پردیس علوم
دانشکده ریاضی، آمار و علوم کامپیوتر

گروه‌های صوری لوبین ـ تیت و نظریه میدان رده‌ای موضعی

نگارنده:

محمد مسعود احمدی

استاد راهنما:

دکتر امیر قادرمرزی

پایان‌نامه برای دریافت درجه کارشناسی
در رشته ریاضیات و کاربردها

تیر ماه ۱۴۰۱

چکیده

نظریهٔ میدان رده‌ای موضعی شاخه‌ای از نظریه اعداد است که به توصیف و رده‌بندی توسیع‌های گالوای میدان‌های موضعی می‌پردازد. از جمله نتایج اولیه و مهم این شاخه قانون تقابل موضعی است که شرح آن انگیزه اصلی نگارش این پایان‌نامه است. به این منظور پس از بیان برخی تعاریف و قضایا درباره دامنه‌های ددکیند، میدان‌های موضعی و توسیع‌های جبری آن‌ها و همچنین بیان تعاریف و نتایج اولیه درباره گروه‌های صوری، به تعریف گروه‌های صوری لوبین‌ـتیت پرداخته و به کمک آن‌ها وجود، یکتایی و برخی از خواص نگاشت تقابل موضعی را اثبات می‌کنیم.

سپاسگزاری

از استاد راهنمای این پایان‌نامه، جناب آقای دکتر امیر قادرمرزی، بابت راهنمایی‌هایشان سپاس‌گزارم. ایشان همواره با روی گشاده، پاسخ‌گوی سوالات من بودند و با صبر و حوصله‌ای مثال‌زدنی بی‌نظمی‌های مرا تحمل می‌کردند. از دوستانم بابت حضور دلگرم‌کننده‌شان در طول دوره تحصیلم در دانشگاه تهران ممنونم. از دوست خوبم، آقای ادیب عبداللهی، که مشورت با او به من در نگارش این پایان‌نامه کمک شایانی کرد، سپاس‌گزارم. از خانواده‌ام که در تمام مراحل زندگی پشتیبان و حامی من بودند، بی‌نهایت سپاس‌گزارم.

پیشگفتار

هدف نظریه میدان رده‌ای شناخت و طبقه‌بندی توسیع‌های گالوای میدان‌های سرتاسری یا موضعی است. ریاضی‌دانانی چون کرونکر، وبر، هیلبرت، تاکاگی، آرتین، هسه و دیگران در حدود سال‌های بین ۱۸۵۰ تا ۱۹۳۰ میلادی توانستند توسیع‌های آبلی میدان‌های موضعی و سرتاسری را به طور کامل شناسایی و توصیف کنند. آن‌چه که امروز نظریهٔ میدان رده‌ای خوانده می‌شود، نتیجهٔ تلاش‌های آنان است. از طرف دیگر تلاش‌ها برای توصیف توسیع‌های غیرآبلی تا به امروز در قالب برنامه لنگلندز ادامه داشته است. یکی از دستاوردهای نظریهٔ میدان رده‌ای قانون‌های تقابل اند که به ما اجازه می‌دهد تا تمامی توسیع‌های متناهی آبلی یک میدان سرتاسری یا موضعی را شناسایی کنیم.

در این پایان‌نامه، به اثبات قضیه تقابل موضعی خواهیم پرداخت. این قضیه تمامی توسیع‌های آبلی میدان‌های موضعی را توصیف کرده و ساختار جبری آن‌ها را به طور کامل مشخص می‌کند. هر چند تاکنون روش‌های متنوعی برای اثبات این قضیه به کار گرفته شده اند، روشی که ما در این پایان‌نامه مورد بررسی و مطالعه قرار داده‌ایم، استفاده از نظریهٔ گروه‌های صوری است. به زبان ساده، گروه‌های صوری را می‌توان قواعد گروهی بدون گروه دانست. ایده درخشان استفاده از گروه‌های صوری در نظریهٔ میدان رده‌ای را نخستین بار جاناتان لوبین و جان تیت در مقاله تاثیرگذارشان [۴] مطرح کردند.

در فصل اول به بیان برخی مقدمات جبری که در ادامه مورد نیاز واقع خواهند شد می‌پردازیم. عمده مطالب این فصل برگرفته از [۱] است. در فصل دوم میدان اعداد $p-$ای و تعمیم آن‌ها که میدان‌های موضعی خوانده می‌شوند، را معرفی می‌کنیم. فصل سوم این پایان‌نامه به گروه‌های صوری اختصاص دارد. در بخش اول این فصل و پیش از بیان تعریف گروه‌های صوری، کاربردی از گروه‌های صوری در حساب خم‌های بیضوی را بیان می‌کنیم به این امید که به آشکار شدن انگیزه‌های در پس تعاریف و نتایج بخش دوم فصل، کمک کند. در نهایت فصل چهارم و پایانی این متن به اثبات قضیهٔ تقابل موضعی به کمک گروه‌های صوری لوبین‌ـتیت اختصاص دارد.

فهرست مطالب

فصل ۱

مقدمات جبری

در این فصل مقدمات جبری مورد نیاز برای ورود به نظریهٔ میدان رده‌ای را در حد نیاز بیان می‌کنیم. تعاریف و نتایج موجود در بخش های اول، دوم و زیربخش اول از بخش سوم به صورت بسیار کامل‌تر در کتاب‌های درسی استاندارد جبر جابه‌جایی یافت می‌شوند. همچنین برای مطالب مربوط به دامنه‌های ددکیند و نظریه انشعاب می‌توانید به کتاب‌های درسی استاندارد نظریهٔ جبری اعداد مانند [۱] یا [۶] رجوع کنید.

