نظریهٔ گالوا

پاوامن مورتی
و همکاران

ترجمهٔ محمدتقی دیبایی

نظریهٔ گالوا

پاوامن مورتی
و همکاران

ترجمهٔ محمدتقی دیبایی

مرکز نشر دانشگاهی، تهران

بسم الله الرحمن الرحیم

فهرست مطالب

عنوان	صفحه

یادداشت سردبیر

این کتاب کوچك کــه درباب نظریهٔ گالواست، سومین کتاب ازسری جزوات ریاضی است که انتشار آنها از ۱۹۶۳ آغاز شده است. این کتاب شامل مطالب تجدید نظر شدهٔ یادداشتهای مربوط بــه درسهایی است کــه توسط ام. پاوامن‌مورتی، ك. جی. راماناتان، سی. اس. سشادری، یو. شوکلا و آر. سریدهــاران در تابستان ۱۹۶۴ درطول ۴ هفته، بــه گروهی متشکل از دانشجویان ومعلمین کــه برخی درجبر مبتدی بودند ارائه شده است. این درس علاقــه و اشتیاق حاضرین را برانگیخت. امتنان خاص به مؤلفان وبه پروفسور ام. اس. ناراسیمهان، که به‌عنوان رئیس کمیتهٔ دورهٔ تابستانی مسئول تشکیل این دوره بود، ابراز می‌گردد. تشکر شخصی خود را به پروفسور راقاوان ناراسیمهان کــه عملاً ویرایش این اثر را انجام داده است ابراز می‌دارم.

ك. چاندراسخاران

پیشگفتار

این جزوه مشتمل است بریادداشتهای مربوط به‌درسهایی که درباب نظریهٔ گالوا در ۱۹۶۴، دریك دورهٔ تابستانی انستیتو تاتا برای تحقیقات بنیادی تدریس شده‌است. شرکت‌کنندگان عده‌ای ازمعلمین ودانشجویان دانشگاههای هند بودند که به‌کسب اطلاعاتی کلـی در باب این‌موضوع علاقه داشتند. سخنرانان عبارت بودنداز ام. پاوامن مورتی، ك.جی.رامانا تان سی.اس.سشادری، یو.شوکلا و آر.سریدهاران.

مقدمات نظریهٔ مجموعه‌ها دانسته فرض می‌شوند. فصول ۱ و ۲ به‌مباحثی از گروهها، حلقه‌ها و فضاهای برداری، به میزان لازم برای مطالعهٔ نظریهٔ گالوا، اختصاص دارند. در فصل ۳، توسیعهای میدان تاحدی به‌تفصیل مورد مطالعه قرارمی گیرند؛ این‌فصل باقضیه‌ای در باب سادگی یك توسیع جداپذیر متناهی خاتمه می‌یابد. قضیهٔ بنیادی نظریهٔ گالوا در فصل ۴ ثابت می‌شود. درفصل ۵، کاربردهایـی از نظریهٔ گالوا جهت حل معادلات جبری وترسیمات هندسی ارائه می گردد.

فصل ۱

گروه

۱. گروه و هomomorفیسم

تعریف. یك گروه زوجی است مـانند (G, ψ) که در آن G یك مجموعـه است و $\psi: G\times G \to G$ نگاشتی است با ویژگیهای ذیل ($\psi(x, y)$ با xy نشان داده میشود):

آ. بهازای هر $x, y, z \in G$ ، $(xy)z = x(yz)$ (شرکتپذیری)،

ب. عضوی مانند e در G وجود داردکه به ازای هر $x\in G$، $ex = xe = x$،

ج. اگر $x\in G$، عضوی مانند $x'\in G$ وجود دارد که

$$x'x = xx' = e.$$

چند تذکر: ۱. نگاشت ψ را عمل گروه مینامند و وقتی از مضمون روشن باشد، گروه را مختصراً با G نمایش میدهند.

۲. عضو e منحصر بهفرد است. زیرا اگر $e_1\in G$ چنان باشد که بهازای هر $x\in G$ ، $e_1x = xe_1 = x$ ، آنگاه، درحالت خاص، داریم $e = ee_1 = e_1$. عضو e را عضوهمانی G مینامند.

۳. به ازای هر $x\in G$ ، عضو $x'\in G$ منحصر به فرد است. زیرا اگر $x''\in G$ چنان باشدکه $x''x = xx'' = e$ ، آنگاه

$$x'' = x''e = x''(xx') = (x''x)x' = ex' = x'.$$

عضو x' را وارون x مینامند و آن را با x^{-1} نمایش میدهند.

۴. بنابر خاصیت شرکتپذیری، با فرض $x, y, z\in G$ ، تعریف می‌کنیم

$$xyz=(xy)z=x(yz).$$

به‌طور کلی، حاصلضرب $x_1x_2\ldots x_n$ که در آن $x_1, x_2, \ldots, x_n\in G$ ، خوشتعریف است (اثبات به استقرا). به‌ازای $x\in G$، می‌نویسیم:

(i) به ازای $n>0$ ، $x^n=xx\ldots x$ (n عامل)،

(ii) $x^0=e$،

(iii) به‌ازای $n<0$ ، $x^n=(x^{-1})^{-n}$.

گروهی مانند G را آبلی یا تعویضپذیر گویند، هرگاه

به‌ازای هر $x, y\in G$ ، $xy=yx$.

دریک گروه آبلی، گاهی می‌نویسیم $\psi(x, y)=x+y$ و در این گروه عمل را جمع می‌خوانیم. در این صورت همانی را با 0 و وارون عضوی مانند x را با $-x$ نمایش می‌دهیم. همچنین می‌نویسیم:

اگر $n>0$ ، $nx=x+x+\ldots+n$ (n جمله)،

$0x=0$،

اگر $n<0$ ، $nx=(-n)(-x)$.

گروهی‌مانند G را یك گروه متناهی گویند اگرمجموعهٔ G متناهی باشد. تعداداعضای یك گروه متناهی را مرتبهٔ آن می‌نامند.

چند مثال: ۱. مجموعهٔ $\mathbf{Z}$ (به‌ترتیب $\mathbf{Q}$ ، $\mathbf{R}$ ، $\mathbf{C}$) تحت جمع «معمولی» یك گروه آبلی است.

۲. مجموعهٔ $\mathbf{Q}^*$ (به‌ترتیب، $\mathbf{R}^*$ ، $\mathbf{C}^*$) متشکل از اعداد ناصفرگویا (به ترتیب، حقیقی، مختلط) تحت ضرب «معمولی» یك گروه آبلی است.

۳. مجموعهٔ $\mathbf{Z}/(m)$ متشکل از رده‌های مانده‌ای به هنگ m ، که درآن m عددی است صحیح، تحت عمل جمع $\bar{r}+\bar{s}=\overline{r+s}$ با فرض $\bar{r}, \bar{s}\in\mathbf{Z}/(m)$ ، یك گروه است.

۴. هرنگاشت یك به یك از مجموعهٔ $I_n=\{1, 2, \ldots, n\}$ به روی I_n را یك جایگشت می‌نامند. مجموعهٔ تمام جایگشتهای I_n یك گروه است؛ عمل گروه همان ترکیب نگاشتها است. این گروه را گروه متقارن از درجهٔ n می‌نامند و با S_n نمایش می‌دهند. اگر $\sigma\in S_n$ ، می‌نویسیم

$$\sigma=\begin{pmatrix}1 & 2 & \ldots & n\\ \sigma(1) & \sigma(2) & \ldots & \sigma(n)\end{pmatrix}$$

به ازای $n\geqslant 3$ ، S_n آبلی نیست. مرتبهٔ S_n مساوی با $n!$ است.

تعریف. فرض کنیم G و G' گروه باشند. نگاشتی چون $f: G \to G'$ را یک هومومورفیسم می‌نامیم هرگاه به‌ازای هر $x, y \in G$ ، $f(xy) = f(x)f(y)$.

چند تذکر: ۱. به‌ازای هر گروه G، نگاشت همانی $I_G: G \to G$ یک هومومورفیسم است.

۲. اگر $f: G \to G'$ و $g: G' \to G''$ هومومورفیسم باشد، آنگاه نگاشت $g \circ f G \to G''$ نیز یک هومومورفیسم است.

تعریف. یک هومومورفیسم $f: G \to G'$ را ایزومورفیسم گویند اگر هومومورفیسمی مانند $g: G' \to G$ وجود داشته باشد که $g \circ f = I_G$ و $f \circ g = I_{G'}$. در این صورت می‌نویسیم $G \approx G'$. ایزومورفیسمی چون $f: G \to G$ را یک اتومورفیسم می‌نامند.

چند تذکر: ۱. یک هومومورفیسم یک ایزومورفیسم است اگر وفقط اگر یک به یک و به رو باشد.

۲. یک هومومورفیسم عضو همانی را به‌عضو همانی و وارون هر عضو را به‌وارون تصویر آن عضو می‌نگارد.

چند مثال: ۱. نگاشت طبیعی $q: \mathbf{Z} \to \mathbf{Z}/(m)$ که باضابطهٔ $q(r) = \bar{r}$ ، $r \in \mathbf{Z}$ ، تعریف می‌شود هومومورفیسمی به‌رو است. و این به‌ازای $m \neq ۰$ یک ایزومورفیسم نیست.

۲. نگاشت $f: \mathbf{R} \to \mathbf{Z}$ باضابطهٔ $f(n) = ۲n$ ، یک هومومورفیسم یک به‌یک است که به‌رو نیست.

۳. نگاشت $f: \mathbf{R} \to \mathbf{R}^{*+}$ ($\mathbf{R}^{*+}$ مجموعهٔ اعداد حقیقی مثبت ناصفر است) با ضابطهٔ $f(x) = a^x$ که در آن a یک عدد حقیقی ثابت مثبت بزرگتر از ۱ است و $x \in \mathbf{R}$، یک ایزومورفیسم است.

۴. فرض کنید G یک گروه باشد و $a \in G$. نگاشت $f_a: G \to G$ با ضابطهٔ $f_a(x) = axa^{-۱}$ که در آن $x \in G$ ، اتومورفیسمی است موسوم به اتومورفیسم داخلی داده شده به وسیلهٔ a.

۲. زیرگروه وگروه خارج قسمت

تعریف. زیرگروهی مانند H ازیک گروه G به زیرمجموعه‌ای غیرتهی چون H از G اطلاق می‌شودکه به‌ازای هر $x, y \in H$ ، $x^{-۱}y \in H$.

چند تذکر: ۱. همانی e از G به H تعلق دارد. همچنین اگر $x \in H$ ، آنگاه $x^{-۱} \in H$. در واقع، H تحت عمل القایی گروه یک گروه است.

۲. نگاشت شمول $i: H \to G$ با ضابطهٔ $i(x) = x$ که در آن $x \in H$ ، یک هومومورفیسم است.

چند مثال: ۱. G و $\{e\}$ زیرگروههایی از G هستند.

۲. $\mathbf{Z}$ زیرگروهی از $\mathbf{Q}$، $\mathbf{Q}$ زیرگروهی از $\mathbf{R}$ و $\mathbf{R}$ زیرگروهی از $\mathbf{C}$ است.

۳. مجموعهٔ اعداد صحیح زوج زیرگروهی از $\mathbf{Z}$ است.

فرض کنید $f: G \to G'$ همومورفیسمی گروهی باشد. مجموعهٔ $f(G)$ زیرگروهی از G' است. اگر e' همانی G' باشد، مجموعهٔ $\{x \in G \mid f(x)=e'\}$ زیرگروهی از G است موسوم به هستهٔ f که با $\ker f$ نمایش داده می‌شود. به‌طورکلی، تصویر وارون هر زیرگروهی از G' زیرگروهی از G است.

اشتراك خانواده‌ای از زیرگروههای یك گروه، یك زیرگروه است. اگر S زیرمجموعه‌ای از گروه G باشد، اشتراك خانوادهٔ تمام زیرگروههایی از G که S را دربر داشته باشند زیرگروه پدید آمده توسط S نامیده می‌شود. اگر S متشکل از تنها یك عضو a باشد، زیرگروه پدید آمده توسط $\{a\}$ را زیرگروه دوری پدید آمده توسط a می‌نامند. به سهولت دیده می‌شود که زیرگروه دوری پدیدآمده توسط a متشکل از توانهای a است. گروهی مانند G را دوری گویند اگر بریك زیرگروه دوری پدید آمده توسط یك عضو $a \in G$ منطبق باشد.

چند مثال: ۱. $\mathbf{Z}$ یك گروه دوری نامتناهی است و توسط ۱ پدید می‌آید.

۲. $\mathbf{Z}/(m)$ یك گروه دوری از مرتبهٔ $|m|$ است، هرگاه $m \neq ۰$.

قضیهٔ ۱. هرزیرگروه H از $\mathbf{Z}$ دوری است.

برهان. درحالتی‌که $H=\{۰\}$، چیزی برای اثبات باقی نمی‌ماند. اگر $H \neq \{۰\}$، فرض می‌کنیم m کوچکترین عدد صحیح مثبت در H باشد. حال به‌ازای هر $n \in \mathbf{Z}$، می‌دانیم q و r ی در $\mathbf{Z}$ وجود دارند که $n=qm+r$ و $۰ \leqslant r < m$. اگر $n \in H$، آنگاه $r=n-qm \in H$، واز آنجا نتیجه می‌شود که $r=۰$. دراین‌صورت $H=m\mathbf{Z}$. $\square$

قرارداد. به‌ازای زیرمجموعه‌های A و B ازگروهی مانند G، قرار می‌گذاریم که $AB=\{ab \mid a \in A,\, b \in B\}$. اگر $A=\{a\}$، به‌جای $\{a\}B$ می‌نویسیم aB؛ همین طور اگر $B=\{b\}$، به‌جای $A\{b\}$ می‌نویسیم Ab. اگر $A, B, C \subset G$، بدیهی است که $(AB)C=A(BC)$ و به‌جای هریك از آنها می‌نویسیم ABC.

فرض کنید G یك گروه و H زیرگروهی از آن باشد. فرض می‌کنیم $R=R_H$ نسبت هم ارزی در G تعریف شده به‌صورت: xRy اگر $x^{-۱}y \in H$ که در آن $x, y \in G$، را نمایش دهد. ردهٔ هم ارزی xH را که x بدان تعلق دارد، یك همدستهٔ چپ G به هنگ H می‌نامند. اگر مجموعهٔ خارج قسمت G/R متشکل از کلیهٔ همدسته‌های چپ n عضو داشته باشد، آنگاه n را اندیس H در G می‌خوانند و با $[G:H]$ نمایش می‌دهند.

قضیهٔ ۲. (لاگرانژ) فرض کنید H زیرگروهی از یك گروه متناهی G باشد. آنگاه مرتبهٔ G مساوی با حاصلضرب مرتبهٔ H و اندیس H در G است. به ویژه، مرتبهٔ H

مقسوم علیهی ازمرتبهٔ G است.

برهان. نخست توجه می‌کنیم که نگاشت $t: H \to xH$ با ضابطهٔ $t(h) = xh$ که در آن $h \in H$، نگاشتی یك به یك و به‌روست. بنابراین تعداد اعضای هر همدستهٔ چپ، مساوی با مرتبهٔ H است. ازآنجایی‌که هر دو همدستهٔ چپ متمایز از هم مجزا هستند و اندیس H در G مساوی با تعداد همدسته‌های چپ است، قضیه نتیجه می‌شود. □

عضوی چون a ازیك‌گروه G را از مرتبهٔ n می‌نامیم اگر زیرگروه پدیدآمده‌توسط a از مرتبهٔ n باشد.

نتیجه ۱. مرتبهٔ هرعضو G مقسوم علیهی از مرتبهٔ G است.

نتیجه ۲. هرگروه از مرتبهٔ عددی اول چون p، دوری است.

زیرا اگر a عضوی سوای همانی‌گروه باشد، مرتبه a عدد p را عاد می‌کند و درنتیجه مساوی با p است.

قضیهٔ ۳. احکام ذیل معادل‌اند:

(i) n مرتبهٔ a است،

(ii) n کوچکترین عدد صحیح مثبتی است‌که $a^n = e$،

(iii) $a^n = e$، واگر $a^m = e$ آنگاه $n|m$.

برهان. $(\text{i}) \Rightarrow (\text{ii})$. چون زیرگروه دوری پدید آمده توسط a متناهی است، نتیجه می‌گیریم‌که همهٔ اعضای $(a^i)_{i\in Z}$ متمایز نیستند. اگر $a^p = a^q$، و $p > q$، آنگاه $a^{p-q} = e$. دراین صورت عدد صحیح مثبتی مانند m وجود دارد که $a^m = e$. اگر m را کوچکترین عدد صحیح مثبتی بگیریم که $a^m = e$، ملاحظه می‌کنیم که اعضای $\{a^i | 0 \leqslant i < m\}$ متمایزند و این مجموعه زیرگروهی را تشکیل می‌دهدکه زیرگروه پدید آمده توسط a است. بنابراین، $m = n$.

$(\text{ii}) \Rightarrow (\text{iii})$ فرض‌کنیم $a^m = e$. دراین صورت داریم $m = qn + r$ که در آن $q, r \in Z$ و $0 \leqslant r < n$. ازاینجا $e = a^m = (a^q)^n a^r = a^r$. چون n کوچکترین عدد صحیح مثبتی است که $a^n = e$، نتیجه می‌شود که $r = 0$. بنابراین $X = qn$.

$(\text{iii}) \Rightarrow (\text{i})$ اعضای $(a^i)_{0 \leqslant i < n}$ همه متمایزند. زیرا اگر $a^p = a^q$ که در آن $0 \leqslant p < n$، $0 \leqslant q < n$ و $p > q$، آنگاه $a^{p-q} = e$. پس، بنا برفرض، n عدد $p-q$ را عادمی‌کند، و این غیر ممکن است زیرا $p-q$ از n کوچکتر است. آشکارا $\{a^i | 0 \leqslant i < n\}$ یك زیرگروه دوری پدید آمده توسط a است. □

بزرگترین مرتبهٔ اعضای یك‌گروه متناهی آبلی را توان گروه می‌نامند.

قضیهٔ ۴. اگر m توان یك گروه متناهی‌آبلی G باشد، آنگاه مرتبهٔ هرعضو G مقسوم‌علیهی از m است.

ابتدا لم زیررا ثابت می‌کنیم:

لم. فرض کنیم a و b اعضایی از یك گروه G باشند و $ab=ba$. اگر مرتبه‌های a و b به‌ترتیب m و n باشند و $(m,n)=1$، آنگاه ab ازمرتبهٔ mn است.
برهان. داریم $(ab)^{mn}=a^{mn}b^{mn}=e$. بنابراین، اگر d مرتبهٔ ab باشد، آنگاه $d|mn$. اینك، چون $(ab)^d=e$، داریم $a^d=b^{-d}$ و از آنجا $a^{nd}=e$. درنتیجه $m|nd$. چون $(m,n)=1$، نتیجه می‌شود که $m|d$. همین‌طور، $n|d$. چون $(m,n)=1$، $mn|d$. لذا ثابت می‌شود که ab ازمرتبهٔ mn است. □

برهان قضیه. فرض می‌کنیم a عضوی با بزرگترین مرتبه، یعنی با مرتبهٔ m، باشد و b عضو دلخواهی ازمرتبهٔ n باشد. همچنین فرض می‌کنیم، درصورت امکان، $n\nmid m$. در این صورت عدد اولی مانند p وجود دارد که اگر r (به‌ترتیب s) بزرگترین توان p باشد که n (به ترتیب m) را عاد کند، آنگاه داریم $r>s$. دراین صورت مرتبهٔ a^{p^s} مساوی m/p^s و مرتبهٔ b^{n/p^r} مساوی با p^r است. چون $(m/p^s, p^r)=1$، از لم فوق نتیجه می‌گیریم که مرتبهٔ عضو $a^{p^s}b^{n/p^r}$ مساوی با $(m/p^s)p^r$ است که، چون $r>s$، از m بزرگتر است. این مطلب تعریف a را نقض می‌کند وبنابراین قضیه برقرار است. □

تعریف. یك زیرگروه H ازگروهی مانند G در G نرمال نامیده می‌شود اگر به ازای هر $x\in G$، $xHx^{-1}=H$.

یك زیر گروه H از G نرمال‌است‌اگر وفقط اگر به‌ازای هر $x\in G$، $xHx^{-1}\subset H$.

به‌ازای هر زیرگروه H از G و هر $x\in G$، xHx^{-1} زیرگروهی از G است که مزدوج H نامیده می‌شود. از تعریف نرمال بودن زیرگروه نتیجه می‌شود که یك زیرگروه H نرمال است اگر وفقط اگر تمام مزدوجهای H بر H منطبق باشند.
فرض کنیم $f:G\to G'$ یك هومومورفیسم گروهی‌باشد. تصویرمعکوس یك زیرگروه نرمال از G' زیرگروهی نرمال از G است. به‌علاوه، اگر f به‌رو باشد، تصویر یك زیرگروه نرمال از G یك زیرگروه نرمال از G' است.
زیرگروههای G و $\{e\}$ در G نرمال هستند. هر زیرگروه از G غیر ازخود G را یك زیرگروه سره می‌نامند. اگر گروهی هیچ زیرگروه سرهٔ نرمال سوای $\{e\}$ نداشته باشد، یك گروه ساده نامیده می‌شود.

چند مثال: ۱. دریك گروه آبلی تمام زیرگروهها نرمال هستند.
۲. یك گروه آبلی $G(\neq\{e\})$ ساده است اگر وفقط اگر دوری و از مرتبهٔ اول باشد.
۳. هستهٔ هر هومومورفیسم گروهی $f:G\to G'$ یك زیرگروه نرمال G است.
۴. اگر H و K زیرگروههایی از G باشند و اگر $HK=KH$، آنگاه HK زیرگروهی از G است. اگر یکی از H یا K در G نرمال باشد، شرط $HK=KH$

برقرار است. درصورتی که هم H وهم K زیرگروههایی نرمال از G باشند، آنگاه HK نیز زیرگروهی نرمال از G است.

فرض کنیم G یک گروه و H زیرگروهی نرمال از G باشد. مجموعهٔ G/R متشکل از همدسته‌های چپ G به هنگ[1] H را درنظر می‌گیریم. در G/R با قرار دادن $xH \cdot yH = xyH$ ، که در آن $x, y \in G$ ، یک عمل تعریف می کنیم. ادعا می کنیم که این عمل خوشتعریف است. زیرا اگر $x' \in xH$ و $y' \in yH$ ، یعنی اگر $x' = xh_1$ ، $y' = yh_2$ و $h_1, h_2 \in H$ ، آنگاه $x'y' = xh_1yh_2 = xy(y^{-1}h_2y)h_2 \in xyH$ زیرا $y^{-1}h_1y \in H$. به‌سهولت دیده می‌شود که G/R ، تحت این عمل، یک گروه است؛ عضو همانی $H(=eH)$، و وارون xH عضو $x^{-1}H$ است. این گروه را گروه خارج قسمت G بر H می نامند و با G/H نمایش می‌دهند. نگاشت طبیعی $q: G \to G/H$ با ضابطهٔ $q(x) = xH$ آشکارا همومورفیسمی به‌رو و با هستهٔ H است.

مثال. گروه $Z/(m)$، از رده‌های مانده‌ای به‌هنگ m ، همان گروه خارج قسمت Z/mZ است.

فرض کنیم $f: G \to G'$ همومورفیسمی به‌رو و با هستهٔ H باشد. همومورفیسمی چون $\bar{f}: G/H \to G'$ را باضابطهٔ $\bar{f}(xH) = f(x)$، که در آن $x \in G$، تعریف می کنیم. روشن است که $\bar{f}$ خوشتعریف است و ایزومورفیسمی است از G/H به روی G' و داریم $\bar{f} \circ q = f$، که در آن $q: G \to G/H$ نگاشت طبیعی است. بنابراین، «در حد یک ایزومورفیسم»، هرتصویر همومورفیک یک گروه، یک گروه خارج قسمت است. این مطلب را معمولاً قضیهٔ بنیادی همومورفیسمها می نامند.

چند تذکر: ۱. فرض کنیم G یک گروه باشد و H و K زیرگروههایی نرمال از G باشند که $K \subset H$. همومورفیسم $\bar{f}: G/K \to G/H$ با ضابطهٔ $\bar{f}(xK) = xH$ که در آن $x \in G$ ، به‌رو است و هسته‌اش، به‌وضوح، H/K است. در نتیجه $(G/K)/(H/K) \approx G/H$. (اولین قضیهٔ ایزومورفیسم).

۲. فرض کنیم H و K زیرگروههایی ازگروهی چون G باشند وفرض کنیم K در G نرمال باشد. دراین صورت همومورفیسم $f: H \to HK/K$ با ضابطهٔ $f(h) = hK$ که در آن $h \in H$، دارای هستهٔ $H \cap K$ است و درنتیجه $H/H \cap K \approx HK/K$. (دومین قضیهٔ ایزومورفیسم.)

۳. فرض کنیم G یک گروه دوری پدید آمده توسط عضوی مانند a باشد. نگاشت $f: Z \to G$ با ضابطهٔ $f(n) = a^n$ که در آن $n \in Z$ ، همومورفیسمی به رو است. بنابراین $Z/\ker f \approx G$. چون به‌ازای یک $m \geqslant 0$ ، $\ker f = mZ$ ، نتیجه می گیریم که هرگروه دوری با Z/mZ ایزومورف است. اینک به‌سهولت می توانیم نشان دهیم که همه زیرگروهها وگروههای خارج قسمت یک گروه دوری خود دوری هستند.

۴. اگر G یک گروه با همانی e باشد، داریم $G/\{e\} \approx G$ و $G/G \approx \{e\}$.

فرض کنیم G یک گروه باشد و $a, b \in G$. گوییم a مزدوج b است اگر در G عضوی مانند x وجود داشته باشد که $a = xbx^{-1}$. به سادگی ثابت می‌شود که نسبت مزدوج بودن یک نسبت هم‌ارزی است. یک ردهٔ هم‌ارزی را یک ردهٔ مزدوجی یا یک ردهٔ اعضای مزدوج می‌نامند.

چند تذکر: ۱. زیرمجموعهٔ $\{e\}$ از G یک ردهٔ مزدوجی است.

۲. اگر a مزدوج b باشد، آنگاه a^m مزدوج b^m است؛ $m \in \mathbf{Z}$.

۳. یک زیرگروه H از G نرمال است اگر وفقط اگر مساوی با اجتماعی از رده‌های مزدوجی باشد.

فرض کنیم K زیرمجموعه‌ای از یک گروه G باشد. زیرمجموعهٔ N_K از G که نرمال‌ساز K در G نامیده می‌شود، به‌صورت زیر تعریف می‌شود: $N_K = \{x \in G | xK = Kx\}$.
اگر K متشکل از تنها یک عضو a باشد، نرمال‌ساز $\{a\}$ را با N_a نمایش می‌دهند و آن را نرمال‌ساز a می‌نامند. به سهولت ثابت می‌شود که نرمال‌ساز هر زیرمجموعهٔ K از G زیرگروهی از G است.

تذکر. یک زیرگروه H از G نرمال است اگر وفقط اگر $N_H = G$.

قضیهٔ ۵. فرض کنیم G یک گروه متناهی باشد و $a \in G$. دراین صورت تعداد اعضای مزدوج با a برابر است با اندیس نرمال‌ساز a در G.

