر این صورت، همین روش را با $A_1 = P_2 A_2$ تکرار می‌کنیم تا به دست آوریم $A = P_1 P_2 A_2$ و به همین طریق ادامه می‌دهیم. سرانجام این عمل باید متوقف شود؛ چون A_1 و A_2 و ... هر یک عامل‌های ماقبل خود را عاد کرده و بنابراین طبق لم ۱۷.۸ نسبت به عامل ماقبل خود عامل‌های

کمتری دارند. بدین ترتیب، می‌توان نتیجه گرفت $A = P_1 P_2 \dots P_r$، که هر P_i ماکزیمال است. بنابر نتیجهٔ ۱۶.۸، هر P_i تحویل‌ناپذیر است و بدین ترتیب لم ثابت می‌شود.

برای اثبات یگانگی تجزیه، از لم زیر که از نتایج ۸.۸ و ۱۵.۸ و ۱۶.۸ استنباط می‌شود استفاده خواهیم کرد:

لم ۱۹.۸. *اگر P یک ایده‌آل تحویل‌ناپذیر است و $P|AB$، آنگاه $P|A$ یا $P|B$.*

قضیهٔ ۲۰.۸. (*قضیهٔ اساسی*). *هر ایده‌آل غیر از (۰) یا (۱) قابل تجزیه به حاصل‌ضرب ایده‌آل‌های تحویل‌ناپذیر است. این تجزیه، صرف نظر از ترتیب عامل‌ها یگانه است.*

قسمت اول قضیه قبلاً به عنوان لم ۱۸.۸ ثابت شده است؛ بنابراین ما به قسمت دوم قضیه که مربوط به یگانگی است می‌پردازیم. فرض می‌کنیم که ایده‌آل A را بتوان به دو طریق به ایده‌آل‌های تحویل‌ناپذیر تجزیه کرد، بدین ترتیب که

$$A = P_1 P_2 \dots P_r = P'_1 P'_2 \dots P'_s \quad \text{و} \quad s \geq r \qquad (۸.۲)$$

بنابر لم ۱۹.۸، ایده‌آل P'_1 باید یکی از P_iها، فرضاً P_1 را، عاد کند. پس $P'_1|P_1$ و $P_1 \subset P'_1$. امّا P_1 ماکزیمال است و $P'_1 \neq (1)$؛ بنابراین $P_1 = P'_1$. بنابر نتیجهٔ ۱۴.۸، با تقسیم طرفین رابطهٔ (۸.۲) بر P_1 داریم

$$P_2 \dots P_r = P'_2 \dots P'_s$$

می‌توان این روش را تکرار کرد تا همهٔ عامل‌های سمت چپ حذف شوند. فرض می‌کنیم یک عامل P'_i در سمت راست باقیمانده است. پس $(1) |$

P'_i و $(1) \supset P'_i$، $P'_i = (1)$. از این رو، همهٔ عامل‌های سمت راست نیز تماماً به کار رفته‌اند. بنابراین، بعد از تغییر آرایش P_i ها در صورت لزوم، خواهیم داشت $P_i = P'_i$، $i = 1, \ldots, r$، و $r=s$؛ و بدین طریق اثبات کامل می‌شود.

۳. اثبات جدید. صورت زیر، نتیجه‌ای است که توسط اور[8] و طی بررسیهای او مطرح شده است (به فهرست منابع مراجعه شود). ما هیچ استفاده‌ای از نتایج به دست آمده در بخش ۲ نخواهیم کرد بلکه، کار خود را مستقیماً با اثبات صورت اصلاح‌شده‌ای از قضیهٔ ۲۰.۸ که در آن مفهوم «تحویل‌ناپذیری» با «ماکزیمال بودن» جایگزین شده است، ادامه می‌دهیم. به عنوان نتیجه‌ای از این موضوع، به اثبات نتایج ۱۵.۸ و ۱۶.۸ می‌پردازیم. این کار، ما را قادر می‌سازد که کلمهٔ «تحویل‌ناپذیر» را به جای «ماکزیمال» به کار ببریم و در نتیجه قضیهٔ ۲۰.۸ را به شکل نهایی آن ثابت کنیم. خواننده به یاد می‌آورد که آخرین قضیه‌ای که مجاز بودیم در این پاراگراف از آن استفاده کنیم، قضیهٔ ۷.۸ بود که ادعا می‌کند ایده‌آل‌های ماکزیمال و اول معادل هستند. معادل بودن عامل‌ها و مقسوم‌علیه‌ها در بخش دوم این فصل ثابت شده است، و در اینجا نیز ما نمی‌توانیم از این حقیقت بدون اینکه ابتدا اثباتی برای آن ارائه دهیم استفاده کنیم.

لم ۲۱.۸. *یک ایده‌آل A غیر از (0) یا (1) یک عامل حاصل‌ضرب باید $P_1 \ldots P_s$ باشد، که هر P_i یک عامل A و یک ایده‌آل ماکزیمال است.*

اگر A ماکزیمال است، چیزی برای اثبات نداریم؛ امّا اگر ماکزیمال نیست، آنگاه طبق قضیهٔ ۷.۸، A شامل یک حاصل‌ضرب $\beta\gamma$ است،

8) *Ore*

به‌طوری که β و γ هیچ یک در A نیستند. اگر $A = (\alpha_1, \ldots, \alpha_r)$، فرض می‌کنیم

$$B = (\alpha_1, \ldots, \alpha_r, \beta) \quad \text{و} \quad C = (\alpha_1, \ldots, \alpha_r, \gamma)$$

پس $A \supset BC$، $B \supset A$، و $C \supset A$. حال این روش را با B و C تکرار کرده و ادامه می‌دهیم. در هر مرحله، همهٔ ایده‌آل‌های جدید شامل A هستند و حاصل‌ضرب آنها در Aاست. امّا ادامهٔ این روش طبق قضیهٔ ۵.۸ باید متوقف شود؛ بنابراین بالاخره به ایده‌آل‌های ماکزیمال می‌رسیم.

فرض می‌کنیم P یک ایده‌آل ماکزیمال است. P^{-1} را مجموعهٔ اعداد α صحیح یا غیرصحیح در هیأت K تعریف می‌کنیم، به‌طوری که حاصل‌ضرب $\alpha\pi$ برای همهٔ اعداد π موجود در P، یک عدد صحیح (نه لزوماً در P) است.

لم ۲۲.۸. *اگر P یک ایده‌آل ماکزیمال است، P^{-1} شامل عددی است که یک عدد صحیح جبری نیست.*

فرض می‌کنیم π ـ که صفر نیست ـ یک عدد صحیح در P است و ایده‌آل اصلی (π) را در نظر می‌گیریم. طبق لم پیشگفته (π) شامل یک حاصل‌ضرب $P_1 \ldots P_r$ از ایده‌آل‌های ماکزیمال است. در صورت وجود چند نمونه از چنین حاصل‌ضربهایی، یکی را انتخاب می‌کنیم که برای آن r کمترین مقدار است. حال $P_1 \ldots P_r \supset (\pi) \supset P$، پس طبق نتیجهٔ ۸.۸، P شامل یکی از P_iها ـ مثلاً P_1 ـ است. چون P_1 ماکزیمال است، $P = P_1$. ایده‌آل (π) شامل $P_2 \ldots P_r$ نیست، چون حاصل‌ضربی که کمترین تعداد عامل را داشت برای شروع انتخاب کردیم. پس $P_2 \ldots P_r$ شامل عدد

صحیحی مثل γ است که در (π) نیست. در نتیجه $\frac{\gamma}{\pi}$ یک عدد صحیح نیست، امّا $(\gamma) P \subset PP_2 \dots P_r \subset (\pi)$. این بدین معنی است که اگر π' در P است، آنگاه $\pi'\gamma$ در (π) خواهد بود پس $\frac{\pi'\gamma}{\pi}$ یک عدد صحیح بوده و از این رو $\frac{\gamma}{\pi}$ در P^{-1} است.

اگر A یک ایده‌آل است، حاصل‌ضرب $AP^{-1} = P^{-1}A$ را مجموعهٔ همهٔ حاصل‌ضربهای $\alpha\beta$ تعریف می‌کنیم که α در A و β در P^{-1} است.

لم ۲۳.۸. *اگر P یک ایده‌آل ماکزیمال است، آنگاه $PP^{-1} = (1)$.*

فرض می‌کنیم $A = PP^{-1}$. A یک ایده‌آل است (چرا؟). چون P^{-1} شامل ۱ است. $A \supset P$. امّا P ماکزیمال است؛ بنابراین $A = (1)$ یا $A = P$.

فرض می‌کنیم $A = P$. این فرض، منجر به یک تناقض خواهد شد. بدین ترتیب که فرض می‌کنیم $\omega_1 \dots \omega_n$ یک پایه برای P بوده و $\gamma_1 = \frac{\gamma}{\pi}$ یک عدد غیرصحیح در P^{-1} است (به لم پیشگفته مراجعه شود). حاصل‌ضربهای $\gamma_1 \omega_i$ همگی در $A = P$ هستند و بنابراین می‌توان آنها را به صورت

$$\gamma_1 \omega_i = \sum_{j=1}^{n} a_{ij} \omega_j \ ,$$

نمایش داد، که در آن a_{ij} ها اعداد صحیح گویا هستند. پس دستگاه معادلات

$$(a_{11} - \gamma_1) x_1 + a_{12} x_2 + \dots = 0$$
$$(a_{21} x_1 + (a_{22} - \gamma_1) x_2 + \dots = 0$$
$$\dots\dots\dots\dots\dots\dots$$

$$a_{n1} x_1 + \ldots + (a_{nn} - \gamma_1) x_n = 0$$

یک جواب غیر بدیهی $x_i = \omega_i$ دارد؛ بنابراین دترمینان

$$\begin{vmatrix} a_{11} - \gamma_1 & a_{12} & \ldots & \ldots \\ a_{21} & a_{22} - \gamma_1 & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} - \gamma_1 \end{vmatrix}$$

صفر می‌شود. از این رو، γ_1 در یک معادلهٔ تکین با ضرایب عدد صحیح صدق می‌کند و در نتیجه یک عدد صحیح جبری است. از این تناقض، می‌توان نتیجه گرفت که $A = (1)$.

لم ۲۴.۸. *هر ایده‌آل A که غیر (0) یا (1) است، حاصل‌ضرب ۱۰۶ ایده‌آل‌های ماکزیمال است.*

طبق لم ۲۱.۸، A شامل یک حاصل‌ضرب $P_1 \ldots P_r$ از ایده‌آل‌های ماکزیمال است و ما مانند گذشته حاصل‌ضربی را انتخاب می‌کنیم که برای آن r کمترین مقدار است. حال، با استقراء روی r کار خود را ادامه می‌دهیم.

اگر A شامل تنها یک ایده‌آل ماکزیمال P است، آنگاه $A = P$ و کار تمام است. فرض می‌کنیم قضیه برای ایده‌آل‌هایی که شامل یک حاصل‌ضرب با کمتر از r عامل هستند ثابت شده باشد. چون $A \supset P_1 \ldots P_r$، پس طبق لم ۲۳.۸، $AP_r^{-1} \supset P_1 \ldots P_{r-1}$. طبق فرض استقراء AP_r^{-1} یک حاصل‌ضرب $P'_1 P'_2 \ldots P'_k$ از ایده‌آل‌های ماکزیمال است. با استفادهٔ مجدد از لم ۲۳.۸ نتیجه می‌گیریم که $A = P'_1 P'_2 \ldots P'_k P_r$. بنابراین، A یک حاصل‌ضرب از ایده‌آل‌های ماکزیمال است.

لم ۲۵.۸. *فرض می‌کنیم* $A = P_1 \dots P_r$ *و* $B = Q_1 \dots Q_s$ *حاصل‌ضربهایی از ایده‌آل‌های ماکزیمال غیر (۱) هستند. اگر* $B \supset A$، *آنگاه هر ایده‌آل* Q، *حداقل به اندازهٔ دفعات واقع شدن در* B، *درمیان* P*ها پیدا می‌شود.*

چون Q_1 یک عامل B است، یک مقسوم‌علیه B است (لم ۳.۸). از این رو، $Q_1 \supset B \supset A = P_1 \dots P_r$. بنابر نتیجهٔ ۸.۸، Q_1 شامل یکی از P_iها، مثلاً P_1، است، بنابراین $Q_1 = P_1$، که هر کدام از آنها ماکزیمال و غیر از (۱) هستند. همچنین، بنابر لم ۲۳.۸

$$P_1^{-1} B \supset P_1^{-1} A = P_2 \dots P_r \quad \text{و}$$

پس اگر فرض کنیم حکم برای وقتی که B شامل کمتر از r عامل است برقرار است، نتیجه با استقراء حاصل خواهد شد.

لم ۲۶.۸. *نمایش یک ایده‌آل به صورت حاصل‌ضرب ایده‌آل‌های ماکزیمال، بدون درنظرگرفتن ترتیب یگانه است.*

زیرا فرض می‌کنیم

$$A = P_1 P_2 \dots P_r = Q_1 Q_2 \dots Q_s$$

آنگاه، تنها باید لم پیشگفته را با فرض $A = B$ به کار بگیریم. به عنوان نتیجه‌ای از لم ۲۴.۸ و ۲۶.۸، قضیهٔ زیر را داریم :

قضیهٔ ۲۷.۸. *یک ایده‌آل غیر از (۰) و (۱) را می‌توان، صرف نظر از ترتیب، به‌طور یگانه‌ای به صورت حاصل‌ضرب ایده‌آل‌های ماکزیمال*

نمایش داد.

برای اثبات قضیهٔ اساسی ۸ . ۲۰، کافی است نشان دهیم که کلمهٔ «ماکزیمال» در قضیهٔ ذکرشده می‌تواند با کلمهٔ «تحویل‌ناپذیر» تعویض شود. این معنی قابل اثبات است، اگر بتوان ثابت کرد که یک مقسوم‌علیه، یک عامل است، به عبارت دیگر، اگر $A \supset B$، آنگاه $B|A$. امّا این موضوع از لم ۸ . ۲۵ نتیجه می‌شود؛ زیرا می‌توان نوشت $A = P_1^{e_1} \dots P_r^{er}$ و $B = P_1^{f_1} \dots P_r^{fr}$، که P_iها عامل‌های ماکزیمال مجزای A و B هستند و $e_i \geq f_i$. پس $A = BC$، که در آن $C = P_1^{e_1 - f_1} \dots P_r^{er - fr}$. بدین ترتیب، قضیهٔ اساسی ثابت شده است.

از قضیهٔ ۸ . ۷ و نتیجهٔ ۸ . ۱۶، استنباط می‌شود که ایده‌آل‌های تحویل‌ناپذیر، ماکزیمال و اول یکی هستند. متون مربوط به اعداد جبری غالباً از آخرین کلمه استفاده می‌کنند، و ما نیز متعاقباً از همین سنت پیروی خواهیم کرد.

فصل ۹

نتایج قضیهٔ اساسی

۱. **بزرگترین عامل مشترک دو ایده‌آل.** فرض می‌کنیم A و B دو ایده‌آل در هیأت اعداد جبری K هستند. ایده‌آل C *بزرگترین عامل مشترک*[1] A و B نامیده می‌شود، می‌نویسیم (B و A)، اگر $C|A$ و $C|B$، و اگر هر ایده‌آلی که هم A و هم B را عاد کند، C را نیز عاد می‌کند. بزرگترین عامل مشترک یگانه است؛ زیرا اگر دو ایده‌آل C و D هر دو خواص لازم برای بزرگترین عامل مشترک بودن را دارا باشند، آنگاه $C|D$ و $D|C$. در این حالت بنابر لم ۳.۸، $C \supset D$ و $D \supset C$، و بنابراین $C = D$.

برای یافتن (B و A)، روش ساده‌ای به صورت ذکرشونده وجود دارد. فرض می‌کنیم داشته باشیم $A = (\alpha_1, \ldots, \alpha_r)$ و $B = (\beta_1, \ldots, \beta_s)$. تعریف می‌کنیم $D = (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$. در نتیجه، $D = (A$ و $B)$؛ زیرا بوضوح مشخص است که $D \supset A$ و $D \supset B$، و بنابراین (نتیجهٔ ۱۵.۸) $D|A$ و $D|B$. به علاوه، فرض می‌کنیم $E|A$ و $E|B$. پس $E \supset A$ و $E \supset B$،

---

1) *highest common factor*

و بنابراین $E \supset D$. از این رو، $E \mid D$. روش دیگر یافتن بزرگترین عامل مشترک A و B به این صورت است که فرض می‌کنیم $P_1, \ldots, P_r$ مجموعهٔ کلیهٔ ایده‌آل‌های اول مجزایی است که در تجزیهٔ هر دو ایده‌آل A و B موجود هستند. پس $(A \text{ و } B) = P_1^{e} \ldots P_r^{er}$، که در آن e_i بزرگترین توانی (احتمالاً صفر[۲]) است که به ازای آن P_i^{ei} هم A و هم B را عاد می‌کند.

قضیهٔ ۱.۹. *دو ایده‌آل A و B یک بزرگترین عامل مشترک یگانه $(A \text{ و } B)$ دارند.*

اگر $(A \text{ و } B) = (۱)$، می‌گوییم A و B *نسبت به هم اولند*. در این حالت، معمولاً برای سادگی می‌نویسیم $(A \text{ و } B) = ۱$.

قبلاً دیدیم (قضیهٔ ۱۱.۷) که هر ایده‌آل در هیأت K لزوماً اصلی نیست. حال در موقعیتی هستیم که نشان دهیم یک ایده‌آل همیشه می‌تواند با دو عضو K تولید شود.

لم ۲.۹. *اگر A و B ایده‌آل‌هایی غیر از (۰) هستند، یک عدد صحیح α در A وجود دارد، به‌طوری که*

$$(\frac{(\alpha)}{A}, B) = ۱.$$

اگر α در A است، آنگاه $(\alpha) \supset A$ و $(\alpha) \mid A$؛ و بنابراین صحبت کردن از ایده‌آل $\frac{(\alpha)}{A}$ معنی دارد.

اگر $B = (۱)$، آنگاه لم مورد بحث بدیهی است؛ زیرا می‌توان α را هر عضو A اختیار کرد. پس فرض می‌کنیم $B \neq (۱)$.

فرض می‌کنیم $P_1, \ldots, P_r$ عامل‌های اول مجزای B هستند. اگر $r=۱$،

---

۲) مناسب است توان $C^{۰}$ یک ایده‌آل C را به صورت (۱) تعریف کنیم.

