بسم اللّه الرحمن الرحيم

دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

یک تعریف وجودی بدون پارامتر برای حلقه‌ی ارزیابِ $\mathbb{F}_q[[t]]$ در میدان ارزیابیِ $\mathbb{F}_q((t))$

پایان‌نامه کارشناسی ارشد ریاضی محض

زهرا یادگاری

استاد راهنما

دکتر محسن خانی

۱۴۰۲

تقدیم به:

مادر و پدرم

فهرست مطالب

فهرست مطالب **پنج**

۱ مقدماتی از منطق و جبر **۱**

۱.۱ مفاهیم مقدماتی از منطق ۱

۱.۱.۱ معرفی یک زبان مرتبه اول، ترم‌ها و فرمول‌ها ۱

۲.۱.۱ معرفی یک $\mathcal{L}$ ساختار و تعبیر ترم‌ها و فرمول‌ها ۲

۳.۱.۱ تعریف‌پذیری ۵

۲.۱ مقدمات جبری ۶

۱.۲.۱ توسیع جبری ۶

۲.۲.۱ میدان‌های متناهی ۱۲

۳.۲.۱ میدان‌های کامل ۱۵

۲ حلقه‌های موضعی، نُرم‌دار و هنسلی **۱۹**

۱.۲ حلقه‌های موضعی ۲۰

۱.۱.۲ حلقه‌های موضعی هنسلی ۲۱

۲.۲ حلقه‌های نُرم‌دار ۲۴

۱.۲.۲ لم هنسل ۲۵

۲.۲.۲ حلقه‌ی متشکل از سری‌های توانی ۲۷

۳.۲ اعداد p ـ ادیک ۳۰

۱.۳.۲ قدرمطلق p ـ ادیک ۳۰

۲.۳.۲ ساختن $\hat{\mathbb{Q}}_p$ ۳۲

۳.۳.۲ ساختن $\hat{\mathbb{Z}}_p$ ۳۲

۴.۳.۲ تعریف‌پذیری $\hat{\mathbb{Z}}_p$ در $\hat{\mathbb{Q}}_p$ ۳۶
۵.۳.۲ یک روش جبری برای معرفی $\hat{\mathbb{Z}}_p$ ۳۶

۳ میدان ارزیابی **۴۰**
۱.۳ نگاشت ارزیابی ۴۰
۲.۳ حلقه‌ی ارزیاب ۴۲
۳.۳ سری‌های هان ۴۵
۱.۳.۳ یک نگاشت ارزیابی روی $k((t^\Gamma))$ ۴۶
۲.۳.۳ اثبات میدان بودن سری‌های هان ۴۷

۴ Vـ توپولوژی **۵۰**
۱.۴ میدان‌های توپولوژیک و Vـ توپولوژی ۵۱
۱.۱.۴ توپولوژی میدانی القاء شده توسط یک نگاشت ارزیابی ۵۴
۲.۱.۴ توپولوژی میدانی القاء شده توسط یک قدرمطلق ۵۷
۲.۴ دسته بندی Vـ توپولوژی ۵۸
۱.۲.۴ رتبه‌ی گروه‌های آبلی مرتب ۵۹
۲.۲.۴ مجموعه‌های کراندار ۶۲
۳.۲.۴ مجموعه‌ی تقریباً ارزیاب ۶۶
۴.۲.۴ عناصر پوچ‌توان و خنثی ۶۸
۵.۲.۴ یک Vـ توپولوژی بدون عنصر پوچ‌توان ۷۱
۶.۲.۴ یک Vـ توپولوژی با حداقل یک عنصر پوچ‌توان ۷۴

۵ میدانِ t ـ هنسلی **۸۰**
۱.۵ معرفی فرمول‌های موضعی ۸۱
۲.۵ میدان‌های ω ـ کامل ۸۲
۱.۲.۵ فیلترها ۸۳
۲.۲.۵ معادل بودن موضعی با یک میدان ω ـ کامل ۸۴
۳.۵ یک پایه‌ی متشکل از ایده‌آل‌های ارزیاب در یک Vـ توپولوژی ۸۶
۴.۵ معرفی میدان‌های t ـ هنسلی ۸۹

۵.۵ تعریف یک توپولوژی روی $K[x]_1^n$ ۹۱
۶.۵ یک همسایگی تعریف‌پذیر در یک میدانِ t ـ هنسلی ۹۲

۶ یک تعریف وجودی بدون پارامتر برای حلقه‌ی ارزیابِ $\mathbb{F}_q[[t]]$ در میدان ارزیابیِ $\mathbb{F}_q((t))$ **۹۷**
۱.۶ قضیه‌ی اصلی پایان‌نامه ۹۸
۲.۶ گوی‌های باز و بسته در توپولوژی τ_v ۹۸
۳.۶ یک همسایگی تعریف‌پذیر از صفر ۹۹
۴.۶ یک مجموعه‌ی تعریف‌پذیر بین O_v و m_v ۱۰۲
۵.۶ یک $\exists$ ـ $\mathbb{F}_q$ تعریف از $\mathbb{F}_q[[t]]$ در $\mathbb{F}_q((t))$ ۱۰۵
۶.۶ حذف پارامترها ۱۰۷
۷.۶ فرمول تعریفِ $\mathbb{F}_p[[t]]$ در $\mathbb{F}_p((t))$ ۱۱۰

۷ دو نتیجه‌ی مرتبط **۱۱۳**
۱.۷ گروه ارزیاب گسسته [۱۰] ۱۱۴
۲.۷ اثبات کلی‌تر برای قضیه‌ی مقاله‌ی اصلی [۷] ۱۱۶
۱.۲.۷ معرفی دو زیرمجموعه‌ی U و T از O_v ۱۱۷
۲.۲.۷ یافتن f برای تشکیل مجموعه‌ی U_f ۱۲۰
۳.۲.۷ یافتن مجموعه‌ی T ۱۲۱
۴.۲.۷ یک $\exists$ ـ $\emptyset$ ـ تعریف از O_v در میدانِ K ۱۲۱
۳.۷ مقایسه‌ی اثبات مقاله‌ی اصلی و مقاله‌ی [۷] ۱۲۲

واژه‌نامه فارسی به انگلیسی **۱۲۵**

نمایه

منابع

چکیده:

هدف اصلی این پایان‌نامه اثبات قضیه‌ی زیر از مقاله‌ی [۱] است:

"حلقه‌ی ارزیابِ $\mathbb{F}_q[[t]]$ در میدان ارزیابی $\mathbb{F}_q((t))$ با یک فرمول وجودی و بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است."

منظور از $\mathbb{F}_q((t))$ میدانِ $\{\sum\limits_{i=-n}^{\infty} a_i t^i : a_i \in \mathbb{F}_q, n \in \mathbb{N}\}$ و منظور از $\mathbb{F}_q[[t]]$ حلقه‌ی $\{\sum\limits_{i=0}^{\infty} a_i t^i : a_i \in \mathbb{F}_q\}$ است.
اثبات قضیه‌ی یادشده به نحو سنگینی متکی بر قضیه‌ای در [۲۲] است که بیان می‌کند که در میدان‌های توپولوژیک هنسلی که بسته‌ی جدایی‌پذیر نیستند یک همسایگی کراندار و تعریف‌پذیر از صفر وجود دارد. نشان خواهیم داد که میدانِ $\mathbb{F}_q((t))$ در شروط این قضیه صدق می‌کند و از این رو در آن یک همسایگی کراندار از صفر وجود دارد که با یک فرمول وجودی و با پارامتر از $\mathbb{F}_q$ تعریف می‌شود. در قدم بعدی این همسایگی را با ترفندی جالب به یک مجموعه‌ی تعریف‌پذیرِ Y تبدیل می‌کنیم که شامل $t\mathbb{F}_q[[t]]$ و مشمول در $\mathbb{F}_q[[t]]$ است. سپس با توجه به تساوی $\mathbb{F}_q[[t]] = \mathbb{F}_q + Y$ و تعریف‌پذیری مجموعه‌ی Y و تعریف‌پذیری $\mathbb{F}_q$ (به عنوان ریشه‌های چندجمله‌ای $x^q - x$) نتیجه می‌گیریم که $\mathbb{F}_q[[t]]$ با یک فرمول وجودی ولی با پارامتر از $\mathbb{F}_q$ تعریف‌پذیر است. در نهایت به حذف این پارامترها می‌پردازیم.

در طی این پایان‌نامه، بخش‌هایی از دو مقاله‌ی زیر به طور کامل تشریح شده‌اند:

1) Will Anscombe and Jochen Koenigsmann. An existential $\emptyset$-definition of $\mathbb{F}_q[[t]]$ in $\mathbb{F}_q((t))$, The Journal of Symbolic Logic, 79(4):1336–1343, 2014.

2) Alexander Prestel and Martin Ziegler. Model-theoretic methods in the theory of topological fields, Journal für die Reine und Angewandte Mathematik, vol. 299 (1978), no. 300, pp. 318–341.

رده بندی موضوعی: 03 C 60

واژگان کلیدی: تعریف‌پذیری حلقه‌ی ارزیاب، میدان ارزیابی هنسلی، Vـ توپولوژی، t ـ هنسلی.

پیشگفتار

یکی از موضوعات مهم در مطالعه‌ی یک ساختار در نظریه‌ی مدل‌ها، بررسی مجموعه‌های تعریف‌پذیر در آن است. زیرمجموعه‌ی X از یک $\mathcal{L}$ ساختارِ $\mathcal{M}$ تعریف‌پذیر خوانده می‌شود هرگاه یک $\mathcal{L}$ فرمولِ $\varphi(x)$ موجود باشد به طوری که $X = \{a \in M : \mathcal{M} \vDash \varphi(a)\}$.

در مطالعه‌ی ساختارهای معروف جبری، تشخیص مجموعه‌های تعریف‌پذیر، در گرو شناخت بسیاری از ویژگی‌های جبری ساختار است. مثلاً مجموعه‌های تعریف‌پذیر در میدان‌های بسته‌ی جبری، همان چندگونای [1] جبری هستند که شناسایی آن‌ها شالوده‌ی هندسه‌ی جبری است (برای مطالعه‌ی بیشتر در این زمینه می‌توانید به کتاب‌های [۲۰] و [۱۶] مراجعه کنید). همچنین مجموعه‌های تعریف‌پذیر در میدان‌های بسته‌ی حقیقی، مجموعه‌های شبه‌جبری هستند که مطالعه‌ی آن‌ها اساس هندسه‌ی جبری حقیقی است (برای مطالعه‌ی بیشتر به کتاب [۵] رجوع کنید).

یکی از ساختارهای با اهمیت جبری، *میدان‌های ارزیابی* هستند. فرض کنید K یک میدان و A یک زیرحلقه از آن باشد. می‌گوییم A یک حلقه‌ی ارزیاب است هرگاه به ازای هر $x \in K$ یا $x \in A$ یا $x^{-1} \in A$. هر حلقه‌ی ارزیاب در یک میدان، از یک *نگاشت ارزیابی* روی آن ناشی می‌شود. در واقع اگر K یک میدان شامل حلقه‌ی ارزیاب A باشد، آنگاه یک نگاشتِ v از K به یک گروه مرتب آبلیِ $(\Gamma, +, \leq)$ (با برخی ویژگی‌های مطلوب) موجود است به طوری که مجموعه‌ی A برابر است با $O_v := \{x \in K : 0 \leq v(x)\}$. منظور از یک میدان ارزیابی، یک دوتایی (K, O_v) است که در آن K یک میدان و $O_v \subseteq K$ یک حلقه‌ی ارزیاب است که از یک نگاشت ارزیابیِ $v : K \to \Gamma$ ناشی شده است. در فصل ۳ نشان خواهیم داد که O_v یک حلقه‌ی موضعی است؛ یعنی تنها یک ایده‌آل ماکسیمال دارد که آن را با نمادِ m_v نشان می‌دهیم. از این رو $k_v := \frac{O_v}{m_v}$ یک میدان است که آن را میدان پیمانه‌ها می‌نامیم.

یک مثال مهم از میدان‌های ارزیابی، p ـ ادیک‌ها هستند. به طور خلاصه میدان p ـ ادیک‌ها که آن را با نمادِ $\mathbb{Q}_p$ نشان می‌دهیم از سری‌هایی به صورت $\sum\limits_{i=-n}^{\infty} a_i p^i$ تشکیل شده که در آن هر ضریبِ a_i متعلق به مجموعه‌ی $\{0, 1, \cdots, p-1\}$ است و p یک عدد اول و n یک عدد صحیح است. مطابق آنچه در ۱۱.۳ خواهیم دید، $\mathbb{Z}_p := \{\sum\limits_{i=0}^{\infty} a_i p^i : 0 \leq a_i \leq p-1\}$ یک حلقه‌ی ارزیاب در $\mathbb{Q}_p$ است که به آن حلقه‌ی p ـ ادیک گفته می‌شود. نگاشت ارزیابیِ $v : \mathbb{Q}_p \to \mathbb{Z}$ با ضابطه‌ی $v(\sum\limits_{i=-n}^{\infty} a_i p^i) := \min\{i : a_i \neq 0\}$ این حلقه‌ی ارزیاب را ایجاد می‌کند. به سادگی می‌توان دید که $p\mathbb{Z}_p$ ایده‌آل ماکسیمال این حلقه‌ی ارزیاب است و بنابراین میدان پیمانه‌های این نگاشت

[1] variety

ارزیابی برابر است با $\frac{\mathbb{Z}_p}{p\mathbb{Z}_p} = \mathbb{F}_p$.

یک مثال حائز اهمیت دیگر از میدان‌های ارزیابی، میدانِ $\mathbb{F}_q((t))$ متشکل از سری‌هایی به صورت $\sum_{i=-n}^{\infty} a_i t^i$ است که در آن هر ضریبِ a_i متعلق به $\mathbb{F}_q$ و n یک عدد صحیح است. نگاشت $v : \mathbb{F}_q((t)) \to \mathbb{Z}$ با ضابطه‌ی $v(\sum_{i=-n}^{\infty} a_i t^i) := \min\{i | a_i \neq 0\}$ یک ارزیابی روی این میدان است که حلقه‌ی ارزیاب آن برابر با $\{\sum_{i=0}^{\infty} a_i t^i | a_i \in \mathbb{F}_q\}$ است که آن را با نمادِ $\mathbb{F}_q[[t]]$ نشان می‌دهیم. به سادگی قابل بررسی است که تنها ایده‌آل ماکزیمالِ $\mathbb{F}_q[[t]]$ برابر با $t\mathbb{F}_q[[t]]$ است و از این رو $\frac{\mathbb{F}_q[[t]]}{t\mathbb{F}_q[[t]]} = \mathbb{F}_q$ میدان پیمانه‌های این نگاشت ارزیابی است.

موضوع تعریف‌پذیری حلقه‌های ارزیاب در میدان‌های ارزیابی یکی از مسائل جذاب و چالش برانگیز در نظریه‌ی مدل‌ها است که در سال‌های اخیر، توجه فزاینده‌ای را به خود جلب کرده است. از این رو مقالات بسیاری در این زمینه منتشر شده است که در ادامه قصد داریم به صورت خلاصه به قضایای اصلی برخی از آن‌ها اشاره کنیم. تعاریف مورد نیاز برای نتایج اشاره شده در بندهای پیش رو در داخل پایان‌نامه موجود هستند.

یکی از قدیمی‌ترین نتایج در این زمینه، نتیجه‌ی معروف تعریف‌پذیری حلقه‌ی $\mathbb{Z}_p$ در $\mathbb{Q}_p$ با فرمولِ $\exists y\ 1 + kx^2 = y^2$ برای هر عدد اول p است. در این فرمول اگر p مخالف 2 باشد، آن‌گاه $k = 2$ و اگر $p = 2$ آن‌گاه $k = 8$ (برای مطالعه‌ی اثبات این قضیه به ۴۴.۲ مراجعه کنید). به علاوه اَکْسْ [2] در مقاله‌ی [۲] نشان داده است که اگر F یک میدان دلخواه باشد، آن‌گاه حلقه‌ی ارزیابِ $F[[t]] = \{\sum_{i=0}^{\infty} a_i t^i : i \in \mathbb{N}\}$ در میدان ارزیابیِ $F((t)) = \{\sum_{i=-n}^{\infty} a_i t^i : i \in \mathbb{N}\}$ تعریف‌پذیر است. بعد از آن نیز نتایج تعریف‌پذیری بسیاری روی میدان ارزیابی $F((t))$ با قرار دادن شرط‌هایی روی میدانِ F صورت گرفته است.

اولین تعمیم این نتایج توسط کونیگزمن [3] در مقاله‌ی [۱۴] ارائه شده است. وی اثبات کرد که اگر (K, O_v) یک میدان ارزیابی *هنسلی* باشد که گروه ارزیاب آن *ارشمیدسی* است ولی بخش‌پذیر نیست، آن‌گاه O_v در زبان حلقه‌ها تعریف‌پذیر است. هانگ [4] در یک نتیجه از مقاله‌ی [۱۰]، نشان می‌دهد که فرمول ارائه شده برای تعریف‌پذیری حلقه‌های p ـ ادیک، قابل تعمیم به میدان‌های ارزیابی هنسلی با گروه ارزیابی گسسته است (در فصل ۷ به بررسی این نتیجه و اثبات آن پرداخته‌ایم). همچنین در همین مقاله، با الهام‌گیری از ایده و روش اَکْسْ، قضیه‌ای کلی‌تر در این زمینه بیان شده که به شرح زیر است:

قضیه ۱.۰. فرض کنید $v : K \to \Gamma$ یک نگاشت ارزیابی هنسلی است. اگر Γ بخش‌پذیر نباشد ولی به ازای هر زیرگروه محدب و ناتهیِ Δ از Γ، گروه خارج قسمتیِ Γ/Δ بخش‌پذیر باشد، آن‌گاه O_v تعریف‌پذیر است.

با قراردادن شرایطی روی میدان پیمانه‌ها نیز می‌توان به حلقه‌های ارزیاب تعریف‌پذیر دست پیدا کرد. برای مثال در مقاله‌ی [۷] اثبات شده که اگر (K, O_v) یک میدان ارزیابی هنسلی با *میدان پیمانه‌های* متناهی یا سودو بسته‌ی جبری [5] باشد که بخش جبری آن بسته‌ی جبری نیست، آن‌گاه O_v با یک فرمول وجودی و بدون پارامتر تعریف‌پذیر است

[2] James Ax
[3] Koenigsmann
[4] Jighan Hong
[5] pseudo-algebraically closed

(اثبات این قضیه در حالتی که میدان پیمانه‌ها متناهی باشد در فصل ۷ شرح داده شده است). علاوه بر مواردی که بیان شد، مقالات متعدد دیگری از جمله [۱۵]، [۱۳]، [۱۸] مسئله‌ی تعریف‌پذیری حلقه‌های ارزیاب در میدان‌های ارزیابی را مورد بررسی قرار داده اند. در کنار چنین مقالاتی که توجه‌شان معطوف به تعریف‌پذیری حلقه‌های ارزیاب در میدان‌های ارزیابی است، مقالاتی مانند [۴] مثال‌هایی معرفی کرده‌اند که در آن‌ها حلقه‌ی ارزیاب در میدان ارزیابی تعریف‌پذیر نیست. همچنین در برخی مقالات دیگر مانند [۱۲]، [۸]، [۱۹] تمرکز بر روی تعریف‌پذیری بدون پارامتر و یا تعریف‌پذیری با پیچیدگی سوری کمتر بوده است.

در مقاله‌ی موردنظر این پایان‌نامه تعریف‌پذیری یک حلقه‌ی ارزیاب خاص در یک میدان ارزیابی اثبات شده است. در واقع قضیه‌ی اصلی این مقاله به شرح زیر است:

«حلقه‌ی ارزیابِ $\mathbb{F}_q[[t]]$ در میدان ارزیابیِ $\mathbb{F}_q((t))$ با یک فرمول وجودی بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است.» در این پایان‌نامه اثبات این قضیه، به همراه همه پیش‌نیازهای آن به تفصیل توضیح داده شده است. در ادامه قصد داریم فرایند این اثبات را به طور خلاصه شرح دهیم.

برهان این قضیه، اساساً متکی بر قضیه‌ی زیر از زیگلر - پرستل است:

قضیه ۲.۰. فرض کنید (K, τ) یک میدان tـ هنسلی باشد که بسته‌ی جدایی‌پذیر نیست. یک چندجمله‌ای تحویل‌ناپذیر و جدایی‌پذیرِ f را در $K[x]$ در نظر بگیرید که در K ریشه‌ای ندارد. همچنین فرض کنید $a \in K$ در شرطِ $f'(a) \neq 0$ صدق می‌کند. در این صورت، مجموعه‌ی $U_{f,a} := \{\frac{1}{f(x)} - \frac{1}{f(a)} : x \in K\}$ یک همسایگی باز و کراندار حول 0 است.

با فرضِ دانستن قضیه‌ی فوق، اثبات قضیه‌ی مورد نظر پایان‌نامه در فصل ۶ و طی مراحل زیر صورت می‌پذیرد:

- **مرحله‌ی اول:** خواهیم دید که $K = \mathbb{F}_q((t))$ در شروط قضیه‌ی فوق صدق می‌کند، از این رو $U_{f,a}$ به ازای یک چندجمله‌ای مناسبِ f در $\mathbb{F}_q((t))[x]$ و یک عنصر مناسبِ a در $\mathbb{F}_q((t))$ یک همسایگی باز و کراندار از صفر در میدانِ $\mathbb{F}_q((t))$ است. در این مرحله با به کارگیری یک نتیجه از قضیه‌ی ۲.۰، پارامترهای فرمولی که این همسایگی را تعریف می‌کند را به $\mathbb{F}_q$ تقلیل می‌دهیم.

- **مرحله‌ی دوم:** با استفاده از ویژگی کرانداری و باز بودنِ $U_{f,a}$ می‌توان از آن به یک مجموعه‌ی Y رسید که شامل $t\mathbb{F}_q[[t]]$ و مشمول در $\mathbb{F}_q[[t]]$ است و همچنین توسط یک فرمول وجودی و با پارامتر از $\mathbb{F}_q$ تعریف می‌شود. به سادگی می‌توان نشان داد که $\mathbb{F}_q[[t]] = \mathbb{F}_q + Y$ و از آنجایی که عناصرِ $\mathbb{F}_q$ ریشه‌های چندجمله‌ای $x^q - x$ هستند و Y تعریف‌پذیر است، پس می‌توان نتیجه گرفت که $\mathbb{F}_q[[t]]$ با فرمولِ $\varphi := \exists y(y^q - y = 0 \wedge x \in y + Y)$ تعریف‌پذیر است.

- **مرحله‌ی سوم:** فرمول φ وجودی و با پارامتر از $\mathbb{F}_q$ است. برای حذف این پارامترها ابتدا یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}_p[x]$ از درجه‌ی l را به طوری در نظر می‌گیریم که $l \nmid k$. در این صورت، یک عنصر a در

$\mathbb{F}_q$ وجود دارد به طوری که $D(f)(a) \neq 0$. حال با استفاده از این f و a مجموعه‌ی $U_{f,a}$ را تشکیل می‌دهیم. سپس، با در نظر گرفتن $V := \bigcup\{U_{f,a} : a \in \mathbb{F}_q, Df(a) \neq 0\}$ که یک همسایگی کراندار و تعریف‌پذیر از صفر است و با استفاده از مرحله‌ی ۲ می‌توانیم به یک مجموعه‌ی مطلوبِ Y برسیم که تعریف‌پذیر با یک فرمول وجودی و با پارامتر از $\mathbb{F}_p$ است. نهایتاً چون پارامترها متعلق به $\mathbb{F}_p$ هستند می‌توان آن‌ها را با ترم‌های بسته‌ی نظیرشان جایگزین کرد و اینگونه φ به یک فرمول بدون پارامتر تبدیل می‌شود.

اما قضیه‌ی ۲.۰ که در مقاله‌ی [۱] دانسته فرض شده، به همین صورت مشخص در مقاله‌ای نیامده است. از این رو، به عنوان یکی از اهداف مهم این پایان‌نامه اثبات این قضیه با مطالعه‌ی منابع [۲۲] و [۱۸] استخراج شده و به صورت مبسوط در فصل ۵ آمده است.

علاوه بر آنچه شرح داده شد، در فصل اول پایان‌نامه، پس از معرفی مفاهیم پایه‌ای از منطق، به بحث درباره‌ی مقدمات جبری و به ویژه میدان‌های متناهی و کامل می‌پردازیم. در فصل دوم حلقه‌های موضعی و نُرم‌دار را معرفی می‌کنیم و بعد از آن میدان و حلقه‌های pـ ادیک را شرح می‌دهیم. در فصل سوم ابتدا میدان‌های ارزیابی را معرفی و سپس میدان سری‌های هان را به عنوان یک مثال از آن‌ها بررسی می‌کنیم. مهم‌ترین قضیه اثبات شده در فصل چهارم این است که یک توپولوژی روی یک میدان، Vـ توپولوژی است اگروتنهااگر توپولوژی القاء شده توسط یک ارزیابی یا توپولوژی القاء شده توسط یک نگاشت قدرمطلق باشد.

در ابتدای هر فصل، منبع قضایای آن ذکر شده است. همچنین، در پایان هر فصل به دلیل پیچیدگی اثبات‌ها و تنوع مطالب، یک خلاصه از موضوعات مورد بحث آن فصل ارائه شده است. اثبات بسیاری از لم‌ها توسط نگارنده پایان‌نامه نوشته شده است و در منابع استفاده شده یافت نمی‌شود.

در پایان مایلم مراتب قدردانی و سپاس را نسبت به استاد راهنمای بزرگوارم، آقای دکتر محسن خانی که تعهد، شور و اشتیاق ایشان در حوزه‌ی ریاضیات همواره برایم الهام‌بخش بوده، بجا بیاورم. لازم به ذکر است که شکل‌گیری این پایان‌نامه در قالب پیش‌رو بدون نظرها، پیگیری‌های دلسوزانه و دانش گسترده‌ی ایشان در این زمینه میسّر نبود.

فصل ۱

مقدماتی از منطق و جبر

برای توضیح مقاله‌ی موردنظر این پایان‌نامه، نیاز به مقدماتی از منطق و جبر است. در قسمت منطقی، مهم‌ترین مفهوم مورد نیاز ما «تعریف‌پذیری» است. در قسمت جبری، «جبر میدان‌های متناهی» مورد نیاز ما خواهد بود. مطالب این فصل از کتاب‌های [۱۱] و [۱۶] گردآوری شده‌است.

۱.۱ مفاهیم مقدماتی از منطق

۱.۱.۱ معرفی یک زبان مرتبه اول، ترم‌ها و فرمول‌ها

تعریف ۱.۱. منظور از یک زبان مرتبه اولِ $\mathcal{L}$ مجموعه‌ای به صورتِ اجتماع سه مجموعه‌ی مجزای $\mathcal{F}\cup\mathcal{R}\cup\mathcal{C}$ است که در آن مجموعه‌ی $\mathcal{F}$ را مجموعه‌ی نمادهای تابعی، $\mathcal{R}$ را مجموعه‌ی نمادهای رابطه‌ای و $\mathcal{C}$ را مجموعه‌ی نمادهای ثابت زبان می‌خوانیم. همچنین، برای هر $f\in\mathcal{F}$ یک عدد طبیعی n_f به عنوان تعداد مواضعِ f در نظر گرفته می‌شود. به طور مشابه، برای هر $R\in\mathcal{R}$ یک عددِ n_R را به عنوان تعداد مواضع رابطه‌ی R در نظر می‌گیریم.

توجه کنید که یک «نماد تابعی» با یک تابع فرق می‌کند. تابع یک عمل است از یک مجموعه به مجموعه‌ای دیگر؛ اما نماد تابعی، صرفاً یک اسم است.

مثال ۲.۱. زبان حلقه‌های یکدار به صورتِ $\mathcal{L}_{ring}=\{+,\cdot,0,1\}$ است که در آن $0,1$ نمادهای ثابت هستند و $+,\cdot$ نمادهای تابعی دو موضعی هستند.

یک مجموعه‌ی $\{v_0, v_1, \cdots\}$ از متغیرها را در نظر بگیرید.

تعریف ۳.۱. ($\mathcal{L}$ ترم‌ها) فرض کنید $\mathcal{L}$ یک زبان مرتبه‌ی اول باشد. مجموعه‌ی $\mathcal{L}$ ترم‌ها به صورت استقرایی زیر تعریف می‌شود:

۱. هر نماد ثابتِ $c \in \mathcal{C}$ و هر متغیرِ v یک ترم است.

۲. اگر $t_1, \cdots, t_n$ ترم باشند و f یک نماد تابعی n موضعی باشد، آنگاه $f(t_1, \cdots, t_n)$ نیز یک ترم است.

تعریف ۴.۱. فرض کنید $\mathcal{L}$ یک زبان مرتبه‌ی اول باشد. $\mathcal{L}$ ترم‌هایی که در آن‌ها هیچ متغیری وجود ندارد، *ترم‌های* بسته نامیده می‌شوند. به بیان دیگر، ترم‌های بسته به صورتِ $f(c_1, \cdots, c_n)$ یا c_m هستند که در آن‌ها f یک نماد تابعی و $c_1, \cdots, c_n$ و c_m نمادهای ثابت در زبانِ $\mathcal{L}$ هستند.

پس از آشنایی با $\mathcal{L}$ ترم‌ها، قدم بعدی شناخت $\mathcal{L}$ فرمول‌ها است. به بیان نادقیق، $\mathcal{L}$ فرمول‌ها با استفاده از نمادهای به کار رفته در زبان مرتبه‌ی اولِ $\mathcal{L}$، متغیرهای $\{v_0, v_1, \cdots\}$ و ادوات منطقی $\neg, \wedge, \exists$ و نماد تساوی تولید می‌شوند. در تعریف زیر به طور دقیق(استقرائی) نحوه‌ی ساخت $\mathcal{L}$ فرمول‌ها را بیان کرده‌ایم.

تعریف ۵.۱. ($\mathcal{L}$ فرمول‌ها) فرض کنید $\mathcal{L}$ یک زبان مرتبه‌ی اول باشد. مجموعه‌ی $\mathcal{L}$ فرمول‌ها به صورت زیر حاصل می‌شود:

۱. اگر t_1 و t_2 دو $\mathcal{L}$ ترم باشند، آنگاه $t_1 = t_2$ یک $\mathcal{L}$ فرمول است.

۲. اگر $t_1, \cdots, t_n$ چند $\mathcal{L}$ ترم باشند و $\mathcal{R}$ یک نماد رابطه‌ای n موضعی در $\mathcal{L}$ باشد، آنگاه $\mathcal{R}(t_1, t_2, \cdots, t_n)$ یک $\mathcal{L}$ فرمول است.

۳. اگر ψ یک $\mathcal{L}$ فرمول باشد، آنگاه $\neg\psi$ نیز یک $\mathcal{L}$ فرمول است.

۴. اگر ψ_1, ψ_2 دو $\mathcal{L}$ فرمول باشند، آنگاه $(\psi_1 \wedge \psi_2)$ نیز یک $\mathcal{L}$ فرمول است.

۵. اگر ψ یک $\mathcal{L}$ فرمول باشد، آنگاه $\exists x\psi$ نیز یک $\mathcal{L}$ فرمول است.

۲.۱.۱ معرفی یک $\mathcal{L}$ ساختار و تعبیر ترم‌ها و فرمول‌ها

فرض کنید $\mathcal{L}$ یک زبان مرتبه‌ی اول باشد. یک $\mathcal{L}$ ساختارِ $\mathcal{M}$ از یک مجموعه‌ی M (به نامِ جهانِ $\mathcal{L}$ ساختار) و موارد زیر تشکیل شده است:

۱. برای هر نمادِ ثابت $c \in \mathcal{L}$ یک عنصر مشخصِ $c^{\mathcal{M}} \in M$. به چنین عنصری تعبیر ثابت c در ساختارِ $\mathcal{M}$ می‌گوییم.

۲. برای هر نماد تابعیِ n موضعیِ $f \in \mathcal{L}$ یک تابعِ $f^{\mathcal{M}} : M^n \to M$. به این تابع، تعبیر نماد تابعیِ f در ساختارِ $\mathcal{M}$ می‌گوییم.

۳. برای هر نماد رابطه‌ای n موضعیِ $R \in \mathcal{L}$ یک رابطه‌ی $R^{\mathcal{M}}$ روی M. به این رابطه، تعبیر رابطه‌ی R در ساختارِ $\mathcal{M}$ می‌گوییم.

به ازای هر $f, c, R \in \mathcal{L}$ یک $\mathcal{L}$ ساختارِ $\mathcal{M}$ به صورتِ $\mathcal{M} = (M, \{c^{\mathcal{M}}, f^{\mathcal{M}}, R^{\mathcal{M}}\})$ نوشته می‌شود.

مثال ۶.۱. زبانِ $\mathcal{L} = \{+, \cdot, 0, 1, <\}$ را در نظر بگیرید. در این صورت، $\mathcal{R} = (\mathbb{R}, +, \cdot, 0, 1, \leq)$ یک $\mathcal{L}$ ساختار است.

حال که با $\mathcal{L}$ ساختارها آشنا شدیم قصد داریم ترم‌ها و فرمول‌ها را در این ساختارها تعبیر کنیم. در راستای این کار، ابتدا نگاشت تعبیر را معرفی می‌کنیم.

تعریف ۷.۱. (نگاشت تعبیر) فرض کنید $\mathcal{M}$ یک $\mathcal{L}$ ساختار باشد. منظور از یک *نگاشت تعبیر* در جهانِ M، یک تابع به صورت $\beta : \{v_0, v_1, \cdots\} \to M$ است. دامنه‌ی این تابع، مجموعه‌ی متغیرهاست و بُرد آن جهانِ $\mathcal{L}$ ساختارِ $\mathcal{M}$ است.

تعریف ۸.۱. (تعبیر ترم‌ها) فرض کنید $\mathcal{M}$ یک $\mathcal{L}$ ساختار، β یک تابع تعبیر(مطابق تعریف فوق) و t یک $\mathcal{L}$ ترم باشد. تعبیر ترم t در ساختارِ $\mathcal{M}$ با نگاشت تعبیرِ β را با $t^{\mathcal{M}}[\beta]$ نشان می‌دهیم و آن را به صورت استقراییِ زیر تعریف می‌کنیم:

۱. اگر t یک متغیرِ v باشد، آنگاه قرار می‌دهیم: $t^{\mathcal{M}}[\beta] = \beta(v)$.

۲. اگر t یک ثابتِ c باشد، آنگاه قرار می‌دهیم: $t^{\mathcal{M}}[\beta] = c^{\mathcal{M}}$.

۳. اگر تعبیر ترم‌های $t_1, \cdots, t_n$ را در $\mathcal{L}$ ساختارِ $\mathcal{M}$ بدانیم و f یک نماد تابعیِ n متغیره باشد، آنگاه $f(t_1, \cdots, t_n)$ را به صورت زیر تعبیر می‌کنیم:

$$f^{\mathcal{M}}(t_1, \cdots, t_n)[\beta] = f^{\mathcal{M}}(t_1^{\mathcal{M}}[\beta], \cdots, t_n^{\mathcal{M}}[\beta]).$$

مثال ۹.۱. می‌خواهیم ترمِ $+ \cdot v_1 c_1 \cdot v_2 v_3$ را با نگاشت تعبیرِ $\beta : \{v_1, v_2. v_3\} \to \mathbb{R}$ با ضابطه‌ی $\beta(v_1) = 1$ و $\beta(v_2) = 2$ و $\beta(v_3) = 3$ در ساختارِ $\mathcal{R} = (\mathbb{R}, +, \cdot, 0)$ تعبیر کنیم. ابتدا توجه کنید که می‌توانیم به جای $+ \cdot v_1 c_1 \cdot v_2 v_3$ بنویسیم $(v_1 \cdot c_1) + (v_2 \cdot v_3)$. بنابراین تعبیر ترم فوق در ساختارِ $\mathcal{R}$ به صورت زیر است:

$$((v_1 \cdot c_1) + (v_2 \cdot v_3))^{\mathcal{R}}[\beta] = 1 \cdot 0 + 2 \cdot 3 = 6$$

فرض کنید φ یک $\mathcal{L}$ فرمول، $\mathcal{M}$ یک $\mathcal{L}$ ساختار و β یک نگاشت تعبیرِ متغیرها در M، یعنی جهانِ ساختار $\mathcal{M}$ باشد. منظور از عبارتِ $\mathcal{M} \models \varphi[\beta]$ این است که فرمولِ φ با ارزیابی β از متغیرها در ساختارِ $\mathcal{M}$ درست است. در تعریف زیر به صورتِ دقیق و استقرایی، همین تعریف را بیان کرده‌ایم.

تعریف ۱۰.۱. (درست بودن یک فرمول در یک ساختار) عبارتِ $\mathcal{M} \models \varphi[\beta]$ به صورت استقرایی زیر تعریف می‌شود:

۱. فرض کنید t_1 و t_2 دو ترم باشند.

$$\mathcal{M} \models (t_1 = t_2)[\beta] \iff t_1^{\mathcal{M}}[\beta] = t_2^{\mathcal{M}}[\beta].$$

یعنی زمانی فرمولِ $t_1 = t_2$ در ساختارِ $\mathcal{M}$ درست است که تعبیرهای ترم‌های t_1 و t_2 در این ساختار باهم برابر باشند.

۲. فرض کنید R یک نماد رابطه‌ای در زبان باشد و $t_1, \cdots, t_n$ ترم باشند.

$$\mathcal{M} \models R(t_1, \cdots, t_n)[\beta] \iff R^{\mathcal{M}}(t_1^{\mathcal{M}}[\beta], \cdots, t_2^{\mathcal{M}}[\beta]).$$

یعنی زمانی فرمولِ $R(t_1, \cdots, t_n)$ در ساختارِ $\mathcal{M}$ درست است که تعبیر ترم‌های t_i در این ساختار با یکدیگر در رابطه‌ی $R^{\mathcal{M}}$ باشند.

۳. $\mathcal{M} \models \neg\varphi[\beta]$ هرگاه $\mathcal{M} \not\models \varphi[\beta]$.

۴. فرض کنید ψ_1 و ψ_2 دو $\mathcal{L}$ فرمول باشند.

$$\mathcal{M} \models (\psi_1 \wedge \psi_2)[\beta] \iff \mathcal{M} \models \psi_1[\beta] \quad \text{و} \quad \mathcal{M} \models \psi_2[\beta]$$

۵. فرض کنید ψ یک $\mathcal{L}$ فرمول باشد. $\mathcal{M} \models \exists x\ \psi[\beta]$ هرگاه یک عنصرِ $a \in M$ موجود باشد به طوری که $\mathcal{M} \models \psi[\beta\frac{a}{x}]$ که در آن $\beta\frac{a}{x}$ یک نگاشت تعبیر متغیرهاست و ضابطه‌ی آن به صورت زیر است:

$$\beta\frac{a}{x}(v) = \begin{cases} \beta(v) & v \neq x \\ a & v = x \end{cases}$$

تعریف ۱۱.۱. در یک فرمول، به متغیری که در دامنه‌ی تأثیر یک سور قرار نگیرد، *متغیر آزاد* گفته می‌شود.

فرض کنید $\mathcal{M}$ یک $\mathcal{L}$ ساختار و M جهان آن باشد. همچنین، فرض کنید $a_1, a_2, \cdots, a_n \in M$ و $\varphi(x_1, x_2, \cdots, x_n)$ یک فرمول با متغیرهای آزاد در میان $x_1, x_2, \cdots, x_n$ باشد. اگر β یک نگاشت تعبیر از متغیرها در M با ضابطه‌ی $\beta(x_i) = a_i$ باشد، آنگاه به جای $\mathcal{M} \models \varphi[\beta]$ می‌نویسیم $\mathcal{M} \models \varphi(a_1, a_2, \cdots, a_n)$. همچنین، اگر $t(x_1, \cdots, x_n)$ یک ترم باشد، آنگاه به جای $t^{\mathcal{M}}[\beta]$ می‌نویسیم $t^{\mathcal{M}}(a_1, a_2, \cdots, a_n)$.

۳.۱.۱ تعریف‌پذیری

در منطق، مفهوم "تعریف‌پذیری یک مجموعه در یک ساختار" به معنای امکان توصیف آن مجموعه با استفاده از یک فرمول در یک زبان خاص است.

همان‌طور که در پیشگفتار اشاره شد، در این پایان‌نامه به دنبال اثبات تعریف‌پذیری $\mathbb{F}_q[[t]]$ در ساختارِ $\mathbb{F}_q((t))$ هستیم. به عبارت دیگر، هدف ما پیدا کردن یک فرمول در زبان حلقه‌هاست که عناصر مجموعه‌ی $\mathbb{F}_q[[t]]$ آن را در ساختار $\mathbb{F}_q((t))$ برآورده کنند، اما عناصر خارج از این مجموعه در آن صدق نکنند (جزئیات مربوط به $\mathbb{F}_q[[t]]$ و $\mathbb{F}_q((t))$ را در فصل ۲ بررسی خواهیم کرد).

تعریف ۱۲.۱. (تعریف‌پذیری) فرض کنید $\mathcal{M}$ یک $\mathcal{L}$ ساختار با جهان M باشد و $A \subseteq M$. می‌گوییم مجموعه‌ی $X \subseteq M^n$ یک مجموعه‌ی A ـ *تعریف‌پذیر* است هرگاه $\mathcal{L}$ فرمولِ $\varphi(x_1, \cdots, x_n, a_1, \cdots, a_m)$ موجود باشد که در آن $a_1, ..., a_m \in A$ و

$$X = \{(b_1, \cdots, b_n) \in M^n | \mathcal{M} \vDash \varphi(b_1, \cdots, b_n, a_1, \cdots, a_m)\}.$$

همچنین، می‌گوییم X بدون پارامتر تعریف‌پذیر یا $\emptyset$ ـ تعریف‌پذیر است هرگاه $A = \emptyset$.

مثال ۱۳.۱. ساختار $\mathcal{N} = (\mathbb{N}, <)$ را در نظر بگیرید. مجموعه‌ی $\{n\}$ که در آن n یک عدد طبیعی و ناصفر است را می‌توان با فرمول بدون پارامتر زیر تعریف کرد:

$$\varphi(x) = \exists x_1, x_2, \cdots, x_n(x_1 < x_2 \wedge \cdots x_n < x \wedge \forall y(y < x \to (y = x_0 \vee \cdots \vee y = x_n))).$$

مثال ۱۴.۱. فرض کنید که F یک میدان و $\mathcal{M} = (F[x], +, \cdot, 0, 1)$ یک $\mathcal{L}$ ساختار باشد. در این صورت $F \subseteq F[x]$ تعریف‌پذیر است، زیرا تنها عناصر وارون‌پذیرِ $F[x]$ اعضای F هستند و بنابراین $F = \{x \in F[x] : \mathcal{M} \models x = 0 \vee \exists y\ x \cdot y = 1\}$.

مثال ۱۵.۱. ساختارِ $\mathcal{R} = (\mathbb{R}, 0, 1, \cdot, +)$ را در نظر بگیرید. توجه کنید که اگر چه رابطه‌ی ترتیب به صورت مستقیم در این ساختار قرار ندارد، اما می‌توان با فرمولِ $\varphi(x) = \exists y(y \cdot y = x)$ مجموعه‌ی اعداد حقیقی نامنفی را در $\mathcal{R}$ تعریف کرد؛ زیرا تنها اعداد نامنفی دارای ریشه دوم هستند.

مثال ۱۶.۱. مجموعه‌ی $Y = \{(x, y) \in \mathbb{Z}^2 : x < y\}$ در ساختارِ $\mathcal{M} = (\mathbb{Z}, +, \cdot, 0, 1)$ تعریف‌پذیر است. زیرا بر اساس قضیه‌ی لاگرانژ، هر عدد صحیح مثبت حاصل جمع چهار مربع کامل است، بنابراین داریم:

$$Y = \{(x, y) \in \mathbb{Z}^2 : x < y\} = \{(x, y) \in \mathbb{Z}^2 : \mathcal{M} \models \exists t_1\ \exists t_2\ \exists t_3\ \exists t_4\ \ y = x + t_1^2 + t_2^2 + t_3^2 + t_4^2\}$$

۲.۱ مقدمات جبری

در این بخش، مباحث جبری مورد نیاز برای مطالعه‌ی این پایان‌نامه آورده شده است.

۱.۲.۱ توسیع جبری

اگر L یک میدان و K یک زیرمیدان از آن باشد، آنگاه می‌گوییم L یک توسیع از میدانِ K است و می‌نویسیم $K \subseteq L$.

تعریف ۱۷.۱. فرض کنید K و L دو میدان باشند و $K \subseteq L$. یک عنصرِ $\alpha \in L \setminus K$ را روی K *جبری* می‌نامیم هرگاه یک چندجمله‌ای $f \in K[x]$ موجود باشد به طوری که $f(\alpha) = 0$. همچنین، اگر عنصرِ α روی K جبری نباشد، آن را *متعالی* می‌نامیم.

می‌گوییم توسیعِ $K \subseteq L$ جبری است هرگاه هر عنصرِ $\alpha \in L \setminus K$ روی K جبری باشد. میدانِ K را *بسته‌ی جبری* می‌نامیم هرگاه ریشه‌های هر چندجمله‌ای موجود در $K[x]$، همگی متعلق به K باشند. یک توسیع جبری از میدانِ K که همه‌ی چندجمله‌ای‌های متعلق به $K[x]$ در آن ریشه دارند را *بستار جبری* K می‌نامیم و آن را با نمادِ K^{cl} نشان می‌دهیم.

فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. در این صورت، L یک فضای برداری روی میدانِ K است. (در این فضای برداری، ضرب اسکالر همان عمل ضرب میدانِ L و جمع برداری همان عمل جمع میدانِ L است.)

تعریف ۱۸.۱. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. بُعد فضای برداری L روی میدان K را با $[L : K]$ نشان می‌دهیم. همچنین اگر $[L : K]$ متناهی باشد، گوییم $K \subseteq L$ یک توسیع متناهی است.

لم ۱۹.۱. فرض کنید K و L دو میدان باشند. اگر $K \subseteq L$ یک توسیع متناهی باشد، آنگاه یک توسیع جبری است.

اثبات. می‌خواهیم نشان دهیم که هر عنصرِ $\alpha \in L \setminus K$ روی K جبری است. با برهان خلف، فرض کنید یک عنصرِ α در $L \setminus K$ وجود دارد به طوری که متعالی است. بنابراین عناصر مجموعه‌ی $\{1, \alpha, \alpha^2, \alpha^3, \cdots\}$ مستقل خطی هستند، زیرا در غیر این صورت، یک ترکیب خطی متناهی از آن‌ها برابر با صفر می‌شود و این به معنای داشتن یک چندجمله‌ای با ریشه‌ی α است که با فرض متعالی بودنِ α در تناقض است. از این رو با توجه به مستقل خطی بودن عناصرِ $\{1, \alpha, \alpha^2, \alpha^3, \cdots\}$، می‌توان نتیجه گرفت که $[L : K]$ نامتناهی است و این با فرض تناقض دارد. $\square$

فرض کنید $K \subseteq L$ یک توسیع میدانی و $\alpha \in L \setminus K$ یک عنصر جبری روی K باشد. $f \in K[x]$ را چندجمله‌ای مینیمالِ α می‌نامیم هرگاه $f(\alpha) = 0$ و f از میان چندجمله‌ای‌هایی در $K[x]$ که α ریشه‌ی آن‌هاست، حداقل درجه را داشته باشد.

لم ۲۰.۱. فرض کنید $K \subseteq L$ یک توسیع میدانی و $\alpha \in L \setminus K$ یک عنصر جبری روی K باشد. $f \in K[x]$ چندجمله‌ای مینیمالِ α است اگروتنهااگر f تحویل‌ناپذیر باشد و $f(\alpha) = 0$.

اثبات. فرض کنید f چندجمله‌ای مینیمالِ α باشد. در این صورت $f(\alpha) = 0$. ادعا می‌کنیم که f تحویل‌ناپذیر است. با برهان خلف فرض کنید f تحویل‌پذیر باشد، یعنی $f = gh$ که در آن $g, h \in K[x]$ و $\deg(g), \deg(h) < \deg(f)$. حال از آنجا که $f(\alpha) = g(\alpha)h(\alpha) = 0$، پس یا $g(\alpha) = 0$ یا $h(\alpha) = 0$ که این با مینیمال بودنِ f در تناقض است.

برای اثبات جهت عکس، فرض کنید f تحویل‌ناپذیر باشد و $f(\alpha) = 0$. با برهان خلف، فرض کنید f چندجمله‌ای مینیمالِ α نباشد. بنابراین، یک چندجمله‌ای $h \in K[x]$ وجود دارد که درجه آن کمتر از درجه f است و چندجمله‌ای مینیمالِ α است. حال f را بر h تقسیم می‌کنیم، پس داریم $f = hm + r$. از آنجا که $f(\alpha) = h(\alpha)m(\alpha) + r(\alpha) = 0$ و $h(\alpha) = 0$، پس باید $r(\alpha)$ نیز برابر با صفر باشد. اما این با اینکه h چندجمله‌ای مینیمالِ α است تناقض دارد، زیرا درجه‌ی r کمتر از درجه‌ی h است. □

فرض کنید $K \subseteq L$ یک توسیع میدانی و $\alpha \in L \setminus K$ یک عنصر جبری روی K باشد. در ادامه، قصد داریم میدان تولید شده توسط α و K درون میدانِ L را بررسی کنیم.

ابتدا نگاشتِ $\varphi : K[x] \to L$ که هر $h(x) \in K[x]$ را به $h(\alpha)$ می‌برد را در نظر بگیرید. به سادگی می‌توان دید که این نگاشت یک همریختی است و تصویر آن در L برابر است با $K[\alpha] = \{h(\alpha) : h \in K[x]\}$. هسته‌ی این نگاشت به صورت زیر است:

$$\ker(\varphi) = \{h \in K[x] : h(\alpha) = 0\}$$

از طرفی f چندجمله‌ای مینیمالِ α است، پس هر چندجمله‌ای دیگرِ $h(x) \in K[x]$ با این ویژگی که $h(\alpha)$ برابر با صفر است را عاد می‌کند و در نتیجه $\ker(\varphi) = \langle f \rangle$. بنابراین با توجه به قضیه‌ی اول یکریختی $\mathtt{Im}(\varphi) = K[\alpha] \cong \frac{K[x]}{\langle f \rangle}$، پس $K[\alpha]$ کوچکترین میدان شامل K و α در داخلِ L و یکریخت با $\frac{K[x]}{\langle f \rangle}$ است.

نماد گذاری ۲۱.۱. فرض کنید K و L میدان باشند و $K \subseteq L$، همچنین عناصر $\alpha_1, \cdots, \alpha_n$ متعلق به L باشند. در این صورت، میدان تولید شده توسط K و $\alpha_1, \cdots, \alpha_n$ داخل L را با نمادِ $K(\alpha_1, \cdots, \alpha_n)$ نشان می‌دهیم.

لم ۲۲.۱. فرض کنید $K \subseteq L$ و $\alpha \in L \setminus K$ روی K یک عنصر جبری با چندجمله‌ای مینیمالِ f از درجه‌ی n باشد. در این صورت $[K(\alpha) : K] = n$.

اثبات. از آنجا که $\alpha \in L \setminus K$ یک عنصر جبری روی K با چندجمله‌ای مینیمالِ f است، پس مطابق آنچه در بالا دیدیم $K(\alpha)$ با $\frac{K[x]}{\langle f \rangle}$ یکریخت است. در نتیجه چون درجه‌ی f برابر با n است، پس عناصر $K(\alpha)$ به صورتِ $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ هستند که در آن $a_0, a_1, \cdots, a_{n-1} \in K$. به بیان دیگر همه‌ی عناصرِ $K(\alpha)$ توسط $\{1, \alpha, \cdots, \alpha^{n-1}\}$ تولید می‌شوند. از طرفی، عناصرِ $\{1, \alpha, \cdots, \alpha^{n-1}\}$ روی K مستقل خطی هستند، زیرا اگر

یک ترکیب خطی از آن‌ها مانندِ $a_0 + a_1\alpha + \cdots + a_n\alpha^{n-1}$ برابر با صفر شود، آنگاه α ریشه‌ی یک چندجمله‌ای با درجه‌ی کمتر از n است و این با فرض در تناقض است. بنابراین، $\{1, \alpha, \cdots, \alpha^{n-1}\}$ یک پایه برای فضای برداری $K(\alpha)$ روی K است، پس $[K(\alpha) : K] = n$. □

لم ۲۳.۱. فرض کنید $K \subseteq L \subseteq M$. در این صورت، $[M : K] = [M : L] \times [L : K]$.

اثبات. فرض کنید فضای برداری L روی K توسطِ $\{\alpha_1, \cdots, \alpha_n\}$ و M روی L توسطِ $\{\beta_1, \cdots, \beta_m\}$ تولید شده باشد. ادعا می‌کنیم $\{\alpha_i\beta_j\}_{\substack{0\leq j\leq m\\ 0\leq i\leq n}}$ یک پایه برای فضای برداری M روی K است. برای اثبات این ادعا ابتدا یک عنصر t در M را در نظر بگیرید. در این صورت، $t = r_1\beta_1 + r_2\beta_1 + \cdots + r_m\beta_m$ که در آن ضرایبِ $r_1, r_2, \cdots, r_m$ در L قرار دارند. بنابراین این ضرایب توسط عناصر مجموعه‌ی $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ تولید می‌شوند و اینگونه t یک ترکیب خطی از $\alpha_i\beta_j$ها می‌شود. به بیان دیگر $\{\alpha_i\beta_j\}_{\substack{0\leq j\leq m\\ 0\leq i\leq n}}$ یک مجموعه‌ی مولد برای M روی K است.

حال نشان می‌دهیم که عناصرِ مجموعه‌ی $\{\alpha_i\beta_j\}_{\substack{0\leq j\leq m\\ 0\leq i\leq n}}$ مستقل خطی هستند. اگر یک ترکیب خطی از $\alpha_i\beta_j$ها مانندِ $s_1\alpha_1\beta_1 + s_2\alpha_2\beta_2 \cdots + s_k\alpha_k\beta_k$ که در آن $s_i \in K$ برابر با صفر شود، آنگاه $(s_1\alpha_1)\beta_1 + (s_2\alpha_2)\beta_2 \cdots + (s_k\alpha_k)\beta_k = 0$. با توجه به اینکه عناصر مجموعه‌ی $\{\beta_j\}_{1\leq j\leq m}$ مستقل خطی هستند، نتیجه می‌شود که $s_1\alpha_1 = s_2\alpha_2 = \cdots = s_k\alpha_k = 0$. همچنین، عناصر مجموعه‌ی $\{\alpha_i\}_{1\leq i\leq n}$ نیز مستقل خطی هستند، بنابراین $s_1 = s_2 = \cdots = s_k = 0$. □

نتیجه ۲۴.۱. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد. اگر عناصر $\alpha_1, \cdots, \alpha_n$ که متعلق به $L \setminus K$ هستند روی K جبری باشند، آنگاه $K(\alpha_1, \cdots, \alpha_n)$ یک توسیع جبری است.

نتیجه ۲۵.۱. فرض کنید $K \subseteq L$ یک توسیع میدانی باشد و α_1 و α_2 در K روی L جبری باشند. در این صورت $\alpha_1 + \alpha_2$ و $\alpha_1 \cdot \alpha_2$ نیز روی K جبری هستند.

اثبات. از آنجا که $K \subseteq K(\alpha_1)$ یک توسیع جبری است، پس $[K(\alpha_1) : K]$ متناهی است. همچنین α_2 نیز روی K جبری است و چون $K \subseteq K(\alpha_1)$ پس α_2 روی $K(\alpha_1)$ نیز جبری است، بنابراین $[K(\alpha_1)(\alpha_2) : K(\alpha_1)]$ متناهی است. از طرفی، بنا به قضیه‌ی فوق داریم

$$[K(\alpha_1)(\alpha_2) : K] = [K(\alpha_1)(\alpha_2) : K(\alpha_1)] \times [K(\alpha_1) : K]$$

که با توجه به اینکه $[K(\alpha_1)(\alpha_2) : K(\alpha_1)]$ و $[K(\alpha_1) : K]$ هر دو متناهی هستند نتیجه می‌شود که $[K(\alpha_1)(\alpha_2) : K]$ نیز متناهی است. بنابراین بنا به قضیه‌ی ۱۹.۱، $K(\alpha_1)(\alpha_2)$ یک توسیع جبری از K است، پس همه‌ی عناصرِ $K(\alpha_1)(\alpha_2)$ از جمله $\alpha_1 + \alpha_2$ و $\alpha_1 \cdot \alpha_2$ روی K جبری هستند. □

توجه کنید که اثبات جبری بودنِ $\alpha_1+\alpha_2$ یا $\alpha_1\cdot\alpha_2$ به صورت مستقیم آسان نیست. اما با در نظر گرفتن یک توسیع میدانی به عنوان یک فضای برداری و استفاده از قضایای مرتبط با آن به صورت فوق، این اثبات را ساده‌تر کرده است.

لم ۲۶.۱. فرض کنید $K\subseteq L$ یک توسیع میدانی باشد. در این صورت، $E=\{\alpha\in L:$ جبری است K روی $\alpha\}$ یک میدان است.

اثبات. دو عنصر دلخواهِ α_1 و α_2 در E را در نظر بگیرید. در این صورت، $\alpha_1+\alpha_2$، $\alpha_2\cdot\alpha_1$ و α_1^{-1} در $K(\alpha_1,\alpha_2)$ قرار دارند که یک توسیع جبری از K است. در نتیجه این عناصر روی K جبری هستند، پس با توجه به تعریف مجموعه‌ی E، عناصرِ $\alpha_1+\alpha_2$ و $\alpha_2\cdot\alpha_1$ و α_1^{-1} نیز در E قرار دارند و این یعنی E یک میدان است. $\square$

قضیه ۲۷.۱. فرض کنید $K\subseteq L$ یک توسیع میدانی باشد به طوری که $[L:K]$ متناهی است. در این صورت عناصر جبری $\alpha_1,\cdots,\alpha_n\in L$ موجودند به طوری که $L=K(\alpha_1,\cdots,\alpha_n)$.

اثبات. بنا به فرض، $K\subseteq L$ یک توسیع متناهی است، پس با توجه به لمِ ۱۹.۱ یک توسیع جبری است. یک عنصرِ $\alpha_1\in L\setminus K$ را در نظر بگیرید. در این صورت α_1 روی K جبری است، بنابراین $K\subseteq K(\alpha_1)\subseteq L$. توجه کنید که درجه‌ی چندجمله‌ای مینیمالِ α_1 بیشتر از 1 است، زیرا اگر با برهان خلف فرض کنیم که به ازای $a_0,a_1\in K$ داشته باشیم $a_1\alpha_1-a_0=0$، آنگاه با توجه به اینکه $\alpha_1=a_0/a_1$ و a_0/a_1 متعلق به K است، نتیجه می‌گیریم که α_1 در K قرار دارد و این تناقض است و بنابراین $[K(\alpha_1):K]\geq 2$. حال اگر $K(\alpha_1)=L$ که حکم ثابت می‌شود. اگر $K(\alpha_1)$ با L برابر نبود، یک عنصرِ α_2 در $L\setminus K(\alpha_1)$ در نظر بگیرید. در این صورت $K\subseteq K(\alpha_1)\subseteq K(\alpha_1,\alpha_2)\subseteq L$ و مشابهاً $[K(\alpha_1,\alpha_2):K(\alpha_1)]\geq 2$ که نتیجه می‌دهد

$$[L:K]\geq[K(\alpha_1,\alpha_2):K]=[K(\alpha_1,\alpha_2):K(\alpha_1)]\times[K(\alpha_1):K]=4.$$

چون $[L:K]$ متناهی است، پس این روند پس از انتخابِ $\alpha_1,\cdots,\alpha_n$ متوقف می‌شود و داریم $L=K(\alpha_1,\cdots,\alpha_n)$. $\square$

توسیع جدایی‌پذیر

تعریف ۲۸.۱. یک چندجمله‌ای تحویل‌ناپذیرِ $f\in K[x]$ را *جدایی‌پذیر*[1] روی K می‌نامیم هرگاه f در K^{cl} به عوامل درجه‌ی اول متمایز تجزیه شود؛ به بیان دیگر در K^{cl} ریشه‌ی تکراری نداشته باشد.

یک توسیع میدانی $K\subseteq L$ را جدایی‌پذیر می‌نامیم هرگاه هر عنصر $\alpha\in L\setminus K$ روی K جبری و چندجمله‌ای مینیمال آن روی K جدایی‌پذیر باشد. همچنین می‌گوییم یک میدان، *بسته‌ی جدایی‌پذیر* است هرگاه هیچ توسیع جدایی‌پذیری نداشته باشد.

[1] separable

توجه کنید که بوضوح هر توسیع جدایی‌پذیر لزوماً جبری است.

مثال ۲۹.۱. میدانِ $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ یک توسیع جدایی‌پذیر از $\mathbb{Q}$ است. زیرا هر عنصرِ $a + b\sqrt{2}$ در $\mathbb{Q}(\sqrt{2}) \setminus \mathbb{Q}$ ریشه‌ی چندجمله‌ای $x^2 - 2ax + a^2 - 2b^2$ است که این چندجمله‌ای به صورتِ $(x - a + b\sqrt{2})(x - a - b\sqrt{2})$ تجزیه می‌شود و بنابراین جدایی‌پذیر است.

لم ۳۰.۱. فرض کنید $K \subseteq L$ یک توسیع میدانی و $a \in L \setminus K$ ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیرِ $f(x)$ در $K[x]$ باشد. در این صورت، f چندجمله‌ای مینیمالِ a است.

اثبات. با برهان خلف فرض کنید f چندجمله‌ای مینیمالِ a نیست، یعنی چندجمله‌ای‌هایی در $K[x]$ وجود دارند به طوری که درجه‌ی آن‌ها از f کمتر و a ریشه‌ی آن‌ها است. از میان این چندجمله‌ها، یک چندجمله‌ای g با کمترین درجه را انتخاب می‌کنیم، پس بوضوح $\deg(g) < \deg(f)$ و $g(a) = 0$. حال اگر چندجمله‌ای f را بر g تقسیم کنیم، آن‌گاه طبق الگوریتم تقسیم داریم $f = gh + r$. از آنجا که $f(a) = g(a) = 0$، پس $r(a) = 0$ و چون $\deg(r) < \deg(g)$ با توجه به نحوه‌ی انتخابِ g نتیجه می‌شود که $r = 0$. از این رو $f = gh$ که این با تحویل‌ناپذیریِ f در تناقض است. □

لم ۳۱.۱. فرض کنید K یک میدان و f یک چندجمله‌ای ناصفر در $K[x]$ باشد. در این صورت، f در K^{cl} ریشه‌ی تکراری دارد اگروتنهااگر f و f' ریشه‌ی مشترک داشته باشند.

اثبات. فرض کنید $a \in K^{cl}$ یک ریشه‌ی تکراریِ f باشد. بنابراین $f = (x - a)^2 g$ که در آن $g \in K^{cl}[x]$. از این رو $f' = 2(x - a)g + g'(x - a)^2$، پس $f'(a) = 0$ یعنی a ریشه‌ی مشترک f و f' است.

