بسم اللّه الرحمن الرحيم

دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

تعریف‌پذیری وجودی حلقه‌های ارزیاب هنسلی

پایان‌نامه کارشناسی ارشد آمار

شقایق شیرانی

استادان راهنما

دکتر محسن خانی

دکتر حامد لروند

۱۴۰۲

دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

پایان‌نامه کارشناسی ارشد آمار خانم شقایق شیرانی

تحت عنوان

تعریف‌پذیری وجودی حلقه‌های ارزیاب هنسلی

در تاریخ ۴ بهمن ۱۴۰۲ توسط کمیته‌ی تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت

۱- استاد راهنمای پایان‌نامه	دکتر محسن خانی
۲- استاد راهنمای پایان‌نامه	دکتر حامد لرونی
۳- استاد داور ۱	دکتر مصطفی عین اله زاده
۴- استاد داور ۲	دکتر مسعود پورمهدیان
سرپرست تحصیلات تکمیلی دانشکده	دکتر بیژن طائری

تقدیم به:

مادر و پدرم

فهرست مطالب

چکیده:

هدف اصلی این پایان‌نامه اثبات قضیه‌ی زیر است:

«فرض کنید K یک میدان ارزیابی هنسلی با حلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های F باشد. اگر میدان F متناهی یا شبه‌بسته‌ی جبری باشد، آنگاه حلقه‌ی ارزیاب $\mathcal{O}$ در میدان ارزیابی هنسلی K به صورت وجودی و بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است».

برای اثبات این قضیه ابتدا دو حکم کلی زیر را اثبات می‌کنیم:

۱. اگر زیرمجموعه‌ی U از حلقه‌ی ارزیاب $\mathcal{O}$ شامل ایده‌آل ماکزیمال $\mathfrak{m}$ باشد و $T \subseteq \mathcal{O}$ همه‌ی کلاس‌های باقیمانده را قطع کند، تساوی $\mathcal{O} = U + T$ برقرار است.

۲. اگر چندجمله‌ای $f(X) \in \mathcal{O}[X]$ ویژگی‌های مطلوبی داشته باشد، زیرمجموعه‌ی تعریف‌پذیر $U_f = \{\frac{۱}{f(x)} - \frac{۱}{f(y)} | x, y \in K\}$ از حلقه‌ی ارزیاب $\mathcal{O}$ شامل ایده‌آل ماکزیمال $\mathfrak{m}$ است.

سپس برای دو حالت میدان باقیمانده‌های متناهی و میدان باقیمانده‌های شبه‌بسته‌ی جبری، به صورت متفاوت وجود چندجمله‌ای f را اثبات می‌کنیم. در نهایت نشان می‌دهیم که در حالت میدان باقیمانده‌های متناهی و میدان باقیمانده‌های شبه‌بسته‌ی جبری به ترتیب زیرمجموعه‌های تعریف‌پذیر $T = \{x \in K : x^q - x = ۰\}$ و $T_f = f(K)^{-۱} f(K)^{-۱} \cup \{۰\}$ از حلقه‌ی ارزیاب $\mathcal{O}$، همه‌ی کلاس‌های باقیمانده را قطع می‌کنند.

قضیه‌ی یاد شده در مقاله‌ی [۷] با عنوان دقیق زیر اثبات شده است.

Fehm, Arno. Existential $\emptyset$-definability of henselian valuation rings. The Journal of Symbolic Logic, 80(1):301–307, 2015

رده‌بندی موضوعی: 03 C 60

واژگان کلیدی: تعریف‌پذیری، میدان ارزیابی هنسلی، میدان‌های شبه‌بسته‌ی جبری، میدان‌های متناهی

پیشگفتار

فرض کنید $\mathfrak{M}$ یک ساختار مرتبه اول با جهان M باشد. یک زیرمجموعه‌ی X از M^n را تعریف‌پذیر با پارامترهای $b_1, ..., b_m$ می‌نامیم، هرگاه فرمول $\varphi(x_1, ..., x_n, y_1, ..., y_m)$ وجود داشته باشد به طوری که

$$X = \{(a_1, ..., a_n) \in M^n \mid \mathfrak{M} \models \varphi(a_1, ..., a_n, b_1, ..., b_m)\}.$$

یک مسئله‌ی مهم در بررسی منطقی ساختارهای مرتبه اول، شناسایی مجموعه‌های تعریف‌پذیر در آنهاست. پاسخ به چنین مسئله‌ای عموماً نیازمند اطلاعات کافی راجع به ویژگی‌های جبری، نظریه‌ی اعدادی، توپولوژیک و ... ساختار است. همچنین در بررسی یک مسئله‌ی تعریف‌پذیری، پیچیدگی سوری فرمول یافت شده و بدون پارامتر بودن آن با اهمیت است.

ساختار مورد مطالعه در این پایان‌نامه، میدان‌های ارزیابی هستند. فرض کنید Γ یک گروه آبلی مرتب و K یک میدان باشد. نگاشت $v : K \to \Gamma \cup \{\infty\}$ را یک نگاشت ارزیابی می‌نامیم، هرگاه برای هر $x, y \in K$ ویژگی‌های زیر برقرار باشد:

۱. $v(x + y) \geq \min\{v(x), v(y)\}$،

۲. $v(x \cdot y) = v(x) + v(y)$،

۳. $x = 0 \Leftrightarrow v(x) = \infty$.

منظور از یک میدان ارزیابی، یک زوج (K, A) است که در آن $A \subseteq K$ یک حلقه‌ی ارزیاب برای K باشد؛ یعنی برای هر $x \in K$ داشته باشیم $x \in A$ یا $x^{-1} \in A$. هر حلقه‌ی ارزیاب A در میدان K حلقه‌ی ارزیاب نظیر یک نگاشت ارزیابی $v : K \to \Gamma$ است؛ یعنی نگاشت ارزیابی $v : K \to \Gamma$ وجود دارد به طوری که

$$\mathcal{O} = \{x \in K : v(x) \geq 0\}.$$

در فصل ۳ خواهیم دید که $\mathcal{O}$ یک حلقه‌ی موضعی است؛ یعنی فقط یک ایده‌آل ماکزیمال دارد که آن را با $\mathfrak{m}$ نمایش می‌دهیم و $F = \frac{\mathcal{O}}{\mathfrak{m}}$ یک میدان است که آن را میدان باقیمانده‌ها می‌نامیم.

مقاله‌ی مورد نظر این پایان‌نامه تعمیمی از مقاله‌ی [۱] است. در واقع در این مقاله با بسط دادن روش‌ها و تکنیک‌های مقاله‌ی [۱]، تعریف‌پذیری حلقه‌های ارزیاب در میدان‌های ارزیابی، با در نظر گرفتن دو حالت میدان باقیمانده‌های متناهی و میدان باقیمانده‌های شبه‌بسته‌ی جبری اثبات شده است.

قضایای زیر دو قضیه‌ی اصلی در این پایان‌نامه هستند:

قضیه ۱. فرض کنید K یک میدان ارزیابی هنسلی با حلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های F باشد. اگر F متناهی باشد، یک تعریف وجودی و بدون پارامتر برای حلقه‌ی $\mathcal{O}$ در میدان K وجود دارد.

قضیه ۲. فرض کنید K یک میدان ارزیابی هنسلی باحلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های F باشد. اگر F شبه‌بسته‌ی جبری باشد و F_{alg}، مجموعه نقاطی از F که روی میدان اول F_0 جبری هستند، بسته‌ی جبری نباشد، آنگاه یک تعریف وجودی و بدون پارامتر برای حلقه‌ی $\mathcal{O}$ در میدان K وجود دارد.

در این پایان‌نامه اثبات قضایای فوق را به همراه پیش‌نیازهای لازم، تا حد امکان تشریح کرده‌ایم. در ادامه خلاصه‌ای از روند این اثبات را طی چند مرحله شرح می‌دهیم.

- **مرحله‌ی اول:** خواهیم دید که اگر دو زیرمجموعه‌ی U و T از حلقه‌ی ارزیاب $\mathcal{O}$ دارای این دو ویژگی باشند که $\mathfrak{m} \subseteq U$ و T همه‌ی کلاس‌های باقیمانده را قطع کند، آنگاه $\mathcal{O} = U + T$.

در مراحل بعدی، هدف معرفی مجموعه‌های تعریف‌پذیر U و T با ویژگی‌های ذکر شده است.

- **مرحله‌ی دوم:** مجموعه‌ی U_f را به صورت $U_f = \{\frac{1}{f(x)} - \frac{1}{f(y)} | x, y \in K\}$ تعریف می‌کنیم که در آن $f \in \mathcal{O}[X]$ چندجمله‌ای و برای هر $x \in K$ داریم $f(x) \neq 0$.

- **مرحله‌ی سوم:** اثبات می‌کنیم که $\mathfrak{m} \subseteq U_f \subseteq \mathcal{O}$، هرگاه چندجمله‌ای $f \in \mathcal{O}[X]$ تکین باشد، $\bar{f}$ در F ریشه نداشته باشد و عنصر $a \in \mathcal{O}$ وجود داشته باشد به طوری که $f'(a) \notin \mathfrak{m}$.

در ادامه‌ی مسیر برای دو حالت میدان باقیمانده‌های متناهی و میدان باقیمانده‌های شبه‌بسته‌ی جبری، به صورت جداگانه ابتدا وجود چندجمله‌ای f با ویژگی‌های بیان شده را تضمین می‌کنیم؛ سپس یک زیرمجموعه‌ی T از حلقه‌ی ارزیاب $\mathcal{O}$ را معرفی می‌کنیم به گونه‌ای که همه‌ی کلاس‌های باقیمانده را قطع کند.

- **مرحله‌ی چهارم (برای حالت متناهی):** اگر F متناهی باشد، خواهیم دید که چندجمله‌ای تکین، تحویل‌ناپذیر و جدایی‌پذیر $f \in F_0[X]$ موجود است که در F ریشه ندارد. همچنین عنصر $a \in F$ به گونه‌ای وجود دارد که $f'(a) \neq 0$.

- **مرحله‌ی پنجم (برای حالت متناهی):** اثبات می‌کنیم که اگر $F = \mathbb{F}_q$، مجموعه‌ی تعریف‌پذیر $T := \{x \in K : x^q - x = 0\}$، زیرمجموعه‌ای از حلقه‌ی ارزیاب $\mathcal{O}$ است و $\bar{T} = F$.

پس از پایان این مرحله خواهیم دید که برای حالتی که میدان باقیمانده‌ها متناهی است، حلقه‌ی ارزیاب $\mathcal{O}$ توسط یک فرمول وجودی و بدون پارامتر در میدان K تعریف می‌گردد و اثبات قضیه‌ی ۱ به پایان می‌رسد.

- **مرحله‌ی چهارم (برای حالت شبه‌بسته‌ی جبری):** به طور کلی نشان می‌دهیم که اگر F یک میدان نامتناهی باشد و F_{alg} بسته‌ی جبری نباشد، چندجمله‌ای تکین، تحویل‌ناپذیر و جدایی‌پذیر $f \in F_{\circ}[X]$ و عنصر $a \in F$ وجود دارند به گونه‌ای که f در F ریشه ندارد و $f'(a) \neq \circ$.

  در فصل ۴ خواهیم دید که میدان‌های شبه‌بسته‌ی جبری نامتناهی هستند. بنابراین به طور خاص اگر F یک میدان شبه‌بسته‌ی جبری باشد و F_{alg} بسته‌ی جبری نباشد، یک چندجمله‌ای f با ویژگی‌های فوق موجود است.

- **مرحله‌ی پنجم (برای حالت شبه‌بسته‌ی جبری):** نشان خواهیم داد که مجموعه‌ی $T_f = f(K)^{-1}f(K)^{-1} \cup \{\circ\}$، زیرمجموعه‌ای از حلقه‌ی ارزیاب $\mathcal{O}$ است و اگر چندجمله‌ای $f \in \mathcal{O}[X]$ تکین و $\bar{f}$ خالی از مربع باشد و در F ریشه نداشته باشد، داریم $\bar{T}_f = F$. همچنین خواهیم دید که چندجمله‌ای f مربوط به مرحله‌ی قبلی، ویژگی‌های مورد نظر در این مرحله را نیز داراست.

نهایتاً پس از پایان این مرحله به سادگی خواهیم دید برای حالتی که میدان باقیمانده‌ها شبه‌بسته‌ی جبری است، حلقه‌ی ارزیاب $\mathcal{O}$ توسط یک فرمول وجودی و بدون پارامتر در میدان K تعریف می‌گردد و اثبات قضیه‌ی ۲ نیز در اینجا به پایان می‌رسد.

علاوه بر اثبات قضیه‌ی ۱ نشان خواهیم داد که برای حالتی که میدان باقیمانده‌ها متناهی است، حلقه‌ی ارزیاب $\mathcal{O}$ در میدان K به صورت یکنواخت تعریف می‌گردد. در واقع نشان خواهیم داد که برای هر عدد اول p و عدد صحیح مثبت m، یک فرمول وجودی و بدون پارامتر φ موجود است به طوری که در هر میدان ارزیابی K با حلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های $F = \mathbb{F}_{p^n}$، اگر $m \nmid n$ آنگاه $\varphi(K) = \mathcal{O}$.

آنچه که شرح داده شد خلاصه‌ای از مطالب فصل پنجم این پایان‌نامه است.

علاوه برمطالب فوق، در فصل چهارم به طور مفصل به معرفی میدان‌های شبه‌بسته‌ی جبری پرداخته‌ایم. اهمیت این فصل در اثبات «مقدماتی بودن» میدان‌های شبه‌بسته‌ی جبری است که پس از بررسی مفاهیم جبری و هندسه‌ی جبری گفته شده است.

در فصل سوم به صورت مختصر و در حد نیاز مقاله‌ی اصلی، به معرفی میدان‌های ارزیابی هنسلی پرداخته‌ایم.

در فصل دوم با فرض بر این‌که خواننده‌ی این نوشته با مفاهیم مقدماتی نظریه مدل‌ها آشنایی دارد، صرفاً تعاریف اصلی مورد نیاز را یادآوری کرده‌ایم و تمرکزمان در این فصل بر اثبات حذف سور میدان‌های بسته‌ی جبری بوده است.

در فصل اول با توجه به این‌که مقاله‌ی اصلی نیازمند پیش‌نیازهای جبری زیادی بوده است به طور مفصل به

مفاهیم جبری پرداخته‌ایم. در این فصل علاوه بر معرفی میدان‌های متناهی و تام، توسیع‌های میدانی مختلف را نیز معرفی کرده‌ایم. قضایای وجود پایه‌ی نرمال و بخش توسیع جدایی‌پذیر مهم‌ترین مطالب این فصل هستند.

در بخش مقالات برای مطالعه‌ی بیشتر، ضمن اشاره به پیشینه‌ی تعریف‌پذیری حلقه‌ی ارزیاب در میدان‌های ارزیابی، برخی از مقالات در این زمینه را معرفی و قضایای اصلی مورد بررسی در هر یک از این مقالات را به صورت مختصر بیان کرده‌ایم.

فصل ۱

جبر و نظریه گالوا

۱.۱ مقدمه

در این فصل مفاهیم و قضایای جبری و نظریه‌ی گالوایی مورد نیاز این پایان‌نامه را بیان می‌کنیم. به طور خاص بخش توسیع‌های میدانی و بخش میدان‌های متناهی، مهم‌ترین بخش‌های این فصل هستند. منابع اصلی این فصل [۱۶] و [۱۲] و [۹] هستند. برای اثبات برخی از قضایای این فصل از منابع [۱۴] و [۳] و [۵] نیز کمک گرفته‌ایم.

۲.۱ مباحث مقدماتی

فرض کنید K یک میدان باشد. حلقه‌ی $K[X] = \{a_0 + a_1X + ... + a_nX^n \mid n \in \mathbb{N}, a_i \in K\}$ را حلقه‌ی چندجمله‌ای‌های با تک متغیر X می‌نامیم و میدان کسرهای $K[X]$ را با $K(X)$ نمایش می‌دهیم؛ بنابراین $K(X) = \{\frac{f}{g} \mid f, g \in K[X]\}$.

یک چندجمله‌ای غیر ثابت $f \in K[X]$ را تحویل‌ناپذیر [1] روی K می‌گوییم هرگاه نتوانیم آن را به صورت حاصل‌ضرب دو چندجمله‌ای غیرثابت با ضرایب در K بنویسیم. یک چندجمله‌ای تحویل‌ناپذیر f روی K (از درجه‌ی بیشتر از یک) در خود K هیچ ریشه‌ای ندارد. زیرا اگر $\beta \in K$ ریشه‌ی چندجمله‌ای f باشد، بنا به الگوریتم

[1] irreducible

تقسیم داریم $f(\beta) = ۰$ اگروتنهااگر یک چندجمله‌ای $h \in K[X]$ موجود باشد به طوری که $f = (X - \beta)h$. اما چندجمله‌ای f در میدان $K \subseteq \frac{K[X]}{\langle f \rangle}$ دارای ریشه است. در واقع عنصر $X + \langle f \rangle \in \frac{K[X]}{\langle f \rangle}$ یک ریشه برای آن است. مثلاً اگر $f(X) = a_۰ + a_۱X + a_۲X^۲ \in K[X]$ داریم:

$$\begin{aligned} f(X + \langle f \rangle) &= (a_۰ + \langle f \rangle) + (a_۱ + \langle f \rangle)(X + \langle f \rangle) + (a_۲ + \langle f \rangle)(X + \langle f \rangle)^۲ \\ &= a_۰ + \langle f \rangle + a_۱X + \langle f \rangle + (a_۲ + \langle f \rangle)(X^۲ + \langle f \rangle) \\ &= (a_۰ + \langle f \rangle) + (a_۱X + \langle f \rangle) + (a_۲X^۲ + \langle f \rangle) \\ &= a_۰ + a_۱X + a_۲X^۲ + \langle f \rangle = ۰. \end{aligned}$$

توجه کنید که اگر یک چندجمله‌ای f در K ریشه نداشته باشد، نمی‌توانیم نتیجه بگیریم که f روی K تحویل‌ناپذیر است. برای مثال چندجمله‌ای $f(X) = (X^۲ + ۱)(X^۲ + X + ۲)$ در $\mathbb{R}$ ریشه ندارد، اما تحویل‌پذیر است.

تعریف ۱.۲.۱. توسیع میدانی $K \subseteq L$ را در نظربگیرید. عنصر $\alpha \in L$ را روی K جبری می‌نامیم هرگاه یک چندجمله‌ای ناصفر $f \in K[X]$ موجود باشد به طوری که $f(\alpha) = ۰$. اگر α روی K جبری نباشد، آن را غیرجبری یا متعالی می‌نامیم.

فرض کنید $K \subseteq L$ یک توسیع میدانی و $\alpha \in L$ یک عنصر جبری روی K باشد. چندجمله‌ای تکین $f \in K[X]$ را چندجمله‌ای مینیمال α می‌نامیم هرگاه $f(\alpha) = ۰$ و چندجمله‌ای f در میان چندجمله‌ای‌های متعلق به $K[X]$ که α ریشه‌ی آن‌هاست، حداقل درجه را داشته باشد. در لم زیر نشان می‌دهیم که چندجمله‌ای $f \in K[X]$، چندجمله‌ای مینیمال α است اگروتنهااگر f تحویل‌ناپذیر و α یک ریشه‌ی آن باشد.

لم ۲.۲.۱. فرض کنید $K \subseteq L$ یک توسیع میدانی و $\alpha \in L$ یک عنصر جبری روی K باشند. در این صورت عبارت‌های زیر معادل هستند:

۱. چندجمله‌ای f چندجمله‌ای مینیمال α است.

۲. چندجمله‌ای f یک چندجمله‌ای تحویل‌ناپذیر است، به طوری که $f(\alpha) = ۰$.

اثبات. ابتدا فرض می‌کنیم چندجمله‌ای $f \in K[X]$ چندجمله‌ای مینیمال α باشد. اثبات می‌کنیم که $f \in K[X]$ روی K تحویل‌ناپذیر است. به برهان خلف فرض می‌کنیم که $f(X)$ تحویل‌پذیر باشد. بنابراین چندجمله‌ای‌های $h(X), g(X) \in K[X]$ وجود دارند به طوری که $f(X) = h(X)g(X)$. از طرفی $f(\alpha) = ۰$، پس $h(\alpha)g(\alpha) = ۰$. بنابراین $h(\alpha) = ۰$ یا $g(\alpha) = ۰$. اما درجه‌ی h و درجه‌ی g از درجه‌ی چندجمله‌ای $f(X)$ کمتر هستند که این با فرض مینیمال بودن چندجمله‌ای f در تناقض است.

حال فرض می‌کنیم $\alpha \in L$ ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر مانند f باشد. همچنین به برهان خلف فرض می‌کنیم f چندجمله‌ای مینیمال α نباشد. در این صورت یک چندجمله‌ای $g \in K[X]$ وجود دارد که چندجمله‌ای مینیمال α است و درجه‌ی آن کمتر از درجه‌ی چندجمله‌ای f است. بنا به الگوریتم تقسیم داریم $f = gh + r$. از طرفی $f(\alpha) = ۰$ بنابراین $f(\alpha) = g(\alpha)h(\alpha) + r(\alpha) = ۰$. در نتیجه $r(\alpha) = ۰$، اما با توجه این‌که درجه‌ی r از درجه‌ی g کمتر است و g چندجمله‌ای مینیمال α است، داریم $r = ۰$. از این رو $f(X) = g(X)h(X)$ که با فرض تحویل‌ناپذیر بودن f در تناقض است.

□

اگر $\alpha \in L$ یک عنصر جبری روی K باشد، آنگاه چندجمله‌ای مینیمال α یکتاست. زیرا اگر $g = c_۰ + c_۱X + ... + c_{n-۱}X^{n-۱} + X^n \in K[X]$ و $h = b_۰ + b_۱X + ... + b_{n-۱}X^{n-۱} + X^n \in K[X]$ دو چندجمله‌ای تکین با حداقل درجه باشند به طوری که $g(\alpha) = h(\alpha) = ۰$، بنا به الگوریتم تقسیم $h \mid g$ و $g \mid h$. از طرفی h و g حداقل درجه را دارند، پس بنا به لم ۲.۲.۱، h و g تحویل‌ناپذیرند. بنابراین $f = ug$ به طوری که u یک عنصر یکه است. اما با توجه به این‌که ضریب X^n در h و g عدد یک است، داریم $u = ۱$. در نتیجه $f = g$.

لم ۳.۲.۱. فرض کنید f چندجمله‌ای مینیمال α باشد. در این صورت چندجمله‌ای مینیمال $\alpha^{-۱}$ با چندجمله‌ای مینیمال α، هم درجه است.

اثبات. فرض می‌کنیم $f = a_۰ + a_۱X + ... + a_{n-۱}X^{n-۱} + X^n$ چندجمله‌ای مینیمال α باشد. بنابراین $f(\alpha) = a_۰ + a_۱\alpha + \cdots + a_{n-۱}\alpha^{n-۱} + \alpha^n = ۰$. از ضرب طرفین این عبارت در $(\alpha^{-۱})^n$ داریم:

$$a_۰(\alpha^{-۱})^n + a_۱(\alpha^{-۱})^{n-۱} + \cdots + a_{n-۱}(\alpha^{-۱}) + ۱ = ۰.$$

حال کافی است طرفین رابطه‌ی فوق را در $a_۰^{-۱}$ ضرب کنیم. در این صورت داریم:

$$(\alpha^{-۱})^n + \frac{a_۱}{a_۰}(\alpha^{-۱})^{n-۱} + \cdots + \frac{a_{n-۱}}{a_۰}(\alpha^{-۱}) + \frac{۱}{a_۰} = ۰.$$

ادعا می‌کنیم که چندجمله‌ای $g(X) = X^n + \frac{a_۱}{a_۰}X^{n-۱} + \cdots + \frac{a_{n-۱}}{a_۰}X + \frac{۱}{a_۰}$ چندجمله‌ای مینیمال $\alpha^{-۱}$ است. به منظور اثبات این ادعا کافی است نشان دهیم چندجمله‌ای g در میان چندجمله‌ای‌هایی که $\alpha^{-۱}$ ریشه‌ی آنهاست حداقل درجه را دارد. به برهان خلف فرض می‌کنیم چندجمله‌ای $h = c_mX^m + c_{m-۱}X^{m-۱} + \cdots + c_۱X + c_۰$ با درجه‌ی $m < n$ موجود باشد به طوری که $h(\alpha^{-۱}) = ۰$. مشابه روند ساختن چندجمله‌ای g با ضرب طرفین h در $\frac{\alpha^m}{c_۰}$ داریم $\frac{c_m}{c_۰} + \frac{c_{m-۱}}{c_۰}\alpha + \cdots + \frac{c_۱}{c_۰}\alpha^{m-۱} + \alpha^m = ۰$. بنابراین یک چندجمله‌ای تکین با درجه‌ی $m < n$ ایجاد می‌شود که α ریشه‌ی آن است و این با مینیمال بودن

چندجمله‌ای f در تناقض است. از این رو چندجمله‌ای g چندجمله‌ای مینیمال α^{-1} است و همچنین بنا به نحوه‌ی ساختن چندجمله‌ای g، واضح است که درجه‌ی این چندجمله‌ای دقیقاً با درجه‌ی f برابر است.
□

فرض کنید $K \subseteq L$ یک توسیع میدانی و $\alpha \in L - K$ یک عنصر جبری روی K باشد. در ادامه قصد داریم میدان تولید شده توسط α و K در میدان L را مورد بررسی قرار دهیم.

لم ۴.۲.۱. توسیع میدانی $K \subseteq L$ را در نظر بگیرید و فرض کنید چندجمله‌ای $f \in K[X]$ تحویل‌ناپذیر است. همچنین فرض کنید α یک ریشه برای چندجمله‌ای f در میدان L است. در این صورت $K[\alpha] \cong \frac{K[X]}{\langle f \rangle}$.

اثبات. نگاشت $\varphi : K[X] \to L$ با ضابطه‌ی $\varphi(h(X)) = h(\alpha)$ را در نظر می‌گیریم. به سادگی می‌توان بررسی کرد که این نگاشت یک همریختی است. (برای هر $h_1(X), h_2(X) \in K[X]$ داریم $\varphi(h_1(X) + h_2(X)) = h_1(\alpha) + h_2(\alpha)$ و $\varphi(h_1(X) \cdot h_2(X)) = h_1(\alpha) \cdot h_2(\alpha)$). از طرفی واضح است که تصویر φ در L به صورت $\mathrm{Im}(\varphi) = \{h(\alpha) \mid h \in K[X]\} = K[\alpha]$ و هسته‌ی آن به صورت $\mathrm{Ker}(\varphi) = \{h \in K[X] \mid h(\alpha) = 0\}$ است. ادعا می‌کنیم که $\mathrm{Ker}(\varphi) = \langle f \rangle$. به جهت اثبات این ادعا چندجمله‌ای $h(X) \in K[X]$ را در نظر می‌گیریم و فرض می‌کنیم $h(\alpha) = 0$. کافی است اثبات کنیم $f \mid h$. بنا به الگوریتم تقسیم داریم $h(X) = f(X)g(X) + r(X)$ به طوری که $\deg(r) < \deg(f)$. از طرفی داریم $h(\alpha) = f(\alpha) = 0$ بنابراین $r(\alpha) = 0$. همچنین می‌دانیم چندجمله‌ای f تحویل‌ناپذیر است، پس بنا به لم ۲.۲.۱ حداقل درجه را دارد. درنتیجه $r = 0$ و $h = fg$؛ یعنی $f \mid h$. بنابراین $\mathrm{Ker}(\varphi) = \langle f \rangle$. بنا به قضیه‌ی اول یکریختی $\mathrm{Im}(\varphi) = K[\alpha] \cong \frac{K[X]}{\langle f \rangle}$. □

توجه کنید که در لم فوق چندجمله‌ای $f \in K[X]$ تحویل‌ناپذیر است. بنابراین ایده‌آل $\langle f \rangle$ یک ایده‌آل ماکزیمال و در نتیجه $\frac{K[X]}{\langle f \rangle}$ یک میدان است، پس بنا به لم فوق $K[\alpha]$ کوچکترین میدان شامل K و α در L است و با $\frac{K[X]}{\langle f \rangle}$ یکریخت است.

اگر $K \subseteq L$ و $\alpha_1, \ldots, \alpha_n$ متعلق به L باشند، میدان تولید شده توسط K و $\alpha_1, \ldots, \alpha_n$ در L را با نماد $K(\alpha_1, \ldots, \alpha_n)$ نمایش می‌دهیم. بنابراین اگر α روی K جبری باشد، میدان تولید شده توسط K و α به صورت زیر است:

$$K(\alpha) = \{\frac{h(\alpha)}{g(\alpha)} \mid h, g \in K[X]\} = K[\alpha].$$

فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. در این صورت L به طور خاص یک فضای برداری روی میدان K است. بُعد فضای برداری L روی K را با $[L : K]$ نمایش می‌دهیم.

لم ۵.۲.۱. توسیع میدانی $K \subseteq L$ و عنصر جبری $\alpha \in L - K$ را در نظر بگیرید. فرض کنید f چندجمله‌ای مینیمال α با درجه‌ی n باشد. در این صورت $[K(\alpha) : K] = n$.

اثبات. در لم ۴.۲.۱ دیدیم که $K(\alpha) = K[\alpha] \cong \frac{K[X]}{\langle f \rangle}$. در نتیجه با توجه به این‌که درجه‌ی چندجمله‌ای f برابر با n است، داریم $K(\alpha) = \{a_۰ + \ldots + a_{n-۱}\alpha^{n-۱} \mid a_i \in K\}$. بنابراین هر عنصر از $K(\alpha)$ توسط $\{۱, \alpha, \alpha^۲, \ldots, \alpha^{n-۱}\}$ تولید می‌شود. ادعا می‌کنیم که عناصر $\{۱, \alpha, \alpha^۲, \ldots, \alpha^{n-۱}\}$ روی K مستقل‌خطی هستند. به منظور اثبات این ادعا به برهان خلف فرض می‌کنیم $a_۰ + a_۱\alpha + \ldots + a_n\alpha^{n-۱} = ۰$. در این صورت α ریشه‌ی یک چندجمله‌ای با درجه‌ی کمتر از n است که این با مینیمال بودن چندجمله‌ای f در تناقض است. بنابراین $\{۱, \alpha, \alpha^۲, \ldots, \alpha^{n-۱}\}$ پایه‌ای برای فضای برداری $K(\alpha)$ روی K است. پس $[K(\alpha) : K] = n$. □

لم ۶.۲.۱. فرض کنید $K \subseteq L \subseteq M$، در این صورت $[M : K] = [M : L] \times [L : K]$.

اثبات. فرض می‌کنیم $\{\alpha_۱, \alpha_۲, \ldots, \alpha_n\}$ پایه‌ی فضای‌برداری L روی K و $\{\beta_۱, \beta_۲, \ldots, \beta_m\}$ پایه‌ی فضای‌برداری M روی L باشند. ادعا می‌کنیم $\{\alpha_i\beta_j \mid ۱ \leq i \leq n, ۱ \leq j \leq m\}$ پایه‌ای برای فضای برداری M روی K است. به منظور اثبات این ادعا، فرض می‌کنیم z یک عنصر دلخواه متعلق به M باشد. در این صورت $z = r_۱\beta_۱ + r_۲\beta_۲ + \ldots + r_m\beta_m$ به طوری که $r_i \in L$. از طرفی هر عنصر $r_i \in L$ توسط $\{\alpha_۱, \alpha_۲, \ldots, \alpha_n\}$ تولید می‌شود. پس بوضوح z یک ترکیب خطی از $\alpha_i\beta_j$ است. حال کافی است نشان دهیم $\{\alpha_i\beta_j | ۱ \leq i \leq n, ۱ \leq j \leq m\}$ یک مجموعه‌ی مستقل خطی است. فرض می‌کنیم ترکیب خطی $r_۱\alpha_۱\beta_۱ + \ldots + r_k\alpha_k\beta_k$ که در آن $r_۱, \ldots, r_k$ متعلق به K هستند، صفر شود. در این صورت $(r_۱\alpha_۱)\beta_۱ + \ldots + (r_k\alpha_k)\beta_k = ۰$. اما با توجه به این‌که β_j ها مستقل خطی هستند $r_۱\alpha_۱ = \ldots = r_k\alpha_k = ۰$. بنابراین ترکیب خطی $r_۱\alpha_۱ + \ldots + r_k\alpha_k$ برابر با صفر است. از طرفی α_i نیز مستقل خطی هستند. بنابراین $r_۱ = \ldots = r_k = ۰$.

□

قضیه ۷.۲.۱. فرض کنید K یک میدان و $f \in K[X]$ یک چندجمله‌ای باشد. در این صورت یک میدان $K \subseteq L$ موجود است به طوری که تمام ریشه‌های f در L قرار دارند.

اثبات. فرض می‌کنیم f یک چندجمله‌ای تحویل‌ناپذیر باشد. در این صورت دیدیم که میدان $K \subseteq L_۱$ موجود است که در آن چندجمله‌ای f حداقل یک ریشه دارد. فرض می‌کنیم β ریشه‌ی f در $L_۱$ باشد. در این صورت در میدان $L_۱$ داریم $f = (X - \beta)h(X)$. حال اگر ریشه‌های $h(X)$ همگی در $L_۱$ باشند، به میدان مورد علاقه‌ی خود رسیده‌ایم. در غیر این صورت، چندجمله‌ای $h(X)$ را در $L_۱[X]$ به عوامل تحویل‌ناپذیر تجزیه می‌کنیم. عامل تحویل‌ناپذیر $h_۱(X)$ از $h(X)$ را در نظر می‌گیریم. میدان $K \subseteq L_۱ \subseteq L_۲$ وجود دارد که در آن $h_۱(X)$ دارای ریشه است. با تکرار روند فوق به یک میدان $K \subseteq L$ می‌رسیم که در آن L شامل تمامی ریشه‌های f است.

حال فرض می‌کنیم f تحویل‌پذیر باشد. در این حالت ابتدا آن را به عوامل تحویل‌ناپذیر تجزیه می‌کنیم، سپس مطابق روند گفته شده عمل می‌کنیم. □

تعریف ۸.۲.۱. چندجمله‌ای $f \in K[X]$ و میدان $K \subseteq L$ را به گونه‌ای در نظر بگیرید که L شامل همه‌ی ریشه‌های چندجمله‌ای f باشد. همچنین فرض کنید $S \subseteq L$ مجموعه‌ی همه‌ی ریشه‌های f در L باشد. میدان $K(S)$ را یک میدان شکافنده‌ی f می‌نامیم. همچنین برای یک مجموعه از چندجمله‌ای‌ها با ضرایب در K نیز، میدان شکافنده به طور مشابه تعریف می‌گردد.

میدان شکافنده در حد یکریختی یکتاست و تعریف فوق از L مستقل است.

۳.۱ توسیع‌های میدانی

در این زیربخش چندین توسیع میدانی را معرفی کرده‌ایم و در حد نیاز به بررسی ویژگی‌ها و قضایای مربوط به آن‌ها پرداخته‌ایم. ابتدا توسیع‌های معروف مانند توسیع متناهی، توسیع جبری و ... را یادآوری کرده‌ایم و رفته رفته به توسیع‌های مهم‌تر مانند توسیع جدایی‌پذیر و توسیع منتظم رسیده‌ایم.

۱.۳.۱ توسیع متناهی

توسیع میدانی $K \subseteq L$ را در نظر بگیرید؛ این توسیع را متناهی می‌نامیم هرگاه $[L : K]$ متناهی باشد.
فرض کنید $\alpha \in L - K$ یک عنصر جبری روی K، با چندجمله‌ای مینیمال f باشد. در این صورت بنا به لم ۵.۲.۱ بُعد توسیع $K(\alpha)$ روی K متناهی است.

لم ۱.۳.۱. اگر $K \subseteq L$ یک توسیع متناهی باشد، هر عنصر $\alpha \in L$ روی K جبری است.

اثبات. به برهان خلف فرض می‌کنیم $\alpha \in L - K$ روی K متعالی باشد. در این صورت α ریشه‌ی هیچ چندجمله‌ای با ضرایب در K نیست. پس $\{1, \alpha, \alpha^2, \ldots\}$ روی K مستقل خطی هستند. از این رو $[L : K]$ نامتناهی است که تناقض است.

□

توجه کنید که جهت عکس نتیجه‌ی فوق لزوماً برقرار نیست. به عنوان مثال، میدان تمام اعداد جبری یک توسیع نامتناهی از $\mathbb{Q}$ است و هر عنصر آن روی $\mathbb{Q}$ جبری است.

۲.۳.۱ توسیع جبری

تعریف ۲.۳.۱. توسیع میدانی $K \subseteq L$ را یک توسیع جبری می‌نامیم هرگاه هر عنصر $\alpha \in L - K$ ریشه‌ی یک چندجمله‌ای با ضرایب در K باشد.

در لم ۱.۳.۱ دیدیم که اگر $K \subseteq L$ یک توسیع متناهی باشد، آنگاه هر عنصر $\alpha \in L$ روی K جبری است. بنابراین هر توسیع متناهی یک توسیع جبری است. همچنین در لم ۵.۲.۱ دیدیم که اگر $K \subseteq L$ یک توسیع میدانی و عنصر $\alpha \in L - K$ روی K جبری باشد، آنگاه توسیع $K \subseteq K(\alpha)$ یک توسیع متناهی است. از این رو توسیع $K \subseteq K(\alpha)$ یک توسیع جبری است.

لم ۳.۳.۱. فرض کنید $K \subseteq L$ و $\beta_۱, \beta_۲ \in L$ روی K جبری باشند. در این صورت عناصر $\beta_۱ + \beta_۲$ و $\beta_۱ \cdot \beta_۲$ روی K جبری هستند.

اثبات. فرض می‌کنیم $\beta_۱, \beta_۲ \in L$ روی K جبری باشند. ادعا می‌کنیم توسیع $K(\beta_۱, \beta_۲)$ روی K یک توسیع متناهی است. به جهت اثبات این ادعا توجه کنید که بنا به فرض $\beta_۱, \beta_۲ \in L$ روی K جبری هستند. بنابراین $\beta_۲$ روی $K(\beta_۱)$ نیز جبری است، پس بنا به لم ۵.۲.۱ توسیع $K \subseteq K(\beta_۱)$ و توسیع $K(\beta_۱) \subseteq K(\beta_۱)(\beta_۲)$ متناهی هستند. در نتیجه $[K(\beta_۱) : K]$ و $[K(\beta_۱)(\beta_۲) : K(\beta_۱)]$ متناهی هستند. از طرفی داریم $[K(\beta_۱)(\beta_۲) : K] = [K(\beta_۱)(\beta_۲) : K(\beta_۱)] \times [K(\beta_۱) : K]$. بنابراین $[K(\beta_۱)(\beta_۲) : K]$ نیز متناهی است؛ یعنی توسیع $K(\beta_۱, \beta_۲)$ یک توسیع متناهی روی K است. از این رو بنا به نتیجه‌ی ۱.۳.۱ همه‌ی عناصر موجود در میدان $K(\beta_۱, \beta_۲)$ روی K جبری هستند. به بیان دیگر عناصر $\beta_۱ + \beta_۲$، $\beta_۱ \cdot \beta_۲$، $-\beta_۱$، $-\beta_۲$، $\beta_۱^{-۱}, \beta_۲^{-۱}$ و $\beta_۱ - \beta_۲$ همگی روی K جبری هستند. □

قضیه ۴.۳.۱. فرض کنید $K \subseteq L$ یک توسیع متناهی باشد. در این صورت عناصر جبری $\alpha_۱, ..., \alpha_n \in L$ موجودند به طوری که L میدان تولید شده توسط K و $\alpha_۱, ..., \alpha_n$ در داخل L است. به بیان دیگر $L = K(\alpha_۱, ..., \alpha_n)$.

اثبات. فرض می‌کنیم $\alpha_۱, ..., \alpha_n \in L$ یک پایه برای فضای برداری L روی K باشد. در این صورت واضح است که $L \subseteq K(\alpha_۱, ..., \alpha_n)$. از طرفی $K(\alpha_۱, ..., \alpha_n) \subseteq L$. بنابراین $L = K(\alpha_۱, ..., \alpha_n)$. □

قضیه ۵.۳.۱. فرض کنید توسیع $K \subseteq L$ و توسیع $L \subseteq M$ جبری باشند. در این صورت توسیع $K \subseteq M$ جبری است.

اثبات. عنصر دلخواه $\alpha \in M$ را در نظر می‌گیریم. اگر $\alpha \in L$، آنگاه با توجه به این‌که توسیع $K \subseteq L$ یک توسیع جبری است بوضوح α یک عنصر جبری روی K است.

حال فرض می‌کنیم $\alpha \in M - L$. در این صورت با توجه به این‌که توسیع $L \subseteq M$ جبری است، چندجمله‌ای تحویل‌ناپذیر $f = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in L[X]$ وجود دارد به طوری که $f(\alpha) = 0$. به بیان دیگر عنصر α روی میدان $L' = K(a_0, a_1, ..., a_n)$ جبری است، پس بنا به لم ۵.۲.۱ توسیع $L' \subseteq L'(\alpha)$ یک توسیع متناهی و در نتیجه جبری است. از طرفی $K \subseteq L'$ نیز یک توسیع متناهی است. بنابراین با توجه به این‌که $[L'(\alpha) : K] = [L' : K] \times [L'(\alpha) : L']$، درجه‌ی توسیع $L'(\alpha)$ روی K متناهی است. از این رو توسیع $K \subseteq L'(\alpha)$ یک توسیع متناهی است. بنابراین طبق لم ۱.۳.۱ عنصر α روی K جبری است.
□

فرض کنید $K \subseteq L$ میدان شکافنده‌ی چندجمله‌ای $f \in K[X]$ باشد. در قضیه‌ی زیر اثبات می‌کنیم که هر چندجمله‌ای تحویل‌ناپذیر $g \in K[X]$، اگر یک ریشه در L داشته باشد، آنگاه تمام ریشه‌هایش در L است.

قضیه ۶.۳.۱. فرض کنید $K \subseteq L$ میدان شکافنده‌ی چندجمله‌ای $f \in K[X]$ باشد. همچنین فرض کنید $g \in K[X]$ یک چندجمله‌ای تحویل‌ناپذیر باشد. در این صورت یا تمام ریشه‌های g در L هستند یا g در L هیچ ریشه‌ای ندارد.

اثبات. چندجمله‌ای تحویل‌ناپذیر $g \in K[X]$ را در نظر می‌گیریم و فرض می‌کنیم α یک ریشه‌ی g در L باشد. کافی است نشان دهیم هر ریشه‌ی دیگر از g نیز متعلق به L است. بدین منظور فرض می‌کنیم $L \subseteq H$ میدان شکافنده‌ی f و g باشد و $\beta \in H$ یک ریشه‌ی دیگر برای g است. بنابراین $K(\alpha) \cong K(\beta)$. از طرفی L میدان شکافنده‌ی f روی $K(\alpha)$ است و $L(\beta)$ میدان شکافنده‌ی f روی $K(\beta)$ است، در نتیجه $L(\beta) \cong L$. از این‌که $L(\beta) \cong L$ نتیجه می‌گیریم که $[L(\beta) : K(\beta)] = [L : K(\alpha)]$ و از این‌که $K(\alpha) \cong K(\beta)$ نتیجه می‌گیریم $[K(\alpha) : K] = [K(\beta) : K]$. بنابراین

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

پس $[L : K] = [L(\beta) : K]$. از طرفی با توجه به این‌که $K \subseteq L \subseteq L(\beta)$ داریم:

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

بنابراین $[L : K] = [L(\beta) : K] = [L : K] \times [L(\beta) : L]$ و در نتیجه $[L(\beta) : L] = 1$. از این رو $L(\beta) = L$، پس $\beta \in L$. □

فرض کنید $K \subseteq L$ میدان شکافنده‌ی تمامی چندجمله‌ای‌های موجود در $K[X]$ باشد. در این صورت $L = K(S)$ به طوری که S مجموعه ریشه‌های همه‌ی چندجمله‌ای‌های موجود در $K[X]$ است. بنابراین برای هر α متعلق به L داریم $\alpha \in K(S)$. از این رو بوضوح α روی K جبری است، پس توسیع L روی K یک

توسیع جبری است. همچنین هیچ توسیع جبری سره L' از L وجود ندارد. زیرا اگر L' یک توسیع جبری سره از L باشد، بنا به قضیه‌ی ۵.۳.۱ توسیع L' روی K یک توسیع جبری از K است؛ یعنی هر عنصر از L' ریشه‌ی یک چندجمله‌ای با ضرایب در K است. از طرفی L میدان شکافنده‌ی همه‌ی چندجمله‌ای‌های با ضرایب در K است. بنابراین $L' \subseteq L$ که با فرض $K \subseteq L \subsetneq L'$ در تناقض است. به بیان دیگر اگر $K \subseteq L$ میدان شکافنده‌ی تمام چندجمله‌ای‌های موجود در $K[X]$ باشد، آنگاه هرچندجمله‌ای در $L[X]$ تمام ریشه‌هایش در خود L است.

تعریف ۷.۳.۱. میدان L را بسته‌ی جبری می‌نامیم هرگاه هر چندجمله‌ای $f \in L[X]$ تمام ریشه‌هایش در میدان L باشد. به بیان دیگر میدان L را بسته‌ی جبری می‌نامیم هرگاه هرچندجمله‌ای متعلق به $L[X]$ در L شکافته شود.

تعریف ۸.۳.۱. میدان $K \subseteq L$ را یک بستارجبری K می‌نامیم هرگاه توسیع $K \subseteq L$ یک توسیع جبری باشد و میدان L بسته‌ی جبری باشد. بستارجبری K را با نماد $\tilde{K}$ نمایش می‌دهیم.

به کمک لم زرن می‌توان نشان داد که بستارجبری یک میدان K در حد یکریختی یکتاست.

نتیجه ۹.۳.۱. میدان شکافنده‌ی همه‌ی چندجمله‌های موجود در $K[X]$ یک بستار جبری K است.

۳.۳.۱ توسیع جدایی‌پذیر

مستقل جبری و مجزای خطی

از جبرخطی به یاد داریم که عناصر $a_1, \ldots, a_n$ از یک فضای برداری V روی K را مستقل خطی می‌نامیم هرگاه برای هر ترکیب خطی $r_1a_1 + r_2a_2 + \ldots + r_na_n$ که در آن $r_1, \cdots, r_n \in K$ اگر $r_1a_1 + r_2a_2 + \ldots + r_na_n = 0$ آنگاه $r_1 = r_2 = \ldots = r_n = 0$. پایه‌ی یک فضای برداری بزرگترین مجموعه‌ی مستقل خطی روی این فضاست و اگر B_1 و B_2 دو پایه برای یک فضای برداری باشند، آنگاه $|B_1| = |B_2|$ و اندازه‌ی یک پایه برای فضای برداری را بُعد آن فضا می‌نامیم. در بخش‌های گذشته یک توسیع میدانی $K \subseteq L$ را به عنوان یک فضای برداری بررسی کردیم. در این بخش یک توسیع میدانی را به عنوان یک میدان مورد بررسی قرار می‌دهیم و مفاهیم مستقل جبری و پایه‌ی متعالی را معرفی می‌کنیم. در لم ۵.۲.۱ دیدیم که اگر $\alpha \in L - K$ روی K جبری و f چندجمله‌ای مینیمال α باشد، آنگاه $[K(\alpha) : K] = n = \deg(f)$. همچنین از نتیجه‌ی ۱.۳.۱ می‌توان نتیجه گرفت که اگر $\alpha \in L - K$ متعالی باشد، آنگاه $[K(\alpha) : K]$ نامتناهی است. اما توجه کنید که در هر دو حالت، $K(\alpha)$ به عنوان میدان فقط با یک عنصر تولید می‌شود. این مطلب ایده‌ی تعریف مفهوم استقلال جبری است.

فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. در سرتاسر این بخش منظور از K^{alg} اشتراک بستار جبری K با میدان L است.

تعریف ۱۰.۳.۱ (مستقل 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 n متغیره‌ی $f(X_1, ..., X_n) \in K[X_1, ..., X_n]$ اگر $f(\alpha_1, ..., \alpha_n) = 0$ آنگاه $f = 0$. همچنین یک زیرمجموعه‌ی T از L را مستقل جبری روی K می‌نامیم هرگاه برای هر $t_1, \cdots, t_n \in T$ و هر چندجمله‌ای ناصفر $f(X_1, ..., X_n) \in K[X_1, ..., X_n]$ داشته باشیم $f(t_1, \cdots, t_n) \neq 0$.

از تعریف استقلال جبری مستقیماً موارد زیر نتیجه می‌شوند:

- عنصر α روی K مستقل جبری است هرگاه، α روی K متعالی باشد، به بیان دیگر $\alpha \notin K^{alg}$.
- اگر α, β روی K مستقل جبری باشند، آنگاه برای هر چندجمله‌ای دو متغیره‌ی $f(X_1, X_2) \in K[X_1, X_2]$ اگر $f(\alpha, \beta) = 0$، آنگاه $f = 0$. بنابراین واضح است که عنصر α روی K و $K(\beta)$ متعالی است. همچنین عنصر β روی K و روی $K(\alpha)$ متعالی است. بنابراین $\alpha, \beta \notin K^{alg}$، $\alpha \notin (K(\beta))^{alg}$ و $\beta \notin (K(\alpha))^{alg}$.
- $\alpha_1, \ldots, \alpha_n$ روی K مستقل جبری هستند هرگاه برای هر $1 \leq i \leq n$ داشته باشیم $\alpha_i \notin (K(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n))^{alg}$.

تعریف ۱۱.۳.۱ (پایه‌ی متعالی). فرض کنید $K \subseteq L$ یک توسیع میدانی و زیرمجموعه‌ی T از L روی K مستقل جبری باشد. مجموعه‌ی T را یک پایه‌ی متعالی [۲] برای توسیع $K \subseteq L$ می‌نامیم هرگاه T یک زیرمجموعه‌ی مستقل جبری ماکزیمال روی K باشد.

اگر $K \subseteq L$ یک توسیع میدانی و T یک زیرمجموعه از L باشد، به سادگی می‌توان دید که مجموعه‌ی T یک زیرمجموعه‌ی مستقل جبری ماکزیمال روی K است اگروتنهااگر توسیع $K(T) \subseteq L$ یک توسیع جبری باشد.

تعریف ۱۲.۳.۱. توسیع میدانی $K \subseteq L$ را در نظر بگیرید و فرض کنید $\alpha_1, \ldots, \alpha_n \in L - K$ به گونه‌ای باشند که $L = K(\alpha_1, \ldots, \alpha_n)$. همچنین 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 آن را با $\mathrm{trdeg}(L : K)$ نمایش می‌دهیم.

[2] transcendence basis

بنا به تعریف فوق واضح است که درجه تعالی یک توسیع L روی K صفر است اگروتنهاگر L یک توسیع جبری از K باشد.

در قضیه‌ی زیر اثبات می‌کنیم که درجه‌ی تعالی خوش تعریف است؛ یعنی اگر B_1 و B_2 دو پایه‌ی متعالی برای توسیع $K \subseteq L$ باشند، $|B_1| = |B_2|$.

قضیه ۱۳.۳.۱. توسیع میدانی $K \subseteq L$ را در نظر بگیرید. فرض کنید $\alpha_1, ..., \alpha_n$ و $\beta_1, ..., \beta_m$ دو پایه‌ی متعالی برای توسیع L روی K باشند. در این‌صورت $m = n$.

اثبات. به جهت سادگی در بیان و بهتر منتقل شدن ایده‌ی اثبات، این اثبات را برای حالتی که $n = 3$ شرح می‌دهیم. برای n دلخواه اثبات به صورت مشابه است.

فرض می‌کنیم $\alpha_1, \alpha_2, \alpha_3$ یک پایه‌ی متعالی برای توسیع L روی K است. باید نشان دهیم که اندازه‌ی هر پایه‌ی متعالی دیگر برای توسیع L روی K برابر است با ۳؛ بنابراین فرض می‌کنیم $\beta_1, \dots, \beta_m$ یک پایه‌ی متعالی برای توسیع L روی K باشد، اثبات می‌کنیم که $m = 3$.

از این‌که $\alpha_1, \alpha_2, \alpha_3$ و $\beta_1, \dots, \beta_m$ دو پایه‌ی متعالی برای توسیع L روی K هستند، به ترتیب نتیجه می‌شود که توسیع $K(\alpha_1, \alpha_2, \alpha_3) \subseteq L$ و توسیع $K(\beta_1, \dots, \beta_m) \subseteq L$ جبری هستند. بنابراین عنصر β_1 روی $K(\alpha_1, \alpha_2, \alpha_3)$ جبری است، یعنی یک چندجمله‌ای f با ضرایب در K موجود است 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_i ها در f ظاهر می‌شود. فرض کنید α_1 در f ظاهر شده است، پس به سادگی می‌توان دید که $\alpha_1 \in K(\alpha_2, \alpha_3, \beta_1)^{alg}$ و به طور خاص داریم $K(\alpha_1, \alpha_2, \alpha_3) \subseteq K(\alpha_2, \alpha_3, \beta_1)^{alg}$.

به طور مشابه β_2 روی $K(\alpha_1, \alpha_2, \alpha_3)$ جبری است و $K(\alpha_1, \alpha_2, \alpha_3) \subseteq (K(\alpha_2, \alpha_3, \beta_1))^{alg}$ در نتیجه β_2 روی $(K(\alpha_2, \alpha_3, \beta_1))^{alg}$ جبری است، یعنی β_2 روی $K(\alpha_2, \alpha_3, \beta_1)$ جبری است. بنابراین یک چندجمله‌ای مانند f پیدا می‌شود که $f(\alpha_2, \alpha_3, \beta_1, \beta_2) = 0$ و چندجمله‌ای f حتما شامل یکی از α_i ها است (زیرا در غیر این صورت β_1 و β_2 وابسته‌ی جبری می‌شوند). فرض کنید α_2 در چندجمله‌ای یاد شده باشد. بنابراین $\alpha_2 \in (K(\alpha_3, \beta_1, \beta_2))^{alg}$. دقت کنید که $K(\alpha_1, \alpha_2, \alpha_3) \subseteq (K(\alpha_3, \beta_1, \beta_2))^{alg}$. همچنین β_3 روی $K(\alpha_1, \alpha_2, \alpha_3)$ جبری است. از این رو β_3 روی $(K(\alpha_3, \beta_1, \beta_2))^{alg}$ جبری است. به طور مشابه داریم $\alpha_3 \in (K(\beta_1, \beta_2, \beta_3))^{alg}$ و $K(\alpha_1, \alpha_2, \alpha_3) \subseteq (K(\beta_1, \beta_2, \beta_3))^{alg}$. در نتیجه $\alpha_1, \alpha_2, \alpha_3 \in (K(\beta_1, \beta_2, \beta_3))^{alg}$ پس $K(\alpha_1, \alpha_2, \alpha_3)^{alg} \subseteq K(\beta_1, \beta_2, \beta_3)^{alg}$. از طرفی $L \subseteq (K(\alpha_1, \alpha_2, \alpha_3))^{alg}$. بنابراین $L \subseteq (K(\beta_1, \beta_2, \beta_3))^{alg}$، پس $\beta_1, \beta_2, \beta_3$ پایه‌ی متعالی برای توسیع L روی K است. یعنی $m = 3$.

توجه کنید که m نمی‌تواند کمتر از ۳ باشد، زیرا اگر β_1, β_2 یک پایه‌ی متعالی برای توسیع L روی K باشد، با روندی مشابه روند فوق، اثبات می‌شود که α_1, α_2 یک پایه‌ی متعالی برای توسیع L روی K است که با فرض

پایه‌ی متعالی بودن $\alpha_۱, \alpha_۲, \alpha_۳$ در تناقض است. □

تا اینجا مفهوم مستقل خطی را یادآوری و مفهوم مستقل جبری را معرفی کردیم. همچنین دیدیم که یک توسیع میدانی را می‌توانیم به عنوان یک فضای برداری یا یک میدان مورد بررسی قرار دهیم.

فرض کنید L و K دو توسیع میدانی از یک میدان F باشند. همچنین فرض کنید همه‌ی میدان‌های مورد بحث در ادامه‌ی این زیربخش، زیر میدانی از یک میدان Ω باشند. در ادامه دو مفهوم میدان‌های مجزای خطی و مجزای جبری را معرفی می‌کنیم و در پایان این زیربخش، ارتباط بین این دو مفهوم را بیان می‌کنیم.

تعریف ۱۴.۳.۱ (مجزای خطی)**.** توسیع‌های میدانی $F \subseteq K, L$ را در نظر بگیرید. می‌گوییم میدان‌های L و K روی F مجزای خطی هستند هرگاه هر زیرمجموعه‌ی متناهی از L که روی F مستقل خطی است، روی K نیز مستقل خطی باشد.

گزاره ۱۵.۳.۱. توسیع‌های میدانی $F \subseteq K, L$ را در نظر بگیرید. اگر میدان‌های L و K روی F مجزای خطی باشند، آنگاه $L \cap K = F$.