آنگاه $B = P^j$، $j > 0$. پس تنها لازم است یک α را در A پیدا کنیم که برای آن بتوان نوشت

$$(\frac{(\alpha)}{A}, P) = 1$$

یک عدد صحیح α را در A انتخاب می‌کنیم که در AP نیست. یک چنین عددی وجود دارد؛ زیرا در غیر این صورت $AP \supset A$ و $AP | A$. در نتیجه، چون $A \neq (0)$، $P | (1)$، $P \supset (1)$ و $P = (1)$. این انتخاب α خاصیت مطلوب را دارد؛ زیرا $A \supset (\alpha)$ و $A | (\alpha)$، و بنابراین برای بعضی ایده‌آل‌ها چون C خواهیم داشت $(\alpha) = AC$. در چنین وضعیتی $(P \text{ و } C) = 1$؛ زیرا اگر $(P \text{ و } C) \neq 1$، C و P بزرگترین عامل مشترک P را خواهند داشت؛ و در نتیجه $C = PD$، $(\alpha) = APD$، $AP | (\alpha)$، و $AP \supset (\alpha)$ که این نتیجه با انتخابی که از α داشتیم در تناقض است.

اگر $r > 1$، کافی است α را چنان بیابیم که

$$((\alpha)/A, P_m) = 1 \qquad m = 1, \ldots, r \qquad (9.1)$$

ایده‌آل‌های $A_m = \frac{AP_1 \ldots P_r}{P_m}$ و P_m را درنظر می‌گیریم. بنابر پاراگراف قبل، می‌توان یک عنصر α_m را از A_m انتخاب کرد، به‌طوری که

$$((\alpha_m)/A_m, P_m) = 1 . \qquad (9.2)$$

حال، فرض می‌کنیم $\alpha = \alpha_1 + \ldots + \alpha_r$. چون $A | A_m$، $A \supset A_m$ و هر α_m در A_m است. بنابراین، α در A نیز هست.

اگر بتوانیم نشان دهیم که α در AP_m نیست، آنگاه رابطهٔ (۹.۱) ثابت شده است؛ زیرا اگر $\frac{(\alpha)}{A}$ و P_m یک عامل مشترک داشته باشند، آن عامل باید خود P_m باشد. در این حالت، $\frac{(\alpha)}{A} = P_m D$ و $(\alpha) = AP_m D$؛ پس

$(\alpha) \supset AP_m$ که این یک تناقض است.

برای نشان دادن اینکه $\alpha = \alpha_1 + \ldots + \alpha_r$ در AP_m نیست، باید توجه کرد که هر α_i ، $i \neq m$ ، در AP_m است؛ زیرا

$$(\alpha_i) \subset A_i = \frac{AP_1 \ldots P_r}{P_i} = AP_m \frac{P_1 \ldots P_r}{P_i P_m} \subset AP_m \quad \text{و}$$

و این در حالی است که با توجه به رابطهٔ (۹.۲) ، α_m خودش در AP_m نیست.

قضیهٔ ۳.۹. *فرض می‌کنیم A یک ایده‌آل غیرصفر و β هر عنصر غیرصفر در A است. در این صورت، می‌توان یک عدد α را در A چنان یافت که $A = (\alpha \text{ و } \beta)$.*

تعریف می‌کنیم $B = \frac{(\beta)}{A}$. طبق لم قبل در A یک عدد α موجود است، به‌طوری که

$$(\frac{(\alpha)}{A}, B) = (\frac{(\alpha)}{A}, \frac{(\beta)}{A}) = 1$$

فرض می‌کنیم $(\alpha) = AC$ و $C = \frac{(\alpha)}{A}$. چون $(\beta) = AB$ و $(B \text{ و } C) = 1$، بزرگترین عامل مشترک (α) و (β) ، A است. حال، با توجه به قضیهٔ ۱.۹، $A = (\alpha, \beta)$.

قابل توجه است که در مواقع قرار داشتن α در A، مکرراً از خارج‌قسمت $\frac{(\alpha)}{A}$ استفاده کردیم. در آینده، این خارج قسمت را به صورت $\frac{\alpha}{A}$ نوشته و A/α را به معنای $A \mid (\alpha)$ تلقی خواهیم کرد. α در A است، اگر و تنها اگر $A \mid \alpha$. این معنی را می‌توان با استفاده از نمادهای (سنج A) $\equiv 0$ یا $\alpha \equiv 0$ (A) نیز نشان داد.

۲. یگانگی تجزیهٔ اعداد صحیح. حال به مسئلهٔ یگانگی تجزیهٔ اعداد

صحیح در K، سؤالی که پاسخ به آن را در فصل ۷ موقتاً رها کرده بودیم، بازمی‌گردیم. قضیهٔ بعدی، حدسی را که در آنجا بیان کردیم تأیید می‌کند.

قضیهٔ ۴.۹. *تجزیهٔ اعداد صحیح K به اعداد اول (بدون درنظر گرفتن ترتیب و یکه‌ها) یگانه است؛ اگر و تنها اگر همهٔ ایده‌آل‌های K اصلی باشند.*

قبلاً در قضیهٔ ۵.۷ ثابت کرده‌ایم که چنین تجزیه‌ای ممکن است.

ابتدا فرض می‌کنیم که همهٔ ایده‌آل‌های K اصلی هستند. فرض می‌کنیم عنصری غیرصفر و غیریکه در K دارای دو حالت در تجزیه به اعداد صحیح اول باشد، بدین ترتیب که

$$\alpha = \pi_1 \dots \pi_s = \pi'_1 \dots \pi'_t$$

واضح است که

$$(\alpha) = (\pi_1) \dots (\pi_s) = (\pi'_1) \dots (\pi'_t) \qquad (۹.۳)$$

اگر π یک عدد صحیح اول است، آنگاه (π) یک ایده‌آل اول است، برای اینکه فرض می‌کنیم $(\pi) = BC$. چون B و C هر دو طبق فرض اصلی هستند، $(\beta\gamma) = (\beta)(\gamma) = (\pi)$. بنابر نتیجهٔ ۲.۸، π و $\beta\gamma$ مرتبط هستند، پس یا β و یا γ یکه هستند. از این رو، یکی از دو ایده‌آل B و C ایده‌آل (۱) بوده و (π) اول است. پس رابطهٔ (۹.۳)، دو تجزیهٔ (α) به ایده‌آل‌های اول را ارائه می‌کند. طبق اصل یگانگی تجزیهٔ ایده‌آل‌ها، باید داشته باشیم $S = t$ و، بعد از یک تجدید آرایش مناسب عامل‌ها، $(\pi_i) = (\pi'_i)$. به علاوه π_i/π'_i یکه است. این معنی، شرط کفایت را ثابت می‌کند.

برای اثبات شرط لزوم قضیه، با فرض اینکه تجزیهٔ اعداد صحیح یگانه

است، سعی می‌کنیم نشان دهیم که همهٔ ایده‌آل‌ها اصلی هستند. بدین منظور، کافی است ثابت کنیم که هر ایده‌آل اول P اصلی است. طبق قضیهٔ ۱۳.۸، به ازای برخی اعداد صحیح گویا چون a، $P \mid a$. فرض می‌کنیم $a = \pi_1 \dots \pi_r$ تجزیهٔ a به اعداد صحیح اول در K است. پس $(\pi_r) \dots (\pi_1) = (a)$؛ و بنابراین به ازای بعضی از اعداد اول π در K، خواهیم داشت $\pi \mid p$ (ما ادعا نمی‌کنیم که (π) یک ایده‌آل اول است). بنابراین، $PA = (\pi)$. پس π هم در P و هم در A است، زیرا $\pi \mid A$. بنابر قضیهٔ ۳.۹، می‌توان نوشت $(\pi, \gamma) = P$ و $(\pi, \delta) = A$. بنابراین

$$(\pi) = (\pi, \gamma)(\pi, \delta) = (\pi, \gamma\delta)$$

این حقیقت، نتیجه می‌دهد که $\pi \mid \gamma\delta$. با توجه به اصل یگانگی تجزیه، $\pi \mid \gamma$ یا $\pi \mid \delta$.

ما امکان دوم را کنار می‌گذاریم. اگر $\pi \mid \delta$، آنگاه $A = (\pi, \delta) = (\pi)$، $(\pi) = PA = p(\pi)$، و بنابراین $P = (1)$. چنین امکانی غیرممکن است؛ زیرا P اول است. حالت دیگر، این است که $\pi \mid \gamma$ امّا در این صورت $P = (\pi, \gamma) = (\pi)$ و P اصلی است، و این همان چیزی است که می‌خواستیم.

حال، معیاری برای اصلی بودن همهٔ ایده‌آل‌های K، یعنی برای یگانگی تجزیهٔ اعداد صحیح، ارائه می‌دهیم. این معیار، مربوط به دد کیند و هاسه[3] است.

قضیهٔ ۵.۹. *هر ایده‌آل در K اصلی است، اگر و تنها اگر برای هر دو عدد صحیح غیرصفر α و β که $\beta \nmid \alpha$ و $|N\beta| \geq |N\alpha|$، اعداد صحیح γ و δ*

3) *Dedekind and Hasse*

موجود باشند، به‌طوری که

$$0 < |N(\alpha\gamma - \beta\delta)| < |N\beta|$$

ابتدا فرض می‌کنیم که هر ایده‌آل در K اصلی است. فرض می‌کنیم α و β اعداد صحیح از نوع مورد نظر باشند و $A = (\alpha \text{ و } \beta)$. چون A اصلی است، $(\alpha \text{ و } \beta) = (\omega)$؛ پس در A هر عدد صحیح مضربی از ω است. در حالت خاصِ $\beta = \delta\omega$، $N\beta = N\delta N\omega$. β و ω مرتبط نیستند، زیرا درغیر این صورت $\alpha|\beta$، چون می‌دانیم که $\omega|\alpha$. از این رو $|N\delta| > 1$، و بنابراین $|N\beta| > |N\omega|$. امّا ω در $(\alpha \text{ و } \beta)$ است؛ پس $\omega = \alpha\gamma - \beta\delta$ و بنابراین $|N\beta| > |N(\alpha\gamma - \beta\delta)|$. سرانجام اینکه چون $\beta = \delta\omega$، $\omega \neq 0$ و در نتیجه $|N(\omega)| > 0$.

برعکس، فرض می‌کنیم معیار مورد بحث این قضیه صادق باشد و A را ایده‌آل غیرصفری در K درنظر می‌گیریم. طبق قضیهٔ ۳.۹، می‌توان A را به صورت $A = (\alpha, \beta)$ نوشت. ω را عنصر غیرصفری از A در نظر می‌گیریم که برای آن $|N(\omega)|$ کمترین مقدار است. در نتیجه، $A = (\omega)$؛ زیرا اگر γ عدد صحیح دیگری در A است که $\omega \nmid \gamma$، می‌توان یک ترکیب $\mu\gamma - \nu\omega$ را در A یافت، به‌طوری که

$$0 < |N(\mu\gamma - \nu\omega)| < |N\omega|$$

این موضوع با انتخاب ω در تناقض است؛ پس نمی‌توان یک عدد γ را در A چنان یافت که $\omega \nmid \gamma$.

معیاری که هم اکنون ثابت شد، متأسفانه در عمل خیلی مشکل به کار می‌رود. بعضی اوقات می‌توانیم آن را با فرض $\gamma = 1$ به کار بگیریم که در

این حالت هیأت ما *اقلیدسی*[۴] نامیده می‌شود. تعداد هیأت‌های درجهٔ دوم اقلیدسی حقیقی متناهی است (برای مشاهدهٔ بحثی در این مورد و پاره‌ای ملاحظات بعدی، می‌توان به فصل ۱۴ از کتاب هاردی و رایت نگاه کرد). تنها هیأت‌های درجهٔ دوم موهومی $D - R(\sqrt{D})$ خالی از مربع است که اقلیدسی هستند، آنهایی که به ازای آنها D مساوی است با ۱ـ، ۲ـ، ۳ـ، ۷ـ و ۱۱ ـ. به علاوه، مقادیری از D که در حالت تعمیم یافته‌تر معیار ددکیند ــ هاسه صادق هستند، عبارتند از: ۱۹ـ، ۴۳ـ، ۶۷ـ و ۱۶۳ـ. می‌دانیم که حداکثر می‌توان یک هیأت درجهٔ دوم موهومی یافت که همهٔ ایده‌آل‌های آن اصلی باشند؛ و اگر چنین هیأتی موجود است، D مربوط به آن از نظر عددی بزرگتر از ۵ میلیارد است!

به‌طور خلاصه، مسئلهٔ یگانگی تجزیهٔ اعداد صحیح، اکنون به مسئلهٔ ساده‌تری تبدیل گشته؛ و این در حالی است که مسئلهٔ جدید به هیچ وجه کاملاً حل نشده است. با وجود این، چنانکه بعداً خواهیم دید، نظریهٔ ایده‌آل‌ها نتایجی بمراتب مهمتر از قضایای ۴.۹ و ۵.۹ دارد.

۳. **مسئلهٔ انشعاب.** چنانچه بعداً در این فصل خواهیم دید، هر ایده‌آل اول P در یک هیأت اعداد جبری K دقیقاً یک ایده‌آل (P) را عاد می‌کند، P یک عدد اول گویاست. این بدان معنی است که ایده‌آل‌های اول در K را، می‌توان با در نظر گرفتن تجزیهٔ کامل $(P) = P_1 \dots P_r$ از هر ایده‌آل (P) به ایده‌آل‌های اول P_i در K آشکار ساخت. سؤال مهمی که اکنون پیش می‌آید، این است که چه وقت (P) یک عامل P_i تکراری دارد و چه وقت

---

4) *Euclidean*

همهٔ P_iها مجزا هستند؟ (P)، در حالت اول منشعب[5] و در حالت دوّم غیرمنشعب[6] نامیده می‌شود. جواب سؤال مذکور، با استفاده از قضیهٔ ذکرشونده، که از ددکیند است، داده می‌شود. (P) غیرمنشعب است، اگر و تنها اگر $p \nmid d$، که در آن d مبین k است. اثبات کامل این قضیه مشکل است[7]، و ما تنها *این قسمت از قضیه* را ثابت خواهیم کرد که اگر $p \nmid d$، آنگاه (P) توسط مجذور یک ایده‌آل اول عاد نمی‌شود.

فرض می‌کنیم α یک عدد صحیح در K بوده و α_1، ...، α_n مزدوج‌های آن در K هستند. در این صورت، *اثر*[8] α یا $S(\alpha)$ را به صورت

$$S(\alpha) = \alpha_1 + \ldots + \alpha_n$$

تعریف می‌کنیم. چون $S(\alpha)$ ـ ضریب دوم چندجمله‌ای هیأت برای α است، $S(\alpha)$ یک عدد صحیح گویا است. به علاوه، به ازای هر عدد گویای a، $S(a\alpha) = aS(\alpha)$.

حال فرض می‌کنیم که (P) یک عامل مجذور P^2 داشته باشد. ثابت خواهیم کرد که $p \mid d$. فرض می‌کنیم $(p) = P^2Q$. α را چنان انتخاب می‌کنیم که $PQ \mid \alpha$ و $P^2Q \nmid \alpha$. پس $\alpha \neq 0$ و $\alpha \nmid P$. به علاوه، چون $P^2Q \mid P^2Q^2$، و $P^2Q^2 \mid (\alpha^2)$، و $(\alpha^2) = (\alpha)^2$؛ در نتیجه $P \mid \alpha^2$. چون $P \geq 2$، به ازای هر عدد صحیح β موجود در K، $\alpha^2 \mid \alpha^p \beta^p$. از این رو $p \mid \alpha^p \beta^p$، و $\frac{(\alpha\beta)^p}{p}$ یک عدد صحیح در K است. با ملاحظهٔ پاراگراف قبل نتیجه می‌گیریم که

---

5) *ramified* 6) *unramified*

۷) برای مشاهدهٔ اثباتی در این زمینه، به عنوان مثال می‌توان به فصل سوم از کتاب نظریهٔ *اعداد* اثر لانداو (نك: فهرست منابع) مراجعه کرد.

8) *Trace*

$$S\left(\frac{(\alpha\beta)^p}{p}\right) = \frac{S((\alpha\beta)^p)}{p}$$

یک عدد صحیح گویاست، و بنابراین $S((\alpha\beta)^p)$ در (p) قرار دارد. فرض می‌کنیم β_1، ... ، β_n مزدوج‌های β هستند. پس

$$\begin{aligned}(S(\alpha\beta))^p &= (\alpha_1\beta_1 + \alpha_2\beta_2 + \ldots + \alpha_n\beta_n)^p \\ &= (\alpha_1\beta_1)^p + (\alpha_2\beta_2)^p + \ldots + (\alpha_n\beta_n)^p + p\gamma \\ &= S((\alpha\beta)^p) + p\gamma\end{aligned}$$

که در آن γ یک عدد صحیح در K است. از این رو $(S(\alpha\beta))^p$ نیز، به ازای هر عدد صحیح β موجود در K، در (p) قرار دارد. چون $(S(\alpha\beta))^p$ یک عدد صحیح گویاست، $P \mid S(\alpha\beta)$.

حال، فرض می‌کنیم ω_1 و ... و ω_n یک پایهٔ صحیح برای K است. در این صورت $\alpha = \sum_{k=1}^{n} h_k\,\omega_k$، که در آن h_kها اعداد صحیح گویا هستند. چون $p \nmid \alpha$، همهٔ h_kها توسط p عاد نمی‌شوند. امّا

$$S(\alpha\omega_i) = S(\sum_k h_k\,\omega_k\,\omega_i) = \sum_k h_k\,S(\omega_k\,\omega_i)$$

چون $p \mid S(\alpha\omega_i)$، می‌توان نتیجه گرفت که p آخرین مجموع را عاد می‌کند. برای سادگی کار، فرض می‌کنیم $a_{ki} = S(\omega_k\,\omega_i)$ و $\Delta = |a_{ki}|$. حال، نشان خواهیم داد که $p \mid \Delta$.

فرض می‌کنیم A_{ki} همسازه[9] a_{ki} در دترمینان Δ است. در این صورت

$$\sum_i A_{ij} \sum_k a_{ki}\,h_k = \sum_k h_k \sum_i A_{ij}\,a_{ki} = \Delta h_j$$

---

9) *cofactor*

چون p هر یک از مجموع‌های $\sum_k a_{ki} h_k$ را عاد می‌کند، p، Δh_j را برای هر j عاد می‌نماید. امّا همهٔ h_jها توسط p عاد نمی‌شوند؛ از این رو $P \mid \Delta$. حال، تنها تعیین Δ با $[\omega_1, \ldots, \omega_n] = d$ باقی مانده است. مزدوج ω_i را با $\omega_i^{(j)}$ نشان می‌دهیم. با ضرب کردن دترمینان‌ها به شیوهٔ ذکرشونده

$$d = |\omega_j^{(i)}|^2 = \begin{vmatrix} \omega_1^{(1)} & \ldots & \omega_1^{(n)} \\ \ldots & \ldots & \ldots \\ \omega_n^{(1)} & \ldots & \omega_n^{(n)} \end{vmatrix} \cdot \begin{vmatrix} \omega_1^{(1)} & \ldots & \omega_n^{(1)} \\ \ldots & \ldots & \ldots \\ \omega_1^{(n)} & \ldots & \omega_n^{(n)} \end{vmatrix}$$

$$\left| \sum_j \omega_k^{(j)} \omega_{l'}^{(j)} \right| = |S(\omega_k \omega_i)| = \Delta$$

ما نتیجهٔ مطلوب را ثابت کرده‌ایم.

