نظریهٔ گالوا

محسن خانی

حمزه محمدی

۱۰ مرداد ۱۴۰۱

چکیده

صفحهٔ یادداشتها و جزواتم به آدرس زیر:

https://khani.iut.ac.ir/fa/%DB%8C%D8%A7%D8%AF%D8%AF%D8%A7%D8%B4%D8%AA%D9%87%D8%A7-%D9%88-%D8%AC%D8%B2%D9%88%D8%A7%D8%AA

اکنون پر از جزوه‌ها و یادداشتهای رنگارنگ در حیطه‌های جذاب گوناگون است و نگاه به آنها مرا یاد خاطرات دلنشین سالهای گذشته، تجربه‌های شیرین معلمی و دانشجویان قدیم و جدید می‌اندازد. شاید بینندهٔ این صفحات، که خودش دست‌اندرکار امور دانشگاهی است به ستایش دانشگاهی بپردازد که در آن امکان برگزاری اینچنین درسها و نگارش اینچنین جزوات فراهم شده است.

اما حقیقت چیز دیگری است و همین درس مثال نقضی بزرگ بر این است. مدتها بود که در هر تدریسی، متوجه لنگیدن کمیت دانشجویان در مفاهیم اولیهٔ نظریهٔ گالوا می‌شدم تا این که خودْ به فکر برطرف کردن این نقصان افتادم. برایم غریب و غیر قابل باور بود که دانشجویان کارشناسی ریاضی اثبات قضیهٔ مهمی چون قضیهٔاساسی جبر را نمی‌دانند. درس نظریهٔ گالوا، که به نظر من از مهمترین دروس کارشناسی است، بیش از ده سال بود که در دانشگاه صنعتی اصفهان ارائه نشده بود به طوری که از سامانهٔ دروس نیز نامش حذف شده بود. بنابراین باید این درس را تحت نام «مباحث ویژه» ارائه می‌کردم. نامی که برای دانشجویان ناآشناست و احتمال اخذ درس توسط آنها را کم می‌کند.

ده دانشجوی علاقه‌مند این درس را اخذ کردند اما دانشکده، اجازهٔ تشکیل آن را نمی‌داد، زیرا طبق سیاستهای خردمندانه و دانشمندانهٔ همیشگی، حداقل تعداد دانشجوی لازم برای تشکیل یک کلاس از دید دانشکده ۱۵ نفر بود. من نیز ـ که بناچار باید اعتراف کنم که در این سالها، دانشگاه را جز مانعی در برابر کسب و نشر علم واقعی ندیده‌ام ـ از پافشاری صرف نظر کردم، غافل از این که این بار دانشجویانم به طور خودجوش و جدی پیگیر شدند و نهایتاً با دخالت مستقیم رئیس دانشکده، اجازه وقوع این جرم داده شد (!).

من و آن دانشجویان این فرصت را غنمیت شمردیم و از آن حداکثر بهره را بردیم. از اثبات قضیهٔ اساسی نظریهٔ گالوا گرفته تا قضیهٔ اساسی جبر و قضایای سیلو، درجهٔ تعالی میدانها و هر آنچه من احساس می‌کردم زمان دانشجوی خودم به خوبی برایم توضیح داده نشده است در این دوره تحت پوشش قرار گرفت. درست همان زمانی که کرونا شروع شده بود و اکثر اساتید و دانشجویان دست از کار کشیده بودند، کلاسهای این درس بدون وقفه‌ای طبق معمول توسط

خانم همیشه همراهم، درسا، که آن زمان در انتظار تولد پسرم بود، فیلم‌برداری شد و این فیلمها در لینک زیر قرار گرفت.

https://www.aparat.com/playlist/305753

عادت معهودم این بود که هر درس سایتی برای خود داشته باشد و سایت این درس این بود:

https://mohsen-khani.github.io/9899-2/

چندی بعد، دوست خوبم حمزه، که قبلاً جزوهٔ مدل‌تئوری جبری را نیز تایپ کرده بود، به مشاهدهٔ مجدد این فیلمها پرداخت و بی آنکه من از او خواسته باشم منت نهاد و مطابق فیلمها جزوه‌ای برای این درس تایپ کرد و این جزوه در میان بقیهٔ آن یادداشتهای مختلف قرار گرفت تا دوباره پس از گذر سالها دیدن آن خاطرات خوش دانشجویانم را برایم زنده کند.

پیش از من و تو بسیار بودند و نقش بستند
دیوار زندگی را زین‌گونه یادگاران
وین نغمهٔ محبت بعد از من و تو مانَد
تا در زمانه باقیست آواز باد و باران

خانی، مرداد ۱۴۰۱

فهرست مطالب

۱ جلسه اول: تعاریف اولیه

تعریف ۱ (گروه). فرض کنید مجموعه‌ی G تحت عملگر $+$ بسته باشد و در شرایط زیر صدق کند:

- $\forall a, b, c \in G \ ((a + b) + c = a + (b + c))$
- عنصری چون 0 در G وجود دارد چنان‌که برای هر a در G داشته باشیم: $a + 0 = a$ (یعنی 0 یک عنصر همانی عمل $+$ است).
- $\forall a \in G \ \exists - a \in G \ (a + (-a) = 0)$

در این صورت $(G, +, 0)$ را یک گروه می‌نامیم.

مثال ۲. می‌دانیم که اگر m عددی طبیعی باشد، رابطه همنهشتی به هنگ m یا $\equiv_m$ یک رابطه هم‌ارزی روی $\mathbb{Z}$ تعریف می‌کند. مجموعه همه کلاس‌های هم‌ارزی را با $\mathbb{Z}_m$ نشان می‌دهیم. اگر برای هر عدد صحیح a کلاس هم‌ارزی a را با $\overline{a}$ نشان دهیم، در این صورت: $\mathbb{Z}_m = \{\overline{0}, \ldots, \overline{m-1}\}$. حال عمل $\oplus$ موسوم به جمع با پیمانه m را به صورت زیر تعریف می‌کنیم

$$\forall \overline{a}, \overline{b} \in \mathbb{Z}_m \ (\overline{a} \oplus \overline{b} = \overline{a + b})$$

در این صورت $(\mathbb{Z}_m, \oplus)$ یک گروه است.

تعریف ۳ (گروه آبلی). گروه $(G, +)$ را یک گروه آبلی می‌نامیم هرگاه $\forall a, b \in G \ (a+b = b+a)$

تعریف ۴ (حلقه). منظور از یک حلقه‌ی جابجایی و یکدار، یک مجموعه‌ی F است به همراه دو عمل $+ : F^2 \to F$ و $\cdot : F^2 \to F$ و دو عنصر مشخص 0 و 1 که ویژگی‌های زیر را دارد.

(R_1) $a + (b + c) = (a + b) + c$

(R_2) $a + b = b + a$

(R_3) $a + 0 = a$

(R_4) $\forall a \ \exists b \quad a + b = 0$

(R_5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$(R_6)\ \ a \cdot (b + c) = a \cdot b + a \cdot c$

$(R_7)\ \ a \cdot b = b \cdot a$

$(R_8)\ \ 1 \neq 0, \quad a \cdot 1 = a$

تعریف ۵ (حوزه صحیح). حوزه صحیح یک حلقه‌ی جابجایی و یکدار است که ویژگی زیر را داراست:

$$(R_9) \quad \forall a \neq 0\ \forall b, c \quad a \cdot b = a \cdot c \quad \Longrightarrow \quad b = c$$

تعریف ۶ (میدان). اگر یک حلقه‌ی جابجایی و یکدار ویژگی زیر را داشته باشد به آن یک میدان می‌گوییم

$$(R_{10}) \quad \forall a \neq 0\ \exists b \quad a \cdot b = 1$$

مشاهده:

- ویژگی (R_9) از ویژگی (R_{10}) نتیجه می‌شود.

اثبات. فرض کنید ویژگی (R_{10}) برقرار باشد. فرض کنید $a \cdot b = a \cdot c$. بنا به ویزگی (R_{10})، یک عنصر z وجود دارد به طوری که $z \cdot a = 1$. طرفین عبارت $a \cdot b = a \cdot c$ را در z ضرب کنید: $z \cdot (a \cdot b) = z \cdot (a \cdot c)$. پس $(z \cdot a) \cdot b = (z \cdot a) \cdot c$. بنابراین $b = c$. □

- ویژگی (R_{10}) از ویژگی (R_9) نتیجه می‌شود.

اثبات. $(\mathbb{Z}, +, \cdot, 0, 1)$ ویژگی (R_9) را داراست ولی ویژگی (R_{10}) را دارا نیست. □

- ویژگی (R_9) را می‌توان با ویزگی زیر جایگزین کرد.

$$(R_{11}) \quad \forall a, b \quad a \cdot b = 0 \ \Rightarrow a = 0 \text{ یا } b = 0$$

به طور معادل، اگر هم $a \neq 0$ و هم $b \neq 0$، آنگاه $a \cdot b \neq 0$.

اثبات. ابتدا نشان می‌دهیم که (R_9) از (R_{11}) نتیجه می‌شود. فرض کنید فضای مورد نظر ما ویژگی (R_{11}) را داشته باشد. همچنین فرض کنید $a \cdot b = a \cdot c$ که $a \neq 0$. پس $a \cdot b - a \cdot c = 0$ یعنی $a(b-c) = 0$. بنابر ویژگی (R_{11}) داریم: $b - c = 0$. بنابراین $b = c$. حال نشان می‌دهیم که ویژگی (R_{11}) از ویژگی (R_9) نتیجه می‌شود. فرض کنید (R_9) برقرار است و $ab = 0$. فرض کنید $a \neq 0$. در این صورت $a \cdot b = a \cdot 0$. بنا بر ویژگی (R_9) داریم: $b = 0$. □

لم ۷. هر حوزه‌ی صحیح متناهی یک میدان است.

اثبات. فرض کنید $(\{a_1, \ldots, a_n\}, +, \cdot, 0, 1)$ یک حوزه صحیح متناهی باشد. عنصر $m \in \{a_1, \ldots, a_n\}$ را در نظر بگیرید. فرض کنید m دارای وارون ضربی نباشد. یعنی برای هر a_i داریم: $m \cdot a_i \neq 1$. حال مجموعه‌ی

$$A = \{ma_1, \ldots, ma_n\}$$

را در نظر بگیرید. در این صورت عناصر $a_i \neq a_j$ به گونه‌ای پیدا می‌شوند که $ma_i = ma_j$. بنابراین $a_i = a_j$ و این تناقض است. □

توجه: یک حلقه در صورتی حوزه‌ی صحیح است که زیرحلقه‌ی یک میدان باشد.

لم ۸. هر حلقه‌ای که زیرحلقه‌ی یک میدان باشد حوزه‌ی صحیح است.

اثبات. فرض کنید حلقه‌ی $(D, +, \cdot, 0, 1)$ زیرحلقه‌ی میدانِ $(F, +, \cdot, 0, 1)$ باشد. فرض کنید $a, b, c \in D$ به طوری که $a \neq 0$ و $ab = ac$. از آنجا که $a, b, c \in D \subseteq F$ پس $a, b, c \in F$. بنابراین a در F وارون دارد. فرض کنید $z \in F$ وارون a باشد. پس

$$ab = ac \Rightarrow zab = zac \Rightarrow b = c$$

پس، در F عناصر b و c با هم مساوی هستند. بنابراین در D این دو عنصر با هم برابرند.

□

۲ جلسه دوم: ادامه‌ی تعاریف اولیه

در جلسه‌ی قبل ثابت کردیم که هر حوزه‌ی صحیح متناهی یک میدان است.

مثال ۹. حلقه‌ی جابجایی و یکدار $(\mathbb{Z}_n, +, \cdot)$ که $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ را در نظر بگیرید. آیا $\mathbb{Z}_n$ یک حوزه صحیح است؟ یعنی اگر $a, b \neq 0$، آنگاه $a \cdot b \neq 0$؟ اگر n یک عدد اول نباشد، آنگاه $\mathbb{Z}_n$ حوزه‌ی صحیح نیست. زیرا اگر n اول نباشد، آنگاه اعداد $1 \leq r, s \leq n-1$ به‌گونه‌ای پیدا می‌شوند که $rs = n$. در این صورت $\overline{r} \cdot \overline{s} = \overline{n} = \overline{0}$. اما اگر p عددی اول باشد، آنگاه $\mathbb{Z}_p$ یک حوزه صحیح است. زیرا اگر $\overline{r} \cdot \overline{s} = 0$ یعنی $p|rs$. پس $p|r$ یا $p|s$ یعنی $r = 0$ یا $s = 0$.

نتیجه ۱۰. اگر p یک عدد اول باشد، آنگاه $\mathbb{Z}_p$ یک میدان است.

اثبات اول. فرض کنید $\overline{m} \in \mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$. می‌خواهیم یک وارون ضربی برای $\overline{m}$ پیدا کینم. اعضای $\mathbb{Z}_p$ را در $\overline{m}$ ضرب می‌کنیم:

$$\{\overline{m}\overline{0}, \overline{m}\overline{1}, \dots, \overline{m}\overline{p-1}\}$$

بنابراین $\overline{i} \neq \overline{j}$ وجود دارد که $\overline{m}\overline{i} = \overline{m}\overline{j}$. پس $\overline{m}(\overline{i} - \overline{j}) = 0$ در نتیجه $p|\overline{m}(\overline{i} - \overline{j})$. □

اثبات دوم. فرض کنید $\overline{m} \in \mathbb{Z}_p$. از آنجا که $(m, p) = 1$ پس $m^{p-1} \equiv_p 1$ یعنی $\overline{m^{p-1}} = \overline{1}$. بنابراین $\overline{m^{p-2}}$ معکوس $\overline{m}$ است. □

اثبات سوم. فرض کنید $\overline{m} \in \mathbb{Z}_p$. در این صورت $(m, p) = 1$. بنابراین عناصر a و b به گونه‌ای پیدا می‌شوند که $am + bp = 1$ یعنی $bp = am - 1$ پس $p|am - 1$ یعنی $\overline{a} \cdot \overline{m} = \overline{1}$. □

یادآوری: اگر $(R, +, \cdot, 0, 1)$ زیرحلقه‌ای از میدان $(K, +, \cdot, 0, 1)$ باشد، آنگاه R حوزه‌ی صحیح است.

قضیه ۱۱. فرض کنید $(R, +, \cdot, 0, 1)$ یک حوزه‌ی صحیح باشد. در این صورت یک میدان $Q(R)$ وجود دارد به طوری که

- $(R, +, \cdot, 0, 1)$ زیرحلقه‌ای از میدان $(Q(R), +, \cdot, 0, 1)$ است.

- برای هر میدان $(F,+,\cdot,0,1)$، اگر $(R,+,\cdot,0,1)$ زیرحلقه‌ای از میدان $(F,+,\cdot,0,1)$ باشد، آن‌گاه

$$(R,+,\cdot,0,1)\subseteq(Q(R),+,\cdot,0,1)\subseteq(F,+,\cdot,0,1)$$

اثبات. فرض کنید $(R,+,\cdot,0,1)$ یک حوزه‌ی صحیح باشد. قرار دهید $S=\{(a,b)\,|\,a,b\in R,\ b\neq 0\}$. برای راحتی، اعضای S را به جای (a,b) با $\frac{a}{b}$ نشان می‌دهیم. روی S رابطه‌ی زیر را تعریف می‌کنیم.

$$(a,b)\sim(c,d)\ \Leftrightarrow\ ad=bc$$

ادعا می‌کنیم رابطه‌ی فوق یک رابطه‌ی هم‌ارزی است.

الف) چون $ab=ba$ پس $(a,b)\sim(a,b)$.

ب) فرض کنید $(a,b)\sim(c,d)$. در این صورت $ad=bc$ پس $cb=da$ یعنی $(c,d)\sim(a,b)$.

ج) فرض کنید $(a,b)\sim(c,d)$ و $(c,d)\sim(e,f)$. در این صورت $ad=bc$ و $cf=de$. بنابراین $adf=bcf$ و $bcf=bde$. پس $adf=bde$ بنابراین $af=be$ یعنی $(a,b)\sim(e,f)$.

کلاس هم‌ارزی هر عنصر (a,b) را با $[(a,b)]$ یا $[\frac{a}{b}]$ نشان می‌دهیم. مشاهده می‌کنیم که نگاشت $\varphi:R\to S$ که $\varphi(a)=\frac{a}{1}$ یک نگاشت یک‌به‌یک است. زیرا اگر $\frac{a}{1}=\frac{b}{1}$، آن‌گاه $a=b$. حال جمع بین دو عضو (a,b) و (c,d) را به صورت $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$ تعریف می‌کنیم، توجه کنید که $bd\neq 0$. حال به اثبات خوش‌تعریفی جمع می‌پردازیم. فرض کنید $[(a,b)]=[(a',b')]$ و $[(c,d)]=[(c',d')]$. نشان می‌دهیم که

$$[(ad+bc,bd)]=[(a'd'+b'c',b'd')]$$

از اینکه $[(a,b)]=[(a',b')]$ داریم: $ab'=ba'$ بنابراین $dd'ab'=ba'dd'$. از اینکه $[(c,d)]=[(c',d')]$ داریم: $cd'=dc'$ بنابراین $bb'cd'=dc'bb'$. اکنون از اینکه $dd'ab'=ba'dd'$

و $bb'cd' = dc'bb'$ داریم: $b'd'ad + b'd'bc = bda'd' + bdb'c'$ یعنی $b'd'(ad + bc) = bd(a'd' + b'c')$.

به طور مشابه ضرب را به صورت $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ تعریف می‌کنیم. به سادگی بررسی می‌شود که مجموعه‌ی S با عمل‌هایی که تعریف شد یک میدان است. این میدان را با $Q(R)$ نشان می‌دهیم و به آن میدان کسرهای حوزه‌ی صحیح R می‌گوییم. فرض کنید $(F, +, \cdot, 0, 1)$ یک میدان باشد که $(R, +, \cdot, 0, 1) \subseteq (F, +, \cdot, 0, 1)$. نشان می‌دهیم که $(Q(R)+, \cdot, 0, 1)$ در $(F, +, \cdot, 0, 1)$ نشانده می‌شود. نگاشت زیر را در نظر بگیرید:

$$\begin{aligned} \varphi :&(Q(R)+, \cdot, 0, 1) \to (F, +, \cdot, 0, 1) \\ &\frac{a}{b} \mapsto a \cdot b^{-1} \end{aligned}$$

نگاشت φ یک نشاندن است.

$$\varphi(\frac{a}{b} + \frac{c}{d}) = \varphi(\frac{ad + bc}{bd}) = (ad + bc)(bd)^{-1} = ab^{-1} + cd^{-1} = \varphi(\frac{a}{b}) + \varphi(\frac{c}{d})$$

$$\varphi(\frac{a}{b} \cdot \frac{c}{d}) = \varphi(\frac{ac}{bd}) = ac(bd)^{-1} = ac(b^{-1}d^{-1}) = ab^{-1} \cdot cd^{-1} = \varphi(\frac{a}{b}) \cdot \varphi(\frac{c}{d})$$

□

۳ جلسه سوم: ایده‌آل‌ها

تعریف ۱۲ (زیرحلقه)**.** فرض کنید $(R, +, \cdot)$ یک حلقه جابجایی یکدار باشد. فرض کنید $U \subseteq R$ به گونه‌ای باشد که $(U, +, \cdot)$ یک حلقه باشد در این صورت $(U, +, \cdot)$ را یک زیرحلقه از $(R, +, \cdot)$ می‌نامیم.

تمرین ۱. فرض کنید $(R, +, \cdot)$ یک حلقه باشد و $U \subseteq R$، در این صورت $(U, +, \cdot)$ یک زیرحلقه از $(R, +, \cdot)$ است اگر و تنها اگر برای هر $a, b \in U$ داشته باشیم: $a - b \in U$ و $a \cdot b \in U$.

مثال ۱۳. $(\mathbb{Z}, +, \cdot)$ یک زیرحلقه از حلقه‌ی $(\mathbb{R}, +, \cdot)$ است. $(2\mathbb{Z}, +, \cdot)$ یک زیرحلقه از حلقه‌ی $(\mathbb{Z}, +, \cdot)$ است.

مثال ۱۴. $(\mathbb{Z}_4, +, \cdot)$ زیرحلقه‌ای از $(\mathbb{Z}, +, \cdot)$ نیست.

تعریف ۱۵ (ایده‌آل)**.** فرض کنید $(R, +, \cdot)$ یک حلقه باشد و $(I, +, \cdot)$ یک زیرحلقه‌ی ناتهی از آن باشد که دارای ویژگی زیر است:

$$\forall r \in R \; \forall i \in I \; (r \cdot i \in I)$$

در اینصورت I را ایده‌آلی از R می‌نامیم و با نماد $I \rhd R$ نشان می‌دهیم. به بیان دیگر $I \subseteq R$ یک ایده‌آل است هرگاه شرط‌های زیر را برآورده کند:

- $\forall a, b \in I \; (a - b \in I \wedge a \cdot b \in I)$
- $\forall a \in I \; \forall r \in R \; (r \cdot a \in I)$

مثال ۱۶. $(\mathbb{Z}, +, \cdot)$ یک زیرحلقه از $(\mathbb{Q}, +, \cdot)$ است اما $(\mathbb{Z}, +, \cdot)$ یک ایده‌آل از $(\mathbb{Q}, +, \cdot)$ نیست.

مثال ۱۷. $(2\mathbb{Z}, +, \cdot)$ یک ایده‌آل از $(\mathbb{Z}, +, \cdot)$ است. در حالت کلی برای هر n، $(n\mathbb{Z}, +, \cdot)$ یک ایده‌آل از $(\mathbb{Z}, +, \cdot)$ است.

لم ۱۸. فرض کنید $(R, +, \cdot)$ یک حلقه باشد و $(I_n)_{n \in \mathbb{N}}$ یک خانواده از ایده‌آل‌های R باشد. در اینصورت $\bigcap_{n \in \mathbb{N}} I_n$ یک ایده‌آل از R است.

اثبات. فرض کنید $a, b \in \bigcap_{n \in \mathbb{N}} I_n$ و $r \in R$ در اینصورت برای هر $i \in \mathbb{N}$، $a, b \in I_i$. بنابراین $a - b, a \cdot b \in I_i$ و $r \cdot a \in I_i$. پس $a - b, a \cdot b, r \cdot a \in \bigcap_{n \in \mathbb{N}} I_n$. □

تعریف ۱۹. فرض کنید $(R, +, \cdot)$ یک حلقه باشد و $A \subseteq R$. در اینصورت $\bigcap\limits_{\substack{A \subseteq I \\ I \rhd R}} I$ کوچکترین ایده‌آل شامل مجموعه‌ی A است که به آن ایده‌آل تولید شده توسط مجموعه‌ی A گفته می‌شود.

لم ۲۰. فرض کنید $(R, +, \cdot)$ یک حلقه باشد و $A = \{a_1, \ldots, a_n\} \subseteq R$. در اینصورت ایده‌آل تولید شده توسط A در R را با نماد $\langle A \rangle_R$ نشان می‌دهیم و از عناصر زیر تشکیل شده است:

$$\langle A \rangle_R = \bigcap_{\substack{A \subseteq I \\ I \rhd R}} I = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \,|\, r_i \in R\}$$

اثبات. کافی است ثابت شود که $B = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \,|\, r_i \in R\}$ یک ایده‌آل است (توجه کنید که $A \subseteq B$ و برای هر ایده‌آل $A \subseteq I$ داریم $B \subseteq I$). □

مثال ۲۱. فرض کنید $(D,+,\cdot)$ یک حوزه صحیح باشد و فرض کنید $a,b \in D$. می‌دانیم که $\langle a\rangle_D = \{ra \,|\, r \in D\}$ و $\langle b\rangle_D = \{rb \,|\, r \in D\}$. در اینصورت $\langle a\rangle_D \subseteq \langle b\rangle_D$ اگر و تنها اگر $b|a$ (یعنی $d \in D$ وجود داشته باشد به طوری که $a = bd$)

اثبات. فرض کنید $\langle a\rangle_D \subseteq \langle b\rangle_D$ در اینصورت $a \in \langle a\rangle_D \subseteq \langle b\rangle_D$ پس $a \in \langle b\rangle_D$ بنابراین $r \in D$ موجود است که $a = rb$. برعکس، فرض کنید $a = bd$ که $d \in D$ در اینصورت فرض کنید $ra \in \langle a\rangle_D$ می‌توان نوشت $ra = rbd$ پس $ra \in \langle b\rangle_D$. □

مثال ۲۲. حلقه‌ی $(\mathbb{Z},+,\cdot)$ را در نظر بگیرید. ایده‌آل تولید شده توسط $n \in \mathbb{Z}$ به صورت $\langle n\rangle_{\mathbb{Z}} = \{rn \,|\, r \in \mathbb{Z}\}$. پس

$$\langle n\rangle_{\mathbb{Z}} \subseteq \langle m\rangle_{\mathbb{Z}} \quad \Leftrightarrow \quad m|n$$

تمرین ۲. فرض کنید حلقه‌ی R هیچ ایده‌آلی غیر از R و $\{0\}$ نداشته باشد در اینصرت R یک میدان است. (فرض کنید $r \in R$ یک عضو ناصفر باشد در اینصورت $\langle r\rangle_R = R$ پس $1 \in \langle r\rangle_R$)

تمرین ۳. فرض کنید I یک ایده‌آل از حلقه R باشد. در اینصورت $1_R \in I \Leftrightarrow I = R$.

تعریف ۲۳ (هومومرفیسم)**.** فرض کنید $(R,+_R,\cdot_R)$ و $(S,+_S,\cdot_S)$ دو حلقه باشند. فرض کنید $\varphi : R \to S$ یک تابع باشد که برای هر $a,b \in R$، $\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$ و $\varphi(a \cdot_R b) = \varphi(a) \cdot_S \varphi(b)$ در اینصورت می‌گوییم φ یک هومومرفیسم از R به S است.

تعریف ۲۴. اگر هومومرفیسم φ یک‌به‌یک باشد به آن مونومرفیسم (نشاندن) گفته می‌شود و اگر هومومرفیسم φ یک‌به‌یک و پوشا باشد بدان ایزومرفیسم گفته می‌شود.

تعریف ۲۵. فرض کنید $\varphi : R \to S$ یک هومومرفیسم باشد، هسته‌ی هومومرفیسم φ را با نماد $\mathrm{Ker}(\varphi)$ نشان می‌دهیم و به صورت $\mathrm{Ker}(\varphi) = \{x \in R \,|\, \varphi(x) = 0_S\}$ تعریف می‌شود.

لم ۲۶. اگر $\varphi : S \to R$ هومومرفیسم باشد آنگاه $\varphi(0_S) = \varphi(0_R)$

اثبات. چون φ هومومرفیسم است، پس $\varphi(0_S) = \varphi(0_S + 0_S) = \varphi(0_S) + \varphi(0_S)$ بنابراین $\varphi(0_S) = 0_R$ و در نتیجه داریم $\varphi(0_S) + \varphi(0_S)$ □

لم ۲۷. فرض کنید R و S دو حلقه باشند و $\varphi : S \to R$ یک هومومرفیسم باشد. در اینصورت $\varphi(S) \subseteq R$ یک زیرحلقه است.

اثبات. فرض کنید $\varphi(x), \varphi(y) \in \varphi(S)$. در اینصورت $\varphi(x)+_R\varphi(y) = \varphi(x+_S y) \in \varphi(S)$ (به طور مشابه برای ضرب). □

در لم قبل $\varphi(S)$ را یک تصویر هومومرفیک حلقه‌ی S در حلقه‌ی R می‌نامیم.

تمرین ۴. فرض کنید R و S دو حلقه باشند و $\varphi : S \to R$ یک هومومرفیسم باشد دراینصورت

الف) اگر R و S هر دو حوزه صحیح باشند آنگاه $\varphi(1_S) = 1_R$.

ب) اگر R و S هر دو میدان باشند آنگاه φ مونوفریسم است.

۴ جلسه چهارم: حلقه‌های خارج قسمی و مشخصه میدان‌ها

فرض کنید R یک حلقه دلخواه باشد و $I \subseteq R$ یک ایده‌آل باشد. بین اعضای R رابطه زیر را در نظر بگیرید.

$$x \sim y \Leftrightarrow x - y \in I$$

رابطه فوق یک رابطه هم‌ارزی است. مجموعه‌ی کلاس‌های هم‌ارزی رابطه‌ی فوق را با R/I نشان می‌دهیم و

$$R/I = \{[x] \,|\, x \in R\}.$$

توجه شود که $[0] = \{x \in R \,|\, x \in I\}$. روی R/I جمع و ضرب زیر را تعریف میکنیم:

$$[x] + [y] = [x + y]$$
$$[x] \cdot [y] = [x \cdot y]$$
$$0_{R/I} = [0]$$
$$1_{R/I} = [1]$$

توجه شود که گاهی $[x]$ را با $x + I$ نشان می‌دهیم.
برای خوش‌تعرفی جمع فرض کنید $[x] = [x']$ و $[y] = [y']$، ادعا می‌کنیم که $[x+y] = [x'+y']$.

با توجه به تعریف داریم:

$$[x] = [x'] \Leftrightarrow x - x' \in I$$
$$[y] = [y'] \Leftrightarrow y - y' \in I$$

بنابراین $(x+y) - (x'+y') = (x-x') + (y-y') \in I$. به طور مشابه خوش‌تعریفی ضرب بررسی می‌شود و ثابت می‌شود R/I با جمع و ضرب تعریف شده یک حلقه است.

تعریف ۲۸ (هومومرفیسم طبیعی)**.** فرض کنید R یک حلقه باشد و I یک ایده‌آل از آن باشد. حلقه R/I را در نظر بگیرید. نگاشت $\varphi : R \to R/I$ که $\varphi(x) = [x]$ را هومومرفیسم طبیعی (یا کانونی) می‌نامیم.

توجه شود که هومومرفیسم طبیعی $\varphi : R \to R/I$ تمامی عناصر موجود در I را به $0_{R/I}$ می‌برد.

مثال ۲۹. در حلقه $\mathbb{Z}$، با استفاده از ایده‌آل $\langle n\mathbb{Z}\rangle$، حلقه‌ی $\mathbb{Z}/\langle n\mathbb{Z}\rangle$ را تعریف می‌کنیم که $\mathbb{Z}_n \simeq \mathbb{Z}/\langle n\mathbb{Z}\rangle$ و هومومرفیسم طبیعی $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ به صورت $\varphi(x) = [x]$ تعریف می‌شود.