قضیه ۱۶.۳.۱. فرض کنید $F \subseteq E \subseteq L$ و $F \subseteq K$. همچنین فرض کنید KE یک میدان مرکب باشد (اشتراک همه‌ی زیرمیدان‌هایی از Ω که شامل K و E هستند). در این صورت K و L روی F مجزای خطی هستند اگروتنهااگر K و E روی F، KE و L روی E مجزای خطی باشند.

اثبات. فرض می‌کنیم K و E روی F، KE و L روی E مجزای خطی باشند. همچنین فرض می‌کنیم κ پایه‌ای برای K به عنوان یک فضای برداری روی F باشد و α و λ به ترتیب پایه‌های E روی F و L روی E باشند. در این صورت مشابه اثبات لم ۶.۲.۱ می‌توان دید که $\lambda\alpha$ یک پایه برای L روی F است. به برهان خلف فرض می‌کنیم K و L روی F مجزای خطی نباشند. بنابراین برای ترکیب خطی $\sum_{\lambda,\alpha}(\sum_{\kappa} c_{\kappa,\alpha\lambda}\kappa)\lambda\alpha$ که در آن $c_{\kappa,\alpha\lambda}$ متعلق به F و ناصفر هستند داریم :

$$\sum_{\lambda,\alpha}(\sum_{\kappa} c_{\kappa,\alpha\lambda}\kappa)\lambda\alpha = ۰.$$

در نتیجه $\sum_{\lambda}(\sum_{\kappa,\alpha} c_{\kappa,\alpha\kappa}\kappa\alpha)\lambda = ۰$. از آنجا که λ پایه‌ی L روی E است، هر ترکیب خطی از λ با ضرایب در E ناصفر است. اما یک ترکیب خطی از λ با ضرایب در KE صفر شده است. بنابراین KE و L روی E وابسته‌ی خطی خواهند بود که تناقض است.

برای اثبات جهت عکس قضیه فرض می‌کنیم L و K روی F مجزای خطی هستند. بنابراین واضح است که E و K نیز روی F مجزای خطی هستند. توجه کنید که KE میدان کسرهای حلقه‌ی $E[K]$ است. این حلقه یک فضای برداری روی E است و یک پایه برای K روی F یک پایه برای $E[K]$ روی E است. بنابراین

کافی است نشان دهیم عناصر یک پایه برای K روی F، روی L مستقل خطی باقی می‌مانند. ازآنجا که L و K روی F مجزای خطی هستند بوضوح یک پایه برای K روی F، روی L نیز مستقل خطی است. □

تعریف ۱۷.۳.۱ (مجزای جبری). فرض کنید L و K دو توسیع میدانی از میدان F باشند. می‌گوییم L و K روی F مجزای جبری هستند هرگاه اگر $\alpha_1, \ldots, \alpha_n \in L - F$ روی F مستقل جبری باشند، آنگاه $\alpha_1, \ldots, \alpha_n$ روی K نیز مستقل جبری باشند.

در لم زیر اثبات می‌کنیم که مجزای خطی بودن شرط قوی‌تری از مجزای جبری بودن است. به بیان دیگر مجزای جبری بودن از مجزای خطی بودن نتیجه می شود.

لم ۱۸.۳.۱. فرض کنید L و K دو توسیع میدانی از میدان F باشند. اگر L و K روی F مجزای خطی باشند، آنگاه L و K روی F مجزای جبری هستند.

اثبات. فرض می‌کنیم L و K دو میدان مجزای خطی روی زیر میدان مشترک F باشند. می خواهیم نشان دهیم که L و K روی F مجزای جبری نیز هستند. فرض می‌کنیم عناصر $\alpha_1, \ldots, \alpha_n \in L$ روی K مستقل جبری باشند، باید نشان دهیم $\alpha_1, \ldots, \alpha_n \in L$ روی F مستقل جبری هستند. از آنجا که $\alpha_1, \ldots, \alpha_n \in L$ روی K مستقل جبری هستند، هر ترکیب جبری آن‌ها ناصفر است. بنابراین توان‌های $\alpha_1, \ldots, \alpha_n$ روی F مستقل خطی هستند. (به طور کلی $\alpha_1, \ldots, \alpha_n$ روی F مستقل جبری هستند اگروتنهااگر توان‌های $\alpha_1, \ldots, \alpha_n$ روی F مستقل خطی باشند). از طرفی طبق فرض L و K روی F مجزای خطی هستند. بنابراین واضح است که توان‌های $\alpha_1, \ldots, \alpha_n$ روی K مستقل خطی هستند. در نتیجه $\alpha_1, \ldots, \alpha_n$ روی K مستقل جبری هستند، پس L و K روی F مجزای جبری هستند. □

عکس لم فوق همواره برقرار نیست، مگر آنکه L یک توسیع منتظم از K باشد (به لم ۴۳.۳.۱ مراجعه کنید).

جدایی‌پذیر جبری و قضیه‌ی عنصر اولیه

تعریف ۱۹.۳.۱ (چندجمله‌ای جدایی‌پذیر). چندجمله‌ای $f \in K[X]$ را جدایی‌پذیر روی K می‌نامیم هرگاه f در میدان شکافنده‌ی f روی K به عوامل درجه اول متمایز تجزیه شود؛ به بیان دیگر $f \in K[X]$ را جدایی‌پذیر می‌نامیم هرگاه در میدان شکافنده‌ی f ریشه‌ی تکراری نداشته باشد.

تعریف ۲۰.۳.۱ (عنصر جدایی‌پذیر). توسیع میدانی $K \subseteq L$ را در نظر بگیرید. عنصر جبری $\alpha \in L$ را جدایی‌پذیر می‌نامیم هرگاه چندجمله‌ای مینیمال α ریشه‌ی تکراری نداشته باشد.

تعریف ۲۱.۳.۱ (توسیع جدایی‌پذیر جبری)**.** توسیع جبری $K \subseteq L$ را یک توسیع جدایی‌پذیر [۳] جبری می‌نامیم هرگاه هر عنصر $\alpha \in L$ ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر و جدایی‌پذیر روی K باشد؛ به بیان دیگر چندجمله‌ای مینیمال آن دارای ریشه‌ی تکراری نباشد.

در زیربخش بعدی یک تعریف کلی برای توسیع جدایی‌پذیر ارائه خواهیم کرد که به جبری بودن توسیع وابسته نیست، اما در این زیربخش منظور از توسیع جدایی‌پذیر همان توسیع جدایی‌پذیر جبری است. زمانی که تعریف کلی را بیان کردیم هر کجا تاکیدی بر جبری بودن توسیع باشد از واژه‌ی توسیع جدایی‌پذیر جبری استفاده می‌کنیم.

لم زیر محکی برای تشخیص چندجمله‌ای جدایی‌پذیر است.

لم ۲۲.۳.۱. میدان K و چندجمله‌ای $f \in K[X]$ را در نظر بگیرید. عنصر a در میدان شکافنده‌ی f یک ریشه‌ی مضاعف برای f است اگروتنهااگر a یک ریشه برای f' باشد.

اثبات. به طور کلی فرض می‌کنیم a یک ریشه‌ی تکراری برای f با مرتبه‌ی تکرار d باشد. در این صورت در میدان شکافنده‌ی f داریم $f = (X-a)^d g(X)$ و بوضوح $f(a) = 0$. از طرفی

$$f'(X) = d(X-a)^{d-1} g(X) + g'(X)(X-a)^d.$$

بنابراین $f'(a) = 0$. در نتیجه به طور خاص اگر a یک ریشه‌ی مضاعف برای f باشد داریم $f'(a) = 0$.

برای اثبات جهت عکس فرض می‌کنیم عنصر a متعلق به میدان شکافنده‌ی f باشد و $f'(a) = 0$. از آنجا که a ریشه‌ی چندجمله‌ای f است، در میدان شکافنده‌ی f داریم $f = (X-a)g(X)$. در نتیجه $f' = g(X) + g'(X)(X-a)$. از طرفی $f'(a) = 0$، پس واضح است که $g(a) = 0$. از این رو $g(a) = (X-a)h$. در نتیجه $f = (X-a)^2 h$، به بیان دیگر f شامل عامل $(X-a)^2$ است؛ یعنی a یک ریشه‌ی مضاعف برای f است. □

بنا به لم فوق چندجمله‌ای $f \in K[X]$ غیر جدایی‌پذیر است اگروتنهااگر f و f' در میدان شکافنده‌ی f روی K ریشه‌ی مشترک داشته باشند. در نتیجه چندجمله‌ای $f \in K[X]$ جدایی‌پذیر است اگروتنهااگر f و f' در میدان شکافنده‌ی f روی K ریشه‌ی مشترک نداشته باشند.

در لم زیر نشان می‌دهیم که اگر مشخصه‌ی میدان K صفر باشد، هر چندجمله‌ای تحویل‌ناپذیر $f \in K[X]$ جدایی‌پذیر است.

لم ۲۳.۳.۱. فرض کنید K یک میدان با مشخصه‌ی صفر و $f \in K[X]$ یک چندجمله‌ای تحویل‌ناپذیر باشد. در این صورت f در میدان شکافنده‌ی f ریشه‌ی تکراری ندارد.

[3] separable extension

اثبات. به برهان خلف فرض می‌کنیم $a \in L$ یک ریشه‌ی تکراری برای چندجمله‌ای تحویل‌ناپذیر f باشد. در این صورت بنا به لم ۲۲.۳.۱ چندجمله‌ای‌های f و f' دارای ریشه‌ی مشترک a هستند؛ یعنی $f(a) = ۰$ و $f'(a) = ۰$. از طرفی f تحویل‌ناپذیر است، پس طبق لم ۲.۲.۱ چندجمله‌ای مینیمال a است. از آنجا که مشخصه‌ی میدان صفر است داریم $\deg(f') < \deg(f)$؛ از طرفی $f'(a) = ۰$ که با مینیمال بودن چندجمله‌ای f در تناقض است. بنابراین اگر مشخصه‌ی میدان K صفر باشد، هر چندجمله‌ای تحویل‌ناپذیر $f \in K[X]$ جدایی‌پذیر است. □

نتیجه ۲۴.۳.۱. اگر مشخصه‌ی میدان K صفر باشد، هر توسیع جبری روی K جدایی‌پذیر است.

توجه ۲۵.۳.۱. به سادگی می‌توان دید که اگر $f \in K[X]$ یک چندجمله‌ای تحویل‌ناپذیر باشد، برای هر $g \in K[X]$ داریم $\gcd(f,g) = ۱$ یا $\gcd(f,g) = f$.

توجه ۲۶.۳.۱. فرض کنید L روی K یک توسیع میدانی باشد. همچنین فرض کنید $f, g \in K[X]$ دو چندجمله‌ای ناصفر باشند. در این صورت $\gcd(f,g)$ روی L با $\gcd(f,g)$ روی K برابر است. زیرا بنا به الگوریتم تقسیم داریم $\gcd(f,g) = mf + ng$. بنابراین اگر $\gcd(f,g)$ در K برابر با h باشد، داریم $h \mid f$ و $h \mid g$ در نتیجه $f = f_۱h$ و $g = g_۱h$. حال با جایگذاری در $\gcd(f,g) = mf + ng$ داریم $\gcd(f,g) = mf_۱h + ng_۱h$ از این رو $h \mid \gcd(f,g)$.

لم ۲۷.۳.۱. میدان K را در نظر بگیرید. چندجمله‌ای تحویل‌ناپذیر $f \in K[X]$، جدایی‌پذیر است اگروتنهااگر $\gcd(f,f') = ۱$.

اثبات. از آنجا که $\gcd(f,g)$ روی میدان شکافنده، با $\gcd(f,g)$ روی K برابر است می‌توانیم به جای میدان K میدان شکافنده‌ی f را در نظر بگیریم. فرض می‌کنیم L میدان شکافنده‌ی f باشد. در این صورت $f = \prod(X - r_i)$ به طوری که $r_i \in L$. می‌خواهیم نشان دهیم r_i ها تکراری نیستند اگروتنهااگر $\gcd(f,f') = ۱$. ابتدا فرض می‌کنیم r_i ها تکراری نیستند و به برهان خلف فرض می‌کنیم $\gcd(f,f') \neq ۱$. در این صورت چندجمله‌ای تحویل‌ناپذیر $(X - r_{i_۰})$ موجود است به طوری که $(X - r_{i_۰}) \mid f$ و $(X - r_{i_۰}) \mid f'$. به بیان دیگر چندجمله‌ای‌های h و g موجود هستند به طوری که $f = (X - r_{i_۰})h$ و $f' = (X - r_{i_۰})g$. بنابراین واضح است که $f'(r_{i_۰}) = ۰$. ادعا می‌کنیم که $r_{i_۰}$ یک ریشه‌ی مضاعف برای f است.

بدون کاستن از کلیت فرض می‌کنیم $r_{i_۰} = r_۱$. بنابراین $f = (X - r_۱)h$ به طوری که $h = \prod_{i>۱}(X - r_i)$. در نتیجه $f' = h + h'(X - r_۱)$. از طرفی $f'(r_۱) = ۰$، پس $h(r_۱) = ۰$. از این رو برای یک $i > ۱$ داریم $r_۱ - r_i = ۰$؛ یعنی برای یک $i > ۱$ داریم $r_۱ = r_i = ۰$. در نتیجه $r_۱$ یک ریشه‌ی مضاعف برای f است.

حال برای اثبات جهت عکس، فرض می‌کنیم $\gcd(f,f') = ۱$. می‌خواهیم نشان دهیم f ریشه‌ی تکراری ندارد. بدین منظور به برهان خلف فرض می‌کنیم r یک ریشه‌ی تکراری با مرتبه‌ی تکرار d باشد. در این صورت

$f = (X-r)^d g$. بنابراین $f' = d(X-r)^{d-1}g + g'(X-r)^d$. از این رو بوضوح $(X-r)^{d-1} \mid f$ و $(X-r)^{d-1} \mid f'$ که این با $\gcd(f,f') = 1$ در تناقض است.

□

نتیجه ۲۸.۳.۱. فرض کنید $f(X)$ یک چندجمله‌ای تحویل‌ناپذیر روی K باشد. در این صورت $f(X)$ جدایی‌پذیر است اگروتنهااگر $f'(X) \not\equiv 0$.

اثبات. فرض می‌کنیم $f(X)$ جدایی‌پذیر باشد. بنا به لم ۲۷.۳.۱ داریم $\gcd(f,f') = 1$. حال به برهان خلف فرض می‌کنیم $f'(X) = 0$. در این صورت $\gcd(f,f') = f$ که تناقض است. برای اثبات جهت عکس، فرض می‌کنیم $f'(X) \neq 0$. قرار می‌دهیم $d = \gcd(f,f')$. بنابراین $d \mid f'$ و $d \mid f$. از طرفی $f(X)$ تحویل‌ناپذیر است، پس $d = f(X)$ یا $d = 1$. واضح است که $\deg d \leq \deg f' < \deg f$. از این رو d نمی‌تواند برابر با $f(X)$ باشد؛ یعنی $d \neq f(X)$. بنابراین $d = 1$. در نتیجه $\gcd(f,f') = 1$، پس بنا به لم ۲۷.۳.۱ چندجمله‌ای $f(X)$ روی K جدایی‌پذیر است. □

به طور خلاصه، دیدیم که یک چندجمله‌ای $f \in K[X]$ جدایی‌پذیر است اگروتنهااگر f و f' در میدان شکافنده‌ی f ریشه‌ی مشترک نداشته باشند. همچنین رابطه‌ی تحویل‌ناپذیری و جدایی‌پذیری را مورد بررسی قرار دادیم. دیدیم که اگر چندجمله‌ای $f \in K[X]$ یک چندجمله‌ای تحویل‌ناپذیر و مشخصه‌ی میدان K صفر باشد، آنگاه f جدایی‌پذیر است و به طور کلی چندجمله‌ای تحویل‌ناپذیر $f \in K[X]$ جدایی‌پذیر است، اگروتنهااگر $\gcd(f,f') = 1$ اگروتنهااگر $f'(X) \not\equiv 0$.

در ادامه اثبات خواهیم کرد که هر توسیع جدایی‌پذیر متناهی از یک میدان نامتناهی ساده است؛ یعنی اگر توسیع L روی K یک توسیع جدایی‌پذیر متناهی باشد، عنصر $\theta \in L$ موجود است به طوری که $L = K(\theta)$.

قضیه ۲۹.۳.۱. فرض کنید K یک میدان نامتناهی و $K \subseteq F$ یک توسیع میدانی باشد. اگر $\alpha \in F$ یک عنصر جبری و $\beta \in F$ یک عنصر جدایی‌پذیر روی K باشند، آنگاه $K \subseteq K(\alpha,\beta)$ یک توسیع ساده است.

اثبات. فرض می‌کنیم $p(X) \in K[X]$ چندجمله‌ای مینیمال α و $q(X) \in K[X]$ چندجمله‌ای مینیمال β باشند. قرار می‌دهیم $f = p(X)q(X)$ و فرض می‌کنیم S میدان شکافنده‌ی چندجمله‌ای f روی K باشد. بنابراین $\alpha, \beta \in S$. فرض می‌کنیم $\alpha_1, \ldots, \alpha_m$ و $\beta_1, \ldots, \beta_n$ به ترتیب ریشه‌های $p(X)$ و $q(X)$ در S باشند. همچنین فرض می‌کنیم $\alpha_1 = \alpha$ و $\beta_1 = \beta$. از آنجا که β روی K جدایی‌پذیر است $\beta_1 = \beta, \ldots, \beta_n$ از یکدیگر متمایزند. عنصر a متعلق به K را به صورت زیر در نظر می‌گیریم:

$$a \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}, 1 \leq i \leq m, 2 \leq j \leq n.$$

توجه کنید که با توجه به نامتناهی بودن میدان K، عنصر a با شرایط خواسته شده موجود است. بنابراین $a\beta - a\beta_j + \alpha \neq \alpha_i$. برای راحتی در نمایش $a\beta + \alpha$ را با c نمایش می‌دهیم.

ادعا می‌کنیم که $K(\alpha, \beta) = K(c)$. به منظور اثبات این ادعا ابتدا توجه کنید که برای هر $1 \leq i \leq m$ و $2 \leq j \leq n$ داریم $c - a\beta_j \neq \alpha_i$. حال قرار می‌دهیم $h(X) = p(c - aX) \in K(c)[X]$. در این صورت $h(\beta) = p(\alpha) = 0$ و $h(\beta_j) = p(c - a\beta_j) \neq 0$ برای هر $j = 2, 3, \ldots, n$. در نتیجه تنها ریشه‌ی مشترک $h(X)$ و $q(X)$ در S عنصر β است. فرض می‌کنیم $m(X)$ چندجمله‌ای مینیمال β روی $K(c)$ باشد. در این صورت $m(X) \mid h(X)$. همچنین با در نظر گرفتن $q(X)$ به عنوان یک چندجمله‌ای روی $K(c)$ داریم $m(X) \mid q(X)$. بنابراین از آنجا که تنها ریشه‌ی مشترک $h(X)$ و $q(X)$ در S عنصر β است، داریم $m(X) = X - \beta$. در نتیجه $\beta \in K(c)$ و $\alpha = c - a\beta \in K(c)$، پس واضح است که $K(\alpha, \beta) \subseteq K(c)$. از طرفی با توجه به این‌که $c = a\beta + \alpha$ داریم $K(c) \subseteq K(\alpha, \beta)$. بنابراین $K(\alpha, \beta) = K(c)$؛ یعنی توسیع $K \subseteq K(\alpha, \beta)$ یک توسیع ساده است. □

قضیه ۳۰.۳.۱ (عنصر اولیه [۴]). هر توسیع جدایی‌پذیر متناهی از یک میدان نامتناهی، ساده است.

اثبات. فرض می‌کنیم K یک میدان نامتناهی و $K \subseteq F$ یک توسیع جدایی‌پذیر از درجه‌ی n باشد. بنابراین عناصر $c_1, \ldots, c_n \in F$ موجود هستند به طوری که $F = K(c_1, \ldots, c_n)$ و $c_1, \ldots, c_n$ روی K جدایی‌پذیر هستند. به کمک استقرا روی n اثبات می‌کنیم که توسیع $K \subseteq F$ یک توسیع ساده است. برای $n = 1$ داریم $F = K(c_1)$ و بوضوح حکم برقرار است. حال فرض می‌کنیم، فرض استقرا برای $n - 1$ برقرار باشد؛ یعنی $K(c_1, \ldots, c_{n-1}) = K(c')$ به طوری که $c' \in F$. باید نشان دهیم $d \in F$ موجود است به طوری که $K(c_1, \ldots, c_n) = K(d)$. توجه کنید که

$$K(c_1, \cdots, c_n) = K(c_1, \cdots, c_{n-1})(c_n) = K(c')(c_n) = K(c', c_n).$$

از طرفی c' روی K جبری و c_n روی K جدایی‌پذیر است، پس بنا به قضیه‌ی ۲۹.۳.۱ عنصر $d \in F$ موجود است به طوری که $K(c', c_n) = K(d)$. در نتیجه $K(c_1, \cdots, c_n)$ یک توسیع ساده از K است. □

در بخش‌های بعدی (با یک اثبات متفاوت) خواهیم دید که هر توسیع جدایی‌پذیر متناهی از یک میدان متناهی نیز ساده است.

جدایی‌پذیری

در زیربخش قبلی یک تعریف از توسیع جدایی‌پذیر برای حالتی که توسیع ما یک توسیع جبری است بیان کردیم. حال قصد داریم یک تعریف کلی برای توسیع جدایی‌پذیر ارائه کنیم که به جبری بودن توسیع وابسته نباشد.

[4] primitive element theorem

در ادامه‌ی این زیربخش، هرگاه تعریف قبلی مورد نظر باشد، از واژه‌ی توسیع جدایی‌پذیر جبری استفاده می‌کنیم و در حالت کلی زمانی که تاکیدی بر جبری بودن توسیع نداریم، واژه‌ی توسیع جدایی‌پذیر را به کار می‌بریم.

میدان K با مشخصه‌ی p را در نظر بگیرید. فرض کنید $K^p = \{a^p : a \in K\} \subseteq K$ و نگاشت $\varphi : K \to K$ به صورت $\varphi : a \to a^p$ باشد. از آنجا که مشخصه‌ی میدان، p است به سادگی می‌توان دید که برای هر $a, b \in K$ داریم $(a+b)^p = a^p + b^p$ و $(a \cdot b)^p = a^p \cdot b^p$. در نتیجه این نگاشت یک همریختی است (به لم ۲.۴.۱ رجوع کنید). همچنین به سادگی می‌توان دید که این نگاشت یک به یک است. از طرفی $\mathrm{Im}(\varphi) = K^p$، در نتیجه نگاشت φ پوشا است اگروتنهاگر $K = K^p$.

اگر $K = K^p$، در این صورت به کمک استقرا می‌توانیم نشان دهیم که برای هر $m \geq 0$ داریم $K = K^{p^m}$. همچنین با توجه به این‌که مشخصه‌ی میدان K عدد p است، برای هر $m \geq 0$ و هر $b \in \tilde{K}$ داریم $(X-b)^{p^m} = X^{p^m} - b^{p^m}$.

عنصر $a \in K$ را در نظر بگیرید. بنا به پوشا بودن نگاشت φ روی $\tilde{K}$، عنصر $b \in \tilde{K}$ موجود است به طوری که $a = b^{p^m}$؛ ادعا می‌کنیم که این عنصر یکتاست. به بیان دیگر برای هر $a \in K$ فقط یک عنصر $b \in \tilde{K}$ موجود است به طوری که $a = b^{p^m}$. واضح است که چندجمله‌ای مینیمال b به صورت $X^{p^m} - a$ و تنها ریشه‌ی این چندجمله‌ای عنصر b است. از این رو برای هر $a \in K$ یک عنصر یکتای $b \in \tilde{K}$ موجود است به طوری که p^m امین ریشه‌ی عنصر a است. عنصر b را می‌توانیم به صورت a^{1/p^m} در نظر بگیریم.

فرض کنید m یک عدد مشخص باشد. میدان متشکل از ریشه‌ی p^m ام عناصر K را با K^{1/p^m} نمایش می‌دهیم؛ به بیان دیگر $K^{1/p^m} = \{a^{1/p^m} : a \in K\}$. همچنین کوچکترین توسیع جبری از میدان K که φ روی آن پوشا است را با K^{1/p^∞} نمایش می‌دهیم، این میدان از همه‌ی عناصری از $\tilde{K}$ تشکیل شده است که ریشه‌ی p^m ام یک عنصر در K هستند. در واقع K^{1/p^∞} اجتماع میدان‌های K^{1/p^m} برای $m = 2, 3, \ldots$ است.

لم ۳۱.۳.۱. دو میدان F و K و نشاندن $\sigma : K \to F$ را در نظر بگیرید. اگر $K \subseteq E \subseteq K^{1/p^\infty}$. آنگاه یک نشاندن یکتا $E \to F^{1/p^\infty}$ موجود است.

اثبات. عنصر دلخواه $b \in E \subseteq K^{1/p^\infty}$ را در نظر می‌گیریم. برای هر $b \in K^{1/p^\infty}$ عدد طبیعی m و عنصر $a \in K$ موجود است به طوری که $b = a^{1/p^m}$، یعنی $a = b^{p^m} \in K$. بنابراین نشاندن یکتای $\sigma_1 : E \to F^{1/p^\infty}$ با ضابطه‌ی $\sigma_1 b = (\sigma a)^{1/p^m}$ موجود است.

□

نتیجه ۳۲.۳.۱. میدان K و نشاندن $\sigma : K \to \tilde{K}$ را در نظر بگیرید. اگر $K \subseteq E \subseteq K^{1/p^\infty}$. آنگاه تنها نشاندن $E \to \tilde{K}^{1/p^\infty} = \tilde{K}$ که K را به خودش می‌برد، نگاشت همانی است.

تعریف ۳۳.۳.۱. توسیع $K \subseteq E$ را کاملاً غیر جدایی‌پذیر [۵] می‌نامیم هرگاه E یک توسیع جبری از K باشد و تنها نشاندن موجود از E به $\tilde{K}$ که K را به خودش می‌برد نگاشت همانی باشد.

بنا به تعریف فوق، هر توسیع $K \subseteq E$ کاملاً غیر جدایی‌پذیر است اگروتنهااگر $E \subseteq K^{1/p^\infty}$.

توجه ۳۴.۳.۱. میدان K را با مشخصه‌ی p در نظر بگیرید. فرض کنید $f \in K[X]$ یک چندجمله‌ای تحویل‌ناپذیر روی K با ضرایب $c_i \in K$ باشد. همچنین فرض کنید $m \geq 0$ بزرگترین عدد صحیحی باشد که برای هر $c_i \neq 0$ داریم $p^m \mid i$. یعنی m بزرگترین عدد صحیحی باشد که برای هر $c_i \neq 0$ داریم $i = jp^m$. در این صورت چندجمله‌ای $g = \sum_j d_j X^j$ متعلق به $K^{1/p^m}[X]$ موجود است به طوری که برای هر $i = jp^m$ داریم $c_i = d_l^{p^m}$ و $f = g^{p^m}$.

از این‌که f تحویل‌ناپذیر است به سادگی نتیجه می‌شود که چندجمله‌ای g تحویل‌ناپذیر است. همچنین با توجه به نحوه‌ی انتخاب m ضرایب $d_j \neq 0$ موجود هستند به طوری که j بر p بخش پذیر نیست. در نتیجه $g' = \sum_j j d_j X^{j-1} \neq 0$، پس بنا به نتیجه‌ی ۲۸.۳.۱ چندجمله‌ای g جدایی‌پذیر است. حال فرض کنید $a_1, \ldots, a_n$ ریشه‌های g در بستار جبری K باشند. در این صورت $a_1, \ldots, a_n$ از یکدیگر متمایزند، پس $f = g^{p^m} = \prod_{i=1}^{n} (X - a_i)^{p^m}$. بنابراین f جدایی‌پذیر است اگروتنهااگر $m = 0$.

تعریف ۳۵.۳.۱. فرض کنید $F \subseteq K$ یک توسیع متناهیاً تولید شده باشد. می‌گوییم K روی F به صورت جدایی‌پذیر تولید شده است، هرگاه یک پایه‌ی متعالی $t_1, \ldots, t_r$ برای توسیع $F \subseteq K$ موجود باشد به طوری که K روی $F(t_1, \cdots, t_r)$ جدایی‌پذیر جبری باشد.

قضیه ۳۶.۳.۱. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. شروط زیر معادل هستند:

۱. L و K^{1/p^∞} روی K مجزای خطی باشند.

۲. L و $K^{1/p}$ روی K مجزای خطی باشند.

۳. برای یک عدد طبیعی m، میدان L و K^{1/p^m} روی K مجزای خطی باشند.

۴. هر زیر میدان متناهیاً تولید شده‌ی $K \subseteq E \subseteq L$ جدایی‌پذیر تولید شده باشد.

اثبات. برای دیدن اثبات این قضیه، به منبع [۱۶، صفحه‌ی ۳۷۸، گزاره‌ی ۱.۴]، یا منبع [۹، لم ۱.۶.۲] مراجعه کنید. □

تعریف ۳۷.۳.۱. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. این توسیع را جدایی‌پذیر می‌نامیم هرگاه یکی از شروط قضیه‌ی ۳۶.۳.۱ برقرار باشد.

[5] purely inseparable

بنا به تعریف فوق توسیع $K \subseteq L$ جدایی‌پذیر است هرگاه L از بخش غیر جدایی‌پذیر K مجزای خطی باشد.
در زیربخش قبلی گفتیم که توسیع جبری $K \subseteq L$ را یک توسیع جدایی‌پذیر جبری می‌نامیم هرگاه هر عنصر $\alpha \in L - K$ ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر و جدایی‌پذیر روی K باشد. در این زیربخش به عنوان یک تعریف کلی‌تر گفتیم که توسیع میدانی $K \subseteq L$ جدایی‌پذیر است، هرگاه L و K^{1/p^∞} روی K مجزای خطی باشند. در ادامه نشان می‌دهیم که اگر توسیع $K \subseteq L$ یک توسیع جبری باشد، تعاریف فوق معادل هستند.

لم ۳۸.۳.۱. توسیع میدانی $F \subseteq K$ را در نظر بگیرید و فرض کنید F در K بسته‌ی جبری است؛ یعنی هر عنصر از K که روی F جبری است، متعلق به F است. همچنین فرض کنید x متعلق به یک توسیع از K و روی F جبری باشد. در این صورت $F(x)$ و K روی F مجزای خطی هستند و $[F(x) : F] = [K(x) : K]$.

اثبات. فرض می‌کنیم $f(X) \in F[X]$ چندجمله‌ای مینیمال x باشد. در این صورت $f(X) \in F[X]$ یک چندجمله‌ای تحویل‌ناپذیر است. ادعا می‌کنیم $f(X)$ روی K نیز تحویل‌ناپذیر است. به جهت اثبات این ادعا به برهان خلف فرض می‌کنیم $f(X)$ روی K تحویل‌پذیر باشد. در این صورت $f = gh$ به طوری که $g, h \in K(X)$. از طرفی ضرایب g و h روی F جبری هستند. در نتیجه ضرایب g و h متعلق به F هستند که این با تحویل‌ناپذیر بودن f روی F در تناقض است. بنابراین توان‌هایی از x تشکیل پایه برای $F(x)$ روی F می‌دهند و دقیقاً همین عناصر یک پایه برای $K(x)$ روی K هستند.

□

قضیه ۳۹.۳.۱. توسیع جبری $K \subseteq L$ را در نظر بگیرید. توسیع $K \subseteq L$ جدایی‌پذیر جبری است اگروتنهااگر L و K^{1/p^∞} روی K مجزای خطی باشند.

اثبات. فرض می‌کنیم $K \subseteq L$ یک توسیع جبری باشد و L و K^{1/p^∞} روی K مجزای خطی باشند. همچنین به برهان خلف فرض می‌کنیم $K \subseteq L$ جدایی‌پذیر جبری نباشد. در این صورت عنصر $a \in L$ با چندجمله‌ای مینیمال $f \in K[X]$ موجود است به طوری که f روی K جدایی‌پذیر نیست. چندجمله‌ای $g \in K^{1/p^m}[X]$ به طوری که $f = g^{p^m}$ را در نظر می‌گیریم. از آنجا که f روی K جدایی‌پذیر نیست داریم $m \neq 0$. در نتیجه درجه‌ی چندجمله‌ای g از درجه‌ی چندجمله‌ای f کمتر است. فرض می‌کنیم درجه‌ی چندجمله‌ای f، t است و چندجمله‌ای g از درجه‌ی $s < t$ است. در این صورت عناصر $1, a, a^2, \ldots, a^s, \ldots, a^{t-1} \in K(a)$ روی K مستقل خطی هستند. اما در $K^{1/p^m}(a)$ عناصر $1, a, a^2, \ldots, a^s$ تشکیل پایه می‌دهند و مستقل خطی هستند. بنابراین واضح است که $K(a)$ و K^{1/p^∞} روی K مجزای خطی نیستند و با این فرض که L و K^{1/p^∞} روی K مجزای خطی هستند در تناقض است.
برای اثبات جهت عکس قضیه عنصر جبری $b \in L$ را در نظر می‌گیریم و فرض می‌کنیم $K(b)$ روی K یک توسیع جدایی‌پذیر باشد. می‌دانیم که $[K(b) : K]$ تا نشاندن متفاوت از $K(b)$ به $\tilde{K}$ وجود دارد. (این نشاندن‌ها،

b را به ریشه‌های متفاوت چندجمله‌ای مینیمال b تصویر می‌کند و روی K همانی هستند). بنابراین این نشاندن‌ها را می‌توانیم به $[K(b) : K]$ تا نشاندن متفاوت از $K^{1/p^\infty}(b)$ به $\widetilde{K^{1/p^\infty}} = \tilde{K}$ توسیع دهیم. واضح است که این نشاندن‌ها روی K^{1/p^∞} همانی هستند. در نتیجه تعداد نشاندن‌های متفاوت از $K^{1/p^\infty}(b)$ به $\widetilde{K^{1/p^\infty}}$ با تعداد نشاندن‌های متفاوت از $K(b)$ به $\tilde{K}$ برابر است. بنابراین $[K(b) : K] = [K^{1/p^\infty}(b) : K^{1/p^\infty}]$. از این رو $K(b)$ و K^{1/p^∞} مجزای خطی هستند. در نتیجه L و K^{1/p^∞} مجزای خطی هستند. □

۴.۳.۱ توسیع منتظم

لم ۴۰.۳.۱. توسیع میدانی K روی F را در نظر بگیرید. عبارت‌های زیر معادل هستند:

۱. میدان K روی F جدایی‌پذیر و F در K بسته‌ی جبری است.

۲. K و $\tilde{F}$ روی F مجزای خطی هستند.

اثبات. اثبات ۲ به ۱: فرض می‌کنیم K و $\tilde{F}$ روی F مجزای خطی باشند. در این صورت بنا به گزاره‌ی ۱۵.۳.۱ داریم $K \cap \tilde{F} = F$، بنابراین بوضوح F در K بسته‌ی جبری است.

اثبات ۱ به ۲: بدون کاستن از کلیت فرض می‌کنیم K روی F متناهیاً تولید شده است. در این صورت کافی است نشان دهیم K از هر توسیع جبری متناهی از میدان F، مجزای خطی است. فرض می‌کنیم L یک توسیع جبری متناهی از میدان K است. اگر L روی F جدایی‌پذیر جبری باشد، بنا به قضیه‌ی ۳۰.۳.۱ میدان L توسط یک عنصر تولید شده است. در نتیجه بنا به لم ۳۸.۳.۱ میدان L و K مجزای خطی هستند.

به طور کلی فرض کنید $F \subseteq E$ بزرگترین زیر میدان جدایی‌پذیر از L باشد. بنا به قضیه‌ی ۱۶.۳.۱ کافی است نشان دهیم KE و L روی E مجزای خطی هستند. فرض کنید $t_1, \dots, t_r$ یک پایه‌ی متعالی جداکننده برای K روی F باشد. بنابراین K روی $F(t_1, \dots, t_r)$ یک توسیع جدایی‌پذیر جبری است. از طرفی $t_1, \dots, t_r$ یک پایه‌ی متعالی جداکننده برای KE روی F نیز هست. از این رو KE روی $E(t_1, \dots, t_r)$ یک توسیع جدایی‌پذیر جبری است. در نتیجه KE روی $E(t_1, \dots, t_r)$ یک توسیع جدایی‌پذیر است. بنابراین KE و L روی E مجزای خطی هستند. (زیرا L روی E کاملاً غیر جدایی‌پذیر است).

□

تعریف ۴۱.۳.۱. توسیع میدانی F روی K را منتظم [۶] می‌گوییم هرگاه در یکی از شروط لم ۴۰.۳.۱ صدق کند.

نتیجه ۴۲.۳.۱. فرض کنید $K \subseteq F$ یک توسیع منتظم باشد. در این صورت برای هر $K \subseteq E \subseteq F$ داریم $K \subseteq E$ یک توسیع منتظم است.

[6] Regular extension

لم ۴۳.۳.۱. فرض کنید E یک توسیع منتظم از F و K یک توسیع میدانی از F باشد. در این صورت اگر E و K روی F مجزای جبری باشند، آنگاه E و K روی F مجزای خطی هستند.

اثبات. برای دیدن اثبات، به منبع [۹، لم ۷.۶.۲] مراجعه کنید. □

فرض کنید E و K دو توسیع میدانی از میدان F باشند. در لم ۱۸.۳.۱ دیدیم که اگر E و K روی F مجزای خطی باشند آنگاه E و K مجزای جبری هستند. بنا به لم فوق اگر E یک توسیع منتظم از K باشد، آنگاه E و K روی F مجزای خطی هستند اگروتنهااگر مجزای جبری باشند.

۵.۳.۱ توسیع نرمال

تعریف ۴۴.۳.۱. توسیع $K \subseteq L$ را یک توسیع نرمال می‌نامیم هرگاه هرچندجمله‌ای تحویل‌ناپذیر $f \in K[X]$ که در L یک ریشه دارد، به طور کامل در L به عوامل درجه‌ی اول تجزیه شود.

قضیه ۴۵.۳.۱. فرض کنید $K \subseteq L$ یک توسیع نرمال و متناهی باشد. در این صورت L میدان شکافنده‌ی یک چندجمله‌ای $f \in K[X]$ است.

اثبات. توسیع نرمال و متناهی $K \subseteq L$ را در نظر می‌گیریم. از متناهی بودن این توسیع نتیجه می‌شود که $K \subseteq L$ یک توسیع جبری است. حال عنصر دلخواه a متعلق به $L - K$ را در نظر می‌گیریم. با توجه به این‌که $K \subseteq L$ یک توسیع جبری است، a یک عنصر جبری روی K است. به بیان دیگر a ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر $f \in K[X]$ است. از طرفی $K \subseteq L$ یک توسیع نرمال است. بنابراین از این‌که چندجمله‌ای تحویل‌ناپذیر $f \in K[X]$ در L ریشه دارد نتیجه می‌شود که همه‌ی ریشه‌های f در L قرار دارند. فرض می‌کنیم S مجموعه‌ی همه‌ی ریشه‌های f در L باشد. در این صورت واضح است که $K \subseteq K(S)$ یک توسیع متناهی است و $K(S) \subseteq L$. توجه کنید که اگر $K(S) = L$، حکم بوضوح برقرار است. از این رو کافی است حالتی را بررسی کنیم که $K(S) \neq L$.

فرض می‌کنیم $K(S) \subsetneq L$ و عنصر $\beta \in L - K(S)$ را در نظر می‌گیریم. توسیع $K \subseteq L$ یک توسیع متناهی است. بنابراین $K \subseteq L$ یک توسیع جبری نیز هست، پس β روی K جبری است. در نتیجه β روی $K(S)$ هم جبری است. فرض می‌کنیم g چندجمله‌ای مینیمال β روی $K(S)$ باشد. در این صورت داریم $K \subseteq K(S) \subseteq K(S \cup S')$ به طوری که S' مجموعه‌ی سایر ریشه‌های g است. این روند را تا رسیدن به L ادامه می‌دهیم. توجه کنید که $[K(S) : K] \times [K(S \cup S') : K(S)] < [L : K(S)]$. بنابراین از این‌که $[L : K(S)]$ متناهی است نتیجه می‌شود که روند فوق بعد از متناهی مرحله متوقف خواهد شد. از این رو L میدان شکافنده‌ی یک چندجمله‌ای روی K است. □

نتیجه ۴۶.۳.۱. توسیع متناهی $K \subseteq L$ نرمال است اگروتنهااگر L میدان شکافنده‌ی یک چندجمله‌ای $f \in K[X]$ باشد.

فرض کنید $K \subseteq L$ یک توسیع نرمال متناهی باشد. در این صورت اگر α یک عنصر دلخواه متعلق به $L - K$ باشد، آنگاه روی K جبری است. بنابراین α ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر $f \in K[X]$ است. حال اگر β یک ریشه‌ی دیگر برای چندجمله‌ای f باشد $K(\alpha)$ و $K(\beta)$ یکریخت هستند. بنابراین اتومرفیسمی مانند $\sigma : L \to L$ وجود دارد به طوری که $\sigma(\alpha) = \beta$. به بیان دیگر اتومرفیسمی مانند $\sigma : L \to L$ موجود است به طوری که K را نقطه‌وار حفظ می‌کند، اما $\sigma(\alpha) \neq \alpha$.

قضیه ۴۷.۳.۱. فرض کنید $K \subseteq L$ یک توسیع نرمال متناهی باشد. همچنین فرض کنید E_1 و E_2 دو میدان بین K و L هستند و یک یکریختی مانند $\sigma' : E_1 \to E_2$ وجود دارد به طوری که عناصر K را نقطه‌وار حفظ می‌کند. در این صورت اتومرفیسم $\sigma : L \to L$ موجود است به طوری که عناصر K را نقطه وار حفظ می‌کند و داریم $\sigma' \subseteq \sigma$.

اثبات. فرض می‌کنیم توسیع $K \subseteq L$ نرمال باشد. در این صورت L میدان شکافنده‌ی یک چندجمله‌ای $f \in K[X]$ است. واضح است که $f \in E_1[X]$ و $f \in E_2[X]$، پس بنا به یکتایی میدان شکافنده، اتومرفیسمی مانند $\sigma : L \to L$ موجود است به طوری که عناصر K را نقطه وار حفظ می‌کند و $\sigma' \subseteq \sigma$. □

۶.۳.۱ توسیع گالوایی

گروه گالوایی

تعریف ۴۸.۳.۱. فرض کنید L یک میدان باشد. در این صورت تعریف می‌کنیم :

$$\mathrm{Aut}(L) := \{\sigma : L \to L \mid \text{اتومرفیسم باشد } \sigma\}.$$

مجموعه‌ی $\mathrm{Aut}(L)$ را با عمل ترکیب توابع در نظر بگیرید. به سادگی می‌توان دید که برای هر $\alpha, \beta, \gamma \in \mathrm{Aut}(L)$ داریم $\alpha^{-1}, \alpha \circ \beta \in \mathrm{Aut}(L)$ و $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$. از این رو مجموعه‌ی $\mathrm{Aut}(L)$ با عمل ترکیب توابع تشکیل یک گروه می‌دهد.

تعریف ۴۹.۳.۱. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. در این صورت

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

را گروه گالوایی L روی K می‌نامیم.

توجه ۵۰.۳.۱. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. در این صورت $\mathrm{Gal}(L : K)$ یک زیر گروه از $\mathrm{Aut}(L)$ است. (زیرا اگر $\alpha, \beta \in \mathrm{Gal}(L : K)$، آنگاه بوضوح داریم $\alpha \circ \beta^{-1} \in \mathrm{Gal}(L : K)$).

تعریف ۵۱.۳.۱. فرض کنید $K \subseteq E \subseteq L$ توسیع میدانی باشند. در این صورت تعریف می‌کنیم:
$\Gamma(E) = \{\sigma \in \mathrm{Aut}(L) \mid \forall\, x \in E \;\; \sigma(x) = x\}$.

در واقع اگر $K \subseteq E \subseteq L$، آنگاه $\Gamma(E) = \mathrm{Gal}(L : E)$ و بوضوح داریم $\Gamma(E) \subseteq \mathrm{Gal}(L : K)$.

تعریف ۵۲.۳.۱. فرض کنید L یک میدان باشد و $H \subseteq \mathrm{Aut}(L)$، در این صورت تعریف می‌کنیم:

$$\Phi(H) := \{x \in L \mid \forall \sigma \in H \;\; \sigma(x) = x\}.$$

توجه ۵۳.۳.۱. فرض کنید H زیر گروهی از $\mathrm{Gal}(L : K)$ باشد. در این صورت $K \subseteq \Phi(H) \subseteq L$.

فرض کنید $K \subseteq E_1 \subseteq E_2 \subseteq L$ و E_1 زیرمیدان E_2 باشد. همچنین فرض کنید $\sigma \in \Gamma(E_2)$. در این صورت یک اتومرفیسم $\sigma : L \to L$ تمام نقاط E_2 را حفظ می‌کند. بنابراین با توجه به این‌که $E_1 \subseteq E_2$، اتومرفیسم σ همه‌ی نقاط E_1 را نیز حفظ می‌کند. از این رو $\sigma \in \Gamma(E_1)$. همچنین واضح است که برای هر $\alpha, \beta \in \Gamma(E_1)$ داریم $\alpha \circ \beta^{-1} \in \Gamma(E_1)$. بنابراین $\Gamma(E_2)$ زیرگروهی از $\Gamma(E_1)$ است.
همچنین فرض کنید $H_1 \subseteq H_2 \subseteq \mathrm{Aut}(L)$ زیرگروه باشند. در این صورت برای هر $x \in \Phi(H_2)$ و هر $\sigma \in H_2$ داریم $\sigma(x) = x$. از طرفی $H_1 \subseteq H_2$، پس برای هر $\sigma' \in H_1$ داریم $\sigma' \in H_2$. در نتیجه برای هر $x \in \Phi(H_2)$ داریم $\sigma'(x) = x$. بنابراین $\Phi(H_2)$ زیرمیدان $\Phi(H_1)$ است.

نتیجه ۵۴.۳.۱. فرض کنید $K \subseteq L$. در این صورت موارد زیر برقرار هستند:

۱. اگر $K \subseteq E \subseteq L$، آنگاه $E \subseteq \Phi(\Gamma(E))$. زیرا بنا به تعریف $\Gamma(E)$ و $\Phi(\Gamma(E))$، مجموعه‌ی $\Phi(\Gamma(E))$ برابر است با مجموعه‌ی تمام عناصری در L که توسط تمام اتومرفیسم‌هایی که E را نقطه‌وار حفظ می‌کنند، نقطه‌وار حفظ می‌شوند.

۲. فرض کنید $H \subseteq \mathrm{Gal}(L : K)$. در این صورت $H \subseteq \Gamma(\Phi(H))$. زیرا بنا به تعریف $\Phi(H)$ و $\Gamma(\Phi(H))$، مجموعه‌ی $\Gamma(\Phi(H))$ برابرا ست با مجموعه‌ی اتومرفیسم‌هایی که تمام نقاطی را که توسط اتومرفیسم‌های موجود در H حفظ می‌شوند، حفظ می‌کند.

توسیع گالوایی

تعریف ۵۵.۳.۱. توسیع $K \subseteq L$ را یک توسیع گالوایی می‌نامیم هرگاه $\Phi(\mathrm{Gal}(L : K)) = K$.

لم ۵۶.۳.۱. هر توسیع نرمال و جدایی‌پذیر گالوایی است.

اثبات. فرض کنید $K \subseteq L$ یک توسیع نرمال و جدایی‌پذیر و α یک عنصر دلخواه متعلق به $L - K$ باشد. در این صورت α ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر $f(X) = (X-\alpha)(X-\beta)\cdots(X-\gamma)$ است. از این رو $\sigma \in \mathrm{Gal}(L:K)$ موجود است به طوری که $\sigma(\alpha) \neq \alpha$. بنابراین $\alpha \notin \Phi(\mathrm{Gal}(L:K))$. در نتیجه اگر $K \subseteq L$ نرمال و جدایی‌پذیر باشد آن‌گاه $\Phi(\mathrm{Gal}(L:K)) = K$. □

در ادامه نشان خواهیم داد که عکس قضیه‌ی فوق نیز برقرار است؛ یعنی اثبات می‌کنیم که هر توسیع گالوایی نرمال و جدایی‌پذیر است.

لم ۵۷.۳.۱. فرض کنید $K \subseteq L$ یک توسیع متناهی، نرمال و جدایی‌پذیر باشد. همچنین فرض کنید $[L:K] = n$. در این صورت $|\mathrm{Gal}(L:K)| = n$.

اثبات. برای رسیدن از K به L، یک مسیر جبری به صورت

$$K \subseteq K(\alpha) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \cdots, \alpha_m) = L$$

طی می‌شود. بنابراین $[L:K] = [K(\alpha_1):K] \times [K(\alpha_1,\alpha_2):K] \times \cdots \times [K(\alpha_1,\cdots,\alpha_m):K]$. به بیان دیگر اگر فرض کنیم $[K(\alpha_1,\cdots,\alpha_i):K] = n_i$ داریم $n = n_1 \times n_2 \times \cdots \times n_m$. حال فرض می‌کنیم α_1 ریشه‌ی یک چندجمله‌ای f_1 باشد. از آنجا که L جدایی‌پذیر است f_1 در L شامل n_1 تا ریشه به صورت $\alpha_{11}, \cdots \alpha_{1n_1}$ است. بنابراین n_1 تا یکریختی به صورت $K(\alpha_{11}) \cong \cdots \cong K(\alpha_{1n_1})$ داریم که حافظ K هستند. به همین ترتیب با ثابت نگه داشتن هر یک از این n_1 تا یکریختی، n_2 تا یکریختی دیگر داریم؛ یعنی $K(\alpha_{11},\alpha_{21}) \cong \cdots \cong K(\alpha_{11},\alpha_{2n_2}) \cong \cdots \cong K(\alpha_{1n_1},\alpha_{2n_2})$. بنابراین با ادامه‌ی این روند حداقل $n = n_1 \times n_2 \times \cdots \times n_m$ تا اتومرفیسم از L به L ایجاد می‌شود که K را نقطه‌وار حفظ می‌کنند. همچنین واضح است که هر یکریختی از L به L حتماً به صورت یکی از همین یکریختی‌هاست. در نتیجه $|\mathrm{Gal}(L:K)| = n$. □

توجه ۵۸.۳.۱. به سادگی می‌توان دید که $h(X) = (X-a_1)(X-a_2)\cdots(X-a_r)$ برابر است با

$$h(X) = X^r - (a_1 + \cdots + a_r)X^{r-1} + (a_1a_2 + a_1a_3 + \cdots)X^{r-2} + \cdots + (-1)^r a_1 \cdots a_r.$$

یعنی ضرایب برحسب a_i ها به دست می‌آید.

قضیه ۵۹.۳.۱. فرض کنید $K \subseteq L$ یک توسیع متناهی باشد. در این‌صورت $K \subseteq L$ گالوایی است اگروتنها اگر نرمال و جدایی‌پذیر باشد.

اثبات. در لم ۵۶.۳.۱ دیدیم که هر توسیع نرمال جدایی‌پذیر، گالوایی است. بنابراین کافی است نشان دهیم اگر $K \subseteq L$ گالوایی باشد، آنگاه جدایی‌پذیر و نرمال است.

عنصر دلخواه $\alpha \in L - K$ را در نظر می‌گیریم. از این‌که توسیع $K \subseteq L$ یک توسیع متناهی است نتیجه می‌شود که α ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر $f \in K[X]$ است. نشان می‌دهیم که چندجمله‌ای f در L به عوامل درجه اول تجزیه می‌شود. می‌دانیم $\mathrm{Gal}(L : K)$ یک گروه متناهی است. بدون کاستن از کلیت فرض می‌کنیم $\mathrm{Gal}(L : K) = \{\sigma_1, \ldots, \sigma_n\}$. حال مجموعه‌ی $\{\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\}$ را در نظر می‌گیریم و فرض می‌کنیم مجموعه‌ی $A = \{\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_r(\alpha)\}$ عناصر متمایز آن باشند. قرار می‌دهیم $g(X) = (X - \sigma_1(\alpha))(X - \sigma_2(\alpha)) \cdots (X - \sigma_r(\alpha))$. ادعا می‌کنیم که:

۱. $g(X) \in K[X]$.

۲. $g(X)$ تحویل‌ناپذیر است؛ به بیان دیگر g چندجمله‌ای مینیمال α است.

برای اثبات ادعای اول ابتدا توجه کنید که بنا به توجه ۵۸.۳.۱ ضرایب $g(X)$ برحسب $\sigma_i(\alpha)$ نوشته می‌شوند. از طرفی طبق فرض $K = \Phi(\mathrm{Gal}(L : K))$. بنابراین کافی است نشان دهیم ضرایب چندجمله‌ای g توسط اتومرفیسم‌های موجود در $\mathrm{Gal}(L : K)$ حفظ می‌شوند. فرض می‌کنیم $\beta \in \mathrm{Gal}(L : K)$ یک اتومرفیسم دلخواه باشد. در این صورت $\beta(A) = A$؛ زیرا عناصر A دو به دو متمایزند و ریشه‌های g هستند پس تحت اتومرفیسم β نیز همچنان این دو ویژگی را دارا هستند. به بیان دیگر $\beta(A)$ جایگشتی از A است. بنابراین واضح است که ضرایب g توسط β حفظ می‌شوند. در نتیجه $g \in K[X]$.

برای اثبات ادعای دوم نشان می‌دهیم g چندجمله‌ای مینیمال α است. بدین منظور کافی است نشان دهیم اگر چندجمله‌ای h موجود باشد به طوری که $h(\alpha) = 0$ آن گاه $g \mid h$. فرض می‌کنیم $h(\alpha) = 0$. از این رو هر $\sigma_i(\alpha)$ یک ریشه‌ی چندجمله‌ای h است، پس برای هر $\sigma_i(\alpha)$ داریم $(X - \sigma_i(\alpha)) \mid h$. بنابراین $g \mid h$.

در نتیجه بنا به یکتایی چندجمله‌ای مینیمال داریم :

$$f(X) = g(X) = (X - \sigma_1(\alpha))(X - \sigma_2(\alpha)) \cdots (X - \sigma_r(\alpha)).$$

□

توسیع متناهی $K \subseteq L$ را در نظر بگیرید. اگر مشخصه‌ی میدان L صفر باشد، می‌توان اثبات کرد که توسیع $K \subseteq L$ یک توسیع گالوایی است اگروتنهااگر L میدان شکافنده‌ی یک چندجمله‌ای f روی K باشد.

در پایان این زیربخش اثبات می‌کنیم که هر توسیع گالوایی متناهی از یک میدان نامتناهی، یک پایه‌ی نرمال دارد. به بیان دیگر فرض کنید K یک میدان نامتناهی و $K \subseteq L$ یک توسیع گالوایی و متناهی باشد. در این صورت عنصر $\alpha \in L$ موجود است به طوری که L روی K دارای یک پایه به صورت $\{g(\alpha) | g \in \mathrm{Gal}(L : K)\}$ است. این قضیه یکی از مهم‌ترین قضایای این پایان‌نامه است.

جایگشت دلخواه $\pi : \{۱, \dots, m\} \to \{۱, \dots, m\}$ را در نظر بگیرید. از مبانی ماتریس‌ها یادآوری می‌کنیم که به چنین جایگشتی می‌توان یک ماتریس به صورت زیر نظیر کرد: یک ماتریس $m \times m$ در نظر می‌گیریم برای هر i اگر $\pi(i) = j$، آنگاه درایه‌ی ij ام این ماتریس را عدد ۱ و در غیر این صورت عدد صفر را قرار می‌دهیم. به ماتریس حاصل ماتریس جایگشت می‌گوییم.

به عنوان مثال ماتریس جایگشت $\pi = \begin{bmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۱ & ۴ & ۲ & ۵ & ۳ \end{bmatrix}$ به صورت زیر است:

$$\begin{bmatrix} ۱ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۰ & ۰ \end{bmatrix}.$$

قضیه ۶۰.۳.۱ (پایه نرمال [۷]). هر توسیع گالوایی متناهی از یک میدان نامتناهی یک پایه‌ی نرمال دارد. به بیان دیگر فرض کنید K یک میدان نامتناهی و $K \subseteq L$ یک توسیع گالوایی و متناهی باشد. در این صورت عنصر $\alpha \in L$ موجود است به طوری که L روی K دارای یک پایه به صورت $\{g(\alpha) \mid g \in \mathrm{Gal}(L : K)\}$ است.