قضیهٔ ۹.۶. *اگر $p \nmid d$، آنگاه (p) غیرمنشعب است.*

نتیجهٔ ۹.۷. *فرض می‌کنیم $K = R(\zeta)$، که در آن ζ یک ریشهٔ Pام ابتدایی واحد و p یک عدد اول گویاست. اگر q یک عدد اول گویای غیر از p است، آنگاه (q) در K غیرمنشعب است.*

چنین مفهومی، نتیجهٔ این حقیقت است که $q \nmid d$؛ زیرا $d = (-1)^{\frac{(p-1)}{2}} p^{p-2}$ (قضیهٔ ۱۳.۶).

۴. همنهشتی‌ها و نورم‌ها. هدف بعدی ما ارائه راهی برای اثبات ادعای مطرح شده در فصل ۷ است که یک ایده‌آل، مجموعهٔ اعداد صحیح موجود در K است که توسط یک عدد صحیح ثابت (نه لزوماً در K) عاد شوند. در این مرحله، یادآوری آنچه در بخش ۲ از فصل ۲ کتاب در خصوص همنهشتی مطرح شده است، برای خواننده سودمند خواهد

بود.

فرض می‌کنیم A یک ایده‌آل است. تعریف می‌کنیم α و β به سنج A همنهشت هستند (می‌نویسیم (سنج A) $\alpha \equiv \beta$ یا $(A)\ \alpha \equiv \beta$)، اگر $\alpha - \beta$ در A باشد، یا به عبارت دیگر اگر $A \mid (\alpha - \beta)$. قواعد عملی کردن، با چنین گزاره‌های همنهشتی، همانهایی هستند که در فصل قبل بیان شدند.

اگر α یک عدد صحیح ثابت در K است، مجموعهٔ همهٔ اعداد صحیح همنهشت با α به سنج A را یک کلاس *باقیمانده*[10] به سنج A می‌نامیم. در این حالت، α یک *نما*[11] یندهٔ کلاس نامیده می‌شود. به عنوان مثال، طبق قضیهٔ ۱۱.۷ هر ایده‌آل در R باید به صورت (m) باشد، ۰، ۱، ... ، $m-1$ نماینده‌های m کلاس باقیمانده به سنج (m) هستند.

قضیهٔ ۸.۹. *اگر $A \neq (0)$ یک ایده‌آل در K است، تعداد کلاس‌های باقیمانده به سنج A متناهی است.*

بنابر قضیهٔ ۱۳.۸، می‌توان یک ایده‌آل B را انتخاب کرد، به‌طوری که داشته باشیم $AB = (a)$ که در آن a یک عدد صحیح گویاست. اگر $\mu \equiv \nu (a)$، آنگاه برای هر A که $A \supset a$، $\mu \neq \nu (A)$؛ چراکه $A \mid a$. امّا چنانکه اثبات لم ۴.۸ نشان می‌دهد، تعداد کلاس‌های باقیمانده در K به سنج (a) متناهی است. چون اینکه $\mu \neq \nu (A)$ نتیجه می‌دهد که (سنج (a)) $\mu \not\equiv \nu$، در نتیجه تعداد کلاس‌های باقیمانده به سنج A متناهی است.

تعداد کلاس‌های باقیمانده به سنج A، نورم A نامیده می‌شود و آن را به صورت NA یا $N(A)$ می‌نویسیم. اگر A اصلی است، مثلاً $A = (\alpha)$، برای نمایش آن می‌نویسیم $N((\alpha))$؛ چراکه نماد $N(\alpha)$ می‌تواند برای نورم

---

10) *residue class* 11) *representative*

یک عدد صحیح α به کار برود، و این دو نورم ممکن است مقادیر یکسانی نداشته باشند. باید توجه داشت که $NA = ۱$، اگر و تنها اگر $A = (۱)$.

خواننده به یاد می‌آورد که هر ایده‌آل غیرصفر، یک پایهٔ صحیح دارد (قضیهٔ ۱۰.۷). حال، کمی فراتر از این موضوع را اثبات می‌کنیم.

لم ۹.۹. *اگر $\omega_۱$، ...، ω_n یک پایهٔ صحیح برای هیأت اعداد جبری K است، آنگاه در آن هر ایده‌آل $A \neq (۰)$، یک پایه $\alpha_۱$، ...، α_n به صورت*

$$\alpha_۱ = a_{۱۱}\,\omega_۱$$
$$\alpha_۲ = a_{۲۱}\,\omega_۱ + a_{۲۲}\,\omega_۲$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\alpha_n = a_{n۱}\,\omega_۱ + \ldots + a_{nn}\,\omega_n \quad \text{و}$$

دارد که در آن a_{ij}ها اعداد صحیح گویا بوده و همهٔ a_{ii}ها مثبت هستند.

فرض می‌کنیم $AB = (a)$، که در آن a یک عدد صحیح گویای غیرصفر است. چون a در A است، $a\omega_۱$، ...، $a\omega_n$ نیز در A هستند. فرض می‌کنیم m ثابت است و $۱ \leq m \leq n$. از همهٔ اعضای A که به صورت $a_۱\omega_۱ + \ldots + a_m\omega_m$ هستند، a_iها عدد صحیح گویا هستند و $a_m > ۰$ است (چون $a\omega_m$ و $a\omega_m$ ـ در A قرار دارند، حداقل یک عضو با این خاصیت موجود است)، آن عضوی را انتخاب می‌کنیم که به صورت

$$\alpha_m = a_{m۱}\,\omega_۱ + \ldots + a_{mm}\,\omega_m$$

بوده و برای آن $a_m = a_{mm}$ کمترین مقدار را داشته باشد. با چنین تعریفی α_i، $i = ۱$، ...، n، خاصیت بیان شده در لم را دارد.

در وهلهٔ اول باید گفت که طبق قضیهٔ ۴.۵، α_i تشکیل یک پایه برای K

می‌دهد؛ چون دترمینان

$$\begin{vmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = a_{11} a_{22} \dots a_{nn}$$

غیرصفر است. نشان خواهیم داد که این α_iها نیز تشکیل یک پایه برای A می‌دهند.

فرض می‌کنیم α یک عدد صحیح در Aاست. چون ω_i تشکیل یک پایه صحیح را برای K می‌دهد، می‌توان نوشت

$$\alpha = b_1 \omega_1 + \dots + b_n \omega_n$$

که در آن b_iها اعداد صحیح گویا هستند. طبق قضیهٔ ۱.۱

$$b_n = h_n a_{nn} + r_n \quad \text{و} \quad 0 \le r_n < a_{nn} \quad \text{و}$$

و بنابراین

$$\alpha - h_n \alpha_n = \alpha - h_n (a_{n1} \omega_1 + \dots + a_{nn} \omega_n)$$
$$= b'_1 \omega_1 + \dots + b'_{n-1} \omega_{n-1} + r_n \omega_n$$

در Aاست. طبق تعریف a_{nn}، باید داشته باشیم $r_n = 0$؛ پس

$$\alpha - h_n \alpha_n = b'_1 \omega_1 + \dots + b'_{n-1} \omega_{n-1}$$

حال این روش را با b'_{n-1} تکرار می‌کنیم تا به دست آوریم

$$\alpha - h_n \alpha_n - h_{n-1} - \alpha_{n-1} = b''_1 \omega_1 + \ldots + b''_{n-2} \omega_{n-2} \quad \text{و}$$

و ادامه می‌دهیم تا

$$\alpha - h_n \alpha_n - \ldots - h_1 \alpha_1 = 0 \quad \text{و}$$

$$\alpha = h_1 \alpha_1 + \ldots + h_n \alpha_n$$

از این رو، α را می‌توان بر حسب α_iها با ضرایب صحیح گویا بیان کرد. این نمایش یگانه است؛ چون α_iها یک پایه برای K هستند.

لم مورد بحث (لم ۹.۹)، ما را قادر می‌سازد تا یک فرمول صریح برای نورم یک ایده‌آل به دست آوریم.

قضیهٔ ۱۰.۹. *اگر A یک ایده‌آل در K و α_1، ...، α_n یک پایه برای A است، آنگاه*

$$NA = \left|\frac{\Delta[\alpha_1, \ldots, \alpha_n]}{d}\right|^{1/2} \quad \text{و}$$

که در آن d مبین K است.

ابتدا توجه می‌کنیم که تمام پایه‌های A مبین یکسانی دارند. این موضوع، نتیجهٔ بحثی است که برای اثبات قضیهٔ ۱۰.۶ به کار بردیم. پس می‌توانیم برای A آن پایه‌ای را انتخاب کنیم که در لم ۹.۹ بیان شد. بنابر فرمول (۵.۱)

$$\Delta[\alpha_1, \ldots, \alpha_n] = \begin{vmatrix} a_{11} & 0 & \ldots & 0 \\ a_{21} & a_{22} & 0 & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}^2 \Delta[\omega_1, \ldots, \omega_n]$$

طبق قضیهٔ ۱۰.۶، $d = \Delta[\omega_1, \ldots, \omega_n]$؛ بنابراین

$$\Delta[\alpha_1, \ldots, \alpha_n] = (a_{11}\, a_{22} \ldots a_{nn})^2\, d$$

بدین ترتیب، فرمول قضیه به $NA = a_{11} \ldots a_{nn}$ تقلیل می‌یابد.

آنچه گفته شد، بدین معناست که تنها لازم است نشان دهیم که ... $a_{11}\, a_{nn}$ تعداد کلاس‌های باقیماندهٔ مجزا به سنج A است:

۱ـ هیچ جفتی از $a_{11} \ldots a_{nn}$ وابسته به اعداد به شکل

$$r_1\, \omega_1 + \ldots + r_n\, \omega_n \qquad \text{و} \qquad 0 \le r_n < a_{nn}$$

به سنج A همنهشت نیست؛

۲ـ هر عدد صحیح در K با یکی از این اعداد به سنج A همنهشت است.

برای اثبات مورد ۱، فرض می‌کنیم

$$r_1\, \omega_1 + \ldots + r_n\, \omega_n \equiv r'_1\, \omega_1 + \ldots + r'_n\, \omega_n \ (A) \qquad \text{و}$$

که در آن $0 \le r_n < a_{nn}$ و $0 \le r'_n < a_{nn}$. می‌توان فرض کرد که $r_n > r'_n$. از این رو

$$(r_1 - r'_1)\, \omega_1 + \ldots + (r_{n-1} - r'_{n-1})\, \omega_{n-1} + (r_n - r'_n)\, \omega_n \equiv 0 \ (A)$$

طبق تعریف a_{nn}، $r_n - r'_n = 0$، $r_n = r'_n$. استدلالی مشابه نشان می‌دهد که $r_i = r'_i$، $i = 1, \ldots, n-1$.

حال، مورد ۲ را ثابت می‌کنیم. هر عدد صحیح α در هیأت مورد بحث ما بصورت

$$\alpha = b_1\, \omega_1 + \ldots + b_n\, \omega_n$$

است، به ازای اعداد صحیح گویای b_i. فرض می‌کنیم

$$b_n = h_n a_{nn} + r_n \qquad \text{و} \quad 0 \le r_n < a_{nn}$$

پس

$$\alpha - h_n a_n = b'_1 \omega_1 + \dots + b'_{n-1} \omega_{n-1} + r_n \omega_n$$

با تکرار این روش با b'_{n-1} و b''_{n-1} و ...، داریم

$$\alpha - h_n a_n - \dots - h_1 \alpha_1 = r_1 \omega_1 + \dots + r_n \omega_n$$

که در آن $0 \le r_m < a_{mm}$. بنابراین $\alpha \equiv r_1 \omega_1 + \dots + r_n \omega_n$ به سنج A.

نتیجهٔ ۱۱.۹. *اگر A اصلی است، $A = (\alpha)$، آنگاه $NA = |N\alpha|$.*

به وضوح مشخص است که $\alpha\omega_1, \dots, \alpha\omega_n$ یک پایه برای A است و

$$\Delta[\alpha\omega_1, \dots, \alpha\omega_n] = (N\alpha)^2 \Delta[\omega_1, \dots, \omega_n] = (N\alpha)^2 d$$

امّا طبق قضیهٔ ۱۰.۹، $\Delta[\alpha\omega_1, \dots, \alpha\omega_n] = (NA)^2 d$، و از این رو $(N\alpha)^2 = (NA)^2$. در این حالت، چون $NA > 0$، نتیجهٔ مورد بحث اثبات می‌شود.

۵. خواص دیگر نورم‌ها. مواردی که ذیل عنوان این بخش ذکر خواهند شد، به عنوان راهنمایی جهت آزمون هر یک از نتایج به دست آمده برای حالت خاص $K = R$ قابل استفاده هستند، و خواننده می‌تواند آنها را با آنچه در فصل ۲ آمد، مقایسه کند.

لم ۱۲.۹. همنهشتی

$$((\alpha), A) = 1 \quad \text{و} \quad \alpha\xi \equiv \beta (A)$$

یک جواب ξ دارد که به سنج A یگانه است.

فرض می‌کنیم ξ_1، ...، ξ_{NA} یک دستگاه کامل‌مانده به سنج A است، یعنی مجموعه‌ای از نماینده‌ها، که هر کدام متعلق به یکی از کلاس‌های باقیمانده است. چون $\alpha \neq 0$، مجموعه $\alpha\xi_1$، ...، $\alpha\xi_{NA}$ نیز یک دستگاه کامل‌مانده است؛ چراکه اگر $\alpha\xi_2 \equiv \alpha\xi_1$، آنگاه $\alpha\,|\,(\xi_1 - \xi_2)$ A. در نتیجه چون $((\alpha), A) = 1$، $(\xi_1 - \xi_2)\,|\,A$، و بنابراین $\xi_2 \equiv \xi_1 (A)$ و $\xi_2 = \xi_1$. پس درمیان $\alpha\xi_i$ها تنها یکی وجود دارد که با β به سنج A همنهشت است.

قضیهٔ ۱۳.۹. همنهشتی

$$\alpha\xi \equiv \beta(A)$$

یک جواب ξ دارد، اگر و تنها اگر $\beta \equiv 0\ (D)$، که $D = ((\alpha), A)$. اگر یک جواب موجود باشد، آن جواب به سنج A/D یگانه است.

اگر ξ یک جواب همنهشتی است، انگاه $\rho\,(= \alpha\xi - \beta)$ در A است، و $\rho\,|\,A$. امّا در این صورت $\rho\,|\,D$ و $\alpha\,|\,D$؛ پس $\beta\,|\,D$ و β در D است.

برعکس، فرض می‌کنیم β در D است. طبق تعریف D، می‌توان $\alpha\xi$ را در (α) و K را در A چنان یافت که $\alpha\xi + K = \beta$ پس $\alpha\xi \equiv \beta(A)$.

اگر $\alpha\xi$ و $\alpha\xi'$ هر دو با β همنهشت باشند، آنگاه $\alpha\,(\xi - \xi') \equiv 0\ (A)$. فرض می‌کنیم $A = DA_1$ و $(\alpha) = DA_2$، که در آن A_1 و A_2 نسبت به هم *اولند*. پس $\xi \equiv \xi'\ (A_1)$، $A_1\,|\,(\xi - \xi')$، $A_1\,|\,A_2(\xi - \xi')$، $DA_1\,|\,DA_2\,(\xi - \xi')$ و بالاخره $\xi \equiv \xi'\ (A/D)$.

قضیهٔ ۱۴.۹. $N(AB) = NA \cdot NB$.

اگر A یا B، (۰) باشند، قضیه بدیهی است. از این رو، فرض کنیم A و B مخالف (۰) هستند. در این صورت، بنابر لم ۲.۹ می‌توان در A، γای را چنان یافت که $((\gamma), AB) = A$ یا $((\gamma)/A, B) = 1$. فرض می‌کنیم $\alpha_1, \ldots, \alpha_{NA}$ و $\beta_1, \ldots, \beta_{NA}$ به ترتیب دستگاههای کامل‌مانده‌ای به سنج A و B هستند. پس هیچ جفت از $NA \cdot NB$ عدد به شکل $\alpha_i + \gamma\beta_j$ نمی‌توانند به سنج AB همنهشت باشند؛ زیرا اگر $\alpha + \gamma\beta \equiv \alpha' + \gamma\beta'(AB)$، آنگاه $\alpha + \gamma\beta \equiv \alpha' + \gamma\beta'(A)$. امّا γ در A است؛ بنابراین $\alpha \equiv \alpha'(A)$. چون α و α' عناصر یک دستگاه کامل‌مانده هستند، $\alpha = \alpha'$. از این رو $\gamma(\beta - \beta') \equiv 0 \ (AB)$. چون $((\gamma), AB) = A$، $(\gamma) = AC$، که $(C, B) = 1$، پس $B \mid (\beta - \beta')$. در نتیجه، $\beta \equiv \beta' \ (B)$ و $\beta = \beta'$.

برای اثبات قضیه تنها باید نشان دهیم که هر عدد صحیح α در هیأت K با یکی از اعداد $\alpha_i + \gamma\beta_j$ به سنج AB همنهشت است. α_i را چنان انتخاب می‌کنیم که $\alpha_i \equiv \alpha \ (A)$. حال همنهشتی $\gamma\xi \equiv \alpha - \alpha_i (AB)$ را در نظر می‌گیریم. طبق قضیهٔ ۱۳.۹، این همنهشتی یک جواب دارد؛ چون $\alpha - \alpha_i$ در $((\gamma), AB) = A$ است. به علاوه ξ را می‌توان به سنج $\frac{AB}{A} = B$ به‌طور یگانه انتخاب کرد؛ پس ξ یکی از β_j هاست. در چنین شرایطی، $\alpha \equiv \alpha_i + \gamma\beta_j (AB)$؛ و حکم ثابت شده است.

