دانشگاه رازی

نظریه گالوا

نویسنده: ژوزف روتمن

مترجم: علی نجات دارابی

نظریهٔ گالوا

نوشتهٔ : ژوزف روتمن

ترجمهٔ : علی‌نجات دارابی

انتشارات طاق‌بستان

۱۳۸۰

روتمن، ژوزف
نظریه گالوا / نوشته ژوزف روتمن، ترجمه علی
نجات دارابی. -کرمانشاه : انتشارات طاق‌بستان،
۱۳۷۹
خ، ۱۶۹ ص .
ا. نظریه گالوا. الف. دارابی، علی‌نجات، مترجم،
ب . عنوان
QA
۲۱۱ ۵۱۲/۳۲
۶ ن ۹ ر /

انتشارات دانشگاه رازی
انتشارات طاق‌بستان

عنوان: نظریهٔ گالوا
نویسنده: ژوزف روتمن
مترجم: علی‌نجات دارابی
حروف نگار: اشرف ملکی
لیتوگرافی: سپهر
حروف‌چینی: انتشارات‌طاق‌بستان - تلفکس :۷۷۱۶۴۳
چاپ : چاپ و انتشارات غرب
نوبت چاپ: اول - کرمانشاه، ۱۳۷۹
قطع: وزیری / ۱۶۹ ص
شمارگان: ۳۰۰۰ جلد
قیمت: ۷۰۰ تومان
شابک: ۹۶۴-۵۵۵۱-۸۲-x ISBN:964-5551-82-x

این کتاب ترجمه‌ای است از کتاب

Joseph Rotman , Galois Theory

Springer - Verlag , New York Inc , 1990

مقدمهٔ مترجم

درس نظریهٔ گالوا در حال حاضر تحت عنوان درس جبر ۲ از جمله دروس الزامی رشته‌های ریاضی محض و ریاضی دبیری است. بعلاوه ، با توجه به اینکه موضوع نظریهٔ گالوا یکی از جذابترین شاخه‌های علم جبر است، فراهم کردن متونی به فارسی برای علاقمندان به این موضوع از اهمیتی خاص برخوردار است. طی چندین سال تدریس این درس در گروه ریاضی دانشگاه رازی، علاوه بر متون موجود در این مقوله، سرانجام کتاب نظریهٔ گالوای ژوزف روتمن را برای تدریس و ترجمه انتخاب کردم. این کتاب که از جملهٔ جدیدترین نشریات در رشتهٔ نظریهٔ گالوا (۱۹۹۰) می‌باشد، کتابی درسی و متناسب با سرفصلهای مصوب می‌باشد.

در ترجمهٔ این کتاب ضمن پایبندی به امانت، سلامت متن نیز مد نظر بوده است. اصطلاحات ریاضی براساس واژه‌نامهٔ ریاضی انجمن ریاضی ایران تهیه شده است، و امیدوارم که در بین معادلهای موجود بهترین را انتخاب کرده باشم. به هر تقدیر از تمام دانشجویان عزیز و همکاران محترم دانشگاهی انتظار دارم که بنده را از نظرات عالمانه و انتقادی خویش آگاه سازند.

وظیفهٔ خود می‌دانم که از معاونت محترم پژوهشی و مدیر محترم پژوهشی دانشگاه رازی، مدیر محترم انتشارات طاق‌بستان و کارکنان شریف آن تشکر و قدردانی کنم .

در پایان از همسرم سپاسگزارم که با صرف وقتی که باید در خدمت ایشان می‌بودم این اثر فراهم شد.

و من‌ا... التوفیق

علی‌نجات دارابی

عضو هیأت علمی دانشگاه رازی

مقدمهٔ مؤلف

این کتاب کوچک آموزش نتایج پایهٔ قضیهٔ اساسی نظریهٔ گالوا، حل‌ناپذیری درجهٔ پنجم، توصیف حل‌پذیری چند جمله‌ایها بوسیله رادیکالها، کاربردها و گروههای گالوای چند جمله‌ایهای از درجات پایین را به طور واضح و مؤثر طراحی می‌کند. فرض شده است که خواننده درسهای مقدماتی در جبر خطی (با مفهوم بعد یک فضای برداری بر یک میدان دلخواه از اسکالرها آشنا شده است) و جبر مجرد (یعنی نخستین درس که گروهها و حلقه‌ها و هومومورفیسم‌ها را ذکر می‌کند) را داشته است. با وجود این، بحث حلقه‌های جابجایی، باشروع از تعریف در متن آغاز شده است. این گزارش به منظور روح دادن به بازبینی چیزهای گذشته نوشته شده است، و بنابراین حتی اگر کامل باشد، ممکن است برای کسی که قبلاً هیچی از آن را ندیده است زود باشد. تعداد زیادی از تمرینات همراه این موضوع یک تفسیر سریعتر از آن را مجاز می‌سازد. وقتی این درس را آموزش می‌دهم، معمولاً با آسودگی خاطر از حساب نظریهٔ گروه، همچنین از تعریف، که شامل بعضی از قضایا و مثالها که برای این متن لزومی ندارند شروع می‌کنم. در اینجا، مصمم بودم نتایج مورد نیاز نظریهٔ گروه را به پیوست‌ها: واژه‌نامهٔ عبارات و برهان قضایا موکول کنم. ساختمان متن را با تاکید بر این حقیقت که چند جمله‌ایها و میدانها جایگذاری طبیعی می‌باشند، وگروهها مساعدت کننده نامیده شده‌اند، انتخاب کرده‌ام.

تمام بحث نظریهٔ میدان سفر به قضیهٔ بزرگ گالوا را به تأخیر می‌اندازد. بنابر این، بعضی مباحث مهم (جداپذیری، چند جمله‌ایهای تقسیم دایره، نرم‌ها، توسیع‌های نامتناهی، توابع متقارن) تنها یک تصدیق زودگذر را دریافت می‌کنند و بعضی دیگر (بستارجبری، درجهٔ متعالی، نتایج، اثرها، پایه‌های نرمال، قضیهٔ کومر[1]) روی هم رفته سنگین می‌باشند و به اعتقاد من این مطالب بعد از اینکه خواننده مفاهیم بنیادی را درک کرد اتخاذ شوند.

تعبیر مطلوب من از نظریهٔ گالوا از امیل آرتین[2]، کاپلانسکی[3] و واندرواردن[4] می‌باشد،

---

1. Kummer .

2. E.Artin

وبسیارمدیون آنهامی باشم. برای پیوست «سبک قدیم نظریهٔ گالوا» به گزارشهای جدید، مخصوصاً [Edwards]، [Gaal]، [Tignol] و [Van der waerden]، و کتابهای قدیمی تر، مخصوصاً [Dehn] (و [Burnside and panton] و [Dickson] و [Netto]) تکیه کردم.
از همکارانم در دانشگاه ایلی نویز[5]، اوربانا[6]، که سالها ابهامات را توضیح دادند متشکرم.
همچنین از پیتر برانفلد[7] به خاطر پیشنهاداتش که پیوست ۳ را بهتر کرد و از پیتر ام. نویمان[8] به خاطر نوشتن آموخته‌هایش در پیوست ۴ متشکرم.

امیدوارم که این ویژه نگاشت ، نظریهٔ گالوای لذت بخش را هم یاد و هم آموزش بدهد، و دیگران همانند من زیبایی آن را لمس کنند.

ژوزف روتمن

اوربانا، ایلی نویز

۱۹۹۰

---

3. Kaplansky
4. Van der waerden
5. Illinois
6. Urbana
7. Peter Braunfeld
8. Peter M.Neumann

به خواننده

تمرینات را همانند قسمتی از متن مورد توجه قراردهید، گزاره‌های مربوطه را خوانده و سعی کنید آنها را حل کنید. ستارهٔ قبل از یک تمرین نشانگر آن است که در جای دیگر متن، شاید در یک برهان، به آن اشاره خواهد شد. یک پی‌آمد علامت‌گذاری شده آن است که منظور از قضیهٔ ۵، قضیهٔ پنجم در متن است، قضیهٔ A5، قضیهٔ پنجم در پیوست ۲ (نظریهٔ گروه) می‌باشد، و قضیهٔ B5 قضیهٔ پنجم در پیوست ۳ (ترسیم بوسیلهٔ خط کش و پرگار) می‌باشد.

فهرست مطالب

عنوان | **صفحه**

فهرست مطالب

عنوان **صفحه**

نظریهٔ گالوا

نظریهٔ گالوا اثر متقابل بین چند جمله‌ایها، میدانها و گروهها می‌باشد. فرمول حل معادلهٔ درجهٔ دوم که ریشه‌های معادلهٔ درجهٔ دوم را به دست می‌دهد اساساً بوسیلهٔ بابلیها شناخته شده است. فرمولهای درجهٔ سوم و چهارم در اواسط قرن شانزدهم شناخته شدند. حدوداً سیصدسال بعد، آبل (۱۸۲۴) با استفاده از ایده‌های لاگرانژ و کوشی ثابت کرد که یک چند جمله‌ای درجهٔ پنجم وجود دارد که ریشه‌های آن را نمی‌توان بوسیلهٔ یک فرمول شامل اعمال جبری واقع بر ضرایب چند جمله‌ای به دست آورد. (در حقیقت رافینی[1] در سال ۱۷۹۹ یک برهان از نتیجهٔ مشابه را طرح‌ریزی کرد، اما این برهان اختلاف زیادی با برهان هم عصرش داشت و از این رو پذیرفته نشد.) در سال ۱۸۲۹ آبل یک شرط کافی برای اینکه یک چند جمله‌ای (از هر درجه) دارای چنین فرمولی برحسب ریشه‌هایش باشد، ارائه داد. (این قضیه یک دلیل برای این است که گروههای جابجایی راگروههای آبلی نامیده‌اند.) وگالوا در سال ۱۸۳۱ یک شرط لازم وکافی برای معین کردن مسأله به طور کامل ارائه داد. در اینجا این قضیه را ثابت می‌کنیم .

حلقه‌ها

دستگاه جبری شامل میدانهاو چند جمله‌ایها یک حلقهٔ جابجایی است. فرض می‌کنیم که خواننده با کلمات حلقه و هومورفیسم آشنایی دارد. بنابراین، نه با آسودگی خاطر، اما بحث ما کامل است .

تعریف: مجموعهٔ R همراه با دو عمل دوتایی جمع $(r, r') \longrightarrow r + r'$ و ضرب $(r, r') \longrightarrow rr'$ یک حلقهٔ جابجایی و یکدار است، در صورتی که

---

1. Ruffini

(اَ) $(R, +)$ یک گروه آبلی باشد.

(ب) ضرب دارای خاصیت جابجایی و شرکت‌پذیری باشد.

(ج) عضو 1 از R موجود باشد، به طوری که به ازای هر r از R، $1r = r$.

(د) قانون توزیع پذیری برقرارباشد، یعنی

$$\forall\, r, s, t \in R \;,\quad r(s+t) = rs + rt$$

گروه جمعی R گروه آبلی به دست آمده از آن صرفنظر از عمل ضرب R است .

از اینجا به بعد منظور از یک حلقه، حلقه‌ای جابجایی و یکدار است .

مثالها

۱ . Z (مجموعهٔ اعدادصحیح)، Q (مجموعهٔاعداد گویا)، R (مجموعهٔ اعداد حقیقی)، C (مجموعهٔاعدادمختلط)، هرکدام یک حلقه می‌باشند.

۲ .به ازای عدد صحیح و مثبت n ، حلقهٔ Z_n از مانده‌های صحیح به هنگ n را مانند زیر تعریف می‌کنیم. این اعضا زیر مجموعه‌ای از Z می‌باشند.

$$\bar{a} = \{\, m \in Z ; m \equiv a \pmod n \} = \{ m \in Z ; m = a + kn , \exists k \in Z \}$$

که درآن a عضو Z است. ($\bar{a}$ ردهٔ همنهشتی a به هنگ n نامیده‌شده‌است).جمع و ضرب بوسیلهٔ $\bar{a} \cdot \bar{b} = \overline{ab}$ و $\bar{a} + \bar{b} = \overline{a+b}$ داده شده است. و $\bar{1}$ ، واحد حلقه است . تحقیق اینکه این دو عمل دوتایی خوشتعریف‌اند (یعنی به انتخابهای $\bar{a}$ و $\bar{b}$ بستگی ندارند) و Z_n را به یک حلقه تبدیل می‌کنند ساده است .

توجه داریم که Z_n دقیقاً دارای n عضو است: اگر $a \in Z$، آنگاه یک عدد صحیح r، $0 \le r < n$ موجود است به طوری که $\bar{a} = \bar{r}$ ، بعلاوه رده‌های همنهشتی $\bar{r}$ برای r نمایش داده شده در برد همگی متمایز می‌باشند.

۳ .اگر R یک حلقه باشد، آنگاه چند جمله‌ای $f(x)$ با ضرایب در R (به طور

خلاصه، یک چند جمله‌ای بـر R) را دنبالهٔ $f(x) = (r_0 , r_1 , \ldots , r_n , 0,0,\ldots)$ تعریف می‌کنیم که در آن به ازای هـر i ، $r_i \in R$ و بـه ازای هـر $i>n$ ، $r_i = 0$. اگـر $g(x) = (s_0 ,s_1 , \ldots , s_m , 0,0,\ldots)$ یک چند جمله‌ای دیگر بـر R بـاشد، در ایـن صورت $f(x) = g(x)$ اگر و فقط اگر به ازای هر i ، $r_i = s_i$. مجموعهٔ تمام این چند جمله‌ایها را با $R[x]$ نشان می‌دهیم، و اعمال جمع و ضرب را بر $R[x]$ مانند زیر تعریف می‌کنیم :

$(r_0 , r_1 , \ldots, r_i ,\ldots) + (s_0,s_1,\ldots,s_i,\ldots) = (r_0 + s_0 , r_1 + s_1,\ldots,r_i+s_i,\ldots)$ و $(r_0,r_1,\ldots,r_i,\ldots) (s_0,s_1,\ldots,s_j,\ldots) = (t_0 ,t_1 , \ldots , t_k , \ldots)$ کـه در آن $t_0 = r_0s_0$, $t_1 = r_0s_1 + r_1s_0$ و به طورکلی $t_k = \sum_{i=0}^{k} r_i s_{k-i}$. فرض کنیم $(1 , 0 , 0 , \ldots)$ به 1 خلاصه شده باشد. (اکنون دو معنی برای این نماد وجود دارد.) تحقیق اینکه $R[x]$ یک حلقه ، حلقهٔ چند جمله‌ای بر R است ، ساده اما خسته کننده است .

معنی حرف x در نماد $f(x)$ چیست؟ فرض کنیم که $x = (0,1,0,0,\ldots)$ نمایش یک عضو خاص از $R[x]$ باشد. به سادگی ثابت مـی‌شود کـه $x^2 = (0,0,1,0,\ldots)$. و بو سیلهٔ استقراء ثابت می‌شود که x^i همه جا صـفر بـجز 1 در مکـان i ام است . اکـنون خواننده می‌تواند ثابت کند که

$$f(x) = (r_0 , r_1 , \ldots , r_n, 0 , \ldots) = r_0 + r_1x + \ldots + r_nx^n = \sum r_ix^i$$

(اگر r_0 را با $(r_0 , 0,0,\ldots)$ در $R[x]$ همانند کنیم.) توجه کنید که x یک عضو حلقه می‌باشد نه یک متغیر، و نقش آن همانند یک متغیراست ، به هرحال در تمرین ۱۸ داده شده است .

یادآوری می‌کنیم که خواننده واژهٔ متداول $f(x) = r_0 + r_1 x + \ldots + r_nx^n$ را

مربوط سازد. r_n ضریب پیشرو $f(x)$ است ،که n بزرگترین عدد صحیح با $r_n \neq 0$ است، n را درجهٔ چندجمله‌ای $f(x)$ نامیم و آن را با ∂f نشان می‌دهیم . هرچند جمله‌ای بجز $0=(0,0,...)$ دارای یک درجه است .

چند جمله‌ای تکین چند جمله‌ای است که دارای ضریب پیشرو ۱ است . r_0 جملهٔ ثابت $f(x)$ است ، یک چند جمله‌ای ثابت چند جمله‌ای صفر ، یا یک چند جمله‌ای از درجهٔ صفر است ، چند جمله‌ایهای خطی ، درجهٔ دوم ، درجهٔ سوم ، درجهٔ چهارم و درجه پنجم بترتیب دارای درجات ۱ ، ۲ ، ۳ ، ۴ و ۵ می‌باشند.

از جبر خطی به یاد داریم که یک دستگاه همگن خطی بر یک میدان با r معادله و n مجهول اگر $r<n$ دارای یک جواب غیربدیهی است ، اگر $r = n$ ، باید یک دترمینان را امتحان کرد . اگر $f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) = \sum r_i x^i$ ، آنگاه بوسیلهٔ استقراء بر n به سادگی دیده می‌شود که $r_{n-1} = -\sum \alpha_i$ و $r_{n-2} = \sum_{i<j} \alpha_i\alpha_j$ ، $r_{n-3} = -\sum_{i<j<k} \alpha_i\alpha_j\alpha_k$ ، ... ، $r_0 = (-1)^n \alpha_1\alpha_2 \dots \alpha_n$. بنابراین ، منظور از حل یک دستگاه غیرخطی از n معادله و r مجهول یافتن ریشه‌های α_i از چند جمله‌ای $f(x)$ به صورت ضرایب r_i از آن است ، خواهیم دید که اگر $n \geq 5$ این مسأله بوسیلهٔ رادیکالها حل پذیر نیست .

قضیه ۱ : فرض کنیم R یک حلقه باشد.

(آ) به ازای هر r از R ، $0r = 0$.

(ب) به ازای هر r از R ، $(-1)\, r = -r$ (که $-r$ قرینهٔ جمعی r است یعنی $-r+r=0$).

(ج) به ازای هر r از R ، $(-1)\,(-r) = r$. (بویژه $(-1)\,(-1) = 1$).

برهان : (آ) قانون توزیع‌پذیری نتیجه می‌دهد که $0r = (0 + 0)r = 0r + 0r$ و با تفریق $0r$ از دو طرف معادله نتیجه می‌شود که $0r = 0$.

(ب) داریم $0 = 0r = (-1 + 1)r = (-1)r + r$، اکنون $-r$ را به هر دو طرف معادله اضافه می‌کنیم.

(ج) داریم $-r = (-1) = (-r)(-1) + r(-1) = (-r)(-1) - r$ ... $0 = 0(-1) = (-r + r)(-1) = (-r)(-1) + r(-1) = (-r)(-1) - r$، اکنون r را به دو طرف اضافه می‌کنیم. □

اگر R یک حلقه باشد به طوری که $1 = 0$ و اگر $r \in R$ آنگاه $r = 1r = 0r = 0$، بنابراین R دقیقاً شامل یک عضو است که آنرا 0 می‌نامیم. جایز می‌دانیم که این مثال غیرجالب، یک حلقه، یعنی حلقهٔ صفر باشد. اکنون می‌بینیم چرا تقسیم کردن بر 0 جایز نیست. اگر $a,b \in R$، آنگاه باید $\frac{a}{b}$ موجود و یک عضو از R باشد به طوری که $b(\frac{a}{b}) = a$. بویژه اگر $\frac{a}{0}$ موجود باشد، آنگاه آن عضوی از R با $a = 0(\frac{a}{0})$ می‌باشد. اما بنابر قسمت (آ) قضیهٔ ۱، $0(\frac{a}{0}) = 0$ و ناگزیر R حلقهٔ 0 می‌باشد.

حوزه‌های صحیح و میدانها دو نوع از حلقه‌های مهم می‌باشند.

تعریف : حلقهٔ جابجایی R را یک حوزهٔ صحیح نامیم در صورتی که یک حلقه ناصفر و حاصلضرب هر دو عضو ناصفر در R ناصفر باشد.

توجه کنید که Z_6 یک حوزهٔ صحیح نیست زیرا $\bar{2} \neq 0$, $\bar{3} \neq 0$ اما $\bar{2} \cdot \bar{3} = \bar{6} = 0$. البته، این مثال به ازای هر عدد مرکب n به Z_n تعمیم می‌یابد، اگر n عددی اول باشد، Z_n یک حوزهٔ صحیح است. (اگر $\bar{a}\,\bar{b} = 0$ آنگاه n یک مقسوم علیه ab است، بنابر لم اقلیدس، وقتی که n عددی اول باشد، آنگاه n یا a یا b را عادمی‌کند، یعنی، $\bar{a} = 0$ یا $\bar{b} = 0$).

قضیه ۲ : حلقهٔ ناصفر R یک حوزهٔ صحیح است اگر و فقط اگر در قانون حذف صدق

کند، یعنی اگر $ra = rb$ و $r \neq 0$، آنگاه $a = b$.

برهان : فرض کنیم R یک حوزهٔ صحیح باشد، و $ra = rb$ و $r \neq 0$.
آنگاه $r(a-b) = 0$ چون R یک حوزهٔصحیح‌است ، $a-b \neq 0$ غیرممکن است ، بنابر این $a - b = 0$ و $a = b$.

بالعکس ، فرض کنیم قانون حذف برقرارباشد. اگر $r \neq 0$ و $a \neq 0$ و $ra = 0$، آنگاه $ra = 0 = r0$ نتیجه می‌دهد که $a = 0$، که یک تناقض است. □

تمرین :

۱. فرض کنیم $f(x) , g(x) \in R[x]$.

(آ) نشان دهید که جملهٔ ثابت $f(x)\ g(x)$ برابر حاصلضرب جملات ثابت $g(x)$ و $f(x)$ است .

(ب) اگر R یک حوزهٔ صحیح باشد، آنگاه ضریب پیشرو $f(x)\ g(x)$ برابر حاصلضرب ضرایب پیشرو $f(x)$ و $g(x)$ است .

۲. اگر R یک حوزهٔ صحیح باشد و $g(x)\ ,\ f(x)$ چند جمله‌ایهای ناصفر در $R[x]$ باشند، آنگاه $\partial(fg) = \partial f + \partial g$. نتیجه بگیرید که اگر R یک حوزهٔ صحیح باشد، آنگاه $R[x]$ یک حوزهٔ صحیح است .

۳. حلقهٔ چند جمله‌ایهای با دو متغیر بر R که با $R[x,y]$ نشان داده می‌شود را همانند $A[y]$ که $A=R[x]$ تعریف کنید. بوسیلهٔ استقراء حلقهٔ چند جمله‌ایهای با چند متغیر بر R را تعریف‌کنید، و نشان‌دهیدکه اگر R یک حوزهٔ صحیح‌باشد ، آنگاه $R[X_1 ,..., X_n]$ نیز یک حوزهٔ صحیح است .

*۴. عضو $u \in R$ یک یکال است اگر v ای از R موجود باشد که $uv = 1$. ثابت کنید که اگر R یک حوزهٔ صحیح باشد و g,f اعضای R باشند که در روابط

$ug=f$ و $g=vf$ صدق کنند که $u, v\in R$ آنگاه $uv=1$، یعنی u و v یکال می‌باشند.

(توجه کنید که 2 در Z یکال نیست، زیرا $2\times\frac{1}{2}=1$، اما $\frac{1}{2}\notin Z$، از طرفی دیگر 2 در Q یکال است.)

۵. الگوریتم تقسیم را ثابت کنید: اگر R یک حلقه باشد، و $f(x),g(x)\in R[x]$ و اگر ضریب پیشرو $g(x)$ یکال باشد، آنگاه چند جمله‌ایهای $q(x)$ و $r(x)$ به عنوان خارج قسمت و باقیمانده از $R[x]$ وجود دارند به طوری که $f(x)=q(x)g(x)+r(x)$ که در آن $r(x)=0$ یا $\partial r<\partial g$. (تمرین ۱۳ را ببینید.)

۶. ثابت کنید که قضیهٔ دو جمله‌ای در هر حلقهٔ R برقرار است: اگر $n\geq 1$ آنگاه

$(a+b)^n=\sum_{i=0}^{n}\begin{bmatrix}n\\i\end{bmatrix}a^ib^{n-i}$ که $\begin{bmatrix}n\\i\end{bmatrix}=\frac{n!}{i!(n-i)!}$ نمایش ضریب دو جمله‌ای است.(راهنمایی: ابتدا ثابت کنید که $\begin{bmatrix}n\\i\end{bmatrix}=\begin{bmatrix}n-1\\i-1\end{bmatrix}+\begin{bmatrix}n-1\\i\end{bmatrix}$.)

*۷. اگر p عددی اول باشد، ثابت کنید که به ازای هر i که $i\neq 0,p$، p یک مقسوم علیه $\begin{bmatrix}p\\i\end{bmatrix}$ است. (توجه کنید که ۴ یک مقسوم علیه $\begin{bmatrix}4\\2\end{bmatrix}=6$ نیست.)

۸. اگر $f(x)\in R[x]$، مثلاً، $f(x)=r_0+r_1x+\cdots+r_nx^n$، مشتق آن را تعریف می‌کنیم $f'(x)=r_1+2r_2x+\cdots+nr_nx^{n-1}$ ثابت کنید که

$$[f(x)+g(x)]'=f'(x)+g'(x)$$

و

$$[f(x)g(x)]'=f'(x)g(x)+f(x)g'(x)$$

تعریف: حلقهٔ ناصفر R را یک میدان نامیم، در صورتی که $R-\{0\}$ تحت عمل ضرب یک گروه باشد، یعنی هر عضو ناصفرِ R یکال باشد.

Q، R، C و Z_p مثالهایی از میدانها هستند. هر میدان R یک حوزهٔ صحیح است، زیرا از آن نتیجه می‌شود که گروه $R - \{0\}$ تحت عمل ضرب بسته است ولی عکس آن نادرست است، زیرا Z یک حوزهٔ صحیح است که میدان نیست.

تمرین :

۹. (آ) زیر مجموعهٔ S از حلقهٔ R را یک زیر حلقهٔ R نامیم، در صورتی که S شامل 1 و تحت عمل تفریق و ضرب بسته باشد. نشان دهید که اشتراک هر خانواده از زیر حلقه‌های R یک زیر حلقهٔ R است.

(ب) یک زیر میدان زیر حلقه‌ای است که یک میدان باشد. نشان دهید که یک زیر مجموعه از یک حلقه یک زیر میدان است اگر شامل 1 و تحت تفریق و ضرب و وارونها بسته باشد.

*۱۰. نشان دهید که هر اشتراک از زیرمیدانها یک زیر میدان است.

*۱۱. نشان دهید که هر زیر حلقه از یک میدان یک حوزهٔ صحیح است.

عکس تمرین ۱۱ درست است. فرض کنیم R یک حوزهٔ صحیح باشد. میدان کسرهای آن، F، را می‌توان تعریف کرد، F یک میدان شامل R بعنوان یک زیرحلقه است، و F از R دقیقاً همانند ساختن میدان Q از Z ساخته شده است.

به تفصیل فرض کنیم X مجموعهٔ تمام زوجهای مرتب $(a,b)\in R\times R$ با $b\neq 0$ باشد، رابطهٔ ضرب صلیبی بر مجموعهٔ X را مانند زیر تعریف می‌کنیم:

$(a,b)\sim(c,d)$ اگر و فقط اگر $ad = bc$، این نسبت یک رابطهٔ هم ارزی است و دستهٔ هم‌ارز شامل عضو (a,b) را با $\frac{a}{b}$ نشان می‌دهیم. اعمال جمع و ضرب بر مجموعهٔ F متشکل از تمام دسته‌های هم ارز را مانند زیر تعریف می‌کنیم $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ و $\frac{a}{b}.\frac{c}{d}=\frac{ac}{bd}$. (توجه کنید که $bd\neq 0$ زیرا R یک حوزهٔ صحیح است.) تحقیق اینکه

این اعمال خوشتعریف‌اند و F یک میدان است ساده می‌باشد. بالاخره، می‌توان $r \in R$ را با کسر $\frac{r}{1}$ تعریف کرد، و همچنین R را می‌توان به عنوان یک زیر حلقه از F در نظر گرفت.

۱۲* . (آ) نشان دهید که $Z_p[x]$ یک حوزهٔ صحیح نامتناهی شامل Z_p به عنوانِ یک زیرحلقه است.

(ب) نشان دهید که یک میدان نامتناهی شامل Z_p به عنوان یک زیرمیدان وجود دارد.

۱۳* . اگر R یک حوزهٔصحیح باشد، آنگاه خارج قسمت وباقیماندهٔ الگوریتم تقسیم منحصر بفرد می‌باشند. (حلقه‌های R، به عنوان مثال Z_4، که در آنها حکم متناظر نادرست است وجوددارند.)

۱۴ . نشان دهید که $R[x]$ هرگز میدان نیست.

۱۵ . نشان دهید که Z_n یک میدان است اگر و فقط اگر n عددی اول باشد.

هومورفیسم‌ها و ایده‌آلها

تعریف: اگر R و S دو حلقه باشند، آنگاه تابع $\psi : R \longrightarrow S$ یک هومورفیسم حلقه (یا یک نگاشت حلقه) است اگر به ازای هر r و r' و 1 از R:

$$\psi(r+r')= \psi(r)+ \psi(r') \text{ و } \psi(rr')= \psi(r)\, \psi(r') \text{ و } \psi(1)=1$$

هومورفیسم حلقهٔ $\psi : R \longrightarrow S$ یک ایزومورفیسم است اگر ψ دوسویی[1] باشد، در این حالت‌گوییم‌که R و S ایزومورف‌اندومی‌نویسیم $R \cong S$.

---

۱ - تابع $\psi : X \longrightarrow Y$ را یک به یک نامیم اگر از $\psi(x) = \psi(x')$ نتیجه شود که $x = x'$، و تابع ψ را پوشانامیم اگر به ازای هر y از Y، عضوی از X مانند x موجود باشد به طوری که $\psi(x)=y$ تابع ψ را دوسویی نامیم در صورتی که یک به یک و پوشا باشد.

تمرین :

۱۶ . رابطهٔ $R \cong S$ بر خانوادهٔ تمام حلقه‌ها یک رابطهٔ هم ارزی است .

۱۷ . نگاشت طبیعی $Z \longrightarrow Z_n$ تعریف شده بوسیلهٔ $a \longrightarrow \bar{a}$ یک هomomorfism پوشای حلقه‌ها می‌باشد.

*۱۸ . اگر $a \in R$، نگاشت $e_a : R[x] \longrightarrow R$ را با ضابطهٔ $e_a(f(x)) = \Sigma r_i a^i$ تعریف می‌کنیم . ثابت کنید که e_a یک هومورفیسم حلقه است . (e_a نگاشت ارزیاب در a نامیده شده است.) اگر $f(a) = 0$ ، آنگاه a یک ریشه $f(x)$ نامیده می‌شود.

(این تمرین اجازه می‌دهد که x را به عنوان یک متغیر بر برد R در نظر گرفت ، یعنی هر چند جمله‌ای $f(x) \in R[x]$ یک تابع $R \longrightarrow R$ را مشخص می‌کند . تمرین بعدی را ببینید.)

*۱۹ . یک مثال از چند جمله‌ایهای متمایز $f(x)$ و $g(x)$ از $Z_p[x]$ ارائه دهید به طوری‌که به ازای هر a از Z_p ، $f(a) = g(a)$.

(چند جمله‌ایهای متمایز (همهٔ ضرایب آنها یکی نیستند) ممکن است یک تابع مشابه را مشخص کنند ، این یک دلیل برای تعریف ما از چند جمله‌ایها در چنین روش صوری می‌باشد. در حقیقت ، اگر F یک میدان متناهی باشد (چنین میدانهایی غیر از Z_p وجود دارند) ، تنها تعدادی متناهی توابع $F \longrightarrow F$ وجود دارند. بعد از قضیه ۱۱ خواهیم دید که اگر Z_p بوسیلهٔ هر میدان نامتناهی جایگزین شود این تمرین نادرست است .)

*۲۰ . (آ) نشان دهید که مجموعهٔ همهٔ ثابتهای در $R[x]$ که آن را با $\tilde{R}$ نشان می‌دهیم یک زیر حلقه از $R[x]$ است و $f : R \longrightarrow \tilde{R}$ تعریف شده با ضابطهٔ

$r \longrightarrow (r,0,0,\ldots)$ یک ایزومورفیسم است .

(ب) فرض کنیم R یک حوزهٔ صحیح با میدان کسرهای F باشد. نشان دهید که مجموعهٔ $\{ \frac{r}{1} \in F \,;\, r \in R \}$ یک زیر حلقهٔ F ایزومورف با R است.

۲۱ . اگر $a \in R$ در R یکال باشد و $\psi : R \longrightarrow S$ یک همومورفیسم حلقه‌ها باشد، آنگاه $\psi(a)$ در S یکال است .

۲۲ . اگر $\sigma : R \longrightarrow S$ یک همومورفیسم حلقه باشد، آنگاه $\sigma^* : R[x] \longrightarrow S[x]$ تعریف شده بوسیلهٔ $\Sigma r_i x^i \longrightarrow \Sigma \sigma(r_i) x^i$، نیز یک همومورفیسم حلقه است، اگر σ یک ایزومورفیسم باشد، آنگاه σ^* نیز یک ایزومورفیسم است .

۲۳ . اگر $\psi : R \longrightarrow S$ یک همومورفیسم حلقه باشد، آنگاه تصویر ψ یعنی $\mathrm{Im}\psi$ یک زیر حلقهٔ S است.

تعریف: یک‌ایده‌آل در حلقهٔ R یک زیر مجموعهٔ I شامل صفر است ، به طوری که

(آ) به ازای هر b,a از I نتیجه شود که $a - b \in I$.

(ب) به ازای هر r از R و هر a از I نتیجه شود که $ra \in I$.

هر حلقهٔ R شامل ایده‌آلهای R و $\{0\}$ است.

تمرین :

۲۴ . اگر $\psi : R \longrightarrow S$ یک همومورفیسم حلقه‌باشد،آنگاه هستهٔ آن، $\ker\psi = \{ r \in R \,;\, \psi(r) = 0 \}$ یک ایده‌آل R است.

۲۵ . تابع $R[x] \longrightarrow R$ ، که به هر چندجمله‌ای جملهٔ ثابت آن را مربوط می‌سازد، یک همومورفیسم حلقه است. هستهٔ این همومورفیسم را بیابید.

۲۶ . اگر $r_0 \in R$ ، آنگاه $\{rr_0 ;\, r \in R\}$ یک ایده‌آل در R است. (ایده‌آل اصلی تولید شده بوسیلهٔ r_0 نامیده شده است و با (r_0) نشان داده می‌شود.)

*۲۷. فرض کنیم u یک یکال در حلقهٔ R باشد.

(آ) اگر ایده‌آل I شامل u باشد، آنگاه $I = R$.

(ب) اگر $r \in R$، آنگاه $(r) = (ur)$.

(ج) اگر R یک حوزهٔ صحیح باشد و $r,s \in R$، آنگاه $(r) = (s)$ اگر و فقط اگر به ازای یکالی مانند u در R، $s = ur$.

۲۸. نشان دهید که 1 و -1 تنها یکالهای Z می‌باشند.

*۲۹. اگر F یک میدان باشد، آنگاه تنها یکالهای در $F[x]$ ثابتهای ناصفر هستند.

*۳۰. حلقهٔ R یک میدان است اگر و فقط اگر تنها ایده‌آلهای آن R و $\{0\}$ باشند.

۳۱. اشتراک هر خانواده از ایده‌آلهای R یک ایده‌آل در R است.

*۳۲. اگر $a_1, a_2, \dots, a_n$ اعضایی در حلقهٔ R باشند، آنگاه مجموعهٔ همهٔ ترکیبات خطی، $I = \{ r_1a_1 + r_2a_2 + \cdots + r_n a_n ; r_i \in R , i = 1, 2, \dots, n \}$ یک ایده‌آل در R است، در حقیقت I کوچکترین ایده‌آل شامل $a_1, a_2, \dots, a_n$ است. (یعنی اگر J هر ایده‌آل دیگری از R شامل $a_1, a_2, \dots, a_n$ باشد، آنگاه $I \subset J$).

*۳۳. مجموعهٔ تمام چند جمله‌ایهای $f(x)$ از $Z[x]$ دارای جملهٔ ثابت زوج یک ایده‌آل در $Z[x]$ است، این ایده‌آل شامل تمام ترکیبات خطی x و ۲ می‌باشد.

۳۴. هومورفیسم حلقهٔ $\psi : R \longrightarrow S$ یک به یک است اگر و فقط اگر هستهٔ آن برابر $\{0\}$ باشد. نتیجه بگیرید (با استفاده از تمرین ۳۰) که اگر R یک میدان باشد و $S \neq 0$، آنگاه ψ باید یک به یک و $\mathrm{Im}\psi$ یک زیر میدان از S ایزومورف با R باشد.

حلقه‌های خارج قسمتی

فرض کنیم I یک ایده‌آل حلقهٔ R باشد. برای یک لحظه عمل ضرب را فراموش می‌کنیم، I یک زیرگروه جمعی R است، بعلاوه R آبلی است، درنتیجه I یک زیرگروه نرمال است، بنابراین گروه خارج قسمتی $\frac{R}{I}$ وجود دارد. عناصر $\frac{R}{I}$ همدسته‌های $r + I$ هستند، که $r \in R$، و جمع بوسیلهٔ $(r+I)+(r'+I)=(r+r')+I$ داده شده است. بویژه $0 + I = I$ عضو همانی است. توجه داریم که $r+I=r'+I$ اگر و فقط اگر $r-r' \in I$. بالاخره، به خاطر داریم که هومورفیسم طبیعی $\pi : R \longrightarrow \frac{R}{I}$ تعریف شده بوسیلهٔ $\pi(r) = r + I$ یک هومورفیسم گروه است.

قضیه ۳: فرض کنیم I یک ایده‌ال در حلقهٔ R باشد، در این صورت گروه آبلی $\frac{R}{I}$ همراه با عمل ضرب تشکیل یک حلقه می‌دهد و نگاشت $\pi : R \longrightarrow \frac{R}{I}$ یک هومورفیسم حلقه است.

برهان: عمل ضرب بر $\frac{R}{I}$ را بوسیلهٔ $(r + I)(r' + I) = rr' + I$ تعریف می‌کنیم. دیدن اینکه این عمل خوشتعریف است، فرض کنیم که $r+I=s+I$ و $r'+I=s'+I$ باید نشان دهیم که $rr' + I = ss' + I$، یعنی $rr' - ss' \in I$. اما

$$rr' - ss' = (rr' - rs') + (rs' - ss') = r(r' - s') + (r - s)s'$$

اکنون بنابر فرض $r' - s' \in I$ و $r - s \in I$، بنابراین $r(r'-s') \in I$ و $(r-s)s' \in I$، زیرا I یک ایده‌آل است. بالاخره، مجموع دو عضو از I، عضوی از I است، لذا $rr'+I=ss'+I$ نتیجهٔ مطلوب است.

دیدن اینکه گروه آبلی $\frac{R}{I}$ با این ضرب یک حلقه است ساده می‌باشد. رابطهٔ $(r+I)(r'+I)=rr'+I$ می‌گوید که $\pi(r)\pi(r')=\pi(rr')$ که $\pi(r) = r + I$ نگاشت طبیعی است، در نتیجه π یک هومورفیسم حلقه است. □

تعریف: اگر I یک ایده‌آل حلقهٔ R باشد، آنگاه $\frac{R}{I}$ را حلقهٔ خارج قسمتی R به هنگ I نامیم.

به عنوان مثال، فرض کنیم $R = F[x]$، حلقهٔ چند جمله‌ایها بر میدان F، و I ایده‌آل اصلی شامل تمام مضارب چند جمله‌ای مشخص $p(x)$ از درجهٔ n باشد. اگر $f(x)\in F[x]$، آنگاه بنابر الگوریتم تقسیم چند جمله‌ایهای $q(x)$ و $r(x)$ از $F[x]$ موجود می‌باشند، به طوری که $f(x)=p(x)q(x)+r(x)$ که در آن $r(x) = 0$ یا $\partial r < n$. توجه کنید که $f(x) + I = r(x) + I$، بنابراین می‌توانیم فرض کنیم که هر همدسته (بجز خود I) دارای یک نمایش از درجهٔ کمتر از n است. ضرب در $\frac{R}{I}$ چیست؟ به طور معمول، $(f(x)+I)(g(x) + I)=f(x)g(x)+I$، اما در اینجا می‌توانیم $f(x)g(x)$ را بوسیلهٔ باقیماندهٔ تقسیم آن بر $p(x)$ جایگزین کنیم.

بویژه، $F = R$ و $p(x) = x^2 + 1$ را در نظر می‌گیریم. در $\frac{R[x]}{I}$ هر عضو به صورت $a+bx+I$ می‌باشد که $a,b \in R$. بعلاوه

$$(a+bx+I)(c+dx+I)=(a+bx)(c+dx)+I=ac+(bc+ad)x+bdx^2+I.$$

با به کار بردن الگوریتم تقسیم برای $f(x) = \alpha x^2 + \beta x + \gamma$ و $p(x) = x^2 + 1$ نتیجه می‌شود که $f(x) = \alpha (x^2+1)+(\beta x+\gamma-\alpha)$، از آن نتیجه می‌شود که

$$(a+bx+I)(c+dx+I)=(ac-bd)+(bc+ad)x+I.$$

اکنون $\frac{R[x]}{I}$ واقعاً یک میدان است، ارائه معکوس ضربی $a+bx+I$، (که $a\neq0$ یا $b\neq0$) که آن را $c+dx+I$ می‌نامیم، که در آن $c=\frac{a}{a^2+b^2}$ و $d=\frac{-b}{a^2+b^2}$ ساده است. فرض کنیم خواننده ثابت کند که $\frac{R[x]}{I} \cong C$. بویژه، قسمت موهومی عدد i که $i^2= - 1$، با همدستهٔ $x+I$ متناظر می‌شود.

تمرین :

۳۵ . فرض کنیم n یک عدد صحیح مثبت باشد و $I=(n)$ ایده‌آل اصلی در Z تولید شده بوسیله n باشد ، نشان دهید که حلقهٔ خارج قسمتی $\frac{Z}{I}$ با Z_n ، حلقهٔ مانده‌های به هنگ n ، ایزومورف است .

۳۶ . اگر R یک حلقه باشد ، فرض کنیم $I=(x)$ ایده‌آل اصلی در $R[x]$ تولید شده بوسیلهٔ x باشد، نشان دهید که $R \cong \frac{R[x]}{I}$.

۳۷* . قضیهٔ تناظر را برای حلقه‌ها ثابت کنید . اگر I یک ایده‌آل در حلقهٔ R باشد، آنگاه یک تابع دوسویی از خانوادهٔ تمام ایده‌آلهای میانی J ، که $I\subset J\subset R$ ، به خانوادهٔ تمام ایده‌آلهای در $\frac{R}{I}$ وجود دارد. این تابع دوسویی با ضابطهٔ $J\longrightarrow\pi(J)=\frac{J}{I}=\{a+I;a\in J\}$ داده‌شده‌است ، که $\pi : R \longrightarrow \frac{R}{I}$ هomomorfism طبیعی است . بعلاوه ، اگر $J \subset J'$ ایده‌آلهای میانی باشند، آنگاه $\pi(J)\subset\pi(J')$. (با قضیه A9 مقایسه کنید.)

۳۸ . قضیهٔ اول ایزومورفیسم را ثابت کنید. اگر $\psi : R \longrightarrow S$ یک همومورفیسم حلقه با $\ker\psi=I$ باشد، آنگاه یک ایزومورفیسم $\frac{R}{I} \longrightarrow \mathrm{Im}\psi$ تعریف شده بوسیلهٔ $r + I \longrightarrow \psi(r)$ وجود دارد. (راهنمایی: قضیهٔ اول ایزومورفیسم گروهها (قضیهٔ A5) حافظ ضرب است.)

۳۹* . فرض کنیم I یک ایده‌آل حلقهٔ R و J یک ایده‌آل حلقهٔ S باشد، و $\psi : R\longrightarrow S$ یک ایزومورفیسم حلقه‌ها باشد به طوری که $\psi(I) = J$. ثابت کنید که ایزومورفیسم $\frac{R}{I}\cong\frac{S}{J}$ موجوداست .

حلقهٔ چند جمله‌ایها بر میدانها

قضیه ۴ : اگر F یک میدان باشد ، آنگاه هر ایده‌آل در $F[x]$ یک ایده‌آل اصلی است .

برهان : فرض کنیم I یک ایده‌آل در $F[x]$ باشد ، اگر $I=\{0\}$ آنگاه $I = (0)$ یک ایده‌آل اصلی با مولد صفر است . اگر $I \neq \{0\}$ ، چند جمله‌ای ناصفر $m(x)$ را با کمترین درجه در I انتخاب می‌کنیم ، ادعا می‌کنیم که $I = \big(m(x)\big)$.

واضح است که $\big(m(x)\big) \subseteq I$. برای اثبات عکس جزئیت فرض کنیم $f(x) \in I$. بنابر الگوریتم تقسیم چند جمله‌ایهای $q(x)$ و $r(x)$ موجودند به طوری که $f(x)=q(x)m(x)+r(x)$ که در آن $r(x)=0$ یا $\partial r<\partial m$. اکنون $r(x)=f(x)-q(x)m(x)\in I$ ، اگر $r(x)\neq 0$ ، آنگاه $\partial r<\partial m$ متناقض با این است که $m(x)$ دارای کوچکترین درجه در بین تمام چندجمله‌ایهای در I می‌باشد. بنابراین $r(x)=0$ و $f(x)=q(x)m(x)\in\big(m(x)\big)$. $\square$

بنابر تمرین ۲۷ قسمت (ب) ، چون F یک میدان است $m(x)$ می‌تواند تکین انتخاب شود.

تعریف : حلقهٔ R یک دامنهٔ ایده‌آل اصلی (P.I.D) نامیده می‌شود ، اگر یک حوزهٔ صحیح و هر ایده‌آل آن یک ایده‌آل اصلی باشد.

قضیهٔ قبل نشان می‌دهد که وقتی F یک میدان است ، آنگاه $F[x]$ یک P.I.D است. (البته ، خواننده می‌داند که Z مثالی دیگر از یک P.I.D است) . از طرف دیگر $Z[x]$ یک P.I.D نیست . (به عنوان یک تمرین است که ایده‌آل I شامل تمام چندجمله‌ایهای دارای جملهٔ ثابت زوج یک ایده‌آل اصلی نیست ، تمرین ۳۳ را ببینید).

تعریف : فرض کنیم R یک حلقه باشد ، اگر $r,s\in R$ ، آنگاه r عادمی‌کند s را (یا s مضربی از r است) در صورتی که r' ای از R موجود باشد که $s = rr'$ ، در این حالت می‌نویسیم $r\,|\,s$.

اگر $I = (r_0)$ ، آنگاه r_0 هر عضو s از I را می‌شمارد. توجه کنید که به ازای هر r از

R ، $r \mid r$ ، و r یک یکال است اگر و فقط اگر $r \mid 1$.

تعریف: فرض کنیم F یک میدان باشد ، و $f(x)\,,\,g(x) \in F[x]$. بزرگترین مقسوم علیه مشترک (بمعم) $f(x)$ و $g(x)$ چند جمله‌ای $d(x)$ از $F[x]$ است به طوری که

(آ) $d(x)$ یک مقسوم علیه مشترک $f(x)$ و $g(x)$ باشد، یعنی $d \mid f$ و $d \mid g$.

(ب) اگر $c(x)$ مقسوم علیه مشترک دلخواهی از $f(x)$ و $g(x)$ باشد ، آنگاه $c(x) \mid d(x)$.

(ج) $d(x)$ تکین باشد.

اغلب $d(x)$ با $\left(f(x),g(x)\right)$ نشان داده می‌شود. اگر $\left(f(x),g(x)\right) = 1$ آنگاه $f(x)$ و $g(x)$ را نسبت به هم اول نامیم .

توجه کنید که بزرگترین مقسوم علیه مشترک f و g در صورت وجود ، منحصر بفرد است. اگر d' بزرگترین مقسوم علیه مشترک دیگری باشد ، آنگاه توجه داریم که فقط به عنوان یک مقسوم علیه مشترک وبا استفاده از (ب) $d' \mid d$ به دست می‌آید. به طور مشابه ، اگر به d فقط به عنوان یک مقسوم علیه مشترک توجه شود ، $d \mid d'$. بنابر تمرین ۴ ، به ازای یکال u از $F[x]$ ، $d' = ud$ ، یعنی به ازای ثابت ناصفر u، $d' = ud$.(تمرین ۲۷). چون d و d' هر دو تکین می‌باشند ، لذا $u = 1$ و $d' = d$.

قضیه ۵ : فرض کنیم F یک میدان باشد، و $f(x)\,,\,g(x) \in F[x]$ و $g(x) \neq 0$. در این صورت $\left(f(x),g(x)\right) = d(x)$ موجود است و به صورت ترکیب خطی از $f(x)$ و $g(x)$ می‌باشد، یعنی ، چند جمله‌ایهای $a(x)$ و $b(x)$ موجودند به طوری که $d(x)=a(x)f(x)+b(x)g(x)$.