اثبات. فرض می‌کنیم K یک میدان نامتناهی و توسیع L روی K یک توسیع گالوایی و متناهی باشد. همچنین فرض می‌کنیم $[L : K] = n$ و $\mathrm{Gal}(L : K) = \{\sigma_۱, \dots, \sigma_n\}$ به طوری که $\sigma_۱$ نگاشت همانی است. از این‌که توسیع $K \subseteq L$ یک توسیع گالوایی و متناهی است نتیجه می‌گیریم که یک توسیع جدایی‌پذیر است، پس بنا به قضیه‌ی ۳۰.۳.۱ این توسیع ساده است؛ یعنی عنصر α متعلق به K موجود است به طوری $L = K(\alpha)$. فرض می‌کنیم f چندجمله‌ای مینیمال α باشد. در این صورت f یک چندجمله‌ای تحویل‌ناپذیر از درجه‌ی n است و با توجه به جدایی‌پذیر بودن L روی K، این چندجمله‌ای ریشه‌ی تکراری ندارد. از این رو برای هر $i \neq j$ داریم $\sigma_i(\alpha) \neq \sigma_j(\alpha)$. قرار می‌دهیم $\alpha_i = \sigma_i(\alpha)$، پس داریم $f(X) = \prod_{i=۱}^{n}(X - \alpha_i)$. تعریف می‌کنیم:

$$g(X) = \frac{f(X)}{(X - \alpha) f'(\alpha)},$$

$$g_i(X) = \frac{f(X)}{(X - \alpha_i) f'(\alpha_i)} = \sigma_i(g(X)).$$

به سادگی می‌توان دید که $f'(\alpha_i) = \prod_{\substack{j=۱ \\ i \neq j}}^{n}(\alpha_i - \alpha_j)$. بنابراین با جایگذاری $f(X)$ و $f'(\alpha_i)$ در $g_i(X)$ داریم:

[7] Normal basis theorem

$$g_i(X) = \prod_{\substack{j \neq i \\ 1 \leq j \leq n}} \frac{X - \alpha_j}{\alpha_i - \alpha_j}$$

و

$$g(X) = g_1(X).$$

توجه کنید که بوضوح $g(\alpha) = 1$ و برای هر $i \neq 1$ داریم $g_i(\alpha) = 0$. یک ماتریس $n \times n$ به نام A را به صورت زیر تعریف می‌کنیم $A_{ij}(X) = \sigma_i(\sigma_j(g(X))) = \sigma_i(g_j(X))$. به بیان دیگر $A_{ij}(X) = g_k(X)$ به طوری که $g_k(X) = \sigma_k(g(X))$ و $\sigma_k = \sigma_i\sigma_j$. همچنین واضح است که $k = 1$ اگروتنهااگر $\sigma_i = \sigma_j^{-1}$. بنابراین ماتریس $A(\alpha)$ یک ماتریس جایگشت روی $\mathrm{Gal}(L : K)$ است به طوری که σ_i را به σ_i^{-1} می‌برد. در نتیجه $D(\alpha) := \det A(\alpha) = \pm 1$؛ یعنی چندجمله‌ای $D(X)$ یک چندجمله‌ای ناصفر است. از این رو این چندجمله‌ای متناهی تا ریشه دارد، پس با توجه به نامتناهی بودن K عنصر a متعلق به K موجود است به طوری که $D(a) \neq 0$. حال تعریف می‌کنیم $\beta = g(a)$ و $\beta_i = g_i(a) = \sigma_i(\beta)$.

ادعا می‌کنیم مجموعه‌ی $\{\beta_1, \ldots, \beta_n\}$ یک پایه‌ی نرمال است. به منظور اثبات این ادعا کافی است نشان دهیم $\beta_1, \ldots, \beta_n$ روی K مستقل خطی هستند. از این رو فرض می‌کنیم ترکیب خطی دلخواه $\sum_{j=1}^{n} x_j\beta_j$ برای $x_1, \ldots, x_n \in K$ صفر شود. حال برای هر i با اعمال اتومرفیسم σ_i بر روی این ترکیب خطی داریم $\sum_{j=1}^{n} x_j\sigma_i(g_j(a)) = 0$. به بیان دیگر $A(a) \cdot \bar{x} = \bar{0}$. بنابراین از این که $A(a) = D(a) \neq 0$ نتیجه می‌شود که $\bar{x} = 0$.

□

۴.۱ میدان‌های متناهی

فرض کنید F یک میدان باشد. کوچکترین عدد اول $n \in \mathbb{N}$ که $\underbrace{1 + 1 + \ldots + 1}_{n \text{ بار}} = 0$ را مشخصه‌ی میدان F می‌نامیم. اگر مشخصه‌ی میدان F برابر با n باشد، می‌نویسیم $\mathrm{char}(F) = n$. همچنین اگر به ازای هر $n \in \mathbb{N}$ داشته باشیم $\underbrace{1 + 1 + \ldots + 1}_{n \text{ بار}} \neq 0$ می‌گوییم مشخصه‌ی میدان صفر است و می‌نویسیم $\mathrm{char}(F) = 0$.

فرض کنید F یک میدان متناهی باشد. در این صورت میدان F دارای یک مشخصه‌ی متناهی p است. زیرا بوضوح گروه جمعی F متناهی است، پس بنا به نتیجه‌ای از قضیه‌ی لاگرانژ $\underbrace{1 + 1 + \ldots + 1}_{\text{به اندازه‌ی میدان}} = 0$. بنابراین عدد اول p موجود است به طوری که مشخصه‌ی میدان F برابر است با p.

در لم زیر اثبات می‌کنیم که هر میدان متناهی با مشخصه‌ی p، دارای اندازه‌ای به صورت p^n است که در آن n یک عدد طبیعی است.

لم ۱.۴.۱. فرض کنید F یک میدان متناهی باشد. اگر مشخصه‌ی میدان F عدد اول p باشد، آنگاه برای یک عدد طبیعی $n \in \mathbb{N}$ داریم $|F| = p^n$.

اثبات. از آنجا که مشخصه‌ی میدان F عدد اول p است، داریم $\mathbb{Z}_p \subseteq F$. توسیع $\mathbb{Z}_p \subseteq F$ یک توسیع متناهی است. بنابراین عدد طبیعی $n \in \mathbb{N}$ موجود است به طوری که $[F : \mathbb{Z}_p] = n$. در نتیجه عناصر $\{k_1, ..., k_n\}$ موجود هستند به طوری که $F = \mathbb{Z}_p(k_1, ..., k_n)$. از این رو هر یک از عناصر F به صورت یک ترکیب خطی $a_1k_1 + \ldots + a_nk_n$ است به طوری که $a_1, \ldots, a_n \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. به بیان دیگر هر a_i می‌تواند p تا مقدار متفاوت را اتخاذ کند. بنابراین $|F| = p^n$. □

لم ۲.۴.۱. فرض کنید F یک میدان دلخواه با مشخصه‌ی p باشد. در این صورت نگاشت $\sigma : F \to F$ با ضابطه‌ی $\sigma(x) = x^p$، یک همریختی است. همچنین σ روی $\mathbb{Z}_p$ همانی است؛ یعنی $\mathbb{Z}_p$ را به خودش می‌برد.

اثبات. ابتدا توجه کنید که بوضوح $(x \cdot y)^p = x^p \cdot y^p$. همچنین $(x + y)^p = x^p + y^p$. زیرا $(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \ldots + \binom{p}{p-1}xy^{p-1} + y^p$ و به سادگی می‌توان دید که $p \mid \binom{p}{i}$، پس $(x + y)^p = x^p + y^p$. بنابراین این نگاشت یک همریختی است.

حال کافی است اثبات کنیم که این نگاشت روی $\mathbb{Z}_p$ همانی است. بنا به قضیه‌ی کوچک فرما، برای هر $a \in \mathbb{Z}_p$ داریم $a^p \equiv_p a$؛ یعنی عدد طبیعی k موجود است به طوری که $a^p = kp + a$. از طرفی می‌دانیم مشخصه‌ی میدان $\mathbb{Z}_p$ برابر با p است. در نتیجه $a^p = a$. پس بوضوح نگاشت σ یک همریختی است که روی $\mathbb{Z}_p$ همانی است.

□

مشاهده ۳.۴.۱. فرض کنید $F \subseteq L$ دو میدان متناهی باشند به طوری که $|F| = p^n$ و $|L| = p^k$. در این صورت $n \mid k$.

اثبات. توجه کنید که $\mathbb{Z}_p \subseteq F \subseteq L$. بنابراین $[L : \mathbb{Z}_p] = [L : F] \times [F : \mathbb{Z}_p]$. در نتیجه $k = [L : F]n$؛ یعنی $n \mid k$. □

در قضیه‌ی زیر روش ساخت یک میدان متناهی را می‌بینیم.

قضیه ۴.۴.۱. فرض کنید p یک عدد اول و n یک عدد طبیعی دلخواه باشد. در این صورت یک میدان متناهی با اندازه‌ی p^n موجود است.

اثبات. میدان $\mathbb{Z}_p$ را در نظر می‌گیریم و قرار می‌دهیم $f(x) = x^{p^n} - x \in \mathbb{Z}_p[X]$. حال فرض می‌کنیم F میدان شکافنده‌ی f روی $\mathbb{Z}_p$ باشد. ادعا می‌کنیم چندجمله‌ای f در میدان شکافنده‌ی F دارای ریشه‌ی تکراری نیست. به جهت اثبات این ادعا ابتدا توجه کنید که $f'(x) = p^n x^{p^n-1} - 1$. از طرفی مشخصه‌ی میدان $\mathbb{Z}_p$ برابر با p است. بنابراین $f'(x) = -1$. (واضح است که $0 \neq -1$، زیرا اگر $0 = -1$ آنگاه $0 = 1$ که با این فرض که مشخصه‌ی میدان، عدد اول p است، در تناقض است). پس بنا به لم ۲۲.۳.۱ این چندجمله‌ای ریشه‌ی مضاعف ندارد. بنابراین چندجمله‌ای $f(x) = x^{p^n} - x$ در میدان شکافنده‌ی $\mathbb{Z}_p \subseteq F$، دارای p^n ریشه‌ی متمایز است. از طرفی بنا به لم ۲.۴.۱ مجموعه ریشه‌های چندجمله‌ای f تشکیل میدان می‌دهند. بنابراین عناصر میدان F دقیقاً ریشه‌های $f(x) = x^{p^n} - x$ هستند؛ یعنی $|F| = p^n$.

□

قضیه ۵.۴.۱. فرض کنید F یک میدان متناهی با $|F| = p^n$ باشد. در این صورت F میدان شکافنده‌ی چندجمله‌ای $f(x) = x^{p^n} - x$ روی $\mathbb{Z}_p$ است.

اثبات. از این‌که $|F| = p^n$ نتیجه می‌شود که گروه ضربی $F^\star = F - \{0\}$ دارای $p^n - 1$ عنصر است. بنابراین برای هر $a \in F^\star$ داریم $a^{p^n-1} = 1$. و در نتیجه $a^{p^n} = a$. همچنین واضح است که $0^{p^n} = 0$. در نتیجه برای هر $a \in F$ داریم $a^{p^n} = a$. از این رو همه‌ی عناصر میدان F در معادله‌ی $x^{p^n} = x$ صدق می‌کنند و ریشه‌های متفاوت این معادله هستند. بنابراین F میدان شکافنده‌ی چندجمله‌ای $f(x) = x^{p^n} - x$ روی $\mathbb{Z}_p$ است. □

بنا به آنچه گفته شد، برای هر میدان متناهی عدد اول p و یک عدد طبیعی n موجود است به طوری که $|F| = p^n$. چنین میدانی در واقع میدان شکافنده‌ی چندجمله‌ای $x^{p^n} - x$ روی $\mathbb{Z}_p$ است. به بیان دیگر برای هر عدد اول p و عدد طبیعی n، تحت یکریختی فقط یک میدان متناهی با اندازه‌ی p^n وجود دارد.

در ادامه اثبات خواهیم کرد که اگر F یک میدان متناهی باشد، آنگاه گروه ضربی F، یک گروه دوری است. بدین منظور لازم است مقدماتی از نظریه‌ی گروه‌ها را یادآوری کنیم.

فرض کنید G یک گروه آبلی متناهی باشد. برای هر عنصر $a \in G$ کوچکترین عنصری که a به توان آن عنصر مساوی ۱ می‌شود را مرتبه‌ی آن عنصر می‌نامیم و آن را با $\mathrm{ord}(a)$ نمایش می‌دهیم. بنابراین $a^{\mathrm{ord}(a)} = 1$ و $\mathrm{ord}(a)$ کوچکترین عدد با این ویژگی است. همچنین کوچکترین عدد طبیعی e که برای هر $a \in G$ داشته باشیم $a^e = 1$ را توان گروه G می‌نامیم. به سادگی می‌توان دید که اگر G یک گروه متناهی باشد، آنگاه توان G با ک.م.م مرتبه‌ی همه‌ی عناصر برابر است.

لم ۶.۴.۱. اگر e توان گروه G باشد، آنگاه عنصر $a \in G$ موجود است به طوری که $\mathrm{ord}(a) = e$.

اثبات. فرض می‌کنیم $e = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$، ک.م.م همه‌ی مرتبه‌ها باشد. در این صورت عنصری مانند a_1 موجود است به طوری که $p_1^{\alpha_1} \mid \mathrm{ord}(a_1)$. بنابراین $\mathrm{ord}(a_1) = p_1^{\alpha_1} q_1$، پس $(a_1^{q_1})^{p_1^{\alpha_1}} = 1$. از این رو

$\text{ord}(a_1^{q_1}) = p_1^{\alpha_1}$. در نتیجه عناصر $g_1, \dots, g_k$ موجود هستند به طوری که $\text{ord}(g_i) = p_i^{\alpha_i}$. حال قرار می‌دهیم $a = g_1 \dots g_k$. ادعا می‌کنیم که $\text{ord}(a) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. به منظور اثبات این ادعا ابتدا توجه کنید که بوضوح $(g_1 \dots g_k)^{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}} = 1$. حال فرض می‌کنیم برای یک $n \neq p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ داشته باشیم $(g_1 \dots g_k)^n = 1$. در این صورت $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \mid n$. زیرا بوضوح $(g_1 \dots g_k)^{np_2^{\alpha_2} \dots p_k^{\alpha_k}} = 1$. بنابراین $g_1^{np_2^{\alpha_2} \dots p_k^{\alpha_k}} \times (g_2 \dots g_k)^{np_2^{\alpha_2} \dots p_k^{\alpha_k}} = 1$. در نتیجه $p_1^{\alpha_1} \mid np_2^{\alpha_2} \cdots p_k^{\alpha_k}$، پس $p_1^{\alpha_1} \mid n$. از این رو برای هر $1 \leq i \leq k$ داریم $p_i^{\alpha_i} \mid n$. در نتیجه $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \mid n$.

□

لم ۷.۴.۱. گروه G با توان e را در نظر بگیرید. فرض کنید $|G| = n$. در این صورت $e \mid n$.

اثبات. به برهان خلف فرض می‌کنیم $e \nmid n$. در این صورت عنصر $b, k \in G$ وجود دارند به طوری که $b < n$ و $e = nk + b$. از طرفی برای هر $a \in G$ داریم $a^e = 1$. بنابراین $a^{nk+b} = (a^n)^k . a^b = a^b = 1$ که با تعریف توان گروه در تناقض است. در نتیجه $e \mid n$. □

قضیه ۸.۴.۱. اگر F یک میدان متناهی باشد، آنگاه $F^\star$، یعنی گروه ضربی F، یک گروه دوری است.

اثبات. فرض می‌کنیم F یک میدان متناهی با p^n عضو باشد. در این صورت بوضوح $|F^\star| = |F| - 1 = p^n - 1$ و $F^\star$ متشکل از ریشه‌های ناصفر چندجمله‌ای $x^{p^n} - x$ است. حال فرض می‌کنیم e توان گروه $F^\star$ باشد. در این صورت برای هر عنصر x متعلق به $F^\star$ داریم $x^e = 1$. بنابراین عناصر $F^\star$ ریشه‌های چندجمله‌ای $x^e - 1$ هستند. از این رو با توجه به این‌که چندجمله‌ای $x^e = 1$ حداکثر e تا ریشه دارد؛ داریم $|F^\star| \leq e$. از طرفی طبق لم ۷.۴.۱ توان e اندازه‌ی گروه $F^\star$ را می‌شمارد. بنابراین $e \leq |F^\star|$. در نتیجه $|F^\star| = e$ یعنی $e = p^n - 1$، پس بنا به لم ۶.۴.۱ گروه $F^\star$ دارای عنصری مانند b است به طوری که $\text{ord}(b) = p^n - 1$. در نتیجه $F^\star$ دوری است.

□

نتیجه ۹.۴.۱. فرض کنید $F \subseteq L$ یک توسیع متناهی از میدان متناهی F باشد. در این صورت این توسیع ساده است. به بیان دیگر عنصر α متعلق به L موجود است به طوری که $L = F(\alpha)$.

اثبات. میدان L یک میدان متناهی است، پس بنا به قضیه‌ی ۸.۴.۱ گروه ضربی میدان L یعنی L^* دوری است. بنابراین عنصر α متعلق به L به گونه‌ای موجود است که برای هر عنصر $a \in L^*$ داریم $a = \alpha^i$ به طوری که $i \in \mathbb{N}$. در نتیجه بوضوح $L = F(\alpha)$.

□

فرض کنید F یک میدان متناهی باشد و $|F| = p^n$. دیدیم که این میدان در واقع میدان شکافنده‌ی چندجمله‌ای $x^{p^n} - x$ روی $\mathbb{Z}_p$ است. بنابراین موارد زیر برقرار هستند:

- $\mathbb{Z}_p \subseteq F$.
- توسیع $\mathbb{Z}_p \subseteq F$ یک توسیع گالوایی است.
- $|\mathrm{Gal}(F : \mathbb{Z}_p)| = n$.

لم ۱۰.۴.۱. نگاشت $\sigma : F \longrightarrow F$ با ضابطه‌ی $\sigma(x) = x^p$ را در نظر بگیرید. این نگاشت متعلق به $\mathrm{Gal}(F : \mathbb{Z}_p)$ است.

اثبات. نگاشت $\sigma : F \longrightarrow F$ به طوری که $\sigma(x) = x^p$ را در نظر می‌گیریم. در لم ۲.۴.۱ دیدیم که این نگاشت، $\mathbb{Z}_p$ را نقطه‌وار حفظ می‌کند. همچنین از این‌که مشخصه‌ی میدان p است، نتیجه می‌شود $(x+y)^p = x^p + y^p$ و $(x.y)^p = x^p.y^p$. بنابراین σ یک همریختی است. کافی است نشان دهیم σ یک به یک و پوشا است. برای اثبات پوشا بودن این نگاشت، توجه کنید که هر عنصر $x \in F$ در معادله‌ی $x^{p^n} = x$ صدق می‌کند. بنابراین $(x^{p^{n-1}})^p = x$. در نتیجه نگاشت σ پوشاست. همچنین می‌دانیم که اگر $f : A \longrightarrow A$ یک تابع و A متناهی باشد آن‌گاه f یک به یک است اگروتنهااگر پوشا باشد. از این رو یک به یک بودن این نگاشت از پوشا بودن آن نتیجه می‌شود. بنابراین $\sigma \in \mathrm{Gal}(F : \mathbb{Z}_p)$.

□

لم ۱۱.۴.۱. گروه $\mathrm{Gal}(F : \mathbb{Z}_p)$ دوری است و توسط نگاشت $\sigma : F \longrightarrow F$ با ضابطه‌ی $\sigma(x) = x^p$ تولید می‌شود. به بیان دیگر $\mathrm{Gal}(F : \mathbb{Z}_p) = \langle \sigma \rangle$.

اثبات. فرض می‌کنیم $G = \mathrm{Gal}(F : \mathbb{Z}_p)$ و $H = \langle \sigma \rangle$. از لم ۲.۴.۱ داریم که $\mathbb{Z}_p \subseteq \{\alpha \mid \sigma(\alpha) = \alpha\}$. از طرفی $\sigma(x) = x^p$ و معادله‌ی $x^p = x$ حداکثر p تا ریشه دارد. بنابراین واضح است که $\mathbb{Z}_p = \{\alpha \mid \sigma(\alpha) = \alpha\}$ و $\Phi(H) = \mathbb{Z}_p$. بنابراین $\Phi(H) = \Phi(G)$. در نتیجه $G = H$. □

بنابراین مجموعه‌ی $\mathrm{Gal}(F : \mathbb{Z}_p)$ از $\sigma_i : F \to F$ ها تشکیل شده است که $1 \leq i \leq n$ و $\sigma_i(x) = (\sigma(x))^i = x^{p^i}$. به بیان دیگر

$$\mathrm{Gal}(F : \mathbb{Z}_p) = \{\sigma_i(x) = x^{p^i} \mid 1 \leq i \leq n\}.$$

همچنین توجه کنید که $\sigma_n(x) = x^{p^n} = x$ ثابت گروه است.

در قضیه‌ی ۶۰.۳.۱ دیدیم که هر توسیع گالوایی متناهی از یک میدان نامتناهی یک پایه‌ی نرمال دارد. به بیان دیگر اگر K یک میدان نامتناهی و $K \subseteq L$ یک توسیع گالوایی و متناهی باشد، عنصر $\alpha \in L$ موجود

است به طوری که L روی K دارای یک پایه به صورت $\{g(\alpha) \mid g \in \mathrm{Gal}(L:K)\}$ است. در این بخش قضیه‌ی فوق را برای حالتی که K یک میدان متناهی است اثبات می‌کنیم. برای اثبات این قضیه به مقدماتی از مدول‌ها نیاز داریم که در ادامه به آن‌ها اشاره کرده‌ایم. فرض کنید V و W دو فضای برداری روی میدان K باشند.

یک تابع $f : V \to W$ را نگاشت خطی گوییم هرگاه برای هر دو بردار u و v در V و برای هر ثابت c در K شرایط زیر برقرار باشد: $f(u+v) = f(u) + f(v)$ و $f(cu) = cf(u)$. بنابراین برای هر $v_1, \ldots, v_n \in V$ و هر $c_1, \ldots, c_n \in K$ داریم $f(c_1v_1 + \ldots + c_nv_n) = c_1f(v_1) + \ldots + c_nf(v_n)$. به بیان دیگر یک نگاشت خطی هر ترکیب خطی از عناصر را حفظ می‌کند.

فرض کنید R یک حلقه با عنصر همانی ضربی ۱ باشد. یک R مدول چپ M، شامل گروه آبلی $(M, +)$ و یک عملگر $\cdot : R \times M \to M$ است به طوری که برای هر $r, s \in R$ و هر $x, y \in M$ داریم:

۱. $r \cdot (x+y) = r \cdot x + r \cdot y$

۲. $(r+s) \cdot x = r \cdot x + s \cdot x$

۳. $(r \cdot s) \cdot x = r \cdot (x \cdot s)$

۴. $1 \cdot x = x$

همچنین یک R مدول راست M به طور مشابه با $\cdot : M \times R \to M$ تعریف می‌گردد. بنابراین اگر R یک حلقه‌ی جابجایی باشد، آنگاه R مدول‌های چپ مشابه با R مدول‌های راست هستند و برای راحتی کار به هر دو، R مدول می‌گوییم.

فرض کنید R یک حلقه و M یک R مدول باشد. یک زیرمجموعه‌ی دلخواه $S \subset M$ را در نظر بگیرید. مجموعه‌ی همه‌ی عناصر $r \in R$ که برای هر $s \in S$ داریم $rs = 0$ را یک پوچ‌ساز [8] برای S می‌نامیم. یک پوچ‌ساز برای S را با نماد زیر نمایش می‌دهیم:

$$\mathrm{Ann}_R(S) = \{r \in R : rs = 0 \quad \text{برای هر } s \in S\}.$$

توجه کنید که اگر S یک زیرمجموعه از مدول M باشد، آنگاه $\mathrm{Ann}_R(S)$ یک ایده‌آل روی حلقه‌ی R است.

منظور از یک حوزه‌ی ایده‌آل اصلی یک حوزه‌ی صحیح است که همه‌ی ایده‌آل‌های آن اصلی است. به بیان دیگر هر ایده‌آل از آن را می‌توانیم به کمک یک عنصر تولید کنیم.

[8] Annihilator

قضیه ۱۲.۴.۱. فرض کنید R یک حوزه‌ی ایده‌ال اصلی باشد. برای هر مدول متناهیاً تولید شده‌ی M روی R یک دنباله‌ی نزولی یکتا از ایده‌آل‌های سره‌ی $\langle d_n\rangle \supseteq \cdots \supseteq \langle d_۲\rangle \supseteq \langle d_۱\rangle$ موجود است به طوری که $M \cong \bigoplus_i R/\langle d_i\rangle$.

قضیه ۱۳.۴.۱ (پایه‌ی نرمال)**.** هر توسیع گالوایی متناهی از یک میدان متناهی یک پایه‌ی نرمال دارد.

اثبات. اثبات این قضیه از منبع [۵، قضیه‌ی ۷.۳] گرفته شده است.

فرض می‌کنیم K یک میدان متناهی و $K \subseteq L$ یک توسیع گالوایی و متناهی باشد. همچنین فرض می‌کنیم $[L : K] = n$. در این صورت $\mathrm{Gal}(L : K) = \langle\sigma\rangle = \{\sigma, \cdots, \sigma^{n-۱}, \sigma^n\}$. واضح است که σ یک نگاشت خطی از L به L است. L را به عنوان یک مدول روی حلقه‌ی $K[X]$ در نظر می‌گیریم به طوری که X روی L به عنوان σ عمل می‌کند. بنابراین برای هر α متعلق به L و هر چندجمله‌ای $f(X) \in K[X]$ داریم $f(X)\alpha = f(\sigma)\alpha$. حال توجه کنید که چندجمله‌ای $X^n - ۱$ پوچ‌ساز کل L است. زیرا برای هر α متعلق به L داریم:

$$X^n - ۱(\alpha) = \sigma^n(\alpha) - \alpha = \alpha - \alpha = ۰.$$

حال ادعا می‌کنیم که چندجمله‌ای دیگری با درجه‌ی کمتر از درجه‌ی $X^n - ۱$ وجود ندارد به طوری که پوچ‌ساز کل L باشد. به منظور اثبات این ادعا فرض می‌کنیم چندجمله‌ای $c_۰ + c_۱X + \cdots + c_{n-۱}X^{n-۱} \in K[X]$ پوچ‌ساز کل L باشد. در این صورت برای هر α متعلق به L داریم:

$$c_۰ + c_۱\sigma(\alpha) + \cdots + c_{n-۱}\sigma^{n-۱}(\alpha) = ۰$$

از طرفی بنا به [۱۲، قضیه‌ی ۱.۷]، σ^i ها مستقل خطی هستند. بنابراین $c_۰ = c_۱ = \cdots = c_{n-۱} = ۰$. ایده‌آل پوچ‌ساز

$$\mathrm{Ann}_{K[X]}(L) = \{f(X) \in K[X] : f(\sigma) \equiv ۰ \quad L \text{ روی}\}$$

اصلی است. بنابراین مجبور است که برابر با $X^n - ۱$ باشد. حال بنا به قضیه‌ی ۱۲.۴.۱ ایده‌آل پوچ‌ساز مدول L معادل است با ایده‌آل پوچ‌ساز یک عنصر خاص، به بیان دیگر عنصر $\alpha_۰$ متعلق به L موجود است به طوری که $\mathrm{Ann}_{K[X]}(\alpha_۰) = X^n - ۱$؛ یعنی $f(\sigma)(\alpha_۰) = ۰$ اگروتنهااگر $X^n - ۱ \mid f(X)$. نگاشت $K[X] \to L$ به طوری که $f(x) \to f(\sigma)(\alpha_۰)$ را در نظر می‌گیریم. هسته‌ی این نگاشت $X^n - ۱$ است. از این رو $K[X]/(x^n - ۱)$ در L می‌نشیند. همچنین با توجه به این‌که بُعد فضای برداری $K[X]/(x^n - ۱)$ و L روی K یکسان است، نشاندن $K[X]/(x^n - ۱) \to L$ پوشا نیز هست. در نتیجه تصویر یک پایه از $K[X]/(x^n - ۱)$ یک پایه از L است. بنابراین با توجه به این‌که $۱, X, \ldots, X^{n-۱}$ یک پایه برای $K[X]/(x^n - ۱)$ است تصویر آن یعنی $\alpha_۰, \sigma(\alpha_۰), \ldots, \sigma^{n-۱}(\alpha_۰)$ یک پایه‌ی نرمال برای L روی K است.

□

نتیجه ۱۴.۴.۱. فرض کنید $q = p^n$. توسیع $\mathbb{F}_q/\mathbb{F}_p$ دارای یک پایه‌ی نرمال به صورت $\{\alpha, \alpha^p, ..., \alpha^{p^{n-1}}\}$ است.

اثبات. فرض می‌کنیم $\mathbb{F}_q$ و $\mathbb{F}_p$ دو میدان متناهی باشند به طوری که $q = p^n$. همچنین فرض می‌کنیم $\mathbb{F}_q$ یک توسیع متناهی از $\mathbb{F}_p$ باشد. در این صورت توسیع $\mathbb{F}_q$ روی $\mathbb{F}_p$ یک توسیع گالوایی است. بنا به قضیه‌ی ۱۳.۴.۱ عنصر $\alpha \in \mathbb{F}_q$ موجود است به طوری که $\mathbb{F}_q$ روی $\mathbb{F}_p$ دارای یک پایه به صورت زیر است:

$$\{g(\alpha) \mid g \in \mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p)\} = \{\alpha, \alpha^p, ..., \alpha^{p^{n-1}}\}.$$

□

نتیجه ۱۵.۴.۱. فرض کنید $E \subseteq L$ دو میدان متناهی باشند به طوری که $|E| = p^n$ و $|L| = p^k$. توسیع $E \subseteq L$ گالوایی است.

اثبات. توجه کنید که $\mathbb{Z}_p \subseteq E \subseteq L$ و توسیع $\mathbb{Z}_p \subseteq L$ یک توسیع گالوایی است. به بیان دیگر $\mathbb{Z}_p \subseteq L$ نرمال و جدایی‌پذیر است. بنابراین L میدان شکافنده‌ی یک چندجمله‌ای $f \in \mathbb{Z}_p[X]$ است. واضح است که $f \in E[X]$. بنابراین L میدان شکافنده‌ی یک چندجمله‌ای $f \in E[X]$ نیز است. در نتیجه $E \subseteq L$ نیز یک توسیع نرمال است. حال کافی است نشان دهیم $E \subseteq L$ جدایی‌پذیر است. بدین منظور فرض می‌کنیم $x \in L - E$ ریشه‌ی یک چندجمله‌ای با ضرایب در E باشد. در این صورت x روی $\mathbb{Z}_p[X]$ جبری است. بنابراین ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر $f \in \mathbb{Z}_p[X]$ است. واضح است که $f \in E[X]$. ادعا می‌کنیم f چندجمله‌ای مینیمال x در $E[X]$ است. به منظور اثبات این ادعا فرض می‌کنیم g چندجمله‌ای مینیمال x در $E[X]$ باشد. در این صورت داریم $g = fh + r$. از آنجا که $f(x) = g(x) = 0$ نتیجه می‌شود که $r = 0$. بنابراین $g = fh$ که تناقض است. در نتیجه چندجمله‌ای مینیمال x در $E[X]$ و $\mathbb{Z}_p[X]$ یکسان است؛ یعنی f در $E[X]$ تحویل‌ناپذیر است. همچنین بنا به جدایی‌پذیر بودن $\mathbb{Z}_p \subseteq L$، چندجمله‌ای f در میدان شکافنده‌ی f روی $\mathbb{Z}_p$ به عوامل درجه‌ی اول تجزیه می‌شود. در نتیجه در میدان شکافنده‌ی f روی E نیز به عوامل درجه‌ی اول تجزیه می‌شود.

□

نتیجه ۱۶.۴.۱. بنا به روند اثبات نتیجه‌ی فوق، به طور کلی اگر $F \subseteq E \subseteq L$ و توسیع $F \subseteq L$ یک توسیع گالوایی باشد، آنگاه توسیع $E \subseteq L$ یک توسیع گالوایی است.

توجه ۱۷.۴.۱. فرض کنید F و L دو میدان متناهی باشند به طوری که $|F| = p^n$ و $|L| = p^k$. توسیع متناهی $F \subseteq L$ را در نظر بگیرید. موارد زیر برقرارند:

۱. $|\mathrm{Gal}(L:F)| = \frac{[L:\mathbb{Z}_p]}{[F:\mathbb{Z}_p]} = \frac{k}{n}$.

۲. گروه $\mathrm{Gal}(L:F)$ زیر گروهی از $\mathrm{Gal}(L:\mathbb{Z}_p)$ است.

۳. گروه $\mathrm{Gal}(L:F)$ دوری است. داریم $\mathrm{Gal}(L:F) = \langle \sigma^n \rangle$ به طوری که $n = [F:\mathbb{Z}_p]$.

۵.۱ میدان‌های تام

تعریف ۱.۵.۱. میدان K را یک میدان تام [۹] می‌نامیم، هرگاه هر چندجمله‌ای تحویل‌ناپذیر روی K جدایی‌پذیر باشد.

بنا به تعریف فوق میدان K تام است اگروتنهااگر هر توسیع متناهی از آن، یک توسیع جدایی‌پذیر باشد. در لم ۲۳.۳.۱ دیدیم که اگر K یک میدان با مشخصه‌ی صفر و f یک چندجمله‌ای تحویل‌ناپذیر در $K[x]$ باشد. آنگاه f روی K جدایی‌پذیر است. بنابراین هر میدان با مشخصه‌ی صفر یک میدان تام است.

قضیه ۲.۵.۱. میدان K با مشخصه‌ی p تام است اگروتنهااگر نگاشت $x \to x^p$ روی K یک اتومرفیسم باشد.

اثبات. میدان K با مشخصه‌ی p را در نظر می‌گیریم. ابتدا فرض می‌کنیم K یک میدان تام است و نشان می‌دهیم نگاشت $x \to x^p$ روی K یک اتومرفیسم است. از آنجا که مشخصه‌ی میدان p است، به سادگی می‌توان دید نگاشت $x \to x^p$ روی K یک همریختی است. بنابراین کافی است نشان دهیم این نگاشت پوشا است. بدین منظور، عنصر دلخواه a متعلق به K را در نظر می‌گیریم. اثبات می‌کنیم که $b \in K$ موجود است به طوری که $b^p = a$.

قرار می‌دهیم $f = x^p - a$. از این رو $f' = px^{p-1}$. از طرفی مشخصه‌ی میدان p است. بنابراین $f' = 0$، پس بنا به لم ۲۲.۳.۱ چندجمله‌ای f ریشه‌ی تکراری دارد. اما بنا به فرض K یک میدان تام است؛ یعنی هر چندجمله‌ای تحویل‌ناپذیر روی K جدایی‌پذیر است. بنابراین از این‌که f ریشه‌ی تکراری دارد نتیجه می‌شود که f تحویل‌پذیر است، پس چندجمله‌ای‌های g و h متعلق به $K[X]$ موجود هستند به طوری که $f = gh$.

حال فرض می‌کنیم b یک ریشه برای چندجمله‌ای f باشد. در این صورت $b^n - a = 0$، پس $b^n = a$. همچنین می‌دانیم که b متعلق به بستار جبری K است. ادعا می‌کنیم $b \in K$. به منظور اثبات این ادعا توجه کنید که $f(x) = x^p - a$ و $b^n = a$. در نتیجه $f(x) = x^p - b^n$. حال از آنجا که مشخصه‌ی میدان، p است $f = x^p - b^n = (x-b)^p = gh$. بنابراین واضح است که $g = (x-b)^d$ به طوری که $0 < d < p$. همچنین از آنجا که $g \in K[X]$، ضرایب چندجمله‌ای $g = (x-b)^d = x^d - b^d$، از جمله b^d متعلق به K هستند. از طرفی p یک عدد اول است. بنابراین p و d نسبت به هم اول هستند. بنابراین دو عدد صحیح u و v وجود

[۹] perfect

دارند به طوری که $du+pv=1$. از این رو $b=b^{du+pv}=(b^d)^u(b^p)^v$. حال با توجه به این‌که b^p و b^d متعلق به K هستند و K یک میدان است داریم $(b^d)^u,(b^p)^v\in K$ و در نتیجه $b=(b^d)^u(b^p)^v\in K$.

برای اثبات جهت عکس قضیه فرض می‌کنیم نگاشت $x\to x^p$ روی K یک اتومرفیسم است. به برهان خلف فرض می‌کنیم میدان K تام نیست. در این صورت یک چندجمله‌ای تحویل‌ناپذیر f در $K[X]$ موجود است به طوری که جدایی‌پذیر نیست؛ یعنی f در بستار جبری K ریشه‌ی تکراری دارد، پس بنا به لم ۲۲.۳.۱ چندجمله‌ای f و f' ریشه‌ی مشترک دارند. فرض می‌کنیم α ریشه‌ی مشترک f و f' باشد. از این‌که f تحویل‌ناپذیر است نتیجه می‌شود f چندجمله‌ای مینیمال α است. اما درجه‌ی f' از درجه‌ی f کمتر است. بنابراین $f'\equiv 0$. توجه کنید که $f=a_0+a_1x^1+\cdots+a_nx^n$ و $f'=a_1+2a_2x+\cdots+na_nx^{n-1}$. در نتیجه برای هر $i=1,\dots,n$ اگر $p\nmid i$ داریم $a_i=0$. بنابراین بوضوح $f=a_0+a_px^p+a_{2p}x^{2p}+\cdots$. از طرفی نگاشت $x\to x^p$ روی K یک اتومرفیسم است. در نتیجه این نگاشت پوشاست، پس برای هر $a\in K$ عنصر $b\in K$ موجود است به طوری که $a=b^p$. بنابراین به طور خاص ضرایب چندجمله‌ای f نیز همین شرایط را دارند. از این رو $f=b_0^p+b_1^px^p+b_2^px^{2p}+\cdots$. حال از آنجا که مشخصه‌ی میدان p است داریم:

$$f=b_0^p+b_1^px^p+b_2^px^{2p}+\cdots=(b_0+b_1x+b_2x^2+\cdots)^p,$$

که با تحویل‌ناپذیر بودن f در تناقض است.

□

نتیجه ۳.۵.۱. یک میدان K تام است اگروتنهااگر یکی از موارد زیر برقرار باشد:

۱. مشخصه‌ی میدان K صفر باشد.

۲. مشخصه‌ی میدان K عدد اول p باشد و نگاشت $x\to x^p$ روی K یک اتومرفیسم باشد.

قضیه ۴.۵.۱. هر میدان متناهی تام است.

اثبات. فرض می‌کنیم K یک میدان متناهی باشد. در این صورت عدد اول p موجود است به طوری که $|K|=p^n$ و مشخصه‌ی میدان K برابر است با p. بنابراین به سادگی می‌توان دید نگاشت $x\to x^p$ یک همریختی است. ادعا می‌کنیم که نگاشت $x\to x^p$ روی K یک اتومرفیسم است. از آنجا که K یک میدان متناهی با اندازه‌ی p^n است، هر عنصر از این میدان ریشه‌ی چندجمله‌ای $x^{p^n}-x$ است. بنابراین برای هر عنصر a متعلق به K داریم $a^{p^n}=a$، پس $a=(a^{p^{n-1}})^p$). بنابراین نگاشت $x\to x^p$ پوشا است. از طرفی میدان K متناهی است. بنابراین از پوشا بودن این نگاشت می‌توان نتیجه گرفت که یک به یک نیز است. در نتیجه بنا به قضیه‌ی ۲.۵.۱ میدان K تام است. □

نتیجه ۵.۵.۱. هر میدان اول، تام است.

اثبات. میدان دلخواه K را در نظر می‌گیریم. دو حالت زیر ممکن است رخ بدهد:

۱. میدان K متناهی باشد: در این صورت عدد اول p و عدد طبیعی n موجود است به طوری که اندازه‌ی $|K| = p^n$. بنابراین میدان اول میدان K، میدان متناهی $\mathbb{F}_p$ است، پس بنا به قضیه‌ی ۴.۵.۱ میدان اول K تام است.

۲. میدان K نامتناهی باشد: در این صورت میدان اول میدان K، میدان $\mathbb{Q}$ است. از طرفی می‌دانیم که مشخصه‌ی میدان $\mathbb{Q}$ صفر است، پس بنا به نتیجه‌ی ۳.۵.۱ این میدان تام است.

□

در پایان این زیربخش نشان می‌دهیم که اگر K یک میدان تام باشد، مفاهیم جدایی‌پذیری و خالی از مربع بودن معادل هستند. معادل بودن این دو مفهوم را در بخش ۳.۴.۵ نیاز خواهیم داشت.

تعریف ۶.۵.۱. چندجمله‌ای $f(X) \in K[X]$ را خالی از مربع [۱۰] می‌گوییم هرگاه هیچ چندجمله‌ای غیرثابت h موجود نباشد به طوری که $h^2 \mid f$.

قضیه ۷.۵.۱. فرض کنید K یک میدان تام باشد. در این صورت چندجمله‌ای $f(X) \in K[X]$ جدایی‌پذیر است اگروتنهااگر خالی از مربع باشد.

اثبات. فرض می‌کنیم چندجمله‌ای f جدایی‌پذیر باشد. همچنین به برهان خلف فرض می‌کنیم f خالی از مربع نباشد. در این صورت چندجمله‌ای h موجود است به طوری که $h^2 \mid f$؛ یعنی f ریشه‌ی تکراری دارد و این با جدایی‌پذیر بودن f در تناقض است.

برای اثبات جهت عکس قضیه فرض می‌کنیم چندجمله‌ای f خالی از مربع باشد. همچنین به برهان خلف فرض می‌کنیم f دارای ریشه‌ی تکراری باشد. در این صورت بنا به لم ۲۷.۳.۱ داریم $\gcd(f, f') \neq 1$. بنابراین چندجمله‌ای تحویل‌ناپذیر $h \in K[X]$ موجود است به طوری‌که $h \mid f$ و $h \mid f'$. بنابراین چندجمله‌ای $g \in K[X]$ وجود دارد به طوری که $f = hg$ و $f' = h'g + g'h$. همچنین از این‌که h تحویل‌ناپذیر است و K یک میدان تام است نتیجه می‌شود که h جدایی‌پذیر است، پس بنا به لم ۲۷.۳.۱ داریم $\gcd(h, h') = 1$. از طرفی $h \mid f'$ بنابراین $h \nmid h'$، پس بوضوح $h \mid g$. از این رو $g = hs$. در نتیجه $f = h^2 s$؛ یعنی $h^2 \mid f$ که با خالی از مربع بودن f در تناقض است. □

[10] Square-free polynomial

خلاصه‌ی فصل:

توسیع‌های میدانی معرفی شده در این فصل به شرح زیر است:

۱. توسیع میدانی $K \subseteq L$ را متناهی می‌نامیم هرگاه L به یک عنوان فضای برداری روی K، دارای بُعد متناهی باشد.

۲. توسیع میدانی $K \subseteq L$ را یک توسیع جبری می‌نامیم هرگاه هر عنصر $\alpha \in L$ ریشه‌ی یک چندجمله‌ای با ضرایب در K باشد. هر توسیع متناهی یک توسیع جبری است.

۳. توسیع جبری $K \subseteq L$ را یک توسیع جدایی‌پذیر جبری می‌نامیم هرگاه هر عنصر $\alpha \in L$ ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر جدایی‌پذیر روی K باشد. توسیع میدانی (دلخواه، نه لزوماً جبری) $K \subseteq L$ را یک توسیع جدایی‌پذیر می‌نامیم هرگاه L و $K^{1/p^\infty} = \{a \in \tilde{K} \mid \exists b \in K\,, \exists m > 0 \quad a^{p^m} = b\}$ روی K مجزای خطی باشند.

۴. توسیع میدانی L روی K را منتظم می‌گوییم، هرگاه L و $\tilde{K}$ روی K مجزای خطی باشند.

۵. توسیع $K \subseteq L$ را یک توسیع نرمال می‌نامیم هرگاه هرچندجمله‌ای تحویل‌ناپذیر $f \in K[X]$ که در L یک ریشه دارد به طور کامل در L به عوامل درجه‌ی اول تجزیه شود.

۶. فرض کنید L یک میدان باشد و $H \subseteq \mathrm{Aut}(L)$، منظور از $\Phi(H)$ مجموعه‌ی $\{x \in L \mid \forall \sigma \in H \quad \sigma(x) = x\}$ است. فرض کنید $K \subseteq L$ یک توسیع میدانی و $\mathrm{Gal}(L : K)$ گروه گالوایی L روی K باشد. توسیع $K \subseteq L$ را یک توسیع گالوایی می‌نامیم هرگاه $\Phi(\mathrm{Gal}(L : K)) = K$. یک توسیع متناهی $K \subseteq L$ گالوایی است اگروتنها اگر نرمال و جدایی‌پذیر باشد.

هر توسیع گالوایی متناهی $K \subseteq L$ یک پایه‌ی نرمال دارد؛ یعنی $\alpha \in L$ موجود است به طوری که L روی K دارای یک پایه به صورت $\{g(\alpha) \mid g \in \mathrm{Gal}(L : K)\}$ است.

میدان K را تام می‌گوییم، هرگاه هر چندجمله‌ای تحویل‌ناپذیر روی K جدایی‌پذیر باشد. دیدیم که یک میدان K تام است اگروتنهااگر هر توسیع متناهی از آن، یک توسیع جدایی‌پذیر باشد.

فصل ۲

مقدمات نظریه‌ی مدل‌ها

در این فصل به صورت مختصر مقدماتی از نظریه‌ی مدل‌ها را یادآوری می‌کنیم. هدف اصلی این فصل اثبات حذف سور برای میدان‌های بسته‌ی جبری است که برای اثبات قضیه‌ی ریشه‌ها در بخش ۲.۲.۴ به آن نیاز خواهیم داشت. مطالب این فصل از منبع [۱۸] گرفته شده است.

در این فصل فرض می‌کنیم خواننده با برخی تعاریف و مفاهیم اولیه‌ی نظریه‌ی مدل‌ها، مانند تعریف یک زبان مرتبه‌ی اول، یک ساختار مرتبه‌ی اول، L فرمول‌ها و ... آشنایی دارد. برای مطالعه‌ی این تعاریف اولیه خواننده را به منبع [۱۸] ارجاع می‌دهیم.

۱.۲ تعاریف مقدماتی

در این فصل گاهی به جهت راحتی در نمایش، یک چندتایی را با پر رنگ نوشتن متغیر نشان می‌دهیم. برای مثال $x_1, \dots, x_n$ و $b_1, \dots, b_m$ را به ترتیب با نماد $\boldsymbol{x}$ و $\boldsymbol{b}$ نمایش می‌دهیم.

تعریف ۱.۱.۲. زبان مرتبه اول L را در نظر بگیرید. دو L ساختار $\mathfrak{M}$ و $\mathfrak{N}$ را هم ارز مقدماتی می‌گوییم و با نماد $\mathfrak{M} \equiv \mathfrak{N}$ نمایش می‌دهیم هرگاه برای هر L جمله‌ی φ داشته باشیم:

$$\mathfrak{M} \models \varphi \iff \mathfrak{N} \models \varphi.$$

تعریف ۲.۱.۲. زبان مرتبه اول L را در نظر بگیرید و فرض کنید $\mathfrak{N}$ و $\mathfrak{M}$ دو L ساختار باشند. می‌گوییم $\mathfrak{N}$

یک زیرساختار مقدماتی از $\mathfrak{M}$ است (یا $\mathfrak{M}$ یک توسیع مقدماتی از $\mathfrak{N}$ است) و آن را با نماد $\mathfrak{N} \prec \mathfrak{M}$ نمایش می‌دهیم هرگاه $\mathfrak{N} \subseteq \mathfrak{M}$ و برای هر L فرمول $\varphi(x_1, \ldots, x_n)$ و هر $a_1, \ldots, a_n \in N$ داشته باشیم:

$$\mathfrak{N} \models \varphi(a_1, \cdots, a_n) \iff \mathfrak{M} \models \varphi(a_1, \cdots, a_n).$$

فرض کنید L یک زبان مرتبه اول باشد. هر مجموعه از L جملات را یک تئوری مرتبه‌ی اول می‌نامیم.

تعریف ۳.۱.۲. فرض کنید $\mathfrak{M}$ یک L ساختار باشد. تئوری کامل $\mathfrak{M}$ را با $\mathrm{Th}(\mathfrak{M})$ نمایش می‌دهیم و به صورت زیر تعریف می‌کنیم:

$$\mathrm{Th}(\mathfrak{M}) = \{\varphi \mid \mathfrak{M} \models \varphi \text{ و } \varphi \text{ یک } L \text{ جمله است } \}.$$

بنا به تعریف فوق واضح است که برای هر L جمله‌ی φ داریم $\varphi \in \mathrm{Th}(\mathfrak{M})$ یا $\neg\varphi \in \mathrm{Th}(\mathfrak{N})$.

توجه ۴.۱.۲. فرض کنید L ساختارهای $\mathfrak{M}$ و $\mathfrak{N}$ هم ارز مقدماتی باشند. در این صورت برای هر $\varphi \in \mathrm{Th}(\mathfrak{M})$ داریم $\mathfrak{N} \models \varphi$. بنابراین $\mathrm{Th}(\mathfrak{M}) = \mathrm{Th}(\mathfrak{N})$.

تعریف ۵.۱.۲. یک L تئوری T را کامل گوییم هرگاه برای هر L جمله‌ی φ داشته باشیم $T \models \varphi$ یا $T \models \neg\varphi$. به بیان دیگر یک L تئوری T را کامل می‌نامیم هرگاه هر دو مدل $\mathfrak{N}, \mathfrak{M} \models T$ هم ارز مقدماتی باشند.

تعریف ۶.۱.۲. می‌گوییم مجموعه‌ی ناتهی A یک سامانه‌ی رفت و برگشتی از یکریختی‌های میان زیرساختارهای $\mathfrak{M}$ و $\mathfrak{N}$ است هرگاه برای هر یکریختی $f \in A$ داشته باشیم:

۱. برای هر $a \in M$ یک یکریختی $g \in A$ موجود باشد به طوری که $f \subseteq g$ و $a \in \mathrm{dom}(g)$.

۲. برای هر $b \in N$ یک یکریختی $h \in A$ موجود باشد به طوری که $f \subseteq h$ و $b \in \mathrm{Im}(h)$.

تعریف ۷.۱.۲. فرض کنید $\mathfrak{M}$ یک L ساختار و A یک زیرمجموعه از M باشد. در این صورت L ساختار تولید شده توسط A را به صورت زیر تعریف می‌کنیم:

$$\langle A \rangle = \{t^{\mathfrak{M}}(a_1, \cdots, a_n) \mid a_1, \cdots, a_n \in A \text{ و } t \text{ یک } L \text{ ترم است } \}$$

تعریف ۸.۱.۲. فرض کنید $\mathfrak{M}$ و $\mathfrak{N}$ دو L ساختار و A و B به ترتیب زیرمجموعه‌هایی از M و N باشند. تابع $H : A \to B$ را یک یکریختی جزئی می‌نامیم هرگاه

۱. برای هر نماد تابعی $g(x_1, \ldots, x_n) \in L$ و هر $a_1, \ldots, a_n, b \in A$ داشته باشیم:

$$\mathfrak{M} \models g^{\mathfrak{M}}(a_1, \cdots, a_n) = b \iff \mathfrak{N} \models g^{\mathfrak{N}}(H(a_1), \cdots, H(a_n)) = H(b)$$

۲. برای هر نماد ثابت $c \in L$ اگر $c^{\mathfrak{M}} \in A$ و $c^{\mathfrak{N}} \in B$، آنگاه $H(c^{\mathfrak{M}}) = c^{\mathfrak{N}}$،

۳. برای هر نماد رابطه‌ای $R \in L$ و هر $a_1, \ldots, a_n, b \in A$ داشته باشیم:

$$\mathfrak{M} \models R^{\mathfrak{M}}(a_1, \cdots, a_n) \iff \mathfrak{N} \models R^{\mathfrak{N}}(H(a_1), \cdots, H(a_n)).$$

تعریف ۹.۱.۲. زبان مرتبه اول L و مجموعه‌ی A را در نظر بگیرید. مجموعه‌ی جملات بدون سور با پارامتر در A را با $\mathrm{Diag}(A)$ نمایش می‌دهیم.

تعریف ۱۰.۱.۲. فرض کنید $\mathfrak{M}$ و $\mathfrak{N}$ دو ساختار مرتبه اول باشند به طوری که $\mathfrak{N} \subseteq \mathfrak{M}$. می‌گوییم ساختار $\mathfrak{N}$ در $\mathfrak{M}$ بسته‌ی وجودی است هرگاه برای هر فرمول بدون سور $\varphi(x_1, ..., x_n, y_1, ..., y_m)$ با پارامترهای $n_1, ..., n_m \in N$ داشته باشیم $\mathfrak{N} \models \exists \boldsymbol{y}\ \varphi(\boldsymbol{n}, \boldsymbol{y}) \Leftrightarrow \mathfrak{M} \models \exists \boldsymbol{y}\ \varphi(\boldsymbol{n}, \boldsymbol{y})$.

۲.۲ تایپ‌ها

تعریف ۱.۲.۲. فرض کنید $\mathfrak{M}$ یک L ساختار باشد. همچنین فرض کنید $A \subseteq M$ و $a_1, \cdots, a_n \in M$. تایپ $a_1, \cdots, a_n$ روی مجموعه‌ی A در ساختار $\mathfrak{M}$ را به صورت زیر تعریف می‌کنیم:

$$\mathrm{tp}^{\mathfrak{M}}(\tfrac{a_1, \cdots, a_n}{A}) =$$
$$\{\varphi(x_1, \cdots x_n, b_1, \cdots, b_m) \mid n, m \in \mathbb{N},\ b_i \in A,\ \mathfrak{M} \models \varphi(a_1, \cdots a_n, b_1, \cdots, b_m)\}.$$

به طور خاص اگر $A = \emptyset$ داریم $\mathrm{tp}^{\mathfrak{M}}(a_1, \ldots, a_n) = \{\varphi(x_1, \ldots x_n) \mid n \in \mathbb{N},\ \mathfrak{M} \models \varphi(a_1, \ldots a_n)\}$.

فرض کنید $\mathfrak{M}$ یک L ساختار باشد و $A \subseteq M$. همچنین فرض کنید $p(x_1, \ldots x_n)$ یک مجموعه از L فرمول ها با پارامتر در A باشند. می‌گوییم $p(x_1, \ldots x_n)$ یک تایپ کامل در $\mathfrak{M}$ با پارامترهای A است و می‌نویسیم $p(x_1, \ldots x_n) \in S_n^{\mathfrak{M}}$، هرگاه $p(x_1, \ldots x_n)$ ویژگی‌های زیر را داشته باشد:

۱. برای هر فرمول $\varphi(\boldsymbol{x}, \boldsymbol{a})$ که در آن $\boldsymbol{a} \in A$، داشته باشیم $\varphi(\boldsymbol{x}, \boldsymbol{a}) \in p(\boldsymbol{x})$ یا $\neg\varphi(\boldsymbol{x}, \boldsymbol{a}) \in p(\boldsymbol{x})$.

۲. برای هر تعداد متناهی فرمول $\varphi_1(\boldsymbol{x}, \boldsymbol{b_1}), \ldots, \varphi_k(\boldsymbol{x}, \boldsymbol{b_k})$ متعلق به $p(\boldsymbol{x})$، عنصری مانند $\boldsymbol{c} \in M$ موجود باشد به طوری که $\mathfrak{M} \models \varphi_1(\boldsymbol{c}, \boldsymbol{b_1}) \wedge \cdots \wedge \varphi_k(\boldsymbol{c}, \boldsymbol{b_k})$.

فرض کنید $\mathfrak{M}$ یک L ساختار باشد. همچنین فرض کنید $A \subseteq M$ و $\boldsymbol{b} \in M$. در این صورت $\mathrm{tp}^{\mathfrak{M}}(\frac{\boldsymbol{b}}{A})$ یک تایپ کامل است و بوضوح $tp^{\mathfrak{M}}(\frac{\boldsymbol{b}}{A})$ مجموعه‌ی همه‌ی ویژگی‌های $\boldsymbol{b}$ است.

لم ۲.۲.۲. فرض کنید $p(\boldsymbol{x}) \in S_n^{\mathfrak{M}}$. در این صورت یک توسیع مقدماتی $\mathfrak{M} \prec \mathfrak{N}$ و عناصر $\boldsymbol{a} \in N$ موجود است به طوری که $p(\boldsymbol{x}) = \mathrm{tp}^{\mathfrak{N}}(\frac{\boldsymbol{a}}{A})$.