فرض کنید $\varphi : R \to S$ یک هومومرفیسم باشد که R و S دو حلقه هستند. روی R رابطه هم‌ارزی زیر را در بگیرید:

$$x \sim y \Leftrightarrow \varphi(x) = \varphi(y) \Leftrightarrow \varphi(x) -_S \varphi(y) = 0_S \Leftrightarrow \varphi(x -_R y) = 0_S$$

در واقع رابطه‌ی بالا به صورت زیر است:

$$x \sim y \Leftrightarrow x - y \in \mathrm{Ker}(\varphi)$$

توجه شود که $\mathrm{Ker}(\varphi) \subseteq R$ یک ایده‌آل است (به سادگی بررسی می‌شود). بنابراین رابطه‌ی $\sim$ یک رابطه‌ی هم‌ارزی است و کلاس‌های هم‌ارزی آن، حلقه‌ی $R/\mathrm{Ker}(\varphi)$ را می‌سازند. اکنون نگاشت $\psi : R/\mathrm{Ker}(\varphi) \to S$ که $\psi([x]) = \varphi(x)$ را در نظر بگیرید. نگاشت ψ یک هومومرفیسم یک‌به‌یک است چون اگر $\psi([x]) = \psi([y])$، آنگاه $\psi([x] - [y]) = 0$ یعنی $\psi([x-y]) = 0$ پس $\varphi(x-y) = 0$ یعنی $x - y \in \mathrm{Ker}(\varphi)$ و بنابراین $[x] = [y]$. در واقع ما قضیه زیر را ثابت کردیم:

قضیه ۳۰. فرض کنید $\varphi : R \to S$ یک هومومرفیسم باشد. در اینصورت $R/\mathrm{Ker}(\varphi) \simeq \mathrm{Im}(\varphi)$.

مثال ۳۱. هومومرفیسم $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ که $\varphi(x) = [x]$ را در نظر بگیرید. در اینصورت $\mathrm{Ker}(\varphi) = n\mathbb{Z} = \langle n \rangle$ بنابراین طبق قضیه فوق $\mathbb{Z}/\mathrm{Ker}(\varphi) \simeq \mathrm{Im}(\varphi)$ پس $\mathbb{Z}/\langle n \rangle \simeq \mathbb{Z}_n$.

مشخصه میدان

فرض کنید F یک میدان باشد. فرض کنید

$$\begin{aligned} 2 \cdot 1_F &= 1_F + 1_F \neq 0 \\ 3 \cdot 1_F &= 1_F + 1_F + 1_F \neq 0 \\ 4 \cdot 1_F &= 1_F + 1_F + 1_F + 1_F \neq 0 \\ &\vdots \end{aligned}$$

در واقع فرض کنید برای هر عدد طبیعی n، $n \cdot 1_F = 1_F + 1_F + \cdots + 1_F \neq 0$ در اینصورت میدان F را با مشخصه صفر می‌نامیم. توجه کنید اگر F با مشخصه صفر باشد، آنگاه اولاً برای هر $0 \neq x \in F$ و هر $n \in \mathbb{N}$ داریم: $\underbrace{x + \ldots + x}_{n \text{ بار}} \neq 0$. ثانیاً برای هر $m \neq n$ داریم: $n1_F \neq m1_F$.

قضیه ۳۲. هر میدان با مشخصه صفر حاوی یک کپی از حلقه‌ی $(\mathbb{Z}, +, \cdot)$ است.

اثبات. نگاشت $\varphi : \mathbb{Z} \to F$ که $\varphi(1) = 1_F$ و $\varphi(n) = n1_F$ را در نظر بگیرید. این نگاشت یک هومومرفیسم یک‌به‌یک (مونومرفیسم) است؛ چون

$$\varphi(n+m) = n1_F + m1_F = (n+m)1_F$$

$$\varphi(n \cdot m) = n1_F \cdot m1_F = (\underbrace{1_F + \cdots + 1_F}_{n \text{ بار}}) \cdot (\underbrace{1_F + \cdots + 1_F}_{m \text{ بار}}) = nm1_F = n1_F \cdot m1_F$$

پس نگاشت فوق یک هومومرفیسم است. حال نشان می‌دهیم که نگاشت فوق یک‌به‌یک است:

$$n1_F = m1_F \Leftrightarrow (n-m)1_F = 0 \Leftrightarrow n = m$$

□

تمرین ۵. فرض کنید F_1 و F_2 دو میدان با مشخصه صفر هستند. نشان دهید F_1 و F_2 حاوی یک کپی از میدان کسرهای $\mathbb{Z}$ هستند (نشان دهید نگاشت $\varphi : \mathbb{Q} \to F_1$ که $\varphi(\frac{m}{n}) = (m1_F) \cdot (n1_F)^{-1}$ یک مونومرفیسم است).

فرض کنید F یک میدان باشد که برای یک عدد طبیعی m داشته باشیم: $\underbrace{1_F + \cdots + 1_F}_{m \text{ بار}} = 0_F$ در اینصورت F را یک میدان با مشخصه‌ی ناصفر می‌نامیم. کوچکترین عدد طبیعی m را که $\underbrace{1_F + \cdots + 1_F}_{m \text{ بار}} = 0_F$، مشخصه‌ی میدان می‌نامیم. توجه شود که اگر m مشخصه‌ی میدان F باشد، آنگاه برای هر $x \in F$ داریم: $\underbrace{x + \cdots + x}_{m \text{ بار}} = 0_F$. بنابرین هر میدان متناهی با مشخصه‌ی ناصفر است.

لم ۳۳. اگر مشخصه‌ی میدان F ناصفر باشد، آنگاه مشخصه‌ی F یک عدد اول است.

اثبات. فرض کنید $m = rs$ مشخصه‌ی میدان F باشد. در اینصورت

$$m1_F = \underbrace{(1_F + \cdots + 1_F)}_{r \text{ بار}} \cdot \underbrace{(1_F + \cdots + 1_F)}_{s \text{ بار}} = 0$$

پس $\underbrace{(1_F + \cdots + 1_F)}_{r \text{ بار}} = 0$ یا $\underbrace{(1_F + \cdots + 1_F)}_{s \text{ بار}} = 0$، این تناقض است با اینکه m کوچکترین عدد طبیعی است که $m1_F = 0$. □

مثال ۳۴. $\mathbb{Z}_p$ یک میدان با مشخصه‌ی p است.

قضیه ۳۵. هر میدان با مشخصه‌ی p حاوی یک کپی از $\mathbb{Z}_p$ است.

اثبات. هومومرفیسم $\varphi : \mathbb{Z} \to F$ که $\varphi(n) = n1_F$ را در نظر بگیرید. به عنوان تمرین ثابت کنید که

$$\mathrm{Ker}(\varphi) = \{n \in \mathbb{Z} \,|\, n1_F = 0\} = \{n \in \mathbb{Z} \,|\, p|n\} = \langle p \rangle$$

(راهنمایی: اگر $p \nmid n$، آنگاه $n = pq + r$. بنابراین اگر $n1_F = 0$، پس $pq1_F + r1_F = 0$. بنابراین $r1_F = 0$ و این تناقض است با اینکه p مشخصه‌ی میدان است). پس $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle \simeq \mathrm{Im}(\varphi)$. □

۵ جلسه پنجم: حوزه‌های اقلیدسی

یادآوری: فرض کنید $a, b \in \mathbb{Z}$، می‌گوییم $a|b$ هرگاه $0 \neq c \in \mathbb{Z}$ وجود داشته باشد که $b = ac$.

تعریف ۳۶. فرض کنید D یک حوزه صحیح باشد و $a, b \in D$ می‌گوییم $a|b$ هرگاه $c \in D$ وجود داشته باشد که $b = ac$.

لم ۳۷. فرض کنید D یک حوزه صحیح باشد و $a, b \in D$. در اینصورت $a|b \Leftrightarrow \langle a \rangle \supseteq \langle b \rangle$.

اثبات. توجه شود که $\langle a \rangle = \{ra \,|\, r \in D\}$ و $\langle b \rangle = \{rb \,|\, r \in D\}$. اگر $a|b$، آنگاه $r \in D$ وجود دارد که $b = ra$ یعنی $b \in \langle a \rangle$. بنابراین $\langle b \rangle \subseteq \langle a \rangle$. اگر $\langle b \rangle \subseteq \langle a \rangle$، آنگاه $b \in \langle a \rangle$. پس $r \in D$ وجود دارد که $b = ra$. □

یادآوری: اگر در اعداد صحیح $a|b$ و $b|a$، آنگاه $a = \pm b$.

مشاهده: در یک حوزه صحیح دلخواه D اگر $a|b$ و $b|a$ (یعنی اگر $\langle b \rangle \subseteq \langle a \rangle$ و $\langle a \rangle \subseteq \langle b \rangle$)، آنگاه $a = ub$ که u یک عنصر یکه است یعنی دارای وارون است.

یادآوری: فرض کنید $a, b \in \mathbb{Z}$ که $b \neq 0$. در اینصورت $a = bq + r$ که $|r| < |b|$.

تعریف ۳۸. حوزه صحیح D را اقلیدسی می‌نامیم هرگاه یک تابع $\delta : D \to \mathbb{N}$ که $\delta(0_D) = 0$ وجود داشته باشد به طوری که برای هر $a, 0 \neq b \in D$ بتوان نوشت: $a = bq + r$ که $\delta(r) < \delta(b)$.

توجه شود که در تعریف فوق $\delta(r) = 0 \Leftrightarrow r = 0$.

مشاهده: فرض کنید D یک حوزه اقلیدسی باشد و $a, 0 \neq b \in D$. در اینصورت

$$\begin{aligned} a &= bq_0 + r_0 & \delta(r_0) &< \delta(b) \\ b &= r_0q_1 + r_1 & \delta(r_1) &< \delta(r_0) \\ r_0 &= r_1q_2 + r_2 & \delta(r_2) &< \delta(r_1) \\ r_1 &= r_2q_3 + r_3 & \delta(r_3) &< \delta(r_2) \end{aligned}$$

پس $\delta(r_3) < \delta(r_2) < \delta(r_1) < \delta(r_0) < \delta(b)$. بنابراین با ادامه الگوریتم فوق، باقی‌مانده صفر می‌شود. توجه شود که $r_2|r_1$ و $r_2|r_0$، پس $r_2|b$ و $r_2|a$. همچنین اگر $r'|a$ و $r'|b$، آنگاه $r'|r_2$.

تعریف ۳۹. فرض کنید D یک حوزه صحیح باشد و $a, b \in D$. می‌گوییم d بزرگترین مقسوم‌علیه مشترک a و b است این را با نماد $\gcd(a, b)$ نشان می‌دهیم هرگاه $d|a$ و $d|b$ و برای هر $d' \in D$ اگر $d'|a$ و $d'|b$، آنگاه $d'|d$.

توجه شود که اگر حوزه صحیح D اقلیدسی باشد و $a, 0 \neq b \in D$، آنگاه یک d وجود دارد که $d = \gcd(a, b)$. همچنین اگر $d, d' = \gcd(a, b)$، آنگاه $d|d'$ و $d'|d$ پس $d = ud'$ که u یک عنصر یکه است.

یادآوری: در اعداد صحیح این‌گونه است که اگر $d = \gcd(a, b)$، آنگاه $m, n \in \mathbb{Z}$ وجود دارند که $d = ma + nb$.

لم ۴۰. فرض کنید D یک حوزه صحیح اقلیدسی باشد و $a, 0 \neq b \in D$. در اینصورت $\gcd(a, b) = d$ اگر و تنها اگر $\langle a, b\rangle = \langle d\rangle$.

اثبات. اگر $\gcd(a, b) = d$، آنگاه $d|a$ و $d|b$ پس $\langle a\rangle \subseteq \langle d\rangle$ و $\langle b\rangle \subseteq \langle d\rangle$. بنابراین $\langle a, b\rangle \subseteq \langle d\rangle$. از طرفی توجه کنید که d ترکیبی به صورت $ma + nb$ است پس $d \in \langle a, b\rangle$ یعنی $\langle d\rangle \subseteq \langle a, b\rangle$. اگر $\langle a, b\rangle = \langle d\rangle$، آنگاه $a \in \langle d\rangle$ و $b \in \langle d\rangle$. پس $d|a$ و $d|b$. فرض کنید $d'|a$ و $d'|b$، در اینصورت $a \in \langle d'\rangle$ و $b \in \langle d'\rangle$. بنابراین $\langle d\rangle = \langle a, b\rangle \subseteq \langle d'\rangle$ و در نتیجه $d'|d$. □

توجه شود که در یک حوزه صحیح دلخواه اگر $\langle a, b\rangle = \langle d\rangle$، آنگاه $d = \gcd(a, b)$.

تعریف ۴۱. به هر حوزه صحیح که در آن تمام ایده‌آل‌ها اصلی هستند یک حوزه‌ی ایده‌آل اصلی[1] گفته می‌شود.

قضیه ۴۲. فرض کنید D یک حوزه اقلیدسی باشد. در اینصورت هر ایده‌آلی مانند $I \subseteq D$ به صورت $I = \langle a\rangle$ است (هر حوزه اقلیدسی، یک حوزه ایده‌آل اصلی است. به طور خاص $(\mathbb{Z}, +, \cdot)$ یک حوزه ایده‌آل اصلی است).

اثبات. فرض کنید $I \subseteq D$ یک ایده‌آل باشد. قرار دهید $A = \{\delta(r) \mid r \in I, r \neq 0\} \subseteq \mathbb{N}$. پس A دارای یک عنصر می‌نیمم است، فرض کنید $\delta(r') = \min A$. نشان می‌دهیم $I = \langle r'\rangle$. فرض کنید $r \in I$، در اینصورت $r = r'q + r''$ که $\delta(r'') < \delta(r')$. پس $r'' = 0$ یعنی $r = r'q$. □

[1] Principal ideal domain

نتیجه: در هر حوزه ایده‌آل اصلی، بزرگترین مقسوم‌علیه مشترک دو عنصر a و b همواره موجود است چون $\langle a, b\rangle = \langle d\rangle$.

۶ جلسه ششم: تجزیه یکتا

یادآوری: عدد $p \in \mathbb{Z}$ را یک عدد اول می‌نامیم هرگاه برای هر $a, b \in \mathbb{Z}$ اگر $p = ab$، آنگاه $a = \pm 1$ یا $b = \pm 1$. به بیان دیگر $p \in \mathbb{Z}$ اول است هرگاه برای هر $a \in \mathbb{Z}$ اگر $a|p$، آنگاه $a = \pm 1$ یا $a = \pm p$.

تعریف ۴۳. فرض کنید R یک حلقه باشد. مجموعه‌ی عناصر وارون‌پذیر در R را با $U(R)$ نشان می‌دهیم و $U(R)$ با ضرب R یک گروه است.

تعریف ۴۴. فرض کنید D یک حوزه صحیح باشد. عنصر $p \in D$ را تحویل‌ناپذیر می‌نامیم هرگاه برای هر $a \in D$ اگر $a|p$، آنگاه یا $a \in U(D)$ یا $a = up$ که $u \in U(D)$.

لم ۴۵. فرض کنید D یک حوزه‌ی ایده‌آل اصلی باشد. در اینصورت اگر p یک عنصر تحویل‌ناپذیر باشد، آنگاه $\langle p\rangle$ ماکسیمال است (یعنی هیچ ایده‌آلی مانند I پیدا نمی‌شود به طوری که $\langle p\rangle \subsetneq I \subsetneq D$).

اثبات. فرض کنید $I = \langle r\rangle$ ایده‌آلی باشد که $\langle p\rangle \subsetneq I \subsetneq D$، بنابراین $r|p$. نشان می‌دهیم r یکه نیست و $r \neq up$ و این با تحویل‌ناپذیری p در تناقض است. اگر r یک عنصر یکه باشد، آنگاه $\langle r\rangle = D$. اگر $r = up$، آنگاه $\langle r\rangle = p$. □

تمرین ۶. در یک حوزه صحیح D، نشان دهید $a = ub \Leftrightarrow \langle a\rangle = \langle b\rangle$. همچنین نشان دهید $\langle r\rangle = D \Leftrightarrow r \in U(D)$.

مشاهده: عنصر $p \in D$ را تحویل‌ناپذیر می‌نامیم هرگاه اگر $\langle p\rangle \supseteq \langle a\rangle$، آنگاه یا $\langle a\rangle = D$ یا $\langle a\rangle = \langle p\rangle$.

لم ۴۶. اگر D یک حوزه ایده‌آل اصلی باشد و $\langle p\rangle$ ماکسیمال باشد در اینصورت p تحویل‌ناپذیر است.

اثبات. فرض کنید $r|p$ و $r \notin U$ و $r \neq up$. در اینصورت $\langle p \rangle \subsetneqq \langle r \rangle \neq D$. □

مشاهده: فرض کنید D یک حوزه ایده‌آل اصلی باشد و $p \in D$ یک عنصر تحویل‌ناپذیر باشد. در اینصورت $\langle p \rangle$ یک ایده‌آل ماکسیمال است. فرض کنید $r \in D \setminus \langle p \rangle$ (یعنی $p \not| r$). حال ایده‌آل تولید شده توسط p و r یعنی $\langle p, r \rangle$ را در نظر بگیرید. توجه کنید $\langle p \rangle \subsetneqq \langle p, r \rangle$. بنابراین $1_D \in \langle p, r \rangle$ یعنی عناصر $a, b \in D$ وجود دارند به طوری که $ap + br = 1_D$. به بیان دیگر اگر $r \notin \langle p \rangle$، آنگاه $b \in D$ موجود است به گونه‌ای که $br - 1_D = ap$. به بیان دیگر اگر $r \notin \langle p \rangle$، آنگاه $b \in D$ موجود است به گونه‌ای که $br - 1_D \in \langle p \rangle$. به بیان ایده‌آلی فرض کنید p یک عنصر تحویل‌ناپذیر در یک حوزه ایده‌آل اصلی D باشد. حلقه‌ی $\frac{D}{\langle p \rangle}$ را در نظر بگیرید. فرض کنید $0_{\frac{D}{\langle p \rangle}} \neq r + \langle p \rangle \in \frac{D}{\langle p \rangle}$. بنابراین $r \notin \langle p \rangle$. در اینصورت $b \in D$ موجود است به گونه‌ای که $(r + \langle p \rangle) \cdot (b + \langle p \rangle) = rb + \langle p \rangle = 1 + \langle p \rangle$ یعنی عناصر ناصفر حلقه‌ی $\frac{D}{\langle p \rangle}$ وارون‌پذیر هستند.

قضیه ۴۷. فرض کنید D یک حوزه ایده‌آل اصلی باشد. در این صورت عنصر $p \in D$ تحویل‌ناپذیر است اگر و تنها اگر $\frac{D}{\langle p \rangle}$ یک میدان باشد.

اثبات. فرض کنید $0 \neq r + \langle p \rangle \in \frac{D}{\langle p \rangle}$، یعنی $r \notin \langle p \rangle$. بنابراین $1 \in \langle p, r \rangle = D$. پس $ap + br = 1$ یعنی $br - 1 \in \langle p \rangle$ یعنی $(b + \langle p \rangle)(r + \langle p \rangle) = 1 + \langle p \rangle$. برای اثبات برعکس، فرض کنید $\frac{D}{\langle p \rangle}$ یک میدان باشد. نشان می‌دهیم p تحویل‌ناپذیر است. فرض کنید $r|p$ که $r \neq up$ ($\langle p \rangle \subsetneqq \langle r \rangle$). یعنی $r + \langle p \rangle \neq 0$ یعنی عنصر $r' \in D$ وجود دارد به طوری که $rr' \equiv_{\langle p \rangle} 1$ یعنی $rr' - 1 = ap$. توجه شود که $rr' \in \langle r \rangle$ و $ap \in \langle p \rangle \subset \langle r \rangle$ بنابراین $1 \in \langle r \rangle$ یعنی $\langle r \rangle = D$ یعنی r یک عنصر یکه است. بنابراین $\langle p \rangle$ ماکسیمال است و در نتیجه p تحویل ناپذیر است. □

یادآوری: فرض کنید $p \in \mathbb{Z}$ یک عدد اول باشد. اگر $p|ab$ آنگاه $p|a$ یا $p|b$.

لم ۴۸. فرض کنید D یک حوزه ایده‌آل اصلی باشد و $p \in D$ یک عنصر تحویل‌ناپذیر باشد. در این‌صورت اگر $p|ab$، آنگاه $p|a$ یا $p|b$.

اثبات. فرض کنید $p|ab$ و $p \not| a$. بنابراین $a \notin \langle p \rangle$ پس $\langle p \rangle \subsetneqq \langle a, p \rangle$، یعنی $\langle a, p \rangle = 1$ به طور خاص $1_D \in \langle a, p \rangle$. یعنی $r_1 a + r_2 p = 1_D$. بنابراین $r_1 ab + r_2 pb = b$ حال چون $p|r_1 ab$ و

$p|r_2pb$ پس $p|b$. □

یادآوری: هر عدد صحیح به صورت یکتا به عوامل اول به صورت $p_1^{\alpha_1}\cdots p_n^{\alpha_n}$ قابل تجزیه است.

لم ۴۹. اگر D یک حوزه ایده‌آل اصلی باشد، در اینصورت هیچ زنجیر اکیدا صعودی از ایده‌آل‌ها در داخل D وجود ندارد.

اثبات. فرض کنید D حوزه ایده‌آل اصلی باشد و $I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots$ یک زنجیر از ایده‌آل‌ها باشد، قرار دهید $I = \bigcup_{i\in\mathbb{N}} I_i = \{r \mid \exists i \in \mathbb{N}(r \in I_i)\}$. نشان می‌دهیم I یک ایده‌آل است (اثبات به عنوان تمرین به عهده خواننده). پس $I = \bigcup_{i\in\mathbb{N}} I_i = \langle b\rangle$ به طور خاص $b \in \bigcup_{i\in\mathbb{N}} I_i$، پس $b \in \mathbb{N}$ وجود دارد که $b \in I_n$. بنابراین $\langle b\rangle \subseteq I_n$ پس $I_n = \langle b\rangle$. یعنی در زنجیر $I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots$ داریم: $I_n = I_{n+1} = \cdots$ یعنی زنجیر فوق ایستا است. □

به حلقه‌ای که در آن هیچ زنجیر صعودی نامتناهی از ایده‌آل‌ها وجود نداشته باشد یک حلقه‌ی نوتری گفته می‌شود.

قضیه ۵۰. فرض کنید D یک حوزه ایده‌آل اصلی باشد. در این صورت هر عنصر $a \in D$ به صورت یکتا به عوامل تحویل‌ناپذیر تجزیه می‌شود (یعنی برای هر $a \in D$ عوامل تحویل‌ناپذیر $p_1, \ldots, p_n$ موجودند به طوری که $a = p_1\cdots p_n$ و اگر $a = s_1\cdots s_m$ و s_iها تحویل‌ناپذیر باشند، آنگاه $n = m$ و برای هر $i \in \{1, \ldots, m\}$ یک عنصر $j \in \{1, \ldots, n\}$ موجود است به طوری که $s_i = up_j$. یعنی هر حوزه ایده‌آل اصلی یک حوزه تجزیه یکتاست).

اثبات. ابتدا وجود تجزیه را ثابت می‌کنیم، فرض کنید $a \in D$ یک عنصر غیر یکه باشد. اگر a تحویل‌پذیر باشد آنگاه $a = a_1a_2$. اگر a_1 به صورت $a_1 = a_3a_4$ تحویل‌پذیر باشد، آنگاه $a = a_3a_4a_2$. اگر a_2 به صورت $a_2 = a_5a_6$ تحویل‌پذیر باشد، آنگاه $a = a_3a_4a_5a_6$. اگر این روند نامتناهی بار ادامه پیدا کند، یک زنجیر صعودی از ایده‌آل‌ها در حلقه‌ی D به صورت زیر داریم

$$\langle a\rangle \subsetneqq \langle a_1\rangle \subsetneqq \langle a_3\rangle \subsetneqq \langle a_5\rangle \subsetneqq \cdots$$

توجه شود که عنصر $a \in D$ را تحویل‌ناپذیر می‌نامیم هرگاه برای هر $b \in D$ اگر $b|a$ آنگاه $b = u$ یا $b = au$ که u یک عنصر یکه است. به بیان دیگر برای هر $b \in D$ اگر $b|a$ آنگاه

$\langle b\rangle = D$ یا $\langle b\rangle = \langle a\rangle$. پس عنصر $a \in D$ تحویل‌پذیر است هرگاه $b \in D$ موجود باشد به طوری که $\langle b\rangle \neq D$ و $\langle b\rangle \neq \langle a\rangle$ و $b|a$. به بیان دیگر $\langle a\rangle \subsetneq \langle b\rangle$. پس زنجیر فوق اکیدا صعودی است. اما در لم قبل ثابت کردیم که در یک حوزه ایده‌آل اصلی، هیچ زنجیر صعودی از ایده‌آل‌ها نداریم. بنابراین با اجرای روند فوق به یک تجزیه‌ی a به عوامل تحویل‌ناپذیر می‌رسیم. حال به اثبات یکتایی تجزیه می‌پردازیم. فرض کنید $a = p_1 \cdots p_n$ و $a = q_1 \cdots q_m$، پس $p_1 \cdots p_n = q_1 \cdots q_m$، بدون کاستن از کلیت فرض کنید $p_1|q_1$ پس $p_1 = uq_1$. بنابراین $uq_1 \cdots p_n = q_1 \cdots q_m$ پس $up_2 \cdots p_n = q_2 \cdots q_m$. دوباره بدون کاستن از کلیت فرض کنید $p_2 = u'q_2$، پس $uu'p_3 \cdots p_n = q_3 \cdots q_m$. با ادامه روند فوق نتیجه می‌گیریم که برای هر i یک j وجود دارد که $p_i = uq_j$ و اگر $n \neq m$ برای مثال فرض کنید $m > n$ در اینصورت یکی از p_iها تحویل‌پذیر می‌شود و این خلاف تحویل‌ناپذیری آن‌ها است. □

۷ جلسات هفتم و هشتم: حلقه‌ی چندجمله‌ای‌ها و توسیع‌های ساده

فرض کنید K یک میدان باشد. حلقه‌ی چندجمله‌ای‌های با تک متغیر x روی میدان K که آن‌را با $K[x]$ نشان می‌دهیم از عناصری به صورت زیر تشکیل می‌شود.

$$K[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \mathbb{N}, a_i \in K\}$$

هر عنصر در $K[x]$ را یک چندجمله‌ای با ضرایب در K می‌نامیم. اگر $f \in K[x]$ به صورت زیر باشد،

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

که $a_n \neq 0$، می‌گوییم f یک چندجمله‌ای با درجه n است و می‌نویسیم $\deg f = n$. توجه شود که

$$\deg f = 0 \Leftrightarrow f \in K$$

و درجه 0_K را به صورت $\deg 0 = -\infty$ تعریف می‌کنیم.

تعریف جمع: فرض کنید $f, g \in K[x]$ که $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ و $g =$

$b_0 + b_1x + a_2x^2 + \cdots + b_mx^m$. در اینصورت جمع را به صورت زیر تعریف می‌کنیم (فرض کنید $m > n$)

$$f + g = (a_0 + b_0) + (a_1 + b_1)x + \cdots (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_mx^m$$

توجه شود که $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.

تعریف ضرب: فرض کنید $f, g \in K[x]$ که $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ و $g = b_0 + b_1x + a_2x^2 + \cdots + b_mx^m$. در اینصورت ضرب را به صورت زیر تعریف می‌کنیم:

$$f \cdot g = c_0 + c_1x + c_2x^2 + \cdots + c_{n+m}x^{n+m})$$

که

$$\begin{aligned} c_0 &= a_0b_0 \\ c_1 &= a_0b_1 + a_1b_0 \\ c_2 &= a_0b_2 + a_1b_1 + a_2b_0 \\ &\vdots \end{aligned}$$

بنابراین $\deg(f \cdot g) = \deg(f) + \deg(g)$.

توجه شود که $K[x]$ یک حلقه است که صفر (یک) این حلقه همان صفر(یک) K است. همچنین $K[x]$ یک حوزه صحیح است یعنی اگر $f, g \in K[x]$ و $f \cdot g = 0$، آنگاه $f = 0$ یا $g = 0$. چون اگر $f \cdot g = 0$، آنگاه $\deg(f \cdot g) = -\infty$. پس $\deg(f) + \deg(g) = -\infty$ بنابراین $\deg(f) = -\infty$ یا $\deg(g) = -\infty$ پس یا $f = 0$ یا $g = 0$.

لم ۵۱. فرض کنید $f, g \in K[x]$. $0 \neq g$. در این صورت چندجمله‌ای‌های یکتای $s(x)$ و $r(x)$ موجودند به طوری که $f(x) = g(x)s(x) + r(x)$ و $\deg(r(x)) < \deg(g(x))$.

اثبات. با استقرا روی درجه‌ی چندجمله‌ای f. فرض کنید $\deg(f) = 0$ یعنی $f = a \in K$. در این صورت دو حالت داریم: فرض کنید $\deg(g) = 0$. یعنی $g = b \in K$ پس $a = b \cdot \frac{a}{b} + 0$ که $\deg(0) = -\infty < \deg(b) = 0$. حال فرض کنید $\deg(g) > 0$، در این صورت $a = 0 \cdot g + a$ که $\deg(a) = 0 < \deg(g)$.

فرض کنید حکم مورد نظر برای تمام چندجمله‌های با درجه کمتر از n برقرار باشد. چند جمله‌ای f را در نظر بگیرید به طوری که $\deg(f) = n$. اگر $\deg(g) > \deg(f)$، آنگاه $f = 0 \cdot g + f$. اگر $\deg(g) \leq \deg(f)$، فرض کنید $f = a_0 + a_1 x + \cdots + a_n x^n$ و $g = b_0 + b_1 x + \cdots + b_m x^m$ که $m \leq n$. در این صورت $\frac{a_n}{b_m} x^{n-m} g = h + a_n x^n$ بنابراین $f - \frac{a_n}{b_m} x^{n-m} g = h$ که h یک چندجمله‌ای با درجه کمتر از n است. بنابر فرض استقرا $h = kg + r$ که $\deg(r) \leq \deg(g)$.
پس $f = \frac{a_n}{b_m} x^{n-m} g + kg + r = gH + r$ که $\deg(r) \leq \deg(g)$.
برای اثبات یکتایی فرض کنید $f = gs + r$ و $f = gs' + r'$ که $\deg(r), \deg(r') \leq \deg(g)$.
در اینصورت $gs + r = gs' + r'$ پس $g(s - s') = r' - r$ و این امکان‌پذیر نیست چون درجه‌های دو طرف تساوی با هم برابر نیست. پس $r = r'$ و $s = s'$. □

قضیه ۵۲. $K[x]$ یک حلقه اقلیدسی است.

اثبات. تابع $\delta : K[x] \to \mathbb{N}$ را به صورت $\delta(f) = 2^{\deg(r)}$ تعریف کنید که $2^{-\infty} = 0$. با توجه به لم قبل حلقه‌ی $K[x]$ یک حلقه‌ی اقلیدسی است. □

از قضیه قبل می‌توان نتیجه گرفت که عناصر $K[x]$ به عوامل تحویل‌ناپذیر تجزیه می‌شوند. هر دو عنصر $K[x]$ دارای ب.م.م هستند. هر ایده‌آل $K[x]$ به صورت $\langle f \rangle$ است.

مشاهده: عناصر وارون‌پذیر در $K[x]$ به چه صورت هستند؟ تنها عناصر وارون‌پذیر در $K[x]$ عناصر میدان K هستند چون اگر $f, g \in K[x]$ به طوری که $f \cdot g = 1$، آنگاه چون $\deg(1) = 0$ پس $\deg(f) = \deg(g) = 0$ بنابراین $f, g \in K$.