برهان: بنابر تمرین ۳۲ ، $I = \{a(x)f(x)+b(x)g(x)\ ;\ a(x)\,,\,b(x) \in F[x]\}$ یک ایده‌ال در $F[x]$ و شامل $f(x)$ و $g(x)$ است. چون F یک میدان است ، $F[x]$ یک P.I.D است ، چند جمله‌ای تکین $d(x)$ را با $I = (d(x))$ انتخاب می‌کنیم ، و توجه داریم که d

ترکیب خطی از f و g است. اکنون d یک مقسوم‌علیه‌مشترک f و g است زیرا $f,g\in(d)=I$. بالاخره، اگر c یک مقسوم‌علیه مشترک باشد، آنگاه $c|f$ و $c|g$، یعنی $f=cc'$ و $g=cc''$. بنابراین $d = af + bg = acc' + bcc'' = c\,(ac' + bc'')$ و لذا $c|d$.□

مثال: اگر $a\in Z$، آنگاه $\bar{a}$ یک یکال در Z_n است اگر و فقط اگر $(a,n)=1$.

اگر $\bar{a}$ یک یکال باشد، آنگاه یک عدد صحیح s وجود دارد به طوری که $\bar{a}\bar{s}=1$. بنابر این $as \equiv 1 \pmod n$، یعنی به ازای عددی صحیح مانند t، $as - 1 = tn$، و بنابراین $as - tn = 1$، در نتیجه $(a,n)=1$، هر مقسوم علیه مشترک a و n باید 1 را عاد کند. بالعکس، اگر $(a,n)=1$، آنگاه اعداد صحیح s و t با $as + nt = 1$ وجود دارند. بنابراین $\bar{a}\bar{s}=\bar{1}$.

تمرین :

۴۰. فرض‌کنیم R حلقه‌تمام‌توابع $f:R\longrightarrow R$ تحت‌اعمال‌جمع‌وضرب‌نقطه‌ای‌باشد. اگر $f\ ,\ g\in R$، آنگاه $(f+g)(a)= f(a) + g(a)$ و $(fg)(a)= f(a)g(a)$. نشان دهید که $f(x) = \max\{x,0\}$ و $g(x) = \min\{x,0\}$ دارای هیچ بزرگترین مقسوم علیه مشترکی در R نمی‌باشند.

۴۱*. فرض کنیم $f(x) = \Pi\ (x - a_i)\in F[x]$، که F یک میدان است. نشان دهید که f دارای هیچ ریشهٔ تکراری نیست (به ازای هر a از F، $f(x)$ مضربی از $(x - a)^2$ نیست.) اگر و فقط اگر $(f(x)\ ,\ f'(x))=1$، که $f'(x)$ مشتق $f(x)$ است.

نتیجه ۶: (لم اقلیدس). فرض کنیم F یک میدان باشد. اگر $(f(x)\ ,\ g(x)) = 1$ و $f(x)\,|\,g(x)h(x)$، آنگاه در $F[x]$، $f(x)\,|\,h(x)$.

برهان : چند جمله‌ایهای $a(x)$ و $b(x)$ با $af + bg = 1$ موجودند. بنابراین

$h=afh+bgh$. اما به ازای چند جمله‌ای مانند k، $gh = fk$، لذا $h=f(ah+bk)$ و $f|h$. □

برهان لم اقلیدس دقیقاً همانند برهان معمول لم اقلیدس در $\mathbb{Z}$ ارائه شده است، به طور مشابه برای الگوریتم اقلیدسی که بعداً اثبات می‌شود درست می‌باشد. اگر چند جمله‌ایهای $f(x)$ و $g(x)$ به طور ضمنی داده شده باشند، چگونه می‌توان بزرگترین مقسوم‌علیه مشترک آنها را محاسبه کرد؟ چگونه می‌توان بزرگترین مقسوم علیه مشترک را به عنوان یک ترکیب خطی بیان کرد؟

قضیه ۷: (الگوریتم اقلیدسی). الگوریتمهایی برای محاسبهٔ بمعم که به صورت یک ترکیب خطی بیان می‌شود وجود دارند.

برهان: ایده دقیقاً تکرار الگوریتم تقسیم است. لیست معادلات زیر را در نظر می‌گیریم (به عنوان مثال چند جمله‌ای $f(x)$ را به f خلاصه می‌کنیم).

$$
\begin{array}{llll}
f & = q_1 g + r_1 & & \partial r_1 < \partial g \\
g & = q_2 r_1 + r_2 & & \partial r_2 < \partial r_1 \\
r_1 & = q_3 r_2 + r_3 & & \partial r_3 < \partial r_2 \\
 & \vdots & & \vdots \\
r_{n-2} & = q_n r_{n-1} + r_n & & \partial r_n < \partial r_{n-1} \\
r_{n-1} & = q_{n+1} r_n + r_{n+1} & & \partial r_{n+1} < \partial r_n \\
r_n & = q_{n+2} r_{n+1} \cdot & &
\end{array}
$$

ادعا می‌کنیم که $d=r_{n+1}$ بزرگترین مقسوم علیه مشترک است. (بعداً چند جمله‌ای تکین ساخته می‌شود) . قبل از هر چیز توجه داریم که تکرار باید متوقف شود زیرا درجهٔ باقیمانده اکیداً کاهش می‌یابد. (تعداد مراحل از ∂g کمتر است). ثانیاً، d یک مقسوم علیه

مشترک است و $d=r_{n+1} \mid r_n$ و همچنین معادلهٔ $n+1$ام، $r_{n-1} = q_{n+1} r_n + r_{n+1}$ نشان می‌دهد که $d \mid r_{n-1}$. کار روی لیست سرانجام نتیجه می‌دهد که $d \mid g$ و $d \mid f$. ثالثاً، اگر c یک مقسوم علیه مشترک باشد، با شروع از ابتدای لیست و کار روی آن و اینکه $c \mid f$ و $c \mid g$ نتیجه می‌دهد که $c \mid r_1$، و قس علیهذا. بنابراین، d بزرگترین مقسوم علیه مشترک است. بالاخره، با کار کردن روی لیست از انتها به طرف بالا a و b به‌دست می‌آیند. بنابراین $d=r_{n+1} = r_{n-1} + q_{n+1} r_n$ ترکیب خطی از r_n , r_{n-1} است. از ترکیب آن با $r_n=r_{n-2}-q_n r_{n-1}$ نتیجه می‌شود که $d=r_{n-1}-q_{n+1}(r_{n-2}-q_n r_{n-1})=(1+q_n q_{n+1})r_{n-1}-q_{n+1}r_{n-2}$ یک ترکیب خطی از r_{n-1} , r_{n-2} است. این روند با $d=af+bg$ خاتمه می‌یابد. (توجه: همهٔ q_iها و r_iها به طور صریح از الگوریتم تقسیم شناخته شده‌اند).□

نتیجه ۸ : فرض کنیم $F \subset E$ میدانهایی باشند، و $f(x),g(x) \in F[x] \subset E[x]$. در این صورت (f , g) بمعم محاسبه شده در $F[x]$ همان (f , g) بمعم محاسبه شده در $E[x]$ می‌باشد.

برهان: $f(x)$ و $g(x)$ را در $E[x]$ در نظر می‌گیریم. الگوریتم اقلیدسی بمعم آنها را در $E[x]$ محاسبه می‌کند. اما لیست معادلات (به دست آمده بوسیلهٔ تکرار الگوریتم تقسیم) دارای تمام چند جمله‌ایهای شامل آن جملات بر F می‌باشد. و لذا این لیست همان لیست به دست آمده با کار روی $F[x]$ می‌باشد.□

در نظر می‌گیریم $R = \dfrac{F[x]}{I}$، که F یک میدان است و I ایده‌آل اصلی تولید شده بوسیلهٔ چند جمله‌ای $p(x)$ می‌باشد. اگر $(f(x) , p(x)) = 1$، آنگاه چند جمله‌ایهای $s(x)$ و $t(x)$ از $F[x]$ با $s(x)f(x) + t(x)p(x)=1$ موجود می‌باشند، و این معادله نتیجه می‌دهد که $s(x)f(x)+I=1+I$. بنابراین $f(x) + I$ یک یکال در R با

معکوس $s(x)+I$ است .

تمرین :

۴۲. بزرگترین مقسوم علیه مشترک $x^5 - 2x^2 + 1$ و $x^3 + 3x^2 - x - 3$ را پیداکنید و آن را به صورت یک ترکیب خطی نشان دهید.

۴۳. فرض کنیم $p(x) = x^3 + x + 1 \in Z_2[x]$ و $I = (p(x))$. اگر $f(x)=r+sx+tx^2 \in Z_2[x]$ و $f(x)$ عضو I نباشد، چند جمله‌ای $a(x)$ را طوری بیابید که $p(x) \mid a(x)\, f(x) - 1$ و در $\frac{Z_2[x]}{I}$، داشته باشیم

$$(a(x) + I)\,(f(x) + I) = 1 + I.$$

تعریف: فرض کنیم F یک میدان باشد، و $f(x)\ ,\ g(x) \in F[x]$.کوچکترین مضرب مشترک (کمم) $f(x)$ و $g(x)$ چند جمله‌ای $m(x)$ از $F[x]$ می‌باشد ، به طوری که

(آ) $m(x)$ یک مضرب مشترک از $f(x)$ و $g(x)$ است، یعنی، $f|m$ و $g|m$.

(ب) اگر $c(x)$ مضرب مشترک دیگری از $f(x)$ و $g(x)$ باشد، آنگاه $m(x)|c(x)$.

(ج) $m(x)$ تکین باشد.

تمرین :

۴۴. ثابت کنید که اگر $f(x)\ ,\ g(x) \in F[x]$، که F یک میدان است، آنگاه (f,g)کمم چند جمله‌ای تکین مولد ایده‌آل $(f) \cap (g)$ می‌باشد.

تعریف: چند جمله‌ای ناصفر $p(x) \in F[x]$ بر F تحویل‌ناپذیر است اگر $\partial p \geq 1$ و هیچ تجزیهٔ $p(x) = f(x)\, g(x)$ در $F[x]$ با $\partial f < \partial p$ و $\partial g < \partial p$ موجود نباشد.

توجه داریم که تحویل‌ناپذیری به میدان F وابسته است. بنابر این x^2+1 بر R تحویل‌ناپذیر است، اما بر C تحویل‌پذیر است. چند جمله‌ایهای خطی (درجه ۱) بر هر میدان تحویل‌ناپذیر می‌باشند.

تمرین :

۴۵ . چند جمله‌ای $p(x)\in F[x]$ از درجهٔ ۲ یا ۳ بر F تحویل‌ناپذیر است اگر و فقط اگر F شامل هیچ ریشه‌ای از $p(x)$ نباشد. (این حکم برای چند جمله‌ای درجهٔ ۴ نادرست است، چند جمله‌ای $(x^2+1)^2$ که در $R[x]$ تحویل‌پذیر است دارای هیچ ریشهٔ حقیقی نیست).

*۴۶ . فرض کنیم $p(x)\in F[x]$ تحویل‌ناپذیر باشد. اگر $g(x)\in F[x]$ غیر ثابت باشد، آنگاه یا $(p(x), g(x)) = 1$ یا $p(x) \mid g(x)$.

۴۷ . (لم اقلیدس) اگر $p(x)$ یک چند جمله‌ای تحویل‌ناپذیر باشد و $p(x)$ حاصلضرب $q_1(x)q_2(x)...q_s(x)$ را عاد کند، آنگاه به ازای jای، $j=1,2..., s$، $p(x) \mid q_j(x)$.

۴۸ . (آ) هر چند جمله‌ای ناصفر $f(x)$ در $F[x]$ دارای تجزیه‌ای به صورت $f(x)=ap_1(x)p_2(x)...p_t(x)$ است که در آن a یک ثابت ناصفر و $p_i(x)$ها (لزوماً متمایز نیستند) چند جمله‌ایهای تحویل‌ناپذیر تکین می‌باشند.

(ب) عوامل و مضربهای آنها در این تجزیه به طور منحصر بفرد مشخص می‌شوند. (این همانند قضیهٔ اساسی حساب دارای برهان مشابه به عنوان قضیه است: همچنین اگر $f(x)=bq_1(x)q_2(x)...q_s(x)$، که b ثابت است و $q_j(x)$ها تکین و تحویل ناپذیراند، آنگاه یکتایی بوسیلهٔ لم اقلیدس و استقراء بر $Max\{t,s\}$ ثابت شده است.)

*۴۹ . فرض کنیم $f(x)=ap_1(x)^{k_1}...p_t(x)^{k_t}$ و $g(x)=bp_1(x)^{n_1}...\ p_t(x)^{n_t}$، که $k_i\geq 0$ و $n_i \geq 0$ و a و b ثابتهای ناصفرند، و $p_i(x)$ها چند جمله‌ایهای تحویل‌ناپذیر تکین متمایزهستند (نماهای صفر برای $p_i(x)$ها در تجزیه‌ها مجازمی‌باشد). ثابت‌کنیدکه

$$\text{بمعم}(f, g) = p_1(x)^{m_1} p_2(x)^{m_2} \dots p_t(x)^{m_t}$$ و
$$\text{کمم}(f, g) = p_1(x)^{M_1} p_2(x)^{M_2} \dots p_t(x)^{M_t}$$

که در آن $M_i = \text{Max}\{n_i, k_i\}$ و $m_i = \min\{n_i, k_i\}$.

تبصره: تجزیه یکتا به عوامل تحویل‌ناپذیر در حلقه‌های $F[x_1, x_2, \dots, x_n]$ که در آن F یک میدان است، برقرار است و وجود بزرگترین مقسوم‌علیه مشترک و کوچکترین مضرب مشترک با استفاده از تمرین ۴۹ ثابت می‌شود. (اگر $n \geq 2$، این حلقه‌ها P.I.D نیستند و بمعم آنها به صورت ترکیب خطی نمی‌باشد).

یک رابطهٔ مقدماتی بین تجزیه و ریشه‌ها وجود دارد.

قضیه ۹: فرض کنیم $f(x) \in F[x]$ و $a \in F$. در این صورت $q(x)$ ای از $F[x]$ وجود دارد به طوری که $f(x) = q(x)(x-a) + f(a)$.

برهان: الگوریتم تقسیم را بکار می‌بریم. $f(x)$ رابر $x-a$ تقسیم می‌کنیم یک خارج قسمت و یک باقیماندهٔ ثابت بدست می‌آید (زیرا $x-a$ دارای درجهٔ ۱ است):
$f(x) = q(x)(x-a) + r$. با محاسبه به ازای a نتیجه می‌شود که $f(a)=q(a)(a-a)+r=r$. □

نتیجه ۱۰: فرض کنیم $f(x) \in F[x]$. در این صورت $a \in F$ یک ریشهٔ $f(x)$ است اگر و فقط اگر $x-a \mid f(x)$.

برهان: اگر a یک ریشهٔ $f(x)$ باشد، آنگاه $f(a)=0$، و بنابرقضیه نتیجه می‌شود که $f(x)=q(x)(x-a)$.

بالعکس، اگر $f(x)=q(x)(x-a)$، آنگاه با محاسبه در a نتیجه می‌شود که $f(a)=0$ و a یک ریشهٔ $f(x)$ است. □

قضیه ۱۱: اگر F یک میدان و $f(x) \in F[x]$ از درجهٔ n باشد، آنگاه F شامل حداکثر n

ریشه از $f(x)$ است .

برهان: فرض کنیم که F شامل $n+1$ ریشهٔ متمایز مانند $a_1,a_2,\ldots,a_{n+1}$ از $f(x)$ باشد. بنابرنتیجهٔ ۱۰، $f(x)=(x-a_1)g_1(x)$ به ازای $g_1(x)$ از $F[x]$.اکنون $x-a_2 \mid f(x)$، بنابرلم اقلیدس ، $x-a_2 \mid g_1(x)$ ، بنابراین $f(x)=(x-a_1)(x-a_2)g_2(x)$. به استقراء بر n ، $f(x)=(x-a_1)(x-a_2)\cdots(x-a_{n+1})g_{n+1}(x)$ و این نمی‌تواند برقرارباشد ، زیرا طرف چپ تساوی از درجهٔ n و طرف راست تساوی از درجهٔ بزرگتر از n است. □

قضیهٔ قبل برای حلقه‌های دلخواه R نادرست است ، به عنوان مثال $x^2 - 1$ دارای چهار ریشه در Z_8 است .

توجه داریم که هر چند جمله‌ای $f(x)\in F[x]$ یک تابع $F \longrightarrow F$ ، مثلاً $a \longrightarrow f(a)$ را مشخص می‌کند. به هر حال، در تمرین ۱۹ دیدیم که چند جمله‌ایهای متمایز در $Z_p[x]$ ممکن است یک تابع مشابه را مشخص کنند. این دیدگاه وقتی که میدان ضریب نامتناهی باشد حذف می‌شود. فرض کنیم F یک میدان نامتناهی باشد، و $f(x)\neq g(x)$ دو چند جمله‌ای در $F[x]$ باشند که به ازای هر a از F در $f(a)=g(a)$ صدق کنند. در این صورت $h(x)=f(x) - g(x)$ یک چند جمله‌ای ناصفر و از درجهٔ مثلاً n است. اما تعداد نامتناهی از اعضای $a\in F$ یک ریشهٔ $h(x)$ است، و این متناقض با قضیهٔ ۱۱ می‌باشد.

ایده‌آلهای اول و ایده‌آلهای ماکسیمال

تعریف: ایده‌آل I را در حلقهٔ R اول نامیم در صورتی که $I\neq R$، و از $ab\in I$ نتیجه شود که $a\in I$ یا $b\in I$.

اگر $p(x)\in F[x]$ تحویل ناپذیر باشد، آنگاه $I=(p(x))$ یک ایده‌آل اول است، زیرا از $a(x)b(x)\in I$ نتیجه می‌شود که $p(x) \mid a(x)b(x)$، بنابر لم اقلیدس $p(x) \mid a(x)$ یا

$p(x) \mid b(x)$، بنابراین $a(x) \in I$ یا $b(x) \in I$. چون $I \neq R$، زیرا $\partial p \geq 1$، در نتیجه I یک ایده‌آل اول است .

تمرین :

*۵۰ . اگر $I=(p(x))$ یک ایده‌آل اول در $F[x]$ باشد، که F یک میدان است، آنگاه $p(x)$ تحویل ناپذیراست.

۵۱ . ایده‌آل صفر در حلقهٔ R یک ایده‌آل اول است اگر و فقط اگر R یک حوزهٔ صحیح باشد.

۵۲ . ایده‌آل $I=(n)$ در Z اول است اگر و فقط اگر $n=0$ یا n عددی اول باشد.

*۵۳ . ایده‌آل I در $Z[x]$ شامل تمام چند جمله‌ایهای دارای جملهٔ ثابت زوج یک ایده‌آل اول است.

قضیه ۱۲: ایده‌آل I ، $I \neq R$، یک ایده‌آل اول R است اگر و فقط اگر $\frac{R}{I}$ یک حوزهٔ صحیح باشد.

برهان: فرض کنیم I یک ایده‌آل اول باشد. فرض کنیم که $a+I \neq 0$ و $b+I \neq 0$ که b , a عضو I نیستند. اگر $(a+I)(b+I)=ab+I=0$ آنگاه $ab \in I$، و این متناقض با اول بودن I است. عکس قضیه به طور مشابه ساده است.□

این قضیه یک برهان کوتاه از تمرین ۵۳ را به دست می‌دهد، به راحتی می‌بینیم که $\frac{Z[x]}{I} \cong Z_2$.

تعریف : ایده‌آل واقعی I در حلقهٔ R را یک ایده‌آل ماکسیمال نامیم در صورتی که $I \neq R$ و هیچ ایده‌آل J ای در R موجود نباشد که $I \subset J \subset R$.

قضیه ۱۳ : ایده‌آل واقعی I در حلقهٔ R یک ایده‌آل ماکسیمال است اگر و فقط اگر $\frac{R}{I}$ یک میدان باشد.

برهان: قضیهٔ تناظر (تمرین ۳۷) نشان می‌دهد که I یک ایده‌آل ماکسیمال است اگر و فقط اگر $\frac{R}{I}$ دارای هیچ ایده‌آلی بجز 0 و خود $\frac{R}{I}$ نباشد، تمرین ۳۰ نشان می‌دهد که این خاصیت برقراراست اگر و فقط اگر $\frac{R}{I}$ یک میدان باشد.□

نتیجه ۱۴: هر ایده‌آل ماکسیمال یک ایده‌آل اول است .

برهان: هر میدان یک حوزهٔ صحیح است.□

تمرین :

۵۴ . ایده‌آل صفر در حلقهٔ R یک ایده‌آل ماکسیمال است اگر و فقط اگر R یک میدان باشد.

۵۵ . ایده‌ال I در $Z[x]$ شامل تمام چند جمله‌ایهای دارای جملهٔ ثابت زوج یک ایده‌آل ماکسیمال است .

۵۶ . اگر F یک میدان باشد، آنگاه هستهٔ نگاشت ارزیاب $F[x] \longrightarrow F$ یک ایده‌آل ماکسیمال است .

عکس نتیجهٔ قبل نادرست است . به عنوان مثال، ایده‌آل (x) در $Z[x]$ اول است اما ماکسیمال نیست زیرا $\frac{Z[x]}{(x)} \cong Z$ یک حوزهٔ صحیح است ولی یک میدان نیست .

قضیه ۱۵: اگر R یک دامنهٔ ایده‌آل اصلی باشد، آنگاه هر ایده‌آل اول ناصفر I در R یک ایده‌آل ماکسیمال است .

برهان: فرض کنیم ایده‌آل $I \neq J$ موجود باشد که $I \subset J \subset R$. چون R یک P.I.D است، پس به ازای a و b ای از R، $I=(a)$ و $J=(b)$. اکنون $a \in J$ نتیجه می‌دهد که به ازای r ای از R، $a=rb$ ، و بنابراین $rb \in I$. چون I یک ایده‌آل اول است ، $r \in I$ یا $b \in I$. اگر $b \in I$ آنگاه $J \subset I$ ، یک تناقض است. اگر $r \in I$ ، آنگاه به ازای s ای از R ، $r=sa$ ، و بنابراین $a=rb=sab$ ، لذا $sb=1$ و بنابر قسمت (آ) تمرین ۲۷، $J=(b)=R$. بنابراین،

I یک ایده‌آل ماکسیمال است.□

نتیجه ۱۶: اگر F یک میدان و $p(x)\in F[x]$ تحویل‌ناپذیر باشد، آنگاه $\frac{F[x]}{(p(x))}$ یک میدان شامل کپی ایزومورف با F و یک ریشه از $p(x)$ است .

برهان: چون $p(x)$ تحویل‌ناپذیر است، ایده‌آل اصلی $I=(p(x))$ یک ایده‌آل اول ناصفر است، چون $F[x]$ یک P.I.D است، I یک ایده‌آل ماکسیمال است، و بنابراین $E=\frac{F[x]}{I}$ یک میدان است. دیدن اینکه $a \longrightarrow a+I$ یک ایزومورفیسم از F به $\{a+I;a\in F\}\subseteq E$ است ساده می‌باشد(معمولاً F به زیرمیدانی از E نظیر می‌شود). فرض کنیم $\theta=x+I\in E$، ادعا می‌کنیم که θ یک ریشهٔ $p(x)$ است. می‌نویسیم $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$، که $a_i\in F$. آنگاه در E داریم

$$\begin{aligned}
p(\theta)&=(a_0+I)+(a_1+I)\theta+\ldots+(a_n+I)\theta^n\\
&= (a_0+I)+(a_1+I)(x+I)+\ldots+(a_n+I)(x+I)^n\\
&= (a_0+I)+(a_1x+I)+\ldots+(a_nx^n+I)\\
&= a_0+a_1 x+\ldots+a_nx^n+I = p(x)+I=I
\end{aligned}$$

زیرا $(p(x)) = I$. اما $I=0+I$ عضو صفر $\frac{F[x]}{I}$ است، و بنابراین θ یک ریشهٔ $p(x)$ است. □

به عنوان مثال، چند جمله‌ای $x^2 + 1\in R[x]$ تحویل ناپذیراست و $\frac{R[x]}{(x^2+1)}$ با میدان اعداد مختلط C ایزومورف است .

تعریف: چند جمله‌ای $f(x)\in F[x]$ بر میدان F شکافته می‌شود در صورتی که به صورت حاصلضربی از عوامل خطی باشد. البته، $f(x)$ بر F شکافته می‌شود اگر و فقط اگر F شامل همهٔ ریشه‌های $f(x)$ باشد.

قضیه ۱۷: (کرونکر[1]). فرض کنیم $f(x)\in F[x]$، که F یک میدان است. در این صورت یک‌میدان E شامل F موجود است که $f(x)$ بر آن شکافته می‌شود.

برهان: اثبات به استقراء بر ∂f می‌باشد. اگر $\partial f=1$ ، آنگاه $f(x)$ خطی است وانتخاب می‌کنیم $E=F$. اگر $\partial f>1$ آنگاه می‌نویسیم $f(x)=p(x)g(x)$، که $p(x)$ تحویل‌ناپذیر است. اگر $p(x)$ خطی باشد، آنگاه بر هر میدان E شامل F که $g(x)$ بر آن شکافته شود، $f(x)$ شکافته می‌شود. بعلاوه، بنابه استقراء چنین میدان E برای $g(x)$ وجود دارد، اگر $\partial p>1$ ، آنگاه نتیجهٔ قبل یک میدان B شامل F و یک ریشهٔ θ از $p(x)$ را فراهم می‌سازد. بنابراین در $B[x]$، داریم $p(x) = (x - \theta)h(x)$. بنابه استقراء، یک میدان E شامل B که $h(x)g(x)$ بر آن شکافته می‌شود وجود دارد. بنابراین $f(x)$ بر E شکافته می‌شود. □

اکنون تعریف ریشهٔ تکراری ظاهر شده در تمرین ۴۱ را تعدیل می‌کنیم .

تعریف: اگر $f(x)\in F[x]$ بر میدان E شامل F شکافته شود، آنگاه $f(x)$ دارای هیچ ریشهٔ تکراری نیست، هرگاه به ازای هر a از E ، $f(x)$ مضربی از $(x - a)^2$ نباشد.

با استفاده از تمرین ۴۱ و نتیجهٔ ۸ ، می‌توان دید که $f(x)$ دارای ریشهٔ تکراری نیست اگر و فقط اگر $(f(x) , f'(x)) = 1$.

میدانهای متناهی

تعریف: میدان اول میدان F اشتراک تمام زیر میدانهای F است .

بنابر تمرین ۱۰ ، یک میدان اول واقعاً یک میدان (زیرمیدان) می‌باشد. (بخصوص، آن ناصفر است زیرا هر زیر میدان شامل عضو ۱ می‌باشد.)

---

1. Kronecker

قضیه ۱۸: اگر F یک میدان باشد، آنگاه میدان اول آن با Q یا Z_p به ازای عددی اول مانند p ایزومورف است .

برهان: نگاشت $\psi : Z \longrightarrow F$ را با ضابطهٔ $\psi(n)=n.1$ تعریف می‌کنیم (که ۱ واحد F است). به سادگی دیده می‌شود که ψ یک هومورفیسم حلقه است. اگر $I = \ker\psi$، آنگاه $\frac{Z}{I}$ یک حوزهٔ صحیح است (زیرا با یک زیرحلقه از میدان F ایـزومورف است). بنابراین I یک ایده‌آل اول است، و لذا $I=(0)$ یا به ازای عددی اول مانند p، $I=(p)$. اگر $I = (0)$، آنگاه ψ، Z را در F می‌نشاند. چون میدان اول باید شامل معکوس ضربی هرعدد صحیح‌ناصفرباشد، دراین‌حالت میدان اول با Q ایزومورف است . اگر $I=(p)$، بنابر قضیهٔ اول ایزومورفیسم نتیجه می‌شود که $Z_p \cong \frac{Z}{(p)} \cong \operatorname{Im}\psi$، که یک میدان است ، بنابراین $\operatorname{Im}\psi$ میدان اول F می‌باشد. □

تعریف: یک میدان دارای مشخصهٔ صفر است اگر میدان اول آن با Q ایزومورف باشد ، و دارای مشخصهٔ p است اگر میدان اول آن با Z_p ایزومورف باشد.

تمرین :

۵۷ . فرض کنیم $f(x) , g(x) \in F[x]$. در این صورت $(f , g) \neq 1$ اگر و فقط اگر میدان E شامل F و یک ریشهٔ مشترک از $f(x)$ و $g(x)$ موجود باشد.

۵۸ . اگر میدان F دارای مشخصهٔ p باشد ، آنگاه به ازای هر a از F، $pa = 0$.

۵۹* . اگر میدان F دارای مشخصهٔ p باشد ، آنگـاه بـه ازای هـر a و b از F ، داریـم $(a \pm b)^p = a^p \pm b^p$. (راهنمایی : تمرین ۷ را بکارببرید.)

۶۰ . (آ) اگر F دارای مشخصهٔ p باشد ، آنگاه $\sigma : F \longrightarrow F$ تعریف شده بوسیلهٔ $\sigma(a) = a^{p^i}$ ، به ازای هر $i\geq 0$ یک هومورفیسم میدان است .

(ب) اگرمیدان F دارای مشخصهٔ p باشدو $f(x)\in F[x]$ ، آنگاه $(f(x))^p=f(x^p)$.

۶۱ . به ازای عدد اول p ، هر میدان متناهی دارای مشخصهٔ p ، یک میدان نامتناهی از مشخصهٔ p را ارائه می‌دهد. (راهنمایی: تمرین ۱۲)

۶۲ . اگر F یک میدان با مشخصهٔ صفر باشد و $p(x)\in F[x]$ تحویل‌ناپذیر باشد، آنگاه $p(x)$ دارای ریشهٔ تکراری نیست. (راهنمایی $(p(x),p'(x))$ را در نظر بگیرید.)

تبصرهٔ مقدماتی زیر بسیار مفید است. اگر F یک زیرمیدان E باشد، آنگاه گروه جمعی E را می‌توان به عنوان یک فضای برداری بر میدان F در نظرگرفت. (اگر $e\in E$ و $a\in F$، ضرب اسکالر اعضای a , e تحت عمل ضرب داده شده بر E را به صورت ae تعریف می‌کنیم). بخصوص ، به ازای عدد اول p ، میدان متناهی E یک فضای برداری بر Z_p می‌باشد. اگر $\{\alpha_1,\alpha_2,\dots,\alpha_n\}$ یک پایهٔ مرتب E باشد، آنگاه هر $a\in E$ دارای مختصات $(\lambda_1 , \lambda_2 , \dots , \lambda_n)$ به ازای λ_i در Z_p می‌باشد، بنابراین، به ازای عددی اول مانند p و عددی صحیح و مثبت مانند n ، $|E|=p^n$.

قضیه ۱۹ : (گالوا) به ازای هر عدد اول p و هر عدد صحیح و مثبت n ، یک میدان دارای دقیقاً p^n عضو وجود دارد.

برهان: اگر K یک میدان با $q = p^n = |K|$ باشد، آنگاه $K^*=K-\{0\}$ یک گروه ضربی از مرتبهٔ $q-1$ خواهد بود، بنابر قضیهٔ لاگرانژ (قضیه A3) به ازای هر a از K^* ، $a^{q-1}=1$. از آن نتیجه می‌شود که هر عضو از K یک ریشهٔ چند جمله‌ای $g(x)=x^q - x$ می‌باشد.

اکنون ساختار را شروع می‌کنیم. بنابر قضیهٔ کرونکر، یک میدان E شامل Z_p که $g(x)$ بر آن شکافته می‌شود وجود دارد. تعریف می‌کنیم $F=\{\alpha\in E \ ; \ g(\alpha)=0\}$ ، یعنی F مجموعهٔ تمام ریشه‌های $g(x)$ است. چون $g'(x)=qx^{q-1}-1=-1$ ، (زیرا $q=p^n$ و E از مشخصهٔ p است) ، از آن نتیجه می‌شود که $(g(x),g'(x))=1$ بمعم، و

بنابراین $g(x)$ دارای ریشه‌های تکراری نیست، یعنی $q=p^n=|F|$.

ادعا می‌کنیم که F یک میدان است، که برهان را کامل خواهد کرد. اگر $a, b\in F$، آنگاه $a^q=a$ و $b^q=b$. بنابراین، $(ab)^q=a^qb^q=ab$ و $ab\in F$. بنابر تمرین ۵۹، $(a-b)^q=a^q-b^q=a-b$، لذا $a-b\in F$. بالاخره، اگر $a\neq 0$، آنگاه $a^{q-1}=1$ لذا $a^{-1}=a^{q-2}\in F$. (زیرا F تحت ضرب بسته است).□

در نتیجه ۳۴ خواهیم دید که هردومیدان از مرتبهٔ p^n ایزومورف می‌باشند.

تمرین :

۶۳ . یک میدان چهارعضوی با الحاق یک ریشهٔ مناسب از $x^4 - x$ به Z_2 بسازید.

*۶۴ . جدولهای جمع و ضرب یک میدان دارای هشت عضو ارائه دهید. (راهنمایی: تجزیهٔ x^8-x را بر Z_2 در نظربگیرید.)

۶۵ . نشان دهید که یک میدان چهارعضوی با زیرمیدانی از یک میدان هشت عضوی ایزومورف نیست .

چند جمله‌ایهای تحویل ناپذیر

طرح بعدی ما به دست آوردن برخی ضوابط برای تحویل ناپذیری یک چند جمله‌ای می‌باشد . معمولاً این مشکل است ، و در حالت کلی حل نشده است .

تمرین :

*۶۶ . به یاد داریم که اگر $\sigma:R \longrightarrow S$ یک هومومورفیسم حلقه‌ها باشد، آنگاه $\sigma^*:R[x] \longrightarrow S[x]$ تعریف شده بوسیلهٔ $\sigma^*(\sum r_ix^i)=\sum\sigma(r_i)x^i$ یک هومومورفیسم حلقه‌ها می‌باشد. ثابت کنید که اگر R و S حوزه‌های صحیح باشند و $\sigma^*(p(x))\in S[x]$ تحویل‌ناپذیر و دارای درجهٔ مساوی با درجه $p(x)$ باشد، آنگاه $p(x)$ بر R تحویل‌ناپذیر است. (توجه کنید که اگر $p(x)$ تکین باشد ، شرط

درجه صادق است .)

*۶۷ . فرض کنیم $\sigma : Z \longrightarrow Z_p$ هومومورفیسم طبیعی باشد. با بکار بردن تمرین قبل و انتخاب یک عدد اول مناسبِ p نشان دهید که $f(x)=x^4-10x^2+1$ در $Z[x]$ تحویل‌ناپذیر است .

تبصره: یک چند جمله‌ای تحویل‌ناپذیر در $Z[x]$ ممکن است به ازای عددی اول مانند p به هنگ p تجزیه شود. به عنوان مثال $f(x)=x^3+6x^2+5x+25$ در $Z[x]$ تحویل‌ناپذیراست، زیرا به هنگ ۳ به x^3+2x+1 تبدیل می‌شود، این چند جمله‌ای درجهٔ سوم تحویل‌ناپذیر است، زیرا دارای هیچ ریشه‌ای نیست، تنها انتخابها $\bar{0}$ ، $\bar{1}$, $\bar{2}$ می‌باشند. اما $f(x)$ دارای تجزیهٔ به هنگ ۵ به صورت $x^3+x^2=x^2(x+1)$ است.

۶۸ . اگر $\sigma : R \longrightarrow S$ یک ایزومورفیسم حلقه‌ها باشد، آنگاه $\sigma^*:R[x] \longrightarrow S[x]$ نیز یک ایزومورفیسم حلقه‌ها می‌باشد. نتیجه بگیرید که اگر $p(x)\in R[x]$ تحویل‌ناپذیر باشد، آنگاه $\sigma^*(p(x))\in S[X]$ نیز تحویل‌ناپذیر است .

*۶۹ . اگر $c\in R$ ، که R یک حوزهٔ صحیح می‌باشد، آنگاه نگاشت $f(x) \longrightarrow f(x+c)$ یک اتومورفیسم حلقهٔ $R[x]$ است. نتیجه بگیرید که $p(x)$ تحویل‌ناپذیر است اگر و فقط اگر $p(x+c)$ تحویل‌ناپذیر باشد.

*۷۰ . فرض کنیم $f(x)=a_0+a_1x+\dots+a_nx^n\in Z[x]$. اگر $\frac{r}{s}$ یک ریشهٔ گویای $f(x)$ باشد، آنگاه $r\mid a_0$ و $s\mid a_n$. نتیجه بگیرید که هر ریشهٔ گویای یک چند جمله‌ای تکین در $Z[x]$ باید عددی صحیح باشد.

۷۱ . تجزیهٔ چند جمله‌ایهای زیر را در $Z[x]$ بررسی کنید.

$3x^2-7x-5$ ، $6x^3-3x-18$ ، x^3-7x+1

۷۲. ثابت کنید که اگر $a_0+a_1x+\cdots+a_nx^n\in F[x]$ تحویل‌ناپذیر باشد، آنگاه $a_n+a_{n-1}x+\cdots+a_1x^{n-1}+a_0x^n$ نیز تحویل‌ناپذیر است.

راههای مختلفی برای مشخص کردن اینکه چند جمله‌ای $f(x)$ در $Z[x]$ دارای یک تجزیه در $Z[x]$ است دیده‌ایم. اما تجزیهٔ آن بر $Q[x]$ برای ما واقعاً جالب است.

تعریف: چند جمله‌ای $f(x)=a_0+a_1x+\cdots+a_nx^n\in Z[x]$ را اولیه نامیم، در صورتی که بزرگترین مقسوم علیه مشترک ضرایب آن یک باشد.

ملاحظه می‌شود که اگر $f(x)$ اولیه نباشد، آنگاه عددی اول مانند p وجود دارد که هر یک از ضرایب آن را می‌شمارد.

لم ۲۰: (گاوس[1]). حاصلضرب هر دو چند جمله‌ای اولیهٔ $f(x)$ و $g(x)$ یک چند جمله‌ای اولیه می‌باشد.

برهان: فرض کنیم که $f(x)g(x)=(\sum a_ix^i)(\sum b_jx^j)=\sum c_kx^k$ اولیه نباشد، بنابر این عددی اول مانند P موجود است که به ازای هر k، $p\,|\,c_k$. فرض کنیم a_i و b_j به ترتیب اولین ضرایبی از $f(x)$ و $g(x)$ باشند، که p آنها را عاد نمی‌کند. در این صورت بنابر تعریف حاصلضرب چند جمله‌ایها نتیجه می‌شود که

$$a_ib_j=c_{i+j}-(a_0b_{i+j}+\cdots+a_{i-1}b_{j+1}+a_{i+1}b_{j-1}+\cdots+a_{i+j}b_0).$$

چون هر جملهٔ طرف راست بوسیلهٔ p عاد می‌شود، بنابر این $p\,|\,a_ib_j$. اما لم اقلیدس در Z نتیجه می‌دهد که $p\,|\,a_i$ یا $p\,|\,b_j$، و این یک تناقض است. □

لم ۲۱: هر چند جمله‌ای ناصفر $f(x)\in Q[x]$ دارای تجزیهٔ یکتای $f(x)=c(f)f^*(x)$ می‌باشد، که $c(f)\in Q$ و مثبت است و $f^*(x)\in Z[x]$ اولیه می‌باشد.

---

1. Gauss

تبصره: عدد مثبت گویای $c(f)$ محتوای $f(x)$ نامیده شده است .

برهان: فرض کنیم $f(x)=\frac{a_0}{b_0}+\frac{a_1}{b_1}x+\ldots+\frac{a_n}{b_n}x^n\in Q[x]$. تعریف می‌کنیم $B=b_0b_1\ldots b_n$، به طوری که به ازای $g(x)\in Z[x]$ ، $f(x)=\frac{1}{B}g(x)$. اکنون تعریف می‌کنیم (بزرگترین مقسوم‌علیه مشترک ضرایب $B'=\pm(g(x)$ ، (علامت انتخاب شده $\frac{B'}{B}$ رامثبت می‌سازد). بنابراین $f(x)=c(f)f^*(x)$ ، که $c(f)=\frac{B'}{B}$ و $f^*(x)=\frac{B}{B'}f(x)$ ، تجزیه مورد نظر می‌باشد.

فرض کنیم که $f(x)=dh(x)$یک تجزیهٔ دیگر باشد، آنگاه $f^*(x)=rh(x)$، که $r=\frac{d}{c(f)}$ یک عدد گویای مثبت است. $r=\frac{u}{v}$ را برحسب پایین‌ترین جملات می‌نویسیم، یعنی، u , v اعداد صحیح مثبت و نسبت به هم اول می‌باشند. بنابراین $vf^*(x)=uh(x)$ یک معادله در $Z[x]$ است. ضرایب $uh(x)$ دارای v به عنوان یک مقسوم علیه مشترک است، بنابر لم اقلیدس در Z ، v همهٔ ضرایب $h(x)$ را می‌شمارد. اما $h(x)$ یک چند جمله‌ای اولیه است، بنابراین $v=1$. آرگومان مشابه نشان می‌دهد که $u=1$. بنابراین $r=\frac{d}{c(f)}=\frac{u}{v}=1$ ، لذا $d=c(f)$ و $f^*(x)=h(x)$. □

ملاحظه می‌شود که اگر $f(x)\in Z[x]$ ، آنگاه $c(f)\in Z$. ($c(f)$ دقیقاً برابر بزرگترین مقسوم‌علیه مشترک ضرایب $f(x)$ می‌باشد.)

لم ۲۲. اگر $f(x)\in Q[x]$ به صورت $f(x)=g(x)h(x)$ تجزیه شود، آنگاه $c(f)=c(g)c(h)$ و $f^*(x)=g^*(x)h^*(x)$.

برهان: داریم $f(x)=g(x)h(x)=c(g)g^*(x)c(h)h^*(x)=c(g)c(h)g^*(x)h^*(x)$.

چون $c(g)c(h)$ یک عدد گویای مثبت است و حاصلضرب هر دو چند جمله‌ای اولیه، اولیه می‌باشد، یکتایی تجزیه در لم قبل نتیجه می‌دهد که $c(f)=c(g)c(h)$ و $f^*(x)=g^*(x)h^*(x)$. □

قضیه ۲۳ : اگر $f(x)\in Z[x]$ در $Q[x]$ تجزیه شود، آنگاه $f(x)$ در $Z[x]$ نیز تجزیه می‌شود.(به چند جمله‌ایهایی از درجهٔ یکسان بر Q). به طور معادل، اگر $f(x)\in Z[x]$ بر Z تحویل‌ناپذیر باشد، آنگاه $f(x)$ بر Q تحویل‌ناپذیر است.

برهان: فرض کنیم که در $Q[x]$، $f(x)=g(x)h(x)$. در این صورت در $Q[x]$ داریم $f(x)=c(g)c(h)g^*(x)h^*(x)$ ، که $g^*(x)$ و $h^*(x)$ چند جمله‌ایهای اولیه در $Z[x]$ می‌باشند. اما $c(g)c(h) = c(f)\in Z$ زیرا $f(x)\in Z[x]$. بنابراین، $f(x)=[c(f)g^*(x)]h^*(x)$ یک تجزیه در $Z[x]$ است. □

(برهان قضیهٔ قبل در حالت کلی‌تری می‌تواند سازگار باشد، به جای Z یک دامنهٔ یکتایی تجزیه، و به جای Q میدان کسرهای آن را جایگزین می‌کنیم. این جزء اصلی برهان است که اگر R یک دامنهٔ یکتایی تجزیه باشد، آنگاه $R[x]$ نیز یک دامنهٔ یکتایی تجزیه است، از آن نتیجه می‌شود که اگر F یک میدان باشد، آنگاه $F[x_1,\cdots,x_n]$ یک دامنهٔ یکتایی تجزیه می‌باشد)

قضیه ۲۴: (ضابطهٔ آیزنشتاین[1]). فرض کنیم $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n\in Z[x]$. اگر عددی اول مانند p موجود باشد که به ازای هر $0\leq i<n$ ، p عاد کند a_i را، اما p عاد نکند a_n را و p^2 عاد نکند a_0 را، آنگاه $f(x)$ بر Q تحویل ناپذیر است.

برهان: فرض کنیم $f(x)=(b_0+b_1x+\cdots+b_mx^m)(c_0+c_1x+\cdots+c_kx^k)$ ، بنابر قضیهٔ ۲۳ ، می‌توان فرض کرد که هر دو عامل تجزیه در $Z[x]$ قراردارند. اکنون $p\mid a_0=b_0c_0$ همچنین، بنابر لم اقلیدس در Z، $p\mid b_0$ یا $p\mid c_0$ ، چون p^2 عاد نمی‌کند a_0 را، فقط یکی

1. Eisenstein Criterion

از آنها توسط p عاد می‌شود، فرض کنیم که $p \mid c_0$ اما p عاد نکند b_0 را. ضریب پیشرو $a_n=b_m c_k$ به وسیلهٔ p عاد نمی‌شود، بنابر این p عاد نمی‌کند c_k (یا b_m) را. فرض کنیم c_r اولین ضریبی باشد که بوسیلهٔ p عاد نمی‌شود. (همچنین p عاد می‌کند $c_{r-1},...,c_1,c_0$). اگر $r<n$ ، آنگاه $p \mid a_r$ و $b_0c_r=a_r-(b_1c_{r-1}+...+b_rc_0)$ بوسیلهٔ p عاد می‌شود، بنابراین $p \mid b_0c_r$، و این متناقض با لم اقلیدس است (زیرا p هیچ یک از عوامل را نمی‌شمارد). در نتیجه $r=n$، بنابراین $k=0$ و عامل دوم ثابت است. بنابراین $f(x)$ تحویل ناپذیراست. $\square$

برای توضیح ضابطهٔ آیزنشتاین ، x^5-4x+2 بر Q تحویل ناپذیراست. (این چند جمله‌ای به سادگی به اولین ضابطهٔ ما واگذار نمی‌شود).

تعریف: اگر p یک عدد اول باشد، آنگاه $\Phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+...+x+1$ را چند جمله‌ای تقسیم دایرهٔ p ام می‌نامیم .

نتیجه ۲۵: به ازای هر عدد اول p چند جمله‌ای تقسیم دایره pام بر Q تحویل ناپذیراست .

برهان: تمرین ۶۹ را به یاد آورید، چند جمله‌ای $f(x)$ تحویل‌ناپذیر است اگر و فقط اگر $f(x+c)$ تحویل‌ناپذیر باشد، که c یک ثابت می‌باشد. بخصوص $\Phi_p(x)=\frac{x^p-1}{x-1}$ تحویل‌ناپذیر است اگر و فقط اگر $\Phi_p(x+1)=\frac{(x+1)^p-1}{x}$ تحویل‌ناپذیر باشد. چند جمله‌ای اخیر برابر $x^{p-1}+px^{p-2}+\binom{p}{2}x^{p-3}+...+p$ است ، که $\binom{p}{i}$ ضریب دوجمله‌ای می‌باشد. چون p اول است، با استفاده از تمرین ۷ و بکاربردن ضابطهٔ آیزنشتاین، نتیجه می‌گیریم که $\Phi_p(x)$ تحویل‌ناپذیر است . $\square$

نتیجه ۲۶: اگر $a\neq\pm1$ یک عددصحیح مربع آزادباشد ،آنگاه‌به‌ازای هر $n\geq2$ ، x^n-a بر Q تحویل ناپذیراست .

برهان: چون $a\neq\pm1$، عدد اول p وجود دارد که a را عاد می‌کند، و با بکاربردن ضابطهٔ آیزنشتاین و این عدد اول حکم نتیجه می‌شود. □

نتیجهٔ قبل نشان می‌دهد که چند جمله‌ایهای تحویل‌ناپذیر از درجهٔ دلخواه n بر Q وجود دارند.

فرمولهای کلاسیکی

اکنون فرمولهای کلاسیکی برای ریشه‌های معادلات درجهٔ دوم، درجهٔ سوم و درجهٔ چهارم را به دست می‌آوریم. معادلهٔ درجهٔ دوم $X^2 + bX + c = 0$ را در نظر می‌گیریم. به جای X قرارمی‌دهیم $X = x - \frac{b}{2}$، این معادله به $x^2 - \frac{b^2}{4}+c=0$ تبدیل می‌شود، و از آن نتیجه می‌شود که $x=\pm\frac{1}{2}\sqrt{b^2-4c}$. البته، فرمول معمولی با قراردادن $X+\frac{b}{2}$ بجای x به‌دست می‌آید.

