دانشگاه کاشان

جبر دو

حسن دقیق

گروه ریاضی، آمار و علوم کامپیوتر

مهر ماه سال ۱۳۹۲

فهرست مطالب

فصل ۱
حلقه‌های اقلیدسی

در فصول قبل با دو شاخص از حلقه‌ها، یعنی حلقه‌ی اعداد صحیح ($\mathbb{Z}$) و حلقه‌ی چندجمله‌ای‌ها روی یک میدان F ($F[x]$) آشنا شدیم. یک ویژگی مشابه در این دو مثال، وجود الگوریتم تقسیم در آن‌ها بود. بنابر الگوریتم تقسیم در $\mathbb{Z}$ اگر a و b اعداد صحیح باشند و $b \neq 0$، آن‌گاه اعداد صحیح منحصر به فرد q و r یافت می‌شوند به‌نحوی که

$$a = qb + r \quad \text{و} \quad 0 \leq r < |b|.$$

و بنابر الگوریتم تقسیم در $F[x]$، اگر $f(x)$ و $g(x)$ دو چندجمله‌ای در $F[x]$ باشند و $g(x) \neq 0$، آن‌گاه چندجمله‌ای‌های منحصر به فرد $q(x)$ و $r(x)$ در $F[x]$ یافت می‌شوند به‌نحوی که

$$f(x) = q(x)g(x) + r(x) \quad \text{و} \quad (r(x) = 0 \ \text{یا}\ deg(r(x)) < deg(g(x))).$$

در اثبات بسیاری از گزاره‌ها در مورد حلقه‌های مورد اشاره در بالا، الگوریتم تقسیم ابزار اصلی کار بود. به‌ویژه در اثبات این‌که هر ایده‌آل از این حلقه‌ها اصلی است، از الگوریتم تقسیم کمک گرفتیم. این مشاهده ما را به تعریف خانواده‌ای از حلقه‌ها رهنمون می‌سازد که حلقه‌های $\mathbb{Z}$ و $F[x]$ مثال‌هایی از آن

هستند.

تعریف ۱.۱ فرض کنیم R یک حلقه‌ی جابه‌جایی و $\mathbb{N}^*$ مجموعه‌ی اعداد صحیح نامنفی باشد. تابع $\varphi : R - \{\circ\} \longrightarrow \mathbb{N}^*$ را یک **تابع اقلیدسی روی** R گوییم هرگاه:

(الف) برای هر دو عنصر غیرصفر a و b از R داشته باشیم $\varphi(a) \leq \varphi(ab)$.

(ب) اگر $a \in R$ و $\circ \neq b \in R$ آن‌گاه $q, r \in R$ یافت شوند به‌نحوی که

$$a = qb + r \quad \text{و} \quad (r = \circ \ \text{یا}\ \varphi(r) < \varphi(b))$$

تذکر ۲.۱ توجه کنید که در (ب) تعریف بالا، q و r لزوماً منحصر به فرد نیستند.

مثال ۳.۱ تابع $\varphi : \mathbb{Z} \longrightarrow \mathbb{N}^*$ با ضابطه‌ی $\varphi(n) = |n|$ یک تابع اقلیدسی است. در این مثال، برای a و b داده شده، q و rیافت شده در قسمت (ب) تعریف تابع اقلیدسی منحصر به فرد نیست. به عنوان نمونه اگر $a = ۲۵$ و $b = ۷$، آن‌گاه

$$۲۵ = ۳ \times ۷ + ۴ \quad \text{و} \quad |۴| < |۷|$$
$$۲۵ = ۴ \times ۷ - ۳ \quad \text{و} \quad |-۳| < |۷|$$

مثال ۴.۱ تابع $deg : F[x] - \{\circ\} \longrightarrow \mathbb{N}$ که به هر چندجمله‌ای ناصفر، درجه‌ی آن را نظیر می‌کند یک تابع اقلیدسی است.

تعریف ۵.۱ حلقه‌ی جابجایی R را یک **حلقه‌ی اقلیدسی** گوییم هرگاه یک تابع اقلیدسی روی آن موجود باشد.

در تعریف حلقه‌ی اقلیدسی، حلقه را یک‌دار فرض نکردیم. قضیه‌ی زیر نشان می‌دهد هر حلقه‌ی اقلیدسی

لزوماً یک‌دار است.

قضیه ۶.۱ هر حلقه‌ی اقلیدسی یک‌دار است.

اثبات. فرض کنیم R یک حلقه‌ی اقلیدسی با تابع اقلیدسی φ باشد. مجموعه‌ی

$$A = \{\varphi(r) : \quad r \in R,\ r \neq \circ\}$$

زیرمجموعه‌ای از $\mathbb{N}^*$ است و لذا بنابر اصل خوش ترتیبی دارای کوچکترین عضو است. فرض کنیم $\circ \neq s \in R$ چنان باشد که $\varphi(s)$ برابر این کوچکترین عضو باشد. اگر $a \in R$ دلخواه باشد، بنابر الگوریتم تقسیم در R،

$$a = qs + r$$

که در آن $q, r \in R$ و $r = \circ$ یا $\varphi(r) < \varphi(s)$. از آن‌جا که گزینه‌ی $\varphi(r) < \varphi(s)$ با انتخاب s متناقض است، خواهیم داشت $r = \circ$. پس $a = qs$ و لذا $a \in Rs$ پس $R = Rs$.
حال چون $s \in R$ لذا $R = Rs$. پس $e \in R$ موجود است که $s = es$. نشان می‌دهیم e عضو خنثی عمل ضرب حلقه است. اگر $a \in R$ دلخواه باشد، آن‌گاه $=$ و لذا

$$ea = e(qs) = e(sq) = (es)q = sq = qs = a$$

□

قضیه ۷.۱ در هر حلقه‌ی اقلیدسی، هر ایده‌آل اصلی است.

اثبات. فرض کنیم R یک حلقه‌ی اقلیدسی با تابع اقلیدسی φ و I یک ایده‌آل دلخواه R باشد. اگر $I = \{\circ\}$، آن‌گاه به وضوح I اصلی است. در غیر این صورت $\circ \neq a \in I$ را چنان انتخاب می‌کنیم که $\varphi(a)$ کوچکترین عضو مجموعه‌ی

$$B = \{\varphi(r) \ : \ r \in I \ \text{و}\ r \neq ۰\}$$

باشد. از آن‌جا که $a \in I$ لذا $Ra \subseteq I$. از طرف دیگر اگر $b \in I$دلخواه باشد، طبق الگوریتم تقسیم

$$b = qa + r$$

که در آن $r \in R$ و q و $r = ۰$ یا $\varphi(r) < \varphi(a)$. از آن‌جا که $r = b = qa \in I$، گزینه‌ی $\varphi(r) < \varphi(a)$ با انتخاب a متناقض است . لذا $r = ۰$. در نتیجه $b = qa \in Ra$. پس

$$I = Ra$$

بنابر قضیه‌ی قبل R یک‌دار است و لذا $Ra = \langle a \rangle$ایده‌آل پدید آمده توسط a است. و اثبات تمام است. □ به عنوان یک مثال زیبا از حلقه‌های اقلیدسی، در این بخش حلقه‌ی اعداد گاوسی را معرفی می‌کنیم. این حلقه به عنوان زیرحلقه‌ای از میدان اعداد مختلط به صورت زیر تعریف می‌شود:

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

به راحتی می‌توان نشان داد که $\mathbb{Z}[i]$ با اعمال جمع و ضرب معمولی اعداد مختلط یک حوزه‌ی صحیح است.

تعریف ۸.۱ برای هر $\alpha = a + bi \in \mathbb{Z}[i]$، **نرم** α به صورت $N(\alpha) = a^۲ + b^۲$ تعریف می‌شود.

لم ۹.۱ نرم دارای خواص زیر است:

(الف) برای هر $۰ \neq \alpha \in \mathbb{Z}[i]$، $N(\alpha) \geq ۱$.

(ب) برای هر $\alpha \in \mathbb{Z}[i]$، $N(\alpha) = ۰$ اگر و تنها اگر $\alpha = ۰$.

(ج) برای هر $\alpha, \beta \in \mathbb{Z}[i]$، $N(\alpha\beta) = N(\alpha)N(\beta)$.

اثبات. با استفاده از تعریف به‌راحتی نتیجه می‌شود. □

قضیه ۱۰.۱ تابع نرم یک تابع اقلیدسی روی $\mathbb{Z}[i]$ است.

اثبات. اگر $\alpha, \beta \in \mathbb{Z}[i]$ و $\beta \neq 0$ آن‌گاه $N(\beta) \geq 1$ و لذا

$$N(\alpha) \leq N(\alpha)N(\beta) = N(\alpha\beta).$$

پس شرط الف در تعریف تابع اقلیدسی برقرار است. برای اثبات برقراری شرط (ب) فرض کنیم $\alpha, \beta \in \mathbb{Z}[i]$ و $\beta \neq 0$. β به عنوان یک عدد مختلط ناصفر دارای وارون است(اگر $\beta = c + di$، آن‌گاه $\mathbb{C} \ni \beta^{-1} = \dfrac{c - di}{c^2 + d^2}$). و لذا

$$\tfrac{\alpha}{\beta} = \alpha\beta^{-1} = x + iy \in \mathbb{C}$$

که در آن $x, y \in \mathbb{R}$ (در واقع $x, y \in \mathbb{Q}$). اعداد صحیح q_1 و q_2 را می‌توان چنان انتخاب کرد که

$$\tfrac{-1}{2} \leq x - q_1 \leq \tfrac{1}{2}$$

$$\tfrac{-1}{2} \leq y - q_2 \leq \tfrac{1}{2}$$

حال با فرض $r_1 = x - q_1$ و $r_2 = y - q_2$ و

$$\tfrac{\alpha}{\beta} = (q_1 + q_2 i) + (r_1 + r_2 i).$$

لذا

$$\alpha = (q_1 + q_2 i)\beta + (r_1 + r_2 i)\beta.$$

حال با فرض $q = q_1 + q_2 i$ و $r = (r_1 + r_2 i)\beta$ داریم

$$q \in \mathbb{Z}[i]$$

$$r = \alpha - q\beta \in \mathbb{Z}[i]$$

و

$$\alpha = q\beta + r$$

به‌علاوه

$$\begin{array}{rcl} N(r) &=& N((r_۱ + r_۲ i)\beta) &=& N(r_۱ + r_۲)N(\beta) \\ &=& (r_۱^۲ + r_۲^۲)N(\beta) &\leq& (\frac{۱}{۴} + \frac{۱}{۴})N(\beta) < N(\beta) \end{array}$$

و اثبات تمام است. □

نتیجه ۱۱.۱ $\mathbb{Z}[i]$ یک دامنه‌ی اقلیدسی است.

هر دامنه‌ی اقلیدسی یک دامنه‌ی ایده‌آل اصلی و لذا یک دامنه‌ی یکتایی تجزیه است. پس $\mathbb{Z}[i]$ یک دامنه‌ی یکتایی تجزیه است. چگونه یک عضو دلخواه $\mathbb{Z}[i]$ را به عوامل تحویل‌ناپذیر(و در نتیجه اول) تجزیه کنیم؟ ابتدا ببینیم اعداد صحیح به عنوان عضوی از $\mathbb{Z}[i]$ چگونه تجزیه می‌شوند. اگر n یک عدد صحیح دلخواه باشد، ابتدا n را در $\mathbb{Z}$ به حاصل‌ضرب اعداد اول تجزیه می‌کنیم. ولی این عوامل ممکن است در $\mathbb{Z}[i]$ اول نباشند. (یادآوری می‌کنیم که در یک دامنه‌ی یکتایی تجزیه هر تحویل‌ناپذیر اول است و بالعکس هر اول تحویل‌ناپذیر است.). به عنوان مثال در $\mathbb{Z}$ داریم $۱۵ = ۳ \times ۵$. ولی در $\mathbb{Z}[i]$، ۵ اول نیست زیرا $۵ = (۲ + i)(۲ - i)$. پس باید به این سؤال پاسخ دهیم که چه اعداد صحیح اولی در $\mathbb{Z}[i]$ نیز تحویل‌ناپذیرند.

برای این کار عدد اول فرد $p \in \mathbb{Z}$ را در نظر بگیرید. فرض کنیم p در $\mathbb{Z}[i]$ تحویل‌پذیر باشد. پس

$$p = \alpha\beta$$

که در آن $\alpha, \beta \in \mathbb{Z}[i]$ دو عضو غیر یکال $\mathbb{Z}[i]$ هستند. با نرم گرفتن از دو طرف داریم:

$$p^۲ = N(\alpha)N(\beta)$$

چون $N(\alpha) \neq ۱$ و $N(\beta) \neq ۱$ (چرا؟) لذا $N(\alpha) = N(\beta) = p$. لذا با فرض

$$\alpha = a + bi \quad \text{و} \quad \beta = c + di$$

داریم

$$p = a^۲ + b^۲ = c^۲ + d^۲$$

که در آن $a, b, c, d \in \mathbb{Z}$. از آن‌جا که p فرد است، a و b نمی‌توانند هر دو زوج یا هر دو فرد باشند.
فرض کنیم a زوج و b فرد باشد. مثلاً $a = ۲k$ و $b = ۲l + ۱$. پس

$$p = a^۲ + b^۲ = ۴k^۲ + ۴l^۲ + ۴l + ۱ = ۴K' + ۱$$

لذا $p \equiv ۱(mod\ ۴)$.

برعکس فرض کنیم $p \equiv ۱(mmod\ ۴)$. نشان می‌دهیم p در $\mathbb{Z}[i]$ تحویل‌پذیر است. بنا به فرض $۴|p - ۱$. از آن‌جا که هر زیرگروه متناهی از گروه ضربی یک میدان دوری است(ثابت کردیم) پس $\mathbb{F}_p^*$ مولدی چون g دارد. پس مرتبه‌ی g برابر $p - ۱$ است. پس $g^{\frac{p-۱}{۴}} \in \mathbb{F}_p^*$ دارای مرتبه‌ی ۴ است. (دقت کنیم که بنا به فرض $\frac{p-۱}{۴}$ عددی صحیح است). لذا $a^۲ = g^{\frac{p-۱}{۲}} \in \mathbb{F}_p^*$ عضوی از مرتبه‌ی ۲ است.
از آن‌جا که تنها عضو مرتبه‌ی ۲ در $\mathbb{F}_p^*$ برابر -۱ است(چرا؟) لذا

$$a^۲ \equiv -۱(mod\ p)$$

بنابراین $p|a^۲ + ۱$. و لذا $p|(a - i)(a + i)$ (در حلقه‌ی $\mathbb{Z}[i]$).
اگر p در $\mathbb{Z}[i]$ تحویل‌ناپذیر باشد آن‌گاه pدر $\mathbb{Z}[i]$ اول است و لذا در $\mathbb{Z}[i]$ داریم $p|a - i$ یا $p|a + i$.
اگر $p|a + i$ آن‌گاه $a + i = p(c + di)$ که در آن $c + di \in \mathbb{Z}[i]$. پس $pb = ۱$ که غیر ممکن است.
پس p در $\mathbb{Z}[i]$ تحویل‌پذیر است. بنابراین ثابت کردیم:

قضیه ۱.۱۲ عدد اول $p \in \mathbb{Z}$ در $\mathbb{Z}[i]$ تحویل‌پذیر است اگر و تنها اگر $p \equiv ۱(mod\ ۴)$.

مثال ۱۳.۱ $(۲-i)(۲+i)=۵$، $(۴-i)(۴+i)=۱۷$، $(۳-۲i)(۳+۲i)=۱۳$ ولی ۳ و۷ در $\mathbb{Z}[i]$ تجزیه نمی‌شوند.

مثال ۱۴.۱ برای تجزیه‌ی $۲۱i+۹$ داریم

$$۹+۲۱i=۳(۳+۷i)$$

$$N(۳+۷i)=۵۸=۲\times ۲۹=(۱+i)(۱-i)(۵+۲i)(۵-۲i)$$

$$(۳+۷i)(۳-۷i)=(۱+i)(۱-i)(۵+۲i)(۵-۲i)$$

۴ عامل طرف راست آخرین تساوی تحویل‌ناپذیراند(چون نرم همه‌ی آن‌ها اول است). با عنایت به یکتایی تجزیه $۷i+۳$ و $۷i-۳$ هر دو تحویل‌پذیر اند. به‌راحتی دیده می‌شود که:

$$۹+۲۱i=۳(۳+۷i)=۳(۱+i)(۵+۲i)$$

توجه کنیم که ۳ در $\mathbb{Z}[i]$ نیز تحویل‌ناپذیر است.

§ تمرین

۱. فرض کنیم R یک حلقه‌ی اقلیدسی با تابع اقلیدسی φ باشد.

(الف) نشان دهید اگر $a\in R$ یکال نباشد، آن‌گاه $\varphi(a)>\varphi(۱)$.

(ب) نشان دهید اگر $a,b\in R$ شریک باشند آن‌گاه $\varphi(a)=\varphi(b)$

(ج) آیا عکس (ب) برقرار است؟ ثابت کنید.

۲. فرض کنیم R یک دامنه‌ی صحیح و $\varphi: R-\{۰\}\longrightarrow \mathbb{N}^*$ یک تابع باشد که در شرط (ب) از تعریف تابع اقلیدسی صدق می‌کند. ثابت کنید R یک دامنه‌ی اقلیدسی است.

۳. فرض کنیم $\alpha,\beta\in\mathbb{Z}[i]$. نشان دهید r و q یافت شده در تقسیم α بر β در حالت کلی منحصر به فرد نیست؟ حداکثر چند جواب برای q و r می‌تواند یافت شود؟

۴. نشان دهید اگر $\alpha \in \mathbb{Z}[i]$ و $N(\alpha)$ یک عدد اول باشد آن‌گاه α در $\mathbb{Z}[i]$ تحویل‌ناپذیر است.

۵. ۲۱، ۱۱۹، $۷ + ۵i$، $۶ + ۲۱i$ را در $\mathbb{Z}[i]$ به عوامل اول تجزیه کنید.

۶. نشان دهید حلقه‌ی $\mathbb{Z}[\sqrt{-۵}] = \{a + b\sqrt{-۵} \;:\; a, b \in \mathbb{Z}\}$ یک حلقه‌ی اقلیدسی نیست.

۷. (الف) فرض کنیم $p \in \mathbb{Z}$ یک عدد اول باشد. نشان دهید p را می‌توان به صورت مجموع مربعات دو عدد صحیح نوشت اگر و تنها اگر $p \equiv ۱ (mod\ ۴)$.

۸. نشان دهید اگر $p = a^۲ + b^۲ = c^۲ + d^۲$ که در آن a, b, c, d اعدادی صحیح هستند و $a < b$ و $c < d$ آن‌گاه $a = \pm c$ و $b = \pm d$.

۹. بزرگترین مقسوم علیه مشترک $۸ + ۶i$ و $۱۵i - ۵$ را در $\mathbb{Z}[i]$ بیابید.