نتیجهٔ ۱۵.۹. *اگر NA اول است، A نیز هست.*

قضیهٔ ۱۶.۹. *NA یک عضو A است.*

فرض می‌کنیم $\alpha_1, \ldots, \alpha_{NA}$ و نیز $\alpha_1 + 1, \ldots, \alpha_{NA} + 1$ هر کدام یک دستگاه کامل‌مانده هستند. بنابراین

$$\alpha_1 + \ldots + \alpha_{NA} \equiv (\alpha_1 + 1) + \ldots + (\alpha_{NA} + 1) \ (A)$$ و

$$\circ \equiv NA\ (A)$$

نتیجهٔ ۱۷.۹. *با یک نورم از پیش تعیین شده، تنها تعدادی متناهی از ایده‌آل‌ها وجود دارند.*

زیرا NA تنها می‌تواند در تعدادی متناهی از ایده‌آل‌ها باشد (لم ۴.۸).

قضیهٔ ۱۸.۹ (قضیهٔ فرما) *اگر P یک ایده‌آل اول در K است و $P \nmid \alpha$، آنگاه*

$$\alpha^{NP-1} \equiv 1\ (P)$$

فرض می‌کنیم α_1، ...، α_{NP} یک دستگاه کامل‌مانده به سنج P است، در این صورت، $\alpha\alpha_1$، ...، $\alpha\alpha_{NP}$ نیز یک چنین دستگاهی است. از هر لیست یک عضو، مثلاً α_{NP} و $\alpha\alpha_{NP}$، توسط P عاد می‌شوند. آنها را حذف کرده و اعضای دیگر هر لیست را در یکدیگر ضرب می‌کنیم. به دست می‌آوریم که

$$\alpha_1 \ldots \alpha_{NP-1} \equiv \alpha^{NP-1}\ \alpha_1 \ldots \alpha_{NP-1}\ (P)$$

چرا که $P \nmid \alpha_1 \ldots \alpha_{NP-1}$ و $1 \equiv \alpha^{NP-1}\ (P)$.

با ارائه یک اثبات از قضیه‌ای که در شروع بخش ۳ ذکر شد، این فصل را خاتمه می‌دهیم.

قضیهٔ ۱۹.۹. *اگر P اول است، دقیقاً یک عدد اول گویای مثبت p را عاد می‌کند. پس $NP = p^f$، که $1 \leq f \leq n$ و n مرتبهٔ K روی R است.*

طبق قضیهٔ ۱۳.۸، به ازای بعضی از اعداد صحیح گویای a، $P \mid a$. اگر $a = p_1 p_n \ldots$ تجزیهٔ a به اعداد اول گویا باشد، آنگاه $(a) = (p_1) \ldots (p_n)$. از این رو، برای بعضی از مقادیر i، $P \mid (p_i)$. فرض می‌کنیم $p = |p_i|$. در

نتیجه $P|p$.

اگر $P|p$، $P|q$ که p و q اعداد اول مجزا هستند، آنگاه می‌توان اعداد صحیح گویای m و n را چنان یافت که $mp + nq = ۱$. پس $P|۱$ و $P \supset (۱)$، با این حقیقت که P اول است در تناقض است.

سرانجام اینکه طبق نتیجهٔ ۱۱.۹، $N((p)) = |Np| = p^n$. چون $P|p$، $NP|N((p))$؛ پس $NP = p^f (۱ \leq f \leq n)$.

فصل ۱۰

اعداد رده‌ای و مسئلهٔ فرما

۱. **اعداد رده‌ای.** اکنون تقریباً آماده‌ایم به وعدهٔ خود در مورد ارائه اثباتی برای این موضوع که هر ایده‌آل مجموعه‌ای از اعداد صحیح در $K = R(\theta)$ است که (در حالت بسط یافته) توسط بعضی اعداد صحیح، نه لزوماً موجود، در K عاد می‌شوند، وفا کنیم. اثباتمان، موکول به شناخت عدد رده‌ای خواهد بود.

به منظور اجتناب از ایجاد وقفه در بحث، قضیه‌ای که در فصل بعد اثبات شده را در این‌جا می‌آوریم. اثبات این قضیه، بر اساس ایدهٔ جدیدی است که ترجیح دادیم معرفی آن را به بعد موکول کنیم.

قضیهٔ ۱.۱۰. *اگر K یک هیأت غیر از R و A یک ایده‌آل غیرصفر در K است، یک عدد $\alpha \neq 0$ در A وجود دارد، به‌طوری که*

$$|N\alpha| < N(A)\sqrt{|d|}$$

دو ایده‌آل A و B در K هم‌ارزند، می‌نویسیم $A \sim B$، اگر دو عدد صحیح

غیرصفر α و β در K موجود باشند، به‌طوری که

$$(\alpha)\ A = (\beta)\ B$$

ساده‌ترین خواص رابطه هم‌ارزی به صورت زیر است:

۱ـ $A \sim A$؛

۲ـ $A \sim B$، اگر و تنها اگر $B \sim A$؛

۳ـ اگر $A \sim B$ و $B \sim C$، آنگاه $A \sim C$؛

۴ـ همهٔ ایده‌آل‌های اصلی هم‌ارزند و همهٔ ایده‌آل‌های هم‌ارز با یک ایده‌آل اصلی، اصلی هستند.

مجموعهٔ ایده‌آل‌هایی از K که با یک ایده‌آل ثابت $A \neq (0)$ هم‌ارز هستند، تشکیل یک کلاس را می‌دهند. تعداد این کلاس‌ها (که بزودی نشان می‌دهیم متناهی است) عدد رده‌ای h[1] از هیأت K نامیده می‌شود. اگر عدد رده‌ای ۱ است، آنگاه تمام ایده‌آل‌ها با (۱) هم‌ارز هستند و بنابراین همه اصلی هستند. از قضیهٔ ۴.۹، نتیجه می‌شود که یک هیأت، تجزیهٔ یگانه‌ای از اعداد صحیح به اعداد صحیح اول دارد، اگر و تنها اگر عدد رده‌ای آن ۱ باشد.

قضیهٔ ۲.۱۰. *عدد رده‌ای h یک هیأت متناهی است.*

اگر هیأت R است، $h = 1$ و چیزی برای اثبات باقی نمی‌ماند. اگر K غیر از R است، کافی است نشان دهیم که در هر کلاس از ایده‌آل‌ها یک ایده‌آل B وجود دارد، به‌طوری که $NB < \sqrt{|d|}$، زیرا در این صورت (NB)[2] مساوی است با ۱، ۲، ... یا $|d| - 1$، و طبق نتیجهٔ ۱۷.۹ تنها تعداد

---

1) *class-number h*

متناهی از ایده‌آل‌ها با نورم داده شده وجود دارند.

فرض می‌کنیم کلاسی داده شده و C ایده‌آلی در آن است. A را چنان انتخاب می‌کنیم که AC اصلی باشد، پس $AC \sim$ (۱). بنابر قضیهٔ قبل، می‌توان یک عدد α ($\alpha \neq$ ۰) را در A چنان یافت که $|N\alpha| < N(A)\sqrt{|d|}$ چون $\alpha \mid A$، برای ایده‌آلی مثل B، $(\alpha) = AB$ و همچنین $NA \cdot NB = |N\alpha| = N((\alpha))$؛ بنابراین $NA \cdot NB < N(A)\sqrt{|d|}$ و $NB\sqrt{|d|}$. اکنون، تنها این موضوع باقی مانده است که نشان دهیم $B \sim C$. امّا $AB \sim$ (۱) و $AC \sim$ (۱)؛ بنابراین، $AB \sim AC$، و نتیجه مطلوب به دست می‌آید.

نتیجهٔ ۳.۱۰. *اگر A یک ایده‌آل در K، و h عدد رده‌ای K است، آنگاه A^h اصلی است.*

اگر $A =$ (۰)، $A^h =$ (۰)، نتیجه بدیهی است. فرض می‌کنیم که $A \neq$ (۰). مجموعه‌ای از ایده‌آل‌های A_1، ...، A_h، یکی از هر کلاس موجود در K، را انتخاب می‌کنیم. در این صورت، AA_1، ...، AA_h در کلاس‌های مجزایی قرار می‌گیرند؛ زیرا اگر $AA_j \sim AA_i$، آنگاه $A_i \sim A_j$. از این رو

$$A_1 \dots A_h \sim AA_1 \cdot AA_2 \dots AA_h = A^h A_1 \dots A_h \quad \text{و}$$

و بنابراین $A^h \sim$ (۱)، و A^h اصلی است.

نتیجهٔ ۴.۱۰. *اگر p یک عدد اول گویا است، $p \nmid h$، و داشته باشیم که $A^p \sim B^p$، آنگاه $A \sim B$.*

داریم $(\alpha)\ A^p \sim (\beta)\ B^p$. چون p و h نسبت به هم اولند، می‌توان اعداد صحیح گویای مثبت r و s را چنان یافت که $pr - hs =$ ۱.

پس

$$(\alpha)^r A^{pr} = (\beta)^r B^{pr}$$
$$(\alpha)^r AA^{hs} = (\beta)^r BB^{hs}$$

امّا A^h و B^h اصلی هستند، و از این رو $(\alpha)^r A^{hs}$ و $(\beta)^r B^{hs}$ نیز اصلی هستند.

حال نشان می‌دهیم که هر ایده‌آل در K، مجموعهٔ اعداد صحیح α موجود در K است که توسط یک عدد صحیح k، که لزوماً در K نیست، عاد می‌شود. نباید فرض کرد که k، حتی بدون درنظر گرفتن یکه‌ها، یگانه است. برای مثال، $A = (۲)$ را در R، هیأت اعداد گویا درنظر می‌گیریم. پس A شامل همهٔ اعداد صحیح گویای زوج است، یعنی مجموعهٔ اعداد صحیح موجود در R که توسط ۲ عاد می‌شوند. امّا A همچنین مجموعهٔ اعداد صحیح موجود در R که توسط $\sqrt{۲}$ (در حالت گسترش یافتهٔ عاد کردن) عاد می‌شوند نیز هست؛ زیرا $\frac{n}{\sqrt{۲}}$ یک عدد صحیح جبری است، اگر n زوج باشد، و نه فرد. ولی در این وضعیت، یک حالت یگانگی وجود دارد؛ بدین معنی که در میان همهٔ آن k ها که خاصیت مطلوب را دارند، یکی از آنها توسط بقیه عاد می‌شود، و این یکی بدون در نظر گرفتن یکه‌ها یگانه است. در این حالت خاص که در نظر گرفتیم، عدد صحیح ۲ همان عدد منحصر به فرد است که شامل همهٔ k های دیگر به عنوان عامل است، البته عدد ۲، نیز به همین اندازه سودمند است.

قضیهٔ ۵.۱۰. *برای هر ایده‌آل A در K یک عدد صحیح k، که لزوماً در K نیست، وجود دارد، به‌طوری که*

۱ـ *A مجموعهٔ اعداد صحیح δ موجود در K است که به ازای آنها δ/k*

صحیح است.

۲ـ هر عدد صحیح k' که خاصیت ۱ را داشته باشد، k را عاد می‌کند.

k بدون در نظر گرفتن یکه‌ها یگانه است.

فرض می‌کنیم $A = (\alpha \text{ و } \beta)$. پس بنابر نتیجهٔ ۳.۱۰، $(\alpha \text{ و } \beta)^h = (\omega)$ اصلی است. $k = \omega^{1/h}$ یک عدد صحیح است، چون در معادلهٔ $x^h - \omega = 0$ صدق می‌کند. بسط $E = K(k)$ از K را در نظر می‌گیریم. E شامل K و از این رو همهٔ عناصر A است. حال در K

$$A^h = (\alpha, \beta)^h = (\omega)$$

بنابر قضیهٔ ۱.۸، این ایده‌آل‌ها وقتی به عنوان ایده‌آل‌هایی در هر بسط متناهی K در نظر گرفته شوند مساوی هستند. پس در E، $(\omega) = (k)^h = (\alpha, \beta)^h$. با در نظر گرفتن قضیهٔ یگانگی تجزیه برای ایده‌آل‌ها در E، $(k) = (\alpha, \beta)$. از این رو، هر عضو A توسط k عاد می‌شود. به علاوه

$$k = \lambda\alpha + \upsilon\beta \quad \text{و} \qquad (۱۰.۱)$$

که λ و υ در E هستند.

حال، برعکس، باید نشان دهیم که هر عضو γ در K که توسط k عاد شود، در A است. چون γ و k هر دو در E هستند و $k \mid \gamma$، در نتیجه γ در $(k) = (\alpha, \beta)$ است، که (α, β) به عنوان ایده‌آلی در E درنظر گرفته شده است. می‌خواهیم نشان دهیم که γ در (α, β) است، وقتی (α, β) به عنوان ایده‌آلی در K درنظر گرفته شود، این موضوع هنوز روشن نیست؛ امّا $\gamma = \lambda k$، که λ عدد صحیحی در E است. فرض می‌کنیم k از مرتبهٔ k روی K است، پس $E = K(k)$ و $(E/K) = k$. فرض می‌کنیم k_1، ...،

k_k مزدوج‌های k و λ_1 و ... و λ_k مزدوج‌های λ در E هستند. چون γ در K است، بنابراین همهٔ مزدوج‌های آن نیز چنین هستند. از این رو

$$\gamma = \lambda_i k_i\,,\ i = 1\,,\ \ldots\,,\ k\,,\ \gamma^k = (\lambda_1 \ldots \lambda_k)\ (k_1 \ldots k_k)$$

حاصل‌ضرب $\xi = \lambda_1 \ldots \lambda_k$ بر حسب λ_iها متقارن بوده و بنابراین عدد صحیحی در Kاست. چون kدر $\omega = 0$ ـ x^hصدق می‌کند، هر یک از اعداد k_1، ...، k_k نیز در این رابطه صدق می‌کنند. پس

$$k_i^h = \omega\,,(k_1 \ldots k_k)^h = \omega^k \quad \text{و} \quad \gamma^{hk} = \xi^h\,\omega^k\,;$$

از این رو، بنابر قضیهٔ اساسی نظریهٔ ایده‌آل، به عنوان ایده‌آل‌هایی در K، داریم

$$(\gamma)^{hk} = (\xi)^h\,(\omega)^k = (\xi)^h\,A^{hk} \quad \text{و}$$
$$(\gamma)^k = (\xi)\,A^k \quad \text{و} \quad A^k \mid (\gamma)^k$$

با استفاده از کاربرد دیگر قضیهٔ اساسی، نتیجه می‌شود که $A \mid \gamma$، و بنابراین γدر A است. این معنی، قسمت ۱ قضیه را ثابت می‌کند. و قسمت ۲ نیز از رابطهٔ (۱۰.۱) نتیجه می‌شود.

برای اثبات یگانگی k، فرض می‌کنیم k_1و k_2هر دو خاصیتهای ۱ و ۲ را داشته باشند. پس $k_1 \mid k_2$ و $k_2 \mid k_1$، و بنابراین $k_2 = \delta k_1$، که δ یک یکه است.

۲. حدس فرما. ممکن است که خواننده با مسئلهٔ حل نشدهٔ مشهور زیر آشنا باشد: به ازای کدام مقادیر صحیح مثبت n معادلهٔ

$$x^n + y^n = Z^n \qquad (۱۰.۲)$$

در مجموعه اعداد صحیح گویا جواب دارد؟ برای $n = ۲$، جوابهایی وجود دارند، به عنوان مثال، $۵^۲ = ۴^۲ + ۳^۲$. اثبات این موضوع ساده است که برای $n = ۴$، ممکن نیست جوابی وجود داشته باشد. اثبات مذکور، تنها به خواص سادهٔ اعداد صحیح بستگی دارد و می‌توان آن را تقریباً در هر کتاب نظریهٔ اعداد مقدماتی پیدا کرد. در سال ۱۶۳۷ فرما ادعا کرد که اگر $n > ۲$، هرگز هیچ جوابی برای معادلهٔ (۱۰.۲) موجود نیست (قضیهٔ «آخر» فرما)، امّا هرگز برای این ادعا اثباتی پیدا نشده و تنها حالت یک حدس را دارد. در واقع، بخش بزرگی از نظریهٔ اعداد جبری از تلاش برای اثبات ادعای مزبور به وجود آمده است.

قبل از بحث بیشتر دربارهٔ حدس فرما، گزارهٔ آن را تا اندازه‌ای ساده می‌کنیم. چون هیچ جوابی به ازای $n = ۴$ وجود ندارد، وقتی $n = ۴m$ است نیز ممکن نیست جوابی وجود داشته باشد؛ زیرا معادلهٔ (۱۰.۲) را می‌توان به صورت $(x^n)^۴ + (y^n)^۴ = (Z^n)^۴$ نوشت. هر عدد صحیح $n \neq ۴m$ ، $n > ۲$، را می‌توان به صورت $n = pr$ نوشت که در آن p یک عدد اول فرد است. از این رو، کافی است نشان دهیم که وقتی یک عدد اول فرد است، معادلهٔ (۱۰.۲) هیچ جوابی نخواهد داشت؛ زیرا می‌توان نوشت $(x^r)^p + (y^r)^p = (Z^r)^p$. بالاخره، فرض می‌کنیم $n=p$ و Z را با Z- جایگزین می‌نماییم. چون p فرد است، رابطهٔ (۱۰.۲) به این شکل درمی‌آید که

$$x^p + y^p + Z^p = ۰ \qquad (۱۰.۳)$$

در نتیجه حدس فرما به این صورت خواهد شد : به ازای هیچ عدد

اول فرد p، معادلهٔ (۱۰.۳) جوابی در مجموعهٔ اعداد صحیح گویا ندارد.

بهتر است اعداد اول pرا به صورت ذکرشونده دسته‌بندی کنیم. فرض می‌کنیم h عدد رده‌ای $K(\xi)$ است، که در آن ξ یک pامین ریشهٔ ابتدایی واحد است. اگر $p \nmid h$، pمنظم[2] است، و در غیر این صورت p غیرمنظم[3] است. کومر[4] ثابت کرد که اگر pمنظم است، آنگاه (۱۰.۳) هیچ جوابی در اعداد صحیح گویا ندارد. متأسفانه تعداد اعداد اول غیرمنظم نامتناهی بوده و به ازای آنها وضعیت معادلهٔ (۱۰.۳) تا امروز نامعین است. ما ارتباط حدس فرما را با نظریهٔ اعداد جبری به وسیلهٔ اثبات صورت ضعیفی از قضیهٔ کومر توضیح خواهیم داد. خواننده‌ای که علاقه‌مند به دانستن بیشتر در این خصوص است، باید به جلد ۳ از کتاب *نظریهٔ اعداد* نوشتهٔ لانداو یا مقالهٔ توضیحی واندیور[5]، مذکور در فهرست منابع، مراجعه کند.

حال، به اثبات چند لم می‌پردازیم. ξ همان معنای معمول، یعنی یک p امین ریشهٔ ابتدایی واحد، را خواهد داشت، $p \neq ۲$. $K = R(\xi)$، از درجهٔ $p - ۱$ روی R است. برای جلوگیری از اشتباهات احتمالی، ایده‌آل‌ها به جای پرانتز داخل براکت نوشته خواهند شد. مانند گذشته، λ همان $\xi - ۱$ خواهد بود. همچنین، L ایده‌آل $[\lambda]$ است.