اثبات. تئوری

$$T = \{\varphi(\boldsymbol{m}) \mid \boldsymbol{m} \in M,\ \mathfrak{M} \models \varphi(\boldsymbol{m})\} \cup p(\boldsymbol{c})$$

را در زبان $L = L_M \cup L_A \cup \boldsymbol{c}$ در نظر می‌گیریم. واضح است که هر بخش متناهی از تئوری فوق دارای مدل است. در واقع $\mathfrak{M}$ مدلی برای هر بخش متناهی از این تئوری است، پس بنا به فشردگی این تئوری دارای مدلی مانند $\mathfrak{N}$ است. توجه کنید که $\mathfrak{N}$ مدلی برای $\{\varphi(\boldsymbol{m})|\boldsymbol{m} \in M, \mathfrak{M} \models \varphi(\boldsymbol{m})\}$ است، پس یک توسیع مقدماتی برای $\mathfrak{M}$ است. همچنین $\boldsymbol{c}^{\mathfrak{M}} = \boldsymbol{a} \in N$ موجود است به طوری که $p(\boldsymbol{x}) = tp^{\mathfrak{N}}(\frac{\boldsymbol{a}}{A})$. □

تعریف ۳.۲.۲. فرض کنید $\mathfrak{M}$ یک L ساختار باشد. همچنین فرض کنید $A \subseteq M$ و $a_1, \ldots, a_n \in M$. تعریف می‌کنیم:

$$\mathrm{qftp}(\frac{a_1, \cdots, a_n}{A}) = \{\varphi(x_1, \cdots, x_n, \boldsymbol{b}) \mid \boldsymbol{b} \in A,\ \mathfrak{M} \models \varphi(\boldsymbol{a}, \boldsymbol{b}) \text{ و } \varphi \text{ یک فرمول بدون سور است}\}.$$

$\mathrm{qftp}(\frac{\boldsymbol{a}}{A})$ را تایپ بدون سور $a_1, \ldots, a_n$ روی A می‌نامیم. در واقع $\mathrm{qftp}(\frac{a_1, \cdots, a_n}{A})$ شامل همه‌ی ویژگی‌های بدون سور $a_1, \ldots, a_n$ است.

۳.۲ تعریف‌پذیری

تعریف ۱.۳.۲. فرض کنید $\mathfrak{M}$ یک ساختار مرتبه اول با جهان M باشد. یک مجموعه‌ی $X \subseteq M^n$ را تعریف‌پذیر توسط فرمول $\varphi(x_1, ..., x_n, y_1, ..., y_m)$ با پارامترهای $b_1, ..., b_m$ می‌نامیم هرگاه

$$X = \{(a_1, ..., a_n) \in M^n \mid \mathfrak{M} \models \varphi(a_1, ..., a_n, b_1, ..., b_m)\}.$$

اگر $b_1, ..., b_m \in A \subseteq M$ می‌گوییم X یک مجموعه‌ی تعریف‌پذیر با پارامترهایی در A است.

توجه ۲.۳.۲. ساختار $\mathfrak{M}$ با جهان M را در نظر بگیرید. فرض کنید X و Y دو مجموعه‌ی تعریف‌پذیر در $\mathfrak{M}$ باشند. در این صورت مجموعه‌های $X \cup Y$، $X \cap Y$ و X^c نیز تعریف‌پذیر است.

مثال ۳.۳.۲. در ساختار $(\mathbb{Z}, +, \cdot, ۰, ۱)$ مجموعه‌ی $X = \{(x, y)|x \leq y\}$ تعریف‌پذیر است. زیرا بنا به قضیه‌ی لاگرانژ عدد $x \in \mathbb{Z}$ مثبت است اگروتنهااگر $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ موجود باشند به طوری که $x = a_1^2 + a_2^2 + a_3^2 + a_4^2$. بنابراین داریم:

$$\{x \in \mathbb{Z} \mid x \geq ۰\} = \{x \in \mathbb{Z} \mid \exists a_1, a_2, a_3, a_4 \quad x = a_1^2 + a_2^2 + a_3^2 + a_4^2\}.$$

در نتیجه

$$X = \{(x, y) \mid \exists a_۱, a_۲, a_۳, a_۴ \quad y = x + a_۱^۲ + a_۲^۲ + a_۳^۲ + a_۴^۲\}.$$

مثال ۴.۳.۲. در ساختار $\mathfrak{R} = (\mathbb{R}, +, \cdot, ۰, ۱)$ مجموعه‌ی $X = \{(x, y) \mid x < y\}$ تعریف‌پذیر است. فرمول

$$\varphi(x, y) = \exists z\, (z \neq ۰ \wedge y = x + z^۲)$$

را در نظر بگیرید. واضح است که برای هر $a, b \in \mathbb{R}$ داریم $a < b$ اگروتنهااگر $\mathfrak{R} \models \varphi(a, b)$.

۴.۲ حذف سور

فرض کنید T یک تئوری مرتبه اول باشد. می‌گوییم T سورها را حذف می‌کند یا حذف سور دارد، هرگاه برای هر L فرمول $\varphi(\boldsymbol{x})$ یک L فرمول بدون سور $\psi(\boldsymbol{x})$ موجود باشد به طوری که $T \vdash (\varphi(\boldsymbol{x}) \longleftrightarrow \psi(\boldsymbol{x}))$. به بیان دیگر زمانی که تئوری T حذف سور دارد، اگر $\mathfrak{M} \models T$ آنگاه هر زیرمجموعه‌ی تعریف‌پذیر توسط یک فرمول بدون سور تعریف می‌شود. در این بخش با برخی از محک‌های حذف سور آشنا خواهیم شد.

در قضیه‌ی زیر نشان می‌دهیم که حذف سور یک ویژگی جبری برای تئوری‌هاست.

قضیه ۱.۴.۲. فرض کنید برای هر دو مدل $\mathfrak{M}, \mathfrak{N} \models T$ و هر زیرساختار مشترک $A \subseteq \mathfrak{M}, \mathfrak{N}$ و هر $a_۱, \cdots, a_n \in A$ داشته باشیم:

$$\mathfrak{M} \models \varphi(\boldsymbol{a}) \Longleftrightarrow \mathfrak{N} \models \varphi(\boldsymbol{a}).$$

در این صورت فرمول بدون سور $\psi(\boldsymbol{x})$ پیدا می‌شود به طوری که $T \vdash (\varphi(\boldsymbol{x}) \longleftrightarrow \psi(\boldsymbol{x}))$.

اثبات. قرار می‌دهیم:

$$\Gamma(\boldsymbol{x}) = \{\psi(\boldsymbol{x}) \mid T \vdash \varphi(\boldsymbol{x}) \to \psi(\boldsymbol{x}), \ \text{بدون سور است } \psi\ \}.$$

در واقع $\Gamma(\boldsymbol{x})$ مجموعه‌ی همه‌ی نتایج بدون سور فرمول $\varphi(\boldsymbol{x})$ است. ادعا می‌کنیم که $T \cup \Gamma(\boldsymbol{x}) \vdash \varphi(\boldsymbol{x})$. توجه کنید که در صورتی که این ادعا درست باشد بنا به قضیه‌ی فشردگی، تعداد متناهی تا فرمول $\psi_۱(\boldsymbol{x}), \cdots, \psi_n(\boldsymbol{x}) \in \Gamma(\boldsymbol{x})$ وجود دارند به طوری که $T \cup \{\psi_۱(\boldsymbol{x}), \cdots, \psi_n(\boldsymbol{x})\} \vdash \varphi(\boldsymbol{x})$. به بیان دیگر $T \vdash \psi_۱(\boldsymbol{x}) \wedge \cdots \wedge \psi_n(\boldsymbol{x}) \to \varphi(\boldsymbol{x})$ متناقض است. بنابراین $T \cup \{\psi_۱(\boldsymbol{x}), \cdots, \psi_n(\boldsymbol{x})\} \cup \neg\varphi(\boldsymbol{x})$. از طرفی $\varphi(\boldsymbol{x}) \to \psi_۱(\boldsymbol{x}) \wedge \cdots \wedge \psi_n(\boldsymbol{x})$. از این رو $T \vdash \varphi(\boldsymbol{x}) \leftrightarrow \psi_۱(\boldsymbol{x}) \wedge \cdots \wedge \psi_n(\boldsymbol{x})$. در نتیجه $\varphi(\boldsymbol{x})$ دارای معادل بدون سور است.

به منظور اثبات این ادعا به برهان خلف فرض می‌کنیم $T \cup \Gamma(\boldsymbol{x}) \cup \neg\varphi(\boldsymbol{x})$ سازگار باشد. در این صورت ساختار $\mathfrak{M}$ موجود است به طوری که $\mathfrak{M} \models T$ و عنصر $\boldsymbol{a} \in M$ موجود است به طوری که $\mathfrak{M} \models \Gamma(\boldsymbol{a})$ و $\mathfrak{M} \models \neg\varphi(\boldsymbol{a})$. حال ادعا می‌کنیم که ساختار $\mathfrak{N} \models T$ موجود است به طوری که $\langle \boldsymbol{a} \rangle \subseteq \mathfrak{N}$ و $\mathfrak{N} \models \varphi(\boldsymbol{a})$.

برای اثبات این ادعا نشان می‌دهیم تئوری $T^* = T \cup \varphi(\boldsymbol{a}) \cup \mathrm{Diag}\langle \boldsymbol{a} \rangle$ در زبان $L_{\langle a \rangle}$ سازگار است. به برهان خلف فرض می‌کنیم T^* ناسازگار باشد. در این صورت متناهی تا فرمول $\psi_1(\boldsymbol{a}), \cdots, \psi_n(\boldsymbol{a}) \in \mathrm{Diag}\langle \boldsymbol{a} \rangle$ موجود هستند به طوری که $T \vdash \varphi(\boldsymbol{a}) \to \bigvee \neg\psi_i(\boldsymbol{a})$. از این رو در زبان L داریم $T \vdash \varphi(\boldsymbol{x}) \to \bigvee \neg\psi_i(\boldsymbol{x})$. بنابراین $\bigvee \neg\psi_i(\boldsymbol{a}) \in \Gamma(\boldsymbol{x})$. حال از آنجا که $\mathfrak{M}$ مدلی برای $\Gamma(\boldsymbol{x})$ است، داریم $\mathfrak{M} \models \bigvee \neg\psi_i(\boldsymbol{a})$. از طرفی $\mathfrak{M} \models \bigwedge \psi_i(\boldsymbol{a})$ که این تناقض است. در نتیجه تئوری $T^* = T \cup \varphi(\boldsymbol{a}) \cup \mathrm{Diag}\langle \boldsymbol{a} \rangle$ در زبان $L_{\langle a \rangle}$ سازگار است.

فرض می‌کنیم $\mathfrak{N} \models T^*$. در این صورت $\langle \boldsymbol{a} \rangle \subseteq \mathfrak{N}$ و $\mathfrak{N} \models \varphi(\boldsymbol{a})$. از طرفی $\mathfrak{M} \models \neg\varphi(\boldsymbol{a})$ که با فرض

$$\mathfrak{M} \models \varphi(\boldsymbol{a}) \iff \mathfrak{N} \models \varphi(\boldsymbol{a})$$

در تناقض است. بنابراین $T \cup \Gamma(\boldsymbol{x}) \vdash \varphi(\boldsymbol{x})$.

□

با استقرا روی پیچیدگی فرمول‌ها به سادگی می‌توان دید که اگر فرمول‌های به صورت $\exists y\, \psi(\boldsymbol{x}, y)$ که در آن $\psi(\boldsymbol{x}, y)$ یک فرمول بدون سور است، نسبت به تئوری T معادل بدون سور باشند، آنگاه تئوری T حذف سور دارد. همچنین توجه کنید که هر فرمول بدون سور به صورت $\bigvee \bigwedge \varphi$ است به طوری که φ یک فرمول اتمی یا نقیض اتمی است. بنابراین برای این که یک تئوری T حذف سور داشته باشد، کافی است فرمول‌های به صورت $\exists y\, \psi(\boldsymbol{x}, y)$ به طوری که $\psi(\boldsymbol{x}, y) = \bigwedge$(اتمی یا نقیض اتمی) دارای معادل بدون سور باشند.

در نتیجه فرض کنید برای هر دو مدل $\mathfrak{M}, \mathfrak{N} \models T$ و هر زیرساختار مشترک $A \subseteq \mathfrak{M}, \mathfrak{N}$ و هر $a_1, \cdots, a_n \in A$ داشته باشیم:

$$\mathfrak{M} \models \exists y \varphi(y, \boldsymbol{a}) \iff \mathfrak{N} \models \exists y \varphi(y, \boldsymbol{a}).$$

در این صورت تئوری T حذف سور دارد. به بیان دیگر برای اثبات حذف سور باید نشان دهیم اگر یک دستگاه معادلات با ضرایب در A در $\mathfrak{M}$ جواب داشته باشد آنگاه در $\mathfrak{N}$ هم جواب دارد.

در ادامه محک‌هایی برای حذف سور ارائه می‌کنیم و آن‌ها را بدون اثبات می‌پذیریم.

گزاره ۲.۴.۲ (محک حذف سور)**.** تئوری T را در نظر بگیرید. فرض کنید $\mathfrak{M}, \mathfrak{N} \models T$. اگر هر یکریختی به صورت $\langle \boldsymbol{a} \rangle \cong \langle \boldsymbol{b} \rangle$ در یک سامانه‌ی رفت و برگشتی قرار گیرد آنگاه تئوری T سورها را حذف می‌کند.

به بیان دقیق‌تر تئوری T حذف سور دارد هرگاه برای هر دو مدل $\mathfrak{M}, \mathfrak{N} \models T$ و هر $\boldsymbol{a} \in M$ و $\boldsymbol{b} \in N$ اگر $\langle \boldsymbol{b} \rangle \cong \langle \boldsymbol{a} \rangle$ آنگاه توسیع‌های مقدماتی $M \prec M_1$ و $N \prec N_1$ موجود باشند و یک سامانه‌ی رفت و برگشتی شامل $\langle \boldsymbol{b} \rangle \cong \langle \boldsymbol{a} \rangle$ میان M_1 و N_1 برقرار باشد.

گزاره ۳.۴.۲. تئوری T حذف سور دارد اگروتنهااگر برای هر مدل $\mathfrak{M} \models T$ و هر زیرساختار $A \subseteq \mathfrak{M}$ تئوری

$$T^* = T \cup \mathrm{Diag}(A)$$

در زبان L_A یک تئوری کامل باشد.

تعریف ۴.۴.۲. فرض کنید T یک تئوری کامل در یک زبان مرتبه اول شمارا باشد. همچنین فرض کنید $\mathfrak{M} \models T$. می‌گوییم $\mathfrak{M}$ یک مدل κ اشباع است هرگاه برای هر مجموعه پارامتر $A \subseteq M$ به طوری که $|A| < \kappa$ و هر تایپ $p(\boldsymbol{x}) \in S_n^{\mathfrak{M}}(A)$، عنصری مانند $\boldsymbol{u} \in M$ پیدا شود که برای هر $\varphi \in p(\boldsymbol{x})$ داشته باشیم $\mathfrak{M} \models p(\boldsymbol{u})$. مدل $\mathfrak{M} \models T$ را اشباع می‌نامیم هرگاه $|M|$ اشباع باشد.
به طور خاص مدل $\mathfrak{M} \models T$ را $\aleph_0$ اشباع می‌نامیم هرگاه هر تایپ روی یک مجموعه‌ی متناهی A در $\mathfrak{M}$ برآورده شود.

گزاره ۵.۴.۲ (محک ون دن دریز)**.** تئوری T حذف سور دارد هرگاه برای هر $\mathfrak{M}, \mathfrak{N} \models T$ به طوری که $\mathfrak{N}$ یک مدل $|M|$ اشباع است و هر زیرساختار دلخواه $A \subseteq M$ اگر $f : A \to N$ یک نشاندن باشد، آنگاه f را بتوان به یک نشاندن $f_1 : M \to N$ توسیع داد.

تعریف ۶.۴.۲. تئوری T را مدل کامل می‌نامیم هرگاه برای هر $\mathfrak{M}, \mathfrak{N} \models T$ اگر $\mathfrak{M} \subseteq \mathfrak{N}$، آنگاه $\mathfrak{N}$ یک توسیع مقدماتی از $\mathfrak{M}$ باشد.

لم ۷.۴.۲. فرض کنید تئوری T سورها را حذف کند. در این صورت T مدل کامل است.

اثبات. فرض می‌کنیم $\mathfrak{M}, \mathfrak{N} \models T$ و $\mathfrak{M} \subseteq \mathfrak{N}$. می‌خواهیم نشان دهیم $\mathfrak{N}$ یک توسیع مقدماتی از $\mathfrak{M}$ است. در واقع باید نشان دهیم برای هر $\boldsymbol{m} \in M$ و هر فرمول $\varphi(\boldsymbol{x})$ داریم $\mathfrak{M} \models \varphi(\boldsymbol{m}) \iff \mathfrak{N} \models \varphi(\boldsymbol{m})$. فرض می‌کنیم $\mathfrak{M} \models \varphi(\boldsymbol{x})$. توجه کنید که تئوری T حذف سور دارد. بنابراین $T \models \varphi(\boldsymbol{x}) \longleftrightarrow \psi(\boldsymbol{x})$ به طوری که $\psi(\boldsymbol{x})$ بدون سور است. از این رو داریم :

$$\mathfrak{M} \models \varphi(\boldsymbol{m}) \iff \mathfrak{M} \models \psi(\boldsymbol{m}) \iff \mathfrak{N} \models \psi(\boldsymbol{m}) \iff \mathfrak{N} \models \varphi(\boldsymbol{m}).$$

□

۱.۴.۲ حذف سور میدان‌های بسته‌ی جبری

فرض کنید تئوری میدان‌ها را با $T_{\text{میدان‌ها}}$ نمایش دهیم و

$$\varphi_n = \forall a_0, \cdots, a_n \; \exists x \quad a_0 + a_1 x + \cdots + a_n x^n = 0.$$

در این صورت تئوری میدان‌های بسته‌ی جبری به صورت زیر است:

$$\mathrm{ACF} = T_{\text{میدان‌ها}} \cup \{\varphi_n\}_{n\in\mathbb{N}}$$

توجه کنید که تئوری ACF سازگار است. در واقع $(\mathbb{C}, +, -, \cdot, 0, 1) \models \mathrm{ACF}$.

در قضیه‌ی زیر اثبات می‌کنیم که تئوری میدان‌های بسته‌ی جبری با هر مشخصه‌ای، حذف سور دارد.

قضیه ۸.۴.۲. تئوری ACF حذف سور دارد.

اثبات. فرض می‌کنیم $\mathfrak{M}_1, \mathfrak{M}_2 \models \mathrm{ACF}$ و عناصر a و b به ترتیب متعلق به M_1 و M_2 هستند. همچنین فرض می‌کنیم $\langle b\rangle \cong \langle a\rangle$. باید نشان دهیم یکریختی $\langle b\rangle \cong \langle a\rangle$ در یک سامانه ی رفت و برگشتی قرار می‌گیرد. بدین منظور کمی کلی‌تر فرض می‌کنیم $\mathfrak{M}$ و $\mathfrak{M}'$ به ترتیب زیرساختارهایی از $\mathfrak{M}_1$ و $\mathfrak{M}_2$ باشند به طوری که $\mathfrak{M}' \cong \mathfrak{M}$. توجه کنید که $\mathfrak{M}$ و $\mathfrak{M}'$ حوزه‌ی صحیح هستند. اما می‌توانیم $\mathfrak{M}$ را در میدان کسرهای $\mathfrak{M}$ و $\mathfrak{M}'$ را در میدان کسرهای $\mathfrak{M}'$ بنشانیم. از آنجا که $\mathfrak{M}' \cong \mathfrak{M}$ میدان کسرهای آنها نیز به صورت یکتا ساخته می‌شوند و با هم یکریخت هستند. بنابراین بدون کاستن از کلیت فرض می‌کنیم $\mathfrak{M}$ و $\mathfrak{M}'$ میدان باشند. حال عنصر دلخواه $\alpha \in M_1 - M$ را در نظر می‌گیریم. دو حالت زیر ممکن است رخ دهد:

۱. عنصر α روی $\mathfrak{M}$ جبری باشد: فرض می‌کنیم $f \in \mathfrak{M}[X]$ چندجمله‌ای مینیمال α باشد. در این صورت بنا به لم ۴.۲.۱ داریم:

$$\mathfrak{M}(\alpha) \cong \frac{\mathfrak{M}[X]}{\langle f\rangle}.$$

از آنجا که $f \in \mathfrak{M}[X]$ یک چندجمله‌ای تحویل‌ناپذیر است، تصویر آن در $f \in \mathfrak{M}'[X]$ نیز تحویل‌ناپذیر است. فرض می‌کنیم $h \in \mathfrak{M}'[X]$ تصویر چندجمله‌ای $f \in \mathfrak{M}[X]$ باشد. از طرفی $\mathfrak{M}_2$ یک میدان بسته‌ی جبری است. بنابراین h در $\mathfrak{M}_2$ یک ریشه مانند β دارد. از این رو داریم:

$$\mathfrak{M}(\alpha) \cong \frac{\mathfrak{M}[X]}{\langle f\rangle} \cong \frac{\mathfrak{M}'[X]}{\langle h\rangle} \cong \mathfrak{M}(\beta).$$

۲. عنصر α روی $\mathfrak{M}$ متعالی باشد: در این حالت $\mathfrak{M}(\alpha) \cong \mathfrak{M}(X)$. کافی است یک عنصر متعالی $\beta \in \mathfrak{M}_2 - \mathfrak{M}'$ را به گونه‌ای بیابیم که β روی $\mathfrak{M}'$ متعالی باشد. در این صورت داریم

$$\mathfrak{M}(\alpha) \cong \mathfrak{M}(X) \cong \mathfrak{M}'(X) \cong \mathfrak{M}'(\beta).$$

ادعا می‌کنیم عنصر متعالی β موجود است. برای اثبات این ادعا باید عنصر $\beta \in M_۲ - M'$ به گونه‌ای بیابیم که ریشه‌ی هیچ چندجمله‌ای نباشد. توجه کنید که هر چندجمله‌ای، متناهی تا ریشه دارد و میدان $\mathfrak{M}_۲$ نامتناهی است. بنابراین هر تعداد متناهی چندجمله‌ای را که در نظر بگیریم عنصری وجود دارد که ریشه‌ی مشترک این چندجمله‌ای‌ها نیست، پس بنا به قضیه‌ی فشردگی و اشباع بودن $\mathfrak{M}_۲$ عنصر β با ویژگی‌های خواسته شده موجود است.

□

نتیجه ۹.۴.۲. تئوری ACF مدل کامل است.

خلاصه‌ی فصل:

فرض کنید $\mathfrak{M}$ یک L ساختار مرتبه‌ی اول با جهان M باشد. در این صورت منظور از یک L ساختار تولید شده توسط زیرمجموعه‌ی A از M، مجموعه‌ی $\langle A\rangle = \{t^{\mathfrak{M}}(a_۱, \cdots, a_n) \mid a_۱, \cdots, a_n \in M, t \text{ یک } L \text{ ترم است و } A \text{ است.}\}$ همچنین یک زیرمجموعه‌ی $X \subseteq M^n$ را تعریف‌پذیر توسط فرمول $\varphi(x_۱, ..., x_n, y_۱, ..., y_m)$ با پارامترهای $b_۱, ..., b_m$ می‌نامیم هرگاه $X = \{(a_۱, ..., a_n) \in M^n \mid \mathfrak{M} \models \varphi(a_۱, ..., a_n, b_۱, ..., b_m)\}$.

مجموعه‌ی ناتهی A یک سامانه‌ی رفت و برگشتی از یکریختی‌های میان زیرساختارهای $\mathfrak{M}$ و $\mathfrak{N}$ است هرگاه برای هر یکریختی $f \in A$ داشته باشیم:

۱. برای هر $a \in M$ یک یکریختی $g \in A$ موجود باشد به طوری که $f \subseteq g$ و $a \in \mathrm{dom}(g)$.

۲. برای هر $b \in N$ یک یکریختی $h \in A$ موجود باشد به طوری که $f \subseteq h$ و $b \in \mathrm{Im}(h)$.

سپس مفهوم حذف سور را بیان کردیم. تئوری مرتبه اول T سورها را حذف می‌کند یا حذف سور دارد، هرگاه برای هر L فرمول $\varphi(\boldsymbol{x})$ یک L فرمول بدون سور $\psi(\boldsymbol{x})$ موجود باشد به طوری که $T \vdash (\varphi(\boldsymbol{x}) \longleftrightarrow \psi(\boldsymbol{x}))$.

دیدیم یک محک برای حذف سور به صورت زیر است:

تئوری T حذف سور دارد هرگاه برای هر دو مدل $\mathfrak{M}, \mathfrak{N} \models T$ و هر $\boldsymbol{a} \in M$ و $\boldsymbol{b} \in N$ اگر $\langle \boldsymbol{a}\rangle \cong \langle \boldsymbol{b}\rangle$ آنگاه توسیع‌های مقدماتی $M \prec M_۱$ و $N \prec N_۱$ موجود باشند و یک سامانه‌ی رفت و برگشتی شامل $\langle \boldsymbol{a}\rangle \cong \langle \boldsymbol{b}\rangle$ میان $M_۱$ و $N_۱$ برقرار باشد. به کمک این محک اثبات کردیم که تئوری میدان‌های بسته‌ی جبری حذف سور دارد. همچنین اثبات کردیم که اگر تئوری T سورها را حذف کند، مدل کامل است؛ یعنی برای هر $\mathfrak{M}, \mathfrak{N} \models T$ اگر $\mathfrak{M} \subseteq \mathfrak{N}$ آنگاه $\mathfrak{N}$ یک توسیع مقدماتی از $\mathfrak{M}$ است و از حکم نتیجه گرفتیم که تئوری ACF مدل کامل است.

فصل ۳

میدان‌های ارزیابی

۱.۳ مقدمه

منظور از یک میدان ارزیابی، یک زوج (K, A) است به طوری که $A \subseteq K$ یک حلقه‌ی ارزیاب باشد؛ یعنی برای هر $x \in K$ یا $x \in A$ یا $x^{-1} \in A$. در این پایان‌نامه قصد داریم به تعریف‌پذیری حلقه‌ی ارزیاب A در میدان ارزیابی هنسلی K بپردازیم. بدین منظور، در این فصل میدان‌های ارزیابی و میدان‌های ارزیابی هنسلی را معرفی می‌کنیم. منابع این فصل برای بخش میدان‌های ارزیابی [۶] و برای بخش حلقه‌های موضعی [۱۶] هستند.

۲.۳ حلقه‌های موضعی

یکی از شروط معادل میدان بودن این است که تنها ایده‌آل ماکزیمال حلقه، ایده‌آل صفر باشد. یک شرط کمی ضعیف‌تر این است که حلقه، تنها یک ایده‌آل ماکزیمال داشته باشد. به چنین حلقه‌ای، حلقه‌ی موضعی می‌گوییم:

تعریف ۱.۲.۳. حلقه‌ی جابجایی و یکدار R را موضعی [1] می‌نامیم هرگاه تنها یک ایده‌آل ماکزیمال داشته باشد. ایده‌آل ماکزیمال R را با $\mathfrak{m}$ و این حلقه را به صورت $(R, \mathfrak{m})$ نمایش می‌دهیم.

قضیه ۲.۲.۳. اگر R یک حلقه‌ی جابجایی و یکدار باشد آنگاه موارد زیر با هم معادلند:

[1] Local ring

۱. R موضعی است،

۲. مجموعه عناصر غیر وارون‌پذیر R تشکیل ایده‌آل ماکزیمال می‌دهند،

۳. مجموعه عناصر غیر وارون‌پذیر R تحت عمل جمع بسته است.

اثبات. اثبات ۱ به ۲: فرض می‌کنیم $\mathfrak{m}$ ایده‌آل ماکزیمال حلقه‌ی R باشد. ثابت می‌کنیم $\mathfrak{m} = R - U(R)$. واضح است که عناصر $\mathfrak{m}$ وارون‌پذیر نیستند. زیرا اگر عناصر $\mathfrak{m}$ وارون داشته باشند، این ایده‌آل شامل عنصر یک خواهد بود و در نتیجه $\mathfrak{m}$ برابر با کل حلقه می‌شود. بنابراین $\mathfrak{m} \subseteq R - U(R)$.

حال فرض می‌کنیم $a \in R - U(R)$. از این‌که $a \notin U(R)$ نتیجه می‌گیریم ایده‌آل Ra در R یک ایده‌آل سره است. از طرفی هر ایده‌آل سره زیرمجموعه‌ی یک ایده‌آل ماکزیمال است. بنابراین با توجه به این که فقط یک ایده‌آل ماکزیمال داریم، $Ra \subseteq \mathfrak{m}$. در نتیجه $a \in \mathfrak{m}$، پس $R - U(R) \subseteq \mathfrak{m}$.

اثبات ۲ به ۳: چون $R - U(R)$ یک ایده‌آل است، پس واضح است که تحت عمل جمع بسته است.

اثبات ۳ به ۱: فرض می‌کنیم برای هر $a, b \in R - U(R)$ داریم $a + b \in R - U(R)$. ثابت می‌کنیم $R - U(R)$ یک ایده‌آل است. عناصر $a, b \in R - U(R)$ را در نظر می‌گیریم. ادعا می‌کنیم $a \cdot b \in R - U(R)$. به منظور اثبات این ادعا به برهان خلف فرض می‌کنیم $a \cdot b \notin R - U(R)$. در این صورت $a \cdot b \in U(R)$. بنابراین a وارون‌پذیر است و این تناقض است. از طرفی هر عنصر دلخواه $a \in U(R)$ وارون‌پذیر است، پس $U(R)$ نمی‌تواند شامل یک ایده‌آل ماکزیمال باشد. بنابراین $R - U(R)$ تنها ایده‌آل ماکزیمال R است و در نتیجه R موضعی است.

□

تعریف ۳.۲.۳ (حلقه‌ی هنسلی). فرض کنید $(R, \mathfrak{m})$ یک حلقه‌ی موضعی باشد. حلقه‌ی R را یک حلقه‌ی موضعی هنسلی می‌نامیم هرگاه برای هر $f \in R[x]$ داشته باشیم: اگر $\alpha \in R$ موجود باشد به طوری که $f(\alpha) \in \mathfrak{m}$ و $f'(\alpha) \notin \mathfrak{m}$ آنگاه $a \in R$ موجود باشد که $f(a) = 0$ و $a \equiv_{\mathfrak{m}} \alpha$.

در ادامه حلقه‌ی هنسلی را به نحوی دیگر تعریف می‌کنیم:

فرض کنید $(R, \mathfrak{m})$ یک حلقه‌ی موضعی باشد و میدان $F = R/\mathfrak{m}$ را در نظر بگیرید. برای هر $\alpha \in R$ تصویر کانونی α در F را با $\bar{\alpha}$ نمایش می‌دهیم. تصویر یک چندجمله‌ای $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ متعلق به $R[x]$، در $F[x]$ به صورت $\bar{f}(x) = \bar{a_0} + \bar{a_1} x + \ldots + \bar{a_n} x^n$ است.

حلقه‌ی R را یک حلقه‌ی موضعی هنسلی می‌نامیم هرگاه برای هر $f \in R[x]$، اگر $\alpha \in R$ موجود باشد به طوری که $\bar{f}(\bar{\alpha}) = 0$ و $\bar{f}'(\bar{\alpha}) \neq 0$ آنگاه عنصر $a \in R$ موجود باشد به طوری که $f(a) = 0$ و $\bar{a} = \bar{\alpha}$.

۳.۳ میدان‌های ارزیابی

۱.۳.۳ نگاشت ارزیابی

تعریف ۱.۳.۳. فرض کنید Γ یک گروه آبلی مرتب و K یک میدان باشد. نگاشت $v : K \to \Gamma \cup \{\infty\}$ را یک نگاشت ارزیابی می‌نامیم هرگاه برای هر $x, y \in K$ موارد زیر بر قرار باشد:

۱. $v(x+y) \geq \min\{v(x), v(y)\}$،

۲. $v(x \cdot y) = v(x) + v(y)$،

۳. $x = ۰ \Leftrightarrow v(x) = \infty$.

نتیجه ۲.۳.۳. اگر v یک نگاشت ارزیابی باشد، موارد زیر به صورت مستقیم از تعریف نتیجه می‌شوند:

۱. $v(۱) = v(-۱) = ۰$.

۲. برای هر $x \in K$، داریم $v(x) = v(-x)$،

۳. برای هر $x \in K$، داریم $v(x^{-۱}) = -v(x)$.

اثبات. ۱. واضح است که $v(۱) = v(۱ \cdot ۱) = v(۱) + v(۱)$. کافی است طرفین را منهای $v(۱)$ کنیم. در این صورت داریم $v(۱) = ۰$. از طرفی $v(۱) = v((-۱) \cdot (-۱)) = v(-۱) + v(-۱)$، پس $v(-۱) + v(-۱) = ۰$. بنابراین با توجه به این که گروه ارزیاب مرتب است از این که $v(-۱) + v(-۱) = ۰$ نتیجه می‌شود $v(-۱) = ۰$.

۲. می‌دانیم $v(-x) = v((-۱) \cdot x) = v(-۱) + v(x)$. از طرفی $v(-۱) = ۰$، پس $v(-x) = v(x)$.

۳. می‌دانیم $v(x \cdot x^{-۱}) = v(۱) = ۰$. از طرفی $v(x \cdot x^{-۱}) = v(x) + v(x^{-۱})$، پس $v(x) + v(x^{-۱}) = ۰$. در نتیجه $v(x^{-۱}) = -v(x)$.

□

لم ۳.۳.۳. گروه آبلی مرتب Γ و میدان K را در نظر بگیرید. همچنین فرض کنید نگاشت $v : K \to \Gamma \cup \{\infty\}$ یک نگاشت ارزیابی باشد. در این صورت اگر برای عناصر $x, y \in K$ داشته باشیم $v(x) \neq v(y)$ آنگاه $v(x+y) = \min\{v(x), v(y)\}$.

اثبات. فرض می‌کنیم $v(x) > v(y)$. در این صورت $\min\{v(x), v(y)\} = v(y)$، پس

$$v(x+y) \geq \min\{v(x), v(y)\} = v(y).$$

از طرفی $v(y) = v(x+y-x) \geq \min\{v(x+y), v(-x)\} = \min\{v(x+y), v(x)\}$. بنابراین

$$v(x+y) \geq v(y) \geq \min\{v(x+y), v(x)\}.$$

حال ادعا می‌کنیم $\min\{v(x+y), v(x)\} = v(x+y)$. به جهت اثبات این ادعا به برهان خلف فرض می‌کنیم $\min\{v(x+y), v(x)\} = v(x)$، پس داریم $v(x+y) \geq v(y) \geq v(x)$ که با فرض $v(x) > v(y)$ در تناقض است. در نتیجه $v(x+y) \geq v(y) \geq \min\{v(x+y), v(x)\} = v(x+y)$. بنابراین $v(y) = v(x+y)$.
□

۲.۳.۳ حلقه‌های ارزیاب

تعریف ۴.۳.۳. فرض کنید K یک میدان، Γ یک گروه آبلی مرتب و $v : K \to \Gamma \cup \{\infty\}$ یک نگاشت ارزیابی باشد. حلقه‌ی ارزیاب نظیر نگاشت v را با $\mathcal{O}_v$ نمایش داده و به صورت زیر تعریف می‌کنیم:

$$\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}.$$

توجه ۵.۳.۳. برای هر عنصر $x \in K$ داریم $x \in \mathcal{O}_v$ یا $x^{-1} \in \mathcal{O}_v$. زیرا اگر $x \notin \mathcal{O}_v$ آنگاه $v(x) < 0$. بنابراین $v(x^{-1}) = -v(x) > 0$. در نتیجه $x^{-1} \in \mathcal{O}_v$.

لم ۶.۳.۳. فرض کنید K یک میدان، Γ یک گروه آبلی مرتب و $v : K \to \Gamma \cup \{\infty\}$ یک نگاشت ارزیابی باشد. در این صورت حلقه‌ی ارزیاب $\mathcal{O}_v \subseteq K$، یک حلقه‌ی موضعی است و ایده‌آل ماکزیمال آن به صورت زیر است:

$$\mathfrak{m}_v = \{x \in K \mid v(x) > 0\}.$$

اثبات. بنا به تعریف، $\mathcal{O}_v$ یک زیرمجموعه از میدان K است. ادعا می‌کنیم که برای هر دو عنصر دلخواه $a, b \in \mathcal{O}_v$ داریم $a - b, a \cdot b \in \mathcal{O}_v$. به جهت اثبات این ادعا ابتدا توجه کنید که $v(a-b) \geq \min\{v(a), v(-b)\}$ و $v(a), v(-b) \geq 0$. از این رو $v(a-b) \geq 0$. بنابراین $a - b \in \mathcal{O}_v$. از طرفی $v(a \cdot b) = v(a) + v(b)$ و $v(a), v(b) \geq 0$. بنابراین $v(a \cdot b) = v(a) + v(b) \geq 0$. در نتیجه $a \cdot b \in \mathcal{O}_v$. از این رو $\mathcal{O}_v$ یک زیرحلقه از میدان K است.

حال باید اثبات کنیم که $\mathcal{O}_v$ یک حلقه‌ی موضعی با ایده‌آل ماکزیمال $\mathfrak{m}_v$ است. بدین منظور کافی است نشان دهیم $\mathfrak{m}_v$ از عناصر غیر وارون‌پذیر $\mathcal{O}_v$ تشکیل شده و یک ایده‌آل است. عنصر دلخواه $x \in \mathcal{O}_v$ را در نظر

می‌گیریم. دو حالت زیر ممکن است رخ دهد. یا $x \in \mathcal{O}_v$ به گونه‌ای است، $v(x) = 0$ که در این حالت $v(x^{-1})$ نیز صفر خواهد بود و در نتیجه x^{-1} متعلق به $\mathcal{O}_v$ است. یا $v(x) > 0$. در این صورت داریم $v(x^{-1}) < 0$. بنابراین x^{-1} متعلق به $\mathcal{O}_v$ نیست. بنابراین عناصر غیر وارون پذیر $\mathcal{O}_v$ دقیقاً عناصری هستند که مقدار نگاشت ارزیابی در آن‌ها اکیداً بزرگتر از صفر باشد. به بیان دیگر $\mathfrak{m}_v$ مجموعه عناصر غیر وارون‌پذیر $\mathcal{O}_v$ است. حال عناصر دلخواه $a, b \in \mathfrak{m}_v$ و $r \in \mathcal{O}_v$ را در نظر می‌گیریم، داریم :

۱. $a - b \in \mathfrak{m}_v$: زیرا $v(a - b) \geq \min\{v(a), v(-b)\}$ و $v(a), v(-b) > 0$. بنابراین $v(a - b) \geq \min\{v(a), v(-b)\} > 0$. در نتیجه $a - b \in \mathfrak{m}_v$.

۲. $a \cdot b \in \mathfrak{m}_v$: زیرا $v(a \cdot b) = v(a) + v(b)$ و $v(a), v(b) > 0$، پس $v(a \cdot b) = v(a) + v(b) > 0$.

۳. $r \cdot a \in \mathfrak{m}_v$: زیرا $v(r \cdot a) = v(r) + v(a)$. از طرفی $v(r) \geq 0$ و $v(a) > 0$. بنابراین $v(r \cdot a) = v(r) + v(a) > 0$. در نتیجه $r \cdot a \in M_v$.

بنابراین $\mathfrak{m}_v$ یک ایده‌آل از $\mathcal{O}_v$ است.

□

تعریف ۷.۳.۳. میدان $F = \frac{\mathcal{O}_v}{\mathfrak{m}_v}$ را میدان باقیمانده‌های نگاشت ارزیابی v می‌نامیم.

تعریف ۸.۳.۳ (حلقه‌ی ارزیاب)**.** حلقه‌ی A در میدان K را یک حلقه‌ی ارزیاب برای K می‌نامیم هرگاه برای هر $x \in K$ داشته باشیم $x \in A$ یا $x^{-1} \in A$.

فرض کنید K یک میدان، Γ یک گروه آبلی مرتب و $v : K \to \Gamma \cup \{\infty\}$ یک نگاشت ارزیابی باشد. در توجه ۵.۳.۳ دیدیم که برای هر عنصر $x \in K$ داریم $x \in \mathcal{O}_v$ یا $x^{-1} \in \mathcal{O}_v$. بنابراین $\mathcal{O}_v$ یک حلقه‌ی ارزیاب است. در قضیه‌ی زیر نشان می‌دهیم که هر حلقه‌ی ارزیاب به صورت یک $\mathcal{O}_v$ است.

قضیه ۹.۳.۳. هر حلقه‌ی ارزیاب از یک نگاشت ارزیابی ناشی می‌شود. به بیان دیگر اگر K یک میدان شامل حلقه‌ی ارزیاب A باشد، آنگاه یک گروه مرتب مانند Γ و یک ارزیابی $v : K \to \Gamma \cup \{\infty\}$ وجود دارد به طوری که $A = \mathcal{O}_v$.

اثبات. روی عناصر K رابطه‌ی هم‌ارزی زیر را در نظر می‌گیریم:

$$x \sim y \Leftrightarrow xy^{-1} \in A,\ yx^{-1} \in A.$$

در واقع داریم $x \sim y$ اگروتنهااگر $xy^{-1} \in U(A)$. مجموعه $\Gamma = \{[x]_\sim : x \in K\}$ همرا با عمل ضرب میدان یک گروه است. بنابراین $\Gamma = \frac{K/\{0\}}{U(A)}$. حال روی Γ ترتیب زیر را تعریف می‌کنیم:

$$[x]_\sim > [y]_\sim \Leftrightarrow xy^{-1} \in A,\ yx^{-1} \notin A$$

و

$$[x]_\sim = [y]_\sim \Leftrightarrow xy^{-1} \in A,\ yx^{-1} \in A$$

در این صورت نگاشت $v : K \to \Gamma \cup \{\infty\}$ با ضابطه‌ی $v(x) = [x]_\sim$ یک نگاشت ارزیابی است و داریم

$$\mathcal{O}_v = \{x \in K \mid v(x) \geq 0_\Gamma\} = \{x \in K \mid v(x) \geq v(1_K)\} = \{x \in K \mid x \in A\} = A.$$

□

توجه ۱۰.۳.۳. نگاشت ارزیابی معرفی شده در قضیه‌ی ۹.۳.۳ یکتا است.

نتیجه ۱۱.۳.۳. اگر K یک میدان و $A \subseteq K$ یک حلقه‌ی ارزیاب باشد، آنگاه A یک حلقه‌ی موضعی است.

این فصل را با تعاریف میدان ارزیابی و میدان ارزیابی هنسلی به پایان می‌بریم:

تعریف ۱۲.۳.۳. زوج (K, A) را یک میدان ارزیابی می‌نامیم، هرگاه $A \subseteq K$ یک حلقه‌ی ارزیاب باشد.

تعریف ۱۳.۳.۳. میدان ارزیابی (K, A) را هنسلی می‌نامیم، هرگاه حلقه‌ی A هنسلی باشد.

خلاصه‌ی فصل:

حلقه‌ی جابجایی و یکدار R را موضعی می‌نامیم، هرگاه تنها یک ایده‌آل ماکزیمال داشته باشد. حلقه‌ی موضعی R یک حلقه‌ی موضعی هنسلی است، هرگاه برای هر $f \in R[x]$ داشته باشیم: اگر $\alpha \in R$ موجود باشد به طوری که $\bar{f}(\bar{\alpha}) = 0$ و $\bar{f}'(\bar{\alpha}) \neq 0$، آنگاه عنصر $a \in R$ موجود باشد به طوری که $f(a) = 0$ و $\bar{a} = \bar{\alpha}$.

زیرحلقه‌ی A از میدان K را یک حلقه‌ی ارزیاب برای K می‌نامیم، هرگاه برای هر $x \in K$ داشته باشیم $x \in A$ یا $x^{-1} \in A$. همچنین اگر $A \subseteq K$ یک حلقه‌ی ارزیاب باشد، زوج (K, A) را یک میدان ارزیابی می‌نامیم. فرض کنید Γ یک گروه آبلی مرتب و K یک میدان باشد. نگاشت $v : K \to \Gamma \cup \{\infty\}$ یک نگاشت ارزیابی است، هرگاه برای هر $x, y \in K$ موارد زیر برقرار باشد:

۱. $v(x + y) \geq \min\{v(x), v(y)\}$،

۲. $v(x \cdot y) = v(x) + v(y)$،

۳. $x = 0 \Leftrightarrow v(x) = \infty$.

مجموعه‌ی $\mathcal{O}_v = \{x \in K : v(x) \geq 0\}$ یک حلقه‌ی موضعی با ایده‌آل ماکزیمال $\mathfrak{m}_v = \{x \in K | v(x) > 0\}$ و همچنین $\mathcal{O}_v$ یک حلقه‌ی ارزیاب است. در پایان این فصل دیدیم که هر حلقه‌ی ارزیاب از یک نگاشت ارزیابی ناشی می‌شود. به بیان دیگر اگر K یک میدان شامل حلقه‌ی ارزیاب A باشد، آنگاه یک گروه مرتب مانند Γ و یک ارزیابی $v : K \to \Gamma \cup \{\infty\}$ وجود دارد به طوری که $A = \mathcal{O}_v$.

فصل ۴

میدان‌های شبه‌بسته‌ی جبری

۱.۴ مقدمه

منظور از یک میدان شبه‌بسته‌ی جبری میدانی مانند K است که هر واریته‌ی تعریف شده روی آن، در خود میدان K یک ریشه داشته باشد. در این فصل ابتدا مقدماتی از هندسه جبری مانند: تعریف یک مجموعه‌ی جبری، واریته و واریته‌ی تعریف شده روی یک میدان را یادآوری و سپس اثبات خواهیم کرد که یک میدان K، شبه‌بسته‌ی جبری است اگروتنهااگر هر چندجمله‌ای مطلقاً تحویل‌ناپذیر $f \in K[X,Y]$ در K^2 حداقل یک ریشه داشته باشد. برای مطالعه‌ی مبسوط درباره‌ی مطالب این فصل، منابع [۹] و [۱۷] و [۲۱] را پیشنهاد می‌کنیم.

۲.۴ مقدماتی از هندسه جبری

در سرتاسر این فصل فرض کرده‌ایم که K یک میدان و Ω یک توسیع بسته‌ی جبری از K است، به طوری که درجه‌ی تعالی آن روی K نامتناهی است. همچنین هر میدان دیگری که در این فصل نام برده می‌شود، یک توسیع میدانی از میدان K و زیرمیدانی از Ω است، مگر این‌که غیر از این تصریح شود.

در این فصل گاهی n تایی‌ها را با پر رنگ نوشتن متغیر نمایش می‌دهیم. برای مثال $(x_1, \cdots, x_n)$ را با $\boldsymbol{x}$ نمایش می‌دهیم.

۱.۲.۴ مجموعه‌های جبری

منظور از فضای آفین n تایی A^n، مجموعه‌ی همه‌ی n تایی‌های $\boldsymbol{x} = (x_1, ..., x_n)$ است به طوری که برای هر $i = 1, ..., n$ داریم $x_i \in \Omega$. بنابراین $A^n = \{(x_1, ..., x_n) \mid x_i \in \Omega\}$.

تعریف ۱.۲.۴. برای هر زیرمجموعه‌ی دلخواه $\boldsymbol{a} \subseteq K[\boldsymbol{X}] = K[X_1, ..., X_n]$، مجموعه‌ی جبری تولید شده توسط $\boldsymbol{a}$ را به صورت زیر تعریف می‌کنیم:

$$V(\boldsymbol{a}) = \{\boldsymbol{x} \in A^n \mid \forall f \in \boldsymbol{a} \quad f(\boldsymbol{x}) = 0\}.$$

به عنوان مثال واضح است که برای توابع ثابت یک و صفر به ترتیب داریم $V(\{1\}) = \emptyset$ و $V(\{0\}) = A^n$.

تعریف ۲.۲.۴. مجموعه‌ی دلخواه X را یک مجموعه‌ی جبری می‌نامیم هرگاه $\boldsymbol{a} \subseteq K[\boldsymbol{X}]$ موجود باشد به طوری که $X = V(\boldsymbol{a})$.

لم ۳.۲.۴. فرض کنید $\boldsymbol{a}_1 \subseteq \boldsymbol{a}_2 \subseteq K[\boldsymbol{X}]$. در این صورت $V(\boldsymbol{a}_2) \subseteq V(\boldsymbol{a}_1)$.

اثبات. فرض می‌کنیم $\boldsymbol{x} \in V(\boldsymbol{a}_2)$. در این صورت برای هر $f \in \boldsymbol{a}_2$ داریم $f(\boldsymbol{x}) = 0$. از طرفی $\boldsymbol{a}_1 \subseteq \boldsymbol{a}_2$، پس بوضوح برای هر $g \in \boldsymbol{a}_1$ نیز داریم $g(\boldsymbol{x}) = 0$. بنابراین $\boldsymbol{x} \in V(\boldsymbol{a}_1)$.

□

یادآوری می‌کنیم که رادیکال یک ایده‌آل I در یک حلقه‌ی R به صورت زیر تعریف می‌شود:

$$\sqrt{I} = \{r \in R \mid \exists n \in \mathbb{Z}^+ \quad r^n \in I\}.$$

همچنین ایده‌آل I را یک ایده‌آل رادیکال می‌نامیم هرگاه $I = \sqrt{I}$.

لم ۴.۲.۴. برای هر زیرمجموعه‌ی $A \subseteq A^n$ مجموعه‌ی

$$I_K(A) = \{f \in K[\boldsymbol{X}] \mid \forall \boldsymbol{x} \in A \quad f(\boldsymbol{x}) = 0\}$$

یک ایده‌آل رادیکال در حلقه‌ی $K[\boldsymbol{X}]$ است.

اثبات. ابتدا نشان می‌دهیم $I_K(A)$ یک ایده‌آل در حلقه‌ی $K[\boldsymbol{X}]$ است. بدین منظور، کافی است اثبات کنیم که شرایط زیر برقرار هستند:

۱. برای هر $f_2 \in I_K(A)$ و f_1 داریم $f_1 - f_2 \in I_K(A)$ و $f_1 f_2 \in I_K(A)$،

۲. برای هر $f \in I_K(A)$ و هر $g \in K[\boldsymbol{X}]$ داریم $fg \in I_K(A)$.

فرض می‌کنیم $f_۱, f_۲ \in I_K(A)$. بنابراین برای هر $\boldsymbol{x}$ متعلق به A داریم $f_۱(\boldsymbol{x}) = f_۲(\boldsymbol{x}) = ۰$. در نتیجه برای هر $\boldsymbol{x}$ متعلق به A داریم $f_۱(\boldsymbol{x}) - f_۲(\boldsymbol{x}) = ۰$. همچنین از این‌که $K[\boldsymbol{X}]$ یک حلقه است و $f_۱, f_۲$ به این حلقه تعلق دارند؛ نتیجه می‌شود که $f_۱ - f_۲ \in K[\boldsymbol{X}]$. بنابراین $f_۱ - f_۲ \in I_K(A)$. به طور مشابه می‌توان اثبات کرد که $f_۱ f_۲ \in I_K(A)$.

به جهت اثبات برقراری شرط دوم فرض می‌کنیم $f \in I_K(A)$ و $g \in K[\boldsymbol{X}]$. بنابراین برای هر $\boldsymbol{x}$ متعلق به مجموعه‌ی جبری A داریم $f(\boldsymbol{x}) = ۰$، پس بوضوح $f(\boldsymbol{x})g(\boldsymbol{x}) = ۰$.

حال می‌خواهیم اثبات کنیم ایده‌آل $I_K(A)$ یک ایده‌آل رادیکال است. بدین منظور باید نشان دهیم $I_K(A) = \sqrt{I_K(A)}$. توجه شود که بوضوح $I_K(A) \subseteq \sqrt{I_K(A)}$. بنابراین کافی است نشان دهیم $\sqrt{I_K(A)} \subseteq I_K(A)$. فرض می‌کنیم $f \in \sqrt{I_K(A)}$، پس عدد طبیعی $n \in \mathbb{N}$ موجود است به طوری که $f^n \in I_K(A)$. یعنی برای هر $\boldsymbol{x}$ متعلق به A داریم $f^n(\boldsymbol{x}) = ۰$ و در نتیجه $f(\boldsymbol{x}) = ۰$. بنابراین $f \in I_K(A)$. □

تعریف ۵.۲.۴. برای هر زیرمجموعه‌ی $A \subseteq A^n$، ایده‌آل رادیکال $I_K(A)$ را ایده‌آل وابسته به A می‌نامیم و گاهی به اختصار آن را با نماد $I(A)$ نمایش می‌دهیم.

لم ۶.۲.۴. دو زیرمجموعه‌ی $A_۲$ و $A_۱$ از A^n را در نظر بگیرید. موارد زیر برقرار هستند:

۱. اگر $A_۱ \subseteq A_۲$ آنگاه $I(A_۲) \subseteq I(A_۱)$،

۲. $I(A_۱ \cup A_۲) = I(A_۱) \cap I(A_۲)$.

اثبات. ۱. فرض می‌کنیم $A_۱ \subseteq A_۲$ و عنصر دلخواه $f \in I(A_۲)$ را در نظر می‌گیریم. برای هر $\boldsymbol{x} \in A_۲$ داریم $f(\boldsymbol{x}) = ۰$. از طرفی $A_۱ \subseteq A_۲$، پس برای هر $\boldsymbol{x} \in A_۱$ نیز داریم $f(\boldsymbol{x}) = ۰$. بنابراین $f \in I(A_۱)$ و در نتیجه $I(A_۲) \subseteq I(A_۱)$.

۲. ابتدا اثبات می‌کنیم که $I(A_۱ \cup A_۲) \subseteq I(A_۱) \cap I(A_۲)$. بدین منظور فرض می‌کنیم $f \in I(A_۱ \cup A_۲)$. بنابراین برای هر $\boldsymbol{x}$ متعلق به $A_۱ \cup A_۲$ داریم $f(\boldsymbol{x}) = ۰$. از طرفی $A_۱, A_۲ \subseteq A_۱ \cup A_۲$، پس برای هر $\boldsymbol{x}$ متعلق به $A_۱$ و هر $\boldsymbol{x'}$ متعلق به $A_۲$ داریم $f(\boldsymbol{x}) = f(\boldsymbol{x'}) = ۰$. بنابراین $f \in I(A_۱)$ و $f \in I(A_۲)$. در نتیجه $f \in I(A_۱) \cap I(A_۲)$.

حال کافی است اثبات کنیم $I(A_۱) \cap I(A_۲) \subseteq I(A_۱ \cup A_۲)$. بدین منظور فرض می‌کنیم f یک چندجمله‌ای متعلق به $I(A_۱) \cap I(A_۲)$ باشد. در این صورت $f \in I(A_۱)$ و $f \in I(A_۲)$. بنابراین برای هر $\boldsymbol{x}$ متعلق به $A_۱$ و برای هر $\boldsymbol{x'}$ متعلق به $A_۲$ داریم $f(\boldsymbol{x}) = f(\boldsymbol{x'}) = ۰$، پس برای هر $\boldsymbol{x}$ متعلق به $A_۱ \cup A_۲$ داریم $f(\boldsymbol{x}) = ۰$. در نتیجه $f \in I(A_۱ \cup A_۲)$.

□

لم ۷.۲.۴. زیرمجموعه‌ی $\boldsymbol{a}$ از $K[\boldsymbol{X}]$ را در نظر بگیرید و فرض کنید $V = V(\boldsymbol{a})$. در این صورت داریم $V = V(I(V))$.

اثبات. ابتدا توجه شود که بوضوح $\boldsymbol{a} \subseteq I(V)$. بنابراین طبق لم ۳.۲.۴ داریم $V(I(V)) \subseteq V(\boldsymbol{a})$. از طرفی بنا به تعریف، $I(V) = \{f \mid \forall x \in V(\boldsymbol{a}) \quad f(\boldsymbol{x}) = ۰\}$. بنابراین واضح است که $V(\boldsymbol{a}) \subseteq V(I(V))$. در نتیجه $V(\boldsymbol{a}) = V(I(V))$. □

۲.۲.۴ قضیه‌ی ریشه‌های هیلبرت

زیرمجموعه‌ی $\boldsymbol{a}$ از $K[\boldsymbol{X}]$ را در نظر بگیرید. فرض کنید $V = V(\boldsymbol{a})$ یک مجموعه‌ی جبری باشد. دیدیم که $V = V(I(V))$، پس به طور کلی می‌توانیم بگوییم هر مجموعه‌ی جبری از یک ایده‌آل رادیکال ناشی می‌شود. در این زیربخش نشان خواهیم داد که در واقع هر مجموعه‌ی جبری با یک ایده‌آل رادیکال در تناظر یک به یک است. یعنی ایده‌آل رادیکالی که V از آن ناشی می‌شود یکتاست (۲۶.۲.۴).

تعریف ۸.۲.۴ (حلقه‌ی نوتری). حلقه‌ی R را نوتری می‌نامیم هرگاه هیچ زنجیر صعودی و نامتناهی از ایده‌آل‌های آن وجود نداشته باشد.

به بیان دیگر اگر R یک حلقه‌ی نوتری باشد، برای هر زنجیر صعودی و نامتناهی $I_۱ \subseteq I_۲ \subseteq \cdots$ از ایده‌آل‌های آن، عدد طبیعی $n \in \mathbb{N}$ موجود است به طوری که $I_n = I_{n+۱} = \cdots$.

نتیجه ۹.۲.۴. فرض کنید K یک میدان باشد. در این صورت K نوتری است.

قضیه ۱۰.۲.۴. حلقه‌ی R نوتری است اگروتنهااگر هر ایده‌آل در R متناهیاً تولید شده باشد. به بیان دیگر موارد زیر معادل هستند:

۱. هر ایده‌آل در R متناهیاً تولید شده است.

۲. هر دنباله‌ی صعودی از ایده‌آل‌ها در R ایستا است.