برهان. فرض می‌کنیم ردهٔ مزدوجی شامل عضو a با C نمایش داده شود. نگاشت $\chi : G \to C$ با ضابطهٔ $\chi(x) = xax^{-1}$ را که درآن $x \in G$ درنظرمی گیریم. این نگاشت به رو است. اگر $n \in N_a$، آنگاه، به‌ازای هر $x \in G$،

$$\chi(xn) = (xn)a(xn)^{-1} = x(nan^{-1})x^{-1} = xax^{-1} = \chi(x).$$

این مطلب نشان می‌دهد که هردوعضو متعلق به یک همدستهٔ چپ G به‌هنگ N_a در C تصویر یکسان دارند. به‌عکس، اگر $x, y \in G$ و $\chi(x) = \chi(y)$، آنگاه $xax^{-1} = yay^{-1}$، که $(y^{-1}x)a(y^{-1}x)^{-1} = a$ ازآن نتیجه می‌شود. این بدان معنی است که $y^{-1}x \in N_a$ و درنتیجه x و y به یک همدستهٔ چپ G به‌هنگ N_a تعلق دارند. بنابراین، χ تناظری یک به‌یک بین مجموعهٔ همدسته‌های چپ G، به‌هنگ N_a، ومجموعهٔ مزدوجهای متمایز a القا می‌کند. □

نتیجه. تعداد اعضای مزدوج با a مقسوم‌علیهی ازمرتبهٔ گروه G است. به‌ویژه، اگر G ازمرتبهٔ p^n باشد که درآن p عددی اول است، آنگاه یک ردهٔ مزدوجی دارای p^i عضو است که درآن $0 \leqslant i \leqslant n$ وجود دارد.

عضو $a \in G$ را مرکزی می‌نامیم اگر، به‌ازای هر $x \in G$، $xa = ax$. مجموعهٔ تمام

اعضای مرکزی گروه G مرکز G نامیده می‌شود.

چند تذکر: ۱. عضوی چون a ازیك گروه G مرکزی است اگر و فقط اگر زیرمجموعه $\{a\}$ یك ردهٔ مزدوجی باشد.
۲. مرکز یك گروه، زیرگروهی نرمال است.

قضیهٔ ۶. اگر G گروهی از مرتبهٔ p^n باشد که درآن p عددی اول است و $n \geqslant ۱$، آنگاه مرکز G بیش ازیك عضو دارد.
برهان. فرض کنیم C_i $(۱ \leqslant i \leqslant m)$ رده‌های مزدوجی متمایز G باشند و k_i تعداد اعضای C_i باشد. داریم $k_i | p^n$ (قضیهٔ ۲ وقضیهٔ ۵)، ولذا اگر $k_i \neq ۱$، آنگاه $p | k_i$. فرض کنیم $C_۱$ ردهٔ مزدوجی شامل همانی باشد. اگر مرکز G مساوی با $\{e\}$ باشد، داریم $C_۱ = \{e\}$ و به‌ازای هر $i \neq ۱$، $k_i > ۱$. به‌علاوه

$$p^n = ۱ + \sum_{i \geqslant ۲} k_i$$

چون به‌ازای $i \geqslant ۲$، $p | k_i$، این رابطه ممتنع است. □

۳. گروه حلپذیر

تعریف. یك گروه G را حلپذیر گویند درصورتی که دنباله‌ای از زیرگروههای

$$G = G_۰ \supset G_۱ \supset \dots \supset G_n = \{e\}$$

وجود داشته باشد که $G_{i+۱}$ زیرگروهی نرمال از G_i باشد و $G_i / G_{i+۱}$ آبلی باشد $(۰ \leqslant i \leqslant n)$. چنین دنباله‌ای یك سری حلپذیر G نامیده می‌شود.

تذکر. هر گروه آبلی حلپذیر است.

قضیهٔ ۷. هر زیرگروه و هرگروه خارج قسمت گروهی حلپذیر، گروهی حلپذیر است. به‌عکس، اگر زیرگروهی نرمال چون H ازیك گروه G وجود داشته باشد که H و G/H حلپذیر باشند، آنگاه G حلپذیر است.
برهان. فرض کنیم G یك گروه حلپذیر با سری حلپذیری چون

$$G = G_۰ \supset G_۱ \supset \dots \supset G_n = \{e\}$$

باشد. اگر H زیرگروهی از G باشد، آنگاه

$$H=H\bigcap G_{0}\supset H\bigcap G_{1}\supset\cdots\supset H\bigcap G_{n}=\{e\}$$

یك سری حلپذیر H است، زیرا $H\bigcap G_{i+1}$ یك زیرگروه نرمال $H\bigcap G_i$ است و $(H\bigcap G_i)/(H\bigcap G_{i+1})$ ایزومورف و لذا آبلی است ($0\leqslant i<n$). (نگاشت شمول $H\bigcap G_i\to G_i$ را با نگاشت طبیعی $G_i\to G_i/G_{i+1}$ ترکیب کنید وقضیهٔ بنیادی هومورفیسم را کار بندید). مجدداً، اگر H یك زیرگروه نرمال G و $q:G\to G/H$ هومورفیسم طبیعی باشد، آنگاه

$$G/H=q(G_{0})\supset q(G_{1})\supset\cdots\supset q(G_{n})=\{e\}$$

یك سری حلپذیر G/H است، زیرا $q(G_{i+1})$ یك زیرگروه نرمال $q(G_i)$ است و $q(G_i)/q(G_{i+1})$ که با یك زیرگروه ازخارج قسمت G_i/G_{i+1} ایزومورف است آبلی است ($0\leqslant i<n$).

به‌عکس، فرض کنیم H یك زیرگروه نرمال G باشد و H و G/H حلپذیر باشند. فرض کنیم $q:G\to G/H$ هومورفیسم طبیعی باشد. فرض کنیم

$$H=H_{0}\supset H_{1}\supset\cdots\supset H_{n}=\{e\}$$

و

$$G/H=G'_{0}\supset G'_{1}\supset\cdots\supset G'_{m}=\{e\}$$

به‌ترتیب، سریهای حلپذیر H و G/H باشند. دراین صورت به‌آسانی دیده می‌شودکه

$$G=q^{-1}(G'_{0})\supset q^{-1}(G'_{1})\supset\cdots\supset q^{-1}(G'_{m})(=H=H_{0})\supset H_{1}\supset\cdots\supset H_{n}=\{e\}$$

یك سری حلپذیر G است. □

قضیهٔ ۸. هرگروه ازمرتبهٔ p^n که درآن p عددی اول باشد، حلپذیر است.

برهان. قضیه را به استقرا بر n ثابت می‌کنیم. به‌ازای $n=0$، قضیه بدیهی است. فرض کنید $n\geqslant 1$ وقضیه به‌ازای هر $r<n$ برقرار باشد. فرض‌کنید G گروهی از مرتبهٔ p^n باشد. دراین صورت، بنا برقضیهٔ ۶، مرکز C از G ازمرتبهٔ p^s، $s\geqslant 1$، است. دراین صورت مرتبهٔ G/C، p^{n-s} است و $n-s<n$. بنا بر فرض استقرا، G/C حلپذیر است. حال این قضیه ازقضیهٔ ۷ نتیجه می‌شود. □

قضیهٔ ۹. یك گروه متناهی G حلپذیر است اگر وفقط اگر دنباله‌ای از زیرگروههای

$$G=G_{0}\supset G_{1}\supset\cdots\supset G_{n}=\{e\}$$

وجود داشته باشد که G_{i+1} یك زیرگروه نرمال G_i باشد و G_i/G_{i+1} دوری و از مرتبهٔ اول باشد ($0\leqslant i<n$).

برهان. فرض کنیم G حلپذیر باشد وفرض کنیم

$$G=G_{\circ}\supset G_{\text{۱}}\supset\cdots\supset G_{n}=\{e\}$$

یك سری حلپذیر G باشد. بین G_i و $G_{i+\text{۱}}$ دنباله‌ای از زیرگروههای

$$G_i=H_{i,\circ}\supset H_{i,\text{۱}}\supset\cdots\supset H_{i,m}=G_{i+\text{۱}}$$

راکه $H_{i,j+\text{۱}}$ یك زیرگروه نرمال $H_{i,j}$ است، و مرتبهٔ $H_{i,j}/H_{i,j+\text{۱}}$ عددی است اول، ($\circ\leqslant j<m$)، درج می‌کنیم. برای این‌کار، کافی است نشان دهیم به‌ازای یك گروه متناهی مفروض A ویك زیرگروه نرمال B از A که A/B آبلی باشد، زیرگروه نرمالی چون N از A وشامل B وجود داردکه مرتبهٔ A/N عددی اول است. در واقع N را یك زیرگروه نرمال سرهٔ ماکسیمال A که شامل B باشد می‌گیریم. آشکارا A/N ساده است. اما، A/N که‌تصویر همومورف A/B است آبلی‌است ولذا مرتبه‌اش عددی‌اول‌است. □

۴. گروههای متقارن وحلپذیری

تعریف. فرض کنیم S_n گروه متقارن از درجهٔ n باشد. یك r-دور جایگشتی مانند σ است که r عدد صحیح متمایز $x_{\text{۱}}$، ...، x_r ($\text{۱}\leqslant x_i\leqslant n$) وجود داشته باشدکه $\sigma(x_{\text{۱}})=x_{\text{۲}}$، ...، $\sigma(x_{r-\text{۱}})=x_r$، $\sigma(x_r)=x_{\text{۱}}$ و به‌ازای هر $x\neq x_i$، $\text{۱}\leqslant i\leqslant r$، $\sigma(x)=x$. دراین صورت می‌نویسیم $\sigma=(x_{\text{۱}},x_{\text{۲}},\ldots,x_r)$. یك ۲-دور را یك ترانهش می‌نامند.

چند تذکر: ۱. یك r-دور یك عضو ازمرتبهٔ r است.

۲. اگر $\sigma=(x_{\text{۱}},x_{\text{۲}},\ldots,x_r)$ یك r-دور و τ جایگشتی دلخواه باشد، آنگاه داریم $\tau\sigma\tau^{-\text{۱}}=(y_{\text{۱}},y_{\text{۲}},\ldots,y_r)$ که در آن به‌ازای $\text{۱}\leqslant i\leqslant r$، $\tau(x_i)=y_i$.

قضیهٔ ۱۰. S_n با ترانهشها پدید می‌آید.

برهان. قضیه را به‌استقرا بر n ثابت می‌کنیم. به‌ازای $n=\text{۱},\text{۲}$ حکم بدیهی‌است. فرض‌کنیم قضیه به‌ازای $n-\text{۱}$ برقرار باشد و $\sigma\in S_n$. اگر $\sigma(n)=n$، آنگاه، بنابر فرض استقرا، σ مساوی با حاصلضربی از ترانهشها است. اگر $\sigma(n)=k$ و $k\neq n$، جایگشت $\tau=(k,n)\sigma$ به‌گونه‌ای است که $\tau(n)=n$ و درنتیجه مساوی با حاصلضربی از ترانهشها است. بنابراین $\sigma=(k,n)\tau$ نیز مساوی با حاصلضربی از ترانهشها است. □

نتیجه. S_n با ترانهشهای $(\text{۱},n)$، $(\text{۲},n)$، ...، $(n-\text{۱},n)$ پدید می‌آید.

زیرا $(i,j)=(i,n)(j,n)(i,n)$.

لم. اگر جایگشتی را بتوان به‌صورت حاصلضربی از m ترانهش وهمچنین به‌صورت

حاصلضربی از n ترانهش نوشت، آنگاه $m-n$ زوج است.

برهان. به‌سادگی دیده می‌شود که نگاشت $\{-۱, ۱\} \to f : S_n$ باضابطهٔ

$$f(\sigma)=\prod_{۱\leqslant i<j\leqslant n}\frac{\sigma(i)-\sigma(j)}{i-j}$$

که در آن $\sigma\in S_n$ یك هومومورفیسم گروهی است. اگر σ یك ترانهش باشد، آنگاه $-۱=f(\sigma)$. اگر σ را به صورت حاصلضربی از m (به‌ترتیب n) ترانهش تلقی‌کنیم، داریم $(-۱)^m=f(\sigma)$ (به‌ترتیب $(-۱)^n=f(\sigma)$). بنابراین $m-n$ زوج است. □

تعریف. یك جایگشت را فرد (به‌ترتیب، زوج) می‌نامند اگر بتوان آن را به صورت حاصلضربی از یك تعداد فرد (به‌ترتیب، زوج) ترانهش نوشت.

باید توجه داشت که بنا به‌لم قبل، مفهوم جایگشتهای فرد و زوج خوشتعریف است.

مجموعهٔ جایگشتهای زوج یك زیرگروه نرمال S_n است که با A_n نمایش داده می‌شود و گروه متناوب از درجهٔ n نام دارد. متذکر می‌شویم که اگر $n>۱$، گروه خارج قسمت S_n/A_n ازمرتبهٔ ۲ است.

تذکر. به ازای $n\leqslant ۴$، S_n حلپذیر است. زیرا به‌ازای $n=۱, ۲$ چیزی برای اثبات نیست. به‌ازای $n=۳$،

$$S_۳\supset A_۳\supset\{e\}$$

یك سری حلپذیر $S_۳$ است. به‌ازای $n=۴$،

$$S_۴\supset A_۴\supset V_۴\supset\{e\}$$

یك سری حلپذیر برای $S_۴$ است. در اینجا

$$V_۴=\{e, (۱, ۲)(۳, ۴), (۱, ۳)(۲, ۴), (۱, ۴)(۲, ۳)\}.$$

می‌توان ثابت‌کردکه $V_۴$ یك زیرگروه نرمال $A_۴$ است و $A_۴/V_۴$ گروهی از مرتبهٔ ۳ و لذا دوری است. همچنین، $V_۴$ آبلی است.

قضیهٔ اصلی. به ازای $n>۴$، S_n حلپذیر نیست.

برای اثبات به‌لم زیر نیاز داریم.

لم. اگر زیرگروهی مانند G از S_n $(n>۴)$ شامل تمام ۳-دورها باشد و اگر H زیرگروهی نرمال از G باشد که G/H آبلی باشد، آنگاه H شامل کلیهٔ ۳-دورهاست.

برهان. فرض‌کنیم $q: G\to G/H$ هومومورفیسم طبیعی باشد. اگر $\sigma, \tau\in G$، آنگاه $q(\sigma^{-۱}\tau^{-۱}\sigma\tau)=q(\sigma)^{-۱}q(\tau)^{-۱}q(\sigma)q(\tau)=e$، زیرا G/H آبلی است. بنابراین بـه‌ازای هر $\sigma, \tau\in G$، $\sigma^{-۱}\tau^{-۱}\sigma\tau\in H$. فرض کنیم (i, j, k) یك ۳-دور

دلخواه باشد. چون $n > 4$، می‌توان $\sigma = (i, k, l)$ و $\tau = (j, k, m)$ را چنان اختیار کرد که i، j، k، l و m همه متمایز باشند. دراین صورت

$$\sigma^{-1}\tau^{-1}\sigma\tau = (l, k, i)(m, k, j)(i, k, l)(j, k, m) = (i, j, k) \in H . \quad \square$$

برهان قضیهٔ اصلی. فرض کنیم، درصورت امکان،

$$S_n = G_0 \supset G_1 \supset \cdots \supset G_m = \{e\}$$

یك سری حلپذیر باشد. چون S_n شامل تمام ۳-دورهاست، از لم فوق نتیجه می‌شود که به‌ازای هر i که $1 \leqslant i \leqslant m$، G_i کلیهٔ ۳-دورها را دربردارد. اما به ازای $i = m$، این مطلب به‌روشنی ممتنع است. $\square$

فصل ۲

حلقه و فضای برداری

۱. حلقه و همومورفیسم

تعریف. یک حلقه یک سه تایی مانند (A, ϕ, ψ) است که در آن A یک مجموعه است و ϕ, ψ نگاشتهایی از $A \times A$ به‌توی A هستند (به‌ازای هر $x, y \in A$، می‌نویسیم $\phi(x, y) = x+y$ و $\psi(x, y) = xy$) که

(i) (A, ϕ) یک گروه آبلی است،

(ii) به‌ازای هر $x, y, z \in A$، $x(yz) = (xy)z$ (شرکتپذیری)،

(iii) به‌ازای هر $x, y, z \in A$، $x(y+z) = xy+xz$ و $(y+z)x = yx+zx$ (توزیعپذیری)،

(iv) عضوی مانند $1 \in A$، به نام واحد، وجود دارد که به ازای هر $x \in A$، $1x = x1 = x$.

چند تذکر: ۱. به ϕ و ψ اعمال حلقه گفته می‌شود. ϕ را جمع، و ψ را ضرب حلقه می‌نامند؛ غالباً نماد $(A, +)$ را برای گروه آبلی (A, ϕ) بکار می‌برند.

۲. عضو همانی (A, ϕ) را عضو صفر A می‌نامند و با 0 نشان می‌دهند.

۳. عضو واحد منحصر به‌فرد است.

۴. قانون شرکتپذیری ضرب درمورد هر تعداد عضو معتبر است.

۵. به‌ازای $a, b \in A$ که $ab = ba$ و به‌ازای هرعدد صحیح $n \geqslant 0$، داریم

$(a+b)^n=\sum_{i=0}^{n}\binom{n}{i}a^ib^{n-i}$؛ دراینجا به‌ازای هر $x\in A$ وهرعدد صحیح مثبت m، $x^m=x\ldots x$ (m بار)؛ قرارداد می‌کنیم که $x^0=1$.

۶. به ازای هر $a\in A$، بنابر (iii)، نگاشت $x\to ax$ (به ترتیب $x\to xa$) همومورفیسمی از گروه $(A,+)$ به‌توی خودش است ولذا $a0=0$ (به‌ترتیب، $0a=0$).

تعریف. حلقهٔ A را تعویضپذیر نامند اگر به‌ازای هر $x,y\in A$، $xy=yx$.

چند مثال: ۱. مجموعهٔ $\mathbf{Z}$ (به‌ترتیب $\mathbf{Q}$، $\mathbf{R}$، $\mathbf{C}$) متشکل از اعداد صحیح (به ترتیب اعداد گویا، اعداد حقیقی، اعداد مختلط) با جمع وضرب «معمولی» حلقه‌ای تعویضپذیر است.

۲. گروه جمعی رده‌های مانده‌ای به‌هنگ یك عدد صحیح m یك حلقه است؛ ضرب دراین حلقه بدین صورت تعریف می‌شود: $\bar{r}\bar{s}=\overline{rs}$، که در آن $\bar{r},\bar{s}\in\mathbf{Z}/(m)$.

۳. فرض‌کنیم G گروهی آبلی باشد. مجموعهٔ $\mathrm{Hom}(G,G)$، متشکل از کلیهٔ همومورفیسمهای از G به‌توی G یك حلقه‌است؛ اعمال حلقه به‌صورت زیر تعریف می‌شوند: $(f+g)(x)=f(x)+g(x)$، $(fg)(x)=f(g(x))$، که‌در آن $f,g\in\mathrm{Hom}(G,G)$ و $x\in G$.

توجه‌کنید که درحالت کلی $\mathrm{Hom}(G,G)$ تعویضپذیر نیست.

فرض‌کنیم A یك حلقه باشد. یك زیرحلقهٔ B از A زیرگروهی از $(A,+)$ است که $1\in B$ وبه‌ازای هر $x,y\in B$، $xy\in B$. مشاهده می‌کنیم که B تحت اعمال القایی یك حلقه است. اشتراك هرخانواده‌ای از زیرحلقه‌های A خود یك زیرحلقه است. فرض‌کنیم S زیرمجموعه‌ای از A باشد. اشتراك تمام زیرحلقه‌هایی از A که شامل S هستند زیرحلقهٔ پدید آمده توسط S نامیده می‌شود.

حلقه‌هایی را که از این پس مورد مطالعه قرار می‌دهیم، فرض می‌کنیم تعویضپذیر باشند، مگر اینکه خلافش ذکر شده باشد.

فرض‌کنیم $a,b\in A$. گوییم a، b را عاد می‌کند (یا a مقسوم علیهی از b است و می‌نویسیم $a|b$) اگرعضوی چون $c\in A$ وجود داشته باشد به‌قسمی که $b=ac$. اگر a، b را عاد نکند، می‌نویسیم $a\nmid b$. یك عضو $a\in A$ یك مقسوم علیه صفر نامیده می‌شود اگر $x\in A$ی وجود داشته باشد که $x\neq 0$ و $ax=0$. A یك حوزهٔ صحیح نامیده می‌شود اگر $A\neq\{0\}$، وهیچ مقسوم علیه صفری غیراز 0 نداشته باشد. عضوی مانند $a\in A$ را یك یکال نامند اگر عضوی مانند $a^{-1}\in A$ وجود داشته باشد که $aa^{-1}=a^{-1}a=1$. فرض کنیم A یك حوزهٔ صحیح باشد. عضو ناصفر $a\in A$ را تجزیه‌ناپذیر نامند اگر یکال نباشد واز $a=bc$، $b,c\in A$، نتیجه شود که b یا c یك یکال است.

یك حلقهٔ تعویضپذیر A یك میدان نامیده می‌شود اگر $A^*=A-\{0\}$ تحت عمل ضرب یك گروه باشد، ولذا هرعضو ناصفر یك میدان یك یکال است. روشن است که یك

میدان حداقل دو عضو دارد. یك زیرحلقهٔ R از یك میدان K یك زیرمیدان K نامیده می‌شود اگرحلقهٔ R یك میدان باشد. هر اشتراکی از زیرمیدانهای K خود یك زیرمیدان است. اگر S زیرمجموعه‌ای از K باشد، آنگاه اشتراك کلیهٔ زیرمیدانهایی از K که شامل S باشند زیرمیدان پدید آمده توسط S نامیده می‌شود.

چند مثال: ۱. $\mathbf{Z}$ یك حوزهٔ صحیح است.

۲. $\mathbf{Z}/(m)$ یك میدان است اگر وفقط اگر m اول باشد. زیرا، اگر $m=rs$، که در آن $|r|, |s| \neq ۱$، آنگاه $\bar{r}\bar{s}=\overline{rs}=۰$، درحالی که $\bar{r}, \bar{s} \neq ۰$. بنابراین $\mathbf{Z}/(m)$ حوزهٔ صحیح نیست و به‌طریق اولی‌میدان هم نیست. فرض کنیم m اول باشد، $\bar{r} \in \mathbf{Z}/(m)$ و $\bar{r} \neq ۰$، دراین صورت $(r, m)=۱$، یعنی $s, t \in \mathbf{Z}$ ی وجود دارند که $sr+tm=۱$. آشکارا $\bar{s}\bar{r}=۱$. بنابراین $\mathbf{Z}/(m)$ میدان است.

۳. $\mathbf{Q}$، $\mathbf{R}$، $\mathbf{C}$ میدان هستند.

فرض کنیم A و A' حلقه باشند. نگاشتی چون $f:A \to A'$ را یك هومورفیسم نامند اگر، به‌ازای هر $x, y \in A$،

$$\text{(i)} \quad f(x+y)=f(x)+f(y),$$
$$\text{(ii)} \quad f(xy)=f(x)f(y),$$
$$\text{(iii)} \quad f(۱)=۱.$$

به‌ازای هرحلقه‌ای، نگاشت همانی یك هومورفیسم است. فرض کنیم A، B و C حلقه باشند و فرض کنیم $f:A \to B$ و $g:B \to C$ هومورفیسم باشند. در این صورت $g \circ f:A \to C$ یك هومورفیسم است.

یك هومورفیسم $f:A \to A'$ یك ایزومورفیسم نامیده می‌شود اگر هومورفیسمی مانند $g:A' \to A$ وجود داشته باشد که $g \circ f=I_A$ و $f \circ g=I_{A'}$؛ در این صورت حلقه‌های A و A' را ایزومورف می‌نامیم ومی‌نویسیم $A \approx A'$. یك ایزومورفیسم $f:A \to A$ یك اتومورفیسم نامیده می‌شود.

چند تذکر: ۱. یك هومورفیسم، ایزومورفیسم است اگروفقط اگریك به‌یك وبه‌رو باشد.

۲. فرض کنیم $f:A \to A'$ یك هومورفیسم حلقوی باشد. اگر B زیرحلقه‌ای از A باشد، آنگاه $f(B)$ زیرحلقه‌ای از A' است.

چند مثال: ۱. فرض کنیم A یك حلقه و B زیرحلقه‌ای از A باشد. در این‌صورت نگاشت شمول $i:B \to A$ هومورفیسمی یك به‌یك است.

۲. نگاشت طبیعی $q:\mathbf{Z} \to \mathbf{Z}/(m)$ یك هومورفیسم است.

۳. نگاشت $f:\mathbf{C} \to \mathbf{C}$ با ضابطهٔ $f(z)=\bar{z}$ اتومورفیسمی از $\mathbf{C}$ است.

فرض کنیم A حوزهٔ صحیحی باشد. فرض کنیم A^* مجموعهٔ اعضای ناصفر A را نمایش دهد. برمجموعهٔ $A\times A^*$ نسبت $(a, b)\sim(c, d)$ را با شرط $ad=bc$ تعریف می‌کنیم. چون A یك حوزهٔ صحیح‌است، می‌توان ثابت کرد که‌این‌نسبت یك نسبت هم‌ارزی است. اکنون با تعریف اعمال ذیل، از مجموعهٔ خارج قسمت $K=(A\times A^*)/\sim$ یك حلقه مـی‌سازیم: $a/b+c/d=(ad+bc)/bd$ ، $(a/b)(c/d)=ac/bd$؛ در اینجا a/b ردهٔ هم‌ارزی شامل (a, b) را نمایش می‌دهد. به‌سهولت می‌توان ثابت کرد کـه این اعمال خوشتعریف هستند و K یك حلقه است. در واقع، K یك میدان است؛ وارون a/b، $a\neq 0$، عبارت است از b/a. K را میدان خارج‌قسمت A می‌نامند. نگاشت $i:A\to K$ با ضابطهٔ $i(a)=a/1$ همومورفیسمی یك بـه‌یك است. ما A را با زیرحلقهٔ $i(A)$ از K منطبق خواهیم گرفت. اگر $f:A\to L$ همومورفیسمی یك به‌یك از A به‌توی میدانی مانند L باشد، آنگاه f را می‌توان به‌روشی منحصر به‌فرد به‌همومورفیسمی مانند $\bar{f}$ از K به‌توی L به‌صورت $\bar{f}(a/b)=f(a)f(b)^{-1}$، با شرط $b\neq 0$، توسعه داد. اگر A زیرحلقه‌ای از L باشد، زیر میدان پدید آمده توسط A مساوی با میدان خارج قسمت A است.

مثال. $\mathbf{Q}$ میدان خارج قسمت $\mathbf{Z}$ است.

۲. ایده‌آل وحلقهٔ خارج قسمت

تعریف. فرض‌کنیم A حلقه‌ای تعویضپذیر بـاشد. یك ایده‌آل I از A زیرگروهـی از $(A, +)$ است‌که به‌ازای هر $x\in I$ و هر $a\in A$، داشته باشیم $ax\in I$.

در مورد هرحلقهٔ A، اشتراك هرخانواده ازایده‌آلهای A خود یك ایده‌آل A است. فرض کنیم S زیرمجموعه‌ای از A باشد. اشتراك تمام ایده‌آلهای شامل S را ایده‌آل پدید آمده توسط S می‌نامند. به‌سهولت مشاهده می‌شود که اگر S تهی نباشد، آنگاه این‌ایده‌آل دقیقاً ازتمام حاصل‌جمعهای متناهی به‌شکل $\sum\lambda_i x_i$، $\lambda_i\in A$، $x_i\in S$، تشکیل می‌شود. به‌ازای $a\in A$، ایده‌آل پدیدآمده توسط $\{a\}$، یعنی $\{xa|x\in A\}$، راایده‌آل اصلی پدیدآمده توسط a می‌نامند وبا (a) نمایش می‌دهند. حـوزهٔ صحیحی راکـه هرایده‌آلش اصلی باشد یك حوزهٔ ایده‌آل اصلی می‌نامند.