لم ۱۰.۶. $L^{p-۱} = [p]$ و $NL = p$.

چنانکه در فصل ۶ ثابت شد.

$$p = (۱ - \xi)(۱ - \xi^{۲}) \dots (۱ - \xi^{p-۱}) ,$$

---

2) *regular* 3) *irregular*

4) Kummer 5) Vandiver

و بنابراین

$$[p] = [1 - \xi][1 - \xi^2] \dots [1 - \xi^{p-1}]$$

واضح است که برای $0 < j$، $(1 - \xi^j) | (1 - \xi)$. حال، t را چنان انتخاب می‌کنیم که (سنج p) $jt \equiv 1$. پس

$$1 - \xi = 1 - \xi^{jt} = (1 - \xi^j)(1 + \xi^j + \dots)$$ و

بنابراین $(1 - \xi) | (1 - \xi^j)$. از این رو، $1 - \xi$ و $1 - \xi^j$ مرتبط هستند، و در نتیجه $[1 - \xi^j] = [1 - \xi]$. پس

$$[p] = [1 - \xi]^{p-1} = L^{p-1}$$

چون $(K/R) = p - 1$، $N[p] = |NP| = p^{p-1}$. پس $(NL)^{p-1} = p^{p-1}$ و $NL = p$. طبق نتیجهٔ ۱۵.۹، L یک ایده‌آل اول است.

لم ۷.۱۰. اگر q عدد اول غیر از p و بزرگتر از ۲ است، اعداد i و $e^{2\pi i/q}$ هیچ یک در K نیستند. فرض می‌کنیم i در K است. چون i یکه است، $[1 + i] = [1 - i]$. پس

$$[2] = [1 + i][1 - i] = [1 + i]^2$$

که چون $p \neq 2$، این امر با نتیجهٔ ۷.۹ در تناقض است.

اگر $e^{2\pi i/q}$ در K است، آنگاه طبق بحثی مشابه با روشی که برای اثبات لم ۶.۱۰ به کار رفت

$$[q] = [1 - e^{2\pi i/q}]^{q-1}$$

چون $q > ۲$، $[q]$ منشعب است، که این موضوع نیز با نتیجهٔ ۷.۹ در تناقض است.

یک ریشهٔ واحد α، عددی است که به ازای آن و به ازای بعضی اعداد صحیح مثبت m، $\alpha^m = ۱$. مشخصاً α به صورت $e^{۲\pi it/m}$ است، که t یک عدد صحیح گویا است.

لم ۸.۱۰. *تنها ریشه‌های واحد در* K، $\pm\xi^s$ *هستند* $(۰ < S \le p)$.

فرض می‌کنیم $\alpha = e^{۲\pi it/m}$ در K است. می‌توان فرض کرد که $m > ۰$ و $(m, t) = ۱$. این لم، ادعا می‌کند که $m \mid ۲p$. اگر $m \nmid ۲p$ آنگاه یکی از سه حالت باید درست باشد،

$$p^۲ \mid m \quad , \quad q \mid m \quad \text{یا} \quad ۴ \mid m \ ,$$

q یک عدد اول فرد غیر از p است.

چون $(m, t) = ۱$، می‌توان r را چنان یافت که $t r \equiv ۱ \pmod{m}$ و $t r = ۱ + km$. پس

$$\alpha^r = e^{۲\pi itr/m} = e^{۲\pi i(k+۱/m)} = e^{۲\pi i/m}$$

در K است.

اگر $۴ \mid m$، آنگاه $e^{۲\pi i/۴} = i$ در K است، که این معنی با لم ۷.۱۰ در تناقض است. اگر $q \mid m$، آنگاه $e^{۲\pi i/q}$ در K است، که این موضوع نیز با لم ۷.۱۰ در تناقض است.

اگر $p^۲ \mid m$، آنگاه $\tau = e^{۲\pi i/p^۲}$ در K است. ما نشان خواهیم داد که چنین چیزی غیرممکن است.

τ در معادلهٔ $x^{p^۲} - ۱ = ۰$ صدق می‌کند، امّا به ازای آن رابطهٔ $x^p - ۱ = ۰$

برقرار نیست. از این رو، τ یک ریشهٔ عبارت زیر است

$$\frac{x^{p^2}-1}{x^p-1} = x^{p(p-1)} + x^{p(p-2)} + \ldots + 1$$

بنابر قضیهٔ ۹.۳، τ روی R از مرتبهٔ $p(p-1) > (p-1)$ است، و به همین جهت (نتیجهٔ ۸.۵) نمی‌تواند در K باشد، که روی R از مرتبهٔ $p-1$ است.

لم ۹.۱۰. *برای هر عدد صحیح α موجود در K، یک عدد صحیح گویا a وجود دارد، به‌طوری که*

$$\alpha^p \equiv a \ (L^p \text{ سنج})$$

چون $NL = p$، تعداد p کلاس باقیماندهٔ غیرهمنهشت به سنج L وجود دارد و چنانکه قبلاً دیدیم؛ ۰، ۱، ...، $p-1$ تشکیل یک دستگاه کامل‌مانده به سنج L را می‌دهند. از این رو، به ازای یک عدد صحیح گویای مناسب b، $\alpha \equiv b \ (L)$. حال

$$\alpha^p - b^p = \prod_{m=0}^{p-1} (\alpha - \zeta^m b)$$

چون $\zeta - 1 = \lambda$، $\zeta \equiv 1 \ (L)$، و برای هر یک از p عامل ذکرشده در طرف راست رابطه فوق را می‌توان نوشت

$$\alpha - \zeta^m b = \alpha - b \equiv 0 \ (L)$$

از این رو، $\alpha^p - b^p \equiv 0 \ (L^p)$.

لم ۱۰.۱۰. *اگر همهٔ ضرایب یک چندجمله‌ای تکین اعداد صحیح گویا بوده و همهٔ ریشه‌ها دارای قدر مطلق ۱ باشند، آنگاه این ریشه‌ها،*

ریشه‌های واحد هستند.

فرض می‌کنیم ω_1، ...، ω_k این ریشه‌ها هستند. طبق قضیهٔ توابع متقارن، چندجمله‌ای

$$p_l(x) = (x - \omega_1^l) \dots (x - \omega_2^l)(x - \omega_k^e)$$

برای هر عدد صحیح گویای ثابت $l > 0$، یک چندجمله‌ای تکین با ضرایب صحیح گویاست. فرض می‌کنیم چنین چندجمله‌ای‌هایی با رابطهٔ

$$p_l(x) = x^k + a_{l,k-1}x^{k-1} + \dots + a_{l,0} \quad \text{و} \quad l = 1, 2, \dots$$

نشان داده شوند. هر a_{ij} یک تابع متقارن ابتدایی بر حسب ریشه‌های ω_1، ...، ω_k است؛ چراکه آن ریشه‌ها دارای قدر مطلق ۱ هستند

$$|a_{lt}| \leq (t^k)$$

حال، با توجه به اینکه (t^k) مستقل از l است، پس تنها تعدادی متناهی از چندجمله‌ای‌های متفاوت $p_l(x)$ ممکن است وجود داشته باشد. پس ω_i^l باید برای دو مقدار متفاوت l، مثلاً l_1 و l_2 یکی باشد، که $l_1 > l_2$. پس $\omega_i^{l_2} = \omega_i^{l_1}$ و $\omega_i^{l_1 - l_2} = 1$، و بنابراین، ω_i یک ریشهٔ واحد است.

لم ۱۱.۱۰. *فرض می‌کنیم ε یک یکه در $R(\zeta)$ است. در این حالت $\varepsilon = \zeta^g r$، که در آن g یک عدد صحیح مثبت و r یک عدد حقیقی است.*

چون ۱، ζ، ...، ζ^{p-2} یک پایهٔ صحیح است، $\varepsilon = r(\zeta)$، که $r(\zeta)$ یک چندجمله‌ای بر حسب ζ با ضرایب عدد صحیح گویاست. به ازای عدد s، که $S = 1, \dots, p-1$، عدد $\varepsilon_s = r(\zeta^s)$ با ε مزدوج است. چون $\varepsilon_{p-1} = \pm 1$، $N_\varepsilon = \varepsilon_1 \dots$، $|\varepsilon_s| = 1$، و بنابراین هر ε_s یک یکه است. به علاوه

$$\varepsilon_{p-s} = r(\zeta^{p-s}) = r(\zeta^{-s}) = r(\zeta^{s-}) \quad ,$$

که در آن علامت بار، نشاندهندهٔ مزدوج ـ مختلط بودن است. از این رو $\varepsilon_{p-s} = \overline{\varepsilon_s}$، $\varepsilon_{p-s}\varepsilon_s = |\varepsilon_s|^2 > 0$. از آنجاکه $p-1$ تا ε_s وجود دارند، با ضرب کردن دو به دوی آنها به دست می‌آوریم که $N_\varepsilon = \Pi \varepsilon_s \varepsilon_{p-s} > 0$، و بنابراین $N_\varepsilon = 1$.

اعداد $\varepsilon_s/\varepsilon_{p-s}$، $p-1$، ...، $S = 1$، یکه‌هایی با قدر مطلق ۱ هستند. با توجه به بحث معمول در خصوص توابع متقارن، چندجمله‌ای

$$\prod_{s=1}^{p-1} (x - \frac{\varepsilon_s}{\varepsilon_{p-s}}) = \prod_{s=1}^{p-1} (\varepsilon_{p-s}\, x - \varepsilon_s)$$

ضرایب صحیح گویا دارد. از لم ۱۰.۱۰ نتیجه می‌گیریم که $\varepsilon_s/\varepsilon_{p-s}$ یک ریشهٔ واحد است. در حالت خاص، اگر s را ۱ بگیریم، $\varepsilon/\varepsilon_{p-1}$ یک ریشهٔ واحد است؛ که در این حالت طبق لم ۸.۱۰، $\varepsilon/\varepsilon_{p-1} = \pm\zeta^t = \pm\zeta^{t+p}$. چون p فرد است، یکی از دو عدد t یا $t+p$ باید زوج باشد؛ بنابراین $\varepsilon/\varepsilon_{p-1} = \pm\zeta^{2g}$، که g یک عدد صحیح گویای مثبت است.

اعداد ۰، ۱، ...، $p-1$ به سنج L تشکیل یک دستگاه کامل‌مانده را می‌دهد. از این رو، به ازای یکی از آنها چون v

$$\zeta^{-g}\varepsilon \equiv v \ (L) \qquad (۱۰.۴)$$

امّا $L = |\lambda|$؛ بنابراین μ که مساوی است با $\frac{\zeta^{-g}\varepsilon - v}{\lambda}$ یک عدد صحیح در K است. مزدوج ـ مختلط این عدد یعنی $\bar{\mu}$ نیز یک عدد صحیح در K است؛ زیرا هر دو در یک چندجمله‌ای مینیمال یکسان صدق می‌کنند. پس $\bar{\mu}$ که

$$\bar{\mu} = \frac{\bar{\zeta}^{-g}\bar{\varepsilon} - v}{\bar{\lambda}} = \frac{\zeta^{g}\varepsilon_{p-1} - v}{\bar{\lambda}}$$

یک عدد صحیح است. امّا $\zeta^{p-1} - 1 = \lambda\bar{\lambda}$ با λ مرتبط است (رجوع شود به اثبات لم ۶.۱۰). از این رو، $\frac{\zeta^g \varepsilon_{p-1} - v}{\lambda}$ نیز یک عدد صحیح است. پس بنابر رابطهٔ (۱۰.۴)

$$\zeta^g \varepsilon_{p-1} \equiv v \equiv \zeta^{-g} \varepsilon \ (L)$$

این حقیقت، نشان می‌دهد که $\frac{\varepsilon}{\varepsilon_{p-1}} \equiv \zeta^{2g} \ (L)$.

حال می‌توان تصمیم گرفت که به ازای کدام علامت $\frac{\varepsilon}{\varepsilon_{p-1}} = \pm\zeta^{2g}$، که پیشتر بدان رسیدیم، درست است. اگر علامت $-$ را نگه داریم، آنگاه $\varepsilon\zeta^{2g} \equiv \zeta^{-g} \ (L)$، بنابراین $2g \mid L$ و $2g \mid p-1$، که این نتیجه با لم ۶.۱۰ در تناقض است. این امر، بدان معناست که $\varepsilon_{p-1}\zeta^{2g} = \varepsilon$ و $\zeta^g = \varepsilon_{p-1}\varepsilon^{-g}$. چون سمت راست و سمت چپ معادلهٔ پیشگفتهٔ مزدوج‌ـ مختلط و برابر هستند، باید حقیقی باشند. بدین طریق، لم ثابت شده است.

حال در موقعیتی هستیم که شکل ساده شدهٔ قضیهٔ کومر را ثابت کنیم:

قضیهٔ ۱۲.۱۰. *اگر p یک عدد اول فرد منظم است، آنگاه*

$$x^p + y^p + z^p = 0 \qquad (10.5)$$

هیچ جوابی در اعداد صحیح گویا ندارد که در آن

$$p \nmid x \quad , \quad p \nmid y \quad , \quad p \nmid z$$

فرض می‌کنیم که معادلهٔ فوق به ازای یک عدد p که هیچ یک از اعداد x و y و z را عاد نمی‌کند جوابی داشته باشد، به یک تناقض خواهیم رسید. اگر x و y یک عامل مشترک داشته باشند، آن عامل z را نیز عاد می‌کند، و می‌توان آن را با تقسیم کردن خارج کرد. چنین حقیقتی، این

فرض را که x و y و z عامل مشترکی ندارند، تصدیق می‌کند. از رابطهٔ (۱۰.۵) به دست می‌آوریم

$$\prod_{m=0}^{p-1} (x + \zeta^m y) = -Z^p \quad , \qquad (۱۰.۶)$$

و بنابراین

$$\prod_{m=0}^{p-1} [x + \zeta^m y] = [Z]^p \qquad (۱۰.۷)$$

(باید توجه داشت که تغییر در علامات، دلالت بر انتقال از اعداد به ایده‌آل‌ها دارد.)

هر دو ایده‌آل موجود در سمت چپ رابطهٔ (۱۰.۷) نسبت به هم اولند. برای اثبات این مطلب، فرض می‌کنیم P یک عامل مشترک دو ایده‌آل $[x + \zeta^k y]$ و $[x + \zeta^l y]$ است که $0 \le k \le l \le p-1$. پس P شامل هر دو عنصر $y\zeta^k + x$ و $y\zeta^l + x$ است و از این رو شامل تفاضل آنها یعنی $y\zeta^k(\zeta^{l-k} - 1)$ نیز هست. چون $\zeta^{l-k} - 1$ با $\lambda = \zeta - 1$ مرتبط بوده و ζ^k یکه است، P شامل عدد $y\lambda$ است. به همین جهت، P شامل y یا λ است؛ در واقع $P | y$ یا $P | \lambda$. به علاوه، طبق رابطهٔ (۱۰.۷) $P | Z$؛ پس P شامل z و بنابراین شامل $z^p = x^p + y^p$ است. حال دو امکان وجود دارد. ۱) اگر P شامل y است، شامل $x^p = z^p - y^p$ نیز خواهد بود؛ بنابراین $P | x$، $P | y$، که این معنی با اول بودن x و y نسبت به هم در تناقض است. ۲) اگر $P | \lambda$، آنگاه $P | L$. امّا L اول است، و بنابراین $P = L$. در نتیجه، L شامل Z است، $L | Z$، $NL | NZ$، $p | Z^{p-1}$، و $p | Z$ (در تناقض با این فرض که $P \nmid L$). این مطلب، ادعای مطرح شده در ابتدای پاراگراف را ثابت می‌کند.

حال به رابطهٔ (۱۰.۷) توجه می‌کنیم. چون عامل‌های سمت چپ نسبت به هم اولند، از قضیهٔ اساسی نظریهٔ ایده‌آل نتیجه می‌شود که هر یک از آنها باید توان pام یک ایده‌آل باشند. در حالت خاص، $[x + \zeta y] = A^p$ پس A^p اصلی است، (۱) $\sim A^p$ و، طبق نتیجهٔ ۴.۱۰، (۱) $\sim A$. از این رو، A خود یک ایده‌آل اصلی (δ) است و $[x + \zeta y] = [\delta]^p = [\delta^p]$. این معنی، نشان می‌دهد $x + \zeta y = \varepsilon\delta^p$، که در آن ε یک یکه است.

این مرحله‌ای است که در آن، تصمیمی درست گرفته‌ایم. امّا آیا نمی‌توان نتیجهٔ مشابهی را مستقیماً بر اساس رابطهٔ (۱۰.۶) و بدون توجه به‌نظریهٔ ایده‌آل‌ها استنباط کرد؟ جواب این است که تنها در حالتی که هیأت $R(\zeta)$ عدد رده‌ای ۱ را داشته باشد، یعنی وقتی تجزیهٔ اعداد صحیح به اعداد اول یگانه باشد، می‌توان بدون استفاده از نظریهٔ ایده‌آل‌ها مستقیماً به نتیجه رسید. متأسفانه، هیأت‌های تقسیم دایره با عدد رده‌ای بزرگتر از ۱ وجود دارد.

چون $x + \zeta y = \varepsilon\delta^p$، با استفاده از لم ۱۱.۱۰ نتیجه می‌گیریم که $x + \zeta y = \zeta^g r\delta^p$، که در آن r یک عدد حقیقی است. طبق لم ۹.۱۰، به ازای بعضی اعداد صحیح گویای a، $\delta^p \equiv a\ (L^p)$. از این رو، $x + \zeta y = \zeta^p ra\ (L^p)$ (بنابر لم ۶.۱۰) امّا $p\ ||\ [p]$، و در نتیجه، (سنج p) $x + \zeta y \equiv \zeta^g ra$. چون ζ^g یکه است، $(x + \zeta y) ra \equiv \zeta^{-g}$. همچنین، ra یک عدد حقیقی است؛ بنابراین با در نظرگرفتن مزدوج‌های مختلط درمی‌یابیم که $\zeta^g(x + \zeta^{-1}y) \equiv ra$. با ترکیب دو همنهشتی اخیر، نتیجه می‌شود که

$$x\zeta^{-g} + y\zeta^{1-g} - x\zeta^g - y\zeta^{1-g} \equiv 0 \quad (\text{سنج } p) \qquad (۱۰.۸)$$

برای لحظه‌ای موضوع مورد بحث را رها می‌کنیم تا نشان دهیم که $\zeta+1$ یکه است. چون

$$x^{p-1} + \ldots + 1 = (x - \zeta)(x - \zeta^2) \ldots (x - \zeta^{p-1}) \quad ,$$

با فرض کردن $x = -1$، درمی‌یابیم که $p \mid (\zeta + 1)$، و این ادعای ما را ثابت می‌کند.