۱.۱ ایده‌آل‌های کسری

تعریف ۱.۱. *یک دامنهٔ صحیح یک حلقهٔ جابه‌جایی یک‌دار فاقد مقسوم علیه صفر است.*

در این فصل R را یک دامنهٔ صحیح در نظر می‌گیریم و میدان کسرهای آن را با K نمایش می‌دهیم. می‌توان K را به عنوان یک $R-$مدول در نظر گرفت. در این صورت اگر I و J، $R-$زیرمدول‌های K باشند، می‌توان $R-$زیرمدول‌های زیر را تعریف کرد:

$$I+J=\{x+y \mid x\in I, y\in J\}$$

$$IJ=\{xy \mid x\in I, y\in J\}$$

$$I^{-1}=\{x\in K \mid xI\subset R\}$$

$$R(I)=\{x\in K \mid xI\subset I\}$$

هر ایده‌آل حلقه R را می‌توان به عنوان یک $R-$زیرمدول K در نظر گرفت. با این تعبیر، می‌توان مفهوم ایده‌آل را به صورت زیر تعمیم داد.

تعریف ۲.۱. *به فرض I یک $R-$زیرمدول ناصفر K باشد. I را یک ایده‌آل کسری R می‌نامیم اگر عضو ناصفری مانند a در K باشد به طوری که $aI \subset R$. در این‌جا همواره a را می‌توان به گونه‌ای انتخاب کرد که $a \in R$.*

گزاره ۳.۱. *اگر I و J دو ایده‌آل کسری حلقه R باشند، آن‌گاه $I+J$، $I \cap J$، IJ، I^{-1} و $R(I)$ نیز ایده‌آل‌های کسری R اند.*

اثبات. لم ۲، صفحه ۲ از [۱] را ببینید. ■

تعریف ۴.۱. *ایده‌آل کسری I وارون‌پذیر است اگر $II^{-1} = R$.*

تعریف ۵.۱. *یک مدول را نوتری می‌نامیم اگر هر زیرمدول آن متناهیاً تولید شده باشد.*

برای حلقه‌های نوتری می‌توان توصیف دیگری از کسری بودن یک ایده‌آل ارائه داد:

گزاره ۶.۱. *فرض کنید R نوتری باشد. $R-$زیرمدول ناصفر I از K یک ایده‌آل کسری است اگر و تنها اگر متناهیاً تولید شده باشد.*

اثبات. اگر R نوتری باشد، آن‌گاه چون برای $a \in R$ ناصفر، داریم $I \cong aI$، پس I متناهیاً تولید شده است. برعکس؛ به فرض I متناهیاً تولید شده باشد و $\{v_1, v_2, ..., v_k\} \subset K$ یک مجموعه مولد برای آن باشد. اگر $a \in R$ را مضرب مشترکی از مخرج‌های v_iها در نظر بگیریم، آن‌گاه $aI \subset R$ و حکم ثابت می‌شود. ■

۲.۱ حلقه‌های ارزهٔ گسسته

در این‌جا منظور از K^* گروه ضربی میدان K است. $\mathbb{Z}$ نیز گروه اعداد صحیح تحت عمل جمع است.

تعریف ۷.۱. *نگاشت $v : K \to \mathbb{Z} \cup \infty$ را یک ارزهٔ گسسته می‌نامیم اگر*

۱) *$v \restriction_{K^*} : K^* \to \mathbb{Z}$ یک هم‌ریختی گروهی پوشا باشد،*

۲) $v(0) = \infty$،

۳) $v(x+y) \geq inf\{v(x), v(y)\}$.

اگر v یک ارزهٔ گسسته روی میدان K باشد و ρ عددی دلخواه در بازه $(0,1)$ باشد، آن‌گاه نگاشت $|x|_v = \rho^{v(x)}$ در تعریف یک نُرم روی K صدق می‌کند:

۱) $|x|_v = 0 \iff x = 0$،

۲) $|xy|_v = |x|_v|y|_v$،

۳) $|x+y|_v \leq \max\{|x|_v, |y|_v\}$.

این نُرم یک متریک و در نتیجه آن یک توپولوژی روی K القا می‌کند. می‌توان نشان داد که توپولوژی حاصل از $|.|_v$ مستقل از انتخاب ρ است؛ یعنی اگر $\rho_1, \rho_2 \in (0,1)$، آن‌گاه نرم‌های $|x|_1 = \rho_1^{v(x)}$ و $|x|_2 = \rho_2^{v(x)}$ معادل اند. به علاوه از شرط سوم تعریف ارزهٔ گسسته نتیجه می‌شود که این نرم در نامساوی مثلث قوی صدق می‌کند، یعنی $|x+y|_v \leq max\{|x|_v, |y|_v\}$. نرم‌هایی که نامساوی مثلث قوی برایشان صادق است را ناارشمیدسی می‌نامیم. در نتیجه تمام نرم‌هایی که به کمک یک ارزهٔ گسسته تعریف می‌شوند، ناارشمیدسی اند.

لم ۸.۱. *مجموعه $R_v = \{x \in K \mid v(x) \geq 0\}$ با اعمال جمع و ضرب روی K یک حلقه است. این حلقه را حلقهٔ ارزهٔ v می‌نامیم.*

لم ۹.۱. *مجموعه $\mathfrak{p}_v = \{x \in K \mid v(x) > 0\}$ یک ایده‌آل از حلقه ارزهٔ v است که آن را ایده‌آل ارزهٔ v می‌نامیم.*

به سادگی می‌توان نشان داد که R_v یک دامنه صحیح است که میدان کسرهای آن K است. همچنین $\mathfrak{p}_v$ نیز ایده‌آل ماکسیمالی از R_v است.