مشاهده: $K[x]$ یک حوزه‌ی صحیح است. میدان کسرهای $K[x]$ را با $K(x)$ نشان می‌دهیم و این میدان از عناصری به صورت $\frac{f}{g}$ تشکیل شده است که $f, g \in K[x]$.
عناصر تحویل‌ناپذیر در $K(x)$ به چه صورتی هستند؟

مشاهده: فرض کنید $f \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر باشد. در اینصورت f در K هیچ ریشه‌ای ندارد یعنی برای هر $\beta \in K$ داریم: $f(\beta) \neq 0$.

لم ۵۳. فرض کنید $f \in K[x]$ و $\beta \in K$ در اینصورت $f = (x - \beta)h \Leftrightarrow (x - \beta) | f \Leftrightarrow f(\beta) = 0$ که $h \in K(x)$.

اثبات. فرض کنید $f(\beta) = 0$. بنابر الگوریتم تقسیم $f = (x-\beta)h(x) + r$ که $r \in K$. از طرفی $f(\beta) = 0$ پس $r = 0$ و در نتیجه $f = (x-\beta)h(x)$. اگر $f = (x-\beta)h(x)$، واضح است که $f(\beta) = 0$. □

بنابراین اگر $f \in K[x]$ تحویل‌ناپذیر باشد، آنگاه f در K ریشه ندارد. اما عکس این مطلب برقرار نیست. یعنی اینگونه نیست که اگر یک چندجله‌ای در K ریشه ندارد حتما تحویل‌ناپذیر باشد. برای مثال در $\mathbb{R}[x]$ چندجمله‌ای $f = (x^2+1)(x^2+x+2)$ در $\mathbb{R}$ ریشه ندارد اما تحویل‌پذیر است.

سوال: فرض کنید $f \in K[x]$ تحویل‌ناپذیر باشد. آیا میدان $K \subseteq L$ موجود است که در میدان L چندجمله‌ای f دارای ریشه باشد؟

مشاهده: فرض کنید $f \in K[x]$ تحویل‌ناپذیر باشد. در اینصورت $\frac{K[x]}{\langle f \rangle}$ یک میدان است (بررسی کنید چرا؟). از طرفی یک نشاندن $\varphi : K \to \frac{K[x]}{\langle f \rangle}$ موجود است که $\varphi(r) = r + \langle f \rangle$. به راحتی ثابت می شود که φ یک همریختی یک‌به‌یک است. اگر $a + \langle f \rangle = b + \langle f \rangle$، آنگاه $f | a-b$. چون $a-b$ از درجه صفر است پس باید درجه f نیز صفر باشد و این با تحویل‌ناپذیری f در تناقض است.

چندجمله‌ای تحویل‌ناپذیر $f(x) = a_0 + a_1x + a_2x^2 \in K[x]$ و میدان $L = \frac{K[x]}{\langle f \rangle}$ را در نظر بگیرید. ادعا می‌کنیم تصویر چندجمله‌ای f در $L[x]$ دارای یک ریشه در L است. یکی از ریشه‌های این چندجمله‌ای عنصر $x + \langle f \rangle$ است زیرا:

$$\begin{aligned} f(x+\langle f\rangle) &= (a_0+\langle f\rangle) + (a_1+\langle f\rangle)(x+\langle f\rangle) + (a_2+\langle f\rangle)(x+\langle f\rangle)^2 \\ &= a_0 + \langle f\rangle + a_1x + \langle f\rangle + (a_2+\langle f\rangle)(x^2+\langle f\rangle) \\ &= (a_0+\langle f\rangle) + (a_1x+\langle f\rangle) + (a_2x^2+\langle f\rangle) \\ &= a_0 + a_1x + a_2x^2 + \langle f\rangle \\ &= 0_L \end{aligned}$$

به طور خلاصه، اگر $f \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر باشد، آنگاه میدان $K \subseteq L$ موجود می‌باشد به طوری که f در L دارای حداقل یک ریشه است.

فرض کنید $f \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر روی K باشد. فرض کنید میدان $K \subseteq L$ به

گونه‌ای باشد که عنصر $\beta \in L$ موجود باشد که $f(\beta) = 0$. میدان تولید شده توسط K و β در داخل L به چه صورت است؟

مشاهده: در میان چندجمله‌های موجود در $K[x]$ که در β صفر هستند، چندجمله‌ای f دارای حداقل درجه است. فرض کنید که β ریشه‌ی چندجمله‌ای $g \in K[x]$ باشد و g حداقل درجه را داشته باشد. در اینصورت $f = gh + r(x)$ که $\deg(r) < \deg(g)$. بنابراین $r(\beta) = 0$ پس $r = 0$. در اینصوت $f = gh$ اما f تحویل‌ناپذیر است.

نگاشت $\varphi : K[x] \to L$ که $\varphi(h(x)) = h(\beta)$ را در نظر بگیرید. به راحتی بررسی می‌شود که این نگاشت یک همریختی است. تصویر φ در L به صورت زیر است:

$$\mathrm{Im}(\varphi) = \{h(\beta) | h \in K[x]\} = K[\beta]$$

هسته‌ی φ به صورت زیر است:

$$\mathrm{Ker}(\varphi) = \{h \in K[x] | h(\beta) = 0\}$$

توجه کنید که اگر $h \in K[x]$ و $h(\beta) = 0$، آنگاه $f|h$. طبق الگوریتم تقسیم $h(x) = f(x)s(x) + r(x)$ که $\deg(r) < \deg(f)$. چون $h(\beta) = 0$ پس $r(\beta) = 0$. اما $\deg(r) < \deg(f)$ و از طرفی f در میان چندجمله‌ای‌هایی که در β صفر می‌شوند کمترین درجه را دارد. بنابراین $r = 0$ یعنی $h = fs$ پس $f|h$. بنابراین اگر $h \in K[x]$ و $h(\beta) = 0$ آنگاه $h \in \langle f \rangle$.

در نتیجه $\mathrm{Ker}(f) = \langle f \rangle$. بنابراین $\mathrm{Im}(\varphi) = K[\beta] \simeq \dfrac{K[x]}{\langle f \rangle}$. بنابراین نتایج زیر را داریم:

۱. $K[\beta]$ یک میدان است.

۲. $K[\beta]$ کوچکترین میدان شامل K و β در داخل L است. پس میدان تولید شده توسط K و β در داخل L با $\dfrac{K[x]}{\langle f \rangle}$ ایزومرف است.

۳. فرض کنید L_1 و L_2 دو میدان شامل K باشند و $f \in K[x]$ تحویل‌ناپذیر باشد. فرض کنید $\beta_1 \in L_1$ و $\beta_2 \in L_2$ موجود باشند که در L_1، $f(\beta_1) = 0$ و در L_2، $f(\beta_2) = 0$. در اینصورت $K(\beta_1) = K(\beta_2) \simeq \dfrac{K[x]}{\langle f \rangle}$. یعنی میدان تولید شده توسط K و β_1 در L_1 با میدان تولید شده توسط K و β_2 در L_2 برابر است.

۴. فرض کنید دو میدان K_1 و K_2 با هم یکریخت هستند یعنی یکریختی $\sigma : K_1 \to K_2$ وجود دارد و $K_1 \subseteq L_1$ و $K_2 \subseteq L_2$. فرض کنید $f = a_0 + a_1x + a_2x^2 \in K_1[x]$ تحویل‌ناپذیر باشد، در اینصورت

$$\sigma(f) = \sigma(a_0) + \sigma(a_1)x + \sigma(a_2)x^2 \in K_2[x]$$

حال فرض کنید $\beta_1 \in L_1$ ریشه‌ی f در L_1 باشد و $\beta_2 \in L_2$ ریشه‌ی $\sigma(f)$ در L_2 باشد. در اینصورت

$$\frac{K_1[x]}{\langle f\rangle} \simeq K_1(\beta_1) \simeq K_2(\beta_2) \simeq \frac{K_2[x]}{\langle f\rangle}$$

به عنوان تمرین نشان دهید که اگر $f = a_0 + \ldots + a_nx^n$ در $K_1[x]$ تحویل‌ناپذیر باشد، آن‌گاه $\sigma(f) = \sigma(a_0) + \ldots + \sigma(a_n)x^n$ در $K_2[x]$ تحویل‌ناپذیر است.

۵. فرض کنید $f \in K[x]$ تحویل‌ناپذیر باشد. در اینصورت هر میدانی مانند L که حاوی یک ریشه برای f باشد شامل میدان $\frac{K[x]}{\langle f\rangle}$ است.

۶. فرض کنید $K \subseteq L$ و $\beta \in L$ ریشه‌ی چندجمله‌ای تحویل‌ناپذیر $f \in K[x]$ است. در اینصورت

$$K(\beta) = \{\frac{h(\beta)}{g(\beta)} | h, g \in K[x]\} = K[\beta] = \{a_0 + \ldots + a_n\beta^n | n \in \mathbb{N}, a_i \in K\}$$

بنابرین معکوس عناصری مانند $a_0+\ldots+a_n\beta^n$ عناصری به همین صورت هستند. همچنین چون $\frac{K[x]}{\langle f\rangle} \simeq K[\beta]$ پس یکریختی مانند $\sigma : \frac{K[x]}{\langle f\rangle} \to K[\beta]$ وجود دارد که $\sigma(h(x) + \langle f\rangle) = h(\beta)$. توجه کنید که عناصر $\frac{K[x]}{\langle f\rangle}$ به چه صورتی هستند. فرض کنید $\deg(f) = n$ و $h(x) + \langle f\rangle \in \frac{K[x]}{\langle f\rangle}$ در اینصورت $h(x) = f(x)s(x) + r(x)$ که $\deg(r) < \deg(f)$، یعنی در حلقه‌ی $\frac{K[x]}{\langle f\rangle}$، $h(x) \equiv r(x)$ به بیان دیگر عناصر میدان $\frac{K[x]}{\langle f\rangle}$ به صورت $r(x) + \langle f\rangle$ هستند که $\deg(r) < \deg(f)$. بنابراین

$$\frac{K[x]}{\langle f\rangle} = \{r(x) + \langle f\rangle | r(x) \in K[x], \deg(r) < \deg(f)\}$$

از طرفی می‌دانیم که $\frac{K[x]}{\langle f\rangle} \simeq K[\beta]$ پس میدان $K[\beta]$ در حقیقت از عناصری به صورت $r(x) + \langle f\rangle$ تشکیل شده است که $r(x) \in K[x]$ و $\deg(r) < \deg(f)\}$.

۷. فرض کنید $\deg(f) = n$. در اینصورت عناصر $K[\beta]$ به صورت $a_0 + a_1\beta + \ldots +$ $a_{n-1}\beta^{n-1}$ هستند. به بیان دیگر عناصر $K[\beta]$ ترکیبات خطی از $1, \beta, \beta^2, \ldots, \beta^{n-1}$ با ضرایب اسکالر در K هستند. به بیان دیگر $K[\beta]$ یک فضای برداری روی K است که مولدهای آن $1, \beta, \beta^2, \ldots, \beta^{n-1}$ است.

۸ جلسه نهم: توسیع‌های میدانی به عنوان فضاهای برداری

تعریف ۵۴. فرض کنید $K \subseteq L$ دو میدان باشند. عنصر $\alpha \in L - K$ را روی K جبری می‌نامیم هرگاه یک چندجمله‌ای $f \in K[x]$ موجود باشد به طوری که $f(\alpha) = 0$.

مشاهده: فرض کنید $\alpha \in L - K$ روی K جبری باشد. فرض کنید $g(x) \in K[x]$ یک چندجمله‌ای با حداقل درجه باشد به طوری که $g(\alpha) = 0$. در این صورت $g \in K[x]$ تحویل‌ناپذیر است. از طرفی اگر $\alpha \in L - K$ ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر مانند f باشد، آنگاه f حداقل درجه دارد، زیرا اگر $g(\alpha) = 0$ و درجه‌ی g کمتر از f باشد، آنگاه $f = gh + r$. چون $f(\alpha) = 0$ بنابراین $r(\alpha) = 0$ پس $r = 0$. در این صورت $f = gh$ پس f تحویل‌پذیر می‌شود. بنابراین دو جمله زیر با هم معادل هستند:

f یک چندجمله‌ای با حداقل درجه است به طوی که $f(\alpha) = 0$.

f یک چندجمله‌ای تحویل‌ناپذیر است به طوری که $f(\alpha) = 0$.

مشاهده: فرض کنید $\alpha \in L - K$ روی K جبری باشد و α ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر $f \in K[x]$ باشد. در این صورت اگر $g \in K[x]$ به گونه‌ای باشد که $g(\alpha) = 0$ آنگاه $f|g$. بنابراین اگر α ریشه‌ی دو چندجمله‌ای f و g باشد و هر دو با حداقل درجه باشند آنگاه $f|g$ و $g|f$ بنابراین $f = ug$ که u یک عنصر بکه در K است. بنابراین اگر α روی K جبری باشد یک چندجمله‌ای یکتای تحویل‌ناپذیر به صورت $f = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$ موجود است به طوری که $f(\alpha) = 0$. می‌گوییم f چندجمله‌ای مینیمال α روی K است. همچنین در این صورت میدان تولید شده توسط K و α در داخل L یعنی $K(\alpha)$ با $\dfrac{K[x]}{\langle f \rangle}$ یکریخت است.

توجه: فرض کنید $K \subseteq L$ و $\alpha \in L - K$ روی K جبری باشد و $f \in K[x]$ چندجمله‌ای مینیمال α باشد. در این صورت $K \subseteq K(\alpha) \subseteq L$ و هر عنصری که در میدان تولید شده توسط K و α قرار داشته باشد روی K جبری است.

توجه: اگر α و β روی K جبری باشند، آنگاه $\alpha+\beta$ و $\alpha\cdot\beta$ نیز روی K جبری هستند.

تمرین ۷. فرض کنید $K\subseteq L$ و $\alpha\in L-k$. فرض کنید f چندجمله‌ای مینیمال α باشد. می‌دانیم که

$$K[\alpha]=\{a_0+a_1x+\ldots+a_{n-1}x^{n-1}\}.$$

اگر $h(\alpha)\in K[\alpha]$، آنگاه معکوس $h(\alpha)$ در میدان $K[\alpha]$ چیست؟

تعریف ۵۵. فرض کنید $K\subseteq L$ دو میدان باشند. عنصر $\alpha\in L-K$ را روی K غیرجبری یا متعالی می‌نامیم هرگاه α روی K جبری نباشد.

قضیه ۵۶. اگر $K\subseteq L$ یک توسیع میدانی باشد و $\alpha\in L-K$ یک عنصر متعالی روی K باشد. در اینصورت میدان تولید شده توسط K و α در داخل L ایزومرف است با میدان $K(x)$ (میدان کسرهای $K[x]$).

اثبات. نگاشت $\varphi:K(x)\to L$ که $\varphi(\frac{f(x)}{g(x)})=\frac{f(\alpha)}{g(\alpha)}$ را در نظر بگیرید. به عنوان تمرین نشان دهید که φ یک همریختی یک‌به یک است. ادعا میکنیم که $\mathrm{Ker}(\varphi)=\{0\}$. اگر $\frac{f(\alpha)}{g(\alpha)}=0$، در این صورت $f(\alpha)=0$ و این با غیرجبری بودن α در تناقض است، بنابراین f چندجمله‌ای ثابت 0 است. □

مشاهده: فرض کنید $K\subseteq L$ یک توسیع میدانی باشد. در اینصورت L یک فضای برداری روی میدان K است.

تعریف ۵۷. فرض کنید $K\subseteq L$ یک توسیع میدانی باشد. بعد فضای برداری L روی K را با $[L:K]$ نشان می‌دهیم. می‌گوییم توسیع $K\subseteq L$ یک توسیع متناهی است هرگاه $[L:K]$ متناهی باشد.

نتیجه ۵۸. اگر $K\subseteq L$ یک توسیع متناهی باشد، در اینصورت تمامی عناصر $\alpha\in L$ روی K جبری هستند.

اثبات. فرض کنید $\alpha\in L-K$ روی K متعالی باشد. در اینصورت عناصر $\{1,\alpha,\alpha^2,\ldots\}$ روی K مستقل خطی هستند چون α ریشه‌ی هیچ چندجمله‌ای نیست. یعنی $[L:K]$ نامتناهی است. توجه شود که عکس این نتیجه لزوما درست نیست. □

مشاهده: فرض کنید $K \subseteq L$ و $\alpha \in L - K$ روی K جبری باشد و f چندجمله‌ای مینیمال α باشد که درجه آن n است. در اینصورت $[K(\alpha) : K]$ چیست؟ با توجه به اینکه عناصر $K(\alpha)$ به صورت $a_0 + a_1\alpha + \ldots + a_n\alpha^{n-1}$ هستند، پس تمامی عناصر $K(\alpha)$ توسط پایه‌ی $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ تولید می‌شوند. توجه کنید که $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ روی K مستقل خطی هستند چون اگر $a_0 + a_1\alpha + \ldots + a_n\alpha^{n-1} = 0$، آنگاه α ریشه یک چندجمله‌ای با درجه کمتر از n می‌شود و این با فرض در تناقض است. بنابراین $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ پایه‌ای برای فضای برداری $K(\alpha)$ روی K است. پس $[K(\alpha) : K] = n$ یعنی $K \subseteq K(\alpha)$ یک توسیع جبری است یعنی تمامی عناصر $K(\alpha)$ روی K جبری هستند.

نتیجه ۵۹. توسیع $K \subseteq \frac{K[x]}{\langle f \rangle}$ یک توسیع جبری است. یعنی همه عناصر $\frac{K[x]}{\langle f \rangle}$ روی K جبری هستند.

لم ۶۰. فرض کنید $K \subseteq L \subseteq M$. در اینصورت $[M : K] = [M : L] \times [L : K]$.

اثبات. فرض کنید فضای برداری L روی K توسط $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ تولید شده باشند. فرض کنید پایه‌ی M روی L به عنوان فضای برداری، $\{\beta_1, \beta_2, \ldots, \beta_m\}$ باشد. ادعا می‌کنیم $\{\alpha_i\beta_j\}$ که $1 \leqslant i \leqslant n$ و $1 \leqslant j \leqslant m$، پایه‌ای برای فضای برداری M روی K است. فرض کنید $z \in M$، در اینصورت $z = r_1\beta_1 + r_2\beta_2 + \ldots + r_m\beta_m$ که $r_i \in L$. از طرفی هر عنصر $r_i \in L$ توسط $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ تولید می‌شود. پس z ترکیبی خطی از $\alpha_i\beta_j$ها می‌باشد. حال نشان می‌دهیم $\{\alpha_i\beta_j\}$ مستقل خطی هستند. فرض کنید یک ترکیب خطی از $\alpha_i\beta_j$ها صفر شود، برای مثال فرض کنید $r_1\alpha_1\beta_1 + r_2\alpha_2\beta_1 + r_3\alpha_3\beta_2 = 0$ در اینصورت $(r_1\alpha_1 + r_2\alpha_2)\beta_1 + (r_3\alpha_3)\beta_2 = 0$ اما β_jها مستقل خطی‌اند پس $r_1\alpha_1 + r_2\alpha_2 = 0$ و $r_3\alpha_3 = 0$. چون α_iها مستقل خطی‌اند پس $r_1 = r_2 = r_3 = 0$. □

نتیجه ۶۱. فرض کنید $K \subseteq L$ و $\beta_1, \beta_2 \in L$ روی K جبری باشند. در اینصورت $\beta_1 + \beta_2$ و $\beta_1 \cdot \beta_2$ نیز روی K جبری هستند.

اثبات. توجه کنید که $K \subseteq K(\beta_1)$ یک توسیع جبری است یعنی $[K(\beta_1) : K]$ متناهی است. از طرفی β_2 روی K جبری است. بنابراین β_2 روی $K(\beta_1)$ نیز جبری است. پس $[K(\beta_1)(\beta_2) : K(\beta_1)]$ متناهی است. در نتیجه $[K(\beta_1)(\beta_2) : K] = [K(\beta_1)(\beta_2) : K(\beta_1)] \times [K(\beta_1) : K]$

متناهی است. بنابراین $K(\beta_1)(\beta_2)$ یعنی $K(\beta_1, \beta_2)$ یک توسیع متناهی از K است. بنابراین همه عناصر موجود در $K(\beta_1, \beta_2)$ از جمله $\beta_1 + \beta_2$ و $\beta_1 \cdot \beta_2$ روی K جبری هستند. □

نتیجه ۶۲. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. قرار دهید $M = \{\alpha \in L | \alpha$روی$K$جبری است$\}$ در اینصورت M یک میدان است $(K \subseteq M \subseteq L)$.

اثبات. فرض کنید $\alpha_1, \alpha_2 \in M$. در اینصورت $\alpha_1 + \alpha_2 \in K(\alpha_1, \alpha_2)$ و $\alpha_1 \cdot \alpha_2^{-1}$ و از این رو این عناصر روی K جبری هستند پس در M قرار دارند. □

قضیه ۶۳. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد به طوری که $[L : K]$ متناهی باشد. در اینصورت عناصر جبری $\alpha_1, \ldots, \alpha_n \in L$ موجودند به طوری که $L = K(\alpha_1, \ldots, \alpha_n)$ یعنی L برابر است با میدان تولید شده توسط K و $\alpha_1, \ldots, \alpha_n$ در داخل L.

اثبات. فرض کنید $\alpha_1 \in L - K$. بنابراین α_1 روی K جبری است. بنابراین $K \subseteq K(\alpha_1) \subseteq L$ و α_1 ریشه‌ی یک چندجمله‌ای با درجه‌ی بیش از 1 است چون اگر $x - \alpha_1 = 0$، آنگاه $\alpha_1 \in K$. پس $[K(\alpha_1) : K] \geqslant 2$. اگر $K(\alpha_1) = L$ که حکم ثابت می‌شود. در غیر اینصورت فرض کنید $\alpha_2 \in L - K(\alpha_1)$، در اینصورت $[K(\alpha_1, \alpha_2) : K(\alpha_1)] \geqslant 2$ و $K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq L$. بنابراین $[L : K] \geqslant 4$. این روند پس از انتخاب $\alpha_1, \ldots, \alpha_n$ متوقف می‌شود و $L = K(\alpha_1, \ldots, \alpha_n)$. □

۹ جلسه دهم: میدان شکافنده

فرض کنید f یک چندجمله‌ای تحویل‌ناپذیر در $K[x]$ باشد. فرض کنید L_1 و L_2 دو توسیع میدانی K باشند و $\alpha \in L_1$ و $\beta \in L_2$ ریشه‌های f به ترتیب در L_1 و L_2 باشند. در اینصورت $K(\alpha) \cong K(\beta)$. یعنی ایزومرفیسم $\sigma : K(\alpha) \to K(\beta)$ موجود است که حافظ K است و $\sigma(\alpha) = \beta$.

نتیجه: اگر $f \in K[x]$ تحویل‌ناپذیر باشد. میدان تولید شده توسط K و یک ریشه دلخواه f در یک توسیع میدانی یکتاست.

مشاهده: فرض کنید $\sigma : K_1 \to K_2$ یک ایزومرفیسم باشد و $f \in K_1[x]$ تحویل‌ناپذیر باشد. فرض کنید

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

در این صورت $\sigma(f(x)) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$ که $\sigma(a_i) = b_i$. در اینصورت $\sigma(f(x))$ در $K_2[x]$ تحویل‌ناپذیر است.

مشاهده: فرض کنید $\sigma : K_1 \to K_2$ یک ایزومرفیسم باشد و $K_1 \subseteq L_1$ و $K_2 \subseteq L_2$. فرض کنید $f \in K_1[x]$ تحویل‌ناپذیر باشد. در این صورت $\sigma(f(x))$ در $K_2[x]$ تحویل‌ناپذیر است. اگر $\alpha \in L_1$ و $\beta \in L_2$ ریشه‌های f باشند، در این صورت $K_1(\alpha) \cong K_2(\beta)$.

تعریف ۶۴. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. می‌گوییم این توسیع جبری است هرگاه هر عنصر $\alpha \in L - K$ ریشه‌ی یک چندجمله‌ای با ضرایب در K باشد.

قضیه ۶۵. فرض کنید توسیع $K \subseteq L$ جبری باشد و همچنین $L \subseteq M$ نیز جبری باشد. در این صورت توسیع $K \subseteq M$ جبری است.

اثبات. فرض کنید $\alpha \in M$. اگر $\alpha \in L$، آنگاه چون توسیع $K \subseteq L$ جبری است پس α روی K جبری است. فرض کنید $\alpha \in M - L$، در اینصورت چندجمله‌ای تحویل‌ناپذیر $a_0 + a_1x + \ldots + a_nx^n \in L[x]$ موجود است که $f(\alpha) = 0$. به بیان دیگرعنصر α روی میدان $L' = K(a_0, a_1, \ldots, a_n)$ جبری است. بنابراین $[L'(\alpha) : L']$ یک توسیع جبری متناهی است. از طرفی درجه‌ی توسیع $[L' = K(a_0, a_1, \ldots, a_n) : K]$ نیز متناهی است. بنابراین $[L'(\alpha) : K]$ یک توسیع متناهی است یعنی α روی K جبری است. □

فرض کنید K یک میدان باشد و $f \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر باشد. آیا میدان $K \subseteq L$ موجود است که در آن تمامی ریشه‌های f قرار داشته باشند.

فرض کنید $K \subseteq L$ یک میدان باشد که همه‌ی ریشه‌های f در آن قرار داشته باشند. چندجمله‌ای f چند ریشه می‌تواند داشته باشد؟

فرض کنید $f \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر باشد. می‌دانیم میدان $K \subseteq L_1$ موجود است که در میدان $L_1 = \frac{K[x]}{\langle f \rangle}$، چندجمله‌ای f حداقل یک ریشه دارد، فرض β ریشه‌ی f در L_1 باشد. همچنین $[L_1 : K] = n$ که n درجه‌ی f است. در میدان L_1 داریم: $f = (x - \beta)h(x)$. اگر ریشه‌های $h(x)$ همه در L_1 باشند، به میدان مورد علاقه خود رسیده‌ایم. چندجمله‌ای $h(x)$ را در $L_1[x]$ به عوامل تحویل‌ناپذیر تجزیه کنید. فرض کنید $h_1(x)$ یک عامل تحویل‌ناپذیر از $h(x)$ است. میدانی به صورت $L_1 \subseteq L_2$ پیدا می‌شود که در آن $h_1(x)$ دارای ریشه است. دقت کنید که

$[L_2 : L_1] \leq n-1$. با انجام این روش به یک میدان $K \subseteq L$ می‌رسیم که $[L : K] \leq n!$ و در L تمامی ریشه‌های f قرار دارند.

توجه: همین استدلال برای هر f کار می‌کند. اگر f تحویل‌ناپذیر باشد، آنگاه f را به عوامل تحویل‌ناپذیر تجزیه میکنیم.

تعریف ۶۶. فرض کنید $f \in K[x]$ و $K \subseteq L$ به‌گونه‌ای باشد که در L همه‌ی ریشه‌های f قرار داشته باشد و $S \subseteq L$ همه‌ی ریشه‌های f در L باشد. میدان $K(S)$ را یک میدان شکافنده‌ی[۲] f می‌نامیم.

قضیه ۶۷. فرض کنید L_1 و L_2 دو میدان شامل K باشند به طوری که هم در L_1 و هم در L_2 تمامی ریشه‌های $f \in K[x]$ وجود داشته باشند. در این صورت میدان شکافنده‌ی f در L_1 با میدان شکافنده‌ی f در L_2 ایزومرف است.

اثبات. فرض کنید $K(S_1)$ میدان شکافنده‌ی f در L_1 و $K(S_2)$ میدان شکافنده‌ی f در L_2 باشند. فرض کنید $\alpha_1 \in S_1$، در اینصورت α_1 ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر $g \in K[x]$ است. در این صورت $K(\alpha_1) \cong \frac{K[x]}{\langle g \rangle}$. بنابراین عنصر $\beta_1 \in S_2$ موجود است که ریشه‌ی g است. بنابراین $K(\beta_1) \cong \frac{K[x]}{\langle g \rangle} \cong K(\alpha_1)$. حال عنصر $\alpha_2 \in S_1 \setminus \{\alpha_1\}$ را در نظر بگیرید. عنصر α_2 روی K جبری است، پس α_2 روی $K(\alpha_1)$ جبری است. بنابراین چندجمله‌ای تحویل‌ناپذیر $g \in K(\alpha_1)[x]$ موجود است به طوری که α_2 ریشه‌ی آن است. بنابراین $K(\alpha_1, \alpha_2) = \frac{K(\alpha_1)[x]}{\langle g \rangle}$. از طرفی $K(\alpha_1) \cong K(\beta_1)$ و تصویر g روی $K(\beta_1)$ تحویل‌ناپذیر است بنابراین دارای یک ریشه β_2 است و در نتیجه

$$K(\alpha_1, \alpha_2) \cong K(\beta_1, \beta_2)$$

بنابراین با ادامه این فرایند به این نتیجه میرسیم که $K(S_1) \cong K(S_2)$. □

نتیجه ۶۸. اگر $f \in K[x]$ یک چندجمله‌ای باشد، آنگاه یک میدان شکافنده‌ی f موجود است و آن کوچکترین میدان شامل K است که در آن همه ریشه‌های f قرار دارند. اگر H_1 و H_2 دو میدان شکافنده‌ی f باشند، آنگاه روی K داریم که $H_1 \cong H_2$. یعنی یک ایزومرفیسم $h : H_1 \to H_2$ موجود است به طوری که برای هر $a \in K$ داریم: $h(a) = a$.

[2] Splitiing filed

قضیه ۶۹. فرض کنید $K \subseteq L$ میدان شکافنده‌ی یک چندجمله‌ای $f \in K[x]$ باشد. فرض کنید $g \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر دلخواه باشد. در این صورت یا تمام ریشه‌های g در L هستند یا g در L هیچ ریشه‌ای ندارد. به بیان دیگر هر چندجمله‌ای $g \in K[x]$ اگر یک ریشه در L داشته باشد، آن‌گاه تمام ریشه‌هایش در L است.

اثبات. فرض کنید $g \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر دلخواه باشد که یک ریشه‌ی α در L دارد، میدان $K(\alpha)$ را در نظر بگیرید. فرض کنید $L \subseteq H$ میدان شکافنده‌ی f و g باشد. فرض کنید $\beta \in H$ ریشه‌ی دیگری برای g باشد. در اینصورت روی K داریم: $K(\alpha) \cong K(\beta)$ و $[K(\alpha) : K] = [K(\beta) : K]$. توجه کنید که L میدان شکافنده‌ی f روی $K(\alpha)$ نیز است. از طرفی $L(\beta)$ میدان شکافنده‌ی f روی $K(\beta)$ است. بنابراین $L(\beta) \cong L$. پس

$$[L(\beta)] : K(\beta)] = [L : K(\alpha)]$$

در نتیجه $[L(\beta)] : K] = [L : K]$. بنابراین $[L(\beta)] : L] \times [L : K] = [L : L] \times [L : K]$ بنابراین

$$[L(\beta)] : L] = [L : L] = 1$$

پس $L \subseteq L(\beta)$ و $[L(\beta)] : L] = 1$. یعنی $L(\beta) = L$ پس $\beta \in L$. □

تمرین ۸. فرض کنید $\sigma : K \to K'$ ایزومرف باشد و $f \in K[x]$ باشد. نشان دهید میدان شکافنده‌ی f روی K با میدان شکافنده‌ی $\sigma(f)$ روی K' ایزومرف است.