دوباره به بحث سابق بازمی‌گردیم. مشاهده می‌شود که (سنج p) $g \not\equiv 0$ علت آن است که در غیر این صورت $\zeta^g = 1$ و رابطهٔ (۱۰.۸) به صورت $y(\zeta - \zeta^{-1}) \equiv 0$ و $(\zeta - 1)(\zeta + 1) \equiv 0$ خواهد شد. پس چون $\zeta + 1$ یکه است، $(\zeta - 1) \equiv 0$ یعنی $p \mid y\lambda$. چون $[p] = [\lambda]^{p-1}$، $p > 2$، $\lambda \mid y$، $\lambda^2 \mid y\lambda$، $N\lambda \mid Ny$، و $p \mid y^{p-1}$ که این نتیجه با فرض $p \nmid y$ در تناقض است. به‌طور مشابه، می‌توان نتیجه گرفت که (سنج p) $g \not\equiv 1$؛ زیرا در غیر این صورت رابطهٔ (۱۰.۸) به صورت $x(\zeta^{-1} - \zeta) \equiv 0$ درمی‌آید و بحثی مشابه به کار می‌رود.

پس رابطهٔ (۱۰.۸) را می‌توان به صورت

$$\alpha p = x\zeta^{-g} + y\zeta^{1-g} - x\zeta^{g} - y\zeta^{g-1} \quad , \qquad (۱۰.۹)$$

نوشت، که در آن α یک عدد صحیح در K است و هیچ یک از چهار توان ζ توسط p عاد نمی‌شوند. اعداد ζ، ζ^2، ...، ζ^{p-1} تشکیل یک پایهٔ صحیح برای K می‌دهند، و اعداد ζ^{-g}، ζ^{1-g}، ζ^{g}، و ζ^{g-1} در میان آنها ظاهر می‌شوند. حال مشاهده می‌شود که

$$\alpha = \frac{x}{p}\zeta^{-g} + \frac{y}{p}\zeta^{1-g} - \frac{x}{p}\zeta^{g} - \frac{y}{p}\zeta^{g-1}$$

اگر هیچ جفت از توانها به سنج p همنهشت نیستند، آنگاه $p \mid xy$ و $p \mid y$؛ زیرا α یک عدد صحیح بوده و نمایش آن بر حسب پایهٔ صحیح یگانه است و تنها شامل ضرایب صحیح است. چون طبق فرض $p \nmid x$ و $p \nmid y$، دو تا از توانها باید به سنج p همنهشت باشند. از آنجایی که $g \not\equiv 0$ و $g \not\equiv 1$، تنها امکان باقی‌مانده این است که $2g \equiv 1 \pmod{p}$.

چون $2g \equiv 1 \pmod{p}$ و $\xi^p = 1$، رابطهٔ (۱۰.۹) را می‌توان به صورت

$$\begin{aligned} \alpha p \xi^g &= x + y\xi - x\xi^{2g} - y\xi^{2g-1} \\ &= (x - y)(1 - \xi) = (x - y)\lambda \end{aligned}$$

نوشت. از این رو

$$N\alpha \cdot Np = N(x - y)\, N\lambda \quad \text{و} \quad N\alpha \cdot p^{p-1} = (x - y)^{p-1} \cdot p$$

نتیجه می‌گیرم که $p \mid (x - y)$، یعنی $x \equiv y \pmod{p}$.

اگر خیلی به عقب برگردیم و رابطهٔ (۱۰.۵) را به صورت

$$\prod_{m=0}^{p-1} (x + \xi^m Z) = -y^p \quad ,$$

بنویسیم، بحثی مشابه نشان می‌دهد که $x \equiv Z \pmod{p}$. از این رو

$$0 = x^p + y^p + z^p \equiv x^p + x^p + x^p \equiv 3x^p \pmod{p}$$

پس $p \mid 3x^p$، و این در حالی است که $p \nmid x$؛ از این رو $p = 3$.

تنها عدد اول منظم که به ازای آن رابطهٔ (۱۰.۵) ممکن است یک جواب داشته باشد، عدد $p = 3$ است؛ و این حالت را با نشان دادن اینکه اگر $3 \nmid x$ و $3 \nmid y$ و $3 \nmid z$ معادله $x^3 + y^3 + z^3 = 0$ نمی‌تواند در مجموعهٔ اعداد صحیح گویا جوابی داشته باشد، کنار خواهیم گذاشت. چون -1،

۰، ۱ تشکیل یک دستگاه کامل‌مانده به سنج ۳ را می‌دهند و $3 \nmid x$، (سنج ۳) $x \equiv \pm 1$. از این رو

$$x = 3k \pm 1 \text{ ، } x^3 = 27k^3 \pm 27k^2 + 9k \pm 1 \quad ,$$

پس (سنج ۹) $x^3 \equiv \pm 1$. به‌طور مشابه (سنج ۹) $y^3 \equiv \pm 1$ و (سنج ۹) $z^3 \equiv \pm 1$؛ بنابراین

$$0 = x^3 + y^3 + z^3 \equiv \pm 1 \pm 1 \pm 1 \qquad \text{(سنج ۹)}$$

بدیهی است که این موضوع نمی‌تواند برای هر انتخابی از علامتهای + و - درست باشد؛ و بدین ترتیب قضیهٔ ۱۲.۱۰ ثابت شده است.

فصل ۱۱

لم مینکوفسکی و نظریهٔ یکه‌ها

۱. **لم مینکوفسکی.** اکنون می‌خواهیم لم مشهور «هندسی» مینکوفسکی[1] را معرفی کنیم که در نظریهٔ اعداد کاربردهای مهمی دارد. این لم، در حالت خاص اثبات ساده‌ای را از قضیهٔ ۱.۱۰، که فعلاً بدون اثبات باقی مانده، ارائه می‌دهد. به‌علاوه، لم مذکور ما را قادر خواهد ساخت تا قضیه‌ای اساسی مربوط به ساختار یکه‌ها در یک هیأت اعداد جبری را ثابت کنیم.

قضیهٔ ۱.۱۱. $\{ a_{pq} \}$ را یک مجموعهٔ n^2 عضوی از اعداد حقیقی در نظر می‌گیریم، به‌طوری که در آن n، ...، ۲، ۱ = q و p، ۱ < n و دترمینان $\Delta = |a_{pq}|$ غیرصفر است. فرم‌های $L_p(u_1, \ldots, u_n)$ را به این صورت تعریف می‌کنیم که

$$L_p(u_1, \ldots, u_n) = \sum_{q=1}^{n} a_{pq} u_q \quad \text{و} \quad p = 1, \ldots, n$$

---

1) Minkowski

فرض می‌کنیم $k_1, \ldots, k_n$، n عدد مثبت هستند که حاصل‌ضرب آنها کمتر از $|\Delta|$ نیست. در چنین شرایطی، اعداد صحیح گویای $x_1, \ldots, x_n$ که همگی صفر نیستند موجودند، به‌طوری که برای آنها

$$|L_p(x_1, \ldots, x_n)| < k_p \qquad p = 1, \ldots, n-1$$

$$|L_n(x_1, \ldots, x_n)| \leqslant k_n \tag{۱۱.۱}$$

برای فهمیدن آنکه این قضیه به لحاظ هندسی چه مفهومی دارد، به منظور سادگی کار فرض می‌کنیم که $n = 2$ و $|\Delta| = 1$. پس k_1 و k_2 هر دو اعدادی مثبت هستند. به‌طوری که $k_1 k_2 \geq 1$. فرض می‌کنیم u_1 و u_2 مؤلفه‌های یک نقطه (u_1 و u_2) در صفحه هستند. هر معادله به صورت $|au_1 + bu_2| = c$ یک جفت خط موازی را نشان می‌دهد. از این رو، معادلات

$$|a_{11}u_1 + a_{12}u_2| = k_1 \quad \text{و}$$
$$|a_{21}u_1 + a_{22}u_2| = k_2$$

دو جفت از خطهای موازی را نشان می‌دهند. بنابراین، تمامی چهار خط نشان داده شده در بالا با هم موازی نیستند، چون $\Delta \neq 0$. این موضوع، نتیجه می‌دهد که این چهار خط اضلاع یک متوازی‌الاضلاع هستند. مشکل نیست که نشان دهیم مساحت این متوازی‌الاضلاع برابر است با $4k_1k_2$. چون $k_1k_2 \geq 1$، مساحت مذکور حداقل ۴ است. پس قضیهٔ مورد بحث ما، می‌گوید که یک متوازی الاضلاع به مرکز مبدأ و مساحت حداقل

۴ دارای این خاصیت است که در داخل یا روی محیط آن یک نقطهٔ $(u_۱$ و $u_۲)$، غیر از $(۰,۰)$ و غیر از رئوس، وجود دارد که مؤلفه‌های آن هر دو اعداد صحیح گویا هستند. همان طور که با توجه به مربع محصور به خطوط $u_۱ = \pm ۱$ و $u_۲ = \pm ۱$ مشخص می‌شود، مساحت متوازی‌الاضلاع مورد بحث نمی‌تواند از ۴ کمتر باشد. تعبیر متناظری از آنچه گفته شد برای حالت n بعدی، وقتی «متوازی الاضلاع» را با «متوازی‌السطوح» و ۴ را با ۲^n جایگزین کنیم، وجود دارد.

بحث خود را با اثباتی از قضیهٔ مورد بحث ادامه می‌دهیم. یک نقطهٔ $(x_۱ ، \ldots ، x_n)$ در فضای n بعدی که مؤلفه‌های آن همگی اعداد صحیح گویا، ولی نه همگی صفر (این شرط اخیر بسیار مهم است)، هستند را یک نقطهٔ مشبک[۲] خواهیم نامید. قضیه ثابت می‌کند که حداقل یک نقطهٔ مشبک که در شرایط (۱۱.۱) صدق می‌کند وجود دارد.

فرض می‌کنیم چنین نقطه‌ای وجود نداشته باشد. در این صورت، هر نقطهٔ مشبک در حداقل یکی از نامساوی‌های

$$|L_p(x_۱, \ldots, x_n)| \geq k_p \quad \text{و} \quad p = ۱, ۲, \ldots, n-۱$$
$$|L_n(x_۱, \ldots, x_n)| > k_n$$

صدق می‌کند. همه نقاط مشبک را که به ازای آنها

$$|L_n(x_۱, \ldots, x_n)| > k_n,$$

ولی

2) *Lattic point*

$$|L_p(x_1, \dots, x_n)| < k_p \quad \text{و} \quad p = 1, 2, \dots, n-1$$

درنظر می‌گیریم (در صورت وجود).

این نقاط، به ازای یک ε مثبت و به اندازهٔ کافی کوچک در نامعادله زیر صدق می‌کنند

$$|L_n(x_1, \dots, x_n)| \geq k_n + \varepsilon$$

در نتیجه، هر نقطهٔ مشبک حداقل در یکی از نامعادلات

$$|L_p(x_1, \dots, x_n)| \geq k_p \quad p = 1, \dots, n-1 \quad \text{و}$$

(۱۱.۲)

$$|L_n(x_1, \dots, x_n)| \geq k_n + \varepsilon$$

صدق می‌کند. از این مطلب، به یک تناقض خواهیم رسید.

فرض می‌کنیم $k'_p = k_p$، $p \neq n$ و $k'_n = k_n + \varepsilon$. حال، ناحیهٔ داخل متوازی‌السطوح P_0 را که توسط

$$|L_p(u_1, \dots, u_n)| \underset{<}{\frac{k'_p}{2}} \quad \text{و} \quad p = 1, \dots, n \qquad (11.3)$$

تعریف شده در نظر می‌گیریم. فرض می‌کنیم $g_1, \dots, g_n$ نقطهٔ مشبکی است. فرض می‌کنیم P_0 چنان انتقال یابد که $(0, \dots, 0)$ به $(g_1, \dots, g_n)$ تبدیل گشته و P_0 به یک شکل جدید P_0 $(g_1, \dots, g_n)$ تبدیل گردد که به صورت زیر تعریف شده باشد:

$$|L_p(u_1 - g_1, \dots, u_n - g_n)| < \frac{k'_p}{2} \quad \text{و} \quad p = 1, \dots, n$$

با تغییر دادن $(g_1, \dots, g_n)$، در این روش تعدادی نامتناهی از چنین

$P_0\,(g_1, \ldots, g_n)$ هایی به دست می‌آوریم که همگی با P_0 اصلی به‌طور هندسی همنهشت هستند.

هیچ دوتایی از این متوازی‌السطوح‌ها نمی‌توانند یک نقطهٔ مشترک داشته باشند. علت این است که اگر نامساوی‌های

$$|L_p\,(u_1 - g_1, \ldots, u_n - g_n)| < \frac{k'_p}{2} \quad \text{و} \quad p = 1, \ldots, n$$

و

$$|L_p\,(u_1 - g'_1, \ldots, u_n - g'_n)| < \frac{k'_p}{2} \quad \text{و} \quad p = 1, \ldots, n$$

هر دو درست باشد، که $(g_1, \ldots, g_n) \neq (g'_1, \ldots, g'_n)$، آنگاه

$$|L_p\,(g_1 - g'_1, \ldots, g_n - g'_n)| < k' \quad \text{و} \quad p = 1, \ldots, n,$$

که چنین چیزی با این حقیقت که یکی از نامساوی‌های (۱۱.۲) به ازای هر نقطهٔ مشبک برقرار است، در تناقض است.

حال فرض می‌کنیم L یک عدد صحیح مثبت است، ابر مکعب $|u_q| \leq L \quad (q = 1, \ldots, n)$ را درنظر می‌گیریم. مجموع حجمهای همهٔ $P_0\,(g_1, \ldots, g_n)$ هایی که داخل این مکعب قرار می‌گیرند، کمتر از حجم مکعب یعنی $(2L)^n$ است. فرض می‌کنیم C کران بالای قدر مطلق مؤلفه‌های همهٔ نقاط موجود در P_0 است. در این صورت، هر $P_0\,(g_1, \ldots, g_n)$ داخل مکعب $|u_q| \leq L + C$ قرار می‌گیرد، به شرط اینکه داشته باشیم $|g_q| \leq L$، $q = 1, \ldots, n$، بجز $(2L + 1)^n - 1$ عدد از چنین $P_0\,(g_1, \ldots, g_n)$ هایی وجود دارد؛ چون برای هر g_q شرط $-L \leq g_q \leq L$ برقرار است. هیچ یک از $P_0\,(g_1, \ldots, g_n)$ ها متقاطع

نیستند. از این رو، مکعب $|u_q| \leq L+C$ شامل متوازی‌السطوح‌هایی با حجم کلی $J(۲L+۱)^n$ است، که J حجم یکی از آنها است. حجم کلی این مکعب، $(۲L+۲c)^n$ است. از این رو

$$J \leq \frac{(۲L+۲c)^n}{(۲L+۱)^n}$$

حال فرض می‌کنیم $L \to \infty$. این معنی، نتیجه می‌دهد که $J \leq ۱$. از این رو، حجم $P_۰$ حداکثر ۱ است.

حال با روش دیگری حجم $P_۰$ را محاسبه می‌کنیم. بنابر رابطهٔ (۱۱.۳)، حجم $P_۰$ با انتگرال nگانه

$$J = \int_{|Lp| < \frac{K'p}{۲}} du_۱ \dots du_n$$

به دست می‌آید. حال تغییر متغیر $y_p = L_p(u_۱, \dots, u_n)$ را انجام می‌دهیم. ژاکوبین این تبدیل همان Δ است، بنابراین

$$J = \frac{۱}{|\Delta|} \int_{|yp| < \frac{K'p}{۲}} dy_۱ \dots dy_n = \frac{k'_۱ \dots k'_n}{|\Delta|}$$

امّا طبق فرض قضیهٔ $|\Delta| \geq k_۱ \dots k_n > k_۱ \dots k_{n-۱}(k_n + \varepsilon) = k'_۱ \dots k'_n$. از این رو، $J > ۱$. این موضوع، با نتیجهٔ قبلی که $J \leq ۱$ در تناقض است. اکنون این فرض که هیچ نقطهٔ مشبکی در رابطهٔ (۱۱.۱) صدق نمی‌کند را باید کنار بگذاریم، و بدین ترتیب قضیه ثابت می‌شود.

مهم است بدانیم که وقتی a_{pq} ها مجاز هستند اعداد مختلط را اختیار کنند، قضیه به چه صورت درمی‌آید. در این مرحله، نشان خواهیم داد که با تغییرات مناسب، حتی در این حالت نیز قضیه برقرار است.

$L_p (p = ۱, \dots, n)$ را فرمی درنظر می‌گیریم که به صورت قبل با رابطهٔ

$$\sum_{q=1}^{n} a_{pq}\, u_q \quad \text{و} \qquad p = 1, \ldots, n$$

تعریف شود، با این ویژگی که a_{pq} مختلط است. L_p را چنان شماره‌گذاری می‌کنیم که r_1 تای اول ($0 \le r_1 \le n$) حقیقی بوده[۳] و بقیه آنها موهومی باشند. فرض بر آن است که تعداد اعداد موهومی زوج است، مثلاً $2r_2$ تا، و به ازای هر یک از آنها که در لیست به صورت L_p ($r_1 < p \le r_2$) ظاهر شود، مزدوج ـ مختلط آن L_p نیز در این لیست، به صورت L_{p+r_2}، مشاهده گردد. لیست مورد بحث، حال به صورت زیر درمی‌آید :

$$L_1, \ldots, L_{r_1} \;;\; L_{r_1+1}, \ldots, L_{r_1+r_2} \;;\; L_{r_1+1+r_2}, \ldots, L_{r_1+2r_2}$$

اعداد مزدوج ـ مختلط اعداد موهومی اعداد حقیقی

واضح است که $n = r_1 + 2r_2$. چون در گذشته، فرض بر آن است که k_1، ...، k_n اعداد مثبتی هستند که به ازای آنها $k_1 k_2 \ldots k_n \ge |\Delta|$، و به علاوه این خاصیت را دارند که $k_{r_1+s} = k_{r_1+s+r_2}$ ($s = 1, \ldots, r_2$). بنابراین، k_iهای مربوط به هر جفت از فرم‌های مزدوج ـ مختلط یکی هستند. به‌منظور به کارگیری نتایجی که تاکنون گرفته شده‌اند، یک مجموعهٔ جدید از فرم‌های L'_p را به‌صورت ذکرشونده تعریف می‌نماییم. فرض می‌کنیم

$$L'_p = \begin{cases} L_p\,, & p = 1, \ldots, r_1 \text{ ،} \\ \dfrac{L_p + \bar{L}_p}{\sqrt{2}} = \dfrac{L_p + L_{p+r_2}}{\sqrt{2}}\,, & p = r_1+1, \ldots, r_1 + r_2 \\ \dfrac{L_p - \bar{L}_p}{\sqrt{2}\, i} = \dfrac{L_p - L_{p-r_2}}{\sqrt{2}\, i}\,, & p = r_1+r_2+1, \ldots, r_1 + 2r_2 \end{cases}$$

---

۳) این بدان معناست که هیچ یک از a_{pq}ها که ظاهر می‌شوند موهومی نیستند.