برای اثبات جهت عکس، فرض کنید $a \in K^{cl}$ ریشه‌ی مشترکِ f و f' باشد. بنابراین داریم $f = (x - a)g$ و از این رو $f' = (x - a)g' + g$. از آنجا که a ریشه‌ی f' است، پس $x - a \mid g$. نهایتاً می‌توانیم نتیجه بگیریم که $(x - a)^2 \mid f$، به عبارت دیگر a ریشه‌ی تکراریِ f است. □

در لم بعدی می‌خواهیم نشان دهیم که در مشخصه‌ی صفر چندجمله‌ای‌های تحویل‌ناپذیر، جدایی‌پذیر هستند. به این منظور ابتدا تعریف مشخصه‌ی یک میدان را یادآوری می‌کنیم. فرض کنید $(K, +, \cdot, 0_K, 1_K)$ یک میدان باشد. اگر یک عدد طبیعیِ n وجود داشته باشد به طوری که $n \cdot 1_K = \underbrace{1_K + 1_K + \cdots + 1_K}_{n\text{بار}} = 0$، آن‌گاه می‌گوییم مشخصه‌ی میدانِ K برابر با n است و می‌نویسیم $\mathtt{char}(K) = n$. اگر هیچ nای وجود نداشته باشد به طوری که $n \cdot 1_K = 0$، آن‌گاه می‌گوییم مشخصه‌ی K، صفر است.

توجه کنید که اگر مشخصه‌ی یک میدانِ K ناصفر باشد، آن‌گاه مشخصه‌ی K حتماً یک عدد اول است. برای اثبات این گزاره با برهان خلف فرض کنید $m = s \cdot t$ که در آن $s, t \neq 1$ مشخصه‌ی میدانِ K باشد. در این صورت $m \cdot 1_K = (s \cdot 1_K)(t \cdot 1_K) = 0$ و بنابراین باید $(s \cdot 1_K) = 0$ یا $(t \cdot 1_K) = 0$؛ اما این تناقض است، زیرا m کوچکترین عدد طبیعی است که ویژگیِ $m \cdot 1_K = 0$ را دارد.

توجه ۳۲.۱. اگر K یک میدان باشد و $\mathtt{char}(K) = p$، آنگاه با توجه به اینکه به ازای هر $1 \leq i \leq p-1$ بوضوح $p \mid \binom{p}{i}$ پس به ازای هر $x, y \in K$ داریم $(x+y)^p = x^p + y^p$.

لم ۳۳.۱. اگر K یک میدان با مشخصه‌ی صفر باشد، آنگاه هر چندجمله‌ای تحویل‌ناپذیر، جدایی‌پذیر است.

اثبات. فرض کنید $f \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر باشد. در این صورت بنا به لم ۲۰.۱، f چندجمله‌ای مینیمال هر یک از ریشه‌هایش محسوب می‌شود. از آنجا که مشخصه‌ی میدانِ K برابر با صفر است، پس $\deg(f') < \deg(f)$ و بنابراین f و f' نمی‌توانند ریشه‌ی مشترک داشته باشند. در نتیجه بنا به لم ۳۱.۱، f ریشه‌ی تکراری ندارد و به عبارت دیگر f یک چندجمله‌ای جدایی‌پذیر است. $\square$

نتیجه ۳۴.۱. اگر مشخصه‌ی میدانِ K صفر باشد، آنگاه هر توسیع جبری یک توسیع جدایی‌پذیر است.

توجه ۳۵.۱. در مشخصه‌ی ناصفر یک چندجمله‌ای تحویل‌ناپذیر می‌تواند ریشه‌ی تکراری داشته باشد. برای مثال چندجمله‌ایِ $x^p - t$ در $\mathbb{F}_p(t)[x]$ را در نظر بگیرید که در آن منظور از $\mathbb{F}_p(t)$ میدانِ $\{\frac{f(t)}{g(t)} : f(t), g(t) \in \mathbb{F}_p[t]\}$ است. ابتدا می‌خواهیم نشان دهیم که این چندجمله‌ای تحویل‌ناپذیر است. به این منظور از تعمیم محک آیزنشتاین استفاده می‌کنیم که به شرح زیر است:

فرض کنید R میدان کسرهای دامنه‌ی تجزیه یکتای D و $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ یک چندجمله‌ای در $R[x]$ باشد، همچنین یک عنصر تحویل‌ناپذیر p در R موجود باشد به طوری که شروط زیر را برآورده می‌کند:

۱. عنصرِ p ضرایبِ a_i را به ازای $i = 0, 1, \ldots, n-1$ عاد کند.

۲. عنصرِ p ضریبِ a_n را عاد نکند.

۳. p^2 ضریبِ a_0 را عاد نکند.

در این صورت، می‌توان نتیجه گرفت که چندجمله‌ایِ $f(x)$ در $R[x]$ تحویل‌ناپذیر است.

ابتدا توجه کنید که $\mathbb{F}_p$ یک میدان است، پس بوضوح $\mathbb{F}_p[t]$ یک دامنه‌ی تجزیه‌ی یکتا است و در نتیجه $\mathbb{F}_p(t)$ میدان کسرهای یک دامنه‌ی تجزیه‌ی یکتاست. به سادگی می‌توان دید که برای چندجمله‌ای $x^p - t$ عنصرِ t سه شرط موجود در محک فوق را برآورده می‌کند، پس نتیجه می‌گیریم که چندجمله‌ای $x^p - t$ در $\mathbb{F}_p(t)[x]$ تحویل‌ناپذیر است.

حال فرض کنید α یک ریشه‌ی $x^p - t$ باشد. توسیعِ $\mathbb{F}_p(t)(\alpha)$ از $\mathbb{F}_p(t)$ را در نظر بگیرید. از آنجا که $\mathbb{F}_p \subseteq \mathbb{F}_p(t)(\alpha)$، پس مشخصه‌ی میدانِ $\mathbb{F}_p(t)(\alpha)$ نیز برابر با p است و بنابراین داریم

$$x^p - t = x^p - \alpha^p = (x-\alpha)^p$$

در نتیجه α ریشه‌ی تکراری $x^p - t$ است و از این رو چندجمله‌ایِ $x^p - t$ جدایی‌پذیر نیست.

در انتهای این فصل خواهیم دید که در میدان‌های متناهی، همانند میدان‌ها با مشخصه‌ی صفر، چندجمله‌ای‌های تحویل‌ناپذیر، جدایی‌پذیر هستند.

۲.۲.۱ میدان‌های متناهی

نماد گذاری ۳۶.۱. فرض کنید p یک عدد اول باشد. در ادامه میدان باقی‌مانده‌های اعداد صحیح به پیمانه‌ی p، یعنی میدان متشکل از عناصرِ $\{0, 1, \cdots, p-1\}$ با جمع و ضرب در پیمانهٔ p را با نمادِ $\mathbb{F}_p$ نشان می‌دهیم.

اندازه‌ی یک میدان متناهی

در این بخش، قصد داریم نشان دهیم که هر میدان متناهی دارای اندازه‌ای به صورتِ p^n است که در آن p یک عدد اول و n یک عدد طبیعی است. در راستای این کار، ابتدا لم زیر را ثابت می‌کنیم که یک نتیجه از قضیه‌ی لاگرانژ است. یادآوری می‌کنیم که قضیه‌ی لاگرانژ بیان می‌کند که اگر G یک گروه متناهی و H یک زیرگروه از آن باشد، آن‌گاه توان H توانِ G را عاد می‌کند.منظور از توان یک گروهِ H کوچکترین عدد طبیعیِ n با این ویژگی است که به ازای هر $a \in H$ داشته باشیم $na = 1$.

لم ۳۷.۱. فرض کنید $(G, +)$ یک گروه متناهی باشد و $n = | G |$. در این صورت برای هر $x \in G$ داریم $nx = 0$.

اثبات. زیرگروه دوری تولید شده توسطِ x را در نظر بگیرید. فرض کنید توان این زیرگروه برابر با m باشد. در این صورت قضیه‌ی لاگرانژ ایجاب می‌کند که $m|n$، پس یک عدد صحیح k وجود دارد به طوری که $n = km$. از طرفی، به سادگی می‌توان دید که توان زیرگروهِ $\langle x \rangle$ برابر با مرتبه‌ی عنصرِ x است، پس $mx = 0$ و بنابراین $nx = (km)x = 0$. □

نتیجه ۳۸.۱. فرض کنید K یک میدان متناهی باشد. در این صورت اندازه‌ی K به صورت یک p^n است که در آن p یک عدد اول و n یک عدد طبیعی است.

اثبات. بوضوح گروه جمعیِ K نیز متناهی است، پس بنا به لم فوق داریم $\underbrace{1 + 1 + \cdots + 1}_{\text{به اندازه‌ی میدان}} = 0$ و بنابراین یک عدد اول p وجود دارد به طوری که مشخصه‌ی میدانِ K برابر با p است. بوضوح هر میدان با مشخصه‌ی p شامل میدانِ $\mathbb{F}_p$ است؛ از این رو K یک توسیع میدانی از $\mathbb{F}_p$ و بنابراین یک فضای برداری روی میدانِ $\mathbb{F}_p$ است. با توجه به متناهی بودنِ K می‌توان نتیجه گرفت که $[K : \mathbb{F}_p]$ برابر با یک عدد طبیعیِ n است؛ یعنی فضای برداری K روی $\mathbb{F}_p$ یک پایه‌ی n عضوی دارد. بنابراین هر عنصر در K می‌تواند به صورت ترکیب خطی از عناصر این پایه با ضرایبی از $\mathbb{F}_p$ نوشته شود و از این نتیجه می‌شود که اندازه‌ی K برابر با p^n است. □

ساختن یک میدان متناهی

در بخش قبلی، نشان دادیم که اندازه‌ی هر میدان متناهی برابر است با یک p^n که در آن n یک عدد طبیعی و p یک عدد اول است. حال در این بخش، قصد داریم با طی چند گام به ازای هر p^n دلخواه، یک میدان متناهی به اندازه‌ی p^n بسازیم. خواهیم دید که میدان شکافنده‌ی چندجمله‌ایِ $x^{p^n}-x$ متعلق به $\mathbb{F}_p[x]$، میدان مطلوب ماست. منظور از میدان شکافنده‌ی چندجمله‌ای $x^{p^n}-x$ در $\mathbb{F}_p[x]$ کوچکترین میدان شامل $\mathbb{F}_p$ و همه‌ی ریشه‌های چندجمله‌ای $x^{p^n}-x$ است.

- **گام اول:** چندجمله‌ای $f=x^{p^n}-x$ متعلق به $\mathbb{F}_p[x]$ را در نظر بگیرید. فرض کنید $\mathbb{F}_p\subseteq K$ میدان شکافنده‌ی f باشد. می‌خواهیم نشان دهیم که f در K ریشه‌ی تکراری ندارد. با برهان خلف فرض کنید $\alpha\in K$ ریشه‌ی تکراریِ f باشد، بنابراین $f=(x-\alpha)^2g$ که در آن $g\in K[x]$. در این صورت، داریم $f'=2(x-\alpha)g+g'(x-\alpha)^2$ و در نتیجه $f'(\alpha)=0$. از طرفی چون $\mathbb{F}_p\subseteq K$، پس مشخصه‌ی K برابر با p است و بنابراین $f'=p^nx^{p^n-1}-1=-1\neq 0$ که این با نتیجه‌ی قبلی در تناقض است.

- **گام دوم:** در این گام نشان می‌دهیم که مجموعه‌ی E متشکل از ریشه‌های چندجمله‌ای $f=x^{p^n}-x$، یک میدان شاملِ $\mathbb{F}_p$ است. ابتدا نشان می‌دهیم که E یک میدان است. توجه کنید که بوضوح $1,0\in E$، پس کافی است نشان دهیم اگر $x,y\in E$ آنگاه xy^{-1} و $x-y$ نیز در E هستند. با توجه به اینکه مشخصه‌ی میدانِ K برابر با p است داریم $(x-y)^{p^n}=x^{p^n}-y^{p^n}$. از طرفی x و y در E قرار دارند، بنابراین $x^{p^n}=x$ و $y^{p^n}=y$، پس $(x-y)^{p^n}=x-y$ و در نتیجه $x-y\in E$. همچنین، $(xy^{-1})^{p^n}=x^{p^n}(y^{-1})^{p^n}$ و مشابهاً با توجه به اینکه $x,y\in E$ داریم $(xy^{-1})^{p^n}=xy^{-1}$، پس $xy^{-1}\in E$. حال می‌خواهیم نشان دهیم که E شاملِ $\mathbb{F}_p$ است. اگر $x\in\mathbb{F}_p$، آنگاه با توجه به قضیه‌ی کوچک فرما داریم $x^p=x$ و بنابراین $x^{p^n}=\underbrace{(x^p)^p\cdots)^p}_{n\text{بار}}=x$، این یعنی عناصرِ $\mathbb{F}_p$ نیز همگی ریشه‌ی چندجمله‌ای f هستند، پس $\mathbb{F}_p\subseteq E$.

- **گام سوم:** در این گام می‌خواهیم نشان دهیم که میدانِ K برابر با میدانِ E است؛ به عبارت دیگر میدان شکافنده‌ی f عنصر دیگری به غیر از ریشه‌های f ندارد. در گام دوم دیدیم که E که متشکل از ریشه‌های چندجمله‌ای f است، یک میدان است و $\mathbb{F}_p\subseteq E$. از طرفی از آنجا که K میدان شکافنده‌ی f است، پس کوچکترین میدان شامل $\mathbb{F}_p$ و همه‌ی ریشه‌های چندجمله‌ای f است و بنابراین به سادگی می‌توانیم نتیجه بگیریم که $K=E$ و نهایتاً $|K|=p^n$.

بنابراین تا اینجا نشان دادیم که اگر p یک عدد اول و n یک عدد طبیعی دلخواه باشد، آنگاه یک میدان متناهی با اندازه‌ی p^n موجود است.

نتیجه ۳۹.۱. فرض کنید K یک میدان متناهی باشد و $|K|=p^n$ که در آن p یک عدد اول و n یک عدد طبیعی است. در این صورت همه‌ی عناصر میدانِ K در معادله‌ی $x^{p^n}=x$ صدق می‌کنند.

اثبات. گروه ضربیِ $K^*=K\setminus\{0\}$ دارای p^n-1 عضو است. در نتیجه بنا به لمِ ۳۷.۱، برای هر عنصر ناصفرِ $a\in K$ داریم $a^{p^n-1}=1$، پس $a^{p^n}=a$. به عبارت دیگر، همه‌ی عناصر میدانِ K در معادله‌ی $x^{p^n}=x$ صدق می‌کنند، یعنی ریشه‌های متفاوت چندجمله‌ای $x^{p^n}-x$ هستند. $\square$

این بخش را با اثبات اینکه هر توسیع متناهی، یک توسیع ساده است به پایان می‌رسانیم.

لم ۴۰.۱. اگر n توان گروه متناهی و آبلی G باشد، آنگاه یک عنصرِ $a\in G$ وجود دارد به طوری که $\mathtt{ord}(a)=n$.

اثبات. به سادگی می‌توان دید که توان یک گروه متناهی برابر با ک.م.م مرتبه‌ی عناصر آن است. فرض کنید $n=p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ ک.م.م مرتبه‌ی همه‌ی عناصرِ G باشد. در این صورت، یک عنصرِ $a_1\in G$ موجود است به طوری که $p_1^{n_1}\mid\mathtt{ord}(a_1)$، یعنی $\mathtt{ord}(a_1)=p_1^{n_1}q_1$ و بنابراین $(a_1^{q_1})^{p_1^{n_1}}=1$، پس مرتبه‌ی عنصرِ $g_1=a_1^{q_1}$ برابر است با $p_1^{n_1}$. به طور مشابه عناصرِ $g_2,\cdots,g_k$ موجودند به طوری که $\mathtt{ord}(g_i)=p_i^{n_i}$. ادعا می‌کنیم که مرتبه‌ی عنصرِ $a=g_1g_2\cdots g_k$ برابر با n است. ابتدا توجه کنید که $(g_1g_2\cdots g_k)^n=(g_1g_2\cdots g_k)^{p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}}=1$. حال می‌خواهیم نشان دهیم که اگر به ازای یک عدد طبیعی دیگرِ m نیز داشته باشیم $(g_1g_2\cdots g_k)^m=1$، آنگاه $p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}\mid m$. به این منظور اثبات می‌کنیم که به ازای هر $0\le i\le k$ داریم $p_i^{n_i}\mid m$. به سادگی می‌توان نتیجه گرفت که $(g_1g_2\cdots g_k)^{mp_2^{n_2}\cdots p_k^{n_k}}=1$، یعنی $g_1^{mp_2^{n_2}\cdots p_k^{n_k}}(g_2\cdots g_k)^{mp_2^{n_2}\cdots p_k^{n_k}}=1$ و از آنجا که $(g_2\cdots g_k)^{mp_2^{n_2}\cdots p_k^{n_k}}=1$ نتیجه می‌گیریم که $g_1^{mp_2^{n_2}\cdots p_k^{n_k}}=1$. چون $\mathtt{ord}(g_1)=p_1^{n_1}$، پس $p_1^{n_1}\mid mp_2^{n_2}\cdots p_k^{n_k}$؛ اما p_1 نسبت به $p_2,\cdots,p_k$ اول است، بنابراین $p_1^{n_1}\mid m$. به طور مشابه برای سایر $p_i^{n_i}$ها داریم $p_i^{n_i}\mid m$ و در نتیجه $p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}\mid m$. $\square$

لم ۴۱.۱. اگر K یک میدان متناهی باشد، آنگاه گروه ضربیِ $K^*=K\setminus\{0\}$ دوری است.

اثبات. فرض کنید K یک میدان متناهی با p^n عضو باشد. در این صورت بوضوح $|K^*|=|K|-1=p^n-1$ و همچنین بنا بر نتیجه‌ی ۳۹.۱ گروهِ K^* متشکل از ریشه‌های ناصفرِ $x^{p^n}-x$ است.

حال فرض کنید e توان گروه ضربیِ K^* باشد؛ یعنی به ازای هر $x\in K^*$ داشته باشیم $x^e=1$. به بیان دیگر همه‌ی عناصر گروهِ K^* ریشه‌ی چندجمله‌ای x^e-1 هستند. اما این چندجمله‌ای حداکثر e تا ریشه دارد، پس $|K^*|\le e$. از طرفی طبق قضیه‌ی لاگرانژ توان یک گروه اندازه‌ی گروه را می‌شمارد، بنابراین $e\le|K^*|$ و در نتیجه $e=|K^*|$. از این رو e همان p^n-1 است. بنابراین با توجه به لم فوق یک عنصرِ a در K^* وجود دارد به طوری که $\mathtt{ord}(a)=p^n-1$ و چون K^* یک گروه ضربیِ p^n-1 عضوی است، پس K^* توسط عنصرِ a تولید می‌شود؛ یعنی دوری است. $\square$

قضیه ۴۲.۱. فرض کنید $K\subseteq L$ یک توسیع میدانی باشد به طوری که $[L:K]$ متناهی است. در این صورت، یک عنصر جبریِ α در $L\setminus K$ وجود دارد به طوری که $L=K(\alpha)$.

اثبات. اگر K متناهی باشد، آنگاه با توجه به اینکه L یک توسیع متناهی از K است نتیجه می‌شود که L نیز متناهی است. در این صورت بنا به لمِ ۴۱.۱ گروه ضربیِ L، یعنی $L \setminus \{0\}$ توسط یک عنصرِ $\alpha \in L$ تولید می‌شود و دوری است.

حال فرض کنید K نامتناهی باشد. در قضیه‌ی ۲۷.۱ دیدیم که اگر L یک توسیع متناهی از K باشد، آنگاه عناصرِ $\alpha_1, \alpha_2, \cdots, \alpha_n \in L \setminus K$ وجود دارند به طوری که $L = K(\alpha_1, \alpha_2, \cdots, \alpha_n)$. در ادامه، نشان می‌دهیم که اگر $L = K(\alpha, \beta)$، آنگاه یک عنصرِ γ وجود دارد به طوری که $K(\alpha, \beta) = K(\gamma)$. (برای حالتی که L برابر با $K(\alpha_1, \alpha_2, \cdots, \alpha_n)$ است به طور مشابه می‌توان اثبات کرد.) فرض کنید f و g به ترتیب چندجمله‌ای‌های مینیمالِ α و β روی K باشند به طوری که $\deg(g) = n$ و $\deg(f) = m$. همچنین فرض کنید $\{\alpha = \alpha_1, \cdots, \alpha_m\}$ و $\{\beta = \beta_1, \cdots, \beta_n\}$ به ترتیب ریشه‌های f و g باشند. حال چندجمله‌ای‌های $(\alpha - \alpha_i) + (\beta - \beta_j)x = 0$ را به ازای هر $i \leq i \leq 1$ و $n \geq j \leq 1$ در نظر بگیرید. از آنجا که K نامتناهی است، پس یک عنصرِ $\lambda \in K$ وجود دارد به طوری که ریشه‌ی هیچیک از چندجمله‌ای‌های فوق نیست. قرار دهید $\gamma := \alpha + \beta\lambda$. ادعا می‌کنیم که $K(\gamma) = K(\alpha, \beta)$.

توجه کنید که چون $\beta\lambda = \gamma - \alpha$، پس β یک ریشه‌ی مشترک از چندجمله‌ای‌های $g(x)$ و $f(\gamma - \lambda x)$ در $K(\gamma)[x]$ است. اگر ϵ یک ریشه‌ی مشترک دیگر این دو چندجمله‌ای در یک توسیعی از K باشد، آنگاه $g(\epsilon) = f(\gamma - \lambda\epsilon) = 0$ و بنابراین به ازای یک $1 \leq j \leq n$ داریم $\epsilon = \beta_j$ و به ازای یک $1 \leq i \leq m$ داریم $\gamma - \lambda\epsilon = \alpha_i$. در نتیجه $\alpha + \beta\lambda - \lambda\beta_j = \alpha + \lambda(\beta - \beta_j) = \alpha_i$، اما در این صورت $\alpha - \alpha_i + \lambda(\beta - \beta_j) = 0$ که این با نحوه‌ی انتخابِ λ در تناقض است. بنابراین $\gcd(g(x), f(\gamma - \lambda x)) = x - \beta$ و در نتیجه $x - \beta \in K(\gamma)[x]$، یعنی $\beta \in K(\gamma)$. از این رو $\alpha = \gamma - \beta\lambda$ نیز در $K(\gamma)$ قرار دارد و اینگونه نتیجه می‌شود که $K(\alpha, \beta) = K(\gamma)$. □

۳.۲.۱ میدان‌های کامل

همان‌طور که در توجه ۳۵.۱ دیدیم در مشخصه‌ی p لزوماً هر چندجمله‌ای تحویل‌ناپذیر، جدایی‌پذیر نیست. در این بخش به میدان‌هایی می‌پردازیم که در آن‌ها تحویل‌ناپذیری هر چندجمله‌ای معادل با جدایی‌پذیر بودن آن باشد.

تعریف ۴۳.۱. یک میدانِ K *کامل* [۲] نامیده می‌شود هرگاه هر چندجمله‌ای تحویل‌ناپذیر در $K[x]$، جدایی‌پذیر باشد.

توجه ۴۴.۱. با توجه به لمِ ۳۳.۱ هر میدان با مشخصه‌ی صفر، کامل است.

توجه ۴۵.۱. اگر f یک چندجمله‌ای تحویل‌ناپذیر در $K[x]$ باشد، آنگاه به ازای هر چندجمله‌ایِ $g \in K[x]$ یا $\gcd(f, g) = 1$ یا $\gcd(f, g) = f$.

قضیه ۴۶.۱. یک میدانِ K کامل است اگروتنهااگر یکی از موارد زیر برقرار باشد:

[2] perfect field

۱. $\mathtt{char}(K)=0$،

۲. $\mathtt{char}(K)=p$ و نگاشتِ $x\mapsto x^p$ یک اتومورفیسم روی K است.

اثبات. ابتدا می‌خواهیم نشان دهیم که اگر میدانِ K با مشخصه‌ی p کامل باشد، آنگاه نگاشتِ $x\mapsto x^p$ یک اتومورفیسم روی K است. با توجه به اینکه مشخصه‌ی میدانِ K برابر با p است، به سادگی می‌توان نشان داد که نگاشت فوق یک هومومورفیسم یک به یک است. برای اثبات پوشا بودن این نگاشت نشان خواهیم داد که برای هر $a\in K$ یک عنصرِ b در K وجود دارد به طوری که $b^p=a$. به این منظور یک عنصرِ a در K را در نظر بگیرید و قرار دهید $f=x^p-a$. چون مشخصه‌ی K برابر با p است، پس $f'=px^{p-1}=0$ و بنابراین با توجه به لمِ ۳۱.۱، چندجمله‌ایِ f ریشه‌ی تکراری دارد. اما K یک میدان کامل است، یعنی چندجمله‌ای‌های تحویل‌ناپذیر در $K[x]$، ریشه‌ی تکراری ندارند؛ پس نتیجه می‌گیریم که f یک چندجمله‌ای تحویل‌پذیر است و از این رو $f=gh$ که در آن $g,h\in K[x]$ و $\deg(g),\deg(h)<\deg(f)=p$. حال فرض کنید $b\in K^{cl}$ یک ریشه‌ی f باشد. در این صورت $b^p=a$ و با توجه به اینکه مشخصه‌ی میدانِ K برابر با p است، داریم

$$f=x^p-a=x^p-b^p=(x-b)^p=gh.$$

بنابراین $g=(x-b)^d$ که در آن $0<d<p$. از آنجا که $g\in K[x]$، پس ضرایب آن متعلق به K است و به ویژه $b^d\in K$. از طرفی، چون p یک عدد اول است، پس p و d نسبت به یکدیگر اول هستند و بنابراین اعداد صحیحِ u و v یافت می‌شوند به طوری که $du+pv=1$، در نتیجه $b=(b^d)^u(b^p)^v$. توجه کنید که چون b^p و b^d در K قرار دارند و K یک میدان است، پس توان‌های این دو نیز متعلق به K است، یعنی $(b^d)^u,(b^p)^v\in K$ و از این رو حاصل ضرب این دو عنصر، یعنی b در K است.

برای اثبات جهت عکس، با برهان خلف فرض کنید میدانِ K کامل نباشد. در این صورت، یک چندجمله‌ای تحویل‌ناپذیرِ $f=\sum_{i=0}^{n}a_ix^i$ در $K[x]$ وجود دارد به طوری که در K^{cl} دارای ریشه‌ی تکراری است، پس بنا به لمِ ۳۱.۱ f و f' ریشه‌ی مشترک دارند؛ اما f تحویل‌ناپذیر است و از آنجا که $\deg(f')\leq\deg(f)$ نتیجه می‌شود که $f'=0$. توجه کنید که $f'=\sum_{i=0}^{n}ia_ix^{i-1}=0$، یعنی به ازای هر i که $p\nmid i$ داریم $a_i=0$ و بنابراین $f=a_0+a_px^p+a_{2p}x^{2p}+\cdots$. با توجه به فرض، نگاشتِ $x\mapsto x^p$ اتومورفیسم است، پس پوشاست و در نتیجه هر یک از ضرایب چندجمله‌ای فوق برابر با b_i^p به ازای $b_i\in K$ است، از این رو $f=b_0^p+b_1^px^p+b_2^px^p+\cdots$. از آنجا که مشخصه‌ی میدانِ K برابر با p است، پس $f=b_0^p+b_1^px^p+b_2^px^p+\cdots=(b_0+b_1x+b_2x^2+\cdots)^p$ و این با تحویل‌ناپذیر بودنِ f در تناقض است. □

نتیجه ۴۷.۱. میدان‌های متناهی، کامل هستند.

اثبات. فرض کنید K یک میدان متناهی با اندازه‌ی p^n باشد. در این صورت مشخصه‌ی آن p است و همچنین عناصر آن ریشه‌های چندجمله‌ایِ $x^{p^n}-x$ هستند. ادعا می‌کنیم که نگاشتِ $x\mapsto x^p$ یک اتومورفیسم روی K است. از آنجا

که به ازای هر x در K داریم $x^{p^n}=x$، پس $(x^{p^{n-1}})^p=x$؛ به بیان دیگر نگاشتِ $x\mapsto x^p$ یک نگاشت پوشاست. با توجه به اینکه مشخصه‌ی میدانِ K برابر با p است، به سادگی می‌توان نتیجه گرفت که نگاشت مذکور یک همریختی یک به یک است و در نتیجه بنا به قضیه‌ی ۴۶.۱ میدانِ K کامل است. □

قضیه ۴۸.۱. یک میدانِ K کامل است اگروتنهااگر هر توسیع متناهی آن، یک توسیع جدایی‌پذیر باشد.

اثبات. فرض کنید K یک میدان کامل باشد. اگر $K\subseteq L$ یک توسیع متناهی باشد، آنگاه بنا به لمِ ۱۹.۱ یک توسیع جبری است و بنابراین هر عنصرِ a در $L\setminus K$ ریشه‌ی یک چندجمله‌ای تحویل‌ناپذیر در $K[x]$ است. از آنجا که K یک میدان کامل است، پس هر چندجمله‌ای تحویل‌ناپذیر، جدایی‌پذیر است. در نتیجه هر $a\in L\setminus K$ ریشه‌ی یک چندجمله‌ای جدایی‌پذیر در $K[x]$ است، از این رو L یک توسیع جدایی‌پذیر از K است.

برای اثبات جهت عکس، فرض کنید هر توسیع متناهی از میدانِ K، جدایی‌پذیر باشد. می‌خواهیم نشان دهیم که K یک میدان کامل است. به این منظور، یک چندجمله‌ای تحویل‌ناپذیرِ $f\in K[x]$ در نظر بگیرید. فرض کنید α یک ریشه‌ی f در K^{cl} باشد. حال میدان $L=K(\alpha)$ را در نظر بگیرید. بوضوح L یک توسیع متناهی از K است، پس بنا به فرض یک توسیع جدایی‌پذیر است و در نتیجه چندجمله‌ای مینیمالِ α در $K[x]$، یعنی f جدایی‌پذیر است. □

---

* خلاصه‌ی فصل:

در بخش مربوط به مقدمات منطقی، ابتدا یک زبان مرتبه‌ی اول را معرفی کردیم. یک زبان مرتبه اولِ $\mathcal{L}$ متشکل از نمادهای ثوابت، نمادهای تابعی و نمادهای رابطه‌ای است. برای یک زبانِ $\mathcal{L}$ به صورت استقرایی به ترتیب ترم‌ها و فرمول‌ها را تعریف کردیم. این ترم‌ها و فرمول‌ها در یک $\mathcal{L}$ ساختار تعبیر و معنا می‌شوند. منظور از یک $\mathcal{L}$ ساختارِ $\mathcal{M}$ یک مجموعه‌ی M به عنوان جهان $\mathcal{L}$ ساختار است که در آن به ازای هر نماد ثابتِ c در $\mathcal{L}$ یک عنصر مشخصِ $c^{\mathcal{M}}$ وجود دارد. همچنین، به ازای هر نماد تابعیِ n موضعیِ f یک تابعِ $f:M^n\to M$ و به ازای هر نماد رابطه‌ایِ R در زبان یک $R^{\mathcal{M}}$ روی M وجود دارد. منظورمان از $\mathcal{M}\models\varphi(a_1,a_2,\cdots,a_n)$ این است که اگر در فرمولِ $\varphi(x_1,x_2,\cdots,x_n)$ به جای متغیرهای $x_1,x_2,\cdots,x_n$ عناصرِ $a_1,a_2,\cdots,a_n\in M$ را جایگذاری کنیم، آنگاه $\varphi(a_1,a_2,\cdots,a_n)$ در ساختارِ $\mathcal{M}$ درست است.

در انتهای این بخش، با مفهوم تعریف‌پذیری یک مجموعه در یک $\mathcal{L}$ ساختار $\mathcal{M}$ آشنا شدیم و دیدیم که یک مجموعه‌ی $X\subseteq M$ (M جهان $\mathcal{L}$ ساختار $\mathcal{M}$ است) تعریف‌پذیر بدون پارامتر است هرگاه یک فرمول بدون پارامتر $\varphi(x)$ در یک زبان $\mathcal{L}$ وجود داشته باشد به طوری که $X=\{a\in M:\mathcal{M}\models\varphi(a)\}$.

در بخش بعدی به مقدمات جبری پرداختیم.

اگر K و L دو میدان باشند و $K\subseteq L$ آنگاه می‌گوییم L یک توسیع از میدانِ K است. اگر به ازای هر $a\in L\setminus K$ یک چندجمله‌ای تحویل‌ناپذیرِ f در $K[x]$ وجود داشته باشد به طوری که $f(a)=0$، آنگاه به این توسیع، توسیع

جبری می‌گوییم. همچنین وقتی می‌گوییم $K \subseteq L$ یک توسیع جدایی‌پذیر است، یعنی به ازای هر $a \in L \setminus K$ یک چندجمله‌ای جدایی‌پذیرِ f در $K[x]$ وجود دارد به طوری که $f(a) = 0$. منظور از یک چندجمله‌ای جدایی‌پذیر، چندجمله‌ای است که در K^{cl} ریشه‌ی تکراری ندارد. توجه کنید که اگر $K \subseteq L$، آنگاه L یک فضای برداری روی K است. حال اگر بُعد فضای برداری L روی K متناهی باشد می‌گوییم توسیعِ L از K متناهی است. نشان دادیم که هر توسیع متناهی، جبری است و به طور ویژه یک توسیع ساده است، یعنی یک عنصرِ $a \in L \setminus K$ وجود دارد به طوری که $L = K(a)$.

در قسمت بعدی این بخش، دیدیم که اندازه‌ی هر میدان متناهی به صورت یک p^n است که در آن p یک عدد اول و n یک عدد طبیعی است. چنین میدانی در واقع میدان متشکل از ریشه‌های چندجمله‌ای $x^{p^n} - x$ است. در نهایت با میدان‌های کامل آشنا شدیم. یک میدانِ K را کامل می‌نامیم هرگاه هر چندجمله‌ای تحویل‌ناپذیرِ f در $K[x]$ جدایی‌پذیر باشد. دیدیم که یک میدانِ K کامل است اگروتنهااگر یا مشخصه‌ی آن صفرباشد یا $\mathtt{char}(K) = p$ و $x \mapsto x^p$ یک اتومورفیسم روی K باشد. به علاوه، نشان دادیم که یک شرط معادل با کامل بودن یک میدان، این است که هر توسیع متناهی از آن یک توسیع جدایی‌پذیر باشد.

فصل ۲

حلقه‌های موضعی، نُرم‌دار و هنسلی

یکی از شروط میدان بودن، این است که تنها ایده‌آل ماکسیمال حلقه، ایده‌آل صفر باشد. شرط کمی ضعیفتر، این است که حلقه فقط یک ایده‌آل ماکسیمال داشته باشد؛ به چنین حلقه‌ای موضعی گفته می‌شود. در این فصل، به معرفی حلقه‌های موضعی و نُرم‌دار پرداخته و برخی از ویژگی‌های آن‌ها را بررسی می‌کنیم. یکی از مهم‌ترین لم‌هایی که در ادامه به آن می‌پردازیم، لم هنسل است که بیان می‌کند حلقه‌های موضعی و نرم‌دارِ کامل، هنسلی هستند؛ یعنی اگر R یک حلقه‌ی موضعی و نرم‌دار کامل و m تنها ایده‌آل ماکسیمال آن باشد، آن‌گاه هر چندجمله‌ای که یک ریشه‌ی ساده در R/m داشته باشد، در R نیز یک ریشه دارد(برای تعریف حلقه‌ی نرم‌دارِ کامل به ۱۵.۲ رجوع کنید). یکی از مثال‌های مهم حلقه‌های نرم‌دار هنسلی، حلقه‌ی p ـ ادیک‌ها است که در این فصل آن را معرفی می‌کنیم و به طور دقیق شالوده‌ی آن را شرح خواهیم داد.

مطالب این فصل از کتاب‌های [۲۱] و [۹] گردآوری شده است.

پیش از شروع بحث یک لم مقدماتی جبری که در ادامه به آن نیاز داریم را اثبات می‌کنیم:

لم ۱.۲. اگر R یک حلقه و I یک ایده‌آل ماکسیمال آن باشد، آن‌گاه $\frac{R}{I}$ یک میدان است.

اثبات. می‌خواهیم نشان دهیم که هر عنصر ناصفر در $\frac{R}{I}$ وارون ضربی دارد. به این منظور یک عنصر دلخواه و ناصفرِ $x + I$ در $\frac{R}{I}$ را در نظر می‌گیریم و نشان می‌دهیم که یک عنصرِ $y + I$ در $\frac{R}{I}$ وجود دارد به طوری که $(x+I)(y+I) = 1+I$، یعنی $xy + I = 1 + I$ یا به بیان دیگر $xy - 1 \in I$. ابتدا مجموعه‌ی $M = \{xr + s : r \in R, s \in I\}$ را در نظر بگیرید. به سادگی می‌توان دید که M یک ایده‌آل در R است که شاملِ I

می‌شود. توجه کنید که $x1_R + 0_R = x$ در M قرار دارد؛ اما چون $x + I$ یک عنصر ناصفر در $\frac{R}{I}$ است، پس $x \notin I$ و بنابراین $M \neq I$. از آنجا که I یک ایده‌آل ماکسیمالِ R است و $M \neq I$ نتیجه می‌گیریم که $M = R$. بنابراین 1_R متعلق به M است، یعنی عناصرِ $y \in R$ و $s \in I$ وجود دارند به طوری که $xy + s = 1_R$ و در نتیجه $xy - 1 \in I$. □

۱.۲ حلقه‌های موضعی

تعریف ۲.۲. یک حلقه‌ی جابه‌جایی و یکدارِ R را موضعی می‌نامیم هرگاه تنها یک ایده‌آل ماکسیمال داشته باشد. اگر m ایده‌آل ماکسیمالِ R باشد، آنگاه این حلقه را به صورت زوج (R, m) نمایش می‌دهیم. همچنین، میدانِ $k := R/m$ را *میدان پیمانه‌ها* می‌نامیم.

توجه ۳.۲. فرض کنید (R, m) یک حلقه‌ی موضعی باشد. به سادگی می‌توان بررسی کرد که نگاشت کانونیِ $h : R \to k$ که هر $x \in R$ را به $\bar{x} := x + m$ می‌برد، یک نگاشت همومورفیسم است.

نماد گذاری ۴.۲. فرض کنید R یک حلقه است. در این صورت عناصر وارون‌پذیرِ R را با $U(R)$ نشان می‌دهیم.

در قضیه‌ی زیر نشان می‌دهیم ایده‌آل ماکسیمال یک حلقه‌ی موضعی دقیقاً از عناصر وارون‌ناپذیر حلقه تشکیل شده است.

قضیه ۵.۲. اگر R یک حلقه‌ی جابه‌جایی و یکدار باشد، آنگاه موارد زیر با یکدیگر معادلند:

۱. R یک حلقه‌ی موضعی است،

۲. مجموعه‌ی عناصر وارون‌ناپذیر R تشکیل یک ایده‌آل ماکسیمال می‌دهند،

۳. مجموعه‌ی عناصر وارون‌ناپذیر R تحت عمل جمع بسته است.

اثبات. اثبات ۱ به ۲: فرض کنید R یک حلقه‌ی موضعی و m ایده‌آل ماکسیمال آن باشد. می‌خواهیم نشان دهیم که $m = R \setminus U(R)$. از آنجا که m یک ایده‌آل سره است، پس عناصر آن در R وارون ندارند و بنابراین $m \subseteq R \setminus U(R)$. حال یک عنصر دلخواهِ a در $R \setminus U(R)$ در نظر بگیرید. چون $a \notin U(R)$، پس ایده‌آلِ Ra در حلقه‌ی R سره است. از طرفی، هر ایده‌آل سره زیرمجموعه‌ی یک ایده‌آل ماکسیمال است و چون بنا به فرض، R تنها دارای یک ایده‌آل ماکسیمالِ m است، پس $Ra \subseteq m$. از آنجا که R یک حلقه‌ی یکدار است، پس از $Ra \subseteq m$ می‌توان نتیجه گرفت که $a \in m$، بنابراین $R \setminus U(R) \subseteq m$.

اثبات ۲ به ۳: چون $R \setminus U(R)$ یک ایده‌آل است، پس بوضوح تحت عمل جمع بسته است.

اثبات ۳ به ۱: فرض کنید برای هر $x, y \in R \setminus U(R)$ داریم $x + y \in R \setminus U(R)$. می‌خواهیم ثابت کنیم که $R \setminus U(R)$ یک ایده‌آل ماکسیمال است. فرض کنید $x \in R \setminus U(R)$ و $y \in R$. در این صورت ادعا می‌کنیم که

$x\cdot y\in R\setminus U(R)$. با برهان خلف فرض کنید $x\cdot y\in U(R)$ بنابراین نتیجه می‌شود که x وارون‌پذیر است و این تناقض است. تا اینجا نشان دادیم که $R\setminus U(R)$ یک ایده‌آلِ R است. همچنین، از آنجا که $U(R)$ متشکل از عناصر وارون‌پذیر است، پس نمی‌تواند شامل یک ایده‌آل ماکسیمال سره باشد، بنابراین $R\setminus U(R)$ تنها ایده‌آل ماکسیمال حلقه‌ی R است و در نتیجه R موضعی است. □

نتیجه ۶.۲. اگر (R,m) یک حلقه‌ی موضعی باشد، آن‌گاه به ازای هر $x\in R$ داریم یا $x\in U(R)$ یا $1+x\in U(R)$.

اثبات. با برهان خلف، فرض کنید یک عنصرِ x در R موجود باشد به طوری که همزمان $x\in R\setminus U(R)$ و $1+x\in R\setminus U(R)$. چون $x\in R\setminus U(R)$، پس $-x\in R\setminus U(R)$. بنا به قسمت ۳ قضیه‌ی ۵.۲ مجموعه‌ی عناصر وارون‌ناپذیر R تحت عمل جمع بسته اند، بنابراین $1+x-x=1\in R\setminus U(R)$ که این تناقض است، زیرا بوضوح 1 وارون‌پذیر است. □

توجه ۷.۲. اگر R یک حلقه‌ی موضعی باشد نمی‌توانیم نتیجه بگیریم که $R[x]$ موضعی است، زیرا در $R[x]$ عناصر $2x$ و $1-2x$ وارون ندارند؛ اما $1-2x+2x=1$ وارون دارد. بنابراین عناصر وارون‌ناپذیر نسبت به عمل جمع بسته نیستند و در نتیجه $R[x]$ موضعی نیست.

۱.۱.۲ حلقه‌های موضعی هنسلی

فرض کنید (R,m) یک حلقه‌ی موضعی و $k=\frac{R}{m}$ میدان پیمانه‌های آن باشد. اگر بخواهیم تصویر یک چندجمله‌ایِ $f(x)=a_0+a_1x+\cdots+a_nx^n$ متعلق به $R[x]$ را در $k[x]$ بدست بیاوریم کافی است هر ضریبِ f را با کلاس پیمانه‌ی متناظر آن جایگزین کنیم؛ به عبارت دیگر $\bar{f}(x)=\overline{a_0}+\overline{a_1}x+\cdots+\overline{a_n}x^n$.

می‌گوییم (R,m) یک حلقه‌ی هنسلی است هرگاه به ازای هر $f(x)\in R[x]$ اگر $\bar{f}$ در k ریشه‌ی ساده داشته باشد، آن‌گاه f در R ریشه داشته باشد.(رجوع به تعریفِ ۸.۲)

در این بخش، چند شرط معادل با ویژگی هنسلی را نیز بیان خواهیم کرد که در فصل ۵، مربوط به میدان‌های t ـ هنسلی، به آن‌ها نیاز خواهیم داشت. یکی از مزایای ویژگی هنسلی برای یک میدان، این است که معمولاً میدان پیمانه‌ها ساده‌تر از خود میدان است و در صورتی که این ویژگی در یک میدان برقرار باشد، کافی است برای بررسی بسیاری از مسائل جبری در یک میدان، به میدان پیمانه‌های آن توجه کنیم. لازم به ذکر است که حلقه‌های موضعی هنسلی، ساختارهایی هستند که در زبان حلقه‌ها، مدل یک تئوری مرتبه‌ی اول هستند. جملات چنین تئوری از موارد زیر تشکیل شده است:

۱. جمله‌ای که بیان کند مجموعه‌ی عناصر وارون‌پذیر حلقه تحت جمع بسته است. این جمله موضعی بودن حلقه را تضمین می‌کند.

۲. برای هر $n \geq 1$ جمله‌ای که شرط هنسلی بودن برای چندجمله‌ای‌های با درجه‌ی کمتر یا مساوی از n را بیان کند.

پیش از ادامه‌ی بحث تعریف دقیق هنسلی بودن را بیان می‌کنیم:

تعریف ۸.۲. فرض کنید (R, m) یک حلقه‌ی موضعی باشد. حلقه‌ی R *هنسلی* است هرگاه برای هر $f(x) \in R[x]$ اتفاق زیر رخ دهد:

اگر $\alpha \in R$ موجود باشد به طوری که $f(\alpha) \in m$ و $f'(\alpha) \notin m$، آنگاه یک عنصرِ a در R وجود داشته باشد به طوری که $f(a) = 0$ و $a \overset{m}{\equiv} \alpha$، یعنی $a - \alpha \in m$.

توجه ۹.۲. فرض کنید K یک میدان است. یک چندجمله‌ای $f(x) \in K[x]$ با درجه‌ی کمتر یا مساوی n را در نظر بگیرید. بسط تیلور چندجمله‌ایِ $f(x+y)$ در $K[x,y]$ به صورت زیر است:

$$f(x+y) = \sum_{i=0}^{n} f_{(i)}(x) \cdot y^i.$$

در عبارت فوق هر $f_{(i)}(x)$ در $K[x]$ قرار دارد و به این صورت است که $f_{(0)} = f$ و $f_{(1)} = f'$ و اگر $\mathtt{char}(R) = 0$ آنگاه $f_{(i)}(x) = f^{(i)}(x)/i!$ که در آن $f^{(i)}$ همان i ـ اُمین مشتق f است.

لم ۱۰.۲. فرض کنید (R, m) یک حلقه‌ی هنسلی و $\alpha \in R$ به گونه‌ای باشد که

$$f(\alpha) \in m \quad , \quad f'(\alpha) \notin m.$$

در این صورت **حداکثر** یک $a \in R$ می‌تواند وجود داشته باشد به طوری که $f(a) = 0$ و $a \overset{m}{\equiv} \alpha$؛ یعنی اگر $f(b) = 0$ و $b \overset{m}{\equiv} \alpha$، آنگاه $a = b$.

اثبات. فرض کنید دو عنصرِ b و a در R وجود دارند به طوری که $f(a) = f(b) = 0$ و $a \overset{m}{\equiv} \alpha \overset{m}{\equiv} b$؛ به بیان دیگر یک عنصرِ x در m وجود دارد به طوری که $b = a + x$. می‌خواهیم نشان دهیم که $a = b$. به این منظور در ادامه ثابت می‌کنیم که x برابر با صفر است. از آنجایی که $a \overset{m}{\equiv} \alpha$، پس هر توانی از α هم‌ارز با همان توان از a به پیمانه‌ی ایده‌آل m است، بنابراین $f'(a) \overset{m}{\equiv} f'(\alpha)$. پس از اینکه $f'(\alpha) \notin m$ نتیجه می‌شود که $f'(a) \notin m$، یعنی $f'(a)$ وارون‌پذیر است. حال بسط تیلورِ f را حول عنصرِ a تشکیل می‌دهیم و با توجه به وارون‌پذیریِ $f'(a)$ داریم:

$$f(a+x) = f(a) + f'(a)x + tx^2 = f'(a)x + tx^2 = f'(a)x[1 + f'(a)^{-1}tx]$$

توجه کنید که در عبارت فوق t متعلق به R است. چون m یک ایده‌آل است و $f'(a)^{-1}t \in R$، پس $f'(a)^{-1}tx \in m$؛ به عبارت دیگر $f'(a)^{-1}tx$ وارون‌ناپذیر است. بنابراین بنا به نتیجه‌ی ۶.۲، عنصرِ $1 + f'(a)^{-1}tx$ در $U(R)$ قرار دارد. در نتیجه از آنجا که $f'(a) \in U(R)$، پس $f'(a)[1 + f'(a)^{-1}tx]$ نیز متعلق به $U[R]$ است. از این رو $f(a+x) = 0$ اگروتنهااگر $x = 0$. □

لم ۱۱.۲. فرض کنید (R,m) یک حلقه‌ی موضعی باشد. در این صورت شرایط زیر معادلند:

۱. حلقه‌ی R هنسلی است،

۲. هر چندجمله‌ای $1+x+cd_2x^2+\cdots+cd_nx^n$ که در آن $n\geq 2$ و $c\in m$ و $d_1,\cdots,d_n\in R$، ریشه‌ای در $U(R)$ دارد،

۳. هر چندجمله‌ای $Y^n+Y^{n-1}+cd_2Y^{n-2}+\cdots+cd_n$ که در آن $n\geq 2$ و $c\in m$ و $d_1,\cdots,d_n\in R$، ریشه‌ای در $U(R)$ دارد،

۴. فرض کنید $f(x)\in R[x]$ و $\alpha\in R$ و $c\in m$ شرطِ $f(\alpha)=cf'(\alpha)^2$ را برآورده کنند. در این صورت یک عنصرِ a در R وجود دارد به طوری که $f(a)=0$ و $a\overset{cf'(\alpha)}{\equiv}\alpha$؛ یعنی $a-\alpha$ یک مضرب از $cf'(\alpha)$ است.

اثبات. اثبات ۱ به ۲: چندجمله‌ای $f(x)=1+x+cd_2x^2+\cdots+cd_nx^n$ را که $c\in m$ و $d_1,\cdots,d_n\in R$ در نظر بگیرید. برای $x=-1$ داریم $f(-1)=cd_2+\cdots+cd_n(-1)^n$. از آنجا که هر $cd_i\in m$، پس $f(-1)\overset{m}{\equiv}0$. به علاوه $f'(-1)=1+2cd_2+\cdots+ncd_n(-1)^{n-1}$، بنابرین $f'(-1)\overset{m}{\equiv}1$. چون R یک حلقه‌ی هنسلی است، پس $f(x)$ یک ریشه در $m+1-$ دارد که بنا به نتیجه‌ی ۶.۲ زیرمجموعه‌ای از $U(R)$ است.

اثبات معادل بودن ۲ و ۳ : کافی است در چندجمله‌ای دلخواهِ $g(Y)=Y^n+Y^{n-1}+cd_2Y^{n-2}+\cdots+cd_n$ به جای Y متغیر $1/x$ را جاگذاری کنیم، بنابراین مطابق با قسمت ۲ در همین لم چندجمله‌ای g یک ریشه در $U(R)$ دارد.

اثبات ۲ به ۴: فرض کنید $f(x)\in R[x]$ و $\alpha\in R$ و $c\in m$ شرطِ $f(\alpha)=cf'(\alpha)^2$ را برآورده کنند. بسط تیلورِ f را حول عنصر α و به ازای $x\in R$ در نظر بگیرید:

$$f(\alpha+x)=f(\alpha)+f'(\alpha)x+\sum_{i\geq 2}b_ix^i$$

توجه کنید که هر b_i در عبارت فوق در R قرار دارد. چون بنا به فرض $f(\alpha)=cf'(\alpha)^2$، پس داریم:

$$f(\alpha+x)=cf'(\alpha)^2+f'(\alpha)x+\sum_{i\geq 2}b_ix^i.$$

حال قرار دهید $x=cf'(\alpha)y$ که در آن $y\in R$، بنابراین

$$f(\alpha+cf'(\alpha)y)=cf'(\alpha)^2\Big[\underbrace{1+y+\sum_{i\geq 2}cd_iy^i}_{*}\Big]$$

که در آن $d_i\in R$. مطابق با قسمت ۲ در همین لم ، یک عنصرِ t در $U(R)$ وجود دارد به طوری که ریشه‌ی چندجمله‌ای $*$ باشد. بنابراین اگر a را برابر با $\alpha+cf'(\alpha)t$ در نظر بگیریم، آنگاه $f(a)=0$ و $a\overset{cf'(\alpha)}{\equiv}\alpha$.

اثبات ۴ به ۱: واضح است. □

۲.۲ حلقه‌های نُرم‌دار

در این بخش، قصد داریم برخی از حلقه‌ها که می‌توان بر روی آن‌ها یک نُرم تعریف کرد را معرفی کنیم. در دسته‌ای از این حلقه‌های نُرم‌دار، تمام دنباله‌های کوشی همگرا هستند؛ این نوع حلقه‌ها را "حلقه‌های نُرم‌دار کامل" می‌نامیم. در ادامه، پس از معرفی نُرم روی یک حلقه و حلقه‌های نُرم‌دار کامل، چند قضیه مربوط به آن‌ها را نیز اثبات خواهیم کرد.

تعریف ۱۲.۲. فرض کنید R یک حلقه‌ی جابه‌جایی و یکدار باشد. منظور از یک نُرم روی R تابعی به صورت $|.|: R \to \mathbb{R}^+$ است که برای هر $x, y \in R$:

۱. $|x|= 0$ اگروتنهااگر $x = 0$ و $|1|=|-1|= 1$.

۲. $|x + y| \leq |x|+|y|$.

۳. $|x \cdot y| \leq |x|\cdot|y|$.

اگر شرط زیر را جایگزین شرط دوم در تعریف فوق کنیم، آن‌گاه این نرم را *فرانرم* یا نرم *غیر ارشمیدسی* می‌نامیم.

۲*. $|x + y|\leq \max\{|x|, |y|\}$.

یک حلقه‌ی R همراه با یک نُرم $|.|$ روی آن را به صورت $(R, |.|)$ نمایش می‌دهیم.

توجه ۱۳.۲. برای هر $x \in R$ به سادگی می‌توان نتیجه گرفت که $|x|=|-x|$، بنابراین با داشتن یک نُرم روی حلقه‌ی R می‌توان آن را با متر $d(x, y) =|x - y|$ به یک فضای متریک تبدیل کرد.

تعریف ۱۴.۲. فرض کنید $(a_n)_{n\in\mathbb{N}}$ یک دنباله در حلقه‌ی نرم‌دارِ $(R, |.|)$ باشد. این دنباله را *کوشی* می‌نامیم هرگاه

$$\forall \epsilon > 0 \ \ \exists N \in \mathbb{N} \quad \forall m, n > N \ \ |a_m - a_n|< \epsilon.$$

تعریف ۱۵.۲. یک حلقه‌ی نُرم‌دار $(R, |.|)$ را *کامل* می‌نامیم هرگاه هر دنباله کوشی در آن همگرا باشد.

لم ۱۶.۲. فرض کنید حلقه‌ی R نسبت به نُرم غیر ارشمیدسیِ $|.|$ کامل باشد. در این صورت برای هر دنباله‌ی دلخواه $(a_n)_{n\in\mathbb{N}}$ در R داریم

$$\sum_{n=0}^{\infty} a_n \in R \iff \lim_{n\to\infty} |a_n|= 0.$$

اثبات. فرض کنید $\sum\limits_{n=0}^{\infty} a_n$ متعلق به R باشد. می‌خواهیم نشان دهیم که $\lim\limits_{n\to\infty} |a_n|= 0$. ابتدا قرار می‌دهیم $S_n = a_0 + a_1 + a_2 + \cdots + a_n$. از آنجا که $\lim\limits_{n\to\infty} S_n = \sum\limits_{n=0}^{\infty} a_n$ و بنا به فرض $\sum\limits_{n=0}^{\infty} a_n$ متعلق به R است، پس

$\lim\limits_{n\to\infty} S_{n+1} = \lim\limits_{n\to\infty} S_n$. در نتیجه $\lim\limits_{n\to\infty}(S_{n+1}-S_n) = \lim\limits_{n\to\infty} a_{n+1} = 0$ و بنابراین با توجه به ویژگی نُرم داریم $\lim\limits_{n\to\infty}|a_n|= 0$.

برای اثبات جهت عکس، فرض کنید $\lim\limits_{n\to\infty}|a_n|= 0$. در این صورت ادعا می‌کنیم $(S_n)_{n\in\mathbb{N}}$ یک دنباله‌ی کوشی است. برای هر $m, n \in \mathbb{N}$ به طوری که $m > n$ داریم $|S_m - S_n|=|a_{n+1} + a_{n+2} + \cdots + a_m|\leq \max\limits_{n+1\leq i\leq m}|a_i|$. از آنجا که حد $(|a_n|)_{n\in\mathbb{N}}$ صفر است، پس با توجه به نامساوی فوق نتیجه می‌گیریم که $(S_n)_{n\in\mathbb{N}}$ یک دنباله‌ی کوشی است. حال چون R یک حلقه‌ی کامل است، بنابراین دنباله‌ی $(S_n)_{n\in\mathbb{N}}$ در R همگرا است؛ یعنی $\lim\limits_{n\to\infty} S_n = \sum\limits_{n=0}^{\infty} a_n$ در R قرار دارد. $\square$

لم ۱۷.۲. فرض کنید $(R, |.|)$ یک حلقه‌ی نرم‌دار غیر ارشمیدسی باشد. اگر R یک حلقه‌ی کامل باشد و $a \in R$ به گونه‌ای باشد که $|a|< 1$، آنگاه $1 - a$ وارون‌پذیر است.

اثبات. اگر $|a|< 1$ باشد، آنگاه $\lim\limits_{n\to\infty}|a|^n= 0$. بنابراین، با توجه به لمِ ۱۶.۲، داریم $\sum\limits_{i=0}^{\infty} a^i \in R$. همچنین، از آنجایی که $\sum\limits_{i=0}^{\infty} a^i(1-a) = 1$ ، می‌توان نتیجه گرفت که $1 - a$ در حلقه‌ی R وارون‌پذیر است و وارون آن عنصرِ $\sum\limits_{i=0}^{\infty} a^i$ می‌باشد. $\square$

لم ۱۸.۲. فرض کنید $(R, |.|)$ یک حلقه‌ی نرم‌دار غیر ارشمیدسی و کامل باشد. اگر برای هر $x \in R$ داشته باشیم $|x|\leq 1$ آنگاه $M = \{x \in R : |x|< 1\}$ یک ایده‌آل سره است.

اثبات. ایده‌آل بودن مجموعه‌ی M به سادگی قابل بررسی است. برای اینکه ثابت کنیم M یک ایده‌آل سره است باید نشان دهیم که عناصر موجود در مجموعه‌ی M وارون‌ناپذیرند. با برهان خلف فرض کنید $x^{-1} \in R$ وارون یک عنصرِ x در M باشد، در این صورت $|xx^{-1}|=|1|= 1$. از طرفی، چون $|.|$ یک نرم غیر ارشمیدسی است، پس $|xx^{-1}|\leq|x|, |x^{-1}| < 1$ که با نتیجه قبلی در تناقض است. بنابراین عناصر موجود در M وارون‌ناپذیرند. $\square$

۱.۲.۲ لم هنسل

لم هنسل بیان می‌کند که حلقه‌های موضعی کامل، مثالی از حلقه‌های هنسلی هستند. ایده‌ی اثبات این لم به صورت زیر است:

فرض کنید (R, m) یک حلقه‌ی موضعی باشد که تحت نُرمِ $|.|$ کامل است. در ادامه اگر یک عنصر متعلق به ایده‌آل m باشد، آن را یک عنصر بسیار کوچک [1] تعبیر می‌کنیم. حال یک چندجمله‌ای $f(x)$ در $R[x]$ و یک عنصرِ α در R در نظر بگیرید به طوری که شروطِ $f(\alpha) \in m$ و $f'(\alpha) \notin m$ را برآورده کنند. در این صورت $f(\alpha)$ با توجه به تعبیر فوق، بسیار کوچک است. از اینکه $f'(\alpha) \notin m$ می‌توان نتیجه گرفت که $f'(\alpha)$ وارون‌پذیر است. خواهیم

[1] infinitesimals

دید که اگر $f(\alpha)\neq 0$ آن‌گاه می‌توانیم با به کارگیری روش نیوتون و استفاده از یک عنصر بسیار کوچکِ x مقدارِ $f(\alpha+x)$ را کوچکتر از $f(\alpha)$ کنیم، به بیان دیگر $|f(\alpha+x)|<|f(\alpha)|$. به این منظور، بسط تیلورِ f را حول عنصرِ α تشکیل می‌دهیم:

$$f(\alpha+x)=f(\alpha)+f'(\alpha)x+x^2(\cdots)+\cdots=f'(\alpha)(f'(\alpha)^{-1}f(\alpha)+x+x^2(\cdots)+\cdots).$$

حال قرار دهید $x=-f'(\alpha)^{-1}f(\alpha)$. از آنجا که $f(\alpha)\in m$ و m یک ایده‌آل است، پس $x\in m$، یعنی یک عنصر بسیار کوچک است. به علاوه داریم:

(۱.۲)

$$f(\alpha+x)=f'(\alpha)(f'(\alpha)^{-1}f(\alpha)-f'(\alpha)^{-1}f(\alpha)+(f'(\alpha)^{-1}f(\alpha))^2(\cdots)+\cdots)=f'(\alpha)[f(\alpha)^2 \text{ضریبی از}].$$

توجه کنید که در (۱.۲) عاملِ $f(\alpha)^2$ وجود دارد و بنا به فرض $f(\alpha)$ یک عنصر بسیار کوچک است، پس با انتخابِ x به صورت فوق $|f(\alpha+x)|$ از $|f(\alpha)|$ کوچکتر می‌شود. به این ترتیب مراحل فوق را برای $\alpha+x$ انجام می‌دهیم و با تکرار این روش به یک دنباله‌ی همگرا به یک عنصرِ a در R می‌رسیم به طوری که $f(a)=0$ و $a\overset{m}{\equiv}\alpha$. در ادامه خواهیم دید که یک نسخه دقیق‌تر از فرآیند نامتناهی فوق در اثبات لم هنسل به کار می‌رود.

لم ۱۹.۲. (لم هنسل). فرض کنید R یک حلقه‌ی کامل نسبت به نُرم غیر ارشمیدسیِ $|.|$ باشد و به ازای هر عنصرِ x در R داشته باشیم $|x|\leq 1$. اگر به ازای $f\in R[x]$ یک عنصرِ $\alpha\in R$ وجود داشته باشد به طوری که

$$|f(\alpha)|<1\ \ ,\ \ f'(\alpha)\in U(R)$$

آن‌گاه یک عنصر یکتای a در R وجود دارد به طوری که $f(a)=0$ و $|a-\alpha|<1$.

اثبات. می‌خواهیم یک دنباله‌ی $(a_i)_{i\in\mathbb{N}}$ در R بیابیم به طوری که به یک عنصر a در R همگرا باشد که این عنصر دو شرط $f(a)=0$ و $|a-\alpha|<1$ را برآورده می‌کند. به این منظور از روش درون‌یابی نیوتون استفاده می‌کنیم. ابتدا قرار می‌دهیم $a_0=\alpha$، پس بنا به فرض $|f(a_0)|<1 =:\epsilon$ و $f'(a_0)$ وارون‌پذیر است. سپس، قرار می‌دهیم $a_1=a_0-\frac{f(a_0)}{f'(a_0)}$. از آنجا که $|f'(a_0)|=1$ و $|f(a_0)|\leq\epsilon$، بنابراین $|a_1-a_0|=\frac{|f(a_0)|}{|f'(a_0)|}=|f(a_0)|\leq\epsilon$. در ادامه، برای سادگی $-\frac{f(a_0)}{f'(a_0)}$ را با h نشان می‌دهیم. حال بسط تیلورِ f را حولِ a_0 می‌نویسیم:

$$f(a_1)=f(a_0+h)=f(a_0)+f'(a_0)h+h^2 \text{مضربی از}.$$

چون $f(a_0)+f'(a_0)h=0$، پس

$$|f(a_1)|\leq\frac{|f(a_0)|^2}{|f'(a_0)|^2}|t|=|f(a_0)|^2|t|$$

که در آن t یک عنصر در R است. اما با توجه به فرض، نُرم همه‌ی عناصرِ R کمتر یا مساویِ 1 است، بنابراین $|t|\leq 1$ و در نتیجه $|f(a_1)|\leq|f(a_0)|^2\leq\epsilon^2$. حال ادعا می‌کنیم که $f'(a_1)$ وارون‌پذیر است. برای اثبات این ادعا، توجه کنید که چون $a_1-a_0=-\frac{f(a_0)}{f'(a_0)}$ و $f(a_0)$ وارون‌پذیر نیست، پس a_1-a_0 نیز وارون‌ناپذیر است؛ به بیان دیگر $a_0 \overset{R\setminus U(R)}{\equiv} a_1$. بنابراین $f'(a_0) \overset{R\setminus U(R)}{\equiv} f'(a_1)$ و بدین ترتیب از وارون‌پذیری $f'(a_0)$، وارون‌پذیری $f'(a_1)$ نیز نتیجه می‌شود.