معادلهٔدرجهٔ سوم $X^3 + aX^2 + bX + c = 0$ بعد از قراردادن $X=x - \frac{a}{3}$ به جای X به $x^3 + qx + r = 0$ تبدیل می‌شود. همانند بالا، یک فرمول برای محاسبهٔ ریشه‌های این معادله،یک فرمول برای محاسبه ریشه‌های معادلهٔ اصلی ارائه خواهد داد. فرمول به دست‌آمده ناشی از اسپیپو دل فرو[1] (ca.۱۵۱۵) می‌باشد، یک فرمول معادل بوسیلهٔ تارتاگلیا[2] تقریباً در همان زمان کشف شد، و برای نخستین بار در چاپ کتاب کاردان[3](۱۵۴۵) ظاهر شد. قرارمی‌دهیم $x=y+z$. در این صورت

$$x^3=(y+z)^3=y^3+z^3+3(y^2z+yz^2)=y^3+z^3+3xyz$$

بنابراین $y^3+z^3+(3yz+q)x+r=0$. (۱)

در اینجا محدودیت $x=y+z$ را بر y و z اعمال کردیم. اکنون محدودیت دوم،

1. Scipio del Ferro 2. Tartaglia 3. Cardan

$yz = -\frac{q}{3}$ را اعمال می‌کنیم ،بنابر این در معادلهٔ (۱) ،جملهٔ خطی x حذف می‌شود. داریم $y^3+z^3 = -r$ و $y^3z^3 = -q^3/27$. این دو معادله برحسب y^3 و z^3 حل شده‌اند.به تفصیل $y^3 - q^3/27y^3 = -r$، و بنابراین $y^6+ry^3-q^3/27=0$ و $z^6+rz^3-q^3/27=0$.

از فرمول درجهٔ دوم نتیجه می‌شود که

$$z^3=\frac{1}{2}(-r-\sqrt{r^2+4q^3/27}) \quad \text{و} \quad y^3=\frac{1}{2}(-r-\sqrt{r^2+4q^3/27})$$

چون $y^3z^3= -q^3/27$، می‌توانیم y و z را انتخاب کنیم به طوری که $yz = -q/3$. اگر $\omega=e^{2\pi i/3}$ یک ریشهٔ سوم واحد باشد، در این صورت شش ریشهٔ سوم y، ωy، $\omega^2 y$، z، ωz و $\omega^2 z$ موجود می‌باشند. این ریشه‌ها ممکن است طوری جفت شوند که حاصلضرب آنها برابر $-\frac{q}{3}$ باشد: $(\omega z)(\omega^2 y)=(\omega^2 z)(\omega y) = yz = -\frac{q}{3}$. نتیجه می‌گیریم که $y+z$ و $\omega y+\omega^2 z$ و $\omega^2 y+\omega z$ ریشه‌های چندجمله‌ای درجهٔ‌سوم‌می‌باشند، که $y=\left[\frac{1}{2}(-r+\sqrt{r^2+4q^3/27})\right]^{1/3}$ و $z=\left[\frac{1}{2}(-r-\sqrt{r^2+4q^3/27})\right]^{1/3}$ ، این فرمول درجهٔ سوم می‌باشد.

در کتاب معروف فیزیکدان متفکر آر - فین‌من[1] فرمول درجهٔ سوم که در گسترش علوم پیشرفته مهم بود، یک نتیجهٔ مجهول دیرینه می‌باشد. به خاطر داشته باشیم که سال ۱۵۱۵ همزمان با مارتین لادِر[2] و شروع اصلاحات و دورهٔ تجدید حیات ادبی و فرهنگی به طور واقعی می‌باشد.

فرمول درجهٔ چهار بوسیلهٔ لایگی فراری[3] (ca. ۱۵۴۵)، کشف شد. اما روش دکارت[4] را معرفی می‌کنیم. چند جمله‌ای درجهٔ چهار $X^4+aX^3+bX^2+cX+d$، را

---

1. R.P.Fynman, "what do you care what other people think?" Further adventures of a curios character, Bantam, 1988, page 95.

2. Martin Luther.

3. Luigi Ferrari.

4. Descartes.

در نظر می‌گیریم، $X=x-\frac{a}{4}$ را به جای X قرارمی‌دهیم، چند جمله‌ای به فرم $f(x)=x^4+qx^2+rx+s$ را به دست می آوریم. می نویسیم
$x^4+qx^2+rx+s=(x^2+kx+l)(x^2-kx+m)$ که k، l و m مشخص می شوند. (جملهٔ خطی در عامل دوم $-k$ می‌باشد زیرا درجهٔ چهاردارای جملهٔ درجهٔ سه نیست). اگر k ، l و m معین باشند، آنگاه مسأله با بکاربردن فرمول درجهٔ دوم حل می‌شود. با بسط طرف راست و مساوی قراردادن ضرایب جملات مشابه خواهیم داشت :

$$lm = s \;، \; k(m-l)=r \quad ، \quad l+m-k^2=q$$

از دو معادلهٔ اول نتیجه شود که $2m=k^2+q+\frac{r}{k}$ ، $2l = k^2+q-\frac{r}{k}$.
با قراردادن در معادلهٔ سوم نتیجه می‌شود که $k^6+2qk^4+(q^2-4s)k^2-r^2=0$. این معادله برحسب k^2 از درجهٔ سه می‌باشد (بعداً به طور اساسی با درجه سوم حلال برخورد خواهیم کرد)، و با استفاده از فرمول درجهٔ سوم برحسب k^2 می‌توان آن را حل کرد. اکنون به سادگی l،k ، m مشخص می‌شوند، و بنابراین ریشه‌های f(x) مشخص می‌شوند.

دیدن اینکه چرا نیاکان ما برای یافتن یک فرمول مشابه برای درجهٔ پنجم وسوسه شده‌اند، ساده است، محققاً نتیجهٔ نبوغ آنان بوده است .

میدانهای شکافنده

پیش از این مشاهده کردیم که اگر F یک زیرمیدان E باشد، آنگاه E را می‌توان به عنوان یک فضای برداری بر F در نظر گرفت .

تعریف: اگر F یک زیرمیدان E باشد، گوییم E یک توسیع میدان F است و می‌نویسیم E/F یک توسیع میدان است. بُعد E به عنوان یک فضای برداری بر میدان F در نظر گرفته می‌شود و درجهٔ E بر F نامیده می‌شود و با [E:F] نمایش داده می‌شود. گوییم

E/F یک توسیع متناهی است اگر $[E:F]$ متناهی باشد.

توجه کنیم که کلمهٔ توسیع نقطه نظر را برمی‌گرداند. به جای تمرکز روی زیرمیدانهای F از E، روی میدانهای بزرگتر E شامل F تمرکز می‌کنیم.

قضیه ۲۷: فرض کنیم $p(x)\in F[x]$ یک چند جمله‌ای تحویل ناپذیراز درجهٔ d باشد. در این صورت $E=\dfrac{F[x]}{(p(x))}$ یک توسیع میدان F از درجهٔ d می‌باشد.

برهان: ایده‌ال $(p(x))$ را با I و $x+I$ در E را با α نشان می‌دهیم، کافی است ثابت کنیم که $\{1,\alpha,\alpha^2,...,\alpha^{d-1}\}$ یک پایهٔ E بر F است. اگر به ازای $0\leq i\leq d-1$، a_i از F موجود باشند که $\sum a_i\alpha^i=0$، آنگاه α یک ریشهٔ چند جمله‌ای $f(x)=\sum a_ix^i$ از درجهٔ کمتر از d می‌باشد و متناقض با این است که $p(x)$ یک چند جمله‌ای با کمترین درجه دارای α به عنوان یک ریشه می‌باشد. بنابراین $\{1,\alpha,\alpha^2,...,\alpha^{d-1}\}$ مستقل خطی است. هر عضو از E به صورت $f(x)+I$ می‌باشد، بنابرالگوریتم تقسیم $q(x)$ و $r(x)$ ای موجودند که $f(x)=p(x)q(x)+r(x)$ که $\partial r<\partial p=d$ و $f(x)+I=r(x)+I$. بنابراین E بوسیلهٔ $\{1,\alpha,\alpha^2,...,\alpha^{d-1}\}$ تولید می‌شود و بنابراین آن یک پایه است. $\square$

تعریف: فرض کنیم E/F یک توسیع میدان باشد، و $\alpha_1,\alpha_2,...,\alpha_n\in E$. در این صورت $F(\alpha_1,\alpha_2,...,\alpha_n)$ کوچکترین زیرمیدان E شامل F و $\alpha_n,...,\alpha_2,\alpha_1$ می‌باشد، و آن میدان به‌دست آمده بوسیلهٔ الحاق α_1 , α_2 , ... , α_n به F نامیده می‌شود. توسیع E/F یک توسیع ساده است در صورتی که $\alpha\in E$ موجود باشد که

$$E=F(\alpha)=\{\frac{f(\alpha)}{g(\alpha)}\ ;\ f(x)\ ,\ g(x)\in F[x]\ ,\ g(\alpha)\neq 0\}\ .$$

تعریف: فرض کنیم $\alpha\in E$ و E/F یک توسیع میدان باشد. در این صورت α بر F جبری است اگر α ریشهٔ یک چند جمله‌ای تکین از $F[x]$ باشد، در غیراین صورت α بر F متعالی (غیرجبری) می‌باشد. توسیع E/F جبری نامیده می‌شود اگر هر عضو از E بر

F جبری باشد.

وقتی می‌گوییم که π یا e متعالی است، معمولاً به این معنی است که بر Q متعالی می‌باشند. اگر F یک میدان باشد، فرض کنیم $F(x)$ نمایش میدان تمام توابع گویا بر F، یعنی، میدان کسرهای $F[x]$ باشد، و اعضای آن تمام $\frac{f(x)}{g(x)}$ هایی می‌باشند که $f(x),g(x)\in F[x]$. در این حالت x بر F متعالی است.

تمرین :

*۷۳. اگر σ یک ایزومورفیسم از $F(\alpha_1,\alpha_2,...,\alpha_n)$ به خودش باشد به طوری که به ازای $i=1,2,...,n$، $\sigma(\alpha_i)=\alpha_i$ و به ازای هر $a\in F$، $\sigma(a)=a$، آنگاه σ همانی است.

اگر $\sigma , \tau : F(\alpha_1,\alpha_2,...,\alpha_n) \longrightarrow E$ به طور نقطه‌ای F را ثابت نگه دارند و به ازای هر i، $\sigma(\alpha_i)= \tau(\alpha_i)$ آنگاه $\sigma = \tau$.

*۷۴. اگر E/F یک توسیع متناهی باشد، آنگاه E/F جبری است.

قضیه ۲۸: فرض کنیم E/F یک توسیع میدان باشد، و $\alpha\in E$ بر F جبری باشد.

(آ) یک چند جمله‌ای تحویل‌ناپذیر تکین $p(x)\in F[x]$ دارای α به عنوان یک ریشه وجود دارد.

(ب) $p(x)$ یک چند جمله‌ای تکین از کمترین درجه در $F[x]$ دارای α به عنوان یک ریشه می‌باشد، بنابراین منحصربفرد است.

(ج) بوسیلهٔ یک ایزومورفیسم که F را به طور نقطه‌ای ثابت نگه می‌دارد، $F(\alpha)\cong\frac{F[x]}{(p(x))}$.

(د) $[F(\alpha):F]=\partial p$.

برهان: $p(x)$ را به عنوان یک چند جمله‌ای تکین از کمترین درجه در $F[x]$ دارای α به عنوان یک ریشه انتخاب می‌کنیم. ($p(x)$ وجود دارد زیرا α بر F جبری است) . نگاشت

ارزیاب $F(\alpha) \longrightarrow F[x]$ با ضابطهٔ $f(\alpha) \longrightarrow f(x)$ پوشاست و دارای هستهٔ $(p(x))$ می‌باشد، بنابر قضیهٔ اول ایزومورفیسم نتیجه می‌شود که $F(\alpha)\cong\frac{F[x]}{(p(x))}$. (که F را ثابت نگه می‌دارد). چون $F(\alpha)$ یک میدان است، ایده‌آل $(p(x))$ ماکسیمال است، بنابراین یک ایده‌آل اول است، و لذا $p(x)$ تحویل‌ناپذیر است. بالاخره، بنابر قضیه ۲۷، قسمت (د) برقرار است. □

تعریف: چندجمله‌ای $p(x)$ در قضیهٔ ۲۸، چندجمله‌ای تحویل‌ناپذیر α بر F نامیده می‌شود.

اگر α بر F جبری باشد، آنگاه $F(\alpha)$ همانند توابع گویا برحسب α به سادگی با $F(\alpha)$ به عنوان چند جمله‌ایهای برحسب α توصیف می‌شود. بخصوص، $a(\alpha)$ معکوس ضربی $f(\alpha)$ می‌باشد، که $a(x)f(x)+b(x)p(x)=1$ و $p(x)$ چند جمله‌ای تحویل‌ناپذیر α می‌باشد.

نتیجه ۲۹ : فرض کنیم $\sigma : F \longrightarrow F'$ ایزومورفیسم میدانهاباشد، و $\sigma^*:F[x] \longrightarrow F'[x]$ (تعریف‌شده‌بوسیلهٔ $\sigma^*(\sum r_ix^i)= \sum\sigma(r_i)x^i$)، ایزومورفیسم متناظر از حلقه‌ها باشد، فرض کنیم $p(x)\in F[x]$ تحویل‌ناپذیر باشد و $p^*(x)=\sigma^*(p(x))\in F'[x]$. اگر β یک ریشهٔ $p(x)$ و β' یک ریشه $p^*(x)$ باشد، دراین صورت یک ایزومورفیسم منحصر بفرد $\breve{\sigma} : F(\beta) \longrightarrow F'(\beta')$ با $\breve{\sigma}(\beta)=\beta'$ که توسیع σ می‌باشد وجود دارد.

$$\begin{tikzcd} F(\beta) \arrow[r, "\breve{\sigma}"] \arrow[d, dash] & F'(\beta') \arrow[d, dash] \\ F \arrow[r, "\sigma"'] & F' \end{tikzcd}$$

برهان: ایزومورفیسم $\sigma^*: F[x] \longrightarrow F'[x]$ ایده‌آل $(p(x))$ را به ایده‌آل $(p^*(x))$ می‌برد، و بنابراین وجود $\breve{\sigma}$ از قضیه و تمرین ۳۹ نتیجه می‌شود، یکتایی $\breve{\sigma}$ از تمرین ۷۳ نتیجه می‌شود. (روش دیگر برهان تعریف $\breve{\sigma} : F(\beta) \longrightarrow F'(\beta')$ بوسیلهٔ $\breve{\sigma}(\sum r_i\beta^i) = \sum \sigma(r_i)(\beta')^i$ می‌باشد. البته باید نشان داد که $\breve{\sigma}$ خوشتعریف و یک ایزومورفیسم است). □

تعریف: یک میدان شکافندهٔ $f(x) \in F[x]$ یک توسیع میدان E/F می‌باشد، که $f(x)$ برآن شکافته می‌شود، (به صورت حاصلضرب عوامل خطی نوشته می‌شود) در حالی که $f(x)$ بر هیچ زیر میدان واقعی (سره) از E شکافته نمی‌شود.

مثال: اگر α یک ریشهٔ سوم اولیه واحد باشد، آنگاه $x^3 - 1 \in Q[x]$ بر C شکافته می‌شود، اما میدان شکافندهٔ آن $Q(\alpha)$ می‌باشد.

قضیه ۳۰ : هرچند جمله‌ای $f(x) \in F[x]$ دارای یک میدان شکافنده می‌باشد.

برهان: بنابرقضیهٔ کرونکر (قضیه ۱۷)، یک توسیع میدان K/F وجود دارد که $f(x)$ بر آن شکافته می‌شود. تعریف می‌کنیم $E = F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ که $\alpha_1,\alpha_2,\ldots,\alpha_n$ همهٔ ریشه‌های $f(x)$ در K می‌باشند. واضح است که $f(x)$ بر E شکافته می‌شود، و $f(x)$ بر هر زیرمیدان واقعی از E شکافته نمی‌شود. (که لزوماً یکی از α_iها حذف می‌شود). □

لم ۳۱ : اگر $F \subset B \subset E$ میدانهایی با $[E : B]$ و $[B : F]$ متناهی باشند، آنگاه E/F متناهی است و $[E : F] = [E : B][B : F]$.

برهان: فرض کنیم $\{\alpha_1,\alpha_2,\ldots,\alpha_m\}$ یک پایهٔ E/B، و $\{\beta_1,\beta_2,\ldots,\beta_n\}$ یک پایهٔ B/F باشد. کافی است ثابت کنیم که $\{\beta_j\alpha_i ; 1 \leq i \leq m , 1 \leq j \leq n\}$ یک پایهٔ E/F است. این یک مجموعه مولد است. اگر $\gamma \in E$، آنگاه b_iهایی در B وجود دارند که $\gamma = \sum b_i\alpha_i$. اما هر $b_i = \sum c_{ij}\beta_j$ به ازای c_{ij} در F، بنابراین $\gamma = \sum c_{ij}\beta_j\alpha_i$. برای دیدن

اینکه این مجموعه مستقل می‌باشد، فرض کنیم که $\sum c_{ij}\beta_j\alpha_i = 0$ به ازای c_{ij} در F. اکنون $b_i = \sum c_{ij}\beta_j \in B$، بنابر مستقل بودن α_iها بر B نتیجه می‌شود که به ازای هر i، $b_i=0$. بنابراین به ازای هر i ، $\sum c_{ij}\beta_j = 0$ و بنابر مستقل بودن β_jها بر F نتیجه می‌شود که به ازای هر i,j ، $c_{ij} = 0$ ، همان نتیجهٔ مطلوب است. □

تمرین :

۷۵ . اگر $F \subset B \subset E$ میدانهایی باشند و توسیع E/F متناهی باشد، آنگاه E/B و B/F متناهی‌اند، و $[E:F] = [E:B]\,[B:F]$.

مثال : فرض کنیم $E = Q(\sqrt{2}, \sqrt{3})$ و $F = Q(\sqrt{2})$. اکنون $\sqrt{3}$ بر Q جبری است و چند جمله‌ای تحویل ناپذیرآن $x^2 - 3$ می‌باشد، از آن نتیجه می‌شود که $\sqrt{3}$ بر F جبری است. بعلاوه، چند جمله‌ای تحویل‌ناپذیر $p(x)$ از $\sqrt{3}$ بر $Q(\sqrt{2})$ یک مقسوم‌علیه x^2-3 می‌باشد، همچنین $[E:Q(\sqrt{2})] \leq 2$ (چون $E = Q(\sqrt{2},\sqrt{3}) = Q(\sqrt{2})(\sqrt{3})$). در واقع، $[E:Q(\sqrt{2})]=2$ زیرا $\sqrt{3} \notin Q(\sqrt{2})$ (a و b گویا وجود ندارند که $\sqrt{3}=a+b\sqrt{2}$).

عضو $\alpha = \sqrt{2} + \sqrt{3}$ از E را در نظر می‌گیریم. توجه داریم که α بر Q جبری است زیرا $[E : Q]=[E:Q(\sqrt{2})][Q(\sqrt{2}) : Q] = 4$، بنابر تمرین ۷۴، E/Q یک توسیع جبری است. چند جمله‌ای تحویل‌ناپذیر α چیست؟

$\alpha^2=(\sqrt{2}+\sqrt{3})^2=5+2\sqrt{6}$ و $\alpha^2-5=2\sqrt{6}$، بنابراین $\alpha^4-10\alpha^2+1=0$.

بنابرتمرین ۶۷ ، چند جمله‌ای $p(x)=x^4-10x^2+1$ بر Q تحویل‌ناپذیراست. از آن نتیجه می‌شود که $E=Q(\sqrt{2}, \sqrt{3})=Q(\sqrt{2} + \sqrt{3}) = Q(\alpha)$ ، زیرا

$4=[E:Q]=[E:Q(\alpha)][Q(\alpha):Q]=4[E:Q(\alpha)]$، یعنی E یک توسیع ساده‌است.

α^{-1} چیست؟ چون $\alpha^4-10\alpha^2+1=0$ ، داریم $\alpha(10\alpha - \alpha^3)=1$ بنابراین $\alpha^{-1}=10\alpha-\alpha^3$. باقراردادن $\sqrt{2}+\sqrt{3}$ به‌جای α، α^{-1} رامی‌توان برحسب $\sqrt{2}$ و $\sqrt{3}$ نوشت.

پی‌آمد بعدی نتیجهٔ ۲۹ را تعمیم می‌دهد، چنانکه بیان می‌کند، ضروری نیست که چند جمله‌ایها تحویل‌ناپذیر باشند. قسمت دوم نوع جدیدی از یک چند جمله‌ای را معرفی می‌کند.

تعریف: فرض کنیم $f(x)\in F[x]$ دارای تجزیه به تحویل ناپذیرهای (نه لزوماً متمایز) $f(x)=ap_1(x)p_2(x)...p_t(x)$ باشد. در این صورت $f(x)$ جداپذیر است اگر هر $p_i(x)$ دارای ریشه‌های تکراری نباشد.

فرض کنیم F یک میدان و $q(x)\in F[x]$ تحویل‌ناپذیر باشد. اگر مشتق $q'(x)$ چند جمله‌ای صفر نباشد، آنگاه درجهٔ آن از درجهٔ $q(x)$ کمتر است، بنابراین $(q(x),q'(x))=1$ و بنابر تمرین ۴۱، $q(x)$ جداپذیراست. از آن نتیجه می‌شود که اگر F دارای مشخصهٔ 0 باشد، آنگاه هر چند جمله‌ای جداپذیر است، اگر F دارای مشخصهٔ p باشد، آنگاه ممکن است که $q'(x)=0$ (مثال زیر را ببینید). میدانهایی که در آنها هر چند جمله‌ای غیرثابت جداپذیر می‌باشد کامل نامیده می‌شوند. (اگر E/F یک توسیع باشد، آنگاه $\alpha\in E$ جداپذیر نامیده می‌شود، اگر α متعالی یا چند جمله‌ای تحویل‌ناپذیر آن جداپذیرباشد، یک توسیع جداپذیر نامیده می‌شود اگر هر عضو آن جداپذیرباشد).

مثال :این مثالی از یک توسیع جداناپذیراست. فرض کنیم $K = Z_p(t)$، میدان تمام توابع گویا بر Z_p باشد. چند جمله‌ای $q(x)=x^p - t$ بر K تحویل‌ناپذیراست. میدان شکافندهٔ E/K از آن جداپذیر نمی‌باشد، اگر $\alpha\in E$ یک ریشهٔ $q(x)$ باشد، آنگاه در $E[x]$، $x^p-t=(x-\alpha)^p$ زیرا E دارای مشخصهٔ p است. توجه کنید که $q'(x)=0$.

تمرین :

۷۶ . نشان دهید که میدان F از مشخصهٔ p کامل است اگر و فقط اگر هر عضو از F دارای یک ریشهٔ p ام در F باشد.

۷۷. نشان دهید که هر میدان متناهی F کامل است. (راهنمایی: تابع $F \longrightarrow F$ با ضابطهٔ $a \longrightarrow a^p$ یک به یک است).

قضیه ۳۲: فرض کنیم $\sigma : F \longrightarrow F'$ ایزومورفیسم میدانها باشد و $f(x) \in F[x]$ و $\sigma^*(f(x)) = f^*(x)$ [1] چند جمله‌ای متناظر در $F'[x]$ باشد، فرض کنیم E میدان‌شکافندهٔ $f(x)$ بر F و E' میدان شکافندهٔ $f^*(x)$ بر F' باشد.

(آ) یک ایزومورفیسم $\bar{\sigma}: E \longrightarrow E'$ که σ را گسترش می‌دهد وجود دارد.

(ب) اگر $f(x)$ جداپذیر باشد، آنگاه دقیقاً $[E:F]$ گسترش $\bar{\sigma}$ از σ وجود دارد.

برهان: (آ) اثبات به استقراء بر $[E:F]$ است. اگر $[E:F]=1$، آنگاه $E=F$ و $f(x)$ به صورت حاصلضرب عوامل خطی در $F[x]$ می‌باشد، از آن نتیجه می‌شود که $f^*(x)$ نیز به صورت حاصلضرب عوامل خطی است، و بنابر این $E' = F'$. بنابر این می‌توانیم تعریف کنیم $\bar{\sigma} = \sigma$. اگر $[E:F]>1$، عامل تحویل‌ناپذیر $p(x)$ از $f(x)$ دارای درجهٔ بزرگتر یا مساوی ۲ و یک ریشهٔ β از $p(x)$ را انتخاب می‌کنیم، بنابراین β یک ریشه از $f(x)$ است که باید عضو E باشد. فرض کنیم $p^*(x) \in F'[x]$ متناظر $p(x)$ و $\beta' \in E'$ یک ریشه از $p^*(x)$ باشد. بنابر نتیجه ۲۹، به ازای این β' یک ایزومورفیسم منحصر بفرد $\check{\sigma} : F(\beta) \longrightarrow F'(\beta')$ با $\check{\sigma}(\beta) = \beta'$ که σ را گسترش می‌دهد وجود دارد. اکنون E میدان شکافندهٔ $f(x)$ بر $F(\beta)$ و E' میدان شکافندهٔ $f^*(x)$ بر $F'(\beta')$ است. چون $[F(\beta):F] \geq 2$ و $[E:F] = [E:F(\beta)]\ [F(\beta):F]$، از آن نتیجه می‌شود که $[E:F(\beta)] < [E:F]$. بنابر استقراء گسترش $\bar{\sigma}: E \longrightarrow E$ از $\check{\sigma}$ وجود دارد، بنابر این $\bar{\sigma}$ گسترش σ می‌باشد.

---

۱ - اگر $f(x) = \sum a_i x^i$، آنگاه $\sigma^*(f(x)) = \sum \sigma(a_i) x^i$.

(ب) برهان (آ) را تعدیل می‌کنیم، دوباره به استقراء بر $[E:F]$ عمل می‌کنیم. اگر $[E:F]>1$، آنگاه می‌توانیم $f(x)$ را بوسیلهٔ $g(x)$ بدون تغییری در مسأله جایگزین کنیم. اگر $d>1$، یک ریشهٔ β از $p(x)$ را انتخاب می‌کنیم. اگر $\bar{\sigma}$ یک گسترش دلخواه از σ به E باشد، آنگاه $\sigma(\beta)=\beta'$ یک ریشه از $p^*(x)$ است، چون $f^*(x)$ جداپذیراست، $p^*(x)$ دارای دقیقاً d ریشهٔ $\beta'\in E'$ می‌باشد، بنابر نتیجه ۲۹، به ازای هر β' دقیقاً d ایزومورفیسم $\check{\sigma}:F(\beta)\longrightarrow F'(\beta')$ که گسترش σ می‌باشند وجود دارند. اکنون E میدان شکافندهٔ $f(x)$ بر $F(\beta)$ و E' میدان شکافندهٔ $f^*(x)$ بر $F'(\beta')$ است. چون $[E:F(\beta)]=\frac{[E:F]}{d}$، بنابراستقراء هر یک از d ایزومورفیسمهای $\check{\sigma}$ دارای دقیقاً $\frac{[E:F]}{d}$ توسیع به E می‌باشند ، بنابراین، σ دارای دقیقاً $[E:F]$ توسیع $\bar{\sigma}$ می‌باشد، زیرا هر توسیع τ از σ دارای $\tau|F(\beta)$ برابر $\check{\sigma}$ ای می‌باشد. □

نتیجه ۳۳: اگر $f(x)\in F[x]$، آنگاه هر دو میدان شکافندهٔ $f(x)$ بر F بوسیلهٔ یک ایزومورفیسم که F را به طور نقطه‌ای ثابت نگه می‌دارد ایزومورف می‌باشند.

برهان: انتخاب می‌کنیم $F=F'$ و σ بر F همانی باشد. □

نتیجه ۳۴: (ای - اچ - مور[1]) هر دو میدان از مرتبهٔ p^n ایزومورف می‌باشند.

برهان: هر میدان F از مرتبهٔ p^n میدان شکافندهٔ x^q-x بر Z_p می‌باشد، که $q=p^n$. □

میدان از مرتبهٔ p^n را میدان گالوای از این مرتبه نامند و آن را با $GF(p^n)$ نشان می‌دهند، گرچه $GF(p)$ معمولاً به صورت Z_p نشان داده می‌شود.

تمرین ۶۴ ساختار $GF(8)$ را با راهنمایی به تجزیهٔ $x^8-x=x^8+x$ بر Z_2 سؤال می‌کند. اکنون بر Z_2، $x^8+x=x(x+1)(x^3+x+1)(x^3+x^2+1)$ و هر دو چندجمله‌ای

1. E.H.Moore

درجــهٔ ســوم تــحویل‌ناپذیر مــی‌باشند. مــیدانــهای $\frac{Z_2[x]}{(x^3+x+1)}$ و $\frac{Z_2[x]}{(x^3+x^2+1)}$ ایزومورف‌اند زیرا هر دو میدان از مرتبهٔ ۸ می‌باشند. به طور مشابه می‌توان دید که اگر $p(x)$ و $q(x)$ چــند جــمله‌ایــهای تــحویل‌ناپذیر از درجات مساوی بـر Z_p بـاشند، آنگاه $\frac{Z_p[x]}{(p(x))}$ و $\frac{Z_p[x]}{(q(x))}$ ایزومورف می‌باشند.

حل‌پذیری بوسیلهٔ رادیکالها

تعریف: توسیع میدان B/F یک توسیع محض است اگر $B = F(\alpha)$، کـه بـه ازای عددی صحیح و مثبت m، α^m در F قراردارد.

تعریف: فرض کنیم F یک میدان باشد و $f(x)\in F[x]$، در این صورت $f(x)$ بـوسیلهٔ رادیکالها بر F حل‌پذیر است اگر یک برج از میدانـها مـانند $F = B_0 \subset B_1 \subset \dots \subset B_t$ موجود باشد، که هر $\frac{B_{i+1}}{B_i}$ یک توسیع محض است و B_t شامل میدان شکـافندهٔ E از $f(x)$ بر F است. B_t/F را یک توسیع رادیکال می‌نامند.

تمرین :

۷۸* . اگر $f(x)$ از درجهٔ n و بوسیلهٔ رادیکالها بر F حل‌پذیر باشد، آنگـاه یک بـرج از توسیع های محض $F=B_0 \subset B_1 \subset \dots \subset B_t$ که هر $[B_{i+1}:B_i]$ عددی اول می‌باشد وجود دارد.

۷۹* . فرض کنیم p عددی اول باشد و F یک میدان شامل تمام ریشه‌های p ام یکانی بـاشد. اگــر $a\in F$، ثـابت کـنید کـه $x^p - a$ یـا بـر F شکـافته مـی‌شود یـا تحویل‌ناپذیراست. (به عنوان نتیجهٔ ۵۲ یک حل تفننی ارائه خواهیم داد) .

۸۰ . فرض‌کنیم B/F یک توسیع متناهی باشد . ثابت کنید که توسیع E/B موجود است بــه‌طوری کـه E/F مـیدان شکـافندهٔ چـند جـمله‌ای مـانند $f(x)\in F[x]$ می‌باشد. کوچکترین توسیع E/F با چنین خاصیتی بستار شکافندهٔ B/F نامیده

شده است. (اگر f(x) یک چندجمله‌ای جداپذیر باشد، آنگاه E/F بستار نرمال B/F نامیده شده است).

*۸۱. اگر E/F یک توسیع میدان باشد و B و C میدانهای میانی باشند ($F\subset B\subset E$ و $F\subset C\subset E$)، آنگاه ترکیب آنها، $B\vee C$، زیر میدان E تولید شده بوسیلهٔ B و C، یعنی اشتراک تمام زیرمیدانهای E شامل B و C می‌باشد. نشان دهید که اگر E/F بستار شکافندهٔ B/F باشد، آنگاه $E=B_1 \vee B_2 \vee B_3 \vee \cdots \vee B_r$ که هر B_i بوسیلهٔ یک ایزومورفیسم که F را ثابت نگه می‌دارد با B ایزومورف می‌باشد.

*۸۲. با استفاده از تمرین قبلی ثابت کنید که بستار شکافندهٔ یک توسیع رادیکال خود یک توسیع رادیکال است. نتیجه بگیرید که، در تعریف حل‌پذیری بوسیلهٔ رادیکالها می‌توان فرض کرد که میدان B_t آخری میدان شکافندهٔ چند جمله‌ای بر F می‌باشد.

با نشان دادن اینکه چند جمله‌ایهای درجهٔ دوم، درجهٔ سوم و درجهٔ چهارم بر زیرمیدانهای F از C بوسیلهٔ رادیکالها حل‌پذیر می‌باشند، تعریف حل‌پذیری بوسیلهٔ رادیکالها را نشان می‌دهیم. (فرمولها برای میدان دلخواه F درست نمی‌باشند، به عنوان مثال، وقتی که F دارای مشخصهٔ ۲ باشد، فرمول درجهٔ دوم نمی‌تواند برقرارباشد).

اگر $f(x)=x^2+bx+c\in Q[x]$ ، تعریف می‌کنیم $F = Q(b, c)$ و $B=F(\sqrt{b^2-4c})$. در این صورت B/F یک توسیع محض است و B میدان شکافندهٔ f(x) بر F می‌باشد ، بنابر این f(x) بوسیلهٔ رادیکالها بر F حل‌پذیر می‌باشد.

اگر $f(x)=x^3+qx+r$ ، تعریف می‌کنیم $F = Q(q,r)$ و $B_1=F(\sqrt{r^2+4q^3/27})$ و $B_2=B_1(y)$ ، که $y^3=\frac{1}{2}(-r+\sqrt{r^2+4q^3/27})$. تعریف می‌کنیم $B_3 = B_2(z)$ ، که $z^3=\frac{1}{2}(-r-\sqrt{r^2+4q^3/27})$. فرمول درجهٔ سوم می‌گوید که ریشه‌های f(x) به

صورت $\omega y+\omega' z$ می‌باشند ،که ω و ω' ریشه‌های سوم یکانی‌اند و $(\omega y)(\omega' z)=-\frac{q}{3}$. بنابر این، اگر تعریف کنیم $B_4=B_3(\omega)$ ، آنگاه میدان شکافندهٔ E از f(x) مشمول در B_4 می‌باشد، و f(x) بوسیلهٔ رادیکالها حل‌پذیر است. توجه کنید که ممکن است E یک زیر میدان واقعی از B_4 باشد، زیرا E لازم نیست شامل ω باشد، به عنوان مثال ، f(x) ممکن است دارای سه ریشهٔ حقیقی و E یک زیر میدان R باشد.

اگر $f(x)=x^4+qx^2+rx+s$ ، تعریف می‌کنیم $F=Q(q,r,s)$. در بحث فرمول درجهٔ چهارم دیدیم که کافی است سه عدد l,k و m را پیداکنیم. اکنون k^2 یک ریشه از چند جمله‌ای درجهٔ سوم خاصی در F[x] می‌باشد، به طوری که یک برج از توسیع‌های میدان محض $F\subset B_1\subset\cdots\subset B_4$ با $k^2\in B_4$ موجود می‌باشد. تعریف می‌کنیم $B_5=B_4(k)$. چون $2m=k^2+q+\frac{r}{k}$ و $2l=k^2+q-\frac{r}{k}$ ، B_5 شامل l و m می‌باشد. فرمول درجهٔ چهارم نتیجه می‌دهد که ریشه‌های f(x) همان ریشه‌های $(x^2+kx+l)(x^2-kx+m)$ می‌باشند، به طوری که برج توسیع‌های محض می‌توانند با الحاق $\sqrt{k^2-4l}$ و $\sqrt{k^2-4m}$ دو مرحله طولانی‌تر شود، با توسیع قبلی، B_7 شامل میدان شکافنده f(x) می‌باشد. بنابر این f(x) بوسیلهٔ رادیکالها حل‌پذیر است .

بالعکس، واضح است که اگر چند جمله‌ای f(x) بوسیلهٔ رادیکالها حل‌پذیر باشد، آنگاه یک توصیف برای ریشه‌های آن برحسب جملات ضرایب، اعمال میدان، و استخراج ریشه‌ها وجود دارد.

گروه گالوا

لم بعد اساسی است، گرچه اثبات آن ساده می‌باشد.

لم ۳۵ : فرض‌کنیم $f(x)\in F[x]$ و E/F میدان‌شکافنده f(x) بر F باشد.اگر $\sigma: E\longrightarrow E$ یک اتومورفیسم (یک ایزومورفیسم از E به خودش) باشد، که F را به طور

نقطه‌ای ثابت نگه می‌دارد و اگر α یک ریشه $f(x)$ باشد، آنگاه $\sigma(\alpha)$ نیز یک ریشهٔ $f(x)$ است .

برهان: فرض‌کنیم $f(x) = a_0 + a_1x + \cdots + a_nx^n$ ، به طوری که $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. با بکاربردن σ نتیجه می‌شود که

$$\sigma(a_0)+\sigma(a_1)\sigma(\alpha)+\cdots+\sigma(a_n)\sigma(\alpha^n)=a_0+a_1\sigma(\alpha)+\cdots+a_n\sigma(\alpha)^n=0$$

زیرا σ، میدان F را ثابت نگه می‌دارد. بنابراین $\sigma(\alpha)$ یک ریشهٔ $f(x)$ است. □

تعریف[1]: فرض کنیم E/F یک توسیع میدان باشد. گروه گالوای E/F با $Gal(E/F)$ نشان داده می‌شود و مجموعهٔ تمام اتومورفیسمهای بر E که F را (به طور نقطه‌ای) ثابت نگه می‌دارند، تحت عمل دوتایی ترکیب می‌باشد. اگر $f(x)\in F[x]$ دارای میدان شکافندهٔ E باشد، آنگاه $Gal(E/F)$ گروه گالوای $f(x)$ است.

بررسی اینکه $Gal(E/F)$ یک گروه است ساده می‌باشد.

لم ۳۶ : اگر $f(x)\in F[x]$ دارای n ریشهٔ متمایز در میدان شکافندهٔ E از آن باشد، آنگاه $Gal(E/F)$ با یک زیرگروه از گروه متقارن S_n ایزومورف است .

برهان: فرض کنیم $X = \{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ مجموعهٔ تمام ریشه‌های $f(x)$ در E باشد. بنابرلم ۳۵، اگر $\sigma\in Gal(E/F)$ ، آنگاه $\sigma(X)=X$. به سادگی دیده می‌شود که نگاشت $Gal(E/F) \longrightarrow S_X$ تعریف شده بوسیلهٔ $\sigma \longmapsto \sigma \mid X$ یک هومومورفیسم می‌باشد، بنابر تمرین ۷۳، آن یک به یک است. بالاخره $S_X\cong S_n$. □

به عنوان مثال، گروه گالوای چند جمله‌ای درجهٔ چهارم یک زیرگروه از S_4

---

۱ - این تعریف از گالوا نیست، این تعریف نسخهٔ پیشرفتهٔ ایزومورف با نسخهٔ اصلی است که بوسیلهٔ امیل - آرتین معرفی شده است. عیب این تعریف آن است که به‌نظر نمی‌آید به طور طبیعی ناشی شود، پیوست ۴ را ببینید.

می‌باشد، و گروه گالوای چند جمله‌ای درجهٔ پنجم یک زیرگروه از S_5 می‌باشد.

قضیه ۳۷: اگر $f(x)\in F[x]$ یک چند جمله‌ای جداپذیر و E/F میدان شکافندهٔ آن باشد، آنگاه $|Gal(E/F)|=[E:F]$.

برهان: بنابرقضیهٔ ۳۲ قسمت (ب) با فرض $F=F'$ و $E=E'$ و همانی $\sigma:F\longrightarrow F$، دقیقاً $[E:F]$ ایزومورفیسم بر E که F را ثابت نگه می‌دارند موجود می‌باشند. □

مثالها:

۱. میدان شکافندهٔ x^2+1 بر R میدان C می‌باشد، وبنابرقضیهٔ ۳۶، $|Gal(C/R)|\leq 2$. درحقیقت $|Gal(C/R)|=2$ زیرایک گروه شامل اتومورفیسم $\sigma:z=a+ib\longrightarrow \bar{z}=a-ib$ می‌باشد. توجه کنید که $\sigma:i\longrightarrow -i$ و $\sigma:-i\longrightarrow i$، و بنابراین σ ریشه‌ها را جابه جا می‌کند. می‌توان دید که اعضای گروه گالوا باید به عنوان کلیات مزدوج مختلط در نظر گرفته شوند.

۲. فرض کنیم $f(x)=x^3-1\in Q[x]$، چون Q دارای مشخصهٔ صفر است، $f(x)$ جداپذیراست. اکنون $f(x)=(x-1)(x^2+x+1)$ تجزیهٔ $f(x)$ به تحویل ناپذیرها می‌باشد. اگر E میدان شکافندهٔ $f(x)$ بر Q باشد، آنگاه $E=Q(\omega)$ که ω یک ریشه سوم اولیهٔ یکانی‌است، یعنی ω یک‌ریشهٔ x^2+x+1 است. چون $|Gal(E/Q)|=[E:Q]=2$، بنابر قضیهٔ ۳۷، گروه گالوا دوری از مرتبهٔ ۲ می‌باشد.

۳. فرض کنیم $g(x)=x^3-2\in Q[x]$. $Q(\alpha,\omega)$ میدان شکافندهٔ $f(x)$ می‌باشد، که α ریشهٔ سوم حقیقی ۲ و ω یک ریشهٔ سوم مختلط یکانی است. چون $g(x)$ بر Q تحویل‌ناپذیراست، داریم $[Q(\alpha):Q]=3$. اما $Q(\alpha)$ شامل تمامی اعداد حقیقی است، و بنابراین نمی‌تواند میدان شکافندهٔ E از $g(x)$ باشد. لذا

$$|Gal(E/Q)| = [E:Q] = [E:Q(\alpha)]\,[Q(\alpha):Q]= 3\,[E:Q(\alpha)] > 3$$

بنابر قضیهٔ ۳۶، نتیجه می‌شود که $Gal(E/Q)\cong S_3$

تمرین :

۸۳* . فرض کنیم p عددی اول و F میدان شامل همهٔ ریشه‌های p ام یکانی باشد. اگر E/F یک توسیع محض از درجهٔ p باشد، آنگاه Gal (E/F) دوری از مرتبهٔ p می‌باشد.

۸۴* . فرض کنیم $f(x)\in F[x]$ و E/F یک میدان شکافنده و $G=Gal(E/F)$ گروه گالوا باشد.

(آ) اگر f(x) تحویل‌ناپذیر باشد، آنگاه G به طور متعدی بر مجموعهٔ تمام ریشه‌های f(x) عمل می‌کند. (اگر α و β دو ریشهٔ f(x) در E باشند، عضو σ از G وجود دارد که $\sigma(\alpha)=\beta$). (راهنمایی: قضیهٔ ۳۲(آ)).

(ب) اگر f(x) دارای ریشه‌های تکراری نباشد و G به طور متعدی بر ریشه‌ها عمل کند، آنگاه f(x) تحویل‌ناپذیراست. (راهنمایی: اگر $f(x)=g(x)h(x)$، آنگاه $(g(x),h(x))=1$ بمعم، اگر α یک ریشهٔ g(x) باشد به طوری که $\sigma(\alpha)$ یک ریشهٔ h(x) باشد، آنگاه $\sigma(\alpha)$ یک ریشهٔ مشترک از g(x) و h(x) می‌باشد).

لم ۳۸ : فرض کنیم $F\subset B\subset E$ یک برج از میدانها با میدان شکافندهٔ B/F از چند جمله‌ای f(x) از F[x] باشد. اگر $\sigma\in Gal(E/F)$ آنگاه $\sigma|B\in Gal(B/F)$.

برهان: کافی است ثابت کنیم که $\sigma(B)=B$. اگر $\alpha_1, \alpha_2, \ldots, \alpha_n$ ریشه‌های f(x) باشند، آنگاه $B=F(\alpha_1,\alpha_2,\ldots,\alpha_n)$. اکنون $\sigma(F)=F$ و به ازای هر i، $\sigma(\alpha_i)\in B$، از تمرین ۷۳ نتیجه می‌شود که $\sigma(B)=B$، و این همان نتیجهٔ مطلوب است. □

قضیه ۳۹: فرض کنیم $F\subset B\subset E$ یک برج از میدانهابا میدان شکافندهٔ B/F از چند

جمله‌ای $f(x)$ از $F[x]$ و میدان شکافندهٔ E/F از چندجمله‌ای $g(x)$ از $F[x]$ باشد. در این صورت $Gal(E/B)$ یک زیرگروه‌نرمال $Gal(E/F)$ می‌باشد و $Gal(E/F)/Gal(E/B) \cong Gal(E/F)$.

برهان: $\psi : Gal(E/F) \longrightarrow Gal(B/F)$ را با ضابطهٔ $\psi(\sigma) = \sigma|B$ تعریف می‌کنیم، لم ۳۸ می‌گوید که ψ مقادیرش را در $Gal(B/F)$ می‌گیرد. به سادگی دیده می‌شود که ψ یک هومومورفیسم با هستهٔ $Gal(E/B)$ می‌باشد، لذا یک زیرگروه نرمال $Gal(E/F)$ می‌باشد. اگر $\tau \in Gal(B/F)$ آنگاه قضیهٔ ۳۲ نشان می‌دهد که یک اتومورفیسم $\bar{\tau}$ از E با $\bar{\tau}|B = \tau$ وجود دارد. بنابراین ψ پوشاست، و از قضیهٔ اول ایزومورفیسم (قضیه A5) حکم نتیجه می‌شود. □

تبصره: فرض اینکه E/F یک میدان شکافنده است تنها اجازه می‌دهد که نشان دهیم ψ پوشاست. بدون این فرض تنها می‌توان ثابت کرد که گروه خارج قسمتی با یک زیرگروه از $Gal(B/F)$ ایزومورف می‌باشد.

توجه داریم که یک گروه متناهی حل‌پذیراست اگر دارای یک سری نرمال با گروههای خارج قسمتی آبلی باشد، بعلاوه، هر گروه خارج قسمتی و هر زیر گروه از یک گروه حل‌پذیر، حل‌پذیر می‌باشد(قضیه A20).

قضیه ۴۰: فرض کنیم $f(x) \in F[x]$ از درجهٔ n، و F شامل تمام ریشه‌های p ام یکانی به ازای هر مقسوم علیه اول p از $n!$ باشد. اگر $f(x)$ بوسیلهٔ رادیکالها حل‌پذیر باشد، آنگاه گروه گالوای آن یک گروه حل‌پذیراست.

برهان: چون $f(x)$ بوسیلهٔ رادیکالها حل‌پذیراست، یک توسیع رادیکال $F=B_0 \subset B_1 \subset \ldots \subset B_t$ با $E \subset B_t$ موجود است که E میدان شکافنده $f(x)$ بر F می‌باشد. بنابر تمرین ۷۸ می‌توان فرض کرد که هر $[B_{i+1}:B_i]$ اول است. تعریف می‌کنیم

$G_i=Gal(B_t/B_i)$. بنابر تمرین ۷۹، هر B_{i+1} میدان شکافنده چند جمله‌ای بر B_i می‌باشد، و همچنین قضیهٔ ۳۹ نشان می‌دهد که $G=G_0\supset G_1\supset ... \supset G_t=\{1\}$ یک سری نرمال است، بعلاوه ، $Gal(B_t/B_i)/Gal(B_t/B_{i+1})\cong Gal(B_{i+1}/B_i)$، و بنابر تمرین ۸۳ ، این گروه دوری از مرتبهٔ اول است. بنابراین ، G یک گروه حل‌پذیراست.

بالاخره، تمرین ۸۲ اجازه می‌دهد فرض کنیم که B_t میدان شکافندهٔ یک چندجمله‌ای بر F می‌باشد، همچنین کاربردهای دیگر قضیهٔ ۳۹ نشان می‌دهد که $Gal(E/F)$ یک گروه خارج قسمتی از گروه حل‌پذیر $G=Gal(B_t/F)$ می‌باشد، لذا بنابر قضیهٔ A20، آن حل‌پذیر است. □

ریشه‌های اولیهٔ یکانی

فرض قضیه ۴۰ که F شامل ریشه‌های یکانی خاصی باشد می‌تواند حذف شود. اما یک بحث مقدماتی از نظریهٔ گروهها را قبل از اثبات این موضوع ارائه می‌دهیم.

لم ۴۱: اگر $C=\langle a\rangle$ یک گروه دوری از مرتبهٔ n و مولد a باشد، آنگاه به ازای هر مقسوم‌علیه d از n ، گروه C دارای یک زیرگروه منحصر بفرد از مرتبهٔ d می‌باشد.