(اگر $r_1 = 0$، بدیهی است که این لیست با گروه دوم شروع می‌شود.) مجموعهٔ فرم‌های L'_p حقیقی است، و دترمینان آن مثل مجموعهٔ اولیهٔ فرم‌های L_p همان قدر مطلق $|\Delta|$ را دارد (چرا؟). این موضوع قادرمان می‌سازد تا قضیهٔ ۱۱.۱ را برای L'_p به کاربریم. قبل از انجام این کار، عدد صحیحی مثل a $(1 \leq a \leq n)$ را انتخاب کرده و L'_a را به انتهای لیست L'_p انتقال می‌دهیم. در نتیجه، یک نقطهٔ مشبک $(x_1, \ldots, x_n)$ موجود است، به‌طوری که

$$|L'_p(x_1, \ldots, x_n)| < k_p \quad , \quad p = 1, \ldots, n, p \neq a \quad \text{و}$$
$$|L'_a(x_1, \ldots, x_n)| \leq k_a \tag{۱۱.۴}$$

به‌منظور به کاربردن این نامساوی‌ها برای L_p، اجازه دهید L_p را بر حسب L'_p پیدا کنیم. واضح است که

$$L_p = L'_p \quad \text{و} \quad p = 1, \ldots, r_1 \quad \text{و}$$
$$L_p = \frac{\sqrt{2}}{2}(L'_p - iL'_{p+r_2}) \quad p = r_1 + 1, \ldots, r_1 + r_2$$
$$L_{p+r_2} = \overline{L}_p$$

از این رو

$$|L_p| = |L'_p| \quad \text{و} \quad p = 1, \ldots, r_1 \quad \text{و}$$
$$|L_p| = |L_{p+r_2}| = \frac{1}{\sqrt{2}}\{|L'_p|^2 + |L'_{p+r_2}|^2\}^{1/2} \quad \text{و}$$
$$p = r_1 + 1, \ldots, r_1 + r_2$$

(اگر $r_1 = 0$، از اولین قسمت این دو نمایش صرف‌نظر می‌کنیم.)

حال فرض می‌کنیم a هر عدد صحیح است که $1 \le a \le r_1 + r_2$. از فرمول‌های قبلی و نامساوی‌های (۱۱.۴) نتیجه می‌شود که

$$|L_p(x_1, \dots, x_n)| < k_p \quad \text{و} \quad p = 1, \dots, r_1 + r_2, p \neq a$$
$$|L_a(x_1, \dots, x_n)| \le k_a$$

چون $|L_p| = |L_{p+r_2}|$ $(p = r_1 + 1, \dots, r_1 + r_2)$، ما نتیجهٔ زیر را ثابت کرده‌ایم.

نتیجهٔ ۲.۱۱. *یک نقطهٔ مشبک $x \neq 0$ وجود دارد؛ به‌طوری که*

$$|L_p(x_1, \dots, x_n)| \le k_p \quad \text{و} \quad p = 1, \dots, n$$

به علاوه، نامساوی فوق می‌تواند با یک نامساوی اکید جایگزین شود، به جز برای یک فرم حقیقی L_a یا دو فرم مزدوج ـ مختلط L_a و L_{a+r_2}، که از پیش انتخاب شده‌اند.

یک حالت خاص نتیجهٔ فوق، بهره‌ای ویژه دارد. فرض می‌کنیم $n = 2$، $r_1 = 0$ و $r_2 = 1$، یعنی هر دو فرم ذکر شده در بالا موهومی هستند. در این حالت، $k_1 = k_2$ و

$$|L_1| = |L_2| = \frac{1}{\sqrt{2}} \{ |L'_1|^2 + |L'_2|^2 \}^{1/2}$$

بنابراین، با استفاده از فرمول (۱۱.۴) می‌توان استنباط کرد که $|L_1|$ و $|L_2|$ هر دو کمتر از K_1 هستند. به این استنباط، نمی‌توان مستقیماً از نتیجهٔ ۲.۱۱ دست یافت.

۲. کاربردها. حال در موقعیتی هستیم که می‌توانیم قضیهٔ ۱.۱۰ را ثابت کنیم. فرض می‌کنیم $\alpha_1, \dots, \alpha_n$ یک پایه برای ایده‌آل A بوده و $\alpha_i^{(j)}$ $(j = 1, \dots, n)$ مزدوج‌های α_i هستند. فرم‌های $\sum_{i=1}^{n} \alpha_i^{(j)} u_i$ $(j = 1, \dots, n)$ را در نظر می‌گیریم. در خصوص دترمینان آنها می‌توان نوشت که $\Delta[\alpha_1, \dots, \alpha_n]\}^{1/2} = NA \cdot |d|^{1/2}$. حال، می‌توانیم نتیجهٔ ۲.۱۱ را با مساوی فرض کردن k_pها با $\{NA \cdot |d|^{1/2}\}^{1/n}$ به کار ببریم. بدین طریق، یک نقطهٔ مشبک $x_1, \dots, x_n$ به دست می‌آید، به‌طوری که اگر $\omega_j = \sum_{i=1}^{n} \alpha_i^{(j)} x_i$، آنگاه

$$|\omega_j| \leq \{NA \cdot |d|^{1/2}\}^{1/n} \quad \text{و} \quad j = 1, \dots, n$$

به علاوه، طبق قسمت دوم نتیجه و ملاحظات ذیل آن حداقل یکی از نامساوی‌ها می‌تواند با یک نامساوی اکید جایگزین شود. از این رو

$$|N\omega| = |\omega_1 \dots \omega_n| < NA \cdot |d|^{1/2}$$

نتیجهٔ مهم دیگری از نظریهٔ مینکوفسکی به صورت زیر است:

قضیهٔ ۳.۱۱. *مبین d از یک هیأت اعداد جبری غیر از R این خاصیت را دارد که $|d| > 1$.*

برای اثبات این قضیه، فرض می‌کنیم A ایده‌آل (۱) است. طبق قضیهٔ ۱.۱۰، در (۱) یک عدد صحیح $\alpha \neq 0$ وجود دارد؛ به‌طوری که $|N\alpha| < N((1)) \cdot |d|^{1/2} = |d|^{1/2}$. چون $\alpha \neq 0$، $|N\alpha| \geq 1$. بنابراین $|d| > 1$.

باید در نظر داشت که نتیجهٔ قضیهٔ ۳.۱۱ برای هیأت R نادرست است؛ زیرا در این حالت $d = 1$. همچنین، باید توجه کرد که در این حالت لم

مینکوفسکی قابل استفاده نیست، چون لازم است داشته باشیم $n > ۱$.

آنچه تاکنون گفته شد، در قسمتهای بعدی برای مطالعه یکه‌ها در یک هیأت مورد استفاده قرار خواهد گرفت. اثبات قضیهٔ اساسی توسط اور و در مقالهٔ وی مطرح شده (نك : فهرست منابع) و خواننده آن را برای مرور مطالب اولیه‌ای که در فصل هفتم درباره یکه‌ها ارائه شده‌اند، مفید خواهد یافت.

۳. قضیهٔ مینکوفسکی ـ دیریکله[4] دربارهٔ یکه‌ها. به‌طوری که قبلاً دیدیم، همهٔ یکه‌ها در هیأت درجهٔ دوم حقیقی $R(\sqrt{۲})$ به صورت $\pm(۱+\sqrt{۲})^k$ $(k = ۰, \pm ۱, \ldots)$ هستند. مقصود ما این است که یک تعمیم از این قضیه را برای دیگر هیأت‌های اعداد جبری به دست آوریم.

فرض می‌کنیم $K = R(\theta)$ روی R از درجهٔ n بوده و $\theta_۱, \ldots, \theta_n$ مزدوج‌های θ است. همهٔ θ_i ها در چندجمله‌ای مینیمال یکسان $p(x)$ صدق می‌کنند. چون ضرایب $p(x)$ حقیقی هستند، هر ریشهٔ موهومی θ_i با یک ریشهٔ مزدوج ـ مختلط θ_j جفت شده است. فرض می‌کنیم $r_۱$ تعداد ریشه‌های حقیقی و $۲r_۲$ تعداد ریشه‌های موهومی است که $n = r_۱ + ۲r_۲$. ریشه‌ها را چنان شماره‌گذاری می‌کنیم که $\theta_۱, \ldots, \theta_{r_۱}$ حقیقی، و $\theta_{r_۱+۱}, \ldots, \theta_n$ موهومی باشند[5]. شماره‌گذاری مجموعهٔ اخیر را طوری مرتب می‌کنیم که $\theta_{r_۱+t}$ و $\theta_{r_۱+r_۲+t}$ $(t = ۱, \ldots, r_۲)$ مزدوج‌های ـ مختلط باشند. سرانجام اینکه، فرض می‌کنیم $r = r_۱ + r_۲ - ۱$.

اگر $r = ۰$، ساختار یکه‌ها در K بسادگی تعیین می‌شود؛ زیرا در این

---

4) *Dirichlet*

۵) قابل توجه است که برای این کار قرارداد قبلی خود که $\theta = \theta_۱$ را کنار گذاشتیم.

صورت $n = 1$، $n = 1 + r_2$ یا $r_2 = 1$. حال، چون $r_1 + r_2 = 1$؛ پس $r_2 = 0$ یا $r_2 = 1$ هیأت درجهٔ دوم $n = 2$. اگر $n = 1$، هیأت R است، و اگر $n = 2$، $r_2 = 1$ موهومی است. در خصوص وضعیت یکه‌ها در این حالت‌ها قبلاً در فصل هفتم توضیح داده شده است. بنابراین، از این پس فرض خواهیم کرد که $r \geq 1$.

ملاحظه می‌شود که هر ریشهٔ واحد ρ در K یک یکه است؛ زیرا اگر $\rho^m = 1$، $N(\rho)^m = 1$، و بنابراین $N(\rho) = \pm 1$. تعداد ریشه‌های واحد در K متناهی است؛ زیرا مرتبهٔ هر یک از آنها باید n را عاد کند و تنها تعدادی متناهی از ریشه‌های واحد از هر مرتبه موجود است.

اگر $\varepsilon_1, \ldots, \varepsilon_t$ یکه‌هایی در K باشند، همهٔ اعداد به شکل $\varepsilon = \rho {\varepsilon_1}^{a_1} \ldots {\varepsilon_t}^{a_t}$ نیز چنین خواهند بود، که a_i ها اعداد صحیح گویا بوده و ρ یک ریشهٔ واحد است. آنچه گفته شد، از این حقیقت ناشی می‌شود که حاصل‌ضرب یکه‌ها، یکه است. t یکهٔ $\varepsilon_1, \ldots, \varepsilon_t$ مستقل[6] هستند، اگر رابطه‌ای به صورت

$$ {\varepsilon_1}^{a_1} \ldots {\varepsilon_t}^{a_t} = 1 \qquad (11.5) $$

با a_i های صحیح گویا وجود نداشته باشد، مگر اینکه همهٔ a_i ها حذف شوند. اگر چنین رابطه‌ای موجود باشد و $t > 1$، هر ε_i وابسته[7] به دیگران گفته می‌شود. قابل توجه است که اگر $\varepsilon_1, \ldots, \varepsilon_t$ مستقل باشند، آنگاه رابطه‌ای به صورت

$$ {\varepsilon_1}^{b_1} \ldots {\varepsilon_t}^{b_t} = \rho $$

---

6) *independent* 7) *dependent*

نمی‌تواند با اعداد گویای b_i برقرار باشد؛ چون با افزایش هر طرف با یک توان به اندازه کافی بزرگ، می‌توانیم آن را به شکل (۱۱.۵) تبدیل کنیم.

قضیهٔ اساسی مربوط به ساختار یکه‌های K در ذیل آمده است :

قضیهٔ ۱۱.۴. *اگر* $r \geq ۱$، *آنگاه* r *یکه مستقل* $\xi_۱, \ldots, \xi_r$ *در* K *وجود دارند، چنانکه هر یکه* η *را می‌توان به‌طور یگانه‌ای به صورت*

$$\eta = \rho\, \xi_۱^{a_۱} \ldots \xi_r^{a_r}$$

بیان کرد که در آن a_i *ها اعداد صحیح گویا بوده و* ρ *یک ریشهٔ واحد در* K *است.*

اثبات در سه قسمت انجام خواهد شد. ابتدا وجود r یکه مستقل $\varepsilon_۱, \ldots, \varepsilon_r$ را ثابت می‌کنیم. در مرحلهٔ بعد، ثابت می‌کنیم که r یکه مستقل $\xi_۱, \ldots, \xi_r$ موجودند چنانکه هر یکه‌ای که به $\varepsilon_۱, \ldots, \varepsilon_r$ وابسته است را می‌توان به‌طور یگانه‌ای به صورت مذکور در قضیه بیان کرد. سرانجام نیز، ثابت می‌کنیم که هر $r+۱$ یکه در K وابسته هستند، و بنابراین همه یکه‌ها به $\varepsilon_۱, \ldots, \varepsilon_r$ وابسته هستند.

هر یک از سه مرحله مذکور، در یک بخش جداگانه بحث خواهد شد.

۴. وجود r یکهٔ مستقل. طبق اثبات قضیهٔ ۳.۱۱، یک عدد صحیح $\lambda \neq ۰$ در K وجود دارد، به‌طوری که $|N\lambda| < |d|^{۱/۲}$. همهٔ λ های دارای این خاصیت را درنظر می‌گیریم. هر کدام از آنها، یک ایده‌آل (λ) با نورم $|N\lambda|$ را معین می‌کند. امّا حداکثر تعدادی متناهی از ایده‌آل‌ها با نورم داده شده و از این رو تعدادی متناهی از ایده‌آل‌های $(\lambda_۱), \ldots, (\lambda_s)$ با نورم

کمتر از $|d|^{1/2}$ـ وجود دارد. در نتیجه، هر λ که برای آن، رابطهٔ $|N\lambda| < \frac{1}{2}|d|$ برقرار است، با یکی از اعداد $\lambda_1, \ldots, \lambda_s$ مرتبط است. فرض می‌کنیم $\lambda_j^{(i)}$ مشخص کنندهٔ مزدوج‌های λ_j بوده و l کوچکترین عدد میان $|\lambda_j^{(i)}|$ها $(j = 1, \ldots, S$ و $i = 1, \ldots, n)$ است.

فرض می‌کنیم $\alpha_1, \ldots, \alpha_n$ یک پایهٔ صحیح برای K است. قصد داریم از نتیجهٔ ۲.۱۱ برای فرم‌های

$$\sum_{j=1}^{n} \alpha_j^{(i)} u_j \qquad \text{و} \qquad i = 1, \ldots, n$$

استفاده کنیم. دترمینان آنها، $|d|^{1/2}$ است. در اینجا رجوع به قراردادی که در بخش ۳ دربارهٔ شماره‌گذاری مزدوج‌ها وضع کرده بودیم حائز اهمیت است. با این کار، نتیجه می‌گیریم که r_1 مورد اول از فرم‌های فوق حقیقی هستند، و باقیماندهٔ آنها در جفت‌هایی مزدوج ـ مختلط[۸] قرار می‌گیرند. فرض می‌کنیم a یک عدد صحیح گویا $(1 \le a \le r_1 + r_2)$ است. اگر a با یک فرم حقیقی متناظر باشد، بجز برای حالت $i = a$، k_i را برابر با l می‌گیریم، و اگر a با یک فرم موهومی متناظر باشد نیز، بجز برای حالتهای $i = a$ و $i = a + r_2$، باز k_i را برابر با l فرض می‌کنیم. بقیهٔ k_iها را طوری انتخاب می‌کنیم که حاصل‌ضرب همهٔ k_iها $|d|^{1/2}$ باشد، و بنابراین در دومین حالت $k_a = k_{a+r_2}$. طبق نتیجهٔ ۲.۱۱، می‌توان اعداد صحیح گویای

---

۸) اگر هر یک از فرم‌های باقیمانده حقیقی بود، دوتای آنها بایستی برابر می‌بودند؛ بنابراین $\Delta[\alpha_1, \ldots, \alpha_n] = 0$، که چنین چیزی با این حقیقت که $\alpha_1, \ldots, \alpha_n$ یک پایه است در تناقض است.

$x_1, \ldots, x_n$ که همگی صفر نیستند را چنان یافت که

$$\left| \sum_{j=1}^{n} \alpha_j^{(i)} x_j \right| < 1$$

که این رابطه برای همهٔ iها بجز $i = a$ در حالت اول و $i = a$ و $i = a + r_2$ در حالتِ دوم معتبر است. فرض می‌کنیم μ_a نشاندهندهٔ عدد صحیح $\sum_{j=1}^{n} \alpha_j x_j$ است. در این صورت

$$|N(\mu_a)| = |\mu_a^{(1)}| \ldots |\mu_a^{(n)}| < k_1 \ldots k_n = |d|^{1/2}$$

بنابر پاراگراف قبل، μ_a با یکی از اعداد λ_j مرتبط است؛ پس $\mu_a = \varepsilon_a \lambda_j$، که در آن ε_a یک یکه است. حال مشاهده می‌شود که $|\mu_a^{(i)}| < l$ $(i = 1, \ldots, r_1 + r_2$ و $i \neq a)$. از این رو

$$|\varepsilon_a^{(i)}| = |\mu_a^{(i)}| \, |\lambda_j^{(i)}|^{-1} < l \cdot \frac{1}{l} = 1$$

به ازای هر i که $i = 1, \ldots, r_1 + r_2$ و $i \neq a$. اکنون، $|\varepsilon_a^{(n)}| = |\varepsilon_a^{(1)}| \ldots |\varepsilon_a^{(n)}| = |N\varepsilon_a| = 1$. به‌علاوه، طبق شماره‌گذاری مزدوج‌ها هر یک از عامل‌ها به جز $\varepsilon_a^{(a)}$ و مزدوج ـ مختلط آن، اگر موجود باشد، از نظر قدر مطلق از ۱ کمتر است. در نتیجه، $|\varepsilon_a^{(a)}| > 1$.