در مرحله‌ی دوم قرار می‌دهیم $a_2=a_1-\frac{f(a_1)}{f'(a_1)}$. مشابه با مرحله‌ی قبل می‌توانیم نتیجه بگیریم که $|a_2-a_1|\leq\epsilon^2$ و $|f(a_2)|\leq\epsilon^4$. با تکرار این روش به یک دنباله‌ی $a_0,a_1,a_2,\cdots$ می‌رسیم که در آن به ازای هر n داریم $|a_{n+1}-a_n|\leq\epsilon^{2n}$، بنابراین این دنباله کوشی است. از آنجا که حلقه‌ی R کامل است، پس حد این دنباله در آن وجود دارد؛ به بیان دیگر $\lim_{n\to\infty}a_n=a\in R$. از طرفی، همان‌طور که دیدیم نُرم $f(a_n)$ در هر مرحله کوچکتر می‌شود، پس دنباله‌ی $(f(a_n))_{n\in\mathbb{N}}$ همگرا به صفر است. در نتیجه داریم:

$$f(a)=f(\lim_{n\to\infty}a_n)=\lim_{n\to\infty}f(a_n)=0.$$

همچنین، با توجه به اینکه به ازای هر n داریم $|a_n-\alpha|\leq\epsilon$، پس بوضوح $|a-\alpha|\leq\epsilon<1$. اثبات یکتا بودنِ a نیز دقیقاً مشابه لمِ ۱۰.۲ است. □

۲.۲.۲ حلقه‌ی متشکل از سری‌های توانی

همان‌طور که پیش‌تر اشاره شد، هدف اصلی این پایان‌نامه بررسی تعریف‌پذیری حلقه‌ی خاصِ $\mathbb{F}_q[[t]]$ در میدان $\mathbb{F}_q((t))$ است. در این بخش قصد داریم این حلقه و میدان را معرفی کنیم. به طور کلی اگر R یک حلقه‌ی دلخواه باشد، آنگاه حلقه‌ی متشکل از سری‌های توانی حول R را با نمادِ $R[[t]]$ نشان می‌دهیم؛ به بیان دیگر $R[[t]]$ برابر با $\{\sum\limits_{i=0}^{\infty}a_ix^i : a_i\in R\}$ است. همچنین میدان کسرهای $R[[t]]$ را با نمادِ $R((t))$ نشان می‌دهیم.

در فصل بعد، به بررسی سری‌های کلی‌تری می‌پردازیم که در آن‌ها اندیس‌ها متعلق به یک گروه مرتب آبلی دلخواه هستند. به طور دقیق‌تر، این سری‌ها به صورت ظاهریِ $\sum\limits_{\gamma\in\Gamma}a_\gamma t^\gamma$ نمایش داده می‌شوند که در آن Γ یک گروه مرتب آبلی است. در بخش ۳.۳ به طور مفصل درباره‌ی این سری‌ها صحبت خواهیم کرد.

نماد گذاری ۲۰.۲. اگر R یک حلقه باشد، آنگاه حلقه‌ی سری‌های توانی با متغیر x و ضرایب از R را با $R[[x]]$ نشان می‌دهیم؛ به بیان دیگر $R[[x]]:=\{\sum\limits_{i=0}^{\infty}a_ix^i : a_i\in R\}$.

لم ۲۱.۲. فرض کنید R یک حلقه باشد. در این صورت $\sum\limits_{i=0}^{\infty}a_ix^i\in R[[x]]$ وارون‌پذیر است اگروتنهااگر a_0 در R وارون‌پذیر باشد.

اثبات. فرض کنید $f=\sum\limits_{i=0}^{\infty}a_ix^i$ در $R[[x]]$ وارون‌پذیر باشد. در این صورت $g=\sum\limits_{i=0}^{\infty}b_ix^i$ در $R[[x]]$ وجود دارد به طوری که $(\sum\limits_{i=0}^{\infty}a_ix^i)(\sum\limits_{i=0}^{\infty}b_ix^i)=\sum\limits_{i=0}^{\infty}(\sum\limits_{k=0}^{i}a_kb_{i-k})x^i=1$، یعنی $a_0b_0=1$ و بنابراین a_0 وارون‌پذیر است.

برای اثبات جهت عکس، فرض کنید $f=\sum\limits_{i=0}^{\infty}a_ix^i$ و a_0 در R وارون‌پذیر است. می‌خواهیم یک چندجمله‌ای $g=\sum\limits_{i=0}^{\infty}b_ix^i$ در $R[[x]]$ بیابیم به طوری که $fg=1$، یعنی $fg=a_0b_0+(a_1b_0+a_0b_1)x+\cdots=1+0x+\cdots$. بنابراین باید $b_0a_0=1$ یا به عبارتی $b_0=a_0^{-1}$. همچنین، باید $a_1b_0+a_0b_1=0$، پس $b_1=\frac{-a_1b_0}{a_0}=-a_1a_0^{-2}$. به طور مشابه باید $a_2b_0+a_1b_1+a_0b_2=0$، بنابراین $b_2=\frac{-a_2b_0-a_1b_1}{a_0}=-a_2a_0^{-2}+a_1^2a_0^{-3}$. با تکرار روش فوق می‌توانیم تک تک b_iها را برحسب a_iها به دست می‌آوریم. $\square$

نتیجه ۲۲.۲. فرض کنید (R,m) یک حلقه‌ی موضعی باشد. در این صورت $R[[x]]$ یک حلقه‌ی موضعی است.

اثبات. بنا به لم ۲۱.۲، یک سری توانیِ $f(x)=r_0+r_1x+r_2x^2+\cdots$ در $R[[x]]$ وارون‌پذیر است اگروتنهااگر r_0 در R وارون‌پذیر باشد. در نتیجه مجموعه‌ی $M=\{a_0+r_1x+r_2x^2+\cdots : a_0\in m, r_i\in R\}$ متشکل از عناصر وارون‌ناپذیرِ $R[[x]]$ است. به سادگی می‌توان دید که M یک ایده‌آل در حلقه‌ی $R[[x]]$ است، پس بنا به قضیه‌ی ۵.۲، $(R[[x]],M)$ یک حلقه‌ی موضعی است. $\square$

توجه ۲۳.۲. اگر K یک میدان باشد، آنگاه $K[[t]]$ یک حلقه‌ی موضعی با ایده‌آل ماکسیمالِ $tK[[t]]$ است.

فرض کنید R یک حلقه‌ی غیر بدیهی باشد. ادعا می‌کنیم که یک نُرم روی $R[[x]]$ وجود دارد به طوری که $R[[x]]$ نسبت به آن کامل است. اثبات این ادعا به شرح زیر است:

۱. مرتبه‌ی هر عنصر $f=\sum\limits_{i=0}^{\infty}a_ix^i$ در $R[[x]]$ را به صورت زیر تعریف می‌کنیم:

$$\operatorname{ord}(f)=\begin{cases}\min(\{i: a_i\neq 0\}) & f\neq 0\\ \infty & f=0\end{cases}$$

توجه کنید که اندیس‌های یک سری توانیِ $\sum\limits_{i=0}^{\infty}a_ix^i$ متعلق به مجموعه $\mathbb{N}$ هستند که یک مجموعه‌ی خوش‌ترتیب است؛ به این معنی که هر زیرمجموعه‌ی اعداد طبیعی، عنصر می‌نیمم دارد. بنابراین، $\min(\{i: a_i\neq 0\})$ همواره وجود دارد.

۲. نشان می‌دهیم که روی حلقه‌ی $R[[x]]$ نگاشتِ $|f|:=2^{-\operatorname{ord}(f)}$ یک فرانُرم است. به این منظور کافی است ویژگی‌های یک فرانُرم در تعریفِ ۱۲.۲ را بررسی کنیم:

اولاً اگر $|f|=0$ آنگاه $2^{-\operatorname{ord}(f)}=0$، یعنی $\operatorname{ord}(f)=\infty$ که با توجه به نحوه‌ی تعریفِ $\operatorname{ord}(f)$ نتیجه می‌شود $f=0$. همچنین چون $\operatorname{ord}(1)=\operatorname{ord}(-1)=0$، پس داریم

$$|1|=2^{-\operatorname{ord}(1)}=2^{-\operatorname{ord}(-1)}=2^0=|-1|=1.$$

ثانیاً از آنجا که برای هر $f,g \in R[[x]]$ داریم $\min\{\operatorname{ord}(f), \operatorname{ord}(g)\} \leq \operatorname{ord}(f+g)$ و بنابراین

$$|f+g|= 2^{-\operatorname{ord}(f+g)} \leq 2^{-\min\{\operatorname{ord}(f),\operatorname{ord}(g)\}} = \max\{|f|, |g|\}.$$

ثالثاً چون $\operatorname{ord}(f)+\operatorname{ord}(g) \leq \operatorname{ord}(f\cdot g)$، پس $|f\cdot g|= 2^{-\operatorname{ord}(f\cdot g)} \leq 2^{-(\operatorname{ord}(f)+\operatorname{ord}(g))} =|f|\cdot|g|$.

۳. نهایتاً نشان می‌دهیم که حلقه‌ی $R[[x]]$ تحت این نُرم کامل است. فرض کنید $(f_n)_{n\in\mathbb{N}}$ یک دنباله‌ی کوشی در $R[[x]]$ باشد. ادعا می‌کنیم که حد این دنباله در $R[[x]]$ است.

اگر به ازای $m > n$ داشته باشیم $|f_m - f_n|< 2^{-N}$ آنگاه $\operatorname{ord}(f_m - f_n) > N$، یعنی ضرایب f_n و f_m تا قبل از توان N باهم برابرند؛ به بیان دیگر $f_n = a_0 + a_1x + \cdots + a_Nx^N + a_{N+1}x^{N+1} + \cdots$ و $f_m = a_0 + a_1x + \cdots + a_Nx^N + b_{N+1}x^{N+1} + \cdots$. حال چون بنا به فرض $(f_n)_{n\in\mathbb{N}}$ یک دنباله‌ی کوشی است، پس برای هر n و m به اندازه‌ی کافی بزرگ داریم $|f_m-f_n|< 2^{-N}$ و بنابراین مطابق توضیحات فوق ضرایب f_n و f_m تا قبل از توان Nـ اُم با هم برابرند. در ادامه i ـ اُمین ضریب در f_n را با $K_i(f_n)$ نشان می‌دهیم. تعریف می‌کنیم $a_i = \lim\limits_{n\to\infty} K_i(f_n)$ و این گونه $a_0, a_1, a_2, \cdots$ را به دست می‌آوریم و قرار می‌دهیم $f = \sum\limits_{i=0}^{\infty} a_ix^i$. بنا به نحوه‌ی تعریف f واضح است که $|f_n - f|\to 0$ و بنابراین دنباله‌ی $(f_n)_{n\in\mathbb{N}}$ همگرا به $f \in R[[x]]$ است.

نتیجه ۲۴.۲. اگر R یک حلقه باشد، آنگاه $R[[t]]$ یک حلقه‌ی هنسلی است.

اثبات. مشاهده کردیم که حلقه‌ی $R[[t]]$ با استفاده از نرمی که در بالا تعریف شده است، یک حلقه‌ی کامل است. از این رو، طبق لم هنسل، می‌توان نتیجه گرفت که $R[[t]]$ یک حلقه‌ی هنسلی است. $\square$

تعریف ۲۵.۲. میدان کسرهای حلقه‌ی $R[[t]]$ را با $R((t))$ نمایش می‌دهیم و آن را میدان *سری‌های لوران* می‌نامیم. می‌توان اثبات کرد که $R((t)) := \{\sum\limits_{i=-n}^{\infty} a_ix^i : n\in\mathbb{N}, a_i \in R\}$.

توجه کنید که اندیس‌های سری‌های موجود در $R((t))$ متعلق به $\mathbb{Z}$ هستند. در فصل بعدی یک حالت کلی تر را بررسی می‌کنیم که اندیس چنین سری‌هایی متعلق به یک گروه مرتب آبلیِ Γ باشد. این سری‌ها به صورتِ $\sum_{\gamma\in\Gamma} a_\gamma t^\gamma$ و با دو ویژگی مقابل هستند: اولاً $\{\gamma\in\Gamma : a_\gamma \neq 0\}$ یک مجموعه‌ی خوش‌ترتیب و ثانیاً a_γ به ازای هر $\gamma\in\Gamma$ متعلق به حلقه‌ی R است (برای تعریف خوش‌ترتیب به ۱۳.۳ رجوع کنید). مجموعه‌ی متشکل از چنین سری‌هایی را با نمادِ $R((t^\Gamma))$ نشان می‌دهیم. در لم ۲۲.۳ اثبات خواهیم کرد که $R((t^\Gamma))$ یک میدان است. واضح است که $R((t))$ یک حالت خاص از $R((t^\Gamma))$ هاست و بنابراین از این لم نیز میدان بودن $R((t))$ نتیجه می‌شود.

۳.۲ اعداد p ـ ادیک

۱.۳.۲ قدرمطلق p ـ ادیک

در این بخش یک قدرمطلق غیر ارشمیدسی روی میدان اعداد گویا معرفی می‌کنیم که قدرمطلق pـ ادیک نامیده می‌شود. این قدرمطلق مقدمه‌ی ساخت میدان و حلقه‌ی p ـ ادیک هاست که در بخش بعدی به آن خواهیم پرداخت. در پایان این بخش قضیه‌ای آورده‌ایم که بیان می‌کند هر قدرمطلقی روی $\mathbb{Q}$ معادل با یک قدرمطلق p ـ ادیک یا قدرمطلق طبیعی است.

در سرتاسر این فصل p یک عدد اول است.

تعریف ۲۶.۲. نگاشت $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ را با ضابطه‌ی زیر در نظر بگیرید:

۱. اگر $x \in \mathbb{Z} \setminus \{0\}$ آنگاه $v_p(x) = n$ به طوری که $x = p^n b$ که در آن $b \in \mathbb{Z}$ و $p \nmid b$.

۲. اگر $x \in \mathbb{Q} \setminus \{0\}$ آنگاه چون $x = \frac{a}{b}$ که در آن $a, b \in \mathbb{Z}$، پس تعریف می‌کنیم $v_p(x) = v_p(a) - v_p(b)$.

۳. $v_p(0) = \infty$.

نگاشت v_p را *ارزیابی p ـ ادیک* می‌نامیم.

توجه ۲۷.۲. فرض کنید p یک عدد اول باشد. به سادگی می‌توان دید که نگاشت $v_p : \mathbb{Q} \to \mathbb{Z}$ با ضابطه‌ی معرفی شده در تعریف فوق، برای هر $x, y \in \mathbb{Q}$ دارای ویژگی‌های زیر است:

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

۲. $v_p(xy) = v_p(x) + v_p(y)$،

۳. $v_p(1) = 0$.

تعریف ۲۸.۲. نگاشت $|.|_p : \mathbb{Q} \to \mathbb{R}^+$ با ضابطه‌ی

$$\begin{cases} |x|_p = 2^{-v_p(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

قدرمطلقِ p ـ ادیک نامیده می‌شود.

لم ۲۹.۲. قدرمطلقِ p ـ ادیک، $|.|_p$، یک قدرمطلق غیر ارشمیدسی روی میدان $\mathbb{Q}$ است.

اثبات. برای هر $x, y \in \mathbb{Q}$ داریم:

۱. اگر $x=0$ آن‌گاه بنا به تعریف ۲۸.۲، $|x|_p=0$. حال فرض کنید $x\neq 0$، بنابراین $|x|_p=2^{-v_p(x)}\neq 0$. به علاوه $v_p(1)=v_p(-1)=0$، پس $|1|_p=|-1|_p=2^0=1$.

۲. بنا به توجه ۲۷.۲ داریم $v_p(xy)=v_p(x)+v_p(y)$، بنابراین

$$|xy|_p=2^{-v_p(xy)}=2^{-(v_p(x)+v_p(y))}=2^{-v_p(x)}2^{-v_p(y)}=|x|_p|y|_p$$

۳. بدون کاستن از کلیت فرض کنید $|x|_p\geq|y|_p$. در این صورت $v_p(y)\geq v_p(x)$. بنابراین بنا به توجه ۲۷.۲ داریم $v_p(x+y)\geq\min\{v_p(x),v_p(y)\}=v_p(x)$، پس $|x+y|_p=2^{-v_p(x+y)}\leq 2^{-v_p(x)}=\max\{|x|_p,|y|_p\}$.

□

قضیه‌ی ۳۲.۲ که از کتاب [۹] آورده شده است، اهمیت قدرمطلق p ـ ادیک را بیشتر نمایان می‌کند. با توجه به آن تنها دو قدرمطلق روی $\mathbb{Q}$ داریم یکی قدرمطلقی که در تعریفِ ۳۱.۲ آورده‌ایم و دیگری به صورت یک قدرمطلق p ـ ادیک. از اثبات این قضیه در این پایان‌نامه چشم پوشیده‌ایم اما خواننده می‌تواند آن را در صفحه‌ی ۵۷ تا۵۹ منبع مذکور مطالعه کند.

تعریف ۳۰.۲. دو قدرمطلق روی یک میدان معادل هستند هرگاه توپولوژی یکسانی روی میدان القاء کنند.

راجع به توپولوژی القاء شده روی یک میدان توسط یک نگاشت قدرمطلق در بخشِ ۲.۱.۴ به تفصیل توضیح داده شده است.

تعریف ۳۱.۲. نگاشتِ

$$|x|_\infty=\begin{cases} x & x\geq 0\\ -x & x<0\end{cases}$$

قدرمطلق طبیعی روی $\mathbb{Q}$ نامیده می‌شود.

قضیه ۳۲.۲. هر قدرمطلق غیر بدیهی روی $\mathbb{Q}$ یا معادل است با یکی از قدرمطلق‌های p ـ ادیک یا قدرمطلق طبیعی.

اثبات. به کتابِ [۹] رجوع کنید. □

همان‌طور که در لم قبل نشان دادیم، قدرمطلق p ـ ادیک بر روی اعداد گویا غیر ارشمیدسی است. همچنین، با سادگی می‌توان مشاهده کرد که قدرمطلق ۳۱.۲ یک قدرمطلق ارشمیدسی بر روی اعداد گویا است. بنابراین، یک نتیجه از قضیه فوق این است که قدرمطلق p ـ ادیک تنها قدرمطلق غیر ارشمیدسی بر روی اعداد گویا است.

۲.۳.۲ ساختن $\hat{\mathbb{Q}}_p$

می‌دانیم که میدانِ $\mathbb{R}$ کامل شده‌ی $\mathbb{Q}$ نسبت به قدرمطلق طبیعی است. همان‌طور که در قضیه‌ی ۲۸.۲ بیان کردیم، علاوه بر قدرمطلق طبیعی، یک قدرمطلق دیگر به صورت قدرمطلق p ـ ادیک نیز روی $\mathbb{Q}$ وجود دارد. طبیعی است که از خود بپرسیم کامل شده‌ی اعداد گویا نسبت به قدرمطلق p ـ ادیک چیست؟ در این بخش به این سوال پاسخ داده‌ایم.

قضیه ۳۳.۲. میدان اعداد گویا تحت نُرمِ p ـ ادیک کامل نیست.

اثبات. به صفحه‌ی ۶۳ کتابِ [۹] مراجعه کنید. □

از آنجا که $\mathbb{Q}$ نسبت به $|.|_p$ کامل نیست، پس می‌توانیم کامل شده‌ی آن نسبت به این نگاشت قدرمطلق را تشکیل دهیم. برای این کار، باید حد همه‌ی دنباله‌های کوشی را به $\mathbb{Q}$ اضافه کنیم.

تعریف ۳۴.۲. کامل شده‌ی $\mathbb{Q}$ نسبت به نُرم p ـ ادیک را *میدانِ p ـ ادیک* می‌نامیم و با $\hat{\mathbb{Q}}_p$ نمایش می‌دهیم.

توجه ۳۵.۲. بنا به قضیه‌ی ۳۲.۲، اعداد حقیقی و $\hat{\mathbb{Q}}_p$ تنها میدان‌های کامل شده‌ی اعداد گویا هستند.

۳.۳.۲ ساختن $\hat{\mathbb{Z}}_p$

از آنجا که هر عدد صحیح حداقل یک فاصله از یک عدد صحیح دیگر دارد، بنابراین با نُرم طبیعی دنباله‌های ثابت (یا دنباله‌هایی از یک جایی به بعد ثابت می‌شوند) تنها دنباله‌های کوشی در حلقه‌ی $\mathbb{Z}$ هستند. بوضوح حد چنین دنباله‌هایی یک عدد صحیح است، پس حلقه‌ی اعداد صحیح تحت قدرمطلق طبیعی یک حلقه‌ی کامل است. اما تحت نُرم p ـ ادیک اعداد صحیح می‌توانند به اندازه‌ی دلخواه به یکدیگر نزدیک شوند، بنابراین دنباله‌های کوشی غیر ثابت نیز وجود دارند. در این بخش حلقه‌ای را معرفی می‌کنیم که کامل شده‌ی اعداد صحیح تحت نُرم p ـ ادیک است و چند ویژگی از آن را بررسی می‌کنیم. چنین حلقه‌ای را حلقه‌ی اعداد صحیح pـ ادیک می‌نامیم و آن را با $\hat{\mathbb{Z}}_p$ نشان می‌دهیم.

تعریف ۳۶.۲. برای یک عدد اول p، کامل شده‌ی حلقه‌ی $\mathbb{Z}$ نسبت به نُرم $|.|_p$ را با $\hat{\mathbb{Z}}_p$ نمایش می‌دهیم و آن را *حلقه‌ی p ـ ادیک* می‌نامیم.

لم ۳۷.۲. هر عنصر a در $\hat{\mathbb{Z}}_p$ دارای نمایش یکتا به صورت $\sum_{i=0}^{\infty} b_i p^i$ است به طوری که به ازای هر اندیسِ i داریم $b_i \in \{0, 1, \cdots, p-1\}$.

اثبات. فرض کنید a یک عنصر در $\hat{\mathbb{Z}}_p$ باشد. در این صورت بنا به تعریفِ ۳۶.۲، یک دنباله‌ی کوشیِ $(a_n)_{n\in\mathbb{N}}$ در $\mathbb{Z}$ وجود دارد به طوری که به a همگراست. از آنجا که $(a_n)_{n\in\mathbb{N}}$ یک دنباله‌ی کوشی است، پس برای هر عدد طبیعیِ t یک عدد طبیعیِ N_t وجود دارد به طوری که برای هر $n, m > N_t$ داریم $|a_n - a_m|_p < 2^{-t}$. بنابراین با توجه به نحوه‌ی تعریف این نُرم داریم $v_p(a_n - a_m) > t$، یعنی $a_n \overset{p^t}{\equiv} a_m$.

حال برای به دست آوردن ضرایب سری مورد نظرمان به صورت زیر عمل می‌کنیم:

۱. بنا به توضیحات فوق، به ازای عدد 1 یک عدد طبیعیِ N_1 وجود دارد به طوری که به ازای هر $n, m > N_1$ داریم $a_n \overset{p}{\equiv} a_m \overset{p}{\equiv} b_0$ و بوضوح $b_0 \in \{0, 1, 2, \cdots, p-1\}$.

۲. به طور مشابه به ازای عددِ 2 یک عدد طبیعیِ N_2 وجود دارد به طوری که به ازای هر $n, m > N_2$ داریم $a_n \overset{p^2}{\equiv} a_m \overset{p^2}{\equiv} \alpha_1$. در این صورت $\alpha_1 \in \{0, 1, 2, \cdots, p^2-1\}$. از آنجا که $N_1 \leq N_2$، پس همه‌ی a_nها که $n > N_2$ نیز به پیمانه‌ی p برابر با b_0 می‌شوند، پس داریم $\alpha_1 = b_0 + b_1 p$.

به همین طریق سایر α_iها را به دست می‌آوریم و نهایتاً سری $\sum\limits_{i=0}^{\infty} b_i p^i$ نمایش یکتای a خواهد بود.

$\square$

لم ۳۸.۲. حلقه‌ی $\hat{\mathbb{Z}}_p$ یک حلقه‌ی موضعی هنسلی با ایده‌آل ماکسیمال $p\hat{\mathbb{Z}}_p$ است.

اثبات. برای اینکه اثبات کنیم $(\hat{\mathbb{Z}}_p, p\hat{\mathbb{Z}}_p)$ یک حلقه‌ی موضعی است به صورت زیر عمل می‌کنیم:

۱. ابتدا نشان می‌دهیم که یک عنصر در $\hat{\mathbb{Z}}_p$ وارون‌پذیر است اگروتنهااگر $|x|_p = 1$.

فرض کنید $x = \sum\limits_{i=0}^{\infty} a_i p^i$ یک عنصر در $\hat{\mathbb{Z}}_p$ باشد به طوری که $|x|_p = 1$. در این صورت $p \nmid a_0$، یعنی a_0 در $\mathbb{F}_p = \{1, \cdots, p-1\}$ قرار دارد. حال از آنجا که $\mathbb{F}_p$ یک میدان است و $a_0 \in \mathbb{F}_p \in \{0\}$، پس یک عنصرِ b در $\mathbb{F}_p$ وجود دارد به طوری که وارونِ a_0 است. بنابراین یک عدد صحیحِ q وجود دارد به طوری که $a_0 b = pq + 1$. در نتیجه داریم:

$$xb = a_0 b + b\sum_{i=1}^{\infty} a_i p^i = 1 + pq + b\sum_{i=1}^{\infty} a_i p^i.$$

بوضوح $|pq + b\sum\limits_{i=0}^{\infty} a_i p^i|_p < 1$، پس بنا به لم ۱۷.۲ عنصر xb در $\hat{\mathbb{Z}}_p$ وارون‌پذیر و بنابراین x در $\hat{\mathbb{Z}}_p$ وارون‌پذیر است.

برای اثبات جهت عکس، فرض کنید یک عنصرِ $a = \sum\limits_{i=0}^{\infty} a_i p^i$ در $\hat{\mathbb{Z}}_p$ وارون‌پذیر باشد. در این صورت یک عنصرِ $\sum\limits_{i=0}^{\infty} b_i p^i$ در $\hat{\mathbb{Z}}_p$ وجود دارد به طوری که $(\sum\limits_{i=0}^{\infty} a_i p^i)(\sum\limits_{i=0}^{\infty} b_i p^i) = \sum\limits_{i=0}^{\infty}(\sum\limits_{k=0}^{i} a_k b_{i-k})p^i = 1$. در نتیجه $a_0 b_0 = 1$، پس a_0 در $\mathbb{F}_p$ وارون‌پذیر است، بنابراین $a_0 \neq 0$ و از این نتیجه می‌شود که $|a|_p = 1$.

۲. بنا به لم ۱۸.۲، ایده‌آل $M=\{x\in R:|x|_p<1\}=p\hat{\mathbb{Z}}_p$ یک ایده‌آل سره است. از طرفی بنا به توضیحات فوق، M شامل همه‌ی عناصر وارون‌ناپذیر است و در نتیجه طبق لم ۵.۲، $(\hat{\mathbb{Z}}_p, p\hat{\mathbb{Z}}_p)$ یک حلقه‌ی موضعی است.

همچنین از آنجا که $\hat{\mathbb{Z}}_p$ یک حلقه‌ی موضعی کامل است، پس بنا به لم هنسل یک حلقه‌ی هنسلی است.

□

توجه ۳۹.۲. نگاشتِ $\varphi:\hat{\mathbb{Z}}_p\to\mathbb{F}_p$ را در نظر بگیرید که یک عنصر دلخواهِ $a_0+a_1p+a_2p^2+\cdots$ در $\hat{\mathbb{Z}}_p$ که در آن $a_i\in\{0,1,\cdots,p-1\}$ است را به a_0 می‌برد. به سادگی می‌توان بررسی کرد که این نگاشت یک همریختی پوشاست و $\ker(\varphi)=p\hat{\mathbb{Z}}_p$، پس بنا به قضیه‌ی اول یکریختی داریم $\hat{\mathbb{Z}}_p/p\hat{\mathbb{Z}}_p\cong\mathbb{F}_p$. بنابراین میدان پیمانه‌های حلقه‌ی موضعی p ـ ادیک برابر با $\mathbb{F}_p$ است.

لم ۴۰.۲. اگر x یک عنصر ناصفر در $\hat{\mathbb{Q}}_p$ باشد، آنگاه $x=p^ku$ به طوری که u یک عنصر وارون‌پذیر در $\hat{\mathbb{Z}}_p$ و k یک عدد صحیح است.

اثبات. این قضیه را در چند مرحله‌ی زیر اثبات می‌کنیم:

۱. فرض کنید x یک عنصر ناصفر در $\hat{\mathbb{Q}}_p$ باشد. در این صورت با توجه به تعریف $\hat{\mathbb{Q}}_p$ نتیجه می‌گیریم که x حد یک دنباله‌ی کوشی از اعضای $\mathbb{Q}$ مانندِ $(x_i)_{i\in\mathbb{N}}$ است. می‌دانیم که هر عدد گویای x_i را می‌توان به صورت $\frac{m_i}{n_i}$ نوشت که در آن $m_i,n_i\in\mathbb{Z}$. حال تمام توان‌های p را از صورت و مخرج کسرِ $\frac{m_i}{n_i}$ فاکتور بگیرید، پس $\frac{m_i}{n_i}=p^k\frac{a'_i}{b'_i}$ به طوری که $p\nmid a'_i$ و $p\nmid b'_i$ و $k\in\mathbb{Z}$.

۲. اگر اعداد صحیح a' و b' را در مبنای p، یعنی به صورت $a'=a_0+a_1p+a_2p^2+\cdots+a_np^n$ و $b'=b_0+b_1p+b_2p^2+\cdots+b_np^m$ بنویسیم، آنگاه چون $p\nmid a'_i$ و $p\nmid b'_i$، پس $a_0\neq 0$ و $b_0\neq 0$ و $a_i\in\{1,\cdots,p-1\}$. توجه کنید که چون $a',b'\in\mathbb{Z}$ پس $n,m<\infty$. از طرفی می‌دانیم که $\mathbb{Z}\subseteq\hat{\mathbb{Z}}_p$، در نتیجه $a',b'\in\hat{\mathbb{Z}}_p$ و چون $a_0\neq 0$ و $b_0\neq 0$، پس $|a'|_p=|b'|_p=1$. دراثبات لم ۳۸.۲ دیدیم که عناصر وارون‌پذیر حلقه‌ی $\hat{\mathbb{Z}}_p$ عناصری هستند که قدرمطلق p ـ ادیک آن‌ها برابر با 1 شود، بنابراین a' و b' در $\hat{\mathbb{Z}}_p$ وارون‌پذیر هستند، از این رو $\frac{a'}{b'}$ نیز در $\hat{\mathbb{Z}}_p$ وارون‌پذیر است.

تا اینجا نشان دادیم که هر x_i در دنباله‌ی $(x_i)_{i\in\mathbb{N}}$ را می‌توان به صورت p^ku_i نوشت که در آن u یک عنصر وارون‌پذیر در $\hat{\mathbb{Z}}_p$ و k یک عدد صحیح است و بنابراین

$$p^{k_1}u_1 \quad p^{k_2}u_2 \quad p^{k_3}u_3 \quad \cdots\to x.$$

۳. از آنجا که هر u_i در $\hat{\mathbb{Z}}_p$ وارون‌پذیر است، پس $|u_i|_p=1$ و در نتیجه $|p^{k_i}u_i|_p=|p^{k_i}|_p|u_i|_p=2^{-k_i}$. از طرفی نُرم x برابر با حد نُرم x_iها است و چون x ناصفر است، پس نُرم x_iها از یک اندیسی به بعد به صورت 2^{-k} باقی می‌ماند و کمتر نمی‌شود. به بیان دیگر، x_iها از یک اندیسی به بعد همگی به صورت $p^k u_i$ هستند. با توجه به اینکه دنباله‌ی $(x_i)_{i\in\mathbb{N}}$ کوشی است و $\hat{\mathbb{Z}}_p$ یک حلقه‌ی کامل است، پس $\lim\limits_{i\to\infty} u_i = u$ متعلق به $\hat{\mathbb{Z}}_p$ است. بنابراین $x = \lim\limits_{i\to\infty} p^k u_i = p^k \lim\limits_{i\to\infty} u_i = p^k u$ که در آن $u \in \hat{\mathbb{Z}}_p$.

□

لم ۴۱.۲. هر عنصر a متعلق به $\hat{\mathbb{Q}}_p$ دارای نمایش یکتا به صورت $\sum\limits_{i=n}^{\infty} a_i p^i$ است به طوری که $n \in \mathbb{Z}$ و $a_i \in \{0, 1, \cdots, p-1\}$.

اثبات. در لم ۴۰.۲ نشان دادیم که هر عنصر در $\hat{\mathbb{Q}}_p$ به صورت $x = p^k u$ نوشته می‌شود به طوری که u یک عنصر وارون‌پذیر در $\hat{\mathbb{Z}}_p$ است. حال با توجه به لم ۳۷.۲ داریم $u = a_0 + a_1 p + a_2 p^2 + \cdots$، پس $x = a_0 p^k + a_1 p^{k+1} + \cdots$. □

لم ۴۲.۲. $\hat{\mathbb{Z}}_p = \{x \in \hat{\mathbb{Q}}_p : |x|_p \leq 1\}$.

اثبات. بنا به لم ۳۷.۲ هر عنصر x در $\hat{\mathbb{Z}}_p$ دارای نمایش یکتای $\sum\limits_{i=0}^{\infty} a_i p^i$ است، پس بوضوح $|x|_p \leq 1$ و بنابراین $\hat{\mathbb{Z}}_p \subseteq \{x \in \hat{\mathbb{Q}}_p : |x|_p \leq 1\}$.

حال فرض کنید $x \in \hat{\mathbb{Q}}_p$ به گونه‌ای باشد که $|x|_p \leq 1$. می‌خواهیم نشان دهیم که $x \in \hat{\mathbb{Z}}_p$. با توجه به لم ۴۰.۲ داریم $x = p^k u$ که در آن u_i در $\hat{\mathbb{Z}}_p$ وارون‌پذیر است. در نتیجه از آنجایی که بنا به فرض $|x|_p \leq 1$، پس

$$|x|_p = |p^k u|_p = |p^k|_p |u|_p = 2^{-k} \leq 1$$

و این نتیجه می‌دهد $k \geq 0$. از طرفی، چون u عنصری وارون‌پذیر در $\hat{\mathbb{Z}}_p$ است، پس $u = a_0 + a_1 p + a_2 p^2 + \cdots$ که در آن $a_0 \neq 0$ و بنابراین $x = p^k(a_0 + a_1 p + a_2 p^2 + \cdots)$. از این رو، با توجه به اینکه $k \geq 0$، پس x متعلق به $\hat{\mathbb{Z}}_p$ است. □

نتیجه ۴۳.۲. دیاگرام زیر که در آن هر فلش با ترتیب شمول قرار داده شده است برقرار است:

$$\begin{tikzcd}
\hat{\mathbb{Z}}_p \arrow[r] & \hat{\mathbb{Q}}_p \\
\mathbb{Z} \arrow[u] \arrow[r] & \mathbb{Q} \arrow[u]
\end{tikzcd}$$

۴.۳.۲ تعریف‌پذیری $\hat{\mathbb{Z}}_p$ در $\hat{\mathbb{Q}}_p$

در بخشِ ۱۲.۱ با مفهوم تعریف‌پذیری آشنا شدیم. گفتیم که اگر یک ساختارِ $\mathcal{M} = (M, \cdots)$ داشته باشیم، آنگاه می‌گوییم $A \subseteq M^n$ تعریف‌پذیر است هرگاه $A = \{\bar{x} : \mathcal{M} \models \varphi(\bar{x})\}$ که در آن φ یک فرمول مرتبه اول است و $\bar{x} = (x_1, x_2, \cdots, x_n)$.

در بخش گذشته دیدیم که $\hat{\mathbb{Z}}_p$ یک زیرحلقه از میدانِ $\hat{\mathbb{Q}}_p$ است. سوالی که در این بخش به دنبال پاسخ آن هستیم این است که آیا $\hat{\mathbb{Z}}_p$ در میدانِ $\hat{\mathbb{Q}}_p$ تعریف‌پذیر است؟ به بیان دیگر آیا یک فرمول مرتبه‌ی اولِ φ در زبان حلقه‌ها وجود دارد به طوری که $\hat{\mathbb{Z}}_p = \{x : \hat{\mathbb{Q}}_p \models \varphi(x)\}$؟

قضیه ۴۴.۲. مجموعه‌ی $\hat{\mathbb{Z}}_p$ در $\hat{\mathbb{Q}}_p$ تعریف‌پذیر است.

اثبات. برای $p \neq 2$ نشان می‌دهیم که

$$\forall x \in \hat{\mathbb{Q}}_p \ \ (x \in \hat{\mathbb{Z}}_p \Longleftrightarrow \exists y \ 1 + px^2 = y^2).$$

ابتدا نشان می‌دهیم که اگر a در $\hat{\mathbb{Z}}_p$ باشد، آنگاه در معادله‌ی فوق صدق می‌کند؛ به بیان دیگر اگر $a \in \hat{\mathbb{Z}}_p$ آنگاه معادله‌ی $y^2 - (1 + pa^2) = 0$ در $\hat{\mathbb{Q}}_p$ دارای جواب است. به این منظور قرار می‌دهیم $f(y) = y^2 - (1 + p^2)$. تصویر $f(y)$ در میدان پیمانه‌های حلقه‌ی p ـ ادیک، یعنی $\mathbb{F}_p$ برابر است با $\bar{f}(y) = y^2 - \bar{1}$. توجه کنید که اولاً $\bar{f}(\bar{1}) = 0$ و ثانیاً چون $p \neq 2$، پس $\bar{f}'(\bar{1}) = \bar{2}y = \bar{2} \neq 0$. حال بنا به هنسلی بودن $\hat{\mathbb{Z}}_p$ می‌توان نتیجه گرفت که یک عنصرِ y در $\hat{\mathbb{Z}}_p$ وجود دارد به طوری که $y^2 - (1 + pa^2) = 0$.

برای اثبات جهت عکس، فرض کنید x در معادله‌ی $\exists y \ 1 + px^2 = y^2$ صدق کند، نشان می‌دهیم که $x \in \hat{\mathbb{Z}}_p$. با توجه به لمِ ۴۲.۲ کافی است نشان دهیم که $|x|_p \leq 1$. با برهان خلف فرض کنید چنین نباشد؛ یعنی $|x|_p > 1$. در این صورت با توجه به تعریف قدرمطلقِ $|.|_p$ داریم $v_p(x) < 0$. حال نگاشت p ـ ادیکِ v_p را روی دو طرف معادله‌ی $1+px^2 = y^2$ اعمال می‌کنیم، پس داریم $v_p(1+px^2) = v_p(x^2)$. توجه کنید که چون $v_p(x) < 0$ و $v_p(1) = 0$، پس $v_p(1) \neq v_p(px^2)$ و بنابراین $v_p(1 + px^2) = \min\{0, v_p(px^2)\} = v_p(px^2) = v_p(p) + 2v_p(x) = 1 + 2v_p(x)$. از طرفی $v_p(y^2) = 2v_p(y)$، پس نهایتاً داریم $2v_p(y) = 1 + 2v_p(x)$ که این تناقض است.

برای حالتی که $p = 2$ داریم: $x \in \hat{\mathbb{Z}}_p \iff \exists y \ 1 + 8x^2 = y^2$ و اثبات آن نیز مشابه استدلال فوق است. □

۵.۳.۲ یک روش جبری برای معرفی $\hat{\mathbb{Z}}_p$

خانواده‌ی $\{R_i\}_{i \in \mathbb{N}}$ از حلقه‌ها را همراه با نگاشت‌های هومومورفیسمِ $\pi_{j,i} : R_j \to R_i$ برای هر $i \leq j$ در نظر بگیرید. فرض کنید این نگاشت‌ها دارای دو ویژگی زیر باشند:

۱. به ازای هر $i \in \mathbb{N}$ نگاشتِ $\pi_{i,i}$ روی R_i همانی باشد،

۲. برای هر $i \leq j \leq k$ داشته باشیم $\pi_{k,i} = \pi_{k,j}\ \ o\ \ \pi_{j,i}$.

حد معکوسِ $\{R_i\}_{i\in\mathbb{N}}$ که آن را با نماد $\varprojlim R_n$ نشان می‌دهیم برابر است با مجموعه‌ی متشکل از دنباله‌های $(a_n)_{n\in\mathbb{N}}$ با این ویژگی که $a_n \in R_n$ و $\pi_{j,i}(a_j) = a_i$ برای هر $i \leq j$.

در این بخش می‌خواهیم نشان دهیم که $\hat{\mathbb{Z}}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. در راستای این کار نگاشت‌های همومورفیسم را بین حلقه‌های خارج قسمتی $\mathbb{Z}/p^n\mathbb{Z}$ به ازای هر $n \in \mathbb{N}$ معرفی می‌کنیم و نشان می‌دهیم این همومورفیسم‌ها دو ویژگی فوق را دارند.

تعریف همومورفیسم بین حلقه‌های $\mathbb{Z}/p^n\mathbb{Z}$

خانواده‌ی $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n\in\mathbb{N}}$ از حلقه‌های خارج قسمتی را در نظر بگیرید. در این خانواده، حلقه‌ی $\mathbb{Z}/p^n\mathbb{Z}$ متشکل از باقی‌مانده‌ی اعداد صحیح بر p^n است. نگاشت تصویرِ $\pi_{j,i} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ را به ازای $j \geq i$ در نظر بگیرید. در واقع این نگاشت یک عنصرِ $a_0 + a_1p + a_2p^2 + \cdots + a_{i-1}p^{i-1} + a_ip^i + \cdots + a_{j-1}p^{j-1}$ در $\mathbb{Z}/p^j\mathbb{Z}$ که در آن ضرایب همگی از مجموعه‌ی $\{0, 1, 2, \cdots, p-1\}$ هستند را به $a_0 + a_1p + a_2p^2 + \cdots + a_{i-1}p^{i-1} \in \mathbb{Z}/p^i\mathbb{Z}$ می‌برد. به سادگی می‌توان دید که هر یک از این نگاشت‌ها همومورفیسم هستند. به علاوه این همومورفیسم‌ها دو ویژگی زیر را دارند:

۱. بوضوح نگاشت تصویرِ $\pi_{i,i} : \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ یک نگاشت همانی است.

۲. برای هر $i \leq j \leq k$ نگاشتِ $\pi_{k,j} = \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ را در نظر بگیرید. این نگاشت یک عنصر دلخواهِ $a_0 + a_1p + a_2p^2 + \cdots + a_{i-1}p^{i-1} + a_ip^i + \cdots + a_{j-1}p^{j-1} + a_jp^j + \cdots + a_{k-1}p^{k-1}$ در $\mathbb{Z}/p^k\mathbb{Z}$ را به $a_0 + a_1p + a_2p^2 + \cdots + a_{i-1}p^{i-1} + a_ip^i + \cdots + a_{j-1}p^{j-1}$ در $\mathbb{Z}/p^j\mathbb{Z}$ می‌برد. همچنین، نگاشتِ $\pi_{k,j} = \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ عنصر $a_0 + a_1p + a_2p^2 + \cdots + a_{i-1}p^{i-1} + a_ip^i + \cdots + a_{j-1}p^{j-1}$ را به $a_0 + a_1p + a_2p^2 + \cdots + a_{i-1}p^{i-1}$ در $\mathbb{Z}/p^i\mathbb{Z}$ می‌برد. در نتیجه ترکیب دو نگاشتِ $\pi_{k,j}$ و $\pi_{j,i}$ برابر با نگاشتِ $\pi_{k,i}$ است.

توجه کنید که ویژگی دوم به این معنی است که اگر یک عدد را در پیمانه‌ی p^j بنویسیم و سپس آن را به پیمانه‌ی p^i ببریم حاصل برابر است با اینکه آن عدد را به طور مستقیم به پیمانه‌ی p^i ببریم.

نهایتاً داریم:

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \{a_0 + a_1p + a_2p^2 + \cdots : 0 \leq a_i \leq p-1\}$$

که بنا به لم ۴۱.۲، این مجموعه برابر با حلقه‌ی اعداد p ـ ادیک است.

توجه ۴۵.۲. آنچه که گفته شد در دیاگرام زیر آورده شده است:

$$\begin{tikzcd}
\mathbb{Z}/p\mathbb{Z} & \mathbb{Z}/p^2\mathbb{Z} \arrow[l, "\pi_{2,1}"] & \mathbb{Z}/p^3\mathbb{Z} \arrow[l, "\pi_{3,2}"] \arrow[ll, bend right, "\pi_{3,1}"'] & \mathbb{Z}/p^4\mathbb{Z} \arrow[l, "\pi_{4,3}"] \arrow[ll, bend right, "\pi_{4,2}"'] & \cdots \arrow[l] \\
 & & \hat{\mathbb{Z}}_p \arrow[ull, bend left] \arrow[ul, bend left] \arrow[u] \arrow[ur, bend right] \arrow[urr, bend right] & &
\end{tikzcd}$$

توجه کنید که از $\hat{\mathbb{Z}}_p$ به هر حلقه‌ی $\mathbb{Z}/p^n\mathbb{Z}$ یک همومورفیسم داریم که هر سری در $\hat{\mathbb{Z}}_p$ مانندِ $a_0 + a_1p + a_2p^2 + \cdots$ که در آن $0 \leq a_i \leq p-1$ را در n ـ اُمین ترم قطع می‌کند، یعنی این نگاشت، سری فوق را به $a_0 + a_1p + a_2p^2 + \cdots + a_{n-1}p^{n-1}$ می‌برد.

---

* خلاصه‌ی فصل:

در این فصل به دو موضوع اصلی پرداخته شده است:

۱. حلقه‌های موضعی هنسلی: یک حلقه‌ی R را "موضعی" می‌نامیم هرگاه فقط یک ایده‌آل ماکسیمال داشته باشد. این ایده‌آل ماکسیمال را با m نشان می‌دهیم و شامل همه‌ی عناصر وارون‌ناپذیرِ R است. همچنین، میدان $k = R/m$ را "میدان پیمانه‌ها" می‌نامیم.

پس از آن به بررسی دسته‌ای از حلقه‌های موضعی با ویژگی هنسلی پرداختیم. می‌گوییم یک حلقه ویژگی "هنسلی" دارد هرگاه برای هر $f \in R[x]$ که یک عنصر α در R وجود دارد به طوری که یک ریشه‌ی ساده‌ی آن در k باشد، یک عنصر $a \in R$ موجود باشد به طوری که $f(a) = 0$ و $a \overset{m}{\equiv} \alpha$.

در لم هنسل نشان داده‌ایم که حلقه‌های نُرم‌داری که همه‌ی دنباله‌های کوشی در آن همگرا هستند، هنسلی هستند. به عنوان مثال، حلقه‌ی $R[[x]]$ که متشکل از سری‌های توانی حول R است، تحت یک نُرم خاص یک حلقه‌ی کامل و در نتیجه هنسلی است.

۲. میدان و حلقه‌ی p ـ ادیک: نگاشتِ v_p که یک عنصر x در $\mathbb{Q}$ را به یک عدد صحیح k می‌برد به طوری که $x = p^k\frac{a'}{b'}$ و $p \nmid a', p \nmid b'$، نگاشت p ـ ادیک نامیده می‌شود. با استفاده از نگاشت v_p یک قدرمطلق با ضابطه‌ی $|x|_p = 2^{-v(p)}$ روی میدان اعداد گویا تعریف می‌کنیم که آن را قدرمطلق p ـ ادیک می‌نامیم. میدان اعداد گویا با نُرم p ـ ادیک کامل نیست. کامل شده‌ی $\mathbb{Q}$ با نُرم pـ ادیک را میدان pـ ادیک می‌نامیم و آن را

با $\hat{\mathbb{Q}}_p$ نمایش می‌دهیم. به مجموعه‌ی $\{x \in \hat{\mathbb{Q}}_p : |x|_p \leq 1\}$ حلقه‌ی p ـ ادیک‌ها می‌گوییم و آن را با $\hat{\mathbb{Z}}_p$ نشان می‌دهیم. این حلقه در واقع کامل شده‌ی حلقه‌ی $\mathbb{Z}$ تحت نُرم pـ ادیک است. به علاوه، در انتهای فصل نشان دادیم که $\hat{\mathbb{Z}}_p$ حد معکوس حلقه‌های خارج قسمتی $\mathbb{Z}/p^n\hat{\mathbb{Z}}_p$ به ازای هر $n \in \mathbb{N}$ است. به علاوه این حلقه، موضعی با ایده‌آل ماکسیمال $p\hat{\mathbb{Z}}_p$ است.

اگر $p \neq 2$ آن‌گاه فرمولِ $\exists y\ 1 + px^2 = y^2$ و اگر $p = 2$ آن‌گاه فرمولِ $\exists y\ 1 + 8x^2 = y^2$ حلقه‌ی $\hat{\mathbb{Z}}_p$ را در میدانِ $\hat{\mathbb{Q}}_p$ تعریف می‌کند.

فصل ۳

میدان ارزیابی

همان‌طور که پیش‌تر بیان کردیم، موضوع این پایان‌نامه در حوزه‌ی جبر و منطق قرار دارد. در این فصل، به آشنایی با مفاهیم و اصطلاحات جبری مرتبط با میدان‌های ارزیابی پرداخته‌ایم.

در ادامه نگاشت ارزیابی و یک حلقه‌ی ارزیاب را معرفی می‌کنیم و نشان می‌دهیم که هر حلقه‌ی ارزیاب از یک نگاشت ارزیابی به دست می‌آید. در انتهای این فصل، میدان سری‌های هان و ارزیابی روی آن را معرفی می‌کنیم و برخی از ویژگی‌های آن را به تفصیل شرح می‌دهیم. مطالب این فصل از کتاب‌های [۲۱] و [۶] گردآوری و بسط داده شده است.

۱.۳ نگاشت ارزیابی

تعریف ۱.۳. فرض کنید K یک میدان و $(\Gamma, +, \geq)$ یک گروه مرتب آبلی باشد. نگاشتِ $v : K \to \Gamma$ یک نگاشت ارزیابی است هرگاه برای هر $x, y \in K$،

۱. $v(x+y) \geq \min\{v(x), v(y)\}$،

۲. $v(x \cdot y) = v(x) + v(y)$،

۳. $x = 0 \iff v(x) = \infty$.

توجه ۲.۳. در ویژگی اول تعریف فوق، منظور از نماد $\geq$ همان ترتیب گروهِ Γ است. همچنین در ویژگی دوم، منظور از علامتِ $+$ همان عمل گروهِ Γ است.

لم ۳.۳. فرض کنید Γ یک گروه مرتب آبلی، K یک میدان و $v : K \to \Gamma$ یک نگاشت ارزیابی باشد. در این صورت برای $x, y \in K$ موارد زیر نتیجه می‌شوند:

۱. $v(1) = 0$.

۲. $v(-1) = 0$.

۳. $v(x) = v(-x)$.

۴. $v(x^{-1}) = -v(x)$.

۵. اگر $v(y) > v(x)$، آنگاه $v(x+y) = v(x)$.

اثبات.

۱. با توجه به ویژگی ۲ در تعریفِ ۱.۳، داریم: $v(1) = v(1 \cdot 1) = v(1) + v(1)$. از این رابطه می‌توان نتیجه گرفت که $v(1) = 0$.

۲. با استفاده از ویژگی ۲ که در تعریفِ ۱.۳ آمده است و قسمت ۱ در همین لم، داریم:

$$0 = v(1) = v((-1) \cdot (-1)) = v(-1) + v(-1) = 2v(-1).$$

از آنجایی که Γ یک گروه مرتب است، پس تاب ندارد. بنابراین از اینکه $2v(-1) = 0$ نتیجه می‌شود که $v(-1) = 0$.

۳. با توجه به ویژگی ۲ در تعریفِ ۱.۳ و قسمت ۲ در همین لم داریم:

$$v(-x) = v((-1) \cdot x) = v(-1) + v(x) = v(x).$$

۴. با توجه به ویژگی ۱ در همین لم داریم: $0 = v(1) = v(x \cdot x^{-1}) = v(x) + v(x^{-1})$. بنابراین، $-v(x) = v(x^{-1})$.

۵. اگر $v(y) > v(x)$، آنگاه با توجه به ویژگی ۱ در تعریفِ ۱.۳، می‌توان نوشت:

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

از طرفی $\min\{v(x+y), v(y)\} \geq v(x) = v(x+y-y)$. اما از آنجا که $v(x) > v(y)$، پس $\min\{v(x+y), v(y)\}$ نمی‌تواند $v(y)$ شود و بنابراین $\min\{v(x+y), v(y)\} = v(x+y)$، از این رو $v(x) \geq v(x+y)$.

□

۲.۳ حلقه‌ی ارزیاب

یک زیرحلقه از یک میدان را یک حلقه‌ی ارزیاب می‌نامیم هرگاه هر عنصر میدان یا خودش یا وارونش در این زیرحلقه باشد. فرض کنید v یک نگاشت ارزیابی از میدانِ K به یک گروه مرتب آبلی Γ باشد. در این بخش، نشان می‌دهیم که مجموعه‌ی $O_v := \{x \in K : v(x) \geq 0\}$ یک حلقه‌ی ارزیاب از میدانِ K و همچنین یک حلقه‌ی موضعی است. نهایتاً، خواهیم دید که نه تنها به ازای هر نگاشت ارزیابی روی یک میدان، مجموعه‌ی O_v مربوط به آن نگاشت یک حلقه‌ی ارزیاب است، بلکه هر حلقه‌ی ارزیاب در یک میدان نیز از یک نگاشت ارزیابی روی آن ناشی می‌شود و بنابراین به طور خاص هر حلقه‌ی ارزیاب، موضعی است.

لم ۴.۳. فرض کنید K یک میدان، Γ یک گروه آبلی مرتب و $v : K \to \Gamma$ یک نگاشت ارزیابی باشد. در این صورت مجموعه‌ی $O_v := \{x \in K : v(x) \geq 0\}$ یک زیرحلقه از میدانِ K است.

اثبات. از آنجا که $v(0) = \infty \geq 0$ و $v(1) = 0 \geq 0$، پس 0 و 1 در O_v قرار دارند. حال فرض کنید $x, y \in O_v$. در این صورت $v(x) \geq 0$ و $v(y) \geq 0$ و با استفاده از ویژگی‌های نگاشت ارزیابی داریم: $v(x-y) \geq \min\{v(x), v(y)\} \geq 0$ و $v(x \cdot y) = v(x) + v(y) \geq 0$، بنابراین $x - y$ و $x \cdot y$ نیز در O_v قرار دارند. پس با توجه به اینکه 0 و 1 در O_v قرار دارند و O_v تحت عمل تفاضل و ضرب بسته است، می‌توان نتیجه گرفت که O_v یک زیرحلقه از K است. □

لم ۵.۳. فرض کنید K یک میدان، Γ یک گروه آبلی مرتب و $v : K \to \Gamma$ یک نگاشت ارزیابی باشد. در این صورت حلقه‌ی $O_v = \{x \in K : v(x) \geq 0\}$ یک حلقه‌ی موضعی با ایده‌آل ماکسیمالِ $m_v := \{x \in K : v(x) > 0\}$ است.

اثبات. با توجه به ویژگی‌های نگاشت ارزیابی، می‌توان به سادگی نتیجه گرفت که $(m_v, +)$ یک زیرگروه از $(O_v, +)$ است. همچنین، برای هر $t \in O_v$ و $x \in m_v$ داریم $v(tx) = v(t) + v(x) > 0$، یعنی $tx \in m_v$. در نتیجه مجموعه‌ی m_v یک ایده‌آل از حلقه‌ی O_v است.

حال می‌خواهیم نشان دهیم که m_v یک ایده‌آل ماکسیمال از حلقه‌ی O_v است. با برهان خلف، فرض کنید یک ایده‌آل سره‌ی I از حلقه‌ی O_v وجود دارد به طوری که $m_v \subset I$. از این فرض می‌توان نتیجه گرفت که حداقل یک عنصر x در O_v وجود دارد به طوری که $x \in I$ و $x \notin m_v$. در نتیجه $v(x) = 0$، پس $v(x^{-1}) = -v(x) = 0$ و

بنابراین عنصر x^{-1} نیز در O_v است. با توجه به اینکه I یک ایده‌آل از حلقه‌ی O_v است، پس عنصر $1 = x \cdot x^{-1}$ در I قرار دارد، بنابراین $I = O_v$ و این با فرض سره بودنِ I در تناقض است.

نهایتاً می‌خواهیم نشان دهیم که m_v تنها ایده‌آل ماکسیمال حلقه‌ی O_v است. به این منظور نشان می‌دهیم m_v متشکل از همه‌ی عناصر وارون‌ناپذیر حلقه‌ی O_v است. فرض کنید $x \in O_v$ به گونه‌ای باشد که $v(x) > 0$، در این صورت $v(x^{-1}) < 0$ و بنابراین $x^{-1} \notin O_v$. از این نتیجه می‌شود که یک عنصر x در حلقه‌ی O_v وارون‌پذیر است اگروتنهااگر $v(x) = 0$. در نتیجه ایده‌آل ماکسیمالِ m_v از همه‌ی عناصر وارون‌ناپذیر حلقه‌ی O_v تشکیل شده است، از این رو بنا به لم ۵.۲، (O_v, m_v) یک حلقه‌ی موضعی است. □

تعریف ۶.۳. فرض کنید K یک میدان، Γ یک گروه آبلی مرتب و $v : K \to \Gamma$ یک نگاشت ارزیابی باشد. در این صورت، میدانِ $k_v = \frac{O_v}{m_v}$ را *میدان پیمانه‌های نگاشت ارزیابی* v می‌نامیم.

تعریف ۷.۳. زیرحلقه‌ی A از میدانِ K را یک *حلقه‌ی ارزیاب* برای K می‌نامیم هرگاه برای هر $x \in K$ یا $x \in A$ یا $x^{-1} \in A$.

لم ۸.۳. فرض کنید K یک میدان و v یک نگاشت ارزیابی روی آن باشد. در این صورت O_v یک حلقه‌ی ارزیاب است.

اثبات. با توجه به این که برای هر $x \in K$ یا $v(x) < 0$ یا $v(x) \geq 0$، می‌توان نتیجه گرفت که یا x یا x^{-1} در O_v قرار دارد. □

یک رویکرد دیگر به میدان‌های ارزیابی استفاده از تعریف حلقه‌های ارزیاب است. در قضیه‌ی زیر نشان می‌دهیم که هر حلقه‌ی ارزیاب از یک نگاشت ارزیابی ناشی می‌شود.

قضیه ۹.۳. اگر K یک میدان شامل حلقه‌ی ارزیاب A باشد، آنگاه یک گروه مرتبِ Γ و یک نگاشت ارزیابی $v : K \to \Gamma$ وجود دارد به طوری که $A = O_v$.

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

$$x \sim y \iff x/y \in A \text{ و } y/x \in A.$$

به عبارت دیگر $x \sim y$ اگروتنهااگر x/y یک عنصر وارون‌پذیر در A باشد. مجموعه‌ی $\Gamma = \{[x]_\sim : x \in K\}$ همراه با عمل ضرب میدان، یک گروه است. در واقع Γ گروه خارج‌قسمتیِ $K/U(A)$ است که در آن $U(A)$ مجموعه‌ی عناصر وارون‌پذیرِ A است. حال روی گروهِ Γ ترتیبِ $\geq$ را به صورت زیر تعریف می‌کنیم:

$$[x]_\sim \geq [y]_\sim \iff x/y \in A.$$

با توجه به اینکه A یک حلقه‌ی ارزیاب است، به سادگی می‌توان بررسی کرد که $\geq$ روی Γ یک ترکیب خطی است. بنابراین تا اینجا نشان دادیم که $(\Gamma, \cdot, \geq)$ یک گروه مرتب آبلی است. حال نگاشتِ $v : K \to \Gamma$ را به صورت زیر تعریف می‌کنیم:

$$v(x) = \begin{cases} [x]_\sim & x \neq 0 \\ \infty & x = 0 \end{cases}$$

این نگاشت دارای دو ویژگی است:

۱. فرض کنید x و y دو عنصر ناصفر در K باشند. اگر $v(x) \geq v(y)$، آنگاه $x/y \in A$. چون A یک حلقه است و $1 \in A$، پس $x/y + 1 = (x+y)/y$ در A قرار دارد، بنابراین $v(x+y) \geq v(y)$. از آنجا که $\min\{v(x), v(y)\} = v(y)$ پس داریم $v(x+y) \geq \min\{v(x), v(y)\}$.

۲. توجه کنید که Γ یک گروه ضربی است. برای هر دو عنصر $x, y \in K$ عمل جمع را به صورت $[x]_\sim + [y]_\sim := [x \cdot y]_\sim$ بازنویسی می‌کنیم؛ بنابراین تساوی $v(x.y) = v(x) + v(y)$ بوضوح برقرار است.

در نتیجه بنا به تعریفِ ۱.۳، نگاشتِ v یک نگاشت ارزیابی است. با توجه به تعریف نگاشتِ v و تعریف ترتیبِ $\geq$ روی گروهِ Γ داریم:

$$O_v = \{x \in K : v(x) \geq 0_\Gamma\} = \{x \in K : [x]_\sim \geq [1]_\sim\} = \{x \in K : \frac{x}{1} \in A\} = A.$$

□

تعریف ۱۰.۳. زوج (K, O_v) یک *میدان ارزیابی* نامیده می‌شود هرگاه K یک میدان و $O_v \subseteq K$ یک حلقه‌ی ارزیاب باشد.

در ادامه، چند مثال از میدان‌های ارزیابی را بررسی می‌کنیم.

مثال ۱۱.۳.

۱. فرض کنید $\hat{\mathbb{Q}}_p$ میدانِ pـ ادیک باشد (مطابق آنچه در بخشِ ۲.۳.۲ معرفی شد). نگاشتِ $v_p : \hat{\mathbb{Q}}_p \to \mathbb{Z}$ را در نظر بگیرید که یک عنصرِ $x = \sum_{i=-n}^{\infty} a_i p^i$ متعلق به $\hat{\mathbb{Q}}_p$ را به $\min\{i : a_i \neq 0\}$ می‌برد. به سادگی می‌توان بررسی کرد که v_p یک نگاشت ارزیابی است. بنا به ۴۲.۲ و ۳۸.۲ داریم:

$$O_{v_p} = \{x \in \hat{\mathbb{Q}}_p : v_p(x) \geq 0\} = \hat{\mathbb{Z}}_p$$

و

$$m_{v_p} = \{x \in \hat{\mathbb{Q}}_p : v_p(x) > 0\} = p\hat{\mathbb{Z}}_p.$$

حال نگاشتِ $\varphi : \hat{\mathbb{Z}}_p \to \mathbb{F}_p$ را در نظر بگیرید که یک عنصر دلخواهِ $a_0 + a_1p + a_2p^2 + \cdots$ در $\hat{\mathbb{Z}}_p$ را به a_0 می‌برد. به سادگی می‌توان بررسی کرد که این نگاشت یک همریختی پوشاست و $\ker(\varphi) = p\hat{\mathbb{Z}}_p$، پس بنا به قضیه‌ی اول یکریختی داریم $\hat{\mathbb{Z}}_p/p\hat{\mathbb{Z}}_p \cong \mathbb{F}_p$ و این یعنی میدان پیمانه‌های نگاشت v_p برابر با $\mathbb{F}_p$ است.