۱۰ جلسه یازدهم: بستار جبری

تعریف ۷۰. توسیع $K \subseteq L$ را یک توسیع نرمال [۳] می‌نامیم هرگاه هر چندجمله‌ای تحویل‌ناپذیر $g \in K[x]$ که در L یک ریشه داشته باشد به طور کامل در L شکافته شود.

قضیه ۷۱. فرض کنید $K \subseteq L$ یک توسیع نرمال متناهی باشد (متناهی بودن یعنی $[L : K] < \infty$)، در این صورت L میدان شکافنده‌ی یک چندجمله‌ای $f \in K[x]$ است.

[3] Normal extension

اثبات. از آنجا که $K \subseteq L$ یک توسیع متناهی است، توسیع $K \subseteq L$ جبری است. عنصر $\alpha \in L - K$ را در نظر بگیرید. α ریشه یک چندجمله‌ای تحویل‌ناپذیر $f \in K[x]$ است. بنابراین تمامی ریشه‌های چندجمله‌ای f در L قرار دارند. فرض کنید S مجموعه تمامی ریشه‌های f در L باشد. در این صورت $K \subseteq K(S)$ یک توسیع متناهی است و $K(S) \subseteq L$. اگر $K(S) = L$ که حکم ثابت می‌شود. اگر $\beta \in L - K(S)$، آنگاه β روی $K(S)$ جبری است. فرض کنید g چندجمله‌ای مینیمال β روی $K(S)$ باشد. پس $K \subseteq K(S) \subseteq K(S \cup S')$ که S' مجموعه‌ی سایر ریشه‌های g است. این کار را نمی‌توان نامتناهی مرحله انجام داد. بنابراین L میدان شکافنده‌ی یک چندجمله‌ای روی K است. □

تعریف ۷۲. اگر S یک مجموعه از چندجمله‌ها با ضرایب در K باشد، آنگاه میدان شکافنده‌ی S نیز به طور مشابه قابل تعریف است.

سوال: آیا میدان شکافنده‌ی تمامی چندحمله‌ای‌های $f \in K[x]$ وجود دارد؟
فرض کنید $K \subseteq L$ موجود باشد به طوری که L میدان شکافنده‌ی تمامی چندجمله‌ای‌های موجود در $K[x]$ است. در این صورت

(۱) L یک توسیع جبری از K است. چون $L = K(S)$ که S ریشه‌های همه چندجمله‌های موجود در $K[x]$ است. بنابراین اگر $\alpha \in L$، آنگاه $\alpha \in K(S)$ بنابراین $\alpha \in K(\alpha_1, \ldots, \alpha_n)$ پس α روی K جبری است.

(۲) هیچ توسیع جبری L' که $K \subseteq L \subsetneq L'$ وجود ندارد. زیرا اگر همچین L' وجود داشته باشد، آنگاه L' توسیع جبری K است. بنابراین $L \subseteq L'$. در واقع اگر $K \subseteq L$ یک میدان شکافنده‌ی تمام چندجمله‌ای‌های موجود در $K[x]$ باشد، آنگاه هر چندجمله‌ای در $L[x]$ ریشه‌هایش در خود L است. به بیان دیگر L بسته جبری است.

تعریف ۷۳. میدان L را بسته جبری می‌نامیم هرگاه همه چندجمله‌ای‌های موجود در $L[x]$ همه ریشه‌هایشان در خود L باشد. به بیان دیگر هر چندجمله‌ای در $L[x]$ در L شکافته شود.

خلاصه: اگر $K \subseteq L$ میدان شکافنده‌ی همه چندجمله‌های موجود در $K[x]$ باشد، آنگاه اولاً L یک توسیع جبری K است دوماً L بسته جبری است.

تعریف ۷۴. میدان $K \subseteq L$ را یک بستار جبری K می‌نامیم هرگاه اولاً $K \subseteq L$ یک توسیع جبری باشد. ثانیاً L بسته جبری باشد.

اگر L میدان شکافنده‌ی همه چندجمله‌های موجود در $K[x]$ باشد، آنگاه L یک بستار جبری K است.

قضیه ۷۵. فرض کنید K یک میدان باشد، یک بستار جبری $K \subseteq L$ وجود دارد.

اثبات. یک مجموعه $K \subseteq S$ را در نظر بگیرید که $|S| > |K| + \aleph_0$. قرار دهید

$$\mathcal{A} = \{L \subseteq S \text{ و } K \subseteq L \text{ به طوری که } L \text{ روی } K \text{ جبری است}\}$$

روی $\mathcal{A}$ ترتیب زیر را در نظر بگیرید:

$$L_1 \leqslant L_2 \iff L_2 \text{ یک توسیع جبری } L_1 \text{ باشد}$$

فرض کنید $\{L_i\}_{i\in I}$ یک زنجیر در $\mathcal{A}$ باشد. در اینصورت $K \subseteq \bigcup L_i$ و $\bigcup L_i$ یک توسیع جبری از K است. یعنی هر زنجیر در $\mathcal{A}$ دارای یک کران بالا در خود $\mathcal{A}$ است. از این رو S دارای یک عنصر ماکزیمال است به نام $K \subseteq M$. ادعا میکنیم M هیچ توسیع جبری ندارد. فرض کنید $M \subseteq N$ یک توسیع جبری M باشد. در این صورت $|N| < |S|$. بنابراین تصویری از N در S پیدا می‌شود. یعنی M دارای یک توسیع جبری در داخل S است. بنابراین هر میدان K دارای یک بستار جبری مانند L است به طوری که $L = |K| + \aleph_0$. □

قضیه ۷۶. هر دو بستار جبری K با هم ایزومرف هستند.

اثبات. فرض کنید $K \subseteq L_1, L_2$ دو بستار جبری K باشند. قرار دهید:

$$\mathcal{A} = \{K \subseteq N \subseteq L_2 \text{ و } K \subseteq M \subseteq L_1 \text{ به طوری که } \sigma : M \to N \text{ همه ایزومرفیسم‌های}\}$$

روی $\mathcal{A}$ ترتیب زیر را در نظر بگیرید: فرض کنید $\sigma_1 : M_1 \to N_1$ و $\sigma_2 : M_2 \to N_2$، در اینصورت

$$(\sigma_1 \subseteq \sigma_2) M_1 \subseteq M_2, N_1 \subseteq N_2 \iff \sigma_1 \leqslant \sigma_2$$

فرض کنید $\{\sigma_i\}_{i\in I}$ که $\sigma_i : M_i \to N_i$ یک زنجیر از ایزومرفیسم‌ها باشد. در اینصورت (به عنوان تمرین نشان دهید که) $\bigcup \sigma_i : \bigcup M_i \to \bigcup N_i$ یک ایزومرفیسم است. بنابراین $\mathcal{A}$ دارای یک عنصر ماکزیمال است. فرض کنید $\sigma : M \to N$ یک ایزومرفیسم ماکزیمال باشد که $M \subseteq L_1$ و $N \subseteq L_2$. ادعا می‌کنیم که $L_1 - M = \emptyset$ و $L_2 - N = \emptyset$. فرض کنید $\alpha \in L_1 - M$، در اینصورت α روی M جبری است. فرض کنید α ریشه چندجمله‌ای تحویل‌ناپذیر $g \in M[x]$ باشد. فرض کنید β ریشه‌ی تصویر g در L_2 باشد. پس ایزومرفیسمی به صورت $\sigma' : M(\alpha) \to N(\beta)$ وجود دارد. بنابراین یک ایزومرفیسم شامل σ پیدا می‌شود و این ماکزیمال بودن σ را نقض می‌کند. □

قضیه ۷۷. فرض کنید K^{alg} بستار جبری K باشد و $g \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر باشد. فرض کنید α, β دو ریشه‌ی g در K^{alg} باشند. در اینصورت یک اتومرفیسم $\sigma : K^{alg} \to K^{alg}$ موجود است که K را ثابت نگه میدارد و $\sigma(\alpha) = \beta$.

اثبات. تمرین □

نکته: اگر α و β دو ریشه‌ی $g \in K[x]$ باشند و g تحویل‌ناپذیر باشد، آنگاه اتومرفیسم $\sigma : K^{alg} \to K^{alg}$ موجود است که $\sigma(\alpha) = \beta$ و K را نقطه‌وار حفظ می‌کند.

نکته: اگر $\sigma : K^{alg} \to K^{alg}$ یک اتومرفیسم باشد که K را نقطه‌وار حفظ کند و $\sigma(\alpha) = \beta$. فرض کنید α ریشه‌ی چندجمله‌ای $g(x) \in K[x]$ باشد. در اینصورت β نیز ریشه‌ی چندجمله‌ای $g(x)$ است.

۱۱ جلسه دوازدهم: معرفی گروه گالوا

تعریف ۷۸. فرض کنید L یک میدان باشد. در اینصورت $\mathrm{Aut}(L) = \{\sigma : L \to L \mid \sigma$ ایزومرفیسم باشد$\}$.

توجه شود اگر $\alpha, \beta, \gamma \in \mathrm{Aut}(L)$، آنگاه $\alpha \circ \beta$ و α^{-1} نیز ایزوفیسم هستند و همچنین $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$. بنابراین مجموعه‌ی $\mathrm{Aut}(L)$ با عمل ترکیب توابع تشکیل یک گروه می‌دهند.

تعریف ۷۹. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. در اینصورت

$$\mathrm{Aut}(L/K) = \mathrm{Gal}(L : K) := \{\sigma \in \mathrm{Aut}(L) \mid \forall x \in k(\sigma(x) = x)\}$$

لم ۸۰. $\mathrm{Gal}(L:K)$ یک زیرگروهی از $\mathrm{Aut}(L)$ است.

اثبات. اگر $\alpha,\beta\in\mathrm{Gal}(L:K)$، در اینصورت کافی است نشان دهیم که $\alpha\circ\beta^{-1}\in\mathrm{Gal}(L:K)$. به راحتی بررسی می‌شود که $\alpha\circ\beta^{-1}\in\mathrm{Aut}(L)$ و $\alpha\circ\beta^{-1}$ عناصر K را ثابت نگه میدارد. □

تعریف ۸۱. فرض کنید $K\subseteq E\subseteq L$ توسیع میدانی باشند. در اینصورت

$$\Gamma(E):=\{\sigma\in\mathrm{Aut}(L)\,|\,\forall x\in E(\sigma(x)=x)\}$$

در واقع $\Gamma(E)=\mathrm{Gal}(L:E)$ و $\Gamma(E)\subseteq\mathrm{Gal}(L:K)$.

تعریف ۸۲. فرض کنید $H\subseteq\mathrm{Aut}(L)$، در اینصورت $\Phi(H):=\{x\in L\,|\,\forall\sigma\in H\ \sigma(x)=x\}$. دقت کنید که $\Phi(H)$ زیرمیدانی از L است.

توجه کنید که اگر H زیرگروهی از $\mathrm{Gal}(L:K)$ باشد، در اینصورت $K\subseteq\Phi(H)\subseteq L$.

مشاهده: الف) فرض کنید $K\subseteq E_1\subseteq E_2\subseteq L$. اگر E_1 زیرمیدان E_2 باشد، آنگاه $\Gamma(E_2)$ زیرگروهی از $\Gamma(E_1)$ است. فرض کنید $\sigma\in\Gamma(E_2)$، در اینصورت $\sigma:L\to L$ یک اتومرفیسم است که تمام نقاط E_2 را حفظ می‌کند چون $E_1\subseteq E_2$ پس σ تمام نقاط E_1 را نیز حفظ می‌کند. پس $\sigma\in\Gamma(E_1)$. همچنین اگر $\alpha,\beta\in\Gamma(E_1)$، آنگاه $\alpha\circ\beta^{-1}\in\Gamma(E_1)$.
ب) فرض کنید $H_1\subseteq H_2\subseteq\mathrm{Aut}(L)$ زیرگروه باشند. در اینصورت $\Phi(H_1)\supseteq\Phi(H_2)$ زیرمیدان است. فرض کنید $x\in\Phi(H_2)$، در اینصورت برای هر $\sigma\in H_2$ داریم $\sigma(x)=x$. اگر $\sigma'\in H_1$، آنگاه $\sigma'\in H_2$ پس $\sigma'(x)=x$.

لم ۸۳. فرض کنید $K\subseteq E\subseteq L$. در اینصورت $E\subseteq\Phi(\Gamma(E))$.

اثبات. با توجه به تعریف‌های زیر

$$\Gamma(E)=\{\sigma\in\mathrm{Gal}(L:K)\,|\,\forall x\in E(\sigma(x)=x)\}$$
$$\Phi(\Gamma(E))=\{x\in L\,|\,\forall\sigma\in\Gamma(E)\ \sigma(x)=x\}$$

به سادگی بررسی می‌شود که $E\subseteq\Phi(\Gamma(E))$. در واقع $\Phi(\Gamma(E))$ برابر است با مجموعه‌ی تمام عناصری در L که توسط تمام اتومرفیسم‌هایی که E را نقطه‌وار حفظ می‌کنند، نقطه‌وار حفظ می‌شوند.
□

مشاهده: فرض کنید $H \subseteq \mathrm{Gal}(L : K)$، در اینصورت $\Phi(H) = \{x \in L \,|\, \forall \sigma \in H\ \sigma(x) = x\}$ و
$H \subseteq \Gamma(\Phi(H))$. پس $\Gamma(\Phi(H)) = \{\sigma \in \mathrm{Gal}(L : K) \,|\, \forall x \in \Phi(H)(\sigma(x) = x)\}$. در واقع $\Gamma(\Phi(H))$ برابر است با مجموعه‌ی اتومرفیسم‌هایی که تمام نقاطی را که توسط اتومرفیسم‌های موجود در H حفظ می‌شوند را حفظ می‌کند.

تمرین ۹. به طور دقیق ثابت کنید که $E \subseteq \Phi(\Gamma(E))$ و $H \subseteq \Gamma(\Phi(H))$.

مثال ۸۴. چندجمله‌ای $f(x) = x^2 - 2$ روی $\mathbb{Q}[x]$ تحویل‌ناپذیر است (محک‌هایی برای بررسی تحویل‌ناپذیری وجود دارد). بنابراین میدان $\mathbb{Q} \subseteq L$ موجود است که در آن $f(x)$ دارای یک ریشه است. فرض کنید u ریشه $f(x)$ در L باشد. در اینصورت $\mathbb{Q}(u) \cong \mathbb{Q}(\sqrt{2})$ و $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$. مولدهای $\mathbb{Q}(\sqrt{2})$ روی $\mathbb{Q}$ به عنوان یک فضای برداری $1, \sqrt{2}$ هستند. بنابراین $\mathbb{Q}(\sqrt{2})$ از عناصری به صورت $\{a+b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ تشکیل می‌شوند. توجه کنید که $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ پس $\mathbb{Q}(\sqrt{2})$ میدان شکافنده‌ی $f(x)$ است. حال گروه گالوای $\mathrm{Gal}(\mathbb{Q}(u), \mathbb{Q})$ را مشخص می‌کنیم. توجه کنید که $\mathbb{Q}(u) = \{a + bu \,|\, a, b \in \mathbb{Q}\}$ که u ریشه‌ی $x^2 - 2 = 0$ است. اگر $\sigma : \mathbb{Q}(u) \to \mathbb{Q}(u)$ اتومرفیسم باشد، دراینصورت $\sigma(u) = u$ یا $\sigma(u) = -u$. بنابراین $\mathrm{Gal}(\mathbb{Q}(u), \mathbb{Q}) = \{\mathrm{id}, \sigma_1\}$ که σ_1 یک اتومرفیسم روی $\mathbb{Q}(u)$ است که $\sigma_1(a+bu) = a-bu$. پس $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2}), \mathbb{Q})| = 2$ و $[\mathrm{Gal}(\mathbb{Q}(\sqrt{2}), \mathbb{Q})] = 2$

مثال ۸۵. چندجمله‌ای $x^2+1 \in \mathbb{R}[x]$ یک چندجمله‌ای تحویل‌ناپذیر است. بنابراین میدان $\mathbb{R} \subseteq L$ موجود است که این چندجمله‌ای در آن ریشه دارد و $\mathbb{R} \subseteq \frac{\mathbb{R}[x]}{\langle x^2+1 \rangle} \cong L$. فرض کنید i یک ریشه‌ی $x^2 + 1 = 0$ باشد. پس $\mathbb{R}(i) = \{a + bi \,|\, a, b \in \mathbb{R}\}$. دقت کنید که $\mathbb{R}(i)$ شامل هر دو ریشه‌ی $x^2 + 1 = 0$ است و $[\mathbb{R}(i) : \mathbb{R}] = 2$. میدان $\mathbb{R}(i)$ را با $\mathbb{C}$ نشان میدهیم. حال گروه گالوای $\mathrm{Gal}(\mathbb{C}, \mathbb{R})$ را مشخص می‌کنیم. اگر $\sigma \in \mathrm{Gal}(\mathbb{C}, \mathbb{R})$، آنگاه $\sigma(i) = i$ یا $\sigma(i) = -i$. پس $\mathrm{Gal}(\mathbb{C}, \mathbb{R}) = \{\mathrm{id}, \sigma_1\}$ که $\sigma_1(a + bi) = a - bi$. پس $[\mathbb{R}(i) : \mathbb{R}] = 2 = |\mathrm{Gal}(\mathbb{C}, \mathbb{R})|$.

۱۲ جلسه سیزدهم: مثال از گروه گالوا

یادآوری: فرض کنید $K \subseteq L$ و X مجموعه‌ی ریشه‌های چندجمله‌ای $f \in K[x]$ باشد. اگر $\sigma \in \mathrm{Gal}(L, K)$، آنگاه $\sigma(X) = X$ یعنی برای هر $x \in X$ داریم $\sigma(x) \in X$.

مشاهده: فرض کنید $K \subseteq L$ یک توسیع جبری باشد، در واقع $K \subseteq L \subseteq K^{\text{alg}}$ و $f \in K[x]$ یک چندجمله‌ای باشد به طوری که در $L[x]$ داشته باشیم $f(x) = (x-\alpha)(x-\beta)$ که $\alpha \neq \beta$. در این صورت اگر $\sigma \in \text{Gal}(L:K)$، آنگاه $\sigma(\alpha) = \alpha$ یا $\sigma(\alpha) = \beta$. از طرفی یک اتومرفیسم $\sigma \in \text{Gal}(L:K)$ موجود است به طوری که $\sigma(\alpha) = \beta$. به بیان دیگر $\alpha, \beta \notin \Phi(\text{Gal}(L:K))$. بنابراین اگر $K \subseteq L$ یک توسیع جبری باشد و $\alpha \in L$ که $f(x) = (x-\alpha)(x-\beta)$. در این صورت $K = \Phi(\text{Gal}(L:K))$.

تمرین ۱۰. فرض کنید $K \subseteq L$ یک توسیع جبری باشد و $\alpha, \beta \in L$. اگر $f(x) = (x-\alpha)^2(x-\beta)$، در این صورت برای هر $\sigma : K^{\text{alg}} \to K^{\text{alg}}$ داریم: $\sigma(\alpha) = \alpha$ و $\sigma(\beta) = \beta$.

مشاهده: فرض کنید $K \subseteq L$ یک توسیع متناهی باشد یعنی $[L:K] < \infty$. در این صورت $|\text{Gal}(L:K)| < \infty$.

مثال ۸۶. گروه گالوای $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ را محاسبه کنید.
توجه شود که $x^3 = 2$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است و در $\mathbb{C}$ به صورت زیر تجزیه می‌شود:

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$$

همچنین توجه شود که عناصر $1, \sqrt[3]{2}, (\sqrt[3]{2})^2$ توسط $\mathbb{Q}(\sqrt[3]{2})$ روی $\mathbb{Q}$ تولید می‌شوند. فرض کنید $\sigma : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$ پس $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ و $\sigma(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$. به بیان دیگر اگر $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$، آنگاه $\sigma = \text{id}$. بنابراین $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ و $|\text{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})| = 1$

مثال ۸۷. گروه گالوای $\text{Gal}(\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q})$ را مشخص کنید.
چندجمله‌ای $x^2 - 2$ روی $\mathbb{Q}$ تحویل‌ناپذیر است و تمام ریشه‌های این چندجمله‌ای در میدان $\mathbb{Q}(\sqrt{2})$ قرار دارند. از طرفی $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. همچنین $i\sqrt{3}$ ریشه‌ی معادله‌ی $x^2 + 3 = 0$ با ضرایب در $\mathbb{Q}$ هم با ضرایب در $\mathbb{Q}(\sqrt{2})$ است. ادعا می‌کنیم که $x^2 + 3$ روی $\mathbb{Q}(\sqrt{2})[x]$ تحویل‌ناپذیر است. توجه شود که $i\sqrt{3}, -i\sqrt{3} \notin \mathbb{R}$ ریشه‌های $x^2 + 3$ هستند. بنابراین $i\sqrt{3}, -i\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. پس $[\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q}]$ دارای پایه‌ی $\{1, i\sqrt{3}\}$ است. همچنین $[\mathbb{Q}(\sqrt{2} : \mathbb{Q})]$ پایه‌ی $\{1, \sqrt{2}\}$ است. بنابراین $\{1, \sqrt{2}, i\sqrt{3}, i\sqrt{6}\}$ یک پایه برای $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$ روی $\mathbb{Q}$ است. حال فرض کنید $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q}))$. در این صورت

$\sigma(\sqrt{2}) = \sqrt{2}$ یا $\sigma(\sqrt{2}) = -\sqrt{2}$ و $\sigma(i\sqrt{3}) = i\sqrt{3}$ یا $\sigma(i\sqrt{3}) = -i\sqrt{3}$، همچنین $\sigma(i\sqrt{6}) = \sigma(i\sqrt{3}) \times \sigma(\sqrt{2})$. بنابراین اتومرفیسم‌های زیر را داریم:

$$\sigma_1 : a + b\sqrt{2} + c(i\sqrt{3}) + d(\sqrt{6}) \mapsto a + b\sqrt{2} + c(i\sqrt{3}) + d(\sqrt{6})$$
$$\sigma_2 : a + b\sqrt{2} + c(i\sqrt{3}) + d(\sqrt{6}) \mapsto a - b\sqrt{2} + c(i\sqrt{3}) - d(\sqrt{6})$$
$$\sigma_3 : a + b\sqrt{2} + c(i\sqrt{3}) + d(\sqrt{6}) \mapsto a + b\sqrt{2} - c(i\sqrt{3}) - d(\sqrt{6})$$
$$\sigma_4 : a + b\sqrt{2} + c(i\sqrt{3}) + d(\sqrt{6}) \mapsto a - b\sqrt{2} - c(i\sqrt{3}) + d(\sqrt{6})$$

بنابراین $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q}) = \{\mathrm{id}, \sigma_2, \sigma_3, \sigma_4\}$.

مثال ۸۸. در مثال قبل، مجموعه‌های

$$H_1 = \{\mathrm{id}, \sigma_1\}$$
$$H_2 = \{\mathrm{id}, \sigma_2\}$$
$$H_3 = \{\mathrm{id}, \sigma_3\}$$
$$H_4 = \{\mathrm{id}\}$$
$$H_5 = \{\mathrm{id}, \ldots, \sigma_4\}$$

زیرگروه‌هایی از $\{\mathrm{id}, \sigma_2, \sigma_3, \sigma_4\}$ هستند و متناظر با این زیرگروه‌ها، میدان‌هایی به صورت زیر داریم که همه‌ی میدانهای بین $\mathbb{Q}$ و $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$ هستند.

$$\Phi(H_1) = \{a + c(i\sqrt{3}) \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(i\sqrt{3})$$
$$\Phi(H_2) = \mathbb{Q}(\sqrt{2})$$
$$\Phi(H_3) = \mathbb{Q}(i\sqrt{6})$$
$$\Phi(H_4) = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$$
$$\Phi(H_5) = \Phi(\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q})) = \mathbb{Q}$$

تعریف ۸۹. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. اگر $\Phi(\mathrm{Gal}(L : K)) = K$، در این صورت این توسیع را یک توسیع گالوایی می‌نامیم.

۱۳ جلسه چهاردهم: اثبات یک قضیه درباره‌ی گروه گالوای متناهی

لم ۹۰. فرض کنید $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathrm{Aut}(L)$ تعدادی اتومرفیسم باشند که دو به دو با یکدیگر متفاوت باشند. در اینصورت اگر برای هر $x \in L$ داشته باشیم: $r_1\alpha_1(x) + \cdots + r_n\alpha_n(x) = 0$ که $r_i \in L$، آنگاه

$$r_1 = r_2 = \cdots = r_n = 0.$$

اثبات. با استقرا روی تعداد اتومرفیسم‌ها، برای $n = 1$ توجه شود که اگر برای هر $x \in L$ داشته باشیم: $r_1\alpha_1(x) = 0$ آنگاه $r_1 = 0$. فرض کنید که حکم برای اتومرفیسم‌های کمتر از n برقرار باشد. فرض کنید

$$\forall x \in L \quad r_1\alpha_1(x) + \cdots + r_n\alpha_n(x) = 0. \qquad (۱)$$

می‌دانیم که $\alpha_1 \neq \alpha_n$، بنابراین نقطه‌ای مانند $u \in L$ موجود است که $\alpha_1(u) \neq \alpha_n(u)$. توجه کنید که

$$\forall x \in L \quad r_1\alpha_1(ux) + \cdots + r_n\alpha_n(ux) = 0.$$

پس

$$\forall x \in L \quad r_1\alpha_1(u)\alpha_1(x) + \cdots + r_n\alpha_n(u)\alpha_n(x) = 0. \qquad (۲)$$

اکنون معادله‌ی (۱) را در $\alpha_n(u)$ ضرب می‌کنیم: $r_1\alpha_n(u)\alpha_1(x) + \cdots + r_n\alpha_n(u)\alpha_n(x) = 0$. حاصل را از معادله‌ی (۲) کم میکنیم:

$$r_1\alpha_1(x)(\alpha_1(u) - \alpha_n(u)) + r_2\alpha_2(x)(\alpha_2(u) - \alpha_n(u)) + \ldots + r_{n-1}\alpha_{n-1}(x)(\alpha_{n-1}(u) - \alpha_n(u)) = 0$$

این خلاف فرض است چون $\alpha_1(u) \neq \alpha_n(u)$. □

مشاهده: هر دستگاه معادلات به صورت زیر که در آن تعداد مجهولات بیشتر از تعداد معادلات باشد حتما دارای یک جواب نابدیهی است (در یک میدان مناسب مانند $\mathbb{R}$).

$$\begin{cases} r_1x_1 + r_2x_2 + r_3x_3 + r_4x_4 = 0 \\ r'_1x_1 + r'_2x_2 + r'_3x_3 + r'_4x_4 = 0 \end{cases}$$

به طور دقیق‌تر، فرض کنید $m > n$ و $T : K^m \to K^n$ یک تبدیل خطی باشد. در اینصورت T متناظر با یک ماتریس $A_{n\times m}$ است و می‌توان نوشت:

$$T\begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix} = A_{n\times m}\begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix}$$

از طرفی $\dim(\mathrm{Ker}(T)) + \dim(\mathrm{Im}(T)) = m$. بنابراین $\dim(\mathrm{Ker}(T)) \geq 1$. یعنی معادله‌ی $A\begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix} = 0$ قطعاً دارای جواب نابدیهی است. به طور خلاصه فرض کنید $A_{n\times m}$ یک ماتریس از عناصر میدان L باشد به طوری که $m > n$. در این صورت بردار ناصفر $\begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix}$ از عناصر L موجود است به طوری که $A_{n\times m}\begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix} = 0$.

قضیه ۹۱. فرض کنید $K \subseteq L$ یک توسیع میدانی متناهی باشد و G یک زیر گروه متناهی از $\mathrm{Gal}(L : K)$ باشد. در اینصورت $|G| = [L : \Phi(G)]$.