اثبات. اثبات ۱ به ۲: فرض می‌کنیم زنجیر $I_۱ \subseteq I_۲ \subseteq \cdots$ یک زنجیر از ایده‌آل‌ها در حلقه‌ی R باشد. در این صورت $\bigcup I_i$ یک ایده‌آل است. از طرفی بنا به فرض همه‌ی ایده‌آل‌ها متناهیاً تولید شده هستند، پس ایده‌آل $\bigcup I_i$ نیز متناهیاً تولید شده است. بنابراین $\bigcup I_i = \langle a_۰, ..., a_n \rangle$ است. واضح است که یک ایده‌آل I_k متعلق به زنجیر $I_۱ \subseteq I_۲ \subseteq \cdots$ موجود است به طوری که $a_۰, ..., a_n \in I_k$، یعنی $\bigcup I_i = I_k$، پس $I_k = I_{k+۱} = I_{k+۲} = \cdots$.

اثبات ۲ به ۱: حلقه‌ی نوتری R را در نظر می‌گیریم و به برهان خلف فرض می‌کنیم ایده‌آل I از R متناهیاً تولید شده نباشد. عنصر دلخواه $a_0 \in I$ را در نظر می‌گیریم؛ از آنجا که ایده‌آل I متناهیاً تولید شده نیست داریم $I \neq \langle a_0 \rangle$. بنابراین عنصر a_1 متعلق به ایده‌آل I موجود است به طوری که $\langle a_0 \rangle \subset \langle a_0, a_1 \rangle$. با ادامه‌ی روند فوق به یک زنجیر نا ایستا $\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle \subset \cdots$ از ایده‌آل‌ها خواهیم رسید که با فرض ما در تناقض است. □

قضیه ۱۱.۲.۴. (قضیه‌ی پایه‌ای هیلبرت) فرض کنید R نوتری باشد. در این صورت $R[X]$ نوتری است.

اثبات. با توجه به قضیه‌ی ۱۰.۲.۴ کافی است نشان دهیم هر ایده‌آل I در حلقه‌ی $R[X]$ متناهیاً تولید شده است. به برهان خلف فرض می‌کنیم ایده‌آل $I \in R[X]$ متناهیاً تولید شده نباشد. یک چندجمله‌ای $f_0 \in I$ با درجه‌ی مینیمال انتخاب می‌کنیم. در این صورت واضح است که $I \neq \langle f_0 \rangle$. فرض می‌کنیم $f_1 \in I - \langle f_0 \rangle$ یک چندجمله‌ای با حداقل درجه باشد. به طور مشابه $I \neq \langle f_0, f_1 \rangle$. بنابراین عنصر $f_2 \in I - \langle f_0, f_1 \rangle$ را با حداقل درجه انتخاب می‌کنیم. با ادامه‌ی این روند دنباله‌ی $f_0, f_1, \cdots$ از چندجمله‌ای ها ایجاد می‌گردد. بوضوح درجه‌ی چندجمله‌ای انتخاب شده در هر مرحله از درجه‌ی چندجمله‌ای انتخاب شده در مرحله‌ی قبل بیشتر است. در هر مرحله از روند فوق، ضریب بزرگترین جمله در چندجمله‌ای انتخاب شده را در نظر می‌گیریم و فرض می‌کنیم $a_0, a_1, a_2, \ldots$ دنباله‌ای از این ضرایب باشد. در این صورت ایده‌آل تولید شده توسط $a_0, a_1, a_2, \cdots$، یعنی $I' = \langle a_0, a_1, a_2, \cdots \rangle$ یک ایده‌آل در R است. از طرفی R یک حلقه‌ی نوتری است. در نتیجه I' متناهیاً تولید شده است؛ یعنی $I' = \langle a_0, a_1, a_2, \cdots, a_n \rangle$. بنابراین ضریب بزرگترین جمله در چندجمله‌ای f_{n+1}، یعنی a_{n+1} به صورت $r_0 a_0 + r_1 a_1 + \cdots + r_n a_n$ است، پس می‌توانیم یک ترکیب خطی مانند $\sum_{i=1}^{n} h_i f_i$ را به گونه‌ای بسازیم که درجه‌ی چندجمله‌ای $H = f_{n+1} - \sum_{i=1}^{n} h_i f_i$ از درجه‌ی چندجمله‌ای f_{n+1} کمتر باشد. از طرفی چندجمله‌ای H متعلق به $I - \langle f_0, \cdots, f_n \rangle$ است و این با انتخاب f_{n+1} به عنوان چندجمله‌ای با حداقل درجه در تناقض است.

□

نتیجه ۱۲.۲.۴. اگر K یک میدان باشد، آنگاه $K[\boldsymbol{X}]$ یک حلقه‌ی نوتری است.

بنا به آنچه که تا اینجا گفته شد، اگر K یک میدان باشد، هر ایده‌آل در $K[\boldsymbol{X}]$ متناهیاً تولید شده است.

لم ۱۳.۲.۴. ایده‌آل $\boldsymbol{a}$ در $K[\boldsymbol{X}]$ را در نظر بگیرید. فرض کنید $\boldsymbol{a} = \langle f_1, f_2, \cdots, f_n \rangle$ در این صورت $V(\boldsymbol{a}) = V(\{f_1, f_2, \cdots, f_n\})$.

اثبات. ابتدا اثبات می‌کنیم $V(\boldsymbol{a}) \subseteq V(\{f_1, f_2, \cdots, f_n\})$. بدین منظور فرض می‌کنیم $\boldsymbol{x} \in V(\boldsymbol{a})$. در این صورت به ازای هر $f \in \boldsymbol{a}$ داریم $f(\boldsymbol{x}) = 0$. از طرفی $\boldsymbol{a}$ ایده‌آل تولید شده توسط $\{f_1, \cdots, f_n\}$

است؛ یعنی $\{f_۱,\cdots,f_n\}\subseteq \boldsymbol{a}$. بنابراین برای هر $f\in\{f_۱,\cdots,f_n\}$ نیز داریم $f(\boldsymbol{x})=۰$. در نتیجه $\boldsymbol{x}\in V(\{f_۱,\cdots,f_n\})$.

حال کافی است اثبات کنیم $V(\{f_۱,\cdots,f_n\})\subseteq V(\boldsymbol{a})$. عنصر دلخواه $\boldsymbol{x}$ متعلق به $V(\{f_۱,\cdots,f_n\})$ را در نظر می‌گیریم. برای هر $f_i\in\{f_۱,\cdots,f_n\}$ داریم $f_i(\boldsymbol{x})=۰$. از طرفی $\boldsymbol{a}$ ایده‌آل تولید شده توسط $\{f_۱,\cdots,f_n\}$ است. بنابراین واضح است که برای هر $g\in\boldsymbol{a}$ داریم $g(\boldsymbol{x})=r_۱f_۱(\boldsymbol{x})+\cdots+r_nf_n(\boldsymbol{x})=۰$، پس $\boldsymbol{x}\in V(\boldsymbol{a})$. □

تا اینجا دیدیم که هر مجموعه‌ی جبری V از ایده‌آل رادیکال $I(V)$ ناشی می‌شود؛ یعنی $V=V(I(V))$. از طرفی $I(V)$ یک ایده‌آل متناهیاً تولید شده است. در نتیجه $I(V)=\langle f_۱,\cdots,f_n\rangle$، پس $V=V(\{f_۱,\cdots,f_n\})$.

تعریف ۱۴.۲.۴. فرض کنید R یک حلقه‌ی دلخواه باشد. ایده‌آل $I\subseteq R$ را تحویل‌ناپذیر می‌نامیم هرگاه برای هر $I_۱,I_۲\neq I$ داشته باشیم $I\neq I_۱\cap I_۲$.

در قضیه‌ی زیر اثبات می‌کنیم که در حلقه‌های نوتری هر ایده‌آل را می‌توان به ایده‌آل‌های تحویل‌ناپذیر تجزیه کرد.

قضیه ۱۵.۲.۴. اگر R یک حلقه‌ی نوتری و $I\subseteq R$ یک ایده‌آل باشد آنگاه عدد طبیعی $n\in\mathbb{N}$ موجود است به طوری که $I=I_۱\cap I_۲\cap\ldots\cap I_n$ و I_i ها تحویل‌ناپذیر هستند.

اثبات. فرض می‌کنیم I تحویل‌پذیر باشد. در این صورت $I_۱,I_۲\subseteq R$ وجود دارند به طوری که $I=I_۱\cap I_۲$. سپس $I_۱$ و $I_۲$ را بررسی می‌کنیم؛ در صورتی که $I_۱$ یا $I_۲$ تحویل‌پذیر باشند، مشابه مرحله‌ی قبل آنها را تجزیه می‌کنیم. ادعا می‌کنیم که این روند پس از متناهی مرحله متوقف می‌شود. به بیان دیگر پس از متناهی مرحله ایده‌آل I به طور کامل تجزیه می‌شود. به منظور اثبات این ادعا توجه کنید که با تکرار روند فوق، یک زنجیر صعودی به صورت $I'\subseteq I'_۱\subseteq I'_۲\subseteq\cdots$ ایجاد می‌گردد. واضح است که $\bigcup I_i$ یک ایده‌آل در حلقه‌ی R است. از طرفی R یک حلقه‌ی نوتری است. بنابراین ایده‌آل $\bigcup I_i$ و در نتیجه زنجیر $I'\subseteq I'_۱\subseteq I'_۲\subseteq\cdots$ متناهیاً تولید شده است؛ یعنی این زنجیر پس از متناهی مرحله متوقف می‌شود.

□

یادآوری می‌کنیم که یک ایده‌آل I اولیه است؛ هرگاه به ازای هر a و b متعلق به I، اگر $ab\in I$ آنگاه $a\in I$ یا $b\in\sqrt{I}$. همچنین واضح است که اگر ایده‌آل I اولیه باشد، آنگاه $\sqrt{I}$ اول است.

قضیه ۱۶.۲.۴. فرض کنید R یک حلقه‌ی نوتری باشد. در این صورت هر ایده‌آل تحویل‌ناپذیر I، اولیه است.

اثبات. فرض می‌کنیم ایده‌آل I در حلقه‌ی R تحویل‌ناپذیر است. برای اثبات این‌که I یک ایده‌آل اولیه است، ابتدا اثبات می‌کنیم که اگر ایده‌آل $\langle ۰ \rangle$ تحویل‌ناپذیر باشد آنگاه اولیه است. سپس حلقه‌ی نوتری R/I را در نظر می‌گیریم. از آنجا که ایده‌آل $\langle ۰ \rangle$ در حلقه‌ی R/I همان ایده‌آل I در حلقه‌ی R است، از اولیه بودن ایده‌آل $\langle ۰ \rangle$ در حلقه‌ی R/I، نتیجه می‌گیریم I در حلقه‌ی R اولیه است.

حال فرض می‌کنیم ایده‌آل $\langle ۰ \rangle$ تحویل‌ناپذیر باشد. همچنین فرض می‌کنیم عنصر ab متعلق به ایده‌آل $\langle ۰ \rangle$ است، ولی a به این ایدآل تعلق ندارد. کافی است نشان دهیم عدد طبیعی $n \in \mathbb{N}$ به گونه‌ای موجود است که b^n متعلق به رادیکال $\langle ۰ \rangle$ است. به بیان دیگر فرض می‌کنیم $a \neq ۰$ و $a \cdot b = ۰$. نشان می‌دهیم عدد طبیعی $n \in \mathbb{N}$ به گونه‌ای موجود است که $b^n = ۰$. به برهان خلف فرض می‌کنیم برای هر عدد طبیعی $n \in \mathbb{N}$ داریم $b^n \neq ۰$. زنجیر $\cdots \subseteq \{x \mid xb^۲ = ۰\} \subseteq \{x \mid xb = ۰\}$ از ایده‌آل را در نظر می‌گیریم. از آنجا که حلقه‌ی R نوتری است هر زنجیر از ایده‌آل‌ها از جمله زنجیر $\cdots \subseteq \{x \mid xb^۲ = ۰\} \subseteq \{x \mid xb = ۰\}$ ایستا است. بنابراین عدد طبیعی $n \in \mathbb{N}$ موجود است به طوری که $\{x \mid xb^n = ۰\} = \{x \mid xb^{n+۱} = ۰\} = \cdots$؛ یعنی برای هر x داریم $xb^n = ۰$ اگروتنها اگر $xb^{n+۱} = ۰$. حال ادعا می‌کنیم که در این صورت داریم $\langle a \rangle \cap \langle b^n \rangle = ۰$.

به منظور اثبات این ادعا عنصر دلخواه t متعلق به $\langle a \rangle \cap \langle b^n \rangle$ را در نظر می‌گیریم. بنابراین $r, r' \in R$ به گونه‌ای موجود است که $t = ra$ و $t = r'b^n$. از طرفی $tb = r'b^{n+۱} = ۰$؛ زیرا $t = ra$، پس $tb = rab$. طبق فرض داریم $ab = ۰$ در نتیجه $tb = r'b^{n+۱} = ۰$. بنابراین با توجه به این‌که برای هر x داریم $xb^n = ۰$ اگروتنها اگر $xb^{n+۱} = ۰$، از این‌که $r'b^{n+۱} = ۰$ نتیجه می‌شود $t = r'b^n = ۰$. بنابراین $\langle a \rangle \cap \langle b^n \rangle = ۰$ که با فرض تحویل‌ناپذیر بودن ایده‌آل $\langle ۰ \rangle$ در تناقض است.

حال ایده‌آل تحویل‌ناپذیر I در حلقه‌ی R و حلقه‌ی R/I را در نظر می‌گیریم. ایده‌آل $\langle ۰ \rangle$ در حلقه‌ی R/I تحویل‌ناپذیر و در نتیجه اولیه است. بنابراین ایده‌آل I در حلقه‌ی R اولیه است. □

لم ۱۷.۲.۴. فرض کنید R یک حلقه‌ی دلخواه، I و J دو ایده‌آل در R باشند. در این صورت داریم $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

اثبات. ابتدا نشان می‌دهیم $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. بدین منظور عنصر دلخواه $f \in \sqrt{I \cap J}$ را در نظر می‌گیریم. بنا به تعریف ایده‌آل رادیکال، عدد طبیعی $n \in \mathbb{N}$ به گونه‌ای موجود است که $f^n \in I \cap J$. بنابراین $f^n \in I$ و $f^n \in J$، پس $f \in \sqrt{I}$ و $f \in \sqrt{J}$ در نتیجه $f \in \sqrt{I} \cap \sqrt{J}$.

حال فرض می‌کنیم $f \in \sqrt{I} \cap \sqrt{J}$. بنابراین $f \in \sqrt{I}$ و $f \in \sqrt{J}$؛ یعنی اعداد طبیعی $n, m \in \mathbb{N}$ به گونه‌ای موجود هستند که $f^n \in I$ و $f^m \in J$. از طرفی با توجه به این‌که I و J ایده‌آل‌هایی در حلقه‌ی R هستند، بوضوح $f^n f^m = f^{n+m} \in I$ و $f^n f^m = f^{n+m} \in J$. بنابراین $f^{n+m} \in I \cap J$ از این رو $f \in \sqrt{I \cap J}$.
□

نتیجه ۱۸.۲.۴. فرض کنید R نوتری و I یک ایده‌آل رادیکال باشد. در این صورت I به عوامل اول تجزیه می‌شود.

اثبات. فرض می‌کنیم I یک ایده‌آل رادیکال در حلقه‌ی نوتری R باشد. بنا به قضیه‌ی ۱۵.۲.۴ ایده‌آل I را می‌توان به عوامل تحویل‌ناپذیر تجزیه کرد. بنابراین طبق قضیه‌ی ۱۶.۲.۴ داریم $I = I_1 \cap I_2 \cap ... \cap I_n$ به طوری I_i ها ایده‌آل اولیه هستند. حال از آنجا که رادیکال یک ایده‌ال اولیه، اول است کافی است نشان دهیم $I = \sqrt{I} = \sqrt{I_1} \cap \sqrt{I_2} \cap ... \cap \sqrt{I_n}$. توجه کنید که I یک ایده‌آل رادیکال است، بنابراین $I = \sqrt{I}$، پس بنا به لم ۱۷.۲.۴ داریم $I = \sqrt{I} = \sqrt{I_1} \cap \sqrt{I_2} \cap ... \cap \sqrt{I_n}$.

□

در قضیه‌ی زیر اثبات می‌کنیم که اگر $\boldsymbol{a} \subseteq K[\boldsymbol{X}]$ یک ایده‌آل باشد و $\boldsymbol{a} \neq K[\boldsymbol{X}]$ آنگاه $V(\boldsymbol{a})$ تهی است.

قضیه ۱۹.۲.۴. فرض کنید K یک میدان و $\boldsymbol{a}$ ایده‌آل تولید شده توسط $f_1(\boldsymbol{X}), \cdots, f_m(\boldsymbol{X}) \in K[\boldsymbol{X}]$ باشد. همچنین فرض کنید $\boldsymbol{a} \neq K[\boldsymbol{X}]$. در این صورت $x_1, \cdots, x_n \in \tilde{K}$ موجود است به طوری که برای هر $i = 1, \cdots, m$ داریم $f_i(\boldsymbol{x}) = 0$.

اثبات. به کمک لم زرن می‌توان اثبات کرد که ایده‌آل ماکزیمال $\mathfrak{m}$ به گونه‌ای موجود است که $\boldsymbol{a} \subset \mathfrak{m}$. میدان $F = \frac{K[\boldsymbol{X}]}{\mathfrak{m}}$ را در نظر می‌گیریم. فرض می‌کنیم $\mathfrak{m} = \{f_1, \cdots, f_k\}$. در این صورت $F \models \exists \boldsymbol{x} \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) = 0$. زیرا برای هر $f_i \in \mathfrak{m}$ داریم $f_i(\boldsymbol{x} + \mathfrak{m}) = 0$. بنابراین در بستار جبری F نیز $\tilde{F} \models \exists \boldsymbol{x} \bigwedge_{i=1}^{n} f_i(\boldsymbol{x}) = 0$. از طرفی تئوری میدان‌های بسته‌ی جبری مدل کامل است، پس $\tilde{K}$ به طور مقدماتی در $\tilde{F}$ می‌نشیند. در نتیجه $\tilde{K} \models \exists \boldsymbol{x} \bigwedge_{i=1}^{n} f_i(\boldsymbol{x}) = 0$.

□

عکس نقیض قضیه‌ی ۱۹.۲.۴ را در نتیجه‌ی زیر بیان می‌کنیم.

نتیجه ۲۰.۲.۴. فرض کنید K یک میدان و $\boldsymbol{a}$ ایده‌آل تولید شده توسط $f_1(\boldsymbol{X}), \cdots, f_m(\boldsymbol{X}) \in K[\boldsymbol{X}]$ باشد. اگر $f_1(\boldsymbol{X}), \cdots, f_m(\boldsymbol{X})$ هیچ ریشه‌ی مشترکی در $\tilde{K}$ نداشته باشند، آنگاه $\boldsymbol{a} = K[\boldsymbol{X}]$. به بیان دیگر اگر $V(\boldsymbol{a})$ ناتهی باشد آنگاه $\boldsymbol{a} = K[X]$.

نتیجه ۲۱.۲.۴. میدان K و چندجمله‌ای $f \in K[X]$ را در نظر بگیرید. اگر f در $\tilde{K}$ ریشه نداشته باشد، آنگاه $\langle f \rangle = K[X]$.

در قضیه‌ی ۱۹.۲.۴ دیدیم که اگر $\boldsymbol{a} \subseteq K[\boldsymbol{X}]$ یک ایده‌آل باشد و $\boldsymbol{a} \neq K[\boldsymbol{X}]$ آنگاه $V(\boldsymbol{a})$ ناتهی است. در لم زیر کلی‌تر نشان می‌دهیم که اگر $g \notin I$ آنگاه $\boldsymbol{x} \in V(I)$ موجود است که $g(\boldsymbol{x}) \neq 0$.

لم ۲۲.۲.۴. فرض کنید K یک میدان و $\boldsymbol{a}$ ایده‌آل تولید شده توسط $f_1, \cdots, f_m \in K[\boldsymbol{X}]$ باشد. همچنین چندجمله‌ای $g \in K[\boldsymbol{X}]$ را به گونه‌ای در نظر بگیرید که برای هر $\boldsymbol{x} \in \tilde{K}$ اگر $f_1(\boldsymbol{x}) = \cdots = f_m(\boldsymbol{x}) = 0$ آنگاه $g(\boldsymbol{x}) = 0$. در این صورت توانی از g عضو ایده‌آل $\boldsymbol{a}$ است. به بیان دیگر اگر $g \in I(V(\boldsymbol{a}))$، آنگاه $g \in \sqrt{\boldsymbol{a}}$.

اثبات. بدون کاستن از کلیت فرض می‌کنیم $g \neq 0$. متغیر جدید Y و چندجمله‌ای جدید $1 - Yg(\boldsymbol{X})$ را در نظر می‌گیریم. واضح است که چندجمله‌ای‌های $f_1(\boldsymbol{X}), \cdots, f_m(\boldsymbol{X}), 1 - Yg(\boldsymbol{X}) \in K[\boldsymbol{X}, Y]$ هیچ ریشه‌ی مشترکی در $\tilde{K}^{n+1}$ ندارند، پس بنا به نتیجه‌ی ۲۰.۲.۴ $\langle f_1(\boldsymbol{X}), \cdots, f_m(\boldsymbol{X}), 1 - Yg(\boldsymbol{X})\rangle = K[\boldsymbol{X}, Y]$. بنابراین عناصر $a_1, \cdots, a_m, b \in K[\boldsymbol{X}, Y]$ موجود هستند به طوری که

$$1 = \sum_{i=1}^{m} a_i(\boldsymbol{X}, Y) f_i(\boldsymbol{X}) + b(\boldsymbol{X}, Y)(1 - Yg(\boldsymbol{X})).$$

حال اگر به جای متغیر Y چندجمله‌ای $g(\boldsymbol{X})^{-1}$ را قرار دهیم، داریم $1 = \sum_{i=1}^{m} a_i(\boldsymbol{X}, g(\boldsymbol{X})^{-1}) f_i(\boldsymbol{X})$. بنابراین برای هر عدد طبیعی r که از درجه‌ی Y، در هر یک از $a_i(\boldsymbol{X}, Y)$ بزرگتر است، یعنی $r \leq \max_{1 \leq i \leq m} \deg_Y a_i(\boldsymbol{X}, Y)$ داریم $g(\boldsymbol{X})^r = \sum_{i=1}^{m} g(\boldsymbol{X})^r a_i(\boldsymbol{X}, g(\boldsymbol{X})^{-1}) f_i(\boldsymbol{X})$. واضح است که $g(\boldsymbol{X})^r a_i(\boldsymbol{X}, g(\boldsymbol{X})^{-1}) \in K[\boldsymbol{X}]$، پس $g(\boldsymbol{X})^r \in \boldsymbol{a}$.

□

در اثبات قضیه‌ی فوق r را به این علت بزرگتر از درجه‌ی Y در هر یک از $a_i(\boldsymbol{X}, Y)$ ها در نظر گرفتیم که $g(\boldsymbol{X})^{-1}$ عضو میدان $K(\boldsymbol{X})$ است و لزوماً در $K[\boldsymbol{X}]$ قرار ندارد. از طرفی برای این‌که $g(\boldsymbol{X})^r$ عضو $\boldsymbol{a}$ باشد لازم است $g(\boldsymbol{X})^r a_i(\boldsymbol{X}, g(\boldsymbol{X})^{-1})$ متعلق به حلقه‌ی $K[\boldsymbol{X}]$ باشند. در واقع ما r را به گونه‌ای انتخاب کرده‌ایم که مخرج‌ها (یعنی $g(\boldsymbol{X})^{-1}$) را در $g(\boldsymbol{X})^r a_i(\boldsymbol{X}, g(\boldsymbol{X})^{-1})$ از بین ببرد.

در لم زیر صورت دیگری از لم ۲۲.۲.۴ را همراه با یک اثبات در نظریه مدل‌ها بیان می‌کنیم.

لم ۲۳.۲.۴. فرض کنید K یک میدان بسته‌ی جبری و I یک ایده‌آل رادیکال در $K[\boldsymbol{X}]$ باشد. همچنین فرض کنید چندجمله‌ای $g \in K[\boldsymbol{X}]$ متعلق به ایده‌آل I نباشد. در این صورت عنصر $\boldsymbol{x} \in K$ موجود است به طوری که $\boldsymbol{x} \in V(I)$ و $g(\boldsymbol{x}) \neq 0$.

اثبات. فرض می‌کنیم I یک ایده‌آل رادیکال باشد و $g \notin I$. بنا به نتیجه‌ی ۱۸.۲.۴ داریم $I = p_1 \cap \ldots \cap p_k$ به طوری که p_i ها ایده‌آل اول هستند. بدون کاستن از کلیت فرض می‌کنیم $g \notin p_1$ و حلقه‌ی $\frac{K[\boldsymbol{X}]}{p_1}$ را در نظر می‌گیریم. بنابراین با توجه به این‌که $g \notin p_1$ داریم $g(x_1 + p_1, \ldots, x_n + p_1) \neq 0$. از طرفی ایده‌آل I متناهیاً تولید شده است؛ یعنی $I = \langle f_1, \ldots, f_m\rangle$ و برای هر $i = 1, \ldots, m$ داریم $f_i(x_1 + p_1, \ldots, x_n + p_1) = 0$.

بنابراین

$$\frac{K[\boldsymbol{X}]}{p_1} \models \exists \boldsymbol{x} \quad \bigwedge f_i(\boldsymbol{x}) = 0 \wedge g(\boldsymbol{x}) \neq 0.$$

از طرفی

$$K \subseteq \frac{K[\boldsymbol{X}]}{p_1} \subseteq (\frac{K[\boldsymbol{X}]}{p_1})^{alg}$$

بنابراین در بستار جبری $\frac{K[\boldsymbol{X}]}{p_1}$ داریم $(\frac{K[\boldsymbol{X}]}{p_1})^{alg} \models \exists \boldsymbol{x} \quad \bigwedge f_i(\boldsymbol{x}) = 0 \wedge g(\boldsymbol{x}) \neq 0$. همچنین می‌دانیم تئوری میدان‌های بسته‌ی جبری حذف سور دارد. بنابراین فرمول $\exists \boldsymbol{x} \quad \bigwedge f_i(\boldsymbol{x}) = 0 \wedge g(\boldsymbol{x}) \neq 0$ دارای معادل بدون سور است، پس داریم $K \models \exists \boldsymbol{x} \quad \bigwedge f_i(\boldsymbol{x}) = 0 \wedge g(\boldsymbol{x}) \neq 0$. به بیان دیگر

$$K \models \exists \boldsymbol{x} \quad (\boldsymbol{x} \in V(I) \wedge g(\boldsymbol{x}) \neq 0).$$

□

نتیجه ۲۴.۲.۴. فرض کنید $\boldsymbol{a} \subseteq K[\boldsymbol{X}]$ یک ایده‌آل باشد. در این صورت موارد زیر برقرار است.

۱. $I(V(\boldsymbol{a})) = \sqrt{\boldsymbol{a}}$.

۲. اگر $\boldsymbol{a}$ یک ایده‌آل رادیکال یا به طور خاص یک ایده‌آل اول باشد، آنگاه $I(V(\boldsymbol{a})) = \boldsymbol{a}$.

اثبات. فرض می‌کنیم چندجمله‌ای g متعلق به $I(V(\boldsymbol{a}))$ باشد. در این صورت برای هر $\boldsymbol{x} \in V(\boldsymbol{a})$ داریم $g(\boldsymbol{x}) = 0$ پس بنا به لم ۲۲.۲.۴ توانی از g در $\boldsymbol{a}$ قرار می‌گیرد؛ یعنی $g \in \sqrt{\boldsymbol{a}}$. حال فرض می‌کنیم $g \in \sqrt{\boldsymbol{a}}$ یعنی عدد طبیعی $n \in \mathbb{N}$ موجود است به طوری که $g^n \in \boldsymbol{a}$، پس برای هر $\boldsymbol{x} \in V(\boldsymbol{a})$ داریم $g^n(\boldsymbol{x}) = 0$. در نتیجه برای هر $\boldsymbol{x} \in V(\boldsymbol{a})$ داریم $g(\boldsymbol{x}) = 0$؛ یعنی $g \in I(V(\boldsymbol{a}))$. همچنین اگر ایده‌آل $\boldsymbol{a}$ یک ایده‌آل رادیکال یا یک ایده‌آل اول باشد، داریم $\boldsymbol{a} = \sqrt{\boldsymbol{a}}$. بنابراین $I(V(\boldsymbol{a})) = \boldsymbol{a}$. □

نتیجه ۲۵.۲.۴. فرض کنید K یک میدان بسته‌ی جبری باشد و $I_1 \subsetneq I_2$ دو ایده‌آل رادیکال باشند. در این صورت $V(I_2) \subsetneq V(I_1)$.

اثبات. فرض می‌کنیم چندجمله‌ای g متعلق به $I_2 - I_1$ باشد. بنا به لم ۲۳.۲.۴ عنصر $\boldsymbol{x} \in K$ موجود است به طوری که $\boldsymbol{x} \in V(I_1)$ و $g(\boldsymbol{x}) \neq 0$؛ یعنی $K \models \exists \boldsymbol{x} \quad (\boldsymbol{x} \in V(I_1) \wedge g(\boldsymbol{x}) \neq 0)$. به بیان دیگر $K \models \exists \boldsymbol{x} \quad (\boldsymbol{x} \in V(I_1) - V(I_2))$.

□

قضیه ۲۶.۲.۴ (قضیه‌ی ریشه‌های هیلبرت [1]). فرض کنید K یک میدان بسته‌ی جبری باشد. بین ایده‌آل‌های رادیکال در $K[\boldsymbol{X}]$ و مجموعه‌های جبری $V \subseteq K^n$ یک تناظر یک به یک وجود دارد.

[1] Hilbert Nullstellensatz

اثبات. دیدیم که هر مجموعه‌ی جبری V از یک ایده‌آل رادیکال $I \subseteq K[\boldsymbol{X}]$ ناشی می‌شود. بنابراین یک نگاشت پوشا از I به V داریم؛ یعنی برای هر مجموعه‌ی جبری V، یک ایده‌آل رادیکال $I \subseteq K[\boldsymbol{X}]$ به گونه‌ای موجود است که $V = V(I)$. حال کافی است نشان دهیم این نگاشت یک به یک نیز هست. فرض می‌کنیم $I_۱ \neq I_۲$ دو ایده‌آل رادیکال در $K[\boldsymbol{X}]$ باشند. می‌خواهیم نشان دهیم $V(I_۱) \neq V(I_۲)$.

به برهان خلف فرض می‌کنیم $V(I_۱) = V(I_۲)$. در این صورت $I(V(I_۱)) = I(V(I_۲))$، پس بنا به قسمت ۲ نتیجه‌ی ۲۴.۲.۴ داریم $I_۱ = I_۲$ که با فرض در تناقض است. □

۳.۲.۴ توپولوژی زاریسکی

در این بخش نشان می‌دهیم که مجموعه‌های جبری در A^n، تحت اجتماع متناهی و اشتراک دلخواه، بسته هستند. بنابراین مجموعه‌های جبری در A^n، مجموعه‌های بسته‌ی یک توپولوژی روی فضای آفین A^n هستند که به این توپولوژی، توپولوژی زاریسکی می‌گوییم.

لم ۲۷.۲.۴. ایده‌آل‌های $\boldsymbol{a}, \boldsymbol{b} \subseteq K[\boldsymbol{X}]$ را در نظر بگیرید. مجموعه‌ی $V(\boldsymbol{a}) \cup V(\boldsymbol{b})$ یک مجموعه‌ی جبری است.

اثبات. ایده‌آل‌های $\boldsymbol{a}, \boldsymbol{b} \subseteq K[\boldsymbol{X}]$ را در نظر می‌گیریم. کافی است نشان دهیم $V(\boldsymbol{a}) \cup V(\boldsymbol{b})$ با یک مجموعه‌ی جبری برابر است. با توجه به این‌که هر ایده‌آل در $K[\boldsymbol{X}]$ متناهیاً تولید شده است، فرض می‌کنیم $\boldsymbol{a} = \langle f_۱, ..., f_n \rangle$ و $\boldsymbol{b} = \langle g_۱, ..., g_m \rangle$. سپس مجموعه‌ی $\boldsymbol{ab} = \{f_۱g_۱, \ldots, f_۱g_m, \ldots, f_ng_۱, \ldots, f_ng_m\} \subseteq K[\boldsymbol{X}]$ را در نظر می‌گیریم. ادعا می‌کنیم $V(\boldsymbol{a}) \cup V(\boldsymbol{b}) = V(\boldsymbol{ab})$. به منظور اثبات این ادعا فرض می‌کنیم $\boldsymbol{x}$ یک عنصر دلخواه، متعلق به $V(\boldsymbol{a}) \cup V(\boldsymbol{b})$ باشد. در این صورت یا برای هر $f_i \in \boldsymbol{a}$ داریم $f_i(\boldsymbol{x}) = ۰$ یا برای هر $g_j \in \boldsymbol{b}$ داریم $g_j(\boldsymbol{x}) = ۰$، پس بوضوح برای هر $f_ig_j \in \boldsymbol{ab}$ داریم $f_i(\boldsymbol{x})g_j(\boldsymbol{x}) = ۰$؛ یعنی $\boldsymbol{x} \in V(\boldsymbol{ab})$. حال فرض می‌کنیم $\boldsymbol{x} \in V(\boldsymbol{ab})$ و $\boldsymbol{x} \notin V(\boldsymbol{a})$. در این صورت چندجمله‌ای f متعلق به ایده‌آل $\boldsymbol{a}$ به گونه‌ای موجود است که $f(\boldsymbol{x}) \neq ۰$. مجموعه‌ی $f\boldsymbol{b} = \{fg_۱, fg_۲, \ldots\}$ را در نظر می‌گیریم؛ واضح است که $f\boldsymbol{b} = \{fg_۱, fg_۲, \ldots\} \subseteq \boldsymbol{ab}$. از طرفی $\boldsymbol{x} \in V(\boldsymbol{ab})$، پس برای هر $fg_j \in f\boldsymbol{b}$ نیز داریم $f(\boldsymbol{x})g_j(\boldsymbol{x}) = ۰$. در نتیجه برای هر g_j متعلق به $\boldsymbol{b}$ داریم $g_j(\boldsymbol{x}) = ۰$؛ یعنی $\boldsymbol{x} \in V(\boldsymbol{b})$.

بنابراین اثبات کردیم که $V(\boldsymbol{a}) \cup V(\boldsymbol{b})$ با مجموعه‌ی جبری $V(\boldsymbol{ab})$ برابر است. در نتیجه $V(\boldsymbol{a}) \cup V(\boldsymbol{b})$ یک مجموعه‌ی جبری است. □

نتیجه ۲۸.۲.۴. اجتماع هر تعداد متناهی از مجموعه‌های جبری، یک مجموعه‌ی جبری است؛ یعنی اگر $V(\boldsymbol{a}_۱), \ldots, V(\boldsymbol{a}_m)$ متناهی تا مجموعه‌ی جبری باشند، آنگاه $\bigcup_{i=۱}^{m} V(\boldsymbol{a}_i)$ یک مجموعه‌ی جبری است.

لم ۲۹.۲.۴. اشتراک هر تعداد دلخواه از مجموعه‌های جبری، یک مجموعه‌ی جبری است.

اثبات. فرض می‌کنیم $\{\boldsymbol{V(a_i)}\}_{i\in I}$ یک خانواده از مجموعه‌های جبری باشد. ادعا می‌کنیم $\bigcap_{i\in I} V(\boldsymbol{a}_i) = V(\bigcup_{i\in I} \boldsymbol{a}_i)$. توجه کنید که با اثبات درستی این ادعا در واقع نشان داده‌ایم که $\bigcap_{i\in I} V(\boldsymbol{a}_i)$ یک مجموعه‌ی جبری است.

به جهت اثبات این ادعا، فرض می‌کنیم $\boldsymbol{x}$ یک عنصر دلخواه متعلق به $\bigcap_{i\in I} V(\boldsymbol{a}_i)$ باشد. در این صورت برای هر $i \in I$ داریم $\boldsymbol{x} \in V(\boldsymbol{a}_i)$؛ یعنی برای هر $i \in I$ و هر $f \in \boldsymbol{a}_i$ داریم $f(\boldsymbol{x}) = 0$. بنابراین واضح است که برای هر $f \in \bigcup_{i\in I} \boldsymbol{a}_i$ داریم $f(\boldsymbol{x}) = 0$. در نتیجه $\boldsymbol{x} \in V(\bigcup_{i\in I} \boldsymbol{a}_i)$. حال کافی است اثبات کنیم $V(\bigcup_{i\in I} \boldsymbol{a}_i) \subseteq \bigcap_{i\in I} V(\boldsymbol{a}_i)$. بدین منظور فرض می‌کنیم $\boldsymbol{x}$ یک عنصر دلخواه متعلق به $V(\bigcup_{i\in I} \boldsymbol{a}_i)$ باشد. در این صورت برای هر $f \in \bigcup_{i\in I} \boldsymbol{a}_i$ داریم $f(\boldsymbol{x}) = 0$. بنابراین بوضوح برای هر $i \in I$ داریم $\boldsymbol{x} \in V(\boldsymbol{a}_i)$. در نتیجه $\boldsymbol{x} \in \bigcap_{i\in I} V(\boldsymbol{a}_i)$.

□

۴.۲.۴ واریته

دیدیم که مجموعه‌های جبری فضای آفین A^n زیرمجموعه‌های بسته‌ی توپولوژی زاریسکی هستند؛ بنابراین از این پس به جای مجموعه‌ی جبری از واژه‌ی مجموعه‌ی بسته‌ی زاریسکی یا مجموعه‌ی بسته استفاده می‌کنیم.

تعریف ۳۰.۲.۴. مجموعه‌ی بسته‌ی V را تحویل‌پذیر گوییم هرگاه دو مجموعه‌ی بسته‌ی $V_1, V_2 \neq V$ موجود باشند به طوری که $V = V_1 \cup V_2$. در غیر این صورت V را تحویل‌ناپذیر می‌نامیم.

تعریف ۳۱.۲.۴. مجموعه‌های بسته‌ی تحویل‌ناپذیر را واریته می‌نامیم.

فرض کنید $V(I)$ یک واریته باشد به گونه‌ای که $I \subseteq K[\boldsymbol{X}]$. در ادامه گاهی به جهت دقت بیشتر به جای این‌که بگوییم $V(I)$ یک واریته است از واژه‌ی K ـواریته استفاده می‌کنیم. به بیان دیگر منظور از یک K واریته، یک مجموعه‌ی بسته‌ی تحویل‌ناپذیر $V(I)$ است به طوری که $I \subseteq K[\boldsymbol{X}]$.

تعریف ۳۲.۲.۴. فرض کنید V یک واریته باشد. در این صورت $V(K) = \{\boldsymbol{x} \in K^n \mid \boldsymbol{x} \in V\}$.

در لم زیر نشان می‌دهیم که ایده‌آل متناظر با یک واریته، اول است.

لم ۳۳.۲.۴. مجموعه‌ی بسته‌ی V یک واریته است اگروتنهااگر ایده‌آل متناظر با آن اول باشد. به بیان دیگر مجموعه‌ی بسته‌ی V تحویل‌ناپذیر است اگروتنهااگر $I(V) = p$ یک ایده‌آل اول باشد.

اثبات. ابتدا فرض می‌کنیم مجموعه‌ی بسته‌ی V یک واریته و $\boldsymbol{a} = I(V)$ ایده‌آل وابسته به آن باشد. به برهان خلف فرض می‌کنیم $\boldsymbol{a}$ اول نباشد. در این صورت چندجمله‌ای‌های $g, f \in K[\boldsymbol{X}]$ موجود هستند به طوری که $f \cdot g$ متعلق به ایده‌آل $\boldsymbol{a}$ است؛ اما $f \notin \boldsymbol{a}$ و $g \notin \boldsymbol{a}$. قرار می‌دهیم $\boldsymbol{b} = \langle \boldsymbol{a}, f \rangle$ و $\boldsymbol{b}' = \langle \boldsymbol{a}, g \rangle$. واضح است که $\boldsymbol{a} \subsetneq \boldsymbol{b}$ و $\boldsymbol{a} \subsetneq \boldsymbol{b}'$. از این رو بنا به نتیجه‌ی ۲۵.۲.۴ داریم $V(\boldsymbol{b}) \subsetneq V(\boldsymbol{a})$ و $V(\boldsymbol{b}') \subsetneq V(\boldsymbol{a})$. ادعا می‌کنیم $V(\boldsymbol{b}) \cup V(\boldsymbol{b}') = V(\boldsymbol{a})$. به منظور اثبات این ادعا ابتدا نشان می‌دهیم $V(\boldsymbol{b}) \cup V(\boldsymbol{b}') \subseteq V(\boldsymbol{a})$. فرض می‌کنیم $\boldsymbol{x}$ یک عنصر دلخواه متعلق به $V(\boldsymbol{b}) \cup V(\boldsymbol{b}')$ باشد، پس $\boldsymbol{x} \in V(\boldsymbol{b})$ یا $\boldsymbol{x} \in V(\boldsymbol{b}')$. از طرفی $V(\boldsymbol{b}), V(\boldsymbol{b}') \subsetneq V(\boldsymbol{a})$. بنابراین در هر دو حالت داریم $\boldsymbol{x} \in V(\boldsymbol{a})$.

حال کافی است نشان دهیم $V(\boldsymbol{a}) \subseteq V(\boldsymbol{b}) \cup V(\boldsymbol{b}')$. فرض می‌کنیم $\boldsymbol{x}$ یک عنصر دلخواه متعلق به $V(\boldsymbol{a})$ باشد، پس با توجه به این‌که $f \cdot g$ متعلق به ایده‌آل $\boldsymbol{a}$ است، داریم $f \cdot g(\boldsymbol{x}) = ۰$. بنابراین $f(\boldsymbol{x}) = ۰$ یا $g(\boldsymbol{x}) = ۰$، پس واضح است که $\boldsymbol{x} \in V(\boldsymbol{b})$ یا $\boldsymbol{x} \in V(\boldsymbol{b}')$؛ یعنی $\boldsymbol{x} \in V(\boldsymbol{b}) \cup V(\boldsymbol{b}')$. در نتیجه $V(\boldsymbol{a}) = V(\boldsymbol{b}) \cup V(\boldsymbol{b}')$ که با تحویل‌ناپذیر بودن $V(\boldsymbol{a})$ در تناقض است.

حال می‌خواهیم جهت عکس این لم را اثبات کنیم. مجموعه‌ی بسته‌ی V را در نظر می‌گیریم و فرض می‌کنیم $I(V) = \boldsymbol{a}$ یک ایده‌آل اول است. نشان می‌دهیم که V یک واریته است. بدین منظور به برهان خلف فرض می‌کنیم دو مجموعه‌ی جبری $V(\boldsymbol{b}), V(\boldsymbol{b}') \neq V(\boldsymbol{a})$ موجود باشند به طوری که $V(\boldsymbol{a}) = V(\boldsymbol{b}) \cup V(\boldsymbol{b}')$. در این صورت واضح است که $V(\boldsymbol{b}) \subsetneq V(\boldsymbol{a})$ و $V(\boldsymbol{b}') \subsetneq V(\boldsymbol{a})$. بنابراین از لم ۶.۲.۴ داریم که $\boldsymbol{a} \subsetneq \boldsymbol{b}$ و $\boldsymbol{a} \subsetneq \boldsymbol{b}'$؛ یعنی چندجمله‌ای f متعلق به $\boldsymbol{b}$ موجود است به طوری که $f \notin \boldsymbol{a}$، همچنین یک چندجمله‌ای g متعلق به $\boldsymbol{b}'$ موجود است به طوری که $g \notin \boldsymbol{a}$. ادعا می‌کنیم که $f \cdot g$ در $V(\boldsymbol{b}) \cup V(\boldsymbol{b}')$ صفر می‌شود؛ یعنی برای هر عنصر $\boldsymbol{x}$ متعلق به $V(\boldsymbol{b}) \cup V(\boldsymbol{b}')$ داریم $f \cdot g(\boldsymbol{x}) = ۰$. به جهت اثبات این ادعا فرض می‌کنیم $\boldsymbol{x} \in V(\boldsymbol{b}) \cup V(\boldsymbol{b}')$ یک عنصر دلخواه باشد. در این صورت $\boldsymbol{x} \in V(\boldsymbol{b})$ یا $\boldsymbol{x} \in V(\boldsymbol{b}')$. پس $f(\boldsymbol{x}) = ۰$ یا $g(\boldsymbol{x}) = ۰$. در نتیجه $fg(\boldsymbol{x}) = ۰$. بنابراین برای هر $\boldsymbol{x} \in V(\boldsymbol{a})$ داریم $f \cdot g(\boldsymbol{x}) = ۰$؛ یعنی چندجمله‌ای $f \cdot g$ متعلق به ایده‌آل $\boldsymbol{a}$ است. از طرفی $f, g \notin \boldsymbol{a}$، که با اول بودن $\boldsymbol{a}$ در تناقض است. □

فرض کنید V یک K ـواریته باشد به طوری که $I_K(V) = \langle f_۱, ..., f_m \rangle \subseteq K[\boldsymbol{X}]$. توسیع میدانی L از K را در نظر بگیرید. واضح است که برای هر $i = ۱, ..., m$ داریم $f_i \in L[\boldsymbol{X}]$. بنابراین V یک L مجموعه‌ی جبری نیز هست. اما نکته‌ی حائز اهمیت این است که امکان دارد طی این توسیع مجموعه‌ی جبری V، تحویل‌ناپذیر باقی نماند و تحویل‌پذیر شود.

به عنوان مثال، فرض کنید $f \in K[\boldsymbol{X}]$ یک چندجمله‌ای تک متغیره با درجه‌ی بیشتر از ۱ و $\tilde{K}$ بستار جبری K باشد. واضح است که f در $\tilde{K}$ به عوامل خطی تجزیه می‌شود. بنابراین V به عنوان یک L مجموعه‌ی جبری لزوماً یک L ـواریته نیست.

تعریف ۳۴.۲.۴. فرض کنید V یک K ـواریته باشد. واریته‌ی V را مطلقاً تحویل‌ناپذیر [۲] گوییم هرگاه در هر

[2] absolutely irreducible

توسیع از K تحویل‌ناپذیر باقی بماند.

فرض کنید V یک K واریته‌ی مطلقاً تحویل‌ناپذیر باشد به طوری که $I_K(V) = \langle f_1, ..., f_m \rangle \subseteq K[\boldsymbol{X}]$. توسیع میدانی L از K را در نظر بگیرید. همان طور که گفتیم V یک L ـواریته نیز هست. توجه کنید که $I_K(V) \subseteq I_L(V)$. اما لزوماً این گونه نیست که $I_L(V) = L \cdot I_K(V)$.

تعریف ۳۵.۲.۴. فرض کنید V یک K ـواریته‌ی مطلقاً تحویل‌ناپذیر باشد. واریته‌ی V را تعریف شده روی K می‌نامیم هرگاه $I_{\tilde{K}}(V) = \tilde{K} I_K(V)$. به بیان دیگر واریته‌ی V را تعریف شده روی K می‌نامیم هرگاه $I_{\tilde{K}}(V)$ توسط چندجمله‌ای‌هایی در $K[\boldsymbol{X}]$ تولید شده باشد.

۵.۲.۴ نقاط عمومی و ویژه‌سازی

در این زیربخش دو مفهوم نقطه‌ی عمومی و ویژه‌سازی را تعریف می‌کنیم و اثبات می‌کنیم که نقاط متعلق به یک واریته‌ی V، ویژه‌سازی‌های نقطه‌ی عمومی آن هستند.

لم ۳۶.۲.۴. میدان K را در نظر بگیرید و فرض کنید p یک ایده‌آل اول از $K[\boldsymbol{X}]$ باشد. در این صورت $K[\boldsymbol{X}]/p$ در Ω می‌نشیند.

اثبات. نگاشت کانونی $\varphi : K[\boldsymbol{X}] \to \frac{K[\boldsymbol{X}]}{p}$ را در نظر می‌گیریم. می‌دانیم که $Ker(\varphi) = \{f \in K[\boldsymbol{X}] \mid f \in p\}$. بنابراین اگر $\boldsymbol{\xi}$ را تصویر $\boldsymbol{X}$ در $\frac{K[\boldsymbol{X}]}{p}$ در نظر بگیریم داریم $f(\boldsymbol{\xi}) = 0$ اگروتنهااگر $f \in p$. در نتیجه $\frac{K[\boldsymbol{X}]}{p} \cong K[\boldsymbol{\xi}] \subseteq \Omega$، پس بوضوح یکریختی $K[\boldsymbol{\xi}] \cong \frac{K[\boldsymbol{X}]}{p}$ یک نشاندن از $\frac{K[\boldsymbol{X}]}{p}$ به Ω است. به بیان دیگر فرض کنید p یک ایده‌آل در $K[\boldsymbol{X}]$ باشد. در این صورت p متناهیاً تولید شده است؛ یعنی $\{f_1, \cdots, f_n\} \subset K[\boldsymbol{X}]$ موجود است به طوری که $p = \langle f_1, \cdots, f_n \rangle$. از طرفی میدان Ω بسته‌ی جبری است؛ بنابراین از قضیه‌ی ۱۹.۲.۴ نتیجه می‌شود که برای هر $\{f_1, \cdots, f_n\} \subset K[\boldsymbol{X}]$ عنصر $\boldsymbol{\xi} \in \Omega$ موجود است به طوری که برای هر $i = 1, ..., n$ داریم $f_i(\boldsymbol{\xi}) = 0$. در نتیجه عنصر $\boldsymbol{\xi} \in \Omega$ موجود است به طوری که $f(\boldsymbol{\xi}) = 0$ اگروتنهااگر برای هر $f(\boldsymbol{x}) \in p$. حال نگاشت $\varphi : K[\boldsymbol{X}] \to K[\boldsymbol{\xi}]$ را در نظر می‌گیریم واضح است که $\mathrm{Ker}(\varphi) = p$. بنابراین $K[\boldsymbol{X}]/p \cong K[\boldsymbol{\xi}] \subseteq \Omega$؛ یعنی $K[\boldsymbol{X}]/p$ در Ω می‌نشیند. □

در تعریف زیر مفهوم نقطه‌ی صفر عمومی را برای یک ایده‌آل معرفی می‌کنیم. این تعریف در واقع بیان دیگری از لم ۳۶.۲.۴ است. در واقع $\boldsymbol{\xi}$ مربوط به اثبات این لم یک نقطه‌ی عمومی است.

تعریف ۳۷.۲.۴. برای هر ایده‌آل اول p، نقطه‌ی $\boldsymbol{x} \in A^n$ را نقطه‌ی صفر عمومی [۳] p می‌نامیم هرگاه برای هر چندجمله‌ای $f \in K[\boldsymbol{X}]$ داشته باشیم $f \in p$ اگروتنهااگر $f(\boldsymbol{x}) = 0$.

[3] generic zero

لم ۳۸.۲.۴. فرض کنید $\boldsymbol{x}$ یک نقطه‌ی صفر عمومی برای ایده‌آل اول p باشد. عنصر $\boldsymbol{x}' \in A^n$ را در نظر بگیرید. فرض کنید یک یکریختی $\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{x}']$ موجود باشد به طوری که برای هر $f \in K[\boldsymbol{x}]$ داشته باشیم $f(\boldsymbol{x}) \xrightarrow{\varphi} f(\boldsymbol{x}')$، آنگاه $\boldsymbol{x}'$ یک نقطه‌ی صفر عمومی دیگر برای p است.

اثبات. از این‌که $K[\boldsymbol{x}] \cong K[\boldsymbol{x}']$ نتیجه می‌شود که برای هر چندجمله‌ای f متعلق به $K[\boldsymbol{X}]$ داریم $f(\boldsymbol{x}) = ۰$ اگروتنهااگر $f(\boldsymbol{x}') = ۰$. از طرفی بنا به فرض، نقطه‌ی $\boldsymbol{x}$ یک نقطه‌ی صفر عمومی است. بنابراین $f \in p$ اگروتنهااگر $f(\boldsymbol{x}) = ۰$ و $K[\boldsymbol{X}]/p \cong K[\boldsymbol{x}]$. در نتیجه داریم $f \in p$ اگروتنهااگر $f(\boldsymbol{x}') = ۰$ و $K[\boldsymbol{X}]/p \cong K[\boldsymbol{x}] \cong K[\boldsymbol{x}']$، پس $\boldsymbol{x}'$ یک نقطه‌ی صفر عمومی برای p است.

□

لم ۳۹.۲.۴. عنصر $\boldsymbol{x} \in A^n$ را در نظر بگیرید و فرض کنید $p = \{f \in K[\boldsymbol{X}] \mid f(\boldsymbol{x}) = ۰\}$. در این صورت p یک ایده‌آل اول است.

اثبات. اثبات این‌که p یک ایده‌آل است، کاملاً مشابه اثبات لم ۴.۲.۴ است. از این رو از تکرار دوباره‌ی آن می‌پرهیزیم. بنابراین کافی است اثبات کنیم ایده‌آل p، اول است. بدین منظور فرض می‌کنیم $f \cdot g$ متعلق به p است. در این صورت $f \cdot g(\boldsymbol{x}) = ۰$. بنابراین $f(\boldsymbol{x}) = ۰$ یا $g(\boldsymbol{x}) = ۰$. در نتیجه $f \in p$ یا $g \in p$. □

ایده‌آل اول معرفی شده در لم قبل را ایده‌آل تولید شده توسط نقطه‌ی $\boldsymbol{x}$ (یا ایده‌آل مربوط به $\boldsymbol{x}$) می‌نامیم. واضح است که عنصر $\boldsymbol{x}$، نقطه‌ی صفر عمومی برای p است.

تعریف ۴۰.۲.۴. فرض کنید ایده‌آل‌های p' و p به ترتیب توسط $\boldsymbol{x}'$ و $\boldsymbol{x}$ تولید شده باشند. می‌گوییم $\boldsymbol{x}'$ یک ویژه‌سازی از $\boldsymbol{x}$ است هرگاه $p \subset p'$.

به بیان دیگر $\boldsymbol{x}'$ یک ویژه‌سازی از $\boldsymbol{x}$ است هرگاه برای هر چندجمله‌ای f متعلق به $K[\boldsymbol{X}]$ اگر $f(\boldsymbol{x}) = ۰$ آنگاه $f(\boldsymbol{x}') = ۰$.

دو نقطه‌ی $\boldsymbol{x}$ و $\boldsymbol{x}'$ را در نظر بگیرید. فرض کنید $\boldsymbol{x}'$ یک ویژه‌سازی از $\boldsymbol{x}$ باشد. در این صورت نگاشت $\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{x}']$ با ضابطه‌ی $f(\boldsymbol{x}) \xrightarrow{\varphi} f(\boldsymbol{x}')$ (برای هر $f \in K[\boldsymbol{x}]$) یک همریختی است. از طرفی اگر نگاشت $\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{x}']$ یک همریختی باشد، بنا به تعریف همریختی برای هر $f \in K[\boldsymbol{X}]$ اگر $f(\boldsymbol{x}) = ۰$ آنگاه $f(\boldsymbol{x}') = ۰$. در نتیجه $\boldsymbol{x}'$ یک ویژه‌سازی از $\boldsymbol{x}$ است. بنابراین $\boldsymbol{x}'$ یک ویژه‌سازی از $\boldsymbol{x}$ است اگروتنهااگر نگاشت $\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{x}']$ یک همریختی باشد.

تعریف ۴۱.۲.۴. فرض کنید ایده‌آل‌های p' و p به ترتیب توسط $\boldsymbol{x}'$ و $\boldsymbol{x}$ تولید شده باشند. می‌گوییم $\boldsymbol{x}'$ یک ویژه‌سازی عمومی از $\boldsymbol{x}$ است یا $\boldsymbol{x}'$ و $\boldsymbol{x}$ معادل هستند هرگاه $p = p'$. به بیان دیگر می‌گوییم $\boldsymbol{x}'$ یک ویژه‌سازی عمومی از $\boldsymbol{x}$ است هرگاه نگاشت $f(\boldsymbol{x}) \to f(\boldsymbol{x}')$ یکریختی باشد ($K[\boldsymbol{x}] \cong K[\boldsymbol{x}']$).

لم زیر اهمیت نقطه‌ی عمومی را نشان می‌دهد.

لم ۴۲.۲.۴. واریته‌ی V را در نظر بگیرید. فرض کنید p ایده‌آل اول مربوط به V باشد. همچنین فرض کنید که $\boldsymbol{x}$ نقطه‌ی صفر عمومی p است. برای هر عنصر $\boldsymbol{x'} \in V$ داریم $\boldsymbol{x'}$ اگروتنهااگر یک ویژه‌سازی از $\boldsymbol{x}$ باشد.