۲. فرض کنید $K = \mathbb{C}(t) = \{\frac{f(t)}{g(t)} : f(t), g(t) \in \mathbb{C}[t]\}$. برای هر $f = \frac{g(t)}{h(t)}$ در K قرار دهید $v(f) = n$ هرگاه $f = t^n \cdot \frac{g_1(t)}{h_1(t)}$ و $g_1(0) \neq 0, h_1(0) \neq 0$. به سادگی می‌توان بررسی کرد که v یک نگاشت ارزیابی است. در این صورت، داریم:

$$O_v = \{\frac{g}{h} : h, g \in \mathbb{C}[t], v(\frac{g}{h}) \geq 0\} = \{\frac{g}{h} : h, g \in \mathbb{C}[t], h(0) \neq 0\}$$

و

$$m_v = \{\frac{g}{h} : h, g \in \mathbb{C}[t], v(\frac{g}{h}) > 0\} = \{\frac{g}{h} : h, g \in \mathbb{C}[t], h(0) \neq 0, g(0) = 0\}.$$

توجه کنید که نگاشت $\varphi : O_v \to \mathbb{C}$ با ضابطه‌ی $\varphi(\frac{g(t)}{h(t)}) = \frac{g(0)}{h(0)}$ یک همریختی پوشا است و بوضوح $\ker(\varphi) = m_v$، پس بنا به قضیه‌ی اول یکریختی داریم $k_v = \frac{O_v}{m_v} \cong \mathbb{C}$.

تعریف ۱۲.۳. میدان ارزیابی (K, O_v) را هنسلی می‌نامیم هرگاه O_v یک حلقه‌ی هنسلی باشد(برای تعریف یک حلقه‌ی هنسلی به ۸.۲ رجوع کنید).

۳.۳ سری‌های هان

در این بخش خواهیم دید که برای هر گروه مرتب آبلی Γ و میدان k می‌توان یک میدان ارزیابی ساخت به طوری که گروه ارزیاب آن برابر با Γ و میدان پیمانه‌های آن k باشد. مطالب این بخش از کتابِ [۱۷] گردآوری شده است.

تعریف ۱۳.۳. یک مجموعه‌ی مرتب A را خوش‌ترتیب می‌نامیم هرگاه هر زیرمجموعه‌ی ناتهی آن دارای عنصر می‌نیمم باشد.

به طور معادل با فرض اصل انتخاب، A خوش‌ترتیب است هرگاه در آن هیچ دنباله‌ی نامتناهی نزولی وجود نداشته باشد.

لم ۱۴.۳. فرض کنید Γ یک گروه مرتب آبلی باشد و $A, B \subseteq \Gamma$ دو مجموعه‌ی خوش‌ترتیب باشند. در این صورت، مجموعه‌ی $A+B := \{\alpha+\beta : \alpha \in A, \beta \in B\}$ یک مجموعه‌ی خوش‌ترتیب است. همچنین، برای هر $\gamma \in A+B$ مجموعه‌ی $\{(\alpha, \beta) \in A \times B : n \in \mathbb{N} \ , \ \gamma = \alpha + \beta\}$ متناهی است.

اثبات. با برهان خلف، فرض کنید $(a_0,b_0),(a_1,b_1),\cdots$ یک دنباله‌ی نامتناهی از اعضای مجزای $A\times B$ باشد به طوری که $\underbrace{a_i+b_i=a_j+b_j=\gamma}_{*}$. در این صورت $(a_i)_{i\in\mathbb{N}}$ یک دنباله‌ی اکیداً یکنواست. از آنجا که A یک مجموعه‌ی خوش‌ترتیب است، بنابراین این دنباله نمی‌تواند اکیداً نزولی باشد و در نتیجه یک دنباله‌ی اکیداً صعودی است. از طرفی، برای اینکه رابطه‌ی $*$ برقرار شود باید $b_0>b_1>\cdots$ و این تناقض است، زیرا B یک مجموعه‌ی خوش‌ترتیب است، پس در آن هیچ دنباله‌ی نامتناهی نزولی وجود ندارد. $\square$

تعریف ۱۵.۳. (سری هان) فرض کنید k یک میدان و $(\Gamma,+,\geq)$ یک گروه مرتب آبلی باشد. به یک سری ظاهری $f(t)=\sum\limits_{\gamma\in\Gamma}a_\gamma t^\gamma$ که در آن $a_\gamma\in k$، *سری هان* [1] گوییم هرگاه $\operatorname{supp}(f):=\{\gamma\in\Gamma : a_\gamma\neq 0\}$ یک زیرمجموعه‌ی خوش‌ترتیب از Γ باشد.

مجموعه‌ی متشکل از سری‌های هان را با $k((t^\Gamma))$ نمایش می‌دهیم. حال روی این مجموعه اعمال جمع و ضرب را به صورت زیر تعریف می‌کنیم:

$$\sum_{\gamma\in\Gamma}a_\gamma t^\gamma+\sum_{\gamma\in\Gamma}b_\gamma t^\gamma=\sum_{\gamma\in\Gamma}(a_\gamma+b_\gamma)t^\gamma$$
$$\Big(\sum_{\gamma\in\Gamma}a_\gamma t^\gamma\Big)\Big(\sum_{\gamma\in\Gamma}b_\gamma t^\gamma\Big)=\sum_{\gamma}\Big(\sum_{\alpha+\beta=\gamma}a_\alpha b_\beta\Big)t^\gamma$$

توجه داشته باشید که عمل ضربی که در بالا تعریف کردیم، خوش‌تعریف است. زیرا بر اساس لم ۱۴.۳، برای هر γ در $A+B$، تعداد زوج‌های (α,β) در $A\times B$ با این ویژگی که $\gamma=\alpha+\beta$ متناهی است. بنابراین، می‌توان نتیجه گرفت که $\sum\limits_{\alpha+\beta=\gamma}a_\alpha b_\beta$، به عنوان یک مجموع از تعداد متناهی تا عنصر میدانِ k، نیز در k قرار می‌گیرد.

توجه ۱۶.۳. مجموعه‌ی $k((t^\Gamma))$ با عمل جمع و ضرب تعریف شده در بالا، یک حوزه‌ی صحیح است.

۱.۳.۳ یک نگاشت ارزیابی روی $k((t^\Gamma))$

نماد گذاری ۱۷.۳. در یک سری هانِ $f=\sum\limits_{\gamma\in\Gamma}a_\gamma t^\gamma$، عنصرِ a_0 یعنی جمله‌ی با اندیس صفر گروه را جمله‌ی ثابت سری f می‌نامیم.

نگاشت $v:k((t^\Gamma))\setminus\{0\}\to\Gamma$ را با ضابطه‌ی $v\left(\sum\limits_{\gamma\in\Gamma}a_\gamma t^\gamma\right):=\min\{\gamma : a_\gamma\neq 0\}$ در نظر بگیرید. به سادگی می‌توان دید که v یک نگاشت ارزیابی روی حوزه‌ی صحیحِ $k((t^\Gamma))$ است. حلقه‌ی ارزیاب آن را با $K[[t^\Gamma]]$ نشان می‌دهیم و به صورت زیر است:

$$\begin{aligned}O_v=k[[t^\Gamma]]&:=\{x\in k((t^\Gamma)) : v(x)\geq 0\}=\{f\in k((t^\Gamma)) : \operatorname{supp}(f)\subseteq\Gamma^{\geq 0}\}\\&=\{f : \text{توان منفی نداشته باشد } f\}.\end{aligned}$$

[1] Hahn series

حال نگاشت $g : k[[t^\Gamma]] \to k$ را در نظر بگیرید که هر $f \in k[[t^\Gamma]]$ را به جمله‌ی ثابتش می‌برد. به سادگی می‌توان دید که این نگاشت یک همریختی پوشا است و دارای هسته‌ای به شکل زیر می‌باشد:

$$\ker(g) = \{f : \text{کوچکترین توان } f \text{ مثبت است}\} = \{f : v(f) > 0\} = m_v$$

بنابراین، بر اساس قضیه اول یکریختی، داریم: $k_v = \frac{k[[t^\Gamma]]}{m_v} \cong k$.

توجه ۱۸.۳. توجه کنید که نگاشت ارزیابی فوق خوش‌تعریف است، زیرا هر سری $f = \sum\limits_{\gamma \in \Gamma} a_\gamma t^\gamma$ در $k((t^\Gamma))$ دارای این ویژگی است که $\operatorname{supp}(f) = \{\gamma \in \Gamma : a_\gamma \neq 0\}$ یک مجموعه‌ی خوش‌ترتیب است، در نتیجه $\min\{\gamma \in \Gamma : a_\gamma \neq 0\}$ وجود دارد.

۲.۳.۳ اثبات میدان بودن سری‌های هان

در ادامه قصد داریم نشان دهیم که $k((t^\Gamma))$ یک میدان است. در راستای این کار، به لم بعدی نیاز داریم که لمی قوی‌تر از لم ۱۴.۳ است:

نماد گذاری ۱۹.۳. فرض کنید A یک مجموعه باشد. منظورمان از $A^{<\mathbb{N}}$، مجموعه‌ی همه‌ی دنباله‌های متناهی از اعضای A است.

لم ۲۰.۳. فرض کنید Γ یک گروه مرتب آبلی و $A \subseteq \Gamma^{>0}$ یک مجموعه‌ی خوش‌ترتیب باشد. در این صورت، $[A] := \{\alpha_1 + \alpha_2 + \cdots + \alpha_n : (\alpha_1, \alpha_2, \cdots \alpha_n) \in A^{<\mathbb{N}}\}$ نیز خوش‌ترتیب است و برای هر $\gamma \in [A]$ مجموعه‌ی $\{(\alpha_1, \cdots, \alpha_n) \in A^{<\mathbb{N}} : n \in \mathbb{N}, \alpha_1 + \cdots + \alpha_n = \gamma\}$ متناهی است.

اثبات. به صفحه‌ی ۲۳ کتابِ [۱۷] مراجعه کنید. □

نتیجه ۲۱.۳. فرض کنید $f \in k[[t^\Gamma]]$ به گونه‌ای باشد که $v(f) > 0$. در این صورت $\sum\limits_{n=0}^{\infty} f^n$ یک عنصر خوش‌تعریف در $k((t^\Gamma))$ است.

اثبات. ضریبِ t^γ در f^n به ازای یک n مشخص برابر است با مجموع nتا از ضرایبِ f با این ویژگی که مجموع اندیس‌های این ضرایب برابر با γ شود. با توجه به لم فوق، فقط تعداد متناهی تا عدد طبیعیِ n وجود دارد که می‌توان به تعداد آن‌ها از میان ضرایبِ f ضرایبی را یافت که مجموع اندیس‌های آن‌ها برابر با γ شود. در نتیجه فقط تعداد متناهی تا n وجود دارد که در آن‌ها ضریبِ t^γ در f^n ناصفر باشد.

توجه کنید که به ازای هر $\gamma \in \Gamma$، ضریب t^γ در $\sum\limits_{n=0}^{\infty} f^n$ برابر با مجموع ضرایبِ t^γ در هر f^n است. از آنجا که فقط تعداد متناهی‌تا n وجود دارد به طوری که ضریبِ t^γ در f^n ناصفر باشد، پس ضریب هر t^γ در $\sum\limits_{n=0}^{\infty} f^n$ تنها مجموع متناهی تا عنصر است. □

لم ۲۲.۳. فرض کنید k یک میدان و Γ یک گروه مرتب آبلی باشد. در این صورت، حوزه‌ی صحیحِ $k((t^\Gamma))$ یک میدان است.

اثبات. برای اثبات این لم، کافی است نشان دهیم که هر عنصر ناصفر در $k((t^\Gamma))$ یک عنصر وارون‌پذیر است.

فرض کنید $g \in k((t^\Gamma)) \setminus \{0\}$ یک عنصر دلخواه باشد. توجه کنید که می‌توان g را به صورتِ $ct^\gamma(1-f)$ نوشت که در آن $c \in k^\times$ و $v(f) > 0$. از آنجا که $v(f) > 0$، پس با توجه به نتیجه‌ی ۲۱.۳ داریم $\sum\limits_{n=0}^{\infty} f^n \in k((t^\Gamma))$. بوضوح $(1-f)\sum\limits_{n=0}^{\infty} f^n = (1+f+f^2+\cdots)-(f+f^2+\cdots) = 1$ و این یعنی $\sum\limits_{n=0}^{\infty} f^n$ وارونِ $1-f$ است. در نتیجه $g^{-1} = c^{-1}t^{-\gamma}(1-f)^{-1} = c^{-1}t^{-\gamma}\sum\limits_{n=0}^{\infty} f^n$. چون $c^{-1} \in k$ و نشان دادیم که $\sum\limits_{n=0}^{\infty} f^n \in k((t^\Gamma))$، پس g^{-1} نیز در $k((t^\Gamma))$ قرار دارد. □

نتیجه ۲۳.۳. فرض کنید k یک میدان و Γ یک گروه مرتب آبلی باشد. زوجِ $(k((t^\Gamma)), k[[t^\Gamma]])$ یک میدان ارزیابی است.

توجه ۲۴.۳. در حالتی که $\Gamma = \mathbb{Z}$ میدانِ $k((t^\mathbb{Z}))$، متشکل از سری‌های لوران روی میدان k است که آن را در بخش ۲.۲.۲ شرح دادیم.

نماد گذاری ۲۵.۳. در ادامه، میدان $k((t^\mathbb{Z}))$ را برای سادگی با نمادِ $k((t))$ نشان می‌دهیم.

لم ۲۶.۳. فرض کنید k یک میدان باشد. در این صورت میدان ارزیابی $(k((t)), k[[t]])$ یک میدان هنسلی است.

اثبات. در نتیجه‌ی ۲۴.۲ دیدیم که حلقه‌ی $k[[t]]$ هنسلی است، بنابراین $(k((t)), k[[t]])$ یک میدان هنسلی است. □

قضیه ۲۷.۳. فرض کنید k یک میدان و Γ یک گروه آبلی باشد. در این صورت میدان ارزیابیِ $(k((t^\Gamma)), k[[t^\Gamma]])$ هنسلی است.

اثبات. برای اثبات به صفحه‌ی ۲۴ جزوه‌ی [۱۷] مراجعه کنید. □

*** خلاصه‌ی فصل:**

اگر K یک میدان باشد، آنگاه $A \subseteq K$ را یک حلقه‌ی ارزیاب می‌نامیم هرگاه به ازای هر $x \in K$ یا $x \in A$ یا $x^{-1} \in A$. فرض کنید K یک میدان و Γ یک گروه مرتب باشد. نگاشت $v : K \to \Gamma$ یک نگاشت ارزیابی است هرگاه برای هر $x, y \in K$،

۱. $v(x+y) \geq \min\{v(x), v(y)\}$،

۲. $v(x \cdot y) = v(x) + v(y)$،

۳. $x = 0 \iff v(x) = \infty$.

مجموعه‌ی $O_v : \{x \in K : v(x) \geq 0\}$ یک حلقه‌ی موضعی با ایده‌آل ماکسیمالِ $m_v = \{x \in O_v : v(x) > 0\}$ و همچنین یک حلقه‌ی ارزیاب است. به ویژه برای هر حلقه‌ی ارزیابِ A در میدانِ K، یک گروه مرتب آبلیِ Γ و یک نگاشت ارزیابیِ $v : K \to \Gamma$ وجود دارد به طوری که $A = O_v$.

فرض کنید k یک میدان و Γ یک گروه مرتب آبلی باشد. در این صورت $k((t^\Gamma))$ میدان شامل سری‌هایی به صورت $f = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma$ است که اولاً $a_\gamma \in k$، ثانیاً $\mathrm{supp}(f) := \{\gamma \in \Gamma : a_\gamma \neq 0\}$ یک زیرمجموعه‌ی خوش‌ترتیب از Γ است. روی این میدان، یک نگاشت ارزیابی $v : k((t^\Gamma)) \to \Gamma$ تعریف می‌شود که هر $\sum_{\gamma \in \Gamma} a_\gamma t^\gamma$ از $k((t^\Gamma))$ را به $\min\{\gamma : a_\gamma \neq 0\}$ می‌برد. حلقه‌ی ارزیاب این نگاشت برابر است با $k[[t^\Gamma]] = \{x \in k((t^\Gamma)) : v(x) \geq 0\} = \{f : f\}$ توان منفی نداشته باشد و ایده‌آل ماکسیمال این حلقه، $tk[[t^\Gamma]]$ است و در این صورت میدان پیمانه‌ها برابر با k است.

فصل ۴

Vـ توپولوژی

منظور از یک میدان توپولوژیک، یک میدان است که روی آن یک توپولوژی وجود دارد که با آن توپولوژی، اعمال میدان، یعنی توابع جمع و ضرب و وارون‌گیری، پیوسته هستند. یک توپولوژی روی یک میدان را Vـ توپولوژی می‌نامیم هرگاه برای هر بازِ U حول نقطه‌ی صفر یک باز V حول نقطه‌ی صفر وجود داشته باشد، به طوری که

$$x \cdot y \in V \to (x \in U \vee y \in U).$$

به تعبیری، یک توپولوژی میدانی زمانی یک Vـ توپولوژی است که در آن حاصل‌ضرب دو عنصر که هیچکدام «کوچک» نیستند، عنصر کوچکی نشود. در مورد Vـ توپولوژی در بخش‌های پیش‌رو دقیق‌تر سخن گفته‌ایم.

وقتی روی یک میدان یک نگاشت ارزیابی (مانند تعریفِ ۱.۳) وجود داشته باشد، این نگاشت ارزیابی (همان‌گونه که توضیح خواهیم داد) منجر به ایجاد یک توپولوژی هاسدورف روی میدان می‌شود که تحت آن توپولوژی نیز اعمال میدان پیوسته هستند. این توپولوژی که به آن توپولوژی القاء شده توسط ارزیابی گفته می‌شود، مثال خاصی از یک Vـ توپولوژی است.

در این فصل، پس از معرفی دقیق میدان‌های توپولوژیک و توپولوژی القاء شده توسط یک نگاشت ارزیابی، خواهیم دید که در واقع یک توپولوژی روی یک میدان، Vـ توپولوژی است اگروتنهااگر توپولوژی القاء شده توسط یک ارزیابی یا توپولوژی القاء شده توسط یک نگاشت قدرمطلق باشد.

مطالب این فصل از کتاب [۶] گردآوری و بسط داده شده است.

۱.۴ میدان‌های توپولوژیک و Vـ توپولوژی

تعریف ۱.۴. دوتایی (K,τ) یک میدان توپولوژیک نامیده می‌شود هرگاه τ یک توپولوژی هاسدورف روی میدان K باشد که نسبت به آن اعمال میدان، یعنی نگاشت‌های ضرب و جمع و نگاشتی که هر عنصر را به وارون ضربی‌اش می‌برد، پیوسته است.

در ادامه، ادعا کرده‌ایم که برای شناساندن یک توپولوژی میدانی، کافی است یک پایه‌ی متشکل از همسایگی‌های حول صفر را در نظر بگیریم. علت این امر، این است که همسایگی‌های حول سایر نقاط، با انتقال همسایگی‌های حول صفر به دست می‌آیند. برای این منظور، در لم زیر نشان می‌دهیم که اگر U یک همسایگی باز صفر باشد، آنگاه $U+a$ به ازای هر $a\in K$ یک باز حول a است.

یادآوری ۲.۴. دو فضای توپولوژیک X و Y را در نظر بگیرید. پیوسته بودن یک نگاشت $f:X\to Y$ در یک نقطه‌ی $x\in X$ به این معناست که برای هر همسایگی حول $f(x)$ مانند U یک همسایگیِ W از x وجود داشته باشد به طوری که $f(W)\subset U$. می‌گوییم یک تابع $f:X\to Y$ پیوسته است هرگاه در تمام نقاطِ X پیوسته باشد؛ معادلاً تصویر وارون هر باز از Y، یک مجموعه‌ی باز در X باشد.

لم ۳.۴. فرض کنید (K,τ) یک میدان توپولوژیک باشد. اگر U یک همسایگی باز حول صفر و a یک عنصر از میدانِ K باشد، آنگاه $U+a$ یک همسایگی باز حول a است.

اثبات. می‌خواهیم نشان دهیم که تابعی که هر $x\in K$ را به $x-a$ می‌برد، پیوسته است. اولاً بوضوح تابع همانی، یعنی تابعی که هر $x\in K$ را به خودش می‌برد، یک تابع پیوسته است. ثانیاً تابع ثابتی که هر $x\in K$ را به عنصر $-a$ می‌برد یک تابع پیوسته است. از طرفی، به سادگی می‌توان نشان داد که حاصل جمع دو تابع پیوسته نیز یک تابع پیوسته است. بنابراین تابعی که هر $x\in K$ را به $x-a$ می‌برد، یک تابع پیوسته است. حال با توجه به پیوستگی این تابع، برای هر همسایگی باز حول صفرِ U مجموعه‌ی $f^{-1}(U)$ نیز باز خواهد بود. به عبارت دیگر، برای هر همسایگی باز حول صفرِ U گوی $U+a$ نیز باز است. $\square$

توجه ۴.۴. اگر τ یک توپولوژی میدانی باشد، آنگاه مجموعه‌ی متشکل از همسایگی‌های صفر در این توپولوژی را به یک فیلتر تبدیل می‌کنیم، یعنی به این مجموعه همه‌ی $U\subseteq K$ را که شامل حداقل یک همسایگی از صفر هستند اضافه می‌کنیم. با توجه به توضیحات قبلی، از این پس به جای توپولوژی میدانی τ روی یک میدان K، فیلتر مذکور را در نظر می‌گیریم ولی دوباره از همان نمادِ τ برای آن استفاده می‌کنیم. پس وقتی دوتایی (K,τ) را یک میدان توپولوژیک در نظر می‌گیریم، τ یک فیلتر است؛ یعنی شامل عناصر زیر است:

۱. همسایگی‌های صفر،

۲. زیرمجموعه‌های K که حداقل یک همسایگی صفر را شامل می‌شوند.

نماد گذاری ۵.۴. اگر A, B دو مجموعه باشند، آنگاه مجموعهٔ $\{x \cdot y : x \in A, y \in B\}$ را با نمادِ $A \cdot B$ و $\{x + y : x \in A, y \in B\}$ را با نمادِ $A \pm B$ نمایش می‌دهیم.

در ادامه وقتی می‌گوییم «همسایگی» منظورمان یک «همسایگی از صفر» است. در تعریف زیر با استفاده از آنچه که تا اینجا شرح دادیم یک میدان توپولوژیک را به صورت زیر بازتعریف می‌کنیم.

تعریف ۶.۴. فرض کنید K یک میدان و τ' یک توپولوژی روی K باشد. می‌گوییم (K, τ') یک میدان توپولوژیک است هرگاه فیلتر تولید شده توسط همسایگی‌های صفرِ τ در توپولوژی τ' شرایط زیر را برآورده کند:

۱. $\bigcap_{U \in \tau} U = \{0\}$،

۲. برای هر جفت $U, V \in \tau$ یک $W \in \tau$ وجود دارد به طوری که $W \subseteq U \cap V$،

۳. برای هر $U \in \tau$ یک $W \in \tau$ وجود دارد به طوری که $W \pm W \subseteq U$،

۴. برای هر $U \in \tau$ یک $W \in \tau$ وجود دارد به طوری که $W \cdot W \subseteq U$،

۵. برای هر $U \in \tau$ یک $W \in \tau$ وجود دارد به طوری که $(1 + W)^{-1} \subseteq 1 + U$.

به علاوه اگر τ شرط زیر را نیز برآورده کند، آنگاه به (K, τ') یک *میدان Vـ توپولوژیک* گفته می‌شود:

۶. برای هر $U \in \tau$ یک $V \in \tau$ وجود دارد به طوری که برای هر دو عنصر $x, y \in K$ داریم $x \cdot y \in V \rightarrow (x \in U \vee y \in U)$.

در ادامه، در مورد ماهیت هر یک از ویژگی‌های بالا توضیح می‌دهیم.

- **شرط ۱:** این شرط بیان می‌کند که τ یک توپولوژی هاسدورف است (البته همان‌طور که در ادامه خواهیم دید برای اثبات این موضوع لازم است از شرط‌های ۱ تا ۳ استفاده کنیم). قبل از اینکه به طور دقیق این ویژگی را بررسی کنیم تعریف یک توپولوژی هاسدورف را یادآوری می‌کنیم.

  یک توپولوژی τ هاسدورف است هرگاه در آن برای هر دو نقطه‌ی متفاوت x و y، یک همسایگی U از x و یک همسایگی V از y وجود داشته باشد به گونه‌ای که $U \cap V = \emptyset$. به بیان دیگر در توپولوژی هاسدورف می‌توان نقاط متفاوت را دو به دو با استفاده از همسایگی‌ها از یکدیگر جدا کرد.

  بوضوح شرط ۱ معادل با جمله‌ی $\underbrace{\forall x (x \neq 0 \rightarrow \exists V \; x \notin V)}_{*}$ است. حال دو عنصر متفاوت $x, y \in K$ را در نظر بگیرید. مطابق $*$ یک همسایگی U در τ وجود دارد به طوری که $x - y \notin U$ و مشابهاً یک همسایگی

$V \in \tau$ وجود دارد به طوری که $y - x \notin V$. بنا به ویژگی ۲ در تعریفِ ۶.۴، یک همسایگی $W \in \tau$ وجود دارد به طوری که $W \subseteq U \cap V$. بنابراین W شامل هیچ‌یک از دو عنصر $y - x$ و $x - y$ نیست. حال ویژگی ۳ در تعریف ۶.۴ را به کار می‌گیریم و گوی $W_1 \in \tau$ را به گونه‌ای انتخاب می‌کنیم که $W_1 - W_1 \subseteq W$ انتخاب می‌کنیم. قرار دهید $W_2 := W \cap W_1$. ادعا می‌کنیم که $W_2 + x$ و $W_2 + y$ به ترتیب همسایگی‌هایی از x و y هستند که با هم اشتراک ندارند.

در راستای اثبات این ادعا، ابتدا توجه کنید ویژگی ۲ تضمین می‌کند که W_2 ناتهی است و از آنجا که W_2 زیرمجموعه‌ی W است، پس شامل $y - x$ و شامل $x - y$ نیست. مجموعه‌ی $W_2 + y := \{u + y : u \in W_2\}$ یک همسایگی از y است، زیرا W_2 یک همسایگی از 0 است پس با جمع عناصر آن با y به یک همسایگی از y می‌رسیم. البته با انتخاب هوشمندانه‌ی W_2 به نحوی که شامل $x - y$ نباشد این شرط را نیز برآورده کردیم که همسایگی $W_2 + y$ شامل x نباشد. با استدلالی مشابه مجموعه‌ی $W_2 + x := \{v + x : v \in W_2\}$ یک همسایگی از x است که شامل y نیست.

همچنین، اشتراکِ $W_2 + x$ و $W_2 + y$ صفر است؛ زیرا در غیر این صورت یک عنصرِ t در $(W_2 + y) \cap (W_2 + x)$ وجود دارد که این نتیجه می‌دهد $t - y \in W_2$ و $t - x \in W_2$. حال مجموعه‌ی $W_2 - W_2 := \{u - v : u, v \in W_2\}$ را در نظر بگیرید. داریم

$$(t - y) - (t - x) = x - y \in W_2 - W_2 \subseteq W_1 - W_1 \subseteq W$$

که این تناقض است، زیرا $x - y \notin W$ و در نتیجه ادعای فوق ثابت می‌شود.

- **شرط ۳:** K^2 را با توپولوژی حاصل‌ضربیِ $\tau \times \tau$ در نظر بگیرید. می‌گوییم نگاشت $+$ بین دو فضای توپولوژیک K^2 و K پیوسته است هرگاه برای هر $U \in \tau$ یک همسایگی $V \times W \in \tau \times \tau$ وجود داشته باشد که $V + W \subseteq U$.

  در این صورت، برقراری ویژگی ۳ به معنی پیوسته بودن توابع $\pm : K^2 \to K$ است، زیرا این ویژگی بیان می‌کند برای هر $U \in \tau$ یک همسایگی $W \in \tau$ وجود دارد که $W - W \in U$. پس کافی است در بند قبل، به جای هر دوی W و V همسایگی W را در نظر بگیریم.

- **شرط ۴:** با استدلالی مشابه، ویژگی ۴ به معنای پیوسته بودن نگاشت ضرب است.

- **شرط ۵:** یک نکته‌ی قابل توجه در مورد شرط ۵ این است که برای بررسی پیوستگی نگاشتی که هر عنصر ناصفر را به وارون ضربی‌اش می‌برد، کافی است شرط پیوستگی را برای گوی‌های حول عنصر $1 \in K$ (یعنی همان $U + 1$ که U یک همسایگی صفر است) بررسی کنیم، زیرا اگر این نگاشت را f بنامیم و f بخواهد حول هر عنصر دلخواه $a \in K^\times$ پیوسته باشد، آنگاه $\frac{1}{a}f$ باید حولِ 1 پیوسته باشد.

توجه ۷.۴. اگر کوچک بودن یک عنصر را این‌گونه تعبیر کنیم که آن عنصر عضو یک همسایگی صفر باشد، آن‌گاه ویژگی ۶ بیانگر این است که اگر حاصل‌ضرب دو عنصر کوچک باشد، آن‌گاه حداقل یکی از فاکتورهای آن کوچک است.

توجه ۸.۴. در یک میدان توپولوژیکِ (K,τ) به ازای هر $x \in K^{\times}$ و $U \in \tau$ یک گوی $W \in \tau$ وجود دارد به طوری که $xW \subseteq U$. به بیان دیگر، اگر یک عنصر $x \in K$ را در نظر بگیریم، آن‌گاه مجموعه‌ی $\{xW : W \in \tau\}$ یک پایه برای همسایگی‌های حول صفر در τ است.

۱.۱.۴ توپولوژی میدانی القاء شده توسط یک نگاشت ارزیابی

در فصل ۳ با مفهوم یک نگاشت ارزیابِ v از یک میدان K به یک گروه مرتب آبلی Γ آشنا شدیم. در این بخش نشان می‌دهیم که یک نگاشت ارزیابی یک توپولوژی روی یک میدان القاء می‌کند که ویژگی‌های قابل توجهی دارد. برخی از این ویژگی‌ها را به تفصیل بررسی و اثبات کرده‌ایم و همچنین نشان خواهیم داد که این توپولوژی مثالی از یک Vـ توپولوژی است.

تعریف ۹.۴. نگاشت ارزیابی $v : K \to \Gamma$ را در نظر بگیرید. برای هر $\gamma \in \Gamma$ گوی باز به شعاعِ γ و مرکزِ a را با $U_\gamma(a)$ نشان می‌دهیم و آن را به صورت زیر تعریف می‌کنیم:

$$U_\gamma(a) := \{x \in K : v(x-a) > \gamma\}.$$

همچنین، مجموعه‌ی $\overline{U_\gamma}(a) := \{x \in K : v(x-a) \geq \gamma\}$ را گوی بسته حول عنصر a با شعاع $\gamma \in \Gamma$ می‌نامیم.

توجه ۱۰.۴. $\overline{U_\gamma}(a)$ بستارِ $U_\gamma(a)$ است.

نماد گذاری ۱۱.۴. توپولوژی ایجاد شده توسط بازهای پایه‌ای $U_\gamma(a)$ را با نمادِ τ_v نشان می‌دهیم.

توجه ۱۲.۴. هر انتقال گویِ $U_\gamma(0)$ به صورتِ $a + U_\gamma(0)$ برابر با گوی بازِ $U_\gamma(a)$ است.

قضیه ۱۳.۴. فرض کنید $v : K \to \Gamma$ یک نگاشت ارزیابی باشد. در این صورت (K,τ_v) یک میدان توپولوژیک است.

اثبات. باید نشان دهیم که فیلتر تولید شده توسطِ $\{U_\gamma(0) : \gamma \in \Gamma\}$ شرط‌های ۱ تا ۵ در تعریفِ ۶.۴ را برآورده می‌کند.

۱. اگر $x \in \bigcap_{\gamma\in\Gamma} U_\gamma(0)$، آن‌گاه به ازای هر $\gamma \in \Gamma$ داریم $v(x) > \gamma$ که این فقط در صورتی امکان‌پذیر است که x برابر با 0 باشد.

۲. دو گوی باز حول صفرِ $U_\gamma(0)$ و $U_\delta(0)$ را در نظر بگیرید. بدون کاستن از کلیت فرض کنید $\delta \geq \gamma$. در این صورت، به سادگی می‌توان نتیجه گرفت که $U_\delta(0) \subseteq U_\gamma(0)$. حال گوی باز $U_\eta(0)$ که در آن $\eta \geq \gamma$ را در نظر بگیرید. بنابراین داریم $U_\eta(0) \subseteq U_\gamma(0) \cap U_\delta(0) = U_\gamma(0)$. در واقع، هر گوی حول 0 که شعاع آن بیشتر از γ باشد زیرمجموعه‌ی $U_\gamma(0)$، یعنی زیرمجموعه‌ی $U_\gamma(0) \cap U_\delta(0)$ است.

۳. ادعا می‌کنیم که برای هر $U_\gamma(0)$ یک گوی $U_\delta(0)$ وجود دارد به طوری که $U_\delta(0) \pm U_\delta(0) \subseteq U_\gamma(0)$. برای اثبات این ادعا، کافی است δ را بزرگتر از γ انتخاب کنیم. در این صورت، اگر یک عنصر دلخواهِ t در $U_\delta(0) \pm U_\delta(0)$ در نظر بگیریم، آنگاه $t = m \pm n$ به طوری که $m, n \in U_\delta(0)$. بنابراین داریم $v(t) = v(m \pm n) \geq \min\{v(m), v(n)\} > \delta \geq \gamma$، پس $t \in U_\gamma(0)$.

۴. ادعا می‌کنیم که برای هر $U_\gamma(0)$ یک گوی باز $U_\delta(0)$ که در آن δ بزرگتر از $\gamma/2$ است، شرط $U_\delta(0) \cdot U_\delta(0) \subseteq U_\gamma(0)$ را برآورده می‌کند. برای اثبات این ادعا، یک عنصر دلخواهِ t در $U_\delta(0) \cdot U_\delta(0)$ در نظر بگیرید. در این صورت، به ازای $m, n \in U_\delta(0)$ داریم $t = m \cdot n$. بنابراین $v(t) = v(m \cdot n) = v(m) + v(n) > \gamma/2 + \gamma/2 = \gamma$ که نتیجه می‌دهد $t \in U_\gamma(0)$.

۵. ادعا می‌کنیم که به ازای هر گوی $U_\gamma(0)$ گوی $U_\delta(0)$ که در آن δ مثبت و بزرگتر از γ است در شرط $(1 + U_\delta(0))^{-1} \subseteq 1 + U_\gamma(0)$ صدق می‌کند. برای اثبات این ادعا کافی است نشان دهیم که به ازای هر t متعلق به $U_\delta(0)$، عنصرِ $\frac{1}{1+t} - 1$ در $U_\gamma(0)$ قرار دارد؛ به بیان دیگر باید نشان دهیم که $v(\frac{-t}{1+t})$ بزرگتر از γ است. توجه کنید که $v(\frac{-t}{1+t}) = v(-t) - v(1+t) = v(t) - v(1+t)$ و از آنجا که $v(t)$ بنا به فرض مثبت است، پس $v(\frac{-t}{1+t}) = v(t) - v(1+t) = v(t) - \min\{0, v(t)\} = v(t)$، در نتیجه $v(\frac{-t}{1+t}) = v(t) > \delta > \gamma$.

□

توپولوژی τ_v ویژگی‌های جالب توجهی دارد که در ادامه برخی از آن‌ها را اثبات کرده‌ایم.

۱. برای هر $b \in U_\gamma(a)$ داریم $U_\gamma(a) = U_\gamma(b)$.

اثبات. ابتدا می‌خواهیم نشان دهیم که $U_\gamma(a) \subseteq U_\gamma(b)$. یک عنصر دلخواه x در $U_\gamma(a)$ را در نظر بگیرید. بنا به تعریف گوی $U_\gamma(a)$، داریم $v(x-a) > \gamma$. از آنجا که بنا به فرض b در $U_\gamma(a)$ است، پس $v(b-a) > \gamma$ و بنابراین $v(x-b) = v(x-a+a-b) \geq \min\{v(x-a), v(a-b)\} > \gamma$، در نتیجه $x \in U_\gamma(b)$. گزاره‌ی $U_\gamma(b) \subseteq U_\gamma(a)$ نیز با استدلالی مشابه با استدلال فوق اثبات می‌گردد. □

۲. اگر $U_\gamma(a)$ و $U_\delta(b)$ دو گوی در این توپولوژی باشند که اشتراک ناتهی دارند، آنگاه یا $U_\gamma(a) \subseteq U_\delta(b)$ یا $U_\delta(b) \subseteq U_\gamma(a)$؛ به بیان دیگر گوی‌های باز با اشتراک ناتهی تشکیل یک زنجیر می‌دهند.

اثبات. بدون کاستن از کلیت فرض کنید $\gamma \geq \delta$. عناصر دلخواه $x \in U_\delta(b) \cap U_\gamma(a)$ و $t \in U_\gamma(a)$ را در نظر بگیرید. بنا به تعریف گوی‌های باز در توپولوژی τ_v داریم $v(t-x) = v(t-a+a-x) \geq \min\{v(t-a), v(a-x)\} > \gamma \geq \delta$، در نتیجه $v(t-x) > \delta$. از طرفی، $v(t-b) = v(t-x+x-b) \geq \min\{v(t-x), v(x-b)\} > \delta$، پس $t \in U_\delta(b)$ و بنابراین نتیجه می‌شود که $U_\gamma(a) \subseteq U_\delta(b)$. $\square$

۳. در این توپولوژی هر گوی $U_\gamma(a)$ و $\overline{U_\gamma(a)}$ هم یک مجموعه‌ی باز است هم یک مجموعه‌ی بسته.

اثبات. می‌خواهیم اثبات کنیم که یک گوی باز ِ $U_\gamma(a)$، یک مجموعه‌ی بسته هم هست. به این منظور، کافی است نشان دهیم مکمل آن نیز یک مجموعه‌ی باز است. ادعا می‌کنیم $\{x : v(x-a) \leq \gamma\} = \bigcup_{v(b-a)\leq\gamma} U_{v(b-a)}(b)$. برای اثبات این ادعا، فرض کنید $t \in \{x : v(x-a) \leq \gamma\}$. در این صورت، $v(t-a) \leq \gamma$ و از آنجا که بوضوح $t \in U_{v(t-a)}(t)$، پس نتیجه می‌شود که $\{x : v(x-a) \leq \gamma\} \subseteq \bigcup_{v(b-a)\leq\gamma} U_{v(b-a)}(b)$.

حال یک عنصر t در $\bigcup_{v(b-a)\leq\gamma} U_{v(b-a)}(b)$ را در نظر بگیرید. در این صورت یک گوی به مرکز ِ b' و شعاع $v(b'-a)$ که شرط $v(b'-a) \leq \gamma$ را برآورده می‌کند وجود دارد به طوری که t متعلق به آن است. بنابراین $v(t-b') > v(b'-a)$ و در نتیجه داریم:

$$v(t-a) = v(t-a+b'-b') = \min\{v(t-b'), v(b'-a)\} = v(b'-a)$$

پس $v(t-a) = v(b'-a) \leq \gamma$ و از این رو $t \in \{x : v(x-a) \leq \gamma\}$، در نتیجه $\bigcup_{v(b-a)\leq\gamma} U_{v(b-a)}(b) \subseteq \{x : v(x-a) \leq \gamma\}$.

بنابراین نشان دادیم که مکمل یک گوی باز را می‌توانیم به صورت اجتماع گوی‌های باز بنویسیم و این نتیجه می‌دهد که هر گوی باز یک مجموعه‌ی بسته است. به روش مشابه می‌توان نشان داد که هر گوی بسته‌ی $\overline{U_\gamma(a)} = \{x : v(x-a) \geq \gamma\}$ برابر با $\bigcup_{v(b-a)\geq\gamma} U_{v(b-a)}(b)$ و بنابراین یک مجموعه‌ی باز است. $\square$

قضیه ۱۴.۴. τ_v یک Vـ توپولوژی است.

اثبات. برای یک گوی باز دلخواه $U_\gamma(0)$، گوی باز $V = U_{2\gamma}(0)$ در تعریف Vـ توپولوژی صدق می‌کند، زیرا اگر $v(x \cdot y) > 2\gamma$ آنگاه $v(x) + v(y) > 2\gamma$ و در نتیجه یا $v(x) > \gamma$ یا $v(y) > \gamma$؛ یعنی یا x یا y در $U_\gamma(0)$ قرار دارد. $\square$

۲.۱.۴ توپولوژی میدانی القاء شده توسط یک قدرمطلق

ممکن است توپولوژی روی یک میدان توسط یک نگاشت قدرمطلق القاء شده باشد. خواهیم دید که این توپولوژی مثال دیگری از یک Vـ توپولوژی است.

تعریف ۱۵.۴. منظور از یک نگاشت قدرمطلق [1] روی یک میدان K نگاشتِ $|\ | : K \to \mathbb{R}^+$ است که سه ویژگی زیر را دارد:

۱. $|x| = 0$ اگروتنهااگر $x = 0$،

۲. $|x \cdot y| = |x| \cdot |y|$،

۳. $|x + y| \leq |x| + |y|$.

اگر نگاشت قدرمطلق فوق، شرط $|x + y| \leq \max\{|x|, |y|\}$ را، که شرط قوی‌تری نسبت به شرط ۳ است، برآورده کند به آن یک قدرمطلقِ *غیر ارشمیدسی* و در غیر این صورت یک قدرمطلق *ارشمیدسی* نامیده می‌شود.

تعریف ۱۶.۴. فرض کنید K یک میدان و $|\ |$ یک قدرمطلق روی آن باشد. در این صورت $|\ |$ روی K یک توپولوژی القاء می‌کند که بازهای پایه‌ای آن به صورت $B(a, r) := \{x \in K \mid |x - a| < r\}$ برای هر $r \in \mathbb{R}^+$ و $a \in K$ هستند. این توپولوژی را با $\tau_{||}$ نشان می‌دهیم.

قضیه ۱۷.۴. اگر K یک میدان و $||$ یک قدرمطلق روی آن باشد، آنگاه $(K, \tau_{||})$ یک میدان توپولوژیک است.

اثبات. باید نشان دهیم که فیلتر تولید شده توسطِ $\{B(0, r) : r \in \mathbb{R}^+\}$ شرط‌های ۱ تا ۵ در تعریفِ ۶.۴ را برآورده می‌کند.

۱. اشتراک همه‌ی بازهای حول صفر در این توپولوژی برابر با عنصر 0 است، زیرا تنها زمانی x در اشتراک تمامی بازهای حول صفر قرار می‌گیرد که به ازای هر $r \in \mathbb{R}^+$ داشته باشیم $|x| < r$. به بیان دیگر x باید عنصر بی نهایت کوچک باشد. اما اعداد حقیقی دارای خاصیت ارشمیدسی است و چنین عنصری در آن وجود ندارد. بنابراین $|x| = 0$ و بنا به ویژگی ۱ در تعریفِ ۱۵.۴ داریم $x = 0$.

۲. برای هر دو باز $B(0, r_1)$ و $B(0, r_2)$ که $r_1 < r_2$ داریم $B(0, r_1) \cap B(0, r_2) = B(0, r_1)$، بنابراین هر گوی حول صفر با شعاع کمتر از r_1 زیرمجموعه‌ی اشتراک دو گوی $B(0, r_1)$ و $B(0, r_2)$ است.

۳. نگاشت جمع پیوسته است، زیرا به ازای هر باز حول 0 مانند $B(0, r)$ باز $B(0, r/2)$ ویژگی مطلوبِ $B(0, r/2) + B(0, r/2) \subseteq B(0, r)$ را دارد.

[1] absolute value

۴. نگاشت ضرب نیز پیوسته است، چون به ازای هر گوی حول صفرِ $B(0,r)$، گوی باز $B(0,\sqrt{r})$ در شرط $B(0,\sqrt{r})\cdot B(0,\sqrt{r})\subseteq B(0,r)$ صدق می‌کند.

۵. می‌خواهیم نشان دهیم که برای هر بازِ $B(0,r)$، خودِ بازِ $B(0,r)$ در شرطِ $(1+B(0,r))^{-1}\subseteq 1+B(0,r)$ صدق می‌کند. به این منظور، یک عنصر دلخواهِ x را در $(1+B(0,r))^{-1}$ در نظر بگیرید. در این صورت $x=\frac{1}{1+t}$ که در آن $|t|<r$. ادعا می‌کنیم که $|\frac{1}{1+t}|<1+r$ یا به بیان دیگر $1<(1+r)|1+t|$. از آنجا که داریم

$$1<|1+t|(1+r)\leq(1+|t|)(1+r)<(1+r)(1+r)=r^2+2r+1$$

و r یک عدد حقیقی مثبت است، پس نامساوی فوق برقرار است و در نتیجه $x\in 1+B(0,r)$.

□

لم ۱۸.۴. $\tau_{||}$ یک Vـ توپولوژی است.

اثبات. به ازای هر گوی بازِ $B(0,r)$ گوی $B(0,r^2)$ دارای این ویژگی است که برای $x,y\in K$ اگر $x\cdot y\in B(0,r^2)$ آن‌گاه $x\in B(0,r)$ یا $y\in B(0,r)$، زیرا اگر $|x\cdot y|=|x|\cdot|y|<r^2$ آن‌گاه $|x|<r$ یا $|y|<r$. □

۲.۴ دسته بندی Vـ توپولوژی

در دو بخش قبلی نشان دادیم که $\tau_{||}$ و τ_v هر دو Vـ توپولوژی هستند؛ اما در ادامه می‌خواهیم اثبات کنیم که اساساً Vـ توپولوژی دیگری به غیر از توپولوژی‌های به صورتِ $\tau_{||}$ و τ_v وجود ندارد:

قضیه ۱۹.۴. اگر K یک میدان و τ یک توپولوژی روی آن باشد، آنگاه τ یک Vـ توپولوژی است اگروتنهااگر یک نگاشت قدرمطلق ارشمیدسی و یا یک نگاشت ارزیابی روی K وجود داشته باشد به گونه‌ای که توپولوژی القاء شده توسط آن برابر τ باشد.

ادامه‌ی این فصل به اثبات قضیه‌ی فوق اختصاص دارد. ابتدا در یک میدان Vـ توپولوژیک، مجموعه‌ی عناصر پوچ‌توان را تعریف خواهیم کرد. به طور خلاصه، یک عنصر ناصفرِ x در صورتی پوچ‌توان است که دنباله‌ی $(x^n)_{n\in\mathbb{N}}$ یک دنبالهٔ همگرا به صفر باشد. سپس، نشان خواهیم داد که میدان‌های دارای Vـ توپولوژی دو دسته هستند؛ آن‌هایی که هیچ عنصر پوچ‌توانی ندارند و آن‌هایی که دارای حداقل یک عنصر پوچ‌توان هستند. میدان‌های دسته‌ی اول دارای یک نگاشت ارزیابی و میدان‌های دستهٔ دوم دارای یک نگاشت قدرمطلق هستند که توپولوژی روی آن‌ها را القاء می‌کند.

۱.۲.۴ رتبه‌ی گروه‌های آبلی مرتب

برای اثبات قضیه‌ی ۱۹.۴، نیاز به یک قضیه داریم که بیان می‌کند هر گروه مرتب آبلی از رتبه‌ی 1 ایزومورف ترتیبی با یک زیرگروه نابدیهی از $(\mathbb{R}, +, 0, \leq)$ است. در این بخش، با هدف اثبات این قضیه، مفاهیمی مانند مجموعه‌ی محدب، ترتیب ارشمیدسی و در نهایت، رتبه‌ی یک گروه مرتب را معرفی و برخی قضایای مربوط با آن‌ها را اثبات می‌کنیم.

در بخش‌های گذشته، از گروه‌های مرتب آبلی در قسمت‌های مختلفی استفاده کرده‌ایم؛ حال در این بخش، قصد داریم دسته‌ی خاصی از آن‌ها به نام گروه‌های مرتبه ۱ را معرفی و بررسی کنیم. به این منظور ابتدا تعریف دقیق این گروه‌ها را یادآوری می‌کنیم:

تعریف ۲۰.۴. هرگاه می‌گوییم Γ یک گروه مرتب آبلی است در واقع منظورمان این است که $(\Gamma, +, 0)$ یک گروه آبلی با یک محمول دوتایی $\leq$ است به طوری که برای هر $\gamma, \delta, \lambda \in \Gamma$، ویژگی‌های زیر برقرار است:

۱. $\gamma \leq \gamma$،

۲. $\gamma \leq \delta, \delta \leq \gamma \Longrightarrow \gamma = \delta$،

۳. $\gamma \leq \delta, \delta \leq \lambda \Longrightarrow \gamma \leq \lambda$،

۴. $\gamma \leq \delta$ یا $\delta \leq \gamma$،

۵. $\gamma \leq \delta \Longrightarrow \gamma + \lambda \leq \delta + \lambda$.

چهار شرط اول بیان می‌کنند که $\leq$ یک ترتیب خطی روی Γ است. شرط ۵ بیانگر یکنوایی این ترتیب نسبت به عمل جمع است.

تعریف ۲۱.۴. یک زیرگروه Δ از یک گروه آبلی مرتب Γ را محدب [2] می‌نامیم هرگاه به ازای $\gamma \in \Gamma$ و $\delta \in \Delta$ اگر $\delta \leq \gamma \leq 0$ آن‌گاه γ نیز متعلق به Δ باشد.

تعریف ۲۲.۴. تعداد زیرگروه‌های محدب یک گروه مرتب آبلیِ Γ را مرتبه‌ی آن می‌نامیم. در حالت خاص، در صورتی که $\{0\}$ تنها زیرگروه محدب Γ باشد می‌گوییم Γ از مرتبه‌ی 1 است.

تعریف ۲۳.۴. یک ترتیب $\leq$ روی یک گروه مرتب آبلی Γ ارشمیدسی نامیده می‌شود هرگاه شرط زیر را برآورده کند:

برای هر γ و هر $\epsilon > 0$ در Γ یک عدد طبیعی $n \in \mathbb{N}$ وجود داشته باشد به طوری که $\gamma \leq n\epsilon$.

[2] convex

لم ۲۴.۴. هر گروه آبلی با ترتیب ارشمیدسی دارای رتبه‌ی 1 است.

اثبات. یک گروه آبلی و مرتب ارشمیدسیِ Γ را در نظر بگیرید. با برهان خلف فرض کنید که رتبه‌ی Γ برابر با 1 نیست، یعنی یک زیرگروه سره‌ی محدب نابدیهیِ Δ در Γ وجود دارد. حال توجه کنید که چون Γ یک گروه مرتب ارشمیدسی است، پس برای هر عنصر مثبتِ γ در $\Gamma \setminus \Delta$ و عنصر مثبتِ δ در Δ یک عدد طبیعی n وجود دارد به طوری که $0 \leq \gamma \leq n\delta$. از آنجا که Δ یک زیرگروهِ Γ است، پس نسبت به عمل گروه، یعنی $+$ بسته است و بنابراین از اینکه δ متعلق به Δ است نتیجه می‌شود که $n\delta$ نیز در Δ قرار دارد. به علاوه چون Δ یک زیرگروه محدب است، نتیجه می‌شود که $\gamma \in \Delta$ و این یعنی $\Delta = \Gamma$ که با فرض زیرگروه سره بودنِ Δ متناقض است. $\square$

برعکس قضیه‌ی فوق نیز درست است.

قضیه ۲۵.۴. هر گروه مرتب آبلی که دارای رتبه‌ی 1 است ویژگی ارشمیدسی دارد.

اثبات. می‌خواهیم اثبات کنیم برای یک عنصر مثبتِ ϵ در Γ و هر $\gamma \in \Gamma$، یک عدد طبیعی n وجود دارد به طوری که $\gamma, -\gamma < n\epsilon$. به این منظور، مجموعه‌ی $\Delta := \{\gamma \in \Gamma : \gamma \ , -\gamma \leq n\epsilon, n \in \mathbb{N}\}$ را در نظر بگیرید. ادعا می‌کنیم که این مجموعه یک زیرگروه محدب از Γ است. در راستای اثبات این ادعا، ابتدا نشان می‌دهیم که Δ یک زیرگروه از Γ است. بوضوح $0 \in \Delta$ و اگر $\gamma \in \Delta$ آنگاه $-\gamma \in \Delta$. حال دو عنصرِ γ_1 و γ_2 را در Δ در نظر بگیرید. در این صورت، اعداد طبیعی n_1 و n_2 وجود دارند به طوری که به ترتیب $\gamma_1 < n_1\epsilon \ , \ -\gamma_1$ و $\gamma_2 < n_2\epsilon \ , \ -\gamma_2$ و در نتیجه $(\gamma_1 + \gamma_2) < (n_1 + n_2)\epsilon \ , \ -(\gamma_1 + \gamma_2)$، بنابراین Δ تحت عمل $+$ بسته است. از این رو، Δ یک زیرگروه از Γ است.

محدب بودن این مجموعه نیز با توجه به نحوه‌ی تعریف آن بوضوح قابل استنباط است. بنابراین Δ یک زیرگروه محدب از Γ است. توجه کنید که Γ دارای رتبه‌ی 1 است، پس یا $\Delta = \{0\}$ یا $\Delta = \Gamma$؛ اما از آنجا که بوضوح عنصر مثبتِ ϵ در Δ قرار دارد، پس $\Delta \neq \{0\}$ و بنابراین $\Delta = \Gamma$. در نتیجه Γ دارای خاصیت ارشمیدسی است. $\square$

قضیه‌ی بعدی شرط لازم و کافی برای رتبه یک بودن یک گروه مرتب آبلی را بیان می‌کند.

قضیه ۲۶.۴. یک گروه آبلی مرتب Γ از رتبه‌ی 1 است اگروتنهااگر ایزومورف ترتیبی با یک زیرگروه نابدیهی از $(\mathbb{R}, +, 0, \leq)$ با همان ترتیب متعارف $\mathbb{R}$ باشد.

قبل از اینکه به اثبات این قضیه بپردازیم یادآوری می‌کنیم که دو مجموعه‌ی مرتب A و B ایزومورف ترتیبی هستند اگر یک تابع دوسویی مانند $f : (A, <_A) \to (B, <_B)$ وجود داشته باشد به طوری که برای هر دو عنصر a_1و a_2 در A داشته باشیم $a_1 <_A a_2$ اگروتنهااگر $f(a_1) <_B f(a_2)$، یعنی نگاشت f حافظ ترتیب باشد.

اثبات. اثبات این قضیه در چند مرحله انجام می‌شود.

- **مرحله‌ی اول:** همان‌طور که در قضیه‌ی ۲۵.۴ دیدیم، هر گروه مرتبه‌ی 1 دارای خاصیت ارشمیدسی است. برای ادامه، یک عنصر مثبتِ ϵ را در Γ در نظر بگیرید.

- **مرحله‌ی دوم:** برای هر $\alpha \in \Gamma$ دو مجموعه‌ی زیر را تعریف می‌کنیم:

$$L(\alpha) := \{m/n \in \mathbb{Q} : n > 0, m\epsilon \leq n\alpha\} \quad \text{و} \quad U(\alpha) := \{m/n \in \mathbb{Q} : n > 0, m\epsilon \geq n\alpha\}$$

ادعا می‌کنیم که برای هر $\alpha \in \Gamma$ موارد زیر برقرارند:

۱. $L(\alpha) \cup U(\alpha) = \mathbb{Q}$،

۲. $U(\alpha) \neq \emptyset$ و $L(\alpha) \neq \emptyset$،

۳. اگر $\beta \in L(\alpha)$ و $\beta' \in U(\alpha)$ آن‌گاه $\beta \leq \beta'$.

در واقع، این ادعا به این معناست که $L(\alpha)$ و $U(\alpha)$ یک برش ددِکیند در $\mathbb{Q}$ است. در ادامه، ۴ ادعای فوق را به ترتیب ثابت می‌کنیم.

۱. از آنجا که Γ یک گروه مرتب است، پس $m\epsilon \leq n\alpha$ یا $m\epsilon \geq n\alpha$. بنابراین هر $m/n \in \mathbb{Q}$ یا در $L(\alpha)$ است یا در $U(\alpha)$ ، پس $L(\alpha) \cup U(\alpha) = \mathbb{Q}$.

۲. اگر $U(\alpha) = \emptyset$ آن‌گاه با توجه به قسمت ۱ داریم $L(\alpha) = \mathbb{Q}$، پس به ازای هر $m \in \mathbb{Z}$ داریم $m\epsilon \leq \alpha$؛ اما این با ارشمیدسی بودن Γ (که در مرحله اول اثبات کردیم) در تناقض است، پس $U(\alpha) \neq \emptyset$. به طور مشابه می‌توان اثبات کرد که $L(\alpha) \neq \emptyset$.

۳. می‌خواهیم اثبات کنیم که اگر $m/n \in L(\alpha)$ و $m'/n' \in U(\alpha)$ آن‌گاه $m/n \leq m'/n'$. بنا به تعریفِ $U(\alpha)$ و $L(\alpha)$ داریم $m\epsilon \leq n\alpha$ و $m'\epsilon \geq n'\alpha$. با ضرب این دو نامساوی به ترتیب در n' و n و کنار هم قرار دادن آن‌ها به $mn'\epsilon \leq nn'\alpha = n'n\alpha \leq m'n\epsilon$ می‌رسیم. با توجه به اینکه ϵ یک مقدار مثبت است، می‌توان آن را از طرفین این نامساوی حذف کرد، پس داریم $mn' \leq m'n$ و این همان نتیجه مطلوب ماست، یعنی $m/n \leq m'/n'$.

- **مرحله‌ی سوم:** نگاشت $r : \Gamma \to \mathbb{R}$ با این ضابطه که هر $\alpha \in \Gamma$ را به عدد حقیقی متناظر با برش ددکیند $L(\alpha)$ و $U(\alpha)$ ببرد، را در نظر بگیرید. در ادامه، اثبات می‌کنیم که این نگاشت، یک نشاندن یعنی هومومورفیسمی یک به یک است.

این نگاشت، ترتیب را حفظ می‌کند، زیرا بوضوح از اینکه $\alpha \leq \beta$ نتیجه می‌شود که $r(\alpha) \leq r(\beta)$. حال می‌خواهیم نشان دهیم که نگاشتِ r عملِ $+$ را نیز حفظ می‌کند. به این منظور، دو عنصر $m/n \in L(\alpha)$ و $m'/n' \in L(\beta)$ را در نظر بگیرید. توجه کنید که می‌توانیم از ابتدا، بدون کاستن از کلیت، فرض کنیم $n = n'$

زیرا به جای دو کسر فوق، می‌توانیم mn'/nn' و nm'/nn' را در نظر بگیریم که اولاً $m/n = mn'/nn'$ و $m'/n' = nm'/nn'$، ثانیاً مخرج این دو کسر با هم برابر هستند. حال از آنجا که $m\epsilon \leq n\alpha$ و $m'\epsilon \leq n\beta$، پس $(m+m')\epsilon \leq n(\alpha+\beta)$؛ یعنی $(m+m')/n \in L(\alpha+\beta)$ و از این به سادگی می‌توان نتیجه گرفت که $r(\alpha+\beta) \geq r(\alpha)+r(\beta)$ (در واقع تنها کافی است $L(\alpha)+L(\beta) \subseteq L(\alpha+\beta)$ را تحلیل کنیم!). به طور مشابه می‌توان نتیجه گرفت که $U(\alpha)+U(\beta) \subseteq U(\alpha+\beta)$، پس $r(\alpha+\beta) \leq r(\alpha)+r(\beta)$ و در نتیجه $r(\alpha+\beta) = r(\alpha)+r(\beta)$.

- **مرحله‌ی چهارم:** نهایتاً می‌خواهیم نشان دهیم که نگاشتِ r یک به یک است؛ به بیان دیگر $\ker(r) = 0$. فرض کنید به ازای یک α در Γ داریم $r(\alpha) = 0$. در این صورت، به ازای هر $n > 0$ عنصرِ $-1/n$ در $L(\alpha)$ و $1/n$ در $U(\alpha)$ قرار دارد، بنابراین $-\epsilon \leq n\alpha \leq \epsilon$. اما از آنجا که گروه Γ خاصیت ارشمیدسی دارد نتیجه می‌شود که $\alpha = 0$.

$\square$

تعریف ۲۷.۴. فرض کنید $v : K \to \Gamma$ یک نگاشت ارزیابی باشد. رتبه‌ی نگاشت ارزیابیِ v را همان رتبه‌ی گروه ارزیابیِ Γ تعریف می‌کنیم.

۲.۲.۴ مجموعه‌های کراندار

در این بخش مفهوم مجموعه‌های کراندار و کراندار دور از صفر را در یک میدان توپولوژیک معرفی می‌کنیم و نشان می‌دهیم که یک توپولوژی روی یک میدان، زمانی Vـ توپولوژی است که کراندار بودن هر مجموعه‌ی S در آن معادل با کراندار دور از صفر بودن مجموعه‌ی $S^{-1} = \{\frac{1}{x} : x \in S\}$ باشد.

لم ۲۸.۴. اگر (K,τ) یک میدان Vـ توپولوژیک باشد، آنگاه یک گویِ U در τ موجود است به طوری که $K^\times = (K/U) \cup (K/U)^{-1}$.

اثبات. با برهان خلف فرض کنید به ازای هر $W \in \tau$ مجموعه‌ی $K^\times$ برابر با $(K/W)\cup(K/W)^{-1}$ نباشد؛ به عبارت دیگر به ازای هر $W \in \tau$ یک عنصر $x_W \in K^\times$ وجود دارد به طوری که $x_W \notin (K/W)$ و $x_W \notin (K/W)^{-1}$، بنابراین $x_W, x_W^{-1} \in W$. از آنجا که τ طبق فرض یک Vـ توپولوژی است، پس بنا به ویژگی ۴ در تعریفِ ۶.۴ برای هر $U \in \tau$ یک گویِ W در τ وجود دارد به طوری که $W \cdot W \subseteq U$ و از این رو $1 = x_W \cdot x_W^{-1} \in U$. بنابراین 1 عضو همه‌ی گوی‌ها است که این با شرط ۱ در تعریفِ ۶.۴ در تناقض است. $\square$

تعریف ۲۹.۴ (مجموعه‌ی کراندار). میدان توپولوژیکِ (K,τ) را در نظر بگیرید. یک زیرمجموعه‌ی S از میدان K را *کراندار* می‌نامیم هرگاه برای هر $U \in \tau$ یک $V \in \tau$ وجود داشته باشد به طوری که $V \cdot S \subseteq U$.

لم ۳۰.۴. فرض کنید $v : K \to \Gamma$ یک نگاشت ارزیابی و (K, τ_v) یک میدان توپولوژیک باشد که در آن τ_v یک توپولوژی القاء شده توسط نگاشتِ v روی K است. در این صورت، $S \subseteq K$ کراندار است اگروتنهااگر $v(S) = \{v(s) : s \in S\}$ یک مجموعه‌ی از پایین کراندار باشد.

اثبات. فرض کنید یک عنصرِ r در Γ وجود دارد به طوری که عناصر مجموعه‌ی $v(S) = \{v(s) : s \in S\}$ همگی از آن بیشتر باشند. در این صورت به سادگی می‌توان دید که به ازای هر گوی $U_\gamma(0)$ در این توپولوژی، یک گوی $U_{\gamma-r}(0)$ وجود دارد به طوری که $U_{\gamma-r}(0) \cdot S \subseteq U_\gamma(0)$ و با توجه به تعریفِ ۲۹.۴ نتیجه می‌گیریم که S یک مجموعه‌ی کراندار است.