تعریف ۱۰.۱. *زیرگروه $U_v = \{x \in K \mid v(x) = 0\}$ از K^* را گروه یکه‌های R_v می‌نامیم.*

U_v دقیقا شامل اعضایی از R_v است که دارای وارون ضربی در R_v اند. همچنین بنا به تعریف یک نگاشت ارزه می‌دانیم که می‌توان عضوی از K مانند π یافت به طوری که $v(\pi) = 1$. چنین عضوی را یک یکنواخت‌ساز یا به طور معادل یک عضو اول می‌نامیم. در نتیجه برای یک یکنواخت‌ساز مانند π، می‌توان هر $a \in K$ را به طور یکتا به شکل $a = u\pi^n$ نمایش داد که در آن $u \in U_v$ و $n = v(a)$.

گزاره ۱۱.۱. *R_v یک دامنهٔ ایده‌آل اصلی (به اختصار PID) است.*

اثبات. به فرض I یک ایده‌آل کسری R_v باشد. تعریف می‌کنیم $v(I) = inf\{v(x) \mid x \in I\}$. به وضوح $v(I) \in \mathbb{Z} \cup \infty \cup -\infty$. اما طبق تعریف ایده‌آل کسری $a \in K$ای هست به طوری که aI یک ایده‌آل صحیح R_v باشد. در نتیجه $v(I) = v(aI) - v(a) \geq -v(a)$. پس بنا به اصل خوش‌ترتیبی، می‌توان $b \in I$ را چنان یافت که $v(I) = v(b)$. حال داریم:

$$bR_v \subset I \subset \{x \in K \mid v(x) \geq v(I)\} = \{x \in K \mid v(x) \geq v(b)\} = bR_v.$$

و لذا نتیجه می‌شود که $I = bR_v$.

■

نتیجه ۱۲.۱. $I = \mathfrak{p}_v^{v(I)}$.

از نتیجه فوق درمی‌یابیم که $\mathfrak{p}_v$ تنها ایده‌آل اول ناصفر و در نتیجه تنها ایده‌آل ماکسیمال حلقه R_v است.

تعریف ۱۳.۱. *یک حلقه ارزهٔ گسسته عبارت است از یک دامنهٔ ایده‌آل صحیح که دارای یک و فقط یک ایده‌آل اول ناصفر باشد.*

بدین ترتیب مشاهده می‌شود که حلقه ارزهٔ یک نگاشت ارزهٔ گسسته، یک حلقه ارزهٔ گسسته است. حال ادعا می‌کنیم که عکس این موضوع نیز برقرار است:

گزاره ۱۴.۱. *حلقهٔ ارزهٔ گسسته R یک حلقه ارزه R_v برای نگاشت ارزهٔ یکتای v است که روی میدان کسرهای R تعریف می‌شود.*

اثبات. به فرض $\mathfrak{p} = \pi R$ ایده‌آل اول یکتای R باشد. چون R یک دامنهٔ ایده‌آل اصلی است پس یک دامنه تجزیهٔ یکتا نیز است. لذا برای هر $x \in R$ داریم $x = u\pi^n$ که u عنصری وارون‌پذیر از R و n عدی صحیح و نامنفی است. در نتیجه هر $x \in K$ را نیز می‌توان به شکل حاصل‌ضرب یک عضو وارون‌پذیر از R و توانی π نوشت با این تفاوت که این بار توان می‌تواند مقادیر منفی را نیز اتخاذ کند. پس برای هر $x \in K$، می‌توان $u \in R$ وارون‌پذیر و $n \in \mathbb{Z}$یافت که $x = u\pi^n$. اگر تعریف کنیم $v(x) = n$، آن‌گاه یک نگاشت ارزهٔ گسسته خواهد بود که $R = R_v$. ■

برای بیان توصیف دیگری از حلقه‌های ارزهٔ گسسته به تعریف زیر نیاز است:

تعریف ۱۵.۱. *حلقه R بسته صحیح است اگر هر عضو میدان کسرهای آن که ریشه یک چندجمله‌ای تکین با ضرایب در R باشد، عضوی از R باشد.*

گزاره ۱۶.۱. *دامنهٔ صحیح R یک حلقه ارزهٔ گسسته است اگر و تنها اگر نوتری و بسته صحیح بوده و یک و فقط یک ایده‌آل اول ناصفر داشته باشد.*

اثبات. به [۱] نگاه کنید. ■

۳.۱ دامنه‌های ددکیند

دامنه‌های ددکیند از مهم‌ترین اشیا مورد مطالعه در نظریهٔ جبری اعداد اند و از خواص و ویژگی‌های آن‌ها در ادامه به طور وسیعی استفاده خواهد شد. به طور کلی دامنه‌های ددکیند را می‌توان تعمیمی از دامنه‌های تجزیه یکتا به شمار آورد با این تفاوت که به جای آن که هر عضو آن تجزیه‌ای یکتا به حاصل ضرب عوامل اول داشته باشد، هر ایده‌آل آن تجزیه‌ای یکتا به حاصل‌ضرب ایده‌آل‌های اول دارد. دامنه‌های ددکیند را می‌توان به صورت موضعی نیز توصیف کرد اما پیش از این کار لازم است تا برخی تعاریف و نتایج مربوط موضعی‌سازی حلقه‌ها بیان شوند.

۱.۳.۱ موضعی‌سازی

موضعی‌سازی را می‌توان به معنای تشکیل کسر در نظر گرفت. تعریف زیر این موضوع را دقیق‌تر مشخص می‌کند:

تعریف ۱.۱۷. *به فرض T زیرمجموعه‌ای از R باشد که نسبت به ضرب بسته است. موضعی‌سازی R در $R \setminus T$ عبارت است از:*

$$RT^{-1} = \{\frac{a}{b} \in K \mid a \in R, b \in R \setminus T\}.$$

همچنین به سادگی مشاهده می‌شود که RT^{-1} زیرحلقه‌ای از K است.