برهان: اگر $n=dc$ نشان می‌دهیم که a^c از مرتبهٔ d می‌باشد (وبنابراین $\langle a^c\rangle$ یک زیرگروه از مرتبه d است). واضح است که $(a^c)^d=1$، ادعا می‌کنیم که d کوچکترین توان است. اگر $(a^c)^r=1$ ، آنگاه $n\mid cr$ ، بنابراین $cr=ns=dcs$ (به ازای عدد صحیح s) و $r=ds\geq d$. برای اثبات یکتایی ، فرض کنیم که $\langle x\rangle$ یک زیرگروه از مرتبهٔ d باشد(بنابر لم A1 ، به خاطر داریم که هر زیرگروه از یک گروه دوری، دوری است). اکنون $x=a^m$ و $1=x^d=a^{md}$ ، بنابراین به ازای عدد صحیح k ، $md=nk$. بنابر این $x=a^m=(a^{n/d})^k=(a^c)^k$ ، بنابراین $\langle x\rangle\subset\langle a^c\rangle$. چون هر دو زیر گروه از مرتبهٔ d می‌باشند، در نتیجه $\langle x\rangle=\langle a^c\rangle$ □

یادآوری قضیه A2 : اگر C یک گروه دوری از مرتبهٔ n و مولد x باشد ، آنگاه x^k نیز یک مولد C می‌باشد اگر و فقط اگر k و n نسبت به هم اول باشند. در نتیجه اگر g(C) نمایش مجموعهٔ تمام مولدهای C باشد، آنگاه $\varphi(n) = |g(C)|$ ، که φ تابع φ اولر می‌باشد. ($\varphi(1)=1$ و اگر $n>1$ ، آنگاه $\varphi(n)=|\{k\in Z \; ; \; (k,n)=1 \; , \; 1\le k<n\}|$) .

قضیه ۴۲: اگر n یک عدد صحیح مثبت باشد، آنگاه $n = \sum\limits_{\substack{d|n \\ 1\le d\le n}} \varphi(d)$.

برهان: اگر G یک گروه باشد، به سادگی می‌توان دید که $G = \cup\, g(C)$ که C بر همهٔ زیرگروههای دوری G تغییر می‌کند. اگر G یک گروه دوری از مرتبهٔ n باشد، آنگاه با شمارش نتیجه می‌شود که $n=\sum |g(C)| = \sum\limits_{\substack{d|n \\ 1\le d\le n}} \varphi(d)$ ، که مجموع بر تمام مقسوم علیه‌های d از n تغییر می‌کند، و هر d با تکرار تعداد زیرگروههای دوری از مرتبهٔ d رخ می‌دهد. بنابر لم، هر d دقیقاً یک بار رخ می‌دهد. □

قضیه ۴۳: گروه G از مرتبهٔ n دوری است اگر و فقط اگر به ازای هر مقسوم علیه d از n ، حداکثر یک زیرگروه دوری مرتبهٔ d موجود باشد.

برهان: اگر G دوری باشد، آنگاه نتیجه از لم ۴۱ به دست می‌آید. بالعکس، G را به صورت اجتماع مجزای $G=\cup g(C)$ می‌نویسیم. بنابر این $n=|G| = \sum |g(C)|$ ، که مجموع بر همهٔ زیر گروههای دوری C از G می‌باشد. چون G دارای حداکثر یک زیرگروه دوری از مرتبهٔ d می‌باشد، قضیه ۴۲ نتیجه می‌دهد که $n=\sum |g(C)| \le \sum \varphi(d)=n$. بنابر این ، به ازای هر مقسوم علیه d از n گروه G دارای دقیقاً یک زیرگروه دوری از مرتبهٔ d می‌باشد، بخصوص، یک زیرگروه دوری از مرتبهٔ n موجود می‌باشد و G دوری است. □

قضیه ۴۴: اگر F یک میدان با گروه ضربی $F^* = F - \{0\}$ باشد، آنگاه هر زیرگروه متناهی G از F^* دوری است .

برهان: فرض کنیم $|G|=n$ و $d|n$. اگر C یک زیرگروه دوری G از مرتبهٔ d باشد، آنگاه قضیهٔ لاگرانژ نتیجه می‌دهد که $x^d=1$ به ازای هر d عضو x از C . اگر زیرگروه دوری دیگر از مرتبهٔ d موجود باشد، آنگاه G شامل حداقل $d+1$ عضو x با $x^d=1$ می‌باشد. اما چند جمله‌ای x^d-1 دارای حداکثر d ریشه در یک میدان می‌باشد، و لذا G دارای حداکثر یک زیرگروه دوری از مرتبه d می‌باشد. اکنون قضیهٔ ۴۳ نشان می‌دهد که G دوری است. □

نتیجه ۴۵: اگر n یک عدد صحیح مثبت و ثابت باشد، آنگاه همهٔ ریشه‌های nام یکانی در میدان F تشکیل یک گروه ضربی دوری می‌دهند.

نتیجه ۴۶: اگر F یک میدان متناهی باشد، آنگاه F^* دوری است و به ازای α ای، $F=Z_p(\alpha)$.

تعریف: یک مولد از F^* وقتی که F متناهی است یک عنصر اولیه نامیده می‌شود.

لم ۴۷ : اگر α یک عنصر اولیهٔ $GF(p^n)$ باشد، آنگاه α ریشهٔ یک چند جمله‌ای تحویل‌ناپذیر از درجهٔ n می‌باشد.

برهان: اگر چند جمله‌ای تحویل‌ناپذیر α بر Z_p از درجهٔ d باشد، آنگاه $Z_p(\alpha)$ از مرتبهٔ p^d می‌باشد . اما این زیرمیدان همهٔ $GF(p^n)$ می‌باشد، زیرا α یک عنصر اولیه است، بنابراین $d=n$ □

قضیه ۴۸: $Gal\ (GF(p^n)/GF(p)) \cong Z_n$ با مولد $u \longrightarrow u^p$.

تبصره: این مولد اتومورفیسم فروبینیوس نامیده شده است .

برهان: $GF(p^n)$ را با K و گروه گالوا را با G نشان می‌دهیم. اگر α یک عنصر اولیه

باشد، آنگاه چند جمله‌ای تحویل‌ناپذیر $p(x)$ از آن دارای درجهٔ n می‌باشد (لم ۴۷) ، و بنابر این K شامل حداکثر n ریشه از آن می‌باشد. اگر $\sigma\in G$، آنگاه σ به طور کامل با $\sigma(\alpha)$ مشخص می‌شود (زیرا هر عضو ناصفر از K به صورت α^i می‌باشد و $(\sigma(\alpha^i)=\sigma(\alpha)^i)$. اما بنابر لم ۳۵، $\sigma(\alpha)$ یک ریشهٔ $p(x)$ می‌باشد، از آن نتیجه می‌شود که $|G| \leq n$. از طرف دیگر $\sigma: u \longrightarrow u^p$ در G قرار دارد، بعلاوه ،اگر $j<n$، آنگاه $\sigma^j \neq 1$ (در غیر این صورت به ازای هر u، $u^{p^j}=u$، و K باید شامل p^n ریشه از $x^{p^j}-x$ باشد ، و این یک تناقض است). وقضیه نتیجه می‌شود. □

لم ۴۹ : فرض کنیم n یک عدد صحیح مثبت و F یک میدان باشد. اگر مشخصهٔ F صفر یا عدد اول p باشد که مقسوم علیه n نیست، آنگاه x^n-1 دارای n ریشهٔ متمایز در یک میدان شکافنده می‌باشد.

برهان : اگر $f(x)=x^n-1$، آنگاه مشتق آن $f'(x)=nx^{n-1}$ می‌باشد. بنابر فرض $f'(x)\neq 0$، و لذا $(f,f')=1$ بمعم، بنابر این $f(x)$ دارای ریشه‌های تکراری نیست. □

چیزی که باید در مورد مشخصهٔ p گفت آن است که $(x-1)^p=x^p-1$.

تعریف: فرض کنیم n یک عدد صحیح مثبت ثابت و F یک میدان باشد. یک مولد از گروه تمام ریشه‌های n ام یکانی را یک ریشهٔ اولیهٔ یکانی نامند، اگر مشخصه F صفر یا یک عدد اول باشد که مقسوم علیه n نیست.

$e^{2\pi i/n}$ یک ریشهٔ اولیهٔ یکانی در C است .

قضیه ۵۰: اگر F یک میدان باشد و $E=F(\alpha)$ که α یک ریشهٔ n ام اولیهٔ یکانی است، آنگاه $Gal(E/F)$ آبلی است .

برهان: توجه کنید که E میدان شکافندهٔ x^n-1 می‌باشد ، زیرا α یک ریشهٔ nام اولیهٔ یکانی است. اکنون به ازای هر $\sigma\in Gal(E/F)$، $\sigma(\alpha)=\alpha^i$، بعلاوه، قضیهٔ A2 قسمت

(ب) می‌گوید که i و n باید نسبت به هم اول باشند، از طرفی $|\sigma < \alpha >$ یک اتومورفیسم از $<\alpha>$ می‌باشد. نگاشت $\psi: Gal(E/F) \longrightarrow (\frac{Z}{nZ})^*$ را بوسیلهٔ $\bar{i} \longrightarrow \sigma$ که $\sigma(\alpha)=\alpha^i$ تعریف می‌کنیم. ($(\frac{Z}{nZ})^*$ گروه ضربی همهٔ کلاسهای همنهشت صحیح نسبت به هم اول به هنگ p می‌باشد). بررسی اینکه ψ یک هومورفیسم است ساده می‌باشد. بنابر تمرین ۷۳، ψ یک به یک است. بنابراین $Gal(E/F)$ با زیرگروهی از یک گروه آبلی ایزومورف می‌باشد، بنابراین $Gal(E/F)$ آبلی است. □

توجه کنید که $(\frac{Z}{nZ})^*$ لازم نیست که دوری باشد، به عنوان مثال، $(\frac{Z}{8Z})^*$ شامل کلاسهای همنهشت ۷,۵,۳,۱ است ، و با گروه چهار ایزومورف می‌باشد.

(یک معکوس جزیی ژرف قضیهٔ ۵۰ موجود می‌باشد. قضیهٔ کرونکر - وبر[1] بیان می‌کند که هر توسیع آبلی متناهی از Q (یعنی توسیع متناهی E/Q با گروه آبلی $(Gal(E/Q)$) می‌تواند در یک توسیع دایره‌ای $Q(\omega)$ که ω ریشهٔ یکانی است محاط شود).

مثال: اگر p عددی اول باشد، آنگاه $\zeta=e^{2\pi i/p}$ یک ریشهٔ p ام اولیهٔ یکانی بر Q است. همانند برهان قضیهٔ ۵۰ ، $Q(\zeta)$ میدان شکافندهٔ x^p-1 بر Q می‌باشد. اما $x^p-1=(x-1)\Phi_p(x)$ که $\Phi_p(x)$ چند جمله‌ای تقسیم دایرهٔ p ام می‌باشد، چون $\Phi_p(x)$ بر Q تحویل‌ناپذیر است (نتیجه ۲۵) ، داریم $|Gal(Q(\zeta)/Q)|=p-1$. اکنون قضیهٔ ۵۰ نتیجه می‌دهد که $Gal(Q(\zeta)/Q)\cong(Z_p)^*$ ، بنابر نتیجهٔ ۴۶ گروه اخیر دوری می‌باشد، و گروه ضربی از یک میدان است .

---

1. Kronecker - weber

فرض کنیم کاربرد مختلف قضیهٔ ۵۰ ارائه حل پیچیده‌ای برای تمرین ۷۹ باشد.

قضیه ۵۱: فرض کنیم F شامل یک ریشهٔ n ام اولیهٔ یکانی باشد، و فرض کنیم $f(x)=x^n-a$. اگر E/F یک میدان شکافندهٔ f(x) باشد، آنگاه یک تحدید، انژکسیون $G=Gal(E/F) \longrightarrow Z_n$ را نتیجه می‌دهد. بعلاوه، f(x) تحویل‌ناپذیر است اگر و فقط اگر این نگاشت پوشا باشد.

برهان: اگر ω یک ریشهٔ n ام اولیهٔ یکانی و α یک ریشهٔ f(x) باشد، آنگاه لیست تمام ریشه‌های f(x) برابر α , $\alpha\omega$, $\alpha\omega^2$, … , $\alpha\omega^{n-1}$ می‌باشد. اگر $\sigma\in G$، آنگاه $\sigma(\alpha)=\alpha\omega^i$ و σ به طور کامل بوسیلهٔ i مشخص می‌شود، از آن به سادگی نتیجه می‌شود که $\sigma \longrightarrow \bar{i}$ یک انژکسیون را معین می‌کند. اکنون این نگاشت پوشاست اگر و فقط اگر G به طور تعدی بر ریشه‌های f(x) اثر کند. بنابر تمرین ۸۴، این معادل تحویل‌ناپذیری f(x) می‌باشد. □

قضیه ۵۲: فرض کنیم p عددی اول و F میدان شامل یک ریشهٔ p ام اولیهٔ یکانی باشد. اگر $a\in F$، آنگاه x^p-a یا شکافته می‌شود یا تحویل‌ناپذیر است.

برهان: نگاشت $Gal\ (E/F) \longrightarrow Z_p$ را از قضیه در نظر می‌گیریم. اگر f(x) شکافته شود آنگاه تصویر آن بدیهی است. اگر f(x) شکافته نشود، آنگاه تصویر آن یک زیرگروه غیربدیهی از Z_p می‌باشد. اما Z_p دارای هیچ زیرگروه غیربدیهی واقعی نیست، بنابر این نگاشت باید پوشا باشد و f(x) تحویل‌ناپذیر است. □

حل‌ناپذیری درجهٔ پنجم

یادآوری قضیهٔ A21: اگر گروه G دارای زیرگروه نرمال حل‌پذیر H باشد به طوری که G/H حل‌پذیر باشد، آنگاه G حل‌پذیر است. این توصیف بهبود قضیهٔ ۴۰ می‌باشد که فرض در مورد ریشه‌های یکانی لازم نیست.

قضیه ۵۳: فرض کنیم $f(x)\in F[x]$ بوسیلهٔ رادیکالها بر میدان F حل‌پذیر باشد، و E/F میدان شکافندهٔ آن باشد. در این صورت $Gal(E/F)$ یک گروه حل‌پذیر است .

برهان: بنابر فرض یک توسیع رادیکال $F=B_0\subset B_1\subset...\subset B_t$ با $E\subset B_t$ موجود می‌باشد. فقط تعداد متناهی ریشه‌های یکانی، مثلاً، ریشه‌های k_1 ام ، k_2 ام ،...، k_s ام یکانی به F الحاق شده‌اند. اگر k حاصلضرب همهٔ k_iها باشد، آنگاه یک ریشهٔ k ام اولیهٔ یکانی، مثلاً، α وجود دارد. (اگر F دارای مشخصهٔ صفر باشد، مطمئناً این درست است. اگر F دارای مشخصهٔ p باشد، آنگاه می‌توانیم فرض کنیم که هیچ k_i ای بوسیلهٔ p عاد نمی‌شود زیرا تنها ریشهٔ p ام یکانی ۱ می‌باشد). با تعدیل برج اصلی بوسیلهٔ الحاق α ابتدا، $F=B_0\subset F_1(\alpha)\subset B_1(\alpha)\subset...\subset B_t(\alpha)=B'$.
توجه کنیم که هر توسیع در این برج محض است و $E\subset B_t(\alpha)$. چون $F(\alpha)/F$ یک میدان شکافنده است، تبصرهٔ بعد از قضیه ۳۹ نشان می‌دهد که $Gal(B'/F)/Gal(B'/F(\alpha))$ با یک زیر گروه از گروه آبلی $Gal(F(\alpha)/F)$ ایزومورف می‌باشد، لذا، بنابر قضیهٔ ۵۰ ، خود نیز آبلی است. بنابر قضیهٔ ۴۰، گروه $Gal(B'/F)$ دارای زیرگروه نرمال حل‌پذیر $Gal(B'/F(\alpha))$ می‌باشد که آبلی است، بنابراین ، گروه خارج قسمتی حل‌پذیراست، از قضیهٔ A21 نتیجه می‌شود که $Gal(B'/F)$ حل‌پذیر می‌باشد. بالاخره، بنابر تمرین ۸۲ می‌توان فرض کرد که B'/F یک میدان شکافنده است، همچنین با بکار بردن قضیهٔ ۳۹ نشان می‌دهد که $Gal(E/F)$ یک گروه خارج قسمتی از گروه حل‌پذیر $Gal(B'/F)$ می‌باشد و لذا بنابر قضیهٔ A20، حل‌پذیراست . □

قضیهٔ ۵۴: (آبل - رافینی). چند جمله‌ای درجه پنجم $f(x)\in Q[x]$ وجود دارد که

بوسیلهٔ رادیکالها حل‌پذیر نیست .

برهان: فرض کنیم $f(x)=x^5-4x+2$، بنابر ضابطهٔ آیزنشتاین $f(x)$ بر Q تحویل‌ناپذیراست. فرض کنیم E/Q میدان شکافندهٔ $f(x)$ مشمول در C[1] باشد، و فرض‌کنیم $G=Gal(E/Q)$. اگر α یک‌ریشهٔ $f(x)$ باشد، آنگاه $[Q(\alpha):Q]=5$، و همچنین $|G|=[E:Q(\alpha)][Q(\alpha):Q]$ بوسیلهٔ ۵ عاد می‌شود. اکنون بابکاربردن حساب مقدماتی $f(x)$ دارای دقیقاً دو نقطهٔ بحرانی $\pm\sqrt[4]{4/5}$ می‌باشد، و $f(\sqrt[4]{4/5})<0$ و $f(-\sqrt[4]{4/5})>0$، به سادگی از آن نتیجه می‌شود که $f(x)$ دارای دقیقاً سه ریشهٔ حقیقی می‌باشد. با در نظر گرفتن G به عنوان یک گروه از جایگشتها بر ۵ ریشه، توجه داریم که G شامل یک ۵ - دور (تنها عضو از مرتبهٔ ۵ در S_5) و σ است که σ دو ریشهٔ مختلط را با هم جابه جا می‌کند ، در حالی که سه ریشهٔ حقیقی را ثابت نگه می‌دارد. (بنابر این σ یک ترانهش است). بنابر قضیهٔ A37 ، گروه S_5 بوسیلهٔ هر ترانهش و هر ۵ - دور تولید می‌شود، همچنین $G\cong S_5$، لذا بنابر قضیهٔ A32 ، G یک گروه حل‌پذیر نیست. و قضیهٔ ۵۳ نشان می‌دهد که $f(x)$ بوسیلهٔ رادیکالها حل‌پذیر نیست. □

استقلال مشخصه‌ها

تعریف: یک مشخصهٔ گروه G در میدان E یک هومومورفیسم $\sigma : G \longrightarrow E^*$ می‌باشد ، که در آن $E^*=E-\{0\}$ گروه ضربی E است .

تعریف: مجموعهٔ $\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$ از مشخصه‌های گروه G در میدان E مستقل می‌باشد، در صورتی که یک بردار ناصفر $(a_i)\in E^n$ موجود نباشد به طوری که به ازای هر x از G، $\sum a_i\sigma_i(x)=0$.

---

۱ - **قضیهٔ اساسی جبر (قضیهٔ ۷۱) را فرض کرده‌ایم.**

لم ۵۵: (ددکیند[1]). هر مجموعهٔ $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ از مشخصه‌های متمایز گروه G در میدان E مستقل است.

برهان: اثبات به استقراء بر n می‌باشد. اگر $n=1$ آنگاه $a_1\sigma_1(x)=0$ نتیجه می‌دهد که $a_1=0$ زیرا $\sigma_1(x)\neq 0$. فرض کنیم $n>1$ و به ازای هر x از G معادلهٔ

$$a_1\sigma_1(x)+a_2\sigma_2(x)+\dots+a_n\sigma_n(x)=0 \quad (۱)$$

برقرار باشد، که همهٔ a_iها صفر نیستند. با بکار بردن استقراء و ضرب a_n^{-1} در صورت لزوم، می‌توان فرض کرد که همهٔ a_iها ناصفرند. فرض کنیم که $a_n=1$. چون $\sigma_n\neq\sigma_1$، y ای از G وجود دارد که $\sigma_n(y)\neq\sigma_1(y)$. با جایگذاری yx به جای x در معادلهٔ (۱) به‌دست می‌آید.

$$a_1\sigma_1(y)\sigma_1(x)+\cdots+a_{n-1}\sigma_{n-1}(y)\sigma_{n-1}(x)+\sigma_n(y)\sigma_n(x)=0\,.$$

با ضرب $\sigma_n(y)^{-1}$ معادلهٔ $a_1\sigma_n(y)^{-1}\sigma_1(y)\sigma_1(x)+\cdots+\sigma_n(x)=0$ به دست می‌آید، با تفریق این معادله از معادلهٔ (۱)، یک مجموع با $n-1$ جملهٔ $a_1[1-\sigma_n(y)^{-1}\sigma_1(y)]\sigma_1(x)+\cdots=0$ به دست می‌آید. بنابراستقراء هر یک از ضرایب 0 می‌باشد. چون $a_1\neq 0$، داریم $1=\sigma_n(y)^{-1}\sigma_1(y)$، بنابراین $\sigma_n(y)=\sigma_1(y)$، و این یک تناقض است. □

نتیجه ۵۶: هر مجموعهٔ $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ از اتومورفیسمهای متمایز میدان E مستقل خطی می‌باشد.

برهان: تحدید اتومورفیسم σ از E به گروه ضربی E^*، هomomorphism $\sigma: E^* \longrightarrow E^*$ می‌باشد، بنابراین یک مشخصه است. □

---

1. Dedekind

تعریف: فرض کنیم $\mathrm{Aut}\ (E)$ گروه همهٔ اتومورفیسمهای میدان E باشد. اگر G یک زیرمجموعه از $\mathrm{Aut}\ (E)$ باشد، آنگاه $E^G=\{\alpha\in E;\sigma(\alpha)=\alpha,\forall\sigma\in G\}$ میدان ثابت نامیده می‌شود.

دیدن اینکه E^G یک زیرمیدان E است ساده می‌باشد. مهمترین مورد این تعریف هنگامی است که G یک زیرگروه از $\mathrm{Aut}(E)$ باشد، اما هنگامی که G تنها یک زیرمجموعه می‌باشد، یک کاربرد وجود دارد. توجه کنید که $H\subset G$ نتیجه می‌دهد که $E^G\subset E^H$.

مثالها

۱. اگر E/F یک توسیع میدان با گروه گالوای $G=\mathrm{Gal}(E/F)$ باشد، آنگاه $F\subset E^G\subset E$، به زودی ملاحظه خواهیم کرد که E^G/F یک توسیع واقعی می‌باشد.

۲. فرض کنیم $E=F(x_1,x_2,\cdots,x_n)$ توابع گویای چند متغیره بر میدان F باشد. در این صورت $G\cong S_n$ می‌تواند به عنوان یک زیرگروه از $\mathrm{Aut}(E)$ در نظر گرفته شود، آن بوسیلهٔ جابه جاکردن متغیرها عمل می‌کند. اعضای میدان ثابت E^G توابع متقارن[1] بر F نامیده شده‌اند.

لم ۵۷: اگر $G=\{\sigma_1,\sigma_2,\ldots,\sigma_n\}$ یک مجموعه از اتومورفیسمهای E باشد، آنگاه $[E:E^G]\geq n$.

برهان: در غیراین صورت $[E:E^G]=r<n$. فرض کنیم $\{\alpha_1,\alpha_2,\cdots,\alpha_r\}$ یک پایه از

---

۱. **توابع متقارن به طور طبیعی ناشی می‌شوند: اگر** $f(x)=\prod(x-\alpha_i)=x^n+s_{n-1}x^{n-1}+\ldots+s_1x+s_0$، **آنگاه هر ضریب s_j یک تابع متقارن از ریشه‌های $\alpha_1,\alpha_2,\ldots,\alpha_n$ است. این مشاهده نقطهٔ شروع لاگرانژ و گالوا می‌باشد. (پیوست ۴ را ببینید).**

E/E^G باشد. دستگاه خطی بر E از r معادله و n مجهول را در نظر می‌گیریم :

$$\sigma_1(\alpha_1)x_1+\cdots+\sigma_n(\alpha_1)x_n=0$$
$$\sigma_1(\alpha_2)x_1+\cdots+\sigma_n(\alpha_2)x_n=0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\sigma_1(\alpha_r)x_1+\cdots+\sigma_n(\alpha_r)x_n=0$$

چون $r<n$، یک جواب غیربدیهی $(x_1,x_2\ ,\ \dots\ ,\ x_n)$ وجود دارد. به ازای هر $\beta\in E$ داریم $\beta=\sum b_i\alpha_i$ که $b_i\in E^G$. با ضرب سطر i ام دستگاه در $\sigma_1(b_i)$ یک دستگاه با سطر i ام، $\sigma_1(b_i)\sigma_1(\alpha_i)x_1+\ \cdots\ +\sigma_1(b_i)\sigma_n(\alpha_i)x_n=0$ به‌دست‌می‌آید. امابه‌ازای هر $i\ ,\ j$، $\sigma_1(b_i)=b_i=\sigma_j(b_i)$ زیرا $b_i\in E^G$. بنابراین دستگاه دارای سطر i ام $\sigma_1(b_i\alpha_i)x_1+\ \cdots\ +\sigma_n(b_i\alpha_i)x_n=0$ می‌باشد. اکنون با جمع کردن به‌دست می‌آوریم $\sigma_1(\beta)x_1+\ \cdots\ +\sigma_n(\beta)x_n=0$. چون β عضو دلخواهی از E است، برخلاف استقلال مشخصه‌های $\{\sigma_1,\sigma_2\ ,\ \cdots\ ,\ \sigma_n\}$ می‌باشد. این تناقض قضیه را ثابت می‌کند. □

قضیه ۵۸: اگر $G=\{\sigma_1,\sigma_2\ \cdots\ ,\sigma_n\}$ یک زیر گروه از $Aut(E)$ باشد، آنگاه $[E:E^G]=|G|$.

برهان: کافی است ثابت کنیم که $[E:E^G]\leq|G|$. در غیراین صورت اگر $[E:E^G]>n$. فرض کنیم $\{\omega_1,\omega_2,\cdots,\omega_{n+1}\}$ بردارهای مستقل خطی در E بر E^G باشد. دستگاه n معادله و $n+1$ مجهول زیر را در نظر می‌گیریم :

$$\sigma_1(\omega_1)x_1+\cdots+\sigma_1(\omega_{n+1})x_{n+1}=0$$
$$\sigma_2(\omega_1)x_1+\cdots+\sigma_2(\omega_{n+1})x_{n+1}=0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\sigma_n(\omega_1)x_1+\cdots+\sigma_n(\omega_{n+1})x_{n+1}=0$$

یک جواب غیربدیهی $(x_1\ ,\ \cdots\ ,\ x_{n+1})$ برای‌دستگاه بر E وجود دارد، بایک عمل آن را متعارف می‌کنیم . یک جواب با کوچکترین عدد r از مولفه‌های ناصفر، مثلاً ،

$(a_1,a_2,\cdots,a_r,0,\cdots,0)$ را انتخاب می‌کنیم، با تغییراندیس ω_i، می‌توان فرض کرد که همهٔ مؤلفه‌های ناصفر ابتدا آمده‌اند. توجه کنیم که $r\neq 1$، اگر $\sigma_1(\omega_1)a_1=0$ نتیجه می‌شود که $a_1=0$. می‌توانیم فرض کنیم که $a_r=1$، اگر لازم باشد آن را در معکوسش ضرب می‌کنیم. توجه کنیم که همهٔ a_iها عضو E^G می‌باشند، در غیر این صورت سطر متناظر با عضو همانی G برخلاف استقلال خطی $\{\omega_1,\omega_2,\cdots,\omega_{n+1}\}$ است. درفرض قبلی اگر $a_1\notin E^G$ (این نیز می‌تواند با تغییر اندیس ω_i کامل شود). بنابراین σ_k ای با $\sigma_k(a_1)\neq a_1$ وجود دارد. دستگاه اصلی دارای سطر j ام،

(۱) $\sigma_j(\omega_1)a_1+\cdots+\sigma_j(\omega_{r-1})a_{r-1}+\sigma_j(\omega_r)=0$ می‌باشد. با تأثیر σ_k بر معادلهٔ (۱)، معادلهٔ $\sigma_k\sigma_j(\omega_1)\sigma_k(a_1)+\cdots+\sigma_k\sigma_j(\omega_{r-1})\sigma_k(a_{r-1})+\sigma_k\sigma_j(\omega_r)=0$ به‌دست می‌آید. چون G یک گروه است، $\sigma_k\sigma_1,\cdots,\sigma_k\sigma_n$ دقیقاً یک جایگشت از $\sigma_1,\sigma_2,\cdots,\sigma_n$ می‌باشد. قرارمی‌دهیم $\sigma_k\sigma_j=\sigma_i$، دستگاه دارای سطر i ام،

$\sigma_i(\omega_1)\sigma_k(a_1)+\cdots+\sigma_i(\omega_{r-1})\sigma_k(a_{r-1})+\sigma_i(\omega_r)=0$ می‌باشد. با تفریق این معادله از سطر i ام معادلهٔ (۱) یک دستگاه جدید با سطر i ام،

$\sigma_i(\omega_1)[a_1-\sigma_k(a_1)]+\cdots+\sigma_i(\omega_{r-1})[a_{r-1}-\sigma_k(a_{r-1})]=0$ به‌دست می‌آید. چون $a_1-\sigma_k(a_1)\neq 0$، یک جواب غیربدیهی از دستگاه اصلی دارای مؤلفه‌های ناصفر کمتر از r به‌دست آورده‌ایم که یک تناقض است. □

نتیجه ۵۹: اگر H, G زیرگروههایی از $Aut(E)$ باشند که $E^G=E^H$، آنگاه $G=H$.

برهان: اگر $\sigma\in G$، آنگاه‌بوضوح σ، E^G را ثابت نگه می‌دارد. برای اثبات عکس، فرض کنیم σ، E^G را ثابت نگه دارد و $\sigma\notin G$. در این صورت E^G بوسیلهٔ $n+1$ عضو در $G\cup\{\sigma\}$ ثابت نگه‌داشته می‌شود، بنابر لم ۵۷ و قضیهٔ ۵۸ تناقض $n=|G|=[E:E^G]\geq[E:E^{G\cup\{\sigma\}}]\geq n+1$ نتیجه می‌شود. بنابراین، اگر σ، E^G را

ثابت نگه دارد، آنگاه $\sigma\in G$. اگر $\sigma\in G$ آنگاه σ، $E^G=E^H$ را ثابت نگه می‌دارد، و لذا $\sigma\in H$. عکس جزئیت به طریق مشابه اثبات می‌شود. □

توسیع‌های گالوا

مبحث گروههای گالوا با یک جفت از میدانها شروع شد، مثلاً، توسیع E/F که میدان شکافندهٔ چند جمله‌ای $f(x)\in F[x]$ می‌باشد. فرض کنیم که $G = Gal(E/F)$، دیدن اینکه $F\subset E^G\subset E$ ساده است. یک سؤال طبیعی است که چه وقت $F=E^G$، در حالت کلی جواب منفی است. به عنوان مثال اگر $F = Q$ و $E=Q(\alpha)$ که α یک ریشهٔ سوم حقیقی ۲ می‌باشد، آنگاه $G=Gal(E/F)=Gal(Q(\alpha)/Q)=\{1\}$. (اگر $\sigma\in G$، آنگاه $\sigma(\alpha)$ یک ریشهٔ x^3-2 می‌باشد، اما E شامل دو ریشهٔ مختلط دیگر این چند جمله‌ای نمی‌باشد.) بنابراین $E^G=E\neq F$.

قضیه ۶۰ : شرایط زیر برای توسیع متناهی E/F با گروه گالوای $G=Gal(E/F)$ معادلند.

(آ) $F=E^G$.

(ب) هر تحویل‌ناپذیر $p(x)\in F[x]$ با یک ریشه در E جداپذیر است و همهٔ ریشه‌های آن عضو E می‌باشند، یعنی، $p(x)$ بر E شکافته می‌شود.

(ج) E میدان شکافندهٔ چند جمله‌ای جداپذیر $f(x)\in F[x]$ می‌باشد.

برهان: (آ) ⇐ (ب) فرض کنیم $p(x)\in F[x]$ یک چند جمله‌ای تحویل‌ناپذیر دارای ریشهٔ α در E باشد، و فرض کنیم α_1 , α_2 , … , α_n اعضای متمایز مجموعهٔ $\{\sigma(\alpha) ; \sigma \in G\}$ باشند. $g(x)\in E[x]$ را بوسیلهٔ $g(x)=\Pi(x-\alpha_i)$ تعریف می‌کنیم. اکنون هر σ از G، α_i را جابه جا می‌کند، همچنین هر σ ضرایب $g(x)$ را ثابت نگه می‌دارد، یعنی ضرایب $g(x)$ در $E^G=F$ قراردارند. بنابراین $g(x)$ یک چند جمله‌ای در

$F[x]$ دارای ریشه‌های تکراری نمی‌باشد. اکنون $p(x)$ و $g(x)$ دارای یک ریشهٔ مشترک در E می‌باشند، و همچنین بزرگترین مقسوم‌علیه مشترک آنها در $E[x]$ برابر ۱ نیست، از نتیجهٔ ۸ نتیجه می‌شود که بزرگترین مقسوم علیه مشترک آنها در $F[x]$ برابر ۱ نیست. چون $p(x)$ تحویل‌ناپذیراست، باید $g(x)$ را عاد کند. بنابراین $p(x)$ دارای ریشه‌های تکراری نیست، لذا جداپذیر می‌باشد و بر E شکافته می‌شود.

(ب) ⇐ (ج) انتخاب می‌کنیم $\alpha_1 \in E$ که $\alpha_1 \notin F$. چون E/F یک توسیع متناهی است، α_1 باید بر F جبری باشد، فرض کنیم $p_1(x) \in F[x]$ چندجمله‌ای تحویل‌ناپذیر α_1 باشد. بنابر فرض $p_1(x)$ یک چند جمله‌ای جداپذیراست که بر E شکافته می‌شود، فرض کنیم $K_1 \subset E$ میدان شکافندهٔ آن باشد. اگر $K_1 = E$ حکم برقرار است. در غیراین صورت، انتخاب می‌کنیم $\alpha_2 \in E$ که $\alpha_2 \notin K_1$. بنابر فرض یک چند جمله‌ای تحویل‌ناپذیر جداپذیر $p_2(x) \in F[x]$ دارای α_2 به عنوان یک ریشه وجود دارد. فرض کنیم $K_2 \subset E$ میدان شکافندهٔ چند جمله‌ای جداپذیر $p_1(x)p_2(x)$ باشد. اگر $K_2 = E$ حکم برقرار است. در غیراین صورت این روند را تکرار می‌کنیم. این فرآیند باید با $K_m = E$ به ازای m ای خاتمه یابد زیرا E/F متناهی است.

(آ) ⇐ (ج) بنابرقضیهٔ ۳۷، $|G| = [E:F]$. اما قضیه ۵۸ نتیجه می‌دهد که $[E:E^G] = |G|$ لذا $[E:F] = [E:E^G]$. چون $F \subset E^G$، از آن نتیجه می‌شود که $F = E^G$. □

تعریف: توسیع میدان متناهی E/F گالوا (نرمال) می‌باشد اگر در هریک از شرایط معادل قضیهٔ ۶۰ صدق کند.

تبصره: اصطلاح توسیع گالوا هنوز استاندارد نمی‌باشد، برخی از مؤلفین یک توسیع گالوا را نرمال می‌نامند، برخی یک توسیع را نرمال نامند در صورتی که میدان شکافندهٔ

یک چند جمله‌ای نه لزوماً جداپذیر باشد.

تمرین

*۸۵. اگر E/F یک توسیع گالوا و B یک میدان میانی باشد، آنگاه E/B یک توسیع گالوا می‌باشد.

۸۶. اگر F دارای مشخصهٔ مخالف ۲ و E/F یک توسیع میدان با $[E:F]=2$ باشد، آنگاه E/F یک توسیع گالوا می‌باشد.

۸۷. نشان دهید که توسیع گالوا بودن لازم نیست متعدی باشد، یعنی اگر $F\subset B\subset E$ و E/B و B/F توسیع‌های گالوا باشند، آنگاه E/F لازم نیست توسیع گالوا باشد. (راهنمایی: $Q\subset Q(\alpha)\subset Q(\beta)$ را در نظر بگیرید، که α ریشهٔ دوم ۲ و β ریشهٔ چهارم ۲ می‌باشد.)

*۸۸. فرض کنیم $E=F(x_1,x_2,\dots,x_n)$ و S زیرمیدانی از همهٔ توابع متقارن باشد. ثابت کنید که $[E:S]=n!$ و $Gal(E/S)\cong S_n$. (راهنمایی: نشان دهید که E/S میدان شکافندهٔ چندجمله‌ای جداپذیر $f(t)=\Pi(t-\alpha_i)$ می‌باشد.)

۸۹. فرض کنیم E/F یک توسیع گالوا و $p(x)\in F[x]$ تحویل‌ناپذیر باشد. نشان دهید که همهٔ عوامل تحویل‌ناپذیر $p(x)$ در $E[x]$ دارای درجه یکسان می‌باشند. (راهنمایی: از تمرین ۸۱ استفاده کنید.)

*۹۰. با ارائه یک میدان F و یک گروه متناهی G از مرتبهٔ n، نشان دهید که یک زیرمیدان $K\subset E=F(x_1,\cdots,x_n)$ وجود دارد که $Gal(E/K)\cong G$. (راهنمایی: تمرین ۸۸ و قضیهٔ کیلی (قضیه A24) را بکار ببرید.)

یک تفسیر از توسیع گالوا برای میدانهای میانی وجود دارد.

تعریف: فرض کنیم E/F یک توسیع گالوا و B و C میدانهای میانی باشند. اگر یک

ایزومورفیسم $B \longrightarrow C$ که F را ثابت نگه می‌دارد موجود باشد، آنگاه C یک مزدوج B نامیده می‌شود.

لم ۶۱ : فرض کنیم E/F یک توسیع گالوا و B یک میدان میانی باشد. شرایط زیر معادل می‌باشند.

(آ) B دارای هیچ مزدوجی بجز خود B نیست.

(ب) اگر $\sigma \in Gal(E/F)$ آنگاه $\sigma|_B \in Gal(B/F)$.

(ج) B/F یک توسیع گالوا می‌باشد.

برهان: (آ) ⇐ (ب) بدیهی است .

(ب) ⇐ (ج) فرض کنیم $p(x) \in F[x]$ یک چند جمله‌ای تحویل‌ناپذیر دارای یک ریشه β در B باشد. چون $B \subset E$ و E/F گالوا می‌باشد، همهٔ ریشه‌های p(x) در E قراردارند. فرض کنیم یک ریشهٔ $\beta' \in E$ موجود باشد که $\beta' \notin B$. بنابر قضیهٔ ۳۲، یک ایزومورفیسم $\tau: F(\beta) \longrightarrow F(\beta')$ که F را ثابت نگه می‌دارد وجود دارد که به $\sigma \in Gal(E/F)$ گسترش می‌یابد، زیرا E/F یک توسیع گالوا می‌باشد. اما $\sigma(B) \cong B$ و $\sigma(B) \neq B$، زیرا $\beta' \in \sigma(B)$ و $\beta' \notin B$.

(آ) ⇐ (ج) B/F میدان شکافندهٔ چند جمله‌ای مانند f(x) بر F می‌باشد. همچنین $B = F(\alpha_1, \ldots, \alpha_n)$ که $\alpha_1, \ldots, \alpha_n$ همهٔ ریشه‌های f(x) می‌باشند. چون هر $\sigma \in Gal(E/F)$ باید یک ریشه از f(x) را به یک ریشه از f(x) انتقال دهد، از آن نتیجه می‌شود که σ باید B را به خودش ببرد. □

قضیهٔ اساسی نظریهٔ گالوا

تعریف: یک شبکه یک مجموعهٔ به طور جزیی مرتب $(L, \leq)$ می‌باشد که در آن هر جفت از اعضای a , b از L دارای کوچکترین کران بالای $a \vee b$ و بزرگترین کران پایین

$a \wedge b$ می‌باشد.

به خاطر داریم که L یک مجموعهٔ به طور جزیی مرتب است اگر $\leq$ یک رابطهٔ دوتایی منعکس، متعدی و پاد متقارن باشد. عضو c یک کران بالای b,a می‌باشد ، اگر $a \leq c$ و $b \leq c$. و عضو d کوچکترین کران بالای a و b است ، اگر یک کران بالا باشد و به ازای هر کران بالای c، $d \leq c$. بزرگترین کران پایین به طور مشابه تعریف می‌شود، نامساویها عکس می‌شوند.

مثالها

۱ . اگر X یک مجموعه باشد، فرض کنیم L خانوادهٔ همهٔ زیر مجموعه‌های X باشد، و $A \leq B$ به معنی $A \subset B$ تعریف می‌کنیم. آنگاه L یک شبکه می‌باشد، و $A \wedge B = A \cap B$ و $A \vee B = A \cup B$.

۲. اگر G یک گروه باشد، فرض کنیم $Sub(G)$ خانوادهٔ همهٔ زیرگروههای G باشد، و $H \leq K$ به معنی $H \subset K$ تعریف می‌کنیم. آنگاه $Sub(G)$ یک شبکه است که $H \vee K$ زیرگروه تولید شده بوسیلهٔ H و K می‌باشد و $H \wedge K = H \cap K$.

۳. فرض کنیم E/F یک توسیع میدان و $Lat\ (E/F)$ خانوادهٔ همهٔ میدانهای میانی باشد، و $B \leq C$ به معنی $B \subset C$ تعریف می‌کنیم. آنگاه $Lat(E/F)$ یک شبکه است که $B \vee C$ ترکیب آنها می‌باشد و $B \wedge C = B \cap C$.

۴. فرض کنیم L مجموعهٔ همهٔ اعداد صحیح $n \leq 1$ باشد، و تعریف می‌کنیم $n \leq m$ به معنی $n \mid m$. در این صورت L یک شبکه می‌باشد که $n \vee m$ و $n \wedge m$ به ترتیب کوچکترین مضرب مشترک و بزرگترین مقسوم علیه مشترک n و m می‌باشند.

لم ۶۲: اگر L و L' دوشبکه‌باشند و $\gamma: L \longrightarrow L'$ یک دو سویی معکوس کنندهٔ ترتیب باشد ($a \leq b$ نتیجه می‌دهد که $\gamma(b) \leq \gamma(a)$) ، آنگاه

$\gamma(a\vee b)=\gamma(a)\wedge\gamma(b)$ و $\gamma(a\wedge b)=\gamma(a)\vee\gamma(b)$.

برهان: اکنون $a,b\leq a\vee b$ نتیجه می‌دهد که $\gamma(a),\gamma(b)\geq\gamma(a\vee b)$ یعنی $\gamma(a\vee b)$ یک‌کران پایین $\gamma(a)$و $\gamma(b)$می‌باشد. از آن نتیجه می‌شود که $\gamma(a)\wedge\gamma(b)\geq\gamma(a\vee b)$، چون γ پوشاست، c ای از L وجود دارد که $\gamma(c)=\gamma(a)\wedge\gamma(b)$ با بکار بردن γ^{-1}(به سادگی دیده می‌شود که γ^{-1}معکوس کنندهٔ ترتیب می‌باشد)$a,b\leq c\leq a\vee b$ به دست می‌آید. بنابراین $c=a\vee b$ و $\gamma(a\vee b)=\gamma(c)=\gamma(a)\wedge\gamma(b)$. آرگومان مشابه قسمت دوم گزاره را اثبات می‌کند. □

قضیه ۶۳: (قضیهٔ اساسی نظریهٔ گالوا). فرض کنیم E/F یک توسیع گالوا با گروه گالوای $G=\mathrm{Gal}(E/F)$ باشد.

(آ) تابع $\gamma:\mathrm{Sub}(G)\longrightarrow \mathrm{Lat}\,(E/F)$ تعریف‌شده‌بوسیلهٔ $H \longrightarrow E^H$ یک دوسویی معکوس کنندهٔ ترتیب با معکوس $\delta:B \longrightarrow \mathrm{Gal}(E/B)$ می‌باشد.

(ب) $E^{\mathrm{Gal}(E/B)}=B$ و $\mathrm{Gal}\,(E/E^H)=H$

(ج) $E^{H\vee K}=E^H\cap E^K$ و $E^{H\cap K}=E^H\vee E^K$

و $\mathrm{Gal}(E/B\vee C)=\mathrm{Gal}(E/B)\cap \mathrm{Gal}\,(E/C)$

و $\mathrm{Gal}\,(E/B\cap C) = \mathrm{Gal}\,(E/B)\vee \mathrm{Gal}\,(E/C)$

(د) $[G:H]=[E^H:F]$ و $[B:F]=[G:\mathrm{Gal}\,(E/B)]$

(ه) B/F یک توسیع گالواست اگر و فقط اگر $\mathrm{Gal}(E/B)$ یک زیرگروه نرمال G باشد.

برهان: (آ) دیدن اینکه γ معکوس کنندهٔ ترتیب می‌باشد ساده است: $K\leq H$ نتیجه می‌دهد که $E^H\leq E^K$. اینکه γ یک به یک است دقیقاً گزارهٔ نتیجهٔ ۵۹ می‌باشد. برای

دیدن اینکه γ پوشاست، ترکیب $\mathrm{Lat}(E/F) \xrightarrow{\delta} \mathrm{Sub}(G) \xrightarrow{\gamma} \mathrm{Lat}(E/F)$
را در نظر می‌گیریم، که δ نگاشت $\delta(B) = \mathrm{Gal}\,(E/B)$ می‌باشد. لذا
$\gamma\delta\,(B) = \gamma\,(\mathrm{Gal}\,(E/B)) = E^{\mathrm{Gal}(E/B)}$. بنابر تمرین ۸۵، گالوا بودن E/F نتیجه می‌دهد که به ازای هر میدان میانی B، توسیع E/B گالوا می‌باشد، بنابراین قضیهٔ ۶۰ نتیجه می‌دهد که $B = E^{\mathrm{Gal}(E/B)}$، لذا $\gamma\delta$ همانی است و γ پوشا می‌باشد. در نتیجه γ یک دوسویی با معکوس δ است.

(ب) دقیقاً این گزاره است که $\delta\gamma$ و $\gamma\delta$ توابع همانی می‌باشند.

(ج) دو معادلهٔ اول از لم ۶۲ نتیجه می‌شوند زیرا γ یک دوسویی معکوس کنندهٔ ترتیب است، چون $\delta=\gamma^{-1}$ نیز یک دوسویی معکوس کنندهٔ ترتیب است دو معادلهٔ دوم نتیجه می‌شوند.

(د) $[B:F]=[E:F]/[E:B]=|G|/|\mathrm{Gal}(E/B)|=[G:\mathrm{Gal}(E/B)]$

بنابر این درجهٔ B/F برابر اندیس $\mathrm{Gal}(E/B)$ در G می‌باشد. معادلهٔ دوم از جایگذاری $B=E^H$ نتیجه می‌شود، زیرا $\mathrm{Gal}(E/E^H)=H$.

(ه) اگر B/F گالوا باشد، آنگاه در قضیهٔ ۳۹ دیدیم که $\mathrm{Gal}(E/B)$ یک زیرگروه نرمال G می‌باشد . بالعکس، فرض کنیم که H یک زیرگروه نرمال G باشد، آیا E^H/F یک توسیع گالوا می‌باشد؟ اگر $\sigma\in G$ آنگاه بنابرنرمال بودن H در G به ازای τ' ای از H ، $\tau\sigma(\alpha)=\sigma\tau'(\alpha)$، و $\sigma\tau'(\alpha)=\sigma(\alpha)$ زیرا τ' ، α را ثابت نگه می‌دارد . بنابراین $\alpha\in E^H$ نتیجه می‌دهد که $\sigma(\alpha)\in E^H$ ، یعنی $\sigma(E^H)\subset E^H$، در واقع $\sigma(E^H)=E^H$ زیرا هر دو دارای بعد یکسان بر F می‌باشند. بنابرلم ۶۱، E^H/F یک توسیع گالوا می‌باشد. □

کاربردها

نتیجه ۶۴: توسیع گالوای E/F تنها دارای تعدادی متناهی میدانهای میانی است .

برهان: اگر گالوای آن متناهی است، بنابر این تنها دارای تعدادی متناهی زیرگروه است. □

قضیه ۶۵: (اشتاینیتز[1]) توسیع متناهی E/F ساده است اگر و فقط اگر تنها دارای تعدادی متناهی میدانهای میانی باشد.