برای اثبات جهت عکس، فرض کنید $S \subseteq K$ یک مجموعه‌ی کراندار باشد. بنابراین با توجه به تعریفِ ۲۹.۴ به ازای هر $U_\gamma(0) \in \tau_v$ یک گویِ $U_\delta(0)$ در τ وجود دارد به طوری که $U_\delta(0) \cdot S \subseteq U_\gamma(0)$. در نتیجه به ازای هر $u \in U_\delta(0)$ و $s \in S$ داریم $v(u \cdot s) > \gamma$، پس $v(u) + v(s) > \gamma$ و بنابراین $v(s) > \gamma - v(u)$، به این ترتیب مجموعه‌ی $v(S)$ از پایین کراندار است. $\square$

لم زیر ما را در شناخت مجموعه‌های کراندار یاری می‌رساند و برخی از ویژگی‌های آن را بیان می‌کند:

لم ۳۱.۴.

۱. مجموعه‌ی M کراندار است اگروتنهااگر برای هر $U \in \tau$ یک عنصر x در $K^\times$ وجود داشته باشد به طوری که $xM \subseteq U$.

۲. اگر M یک مجموعه‌ی متناهی باشد، آنگاه M کراندار است.

۳. اگر $N \subseteq M$ و M کراندار باشد، آنگاه N نیز کراندار است.

۴. اگر مجموعه‌های M و N کراندار باشند، آنگاه $M \pm N, M \cdot N$ نیز کراندار هستند.

اثبات. ۱. اگر M یک مجموعه‌ی کراندار باشد، آنگاه بوضوح بنا به تعریف یک مجموعه‌ی کراندار، برای هر $U \in \tau$ یک عنصرِ x در $K^\times$ وجود دارد به طوری که $xM \subseteq U$.

برای اثبات جهت عکس، یک گوی دلخواه U در τ را در نظر بگیرید. ابتدا توجه کنید که بنا به ویژگی ۴ در تعریفِ ۶.۴، یک گوی V در τ وجود دارد به طوری که $V \cdot V \subseteq U$. همچنین، طبق فرض به ازای گویِ V یک عنصر x در $K^\times$ وجود دارد به طوری که $xM \subseteq V$، پس داریم $V \cdot xM \subseteq V \cdot V \subseteq U$. از طرفی، بنا به ۸.۴ برای گوی V و عنصر x^{-1}، یک گوی $W \in \tau$ وجود دارد به طوری که $Wx^{-1} \subseteq V$. در نتیجه داریم $W \cdot M \subseteq VxM \subseteq V \cdot V \subseteq U$، بنابراین M یک مجموعه‌ی کراندار است.

درستی ۲ و ۳ به سادگی قابل بررسی است.

اثبات ۴. یک گوی دلخواهِ U در τ در نظر بگیرید. بنا به ویژگی ۳ در تعریفِ ۶.۴، گوی‌های V_1 و V_2 در τ وجود دارند به طوری که $V_1 \pm V_1 \subseteq U$ و $V_2 \pm V_2 \subseteq U$. همچنین، یک گویِ V در τ وجود دارد به طوری که $V \subseteq V_1 \cap V_2$، بنابراین $V \pm V \subseteq U$. از آنجا که بنا به فرض M و N کراندار هستند، پس به ترتیب گوی‌های W_1 و W_2 وجود دارند به طوری که $W_1 \cdot M \subseteq V$ و $W_2 \cdot N \subseteq V$. حال یک گویِ W در τ را به گونه‌ای انتخاب می‌کنیم که $W \subseteq W_1 \cap W_2$، پس داریم $W \cdot (M \pm N) \subseteq W_1 \cdot M \pm W_2 \cdot N \subseteq V \pm V \subseteq U$ و این کرانداری $M \pm N$ را نتیجه می‌دهد.

حال می‌خواهیم کرانداری $M \cdot N$ را اثبات کنیم. از آنجا که N و M مجموعه‌های کرانداری هستند، پس اولاً برای گوی دلخواهِ U در τ یک گوی V متعلق به τ وجود دارد به طوری که $V \cdot N \subseteq U$، ثانیاً به ازای گوی V یک گوی W وجود دارد به طوری که $W \cdot M \subseteq V$، بنابراین داریم $W \cdot (M \cdot N) \subseteq V \cdot N \subseteq U$ و این کرانداریِ $M \cdot N$ را نتیجه می‌دهد. $\square$

لم ۳۲.۴. به ازای هر $W \in \tau$ مجموعه‌ی $(K \setminus W)^{-1}$ کراندار است اگروتنهااگر یک گویِ V در τ وجود داشته باشد به طوری که $V \cdot (K \setminus W)^{-1} \subseteq W$.

اثبات. فرض کنید به ازای هر $W \in \tau$ یک گوی V در τ وجود دارد به طوری که $V \cdot (K \setminus W)^{-1} \subseteq W$. می‌خواهیم اثبات کنیم که $(K \setminus W)^{-1}$ کراندار است. در راستای این کار، یک گوی دلخواه $U \in \tau$ را در نظر بگیرید. از آنجا که $(K \setminus W) \subseteq (K \setminus W \cap U)$، پس $(K \setminus W)^{-1} \subseteq (K \setminus W \cap U)^{-1}$ و بنابراین با توجه به فرض داریم: $V \cdot (K \setminus W)^{-1} \subseteq V \cdot (K \setminus W \cap U)^{-1} \subseteq W \cap U \subseteq U$. پس بنا به تعریفِ ۲۹.۴، $(K \setminus W)^{-1}$ کراندار است.

اثبات جهت عکس بنا به تعریف یک مجموعه‌ی کراندار واضح است. $\square$

قضیه ۳۳.۴. (K, τ) یک میدان Vـ توپولوژیک است اگروتنهااگر برای هر $W \in \tau$، مجموعه‌ی $(K \setminus W)^{-1}$ کراندار باشد.

اثبات. فرض کنید τ یک Vـ توپولوژی باشد. می‌خواهیم نشان دهیم که به ازای هر $W \in \tau$ مجموعه‌ی $(K \setminus W)^{-1}$ کراندار است. با توجه به اینکه τ یک Vـ توپولوژی است، به ازای گوی W یک گوی V در τ وجود دارد که در شرط ۶ تعریفِ ۶.۴ صدق کند. حال ادعا می‌کنیم $V \cdot (K \setminus W)^{-1} \subseteq W$. برای اثبات این ادعا، فرض کنید یک عنصرِ x متعلق به $K \setminus W$ باشد. در این صورت بوضوح $x^{-1} \in (K \setminus W)^{-1}$. حال یک عنصرِ v در V در نظر بگیرید؛ واضح است که $v = v \cdot x^{-1} \cdot x \in V$. از آنجا که مجموعه‌ی V دارای این ویژگی است که اگر حاصل‌ضرب دو عنصر در آن باشد، آنگاه حداقل یکی از آن‌ها در W است، پس می‌توان نتیجه گرفت که $v \cdot x^{-1} \in W$ و بنابراین $V \cdot (K \setminus W)^{-1} \subseteq W$. در نتیجه، با توجه به لم ۳۲.۴، مجموعه‌ی $(K \setminus W)^{-1}$ کراندار است.

برای اثبات جهت عکس، فرض کنید به ازای هر $W \in \tau$ مجموعه‌ی $(K \setminus W)^{-1}$ کراندار باشد. می‌خواهیم نشان دهیم که τ یک Vـ توپولوژی است، یعنی در شرط ۶ در تعریفِ ۶.۴ صدق می‌کند. به این منظور،

توجه کنید که چون بنا به فرض $(K\setminus W)^{-1}$ کراندار است، پس به ازای گوی W یک گوی V در τ وجود دارد به طوری که $(K\setminus W)^{-1}\cdot V\subseteq W$. حال برای هر $x,y\in K$ اگر $x\cdot y\in V$ و $x\notin W$، آن‌گاه $y=x^{-1}\cdot x\cdot y\in (K\setminus W)^{-1}\cdot V$ و در نتیجه $y\in W$، بنابراین τ شرط ۶ در تعریفِ ۶.۴ را برآورده می‌کند.
$\square$

لم ۳۴.۴. اگر (K,τ) یک میدان Vـ توپولوژیک باشد، آن‌گاه حداقل یک گوی $U\in\tau$ وجود دارد به طوری که کراندار است.

اثبات. چون (K,τ) یک میدان Vـ توپولوژیک است، پس بنا به لم ۲۸.۴ یک گوی U در τ وجود دارد به طوری که $K^{\times}=(K/U)\cup(K/U)^{-1}$ و بنابراین $U\setminus\{0\}\subseteq (K\setminus U)^{-1}$. از طرفی بنا به تعریفِ ۳۳.۴ از میدان Vـ توپولوژیک، $(K/U)^{-1}$ یک مجموعه‌ی کراندار است و بنابراین بنا به قسمت ۳ در لم ۳۱.۴، مجموعه‌ی U به عنوان زیرمجموعه‌ی $(K/U)^{-1}$، نیز کراندار است. $\square$

تعریف ۳۵.۴. میدان توپولوژیک (K,τ) را در نظربگیرید. یک مجموعه‌ی $A\subseteq K$ را *کراندار دور از صفر* [۳] می‌نامیم هرگاه یک گوی باز U در τ وجود داشته باشد به طوری که $U\cap A\neq 0$.

لم ۳۶.۴. اگر S یک مجموعه‌ی کراندار باشد، آن‌گاه S^{-1} کراندار دور از صفر است.

اثبات. بنا به ویژگی اول میدان‌های توپولوژیک، یک گوی بازِ U در τ موجود است به طوری که $1\notin U$. از آنجا که S یک مجموعه‌ی کراندار است، پس برای گوی U یک گوی V در τ وجود دارد به طوری که $V\cdot S\subseteq U$، پس 1 متعلق به $V\cdot S$ نیز نیست و این یعنی $V\cap S^{-1}=\emptyset$. $\square$

قضیه ۳۷.۴. (K,τ) یک *میدانVـ توپولوژیک* است اگروتنهااگر کرانداری هر مجموعه‌ی S معادل با این باشد که S^{-1} کراندار دور از صفر باشد.

اثبات. فرض کنید (K,τ) یک میدان Vـ توپولوژیک باشد. می‌خواهیم نشان دهیم که کرانداری هر مجموعه‌ی S معادل با کراندار دور از صفر بودن S^{-1} است. از آنجا که در لم ۳۶.۴ نشان دادیم که اگر مجموعه‌ی S کراندار باشد، آن‌گاه S^{-1} کراندار دور از صفر است، پس کافی است نشان دهیم که اگر S^{-1} کراندار دور از صفر باشد، آن‌گاه S کراندار است. حال چون S^{-1} کراندار دور از صفر است، پس یک گوی $U\in\tau$ وجود دارد به طوری که $S^{-1}\subseteq (K\setminus U)$، در نتیجه $S\subseteq (K\setminus U)^{-1}$. از آنجا که (K,τ) یک میدان Vـ توپولوژیک است، پس بنا به قضیه‌ی ۳۳.۴، مجموعه‌ی $(K\setminus U)^{-1}$ کراندار است و بنابراین طبق ویژگی ۳ در لم ۳۱.۴، مجموعه‌ی S نیز کراندار است.

برای اثبات جهت عکس، توجه کنید که چون کرانداری هر مجموعه‌ی S معادل با کراندار دور از صفر بودن S^{-1} است، پس از کراندار دور از صفر بودن مجموعه‌ی $(K\setminus U)$ به ازای هر $U\in\tau$ می‌توان نتیجه گرفت که $(K\setminus U)^{-1}$ کراندار است. در نتیجه بنا به قضیه‌ی ۳۶.۴، (K,τ) یک میدان Vـ توپولوژیک است. $\square$

[3] bounded away from zero

لم ۳۸.۴. فرض کنید (K,τ) یک میدان توپولوژیک باشد، آنگاه خودِ K به عنوان یک زیرمجموعه از K کراندار نیست.

اثبات. با برهان خلف فرض کنید K کراندار باشد. در این صورت بنا به قسمت ۱ در لم ۳۱.۴، برای هر $U_i \in \tau$ یک عنصر x_i در $K^\times$ وجود دارد به طوری که $K \subseteq x_i^{-1}U_i$. از طرفی هر $x_i^{-1}U_i$ یک گوی باز است که نشان دادیم شامل K می‌شود و بنابراین K در اشتراک همه‌ی گوی‌های باز قرار دارد که این با ویژگی ۱ تعریفِ ۶.۴ در تناقض است. □

۳.۲.۴ مجموعه‌ی تقریباً ارزیاب

در این بخش مجموعه‌های تقریباً ارزیاب را معرفی می‌کنیم و نشان می‌دهیم که نسبت به جمع *تقریباً* بسته هستند. همچنین خواهیم دید که در یک میدان Vـ توپولوژیک همیشه یک مجموعهٔ تقریباً ارزیاب وجود دارد.

تعریف ۳۹.۴. یک زیرمجموعه‌ی S از میدان K یک مجموعه‌ی *تقریباً ارزیاب* نامیده می‌شود هرگاه دارای ویژگی‌های زیر باشد:

۱. S یک همسایگی باز و کراندار از صفر است.

۲. $1 \in S$، $S \neq K$ و $S \cdot S \subseteq S$.

۳. $K^\times \subseteq \dot{S}(\dot{S})^{-1}$ که در آن $\dot{S} = S \setminus \{0\}$.

۴. یک عنصرِ $d \in \dot{S}$ وجود دارد به طوری که برای هر $x \in K$، داریم $x \in S$ یا $x^{-1} \in d^{-1}S$.

لم ۴۰.۴. فرض کنید (K,τ) یک میدانِ Vـ توپولوژیک باشد. در این صورت، برای هر گوی کراندار $U \in \tau$، مجموعه‌ی $O := \{x \in K \mid xU \subseteq U\}$ یک مجموعه‌ی تقریباً ارزیاب است.

اثبات. نشان می‌دهیم که مجموعه‌ی O ویژگی ۱ تا ۴ در تعریفِ ۳۹.۴ را دارد:

۱. از آنجا که U کراندار است، پس بنا به تعریف یک مجموعه‌ی کراندار، یک گوی $W \in \tau$ وجود دارد به طوری که $W \cdot U \subseteq U$ و بنابراین با توجه به تعریف مجموعه‌ی O داریم $W \subseteq O$، در نتیجه O یک همسایگی از صفر است. به علاوه، با توجه به تعریف مجموعه‌ی O به سادگی نتیجه می‌شود که $O \cdot U \subseteq U$، پس برای یک عنصر ناصفرِ x در U داریم $O \subseteq Ux^{-1}$. حال توجه کنید که U یک مجموعه‌ی کراندار است و همچنین $\{x^{-1}\}$ کراندار است، در نتیجه Ux^{-1} کراندار و نهایتاً زیرمجموعه‌ی آن، یعنی O کراندار است.

۲. چون O یک مجموعه‌ی کراندار است و طبق لم ۳۸.۴ میدان K کراندار نیست، پس $K \neq O$. به علاوه، بوضوح بنا به تعریف مجموعه‌ی O، عنصر 1 در O است. حال اگر $x, y \in O$ آنگاه بنا به تعریف مجموعه‌ی O داریم $x \cdot yU \subseteq xU \subseteq U$؛ یعنی $x \cdot y \in O$ و در نتیجه $O \cdot O \subseteq O$.

۳. یک عنصر دلخواه x در $K^{\times}$ در نظر بگیرید. بنا به ۸.۴، برای O به عنوان یک همسایگی صفر و عنصر مفروض x یک گوی $W \in \tau$ وجود دارد به طوری که $xW \subseteq O$. از آنجا که (K, τ) یک میدان Vـ توپولوژیک است، پس بنا به ویژگی ۲ در تعریفِ ۶.۴، یک گوی $V \in \tau$ وجود دارد به طوری که $V \subseteq O \cap W$. بنابراین برای هر عنصر ناصفرِ $y \in V$ و عنصرِ $z := xy \in O$ داریم $x = z(y)^{-1} \in O(O)^{-1}$.

۴. یک عنصر دلخواهِ x در K را در نظر بگیرید. اگر x در O باشد که حکم برقرار است؛ در غیر این صورت $x \in K \setminus O$. همان‌طور که در اثبات قسمت ۱ در همین لم دیدیم، یک گوی $W \in \tau$ وجود دارد به طوری که $W \subseteq O$، بنابراین $(K \setminus O)^{-1} \subseteq (K \setminus W)^{-1}$. از طرفی چون τ یک Vـ توپولوژی است، پس $(K \setminus W)^{-1}$ کراندار و $(K \setminus O)^{-1}$ به عنوان زیرمجموعه‌ی آن نیز کراندار است. مطابق با ویژگی ۱ از مجموعه‌های کراندار در لم ۳۱.۴، یک عنصر d در $K^{\times}$ برای گوی باز O وجود دارد به طوری که $d(K \setminus O)^{-1} \subseteq O$، پس $(K \setminus O)^{-1} \subseteq d^{-1}O$. اینگونه نتیجه‌ی مطلوبِ $x^{-1} \in d^{-1}O$ حاصل می‌شود.

$\square$

در لم زیر می‌خواهیم نشان دهیم که هر مجموعه‌ی تقریباً ارزیاب، نسبت به جمع «تقریباً» بسته است.

لم ۴۱.۴. میدانِ Vـ توپولوژیکِ (K, τ) را در نظر بگیرید. اگر O یک مجموعه‌ی تقریباً ارزیاب در K باشد، آنگاه یک عنصر $c \in \dot{O}$ وجود دارد به طوری که $c(O \pm O) \subseteq O$.

اثبات. از آنجا که O یک مجموعه‌ی تقریباً ارزیاب است، پس یک همسایگی باز در τ است. در نتیجه با توجه به اینکه (K, τ) یک میدان توپولوژیک است، یک گوی $W \in \tau$ وجود دارد به طوری که $W \pm W \subseteq O$. از طرفی چون O یک مجموعه‌ی کراندار است، پس یک عنصرِ c در $K^{\times}$ وجود دارد به طوری که $cO \subseteq W$ و بنابراین $c(O \pm O) \subseteq cO \pm cO \subseteq W \pm W \subseteq O$. نهایتاً از آنجا که 0 و 1 در O هستند، پس عنصر c در O قرار دارد. $\square$

لم ۴۲.۴. فرض کنید (K, τ) یک میدان Vـ توپولوژیک باشد. گردایه‌ی $\tau_O = \{xO \mid x \in K^{\times}\}$ که در آن O مجموعه‌ی تقریباً ارزیاب معرفی شده در ۴۰.۴ است، یک توپولوژی یکسان با τ روی K تولید می‌کند.

اثبات. از آنجا که O یک مجموعه‌ی کراندار است، پس بنا به قسمت ۴ در لم ۳۱.۴، برای هر $W \in \tau$ یک عنصر $x \in K$ موجود است به طوری که $xO \subseteq W$. از طرفی بنا به توجه ۸.۴ و اینکه O یک همسایگی از صفر است، برای هر $x \in K$ یک گوی $W \in \tau$ وجود دارد به طوری که $xW \subseteq O$؛ به بیان دیگر $W \subseteq x^{-1}O$. چون نشان دادیم که

هر گوی $xO \in \tau_O$ شامل یک گوی از توپولوژی τ و هر گوی در توپولوژی τ شامل یک xO است نتیجه می‌گیریم که $\tau_O = \tau$. □

در ادامه، وقتی می‌گوییم یک مجموعه‌ی تقریباً ارزیابِ O توپولوژی یکسان با τ روی میدانِ K القاء می‌کند، منظورمان این است که $\tau_O = \tau$.

۴.۲.۴ عناصر پوچ‌توان و خنثی

در این بخش ابتدا عناصر پوچ‌توان و خنثی را معرفی می‌کنیم و برخی از ویژگی‌های آن‌ها را بیان و اثبات می‌کنیم. در بخش‌های بعدی خواهیم دید که عناصر پوچ‌توان نقش کلیدی در دسته‌بندی میدان‌های Vـ توپولوژیک دارند، به بیان دیگر اگر (K, τ) یک میدان Vـ توپولوژیک باشد و در K هیچ عنصر پوچ‌توانی وجود نداشته باشد، آن‌گاه یک ارزیابی روی میدان وجود دارد که توپولوژی یکسان با τ القاء می‌کند و اگر حداقل یک عنصر پوچ‌توان در K موجود باشد، آن‌گاه یک نگاشت قدرمطلق روی میدان قابل تعریف است که توپولوژی برابری با τ القاء می‌کند.

تعریف ۴۳.۴. میدان توپولوژیکِ (K, τ) را در نظر بگیرید. یک عنصر $x \in K$ *پوچ‌توان*[۴] نامیده می‌شود هرگاه $x = 0$ یا دنباله‌ی $(x^n)_{n\in\mathbb{N}}$ در توپولوژی τ به 0 همگرا باشد؛ یعنی برای هر $W \in \tau$ یک عدد طبیعیِ n_0 وجود داشته باشد به طوری که x^n به ازای هر $n \geq n_0$ در W قرار بگیرد. همچنین، یک عنصر x در $K^\times$ خنثی نامیده می‌شود هرگاه هیچ‌یک از x و x^{-1} پوچ‌توان نباشند.

نماد گذاری ۴۴.۴. مجموعه‌ی متشکل از همه‌ی عناصر پوچ‌توان را با N_0 مجموعه‌ی متشکل از عناصر خنثی را با N^* و مجموعه‌ی متشکل از عناصر خنثی و پوچ‌توان را با N نشان می‌دهیم.

لم ۴۵.۴. میدان Vـ توپولوژیکِ (K, τ) را در نظر بگیرید. فرض کنید O یک حلقه‌ی تقریباً ارزیاب در K است. اگر $x \in \dot{O}$ پوچ‌توان نباشد، آن‌گاه مجموعه‌ی $\{x^{-n} \mid n \in \mathbb{N}\}$ کراندار است.

اثبات. چون (K, τ) یک میدان Vـ توپولوژیک است، پس به ازای هر $W \in \tau$ مجموعه‌ی $(K \setminus W)^{-1}$ کراندار است. بنابراین، برای اثبات کرانداری مجموعه‌ی $\{x^{-n} \mid n \in \mathbb{N}\}$ کافی است نشان دهیم که یک گوی $W \in \tau$ وجود دارد به طوری که $\{x^{-n} \mid n \in \mathbb{N}\} \subseteq (K \setminus W)^{-1}$. اگر به ازای هر $u \in K^\times$ یک عدد طبیعی r وجود داشته باشد به طوری که $x^r \in uO$، آن‌گاه با توجه به اینکه $x \in O$ و $O \cdot O \subseteq O$ داریم $x^r \cdot x = x^{r+1} \in uO \cdot O \subseteq uO$ و به این ترتیب برای هر $n \geq r$ نیز داریم $x^n \in uO$. از طرفی، در لم ۴۲.۴ نشان دادیم که مجموعه‌ی $\tau_O = \{uO \mid u \in K^\times\}$ یک توپولوژی یکسان با τ القاء می‌کند، پس می‌توان نتیجه گرفت که x یک عنصر پوچ‌توان است و این با فرض در تناقض است. بنابراین یک عنصرِ $u \in K^\times$ وجود دارد به طوری که هیچ توانی از x در uO نیست، یعنی $\{x^n \mid n \in \mathbb{N}\} \subseteq K \setminus uO$ و در نتیجه $\{x^{-n} \mid n \in \mathbb{N}\} \subseteq (K \setminus uO)^{-1}$. □

[4] nilpotent

لم ۴۶.۴. میدان Vـ توپولوژیکِ (K, τ) را در نظر بگیرید. اگر حداقل یک عنصر ناصفر و پوچ‌توانِ y در K وجود داشته باشد، آنگاه یک همسایگی $W \in \tau$ وجود دارد به طوری که همه‌ی عناصر آن پوچ‌توان هستند.

اثبات. حلقه‌ی تقریباً ارزیابِ O از K را در نظر بگیرید. ادعا می‌کنیم که مجموعه‌ی $E := yO$ یک همسایگی در τ است که همه‌ی عناصر آن پوچ‌توان است. از آنجا که O کراندار است، پس برای هر $U \in \tau$ یک گوی V وجود دارد به طوری که $V \cdot O \subseteq U$. از طرفی y یک عنصر پوچ‌توان است، پس یک عدد طبیعی n_0 وجود دارد به طوری که برای هر $n \geq n_0$، داریم $y^n \in V$. همچنین، چون O یک حلقه‌ی تقریباً ارزیاب است، پس $O \cdot O \subseteq O$ و در نتیجه برای هر $u \in E$ و هر $n \geq n_0$ داریم $u^n \in y^n O \subseteq V \cdot O \subseteq U$ و این یعنی هر $u \in E$ پوچ‌توان است. □

حال برخی از ویژگی‌های عناصر پوچ‌توان و خنثی را که در اثبات قضیه‌های ۵۲.۴ و ۶.۲.۴ به آن نیاز داریم را بیان می‌کنیم:

لم ۴۷.۴. میدان توپولوژیکِ (K, τ) را در نظر بگیرید.

۱. اگر x و y دو عنصر پوچ‌توان در K باشند، آنگاه $x \cdot y$ نیز پوچ‌توان است.

۲. اگر حداقل یک عنصر ناصفر و پوچ‌توانِ x در K موجود باشد، آنگاه N_0 یک همسایگی کراندار در τ است.

۳. اگر حداقل یک عنصر ناصفر و پوچ‌توانِ x در K موجود باشد، آنگاه N یک همسایگی کراندار در τ است.

۴. اگر x یک عنصر پوچ‌توان و y یک عنصر خنثی باشد، آنگاه $x \cdot y$ پوچ‌توان است.

۵. اگر x و y دو عنصر خنثی باشند، آنگاه $x \cdot y$ خنثی است.

۶. مجموعه‌ی N^* یک زیرگروه از گروه حاصل‌ضربی $(K^\times, \cdot)$ است.

۷. اگر یک عنصر ناصفرِ x پوچ‌توان باشد، آنگاه برای هر $y \neq 0$ یک عدد طبیعی m موجود است به طوری که $x^m \cdot y^{-1}$ پوچ‌توان باشد.

اثبات. ۱. بنا به ویژگی ۴ در تعریفِ ۶.۴، برای گوی دلخواه $U \in \tau$ یک گوی W وجود دارد به طوری که $W \cdot W \subseteq U$. چون مطابق فرض x و y پوچ‌توان هستند، پس به ازای گوی W توان‌های n_0 و n_1 وجود دارند به طوری که برای هر $n \geq n_0, n_1$ داریم $x^n, y^n \in W$. توجه کنید که بوضوح برای هر $n \geq \max\{n_0, n_1\} := n_2$ نیز داریم $x^n, y^n \in W$. پس برای هر $U \in \tau$ یک عنصر n_2 وجود دارد به طوری که برای هر $n \geq n_2$ داریم $x^n \cdot y^n \in W \cdot W \subseteq U$ و این یعنی $x \cdot y$ پوچ‌توان است.

۲. در لم ۴۶.۴ دیدیم که یک همسایگی $W \in \tau$ وجود دارد به طوری که همه‌ی عناصر آن پوچ‌توان هستند، بنابراین $W \subseteq N_0$ و این یعنی N_0 نیز یک همسایگی در τ است. حال می‌خواهیم نشان دهیم که N_0 کراندار است.

ابتدا ادعا می‌کنیم که هیچ‌یک از عناصر $(W^\times)^{-1}$ پوچ‌توان نیستند. با برهان خلف فرض کنید $z \in (W^\times)^{-1}$ یک عنصر پوچ‌توان باشد. بنابراین با توجه به قسمت قبل $z \cdot z^{-1} = 1$ نیز یک عنصر پوچ‌توان است که این تناقض است، زیرا بوضوح 1 پوچ‌توان نیست. در نتیجه $N_0^\times \subseteq (K \setminus W^{-1}) = (K \setminus W)^{-1}$. از طرفی، چون τ یک Vـ توپولوژی است، پس $(K \setminus W)^{-1}$ کراندار و در نتیجه زیرمجموعه‌ی آن، یعنی $N_0^\times$ نیز کراندار است. نهایتاً از آنجا که $N_0^\times$ و $\{0\}$ هر دو مجموعه‌هایی کراندار هستند و $N = N_0^\times \cup \{0\}$ نتیجه می‌گیریم که N_0 یک مجموعه‌ی کراندار است.

۳. در لم ۴۶.۴ دیدیم که یک همسایگی $W \in \tau$ وجود دارد به طوری که همه‌ی عناصر آن پوچ‌توان هستند، پس $W \subseteq N$ و از این نتیجه می‌شود که N نیز یک همسایگی در τ است. همچنین، در قسمت قبل نشان دادیم که عناصر $(W^\times)^{-1}$ پوچ‌توان نیستند. حال ادعا می‌کنیم که عناصرِ $(W^\times)^{-1}$ خنثی هم نیستند. با برهان خلف، فرض کنید یک عنصرِ x در $(W^\times)^{-1}$ خنثی باشد. در این صورت $x^{-1} \in W^\times$، یعنی x^{-1} پوچ‌توان است که این با خنثی بودنِ x تناقض دارد. بنابراین $N \subseteq (K \setminus W^{-1}) = (K \setminus W)^{-1}$ و مشابه با استدلال قبلی N یک مجموعه‌ی کراندار است.

۴. فرض کنید y یک عنصر خنثی باشد. ادعا می‌کنیم که به ازای هر $n \in \mathbb{Z}$، عنصر y^n نیز خنثی است. با برهان خلف فرض کنید به ازای یک عدد صحیحِ n عنصرِ y^n خنثی نباشد، یعنی y^n یا y^{-n} پوچ‌توان باشد. در این صورت، بوضوح y یا y^{-1} پوچ‌توان می‌شود و این با خنثی بودن y در تناقض است، در نتیجه به ازای هر $n \in \mathbb{N}$ داریم $y^n \in N$. از طرفی، از آنجا که در قسمت قبل نشان دادیم مجموعه‌ی N کراندار است، پس برای هر $W \in \tau$ یک گوی $V \in \tau$ وجود دارد به طوری که $V \cdot N \subseteq W$. به علاوه مطابق فرض x یک عنصر پوچ‌توان است، پس برای گوی V، یک عدد طبیعی n_0 وجود دارد به طوری که به ازای هر $n \geq n_0$ داریم $x^n \in V$. بنابراین به ازای هر $n \geq n_0$، داریم $x^n \cdot y^n \in V \cdot N \subseteq W$، یعنی عنصرِ $x \cdot y$ پوچ‌توان است.

۵. با برهان خلف فرض کنید $x \cdot y$ خنثی نباشد. بنابراین یا $x \cdot y$ پوچ‌توان است یا $(x \cdot y)^{-1}$. اگر $(x \cdot y)^{-1}$ پوچ‌توان باشد، آنگاه بنا به قسمت ۴، $y \cdot (x \cdot y)^{-1} = x^{-1}$ پوچ‌توان است که این با خنثی بودن عنصر x در تناقض است و اگر $x \cdot y$ پوچ‌توان باشد، آنگاه به طور مشابه عنصر $x = (x \cdot y) \cdot y^{-1}$ پوچ‌توان است که این نیز با خنثی بودن x در تناقض است. بنابراین فرض خلف باطل و حکم مسئله ثابت می‌شود.

۶. اولاً از آنجا که 1 عنصری خنثی است، پس $1 \in N^* = N \setminus N_0$. ثانیاً در قسمت قبل دیدیم که اگر دو عنصر خنثی باشند، آنگاه حاصل‌ضرب آن‌ها نیز یک عنصر خنثی است، در نتیجه N^* تحت عمل ضرب بسته است. همچنین، اگر x یک عنصر خنثی باشد، آنگاه x^{-1} نیز خنثی است. بنابراین $(N^*, \cdot)$ یک زیرگروه از گروه حاصل‌ضربی $(K^\times, \cdot)$ است.

۷. در قسمت ۲ نشان دادیم که N_0 یک همسایگی در τ است و چون τ یک توپولوژی میدانی است، می‌توان نتیجه گرفت که yN_0 نیز یک همسایگی در τ است. از آنجا که x یک عنصر پوچ‌توان است، پس برای همسایگی yN_0 یک عدد $n_0 \in \mathbb{N}$ وجود دارد به طوری که برای هر $n \geq n_0$ داریم $x^n \in yN_0$، بنابراین $x^n \cdot y^{-1} \in N_0$. □

لم ۴۸.۴. مجموعه‌ی N (مجموعه‌ی متشکل از عناصر پوچ‌توان و خنثی) یک مجموعه‌ی تقریباً ارزیاب در میدان K

است.

اثبات. برای اثبات باید نشان دهیم که مجموعه‌ی N ویژگی‌های ۱ تا ۴ در تعریفِ ۳۹.۴ را دارد.

در لم ۴۷.۴ اثبات کردیم که مجموعه‌ی N یک همسایگی کراندار از صفر است که تحت عمل ضرب بسته است. به علاوه، از آنجا که عنصر 1 یک عنصر خنثی است، پس $1 \in N$. حال یک عنصر $x \in K^\times$ را در نظر بگیرید. فرض کنید x یک عنصر خنثی نباشد. در این صورت یا x یا x^{-1} یک عنصر پوچ‌توان است و از این نتیجه می‌شود که اگر $x \notin N$، آنگاه $x^{-1} \in N$ □

این زیربخش را با دو مثال که در آن‌ها عناصر پوچ‌توان و خنثی را بررسی کرده‌ایم، به پایان می‌رسانیم.

مثال ۴۹.۴. یک قدر مطلق ارشمیدسیِ $||$ را روی میدانِ K در نظر بگیرید. همه‌ی عناصرِ $x \in K$ که قدرمطلق آن‌ها کمتر از 1 است، پوچ‌توان هستند؛ زیرا یا $x = 0$ یا بوضوح $(x^n)_{n\in\mathbb{N}}$ همگرا به صفر است. همچنین، یک عنصرِ $x \in K$ خنثی است اگروتنهااگر $|x| = 1$.

مثال ۵۰.۴. یک نگاشت ارزیابی $v : K \to \Gamma$ را در نظر بگیرید که رتبه‌ی آن 1 باشد. یادآوری می‌کنیم که ایده‌آل ماکسیمالِ m_v از حلقه‌ی ارزیابِ O_v برابر است با $\{x \in O_v : v(x) > 0\}$. ادعا می‌کنیم که به ازای هر $x \in m_v$ دنباله‌ی $(x^n)_{n\in\mathbb{N}}$ یک دنباله‌ی همگرا به صفر است. برای اثبات این ادعا، یک همسایگی صفرِ $U_\gamma(0) \in \tau_v$ را در نظر بگیرید. از آنجا که Γ دارای رتبه‌ی 1 است، پس بنا به قضیه‌ی ۲۵.۴ خاصیت ارشمیدسی دارد. بنابراین برای $v(x) > 0$ و $\gamma \in \Gamma$ یک عدد طبیعی n_0 وجود دارد به طوری که $\gamma \leq n_0 v(x)$. از طرفی با توجه به ویژگی‌های نگاشت ارزیابی داریم $n_0 v(x) = v(x^{n_0})$ و بوضوح با توجه به مثبت بودنِ $v(x)$، به ازای هر $n \geq n_0$ نیز داریم $\gamma \leq n_0 v(x) \leq n v(x) = v(x^n)$. به بیان دیگر به ازای هر $n \geq n_0$ داریم $x^n \in U_\gamma(0)$. در نتیجه برای هر همسایگی صفرِ W در τ_v یک عدد طبیعی n_0 وجود دارد به طوری که به ازای هر $n \geq n_0$ داریم $x^n \in W$ و این یعنی x یک عنصر پوچ‌توان است. بنابراین هر عنصر موجود در m_v پوچ‌توان است. همچنین، هر عنصرِ x در $O \setminus M$ یک عنصر خنثی است، زیرا $v(x) = v(x^{-1}) = 0$ و از این نتیجه می‌شود که هیچ‌یک از x و x^{-1} پوچ‌توان نیستند.

۵.۲.۴ یک Vـ توپولوژی بدون عنصر پوچ‌توان

تا اینجا مفاهیم مورد نیاز برای اثبات قضیه‌ی ۱۹.۴ را بیان کردیم. در بخش ۴۰.۴ گفتیم که در هر میدان Vـ توپولوژیک یک مجموعهٔ تقریباً ارزیاب وجود دارد. در این بخش نشان می‌دهیم که اگر در میدان Vـ توپولوژیک یاد شده، هیچ عنصر پوچ‌توانی وجود نداشته باشد، آنگاه می‌توان این مجموعه‌ی تقریباً ارزیاب را به یک حلقه‌ی ارزیاب تبدیل کرد. به بیان دیگر، اثبات می‌کنیم که توپولوژی τ یک Vـ توپولوژی بدون عنصر پوچ‌توان است اگروتنهااگر این توپولوژی توسط یک حلقه‌ی ارزیاب در K القاء شده باشد.

لم ۵۱.۴. یک میدان Vـ توپولوژیکِ (K,τ) که هیچ عنصر پوچ‌توانی ندارد را در نظر بگیرید. فرض کنید O یک مجموعه‌ی تقریباً ارزیاب است و $d \in \dot{O}$ وجود دارد به طوری که $(K \setminus O)^{-1} \subseteq d^{-1}O$ (مطابق با تعریفِ ۳۹.۴ چنین عنصرِ d وجود دارد). در این صورت $\tilde{O} := \{x \in K \mid xO \subseteq d^{-n}O, n \geq 0$ برای یک$\}$ یک مجموعه‌ی تقریباً ارزیاب است.

اثبات. برای اثبات کافی است ویژگی‌های بیان شده در تعریفِ ۳۹.۴ را برای $\tilde{O}$ بررسی کنیم:

۱. با توجه به این که مجموعه‌ی O تقریباً ارزیاب است، پس $O \cdot O \subseteq O$ و بنابراین طبق تعریف مجموعه‌ی $\tilde{O}$ داریم $O \subseteq \tilde{O}$. این به معنی این است که $\tilde{O}$ یک همسایگی در توپولوژی τ است.

برای اثبات کرانداری $\tilde{O}$، ابتدا توجه کنید که چون $1 \in O$، پس $\tilde{O} \subseteq \bigcup_{n\geq 0} d^{-n}O$. از آنجا که در میدان مورد نظر هیچ عنصر پوچ‌توانی وجود ندارد، لذا از لمِ ۴۵.۴ می‌توان استفاده کرد و نتیجه گرفت که مجموعه‌ی $\{d^{-n} \mid n \in \mathbb{N}\}$ کراندار است. با توجه به این که O نیز کراندار است، پس $O\{d^{-n} \mid n \in \mathbb{N}\}$ کراندار است. از این رو، $\tilde{O}$ نیز کراندار است.

۲. باتوجه به نحوه‌ی ساخت مجموعه‌ی $\tilde{O}$ به سادگی می‌توان استنباط کرد که $\tilde{O} \cdot \tilde{O} \subseteq \tilde{O}$ و $1 \in \tilde{O}$.

۳. از آنجا که O یک مجموعه‌ی تقریباً ارزیاب است، پس $O \cdot O \subseteq O$ و از این نتیجه می‌شود که $O \subseteq \tilde{O}$. بنابراین $(K \setminus \tilde{O})^{-1} \subseteq (K \setminus O)^{-1} \subseteq d^{-1}O \subseteq \tilde{O}$. حال توجه کنید که بوضوح برای هر $x \in K$ داریم یا $x \in \tilde{O}$ یا $x \in (K \setminus \tilde{O})$. اگر $x \in (K \setminus \tilde{O})$، آنگاه $x^{-1} \in (K \setminus \tilde{O})^{-1}$ و در نتیجه $x^{-1} \in \tilde{O}$.

□

قضیه ۵۲.۴. فرض کنید (K,τ) یک میدان توپولوژیک باشد. در این صورت:
توپولوژی τ یک Vـ توپولوژی بدون عنصر پوچ‌توان است اگروتنهااگر این توپولوژی توسط یک حلقه‌ی ارزیاب O^* در K القاء شده باشد.

اثبات. فرض کنید توپولوژیِ τ روی میدانِ K توسط یک حلقه‌ی ارزیاب القاء شده باشد. در این صورت، همان‌طور که در قضیه‌ی ۱۴.۴ اثبات کردیم، τ یک Vـ توپولوژی است.

برای اثبات جهت عکس، فرض کنید (K,τ) یک میدانِ Vـ توپولوژیک باشد. در ادامه، می‌خواهیم نشان دهیم که یک حلقه‌ی ارزیاب در K وجود دارد به طوری که توپولوژی القاء شده توسط آن برابر با τ است.

در لمِ ۳۴.۴ دیدیم که اگر (K,τ) یک میدانِ Vـ توپولوژیک باشد، آنگاه یک مجموعه‌ی کراندار در K وجود دارد. حال با استفاده از این مجموعه‌ی کراندار، مجموعه‌ی تقریباً ارزیاب O را مطابق با لم ۴۰.۴ تشکیل می‌دهیم. با توجه به قسمت ۴ تعریفِ ۳۹.۴، می‌توانیم یک عنصرِ d در O انتخاب کنیم به طوری که در شرطِ $(K\setminus O)^{-1} \subseteq d^{-1}O$

صدق کند. سپس، مجموعه‌ی $\tilde{O}$ را به صورت زیر تعریف می‌کنیم:

$$\tilde{O} := \{x \in K \mid xO \subseteq d^{-n}O, n \geq 0 \text{ برای هر}\}.$$

بنا به لم ۵۱.۴، مجموعه‌ی $\tilde{O}$ یک مجموعه‌ی تقریباً ارزیاب است که به ازای هر $x \in K$ یا $x \in \tilde{O}$ یا $x^{-1} \in \tilde{O}$. بنابراین، طبق لم ۴۱.۴، یک عنصر $c \in \tilde{O}^{\times}$ وجود دارد به طوری که شرطِ $c(\tilde{O} \pm \tilde{O}) \subseteq \tilde{O}$ را برآورده می‌کند. پس بوضوح داریم:

$$\tilde{O} \pm \tilde{O} \subseteq c^{-1}\tilde{O}$$

و در نتیجه

$$\tilde{O} \pm \tilde{O} \pm \tilde{O} \pm \tilde{O} \subseteq c^{-1}(\tilde{O} \pm \tilde{O}) \subseteq c^{-2}\tilde{O}.$$

به این ترتیب، در حالت کلی‌تر داریم

$$\underbrace{\tilde{O} \pm ... \pm \tilde{O}}_{2^n \text{بار}} \subseteq c^{-n}\tilde{O}. \qquad (۱.۴)$$

تا اینجا، مجموعه‌ی $\tilde{O}$ را به دست آوردیم که به طور قابل توجهی ویژگی‌های یک حلقه‌ی ارزیاب را دارد؛ اما یک زیرحلقه از K نیست، زیرا تحت عمل جمع بسته نیست. بنابراین در مرحله‌ی آخر، زیرحلقه‌ی تولید شده توسط $\tilde{O}$ در میدانِ K را در نظر می‌گیریم. بوضوح این زیرحلقه برابر با $O^* = \{x_1 + ... + x_m \mid m \geq 1, x_1, ..., x_m \in \tilde{O} \cup -\tilde{O}\}$ است. (یک زیرحلقه‌ی K که توسطِ $\tilde{O}$ تولید شده، برابر با کوچکترین زیرحلقه‌ی K شاملِ $\tilde{O}$ است. به عبارت دیگر، زیرحلقه‌ی مطلوب با توجه به اینکه $\tilde{O}$ تحت عمل ضرب و وارون‌گیری ضربی بسته است، با افزودن وارون جمعی عناصر آن و مجموع متناهی از عناصر $\tilde{O}$ به دست می‌آید.) نهایتاً، ادعا می‌کنیم که O^* حلقه‌ی ارزیاب موردنظر ماست. برای اثبات این ادعا، یک عنصر دلخواهِ $x \in K$ را در نظر بگیرید. در این صورت، $x \in \tilde{O} \subseteq O^*$ یا $x^{-1} \in \tilde{O} \subseteq O^*$، پس O^* یک حلقه‌ی ارزیاب در K است. تنها چیزی که اثبات آن باقی مانده، این است که O^* یک توپولوژی یکسان با τ روی میدان K القاء می‌کند. اولاً چون $\tilde{O} \subseteq O^*$، پس زیرحلقه‌ی O^* یک همسایگی در τ است. ثانیاً با توجه به رابطه‌ی (۱.۴) به سادگی می‌توان دید که $O^* \subseteq \tilde{O}\{c^{-n} \mid n \in \mathbb{N}\}$. از آنجا که c یک عنصر خنثی است، پس مجموعه‌ی $\{c^{-n} \mid n \in \mathbb{N}\}$ کراندار است و با توجه به کرانداری $\tilde{O}$ نتیجه می‌گیریم که $\tilde{O}\{c^{-n} \mid n \in \mathbb{N}\}$ کراندار و در نتیجه O^* کراندار است. نهایتاً، چون $O \subseteq \tilde{O} \subseteq O^*$ پس مانند O، توپولوژی القاء شده توسط O^* با τ یکسان است. □

۶.۲.۴ یک Vـ توپولوژی با حداقل یک عنصر پوچ‌توان

در این بخش قصد داریم قضیه‌ی زیر را اثبات کنیم:

"اگر (K,τ) یک میدان Vـ توپولوژیک با حداقل یک عنصر پوچ‌توان باشد آن‌گاه یک قدرمطلق ارشمیدسی روی K وجود دارد به طوری که روی آن یک توپولوژی یکسان با τ القاء می‌کند."

روش اثبات این قضیه به صورت زیر است:

۱. یک رابطه‌ی هم‌ارزی روی میدانِ K تعریف می‌کنیم و نشان می‌دهیم که مجموعه‌ی Γ متشکل از کلاس‌های هم‌ارزی این رابطه یک گروه مرتب ارشمیدسی است.

۲. چون Γ ارشمیدسی است، پس یک نشاندن از آن به $\mathbb{R}$، مطابق با قضیه‌ی ۲۵.۴، وجود دارد. با ترکیب این نگاشت نشاندن و نگاشت کانونی که هر عنصرِ K را به کلاس هم‌ارزی‌اش می‌برد به نگاشتِ φ دست می‌یابیم و با استفاده از آن یک نگاشتِ $||$ تعریف می‌کنیم.

۳. نشان می‌دهیم $||$ یک نگاشت قدرمطلق روی K است و یک توپولوژی برابر با τ القاء می‌کند.

قضیه ۵۳.۴. اگر τ روی میدانِ K یک Vـ توپولوژی با حداقل یک عنصر پوچ‌توان باشد، آن‌گاه یک قدرمطلق ارشمیدسی روی K وجود دارد به طوری که روی K یک توپولوژی یکسان با τ القاء می‌کند.

اثبات. جهت اثبات این قضیه، مراحل زیر را طی خواهیم کرد:

- **مرحله‌ی اول:** محموعه‌ی N، یعنی مجموعه‌ی متشکل از عناصر پوچ‌توان و خنثی در K را در نظر بگیرید. حال رابطه‌ی R را برای هر عنصر x و y در میدان K به صورت زیر در نظر بگیرید:

$$yRx \iff x \in yN$$

توجه کنید که این رابطه بازتابی [5] است، زیرا 1 در N قرار دارد و لذا $x \in xN$، به عبارت دیگر xRx. همچنین، R متعدی [6] است، زیرا اگر xRy و yRz، آن‌گاه $y \in xN$ و $z \in yN$. بنابراین $y = x \cdot t$ که در آن $t \in N$، پس $z \in x \cdot tN$ و می‌توان نتیجه گرفت که $z \in xN$، به عبارت دیگر xRz.

می‌خواهیم نشان دهیم که xRy و yRx اگروتنهااگر $x \cdot y^{-1} \in N^*$، یعنی $x \cdot y^{-1}$ یک عنصر خنثی باشد. فرض کنید xRy و yRx. در این صورت، با توجه به نحوه‌ی تعریف رابطه‌ی R داریم $y \cdot x^{-1} \in N$ و $x \cdot y^{-1} \in N$. بنابراین دو عنصرِ $x \cdot y^{-1}$ و $y \cdot x^{-1}$ خنثی هستند، زیرا اگر حداقل یکی از این دو عنصر پوچ‌توان باشد، آن‌گاه طبق لم ۴۷.۴ حاصل‌ضرب آن‌ها نیز پوچ‌توان است که این با خنثی بودن 1 تناقض دارد؛

[5] reflexive
[6] transitive

در نتیجه $x \cdot y^{-1} \in N^*$. برای اثبات جهت عکس، فرض کنید $x \cdot y^{-1} \in N^*$. در این صورت، با توجه به توضیحات فوق $y \cdot x^{-1} \in N^*$ و بنابراین xRy و yRx.

حال رابطه‌ی $\equiv$ را به ازای هر $x, y \in K^\times$ به صورت زیر تعریف می‌کنیم:

$$x \equiv y \iff xRy \text{ و } yRx$$

ادعا می‌کنیم که این رابطه هم‌ارزی [7] است:

۱. به ازای هر $x \in K$ داریم $x \equiv x$، زیرا دیدیم که R یک رابطه‌ی بازتابی است.

۲. این رابطه با توجه به نحوه‌ی تعریف آن، بوضوح تقارنی است.

۳. رابطه‌ی یاد شده متعدی است، زیرا اگر $x \equiv y$ و $y \equiv z$ آنگاه به ترتیب داریم xRy، yRx و yRz، zRy. حال با توجه به اینکه R متعدی است، نتیجه می‌گیریم xRz و zRx که این یعنی $x \equiv z$.

- **مرحله‌ی دوم:** مجموعه‌ی $\Gamma := K^\times / \equiv$ را در نظر بگیرید. به عبارت دیگر، $\Gamma = \{[x]_\equiv : x \in K\}$. با توجه به نحوه‌ی تعریف این رابطه‌ی هم‌ارزی، به سادگی می‌توان دید که $[x]_\equiv$ برابر با xN^* است و بنابراین، $\Gamma = K^\times / N^*$. حال روی گروه Γ یک ترتیبِ $\leq$ را به صورت زیر تعریف می‌کنیم:

$$[x]_\equiv \leq [y]_\equiv \iff xRy$$

ادعا می‌کنیم که $\leq$ یک ترتیب ارشمیدسی روی Γ است. برای اثبات این ادعا، ابتدا توجه کنید که اگر $t \in N^*$، آنگاه بوضوح $[t]_\equiv$ برابر با صفر گروهِ Γ است. بنابراین $[x]_\equiv$ یک عنصر مثبت در Γ است اگروتنهااگر x یک عنصر پوچ‌توان در K باشد. حال فرض کنید x یک عنصر پوچ‌توان باشد و $y \in K^\times$. در این صورت، بنا به قسمت ۷ لم ۴۷.۴، یک عدد طبیعیِ m وجود دارد به طوری که $x^m \cdot y^{-1}$ یک عنصر پوچ‌توان است. در نتیجه، $x^m \in yN$ یعنی yRx^m، پس $[y]_\equiv \leq [x]_\equiv^m$.

در لم ۲۴.۴، ثابت کردیم که یک گروه آبلی با ترتیب ارشمیدسی، رتبه‌ی 1 دارد. با توجه به این که در بالا نشان داده‌ایم ترتیب گروه Γ ارشمیدسی است، می‌توان نتیجه گرفت که این گروه دارای رتبه‌ی 1 است. اکنون قضیه‌ی زیر را یادآوری می‌کنیم که در ۲۶.۴ آن را اثبات کرده‌ایم.

یادآوری ۵۴.۴. یک گروه مرتب آبلی Γ دارای رتبه‌ی 1 است اگروتنهااگر ایزومورف ترتیبی با یک زیرگروه نابدیهی از $(\mathbb{R}, +, 0, \leq)$ باشد.

[7] equivalence relation

از آنجا که Γ رتبه‌ی 1 دارد، پس بنا به این قضیه یک نگاشت نشاندنِ r از Γ به $\mathbb{R}$ وجود دارد. با ترکیبِ r و نگاشت کانونی که هر عنصرِ $x \in K$ را به $[x]_\equiv$ می‌برد به نگاشتی از K به $\mathbb{R}$ می‌رسیم و آن را با φ نشان می‌دهیم.

- **مرحله‌ی سوم:** با استفاده از نگاشتِ φ نگاشت $|\ |: K \to \mathbb{R}^+$ را به صورت زیر تعریف می‌کنیم:

$$|x| = \begin{cases} 0 & x = 0 \\ e^{-\varphi(x)} & x \neq 0 \end{cases} \tag{۲.۴}$$

در ادامه، نشان خواهیم داد که نگاشت فوق دارای ویژگی‌های قدرمطلق است که در تعریفِ ۱۵.۴ آن‌ها را بیان کرده‌ایم. با توجه به اینکه برای تعریف نگاشت فوق از تابع نمایی(e^x) استفاده کرده‌ایم، به سادگی برای هر $x, y \in K$، نتایج زیر برقرار است:

۱. $|x| \geq 0$،

۲. $|xy| = |x|\ |y|$،

۳. $|x| = 0$ اگروتنهااگر $x = 0$.

بنابراین برای تکمیل اثبات قدرمطلق بودن نگاشت (۱.۱)، تنها اثبات ویژگی نامساوی مثلثی باقی می‌ماند که در ادامه به آن می‌پردازیم.

ابتدا، نشان می‌دهیم که به ازای یک عدد حقیقی مثبتِ v، نگاشت $|\ |^v$ قدر مطلق است.

بنا به لم ۴۸.۴، N یک مجموعه‌ی تقریباً ارزیاب است، بنابراین یک عنصرِ $c \in N^\times$ وجود دارد به طوری که $c(N \pm N) \subseteq N$. ادعا می‌کنیم که برای هر $x, y \in K^\times$ داریم $|x+y| \leq |c^{-1}| \max\{|x|, |y|\}$. برای اثبات این ادعا، دو عنصرِ $x, y \in K^\times$ را در نظر بگیرید. بدون کاستن از کلیت فرض کنید $|x| \leq |y|$. به عبارت دیگر، $e^{-\varphi(x)} \leq e^{-\varphi(y)}$ بنابراین $\varphi(y) \leq \varphi(x)$. با توجه به اینکه r ترتیب را حفظ می‌کند، نتیجه می‌گیریم که $[y]_\equiv \leq [x]_\equiv$، پس yRx. بنابراین بنا به نحوه‌ی تعریف رابطه‌ی R، یک عنصرِ $z \in N$ وجود دارد به طوری که $x = yz$. در نتیجه با توجه به اینکه $c(N \pm N) \subseteq N$ و $1 \in N$ داریم $x + y = y \cdot (z+1) \in y \cdot c^{-1}N$، پس $yc^{-1}R(x+y)$، یعنی $[yc^{-1}]_\equiv \leq [x+y]_\equiv$ و از این رو، $|x+y| \leq |c^{-1}||y|$.

از طرفی، $c \in N$ و بنابراین $|c| \leq 1$، در نتیجه $|c^{-1}| \geq 1$. حال یک عنصرِ v در $\mathbb{R}^+$ را آنقدر کوچک انتخاب می‌کنیم که $|c^{-1}|^v \leq 2$. برای ادامه‌ی اثبات به جای $|\ |^v$ از همان نمادِ $|\ |$ استفاده می‌کنیم. پس تا اینجا نشان دادیم که $|x+y| \leq 2\max\{|x|, |y|\}$.

نامساوی فوق را برای $n = 2^m$ و $x_1, x_2, ..., x_n \in K$ به صورت زیر بازنویسی می‌کنیم:

$$|x_1 + x_2 + ... + x_n| \leq n \max_i |x_i|. \tag{۳.۴}$$

حال n را یک عدد طبیعی دلخواه در نظر بگیرید. سپس برای i از $n+1$ تا اولین توانِ 2 بزرگتر از n، عنصر x_i را برابر با صفر قرار می‌دهیم. در این صورت با توجه به نامساوی (۳.۴) داریم:

$$|x_1 + x_2 + ... + x_n| \leq 2n \max_i |x_i|.$$

در نتیجه، به طور خاص برای $n = 1$ و هر عنصر مثبتِ x نامساوی $|x| < 2x$ برقرار است. بنابراین

$$\begin{aligned} |x+y|^n = |(x+y)^n| &\leq 2(n+1) \max_i \left\{ |\tbinom{n}{i} x^i y^{n-i}| \right\} \\ &\leq 4(n+1) \max_i \left\{ |x|^i |y|^{n-i} \right\} \\ &\leq 4(n+1) \sum_{i=1}^{n} \binom{n}{i} |x|^i |y|^{n-i} = 4(n+1)(|x| + |y|)^n. \end{aligned}$$

حال اگر از طرفین ریشه‌ی nـ اُم بگیریم به نامساوی

$$|x+y| \leq \sqrt[n]{4(n+1)}(|x| + |y|)$$

می‌رسیم که نهایتاً با میل دادن n به بی‌نهایت نتیجه مطلوبِ $|x+y| \leq |x| + |y|$ حاصل می‌شود. در نتیجه $|\ |$ یک نگاشت قدرمطلق است.

- **مرحله‌ی چهارم:** بنا به آنچه که در بخشِ ۲.۱.۴ دیدیم، نگاشت قدرمطلقِ $|\ |$ روی K توپولوژیِ $\tau_{||}$ را القاء می‌کند که در آن مجموعه‌ی متشکل از گوی‌هایی به صورت $S(\epsilon) = \{x \in K : |x| < \epsilon\}$ به ازای هر عدد حقیقی و مثبتِ ϵ، یک پایه برای همسایگی‌های حول 0 است. در ادامه، می‌خواهیم نشان دهیم که $\tau_{||} = \tau$، به بیان دیگر $||$ یک توپولوژی برابر با Vـ توپولوژیِ τ روی میدانِ K القاء می‌کند.

۱. هر گوی $S(\epsilon)$ شامل یک گوی $W \in \tau$ است: یک عنصر $a \in K$ را انتخاب می‌کنیم که در شرط $|a|^{-1} < \epsilon$ صدق کند. در لم ۴۷.۴ ثابت کردیم که مجموعه‌ی متشکل از همه‌ی عناصر پوچ‌توان (N_0) یک همسایگی در τ است. حال بنا به توجه ۸.۴ یک گوی $W \in \tau$ وجود دارد به طوری که $aW \subseteq N_0$ یا به بیان دیگر $W \subseteq a^{-1}N_0$. ادعا می‌کنیم که $a^{-1}N_0 = S(|a^{-1}|)$.

برای اثبات این ادعا، فرض کنید $x \in S(|a^{-1}|)$. در این صورت $|x| < |a^{-1}|$، بنابراین با توجه به نحوه‌ی تعریف نگاشتِ $|\ |$ در (۱.۱)، داریم $e^{-\varphi(x)} \leq e^{-\varphi(a^{-1})}$ و در نتیجه $\varphi(a^{-1}) < \varphi(x)$. از آنجا که φ ترکیب دو نگاشت r و نگاشت کانونی است و در قسمتی از اثبات قضیه‌ی ۲۶.۴ نشان

دادیم که نگاشت r ترتیب را حفظ می‌کند، پس $[x]_\equiv < [a^{-1}]_\equiv$. مطابق تعریف ترتیب در گروه Γ از اینکه $[x]_\equiv < [a^{-1}]_\equiv$ نتیجه می‌گیریم که $x \in a^{-1}N$. توجه کنید که به ویژه $x \in a^{-1}N_0$، یعنی عنصر x به صورت حاصل‌ضرب a^{-1} یک عنصر پوچ‌توان است، زیرا در غیر این صورت اگر x برابر با $a^{-1} \cdot t$ باشد که در آن t یک عنصر خنثی است، آنگاه $[x]_\equiv = [a^{-1}]_\equiv$. بنابراین تا اینجا نشان دادیم که $S(|a^{-1}|) \subseteq a^{-1}N_0$. حال می‌خواهیم نشان دهیم که $a^{-1}N_0 \subseteq S(|a^{-1}|)$. به این منظور، یک عنصر دلخواهِ x در $a^{-1}N_0$ در نظر بگیرید. بنابراین با توجه به نحوه‌ی تعریف ترتیبِ $\leq$ روی Γ داریم $[x]_\equiv < [a^{-1}]_\equiv$ و در نتیجه $e^{-\varphi(x)} < e^{-\varphi(a^{-1})}$، یعنی $|x| < |a^{-1}|$ پس $x \in S(|a^{-1}|)$.

در نتیجه نهایتاً داریم $W \subseteq S(|a^{-1}|) \subseteq S(\epsilon)$.

۲. هر گوی $W \in \tau$ شامل یک بازِ $S(\epsilon)$ است: از آنجا که مطابق با لم **۴۷.۴** مجموعه‌ی N_0 کراندار است، پس به ازای هر $W \in \tau$، یک عنصر $b \in K^\times$ وجود دارد به طوری که $bN_0 \subseteq W$. همان‌طور که در بالا نشان دادیم $bN_0 = S(|b|)$، بنابراین $S(|b|) \subseteq W$.

$\square$

---

* خلاصه‌ی فصل:

می‌گوییم (K, τ) یک میدان توپولوژیک است هرگاه τ یک توپولوژی هاسدورف روی میدان K باشد که اعمال میدان نسبت به آن پیوسته هستند. در این صورت، برای شناساندن این توپولوژی کافی است یک پایه‌ی متشکل از همسایگی‌های حول صفر را به کار گیریم، زیرا سایر همسایگی‌ها حول دیگر نقاط با انتقال همسایگی‌های صفر به دست می‌آیند. اگر در یک توپولوژی میدانی τ به ازای هر گوی $U \in \tau$ مجموعه‌ی $(K \setminus U)^{-1}$ کراندار باشد، آنگاه می‌گوییم τ یک Vـ توپولوژی است.

توپولوژی القاء شده توسط یک نگاشت ارزیابی و یک نگاشت قدر مطلق Vـ توپولوژی هستند و به علاوه قضیه‌ای بیان می‌کند که هر Vـ توپولوژی از یک ارزیابی یا یک قدرمطلق ناشی شده است. در واقع بسته به تعداد عناصر پوچ‌توان در میدان Vـ توپولوژیک دو حالت زیر رخ می‌دهد:

۱. اگر هیچ عنصر پوچ‌توانی در میدان Vـ توپولوژیک وجود نداشته باشد، در این صورت یک نگاشت ارزیابی روی میدان وجود دارد که توپولوژی یکسانی با τ القاء می‌کند. برای اثبات این حالت کافی است یک حلقه‌ی تقریباً ارزیاب خاصی را در K در نظر بگیریم و سپس با چند ترفند آن را تبدیل به یک حلقه‌ی ارزیاب کنیم. نگاشت ارزیابی که از این حلقه‌ی ارزیاب ناشی می‌شود همان نگاشت مطلوب ماست.

۲. اگر حداقل یک عنصر پوچ‌توان در میدان Vـ توپولوژیک وجود داشته باشد، در این صورت یک نگاشت قدرمطلق روی میدان وجود دارد که یک توپولوژی برابر با τ القاء می‌کند. برای اثبات این حالت ابتدا یک رابطه‌ی هم‌ارزی روی میدان تعریف می‌کنیم و مجموعه‌ی متشکل از کلاس‌های هم‌ارزی آن را Γ می‌نامیم. این مجموعه بنا به ویژگی‌های مناسبی که رابطه‌ی هم‌ارزی مذکور دارد، یک گروه مرتب ارشمیدسی است. در نتیجه یک نگاشت نشاندن از آن به $\mathbb{R}$ وجود دارد. همچنین یک نگاشت کانونی از میدان به مجموعه‌ی Γ وجود دارد که هر عنصر از میدان را به کلاس هم ارزی آن می‌برد. ترکیب این دو نگاشت را φ می‌نامیم که نگاشتی از میدان به $\mathbb{R}$ است. نگاشت قدرمطلق مطلوب ما به ازای عناصر ناصفر $e^{-\varphi(x)}$ و برای 0 برابر با صفر است.