چند مثال: ۱. $\{0\}$ و A ایده‌آلهایی از A هستند.

۲. $\mathbf{Z}$ یك حوزهٔ ایده‌آل اصلی است، زیرا ایده‌آلهـای $\mathbf{Z}$ دقیقاً زیر گروههای $\mathbf{Z}$ هستند.

۳. فـرض‌کنیـم $f:A\to A'$ یـك همومـورفیسم بـاشد، در ایـن صـورت $\ker f=\{x\in A|f(x)=0\}$ ایده‌آلی از A است.

قضیهٔ ۱. یك حلقهٔ تعویضپذیر A میدان است اگر و فقط اگر $1\neq 0$ و سوای A و $\{0\}$ هیچ ایده‌آلی نداشته باشد.

برهان. فرض کنیم A میدان باشد. روشن است که $0 \neq 1$. فرض کنیم I ایده‌آل ناصفری از A باشد. در این صورت عضوی چون $a \in I$ وجود دارد که $a \neq 0$. چون $a^{-1}a \in I = 1$، پس $A = I$. به عکس، فرض کنیم $0 \neq 1$ و $\{0\}$ و A تنها ایده‌آلهای A باشند. دراین‌صورت به‌ازای هر $a \in A$، $a \neq 0$، $(a) = A$. بنابراین عضوی مانند $b \in A$ وجود دارد که $ba = 1$، پس A میدان است. $\square$

فرض کنیم I یك ایده‌آل A باشد. گروه جمعی A/I با عمل ضرب $(x+I)(y+I) = xy+I$، $x, y \in A$، حلقه‌ای است موسوم به‌حلقهٔ خارج قسمت. با توجه به‌اینکه I یك ایده‌آل است، این عمل ضرب خوشتعریف است. نگاشت طبیعی $q: A \to A/I$ هومومورفیسمی به‌رو با هستهٔ I است.

مثال. حلقهٔ $\mathbf{Z}/(m)$ ازرده‌های مانده‌ای به‌هنگ m همان حلقهٔ خارج قسمت $\mathbf{Z}$ بر ایده‌آل اصلی (m) است.

فرض کنیم $f: A \to A'$ هومومورفیسمی به‌رو و I هستهٔ f باشد. هومومورفیسم f با قراردادن $\bar{f}(x+I) = f(x)$، به‌ازای $x \in A$، هومومورفیسمی چون $\bar{f}: A/I \to A'$ القا می‌کند؛ به‌سهولت ثابت می‌شود که $\bar{f}$ ایزومورفیسمی حلقوی است و $\bar{f} \circ q = f$ که در آن q نگاشت طبیعی $A \to A/I$ است. این‌مطلب به‌قضیهٔ بنیادی هومومورفیسمهای حلقوی موسوم است.

تذکر. فرض کنیم K یك میدان باشد. هومومورفیسم $f: \mathbf{Z} \to K$ با ضابطهٔ $f(n) = n1 (= 1 + \dots + 1$ و n بار) را در نظر می‌گیریم. بنابرقضیهٔ بنیادی هومومورفیسمها، داریم $\mathbf{Z}/\ker f \approx f(\mathbf{Z})$. می‌دانیم‌عضوی چون $p \geqslant 0$ وجود دارد که $\ker f = (p)$. p را مشخصهٔ میدان K می‌نامیم. روشن است که به‌ازای هر $a \in K$، $pa = 0$. اگر $p \neq 0$، آنگاه p عددی اول است. آشکارا $p \neq 1$ واگر $p = rs$، $r > 0$ و $s > 0$، آنگاه $f(p) = f(r)f(s) = 0$. از آنجایی که K یك میدان است $f(r) = 0$ یا $f(s) = 0$؛ به‌عبارت دیگر $p|r$ یا $p|s$. چون $r \geqslant 1$ و $s \geqslant 1$، نتیجه می‌شود که $r = 1$ یا $s = 1$. بنابراین $\mathbf{Z}/(p)$ یك میدان است و K دارای زیرمیدانی ایزومورف با $\mathbf{Z}/(p)$ است. اگر $p = 0$، آنگاه هومومورفیسم یك به‌یك $f: \mathbf{Z} \to K$ را می‌توان به‌ایزومورفیسمی از $\mathbf{Q}$ به‌روی زیرمیدانی از K توسعه داد. بدین‌ترتیب، K دارای زیرمیدانی ایزومورف با $\mathbf{Q}$ است و قضیهٔ ذیل را داریم.

قضیهٔ ۲. هرمیدان شامل زیرمیدانی است‌که یا با میدان اعدادگویا ایزومورف است یا با میدان رده‌های مانده‌ای اعداد صحیح به‌هنگ یك عدد اول مانند p.

هریك از میدانهای $\mathbf{Q}$ و $\mathbf{Z}(p)$ راکه در آن p عددی اول است، یك میدان اول می‌نامند.

اگر K میدانی با مشخصهٔ $p > 0$ باشد، آنگاه، به‌ازای هر $a, b \in K$ داریم

$$(a+b)^p=\sum_{i=0}^{p}\binom{p}{i}a^ib^{p-i}=a^p+b^p$$

نگاشت $x \rightarrow x^p$ همومورفیسمی یك به‌یك از K به‌توی K است.

فرض کنیم K میدانی متناهی باشد (یعنی K دارای تعداد متناهی عضو باشد)؛ در این‌صورت مشخصهٔ K یعنی p مثبت است. دراین‌صورت نگاشت $x \rightarrow x^p$ یك اتومورفیسم K است.

۳. حلقهٔ چندجمله‌ایها

فرض کنیم A یك حلقه باشد. مجموعهٔ R متشکل از دنباله‌های $f=(a_0, a_1, \dots, a_n, \dots)$ را که درآن $a_n \in A$ و به‌استثنای تعدادی متناهی از nها، $a_n=0$، درنظر می‌گیریم. فرض کنیم $f, g \in R$، $f=(a_0, \dots, a_n, \dots)$ و $g=(b_0, \dots, b_n, \dots)$. ذیلاً با تعریف دوعمل جمع وضرب، از R یك حلقه می‌سازیم:

$$f+g=(a_0+b_0, \dots, a_n+b_n, \dots);\ fg=(c_0, \dots, c_n, \dots),\ c_n=\sum_{i+j=n}a_ib_j$$

عضو همانی R عبارت است از $(1, 0, 0, \dots)$. نگاشت $f: A \rightarrow R$ که با ضابطهٔ $f(a)=(a, 0, 0, \dots)$ تعریف می‌شود مسلماً یك همومورفیسم یك به یك است و ما A را با زیرحلقهٔ $f(A)$ از R یکی می‌گیریم. اگربنویسیم $X=(0, 1, 0, \dots)$، آنگاه، به‌ازای $i>0$، $X^i=(d_0, d_1, \dots)$ که درآن $d_i=1$ و به‌ازای $j \neq i$، $d_j=0$. به‌سهولت می‌توان دیدکه هر $f \in R$ را می‌توان به‌طور منحصربه‌فرد به‌شکل یك مجموع متناهی نظیر $\sum a_iX^i$، $a_i \in A$، نوشت. حلقهٔ R را با $A[X]$ نمایش می‌دهند، وآن را حلقهٔ چندجمله‌ایهای با یك متغیرروی A می‌نامند. به‌هریك ازاعضای $A[X]$ یك چندجمله‌ای اطلاق می‌شود.

فرض کنیم A و B حلقه باشند و $\phi: A \rightarrow B$ یك همومورفیسم حلقوی باشد. در این صورت ϕ یك توسیع منحصربه‌فرد به‌یك همومورفیسم حلقوی $\phi: A[X] \rightarrow B[X]$ دارد که $\phi(X)=X$. برای این‌کار تنها باید بنویسیم $\phi(\sum a_iX^i)=\sum\phi(a_i)X^i$.

فرض کنیم B یك حلقه و A یك زیرحلقهٔ آن باشد. به‌ازای هر $\alpha \in B$، با قراردادن $\psi(\sum a_iX^i)=\sum a_i\alpha^i$ نگاشت $\psi: A[X] \rightarrow B$ راتعریف می‌کنیم. به‌سهولت ثابت می‌شود که ψ یك همومورفیسم حلقوی است. می‌نویسیم $\psi(A[X])=A[\alpha]$ و به‌ازای $f(X)=\sum a_iX^i \in A[X]$، می‌نویسیم $\psi(f)=f(\alpha)(=\sum a_i\alpha^i)$. اگر $f(\alpha)=0$، α را یك ریشهٔ f می‌نامیم.

فرض کنیم $f=\sum a_iX^i \in A[X]$ و $f \neq 0$. در این‌صورت بنا برتعریف، درجهٔ f (نماد: $\deg f$) بزرگترین عدد صحیحی چون n است که به‌ازای آن $a_n \neq 0$. به a_n ضریب پیشرو f اطلاق می‌شود. اگر $a_n=1$، f را یك چندجمله‌ای تکین می‌نامند. اگر

$f\neq \circ$، $g\neq\circ$ و $f+g\neq\circ$، آنگاه‌داریم $\deg(f+g)\leqslant \max(\deg f,\deg g)$.
یك چند جمله‌ای از درجهٔ ۱ یك چند جمله‌ای خطی نام دارد.

چند تذکر: ۱. اگر A یك حوزهٔ صحیح باشد، $f, g\in A[X]$، $f\neq\circ$ و $g\neq\circ$، آنگاه $fg\neq\circ$؛ یعنی $A[X]$ یك حوزهٔ صحیح است و داریم $\deg(fg)=\deg f+\deg g$.
۲. اگر A یك حوزهٔ صحیح باشد، آنگاه یکالهای $A[X]$ دقیقاً همان یکالهای A هستند.

قضیهٔ ۳ (الگوریتم اقلیدسی). فرض می‌کنیم A یك حلقهٔ تعویضپذیر باشد. فرض می‌کنیم $f, g\in A[X]$، و g یك چندجمله‌ای تکین باشد. در این‌صورت اعضایی چون $q, r\in A[X]$، باشرط $r=\circ$ یا $\deg r<\deg g$، وجود داردکه $f=qg+r$. به‌علاوه، q و r منحصربه‌فرد هستند.

برهان. فرض می کنیم $\deg f=n$ و $\deg g=m$. اگر $n<m$، قرار می‌دهیم $q=\circ$ و $r=f$. اگر $n\geqslant m$، قضیه را به‌استقرا بر n ثابت می کنیم. فرض می کنیم حکم برای کلیهٔ چندجمله‌ایهای از درجهٔ کوچکتر از n برقرار باشد. اگر a_n ضریب پیشرو f باشد، داریم $\deg(f-a_nX^{n-m}g)<n$، و لذا بنا بر فرض استقرا

$$f-a_nX^{n-m}g=q_1g+r_1$$

که در آن $r_1=\circ$ یا $\deg r_1<m$. در این صورت $f=qg+r$ که در آن $q=a_nX^{n-m}+q_1$ و $r=r_1$.

حال یکتایی را ثابت می‌کنیم. فرض‌کنیم علاوه برعبارت فوق داشته باشیم $f=q'g+r'$ که در آن $r'=\circ$ یا $\deg r'<m$. دراین‌صورت $(q-q')g=r'-r$. اگر $r'\neq r$، آنگاه $q\neq q'$، و چون g یك چندجمله‌ای تکین است داریم $\deg(r'-r)\geqslant m$. این یك تناقض است. پس $r'=r$. چون g تکین است، نتیجه می گیریم که $q'=q$. □

تذکر: قضیهٔ بالادرحالت عمومی‌تری که ضریب پیشرو g یك یکال باشد هم برقرار است. درحالت خاص، اگر A میدان باشدکافی است $g\neq\circ$ فرض شود.

نتیجه. اگر $f\in A[X]$، آنگاه $\alpha\in A$ یك ریشهٔ f است اگر و فقط اگر $X-\alpha$، f را عاد کند.

برهان. بنا برقضیهٔ فوق داریم $f=q(X-\alpha)+a$ که در آن $a\in A$. در این صورت $f(\alpha)=q(\alpha)\circ+a$؛ یعنی $f(\alpha)=\circ$ اگروفقط اگر $X-\alpha$، f راعادکند. □

فرض‌کنیم $f\in A[X]$ و $f\neq\circ$. گوییم $\alpha\in A$ یك ریشهٔ سادهٔ f است اگر $X-\alpha|f$ ولی $(X-\alpha)^2\nmid f$. اگر $(X-\alpha)^r|f$ و $r>1$، α را یك ریشهٔ مکرر f می‌نامیم.

قضیهٔ ۴. فرض‌کنیم A یك حوزهٔ صحیح و f یك عضو درجهٔ n از $A[X]$ باشد. دراین صورت f حداکثر n ریشه دارد.

برهان. اگر $\alpha \in A$ ریشه‌ای برای f باشد، داریم $f=(X-\alpha)g$ که در آن $g \in A[X]$ و $\deg g = n-1$. اگر $\beta \in A$، $\beta \neq \alpha$، ریشه‌ای برای f باشد، داریم $0=f(\beta)=(\beta-\alpha)g(\beta)$. ازآنجایی که A یك حوزهٔ صحیح‌است، داریم $g(\beta)=0$. اینك، قضیه به‌استقرا بر n حاصل می‌شود. □

قضیهٔ ۵. فرض‌کنیم K میدان باشد. در این‌صورت $K[X]$ یك حوزهٔ ایده‌آل اصلی است.

برهان. فرض کنیم I ایده‌آلی ناصفر از $K[X]$ باشد. فرض کنیم $g \in I$ یك چندجمله‌ای ناصفر ازکمترین‌درجه باشد. به‌ازای هر $f \in I$ که $f \neq 0$، بنابرقضیهٔ ۳، داریم $f=qg+r$ که $r=0$ یا $\deg r < \deg g$. چون $r=f-qg \in I$، داریم $r=0$. بنابراین $I=(g)$. □

قضیهٔ ۶. فرض‌کنیم K میدان باشد. دراین صورت هرچندجمله‌ای غیر ثابت $f \in K[X]$ را می‌توان به‌صورت حاصلضربی‌چون $f=c\prod_{i=1}^{m} p_i$، که $c \in K$ و p_iها چندجمله‌ایهای تکین تجزیه‌ناپذیری هستند، نمایش‌داد. به‌علاوه، این عبارت صرفنظر از ترتیب عوامل منحصر به‌فرد است.

برهان. وجود این عبارت را به‌استقرا بر $n=\deg f$ ثابت می‌کنیم. اگر $n=0$، $f \in K$ و چیزی برای اثبات باقی نمی‌ماند. به‌علاوه، اگر f تجزیه‌ناپذیر باشد، آنگاه $f=c(c^{-1}f)$ که در آن $c \in K$ به قسمی انتخاب می‌شود که $c^{-1}f$ یك چندجمله‌ای تکین تجزیه‌ناپذیر باشد. اگر f تجزیه‌ناپذیر نباشد، آنگاه $f=gh$ که در آن $\deg h \neq 0$ و $\deg g \neq 0$. از آنجایی‌که $\deg g < n$ و $\deg h < n$، بنابر فرض استقرا، $g=a\prod_{i=1}^{r} p_i$ و $h=b\prod_{j=1}^{s} q_j$ که درآنها $a, b \in K$، و p_i و q_j چند جمله‌ایهای تکین تجزیه‌ناپذیری هستند. در این صورت $f=ab\prod_{i=1}^{r} p_i \prod_{j=1}^{s} q_j$.

جهت اثبات یکتایی به‌لم ذیل نیاز داریم

لم. فرض کنیم p یك چندجمله‌ای تجزیه‌ناپذیر در $K[X]$ باشد. در این صورت $K[X]/(p)$ میدان است. درحالت خاص، اگر $p|gh$ که درآن $g, h \in K[X]$، آنگاه $p|g$ یا $p|h$.

برهان. فرض‌کنیم $\bar{g} \in K[X]/(p)$ و $\bar{g} \neq 0$. فرض‌کنیم $g \in K[X]$ نماینده‌ای از $\bar{g}$ باشد. دراین‌صورت $g \notin (p)$. ایده‌آل I پدیدآمده توسط p و g را درنظرمی گیریم. ازآنجایی که $K[X]$ یك حوزهٔ ایده‌آل اصلی است، عضوی چون $t \in K[X]$ وجود دارد که $I=(t)$. چون $p \in I$، داریم $p=wt$ که در آن $w \in K[X]$. ادعا می‌کنیم که w

یکال نیست. زیرا درغیر این صورت $I=(p)$ و درنتیجه $g\in(p)$ که خود فرض ما را نقض می‌کند. چون p تجزیه‌ناپذیر است، t یکال است. بنابراین $I=K[X]$ و به ازای اعضایی چون $u, v\in K[X]$، $1=up+vg$. پس $1=\bar{v}\bar{g}$ که در آن $\bar{v}\in K[X]/(p)$ ردهٔ حاوی v است. این مطلب لم را ثابت می‌کند. $\square$

فرض کنیم $f=c\prod_{i=1}^{r}p_i=c'\prod_{j=1}^{s}p'_j$ ؛ $c, c'\in K$ و p_i و p'_j چندجمله‌ایهای تجزیه‌ناپذیر تکینی از $K[X]$ هستند. روشن است که $c=c'$. درنتیجه داریم $\prod_{i=1}^{r}p_i=\prod_{j=1}^{s}p'_j$.

یکتایی را به‌استقرا بر r ثابت می‌کنیم. چون p_r حاصلضرب $\prod_{j=1}^{s}p'_j$ را عاد می‌کند، بنابر لم فوق، p_r یکی ازعوامل $\prod_{j=1}^{s}p'_j$ را عاد می‌کند.می‌توانیم فرض کنیم $p_r \mid p'_s$. چون p_r و p'_s چند جمله‌ایهای تجزیه‌ناپذیر و تکین هستند، داریم $p_r=p'_s$. بنابراین $\prod_{i=1}^{r-1}p_i=\prod_{j=1}^{s-1}p'_j$. اینك، بنابر فرض استقرا، یکتایی حاصل می‌شود. $\square$

قضیهٔ ۷ (گاوس). هر چندجمله‌ای تجزیه ناپذیر غیر ثابت در $\mathbf{Z}[X]$ در $\mathbf{Q}[X]$ نیز تجزیه‌ناپذیر است.

برهان. فرض کنیم f یك چندجمله‌ای تجزیه‌ناپذیر غیر ثابت در $\mathbf{Z}[X]$ باشد. در این صورت بزرگترین مقسوم علیه مشترك ضرایب f مساوی با ۱ است. درصورت امکان، فرض می‌کنیم $f=gh$ که $g, h\in\mathbf{Q}[X]$، $\deg g>0$ و $\deg h>0$. دراین‌صورت $df=g'h'$ که $d\in\mathbf{Z}$، $d>0$، $g', h'\in\mathbf{Z}[X]$، $\deg g'>0$ و $\deg h'>0$. فرض کنیم d_1 (به‌ترتیب d_2) بزرگترین مقسوم علیه مشترك ضرایب g' (به ترتیب h') باشد. از آنجایی که بزرگترین مقسوم علیه مشترك ضرایب f مساوی با ۱ است، نتیجه می‌شود که $d_1d_2 \mid d$. پس، بدون اینکه به‌کلیت برهان خللی وارد آید، می‌توان فرض کرد که بزرگترین مقسوم علیه مشترك ضرایب g' (به‌ترتیب h') مساوی ۱ باشد. فرض کنیم p عامل اولی از d باشد. فرض کنیم $\eta:\mathbf{Z}[X]\to\mathbf{Z}/(p)[X]$ همومورفیسم حلقوی با ضابطهٔ $\eta(\sum a_iX^i)=\sum\bar{a}_iX^i$ باشد که در آن $\bar{a}_i$ ردهٔ حاوی a_i است. داریم $\eta(df)=\eta(g')\eta(h')=0$. از آنجایی که $\mathbf{Z}/(p)[X]$ یك حوزهٔ صحیح است، $\eta(g')=0$ یا $\eta(h')=0$ ؛ یعنی p تمام ضرایب g'، یا تمام ضرایب h' را عاد می‌کند ــ یك تناقض. بنابراین $d=1$، یعنی $f=g'h'$. چون f در $\mathbf{Z}[X]$ تجزیه‌ناپذیر است، یا g' یك یکال است یا h'. این یك تناقض است $\square$

قضیهٔ ۸ (محك ایزنشتاین برای تجزیه‌ناپذیری). فرض کنیم

$$f=a_0+a_1X+\dots+a_nX^n\in\mathbf{Z}[X]$$

فرض کنیم به‌ازای $i<n$، $a_i\equiv 0\pmod p$، $a_n\not\equiv 0\pmod p$ و $a_0\not\equiv 0\pmod{p^2}$

(در اینجا p عددی اول است). در این صورت f در $\mathbf{Q}[X]$ تجزیه‌ناپذیر است.

برهان. می‌توانیم فرض کنیم که بزرگترین مقسوم‌علیه مشترک ضرایب f مساوی با ۱ باشد. به‌خاطر قضیهٔ فوق، کافی است ثابت کنیم که f در $\mathbf{Z}[X]$ تجزیه ناپذیر است. فرض کنیم درصورت امکان، $f = gh$ که $g, h \in \mathbf{Z}[X]$ ، $\deg g > 0$ ، $\deg h > 0$. فرض کنیم $\eta : \mathbf{Z}[X] \to \mathbf{Z}/(p)[X]$ همومورفیسم حلقوی با ضابطهٔ $\eta(\sum b_i X^i) = \sum \bar{b}_i X^i$ باشد که $\bar{b}_i$ ردهٔ مانده‌ای حاوی b_i است. با قرار دادن $\eta(u) = \bar{u}$ ، $u \in \mathbf{Z}[X]$ ، داریم $\bar{f} = \bar{g}\bar{h}$. از آنجایی که $\bar{f} = \bar{a}_n X^n$ ، ازیکتایی تجزیه در $\mathbf{Z}/(p)[X]$ نتیجه می‌شود که $\bar{g} = \bar{b} X^l$ و $\bar{h} = \bar{c} X^{n-l}$. چون $a_n \not\equiv 0 \pmod p$ ، داریم $l = \deg \bar{g} = \deg g > 0$ و $n - l = \deg \bar{h} = \deg h > 0$. بنابراین جمله‌های ثابت g و h بر p بخش‌پذیرند ودرنتیجه $a_0 \equiv 0 \pmod{p^2}$. این مطلب شرط حاکم بر a_0 را نقض می‌کند. □

۴. فضاهای برداری

تعریف. یک فضای برداری روی میدانی مانند K یک سه‌تایی مرتب $(V, +, \psi)$ است که

(۱) $(V, +)$ یک گروه آبلی باشد،

(۲) تابع $\psi : K \times V \to V$ (می‌نویسیم $\psi(\lambda, x) = \lambda x$) چنان باشدکه

(آ) $\lambda(x+y) = \lambda x + \lambda y$ ،

(ب) $(\lambda+\mu)x = \lambda x + \mu x$ ،

(ج) $\lambda(\mu x) = (\lambda\mu)x$ ،

(د) $1x = x$ ؛

که دراینجا $\lambda, \mu \in K$ و $x, y \in V$.

چند تذکر: ۱. اعضای K را عدد واعضای V را بردار می‌نامند.

۲. $\lambda x = 0$ اگر و فقط اگر $\lambda = 0$ یا $x = 0$ زیرا (آ) (به ترتیب (ب)) نتیجه می‌دهد $\lambda 0 = 0$ (به ترتیب $0x = 0$). از سوی دیگر، اگر $\lambda x = 0$ و $\lambda \neq 0$ ، داریم $0 = \lambda^{-1}(\lambda x) = (\lambda^{-1}\lambda)x = 1x = x$.

چند مثال: ۱. فرض کنیم K یک میدان و k زیرمیدانی از K باشد. دراین‌صورت K یک فضای برداری روی k است اگر، به ازای $\lambda \in k$ و $x \in K$ ، قرار دهیم $\psi(\lambda, x) = \lambda x$.

۲. به‌ازای هرمیدان K ، مجموعهٔ K^n متشکل از تمام n-تاییهای مرتب $(\lambda_1, \ldots, \lambda_n)$، $\lambda_i \in K$ ، یک فضای برداری روی K است اگر قرار دهیم

$$(\lambda_1, \ldots, \lambda_n) + (\mu_1, \ldots, \mu_n) = (\lambda_1 + \mu_1, \ldots, \lambda_n + \mu_n),$$

و

$$\lambda(\lambda_1, \ldots, \lambda_n) = (\lambda\lambda_1, \ldots, \lambda\lambda_n).$$

۳. به‌ازای هرمیدان K، حلقهٔ $K[X]$ یك فضای‌برداری روی K می‌شود اگر قرار دهیم $\psi(\lambda, f) = \lambda f$، که در آن $\lambda \in K$ و $f \in K[X]$.

یك زیرمجموعهٔ W از V را یك زیرفضای V نامند اگر W زیرگروهی از $(V, +)$ باشد و به‌ازای $\lambda \in K$ و $x \in W$، $\lambda x \in W$. دراین صورت تحت عمل القایی، W یك فضای برداری روی K است. W را یك زیرفضای سرهٔ V نامیم اگر $V \neq W$.

چند مثال: ۱. (0) و V زیرفضاهایی از V هستند.

۲. اگر K یك میدان باشد، هر ایده‌آل $K[X]$ یك زیرفضای $K[X]$ است.

۳. اشتراك هرخانواده‌ای از زیرفضاهای V یك زیرفضای V است. اگر S زیرمجموعه‌ای از V باشد، اشتراك W از خانوادهٔ تمام زیرفضاهای شامل S را زیرفضای پدیدآمده توسط S و S را یك‌مجموعه ازمولدهای زیرفضای W می‌نامند. به‌سهولت مشاهده می‌شودکه اگر S تهی نباشد، W دقیقاً متشکل ازتمام اعضای به شکل $\sum_{i=1}^{n} \lambda_i x_i$ است که $\lambda_i \in K$، $x_i \in S$ و $n > 0$؛ اگر $S = \phi$، آنگاه $W = \{0\}$.

فرض کنیم V و W فضاهایی برداری روی میدانی مانند K باشند. نگاشتی چون $f: V \to W$ را یك K-نگاشت خطی[1] نامند اگر f همومورفیسمی از $(V, +)$ به‌توی $(W, +)$ باشد و به‌ازای $\lambda \in K$ و $x \in V$، $f(\lambda x) = \lambda f(x)$. یك K-نگاشت خطی $f: V \to W$ را یك ایزومورفیسم نامند اگر K-نگاشتی خطی چون $g: W \to V$ وجود داشته باشدکه $g \circ f = I_V$ و $f \circ g = I_W$. به‌سهولت دیده می‌شودکه یك K-نگاشت خطی $f: V \to W$ یك ایزومورفیسم است اگر وفقط اگر f یك به‌یك و به‌رو باشد.

چند مثال: ۱. نگاشت $p_i: K^n \to K$ با ضابطهٔ $p_i(x_1, \ldots, x_n) = x_i$ یك K-نگاشت خطی است. نگاشتهای p_i را تصویری می‌نامند.

۲. نگاشت $z \to \bar{z}$ یك $\mathbf{R}$-ایزومورفیسم خطی‌ازفضای برداری $\mathbf{C}$ به‌روی $\mathbf{C}$ است.