فرض کنید R یک دامنهٔ صحیح باشد. اگر در تعریف فوق قرار دهیم، $T = \{0\}$، آن‌گاه $RT^{-1} = K$. در نتیجه بزرگترین موضعی‌سازی ممکن همان میدان‌کسرهای حلقه R است. مهم‌ترین مثال از موضعی‌سازی زمانی است که $T = R \setminus \mathfrak{p}$ که در آن $\mathfrak{p}$ ایده‌آل اولی از R باشد. در این صورت به جای RT^{-1} از نمادگذاری $R_{\mathfrak{p}}$ استفاده می‌کنیم و $R_{\mathfrak{p}}$ را موضعی سازی R در $\mathfrak{p}$ می‌نامیم.

گزاره ۱.۱۸. *ایده‌آل‌های اول $\mathfrak{Q}$ از RT^{-1} با ایده‌آل‌های اول $\mathfrak{q} \subset R - T$ از R در تناظر یک به یک اند.*

اثبات. نگاشت‌های

$$\mathfrak{q} \mapsto \mathfrak{q}T^{-1} \quad \text{و} \quad \mathfrak{Q} \mapsto \mathfrak{Q} \cap R$$

را در نظر بگیرید. این دو نگاشت وارون یک دیگر اند. ■

تعریف ۱.۱۹. *حلقهٔ R را یک حلقهٔ موضعی می‌نامیم اگر دارای ایده‌آل ماکسیمال یکتا باشد.*

نخستین مثال حلقه‌های موضعی میدان‌ها اند. به علاوه می‌توان گفت که حلقه‌های ارزهٔ گسسته، حلقه‌هایی موضعی اند که هر ایده‌آل آن‌ها اصلی است.

برای ایده‌آل اول $\mathfrak{p}$، $R_{\mathfrak{p}}$ یک حلقهٔ موضعی است که ایده‌آل ماکسیمال یکتای آن $m_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$ است. همچنین اگر $\mathfrak{p}$ در R ماکسیمال باشد، آن‌گاه

$$A/\mathfrak{p}^n \cong A_{\mathfrak{p}}/m_{\mathfrak{p}}^n \quad \forall n \geq 1.$$

در ادامه خواهیم دید که هر ایده‌آل اول در یک دامنهٔ ددکیند، ماکسیمال نیز است و در نتیجه یک‌ریختی فوق برای دامنه‌های ددکیند همواره برقرار است.

۲.۳.۱ دامنه‌های ددکیند

گزاره ۲۰.۱. *شروط زیر برای دامنهٔ صحیح R معادل اند. اگر R در (یکی از) این شروط صدق کند، یک دامنهٔ ددکیند نامیده می‌شود:*

۱) *R نوتری و بسته صحیح است و ایده‌آل‌های اول ناصفر آن ماکسیمال اند.*

۲) *R نوتری است و برای هر ایده‌آل اول ناصفر $\mathfrak{p}$، $R_{\mathfrak{p}}$ یک حلقهٔ ارزهٔ گسسته است.*

۳) *هر ایده‌آل کسری R وارون پذیر است.*

اثبات. صفحه ۶، گزاره ۱ از [۱] را ببینید. ■

شرط دوم گزاره فوق نتیجه می‌دهد که موضعی‌سازی یک دامنه ددکیند در هر ایده‌آل اول ناصفرش، برابر با حلقه ارزهٔ یک نگاشت ارزهٔ گسسته است. این نگاشت ارزه را با $v_{\mathfrak{p}}$ نمایش می‌دهیم.

شرط سوم از گزاره فوق بیان می‌کند که مجموعهٔ ایده‌آل‌های کسری R تحت عمل ضرب تشکیل یک گروه آبلی می‌دهد. این گروه را با $\mathcal{P}(R)$ نشان می‌دهیم. به علاوه می‌توان نشان داد که ایده‌آل‌های اول R مولد این گروه اند و هر عضو این گروه نمایشی یکتا به صورت حاصل‌ضرب ایده‌آل‌های اول R دارد.

گزاره ۲۱.۱. *$\mathcal{P}(R)$ یک گروه آبلی است که روی ایده‌آل‌های اول R آزاد است. به علاوه نمایش هر ایده‌آل کسری I در این گروه به شکل زیر است:*

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}.$$

اثبات. صفحه ۸، گزاره ۲ از [۱] را ببینید. ■

۴.۱ تجزیه ایده‌آل‌ها در توسیع‌ها

در بخش قبل دیدیم که در یک دامنهٔ ددکیند هر ایده‌آل‌های کسری را می‌توان به طور یکتا به حاصل‌ضرب ایده‌آل‌های اول تجزیه کرد. اکنون به بررسی نحوه تغییر تجزیه یک ایده‌آل در اثر گسترش یافتن دامنهٔ ددکیند می‌پردازیم. به عنوان مثال ایده‌آل‌های $2\mathbb{Z}$ و $3\mathbb{Z}$ هر دو در حلقه اعداد صحیح که یک دامنهٔ ددکیند است، اول اند. اما اگر ایده‌آل‌های $2\mathbb{Z}[i]$ و $3\mathbb{Z}[i]$ را در حلقه $\mathbb{Z}[i]$ (که در ادامه نشان می‌دهیم یک دامنهٔ ددکیند است) در نظر بگیریم، می‌بینیم که $2\mathbb{Z}[i]$ دیگر اول نیست زیرا $2\mathbb{Z}[i] =< 1+i >^2$ در حالی که $3\mathbb{Z}[i]$ همچنان اول می‌ماند.