فصل ۵

میدانِ t ـ هنسلی

در این فصل، قصد داریم به یک دسته از میدان‌های توپولوژیک به نام میدان‌های t ـ هنسلی بپردازیم و برخی از ویژگی‌های آن‌ها را بررسی کنیم. برای بیان ویژگی‌های منطقی میدان‌های t ـ هنسلی از فرمول‌های خاصی که فرمول‌های موضعی نام دارند، استفاده می‌کنیم.

هدف اصلی این فصل، این است که نشان دهیم اگر (K,τ) یک میدان t ـ هنسلی باشد که بسته‌ی جدایی‌پذیر نیست، آن‌گاه یک همسایگی باز و کراندار و تعریف‌پذیر حول صفر وجود دارد. این همسایگی را به صورت $U_{f,a} := \{\frac{1}{f(x)} - \frac{1}{f(a)} : x \in K\}$ می‌سازیم که در آن $f \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر و جدایی‌پذیر است به طوری که در K ریشه‌ای ندارد و همچنین $a \in K$ در شرط $f'(a) \neq 0$ صدق می‌کند. در این راستا، دو قضیه اثبات می‌کنیم: ابتدا اثبات می‌کنیم که $\{f(x)^{-1} : x \in K\}$ یک مجموعه‌ی کراندار است و سپس نشان می‌دهیم که $\{f(a) : f'(a) \neq 0\}$ یک مجموعه‌ی باز است. برای اثبات این دو قضیه یکی از مهم‌ترین قضایایی که به کار می‌گیریم، این است که اگر (K,τ) یک میدانِ t ـ هنسلی باشد، آن‌گاه برای τ یک پایه متشکل از ایده‌آل‌های ارزیاب هنسلی وجود دارد(برای تعریف ایده‌آل ارزیاب هنسلی به ۳۲.۵ رجوع کنید.)

مطالب این فصل از مقاله‌ی [۲۲] جمع‌آوری و بسط داده شده است.

۱.۵ معرفی فرمول‌های موضعی

در این بخش، نوع خاصی از فرمول‌ها به نام فرمول‌های موضعی را معرفی می‌کنیم که با استفاده از آن‌ها می‌توان ویژگی‌های یک میدان توپولوژیک (K,τ) را بیان کرد. این فرمول‌ها در یک دستور زبان خاصی نوشته می‌شوند که در آن دو دسته متغیر وجود دارد: متغیرهای مربوط به عناصر میدانِ K که با نمادهای $x,y,z,\cdots$ و متغیرهای مربوط به گوی‌های باز در توپولوژی τ که با نمادهای $U,V,W,\cdots$ نشان داده می‌شوند. فرمول‌ها در این زبان به صورت استقرایی و به شرح زیر ساخته می‌شوند:

- **ترم:** یک ترم از نمادهای ثوابت 0 و 1 و متغیرهای $x,y,\cdots$ و نمادهای تابعی $+,-,\cdot$ ساخته می‌شود.
- **فرمول اتمی:** فرمول‌های اتمی به صورتِ $t_1=t_2$ و $t_1\in U$ هستند که در آن t_1 و t_2 ترم هستند و U یک باز است.
- **فرمول:** فرمول‌ها از فرمول‌های اتمی و ادوات منطقی $\neg$، $\vee$، $\wedge$، $\exists$، $\forall$ ساخته می‌شوند. توجه کنید که سورهای $\exists$ و $\forall$ روی هر دو نوع متغیر $x,\cdots$ و $U,\cdots$ اعمال می‌شوند.

تعریف ۱.۵. می‌گوییم فرمولِ φ در حالت *نرمال نقیض* [1] است هرگاه در آن علامت نقیض فقط قبل از فرمول‌های اتمی به کار رفته باشد.

مثال ۲.۵. فرمولِ $\neg(t_1=t_2)\vee\neg(t_1\in U)$ یک فرمول در حالت نرمال نقیض است.

توجه ۳.۵. می‌توان با استفاده از قوانین منطقی هر فرمولِ φ را به یک فرمول معادل [2] در حالت نرمال نقیض تبدیل کرد که آن را با نماد $\bar{\varphi}$ نشان می‌دهیم. مثلاً $\neg(t_1=t_2\wedge t_2\in U)$ معادل است با $\neg(t_1=t_2)\vee\neg(t_2\in U)$ که یک فرمول در حالت نرمال نقیض است.

تعریف ۴.۵. فرض کنید فرمولِ φ در حالت نرمال نقیض باشد. می‌گوییم φ در U مثبت است هرگاه هیچ زیرفرمولی به صورتِ $\neg(t\in U)$ نداشته باشد. همچنین می‌گوییم فرمولِ φ در U منفی است هرگاه در φ فرمول اتمی $t\in U$ فقط به صورت $\neg(t\in U)$ به کار رفته باشد.

توجه کنید که یک فرمول نامنفی در یک U لزوماً در U مثبت نیست، مثلاً $(t\in U)\vee\neg(t\in U)$.

تعریف ۵.۵. فرمولِ φ را یک *فرمول موضعی* می‌نامیم هرگاه در $\bar{\varphi}$ سور $\exists U$ فقط به شرطی در زیرفرمولی مانند ψ قرار بگیرد که ψ یک فرمول منفی در U باشد و سورِ $\forall U$ تنها در زیرفرمول‌هایی که در U مثبت هستند، به کار رفته باشد. منظور از یک جمله‌ی موضعی، یک فرمول موضعی بدون متغیر آزاد است.

[1] negation normal form
[2] logically equivalent

مثال ۶.۵. فرمولِ $\varphi = \forall U \ \ \forall x \ \ \exists V \ \ \forall y \ (y \in V \to x \cdot y \in U)$ یک فرمول موضعی است، زیرا $\bar{\varphi} = \forall U \ \ \forall x \ \ \exists V \ \ \forall y \ (x.y \in U \vee \neg(y \in V))$ که در آن $\forall U$ برای یک زیرفرمول اتمیِ $(x \cdot y \in U)$ که در U مثبت است و $\exists V$ برای یک زیرفرمول اتمیِ $\neg(y \in V)$ که در V منفی است، به کار رفته است.

توجه ۷.۵. ویژگی‌های یک میدان Vـ توپولوژیک، که در تعریفِ ۶.۴ بیان شد، را می‌توان با استفاده از فرمول‌های موضعی به صورت زیر بیان کرد:

۱. $\forall U \ \exists x \ (x \neq 0 \wedge x \in U) \wedge \forall x (x = 0 \leftrightarrow \forall V \ x \in V)$

۲. $\forall U \ \forall V \ \exists W \ \forall x \ (x \in U \wedge x \in V \to x \in W)$

۳. $\forall U \ \exists V \ \forall x \ \forall y \ (x \in V \wedge y \in V \to x - y \in U)$

۴. $\forall U \ \exists V \ \forall x \ \forall y \ (x \in V \wedge y \in V \to x \cdot y \in U)$

۵. $\forall U \ \exists V \ \forall x \ \exists y \ (x \in V \to (y \in U \wedge (1+x) \cdot (1+y) = 1))$

۶. $\forall U \ \exists V \ \forall x \ \forall y \ (x \cdot y \in V \to (x \in U \vee y \in U))$

توجه کنید که مشابه فصل ۴، همسایگی‌های حول نقطه‌ی صفر در نظر گرفته شده اند.

تعریف ۸.۵. می‌گوییم دو میدان توپولوژیکِ (K, τ) و (K', τ') *به طور موضعی معادلند* هرگاه برای هر جمله‌ی موضعی φ داشته باشیم:

$$(K, \tau) \models \varphi \iff (K', \tau') \models \varphi.$$

۲.۵ میدان‌های ω ـ کامل

در انتهای این بخش، خواهیم دید که بنا به قضیه‌ی ۱۹.۵، می‌توانیم برای هر میدان توپولوژیک، یک میدان توپولوژیکِ ω ـ کامل پیدا کنیم که با آن به طور موضعی معادل است؛ یعنی برای میدان توپولوژیکِ (K, τ) یک میدان توپولوژیکِ (K^*, τ^*) وجود دارد به طوری که اولاً هر جمله‌ی موضعی در (K, τ) برقرار است اگروتنهااگر در (K^*, τ^*) برقرار باشد، ثانیاً τ^* یک توپولوژی ω ـ کامل است، یعنی اشتراک هر شمارا تا مجموعه در τ^* باز هم متعلق به τ^* است. به این ترتیب، هرگاه بخواهیم بررسی کنیم که یک فرمول موضعی در یک میدان توپولوژیک برقرار است یا خیر، می‌توانیم فرض کنیم که آن میدان توپولوژیک، ω ـ کامل است.

برای اثبات قضیه‌ی مذکور نیازمند مقدماتی درباره‌ی فرافیلترها هستیم که در زیربخش پیش‌رو به آن می‌پردازیم.

۱.۲.۵ فیلترها

تعریف ۹.۵. فرض کنید I یک مجموعه‌ی ناتهی باشد. یک گردایه‌ی F از زیرمجموعه‌های I را یک فیلتر روی I می‌نامیم، هرگاه شرایط زیر برقرار باشد:

۱. اگر $A, B \in F$ آنگاه $A \cap B \in F$،

۲. اگر $A \in F$ و $A \subseteq B$ آنگاه $B \in F$،

۳. $I \in F$ و $\emptyset \notin F$.

مثال ۱۰.۵. مجموعه‌ی $\{X \subseteq \mathbb{N} : \mathbb{N} \setminus X$متناهی است$\}$ یک فیلتر روی $\mathbb{N}$ است که به آن فیلتر فِرِشه می‌گویند.

تعریف ۱۱.۵. یک فیلتر τ را ω ـ *کامل* می‌نامیم هرگاه تحت اشتراک‌گیری شمارا بسته باشد. به بیان دیگر، اشتراک هر **شمارا** تا مجموعه در τ باز هم متعلق به τ باشد. همچنین، یک میدان توپولوژیکِ (K, τ) را ω ـ کامل می‌نامیم، هرگاه τ یک فیلترِ ω ـ کامل باشد.

تعریف ۱۲.۵. فرض کنید که I یک مجموعه‌ی ناتهی باشد و $A \subseteq I$. در این صورت، به مجموعه‌ی $\langle A \rangle = \{B \subseteq I : A \subseteq B\}$ *فیلتر اصلی تولید شده توسط* A گفته می‌شود. اگر F یک فیلتر روی I باشد و هیچ زیرمجموعه‌ی A از I وجود نداشته باشد به طوری که $F = \langle A \rangle$، آنگاه F را یک *فیلتر غیراصلی* می‌نامیم.

به عنوان مثال به سادگی می‌توان دید که فیلتر فرشه یک فیلتر غیراصلی روی $\mathbb{N}$ است.

تعریف ۱۳.۵. فیلترِ F روی مجموعه‌ی I را یک *فرافیلتر* روی I می‌نامیم هرگاه به ازای هر $A \subseteq I$ داشته باشیم، $A \in F$ یا $A^c \in F$.

در واقع اگر F نسبت به رابطه‌ی شمول، یک عنصر ماکسیمال برای مجموعه‌ی فیلترهای روی یک مجموعه‌ی I باشد، آنگاه می‌توان نشان داد که F یک فرافیلتر است.

لم ۱۴.۵. فرض کنید I یک مجموعه‌ی ناتهی و F یک فیلتر روی آن باشد. در این صورت، یک فرافیلترِ F^* وجود دارد به طوری که $F \subseteq F^*$.

اثبات. مجموعه‌ی $\mathcal{P}_F = \{F' :$ یک فیلتر شامل F است $F'\}$ را در نظر بگیرید. توجه کنید که چون $F \in \mathcal{P}_F$، پس $\mathcal{P}_F$ ناتهی است. به سادگی می‌توان بررسی کرد که $(\mathcal{P}_F, \subseteq)$ در شرط لم زُرن صدق می‌کند. بنابراین، $\mathcal{P}_F$ دارای یک عنصر ماکسیمالِ F^* است. بنا به توضیحات فوق، این عنصر ماکسیمال یک فرافیلتر روی مجموعه‌ی I است. □

نتیجه ۱۵.۵. یک فرافیلتر روی $\mathbb{N}$ شامل فیلتر فرشه وجود دارد.

لم ۱۶.۵. هر فرافیلتر غیراصلی روی $\mathbb{N}$ شامل فیلتر فرشه است.

اثبات. فرض کنید F یک فرافیلتر غیراصلی روی $\mathbb{N}$ باشد. توجه کنید که چون F یک فرافیلتر است، پس به ازای هر $x \in \mathbb{N}$ داریم یا $\{x\} \in F$ یا $\mathbb{N} \setminus \{x\} \in F$. اما F غیراصلی است، بنابراین $\{x\} \notin F$، زیرا در غیر این صورت F یک فرافیلتر اصلی تولید شده توسط $\{x\}$ خواهد بود، پس $\mathbb{N} \setminus \{x\} \in F$. حال یک مجموعه‌ی متناهی $A \subseteq \mathbb{N}$ را در نظر بگیرید. در این صورت $\mathbb{N} \setminus A = \bigcap\limits_{x \in A} (\mathbb{N} \setminus \{x\})$ و به بیان دیگر $\mathbb{N} \setminus A$ برابر با اشتراک تعداد متناهی تا عضو از F است، بنابراین $\mathbb{N} \setminus A \in F$. از این رو، به ازای هر مجموعه‌ی متناهی $A \subseteq \mathbb{N}$ داریم $\mathbb{N} \setminus A \in F$، پس F شامل همه‌ی مجموعه‌های متمم متناهی و در نتیجه شامل فیلتر فرشه است. □

لم ۱۷.۵. فرض کنید F یک فرافیلتر غیراصلی روی $\mathbb{N}$ باشد. در این صورت، یک دنباله به صورت $\mathbb{N} = F_1 \supseteq F_2 \supseteq \cdots$ از اعضای F با اشتراک تهی وجود دارد.

اثبات. قرار دهید $F_1 = \mathbb{N}$. برای هر $n \geq 2$ تعریف می‌کنیم $F_n = \{i \in \mathbb{N} : i \geq n\}$. برای اینکه اثبات کنیم دنباله‌ی فوق یک دنباله نزولی از زیرمجموعه‌های F با اشتراک تهی است، باید دو شرط را بررسی کنیم: برای هر $n \in \mathbb{N}$ اولاً $F_n \in F$ و ثانیاً $F_{n+1} \subseteq F_n$.

برای شرط اول، توجه کنید که چون F یک فیلتر روی $\mathbb{N}$ است، پس شامل $F_1 = \mathbb{N}$ می‌شود. از طرفی F_n شامل تمام اعداد طبیعی بزرگتر یا مساوی n است، پس $\mathbb{N} \setminus F_n$ متناهی است. بنابراین با توجه به اینکه F یک فرافیلتر غیراصلی است، پس بنا به لم فوق شامل فیلتر فرشه است و از این نتیجه می‌شود که برای هر $n \geq 2$ نیز F_n متعلق به F است.

برای شرط دوم، توجه کنید که برای هر $n \in \mathbb{N}$، مجموعه‌ی F_{n+1} شامل تمامی اعداد طبیعی بزرگتر مساوی $n+1$ است، بنابراین بوضوح $F_{n+1} \subseteq F_n$. همچنین با توجه به نحوه‌ی ساخت این دنباله واضح است که اشتراک همه‌ی اعضای آن، تهی است. □

۲.۲.۵ معادل بودن موضعی با یک میدان ω ـ کامل

فرض کنید (K, τ) یک میدان توپولوژیک باشد. برای یافتن میدان توپولوژیک ω ـ کاملِ (K^*, τ^*) که به طور موضعی با (K, τ) معادل است ابتدا یک فرافیلتر غیراصلی روی $\mathbb{N}$ در نظر می‌گیریم. نشان می‌دهیم که مجموعه‌ی M متشکل از تمام عناصرِ $(a_i)_{i \in \mathbb{N}} \in K^{\mathbb{N}}$ به طوری که $\{i : a_i = 0\} \in F$ یک ایده‌آل ماکسیمال از حلقه‌ی $K^{\mathbb{N}}$ است و از این رو $K^* = K^{\mathbb{N}}/M$ یک میدان است. سپس برای هر $U = (U_0, U_1, \cdots) \in \tau^{\mathbb{N}}$، مجموعه‌ی U^* را به صورت $\{a^* : a \in K^{\mathbb{N}}, \{i : a_i \in U_i\} \in F\}$ تعریف می‌کنیم. نهایتاً خواهیم دید که فیلتر تولید شده توسط مجموعه‌ی متشکل از همه‌ی U^*ها، یک فیلتر ω ـ کامل روی K^* است. برهان به طور موضعی معادل بودن (K^*, τ^*) با (K, τ) را به عهده‌ی خواننده قرار می‌دهیم. البته اثبات این قضیه در پیوست مقاله‌ی [۲۲] به تفصیل آورده شده است.

لم ۱۸.۵. فرض کنید K یک میدان و F یک فرافیلتر غیر اصلی روی $\mathbb{N}$ باشد. در این صورت، مجموعه‌ی M متشکل از همه‌ی عناصرِ $(a_i)_{i\in\mathbb{N}} \in K^{\mathbb{N}}$ با این ویژگی که $\{i : a_i = 0\}$ در F باشد(عناصر تقریباً همه جا صفر)، یک ایده‌آل ماکسیمال از حلقه‌ی $K^{\mathbb{N}}$ است.

اثبات. نشان می‌دهیم که اولاً مجموعه‌ی M یک ایده‌آل از حلقه‌ی $K^{\mathbb{N}}$ است. ثانیاً این ایده‌آل ، ماکسیمال است.

به این منظور، دو عنصر دلخواهِ $(a_i)_{i\in\mathbb{N}}$ و $(b_i)_{i\in\mathbb{N}}$ را در M در نظر بگیرید. بنابراین داریم $\{i : a_i = 0\} \in F$ و $\{i : b_i = 0\} \in F$. توجه کنید که داریم

$$\{i : a_i = 0\} \cap \{i : b_i = 0\} \subseteq \{i : (a_i + b_i) = 0\}$$

لذا با توجه به ویژگی‌های ۱ و ۲ در تعریفِ ۹.۵، نتیجه می‌گیریم که $\{i : (a_i + b_i) = 0\} \in F$ و از این رو، $(a_i + b_i)_{i\in\mathbb{N}} \in M$. همچنین، بوضوح مجموعه‌ی M شامل عنصرِ 0 حلقه‌ی $K^{\mathbb{N}}$، یعنی $(0, 0, \cdots)$ است و اگر $(a_i)_{i\in\mathbb{N}} \in M$، آنگاه $(-a_i)_{i\in\mathbb{N}} \in M$. پس تا اینجا نشان دادیم که $(M, +)$ یک زیرگروه از $(K^{\mathbb{N}}, +)$ است. حال فرض کنید $(b_i)_{i\in\mathbb{N}} \in K^{\mathbb{N}}$ و $(a_i)_{i\in\mathbb{N}} \in M$. در این صورت، $\{i : a_i = 0\} \in F$ و از آنجا که $\{i : a_i = 0\} \subseteq \{i : a_ib_i = 0\} = \{i : a_i = 0\} \cup \{i : b_i = 0\}$ نتیجه می‌گیریم که $\{i : a_ib_i = 0\} \in F$، پس $(a_ib_i)_{i\in\mathbb{N}} \in M$. بنابراین M یک ایده‌آل از حلقه‌ی $K^{\mathbb{N}}$ است.

برای اثبات اینکه M یک ایده‌آل ماکسیمال است، نشان می‌دهیم که اگر یک عنصر دیگر از حلقه‌ی $K^{\mathbb{N}}$ به M اضافه کنیم، ایده‌آل تولید شده توسط M و این عنصر، شامل عنصر یکه می‌شود.

فرض کنید $(b_i)_{i\in\mathbb{N}} \in K^{\mathbb{N}}$ در ایده‌آلِ M نباشد، یعنی مجموعه‌ی $\{i : b_i = 0\}$ در F قرار ندارد. از آنجایی که F یک فرافیلتر است، پس $\{i : b_i \neq 0\} \in F$. حال یک دنباله‌ی $(b'_i)_{i\in\mathbb{N}}$ از عناصرِ K را به این صورت تعریف می‌کنیم: برای هر $i \in \mathbb{N}$ که $b_i = 0$، قرار می‌دهیم $b'_i = 1$ و برای هر $i \in \mathbb{N}$ که $b_i \neq 0$، قرار می‌دهیم $b'_i = 0$. با توجه به اینکه $\{i : b'_i = 0\} = \{i : b_i \neq 0\}$، پس $\{i : b'_i = 0\}$ در F قرار دارد؛ در نتیجه $(b')_{i\in\mathbb{N}} \in M$. حال عنصرِ $(b_i + b'_i)_{i\in\mathbb{N}}$ را در نظر بگیرید. از آنجا که تک تک اعضای این دنباله ناصفر هستند، پس یک عنصر وارون‌پذیر در $K^{\mathbb{N}}$ است. بنابراین ایده‌آل تولید شده توسط M و عنصر $(b_i)_{i\in\mathbb{N}}$ شامل عنصر وارون‌پذیر $(b_i + b'_i)_{i\in\mathbb{N}}$ است، پس 1 نیز در این ایده‌آل قرار می‌گیرد. در نتیجه $M\langle(b_i)_{i\in\mathbb{N}}\rangle$، یعنی ایده‌آل تولید شده توسط M و عنصر $(b_i)_{i\in\mathbb{N}}$ برابر با $K^{\mathbb{N}}$ است. به عبارت دیگر، نشان دادیم که هر ایده‌آل N روی حلقه‌ی $K^{\mathbb{N}}$ که $M \subset N$ برابر با خودِ حلقه‌ی $K^{\mathbb{N}}$ است، پس M یک ایده‌آل ماکسیمال است. □

قضیه ۱۹.۵. هر میدان توپولوژیکِ (K, τ) با یک میدان توپولوژیکِ ω ـ کامل به طور موضعی معادل است.

اثبات. یک فرافیلتر غیراصلی F روی $\mathbb{N}$ در نظر بگیرید. بنا به لم ۱۸.۵ مجموعه‌ی M متشکل از تمام عناصرِ $(a_i)_{i\in\mathbb{N}} \in K^{\mathbb{N}}$ به طوری که $\{i : a_i = 0\} \in F$ یک ایده‌آل ماکسیمال از حلقه‌ی $K^{\mathbb{N}}$ است؛ پس $K^* = K^{\mathbb{N}}/M$ یک میدان است.

فرض کنید a یک عنصر از $K^{\mathbb{N}}$ باشد. تصویر این عنصر را تحت نگاشت کانونی از $K^{\mathbb{N}}$ به K^* را با a^* نشان می‌دهیم. با استقرا روی ترم‌ها می‌توان نشان داد که برای هر دو ترمِ t_1 و t_2 و عناصر $a_1, \cdots, a_n \in K^{\mathbb{N}}$ داریم:

$$t_1^{K^*}[a_1^*, \cdots, a_n^*] = t_2^{K^*}[a_1^*, \cdots, a_n^*] \iff \{i \in \mathbb{N} : t_1^K[a_{1i}, \cdots, a_{ni}] = t_2^K[a_{1i}, \cdots, a_{ni}]\} \in F.$$

در عبارت فوق به ازای هر $a_j \in K^{\mathbb{N}}$، منظور از نمادِ a_{ji} همان iاُمین عنصر دنباله‌ی a_j است.

برای هر $U = (U_0, U_1, \cdots) \in \tau^{\mathbb{N}}$، مجموعه‌ی U^* را به صورت زیر تعریف می‌کنیم:

$$U^* = \{a^* : a \in K^{\mathbb{N}}, \{i : a_i \in U_i\} \in F\}.$$

در واقع U^* از عناصر $(a_i)_{i\in\mathbb{N}}$ تشکیل شده که تقریباً همه جا a_i در U_i باشد. فرض کنید مجموعه‌ی β متشکل از همه U^*هایی باشد که U متعلق به $\tau^{\mathbb{N}}$ است. حال فیلتر تولید شده توسط مجموعه‌ی β را در نظر بگیرید و آن را τ^* بنامید. می‌خواهیم نشان دهیم که τ^* یک فیلتر ω ـ کامل است. به عبارت دیگر فرض کنید $V_1 = (V_1^i)_{i\in\mathbb{N}}$ و $V_2 = (V_2^i)_{i\in\mathbb{N}}$ و $V_3 = (V_3^i)_{i\in\mathbb{N}}$ و $\cdots$ شمارا تا گوی در $\tau^{\mathbb{N}}$ باشند. برای اثباتِ ω ـ کامل بودن فیلتر τ^*، باید یک گوی $U \in \tau^{\mathbb{N}}$ بیابیم که به ازای هر $j \in \mathbb{N}$ داشته باشیم $U^* \subseteq V_j^*$. از آنجا که F یک فرافیلتر غیراصلی روی $\mathbb{N}$ است، پس بنا به لم ۱۷.۵ یک دنباله به شکل $\mathbb{N} = F_1 \supseteq F_2 \supseteq \cdots$ از اعضای F با اشتراک تهی وجود دارد. حال مجموعه‌ی $U = (U_0, U_1, U_2, \cdots)$ را به صورت زیر تعریف می‌کنیم:

$$U_i = V_1^i \cap \cdots \cap V_j^i \quad , \quad i \in F_j \setminus F_{j+1}.$$

ادعا می‌کنیم که U همان گوی مطلوب ماست، یعنی $U^* = V_1^* \cap V_2^* \cap V_3^* \cap \cdots$. توجه کنید که برای هر $(a_i)_{i\in\mathbb{N}} \in K^{\mathbb{N}}$ داریم:

$$\{i : a_i \in U_i\} \cap F_j \subset \{i : a_i \in V_j^i\}. \tag{۱.۵}$$

بنا به تعریفِ U^* اگر $a^* \in U^*$، آنگاه $\{i : a_i \in U_i\} \in F$. بنابراین از رابطه‌ی (۱.۵) و ویژگی ۱ تعریفِ ۹.۵ داریم $\{i : a_i \in V_j^i\} \in F$، پس $a^* \in V_j^*$ و در نتیجه τ^* یک توپولوژی ω ـ کامل است. نهایتاً با استقرا روی ساخت فرمول‌ها می‌توان نشان داد که (K, τ) و (K^*, τ^*) به طور موضعی معادلند. (برای مشاهده‌ی اثبات کامل، به پیوست مقاله‌ی [۲۲] مراجعه کنید.) □

۳.۵ یک پایه‌ی متشکل از ایده‌آل‌های ارزیاب در یک Vـ توپولوژی

تعریف ۲۰.۵. فرض کنید K یک میدان باشد. مجموعه‌ی ناتهی $M \subseteq K$ را یک *ایده‌آل ارزیابِ* K می‌نامیم هرگاه $M + M \subset M$، $M \cdot M \subset M$ و $1 \notin M$ همچنین برای هر $x, y \in K$ اگر $x \cdot y \in M$، آنگاه $x \in M$ یا $y \in M$.

در ادامه برای یک Vـتوپولوژیِ τ که ω ـ کامل است یک پایه متشکل از بازهایی می‌سازیم که همگی ایده‌آل ارزیاب هستند. این کار را در چند مرحله انجام می‌دهیم: ابتدا برای هر $U \in \tau$، یک گوی $U_0 \in \tau$ انتخاب می‌کنیم که $U_0 \subset U$ و $1 \notin U_0$. سپس یک دنباله‌ی نزولی از گوی‌های موجود در τ مانندِ $U_0 \supset U_1 \supset U_2 \supset \cdots$ تشکیل می‌دهیم به گونه‌ای که $U_{n+1} + U_{n+1} \subset U_n$ و $U_{n+1} \cdot U_{n+1} \subset U_n$ و برای هر $x, y \in K$ داشته باشیم $x \cdot y \in U_{n+1} \to x \in U_n \vee y \in U_n$. سپس نشان می‌دهیم که $M_U = \bigcap_{n \in \mathbb{N}} U_n$ یک ایده‌آل ارزیاب است. سرانجام M_Uها پایه‌ی مورد نظر ما را تشکیل می‌دهند.

لم ۲۱.۵. فرض کنید (K, τ) یک میدان توپولوژیک و $V \subseteq K$ یک مجموعه‌ی کراندار باشد. در این صورت $\{xV : x \in K \setminus \{0\}\}$ یک پایه برای توپولوژی τ است.

اثبات. از آنجا که V یک مجموعه‌ی کراندار است، پس بنا به لم ۳۱.۴ به ازای هر $U \in \tau$ یک عنصرِ x در $K \setminus \{0\}$ وجود دارد به طوری که $xV \subset U$. با توجه به اینکه (K, τ) یک میدان توپولوژیک است، پس هر xV یک مجموعه‌ی باز است و از این نتیجه می‌شود که مجموعه‌ی $\{xV : x \in K \setminus \{0\}\}$ یک پایه برای توپولوژی τ است. □

لم ۲۲.۵. فرض کنید (K, τ) یک میدان توپولوژیک و σ یک توپولوژی میدانی دیگر روی K باشد که شامل یک مجموعه‌ی کراندار از توپولوژی τ است. در این صورت $\tau \subset \sigma$.

اثبات. فرض کنید V یک مجموعه‌ی کراندار در توپولوژی τ باشد که در σ نیز قرار دارد. بنا به لم ۲۱.۵، مجموعه‌ی $S = \{xV : x \in K \setminus \{0\}\}$ یک پایه برای توپولوژی τ است. از طرفی چون V در σ قرار دارد و σ یک توپولوژی میدانی است، پس به ازای هر $x \in K$ داریم $xV \in \sigma$. به بیان دیگر σ شامل یک پایه از τ است، در نتیجه $\tau \subset \sigma$. □

تعریف ۲۳.۵. یک توپولوژی τ روی یک میدانِ K را مینیمال می‌نامیم هرگاه هر توپولوژی τ' روی K از τ ظریف‌تر باشد، به بیان دیگر، به ازای هر τ' که یک توپولوژی روی میدانِ K است داشته باشیم $\tau \subseteq \tau'$.

قضیه ۲۴.۵. فرض کنید (K, τ) یک میدان Vـ توپولوژیک باشد. در این صورت τ یک توپولوژی مینیمال روی K است.

اثبات. با برهان خلف، فرض کنید یک توپولوژی میدانیِ τ' روی میدانِ K وجود دارد به طوری که $\tau' \subset \tau$. با توجه به ویژگی ۱ در تعریفِ ۶.۴، یک مجموعه‌ی W در τ' وجود دارد به طوری که $1 \notin W$. از طرفی با توجه به ویژگی ۴ در تعریفِ ۶.۴، برای W یک گویِ U در τ' وجود دارد به طوری که $U \cdot U \subseteq W$ و بنابراین $1 \notin U \cdot U$. در نتیجه $U \cap U^{-1} = \emptyset$، یعنی U^{-1} کراندار دور از صفر توسط U است. اما از آنجا که τ یک Vـ توپولوژی است، پس بنا به قضیه‌ی ۳۷.۴، گوی U در توپولوژی τ کراندار است. نهایتاً با توجه به لمِ ۲۲.۵، چون τ' شامل یک مجموعه‌ی کراندار از توپولوژی τ است، پس نتیجه می‌گیریم که $\tau \subset \tau'$ و این تناقض است. □

توجه ۲۵.۵. فرض کنید M یک ایده‌آل ارزیاب در یک میدانِ K باشد. قرار دهید $E = \{x \in K : x, x^{-1} \notin M\}$. در این صورت $A_M = M \cup E$ یک حلقه‌ی ارزیاب از میدانِ K است که M ایده‌آل ماکسیمال آن است. در نتیجه به ازای هر ایده‌آل ارزیاب، یک حلقه‌ی ارزیاب وجود دارد. بنابراین نظیر هر ایده‌آل ارزیابِ M یک توپولوژی τ_M وجود دارد که از حلقه‌ی A_M به دست می‌آید. به این توپولوژی، *توپولوژی تولید شده توسط* M می‌گوییم.

توجه ۲۶.۵. فرض کنید M یک ایده‌آل ارزیاب و A_M حلقه‌ی ارزیاب نظیر آن باشد. در این صورت برای هر $b \in K$ داریم $b \in A_M$ اگروتنهااگر $b^{-1} \notin M$.

قضیه ۲۷.۵. فرض کنید (K, τ) یک میدانِ Vـ توپولوژیکِ ω ـ کامل باشد. در این صورت، توپولوژی τ یک پایه دارد که از ایده‌آل‌های ارزیاب تشکیل شده است؛ همچنین هر کدام از این ایده‌آل‌ها به تنهایی یک توپولوژی روی K تولید می‌کند که با τ برابر است.

اثبات. این قضیه در چهار مرحله و به شرح زیر اثبات می‌گردد:

۱. گوی دلخواهِ $U \in \tau$ را در نظر بگیرید. یک گوی U_0 در τ را با ویژگی‌های $U_0 \subset U$ و $1 \notin U_0$ انتخاب می‌کنیم. برای این کار، از ویژگی‌های ۱ و ۲ در تعریفِ ۷.۵ استفاده می‌کنیم. حال با کمک ویژگی‌های ۲ و ۳ و ۴ و ۶ در تعریف ۷.۵، دنباله‌ی نزولی $U_0 \supset U_1 \supset U_2 \supset \cdots$ را تشکیل می‌دهیم به گونه‌ای که $U_{n+1} + U_{n+1} \subset U_n$ و $U_{n+1} \cdot U_{n+1} \subset U_n$ و برای هر $x, y \in K$ داریم $x \cdot y \in U_{n+1} \to x \in U_n \vee y \in U_n$. توجه کنید که چون τ بنا به فرض ω ـ کامل است، پس مجموعه‌ی $M_U = \bigcap_{n \in \mathbb{N}} U_n$ متعلق به τ است.

۲. ادعا می‌کنیم که M_U یک ایده‌آل ارزیاب است. برای اثبات این ادعا کافی است ویژگی‌های بیان شده در تعریفِ ۲۰.۵ را بررسی کنیم. با توجه به نحوه‌ی ساخت مجموعه‌ی M_U در مرحله‌ی قبل، به سادگی می‌توان نتیجه گرفت که $M_U + M_U \subset M_U$ و $M_U \cdot M_U \subset M_U$. حال اگر $x \cdot y \in M_U$، آنگاه به ازای هر $n \in \mathbb{N}$ داریم $x \cdot y \in U_n$. فرض کنید $x \cdot y \in U_i$ و $x \notin U_{i-1}$ در این صورت با توجه به نحوه‌ی ساخت هر U_i داریم $y \in U_{i-1}$. توجه کنید که بنا به نزولی بودن دنباله‌ی $(U_n)_{n \in \mathbb{N}}$ به ازای هر $j > i$ نیز داریم $x \notin U_j$ و در نتیجه مشابهاً $y \in U_j$. همچنین با توجه به اینکه $U_0 \supset U_1 \supset U_2 \supset \cdots$، پس به ازای هر $j < i$ نیز عنصرِ y در U_j قرار دارد و بنابراین به ازای هر $i \in \mathbb{N}$ داریم $y \in U_n$ و در نتیجه $y \in M_U$. از این رو M_U یک ایده‌آل ارزیاب است.

۳. حلقه‌ی ارزیاب نظیر این ایده‌آل ارزیاب را با A_U نشان می‌دهیم. بنا به قضیه‌ی ۹.۳، یک نگاشت ارزیابی روی میدانِ K وجود دارد به طوری که $O_v = A_U$. این نگاشت ارزیابی یک توپولوژی روی میدانِ K القاء می‌کند که آن را با τ_v نشان می‌دهیم. M_U به عنوان ایده‌آل ماکسیمالِ A_U یک گوی کراندار در τ_v است و در مرحله‌ی ۱، نشان دادیم که $M_U \in \tau$. بنابراین با توجه به لمِ ۲۲.۵ نتیجه می‌شود که $\tau_v \subset \tau$.

۴. با توجه به اینکه τ یک Vـ توپولوژی است، طبق قضیه‌ی ۲۴.۵ یک توپولوژی مینیمال است، بنابراین $\tau_v = \tau$.

طبق مراحل فوق، برای هر $U \in \tau$ یک M_U می‌سازیم. مجموعه‌ی $\mathfrak{B} = \{M_U\}_{U\in\tau}$، یک پایه‌ای متشکل از ایده‌آل‌های ارزیاب برای τ است، زیرا به ازای هر $U \in \tau$ یک $M_U \in \mathfrak{B}$ وجود دارد به طوری که $M_U \subseteq U$. به علاوه همان‌طور که در مرحله‌ی ۴ دیدیم، هر M_U به تنهایی یک توپولوژی روی K تولید می‌کند که برابر با τ است.

□

۴.۵ معرفی میدان‌های t ـ هنسلی

تعریف ۲۸.۵. یک میدان توپولوژیکِ (K,τ) را t ـ *هنسلی* می‌نامیم، هرگاه به طور موضعی با یک میدان توپولوژیکِ (L,τ_v) معادل باشد به طوری که (L,O_v) یک میدان ارزیابی هنسلی است.

در این بخش، نشان می‌دهیم که میدان‌های t ـ هنسلی یک پایه‌ی متشکل از ایده‌آل‌های ارزیاب هنسلی دارند(برای تعریف یک ایده‌آل ارزیاب هنسلی به ۳۲.۵ رجوع کنید.)

نماد گذاری ۲۹.۵. در ادامه، منظورمان از (K,O_v) یک زوج است که در آن K یک میدان و O_v یک حلقه‌ی ارزیاب از آن است. ایده‌آل ماکسیمال این حلقه را با m_v نشان می‌دهیم.

یادآوری ۳۰.۵. یک میدان ارزیابی (K,O_v) هنسلی است هرگاه هر چندجمله‌ای به صورتِ $X^n + X^{n-1} + c_{n-2}X^{n-2} + \cdots + c_0$ که در آن $n \geq 2$ و $c_i \in m_v$ یک ریشه در K داشته باشد(مطابق با آنچه در لم ۱۱.۲ اثبات کردیم).

قضیه ۳۱.۵. فرض کنید (K,τ) یک میدانِ Vـ توپولوژیک باشد. در این صورت (K,τ) یک میدانِ t ـ هنسلی است اگروتنهااگر شرط زیر برقرار باشد:

$(*)$ به ازای هر $n \geq 2$ یک گویِ U در τ وجود داشته باشد به طوری که هر چندجمله‌ای به صورت $x^n + x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ که در آن ضرایب همگی از U هستند، یک ریشه در K داشته باشد.

اثبات. اگر (K,τ) یک میدانِ t ـ هنسلی باشد، آن‌گاه بنا به تعریف ۲۸.۵ به طور موضعی معادل است با یک (L,τ_v) به طوری که (L,O_v) یک میدان ارزیابی هنسلی است. در این صورت اگر U را m_v در نظر بگیریم، آن‌گاه بنا به ۳۰.۵ هر چندجمله‌ای به صورتِ $x^n + x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ که در آن $a_i \in m_v$، در میدانِ L یک ریشه دارد. حال توجه کنید که شرط $(*)$ را برای هر $n \geq 1$ می‌توان به صورت زیر نوشت که یک جمله‌ی موضعی است:

$$\varphi_n = \exists U\ \forall y_{n-2},\cdots,y_0\ (y_{n-2}\in U \wedge \cdots y_0 \in U) \to \exists x\ (x^n + x^{n-1} + y_{n-2}x^{n-2} + \cdots + y_0 = 0).$$

از یک سو، ثابت کردیم که شرط $(*)$ در (L,τ_v) برقرار است. از سوی دیگر، با توجه به اینکه (K,τ) به طور موضعی با (L,τ_v) معادل است و شرطِ $(*)$ به صورت جمله‌های موضعی است، پس می‌توان نتیجه گرفت که شرط $(*)$ در (K,τ) نیز برقرار است.

برای اثبات جهت عکس، فرض کنید شرطِ $(*)$ در میدان Vـ توپولوژیکِ (K,τ) برقرار باشد. به بیان دیگر به ازای هر $n\in\mathbb{N}$، یک گویِ U_n در τ وجود دارد به طوری که چندجمله‌ای‌های $x^n+x^{n-1}+\cdots+y_0$ از درجه‌ی n با ضرایب از U_n در K ریشه دارند. از آنجا که شرطِ $(*)$ را می‌توانیم به صورت جمله‌های موضعی بنویسیم، پس بنا به لم ۱۹.۵ بدون کاستن از کلیت (K,τ) را یک میدان ω ـ کامل در نظر می‌گیریم. حال مطابق با قضیه‌ی ۲۷.۵، به ازای هر U_n ایده‌آل ارزیابِ $M_{U_n}\in\tau$ را تشکیل می‌دهیم. با توجه به این که (K,τ) را یک میدان ω ـ کامل در نظر گرفتیم، مجموعه‌ی $M=\bigcap\limits_{n\in\mathbb{N}} M_{U_n}$ در τ قرار دارد.

مشابه اثبات لمِ ۲۷.۵ می‌توان نتیجه گرفت که M یک ایده‌آل ارزیاب است که به ازای هر $n\geq 1$ داریم $M\subseteq U_n$. همان‌طور که در ۲۵.۵ توضیح داده شد، یک حلقه ارزیاب A_M نظیرِ M وجود دارد به طوری که ایده‌آل ماکسیمال آن همان M است. A_M از یک نگاشت ارزیابیِ v ناشی می‌شود که توپولوژی τ_v را القاء می‌کند. با توجه به اینکه به ازای هر $n\geq 2$ داریم $M\subseteq U_n$، پس بنا به ویژگی هر گوی U_n می‌توانیم نتیجه بگیریم که هر چندجمله‌ای به صورت $x^n+x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_0$ که در آن $a_i\in M$ در K یک ریشه دارد. بنابراین طبق ۳۰.۵، (K,A_M) یک میدان هنسلی و در نتیجه (K,τ_v) یک میدانِ t ـ هنسلی است. از طرفی در قضیه‌ی ۲۷.۵ نشان دادیم که هر ایده‌آل ارزیاب در میدانِ K یک توپولوژی یکسان با τ القاء می‌کند. به عبارت دیگر $\tau_v=\tau$، بنابراین (K,τ) نیز یک میدانِ t ـ هنسلی است. □

تعریف ۳۲.۵. یک ایده‌آل ارزیاب M از میدانِ K را هنسلی می‌نامیم، هرگاه حلقه‌ی ارزیاب A_M (مطابق توجهِ ۲۵.۵) یک حلقه‌ی هنسلی باشد.

نتیجه ۳۳.۵. هر میدان t ـ هنسلی و ω ـ کاملِ (K,τ) یک پایه متشکل از ایده‌آل‌های ارزیاب هنسلی دارد.

اثبات. در قضیه‌ی ۳۱.۵، یک ایده‌آل ارزیاب هنسلی M و در قضیه‌ی ۲۷.۵ یک پایه‌ی متشکل از ایده‌آل‌های ارزیاب $\{M_i\}_{i\in\mathbb{N}}$ برای توپولوژی τ پیدا کردیم. حال مجموعه‌ی $\{M\cap M_i\}_{i\in\mathbb{N}}$ را در نظر بگیرید. به سادگی می‌توان دید که این مجموعه، یک پایه‌ی متشکل از ایده‌آل‌های ارزیاب هنسلی است. □

مثال ۳۴.۵. نگاشت ارزیابی $v:\mathbb{F}_q((t))\to\mathbb{F}_q$ را در نظر بگیرید که هر سری لوران در $\mathbb{F}_q((t))$ را به کوچکترین توان آن می‌برد. این نگاشت یک توپولوژی روی $\mathbb{F}_q((t))$ القاء می‌کند که آن را با نماد τ_v نشان می‌دهیم. از آنجا که بنا به قضیه‌ی ۲۶.۳، میدان ارزیابی $(\mathbb{F}_q((t)),\mathbb{F}_q[[t]])$ هنسلی است، پس $(\mathbb{F}_q((t)),\tau_v)$ یک میدانِ t ـ هنسلی است.

۵.۵ تعریف یک توپولوژی روی $K[x]_1^n$

در این بخش، با توجه به یک میدان توپولوژیکِ (K,τ)، قصد داریم یک توپولوژی روی مجموعه‌ی چندجمله‌ای‌های تکین با حداکثر درجه‌ی n در $K[x]$ تعریف کنیم. در این راستا، بوضوح باید یک پایه برای همسایگی‌های حول هر چندجمله‌ای تکین با حداکثر درجه‌ی n معرفی کنیم.

نماد گذاری ۳۵.۵. فرض کنید K یک میدان باشد و $S \subset K$. مجموعه‌ی چندجمله‌ای‌هایی که ضرایب آن‌ها از $S \cup \{0\}$ است، با $S[x]$ نمایش داده می‌شود. همچنین با نمادِ $S[x]^n$، مجموعه‌ی تمام چندجمله‌ای‌های $f \in S[x]$ با درجه‌ی حداکثر n نمایش داده می‌شود. به علاوه با $S[x]_1^n$، مجموعه‌ی تمام چندجمله‌ای‌های تکینِ $f \in S[x]^n$ را نشان می‌دهیم.

فرض کنید (K,τ) یک میدان توپولوژیک باشد. می‌خواهیم روی مجموعه $K[x]_1^n$ یک توپولوژی تعریف کنیم. به این منظور برای هر چندجمله‌ای $f \in K[x]_1^n$، خانواده‌ی $\{f + U[x]^{n-1}\}_{U\in\tau}$ را به عنوان پایه‌ی همسایگی‌های حول f در نظر می‌گیریم.

قضیه ۳۶.۵. فرض کنید (K,τ) یک میدانِ Vـ توپولوژیک باشد. در این صورت شرایط زیر معادلند:

۱. (K,τ) یک میدانِ t ـ هنسلی است؛ یعنی به ازای هر $n \geq 1$، یک گوی $U \in \tau$ وجود دارد به طوری که برای هر چندجمله‌ای به صورتِ $x^{n+1} + x^n + a_{n-1}x^{n-1} + \cdots + a_0$ که در آن ضرایبِ a_i همگی در U هستند، در K ریشه‌ای دارد.

۲. برای هر n مجموعه‌ی $E_n = \{f \in K[x]_1^n : \deg(f) = n,$ ریشه‌ی ساده دارد K در $f\}$ یک مجموعه‌ی باز در $K[x]_1^n$ است.

اثبات. **اثبات از ۱ به ۲:** برای اثبات این که مجموعه‌ی E_n یک مجموعه‌ی باز است، کافی است نشان دهیم که هر f در این مجموعه، یک نقطه‌ی درونی است. به عبارت دیگر باید یک همسایگی U_f از f پیدا کنیم به طوری که $U_f \subseteq E_n$.

ابتدا توجه کنید که طبق فرض، میدان (K,τ) یک میدانِ t ـ هنسلی است و بنابراین بنا به نتیجه‌ی ۳۳.۵، (K,τ) یک پایه‌ی متشکل از ایده‌آل‌های ارزیاب هنسلی دارد.

حال یک چندجمله‌ای دلخواهِ f در E_n را در نظر بگیرید. فرض کنید $\{a_0, a_1, \cdots, a_{n-1}\}$ مجموعه‌ی ضرایب آن باشد. از پایه‌ی مذکور τ که از ایده‌آل‌های ارزیاب هنسلی تشکیل شده است، برای هر $0 \leq i \leq n-1$ یک ایده‌آل ارزیاب M_i با ویژگیِ $a_i \in M_i$ انتخاب می‌کنیم. از آنجا که M_i یک ایده‌آل است، پس $a_i^{-1} \notin M_i$. اشتراک همه‌ی M_i ها به ازای هر $0 \leq i \leq n-1$ را M' می‌نامیم.

فرض کنید a یک ریشه‌ی ساده از f باشد. یک ایده‌آل ارزیاب هنسلی M^* را به گونه‌ای انتخاب می‌کنیم که $f'(a) \notin M^*$. برای این منظور کافی است M^* را به گونه‌ای پیدا کنیم که $\frac{1}{f'(a)} \in M^*$ و با توجه به پایه بودن مجموعه‌ی ایده‌آل‌های ارزیاب هنسلی مذکور، این کار شدنی است. حال ایده‌آل هنسلی $M = M^* \cap M'$ را در نظر می‌گیریم. با توجه به این‌که به ازای هر $0 \leq i \leq n-1$ داریم $a_i^{-1} \notin M$، پس $a_i \in A_M$ و در نتیجه $f \in A_M[x]$. ادعا می‌کنیم که $U_f = f + M[x]^{n-1}$ زیرمجموعه‌ی E_n است. برای اثبات این ادعا، یک چندجمله‌ای g از گوی $U_f = f + M[x]^{n-1}$ در نظر بگیرید. به سادگی می‌توان دید که

$$g(a) \equiv f(a) \equiv 0 \pmod{M} \qquad \text{و} \qquad g'(a) \equiv f'(a) \not\equiv 0 \pmod{M}.$$

حال از آنجا که A_M یک حلقه‌ی ارزیاب هنسلی است، پس یک عنصرِ b در $a + M$ وجود دارد به طوری که ریشه‌ی ساده‌ی g است. بنابراین نتیجه می‌شود که هر $g \in U_f$ یک ریشه‌ی ساده در K دارد. به بیان دیگر $U_f \subseteq E_n$.

اثبات از ۲ به ۱: می‌خواهیم نشان دهیم که در صورت برقراری شرط ۲، برای هر $n \geq 1$، یک گوی $U \in \tau$ وجود دارد به طوری که هر چندجمله‌ای $f = x^{n+1} + x^n + a_{n-1}x^{n-1} + \cdots + a_0$ که در آن ضرایب همگی از U هستند، حداقل یک ریشه در K دارد. برای این منظور، چندجمله‌ای $f = x^{n+1} + x^n$ را در نظر بگیرید. با توجه به اینکه $f = x^n(x+1)$، پس f در K یک ریشه‌ی ساده دارد که همان -1 است و بنابراین $f \in E_{n+1}$. مجموعه‌ی E_{n+1} یک مجموعه‌ی باز است، پس یک گوی U در τ وجود دارد به طوری که هر چندجمله‌ای g در $f + U[x]_1^{n-1}$ حداقل یک ریشه‌ی ساده در K دارد. □

۶.۵ یک همسایگی تعریف‌پذیر در یک میدانِ t ـ هنسلی

سرانجام به اثبات قضیه‌ی مورد نظر این فصل می‌رسیم. فرض کنید (K, τ) یک میدان t ـ هنسلی باشد که بسته‌ی جدایی‌پذیر نیست. یک چندجمله‌ای تحویل‌ناپذیر و جدایی‌پذیرِ $f \in K[x]$ را در نظر بگیرید که در K ریشه‌ای ندارد. همچنین فرض کنید یک عنصر a در K در شرط $f'(a) \neq 0$ صدق کند. در این بخش، نشان می‌دهیم که مجموعه‌ی $U_{f,a} := \{\frac{1}{f(x)} - \frac{1}{f(a)} : x \in K\}$ یک همسایگی باز و کراندار حول 0 است.

تعریف ۳۷.۵. فرض کنید $f \in K[x]$ یک چندجمله‌ای و a یک عنصر از میدانِ K باشد. عنصر $f(a) \in K$ را یک مقدار ساده‌ی f می‌نامیم هرگاه $f'(a) \neq 0$.

قضیه ۳۸.۵. فرض کنید (K, τ) یک میدانِ t ـ هنسلی و $f \in K[x]$ یک چندجمله‌ای تکین باشد. مجموعه‌ی متشکل از مقادیر ساده‌ی f، یعنی $S = \{f(a) : a \in K, f'(a) \neq 0\}$ یک مجموعه‌ی باز است.

اثبات. می‌خواهیم اثبات کنیم که هر مقدار ساده‌ی b از چندجمله‌ای f، یک نقطه‌ی درونی از مجموعه‌ی S است. به بیان دیگر، یک همسایگی U_b از b وجود دارد به طوری که $U_b \subseteq S$.

بدون کاسته شدن از کلیت، فرض کنید $\deg(f) = n$. همچنین، فرض کنید b یک مقدار ساده از چندجمله‌ای f باشد؛ به عبارت دیگر، به ازای یک $a \in K$ داریم $f(a) = b$ و $f'(a) \neq 0$. در این صورت، چندجمله‌ای $f(x) - b$ یک ریشه‌ی ساده دارد که همان عنصر a است. با توجه به قضیه‌ی ۳۶.۵، مجموعه‌ی چندجمله‌ای‌هایی از $K[x]_1^n$ که در K ریشه‌ی ساده دارند، در توپولوژی که روی $K[x]_1^n$ تعریف کردیم یک مجموعه‌ی باز است. بنابراین، از آنجا که $f(x) - b$ در این مجموعه قرار دارد، پس یک نقطه‌ی درونی از آن است. به عبارت دیگر، یک گوی $U \in \tau$ وجود دارد به طوری که هر چندجمله‌ایِ g متعلق به $f(x) - b + U[x]^{n-1}$ یک ریشه‌ی ساده در K دارد. به ویژه، هر چندجمله‌ای به صورتِ $f(x) - b + a_i$ که $a_i \in U$ یک ریشه‌ی ساده در K دارد؛ یعنی $t \in K$ وجود دارد به طوری که $f(t) - b + a_i = 0$. به عبارت دیگر، $f(t) = b - a_i$ و بنابراین $b - a_i$ یک مقدار ساده‌ی f است. از این رو همه‌ی عناصر موجود در $b - U$ مقادیر ساده‌ی f هستند و در نتیجه $b - U$ همان همسایگی مطلوب حولِ b است. □

لم ۳۹.۵. فرض کنید K یک میدان و $A \subseteq K$ یک حلقه‌ی ارزیاب و M ایده‌آل ماکسیمال A باشد، همچنین f یک چندجمله‌ای در $A[x]$ باشد. اگر $b \in K$ به گونه‌ای باشد که $f(b) \in M$ آنگاه $b \in A$.

اثبات. از آنجا که A یک حلقه‌ی ارزیاب است، پس طبق قضیه‌ی ۹.۳ یک نگاشت ارزیابی v از میدانِ K به یک گروه مرتب آبلی Γ وجود دارد به طوری که $O_v = A$. حال چندجمله‌ای دلخواه و تکینِ $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ را در $A[x]$ در نظر بگیرید. فرض کنید $b \in K$ به گونه‌ای باشد $f(b) \in M$، یعنی $v(f(b)) > 0$. با برهان خلف فرض کنید $b \notin A$، یعنی $v(b) < 0$. از طرفی،

$$v(f(b)) = v(b^n + a_{n-1}b^{n-1} + \cdots + a_0) = \min\{nv(b), (n-1)v(b) + v(a_{n-1}) \cdots, v(a_0)\}.$$

با توجه به اینکه برای هر $0 \leq i \leq n-1$، داریم $v(a_i) \geq 0$، پس

$$\min\{nv(b), (n-1)v(b) + v(a_{n-1}) \cdots, v(a_0)\} = nv(b) < 0$$

و بنابراین $v(f(b)) < 0$ که تناقض است. پس باید $v(b) \geq 0$، یعنی $b \in A$. □

لم ۴۰.۵. فرض کنید $f \in K[x]$ یک چندجمله‌ای جدایی‌پذیر باشد. در این صورت f و f' در $K[x]$ نسبت به هم اول هستند.

اثبات. یادآوری می‌کنیم که یک چندجمله‌ای f از درجه‌ی n در $K[x]$ یک چندجمله‌ای جدایی‌پذیر است، هرگاه در $K^{alg}[x]$ به صورتِ $(x-a_1)(x-a_2)\cdots(x-a_n)$ تجزیه شود که در آن $a_i \neq a_j$.

با برهان خلف، فرض کنید دو چندجمله‌ای f و f' در $K[x]$ نسبت به هم اول نباشند، یعنی $\gcd(f, f') \neq 1$. در این صورت $h \in K[x]$ وجود دارد به طوری که $h \mid f$ و $h \mid f'$. حال فرض کنید $a \in K^{alg}$ یک ریشه‌ی h باشد، بنابراین $x - a \mid h$ و در نتیجه $x-a|f'$ و $x-a|f$. از این رو، $f = (x-a)g$ که در آن $g \in K^{alg}[x]$ و در نتیجه داریم

$f' = g + g'(x-a)$. از آنجا که $x-a \mid f'$ نتیجه می‌گیریم که $x-a \mid g$. بنابراین با توجه به اینکه $f=(x-a)g$ داریم $(x-a)^2 \mid f$ و این با جدایی‌پذیر بودن f در تناقض است. □

در نتیجه اگر f یک چندجمله‌ای جدایی‌پذیر باشد، آنگاه چندجمله‌ای‌های $u(x)$ و $v(x)$ چنان موجودند که $f(x)u(x) + f'(x)v(x) = 1$.

قضیه ۴۱.۵. فرض کنید (K,τ) یک میدانِ t ـ هنسلی و $f \in K[x]$ یک چندجمله‌ای تکین و جدایی‌پذیر از درجه‌ی n باشد که در K ریشه‌ای ندارد. در این صورت $f(K) = \{f(x) : x \in K\}$ یک مجموعه‌ی کراندار دور از صفر است.

اثبات. ابتدا توجه کنید که عبارتِ «اگر $f \in K[x]$ یک چندجمله‌ای تکین و جدایی‌پذیر باشد که در K ریشه‌ای نداشته باشد آنگاه $f(K)$ یک مجموعه‌ی کراندار دور از صفر است» را می‌توان به صورت زیر نوشت که یک جمله‌ی موضعی است:

$$\varphi_n = \forall a_0, a_1, \cdots, a_{n-1} \exists x (x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \to$$
$$nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 \neq 0) \wedge \forall x (x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \neq 0)$$
$$\to \exists U \forall x f(x) \notin U$$

بنابراین با توجه به قضیه‌ی ۱۹.۵، می‌توانیم (K,τ) را یک میدانِ ω ـ کامل در نظر بگیریم. فرض کنید $\{a_0, a_1, \cdots, a_{n-1}\}$ مجموعه‌ی ضرایب چندجمله‌ای f باشد. با توجه به نتیجه‌ی ۳۳.۵، برای τ یک پایه وجود دارد که متشکل از ایده‌آل‌های ارزیاب هنسلی است. از این پایه برای هر $0 \le i \le n-1$، یک ایده‌آل ارزیابِ M_i با این ویژگی که a_i در M_i باشد، انتخاب می‌کنیم . توجه کنید که چون M_i یک ایده‌آل است، پس $a_i^{-1} \notin M_i$. اشتراک همه‌ی M_i ها به ازای هر $0 \le i \le n-1$ را M' می‌نامیم. حال توجه کنید که f یک چندجمله‌ای جدایی‌پذیر است، پس بنا به لم ۴۰.۵، f نسبت به f' اول است. در نتیجه دو چندجمله‌ای u و v در $K[x]$ وجود دارند به طوری که $fu + f'v = 1$. مشابه با روشی که M' را یافتیم، ایده‌آل‌های ارزیاب M'' و M^* را انتخاب می‌کنیم به طوری که M'' شامل وارون ضرایب u و M^* شامل وارون ضرایب v نباشد. سپس، ایده‌آل ارزیاب هنسلیِ $M = M^* \cap M' \cap M''$ را در نظر می‌گیریم. با توجه به این‌که وارون ضرایب f و u و v در M نیستند، پس $f, u, v \in A_M[x]$.

حال ادعا می‌کنیم که $f(K) \cap M = \emptyset$. برای اثبات این ادعا، با برهان خلف فرض کنید به ازای یک $a \in K$ داشته باشیم $f(a) \in M$. در این صورت بنا به لم ۳۹.۵، داریم $a \in A_M$. اگر $f'(a) \in M$، آنگاه با توجه به اینکه M یک ایده‌آل ارزیاب است و $f(a), u(a), v(a) \in A_M$، داریم $f(a)u(a) + f'(a)v(a) \in M$ و بنابراین $1 \in M$. اما توجه کنید که M یک ایده‌آل ارزیاب است و $1 \notin M$ پس نتیجه‌ی مذکور یک تناقض است، بنابراین $f'(a) \notin M$. حال با توجه به اینکه M یک ایده‌آل ارزیاب هنسلی است و $f(a) \in M$ و $f'(a) \notin M$ می‌توان نتیجه گرفت که f در

A_M یک ریشه دارد، پس بوضوح f در K یک ریشه دارد که با فرض در تناقض است. بنابراین، از آنجا اثبات کردیم $f(K) \cap M = \emptyset$، پس $f(K)$ یک مجموعه‌ی کراندار دور از صفر توسط گوی باز M است. □

نتیجه ۴۲.۵. فرض کنید (K,τ) یک میدانِ t ـ هنسلی و $f \in K[x]$ یک چندجمله‌ای تکین و جدایی‌پذیر باشد که در K ریشه‌ای ندارد. در این صورت $\{f(x)^{-1} : x \in k\}$ یک مجموعه‌ی کراندار است.

اثبات. با توجه به قضیه‌ی قبل، یک ایده‌آل ارزیاب هنسلی M در τ وجود دارد به طوری که $f(K)\cap M = \emptyset$. متناظر با این ایده‌آل ارزیابِ M یک حلقه‌ی ارزیاب هنسلی A_M وجود دارد که ایده‌آل ماکسیمال آن همان M است. همچنین، یک نگاشت ارزیابی v از میدانِ K به یک گروه مرتب آبلی Γ وجود دارد به طوری که $O_v = A_M$. این نگاشت ارزیابی یک توپولوژی روی K القاء می‌کند که آن با τ_v نشان می‌دهیم. در قضیه‌ی ۲۷.۵ اثبات کردیم که $\tau_v = \tau$.

توجه کنید که $v(M) = \{v(x) : x \in M\}$ یک مجموعه‌ی از پایین کراندار است، پس بنا به لمِ ۳۰.۴ مجموعه‌ی M کراندار است. از طرفی از آنجا که $f(K) \cap M = \emptyset$ و $M = \{x \in K : v(x) > 0\}$، پس به ازای هر $x \in K$ داریم $v(f(x)) \leq 0$، بنابراین $v(f(x)^{-1}) = -v(f(x)) > 0$ و در نتیجه $\{f(x)^{-1} : x \in k\} \subseteq M$. از این رو، $\{f(x)^{-1} : x \in k\}$ نیز یک مجموعه‌ی کراندار است. □

نماد گذاری ۴۳.۵. مجموعه‌ی $\{f(x)^{-1} : x \in K\}$ را با نماد $f(K)^{-1}$ نشان می‌دهیم.

قضیه ۴۴.۵. فرض کنید (K,τ) یک میدان t ـ هنسلی باشد که بسته‌ی جدایی‌پذیر نیست. یک چندجمله‌ای تحویل‌ناپذیر و جدایی‌پذیرِ f در $K[x]$ را در نظر بگیرید که در K ریشه‌ای ندارد. همچنین فرض کنید $a \in K$ در شرطِ $f'(a) \neq 0$ صدق می‌کند. در این صورت، مجموعه‌ی $U_{f,a} := \{\frac{1}{f(x)} - \frac{1}{f(a)} : x \in K\}$ یک همسایگی باز و کراندار حول 0 است.

اثبات. با توجه به نتیجه‌ی ۴۲.۵، می‌دانیم که مجموعه‌ی $f(K)^{-1}$ یک مجموعه‌ی کراندار است. بنابراین طبق لم ۳۱.۴، $f(K)^{-1} - f(K)^{-1}$ نیز کراندار است. از آنجا که $f(K)^{-1} - f(a)^{-1} \subset f(K)^{-1} - f(K)^{-1}$، پس $f(K)^{-1} - f(a)^{-1}$ نیز کراندار است.