۱۰. فرض کنیم $۰ \neq \alpha \in \mathbb{Z}[i]$. نشان دهید $\dfrac{\mathbb{Z}[i]}{\langle \alpha \rangle}$ یک حلقه‌ی متناهی است.

۱۱. (الف) نشان دهید $\mathbb{Z}[\sqrt{۲}] = \{a + b\sqrt{۲} \;:\; a, b \in \mathbb{Z}\}$ با تابع $\varphi(a + b\sqrt{۲}) = a^۲ - b^۲$ یک دامنه‌ی اقلیدسی است.

۱۲. (الف) نشان دهید $\mathbb{Z}[\sqrt{-۲}] = \{a + b\sqrt{-۲} \;:\; a, b \in \mathbb{Z}\}$ با تابع $\varphi(a + b\sqrt{-۲}) = a^۲ + b^۲$ یک دامنه‌ی اقلیدسی است.

فصل ۲
توسیع میدان‌ها و عناصر جبری

در این فصل به صورت دقیق‌تر به بررسی ریشه‌های یک چندجمله‌ای روی یک میدان می‌پردازیم.

تعریف ۱.۲ میدان E را یک توسیع میدان F گوییم هرگاه F یک زیرمیدان E باشد. در این صورت می‌نویسیم $F \leq E$. به عنوان مثال $\mathbb{R}$ یک توسیع $\mathbb{Q}$ و $\mathbb{C}$ یک توسیع $\mathbb{R}$ و یک توسیع $\mathbb{Q}$ است.

فرض کنیم $f(x)$ یک چندجمله‌ای روی میدان F از درجه‌ی n باشد. قبلاً ثابت کردیم $f(x)$ حداکثر n ریشه در F دارد. قضیه‌ی بعد می‌گوید که توسیعی از F مانند E وجود دارد که f در آن حداقل یک ریشه دارد.

قضیه ۲.۲ (کرونکر) فرض کنیم F یک میدان و $f(x)$ یک چندجمله‌ای غیرثابت در $F[x]$ باشد. در این صورت توسیعی از F مانند E و $\alpha \in E$ وجود دارد به نحوی که $f(\alpha) = 0$.

اثبات. ابتدا توجه کنیم که $f(x)$ را می‌توان به صورت حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر در $F[x]$ نوشت. فرض کنیم $p(x)$ یک چندجمله‌ای تحویل‌ناپذیر در $F[x]$ باشد که $f(x)$ را می‌شمارد.

کافیست Eو $\alpha \in E$ را بیابیم به نحوی که $p(\alpha) = ۰$.

$p(x)$ در $F[x]$ تحویل‌ناپذیر و لذا $\langle p(x) \rangle$ یک ایده‌آل ماکسیمال $F[x]$ و در نتیجه

$$E = \frac{F[x]}{\langle p(x) \rangle}$$

یک میدان است. نگاشت $\varphi : F \longrightarrow E$ با ضابطه‌ی $\varphi(a) = a + \langle p(x) \rangle$ یک همریختی است. این همریختی یک به یک است(ثابت کنید). لذا F با زیرمیدان $\varphi(F)$ از E یکریخت است. پس با یکی گرفتن Fو $\varphi(F)$ (ویکی گرفتن $\alpha \in F$ با $a + \langle p(x) \rangle \in E$) می‌توان F را زیرمیدانی از Eفرض کرد. حال قرار می‌دهیم $\alpha = x + \langle p(x) \rangle$. در این صورت $\alpha \in E$. فرض کنیم

$$p(x) = a_۰ + a_۱ x + \ldots + a_n x^n \in F[x], \ a_n \neq ۰$$

در این صورت

$$\begin{aligned} p(\alpha) &= a_۰ + a_۱ \alpha + a_۲ \alpha^۲ + \ldots + a_n \alpha^n \\ &= (a_۰ + \langle p(x) \rangle) + (a_۱ + \langle p(x) \rangle)(x + \langle p(x) \rangle) + \ldots + (a_n + \langle p(x) \rangle)(x + \langle p(x) \rangle)^n \\ &= (a_۰ + a_۱ x + \ldots + a_n x^n) + \langle p(x) \rangle = p(x) + \langle p(x) \rangle = \langle p(x) \rangle = O_E \end{aligned}$$

□

توجه کنیم که در تساوی‌های بالا از یکی گرفتن $a_i \in F$ با $a_i + \langle p(x) \rangle \in E$ استفاده کردیم.

تبصره ۳.۲ با علامات قضیه‌ی بالا، چون α ریشه‌ی $f(x)$ در E است پس اگر $f(x)$ از درجه‌ی $m \geq ۱$ باشد، آن‌گاه

$$f(x) = (x - \alpha) g(x)$$

که در آن $g(x) \in E[x]$ و $g(x)$ از درجه‌ی $m - ۱$ است. با به‌کار بردن قضیه‌ی فوق این بار برای g می‌توان توسیع $E_۲$ از E و $\alpha_۲ \in E_۲$ یافت به نحوی که $g(\alpha_۲) = ۰$. با ادامه‌ی این روند توسیع‌های $E_۱ = E, E_۲, \ldots, E_n$ به صورت زیر بدست می‌آیند:

$$F \leq E_۱ \leq E_۲ \leq \ldots \leq E_n$$

و در E_nداریم

$$f(x) = (x - \alpha)(x - \alpha_۲)\ldots(x - \alpha_n)$$

لذا E_n توسیعی از F است که fدر آن دقیقاً n ریشه(نه لزوماً متمایز) دارد.

مثال ۴.۲ $f(x) = x^۲ + ۱ \in \mathbb{R}[x]$ را در نظر بگیرید. $f(x)$روی $\mathbb{R}$تحویل‌ناپذیر است. و لذا

$$E = \frac{\mathbb{R}}{\langle (x^۲ + ۱) \rangle}$$

یک میدان است. حال با فرض $\alpha = x + \langle x^۲ + ۱ \rangle$ و یکی گرفتن $۱ \in \mathbb{R}$ با $۱ + \langle ^۲+۱ \rangle \in E$ داریم

$$\alpha^۲ + ۱ = (x + \langle ^۲+۱ \rangle)^۲ + (۱ + \langle ^۲+۱ \rangle) = x^۲ + ۱ + \langle ^۲+۱ \rangle = \langle ^۲+۱ \rangle = O_E$$

پس α یک ریشه‌ی $f(x)$ در E است.

اگر $u \in E$ دلخواه باشد آن‌گاه $u = g(x) + \langle x^۲ + ۱ \rangle$ که در آن $g(x) \in \mathbb{R}[x]$. با تقسیم $g(x)$در $x^۲ + ۱$ در $\mathbb{R}[x]$(بنابر الگوریتم تقسیم)

$$g(x) = q(x)(x^۲ + ۱) + r(x)$$

که در آن $q(x), r(x) \in \mathbb{R}[x]$ و $r(x) = ۰$ یا $r(x)$ از درجه‌ی حداکثر۱ است. پس

$$r(x) = a + bx \quad (a, b \in \mathbb{R})$$

لذا

$$u = g(x) + \langle x^۲ + ۱ \rangle = (a + bx) + \langle x^۲ + ۱ \rangle =$$

$$(a + \langle x^۲ + ۱ \rangle) + (b + \langle x^۲ + ۱ \rangle)(x + \langle x^۲ + ۱ \rangle) = a + b\alpha$$

بنابراین

$$E = \{a + b\alpha : \ a, b \in \mathbb{R}\}$$

و از طرف دیگر $\alpha^{۲} = -۱$ لذا با نام‌گذاری α با i میدان E همان $\mathbb{C}$، میدان اعداد مختلط است.

با عنایت به اهمیت ریشه‌ی چندجمله‌ای‌ها تعریف زیر را در نظر می‌گیریم.

تعریف ۵.۲ فرض کنیم E یک توسیع میدان F باشد و $\alpha \in E$. گوییم α روی F جبری است هرگاه چندجمله‌ای ناصفر $f(x) \in F[x]$ موجود باشد به نحوی که $f(\alpha) = ۰$. اگر α روی F جبری نباشد گوییم α روی Fمتعالی(غیرجبری) است. اگر هر عضو E روی F جبری باشد، گوییم E یک توسیع جبری F است.

مثال ۶.۲ $\sqrt{۲} \in \mathbb{R}$ روی جبری است. زیرا ریشه ی چندجمله ای $x^{۲} - ۲ \in \mathbb{Q}[x]$ است.

$i \in \mathbb{C}$ روی $\mathbb{Q}$ جبری است. زیرا ریشه‌ی $x^{۲} + ۱ \in \mathbb{Q}[x]$ است.

$\pi \in \mathbb{R}$ روی $\mathbb{R}$ جبری است. زیرا ریشه‌ی $x - \pi \in \mathbb{R}[x]$ است. ولی می‌توان ثابت کرد که π روی $\mathbb{Q}$ جبری نیست.

مثال ۷.۲ $\sqrt{۲} + \sqrt{۳} \in \mathbb{R}$ روی $\mathbb{Q}$ جبری است. برای دیدن این قرار دهید $u = \sqrt{۲} + \sqrt{۳}$. در این صورت

$$u^{۲} = ۵ + ۲\sqrt{۶}$$

$$u^{۲} - ۵ = ۲\sqrt{۶}$$

$$(u^{۲} - ۵)^{۲} = ۲۴$$

$$u^{۴} - ۱۰u^{۲} + ۱ = ۰$$

لذا$\sqrt{۳} + \sqrt{۲}$ یک ریشه‌ی چندجمله‌ای $f(x) = x^{۴} - ۱۰x^{۲} + ۱$ است.(ثابت کنید این چندجمله‌ای روی $\mathbb{Q}$ تحویل‌ناپذیر است.)

تعریف ۸.۲ عدد $\alpha \in \mathbb{C}$ را یک عدد جبری می‌گوییم هرگاه روی $\mathbb{Q}$ جبری باشد. در غیر این صورت آن را یک عدد متعالی گوییم.

اعداد گویا، اعدادی که رادیکال اعداد گویا هستند مانند $\sqrt{۲}$، $\sqrt{۱+\sqrt[۳]{۵}}$، $\sqrt{\sqrt{۲}+\sqrt[۳]{۷}}$ و ... اعداد جبری هستند. با وجود این مجموعه‌ی اعداد جبری مجموعه‌ای شماراست.(ثابت کنید). بنابراین مجموعه‌ی اعداد متعالی ناشماراست. اعدادی مانند e، $e^{۲}$، π و ....

حال فرض کنیم E یک توسیع F و $\alpha \in E$ روی Fجبری باشد. در این صورت به تعداد نامتناهی چندجمله‌ای در $F[x]$ موجود است که α ریشه‌ی آن است. فرض کنیم $p(x)$ یک چندجمله‌ای تکین در $F[x]$ باشد به نحوی که $p(\alpha) = ۰$ و درجه‌ی p کمترین مقدار ممکن را داشته باشد. این چندجمله‌ای منحصر به فرد است. زیرا اگر $q(x)$ یک چندجمله‌ای تکین دلخواه در $F[x]$ با کمترین درجه باشد، آن‌گاه بنابر الگوریتم تقسیم در $F[x]$،

$$q(x) = f(x)p(x) + r(x)$$

که در آن $f(x), r(x) \in F[x]$ و $r(x) = ۰$ یا $deg\ r(x) < deg\ p(x)$. حال

$$r(\alpha) = q(\alpha) - f(\alpha)p(\alpha) = ۰$$

فرض کنیم $r(x) \neq ۰$. در این صورت با ضرب $r(x)$ در وارون ضریب پیشروش، چندجمله‌ای تکین $r_۱(x)$ بدست می‌آید به نحوی که $r_۱(\alpha) = ۰$. این با انتخاب $p(x)$ متناقض است زیرا $deg\ r_۱(x) < deg\ p(x)$. پس $r(x) = ۰$ و لذا

$$q(x) = f(x)p(x)$$

از آن‌جا که $p(x)$ و $q(x)$ دارای درجه‌ی مساوی و لذا $f(x) = c \in F$ یک چندجمله‌ای ثابت است. حال از تکین بودن $p(x)$ و $q(x)$ نتیجه می‌شود که $c = ۱$ و لذا $p(x) = q(x)$. لذا می‌توان تعریف زیر

را ارائه نمود.

تعریف ۹.۲ فرض کنیم E یک توسیع F و $\alpha \in E$ روی Fجبری باشد. چندجمله‌ای تکین $p(x) \in F[x]$ را چندجمله‌ای مینیمال α روی F می‌گوییم هرگاه $p(\alpha) = ۰$ و $p(x)$ دارای کمترین درجه‌ی ممکن باشد.

تبصره ۱۰.۲ توجه کنیم که با تغییر F چندجمله‌ای مینیمال α روی F نیز ممکن است تغییر کند. مثلاً $p(x) = x^۲ + ۱$ چندجمله‌ای مینیمال $i \in \mathbb{C}$ روی $\mathbb{Q}$ است. $p(x)$ چندجمله‌ای مینیمال i روی $\mathbb{R}$ نیز هست. ولی چندجمله‌ای مینیمال i روی $\mathbb{C}$ برابر $x - i \in \mathbb{C}[x]$ است. توجه کنید که $x - i \notin \mathbb{R}[x]$.

نمادگذاری ۱۱.۲ با توجه به توضیحات قبل از تعریف، چندجمله‌ای مینیمال α روی F منحصر به فرد است. و آن‌را با $p_{\alpha,F}(x)$ یا $irr(\alpha, F)$ و در صورتی که F مشخص باشد و ابهامی پیش نیاید، آن‌را با $p_\alpha(x)$ نمایش می‌دهیم.

برخی خواص جالب و مفید چندجمله‌ای مینیمال در قضیه‌ی ذیل ارائه گردیده‌اند:

قضیه ۱۲.۲ فرض کنیم E یک توسیع Fو $\alpha \in E$ روی F جبری و $p(x)$ چندجمله‌ای مینیمال α روی F باشد. در این صورت«

(الف) $p(x)$ در $F[x]$ تحویل‌ناپذیر است.

(ب) اگر $f(x) \in F[x]$ و $f(\alpha) = ۰$ آن‌گاه $p(x)|f(x)$(در $F[x]$).

(ج) اگر $f(x) \in F[x]$ یک چندجمله‌ای تکین و تحویل‌ناپذیر در $F[x]$ باشد و $f(\alpha) = ۰$ آن‌گاه $f(x) = p(x)$.

اثبات. (الف) اگر $p(x)$ در $F[x]$ تحویل‌پذیر باشد آن‌گاه می‌توان $p(x)$ را به صورت

$$p(x) = g(x)h(x)$$

نوشت که در آن $g(x), h(x) \in F[x]$ دو چندجمله‌ای تکین با درجه‌ی کمتر از درجه‌ی $p(x)$ هستند. از $g(\alpha), h(\alpha) \in E$ و $p(\alpha) = g(\alpha)h(\alpha) = ۰$ نتیجه می‌شود که $g(\alpha) = ۰$ یا $h(\alpha) = ۰$ و این متناقض با مینیمال بودن $p(x)$ است.

(ب) با تقسیم $f(x)$ بر $p(x)$ داریم $f(x) = q(x)p(x) + r(x)$ که در آن $q(x), r(x) \in F[x]$ و $r(x) = ۰$ یا $deg\ r(x) < deg\ p(x)$. داریم:

$$r(\alpha) = f(\alpha) - q(\alpha)p(\alpha) = ۰$$

اگر $r(x) \neq ۰$، با ضرب $r(x)$ در وارون ضریب پیشرو خودش چندجمله‌ای تکین $r_۱(x) \in F[x]$ بدست می‌آید به نحوی که $r_۱(\alpha) = ۰$. و این متناقض با مینیمال بودن $p(x)$ است زیرا $deg\ r_۱(x) < deg\ p(x)$. پس $r(x) = ۰$ و لذا $p(x)|f(x)$.

(ج) از (ب) نتیجه می‌شود که $p(x)|f(x)$ چون بنا به فرض $f(x)$ نیز تحویل‌ناپذیر است نتیجه می‌شود که $f(x) = cp(x)$ که در آن $۰ \neq c \in F[x]$. حال از تکین بودن $p(x)$ و $f(x)$ نتیجه می‌شود که $c = ۱$ و لذا $f(x) = p(x)$. □

تبصره ۱۳.۲ با توجه به قضیه‌ی بالا چندجمله‌ای مینیمال $\alpha \in E$ روی F ($F \leq E$) تحویل‌ناپذیر است و بالعکس هر چندجمله‌ای تکین تحویل‌ناپذیر $f(x) \in F[x]$ که در شرط $f(\alpha) = ۰$ صدق کند، با چندجمله‌ای تحویل‌ناپذیر α روی F مساوی است. به همین دلیل چندجمله‌ای تحویل‌ناپذیر α روی F را چندجمله‌ای تحویل‌ناپذیر α روی F نیز گوییم. در واقع چندجمله‌ای مینیمال α روی F را می‌توان به صورت زیر نیز تعریف کرد:

تعریف ۱۴.۲ فرض کنیم E توسیع Fو $\alpha \in E$ روی Fجبری باشد. در این صورت چندجمله‌ای تکین تحویل‌ناپذیر $p(x) \in F[x]$ را که در شرط $p(\alpha) = \circ$ صدق می‌کند، چندجمله‌ای مینیمال α رویF(یا چندجمله‌ای تحویل‌ناپذیر α روی F) گوییم و با $p_{\alpha,F}(x)$ یا $irr(\alpha, F)$ نمایش می‌دهیم. توجه کنیم که از قضیه‌ی قبل نتیجه می‌شود که این چندجمله‌ای منحصر به فرد است.

تعریف ۱۵.۲ فرض کنیم E یک توسیع F و $\alpha \in E$ روی F جبری و چندجمله‌ای مینیمال α روی F از درجه‌ی n باشد. در این صورت گوییم α روی F جبری از درجه‌ی n است، یا درجه‌ی جبری بودن α روی F برابر n است، یا درجه‌ی α روی F برابر n است.

مثال ۱۶.۲ $\alpha = i\sqrt[۴]{۲} \in \mathbb{C}$ یک ریشه‌ی $p(x) = x^۴ - ۲$ است. این چندجمله‌ای روی $\mathbb{Q}$ تحویل‌ناپذیر است. پس $p(x)$ چندجمله‌ای مینیمال α روی $\mathbb{Q}$، و لذا α روی $\mathbb{Q}$ جبری از درجه‌ی ۴ است. روی $\mathbb{R}$ داریم:

$$x^۴ - ۲ = (x^۲ - \sqrt{۲})(x^۲ + \sqrt{۲})$$

α ریشه‌ی $x^۲ + \sqrt{۲}$ و این چندجمله‌ای روی $\mathbb{R}$ تحویل‌ناپذیر و لذا α روی $\mathbb{R}$ جبری از درجه‌ی ۲ است. نهایتاً روی $\mathbb{C}$

$$x^۲ + \sqrt{۲} = (x - i\sqrt[۴]{۲})(x + i\sqrt[۴]{۲})$$

و α ریشه‌ی $x - i\sqrt[۴]{۲}$ و لذا α روی $\mathbb{C}$ جبری از درجه‌ی ۱ است.