برهان: فرض کنیم که $E=F(\alpha)$ و $p(x)$ چند جمله‌ای تحویل‌ناپذیر α بر F باشد. به ازای میدان میانی B، فرض کنیم $g(x)$ چند جمله‌ای تحویل‌ناپذیر α بر B باشد. اگر B'زیرمیدان B تولید شده بوسیلهٔ F و ضرایب $g(x)$ باشد، آنگاه $g(x)$ نیز بر B' تحویل‌ناپذیر است. چون $E=B(\alpha)=B'(\alpha)$ ، در نتیجه $[E:B]=[B(\alpha):B]$ و $[E:B']=[B'(\alpha):B']$ ، بنابراین $[E:B]=[E:B']$ ، زیرا هر دو برابر درجهٔ $g(x)$ می‌باشند. بنابراین $B=B'$ و B کاملاً بوسیلهٔ $g(x)$ مشخص شده است. اما $g(x)$ یک مقسوم علیه $p(x)$ است ، چون فقط تعدادی متناهی مقسوم علیه‌های تکین از $p(x)$ بر E وجود دارند، تنها تعدادی متناهی میدانهای میانی B وجود دارند.

فرض کنیم که E/F تنها دارای تعدادی متناهی میدانهای میانی باشد. اگر F متناهی باشد ، آنگاه نتیجه ۴۶ نشان می‌دهد که E/F ساده است ، دقیقاً برابر الحاق یک عضو اولیه به F است. بنابر این می‌توانیم فرض کنیم که F نامتناهی است. اکنون به استقراء بر n ، $E=F(\alpha_1,...,\alpha_n)$ ، کافی است ثابت کنیم که $E=F(\alpha,\beta)$ یک توسیع ساده است. همهٔ اعضای γ به‌فرم $\gamma=\alpha+a\beta$ که $a\in F$ را درنظرمی‌گیریم ، چون F نامتناهی‌است تعداد چنین γ هایی نامتناهی است. چون فقط تعدادی متناهی میدانهای میانی وجود دارند، فقط تعدادی متناهی میدانهای به فرم $F(\gamma)$ وجود دارند. بنابر این اعضای متمایز

---

1. Steinitz

با $a,a'\in F$ وجود دارند که $F(\gamma)=F(\gamma')$. بوضوح $\gamma'=\alpha+a'\beta$. $F(\gamma)\subset F(\alpha\ ,\beta)$ برای عکس شمول، $F(\gamma)=F(\gamma')$ شامل $\gamma-\gamma'=(a-a')\beta$ است. چون $a\neq a'$ داریم $\beta\in F(\gamma)$. اما $\alpha=\gamma-\alpha\beta\in F(\gamma)$، لذا $F(\alpha\ ,\beta)\subset F(\gamma)$ ، و همان نتیجهٔ مطلوب است. □

نتیجه ۶۶: اگر E/F یک توسیع سادهٔ متناهی باشد و B یک میدان میانی باشد، آنگاه توسیع B/F ساده است .

نتیجه ۶۷: (قضیهٔ عنصر اولیه). هر توسیع گالوای E/F ساده است .

برهان: بی درنگ از نتیجهٔ ۶۴ و قضیهٔ ۶۵ نتیجه می‌شود . □

با استفاده از برهان قضیه ۶۵، نشان دادن اینکه می‌توان یک عضو اولیه از $F(\alpha_1,\cdots,\alpha_n)$ به فرم $a_1\alpha_1+\cdots+a_n\alpha_n$ که $a_i\in F$ انتخاب کرد ساده می‌باشد.

نتیجهٔ ۶۸: میدان گالوای $GF(p^n)$ به ازای هر مقسوم علیه d از n دارای دقیقاً یک زیر میدان از مرتبهٔ p^d می‌باشد.

برهان: در قضیهٔ ۴۸ دیدیم که $Gal(GF(p^n)\ /GF(p))\cong Z_n$، بعلاوه لم ۴۱ نشان می‌دهد که گروه دوری از مرتبهٔ n به ازای هر مقسوم علیه d از n دارای دقیقاً یک زیرگروه از مرتبهٔ d می‌باشد. اکنون یک زیرگروه از مرتبهٔ d دارای اندیس $\frac{n}{d}$ است، و همچنین قضیهٔ اساسی می‌گوید که میدان میانی متناظر دارای درجهٔ $\frac{n}{d}$ است. اما اعداد $\frac{n}{d}$ همانند تغییر d بر همهٔ مقسوم‌علیه‌های n ، تغییر می‌کنند . □

حتی درست‌تر است که ، شبکهٔ تمام میدانهای میانی همانند شبکهٔ تمام زیرگروههای Z_n می‌باشد، و این به نوبت خود همانند شبکهٔ تمام مقسوم علیه‌های n تحت کمم و بمعم است. (یک زیر شبکه از شبکهٔ مثال ۴).

نتیجه ۶۹: اگر E/F یک توسیع گالوا باشد که $Gal(E/F)$ آبلی است، آنگاه هر میدان

میانی B/F یک توسیع گالوا می‌باشد.

برهان: هر زیرگروه از یک گروه آبلی یک زیرگروه نرمال است . □

نتیجه ۷۰: فرض کنیم $f(x)\in F[x]$ یک چند جمله‌ای جداپذیر و E/F یک میدان شکافنده باشد. فرض کنیم $f(x) = g(x)h(x)$ که $g(x)\,,\, h(x)\in F[x]$ و B/F و C/F بترتیب میدانهای شکافندهٔ $g(x)$ و $h(x)$ مشمول در E باشند . اگر $B\cap C=F$ (چنین میدانهایی بر F متمایز خطی نامیده می‌شوند)، در این صورت

$$\mathrm{Gal}\,(E/F) \cong \mathrm{Gal}\,(B/F) \times \mathrm{Gal}(C/F)\,.$$

برهان: به یاد داریم که اگر H و K زیرگروههایی از گروه G باشند، آنگاه G به صورت حاصلضرب مستقیم آنها است و بوسیلهٔ $G = H\times K$ نشان داده می‌شود ، اگر H و K هر دو در G نرمال باشند و $H\cap K = \{1\}$ و $H\vee K = HK = G$. فرض کنیم $G=\mathrm{Gal}(E/F)$. چون B/F و C/F توسیع‌های گالوا هستند $\mathrm{Gal}(E/B)$ و $\mathrm{Gal}(E/C)$ زیرگروههای نرمال G می‌باشند. بنابر فرض نتیجه می‌شود که $B\vee C=E$، بنابراین $\mathrm{Gal}\,(E/B)\cap\mathrm{Gal}(E/C)=\mathrm{Gal}(E/B\vee C) = \mathrm{Gal}\,(E/E) = \{1\}$. همچنین $\mathrm{Gal}\,(E/B)\,\mathrm{Gal}\,(E/C) = \mathrm{Gal}(E/B\cap C) = \mathrm{Gal}\,(E/F) = G$. بنابراین G یک حاصلضرب مستقیم است. بالاخره ، چون $\frac{H\times K}{H} \cong K$ ، از قضیهٔ ۳۹ نتیجه می‌شود که $\mathrm{Gal}\,(B/F) \cong \frac{G}{\mathrm{Gal}\,(E/B)} \cong \mathrm{Gal}\,(E/C)$ و $\mathrm{Gal}(E/B)\cong\mathrm{Gal}(C/F)$. □

همچنین بوسیلهٔ قضیه اساسی می‌توان مثالهای نقض را معرفی کرد ، زیرا آن مسائل در مورد میدانها (که معمولاً ساختار نامتناهی دارند) را به مسائل در مورد گروههای متناهی انتقال می‌دهد . به عنوان مثال ، فرض کنیم E/F یک توسیع گالوا باشد ، و B و C میدانهای میانی بترتیب از درجات 2^b و 2^c باشند ، آیا درجهٔ ترکیب آنها، $B\vee C$ نیز توانی

از ۲ است؟ اگر $G = Gal\ (E/F)$ و H و K بترتیب زیرگروههای متناظر با B و C باشند، آنگاه قضیهٔ اساسی نتیجه می‌دهد که $[B \vee C:F] = [G:H \cap K]$. سـؤال منتقل شده این است که : اگر $[G:H] = 2^b$ و $[G:K] = 2^c$ آیا $[G:H \cap K]$ توانی از ۲ می‌باشد؟ در تمرین ۸۸ دیدیم که یک توسیع گالوای E/F با $Gal\ (E/F) \cong S_4$ وجود دارد. فرض کنیم H زیرگروه تمام جایگشتهای بر مجموعهٔ $\{3\ ,\ 2\ ,\ 1\}$ باشد (یعنی ، به ازای هر σ از S_4، $\sigma(4)=4$) و K زیرگروه تمام جایگشتهای بر مجموعهٔ $\{2,3,4\}$ باشد. اکـنون $[S_4:H]=[S_4:K]=4$ امـا $[S_4:H \cap K]=12$ زیـرا $H \cap K=\{(1),(2,3)\}$ از مرتبهٔ ۲ است).

تمرین :

۹۱. (آ) فرض کنیم E/F یک توسیع گالوا باشد، آیا ضروری است کـه یک مـیدان میانی از درجهٔ اول بر F موجود باشد؟ (راهنمایی گروه متناوب A_6 دارای هیچ زیرگروهی با اندیس اول نیست (قضیه A35 را ببینید).)

(ب) همان سوال (آ) با این فرض اضافی که $Gal(E/F)$ یک گروه حل‌پذیراست.

اکنون در صدد اثبات قضیهٔ اساسی جبر هستیم. فرض کنیم که R در یک صورت ضعیف از قضیهٔ مقدار میانی صدق کند: اگر $f(x) \in R[x]$ و $b\ ,\ a$ ای از R موجود باشند به طوری که $f(a)>0$ و $f(b)<0$، آنگاه $f(x)$ یک ریشهٔ حقیقی دارد. دراینجا چند نتیجه مقدماتی عبارتند از

(۱). هر عدد حقیقی و مثبت r دارای یک ریشهٔ دوم حقیقی است .

اگر $f(x)=x^2-r$ ، آنگاه $f(1+r)>0$ و $f(0)<0$.

(۲). هر درجهٔ دوم $g(x) \in C[x]$ دارای یک ریشهٔ مختلط است.

ابتدا، **هر عدد مختلط** دارای یک ریشهٔ دوم **مختلط** است: باید اعداد حقیقی $y\ ,\ x$

با $(x+iy)^2=a+ib$ را پیداکرد و این ساده است. فرمول درجهٔ دوم مورد نیاز خواهد برد و عبارت زیر رادیکال (مبین) به یک عدد حقیقی نامنفی تبدیل می‌شود. اکنون کاربرد دیگر فرمول درجهٔ دوم ارائه ریشه‌های مختلط $g(x)$ می‌باشد.

(۳). میدان C دارای هیچ توسیعی از درجهٔ ۲ نیست .

چنین توسیعی باید شامل عضوی باشد که چند جمله‌ای تحویل‌ناپذیر آن از درجهٔ ۲ در $C[x]$ است و (۲) نشان می‌دهد که چنین چند جمله‌ای وجود ندارد.

(۴). هر $f(x)\in R[x]$ از درجهٔ فرد یک ریشهٔ حقیقی دارد.

فرض کنیم $f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n\in R[x]$. تعریف می‌کنیم $t=1+\sum|a_i|$. اکنون به ازای هر i، $|a_i| \le t-1$ و

$$|a_0+a_1t+\cdots+a_{n-1}t^{n-1}| \le (t-1)(1+t+\cdots+t^{n-1}) = t^n-1 < t^n .$$

از آن نتیجه می‌شود که $f(t)>0$ (به ازای هر n نه لزوماً فرد) زیرا جملات ابتدایی بوسیلهٔ t^n مشخص شده است. وقتی n فرد است، $f(-t)<0$ زیرا $(-t)^n=(-1)^nt^n<0$ ، و بنابراین ارزیابی مشابه همانند بالانشان می‌دهد که $f(-t)<0$.

(۵). توسیع میدان E/R از درجهٔ فرد بزرگتر از ۱ وجود ندارد.

اگر $\alpha\in E$، آنگاه بنابر (۴) چند جمله‌ای تحویل‌ناپذیر آن باید دارای درجهٔ زوج باشد، به طوری که $[R(\alpha):R]$ زوج است. بنابراین $[E:R]=[E:R(\alpha)][R(\alpha):R]$ زوج است .

قضیه ۷۱ : (قضیهٔ اساسی جبر). هر چند جمله‌ای غیرثابت $f(x)\in C[x]$ دارای یک ریشهٔ مختلط است .

برهان : اگر $f(x)\in C[x]$، آنگاه $\bar{f}(x)\in R[x]$ $f(x)$، که $\bar{f}(x)$ از $f(x)$ با در نظر گرفتن مزدوج مختلط هر یک از ضرایب حاصل شده است. چون $f(x)$ دارای یک ریشهٔ مختلط

است اگر و فقط اگر $\bar{f}(x)$ $f(x)$ دارای یک ریشهٔ مختلط باشد، کافی است ثابت کنیم که هر چند جمله‌ای حقیقی دارای یک ریشهٔ مختلط است.

فرض کنیم $p(x)$ یک چند جمله‌ای تحویل‌ناپذیر در $R[x]$ باشد، و فرض کنیم E/R میدان شکافندهٔ $(x^2+1)p(x)$ باشد که شامل C است. چون R دارای مشخصهٔ صفر است، E/R یک توسیع گالواست، فرض کنیم G گروه گالوای آن باشد. اگر $|G|=2^m k$ ، که k فرد است، آنگاه بنابر قضیهٔ سیلو (قضیهٔ A13) G دارای یک زیرگروه H از مرتبهٔ 2^m می‌باشد ، فرض کنیم $B=E^H$ میدان میانی متناظر باشد. اکنون درجهٔ $[B:R]$ برابر اندیس $[G:H]=k$ است. اما در بالا دیدیم که R دارای هیچ توسیعی از درجهٔ فرد بزرگتر از ۱ نیست، بنابراین $k=1$ و G یک ۲-گروه است. بنابر قضیهٔ A23 ، زیرگروه $Gal(E/C)$ از G (متناظر با C) دارای یک زیرگروه با اندیس ۲ می‌باشد، میدان میانی متناظر با آن یک توسیع از C از درجهٔ ۲ است، و این متناقض با (۳) بالا می‌باشد. در نتیجه $Gal(E/C)=\{1\}$ و $E=C$. $\square$

قضیهٔ بزرگ گالوا

عکس قضیهٔ ۵۳ (که فقط در مورد مشخصه‌های صفر برقراراست) را ثابت می‌کنیم. حل‌پذیری گروه گالوا حل‌پذیری بوسیلهٔ رادیکالهای یک چند جمله‌ای را نتیجه می‌دهد. اولی دارای یک نام خیلی ظریف حاکی از استفاده آن به عنوان یک وسیله برای رفع کمبود احتمالی ریشه‌های یکانی در میدان زمینه می‌باشد.

لم ۷۲ : (گنگ‌های فرعی). فرض کنیم E/F میدان شکافندهٔ $f(x)\in F[x]$ با گروه گالوای $G=Gal(E/F)$ باشد. اگر F^*/F یک توسیع و E^*/F^* میدان شکافندهٔ $f(x)$ شامل E باشد، آنگاه تحدید $\sigma \longrightarrow \sigma|E$ هomomorفیسم یک به یک $Gal(E^*/F^*) \longrightarrow Gal(E/F)$ می‌باشد.

برهان : از فرض نتیجه می‌شود که $E=F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ و $E^*=F^*(\alpha_1,\alpha_2,\cdots,\alpha_n)$ که $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ مجموعهٔ ریشه‌های $f(x)$ می‌باشد. اگر $\sigma\in Gal(E^*/F^*)$، آنگاه σ اعضای مجموعهٔ $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ را جابه جا می‌کند و F^* را ثابت نگه می‌دارد، لذا F را ثابت نگه می‌دارد، بنابراین $\sigma|_E\in Gal(E/F)$. با بکار بردن تمرین ۷۳ دیده می‌شود که $\sigma|_E \longrightarrow \sigma$ یک به یک است. □

تعریف: اگر E/F یک توسیع گالوا باشد و $\alpha\in E^{\#}=E-\{0\}$، نرم α را با $N(\alpha)$ نشان می‌دهیم و تعریف می‌کنیم $N(\alpha)=\prod_{\sigma\in G}\sigma(\alpha)$.

در اینجا چند خاصیت مقدماتی نرم که دارای برهانهای ساده به عنوان تمرین می‌باشند، عبارتند از

(آ) اگر $\alpha\in E^{\#}$، آنگاه $N(\alpha)\in F^{\#}$ (زیرا $N(\alpha)\in E^G=F$).

(ب) $N(\alpha\beta)=N(\alpha)N(\beta)$، به طوری که $N:E^{\#} \longrightarrow F^{\#}$ یک همومورفیسم است.

(ج) اگر $a\in F$، آنگاه $N(a)=a^n$ که $n=[E:F]$.

(د) اگر $\sigma\in G$ و $\alpha\in E^{\#}$، آنگاه $N(\sigma(\alpha))=N(\alpha)$.

دربارهٔ هسته و تصویر یک همومورفیسم داده شده سؤال می‌شود. محاسبهٔ تصویر نرم ساده نیست، نتیجهٔ بعدی (که یک تفسیر از نودمین قضیهٔ هیلبرت (۱۸۹۷) در نظریهٔ جبری اعداد می‌باشد) هستهٔ نرم را در یک حالت خاص محاسبه می‌کند.

لم ۷۳ : (قضیه ۹۰ هیلبرت). فرض کنیم E/F یک توسیع گالوا باشد که گروه گالوای $G=Gal(E/F)$ دوری از مرتبهٔ n است، فرض کنیم σ یک مولد G باشد. در این صورت $N(\alpha)=1$ اگر و فقط اگر βای از E موجود باشد که $\alpha=\beta\sigma(\beta)^{-1}$.

برهان: اگر $\alpha=\beta\sigma(\beta)^{-1}$، آنگاه

$$N(\alpha)=N(\beta\sigma(\beta)^{-1})=N(\beta)N(\sigma(\beta)^{-1})=N(\beta)N(\beta)^{-1}=1 .$$

بالعکس، نرم‌های جزیی $\delta_0=\alpha$, $\delta_1=\alpha\sigma(\alpha)$, $\delta_2=\alpha\sigma(\alpha)\sigma^2(\alpha)$, $\cdots$, $\delta_{n-1}=\alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha)=N(\alpha)=1$ را تعریف می‌کنیم . دیدن اینکه به ازای هر $0\leq i \leq n-2$ ، (۱) $\alpha\sigma(\delta_i)=\delta_{i+1}$ ساده می‌باشد . بنابراستقلال مشخصه‌های $\{1 , \sigma , \sigma^2 , \cdots , \sigma^{n-1}\}$ ، γ ای از E وجود دارد که $\delta_0\gamma+\delta_1\sigma(\gamma)+\cdots+\delta_i\sigma^{i}(\gamma)+\cdots+\delta_{n-2}\sigma^{n-2}(\gamma)+\sigma^{n-1}(\gamma)\neq 0$ ، این مجموع را β می‌نامیم. با بکاربردن معادلهٔ (۱)، به سادگی ملاحظه می‌شود که

$$\sigma(\beta)=\alpha^{-1}[\delta_1\sigma(\gamma)+\cdots+\delta_i\sigma^{i}(\gamma)+\cdots+\delta_{n-1}\sigma^{n-1}(\gamma)]+\sigma^{n}(\gamma) .$$

اما $\sigma^n=1$ ، همچنین در جملهٔ قبل دقیقاً $\gamma=\alpha^{-1}\delta_0\gamma$. بنابراین $\sigma(\beta)=\alpha^{-1}\beta$ ، و همان نتیجهٔ مطلوب است . □

نتیجه ۷۴: فرض کنیم E/F یک توسیع گالوا از درجهٔ اول p باشد. اگر F دارای یک ریشهٔ p ام اولیهٔ یکانی باشد، آنگاه $E=F(\beta)$ که $\beta^p\in F$ ، و بنابراین E/F یک توسیع محض است .

برهان : اگر ω یک ریشهٔ p ام اولیهٔ یکانی باشد ، آنگاه $N(\omega)=\omega^p=1$ زیرا $\omega\in F$. اکنون $G = Gal(E/F)$ از مرتبهٔ p است، بنابراین دوری است، فرض کنیم σ یک مولد آن باشد. بنابر قضیهٔ ۹۰ هیلبرت به ازای βای از E داریم $\omega=\beta\sigma(\beta)^{-1}$. بنابراین $\sigma(\beta)=\beta\omega^{-1}$. از آن نتیجه می‌شود که $\sigma(\beta^p)=(\beta\omega^{-1})^p=\beta^p$ ، و همچنین $\beta^p\in E^G=F$ زیرا σ یک مولد G و E/F یک توسیع گالوا می‌باشد . توجه کنیم که $\beta\notin F$، مگر $\omega=1$، به طوری که $F(\beta)\neq F$ یک میدان میانی باشد . بنابراین $E=F(\beta)$، زیرا $[E:F]=p$ ، و لذا E دارای هیچ میدان میانی واقعی نیست . □

قضیهٔ زیر عکس قضیهٔ ۵۳ می‌باشد.

قضیه ۷۵ : (گالوا) . فرض کنیم F یک میدان از مشخصهٔ صفر باشد ، فرض کنیم E/F

یک توسیع گالوا و $G=Gal(E/F)$ یک گروه حل‌پذیر باشد. در این صورت E را می‌توان در یک توسیع رادیکال از F محاط کرد.

بنابراین، گروه گالوای یک چند جمله‌ای بر یک میدان از مشخصهٔ صفر یک گروه حل‌پذیر است اگر و فقط اگر این چند جمله‌ای بوسیلهٔ رادیکالها حل‌پذیر باشد.

برهان: اثبات به‌استقراء بر $[E:F]$ می‌باشد. مرحلهٔ پایه به‌طوربدیهی درست است. چون G حل‌پذیر است، نتیجهٔ A17 زیرگروه نرمال H با اندیس اول p را فراهم می‌سازد. فرض کنیم ω یک ریشهٔ p ام اولیهٔ یکانی باشد (که وجود دارد زیرا F دارای مشخصهٔ صفر است)، و تعریف می‌کنیم $F^*=F(\omega)$ و $E^*=E(\omega)$. مشاهده می‌کنیم که E^*/F یک توسیع گالواست (اگر E/F یک میدان شکافندهٔ $f(x)\in F[x]$ باشد، آنگاه E^*/F یک میدان شکافندهٔ چند جمله‌ای لزوماً جداپذیر $f(x)(x^p-1)$ است)، بنابراین E^*/F^* نیز یک توسیع گالوا می‌باشد. اگر E^* را بتوان در یک توسیع رادیکال R^*/F^* محاط کرد، آنگاه E را نیز می‌توان در R^* محاط کرد. اما F^*/F یک توسیع محض است، به طوری که R^* یک توسیع رادیکال F است، بنابر این E را می‌توان در یک توسیع رادیکال از F محاط کرد، و همان نتیجهٔ مطلوب است.

فرض کنیم $G^*=Gal(E^*/F^*)$، بنابر قضیهٔ گنگ‌های فرعی هomomorفیسم یک‌به یک $\psi:G^* \longrightarrow G= Gal(E/F)$ (مثلاً $\sigma \longrightarrow \sigma|_E$) وجود دارد، و بنابراین G^* حل‌پذیر است (با یک زیرگروه از یک گروه حل‌پذیر ایزومورف است). زیرگروه $Im\psi(\cong G^*)$ از G رادرنظر می‌گیریم. اگر $Im\psi$ یک زیرگروه واقعی باشد، آنگاه $[E^*:F^*]=|G^*|<|G|=[E:F]$. بنابراستقراء، E^* رامی‌توان در یک توسیع رادیکال از F^* محاط کرد. اگر $Im\psi=G$، فرض کنیم $B=E^k$ (که $K=\psi^{-1}(H)\subset G^*$)، آنگاه

B/F^* یک توسیع گالوا از درجهٔ اول p و F^* یک توسیع محض است. اکنون E^*/B یک توسیع گالوا از درجهٔ کمتر از $[E^*:F^*]=|G^*|=|G|=[E:F]$ است. چون $Gal(E^*/B)$ حل‌پذیراست (یک زیرگروه از گروه حل‌پذیر G^* است)، بنابر فرض استقراء E^* را می‌توان در یک توسیع رادیکال R' از B محاط کرد. چون B/F^* یک توسیع محض است، می‌بینیم که R'/F^* نیز یک توسیع رادیکال است. □

در ابتدا قضیهٔ آبل، که یک چند جمله‌ای با گروه گالوای جابجایی بوسیلهٔ رادیکالها حل‌پذیر است، بوسیلهٔ گالوا جایگزین شد(به دلیل این قضیه است که امروزه چنین گروههایی آبلی نامیده می‌شوند).

قضیهٔ ژرف فیت[1] و تامسون[2] (۱۹۶۳) می‌گوید که هرگروه از مرتبهٔ فرد حل‌پذیر است. از آن نتیجه می‌شود که اگر F یک میدان با مشخصهٔ صفر باشد و $f(x)\in F[x]$ یک چند جمله‌ای که گروه گالوای آن از درجهٔ فرد است، به طور معادل، که میدان شکافندهٔ آن دارای درجهٔ فرد بر F است، آنگاه $f(x)$ بوسیلهٔ رادیکالها حل‌پذیر است.

فرض کنیم که گروه گالوای G از چند جمله‌ای $f(x)\in Q[x]$ معلوم باشد که G حل‌پذیر است. به عنوان تمرین، با استفاده از این اطلاعات می‌توان ریشه‌های $f(x)$ را پیداکرد؟ جواب مثبت است، پیشنهاد می‌کنیم که خواننده کتابهای [Edwards] و [Gaal] را برای چگونگی انجام این عمل را ببینند.

مبین‌ها

فرض کنیم F یک میدان از مشخصهٔ صفر و $f(x)\in F[x]$ یک چند جمله‌ای از درجهٔ n دارای میدان شکافندهٔ E/F باشد، فرض کنیم $G=Gal(E/F)$. اگر $\alpha_1, \alpha_2, \cdots, \alpha_n$

---

1. Feit　　2. Thomson

ریشه‌های $f(x)$ در E (با تکرار ریشه‌ها از هر مرتبه‌ای) باشند، تعریف می‌کنیم $\Delta=\prod_{i<j}(\alpha_i-\alpha_j)$. عدد Δ به اندیس‌گذاری ریشه‌ها بستگی دارد، اندیس‌گذاری جدیدی ممکن است علامت Δ را تغییر دهد. بنابر این $D=\Delta^2$ فقط به مجموعهٔ ریشه‌ها بستگی دارد.

تعریف : $D=\Delta^2$ مبین چند جمله‌ای $f(x)\in F[x]$ است.

واضح است که $f(x)$ دارای ریشهٔ تکراری است اگر و فقط اگر $D=0$. هر $\sigma\in G$، α_1 , α_2 , $\cdots$, α_n را جابه جا می‌کند، به طوری که $\sigma(\Delta)=\pm\Delta$، بنابر این $\Delta^2=D\in E^G=F$.

اگر $f(x) = x^2 + bx + c$، آنگاه فرمول درجهٔ دوم ریشه‌های $\alpha = \frac{1}{2}(-b+\sqrt{b^2-4c})$ و $\beta = \frac{1}{2}(-b-\sqrt{b^2-4c})$ از $f(x)$ را نتیجه می‌دهد. از آن نتیجه می‌شود که $D=\Delta^2=(\alpha-\beta)^2=b^2-4c$.

اگر $f(x)$ یک چند جمله‌ای درجهٔ سوم با ریشه‌های α , β , γ باشد، آنگاه $D=\Delta^2=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$. چگونگی محاسبهٔ D برحسب ضرایب $f(x)$ واضح نیست.

تعریف : چند جمله‌ای $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$ را تقلیل یافته نامیم، اگر $a_{n-1}=0$.
اگر $f(x)$ یک چند جمله‌ای تکین از درجهٔ n باشد، آنگاه $\tilde{f}(x)$ چند جمله‌ای تقلیل یافتهٔ متناظر با آن است که از $f(x)$ با تغییر متغیر $y=x-\frac{a_{n-1}}{n}$ به دست آمده است.

قضیه ۷۶ : (آ) چند جمله‌ای $f(x)$ و چند جمله‌ای تقلیل یافتهٔ متناظر با آن یعنی $\tilde{f}(x)$ دارای مبین یکسان می‌باشند.

(ب) مبین درجهٔ سوم تقلیل یافتهٔ $\tilde{f}(x) = x^3+qx+r$ برابر $D=-4q^3-27r^2$ است .

برهان: (آ) اگر $\alpha_1 , \alpha_2 , \cdots , \alpha_n$ ریشه‌های $f(x)$ باشند، آنگاه $\beta_1 , \beta_2 , \cdots , \beta_n$ ریشه‌های $\tilde{f}(x)$ می‌باشند، که $\beta_i=\alpha_i+\frac{a_{n-1}}{n}$. بنابراین $\prod_{i<j}(\alpha_i-\alpha_j)=\prod_{i<j}(\beta_i-\beta_j)$ ، و بنابراین مبین‌ها (که مربع اینها هستند) برابر می‌باشند.

(ب) فرمول درجهٔ سوم ریشه‌های زیر از $\tilde{f}(x)$ را نتیجه می‌دهد :

$$\alpha_1 = y + z \quad , \quad \alpha_2 = \omega y + \omega^2 z \quad , \quad \alpha_3 = \omega^2 y + \omega z$$

در اینجا، ω یک ریشهٔ سوم یکانی است، $y = [\frac{1}{2}(-r+\sqrt{R})]^{1/3}$ و $z=[\frac{1}{2}(-r-\sqrt{R})]^{1/3}$ و $R=r^2+\frac{4q^3}{27}$. بنابراین

$$\Delta = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)$$
$$= (y+z-\omega y-\omega^2 z)(y+z-\omega^2 y-\omega z)(\omega y+\omega^2 z-\omega^2-\omega^2 y-\omega z)$$

به سادگی دیده می‌شود که $\alpha_1-\alpha_2=(1-\omega)(y-\omega^2 z)$,

$$\alpha_1-\alpha_3=-\omega^2(1-\omega)(y-\omega z) \quad , \quad \alpha_2-\alpha_3=\omega(1-\omega)(y-z)$$

بنابراین $\Delta = -(1-\omega)^3\omega^3(y-z)(y-\omega z)(y-\omega^2 z)$. اکنون $\omega^3=1$ نتیجه می‌دهد که $-(1-\omega)^3\omega^3=3\sqrt{3}\, i$ (که $i^2=-1$) ، بعلاوه همانی $\zeta^3-1=(\zeta-1)(\zeta-\omega)(\zeta-\omega^2)$ با $\zeta=\frac{y}{z}$ نتیجه می‌دهد که $(y-z)(y-\omega z)(y-\omega^2 z)=y^3-z^3=\sqrt{R}$. بنابراین $\Delta = 3\sqrt{3}\, i\sqrt{R}$ و $D=\Delta^2=-27R=-27r^2-4q^3$. □

تمرین :

*۹۲. یک چند جمله‌ای و چند جمله‌ای تقلیل یافتهٔ متناظر با آن دارای گروه گالوای یکسان می‌باشند.

۹۳. (آ) اگر $f(x)=x^3+ax^2+bx+c$ ، آنگاه چند جمله‌ای تقلیل یافتهٔ متناظر باآن x^3+qx+r است که $q=b-\frac{a^3}{3}$ و $r=\frac{2a^3}{27}-\frac{ab}{3}+c$.

(ب) نشان دهید که مبین $f(x)$ برابر $D=a^2b^2-4b^3-4a^3c-27c^2+18abc$ می‌باشد.

تبصره: ارتباطی بین مبین و گروه متناوب A_n وجود دارد. اگر $\pi \in S_n$، فرض کنیم π بر $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$ بوسیلهٔ جابه‌جا کردن زیرنویسها اثر کند، بنابراین $\pi(\Delta) = \pm \Delta$. نگاشت $\theta : S_n \longrightarrow Z_2$ را با ضابطهٔ $\theta(\pi) = \bar{0}$ اگر $\pi(\Delta)=\Delta$، و $\theta(\pi) = \bar{1}$ اگر $\pi(\Delta)=-\Delta$ تعریف می‌کنیم. دیدن اینکه θ یک همومورفیسم پوشا با هستهٔ A_n است ساده می‌باشد، زیرا گروه متناوب A_n زیرگروه منحصر بفرد S_n با اندیس ۲ می‌باشد. (قضیهٔ A28).

گروههای گالوای چند جمله‌ایهای درجهٔ دوم، درجهٔ سوم و درجهٔ چهارم

در این بخش پایانی، چگونگی محاسبهٔ گروههای گالوای چند جمله‌ایهای از درجات پایین بر Q را نشان می‌دهیم. به خاطر داریم که گروه گالوای یک چند جمله‌ای از درجهٔ n زیرگروه S_n است (به عنوان گروه تمام جایگشتهای بر ریشه‌ها در نظر گرفته شد، البته، بعضی از این جایگشتها ممکن است دیگر اتومورفیسمهای میدان نباشند).

لم ۷۷ : فرض کنیم $f(x) \in F[x]$ دارای مبین $D = \Delta^2$ و گروه گالوای $G=Gal(E/F)$ باشد. اگر $H=G \cap A_n$، آنگاه $E^H=F(\Delta)$، بعلاوه، $\sqrt{D} \in F$ اگر و فقط اگر G یک زیرگروه A_n باشد.

برهان: بوضوح $F(\Delta) \subset E^H$ و $[E^H:F] = [G:H] \leq 2$، کافی است ثابت کنیم که $[F(\Delta):F]=[G:H]$. اگر $[G:H]=2$، آنگاه σ ای از G هست که $\sigma \notin H$ و $\sigma(\Delta) \neq \Delta$، بنابراین $\Delta \notin E^H=F$ و $[F(\Delta) : F] = 2$. اگر $[G:H] = 1$، آنگاه $G=H$ و $F(\Delta) \subset E^H=E^G=F$، بنابر این $[F(\Delta):F]=1$.

برای اثبات گزارهٔ دوم، قضیهٔ اساسی نظریهٔ گالوا می‌گوید که اگر $F(\Delta)=E^H=F$

و فقط اگر $G=H$ (زیرا $E^G=F$). چون $H=G\cap A_n$، به این معنی است که $G \subset A_n$. $\square$

اگر $f(x)\in Q[x]$ از درجهٔ ۲ باشد، آنگاه گروه گالوای آن از مرتبه ۱ یا ۲ می‌باشد (زیرا گروه متقارن S_2 از مرتبهٔ 2 است). اگر $f(x)$ شکافته شود گروه گالوا از مرتبه ۱ است، اگر $f(x)$ شکافته نشود، یعنی اگر $f(x)$ تحویل‌ناپذیر باشد، گروه گالوای آن از مرتبهٔ ۲ است.

اگر $f(x)\in Q[x]$ یک درجهٔ سوم دارای یک ریشهٔ گویا باشد، در این صورت گروه گالوای G از آن همانند عامل درجهٔ دوم آن است. در غیراین صورت $f(x)$ تحویل‌ناپذیر است، چون $|G|$ مضربی از ۳ است و $G\subset S_3$، از آن نتیجه می‌شود که یا $G\cong A_3\cong Z_3$ یا $G\cong S_3$.

قضیه ۷۸ : فرض کنیم $f(x)\in Q[x]$ یک درجهٔ سوم تحویل‌ناپذیر با گروه گالوای G و مبین D باشد.

(آ) $f(x)$ دارای دقیقاً یک ریشهٔ حقیقی است اگر و فقط اگر $D<0$، در این حالت $G\cong S_3$.

(ب) $f(x)$ دارای سه ریشهٔ حقیقی است اگر و فقط اگر $D>0$. در این حالت یا $\sqrt{D}\in Q$ و $G\cong Z_3$ یا $\sqrt{D}\notin Q$ و $G\cong S_3$.

برهان : توجه کنیم که $D\neq 0$ زیرا Q دارای مشخصهٔ صفر و کامل است، بنابراین چند جمله‌ایهای تحویل‌ناپذیر دارای هیچ ریشهٔ تکراری نیستند. اگر $f(x)$ دارای سه ریشه حقیقی باشد، آنگاه Δ حقیقی است و $D = \Delta^2>0$. بالعکس، فرض کنیم که $f(x)$ دارای یک ریشهٔ حقیقی α و دو ریشهٔ مختلط $\beta=u+iv$ و $\bar{\beta}=u-iv$ باشد. بنابر قضیهٔ ۷۶ (آ)، وقتی که جملهٔ درجهٔ دوم $f(x)$ را حذف می‌کنیم مبین تغییر نمی‌کند،

همچنین می‌توان فرض کرد که این عمل انجام شده است، بنابر این $\alpha + \beta + \bar{\beta} = 0$ و $\alpha = -2u$. بنابراین

$\Delta = (\alpha-\beta)(\alpha-\bar{\beta})(\beta-\bar{\beta}) = (-3u-iv)(-3u+iv)(2iv) = (9u^2+v^2)(2iv)$،

و لذا $D = \Delta^2 = -4v^2(9u^2+v^2)^2 < 0$.

فرض کنیم که E/Q میدان شکافندهٔ $f(x)$ باشد. اگر $f(x)$ دارای دقیقاً یک ریشهٔ حقیقی α باشد، آنگاه $E \neq Q(\alpha)$. بنابر این $|G| > 3$ و $G \cong S_3$. اگر $f(x)$ دارای سه ریشهٔ حقیقی باشد، آنگاه $D>0$ و $\sqrt{D}$ حقیقی است. بنابر لم ۷۷، $G \cong A_3 \cong Z_3$ اگر و فقط اگر $\sqrt{D}$ گویا باشد، بنابر این $G \cong S_3$ اگر $\sqrt{D}$ گنگ باشد. □

چند جمله‌ای درجهٔ چهارم تقلیل یافتهٔ $f(x) = x^4+qx^2+r\ x+s \in Q[x]$ را در نظر می‌گیریم، فرض کنیم E/Q میدان شکافندهٔ آن و $G = Gal(E/Q)$ گروه گالوای آن باشد. (بنابر تمرین ۹۲ بدون کاستن از کلیت، فرض کنیم که $f(x)$ تقلیل یافته است.) اگر $f(x)$ دارای یک ریشهٔ گویای r باشد، آنگاه $f(x) = (x-r)h(x)$، و گروه گالوای آن با گروه گالوای عامل درجهٔ سوم $h(x)$ از آن یکسان است، و این بنابر قضیهٔ ۷۸ محاسبه شده است. فرض کنیم که $f(x) = p(x)q(x)$ حاصلضرب دو درجهٔ دوم تحویل‌ناپذیر باشد، فرض کنیم α یک ریشه از $p(x)$ و β یک ریشه از $q(x)$ باشد. اگر $Q(\alpha) \cap Q(\beta) = Q$، یعنی اگر میدانها متمایز خطی باشند، آنگاه نتیجهٔ ۷۰ نشان می‌دهد که $G \cong V$، در غیر این صورت $\alpha \in Q(\beta)$ به طوری که $Q(\beta) = Q(\alpha, \beta) = E$، و G از مرتبهٔ ۲ است.

در حالتی که $f(x)$ تحویل‌ناپذیر است مسأله را رها می‌کنیم. اکنون ایدهٔ اساسی مقایسهٔ G با گروه چهار کلاین، مثلاً، زیرگروه نرمال

$V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ از S_4 است، به طوری که بتوانیم

میدان ثابت $V\cap G$ را تعیین کنیم. اگر $\alpha_4,\alpha_3,\alpha_2,\alpha_1$ چهار ریشهٔ متمایز $f(x)$ باشند، آنگاه اعداد $u=(\alpha_1+\alpha_2)(\alpha_3+\alpha_4)$ و $v=(\alpha_1+\alpha_3)(\alpha_2+\alpha_4)$ و $w=(\alpha_1+\alpha_4)(\alpha_2+\alpha_3)$ را در نظر می‌گیریم. واضح است که اگر $\sigma\in V\cap G$، آنگاه σ اعداد u , v , w را ثابت نگه می‌دارد.

بالعکس، بررسی هر ۲۴ جایگشت نشان می‌دهد که اگر $\sigma\in S_4$، آنگاه σ عدد $(\alpha_i+\alpha_j)(\alpha_k+\alpha_l)$ را ثابت نگه می‌دارد. بنابر این $\sigma\in V\cup\{(i,j)\ ,\ (k,l)\ ,\ (i\ ,\ k\ ,\ j\ ,\ l)\ ,\ (i\ ,\ l\ ,\ j\ ,\ k)\}$. از آن نتیجه می‌شود که $\sigma\in G$ هر یک از اعضای w,v,u را ثابت نگه می‌دارد اگر و فقط اگر $\sigma\in V\cap G$، و لذا $Q(u,v,w)$ میدان پایای $V\cap G$ می‌باشد.

تعریف : $g(x)=(x-u)(x-v)(x-w)$ را درجهٔ سوم حلال[۱] $f(x)=x^4+qx^2+rx+s$ می‌نامند.

قضیه ۷۹: اگر $g(x)$ درجه سوم حلال $f(x)=x^4+q\ x^2+r\ x+s$ باشد، آنگاه

$$g(x) = x^3 - 2qx^2 + (q^2 - 4s)\ x + r^2 .$$

برهان: در مبحث فرمول درجهٔ چهارم کلاسیکی، دیدیم که $f(x)=(x^2+kx+L)(x^2-kx+m)$ و k^2 یک ریشهٔ چند جمله‌ای $h(x)=x^3+2q\alpha_x{}^2+(q^2-4s)x-\alpha_r{}^2$ است، یک چند جمله‌ای متفاوت با عبارت ادعا

---

۱. درجه سوم حلال دیگری در نوشته‌ها وجود دارد که از ترکیب دیگر ریشه‌های پایا تحت V ناشی می‌شود. تعریف می‌کنیم $u'=\alpha_1\alpha_2+\alpha_3\alpha_4$ ، $v'=\alpha_1\alpha_3+\alpha_2\alpha_4$ ، $w'=\alpha_1\alpha_4+\alpha_2\alpha_3$ ، و تعریف می‌کنیم $h(x)=(x-u')(x-v')(x-w')$. این درجهٔ سوم (که متمایز از $g(x)$ است) خیلی شبیه $g(x)$ رفتار می‌کند. دلیل ترجیح دادن $g(x)$ ، تمرین ۹۴ می‌باشد، برای محاسبهٔ مبین یک درجهٔ چهارم می‌توان $g(x)$ را به کار برد.

شده برای $g(x)$ تنها در علامت درجهٔ دوم و جملات ثابت آن می‌باشد. بنابر این، عدد β یک ریشهٔ $h(x)$ است اگر و فقط اگر $-\beta$ یک ریشهٔ $g(x)$ باشد.

فرض کنیم چهار ریشهٔ $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ از $f(x)$ طوری اندیسگذاری شده باشند که α_1 ، α_2 ریشه‌های x^2+kx+1 و α_3 ، α_4 ریشه‌های x^2-kx+m باشند. در این صورت $k=-(\alpha_1+\alpha_2)$ و $-k=-(\alpha_3+\alpha_4)$ ، بنابراین $u=(\alpha_1+\alpha_2)(\alpha_3+\alpha_4)=-k^2$ ، و $-u$ یک ریشهٔ $h(x)$ است.

اکنون $f(x)$ را به دو درجهٔ دوم، مثلاً $f(x)=(x^2+k'x+l')(x^2-k'x+m')$ تجزیه می‌کنیم، که α_1 ، α_3 ریشه‌های عامل اولی و α_2 ، α_4 ریشه‌های عامل دومی باشند. آرگومان مشابه همانند بالا نشان می‌دهد که $v=(\alpha_1+\alpha_3)(\alpha_2+\alpha_3)=-k'^2$، بنابر این $-v$ یک ریشهٔ $h(x)$ است. به طور مشابه، $-w=-(\alpha_1+\alpha_4)(\alpha_2+\alpha_3)$ یک ریشهٔ $h(x)$ است. بنابر این $h(x)=(x+u)(x+v)(x+w)$ ، و نیز $g(x)=(x-u)(x-v)(x-w)$ با تغییر علامت درجهٔ دوم و جملات ثابت از $h(x)$ به دست آمده است. □

تمرین :

۹۴*. اگر $f(x)$ یک درجهٔ چهارم باشد، آنگاه مبین آن برابر قرینهٔ مبین درجهٔ سوم حلال آن می‌باشد. (راهنمایی : $u-v=-(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)$,

$(v-w=-(\alpha_1-\alpha_2)(\alpha_3-\alpha_4)$, $u-w=-(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)$.

۹۵. اگر درجهٔ سوم حلال چند جمله‌ای درجهٔ چهارم $f(x)$ برابر x^3+ax^2+bx+c باشد، آنگاه مبین $f(x)$ برابر

$D=-16a^4c+4a^3b^2+128a^2c^2-144ab^2c+27b^4-256c^3$ می‌باشد.

۹۶. نشان دهید که $x^3+ax+2\in R[x]$ دارای سه ریشهٔ حقیقی است اگر و فقط اگر $a\leq -3$.

*۹۷. فرض کنیم G زیرگروهی از S_4 با $|G|$ مضربی از ۴ باشد ، تعریف می‌کنیم $m=|G/G\cap V|$ که V گروه چهار کلاین است .

(آ) ثابت کنید که m یک مقسوم‌علیه ۶ است .

(ب) اگر $m=6$ ، آنگاه $G=S_4$. اگر $m=3$ ، آنگاه $G=A_4$. اگر $m=1$ ، آنگاه $G=V$. اگر $m=2$ ، آنگاه $G\cong D_8$ یا $G\cong Z_4$ یا $G\cong V$.

(راهنمایی : این تمرین قضیه A33 در نظریهٔ گروه می‌باشد .)

*۹۸. فرض کنیم G یک زیرگروه S_4 با $|G|=4$ باشد . اگر G به طور تعدی بر مجموعهٔ $X=\{1,2,3,4\}$ اثر کند و $|G\cap V|=2$ ، آنگاه $G\cong D_8$ یا $G\cong Z_4$.

(**تبصره:** اگر G به طور تعدی بر X اثر کند ، آنگاه $|G|$ مضربی از ۴ است (لم A10).
در تمرین ۹۷ ، وقتی که $m=2$ ، این فرض قویتر امکان $G\cong V$ را حذف می‌کند.)

قضیه ۸۰ : فرض کنیم $f(x)\in Q[x]$ یک چند جمله‌ای درجهٔ چهارم تحویل‌ناپذیر با گروه گالوای G باشد ، فرض کنیم m مرتبهٔ گروه گالوای درجهٔ سوم حلال آن باشد .

(آ) اگر $m=6$ ، آنگاه $G\cong S_4$.

(ب) اگر $m=3$ ، آنگاه $G\cong A_4$.

(ج) اگر $m=1$ ، آنگاه $G\cong V$.

(د) اگر $m=2$ ، آنگاه $G\cong D_8$ یا $G\cong Z_4$.

تبصره: توجه کنید که در حالت مبهم (د) دو گروه ممکن ، دارای مراتب متفاوت می‌باشند. تمرین ۱۰۴ را ببینید .

برهان: دیدیم که $Q(u,v,w)$ میدان پایای $V\cap G$ می‌باشد. بنابر قضیهٔ اساسی،

$$|G/V\cap G|=[G:V\cap G]=[Q(u,v,w):Q]=|Gal(Q(u,v,w)/Q)|.$$

چون $f(x)$ تحویل‌ناپذیر است، بنابر تمرین ۸۴، G به طور تعدی بر ریشه‌های آن اثر می‌کند، بنابر این $|G|$ بوسیلهٔ ۴ عاد می‌شود (لم A10)، و قضیه از تمرینات ۹۷ و ۹۸ نتیجه می‌شود. □

مثالها :

۱. فرض کنیم $f(x)=x^4-4x+2\in Q[x]$، بنابر ضابطهٔ آیزنشتاین $f(x)$ تحویل‌ناپذیر است. درجهٔ سوم حلال $g(x)=x^3-8x+16$ می‌باشد. اکنون $g(x)$ تحویل‌ناپذیر است، زیرا اگر به هنگ ۵ تحویل شود، x^3+2x+1 به دست می‌آید، و این چند جمله‌ای بر Z_5 تحویل‌ناپذیر است، زیرا دارای هیچ ریشه‌ای نیست. مبین $g(x)$ برابر ۴۸۶۴- است، همچنین قضیهٔ ۷۸ نشان می‌دهد که گروه گالوای $g(x)$ با S_3 ایزومورف است،بنابر این از مرتبه ۶ است .

۲. فرض کنیم $f(x)=x^4-10x^2+1\in Q[x]$، بنابر تمرین ۶۷، $f(x)$ تحویل‌ناپذیر است. $x^3+20x^2+96x=x(x+8)(x+12)$ درجهٔ سوم حلال است. در این حالت، $Q(u,v,w)=Q$ و $m=1$. بنابر این $G\cong V$ (تعجبی ندارد به یادآوریم که $f(x)$ همانند چند جمله‌ای تحویل‌ناپذیر α، که $Q(\alpha)=Q(\sqrt{2},\sqrt{3})$ ناشی شود.)