فرض کنید که R یک دامنهٔ ددکیند و K میدان کسرهای آن باشد. L را یک توسیع میدانی متناهی K بگیرید بستار صحیح R در L را حلقه اعداد صحیح L می‌نامیم و آن را با S نمایش می‌دهیم. از آن‌جایی که هدف این پایان‌نامه مطالعه گروه‌های گالوای رده‌ای از توسیع‌ها است، توسیع میدانی L/K را جدایی‌پذیر در نظر می‌گیریم.

گزاره ۱.۲۲. *S یک دامنه ددکیند است. به علاوه برای هر ایده‌آل اول ناصفر $\mathfrak{P}$ در S ایده‌آل اول ناصفری مانند $\mathfrak{p}$ در R هست به طوری که $\mathfrak{P} \subset \mathfrak{p}S$ و برای هر ایده‌آل اول ناصفر $\mathfrak{P}$ در R، ایده‌آل اول ناصفری مانند $\mathfrak{P}$ در S هست به طوری که $\mathfrak{p} = \mathfrak{P} \cap R$.*

اثبات. صفحه ۱۳، گزاره ۱ از [۱] را ببینید. ■

فرض کنید $\mathfrak{P}$ یک ایده‌آل اول S باشد. تعریف کنید $\mathfrak{p} = \mathfrak{P} \cap R$. در این صورت میدان رده‌ای مانده‌های ایده‌آل $\mathfrak{p}$ (یعنی $k_1 = R/\mathfrak{p}$) به طور طبیعی در میدان رده‌ای مانده‌های $\mathfrak{P}$ (یعنی $k_2 = S/\mathfrak{P}$) می‌نشیند.

تعریف ۱.۲۳. *$f(\mathfrak{P}/\mathfrak{p}) = [k_2 : k_1]$ را درجه رده‌ای مانده‌ها می‌نامیم.*

تعریف ۱.۲۴. *$e(\mathfrak{P}/\mathfrak{p}) = v_{\mathfrak{P}}(\mathfrak{p}S) = \inf\{v_{\mathfrak{P}}(x) \mid x \in \mathfrak{p}S\}$ را شاخص انشعاب می‌نامیم.*

اگر $\bar{K}$ میدان حاصل از کامل‌سازی K نسبت نُرم $|\cdot|_{v_{\mathfrak{p}}}$ باشد و $\bar{\mathfrak{p}}$ نیز ایده‌آل اول و ماکسیمال یکتای عناصر با ارزهٔ مثبت در $\bar{R}$ باشد، آن‌گاه:

گزاره ۱.۲۵.

$$f(\bar{\mathfrak{p}}/\mathfrak{p}) = 1,$$
$$e(\bar{\mathfrak{p}}/\mathfrak{p}) = 1.$$

اثبات. صفحه ۱۸، گزاره ۲ از [۱] را ببینید. ■

اگر $R_1 \subset R_2 \subset R_3$ سه دامنهٔ ددکیند باشند و برای $i = 1, 2, 3$ ایده‌آل $\mathfrak{p}_i$ در R_i اول باشد، آن‌گاه:

گزاره ۱.۲۶.

$$f(\mathfrak{p}_3/\mathfrak{p}_1) = f(\mathfrak{p}_3/\mathfrak{p}_2)f(\mathfrak{p}_2/\mathfrak{p}_1),$$
$$e(\mathfrak{p}_3/\mathfrak{p}_1) = e(\mathfrak{p}_3/\mathfrak{p}_2)e(\mathfrak{p}_2/\mathfrak{p}_1).$$

اثبات. صفحه ۱۸، گزاره ۱ از [۱] را ببینید. ■

نتیجه ۲۷.۱. *با توجه به گزاره‌های ۲۵.۱ . و ۲۶.۱ . می‌توان نتیجه گرفت که برای محاسبه درجه رده‌ای مانده‌ها یا شاخص انشعاب ایده‌آل $\mathfrak{P}$ روی ایده‌آل $\mathfrak{p}$ می‌توان R و S را به وسیله موضعی‌سازی در این ایده‌آل‌ها به حلقه‌های ارزهٔ گسسته تبدیل کرد و سپس به وسیله نُرم به دست آمده از تابع ارزه، K و L را کامل کرد و در نهایت درجه رده‌ای مانده‌ها یا شاخص انشعاب $\mathfrak{P}$ روی $\mathfrak{p}$ را محاسبه کرد.*

بنا بر نتیجه فوق، از این پس فرض می‌کنیم که R یک حلقهٔ ارزهٔ گسسته باشد. همچنین با جایگزینی کامل‌سازی K نسبت به نرم $|\cdot|_{v_\mathfrak{p}}$ به جای K می‌توان فرض کرد که میدان K کامل است.

ادعا می‌کنیم که اگر L یک توسیع میدانی K از درجه n باشد و S نیز بستار صحیح R در L باشد، آن‌گاه نُرم $|\cdot|_{v_\mathfrak{p}}$ به طور یکتا به L توسعه می‌یابد و در نتیجه آن L نیز کامل بوده و S حلقهٔ ارزهٔ آن است. نخست نشان می‌دهیم که L کامل است.

لم ۲۸.۱. *اگر K یک میدان باشد که نسبت به نُرم $|\cdot|$ کامل است و V یک $K-$فضای برداری نُرم‌دار از بعد متناهی باشد، آن‌گاه برای هر پایه $\{v_1, \cdots, v_n\}$ از V، نُرم داده شده روی V با نُرم زیر معادل است:*

$$\|x_1v_1 + \cdots + x_nv_n\| \coloneqq \max\{|x_1|, \cdots, |x_n|\}.$$

در نتیجه V نیز کامل است و یک‌ریختی

$$K^n \to V, \quad (x_1, \cdots, x_n) \mapsto x_1v_1 + \cdots + x_nv_n$$

یک همسان‌ریختی است.