فرض کنیم V یك فضای برداری و W زیرفضایی از V باشد. گروه جمعی V/W که در آن نوشته شود $\lambda\bar{x} = \overline{\lambda x}$، $\bar{x} \in V/W$ و $\lambda \in K$، به یك فضای برداری تبدیل می‌شود. فضای برداری V/W را فضای خارج‌قسمت V بر W می‌نامند. نگاشت طبیعی $q: V \to V/W$ یك K-نگاشت خطی است.

تذکر: به‌سهولت می‌توان دیدکه اگر $f: V \to W$ یك نگاشت خطی باشد، آنگاه $\ker f$ یك زیرفضای V است واگر f به‌رو باشد، این‌نگاشت ایزومورفیسمی خطی چون $\bar{f}$، از $V/\ker f$ به‌روی W، القا می‌کند.

---

۱. یا تبدیل خطی. ـم.

فرض کنیم x_i ، $1 \leqslant i \leqslant n$ ، عضو V باشد. گوییم این عضوها مستقل خطی هستند اگر $\sum_{1 \leqslant i \leqslant n} \lambda_i x_i = 0$ ، $\lambda_i \in K$ ، ایجاب کند که به‌ازای هر i ، $1 \leqslant i \leqslant n$ ، $\lambda_i = 0$.

یك زیرمجموعهٔ S از V را مستقل خطی گویند اگر هر زیرمجموعهٔ متناهی از S مستقل خطی باشد. مجموعهٔ متشکل از تنها یك عضو ناصفر V مستقل خطی است. توجه کنید که هر زیرمجموعهٔ یك مجموعهٔ مستقل‌خطی خود نیز مستقل خطی‌است. S را وابستهٔ خطی گویند اگر مستقل خطی نباشد.

تعریف. یك زیرمجموعهٔ S از V را یك مبنا (یا یك K-مبنا) از V می‌نامند اگر S مستقل خطی باشد و V را پدید آورد.

روشن است که S یك مبنای V است اگر وفقط اگر هرعضو $v \in V$ را بتوان به‌طور منحصر به‌فرد به‌صورت حاصلجمعی متناهی چون $v = \sum \lambda_i s_i$ ، $\lambda_i \in K$ و $s_i \in S$، نوشت.

چند مثال: ۱. مجموعهٔ $\{1, X, X^2, \dots\}$ مبنایی برای فضای برداری $K[X]$ است.

۲. به‌ازای هرمیدان K ، عضوهای $e_i = (\delta_{i1}, \dots, \delta_{in})$ ، $1 \leqslant i \leqslant n$، که در آن اگر $i \neq j$ ، $\delta_{ij} = 0$ و اگر $i = j$ ، $\delta_{ij} = 1$، مبنایی برای فضای برداری K^n تشکیل می‌دهند.

قضیهٔ ۹. فرض کنیم V یك فضای برداری باشد. فرض کنیم x_i ها، $1 \leqslant i \leqslant m$، V را پدید آورند. اگر S یك مجموعهٔ مستقل خطی دلخواه از V باشد،آنگاه S حداکثر m عضو دارد.

برهان. قضیه را به‌استقرا بر m ثابت خواهیم‌کرد. اگر $m = 0$، آنگاه $V = (0)$ و $S = \varnothing$. فرض کنیم $m > 0$ وفرض کنیم $y_1, \dots, y_n$ تعداد متناهی ازاعضای S باشند. فرض‌کنیم V' زیرفضای V، پدید آمده توسط $x_2, \dots, x_m$ باشد. اگر $y_i \in V'$ ، $1 \leqslant i \leqslant n$، آنگاه بنابر فرض استقرا $n \leqslant m-1$. پس فرض می‌کنیم به‌ازای اندیسی چون i، فرضاً $i = 1$ ، $y_i \notin V'$. دراین صورت $y_1 = \sum_{i=1} \alpha_i x_i$ ، $\alpha_1 \neq 0$ ، پس $\beta_i \in K$ که $x_1 = \beta_1 y_1 + \sum_{2 \leqslant i \leqslant m} \beta_i x_i$، بنابراین V توسط اعضای $y_1, x_2, \dots, x_m$ پدید می‌آید. لذا عضوی چون $\lambda_i \in K$، $2 \leqslant i \leqslant n$ ، وجود دارد که $y_i - \lambda_i y_1 \in V'$. واضح‌است که اعضای $y_i - \lambda_i y_1$ ، $2 \leqslant i \leqslant n$ ، مستقل خطی هستند و درنتیجه، بنا بر فرض استقرا، $n - 1 \leqslant m - 1$. پس S حداکثر m عضو دارد. □

نتیجهٔ ۱. اگر $\{x_1, \dots, x_m\}$ و $\{y_1, \dots, y_n\}$ دومبنا برای V باشند آنگاه $m = n$.

گوییم یك فضای برداری V از بعد n است (نماد: $\dim V = n$) اگر مبنایی با n عضو برای V وجود داشته باشد. اگر $\dim V = n$ آنگاه، بنا برنتیجهٔ ۱ هرمبنای V دارای n عضو است.

نتیجهٔ ۲. فرض کنیم W زیرفضایی از V باشد و $\dim V = n$. دراین صورت W مبنایی بـا حداکثر n عضو دارد. یعنی $\dim W \leqslant \dim V$. اگر W زیرفضایی سره از V باشد، آنگاه $\dim W < \dim V$.

برهان. هرمجموعهٔ مستقل‌خطی از V، متشکل‌ازحداکثر n عضو است. یك مجموعهٔ مستقل خطی ماکسیمال ازاعضای W اختیار می کنیم. این مجموعه مبنایی برای W تشکیل می‌دهد. بدین‌ترتیب $\dim W \leqslant \dim V$. ازآنجایی کـه هرمجموعهٔ مستقل خطی متشکل از n عضو فضای برداری V را پدید می‌آورد، نتیجه می‌شود کـه اگر W یك زیرفضای سرهٔ V باشد آنگاه $\dim W < \dim V$. □

قضیهٔ ۱۰. فرض‌کنیم V یك فضای برداری روی میدان نامتناهی K باشد. دراین‌صورت V نمی‌تواند مساوی با اجتماع تعدادی متناهی از زیرفضاهای سرهٔ خود باشد.

برهان. ثابت می‌کنیم کـه اگر (V_i)ها، $1 \leqslant i \leqslant n$، n زیـرفضای سرهٔ V باشند، آنگاه $x \in V$ ی وجود دارد که $x \notin \bigcup_{i=1}^{n} V_i$. این‌مطلب را به‌استقرا بر n ثابت می‌کنیم. اگر $n = 1$، x را طوری اختیار می‌کنیم کـه $x \notin V_1$. فرض می‌کنیم عضوی مـانند e از V وجود داردکه $e \notin V_i$، $1 \leqslant i \leqslant n-1$. اگر $e \notin V_n$، چیزی برای اثبات نداریم. فرض کنیم $e \in V_n$. fی را اختیار می‌کنیم که $f \notin V_n$. دراین صورت به ازای هر $\lambda \in K^*$، $e + \lambda f \notin V_n$.[1] ادعا می‌کنیم که عضوی چون $\lambda_0 \in K^*$ وجود داردکه $e + \lambda_0 f \notin V_i$، $1 \leqslant i \leqslant n$. زیرا درغیر این‌صورت، چون K نامتناهی‌است، $\lambda, \lambda' \in K^*$ی وجود دارند کـه $\lambda \neq \lambda'$ و بـه ازای یك $i < n$، $e + \lambda f, e + \lambda' f \in V_i$. در این صـورت $(\lambda - \lambda') f \in V_i$، ولذا $f \in V_i$. پس $e \in V_i$، که این یك تناقض است. □

---

۱. $K^* = K - \{0\}$. توجه‌کنید اگر $\lambda = 0$، رابطهٔ $e + \lambda f \notin V_n$ بـا توجه به فرض درست نیست.ـم.

فصل ۳

توسیعهای یك میدان

۱. توسیع جبری

فرض‌کنیم K یك میدان و k زیرمیدانی از K باشد. در این صورت K را یك توسیع k می‌نامند و می‌نویسند K/k. دو توسیع K/k و K'/k را k-ایزومورف نامند اگر ایزومورفیسمی چون σ از K به‌روی K' وجود داشته باشد که $\sigma|k$ نگاشت همانی باشد. دراین صورت σ را یك k-ایزومورفیسم می‌نامند. فرض‌کنیم $\alpha_1, \ldots, \alpha_n \in K$. آن زیرمیدان (به‌ترتیب، زیرحلقه) از K راکه توسط k و $\alpha_1, \ldots, \alpha_n$ پدید آید با $k(\alpha_1, \ldots, \alpha_n)$ (به ترتیب $k[\alpha_1, \ldots, \alpha_n]$) نمایش می‌دهیم. روشن است که $k[\alpha_1, \ldots, \alpha_n]$ یك‌زیرحلقهٔ $k(\alpha_1, \ldots, \alpha_n)$ است. آشکارا هر $\alpha \in k(\alpha_1, \ldots, \alpha_n)$ را می‌توان به شکل $\alpha = \dfrac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}$، که در آن

$$f(\alpha_1, \ldots, \alpha_n) = \sum_{i_1, \ldots, i_n} a_{i_1 \ldots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n},$$

$$g(\alpha_1, \ldots, \alpha_n) = \sum_{j_1, \ldots, j_n} b_{j_1 \ldots j_n} \alpha_1^{j_1} \cdots \alpha_n^{j_n},$$

$a_{i_1 \ldots i_n}, b_{j_1 \ldots j_n} \in k$، و $g(\alpha_1, \ldots, \alpha_n) \neq 0$ نوشت. به‌ازای $\alpha \in K$، میدان $k(\alpha)$ را یك توسیع سادهٔ k می‌نامند. نگاشت $\phi : k[X] \to k[\alpha]$ با ضابطهٔ $\phi(g) = g(\alpha)$، $g \in k[X]$، به وضوح یك همومورفیسم حلقوی به‌رو است.

حالت ۱: $\ker\phi=(0)$، یعنی α ریشهٔ هیچ چندجمله‌ای ناصفر روی k نیست. دراین حالت α روی k متعالی است. لذا، همومورفیسم یك به یك $\phi: k[X] \to k(\alpha)$ را می‌توان به‌همومورفیسمی از $k(X)$، میدان کسرهای $k[X]$، به‌روی زیرمیدانی از $k(\alpha)$ توسعه داد. به‌هرحال، این زیرمیدان شامل α و k است و بنابراین باید بر $k(\alpha)$ منطبق شود. پس $k(\alpha)$ با $k(X)$ ایزومورف است.

حالت ۲: $\ker\phi\neq(0)$، یعنی α ریشهٔ یك چندجمله‌ای ناصفر است. دراین‌صورت α روی k جبری است. از آنجایی که هر ایده‌آلی در $k[X]$ ایده‌آلی اصلی است (فصل ۲، قضیهٔ ۱)، به ازای $f\in k[X]$ی داریم $\ker\phi=(f)$. روشن است که f یك مقدار ثابت نیست. چندجمله‌ای f تجزیه‌ناپذیر است. در واقع، فرض‌می‌کنیم $f=gh$ که هم $\deg g$ وهم $\deg h$ از $\deg f$ کوچکتر باشند. دراین صورت داریم $0=f(\alpha)=g(\alpha)h(\alpha)$. درنتیجه $g(\alpha)=0$ یا $h(\alpha)=0$، یعنی $g\in(f)$ یا $h\in(f)$. این نتایج، با توجه به‌شرطی که روی درجات g و h گذاشتیم ممتنع هستند.

بدین ترتیب ایزومورفیسم $k[X]/(f)\approx k[\alpha]$ را داریم. از آنجایی که $k[X]/(f)$ میدان است (رجوع کنید به‌فصل ۲)، نتیجه می‌شود که $k[\alpha]$ هم میدان است، وچون این میدان شامل α و k است، داریم $k[\alpha]=k(\alpha)$. بنابراین $k(\alpha)\approx k[X]/(f)$. می‌توانیم فرض کنیم که f یك چندجمله‌ای تکین باشد. در این صورت این چندجمله‌ای f را چندجمله‌ای مینیمال α روی k می‌نامند.

یك توسیع K/k را یك توسیع جبری نامند اگر هر $\alpha\in K$، روی k جبری باشد. توجه می‌کنیم که اگر $\alpha\in K$ روی k جبری باشد، آنگاه روی هرمیدان L، $K\supset L\supset k$، نیز جبری است.

قضیهٔ ۱. فرض کنیم $\alpha\in K$ روی k جبری باشد وفرض کنیم n درجهٔ چند جمله‌ای مینیمال آن را نمایش دهد. در این‌صورت $k(\alpha)$، به‌عنوان یك فضای برداری روی k، دارای بعد n روی k است.

برهان. در واقع، $1, \alpha, \ldots, \alpha^{n-1}$ برای $k(\alpha)$ یك k-مبنا تشکیل می‌دهند. زیرا α نمی‌تواند در یك چندجمله‌ای از درجهٔ کمتر از n صدق کند و در نتیجه اعضای $1, \alpha, \ldots, \alpha^{n-1}$ روی k مستقل خطی هستند. به‌علاوه، به‌استقرا روشن است که هر α^i را می‌توان به‌صورت ترکیبی خطی از $1, \alpha, \ldots, \alpha^{n-1}$، باضرایب در k، نوشت. □

فرض کنیم K/k توسیعی باشد که K یك فضای برداری با بعد n روی k باشد. در این صورت K را یك توسیع متناهی k می‌نامیم و می‌نویسیم $[K:k]=n$ (K درجهٔ n روی k نام دارد). اگر $\alpha_1, \ldots, \alpha_n\in K$ مبنایی برای K روی k تشکیل دهند، داریم $K=k(\alpha_1, \ldots, \alpha_n)$.

قضیهٔ ۲. هرتوسیع متناهی K/k یك توسیع جبری است.

برهان. به‌ازای هر $\alpha \in K$، $\alpha \neq 0$، عدد صحیح ناصفری مانند n وجود دارد که اعضای $1, \alpha, \ldots, \alpha^n$، روی k، وابستهٔ خطی هستند و در نتیجه اعضایی چون $a_0, \ldots, a_n \in k$ وجود دارند که دست‌کم به‌ازای یك i، $a_i \neq 0$ و $\sum_{0 \leqslant i \leqslant n} a_i \alpha^i = 0$.
به‌عبارت دیگر، α ریشهٔ یك چندجمله‌ای ناصفر $\sum_{0 \leqslant i \leqslant n} a_i X^i$ است. □

قضیهٔ ۳. فرض کنیم K/k و L/K توسیعهایی باشند که $[K:k]=m$ و $[L:K]=n$. دراین صورت $[L:K]=mn$.

برهان. فرض کنیم $\alpha_1, \ldots, \alpha_m$ یك k-مبنا برای K تشکیل دهند و $\beta_1, \ldots, \beta_n$ یك K-مبنا برای L باشد. ادعا می‌کنیم که اعضای $\alpha_i\beta_j$، $1 \leqslant i \leqslant m$، $1 \leqslant j \leqslant n$، یك k-مبنا برای L تشکیل می‌دهند. در واقع فرض کنیم $\alpha \in L$. دراین‌صورت $\alpha = \sum_{1 \leqslant j \leqslant n} t_j \beta_j$، که $t_j \in K$. فرض کنیم $t_j = \sum_{1 \leqslant i \leqslant m} s_{ij}\alpha_i$ و $s_{ij} \in k$. در این صورت داریم $\alpha = \sum_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} s_{ij}\alpha_i\beta_j$. بنابراین $\alpha_i\beta_j$ها L را، به عنوان فضایی برداری روی k، پدید می‌آورند. ازطرف دیگر، فرض کنیم $\sum_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} s_{ij}\alpha_i\beta_j = 0$ که درآن $s_{ij} \in k$. دراین‌صورت باید، به‌ازای هر j، داشته باشیم $\sum_{1 \leqslant i \leqslant m} s_{ij}\alpha_i = 0$. این رابطه ایجاب می‌کند که، به‌ازای هر i و j باشرط $1 \leqslant i \leqslant m$ و $1 \leqslant j \leqslant n$، $s_{ij} = 0$. پس $\alpha_i\beta_j$ها مستقل خطی هستند. □

نتیجهٔ ۱. فرض‌کنیم K/k توسیعی دلخواه باشد و $\alpha_1, \ldots, \alpha_n \in K$ روی k جبری باشند. دراین صورت، $k(\alpha_1, \ldots, \alpha_n)/k$ یك توسیع متناهی است.

برهان. در واقع، این نتیجه به‌ازای $n=1$ قبلاً ثابت شده است (قضیهٔ ۱). بنابراستقرا، فرض کنیم $k(\alpha_1, \ldots, \alpha_{n-1})/k$ یك توسیع متناهی باشد دراین صورت $k(\alpha_1, \ldots, \alpha_n) = k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ یك توسیع متناهی $k(\alpha_1, \ldots, \alpha_{n-1})$ است. اینك نتیجهٔ موردنظر از قضیهٔ ۳ حاصل می‌شود. □

ازنتیجهٔ ۱ برمی‌آید که اگر $\alpha, \beta \in K$ روی k جبری باشند، آنگاه $\alpha+\beta$، $\alpha^{-1} (\alpha \neq 0)$ و $\alpha\beta$ روی k جبری هستند.

نتیجهٔ ۲. اگر K/k و L/K توسیعهایی جبری باشند، آنگاه L/k توسیعی جبری است.

برهان. فرض کنیم $\alpha \in L$ و فرض کنیم $\sum_{0 \leqslant i \leqslant n} a_i\alpha^i = 0$ که $a_0, \ldots, a_n \in K$ و دست‌کم به‌ازای یك i داشته باشیم $a_i \neq 0$. روشن است که α روی $k(a_0, \ldots, a_n)$ جبری است. ازآنجایی که، بنابرنتیجهٔ ۱، $k(a_0, \ldots, a_n)/k$ یك توسیع متناهی است، از قضیهٔ ۳ نتیجه می‌شود که $k(\alpha, a_0, \ldots, a_n)/k$ هم یك توسیع متناهی‌است. پس، بنابرقضیهٔ ۲، α روی k جبری است. □

چند مثال: ۱. هرمیدانی توسیعی ازمیدان اول خودش است.
۲. $\mathbf{C}/\mathbf{R}$ یك توسیع از درجهٔ ۲ است.
۳. به‌ازای هرمیدان k، $k(X)/k$ جبری نیست؛ در اینجا $k(X)$ میدان خارج‌قسمت $k[X]$ است. در واقع، X روی k متعالی است.

۲. میدان شکافنده و توسیع نرمال

تعریف. فرض‌کنیم k یك میدان باشد و $f \in k[X]$. یك توسیع K/k را یك میدان شکافندهٔ f می‌نامند اگر

$$\text{(i)} \qquad f(X)=c\prod_{1\leqslant i\leqslant n}(X-\alpha_i); \quad \alpha_i \in K\ ,\ c\in k\ ;$$

$$\text{(ii)} \qquad K=k(\alpha_1\ ,\ \ldots\ ,\ \alpha_n).$$

قضیهٔ ۴. هرچند جمله‌ای غیرثابت $f \in k[X]$ دارای یك میدان شکافنده است.

برهان. فرض‌کنیم $f \in k[X]$ یك چندجمله‌ای تجزیه‌ناپذیر باشد. دراین صورت $k[X]/(f)$ یك میدان است (رجوع‌کنید به‌فصل ۲). نگاشت $a \to \bar{a}$ از k به‌توی $k[X]/(f)$ که درآن $\bar{a}$ مساوی با همدستهٔ a در $k[X]/(f)$ است، آشکارا همومورفیسمی یك به‌یك‌است وما k را با تصویرش یکی می گیریم. بنابراین، $k[X]/(f)$ یك توسیع k است. فرض می کنیم $q: k[X] \to k[X]/(f)$ نگاشت طبیعی را نمایش دهد؛ قرار می‌دهیم $q(X)=\alpha$. روشن است‌که $f(\alpha)=0$. فرض‌کنیم $\deg f=n$. چون $1\ ,\ \alpha\ ,\ \ldots\ ,\ \alpha^{n-1}$ مبنایی برای $k[X]/(f)$ به‌عنوان یك فضای برداری روی k است (قضیهٔ ۱)، داریم $[k[X]/(f):k]=\deg f$.

اینك قضیه را به‌استقرا بر $n=\deg f$ ثابت می‌کنیم. اگر $n=1$، f یك چندجمله‌ای خطی است و آشکارا k یك میدان شکافندهٔ f است. فرض می کنیم $n\geqslant 2$ و نیز فرض‌می کنیم به‌ازای هرچندجمله‌ای g از درجهٔ $n-1$ روی هرمیدانی، یك توسیع متناهی وجود داشته باشدکه درآن بتوان g را به صورت حاصلضربی از عوامل خطی نوشت. فرض می کنیم f یك چندجمله‌ای از درجهٔ n باشد و f_1 عاملی تجزیه‌ناپذیر از f باشد. فرض کنیم $K_1=k(\alpha)$ توسیعی از k باشدکه $f_1(\alpha)=0$. دراین صورت $f(\alpha)=0$ و ازآنجا $f=(X-\alpha)g$، $g\in K_1[X]$ و $\deg g=n-1$ (نتیجهٔ قضیهٔ ۳، فصل ۲). بنابر فرض استقرا، یك توسیع متناهی برای K_1 وجود دارد که درآن g را می‌توان به‌صورت حاصلضربی ازعوامل خطی نوشت. پس، یك توسیع متناهی مانند K/k وجود داردکه $f(X)=c\prod\limits_{1\leqslant i\leqslant n}(X-\alpha_i)$، $\alpha_i\in K$، $c\in k$. دراین صورت $k(\alpha_1\ ,\ \ldots\ ,\ \alpha_n)$ یك میدان شکافندهٔ f است. این، برهان قضیه را کامل می کند. □

فرض‌کنیم k و k' میدان باشند و $\sigma: k \to k'$ یك ایزومورفیسم باشد. اگر، به ازای هرچندجمله‌ای $f=a_0+\cdots+a_nX^n \in k[X]$ تعریف کنیم

$\bar{\sigma}(f) = \sum_{0 \leqslant i \leqslant n} \sigma(a_i)X^i$، ایزومورفیسمی چون $\bar{\sigma}: k[X] \to k'[X]$ داریم که $\bar{\sigma}|k = \sigma$.
از این پس غالباً به‌جای $\bar{\sigma}$ می‌نویسیم σ. اگر $f \in k[X]$ تجزیه‌ناپذیر باشد، آنگاه $\sigma(f)$ در $k'[X]$ تجزیه‌ناپذیر است و از آنجا یک ایزومورفیسم القایی خواهیم داشت: $k[X]/(f) \approx k'[X]/(\sigma(f))$. از آنجایی که به‌ازای هر ریشهٔ α از f، ایزومورفیسمی چون $k[X]/(f) \approx k(\alpha)$ وجود دارد که همدستهٔ X را بر α می‌نگارد، چنین نتیجه می‌شود که اگر α (به‌ترتیب، α') ریشه‌ای از f (به‌ترتیب، $\sigma(f)$) باشد، ایزومورفیسمی به‌صورت $k(\alpha) \approx k'(\alpha')$ وجود دارد که (در آن α بر α' نگاشته می‌شود) تحدید آن به k مساوی با σ است.

درحالت خاص، اگر $k' = k$ و σ نگاشت همانی باشد، آنگاه به‌ازای هر دو ریشهٔ α و α' از f یک k-ایزومورفیسم $k(\alpha) \approx k(\alpha')$ وجود دارد که α را بر α' می‌نگارد.

تعریف. فرض کنیم K/k توسیعی جبری باشد. دوعضو $\alpha, \alpha' \in K$ روی k مزدوج نامیده می‌شود اگر k-ایزومورفیسمی از $k(\alpha)$ به‌روی $k(\alpha')$ وجود داشته باشدکه α را بر α' بنگارد.

قضیهٔ ۵. فرض کنیم K/k توسیعی جبری باشد و $\alpha, \alpha' \in K$. دراین صورت α و α' روی k مزدوج هستند اگر وفقط اگر روی k، چندجمله‌ای مینیمال همانند داشته باشند.

برهان. اگر α و α' روی k چندجمله‌ای مینیمال همانند داشته باشند، قبلاً ثابت کردیم که α و α' مزدوج هستند. به‌عکس، فرض کنیم α و α' روی k مزدوج باشند. فرض کنیم f و g، به‌ترتیب، چندجمله‌ایهای مینیمال α و α' را نشان دهند. فرض کنیم $\sigma: k(\alpha) \to k(\alpha')$، k-ایزومورفیسمی باشد که $\sigma(\alpha) = \alpha'$. داریم

$$0 = \sigma(f(\alpha)) = f(\sigma(\alpha)) = f(\alpha').$$

بنابراین، $g|f$. از آنجایی که f تکین وتجزیه‌ناپذیر است، داریم $f = g$. □

قضیهٔ ۶. فرض کنیم k و k' میدانهایی باشند و $\sigma: k \to k'$ یک ایزومورفیسم باشد. فرض کنیم f یک چندجمله‌ای با ضرایب در k باشد وفرض کنیم K و K'، به‌ترتیب، میدانهای شکافندهٔ f و $\sigma(f)$ باشند. دراین صورت k-ایزومورفیسمی مانند $\tau: K \to K'$ وجود دارد که $\tau | k = \sigma$.

برهان. روند استقرا بردرجهٔ f را درپیش می‌گیریم. اگر $\deg f = 0$، چیزی برای اثبات باقی نمی‌ماند. فرض کنیم $\deg f \geqslant 1$ و f_1 یک عامل تجزیه‌ناپذیر f باشد. فرض کنیم α ریشه‌ای از f_1 و α' ریشه‌ای دلخواه از $\sigma(f_1)$ باشد. بنابرآنچه که دربالا دیدیم، σ را می‌توان به ایزومورفیسمی مانند $\sigma_1: k(\alpha) \to k'(\alpha')$ توسعه داد که $\sigma_1(\alpha) = \alpha'$. فرض کنیم $f = (X - \alpha)g$ و $g \in k(\alpha)[X]$. دراین صورت $\sigma(f) = (X - \alpha')\sigma_1(g)$. اگر میدان K (به ترتیب، K') یک میدان شکافندهٔ چندجمله‌ای

g (به‌ترتیب، $(\sigma_1(g)$) روی $k(\alpha)$ (بـه‌ترتیب، $(k'(\alpha')$) باشد، بنابر فرض استقرا، σ_1 را می‌توان به‌ایزومورفیسمی مانند $\tau: K \to K'$ توسعه داد. به‌وضوح داریم $\tau|k=\sigma$. □

درحالت خاص، با مساوی گـرفتن k و k' وهمچنین σ=نگاشت همانی، نتیجهٔ ذیل حاصل می‌شود.

نتیجه. هر دومیدان شکافندهٔ یك چندجمله‌ای، ایزومورف هستند؛ یعنی، میدان‌شکافندهٔ یك چندجمله‌ای «درحد یك k-ایزومورفیسم» منحصر به‌فرد است.

با توجه بـه نتیجهٔ بالا، ما صحبت از «میدان شکافندهٔ» یك چندجمله‌ای f روی k می‌کنیم.

فرض کنیم k میدان باشد وفرض کنیم K و K' توسیعهایی از k باشند. همومورفیسمی یك به‌یك چون $\sigma: K \to K'$ راکـه $\sigma|k$ نگاشت همانی باشد، یك k-ایزومورفیسم از K به‌توی K' می‌نامند.