اثبات. فرض کنید $G = \{\alpha_1, \alpha_2, \ldots, \alpha_m \,|\, \alpha_i \in \mathrm{Gal}(L : K)\}$ و $\{z_1, z_2, \ldots, z_n\}$ یک پایه‌ی L روی $\Phi(G)$ باشد (یعنی $|G| = m$ و $[L : \Phi(G)] = n$). ماتریس زیر را در نظر بگیرید

$$A_{n\times m}\begin{bmatrix} \alpha_1(z_1) & \alpha_2(z_1) & \cdots & \alpha_m(z_1) \\ \vdots & & & \\ \alpha_1(z_n) & \alpha_2(z_n) & \cdots & \alpha_m(z_n) \end{bmatrix}$$

ادعا می کنیم فرضِ $m > n$ منجر به تناقض می‌شود. فرض کنید $m > n$. بنابر مشاهده قبل،

عناصر $\begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix}$ از میدان L موجودند به طوری که $A_{n\times m}\begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix} = 0$. یعنی

$$\begin{cases} \alpha_1(z_1)v_1 + \alpha_2(z_1)v_2 + \ldots + \alpha_m(z_1)v_m = 0 \\ \vdots \\ \alpha_1(z_n)v_1 + \alpha_2(z_n)v_2 + \ldots + \alpha_m(z_n)v_m = 0 \end{cases} \quad (۳)$$

نشان می دهیم که یک ترکیب خطی از $\{\alpha_1, \ldots, \alpha_m\}$ با ضرایب ناصفر صفر می‌شود و این تناقض با لم قبل است. فرض کنید $b \in L$ یک عنصر دلخواه باشد. عناصر $r_1, r_2, \ldots, r_n \in \Phi(G)$ موجودند به طوری که $b = r_1z_1 + r_2z_2 + \ldots + r_nz_n$. از آنجا که $r_i \in \Phi(G)$، برای هر اتومرفیسم $\alpha \in G$ داریم: $\alpha(r_i) = r_i$. حال سطر اول دستگاه (۳) را در r_1، سطر دوم را در r_2 و به این ترتیب سطر nام را در r_n ضرب می‌کنیم:

$$\begin{cases} r_1\alpha_1(z_1)v_1 + r_1\alpha_2(z_1)v_2 + \ldots + r_1\alpha_m(z_1)v_m = 0 \\ \vdots \\ r_n\alpha_1(z_n)v_1 + r_n\alpha_2(z_n)v_2 + \ldots + r_n\alpha_m(z_n)v_m = 0 \end{cases}$$

بنابراین

$$\begin{cases} \alpha_1(r_1z_1)v_1 + \alpha_2(r_1z_1)v_2 + \ldots + \alpha_m(r_1z_1)v_m = 0 \\ \vdots \\ \alpha_1(r_nz_n)v_1 + \alpha_2(r_nz_n)v_2 + \ldots + \alpha_m(r_nz_n)v_m = 0 \end{cases}$$

پس می‌توان نوشت:

$$v_1(\alpha_1(r_1z_1) + \alpha_1(r_2z_2) + \cdots + \alpha_1(r_nz_n)) + v_2(\alpha_2(r_1z_1) + \alpha_2(r_2z_2) + \cdots + \alpha_2(r_nz_n)) + \ldots + v_m(\alpha_m(r_1z_1) + \alpha_m(r_2z_2) + \cdots + \alpha_m(r_nz_n)) = 0$$

که

$$\alpha_1(b) = \alpha_1(r_1z_1) + \alpha_1(r_2z_2) + \cdots + \alpha_1(r_nz_n)$$
$$\alpha_2(b) = \alpha_2(r_1z_1) + \alpha_2(r_2z_2) + \cdots + \alpha_2(r_nz_n)$$
$$\vdots$$
$$\alpha_m(b) = \alpha_m(r_1z_1) + \alpha_m(r_2z_2) + \cdots + \alpha_m(r_nz_n)$$

یعنی $v_1\alpha_1(b) + \ldots + v_m\alpha_m(b) = 0$ و این تناقض است.
اکنون ادعا می‌کنیم که فرضِ $n > m$ نیز منجر به تناقض می‌شود. ماتریس زیر را در نظر بگیرید:

$$A = \begin{bmatrix} \alpha_1(z_1) & \alpha_1(z_2) & \ldots & \alpha_1(z_{m+1}) \\ \alpha_2(z_1) & \alpha_2(z_2) & \ldots & \alpha_2(z_{m+1}) \\ \vdots & & & \\ \alpha_m(z_1) & \alpha_m(z_2) & \ldots & \alpha_m(z_{m+1}) \end{bmatrix}$$

پس عنصر $V = \begin{bmatrix} v_1 \\ \vdots \\ v_{m+1} \end{bmatrix}$ موجود است که $A \begin{bmatrix} v_1 \\ \vdots \\ v_{m+1} \end{bmatrix} = 0$. بنابراین داریم:

$$\begin{cases} \alpha_1(z_1)v_1 + \alpha_1(z_2)v_2 + \cdots + \alpha_1(z_{m+1})v_{m+1} = 0 \\ \vdots \\ \alpha_m(z_1)v_1 + \alpha_m(z_2)v_2 + \cdots + \alpha_m(z_{m+1})v_{m+1} = 0 \end{cases}$$

از بین جواب‌های $AV = 0$، جوابی را انتخاب کنید که در آن حداقلِ v_iها ناصفر باشند. برای مثال فرض کنید

$v_1, v_2, \ldots v_r \neq 0$ و $v_{r+1}, v_{r+2}, \ldots v_{m+1} = 0$. پس

$$A = \begin{bmatrix} \alpha_1(z_1) & \alpha_1(z_2) & \ldots & \alpha_1(z_r) \\ \alpha_2(z_1) & \alpha_2(z_2) & \ldots & \alpha_2(z_r) \\ \vdots & & & \\ \alpha_m(z_1) & \alpha_m(z_2) & \ldots & \alpha_m(z_r) \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_r \end{bmatrix} = 0$$

پس

$$\begin{cases} \alpha_1(z_1)v_1 + \alpha_1(z_2)v_2 + \cdots + \alpha_1(z_r)v_r = 0 \\ \vdots \\ \alpha_m(z_1)v_1 + \alpha_m(z_2)v_2 + \cdots + \alpha_m(z_r)v_r = 0 \end{cases}$$

حال تمام معادلات بالا را بر v_r تقسیم می‌کنیم:

$$\begin{cases} \alpha_1(z_1)v'_1 + \alpha_1(z_2)v'_2 + \cdots + \alpha_1(z_r) = 0 \\ \vdots \\ \alpha_m(z_1)v'_1 + \alpha_m(z_2)v'_2 + \cdots + \alpha_m(z_r) = 0 \end{cases} \quad (۴)$$

که در آن $v'_i = \dfrac{v_i}{v_r}$. بدون کاستن از کلیت مسئله فرض کنید $\alpha_1 = \mathrm{id}$. بنابراین $z_1v_1 + z_2v_2 + \ldots + z_rv_r = 0$. توجه شود که z_iها روی اسکالرهای آمده از $\Phi(G)$ مستقل خطی هستند. بنابراین فرض کنید $v_1 \notin \Phi(G)$. فرض کنید $\alpha_2(v_1) \neq v_1$. حال α_2 را در معادلات دستگاه (۴) اثر می‌دهیم:

$$\begin{cases} \alpha_2\alpha_1(z_1)\alpha_2(v'_1) + \alpha_2\alpha_1(z_2)\alpha_2(v'_2) + \cdots + \alpha_2\alpha_1(z_r) = 0 \\ \vdots \\ \alpha_2\alpha_m(z_1)\alpha_2(v'_1) + \alpha_2\alpha_m(z_2)\alpha_2(v'_2) + \cdots + \alpha_2\alpha_m(z_r) = 0 \end{cases}$$

توجه شود که $G = \{\alpha_1, \ldots, \alpha_m\} = \{\alpha_2\alpha_1, \ldots, \alpha_2\alpha_m\}$ و دستگاه معادلات فوق به صورت زیر است:

$$A = \begin{bmatrix} \alpha_2\alpha_1(z_1) & \alpha_2\alpha_1(z_2) & \ldots & \alpha_2\alpha_1(z_r) \\ \alpha_2\alpha_2(z_1) & \alpha_2\alpha_2(z_2) & \ldots & \alpha_2\alpha_2(z_r) \\ \vdots & & & \\ \alpha_2\alpha_m(z_1) & \alpha_2\alpha_m(z_2) & \ldots & \alpha_2\alpha_m(z_r) \end{bmatrix} \begin{bmatrix} \alpha_2(v'_1) \\ \vdots \\ \alpha_2(v'_{r-1}) \\ 1 \end{bmatrix} = 0$$

بنابراین می‌توان فرض کرد دستگاه زیر را داریم:

$$\begin{cases} \alpha_1(z_1)\alpha_2(v'_1) + \alpha_1(z_2)\alpha_2(v'_2) + \cdots + \alpha_1(z_r) = 0 \\ \vdots \\ \alpha_m(z_1)\alpha_2(v'_1) + \alpha_m(z_2)\alpha_2(v'_2) + \cdots + \alpha_m(z_r) = 0 \end{cases} \quad (۵)$$

حال معادلات دستگاه بالا را از معادلات دستگاه (۴) کم می‌کنیم:

(۶)
$$\begin{cases} \alpha_1(z_1)(v_1' - \alpha_2(v_1')) + \alpha_1(z_2)(v_2' - \alpha_2(v_2')) + \cdots + \alpha_1(z_{r-1})(v_{r-1}' - \alpha_2(v_{r-1}')) = 0 \\ \vdots \\ \alpha_m(z_1)(v_1' - \alpha_2(v_1')) + \alpha_m(z_2)(v_2' - \alpha_2(v_2')) + \cdots + \alpha_m(z_{r-1})(v_{r-1}' - \alpha_2(v_{r-1}')) = 0 \end{cases}$$

و این در تناقض است با اینکه دستگاه (۴) کوچکترین دستگاه ممکن است. □

۱۴ جلسه پانزدهم: توسیع‌های نرمال

تعریف ۹۲. توسیع میدانی $K \subseteq L$ را یک توسیع نرمال می‌نامیم هرگاه هر چندجمله‌ای تحویل‌ناپذیر $f \in K[x]$ اگر یک ریشه در L داشته باشد، آنگاه به طور کامل در L به عوامل درجه‌ی اول تجزیه شود.

مشاهده: اگر توسیع $K \subseteq L$ نرمال باشد و $K \subseteq E \subseteq L$، آنگاه توسیع $E \subseteq L$ نیز نرمال است.

قضیه ۹۳. فرض کنید $K \subseteq L$ یک توسیع نرمال متناهی باشد و $K \subseteq E_1 \cong_K E_2 \subseteq L$ یعنی E_1 و E_2 دو میدان بین K و L هستند و یک یکریختی مانند $\sigma' : E_1 \to E_2$ وجود دارد که عناصر K را نقطه‌وار حفظ می‌کند. در اینصورت اتومرفیسم $\sigma \in \mathrm{Gal}(L : K)$ موجود است به طوری که $\sigma' \subseteq \sigma$.

اثبات. چون توسیع $K \subseteq L$ نرمال است پس L میدان شکافنده‌ی چندجمله‌ای $f \in K[x]$ است. در اینصورت $f \in E_1[x]$ و $f \in E_2[x]$. بنابر یکتایی میدان شکافنده، اتومرفیسمی مانند $\sigma : L \to L$ با شرط خواسته شده پیدا می‌شود. □

نتیجه ۹۴.
- فرض کنید $K \subseteq L$ یک توسیع نرمال متناهی باشد و $f \in K[x]$ تحویل‌ناپذیر باشد. در اینصورت فرض کنید α_1 و α_2 دو ریشه‌ی متمایز f در L باشند. می‌دانیم که $K[\alpha_1] \cong K[\alpha_2]$، بنابراین اتومرفیسمی از L به L موجود است که توسیعی از این یکریختی است.

- فرض کنید $K \subseteq L$ یک توسیع نرمال متناهی باشد. در این صورت اگر $\alpha \in L - K$، آنگاه α روی K جبری است. پس α ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیرِ $f \in K[x]$ است. فرض کنید β ریشه‌ی دیگری برای f در L باشد. در این صورت اتومرفیسم $\sigma : L \to L$ موجود است که $\sigma(\alpha) = \beta$.

فرض کنید $K \subseteq L$ یک توسیع متناهی دلخواه باشد. در این صورت این توسیع، جبری است، یعنی $L = K(\alpha_1, \ldots, \alpha_n)$ که α_iها روی K جبری هستند. فرض کنید α_i ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر $f_i \in K[x]$ باشد. چندجمله‌ای $f_1 \times f_2 \times \cdots \times f_n$ را در نظر بگیرید و فرض کنید $K \subseteq L \subseteq N$ که N میدان شکافنده‌ی $f_1 \times f_2 \times \cdots \times f_n$ روی K باشد. در این صورت N یک توسیع نرمال از K است. توجه کنید که هیچ زیر میدانی از N توسیع نرمال K شامل L نیست. در اینصورت می‌گوییم N بستار نرمال K شامل L است.

تعریف ۹۵. فرض کنید $K \subseteq L \subseteq N$ یک توسیع متناهی باشد. میدان $K \subseteq L \subseteq N$ را یک بستار نرمال K شامل L می‌نامیم هرگاه $K \subseteq N$ نرمال باشد و هیچ میدانِ $K \subseteq L \subseteq N' \subsetneqq N$ توسیع نرمال K نباشد.

مشاهده: فرض کنید $K \subseteq L_1$ و $K \subseteq L_2$ توسیع‌های جبری متناهی باشند و $L_1 \cong_K L_2$. در این صورت بستار نرمال K شامل L_1 با بستار نرمال K شامل L_2 ایزومرف است. در واقع چون L_1 و L_2 توسیع‌های جبری متناهی هستند پس

$$L_1 = K(\alpha_1, \ldots, \alpha_n) \cong L_2 = K(\beta_1, \ldots, \beta_n)$$

اگر N_1 بستار نرمال K شامل L_1 و N_2 بستار نرمال K شامل L_2 باشند، آنگاه N_1 و N_2 هر دو ایزومرف با میدان شکافنده‌ی چندجمله‌ای $f_1 \times \cdots \times f_n$ روی K هستند که f_iها چندجمله‌ای‌های می‌نیمال α_iها هستند.

قضیه ۹۶. فرض کنید $K \subseteq L$ یک توسیع نرمال باشد و $K \subseteq E \subseteq L$. در این صورت توسیع $K \subseteq E$ نرمال است اگر و تنها اگر برای هر Kـاتومرفیسم $\sigma : L \to L$ داشته باشیم: $\sigma|_E : E \to E$ یک Kـ اتومرفیسم باشد.

اثبات. فرض کنید توسیع $K \subseteq E$ نرمال باشد. در این صورت $E = K(\alpha_1, \ldots, \alpha_n)$ که

$\alpha_1, \ldots, \alpha_n$ ریشه‌های f هستند. حال اگر σ را به E محدود کنیم:

$$\sigma : K(\alpha_1, \ldots, \alpha_n) \to K(\beta_1, \ldots, \beta_n)$$

در این صورت تصویر σ از E خارج نمی‌شود. برای جهت عکس، می‌دانیم که $E = K(\alpha_1, \ldots, \alpha_n)$ که $\alpha_1, \ldots, \alpha_n$ روی K جبری هستند. نشان می‌دهیم که توسیع $K \subseteq E$ نرمال است. اگر $f \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر باشد که یک ریشه در E دارد. در این صورت $\sigma(\alpha) = \beta$ نیز ریشه‌ای برای $f \in K[x]$ است. پس یک Kـاتومرفیسمِ $\sigma : L \to L$ موجود است به طوری که $\sigma(\alpha) = \beta$. چون $\sigma(\alpha) \in E$ پس $\beta \in E$. □

۱۵ جلسه شانزدهم: توسیع گالوایی: نرمال و جدایی‌پذیر

یادآوری: اگر $K \subseteq L$ یک توسیع نرمال باشد، $f \in K[x]$ تحویل‌ناپذیر باشد و $\alpha, \beta \in$ دو ریشه‌ی متمایز f باشند. در این صورت $\sigma \in \mathrm{Gal}(L : K)$ موجود است به طوری که $\sigma(\alpha) = \beta$. به بیان دیگر اگر $\alpha \in L - K$ ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیرِ $f \in K[x]$ باشد که f ریشه‌ی دیگری مانند β نیز داشته باشد. در این صورت $\alpha \notin \Phi(\mathrm{Gal}(L : K))$.

مشاهده: فرض کنید $f \in K[x]$ تحویل‌ناپذیر باشد و $K \subseteq L$ میدان شکافنده‌ی f باشد. فرض کنید $f(x) = (x - \alpha)^2 g(x)$ که $\alpha \in L$، در این صورت $f'(x) = 2(x - \alpha)g(x) + g'(x)(x - \alpha)^2$ پس $f'(\alpha) = 0$ و $\deg(f') < \deg(f)$. در حالت کلی فرض کنید $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ در این صورت

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + a_1.$$

اگر میدان K میدانی با مشخصه صفر باشد، آنگاه $f' \neq 0$. پس اگر مشخصه K صفر باشد، یک چندجمله‌ای تحویل‌ناپذیر $f \in K[x]$ در میدان شکافنده نمی‌تواند ریشه‌ی تکراری داشته باشد. اگر میدان K دارای مشخصه p باشد و f تحویل‌ناپذیر باشد، در صورتی f می‌تواند در میدان شکافنده ریشه‌ی تکرای داشته باشد که

$$f = a_0 + a_1 x^p + a_2 x^{2p} + a_3 x^{3p} + \ldots + a_n x^{np}$$

چون در این صورت $f' = 0$.

تعریف ۹۷. چندجمله‌ای تحویل‌ناپذیر $f \in K[x]$ جدایی‌پذیر[۴] روی K می‌نامیم هرگاه f در میدان شکافنده‌ی f روی K به عوامل درجه اول تجزیه شود.
توسیع $K \subseteq L$ را یک توسیع میدانی جدایی‌پذیر می‌نامیم هرگاه هر عنصر $\alpha \in L - K$ ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر جدایی‌پذیر روی K باشد.

مشاهده:

- اگر مشخصه میدان K صفر باشد، در این صورت هر توسیع جبری، جدایی‌پذیر است.
- فرض کنید $K \subseteq L$ یک توسیع نرمال و جدایی‌پذیر باشد و $\alpha \in L-K$. پس α ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر f است. پس f به صورت $f(x) = (x-\alpha)(x-\beta)\cdots(x-\gamma)$ است. پس $\sigma \in \mathrm{Gal}(L : K)$ موجود است به طوری که $\sigma(\alpha) \neq \alpha$. به بیان دیگر اگر $K \subseteq L$ نرمال و جدایی‌پذیر باشد، آنگاه $\Phi(\mathrm{Gal}(L : K)) = K$.

تعریف ۹۸. توسیع $K \subseteq L$ را یک توسیع گالوایی می‌نامیم هرگاه $\Phi(\mathrm{Gal}(L : K)) = K$.

مشاهده:

- پس هر توسیع نرمالِ جدایی‌پذیر، گالوایی است.
- اگر $K \subseteq L$ یک توسیع متناهی نرمال جدایی‌پذیر باشد و $[L : K] = n$، آنگاه $|\mathrm{Gal}(L : K)| = n$. توجه کنید که $K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_m) = L$. پس

$$[L : K] = [K(\alpha_1) : K] \times [K(\alpha_1, \alpha_2) : K] \times \cdots [K(\alpha_1, \ldots, \alpha_m) : K]$$

یعنی $n = n_1 \times n_2 \times \cdots \times n_m$. بنابراین تعداد اتومرفیسم‌های روی L که K را نقطه‌وار حفظ می‌کنند به صورت $n = n_1 \times n_2 \times \cdots \times n_m$ است چون n_1 تصویر مختلف از $K(\alpha_1)$ و n_2 تصویر مختلف از $K(\alpha_1, \alpha_2)$ و به این ترتیب $n_1 \times n_2 \times \cdots \times n_m$ تصویر مختلف از L داریم (در اینجا قصد نداریم اثبات دقیق‌تری از این مشاهده ارائه دهیم).

[4] Separable

قضیه ۹۹. فرض کنید $K \subseteq L$ یک توسیع متناهی باشد، در این صورت $K \subseteq L$ گالوایی است اگر و تنها اگر نرمال و جدایی‌پذیر است (در مشخصه صفر اگر و تنها اگر L میدان شکافنده‌ی یک چندجمله‌ای f روی K باشد).

اثبات. می‌دانیم که هر توسیع نرمالِ جدایی‌پذیر، گالوایی است. حال فرض کنید توسیع $K \subseteq L$ گالوایی باشد یعنی $\Phi(\mathrm{Gal}(L : K)) = K$. نشان می دهیم $K \subseteq L$ جدایی‌پذیر و نرمال است. فرض کنید $\alpha \in L - K$ یک عنصر دلخواه باشد و α ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر $f \in K[x]$ باشد. نشان می دهیم که چندجمله‌ای f در L به عوامل درجه اول تجزیه می‌شود. توجه کنید که $\mathrm{Gal}(L : K)$ یک گروه متناهی است برای مثال فرض کنید $\mathrm{Gal}(L : K) = \{\alpha_1, \ldots, \alpha_n\}$. مجموعه‌ی زیر را در نظر بگیرید $\{\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\}$ و فرض کنید $A = \{\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_r(\alpha)\}$ عناصری متمایز باشند. چندجمله‌ای زیر را در نظر بگیرید:

$$g(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \ldots (x - \sigma_r(\alpha))$$

ادعا می‌کنیم اولاً $g(x) \in K[x]$، دوماً g تحویل‌ناپذیر است (به بیان دیگر g چندجمله‌ای مینیمال α است). برای اثبات ادعای اول، توجه کنید که ضرایب موجود در $h(x) = (x - a_1)(x - a_2) \ldots (x - a_r)$ به صورت ضریبی از a_iها می باشد. بنابراین ضرایب موجود در $g(x)$ بر حسب $\sigma_i(\alpha)$ها نوشته می‌شوند. می‌دانیم که $K = \mathrm{Gal}(L : K)$، کافیست نشان دهیم که تمامی ضرایب چندجمله‌ای g توسط همه‌ی اتومرفیسم‌های موجود در $\mathrm{Gal}(L : K)$ حفظ می‌شوند. فرض کنید $\beta \in \mathrm{Gal}(L : K)$ یک اتومرفیسم دلخواه باشد. در اینصورت $\beta(A) = A$ چون A مجموعه‌ی ریشه‌های چندجمله‌ای g است و $\beta(A)$ جایگشتی از A است. توجه کنید که ضرایب g توسط β حفظ می‌شوند، برای مثال ضریب ثابت g به صورت $a_0 = \sigma_1(\alpha)\sigma_2(\alpha) \cdots \sigma_r(\alpha)$ است و $\beta(a_0) = a_0$. ضریب x^{r-1} در g به صورت $a_{r-1} = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_r(\alpha)$ است و $\beta(a_{r-1}) = a_{r-1}$. پس $g \in K[x]$. برای اثبات ادعای دوم (g تحویل‌ناپذیر است)، کافیست نشان دهیم که اگر $h(\alpha) = 0$، آنگاه $g|h$. فرض کنید $h(\alpha) = 0$. هر $\sigma_i(\alpha)$ یک ریشه‌ی چندجمله‌ای h است پس $(x - \sigma_i(\alpha))|h$، بنابراین $g|h$. □

۱۶ جلسه هفدهم: قضیه اساسی نظریه گالوا

یادآوری:

- اگر $K \subseteq L$ میدان شکافنده‌ی یک چندجمله‌ای $f \in K[x]$ باشد، آنگاه توسیع $K \subseteq L$ نرمال است.
- هر توسیع نرمالِ $K \subseteq L$، میدان شکافنده‌ی یک چندجمله‌ای $f \in K[x]$ است.
- فرض کنید $K \subseteq L$ یک توسیع نرمال باشد و $K \subseteq E \subseteq L$. در این صورت توسیع $E \subseteq L$ نیز نرمال است؛ چون وقتی $K \subseteq L$ یک توسیع نرمال باشد، آنگاه L میدان شکافنده‌ی یک چندجمله‌ای $f \in K[x]$ است. واضح است که $f \in E[x]$، بنابراین L میدان شکافنده‌ی $f \in E[x]$ نیز هست.
- توسیع $K \subseteq L$ را جدایی‌پذیر می‌نامیم هرگاه هر عنصر $x \in L-K$ ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیرِ $f \in K[x]$ باشد و این چندجمله‌ای در بستار نرمال K شامل L به طور کامل به عوامل درجه‌ی اول تجزیه شود.
- فرض کنید $K \subseteq L$ یک توسیع متناهی و جدایی‌پذیر و $K \subseteq E \subseteq L$. در این صورت $E \subseteq L$ نیز جدایی‌پذیر است؛ فرض کنید $x \in L-E$ ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر با ضرایب در E باشد. بنابراین x روی K جبری است، پس x ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیرِ $f \in K[x]$ است. توجه کنید که $f \in E[x]$ و کافیست نشان دهیم که از میان چندجمله‌ای‌های موجود در $E[x]$ که در x صفر می شوند f حداقل درجه را دارد. اگر $g \in E[x]$ دارای حداقل درجه باشد، آنگاه $f = gh + r$ که $\deg(r) < \deg(g)$ و $r \in E[x]$. بنابراین چندجمله‌ای مینیمال x در K و E یکسان است و می‌دانیم که این چندجمله‌ای در بستار نرمال K شامل L به عوامل درجه‌ی اول تجزیه می‌شود.
- با توجه به اینکه توسیع $K \subseteq L$ یک توسیع گالوایی است اگر و تنها اگر نرمال و جدایی‌پذیر باشد، اگر $K \subseteq L$ یک توسیع گالوایی و $K \subseteq E \subseteq L$ یک میدان میانی باشد. آنگاه توسیع $E \subseteq L$ یک توسیع گالوایی است. بنابراین برای هر میدان میانی $K \subseteq E \subseteq L$ داریم:

$\Phi(\Gamma(E)) = E$ که $\Gamma(E)$ برابر است با همه‌ی اتومرفیسم‌های موجود در $\mathrm{Gal}(L : K)$ که تمامی نقاط E را حفظ می‌کنند.

قضیه ۱۰۰. اگر $K \subseteq L$ یک توسیع گالوایی باشد، آنگاه یک تناظر یک‌به‌یک میان میدان‌های میانی $K \subseteq E \subseteq L$ و زیرگروه‌های گروه $\mathrm{Gal}(L : K)$ وجود دارد.

اثبات. فرض کنید $K \subseteq L$ یک توسیع گالوایی باشد. دو مجموعه‌ی زیر را در نظر بگیرید.

$$\mathcal{A} = \{\text{همه‌ی میدان‌های میانی } K \subseteq E \subseteq L\}$$
$$\mathcal{B} = \{\text{همه‌ی زیرگروه‌های گروه } \mathrm{Gal}(L : K)\}$$

نگاشت $\sigma : \mathcal{A} \to \mathcal{B}$ که $\sigma(E) = \Gamma(E)$ یک نگاشت یک‌به‌یک است؛ فرض کنید $\Gamma(E_1) = \Gamma(E_2)$، پس $\Phi(\Gamma(E_1)) = \Phi(\Gamma(E_2))$ در نتیجه $E_1 = E_2$. ادعا می کنیم نگاشت فوق پوشا نیز هست. فرض کنید $H \in \mathcal{B}$. نشان می دهیم که $\Gamma(\Phi(H)) = H$. می‌دانیم که $H \subseteq \Gamma(\Phi(H))$ و همچنین می‌دانیم که اگر $K \subseteq E \subseteq L$ یک میدان میانی باشد، آنگاه $E \subseteq \Phi(\Gamma(E))$. بنابراین $\Phi(H) \subseteq \Phi(\Gamma(\Phi(H)))$. از طرفی می‌دانیم که $H \subseteq \Gamma(\Phi(H))$ پس $\Phi(H) \supseteq \Phi(\Gamma(\Phi(H)))$. بنابراین $\Phi(\Gamma(\Phi(H))) = \Phi(H)$. کافیست نشان دهیم که $|\Gamma(\Phi(H))| = |H|$. می‌دانیم که اگر G زیرگروهی متناهی از $\mathrm{Gal}(L : K)$ باشد، آنگاه $|G| = [L : \Phi(G)]$. بنابراین $|H| = [L : \Phi(H)]$. از طرفی $|H| = |\Gamma(\Phi(H))| = [L : \Gamma(\Phi(H))]$. □

۱۷ جلسه هجدهم: قسمت دوم قضیه اساسی نظریه گالوا

یادآوری:

- فرض کنید G یک گروه باشد و H زیرگروهی از G باشد. رابطه هم‌ارزی زیر را در نظر بگیرید:

$$\forall a, b \in G \quad a \sim b \Leftrightarrow ab^{-1} \in G$$

به بیان دیگر می‌توان گفت:

$$a \sim b \Leftrightarrow a \in Hb \Leftrightarrow Ha = Hb \Leftrightarrow \exists h \in H \quad a = hb$$

کلاس‌های هم‌ارزی رابطه فوق مجموعه‌های $\{Hb \,|\, b \in G\}$ هستند. توجه کنید برای هر $b \in G$ داریم:

$$|Hb| = |\{hb \in h \in H\}| = |H|.$$

به طور مشابه می‌توان رابطه هم‌ارزی زیر را تولید کرد:

$$a \sim b \Leftrightarrow aH = bH \quad (\Leftrightarrow b^{-1}a \in H \Leftrightarrow \exists h \in Ha = bh)$$

در این حالت نیز $|aH| = |H|$.

- قضیه لاگرانژ بیان می کند که اگر G یک گروه متناهی باشد و H زیرگروهی از G باشد، آن‌گاه $|H| \mid |G|$.

نتیجه ۱۰۱. فرض کنید G یک گروه متناهی باشد و H زیرگروهی از G باشد. فرض کنید

$$\mathcal{A} = \{aH \,|\, a \in G\}$$
$$\mathcal{B} = \{Ha \,|\, a \in G\}.$$

در این صورت $|\mathcal{A}| = |\mathcal{B}|$.

تعریف ۱۰۲. زیرگروه H از گروه G را نرمال می‌نامیم و با نماد $H \triangleleft G$ نشان می‌دهیم هرگاه $\mathcal{A} = \mathcal{B}$. به بیان دیگر هرگاه هر هم‌مجموعه‌ی راست یک هم‌مجموعه‌ی چپ باشد.

مشاهده: زیرگروه H از گروه G نرمال است اگر و تنها اگر برای هر $a \in G$ داشته باشیم: $Ha = aH$. به بیان معادل، زیرگروه H نرمال است اگر و تنها اگر برای هر $a \in G$ داشته باشیم: $a^{-1}Ha = H$ $(aHa^{-1} = H)$.
توجه شود که اگر $H \subseteq G$ نرمال باشد، در این صورت برای هر $a, b \in G$ داریم: $Ha \cdot Hb = Hab$؛ فرض کنید $hah'b \in Ha \cdot Hb$. چون $ah' \in aH$ و $aH = Ha$ پس $ah' \in Ha$ و $ah' = h''a$. در نتیجه $hah'b = hh''ab \in Hab$ پس $Ha \cdot Hb \subseteq Hab$. حال فرض کنید $hab \in Hab$. می‌توان نوشت که $hab = ha \cdot 1b \in Ha \cdot Hb$، پس $Hab \subseteq Ha \cdot Hb$.

تمرین ۱۱. نشان دهید که $H \subseteq G$ نرمال است اگر و تنها اگر برای هر $a, b \in H$ داشته باشیم: $Ha \cdot Hb = Hab$.

فرض کنید $H \lhd G$. قرار دهید: $\frac{G}{H} = \{Ha \,|\, a \in G\}$. در این صورت با ضربی که تعریف کردیم $\frac{G}{H}$ تشکیل یک گروه می‌دهد که به آن یک گروه خارج‌قسمتی گفته می‌شود. هومومرفیسم طبیعی $\varphi : G \to \frac{G}{H}$ که $\varphi(x) = xH$ را داریم.

تمرین ۱۲. زیر گروه N از G نرمال است اگر و تنها اگر گروه H و هموفریسم $\varphi : G \to H$ موجود باشند به طوری که $\mathrm{Ker}(\varphi) = N$.

یادآوری: فرض کنید $K \subseteq L$ یک توسیع نرمال باشد. در این صورت $K \subseteq E \subseteq L$ نرمال است اگر و تنها اگر برای هر اتومرفیسم $\sigma \in \mathrm{Gal}(L : K)$، داشته باشیم: $\sigma(E) = E$.

قضیه ۱۰۳. فرض کنید $K \subseteq L$ یک توسیع گالوایی باشد و $K \subseteq E \subseteq L$. در این صورت $K \subseteq E$ نرمال است اگر و تنها اگر $\Gamma(E) \lhd \mathrm{Gal}(L : K)$.