اثبات. صفحه ۱۳۲، گزاره ۹.۴. از [۷] را ببینید. ■

از آن‌جایی که میدان L را می‌توان به عنوان یک $K-$فضای برداری از بعد n در نظر گرفت، لم فوق نشان می‌دهد که نُرم $|\cdot|_{v_\mathfrak{p}}$ تنها به یک ردهٔ هم‌ارزی از نُرم‌ها روی L توسعه می‌یابد و L نسبت به توپولوژی حاصل از این نُرم‌ها کامل است. گزارهٔ بعد نشان می‌دهد که این ردهٔ هم‌ارزی از نُرم‌ها تنها یک عضو دارد.

گزاره ۲۹.۱. *اگر میدان K نسبت به نُرم $|\cdot|_K$ کامل باشد و L/K یک توسیع جبری از درجه n باشد، آن‌گاه نُرم $|\cdot|_K$ به طور یکتا به نُرم*

$$|\cdot|_L : \alpha \mapsto \sqrt[n]{|N_{L/K}(\alpha)|_K}$$

روی L توسعه می‌یابد.

اثبات. به [۷] صفحه ۱۳۱، قضیه ۸.۴. نگاه کنید. ■

نتیجه ۳۰.۱. *اگر R یک حلقهٔ ارزهٔ گسسته و K کامل باشد، آن‌گاه S نیز یک حلقهٔ ارزهٔ گسسته و L نیز کامل است.*

از این پس $\mathfrak{p}$ را ایده‌آل اول یکتای R و $\mathfrak{P}$ را ایده‌آل اول یکتای S در نظر بگیرید. با توجه به یکتایی این ایده‌آل‌ها تنها یک درجه رده‌ای مانده‌ها و یک شاخص انشعاب برای توسیع L/K قابل تعریف است که آن‌ها را به ترتیب با $f = f(L/K)$ و $e = e(L/K)$ نمایش می‌دهیم.

گزاره بعد رابطه بین درجه رده‌ای مانده‌ها، شاخص انشعاب و درجه توسیع را بیان می‌کند.

گزاره ۳۱.۱.

$$e(L/K)f(L/K) = [L : K].$$

اثبات. از تعریف شاخص انشعاب نتیجه می‌شود که $\mathfrak{p}S = \mathfrak{P}^e$. در نتیجه k_K-فضای برداری $S/\mathfrak{p}S$ به شکل جمع مستقیم $S/\mathfrak{P} \oplus \mathfrak{P}/\mathfrak{P}^2 \oplus \cdots \oplus \mathfrak{P}^{e-1}/\mathfrak{P}^e$ قابل نمایش است. همه این جمع‌وندها با یک‌دیگر یک‌ریخت بوده و همگی با k_L یک‌ریخت اند. بنا به تعریف درجه رده‌ای مانده‌ها، هر کدام از این جمع‌وندها یک k_K-فضای برداری fـبعدی اند. در نتیجه $S/\mathfrak{p}S$ یک فضای برداری ef بعدی روی k_K است. از طرف دیگر S یک $R-$مدول آزاد از بعد $[L : K]$ است. در نتیجه $S/\mathfrak{p}S$ یک فضای برداری روی $k_K = R/\mathfrak{p}$ از بعد $[L : K]$ است. بنا بر این، $[L : K] = ef$. ■

گروه یکه‌های حلقه‌های R و S را به ترتیب با U_K و U_L نمایش می‌دهیم. $j : K^* \to L^*$ نیز نشاندن کانونی اعضای ناصفر K در میدان L است.

نتیجه ۳۲.۱. *نمودار زیر جابه‌جایی و دارای سطرهای دقیق است.*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U_K & \hookrightarrow & K^* & \xrightarrow{v_{\mathfrak{p}_K}} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle e} & & \\
0 & \longrightarrow & U_L & \hookrightarrow & L^* & \xrightarrow{v_{\mathfrak{p}_L}} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle f} & & \\
0 & \longrightarrow & U_K & \hookrightarrow & K^* & \xrightarrow[v_{\mathfrak{p}_K}]{} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

۱.۴.۱ توسیع‌های غیرمنشعب

تعریف ۳۳.۱. *توسیع میدانی L روی K را غیرمنشعب می‌نامیم اگر $e(L/K) = 1$ و توسیع k_L/k_K جدایی‌پذیر باشد. به بیان دیگر L روی K غیرمنشعب است اگر هر یکنواخت‌ساز K، در L نیز یکنواخت‌ساز باشد.*

از تعریف فوق نتیجه می‌شود که در یک توسیع غیرمنشعب، $[k_L : k_K] = f = [L : K]$.
همهٔ میدان‌های مورد مطالعه ما در ادامه این متن (یعنی میدان‌های اعداد $p-$ای و میدان توابع گویا روی یک میدان متناهی) دارای میدان رده‌ای مانده‌های متناهی اند و می‌دانیم که میدان‌های متناهی دارای توسیع یکتا از درجه مشخص اند. در نتیجه می‌توان حدس زد که دست کم در موارد با میدان رده‌ای مانده‌های متناهی، مشخص کردن k_L/k_K، توسیع غیرمنشعب L/K را نیز به صورت یکتا مشخص کند. گزاره زیر در این باره است.