قضیهٔ ۷. فرض کنیم K میدان شکافندهٔ یك چندجمله‌ای f روی یك میدان k باشد وفرض کنیم L/K توسیعی دلخواه باشد. دراین صورت، به ازای هر k-ایزومورفیسم σ از K به‌توی L داریم $\sigma(K)=K$.

برهان. فرض کنیم $\alpha_1, \ldots, \alpha_n$ ریشه‌های f در K باشند. چون $\sigma(\alpha_i)$ نیز ریشه‌ای از f است وچـون f در L حـداکثر n ریشه دارد، باید بـه ازای اندیسی چون j، $\sigma(\alpha_i)=\alpha_j$. σ، چون یك به‌یك است، جایگشتی برمجموعهٔ اعضای $\alpha_1, \ldots, \alpha_n$ است. درنتیجه $\sigma(K)=K$. □

قضیهٔ ۸. فرض کنیم K میدان شکافندهٔ یك چندجمله‌ای f روی k باشد وفرض کنیم ϕ یك چندجمله‌ای تجزیه‌ناپذیر روی k باشد. اگر ϕ در K ریشه‌ای داشته باشد، آنگاه ϕ در K به‌حاصلضرب عوامل خطی تجزیه می‌شود. به‌عکس، اگر K/k توسیعی متناهی باشد که هر چندجمله‌ای تجزیه‌ناپذیر روی k، و دارای ریشه‌ای در K، مساوی بـا حاصلضربی از عوامل خطی در K باشد، آنگاه K میدان شکافندهٔ یك چندجمله‌ای روی k است.

برهان. فرض کنیم $K=k(\alpha_1, \ldots, \alpha_n)$، که در آن $\alpha_1, \ldots, \alpha_n$ ریشه‌های f هستند، میدان شکافندهٔ f باشد. فرض کنیم $\beta \in K$ ریشه‌ای از ϕ باشد و L میدان شکافندهٔ ϕ روی K بـاشد. فـرض کنیم β' ریشه‌ای دلخواه از ϕ در L بـاشد. دراین صورت k-ایزومورفیسمی مانند $\sigma: k(\beta) \to k(\beta')$ وجود داردکه $\sigma(\beta)=\beta'$. از آنجایی کـه میدان شکافندهٔ f (به‌ترتیب، $\sigma(f)=f$) روی $k(\beta)$ (به‌ترتیب، روی $k(\beta')$) مساوی با $K(\beta)=k(\beta, \alpha_1, \ldots, \alpha_n)=K$ (به‌ترتیب، $K(\beta')=k(\beta', \alpha_1, \ldots, \alpha_n)$) است، σ را می‌توان به k-ایزومورفیسمی از K بـه‌روی $K(\beta')$ توسعه داد. چون K یك میدان شکافنده است، ازقضیهٔ ۷ نتیجه می‌شودکه این k-ایزومورفیسم اتومورفیسمی از K است، یعنی $K=K(\beta')$ یا $\beta' \in K$.

اکنون فرض می‌کنیم K/k توسیعی متناهی باشد که هر چندجمله‌ای تجزیه‌ناپذیر روی k با ریشه‌ای در K، مساوی با حاصلضربی از عوامل خطی در K باشد. فرض کنیم $K=k(\alpha_1, \ldots, \alpha_n)$ و فرض کنیم $f_1, \ldots, f_n$، به‌ترتیب، چندجمله‌ایهای مینیمال $\alpha_1,\ldots,\alpha_n$ را نشان دهند. روشن‌است که K میدان شکافندهٔ چندجمله‌ای $\prod\limits_{1\leqslant i\leqslant n} f_i$ است. □

تعریف. یك توسیع نرمال K/k توسیعی جبری است‌که هرچندجمله‌ای تجزیه‌ناپذیر روی k که ریشه‌ای در K داشته باشد، مساوی با حاصلضربی ازعوامل خطی در K باشد. از قضیهٔ ۸ نتیجه می‌شود که‌توسیعهای نرمال متناهی دقیقاً همان میدانهای‌شکافنده‌هستند.

قضیهٔ ۹. فرض کنیم K/k یك توسیع متناهی باشد. دراین صورت یك توسیع نرمال متناهی مانند L/k وجود داردکه K زیرمیدانی از L باشد. فرض کنیم K_i/k، $i=1, 2, \ldots, n$، توسیعهایی متناهی باشند. آنگاه یك توسیع نرمال متناهی مانند L/k و k-ایزومورفیسمهایی مانند σ_i از K_i به‌توی L وجود دارند.

برهان. فرض کنیم $K=k(\alpha_1, \ldots, \alpha_n)$ و فرض کنیم f_i، $1\leqslant i\leqslant n$، چندجمله‌ای مینیمال α_i روی k باشد. میدان شکافندهٔ چندجمله‌ای $\phi=\prod\limits_{1\leqslant i\leqslant n} f_i$، به‌عنوان یك چندجمله‌ای روی K، به‌وضوح میدان شکافندهٔ ϕ روی k است ومی‌توانیم L را مساوی با این میدان بگیریم.

اکنون فرض‌می کنیم K_i/k، $1\leqslant i\leqslant n$، توسیعهایی متناهی باشند.فرض کنیم‌توسیع نرمال‌متناهی N_i/k، $1\leqslant i\leqslant n$، چنان‌باشدکه‌به‌ازای $1\leqslant i\leqslant n$، K_i زیرمیدانی از N_i باشد.فرض کنیم N_i میدان شکافندهٔ چندجمله‌ای ϕ_iرویK باشد. می‌نویسیم $\phi=\prod\limits_{1\leqslant i\leqslant n} \phi_i$. میدان شکافندهٔ ϕ روی k را L می گیریم. ازآنجایی‌که ϕ_i در L شکافته می‌شود، L شامل میدان شکافنده‌ای برای ϕ_i، $1\leqslant i\leqslant n$، است. بنابراین k-ایزومورفیسمی از N_i (و در نتیجه از K_i) به‌توی L وجود دارد. □

چند مثال: ۱. فرض‌کنیم α ریشه‌ای از $X^3-2\in \mathbf{Q}[X]$ باشد. دراین صورت $\mathbf{Q}(\alpha)/\mathbf{Q}$ یك توسیع نرمال نیست.

۲. میدان $\mathbf{C}$ متشکل از اعداد مختلط طوری است که هرچندجمله‌ای غیرثابت با ضرایب در $\mathbf{C}$ دارای ریشه‌ای در $\mathbf{C}$ است (قضیهٔ بنیادی جبر)؛ به‌عبارت دیگر، $\mathbf{C}$ میدان شکافندهٔ هرچندجمله‌ای در $\mathbf{C}[X]$ را دربر دارد. چنین میدانهایی را جبراً بسته می‌نامند.

۳. توسیع جداپذیر

تعریف. فرض کنیم k یك میدان باشد. یك چندجمله‌ای تجزیه‌ناپذیر $f\in k[X]$ را جداپذیر نامند اگر (درمیدان شکافنده) همه ریشه‌هایش ساده باشند. درغیر این صورت، f را

جداناپذیر می‌نامند. یك چندجمله‌ای غیرثابت $f \in k[X]$ را جداپذیرگویند اگر کلیهٔ عوامل تجزیه‌ناپذیرش جداپذیر باشند.

فرض کنیم K/k یك توسیع جبری باشد. عضوی چون $\alpha \in K$ روی k جداپذیر نامیده می‌شود اگر چندجمله‌ای مینیمال α روی k جداپذیر باشد. عضوی مانند α از K که جداپذیر نباشد، یك عضو جداناپذیر نامیده می‌شود. یك توسیع جبری K/k را جداپذیر نامند. هرگاه تمام عضوهایش روی k جداپذیر باشند؛ درغیراین‌صورت این توسیع جبری جداناپذیر نامیده می‌شود.

اگر $\alpha \in K$ روی k جداپذیر باشد، α روی هرمیدان L که $K \supset L \supset k$ نیز جداپذیر است. در واقع چندجمله‌ای مینیمال g برای α روی L، چندجمله‌ای مینیمال f برای α روی k را عاد می‌کند. چون f جداپذیر است، نتیجه می‌شود که g نیز جداپذیر است.

قبل از ادامهٔ بحث دربارهٔ توسیعهای جداپذیر درباب ریشه‌های چندجمله‌ایها، به‌معرفی چند نتیجه می‌پردازیم.

فرض‌کنیم $f \in k[X]$ و فرض‌کنیم $f = \sum_{0 \leqslant i \leqslant n} a_i X^i$. مشتق f را که با f' نشان داده می‌شود، با ضابطهٔ $f' = \sum_{1 \leqslant i \leqslant n} i a_i X^{i-1}$ تعریف می‌کنیم. ویژگیهای ذیل به سهولت ثابت می‌شوند؛ فرض این است که $f, g \in k[X]$ و $a \in k$.

(i) اگر $f \in k$، آنگاه $f' = 0$،

(ii) $(f+g)' = f' + g'$،

(iii) $(fg)' = fg' + f'g$،

(iv) $(af)' = af'$.

فرض‌کنیم $\alpha \in k$ ریشه‌ای ازیك چندجمله‌ای f باشد. فرض‌کنیم $f = (X-\alpha)g$. دراین صورت داریم

$$f' = (X-\alpha)g' + g.$$

ازاینجا نتیجه می‌شود که $g(\alpha) = f'(\alpha)$.

قضیهٔ ۱۰. فرض‌کنیم $f \in k[X]$ یك چندجمله‌ای غیرثابت و α ریشه‌ای ازآن باشد. دراین صورت α ریشه‌ای مکرر است اگر وفقط اگر $f'(\alpha) = 0$.

برهان. فرض‌کنیم $f = (X-\alpha)g$. روشن است که α یك ریشهٔ مکرر f است اگر وفقط اگر $g(\alpha) = 0$. چون $f'(\alpha) = g(\alpha)$، قضیه ثابت می‌شود. □

نتیجهٔ ۱. فرض کنیم f یك چندجمله‌ای تجزیه‌ناپذیرباشد. دراین صورت f ریشه‌ای مکرر دارد اگر وفقط اگر $f' = 0$.

برهان. می‌توانیم فرض‌کنیم که f تکین است. فرض‌کنیم α ریشه‌ای از f باشد.

بنابر نتیجهٔ بالا، α یك ریشهٔ مکرر f است اگر وفقط اگر α ریشه‌ای از f' باشد. چون f چندجمله‌ای مینیمال α است، این حکم برقرار است اگر وفقط اگر $f|f'$. اگر $f' \neq 0$، داریم $\deg f' < \deg f$ ولذا f نمی‌تواند f' را عاد کند. □

نتیجهٔ ۲. هرچندجمله‌ای تجزیه‌ناپذیر f روی یك میدان با مشخصهٔ ۰، جداپذیر است. یك چندجمله‌ای تجزیه‌ناپذیر f روی میدانی مانند k با مشخصهٔ $p > 0$، جداناپذیر است اگر وفقط اگریك چندجمله‌ای چون $g \in k[X]$ وجود داشته باشدکه $f(X) = g(X^p)$.

فرض کنیم f جداناپذیر باشد و $f(X) = \sum_{0 \leqslant i \leqslant n} a_i X^i$. بنابر نتیجهٔ ۱، باید داشته باشیم $\sum_{1 \leqslant i \leqslant n} iaX^{i-1} = 0$. نتیجه می‌شود $ia_i = 0$ که در آن $1 \leqslant i \leqslant n$. درصورتی که k با مشخصهٔ ۰ باشد، مطلب اخیر نتیجه می‌دهد که به‌ازای $i \geqslant 1$، $a_i = 0$. اگر k بامشخصهٔ $p \neq 0$ باشد و اگر $a_i \neq 0$، داریم $p|i$. □

چند تذکر: ۱. فرض کنیم k میدانی با مشخصهٔ ۰ باشد. دراین صورت هر توسیع جبری k، جداپذیر است.

۲. فرض کنیم k میدانی با مشخصهٔ $p \neq 0$ باشد وعضوی مانند α داشته باشدکه چندجمله‌ای $f = X^p - \alpha$ در k ریشه نداشته باشد. در این صورت ادعا می‌کنیم که $X^p - \alpha$ روی k چندجمله‌ای تجزیه‌ناپذیری است که روی k جداناپذیر است. فرض کنیم β_1 و β_2 دو ریشهٔ این چندجمله‌ای (دریك میدان شکافنده) باشند. آنگاه $\alpha = \beta_1^p = \beta_2^p$ و ازآنجا $\beta_1 = \beta_2$. بنابراین کلیهٔ ریشه‌های این چندجمله‌ای با هم مساوی، فرضاً مساوی با β، هستند. فرض کنیم g چندجمله‌ای مینیمال β باشد. اگر h یك عامل تکین تجزیه‌ناپذیر f باشد، داریم $h(\beta) = 0$ و ازآنجا $h = g$. بدین‌ترتیب عددی صحیح مانند i وجود دارد که $f = g^i$. این تساوی ایجاب می‌کند که اگر n مساوی با درجهٔ g باشد، $p = ni$. چون g خطی نیست، $n \neq 1$ پس $i = 1$.

درحالت خاص، فرض کنیم $k(x)$ میدان توابع گویا، با یك متغیر x، روی یك میدان با مشخصهٔ $p \neq 0$ باشد. دراین صورت $X^p - x$ یك چندجمله‌ای تجزیه‌ناپذیر جداناپذیر روی $k(x)$ است. زیرا اگر $X^p - x$ در $k(x)$ ریشه‌ای داشته باشد، چندجمله‌ایهایی چون $g, h \in k[x]$ وجود دارند که $x = (g/h)^p$، یعنی $xh^p = g^p$. اما ازاین رابطه نتیجه می‌شودکه $p \deg h + 1 = p \deg g$، که ممتنع است. بنابراین، توسیعهایی جبری جداناپذیر وجود دارند.

لم. فرض کنیم K/k و L/K توسیعهایی متناهی باشند. فرض کنیم N/k یك توسیع نرمال متناهی k باشدکه L زیرمیدانی از N باشد، فرض کنیم m تعداد k-ایزومورفیسمهای (متمایز) از K به‌توی N باشد و n تعداد K-ایزومورفیسمهای (متمایز) از L به توی N باشد. دراین صورت تعداد k-ایزومورفیسمهای متمایز از L به‌توی N مساوی با mn است.

برهان. فرض کنیم $(\sigma_i)_{1 \leqslant i \leqslant m}$، k-ایزومورفیسمهای متمایز از K به توی N باشند

وفرض کنیم $(\tau_j)_{1\leqslant j\leqslant n}$، K-ایزومورفیسمهای متمایز از L به توی N باشند. به ازای $1\leqslant i\leqslant m$، فرض کنیم $\bar{\sigma}_i$ توسیعی از σ_i به اتومورفیسمی از N باشد؛ (چنین اتومورفیسمی، بنا بر قضیهٔ ۶، وجود دارد). ادعا می کنیم که $\bar{\sigma}_i\circ\tau_j$ها دو به‌دو متمایز هستند. فرض کنیم به‌ازای هر $x\in L$، $\bar{\sigma}_i\circ\tau_j(x)=\bar{\sigma}_r\circ\tau_s(x)$. دراین صورت، به‌ازای هر $x\in K$، داریم $\sigma_i(x)=\sigma_r(x)$ که نتیجه می‌دهد $i=r$. بنابراین به ازای هر $x\in L$، داریم $\tau_j(x)=\tau_s(x)$ که نتیجه می‌دهد $j=s$. فرض کنیم θ، k-ایزومورفیسم دلخواهی از L به‌توی N باشد. آشکارا به‌ازای اندیسی چون i، $\theta|K=\sigma_i$. درنتیجه $((\bar{\sigma}_i)^{-1}\circ\theta)|K$ عضو همانی است و از آنجا به ازای اندیسی چون j، $(\bar{\sigma}_i)^{-1}\circ\theta=\tau_j$. بنابراین $\theta=\bar{\sigma}_i\circ\tau_j$. □

قضیهٔ ۱۱. فرض کنیم K/k یك توسیع از درجهٔ n باشد ویك توسیع نرمال متناهی N/k چنان باشد که K زیرمیدانی از N باشد. دراین صورت حداکثر n تا k-ایزومورفیسم از K به‌توی N وجود دارد.

برهان. قضیه را به‌استقرا بر $[K:k]$ ثابت می‌کنیم. اگر $[K:k]=1$ چیزی برای اثبات باقی نمی‌ماند. فرض کنیم $[K:k]>1$. عضوی مانند $\alpha\in K$ انتخاب می‌کنیم که $\alpha\notin k$. آنگاه $[K:k(\alpha)]<[K:k]$. بنا براین، بنا بر فرض استقرا، تعداد $k(\alpha)$-ایزومورفیسمهای از K به توی N حداکثر $[K:k(\alpha)]$ است. ازسوی دیگر، به‌ازای هر $\alpha\in K$، تعداد مزدوجهای (متمایز) α حداکثر مساوی با درجهٔ چندجمله‌ای مینیمال α است. از آنجایی که هر k-ایزومورفیسمی از $k(\alpha)$ به‌توی N، α را به‌مزدوجی از α می برد وچون به‌ازای هر مزدوجی مانند $\beta\in N$، k-ایزومورفیسم منحصربه‌فردی از $k(\alpha)$ به‌توی N وجود داردکه α را بر β می‌نگارد، نتیجه می‌شودکه تعداد k-ایزومورفیسمهای متمایز از $k(\alpha)$ به‌توی N حداکثر $[k(\alpha):k]$ است. اینك‌قضیه از لم فوق حاصل می‌شود. □

قضیهٔ ۱۲. یك توسیع متناهی از درجهٔ n، K/k، جداپذیر است اگر و فقط اگر به‌ازای هرتوسیع نرمال متناهی N/k که K زیرمیدانی از N باشد، n تا k-ایزومورفیسم متمایز از K به‌توی N وجود داشته باشد.

برهان. فرض کنیم K/k جداپذیر باشد. فرض کنیم K زیرمیدانی از یك توسیع نرمال متناهی N از k باشد. حکم را به‌استقرا بر n ثابت می‌کنیم. اگر $n=1$، چیزی برای اثبات باقی نمی‌ماند. فرض کنیم $n>1$. عضوی مانند $\alpha\in K$ انتخاب می‌کنیم که $\alpha\notin k$. در این صورت $[K:k(\alpha)]<n$ و چون $K/k(\alpha)$ جداپذیر است، تعداد $k(\alpha)$-ایزومورفیسمهای متمایز از K به‌توی N دقیقاً $[K:k(\alpha)]$ است. ازسوی دیگر، چون α جداپذیر است، تمام ریشه‌های چندجمله‌ای مینیمال آن ساده هستند و از آنجا تعداد k-ایزومورفیسمهای متمایز از $k(\alpha)$ به‌توی N، $[k(\alpha):k]$ است. اکنون لم فوق، حکم را ثابت می‌کند.

به‌عکس، فرض‌کنیم K/k دارای n ایزومورفیسم متمایز به‌توی یك توسیع نرمال متناهی N/k که K را به‌عنوان یك زیرمیدان دربر دارد باشد. فرض‌کنیم $\alpha \in K$. بنابر قضیهٔ ۱۱، تعداد $k(\alpha)$-ایزومورفیسمهای متمایز از K به توی N حداکثر $[K:k(\alpha)]$ است. چون $n=[K:k(\alpha)][k(\alpha):k]$، پس تعداد k-ایزومورفیسمهای متمایز از $k(\alpha)$ به‌توی N مساوی $[k(\alpha):k]$ است، یعنی تمام مزدوجهای α متمایز هستند. بنابراین α جداپذیر است. □

نتیجهٔ ۱. اگر K/k یك توسیع جداپذیر متناهی باشد و L/K نیز یك توسیع جداپذیر متناهی باشد، آنگاه L/k جداپذیر است.

برهان. به‌استناد لم فوق، نتیجه می‌گیریم که تعداد k-ایزومورفیسمهای متمایز از L به‌توی هر توسیع نرمالی مانند N/k که L زیرمیدانی از آن باشد، مساوی $[L:K][K:k]=[L:k]$ است. بنابراین L/k جداپذیر است. □

نتیجهٔ ۲. اگر $\alpha_1, \ldots, \alpha_n \in K$ روی k جداپذیر باشند، آنگاه $k(\alpha_1, \ldots, \alpha_n)/k$ جداپذیر است.

۴. میدان متناهی

فرض‌کنیم F یك میدان متناهی با مشخصهٔ $p \neq 0$ باشد. دراین صورت می‌دانیم که $F/(\mathbf{Z}/(p))$ یك توسیع متناهی است. فرض‌کنیم $[F:\mathbf{Z}/(p)]=n$. فرض‌کنیم $\alpha_1, \ldots, \alpha_n \in F$ مبنایی برای F روی $\mathbf{Z}/(p)$ تشکیل دهند. دراین صورت هرعضو F رامی‌توان به‌طور منحصر به‌فرد به‌صورت $\sum_{1 \leqslant i \leqslant n} a_i\alpha_i$ که درآن $a_i \in \mathbf{Z}/(p)$ نوشت. چون $\mathbf{Z}/(p)$ دارای p عضو است، نتیجه می‌گیریم که F دارای p^n عضو است. اینك $F^* = F - \{0\}$ یك گروه از مرتبهٔ $p^n - 1$ است و درنتیجه هر عضو ناصفر F یك ریشهٔ چندجمله‌ای $X^{p^n-1} - 1$ است. بنابراین هر عضو F در چندجمله‌ای $X^{p^n} - X \in \mathbf{Z}/(p)[X]$ صدق می‌کند. چون F دارای p^n عضو است، نتیجه می‌شود که F میدان شکافندهٔ چندجمله‌ای $X^{p^n} - X$ روی $\mathbf{Z}/(p)$ است. ازآنجایی که تمام ریشه‌های این چندجمله‌ای متمایزند، نتیجه می‌گیریم که F یك توسیع جداپذیر $\mathbf{Z}/(p)$ است. با توجه به یکتایی میدانهای شکافنده، در می‌یابیم که هر دومیدان متناهی با تعداد اعضای متساوی، ایزومورف هستند. همچنین واضح است که هر توسیع جبری یك میدان متناهی، جداپذیر است.

قضیهٔ ۱۳. به‌ازای هرمیدان متناهی F، $F^* = F - \{0\}$ یك گروه دوری است.

برهان. فرض‌کنیم α یك عضو ازمرتبهٔ ماکسیمم، فرضاً n، از F^* باشد. دراین‌صورت، به‌ازای هر $\beta \in F^*$، $\beta^n = 1$ (قضیهٔ ۴، فصل ۱). ازآنجایی که چندجمله‌ای $X^n - 1$ حداکثر n ریشه دارد، نتیجه می‌گیریم که مرتبهٔ F^* حداکثر n است. ازطرف دیگر $1, \alpha, \ldots, \alpha^{n-1} \in F^*$. بنابراین F^* توسط α پدید می‌آید. □

تذکر: فرض کنیم F یك میدان متناهی با اعضای $a_n, \dots, a_\circ = 1$ باشد. در این صورت چندجمله‌ای $f(X) = a_\circ + \prod_{\circ \leqslant i \leqslant n} (X - a_i)$ در F ریشه ندارد. پس یك میدان متناهی جبراً بسته نیست.

۵. ساده بودن توسیعهای جداپذیر متناهی

قضیهٔ اصلی. فرض کنیم K/k یك توسیع جداپذیر متناهی باشد. دراین صورت عضوی مانند $\alpha \in K$ وجود دارد که $K = k(\alpha)$ (یعنی، هرتوسیع جداپذیر متناهی، توسیعی ساده است).

برهان. حالت (۱). k یك میدان متناهی است. در این صورت K که توسیعی متناهی ازمیدانی متناهی است، خود میدانی متناهی است. درنتیجه K^*، بنا برقضیهٔ ۱۳، گروهی دوری است. فرض کنیم α یك مولد باشد، دراین صورت داریم $K = k(\alpha)$.

حالت (۲). k یك میدان نامتناهی است. فرض کنیم $n = [K : k]$. فرض کنیم N/k یك توسیع نرمال متناهی شامل K به‌عنوان یك زیرمیدان باشد. چون K/k جداپذیر است، بنا برقضیه ۱۲، نتیجه می‌شود که n تا k-ایزومورفیسم متمایز $\sigma_n, \dots, \sigma_1$ از K به‌توی N وجود دارند. به‌ازای هر $i \neq j$، فرض می‌کنیم $V_{ij} = \{x \in K \mid \sigma_i(x) = \sigma_j(x)\}$. دراین صورت، آشکارا V_{ij} زیرفضایی از فضای برداری K روی k است. از آنجایی که بنا بر فرض به‌ازای $i \neq j$، $\sigma_i \neq \sigma_j$، پس V_{ij} زیرفضای سرهٔ K است. بنا بر قضیهٔ ۱۵، فصل ۲، $\bigcup_{i \neq j} V_{ij}$ یك زیرمجموعهٔ سرهٔ K است. پس، عضوی چون $\alpha \in K$ وجود دارد که به‌ازای هر $i \neq j$، $\sigma_i(\alpha) \neq \sigma_j(\alpha)$. لذا α دارای n مزدوج متمایز است، و داریم $n = [k(\alpha) : k]$. بنا براین $K = k(\alpha)$. □

فصل ٤

قضیهٔ بنیادی نظریهٔ گالوا

فرض کنیم K یك میدان باشد. اگر σ_1 و σ_2 دو اتومورفیسم K باشند، نگاشت $\sigma_1 \circ \sigma_2 : K \to K$ که با رابطهٔ $(\sigma_1 \circ \sigma_2)(x) = \sigma_1(\sigma_2(x))$، $x \in K$، تعریف می‌شود مجدداً اتومورفیسمی از K است. بنابراین اگر A مجموعهٔ تمام اتومورفیسمهای K باشد، به سهولت ثابت می‌شود که A تحت عمل گروهی $\phi : A \times A \to A$ که به صورت $\phi(\sigma_1, \sigma_2) = \sigma_1\sigma_2 = \sigma_1 \circ \sigma_2$ تعریف می‌شود یك گروه است. اگر G زیرگروهی از A باشد، G را یك گروه از اتومورفیسمهای K می‌نامیم. فرض کنیم k زیرمیدانی از K باشد. دراین صورت زیرمجموعهٔ متشکل از تمام اعضای A را که k-اتومورفیسمی از K باشند با $G(K/k)$ نمایش می‌دهیم؛ به عبارت دیگر، عضوی چون σ از A به $G(K/k)$ تعلق دارد اگر وفقط اگر به ازای هر $x \in k$، $\sigma(x) = x$. ملاحظه می‌کنیم که $G(K/k)$ زیرگروهی از A است.

یك توسیع K/k از میدانها را یك توسیع گالوایی نامند اگر متناهی، نرمال و جداپذیر باشد. دراین صورت گروه $G(K/k)$ از k-اتومورفیسمهای K را **گروه گالوایی K روی k** می‌نامند.

اگر G گروهی‌از اتومورفیسمهای میدانی مانند K باشد، آنگاه مجموعهٔ k متشکل از اعضایی چون $x \in K$ که به ازای هر $\sigma \in G$، $\sigma(x) = x$، زیرمیدانی از K است و **میدان ثابت G** نام دارد.

فرض کنیم G گروهی از اتومورفیسمهای میدانی مانند K باشد و $f = \sum_{i=0}^{n} a_i X^i$

یك چندجملــه‌ای روی K باشد. دراین صورت اگر $\sigma \in G$، چندجملــه‌ای $\sigma(f)$ را بــا $\sigma(f) = \sum_{i=0}^{n} \sigma(a_i) X^i$ تعریف می کنیم. اگر به‌ازای هر $\sigma \in G$، f = $\sigma(f)$، ضرایب a_i به‌میدان ثابت k از G تعلق دارند.