اثبات. فرض کنید $K \subseteq E$ یک توسیع نرمال باشد. فرض کنید $\sigma \in \mathrm{Gal}(L : K)$. نشان می‌دهیم که

$$\sigma\Gamma(E)\sigma^{-1} \subseteq \Gamma(E).$$

اتومرفیسم $f \in \Gamma(E)$ را در نظر بگیرید. باید نشان دهیم که $\sigma f \sigma^{-1} : L \to L$ تمام نقاط E را حفظ می‌کند. اگر $e \in E$، آنگاه $\sigma f \sigma^{-1}(e) = e$. برای جهت عکس، فرض کنید: $\Gamma(E) \lhd \mathrm{Gal}(L : K)$. نشان می‌دهیم که برای هر اتومرفیسم $\sigma \in \mathrm{Gal}(L : K)$ داریم: $\sigma(E) = E$. فرض کنید $\sigma \in \mathrm{Gal}(L : K)$. برای نشان دادن اینکه $\sigma(E) = E$ کافیست نشان دهیم که $\Gamma(\sigma(E)) = \Gamma(E)$. می‌دانیم که $\Gamma(E) \lhd \mathrm{Gal}(L : K)$، پس $\sigma\Gamma(E)\sigma^{-1} = \Gamma(E)$. ادعا می‌کنیم که $\sigma\Gamma(E)\sigma^{-1} = \Gamma(\sigma(E))$. فرض کنید $f \in \sigma\Gamma(E)\sigma^{-1}$، در این صورت $f = \sigma h \sigma^{-1}$ که $h \in \Gamma(E)$. باید نشان دهیم که f عناصر موجود در $\sigma(E)$ را حفظ می‌کند.

$$f(\sigma(e)) = \sigma h \sigma^{-1}(\sigma(e)) = \sigma h(e) = \sigma(e).$$

حال فرض کنید $f \in \Gamma(\sigma(E))$ یعنی f تمامی عناصر موجود در $\sigma(E)$ را حفظ کند. کافیست نشان دهیم $\sigma^{-1} f \sigma \in \Gamma(E)$. فرض کنید $e \in E$. در اینصورت $\sigma^{-1} f \sigma(e) = \sigma^{-1}\sigma(e) = e$. □

قضیه ۱۰۴. فرض کنید $K \subseteq L$ یک توسیع گالوایی باشد و $K \subseteq E \subseteq L$ نرمال باشد. در این صورت

$$\mathrm{Gal}(E : K) \cong \frac{\mathrm{Gal}(L : K)}{\mathrm{Gal}(L : E)}$$

اثبات. هومومرفیسم $\varphi : \mathrm{Gal}(L : K) \to \mathrm{Gal}(E : K)$ که $\varphi(\sigma) = \sigma|_E$ را در نظر بگیرید. به سادگی بررسی می‌شود که $\mathrm{Ker}(\varphi) = \mathrm{Gal}(L : E)$. □

تا اینجا **قضیه اساسی نظریه گالوا** را ثابت کردیم که به طور خلاصه به صورت زیر بیان می‌شود: فرض کنید $K \subseteq L$ یک توسیع گالوایی باشد. در این صورت یک تناظر یک‌به‌یک مانند φ بین میدان‌های میانی $K \subseteq E \subseteq L$ و زیرگروه‌های $H \subseteq \mathrm{Gal}(L : K)$ وجود دارد که $\varphi(E) = \mathrm{Gal}(L : E)$. $\Gamma(E) = \mathrm{Gal}(L : E)$. به بیان دیگر برای هر میدان میانی E داریم $\Phi(\Gamma(E)) = E$ و برای هر زیرگروه $H \subseteq \mathrm{Gal}(L : K)$ داریم: $\Gamma(\Phi(H)) = H$. همچنین

$$[L : E] = |\mathrm{Gal}(L : E)|$$
$$[L : K] = |\mathrm{Gal}(L : K)|$$
$$[E : K] = \frac{[L : K]}{[L : E]}$$
$$[E : K] = \frac{|\mathrm{Gal}(L : K)|}{|\mathrm{Gal}(L : E)|}$$

علاوه بر این، میدان میانی $K \subseteq E$ نرمال است اگر و تنها اگر $\Gamma(E) \lhd \mathrm{Gal}(L : E)$ و در این صورت

$$\mathrm{Gal}(E : K) \cong \frac{\mathrm{Gal}(L : K)}{\mathrm{Gal}(L : E)}$$

۱۸ جلسه نوزدهم: مروری بر گروه‌های آبلی متناهی

تعریف ۱۰۵. فرض کنید G یک گروه آبلی باشد و $U_1, U_2, \ldots, U_n$ زیرگروه‌هایی از G باشند. در این صورت می‌گوییم G حاصل‌جمع مستقیم زیرگروه‌های $U_1, U_2, \ldots, U_n$ است و می‌نویسیم $G = U_1 \bigoplus U_2 \bigoplus \ldots \bigoplus U_n$ هرگاه هر عنصر $a \in G$ به طور یکتا به صورت زیر نوشته شود:

$$a = u_1 + u_2 + \ldots + u_n$$

که $u_i \in U_i$. بنابراین اگر $a = u_1 + u_2 + \ldots + u_n = u'_1 + u'_2 + \ldots + u'_n$، آنگاه

$$(u_1 = u'_1) \wedge (u_2 = u'_2) \wedge \cdots \wedge (u_n = u'_n).$$

به بیان دیگر اگر $u_1 + u_2 + \ldots + u_n = 0$، آنگاه برای هر i داریم: $u_i = 0$.

نتیجه ۱۰۶. در تعریف قبل برای هر i و j داریم: $U_i \cap U_j = \{0\}$. زیرا برای مثال اگر $a \in U_i \cap U_j$، آنگاه
$a = a + 0 + 0 + \ldots + 0$ و $a = 0 + a + 0 + \ldots + 0$، یعنی a به دو طریق متفاوت نوشته می‌شود.

اگر $U_1, U_2, \ldots, U_n$ گروه‌هایی دلخواه باشند، آنگاه $U_1 \bigoplus U_2 \bigoplus \ldots \bigoplus U_n$ قابل تعریف است و اعضای این گروه به صورت $(a_1, a_2, \ldots, a_n)$ که $a_i \in U_i$. اگر $(a_1, a_2, \ldots, a_n)$ و $(b_1, b_2, \ldots, b_n)$ دو عضو از این گروه باشند، جمع آن‌ها به صورت $(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$ تعریف می‌شود.

یادآوری: فرض کنید G یک گروه آبلی متناهی باشد و $a \in G$. در این صورت می‌نویسیم: $\text{ord}(a) = n$ اگرو تنها اگر n کوچکترین عدد طبیعی باشد به طوری که $\underbrace{a + \ldots + a}_{n \text{ بار}} = 0$.
توجه شود که در یک گروه متناهی هر عنصر $a \in G$ دارای مرتبه است. همچنین برای هر $a \in G$ داریم: $\text{ord}(a) \mid |G|$.
از این به بعد برای راحتی کار، $\underbrace{a + \ldots + a}_{n \text{ بار}}$ را با na نشان می‌دهیم. فرض کنید $n \in \mathbb{N}$ به گونه‌ای باشد که $na = 0$. در این صورت $\text{ord}(a) \mid n$. زیرا فرض کنید $\text{ord}(a) = m$. داریم: $n = mq + r$ که $r < m$. بنابراین $na = mqa + ra$ پس $ra = 0$ و $r < m$. بنابراین $r = 0$ پس $m|n$.

لم ۱۰۷. فرض کنید $(G, +, 0)$ یک گروه آبلی متناهی باشد و $a \in G$ به گونه‌ای باشد که $\text{ord}(a) = ma$ که $(m, n) = 1$. در این صورت a را می‌توان به صورت یکتا به صورت $a = b + c$ نوشت به طوری که $\text{ord}(b) = m$ و $\text{ord}(c) = n$

اثبات. از آنجا که $(m, n) = 1$، اعداد صحیح s و t موجودند که $sm + tn = 1$، بنابراین $a = (sm)a + (tn)a$. ادعا می‌کنیم که $\text{ord}((sm)a) = n$. اولاً $n(sma) = 0$. حال فرض

کنید $n'(sma) = 0$، در این صورت $(n'sm)a = 0$ و از آنجا که مرتبه a برابر mn است داریم: $mn|n'sma$ پس $n|n's$. از طرفی $(n, s) = 1$ پس $n|n'$. به طور مشابه نشان داده می‌شود که $\text{ord}((tn)a) = m$. حال به اثبات یکتایی می‌پردازیم، فرض کنید $a = b + c$ و $a + b' + c'$ که $\text{ord}(b) = \text{ord}(b') = m$ و $\text{ord}(c) = \text{ord}(c') = n$ که $\text{ord}(a) = mn$. بنابراین $b + c = b' + c'$ یعنی $(b - b') = (c' - c)$. فرض کنید $(b - b') = (c' - c) = d$. پس $md = nd = 0$ بنابراین $\text{ord}(d) \mid m$ و $\text{ord}(d) \mid n$. یعنی $\text{ord}(d) = 1$ پس $c = c'$ و $b = b'$. □

لم فوق را می‌توان تعمیم داد، یعنی برای مثال اگر $\text{ord}(a) = mnk$ که m، n و k دو به دو نسبت بهم اول باشد، آنگاه a را می‌توان به صورت یکتا بصورت $a = a_1 + a_2 + a_3$ نوشت. توجه کنید که $(mn, k) = 1$، بنابراین می‌توان نوشت: $a = b + c$ که $\text{ord}(b) = mn$ و $\text{ord}(c) = k$. همچنین b را می‌توان به صورت $b = a_1 + a_2$ نوشت. به طور کلی اگر $\text{ord}(a) = m_1 m_2 \cdots m_k$ که $(m_i, m_j) = 1$، آنگاه (به صورت یکتا) $a = a_1 + a_2 + \ldots + a_k$ که $\text{ord}(a_i) = m_i$.

فرض کنید G یک گروه آبلی متناهی باشد که $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. در این صورت هر عنصر $a \in G$ مرتبه‌اش $|G|$ را عاد می‌کند. قرار دهید

$$U_i = \{a \in G \mid \text{ord}(G) \text{ توانی از } p_i \text{ باشد}\}$$

ادعا می‌کنیم که هر U_i یک زیرگروه از G است. فرض کنید $a, b \in U_i$ نشان می‌دهیم که $a - b \in U_i$. چون $a, b \in U_i$ پس $p_i^{\beta_1} a = 0$ و $p_i^{\beta_2} b = 0$. بنابراین $p_i^{\beta_1+\beta_2}(a - b) = 0$. پس $\text{ord}(a - b) \mid p_i^{\beta_1+\beta_2}$ یعنی مرتبه‌ی $a - b$ توانی از p_i است. از طرفی فرض کنید $a \in G$ دلخواه باشد و $\text{ord}(a) = p_1^{\beta_1} \cdots p_k^{\beta_k}$. در این صورت a را می‌توان به صورت یکتا به صورت حاصل‌جمعی از عناصر با مرتبه‌های $p_i^{\beta_i}$ نوشت. بنابراین قضیه زیر را داریم.

قضیه ۱۰۸. اگر G یک گروه آبلی متناهی باشد، آنگاه G حاصل‌جمعی مستقیم از pـزیرگروه‌ها است. یعنی

$$G = U_1 \bigoplus U_2 \bigoplus \cdots \bigoplus U_k$$

و مرتبه هر عنصر در U_i توانی از یک عدد اول p_i است.

قضیه ۱۰۹ (قضیه اساسی گروه‌های آبلی متناهی). فرض کنید G یک گروه آبلی متناهی باشد. در

این صورت G حاصل‌جمعی مستقیم از زیرگروه‌های دوری است. به بیان دیگر $a_1, \dots, a_n \in G$ موجودند به طوری که $G = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \cdots \oplus \langle a_n \rangle$.

اثبات. بنابر قضیه قبل، فرض می‌کنیم که G یک pـ گروه است. فرض کنید $a \in G$ عنصری با مرتبه‌ی ماکزیمال باشد. اگر $G = \langle a \rangle$، در این صورت حکم ثابت شده است. فرض کنید $G \neq \langle a \rangle$. هدف پیدا کردن عناصر $a_1, a_2, \dots a_k$ است که $\langle a_1, a_2, \dots a_k \rangle = \langle a_1 \rangle \oplus \cdots \oplus \langle a_k \rangle$. فعلا به دنبال عنصر a_2 هستیم به طوری که $a_2 \in G - \langle a_1 \rangle$ و $\langle a_1, a_2 \rangle = \langle a_1 \rangle \oplus \langle a_2 \rangle$. فرض کنید $b \in G - \langle a_1 \rangle$. فرض کنید λ کوچکترین عددی باشد که $\lambda b \in \langle a_1 \rangle$. بنابراین $\lambda b = \mu a_1$ که $\lambda, \mu \in \mathbb{N}$. قرار دهید $a_2 = b - \frac{\mu}{\lambda} a_1$ (بعداً نشان می‌دهیم که $\lambda | \mu$). دقت کنید که $\lambda a_2 = 0$. ادعا می‌کنیم که $\langle a_1, a_2 \rangle = \langle a_1 \rangle \oplus \langle a_2 \rangle$. فرض کنید $ma_1 = na_2$، در این صورت $ma_1 = nb - n\frac{\mu}{\lambda} a_1$. یعنی $nb \in \langle a_1 \rangle$ پس $\lambda | n$ و $na_2 = 0$. اثبات اینکه $\lambda | \mu$، توجه کنید که $b \in G$، بنابراین $\mathrm{ord}(b) = p^\beta$. از طرفی $\mathrm{ord}(a_1) = p^\alpha$ دقت کنید که باید داشته باشیم: $\beta \leq \alpha$. ادعا می‌کنیم که λ به صورت توانی از p است. توجه کنید که $p^\beta = \lambda q + r$ پس $p^\beta b = \lambda q b + r b$. چون $p^\beta b, \lambda q b \in \langle a_1 \rangle$ پس $r = 0$. حال نشان می‌دهیم که $\lambda | \mu$. می‌دانیم که $\lambda b = \mu a_1$ پس $\frac{p^\beta}{\lambda} \lambda b = \frac{p^\beta}{\lambda} \mu a_1$. در نتیجه $0 = p^\beta \frac{\mu}{\lambda} a_1$ پس $p^\alpha | p^\beta \frac{\mu}{\lambda}$. بنابراین $\frac{\mu}{\lambda} \in \mathbb{N}$.
فرض کنید a_1 و a_2 را پیدا کرده‌ایم که $\langle a_1, a_2 \rangle = \langle a_1 \rangle \oplus \langle a_2 \rangle$. فرض کنید $b \in G - \langle a_1, a_2 \rangle$، عدد λ را به گونه‌ای در نظر بگیرید که $\lambda b \in \langle a_1, a_2 \rangle$. بنابراین $\lambda b = \mu_1 a_1 + \mu_2 a_2$، مشابه حالت قبل، بررسی می‌شود که $\lambda = p^\beta = \mathrm{ord}(b)$ و $\lambda | \mu_1, \mu_2$. عنصر $a_2 = b - \frac{\mu_1}{\lambda} a_1 - \frac{\mu_2}{\lambda} a_2$ را در نظر بگیرید و ثابت می‌شود که $\langle a_1, a_2, a_3 \rangle = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \langle a_3 \rangle$. با ادامه‌ی این روند خواهیم داشت که $G = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \cdots \oplus \langle a_n \rangle$. □

۱۹ جلسه بیستم: مروری بر گروه‌های متناهی (قضیه‌ی سیلو)

فرض کنید G یک گروه باشد، $N \triangleleft G$ و $H \subseteq G$ زیرگروه باشد. زیرگروه تولید شده توسط $H \cup N$ در G را با $\langle H, N \rangle$ نشان می‌دهیم.می‌توان نشان داد که $\langle H, N \rangle = HN = \{hn \,|\, h \in H, n \in N\}$.

تمرین ۱۳. با فرض‌هایی که در بالا گفته شد، نشان دهید که HN یک گروه است.

قضیه ۱۱۰. فرض کنید G یک گروه باشد، $N \lhd G$ و $H \subseteq G$ زیرگروه باشد. در این صورت

$$\frac{HN}{N} \cong \frac{H}{H \cap N}$$

اثبات. به سادگی بررسی می‌شود که $N \lhd HN$ و $H \cap N \lhd H$. نگاشت $\varphi : H \to \frac{G}{N}$ که $\varphi(x) = xN$ را در نظر بگیرید. به عنوان تمرین بررسی کنید که φ یک هومومرفیسم است. توجه شود که

$$\mathrm{Im}(\varphi) = \{xN \,|\, x \in H\} = \frac{HN}{N}$$
$$\mathrm{Ker}(\varphi) = \{x \in H \,|\, xN = N\} = \{x \in H \,|\, x \in N\} = H \cap N$$

بنابراین $\frac{H}{\mathrm{Ker}(\varphi)} \cong \mathrm{Im}(\varphi)$، در نتیجه $\frac{HN}{N} \cong \frac{H}{H \cap N}$. □

قضیه ۱۱۱. فرض کنید G یک گروه آبلی متناهی باشد و $p \,||G|$ که p یک عدد اول است. در این صورت G دارای عنصری با مرتبه‌ی p است.

اثبات. با استقرا روی اندازه‌ی G. فرض کنید حکم برای گروه‌های با اندازه اکیداً کمتر از اندازه‌ی G برقرار باشد. فرض کنید $M \subseteq G$ یک زیرگروه ماکزیمال سره باشد. دو حالت ممکن است رخ دهد، حالت اول: اگر $p \,||M|$، آنگاه بنابر فرض استقرا، M عنصری با مرتبه‌ی p دارد. حالت دوم: اگر $p \not| \,|M|$. فرض کنید $a \in G - M$، توجه کنید $\langle a \rangle M = G$. بنا به قضیه قبل، $\frac{\langle a \rangle M}{M} \cong \frac{\langle a \rangle}{M \cap \langle a \rangle}$. بنابراین $\frac{|G|}{|M|} = \frac{\mathrm{ord}(a)}{|M \cap \langle a \rangle|}$. پس $p|\mathrm{ord}(a)$، یعنی اگر $\mathrm{ord}(a) = r$، آنگاه $a^r = 1$. یعنی $(a^{\frac{r}{p}})^p = 1$ پس $\mathrm{ord}(a^{\frac{r}{p}}) = p$. □

فرض کنید G یک گروه باشد. رابطه‌ی زیر را روی G در نظر بگیرید:

$$a \sim b \quad \Leftrightarrow \quad \exists g \in G ga = bg \quad \Leftrightarrow \quad gag^{-1} = b$$

به عنوان تمرین بررسی کنید که رابطه‌ی فوق یک رابطه هم‌ارزی است. کلاس هم‌ارزی یک عنصر $a \in G$ را با $C(a)$ نشان می‌دهیم و $C(a) = \{gag^{-1} \,|\, g \in G\}$. می‌توان فرض کنید که G

توسط کلاس‌های هم‌ارزی $C(a_1), C(a_2), \ldots, C(a_k)$ افراز می‌شود. توجه کنید که $a \in C(a)$ و $C(e) = \{geg^{-1} \mid g \in G\} = \{e\}$ یعنی

$$|G| = 1 + |C(a_1)| + \ldots + |C(a_k)|$$

تعریف ۱۱۲. برای هر عنصر $a \in G$ تعریف کنید: $Z(a) = \{g \in G \mid ga = ag\} = \{g \in G \mid gag^{-1} = a\}$.

تمرین ۱۴. نشان دهید که $Z(a)$ یک زیرگروه از گروه G است.

قضیه ۱۱۳. فرض کنید G یک گروه باشد و $a \in G$. در اینصورت $|C(a)| = [G : Z(a)] = \frac{|G|}{Z(a)}$.

اثبات. فرض کنید $xax^{-1}, yay^{-1} \in C(a) = \{xax^{-1} \mid x \in G\}$. در این صورت

$$xax^{-1} = yay^{-1} \Leftrightarrow ax^{-1} = x^{-1}yay^{-1} \Leftrightarrow ax^{-1}y = x^{-1}ya \Leftrightarrow x^{-1} \in Z(a)$$

بنابراین تعداد عناصر مختلف موجود در $C(a)$ متناظر هست با تعداد کلاس‌های مختلف هم‌مجموعه‌های روی $[G : Z(a)]$. □

تعریف ۱۱۴. فرض کنید G یک گروه باشد. تعریف کنید: $Z(G) = \{a \in G \mid \forall g \in G \quad ag = ga\}$.

تمرین ۱۵. نشان دهید که $Z(G) \lhd G$.

قضیه ۱۱۵ (قضیه سیلو). فرض کنید G یک گروه متناهی باشد و $|G| = p^r m$ که p یک عدد اول است و $p \nmid m$ یعنی $p \mid |G|, p^2 \mid |G|, \ldots, p^r \mid |G|$ و $p^{r+1} \nmid |G|$. در این صورت G دارای یک زیرگروه با اندازه p^r است.

اثبات. با استقرا روی $|G|$. فرض کنید حکم برای گروه‌های با اندازه اکیداً کمتر از اندازه G برقرا باشد. فرض کنید G توسط کلاس‌های هم‌ارزی $C(a_1), C(a_2), \ldots, C(a_n)$ افراز شده باشد. توجه کنید که

$$|G| = p^r m = |C(a_1)| + |C(a_2)| + \ldots + |C(a_n)|$$

فرض کنید $|C(a)| \neq 1$ و $p \nmid |C(a)|$. پس $p \nmid \frac{|G|}{Z(a)} = \frac{p^r m}{|Z(a)|}$. بنابراین $p^r | Z(a)$، از طرفی $p^{r+1} \nmid Z(z)$ اما $Z(a)$ یک گروه سره از G است و بنابر فرض استقرا $Z(a)$ دارای یک زیرگروه با اندازه‌ی p^r است. بنابراین فرض کنید برای هر a_i یا $p | C(a_i)|$ یا $|C(a_i)| = 1$. مشاهده کنید که

$$\begin{aligned} |C(a)| = 1 &\Leftrightarrow C(a) = \{a\} \\ &\Leftrightarrow \{x^{-1}ax \,|\, x \in g\} = \{a\} \\ &\Leftrightarrow \forall x \in g(x^{-1}ax = a) \\ &\Leftrightarrow \forall x \in g(ax = xa) \\ &\Leftrightarrow a \in Z(G) \end{aligned}$$

بنابراین $|G| = p^r m = |Z(G)| + pv$. توجه کنید که $p \,||Z(G)|$ و $Z(G)$ یک گروه آبلی است. بنابراین $Z(G)$ حاوی یک عنصر a با مرتبه p است، یعنی $|\langle a \rangle| = p$. پس $|\frac{G}{\langle a \rangle}| = p^{r-1}m$. بنابراین بنا به فرض استقرا $\frac{G}{\langle a \rangle}$ دارای یک زیرگروه است به صورت $\frac{U}{\langle a \rangle}$ که $U \subseteq G$ به طوری که $|\frac{U}{\langle a \rangle}| = p^{r-1}$. بنابراین U زیرگروهی از G است و $|U| = p^r$. □

نتیجه ۱۱۶. فرض کنید G یک گروه متناهی باشد و $p \,||G|$ که p عددی اول است. در این صورت G حاوی عنصری با مرتبه‌ی p است.

اثبات. فرض کنید $p^r \,||G|$ و $p^{r+1} \nmid |G|$. در این صورت G دارای زیرگروهی با اندازه p^r است. مرتبه‌ی تمام عناصر موجود در این زیرگروه به صورت p^k است. فرض کنید a عنصری با مرتبه‌ی p^k باشد، یعنی $a^{p^k} = e$. یعنی عنصر $a^{p^{k-1}}$ عنصر مورد نظر ماست. □

۲۰ جلسات بیست‌یکم و بیست‌دوم: قضیه اساسی جبر

یادآوری:

- فرض کنید $K \subseteq L$ یک توسیع گالوایی باشد و $G = \mathrm{Gal}(L : K)$. برای هر زیرگروه $H \subseteq G$ یک میدان میدانی $K \subseteq \Phi(H) \subseteq L$ وجود دارد و $[\Phi(H) : K] = [G : H]$. از طرفی $[L : \Phi(H)] = |H|$ و $[L : K] = |G|$ به طور خاص اگر $H \subseteq G$ به‌گونه‌ای باشد که $[G : H] = n$، آنگاه $[\Phi(H) : K] = n$.

- اگر G یک گروه متناهی باشد که $p \mid |G|$ و n بزرگترین عددی باشد که $p^n \mid |G|$، آنگاه G دارای یک زیرگروه H با اندازه p^n است و H را یک pـ زیرگروه سیلوی G می‌نامیم. با توجه به اینکه $[G : H] = \frac{|G|}{|H|}$، اگر H یک زیرگروه pـ سیلوی G باشد، آنگاه $p \nmid [G : H]$.

تمرین ۱۶. با فرضیات قضیه سیلو، ثابت کنید که G دارای زیرگروهی با هر اندازه‌ی p^i برای $1 \leq i \leq n$ است.

با توجه به اینکه چندجمله‌ای $x^2 + 1 \in \mathbb{R}[x]$ تحویل‌ناپذیر است. میدان $\mathbb{R} \subseteq \frac{\mathbb{R}[x]}{\langle x^2+1 \rangle}$ را میدان اعداد مختلط می‌نامیم و آن‌را با $\mathbb{C}$ نشان می‌دهیم. در واقع $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ و $[\mathbb{C} : \mathbb{R}] = 2$.

مشاهده:

- هر چندجمله‌ای با درجه‌ی فرد در $\mathbb{R}[x]$ دارای یک ریشه در $\mathbb{R}$ است. پس چندجمله‌ای‌های تحویل‌ناپذیر در $\mathbb{R}[x]$ حتما دارای درجه زوج هستند.
- چندجمله‌ای‌های با درجه 2 در $\mathbb{C}[x]$ به طور کامل در $\mathbb{C}$ تجزیه می‌شوند.
- فرض کنید توسیع $K \subseteq L$ جبری و جدایی‌پذیر باشد و $K \subseteq L \subseteq N$ بستار نرمال K شامل L باشد. هر چندجمله‌ای با ضرایب K اگر یک ریشه در L داشته باشد، همه‌ی ریشه‌های آن در N است. اگر $f \in K[x]$ در L هیچ ریشه‌ای نداشته باشد در N هم هیچ ریشه‌ای ندارد.

تمرین ۱۷. اگر $K \subseteq L$ جدایی‌پذیر باشد و $K \subseteq L \subseteq N$ بستار نرمال K شامل L باشد، آنگاه $K \subseteq L$ جدایی‌پذیر است ($K \subseteq L$ توسیع گالوایی است).

قضیه ۱۱۷. فرض کنید K یک میدان نامتناهی باشد و $K \subseteq L$ یک توسیع جدایی‌پذیر متناهی باشد $([L : K] = n)$. در این صورت $K \subseteq L$ یک توسیع ساده است، یعنی $L = K(u)$.

اثبات. فرض کنید $u \in L - K$ به گونه‌ای باشد که $[K(u) : K]$ ماکزیمال باشد. فرض کنید $v \in L - K(u)$، در این صورت تمامی میدان‌های به صورت $K(u + v)$ را در نظر بگیرید. ادعا می‌کنیم که $a, b \in K$ موجودند به طوری که $K(u + av) = K(u + bv)$. اگر این گونه نباشد، آنگاه نامتناهی میدان متفاوت بین K و L پیدا می‌شوند. این امکان‌پذیر نیست؛ زیرا اگر بستار نرمال

L را به صورت $K \subseteq L \subseteq N$ را در نظر بگیریم، آنگاه این توسیع گالوایی است. بنابراین تعداد میدان‌های بین K و L برابر است با اندازه گروه $\mathrm{Gal}(N : K)$. پس فرض کنید $a, b \in K$ موجودند به طوری که $K(u + av) = K(u + bv)$. پس $u + av, u + bv \in K(u + av)$ و در نتیجه $(a-b)v \in K(u+av)$ پس $u, v \in K(u+av)$. در این صورت $K \subseteq K(u) \subsetneq K(u+av)$ و این با ماکزیمال بودن $[K(u) : K]$ در تناقض است. □

قضیه ۱۱۸. در میدان اعداد مختلط $\mathbb{C}$، هر چندجمله‌ای $f \in \mathbb{C}[x]$ به طور کامل تجزیه می‌شود. به بیان دیگر هیچ توسیع جبری $K \subsetneq \mathbb{C}$ وجود ندارد.

اثبات. توسیع $\mathbb{R} \subseteq \mathbb{C}$ را در نظر بگیرید. اگر $\mathbb{C}$ بسته جبری نباشد، آنگاه یک توسیع گالوایی $\mathbb{R} \subsetneq L$ موجود است که $\mathbb{R} \subseteq \mathbb{C} \subseteq L$. توجه کنید $[L : \mathbb{R}] = [L : \mathbb{C}][\mathbb{C} : \mathbb{R}]$ و $[\mathbb{C} : \mathbb{R}] = 2$ پس $2|[L : \mathbb{R}]$. به بیان دیگر اگر $G = \mathrm{Gal}(L : \mathbb{R})$، آنگاه $2||G|$. بنابراین G دارای یک زیرگروه 2ـسیلو به نام H است و $|H| = 2^n$. ادعا می‌کنیم که $H = G$. فرض کنید $H \neq G$، پس $\mathbb{R} \subseteq \Phi(H) \subseteq L$ را در نظر بگیرید. در این اینصورت $[\Phi(H) : \mathbb{R}] = [G : H] = \dfrac{|G|}{|H|}$. پس $[\Phi(H) : \mathbb{R}]$ یک توسیع با درجه‌ی فرد است. بنا به قضیه قبل، $\Phi(H) = \mathbb{R}(u)$ که u ریشه‌ی چندجمله‌ای تحویل‌ناپذیر با درجه‌ی فرد است و این تناقض است.
اکنون با توجه به اینکه $\mathbb{C} \subseteq L$ یک توسیع گالوایی است، $[L : \mathbb{R}] = 2^n$ و $[\mathbb{C} : \mathbb{R}] = 2$ داریم:

$$\mathrm{Gal}(L : \mathbb{C}) = [L : \mathbb{C}] = \frac{[L : \mathbb{R}]}{[\mathbb{C} : \mathbb{R}]} = 2^{n-1}$$

ادعا می‌کنیم $n = 1$. فرض کنید $n > 1$، در این صورت $\mathrm{Gal}(L : \mathbb{C})$ دارای یک زیرگروه سره H' با اندیس 2 خواهد بود، یعنی $[\mathrm{Gal}(L : \mathbb{C}) : H'] = 2$. بنابراین میدان $\mathbb{C} \subsetneq \Phi(H') \subseteq L$ پیدا می‌شود که $[\Phi(H') : \mathbb{C}] = 2$. این تناقض است چون اگر $[\Phi(H') : \mathbb{C}]$، آنگاه $\mathbb{C}(u) = \Phi(H')$ که u ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر با درجه‌ی 2 است اما ما می‌دانیم که هر چندجمله‌ای با درجه 2 به طور کامل در $\mathbb{C}[x]$ تجزیه می‌شود. □

نتیجه ۱۱۹. با توجه به اینکه اگر $f(x) \in \mathbb{C}[x]$، آنگاه $f(x) = (x - a_1)^{n_1} \dots (x - a_k)^{n_k}$. فرض کنید $f(x) \in \mathbb{R}[x]$، در این صورت تجزیه‌ی $f(x) = (x - a_1)^{n_1} \dots (x - a_k)^{n_k}$ در $\mathbb{C}$ را برای f داریم. مشاهده کنید که اگر $z = a + bi$ ریشه‌ی $f(x) \in \mathbb{R}[x]$ باشد، آنگاه $\overline{z} = a - bi$

نیز ریشه‌ی f است. همچنین $(x-z)(x-\overline{z}) = x^2 - (z+\overline{z}) + z\overline{z}$ که $z+\overline{z}, z\overline{z} \in \mathbb{R}$.
بنابراین، هر چندجمله‌ای $f \in \mathbb{R}[x]$ به عوامل تحویل‌ناپذیر از درجه‌ی یک و دو تجزیه می‌شود.

۲۱ جلسه بیست و سوم: استقلال جبری و درجه تعالی

در این جلسه، همه‌ی میدان‌ها را با مشخصه صفر در نظر میگیریم. در جبر خطی، عناصر $a_1, \ldots, a_n$ از فضای برداری V روی K را مستقل خطی می‌نامیم هرگاه اگر

$$r_1 a_1 + r_2 a_2 + \ldots + r_n a_n = 0$$

که $r_i \in K$، آنگاه $r_1 = r_2 = \ldots = r_n = 0$. پایه‌ی یک فضای برداری برابر است با یک مجموعه‌ی مستقل خطی ماکزیمال و اگر B_1 و B_2 دو پایه برای یک فضای برداری باشند، آنگاه $|B_1| = |B_2|$. اندازه یک پایه برای فضای برداری را بُعد آن فضا می‌نامیم. در این درس هم برای توسیع میدانی $K \subseteq L$، بعد $[L : K]$ را به صورت بعد فضای برداری L روی K در نظر گرفتیم.