تبصره : اگر d یک مقسوم علیه $|S_4|$ باشد، آنگاه می‌دانیم که S_4 دارای یک زیرگروه از مرتبهٔ d است. اگر $d=4$، آنگاه V و Z_4 زیرگروههای غیر ایزومورف از مرتبهٔ d می‌باشند. به ازای هر مقسوم علیه دیگر d، هر دو زیرگروه از مرتبهٔ d ایزومورف هستند. نتیجه می‌گیریم که گروه گالوای G از یک چند جمله‌ای درجهٔ چهارم بوسیلهٔ مرتبهٔ آن با یک ایزومورفیسم مشخص می‌شود، مگر $|G|=4$.

۹۹. گروه گالوای x^4+x^2-6 را بر Q محاسبه کنید.

۱۰۰. گروه گالوای x^4+x^2+1 را بر Q محاسبه کنید.

۱۰۱. گروه گالوای $4x^4+12x+9$ را بر Q محاسبه کنید.

۱۰۲. (آ) یک چند جمله‌ای درجهٔ پنجم بوسیلهٔ رادیکالها حل‌پذیر است اگر و فقط اگر گروه گالوای آن دارای مرتبهٔ کمتر یا مساوی ۲۴ باشد.

(ب) یک چند جمله‌ای درجهٔ پنجم تحویل‌ناپذیر بوسیلهٔ رادیکالها حل‌پذیر است اگر و فقط اگر گروه گالوای آن دارای مرتبهٔ کمتر یا مساوی ۲۰ باشد.

(راهنمایی: زیرگروه G از S_5 حل‌پذیر است اگر و فقط اگر $|G| \leq 24$، قضیهٔ A38 را ببینید.)

سه تمرین بعد از کاپلانسکی[1] (۱۹۷۲) می‌باشند.

۱۰۳. فرض کنیم $f(x) \in Q[x]$ یک درجهٔ چهارم تحویل‌ناپذیر با گروه گالوای G باشد، اگر $f(x)$ دارای دقیقاً دو ریشهٔ حقیقی باشد، آنگاه یا $G \cong S_4$ یا $G \cong D_8$.

۱۰۴. فرض کنیم x^4+ax^2+b یک چند جمله‌ای تحویل‌ناپذیر بر Q دارای گروه گالوای G باشد.

(آ) اگر b یک توان دوم در Q باشد، آنگاه $G \cong V$.

(ب) اگر b یک توان دوم در Q نباشد اما $b(a^2-4b)$ یک توان دوم باشد، آنگاه $G \cong Z_4$.

(ج) اگر b و $b(a^2-4b)$ در Q توان دوم نباشند، آنگاه $G \cong D_8$.

۱۰۵. فرض کنیم $x^4+bx^3+cx^2+bx+1 \in Q[x]$ دارای گروه گالوای G باشد.

---

1. Kaplansky.

(آ) اگر $h=c^2+4c+4-4b^2$ یک توان دوم در Q باشد ، آنگاه $G\cong V$.

(ب) اگر h یک توان دوم در Q نباشد، اما (b^2-4c+8)یک توان دوم باشد، آنگاه $G\cong Z_4$.

(ج) اگر h و $h(b^2-4c+8)$ توان دوم در Q نباشند، آنگاه $G\cong D_8$.

سخن آخر

مقدمه‌ای بر نظریهٔ گالوا را دیدید ، البته، مقدمهٔ بیشتری وجود دارد. مطالعهٔ عمیق‌تر میدانهای آبلی، یعنی، میدانهای دارای گروههای آبلی (احتمالاً نامتناهی)، با قضیه کومر[1] شروع می‌شود و به نظیهٔ میدان رده‌ای ادامه می‌یابد. گروههای گالوای نامتناهی توپولوژیکی می‌باشند، و یک تابع دو سویی بین میدانهای میانی و زیرگروههای بسته وجود دارد. قضایا از اهمیت بنیادی در نظریهٔ جبری اعداد برخوردارند. همچنین یک نظریهٔ گالوا که جبرهای تقسیم را رده‌بندی می‌کند [Jacobson (1956)] را ببینید) و یک نظریهٔ گالوا که حلقه‌های جابجایی را رده‌بندی می‌کند، وجود دارد. ([Chase,Harrison,Rosenberg] را ببینید) .

مشخص کردن گروههای متناهی مجرد G که می‌توانند به عنوان گروههای گالوا بر Q تحقق یابند یک مسأله باز جالب می‌باشد. (تمرین ۹۰ نشان می‌دهد که G معمولاً می‌تواند بر بعضی از میدانهای زمینه تحقق یابد). مثالهای خاص بسیاری شناخته شده‌اند. به عنوان مثال، گروههای متناوب و متقارن به عنوان گروههای گالوا می‌توانند بر Q تحقق یابند (یک برهان برای S_n در [Hadlock , p. 210] می‌توان یافت) ، برای یک برهان که کواترنیونها می‌توانند به عنوان گروه گالوا بر Q تحقق یابد،

---

1. **Kummer**

([R.A.Dean, Amer. Math. Monthly (1981) , pp.42-45] را ببینید، که نشان داده است گروه گالوای $x^8 - 72x^6 + 180x^4 - 144x^2 + 36$ می‌باشد). یک نتیجهٔ عمیق از شافارویچ[۱] (۱۹۵۴) است که هر گروه حل‌پذیر می‌تواند به عنوان یک گروه گالوا بر Q تحقق یابد. بعد از رده‌بندی گروههای سادهٔ متناهی در سال ۱۹۸۰ ، تلاشهایی برای تحقق یافتن آنها به عنوان گروههای گالوا بر Q ، با موفقیت بسیاری صورت گرفت. به هر حال، هنوز معلوم نیست که آیا هر گروه سادهٔ متناهی یک گروه گالوا بر Q می‌باشد.

نظریهٔ گالوا در متغیرهای مختلط وجود دارد.

([Miller,Blichfeldt,Dickson,chap.XX.p.378] را ببینید). در سال ۱۸۵۰ پوسیوکس[۲] گروه منودرامی[۳] یک ردهٔ مشخص از توابع $f(t,z)$ دو متغیرهٔ مختلط، مثلاً، $f(t,z)\in C(t)[z]$ را مطالعه کرد. در سال ۱۸۵۱ ، هرمیت نشان داد که این گروه منودرامی با گروه گالوای $f(t,z)$ بر میدان توابع $C(t)$ ایزومورف است.

نظریهٔ گالوا در معادلات دیفرانسیل ناشی از ریت[۴] و کولچین[۵] وجود دارد ([Kaplansky (1957)] را ببینید). مشتق‌گیری از میدان F یک هومورفیسم جمعی $D : F \longrightarrow F$ با $D(xy)=xD(y)+D(x)y$ است ، و دوتایی مرتب (F,D) میدان دیفرانسیل نامیده شده است. میدان دیفرانسیل (F,D) با توسیع F (احتمالاً نامتناهی) از C مفروض است ، گروه گالوای دیفرانسیل آن یک زیرگروه از $Gal(F/C)$ می‌باشد که شامل تمام σ هایی است که با D جابه جا می‌شوند. اگر این گروه به طور مناسب توپولوژیکی باشد و توسیع F/C در شرط مشابه توسیع گالوا صدق کند (توسیع پیکارد[۶]

---

1. Shafarevich **2. Puiseux** **3. Monodromy**

4. Ritt **5. Kolchin** **6. Picard**

– ویسوت[1] نامیده شده است)، آنگاه یک تابع دوسویی بین میدانهای دیفرانسیل میانی و زیرگروههای بستهٔ گروه گالوای دیفرانسیل وجود دارد.

نظریهٔ گالوا در توپولوژی جبری وجود دارد. فضای پوشش یک فضای توپولوژیکی X دوتایی مرتب $(\bar{X},p)$ است که $p: \bar{X} \longrightarrow X$ یک نوع خاص از نگاشتهای پیوسته است. اعضای گروه $\mathrm{Cov}\ (\bar{X}/X)$ همانند

$\{h: \bar{X} \longrightarrow X;\ ph = p$, یک همورفیسم است $h\}$ تعریف شده است و دوگان اعضای گروه گالوا در حالت زیر می‌باشد. اگر $i: F \longrightarrow E$ نگاشت شمول باشد ، که E/F یک توسیع گالوا است ، آنگاه اتومورفیسم σ از E در گروه گالوا قراردارد اگر و فقط اگر $\sigma i = i$. وقتی $\bar{X}$ همبند ساده است ، آنگاه $\mathrm{Cov}\ (\bar{X}/X) \cong \pi_1(X)$، که $\pi_1(X)$ گروه بنیادی X است ، بعلاوه، یک تابع دوسویی بین خانوادهٔ تمام فضاهای پوشش X و خانوادهٔ تمام زیرگروههای گروه بنیادی X وجود دارد.

من از نبوغ گالوا (۱۸۳۲ - ۱۸۱۱) هیبت زده هستم. او یکی از مسائل خارق‌العادهٔ ریاضی را در زمان خودش حل کرد، و حل او عالی است و همچنین در خلال کارهایش، دو نظریهٔ توانای، نظریهٔ گروه و نظریهٔ گالوا را خلق کرد. کار او هنوز دارای نفوذ و قدرت است. همهٔ این کارها را در سن ۱۹ سالگی انجام داد، و یک سال بعد کشته شد.

---

1. **Vessiot**

پیوست ۱ . واژه‌نامهٔ نظریهٔ گروه

گروه آبلی: یک گروه که در آن ضرب دارای خاصیت جابجایی است .

گروه متناوب A_n: زیرگروهی از S_n شامل تمام جایگشتهای زوج و از مرتبهٔ $\frac{n!}{2}$ است .

شرکت‌پذیری: به ازای هر z,y,x داشته باشیم $(xy)z=x(yz)$. از آن نتیجه می‌شود که پرانتزها برای هر سه عامل یا بیشتر لازم نیست .

اتومورفیسم: یک ایزومورفیسم از یک گروه به خودش می‌باشد .

جابجایی: برای هر x , y داشته باشیم $xy=yx$.

همدستهٔ H **در** G : یک زیرمجموعه از G به صورت $gH=\{gh;h\in H\}$ است که H یک زیرگروه از G است و $g\in G$. تمام همدسته‌های H گروه G را افراز می‌کنند، بعلاوه، $gH=g'H$ اگر و فقط اگر $g^{-1}g'\in H$.

گروه دوری: گروه G شامل عضو g (مولد نامیده شده است) است به طوری که هر عضو از G به صورت توانی از g می‌باشد .

گروه دو وجهی D_{2n}: یک گروه از مرتبهٔ $2n$ شامل یک عضو a از مرتبهٔ n و یک عضو b از مرتبهٔ ۲ است به طوری که $bab=a^{-1}$.

جایگشت زوج: جایگشتی که به صورت حاصلضرب یک تعداد زوج از ترانهش‌ها است. هر $r-$ دور به ازای r فرد ، یک جایگشت زوج است .

عامل‌گروههاازیک‌سری‌نرمال $G=G_0\supset G_1\supset\cdots\supset G_n=\{1\}$: گروههای $\frac{G_i}{G_{i+1}}$ می‌باشد .

گروه چهار V : یک زیرگروه نرمال از S_4 شامل عضو همانی و اعضای $(1,2)(3,4)$ و $(2,4)$ $(1,3)$ و $(2,3)$ $(1,4)$ می‌باشد .

یک مولد از گروه دوری G : عضو $g\in G$ که توانهای آن همهٔ اعضای G را

نتیجه می‌دهد، یک گروه دوری ممکن است دارای چند مولد متفاوت باشد .

گروه : مجموعهٔ G همراه با یک ضرب شرکت‌پذیر است به طوری که به ازای هر x از G یک عضو منحصر بفرد e از G موجود است که $ex=x=xe$ (e عضو همانی G نامیده‌می‌شود) و به‌ازای هر $x\in G$ یک‌عضومنحصربفرد y از G موجود است که $xy=yx=e$ (y وارون x نامیده می‌شود) . معمولاً عضو e با ۱ و عضو y با x^{-1} نشان داده می‌شوند .

هومومورفیسم: تابع $f : G \longrightarrow H$ است که G و H گروه می‌باشند ، به طوری که به ازای هر x و y از G ، $f(xy)=f(x)f(y)$. معمولاً f دارای این خاصیت است که $f(1)=1$ و $f(x^{-1})=f(x)^{-1}$.

تصویر هومومورفیسم $f:G \longrightarrow H$: زیرگروهی از H شامل همهٔ $f(x)$ ها به ازای هر $x\in G$ می‌باشد .

اندیس $[G : H]$: تعداد همدسته‌های زیرگروه H در G است و برابر $\frac{|G|}{|H|}$ می‌باشد .

ایزومورفیسم : یک هومومورفیسم دو سویی است .

هستهٔ هومومورفیسم $f : G \longrightarrow H$: یک زیرگروه نرمال از G شامل همهٔ اعضای x از G است که $f(x)=1$.

نگاشت طبیعی : اگر H یک زیرگروه نرمال از گروه G باشد ، آنگاه یک نگاشت طبیعی ، هومومورفیسم $\pi : G \longrightarrow \frac{G}{H}$ تعریف شده بوسیله $\pi(x)=xH$ می‌باشد .

سری‌نرمال از G : یک‌دنباله‌از زیرگروههای $G=G_0 \supset G \supset \cdots \supset G_n=\{1\}$ است که هر G_{i+1} در G_i نرمال است . (زیرگروه G_i ممکن است یک زیرگروه نرمال از G نباشد .)

زیرگروه‌نرمال: یک‌زیرگروه H از G است‌به‌طوری‌که‌به ازای هر g از G، $gHg^{-1}=H$.

مرتبهٔ عضو x از G : کوچکترین عدد صحیح و مثبت m، در صورت وجود، می‌باشد به‌طوری که $x^m = 1$، در غیراینصورت مرتبهٔ x نامتناهی است.

مرتبهٔ گروه G یعنی $|G|$: تعداد اعضای گروه G است.

p – گروه: یک گروه متناهی از مرتبهٔ توانی از عدد اول p است.

جایگشت : یک تابع دوسویی از یک مجموعه به خودش است، همهٔ جایگشتها تشکیل یک گروه تحت ترکیب توابع می‌دهند.

گروه خارج قسمتی G/H: اگر H یک زیر گروه نرمال از G باشد، خانوادهٔ تمام همدسته‌های gH از H با عمل ضرب تعریف شده بوسیلهٔ $gHg'H = gg'H$ گروه خارج قسمتی G/H است. مرتبهٔ G/H برابر $|G|/|H|$ است. عضو همانی آن $1H=H$ و معکوس gH عضو $g^{-1}H$ است.

گروه ساده G : یک گروه نابدیهی $(\neq\{1\})$ که تنها زیرگروههای نرمال آن $\{1\}$ و G می‌باشند.

گروه حل‌پذیر: یک گروه دارای یک سری نرمال با عاملهای خارج قسمتی آبلی است.

زیر گروه H از G: یک زیرمجموعه از G شامل ۱ است که تحت ضرب و معکوسها بسته است.

زیرگروه تولید شده بوسیلهٔ زیرمجموعهٔ X : کوچکترین زیرگروهی از G شامل X است، این زیرگروه شامل تمام حاصلضربهای $x_1^a\ x_2^b\ \dots\ x_n^z$ است که $x_i \in X$ و نماها ± 1 می‌باشند.

p – زیرگروه سیلوی G: یک زیرگروه از G از مرتبهٔ p^n است، که p^n بزرگترین توانی از p است که $|G|$ را عاد می‌کند. معمولاً چنین زیرگروههایی وجود دارند، و

هر دو چنین زیرگروهی مزوج می‌باشند ، بنابراین ایزومورف‌اند.

گروه متقارن S_n : گروه همهٔ جایگشتهای بر مجموعهٔ $\{1,2,...,n\}$ تحت ترکیب توابع است و از مرتبهٔ $n!$ می‌باشد .

پیوست ۲ . نظریه گروه استفاده شده در متن

فرض بر این است که تمام گروههای در این پیوست متناهی باشند حتی اگر چند تا از قضایا در حالت نامتناهی نیز برقرار باشند. تعاریف عبارات را در واژه‌نامه، پیوست ۱، می‌توان یافت.

قضیه A1 : هر زیرگروه S از یک گروه دوری $G = < a >$، دوری است.

برهان : اگر $S = \{1\}$ آنگاه S دوری با مولد ۱ است. در غیراین صورت فرض کنیم m کوچکترین عدد صحیح مثبتی باشد که $a^m \in S$، ادعا می‌کنیم که $S = < a^m >$. واضح است که $< a^m > \subset S$. برای عکس جزئیت، فرض کنیم $s=a^k \in S$. بنابر الگوریتم تقسیم اعداد صحیح q و r وجود دارند به طوری که $k = qm+r$ و $0 \leq r<m$. اما $a^k=a^{mq+r}=(a^m)^q a^r$ نتیجه می‌دهد که $a^r \in S$. اگر $r>0$، متناقض با مینیمال بودن m است، بنابراین $r = 0$ و $a^k=(a^m)^q \in <a^m>$. □

قضیه A2 : (آ) اگر $a \in G$ یک عضو از مرتبهٔ n باشد، آنگاه $a^m=1$ اگر و فقط اگر $n|m$.

(ب) اگر $G = < a >$ یک گروه دوری از مرتبهٔ n باشد، آنگاه a^k یک مولد G است اگر و فقط اگر $(k , n) = 1$.

برهان : (آ) الگوریتم تقسم اعداد صحیح q و r با $m=nq+r$ که $0 \leq r<n$ را فراهم می‌سازد. از آن نتیجه می‌شود که $a^r=a^{m-nq}=a^m a^{-nq}=1$. اگر $r>0$، در این صورت متناقض با این است که n کوچکترین عدد صحیح مثبت می‌باشد که $a^n=1$. بنابراین $r = 0$ و $n|m$.

(ب) به یاد داریم که دو عدد صحیح نسبت به هم اولند اگر و فقط اگر ترکیب خطی صحیحی از آنها برابر ۱ باشد.

اگر a^k مولد G باشد، آنگاه $a \in <a^k>$، بنابراین به ازای t ای از Z، $a=a^{kt}$

بنابراین $a^{kt-1}=1$ ، بنابر (آ) ، $n\,|\,kt-1$ ، لذا به ازای v ای از Z ، $nv=kt-1$ ، یعنی ، $(k,n)=1$.

بالعکس ، اگر $(k\ ,\ n)\ =\ 1$ ، آنگاه به ازای $t,u\in Z$ ، $nt+ku=1$ ، بنابراین $a=a^{nt+ku}=a^{nt}a^{ku}=a^{ku}\in<a^k>$. بنابراین هر توانی از a نیز در $<a^k>$ قراردارد و $G=<a^k>$. □

قضیه A3 : (لاگرانژ). اگر H زیرگروهی از G باشد، آنگاه $|G|=[G:H]|H|$.

برهان: همدسته‌های H در G گروه G را افراز می‌کنند . (نسبت $x\sim y$ ، تعریف شده بوسیلهٔ $y\ =\ xh$ به ازای h ای از H ، یک نسبت هم ارزی بر G است که کلاسهای هم ارزی همدسته‌های H می‌باشند.) بعلاوه به ازای هر x از G ، $|H|=|xH|$ (زیرا $h\longrightarrow xh$ یک دو سویی است) ، لذا $|G|$ برابر حاصلضرب تعداد همدسته‌ها در اندازهٔ مشترک آنها می‌باشد . □

از آن نتیجه می‌شود که $[G:H]=\dfrac{|G|}{|H|}$. بویژه ، اگر H یک زیرگروه نرمال از G باشد ، (به طوری که گروه خارج قسمتی G/H تعریف شده باشد) آنگاه $|G/H|=[G:H]=|G|/|H|$.

لم A4 : فرض کنیم $f\ :\ G\longrightarrow H$ یک همومورفیسم با هستهٔ K باشد . در این صورت f یک به یک است اگر و فقط اگر $K=\{1\}$.

برهان : اگر f یک به یک باشد ، آنگاه $x\neq 1$ نتیجه می‌دهد که $f(x)\neq f(1)=1$ ، و بنابر این $x\notin K$. بالعکس ، فرض کنیم $K=\{1\}$ و به ازای x و y از G ، $f(x)\ =\ f(y)$. در این صورت $1=f(x)f(y)^{-1}=f(x)f(y^{-1})=f(xy^{-1})$ و $xy^{-1}\in K=\{1\}$. بنابراین $x=y$ و f یک به یک است . □

اگر $f{:}G\longrightarrow H$ یک همومورفیسم باشد ، آنگاه تصویر f را با Imf و هستهٔ f را

با kerf نشان می‌دهیم .

قضیه A5 : (قضیهٔ اول ایزومورفیسم) . اگر $f : G \longrightarrow H$ یک هومورفیسم باشد، آنگاه kerf یک زیرگروه نرمال G است و $\frac{G}{\text{kerf}} \cong \text{Imf}$.

برهان : فرض کنیم $K=\text{kerf}$. نشان می‌دهیم K یک زیرگروه است . K شامل ۱ است (زیرا $f(1)=1$) . اگر $x,y \in K$ (به طوری که $f(x)=1=f(y)$) ، آنگاه $f(xy)=f(x)f(y)=1$ و $xy \in K$. اگر $x \in K$ ، آنگاه $f(x^{-1})=f(x)^{-1}=1$ و $x^{-1} \in K$.

بعلاوه ، زیرگروه K نرمال است : اگر $x \in K$ و $g \in G$ ، آنگاه $f(g\,x\,g^{-1})=f(g)f(x)f(g^{-1})=f(g)f(g^{-1})=1$ و بنابراین $gxg^{-1} \in K$.

نگاشت $\varphi : G/K \longrightarrow \text{Imf}$ را با ضابطهٔ $\varphi(xK)=f(x)$ تعریف می‌کنیم .

اکنون φ خوشتعریف است : زیرا اگر $x'K=xK$ ، آنگاه به ازای k ای از K ، $x'=xk$ و $f(x')=f(xk)=f(x)f(k)=f(x)$. بررسی اینکه φ یک هومورفیسم با $\text{Im}\varphi=\text{Imf}$ است ساده می‌باشد (زیرا f یک همورفیسم است). بالاخره ، بنابر لم A4 ، φ یک به یک است ، زیرا $\varphi(xK)=1$ نتیجه می‌دهد که $f(x)=1$ ، بنابراین $x \in K$ و $xK=K$. □

اگر H و K زیرگروههایی از G باشند ، آنگاه $K \vee H$ کوچکترین زیرگروه G شامل K و H است ، یعنی $K \vee H$ زیرگروه G تولید شده بوسیلهٔ $K \cup H$ است .

لم A6 : اگر H و K زیرگروههای G باشند و K در G نرمال باشد، آنگاه $K \vee H = KH = \{kh \;;\; k \in K \;,\; h \in H\} = HK$.

برهان : بوضوح $KH \subset K \vee H$. برای عکس جزئیت ، کافی است ثابت کنیم که KH یک زیرگروه است ، زیرا KH شامل $K \cup H$ است .

اکنون $khk_1h_1 = k(hk_1h^{-1})hh_1=(kk_2)(hh_1) \in KH$ به ازای k_2 ای از K (زیرا K نرمال است) . همچنین $(kh)^{-1}=h^{-1}k^{-1}=(h^{-1}k^{-1}h)h^{-1}=k'h^{-1} \in KH$ به

ازای k' ای از K (دوباره ، زیرا K نرمال است) . بنابراین KH یک زیرگروه است .

اگر $hk \in HK$ ، آنگاه به ازای k' ای از K ، $hk=(hkh^{-1})h=k'h \in KH$ ، و بنابر این $HK \subset KH$ ، عکس جزئیت به طریق مشابه اثبات می‌شود . □

اگر H و K زیرگروههایی از G باشند و K نرمال باشد ، آنگاه به سادگی دیده می‌شود که خانواده همدسته‌های hK از K با $h \in H$ یک زیرگروه از G/K است . در واقع با استفاده از لم A6 ، می‌توان بررسی کرد که این زیرگروه برابر KH/K می‌باشد .

قضیه A7 : (قضیهٔ دوم ایزومورفیسم) . اگر H و K زیرگروههای G باشند و K در G نرمال باشد . آنگاه $K \cap H$ یک زیرگروه نرمال H است و $\dfrac{H}{K \cap H} \cong \dfrac{KH}{K}$.

برهان : فرض کنیم $\pi : G \longrightarrow G/K$ یک نگاشت طبیعی تعریف شده بوسیلهٔ $\pi(x)=xK$ باشد ، و فرض کنیم $f : H \longrightarrow G/K$ تحدید $\pi|_H$ باشد . اکنون $\ker f = K \cap H$ و $\operatorname{Im} f$ خانوادهٔ تمام همدسته‌های xK در G/K با $x \in H$ است (بنابراین $\operatorname{Im} f = KH/K$) . اکنون از قضیهٔ اول ایزومورفیسم نتیجه به‌دست می‌آید . □

قضیه A8 : (قضیهٔ سوم ایزومورفیسم) . اگر S و K زیرگروههای نرمال G باشند و $S \subset K$ ، آنگاه K/S یک زیرگروه نرمال G/S است و $G/K \cong (G/S)/(K/S)$.

برهان : تابع $f : G/S \longrightarrow G/K$ تعریف شده بوسیلهٔ $f(xS) = xK$ خوشتعریف است ، زیرا $S \subset K$. بررسی اینکه f یک همومورفیسم پوشا با هستهٔ K/S است ساده می‌باشد، و لذا قضیه از قضیهٔ اول ایزومورفیسم نتیجه می‌شود . □

قضیه A9 : (قضیهٔ تناظر) . فرض کنیم K یک زیرگروه نرمال از G و S^* یک زیرگروه از $G^* = G/K$ باشد .

(آ) یک زیرگروه میانی منحصربفرد S ، یعنی $K \subset S \subset G$ ، با $S^* = \dfrac{S}{K}$ وجوددارد.

(ب) اگر S^* یک زیر گروه نرمال از G^* باشد ، آنگاه S در G نرمال است .

(ج) $[G^*:S^*]=[G:S]$.

(د) اگر T^* در S^* نرمال باشد ، آنگاه T در S نرمال است و $\frac{S^*}{T^*}\cong\frac{S}{T}$.

برهان: (آ) تعریف می‌کنیم $S=\{x\in G \,;\, xK\in S^*\}$.

(ب) اگر $a\in G$ و $x\in S$، آنگاه $axa^{-1}K=aKxK\,a^{-1}K\in S^*$ ، زیرا S^* در G^* نرمال است ، بنابر این $axa^{-1}\in S$.

(ج) $$[G^*:S^*]=\frac{|G^*|}{|S^*|}=\frac{|G/K|}{|S/K|}=\frac{|G|/|K|}{|S|/|K|}=|G|/|S|=[G:S]$$

(د) بنابر (ب) ، T در S نرمال است ، و بنابر قضیهٔ سوم ایزومورفیسم

$$S^*/T^*=(S/K)/(T/K)\cong S/T. \qquad \square$$

تعریف: گروه G بر مجموعهٔ X اثر می‌کند در صورتی که تابع $G\times X \longrightarrow X$ تعریف شده بوسیلهٔ $(g,x)=g.x$ موجود باشد، به طوری که

(آ) به ازای هر x از X ، $1.x=x$ ، که ۱ عضو همانی G است .

(ب) به ازای هر x از X و هر h,g از G ، $(gh).x=g.(h\,x)$.

تعریف: اگر G بر X اثر کند و $x\in X$، آنگاه $o(x)=\{gx \,;\, g\in G\}\subset X$ مدار x و $G_x=\{g\in G \,;\, g.x=x\}\subset G$ پایدارساز x می‌باشد.

گروه G به طور تعدی بر مجموعهٔ X اثر می‌کند، اگر به ازای هر x و y از X، g ای از G موجود باشد که $g.x=y$. در این حالت $o(x)=X$.

هر گروه G بوسیلهٔ تزویج بر خودش (در اینجا $X=G$) اثر می‌کند: تعریف می‌کنیم $g.x=gxg^{-1}$. مدار $o(x)$ از $x\in G$ ردهٔ مزدوجی $\{y\in G \,;\, y=gxg^{-1}\,,\ \exists g\in G\}$ از آن است. پایدار ساز x برابر $\{g\in G \,;\, x=g.x=g\,x\,g^{-1}\}=\{g\in G \,;\, g\,x=x\,g\}$ است(زیرگروه آخری مرکزساز x در G نامیده می‌شود و با $C_G(x)$ نشان داده می‌شود).

خواننده می‌تواند بررسی کند که خانواده تمام مدارها یک افراز X است، به ازای

نسبت $x\sim y$ بر X، تعریف شده بوسیلهٔ $y=g.x$ به ازای g ای از G یک نسبت هم ارزی است که رده‌های هم ارز مدارها هستند.

قضیه A10: اگر G بر مجموعهٔ X با $|X|=n$ اثر کند و اگر $x\in X$، آنگاه $|o(x)|=[G:G_x]$. بویژه، اگر G به طور تعدی بر X اثر کند، آنگاه $|G|=n|G_x|$.

برهان: $\varphi: o(x) \longrightarrow \{gG_x\ ;\ \text{است}\ G\ \text{در}\ G_x\ \text{یک همدستهٔ}\ gG_x\}$ را با $\varphi(g.x)=gG_x$ تعریف می‌کنیم. اکنون φ خوشتعریف است، زیرا اگر $g.x=h.x$ (که $g,h\in G$)، آنگاه $h^{-1}g.x=x$، لذا $h^{-1}g\in G_x$ و در نتیجه $gG_x=hG_x$. عکس این آرگومان نشان می‌دهد که φ یک به یک است: اگر $\varphi(g.x)=\varphi(h.x)$ آنگاه $gG_x=hG_x$، لذا $h^{-1}g\in G_x$ و $g.x=h.x$. بالاخره φ پوشاست، به ازای همدستهٔ gGx، $\varphi(g.x)=gG_x$ بنابراین، φ یک دو سویی است.

اگر G به طور تعدی بر X اثر کند، آنگاه $o(x)=X$ و $|o(x)|=n=|X|$، بنابراین، $n=[G:G_x]=|G|/|G_x|$ و $|G|=n|G_x|$. □

نتیجه A11: اگر $x\in G$، آنگاه تعداد مزدوجهای آن برابر $[G:C_G(x)]$ می‌باشد.

برهان: این حالت خاصی از G است که بر خودش بوسیلهٔ تزویج اثر کند. □

لم A12: اگر p یک عدد اول باشد که مقسوم علیه m نیست و $k\geq 1$، آنگاه p عاد نمی‌کند $\binom{p^km}{p^k}$ را.

برهان: ضریب دو جمله‌ای را همانند زیر می‌نویسیم:

$$\binom{p^km}{p^k}=\frac{p^km(p^km-1)\dots(p^km-i)\dots(p^km-p^k+1)}{p^k(p^k-1)\dots(p^k-i)\dots(p^k-p^k+1)}.$$

چون p عددی اول است، هر عامل p از صورت کسر (یا مخرج کسر) از یک

عامل از $p^k m-i$ (یا p^k-i) ناشی می‌شود . بزرگترین توانی از p مثلاً $p^{t(i)}$ که مقسوم‌علیه $p^k m-i$ است ، همان بزرگترین توانی از p است که مقسوم‌علیه p^k-i است (زیرا P مقسوم علیه m نیست) . هر عامل از p بالا بوسیلهٔ یک عامل از p پایین حذف شده است ، و لذا ضریب دو جمله‌ای دارای هیچ عامل p نیست . $\square$

قضیه A13 : (سیلو) . اگر G یک گروه از مرتبهٔ $p^k m$ باشد که p عددی اول است و مقسوم علیه m نیست ، آنگاه G شامل یک زیرگروه از مرتبهٔ p^k است .

برهان : (وایلنت[1]) . اگر X خانواده تمام زیرمجموعه‌های p^k عضوی از G باشد ، آنگاه لم A12 نشان می‌دهد که p عاد نمی‌کند $|X|$ را. فرض کنیم G بر X بوسیلهٔ انتقال چپ اثر کند : اگر $B \subset G$ و $|B|=p^k$ آنگاه $g.B=\{gb \; ; \; b\in B\}$. مداری مانند $o(B)$ موجود است که p عاد نمی‌کند $|o(B)|$ را (در غیراینصورت p کاردینال هر مدار را عاد می‌کند ، بنابراین $(p \,|\, |X|)$. چنین زیرمجموعهٔ B عضو X را انتخاب می‌کنیم. اکنون $|G|/|G_B|=[G:G_B]=|o(B)|$ نسبت به p اول است، از آن نتیجه می‌شود که $|G_B|=p^k m'\geq p^k$ به ازای m' ای که $m'|m$. از طرف دیگر ، اگر $b_0\in B$ و $g\in G_B$ ، آنگاه $gb_0\in g.B=B$ (تعریف پایدارساز) ، بعلاوه ، اگر h , g اعضای متمایز G_B باشند ، آنگاه gb_0 و hb_0 اعضای متمایز B می‌باشند . بنابراین $|G_B|\leq |B|=p^k$ ، و لذا G_B یک زیرگروه از مرتبهٔ p^k است . $\square$

تعریف : اگر $|G|=p^k m$ ، که p عددی اول است و مقسوم علیه m نیست ، آنگاه یک زیرگروه از G از مرتبهٔ p^k یک p- زیرگروه سیلوی G نامیده شده است .

می‌دانیم که هر دو p- زیرگروه سیلو از G ایزومورف‌اند (در واقع مزدوج

---

1. Wielandt

می‌باشند) ، و به ازای عددی صحیح مانند r ، $r \geq 0$ ، دقیقاً $1+rp$ تا از آنها وجود دارد .

نتیجه A14 : (کوشی) . اگر p عددی اول و مقسوم‌علیه $|G|$ باشد ، آنگاه G شامل عضوی از مرتبه p است .

برهان : فرض کنیم H یک p - زیرگروه سیلوی G باشد ، عضو $x \in H^{\#}=H-\{1\}$ را انتخاب می‌کنیم . بنابر قضیهٔ لاگرانژ ، به ازای t ای مرتبهٔ x برابر p^t می‌باشد . اگر $t=1$ حکم برقرار است ، اگر $t>1$ ، آنگاه دیدن اینکه $x^{p^{t-1}}$ از مرتبهٔ p می‌باشد ساده است . □

لم A15 : هر گروه آبلی متناهی $G \neq \{1\}$ شامل یک زیر گروه با اندیس اول است .

برهان : اثبات به استقراء بر k ، تعداد عاملهای اول $|G|$ (لزوماً متمایز نیستند) می‌باشد . اگر $k=1$ ، آنگاه G از مرتبهٔ اول و $\{1\}$ دارای اندیس اول است . فرض کنیم $k>1$. بنابر قضیهٔ کوشی، G شامل عضو x از مرتبهٔ اول است ، چون G آبلی است ، زیرگروه دوری H تولید شده بوسیلهٔ x نرمال است ، بنابر این گروه خارج قسمتی G/H تعریف شده است . بنابر استقراء G/H دارای زیرگروه S^* با اندیس اول است ، و قضیهٔ تناظر زیرگروه S از G با اندیس اول را نتیجه می‌دهد . □

قضیه A16 : گروه $G \neq \{1\}$ حل‌پذیر است (دارای یک سری نرمال با عاملهای آبلی است) اگر و فقط اگر G دارای یک سری نرمال با عاملهای از مرتبهٔ اول باشد .

برهان : کفایت بدیهی است . لزوم را بوسیلهٔ استقراء بر $|G|$ ثابت می‌کنیم. فرض کنیم که $G=G_0 \supset G_1 \supset \cdots \supset G_n=\{1\}$ یک سری نرمال با عاملهای آبلی G_i/G_{i+1} به ازای هر i باشد ، بعلاوه ، می‌توان فرض کرد که $G \neq G_1$. بنابر لم A15 ، گروه آبلی G/G_1 دارای یک زیرگروه (لزوماً نرمال) S^* با اندیس اول است ، قضیهٔ تناظر یک زیرگروه میانی S $(G_1 \subset S \subset G)$ با S نرمال در G و $[G:S]=[G/G_1 : S^*]$ اول را نتیجه می‌دهد. اکنون S یک گروه حل‌پذیر است (سری نرمال $S \supset G_1 \supset G_2 \supset \cdots \supset G_n=\{1\}$

را در نظر می‌گیریم ، S/G_1 آبلی است زیرا یک زیرگروه از گروه آبلی G/G_1 است) ، و استقراء یک سری نرمال با عاملهای از مرتبهٔ اول را فراهم می‌سازد . □

نتیجهٔ A17 : هر گروه حل‌پذیر دارای یک زیرگروه با اندیس اول است .

توجه داریم که جابجاگر دو عضو x و y از گروه G عبارتست از $[x,y]=x^{-1}y^{-1}xy$ زیرگروه جابجاگر G' از G زیر گروه تولید شده بوسیلهٔ تمام جابجاگرها می‌باشد (حاصلضرب دو جابجاگر ممکن است یک جابجاگر نباشد) . توجه کنید که G' یک زیرگروه نرمال G است ، زیرا اگر $a\in G$ ، آنگاه $a[x,y]a^{-1}=[axa^{-1},aya^{-1}]$ ، بعلاوه G/G' آبلی است .

لم A18 : اگر H یک زیرگروه نرمال از G باشد ، آنگاه G/H آبلی است اگر و فقط اگر $G'\subset H$.

برهان : اگر G/H آبلی باشد ، آنگاه به ازای هر x , y از G داریم $xyH=xHyH=yHxH=yxH$ و بنابر این $xyx^{-1}y^{-1}\in H$ ، از آن نتیجه می‌شود که $G'\subset H$.

بالعکس ، اگر $G'\subset H$ ، آنگاه قضیهٔ سوم ایزومورفیسم نشان می‌دهد که G/H یک گروه خارج قسمتی از گروه آبلی G/G' است ، لذا آبلی است . □

تعریف : زیرگروههای جابجاگر از درجهٔ بالاتر به طور استقرایی تعریف شده‌اند: $G^{(0)}=G$ ، $G^{(i+1)}=(G^{(i)})'$ ، یعنی $G^{(i+1)}$ زیرگروه جابجاگر $G^{(i)}$ است .

لم A19 : گروه G حل‌پذیر است اگر و فقط اگر به ازای n ای ، $G^{(n)}=\{1\}$.

برهان : اگر G حل‌پذیر باشد ، آنگاه یک سری نرمال $G=G_0\supset G_1\supset\cdots\supset G_n=\{1\}$ با عاملهای آبلی G_i/G_{i+1} موجود است . به استقراء بر i ، ثابت می‌کنیم که $G^{(i)}\subset G_i$ ، و از این ، نتیجه به‌دست می‌آید . اگر $i=0$ ، آنگاه $G_i=G_0=G$. به استقراء فرض کنیم که

$G^{(i)}\subset G_i$، در این صورت $G^{(i+1)}=(G^{(i)})'\subset G'_i$. اما آبلی بودن G_i/G_{i+1} بنابر لم A18، نتیجه می‌دهد که $G'_i\subset G_{i+1}$، و لذا $G^{(i+1)}\subset G_{i+1}$.

بالعکس، اگر $G^{(n)}=\{1\}$، آنگاه $G=G^{(0)}\supset G'\supset G^{(2)}\supset\cdots\supset G^{(n)}=\{1\}$ یک سری نرمال با عاملهای آبلی است، بنابراین G حل‌پذیر است. □

قضیه A20 : اگر G یک گروه حل‌پذیر باشد، آنگاه هر زیرگروه و هر گروه خارج قسمتی از G نیز حل‌پذیر است.

برهان : اگر H یک زیرگروه G باشد، آنگاه بوسیلهٔ استقراء اثبات اینکه به ازای هر i، $H^{(i)}\subset G^{(i)}$ ساده است. بنابر این از $G^{(n)}=\{1\}$ نتیجه می‌شود که $H^{(n)}=\{1\}$ و H حل‌پذیر است.

اگر $\varphi : G \longrightarrow K$ یک هومورفیسم پوشا باشد، آنگاه $\varphi(G')=K'$. اگر $uvu^{-1}v^{-1}$ یک جابجاگر در K باشد، اعضای x , y از G با $\varphi(x)=u$ و $\varphi(y)=v$ را انتخاب می‌کنیم، در این صورت $\varphi(xyx^{-1}y^{-1})=uvu^{-1}v^{-1}$. به استقراء، به سادگی ثابت می‌شود که به ازای هر i، $\varphi(G^{(i)})=K^{(i)}$. بنابر این اگر G حل‌پذیر باشد، آنگاه به ازای n ای $G^{(n)}=\{1\}$ و $K^{(n)}=\{1\}$، بنابر این K حل‌پذیر است. اکنون $K = G/N$ را اختیار می‌کنیم، که N زیرگروه نرمالی از G است، و φ را هومومورفیسم طبیعی $G \longrightarrow G/N$ اختیار می‌کنیم. □

قضیه A21 : فرض کنیم G یک گروه با زیرگروه نرمال H باشد. اگر H و G/H گروههایی حل‌پذیر باشند، آنگاه G حل‌پذیر است.

برهان : فرض کنیم $G/H=G^*=G_0^*\supset G^*_1\supset\cdots\supset G^*_m=\{1\}$ یک سری نرمال با عاملهای آبلی باشد. بنابر قضیهٔ تناظر سری نرمال $G=G_0\supset G_1\supset\cdots\supset G_m=H$ با هر G_i نرمال در G_{i-1} و هر عامل آبلی وجود دارد. چون H حل‌پذیر است، یک سری

نرمال $H=H_0\supset H_1\supset\cdots\supset H_n=\{1\}$ با عاملهای آبلی وجود دارد . از ترکیب این دو سری به یکدیگر یک سری نرمال برای G با عاملهای آبلی به‌دست می‌آید . □

تعریف : مرکز گروه G عبارتست از $Z(G)=\{g\in G\ ;\ g\,x=xg\ \forall x\in G\}$.

دیدن اینکه $Z(G)$ یک زیرگروه نرمال آبلی از G می‌باشد ساده است . همچنین ، $g\in Z(G)$ اگر و فقط اگر ردهٔ مزدوج g برابر $\{g\}$ باشد ، لذا $|Z(G)|$ تعداد رده‌های مزدوج با کاردینال ۱ می‌باشد .

گروههای G با $Z(G)=\{1\}$ وجود دارند ، به عنوان مثال ، $Z(S_3)=\{1\}$.

لم A22 : اگر p عددی اول و G یک $p-$گروه باشد ، آنگاه $Z(G)\neq\{1\}$.

برهان : گروه G را به رده‌های مزدوجی آن افراز می‌کنیم . با بکار بردن تبصرهٔ در مورد رده‌های مزدوجی با کاردینال ۱ ، اجتماع مجزای $G=Z(G)\cup C_1\cup\cdots\cup C_t$ وجود دارد که C_i ها رده‌های مزدوجی با کاردینال بزرگتر از ۱ می‌باشند . اگر $x_i\in C_i$ را انتخاب کنیم، آنگاه از نتیجهٔ A11 نتیجه می‌شود که $|G|=|Z(G)|+\sum[G:C_G(x_i)]$. بنابر قضیهٔ لاگرانژ به ازای هر i ، $[G:C_G(x_i)]$ بر p بخش‌پذیر است ، و بنابر این $p\,|\,|Z(G)|$. □

قضیه A23 : هر pـ گروه G حل‌پذیر است ، و اگر $G\neq\{1\}$ آنگاه G دارای یک زیرگروه با اندیس p است .

برهان : با استقراء بر $|G|$ ثابت می‌کنیم که G حل‌پذیر است . اگر $|G|\neq 1$ آنگاه بنابر لم A22، $Z(G)\neq\{1\}$. اگر $Z(G)=G$ آنگاه G آبلی است ، لذا حل‌پذیر است. اگر $Z(G)\neq G$ ، آنگاه $G/Z(G)$ یک pـ گروه از مرتبهٔ کمتر از $|G|$ است ، در این صورت بنابر استقراء حل‌پذیر است . چون $Z(G)$ بنابرآبلی بودن حل‌پذیراست ، قضیهٔ A21 نشان می‌دهد که G حل‌پذیر است . گزارهٔ دوم از نتیجهٔ A17 به دست می‌آید . □

فرض کنیم از گروههای مجرد به گروههای جایگشتی گذر کرده‌ایم . قضیهٔ کیلی

نشان می‌دهد که این از کلیت نمی‌کاهد .

به خاطر داریم که S_X گروه متقارن بر مجموعهٔ X ، مجموعهٔ تمام جایگشتهای (دو سویی‌های) بر X تحت ترکیب است . اگر $X=\{x_1 , x_2 , \cdots , x_n\}$ آنگاه یک ایزومورفیسم $S_X \longrightarrow S_n$ (مثلاً $\alpha \longrightarrow \theta\alpha\theta^{-1}$ ، که $\theta(x_i)=i$) و معمولاً این دو گروه همانند می‌شوند .

قضیه A24 : (کیلی). هر گروه G از مرتبهٔ n با یک زیرگروه از S_n ایزومورف است .

برهان : اگر $a\in G$ ، آنگاه تابع $\lambda_a:G \longrightarrow G$ تعریف شده بوسیلهٔ $\lambda_a(x) = ax$ یک دو سویی است ، و وارون آن $\lambda_{a^{-1}}(x)= a^{-1}x$ می‌باشد ، بنابر این $\lambda_a\in S_G\cong S_n$. $\lambda:G \longrightarrow S_G$ را بوسیلهٔ $\lambda(a)= \lambda_a$ تعریف می‌کنیم . باقی می‌ماند ثابت کنیم که λ یک همومورفیسم یک به یک است .

اگر $a,b\in G$ متمایز باشند ، آنگاه $\lambda_a\neq\lambda_b$ (زیرا دو تابع دارای مقادیر مختلف در $1\in G$ می‌باشند) . بالاخره ، λ یک همومورفیسم است : $\lambda_a\lambda_b(x)=\lambda_a(bx)=a(bx)$ و $\lambda_{ab}(x)=(ab)x$ ، بنابر این قانون شرکت‌پذیری نتیجه می‌دهد که $\lambda_{ab}=\lambda_a \lambda_b$ و این همان نتیجه مطلوب است . □

لم A25 : گروه متناوب A_n بوسیلهٔ دورهای به طول ۳ (۳ - دورها) تولید می‌شود .

برهان : اگر $\alpha\in A_n$ ، آنگاه $\alpha=\tau_1\tau_2\cdots\tau_m$ که هر τ_i یک ترانهش و m زوج است ، بنابر این $\alpha=(\tau_1\tau_2)(\tau_3\tau_4)\cdots(\tau_{m-1}\tau_m)$. اگر τ_{2k-1} و τ_{2k} متمایز نباشند ، آنگاه حاصلضرب آنها یعنی[1] $\tau_{2k-1}\tau_{2k}=(a,b)(a,c)=(a,c,b)$ یک ۳- دور است . اگر τ_{2k-1} , τ_{2k} متمایز

---

۱ - **ضرب جایگشتها را از راست به چپ انجام می‌دهیم** : $(\sigma\tau)(a)=\sigma(\tau(a))$ ، **یعنی** $\sigma\tau:a \longrightarrow \tau a \longrightarrow \sigma(\tau a)$. **بخصوص**، $(a,b)(a,c)=(a,c,b)$ **زیرا** $c \longrightarrow a \longrightarrow b$ و $b \longrightarrow b \longrightarrow a$ و $(a,b)(a,c):a \longrightarrow c \longrightarrow c$.

باشند ، آنگاه

$$\tau_{2k-1}\tau_{2k}=(a,b)(c,d)=(a,b)(b,c)(b,c)(c,d)=(b,c,a)(c,d,b)$$

بنابر این α حاصلضرب ۳- دورها می‌باشد . □

لم A26 : گروه متناوب A_n زیرگروه جابجاگر S_n می‌باشد .

برهان : چون S_n/A_n آبلی است (از مرتبهٔ ۲ می‌باشد) ، از لم A18 نتیجه می‌شود که $S'_n \subset A_n$. چون A_n بوسیلهٔ دورهای به طول ۳ تولید می‌شود ، کافی است ثابت کنیم که هر $\sigma=(i,j,k)$ یک جابجاگر است . اکنون $\sigma^{-1}=\sigma^2=(i,k,j)=(i,j)(i,k)$ ، به طوری که $\sigma=\sigma^4=(i,j)(i,k)(i,j)(i,k)$ ، یک جابجاگر است زیرا $(i,j)=(i,j)^{-1}$. □

لم A27 : اگر $\gamma=(i_0,i_1,\cdots,i_{k-1})$ یک k - دور در S_n باشد و $\alpha\in S_n$ ، آنگاه $\alpha\gamma\alpha^{-1}$ نیز یک k - دور است ، در واقع ، $\alpha\gamma\alpha^{-1}=(\alpha i_0 , \alpha i_1 , \cdots , a i_{k-1})$.