قضیهٔ ۱. فرض‌کنیم K/k یك توسیع گالوایی باشد. دراین صورت $G(K/k)$ یك گروه متناهی از مرتبهٔ $[K : k]$ است و k برمیدان ثابت $G(K/k)$ منطبق است.

برهان. این مطلب یك نتیجهٔ آنی ازنتایجی است‌کــه درفصل قبل به‌دست آمد. از قضایای ۷ و ۱۲ ازفصل ۳ نتیجه می‌شودکه $G(K/k)$ متناهی است ومــرتبهٔ G مساوی با $[K : k]$ است. برای اثبات اینکه k برمیدان ثابت $G(K/k)$ منطبق است، می‌توان فرض کرد کــه $K \neq k$. حال اگر α عضوی از K باشدکــه متعلق به k نباشد، عضوی مانند $\beta \in K$، $\beta \neq \alpha$، وجود داردکه α و β روی k مزدوج هستند، زیراکــه K/k نرمال و جداپذیر است (بخش۲ و بخش ۳ ازفصل۳). اینك $k(\alpha)$ و $k(\beta)$، k-ایزومورف هستند وچون این ایزومورفیسم‌را می‌توان به k-اتومورفیسمی‌از K توسعه داد (قضیهٔ۶، فصل۳)، عضوی مانند $\sigma \in G(K/k)$ وجود داردکه $\sigma(\alpha) = \beta$. این مطلب نشان می‌دهدکه میدان ثابت $G(K/k)$ همان k است. □

قضیهٔ اصلی زیر، به‌مفهومی، عکس قضیهٔ ۱ است.

قضیهٔ اصلی ۱. فرض کنیم H گروهی متناهی از اتومورفیسمهای میدانــی مانند K باشد. دراین صورت اگر k میدان ثابت H باشد، آنگاه K/k یك توسیع گالوایی است و $H = G(K/k)$.

برهان. فرض‌کنیم $\sigma_1, \ldots, \sigma_n$ اعضای متمایز H باشند. فرض کنیم α عضوی‌از K باشد و $\beta_1, \ldots, \beta_m$ اعضای متمایز دربین $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ باشند. حال اگر σ عضوی‌از H باشد، آنگاه $\sigma(\beta_1), \ldots, \sigma(\beta_m)$ بازهم متمایزند، زیرا σ یك‌اتومورفیسم است. به علاوه، چون $\sigma\sigma_1, \ldots, \sigma\sigma_n$ جایگشتی از $\sigma_1, \ldots, \sigma_n$ است نتیجه مــی‌شود $\sigma(\beta_1), \ldots, \sigma(\beta_m)$ جایگشتی از $\beta_1, \ldots, \beta_m$ است. چندجمله‌ای $f \in K[X]$ را که با $f = \prod_{i=1}^{m} (X - \beta_i)$ تعریف می‌شود در نظر می گیریــم. به ازای هر $\sigma \in H$، داریــم $\sigma(f) = \prod_{i=1}^{m}(X - \sigma(\beta_i)) = \prod_{i=1}^{m} (X - \beta_i) = f$. در نتیجه f یك چندجمله‌ای روی k است. تمام‌ریشه‌های f در K هستند و متمایزند، پس f روی k یك چندجمله‌ای جداپذیر است. بــه‌علاوه، f روی k تجزیه ناپذیر است. در واقع، اگر g چندجمله‌ای مینیمال α روی k باشد، داریم $\sigma_i(g(\alpha)) = 0$ = $g(\sigma_i(\alpha))$. پس $\deg g \geqslant \deg f$. ازآنجایــی که $g|f$، داریــم $g = f$. چون $f(\alpha) = 0$، α روی k جبری و جــداپــذیر است و $[k(\alpha) : k] \leqslant n$ که در آن n مرتبهٔ H است. بدین ترتیب، K/k توسیعی جداپذیر و جبری است.

فرض کنیم N/k توسیعی متناهی و N زیرمیدانی از K باشد. دراین صورت چون N/k جداپذیر است، به ازای عضوی چون $\beta \in K$، $N=k(\beta)$ (قضیهٔ اصلی، بخش ۵، فصل ۳). بنابراین، داریم $[N:k] \leqslant n$. اکنون N را چنان انتخاب می کنیم که N/k متناهی باشد و $[N:k]$، درمیان تمام زیرمیدانهای از K که توسیع متناهی k باشند، ماکسیمم باشد. داریم $N=k(\alpha)$. حال فرض کنیم θ عضوی دلخواه از K باشد. فرض کنیم M زیرمیدان K، پدید آمده توسط N و θ باشد. دراین صورت M/k متناهی است (نتیجهٔ ۱، قضیهٔ ۳، فصل ۳) ودر نتیجه، نظر به انتخاب N، داریم $[M:k] \leqslant [N:k]$. اما M شامل N است، پس $[M:k]=[N:k][M:N]$ (قضیهٔ ۳، فصل ۳). نتیجه اینکه $[M:N]=1$ ولذا $M=N$. بنابراین، هرعضو K به N تعلق دارد، یعنی $K=N$. بدین ترتیب، ثابت کردیم که K/k یك توسیع جداپذیر متناهی است. اینك $K=k(\alpha)$ و چون $\sigma_1, \ldots, \sigma_n$ k-اتومورفیسمهای متمایز K هستند، $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ متمایزند. بنابراین چندجمله‌ای $f=\prod_{i=1}^{n}(X-\sigma_i(\alpha))$ روی k از درجهٔ n، و همان چندجمله‌ای مینیمال α روی k است و K آشکارا میدان شکافندهٔ f است. بدین ترتیب، داریم $H \subset G(K/k)$ ومرتبهٔ $G(K/k)$ مساوی با n است (قضیهٔ ۱۱، فصل ۳) پس $H=G(K/k)$. این مطلب برهان قضیهٔ اصلی را پایان می‌دهد. □

فرض کنیم K/k توسیعی گالوایی باشد. فرض کنیم $S(K/k)$ مجموعهٔ تمام زیرمیدانهای از K و شامل k را نمایش دهد و $S(G)$ مجموعهٔ تمام زیرگروههای از $G=G(K/k)$ را. نگاشتهای

$$\Phi : S(K/k) \rightarrow S(G)$$

$$\Psi : S(G) \rightarrow S(K/k)$$

را به‌صورت ذیل تعریف می کنیم: اگر K_1 عضوی از $S(K/k)$، یعنی زیرمیدانی از K وشامل k باشد، K/K_1 نیز توسیعی گالوایی است (متناهی بودن وجداپذیربودن K/K_1 آشکار است؛ برای نشان دادن نرمال بودن K/K_1، می‌توان از این واقعیت بهره گرفت که K میدان شکافندهٔ یك چند جمله‌ای مانند f روی k است ودر نتیجه K میدان شکافندهٔ f روی K_1 هم هست، لذا نرمال بودن K/K_1 حاصل می‌شود). اکنون قرار می‌دهیم: $\Phi(K_1)=G(K/K_1)$. اگر H زیرگروهی از G باشد، $\Psi(H)$ را میدان ثابت H می گیریم.

قضیهٔ اصلی ۲ (قضیهٔ بنیادی نظریهٔ گالوا). نگاشتهای $\Phi \circ \Psi : S(G) \rightarrow S(G)$ و $\Psi \circ \Phi : S(K/k) \rightarrow S(K/k)$ نگاشتهای همانی هستند.

برهان. همانی بودن نگاشت $\Psi \circ \Phi : S(K/k) \rightarrow S(K/k)$ معادل است با این حکم که اگر K_1/k توسیعی باشد که K_1 زیرمیدانی از K باشد، آنگاه K_1 میدان ثابت $G(K/K_1)$ است. این مطلب از قضیهٔ ۱ نتیجه می شود. همانی بودن $\Phi \circ \Psi : S(G) \rightarrow S(G)$

معادل است با این حکم که اگر H زیرگروهی از G و K_1 میدان ثابت H باشد، آنگاه $H=G(K/K_1)$. این مطلب از قضیهٔ اصلی ۱ نتیجه می‌شود.

نتیجه. فرض کنیم K_1/k توسیعی باشد که K_1 زیرمیدانی از K باشد. در این صورت K_1/k یك توسیع گالوایی است اگر و فقط اگر $G(K/K_1)$ یك زیرگروه نرمال $G(K/k)$ باشدکه دراین صورت یك ایزومورفیسم طبیعی از $G(K_1/k)$ به‌روی گروه خارج‌قسمت $G(K/k)/G(K/K_1)$ وجود دارد.

برهان. اگر σ عضوی از $G(K/k)$ باشد، آنگاه $\sigma(K_1)$ نیز زیرمیدانی از K و شامل k است و به‌سهولت ثابت می‌شود که $G(K/\sigma(K_1))$همان زیرگروه $\sigma G(K/K_1)\sigma^{-1}$ از $G(K/k)$ است. اینك K_1/k نرمال است اگر وفقط اگر به‌ازای هر $\sigma\in G(K/k)$، $\sigma(K_1)=K_1$ (این مطلب از قضیهٔ ۷، فصل ۳ حاصل می‌شود). حال اگر $\sigma(K_1)=K_1$، آنگاه به ازای هر $\sigma\in G(K/k)$، $\sigma G(K/K_1)\sigma^{-1}=G(K/K_1)$ که نشان می‌دهد $G(K/K_1)$ یك‌زیرگروه نرمال $G(K/k)$ است. به‌عکس، اگر به‌ازای هر $\sigma\in G(K/k)$، $\sigma G(K/K_1)\sigma^{-1}=G(K/K_1)$، آنگاه، به‌ازای هر $\sigma\in G(K/K_1)$، میدان ثابت $G(K/K_1)$ با میدان ثابت $\sigma G(K/K_1)\sigma^{-1}$ یکی است. بنابرقضیهٔ ۱، میدان ثابت $G(K/K_1)$ مساوی با K_1 است ومیدان ثابت $\sigma G(K/K_1)\sigma^{-1}$ مساوی با $\sigma(K_1)$ است. درنتیجه، به‌ازای هر $\sigma\in G(K/k)$، $K_1=\sigma(K_1)$ که‌نشان می‌دهد K_1 نرمال‌است. این، برهان قسمت اول نتیجه راکامل می‌کند.[1]

حالا، فرض کنیم K_1 یك توسیع k باشد، $K\supset K_1\supset k$، و K_1/k نرمال باشد قبلاً دیده‌ایم که اگر $\sigma\in G(K/k)$، داریم $\sigma(K_1)=K_1$. لذا نگاشتی مانند $f:G(K/k)\to G(K_1/k)$ به‌دست می‌آوریم؛ وآن اینکه، اگر σ عضوی‌از $G(K/k)$ باشد، $f(\sigma)$ تحدید σ به K_1 است. به‌آسانی ثابت می‌شودکه f همومورفیسمی گروهی است. به‌علاوه f به‌روست؛ زیرا هر kـاتومورفیسم از K_1 را می‌توان به kـاتومورفیسمی از K توسعه داد (قضیهٔ ۶، فصل ۳). هستهٔ f دقیقاً مساوی با $G(K/K_1)$ است، پس $G(K/k)/G(K/K_1)$ به‌طور طبیعی با $G(K_1/k)$ ایزومورف است. و این همان است که می‌خواستیم. □

فرض‌کنیم K_1/k و K_2/k دو توسیع از میدانی چون k باشندکه K_1 و K_2 نیز زیرمیدانی از یك توسیع مانند N از k باشند. زیرمیدان پدید آمده توسط K_1 و K_2 از N را با K_1K_2 نمایش می‌دهیم (توسیع K_1K_2/k را غالباً ترکیبی از K_1/k و K_2/k روی k می‌نامند). توجه می‌کنیم که $K_1K_2\supset K_1$ و $K_1K_2\supset K_2$.

قضیهٔ ۲. فرض کنیم K_1/k توسیعی گالوایی باشد. دراین صورت K_1K_2/K_2 نیز یك توسیع گالوایی است. به‌علاوه، یك همومورفیسم طبیعی مانند

---

[1] توجه‌کنیدکه چون K/k توسیعی‌گالوایی است (گرچه درمتن تصریح نشده) پس K/k جداپذیر است ولذا K_1/k نیز جداپذیر است.ـم.

$$f:G(K_۱K_۲/K_۲)\to G(K_۱/k)$$

وجود داردکه هسته‌اش عضو همانی است؛ به‌عبارت دیگر، $G(K_۱K_۲/K_۲)$ را می‌توان با زیرگروهی از $G(K_۱/k)$ یکی گرفت .

برهان. میدان $K_۱$ میدان شکافندهٔ یك چندجمله‌ای جداپذیر مانند h روی k است. از آنجایی که $K_۲$ شامل k است، h را می‌توان به عنوان یك چندجمله‌ای روی $K_۲$ هم درنظر گرفت و دراین صورت ملاحظه می‌کنیم که $K_۱K_۲$ میدان شکافندهٔ چندجمله‌ای h روی $K_۲$ است. ازاینجا نتیجه می‌شودکه $K_۱K_۲/K_۲$ یك توسیع گالوایی است.

فرض کنیم σ عضوی از $G(K_۱K_۲/K_۲)$ باشد. چون، به‌ازای هر $x\in K_۲$، $x=\sigma(x)$، پس به‌ازای هر $x\in k$، $\sigma(x)=x$. به‌علاوه، چون $K_۱/k$ یك توسیع نرمال است پس $\sigma(K_۱)=K_۱$. بدین‌ترتیب، نگاشتی مانند $f:G(K_۱K_۲/K_۲)\to G(K_۱/k)$ به‌دست می‌آوریم که اگر $\sigma\in G(K_۱K_۲/K_۲)$، $f(\sigma)$ تحدید σ به $K_۱$ است. به‌علاوه‌اگر σ عضو همانی نباشد، $f(\sigma)$ عضو همانی $K_۱/k$ نیست، زیرا در غیر این صورت σ باید اتومورفیسم همانی برای $K_۱K_۲$ باشد چراکه $K_۱K_۲$ توسط $K_۱$ و $K_۲$ پدید می‌آید. این مطلب برهان قضیه را کامل می‌کند. □

تذکر : درحالت‌کلی، f لازم نیست به‌رو باشد؛ مثلاً، در حالتی‌که $K_۲=K_۱$، داریم $K_۱K_۲=K_۲$. در این‌صورت $G(K_۱K_۲/K_۲)$ تنها یك عضو دارد و $K_۱/k$ را می‌توان چنان اختیارکردکه $G(K_۱/k)$ بیش‌از یك عضو داشته باشد .

قضیهٔ اصلی ۳. فرض کنیم k یك میدان متناهی متشکل از q عضو باشد و K یك توسیع متناهی k باشد. دراین صورت K/k یك توسیع گالوایی است و گروه گالوایی $G(K/k)$ دوری‌است. **اگر $\sigma:K\to K$ نگاشتی باشدکه توسط $\sigma(a)=a^q$ تعریف شود،** آنگاه σ یك kـاتومورفیسم است و نیز یك مولد برای $G(K/k)$ است.

برهان. فرض‌کنیم p مشخصهٔ k باشد و $\mathbf{Z}/(p)$ میدان اول بامشخصهٔ p باشد. داریم $K\supset k\supset \mathbf{Z}/(p)$. قبلاً دیده‌ایم که $K/\mathbf{Z}/(p)$ توسیعی گالوایی است (بخش۴، فصل ۳). در این صورت K/k نیز یك توسیع گالوایی است. نگاشت $\sigma:K\to K$ را که باضابطهٔ $\sigma(a)=a^q$ تعریف می‌شود، در نظر می‌گیریم. اگر $a\in k$، $\sigma(a)=a$ زیرا که‌گروه ضربی k^* از مرتبهٔ $(q-۱)$ است، وبه‌ازای هر $a\in k^*$، $a^{q-۱}=۱$ که ازآن $a^q=a$ نتیجه می‌شود. اگر a عضو صفر باشد، بازهم $a^q=a$. به‌سهولت ثابت می‌شودکه σ اتومورفیسمی‌از K است. فرض‌کنیم $m=[K:k]$. گروه $G(K/k)$ از مرتبهٔ m است واگر ثابت‌کنیم که عضو σ از مرتبهٔ m است، نتیجه می‌شود که $G(K/k)$ دوری است و σ یك مولد $G(K/k)$ است. باتوجه به‌اینکه گروه ضربی K^* دوری است (قضیهٔ ۱۳، فصل ۳)، فرض می‌کنیم α یك مولد K^* باشد. بنابراین مرتبهٔ α مساوی با $q^m-۱$ است. داریم $\sigma(\alpha)=\alpha^q$. فرض کنیم که σ به‌عنوان عضوی از $G(K/k)$ ازمرتبهٔ s باشد، یعنی $\alpha^{q^s}=\alpha$ و s کوچکترین عدد صحیح مثبت واجد این ویژگی باشد. نتیجه می‌گیریم که $s=m$ واز آنجا قضیهٔ اصلی ثابت می‌شود. □

فصل ۵

کاربردهای نظریهٔ گالوا

نمادگذاری. فرض کنیم K میدانی با مشخصهٔ p و m عدد صحیح مثبتی باشد. در صورتی که یکی از شرایط زیر برقرار باشد، می‌نویسیم $[m, p]=1$:

(۱) $p=0$ و m دلخواه باشد،

(۲) $p>0$ و m و p متباین باشند.

۱. توسیع دوری

فرض کنیم K میدانی با مشخصهٔ p و m عدد صحیح مثبتی باشد که $[m, p]=1$.

چند جمله‌ای $f=X^m-1$ در $K[X]$ را در نظر می‌گیریم. اگر ρ ریشه‌ای از f باشد، آنگاه $f'(\rho)=m\rho^{m-1}\neq 0$ و لذا تمام ریشه‌های f متمایزند (قضیهٔ ۱۰، فصل ۳). فرض کنیم $\rho_1, \dots, \rho_m$ ریشه‌های f باشند. $\rho_1, \dots, \rho_m$ را ریشه‌های mم واحد می‌نامند. این ریشه‌ها تحت عمل ضرب گروهی آبلی تشکیل می‌دهند. فرض کنیم t توان این گروه آبلی باشد. در این صورت، به‌ازای $1\leqslant i\leqslant m$، $\rho_i^t=1$ (قضیهٔ ۴، فصل ۱). از آنجایی که X^t-1 در میدان شکافنده‌اش بر K فقط t ریشه دارد، ملاحظه می‌کنیم که $t=m$. این بدین معناست که ρ_iها $(1\leqslant i\leqslant m)$ یک گروه دوری از مرتبهٔ m تشکیل می‌دهند. هر مولد این گروه را یک ریشهٔ mم اولیهٔ واحد می‌نامند. اگر ρ یک ریشهٔ mم اولیهٔ واحد باشد، داریم

$$f = X^m - 1 = \prod_{0 \leqslant i \leqslant m-1} (X - \rho^i),$$

ومیدان $L = K(\rho)$، به‌وضوح، میدان شکافندهٔ f بر K است. توسیع L/K جداپذیر است زیرا کلیهٔ ریشه‌های f متمایزند. بنابراین، L/K یك توسیع گالوایی است.

فرض کنیم G گروه گالوایی L/K باشد و $\sigma \in G$. اگر ρ یك ریشهٔ mم اولیهٔ واحد باشد، $\sigma(\rho)$ نیز چنین است و از آنجا داریم $\sigma(\rho) = \rho^v$ که در آن $(v, m) = 1$ وعدد صحیح v به‌هنگ m به‌طور یکتا تعیین می‌شود. فرض کنیم R_m گروه ضربی رده‌های مانده‌ای به‌هنگ m را نشان دهد که با m متباین هستند. به‌آسانی ثابت می‌شود که نگاشت $\sigma \to \bar{v}$ که در آن $\bar{v}$ ردهٔ مانده‌ای حاوی v به‌هنگ m است، همومورفیسمی مانند ϕ از G به‌توی R_m تعریف می کند. اگرعضوی چون $\sigma \in G$ چنان باشد که $\sigma(\rho) = \rho$، آنگاه، به‌ازای هر i، $0 \leqslant i \leqslant m-1$، داریم $\sigma(\rho^i) = \rho^i$ و در نتیجه σ عضو همانی e برای G است. بنابراین $\ker \phi = (e)$، یعنی G با زیرگروهی از R_m ایزومورف است. بدین ترتیب قضیهٔ ذیل را ثابت کرده‌ایم.

قضیهٔ ۱. فرض کنیم L میدان شکافندهٔ $X^m - 1$ بر K باشد. دراین‌صورت $L = K(\rho)$ که در آن ρ یك ریشهٔ mم اولیهٔ واحد است و L/K یك توسیع گالوایی است که گروه گالواییش با زیرگروهی از R_m ایزومورف است:

توسیعی چون F/E را یك توسیع دوری نامند اگر توسیعی گالوایی باشد وگروه گالواییش هم دوری باشد.

تذکر: فرض کنیم عدد صحیح m مفروض درقضیهٔ ۱ عددی اول باشد. دراین‌صورت R_m دوری است. (قضیهٔ ۱۳، فصل ۳). لذا G دوری است، یعنی L/K توسیعی دوری است.

قضیهٔ ۲. فرض کنیم میدان K حاوی کلیهٔ ریشه‌های mم واحد باشد. فرض کنیم L میدان شکافندهٔ چندجمله‌ای $f = X^m - \omega$، $\omega \in K$، بر K باشد. اگر $\alpha \in L$ ریشه‌ای از f باشد، آنگاه $L = K(\alpha)$ و L/K یك توسیع دوری است. اگر m عددی اول باشد، آنگاه یا $L = K$ یا $[L : K] = m$.

برهان. اگر ρ یك ریشهٔ mم اولیهٔ واحد باشد داریم

$$f = \prod_{0 \leqslant i \leqslant m-1} (X - \alpha \rho^i)$$

نتیجه اینکه $L = K(\alpha)$. چون $[m, p] = 1$، f بر K جداپذیر و در نتیجه L/K توسیعی گالوایی است.

فرض کنیم G گروه گالوایی L/K باشد. به‌ازای هر $\sigma \in G$، داریم $\sigma(\alpha) = \alpha \rho^i$ که در آن i عدد صحیحی است که به هنگ m به‌طور یکتا تعیین می‌شود. به‌سهولت ثابت می‌شود که نگاشت $\sigma \to i \pmod m$ همومورفیسمی مانند ϕ از G به توی $\mathbf{Z}/(m)$

تعریف می‌کنند و $\ker\phi=(e)$. بنابراین G با زیرگروهی از گروه دوری $\mathbf{Z}/(m)$ ایزومورف است و درنتیجه G دوری است. اگر m عددی اول باشد، $\mathbf{Z}/(m)$ زیرگروهی غیر از $(\circ)$ و $\mathbf{Z}/(m)$ ندارد، پس $G=(e)$ یا $G\approx\mathbf{Z}/(m)$. ازاینجا نتیجه می‌شود که یا $L=K$ یا $[L:K]=m$ (قضیهٔ ۱، فصل ۴). □

قضیهٔ ۳. فرض‌کنیم m عددی اول باشد و K حاوی تمام ریشه‌های mم واحد باشد. فرض‌کنیم L/K یك توسیع دوری باشدکه $[L:K]=m$. در این صورت عضوی مانند $\omega\in K$ وجود دارد که L میدان شکافندهٔ $X^m-\omega$ بر K است.

جهت اثبات این قضیه به‌لم زیر نیاز داریم

لم. فرض‌کنیم ρ یك ریشهٔ mم اولیهٔ واحد باشد و m عددی اول. در این‌صورت، اگر a عددی صحیح باشد، داریم

$$\sum_{\circ\leqslant i\leqslant m-1}\rho^{ia}=\begin{cases}\circ & \text{اگر } m\nmid a،\\ m & \text{اگر } m\mid a،\end{cases}$$

برهان‌لم. اگر $m|a$، به‌ازای هر عددصحیح i، $\rho^{ia}=1$. دراین‌صورت $\sum_{\circ\leqslant i\leqslant m-1}\rho^{ia}=m$.
اگر $m\nmid a$، $\theta=\rho^a$ هم یك ریشهٔ mم اولیهٔ واحد است زیراکه m عددی اول است. بنابراین مقدار $\sum_{\circ\leqslant i\leqslant m-1}\theta^i=\sum_{\circ\leqslant i\leqslant m-1}\rho^{ia}$ مساوی با حاصلجمع ریشه‌های چندجمله‌ای X^m-1 است. پس $\sum_{\circ\leqslant i\leqslant m-1}\rho^{ia}=\circ$. □

برهان قضیهٔ ۳. از آنجایی که L/K جداپذیر است، به‌ازای عضوی چون $\beta\in L$، $L=K(\beta)$ (قضیهٔ اصلی بخش ۵، فصل ۳). فرض کنیم f چندجمله‌ای مینیمال β روی K باشد. L/K نرمال است، f روی L به‌عوامل خطی تجزیه می‌شود؛ پس فرض می‌کنیم $f=(X-\beta_1)\dots(X-\beta_m)$، $\beta=\beta_1$. فرض کنیم σ مولدی برای گروه گالوایی L/K باشد. بدون اینکه خللی به‌کلیت برهان وارد شود، می‌توان فرض کرد که، به‌ازای $1\leqslant i\leqslant m-1$، $\sigma(\beta_i)=\beta_{i+1}$، و همچنین $\sigma(\beta_m)=\beta_1$. فرض کنیم $\alpha_k\in L$ها، $1\leqslant k\leqslant m$، به‌صورت زیر تعریف شوند.[1]

$$\alpha_k=\sum_{\circ\leqslant i\leqslant m-1}\rho^{ki}\beta_{i+1}$$

بنا بر لم فوق، داریم

$$\sum_{1\leqslant k\leqslant m}a_k=\sum_{\circ\leqslant i\leqslant m-1}\beta_{i+1}\Big(\sum_{1\leqslant k\leqslant m}\rho^{ki}\Big)=m\beta_1$$

---

۱. عبارت مذکور برای α_k را بسط لاگرانژ می‌نامند.

به‌علاوه، $\sum_{1\leqslant i\leqslant m} \beta_i = \alpha_m$ و بنابراین به K تعلق دارد. چون $m\beta_1$ در K نیست، نتیجه می‌گیریم که عدد صحیحی چون k، $1 \leqslant k \leqslant m-1$، وجود دارد که $\alpha_k \notin K$. فرض کنید $\alpha = \alpha_k$. حال داریم

$$\begin{aligned}\sigma(\alpha) &= \sum_{0\leqslant i\leqslant m-1} \rho^{ki}\,\sigma(\beta_{i+1}) \\ &= \sum_{0\leqslant i\leqslant m-2} \rho^{ki}\,\beta_{i+2} + \rho^{k(m-1)}\beta_1 \\ &= \rho^{-k} \sum_{0\leqslant i\leqslant m-1} \rho^{ki}\,\beta_{i+1} = \rho^{-k}\alpha,\end{aligned}$$

و درنتیجه $\sigma(\alpha^m) = (\sigma(\alpha))^m = \alpha^m$. از آنجا که σ گروه گالوایی G را پدید می‌آورد، به‌ازای هر $\tau \in G$، $\tau(\alpha^m) = \alpha^m$. پس $\alpha^m = \omega \in K$. چون $[K(\alpha):K]$ عدد m را که عددی اول است عاد می‌کند، $[K(\alpha):K]$ یا ۱ است یا m. با توجه به‌اینکه $\alpha \notin K$، $[K(\alpha):K] = m$ و درنتیجه $L = K(\alpha)$. نتیجه اینکه L میدان شکافندهٔ $X^m - \omega$ بر K است، وبرهان قضیه کامل می‌شود. □

نتیجه. فرض کنید مشخصهٔ K مخالف ۲ باشد و فرض کنید L/K توسیعی باشد که $[L:K] = 2$. آنگاه عضوی مانند $\alpha \in L$ وجود داردکه $\alpha^2 \in K$ و $L = K(\alpha)$.