تعریف ۱۲۰. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. در این صورت می‌گوییم L روی K متناهیاً تولید می‌شود هرگاه عناصر $\alpha_1, \ldots, \alpha_n \in L$ موجود باشند به طوری که $L = K(\alpha_1, \ldots, \alpha_n)$.

توجه کنید اگر $\alpha \in L - K$ روی K جبری باشد، آنگاه $[K(\alpha) : K] = n = \deg(f)$ که f چندجمله‌ای مینیمال α است. اما به عنوان میدان $K(\alpha)$ فقط با یک عنصر تولید می‌شود. اگر $\alpha \in L - K$ متعالی باشد، آنگاه $[K(\alpha) : K] = +\infty$ از لحاظ میدانی، $K(\alpha)$ با یک عنصر α روی K تولید می‌شود.

تعریف ۱۲۱ (استقلال جبری)**.** فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. عناصر $\alpha_1, \ldots, \alpha_n \in L - K$ را مستقل جبری روی K می‌نامیم هرگاه برای هر چندجمله‌ای $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ متغیره‌ی n اگر $f(\alpha_1, \ldots, \alpha_n) = 0$، آنگاه $f = 0$.

مشاهده:

- α روی K مستقل جبری است هرگاه α روی K متعالی باشد، به بیان دیگر $\alpha \notin K^{\text{alg}}$.
- اگر α, β روی K مستقل جبری باشند، آنگاه

- α روی K متعالی است، یعنی $\alpha \notin K^{\text{alg}}$.
- β روی K متعالی است، یعنی $\beta \notin K^{\text{alg}}$.
- α روی $K(\beta)$ متعالی است، یعنی $\alpha \notin (K(\beta))^{\text{alg}}$.
- β روی $K(\alpha)$ متعالی است، یعنی $\beta \notin (K(\alpha))^{\text{alg}}$.

- $\alpha_1, \ldots, \alpha_n$ روی K مستقل جبری هستند یعنی برای هر $1 \leq i \leq n$، $\alpha_i \notin (K(\alpha_1, \ldots, \alpha_n))^{\text{alg}}$.

تعریف ۱۲۲. فرض کنید $K \subseteq L$ و $L = K(\alpha_1, \ldots, \alpha_n)$ که $\alpha_1, \ldots, \alpha_n \in L - K$. فرض کنید $B \subseteq L$ یک زیرمجموعه‌ی مستقل جبری ماکزیمال روی K باشد. اندازه‌ی مجموعه‌ی B یعنی $|B|$ را درجه تعالی L روی K می‌نامیم و آن‌را با $\text{trdeg}(\frac{L}{K})$ یا $\text{trdeg}(L : K)$ نشان می‌دهیم. برای مثال $\text{trdeg}(\mathbb{C} : \mathbb{Q}) = 2^{\aleph_0}$.

توجه کنید که $[L : K(B)]$ متناهی است پس $L \subseteq K(B)$ یک توسیع جبری است. همچنین مجموعه‌ی B متناهی است؛ می‌دانیم که $[L : K(B)]$ متناهی است، پس $L = K(B)(\alpha)$ که α جبری است. از طرفی چون $L = K(\alpha_1, \ldots, \alpha_n)$ پس $\alpha_1, \ldots, \alpha_n \in K(B)(\alpha)$. بنابراین $B' \subseteq B$ موجود است به طوری که $[L : K(B')]$ متناهی است.

تمرین ۱۸. الف) نشان دهید که اگر $[L : K]$ متناهی باشد، آنگاه لزوماً توسیع $K \subseteq L$ جبری نیست.
ب) فرض کنید $K \subseteq L$ و $L = K(\alpha_1, \ldots, \alpha_n)$ که $\alpha_1, \ldots, \alpha_n \in L - K$. فرض کنید $B \subseteq L$ یک زیرمجموعه‌ی مستقل جبری ماکزیمال روی K باشد. نشان دهید که $[L : K(B)]$ متناهی است.

لم ۱۲۳. فرض کنید $K \subseteq L$ و $L = K(\alpha_1, \ldots, \alpha_n)$. فرض کنید $B = \{b_1, \ldots b_n\}$ و $C = \{c_1, \ldots c_m\}$ مجموعه‌های مستقل جبری باشند به طوری که $[L : K(B)]$ و $[L : K(C)]$ متناهی باشند. در این صورت $|C| = |B|$.

اثبات. فرض کنید $m < n$. توجه کنید که $K(x_1, \ldots, x_m) \cong K(c_1, \ldots, c_m) \cong K(b_1, \ldots, b_m)$. چون $[L : K(C)]$ متناهی است، پس $[L : K(b_1, \ldots, b_m)]$ متناهی است و این تناقض است (در قضیه ۱۲۶، این لم را به صورت دقیق ثابت کرده‌ایم). □

قضیه ۱۲۴. فرض کنید L_1 و L_2 دو میدان بسته جبری باشند به طوری که هر دو شامل K باشند و

$$\text{trdeg}(\frac{L_1}{K}) = \text{trdeg}(\frac{L_2}{K})$$

در این صورت $L_1 \cong_K L_2$.

اثبات. فرض کنید B_1 پایه‌ی L_1 و B_2 پایه‌ی L_2 روی K باشند. در این صورت $K(B_1) \cong K(B_2)$. بنابراین L_i بستار جبری $K(B_i)$ است پس $L_1 \cong_K L_2$. □

لم ۱۲۵. هر دو میدان بسته‌ی جبری هم‌اندازه و ناشمارا با هم ایزومرف هستند.

اثبات. فرض کنید L_1 و L_2 دو میدان بسته جبری با اندازه $2^{\aleph_0}$ باشند. پس هر دو میدان شامل $\mathbb{Q}$ هستند (اگر مشخصه p بود، آنگاه شامل $\mathbb{Z}_p$ می‌شدند). توجه کنید که $\text{trdeg}(\frac{L_1}{\mathbb{Q}}) = \text{trdeg}(\frac{L_2}{\mathbb{Q}}) = 2^{\aleph_0}$. پس بنا به قضیه قبل، $L_1 \cong_K L_2$. □

تمرین ۱۹. آیا دو میدان بسته‌ی جبری شمارا نیز با هم ایزومرف هستند؟

قضیه ۱۲۶. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد و $\alpha_1, \ldots, \alpha_n$ یک پایه‌ی تعالی L روی K باشد، یعنی توسیع $K(\alpha_1, \ldots, \alpha_n) \subseteq L$ جبری است. همچنین فرض کنید $\beta_1, \ldots, \beta_m$ یک پایه‌ی تعالی دیگری برای L روی K باشد، یعنی توسیع $K(\beta_1, \ldots, \beta_m) \subseteq L$ جبری است. در این صورت $m = n$

اثبات. برای راحتی، فرض کنید $\alpha_1, \alpha_2, \alpha_3$ و $\beta_1, \ldots, \beta_m$ پایه‌های تعالی برای L روی K باشند. نشان می‌دهیم که $m = 3$. توجه کنید که توسیع $K(\alpha_1, \alpha_2, \alpha_3) \subseteq L$ جبری است. بنابراین β_1 روی $K(\alpha_1, \alpha_2, \alpha_3)$ جبری است. یعنی یک چندجمله‌ای f با ضرایب در K یافت می‌شود به طوری که $f(\alpha_1, \alpha_2, \alpha_3, \beta_1) = 0$. توجه کنید که β_1 روی K جبری نیست. بنابراین حداقل یکی از α_iها در f ظاهر می‌شود. فرض کنید α_1 در f ظاهر شده است. از اینکه $f(\alpha_1, \alpha_2, \alpha_3, \beta_1) = 0$ نتیجه می‌گیریم که $\alpha_1 \in K(\alpha_2, \alpha_3, \beta_1)$. به طور خاص، $K(\alpha_1, \alpha_2, \alpha_3) \subseteq (K(\alpha_2, \alpha_3, \beta_1))^{\text{alg}}$. به طور مشابه β_2 روی $K(\alpha_1, \alpha_2, \alpha_3)$ جبری است یعنی β_2 روی $(K(\alpha_2, \alpha_3, \beta_1))^{\text{alg}}$ جبری است یعنی β_2 روی $K(\alpha_2, \alpha_3, \beta_1)$ جبری است. بنابراین چندجمله‌ای مانند f پیدا می‌شود که $f(\alpha_2, \alpha_3, \beta_1, \beta_2) = 0$ و چندجمله‌ای f حتما شامل یکی از α_iها است. فرض کنید α_2 در

چندجمله‌ای یاد شده استفاده شده باشد. بنابراین $\alpha_2 \in (K(\alpha_3,\beta_1,\beta_2))^{\text{alg}}$. دقت کنید که $K(\alpha_1,\alpha_2,\alpha_3) \subseteq (K(\alpha_3,\beta_1,\beta_2))^{\text{alg}}$. حال β_3 روی $K(\alpha_1,\alpha_2,\alpha_3)$ و از این رو روی $K(\alpha_3,\beta_1,\beta_2)$ جبری است و مشابه قبل $\alpha_3 \in (K(\beta_1,\beta_2,\beta_3))^{\text{alg}}$. در نتیجه $\alpha_1,\alpha_2,\alpha_3 \in (K(\beta_1,\beta_2,\beta_3))^{\text{alg}}$. پس $(K(\alpha_1,\alpha_2,\alpha_3))^{\text{alg}} \supseteq L$، بنابراین $(K(\beta_1,\beta_2,\beta_3))^{\text{alg}} \supseteq L$ □

۲۲ جلسه بیست و چهارم: حدس شانوئل، ترسیم توسط خطکش و پرگار

درجه تعالی $\mathbb{Q}(e)$ روی $\mathbb{Q}$، یعنی $\frac{\mathbb{Q}(e)}{\mathbb{Q}}$ چند است؟ درجه تعالی $\mathbb{Q}(\pi)$ روی $\mathbb{Q}$، یعنی $\frac{\mathbb{Q}(\pi)}{\mathbb{Q}}$ چند است؟ درجه تعالی $\mathbb{Q}(e,\pi)$ روی $\mathbb{Q}$، یعنی $\frac{\mathbb{Q}(e,\pi)}{\mathbb{Q}}$ چند است؟ آیا $e \in (\mathbb{Q}(\pi))^{\text{alg}}$؟ آیا یک چندجمله‌ای با ضرایب در $\mathbb{Q}(\pi)$ پیدا می‌شود که e ریشه‌ی آن باشد؟

قضیه ۱۲۷ (لیندمان‌ـ وایراشتراس). فرض کنید $\alpha_1,\alpha_2,\ldots,\alpha_n$ عناصری باشند که روی $\mathbb{Q}$ جبری و مستقل خطی هستند. در این صورت $e^{\alpha_1},e^{\alpha_2},\ldots,e^{\alpha_n}$ روی $\mathbb{Q}$ مستقل جبری هستند، یعنی $\text{tr}(\frac{e^{\alpha_1},e^{\alpha_2},\ldots,e^{\alpha_n}}{\mathbb{Q}}) = n$.

اثبات. به مراجع مربوط در این زمینه مراجعه نمایید. □

قضیه بالا به این صورت نیز بیان می‌شود: فرض کنید $\alpha_1,\alpha_2,\ldots,\alpha_n$ عناصر جبری متفاوت روی $\mathbb{Q}$ باشند. در این صورت $e^{\alpha_1},e^{\alpha_2},\ldots,e^{\alpha_n}$ روی $\mathbb{Q}$ مستقل خطی هستند.

نتیجه ۱۲۸. عدد e روی $\mathbb{Q}$ متعالی است یعنی $\text{tr}(\frac{e}{\mathbb{Q}}) = 1$، یعنی $e \notin (\mathbb{Q})^{\text{alg}}$.

اثبات. فرض کنید e روی $\mathbb{Q}$ جبری باشد، یعنی فرض کنید $a_0 + a_1e + a_2e^2 + \ldots + a_n^n$ و بنا به قضیه قبل، این غیرممکن است. □

نتیجه ۱۲۹. عدد π روی $\mathbb{Q}$ متعالی است.

اثبات. اگر π روی $\mathbb{Q}$ جبری باشد، آنگاه πi نیز روی $\mathbb{Q}$ نیز جبری است. بنابراین فرض کنید $\alpha_1 = \pi i$ و $\alpha_2 = 0$. در این صورت $e^{\pi i}$ و e^0 باید روی $\mathbb{Q}$ مستقل خطی باشند، اما $\{-1,1\}$ روی $\mathbb{Q}$ مستقل خطی نیستند. □

حدس شانوئل: اگر $\alpha_1, \ldots, \alpha_n$ روی $\mathbb{Q}$ مستقل خطی باشند، آنگاه $\mathrm{tr}(\frac{\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_n}}{\mathbb{Q}}) \geq n$.

نتیجه ۱۳۰. اگر حدس شانوئل برقرار باشد، آنگاه e, π مستقل جبری هستند. کافیست قرار دهید $\alpha_1 = \pi i$ و $\alpha_2 = 1$. پس $\mathrm{tr}(\frac{1, \pi i, e, -1}{\mathbb{Q}}) \geq 2$. چون $\{1, -1\}$ جبری هستند پس $\{e, \pi i\}$ مستقل جبری هستند. چون i جبری است نتیجه می‌گیریم $\{e, \pi\}$ مستقل جبری هستند.

مسائل ترسیم توسط خطکش و پرگار

آیا می‌توان با استفاده از خطکش و پرگار، مربعی رسم کرد که مساحت آن برابر مساحت دایره‌ای به شعاع r باشد. خطکش مورد نظر در اینجا خطکشی است که درجه‌بندی ندارد و فقط می‌توان با آن روی دو نقطه داده شده خطی رسم کرد، اما طول واحد را داریم.

مثال ۱۳۱. فرض کنید نقاط A و B ساخته شده باشند. می‌توان عمودمنصف خطِ بین دو نقطه داده شده را با استفاده از خطکش و پرگار رسم کرد.

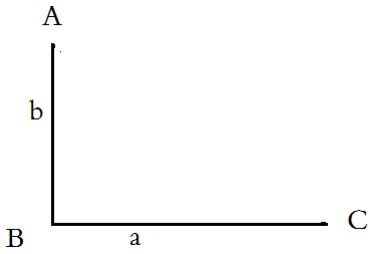
مثال ۱۳۲. اگر طول r قابل رسم باشد، آنگاه طول‌های $2r$، $3r$ و ... قابل ایجاد است.

مثال ۱۳۳. فرض کنید نقاط A، B و C در سیستم باشند و نقطه‌ی C روی پاره‌خط AB واقع نباشد. با استفاده از خطکش خطی از C عمود بر AB رسم کنید.
ابتدا دایره‌ای به مرکز C رسم می‌کنیم که خط AB را در نقاط M و N قطع کند. حال عمودمنصف خط MN را رسم می‌کنیم و نقطه O وسط خط MN را به نقطه C وصل می‌کنیم. دو مثلث COM و CON هم‌نهشت هستند. پس خط CO بر خط AB عمود است.

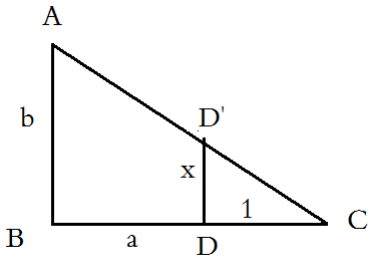
مثال ۱۳۴. فرض کنید نقطه C روی خط AB واقع باشد. از نقطه C می‌توان خطی عمود بر AB رسم کرد.
اگر نقاط C و A روی هم قرار نگرفته باشد، آنگاه به مرکز C و شعاع CA دایره‌ای رسم می‌کنیم. فرض کنید دایره، خط AB را در نقطه‌ی A' قطع کند. عمودمنصف خط AA' از نقطه‌ی C می‌گذرد. حال فرض کنید نقاط A و C روی هم قرار گرفته باشند. دایره‌ای به مرکز A و شعاع AB رسم می‌کنیم. فرض کنید دایره خط AB را در نقطه‌ای به نام D قطع کند. عمودمنصف خط DB از نقطه C می‌گذرد.

مثال ۱۳۵. فرض کنید طول‌های a و b ایجاد شده باشند. نشان دهید که طول‌های $a+b$، $a-b$، ab و $\frac{b}{a}$ نیز قابل ایجاد هستند.

برای ایجاد طول $\frac{b}{a}$، ابتدا توجه کنید که می‌توان طول b را بر طول a عمود ایجاد کرد.



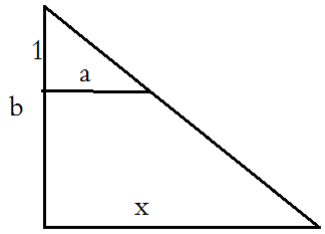
نقاط A و C را بهم وصل می‌کنیم تا مثلثی ایجاد شود. سپس روی طول a با شروع از نقطه‌ی C به اندازه واحد مشخص می‌کنیم. فرض کنید طول CD به اندازه واحد باشد که نقطه‌ی D روی طول a است. از نقطه‌ی D عمودی بر طول a رسم می‌کنیم و فرض کنید این عمود خط AC را در D' قطع کند، فرض کنید طول خط DD' برابر x باشد.



بنا بر تشابه مثلث‌ها داریم:

$$\frac{1}{a}=\frac{x}{b} \;\Rightarrow\; x=\frac{b}{a}$$

برای رسم $x=ab$، مشابه حالت قبل باید مثلثی به صورت زیر ایجاد کنیم.

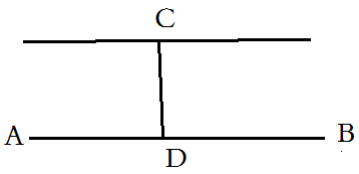


بنا بر تشابه مثلث‌ها داریم:

$$\frac{1}{b} = \frac{a}{x} \Rightarrow x = ab$$

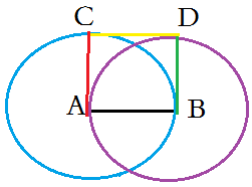
مثال ۱۳۶. فرض کنید در سیستم خط AB و نقطه‌ی C را داریم. از نقطه‌ی C خطی موازی AB رسم کنید.

ابتدا از نقطه‌ی C خط CD را عمود بر AB رسم می‌کنیم. حال از نقطه‌ی C خطی عمود بر CD رسم می‌کنیم و این خط عمود، با خط AB موازی است.



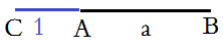
مثال ۱۳۷. یک مربع روی پاره‌خط AB داده شده، رسم کنید.

به مرکز A و شعاع به اندازه AB دایره‌ای رسم می‌کنیم. سپس به مرکز B و شعاع به اندازه AB دایره‌ی دیگری رسم می‌کنیم. از نقطه‌ی A عمودی بر خط AB رسم می‌کنیم که دایره‌ی اول را در نقطه‌ای به نام C قطع کند. به طور مشابه، از نقطه‌ی B عمودی بر خط AB رسم می‌کنیم که دایره‌ی دوم را در نقطه‌ای به نام D قطع کند. چهار ضلعی $ABCD$ یک مربع است.



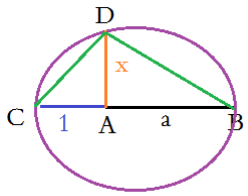
مثال ۱۳۸. فرض کنید طول a را داریم، طول $\sqrt{a}$ را ایجاد کنید.

فرض کنید طول پاره‌خط AB برابر a باشد. از نقطه‌ی A و در امتداد پاره خط AB به اندازه واحد ایجاد کنید.

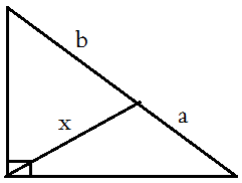


حال وسط پاره‌خط CB را پیدا کنید و آن‌را O بنامید. دایره‌ای به مرکز O و شعاع OB رسم کنید. سپس از نقطه‌ی A عمودی بر خط AB رسم کنید. محل تقاطع دایره و خط عمود را D را بنامید.

نقطه‌ی D را به C و B وصل کنید. زاویه‌ی D یک زاویه قائمه است، بنابراین می‌توان ثابت کرد که $x = \sqrt{a \times 1}$.



تمرین ۲۰. فرض کنید یک مثلث قایم‌الزاویه به صورت زیر داریم. نشان دهید که $x = \sqrt{a \times b}$.



تمرین ۲۱. فرض کنید یک مستطیل با اضلاع a و b داریم. با استفاده از مثال قبل، یک مربع بسازید که مساحت آن با مساحت مستطیل داده شده برابر باشد.

۲۳ جلسه بیست و پنجم: برخی مسائل کلاسیک ترسیم توسط خط‌کش و پرگار

تعریف ۱۳۹. فرض کنید $F \subseteq \mathbb{R}$ یک میدان باشد. در این صورت $\{(a,b) \mid a,b \in F\}$ را صفحه‌ی F^2 می‌نامیم. فرض کنید $P = (a_1, b_1), Q = (a_2, b_2) \in F^2$. در این صورت خط گذرنده میان P و Q دارای معادله‌ای به صورت $y = mx + b$ است. به طور مشابه معادله‌ی دایره‌ای به مرکز (a_1, b_1) و به شعاع فاصله‌ی میان آن دو به صورت زیر است:

$$(x - a_1)^2 + (y - b_1)^2 = (a_2 - a_1)^2 + (b_2 - b_1)^2$$

مشاهده:

- فرض کنید L_1 و L_2 دو خط متقاطع در F^2 باشند. آیا نقطه تقاطع این دو خط نیز در F^2 است؟ بله، $L_1 \cap L_2 = \emptyset$ یا $L_1 \cap L_2 \in F^2$.

- فرض کنید c_1 و c_2 دو دایره در F^2 باشند. آیا نقاط تقاطع این دو دایره در F^2 هستند؟ فرض کنید

$$c_1 : x^2 + y^2 + ax + by + c = 0$$
$$c_2 : x^2 + y^2 + a'x + b'y + c' = 0$$

برای پیدا کردن محل تقاطع به یک معادله‌ی درجه‌ی ۲ بر حسب x به صورت $x^2+bx+c = 0$ می رسیم. می‌دانیم که جواب‌های معادله به صورت $\frac{-b \pm \sqrt{\Delta}}{2a}$ است. اگر $\sqrt{\Delta} \in F$، آنگاه $x \in F$. اگر $\sqrt{\Delta} \notin F$، آنگاه $x \in F(\sqrt{\Delta})$ و $y \in F(\sqrt{\Delta})$. به بیان دیگر، فرض کنید C, D محل تقاطع دو دایره باشد. در این صورت $F \subseteq F(C)$ و $[F(C) : F] = 2$. به طور خلاصه، محل تقاطع دو دایره در میدان $F(\sqrt{\Delta})$ قرار میگیرد که $[F(\sqrt{\Delta}) : F] = 2$.

- فرض کنید C یک دایره و L یک خط در F^2 باشند. در این صورت $C \cap L = \emptyset$ یا $C \cap L = \{P\} \in F^2$ یا $C \cap L = \{P, Q\}$ که یا $P, Q \in F$ یا $P, Q \in F(\sqrt{\Delta})$ و $[F(\sqrt{\Delta}) : F] = 2$.

- معادله‌ی $x^2 + ax + b$ را در نظر بگیرید که $a, b \in F$. این معادله یا دو ریشه در F دارد یا یک ریشه در F دارد یا دو ریشه در $F(\sqrt{\Delta})$ دارد به طوری که $[F(\sqrt{\Delta}) : F] = 2$. دقت کنید که اگر این معادله یک ریشه در F داشته باشد، آنگاه ریشه‌ی دیگر آن نیز در F است.

تعریف ۱۴۰. عدد حقیقی $c \in \mathbb{R}$ را ساخته‌شدنی می‌نامیم هرگاه $(c, 0)$ قابل ایجاد توسط خطکش و پرگار باشد (اگر و تنها اگر $(0, c)$ قابل ایجاد توسط خطکش و پرگار باشد).
نقطه‌ی $(c, d) \in F^2$ را ساخته‌شدنی می‌نامیم هرگاه $(c, 0)$ و $(0, d)$ قابل ایجاد توسط خطکش و پرگار باشد (اگر و تنها اگر (d, c) قابل ایجاد توسط خطکش و پرگار باشد).

مشاهده:

- تمام نقاط $a \in \mathbb{Q}$ قابل ایجاد هستند.

- اگر $a, b \in \mathbb{R}$ قابل ایجاد باشند، آنگاه $a + b$، $a - b$ و $\frac{a}{b}$ نیز قابل ایجاد هستند. بنابراین نقاط ساخته شدنی تشکیل یک زیرمیدان از $\mathbb{R}$ می‌دهند.

قضیه ۱۴۱. فرض کنید $c \in \mathbb{R}$ ساخته‌شدنی باشد. در این صورت $n \in \mathbb{N}$ وجود دارد که : $[\mathbb{Q}(c) : \mathbb{Q}] = 2^n$

اثبات. اگر c ساخته‌شدنی باشد با تعداد متناهی مرتبه به کار بردن خطکش و پرگار ایجاد می‌شود. در هر مرحله اشتراک خطوط و دوایر با هم محاسبه می‌شود. بنابراین می‌توانیم فرض کنید که $c \in \mathbb{Q}[\sqrt{\Delta_1}, \ldots, \sqrt{\Delta_n}]$. پس

$$\mathbb{Q} \subseteq \mathbb{Q}(c) \subseteq \mathbb{Q}[\sqrt{\Delta_1}, \ldots, \sqrt{\Delta_n}]$$

در نتیجه $[\mathbb{Q}(c) : \mathbb{Q}] = 2^n$. □

قضایای کلاسیک

قضیه ۱۴۲. با استفاده از خطکش و پرگار نمی‌توان یک زاویه‌ی 60 را سه قسمت مساوی تقسیم کرد.

اثبات. اگر زاویه‌ی $20°$ قابل ایجاد باشد، آنگاه $\cos(20°)$ قابل ایجاد است. یعنی $c = \cos(20)$ توسط خطکش و پرگار ایجاد شده است. پس $[\mathbb{Q}(c) : \mathbb{Q}] = 2^n$. توجه کنید که

$$\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha)$$

پس اگر $\alpha = 20°$، آنگاه $\frac{1}{2} = 4x^3 - 3x$ که $x = \cos(20)$. یعنی $8x^3 - 6x - 1 = 0$. ادعا می‌کنیم که چندجمله‌ای $g(x) = 8x^3 - 6x - 1 = 0$ روی $\mathbb{Q}$ تحویل‌ناپذیر است. مشاهده کنید که اگر چندجمله‌ای فوق در $\mathbb{Q}[x]$ قابل تجزیه باشد، دارای ریشه در $\mathbb{Q}$ است. همچنین می‌دانیم که اگر چندجمله‌ای مانند $a_0 + a_1x + \ldots + a_nx^n$ با ضرایب در $\mathbb{Z}$ دارای ریشه‌ی گویایی مانند $\frac{c}{d}$ باشد که $(c, d) = 1$، آنگاه $c|a_0$ و $d|a_n$. بنابراین اگر چندجمله‌ای g در $\mathbb{Q}$ ریشه‌ای مانند $\frac{c}{d}$ داشته باشد، آنگاه $c| - 1$ و $d|8$. بنابراین $c = 1$ یا $c = -1$ و $d = 1$ یا $d = 2$ یا $d = 4$. بررسی می‌شود که برای این مقادیر، $\frac{c}{d}$ ریشه‌ی g نیست. □

قضیه ۱۴۳. فرض کنید یک مکعب با طول ضلع 1 داده شده است. نشان دهید که نمی‌توان مکعبی ایجاد کرد که حجم آن دو برابر حجم مکعب داده شده باشد.

اثبات. اگر بتوانیم مکعبی با حجم 2 ایجاد کنیم، آنگاه چندجمله‌ای $x^3 - 2$ باید در $\mathbb{Q}$ ریشه داشته باشد. اما $x^3 - 2$ روی $\mathbb{Q}$ تحویل‌ناپذیر است. □

قضیه ۱۴۴. فرض کنید دایره‌ای به شعاع 1 داده شده است. نشان دهید که نمی‌توان مربعی هم‌مساحت با آن رسم کرد.

اثبات. اگر بتوان مربعی به طول ضلع $\sqrt{\pi}$ ایجاد کرد، آنگاه باید معادله‌ی $x - \sqrt{\pi} = 0$ در $\mathbb{Q}$ ریشه داشته باشد. اما $\sqrt{\pi}$ روی $\mathbb{Q}$ جبری نیست زیرا π جبری نیست. □

۲۴ جلسه‌ی بیست و ششم: تحویل‌ناپذیری روی اعداد گویا، لم گاوس و محک آیزن‌اشتاین

یادآوری:

- چندجمله‌ای $f \in K[x]$ را تحویل‌ناپذیر می‌نامیم هرگاه نتوان f را به صورت $f = gh$ تجزیه کرد که $g, h \in K[x]$ و درجه‌های g و h بزرگتر مساوی 1 باشند.
- تحویل‌ناپذیری به میدان مورد نظر بستگی دارد. برای مثال چندجمله‌ای $x^2 + 1$ در $\mathbb{Q}[x]$ و $\mathbb{R}[x]$ تحویل‌ناپذیر است اما در $\mathbb{C}[x]$ تحویل‌پذیر است. برای مثال چندجمله‌ای $x^2 - 2$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است اما در $\mathbb{R}[x]$ به صورت $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ تحویل‌پذیر می‌شود.
- اگر $f \in \mathbb{Q}[x]$ تحویل‌ناپذیر باشد، آنگاه $f \in \mathbb{C}[x]$ به طور کامل تجزیه می‌شود. دقت شود که f در $\mathbb{C}[x]$ به عوامل درجه‌ی اول تجزیه می‌شود، یعنی ریشه‌ی تکراری در $\mathbb{C}$ نباید داشته باشد.
- در $\mathbb{C}[x]$ تمامی چندجمله‌ای‌ها به عوامل اول تجزیه می‌شود، یعنی در $\mathbb{C}[x]$ تنها چندجمله‌ای‌های تحویل‌ناپذیر، چندجمله‌ای‌های درجه‌ی اول هستند.
- در $\mathbb{R}[x]$ چندجمله‌ای‌ها به عوامل درجه‌ی اول و درجه‌ی دوم تجزیه می‌شود، یعنی تنها چندجمله‌ای‌های تحویل‌ناپذیر به صورت $x + a$ و $ax^2 + bx + c$ که $\Delta < 0$، هستند.
- دقت کنید که ریشه نداشتن به معنی تحویل‌ناپذیری نیست. برای مثال چندجمله‌ای $f(x) = (x^2 + 1)(x^2 + 1) \in \mathbb{Q}[x]$ در $\mathbb{Q}$ هیچ ریشه‌ای ندارد اما تحویل‌پذیر است.