۱.۲ میدان‌های میانی و تولید شده

فرض کنیم Kیک توسیع E و E یک توسیع F باشد. در این صورت K یک توسیع F نیز هست. E را یک میدان میانی F و Kگوییم. در این فصل به مطالعه‌ی میدان‌های میانی می‌پردازیم. ابتدا توجه کنیم که اگر E یک توسیع F باشد، و $a \in F$ و $u \in E$، آن‌گاه با ضرب a و u به عنوان دو عضو از E داریم $au \in E$. به آسانی می‌توان دید که با این ضرب، E یک فضای برداری روی F است. این مشاهده ما را قادر می‌سازد که در ادامه‌ی کار مفاهیم جبرخطی را به کمک بگیریم. خواهیم دید که این ابزار بسیار کارآمد است. ابتدا به تعریف زیر توجه کنید.

تعریف ۱۷.۲ (درجه‌ی یک توسیع): فرض کنیم E یک توسیع F باشد. بعد فضای برداری E روی میدان F را درجه‌ی E روی F گوییم و با $[E:F]$ نمایش می‌دهیم. اگر $[E:F]$ متناهی باشد آن‌گاه توسیع را از درجه‌ی متناهی گوییم و به‌طور خلاصه می‌گوییم E یک توسیع متناهی F است. اگر $[E:F]$ بی‌نهایت باشد E را یک توسیع نامتناهی F گوییم.

توجه کنیم که جمله‌ی "E توسیع متناهی F است." بدین معنی نیست که E متناهی است.

مثال ۱۸.۲ $\mathbb{C}$ یک توسیع متناهی از $\mathbb{R}$ است. زیرا $\{۱, i\}$ یک پایه‌ی $\mathbb{C}$روی $\mathbb{R}$ است. لذا

$$[\mathbb{C}:\mathbb{R}] = ۲.$$

همچنین اگر قرار دهیم $\mathbb{Q}(\sqrt{۲}) = \{a + b\sqrt{۲} : \ a.b \in \mathbb{Q}\}$ در این صورت $\mathbb{Q}(\sqrt{۲})$ یک زیرمیدان $\mathbb{R}$ است(ثابت کنید) و $[\mathbb{Q}(\sqrt{۲}) : \mathbb{Q}] = ۲$.

به عنوان اولین کاربرد جبرخطی به قضیه‌ی زیر توجه کنید که به قضیه‌ی برج معروف است.

قضیه ۱۹.۲ (قضیه‌ی برج): فرض کنیم K یک توسیع E و E یک توسیع F باشد. یعنی

$$F \leq E \leq K.$$

K یک توسیع متناهی F است، اگر وتنها اگر K توسیع متناهی E و E یک توسیع متناهی Fباشد. و در این صورت:

$$[K:F]=[K:E][E:F]$$

اثبات. فرض کنیم Kیک توسیع متناهی F باشد. در این صورت E یک زیرفضای K(به عنوان فضای برداری روی F) است و لذا از بعد متناهی است و $[E:F]\leq[K:F]$. از طرف دیگر اگر $\{w_1,w_2,\dots,w_t\}$ یک پایه‌ی K روی F باشد، آن‌گاه هر عضو Kیک ترمیب خطی از $w_1,\dots,w_t$ با ضرایب در F است. این ضرایب در E نیز هستند. پس هر عضو Kیک ترکیب خطی از $w_1,w_2,\dots,w_t$ با ضرایب در E است. لذا $w_1,w_2,\dots,w_t$فضای K را به عنوان فضای برداری روی E می‌پیماید. پس

$$[K:E]\leq t=[K:F]$$

و لذا $[K:E]$ نیز متناهی است.

برعکس، فرض کنیم Kیک توسیع متناهی E و E یک توسیع متناهی Fباشد. فرض کنیم $u_1,u_2,\dots,u_m\in K$ یک پایه‌ی K روی E و فرض کنیم $v_1,v_2,\dots,v_n\in E$ یک پایه‌ی E روی F باشد. حال $u\in K$ را دلخواه در نظر بگیرید. در این صورت $u_1,u_2,\dots,u_m$ یک پایه‌ی Kروی E است لذا،

$$u=b_1u_1+b_2u_2+\dots+b_mu_m,\qquad b_i\in E,\ i=1,2,\dots,m$$

از طرف دیگر $v_1,v_2,\dots,v_n$ یک پایه‌ی E روی F است و لذا برای هر $1\leq i\leq m$،

$$b_i = a_{i۱}v_۱ + a_{i۲}v_۲ + \ldots + a_{in}v_n, \quad a_{ij} \in F, \ \ j = ۱, ۲, \ldots, n$$

بنابراین

$$u = \sum_{j=۱}^{m} b_i u_i = \sum_{i=۱}^{m} (\sum_{j=۱}^{n} a_{ij}v_j)u_i = \sum_{i=۱}^{m}\sum_{j=۱}^{n} a_{ij}(u_iv_j).$$

بنابراین مجموعه‌ی $\{u_iv_j \ : \ ۱ \leq i \leq m, \ ۱ \leq j \leq n\}$ فضای Kرا روی Fمی‌پیماید. از طرف دیگر فرض کنیم $\sum_{۱\leq i\leq m, ۱\leq j\leq n} a_{ij}(u_iv_j) = ۰$ و برای $۱ \leq j \leq n$، $۱ \leq i \leq m$، $a_{ij} \in F$. در این صورت

$$\sum_{i=۱}^{m} (\sum_{j=۱}^{n} (a_{ij}v_j))u_i = ۰$$

در این صورت برای هر $۱ \leq i \leq m$ قرار می‌دهیم $b_i = \sum_{j=۱}^{n} a_{ij}v_j \in E$. لذا

$$\sum_{i=۱}^{m} b_iu_i = ۰$$

چون $b_i \in E$ برای هر $۱ \leq i \leq n$ و $u_۱, u_۲, \ldots, u_m \in K$ روی E مستقل‌اند، لذا

$$b_۱ = b_۲ = \ldots = b_m = ۰$$

حال برای هر $۱ \leq i \leq m$ داریم

$$\sum_{j=۱}^{n} a_{ij}v_j = b_i = ۰$$

از استقلال خطی $v_۱, v_۲, \ldots, v_n \in E$ روی F نتیجه می‌شود که

$$a_{i۱} = a_{i۲} = \ldots = a_{in} = ۰$$

بنابراین ثابت کردیم برای هر $۱ \leq i \leq m$ و $۱ \leq j \leq n$، $a_{ij} = ۰$. بنابراین مجموعه‌ی

$$\{u_iv_j \ \ ۱ \leq i \leq m, \ ۱ \leq j \leq n\}$$

روی F مستقل خطی و بنابراین یک پایه روی F است. این پایه دارای mn عضو است. پس

$$[K : F] = mn = [K : E][E : F].$$

□

فرض کنیم K یک توسیع F باشد و $\alpha \in K$. میدان‌های میانی K و F وجود دارند که شامل α هستند. مثلاً K خود یک میدان میانی K و F است که α را در بر دارد. اما کوچکترین میدان میانی شامل α چیست؟ فرض کنیم E کوچکترین توسیع میانی شامل α باشد. پس $F \leq E \leq K$ و $\alpha \in E$. دقت کنید که E وجود دارد و در واقع اشتراک همه‌ی میدان‌های میانی Kو F است که شامل α هستند.

تعریف ۲۰.۲ فرض کنیم K یک توسیع F باشد. ($F \leq K$) و فرض کنیم $S \subseteq E$ یک مجموعه باشد.

(الف) یک زیرحلقه از K که شامل F است را یک حلقه‌ی میانی K و F می‌گوییم.

(ب) یک زیرمیدان از Kکه شامل F است را یک میدان میانی K و F می‌گوییم.

(ج) کوچکترین زیرحلقه‌ی K که شامل F و S است را حلقه‌ی میانی تولید شده توسط S روی F می‌نامیم، و با $F[S]$ نمایش می‌دهیم.

(د) کوچکترین زیرمیدان K که شامل F و S است را میدان میانی تولید شده توسط S روی F می‌نامیم، و با $F(S)$ نمایش می‌دهیم.

فرض کنیم

$$\mathcal{R} = \{R : \text{ زیرحلقه‌ی } K \text{ است که شامل } S \text{ و } F \text{ می‌باشد } R\}$$

$$\mathcal{L} = \{L : \text{ زیرمیدان } K \text{ است که شامل } S \text{ و } F \text{ می‌باشد } L\}$$

$\mathcal{R}$ و $\mathcal{L}$ ناتهی هستند. زیرا K در هر دو قرار دارد. از طرف دیگر به وضوح $\mathcal{L} \subseteq \mathcal{R}$، زیرا هر زیرمیدان Kیک زیر حلقه‌ی K نیز هست. از آن‌جا که اشتراک زیرحلقه‌ها یک زیرحلقه و اشتراک زیرمیدان‌ها

یک زیرمیدان است لذا اشتراک اعضای $\mathcal{R}$ در واقع کوچکترین زیرحلقه‌ی Kاست که شامل F و S است. یعنی

$$F[S] = \bigcap_{R \in \mathcal{R}} R$$

به طریق مشابه

$$F(S) = \bigcap_{L \in \mathcal{L}} L$$

به علاوه از $\mathcal{L} \subseteq \mathcal{R}$ نتیجه می‌شود که

$$F[S] \subseteq F(S)$$

در حالتی که $S = \{\alpha_۱, \alpha_۲, \ldots, \alpha_n\}$ یک مجموعه‌ی متناهی است، $F[S]$ و $F(S)$ را به ترتیب به صورت $F[\alpha_۱, \alpha_۲, \ldots, \alpha_n]$ و $F(\alpha_۱, \alpha_۲, \ldots, \alpha_n)$ نمایش می‌دهیم.
تعاریف بالا از $F[S]$ و $F(S)$ اعضای مجموعه‌ها را معرفی نمی‌کند. برای سادگی ابتدا حالتی را در نظر بگیرید که S مجموعه‌ی تک عضوی $S = \{\alpha\}$ باشد که $\alpha \in K$. حلقه‌ی $F[\alpha]$ شامل α است و لذا برای هر عدد طبیعی n،

$$\alpha, \alpha^۲, \alpha^۳, \ldots, \alpha^n \in F[\alpha]$$

می‌باشد. اگر $a_۰, a_۱, \ldots, a_n \in F$، آن‌گاه از این‌که $F \subseteq F[\alpha]$ نتیجه می‌شود

$$a_۰ + a_۱\alpha + a_۲\alpha^۲ + \ldots + a_n\alpha^n \in F[\alpha]$$

این‌ها در واقع همه‌ی اعضای $F[\alpha]$ هستند. زیرا داریم:

قضیه ۲۱.۲ فرض کنیم K یک توسیع F و $\alpha \in K$. در این صورت

$$F[\alpha] = \{f(\alpha) :\ f(x) \in F[x]\}$$

اثبات. قرار دهیم $R = \{f(\alpha) :\ f(x) \in F[x]\}$. با توجه به توضیح قبل از قضیه داریم

$$R \subseteq F[\alpha]$$

به‌راحتی می‌توانید ببینید که R خود یک حلقه است که شامل α و F است. لذا با توجه به تعریف $F[\alpha]$ داریم :

$$F[\alpha] \subseteq R$$

و اثبات تمام است. $\square$

در مورد $F(\alpha)$ چه می‌توان گفت؟ دیدیم که $F[\alpha] \subseteq F(\alpha)$. اگر $f(x), g(x) \in F[x]$، آن‌گاه $f(\alpha), g(\alpha) \in F[\alpha]$. و لذا اگر $g(\alpha) \neq ۰$،آن‌گاه وارون $g(\alpha)$ نیز در $F(\alpha)$ است.(چون $F(\alpha)$ یک میدان است.) پس $\frac{f(\alpha)}{g(\alpha)} = f(\alpha)(g(\alpha))^{-۱} \in F(\alpha)$. این‌ها در واقع همه‌ی اعضای $F(\alpha)$ هستند. زیرا داریم:

قضیه ۲۲.۲ داریم

$$F(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : \ f(x), g(x) \in F[x], \ g(\alpha) \neq ۰\}$$

اثبات. قرار دهید

$$E = \{\frac{f(\alpha)}{g(\alpha)} : \ f(x), g(x) \in F[x], \ g(\alpha) \neq ۰\}$$

مشابه اثبات قضیه‌ی قبل به راحتی دیده می‌شود که $F(\alpha) = E$. $\square$

در حالت کلی‌تر داریم:

قضیه ۲۳.۲ فرض کنیم Kیک توسیع F باشد و $\alpha_۱, \alpha_۲, \ldots, \alpha_n \in K$ و $S \subseteq K$. در این صورت:

$$F[\alpha_۱, \alpha_۲, \ldots, \alpha_n] = \{f(\alpha_۱, \alpha_۱, \ldots, \alpha_n) :\ f(x_۱, x_۲, \ldots, x_n) \in F[x_۱, x_۲, \ldots, x_n]\}$$

$$F(\alpha_۱, \alpha_۲, \ldots, \alpha_n) = \{\frac{f(\alpha_۱, \alpha_۲, \ldots, \alpha_n)}{g(\alpha_۱, \alpha_۲, \ldots, \alpha_n)} :\ f(x_۱, x_۲, \ldots, x_n), g(x_۱, x_۲, \ldots, x_n) \in F[x_۱, x_۲, \ldots, x_n],\ g(\alpha_۱, \alpha_۲, \ldots, \alpha_n) \neq ۰\}$$

$$F[S] = \{f(\beta_۱, \beta_۲, \ldots, \beta_m) : f \in F[x_۱, x_۲, \ldots, x_m]; m \in \mathbb{N}^*, \beta_۱, \beta_۲, \ldots, \beta_m \in S\}$$

$$F(S) = \{\frac{f(\beta_۱, \beta_۲, \ldots, \beta_m)}{g(\beta_۱, \beta_۲, \ldots, \beta_m)} :\ f(x_۱, x_۲, \ldots, x_m), g(x_۱, x_۲, \ldots, x_m) \in F[x_۱, x_۲, \ldots, x_m],\ g(\beta_۱, \beta_۲, \ldots, \beta_m) \neq ۰\}$$

اثبات. اثبات مشابه دو قضیه‌ی قبل است. □

مثال ۲۴.۲ توسیع $\mathbb{Q} \subseteq \mathbb{R}$ و $\sqrt{۲} \in \mathbb{R}$ را در نظر بگیرید. در این صورت

$$\mathbb{Q}[\sqrt{۲}] = \{f(\sqrt{۲}) :\ f(x) \in \mathbb{Q}[x]\}$$

$$\mathbb{Q}(\sqrt{۲}) = \{\frac{f(\sqrt{۲})}{g(\sqrt{۲})} :\ f(x), g(x) \in \mathbb{Q}[x],\ \ g(sqrt۲) \neq ۰\}$$

اگر $u \in \mathbb{Q}[\sqrt{۲}]$ دلخواه باشد آن‌گاه $u = f(\alpha)$ که در آن $f(x) \in \mathbb{Q}[x]$. بنابر الگوریتم تقسیم در $\mathbb{Q}[x]$، $a, b \in \mathbb{Q}$ و $f(x) = (x^۲ - ۲)g(x) + a + bx$. بنابراین $f(\sqrt{۲}) = a + b\sqrt{۲}$. بنابراین

$$\mathbb{Q}[\sqrt{۲}] = \{a + b\sqrt{۲} :\ a, b \in \mathbb{Q}\}$$

به طریق مشابه

$$\mathbb{Q}(\sqrt{۲}) = \{\frac{a + b\sqrt{۲}}{c + d\sqrt{۲}} :\ a, b, c, d \in \mathbb{Q} \ \text{و}\ \ c + d\sqrt{۲} \neq ۰\}$$

بیش از این نیز می‌توان گفت:

$$\frac{a+b\sqrt{۲}}{c+d\sqrt{۲}}=\frac{(a+b\sqrt{۲})(c-d\sqrt{۲})}{c^{۲}-۲d^{۲}}=\frac{ac-۲bd}{c^{۲}-۲d^{۲}}+\frac{bc-ad}{c^{۲}-۲d^{۲}}\sqrt{۲}\in\mathbb{Q}[\sqrt{۲}]$$

بنابراین $\mathbb{Q}[\sqrt{۲}]=\mathbb{Q}(\sqrt{۲})$. یعنی برای هر عضو $\frac{f(\sqrt{۲})}{g(\sqrt{۲})}\in\mathbb{Q}(\sqrt{۲})$ می‌توان مخرج را به ۱ تبدیل کرد. این اتفاقی نیست. قضیه‌ی زیر نشان می‌دهد که تساوی $\mathbb{Q}(\sqrt{۲})$ با $\mathbb{Q}[\sqrt{۲}]$ نتیجه‌ای از جبری بودن $\sqrt{۲}$ روی $\mathbb{Q}$ است.

قضیه ۲۵.۲ فرض کنیم E یک توسیع F و $\alpha\in E$ روی F جبری از درجه‌ی n با چندجمله‌ای مینیمال $p(x)\in F[x]$ روی F باشد. در این صورت

(الف) $F(\alpha)=F[\alpha]$

(ب) $[F(\alpha):F]=n$ و $۱,\alpha,\alpha^{۲},\dots,\alpha^{n-۱}$ یک پایه‌ی $F(\alpha)$ روی F است. یعنی هر عنصر $u\in F(\alpha)$ نمایشی منحصر به فرد به صورت $u=a_{۰}+a_{۱}\alpha+\dots+a_{n-۱}\alpha^{n-۱}$ دارد که در آن $a_{۰},a_{۱},\dots,a_{n-۱}\in F$.