بالعکس ، اگر $\gamma'=(i'_0,i'_1,\cdots,i'_{k-1})$ یک k– دور دیگری باشد ، آنگاه α ای از S_n موجود است که $\gamma'=\alpha\gamma\alpha^{-1}$.

برهان : اگر $l\neq\alpha i_j$ ، $0\leq j\leq k-1$ ، آنگاه $\alpha^{-1}l\neq i_j$ و بنابر این $\gamma(\alpha^{-1}l)=\alpha^{-1}l$ ، لذا $\alpha\gamma\alpha^{-1}(l) = \alpha\gamma(\alpha^{-1}l)=\alpha(\alpha^{-1}l)=l$ ، یعنی $\alpha\gamma\alpha^{-1}$ ثابت نگه می‌دارد l را . اگر $l=\alpha i_j$ ، آنگاه $\alpha\gamma\alpha^{-1}(l)=\alpha\gamma(i_j)=\alpha(i_{j+1}) = \alpha i_{j+1}$ (زیرنویسها را به هنگ k تعبیر کنید) . بنابراین $\alpha\gamma\alpha^{-1}$ و $(\alpha i_0 , \alpha i_1, \cdots , \alpha i_{k-1})$ برابر می‌باشند .

بالعکس ، γ , γ' مفروض‌اند ، جایگشت α با $\alpha i_j=i'_j$ به ازای هر i انتخاب می‌کنیم . در این صورت قسمت اول برهان نشان می‌دهد که $\gamma'=\alpha\gamma\alpha^{-1}$. □

تبصره : لم ، با جایگذاری γ یک حاصلضرب از دورهای از هم جدا ، به جای γ یک دور است ، به‌روش مشابه ثابت می‌شود .

قضیه A28 : گروه متناوب A_n تنها زیرگروه S_n با اندیس ۲ است .

برهان : ابتدا نشان می‌دهیم که به ازای هر گروه G ، یک زیرگروه H با اندیس ۲ باید نرمال باشد . اگر $a\in G$ و $a\notin H$ ، آنگاه $aH\cap H=\varnothing$ ، و بنابر فرض $aH\cup H=G$ ، بنابراین aH مکمل H است . چون $aH\cap H=\varnothing$ ، از آن نتیجه می‌شود که $Ha\subset aH$. اکنون $a\notin H$ و $h\in H$ نتیجه می‌دهد که $ha=ah'$ به ازای h' ای از H ، و بنابراین $a^{-1}ha=h'\in H$ ، بنابراین H زیرگروه نرمال G است .

اگر $[S_n:H]=2$ ، آنگاه H در S_n نرمال است ، و لم A18 نتیجه می‌دهد که $A_n=S'_n\subset H$ (زیرا S_n/H از مرتبهٔ ۲ است ، بنابر این آبلی است) . اما $|H|=\frac{n!}{2}=|A_n|$ ، و لذا $H=A_n$. □

قصد داریم ثابت کنیم که A_5 یک گروه ساده است .

لم A29 : (آ) بیست ۳- دور در S_5 وجود دارند ، و همهٔ آنها در S_5 مزدوج می‌باشند .

(ب) همهٔ ۳- دورها در A_5 مزدوج می‌باشند .

برهان : (آ) تعداد ۳ - دورهای (a,b,c) برابر $20 = \frac{5\times4\times3}{3}$ می‌باشد . (چون $(a,b,c)=(b,c,a)=(c,a,b)$ بر ۳ تقسیم می‌شود) . بنابر لم A27 از مزدوج بودن هر دو ۳ - دور یک ۳ - دور دیگر نتیجه می‌شود .

(ب) ۳ - دورهای γ و γ' مفروض‌اند ، باید یک جایگشت زوج α با $\gamma'=\alpha\gamma\alpha^{-1}$ را پیداکنیم . این عمل را می‌توان به طور مستقیم انجام داد ، اما آن مستلزم در نظر گرفتن حالتهای مختلفی است ، در اینجا برهان دیگری ارائه می‌شود .

اگر $\alpha=(1,2,3)$ و $C_S(\alpha)$ مرکزساز α در S_5 باشد ، آنگاه از نتیجهٔ A11 به دست می‌آید $[S_5 : C_S(\alpha)] = 20$ ، بنابر این $|C_S(\alpha)|=6$. اما می‌توانیم شش عضو را که با α جابه‌جامی‌شوندنمایش دهیم : $1 ,\alpha , \alpha^2 , (4,5) , (4,5)\alpha , (4,5)\alpha^2$. تنها سه تای اولی از این جایگشتها زوج هستند، و بنابراین $|C_A(\alpha)|=3$ که $C_A(\alpha)$

مـــرکزساز α در A_5 است. بـنابر نـتیجهٔ A11 تـعداد مـزدوجهای α در A_5 بـرابـر $[A_5:C_A(\alpha)]=|A_5|/|C_A(\alpha)|=60/3=20$ می‌باشد. بـنابر ایـن هـمهٔ ۳- دورهـا بـا $\alpha=(1,2,3)$ در A_5 مزدوج می‌باشند. □

قضیه **A30** : A_5 یک گروه ساده است .

برهان: اگر $H\neq\{1\}$ یک زیرگروه نرمال از A_5 باشد و $\sigma\in H$، آنگاه هر مزدوج σ در A_5 نیز در H قراردارد. بویژه ، اگر H شامل یک ۳ - دور باشد ، آنگاه بنابر لم A29 (ب) شامل تمام ۳ - دورها می‌باشد ، در این صورت بنابر لم A25، $H = A_5$.

فرض کنیم $\sigma\in H$ و $\sigma\neq 1$. بعد از یک طبقه‌بندی ، مـی‌توانـیم فـرض کـنیم کـه $\sigma=(1,2,3)$ یا $\sigma=(1,2)(3,4)$ یا $\sigma=(1,2,3,4,5)$ (اینها تنها ساختار دورهای مـمکن از جایگشتهای (زوج) در A_5 می‌باشند). اگر $\sigma=(1,2,3)$، آنگاه $H=A_5$، همانطور که در بـالا مـلاحظه کـردیم . اگـر $\sigma=(1,2)(3,4)$، تـعریف مـی‌کنیم $\tau=(1,2)(3,5)$، آنگـاه $\tau\sigma\tau^{-1}=(\tau(1),\tau(2))(\tau(3),\tau(4))=(1,2)(4,5)$ و $\tau\sigma\tau^{-1}\sigma^{-1}=(3,4,5)\in H$.

بـــالاخره ، اگـــر $\sigma=(1,2,3,4,5)$، تـعریف مـــی‌کنیم $\tau=(1,3,2)$، در ایـــن صـــورت $\sigma\tau^{-1}\sigma^{-1}=(\sigma(1),\sigma(2),\sigma(3))=(2,3,4)$ و $\tau\sigma\tau^{-1}\sigma^{-1}=(1,3,4)$. در هر حالت ، H باید شامل یک ۳ - دور باشد. بنابر این، A_5 شامل هیچ زیرگروه نـرمال واقـعی غـیربدیهی نیست و لذا A_5 یک گروه ساده است . □

نتیجه **A31** : $\{1\}$ و A_5 و S_5 تنها زیرگروههای نرمال S_5 می‌باشند.

برهان : فرض کنیم $H\neq\{1\}$ یک زیرگروه نرمال S_5 باشد. از قضیهٔ دوم ایـزومورفیسم نتیجه می‌شود که $H\cap A_5$ یک زیرگروه نرمال A_5 است. چون A_5 یک گروه ساده است ، یا $H\cap A_5=A_5$ یا $H\cap A_5 = \{1\}$. در حالت اول ، $A_5\subset H$ و $H=A_5$ یا $H=S_5$. اگر $H\cap A_5=\{1\}$، ادعا مـی‌کنیم کـه $|H|=2$. اگـر بـه ازای h,k از H و α , β از A_5،

$h\alpha=k\beta$ ، آنگاه $k^{-1}h=\beta\alpha^{-1}\in H\cap A_5=\{1\}$ و $h=k$ و $\alpha=\beta$ ، بنابراین S_5 ، شامل $|A_5||H|=60|H|$ عضو متمایز است . اگر $h\in H$ و $h\neq 1$ ، آنگاه $h=(a,b)$ (تنها اعضای دیگر از مرتبهٔ ۲ به شکل $(a,b)(c,d)$ و جایگشتهای زوج می‌باشند) ، و یافتن یک مزدوج متمایز از h ساده است ، و این متناقض با نرمال بودن H می‌باشد . □

قضیه A32 : S_n به ازای $n\leq 4$ حل‌پذیر است ، اما به ازای $n\geq 5$ حل‌پذیر نیست .

برهان: اگر $m<n$ ، آنگاه S_m با یک زیر گروه از S_n ایزومورف است . چون هر زیر گروه از یک گروه حل‌پذیر خود حل‌پذیر است (قضیه A20) ، کافی است نشان دهیم که S_4 حل‌پذیر است و S_5 حل‌پذیر نیست. سری $\{1\}\subset V\subset A_4\subset S_4$ ، یک سری نرمال از S_4 است که دارای عاملهای آبلی است ، که در آن V گروه چهارکلاین است (گروههای خارج قسمتی به ترتیب از مرتبهٔ ۲،۳و۴ می‌باشند ، بنابر این آبلی می‌باشند) .

اگر S_5 حل‌پذیر باشد ، آنگاه زیرگروه A_5 از آن نیز حل‌پذیر خواهد بود . چون A_5 ساده است ، تنها سری نرمال آن $\{1\}\subset A_5$ است ، و تنها عامل خارج قسمتی آن گروه غیرآبلی $A_5/\{1\}\cong A_5$ است . □

اکنون تمرین ۹۷ را مطرح می‌کنیم ، اساس نظریهٔ گروه محاسبهٔ گروههای گالوای چند جمله‌ایهای درجهٔ چهارم تحویل‌ناپذیر بر Q می‌باشد .

قبل از هر چیز ، زیرگروههای G از S_4 که مرتبهٔ آنها مضربی از ۴ است را لیست می‌کنیم . $|G|=4, 8, 12, 24$. اگر $|G|=4$ ، آنگاه تنها گروههای مجرد G ، Z_4 و $Z_2\times Z_2$ می‌باشند ، و هر دو به عنوان زیرگروههایی از S_4 رخ می‌دهند (بویژه $V\cong Z_2\times Z_2$) . یک زیرگروه از مرتبهٔ ۸ ایزومورف با گروه دو وجهی D_8 وجود دارد، مثلاً ، تقارنهای یک مربع به عنوان جایگشتهای چهارکنج در نظر گرفته می‌شوند ، چون

یک زیرگروه از مرتبهٔ ۸ یک ۲ -زیرگروه سیلو از S_4 است ، همهٔ زیرگروههای از مرتبهٔ ۸ با D_8 ایزومورف می‌باشند . قضیه A28 نشان می‌دهد که A_4 تنها زیرگروه از مرتبهٔ ۱۲ است و البته خود S_4 تنها زیرگروه از مرتبهٔ ۲۴ است .

اگر $G \subset S_4$ و V گروه چهار باشد (که یک زیرگروه نرمال از S_4 است) ، آنگاه قضیه دوم ایزومورفیسم نتیجه می‌دهد که $G \cap V$ در G نرمال است و $G/G \cap V \cong GV/V \subset S_4/V$. تعریف می‌کنیم $m = |G/G \cap V|$ ، از آن نتیجه می‌شود که m یک مقسوم علیه $[S_4:V]=24/4=6$ است . ($S_4/V \cong S_3$، بررسی این حقیقت لازم نیست.)

قضیه A33 : (تمرین ۹۷). فرض کنیم $G \subset S_4$ از مرتبهٔ مضربی از ۴ باشد و فرض کنیم $m = |G/G \cap V|$. اگر $m=6$، آنگاه $G=S_4$. اگر $m=3$، آنگاه $G=A_4$.
اگر $m=1$، آنگاه $G=V$. اگر $m=2$، آنگاه $G \cong V$ یا $G \cong Z_4$ یا $G \cong D_8$.

برهان : اگر 3 یا $m=6$، آنگاه $|G| \geq 12$ ، ($|G|$ بر ۳ و بنابر فرض بر ۴ بخش‌پذیر است). بنابر قضیهٔ A28، A_4 تنها زیرگروه S_4 از مرتبهٔ ۱۲ است ، و بنابراین در هر حالت $A_4 \subset G$. اما $V \subset A_4$. به سادگی از آن نتیجه می‌شود که اگر $m=6$ ناگزیر $G=S_4$ و اگر $m=3$ ناگزیر $G=A_4$.

اگر $m=1$، آنگاه $G=G \cap V$ و $G \subset V$ ، چون $|G|$ مضربی از ۴ است ، از آن نتیجه می‌شود که $G=V$.

اگر $m=2$، آنگاه $|G|=2|G \cap V|$ ، چون $|V|=4$ ، داریم $|G \cap V|$ برابر ۱ یا ۲ یا ۴ می‌باشد . نمی‌توانیم داشته باشیم $|G \cap V|=1$ ، مگر آنکه $|G|=2$، که مضربی از ۴ نیست . اگر $|G \cap V|=4$ ، آنگاه $|G|=8$ و $G \cong D_8$ (در بالا ملاحظه کردیم که D_8 یک ۲- زیرگروه سیلو است) . اگر $|G \cap V|=2$ ، آنگاه $|G|=4$ و

$G \cong Z_4$ یا $G \cong V$ (اینها تنها گروههای مجرد از مرتبهٔ ۴ می‌باشند). □

احتمال $m=2$ و $G \cong V$ می‌توانند رخ دهد. فرض کنیم گروه $G=\{1, (1,2)(3,4), (1,2), (3,4)\}$ کپی ایزومورف با V در S_4 باشد. توجه کنید که $G \cap V=\{1,(1,2)(3,4)\}$ و $m=|G/G\cap V|=4/2=2$. گروه G به طور تعدی بر $\{1,2,3,4\}$ اثر نمی‌کند زیرا، به عنوان مثال، g ای از G با $g(1)=3$ وجود ندارد. تمرین ۹۸، برای حذف حالت $G \cong V$ از لیست‌انتخابها برای G وقتی که $m=2$، فرض اضافی G به طور تعدی اثر می‌کند را می‌گیرد.

لم A34: اگر G یک گروه و H یک زیرگروه با اندیس n باشد، آنگاه یک هومومورفیسم $\varphi:G \longrightarrow S_n$ با $\ker\varphi \subset H$ وجود دارد.

برهان: فرض کنیم X خانوادهٔ تمام همدسته‌های H در G باشد، چون $n=|X|$، دیدن اینکه $S_X \cong S_n$ ساده است (که S_X گروه تمام جایگشتهای بر X است). به ازای $g \in G$، $\varphi(g):X \longrightarrow X$ را با $\varphi(g)(aH)=gaH$ تعریف‌می‌کنیم(که $a \in G$)، توجه‌کنیم که $\varphi(g)$ یک‌دوسویی‌است، زیرا معکوس‌آن $\varphi(g^{-1})$ است. φ یک هومومورفیسم است، زیرا $\varphi(g)\varphi(g')(aH)=\varphi(g)(g'aH)=g(g'aH)$ و $\varphi(gg')(aH)=gg'(aH)$. اگر $\varphi(g)$ بر X همانی باشد، آنگاه به ازای هر a از G، $\varphi(g)(aH)=aH$، بویژه، $\varphi(g)(H)=H$، لذا $gH=H$ و $g \in H$. □

قضیه A35: A_6 دارای هیچ زیرگروهی با اندیس اول نیست.

برهان: معلوم شده است که A_6 یک گروه ساده از مرتبهٔ $360=2^3.3^2.5$ می‌باشد. اگر H یک زیر گروه نرمال با اندیس اول باشد، آنگاه $[A_6:H]$ برابر ۲ یا ۳ یا ۵ می‌باشد. بنابر لم A34، یک هومومورفیسم $\varphi:A_6 \longrightarrow S_n$ که $n=2$، 3 یا 5، با $\ker\varphi \subset H$ وجود دارد، بویژه، $\ker\varphi$ یک زیرگروه‌نرمال از A_6 با $\ker\varphi \neq A_6$ است. چون A_6

ساده‌است ، $\ker\varphi=\{1\}$ و φ یک به یک است . اما این غیرممکن است زیرا $|S_5|=120<360$. □

لم A36 : S_5 دارای هیچ زیرگروهی از مرتبهٔ ۳۰ یا از مرتبهٔ ۴۰ نیست .

برهان : فرض کنیم H یک زیرگروه از مرتبهٔ ۳۰ باشد ، یعنی H دارای اندیس $[S_5:H]=4$ باشد . از لم A34 یک همومورفیسم $\varphi:S_5\longrightarrow S_4$ با $\ker\varphi\subset H$ نتیجه می‌شود . اما $\ker\varphi$ یک زیرگروه نرمال S_5 است، و بنابراین مرتبهٔ آن باید ۱، ۶۰ یا ۱۲۰ باشد (نتیجهٔ A31) . چون $|H|=30$ ، از آن نتیجه می‌شود که $\ker\varphi=\{1\}$ ، و S_5 با یک زیرگروه از S_4 ایزومورف است ، و این یک تناقض است . آرگومان مشابه نشان می‌دهد که S_5 دارای هیچ زیرگروهی با اندیس ۳ نیست . □

قضیه A37 : اگر α یک ۵- دور در S_5 و τ یک ترانهش در S_5 باشد ، آنگاه $<\alpha,\tau>=S_5$.

برهان : فرض کنیم $H=<\alpha,\tau>$ زیرگروه تولید شده بوسیلهٔ α و τ باشد . می‌توانیم فرض کنیم که $\alpha=(1,2,3,4,5)$ و $\tau=(1,i)$. اکنون توانی از α، مثلاً ، α^k عضو i را به ۱ انتقال می‌دهد ، همچنین لم A27 نتیجه می‌دهد که به ازای j ای ، $\alpha^k(1,i)\alpha^{-k}=(j,1)$ (در حقیقت ، $j=\alpha^k 1$) . توجه کنیم که $i\neq j$ زیرا $(1,i)$ یک عامل متمایز از ۵ - دور α^k نیست. اما $(1,i)(1,j)=(1,j,i)$ یک عضو از مرتبهٔ ۳ است . مرتبهٔ H بر ۲ ، ۳ و ۵ بخش‌پذیر است ، بنابراین $|H|\geq 30$. بنابر لم A36 ، 120 یا $60 = |H|$. اگر $|H|=60$ ، آنگاه بنابر قضیهٔ A28 ، $H=A_5$ ، اما $H\neq A_5$ زیرا $\tau\in H$ یک جایگشت فرد است . بنابر این $H=S_5$. □

(محاسبهٔ بیشتر برهان نشان می‌دهد که ابتدا هر ترانهش می‌تواند از α و τ به دست آید ، و آنگاه S_5 بوسیلهٔ ترانهش‌ها تولید می‌شود .)

قضیه A38 : زیر گروه H از S_5 حل‌پذیر است اگر و فقط اگر $|H| \leq 24$.

برهان : این حقیقت که هر گروه از مرتبهٔ کمتر یا مساوی ۲۴ حل‌پذیر است را به خواننده واگذار می‌کنیم (خواه یک زیر گروه از S_5 باشد یا نباشد ، در حقیقت هر گروه از مرتبهٔ کمتر از ۶۰ حل‌پذیر است) .

چون $|S_5| = 120$ ، تنها مقسوم‌علیه‌های $|S_5|$ بزرگتر از ۲۴ عبارتند از ۳۰ , ۴۰ , ۶۰ , ۱۲۰ . اکنون بنابر قضیهٔ A32 ، خود S_5 حل‌پذیر نیست ، همچنین ، A_5 تنها زیرگروه از مرتبهٔ ۶۰ است (قضیه A28) ، و آن حل‌پذیر نیست زیرا ساده و غیرآبلی است (قضیه A30) . لم A36 برهان را کامل می‌کند . □

از قضیهٔ A38 در تمرین ۱۰۲ استفاده شده است . به طور ضمنی در قسمت دوم این تمرین است که S_5 دارای یک زیرگروه از مرتبه ۲۰ است ، نرمالساز یک ۵- زیرگروه سیلو چنین زیرگروهی می‌باشد . البته S_5 دارای یک زیرگروه حل‌پذیر از مرتبهٔ ۲۴ ، مثلاً، S_4 است .

پیوست ۳. ترسیم با خط‌کش و پرگار

می‌خواهیم نشان دهیم که حل مسائل کلاسیکی یونان : تربیع دایره ، تضعیف مکعب ، تثلیث یک زاویه غیرممکن می‌باشند. چنانکه خواهیم دید ، در این بحث تنها نظریهٔ میدان مقدماتی به‌کار می‌رود و نظریهٔ گالوا مورد نیاز نمی‌باشد.

بیان‌کردن مسائل به طور دقیق و موافق با قواعد زمینه ضروری می‌باشد. به عنوان مثال ، واضح است که یک زاویهٔ ۶۰ درجه را می‌توان با یک نقاله (یا هر وسیلهٔ اندازه‌گیری زاویه) تثلیث کرد ، در پایان، می‌توان هر عدد را بر ۳ تقسیم کرد. به هر حال مسائل یونان مشخص می‌کنند که تنها دو ابزار مجاز می‌باشند ، و هر یک باید تنها به یک روش مورد استفاده قرارگیرند. فرض کنیم P و Q دو نقطه در صفحه باشند، پاره خط با نقاط انتهایی P و Q را با PQ ، و طول این پاره خط را با $|PQ|$ نشان می‌دهیم. یک خط‌کش (یا چوب لبه صاف) وسیله‌ای است که می‌توان با آن خط $L(P,Q)$ مشخص شده بوسیلهٔ P و Q را رسم کرد ، یک پرگار وسیله‌ای است که با آن یک دایره به شعاع $|PQ|$ و مرکز P یا Q را رسم می‌کنیم. این دایره‌ها را به ترتیب با $C(P,Q)$ یا $C(Q,P)$ نشان می‌دهیم. چون هر ترسیم فقط دارای تعدادی متناهی مرحله است ، قادر خواهیم بود نقاط ساخت‌پذیر را به طور استقرایی تعریف کنیم .

یک صفحه مفروض است ، ابتدا بوسیلهٔ انتخاب دو نقطهٔ متمایز A و B ، یک دستگاه مختصات را بنا می‌کنیم ، خطی که بوسیلهٔ این نقاط مشخص می‌شود را محور x ها می‌نامیم. بوسیلهٔ یک پرگار دو دایره به شعاع $|AB|$ و به ترتیب با مراکز A و B رسم می‌کنیم. این دو دایره در دو نقطه متقاطع می‌باشند، و خطی که بوسیلهٔ این دو نقطه مشخص می‌شود ، عمود منصف AB است و محور yها نامیده شده است ، و محور xها را در نقطهٔ o ، که مبدأ نامیده شده است قطع می‌کند. فاصلهٔ $|0A|$ را برابر ۱ تعریف

مـی‌کنیم . بـه ایـن تـرتیب مـختصات را در یک صـفحه مـعرفی کـرده‌ایم ، بـویژه $A = (1,0)$ و $B = (-1,0)$.

تعریف: اگر X یک مجموعه از نقاط باشد ، آنگاه نقطهٔ Q بر X ، 0 - ساخت‌پذیر است اگر $Q \in X$ و نقطه Q بر X ، n - ساخت‌پذیر است اگر نقاط $P_1, P_2, \ldots, P_{n-1}$ موجود باشند به طوری که

(۱) هر P_i بر X ، $k(i)$- ساخت‌پذیر باشد ، که $k(i) < n$.

(۲) نقاط (نه لزوماً متمایز) E, F, G, H در $X \cup \{P_1, P_2, \ldots, P_{n-1}\}$ موجود باشند که یا

(آ) نقطهٔ Q تقاطع $L(E,F)$ و $L(G,H)$ باشد. یا

(ب) نقطه Q تقاطع $L(E,F)$ و $C(G,H)$ باشد. یا

(ج) نقطه Q تقاطع $C(E,F)$ و $C(G,H)$ باشد .

نـقطهٔ Q بـر X سـاخت‌پذیر است در صـورتی کـه بـر X بـه ازای n ای ، $n \geq 0$ ، n - ساخت‌پذیر باشد . بالاخره ، نـقطهٔ Q بـه طـور مـطلق سـاخت‌پذیر است اگـر بـر مجموعهٔ $X = \{A = (0,1)$ و $B = (-1,0)\}$ ساخت‌پذیر باشد .

اقلیدس ثابت کرد که هر پاره خط PQ می‌تواند نصف شود ، بنابر تعریف ، نقطهٔ میانی M بر $X = \{P,Q\}$ ساخت‌پذیر است . به هر حال ، واضح است که تنها تعدادی شما را نقاط مطلقاً ساخت‌پذیر وجود دارند (بـار دیگـر نـقاط A و B مـتمایز انـتخاب شده‌اند) .

در این بحث ، به طور آزاد هر نتیجهٔ استاندارد هندسهٔ اقلیدسی را به کار می‌بریم. بعلاوه ، عدد مختلط $z = x + iy$ را با نقطهٔ (x,y) همانند می‌کنیم ، بویژه می‌توانیم از اعداد مختلط ساخت‌پذیر و اعداد حقیقی ساخت‌پذیر صحبت کنیم .

لم B1 : نـقطهٔ $P = (x,y)$ سـاخت‌پذیر است اگـر و فـقط اگـر نـقاط $(x,0)$ و $(y,0)$

ساخت‌پذیر باشند. بنابر این، عدد مختلط $z=x+iy$ ساخت‌پذیر است اگر و فقط اگر قسمت حقیقی x از آن و قسمت موهومی y از آن ساخت‌پذیر باشند.

برهان : نقطهٔ $(x,0)$ ساخت‌پذیر است، زیرا تقاطع محور x ها و خط عمود مار بر P است، به طور مشابه، $(0,y)$ ساخت‌پذیر است. اما $(y,0)$ تقاطع محور x ها و دایرهٔ به شعاع y و مرکز مبدأ 0 است، بنابر این ساخت‌پذیر است.

بالعکس، فرض کنیم که $(x,0)$ و $(y,0)$ ساخت‌پذیر باشند. نقطهٔ $(0,y)$ ساخت‌پذیر است، تقاطع محور y ها و دایرهٔ به شعاع y و مرکز مبدأ است. می‌توان خط عمودی در $(x,0)$ و نیز خط افقی در $(0,y)$ را رسم کرد، و (x,y) تقاطع این خطوط می‌باشد. □

لم B2 : فرض کنیم K نمایش مجموعهٔ تمام اعداد ساخت‌پذیر باشد. در این صورت K یک زیرمیدان از C است اگر و فقط اگر $K \cap R$ یک زیرمیدان از R باشد. بعلاوه، اگر $K \cap R$ یک زیر میدان باشد که در آن اعضای مثبت دارای ریشه‌های دوم باشند، آنگاه K تحت ریشه‌های دوم بسته است.

برهان : لزوم واضح است.

بالعکس، فرض کنیم $K \cap R$ یک زیرمیدان از R باشد و $z=a+ib$ و $\omega=c+id$ اعضای K باشند. بنابر لم B1، $a,b,c,d \in K$. اکنون $z+\omega=a+c+i(b+d)$. بنابر فرض $a+c\ ,\ b+d \in K \cap R$، و نیز لم B1 نتیجه می‌دهد که $z+\omega \in K$. آرگومان مشابه نتیجه می‌دهد که $z\omega \in K$ و $z^{-1} \in K$.

فرض کنیم که $K \cap R$ یک زیر میدان باشد که اعضای آن دارای ریشه‌های دوم در $K \cap R$ باشند. اگر $z=x+iy \in K$ آنگاه $r^2=x^2+y^2 \in K \cap R$، و بنابر این $r \in K \cap R$. اکنون z را به صورت قطبی $z=re^{i\theta}$ می‌نویسیم. بنابر فرض نتیجه می‌شود که

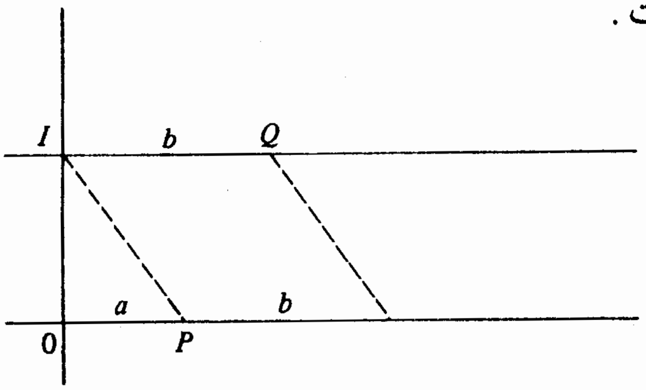
$\sqrt{r} \in K \cap R$، و $e^{i\theta/2}$ ساخت‌پذیر است زیرا هر زاویه می‌تواند نصف شود . □

قضیه B3 : مجموعهٔ تمام اعداد ساخت‌پذیر K یک زیر میدان از C است یعنی تحت ریشه‌های دوم بسته است .

برهان : کافی است که خواص $K \cap R$ را در لم B2 ثابت کنیم . فرض کنیم a و b اعداد حقیقی ساخت‌پذیر باشند .

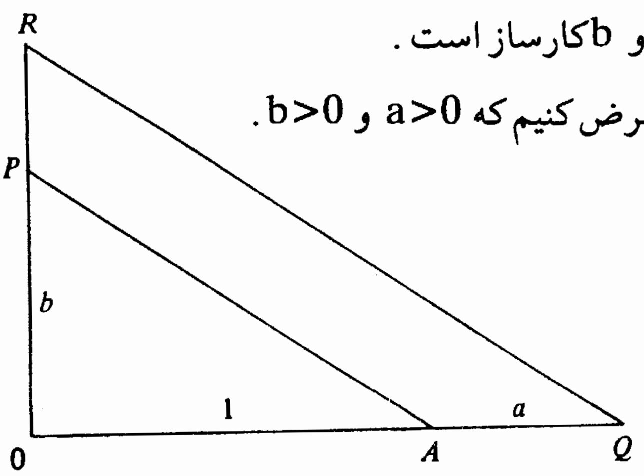
(آ) a − ساخت‌پذیر است . اگر $p=(a,0)$ یک نقطهٔ ساخت‌پذیر باشد ، آنگاه $(-a,0)$ تقاطع محور x ها و دایرهٔ $C(0,P)$ است .

(ب) $a+b$ ساخت‌پذیر است .



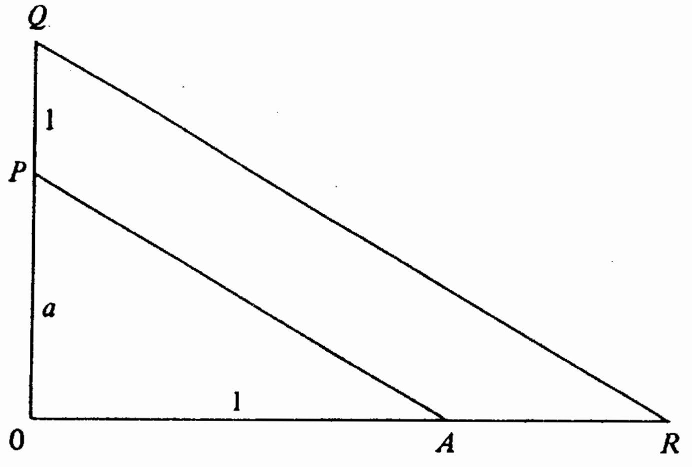
فرض کنیم $I=(0,1)$ و $p=(a,0)$ و $Q=(1,b)$ ، دیدن اینکه Q ساخت‌پذیر می‌باشد ساده است . خط ماربر Q موازی با IP محور x ها را در نقطهٔ $(a+b,0)$ قطع می‌کند ، و همان نتیجه مطلوب است. گرچه تصویر رسم شده با a و b مثبت است ، واضح است که این ترسیم برای هر انتخاب از علائم a و b کارساز است .

(ج) ab ساخت‌پذیر است . می‌توانیم فرض کنیم که $a>0$ و $b>0$.



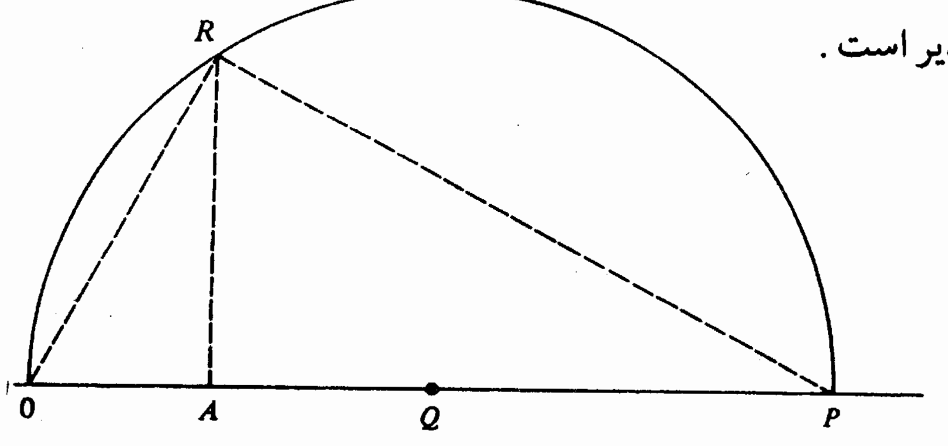
در این تصویر $A=(1,0)$ و $Q=(1+a,0)$ و $P=(0,b)$. تعریف می‌کنیم R تقاطع محور y ها و خط مار بر Q موازی با AP باشد. چون مثلثهای OAP و OQR متشابه‌اند لذا $|OQ|/|OA|=|OR|/|OP|$، بنابر این $(a+1)/1=(b+|PR|)/b$. از آن نتیجه می‌شود که $|PR|=ab$ و $(ab,0)$ ساخت‌پذیر است.

(د) a^{-1} ساخت‌پذیر است.



ترسیم همانند (ج) با یک تفاوت در انتخاب نقاط می‌باشد. فرض کنیم $A=(1,0)$ و $P=(0,a)$ و $Q=(0,1+a)$. نقطهٔ R را تقاطع محور xها و خط ماربر Q و موازی AP تعریف می‌کنیم. همانند (ج)، می‌توان تشابه مثلثها را برای به دست آوردن $|AR|=a^{-1}$ به‌کاربرد. بنابر این، $(a^{-1},0)$ ساخت‌پذیر است.

(هـ) $\sqrt{a}$ ساخت‌پذیر است.



فرض کنیم $A=(1,0)$ و $P=(1+a,0)$، Q نقطه وسط OP را رسم می‌کنیم. نقطهٔ R را تقاطع دایرهٔ $C(Q,0)$ با خط عمود ماربر A تعریف می‌کنیم. مثلثهای AOR و ARP متشابه‌اند، بنابر این $|OA|/|AR|=|AR|/|AP|$، و لذا $|AR|=\sqrt{a}$. □

چون هر زیر میدان از C شامل Q است، از آن نتیجه می‌شود که K شامل همهٔ نقاط (x,y) با مختصات گویا می‌باشد.

نتیجه B4 : اگر c,b,a ساخت‌پذیر باشند، آنگاه ریشه‌های چند جمله‌ای درجهٔ دوم ax^2+bx+c نیز ساخت‌پذیراند.

برهان : این از قضیه و فرمول درجهٔ دوم نتیجه می‌شود. □

به خاطر داریم که اگر E یک زیر میدان از C (لزوماً) شامل Q باشد، آنگاه E را می‌توان به عنوان یک فضای برداری بر Q در نظر گرفت، و بُعد آن بوسیلهٔ $[E:Q]$ نشان داده شد. اگر $z\in C$، آنگاه $Q(z)$ کوچکترین زیرمیدان C شامل z است.

لم B5 : فرض کنیم K یک زیر میدان C باشد.

(آ) خط با معادلهٔ $y=ax+b$ یا $x=b$ به ازای F , E از K به صورت $L(E,F)$ است اگر و فقط اگر $a,b\in K$.

(ب) دایرهٔ به معادلهٔ $(x-a)^2+(y-b)^2=c^2$ به ازای E , F از K به صورت $C(E,F)$ است اگر و فقط اگر $a,b,c\in K$.

برهان : اگر $E=(p,q)$ و $F=(s,t)$ در K باشند، آنگاه معادلات $L(E,F)$ و $C(E,F)$، اعداد c,b,a را برحسب جملاتی از ترکیبات گویا و ریشه‌های دوم t,s,q,p در K بیان می‌کنند. بالعکس، خط مفروض شامل نقاط $E=(0,b)$ و $F=(-\frac{b}{a}\ ,\ 0)$ از K می‌باشد (در حالت دوم، $E=(b,0)$ و $F=(b,1)$). دایرهٔ به معادلهٔ مفروض $C(E,F)$

است ، که $E=(a,b)$ و $F=(a,b+c)$. □

قضیه B6 : عدد مختلط z ساخت‌پذیر است اگر و فقط اگر یک برج از میدانهای $Q=K_0 \subset K_1 \subset \cdots \subset K_n$ موجود باشد که به ازای هر i ، $[K_{i+1}:K_i] \leq 2$ و $z \in K_n$.

برهان: اگر z ساخت‌پذیر باشد، یک دنباله از نقاط 1 , -1 , z_1 , z_2 , $\cdots$, $z=z_n$ موجود است که هر z_i از $\{1,-1,z_1,\cdots,z_{i-1}\}$ قابل حصول است . تعریف می‌کنیم $K_i=Q(z_1,\cdots,z_i)$. $u=z_{i+1}$ مفروض است ، نقاط H,G,F,E از K_i با یکی از $u=L(E,F) \cap L(G,H)$ ، $u \in L(E,F) \cap C(G,H)$ ، $u \in C(E,F) \cap C(G,H)$ وجود دارند. خواننده می‌تواند مختصات نقاط را از تقاطع ببیند و محاسبه کند، در حالت اول $u \in K_i$ ، در حالی که در دو حالت دیگر u یک ریشه از چند جمله‌ای درجهٔ دوم بر K_i است .

بالعکس ، یک برج از میدانها مفروض است ، به ازای هر i عضو u_i از K_i را با $K_{i+1}=K_i(u_{i+1})$ انتخاب می‌کنیم . به استقراء ، ثابت می‌کنیم که هر عضو از K_i ساخت‌پذیر است. آغاز استقراء به ازای $K_0=Q$ می‌باشد . اکنون هر عضو v از K_{i+1} یک ریشه از چند جمله‌ایی درجه دوم بر K_i است ، و بنابر این از نتیجه B4 به دست می‌آید که v ساخت‌پذیر است . □

نتیجه B7 : اگر عدد مختلط z ساخت‌پذیر باشد، آنگاه $[Q(z):Q]$ توانی از ۲ است .

برهان : این از قضیه و لم ۳۱ نتیجه می‌شود. □

تبصره : عکس این نتیجه نادرست است . به ازای هر $m \leq 2$ ، یک چند جمله‌ای $p(x)$ از $Q[x]$ از درجهٔ $n=2^m$ که دارای گروه گالوای $G=Gal(E/Q) \cong S_n$ می‌باشد وجود دارد. [Hadlock ، صفحهٔ ۲۱۸] را ببینید). به عنوان مثال ، در متن نشان دادیم که

$p(x)$ x^4-4x+2 بـر Q تـحویل‌ناپذیر و دارای گـروه گـالوای S_4 است . هـر ریشـه از $p(x)$ ساخت‌پذیر بود ، در این صـورت قـضیه $B3$ نـتیجه مـی‌دهد کـه هـر عـضو از E بـاید ساخت‌پذیر باشد. به هر حال ، اگر H یک ۲ − زیرگروه سیلوی G باشد، آنگاه $[G:H]$ یک عدد فرد است ، بنابراین میدان میانی E^H دارای درجهٔ فـرد $([E^H:Q]=[G:H])$ است و لذا هیچ یک از اعضای آن بنابر نتیجهٔ $B7$ ساخت‌پذیر نیستند . و این تناقض نشان می‌دهد که بعضی از ریشه‌های $p(x)$ ساخت‌پذیر نیستند (هنوز هر ریشه از درجهٔ 2^m بر Q است) .

اکنون یک موضوع ساده مرتب کردن بعضی از مسائل معروف است .

(۱) تربیع دایره غیرممکن است .

مسأله رسم کردن یک مربع که مساحت آن برابر مساحت یک دایره به شعاع یک است ، بوسیلهٔ خط‌کش و پرگار می‌باشد ، به عـبارتی دیگـر ، سؤال مـی‌شود آیـا $\sqrt{\pi}$ ساخت‌پذیر است . اما یک نتیجه کلاسیک آن است که π، و از این رو $\sqrt{\pi}$ بر Q متعالی است ([Hadlock صفحهٔ ۴۷] را ببینید) ، و بنابراین در هیچ توسیع متناهی از Q، که صرفاً از درجهٔ توانی از ۲ باشد قرار نمی‌گیرد .

(۲) تضعیف مکعب غیرممکن است .

مسأله ترسیم یک مکعب است که حجم آن ۲ می‌باشد ، به عبارتی دیگر ریشهٔ سوم ۲ که آن را α می‌نامیم ، ساخت‌پذیر است ؟ اکنون بنابر ضابطهٔ آیزنشتاین x^3-2، بر Q تحویل‌ناپذیر است ، و لذا $[Q(\alpha):Q]=3$، که توانی از ۲ نیست . حکم از نتیجهٔ $B7$ به دست می‌آید .

(۳) تثلیث یک زاویهٔ دلخواه غیرممکن است .

زاویهٔ θ با دو خط متقاطع مفروض است ، بدون کاستن از کلیت فرض کنیم کـه

خطوط در مبدأ متقاطع‌اند و یکی از این دو خط محور x ها می‌باشد. اگر بتوانیم ثلث کنندهٔ (سه بخش کنندهٔ) زاویه را رسم کنیم، آنگاه می‌توانیم نقطهٔ $(\cos\frac{\theta}{3}, \sin\frac{\theta}{3})$ را رسم کنیم که تقاطع ثلث کننده و دایرهٔ واحد است، لذا بنابر لم B1، $\cos\frac{\theta}{3}$ ساخت‌پذیر خواهد بود. اکنون بعضی از زاویا، مثلاً، $\theta=\frac{\pi}{2}$ می‌تواند تثلیث شود. از طرفی دیگر نشان خواهیم داد که زاویهٔ $\theta=\frac{\pi}{3}$ نمی‌تواند تثلیث شود. با محاسبهٔ قسمت حقیقی $e^{3i\theta}=(\cos\theta+i\sin\theta)^3$ اتحاد مثلثاتی $\cos3\theta=4\cos^3\theta-3\cos\theta$ نتیجه می‌شود. تعریف می‌کنیم $u=2\cos\theta$ و $\theta=\frac{\pi}{9}$، به معادلهٔ $u^3-3u-1=0$ می‌رسیم. دیدن اینکه این چند جمله‌ای درجهٔ سوم تحویل‌ناپذیر است ساده می‌باشد (دارای هیچ ریشهٔ گویا نیست، اکنون تمرین ۷۰ را بکار ببرید)، و لذا $[Q(u):Q]=3$. نتیجهٔ B7 نشان می‌دهد که u ساخت‌پذیر نمی‌باشد.

(۴) p ضلعی‌های منتظم

نظریه گالوا در طرح این مسأله به کار می‌رود.

قضیه B8 : (گاوس). اگر p یک عدد اول فرد باشد، آنگاه p ضلعی منتظم ساخت‌پذیر است اگر و فقط اگر به ازای t ای، $t\geq0$، $p=2^{2^t}+1$.

برهان : دوباره سؤال از ساخت‌پذیری یک نقطه بر دایرهٔ واحد، مثلاً، $z=e^{2\pi i/p}$ می‌باشد. اکنون چند جمله‌ای تحویل‌ناپذیر z بر Q چند جمله‌ای تقسیم دایرهٔ $\Phi_p(x)$ از درجهٔ $p-1$ است (نتیجهٔ ۲۵).

فرض کنیم z ساخت‌پذیر باشد. بنابر نتیجهٔ B7، به ازای s ای، $p-1=2^s$. ادعا می‌کنیم که s توانی از ۲ می‌باشد. در غیراین صورت، عدد فرد k با $s=km$ موجود است. اما x^k+1 بر Z تجزیه می‌شود (زیرا ۱− یک ریشهٔ آن است)، جایگذاری $x=2^m$ یک تجزیهٔ غیر مجاز برای p نتیجه می‌دهد.

بالعکس، فرض کنیم که $p=2^{2^t}+1$ اول باشد. چون z یک ریشهٔ p ام اولیهٔ

یکـــانی است ، $Q(z)$ مـــیدان شکـــافندهٔ $\Phi_p(x)$ بـــر Q است . بـــنابر ایـــن $|Gal(Q(z)/Q)|=2^{2^t}$ وگروه گالوا یک ۲ -گروه است . اما یک ۲ -گروه دارای یک سری نرمال است که هر عامل آن از مرتبهٔ ۲ می‌باشد (این به سادگی از قضیهٔ A23 نتیجه مـــی‌شود) ، بـــنابر قـــضیهٔ اســـاسی نـــظریهٔ گـــالوا ، یک بـــرج از مـــیدانـــهای $Q\subset K_1\subset\ldots\subset K_m=Q(z)$ وجود دارد که به ازای هر i ، $[K_{i+1}:K_i]=2$ ، یعنی z ساخت‌پذیر است . □

گاوس یک ترسیم هندسی از ۱۷ ضلعی منتظم را به طور واقعی ارائه داد .

تبصره : اعداد اول به فرم $2^{2^t}+1$ اول‌های فرما نامیده شده‌اند . مقادیر t ، $0\le t\le 4$ اعداد اول را نتیجه می‌دهند (آنها ۳ , ۵ , ۱۷ , ۲۵۷, ۶۵ , ۵۳۷ می‌باشند) ، مقادیر بعدی t اعداد اول را نتیجه نمی‌دهند ، و نامعلوم است که آیا اول‌های فرمای دیگری موجود است .

نتیجه B9 : ترسیم یک هفت ضلعی منتظم یا یک یازده ضلعی منتظم یا یک سیزده ضلعی منتظم غیرممکن است .

برهان : ۷ و ۱۱ و ۱۳ اول‌های فرما نیستند . □

نتیجهٔ زیر دانسته شده است ([صفحهٔ ۱۰۶ ، Hadlock] را ببینید) .

قضیه : یک n ضلعی منتظم ساخت‌پذیر است اگر و فقط اگر n به صورت حاصلضرب توانی از ۲ و اول‌های متمایز فرما باشد .

از آن نتیجه می‌شود که ۹ ضلعی منتظم و ۱۴ ضلعی منتظم ساخت‌پذیر نیستند، از طرفی دیگر یک ۱۵ ضلعی منتظم ساخت‌پذیر است .

پیوست ۴. سبک قدیم نظریهٔ گالوا

اگر آن خوبی شایستهٔ گالواست، آنگاه آن خوبی شایستهٔ من است!

«جیمی، کهنه کار نظریهٔ گالوا»

من مخلوق قرن بیستم هستم، دستگاههای جبری و گروههای اتومورفیسم آنها جزیی از شیر مادرم می‌باشند. هنگامی که تعریف گروه گالوا را برای این متن می‌نوشتم یک سؤال بدیهی کردم : در سال ۱۸۲۰ چگونه این تفکر برای گالوا رخ داد؟ البته، جواب این است که او فکر چنین مواقعی را نکرد، زیرا در قرن اول، ۱۹۳۰ - ۱۸۳۰، گروه گالوا یک گروه از جایگشتها بود. بعداً در سال ۱۹۲۰، امیل آرتین ایدهٔ امیل نوتر را گسترش داد و متعاقب آن به دِدکیند رسید و تصدیق کرد که توصیف گروههای گالوا بر حسب اتومورفیسمهای میدان، برازنده‌تر و مفیدتر است (نسخهٔ آرتین با نسخهٔ اصلی یکسان است). در سال ۱۹۳۰، واندر واردن[1] بسیاری از دیدگاههای آرتین را با متن با نفوذ و قدرت خود «جبر پیشرفته»، تلفیق کرد، و یک دههٔ بعد آرتین سخنرانیهایش را منتشر کرد. چنین موفق، با داشتن ایده‌های آرتین ثابت کرد که آنها دارای گرفتگی واقعی در ابتدای تفاسیر می‌باشند. اما انحراف اجتناب‌ناپذیر تعریف را داریم، نظریهٔ گروه مطالعهٔ چند جمله‌ایها را که بیشتر از صورت آن به طور طبیعی ناشی می‌شود تحمیل کرده است. این پیوست کوششی برای اصلاح مسألهٔ آموزش و پرورش به وسیله گفتن این داستان است که در ابتدا اتفاق افتاده است. خواننده می‌تواند [Edwards] یا [Tignol] را بخواند و با یک گزارش کاملتر علاقمند شود.