اثبات واضح است.

تذکر: قضایای ۲ و ۳، درصورت حذف این‌شرط که K حاوی تمام ریشه‌های mم واحد است، بی‌اعتبار می‌گردند.

۲. حلپذیری با رادیکالها

فرض کنیم K میدانی با مشخصهٔ p باشد. توسیعی مانند L/K را یك توسیع رادیکالی ساده نامند اگر در L عضوی چون α وجود داشته باشد که $\omega = \alpha^m \in K$، $[m, p] = 1$ و $L = K(\alpha)$. گاهی می‌نویسیم $\alpha = \omega^{1/m}$ و α را یك رادیکال ساده بر K می‌نامیم. یك توسیع L/K یك توسیع رادیکالی نامیده می‌شود اگر زیرمیدانهایی چون K_i $(1 \leqslant i \leqslant n)$ شامل K وجود داشته باشند که $K_1 = K$، $K_n = L$، $K_{i+1} \supset K_i$، و توسیع K_{i+1}/K_i توسیع رادیکالی ساده‌ای باشد. در این‌صورت هرعضو L را یك رادیکال بر K می‌نامند.

اگر L/K و M/L توسیعهایی رادیکالی باشند، آنگاه M/K نیز توسیعی‌رادیکالی است. متذکر می‌شویم که هرتوسیع رادیکالی ساده، یك توسیع متناهی و جداپذیراست و در نتیجه هر توسیع رادیکالی هم یك توسیع متناهی و جداپذیراست. فرض کنیم L/K یك توسیع رادیکالی باشد، N/L توسیعی دلخواه، و F زیرمیدانی از N شامل K باشد. دراین‌صورت به‌سهولت ملاحظه می‌شود که LF/F توسیعی رادیکالی است که در آن LF

میدان پدید آمده توسط L و F در N است. از این مطلب نتیجه می‌شود که اگر L/K توسیعی دلخواه باشد و L_i $(i=1, 2)$ زیر میدانهایی از L شامل K باشند که L_i/K $(i=1, 2)$ رادیکالی باشند، آنگاه L_1L_2/K توسیعی رادیکالی است، زیرا L_1L_2/L_1 و L_1/K توسیعهایی رادیکالی هستند. حالا اگر L_i $(1 \leqslant i \leqslant l)$ تعداد متناهی از زیرمیدانهای L شامل K باشند که L_i/Kها، به ازای $1 \leqslant i \leqslant l$، رادیکالی باشند، به استقرا بر l آشکار است که $(L_1L_2 \ldots L_l)/K$ نیز توسیعی رادیکالی است.

قضیهٔ ۴. فرض‌کنیم L/K توسیعی رادیکالی باشد. در این صورت توسیعی مانند M/L وجود دارد که M/K یك توسیع رادیکالی گالوایی است.

برهان. آشکارا کافی است ثابت کنیم که یك توسیع رادیکالی گالوایی M/K و K-ایزومورفیسمی از L به‌روی زیرمیدانی از M وجود دارند.

برهان به‌استقرا بر $[L:K]$ است. اگر $[L:K]=1$، چیزی برای اثبات باقی نمی‌ماند. فرض کنیم $[L:K]=n>1$. در این‌صورت یك توسیع رادیکالی مانند L_1/K وجود دارد که $L=L_1(\alpha)$، $\alpha^m=a\in L_1$، $[m, p]=1$ و $L\neq L_1$. از آنجایی که $[L_1:K]<n$، بنا برفرض استقرا، یك توسیع رادیکالی گالوایی مانند M_1/K وجود دارد که L_1 زیرمیدانی از M_1 است. فرض کنیم G گروه گالوایی M_1/K باشد. می‌نویسیم

$$f=\prod_{\sigma\in G}(X^m-\sigma(a))$$

روشن است که $f\in K[X]$. فرض کنیم M میدان شکافندهٔ f بر M_1 باشد. بدیهی است که M/M_1 یك توسیع رادیکالی است[1] و در نتیجه M/K نیز توسیعی رادیکالی است. به‌علاوه، M/K توسیعی گالوایی است، زیرا اگر M_1 میدان شکافندهٔ یك چندجمله‌ای مانند ϕ بر K باشد، آنگاه M میدان شکافندهٔ چندجمله‌ای ϕf بر K است. نگاشت شمول از L_1 به‌توی M_1 را می‌توان به‌ایزومورفیسمی از $L=L_1(\alpha)$ به‌توی زیرمیدانی از M توسعه داد (رجوع کنید به بخش ۲، فصل ۳). این مطلب برهان قضیه را تمام می‌کند. □

قضیهٔ ۵. فرض‌کنیم L/K یك توسیع رادیکالی گالوایی باشد. در این صورت گروه گالوایی L/K حلپذیر است.

برهان. بنا برتعریف توسیع رادیکالی، زیر میدانهایی مانند K_i $(1\leqslant i\leqslant n)$ از L وجود دارند که $K_n=L$، $K_1=K$، $K_{i+1}=K_i(\beta_i)$، $\beta_i^{m_i}=a_i\in K_i$، و $[m_i, p]=1$

---

۱. زیرا اگر میدان شکافندهٔ $X^m-\sigma(a)$ را روی M_1 به M^σ نمایش دهیم، آنگاه داریم $M^\sigma=M_1(u, \rho)$ که در آن u یك ریشهٔ $X^m-\sigma(a)$ است و ρ یك ریشهٔ mام اولیهٔ واحد است. چون $M_1(\rho)/M_1$ و $M_1(\rho, u)/M_1(\rho)$ رادیکالی ساده هستند پس M^σ/M_1 رادیکالی است. بنابراین $M=\prod_{\sigma\in C}M^\sigma$ (میدان شکافندهٔ f بر M_1) که $\prod_{\sigma\in G}M^\sigma$ میدان پدید آمده توسط M^σ، $\sigma\in G$، است روی M_1 رادیکالی است.ـم.

$(1 \leqslant i \leqslant n-1)$. فرض کنیم $m = \prod_{1\leqslant i \leqslant n-1} m_i$. آشکارا $[m, p]=1$. فرض کنیم L میدان شکافندهٔ یك چندجمله‌ای مانند $f \in K[X]$ بر K باشد. اگر M میدان شکافندهٔ چندجمله‌ای $f(X^m-1)=\phi$ بر L باشد، آنگاه M میدان شکافندهٔ ϕ بر K نیز هست. از آنجایی که ϕ بر K جداپذیر است، نتیجه می‌شود M/K یك توسیع گالوایی است. فرض کنیم F آن زیرمیدان از M، پدید آمده توسط K و ریشه‌های X^m-1، باشد. فرض کنیم F_i $(1 \leqslant i \leqslant n)$ زیرمیدان M، پدید آمده توسط F و K_i، باشد. قرار می‌دهیم $F_\circ = K$. روشن است که $F_1=F$، $F_n = M$ و $F_{i+1}=F_i(\beta_i)$ $(1\leqslant i\leqslant n-1)$. چون F تمام ریشه‌های mام واحد را دربر دارد، نتیجه می‌شود که F_{i+1}/F_i $(1\leqslant i\leqslant n-1)$ توسیعی دوری است (قضیهٔ ۲).

ادعا می کنیم که G، گروه گالوایی M/K، حلپذیر است. فرض کنیم G_i زیرگروه G بامیدان ثابت F_i باشد $(1\leqslant i\leqslant n)$. داریم $G=G_\circ \supset G_1 \supset G_2 \supset \ldots \supset G_n=\{e\}$. از آنجایی که F_{i+1}/F_iها $(\circ \leqslant i \leqslant n-1)$ نرمال هستند، نتیجه می‌شود که G_{i+1} یك زیرگروه نرمال G_i است و از آنجا G_i/G_{i+1} را می‌توان با گروه گالوایی F_{i+1}/F_i $(\circ \leqslant i \leqslant n-1)$ یکی گرفت (مراجعه کنید به نتیجهٔ قضیهٔ اصلی ۲، فصل ۴). بنابر قضیهٔ ۱، $G_\circ/G_1$ آبلی است و در بالا مشاهده کردیم که G_i/G_{i+1} $(1\leqslant i\leqslant n-1)$ دوری است. بنابراین یك سری حلپذیر برای G وجود دارد (بخش ۳، فصل ۱) و لذا G حلپذیر است.

چون گروه گالوایی L/K را می‌توان با یك گروه خارج قسمت از G یکی گرفت (رجوع کنید به نتیجهٔ قضیهٔ اصلی ۲، فصل ۴)، نتیجه می گیریم که گروه گالوایی L/K حلپذیر است (قضیهٔ ۷، فصل ۱). □

قضیهٔ ۶. فرض کنیم L/K یك توسیع گالوایی از درجهٔ n باشد و $G=G(L/K)$ حلپذیر باشد. فرض کنیم $[n, p]=1$. در این صورت توسیعی مانند M/L وجود دارد که M/K یك توسیع رادیکالی است.

برهان. قضیه را به‌استقرا بر مرتبهٔ G ثابت می‌کنیم. اگر $G=\{e\}$، چیزی برای اثبات باقی نمی‌ماند. در غیراین‌صورت، زیرگروهی مانند G_1 از G وجود دارد که G/G_1 دوری است و مرتبه‌اش عددی اول است (و دراین صورت، مرتبهٔ G_1 اکیداً از مرتبهٔ G کمتراست؛ قضیهٔ ۹، فصل ۱). فرض کنیم L_1 میدان ثابت G_1 باشد. آنگاه L/L_1 و L_1/K توسیعهایی گالوایی هستند که گروههای گالواییشان، به‌ترتیب، G_1 و G/G_1 هستند (قضیهٔ اصلی ۲، فصل ۴). فرض کنیم m مرتبهٔ G/G_1 باشد. در این‌صورت $[m, p]=1$. فرض کنیم N میدان شکافندهٔ X^m-1 روی L باشد و F زیرمیدانی از N باشد که توسط K و ریشه‌های X^m-1 پدید می آید. فرض کنیم L_1F (به‌ترتیب، LF) آن زیرگروه از N باشد که توسط L_1 و F (به‌ترتیب L و F) پدید می آید.

اکنون L_1F/F توسیعی گالوایی‌است و $G(L_1F/F)$ با زیرگروهی از $G(L_1/K)$ ایزومورف است. (قضیهٔ ۲، فصل ۴)، از آنجایی که m اول، $G(L_1F/F)=\{e\}$ یا گروه

دوری از مرتبهٔ m است. با توجه به‌اینکه F حاوی تمام ریشه‌های mم واحد است، نتیجه می‌شود که L_1F/F یك توسیع رادیکالی ساده است (قضیهٔ ۳).

توسیع LF/L_1F گالوایی است و $G(LF/L_1F)$ با زیرگروهی از $G(L/L_1)$ ایزومورف است، زیرا که LF آن زیرمیدان از N است که توسط L و L_1F پدید می‌آید (قضیهٔ ۲، فصل ۴). از اینجا نتیجه می‌شود که $G(LF/L_1F)$ حلپذیر است (قضیهٔ ۷، فصل ۱) و نیز اگر r مرتبهٔ آن باشد، $[r, p]=1$. آنگاه، بنا برفرض استقرا توسیعی مانند M/LF وجود دارد که M/L_1F یك توسیع رادیکالی است. از آنجایی که F/K یك توسیع رادیکالی است، ، نتیجه می‌گیریم که M/K هم یك توسیع رادیکالی است. این مطلب برهان قضیه را کامل می‌کند.
□

فرض کنیم $f \in K[X]$. دراین‌صورت f روی K حلپذیر با رادیکالها نامیده می‌شود اگر میدان شکافندهٔ f روی K زیرمیدانی از یك توسیع رادیکالی‌روی K باشد. به‌آسانی دیده می‌شود که fروی K حلپذیر با رادیکالهاست اگر و فقط اگر هرعامل تجزیه‌ناپذیر f، روی K حلپذیر با رادیکالها باشد.

قضیهٔ اصلی ۱. فرض‌کنیم $f \in K[X]$ و L میدان شکافندهٔ f روی K باشد. فرض کنیم $[n, p]=1$ که در آن $n=[L:K]$. در این صورت L/K توسیعی گالوایی است و f حلپذیر با رادیکالهاست اگر و فقط اگر $G(L/K)$ حلپذیرباشد.

برهان. فرض کنیم α عضوی از L باشد. فرض کنیم g چندجمله‌ای مینیمال α روی K و m درجه‌اش باشد. ازآنجایی‌که $m=[K(\alpha):K]$، داریم $m \mid n$ و در نتیجه $[m, p]=1$. بنابراین g روی K جداپذیر است. لذا α روی K جداپذیر است و از آنجا نتیجه می‌شود که L/K یك توسیع گالوایی‌است. حال، فرض کنیم $G(L/K)$ حلپذیر باشد. از قضیهٔ ۶ نتیجه می‌گیریم توسیعی مانند M/L وجود دارد که M/K یك توسیع رادیکالی است. به‌عکس، فرض کنید M/L توسیعی باشد که M/K یك توسیع رادیکالی باشد. با استفاده از قضیهٔ ۴، می‌توان فرض کرد که M/K یك توسیع رادیکالی گالوایی است. بنابرقضیهٔ ۵، مشاهده می‌کنیم که $G(M/K)$ حلپذیراست. از آنجایی $G(L/K)$ با یك گروه خارج قسمت از $G(M/K)$ ایزومورف است، نتیجه می‌گیریم که $G(L/K)$ حلپذیر است.
□

تذکر: اگر درقضیهٔ بالا، f به‌گونه‌ای باشد که بافرض $m=\deg f$، $[m!, p]=1$، نتیجه می‌گیریم که $[n, p]=1$.

۳. حلپذیری معادلهٔ جبری

فرض کنیم H زیرگروهی از گروه متقارن S_n برمجموعهٔ $\{x_1, \dots, x_n\}$ باشد. گوییم H متعدی است هرگاه به‌ازای هر x_i و x_j، عضوی چون $\sigma \in H$ وجود داشته باشد که $\sigma(x_i)=x_j$.

فرض کنیم $f \in K[X]$ و این چندجمله‌ای روی K جداپذیر باشد. فرض کنیم L میدان شکافندهٔ f روی K باشد. دراین صورت L/K یك توسیع گالوایی است. گروه $G=G(L/K)$ را گروه چندجمله‌ای f روی K می‌نامند.

اینك فرض کنیم f تجزیه‌ناپذیر باشد، و $\alpha_1, \ldots, \alpha_n$ ریشه‌هایش باشند. به ازای هر ریشهٔ α_i از f و هر $\sigma \in G$، $\sigma(\alpha_i)$ نیز یك ریشهٔ f است ولذا به‌ازای عددی چون j، $\sigma(\alpha_i)=\alpha_j$. بنابراین، σ جایگشتی چون $\bar{\sigma}$ از مجموعهٔ $\{\alpha_1, \ldots, \alpha_n\}$ را القا می‌کند.

نگاشت $\sigma \to \bar{\sigma}$ از G به‌توی گروه جایگشتی S_n که به‌صورت بالا تعریف شد، آشکارا ایزومورفیسمی از G به‌روی زیرگروهی از S_n است. G را با تصویر G تحت این نگاشت، یکی می‌گیریم و درنتیجه G را به‌عنوان یك گروه جایگشتی تلقی می‌کنیم. زیرگروه G از S_n متعدی است، زیرا بـه‌ازای هر دو ریشهٔ α_i و α_j، K-اتومورفیسمی چون σ از L وجود داردکه $\sigma(\alpha_i)=\alpha_j$ (قضیهٔ ۶، فصل ۳).

قضیهٔ اصلی ۲. فرض کنیم که مشخصهٔ p ازمیدان K مخالف با ۲ و ۳ باشد و $f \in K[X]$ از درجهٔ نابیشتر از ۴ باشد. آنگاه f روی K با رادیکالها حلپذیر است.

برهان. می‌توان فرض کرد که f تجزیه‌ناپذیر باشد. اگر $n=\deg f$، داریم $[n!, p]=1$. درنتیجه، اگر L میدان شکافندهٔ f روی K باشد و $m=[L:K]$، داریم $[m, p]=1$. بنابرآنچه‌که دربالا دیدیم، $G(L/K)$ را می‌توان با زیرگروهی از S_n، $n \leqslant 4$، یکی دانست. ازآنجایی‌که S_n، به‌ازای $n \leqslant 4$، حلپذیر است (بخش ۴، فصل ۱)، نتیجه می‌گیریم که $G(L/K)$ نیزحلپذیر است (قضیهٔ ۷، فصل ۱). اینك این قضیه، ازقضیهٔ اصلی ۱ نتیجه می‌شود. □

به‌ازای میدان مفروضی چون K، این سؤال را مطرح می‌کنیم که آیا روی K یك چندجمله‌ای جداپذیر وجود داردکه روی K با رادیکالها حلپذیر نباشد. جواب همیشه مثبت نیست.

به‌عنوان نمونه. به‌مثالهای زیر توجه می‌کنیم.

(۱) فرض می‌کنیم $K=\mathbf{C}$ میدان اعداد مختلط باشد. «قضیهٔ بنیادی جبر» ایجاب می‌کندکه هرچندجمله‌ای تجزیه‌ناپذیر f روی $\mathbf{C}$ خطی باشد. این مطلب بدین معناست که میدان شکافندهٔ f روی $\mathbf{C}$ خود $\mathbf{C}$ است. بنابراین، گروه چندجمله‌ای f بـه عنصر همانی تحویل می‌یابد؛ به‌ویژه f با رادیکالها حلپذیر است!

(۲) فرض کنیم $K=\mathbf{R}$ میدان اعداد حقیقی‌باشد و f یك چندجمله‌ای تجزیه‌ناپذیر روی $\mathbf{R}$ باشد. چون $[\mathbf{C}:\mathbf{R}]=2$ وچون f در $\mathbf{C}$ به‌عوامل خطی شکافته می‌شود، نتیجه می‌گیریم که میدان شکافندهٔ f روی $\mathbf{R}$ یا $\mathbf{C}$ است یا $\mathbf{R}$. بنابراین گروه چندجمله‌ای f از مرتبهٔ نابیشتر از ۲ است. پس f روی $\mathbf{R}$ با رادیکالها حلپذیر است.

(۳) فرض کنیم K یك میدان متناهی و L/K یك توسیع متناهی باشد. می‌دانیم که L/K دوری است (قضیهٔ اصلی ۳، فصل ۴). به‌ویژه $G(L/K)$ حلپذیر است.

با این وصف، اینك نشان می‌دهیم که چندجمله‌ایهای تجزیه‌ناپذیر روی $\mathbf{Q}$، میدان

اعداد گویا، وجود دارند که گروهشان روی $\mathbf{Q}$ حلپذیر نیست.

قضیهٔ ۰۷ فرض می‌کنیم G یك گروه متعدی از گروه جایگشتی S_p، که در آن p عددی اول است، باشد. فرض می‌کنیم G شامل یك ترانهش باشد. در این صورت $G=S_p$.
برهان. S_p را به‌عنوان گروه جایگشتی $I_p=\{1, 2, \ldots, p\}$ در نظر می‌گیریم. فرض کنیم H زیرگروه پدید آمده توسط ترانهشهای موجود در G باشد. در این صورت $H\neq\{e\}$ و این گروه یك زیرگروه نرمال G است، زیرا اگر (i, j) یك ترانهش در G باشد، داریم $\sigma(i, j)\sigma^{-1}=(\sigma(i), \sigma(j))$ و اگر $\tau=\prod\limits_{1\leqslant k\leqslant n}\tau_k$ که در آن τ_k یك ترانهش در G باشد، آنگاه $\sigma\tau\sigma^{-1}=\prod\limits_{1\leqslant k\leqslant n}(\sigma\tau_k\sigma^{-1})$. ادعا می‌کنیم که H یك زیرگروه متعدی از S_p است. این مطلب نتیجه‌ای از لم ذیل است. □

لم. فرض کنیم G یك زیرگروه متعدی از S_p، که در آن p عددی اول است، باشد. اگر H یك زیرگروه نرمال از G باشد که $H\neq\{e\}$، آنگاه H نیز یك زیرگروه متعدی از S_p است

برهان لم. در I_p نسبتی هم‌ارزی به صورت ذیل معرفی می‌کنیم. می‌نویسیم $i\sim j$ اگر عضوی چون $h\in H$ وجود داشته باشد که $h(i)=j$. فرض کنیم $H(i)$ ردهٔ هم‌ارزی حاوی $i\in I_p$ باشد. در این صورت $H(i)$ عبارت است از زیرمجموعهٔ $\{\sigma(i)|\sigma\in H\}$ از I_p. ادعا می‌کنیم که اگر i و j در I_p باشند، $H(i)$ و $H(j)$ به‌تعداد مساوی عضو دارند. در واقع عضوی چون $\tau\in G$ وجود دارد که $H(j)=i$ وچون H نرمال است، داریم $H(i)=H(\tau(j))=\tau H(j)$. از آنجایی که τ یك نگاشت یك به‌یك از I_p به‌روی I_p است، $H(j)$ و $\tau H(j)$ به‌تعداد مساوی عضو دارند و ادعا ثابت می‌شود. چون I_p مساوی با اجتماع مجزای رده‌های هم‌ارزی متمایز $H(i)$ است، اگر m تعداد اعضای $H(i)$ باشد، داریم $m|p$. نظر به‌اینکه $H\neq\{e\}$، داریم $m\neq 1$، و از آنجا نتیجه می‌شود که $m=p$.
بنا براین $H(i)=I_p$؛ یعنی H یك زیرگروه متعدی G است. □

اکنون به‌تکمیل برهان قضیه می‌پردازیم. در H ترانهشی مانند (i_1, i_2) وجود دارد. فرض کنیم $i_2, \ldots, i_q$ کلیهٔ اعضایی از I_p باشند که $(i_1, i_j)\in H$، $2\leqslant j\leqslant q$. بدون اینکه به‌کلیت برهان خللی وارد شود، فرض می‌کنیم که $i_1=1$، $i_2=2$؛ ...، $i_q=q$. اگر $q=p$، آنگاه $H=S_p$ و از آنجا $G=S_p$ و قضیه ثابت می‌شود. فرض کنیم که $q<p$. در این‌صورت، به‌ازای $1\leqslant i\leqslant q$، $(1, i)\in H$ و به‌ازای $j>q$، $(1, j)\notin H$. از آنجایی که H متعدی است، عضوی چون $\sigma\in H$ وجود دارد که $\sigma(1)=p$. حالا $\sigma=\tau_1\ldots\tau_h$ که در آن τ_kها، $1\leqslant k\leqslant h$، ترانهشهایی از H هستند. فرض کنید کلیهٔ τ_kها، $1\leqslant k\leqslant h$، مجموعهٔ $\{1, \ldots, q\}$ را پایا نگهدارند؛ یعنی، اگر $1\leqslant i\leqslant q$، آنگاه به‌ازای هر k که $1\leqslant k\leqslant h$ داشته باشیم $1\leqslant\tau_k(i)\leqslant q$. در این صورت، به‌ازای هر i که $1\leqslant i\leqslant q$، داریم $1\leqslant\sigma(i)\leqslant q$، که یك تناقض است. بنا براین، عضوی چون

τ_k، $1 \leqslant k \leqslant h$، وجود دارد که به‌شکل (i_1, i_2) است و در آن $1 \leqslant i_1 \leqslant q$ و $i_2 > q$.
پس داریم

$$(1, i_1)(i_1, i_2)(1, i_1)^{-1} = (1, i_2) \in H.$$

این مطلب به‌یك تناقض منجر می‌شود. لذا $q = p$ وقضیه ثابت می‌شود. □

قضیهٔ ۸. فرض کنیم $f \in \mathbf{Q}[X]$، که در آن $\mathbf{Q}$ میدان اعداد گویاست، چنان باشدکه (۱) $\deg f = p$ و p عددی اول است، (۲) f تجزیه‌ناپذیر است و، (۳) (در میدان اعداد مختلط $\mathbf{C}$) f درست $(p-2)$ ریشهٔ حقیقی دارد. در این‌صورت گروه چندجمله‌ای f مساوی با S_p است.

برهان. با توجه به‌اینکه قضیه به‌ازای $p = 2$ بدیهی است، فرض می‌کنیم $p \geqslant 3$. نگاشت $\mathbf{C} \to \mathbf{C}$ با ضابطهٔ $z \to \bar{z}$ (که در آن $\bar{z}$ مزدوج مختلط z است) آشکارا یك $\mathbf{R}$-اتومورفیسم از $\mathbf{C}$ است. بنابراین اگر $\alpha \in \mathbf{C}$ ریشه‌ای ازیك چندجمله‌ای g با ضرایب حقیقی باشد، آنگاه $\bar{\alpha}$ نیز ریشه‌ای از g است.

فرض کنیم $f = \prod_{1 \leqslant i \leqslant p} (X - \alpha_i)$ چنان باشد که، به ازای $3 \leqslant i \leqslant p$، α_iها حقیقی باشند. داریم $\alpha_2 = \bar{\alpha}_1$. دراین صورت نگاشت از $\mathbf{C}$ به‌روی $\mathbf{C}$ با ضابطهٔ $z \to \bar{z}$، اتومورفیسمی مانند σ ازمیدان شکافندهٔ f روی $\mathbf{R}$ القا می‌کند و σ هم ترانهش (α_1, α_2) برمجموعهٔ $\{\alpha_1, \ldots, \alpha_p\}$ را القا می‌نماید. در نتیجه گروه چندجمله‌ای f حاوی یك ترانهش است وچون این گروه بر مجموعهٔ $\{\alpha_1 \ldots, \alpha_p\}$ متعدی است (f تجزیه‌ناپذیر است)، نتیجه می‌شودکه گروه چندجمله‌ای f مساوی با S_p است (قضیهٔ ۷). □

قضیهٔ اصلی ۳. به‌ازای هرعدد اول p، یك چندجمله‌ای چون $f \in \mathbf{Q}[X]$ وجود داردکه گروه آن S_p است. درحالت خاص، چندجمله‌ایهایی روی $\mathbf{Q}$ وجود دارند که روی $\mathbf{Q}$ با رادیکالها حلپذیر نیستند.

برهان. به‌ازای $p = 2$، می‌توان هرچندجمله‌ای تجزیه‌ناپذیر از درجهٔ ۲ (مثلاً $X^2 + 1$) را انتخاب کرد.

اگر $p \geqslant 3$، چندجمله‌ای تجزیه‌ناپذیری‌مانند f ازدرجهٔ p روی $\mathbf{Q}$ می‌سازیم که f دقیقاً $p - 2$ ریشهٔ حقیقی (در $\mathbf{C}$) داشته باشد. در این صورت، بنابرقضیهٔ ۸، گروه چندجمله‌ای f مساوی با S_p خواهد بود.

اگر $p = 3$، می‌توان نوشت $f = X^3 - 2$. آشکارا (مثلاً، با توجه به محك ایزنشتاین (قضیهٔ ۸، فصل ۲)) f تجزیه‌ناپذیر است.