اثبات. فرض می‌کنیم V یک واریته و p ایده‌آل مربوط به آن باشد. همچنین فرض می‌کنیم $\boldsymbol{x}$ نقطه‌ی صفر عمومی p باشد. ابتدا نشان می‌دهیم هر نقطه‌ی $\boldsymbol{x'}$ دلخواه متعلق به V یک ویژه‌سازی از $\boldsymbol{x}$ است. بدین منظور فرض می‌کنیم $\boldsymbol{x'}$ یک نقطه‌ی دلخواه متعلق به V باشد. در این صورت برای هر f متعلق به ایده‌آل p داریم $f(\boldsymbol{x'}) = ۰$. از طرفی طبق فرض، $\boldsymbol{x}$ یک نقطه‌ی صفر عمومی برای ایده‌آل p است. بنابراین $f \in p$ اگروتنهااگر $f(\boldsymbol{x}) = ۰$. در نتیجه برای هر $f \in K[\boldsymbol{X}]$ اگر $f(\boldsymbol{x}) = ۰$ آنگاه $f(\boldsymbol{x'}) = ۰$.

حال برای اثبات جهت عکس لم، فرض می‌کنیم $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ باشد. در این صورت برای هر $f \in K[\boldsymbol{X}]$ اگر $f(\boldsymbol{x}) = ۰$ آنگاه $f(\boldsymbol{x'}) = ۰$. از طرفی $\boldsymbol{x}$ نقطه‌ی صفر عمومی p است، پس $f \in p$ اگروتنهااگر $f(\boldsymbol{x}) = ۰$. بنابراین برای هر $f \in p$ داریم $f(\boldsymbol{x'}) = ۰$. در نتیجه $\boldsymbol{x'} \in V$.

□

نتیجه ۴۳.۲.۴. واریته‌ی V را در نظر بگیرید. فرض کنید p ایده‌آل مربوط به V و $\boldsymbol{x}$ یک نقطه‌ی صفر عمومی برای p باشد. همچنین فرض کنید که p' ایده‌آل تولید شده توسط یک نقطه‌ی دلخواه $\boldsymbol{x'}$ باشد. در این صورت موارد زیر برقرار هستند:

۱. اگر $\boldsymbol{x'} \in V$ آنگاه $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ است.

۲. اگر $p \subset p'$ آنگاه $\boldsymbol{x'} \in V$.

تعریف ۴۴.۲.۴. فرض کنید V یک واریته و p ایده‌آل اول مربوط به آن باشد. نقطه‌ی $\boldsymbol{x}$ را نقطه‌ی عمومی V می‌نامیم هرگاه $\boldsymbol{x}$ نقطه‌ی صفر عمومی ایده‌آل p باشد.

لم ۴۵.۲.۴. فرض کنید V یک واریته و $\boldsymbol{x}$ یک نقطه‌ی عمومی برای V باشد. در این صورت $\boldsymbol{x'}$ یک ویژه‌سازی عمومی از $\boldsymbol{x}$ است اگروتنهااگر $\boldsymbol{x'}$ نیز یک نقطه‌ی عمومی برای V باشد.

اثبات. فرض می‌کنیم V یک واریته و $\boldsymbol{x}$ یک نقطه‌ی عمومی برای V باشد. در این صورت برای هر چندجمله‌ای $f \in K[\boldsymbol{X}]$ داریم $f(\boldsymbol{x}) = ۰$ اگروتنهااگر $f \in I(V)$. حال فرض می‌کنیم $\boldsymbol{x'}$ یک ویژه‌سازی عمومی از $\boldsymbol{x}$ است. بنابراین $K[\boldsymbol{x}] \cong K[\boldsymbol{x'}]$. از این رو برای هر $f \in K[\boldsymbol{X}]$ داریم $f(\boldsymbol{x}) = ۰$ اگروتنهااگر $f(\boldsymbol{x'}) = ۰$. در نتیجه $f \in I(V)$ اگروتنهااگر $f(\boldsymbol{x'}) = ۰$؛ یعنی $\boldsymbol{x'}$ یک نقطه‌ی عمومی برای V است. حال فرض می‌کنیم $\boldsymbol{x}$ و $\boldsymbol{x'}$ نقاط عمومی V باشند. در این صورت برای هر چندجمله‌ای $f \in K[\boldsymbol{X}]$ داریم $f(\boldsymbol{x}) = ۰$ اگروتنهااگر $f(\boldsymbol{x'}) = ۰$. در نتیجه $K[\boldsymbol{x}] \cong K[\boldsymbol{x'}]$. بنابراین $\boldsymbol{x}$ و $\boldsymbol{x'}$ ویژه‌سازی عمومی یکدیگرند. □

لم ۴۶.۲.۴. نقطه‌ی $\boldsymbol{x} \in A^n$ و دو میدان $K \subseteq L$ را در نظر بگیرید. فرض کنید p_K و p_L به ترتیب ایده‌آل‌های اول از $K[\boldsymbol{X}]$ و $L[\boldsymbol{X}]$ باشند. در این صورت داریم $p_L = L \cdot p_K$ اگروتنهااگر L از $K(\boldsymbol{x})$ مجزای خطی روی K باشد.

اثبات. برای دیدن اثبات، به منبع [۹، لم ۱.۲.۱۰] مراجعه کنید. □

لم ۴۷.۲.۴. فرض کنید V یک واریته با نقطه‌ی عمومی $\boldsymbol{x}$ باشد. در این صورت V یک واریته‌ی تعریف شده روی K است اگروتنهااگر $K(\boldsymbol{x})/K$ یک توسیع منتظم باشد.

اثبات. واریته‌ی V با نقطه‌ی عمومی $\boldsymbol{x}$ را در نظر می‌گیریم. فرض می‌کنیم $K(\boldsymbol{x})$ یک توسیع منتظم از K باشد. می‌خواهیم نشان دهیم V یک واریته‌ی تعریف شده روی K است. بدین منظور فرض می‌کنیم L یک توسیع از K باشد؛ کافی است نشان دهیم V در L تحویل‌ناپذیر است و $I_L(V) = L.I_K(V)$. توجه کنید که برای توسیع L از K دو وضعیت ممکن است رخ دهد. وضعیت اول $K \subseteq L \subseteq \tilde{K}$ و وضعیت دوم به صورت $K \subseteq \tilde{K} \subseteq L$ است. ادعا می‌کنیم در هر دو حالت $K(\boldsymbol{x})$ از L مجزای خطی است. به منظور اثبات این ادعا ابتدا حالت اول را بررسی می‌کنیم. توسیع $K(\boldsymbol{x})$ روی K منتظم است، پس $K(\boldsymbol{x})$ و $\tilde{K}$ روی K مجزای خطی هستند. بنابراین واضح است که $K(\boldsymbol{x})$ از L مجزای خطی است.

برای بررسی وضعیت دوم بدون کاستن از کلیت می‌دانیم L و $K(\boldsymbol{x})$ روی K مستقل جبری هستند. (اگر L و $K(\boldsymbol{x})$ روی K مستقل جبری نبودند، کافی است یک نقطه‌ی عمومی دیگر را به جای $\boldsymbol{x}$ در نظر بگیریم). بنابراین از لم ۴۳.۳.۱ داریم $K(\boldsymbol{x})$ از L مجزای خطی است. حال فرض می‌کنیم p_K و p_L به ترتیب ایده‌آل‌های اول از $K[\boldsymbol{X}]$ و $L[\boldsymbol{X}]$ باشند. بنا به لم ۴۶.۲.۴ داریم $I_L(V) \subseteq p_L = L \cdot p_K$. همچنین $I_K(V) = p_K$، پس $I_L(V) \subseteq p_L = L \cdot p_K = L \cdot I_K(V)$. از طرفی واضح است که $L \cdot I_K(V) \subseteq I_L(V)$. بنابراین $I_L(V) \subseteq p_L = L \cdot p_K = L \cdot I_K(V) \subseteq I_L(V)$. در نتیجه موارد زیر برقرار هستند:

۱. $I_L(V) = p_L$. بنابراین ایده‌آل $I_L(V)$ یک ایده‌آل اول است و از لم ۳۳.۲.۴ نتیجه می‌شود که V در L تحویل‌ناپذیر است.

۲. $I_L(V) = L \cdot I_K(V)$.

بنابراین واریته‌ی V مطلقاً تحویل‌ناپذیر است و برای هر توسیع L از K داریم $I_L(V) = L \cdot I_K(V)$، پس به طور خاص $I_{\tilde{K}}(V) = \tilde{K} \cdot I_K(V)$. از این رو واریته‌ی V یک واریته‌ی تعریف شده روی K است.

برای اثبات جهت عکس این لم، فرض می‌کنیم V یک واریته‌ی تعریف شده روی K باشد. در این صورت داریم $I_{\tilde{K}}(V) = \tilde{K} \cdot I_K(V)$، پس طبق لم ۴۶.۲.۴ داریم $K(\boldsymbol{x})$ از $\tilde{K}$ مجزای خطی است. بنابراین توسیع $K(\boldsymbol{x})$ روی K منتظم است.

□

لم ۴۸.۲.۴. توسیع منتظم F از K را در نظر بگیرید و فرض کنید $x_1, \dots, x_n$ عناصری از F باشند. کلاس همه‌ی K ـ‌ویژه‌سازی‌های $\boldsymbol{x}$ یک واریته‌ی تعریف شده روی K است.

اثبات. واریته‌ی V را به گونه‌ای در نظر می‌گیریم که $\boldsymbol{x}$ نقطه‌ی عمومی V باشد. از طرفی $K \subseteq K(\boldsymbol{x}) \subseteq F$، پس بنا به لم ۴۲.۳.۱ و با توجه به این‌که F روی K منتظم است داریم $K \subseteq K(\boldsymbol{x})$ منتظم است. بنابراین از لم ۴۷.۲.۴ داریم V یک واریته‌ی تعریف شده روی K است. □

۶.۲.۴ بُعد واریته‌ها

تعریف ۴۹.۲.۴. برای هر نقطه‌ی دلخواه $\boldsymbol{x} \in A^n$، درجه تعالی $K(\boldsymbol{x})$ روی K را بُعد نقطه‌ی $\boldsymbol{x}$ می‌نامیم. بُعد یک نقطه‌ی $\boldsymbol{x} \in A^n$ را با نماد $\dim_K(\boldsymbol{x})$ نمایش می‌دهیم.

تعریف ۵۰.۲.۴. فرض کنید V یک واریته و $\boldsymbol{x}$ نقطه‌ی عمومی آن باشد. در این صورت تعریف می‌کنیم $\dim(V) = \dim_K(\boldsymbol{x})$.

در نتیجه‌ی ۱۸.۲.۴ دیدیم که یک ایده‌آل رادیکال را می‌توان به صورت اشتراک ایده‌آل‌های اول نوشت. بنابراین برای هر مجموعه‌ی جبری A واریته‌های $V_1, \cdots, V_n$ موجود هستند به طوری که $A = \bigcup_{i=1}^{n} V_i$؛ یعنی هر مجموعه‌ی جبری A را می‌توان به صورت اجتماع متناهی تا واریته نوشت. در واقع اگر $I = p_1 \cap p_2$ آنگاه $V(I) = V(p_1) \cap V(p_2)$

تعریف ۵۱.۲.۴. فرض کنید $A = \bigcup_{i=1}^{n} V_i$ یک مجموعه‌ی جبری باشد. بُعد A را به صورت زیر تعریف می‌کنیم

$$\dim(A) = \max\{\dim(V_1), \cdots, \dim(V_n)\}.$$

تعریف ۵۲.۲.۴. ۱. هر K ـ‌واریته‌ی V با بعد ۱ را یک K ـ‌منحنی می‌نامیم.

۲. هر K ـ‌واریته‌ی $W \subseteq A^n$ با بعد $n-1$ را یک ابر رویه می‌نامیم. هر ابر رویه به فرم یک $V(f)$ است به طوری که $f \in K[\boldsymbol{X}]$ یک چندجمله‌ای تحویل‌ناپذیر است.

نتیجه ۵۳.۲.۴. فرض کنید $f \in K[X_1, \cdots, X_n]$ یک چندجمله‌ای تحویل‌ناپذیر باشد. همچنین فرض کنید $x_1, \cdots, x_n$ به گونه‌ای باشند که $f(x_1, \cdots, x_n) = 0$ و درجه تعالی $K(x_1, \cdots, x_n)$ روی K برابر با $n-1$ باشد. در این صورت چندجمله‌ای f مطلقاً تحویل‌ناپذیر است اگروتنهااگر توسیع $K(x_1, \cdots, x_n)$ روی K منتظم باشد.

اثبات. فرض می‌کنیم $f \in K[\boldsymbol{X}]$ یک چندجمله‌ای تحویل ناپذیر و $\boldsymbol{x}$ به گونه‌ای باشند که $f(\boldsymbol{x}) = ۰$. همچنین فرض می‌کنیم درجه تعالی $K(\boldsymbol{x})$ روی K برابر با $n - ۱$ است. ابر رویه‌ی $V = V(f)$ را در نظر می‌گیریم. می‌دانیم V یک واریته با نقطه‌ی عمومی $\boldsymbol{x}$ است، پس طبق لم ۴۷.۲.۴ واریته‌ی V یک واریته‌ی تعریف شده روی K است اگروتنهااگر توسیع $K(\boldsymbol{x})$ روی K یک توسیع منتظم باشد. از این رو اگر $K(\boldsymbol{x})$ روی K یک توسیع منتظم باشد، آنگاه واریته‌ی V یک واریته‌ی مطلقاً تحویل‌ناپذیر است. در نتیجه چندجمله‌ای f مطلقاً تحویل‌ناپذیر است. همچنین اگر چندجمله‌ای f مطلقاً تحویل‌ناپذیر باشد. بوضوح واریته‌ی V یک واریته‌ی تعریف شده روی K است. در نتیجه $K(\boldsymbol{x})$ روی K یک توسیع منتظم است. □

قضیه ۵۴.۲.۴. فرض کنید $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ روی میدان K باشد. در این صورت $\dim(\boldsymbol{x'}) \leq \dim(\boldsymbol{x})$.

اثبات. فرض می‌کنیم $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ است و $\dim(\boldsymbol{x'}) = r$. همچنین فرض می‌کنیم $x'_۱, \cdots, x'_r$ متعلق به $\boldsymbol{x'}$، روی میدان K مستقل جبری باشند. ادعا می‌کنیم که $x_۱, \ldots, x_r$ متعلق به $\boldsymbol{x}$ نیز مستقل جبری هستند. برای اثبات این ادعا به برهان خلف فرض می‌کنیم $f(x_۱, \ldots, x_r) = ۰$. از آن جا که $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ است، برای هر چندجمله‌ای $f \in K[\boldsymbol{X}]$ اگر $f(x_۱, \ldots, x_n) = ۰$ آنگاه $f(x'_۱, \ldots, x'_n) = ۰$. بنابراین از این‌که $f(x_۱, \ldots, x_r) = ۰$ نتیجه می‌شود $f(x'_۱, \ldots, x'_r) = ۰$، که با مستقل جبری بودن $x'_۱, \ldots, x'_r$ در تناقض است، پس بُعد $\boldsymbol{x}$ حداقل r است. بنابراین $\dim(\boldsymbol{x'}) \leq \dim(\boldsymbol{x})$.

□

توجه ۵۵.۲.۴. توجه کنید عکس قضیه‌ی فوق برقرار نیست؛ یعنی از این‌که $\dim(\boldsymbol{x'}) \leq \dim(\boldsymbol{x})$ نمی‌توانیم نتیجه بگیریم $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ است.

قضیه ۵۶.۲.۴. فرض کنید $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ روی میدان K باشد. در این صورت داریم $\dim(\boldsymbol{x'}) = \dim(\boldsymbol{x})$ اگروتنهااگر $\boldsymbol{x'}$ و $\boldsymbol{x}$ ویژه‌سازی عمومی یکدیگر باشند.

اثبات. ابتدا فرض می‌کنیم $\boldsymbol{x'}$ و $\boldsymbol{x}$ ویژه‌سازی عمومی یکدیگر باشند. در این صورت $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ و $\boldsymbol{x}$ یک ویژه‌سازی از $\boldsymbol{x'}$ است. بنابراین از قضیه‌ی ۵۴.۲.۴ داریم $\dim(\boldsymbol{x'}) \leq \dim(\boldsymbol{x})$ و $\dim(\boldsymbol{x}) \leq \dim(\boldsymbol{x'})$. در نتیجه $\dim(\boldsymbol{x}) = \dim(\boldsymbol{x'})$.

حال برای اثبات جهت عکس قضیه فرض می‌کنیم $\dim(\boldsymbol{x'}) = \dim(\boldsymbol{x})$. می‌خواهیم اثبات کنیم $\boldsymbol{x}$ و $\boldsymbol{x'}$ ویژه‌سازی عمومی یکدیگرند. بدین منظور کافی است نشان دهیم $K[\boldsymbol{x}] \cong K[\boldsymbol{x'}]$. از آنجا که $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ است، یک همریختی $\varphi : K[\boldsymbol{x}] \to K[\boldsymbol{x'}]$ موجود است به طوری که نگاشت φ چندجمله‌ای $f(\boldsymbol{x})$ را به $f(\boldsymbol{x'})$ تصویر می‌کند. ادعا می‌کنیم نگاشت φ یک یکریختی نیز هست. به منظور اثبات این ادعا کافی است نشان دهیم $\mathrm{Ker}(\varphi) = ۰$. ابتدا فرض می‌کنیم $x'_۱, \ldots, x'_r$ یک پایه‌ی متعالی $K[\boldsymbol{x}]$ روی K باشد. در این صورت با توجه به این‌که $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ است، $x_۱, \ldots, x_r$ یک پایه‌ی متعالی برای $K[\boldsymbol{x}]$ است.

حال به برهان خلف فرض می‌کنیم $y \neq ۰ \in K[\boldsymbol{X}]$ و $\varphi(y) = ۰$. در این صورت y در یک معادله‌ی ساده شده به صورت $a_n y^n + \ldots + a_۰ = ۰$ صدق می‌کند به طوری که $a_j \in K[x_۱, \ldots, x_r]$ و $a_۰ \neq ۰$. بنابراین داریم $\varphi(a_n y^n + \ldots + a_۰) = \varphi(۰)$. از طرفی فرض کردیم $\varphi(y) = ۰$، پس داریم

$$\varphi(a_n y^n + \ldots + a_۰) = \varphi(a_۰) = \varphi(۰) = ۰.$$

در نتیجه $\varphi(a_۰) = ۰$. اما توجه کنید که نگاشت φ روی $K[x_۱, ..., x_r]$ یک یکریختی است؛ یعنی $K[x_۱, ..., x_r] \cong K[x'_۱, ..., x'_r]$. بنابراین از این‌که $a_۰ \neq ۰$ نتیجه می‌شود $\varphi(a_۰) \neq ۰$ که این تناقض است. □

نتیجه ۵۷.۲.۴. فرض کنید $\boldsymbol{x'}$ و $\boldsymbol{x}$ دو نقطه‌ی عمومی برای واریته‌ی V باشند. در این صورت بنا به لم ۴۵.۲.۴ $\boldsymbol{x'}$ و $\boldsymbol{x}$ ویژه‌سازی عمومی یکدیگرند. بنابراین $\dim(\boldsymbol{x'}) = \dim(\boldsymbol{x})$. در نتیجه بعد واریته‌ی V مستقل از انتخاب نقطه‌ی عمومی آن است.

قضیه ۵۸.۲.۴. فرض کنید $W \subseteq V$ دو واریته باشند. در این صورت $\dim(W) \leq \dim(V)$.

اثبات. فرض می‌کنیم $W \subseteq V$ دو واریته باشند. همچنین فرض می‌کنیم p و p' به ترتیب ایده‌آل های اول مربوط به V و W با نقاط عمومی $\boldsymbol{x}$ و $\boldsymbol{x'}$ باشند. از آنجا که $W \subseteq V$ داریم $p \subset p'$، پس $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ است. بنابراین از قضیه‌ی ۵۴.۲.۴ داریم $\dim(\boldsymbol{x'}) \leq \dim(\boldsymbol{x})$. در نتیجه $\dim(W) \leq \dim(V)$.
□

قضیه ۵۹.۲.۴. فرض کنید $W \subseteq V$ دو واریته باشند. در این صورت داریم $W = V$ اگروتنهااگر $\dim(W) = \dim(V)$.

اثبات. دو واریته‌ی W و V را در نظر می‌گیریم. فرض می‌کنیم p و p' به ترتیب ایده‌آل های اول مربوط به V و W با نقاط عمومی $\boldsymbol{x}$ و $\boldsymbol{x'}$ باشند. همچنین فرض می‌کنیم $\dim(W) = \dim(V)$. در این صورت $\dim(\boldsymbol{x'}) = \dim(\boldsymbol{x})$، پس بنا به قضیه‌ی ۵۴.۲.۴ داریم $K[\boldsymbol{x}] \cong K[\boldsymbol{x'}]$. بنابراین واضح است که $p = p'$، در نتیجه $V = W$. مراحل فوق برگشت پذیر است یعنی برای اثبات جهت عکس کافی است مسیر فوق را به صورت معکوس طی کنیم.
□

گفتیم برای هر مجموعه‌ی جبری A واریته‌های $V_۱, \cdots, V_n$ موجود هستند به طوری که $A = \bigcup_{i=۱}^{n} V_i$. بنابراین هر مجموعه‌ی جبری از اجتماع متناهی تا واریته ایجاد شده است. دیدیم که اعضای هر واریته ویژه‌سازی‌های نقطه‌ی عمومی آن واریته هستند. برای هر واریته‌ی V_i یک نقطه‌ی عمومی در نظر بگیرید. در این صورت متناهی تا نقطه داریم که بوضوح اعضای مجموعه‌ی جبری A، ویژه‌سازی‌های این نقاط هستند.

قضیه ۶۰.۲.۴. یک نقطه‌ی $\boldsymbol{x'}$ از A نقطه‌ی عمومی یک مولفه از A است اگروتنهااگر هیچ نقطه‌ی $\boldsymbol{x}$ در A وجود نداشته باشد به طوری که $\dim(\boldsymbol{x}) > \dim(\boldsymbol{x'})$ و $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ باشد.

اثبات. مجموعه‌ی جبری A را در نظر می‌گیریم. واریته‌های $V_1, \cdots, V_n$ موجود هستند به طوری‌که $A = \bigcup_{i=1}^{n} V_i$. فرض می‌کنیم $\boldsymbol{x'}$ یک نقطه‌ی عمومی برای مولفه‌ی $V_i \in \{V_1, \cdots, V_n\}$ از مجموعه جبری A باشد. به برهان خلف فرض می‌کنیم $\boldsymbol{x'}$ یک ویژه‌سازی از عنصر $\boldsymbol{x}$ است و $\dim(\boldsymbol{x}) > \dim(\boldsymbol{x'})$.

ادعا می‌کنیم $\boldsymbol{x}$ متعلق به واریته‌ی V_i نیست. به منظور اثبات این ادعا به برهان خلف فرض می‌کنیم $\boldsymbol{x}$ متعلق به واریته‌ی V_i باشد. در این صورت $\boldsymbol{x}$ یک نقطه‌ی عمومی دیگر برای V_i است. بنابراین $\dim(\boldsymbol{x}) = \dim(\boldsymbol{x'})$ که تناقض است. در نتیجه یک واریته W شامل $\boldsymbol{x}$ موجود است به طوری $V_i \subset W$ و این با تجزیه‌ی مجموعه جبری A به مجموعه‌های جبری تحویل‌ناپذیر(واریته‌ها) در تناقض است. حال نقطه‌ی $\boldsymbol{x'} \in A$ را در نظر می‌گیریم و فرض می‌کنیم هیچ نقطه‌ی $\boldsymbol{x} \in A$ وجود ندارد به طوری که $\boldsymbol{x'}$ یک ویژه‌سازی از $\boldsymbol{x}$ باشد و $\dim(\boldsymbol{x}) > \dim(\boldsymbol{x'})$. از این‌که $\boldsymbol{x'}$ متعلق به A است نتیجه می‌شود واریته‌ی $V_i \in \{V_1, \cdots, V_n\}$ موجود است به طوری که $\boldsymbol{x'} \in V_i$. در این صورت $\boldsymbol{x'}$ یک ویژه‌سازی از نقطه عمومی واریته‌ی V_i است.

بنابراین اگر $\boldsymbol{x}$ نقطه‌ی عمومی V_i باشد داریم $\dim(\boldsymbol{x}) \geq \dim(\boldsymbol{x'})$. از طرفی بنا به فرض $\dim(\boldsymbol{x}) \neq \dim(\boldsymbol{x'})$ از این رو $\dim(\boldsymbol{x}) = \dim(\boldsymbol{x'})$. در نتیجه $\boldsymbol{x}$ و $\boldsymbol{x'}$ ویژه‌سازی عمومی یکدیگرند، پس بنا به لم ۴۵.۲.۴ نقطه‌ی $\boldsymbol{x'}$ یک نقطه‌ی عمومی برای V_i است.

□

خلاصه‌ای از آنچه در این بخش گفته شده را به بیان دیگر مطرح می‌کنیم. به طور کلی فرض کنید $\boldsymbol{x} \in A^n$ یک n تایی مرتب باشد. بُعد $\boldsymbol{x}$ برابر است با درجه‌ی تعالی $K(\boldsymbol{x})$ روی K. یعنی $\dim \boldsymbol{x} = r$ اگر $\{x_{i_1}, \ldots, x_{i_r} | x_i \in \boldsymbol{x}, \quad i = 1, \ldots, r\}$ بزرگترین مجموعه‌ی مستقل جبری متشکل از عناصر $\boldsymbol{x}$ باشد. حال بُعد یک مجموعه جبری A را به کمک بُعد عناصر آن، به صورت زیر تعریف می‌کنیم: $\dim(A) = \dim(\boldsymbol{x})$ وقتی که $\boldsymbol{x}$ بزرگترین بعد را در میان عناصر A دارد. به طور خاص اگر مجموعه‌ی جبری V یک واریته باشد، از آنجا که بزرگترین بعد مربوط به نقطه عمومی است، بعد V برابر با بعد نقطه عمومی آن است. توجه کنید که بعد یک مجموعه‌ی جبری $V \subseteq A$ با درجه‌ی تعالی آن متفاوت است؛ در واقع بعد یک مجموعه‌ی جبری برابر است با درجه‌ی تعالی نقطه عمومی یکی از مولفه‌هایش.

۳.۴ میدان‌های شبه‌بسته‌ی جبری

تعریف ۱.۳.۴. میدان K را شبه‌بسته‌ی جبری گوییم هرگاه هر واریته‌ی تعریف شده روی K، یک ریشه در K داشته باشد.

لم ۲.۳.۴. میدان‌های بسته‌ی جبری، شبه‌بسته‌ی جبری هستند.

اثبات. فرض می‌کنیم $\tilde{K}$ یک میدان بسته‌ی جبری باشد. نشان می‌دهیم که هر ایده‌آل در $\tilde{K}[\boldsymbol{X}]$ یک ریشه در خود $\tilde{K}$ دارد. بدین منظور ایده‌آل دلخواه $I \subsetneq \tilde{K}[\boldsymbol{X}]$ را در نظر می‌گیریم. می‌دانیم که هر ایده‌آل در $\tilde{K}[\boldsymbol{X}]$ متناهیاً تولید شده است. بنابراین $f_1, \dots, f_m \in \tilde{K}[\boldsymbol{X}]$ به گونه‌ای موجود هستند که $I = \langle f_1, \dots, f_m \rangle$. از طرفی با توجه به این‌که $\tilde{K}$ یک میدان بسته‌ی جبری است، از قضیه‌ی ۱۹.۲.۴ نتیجه می‌شود که هر $f_1, \dots, f_m \in K[\boldsymbol{X}]$ یک ریشه‌ی مشترک در $\tilde{K}$ دارند، پس بنا به لم ۱۳.۲.۴ ایده‌آل I یک ریشه در $\tilde{K}$ دارد. از طرفی هر مجموعه‌ی جبری V با یک ایده‌آل رادیکال در تناظر یک به یک است؛ یعنی ایده‌آل I موجود است به طوری که $V = V(I)$. در نتیجه هر مجموعه‌ی جبری یک ریشه در $\tilde{K}$ دارد. بنابراین به طور خاص هر واریته‌ی تعریف شده روی $\tilde{K}$ یک ریشه در $\tilde{K}$ دارد. زیرا ایده‌آل تولید شده توسط I ریشه دارد.

□

توجه شود که جهت عکس لم فوق برقرار نیست؛ یعنی اگر K یک میدان شبه‌بسته‌ی جبری باشد نمی‌توان نتیجه گرفت K بسته‌ی جبری است. زیرا در میدان‌های شبه‌بسته‌ی جبری می‌دانیم که واریته‌های تعریف شده روی K در K ریشه دارند. اما نمی‌توانیم ادعا کنیم هر چندجمله‌ای متعلق به $K[\boldsymbol{X}]$ در K یک ریشه دارد.

تعریف ۳.۳.۴. فضای توپولوژیک X را در نظر بگیرید و فرض کنید A زیرمجموعه‌ای از X باشد. می‌گوییم A در X چگال است هرگاه هر نقطه‌ی x متعلق به X، یا متعلق به A باشد یا یک نقطه‌ی حدی از A باشد. به بیان دیگر A در X چگال است هرگاه کوچکترین زیرمجموعه‌ی بسته از X که شامل A است خود X باشد.

قضیه ۴.۳.۴. فرض کنید K یک میدان شبه‌بسته‌ی جبری و V یک واریته‌ی تعریف شده روی K باشد. در این صورت $V(K)$ در V چگال است.

اثبات. برای اثبات این‌که $V(K)$ در V چگال است، باید نشان دهیم V کوچکترین مجموعه‌ی بسته‌ی شامل $V(K)$ است؛ یعنی اگر مجموعه‌ی جبری $W(K)$ شامل $V(K)$ باشد، آنگاه W شامل V نیز هست. بدین منظور، حکمی کلی تر اثبات می‌کنیم که هر مجموعه‌ی بسته‌ی شامل $V(K)$ حتماً شامل V است.

فرض می‌کنیم $\boldsymbol{x} = (x_1, \dots, x_n)$ یک نقطه‌ی عمومی برای V باشد. همچنین فرض می‌کنیم W یک مجموعه‌ی جبری باشد به طوری که $V \nsubseteq W$ و $I(W) = \langle g_1, ..., g_m \rangle$. بنابراین طبق لم ۱۳.۲.۴ داریم $W = V(g_1, \dots, g_m)$. ادعا می‌کنیم g متعلق به $\{g_1, \dots, g_m\}$ موجود است به طوری که $g(\boldsymbol{x}) \neq 0$. به منظور اثبات این ادعا به برهان خلف فرض می‌کنیم برای هر g متعلق به $\{g_1, \dots, g_m\}$ داریم $g(\boldsymbol{x}) = 0$. از این رو با توجه به این‌که $\boldsymbol{x}$ نقطه عمومی V است، برای هر $\boldsymbol{x}' \in V$ و هر $g \in \{g_1, \dots, g_m\}$ داریم $g(\boldsymbol{x}') = 0$. در نتیجه $V \subseteq W$ که با فرض $V \nsubseteq W$ در تناقض است.

بنابراین g متعلق به $\{g_۱, \dots, g_m\}$ موجود است به طوری که $g(\boldsymbol{x}) \neq ۰$، پس $g(\boldsymbol{x})$ وارون‌پذیر است؛ یعنی $\boldsymbol{y} \in \Omega$ موجود است به طوری که $y \cdot g(\boldsymbol{x}) = ۱$. حال مجموعه‌ی جبری V' را به گونه‌ای در نظر می‌گیریم که $(\boldsymbol{x}, y)$ نقطه‌ی عمومی آن باشد. در ادامه اثبات می‌کنیم نقطه‌ی $(\boldsymbol{x}', y)$ متعلق به $V'(K)$ موجود است به طوری که $\boldsymbol{x}' \in V(K)$، اما $\boldsymbol{x}'$ متعلق به $W(K)$ نیست و در نتیجه $V(K) \nsubseteq W(K)$.

از آنجا که y وارون $g(\boldsymbol{x})$ است داریم $y \in K(\boldsymbol{x})$. در نتیجه $K(\boldsymbol{x}, y) = K(\boldsymbol{x})$. از طرفی بنا به لم **۴۷.۲.۴** توسیع $K(\boldsymbol{x})$ یک توسیع منتظم از K است. بنابراین $K(\boldsymbol{x}, y)$ نیز یک توسیع منتظم از K است، پس بنا به لم **۴۷.۲.۴** واریته‌ی V' یک واریته‌ی تعریف شده روی K است. نهایتاً از آنجا که K یک میدان شبه‌بسته‌ی جبری است و V' یک واریته‌ی تعریف شده روی K است از تعریف میدان شبه‌بسته‌ی جبری داریم V' در خود K یک ریشه دارد؛ یعنی $(\boldsymbol{x}', y')$ در K موجود است به طوری که $(\boldsymbol{x}', y') \in V'$.

با توجه به این‌که $(\boldsymbol{x}, y)$ نقطه عمومی V' است، می‌دانیم $(\boldsymbol{x}', y')$ یک ویژه‌سازی از $(\boldsymbol{x}, y)$ است. از طرفی $y \cdot g(\boldsymbol{x}) - ۱ = ۰$، پس $y'g(\boldsymbol{x}') = ۱$. در نتیجه $g(\boldsymbol{x}') \neq ۰$. بنابراین $\boldsymbol{x}' \notin W$. اما با توجه به این‌که $\boldsymbol{x}$ نقطه‌ی عمومی V است؛ برای هر $f \in I(V)$ داریم $f(\boldsymbol{x}) = ۰$. از طرفی $(\boldsymbol{x}, y)$ نقطه‌ی عمومی V' است در نتیجه برای هر f داریم؛ اگر $f(\boldsymbol{x}) = ۰$ آنگاه $f(\boldsymbol{x}') = ۰$. بنابراین $\boldsymbol{x}' \in V$ و چون $\boldsymbol{x}' \in K$ داریم $\boldsymbol{x}' \in V(K)$. از این رو $\boldsymbol{x}' \in V(K)$ و $\boldsymbol{x}' \notin W(K)$ در نتیجه $V(K) \nsubseteq W(K)$.

□

قضیه ۵.۳.۴. فرض کنید K یک میدان شبه‌بسته‌ی جبری باشد. در این صورت K یک میدان نامتناهی است.

اثبات. فرض می‌کنیم K یک میدان شبه‌بسته‌ی جبری باشد. برای این‌که اثبات کنیم K یک میدان نامتناهی است. نشان می‌دهیم برای هر زیرمجموعه‌ی متناهی $\{a_۱, \dots, a_m\}$ از K عنصر $a_{m+۱}$ متعلق به K موجود است به طوری که $a_{m+۱} \notin K$؛ یعنی $K \neq \{a_۱, ..., a_m\}$.

فرض می‌کنیم $\{a_۱, \dots, a_m\}$ عناصری از K باشند. مجموعه‌ی بسته‌ی $A^۱$ را در نظر می‌گیریم. بوضوح $A^۱$ یک واریته‌ی تعریف شده روی K است، پس بنا به قضیه‌ی **۴.۳.۴** داریم $A(K)$ در A چگال است. همچنین توجه کنید که $A(K) = K$، از این رو K در A چگال است. حال واریته‌ی $W = V(\prod_{i=۱}^{m}(X - a_i))$ را در نظر می‌گیریم. واضح است که $W = \{a_۱, \dots, a_m\}$، پس $W = W(K)$. ادعا می‌کنیم $A(K) \nsubseteq W(K)$. به منظور اثبات این ادعا به برهان خلف فرض می‌کنیم $A(K) \subseteq W(K)$. از آنجا که $K = A(K)$ در A چگال است داریم $W \nsubseteq A$ که این تناقض است (زیرا بوضوح $W \subseteq A$). در نتیجه $A(K) \nsubseteq W(K)$؛ یعنی $K \nsubseteq \{a_۱, \dots, a_m\}$. در نتیجه عنصر $a_{m+۱}$ متعلق به K موجود است به طوری که $a_{m+۱}$ به مجموعه‌ی $\{a_۱, \dots, a_m\}$ تعلق ندارد.

□

نتیجه ۶.۳.۴. فرض کنید K یک میدان شبه‌بسته‌ی جبری و V یک واریته‌ی تعریف شده روی K باشد. همچنین فرض کنید چندجمله‌ای $g \in K[\boldsymbol{X}]$ روی $V(K)$ صفر شود. در این صورت g متعلق به $I_K(V)$ است. به بیان دیگر اگر چندجمله‌ای g در تمام نقاط متعلق به $V(K)$ صفر شود، آنگاه g در تمام نقاط V صفر می‌شود.

اثبات. فرض می‌کنیم برای هر $\boldsymbol{x'}$ متعلق به $V(K)$ داریم $g(\boldsymbol{x'}) = ۰$. می‌خواهیم نشان دهیم برای هر $\boldsymbol{x}$ متعلق به V داریم $g(\boldsymbol{x}) = ۰$. نقطه‌ی عمومی $\boldsymbol{y} \in V$ را در نظر می‌گیریم. کافی است نشان دهیم $g(\boldsymbol{y}) = ۰$. به برهان خلف فرض می‌کنیم $g(\boldsymbol{y}) \neq ۰$. قرار می‌دهیم $I := \{I(V), g\}$ و $W = V(I)$. (توجه کنید که $g \notin I(V)$، پس $I \neq I(V)$). بنا به فرض برای هر $\boldsymbol{x} \in V(K)$ داریم $g(\boldsymbol{x}) = ۰$ و برای هر $f \in I(V)$ نیز داریم $f(\boldsymbol{x}) = ۰$. از این رو $\boldsymbol{x} \in W$؛ یعنی $V(K) \subseteq W$. از طرفی بنا به قضیه‌ی **۴.۳.۴** $V(K)$ در V چگال است. بنابراین $W \nsubseteq V$. اما بوضوح برای هر $\boldsymbol{x} \in W$ و هر $f \in I(V)$ داریم $f(\boldsymbol{x}) = ۰$؛ یعنی $\boldsymbol{x}$ متعلق به V است، پس $W \subseteq V$ که تناقض است.

□

قضیه ۷.۳.۴. فرض کنید K یک میدان شبه‌بسته‌ی جبری و $F = K(\boldsymbol{x})$ یک توسیع منتظم باشد. همچنین فرض کنید y یک عنصر ناصفر از $K[\boldsymbol{x}]$ باشد. در این صورت همریختی $\varphi : K[\boldsymbol{x}] \to K$ به گونه‌ای موجود است که $\varphi(y) \neq ۰$.

اثبات. واریته‌ی V را به گونه‌ای در نظر می‌گیریم که $\boldsymbol{x}$ نقطه‌ی عمومی آن باشد. بنا به لم **۴۷.۲.۴** واریته‌ی V یک واریته‌ی تعریف شده روی K است. حال فرض می‌کنیم y یک عنصر ناصفر از $K[\boldsymbol{x}]$ است، یعنی چندجمله‌ای $g \in K[\boldsymbol{X}]$ به گونه‌ای موجود است که $g(\boldsymbol{x}) = y \neq ۰$. می‌خواهیم نشان دهیم همریختی $\varphi : K[\boldsymbol{x}] \to K$ به گونه‌ای موجود است که $\varphi(y) \neq ۰$. بدین منظور نشان می‌دهیم عنصر $\boldsymbol{a} \in K$ به گونه‌ای موجود است که برای هر $f \in K[\boldsymbol{X}]$ اگر $f(\boldsymbol{x}) = ۰$ آنگاه $f(\boldsymbol{a}) = ۰$ و $g(\boldsymbol{a}) \neq ۰$.

مجموعه‌ی باز زاریسکی $U = \{a \in V \mid g(a) \neq ۰\}$ را در نظر می‌گیریم. $\boldsymbol{x} \in U$، پس U ناتهی است. از طرفی بنا به قضیه‌ی **۴.۳.۴** $V(K)$ در V چگال است. از این رو اشتراک $V(K)$ با هر زیرمجموعه‌ی باز از V ناتهی است. بنابراین $U \cap V(K) \neq \emptyset$؛ یعنی عنصر $x \in V(K)$ موجود است به طوری که $x \in U$. به بیان دیگر $U(K)$ ناتهی است. عنصر $a \in U(K)$ را در نظر می‌گیریم. با توجه به تعریف مجموعه‌ی U، داریم $a \in V(K)$. بنابراین برای هر $f \in I(V)$ داریم $f(a) = ۰$. از طرفی $\boldsymbol{x}$ نقطه‌ی عمومی V است، پس واضح است که $\boldsymbol{a}$ یک ویژه‌سازی از $\boldsymbol{x}$ است. بنابراین $\boldsymbol{a}$ یک نقطه‌ی متعلق به K است به طوری که برای هر $f \in K[\boldsymbol{X}]$ داریم اگر $f(\boldsymbol{x}) = ۰$ آنگاه $f(\boldsymbol{a}) = ۰$. همچنین $g(\boldsymbol{a}) \neq ۰$. بنابراین کافی است تصویر $\boldsymbol{x}$ در K را $\boldsymbol{a}$ در نظر بگیریم و این ویژه‌سازی را به یک همریختی $\varphi : K[\boldsymbol{x}] \to K$ توسیع می‌دهیم که $\varphi(y) \neq ۰$. □

تعریف ۸.۳.۴. فرض کنید $f \in K[X, Y]$ یک چندجمله‌ای مطلقاً تحویل‌ناپذیر باشد. مجموعه‌ی $\Gamma = \{(x, y) \in A^۲ \mid f(x, y) = ۰\}$ را یک منحنی مسطح تعریف شده روی K می‌نامیم.

یک چندجمله‌ای $f(X,Y) \in K[X,Y]$ را می‌توانیم به صورت

$$f(X,Y) = f(X,Y)_d + f_{d-1}(X,Y) + \ldots + f_0(X,Y)$$

بنویسیم که در آن $f(X,Y)_k$ یک چندجمله‌ای همگن از درجه‌ی $k = 0, \ldots, d$ است و $f(X,Y)_d \neq 0$. در این صورت درجه‌ی منحنی مسطح $\Gamma = \{(x,y) \in A^2 \mid f(x,y) = 0\}$ برابر با d است.

یک چندجمله‌ای مطلقاً تحویل‌ناپذیر $f \in K[X,Y]$ و منحنی مسطح $\Gamma = \{(x,y) \in A^2 \mid f(x,y) = 0\}$ تعریف شده روی میدان K را در نظر بگیرید. فرض کنید (x,y) یک نقطه‌ی عمومی برای آن باشد. با توجه به این‌که چندجمله‌ای f مطلقاً تحویل‌ناپذیر است. بنا به نتیجه‌ی ۵۳.۲.۴، توسیع $K(x,y)$ روی K یک توسیع منتظم است. بنابراین طبق لم ۴۷.۲.۴، منحنی مسطح Γ یک واریته‌ی تعریف شده روی K است.

قضیه ۹.۳.۴. فرض کنید K یک میدان نامتناهی و L یک توسیع جبری از آن باشد. در این صورت میدان L یک میدان شبه‌بسته‌ی جبری است اگروتنهااگر هر منحنی مسطح تعریف شده روی K یک ریشه در L داشته باشد.

اثبات. برای دیدن اثبات، به منبع [۹، قضیه‌ی ۳.۲.۱۱] مراجعه کنید. □

نتیجه ۱۰.۳.۴. میدان K شبه‌بسته‌ی جبری است اگروتنهااگر هر چندجمله‌ای مطلقاً تحویل‌ناپذیر $f(X,Y) \in K[X,Y]$ یک ریشه در K داشته باشد.

نتیجه ۱۱.۳.۴. هر توسیع جبری از یک میدان شبه‌بسته‌ی جبری، شبه‌بسته‌ی جبری است.

اثبات. فرض می‌کنیم K یک میدان شبه‌بسته‌ی جبری و L یک توسیع جبری از آن باشد. کافی است نشان دهیم L نیز شبه‌بسته‌ی جبری است. در قضیه‌ی ۵.۳.۴ دیدیم هر میدان شبه‌بسته‌ی جبری نامتناهی است. از این رو K یک میدان نامتناهی است. بنابراین از قضیه‌ی ۹.۳.۴ نتیجه می‌شود که L نیز یک میدان شبه‌بسته‌ی جبری است. □

قضیه ۱۲.۳.۴. هر توسیع جبری نامتناهی از یک میدان متناهی، یک میدان شبه‌بسته‌ی جبری است.

اثبات. برای دیدن اثبات این قضیه به منبع [۹، نتیجه‌ی ۴.۲.۱۱] مراجعه کنید. □

در پایان این زیربخش یک مسئله‌ی باز در زمینه‌ی میدان‌های شبه‌بسته‌ی جبری را مطرح می‌کنیم.

تعریف ۱۳.۳.۴. میدان K را شبه‌بسته‌ی مینیمال می‌نامیم هرگاه هیچ زیرمیدان سره از آن شبه‌بسته‌ی جبری نباشد.

مسئله ۱۴.۳.۴. آیا یک میدان شبه‌بسته‌ی جبری مینیمال وجود دارد که توسیع جبری از یک میدان متناهی نباشد؟

۱.۳.۴ اصل بندی مرتبه‌ی اول برای میدان‌های شبه‌بسته‌ی جبری

در زیربخش قبلی دیدیم که یک تعریف معادل برای ویژگی شبه‌بسته‌ی جبری بودن به صورت زیر است: میدان K شبه‌بسته‌ی جبری است اگروتنهااگر هر منحنی مسطح تعریف شده روی K، در K ریشه داشته باشد. به بیان دیگر میدان K شبه‌بسته‌ی جبری است اگرو تنهااگر هر چندجمله‌ای مطلقاً تحویل‌ناپذیر $f(X,Y) \in K[X,Y]$ یک ریشه در $K^۲$ داشته باشد. در این بخش نشان خواهیم داد که تعریف فوق را می‌توان به صورت مرتبه اول بیان کرد؛ یعنی ویژگی شبه‌بسته‌ی جبری بودن یک ویژگی مرتبه‌ی اول است.

فرض کنید R یک حوزه‌ی صحیح و K میدان کسرهای آن باشد. مجموعه‌ی همه‌ی چندجمله‌ای‌های $f \in R[X_۱, ..., X_n]$ که در آن برای هر $i = ۱, ..., n$، $\deg_{X_i}(f) < d$ را با $S_R(n,d)$ نمایش می‌دهیم. بنابراین $S_R(n,d)$ مجموعه چندجمله‌ای‌های $f \in R[X_۱, ..., X_n]$ است به طوری که درجه‌ی هر متغیر در f کمتر از d است.

تعریف ۱۵.۳.۴ (تعویض کرونکر)**.** نگاشت $S_d : S_R(n,d) \to S_R(۱, d^n)$ که برای هر $i = ۱, ..., n$ به صورت $X_i \to Y^{d^{i-۱}}$ عمل می‌کند را تعویض کرونکر می‌نامیم.

توجه ۱۶.۳.۴. نحوه‌ی عملکرد تعویض کرونکر به صورت زیر است:

$$\begin{aligned} X_۱ &\to Y^{d^۰} = Y, \\ X_۲ &\to Y^d, \\ X_n &\to Y^{d^{n-۱}}. \end{aligned}$$

در نتیجه

$$\begin{aligned} X_۱^{i_۱} &\to Y^{i_۱}, \\ X_۲^{i_۲} &\to (Y^{i_۲})^d = Y^{i_۲ d}, \\ X_n^{i_n} &\to (Y^{i_n})^{d^{n-۱}} = Y^{i_n d^{n-۱}}. \end{aligned}$$

بنابراین داریم:

$$f(X_۱, ..., X_n) = \sum a_i X_۱^{i_۱} ... X_n^{i_n} \Longrightarrow S_d(f)(Y) = \sum a_i Y^{i_۱ + ... + i_n d^{n-۱}}.$$

واضح است که تعویض کرونکر ضرایب چندجمله‌ای را بدون تغییر حفظ می‌کند.

توجه ۱۷.۳.۴. ۱. نگاشت $(i_۱, ..., i_n) \to i_۱ + i_۲ d + ... + i_n d^{n-۱}$ یک‌به‌یک و پوشاست.

۲. دو چندجمله‌ای دلخواه f و g متعلق به $S_R(n,d)$ را در نظر بگیرید. واضح است که داریم $S_d(f\cdot g)=S_d(f)S_d(g)$.

لم ۱۸.۳.۴. اگر چندجمله‌ای $f\in S_R(n,d)$ در $\tilde{K}$ تجزیه شود، آنگاه در یک توسیع میدانی متناهی از K با درجه‌ی حداکثر $(d^n-1)!$ تجزیه می‌شود.

اثبات. چندجمله‌ای دلخواه $f\in S_R(n,d)$ را در نظر می‌گیریم و فرض می‌کنیم f در $\tilde{K}[X_1\cdots X_n]$ تجزیه شود. بنابراین $f=g\cdot h$ به طوری که $g,h\in \tilde{K}[X_1,\cdots X_n]$. واضح است که $S_d(f)=S_d(g\cdot h)=S_d(g)S_d(h)$. با توجه به تعویض کرونکر $S_d(f)$ یک چندجمله‌ای تک متغیره با ضرایب در میدان K است. بنابراین از این‌که $S_d(f)$ در $\tilde{K}$ به صورت $S_d(g)S_d(h)$ تجزیه شده است، نتیجه می‌شود که $S_d(f)$ حداکثر در یک توسیع متناهی از میدان K از درجه‌ی $(d^n-1)!$ تجزیه می‌شود. در نتیجه $S_d(g)$ و $S_d(h)$ متعلق به یک توسیع متناهی از میدان K با حداکثر درجه‌ی $(d^n-1)!$ هستند. به بیان دیگر ضرایب $S_d(g)$ و $S_d(h)$ متعلق به یک توسیع متناهی از میدان K با حداکثر درجه‌ی $(d^n-1)!$ است. حال با توجه به این‌که تعویض کرونکر ضرایب چندجمله‌ای را حفظ می‌کند، g و h دو چندجمله‌ای n متغیره با ضرایب در یک توسیع متناهی از میدان K با حداکثر درجه‌ی $(d^n-1)!$ هستند به طوری که $f=g\cdot h$. □

گزاره ۱۹.۳.۴. میدان K با مشخصه‌ی p را در نظر بگیرید. چندجمله‌ای $f\in S_K(n,d)$ مطلقاً تحویل‌ناپذیر است اگروتنهااگر دو شرط زیر برقرار باشد:

۱. چندجمله‌ای f در هر توسیع جدایی‌پذیر متناهی از K با حداکثر درجه‌ی $(d^n-1)!$ تحویل‌ناپذیر باشد،

۲. هیچ چندجمله‌ای $g\in \tilde{K}[\boldsymbol{X}]$ موجود نباشد به طوری که $f=g^p$.

قضیه ۲۰.۳.۴. میدان K با مشخصه‌ی p را در نظر بگیرید. فرض کنید $f\in S_K(n,d)$ یک چندجمله‌ای مطلقاً تحویل‌ناپذیر باشد. در این صورت برای هر چندجمله‌ای تحویل‌ناپذیر $h\in K[T]$ از درجه‌ی حداکثر $(d^n-1)!$، هیچ $g_1,g_2,g_3\in K[T,\boldsymbol{X}]$ وجود ندارد به طوری که

۱. $\deg_T(g_i)<(d^n-1)!$ و $\deg_{x_j}(g_i)<d$ برای $i=1,2$ و $j=1,...,n$،

۲. $\deg_T(g_3)<2((d^n-1)!)$ و $\deg_{x_j}(g_3)<d$ برای $j=1,...,n$،

۳. $f(\boldsymbol{X})=g_1(T,\boldsymbol{X})g_2(T,\boldsymbol{X})+g_3(T,\boldsymbol{X})h(T)$،

۴. حداقل برای یک $1\le j\le n$ داریم $\frac{\partial f}{\partial X_j}\not\equiv 0$.

اثبات. بنا به گزاره‌ی ۱۹.۳.۴ چندجمله‌ای $f \in S_K(n,d)$ مطلقاً تحویل‌ناپذیر است اگروتنهااگر اولاً روی هر توسیع جدایی‌پذیر از K با حداکثر درجه‌ی $(d^n-1)!$ تحویل‌ناپذیر باشد. ثانیاً اگر p امین توان از یک چندجمله‌ای روی $\tilde{K}$ نباشد.

ابتدا شرط اول را بررسی می‌کنیم. بنا به قضیه‌ی ۳۰.۳.۱ هر توسیع جدایی‌پذیر از درجه‌ی متناهی، یک توسیع ساده است. بنابراین هر توسیع جدایی‌پذیر از K به صورت یک $K[\boldsymbol{X}][T]$ است به طوری که T ریشه‌ی یک چندجمله‌ای h است. از طرفی $K[\boldsymbol{X}][t] \cong \frac{K[\boldsymbol{X},T]}{\langle h\rangle}$. بنابراین تجزیه شدن چندجمله‌ای f در یک توسیع جدایی‌پذیر معادل با تجزیه شدن در $\frac{K[\boldsymbol{X},T]}{\langle h\rangle}$ است؛ یعنی $f(\boldsymbol{X}) = g_1(T,\boldsymbol{X})g_2(T,\boldsymbol{X}) + g_3(T,\boldsymbol{X})h(T)$. به بیان دیگر این‌که چندجمله‌ای $f(\boldsymbol{X})$ روی هر توسیع جدایی‌پذیر از K با حداکثر درجه‌ی $(d^n-1)!$ تحویل‌ناپذیر باشد؛ معادل است با این‌که برای هر چندجمله‌ای تحویل‌ناپذیر $h \in K[T]$ از درجه‌ی حداکثر $(d^n-1)!$، هیچ $g_1, g_2, g_3 \in K[\boldsymbol{X}, T]$ وجود نداشته باشند به طوری که

۱. $\deg_T(g_i) < (d^n-1)!$ و $\deg_{x_j}(g_i) < d$ برای $i = 1, 2$ و $j = 1, ..., n$،

۲. $\deg_T(g_3) < 2((d^n-1)!)$ و $\deg_{x_j}(g_3) < d$ برای $j = 1, ..., n$،

۳. $f(\boldsymbol{X}) = g_1(T,\boldsymbol{X})g_2(T,\boldsymbol{X}) + g_3(T,\boldsymbol{X})h(T)$.

حال کافی است نشان دهیم شرط دوم، معادل است با این‌که چندجمله‌ای f حداقل یک مشتق جزئی داشته باشد. فرض کنید $f = g^p$ به طوری که g یک چندجمله‌ای متعلق به $\tilde{K}[\boldsymbol{X}]$ باشد. در این صورت مشتق جزئی از f نسبت به هر یک از متغیرها، شامل ضریب p است و چون مشخصه‌ی میدان p است این مشتق جزئی برابر با صفر خواهد بود. بنابراین این شرط که f، p امین توان از یک چندجمله‌ای روی $\tilde{K}$ نیست، معادل است با این‌که مشتق جزئی f حداقل نسبت به یکی از متغیرهای $X_1, \cdots, X_n$ مخالف صفر است؛ یعنی حداقل برای یک $1 \le j \le n$ داریم $\frac{\partial f}{\partial X_j} \not\equiv 0$.

□

توجه کنید برای این‌که در ادامه بتوانیم جملات فوق را به صورت مرتبه اول بیان کنیم لازم است درجه‌ی چندجمله‌ای‌ها محدود و مشخص باشند. از طرفی با توجه به این‌که این تجزیه در یک توسیع متناهی از K صورت می‌گیرد، درجات محدود هستند و دو شرط اول، صرفاً به جهت تعیین کردن یک کران بالا برای این درجات و محدود کردن آنها است.

قضیه ۲۱.۳.۴. فرض کنید $f = \sum_{i=0}^{d-1}\sum_{j=0}^{d-1} a_{ij}X^iY^j \in S_K(2,d)$ یک چندجمله‌ای باشد. جمله‌ی « f یک چندجمله‌ای مطلقاً تحویل‌ناپذیر است » را می‌توانیم در زبان $L_{ring} \cup \{a_{ij}\}$ به صورت مرتبه اول بیان کنیم.

اثبات. کافی است شروط ذکر شده در قضیه‌ی ۲۰.۳.۴ را به صورت مرتبه‌ی اول بنویسیم.

۱. یک چندجمله‌ای $h \in K[T]$ از درجه‌ی حداکثر $(d^n - ۱)!$ به صورت $h = \sum_{i=۰}^{(d^n-۱)!-۱} b_i T^i$ است.

۲. یک چندجمله‌ای $g_۱ \in K[X,Y,T]$ به طوری‌که $\deg_T(g_۱) < (d^n-۱)!$ و $\deg_X(g_۱), \deg_Y(g_۱) < d$ به صورت $g_۱ = \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱}\sum_{k=۰}^{(d^n-۱)!-۱} c_{ijk}X^iY^jT^k$ است.

۳. به طور مشابه $g_۲ = \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱}\sum_{k=۰}^{(d^n-۱)!-۱} q_{ijk}X^iY^jT^k$.

۴. یک چندجمله‌ای $g_۳ \in K[X,Y,T]$ به طوری که $\deg_T(g_۳) < ۲((d^n - ۱)!)$ و $\deg_X(g_۳), \deg_Y(g_۳) < d$ به صورت $g_۳ = \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱}\sum_{K=۰}^{۲((d^n-۱)!)-۱} l_{ijk}X^iY^jT^k$ است.

۵. مشتق جزئی f نسبت به X به صورت $\sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱} ia_{ij}X^{i-۱}Y^j$ است.