توجه کنید که چون a متعلق به K است، پس $0 = \frac{1}{f(a)} - \frac{1}{f(a)}$ در $U_{f,a}$ قرار دارد. تنها چیزی که از اثبات آن باقی مانده، این است که $U_{f,a}$ یک مجموعه‌ی باز است. از آنجا که مطابق فرض، $f(a)$ یک مقدار ساده‌ی f است، پس بنا به قضیه‌ی ۳۸.۵ حول $f(a)$ یک همسایگی U وجود دارد که تمام نقاط آن به صورت $f(t)$ هستند و $f'(t) \neq 0$. بنابراین حولِ $\frac{1}{f(a)}$ همسایگی $\frac{1}{U}$ وجود دارد که در این همسایگی همه‌ی عناصر به صورت $\frac{1}{f(t)}$ هستند و $f'(t) \neq 0$. در نتیجه، $U^* = \frac{1}{U} - \frac{1}{f(a)}$ یک همسایگی صفر است که همه‌ی عناصر آن به صورت $\frac{1}{f(t)} - \frac{1}{f(a)}$ هستند، پس $U^* \subseteq U_{f,a}$. حال توجه کنید که τ یک فیلتر متشکل از همسایگی‌های حول صفر است و چون $U^* \in \tau$ و نشان دادیم که $U^* \subseteq U_{f,a}$ می‌توان نتیجه گرفت که $U_{f,a}$ نیز در τ قرار دارد و این یعنی یک مجموعه‌ی باز است. □

* خلاصه‌ی فصل:

هدف اصلی این فصل، اثبات قضیه زیر است:

فرض کنید (K,τ) یک میدان t ـ هنسلی باشد که بسته‌ی جدایی‌پذیر نیست. همچنین، یک چندجمله‌ای تحویل‌ناپذیر و جدایی‌پذیر $f\in K[x]$ را در نظر بگیرید که در K ریشه‌ای ندارد. فرض کنید یک عنصرِ a متعلق به K در شرط $f'(a)\neq 0$ صدق کند. در این صورت، مجموعه $U_{f,a}:=\{\frac{1}{f(x)}-\frac{1}{f(a)}: x\in K\}$ یک همسایگی باز و کراندار حول 0 است. برای اثبات این قضیه، موارد زیر را اثبات کرده‌ایم:

۱. برای یک میدانِ t ـ هنسلی یک پایه متشکل از ایده‌آل‌های ارزیاب هنسلی وجود دارد. در اینجا، منظور از "ایده‌آل ارزیاب" زیرمجموعه‌ای مانند M از میدان K با ویژگی‌های زیر است:

$1\notin M$، $M+M\subset M$، $M\cdot M\subset M$ و برای هر $x,y\in K$، اگر $x\cdot y\in M$ آن‌گاه $x\in M$ یا $y\in M$.

۲. نشان دادیم که مجموعه‌ی $f(K)=\{f(x): x\in K\}$ یک مجموعه‌ی کراندار دور از صفر است. در واقع، از پایه‌ی متشکل از ایده‌آل‌های ارزیاب هنسلی یک گوی M می‌توان انتخاب کرد به طوری که $f(K)\cap M=\emptyset$. در نتیجه مجموعه‌ی $f(K)^{-1}=\{f(x)^{-1}: x\in K\}$ یک مجموعه‌ی کراندار است و بنابراین $f(K)^{-1}-f(K)^{-1}$ نیز کراندار است. به این ترتیب با توجه به اینکه $f(K)^{-1}-f(a)^{-1}\subset f(K)^{-1}-f(K)^{-1}$، نتیجه می‌شود که مجموعه‌ی $f(K)^{-1}-f(a)^{-1}$ کراندار است.

۳. مجموعه‌ی متشکل از مقادیر ساده f، یعنی $\{f(a): a\in K, f'(a)\neq 0\}$ یک مجموعه باز در τ است. در نتیجه حول $f(a)$ یک همسایگی U وجود دارد که تمام نقاط آن به صورت $f(t)$ هستند و $f'(t)\neq 0$. بنابراین حولِ $\frac{1}{f(a)}$ همسایگی $\frac{1}{U}$ وجود دارد که در این همسایگی همه‌ی عناصر به صورت $\frac{1}{f(t)}$ هستند و $f'(t)\neq 0$. از این رو $U^*=\frac{1}{U}-\frac{1}{f(a)}$ یک همسایگی صفر است که همه‌ی عناصر آن به صورت $\frac{1}{f(t)}-\frac{1}{f(a)}$ هستند، در نتیجه $U^*\subseteq U_{f,a}$. چون τ یک فیلتر متشکل از همسایگی‌های حول صفر است، پس $U_{f,a}$ نیز در τ قرار دارد و نهایتاً یک مجموعه‌ی باز است.

فصل ۶

یک تعریف وجودی بدون پارامتر برای حلقه‌ی ارزیابِ $\mathbb{F}_q[[t]]$ در میدان ارزیابیِ $\mathbb{F}_q((t))$

در فصل ۳ به ازای یک میدانِ k، میدانِ $k((t))$ و حلقه‌ی $k[[t]]$ را معرفی کردیم. در این فصل، میدانِ k را میدان متناهیِ $\mathbb{F}_q$ در نظر می‌گیریم. یادآوری می‌کنیم که $\mathbb{F}_q((t))$ میدان متشکل از سری‌هایی به صورتِ $\sum\limits_{i=-n}^{\infty} a_i t^i$ است که در آن هر a_i متعلق به $\mathbb{F}_q$ و n یک عدد طبیعی است. نگاشتِ $v : \mathbb{F}_q((t)) \to \mathbb{Z}$ با ضابطه‌ی $v(\sum\limits_{i=-n}^{\infty} a_i t^i) = \min\{i|a^i \neq 0\}$ یک ارزیابی روی این میدان است که حلقه‌ی ارزیاب آن، $\mathbb{F}_q[[t]] = \{\sum\limits_{i=0}^{\infty} a_i t^i | a_i \in \mathbb{F}_q\}$ و میدان پیمانه‌های آن $\frac{\mathbb{F}_q[[t]]}{t\mathbb{F}_q[[t]]} = \mathbb{F}_q$ است. در مقاله‌ی مرجع اصلی این پایان‌نامه [۱]، به اثبات قضیه‌ی زیر پرداخته شده است:

«حلقه‌ی ارزیابِ $\mathbb{F}_q[[t]]$ در میدان ارزیابیِ $\mathbb{F}_q((t))$ با فرمولی بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است.»

روش اثبات این قضیه، به صورت پیش رو است:

در مرحله‌ی اول، نشان می‌دهیم که $K = \mathbb{F}_q((t))$ در شروط قضیه‌ی ۴۴.۵، که در فصل قبل آن را اثبات کردیم، صدق می‌کند و در نتیجه در این میدان، یک همسایگی کراندار از صفر وجود دارد که توسط یک فرمول وجودی و با پارامتر از $\mathbb{F}_q((t))$ تعریف‌پذیر است. پس از آن، پارامترهای این فرمول را از $\mathbb{F}_q((t))$ به $\mathbb{F}_q$ تقلیل می‌دهیم (به کمک نتیجه‌ی ۱۲.۶).

در مرحله‌ی دوم، با به کارگیری یک ترفند جالب با حفظ تعریف‌پذیری، این همسایگی تعریف‌پذیر از صفر را به یک مجموعه‌ی Y تبدیل می‌کنیم که $t\mathbb{F}_q[[t]] \subseteq Y \subseteq \mathbb{F}_q[[t]]$. همچنین نشان خواهیم داد که $\mathbb{F}_q[[t]]$ برابر است با

$\mathbb{F}_q + Y$ و از این رو با توجه به تعریف‌پذیریِ Y و $\mathbb{F}_q$ نتیجه می‌شود که $\mathbb{F}_q[[t]]$ نیز تعریف‌پذیر است.

در مرحله‌ی آخر، پارامترهای تعریف به دست آمده در مرحله‌ی دوم را حذف می‌کنیم.

۱.۶ قضیه‌ی اصلی پایان‌نامه

نماد گذاری ۱.۶. به جای نوشتن «تعریف‌پذیر با فرمول وجودی و با پارامتر از مجموعه‌ی C»، از کوتاه‌نوشت «$\exists$ ـ C ـتعریف‌پذیر» استفاده می‌کنیم. به طور خاص به جای نوشتن «تعریف‌پذیر با فرمول وجودی و بدون پارامتر»، می‌نویسیم «$\exists$ ـ $\emptyset$ ـتعریف‌پذیر».

قضیه‌ی اصلی مورد نظر ما در این فصل به صورت زیر است:

قضیه ۲.۶. حلقه‌ی ارزیابِ $\mathbb{F}_q[[t]]$ در میدان ارزیابی $\mathbb{F}_q((t))$ در زبان حلقه‌ها $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر است.

توجه ۳.۶. بوضوح اگر (K, O_v) یک میدان ارزیابی باشد، آنگاه حلقه‌ی ارزیابِ O_v در زبانِ $\mathcal{L} := \{+, -, \cdot, 0, 1\} \cup \{v(y) \leq v(x)\}$، که در آن یک محمول دوتاییِ $v(x) \leq v(y)$ قرار داده شده است، توسط فرمولِ $\varphi(x) := v(1) \leq v(x)$ تعریف‌پذیر است؛ اما ما به دنبال تعریف‌پذیریِ O_v در زبان حلقه‌ها، یعنی $\mathcal{L}_{ring} := \{+, -, \cdot, 0, 1\}$ هستیم.

۲.۶ گوی‌های باز و بسته در توپولوژی τ_v

فرض کنید $v : K \to \Gamma$ یک نگاشت ارزیابی باشد. در بخش ۱.۱.۴، نشان دادیم که این نگاشت یک توپولوژی روی میدانِ K القاء می‌کند که آن را با نماد τ_v نمایش می‌دهیم. در این بخش، تعریف گوی‌های باز و بسته در این توپولوژی را یادآوری و برخی ویژگی‌های آن‌ها را که برای اثبات‌های بعدی مورد نیاز است، بیان و اثبات می‌کنیم.

یادآوری ۴.۶. برای هر $n \in vK$، داریم:

۱. $S(n) := \{x : v(x) = n\}$.

۲. $B(n) := \{x : v(x) > n\}$، گوی باز حول 0 و به شعاع n است.

۳. $\bar{B}(n) := \{x : v(x) \geq n\}$، گوی بسته حول 0 و به شعاع n است.

نماد گذاری ۵.۶. اجتماع دو مجموعه‌ی مجزا را با نماد $\sqcup$ نمایش می‌دهیم.

لم ۶.۶. برای $n \in vK$ داریم:

۱. $B(n) \subseteq S(n) - S(n)$.

۲. $\bar{B}(n) = S(n) \sqcup B(n)$.

۳. $\bar{B}(n) - \bar{B}(n) = \bar{B}(n)$.

اثبات.

۱. عناصر دلخواهِ $x \in B(n)$ و $y \in S(n)$ را در نظر بگیرید. در این صورت $v(y) = n < v(x)$، بنابراین $v(x+y) = \min\{v(x), v(y)\} = v(y) = n$. از این تساوی نتیجه می‌شود که $x + y \in S(n)$، پس $x = (x+y) - y \in S(n) - S(n)$.

۲. عنصر دلخواه $x \in \bar{B}(n)$ را در نظر بگیرید. بنا به تعریف گوی بسته در ۴.۶، داریم $v(x) \geq n$. بنابراین ممکن است $v(x) = n$ یا $v(x) > n$.

۳. عناصر دلخواهِ $x, y \in \bar{B}(n)$ را در نظر بگیرید. در این صورت $v(x) \geq n$ و $v(y) \geq n$، بنابراین $v(x-y) \geq \min\{v(x), v(y)\} \geq n$ در نتیجه $x - y \in \bar{B}(n)$.

□

۳.۶ یک همسایگی تعریف‌پذیر از صفر

نماد گذاری ۷.۶. مشتق مرتبه‌ی اول چندجمله‌ای $f(x)$ را با نمادِ $D(f)$ نشان می‌دهیم.

مهم‌ترین قضیه‌ای که در فصل گذشته اثبات کردیم، قضیه‌ی ۴۴.۵ است که در اینجا به عنوان یک یادآوری آن را مجدداً بیان می‌کنیم. در ادامه خواهیم دید که قضیه‌ی ۲.۶ بر پایه‌ی قضیه‌ی ۴۴.۵ اثبات می‌شود.

یادآوری ۸.۶. فرض کنید (K, τ) یک میدان t ـ هنسلی است که بسته‌ی جدایی‌پذیر نیست و $f \in K[x]$ یک چندجمله‌ای تحویل‌ناپذیر و جدایی‌پذیر است که در K ریشه‌ای ندارد و همچنین فرض کنید یک عنصرِ a در K شرط $D(f)(a) \neq 0$ را برآورده می‌کند. در این صورت، مجموعه‌ی $U_{f,a} := \{\frac{1}{f(x)} - \frac{1}{f(a)} : x \in K\}$ یک همسایگی باز و کراندار حول 0 است.

به سادگی می‌توان دید که $U_{f,a}$ با فرمولِ $\exists\, y, z, t, s\ (x = s - t \wedge sf(y) = 1 \wedge tf(a) = 1)$ تعریف‌پذیر است. توجه کنید که پارامترهای این فرمول، عنصرِ a و ضرایب چندجمله‌ای f هستند و در نتیجه به میدانِ K تعلق دارند.

در این بخش، یک نتیجه از قضیه‌ی مذکور را بیان می‌کنیم که به کمک آن می‌توانیم این پارامترها را به یک زیرمیدان از K تقلیل دهیم.

توجه ۹.۶. فرض کنید K یک میدان و f یک چندجمله‌ای در $K[x]$ باشد. اگر مشخصه‌ی K صفر باشد، آنگاه $\deg(D(f)) = n - 1$؛ اما اگر مشخصه‌ی K ناصفر باشد، آنگاه $\deg(D(f)) \leq n - 1$.

یادآوری ۱۰.۶. این که یک میدان K بسته‌ی جدایی‌پذیر نیست، یعنی K یک توسیع جدایی‌پذیر دارد. به بیان دیگر، یک چندجمله‌ای جدایی‌پذیر در $K[x]$ موجود است که در K ریشه‌ای ندارد.

همچنین، وقتی می‌گوییم زیرمیدان C از میدان K به طور نسبی بسته‌ی جبری است، یعنی اگر $f \in C[x]$ در K ریشه داشته باشد آنگاه این ریشه متعلق به خودِ C است؛ به بیان دیگر، $C^{alg} \cap K = C$.

لم ۱۱.۶. فرض کنید K یک میدان و C یک زیرمیدان به طور نسبی بسته‌ی جبری از K باشد که بسته‌ی جدایی‌پذیر نیست. در این صورت یک چندجمله‌ای جدایی‌پذیر و غیر خطیِ f در $C[x]$ وجود دارد به طوری که در K ریشه‌ای ندارد.

اثبات. از آنجا که میدانِ C بسته‌ی جدایی‌پذیر نیست، پس یک چندجمله‌ای جدایی‌پذیر f در $C[x]$ وجود دارد که در C ریشه‌ای ندارد. ادعا می‌کنیم که f در K نیز ریشه‌ای ندارد. با برهان خلف، فرض کنید f یک ریشه در K داشته باشد. با توجه به اینکه C یک زیرمیدان به طور نسبی بسته‌ی جبری از K است، پس این ریشه متعلق به C است و این تناقض است.

توجه کنید که این چندجمله‌ای حتماً غیرخطی است، زیرا با توجه به میدان بودنِ C، ریشه‌ی هر چندجمله‌ای به صورت $ax + b \in C[x]$ در C قرار دارد. □

نتیجه ۱۲.۶ (از یادآوریِ ۸.۶). فرض کنید (K, τ) یک میدان t ـ هنسلی و $C \subseteq K$ یک زیرمیدان به طور نسبی بسته‌ی جبری از K باشد که بسته‌ی جدایی‌پذیر نیست. در این صورت $V \subseteq K$ وجود دارد به طوری که یک همسایگی کراندار از صفر در توپولوژی τ و $\exists$ ـ C ـ تعریف‌پذیر است.

اثبات. قرار است همسایگی مطلوبِ V به صورت یک $U_{f,a}$ به ازای یک چندجمله‌ای مناسبِ f و یک عنصر مناسبِ a باشد. بنابراین، در ادامه به دنبال یک چندجمله‌ای جدایی‌پذیر و تحویل‌ناپذیرِ $f \in C[x]$ هستیم که در K ریشه‌ای نداشته باشد. همچنین، باید یک عنصرِ a در C پیدا کنیم به طوری که $D(f(a)) \neq 0$. بسته به اندازه‌ی C دو حالت رخ می‌دهد:

حالت اول. اگر C یک میدان نامتناهی باشد، آنگاه یک چندجمله‌ای جدایی‌پذیر، تحویل‌ناپذیر و غیر خطی $f \in C[x]$ انتخاب می‌کنیم که در K ریشه‌ای نداشته باشد. توجه کنید که بنا به لم ۱۱.۶، چنین چندجمله‌ای وجود دارد. فرض کنید $\deg(f) = n$. در این صورت $\deg(D(f)) \leq n - 1$ و بنابراین تعداد ریشه‌های $D(f)$ حداکثر

$n-1$ تاست. با توجه به اینکه C یک میدان نامتناهی است، پس حداقل یک عنصرِ a در C وجود دارد به طوری که ریشه‌ی $D(f)$ نباشد.

حالت دوم. اگر C یک میدان متناهی باشد، آنگاه به صورت $\mathbb{F}_q$ است، که در آن q یک توان از عدد اول p است. در این حالت یک چندجمله‌ای f با توجه به نکات زیر انتخاب می‌کنیم:

با توجه به این‌که $\mathbb{F}_{q^2}$ یک توسیع متناهی از $\mathbb{F}_q$ است ($[\mathbb{F}_{q^2} : \mathbb{F}_q] = 2$) و هر توسیع متناهی یک توسیع جبری است، می‌توان $\mathbb{F}_{q^2}$ را به صورت $\mathbb{F}_q(\alpha)$ نوشت که در آن α روی $\mathbb{F}_q$ جبری است و چندجمله‌ای مینیمال آن درجه‌ی 2 دارد.

حال چندجمله‌ای f را همان چندجمله‌ای مینیمال عنصرِ α در نظر می‌گیریم و نشان می‌دهیم که f یک چندجمله‌ای تحویل‌ناپذیر و جدایی‌پذیر است که در K ریشه‌ای ندارد. از آنجا که f یک چندجمله‌ای مینیمال است، در نتیجه تحویل‌ناپذیر نیز هست. همچنین، با توجه به اینکه f چندجمله‌ای مینیمال عنصرِ α است و درجه‌ی 2 دارد، نمی‌تواند به صورتِ $(x-\alpha)^2$ باشد و این یعنی f جدایی‌پذیر است. تنها چیزی که اثبات آن باقی مانده، این است که نشان دهیم f در K ریشه‌ای ندارد.

اولاً f در $\mathbb{F}_q$ ریشه‌ای ندارد، زیرا f یک چندجمله‌ای جدایی‌پذیر از درجه‌ی 2 است، پس $f = (x-\alpha)(x-\beta)$. می‌دانیم که $\alpha \notin \mathbb{F}_q$ حال با برهان خلف فرض کنید β در $\mathbb{F}_q$ باشد. از آنجا که $0 \in \mathbb{F}_q$ و $f \in \mathbb{F}_q[x]$، پس $f(0) = \alpha\beta \in \mathbb{F}_q$. همچنین، با توجه به این که $\mathbb{F}_q$ یک میدان است و فرض کردیم β در آن قرار دارد، بنابراین $\beta^{-1} \in \mathbb{F}_q$ و در نتیجه $\alpha\beta\beta^{-1} = \alpha$ در $\mathbb{F}_q$ قرار دارد که این تناقض است.

ثانیاً مطابق با فرض $\mathbb{F}_q$ یک زیرمیدان به طور نسبی بسته جبری از میدان K است، بنابراین از آنجایی که چندجمله‌ای f در $\mathbb{F}_q$ ریشه‌ای ندارد، نتیجه می‌شود که f در K نیز ریشه‌ای ندارد.

حال توجه کنید که $\deg(f) = 2$، پس $\deg(D(f)) \leq 1$ و این یعنی $D(f)$ حداکثر یک ریشه دارد. می‌دانیم که میدان $\mathbb{F}_q$ حداقل دو عنصر دارد، بنابراین حتماً یک عنصر a در C موجود است به طوری که ریشه‌ی $D(f)$ نباشد.

اکنون قصد داریم در این حالت، یک مورد خاص را جداگانه بررسی کنیم که ممکن است در اثبات فوق مبهم باشد. فرض کنید $\mathbb{F}_q = \mathbb{F}_2$. می‌خواهیم بررسی کنیم که اگر چندجمله‌ای $f \in \mathbb{F}_2[x]$ را مطابق با آنچه توضیح دادیم، از درجه‌ی 2 انتخاب کنیم آیا ممکن است $D(f)$ برابر با 0 شود (اگر چنین شود نمی‌توان یک عنصر $a \in K$ یافت به طوری که $D(f)(a) \neq 0$). توجه کنید که در این حالت خاص، چندجمله‌ای مینیمال α که $\mathbb{F}_2(\alpha) = \mathbb{F}_4$ به صورتِ $f = x^2+x+1$ است، زیرا تمامی چندجمله‌ای‌های دیگر در $\mathbb{F}_2[x]$ که از درجه‌ی دو هستند، چندجمله‌ای‌های x^2 و x^2+1 و x^2+x هستند و این چندجمله‌ای‌ها در $\mathbb{F}_2$ ریشه دارند و به ویژه همه‌ی ریشه‌های آن‌ها در $\mathbb{F}_2$ است؛ پس هیچ یک نمی‌توانند چندجمله‌ای مینیمال α باشند. از طرفی، $D(x^2+x+1) = 1 \neq 0$ و بنابراین در این حالت نیز می‌توانیم یک عنصر a در $\mathbb{F}_2$ بیابیم به طوری که $D(f)(a) \neq 0$ (در واقع، کافی است a را همان عنصر 1 در نظر بگیریم).

نهایتاً برای یک چندجمله‌ای مناسبِ $f \in C[x]$ و یک عنصر مناسبِ $a \in C$ که در بالا وجودشان را تضمین

کردیم، مجموعه‌ی $V := U_{f,a} = \{\frac{1}{f(x)} - \frac{1}{f(a)} : x \in K\}$ را تشکیل می‌دهیم. باتوجه به قضیه‌ی ۸.۶، این مجموعه یک همسایگی باز و کراندار از صفر است و $\exists$ ـ C ـ تعریف‌پذیر بودن آن نیز به سادگی نتیجه می‌شود. $\square$

۴.۶ یک مجموعه‌ی تعریف‌پذیر بین O_v و m_v

میدانِ $K := F((t))$، یعنی میدان متشکل از سری‌های لوران روی میدانِ F را در نظر بگیرید. نگاشتِ $v : K \to \mathbb{Z}$ که هر سریِ $\sum\limits_{i=-n}^{\infty} a_i t^i$ را به $\min\{i : a_i \neq 0\}$ می‌برد، یک نگاشت ارزیابی روی این میدان است که حلقه‌ی ارزیاب آن برابر با $O_v = F[[t]]$ و ایده‌آل ماکسیمال آن $m_v = tF[[t]]$ است. در این بخش، می‌خواهیم نشان دهیم که چگونه از یک همسایگی کراندار و تعریف‌پذیر از صفر $V \subseteq K$ می‌توان به یک مجموعه‌ی تعریف‌پذیرِ $Y \subseteq K$ رسید که شاملِ m_v و مشمول در O_v است. خلاصه‌ی روش رسیدن از همسایگی صفرِ V به مجموعه‌ی Y به شرح زیر است:

۱. از آنجا که V یک همسایگی از 0 است، پس یک عدد صحیحِ n وجود دارد به طوری که $B(n) \subseteq V$. حال یک عنصر m بزرگتر از n در نظر می‌گیریم. مجموعه‌ی $W := \{x \in K : x^m \in V\}$ یک مجموعه‌ی کراندار، تعریف‌پذیر و شاملِ $S(1)$ است.

۲. مجموعه‌ی $X := W - (W \cup \{0\})$ یک مجموعه‌ی کراندار، تعریف‌پذیر و شاملِ m_v است.

۳. از آنجا که X یک مجموعه‌ی کراندار است، پس یک عدد صحیح h وجود دارد به طوری که $X \subseteq B(-h)$. مجموعه‌ی $Y := \{x : x^h \in X\} - \{x : x^h \in X\}$ یک مجموعه‌ی کراندار و تعریف‌پذیر است که $m_v \subseteq Y \subseteq O_v$.

نماد گذاری ۱۳.۶. فرض کنید K یک میدان و φ یک فرمول در زبان حلقه‌ها باشد. در این صورت، مجموعه‌ی $\{x \in K : \varphi(x)\}$ را با نمادِ $\varphi(K)$ نشان می‌دهیم.

در قضیه‌ی زیر و اثبات آن، جزئیات آنچه در بالا اشاره کردیم را شرح می‌دهیم. در ادامه، C را یک زیرمجموعه از میدان K در نظر بگیرید.

قضیه ۱۴.۶. فرض کنید $V \subseteq K$ یک همسایگی $\exists$ ـC ـ تعریف‌پذیر و کراندار از صفر باشد.

۱. مجموعه‌ی $W \subseteq K$ وجود دارد به طوری که کراندار و $\exists$ ـC ـ تعریف‌پذیر است و $S(1) \subseteq W$.

۲. مجموعه‌ی $X \subseteq K$ وجود دارد به طوری که کراندار و $\exists$ ـC ـ تعریف‌پذیر است و $m_v \subseteq X$.

۳. مجموعه‌ی $Y \subseteq K$ وجود دارد به طوری که کراندار و $\exists$ ـC ـ تعریف‌پذیر است و $m_v \subseteq Y \subseteq O_v$.

اثبات ۱. با توجه به فرض مجموعه‌ی V یک همسایگی از صفر است، بنابراین یک عدد صحیحِ n وجود دارد به طوری که $B(n) \subseteq V$. بدون کاسته شدن از کلیت، می‌توانیم فرض کنیم n نامنفی است. حال یک عنصر m بزرگتر از n در نظر می‌گیریم. در این صورت بوضوح $S(m) \subseteq B(n)$.

از آنجا که V یک همسایگی تعریف‌پذیر از صفر است، پس یک فرمولِ $\phi(x)$ وجود دارد به طوری که $V = \{x \in K : \phi(x)\}$. در ادامه نشان می‌دهیم که مجموعه‌ی $W = \{x \in K : \phi(x^m)\}$ یا به بیان دیگر، $\{x \in K : x^m \in V\}$ همان مجموعه‌ی مطلوب ماست؛ یعنی $S(1) \subseteq W$ و $\exists$ ـ Cـ تعریف‌پذیر و کراندار است.

۱. یک عنصر دلخواهِ x در $S(1)$ در نظر بگیرید. با توجه به اینکه $v(x^m) = mv(x) = m$، داریم $x^m \in S(m)$. از طرفی $S(m) \subseteq B(n) \subseteq V$ و بنابراین $x^m \in V$. از آنجا که مجموعه‌ی W را شامل عناصری در نظر گرفتیم که توان m ـ اُم آن‌ها در V است، پس $x \in W$.

۲. از آنجا که V یک مجموعه‌ی $\exists$ ـ C ـ تعریف‌پذیر است، پس فرمولِ $\phi(x)$ یک فرمول وجودی و با پارامتر از C است. در نتیجه مجموعه‌ی $W = \{x \in K : \phi(x^m)\}$ نیز بوضوح $\exists$ ـ C ـ تعریف‌پذیر است.

۳. با توجه به اینکه V یک مجموعه‌ی کراندار است، یک عدد صحیح l وجود دارد به طوری که $V \subseteq B(l)$. عنصر l' را $\min\{l, -1\}$ در نظر می‌گیریم. ادعا می‌کنیم که $W \subseteq B(l')$.

برای اثبات این ادعا، نشان می‌دهیم که اگر $t \notin B(l')$ آنگاه $t \notin W$، به عبارت دیگر $t^m \notin V$. فرض کنید $t \notin B(l')$، بنابراین داریم $v(t) \leq l' \leq -1 < 0$. در نتیجه $v(t^m) = mv(t) \leq v(t) \leq l' \leq l$ که این یعنی $t^m \notin B(l)$، پس $t^m \notin V$.

اثبات ۲. مجموعه‌ی $W' := W \cup \{0\}$ را در نظر بگیرید. در ادامه نشان می‌دهیم که $X := W - W'$ همان مجموعه‌ی مطلوب ماست؛ یعنی کراندار، $\exists$ ـ Cـ تعریف‌پذیر و شامل m_v است.

۱. مجموعه‌ی W' کراندار است؛ زیرا برابر با اجتماع مجموعه‌ی کراندارِ W و مجموعه‌ی متناهیِ $\{0\}$ است. در نتیجه بنا به قسمت ۴ لمِ ۳۱.۴، می‌توان نتیجه گرفت که مجموعه‌ی $X = W - W'$ نیز یک مجموعه‌ی کراندار است.

۲. دیدیم که مجموعه‌ی W با فرمول وجودی $\phi(x^m)$ تعریف‌پذیر است که پارامترهای آن از مجموعه‌ی C است. مجموعه‌ی $W' = W \cup \{0\}$ را به سادگی می‌توان با فرمولِ $\psi(x) := \phi(x^m) \vee (x = 0)$ تعریف کرد. بوضوح پارامترهای این فرمول همان پارامترهای فرمولِ $\phi(x^m)$ هستند و بنابراین $\psi(x)$ نیز یک فرمول وجودی و با پارامتر از C است. در نهایت، به ازای هر $t, s \in K$ داریم:

$$t - s \in X \iff \phi(t^m) - \psi(s).$$

در نتیجه مجموعه‌ی X نیز $\exists$ ـ C ـ تعریف‌پذیر است.

۳. ابتدا توجه کنید که چون $v(K)=\mathbb{Z}$، پس $m_v=\{x\in K : v(x)>0\}=\bar{B}(1)=S(1)\sqcup B(1)$. با توجه به قسمت ۱ همین لم، $S(1)\subseteq W$ و بنا به ویژگی ۱ در تعریف ۴.۶، $B(1)\subseteq S(1)-S(1)$. بنابراین $B(1)\subseteq S(1)-S(1)\subseteq W-W\subseteq W-(W\cup\{0\})=X$. همچنین، با توجه به اینکه $S(1)\subseteq W$ به سادگی نتیجه می‌شود که $S(1)$ یک زیرمجموعه از $W-\{0\}$ است و $W-\{0\}\subseteq W-(W\cup\{0\})=X$، پس $S(1)$ یک زیرمجموعه از X است و در نهایت داریم $m_v=S(1)\sqcup B(1)\subseteq X$.

اثبات ۳. در قسمت قبل، نشان دادیم که مجموعه‌ی X یک مجموعه‌ی کراندار است که شامل m_v است. بنابراین، یک عدد طبیعی h وجود دارد به گونه‌ای که $X\subseteq B(-h)$. لازم به ذکر است که چون $m_v=B(0)$ و $m_v\subseteq X$، پس گوی بازی که شامل X می‌شود باید شعاعی کمتر از 0 داشته باشد.

حال $\varphi(x)$ را فرمولی در نظر می‌گیریم که بیان کند $x^h\in X$. در ادامه، نشان می‌دهیم که $Y:=\varphi(K)-\varphi(K)$ همان مجموعه‌ی مطلوب ماست؛ یعنی $\exists$ ـC ـ تعریف‌پذیر است و $m_v\subseteq Y\subseteq O_v$.

۱. چون X یک مجموعه‌ی $\exists$ ـC ـ تعریف‌پذیر است، پس $\varphi(x)$ یک فرمول وجودی و با پارامتر از C است. بنابراین، $Y=\varphi(K)-\varphi(K)$ نیز یک مجموعه‌ی $\exists$ ـC ـ تعریف‌پذیر است.

۲. می‌خواهیم اثبات کنیم که Y یک زیرمجموعه از O_v است. برای این منظور، ابتدا نشان می‌دهیم که $\varphi(K)$ یک زیرمجموعه از O_v است. به طور معادل، نشان می‌دهیم که اگر a عضوی از O_v نباشد، آنگاه a نیز عضوی از $\varphi(K)$ نخواهد بود.

فرض کنید a در مجموعه O_v نباشد. با توجه به اینکه $\Gamma=\mathbb{Z}$، داریم $v(a)\leq -1$. بنابراین، $v(a^h)=hv(a)\leq -h$ و از این رو a^h در مجموعه $B(-h)$ قرار نمی‌گیرد. از آنجا که $X\subseteq B(-h)$، پس $a^h\notin X$ و در نتیجه $a\notin\varphi(K)$. حال چون $O_v=\bar{B}(0)$، پس با توجه به قسمت ۳ لم ۴.۶ داریم $O_v-O_v=O_v$ و بنابراین $Y=\varphi(K)-\varphi(K)\subseteq O_v-O_v=O_v$.

توجه کنید که چون Y یک زیرمجموعه از O_v است و $O_v=\bar{B}(0)\subseteq B(-1)$، پس $Y\subseteq B(-1)$ و در نتیجه Y یک مجموعه‌ی کراندار است.

۳. می‌خواهیم نشان دهیم که m_v یک زیرمجموعه از Y است. برای این منظور ابتدا توجه کنید که $\{x^h : v(x)=1\}\subseteq S(h)$. از طرفی با توجه به اینکه $S(h)\subseteq m_v\subseteq X$، نتیجه می‌گیریم که $\{x^h : v(x)=1\}\subseteq X$ و بنا به تعریف مجموعه‌ی $\varphi(K)$ داریم، $S(1)\subseteq\varphi(K)$. با توجه به لم ۴.۶، $B(1)\subseteq S(1)-S(1)$ در نتیجه:

$$B(1)\subseteq S(1)-S(1)\subseteq\varphi(K)-\varphi(K). \qquad (۱.۶)$$

همچنین از آنجا که $0^h = 0 \in m_v \subseteq X$، پس $0 \in \varphi(K)$ و بنابراین:

$$S(1) - 0 \subseteq \varphi(K) - \varphi(K). \tag{۲.۶}$$

نهایتاً با توجه به روابط (۱.۶) و (۲.۶) داریم:

$$m_v = S(1) \sqcup B(1) \subseteq \varphi(K) - \varphi(K) = Y.$$

توجه ۱۵.۶. در اثبات فوق، برای اینکه نشان دهیم یک مجموعه $S \subseteq K$ کراندار است، نشان دادیم که $n \in \mathbb{Z}$ وجود دارد به طوری که $S \subseteq B(n)$. به بیان دیگر، برقراری این شرط را برای اثبات کرانداری یک مجموعه کافی دانستیم. علت این است که اگر داشته باشیم $S \subseteq B(n)$ آنگاه برای هر گوی دلخواهِ $B(n')$ در توپولوژی القاء شده توسط نگاشت ارزیابی روی میدانِ K، گوی $B(n'-n)$ وجود دارد به طوری که $S \cdot B(n'-n) \subseteq B(n')$. در نتیجه مطابق تعریفِ ۲۹.۴، مجموعه‌ی S یک مجموعه‌ی کراندار است.

۵.۶ یک $\exists$ ـ $\mathbb{F}_q$ تعریف از $\mathbb{F}_q[[t]]$ در $\mathbb{F}_q((t))$

در بخش ۳.۶، نشان دادیم که اگر (K, τ) یک میدانِ t ـ هنسلی باشد که بسته‌ی جدایی‌پذیر نیست، آنگاه در τ یک همسایگی کراندار از صفر وجود دارد به طوری که با یک فرمول وجودی و با پارامتر از $C \subseteq K$ تعریف می‌شود. پس از آن در بخشِ ۴.۶، اثبات کردیم که اگر $K = F((t))$ و $V \subseteq K$ یک همسایگی کراندار از صفر باشد که $\exists$ ـ C ـ تعریف‌پذیر است، آنگاه می‌توان از آن به یک مجموعه‌ی $Y \subseteq K$ رسید که شاملِ m_v و مشمول در O_v است و توسط یک فرمول وجودی و با پارامتر از C تعریف می‌شود. در واقع، اهمیتِ $F((t))$ در مسیر رسیدن از V به مجموعه‌ی مطلوبِ Y این بود که $v(F((t))) = \mathbb{Z}$. در این بخش حالت خاصی را در نظر می‌گیریم که F یک میدان متناهی $\mathbb{F}_q$ باشد. ابتدا نشان می‌دهیم چون میدان سری‌های لوران روی $\mathbb{F}_q$ در شرایط قضیه‌ی ۱۲.۶ صدق می‌کند، پس در این میدان با توپولوژی القاء شده توسط نگاشت ارزیابی روی آن یک همسایگی $\exists$ ـ $\mathbb{F}_q$ ـ تعریف‌پذیر از صفر موجود است. سپس، با چند دستکاری مطابق با لمِ ۱۴.۶ از این همسایگی به مجموعه‌ی Y می‌رسیم که تعریف‌پذیر است و $m_v \subseteq Y \subseteq O_v$. در نهایت نشان می‌دهیم که $O_v = \mathbb{F}_q + Y$ و چون $\mathbb{F}_q$ و Y هر دو تعریف‌پذیر هستند، حلقه‌ی ارزیابِ O_v نیز تعریف‌پذیر می‌شود.

یادآوری ۱۶.۶. میدانِ $\mathbb{F}_q((t)) := \{\sum_{i=-n}^{\infty} a_i t^i | a_i \in \mathbb{F}_q\}$ را در نظر بگیرید. نگاشت $v : \mathbb{F}_q((t)) \to \mathbb{Z}$ با ضابطه‌ی $v(\sum_{i=-n}^{\infty} a_i t^i) := \min\{i | a_i \neq 0\}$ یک ارزیابی روی این میدان است که حلقه‌ی ارزیاب آن برابر با $\mathbb{F}_q[[t]] := \{\sum_{i=0}^{\infty} a_i t^i | a_i \in \mathbb{F}_q\}$ و ایده‌آل ماکسیمال آن $t\mathbb{F}_q[[t]]$ است.

نماد گذاری ۱۷.۶. در ادامه‌ی این فصل، میدان $\mathbb{F}_q((t))$ را با K و حلقه‌ی ارزیاب آن، یعنی $\mathbb{F}_q[[t]]$ را با O_v و ایده‌آل ماکسیمال آن، یعنی $t\mathbb{F}_q[[t]]$ را با m_v و توپولوژی القاء شده توسط نگاشت ارزیابی بیان شده در ۱۶.۶ را با τ_v نشان می‌دهیم.

لم ۱۸.۶. در میدان توپولوژیکِ $(\mathbb{F}_q((t)), \tau_v)$ یک همسایگی کراندار و $\exists$ ـ $\mathbb{F}_q$ ـ تعریف‌پذیر از صفر وجود دارد.

اثبات. همان‌طور که در مثالِ ۳۴.۵ دیدیم $(\mathbb{F}_q((t)), \tau_v)$ یک میدان t ـ هنسلی است. در ادامه، نشان می‌دهیم که میدانِ $\mathbb{F}_q$ در $\mathbb{F}_q((t))$ به طور نسبی بسته‌ی جبری است و همچنین، بسته‌ی جدایی‌پذیر نیست.

۱. بوضوح $\mathbb{F}_q$ یک زیرمیدان از $\mathbb{F}_q((t))$ است. ادعا می‌کنیم که $\mathbb{F}_q$ در $\mathbb{F}_q((t))$ به طور نسبی بسته‌ی جبری است. برای اثبات این ادعا، نشان می‌دهیم که هیچ عنصری در $\mathbb{F}_q((t)) \setminus \mathbb{F}_q$ نمی‌تواند ریشه‌ی یک چندجمله‌ای مانند $p(x) \in \mathbb{F}_q[x]$ باشد. توجه کنید که t روی $\mathbb{F}_q$ یک عنصر متعالی است. اگر یک عنصرِ $\sum_{i=-n}^{\infty} a_i t^i$ در $\mathbb{F}_q((t)) \setminus \mathbb{F}_q$ ریشه‌ی چندجمله‌ای $p(x)$ باشد، آنگاه نتیجه می‌شود که t یک عنصر جبری روی $\mathbb{F}_q$ است و این تناقض است.

۲. میدان $\mathbb{F}_q$ بسته‌ی جدایی‌پذیر نیست، زیرا $\mathbb{F}_{q^2}$ یک توسیع جدایی‌پذیر از $\mathbb{F}_q$ است. در واقع، هر توسیع متناهی از میدان‌های متناهی یک توسیع جدایی‌پذیر است.

بنابراین، با توجه به نتیجه‌ی ۱۲.۶، یک همسایگی کراندار و $\exists$ ـ $\mathbb{F}_q$ ـ تعریف‌پذیر از صفر در τ_v وجود دارد. $\square$

لم ۱۹.۶. میدان ارزیابی $(\mathbb{F}_q((t)), O_v)$ را در نظر بگیرید. اگر $Y \subseteq \mathbb{F}_q((t))$ به گونه‌ای باشد که $m_v \subseteq Y \subseteq O_v$، در این صورت $\mathbb{F}_q + m_v = \mathbb{F}_q + Y$.

اثبات. برای اثبات تساوی $\mathbb{F}_q + m_v = \mathbb{F}_q + Y$، ابتدا نشان می‌دهیم $\mathbb{F}_q + m_v \subseteq \mathbb{F}_q + Y$ و سپس $\mathbb{F}_q + Y \subseteq \mathbb{F}_q + m_v$ را اثبات می‌کنیم.

۱. برای اینکه $\mathbb{F}_q + m_v \subseteq \mathbb{F}_q + Y$ را ثابت کنیم، کافی است به این توجه کنیم که $m_v \subseteq Y$. پس، هر عنصری از $\mathbb{F}_q + m_v$ را می‌توان به صورت $a + b$ نوشت که در آن $a \in \mathbb{F}_q$ و $b \in m_v \subseteq Y$، پس $a + b \in \mathbb{F}_q + Y$.

۲. برای نشان دادن $\mathbb{F}_q + Y \subseteq \mathbb{F}_q + m_v$، فرض کنید $a + b_0 + b_1 t + b_2 t^2 + \dots$ یک عنصر دلخواه در $\mathbb{F}_q + Y$ باشد که در آن $a \in \mathbb{F}_q$ و $b_0 + b_1 t + b_2 t^2 + \dots \in Y$. در این صورت $a + b_0 \in \mathbb{F}_q$ و $b_1 t + b_2 t^2 + \dots \in m_v$، پس $a + b_0 + b_1 t + b_2 t^2 + \dots \in \mathbb{F}_q + m_v$.

$\square$

لم ۲۰.۶. O_v یک مجموعه‌ی $\exists$ ـ $\mathbb{F}_q$ ـ تعریف‌پذیر در میدانِ K است.

اثبات. در لم ۱۸.۶ نشان دادیم که در میدان توپولوژیک $(\mathbb{F}_q((t)), \tau_v)$، یک همسایگی کراندار و $\exists - \mathbb{F}_q -$ تعریف‌پذیر از صفر وجود دارد. با استفاده از لم ۱۴.۶، از این همسایگی تعریف‌پذیر از صفر به مجموعه‌ی Y می‌رسیم که $\exists - \mathbb{F}_q -$ تعریف‌پذیر است و $m_v \subseteq Y \subseteq O_v$. ادعا می‌کنیم که مجموعه‌ی O_v توسط فرمولِ $\chi := \exists y(y^q - y = 0 \wedge x \in y + Y)$ تعریف می‌شود.

بوضوح $O_v = \mathbb{F}_q + m_v$. از طرفی، با توجه به لم ۱۹.۶ داریم $\mathbb{F}_q + m_v = \mathbb{F}_q + Y$. لذا O_v برابر با مجموعه‌ی $\mathbb{F}_q + Y = \{x \in K : \exists y \in \mathbb{F}_q, x \in y + Y\}$ است. از آنجا که $\exists y \in \mathbb{F}_q$ به این معنی است که $\exists y \ y^q - y = 0$، بنابراین $\chi(K) = O_v$ و ادعای فوق اثبات می‌شود. $\square$

۶.۶ حذف پارامترها

در لم ۲۰.۶، فرمولِ χ را به دست آوردیم که حلقه‌ی ارزیابِ O_v را با پارامترهایی از میدانِ $\mathbb{F}_q$ تعریف می‌کند. در ادامه، فرض کنید q برابر با p^k باشد. از آنجا که ما برای اثبات قضیه ۲.۶ به دنبال یک فرمول بدون پارامتر برای تعریفِ O_v هستیم، پس قدم نهایی باید حذف این پارامترها از فرمولِ χ باشد. لازم به ذکر است که پارامترهای فرمولِ χ همان پارامترهای فرمولی است که مجموعه‌ی Y را تعریف می‌کند. پس در واقع، هدف این است که پارامترهای فرمولی که با آن مجموعه Y تعریف شده است، حذف شوند.

برای این منظور، ابتدا یک چندجمله‌ای تحویل‌ناپذیر f در $\mathbb{F}_p[x]$ انتخاب می‌کنیم که در $\mathbb{F}_q[x]$ نیز تحویل‌ناپذیر باقی بماند. سپس، به ازای این چندجمله‌ای f و عنصر مناسبِ a در $\mathbb{F}_q$ مجموعه‌ی $U_{f,a} = \{f(x)^{-1} - f(a)^{-1} : x \in K\}$ را تشکیل می‌دهیم. حال توجه کنید که هر عنصر در میدانِ $\mathbb{F}_p$ را می‌توان به صورت یک ترم بسته نوشت (به این معنی که هر $n \in \mathbb{F}_p$ را می‌توان به صورت مجموع n تا 1 نوشت). بنابراین، می‌توان ضرایب چندجمله‌ای f را با ترم‌های بسته معادلشان جایگذاری کرد. همچنین، با در نظر گرفتن این نکته که همه‌ی عناصر میدان $\mathbb{F}_q$ به صورت ریشه‌ی چندجمله‌ای $x^q - x$ قابل بیان هستند و با استفاده از یک ترفند ساده‌ی دیگر، پارامترِ a را نیز حذف می‌کنیم. اینگونه به یک همسایگی کراندار از صفر می‌رسیم که با یک فرمول بدون پارامتر تعریف می‌شود و تبع آن، مجموعه‌ی Y نیز $\exists - \emptyset -$ تعریف‌پذیر خواهد شد.

در ادامه، یک ویژگی را بیان می‌کنیم که اگر یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}_p[x]$ آن را دارا باشد، آنگاه در $\mathbb{F}_q[x]$ نیز تحویل‌ناپذیر باقی می‌ماند.

لم ۲۱.۶. فرض کنید مجموعه‌ی E متشکل از همه‌ی اعداد اولی باشد که عدد صحیحِ k را می‌شمارند. در این صورت، یک عددِ l وجود دارد به طوری که کوچکترین عدد اولی است که در E نیست و $1 + \prod_{p \in E} p$ را عاد می‌کند.

اثبات. برای عدد $1 + \prod_{p \in E} p$ دو وضعیت وجود دارد:

۱. اگر $1+\prod_{p\in E}p$ یک عدد اول باشد، آنگاه عنصر مطلوبِ l خودِ $1+\prod_{p\in E}p$ است، زیرا بوضوح $1+\prod_{p\in E}p$ را عاد می‌کند و در مجموعه‌ی E قرار ندارد.

۲. اگر $1+\prod_{p\in E}p$ مرکب باشد، آنگاه یک عدد اولِ l آن را عاد می‌کند. حال ادعا می‌کنیم که $l\notin E$. با برهان خلف فرض کنید $l\in E$. در این صورت بوضوح $l\mid\prod_{p\in E}p$ و در نتیجه $l\mid(1+\prod_{p\in E}p)-\prod_{p\in E}p=1$ که این تناقض است؛ بنابراین $l\notin E$.

□

لم ۲۲.۶. فرض کنید $f\in\mathbb{F}_p[x]$ یک چندجمله‌ای تحویل‌ناپذیر از درجه‌ی l باشد. اگر $l\nmid k$، آنگاه چندجمله‌ای f در $\mathbb{F}_{p^k}$ نیز تحویل‌ناپذیر باقی می‌ماند.

اثبات. با برهان خلف فرض کنید f در $\mathbb{F}_{p^k}[x]$ تحویل‌پذیر باشد، در این صورت $f=gg_1\cdots g_u$ که در آن g یک عامل تحویل‌ناپذیرِ f است. فرض کنید α یک ریشه‌ی g باشد، بنابراین $\mathbb{F}_{p^k}(\alpha)=\mathbb{F}_{p^{km}}$ که در آن m درجه‌ی g است. توجه کنید که چون α ریشه‌ی f نیز هست، بنابراین در میدانِ $\mathbb{F}_{p^{km}}$ که یک میدان شامل $\mathbb{F}_p$ است، ریشه‌ای از f قرار دارد. از طرفی، f یک چندجمله‌ای تحویل‌ناپذیر از درجه‌ی l در $\mathbb{F}_p$ است، بنابراین $\mathbb{F}_{p^l}$ کوچکترین میدان شامل $\mathbb{F}_p$ است که f در آن ریشه‌ای دارد. در نتیجه $\mathbb{F}_{p^l}\subseteq\mathbb{F}_{p^{km}}$ که نتیجه می‌دهد $l\mid km$. از آنجایی که l اول است، پس $l\mid k$ یا $l\mid m$. اما اولاً بنا به فرض $l\nmid k$ و ثانیاً $m<l$ پس $l\nmid m$ و اینگونه به تناقض می‌رسیم. در نتیجه f در $\mathbb{F}_{p^k}$ نیز تحویل‌ناپذیر است. □

قضیه ۲۳.۶. در میدان توپولوژیکِ $(\mathbb{F}_q((t)),\tau_v)$ یک همسایگی کراندار و $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر از صفر وجود دارد.

اثبات. فرض کنید $q=p^k$. همسایگی صفر مطلوب ما، به صورت $U_{f,a}=\{f(x)^{-1}-f(a)^{-1}:x\in K\}$ به ازای یک چندجمله‌ای مناسبِ f و یک عنصر مناسبِ a است. برای تشکیل این مجموعه، یک چندجمله‌ای تحویل‌ناپذیر f در $\mathbb{F}_p[x]$ می‌یابیم که در $\mathbb{F}_q[x]$ نیز تحویل‌ناپذیر باقی بماند و همچنین، شرطِ $x^q-x\nmid D(f)$ را برآورده کند؛ به عبارت دیگر همه‌ی عناصر $\mathbb{F}_q$ ریشه‌ی مشتق آن نباشند. توجه کنید که مطابق لم ۴۷.۱ میدان‌های متناهی، کامل هستند و بنابراین با یافتن یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}_q[x]$ جدایی‌پذیر بودن آن نیز تضمین می‌شود.

فرض کنید مجموعه‌ی E متشکل از همه‌ی اعداد اولی باشد که عدد صحیحِ k را می‌شمارند. در این صورت، بنا به لم ۲۱.۶ یک عدد l وجود دارد به طوری که کوچکترین عدد اولی است که در E نیست و عدد $1+\prod_{p\in E}p$ را عاد می‌کند. از آنجا که ممکن است در تجزیه‌ی عدد k اعداد اولی که در مجموعه‌ی E هستند با توان‌های بزرگتر از 1 ظاهر شوند، داریم $1+\prod_{p\in E}p\le 1+k$. از طرفی، از اینکه $l\mid 1+\prod_{p\in E}p$ نتیجه می‌شود که $l\le 1+\prod_{p\in E}p$ و بنابراین $l\le 1+k$. با توجه به اینکه $q=p^k$، نهایتاً به سادگی می‌توان نتیجه گرفت که $l\le p^k=q$.

حال چندجمله‌ای $f\in\mathbb{F}_p[x]$ را یک چندجمله‌ای تحویل‌ناپذیر و از درجه‌ی l انتخاب می‌کنیم. ادعا می‌کنیم که f همان چندجمله‌ای مورد نظر ماست؛ یعنی f در $\mathbb{F}_{p^k}[x]$ نیز تحویل‌ناپذیر است و همچنین حداقل یک عنصر در $\mathbb{F}_{p^k}$

وجود دارد به طوری که ریشه‌ی $D(f)$ نباشد. برای اثبات این ادعا توجه کنید که f یک چندجمله‌ای تحویل‌ناپذیر از درجه‌ی l است که $l \nmid k$، پس می‌توان بنا به لم ۲۲.۶ نتیجه گرفت که f در $\mathbb{F}_{p^k}[x]$ نیز تحویل‌ناپذیر باقی می‌ماند. به علاوه، از آنجا که $q \geq l$ داریم $q > l-1 \geq \deg(D(f))$ و بنابراین حتماً عنصری در $\mathbb{F}_q$ موجود است به طوری که ریشه‌ی $D(f)$ نباشد.

بنا به قضیه‌ی ۸.۶، برای هر a متعلق به $\mathbb{F}_q$ که ریشه‌ی $D(f)$ نیست، مجموعه‌ی $U_{f,a} := \{\frac{1}{f(x)} - \frac{1}{f(a)} : x \in K\}$ یک همسایگی کراندار و $\exists$ ـ $\mathbb{F}_q$ ـ تعریف‌پذیر از صفر است. از طرفی، می‌دانیم که اجتماع تعداد متناهی تا همسایگی کراندار از صفر باز هم یک همسایگی کراندار از صفر است، بنابراین $V := \bigcup\{U_{f,a} : a \in \mathbb{F}_q, Df(a) \neq 0\}$ یک همسایگی کراندار از صفر است که با فرمول زیر تعریف می‌شود:

$$\zeta := \exists y(y^q - y = 0 \wedge \neg Df(y) = 0 \wedge x \in U_{f,y}).$$

توجه کنید که پارامترهای این فرمول (همان ضرایب چندجمله‌ای f) از میدانِ $\mathbb{F}_p$ هستند. نهایتاً، از آنجا که هر عنصرِ n در $\mathbb{F}_p = \{0, 1, ..., p-1\}$ را می‌توان به صورت ترم بسته‌ی [1] $\underbrace{1 + \cdots + 1}_{n \text{تا}}$ نمایش داد، پس می‌توانیم ضرایب چندجمله‌ای f را با ترم بسته‌ی نظیر آن‌ها جایگزین کنیم و اینگونه، فرمولِ ζ به یک فرمول بدون پارامتر تبدیل می‌شود که V را تعریف می‌کند. در نتیجه V یک همسایگی $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر از صفر در میدان توپولوژیکِ $(\mathbb{F}_q((t)), \tau_v)$ است. □

قضیه ۲۴.۶. حلقه‌ی ارزیاب O_v یک مجموعه‌ی $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر در K است.

اثبات. با استفاده از لم ۲۳.۶، ابتدا یک همسایگی $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر از صفر می‌یابیم، سپس با به کارگیری لم ۱۴.۶ مجموعه‌ی $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر Y را به دست می‌آوریم که $m_v \subseteq Y \subseteq O_v$. حال مشابه آنچه در لم ۲۰.۶ شرح دادیم، فرمول وجودی زیرحلقه‌ی ارزیابِ O_v را تعریف می‌کند:

$$\varphi := \exists y(y^q - y = 0 \wedge x \in y + Y)$$

توجه کنید که φ به تبع فرمولی که Y را تعریف می‌کند، یک فرمول وجودی و بدون پارامتر است. □

توجه ۲۵.۶. فرمولی که در قضیه‌ی فوق به دست آوردیم به q بستگی دارد، بنابراین این فرمول نسبت به q یکنواخت نیست. در مقاله‌ی [۳] نشان داده شده است که اگر $q = p^k$ آن‌گاه فرمولی برای تعریفِ O_v وجود ندارد که در p یا k یکنواخت باشد.

[1] closed term

۷.۶ فرمول تعریفِ $\mathbb{F}_p[[t]]$ در $\mathbb{F}_p((t))$

در این بخش، قصد داریم یک فرمول را معرفی کنیم که حلقه‌ی ارزیابِ $\mathbb{F}_p[[t]]$ را در میدانِ $\mathbb{F}_p((t))$ تعریف می‌کند. در راستای این کار، ابتدا توجه کنید که $(\mathbb{F}_p((t)), \tau_v)$ یک میدانِ t ـ هسنلی است و $\mathbb{F}_p((t))$ بسته‌ی جدایی‌پذیر نیست، همچنین $f = x^p - x - 1$ و $a = 1$ در شروط قضیه‌ی ۸.۶ صدق می‌کنند، پس مجموعه‌ی $U_{f,1}$ یک همسایگی کراندار و تعریف‌پذیر از صفر در $(\mathbb{F}_p((t)), \tau_v)$ است. سپس، با استفاده از لم ۱۴.۶، از همسایگی $U_{f,1}$ به یک مجموعه‌ی تعریف‌پذیرِ Y می‌رسیم که $t\mathbb{F}_p[[t]] \subseteq Y \subseteq \mathbb{F}_p[[t]]$. نهایتاً مشابه با توضیحات قبلی، فرمولِ $\exists y(y^p - y = 0 \wedge x \in y + Y)$ حلقه‌ی ارزیابِ $\mathbb{F}_p[[t]]$ را در میدانِ $\mathbb{F}_p((t))$ تعریف می‌کند. با توجه به نحوه‌ی ساخت مجموعه‌ی Y، می‌توانیم این فرمول را با استفاده از ترم‌های دقیق‌تری بازنویسی می‌کنیم.

یادآوری ۲۶.۶. اگر G یک گروه با مرتبه‌ی متناهی p باشد، آن‌گاه به ازای هر عنصرِ a در G داریم $a^p = a$.

در لم زیر، نشان می‌دهیم که چندجمله‌ای $f = x^p - x - 1$ یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}_p[x]$ و بنابراین یک چندجمله‌ای جدایی‌پذیر است. همچنین، همان‌طور که خواهیم دید، این چندجمله‌ای در $\mathbb{F}_p$ هیچ ریشه‌ای ندارد.

لم ۲۷.۶. به ازای هر عدد اول p، چندجمله‌ای $f = x^p - x - 1$ در $\mathbb{F}_p[x]$ تحویل‌ناپذیر است.

اثبات. اثبات این لم طی مراحل زیر انجام می‌شود:

۱. برای هر $\alpha \in \mathbb{F}_p$، با توجه به قضیه‌ی لاگرانژ، داریم $\alpha^p = \alpha$ و بنابراین $\alpha^p - \alpha = 0$. در نتیجه به ازای هر $\alpha \in \mathbb{F}_p$ داریم $\alpha^p - \alpha - 1 = -1$، پس چندجمله‌ای f هیچ ریشه‌ای در $\mathbb{F}_p$ ندارد.

۲. فرض کنید α ریشه‌ی f در بستار جبریِ $\mathbb{F}_p$ باشد. در این صورت، $\alpha^p - \alpha - 1 = 0$. از طرفی، چون مشخصه‌ی بستار جبری $\mathbb{F}_p$ نیز p است، پس به ازای هر $s \in \mathbb{F}_p$ داریم $(\alpha + s)^p = \alpha^p + s^p$ و در نتیجه

$$(\alpha + s)^p - (\alpha + s) - 1 = \alpha^p + s^p - \alpha - s - 1 = s^p - s = 0.$$

بنابراین اگر α ریشه‌ی f باشد، آن‌گاه به ازای هر $s \in \mathbb{F}_p$ عنصرِ $\alpha + s$ نیز ریشه‌ی f است.

۳. از آنجا که میدان $\mathbb{F}_p$ دارای p عنصر متمایز است، از مرحله ۲ نتیجه می‌گیریم که مجموعه‌ی $\{\alpha, \alpha_1, \alpha + 2, \ldots, \alpha + p - 1\}$ شامل تمام ریشه‌های چندجمله‌ای f است. به عبارت دیگر، چندجمله‌ای f در میدان شکافنده‌ی خود به صورتِ $(x - \alpha)(x - (\alpha + 1)) \cdots (x - (\alpha + p - 1))$ تجزیه می‌شود. حال با برهان خلف فرض کنید f در $\mathbb{F}_p[x]$ تحویل‌پذیر باشد، پس $f = gh$ به طوری که $g, h \in \mathbb{F}_p[x]$ و درجه‌ی آن‌ها کمتر از f است. بوضوح g و h باید به صورت $(x - (\alpha + s_1)) \cdots (x - (\alpha + s_k))$ باشند که در آن $0 \leq s_i \leq p - 1$. بدون کاستن از کلیت فرض

کنید $g = (x-(\alpha+s_i))(x-(\alpha+s_j)) = x^2-(2\alpha+s_i+s_j)x+(\alpha+s_i)(\alpha+s_j)$. از آنجا که g متعلق به $\mathbb{F}_p[x]$ است، پس بوضوح ضرایب آن از جمله $2\alpha+s_i+s_j$ در $\mathbb{F}_p$ هستند. از طرفی $\mathbb{F}_p$ یک میدان است و $s_i, s_j \in \mathbb{F}_p$، پس $s_i+s_j \in \mathbb{F}_p$ که نتیجه می‌دهد $2\alpha+s_i+s_j-(s_i+s_j) = 2\alpha$ نیز در $\mathbb{F}_p$ قرار دارد. به علاوه عنصر 2 در $\mathbb{F}_p$ وارون‌پذیر است، بنابراین $\alpha = 2^{-1}\cdot 2\alpha$ متعلق به $\mathbb{F}_p$ است که این تناقض است.

□

توجه ۲۸.۶. در لم فوق نشان دادیم که چندجمله‌ای $f = x^p - x - 1$ در $\mathbb{F}_p[x]$ یک چندجمله‌ای تحویل‌ناپذیر است و در $\mathbb{F}_p$ هیچ ریشه‌ای ندارد. از طرفی، $D(f) = -1 \neq 0$. حال مجموعه‌ی $U_{f,1}$ را تشکیل می‌دهیم. این مجموعه بنا به قضیه‌ی ۸.۶، یک همسایگی کراندار و تعریف‌پذیر از صفر در $(\mathbb{F}_p((t)), \tau_v)$ است. با استفاده از لم ۱۴.۶ از این همسایگی کراندار از صفر را به یک مجموعه‌ی کراندار و تعریف‌پذیرِ Y می‌رسیم که $t\mathbb{F}_p[[t]] \subseteq Y \subseteq \mathbb{F}_p[[t]]$. مشابه آنچه که قبلا شرح دادیم، فرمولِ

$$\mu = \exists y(y^p - y = 0 \wedge x \in y + Y)$$

حلقه‌ی ارزیابِ $\mathbb{F}_p[[t]]$ را در میدانِ $\mathbb{F}_p((t))$ تعریف می‌کند. در مراحل زیر، برای هر ترم در فرمول μ، ترم دقیق‌تری را جایگزین می‌کنیم:

۱. در فرمول μ، به جای ترمِ $x \in y+Y$ که در آن $y \in \mathbb{F}_p$، اینطور می‌نویسیم که x منهای یک عنصر در Y، متعلق به $\mathbb{F}_p$ است. از طرفی، در لم ۱۴.۶ نشان دادیم که مجموعه‌ی Y برابر است با $\varphi(K)-\varphi(K)$. بنابراین برای $(a-b) \in Y$ داریم $x-(a-b) \in \mathbb{F}_p$، یعنی $(x-(a-b))^p - (x-(a-b)) = 0$.

۲. توجه کنید که $X = W - W'$ و $\varphi(K) = \{x : x^h \in X\}$. از آنجا که $(a-b) \in Y = \varphi(K)-\varphi(K)$، پس $a, b \in \varphi(K)$ یعنی $a^h = x_1 - x_2$ و $b^h = x_3 - x_4$ که $x_1, x_2, x_3, x_4 \in W$.

۳. مجموعه‌ی W را شامل عناصری از K در نظر گرفتیم که توانِ m ـ اُم آن‌ها در $V = U_{f,1}$ باشد، بنابراین از آنجا که مطابق مرحله‌ی قبل $x_1, x_2, x_3, x_4 \in W$، پس برای هر $1 \leq i \leq 4$ داریم $x_i^m \in U_{f,1}$. در نتیجه بنا به تعریف مجموعه‌ی $U_{f,1}$، عنصر $y_i \in K$ وجود دارد به طوری که $x_i^m = \frac{1}{f(y_i)} - \frac{1}{f(1)} = \frac{1}{f(y_i)} + 1$، بنابراین $f(y_i)(x_i^m - 1) - 1 = 0$.