حال فرض می‌کنیم $p \geqslant 5$. فرض کنیم $a_1, a_2, \ldots, a_{p-2}$ اعداد صحیح زوجی باشندکه

$$a_1 > a_2 > \cdots > a_{p-2},$$

و b عدد صحیح زوج مثبتی باشد. فرض کنیم

$$g=(X^{۲}+b)\prod_{۱\leqslant i\leqslant p-۲}(X-a_i)\cdot$$

فرض کنیم $t_k=\dfrac{a_k+a_{k+۱}}{۲}$، $۱\leqslant k\leqslant p-۳$. واضح است که t_k عددی صحیح است.
همچنین $۲\leqslant (t_k^{۲}+b)$. به‌علاوه $|t_k-a_i|\geqslant ۱$ $(۱\leqslant i\leqslant p-۲)$ و دست کم به‌ازای یک i، $|t_k-a_i|>۱$؛ درنتیجه به ازای $۱\leqslant k\leqslant p-۳$ داریم $|g(t_k)|>۲$. حال، اگر $a_i>x>a_{i+۱}$، $(۱\leqslant i\leqslant p-۳)$، آنگاه بنابراینکه i زوج یا فرد باشد، به‌ترتیب، $g(x)>۰$ یا $g(x)<۰$. بنابراین، برحسب اینکه k زوج یا فرد باشد $(۱\leqslant k\leqslant p-۳)$ داریم $g(t_k)-۲>۰$ یا $g(t_k)-۲<۰$. اینک اگر x به‌اندازهٔ کافی بزرگ باشد، داریم $g(x)-۲>۰$ و درصورتی که $x<a_{p-۲}$، داریم $g(x)-۲<۰$.
بنابراین اگر قرار دهیم $f=g-۲$، f دست کم $(p-۲)$ ریشهٔ حقیقی چون $\alpha_۱,\ldots,\alpha_{p-۲}$ دارد که $\alpha_۱>t_۱$، $t_i>\alpha_{i+۱}>t_{i+۱}$ $(۱\leqslant i\leqslant p-۴)$ و $t_{p-۳}>\alpha_{p-۲}$.
فرض کنیم $\alpha_{p-۱}$ و α_p دو ریشهٔ دیگر f (در $\mathbf{C}$) باشند. داریم

$$\sum_{۱\leqslant i\leqslant p}\alpha_i=\sum_{۱\leqslant i\leqslant p-۲}a_i=t\ (\text{قرارداد}),$$

$$\sum_{۱\leqslant i<j\leqslant p}\alpha_i\alpha_j=b+\sum_{۱\leqslant i<j<p-۲}a_ia_j=b+m\ (\text{قرارداد})\cdot$$

با این قراردادها، داریم

$$\sum_{۱\leqslant i\leqslant p}\alpha_i^{۲}=t^{۲}-۲(b+m)\cdot$$

اکنون b را چنان اختیار می‌کنیم که $t^{۲}-۲(b+m)<۰$. بنابراین، f تنها $(p-۲)$ ریشه حقیقی دارد.
حال نشان می‌دهیم که f تجزیه‌ناپذیر است اگر $f=X^p+\sum_{۱\leqslant i\leqslant p}c_iX^{p-i}$، آشکارا داریم $۲|c_i$ $(۱\leqslant i\leqslant p)$ و $۴\nmid c_p$. اینک تجزیه‌ناپذیری f نتیجه‌ای از محک ایزنشتاین (قضیهٔ ۸، فصل ۲) است.
بالاخره، با توجه به‌اینکه به‌ازای $p\geqslant ۵$، S_p حلپذیر نیست، نتیجه می‌گیریم که چندجمله‌ایهایی روی $\mathbf{Q}$ وجود دارند که روی $\mathbf{Q}$ با رادیکالها حلپذیر نیستند. □

تذکر: اگر $p=۵$، مثالی از یک چندجمله‌ای روی $\mathbf{Q}$ که $S_۵$ گروه آن چندجمله‌ای باشد به‌صورت زیر به دست می‌آید. با علایم موجود در برهان قضیه، می‌توان نوشت $a_۱=۲$، $a_۲=۰$، $a_۳=-۲$ و $b=۶$. دراین صورت

$$f=(X^{۲}+۶)(X-۲)X(X+۲)-۲$$

$$=X^{۵}+۲X^{۳}-۲۴X-۲۰$$

۴. ترسیم با خط‌کش و پرگار

فرض کنیم $\mathbf{E}$ صفحه، یعنی مجموعهٔ $\mathbf{R}\times\mathbf{R}$، باشد. برای $\mathbf{E}$ دستگاه ثابتی از محورهای متعامد در نظر می‌گیریم. مقصود ما از مختصات (x, y) برای نقطه‌ای از $\mathbf{E}$ عبارت است از مختصات آن نقطه نسبت به این محورها. اگر S زیرمجموعه‌ای از $\mathbf{E}$ باشد، قرار می‌دهیم:

$$X(S)=\{x\in\mathbf{R}\,|\,(x, y)\in S \text{ ، به‌ازای عضوی چون } y\in R\}\text{ ،}$$

$$Y(S)=\{y\in\mathbf{R}\,|\,(x, y)\in S \text{ ، به‌ازای عضوی چون } x\in\mathbf{R}\}.$$

آن زیرمیدان از $\mathbf{R}$ را که توسط $X(S)\bigcup Y(S)$ پدید می‌آید، با $K(S)$ نمایش می‌دهیم.

فرض کنیم S زیرمجموعه‌ای از $\mathbf{E}$، متشکل از دست‌کم دو عضو باشد. بدون اینکه به‌کلیت برهان خللی وارد آید، می‌توان فرض کرد که S حاوی $(۰ , ۰)$ و $(۰ , ۱)$ باشد. می‌گوییم S نسبت به ترسیمهای با خط‌کش و پرگار پایدار است (یا S پایدار است) اگر شرایط زیر برقرار باشند:

(۱) به‌ازای A، B، C و D از S، اگر خط ماربر A , B خط ماربر C , D را در نقطه‌ای مانند E قطع کند، آنگاه E در S است.

(۲) به‌ازای A، B، C و D از S، اگر دایرهٔ به‌مرکز A و ماربر B خط ماربر C و D را در نقطه‌ای مانند E از $\mathbf{E}$ قطع کند، آنگاه E در S است.

(۳) به‌ازای A، B، C و D از S، اگر دایرهٔ به‌مرکز A و ماربر B دایرهٔ به مرکز C و ماربر D را در نقطه‌ای مانند E از $\mathbf{E}$ قطع کند، آنگاه E در S است.

فرض کنیم S زیرمجموعهٔ دلخواهی از صفحه، وحاوی $(۰ , ۰)$ و $(۰ , ۱)$ باشد. در این صورت مقطع تمام زیرمجموعه‌های پایدار از $\mathbf{E}$ که شامل S هستند، خود پایدار است. این مجموعه را بستار پایدار S می‌نامند و با $C(S)$ نمایش می‌دهند.

فرض کنیم K زیرمیدانی از $\mathbf{R}$ باشد. K را پایدار می‌نامیم اگر ریشهٔ دوم هر عضو مثبت K به K تعلق داشته باشد. اگر K زیرمیدان دلخواهی از $\mathbf{R}$ باشد، مقطع تمام زیرمیدانهای پایدار از $\mathbf{R}$ که شامل K هستند، خود پایدار است. این میدان را بستار پایدار میدان K می‌نامند و با $C(K)$ نمایش می‌دهند.

قضیهٔ ۹. فرض کنیم S یك زیرمجموعهٔ پایدار $\mathbf{E}$ باشد. دراین صورت داریم $X(S)=Y(S)=K(S)$ و $K(S)$ یك زیرمیدان پایدار $\mathbf{R}$ است. به‌علاوه، $(x , y)\in S$ اگر وفقط اگر x و y به $X(S)$ تعلق داشته باشند. به‌عکس، اگر K یك زیرمیدان پایدار $\mathbf{R}$ باشد، زیرمجموعهٔ S از $\mathbf{E}$ که به صورت $S=\{(x , y)|x , y\in K\}$ تعریف می‌شود، پایدار است.

برهان. به‌کمك ترسیمهای پیش پا افتاده با خط‌کش وپرگار ملاحظه می‌کنیم (۱) $(x , y)\in S$ اگر و فقط اگر $(x , ۰)$، $(۰ , x)$، $(۰ , y)$ و $(y , ۰)$ در S باشند؛ (۲) اگر x , y در $X(S)$ باشند، آنگاه $x-y$، xy^{-1} (درصورتی که $y\neq ۰$) در $X(S)$ هستند؛ و (۳) اگر $x>۰$ و x در $X(S)$ باشد، آنگاه $\sqrt{x}$ در $X(S)$ است. قسمت اول

قضیه، نتیجهٔ سادهای ازاین خواص است. عکس قضیه آناً ازنکات زیر نتیجه میشود.

(۱) اگر خط ماربر A , B خط ماربر C و D را درنقطهای مانند E قطع کند (در اینجا $A, B, C, D \in S$)، آنگاه مختصات E در $K(T)$ هستند: T زیرمجموعهٔ S متشکل ازنقاط A ، B ، C ، و D است؛

(۲) اگر E به اشتراك دایرهٔ به مرکز A و ماربر B، وخط ماربر C و D تعلق داشته باشد (دراینجا $A , B , C , D \in S$)، آنگاه مختصات E بـه توسیعی مانند L از $K(T)$ تعلق داردکه $[L : K(T)] \leqslant ۲$.

(۳) اگر عضوی چون $E \in \mathbf{E}$ به اشتراك دوایری به مراکز A و C و به ترتیب ماربر B و D تعلق داشته باشد (دراینجا $A, B, C, D \in S$)، آنگاه مختصات E بهتوسیعی مانند L از $K(T)$ تعلق داردکه $[L : K(T)] \leqslant ۲$. □

چند تذکر: ۱. فرض کنید S زیرمجموعهٔ متشکل از دونقطهٔ (۰ , ۰) و (۰ , ۱) از $\mathbf{E}$ باشد. آنگاه $C(S)$ آن مجموعه ازنقاطی است که معمولاً بدان مجموعهٔ قابل رسم با خطکش وپرگار و با در دست داشتن واحد طول، اطلاق میشود. در این حالت، داریم $\mathbf{Q} = K(S)$.

۲. فرض کنید S زیرمجموعهای از $\mathbf{E}$ وحاوی (۰ , ۰) و (۰ , ۱) باشد. دراین صورت داریم $K(C(S)) = C(K(S))$.

فرض کنیم N/K یك توسیع رادیکالی باشد. گفته میشودکه این توسیع از نوع ۲ است اگر زیرمیدانهایی مانند N_i $(0 \leqslant i \leqslant n)$ از N وشامل K وجود داشته باشدکه $N_0 = K$ ، $N_n = N$ ، $N_i \subset N_{i+1}$ و $[N_{i+1} : N_i] = 2$ ، $(0 \leqslant i \leqslant n-1)$. توجه کنیدکه اگر M/K توسیع دلخواهی باشد و M_jها $(1 \leqslant j \leqslant m)$ زیرمیدانهایی از M وشامل K باشندکه M_j/Kها $(1 \leqslant j \leqslant m)$ توسیعهای رادیکالی ازنوع ۲ باشند، آنگاه توسیع $(M_1 \ldots M_m)/K$ نیز یك توسیع رادیکالی ازنوع ۲ است.

قضیهٔ ۱۰. فرض کنیم K زیرمیدانی از $\mathbf{R}$ باشد و $x \in C(K)$. دراین صورت زیرمیدانی از $C(K)$ مانند L حاوی x و K وجود داردکه L/K یك توسیع رادیکالی از نوع ۲ باشد.

برهان. بـهازای هرعدد صحیح $i \geqslant 0$، زیرمیدانهای K_i از $C(K)$ را به استقرا بهصورت ذیل تعریف میکنیم: $K_0 = K$ ، K_{i+1} آن زیرمیدان از $C(K)$ است که توسط K_i و ریشههای دوم تمام اعضای مثبت K_i پدید میآید. واضح است که $C(K) = \bigcup_{i \geqslant 0} K_i$.

بهازای عضوی چون $x \in K_i$ ، i. بـه استقرا بر i، این قضیه را در مورد K_i ثابت میکنیم.[1] فرض کنیم این قضیه در مورد تمام عضوهای y در K_{i-1} ثابت شده باشد. چون $x \in k_i$، عضوهاییچون $\theta_1 , \ldots , \theta_n$ در K_i وجود دارندکه $\theta_j^2 \in K_{i-1}$ ، $(1 \leqslant j \leqslant n)$

---

۱. یعنی ثابت میکنیم: بهازای هر $y \in K_i$ ، زیرمیدانی از $C(K)$ مانند L_y حاوی y و K وجود داردکه L_y/K یك توسیع رادیکالی ازنوع ۲ است.ـم.

و $x\in K_{i-1}(\theta_1,\dots,\theta_n)$. دراین‌صورت $x=f(\theta_1,\dots,\theta_n)/g(\theta_1,\dots,\theta_n)$ که در آن

$$f(\theta_1,\dots,\theta_n)=\sum a_{i_1,\dots,i_n}\theta_1^{i_1}\cdots\theta_n^{i_n},$$

$$g(\theta_1,\dots,\theta_n)=\sum b_{j_1,\dots,j_n}\theta_1^{j_1}\cdots\theta_n^{j_n},\ g(\theta_1,\dots,\theta_n)\neq 0$$

و عضوهای $a_{i_1,\dots,i_n}$ و $b_{j_1,\dots,j_n}$ به K_{i-1} تعلق‌دارند. بنا بر فرض استقرا هر یك از عضوهای $a_{i_1,\dots,i_n}$ و $b_{j_1,\dots,j_n}$ به زیرمیدانی از $C(K)$ تعلق دارند که یك توسیع رادیکالی K و از نوع ۲ است. بنا بر این یك توسیع رادیکالی از نوع ۲ و حاوی تمام عضوهای $a_{j_1,\dots,i_n}$ و $b_{j_1,\dots,j_n}$ وجود دارد. بدین ترتیب، داریم $x\in L_1(\theta_1,\dots,\theta_n)$ و $\theta_i^2\in L_1$، $(1\leqslant i\leqslant n)$. L را به‌صورت $L=L_1(\theta_1,\dots,\theta_n)$ اختیار می‌کنیم. بدیهی است که L/L_1 یك توسیع رادیکالی از نوع ۲ است و از آنجا L/K نیز یك توسیع رادیکالی از نوع ۲ است. □

قضیهٔ اصلی۴. فرض‌کنیم K زیرمیدانی از $\mathbf{R}$ باشد. در این صورت عضوی چون y از $\mathbf{R}$ به $C(K)$ تعلق دارد اگر و فقط اگر یك توسیع گالوایی N/K وجود داشته باشد که (به‌ازای عدد صحیحی چون m) $[N:K]=2^m$ و $y\in N$.

برهان. فرض کنیم $y\in C(K)$. دراین‌صورت، بنا بر قضیهٔ ۱۰، زیرمیدانی مانند M از $\mathbf{R}$ وجود داردکه M/K یك توسیع رادیکالی از نوع ۲ است و y در M است. ادعا می‌کنیم که اگر M یك توسیع رادیکالی دلخواه از نوع ۲ باشد، توسیعی مانند N/M وجود داردکه N/K گالوایی است و به‌ازای عددی چون m، $[N:K]=2^m$. در واقع، توسیع گالوایی موردنظراز تکرار برهان قضیهٔ ۴ برای این حالت خاص به‌دست می‌آید.

اکنون فرض‌کنیم N/K یك توسیع گالوایی از درجهٔ 2^m باشدکه y در N باشد. می‌توانیم فرض کنیم که N زیرمیدانی‌از $\mathbf{C}$ است؛ زیرا، N میدان شکافندهٔ یك چندجمله‌ای f روی $K(y)$ است، و بنا برقضیهٔ بنیادی جبر f در $\mathbf{C}$ به‌عوامل خطی تجزیه می‌شود؛ در نتیجه یك $K(y)$- ایزومورفیسم σ از N به‌روی زیرمیدان N' از $\mathbf{C}$، که توسط $K(y)$ و ریشه‌های f در $\mathbf{C}$ پدید می‌آید، وجود دارد. گروه $G(N/K)$ یك سری حلپذیر

$$G(N/K)=G_0\supset G_1\supset G_2\supset\cdots\supset G_n=\{e\}$$

داردکه G_{i+1} یك زیر گروه نرمال از G_i است و G_i/G_{i+1} $(0\leqslant i\leqslant n-1)$ ازمرتبهٔ ۲ است (قضیه‌های ۸، ۹، فصل ۱). اگر K_i میدان ثابت G_i باشد، داریم $K_0=K$، $K_n=N$ و $[K_{i+1},K_i]=2$. به‌استقرا بر i ثابت می‌کنیم که به‌ازای هر i، $K_i\cap\mathbf{R}\subset C(K)$. فرض‌کنیم $K_{i-1}\cap\mathbf{R}\subset C(K)$. داریم $K_i=K_{i-1}(x)$، $x\in K_i$ و $x^2\in K_{i-1}$. دراین صورت هرعضواز K_i به‌شکل $a+bx$ است که $a,b\in K_{i-1}$. بنا بر فرض‌استقرا، قسمتهای حقیقی و موهومی a، b و x^2 در $C(K)$ هستند. به‌علاوه، اگر x عدد مختلطی باشدکه قسمتهای حقیقی و موهومی x^2 در $C(K)$ باشند، آنگاه به‌آسانی دیده می‌شودکه قسمتهای

حقیقی و موهومی x نیز در $C(K)$ هستند. پس $K_i \cap \mathbf{R} \subset C(K)$. از آنجایی که $y \in N \cap \mathbf{R}$، نتیجه می‌گیریم که y در $C(K)$ است و قضیه ثابت می‌شود. □

چند مثال: ۱. تثلیث یک زاویه. فرض کنیم S مجموعهٔ متشکل از نقاط $O=(0,0)$، $P=(1,0)$ و $Q=(x,y)$ باشد که P و Q هردو بر روی یک دایرهٔ C به‌مرکز O واقع هستند. فرض کنیم θ اندازهٔ زاویهٔ $P\hat{O}Q$ باشد و R نقطه‌ای از دایرهٔ C باشد که اندازهٔ $P\hat{O}R$ مساوی $\theta/3$ است. مسئله این است که مشخص کنیم آیا نقطه‌ای از خط مار بر O و R به $C(S)$ تعلق دارد؛ یا به‌عبارت معادل، R در $C(S)$ است. داریم $R=(\cos\theta/3, \sin\theta/3)$ و R در $C(S)$ است اگروفقط اگر $\cos\theta/3$ به $C(K(S))$ تعلق داشته باشد. اکنون $\cos\theta/3$ یک ریشهٔ چندجمله‌ای $f=4X^3-3X-\alpha$ است که در آن $\alpha=\cos\theta$. می‌توان α را چنان اختیار کرد که $\alpha\in\mathbf{Q}$، $0\leqslant\alpha<1$، و f روی $\mathbf{Q}$ تجزیه‌ناپذیر باشد (به‌عنوان مثال $\theta=\pi/2$). به سادگی ملاحظه می‌شود که f روی $K(S)$ نیز تجزیه‌ناپذیر است. دراین‌صورت $\cos\theta/3$، به‌ازای چنین انتخابی برای α، در $C(K(S))$ نیست، زیرا $[K(S)(\cos\theta/3):K(S)]=3$.

۲. تربیع دایره. فرض کنیم S مجموعهٔ متشکل از نقاط $O=(0,0)$ و $P=(1,0)$ باشد. فرض کنیم $R=(x,0)$ نقطه‌ای باشد که مساحت مربع به‌ضلع OR مساوی با مساحت دایرهٔ به‌مرکز O و مار بر P باشد. مسئله این‌است که مشخص کنیم آیا $R\in C(S)$؛ یا به‌عبارت معادل، $x\in C(\mathbf{Q})$. داریم $\pi=x^2$ و معلوم است که π روی $\mathbf{Q}$ جبری نیست. از آنجایی که هرعضو $C(\mathbf{Q})$ روی $\mathbf{Q}$ جبری است، پس $R\notin C(S)$؛ بنابراین تربیع دایرهٔ واحد ممکن نیست.

۳. تضعیف مکعب. فرض کنیم S مجموعهٔ متشکل از $O=(0,0)$ و $P=(1,0)$ باشد. فرض کنیم $R=(x,0)$ نقطه‌ای باشد که حجم مکعب به‌ضلعی چون OR مساوی با دوبرابر حجم مکعب به‌ضلعی چون OP باشد. مسئله این است که مشخص کنیم آیا R در $C(S)$ است؛ یا به‌عبارت معادل، $x\in C(\mathbf{Q})$. آشکارا x یک ریشهٔ چندجمله‌ای $f=X^3-2$ است. از آنجایی که گروه چندجملهٔ f روی $\mathbf{Q}$ مساوی S_3 است، داریم $R\notin C(S)$.

۴. ترسیم چندضلعیهای منتظم با تعداد اضلاع مفروض. فرض کنیم S مجموعهٔ متشکل از نقاط $O=(0,0)$ و $P=(1,0)$ باشد. فرض کنیم Δ یک چند ضلعی منتظم با h ضلع باشد که یکی از رئوسش نقطهٔ P و محاط در دایرهٔ به‌مرکز O و به‌شعاع OP باشد. مسئله این است که مشخص کنیم آیا رئوس Δ در $C(S)$ هستند؛ آشکارا این‌مطلب معادل است با اینکه مشخص شود نقطهٔ $R=(\cos 2\pi/h, \sin 2\pi/h)$ به $C(S)$ تعلق دارد یا خیر. فرض کنیم $\rho=\exp(2\pi i/h)$، $i=\sqrt{-1}$. داریم $\cos 2\pi/h=(\rho+\rho^{-1})/2$. بنابراین $[\mathbf{Q}(\rho):\mathbf{Q}(\cos 2\pi/h)]=2$. حالا $\mathbf{Q}(\rho)/\mathbf{Q}$ یک توسیع گالوایی است زیرا ρ یک ریشهٔ hام اولیهٔ واحد است. بنابر قضیهٔ اصلی ۴، ملاحظه می‌کنیم $R\in C(S)$ اگروفقط اگر به‌ازای عددی صحیح چون m، $[\mathbf{Q}(\rho):\mathbf{Q}]=2^m$.

اکنون فرض می‌کنیم h عددی اول باشد. نشان می‌دهیم که رئوس Δ در $C(S)$ هستند

اگروفقط اگر h یك عدد اول‌فرما باشد،یعنی به‌ازای عددی‌صحیح مانند λ، $h=۲^{۲^\lambda}+۱$.

از آنجایی‌که

$$۱-X^h=(۱-X)(۱+X+\cdots+X^{h-۱})$$

ρ یك ریشهٔ چندجمله‌ای $f=۱+X+\ldots+X^{h-۱}$ است.

می‌نویسیم $X=Y+۱$. در این‌صورت $f(X)=g(Y)$ که در آن

$$g(Y)=Y^{h-۱}+\binom{h}{۱}Y^{h-۲}+\cdots+\binom{h}{h-۱}$$

چون h عددی اول است، h عدد $\binom{h}{j}$، $۱\leqslant j\leqslant h-۱$، را عاد می‌کند و $h^۲$ عدد $h=\binom{h}{h-۱}$ را عاد نمی‌کند. لذا، بنابرمحك ایزنشتاین (قضیهٔ ۸، فصل۲)، g و در نتیجه h، روی $\mathbf{Q}$ تجزیه‌ناپذیر است. پس $[\mathbf{Q}(\rho):\mathbf{Q}]=h-۱$. بنابراین R در $C(S)$ است اگروفقط اگر $h=۱+۲^m$. به‌سهولت دیده می‌شود که (به‌دلیل اول بودن h) عدد m، به‌ازای عددی صحیح، بـه‌شکل ۲^λ است، یعنی h یك عدد اول فرماست. اگر قراردهیم $\lambda=۰, ۱, ۲$، داریم $h=۳, ۵, ۱۷$ که اعدادی اول هستند. بنابراین‌یك مثلث متساوی‌الاضلاع، یك پنج ضلعی ویك هفده ضلعی منتظم را می‌توان با خط‌کش وپرگار رسم کرد.

نامتناهی بودن تعداد اعداد اول فرما معلوم نیست.

فهرست منابع

1. E. Artin: *Galois Theory*, Notre Dame, Indiana, (1959).
2. N. Bourbaki: *Algébre*, Chap. V, Hermann, Paris, (1950).
3. N. Jacobson: *Lectures in Abstract Algebra*, V. III, Van Nostrand, Princeton, (1964).
4. K. G. Ramanathan: *Lectures on the Algebraic Theory of Fields*, Tata Institute of Fundamental Research, (1954).
5. B. L. Van der Waerden: *Modern Algebra*, Vol. I, Ungar, NewYork, (1918).

واژنامهٔ انگلیسی به فارسی

algebraic extension	توسیع جبری
algebraically closed field	میدان جبراً بسته
alternating group	گروه متناوب
characteristic	مشخصه
conjugacy class	ردهٔ مزدوجی
construction	ترسیم
cyclic extension	توسیع دوری
doubling the cube	تضعیف مکعب
extension	توسیع
field extension	توسیع میدان
finite extension	توسیع متناهی
finite normal extension	توسیع نرمال متناهی
finite separable extension	توسیع جداپذیر متناهی
fixed field	میدان ثابت
Galois extension	توسیع گالوایی
Galois group	گروه گالوایی
inclusion map	نگاشت شمول
integral domain	حوزهٔ صحیح

invariant	پایا
irreducible	تجزیه‌ناپذیر
k-linear map	k- نگاشت خطی
Lagrange resolvent	بسط لاگرانژ
multiple root	ریشهٔ مکرر
permutation	جایگشت
polynomial ring	حلقهٔ چندجمله‌ایها
prime field	میدان اول
principle ideal domain	حوزهٔ ایدال اصلی
quotient field	میدان خارج قسمت
radical extension	توسیع رادیکالی
rational function	تابع گویا
residue classes	رده‌های مانده‌ای
separable extension	توسیع جداپذیر
simple extension	توسیع ساده
solvability by radicals	حلپذیری با رادیکالها
splitting field	میدان شکافنده
squaring the circle	تربیع دایره
stable closure	بستار پایدار
transcendental number	عدد متعالی
up to an isomorphism	در حد ایزومورفیسم

واژه‌نامهٔ فارسی به انگلیسی

stable closure	بستار پایدار
Lagrange resolvent	بسط لاگرانژ
invariant	پایا
rational function	تابع گویا
irreducible	تجزیه ناپذیر
squaring the circle	تربیع دایره
construction	ترسیم
doubling the cube	تضعیف مکعب
extension	توسیع
algebraic extension	توسیع جبری
separable extension	توسیع جداپذیر
finite separable extension	توسیع جداپذیر متناهی
cyclic extension	توسیع دوری
radical extension	توسیع رادیکالی
simple extension	توسیع ساده
Galois extension	توسیع گالوایی
finite extension	توسیع متناهی
field extension	توسیع میدان
finite normal extension	توسیع نرمال متناهی
permutation	جایگشت

solvability by radicals	حلپذیری با رادیکالها
polynomial ring	حلقهٔ چندجمله‌ایها
principle ideal domain	حوزهٔ ایدال اصلی
integral domain	حوزهٔ صحیح
up to an isomorphism	در حد ایزومورفیسم
conjugacy class	ردهٔ مزدوجی
residue classes	رده‌های مانده‌ای
multiple root	ریشهٔ مکرر
transcendental number	عدد متعالی
k-linear map	k- نگاشت خطی
Galois group	گروه گالوایی
alternating group	گروه متناوب
characteristic	مشخصه
prime field	میدان اول
fixed field	میدان ثابت
algebraically closed field	میدان جبراً بسته
quotient field	میدان خارج قسمت
splitting field	میدان شکافنده
inclusion map	نگاشت شمول

فهرست راهنما