اثبات. (الف) نگاشت $\varphi_\alpha:F[x]\longrightarrow E$ که در آن برای هر $f(x)\in F[x]$، $\varphi_\alpha(f(x))=f(\alpha)$ یک همریختی حلقه‌هاست. فرض کنیم I هسته‌ی این همریختی باشد. بنابر قضیه‌ی؟،

$$I=\langle p(x)\rangle$$

از طرفی بنابر قضیه‌ی ؟ $p(x)$ در $F[x]$ تحویل‌ناپذیر است. لذا $F[x]/\langle p(x)\rangle$ یک میدان است. از طرف دیگر بنابر قضیه‌ی اول یکریختی

$$\frac{F[x]}{\langle p(x)\rangle}\cong\varphi_\alpha(F[x])$$

همچنین

$$\varphi_\alpha(F[x])=\{f(\alpha):\ f(x)\in F[x]\}=F[\alpha]$$

بنابراین $F[\alpha]$ یک میدان است. از آن‌جا که $F(\alpha)$ کوچکترین میدان شامل α و F است، داریم $F(\alpha)\subseteq F[\alpha]$. از طرفی همواره داریم $F[\alpha]\subseteq F(\alpha)$. پس

$$F(\alpha) = F[\alpha].$$

(ب) فرض کنیم $u \in F(\alpha)$ دلخواه باشد. بنابر (الف)، $u = f(\alpha)$ برای یک $f(x) \in F[x]$. با تقسیم $f(x)$ بر $p(x)$ در $F[x]$ داریم

$$f(x) = q(x)p(x) + r(x)$$

که در آن $q(x), r(x) \in F[x]$ و $r(x) = \circ$ یا $r(x)$ یک چندجمله‌ای از درجه‌ی کمتر از n است. لذا $a_\circ, a_۱, \ldots, a_{n-۱} \in F$ و $r(x) = a_\circ + a_۱x + a_۲x^۲ + \ldots + a_{n-۱}x^{n-۱}$. حال داریم

$$u = f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = a_\circ + a_۱\alpha + \ldots + a_{n-۱}\alpha^{n-۱}.$$

یعنی u یک ترکیب خطی از $۱, \alpha, \alpha^۲, \ldots, \alpha^{n-۱}$ با ضرایب در F است. از طرف دیگر فرض کنیم

$$b_\circ + b_۱\alpha + \ldots + b_{n-۱}\alpha^{n-۱} = \circ \quad \text{و} \quad b_\circ, b_۱, \ldots, b_{n-۱} \in F$$

در این صورت با فرض $g(x) = b_\circ + b_۱x + b_۲x^۲ + \ldots + b_{n-۱}x^{n-۱}$ داریم $g(\alpha) = \circ$. از این، با توجه به قضیه‌ی ؟؟، $p(x)|g(x)$. لذا $g(x) = p(x)h(x)$ برای یک $h(x) \in F[x]$. اگر $h(x) \neq \circ$ آن‌گاه درجه‌ی $g(x)$ بزرگتر یا مساوی درجه‌ی $p(x)$ یعنی n است که غیر ممکن است. پس $h(x) = \circ$ و لذا $g(x) = \circ$. یعنی $b_\circ = b_۱ = \ldots, b_{n-۱} = \circ$. از این نتیجه‌می‌شود که $۱, \alpha, \alpha^۲, \ldots, \alpha^{n-۱}$ روی F مستقل خطی هستند. پس $۱, \alpha, \alpha^۲, \ldots, \alpha^{n-۱}$ یک پایه‌ی $F(\alpha)$ روی F است و $[F(\alpha) : F] = n$.

□

مثال ۲۶.۲ قرار دهید $w = e^{\frac{۲\pi i}{۵}} = cos\frac{۲\pi}{۵} + isin\frac{۲\pi}{۵}$. در این صورت $w^۵ = ۱$ و لذا w یک ریشه‌ی چندجمله‌ای $p(x) = x^۵ - ۱$ است. $p(x)$ روی $\mathbb{Q}$ تجویل‌ناپذیر است(چرا؟). پس $p(x)$ یک چندجمله‌ای مینیمال w روی $\mathbb{Q}$است. لذا $[\mathbb{Q}[w] : \mathbb{Q}] = ۴$ و $۱, w, w^۲, w^۳$ یک پایه‌ی $\mathbb{Q}(w$ روی $\mathbb{Q}$ است. یعنی

$$\mathbb{Q}(w) = \{a_۰ + a_۱w + a_۲w^۲ + a_۳w^۳ :\ a_۰, a_۱, a_۲, a_۳ \in \mathbb{Q}\}$$

چون $w \in \mathbb{Q}(w)$ لذا $u = w + w^۴ + w^۵ \in \mathbb{Q}(w)$. می‌خواهیم u را به صورت ترکیب خطی $۱, w, w^۲, w^۳$ بنویسیم. داریم $w^۵ = ۱$ و $p(w) = ۱ + w + w^۲ + w^۳ + w^۴ = ۰$ و لذا $w^۴ = -۱ - w - w^۲ - w^۳$. پس

$$u = w + (-۱ - w - w^۲ - w^۳) + ۱ = -w^۲ - w^۳$$

وارون u چیست؟ با فرض $g(x) = -x^۲ - x^۳$، دو چندجمله‌ای $p(x)$ و $g(x)$ نسبت به هم اولند. برای بدست آوردن بزرگترین مقسوم‌علیه مشترک $p(x)$ و $g(x)$ با تقسیمات متوالی داریم

$$p(x) = -xg(x) + (x^۲ + x + ۱)$$

$$g(x) = -x(x^۲ + x + ۱) + x$$

$$x^۲ + x + ۱ = (x + ۱)x + ۱$$

و لذا با بازگشت در تساوی‌های فوق داریم

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

$$= (۱ - x^۲ - x)(x^۲ + x + ۱) - (x + ۱)g(x) = (۱ - x^۲ - x)(p(x) + xg(x)) - (x + ۱)g(x)$$

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

با جایگذاری w در رابطه‌ی فوق داریم $۱ = (-w^۲-w^۳)(-۱-w^۲-w^۳)$ بنابراین $v = -۱-w^۲-w^۳$ وارون u است(با انجام ضرب بالا از $uv = ۱$ اطمینان حاصل کنید.)

به مثال متفاوت و جالب بعدی توجه کنید.

مثال ۲۷.۲ میدان سه عنصری $\mathbb{F}_۳ = \mathbb{Z}/۳\mathbb{Z}$ و چندجمله‌ای $p(x) = x^۲ + ۱ \in \mathbb{F}_۳[x]$ را در نظر بگیرید. این چندجمله‌ای روی $\mathbb{F}_۳$ تحویل‌ناپذیر است(چرا؟) بنابراین $E = \dfrac{\mathbb{F}_۳[x]}{\langle x^۲ + ۱\rangle}$ یک میدان است. یادآوری می‌کنیم که $p(x)$ در E دارای ریشه‌ای چون α است. و در واقع $E = \mathbb{F}_۳(\alpha)$. دو عضو α و ۱ یک پایه‌ی E روی $\mathbb{F}_۳$ است. لذا

$$E = \{a + b\alpha :\ a, b \in \mathbb{F}_۳\}$$

بنابراین E یک میدان ۹ عنصری است و

$$E = \{۰, ۱, ۲, \alpha, ۱ + \alpha, ۲ + \alpha, ۲\alpha, ۱ + ۲\alpha, ۲ + ۲\alpha\}$$

در این میدان به عنوان مثال

$$(۱ + ۲\alpha)(۲ + ۲\alpha) = ۲ + ۲\alpha + \alpha + \alpha^۲ = ۲ - ۱ = ۱$$

تشکیل جدول ضرب عناصر E تمرین خوبی برای شما خواهد بود. توجه کنید که در جدول مشاهده خواهید کرد که هر عنصر ناصفر دارای وارون است.

مثال ۲۸.۲ قبلاً دیدیم که $\alpha = \sqrt{۲} + \sqrt{۳}$ یک ریشه‌ی چندجمله‌ای $p(x) = x^۴ - ۱۰x^۲ + ۱$ است. داریم

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{۲}) \subseteq \mathbb{Q}(\sqrt{۲}, \sqrt{۳})$$

به راحتی دیده می‌شود که $x^۲ + ۲$ چندجمله‌ای مینیمال $\sqrt{۲}$ روی $\mathbb{Q}$ است. از طرفی $\sqrt{۳}$ ریشه‌ی چندجمله‌ای $x^۲ + ۳$ است. این چندجمله‌ای روی $\mathbb{Q}(\sqrt{۲})$ تحویل‌ناپذیر است(چرا؟). پس بنابر قضیه‌ی برج

$$[\mathbb{Q}(\sqrt{۲}, \sqrt{۳}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{۲}, \sqrt{۳}) : \mathbb{Q}(\sqrt{۲})][\mathbb{Q}(\sqrt{۲}) : \mathbb{Q}] = ۲ \times ۲ = ۴$$

داریم $\alpha \in \mathbb{Q}(\sqrt{۲}, \sqrt{۳})$ و لذا $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{۲}, \sqrt{۳})$. از طرف دیگر $\alpha^۳ = ۱۱\sqrt{۲} + ۹\sqrt{۳}$ و لذا $\alpha^۳ - ۹\alpha = ۲\sqrt{۲}$

$$\sqrt{۲} = \tfrac{-۹}{۲}\alpha + \tfrac{۱}{۲}\alpha^۳ \in \mathbb{Q}(\alpha)$$

در نتیجه $\sqrt{۳} = \alpha - \sqrt{۲} \in \mathbb{Q}(\alpha)$ از $\sqrt{۲}, \sqrt{۳} \in \mathbb{Q}(\alpha)$ نتیجه می‌شود $\mathbb{Q}(\sqrt{۲}, \sqrt{۳}) \subseteq \mathbb{Q}(\alpha)$. بنابراین $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{۲}, \sqrt{۳})$. در نتیجه $[\mathbb{Q}(\alpha) : \mathbb{Q}] = ۴$. از این نتیجه می‌شود که چندجمله‌ای مینیمال α روی $\mathbb{Q}$ از درجه‌ی ۴ است. بنابراین $p(x)$ روی $\mathbb{Q}$ تحویل‌ناپذیر است.

قضیه ۲۹.۲ فرض کنیم E یک توسیع متناهی F باشد. در این صورت E یک توسیع جبری Fاست. یعنی هر عضو Eروی F جبری است.

اثبات. فرض کنیم $[E:F]=n$ و فرض کنیم $\alpha \in E$ دلخواه باشد. در این صورت $n+۱$ عنصر

$$۱, \alpha, \alpha^{۲}, \ldots, \alpha^n \in E$$

روی F وابسته خطی هستند. لذا $a_{۰}, a_{۱}, \ldots, a_n \in F$ وجود دارند که

$$a_{۰} + a_{۱}\alpha + a_{۲}\alpha^{۲} + \ldots + a_n\alpha^n = ۰$$

و حداقل یکی از a_iها ($۰ \leq i \leq n$) مخالف صفر است. بنابراین با فرض $f(x) = a_{۰} + a_{۱}x + a_{۲}x^{۲} + \ldots + a_nx^n$ داریم $۰ \neq f(x) \in F[x]$ و $f(\alpha) = ۰$. لذا α روی Fجبری از درجه‌ی حداکثر n است. و اثبات تمام است. $\square$

قضیه ۳۰.۲ فرض کنیم E یک توسیع F باشد. گزاره‌های زیر معادل‌اند.

(الف) E یک توسیع متناهی F است.

(ب) $\alpha_{۱}, \alpha_{۲}, \ldots, \alpha_n \in E$ وجود دارند به نحوی که هر α_i، $۱ \leq i \leq n$، روی F جبری است و

$$E = F(\alpha_{۱}, \alpha_{۲}, \ldots, \alpha_n).$$

اثبات. فرض کنیم E یک توسیع متناهی F باشد و $[E:F]=m$. اگر $E=F$ آن‌گاه چیزی برای اثبات نداریم و در واقع برای هر $\alpha \in E$ داریم $E = F(\alpha)$. فرض کنیم $E \neq F$. عنصر $\alpha_{۱} \in E - F$ را انتخاب می‌کنیم. خواهیم داشت $F \leq F(\alpha_{۱}) \leq E$ و $F \neq F(\alpha_{۱})$(چرا؟). اگر $F(\alpha_{۱}) = E$ آن‌گاه قضیه ثابت شده است. در غیر این صورت $\alpha_{۲} \in E - F(\alpha_{۱})$ را انتخاب می‌کنیم.

خواهیم داشت $F(\alpha_۱) \leq F(\alpha_۱, \alpha_۲) \leq E$ و $F(\alpha_۱) \neq F(\alpha_۱, \alpha_۲)$ (چرا؟) با tبار تکرار این روند، برج زیر از توسیع‌ها بدست می‌آیند.

$$F \leq F(\alpha_۱) \leq F(\alpha_۱, \alpha_۲) \leq \ldots \leq F(\alpha_۱, \alpha_۲, \ldots, \alpha_t) \leq E$$

که برای هر $۱ \leq i \leq t$، $F(\alpha_۱, \alpha_۲, \ldots, \alpha_i) \neq F(\alpha_۱, \alpha_۲, \ldots, \alpha_i, \alpha_{i+۱})$. لذا برای هر $۱ \leq i \leq t - ۱$، $m_i = [F(\alpha_۱, \alpha_۲, \ldots, \alpha_i, \alpha_{i+۱}) : F(\alpha_۱, \alpha_۲, \ldots, \alpha_i)] \geq ۲$(چرا؟) حال با کاربرد مکرر قضیه‌ی برج داریم:

$$m = [E : F] = [E : F(\alpha_۱, \alpha_۲, \ldots, \alpha_t)][F(\alpha_۱, \alpha_۲, \ldots, \alpha_t) : F(\alpha_۱, \alpha_۲, \ldots, \alpha_{t-۱})] \ldots [F(\alpha_۱, \alpha_۲) : F(\alpha_۱)][F(\alpha_۱) : F]$$

و لذا $m \geq ۲^t$. پس t(تعداد دفعات تکرار روند یافتن α_iها) نمی‌تواند نامتناهی باشد. این بدین معنی است که برای یک $s \geq ۱$ داریم $E = F(\alpha_۱, \alpha_۲, \ldots, \alpha_s)$. همچنین بنابر قضیه‌ی قبل، هر α_i روی F جبری است.

برعکس فرض کنیم (ب) برقرار باشد. در این صورت با به کار بردن مکرر قضیه‌ی برج و قضیه‌ی؟ و مشابه آن‌چه در قسمت اول اثبات دیدیم به سادگی ثابت می‌شود که $E = F(\alpha_۱, \alpha_۲, \ldots, \alpha_n)$ یک توسیع متناهی F است. □

در مثال‌ها دیدیم که مجموع دو عدد جبری $\sqrt{۲}$ و $\sqrt{۳}$ یک عدد جبری بود. این اتفاقی نیست. قضیه‌ی زیر را ببینید:

قضیه ۳۱.۲ فرض کنید Kیک توسیع F باشد. و

$$\overline{F}_K = \{\alpha : \text{جبری است } F \text{ روی } \alpha \quad \text{و} \quad \alpha \in K\}$$

در این صورت $\overline{F}_K$ یک میدان میانی K و F است. به‌ویژه مجموع، تفاضل و حاصل‌ضرب هر دو عنصر جبری، جبری است.

اثبات. فرض کنیم $\alpha_۲ \in \overline{F}_K$ و $\alpha_۲ \neq ۰$. پس $\alpha_۱$ و $\alpha_۲$ روی Fجبری هستند. لذا بنابر قضیه‌ی قبل

$F(\alpha_۱, \alpha_۲)$ یک توسیع متناهی F است. پس هر عنصر $F(\alpha_۱, \alpha_۲)$ روی F جبری است(قضیه‌ی ؟). اما $\alpha_۱ \pm \alpha_۲, \alpha_۱\alpha_۲, \alpha_۱^{-۱}$ همگی در $F(\alpha_۱, \alpha_۲)$ هستند. پس همگی روی F جبری هستند و لذا در $\overline{F}_K$ قرار دارند. پس $\overline{F}_K$ یک میدان است . و $F \leq \overline{F}_K \leq K$. □

تعریف ۳۲.۲ فرض کنیم K یک توسیع F باشد. در این صورت $\overline{F}_K$ را بستار جبری F در K گوییم.

نتیجه ۳۳.۲ مجموعه‌ی اعداد جبری یک میدان است. این میدان را با $\mathbb{A}$ نشان می‌دهیم.

اثبات. بنا به تعریف $\mathbb{A}$ در واقع بستار جبری $\mathbb{Q}$ در $\mathbb{C}$ است. و لذا بنابر قضیه‌ی قبل یک میدان است. □

تذکر ۳۴.۲ بنابه تعریف $\mathbb{A}$ یک توسیع جبری $\mathbb{Q}$ است. برای هر $n > ۱$ چندجمله‌ای $x^n - ۲$ روی $\mathbb{Q}$ تحویل‌ناپذیر است(چرا؟) و لذا ریشه‌ی $\sqrt[n]{۲}$ از آن، روی $\mathbb{Q}$ جبری از درجه‌ی n است. از طرفی

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt[n]{۲}) \leq \mathbb{A}.$$

لذا

$$[\mathbb{A} : \mathbb{Q}] = [\mathbb{A} : \mathbb{Q}(\sqrt[n]{۲})][\mathbb{Q}(\sqrt[n]{۲}) : \mathbb{Q}] \geq n$$

چون n دلخواه است لذا $[\mathbb{A} : \mathbb{Q}] = \infty$. این نشان می‌دهد که عکس قضیه‌ی ؟ برقرار نیست. یعنی یک توسیع جبری ممکن است یک توسیع متناهی نباشد.

بنابر قضیه‌ی برج اگر Kیک توسیع متناهی E و Eیک توسیع متناهی F باشد، آن‌گاه K یک توسیع متناهی F است. مشابه این قضیه برای جبری بودن نیز برقرار است. این قضیه می‌گوید، جبری روی جبری، جبری است.

قضیه ۳۵.۲ فرض کنیم K یک توسیع جبری E و E یک توسیع جبری F باشد. در این صورت K یک توسیع جبری F است.

اثبات. فرض کنیم $\alpha \in K$. چون K توسیع جبری E است پس $\circ \neq f(x) \in E[x]$ موجود است که $f(\alpha) = \circ$. فرض کنیم

$$f(x) = b_\circ + b_۱ x + \ldots + b_n x^n$$

فرض کنیم $L = F(b_\circ, b_۱, \ldots, b_n) \subseteq E$. در این صورت $f(x) \in L[x]$. از طرفی چون E روی F جبری است لذا $b_\circ, b_۱, \ldots b_n$ روی F جبری است و لذا بنابر قضیه‌ی ؟ ، L یک توسیع متناهی از F است. به علاوه α روی L جبری از درجه‌ی حداکثر n است. بنابراین

$$[L(\alpha) : F] = [L(\alpha) : L][L : F] \leq \infty$$

پس $L(\alpha)$ یک توسیع متناهی و در نتیجه جبری F است. پس هر عضو $L(\alpha)$ از جمله α روی F جبری است. چون $\alpha \in K$ دلخواه بود پس K یک توسیع جبری F است. $\square$

§ تمرین

۱. چندجمله‌ای مینیمال اعداد جبری $\sqrt{۳ - \sqrt{۶}}$، $\sqrt{۷} + ۳$ و $i + \sqrt[۳]{۲}$ روی $\mathbb{Q}$ را بیابید.

۲. چندجمله‌ای مینیمال $i + \sqrt[۳]{۲}$ روی $\mathbb{Q}(i)$ چیست؟

۳. فرض کنیم E یک توسیع F و $\alpha \in E$ روی F متعالی باشد. ثابت کنید $\alpha^۲$ نیز روی F متعالی است. به طور کلی اگر $g(x) \in F[x]$ یک چندجمله‌ای غیرثابت باشد، ثابت کنید $g(\alpha) \in E$ روی F متعالی است.

۴. فرض کنیم E توسیع F و $\alpha \in E$ متعالی باشد. ثابت کنید $F[\alpha] \cong F[x]$ و $F(\alpha) \cong F(x)$.

۵. اگر E یک توسیع F و $[E:F]$ عددی اول باشد، ثابت کنید هیچ میدان میانی برای K و F به جز K و F وجود ندارد.