۶. به طور مشابه مشتق جزئی f نسبت به Y به صورت $\sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱} ja_{ij}X^iY^{j-۱}$ است.

توجه کنید که d یک عدد طبیعی مثبت و مشخص است. همچنین منظور از عبارت‌هایی مانند X^d در واقع $\underbrace{X \times \cdots \times X}_{d\text{بار}}$ است. بنابراین جمله‌ی

$$\forall b_i(\neg(\exists c_{ijk}, q_{ijk}, l_{ijk}(\forall X,Y,T(\sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱} a_{ij}X^iY^j = \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱}\sum_{k=۰}^{(d^n-۱)!-۱} c_{ijk}X^iY^jT^k \cdot \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱}\sum_{k=۰}^{(d^n-۱)!-۱} q_{ijk}X^iY^jT^k + \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱}\sum_{K=۰}^{۲((d^n-۱)!)-۱} l_{ijk}X^iY^jT^k \cdot \sum_{i=۰}^{(d^n-۱)!-۱} b_iT^i)))) \wedge (\sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱} ia_{ij}X^{i-۱}Y^j \neq ۰ \vee \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱} ja_{ij}X^iY^{j-۱} \neq ۰)$$

در زبان $L_{ring} \cup \{a_{ij}\}$ بیان می‌کند چندجمله‌ای $f = \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱} a_{ij}X^iY^j$ مطلقاً تحویل‌ناپذیر است.

□

قضیه ۲۲.۳.۴. ویژگی شبه‌بسته‌ی جبری بودن یک ویژگی مرتبه اول است.

اثبات. دیدیم که میدان K شبه‌بسته‌ی جبری است اگروتنهااگر هر چندجمله‌ای مطلقاً تحویل‌ناپذیر $f(X,Y) \in K[X,Y]$ یک ریشه در K داشته باشد. از طرفی بنا به قضیه‌ی ۲۱.۳.۴ مطلقاً تحویل‌ناپذیر بودن یک ویژگی مرتبه اول است. همچنین به وضوح ریشه داشتن را می‌توان به صورت مرتبه اول نوشت بنابراین تعریف شبه‌بسته‌ی جبری را می‌توان در زبان حلقه‌ها به صورت زیر نوشت.

جمله‌ی زیر بیان می‌کند که هر چندجمله‌ای مطلقاً تحویل‌ناپذیر $f(X,Y) \in S_K(۲,d)$ یک ریشه در $K^۲$ دارد.

$$\theta_d = \forall a_{ij}((\forall b_i(\neg(\exists c_{ijk}, q_{ijk}, l_{ijk}(\forall X,Y,T(\sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱} a_{ij}X^iY^j = \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱}\sum_{k=۰}^{(d^n-۱)!-۱} c_{ijk}X^iY^jT^k \cdot$$
$$\sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱}\sum_{k=۰}^{(d^n-۱)!-۱} q_{ijk}X^iY^jT^k + \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱}\sum_{K=۰}^{۲((d^n-۱)!)-۱} l_{ijk}X^iY^jT^k \cdot \sum_{i=۰}^{(d^n-۱)!-۱} b_iT^i)))) \wedge$$
$$(\sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱} ia_{ij}X^{i-۱}Y^j \neq ۰ \vee \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱} ja_{ij}X^iY^{j-۱} \neq ۰)) \rightarrow (\exists X,Y \sum_{i=۰}^{d-۱}\sum_{j=۰}^{d-۱} a_{ij}X^iY^j = ۰))$$

کافی است جمله‌ی فوق را برای هر $d = ۱,۲,\cdots$ بنویسیم. در این صورت جملات $\theta_۱, \theta_۲, \ldots$ در زبان حلقه‌ها وجود دارند به طوری که میدان K شبه‌بسته‌ی جبری است اگر وتنها اگر جملات $\theta_۱, \theta_۲, \ldots$ برقرار باشند. □

قضیه ۲۳.۳.۴. میدان K شبه‌بسته‌ی جبری است اگروتنهااگر در هر توسیع منتظم خود، بسته‌ی وجودی باشد.

اثبات. ابتدا فرض می‌کنیم K یک میدان شبه‌بسته‌ی جبری و F یک توسیع منتظم از K باشد. باید نشان دهیم برای هر فرمول $\varphi\{X_۱, \cdots, X_n, \boldsymbol{b}\}$ که در آن $\boldsymbol{b}$ پارامترهایی از K هستند اگر $F \models \exists \boldsymbol{x} \;\; \varphi(\boldsymbol{x}, \boldsymbol{b})$ آنگاه $K \models \exists \boldsymbol{x} \;\; \varphi(\boldsymbol{x}, \boldsymbol{b})$. می‌دانیم هر فرمول در زبان حلقه‌ها به صورت

$$\bigvee_{i\in I}\bigwedge_{j\in J_i}[f_{ij}(\boldsymbol{X}, \boldsymbol{b}) = ۰ \wedge g_i(\boldsymbol{X}, \boldsymbol{b}) \neq ۰]$$

است. بنابراین فرض می‌کنیم $F \models \exists \boldsymbol{x} \;\; \bigvee_{i\in I}\bigwedge_{j\in J_i}[f_{ij}(\boldsymbol{x}, \boldsymbol{b}) = ۰ \wedge g_i(\boldsymbol{x}, \boldsymbol{b}) \neq ۰]$ باید نشان دهیم عنصر $\boldsymbol{x'}$ متعلق به K^n به گونه‌ای موجود است که $K \models \bigvee_{i\in I}\bigwedge_{j\in J_i}[f_{ij}(\boldsymbol{x'}, \boldsymbol{b}) = ۰ \wedge g_i(\boldsymbol{x'}, \boldsymbol{b}) \neq ۰]$.

بنا به لم ۴۸.۲.۴ مجموعه‌ی همه‌ی ویژه‌سازی‌های $\boldsymbol{x}$ یک واریته‌ی تعریف شده V روی K است. با توجه به این‌که برای هر $i \in I$ داریم $g_i(\boldsymbol{x}) \neq ۰$، پس بوضوح $\prod_{i\in I} g_i(\boldsymbol{x}) \neq ۰$. بنابراین $\prod_{i\in I} g_i(\boldsymbol{x})$ وارون‌پذیر است؛ یعنی $\boldsymbol{y} \in \Omega$ موجود است به طوری که $\prod_{i\in I} g_i(\boldsymbol{x}).y = ۱$. حال مجموعه‌ی جبری V' را به گونه‌ای در نظر می‌گیریم که $(\boldsymbol{x}, y)$ نقطه‌ی عمومی آن باشد. از آنجا که y وارون $\prod_{i\in I} g_i(\boldsymbol{x})$ است داریم $y \in K(\boldsymbol{x})$. در نتیجه $K(\boldsymbol{x}, y) = K(\boldsymbol{x})$. از طرفی بنا به لم ۴۷.۲.۴ توسیع $K(\boldsymbol{x})$ یک توسیع منتظم از K است. بنابراین $K(\boldsymbol{x}, y)$ نیز یک توسیع منتظم از K است، پس بنا به لم ۴۷.۲.۴ واریته‌ی V' یک واریته‌ی تعریف شده روی K است. نهایتاً از آنجا که K یک میدان شبه‌بسته‌ی جبری است و V' یک واریته‌ی تعریف شده روی K است بنا به تعریف میدان شبه‌بسته‌ی جبری V' در خود K یک ریشه دارد؛ یعنی $(\boldsymbol{x'}, y')$ در K موجود است به طوری که $(\boldsymbol{x'}, y') \in V'$. با توجه به این‌که $(\boldsymbol{x}, y)$ نقطه عمومی V' است می‌دانیم $(\boldsymbol{x'}, y')$ یک ویژه سازی از $(\boldsymbol{x}, y)$ است. از طرفی $y \prod_{i\in I} g_i(\boldsymbol{x'}) - ۱ = ۰$، پس $y' \prod_{i\in I} g_i(\boldsymbol{x'}) = ۱$. در نتیجه $\prod_{i\in I} g_i(\boldsymbol{x'}) \neq ۰$. بنابراین برای هر $i \in I$ داریم $g_i(\boldsymbol{x'}) \neq ۰$. از طرفی با توجه به این‌که $(\boldsymbol{x'}, y')$ یک ویژه‌سازی از $(\boldsymbol{x}, y)$ است برای هر چندجمله‌ای

f داریم اگر $f(\boldsymbol{x}) = ۰$ آنگاه $f(\boldsymbol{x'}) = ۰$. در نتیجه $K \models \bigvee_{i\in I}\bigwedge_{j\in J_i}[f_{ij}(\boldsymbol{x'},\boldsymbol{b}) = ۰ \wedge g_i(\boldsymbol{x'},\boldsymbol{b}) \neq ۰]$؛ یعنی $K \models \exists \boldsymbol{x} \bigvee_{i\in I}\bigwedge_{j\in J_i}[f_{ij}(\boldsymbol{x},\boldsymbol{b}) = ۰ \wedge g_i(\boldsymbol{x},\boldsymbol{b}) \neq ۰]$.

حال برای اثبات جهت عکس، فرض می‌کنیم K در هر توسیع منتظم بسته‌ی وجودی باشد. می‌خواهیم نشان دهیم K یک میدان شبه‌بسته‌ی جبری است. بنابراین کافی است نشان دهیم هر واریته‌ی تعریف شده روی K در خود K یک ریشه دارد.

واریته‌ی V تعریف شده روی K را با نقطه عمومی $\boldsymbol{x}$ در نظر می‌گیریم. می‌دانیم که هر ایده‌آل از $K[\boldsymbol{X}]$ متناهیاً تولید شده است، پس چندجمله‌ای‌های $f_۱, \cdots, f_n$ وجود دارند به طوری که $I(V) = \langle f_۱, \cdots, f_n\rangle$. بنابراین برای هر $i = ۱, \cdots, n$ داریم $f_i(\boldsymbol{x}) = ۰$. یعنی $F \models \exists \boldsymbol{x} \bigwedge_{i=۱}^{n} f_i(\boldsymbol{x}) = ۰$.

از طرفی بنا به لم **۴۷.۲.۴** توسیع $F = K(\boldsymbol{x})$ روی K یک توسیع منتظم است. بنابراین K در F بسته‌ی وجودی است. در نتیجه $K \models \exists \boldsymbol{x} \bigwedge_{i=۱}^{n} f_i(\boldsymbol{x}) = ۰$؛ یعنی عنصر $\boldsymbol{a} \in K$ موجود است به طوری که برای هر $i = ۱, \cdots, n$ داریم $f_i(\boldsymbol{a}) = ۰$. پس بنا به لم **۱۳.۲.۴** عنصر $\boldsymbol{a}$ متعلق به واریته‌ی V است. به بیان دیگر واریته‌ی V یک ریشه در K دارد.

□

خلاصه‌ی فصل:

فرض کنید K یک میدان و Ω یک توسیع بسته‌ی جبری از آن است. گفتیم که $A^n = \{(x_۱, ..., x_n) \mid x_i \in \Omega\}$ و برای هر زیرمجموعه‌ی دلخواه $\boldsymbol{a} \subseteq K[\boldsymbol{X}] = K[X_۱, ..., X_n]$، مجموعه‌ی جبری تولید شده توسط $\boldsymbol{a}$ را به صورت $V(\boldsymbol{a}) = \{\boldsymbol{x} \in A^n \mid \forall f \in \boldsymbol{a} \quad f(\boldsymbol{x}) = ۰\}$ تعریف کردیم و گفتیم که مجموعه‌ی دلخواه X را یک مجموعه‌ی جبری می‌نامیم هرگاه $\boldsymbol{a} \subseteq K[\boldsymbol{X}]$ موجود باشد به طوری که $X = V(\boldsymbol{a})$. برای هر زیرمجموعه‌ی $A \subseteq A^n$ مجموعه‌ی $I_K(A) = \{f \in K[\boldsymbol{X}] \mid \forall \boldsymbol{x} \in A \quad f(\boldsymbol{x}) = ۰\}$ یک ایده‌آل رادیکال در حلقه‌ی $K[\boldsymbol{X}]$ است که آن را ایده‌آل وابسته به A می‌نامیم. نشان دادیم که مجموعه‌های جبری در A^n، مجموعه‌های بسته‌ی توپولوژی زاریسکی هستند از این رو به آن‌ها مجموعه‌ی بسته می‌گوییم.

یک مجموعه‌ی بسته‌ی V تحویل‌پذیر است هرگاه دو مجموعه‌ی بسته‌ی $V_۱, V_۲ \neq V$ موجود باشند به طوری که $V = V_۱ \cup V_۲$. همچنین گفتیم که منظور از یک واریته یک مجموعه‌ی بسته‌ی تحویل‌ناپذیر است.

فرض کنید V یک K واریته باشد. می‌گوییم V مطلقاً تحویل‌ناپذیر است هرگاه در هر توسیع از K تحویل‌ناپذیر باقی بماند. اگر V یک K واریته‌ی مطلقاً تحویل‌ناپذیر باشد، می‌گوییم V یک واریته‌ی تعریف شده روی K است هرگاه $I_{\tilde{K}}(V) = \tilde{K} I_K(V)$.

میدان K شبه‌بسته‌ی جبری است هرگاه هر واریته‌ی تعریف شده روی K، یک ریشه در K داشته باشد. اثبات کردیم که اگر میدان K یک میدان شبه‌بسته‌ی جبری و V یک واریته‌ی تعریف شده روی K باشد، در این

صورت K نامتناهی است و $V(K)$ در V چگال است. دیدیم که یک تعریف معادل برای میدان شبه‌بسته‌ی جبری به صورت زیر است:

میدان K شبه‌بسته‌ی جبری است اگروتنهااگر هر چندجمله‌ای مطلقاً تحویل‌ناپذیر $f(X,Y) \in K[X,Y]$ یک ریشه در K^2 داشته باشد.

به کمک این تعریف اثبات کردیم که ویژگی شبه‌بسته‌ی جبری بودن یک ویژگی مرتبه اول است.

فصل ۵

تعریف‌پذیری وجودی حلقه‌های ارزیاب هنسلی

۱.۵ مقدمه

در این فصل تعریف‌پذیری حلقه‌های ارزیاب هنسلی را مورد بررسی قرار می‌دهیم و ثابت می‌کنیم که اگر $(K, \mathcal{O})$ یک میدان ارزیابی هنسلی با میدان باقیمانده‌های متناهی یا شبه‌بسته‌ی جبری باشد، حلقه‌ی ارزیاب آن با یک فرمول وجودی و بدون پارامتر در زبان حلقه‌ها تعریف می‌گردد. بدین منظور ابتدا اثبات می‌کنیم که اگر دو زیرمجموعه‌ی U و T از حلقه‌ی ارزیاب $\mathcal{O}$ در زبان حلقه‌ها، به گونه‌ای باشند که $\mathfrak{m} \subseteq U$ و T همه‌ی کلاس‌های باقیمانده را قطع کند (تعریف ۱.۲.۵)، آنگاه می‌توانیم $\mathcal{O}$ را به صورت $\mathcal{O} = U + T$ در نظر بگیریم. سپس برای حالتی که میدان باقیمانده‌ها متناهی یا شبه‌بسته‌ی جبری باشد U و T را به گونه‌ای معرفی می‌کنیم که اولاً تعریف‌پذیر باشند، ثانیاً ویژگی‌های مطلوب ما را داشته باشند. در نهایت تعریف‌پذیری $\mathcal{O}$ را از تعریف‌پذیری U و T نتیجه می‌گیریم. در واقع مطالب این فصل محتوای مقاله‌ی اصلی این پایان‌نامه، یعنی منبع [۷] است.

در سرتاسر این فصل فرض می‌کنیم که K یک میدان ارزیابی هنسلی با حلقه‌ی ارزیاب $\mathcal{O} \subseteq K$، ایده‌آل ماکزیمال $\mathfrak{m} \subseteq \mathcal{O}$ و میدان باقیمانده‌های $F = \mathcal{O}/\mathfrak{m}$ است. برای هر $a \in \mathcal{O}$ تصویر کانونی a در میدان باقیمانده‌ها را به صورت $\bar{a} = a + \mathfrak{m} \in F$ و تصویر هر چندجمله‌ای $f \in \mathcal{O}[X]$ در $F[X]$ را با نماد $\bar{f}$ نمایش می‌دهیم. همچنین از نماد $F_\circ$ برای نمایش میدان اول F استفاده می‌کنیم. بنابراین اگر F متناهی باشد، $F_\circ$ به صورت یک $\mathbb{F}_p$ است و اگر F نامتناهی باشد $F_\circ$ همان میدان $\mathbb{Q}$ است.

۲.۵ دو زیرمجموعه‌ی تعریف‌پذیر از $\mathcal{O}$

در این بخش ویژگی‌هایی را بیان می‌کنیم که اگر دو زیرمجموعه‌ی T و U از حلقه‌ی ارزیاب $\mathcal{O}$ دارای این ویژگی‌ها باشند داریم $\mathcal{O} = T + U$.

در سرتاسر این فصل تصویر یک مجموعه‌ی $T \subseteq \mathcal{O}$ در F را با نماد $\bar{T}$ نمایش می‌دهیم، بنابراین $\bar{T} = \{\bar{t} \mid t \in T\}$.

تعریف ۱.۲.۵. فرض کنید $T \subseteq \mathcal{O}$، می‌گوییم مجموعه‌ی T همه‌ی کلاس‌های باقیمانده را قطع می‌کند هرگاه $\bar{T} = F$.

لم ۲.۲.۵. فرض کنید $T, U \subseteq \mathcal{O}$ به گونه‌ای باشند که $\mathfrak{m} \subseteq U$ و T همه‌ی کلاس‌های باقیمانده را قطع کند، آنگاه $\mathcal{O} = T + U$.

اثبات. ابتدا نشان می‌دهیم که $T + U \subseteq \mathcal{O}$. بدین منظور عنصر دلخواه $t + u \in T + U$ را در نظر می‌گیریم. بنا به فرض داریم $T, U \subseteq \mathcal{O}$، پس $t, u \in \mathcal{O}$. بنابراین با توجه به این‌که $\mathcal{O}$ یک حلقه است داریم $t + u \in \mathcal{O}$. در نتیجه $T + U \subseteq \mathcal{O}$. حال باید نشان دهیم که $\mathcal{O} \subseteq T + U$. عنصر دلخواه $x \in \mathcal{O}$ را در نظر می‌گیریم. بنا به فرض، T همه‌ی کلاس‌های باقیمانده را قطع می‌کند. بنابراین عنصر t متعلق به T موجود است به طوری که $\bar{t} = \bar{x}$، به بیان دیگر $\bar{x} = t + \mathfrak{m}$. از این رو عنصر a متعلق به $\mathfrak{m}$ موجود است به طوری که $x = t + a$. در نتیجه $\mathcal{O} \subseteq T + \mathfrak{m}$؛ از طرفی $\mathfrak{m} \subseteq U$. بنابراین $\mathcal{O} \subseteq T + \mathfrak{m} \subseteq T + U$ و در نهایت $\mathcal{O} = T + U$. □

نتیجه ۳.۲.۵. فرض کنید $T, U \subseteq \mathcal{O}$ در شرایط لم ۲.۲.۵ صدق کنند. در این صورت اگر U و T به ترتیب توسط فرمول‌های φ و ψ تعریف شوند، آنگاه $\mathcal{O}$ به سادگی توسط فرمول زیر تعریف می‌شود:

$$\eta(x) \equiv (\exists t, u)(x = t + u \wedge \varphi(u) \wedge \psi(t)).$$

همچنین واضح است که اگر فرمول‌های φ و ψ وجودی و بدون پارامتر باشند؛ فرمول η نیز وجودی و بدون پارامتر خواهد بود.

۳.۵ معرفی یک مجموعه‌ی تعریف‌پذیر بین $\mathfrak{m}$ و $\mathcal{O}$

در این بخش قصد داریم برای هر چندجمله‌ای مطلوب f یک زیرمجموعه‌ی $U_f \subseteq \mathcal{O}$ را به گونه‌ای معرفی کنیم که تعریف‌پذیر باشد و $\mathfrak{m} \subseteq U_f$. بدین منظور چندجمله‌ای $f \in \mathcal{O}[X]$ را به گونه‌ای در نظر می‌گیریم که در K ریشه نداشته باشد. اثبات می‌کنیم که اگر $f \in \mathcal{O}[X]$ یک چندجمله‌ای تکین باشد، $\bar{f}$ در F ریشه نداشته

باشد و یک عنصر a متعلق به $\mathcal{O}$ موجود باشد به طوری که $f'(a) \notin \mathfrak{m}$، آنگاه برای مجموعه‌ی تعریف‌پذیر $U_f := \{\frac{۱}{f(x)} - \frac{۱}{f(y)} \mid x, y \in K\}$ داریم $\mathfrak{m} \subseteq U_f \subseteq \mathcal{O}$.

تعریف ۱.۳.۵. چندجمله‌ای $f \in \mathcal{O}[X]$ را در نظر بگیرید و فرض کنید برای هر $x \in K$ داریم $f(x) \neq ۰$. قرار می‌دهیم $f(K)^{-۱} = \{\frac{۱}{f(x)} \mid x \in K\}$. مجموعه‌ی U_f را به صورت زیر تعریف می‌کنیم:

$$U_f = f(K)^{-۱} - f(K)^{-۱} := \{\frac{۱}{f(x)} - \frac{۱}{f(y)} \mid x, y \in K\}.$$

همچنین برای هر $a \in K$ تعریف می‌کنیم:

$$U_{f,a} = f(K)^{-۱} - f(a)^{-۱} := \{\frac{۱}{f(x)} - \frac{۱}{f(a)} | x \in K\}.$$

لم ۲.۳.۵. چندجمله‌ای $f \in \mathcal{O}[X]$ را در نظر بگیرید، U_f در میدان K به صورت وجودی تعریف‌پذیر است. همچنین اگر $f \in \mathbb{Z}[X]$، آنگاه U_f به صورت وجودی و بدون پارامتر تعریف‌پذیر است.

اثبات. بنا به تعریف U_f واضح است که فرمول وجودی زیر، آن را در K تعریف می‌کند. به بیان دیگر U_f در K به صورت وجودی تعریف‌پذیراست.

$$\varphi_f(x) \equiv (\exists y, z, y_۱, z_۱)(x = y_۱ - z_۱ \wedge y_۱ f(y) = ۱ \wedge z_۱ f(z) = ۱).$$

واضح است که پارامترهای فرمول فوق در واقع ضرایب چندجمله‌ای f هستند. بنابراین اگر $f \in \mathcal{O}[X]$ آنگاه فرمول معرفی شده، یک فرمول وجودی با پارامتر است. اما از آنجا که عناصر حلقه‌ی $\mathbb{Z}$ همگی به کمک عنصر ثابت ۱ ایجاد می‌شوند اگر $f \in \mathbb{Z}[X]$، آنگاه ضرایب این چندجمله‌ای توسط ثابت ۱ ایجاد می‌شوند و در این صورت فرمول $\varphi_f(x)$ یک فرمول وجودی و بدون پارامتر خواهد بود. □

یادآوری می‌کنیم که چندجمله‌ای $f \in \mathcal{O}[X]$ را تکین می‌نامیم هرگاه ضریب جمله‌ی اول آن (جمله‌ای که بالاترین درجه را دارد) برابر با ۱ باشد. به بیان دیگر منظور از چندجمله‌ای تکین f یک چندجمله‌ای به صورت $f(x) = x^n + c_{n-۱}x^{n-۱} + \ldots + c_۰$ است.

لم ۳.۳.۵. فرض کنید $f \in \mathcal{O}[X]$ یک چندجمله‌ای تکین است و $\bar{f}$ در F ریشه ندارد. در این صورت داریم $f(K)^{-۱} = \{\frac{۱}{f(x)} \mid x \in K\} \subseteq \mathcal{O}$.

اثبات. عنصر دلخواه $b \in K$ را در نظر می‌گیریم؛ باید نشان دهیم $\frac{۱}{f(b)} \in \mathcal{O}$. به بیان دیگر باید نشان دهیم $v\left(\frac{۱}{f(b)}\right) \geq ۰$. از آنجا که $v\left(\frac{۱}{f(b)}\right) = v(۱) - v(f(b))$ و $v(۱) = ۰$ داریم $v\left(\frac{۱}{f(b)}\right) = -v(f(b))$. بنابراین کافی است اثبات کنیم $-v(f(b)) \geq ۰$ یا به عبارتی $v(f(b)) \leq ۰$.

می‌دانیم $b \in K$، پس بسته به این‌که $b \in \mathcal{O}$ یا $b \notin \mathcal{O}$ دو حالت رخ می‌دهد:

۱. $b \in \mathcal{O}$: اثبات می‌کنیم که در این حالت $v(f(b)) = ۰$. با توجه به این‌که $\mathcal{O}$ یک حلقه است، از این‌که $b \in \mathcal{O}$ و f یک چندجمله‌ای متعلق $\mathcal{O}[X]$ است، نتیجه می‌شود که $f(b) \in \mathcal{O}$. از طرفی بنا به فرض می‌دانیم که $\bar{f}$ در F ریشه ندارد. بنابراین $\bar{f}(\bar{b}) \neq ۰$. همچنین $\overline{f(b)} = \bar{f}(\bar{b})$، پس $\overline{f(b)} \neq ۰$. به بیان دیگر $f(b) \notin \mathfrak{m}$. بنابراین $v(f(b)) = ۰$.

۲. $b \notin \mathcal{O}$: اثبات می‌کنیم که در این حالت $v(f(b)) < ۰$. فرض می‌کنیم چندجمله‌ای f از درجه‌ی n باشد. از آنجا که f تکین است داریم $f(b) = b^n + c_{n-۱}b^{n-۱} + \ldots + c_۰$. بنابراین

$$v(f(b)) \geq \min\{v(b^n), v(c_{n-۱}b^{n-۱}), \cdots, v(c_۰)\}.$$

از طرفی

$$\min\{v(b^n), v(c_{n-۱}b^{n-۱}), \cdots, v(c_۰)\} = \min\{v(b^n), v(c_{n-۱}) + (n-۱)v(b), \cdots, v(c_۰)\}$$

پس $v(f(b)) \geq \min\{v(b^n), v(c_{n-۱})+(n-۱)v(b), \cdots, v(c_۰)\}$. ادعا می‌کنیم $v(f(b)) = v(b^n)$.
برای اثبات این ادعا کافی است نشان دهیم:

$$v(b^n) \neq v(c_{n-۱}b^{n-۱}), \cdots, v(b^n) \neq v(c_۰)$$

و

$$\min\{v(b^n), v(c_{n-۱}) + (n-۱)v(b), ..., v(c_۰)\} = v(b^n).$$

توجه کنید که برای هر $i = ۱, \ldots, n$ داریم $c_i \in \mathcal{O}$. بنابراین $v(c_i) \geq ۰$. از طرفی $b \notin \mathcal{O}$، پس $v(b) < ۰$. همچنین می‌دانیم f یک چندجمله‌ای تکین است و b^n بزرگترین جمله در f است؛ یعنی b^n بالاترین درجه را دارد و ضریب آن دقیقاً برابر با ۱ است. از این رو برای هر $i < n$ داریم $v(b^n) \lneqq v(c_ib^i)$.
(زیرا $v(b^n) = nv(b)$ و $v(c_ib^i) = v(c_i) + iv(b)$). بنابراین $v(f(b)) = v(b^n) = nv(b)$، پس با توجه به این‌که $v(b) < ۰$ داریم $v(f(b)) < ۰$.

بنابراین برای هر b متعلق به K داریم $v\left(\frac{۱}{f(b)}\right) \geq ۰$. در نتیجه $\frac{۱}{f(b)} \in \mathcal{O}$. □

نتیجه ۴.۳.۵. فرض کنید $f \in \mathcal{O}[X]$ یک چندجمله‌ای تکین است و $\bar{f}$ در F ریشه ندارد. در این صورت برای هر عنصر $a \in K$ داریم $U_{f,a} \subseteq \mathcal{O}$.

اثبات. عنصر دلخواه $\frac{۱}{f(a)} - \frac{۱}{f(x)}$ متعلق به $U_{f,a}$ را در نظر می‌گیریم. از آنجا که a متعلق به K است داریم $\frac{۱}{f(a)} \in f(K)^{-۱}$. از طرفی بنا به لم ۳.۳.۵ داریم $f(K)^{-۱} \subseteq \mathcal{O}$. بنابراین $\frac{۱}{f(a)}, \frac{۱}{f(x)} \in \mathcal{O}$. حال از این‌که $\mathcal{O}$ یک حلقه است، نتیجه می‌شود که $\frac{۱}{f(a)} - \frac{۱}{f(x)} \in \mathcal{O}$. □

لم ۵.۳.۵. فرض کنید $f \in \mathcal{O}[X]$ یک چندجمله‌ای تکین است و $\bar{f}$ در F ریشه ندارد. برای هر عنصر $a \in \mathcal{O}$ اگر $f'(a) \notin \mathfrak{m}$ آنگاه $\mathfrak{m} \subseteq U_{f,a}$.

اثبات. عنصر دلخواه $b \in \mathfrak{m}$ را در نظر می‌گیریم. می‌خواهیم نشان دهیم که $b \in U_{f,a}$. بدین منظور کافی است نشان دهیم عنصر $d \in K$ موجود است به طوری که $\frac{1}{f(a)} - \frac{1}{f(d)} = b$؛ یعنی $bf(d) - 1 + \frac{f(d)}{f(a)} = 0$.
به بیان دیگر باید نشان دهیم معادله‌ی $bf(x)f(a) + f(x) - f(a)$ در K ریشه دارد. بدین منظور قرارمی‌دهیم $g(x) = bf(x)f(a) + f(x) - f(a)$. نشان می‌دهیم که $g'(a) \notin \mathfrak{m}$ و $g(a) \in \mathfrak{m}$. سپس از این‌که حلقه‌ی $\mathcal{O}$ هنسلی است نتیجه می‌گیریم $g(x)$ در K ریشه دارد.
داریم $g'(x) = bf'(x)f(a) + f'(x) = f'(x)(bf(a) + 1)$. بنابراین $g'(a) = f'(a)(bf(a) + 1)$.
ادعا می‌کنیم که $v(g'(a)) = 0$. به منظور اثبات این ادعا ابتدا توجه کنید که $a \in \mathcal{O}$، $f \in \mathcal{O}[x]$ و $\mathcal{O}$ یک حلقه است. بنابراین $f'(a) \in \mathcal{O}$. اما با توجه به فرض $f'(a) \notin \mathfrak{m}$، پس $v(f'(a)) = 0$. از طرفی $v(g'(a)) = v(f'(a)) + v(bf(a) + 1)$. از این رو $v(g'(a)) = v(bf(a) + 1)$.
توجه کنید که $v(bf(a) + 1) \geq \min\{v(bf(a)), v(1)\}$ و $v(bf(a)) = v(b) + v(f(a))$. بنابراین $v(g'(a)) \geq \min\{v(b) + v(f(a)), v(1)\}$. طبق فرض $a \in \mathcal{O}$، پس بنا به بخش (۱) اثبات لم ۳.۳.۵ داریم $v(f(a)) = 0$. همچنین $b \in \mathfrak{m}$، پس $v(b) > 0$. بنابراین $v(b) + v(f(a)) = v(b) > 0$. از طرفی $v(1) = 0$. از این رو $v(1) \neq v(b)$ و $\min\{v(b), v(1)\} = v(1) = 0$. در نتیجه $v(g'(a)) = \min\{v(b), v(1)\} = v(1) = 0$. بنابراین $g'(a) \notin \mathfrak{m}$.
حال کافی است نشان دهیم $g(a) \in \mathfrak{m}$. می‌دانیم $g(a) = bf(a)f(a) + f(a) - f(a) = bf(a)f(a)$. بنابراین $v(g(a)) = v(bf(a)f(a)) = v(b) + 2v(f(a))$. بنا به فرض $a \in \mathcal{O}$، پس با توجه به بخش (۱) اثبات لم ۳.۳.۵ داریم $v(f(a)) = 0$. از طرفی $b \in \mathfrak{m}$، پس $v(b) > 0$. بنابراین $v(g(a)) = v(b) > 0$. در نتیجه $g(a) \in \mathfrak{m}$.
بنابراین از هنسلی بودن حلقه‌ی $\mathcal{O}$ نتیجه می‌شود که عنصر d متعلق به $\mathcal{O}$ (به طور کلی $d \in K$) موجود است به طوری که $g(d) = 0$. به بیان دیگر عنصر d متعلق به $\mathcal{O}$ موجود است به طوری که $b = \frac{1}{f(d)} - \frac{1}{f(a)}$. □

به طور خلاصه اگر $f \in \mathcal{O}[X]$ یک چندجمله‌ای تکین باشد و $\bar{f}$ در F ریشه نداشته باشد، برای هر عنصر $a \in \mathcal{O}$ اگر $f'(a) \notin \mathfrak{m}$ آنگاه $\mathfrak{m} \subseteq U_{f,a} \subseteq \mathcal{O}$. اما به دلایلی که در ادامه توضیح خواهیم داد، علی‌رغم آنکه $U_{f,a}$ شرایط مطلوب ما را دارد از آن استفاده نمی‌کنیم. در لم زیر اثبات می‌کنیم که اگر چندجمله‌ای $f \in \mathcal{O}[X]$ و یک عنصر $a \in \mathcal{O}$ به گونه‌ای موجود باشند که شرایط لم قبل را برآورده کنند، آنگاه $\mathfrak{m} \subseteq U_f \subseteq \mathcal{O}$.

لم ۶.۳.۵. فرض کنید $f \in \mathcal{O}[X]$ یک چندجمله‌ای تکین باشد، $\bar{f}$ در F ریشه نداشته باشد و عنصر $a \in \mathcal{O}$ وجود داشته باشد به طوری که $f'(a) \notin \mathfrak{m}$ آنگاه $\mathfrak{m} \subseteq U_f \subseteq \mathcal{O}$.

اثبات. ابتدا نشان می‌دهیم $U_f = \{\frac{۱}{f(x)} - \frac{۱}{f(y)} \mid x, y \in K\} \subseteq \mathcal{O}$. بدین منظور عناصر دلخواه $a, b \in K$ را در نظر می‌گیریم. باید نشان دهیم $u = \frac{۱}{f(a)} - \frac{۱}{f(b)} \in \mathcal{O}$. بنا به فرض چندجمله‌ای f تکین است و $\bar{f}$ در F ریشه ندارد، بنابراین از لم ۳.۳.۵ داریم $f(K)^{-۱} = \{\frac{۱}{f(x)} \mid x \in K\} \subseteq \mathcal{O}$، پس $\frac{۱}{f(a)}, \frac{۱}{f(b)} \in \mathcal{O}$ و چون $\mathcal{O}$ یک حلقه است داریم $u = \frac{۱}{f(a)} - \frac{۱}{f(b)} \in \mathcal{O}$. در نتیجه $U_f \subseteq \mathcal{O}$.

حال فرض کنید عنصر a متعلق به $\mathcal{O}$ به گونه‌ای باشد که $f'(a) \notin \mathfrak{m}$. از این‌که $a \in \mathcal{O}$ نتیجه می‌شود که $\frac{۱}{f(a)} \in f(K)^{-۱}$. بنابراین $f(K)^{-۱} - \frac{۱}{f(a)} \subseteq f(K)^{-۱} - f(K)^{-۱}$. یا به بیان دیگر $U_{f,a} \subseteq U_f$. از طرفی بنا به لم ۵.۳.۵ داریم $\mathfrak{m} \subseteq U_{f,a}$. از این رو $\mathfrak{m} \subseteq U_{f,a} \subseteq U_f$. در نتیجه $\mathfrak{m} \subseteq U_f \subseteq \mathcal{O}$. □

تا اینجا دیدیم که اگر $U, T \subseteq \mathcal{O}$ به گونه‌ای باشند که $\mathfrak{m} \subseteq U$ و $\bar{T} = F$ آنگاه $\mathcal{O} = U + T$ و از تعریف‌پذیری آن‌ها تعریف‌پذیری $\mathcal{O}$ نتیجه می‌شود. همچنین دیدیم که اگر $f \in \mathcal{O}[X]$ یک چندجمله‌ای تکین باشد، $\bar{f}$ در F ریشه نداشته باشد و عنصر $a \in \mathcal{O}$ وجود داشته باشد به طوری که $f'(a) \notin \mathfrak{m}$ آنگاه برای مجموعه‌ی تعریف پذیر $U_f = f(K)^{-۱} - f(K)^{-۱}$ داریم $\mathfrak{m} \subseteq U_f \subseteq \mathcal{O}$. بنابراین در ادامه با در نظر گرفتن میدان باقیمانده‌های مناسب، شرایطی را ایجاد می‌کنیم که تحت آن بتوانیم اثبات کنیم چندجمله‌ای f با ویژگی‌های ذکر شده وجود دارد. همچنین $T \subseteq \mathcal{O}$ را به گونه‌ای معرفی می‌کنیم که $\bar{T} = F$.

۴.۵ میدان باقیمانده‌های متناهی

در این بخش فرض می‌کنیم که میدان باقیمانده‌ها متناهی است و نشان می‌دهیم که در این حالت چندجمله‌ای $f \in \mathcal{O}[X]$ موجود است به طوری که U_f در شرایط لم ۶.۳.۵ صدق می‌کند. سپس مجموعه‌ی T را به گونه‌ای تعریف می‌کنیم که ویژگی‌های ذکر شده در لم ۲.۲.۵ را داشته باشد و در آخر اثبات می‌کنیم که حلقه‌ی $\mathcal{O}$ به صورت وجودی و بدون پارامتر تعریف‌پذیر است.

۱.۴.۵ وجود چندجمله‌ای مناسب f

مشاهده ۱.۴.۵. برای هر عدد طبیعی n و هر $a_۱, \ldots, a_n \in \mathbb{Z}$ داریم:

$$\prod_{i=۱}^{n}(x + a_i) = x^n + a_{n-۱}x^{n-۱} + a_{n-۲}x^{n-۲} + \cdots + a_۱$$

که در آن برای هر $k < n$، ضریب a_{n-k} برابر است با مجموع همه‌ی k تایی‌ها؛ یعنی $a_{n-k} = \sum_{i=۱} a_{i_۱} \ldots a_{i_k}$. بنابراین $a_{n-۱} = \sum_{i=۱}^{n} a_i$ و $a_۱ = \prod_{i=۱}^{n} a_i$.

لم ۲.۴.۵. برای هر عدد اول p و هر عدد صحیح مثبت m، چندجمله‌ای تکین، تحویل‌ناپذیر و جدایی‌پذیر $f \in \mathbb{F}_p[X]$ از درجه‌ی m وجود دارد به طوری که $f'(۰) \neq ۰$.

اثبات. فرض می‌کنیم $q = p^m$. توسیع $\mathbb{F}_q/\mathbb{F}_p$ یک توسیع گالوایی است. بنابراین، با توجه به نتیجه‌ی ۱۴.۴.۱ عنصر $\alpha \in \mathbb{F}_q$ موجود است به طوری که $\{\alpha, \alpha^p, ..., \alpha^{p^{m-۱}}\}$ یک پایه‌ی نرمال برای این توسیع است. همچنین با توجه به این‌که درجه‌ی توسیع $\mathbb{F}_q/\mathbb{F}_p$ برابر است با m، بوضوح چندجمله‌ای مینیمال α از درجه‌ی m است. حال فرض کنید $f \in \mathbb{F}_p[X]$ چندجمله‌ای مینیمال $\alpha^{-۱}$ باشد. ادعا می‌کنیم که این چندجمله‌ای همه‌ی ویژگی‌های مطلوب را داراست.

بنا به تعریف چندجمله‌ای مینیمال، این چندجمله‌ای تکین و تحویل ناپذیر است. از طرفی $\mathbb{F}_p$ متناهی است، پس بنا به قضیه‌ی ۴.۵.۱ تام است. از این رو هر چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}_p$ جدایی‌پذیر است. بنابراین چندجمله‌ای f جدایی‌پذیر نیز است. کافی است اثبات کنیم که $f'(۰) \neq ۰$.

چندجمله‌ای مینیمال α از درجه‌ی m است، پس بنا به لم ۳.۲.۱ درجه‌ی چندجمله‌ای f نیز m است. بنابراین

$$f(x) = a_۰ + a_۱x + \cdots + a_{m-۱}x^{m-۱} + x^m$$

و

$$f'(x) = a_۱ + \cdots + (m-۱)a_{m-۱}x^{m-۲} + mx^{m-۱}.$$

بنابراین $f'(۰) = a_۱$، پس کافی است اثبات کنیم $a_۱ \neq ۰$. از آنجا که f چندجمله‌ای مینیمال $\alpha^{-۱}$ است داریم $f(\alpha^{-۱}) = a_۰ + a_۱\frac{۱}{\alpha} + \ldots + a_{m-۱}(\frac{۱}{\alpha})^{m-۱} + (\frac{۱}{\alpha})^m = ۰$. از ضرب طرفین چندجمله‌ای فوق در α^m داریم $\alpha^m f(\alpha^{-۱}) = a_۰\alpha^m + a_۱\alpha^{m-۱} + \ldots + a_{m-۱}\alpha + ۱ = ۰$. حال با تقسیم طرفین بر $a_۰$ به چندجمله‌ای تکین $\frac{\alpha^m f(\alpha^{-۱})}{a_۰} = \alpha^m + \frac{a_۱}{a_۰}\alpha^{m-۱} + \ldots + \frac{a_{m-۱}}{a_۰}\alpha + \frac{۱}{a_۰} = ۰$ می‌رسیم. بنابراین $g(x) = \frac{\alpha^m f(x)}{a_۰} = x^m + \frac{a_۱}{a_۰}x^{m-۱} + \ldots + \frac{a_{m-۱}}{a_۰}x + \frac{۱}{a_۰}$ یک چندجمله‌ای تکین با درجه‌ی m است که در α صفر می‌شود، که با توجه به یکتا بودن چندجمله‌ای مینیمال، $g(x)$ چندجمله‌ای مینیمال α است. بنا به تعریف پایه‌ی نرمال، ریشه‌های چندجمله‌ای $g(x)$ به صورت $\{\alpha, \alpha^p, ..., \alpha^{p^{m-۱}}\}$ است. بنابراین $g(x) = (x-\alpha)(x-\alpha^p)...(x-\alpha^{p^{m-۱}})$، پس بنا به مشاهده‌ی ۱.۴.۵ داریم:

$$g(x) = x^m + \frac{a_۱}{a_۰}x^{m-۱} + ... + \frac{a_{m-۱}}{a_۰}x + \frac{۱}{a_۰} = x^m + x^{m-۱}\sum_{i=۰}^{m-۱}\alpha^{p^i} + ... + \prod_{i=۰}^{m-۱}\alpha^{p^i}.$$

از این رو $\frac{a_۱}{a_۰} = \sum_{i=۰}^{m-۱}\alpha^{p^i}$ و $\frac{۱}{a_۰} = \prod_{i=۰}^{m-۱}\alpha^{p^i}$. بنابراین $a_۱ = \frac{\sum_{i=۰}^{m-۱}\alpha^{p^i}}{\prod_{i=۰}^{m-۱}\alpha^{p^i}}$. از طرفی با توجه به این‌که $\{\alpha, \alpha^p, ..., \alpha^{p^{m-۱}}\}$ یک پایه‌ی نرمال است؛ هر ترکیب خطی از عناصر آن، از جمله $\sum_{i=۱}^{m-۱}\alpha^{p^i}$ ناصفر است. از این رو $a_۱ = \frac{\sum_{i=۰}^{m-۱}\alpha^{p^i}}{\prod_{i=۰}^{m-۱}\alpha^{p^i}} \neq ۰$. در نتیجه $f'(۰) \neq ۰$. □

در لم زیر، اثبات می‌کنیم که چندجمله‌ای $f \in F_\circ[X]$ به گونه‌ای موجود است که ویژگی‌های ذکر شده در لم قبل را داراست و علاوه بر آن در F ریشه ندارد.

لم ۳.۴.۵. اگر F متناهی باشد، چندجمله‌ای $f \in F_\circ[X]$ موجود است به طوری که در F ریشه ندارد و تحویل‌ناپذیر، جدایی‌پذیر و تکین است. همچنین عنصر $a \in F$ به گونه‌ای وجود دارد که $f'(a) \neq \circ$.

اثبات. برای اثبات این لم، از لم ۲.۴.۵ کمک می‌گیریم. فرض می‌کنیم $q = p^k$ و $F = \mathbb{F}_q$ یک میدان متناهی باشد. در این صورت $F_\circ = \mathbb{F}_p$، پس بنا به لم ۲.۴.۵ برای هر عدد صحیح مثبت m چندجمله‌ای $f \in \mathbb{F}_p[X]$ از درجه‌ی m وجود دارد به طوری که تکین، تحویل‌ناپذیر و جدایی‌پذیر است و $f'(\circ) \neq \circ$. بنابراین کافی است a را $\circ$ در نظر بگیریم. در این صورت برای هر عدد صحیح مثبت m می‌توان گفت چندجمله‌ای $f \in F_\circ[X]$ از درجه‌ی m وجود دارد که تکین، تحویل‌ناپذیر و جدایی‌پذیر است و عنصر $a \in F$ به گونه‌ای موجود است که $f'(a) \neq \circ$. ادعا می‌کنیم که اگر m را به گونه‌ای در نظر بگیریم که $[F : F_\circ]$ را عاد نکند، آنگاه f در F ریشه ندارد.

فرض می‌کنیم m به گونه‌ای باشد که $[F : F_\circ]$ را عاد نکند و به برهان خلف عنصر b متعلق به F موجود باشد به طوری که $f(b) = \circ$. در این صورت $F_\circ(b) \subseteq F$. از طرفی چندجمله‌ای f یک چندجمله‌ای تحویل‌ناپذیر است پس چندجمله‌ای مینیمال b است . همچنین درجه‌ی f برابر است با m و مشخصه‌ی میدان $F_\circ$ برابر است با p. بنابراین طبق لم ۵.۲.۱ داریم $|F_\circ(b)| = p^m$. از طرفی $|F| = p^k$، پس بنا به مشاهده‌ی ۳.۴.۱ داریم $m \mid k$ که با فرض در تناقض است. در نتیجه f در F ریشه ندارد.

توجه کنید که اگر $F = \mathbb{F}_p$. بوضوح از تحویل‌ناپذیر بودن f نتیجه می‌شود f در $F = F_p$ ریشه ندارد. بنابراین در این حالت بررسی این‌که f در F ریشه ندارد به سادگی صورت می‌گیرد و نیازی به روند فوق نیست. □

۲.۴.۵ معرفی T و تعریف‌پذیری حلقه‌ی $\mathcal{O}$

قضیه ۴.۴.۵. فرض کنید K یک میدان ارزیابی هنسلی، با میدان باقیمانده‌های $F = \mathbb{F}_q$ باشد. قرار دهید $T := \{x \in K \mid x^q - x = \circ\}$. در این صورت $T \subseteq \mathcal{O}$ و $\bar{T} = F$.

اثبات. قرار می‌دهیم $g(X) = X^q - X \in \mathbb{Z}[X]$. بنابراین $T = \{x \in K \mid g(x) = \circ\}$. ابتدا اثبات می‌کنیم $T \subseteq \mathcal{O}$. بدین منظور عنصر دلخواه x متعلق به T را در نظر می‌گیریم داریم $x^q - x = \circ$، بنابراین دو حالت زیر ممکن است رخ دهد:

۱. $x = \circ$: در این حالت بوضوح $x \in \mathcal{O}$.

۲. $x \neq 0$: نشان می‌دهیم که در این حالت $v(x) = 0$ و در نتیجه $x \in \mathcal{O}$.

از آنجا که $x^q - x = 0$ داریم $x^q = x$. بنابراین $qv(x) = v(x)$. از طرفی Γ یک گروه ارزیاب است، پس یک گروه مرتب و در نتیجه بدون تاب است. بنابراین از این‌که $qv(x) = v(x)$ نتیجه می‌شود $v(x) = 0$ پس $x \in \mathcal{O}$.

حال کافی است اثبات کنیم $\bar{T} = F$. ابتدا توجه کنید که $\bar{g}(x) = \bar{1}X^q - \bar{1}X$ و $\bar{g}'(x) = \bar{1}qx^{q-1} - \bar{1}$. از آنجا که مشخصه‌ی میدان F برابر است با q، داریم $qx^{q-1} = \underbrace{x^{q-1} + \ldots + x^{q-1}}_{q \text{ بار}} = 0$. در نتیجه $\bar{g}' = -\bar{1} \neq 0$. از طرفی می‌دانیم که برای هر عنصر $\bar{x} \in F$ داریم $\bar{x}^q - \bar{x} = 0$، پس واضح است که $\bar{g}(\bar{x}) = 0$. حال از آنجا که $\bar{g}(\bar{x}) = 0$ و $\bar{g}' = -\bar{1} \neq 0$ از هنسلی بودن حلقه‌ی $\mathcal{O}$ نتیجه می‌شود که عنصر $a \in \mathcal{O}$ موجود است به طوری که $g(a) = 0$ و $\bar{a} = \bar{x}$. از این رو برای هر $\bar{x} \in F$، عنصر $a \in T$ موجود است به طوری که $a \in \bar{x}$. بنابراین $\bar{T} = F$.

توجه کنید که چون $\bar{T} = F$ واضح است که مجموعه‌ی T نمی‌تواند به صورت $T = \{0\}$ باشد. □

قضیه‌ی زیر اصلی‌ترین قضیه‌ی این بخش است. در این قضیه به کمک مطالبی که تا اینجا بیان کردیم اثبات می‌کنیم که اگر میدان باقیمانده‌ها متناهی باشد، حلقه‌ی ارزیاب $\mathcal{O}$ به صورت وجودی و بدون پارامتر تعریف‌پذیر است.

قضیه ۵.۴.۵. فرض کنید K یک میدان ارزیابی هنسلی با حلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های F باشد. اگر F متناهی باشد، یک تعریف وجودی و بدون پارامتر برای حلقه‌ی $\mathcal{O}$ در میدان K وجود دارد.

اثبات. با توجه به این‌که میدان F متناهی است فرض می‌کنیم $F = \mathbb{F}_q$ و چندجمله‌ای $g = X^q - X \in \mathbb{Z}[X]$ را در نظر می‌گیریم. قرار می‌دهیم $\psi(x) \equiv (g(x) = 0)$ و T را به صورت $T = \psi(K) = \{x \in K \mid g(x) = 0\}$ تعریف می‌کنیم. بنا به قضیه‌ی ۴.۴.۵ داریم $T \subseteq \mathcal{O}$ و $\bar{T} = F$. از طرفی بنا به لم ۳.۴.۵ چندجمله‌ای $f \in \mathbb{F}_p[X]$ موجود است به طوری که در F ریشه ندارد، تحویل‌ناپذیر، جدایی‌پذیر و تکین است. همچنین عنصر $a \in F$ به گونه‌ای موجود است که $f'(a) \neq 0$. می‌دانیم $f \in \mathbb{F}_p[X]$ و $a \in F$ به ترتیب تصویر کانونی یک $\tilde{f} \in \mathbb{Z}[X]$ و $\tilde{a} \in \mathcal{O}$ هستند، پس اصطلاحاً با برکشیدن چندجمله‌ای f و عنصر $a \in F$ چندجمله‌ای تکین و بدون پارامتر $\tilde{f} \in \mathbb{Z}[X]$ و عنصر $\tilde{a} \in \mathcal{O}$ را داریم به طوری که $\tilde{f}'(\tilde{a}) \notin \mathfrak{m}$. حال فرمول $\varphi_{\tilde{f}}(x) \equiv (\exists y, z, y_1, z_1)(x = y_1 - z_1 \wedge y_1 \tilde{f}(y) = 1 \wedge z_1 \tilde{f}(z) = 1)$ که در لم ۲.۳.۵ تعریف کردیم را در نظر می‌گیریم و قرار می‌دهیم $U_{\tilde{f}} := \varphi_{\tilde{f}}(K)$. بنا به لم ۶.۳.۵ داریم $\mathfrak{m} \subseteq U_{\tilde{f}} \subseteq \mathcal{O}$. حال فرمول وجودی و بدون پارامتر $\eta_{\tilde{f}}(x) \equiv (\exists u, t)(x = u + t \wedge \varphi_{\tilde{f}}(u) \wedge \psi_{\tilde{f}}(t))$ را در نظر می‌گیریم بنا به نتیجه‌ی ۳.۲.۵ داریم $\eta(K) = \mathcal{O}$؛ یعنی $\mathcal{O}$ به صورت وجودی و بدون پارامتر تعریف‌پذیر است. □

توجه ۶.۴.۵.

۱. همان طور که در ابتدای بحث گفته شد یکی از اهداف ما در این بخش یافتن مجموعه‌ی U_f به گونه‌ای بود که $\mathfrak{m} \subseteq U_f \subseteq \mathcal{O}$. در نتیجه‌ی ۴.۳.۵ و لم ۵.۳.۵ دیدیم که $\mathfrak{m} \subseteq U_{f,a} \subseteq \mathcal{O}$. اما $U_{f,a}$ را به عنوان مجموعه‌ی مطلوب انتخاب نکردیم و مجموعه‌ی U_f را تعریف و مورد استفاده قرار دادیم. در بخش حذف پارامتر اثبات قضیه‌ی ۵.۴.۵، علت انتخاب U_f و عدم انتخاب $U_{f,a}$ مشهود است. با دقت در اثبات لم ۳.۴.۵ خواهیم دید که چندجمله‌ای $f \in F_\circ[X]$ و $a \in F$ با شرایط مطلوب ما وجود دارند. سپس با برکشیدن $f \in F_\circ[X]$ و $a \in F$ به $\tilde{f} \in \mathbb{Z}[X]$ و عنصر $\tilde{a} \in \mathcal{O}$ می‌رسیم که در شرایط لم ۵.۳.۵ صدق می‌کنند. اما توجه کنید از این‌که $a \in F$ نتیجه می‌شود، $\tilde{a}$ متعلق به $\mathcal{O}$ است و لزوماً هنگام برکشیدن $\tilde{a}$ داخل $\mathbb{Z}$ قرار نمی‌گیرد. در این صورت مجموعه‌ی $U_{f,a}$ را نمی‌توانیم بدون پارامتر تعریف کنیم. بنابراین به جهت رفع این مشکل از مجموعه‌ی U_f استفاده می‌کنیم که در فرمول آن از a استفاده نشده است.

۲. نکته‌ی قابل توجه دیگر این است که اثبات کردیم یک چندجمله‌ای f با ویژگی‌های مطلوب ما در «میدان اول» وجود دارد. مهم‌ترین دلیل انتخاب f از $F_\circ$ این است که اگر ضرایب چندجمله‌ای f متعلق به $F_\circ$ باشند با برکشیدن، ضرایب چندجمله‌ای $\tilde{f}$ در $\mathbb{Z}$ قرار می‌گیرند. در این صورت همه‌ی ضرایب با عنصر ثابت ۱ تولید می‌شوند و در نتیجه پارامترها حذف می‌گردند.

۳.۴.۵ یک حالت خاص از میدان باقیمانده‌های متناهی

برای هر $d \in \mathbb{N}$ تعریف می‌کنیم $c(d) = (2d-1)^4$. در بخش قبل دیدیم به طور کلی زمانی که F متناهی باشد چندجمله‌ای $f \in \mathcal{O}[X]$ به گونه‌ای موجود است که $\mathfrak{m} \subseteq U_f \subseteq \mathcal{O}$. در این زیربخش به عنوان یک حالت خاص از میدان باقیمانده‌های متناهی، فرض می‌کنیم میدان F متناهی و $|F| > c(\deg(f))$ باشد. با در نظر گرفتن شرط فوق مجموعه‌ی T را به نحوی معرفی می‌کنیم که $T \subseteq \mathcal{O}$ و $\bar{T} = F$.

قضیه ۷.۴.۵. فرض کنید $f \in F[X]$ یک چندجمله‌ای غیر ثابت و خالی از مربع باشد. برای هر عنصر دلخواه $c \in F$، چندجمله‌ای $f(X)f(Y) - c \in F[X,Y]$ مطلقاً تحویل‌ناپذیر است.

اثبات. برای دیدن اثبات این قضیه به منبع [۱۰، گزاره‌ی ۱-۱] مراجعه کنید. □

قضیه ۸.۴.۵. فرض کنید $f(X,Y) \in \mathbb{F}_q[X,Y]$ یک چندجمله‌ای مطلقاً تحویل‌ناپذیر از درجه‌ی d و Γ منحنی آفین تعریف شده توسط $f(X,Y) = 0$ باشد. در این صورت اگر $q > (d-1)^4$ آنگاه $\Gamma(\mathbb{F}_q)$ ناتهی است.

اثبات. برای دیدن اثبات این قضیه به منبع [۹، نتیجه‌ی ۲.۴.۵] مراجعه کنید. □

چندجمله‌ای $f \in F[X]$ را در نظر بگیرید. در سرتاسر این فصل منظور از نماد $f(F)f(F)$ مجموعه‌ی $\{f(x)f(y) \mid x, y \in F\}$ است.