گزاره ۳۴.۱. *فرض کنید F یک توسیع جبری میدان K و k_F میدان رده‌ای مانده‌های آن باشد (می‌توان فرض کرد که F بستار جبری K باشد). در این صورت نگاشت $L \mapsto k_L$ یک تناظر یک‌به‌یک میان توسیع‌های غیرمنشعب متناهی از K که مشمول در F باشند و توسیع‌های متناهی از k_K که مشمول در k_F باشند، برقرار می‌سازد.*

$$\{L \subset F \mid L/K \text{ متناهی و غیرمنشعب}\} \longleftrightarrow \{l \subset k_F \mid l/k_K \text{ متناهی و جدایی‌پذیر}\}$$

به علاوه برای توسیع‌های غیرمنشعب و متناهی L_1 و L_2 از K درون F داریم:

$$L_1 \subset L_2 \iff k_{L_1} \subset k_{L_2}.$$

هم‌چنین توسیع L/K گالوا است اگر و تنها اگر k_L/k_K گالوا باشد که در این صورت $Gal(L/K)$ به صورت کانونی با $Gal(k_L/k_K)$ یک‌ریخت می‌شود.

اثبات. در اینجا تنها وجود یک‌ریختی کانونی میان گروه‌های گالوا را اثبات می‌کنیم. برای مشاهده اثبات کامل گزاره به [۶] صفحه ۱۲۷، گزاره ۵۰.۷. نگاه کنید.
با فرض گالوا بودن توسیع‌های L/K و k_L/k_K و با توجه به نتیجه ۱.۳۰. برای هر $\gamma \in Gal(L/K)$ داریم:

$$v_{\mathfrak{p}_L}(x) = \frac{1}{f} v_{\mathfrak{p}_K}(N_{L/K}(x)) = v_{\mathfrak{p}_L}(\gamma(x)).$$

در نتیجه عمل گروه گالوا روی L، حلقه ارزهٔ S و ایده‌آل ماکسیمال $\mathfrak{p}_L$ را ثابت نگه می‌دارد. لذا نگاشت $\gamma \mapsto \bar{\gamma}$ که در آن $\bar{\gamma} : x \mod \mathfrak{p}_L \mapsto \gamma(x) \mod \mathfrak{p}_L$، همان یک‌ریختی کانونی مورد نظر است. ■

نتیجه ۳۵.۱. *به ازای هر عدد صحیح مثبت n، یک و تنها یک توسیع غیر منشعب از درجه n روی K (در حد $K-$یک‌ریختی) وجود دارد.*

نتیجه ۳۶.۱. *به فرض L/K یک توسیع جبری دلخواه باشد. در این صورت زیرمیدان L_0 از L شامل K وجود دارد به طوری که L_0/K غیرمنشعب است و هر توسیع غیرمنشعب روی K، زیرمیدانی از L_0 است. L_0 را توسیع غیرمنشعب ماکسیمال K در L می‌نامیم.*

مثال ۳۷.۱. *به فرض k_K، میدان رده‌ای مانده‌های میدان K، میدانی متناهی از مشخصه $p \neq 0$ و دارای q عضو باشد. می‌دانیم که توسیع یکتای k/k_K از درجه n وجود دارد به طوری که k میدان شکافنده چندجمله‌ای $X^{q^n} - X$ روی k_K است. از نظریه گالوا می‌دانیم که $Gal(k/k_K)$ گروه دوری از مرتبه n و مولد آن نگاشت فروبنیوس $\sigma : x \mapsto x^q$ است. حال بنا به تناظر بیان شده در گزاره ۱.۳۲ . نتیجه می‌شود که برای هر n، توسیع نامنشعب K_n از K از درجه n وجود دارد که (در حد $K-$یک‌ریختی) یکتا است و میدان رده‌ای مانده‌های آن نیز k است. به علاوه K_n میدان شکافنده چندجمله‌ای $X^{q^n} - X$ روی K بوده و گروه گالوای آن گروه دوری از مرتبه n است. مولد این گروه نیز نگاشتی است که تحت یک‌ریختی کانونی توصیف شده در اثبات گزاره ۱.۳۲ .، به نگاشت فروبنیوس مولد $Gal(k/k_K)$ تصویر شود؛ به عبارت دقیق‌تر $\sigma \in Gal(K_n/K)$ مولد $Gal(K_n/K)$ است اگر و تنها اگر برای هر x در حلقه ارزهٔ K_n داشته باشیم $\sigma(x) \equiv x^q \mod \mathfrak{p}_{K_n}$.*

۲.۴.۱ توسیع‌های کاملا منشعب

تعریف ۳۸.۱. *توسیع میدانی L روی K را کاملا منشعب می‌نامیم اگر $f(L/K) = 1$.*

در ادامه شرطی لازم و کافی برای کاملا منشعب بودن یک توسیع بیان خواهیم کرد که به ما اجازه می‌دهد توسیع‌های کاملا منشعب از درجات دلخواه روی میدان K بسازیم.

تعریف ۳۹.۱. *چندجمله‌ای $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$ را یک چندجمله‌ای آیزنشتاین می‌نامیم هر گاه*

$$v_{\mathfrak{p}}(a_n) = 0, \quad v_{\mathfrak{p}}(a_0) = 1, \quad v_{\mathfrak{p}}(a_i) \geq 1 \quad i = 1, 2, \cdots n-1.$$

مشاهده می‌شود که تعریف فوق همان تعریف متداول چندجمله‌ای آیزنشتاین برای ایده‌آل اول $\mathfrak{p}$ است.

گزاره ۴۰.۱. *چندجمله‌ای آیزنشتاین $f(X)$ تحویل‌ناپذیر است. اگر Π یک ریشه $f(X)$ باشد، آن‌گاه توسیع $L = K(\Pi)$ یک توسیع کاملا منشعب است. به علاوه، Π یک یکنواخت‌ساز L است.*

برعکس، اگر توسیع L/K کاملا منشعب و Π یک یکنواخت‌ساز L باشد، آن‌گاه چندجمله‌ای مینیمال Π روی K آیزنشتاین است و $L = K(\Pi)$. همچنین $S = R[\Pi]$.