۶. فرض کنیم عدد جبری α ریشه‌ی چندجمله‌ای $x^۷ + ۲x + ۸$ باشد و $\beta \in \mathbb{Q}(\alpha)$ و $\beta \notin \mathbb{Q}$. ثابت کنید $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

۷. فرض کنیم عدد جبری α ریشه‌ی چندجمله‌ای $x^{۱۵} + ۶x^۲ + ۱۲x + ۳$ باشد و $\beta = \alpha^۴ + \alpha^۳ + ۱$ و $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$. مطلوبست $[\mathbb{Q}(\beta) : \mathbb{Q}]$.

۸. فرض کنیم $\alpha \in \mathbb{R}$ یک عدد متعالی باشد. زیرمیدان F از $\mathbb{R}$ را چنان بیابید که α روی F جبری از درجه‌ی ۳ باشد.

۹. با فرض این‌که می‌دانیم عدد e متعالی است، زیرمیدان F از $\mathbb{R}$ را بیابید به نحوی که $e + ۱$ روی F جبری از درجه‌ی ۲ باشد.

۱۰. فرض کنیم Eتوسیع F باشد و $\alpha \in E$ و $\alpha \notin \overline{F}_E$. ثابت کنید α روی $\overline{F}_E$ متعالی است.

۱۱. فرض کنیم E یک توسیع F باشد و $\alpha \in E$. ثابت کنید α روی F جبری از درجه‌ی یک است اگر و تنها اگر $\alpha \in F$.

۱۲. فرض کنیم F یک میدان باشد و $\alpha \in F(x) - F$. ثابت کنید α روی F متعالی است.

۱۳. فرض کنیم E یک توسیع F باشد و $\alpha, \beta \in E$ و β روی $F(\alpha)$ جبری و β روی F متعالی است. ثابت کنید α روی $F(\beta)$ جبری است.

۱۴. یک پایه برای $\mathbb{Q}(\sqrt{۲}, \sqrt{۷})$ روی $\mathbb{Q}$ بیابید. سپس ثابت کنید $\mathbb{Q}(\sqrt{۲}, \sqrt{۷}) = \mathbb{Q}(\sqrt{۲} + \sqrt{۷})$. سرانجام چندجمله‌ای مینیمال $\alpha = \sqrt{۲} + \sqrt{۷}$ روی $\mathbb{Q}$ را بیابید.

فصل ۳
نظریه‌ی گالوا

موضوع این فصل مقدمه‌ای بر نظریه‌ی گالواست. این نظریه به مطالعه و بررسی میدان‌های میانی یک توسیع به کمک نظریه‌ی گروه‌ها می‌پردازد. ابتدا به یک مثال توجه کنید. در فصل قبل دیدیم که بینهاین میدان میانی برای توسیع $\mathbb{R}$ از $\mathbb{Q}$ وجود دارد. به عنوان نمونه، اگر n یک عدد طبیعی خالی از مربع باشد، آن‌گاه

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{n}) \subseteq \mathbb{R}$$

$\mathbb{Q}(\sqrt{n})$ برای هر عدد خالی از مربع طبیعی n یک توسیع درجه ۲ از $\mathbb{Q}$ است. بنابراین، این سئوال طبیعی به نظر می‌رسد که آیا $\mathbb{Q}(\sqrt{n})$ها برای اعداد مختلف n می‌توانند میدان‌های یکریخت باشند؟ مثلاً آیا $\mathbb{Q}(\sqrt{۲})$ و $\mathbb{Q}(\sqrt{۳})$ یکریخت‌اند؟ یادآوری می‌کنیم که

$$\mathbb{Q}(\sqrt{۲}) = \{a + b\sqrt{۲} \ : \ a, b \in \mathbb{Q}\}$$

$$\mathbb{Q}(\sqrt{۳}) = \{a + b\sqrt{۳} \ : \ a, b \in \mathbb{Q}\}$$

مکرر در کلاس در برابر این پرسش که آیا این دو میدان یکریخت‌اند با پاسخ مثبت روبرو شده‌ام. ساده است. تعریف می کنیم:

$$\varphi : \mathbb{Q}(\sqrt{۲}) \longrightarrow \mathbb{Q}(\sqrt{۳})$$
$$\varphi(a + b\sqrt{۲}) = a + b\sqrt{۳}$$

توجه کنیم که اگر $u, v \in \mathbb{Q}(\sqrt{۲})$ و $u = a + b\sqrt{۲}$ و $v = a' + b'\sqrt{۲}$ که در آن $a, b, a', b' \in \mathbb{Q}$، آن‌گاه

$$\varphi(u + v) = \varphi((a + a') + (b + b')\sqrt{۲}) = (a + a') + (b + b')\sqrt{۳} = \varphi(u) + \varphi(v).$$

یعنی φ یک همریختی گروه‌هاست. اما به راحتی می‌توانید ببینید که در حالت کلی $\varphi(uv)$ با $\varphi(u)\varphi(v)$ برابر نیست. مثلاً

$$\varphi(\sqrt{۲} \times \sqrt{۲}) = \varphi(۲) = ۲$$

و

$$\varphi(\sqrt{۲}) \times \varphi(\sqrt{۲}) = \sqrt{۳} \times \sqrt{۳} = ۳$$

و لذا $\varphi(\sqrt{۲} \times \sqrt{۲}) \neq \varphi(\sqrt{۲}) \times \varphi(\sqrt{۲})$.

بنابراین φ یک همریختی میدان‌ها نیست. به‌طور کلی فرض کنیم $f : \mathbb{Q}(\sqrt{۲}) \longrightarrow \mathbb{Q}(\sqrt{۳})$ یک همریختی ناصفر میدان‌ها باشد. در این صورت $\varphi(\sqrt{۲}) = a_۰ + b_۰\sqrt{۳}$ برای یک $a_۰, b_۰ \in \mathbb{Q}$. لذا

$$۲ = \varphi(۲) = \varphi(\sqrt{۲} \times \sqrt{۲}) = (\varphi(\sqrt{۲}))^۲ = (a_۰ + b_۰\sqrt{۳})^۲ = a_۰^۲ + ۳b_۰^۲ + ۲a_۰b_۰\sqrt{۳}$$

و لذا

$$\sqrt{۳} = \frac{۲ - a_۰^۲ - ۳b_۰}{۲a_۰b_۰}$$

یعنی $\sqrt{۳}$ عددی گویاست که غیر ممکن است. پس تنها همریختی از میدان $\mathbb{Q}(\sqrt{۲})$ به میدان $\mathbb{Q}(\sqrt{۳})$ همریختی صفر است. پس $\mathbb{Q}(\sqrt{۲})$ و $\mathbb{Q}(\sqrt{۳})$ یکریخت نیستند. لم بعد نشان می‌دهد این یک اتفاق

نیست.

تعریف ۱.۳ فرض کنیم E یک توسیع F و $\alpha, \beta \in E$ روی F جبری باشند. گوییم α و β مزدوج هستند، هرگاه چندجمله‌ای مینیمال آن‌ها یکی باشد.

مثال ۲.۳ $\sqrt{۲}$ و $-\sqrt{۲}$ روی $\mathbb{Q}$ مزدوج‌اند. $\sqrt{۳}$ و $-\sqrt{۳}$ روی $\mathbb{Q}$ مزدوج‌اند. همچنین چهار عدد $\sqrt{۲}+\sqrt{۳}$، $\sqrt{۳}-\sqrt{۲}$، $\sqrt{۲}-\sqrt{۳}$ و $-\sqrt{۲}-\sqrt{۳}$ روی $\mathbb{Q}$ مزدوج‌اند. زیرا همگی ریشه‌های چندجمله‌ای تحویل‌ناپذیر $x^۴-۱۰x^۲+۱$ می‌باشند. اگر $a, b \neq ۰$ دو عدد حقیقی باشند آن‌گاه $a+bi$ و $a-bi$ روی $\mathbb{R}$ مزدوج‌اند، زیرا هر دو ریشه‌ی معادله‌ی $x^۲-۲ax+a^۲+b^۲$ هستند.

تعریف ۳.۳ فرض کنیم E و K دو توسیع F باشند. تکریختی $\sigma : E \longrightarrow K$ را یک F- تکریختی گوییم هرگاه برای هر $\alpha \in F$ داشته باشیم $\sigma(\alpha) = \alpha$. به عبارت دیگر σ یک تکریختی است هرگاه $\sigma|_F = id_F$. اگر $\sigma : E \longrightarrow K$ یک F- تکریختی باشد و $\alpha \in F$ و $u \in E$ آن‌گاه

$$\sigma(\alpha u) = \sigma(\alpha)\sigma(u) = \alpha\sigma(u).$$

بنابراین σ یک نگاشت خطی بین دو فضای برداری E و K روی F است. بر عکس هر نگاشت خطی از فضای برداری E به فضای برداری K (روی F) یک F- تکریختی است.

لم ۴.۳ فرض کنیم E یک توسیع F و $\alpha \in E$ روی F جبری باشد. فرض کنیم $\varphi : F(\alpha) \longrightarrow E$ یک F- همریختی باشد. در این صورت $\varphi(\alpha)$ یک مزدوج α روی F است.

اثبات. فرض کنیم $P(x) = a_۰ + a_۱x + a_۲x^۲ + \ldots + a_nx^n \in F[x]$ چندجمله‌ای مینیمال α روی F باشد($a_n = ۱$). در این صورت $\varphi(\alpha) = ۰$ و لذا

$$\circ = \varphi(\circ) = \varphi(a_\circ + a_1\alpha + \ldots + a_n\alpha^n) = \varphi(a_\circ) + \varphi(a_1)\varphi(\alpha) + \ldots + \varphi(a_n)\varphi(\alpha^n)$$
$$= a_\circ + a_1\varphi(\alpha) + \ldots + a_n(\varphi(\alpha))^n = P(\varphi(\alpha))$$

لذا $P(\varphi(\alpha)) = \circ$. یعنی $P(x)$ چندجمله‌ای مینیمال $\varphi(\alpha)$ نیز هست. لذا $\varphi(\alpha)$ مزدوج α روی F است. $\square$

تبصره ۵.۳ فرض کنیم E و Kدو توسیع $\mathbb{Q}$ باشند. در این صورت هر همریختی ناصفر از E به Kیک $\mathbb{Q}$ همریختی است.(ثابت کنید).

مثال ۶.۳ فرض کنیم E یک توسیع $\mathbb{Q}$و $\varphi : \mathbb{Q}(\sqrt{۲}) \longrightarrow E$ یک همریختی ناصفر میدان‌ها باشد. در این صورت φ یک $\mathbb{Q}$- همریختی است. و لذا $\varphi(\sqrt{۲})$ باید مزدوج $\sqrt{۲}$ روی $\mathbb{Q}$ باشد. لذا $\varphi(\sqrt{۲}) = \sqrt{۲}$ یا $\varphi(\sqrt{۲}) = -\sqrt{۲}$.

قضیه‌ی بعد در واقع لم قبل را تکمیل می‌کند.

قضیه ۷.۳ فرض کنیم E یک توسیع F و $\alpha, \beta \in E$ روی F جبری باشند. در این صورت α و β روی F مزدوج‌اند اگر و تنها اگر F-یکریختی $\varphi : F(\alpha) \longrightarrow F(\beta)$ موجود باشد به‌نحوی که $\varphi(\alpha) = \beta$.

اثبات. اگر F- یکریختی $\varphi : F(\alpha) \longrightarrow F(\beta)$ موجود باشد به‌نحوی که $\varphi(\alpha) = \beta$، آنگاه بنا بر لم قبل، α و β روی F مزدوج‌اند.

برعکس فرض کنیم α و β روی F مزدوج باشند. فرض کنیم $p(x)$ چندجمله‌ای مینیمال مشترک α و β روی F باشد. در این صورت $\varphi_\alpha : F[x] \longrightarrow F(\alpha)$ و $\varphi_\beta : F[x] \longrightarrow F(\beta)$ با ضابطه‌ی $\varphi_\alpha(f(x)) = f(\alpha)$ و $\varphi_\beta(f(x)) = f(\beta)$ هر دو همریختی حلقه‌ها با هسته‌ی $p(x)$ هستند. بنابر قضیه‌ی اول یکریختی، نگاشت‌های

$$\widehat{\varphi_\alpha} : \frac{F[x]}{\langle p(x)\rangle} \longrightarrow f(\alpha)$$
$$\widehat{\varphi_\alpha}(f(x) + \langle p(x)\rangle) = f(\alpha)$$

و

$$\widehat{\varphi_\beta} : \frac{F[x]}{\langle p(x)\rangle} \longrightarrow f(\beta)$$
$$\widehat{\varphi_\beta}(f(x) + \langle p(x)\rangle) = f(\beta)$$

هر دو یکریختی هستند. لذا

$$\varphi_{\alpha,\beta} = \widehat{\varphi_\beta} o \widehat{\varphi_\alpha}^{-۱} : F(\alpha) \longrightarrow F(\beta)$$

یک یکریختی میدان‌هاست. به‌علاوه $\widehat{\varphi_\alpha}(x + \langle p(x)\rangle) = \alpha$ و $\widehat{\varphi_\beta}(x + \langle p(x)\rangle = \beta$ و برای هر $u \in F$،

$$\varphi_{\alpha,\beta}(u) = \widehat{\varphi_\beta}\widehat{\varphi_\alpha}^{-۱}(u) = \widehat{\varphi_\beta}(u + \langle p(x)\rangle) = u$$

و لذا $\varphi_{\alpha,\beta}$ یک F- یکریختی است. □

مثال ۸.۳ $\sqrt{۲}$ و $-\sqrt{۲}$ مزدوج‌اند و $\varphi_{\sqrt{۲},-\sqrt{۲}} : \mathbb{Q}(\sqrt{۲}) \longrightarrow \mathbb{Q}(\sqrt{۲})$ که $\varphi_{\sqrt{۲},-\sqrt{۲}}(a+b\sqrt{۲}) = a - b\sqrt{۲}$.

تعریف ۹.۳ فرض کنیم Eیک میدان باشد. هر یکریختی میدان از Eبه E را یک خودریختی E می‌گوییم. مجموعه‌ی خودریختی‌های E را با $Aut(E)$نمایش می‌دهیم.

قضیه ۱۰.۳ برای هر میدان E، مجموعه‌ی $Aut(E)$ با عمل ترکیب توابع، یک گروه است.

اثبات. فرض کنیم $f, g \in Aut(E)$. در این صورت برای هر $\alpha, \beta \in E$ داریم

$$(fog)(\alpha+\beta) = f(g(\varphi+\beta)) = f(g(\alpha)+g(\beta)) = f(g(\alpha)) + f(g(\beta)) =$$
$$(fog(\alpha) + fog(\beta)$$

به طریق مشابه

$$(fog)(\alpha\beta) = (fog)(\alpha)(fog)(\beta)$$

و لذا $fog \in Aut(E)$. همچنین تابع همانی E، id_E یک یکریختی است. به‌علاوه اگر فرض کنیم $\alpha = f(\alpha_۱)$ و $\beta = f(\beta_۱)$، آن‌گاه $\alpha+\beta = f(\alpha_۱+\beta_۱)$ و لذا

$$f^{-۱}(\alpha+\beta) = \alpha_۱ + \beta_۱ = f^{-۱}(\alpha) + f^{-۱}(\beta)$$

و لذا $f^{-۱} \in Aut(E)$. و اثبات تمام است. $\square$

تعریف بعد کلید مطالعه‌ی توسیع میدان‌ها و زیربنای نظریه‌ی گالواست:

تعریف ۱۱.۳ فرض کنیم E یک توسیع F باشد. $\sigma \in Aut(E)$ را یک F- خودریختی گوییم هرگاه $\sigma(\alpha) = \alpha$، برای هر $\alpha \in F$. در این صورت همچنین می‌گوییم σ عناصر F را ثابت نگه می دارد. مجموعه‌ی F- خودریختی‌های E را با $Aut_F(E)$ یا $G(E/F)$ یا $Gal(E/F)$ نشان می‌دهیم، و آن‌را گروه گالوای E روی F گوییم.

تبصره ۱۲.۳ اگر F میدان اول E باشد، آن‌گاه $Aut(E) = Aut_F(E)$. (ثابت کنید). یادآوری می‌کنیم که در حالتی که مشخصه‌ی میدان صفر باشد، میدان اول آن $\mathbb{Q}$ است و در حالتی که مشخصه‌ی E برابر عدد اول p باشد، آن‌گاه میدان اول آن، میدان $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ است.

قضیه‌ی بعد نشان می‌دهد که $Gal(E/F)$در واقع یک گروه است:

قضیه ۱۳.۳ فرض کنیم E یک توسیع F باشد. در این صورت $Aut_F(E)$ یک زیرگروه $Aut(E)$ است.

اثبات. به‌راحتی مشابه اثبات قضیه‌ی ؟؟؟ ثابت می‌شود. $\square$

مثال ۱۴.۳ فرض کنیم E یک توسیع F و $\alpha \in E$ روی F جبری باشد. فرض کنیم $\varphi : F(\alpha) \longrightarrow F(\alpha)$ یک F- خودریختی باشد و $u \in F(\alpha)$. در این صورت $u = a_۰ + a_۱\alpha + \ldots + a_{n-۱}\alpha^{n-۱}$ که در آن n درجه‌ی جبری بودن α روی F است و $a_۰, a_۱, \ldots, a_{n-۱} \in F$. لذا

$$\varphi(u) = \varphi(a_۰ + a_۱\alpha + \ldots + a_{n-۱}\alpha^{n-۱}) = a_۰ + a_۱\varphi(\alpha) + \ldots + a_{n-۱}\varphi(\alpha)^{n-۱}$$

بنابراین برای تعریف u، تعریف $\varphi(\alpha)$ کافی است. از طرفی بنابر لم ؟؟؟، $\varphi(\alpha)$ مزدوج α روی F است. از آن‌جا که α حداکثر n مزدوج روی F دارد، لذا برای $F(\alpha)$ حداکثر n انتخاب موجود است. بنابراین

$$|Aut_F F(\alpha)| \leq n$$

به‌ویژه $Aut_F F(\alpha)$ متناهی است.

مثال ۱۵.۳ اگر $\sigma \in Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{۲}))$، آن‌گاه $\sigma(\sqrt{۲}) = \pm\sqrt{۲}$. اگر $\sigma(\sqrt{۲}) = \sqrt{۲}$ آن‌گاه $\sigma = id_{\mathbb{Q}(\sqrt{۲})}$، نگاشت همانی $\mathbb{Q}(\sqrt{۲})$ است. و اگر $\sigma(\sqrt{۲}) = -\sqrt{۲}$، آن‌گاه

$$\sigma(a + b\sqrt{۲}) = a - b\sqrt{۲} \quad , a, b \in \mathbb{Q}$$

و لذا $\sigma = \varphi_{\sqrt{۲},-\sqrt{۲}}$. بنابراین $Aut(\mathbb{Q}(\sqrt{۲})) = \{id_{\mathbb{Q}(\sqrt{۲})}, \varphi_{\sqrt{۲},-\sqrt{۲}}\}$.