لم ۹.۴.۵. فرض کنید $f \in F[X]$ یک چندجمله‌ای غیر ثابت و خالی از مربع باشد. اگر F متناهی با $|F| \geq c(\deg(f))$ باشد، آنگاه $F = f(F)f(F) \cup \{۰\}$.

اثبات. ابتدا اثبات می‌کنیم $f(F)f(F) \cup \{۰\} \subset F$. عنصر دلخواه $a \in f(F)f(F) \cup \{۰\}$ را در نظر می‌گیریم. یکی از دو حالت زیر رخ می‌دهد:

۱. $a = ۰$: در این حالت با توجه به این‌که F میدان است پس شامل ۰ است. بنابراین $a \in F$.

۲. $a \in f(F)f(F)$: در این حالت $x, y \in F$ موجود هستند به طوری که $a = f(x)f(y)$. از طرفی $f \in F[X]$ و F یک میدان است. بنابراین $f(x), f(y) \in F$ و در نتیجه $f(x)f(y) \in F$. از این رو $a \in F$.

بنابراین $f(F)f(F) \cup \{۰\} \subseteq F$. حال کافی است نشان دهیم $F \subseteq f(F)f(F) \cup \{۰\}$، بدین منظور عنصر دلخواه $۰ \neq c \in F$ را در نظر می‌گیریم (واضح است که اگر $c = ۰$ آنگاه $c \in f(F)f(F) \cup \{۰\}$). بنا به قضیه‌ی ۷.۴.۵ چندجمله‌ای $f(X)f(Y) - c \in F[X, Y]$ مطلقاً تحویل‌ناپذیر است. از طرفی طبق فرض F متناهی با $|F| > c(\deg(f))$ است. فرض می‌کنیم درجه‌ی چندجمله‌ای f برابر است با d. بنابراین $q = |F| > (۲d - ۱)^۴ > (d - ۱)^۴$، پس بنا به قضیه‌ی ۸.۴.۵ عناصر $x, y \in F$ وجود دارند به طوری که $f(x)f(y) - c = ۰$؛ یعنی $f(x)f(y) = c$. از این رو $c = f(x)f(y) \in f(F)f(F) \cup \{۰\}$. در نتیجه $F \subseteq f(F)f(F) \cup \{۰\}$.

□

تعریف ۱۰.۴.۵. چندجمله‌ای $f \in \mathcal{O}[X]$ را در نظر بگیرید و فرض کنید برای هر $x \in K$ داریم $f(x) \neq ۰$. تعریف می‌کنیم $T_f := f(K)^{-۱}f(K)^{-۱} \cup \{۰\}$.

لم زیر بیان می‌کند که T ویژگی‌های ذکر شده در لم ۲.۲.۵ را دارد و لم بعدی به اثبات تعریف‌پذیری T می‌پردازد.

لم ۱۱.۴.۵. چندجمله‌ای تکین $f \in \mathcal{O}[X]$ را در نظر بگیرید. فرض کنید که $\bar{f}$ خالی از مربع باشد و در F ریشه نداشته باشد. در این صورت $T_f \subseteq \mathcal{O}$. علاوه بر این فرض‌ها اگر F متناهی با $|F| > c(\deg(f))$ باشد، آنگاه $\bar{T_f} = F$.

اثبات. ابتدا اثبات می‌کنیم که $T_f \subseteq \mathcal{O}$. عنصر دلخواه $a \in T_f$ را در نظر می‌گیریم یکی از دو حالت زیر رخ می‌دهد:

۱. $a = ۰$: در این حالت چون $\mathcal{O}$ حلقه است شامل عنصر ۰ است. بنابراین $a = ۰ \in \mathcal{O}$.

۲. $a \in f(K)^{-۱}f(K)^{-۱}$: در این حالت عناصر $\frac{۱}{f(x)}, \frac{۱}{f(y)} \in f(K)^{-۱}$ وجود دارند به طوری که $a = \frac{۱}{f(x)}\frac{۱}{f(y)}$. بنا به فرض $\bar{f}$ در F ریشه ندارد. بنابراین از لم ۳.۳.۵ داریم که $f(K)^{-۱} \subseteq \mathcal{O}$، پس $\frac{۱}{f(x)}, \frac{۱}{f(y)} \in \mathcal{O}$. از طرفی $\mathcal{O}$ یک حلقه است. بنابراین داریم $\frac{۱}{f(x)}\frac{۱}{f(y)} \in \mathcal{O}$؛ یعنی $a \in \mathcal{O}$.

بنابراین $T_f = f(K)^{-۱}f(K)^{-۱} \cup \{۰\} \subseteq \mathcal{O}$. حال فرض می‌کنیم F یک میدان متناهی با $|F| > c(\deg(f))$ است. اثبات می‌کنیم $\bar{T}_f = F$. ابتدا به طور کلی نشان می‌دهیم که $\bar{T} \subseteq F$. عناصر F به صورت $\bar{a} = a + \mathfrak{m}$ و عناصر $\bar{T}$ به صورت $\bar{b} = b + \mathfrak{m}$ به طوری که $a \in \mathcal{O}$، $b \in T_f$ و $\mathfrak{m}$ ایده‌آل ماکزیمال $\mathcal{O}$ است. همچنین دیدیم که $T_f \subseteq \mathcal{O}$ بنابراین $\bar{T}_f \subseteq F$.

حال کافی است نشان دهیم که $F \subseteq \bar{T}_f = \overline{f(K)^{-۱}f(K)^{-۱}} \cup \{\bar{۰}\}$. بدین منظور عناصر وارون پذیر و غیر وارون‌پذیر F را به صورت جداگانه مورد بررسی قرار می‌دهیم و اثبات می‌کنیم که عناصر وارون‌پذیر و غیر وارون‌پذیر F همگی عضو $\bar{T}_f$ هستند. در نتیجه $F \subseteq \bar{T}_f$. از این‌که F میدان است نتیجه می‌شود تمام عناصر آن وارون پذیر هستند مگر عنصر صفر این میدان، از طرفی مجموعه‌ی $\bar{T}_f$ شامل $\bar{۰}$ است. بنابراین بوضوح تنها عنصر غیر وارون‌پذیر F عضو $\bar{T}_f$ است. حال فرض کنید $F^\times$ مجموعه عناصر غیر وارون‌پذیر F باشد. بنابراین $F^\times \subseteq F$. از طرفی F متناهی با $|F| > c(\deg(f))$ است، پس بنا به لم ۹.۴.۵ داریم $F^\times \subseteq F = \bar{f}(F)\bar{f}(F)$. در نتیجه با وارون گرفتن از طرفین داریم $(\bar{f}(F)\bar{f}(F))^{-۱} \subseteq F^\times$. ادعا می‌کنیم که:

$$(\bar{f}(F)\bar{f}(F))^{-۱} \subseteq (\overline{f(\mathcal{O})} \cdot \overline{f(\mathcal{O})})^{-۱} \subseteq \overline{f(K)^{-۱}f(K)^{-۱}} \subseteq \bar{T}_f.$$

به منظور اثبات ادعای فوق عنصر دلخواه $\bar{f}(\bar{x})\bar{f}(\bar{y}) \in \bar{f}(F)\bar{f}(F)$ را در نظر می‌گیریم. می‌دانیم که $\bar{f}(\bar{x})\bar{f}(\bar{y}) = \overline{f(x)} \cdot \overline{f(y)}$ و $\overline{f(x)} \cdot \overline{f(y)} \in \overline{f(\mathcal{O})} \cdot \overline{f(\mathcal{O})}$. بنابراین $\overline{f(\mathcal{O})} \cdot \overline{f(\mathcal{O})} \subseteq \bar{f}(F)\bar{f}(F)$. در نتیجه $(\bar{f}(F)\bar{f}(F))^{-۱} \subseteq (\overline{f(\mathcal{O})} \cdot \overline{f(\mathcal{O})})^{-۱}$. حال فرض می‌کنیم که $\bar{f}(x)\bar{f}(y) \in \overline{f(\mathcal{O})} \cdot \overline{f(\mathcal{O})}$. از آنجا که $\mathcal{O} \subseteq K$ داریم $\bar{f}(x)\bar{f}(y) \in \overline{f(K)} \cdot \overline{f(K)}$. بنابراین

$$(\bar{f}(x)\bar{f}(y))^{-1} = \bar{f}(x)^{-1}\bar{f}(y)^{-1} \in (\overline{f(K)}.\overline{f(K)})^{-1} = (\overline{f(K)})^{-1}.(\overline{f(K)})^{-1} = \overline{f(K)^{-1}}.\overline{f(K)^{-1}} = \overline{f(K)^{-1}f(K)^{-1}}.$$

در نتیجه $\bar{T}_f = F$. □

لم ۱۲.۴.۵. چندجمله‌ای $f \in \mathcal{O}[X]$ را در نظر بگیرید. مجموعه‌ی $T_f = f(K)^{-1}f(K)^{-1} \cup \{0\} \subseteq \mathcal{O}$ تعریف‌پذیر وجودی است و اگر $f \in \mathbb{Z}[X]$ آنگاه T_f به صورت وجودی و بدون پارامتر تعریف‌پذیر است .

اثبات. با توجه به تعریف T_f واضح است که می‌توانیم آن را با فرمول وجودی زیر تعریف کنیم:

$$\psi_f(x) \equiv (\exists y, z, y_1, z_1)(x = 0 \vee (x = y_1 z_1 \wedge y_1 f(y) = 1 \wedge z_1 f(z) = 1)).$$

همچنین واضح است که تمام پارامترهای این فرمول مربوط به ضرایب چندجمله‌ای f است. به بیان دیگر در صورتی این فرمول بدون پارامتر خواهد بود که f بدون پارامتر باشد. از طرفی عناصر حلقه‌ی $\mathbb{Z}$ همگی به کمک عنصر ثابت ۱ ایجاد می‌شوند. از این رو اگر $f \in \mathbb{Z}[X]$، آنگاه همه‌ی ضرایب f توسط ثابت ۱ ایجاد می‌شوند و در نتیجه فرمول $\psi_f(x)$ یک فرمول وجودی و بدون پارامتر خواهد بود. بنابراین در این حالت T به صورت وجودی و بدون پارامتر تعریف‌پذیر است. □

در قضیه‌ی بعدی اثبات می‌کنیم که فرمول وجودی $\eta_f(x) \equiv (\exists u, t)(x = u + t \wedge \varphi_f(u) \wedge \psi_f(t))$ که در آن φ_f و ψ_f به ترتیب فرمول‌های تعریف شده در لم ۲.۳.۵ و لم ۱۲.۴.۵ هستند؛ حلقه‌ی ارزیاب $\mathcal{O}$ را تعریف می‌کند.

قضیه ۱۳.۴.۵. فرض کنید چندجمله‌ای تکین $f \in \mathcal{O}[X]$ به گونه‌ای باشد که $\bar{f}$ خالی از مربع باشد و در F ریشه نداشته باشد. در این صورت $\eta_f(K) \subseteq \mathcal{O}$. به علاوه اگر عنصر $a \in \mathcal{O}$ وجود داشته باشد به طوری که $f'(a) \notin \mathfrak{m}$ و میدان F متناهی با $|F| > c(\deg(f))$ باشد، آنگاه $\eta_f(K) = \mathcal{O}$.

اثبات. فرض می‌کنیم $U_f = \varphi_f(K)$. بنابراین U_f برابر است با مجموعه عناصری از میدان K که در فرمول زیر صدق می‌کنند:

$$\varphi_f(x) \equiv (\exists y, z, y_1, z_1)(x = y_1 - z_1 \wedge y_1 f(y) = 1 \wedge z_1 f(z) = 1).$$

بنا به لم ۶.۳.۵ داریم $U_f \subseteq \mathcal{O}$. حال مجموعه‌ی T را به صورت $T = \psi_f(K)$ در نظر می‌گیریم. در این صورت T برابر است با مجموعه عناصری از میدان K که در فرمول $\psi_f(x) \equiv (\exists y, z, y_1, z_1)(x = 0 \vee (x = y_1 z_1 \wedge y_1 f(y) = 1 \wedge z_1 f(z) = 1))$ صدق می‌کنند، پس بنا به لم ۱۱.۴.۵ داریم $T_f \subseteq \mathcal{O}$. در نتیجه با توجه به حلقه بودن $\mathcal{O}$ واضح است که $\eta_f(K) = T_f + U_f \subseteq \mathcal{O}$.

حال فرض می‌کنیم $a \in \mathcal{O}$ به گونه‌ای باشد که $f'(a) \notin \mathfrak{m}$ بنابراین از لم ۶.۳.۵ داریم $\mathfrak{m} \subseteq U_f$. از طرفی F متناهی با $|F| > c(\deg(f))$ است. بنابراین از لم ۱۱.۴.۵ داریم که $\bar{T}_f = F$. در نتیجه U_f و T_f در شرایط لم ۲.۲.۵ صدق می‌کنند، پس با توجه به این لم داریم $\eta_f(K) = \mathcal{O}$. □

توجه ۱۴.۴.۵. میدان دلخواه K را در نظر بگیرید. در قضیه‌ی ۷.۵.۱ دیدیم که اگر K تام باشد، چندجمله‌ای $f(x) \in K[X]$ جدایی‌پذیر است اگروتنهااگر خالی از مربع باشد. به بیان دیگر اگر K تام باشد، مفاهیم جدایی‌پذیری و خالی از مربع بودن معادلند. بنابراین با توجه به این‌که میدان اول تام است، چندجمله‌ای جدایی‌پذیر f که وجود آن را در لم ۳.۴.۵ اثبات کردیم در واقع یک چندجمله‌ای خالی از مربع است و شرایط مطلوب ما را دارد. در نتیجه نیازی به یافتن f جدید برای این بخش نداریم.

نتیجه ۱۵.۴.۵. فرض کنید K یک میدان ارزیابی هنسلی باحلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های F است. اگر F متناهی با $|F| > c(\deg(f))$ باشد، یک تعریف وجودی بدون پارامتر برای حلقه‌ی $\mathcal{O}$ در میدان K وجود دارد.

اثبات. چندجمله‌ای $f \in F_\circ[X]$ مربوط به لم ۳.۴.۵ را در نظر بگیرید. این چندجمله‌ای در F ریشه ندارد، تکین، تحویل‌ناپذیر و جدایی‌پذیر است. از قضیه‌ی ۵.۵.۱ داریم $F_\circ[X]$ تام است. بنابراین از این‌که چندجمله‌ای f جدایی‌پذیر است، نتیجه می‌شود که خالی از مربع نیز است. همچنین عنصر $a \in F$ وجود دارد به گونه‌ای که $f'(a) \neq 0$. حال فرض کنید که $\tilde{f} \in \mathbb{Z}[X]$ یک بر کشیدن [۱] تکین از f باشد و $\tilde{a} \in \mathcal{O}$ یک بر کشیدن از a باشد. در این صورت $\tilde{f}'(\tilde{a}) \notin \mathfrak{m}$ و بنا به قضیه‌ی ۱۳.۴.۵ داریم $\eta_{\tilde{f}}(K) = \mathcal{O}$. بنابراین حلقه‌ی $\mathcal{O}$ توسط فرمول وجودی و بدون پارامتر

$$\eta_{\tilde{f}} \equiv (\exists u, t)(x = u + t \wedge \varphi_{\tilde{f}} \wedge \psi_{\tilde{f}})$$

تعریف می‌گردد. □

لازم به ذکر است که تعریف فوق به q وابسته نیست. به بیان دیگر این تعریف، یک تعریف یکنواخت است. در پایان این فصل به کمک این تعریف یک تعریف یکنواخت برای حالت کلی ارائه خواهیم کرد.

توجه ۱۶.۴.۵. همان طور که گفته شد، در این زیربخش با در نظر گرفتن یک حالت خاص برای میدان باقیمانده‌ها (میدان باقیمانده‌های متناهی با $|F| > c(\deg(f))$) یک تعریف وجودی، متفاوت با تعریف بیان شده در زیربخش قبلی برای حلقه‌ی ارزیاب ارائه کردیم (به نتیجه‌ی ۱۵.۴.۵ مراجعه کنید). تفاوت این تعریف با تعریف ارائه شده در قضیه‌ی ۵.۴.۵ در نحوه‌ی معرفی T_f است. این تفاوت در T_f باعث می‌شود که فرمول ψ_f و در نتیجه فرمول η_f به دو شکل متفاوت نوشته شود. همچنین لازم به ذکر است که T_f مورد استفاده در این بخش با همان چندجمله‌ای سازنده‌ی U_f ساخته می‌شود. بنابراین فرمولی که در نتیجه‌ی ۱۵.۴.۵ معرفی می‌شود فقط به یک چندجمله‌ای f وابسته است.

[1] lift

۵.۵ میدان باقیمانده‌های شبه‌بسته‌ی جبری

در این بخش میدان باقیمانده‌ها را شبه بسته‌ی جبری در نظر می‌گیریم. ابتدا نشان می‌دهیم که در این حالت نیز چندجمله‌ای $f \in \mathcal{O}[X]$ موجود است به طوری که $U_f = f(K)^{-1} - f(K)^{-1}$ در شرایط لم ۶.۳.۵ صدق می‌کند. سپس مجموعه‌ی T را به گونه‌ای معرفی می‌کنیم که تعریف‌پذیر باشد و ویژگی‌های ذکر شده در لم ۲.۲.۵ را داشته باشد. در ادامه‌ی این فصل منظور از بستار جبری F_0 روی F، اشتراک بستار جبری F_0 با F است که آن را با نماد F_{alg} نمایش می‌دهیم.

۱.۵.۵ معرفی T و تعریف‌پذیری حلقه‌ی $\mathcal{O}$

در فصل گذشته دیدیم که میدان K شبه‌بسته‌ی جبری است اگروتنهااگر برای هر چندجمله‌ای مطلقاً تحویل‌ناپذیر $f \in K[X,Y]$ عنصر $(a,b) \in K^2$ موجود باشد به طوری که $f(a,b) = 0$.

در لم ۹.۴.۵ دیدیم که اگر $f \in F[X]$ یک چندجمله‌ای غیر ثابت و خالی از مربع و F یک میدان متناهی با $|F| \geq c(\deg(f))$ باشد آنگاه $F = f(F)f(F) \cup \{0\}$. در لم زیر مشابه این لم را برای حالتی که F یک میدان شبه‌بسته‌ی جبری باشد بیان کرده‌ایم.

لم ۱.۵.۵. فرض کنید $f \in F[X]$ یک چندجمله‌ای غیر ثابت و خالی از مربع باشد. اگر F شبه‌بسته‌ی جبری باشد آنگاه $F = f(F)f(F) \cup \{0\}$.

اثبات. اثبات این‌که $f(F)f(F) \cup \{0\} \subset F$ کاملاً مشابه اثبات ۹.۴.۵ است. بنابراین از تکرار آن می‌پرهیزیم. کافی است نشان دهیم $F \subseteq f(F)f(F) \cup \{0\}$. بدین منظور عنصر دلخواه $0 \neq c \in F$ را در نظر می‌گیریم (واضح است که اگر $c = 0$ آنگاه $c \in f(F)f(F) \cup \{0\}$). بنا به قضیه‌ی ۷.۴.۵ چندجمله‌ای $f(X)f(Y) - c \in F[X,Y]$ مطلقاً تحویل‌ناپذیر است. بنابراین از این‌که میدان F شبه‌بسته‌ی جبری است نتیجه می‌شود عناصر $x, y \in F$ وجود دارند به طوری که $f(x)f(y) - c = 0$ یا به طور معادل $c = f(x)f(y)$. از طرفی $f(x)f(y) \in f(F)f(F) \cup \{0\}$، پس داریم $c \in f(F)f(F) \cup \{0\}$. در نتیجه $F \subseteq f(F)f(F) \cup \{0\}$. یعنی اگر F شبه‌بسته‌ی جبری باشد $F = f(F)f(F) \cup \{0\}$.

□

چندجمله‌ای $f \in \mathcal{O}[X]$ را در نظر بگیرید و فرض کنید برای هر $x \in K$ داریم $f(x) \neq 0$. در این بخش T_f را همان مجموعه‌ی $T_f = f(K)^{-1}f(K)^{-1} \cup \{0\}$ که در بخش قبلی تعریف کردیم در نظر می‌گیریم.

نتیجه ۲.۵.۵. چندجمله‌ای تکین $f \in \mathcal{O}[X]$ را در نظر بگیرید و فرض کنید که $\bar{f}$ خالی از مربع باشد و در F ریشه نداشته باشد، در این صورت $T_f \subseteq \mathcal{O}$. اگر علاوه بر این فرض‌ها F شبه‌بسته‌ی جبری باشد، آنگاه $\bar{T}_f = F$.

اثبات. اثبات کاملا مشابه اثبات لم ۱۱.۴.۵ است با این تفاوت که در این اثبات چون F شبه‌بسته‌ی جبری است به جای لم ۹.۴.۵ از لم ۱.۵.۵ کمک می‌گیریم.

□

تا این جا دیدیم که T_f ویژگی‌های ذکر شده در لم ۲.۲.۵ را داراست. همچنین در لم ۱۲.۴.۵ دیدیم که T_f تعریف‌پذیر است. در ادامه قصد داریم تعریف‌پذیری حلقه‌ی ارزیاب $\mathcal{O}$ را برای حالتی که میدان باقیمانده‌ها شبه‌بسته‌ی جبری است بررسی کنیم.

۲.۵.۵ وجود چندجمله‌ای مناسب f

در این زیربخش نشان می‌دهیم برای حالتی که میدان باقیمانده‌ها شبه‌بسته‌ی جبری است چندجمله‌ی تکین $f \in \mathcal{O}[X]$ موجود است به طوری که $\bar{f}$ در F ریشه ندارد و عنصر $a \in \mathcal{O}$ موجود است به طوری که $f'(a) \notin \mathfrak{m}$.

لم ۳.۵.۵. میدان دلخواه K را در نظر بگیرید. اگر $f(X) \in K[X]$ یک چندجمله‌ای جدایی‌پذیر باشد آنگاه $f' \not\equiv 0$.

اثبات. فرض کنید چندجمله‌ای f جدایی‌پذیر باشد. در این صورت f در بستار جبری K به عوامل درجه‌ی یک تجزیه می‌شود. بنابراین بدون کاستن از کلیت داریم $f(x) = (x - a_1)(x + a_2)\dots(x - a_n)$ و در نتیجه $f' = (x + a_2)\dots(x - a_n) + (x - a_1)(x - a_3)\dots(x - n) + (x - a_1)\dots(x + a_{n-1})$. به برهان خلف فرض کنید $f' = 0$. دو حالت زیر ممکن است رخ دهد:

۱. همه‌ی عوامل f' مساوی صفر هستند: در این حالت تک تک جملات با هم برابرند یعنی

$$\begin{cases} (x + a_2)(x - a_3)\cdots(x - a_n) = (x - a_1)(x - a_3)\cdots(x - a_n) \\ (x - a_1)(x - a_3)\cdots(x - a_n) = (x - a_1)(x + a_2)(x + a_4)\cdots(x - a_n) \\ \cdots \\ (x - a_1)\cdots(x - a_{n-2})(x - a_n) = (x - a_1)(x + a_2)\cdots(x + a_{n-1}) \end{cases}$$

بنابراین $(x - a_1) = (x + a_2) = (x - a_3) = \ldots = (x - a_n)$ و در نتیجه $f = (x - a_1)^n$.

۲. بعضی از عوامل علامت قرینه دارند و بعضی عوامل برابر با صفرند:

به منظور ارائه‌ی یک بررسی کلی بدون کاستن از کلیت فرض می‌کنیم حالت زیر رخ دهد:

$$\begin{cases} (x+a_۲)(x-a_۳)\cdots(x-a_n)=(x-a_۱)(x-a_۳)\cdots(x-a_n)=۰ \\ (x-a_۱)(x-a_۳)\cdots(x-a_n)=-(x-a_۱)(x+a_۲)(x+a_۴)\cdots(x-a_n) \\ \cdots \\ (x-a_۱)\ldots(x-a_{n-۲})(x-a_n)=-(x-a_۱)(x+a_۲)\ldots(x+a_{n-۱}) \end{cases}$$

بنابراین

$$\begin{cases} (x+a_۲)=(x-a_۱)\Rightarrow a_۲=-a_۱\Rightarrow (x+a_۲).(x-a_۱)=(x+a_۲)^۲ \\ (x-a_۳)=-(x+a_۲)\Rightarrow (x-a_۳)(x+a_۲)=-(x+a_۲)^۲ \\ \cdots \\ (x-a_n)=-(x+a_{n-۱})\Rightarrow (x+a_{n-۱})(x-a_n)=-(x+a_{n-۱})^۲ \end{cases}$$

پس در هر صورت تجزیه‌ی چندجمله‌ای f، شامل عوامل با درجات بیشتر از یک است که با جدایی‌پذیر بودن f در تناقض است.

□

لم ۴.۵.۵. اگر F نامتناهی باشد و F_{alg} بسته‌ی جبری نباشد، چندجمله‌ای تکین، تحویل‌ناپذیر و جدایی‌پذیر $f\in F_۰[X]$ و عنصر $a\in F$ وجود دارند به گونه‌ای که f در F ریشه ندارد و $f'(a)\neq ۰$.

اثبات. از این‌که F_{alg} بسته‌ی جبری نیست نتیجه می‌شود که چندجمله‌ای تکین و تحویل‌ناپذیر $f\in F_۰[X]$ وجود دارد که در F_{alg} ریشه ندارد. از طرفی F_{alg} به صورت اشتراک بستار جبری $F_۰$ با F است و هر چندجمله‌ای $f(x)\in F_۰[X]$ در بستار جبری $F_۰$ ریشه دارد. بنابراین از این‌که f در F_{alg} ریشه ندارد نتیجه می‌شود که f در F ریشه ندارد. بنا به نتیجه‌ی ۵.۵.۱ داریم که $F_۰$ یک میدان کامل است. بنابراین هر چندجمله‌ای تحویل‌ناپذیر در $F_۰$ جدایی‌پذیر است. از این رو چندجمله‌ای تحویل‌ناپذیرِ f جدایی‌پذیر نیز است، پس بنا به لم ۳.۵.۵ داریم $f'\neq ۰$؛ یعنی f' چندجمله‌ای ثابت صفر نیست. از طرفی هرچندجمله‌ای حداکثر متناهی تا ریشه دارد. از این رو f' در F حداکثر متناهی تا ریشه دارد و با توجه به این‌که F نامتناهی است؛ عنصر $a\in F$ موجود است به طوری که $f'(a)\neq ۰$. □

در قضیه‌ی بعدی اثبات می‌کنیم که فرمول وجودی $\eta_f(x) \equiv (\exists u,t)(x = u + t \wedge \varphi_f(u) \wedge \psi_f(t))$ که در آن φ_f و ψ_f به ترتیب فرمول‌های تعریف شده در لم ۲.۳.۵ و لم ۱۲.۴.۵ هستند؛ حلقه‌ی ارزیاب $\mathcal{O}$ را تعریف می‌کند.

قضیه ۵.۵.۵. فرض کنید چندجمله‌ای تکین $f \in \mathcal{O}[X]$ به گونه‌ای باشد که $\bar{f}$ خالی از مربع باشد و در F ریشه نداشته باشد. در این صورت $\eta_f(K) \subseteq \mathcal{O}$. به علاوه اگر عنصر $a \in \mathcal{O}$ وجود داشته باشد به طوری که $f'(a) \notin \mathfrak{m}$ و میدان F شبه‌بسته‌ی جبری باشد آنگاه $\eta_f(K) = \mathcal{O}$.

اثبات. مجموعه‌ی U_f را مجموعه عناصری از میدان K در نظر می‌گیریم که در فرمول

$$\varphi_f(x) \equiv (\exists y,z,y_1,z_1)(x = y_1 - z_1 \wedge y_1 f(y) = 1 \wedge z_1 f(z) = 1)$$

صدق می‌کنند و مجموعه‌ی T را مجموعه عناصری از میدان K در نظر می‌گیریم که در فرمول

$$\psi_f(x) \equiv (\exists y,z,y_1,z_1)(x = 0 \vee (x = y_1 z_1 \wedge y_1 f(y) = 1 \wedge z_1 f(z) = 1))$$

صدق می‌کنند. اثبات این‌که $\eta_f(K) \subseteq \mathcal{O}$ کاملاً مشابه اثبات قضیه‌ی ۱۳.۴.۵ است. بنابراین از تکرار مجدد آن خودداری می‌کنیم. فرض می‌کنیم $a \in \mathcal{O}$ به گونه‌ای باشد که $f'(a) \notin \mathfrak{m}$. نشان می‌دهیم $\eta_f(K) = \mathcal{O}$. از لم ۶.۳.۵ داریم $\mathfrak{m} \subseteq U_f$. از طرفی F شبه‌بسته‌ی جبری است. بنابراین از نتیجه‌ی ۲.۵.۵ داریم که $\bar{T_f} = F$. در نتیجه U_f و T_f در شرایط لم ۲.۲.۵ صدق می‌کنند. از این رو $\eta_f(K) = \mathcal{O}$. □

در پایان به اصلی‌ترین قضیه‌ی این بخش است می‌رسیم. در این قضیه اثبات می‌کنیم که اگر میدان باقیمانده‌ها شبه‌بسته‌ی جبری باشد حلقه‌ی ارزیاب $\mathcal{O}$ به صورت وجودی و بدون پارامتر تعریف‌پذیر است.

قضیه ۶.۵.۵. فرض کنید K یک میدان ارزیابی هنسلی باحلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های F است. اگر F شبه‌بسته‌ی جبری باشد و F_{alg} بسته‌ی جبری نباشد، یک تعریف وجودی بدون پارامتر برای حلقه‌ی $\mathcal{O}$ در میدان K وجود دارد.

اثبات. چندجمله‌ای $f \in F_0[X]$ مربوط به لم ۴.۵.۵ را در نظر می‌گیریم. این چندجمله‌ای در F ریشه ندارد، تکین، تحویل‌ناپذیر و جدایی‌پذیر است. از طرفی بنا به نتیجه‌ی ۵.۵.۱ میدان F_0 تام است. بنابراین f خالی از مربع نیز هست. همچنین عنصر $a \in F$ وجود دارد به گونه‌ای که $f'(a) \neq 0$. حال فرض می‌کنیم که $\tilde{f} \in \mathbb{Z}[X]$ یک بر کشیدن تکین از f و $\tilde{a} \in \mathcal{O}$ یک بر کشیدن از a باشد. بنابراین $\tilde{f}'(a) \notin \mathfrak{m}$. در نتیجه بنا به قضیه‌ی ۵.۵.۵ داریم $\eta_f(K) = \mathcal{O}$. به بیان دیگر $\mathcal{O}$ توسط فرمول وجودی و بدون پارامتر

$$\eta_{\tilde{f}} \equiv (\exists u,t)(x = u + t \wedge \varphi_{\tilde{f}} \wedge \psi_{\tilde{f}})$$

تعریف می‌گردد. □

۶.۵ تعریف یکنواخت

دیدیم که اگر K یک میدان ارزیابی هنسلی با حلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های $F = \mathbb{F}_q$ باشد. حلقه‌ی $\mathcal{O}$ توسط فرمول وجودی و بدون پارامتر $\eta_f \equiv (\exists u,t)(x = u + t \wedge \varphi_f \wedge \psi_f)$ به طوری که $\varphi_f(x) \equiv (\exists y,z,y_۱,z_۱)(x = y_۱ - z_۱ \wedge y_۱ f(y) = ۱ \wedge z_۱ f(z) = ۱)$ و $\psi_f(x) \equiv (x^q - x = ۰)$ در میدان K تعریف‌پذیر است. اما واضح است که این فرمول به q وابسته است و یکنواخت نیست. همچنین در نتیجه‌ی ۱۵.۴.۵ دیدیم که به طور خاص زمانی که $|F| > c(\deg(f))$ با در نظر گرفتن $\psi_f(x) \equiv (\exists y,z,y_۱,z_۱)(x = ۰ \vee (x = y_۱ z_۱ \wedge y_۱ f(y) = ۱ \wedge z_۱ f(z) = ۱))$. حلقه‌ی $\mathcal{O}$ توسط فرمول وجودی و بدون پارامتر η_f به صورت یکنواخت تعریف‌پذیر است؛ در این بخش یک تعریف مستقل از q برای تعریف حلقه‌ی ارزیاب $\mathcal{O}$ در میدان K ارائه می‌کنیم.

قضیه ۱.۶.۵. عدد اول p و عدد صحیح m را در نظر بگیرید. فرمول وجودی و بدون پارامتر φ موجود است به طوری که $\varphi(K) = \mathcal{O}$ برای هر میدان ارزیابی K با حلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌ی $F = \mathbb{F}_{p^n}$ که $m \nmid n$.

اثبات. فرض می‌کنیم $F = \mathbb{F}_{p^n}$ به طوری که $m \nmid n$. بنا به لم ۲.۴.۵ یک چندجمله‌ای تحویل‌ناپذیر f با درجه‌ی m متعلق به $\mathbb{F}_p$ موجود است. با توجه به این‌که $m \nmid n$ از لم ۳.۴.۵ داریم f در F ریشه ندارد و عنصر $a \in F$ موجود است به طوری که $f'(a) \neq ۰$. حال فرض می‌کنیم چندجمله‌ای $\tilde{f} \in \mathbb{Z}[X]$ و عنصر $\tilde{a} \in \mathcal{O}$ از برکشیدن f و $a \in F$ ایجاد شده باشند. بنا به قضیه‌ی ۱۳.۴.۵ به طور کلی داریم $\eta_{\tilde{f}}(K) \subseteq \mathcal{O}$ و اگر $p^n > (۲m-۱)^۴$ آنگاه $\eta_{\tilde{f}}(K) = \mathcal{O}$. حال برای هر عدد طبیعی k که $m \nmid k$ قرار می‌دهیم:

$$\psi_k(x) \equiv x^{p^k} - x = ۰$$

و

$$\eta_k \equiv (\exists u,t)(x = u + t \wedge \varphi_{\tilde{f}} \wedge \psi_k)$$

بنابراین طبق قضیه‌ی ۴.۴.۵ داریم $\eta_k(K) \subseteq \mathcal{O}$ و اگر $n = k$ آنگاه $\eta_k(K) = \mathcal{O}$.

مجموعه‌ی $M = \{k \in \mathbb{N} : m \nmid k, p^k \leq c(m)\}$ را در نظر می‌گیریم. فرمول وجودی و بدون پارامتر

$$\psi(x) \equiv \eta_{\tilde{f}}(x) \vee \bigvee_{k \in M} \eta_k(x).$$

حلقه‌ی ارزیاب هر میدان K با $F = \mathbb{F}_{p^n}$ به طوری که $m \nmid n$ را تعریف می‌کند و به q وابسته نیست. □

خلاصه‌ی فصل:

فرض کنید K یک میدان ارزیابی هنسلی باحلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های F باشد. در این فصل اثبات کردیم که اگر F متناهی یا شبه‌بسته‌ی جبری باشد آنگاه حلقه‌ی ارزیاب $\mathcal{O}$ در میدان ارزیابی K در زبان حلقه‌ها به صورت وجودی و بدون پارامتر تعریف‌پذیر است. برای اثبات این قضیه به صورت زیر عمل کردیم: در بخش اول این فصل اثبات کردیم که اگر دو زیرمجموعه‌ی U و T از حلقه‌ی ارزیاب $\mathcal{O}$ دارای این دو ویژگی باشند که $\mathfrak{m} \subseteq U$ و T همه‌ی کلاس‌های باقیمانده را قطع کند، آنگاه $\mathcal{O} = U + T$. سپس مجموعه‌ی U_f را به صورت $U_f = \{\frac{1}{f(x)} - \frac{1}{f(y)} | x, y \in K\}$، تعریف کردیم که در آن $f \in \mathcal{O}[X]$ و برای هر $x \in K$ داریم $f(x) \neq 0$. همچنین نشان دادیم که $\mathfrak{m} \subseteq U_f \subseteq \mathcal{O}$ هرگاه چندجمله‌ای $f \in \mathcal{O}[X]$ تکین باشد، $\bar{f}$ در F ریشه نداشته باشد و عنصر $a \in \mathcal{O}$ وجود داشته باشد به طوری که $f'(a) \notin \mathfrak{m}$.

در بخش دوم فرض کردیم میدان باقیمانده‌ها متناهی است و به کمک این فرض ابتدا وجود چندجمله‌ای f با ویژگی‌های بیان شده را اثبات کردیم. سپس یک زیرمجموعه‌ی T از حلقه‌ی ارزیاب $\mathcal{O}$ را به گونه‌ای معرفی کردیم که همه‌ی کلاس‌های باقیمانده را قطع کند. در واقع ابتدا نشان دادیم که اگر میدان باقیمانده‌ها F متناهی باشد، چندجمله‌ای $f \in F_0[X]$ موجود است به طوری که در F ریشه ندارد و تحویل‌ناپذیر، جدایی‌پذیر و تکین است. همچنین عنصر $a \in F$ به گونه‌ای وجود دارد که $f'(a) \neq 0$. سپس اثبات کردیم که اگر $F = \mathbb{F}_q$ مجموعه‌ی تعریف‌پذیر $T := \{x \in K : x^q - x = 0\}$ زیرمجموعه‌ای از حلقه‌ی ارزیاب $\mathcal{O}$ است و $\bar{T} = F$. در پایان این بخش دیدیم که برای حالتی که میدان باقیمانده‌ها متناهی است، حلقه‌ی ارزیاب $\mathcal{O}$ توسط یک فرمول وجودی و بدون پارامتر در میدان K تعریف می‌گردد و قضیه‌ی زیر به اثبات می‌رسد: فرض کنید K یک میدان ارزیابی هنسلی باحلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های F باشد. اگر F متناهی باشد، یک تعریف وجودی و بدون پارامتر برای حلقه‌ی $\mathcal{O}$ در میدان K وجود دارد.

در بخش سوم قضیه‌ی فوق را برای یک حالت خاص از میدان باقیماندهای متناهی اثبات کردیم. در واقع در این بخش چندجمله‌ای $f \in F_0[X]$ که وجود آن را در بخش قبل اثبات کردیم را در نظر گرفتیم و نشان دادیم که اگر $|F| > (2(\deg(f)) - 1)^4$ زیرمجموعه‌ی $T_f := f(K)^{-1} f(K)^{-1} \cup \{0\}$ از همه‌ی کلاس‌های باقیمانده را قطع می‌کند.

در بخش چهارم ابتدا به طور کلی نشان دادیم که اگر F یک میدان نامتناهی باشد و F_{alg} بسته‌ی جبری نباشد. چندجمله‌ای تکین، تحویل‌ناپذیر و جدایی‌پذیر $f \in F_0[X]$ و عنصر $a \in F$ وجود دارند به گونه‌ای که f در F ریشه ندارد و $f'(a) \neq 0$. سپس از این‌که میدان‌های شبه‌بسته‌ی جبری نامتناهی هستند نتیجه گرفتیم که اگر F یک میدان شبه‌بسته‌ی جبری باشد و F_{alg} بسته‌ی جبری نباشد، یک چندجمله‌ای f با ویژگی‌های فوق موجود است. در نهایت نشان دادیم که مجموعه‌ی $T_f = f(K)^{-1} f(K)^{-1} \cup \{0\}$ زیرمجموعه‌ای از حلقه‌ی ارزیاب $\mathcal{O}$ است و $\bar{T}_f = F$ هرگاه چندجمله‌ای $f \in \mathcal{O}[X]$ تکین و $\bar{f}$ خالی از مربع باشد و در F ریشه نداشته

باشد. در پایان این بخش دیدیم که برای حالتی که میدان باقیمانده‌ها شبه‌بسته‌ی جبری است، حلقه‌ی ارزیاب $\mathcal{O}$ توسط یک فرمول وجودی و بدون پارامتر در میدان K تعریف می‌گردد و قضیه‌ی زیر به اثبات می‌رسد:

فرض کنید K یک میدان ارزیابی هنسلی با حلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های F باشد. اگر F شبه‌بسته‌ی جبری باشد، یک تعریف وجودی و بدون پارامتر برای حلقه‌ی $\mathcal{O}$ در میدان K وجود دارد.

در آخرین بخش این فصل نشان دادیم که برای حالتی که میدان باقیمانده‌ها متناهی است، حلقه‌ی ارزیاب $\mathcal{O}$ در میدان K به صورت یکنواخت تعریف می‌گردد. در واقع در این بخش قضیه‌ی زیر را اثبات کردیم:

برای هر عدد اول p و عدد صحیح m یک فرمول وجودی و بدون پارامتر φ موجود است به طوری که در هر میدان ارزیابی K با حلقه‌ی ارزیاب $\mathcal{O}$ و میدان باقیمانده‌های $F = \mathbb{F}_{p^n}$ اگر $m \nmid n$ آنگاه $\varphi(K) = \mathcal{O}$.

مقالات برای مطالعه‌ی بیشتر

مطالعه‌ی تعریف پذیری حلقه‌های ارزیاب در میدان های ارزیابی با مطالعات جولیا رابینسون در این زمینه [۲۰] آغاز شده است و سابقه‌ی دیرینه‌ای دارد. در سال‌های اخیر بررسی این مسئله توجه زیادی را به خود جلب کرده و مقالات زیادی در این زمینه نوشته شده است. در این جا به طور خلاصه قضایای اصلی برخی از این مقالات را ذکر کرده‌ایم. بدیهی است که در این پایان‌نامه امکان تعریف همه‌ی مفاهیم مورد نیاز این فهرست را نداشته‌ایم. در مقاله‌ی [۲۰] تعریف پذیری حلقه‌ی $\mathbb{Z}_p$ در $\mathbb{Q}_p$ اثبات شده است:

قضیه ۱. حلقه‌ی ارزیاب $\mathbb{Z}_p$ روی $\mathbb{Q}_p$ با فرمول $\exists y(y^۲ = ۱ + kx^۲)$ تعریف‌پذیر است، که در آن اگر $p = ۲$ آنگاه $k = p$ و در غیر این صورت $k = ۸$.

به طور مشابه در مقاله‌ی [۲] اثبات شده است که $F[[t]]$ در $F((t))$ تعریف‌پذیر است:

قضیه ۲. برای هر میدان F حلقه‌ی ارزیاب $F[[t]]$ در $F((t))$ با فرمول

$$\exists w, y \forall u, x_۱, x_۲ \exists z \forall y_۱, y_۲((z^m = ۱ + wx_۱^m x_۲^m \vee y_۱^m \neq ۱ + wx_۱^m \vee y_۲^m \neq ۱ + wx_۲^m) \\ \wedge u^m \neq w \wedge y^m = ۱ + wx^m)$$

تعریف‌پذیر است، که در آن $m > ۱$ و $\mathrm{char}(F) \nmid m$.

قضیه‌ی زیر در مقاله‌ی [۱۵] اثبات شده است:

قضیه ۳. فرض کنید (K, v) یک میدان ارزیابی هنسلی باشد. اگر گروه ارزیاب آن ارشمیدسی باشد و بخش‌پذیر نباشد آنگاه حلقه‌ی ارزیاب $\mathcal{O}$ در میدان K در زبان حلقه‌ها و بدون پارامتر تعریف‌پذیر است.

در مقاله‌ی [۱۱] اثبات شده است که:

قضیه ۴. فرض کنید (K, v) یک میدان ارزیابی هنسلی باشد. اگر گروه ارزیاب آن منتظم باشد و بخش‌پذیر نباشد آنگاه حلقه‌ی ارزیاب $\mathcal{O}$ در میدان K در زبان حلقه‌ها و بدون پارامتر تعریف‌پذیر است.

همان طور که دیدیم در مقالات فوق با در نظر گرفتن ویژگی‌هایی روی گروه ارزیاب، تعریف‌پذیری حلقه‌ی ارزیاب هنسلی اثبات شده است. در مقاله‌ی [۱۳] شرایطی را برای میدان باقیمانده‌ها در نظر گرفته است:

قضیه ۵. فرض کنید (K, v) یک میدان ارزیابی هنسلی باشد. در این صورت حلقه‌ی ارزیاب $\mathcal{O}$ در میدان ارزیابی K بدون پارامتر تعریف‌پذیر است هرگاه میدان باقیمانده‌ها در یکی از شرایط زیر صدق کند:

۱. برای عدد اول $p > ۲$ میدان باقیمانده‌ها نه p ـهنسلی و نه p ـبسته باشد.

۲. میدان باقیمانده‌ها هیلبرتی باشد.

۳. میدان باقیمانده‌ها شبه‌بسته‌ی جبری باشد و بسته‌ی جدایی‌پذیر نباشد.

در مقاله‌ی [۲۲] اثبات شده است که یک میدان ارزیابی وجود دارد به طوری که حلقه‌ی ارزیاب آن را نمی‌توان با یک فرمول بدون پارامتر تعریف کرد:

قضیه ۶. یک میدان ارزیابی هنسلی K با مشخصه‌ی صفر وجود دارد که نه بسته‌ی جبری است و نه بسته‌ی حقیقی است. و هیچ تعریف بدون پارامتری وجود ندارد که حلقه‌ی ارزیاب را در میدان K تعریف کند.

در مقاله‌ی [۱] یک مثال از تعریف‌پذیری وجودی حلقه‌ی ارزیاب در میدان ارزیابی بیان شده است:

قضیه ۷. حلقه‌ی ارزیاب $F_q[[t]]$ در $F_q((t))$ با یک فرمول وجودی و بدون پارامتر تعریف‌پذیر است

در ادامه قضایای اصلی چند نمونه از مقالاتی که به تعریف‌پذیری حلقه‌ی ارزیاب با پیچیدگی سوری $\exists\forall - \emptyset$ پرداخته‌اند را آورده‌ایم. در مقاله‌ی [۸] ثابت شده است که:

قضیه ۸. فرض کنید (K, v) یک میدان ارزیابی هنسلی باشد. اگر میدان باقیمانده‌ها منتظم و غیربخش‌پذیر باشد، حلقه‌ی ارزیاب $\mathcal{O}$ در میدان K با یک فرمول $\exists\forall$ و بدون پارامتر تعریف می‌گردد.

مقالات زیر یک تعریف یکنواخت برای حلقه‌ی ارزیاب ارائه کرده‌اند. در مقاله‌ی [۱۹] اثبات شده است که:

قضیه ۹. یک فرمول $\exists\forall$ و بدون پارامتر موجود است که حلقه‌ی ارزیاب $\mathcal{O}$ را در هر میدان ارزیابی (K, v) با میدان باقیمانده‌های متناهی یا شبه‌متناهی تعریف می‌کند.

در مقاله‌ی [۴] اثبات شده است که:

قضیه ۱۰. یک فرمول $\exists\forall$ بدون پارامتر وجود دارد که حلقه‌ی ارزیاب $\mathcal{O}$ را در میدان‌های ارزیابی که میدان باقیمانده‌هایشان متناهی یا شبه‌متناهی یا هیلبرتی است به صورت یکنواخت تعریف می‌کند.

واژه‌نامه‌ی فارسی به انگلیسی

الف

ایده‌آل ماکسیمال ..... Maximal ideal
ارزیابی ..... Valuation
ایده‌آل اول ..... Prime ideal
ایده‌آل اولیه ..... Primary ideal

ب

بستار جبری ..... Algebraic closure
بسته‌ی وجودی ..... Existentially closed
بدون تاب ..... Torsion-free
برکشیدن ..... Lift
بخش‌پذیر ..... Divisible

پ

پوچ‌ساز ..... Annihilator
پایه‌ی نرمال ..... Normal basis

ت

تحویل‌ناپذیر ..... Irreducible
توسیع جبری ..... Algebraic extension
توسیع میدانی ..... Field extension
توسیع منتظم ..... Regular extension
توسیع جدایی‌پذیر ..... Separable extension

توسیع نرمال ..... Normal extension

توسیع گالوایی ..... Galois extension

تکین ..... Monic

توسیع مقدماتی ..... Elementary extension

ج

جدایی‌ناپذیر ..... Inseparable

چ

چندجمله‌ای همگن ..... Homogeneous polynomial

چندجمله‌ای خالی از مربع ..... Square-free polynomial

ح

حلقه‌ی موضعی ..... Local ring

حلقه‌ی هنسلی ..... Henselian ring

د

درجه تعالی ..... Transcendence degree

ع

عنصر متعالی ..... Transcendental element

ف

فضای آفین ..... Affine space

فرمول وجودی ..... Existential formula

ک

کاملاً جدایی‌ناپذیر ..... Purely inseparable

گ

گروه مرتب آبلی ..... Ordered abelian group

گروه ارزیاب ..... Value group

م

مجموعه‌ی جبری ..... Algebraic Set
مطلقاً تحویل‌ناپذیر ..... Absolutely irreducible
مستقل جبری ..... Algebraically independent
مجزای خطی ..... linearly disjoint
میدان تام ..... Perfect field
میدان شبه‌بسته‌ی جبری ..... Pseudo algebraically closed field
میدان متناهی ..... Finite field
میدان شکافنده ..... Splitting field
میدان ارزیابی ..... Valued field
میدان باقیمانده‌ها ..... Residue field

و

ویژه‌سازی ..... Specialization
واریته ..... Variety

ه

هسته ..... Kernel

نمایه

منابع

[1] Anscombe, Will and Koenigsmann, Jochen. "an existential -definition of". *The Journal of Symbolic Logic*, 79(4):1336–1343, 2014.

[2] Ax, James. On the undecidability of power series fields. In *Proc. Amer. Math. Soc*, volume 16, pages 4–4, 1965.

[3] Campillo, Antonio, Kuhlmann, Franz-Viktor, and Teissier, Bernard. *Valuation theory in interaction.*

[4] Cluckers, Raf, Derakhshan, Jamshid, Leenknegt, Eva, and Macintyre, Angus. "uniformly defining valuation rings in henselian valued fields with finite or pseudo-finite residue fields". *Annals of Pure and Applied Logic*, 164(12):1236–1246, 2013.

[5] Conrad, Keith. "linear independence of characters". *Online Notes*, 2008.

[6] Engler, Antonio J and Prestel, Alexander. *Valued fields.* Springer Science & Business Media, 2005.

[7] Fehm, Arno. "existential -definability of henselian valuation rings". *The Journal of Symbolic Logic*, 80(1):301–307, 2015.

[8] Fehm, Arno and Prestel, Alexander. "uniform definability of henselian valuation rings in the macintyre language". *Bulletin of the London Mathematical Society*, 47(4):693–703, 2015.

[9] Fried, Michael D, Jarden, Moshe, et al. *Field arithmetic*, volume 11. Springer, 2005.

[10] Heinemann, Bernhard and Prestel, Alexander. Fields regularly closed with respect to finitely many valuations and orderings. In *Canadian Mathematical Society Conference Proceedings*, volume 4, pages 297–336, 1984.

[11] Hong, Jizhan. "definable non-divisible henselian valuations". *Bulletin of the London Mathematical Society*, 46(1):14–18, 2014.

[12] Howie, John Mackintosh and Howie, John M. *Fields and Galois theory*. Springer, 2006.

[13] Jahnke, Franziska and Koenigsmann, Jochen. "definable henselian valuations". *The Journal of Symbolic Logic*, 80(1):85–99, 2015.

[14] Kim, Sungjin. Nomal basis theorem. https://www.csun.edu/ sungjin/NBT.pdf.

[15] Koenigsmanny, Jochen. *Elementary characterization of fields by their absolute Galois group*. PhD thesis, Citeseer, 1998.

[16] Lang, Serge. *Algebra*, volume 211. Springer Science & Business Media, 2012.

[17] Lang, Serge. *Introduction to algebraic geometry*. Courier Dover Publications, 2019.

[18] Marker, David. *Model theory: an introduction*, volume 217. Springer Science & Business Media, 2006.

[19] Prestel, Alexander. "definable henselian valuation rings". *The Journal of Symbolic Logic*, 80(4):1260–1267, 2015.

[20] Robinson, Julia. The decision problem for fields. In *The Theory of Models*, pages 299–311. Elsevier, 2014.

[21] Tent, Katrin and Ziegler, Martin. *A course in model theory*. number 40. Cambridge University Press, 2012.

[22] Ziegler, Martin and Prestel, Alexander. "model theoretic methods in the theory of topological fields". 1978.

Existential $\emptyset$-definability of henselian valuation rings

Shaghayegh Shirani
shaghayegh_shirani@math.iut.ac.ir
January, 2024
Master of Science Thesis (in Farsi)
Departement of Mathematical Sciences
Isfahan University of Technology, Isfahan 84156-8311, Iran

Supervisor: Dr. Mohsen Khani, `mohsen.khani@iut.ac.ir`
Supervisor: Dr. Hamed Lorvand, `lorvandhamed@iut.ac.ir`
2000 MSC: 03C60
Keywords: Definablity, henselian valued fields, Pseudo-algebraically closed fields, finite fields

---

Abstract:
This M.Sc. thesis is based on the following paper:

- Fehm, Arno. *Existential-definability of henselian valuation rings.* The Journal of Symbolic Logic, 80(1):301–307, 2015.

Suppose that $\mathfrak{M}$ is a first-order structure with domain M, A is a given subset of M, and n is a natural number. A set $X \subseteq M^n$ is called definable in $\mathfrak{M}$ with parameters from A if there exists a formula $\varphi(x_1, ..., x_n, y_1, ..., y_m)$ and elements $b_1, \ldots, b_n \in A$ such that $X = \{(a_1, ..., a_n) \in M^n \mid \mathfrak{M} \models \varphi(a_1, ..., a_n, b_1, ..., b_m)\}$. Identifying definable sets, and the complexity of their definition, in a particular first order structure is of crucial importance in model theory. This thesis concerns the definability of valuation ring in a henselian valued field, where the residue field is finite or pseudo-algebraically closed.
A field K is *pseudo-algebraically closed* if for every absolutely irreducible polynomial $f \in K[X, Y]$ there is a point $(a, b) \in K^2$ with $f(a, b) = 0$.
Assume that K is a field and Γ is an ordered abelian group. A *valuation map* $v : K \to \Gamma \cup \{\infty\}$ is a map that satisfies the following properties for all x, y in K:

1. $v(x + y) \geq \min\{v(x), v(y)\}$
2. $v(x \cdot y) = v(x) + v(y)$
3. $x = 0 \Leftrightarrow v(x) = \infty$.

The set $\mathcal{O} = \{x \in K : v(x) \geq 0\}$ is a called a *valuation ring* of K, and the pair $(K, \mathcal{O})$ is called a *valued field*. The ring $\mathcal{O}$ is local, that is it has a unique maximal ideal $\mathfrak{m} = \{x \in K : v(x) > 0\}$.

The field $F = \frac{\mathcal{O}}{\mathfrak{m}}$ is referred to as the *residue field*. The canonical image of an element $a \in \mathcal{O}$ in F is denoted by $\bar{a}$.
A valued field $(K, \mathcal{O})$ is called *henselian* if for each $f \in \mathcal{O}[X]$ and $a \in \mathcal{O}$ with $\bar{f}(\bar{a}) = 0$ and $\bar{f}'(\bar{\alpha}) \neq 0$ in the residue field, there exists some $b \in \mathcal{O}$ such that $f(b) = 0$ and $\bar{b} = \bar{a}$.
The main theorem of the thesis is the following:

> Let K be a henselian valued field with valuation ring $\mathcal{O}$ and residue field F. If F is finite or pseudo-algebraically closed and the algebraic part of F is not algebraically closed, then there exists an existential definition of $\mathcal{O}$ in K, with no parameters.

To establish this theorem, we first verify that:

1. If $U, T \subseteq \mathcal{O}$ are such that $\mathfrak{m} \subseteq U$ and T meets all residue classes (i.e. $\bar{T} = F$), then $\mathcal{O} = U + T$.

2. If $f \in \mathcal{O}[X]$ is a monic polynomial such that $\bar{f}$ has no zero in F, and $a \in \mathcal{O}$ is such that $f'(a) \notin \mathfrak{m}$, then $U := f(K)^{-1} - f(K)^{-1}$ satisfies $\mathfrak{m} \subseteq U \subseteq \mathcal{O}$.

We deduce the existence of the polynomial f in different ways for cases of finite and pseudo-algebraically closed residue field. Finally, we show that when F is finite (pseudo-algebraically closed) the definable subset $T = \{x \in K : x^q - x = 0\}$ ($T_f = f(K)^{-1} f(K)^{-1} \cup \{0\}$) of $\mathcal{O}$ meets all residue classes.

Isfahan University of Technology

Department of Mathematical Sciences

Existential -Definability of henselian valuation rings

A Thesis

Submitted in Partial Fulfillment of the Requirements

for the Master of Science (M. Sc.)

By

Shaghayegh Shirani

Evaluated and approved by the thesis committee, on 2024/1/24

1- Dr. Mohsen Khani, Assistant Professor (Supervisor)

2- Dr. Hamed Lorvand, Assistant Professor (Supervisor)

3- Dr. Mostafa Einollahzadeh, Assistant Professor Professor (Examiner)

4- Dr. Masoud Pourmahdian, Associate Professor (Examiner) on behalf

Dr. Bijan Taeri, Professor (Department graduate coordinator)

Isfahan University of Technology

Department of Mathematical Sciences

Thesis Submitted for the Award of Master of Science (M. Sc.) in Mathematics

Existential -definability of henselian valuation rings

Shaghayegh Shirani

Supervisor: Dr. Mohsen Khani

Supervisor: Dr. Hamed Lorvand

January 2024