نمادها و جملات پیشرفته را به کار می‌بریم حتی اگر آنها در قرن هیجدهم

---

1. Van der Waerden .

ناشناخته باشند. بویژه F نمایش یک زیرمیدان از اعداد مختلط خواهد بود. جایگشتها با مسألهٔ یافتن ریشه‌های یک چند جمله‌ای به طور همزمان ناشی می‌شوند. اگر

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i) = x^n + b_{n-1}x^{n-1} + \dots + b_1 x + b_0$$

آنگاه‌به‌سادگی می‌بینیم که b_{n-j} هم علامت مجموع تمام حاصلضربهای j ریشهٔ α_iاست:

$$b_{n-j} = (-1)^j \sum_{1 \le i_1 < i_2 < \cdots < i_j \le n} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_j} .$$

بنابر این

$$b_{n-1} = -\Sigma\alpha_i = -(\alpha_1 + \alpha_2 + \cdots + \alpha_n)$$

$$b_{n-2} = \sum_{i<j} \alpha_i \alpha_j$$

$$b_{n-3} = \sum_{i<j<k} \alpha_i \alpha_j \alpha_k$$

$$\vdots$$

$$b_0 = (-1)^n \alpha_1 \alpha_2 \alpha_n .$$

چون ضرایب b_{n-j} تغییر نمی‌کنند اگر ریشه‌ها دوباره اندیسگذاری شوند، واضح است که آنها توابع متقارن از ریشه‌ها به معنی زیر می‌باشند.

تعریف: چند جمله‌ای $g(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ متقارن است اگر به ازای هر σ از S_n، $g(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) = g(x_1, \cdots, x_n)$.

هریک‌ازچندجمله‌ایهای $e_j(x_1, \cdots, x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_j \le n} x_{i_1} x_{i_2} \cdots x_{i_j}$ متقارن‌است،

$e_1, \dots, e_n$ توابع متقارن مقدماتی نامیده می‌شوند. توجه کنید که

$$e_j(\alpha_1, \dots, \alpha_n) = (-1)^j b_{n-j}.$$

نتیجهٔ زیر به خوبی شناخته شده است.

قضیهٔ اساسی توابع متقارن: اگر $g(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ متقارن باشد،

آنگاه $h(x_1, \cdots, x_n) \in F[x_1, \ldots, x_n]$ که لزوماً متقارن نیست موجود است ، به طوری که $g(x_1, \cdots, x_n) = h(e_1, \cdots, e_n)$.

برای برهان، [Hadlock صفحهٔ ۴۲] را ببینید. در سال ۱۷۷۰، وارینگ[1] یک الگوریتم برای یافتن h منتشر کرد. به عنوان مثال ،

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = e_1^2 - 2e_2$$

نتیجه : فرض کنیم $f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \in F[x]$ دارای ریشه‌های مختلط $\alpha_1, \cdots, \alpha_n$ باشد، اگر $g(x_1, \cdots, x_n) \in F[x_1, \ldots, x_n]$ متقارن باشد، آنگاه $g(\alpha_1, \cdots, \alpha_n) \in F$.

برهان : بنابر قضیهٔ اساسی، $h(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ موجود است که $g(x_1, \cdots, x_n) = h(e_1, \cdots, e_n)$. به طور معادل به ازای $(x_1, \cdots, x_n) = (\alpha_1, \cdots, \alpha_n)$ نتیجه می‌شود که $g(\alpha_1, \cdots, \alpha_n) = h(-b_{n-1}, \cdots, \pm b_0) \in F$. □

فرمولهای کلاسیکی برای چند جمله‌ایهای درجهٔ سوم و درجهٔ چهارم بیش از دو قرن پیش کشف و نیز به خوبی شناخته شده‌اند. توجه داریم که ریشه‌های $f(x) = x^3 + qx + r$ عبارتند از: $\alpha_1 = y + z$, $\alpha_2 = \omega y + \omega^2 z$, $\alpha_3 = \omega^2 y + \omega z$ (دراینجا، ω یک ریشهٔ سوم اولیهٔ یکانی است ، $y^3 = \frac{1}{2}(-r + \sqrt{R})$, $z^3 = \frac{1}{2}(-r - \sqrt{R})$, $R = r^2 + \frac{4q^3}{27}$). در سال ۱۷۷۰ ، لاگرانژ و واندرموند، به منظور یافتن پایهٔ اساسی فرمولهای شناخته شده به طور مستقل تحقیق کردند . و رادیکالها را برحسب ریشه‌های α_i بیان کردند : $3z = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3$, $3y = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$.

1. waring

به ازای α_1 , α_2 , α_3 داده شده و ریشهٔ سوم یکانی ζ (لزوماً اولیه نیست)، فرض کنیم $\psi(\zeta)=(\alpha_1+\zeta\,\alpha_2 + \zeta^2\alpha_3)^3$، دراین صورت $(3y)^3 = \psi(\omega)$, $(3z)^3=\psi(\omega^2)$ و به‌ازای $i = 1 , 2 , 3$، $\alpha_i = \frac{1}{3}\left[\sqrt[3]{\psi(\omega)} + \sqrt[3]{\psi(\omega^2)}\right]$، اگر یکی از ریشه‌های سوم به طور خاص انتخاب شود.

چگونه می‌توان دو عدد $\psi(\omega)$ و $\psi(\omega^2)$ را مشخص کرد؟ ریشه‌های $\alpha_3,\alpha_2,\alpha_1$ را به عنوان مجهولات در نظر می‌گیریم و تعریف می‌کنیم :

$\varphi_1(x_1 , x_2 , x_3) = x_1 + \omega x_2 + \omega^2 x_3$ و $\varphi_2(x_1 , x_2 , x_3) = x_1\, \omega^2 x_2 + \omega x_3$.

φ_1 , φ_2 متقارن نیستند. اما ترانهش $(2,3)$، φ_1 , φ_2 را با هم تعویض می‌کند (تحت ترانهش $(2,3)$ داریم $x_1 \longrightarrow x_1$ و $x_2 \longrightarrow x_3$ و $x_3 \longrightarrow x_2$) و ۳- دور $(1,3,2)$ هر دوی φ_1^3 و φ_2^3 را ثابت نگه می‌دارد (به عنوان مثال ، $(1,3,2)$، φ_1^3 را به $(x_3 + \omega x_1 + \omega^2 x_2)^3 = [\omega(\omega^2 x_3 + x_1 + \omega x_2)]^3 = \varphi_1^3$ می‌برد ، این یک دلیل برای درجهٔ سوم بودن φ_1 , φ_2 است). از آن نتیجه می‌شود که $\varphi_1^3 + \varphi_2^3$ و $\varphi_1^3\,\varphi_2^3$ توابع متقارن می‌باشند (هر یک تحت $(2,3)$ و $(1,3,2)$ پایا هستند و این دو جایگشت گروه متقارن S_3 را تولید می‌کنند). الگوریتم قضیهٔ اساسی توابع متقارن $\varphi_1^3 + \varphi_2^3$ و $\varphi_1^3\,\varphi_2^3$ را برحسب توابع متقارن مقدماتی بیان می‌کند . چون $\varphi_1(\alpha_1,\alpha_2,\alpha_3)^3 = \psi(\omega)$ و $\varphi_2(\alpha_1 , \alpha_2 , \alpha_3)^3 = \psi(\omega^2)$، نتیجهٔ قضیهٔ اساسی $b_1=\psi(\omega) + \psi(\omega^2)$ و $b_0=\psi(\omega)\psi(\omega^2)$ را بر حسب ضرایب q و r از $f(x)$ بیان می‌کند. قبلاً دیدیم که $\psi(\omega)$ و $\psi(\omega^2)$ معلوم‌اند ، می‌توانیم ریشه‌های $\alpha_3,\alpha_2,\alpha_1$ از $f(x)$ را پیداکنیم. اما $x^2 - b_1x + b_0 = (x - \psi(\omega))\ (x - \psi(\omega^2))$ و بنابر این $\psi(\omega)$ و $\psi(\omega^2)$ بوسیلهٔ فرمول درجهٔ دوم به دست می‌آیند. (بیشتر از چهار چند جمله‌ای به دست آمده از $\varphi_1(x_1,x_2,x_3)$ بوسیلهٔ جا به جا کردن متغیرها وجود دارند :

$\omega\varphi_1$ ، $\omega^2\varphi_1$ ، $\omega\varphi_2$ ، $\omega^2\varphi_2$. اینها ریشه‌های سوم دیگر $\psi(\omega)$ و $\psi(\omega^2)$ هستند ، و بنابر این از فرمول درجهٔ سوم به دست آمده‌اند وقتی که شرط $yz = -\frac{q}{3}$ اعمال شده است.)

لاگرانژ و واندرموند هر دو یک تحلیل مشابه از چند جمله‌ای درجهٔ چهارم کردند. اگر α_1 ، α_2 ، α_3 ، α_4 ریشه‌ها باشند ، در این صورت تعریف کردند که

$$\varphi_1(x_1 , x_2 , x_3 , x_4) = x_1 + ix_2 + i^2x_3 + i^3x_4$$

که $i^2 = -1$ ، و نشان دادند که $\varphi_1{}^4$ یک نقش قطعی در به دست آوردن فرمول کلاسیکی بازی می‌کند.

لاگرانژ این تحلیل را به چند جمله‌ایهای $f(x)$ از درجهٔ n تعمیم داد. اگر ζ یک ریشهٔ n ام یکانی (لزوماً اولیه نیست) باشد و اگر $\alpha_1 , \cdots , \alpha_n$ ریشه‌های $f(x)$ باشند ، ابتدا تعریف می‌کنیم

$$\varphi_1(\zeta) = \alpha_1 + \alpha_2\,\zeta + \alpha_3\zeta^2 + \cdots + \alpha_n\zeta^{n-1}$$

$$\varphi_2(\zeta) = \alpha_2 + \alpha_3\,\zeta + \alpha_4\zeta^2 + \cdots + \alpha_1\zeta^{n-1}$$

$$\varphi_n(\zeta) = \alpha_n + \alpha_1\,\zeta + \alpha_2\zeta^2 + \cdots + \alpha_{n-1}\zeta^{n-1}$$

و سپس تعریف می‌کنیم $\psi(\zeta) = \varphi_1(\zeta)^n$. البته می‌توانیم $\psi(1) = (\alpha_1 + \alpha_2 + \cdots + \alpha_n)^n$ را محاسبه کنیم زیرا مجموع α_iها ، علامت ضریب x^{n-1} در $f(x)$ است .

لم : اگر $f(x)$ از درجهٔ n باشد، آنگاه ریشه‌های $\alpha_1 , \cdots , \alpha_n$ از $f(x)$ بوسیلهٔ $n - 1$ عدد $\psi(\omega)$ ، $\psi(\omega^2)$ ، ، $\psi(\omega^{n-1})$ مشخص شده‌اند ، که ω یک ریشهٔ n ام اولیهٔ یکانی است .

برهان : به ازای k ثابت با $1 \leq k \leq n - 1$ ، داریم $\sum_{i=0}^{n-1} \omega^{kj} = 0$ (مجموع این سری

هندسی $0 = \frac{1 - (\omega^k)^n}{1-\omega^k}$ است زیرا $\omega^{kn} = 1 \quad , \quad (\omega^k \neq 1)$. لذا بنابر تبصرهٔ نخست

$$\sum_{j=0}^{n-1} \varphi_1(\omega^j) = \sum (\alpha_1 + \alpha_2\omega^j + \alpha_3\omega^{2j} + \cdots + \alpha_n\omega^{(n-1)j})$$
$$= n\,\alpha_1 + \alpha_2\,\Sigma\omega^j + \alpha_3\,\Sigma\omega^{2j} + \cdots + \alpha_n\Sigma\omega^{(n-1)j} = n\alpha_i$$

به طور مشابه ، $\sum_j \varphi_i(\omega^j) = n\alpha_i$. اگر $\psi(\omega^j) = \varphi_1\,(\omega^j)^n$ معلوم باشد ، آنگاه $\varphi_1(\omega^j)$ و نیز به ازای هر ریشه nام یکانی ζ ، $\zeta\varphi_1(\omega^j)$ معلوم است .

اما دیدن اینکه به ازای هر ζ ، $\varphi_i(\zeta) = \zeta^{-i-1}\,\varphi_1\,\zeta$ ساده است. بنابراین ریشه‌های $\alpha_1 , \alpha_2 , \cdots , \alpha_n$ ، بوسیلهٔ $\psi(\omega) , \psi(\omega^2) , \ldots , \psi(\omega^{n-1})$ مشخص شده‌اند. □

این لم ، به طور اساسی ناشی از بزوت[۱] (۱۷۶۵) می‌باشد ، که می‌گوید n ریشهٔ چند جمله‌ای f(x) از درجهٔ n می‌توانند برحسب $n - 1$ عدد $\psi(\omega) , \cdots , \psi(\omega^{n-1})$ یافت شوند ، یعنی، یک چند جمله‌ای از درجهٔ $n - 1$ ، مثلاً ، $\rho(x) = \prod (x - \psi(\omega^j))$ وجود دارد ، که ریشه‌های آن ریشه‌های f(x) را مشخص می‌کنند. آیا این یک گام استقراء برای یافتن ریشه‌های یک چند جمله‌ای از درجهٔ دلخواه n ارائه نمی‌دهد؟ متأسفانه ، جواب منفی است ، زیرا ضرایب $\rho(x)$[۲] را نمی‌دانیم. حداقل فرض ما این است که ضرایب در میدان F قرارگیرند ، و این دقیقاً گروهها را به نظریه معرفی می‌کند! ایدهٔ لاگرانژ $\rho(x)$ را بوسیلهٔ یک چند جمله‌ای قابل کنترل در F[x] جایگزین کرد.

عدد $\psi(\omega) = (\alpha_1 + \alpha_2\omega + \cdots + \alpha_n\omega^{n-1})^n$ در α متقارن نیست ، فرض کنیم به ناچار متقارن باشد. اگر $g(x_1 , x_2 , \cdots , x_n) \in F\,[x_1 , \cdots , x_n]$ و $\sigma \in S_n$ ، چند جمله‌ای σg را بوسیلهٔ $\sigma g(x_1 , \cdots , x_n) = g\,(x_{\sigma 1} , \cdots , x_{\sigma n})$ تعریف می‌کنیم ،

---

1. Bezout.

۲ - آرگومان مذکور را ارائه دادیم که این ضرایب شناخته شده‌اند وقتی که $n=3$.

متغیرها را تنها همانند σ جا به جا می‌کند. چند جمله‌ای متقارن شدهٔ $g^*(x) = \prod_{\sigma \in S_n} (x - \sigma g(x_1 , \cdots , x_n))$ را در نظر می‌گیریم، ضرایب آن به صورت $e(\sigma_1 g(x_1 , \cdots , x_n) , \cdots , \sigma_{n!}\, g(x_1 , \cdots , x_n))$ می‌باشند، که e یک تابع متقارن مقدماتی (از $n!$ جملهٔ $(\sigma g(x_1 , \cdots , x_n)$ است و جایگشتهای $\sigma_1 , \sigma_2 , \ldots , \sigma_{n!}$ در S_n لیست شده‌اند. اگر τ یک جایگشت دلخواه در S_n باشد ، آنگاه

$$e\ (\sigma_1 g\ (x_{\tau 1} , \cdots , x_{\tau n}) , \cdots , \sigma_{n!}\ g\ (x_{\tau 1} , \cdots , x_{\tau n}))$$
$$= e\ (\sigma_1 \tau g\ (x_1 , \cdots , x_n) , \cdots , \sigma_{n!} \tau g\ (x_1 , \cdots , x_n)).$$

چون σ_i بر تمام S_n تغییر می‌کند، لذا $\sigma_i \tau$ نیز بر تمام S_n تغییر می‌کند. تعویض x_i بوسیلهٔ τ منجر به تعویض مختصات آرگومان e می‌شوند ، چون e متقارن است ، از آن نتیجه می‌شود که ضرایب $g^*(x)$ در x_i متقارن می‌باشند. $(x_1 , \cdots , x_n)$ را بوسیلهٔ $(\alpha_1,\cdots,\alpha_n)$ جایگذاری می‌کنیم لذا بنابر نتیجهٔ قضیه اساسی توابع متقارن ، یک چند جمله‌ای برحسب x با ضرایب در F به دست می‌آید. اگر چه درجهٔ $g^*(x)$ بزرگ است ($n!$است) ، دارای یک خاصیت مهم است : هر یک از ریشه‌های $g(\alpha_1, \alpha_2, \cdots , \alpha_n)$ از آن بقیهٔ ریشه‌ها را مشخص می‌کند: به ازای $\sigma \in S_n$،

$$\sigma g(\alpha_1 , \cdots , \alpha_n) = g(\alpha_{\sigma 1} , \cdots , \alpha_{\sigma n})$$

بویژه $\psi(\omega) = (\alpha_1 + \alpha_2 \omega + \cdots + \alpha_n \omega^{n-1})^n$ را همانند یک تابع n متغیره در نظر می‌گیریم. در این صورت $\psi^*(x) = \prod_{\sigma} (x - \sigma \psi\ (x_1 , \ldots , x_n))$ یک چند جمله‌ای با ضرایب در $F(x_1, \ldots , x_n)$[1] است و با جایگذاری $(x_1 , \cdots , x_n)$ بوسیلهٔ $(\alpha_1 , \cdots , \alpha_n)$ یک چند جمله‌ای در $F[x]$ به دست می‌آید.

---

۱ - $F(x_1,\cdots,x_n)$ میدان کسرهای $F[x_1,\cdots,x_n]$ است، اعضای آن توابع گویای $a(x_1 , \ldots ,x_n)/b(x_1 , \ldots , x_n)$ است که $a,b \in F[x_1 , \ldots , x_n]$ ، $b \neq 0$.

$\psi(\omega)$ یکی از ریشه‌های $\psi^*(x)$ است. اکنون فرض کنیم که n اول باشد. اگر $1 \le j \le n-1$، آنگاه ω^j یک ریشهٔ nام اولیهٔ یکانی است، بنابر این ω^j , ω^{2j} , … , $\omega^{(n-1)j}$ یک جایگشت، مثلاً σ، از ω , $\omega 2$, …, ω^{n-1} است، و لذا $\psi(\omega^j) = \sigma\psi(\omega)$. از آن نتیجه می‌شود که $\psi(\omega)$, $\psi(\omega^2)$, … , $\psi(\omega^{n-1})$ ریشه‌های $\psi^*(x)$ می‌باشند. (به ازای هر j اگر j نسبت به n اول انتخاب شود آرگومان مشابه به کار می‌رود.)

اگر $g(x_1 , \cdots , x_n) \in F[x_1 , \cdots , x_n]$، آنگاه می‌توانیم $g^*(x)$ را بوسیلهٔ حذف تکرارها ساده کنیم: اگر $\sigma_i g = \sigma_k g$، یکی از آنها را نادیده می‌گیریم.

تعریف: چند جمله‌ای $g(x_1 , \cdots , x_n)$ را r مقداری[1] نامیم، که در آن $1 \le r \le n!$، در صورتی که دقیقاً r چند جمله‌ای متمایز به فرم σg به ازای $\sigma \in S_n$ موجود باشند.

بنابر این توابع یک مقداری توابع متقارن هستند، معمولاً مبین دو مقداری است. در حالتی از یک درجهٔ سوم، $\psi(x_1,x_2,x_3) = (x_1 + x_2\omega + x_3\omega^2)^3$ یک دو مقداری است و $g(x_1,x_2,x_3) = x_1$ سه مقداری است.

بوضوح، $\psi^*(x)$ باید بوسیلهٔ عامل درجهٔ rام $\lambda(x)$ از آن جایگزین شود، که $\lambda(x)$ از $\psi^*(x)$ بوسیلهٔ حذف عوامل تکراری به دست آمده است. (ψ، r مقداری است.) $\lambda(x)$ حلال لاگرانژ $f(x)$ نامیده شده است، این جایگذاری لاگرانژ برای چند جمله‌ای $\rho(x)$ از درجهٔ $n - 1$ است. چگونه می‌توانیم r را محاسبه کنیم؟

تعریف: اگر $g(x_1 , \cdots , x_n) \in F[x_1 , \cdots , x_n]$، آنگاه $G(g)= \{\sigma \in \Sigma_n ; \sigma g = g\}$.

لاگرانژ ادعا کرد (اما برهان او ناتمام است) که[2] $r = n!/|G(g)|$. بویژه، یک

---

۱ - این اصطلاح استاندارد است و در همهٔ منابع قدیمی‌تر واقع شده است. با استعمال پیشرفتهٔ آن هیچ ابهامی نیست که به عنوان مثال، رابطهٔ (نه تابع) $f(x) = \pm\sqrt{x}$ یک تابع دو مقداری است.

۲ - در اینجا یک برهان پیشرفته هست. گروه S_n بر $F[x_1,\ldots,x_n]$ بوسیلهٔ جا به جا کردن متغیرها

تابع $n!$ مقداری $g(x_1 , \dots , x_n)$ یک چند جمله‌ای با $G(g) = \{1\}$ است.

دو روش برای در نظر گرفتن یک جایگشت از n حرف وجود دارد. روش اول همانند یک کلمهٔ به طول n شامل حروف غیرتکراری است، روش دوم همانند یک دوسویی است. نسخهٔ اخیر ترکیب را طلب می‌کند: می‌توان حاصلضرب دو جایگشت را جایگشت سومی گرفت. باورکردنی به نظر می‌آید که لاگرانژ خبر نداشت که $G(g)$ یک زیرگروه S_n است، زیرا او جایگشتها را همانند کلمات در برهانش در نظر گرفته بود.

قضیه تابع گویای لاگرانژ: اگر[3] $g,h\in F[x_1,\cdots,x_n]$، آنگاه $G(h)\subset G(g)$ اگر و فقط اگر g یک تابع گویا از h باشد، یعنی، یک تابع گویای $\theta(x)\in F[x]$ با $g=\theta(h)$ موجود باشد.

نتیجه ۱: اگر $g , h \in F [x_1 , \cdots ,x_n]$، آنگاه $G(g) = G(h)$ اگر و فقط اگر هر یک از h , g توابع گویایی از دیگری باشد.

نتیجه ۲: اگر $h\in F[x_1,\cdots,x_n]$ یک تابع $n!$ مقداری باشد، آنگاه هر $g\in F[x_1,\dots,x_n]$ یک تابع گویا از h است.

نتیجه ۳: اگر $h\in F[x_1 , \cdots , x_n]$ یک تابع $n!$ مقداری باشد، آنگاه هر x_i یک تابع گویا از h است.

نتیجه ۴: (قضیهٔ عضو اولیه). اگر $\alpha_1 , \cdots , \alpha_n$ ریشه‌های $f(x)\in F[x]$ باشند، آنگاه η ای با $F(\alpha_1,\cdots,\alpha_n) = F (\eta)$ وجود دارد. بعلاوه، به ازای هر $i=1,\cdots,n$ توابع گویای $\theta_i(x)\in F[x]$ با $\alpha_i = \theta_i(\eta)$ وجود دارند.

برهان: فرض کنیم $h(x_1 , \cdots , x_n)\in F[x_1, \cdots ,x_n]$ یک تابع $n!$ مقداری باشد، به

عمل می‌کند، $G(g)$ پایدارساز g و r اندازهٔ مدار g می‌باشد. قضیهٔ A10 نتیجه می‌دهد که $r=[S_n:G(g)]=\frac{n!}{|G(g)|}$.

ازای هر i ، $g_i(x_1 , \cdots , x_n) \in F[x_1 , \ldots , x_n]$ را بوسیلهٔ $g_i(x_1 , \cdots , x_n)$ تعریف می‌کنیم. بنابر نتیجهٔ ۳ ، توابع گویای $\theta_i(x) \in F[x]$ وجوددارند به طوری که $x_i = g(x_1 , \cdots , x_n) = \theta_i(h(x_1 , \cdots , x_n))$. تعریف می‌کنیم $\eta = h(\sigma_1, \ldots, \sigma_n)$. □

می‌خواهیم این کار لاگرانژ را در سال ۱۷۷۰ خلاصه کنیم. چند جمله‌ای $f(x) \in F[x]$ از درجهٔ n یک چند جمله‌ای ψ از n متغیر را مشخص می‌کند . این چند جمله‌ای یک زیر گروه $G(\psi)$ از S_n را مشخص می‌کند ، از تقارن‌سازی ψ چند جمله‌ای $\psi^*(x) \in F[x]$ نتیجه می‌شود که برای یافتن ریشه‌های آن وقتی n یک عدد اول است ، کافی است ریشه‌های $f(x)$ را پیدا کنیم. با کنار گذاشتن ریشه‌های تکراری $\psi^*(x)$ حلال لاگرانژ $\lambda(x) \in F[x]$ یک چند جمله‌ای از درجهٔ r باقی می‌ماند.

لاگرانژ امیدوار بود که روش او می‌تواند چند جمله‌ای عمومی از درجهٔ n را حل کند. از طرف دیگر تحلیل او از یک درجهٔ پنجم ، او را به یک درجه ششم مهارنشدنی هدایت کرد ، بدون هیچ ابهامی روش یافتن یک ریشه او را دلسرد کرد.

این موضوع پیشرفت شصت سال از لاگرانژ تا گالوا بود. در سال ۱۸۰۳ ، گاوس ریشه‌های یکانی و چند جمله‌ایهای تقسیم دایره را تجزیه و تحلیل کرد (یک نتیجهٔ آن مشخص کردن چند ضلعی‌های منتظم ساخت‌پذیر بوسیلهٔ خط‌کش و پرگار است). رافینی (۱۷۹۹) و آبل (۱۸۲۴) به طور اساسی حل‌ناپذیری درجهٔ پنجم عمومی را ثابت کردند (هیچ یک از این دو برهان در تمام جزئیات درست نبودند ، اما برهان آبل پذیرفته شد و برهان رافینی پذیرفته نشد). در سال ۱۸۲۹ ، آبل ثابت کرد که چند جمله‌ایهای خاص $f(x)$ معمولاً بوسیلهٔ رادیکالها حل‌پذیر می‌باشند : اگر $\alpha_1 , \cdots , \alpha_n$ ریشه‌های $f(x)$ باشند ،و به ازای هر $i = 1 , \cdots , n$ توابع گویای $\theta_i(x)$ با $\alpha_i = \theta_i(\alpha_1)$ موجودباشند و به ازای هر i , j ، $\theta_i(\theta_j(\alpha_1)) = \theta_j(\theta_i(\alpha_1))$ (به زبان پیشرفته ، گروه گالوا آبلی است ، این

دلیل ریشه یابی صفت است) . (برای بحث بیشتر [Tignol ، صفحهٔ ۳۱۶] را ببینید.)

گرچه نظریهٔ گروه قبل از گالوا وجود نداشت ، برخی از نتایجی که امروزه می‌توانند به عنوان نظریه گروه دیده شوند موجود بودند . رافینی نشان داد که به ازای $r=3,4,8$ توابع r مقداری پنج متغیره‌ای وجود ندارند ، یعنی ، S_n زیرگروههایی با اندیس ۳ ، ۴ یا ۸ ندارد . آباتی[1] (۱۸۰۳) ثابت کرد که $|G(g)|$ به درستی $n!$ را عاد می‌کند ، به طوری که حکم لاگرانژ در مورد درجهٔ r صحیح است . بنابر این ، آباتی قضیهٔ لاگرانژ (قضیه A3) را برای زیر گروههای S_n ثابت کرد ، احتمالاً تمام قضیه در ابتدا بوسیلهٔ گالوا ثابت شده است . آباتی همچنین ثابت کرد : اگر $n \geq 5$ ، آنگاه S_n دارای هیچ زیرگروهی با اندیس ۳ یا ۴ نیست ، (قضیه A28) A_n تنها زیر گروه S_n با اندیس ۲ است . کوشی (۱۸۱۵) حساب جایگشتها ، مثلاً ، تجزیه به دورهای مجزا را بنا نهاد ، او ثابت کرد که ، به ازای عدد اول n ، S_n دارای هیچ زیر گروهی با اندیس r ، $2 < r \leq n$ نیست .

گالوا دانست که بعضی از چند جمله‌ایها بوسیلهٔ رادیکالها حل‌پذیر و بعضی حل‌پذیر نیستند ، و مستدل شد که آن به ریشه‌ها وابسته است . حلال لاگرانژ $\lambda(x)$ دارای این حساسیت نیست . در حقیقت ، به نظر می‌رسد که لاگرانژیک فرمول برای ریشه‌های چند جمله‌ای عمومی $x^n + b_{n-1} x^{n-1} + \cdots + b_0$ تحقیق کرده است : ریشه‌های هر چند جمله‌ای مشخص $f(x)$ از درجهٔ n از «فرمول کلی» و به وسیلهٔ جایگذاری ضرایب معین $f(x)$ به دست می‌آیند. (فرمولهای کلاسیکی چند جمله‌ایهای از درجهٔ کمتر یا مساوی ۴ به این صورت هستند.) اگر $f(x) \in F[x]$ دارای ریشه‌های $\alpha_1, \cdots, \alpha_n$ باشد ،

---

1. Abbati

لاگرانژ ابتدا α_1 , α_2 , $\cdots$, α_n را به عنوان مجهولات در نظر گرفت و سپس $\psi(x_1 , \cdots , x_n) = (x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{n-1} x_n)^n$ را تشکیل داد، با متقارن‌سازی $\psi^*(x_1 , \cdots , x_n) = \prod_{\sigma\in S_n} (x - \sigma\psi(x_1, \cdots , x_n))$ را به دست آورد، تعریف کرد $\lambda(x)$ عامل ψ^* از درجهٔ r برحسب x باشد که حاصلضرب تمام چند جمله‌ایهای متمایز $\sigma\psi$ است، و بالاخره $(x_1 , \cdots , x_n)$ را به $(\alpha_1, \cdots ,\alpha_n)$ قبلی تخصیص داد. اما، حتی اگر $\sigma\psi(x_1 , \cdots , x_n)$ و $\tau\psi(x_1 , \cdots , x_n)$ چند جمله‌ایهای متمایز باشند، بازهم ممکن است اتفاق بیافتد که $\tau\psi(\alpha_1, \cdots ,\alpha_n) = \sigma\psi(\alpha_1 , \cdots ,\alpha_n)$.
حلال لاگرانژ $\lambda(x) = (x;x_1,\cdots,x_n)$ به عنوان یک چند جمله‌ای بر $F(x_1 , \cdots , x_n)$ دارای ریشه‌های متمایز، به عنوان یک چند جمله‌ای بر F است، $\lambda(x) = \lambda(x;x_1,\cdots,x_n)$ ممکن است دارای ریشه‌های تکراری باشد. می‌توان این ریشه‌های اضافی را کنار گذاشت، اما متأسفانه، ممکن است که $\{\sigma\in S_n; (\sigma\psi) (\alpha_1, \cdots , \alpha_n) = \psi(\alpha_1 , \ldots , \alpha_n)\}$ زیرگروه S_n نباشد و این از درست بودن تعمیم قضیهٔ تابع گویای لاگرانژ جلوگیری می‌کند.

در خاتمه، گالوا $\psi(x_1 , \cdots , x_n)$ را کنار گذاشت، بهترین کار وقتی که درجه n اول است، او آن را بوسیلهٔ یک تابع n! مقدری $V(x_1 , \cdots , x_n)$ با یک خاصیت اضافی: همهٔ (σV) $(\alpha_1, \cdots , \alpha_n)$ها متمایزند جایگزین کرد (البته، این ناگزیر کرد که همهٔ α_iها متمایز باشند، این نقطهٔ کوچکتر به سادگی در تمرین ۴۱ به کار رفت). فرض کنیم (بعد از ادواردز) چنین تابع V را یک حلال گالوای[۱] f(x) بنامیم. گالوا ثابت کرد که چنین حلالهایی وجود دارند، و در حقیقت، به ازای c_1 , c_2 , $\cdots$, c_n مناسبی از F به صورت $V(x_1 , \ldots , x_n) = c_1 x_1 + c_2 x_2 + \ldots + c_n x_n$ می‌باشند $V(\alpha_1, \cdots ,\alpha_n)$ را

---

۱ - در حقیقت، من ترجیح می‌دهم که چند جمله‌ای $\gamma(x)$ زیر، چند جمله‌ای حلال گالوا نامیده شود، زیرا آن مشابه $\lambda(x)$ است در حالیکه V مشابه ψ است .

بـوسیلهٔ ν_1 نشـان مـی‌دهیم. چـون V یک تـابع !n مـقداری است ، تـوابـع گـویای $\theta_1(x),\cdots,\theta_n(x)$ در $F(x)$ وجود دارند به طوری که به ازای هر i ، $\alpha_i = \theta_i(\nu_1)$.

مرحله اول باید متقارن‌سازی V باشد : تعریف می‌کنیم

$V^*(x ; x_1 , \cdots , x_n) = \prod_{\sigma\in S_n} (x - \sigma V (x_1 , \cdots , x_n))$ ، و سپس یک عامل از V^* بوسیلهٔ حذف ریشه‌های تکراری انتخاب می‌کنیم .گالوا این را به طور غیرمستقیم انجام داد . فرض کنیم $\gamma(x)$ یک چند جمله‌ای تحویل‌ناپذیر از ν_1 بر F باشد ، و فـرض کـنیم $\nu_1,\cdots,\nu_m$ ریشه‌های $\gamma(x)$ باشند.

تمرین ۴۶ را یادآوری می‌کنیم : اگر $p(x) , h(x) \in F[x]$ چند جمله‌ایهایی دارای یک ریشهٔ مشترک باشند و $p(x)$ تحویل‌ناپذیر باشد ، آنگاه $p(x)$ عاد می‌کند $h(x)$ را. از آن یک بار نتیجه می‌شود که $\gamma(x)$ عاد می‌کند $V^*(x) = V^*(x; \alpha_1, \cdots , \alpha_n)$ را ، و نیز هـــر ریشـــهٔ ν_j از $\gamma(x)$ بـــه ازای جـــایگشتی مـــانند σ از S_n بـــه صـــورت $\sigma V(\alpha_1, \cdots ,\alpha_n)$ است. اما گـالوا بـه یک تـوصیف واضح‌تر از σ نـیاز داشت. ایـن یک تـعمیم سـاده از تـمرین ۴۶ مـی‌باشد: فـرض کـنیم $p(x)\in F[x]$ یک چـند جـمله‌ای تحویل‌ناپذیر باشد و فرض کنیم $\Phi(x)\in F(x)$ یک تابع گویا باشد، اگر به ازای ریشه‌ای مانند ν از $p(x)$ ، $\Phi(\nu) = 0$ ، آنگاه به ازای هر ریشهٔ ν' از $p(x)$ ، $\Phi(\nu')=0$.

گزاره: فرض کنیم $f(x)\in F[x]$ دارای ریشه‌های متمایز $\alpha_1 , \cdots , \alpha_n$ باشد ، فرض کنیم $\nu_1 , \cdots , \nu_m$ همانند بالا بـاشند ، و فـرض کـنیم $\alpha_i = \theta_i(\nu_1)$ ، کـه بـه ازای هـر i ، $\theta_i(x)\in F(x)$. در ایـن صـورت بـه ازای هـر $j=1 , \cdots , m$ ، تـابع $\sigma_j(\alpha_i) = \sigma_j(\theta_i(\nu_1)) = \theta_i(\nu_j)$ ، $i = 1 , \cdots , n$ ، یک جایگشت از ریشه‌های $\sigma_1 , \cdots , \sigma_n$ است .

بـــرهان : $\Phi(x) \in F(x)$ را بـوسیلهٔ $\Phi(x) = f(\theta_i(x))$ تـعریف مـی‌کنیم. اکـنون

$0 = f(\alpha_i) = f(\theta_i(\nu_1)) = \Phi(\nu_1)$، چون $\gamma(x)$ تحویل‌ناپذیر است، تعمیم تمرین ۴۶ نشان می‌دهد که $f(\theta_i(\nu_j)) = \Phi(\nu_j) = 0$، یعنی، $\theta_i(\nu_j)$ یک ریشهٔ $f(x)$ است، بنابر این یکی از α ها می‌باشد. برای دیدن اینکه σ_j یک جایگشت است، کافی است ثابت کنیم که یک تابع یک به یک است. فرض کنیم که $\theta_i(\nu_j) = \theta_k(\nu_j)$. اکنون $\Phi(x) = \theta_i(x) - \theta_k(x)$ یک تابع گویا با $\Phi(\nu_j) = 0$ است، از آن نتیجه می‌شود که $\alpha_i - \alpha_k = \theta_i(\nu_1) - \theta_k(\nu_1) = \Phi(\nu_1) = 0$. چون همهٔ ریشه‌های $f(x)$ متمایز هستند، $i = k$، و همان نتیجهٔ مطلوب است. □

گالوا، گروه گالوای چند جمله‌ای $f(x)$ را مانند $\mathrm{Gal}(f) = \{\sigma_j ; \sigma_j(\alpha_i) = \sigma_j(\theta_i(\nu_1)) = \theta_i(\nu_j)\}$ تعریف کرد. این شروع مقالهٔ گالوا در سال ۱۸۳۱ است، که او در آن چند جمله‌ایهای حل‌پذیر بوسیلهٔ رادیکالها را مانند چند جمله‌ایهای دارای گروه گالوا حل‌پذیر توصیف کرد. (به عنوان یک برهان که این تعریف معادل تعریف پیشرفته برحسب اتومورفیسمها می‌باشد، [Tignol صفحه ۳۲۹] را ببینید.)

نظریه گروه دقیق اثری در فضا بود، اما تنها گالوا مفهوم آنها را تشخیص و گسترش داد، او نظریهٔ گروه را ابداع کرد و معمای ریشه‌های چند جمله‌ایها را حل کرد. حتی این مؤثرتر است وقتی که تحقق می‌یابیم که این امر کمتر از پیدایش جبر پیشرفته نیست.

* * *

منابع

Artin , E., Galois Theory (second edition) , Notre Dame , 1955.

Burnside , W.S., and Panton , A.W., The Theory of Equations , vol. II, Long mans , Green , 1899.

Chase , S., Harrison , D., and Rosenberg , A., Galois Theory and Cohomology of commutative Rings, Mem . Amer. Math. Soc.,1965.

Dehn , E., Algebraic Equations , Columbia University Press , 1930.

Edwards , H.M., Galois Theory , Springer , 1984.

Gaal, L., Classical Galois Theory with Examples (fourth edition) , Chelsea , 1988.

Hadlock, C.R., Field Theory and Its Classical Problems, Math. Assn. Amer., 1978.

Jacobson , N., Structure of Rings, Amer. Math. Soc., 1956.

Jacobson, N., Basic Algebra I, Freeman , 1974.

Kaplansky, I., An Introduction to Differential Algebra, Hermann, 1957.

Kaplansky, I., Fields and Rings (second edition), University Chicago Press, 1974.

Miller, G.A., Blichfeldt , H.F., and Dickson, L.E., Theory and Applications of Finite Groups, Wiley, 1916 (Dover, 1961).

Netto, E., Theory of Substitutions, 1882, reprinted Chelsea, 1961.

Tignol, J.-p., Galois's Theory of Algebraic Equations, Wiley, 1988.

van der Waerden, B.L., Modern Algebra I, Ungar , 1953 .

van der Waerden, B.L., A History of Algebra, Springer, 1985.

واژه‌نامه انگلیسی به فارسی

Abelian	آبلی
Accessory	فرعی
... irrationalities	گنگ‌های فرعی
Act	عمل کردن
Acts transitively	به طور تعدی عمل می‌کند
Addition	جمع
Additive	جمعی
... group	گروه جمعی
Adjoin	الحاق کردن
Algebraic	جبری
... operations	اعمال جبری
... system	دستگاه جبری
Alternating	متناوب
... group	گروه متناوب
Argument	آرگومان
Associative	شرکت‌پذیری
Bijection	تابع دوسویی
Binary	دوتایی
... operation	عمل دوتایی

Binomial	دوجمله‌ای
... theorem	قضیه دوجمله‌ای
Biquadratic	دو مجذوری
Bound	کران
Cancellation	حذف
... law	قانون حذف
Cardinal	کاردینال - اصلی
... number	عدد اصلی
Center	مرکز
... of a group	مرکز گروه
Centralizer	مرکز ساز
Chain	زنجیر
Character	مشخص
Characteristic	مشخصه
Circle	دایره
Class	رده
Classical formula	فرمول کلاسیکی
Closure	بستار
Coefficient	ضریب
... of the polynomial	ضریب یک چند جمله‌ای
Commutative	جایجایی

... group	گروه جابجایی
... ring	حلقهٔ جابجایی
Commutator	جابجاگر
... subgroup	زیرگروه جابجاگر
Compass	پرگار
Complex	مختلط
... number	عدد مختلط
Component	مؤلفه
Composition	ترکیب
Congruence	همنهشتی
... class	ردهٔ همنهشتی
Conjugate	مزدوج
Conjugacy class	ردهٔ مزدوجی
Constant	ثابت
... term	جملهٔ ثابت
Constructible	ساخت‌پذیر - ساخته شدنی
... numbers	اعداد ساخت‌پذیر
Construction	ترسیم
Converse	عکس
Coordinates	مختصات
Corollary	نتیجه

Correspondence	تناظر
... theorem	قضیه تناظر
Contain	شامل بودن
Content	محتوا
Conteradiction	تناقض
Coset	همدسته
Criterion	ضابطه – محک
Cubic	درجهٔ سوم – مکعبی
... formula	فرمول درجهٔ سوم
Cub root of unity	ریشهٔ سوم یکانی
Cycle	دور
Cyclotomic	تقسیم دایره – دایره بُر
... polynomial	چند جمله‌ای تقسیم دایره
Decomposition	تجزیه
Degree	درجه
Denominator	مخرج کسر
Dependent	وابسته – وابستگی
Derivative	مشتق
Dihedral	دو وجهی
... group	گروه دو وجهی
Dimension	بعد

Direct product	حاصلضرب مستقیم
Discriminant	مبین
Disjoint	از هم جدا - متمایز
... union	اجتماع از هم جدا
Distributive	توزیع‌پذیری - پخشی
... Law	قانون توزیع‌پذیری
Division	تقسیم
... algorithm	الگوریتم تقسیم
Divisor	مقسوم علیه
Domain	حوزه - دامنه
Duplication	تضعیف - مضاعف کردن
Eisenstein's Criterion	ضابطهٔ آیزنشتاین
Element	عضو
Elementary	مقدماتی
... symmetric functions	توابع متقارن مقدماتی
Equation	معادله
Equivalence	هم ارزی
... class	ردهٔ هم ارزی
... relation	رابطهٔ هم ارزی
Equivalent	هم ارز - معادل
Evaluation	ارزیاب

... map	نگاشت ارزیاب
Extension	توسیع
... field	توسیع میدان
Factor	عامل
Factorization	تجزیه
Field	میدان
... of fractions	میدان کسرها
Finite	متناهی
... extension	توسیع متناهی
Fixed	ثابت - پایا
... field	میدان ثابت
Fraction	کسر
Function	تابع
Fundamental	اساسی
... theorem	قضیه اساسی
Generated by	تولید شده بوسیلهٔ
Generator	مولد
Greatest	بزرگترین
... common divisor	بزرگترین مقسوم علیه مشترک
... lower bound	بزرگترین کران پایین
Group	گروه

... of permutations	گروه جایگشتها
Homomorphism	همریختی
Ideal	ایده‌آل
Identity	همانی - خنثی
... element	عضو خنثی
Image	تصویر
Imbed	نشاندن
Inclusion	شمول - جزئیت
Independence	استقلال
... of characters	استقلال مشخصه‌ها
Independent	مستقل
Index	اندیس
Induction	استقراء
Infinite	نامتناهی
Insolvable	حل‌ناپذیر
Isomorphism	یکریختی - ایزومورفیسم
Integer	صحیح
... number	عدد صحیح
Intersetion	تقاطع - اشتراک
Intermediate	میانی
... field	میدان میانی

... subgroup	زیرگروه میانی
Inverse	عکس - وارون
Irrational	گنگ - اصم
Irreducible	تحویل‌ناپذیر
... polynomial	چند جمله‌ای تحویل‌ناپذیر
Kernel	هسته
Lattice	شبکه
Leading	پیشرو
... coefficient	ضریب پیشرو
Least	کوچکترین
... common multiple	کوچکترین مضرب مشترک
... upper bound	کوچکترین کران بالا
Lemma	لم
Linear	خطی
... combination	ترکیب خطی
... factors	عوامل خطی
Linealy disjoint	متمایز خطی - از هم جدای خطی
... independent	استقلال خطی
Map	نگاشت
Manageable	کنترل‌پذیر - قابل اداره
... polynomial	چندجمله‌ای کنترل‌پذیر

Maximal	ماکسیمال
... ideal	ایده‌ال ماکسیمال
Minimal	می‌نیمال
... polynomial	چند جمله‌ای می‌نیمال
Monic	تکین
... polynomial	چندجمله‌ای تکین
Multiplication	ضرب
Multiplicative	ضربی
... group	گروه ضربی
N - cycle	n - دور
Necessary	لازم
... codition	شرط لازم
Nonlinear	غیرخطی
Nontrivial	غیربدیهی
... subgroup	زیرگروه غیر بدیهی
Nonzero	ناصفر - غیر صفر
Norm	نرم
Normal	نرمال
... closure	بستار نرمال
... extension	توسیع نرمال
... series	سری نرمال

Normalizer	نرمالساز
Numerator	صورت کسر
Orbit	مدار
Order	مرتبه – ترتیب
... reversing	معکوس کنندهٔ ترتیب
... reversing bijection	دوسویی معکوس کنندهٔ ترتیب
Origin	مبدأ
Partially ordered set	مجموعهٔ به طور جزئی مرتب
Perfect	کامل
Permutation	جایگشت
Perpendicular	متعامد
... bisector	عمود منصف
Point wise	نقطه‌ای
... operations	اعمال نقطه‌ای
Polynomial	چند جمله‌ای
... ring	حلقهٔ چند جمله‌ایها
Prime	اول
... field	میدان اول
... ideal	ایده‌ال اول
Primitive	اولیه
... element	عضو اولیه

... polynomial	چند جمله‌ای اولیه
... roots of unity	ریشه‌های اولیهٔ یکانی
Principal	اصلی
... ideal	ایده‌آل اصلی
... ideal domain	دامنهٔ ایده‌ال اصلی
Protractor	نقاله
Pure	محض
... extention	توسیع محض
Quadratic	درجهٔ دوم
... formula	فرمول درجهٔ دوم
... polynomial	چند جمله‌ای درجهٔ دوم
Quartic	درجهٔ چهارم
... formula	فرمول درجهٔ چهارم
Quintic	درجهٔ پنجم
... formula	فرمول درجهٔ پنجم
Quotient	خارج قسمت
... ring	حلقهٔ خارج قسمت
... group	گروه خارج قسمت
Radical	رادیکال
... extension	توسیع رادیکال
Radius	شعاع

Range	برد
Rational	گویا
... function	تابع گویا
Real	حقیقی
... root	ریشهٔ حقیقی
Reduced	تحویل شده - تقلیل یافته
Regular	منتظم
... n - gon	n ضلعی منتظم
Relation	رابطه
Remark	تبصره
Remainder	باقیمانده
Repeated	تکراری
... root	ریشهٔ تکراری
Resolvent	حلال
... cubic	درجهٔ سوم حلال
Restriction	تحدید
Ring	حلقه
... homomorphism	همریختی حلقه
Root	ریشه
R - valued	r - مقداری
Separable	جداپذیر
... Polynomial	چند جمله‌ای جداپذیر

Sequence	دنباله
Set	مجموعه
Simple	ساده
... extension	توسیع ساده
Solution	حل
Solvable	حل‌پذیر
... group	گروه حل‌پذیر
... by radical	بوسیلهٔ رادیکال حل‌پذیر
Span	تولید کردن
Split	شکافتن - از هم جدا شدن
... closure	بستار تجزیه
Spliting field	میدان شکافنده
Square	مربع
... free	مربع آزاد
Squaring the circle	تربیع دایره
Stabilizer	پایدار ساز
Subgroup	زیرگروه
Subfield	زیرمیدان
subring	زیرحلقه
Subtract	تفریق
Sufficient	کافی
... condition	شرط کافی

Symmetric	متقارن
... function	تابع متقارن
... group S_n	گروه متقارن S_n
System	دستگاه
Theorem	قضیه
Tower	برج
Transcendental	غیرجبری - متعالی
Transposition	ترانهش
Triangle	مثلث
Trisecting an angle	تثلیث زاویه
Trivial	بدیهی
Union	اجتماع
Unique	یکتا - منحصربفرد
Unit	یکال - واحد
Variable	متغیر
Vector	بردار
... space	فضای برداری
Well - defined	خوشتعریف
X - axis	محور xها
Y - axis	محور yها
Zero	صفر
... ring	حلقهٔ صفر

انتشارات طاق‌بستان

شابک: ۹۶۴-۵۵۵۱-۸۲-X 964-5551-82-X

قیمت: ۷۰۰تومان