مثال ۱۶.۳ اگر $E = F$ آن‌گاه روشن است که $Aut_F(E) = \{id_E\}$. و لذا $Aut_F(E)$ تنها یک عضو دارد. حتی اگر $E \neq F$ و E توسیع F باشد ممکن است $Aut_F(E) = \{id_E\}$ اتفاق افتد. برای

مثال فرض کنیم $\alpha = \sqrt[3]{2}$ ریشه‌ی سوم حقیقی ۲ باشد. در این صورت چندجمله‌ای مینیمال α روی $\mathbb{Q}$، $p(x) = x^3 - 2$ است. که ریشه‌های آن عبارت‌اند از α و $w\alpha$ و $w^2\alpha$ که در آن $w = e^{\frac{2\pi i}{3}}$ ریشه‌ی سوم واحد است. در واقع $w = \frac{1}{2} - \frac{\sqrt{2}}{2}i$ و $w^2 = \frac{-1}{2} - \frac{\sqrt{3}}{2}i$. فرض کنیم $\varphi : \mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\alpha)$ یک خودریختی باشد. در این صورت بنابر لم ؟؟؟، $\varphi(\alpha)$ باید یکی از مقادیر α و $w\alpha$ و $w^2\alpha$ باشد. اما $w\alpha$ و $w^2\alpha$ اعدادی غیر حقیقی هستند و لذا در $\mathbb{Q}(\alpha)$ نیستند. پس تنها گزینه‌ی $\varphi(\alpha) = \alpha$ باقی می‌ماند. پس $\varphi = id_{\mathbb{Q}(\sqrt{2})}$. پس $Aut_{\mathbb{Q}}\mathbb{Q}(\alpha) = \{id_{\mathbb{Q}(\alpha)}\}$.

مثال ۱۷.۳ فرض کنیم $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $p_1(x) = x^2 - 3$ چندجمله‌ای مینیمال $\sqrt{3}$ روی $\mathbb{Q}(\sqrt{2})$ است. لذا $\sqrt{3}$ و $-\sqrt{3}$ روی $\mathbb{Q}(\sqrt{2})$ مزدوج‌اند و

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \{a + b\sqrt{3} :\ a, b \in \mathbb{Q}(\sqrt{2})\}$$

و لذا

$$\sigma = \varphi_{\sqrt{3}, -\sqrt{3}} :\ \mathbb{Q}(\sqrt{2}, \sqrt{3}) \longrightarrow \mathbb{A}(\sqrt{2}, \sqrt{3})$$
$$\sigma(a + b\sqrt{3}) = a - b\sqrt{3} \quad a, b \in \mathbb{Q}(\sqrt{2})$$

یک یکریختی Kاست که عناصر $\mathbb{Q}(\sqrt{2})$را ثابت نگه می‌دارد(قضیه‌ی ؟؟؟ را ببینید). به طریق مشابه $\sqrt{2}$ و $-\sqrt{2}$ روی $\mathbb{Q}(\sqrt{3}$ مزدوج‌اند و لذا

$$\tau = \varphi_{\sqrt{2}, -\sqrt{2}} : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$$
$$\tau(a + b\sqrt{2}) = a - b\sqrt{2} \quad (a, b \in \mathbb{Q}(\sqrt{3}))$$

یک خودریختی K است که عناصر $\mathbb{Q}(\sqrt{3})$ را ثابت نگه می‌دارد. لذا $\sigma o \tau$ نیز یک خودریختی K است. دقت کنید که $\sigma o \tau(\sqrt{2}) = -\sqrt{2}$ و $\sigma o \tau(\sqrt{3}) = -\sqrt{3}$.

بنابراین چهار نگاشت id_K، σ، τ و $\sigma\tau$ عناصری از $Aut(K)$ هستند. از طرف دیگر اگر $\varphi : K \longrightarrow K$ یک خودریختی باشد آن‌گاه مقدار $\varphi(\sqrt{2})$ و $\varphi(\sqrt{3})$ کاملاًφ را مشخص می‌کند(چرا؟). اما برای

$\varphi(\sqrt{۲})$ دو انتخاب داریم و $\varphi(\sqrt{۳})$ نیز دو انتخاب داریم. لذا برای تعریف φ حداکثر چهار انتخاب داریم. پس $|Aut(K)| \leq ۴$. چون قبلاً چهار عضو برای $Aut(K)$ یافتیم لذا

$$Gal(K/\mathbb{Q}) = Aut(K) = \{id_K, \sigma, \tau, \sigma\tau\}$$

در پایان توجه کنید که $\sigma^۲ = \tau^۲ = (\sigma\tau)^۲ = id_F$ و لذا $Aut(K)$ گروه چهارتایی کلاین است.

قضیه‌ی زیر ارتباطی کارگشا بین زیرگروه‌های $Gal(K/F)$ و میدان‌های میانی K و F برقرار می‌کند:

قضیه ۱۸.۳ فرض کنیم K یک توسیع F و G گروه گالوای K روی F باشد.

(الف) اگر H یک زیرگروه G باشد، آن‌گاه $H' = \{u \in K : \ \sigma(u) = u, \sigma \in H\}$ یک میدان میانی E و F است.

(ب) اگر $F \leq E \leq K$ یک میدان میانی K و F باشد آن‌گاه $E' = \{\sigma \in G : \ \sigma(u) = u, u \in E\}$ یک زیرگروه G است.(توجه کنید که $E' = Gal(K/E)$.)

اثبات. به‌راحتی با استفاده از تعریف ثابت می‌شود. □

تناظر موجود بین زیرگروه‌های G و میدان‌های میانی K و F در قضیه‌ی فوق در حالت کلی یک تناظر یک به یک نیست.

مثال ۱۹.۳ الف) اگر قرار دهیم $K = \mathbb{Q}(\sqrt{۲}, \sqrt{۳})$ و $F = \mathbb{Q}$، آن‌گاه در مثال قبل دیدیم

$$G = Gal(K/F) = Aut(K) = \{id_K, \sigma, \tau, \sigma\tau\}.$$

زیرگروه‌های G، $H_۱ = \{id)K\}$، $H_۲ = \{id_K, \sigma\}$، $H_۳ = \{id_K, \tau\}$، $H_۴ = \{id_K, \sigma\tau\}$ و $H_۵ = G$ هستند. میدان‌های میانی متناظر این زیرگروه‌ها، $H'_۱ = K$، $H'_۲ = \mathbb{Q}(\sqrt{۲})$، $H'_۳ = \mathbb{Q}(\sqrt{۳})$، $H'_۴ = \mathbb{Q}(\sqrt{۶})$ و $H'_۵ = \mathbb{Q}$ هستند.(ثابت کنید). به راحتی می‌توانید ثابت کنید که $H'_۱$، $H'_۲$، $H'_۳$، $H'_۴$ و $H'_۵$ تنها میدان‌های میانی K و F هستند. و لذا در این حالت قضیه‌ی ؟؟؟ یک تناظر یک به یک بین زیرگروه‌های G و میدان‌های میانی K و F برقرار می‌کند. توجه کنید که در این‌جا با قرار دادن $H'' := (H')'$ داریم

$H''_۱ = K' = Gal(K/\mathbb{Q}) = H_۱$

$H''_۲ = (\mathbb{Q}(\sqrt{۲}))' = Gal(K/\mathbb{Q}(\sqrt{۲})) = H_۲$

$H''_۳ = (\mathbb{Q}(\sqrt{۳}))' = Gal(K/\mathbb{Q}(\sqrt{۳})) = H_۳$

$H''_۴ = (\mathbb{Q}(\sqrt{۶}))' = Gal(K/\mathbb{Q}(\sqrt{۶})) = H_۴$

$H''_۵ = \mathbb{Q}' = Gal(K/\mathbb{Q}) = H_۵$

(ب) حال قرار دهید $K = \mathbb{Q}(\sqrt[۳]{۲})$ و $F = \mathbb{Q}$. در این حالت دیدیم که $G = \{id_K\}$. در این‌جا، G تنها یک زیرگروه داردکه خود G است. ولی K و F دو میدان میانی هستند. و لذا تناظر بین زیرگروه‌های G و میدان‌های میانی K و F یک تناظر یک به یک نیست. در واقع $G' = K$ و لی $\mathbb{Q}$ متناظر هیچ زیرگروهی از G نیست. به‌علاوه

$$\mathbb{Q}' = Gal(K/\mathbb{Q}) = \{id_F\} = G$$
$$\mathbb{Q}'' := (\mathbb{Q}')' = G' = K$$

و لذا $\mathbb{Q}'' = \mathbb{Q}$.

در مثال قبل، حالت (الف) داشتیم $G' = F$ ولی در قسمت (ب)، $G' \neq F$. بنابر قضیه‌ی اساسی گالوا که به زودی می‌بینیم، در حالتی که K توسیع متناهی F است، شرط $G' = F$، تناظر ناشی از قضیه‌ی ؟؟؟ را یک تناظر یک به یک می‌کند. بنابراین تعریف زیر را ارائه می‌دهیم:

تعریف ۲۰.۳ فرض کنیم Kیک توسیع F و $G = Gal(K/F)$گروه گالوای K روی F باشد. K را یک توسیع گالوای F گوییم هرگاه $G' = F$.

مثال ۲۱.۳ مثال قبل نشان می‌دهد $\mathbb{Q}(\sqrt{۲}, \sqrt{۳})$ توسیع‌های گالوای $\mathbb{Q}$ است، ولی $\mathbb{Q}(\sqrt[۳]{۲})$ یک توسیع گالوای $\mathbb{Q}$ نیست.

تبصره ۲۲.۳ (الف) فرض کنیم K یک توسیع گالوای F باشد و $\alpha \in K - F$. در این صورت $\sigma \in Gal(K/F)$ موجود است به‌نحوی که $\sigma(\alpha) \neq \alpha$.

(ب) فرض کنیم K یک توسیع دلخواه F باشد و $G = Gal(K/F)$. قرار می‌دهیم $F_1 = G'$. در این صورت $F \leq F_1 \leq K$. در حالتی که توسیع K روی F گالوا باشد بنا به تعریف $F_1 = F$. و در حالت کلی Kروی F_1 گالواست.

اکنون می‌توانیم قضیه‌ی گالوا را بیان کنیم

قضیه ۲۳.۳ (قضیه‌ی اساسی گالوا) فرض کنیم K یک توسیع متناهی و گالوای F باشد. و فرض کنیم $G = Gal(K/F)$ گروه گالوای Kروی F باشد.

(الف) نگاشتی که به هر میدان میانی K و F مانند E، زیرگروه $E' = Gal(K/E)$ از G را نظیر می‌کند یک تناظر یک به یک بین میدان‌های میانی K و F و زیرگروه‌های G است.

(ب) اگر $F \leq E_1 \leq E_2 \leq K$ دو زیرمیدان میانی Kو F باشند، آن‌گاه E'_1 و E'_2زیرگروه‌های G هستند و $E'_2 \leq E'_1$ و $[E'_1 : E'_2] = [E_2 : E_1]$، به‌ویژه $|G| = [K : F]$.(در این‌جا $[E_2 : E_1]$ درجه‌ی توسیع $E_1 \leq E_2$ و $[E'_1 : E'_2]$ شاخص زیرگروه E'_2 در E'_1 است.)

(ج) اگر $F \leq E \leq K$، آن‌گاه K روی Fگالواست. اما E روی F فقط و فقط وقتی گالواست که E' در G نرمال باشد. و در این حالت $Gal(E/F) \cong G/E'$.

تبصره ۲۴.۳ شکل کلی‌تری از قضیه‌ی فوق نیز وجود دارد که در آن توسیع لزوماً متناهی نیست.

برای اثبات قضیه‌ی بالا، به مقدمات و گزاره‌هایی نیاز داریم، که در اینجا به آن‌ها می‌پردازیم.

لم ۲۵.۳ فرض کنیم K یک توسیع F باشد و $G = Gal(K/F)$. در این صورت:

(الف) اگر $F \leq E_2 \leq E_2 \leq K$ دو میدان میانی باشند، آن‌گاه $E'_2 \leq E'_1$.

(ب) اگر $H_1 \leq H_2 \leq G$ دو زیرگروه G باشند، آن‌گاه $H'_2 \leq H'_1$.

اثبات. به راحتی از تعریف نتیجه می‌شود. □

لم ۲۶.۳ فرض کنیم Kیک توسیع F باشد و $G = Gal(K/F)$. در این صورت:

(الف) اگر $F \leq E \leq K$ یک میدان میانی باشد، آنگاه $E \leq E''$ (که در آن $E'' = (E')'$.)

(ب) اگر $H \leq G$ یک زیرگروه باشد، آنگاه $H \leq H''$ (که در آن $H'' = (H')'$.)

اثبات. به راحتی از تعریف نتیجه می‌شود. □

تعریف ۲۷.۳ فرض کنیم K یک توسیع F باشد و $G = Gal(K/F)$.

(الف) میدان میانی $f \leq E \leq K$ را بسته گوییم هرگاه $H'' = H$.

اثبات وجود تناظر یک به یک بین میدان‌های میانی بسته K وF و زیرگروه‌های بسته‌ی $G = Gal(K/F)$ ساده است. به قضیه‌ی زیر توجه کنید:

قضیه ۲۸.۳ فرض کنیم K یک توسیع F باشد. در این صورت تناظری یک به یک بین میدان‌های میانی بسته‌ی K و F و زیرگروه‌های بسته‌ی $G = Gal(K/F)$ وجود دارد. در این تناظر میدان میانی E به زیرگروه E' از G نظیر می‌شود.

اثبات. فرض کنیم $\mathcal{A}$ مجموعه‌ی میدان‌های میانی بسته K و F و $\mathcal{S}$ مجموعه‌ی زیرگروه‌های بسته G باشد. نگاشت

$$\varphi : \mathcal{A} \longrightarrow \mathcal{S}$$

$$\varphi(E) = E', \quad \forall E \in \mathcal{A}$$

را تعریف می‌کنیم. ابتدا توجه می‌کنیم که اگر $E \in \mathcal{A}$ آنگاه $E' \in \mathcal{S}$. زیرا بنابر لم ؟؟؟، $E \leq E''$، و بنابر لم ؟؟؟ $E' \leq (E')''$. از طرف دیگر بنابر لم ؟؟؟ $(E'')' \leq E'$. لذا

$$(E')'' = ((E')')' = (E'')' \leq E' \leq (E')''$$

و بنابراین $(E')'' = E'$. لذا E' بسته است. یعنی $E' \in \mathcal{C}$. به طریق مشابه نگاشت

$$\psi : \mathcal{S} \longrightarrow \mathcal{A}$$
$$\psi(H) = H', \quad \forall H \in \mathcal{S}$$

خوش تعریف است. برای هر $E \in \mathcal{A}$ داریم $\psi\varphi(E) = E'' = E$ و برای هر $H \in \mathcal{S}$ داریم $\varphi\psi(H) = H$. بنابراین φ یک تابع دوسویی است و اثبات تمام است. $\square$

با عنایت به قضیه‌ی فوق، برای اثبات قسمت ؟؟ قضیه‌ی ؟؟؟ کافیست ثابت کنیم که برای توسیع‌های متناهی گالوا، همه‌ی میدان‌های میانی و همه‌ی زیرگروه‌های G بسته‌اند. برای اثبات این موضوع ابتدا به اثبات چند گزاره می‌پردازیم:

لم ۲۹.۳ فرض کنیم K یک توسیع F و $E_۱$ و $E_۲$ دو میدان میانی K و F باشند به طوری که $E_۱ \leq E_۲$ و $[E_۲ : E_۱]$ متناهی باشد. فرض کنیم $E_۲ = E_۱(\alpha)$ برای یک $\alpha \in E_۲$. در این صورت

$$[E'_۱ : E'_۲] \leq [E_۲ : E_۱]$$

اثبات. فرض کنیم $f(x) \in E_۱[x]$ چندجمله‌ای مینیمال α روی $E_۱$ باشد. فرض کنیم $\sigma_۱, \sigma_۲, \ldots, \sigma_s \in E'_۱$ چنان باشند که $\sigma_۱ E'_۲, \sigma_۲ E'_۲, \ldots, \sigma_s E'_۲$ همه‌ی همدسته‌های متایز $E'_۲$ در $E'_۱$ باشند. و فرض کنیم $\alpha_۱ = \alpha, \alpha_۲, \ldots, \alpha_t$ همه‌ی ریشه‌های متمایز f در K باشند. نگاشت

$$\varphi : \{\sigma_۱, \sigma_۲, \ldots, \sigma_s\} \longrightarrow \{\alpha_۱, \alpha_۲, \ldots, \alpha_t\}$$
$$\varphi(\sigma_i) = \sigma_i(\alpha)$$

را در نظر می‌گیریم. ابتدا توجه کنیم که برای $۱ \leq i \leq s$، σ_i یک $E_۱$− خودریختی F است، و لذا $\sigma_i(\alpha) \in K$ باید مزدوج α روی E باشد. پس $\sigma_i(\alpha) = \alpha_j$ برای یک $۱ \leq j \leq t$. فرض کنیم برای $۱ \leq i \leq j \leq s$ داریم $\varphi(\sigma_i) = \varphi(\sigma_j)$. پس $\sigma_i(\alpha) = \sigma_j(\alpha)$. فرض کنیم $u \in E_۲$

دلخواه باشد. پس $u = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ که در آن $n = [E_2 : E_1] = deg(f(x))$ و $a_0, a_1, \ldots, a_{n-1} \in E_1$. لذا

$$\sigma_i(u) = \sigma_i(a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\sigma_i(\alpha+) \ldots + a_{n-1}\sigma_i(\alpha)^{n-1}$$
$$= a_0 + a_1\sigma_j(\alpha+) \ldots + a_{n-1}\sigma_j(\alpha)^{n-1} = \sigma_j(u)$$

لذا $\sigma_i(u) = \sigma_j(u)$. برای هر $u \in E_2$. بنابراین $\sigma_j^{-1}\sigma_i(u) = u$ برای هر $u \in E_2$. پس $\sigma_j^{-1}\sigma_i \in E_2'$ و لذا $\sigma_i E_2' = \sigma_j E_2'$ و این با متمایز بودن s هم‌دسته‌ی $\sigma_1 E_2', \ldots, \sigma_s E_2'$ متناقض است. پس φ یک به یک است و $[E_1' : E_2'] = s \leq t \leq [E_2 : E_1]$ و اثبات تمام است. □

لم ۳۰.۳ فرض کنید K یک توسیع F و E_1 و E_2 دو میدان میانی K و F باشند و $E_1 \leq E_2$. اگر $[E_2 : E_1]$ متناهی باشد، آن‌گاه $[E_1' : E_2']$ نیز متناهی است و $[E_1' : E_2'] \leq [E_2 : E_1]$.