در نهایت، فرمول زیر $\mathbb{F}_p[[t]]$ را در $\mathbb{F}_p((t))$ تعریف می‌کند:

$$\exists a, b, x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \Big((x-(a-b))^p - (x-(a-b)) = 0 \wedge a^h = x_1 - x_2 \wedge b^h = x_3 - x_4 \wedge \bigwedge_{i=1}^{4} f(y_i)(x_i^m - 1) - 1 = 0 \Big).$$

* خلاصه‌ی فصل:

قضیه‌ی اصلی این فصل، این است که حلقه‌ی ارزیابی $\mathbb{F}_q[[t]]$ در میدان ارزیابی $\mathbb{F}_q((t))$ با یک فرمول وجودی و بدون پارامتر و در زبان حلقه‌ها تعریف‌پذیر است. اثبات این قضیه در چند مرحله و به شرح زیر انجام می‌شود:

۱. از آنجا که $(\mathbb{F}_q((t)), \tau_v)$ یک میدان t ـ هنسلی و $\mathbb{F}_q \subseteq \mathbb{F}_q((t))$ یک زیرمیدان به طور نسبی بسته‌ی جبری است که بسته‌ی جدایی‌پذیر نیست، پس یک همسایگی $\exists$ ـ $\mathbb{F}_q$ تعریف‌پذیر و کراندار از صفرِ V در τ_v وجود دارد.

۲. از همسایگی V می‌توان به یک مجموعه‌ی $\exists$ ـ $\mathbb{F}_q$ تعریف‌پذیرِ Y رسید که شامل m_v و مشمول در O_v است.

۳. چون $O_v = \mathbb{F}_q + Y$ و عناصر $\mathbb{F}_q$ ریشه‌ی چندجمله‌ای $x^q - x$ هستند، بنابراین می‌توان مجموعه‌ی O_v را با فرمول $\varphi := \exists y(y^q - y = 0 \wedge x \in y + Y)$ تعریف کرد.

۴. فرمول φ وجودی و با پارامتر از $\mathbb{F}_q$ است. برای حذف این پارامترها ابتدا یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{F}_p[x]$ از درجه‌ی l را به طوری در نظر می‌گیریم که $l \nmid k$. در این صورت، یک عنصر $a \in \mathbb{F}_q$ وجود دارد به طوری که $D(f)(a) \neq 0$. حال با استفاده از این f و a مجموعه‌ی $U_{f,a}$ را تشکیل می‌دهیم. سپس، با در نظر گرفتن $V := \bigcup\{U_{f,a} : a \in \mathbb{F}_q, Df(a) \neq 0\}$ که یک همسایگی کراندار و تعریف‌پذیر از صفر است و با استفاده از مرحله‌ی ۲ می‌توانیم به یک مجموعه‌ی مطلوبِ Y برسیم که $\exists$ ـ $\mathbb{F}_p$ ـ تعریف‌پذیر است. از آنجا که عناصرِ $\mathbb{F}_p$ را می‌توان به صورت ترم‌های بسته نوشت، پس فرمول φ به یک فرمول بدون پارامتر تبدیل می‌شود.

فصل ۷

دو نتیجه‌ی مرتبط

در فصل قبل، اثبات کردیم که حلقه‌ی ارزیابِ $\mathbb{F}_q[[t]]$ در میدان ارزیابی $\mathbb{F}_q((t))$ با یک فرمول وجودی و بدون پارامتر تعریف‌پذیر است. برای این اثبات، از ویژگی‌های t ـ هنسلی بودن و بسته‌ی جدایی‌پذیر نبودن میدان ارزیابی $\mathbb{F}_q((t))$ استفاده کردیم. در این فصل توجهمان را معطوف به ویژگی‌های دیگری از این میدان ارزیابی می‌کنیم و تعریف‌پذیری $\mathbb{F}_q[[t]]$ در $\mathbb{F}_q((t))$ را با دو روش دیگر اثبات می‌کنیم.

در ادامه ابتدا یک قضیه از مقاله‌ی [۱۰] را بررسی می‌کنیم. این قضیه بیان می‌کند که اگر (K, O_v) یک میدان ارزیابی p ـ مطلوب باشد که گروه ارزیاب آن گسسته است، آنگاه حلقه‌ی ارزیابِ O_v با یک فرمول وجودی و تک پارامتر در زبان حلقه‌ها تعریف‌پذیر است (برای تعریف یک میدانِ p ـ مطلوب به مقاله‌ی [۱۰] و برای تعریف یک گروه گسسته به تعریفِ ۲.۷ رجوع کنید). به طور خاص بنا به تعریفِ p ـ مطلوب، میدان‌های هنسلی، p ـ مطلوب هستند و ما در این فصل فقط به آن‌ها می‌پردازیم. با توجه به اینکه میدان ارزیابیِ $(\mathbb{F}_q((t)), \mathbb{F}_q[[t]])$ هنسلی و گروه ارزیاب آن برابر با $\mathbb{Z}$ است، می‌توان از نتیجه‌ی این مقاله استفاده کرد و نتیجه گرفت که $\mathbb{F}_q[[t]]$ تعریف‌پذیر است.

بعد از آن به بررسی مقاله‌ی [۷] می‌پردازیم که در آن اثبات شده است که اگر (K, O_v) یک میدان ارزیابی هنسلی باشد و میدان پیمانه‌های آن متناهی یا سودو بسته‌ی جبری باشد، آنگاه O_v با یک فرمول وجودی و بدون پارامتر در زبان حلقه‌ها تعریف می‌شود(برای تعریف میدان سودو بسته‌ی جبری به همان مقاله‌ی [۷] مراجعه کنید). البته ما در این فصل فقط حالت خاصی که میدان پیمانه‌ها متناهی است را بررسی می‌کنیم.

نماد گذاری ۱.۷. یک میدان را با نمادِ K نشان می‌دهیم. اگر O_v یک حلقه‌ی ارزیاب در میدانِ K باشد، آنگاه نگاشت ارزیاب نظیر آن را با $v : K \to v(K)$ نشان می‌دهیم که در آن $v(K)$ گروه ارزیاب است. همچنین، با m_v و

k_v به ترتیب ایده‌آل ماکسیمال حلقه‌ی ارزیاب و میدان پیمانه‌های نظیر آن را نمایش می‌دهیم. در ادامه منظورمان از p یک عدد اول است.

۱.۷ گروه ارزیاب گسسته [۱۰]

تعریف ۲.۷. یک گروه مرتب Γ را گسسته می‌نامیم هرگاه $\Gamma \cong \mathbb{Z}$.

در این بخش، قصد داریم نشان دهیم که اگر (K, O_v) یک میدان ارزیابی هنسلی باشد و $v(K)$ یک گروه گسسته باشد، آنگاه O_v در K با یک فرمول وجودی و تک پارامتر در زبان حلقه‌ها تعریف‌پذیر است. این قضیه طی دو مرحله اثبات می‌شود. در مرحله‌ی اول، نشان می‌دهیم که اگر $\gamma \in v(K)$ یک عنصر p ـ بخش‌پذیر نباشد، آنگاه مجموعه‌ی $\{x \in K : pv(x) + \gamma > 0\}$ تعریف‌پذیر است. در مرحله‌ی دوم، اثبات می‌کنیم که اگر γ را کوچکترین عنصر مثبتِ $v(K)$ در نظر بگیریم، آنگاه مجموعه‌ی $\{x \in K : pv(x) + \gamma > 0\}$ برابر با O_v می‌شود و بنابراین با توجه به مرحله‌ی اول، O_v تعریف‌پذیر است.

تعریف ۳.۷. فرض کنید $(G, +)$ یک گروه آبلی و g متعلق به G و n یک عدد طبیعی باشد. می‌گوییم g یک عنصر nـ بخش‌پذیر است هرگاه یک عنصرِ y در G وجود داشته باشد به طوری که $ny = g$.

قضیه ۴.۷. فرض کنید (K, O_v) یک میدان ارزیابی هنسلی باشد. اگر $\gamma \in v(K)$ یک عنصرِ pـ بخش‌پذیر نباشد، آنگاه مجموعه‌ی $E = \{x \in K : pv(x) + \gamma > 0\}$ در میدانِ K و در زبان حلقه‌ها تعریف‌پذیر است.

اثبات. به سادگی می‌توان دید که 0 متعلق به E است، بنابراین $E \neq \emptyset$. از آنجا که γ در $v(K)$ قرار دارد، پس یک عنصرِ ϵ در K موجود است به طوری که $v(\epsilon) = \gamma$. در ادامه نشان می‌دهیم که فرمول زیر مجموعه‌ی E تعریف می‌کند:

$$\varphi(x) = \exists y (y^p - y^{p-1} = \epsilon x^p).$$

به عبارت دیگر، اثبات می‌کنیم که اگر $x \in E$، آنگاه در فرمول $\varphi(x)$ صدق می‌کند. همچنین، اگر یک عنصرِ x در K در فرمول $\varphi(x)$ صدق کند، آنگاه $x \in E$.

۱. ابتدا نشان می‌دهیم که اگر $x \in E$، آنگاه $\exists y (y^p - y^{p-1} - \epsilon x^p = 0)$. از اینکه $x \in E$ نتیجه می‌گیریم که $pv(x) + \gamma > 0$. با توجه به ویژگی‌های یک نگاشت ارزیابی، عبارتِ $pv(x) + \gamma > 0$ یعنی $v(\epsilon x^p) > 0$ و بنابراین $\epsilon x^p \in m_v$. از آنجا که (K, O_v) یک میدان ارزیابی هنسلی است، پس بنا به قسمت ۳ لمِ ۱۱.۲، چندجمله‌ای $f(y) = y^p - y^{p-1} - \epsilon x^p$ یک ریشه در K دارد.

۲. حال نشان می‌دهیم که اگر $y^p - y^{p-1} - \epsilon x^p = 0$، آنگاه $x \in E$. با برهان خلف فرض کنید $x \notin E$، یعنی $pv(x) + \gamma \leq 0$. اما توجه کنید که $pv(x) + \gamma$ نمی‌تواند برابر با صفر شود، زیرا در این صورت γ یک عنصر pـ بخش‌پذیر است که این با فرض تناقض دارد. در نتیجه بسته به علامت $v(y)$ دو حالت زیر رخ می‌دهد:

حالت اول. $v(y) \geq 0$: با استفاده از ویژگی‌های یک نگاشت ارزیابی داریم

$$v(y^p - y^{p-1} - \epsilon x^p) = \min\{pv(y), (p-1)v(y), pv(x) + \gamma\}.$$

چون $v(y) \geq 0$، پس $pv(y) \geq (p-1)v(y) \geq 0$، همچنین فرض کردیم که $pv(x) + \gamma < 0$ و بنابراین $v(y^p - y^{p-1} - \epsilon x^p) = pv(x) + \gamma < 0$. اما توجه کنید که $y^p - y^{p-1} - \epsilon x^p = 0$، بنابراین $v(y^p - y^{p-1} - \epsilon x^p) = v(0) = \infty$ و این تناقض است.

حالت دوم. $v(y) < 0$: در این صورت $pv(y) < (p-1)v(y) < 0$، پس نتیجه می‌گیریم که $v(y^p - y^{p-1} - \epsilon x^p) = \min\{pv(y), (p-1)v(y), pv(x) + \gamma\} < 0$. چون $y^p - y^{p-1} - \epsilon x^p = 0$، پس $v(y^p - y^{p-1} - \epsilon x^p) = v(0) = \infty$ و این تناقض است.

بنابراین اگر $\exists y \quad y^p - y^{p-1} - \epsilon x^p = 0$، آنگاه $pv(x) + \gamma$ نمی‌تواند منفی باشد و در نتیجه $pv(x) + \gamma > 0$، به بیان دیگر $x \in E$. □

قضیه ۵.۷. فرض کنید (K, O_v) یک میدان ارزیابی هنسلی باشد. اگر $v(K)$ گسسته باشد، آنگاه O_v در زبان حلقه‌ها تعریف‌پذیر است.

اثبات. با توجه به اینکه $v(K)$ یک گروه گسسته است، پس $v(K) \cong \mathbb{Z}$. بنابراین از آنجا که در $\mathbb{Z}$ عدد 1 کوچکترین عنصر مثبت است، می‌توان نتیجه گرفت که در $v(K)$ نیز کوچکترین عنصر مثبت وجود دارد. حال فرض کنید عنصرِ $v(\epsilon)$ به ازای $\epsilon \in K$، کوچکترین عنصر مثبتِ $v(K)$ باشد. توجه کنید که $v(\epsilon)$ یک عنصر p ـبخش‌پذیر نیست، زیرا اگر یک عنصر $y \in v(K)$ وجود داشته باشد به طوری که $v(\epsilon) = py$، آنگاه بوضوح $0 < y < v(\epsilon)$ و این با ویژگی کوچکترین عنصر مثبت بودنِ $v(\epsilon)$، در تناقض است. بنا به قضیه‌ی ۴.۷، مجموعه‌ی $E = \{x \in K : v(\epsilon x^p) > 0\}$ در زبان حلقه‌ها تعریف‌پذیر است. ادعا می‌کنیم که $O_v = E$. برای اثبات این ادعا نشان می‌دهیم که هر عنصر دلخواهِ O_v در E است و بالعکس.

۱. یک عنصر دلخواهِ $x \in O_v$ را در نظر بگیرید. در این صورت، $v(x) \geq 0$ و چون $v(\epsilon)$ نیز مثبت است، پس $v(\epsilon x^p) = v(\epsilon) + pv(x) > 0$، بنابراین $x \in E$.

۲. یک عنصر دلخواهِ $x \in E$ را در نظر بگیرید. با برهان خلف فرض کنید $x \notin O_v$، یعنی $v(x) < 0$. از آنجا که $v(\epsilon)$ را کوچکترین عدد مثبت در $v(K)$ در نظر گرفتیم، می‌توان نتیجه گرفت که $v(\epsilon x^p) = v(\epsilon) + pv(x) < 0$ و در نتیجه $x \notin E$ که این تناقض است.

□

لم ۶.۷. حلقه‌ی ارزیابِ $\mathbb{F}_q[[t]]$ در میدانِ $\mathbb{F}_q((t))$ با یک فرمول وجودی و تک پارامتر در زبان حلقه‌ها تعریف‌پذیر است.

اثبات. یادآوری می‌کنیم که $\mathbb{F}_q((t))$ میدان سری‌های لوران روی $\mathbb{F}_q$ است. نگاشت $v : \mathbb{F}_q((t)) \to \mathbb{Z}$ با ضابطه‌ی $v(\sum_{i=-n}^{\infty} a_i t^i) := \min\{i | a_i \neq 0\}$ یک ارزیابی روی این میدان است که حلقه‌ی ارزیاب آن، $\mathbb{F}_q[[t]]$ است. بنا به لم ۲۶.۳، میدان ارزیابی $(\mathbb{F}_q((t)), \mathbb{F}_q[[t]])$ هنسلی است. بنابراین با توجه به اینکه $v(\mathbb{F}_q((t))) = \mathbb{Z}$، می‌توان بنا به قضیه‌ی ۵.۷ نتیجه گرفت که حلقه‌ی ارزیاب $\mathbb{F}_q[[t]]$ با یک فرمول وجودی و تک پارامتر در میدان $\mathbb{F}_q((t))$ تعریف‌پذیر است. □

۲.۷ اثبات کلی‌تر برای قضیه‌ی مقاله‌ی اصلی [۷]

نماد گذاری ۷.۷. منظورمان از (K, O_v)، یک میدان ارزیابی است که O_v حلقه‌ی ارزیاب آن با ایده‌آل ماکسیمالِ m_v است. میدان پیمانه‌های آن، یعنی O_v/m_v را نیز با نماد k_v نشان می‌دهیم. از نمادِ «$^-$» برای تصویر کانونی عناصر در میدان پیمانه‌ها استفاده می‌کنیم.

در این بخش، قصد داریم به مقاله‌ی [۷] بپردازیم که یک حالت کلی‌تر از قضیه‌ی اثبات شده در مقاله‌ی اصلی پایان‌نامه را بیان می‌کند. در این مقاله ثابت شده است که اگر (K, O_v) یک میدان ارزیابی هنسلی باشد که میدان پیمانه‌های آن متناهی است، آنگاه O_v در زبان حلقه‌ها $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر است. اثبات این قضیه به شرح زیر است:

۱. اگر میدان پیمانه‌ها متناهی باشد، آنگاه می‌توان یک چندجمله‌ای تکینِ f در $\mathbb{Z}[x]$ پیدا کرد به طوری که $\bar{f}$ در میدان پیمانه‌ها ریشه ندارد و همچنین یک عنصر a در O_v موجود است به طوری که در شرطِ $f'(a) \notin m_v$ صدق می‌کند.

۲. با استفاده از هنسلی بودن میدان ارزیابی (K, O_v) و ویژگی‌های چندجمله‌ای f نشان می‌دهیم که $U_f = \{f(x)^{-1} - f(y)^{-1} : x, y \in K\}$ یک مجموعه‌ی $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر است که شامل m_v و مشمول در O_v است.

۳. نشان می‌دهیم که مجموعه‌ی T متشکل از ریشه‌های چندجمله‌ای $x^q - x$ در میدانِ K، شرطِ $\bar{T} = k_v$ را برآورده می‌کند.

۴. در مرحله‌ی آخر نشان می‌دهیم که $O_v = U_f + T$ و از آنجا که بنا به مراحل قبل U_f و T هر دو $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر هستند، نتیجه می‌گیریم که O_v نیز $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر است.

توجه کنید که از این قضیه نیز می‌توانیم نتیجه بگیریم که حلقه‌ی ارزیابِ $\mathbb{F}_q[[t]]$ در میدانِ $\mathbb{F}_q((t))$ در زبان حلقه‌ها $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر است، زیرا میدان پیمانه‌های آن برابر با میدن متناهیِ $\mathbb{F}_q$ است.

به منظور جلوگیری از ابهام و روشن‌تر شدن مطلب، در پایان این فصل به شباهت‌ها و تفاوت‌های اثبات مذکور با اثباتی که در فصل قبل مورد بررسی قرار گرفت، اشاره خواهیم کرد.

۱.۲.۷ معرفی دو زیرمجموعه‌ی U و T از O_v

نماد گذاری ۸.۷. یک چندجمله‌ایِ f در $O_v[x]$ را در نظر بگیرید. منظورمان از نمادِ $f(K)^{-1}$ مجموعه‌ی $\{f(x)^{-1} : x \in K\}$ است. به علاوه به ازای یک عنصرِ a در K مجموعه‌ی $\{f(x)^{-1} - f(a)^{-1} : x \in K\}$ را با نمادِ $U_{f,a}$ نشان می‌دهیم.

لم ۹.۷. فرض کنید $f \in O_v[x]$ یک چندجمله‌ای تکین باشد به طوری که $\bar{f}$ در k_v ریشه‌ای ندارد. یک عنصرِ a در K را در نظر بگیرید. در این صورت، موارد زیر برقرار هستند:

۱. $f(K)^{-1} \subseteq O_v$،

۲. $U_{f,a} \subseteq O_v$،

۳. اگر $a \in O_v$ و $f'(a) \notin m_v$، آن‌گاه $m_v \subseteq U_{f,a}$.

اثبات.

۱. یک عنصر دلخواهِ $f(t)^{-1}$ در $f(K)^{-1}$ در نظر بگیرید. می‌خواهیم نشان دهیم که $f(t)^{-1} \in O_v$. عنصر t متعلق به K است، از این رو بسته به اینکه $t \in O_v$ یا $t \notin O_v$ دو حالت زیر رخ می‌دهد :

حالت اول. $t \in O_v$: چون f یک چندجمله‌ای با ضرایب از O_v است و فرض کرده‌ایم که t در O_v قرار دارد، پس با توجه به حلقه بودن O_v می‌توان نتیجه گرفت که $f(t)$ در O_v است، یعنی $\underbrace{v(f(t)) \geq 0}_{*}$. از طرفی بنا به فرض $\bar{f}$ در k_v ریشه ندارد، پس $\bar{f}(\bar{t}) \neq 0$ و به عبارت دیگر $f(t) \notin m_v$. حال با توجه به $*$ نتیجه می‌گیریم که $v(f(t)) = 0$ و بنابراین $v(f(t)^{-1}) = 0$، پس $f(t)^{-1} \in O_v$.

حالت دوم. $t \notin O_v$: بدون کاستن از کلیت فرض کنید $f \in O_v[x]$ از درجه‌ی n باشد. در این صورت با توجه به اینکه f یک چندجمله‌ای تکین است، پس $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. چون فرض کردیم $t \notin O_v$، پس $v(t) < 0$. از طرفی $f \in O_v[x]$، بنابراین به ازای هر $0 \leq i \leq n-1$ داریم $v(a_i) \geq 0$ و در نتیجه

$$v(f(t)) = v(t^n + a_{n-1}t^{n-1} + \cdots + a_0) = \min\{nv(t), v(a_{n-1}) + (n-1)v(t), \cdots, v(a_0)\} = nv(t).$$

از این رو $v(f(t)) = nv(t) < 0$ و بنابراین $v(f(t)^{-1}) = -v(f(t)) > 0$، یعنی $f(t)^{-1} \in O_v$.

۲. یک عنصر دلخواهِ $f(t)^{-1} - f(a)^{-1}$ متعلق به $U_{f,a} = f(K)^{-1} - f(a)^{-1}$ را در نظر بگیرید. از آنجا که مطابق قسمت ۱ همین لم $f(K)^{-1} \subseteq O_v$، پس $f(t)^{-1}, f(a)^{-1} \in O_v$ و با توجه به حلقه بودنِ O_v نتیجه می‌گیریم که $f(t)^{-1} - f(a)^{-1} \in O_v$.

۳. فرض کنید t یک عنصر دلخواهِ m_v باشد. می‌خواهیم نشان دهیم که t متعلق به $U_{f,a}$ است. بدین منظور، باید یک عنصرِ s در K بیابیم به طوری که $t = f(s)^{-1} - f(a)^{-1}$. حال اگر طرفین این تساوی را در $f(s)f(a)$ ضرب کنیم، آنگاه داریم $tf(s)f(a) - f(a) + f(s) = 0$. پس در ادامه هدفمان این است که نشان دهیم چندجمله‌ایِ $g(x) = tf(x)f(a) - f(a) + f(x)$ در K ریشه دارد. برای این کار از فرض هنسلی بودن میدانِ (K, O_v) استفاده می‌کنیم، پس ابتدا ثابت می‌کنیم که $g'(a) \notin m_v$:

با مشتق گیری از g نسبت به x و سپس جایگذاری a در آن داریم:

$$g'(a) = tf'(a)f(a) + f'(a) = f'(a)(tf(a) + 1)$$

بنابراین $v(g'(a)) = v(f'(a)(tf(a) + 1)) = v(f'(a)) + v(tf(a) + 1)$. حال توجه کنید که بنا به فرض $f'(a) \notin m_v$ و چون $a \in O_v$ و $f \in O_v[x]$ داریم $f'(a) \in O_v$، پس نتیجه می‌گیریم که $v(f'(a)) = 0$. از طرفی از آنجا که $a \in O_v$ و $f \in O_v[x]$، پس بوضوح $v(f(a)) \geq 0$. همچنین چون $t \in m_v$، پس $v(t) > 0$ و بنابراین $v(tf(a)) = v(t) + v(f(a)) > 0$. نهایتاً داریم $v(g'(a)) = v(f'(a)) + v(tf(a) + 1) = 0 + \min\{v(t) + v(f(a)), 0\} = 0$، یعنی $g'(a) \notin m_v$. حال نشان می‌دهیم که $g(a) \in m_v$. بوضوح داریم:

$$g(a) = tf(a)f(a) - f(a) + f(a) = tf(a)f(a)$$

حال از آنجا که $a \in O_v$ و $f \in O_v[x]$، پس $f(a) \in O_v$ و بنا به حالت اول در اثبات قسمت ۱ همین لم داریم $v(f(a)) = 0$. همچنین $t \in m_v$، پس $v(t) > 0$ و در نتیجه داریم :

$$v(g(a)) = v(t) + 2v(f(a)) = v(t) > 0$$

یعنی $g(a) \in m_v$. نهایتاً از اینکه $g(a) \in m_v$ و $g'(a) \notin m_v$، پس بنا به هسنلی بودن میدانِ (K, O_v) نتیجه می‌گیریم که یک عنصر s در K وجود دارد به طوری که ریشه‌ی $g(x)$ است یا به عبارتی $t = f(s)^{-1} - f(a)^{-1}$.

□

نماد گذاری ۱۰.۷. مجموعه‌ی $f(K)^{-1} - f(K)^{-1} = \{f(x)^{-1} - f(y)^{-1} : x, y \in K\}$ را با نماد U_f نشان می‌دهیم.

لم ۱۱.۷. فرض کنید $f \in O_v[x]$ یک چندجمله‌ای تکین باشد که $\bar{f}$ در k_v ریشه‌ای ندارد و همچنین، عنصر $a \in O_v$ وجود داشته باشد به طوری که $f'(a) \notin m_v$. در این صورت $m_v \subseteq U_f \subseteq O_v$.

اثبات. می‌خواهیم نشان دهیم که $U_f \subseteq O_v$. عنصر دلخواهِ $f(t)^{-1} - f(s)^{-1}$ در U_f را در نظر بگیرید. بنا به فرض چندجمله‌ای f تکین است و $\bar{f}$ در k_v ریشه ندارد، بنابراین با توجه به قسمت ۱ لم ۹.۷ داریم $f(K)^{-1} \subseteq O_v$. در نتیجه $f(t)^{-1}, f(s)^{-1} \in O_v$ و چون O_v یک حلقه است، پس $f(t)^{-1} - f(s)^{-1} \in O_v$. همچنین بنا به قسمت ۳ لم ۹.۷ داریم $m_v \subseteq U_{f,a}$ و از آنجا که $U_{f,a} \subseteq U_f$، نتیجه می‌گیریم که $m_v \subseteq U_f$. □

توجه ۱۲.۷. مجموعه‌ی U_f در زبان حلقه‌ها $\exists$ ـ O_v ـ تعریف‌پذیر است.

اثبات. می‌دانیم که $U_f = \{f(x)^{-1} - f(y)^{-1} : x, y \in K\}$، پس بنا به نحوه‌ی تعریف مجموعه‌ی U_f به سادگی می‌توان دید که فرمول زیر آن را در میدانِ K تعریف می‌کند. به بیان دیگر $\Psi_f(K) = U_f$.

$$\Psi_f(x) = (\exists y, z, y_1, z_1)(x = y_1 - z_1 \wedge y_1 f(y) = 1 \wedge z_1 f(z) = 1)$$

□

تعریف ۱۳.۷. فرض کنید T یک زیرمجموعه از O_v باشد. می‌گوییم مجموعه‌ی T همه‌ی کلاس‌های میدان پیمانه‌ها را قطع می‌کند هرگاه $\bar{T} = k_v$.

لم ۱۴.۷. اگر $U_f, T \subseteq O_v$ به گونه‌ای باشند که $m_v \subseteq U_f$ و T همه‌ی کلاس‌های میدان پیمانه‌ها را قطع می‌کند، آن‌گاه $O_v = U_f + T$.

اثبات. ابتدا نشان می‌دهیم که $U_f + T \subseteq O_v$. عنصر دلخواهِ $u + t$ در $U_f + T$ را در نظر بگیرید. بنا به فرض $U_f, T \subseteq O_v$ پس به سادگی می‌توان نتیجه گرفت که $u + t \in O_v$. حال باید نشان دهیم که $O_v \subseteq U_f + T$. یک عنصر دلخواهِ x در O_v را در نظر بگیرید. بنا به فرض T همه‌ی کلاس‌های میدان پیمانه‌ها را قطع می‌کند، پس $t \in T$ وجود دارد به طوری که $\bar{t} = \bar{x}$. در نتیجه $x \in \bar{t} = t + m_v$ و بنابراین $x \in T + m_v$. توجه کنید که $m_v \subseteq U_f$، بنابراین $x \in T + U_f$. □

توجه ۱۵.۷. فرض کنید زیرمجموعه‌های U_f و T از O_v در شرایط لم ۱۴.۷ صدق کنند و به ترتیب توسط فرمول‌های φ و ψ تعریف شوند. در این صورت، به سادگی می‌توان دید که O_v با فرمول زیر تعریف می‌شود:

$$\rho(x) = (\exists u, t)(x = u + t \wedge \varphi(u) \wedge \psi(t))$$

۲.۲.۷ یافتن f برای تشکیل مجموعه‌ی U_f

در بخش قبلی، مجموعه‌های U_f و T را معرفی کردیم که ویژگی‌های مطلوبی داشتند و بیان کردیم که در صورت وجود این دو مجموعه، می‌توان O_v را به صورت $U_f + T$ نوشت. توجه کنید که برای ساختن مجموعه‌ی U_f باید یک چندجمله‌ای تکینِ f در $O_v[x]$ بیابیم به طوری که $\bar{f}$ در k_v ریشه نداشته باشد و به ازای یک عنصر a در O_v داشته باشیم $f'(a) \notin m_v$.

در این بخش، یک حالت خاص را بررسی می‌کنیم که میدان پیمانه‌ها متناهی است. نشان می‌دهیم که در این حالت، یک چندجمله‌ای تحویل‌ناپذیر، تکین و جدایی‌پذیرِ $\bar{f}$ در $k_v[x]$ وجود دارد به طوری که در k_v ریشه‌ای ندارد. همچنین، یک عنصر $\bar{a} \in k_v$ نیز وجود دارد به طوری که $\bar{f}'(\bar{a}) \neq 0$. توجه داشته باشید که چندجمله‌ای $\bar{f}$ بسیاری از ویژگی‌های مطلوب برای تشکیل مجموعه‌ی U_f مذکور را داراست؛ اما در $k_v[x]$ قرار دارد و نه در $O_v[x]$. نهایتاً برای رسیدن به چندجمله‌ای و عنصر مد نظرمان، $\bar{f}$ و عنصر $\bar{a}$ را بر می‌کشیم و به یک چندجمله‌ای تکینِ f در $O_v[x]$ که $\bar{f}$ در k_v ریشه ندارد و یک عنصر $a \in O_v$ می‌رسیم که شرطِ $f'(a) \notin m_v$ را برآورده می‌کند.

لم ۱۶.۷. فرض کنید $\mathbb{F}_{p^k}$ یک میدان متناهی باشد. در این صورت موارد زیر برقرارند:

الف) برای هر عدد طبیعی m یک چندجمله‌ای f در $\mathbb{F}_p[x]$ از درجه‌ی m وجود دارد به طوری که تکین، تحویل‌ناپذیر و جدایی‌پذیر است و همچنین $f'(0) \neq 0$.

ب) می‌توان چندجمله‌ای f در بالا را به گونه‌ای پیدا کرد که در $\mathbb{F}_{p^k}$ ریشه نداشته باشد.

اثبات. الف) برای اثبات به [۷] مراجعه کنید.

ب) عدد m را به گونه‌ای انتخاب می‌کنیم که $m \nmid k$. بنا به قسمت الف، یک چندجمله‌ای تکین، جدایی‌پذیر و تحویل‌ناپذیر f در $\mathbb{F}_p[x]$ از درجه‌ی m وجود دارد به طوری که $f'(0) \neq 0$. می‌خواهیم نشان دهیم که چندجمله‌ای f در $\mathbb{F}_{p^k}$ ریشه‌ای ندارد. با برهان خلف، فرض کنید یک عنصرِ b در $\mathbb{F}_{p^k}$ وجود داشته باشد به طوری که $f(b) = 0$. حال $\mathbb{F}_p(b)$ یعنی میدان تولید شده توسط $\mathbb{F}_p$ و عنصرِ b را در نظر بگیرید. از آنجا که درجه‌ی چندجمله‌ای مینیمال عنصرِ b برابر با m است، پس $|\mathbb{F}_p(b)| = p^m$. از طرفی، بوضوح $\mathbb{F}_p(b) = \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^k}$ و از این نتیجه می‌شود که $m \mid k$ که این با نحوه‌ی انتخاب m در تناقض است. □

نتیجه ۱۷.۷. فرض کنید k_v یک میدان متناهیِ $\mathbb{F}_{p^k}$ باشد. در این صورت، چندجمله‌ای $\bar{f} \in \mathbb{F}_p[x]$ وجود دارد به طوری که در k_v ریشه‌ای ندارد و تحویل‌ناپذیر، تکین و جدایی‌پذیر است. همچنین، یک عنصرِ $\bar{a}$ در k_v وجود دارد به طوری که $\bar{f}'(\bar{a}) \neq 0$.

۳.۲.۷ یافتن مجموعه‌ی T

در این بخش نیز حالتی را در نظر می‌گیریم که میدان پیمانه‌ها متناهی باشد و یک مجموعه‌ی $T \subseteq O_v$ معرفی می‌کنیم که همه‌ی کلاس‌های میدان پیمانه‌ها را قطع می‌کند.

لم ۱۸.۷. فرض کنید (K, O_v) یک میدان ارزیابی هنسلی با میدان پیمانه‌ی k_v باشد. اگر k_v یک میدان متناهی باشد در این صورت یک مجموعه‌ی $T \subseteq O_v$ وجود دارد به طوری که همه‌ی کلاس‌های میدان پیمانه‌ها را قطع می‌کند.

اثبات. با توجه به اینکه k_v یک میدان متناهی است، پس به صورت یک $\mathbb{F}_q$ است. چندجمله‌ای $g(x) = x^q - x \in \mathbb{Z}[x]$ را در نظر بگیرید. حال قرار دهید $\psi(x) := (g(x) = 0)$. ادعا می‌کنیم که مجموعه‌ی $\psi(K) = \{x \in K : g(x) = 0\}$ همان مجموعه‌ی T است که به دنبال آن هستیم، یعنی اولاً $T \subseteq O_v$ و ثانیاً $\bar{T} = k_v$.

ابتدا می‌خواهیم نشان دهیم که $T \subseteq O_v$. به این منظور، یک عنصر دلخواهِ $x \in T$ را در نظر بگیرید. در این صورت، بنا به تعریف مجموعه‌ی T عنصر x یک عنصر از میدانِ K است که $x^q - x = 0$. ادعا می‌کنیم که $x \in O_v$. با برهان خلف، فرض کنید $x \notin O_v$. پس $v(x) < 0$. با توجه به اینکه گروه ارزیاب، یک گروه مرتب آبلی است، می‌توان نتیجه گرفت که $v(x) \neq qv(x)$. از آنجا که $v(x)$ منفی است، پس بوضوح $qv(x) < v(x) < 0$ و بنابراین داریم $v(x^q - x) = \min\{qv(x), v(x)\} = qv(x) < 0$. از طرفی چون فرض کردیم $x^q - x = 0$، پس $v(x^q - x) = v(0) = \infty$ و این تناقض است.

حال می‌خواهیم ثابت کنیم که $\bar{T} = k_v$. بوضوح $\bar{T} \subseteq k_v$، بنابراین کافی است نشان دهیم که $k_v \subseteq \bar{T}$. به این منظور، عنصر دلخواهِ $\bar{\alpha}$ در k_v را در نظر بگیرید. ابتدا توجه کنید که تصویر چندجمله‌ای $g(x)$ تحت نگاشت کانونی در میدانِ k_v، یعنی $\bar{g}(x)$ برابر است با $\bar{1}x^q - \bar{1}x$. از آنجا که مشخصه‌ی میدانِ $\mathbb{F}_q$ برابر با q است، پس $\bar{g}'(x) = \bar{1}qx^{q-1} - \bar{1} = -\bar{1} \neq \bar{0}$. چون $\bar{\alpha}$ در k_v است، پس بنا به تعریف یک میدان متناهی داریم $\bar{\alpha}^q - \bar{\alpha} = \bar{0}$ به بیان دیگر، $\bar{g}(\bar{\alpha}) = \bar{0}$. از طرفی، نشان دادیم که $\bar{g}' \neq \bar{0}$، پس از هنسلی بودن میدانِ (K, O_v) نتیجه می‌شود که یک عنصرِ a در O_v وجود دارد به طوری که $g(a) = 0$ و $\bar{a} = \bar{\alpha}$. حال با توجه به تعریف مجموعه‌ی T نتیجه می‌گیریم که عنصر a در T قرار دارد، پس بوضوح $\bar{\alpha} = \bar{a} \in \bar{T}$. □

۴.۲.۷ یک $\exists$ ـ $\emptyset$ ـ تعریف از O_v در میدانِ K

در این بخش، بالاخره به کمک آنچه که تا کنون به دست آورده‌ایم، اثبات می‌کنیم که اگر (K, O_v) یک میدان ارزیابی هنسلی باشد که میدان پیمانه‌های آن متناهی است، آنگاه حلقه‌ی ارزیابِ O_v با یک فرمول وجودی و بدون پارامتر در زبان حلقه‌ها تعریف‌پذیر است.

قضیه ۱۹.۷. فرض کنید (K, O_v) یک میدان ارزیابی هنسلی با میدان پیمانه‌هایِ k_v باشد. اگر k_v یک میدان متناهی باشد، آنگاه O_v در زبان حلقه‌ها $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر است.

اثبات. از آنجا که مطابق فرض k_v یک میدان متناهی است، پس به صورت یک $\mathbb{F}_q$ است که در آن $q = p^k$. با توجه به نتیجه‌ی ۱۷.۷، یک چندجمله‌ای تکین، تحویل‌ناپذیر و جدایی‌پذیرِ $\bar{f}$ در $\mathbb{F}_p[x]$ وجود دارد به طوری که در k_v ریشه‌ای ندارد و همچنین، یک عنصر $\bar{a}$ در k_v وجود دارد به طوری که $\bar{f}'(\bar{a}) \neq 0$. حال با برکشیدن چندجمله‌ای $\bar{f}$ و عنصر $\bar{a}$ به یک چندجمله‌ای تکین، تحویل‌ناپذیر و جدایی‌پذیر در $O_v[x]$ و یک عنصرِ a در O_v دست می‌یابیم به طوری که $f'(a) \notin m_v$. توجه کنید که ضرایب چندجمله‌ای $\bar{f}$ در $\mathbb{F}_p$ قرار دارند، بنابراین به صورتِ $\bar{1}, \bar{2}, \cdots, \overline{p-1}$ هستند. در نتیجه پس از برکشیدنِ $\bar{f}$، ضرایب f به صورتِ $1, 2, \cdots, p-1$ می‌شوند و از این رو $f \in \mathbb{Z}[x]$. نهایتاً مجموعه‌ی $U_f = f(K)^{-1} - f(K)^{-1}$ را تشکیل می‌دهیم. دیدیم که U_f با فرمول $\Psi_f = (\exists y, z, y_1, z_1)(x = y_1 - z_1 \wedge y_1 f(y) = 1 \wedge z_1 f(z) = 1)$ تعریف‌پذیر است. پارامترهای فرمول مذکور، همان ضرایب چندجمله‌ای f هستند. اما چون $f \in \mathbb{Z}[x]$، می‌توانیم ترم‌های بسته‌ی نظیر ضرایب f را به جای آن‌ها قرار دهیم. این کار باعث حذف پارامترها و تبدیل فرمولِ Ψ به یک فرمول بدون پارامتر می‌شود.

مجموعه‌ی T را نیز مطابق لم ۱۸.۷ تشکیل می‌دهیم. بوضوح این مجموعه با فرمول بدون پارامتر $\psi(x) = \exists x(x^q - x = 0)$ تعریف‌پذیر است. نهایتاً با توجه به لم ۱۴.۷، داریم $O_v = U_f + T$. از آنجا که هر دو مجموعه‌ی U_f و T تعریف‌پذیر با فرمولی وجودی و بدون پارامتر هستند، پس به تبع آن O_v نیز تعریف‌پذیر با یک فرمول وجودی و بدون پارامتر است. $\square$

۳.۷ مقایسه‌ی اثبات مقاله‌ی اصلی و مقاله‌ی [۷]

در فصل‌های گذشته دیدیم که در میدان ارزیابیِ $(\mathbb{F}_q((t)), \mathbb{F}_q[[t]])$، میدان پیمانه‌ها برابر با $\mathbb{F}_q$ است. از این رو، با استفاده از یک اثبات متفاوت که در بخشِ ۲.۷ شرح دادیم، می‌توان نشان داد که $\mathbb{F}_q[[t]]$ با یک فرمول بدون پارامتر و وجودی در میدانِ $\mathbb{F}_q((t))$ تعریف‌پذیر است. در این بخش، به توضیح اثبات مذکور برای میدان ارزیابیِ $(\mathbb{F}_q((t)), \mathbb{F}_q[[t]])$ پرداخته و آن را با اثباتی که در فصل ۶ مطرح کردیم، مقایسه خواهیم کرد.

اثبات تعریف‌پذیری $\mathbb{F}_q[[t]]$ در $\mathbb{F}_q((t))$ با روش مقاله‌ی [۷]

مطابق بخش ۲.۷ دو زیرمجموعه‌ی $U_f, T \subseteq \mathbb{F}_q[[t]]$ را به صورت زیر تعریف می‌کنیم:

از آنجا که میدان پیمانه‌های $(\mathbb{F}_q((t)), \mathbb{F}_q[[t]])$ متناهی است، پس بنا به لمِ ۱۸.۷ مجموعه‌ی $T = \{x \in \mathbb{F}_q((t)) : x^q - x = 0\}$ یک زیرمجموعه از $\mathbb{F}_q[[t]]$ است که همه‌ی کلاس‌های میدان پیمانه‌ها را قطع می‌کند. توجه کنید که چندجمله‌ای $x^q - x$ در $\mathbb{F}_q[x]$ قرار دارد و مطابق آنچه در لم ۱۸.۶ دیدیم در $\mathbb{F}_q$ در $\mathbb{F}_q((t))$ به طور

نسبی بسته‌ی جبری است، بنابراین اگر چندجمله‌ای $x^q - x$ در $\mathbb{F}_q((t))$ یک ریشه داشته باشد، آن‌گاه آن ریشه متعلق به $\mathbb{F}_q$ خواهد بود. در نتیجه، $T = \{x \in \mathbb{F}_q((t)) : x^q - x = 0\} = \{x \in \mathbb{F}_q : x^q - x = 0\}$. از طرفی، همه‌ی عناصرِ $\mathbb{F}_q$ ریشه‌ی $x^q - x$ هستند و بنابراین $T = \mathbb{F}_q$.

حال می‌خواهیم مجموعه‌ی U_f را تشکیل دهیم. به این منظور بنا به نتیجه‌ی ۱۷.۷ یک چندجمله‌ای تحویل‌ناپذیر و تکینِ $\bar{f}$ در $\mathbb{F}_p[x]$ می‌توانیم بیابیم که دارای ویژگی‌های زیر است:

۱. درجه‌ی $\bar{f}$ برابر با m است به طوری که $m \nmid k$ (اینگونه $\bar{f}$ در میدان پیمانه‌ها ریشه‌ای نخواهد داشت).

۲. یک عنصر $\bar{a}$ در k_v وجود دارد به طوری که $\bar{f}'(\bar{a}) \neq 0$.

حال چندجمله‌ای $\bar{f}$ و عنصرِ $\bar{a}$ را بر می‌کشیم و به یک چندجمله‌ای f در $\mathbb{F}_q[[t]][x]$ و یک عنصرِ a در $\mathbb{F}_q[[t]]$ می‌رسیم به طوری که $\bar{f}$ در میدان پیمانه‌ها، یعنی $\mathbb{F}_q$ ریشه‌ای ندارد و همچنین، a شرطِ $f'(a) \notin m_v$ را برآورده می‌کند. در این صورت، بنا به لمِ ۱۱.۷ مجموعه‌ی $U_f = \{f(x)^{-1} - f(y)^{-1} : x, y \in \mathbb{F}_q((t))\}$ در شرطِ $t\mathbb{F}_q[[t]] \subseteq U_f \subseteq \mathbb{F}_q[[t]]$ صدق می‌کند. نهایتاً از آنجا که U_f و $\mathbb{F}_q$ تعریف‌پذیر هستند و بنا به لم ۱۴.۷، می‌توان $\mathbb{F}_q[[t]]$ را به صورتِ $U_f + \mathbb{F}_q$ نوشت، پس نتیجه می‌شود که $\mathbb{F}_q[[t]]$ تعریف‌پذیر است.

مرور روش مقاله‌ی اصلی

به اثبات مطرح شده در فصل ۶ بر می‌گردیم. در قضیه‌ی ۲۳.۶، یک چندجمله‌ای تحویل‌ناپذیرِ f در $\mathbb{F}_p[x]$ با ویژگی‌های زیر یافتیم:

۱. درجه‌ی f برابر با m است به طوری که $m \nmid k$ (اینگونه این چندجمله‌ای در $\mathbb{F}_q$ نیز تحویل‌ناپذیر باقی می‌ماند).

۲. چندجمله‌ای f در $\mathbb{F}_q$ ریشه ندارد.

۳. یک عنصرِ a در $\mathbb{F}_q$ وجود دارد به طوری که $f'(a) \neq 0$.

سپس، با استفاده از f و a مذکور، مجموعه‌ی $U_{f,a} = \{f(x)^{-1} - f(a)^{-1} : x \in K\}$ را تشکیل دادیم که بنا به قضیه‌ی ۲۳.۶ یک همسایگی باز و کراندار از صفر است. در نهایت مطابق لمِ ۱۴.۶، به صورت زیر عمل کردیم:

۱. از آنجا که $V := \bigcup\{U_{f,a} : a \in \mathbb{F}_q, f'(a) \neq 0\}$ یک همسایگی باز از 0 است، در نتیجه یک عدد صحیحِ n وجود دارد به طوری که $B(n) \subseteq V$. حال یک عددِ m بزرگتر از n در نظر می‌گیریم. در این صورت مجموعه‌ی $W := \{x \in K : x^m \in V\}$ یک مجموعه‌ی کراندار، تعریف‌پذیر و شاملِ $\{x \in K : v(x) = 1\}$ است.

۲. مجموعه‌ی $X := W \cup (W \cup \{0\})$ یک مجموعه‌ی کراندار، تعریف‌پذیر و شاملِ $t\mathbb{F}_q[[t]]$ است.

۳. از آنجا که X یک مجموعه‌ی کراندار است، پس یک عدد صحیح h وجود دارد به طوری که $X \subseteq B(-h)$. مجموعه‌ی $Y := \{x : x^h \in X\} - \{x : x^h \in X\}$ یک مجموعه‌ی کراندار و تعریف‌پذیر است که $t\mathbb{F}_q[[t]] \subseteq Y \subseteq \mathbb{F}_q[[t]]$.

سپس، با توجه به قضیه‌ی ۲۴.۶ می‌توانیم $\mathbb{F}_q[[t]]$ را به صورت مجموع $U_{f,a}$ و $\mathbb{F}_q$ بنویسیم که هردو تعریف‌پذیر هستند و اینگونه تعریف‌پذیری $\mathbb{F}_q[[t]]$ نتیجه می‌شود.

مقایسه دو روش با یکدیگر

همان‌طور که در دو قسمت قبلی دیدیم، اگر چندجمله‌ای f را مطابقِ ۳.۷ انتخاب کنیم و سپس مجموعه‌ی U_f (به جای $U_{f,a}$) را تشکیل دهیم، آنگاه می‌توانیم مستقیماً نتیجه بگیریم که U_f شاملِ $t\mathbb{F}_q[[t]]$ است و در $\mathbb{F}_q[[t]]$ قرار دارد. در نتیجه، مراحل فوق برای رسیدن از مجموعه‌ی تعریف‌پذیر $U_{f,a}$ به یک مجموعه‌ی مطلوبِ Y از میان برداشته می‌شوند.

*** خلاصه‌ی فصل:**

در این فصل دو نتیجه مرتبط به مقاله‌ی اصلی را شرح دادیم. نتیجه اول بیان می‌کند که اگر گروه ارزیاب یک میدان ارزیابی هنسلی گسسته باشد، آنگاه حلقه‌ی ارزیاب آن با یک فرمول وجودی و تنها با یک پارامتر در زبان حلقه‌ها تعریف می‌شود. روش اثبات این قضیه به صورت زیر است:

۱. اگر $\gamma \in \Gamma$ یک عنصر p ـ بخش‌پذیر نباشد، آنگاه مجموعه‌ی $\{x \in K : pv(x) + \gamma > 0\}$ با فرمولِ $\varphi(x) = \exists y(y^p - y^{p-1} = \epsilon x^p)$ تعریف‌پذیر است.

۲. اثبات کردیم که اگر γ را کوچکترین عنصر مثبت در گروه ارزیاب در نظر بگیریم، آنگاه مجموعه‌ی $\{x \in K : pv(x) + \gamma > 0\}$ برابر با O_v می‌شود، پس بنا به مرحله‌ی ۱ تعریف‌پذیر می‌شود.

نتیجه دوم این بود که اگر (K, O_v) یک میدان ارزیابی هنسلی باشد که میدان پیمانه‌های آن متناهی است، آنگاه O_v در زبان حلقه‌ها $\exists$ ـ $\emptyset$ ـ تعریف‌پذیر است. روش اثبات این قضیه به شرح زیر است:

۱. بنا به یک قضیه در مقاله‌ی [۷] به ازای هر عدد اولِ p و عدد طبیعیِ m یک چندجمله‌ای تکین و تحویل‌ناپذیرِ $\bar{f}$ از درجه‌ی m در $\mathbb{F}_p[x]$ وجود دارد به طوری که $\bar{f}'(0) \neq 0$. از آنجا که k_v یک میدان متناهی است، پس به صورت یک $\mathbb{F}_q$ است که در آن $q = p^k$. حال یک عدد طبیعیِ m را با این ویژگی که k را عاد نکند در نظر می‌گیریم. بنا به قضیه‌ی مذکور، یک چندجمله‌ای تکین، تحویل‌ناپذیر و جدایی‌پذیرِ $\bar{f}$

از درجه‌ی m در $\mathbb{F}_p[x]$ وجود دارد به طوری که به ازای یک عنصرِ $\bar{a}$ در $\mathbb{F}_q$ داریم $\bar{f}'(\bar{a}) \neq 0$. به علاوه، با انتخاب درجه‌ی f، یعنی m به صورت فوق نتیجه می‌شود که $\bar{f}$ در $\mathbb{F}_q$ ریشه‌ای ندارد. با روش برکشیدن از چندجمله‌ای $\bar{f} \in \mathbb{F}_p[x]$ به چندجمله‌ای $f \in \mathbb{Z}[x]$ می‌رسیم و با استفاده از آن مجموعه‌ی $U_f = f(K)^{-1} - f(K)^{-1}$ را تشکیل می‌دهیم. این مجموعه دارای ویژگی $m_v \subseteq U_f \subseteq O_v$ است و با فرمولِ $\Psi_f = (\exists y, z, y_1, z_1)(x = y_1 - z_1 \wedge y_1 f(y) = 1 \wedge z_1 f(z) = 1)$ تعریف می‌شود. نهایتاً از آنجا که f متعلق به $\mathbb{Z}[x]$ است، پس با جایگزین کردن ضرایب این چندجمله‌ای با ترم‌های بسته‌ی نظیرشان به یک فرمول بدون پارامتر برای تعریفِ U_f خواهیم رسید.

۲. مجموعه‌ی $T = \{x \in K : x^q - x = 0\}$ را در نظر بگیرید. این مجموعه همه‌ی کلاس‌های میدان پیمانه‌ها را قطع می‌کند، یعنی $\bar{T} = k_v$.

۳. نهایتاً چون $O_v = U_f + T$ و U_f و T دو مجموعه‌ی تعریف‌پذیر با فرمولی وجودی و بدون پارامتر هستند، پس O_v نیز با فرمول بدون پارامتر و وجودی زیر تعریف‌پذیر است:

$$\rho(x) = (\exists u, t)(x = u + t \wedge \varphi(u) \wedge t^q - t = 0).$$

واژه‌نامه‌ی فارسی به انگلیسی

الف

ایده‌آل ماکسیمال .... maximal ideal
ارزیابی .... valuation
ارشمیدسی .... archimedean

ب

به طور موضعی معادل .... locally equivalent
بستار جبری .... algebraic closure
به طور نسبی بسته‌ی جبری .... relatively algebraically closed
بسته‌ی جدایی‌پذیر .... separably closed
بخش‌پذیر .... divisible

ت

تحویل‌ناپذیر .... irreducible
تعریف‌پذیر .... definable
توسیع جبری .... algebraic extension
توسیع میدان .... field extension
توسیع جدایی‌پذیر .... separable extension
تکین .... monic
توپولوژی هاسدورف .... Hausdorff topology

ح

حلقه‌ی موضعی .... local ring

حلقه‌ی هنسلی .... henselian ring
حالت نرمال نقیض .... negation normal form
حد معکوس .... inverse limit

ع

عنصر متعالی .... transcendental element
عنصر وارون‌پذیر .... invertible element
عنصر پوچ‌توان .... nilpotent element
عنصر خنثی .... neutral element

ف

فیلتر فرشه .... Frechet filter
فرمول موضعی .... local formula
فرمول وجودی .... existential formula

ق

قدرمطلق .... absolute value

ک

کراندار .... bounded
کراندار دور از صفر .... bounded away from zero

گ

گسسته .... discrete
گروه مرتب آبلی .... ordered abelian group
گروه ارزیاب .... valued group

م

میدان کامل .... perfect field
میدان توپولوژیک .... topological field
مجموعه‌ی تقریباً ارزیاب .... almost valuation set

میدان متناهی .... finite field
میدان شکافنده .... splitting field
میدان ارزیابی .... valued field
میدان پیمانه‌ها .... residue field

ن

نگاشت پیوسته .... continuous mapping

نمایه

$A+B := \{x+y : x\in A, y\in B\}$، ۵۲
$A\cdot B := \{x\cdot y : x\in A, y\in B\}$، ۵۲
$A^c := \{x : x\notin A\}$، ۸۳
A^{-1} : مجموعه‌ی متشکل از وارون همه‌ی عناصر متعلق به A، ۶۲
$K[x]_1^n$: مجموعه‌ی تمام چندجمله‌ای‌های تکین با حداکثر درجه‌ی n در $K[x]$ ، ۹۱
$K^{\mathbb{N}}$: مجموعه‌ی دنباله‌های نامتناهی از عناصر میدان K ، ۸۵
K^{cl} : بستار جبریِ میدان K، ۶
$L_{ring} := \{+,-,\cdot,0,1\}$، ۹۸
Vـ توپولوژی، ۵۲
$\mathbb{F}_p := \{0,1,\cdots,p-1\}$، ۱۲
$\mathbb{F}_p(t) := \{\frac{f(t)}{g(t)} : f(t), g(t)\in \mathbb{F}_p[t]\}$، ۱۱
$\prod_{p\in E} p$: حاصل‌ضرب همه‌ی عناصر موجود در مجموعه‌ی E، ۱۰۷
$yO := \{yx : x\in O\}$، ۶۹
$\mathbb{R}^+$: مجموعه‌ی اعداد حقیقی مثبت، ۵۷
$\hat{\mathbb{Z}}_p$: حلقه‌ی p ـ ادیک ، ۳۲
$\hat{\mathbb{Q}}_p$: میدان p ـ ادیک ، ۳۲
$L\setminus K := \{x\in L : x\notin K\}$ ، ۶
عنصر جبری، ۶
عنصر پوچ‌توان، ۶۸
فیلتر ω ـ کامل ، ۸۳
میدان پیمانه‌های نگاشت ارزیابی ، ۴۳
چندجمله‌ای جدایی‌پذیر، ۹
ایده‌آل ارزیاب، ۸۶
ایده‌آل ارزیاب هنسلی، ۹۰
ایده‌آل ماکسیمال نگاشت ارزیابی، ۴۲
بسته‌ی جبری، ۶
بسته‌ی جدایی‌پذیر ، ۹
به طور موضعی معادل، ۸۲
ترتیب ارشمیدسی، ۵۹
ترم‌های بسته، ۲
تعمیم محک آیزنشتاین، ۱۱
توسیع جدایی‌پذیر، ۹
توسیع متناهی، ۶
توسیع میدانی ، ۶
توپولوژی مینیمال، ۸۷
توپولوژی هاسدورف، ۵۲
حلقه‌ی ارزیاب، ۴۲، ۴۳
حلقه‌ی موضعی، ۲۰
حلقه‌ی نُرم‌دار، ۲۴
حلقه‌ی کامل، ۲۴
حلقه‌ی موضعی هنسلی، ۲۱
خوش‌ترتیبی، ۴۵

دنباله‌ی کوشی، ۲۴
زبان مرتبه اول، ۱
سری‌های لوران، ۲۹ ، ۴۸
سری‌های هان، ۴۵
عنصر nـ بخش‌پذیر، ۱۱۴
عنصر خنثی، ۶۸
عنصر متعالی، ۶

فرمول در حالت نرمال نقیض، ۸۱
فرمول موضعی، ۸۱
فیلتر، ۸۳
فیلتر اصلی، ۸۳
فیلتر غیراصلی، ۸۳
فیلتر فرشه، ۸۳
قدرمطلق، ۵۷
قدرمطلق p ـ ادیک، ۳۰
قدرمطلق ارشمیدسی، ۵۷
قدرمطلق غیر ارشمیدسی، ۵۷
لم هنسل، ۲۶
مجموعه‌ی تعریف‌پذیر، ۵
مجموعه‌ی تقریباً ارزیاب، ۶۶
مجموعه‌ی تقریباً بسته، ۶۶
مجموعه‌ی کراندار، ۶۲
مقادیر ساده‌ی یک چندجمله‌ای، ۹۲
میدان t ـ هنسلی ، ۸۹
میدان توپولوژیک، ۵۰
میدان کامل، ۱۵
نُرم غیر ارشمیدسی، ۲۴
نگاشت ارزیابی، ۴۰
نگاشت ارزیابی p ـ ادیک، ۳۰

چندجمله‌ای مینیمال، ۶
گروه آبلی گسسته، ۱۱۴
گروه محدب، ۵۹
گروه مرتب، ۵۹

منابع

[1] Anscombe, W and Koenigsmann, J. “an existential $\varnothing$-definition of $\mathbb{F}_q[[t]]$ in $\mathbb{F}_q((t))$”. *The Journal of Symbolic Logic*, 79(4):1336–1343, 2014.

[2] Ax, J. “on the undecidability of power series fields”. *Proceedings of the American Mathematical Society*, 16(846):846, 1965.

[3] Cluckers, R, Derakhshan, J, Leenknegt, E, and Macintyre, A. “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.

[4] Delon, F and Farré, R. “some model theory for almost real closed fields”. *The Journal of Symbolic Logic*, 61(4):1121–1152, 1996.

[5] Dummit, D and Foote, R. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[6] Engler, A and Prestel, A. *Valued fields*. Springer Science & Business Media, 2005.

[7] Fehm, A. “existential $\varnothing$-definability of henselian valuation rings”. *The Journal of Symbolic Logic*, 80(1):301–307, 2015.

[8] Fehm, A and Jahnke, F. “on the quantifier complexity of definable canonical henselian valuations”. *Mathematical Logic Quarterly*, 61(4-5):347–361, 2015.

[9] Gouvêa, F and Gouvêa, F. *p-adic Numbers*. Springer, 1997.

[10] Hong, J. “definable non-divisible henselian valuations”. *Bulletin of the London Mathematical Society*, 46(1):14–18, 2014.

[11] Howie, J and Howie, J. *Fields and Galois theory*. Springer, 2006.

[12] Jahnke, F and Koenigsmann, J. “definable henselian valuations”. *The Journal of Symbolic Logic*, 80(1):85–99, 2015.

[13] Jahnke, F and Koenigsmann, J. “uniformly defining p-henselian valuations”. *Annals of Pure and Applied Logic*, 166(7-8):741–754, 2015.

[14] Koenigsman, J. *“Elementary characterization of fields by their absolute Galois group”*. PhD thesis, Citeseer, 1998.

[15] Krapp, L, Kuhlmann, S, and Link, M. “definability of henselian valuations by conditions on the value group”. *The Journal of Symbolic Logic*, pages 1–19, 2022.

[16] Marker, D. *Model theory: an introduction*, volume 217. Springer Science & Business Media, 2006.

[17] Marker, D. “model theory of valued fields”. *Online lecture notes*, 2018.

[18] Prestel, A. “algebraic number fields elementarily determined by their absolute galois group”. *Israel Journal of Mathematics*, 73(2):199–205, 1991.

[19] Prestel, A. “definable henselian valuation rings”. *The Journal of Symbolic Logic*, 80(4):1260–1267, 2015.

[20] Shafarevich, I and Reid, M. *Basic algebraic geometry*, volume 2. Springer, 1994.

[21] van den Dries, L, Koenigsmann, J, Macpherson, D, Pillay, A, Toffalori, C, and Wilkie, A. *“Model theory in algebra, analysis and arithmetic”*. Springer, 2012.

[22] Ziegler, M and Prestel, A. “model theoretic methods in the theory of topological fields.”. *Journal für die Reine und Angewandte Mathematik*, 1978.

An existential $\emptyset$-definition of $\mathbb{F}_q[[t]]$ in $\mathbb{F}_q((t))$

Zahra Yadegari

z.yadegari@math.iut.ac.ir

September , 2023

Master of Science Thesis(in Farsi)

Department of Mathematical Sciences
Isfahan University of Technology, Isfahan 84156-83111, Iran

Supervisor: Dr. Mohsen Khani, mohsen.khani@iut.ac.ir

2000 MSC: 03C60

Keywods: Definablity, Valuation ring, Valued fields, Henselian, V- topology, t- Henselian

---

Abstract:
This thesis is based on the following two papers:

1. Will Anscombe and Jochen Koenigsmann. An existential-$\emptyset$-definition of $\mathbb{F}_q[[t]]$ in $\mathbb{F}_q((t))$, The Journal of Symbolic Logic, 79(4):1336–1343, 2014.

2. Alexander Prestel and Martin Ziegler, Model-theoretic methods in the theory of topological fields. Journal für die Reine und Angewandte Mathematik, vol. 299 (1978), no. 300, pp. 318–341.

We aim to show that the valuation ring $\mathbb{F}_q[[t]]$ in the valued field $\mathbb{F}_q((t))$ is existentially definable in the language of rings without any parameters. Here $\mathbb{F}_q((t))$ is the field consisting of series of the form $\{\sum_{i=-n}^{\infty} a_i t^i : a_i \in \mathbb{F}_q, n \in \mathbb{N}\}$ and $\mathbb{F}_q[[t]]$ is the subring $\{\sum_{i=0}^{\infty} a_i t^i : a_i \in \mathbb{F}_q\}$. The proof of the mentioned theorem is in the first reference above, but it relies heavily on a theorem in the second reference above, which asserts that in a topological Henselian field which is not separably closed, there exists a bounded neighborhood of zero that is definable by an existential formula. We will demonstrate that the field $\mathbb{F}_q((t))$ meets the requirements of the latter theorem and hence has a bounded neighborhood of zero definable by an existential formula with parameters from $\mathbb{F}_q$. Next, we use a trick to transform this neighborhood into a definable set Y that contains $t\mathbb{F}_q[[t]]$ and is contained in the valuation ring $\mathbb{F}_q[[t]]$. Now it is easy to verify that $\mathbb{F}_q[[t]]$ is equal to $\mathbb{F}_q + Y$. Then, due to the definability of the set Y and the definability of $\mathbb{F}_q$ as the set of roots of the polynomial $x^q - x$, we conclude that $\mathbb{F}_q[[t]]$ is definable in the language of rings, but at this stage, with parameters from $\mathbb{F}_q$. In the final step of the proof, we find a way to get rid of the parameters of the mentioned definition.

Isfahan University of Technology

Department of Mathematical Sciences

Thesis Submitted for the Award of Master of Science in Mathematics

An existential $\emptyset$-definition of $\mathbb{F}_q[[t]]$ in $\mathbb{F}_q((t))$

Zahra Yadegari

Supervisor: Dr. Mohsen Khani

September 2023