تحویل‌ناپذیری در $\mathbb{Q}[x]$

حال می‌خواهیم تحویل‌ناپذیری چندجمله‌های به صورت $f(x) = x^2 + ax + b$ را در $\mathbb{Q}[x]$ بررسی کنیم. توجه کنید که f در $\mathbb{Q}[x]$ تحویل‌پذیر است اگر و تنها اگر f در $\mathbb{Q}$ دارای ریشه باشد. بنابراین برای چندجمله‌ای $f(x) = x^2 + ax + b \in \mathbb{Q}[x]$، اگر $\Delta < 0$، آنگاه f در $\mathbb{R}[x]$ تحویل‌ناپذیر است. اگر $\Delta > 0$، آنگاه f در $\mathbb{R}[x]$ به صورت $f(x) = (x - \alpha_1)(x - \beta_2)$ تحویل‌پذیر است. در این حالت، چندجمله‌ای f در $\mathbb{Q}[x]$ تحویل‌ناپذیر است اگر و تنها اگر $\beta_1, \beta_2 \notin \mathbb{Q}$.

مثال ۱۴۵. چندجمله‌ای $x^2 - 2 \in \mathbb{Q}[x]$ را در نظر بگیرید. ریشه‌های این چندجمله‌ای $\sqrt{2}$ و $-\sqrt{2}$ است که در $\mathbb{Q}$ نیستند، پس این چندجمله‌ای در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. اما در $\mathbb{R}[x]$ تحویل‌پذیر است.

چندجمله‌ای $x^2 + x + 1 \in \mathbb{Q}[x]$ ریشه‌ای در $\mathbb{R}$ ندارد. پس در $\mathbb{R}[x]$ و $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

با توجه به این که 1 و 2 ریشه‌های چندجمله‌ای $x^2 + x - 2 \in \mathbb{Q}[x]$ هستند و این ریشه‌ها در $\mathbb{Q}$ قرار دارند، پس این چندجمله‌ای در $\mathbb{Q}[x]$ تحویل‌پذیر است.

لم ۱۴۶ (لم گاوس)**.** فرض کنید $f \in \mathbb{Z}[x]$ یک چندجمله‌ای باشد. در این صورت اگر f در $\mathbb{Q}[x]$ تحویل‌پذیر باشد، آنگاه در $\mathbb{Z}[x]$ نیز تحویل‌پذیر است، به بیان دیگر $f \in \mathbb{Z}[x]$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است اگر و تنها اگر در $\mathbb{Z}[x]$ تحویل‌ناپذیر باشد.

اثبات. فرض کنید f در $\mathbb{Q}[x]$ به صورت $f = f_1 f_2$ تحویل‌پذیر باشد. عدد صحیح n پیدا می‌شود که $nf = gh$ و در این صورت $nf, g, h \in \mathbb{Z}[x]$. فرض کنید

$$g = a_0 + a_1 x + \ldots + a_n x^n$$
$$h = b_0 + b_1 x + \ldots + b_m x^m$$

ادعا: فرض کنید $p|n$، در این صورت یا p تمامی ضرایب g را عاد می‌کند یا p تمامی ضرایب h را عاد می‌کند. فرض کنید این‌گونه نباشد. یعنی اگر $p|n$، آنگاه حداقل یک ضریب در g و یک ضریب در h توسط p عاد نشود. فرض کنید a_i اولین ضریب در g باشد که $p \nmid a_i$ و b_j اولین ضریب در h باشد که $p \nmid b_j$. در این صورت ضریب x^{i+j} در nf توسط p عاد می‌شود. برای مثال فرض کنید a_3 اولین ضریب در g باشد که $p \nmid a_3$ و b_2 اولین ضریب در h باشد که $p \nmid b_2$. یعنی $p|a_0$، $p|a_1$،

$p|a_2$ و $p \nmid a_3$. همچنین $p|b_0$، $p|b_1$ و $p \nmid b_2$. در این صورت می‌دانیم که p ضریب x^5 در nf را عاد می‌کند. ضریب x^5 در nf برابر است با

$$a_0b_5 + a_1b_4 + a_2b_3 + a_3b_2 + a_4b_1 + a_5b_0$$

چون $p|a_0$، $p|a_1$ و $p|a_2$ پس $p|a_0b_5 + a_1b_4 + a_2b_3$. همچنین چون $p|b_0$ و $p|b_1$ پس $p|a_4b_1 + a_5b_0$. بنابراین باید $p|a_3b_2$. اما چون p عددی اول است پس یا باید $p|a_3$ یا $p|b_2$ و این امکان‌پذیر نیست. بنابر این ادعا و اینکه می‌توان n را به عوامل اول تجزیه کرد نتیجه میگیریم که f در $\mathbb{Z}[x]$ تجزیه می‌شود. □

مثال ۱۴۷. آیا چندجمله‌ای $x^3 + 2x^2 + 4x + 1$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است؟ تحویل‌ناپذیری این چندجمله‌ای را در $\mathbb{Z}[x]$ بررسی می‌کنیم. اگر این چندجمله‌ای در $\mathbb{Z}[x]$ تحویل‌پذیر باشد باید به صورت زیر تجزیه شود

$$x^3 + 2x^2 + 4x + 1 = (x + a)(x^2 + bx + c)$$

که $a, b, c \in \mathbb{Z}$. پس باید $ac = 1$، بنابراین $a = 1$ یا $a = -1$. اگر 1 و -1 هیچ‌کدام ریشه‌ی f نباشند، آنگاه f در $\mathbb{Z}[x]$ تحویل‌ناپذیر است، در نتیجه در $\mathbb{Q}[x]$ نیز تحویل‌ناپذیر است.

مثال ۱۴۸. آیا چندجمله‌ای $x^3 + 2x^2 + 4x + 6$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است؟ تحویل‌ناپذیری این چندجمله‌ای را در $\mathbb{Z}[x]$ بررسی می‌کنیم. اگر این چندجمله‌ای در $\mathbb{Z}[x]$ تحویل‌پذیر باشد باید به صورت زیر تجزیه شود

$$x^3 + 2x^2 + 4x + 1 = (x + a)(x^2 + bx + c)$$

که $a, b, c \in \mathbb{Z}$. پس باید $ac = 6$، یعنی $a = \pm 2$ یا $a = \pm 3$. بنابراین کافیست بررسی کنیم آیا این اعداد ریشه‌ی f هستند یا نه. اگر هیچ‌کدام ریشه‌ی چندجمله‌ای f نباشند، آنگاه f تحویل‌ناپذیر است.

یادآوری: فرض کنید $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in \mathbb{Z}[x]$. اگر $\frac{a}{b}$ ریشه‌ی f در $\mathbb{Q}$ باشد، آنگاه $a|a_0$ و $b|a_n$.

در مثال قبل، اگر f در $\mathbb{Q}[x]$ تجزیه شود، آنگاه دارای ریشه در $\mathbb{Q}$ است. اگر $\frac{a}{b}$ ریشه‌ی f باشد، آنگاه $a|6$ و $b|1$. پس $a = \pm 2$ یا $a = \pm 3$ باید ریشه‌ی f باشد.

قضیه ۱۴۹ (محک آیزنشتاین). فرض کنید $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in \mathbb{Z}[x]$. فرض کنید عدد اول p وجود داشته باشد به طوری که $p|a_0, p|a_1, \ldots, p|a_{n-1}$ اما $p \nmid a_n$ و $p^2 \nmid a_0$. در این صورت f در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

اثبات. توجه کنید که بنا به لم گاوس، تحویل‌ناپذیری در $\mathbb{Q}[x]$ و $\mathbb{Z}[x]$ با هم معادل‌اند. به برهان خلف فرض کنید چندجمله‌ای مورد نظر در $\mathbb{Z}[x]$ به صورت زیر تجزیه شود.

$$a_0+a_1x+a_2x^2+\ldots+a_nx^n = (b_0+b_1x+\ldots+b_rx^r)(c_0+c_1x+c_2x^2+\ldots+csx^s)$$

با توجه به اینکه $a_0 = b_0c_0$ و $p|a_0$، پس $p|b_0$ یا $p|c_0$ و چون $p^2 \nmid a_0$ پس فقط یکی از این‌ها می‌تواند برقرار باشد. بنابراین، فرض کنید $p|b_0$ و $p \nmid c_0$. با توجه به اینکه $p|a_1 = c_0b_1 + c_1b_0$ و $p \nmid c_0$، پس $p|b_1$. دوباره با توجه به اینکه $p|a_2 = c_0b_2 + c_1b_1 + c_2b_0$ پس $p|b_2$. بنابراین به این ترتیب $p|b_r$، یعنی p همه‌ی b_iها را عاد می‌کند. با توجه با اینکه در ضریب x^n تمامی b_iها استفاده شده‌اند، پس $p|a_n$ و این تناقض است. □

نتیجه ۱۵۰. چندجمله‌ای‌های تحویل‌ناپذیر با درجه به اندازه کافی بزرگ وجود دارند.

مثال ۱۵۱. چندجمله‌ای $x^3 - 2 \in \mathbb{Z}[x]$ را در نظر بگیرید. چون $2| - 2$، $2^2 \nmid -2$ و $2 \nmid 1$ پس این چندجمله‌ای تحویل‌ناپذیر است. همچنین چندجمله‌ای $3 + 6x + 9x^2 + 10x^3$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

مثال ۱۵۲. چندجمله‌ای $3x^3 + 6x^2 + 9x + 10$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. فرض کنید این چندجمله‌ای به صورت زیر تحویل‌پذیر شود:

$$3x^3 + 6x^2 + 9x + 10 = fg$$

که f از درجه‌ی 1 و g از درجه‌ی 2 باشد. پس در میدان کسرها می‌توان نوشت:

$$x^3(3 + 6\frac{1}{x} + 9\frac{1}{x^2} + 10\frac{1}{x^3}) = xf' + x^2g'$$

قرار دهید $y = \frac{1}{x}$، پس $3 + 6y + 9y^2 + 10y^3 = f'g'$. اما بنا به محک آیزنشتاین، چندجمله‌ای $3 + 6y + 9y^2 + 10y^3$ تحویل‌ناپذیر است.

مثال ۱۵۳. چندجمله‌ای‌هایی به صورت $1+x+x^2+\ldots+x^{p-1}\in\mathbb{Q}[x]$ که $p>2$ و عددی اول است. توجه کنید که

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

فرض کنید که $1+x+x^2+\ldots+x^{p-1}=fg$. پس $x^p-1=(x-1)fg$. بنابراین

$$(X+1)^p-1=Xf(X+1)g(X+1)$$

توجه کنید که

$$(X+1)^p-1=\binom{p}{1}X+\binom{p}{2}X^2+\binom{p}{3}X^3+\cdots+\binom{p}{p-1}X^{p-1}+X^p$$

اما بنا به محک آیزنشتاین، چون $p\mid\binom{p}{1},p\mid\binom{p}{2},\ldots,p\mid\binom{p}{p-1}$ و $p\nmid 1$، چندجمله‌ای $(X+1)^p-1$ تحویل‌ناپذیر است.

هومومرفیسم $\varphi:\mathbb{Z}\to\mathbb{Z}_p$ وجود دارد که $\varphi(a)=\overline{a}=a+\langle p\rangle$. فرض کنید

$$f(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n\in\mathbb{Z}[x]$$

و p یک عدد اول باشد که $p\nmid a_n$. بنابراین $\overline{f}=\overline{a_0}+\overline{a_1}x+\overline{a_2}x^2+\ldots+\overline{a_n}x^n\in\mathbb{Z}_p[x]$. حال اگر $f=gh$، آنگاه $\overline{f}=\overline{g}\,\overline{h}$.

قضیه ۱۵۴. فرض کنید $f(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n\in\mathbb{Z}[x]$ و p عددی اول باشد که $p\nmid a_n$. اگر این چندجمله‌ای در $\mathbb{Z}[x]$ تحویل‌پذیر باشد، آنگاه $\overline{f}$ در $\mathbb{Z}_p[x]$ تحویل‌پذیر است.

مثال ۱۵۵. چندجمله‌ای $f(x)=x^3+2x^2+x+1$ را در نظر بگیرید و دقت کنید که $2\nmid 1$. اگر $f=gh$، آنگاه $\overline{f}\in\mathbb{Z}_2[x]$ تحویل‌پذیر می‌شود. اما $\overline{f}=x^3+x+1$ و اگر $\overline{f}$ در $\mathbb{Z}_2[x]$ تحویل‌پذیر شود باید به صورت زیر تجزیه شود:

$$\overline{f}=(x+a)(x^2+ax+b)$$

که $ab=1$ و $a^2+b=1$. اما $\mathbb{Z}_2=\{0,1\}$ و از اینکه $ab=1$ نتیجه می‌گیریم که $a=b=1$. این مقادیر در شرط $a^2+b=1$ صدق نمی‌کنند.

۲۵ جلسه‌ی بیست و هفتم: میدان‌های متناهی

یادآوری: فرض کنید F یک میدان باشد. اگر $n \in \mathbb{N}$ وجود داشته باشد که $\underbrace{1_F + \ldots + 1_F}_{n \text{ بار}} = 0_F$، آنگاه می‌گوییم مشخصه میدان F برابر n است و می‌نویسیم $\mathrm{Char}(F) = n$. می‌توان نوشت:

$$\begin{aligned}\mathrm{Char}(F) = n &\Leftrightarrow \underbrace{1_F + \ldots + 1_F}_{n \text{ بار}} = 0_F \\ &\Leftrightarrow \exists x \neq 0 \in F (\underbrace{x + \ldots + x}_{n \text{ بار}} = 0_F) \\ &\Leftrightarrow \forall x \neq 0 \in F (\underbrace{x + \ldots + x}_{n \text{ بار}} = 0_F)\end{aligned}$$

اگر n مشخصه یک میدان باشد، آنگاه n عددی اول است. اگر هیچ nای وجود نداشته باشد که $\underbrace{1_F + \ldots + 1_F}_{n \text{ بار}} = 0_F$، آنگاه می‌گوییم مشخصه میدان، صفر است. میدان‌های با مشخصه‌ی p همیشه شامل $\mathbb{Z}_p$ و میدان‌های با مشخصه‌ی صفر همیشه شامل $\mathbb{Q}$ هستند.

فرض کنید F یک میدان متناهی باشد. در این صورت گروه جمعی عناصر F متناهی است و $\underbrace{1_F + \ldots + 1_F}_{\text{به اندازه‌ی میدان}} = 0_F$. پس یک میدان متناهی حتما دارای یک مشخصه‌ی متناهی p است.

مشاهده:

- اگر F یک میدان متناهی باشد، آنگاه عدد اول p موجود است به طوری که $\mathbb{Z}_p \subseteq F$.
- عدد $n \in \mathbb{N}$ وجود دارد که $[F : \mathbb{Z}_p] = n$. بنابراین اگر F یک میدان متناهی باشد، آنگاه $|F| = p^n$.
- اگر F دارای مشخصه‌ی p باشد، نگاشت $\sigma : F \to F$ که $\sigma(x) = x^p$ یک هومومرفیسم است (با توجه به اینکه $p | \binom{p}{i}$، به سادگی بررسی می‌شود که $(x+y)^p = x^p + y^p$).
- نگاشت $\sigma : F \to F$ که $\sigma(x) = x^p$ روی $\mathbb{Z}_p$ همانی است. پس برای هر $a \in \mathbb{Z}_p$ داریم $a^p = a$ (قضیه کوچک فرما).

قضیه ۱۵۶ (قضیه کوچک فرما). اگر a یک عدد طبیعی باشد، آنگاه $a^p \equiv_p a$.

اثبات. عناصر $1a, 2a, \dots, (p-1)a$ را در هم ضرب کنید. در این صورت

$$1a \times 2a \times \cdots \times (p-1)a \equiv_p 1 \times 2 \times \cdots \times (p-1)$$

پس $a^p \equiv_p a$ در نتیجه $a^{p-1} \equiv_p 1$، بنابراین $(p-1)!a^{p-1} \equiv_p (p-1)!$. □

ساختن یک میدان متناهی:

میدان $\mathbb{Z}_p$ را در نظر بگیرید و فرض کنید n یک عدد طبیعی دلخواه باشد. چندجمله‌ای $f(x) = x^{p^n} - x \in \mathbb{Z}_p$ را در نظر بگیرید. فرض کنید $\mathbb{Z}_p \subseteq F$ میدان شکافنده‌ی f باشد. چندجمله‌ای f در میدان شکافنده‌ی F دارای ریشه‌ی تکراری نیست. اگر f دارای ریشه تکراری باشد، آنگاه $f = (x-\alpha)^2 g$. پس $f' = 2(x-\alpha)g + g'(x-\alpha)^2$ و $f'(\alpha) = 0$. اما $f' = p^n x^{p^n-1} - 1 \neq 0$.

مشاهده: اگر $f \in K[x]$ یک چندجمله‌ای دلخواه باشد و $(f, f') = 1$، آنگاه f دارای ریشه‌ی تکراری نیست (جدایی‌پذیر است).

اثبات. اگر f دارای ریشه‌ی تکراری باشد، آنگاه f و f' در میدان شکافنده‌ی $L[x]$ دارای یک مقسوم‌علیه مشترک غیر بدیهی هستند. پس f و f' در $K[x]$ نیز ب.م.م غیر بدیهی دارند. چون اگر در میدان K داشته باشیم: $(f, f') = 1$ یعنی $mf + nf' = 1$، آنگاه در میدان L نیز $(f, f') = 1$. □

خلاصه، چندجمله‌ای $x^{p^n} - x$ در میدان شکافنده‌ی $\mathbb{Z}_p \subseteq F$ دارای p^n ریشه‌ی متمایز است.

مشاهده: مجموعه‌ی ریشه‌های چندجمله‌ای $f = x^{p^n} - x$ تشکیل یک میدان می‌دهند. پس میدان $\mathbb{Z}_p \subseteq F$ در واقع تنها متشکل از ریشه‌های $x^{p^n} - x = 0$ است، یعنی $|F| = p^n$.

خلاصه، اگر p یک عدد اول باشد و n یک عدد دلخواه باشد، آنگاه یک میدان متناهی با اندازه‌ی p^n موجود است.

از طرفی فرض کنید F یک میدان متناهی باشد. نشان داده‌ایم $|F| = p^n$. گروه ضربی $F^* = F - \{0\}$ دارای $p^n - 1$ عنصر است. بنابراین برای هر $0 \neq a \in F$ داریم: $a^{p^n-1} = 1$ یعنی $a^{p^n} = a$. پس تمامی عناصر میدان F در معادله‌ی $x^{p^n} = x$ صدق می‌کنند. یعنی ریشه‌های متفاوت این معادله هستند. بنابراین F میدان شکافنده‌ی $x^{p^n} - x$ روی $\mathbb{Z}_p$ است.

نتیجه ۱۵۷. هر میدان متناهی دارای اندازه‌ای به صورت p^n است. چنین میدانی در واقع میدان شکافنده‌ی چندجمله‌ای $x^{p^n} - x$ روی $\mathbb{Z}_p$ است. پس برای هر p و n تنها یک میدان متناهی (بسته به ایزومرفیسم) با اندازه p^n وجود دارد.

در ادامه‌ی بحث، قصد داریم قضیه‌ی زیر را ثابت کنیم.

قضیه ۱۵۸. اگر F یک میدان متناهی باشد، آنگاه F^* یعنی گروه ضربیِ F یک گروه دوری است.

تعریف ۱۵۹ (توان گروه). می‌گوییم توان گروه G برابر است با e هرگاه e کوچکترین عدد طبیعی باشد که برای هر $a \in G$ داشته باشیم: $a^e = 1$.

مشاهده:

- اگر G یک گروه متناهی باشد، آنگاه توان G برابر است با ک.م.م همه‌ی مرتبه‌ها.
- فرض کنید G یک گروه آبلی متناهی باشد. در این صورت مرتبه‌ی هر عنصرِ G متناهی است.

لم ۱۶۰. اگر e توان گروه G باشد، آنگاه عنصر $a \in G$ موجود است به طوری که $\text{ord}(a) = e$.

اثبات. فرض کنید $e = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ ک.م.م همه‌ی مرتبه‌ها باشد. در این صورت عنصری به نام a_1 موجود است به طوری که $P_1^{\alpha_1} | \text{ord}(a_1)$ یعنی $\text{ord}(a_1) = p_1^{\alpha_1} q_1$. پس $(a_1^{q_1})^{p_1^{\alpha_1}} = 1$، بنابراین $\text{ord}(g_1 = a_1^{q_1}) = p_1^{\alpha_1}$. بنابراین عناصر $g_1, \ldots, g_k$ موجودند به طوری که $\text{ord}(g_i) = p_i^{\alpha_i}$. قرار دهید $a = g_1 \cdots g_k$. نشان می‌دهیم:

$$\text{ord}(a) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

توجه کنید که $(g_1 \cdots g_k)^{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} = 1$. فرض کنید که $(g_1 \cdots g_k)^n = 1$. ادعا می‌کنیم که $p_1^{\alpha_1} \cdots p_k^{\alpha_k} | n$. کافیست نشان دهیم برای هر $1 \le i \le k$، $p_i^{\alpha_i} | n$. دقت کنید که $(g_1 \cdots g_k)^{n(p_2^{\alpha_2} \cdots p_k^{\alpha_k})} = 1$، یعنی

$$g_1^{n(p_2^{\alpha_2} \cdots p_k^{\alpha_k})} \times (g_2 \cdots g_k)^{n(p_2^{\alpha_2} \cdots p_k^{\alpha_k})} = 1$$

بنابراین $p_1^{\alpha_1} | n(p_2^{\alpha_2} \cdots p_k^{\alpha_k})$، پس $p_1^{\alpha_1} | n$. □

قضیه ۱۶۱. اگر F یک میدان متناهی باشد، آنگاه F^* یعنی گروه ضربیِ F یک گروه دوری است.

اثبات اول. فرض کنید F یک میدان متناهی با p^n عضو باشد، در این صورت $|F^*| = p^n - 1$ و متشکل از ریشه‌های متفاوت چندجمله‌ای $x^{p^n} - x$ است. توجه کنید که توان گروه ضربی F^* برابر است با $p^n - 1$؛ چون اولاً $x^{p^n - 1} = 1$، ثانیاً، اگر برای یک $m < p^n - 1$ داشته باشیم: $\forall x \in F^* (x^m = 1)$، آنگاه تعداد اعضای F^* برابر می‌شود با m. پس گروه F^* دارای عنصری به نام b است به طوری که $\text{ord}(b) = p^n - 1$ یعنی F^* دوری است. □

اثبات دوم. هر گروه آبلی متناهی مانند G ایزومرف با حاصل‌جمع مستقیم گروه‌های دوری به صورت زیر است:

$$G \cong \mathbb{Z}_{m_1} \bigoplus \mathbb{Z}_{m_2} \bigoplus \cdots \bigoplus \mathbb{Z}_{m_k}$$

که $m_1|m_2|\cdots|m_k$ (برای اثبات این نکته به کتاب‌های جبر مراجعه نمائید). بنابراین با توجه به اینکه F^* یک گروه آبلی متناهی با $p^n - 1$ عنصر است. پس

$$F^* = \langle r_1 \rangle \bigoplus \langle r_2 \rangle \bigoplus \cdots \bigoplus \langle r_k \rangle$$

که $\text{ord}(r_i) = m_i$ و $m_1|m_2|\cdots|m_k$. بنابراین هر عنصر در F^* به توان m_k برابر با 1 است. یعنی عناصر F^* ریشه‌های معادله‌ی $x^{m_k} = 1$ هستند. پس $m_k = |F^*|$ و $F^* \cong \mathbb{Z}_{m_k}$. □

۲۶ جلسه‌ی بیست و هشتم: ادامه‌ی میدان‌های متناهی

یادآوری: اگر F یک میدان متناهی باشد، آنگاه عدد اولی مانند p وجود دارد که $\mathbb{Z}_p \subseteq F$. اگر $[F : \mathbb{Z}_p] = n$، آنگاه $|F| = p^n$. فقط یک میدان با این اندازه وجود دارد و این میدان در واقع میدان شکافنده‌ی $x^{p^n} - x$ روی $\mathbb{Z}_p$ است. علاوه‌بر این ثابت کردیم که اگر F یک میدان متناهی باشد، آنگاه $(F^*, \cdot)$ یک گروه دوری است.

نتیجه ۱۶۲. فرض کنید $F \subseteq L$ یک توسیع از میدان‌های متناهی باشد. در این صورت این توسیع ساده است یعنی یک $\alpha \in L$ وجود دارد که $L = F(\alpha)$.

اثبات. گروه ضربی L^* از عناصری به صورت α^i تشکیل شده است، یعنی α به گونه‌ای است که برای مثال $\alpha^{p^n} = 1$ که $|L| = p^n$. بنابراین $L = F(\alpha)$. □

توجه: اگر F یک میدان متناهی باشد، آنگاه $\mathbb{Z}_p \subseteq F$. پس توسیع $\mathbb{Z}_p \subseteq F$ یک توسیع گالوایی است. بنابراین درباره $\text{Gal}(F : \mathbb{Z}_p)$ بحث می‌کنیم.

اولاً توجه کنید که اگر $|F| = p^n$، آنگاه $|\text{Gal}(F : \mathbb{Z}_p)| = n$. ثانیاً ادعا می‌کنیم که نگاشت فروبینیوس یعنی نگاشت $\sigma : F \to F$ که $\sigma(x) = x^p$ عضوی از $\text{Gal}(F : \mathbb{Z}_p)$ است. توجه کنید که قبلاً نشان دادیم که نگاشت فروبینیوس، $\mathbb{Z}_p$ را نقطه‌وار حفظ می‌کند. همچنین $(x + y)^p = x^p + y^p$ و $(x \cdot y)^p = x^p \cdot y^p$. پس نگاشت فوق یک هومومرفیسم است. نشان

می‌دهیم این نگاشت یک‌به یک و پوشا می‌باشد. برای اثبات پوشا بودن، توجه کنید که هر عنصر $x \in F$ در معادله‌ی $x^{p^n} = x$ صدق می‌کند. یعنی $(x^{p^{n-1}})^p = x$. پس نگاشت فوق پوشاست. یک‌به‌یک بودن از پوشا بودن نتیجه می‌شود. به طور کلی، تابع $f : A \to A$ را در نظر بگیرید. اگر A متناهی باشد، آنگاه f یک‌به‌یک است اگر و تنها اگر پوشا باشد. بنابراین σ یک تابع یک‌به‌یک و پوشا می‌باشد که نقاط $\mathbb{Z}_p$ را حفظ می‌کند. پس $\sigma \in \mathrm{Gal}(F : \mathbb{Z}_p)$.

ادعا: گروه $\mathrm{Gal}(F : \mathbb{Z}_p)$ دوری است و توسط σ تولید می‌شود: $\mathrm{Gal}(F : \mathbb{Z}_p) = \langle \sigma \rangle$.

اثبات. فرض کنید $G = \mathrm{Gal}(F : \mathbb{Z}_p)$ و $H = \langle \sigma \rangle$. توجه کنید که $\mathbb{Z}_p \subseteq \{\alpha \,|\, \sigma(\alpha) = \alpha\}$. از طرفی $\sigma(x) = x^p$، با توجه به اینکه معادله‌ی $x^p = x$ حداکثر p ریشه دارد پس $\mathbb{Z}_p = \{\alpha \,|\, \sigma(\alpha) = \alpha\}$. بنابراین چون $\mathbb{Z}_p \subseteq \Phi(H)$ و $\Phi(H) \subseteq \mathbb{Z}_p$ پس $\Phi(H) = \mathbb{Z}_p$. بنابراین $\Phi(H) = \Phi(G)$ یعنی $G = H$. □

مشاهده:

- $\mathrm{Gal}(F : \mathbb{Z}_p) = \{\sigma_i \,|\, 1 \leq i \leq n\}$ که $\sigma_i : F \to F$ به طوری که $\sigma_i(x) = x^{p^i}$.
- فرض کنید $F \subseteq L$ دو میدان متناهی باشند. در این صورت اگر $|F| = p^n$، آنگاه $|L| = p^k$ که $n|k$.
- فرض کنید $F \subseteq L$ دو میدان متناهی باشند. در این صورت $\mathrm{Char}(F) = \mathrm{Char}(L) = p$. توجه کنید که $\mathbb{Z}_p \subseteq F \subseteq L$ و این توسیع یک توسیع گالوایی است. پس توسیع $F \subseteq L$ نیز گالوایی است. بنابراین مطلوب است که گروه $\mathrm{Gal}(L : F)$ را مشخص کنیم.
- $|\mathrm{Gal}(L : F) = \dfrac{[L : \mathbb{Z}_p]}{[F : \mathbb{Z}_p]}| = \dfrac{p^k}{p^n}$.
- گروه $\mathrm{Gal}(L : F)$ زیرگروهی از $\mathrm{Gal}(L : \mathbb{Z}_p)$ است. چون $\mathrm{Gal}(L : \mathbb{Z}_p)$ دوری است، پس $\mathrm{Gal}(L : F)$ یک گروه دوری است. همچنین چون $\mathrm{Gal}(L : \mathbb{Z}_p) = \langle \sigma \rangle$، پس یک n وجود دارد که $\mathrm{Gal}(L : F) = \langle \sigma^n \rangle$. در واقع $|\mathrm{Gal}(L : \mathbb{Z}_p)| = |\langle \sigma \rangle| = p^k$ و اندازه‌ی گروه $\mathrm{Gal}(L : F) = \langle \sigma^n \rangle$ باید $\dfrac{p^k}{p^n}$ شود. پس $n = [F : \mathbb{Z}_p]$، توجه شود که $\sigma^n = (x^{p^n})^{p^{k-n}} = x^{p^k}$.

- بستار جبری $\mathbb{Z}_p$ یعنی $(\mathbb{Z}_p)^{\text{alg}}$ را مشخص می‌کنیم.
ابتدا برای راحتی کار، هر میدان با p^n عنصر را با F_{p^n} نشان می‌دهیم. یک چندجمله‌ای در $\mathbb{Z}_p$ را در نظر بگیرید. میدان شکافنده‌ی آن چندجمله‌ای به صورت $\mathbb{Z}_p \subseteq F_{p^n}$ است. حال همه‌ی چندجمله‌ای با ضرایب در $\mathbb{Z}_p$ را به صورت $\{f_i \mid i \in \mathbb{N}\}$ لیست می‌کنیم. میدان شکافنده‌ی این چندجمله‌ای‌ها را پیدا می‌کنیم. بنابراین دنباله‌ای از میدان‌های متناهی به صورت

$$\mathbb{Z}_p \subseteq F_{p^n} \subseteq F_{p^m} \subseteq F_{p^k} \subseteq \cdots$$

داریم که $n|m|k|\cdots$. بنابراین $(\mathbb{Z}_p)^{\text{alg}} = \bigcup_{n\in N} F_{p^n}$.

- فرض کنید $a \in (\mathbb{Z}_p)^{\text{alg}}$، این عنصر در یکی از F_{p^i}ها قرار می‌گیرد. پس میدان تولید شده توسط a یعنی $\langle a \rangle$ متناهی است. بنابراین $(\mathbb{Z}_p)^{\text{alg}}$ یک میدان موضعاً متناهی است.

پایان

*** رَبَّنَا تَقَبَّلْ مِنَّا إِنَّكَ أَنْتَ السَّمِيعُ الْعَلِيمُ ***

حمزه محمدی

تابستان ۱۴۰۱

مراجع

[1] Fields and Galois Theory, John M.Howie

[2] Galois Theory, Emil Artin

[3] Algebra, Serge Lang

[4] Algebra, Hungerford

[5] Fields and Galois theory, Patrick Morandi