اثبات. لم را به کمک استقرا روی $[E_2 : E_1]$ ثابت می‌کنیم. اگر $[E_2 : E_1] = 1$ آن‌گاه $E_1 = E_2$ و حکم به وضوح برقرار است. فرض کنیم $[E_2 : E_1] = n \geq 1$ و فرض کنیم حکم برای هر دو میدان میانی L_1 و L_2 به طوری که $L_1 \leq L_2$ و $[L_2 : L_1] < n$ برقرار باشد. عنصر $u \in E_2 - E_1$ را انتخاب می‌کنیم. خواهیم داشت: $E_1 \leq E_1(u) \leq E_2$ و لذا

$$[E_2' \leq E_1(u)' \leq E_1'$$

پس

$$[E_1' : E_2'] = [E_1' : E_1(u)'] \times [E_1(u)' : E_2']$$

چون E_2 توسیع متناهی E_1 است، u روی E_1 جبریست. فرض کنیم $f(x) \in E_1[x]$ چندجمله‌ای مینیمال u روی E_1 و از درجه t باشد. در این صورت $1 < t \leq n$. اگر $t < n$ آن‌گاه $[E_1(u) : E_1] = t < n$ و $[E_2 : E_1(u)] = n/t < n$. بنابراین از فرض استقرا نتیجه می‌شود

$$[E_1' : E_2'] = [E_1' : E_1(u)'] \times [E_1(u)' : E_2] \leq t \times n/t = n = [E_2 : E_1]$$

و لذا حکم برقرار است. فرض کنیم $t = n$. در این صورت $E_1(u) = E_2$ حال از لم ؟؟؟ نتیجه می‌شود

$$[E_1' : E_2'] \leq [E_2 : E_1].$$

$\square$

نتیجه ۳۱.۳ اگر K یک توسیع متناهی F باشد و $G = Gal(K/F)$. در این صورت

$$|G| \leq [K : F]$$

اثبات. در لم قبل قرار دهید $E_1 = F$ و $E_2 = K$. در این صورت $E_1' = G$ و $E_2' = \{id_{E_2}\}$ و لذا

$$|G| = [G : \{id_{E_2}\}] = [E_1' : E_2'] \leq [E_2 : E_1] = [K : F].$$

$\square$

لم بعد نامساوی مشابه با نامساوی لم قبل را برای زیرگروه‌های G ثابت می‌کند.

لم ۳۲.۳ فرض کنیم K یک توسیع F باشد و $G = Gal(K/F)$. فرض کنیم H_1 و H_2 دو زیرگروه G باشند و $H_1 \leq H_2$. اگر $[H_2 : H_1]$ متناهی باشد، آن‌گاه $[H_1' : H_2']$ نیز متناهی است و

$$[H_1' : H_2'] \leq [H_2 : H_1]$$

اثبات. فرض کنیم $[H_2 : H_1] = n$. نشان می‌دهیم فرض $[H_1' : H_2'] > n$ به تناقض منجر می‌شود. فرض کنیم $[H_1' : H_2'] > n$. لذا می‌توان $u_1, u_2, \ldots, u_{n+1} \in H_1'$ انتخاب کرد که روی H_2' مستقل خطی باشند. فرض کنیم $\{\sigma_1 H_1 = H_1, \sigma_2 H_1, \ldots, \sigma_n H_1\}$ مجموعه‌ی همه همدسته‌های متمایز H_1 در H_2 باشند. دستگاه معادلات خطی همگن

$$\sigma_1(u_1)x_1+\sigma_1(u_2)x_2+\ldots+\sigma_1(u_{n+1})x_{n+1}=0$$
$$\sigma_2(u_1)x_1+\sigma_2(u_2)x_2+\ldots+\sigma_2(u_{n+1})x_{n+1}=0$$
$$\vdots \qquad\qquad \vdots$$
$$\sigma_n(u_1)x_1+\sigma_n(u_2)x_2+\ldots+\sigma_n(u_{n+1})x_{n+1}=0$$

با ضرایب در میدان K دارای n معادله و $n+1$ مجهول و لذا دارای جواب غیر صفری مانند $(x_1,x_2,\ldots,x_{n+1})=(b_1,b_2,\ldots,b_{n+1})\neq(0,0,\ldots,0)$ می‌باشد که در آن $b_1,b_2,\ldots,b_{n+1}\in K$ است. از بین همه‌ی این جواب‌های غیر صفر یک جواب را که دارای کمترین مولفه‌ی غیر صفر است انتخاب می‌کنیم.لذا پس از شماره‌گذاری مجدد مجهول ها (در صورت لزوم)، می‌توان جوابی به صورت

$$(a_1,a_2,\ldots,a_r,0,0,\ldots,0)\in K^{n+1}$$

برای دستگاه ۱ یافت که در آن $a_i\neq 0$، برای هر $1\leq i\leq r$. توجه کنیم که $r\geq 1$ و r کوچکترین مقدار ممکن را دارد. با ضرب کلیه مولفه ها در a_1^{-1}، می توان فرض کرد $a_1=1$. برای رسیدن به تناقض کافی است جواب ناصفری برای دستگاه ۱ بیابیم که تعداد مولفه های ناصفرش از r کمتر باشد. با جاگذاری جواب ؟ در اولین معادله دستگاه (۱) داریم

$$\sigma_1(u_1)a_1+\sigma_1(u_2)a_2+\ldots+\sigma_1(u_{n+1})a_{n+1}=0$$

داریم $\sigma_1\in H_1$ و $u_1,u_2,\ldots,u_r\in H_1'$ و لذا $\sigma_1(u_i)=u_i$ برای هر $1\leq i\leq r$. لذا

$$u_1a_1+u_2a_2+\ldots+u_ra_r=0$$

اگر $a_1,a_2,\ldots,a_r\in H_2'$، آن‌گاه از استقلال خطی $u_1,u_2,\ldots,u_r$ روی H_2' نتیجه می‌شود $a_1=a_2=\ldots=a_r=0$ که خلاف فرض است. پس $2\leq i\leq r$ موجود است که $a_i\notin H_2'$.(توجه کنیم که $a_1=1\in H_2'$) بدون کاستن از کلیت، فرض کنیم $a_2\notin H_2'$. پس $\tau\in H_2$ موجود است به‌نحوی که $\tau(a_2)\neq a_2$. چون ؟ یک جواب دستگاه است، لذا برای $1\leq j\leq n$ داریم

$$\sigma_i(u_۱)a_۱ + \sigma_i(u_۲)a_۲ + \ldots + \sigma_i(u_r)a_r = ۰$$

و لذا

$$\tau(\sigma_i(u_۱))\tau(a_۱) + \tau(\sigma_i(u_۲))\tau(a_۲) + \ldots + \tau(\sigma_i(u_{n+۱}))\tau(a_r) = ۰$$

بنابراین

$$(\tau(a_۱), \tau(a_۲), \ldots, \tau(a_r), ۰, ۰, \ldots, ۰) \in K^{n+۱}$$

یک جواب دستگاه

$$(\tau o \sigma_۱)(u_۱)x_۱ + (\tau o \sigma_۱)(u_۲)x_۲ + \ldots + (\tau o \sigma_۱)(u_{n+۱})x_{n+۱} = ۰$$
$$(\tau o \sigma_۲)(u_۱)x_۱ + (\tau o \sigma_۲)(u_۲)x_۲ + \ldots + (\tau o \sigma_۲)(u_{n+۱})x_{n+۱} = ۰$$
$$\vdots \qquad \vdots$$
$$(\tau o \sigma_n)(u_۱)x_۱ + (\tau o \sigma_n)(u_۲)x_۲ + \ldots + (\tau o \sigma_n)(u_{n+۱})x_{n+۱} = ۰$$

است. ادعا می‌کنیم که دستگاه فوق صرف نظر از ترتیب معادلات همان دستگاه ؟ است. برای اثبات این ادعا، ابتدا توجه می‌کنیم که اگر $\tau\sigma_i H_۱ = \tau\sigma_j H_۱$ آن‌گاه $\sigma_j^{-۱}\sigma_i = (\tau\sigma_j)^{-۱}(\tau\sigma_i) \in H_۱$ و لذا $\sigma_i H_i = \sigma_j H_۱$ و در نتیجه $i = j$ (زیرا $\sigma_۱ H_۱, \sigma_۲ H_۱, \ldots, \sigma_n H_۱$ دو به دو متمایزند).

پس $\{\tau\sigma_۱, \tau\sigma_۲, \ldots, \tau\sigma_n\}$ نیز مجموعه‌ی همه‌ی همدسته‌های متمایز $H_۱$ در $H_۲$ است. فرض کنیم $۱ \leq i \leq n$. در این صورت $\tau\sigma_i H_۱ = \sigma_j H_۱$ برای دقیقاً یک $۱ \leq j \leq n$. لذا $\sigma_j^{-۱}(\tau\sigma_i) \in H_۱$ و در نتیجه $\sigma_j^{-۱}(\tau\sigma_i)(u_s) = u_s$ برای $۱ \leq s \leq n+۱$. یعنی $\tau\sigma_i(u_s) = \sigma_j(u_s)$ برای $۱ \leq s \leq n+۱$. این بدین معنی است که معادله‌ی i-ام در دستگاه ؟ همان معادله‌ی j-ام در دستگاه ؟ است. بنابراین ؟ نیز یک جواب دستگاه ؟ است. چون تفاضل دو جواب یک دستگاه همگن، نیز یک جواب دستگاه است. لذا از جواب های ؟ و ؟ جواب جدید

$$(a_۱ - \tau(a_۱), a_۲ - \tau(a_۲), \ldots, a_r - \tau(a_r), ۰, ۰, \ldots, ۰) \in K^{n+۱}$$

برای دستگاه (۱) بدست می‌آید. اما $a_1 = 1$ و لذا $a_1 - \tau(a_1) = 0$. از طرفی $a_2 \neq \tau(a_2)$ و لذا $a_2 - \tau(a_2) \neq 0$. پس جواب ؟ یک جواب ناصفر دستگاه ؟ با حداکثر $r - 1$ مولفه‌ی غیرصفر است. این متناقض با انتخاب جواب ؟ است. این اثبات لم را کامل می‌کند. □

لم ۳۳.۳ فرض کنیم K یک توسیع F باشد و $G = Gal(K/F)$.

(الف) فرض کنیم E_1 و E_2 دو میدان میانی K و Fباشند، $E_1 \leq E_@$، $[E_2 : E_1]$ متناهی و E_1 بسته باشد. آن‌گاه $[E'_1 : E'_2] = [E_2 : E_1]$ و E_2 بسته است.

(ب) فرض کنیم H_1 و H_2 زیرگروه‌های G باشند، $H_1 \leq H_2$ $[H_2 : H_1]$ متناهی و H_1 بسته باشد. آن‌گاه $[H'_1 : H'_2] = [H_2 : H_1]$ و H_2 بسته است.

اثبات. (الف) بنابه فرض $E''_1 = E$ و بنابر لم ؟، $E_2 \leq E''_2$. لذا با کاربرد مکرر لم‌های ؟ و ؟ داریم

$$[E_2 : E_1] \leq [E''_2 : E_1] = [E''_2 : E''_1] \leq [E'_1 : E'_2] \leq [E_2 : E_1]$$

بنابراین $[E'_1 : E'_2] = [E_2 : E_1]$. به‌علاوه از $[E_2 : E_1] = [E''_2 : E_1]$ نتیجه می‌شود که $E''_2 = E_2$. یعنی E_2 بسته است.

(ب) اثبات شبیه (الف) است. □

لم ۳۴.۳ فرض کنبم Kیک توسیع گالوای متناهی F باشد و $G = Gal(K/F)$. در این صورت

(الف) همه‌ی میدان‌های میانی K و F بسته‌اند.

(ب) $|G| = [K : F]$.

(ج) همه‌ی زیرگروه‌های G بسته‌اند.

اثبات. (الف) بنابه تعریف $F' = G$ و لذا $F'' = G'$. چون K توسیع گالوای F است داریم $G' = F$. پس $F'' = F$. پس F بسته است. اگر E یک میدان میانی دلخواه K وF باشد، آن‌گاه

$[E:F]$ متناهی است و لذا بنابر لم ؟، E بسته است.

(ب) F بسته و $[K:F]$ متناهی است و لذا بنابر لم ؟، K بسته است و

$$[F':K'] = [K:F]$$

اما $F' = G$ و $K' = \{id_K\}$ و لذا $[F':K'] = [G:\{id_K\}] = |G|$. پس

$$|G| = [K:F]$$

(ج) به وضوح $\{id_K\}$ بسته است. اگر H یک زیرگروه G باشد، بنابر (ب) H متناهی است و لذا $[H:\{id_K\}]$ متناهی است. لذا از لم ؟ نتیجه می‌شود H بسته است. $\square$

اثبات قضیه‌ی اساسی گالوا

(الف) از قضیه‌ی ؟ و لم ؟ نتیجه می‌شود.

(ب)از لم ؟ نتیجه می‌شود.

(ج) ابتدا فرض کنیم E روی F گالوا باشد. ثابت می‌کنیم نگاشت

$$\varphi : G \longrightarrow Gal(E/F)$$
$$\varphi(\sigma) = \sigma|_E, \quad \sigma \in G$$

خوش تعریف است و یک همریختی گروه‌ها با هسته‌ی E' است.

ابتدا نشان می دهیم برای هر $\sigma \in G$ داریم $\sigma|_E \in Gal(E/F)$. فرض کنیم $u \in E$ و فرض کنیم $f(x) \in F[x]$ چندجمله‌ای مینیمال u روی F باشد. فرض کنیم $u = u_۱, u_۲, \dots, u_r$ ریشه‌های متمایز f در E باشند و فرض کنیم $g(x) = (x-u_۱)(x-u_۲)\dots(x-u_r)$.

فرض کنیم $\tau \in Gal(E/F)$. ر این صورت برای هر $۱ \leq i \leq r$، $\tau(u_i)$ یک مزدوج u_i روی F است. لذا $\tau(u_i) = u_j$ برای یک $۱ \leq j \leq r$. پس τ یک جایگشت روی $\{u_۱, u_۲, \dots, u_r\}$ القا می‌کند. پس $\tau(g(x)) = g(x)$. پس ضرایب $g(x)$ توسط عناصر $\tau \in Gal(E/F)$ ثابت نگه داشته می‌شوند. لذا $g(x) \in Gal(E/F)'[x]$. بنا به فرض E روی F گالواست و لذا از تعریف گالوا بودن

داریم $Gal(E/F)' = F$. پس $g(x) \in F[x]$. از آن‌جا که $f(x)$ چندجمله‌ای مینیمال u روی F است و $g(u) = g(u_۱) = ۰$، خواهیم داشت $f(x)|g(x)$. اما $degg(x) = ۲ < degf(x)$. پس $f(x) = g(x)$.

حال فرض کنیم $\sigma \in G$. در این صورت $\sigma(u) = u_i$ برای یک $۱ \leq i \leq r$. لذا $\sigma(u) \in E$. پس $\sigma(E) \subseteq E$ و $\sigma|_E \in Gal(E/F)$. داریم $\sigma|_E = id_E$ اگر و تنها اگر $\sigma \in E'$. لذا $ker\varphi = E'$. پس E' زیرگروه نرمال G است و $G/E' \cong \varphi(G)$. بنابر لم ؟ داریم

$$|\varphi(G)| = |G/E'| = [G : E'] = [E'' : G'] = [E : F]$$

اما بنابر (الف) $Gal(E/F) = [E : F]$. بنابراین φ پوشاست و لذا $G/E' \cong Gal(E/F)$.

برعکس، فرض کنیم E' در G نرمال باشد. فرض کنیم $\sigma \in G$ و $u \in E$. برای هر $\tau \in E'$ داریم $\sigma^{-۱}\tau\sigma \in E'$، و لذا $\sigma^{-۱}\tau\sigma(u) = u$ و در نتیجه $\tau\sigma(u) = \sigma(u)$. پس $\sigma(u) \in E''$. اما بنابر لم؟، $E'' = E$. پس $\sigma(u) \in E$ و لذا $\sigma|_E \in Gal(E/F)$.

فرض کنیم $u \in E - F$. چون K روی F گالواست $\sigma \in G$ وجود دارد که $\sigma(u) \neq u$. حال $\sigma|_E \in Gal(E/F)$ و $\sigma|_E(u) \neq u$. پس $u \notin Gal(E/F)'$. پس $Gal(E/F)' = F$. این یعنی E روی F گالواست و اثبات تمام است.

نتیجه ۳۵.۳ (قضیه‌ی آرتین) فرض کنیم K یک میدان و G یک زیرگروه از گروه K باشد. فرض کنیم

$$F = \{u \in K : \ \sigma(u) = u, \ \ \forall \sigma \in G\}$$

در این صورت (الف) K روی F گالواست.

(ب) اگر G متناهی باشد، آنگاه K یک توسیع متناهی F است و $G = Gal(K/F)$.

اثبات. (الف) فرض کنیم $G_۱ = Gal(K/F)$. روشن است که $G \leq G_۱$. فرض کنیم $u \in K - F$. در این صورت با توجه به تعریف F، $\sigma \in G$ یافت می‌شود که $\sigma(u) \neq u$. اما از $G \leq G_۱$ نتیجه

می‌شود $\sigma \in G$. بنابراین K روی F گالواست.

(ب)فرض کنیم Gمتناهی باشد. از لم ؟ نتیجه می‌شود:

$$[K:F] = [\{id_K\}' : G'] \leq [G : \{id_K\}] = |G|$$

بنابراین K یک توسیع متناهی F است. حال از لم ؟ نتیجه می‌شود که $G = G''$. اما بنا به فرض $G' = F$ و لذا $G'' = F'$. و $G_1 = F' = G'' = G$. $\square$

فصل ۴
توسیع‌های نرمال و جدایی‌پذیر

در اثبات قضیه‌ی ؟؟؟ دیدیم که اگر E روی F گالوا و جبری باشد و $u \in E$، آن‌گاه چندجمله‌ای مینیمال u روی F به صورت $g(x) = (x-u_۱)(x-u_۲)\dots(x-u_r)$ است که در آن u_iها متمایزند و $u_i \in E$ برای $۱ \leq i \leq r$. این نتیجه ما را به دو تعریف ذیل رهنمون می‌سازد و شرایطی معادل گالوا بودن بدست می‌دهد:

تعریف ۱.۴ فرض کنیم E یک توسیع جبری F باشد و فرض کنیم $\overline{E}$ یک بستار جبری برای E باشد.

(الف) گوییم E یک توسیع نرمال Fاست هرگاه برای هر $u \in E$، اگر $v \in \overline{E}$ مزدوج u روی F باشد آنگاه $v \in E$.

(ب) گوییم E یک توسیع جداپذیر Fاست هرگاه برای هر $u \in E$ اگر u روی F جبری از درجه‌ی n باشد آن‌گاه u دارای n ریشه متمایز در $\overline{E}$ باشد.

تذکر ۲.۴ فرض کنیم E یک توسیع نرمال Fباشد و $u \in E$ و فرض کنیم $f(x) \in F[x]$ چندجمله‌ای مینیمال u روی F باشد. در این صورت در $\overline{E}[x]$ داریم

$$f(x) = (x - u_۱)(x - u_۲)\dots(x - u_n)$$

که در آن $u_۱, u_۲, \dots, u_n \in \overline{E}$ مزدوج‌های u روی F و لذا در Eهستند. لذا $f(x)$ در $E[x]$ به حاصل‌ضرب عوامل درجه ۱ تجزیه می‌شود. مثال زیر نشان می‌دهد که این مزدوج‌ها ممکن است متمایز نباشند.