چون $1 \leq a \leq r_1 + r_2$، a می‌تواند $r + 1$ مقدار $1, \ldots, r + 1$ را اختیار کند. بنابراین، $r + 1$ یکهٔ $\varepsilon_1, \ldots, \varepsilon_{r+1}$ را داریم که به ازای مقادیر i میان ۱ و $r + 1$

$$|\varepsilon_i^{(i)}| > 1 \quad \text{و} \quad |\varepsilon_j^{(i)}| < 1 \ (i \neq j) \qquad (11.6)$$

حال، نشان خواهیم داد که $\varepsilon_1, \ldots, \varepsilon_r$ مستقل هستند. علت این است که

فرض می‌کنیم $\varepsilon_1^{a_1} \dots \varepsilon_r^{a_r} = 1$. در این صورت، چون a_iها اعداد صحیح گویا هستند

$$a_1 \log |\varepsilon_1^{(i)}| + \dots + a_r \log |\varepsilon_r^{(i)}| = 0 \quad \text{و} \quad i = 1, \dots, r$$

اکنون نشان خواهیم داد که همهٔ a_iها باید صفر باشند. در واقع؛ در غیر این صورت دترمینان $|l_{ij}|$ صفر است و $l_{ij} = \log |\varepsilon_j^{(i)}|$ ($i = 1, \dots, r$ و $j = 1, \dots, r$). فرض می‌کنیم $l_i = 1$ ($i = 1, \dots, r_1$) و $e_i = 2$ ($i = r_1 + 1, \dots, r$). در نتیجه، دترمینان $|e_i\, l_{ij}|$ نیز صفر می‌شود؛ زیرا هر سطر آن را در یک ثابت ضرب کرده‌ایم. بنابراین، معادلات به فرم

$$\sum_{i=1}^{r} x_i\, e_i\, l_{ij} = 0 \quad , \qquad j = 1, \dots, r$$

یک جواب غیربدیهی $x_1, \dots, x_r$ دارند. آن x_i را انتخاب می‌کنیم که بزرگترین قدر مطلق را داشته باشد ـ فرض می‌کنیم عنصر مورد نظر ما x_1 است. اولین معادله از نوع فوق‌الذکر

$$-x_1\, e_1\, l_{11} = x_2\, e_2\, l_{21} + \dots + x_r\, e_r\, l_{r1}$$

است، و بنابراین

$$|x_1|\, e_1\, |l_{11}| \leq |x_1|\, (e_2\, |l_{21}| + \dots + e_r\, |l_{r1}|)$$

حال، طبق رابطهٔ (۱۱.۶)، $l_{11} > 0$ و $l_i < 0$ ($i = 2, \dots, r$). از این رو

$$e_1\, l_{11} \leq -e_2\, l_{21} - \dots - e_r\, l_{r1}$$

بنابراین

$$e_1\, l_{11} + e_2\, l_{21} + \dots + e_r\, l_{r1} \leq 0 \qquad (11.7)$$

از این نامساوی، یک تناقض به دست می‌آید.

چون

$$N(\varepsilon_1) = \varepsilon_1^{(1)} \dots \varepsilon_1^{(n)} = 1 ,$$
$$log\,|\varepsilon_1^{(1)}| + \dots + log\,|\varepsilon_1^{(n)}| = 0$$

طبق شماره‌گذاری مزدوج‌ها $|\varepsilon_1^{(k)}| = |\varepsilon_1^{(K+r_2)}|$ $(k > r_1)$. از این رو

$$\sum_{i=1}^{r_1+r_2} e_i\, log\,|\varepsilon_1^{(i)}| = 0$$

امّا این مجموع به صورت

$$e_1 l_{11} + e_2 l_{21} + \dots + e_r l_{r_1} + e_{r_1+r_2}\, log\,|\varepsilon_{1(r+1)}|$$

است. بنابر رابطهٔ (۱۱.۶) جملهٔ آخر منفی بوده و در نتیجه مجموع r جملهٔ اول مثبت است که این معنی با رابطهٔ (۱۱.۷) در تناقض است. پس فرض ما مبنی بر وابسته بودن $\varepsilon_1, \dots, \varepsilon_r$ نادرست بود.

بنابر آنچه گفته شد، به‌طور ضمنی ثابت شده است که دترمینان $|\,|log|\varepsilon_j^{(i)}|\,|$ $(i = 1, \dots, r$ و $j = 1, \dots, r)$ صفر نمی‌شود.

۵. قسمت دوم اثبات. فرض می‌کنیم $\varepsilon_1, \dots, \varepsilon_r$ یکه‌های به دست آمده در بخش قبل هستند. می‌خواهیم وجود یکه‌های مستقل $\xi_1, \dots, \xi_r$ را ثابت کنیم، به‌طوری که هر یکه η وابسته به $\varepsilon_1, \dots, \varepsilon_r$ نمایشی به صورت $\eta = \rho\, \xi_1^{a_1} \dots \xi_r^{a_r}$ داشته باشد، که در آن a_iها اعداد صحیح گویا و ρ یک ریشهٔ واحد در K است. یگانگی این نمایش، از مستقل بودن ξ_iها نتیجه می‌شود.

لم ۵.۱۱. *یک عدد مثبت A وجود دارد، به‌طوری که اگر قدر مطلق $|\omega^{(i)}|$ متعلق به هر یک از مزدوج‌های یک عدد صحیح ω کمتر از $A + ۱$ باشد، آنگاه ω یک ریشهٔ واحد است.*

تنها تعدادی متناهی از اعداد صحیح α در K وجود دارند که همهٔ مزدوج‌های آنها قدر مطلق کمتر از ۲ دارند. برای توجیه مطلب، فرض می‌کنیم

$$(x - \alpha^{(1)}) \dots (x - \alpha^{(n)}) = x^n + a_{n-1} x^{n-1} + \dots + a_0$$

چندجمله‌ای هیأت برای α است. چون هر a_i یک تابع متقارن ابتدائی از ریشه‌ها بوده و هر ریشه دارای قدر مطلق کمتر از ۲ است، داریم

$$|a_i| \leq \binom{n}{i} 2^{n-i}$$

a_i ها اعداد صحیح گویا هستند، و بنابراین تنها می‌توانند تعدادی متناهی از مقادیر متفاوت را اختیار کنند. در نتیجه، تنها تعدادی متناهی از چندجمله‌ای‌های متفاوت به ازای اعداد صحیح نوع مذکور وجود داشته و بدین ترتیب تنها به تعداد متناهی N از چنین اعداد صحیحی موجود است.

A را چنان انتخاب می‌کنیم که $A > 0$ و $(A + 1)^{N+1} < 2$. این A، چنانکه ثابت خواهیم کرد، خاصیت مورد نظر را داراست. فرض می‌کنیم ω یک عدد صحیح است، به‌طوری که $|\omega^{(i)}| < A + 1$ $(i = 1, \dots, n)$. قدر مطلق مزدوج‌های اعداد صحیح به شکل ω^k $(k = 1, \dots, N + 1)$ همگی کمتر از $(A + 1)^k \leq (A + 1)^{N+1} < 2$ هستند؛ بنابراین باید دو توان k و k' $(k' > k)$ موجود باشند، به طوری که $\omega^{k'} = \omega^k$. پس $\omega^{k'-k} = 1$، و ω یک ریشهٔ واحد است. بدین ترتیب، لم ثابت شده است.

فرض می‌کنیم η به یکه‌های $\varepsilon_1, \dots, \varepsilon_r$ وابسته هستند. به ازای برخی اعداد صحیح گویای N

$$\eta = \rho\, \varepsilon_1^{-a_1/N} \dots \varepsilon_r^{-a_r/N} \quad \text{و} \quad \eta^N \varepsilon_1^{a_1} \dots \varepsilon_r^{a_r} = 1$$

که ρ در K است، $\rho^N = 1$ و a_i ها اعداد صحیح گویا هستند. پس η و مزدوج‌های آن به صورت

$$\eta^{(i)} = \rho^{(i)} \varepsilon^{(i)s_1} \dots \varepsilon_r^{(i)s_r} \quad \text{و} \quad i=1, \dots, n \qquad (11.8)$$

که در آن $\rho^{(i)}$ یک N امین ریشهٔ واحد و s_j ها اعداد صحیح گویا هستند.

حال عبارت زیر را در نظر می‌گیریم :

$$\delta = \eta^y \varepsilon_1^{-x_1} \dots \varepsilon_r^{-x_r}$$

می‌خواهیم نشان دهیم که به ازای انتخاب مناسبی از $y, x_1, \dots, x_r$ به‌عنوان اعداد صحیح گویا، σ یک ریشهٔ واحد است. با استفاده از رابطهٔ (۱۱.۸)

$$|\sigma^{(i)}| = |\varepsilon_1^{(i)}|^{ys_1 - x_1} \dots |\varepsilon_r^{(i)}|^{ys_r - x_r} \qquad (11.9)$$

تعداد $r+1$ فرم خطی $L_i(y, x_1, \dots, x_r)$ که در آن

$$L_1 = ys_1 - x_1, \dots, L_r = ys_r - x_r, L_{r+1} = y$$

دترمینانی با قدر مطلق ۱ دارند. طبق قضیهٔ ۱.۱۱، به ازای هر δ $(0<\delta<1)$ مجموعه‌ای از اعداد صحیح گویای $y, x_1, \dots, x_r$ که همگی صفر نیستند وجود دارد، به‌طوری که

$$|y| \leq \delta^{-r} \quad \text{و} \quad |ys_1 - x_1| < \delta, \ldots, |ys_r - x_r| < \delta$$

بدین ترتیب، رابطهٔ (۱۱.۹) به صورت

$$|\sigma^{(i)}| < |\varepsilon_1^{(i)} \ldots \varepsilon_r^{(i)}|^{\delta}$$

درمی‌آید. σ را چنان کوچک انتخاب می‌کنیم که داشته باشیم $|\sigma^{(i)}| < 1 + A$. طبق لم ۵.۱۱، σ یک ریشهٔ واحد است. از تعریف σ نتیجه می‌شود که η را می‌توان به صورت زیر نوشت

$$\eta = \sigma^{1/y} \varepsilon_1^{x_1/y} \ldots \varepsilon_r^{x_r/y}$$

باید در نظر داشت که δ تنها به $\varepsilon_1, \ldots, \varepsilon_r$ وابسته است و $|y|$ کوچکتر از کرانی است که تنها به $\varepsilon_1, \ldots, \varepsilon_r$ بستگی دارد. از این رو، هر یکه η وابسته به $\varepsilon_1, \ldots, \varepsilon_r$ را می‌توان به شکل زیر نوشت

$$\eta = \sigma^{x_0/M} \varepsilon_1^{x_1/M} \ldots \varepsilon_r^{x_r/M} \qquad (۱۱.۱۰)$$

که در آن σ یک ریشهٔ واحد و M یک عدد صحیح مثبت است که تنها به ε_i ها بستگی دارد. این نمایش یگانه است، زیرا ε_i ها مستقل هستند.

لزوماً همهٔ اعداد به صورت (۱۱.۱۰)، به ازای اعداد صحیح گویای اختیاری x_i، به هیأت K متعلق نیستند. امّا همهٔ یکه‌های موجود در K که به صورت مزبور بیان می‌شوند را در نظر می‌گیریم، مثلاً اعداد به فرم $\varepsilon_i^{M/M}$. برای هر i $(i = 1, \ldots, r)$ چنین یکه‌ای را انتخاب می‌کنیم :

$$\xi_i = \sigma^{x_{0i}/M} \varepsilon_1^{x_{1i}/M} \ldots \varepsilon_i^{x_{ii}/M} \ldots \varepsilon_r^{x_{ri}/M}$$

که برای آن حداقل $x_{ii} > 0$.

ξ_i هایی که چنین انتخاب می‌شوند، خاصیت مذکور در شروع این بخش را دارند. علت این است که فرض می‌کنیم η یکه‌ای وابسته به $\varepsilon_1, \ldots, \varepsilon_r$ که لزوماً به صورت (۱۱.۱۰) است. طبق قضیهٔ ۱.۱

$$x_r = a_r x_{r+1} + t_r \quad \text{و} \quad 0 \le t_r < x_{r+1}$$

بنابراین به ازای اعداد صحیح مناسب x'_i

$$\eta\, \xi_r^{-ar} = \sigma^{x'_0/M}\, \varepsilon_1^{x'_1/M} \ \ldots\ \varepsilon_{r-1}^{x'_{r-1}/M}\, \varepsilon_r^{t_r/M}$$

η و ξ_r به $\varepsilon_1, \ldots, \varepsilon_r$ وابسته‌اند؛ پس $\eta\, \xi_r^{-ar}$ نیز چنین است. چون $0 \le t_r < x_{r+1}$ و x_{r+1} مینیمم است، $t_r = 0$ و

$$\eta\, \xi_r^{-ar} = \sigma^{x'_0/M}\, \varepsilon_1^{x'_1/M} \ \ldots\ \varepsilon_{r-1}^{x'_{r-1}/M} \quad \text{و}$$

حال، این روش را با $x'_{r-1}, \ldots$ تکرار می‌کنیم. سرانجام به دست می‌آوریم

$$\eta\, \xi_r^{-ar} \cdot \xi_{r-1}^{-ar-1} \ \ldots\ \xi_1^{-a_1} = \sigma^{x/M}$$

که در آن $\rho = \sigma^{x/M}$ یک ریشهٔ واحد در هیأت است. پس $\eta = \rho\, \xi_1^{a_1} \ldots \xi_r^{ar}$ به فرم مطلوب است.

برای نشان دادن یگانگی این نمایش، تنها باید نشان دهیم که $\xi_1, \ldots, \xi_r$ مستقل هستند. می‌نویسیم

$$\varepsilon_j = \rho_j\, \xi_1^{b_{1j}}\, \xi_2^{b_{2j}} \ \ldots\ \xi_r^{b_{rj}}$$

چون $|\rho_i| = 1$، داریم

$$\log |\varepsilon_j^{(i)}| = b_{1j} \log |\xi_1^{(i)}| + b_{2j} \log |\xi_2^{(i)}| + \ldots + b_{rj} \log |\xi_r^{(i)}| \qquad i, j, 1, \ldots, i$$

اگر ξ_jها مستقل نباشند، آنگاه دترمینان $|| \log |\xi_j^{(i)}||$، طبق بحثی که در بخش قبل به کار بردیم، صفر می‌شود. پس

$$|\log| \varepsilon_j^{(i)}|| = |b_{ij}| \ |\log| \xi_j^{(i)}|| = ۰$$

در تناقض با این حقیقت که $|| \log |\xi_j^{(i)}|| \neq ۰$.

۶. **تکمیل اثبات.** تنها چیزی که باقی مانده، این است که نشان دهیم هر $r+۱$ یکهٔ $\varepsilon_۰, \varepsilon_۱, \ldots, \varepsilon_r$ وابسته هستند. r معادله

$$\sum_{j=۰}^{r} C_j \log |\varepsilon_j^{(i)}| = ۰ \quad \text{و} \quad i = ۱, \ldots, r \qquad (۱۱.۱۱)$$

برحسب $r+۱$ مجهول C_j جوابی برای C_j های حقیقی دارند که همگی صفر نیستند. از این رو

$$|\varepsilon_۰^{(i)}|^{c_۰} \ \ldots \ |\varepsilon_r^{(i)}|^{cr} = ۱ \quad \text{و} \quad i = ۱, \ldots, r \qquad (۱۱.۱۲)$$

چنانکه در انتهای بخش ۴ نشان دادیم، هر یکهٔ ε_j این خاصیت را دارد که

$$e_{r+۱} \ \log |\varepsilon_j^{(r+۱)}| = -\sum_{i=۱}^{r} e_i \ \log |\varepsilon_j^{(i)}|$$

پس با ضرب کردن هر طرف در C_j و مجموع‌گیری از طرفین و با توجه به رابطهٔ (۱۱.۱۱)، به دست می‌آوریم

$$e_{r+۱} \sum_{j=۰}^{r} C_j \log |\varepsilon_j^{(r+۱)}| = -\sum_{j=۰}^{r} C_j \sum_{i=۱}^{r} e_i \ \log|\varepsilon_j^{(i)}|$$

$$= -\sum_{i=۱}^{r} e_i \sum_{j=0}^{r} C_j \log |\varepsilon_j^{(i)}| = ۰$$

از این رو $\sum_{j=0}^{r} C_j \log |\varepsilon_j^{(r+1)}| = 0$، و بنابر این رابطهٔ (۱۱.۱۱) برای $i=r+1$ نیز برقرار است. این نتیجه، از برشمردن مزدوج‌هایی که به ازای آنها (۱۱.۱۱)، و از این رو (۱۱.۱۲)، برای iهای بین ۱ و n برقرار است نتیجه می‌شود.

همهٔ C_jها صفر نیستند ـ می‌توان فرض کرد $C_0 \neq 0$. طبق رابطهٔ (۱۱.۱۲)

$$|\varepsilon_0^{(i)}| = |\varepsilon_1^{(i)}|^{-c_1/c_0} \quad \dots \quad |\varepsilon_r^{(i)}|^{-c_r/c_0} \quad \text{و} \quad i = 1, \dots, n$$

حال، با بحثی مشابه آنچه که ما را از رابطهٔ (۱۱.۸) به رابطهٔ (۱۱.۱۰) رساند، می‌توان نتیجه گرفت که

$$\varepsilon_0 = \sigma^{x_0/M} \quad \varepsilon_1^{x_1/M} \quad \dots \quad \varepsilon_r^{x_r/M}$$

بنابراین، یکه‌های $\varepsilon_0, \dots, \varepsilon_r$ وابسته هستند.

فهرست منابع

1. Birkhoff and MacLane, *Survey of Modern Algebra*, New York, 1948.
2. Hardy and Wright, *The Theory of Numbers*, Oxford, 1938.
3. E. Hecke, *Theorie der Algebraischen Zahlen*, Leipzig, 1923.
4. D. Hilbert, *Die Theorie der Algebraischen Zahlkörper*, No. 7 of Gesammelte Abhandlunge, Berlin, 1932.
5. E. Landau, *Einführung in die Elementare und Analytische Theorie der Algebraischen Zahlen und der Ideale*, Leipzig and Berlin, 1918.
6. E. Landau, *Vorlesungen über Zahlentheorie*, 3 volumes, Leipzig, 1927.
7. O. Ore, *Les Corps Algébriques et la Théorie des Idéaux*, Paris, 1934.
8. L. W. Reid, *The Elements of the Theory of Algebraic Numbers*, New York, 1910.
9. J. M. Thomas, *Theory of Equations*, New York, 1938.
10. H. S. Vandiver, *Fermat's Last Theorem*, American Mathematical Monthly, vol. 53 (1946), pp. 555-578.
11. Herman Weyl, *Algebraic Theory of Numbers*, Princeton, 1940.