مثال ۳.۴ فرض کنیم p یک عدد اول و y یک مجهول باشد. قرار دهید $E = \mathbb{F}_p(y)$ و $F = \mathbb{F}_p(y^p)$. در این صورت E یک توسیع F است. $y \in E$ روی Fجبری با چندجمله‌ای مینیمال $f(x) = x^p - y^p \in F[x]$ است.(ثابت کنید). اما $f(x) = (x-y)^p \in E[x]$. لذا تنها مزدوج y روی F، خود y است.
در اثبات قضیه‌ی ؟؟؟ در واقع ثابت کرده‌ایم که هر توسیع جبری گالوا، یک توسیع نرمال و جداپذیر است. عکس این نیز درست است. برای اثبات این مطلب به قضیه‌ی زیر نیاز داریم.

قضیه ۴.۴ فرض کنیم K یک توسیع جبری Fو $\sigma : F \longrightarrow L$ یک یکریختی میدان‌ها باشد. فرض کنیم $\overline{L}$ یک بستار جبری برای L باشد. در این صورت تکریختی $\tau : E \longrightarrow \overline{L}$ موجود است که $\tau|_F = \sigma$. به عبارت دیگر σ را می‌توان به یک تکریختی $\tau : E \longrightarrow \overline{L}$ توسعه داد.

اثبات. فرض کنیم

$\mathcal{A} = \{(E,\lambda) :$ $F \le E \le K$ یک میدان میانی است و $\lambda : E \longrightarrow \overline{L}$ یک تکریختی است و $\lambda|_F = \sigma\}$

داریم $(F, \sigma) \in \mathcal{A}$ و لذا $\mathcal{A}$ ناتهی است. برای $(E_۱, \lambda_۱) \in \mathcal{A}$ و $(E_۲, \lambda_۲)$ تعریف می‌کنیم

$(E_۱, \lambda_۱) \le (E_۲, \lambda_۲)$ اگر و تنها اگر $E_۱ \le E_۲$ و $\lambda_۲|_{E_۱} = \lambda_۱$

به آسانی می‌توان دید این رابطه، یک رابطه‌ی ترتیب جزئی روی $\mathcal{A}$ است. فرض کنیم $\mathcal{B} \subseteq \mathcal{A}$ یک زیرمجموعه‌ی کاملاً مرتب(زنجیر) از $\mathcal{A}$ باشد. در این صورت تعریف می‌کنیم $E_۱ = \bigcup_{(E,\lambda)\in\mathcal{B}} E$ و $\lambda_۱ : E_۱ \longrightarrow \overline{L}$ که در آن برای هر $u_۱ \in E$

$$u \in E \text{ و } (E,\lambda) \in \mathcal{B} \text{ و } \lambda_۱(u) = \lambda(u)$$

چون $\mathcal{B}$ کاملاً مرتب است، $F \leq E_۱ \leq K$ یک میدان میانی است(ثابت کنید) و $\lambda_۱$ خوش تعریف است(ثابت کنید). به‌علاوه $\lambda_۱|_F = \sigma$. بنابراین $(E_۱, \lambda_۱) \in \mathcal{A}$. روشن است که $(E_۱, \lambda_۱)$یک کران بالا برای $\mathcal{B}$ در $\mathcal{A}$ است. پس هر زیرمجموعه‌ی کاملاً مرتب $\mathcal{A}$ دارای کران بالا در $\mathcal{A}$ است. لذا بنابر لم زرن $\mathcal{A}$ دارای عضو ماکسیمالی مانند $(E_۰, \lambda_۰)$ است. برای اثبات قضیه کافی است ثابت کنیم $E_۰ = K$. فرض کنیم چنین نباشد. پس $\alpha \in K - E_۰$ موجود است. بنا به فرض α روی F و در نتیجه روی $E_۰$ جبری است. فرض کنیم $p(x) \in E_۰[x]$ چندجمله‌ای مینیمال α روی $E_۰$ باشد. در این صورت

$$\varphi_\alpha : \frac{E_۰[x]}{\langle p(x)\rangle} \longrightarrow E_۰(\alpha)$$
$$\varphi_\alpha(f(x) + \langle p(x)\rangle) = f(\alpha) \text{ و } f(x) \in E_۰[x]$$

یک یکریختی است.(چرا؟). فرض کنیم $K_۰ = \lambda(E_۰)$. در این صورت $\lambda : E_۰ \longrightarrow K_۰$ یک یکریختی است و لذا

$$\lambda_x : E_۰[x] \longrightarrow K_۰[x]$$
$$a_۰, a_۱, \ldots, a_n \in E_۰, \lambda_x(a_۰+a_۱x+\ldots+a_nx^n) = \lambda(a_۰)+\lambda(a_۱)x+\ldots+\lambda(a_n)x^n \in K_۰[x]$$

یک یکریختی حلقه‌هاست.(ثابت کنید). لذا اگر قرار دهیم $q(x) = \lambda_x(p(x)) \in K_۰[x]$، آن‌گاه

$$\overline{\lambda_x} : \frac{E_۰[x]}{\langle p(x)\rangle} \longrightarrow \frac{K_۰[x]}{\langle q(x)\rangle}$$
$$\overline{\lambda_x}(f(x) + \langle q(x)\rangle) = \lambda_x(f(x)) + \langle q(x)\rangle$$

یک یکریختی حلقه‌هاست. حال $q(x)$ دارای ریشه‌ای چون β در $\overline{K}$ است. و

$$\varphi_\beta : \frac{K_۰[x]}{\langle q(x)\rangle} \longrightarrow K_۰(\beta)$$
$$\varphi_\beta(f(x) + \langle q(x)\rangle) = f(\beta) \text{ و } f(x) \in K_۰[x]$$

نیز یک یکریختی است. حال

$$E_\circ(\alpha) \xrightarrow{\varphi_\alpha^{-1}} \frac{E_\circ[x]}{\langle p(x)\rangle} \xrightarrow{\overline{\lambda_x}} \frac{K_\circ[x]}{\langle q(x)\rangle} \xrightarrow{\varphi_\beta} K_\circ(\beta) \hookrightarrow \overline{K}$$

یک تکریختی است. به‌علاوه برای $u \in E$ داریم

$$u \longrightarrow u + \langle p(x)\rangle \longrightarrow \lambda(u) + \langle q(x)\rangle \longrightarrow \lambda(u) \longrightarrow \lambda(u)$$

بنابراین اگر ترکیب فوق را $\lambda'_\circ$ بگذاریم، آن‌گاه $(E_\circ(\alpha), \lambda'_\circ) \in \mathcal{A}$. این با ماکسیمال بودن $(E_\circ, \lambda_\circ)$ در $\mathcal{A}$ متناقض است. و اثبات تمام است. $\square$

قضیه ۵.۴ فرض کنیم K یک توسیع جبری F باشد. در این صورت K روی F گالواست، اگر و تنها اگر K روی F نرمال و جداپذیر باشد.

اثبات. فرض کنیم K روی F گالوا باشد. و فرض کنیم $G = Gal(K/F)$. فرض کنیم $u \in K$ و فرض کنیم $p(x) \in F[x]$ چندجمله‌ای مینیمال u روی F باشد. فرض کنیم $u_1 = u, u_2, \dots, u_r$ ریشه‌های $p(x)$ در K باشد. قرار می‌دهیم

$$g(x) = (x-u_1)(x-u_2)\dots(x-u_r) \in K[x]$$

فرض کنیم $\sigma \in G$ دلخواه باشد. در این صورت

$$\sigma(g(x)) = (x-\sigma(u_1))(x-\sigma(u_2))\dots(x-\sigma(u_r))$$

برای هر $1 \le i \le r$، $\sigma(u_i)$ مزدوج u_i روی F است. اما مزدوج‌های u در K دقیقاً $u = u_1, u_2, \dots, u_r$ هستند. لذا $\sigma(u_i) = u_j$ برای یک $1 \le j \le r$ پس $\sigma(g(x)) = g(x)$. فرض کنیم

$$g(x) = a_\circ + a_1 x + \dots + a_r x^r \in E[x]$$

در این صورت

$$\sigma(g(x)) = \sigma(a_\circ) + \sigma(a_1)x + \ldots + \sigma(a_r)x^r = a_\circ + a_1x + \ldots + a_rx^r$$

لذا برای هر $\circ \leq i \leq r$ و هر $\sigma \in G$ داریم $\sigma(a_i) = a_i$. لذا

$$a_i \in G' \text{ و } \circ \leq i \leq r$$

اما چون بنابه فرض K روی F گالواست، داریم $G' = F$. پس $a_i \in F$، $\circ \leq i \leq r$. لذا $g(x) \in F[x]$. همچنین $g(u) = \circ$. چون $f(x) \in F[x]$ چندجمله‌ای مینیمال u روی F است داریم $f(x)|g(x)$، و لذا $deg(f(x)) \leq deg(g(x))$. از طرفی $u_1, u_2, \ldots, u_r$ ریشه‌های متمایز F اند، لذا $deg(F(x)) \geq r = deg(g(x))$. پس $deg(f(x) =) = deg(g(x))$. پس $g(x) = cf(x)$، برای یک $c \in F$. $f(x)$ و $g(x)$ هر دو تکین هستند و لذا $c = 1$. پس $f(x) = g(x)$.

پس K یک توسیع نرمال و جداپذیر F است.

برعکس، فرض کنیم K یک توسیع نرمال و جداپذیر F باشد و فرض کنیم $G = Gal(K/F)$. فرض کنیم $u \in K - F$. فرض کنیم $f(x) \in F[x]$ چندجمله‌ای مینیمال u روی F باشد. چون $u \in F$، لذا $n = deg(f(x)) \geq 2$ چون توسیع جداپذیر Fاست لذا $f(x)$ دارای n ریشه متمایز در $\overline{K}$ است. پس $v \in \overline{K}$ موجود است که $f(v) = \circ$ و $v \neq u$. چون K روی F نرمال است، لذا $v \in K$. F-یکریختی

$$\varphi_{u,v} : F(u) \longrightarrow F(v)$$

را در نظر می‌گیریم. بنابر قضیه‌ی ؟؟؟ یکریختی

$$\sigma : K \longrightarrow \overline{K}$$

موجود است که $\sigma|_{F(u)} = \varphi_{u,v}$. فرض کنیم $\alpha \in K$. در این صورت $\sigma(\alpha) \in \overline{K}$ یک مزدوج α روی F است، و چون Kروی F گالواست $\sigma(\alpha) \in K$. پس $\sigma(K) \subseteq K$ و لذا $\sigma \in G$. حال

$G' = F$. پس $F \le G'$. اما به وضوح $G' \le F$. پس $u \notin G'$. و لذا $\sigma(u) = \varphi_{u,v}(u) = v \neq u$
پس K توسیع گالوای F است. □

تعریف ۶.۴ فرض کنیم F یک میدان، $\overline{F}$ یک بستار جبری برای F و $f(x) \in F[x]$ یک چندجمله‌ای غیرثابت باشد. فرض کنیم $\alpha_۱, \alpha_۲, \ldots, \alpha_n \in \overline{F}$ کلیه‌ی ریشه‌های $f(x)$ باشند. در این صورت $K = F(\alpha_۱, \alpha_۲, \ldots, \alpha_n)$ را یک میدان شکافنده برای $f(x)$ روی F گوییم. توجه کنید که میدان شکافنده $f(x)$ روی F، کوچکترین زیرمیدان $\overline{F}$ است که $f(x)$ در آن به حاصل‌ضرب چندجمله‌ای‌های درجه‌ی یک تجزیه می‌شود.

لم ۷.۴ فرض کنیم $\sigma : F_۱ \longrightarrow F_۲$ یک یکریختی میدان‌ها باشد و $f(x) \in F_۱[x]$. فرض کنیم $K_۱$ یک میدان شکافنده برای f روی $F_۱$ و $K_۲$ یک میدان شکافنده برای $\sigma(f)$ روی $F_۲$ باشد. در این صورت یکریختی $\tau : K_۱ \longrightarrow K_۲$ موجود است که $\tau|_{F_۱} = \sigma$.

اثبات. اثبات با استقرا روی $[K_۱ : F_۱]$. اگر $[K_۱ : F_۱] = ۱$ آن‌گاه $K_۱ = F_۱$ و لذا $f(x)$ در $F_۱[x]$ به حاصل‌ضرب عوامل درجه یک تجزیه می‌شود(ثابت کنید). و لذا $K_۲ = F_۲$. و لذا می‌توان τ را همان σ گرفت. فرض کنیم حکم برای $[K_۱ : F_۱] < n$ برقرار باشد و فرض کنیم $[K_۱ : F_۱] = n \geq ۲$. پس همه‌ی ریشه‌های $f(x)$ در $F_۱$ نیست. لذا $f(x)$ یک عامل تحویل‌ناپذیر مانند $p(x)$ در $F_۱[x]$ دارد که $deg(p(x) \geq ۲$. قرار می‌دهیم $q(x) = \sigma(p(x))$. $q(x)$ در $F_۲[x]$ تحویل‌ناپذیر است. بنا به فرض $p(x)$ در $K_۱$ دارای ریشه‌ای چونα و $q(x)$ در $K_۲$ دارای ریشه‌ای چون β است. مشابه آنچه در اثبات قضیه‌ی ؟؟؟ دیدیم یکریختی $\sigma_۱ : F_۱(\alpha) \longrightarrow F_۲(\beta)$ موجود است که $\sigma_۱|_{F_۱} = \sigma$. حال $K_۱$ میدان تجزیه‌گر f روی $F_۱(\alpha)$ و $K_۲$ میدان تجزیه گر $\sigma_۱(f)$ روی $F_۲(\beta)$ است. به‌علاوه

$$[K_۱ : F_۱(\beta)] \leq [K_۱ : F_۱]$$

لذا بنابه فرض استقرا $\tau : K_1 \longrightarrow K_2$ موجود است که $\tau|_{F_1(\alpha)} = \sigma_1$. چون $\sigma_1|_F = \sigma$ لذا $\tau|_{F_1} = \sigma$ و اثبات تمام است. $\square$

قضیه ۸.۴ فرض کنیم Fیک میدان، $f(x) \in F[x]$ و K یک میدان تجزیه‌گر $f(x)$ روی F باشد. فرض کنیم K روی F جداپذیر باشد. در این صورت K روی Fگالواست.

اثبات. ابتدا توجه می‌کنیم که $K : F$ متناهی است. بنابراین بنابر لم ؟؟؟، $G = Gal(K/F)$ متناهی است. فرض کنیم F_0 میدان ثابت G باشد. در این‌صورت $F \leq F_0$. و بنابر نتیجه‌ی؟؟؟ K روی F گالواست و $G = Gal(K/F_0)$. لذا بنابر قضیه‌ی؟؟؟، $|G| = [K : F_0]$ بنابراین کافیست ثابت کنیم $[K : F] = |G|$. این را با استقرا روی $h = [K : F]$ ثابت می‌کنیم.
حالت $n = 1$ بدیهی است. فرض کنیم $n > 1$ و فرض کنیم حکم برای زمانی که $[K : F] < n$ برقرار باشد. چون $k \neq F$، f در F به عوامل درجه یک تجزیه نمی‌شود. پس چندجمله‌ای تحویل‌ناپذیر $p(x) \in F[x]$ از درجه‌ی $s \geq 2$ موجود است که $p(x)|f(x)$. چون $f(x)$ در $K[x]$ به عوامل درجه یک تجزیه می‌شود لذا $p(x)$ دارای s ریشه‌ی متمایز $u_1, u_2, \ldots, u_s$ در K است. فرض کنیم $H = Gal(K/F(u_1))$. بنابر آنچه در اثبات لم ؟؟؟ دیدیم، نگاشت

$$\varphi : G/H \longrightarrow \{u_1, u_2, \ldots, u_s\}$$

$$\varphi(\sigma H) = \sigma(\alpha_1)$$

یک به یک است(G/H در این‌جا مجموعه‌ی همدسته‌های چپ H در Gاست). حال فرض کنیم $1 \leq i < s$. بنابر لم ؟؟؟، F- یکریختی $\varphi_{u_1,u_i} : F(u) \longrightarrow F(u_i)$ به یکریختی $\lambda_i : K \longrightarrow K$ توسعه می‌یابد. حال $\lambda_i \in G$ و $\varphi(\lambda_i) = u_i$. پس φ پوشاست. لذا $|G/H| = s$. حال

$$[K : F] = [K : F(u_1)][F(u_1) : F]$$

بنا به فرض استقرا $[K : F(u_1)] = |H|$. همچنین $[F(u_1) : F] = deg(p(x)) = s$. لذا

$$[K:F] = |H|s = |H| \times \frac{|G|}{|H|} = |G|$$

و اثبات تمام است. $\square$

نتیجه ۹.۴ فرض کنیم $f(x) \in \mathbb{Q}[x]$ یک چندجمله‌ای غیرثابت و $K \subseteq \mathbb{C}$ یک میدان تجزیه‌گر $f(x)$ روی $\mathbb{Q}$ در این‌صورت K روی $\mathbb{Q}$ گالواست.

اثبات. اگر F دارای مشخصه‌ی صفر باشد، آن‌گاه هر توسیع آن جداپذیر است(ثابت کنید). بنابراین K روی $\mathbb{Q}$ جداپذیر است. حال از قضیه‌ی ؟؟؟ نتیجه می‌شود که Kروی $\mathbb{Q}$ گالواست. $\square$

در قضیه‌ی ؟؟؟ وجود و یکتایی بستار میدان را بیان کردیم. اثبات یکتایی با استفاده از قضیه‌ی ؟؟؟ ساده است.

قضیه ۱۰.۴ اگر F یک میدان و F_1 و F_2 هر دو بستار جبری F باشند، آن‌گاه F_1 و F_2، F-یکریخت هستند.

اثبات. نگاشت $id_F : F \longrightarrow F$ را در نظر می‌گیریم چون $\overline{F_1}$ توسیع جبری F است لذا بنابر قضیه‌ی ؟؟؟، تکریختی $\sigma : \overline{F_1} \longrightarrow \overline{F_2}$ موجود است که $\sigma|_F = id_F$. حال $\sigma^{-1} : \sigma(\overline{F_1}) \longrightarrow \overline{F_1}$ یک تکریختی و $\overline{F_2}$ روی $\sigma(\overline{F_1})$ جبری است. لذا $\tau : \overline{F_2} \longrightarrow \overline{F_1}$ موجود است که $\tau|_{\sigma(\overline{F_1})} = \sigma^{-1}$. فرض کنیم $\beta \in \overline{F_2}$. لذا $\tau(\beta) = \alpha \in \overline{F_1}$. حال $\sigma(\alpha) = \gamma \in \sigma(\overline{F_1})$ و لذا $\alpha = \sigma^{-1}(\gamma)$ پس $\tau(\gamma) = \alpha$. در نتیجه $\beta = \gamma \in \sigma(\overline{F_1})$ و لذا σ پوشاست و اثبات تمام است. $\square$