اثبات. صفحه ۲۳، قضیه ۱ از [۱] را ببینید. ■

گزاره فوق بیانگر تناظر یک‌به‌یک میان توسیع‌های آیزنشتاین و توسیع‌های کاملا منشعب است.

نتیجه ۴۱.۱. *به ازای هر عدد صحیح مثبت n،توسیع کاملا منشعبی از درجه n روی K وجود دارد.*

اثبات. به فرض $c \in K$ یک یک‌نواخت‌ساز K باشد؛ یعنی $v_{\mathfrak{p}}(c) = 1$. در این صورت چندجمله‌ای $f(X) = X^n - cX - c$ یک چندجمله‌ای آیزنشتاین است و بنا به گزاره ۱.۳۸. با اضافه کردن یک ریشه $f(X)$ به K توسیع کاملا منشعب مورد نظر به دست می‌آید. ■

همان‌طور که مشاهده می‌شود فرایند ساخت یک توسیع کاملا منشعب از درجه n به انتخاب یک‌نواخت‌ساز c وابسته است. در نتیجه برخلاف توسیع‌های غیرمنشعب، درباره یکتایی توسیع‌های کاملا منشعب از درجه n نمی‌توان حکمی صادر کرد.

فصل ۲

میدان‌های موضعی

در این فصل میدان‌های موضعی را معرفی کرده و خواهیم دید که نتایج بیان شده در بخش ۴ فصل قبل برای زیرمجموعه بزرگی از میدان‌های موضعی صادق اند. در فصل آینده به کمک این نتایج قاعده تقابل موضعی را بیان و اثبات خواهیم کرد. برای معرفی مفهوم میدان موضعی، ابتدا مهم‌ترین مثال از آن، یعنی میدان اعداد $p-$ای را یررسی خواهیم کرد.

۱.۲ میدان اعداد $p-$ای

اعداد $p-$ای را نخستین بار کرت هنسل، ریاضی‌دان آلمانی، به منظور استفاده از ابزار قدرتمند سری‌های توانی در نظریهٔ اعداد معرفی کرد. در زیربخش اول تلاش خواهیم کرد تا ایدهٔ درخشان هنسل را شرح دهیم و پس از آن در زیربخش دوم به تعریف رسمی اعداد $p-$ای خواهیم پرداخت.

۱.۱.۲ ایدهٔ هنسل

$\mathbb{C}[X]$ را حلقهٔ چندجمله‌ای‌ها با ضرایب مختلط در نظر می‌گیریم. میدان کسرهای این حلقه $\mathbb{C}(X)$ یعنی میدان توابع گویا با ضرایب مختلط است. مجموعه ایده‌آل‌های اول حلقه $\mathbb{C}[X]$ را با $Spec(\mathbb{C}[X])$ نمایش می‌دهیم و به وضوح داریم:

$$Spec(\mathbb{C}[X]) = \{\langle X-\alpha\rangle \mid \alpha \in \mathbb{C}\}$$

. از آنالیز مختلط می‌دانیم که هر تابع تمام‌ریخت را می‌توان به صورت یک سری توانی حول یک نقطه در دامنه آن نوشت. به طور خاص برای هر $\alpha \in \mathbb{C}$ می‌توان هر چندجمله‌ای مانند $f(X) \in \mathbb{C}[X]$ از درجه n را به صورت

$$f(X) = a_0 + a_1(X-\alpha) + a_2(X-\alpha)^2 + \cdots + a_n(X-\alpha)^n$$

نوشت که در آن به ازای $i = 0, 1, \cdots, n$، $a_i = \frac{f^{(i)}(\alpha)}{i!}$.

حلقه $\mathbb{C}[X]$ از بسیاری از جهات مشابه حلقه اعداد صحیح است. پیش‌رفت‌های نظریهٔ توابع مختلط ریاضی‌دانان آن زمان را بر آن داشته بود تا به دنبال راهی برای استفاده از ابزارهای قدرتمند نظریه توابع مختلط مانند سری‌های توانی در نظریهٔ اعداد باشند. از جمله آنان لئوپلد کرونکر، استاد راهنمای هنسل، بود که تلاش داشت تا نظریهٔ توابع مختلط و نظریهٔ اعداد را به یک نظریهٔ واحد تبدیل کند. هنسل با الهام از تلاش‌های استاد راهنمای خود، به این نتیجه رسید که می‌توان همانند چندجمله‌ای‌های با ضرایب مختلط، هر عدد صحیح را به صورت یک سری توانی (متناهی) حول هر کدام از اعضای $Spec(\mathbb{Z})$ نوشت. در واقع چون $Spec(\mathbb{Z})$ همان مجموعه ایده‌آل‌های اول $\mathbb{Z}$ و در تناظر یک‌به‌یک با مجموعه اعداد صحیح اول است، هنسل هر عدد صحیح را به عنوان یک تابع تعریف شده روی مجموعه اعداد اول در نظر گرفت. به طور دقیق‌تر برای هر عدد صحیح a و هر عدد اول p تعریف کرد: $a(p) := a \mod p$. این دیدگاه به وی اجازه داد تا هر عدد صحیح را به صورت یک سری توانی (متناهی) حول یک عدد اول بنویسد. به عنوان مثال به ازای $a = 320$ و $p = 7$ داریم:

$$320 = 5 + 3 \times 7 + 6 \times 7^2.$$

البته در نظریه توابع مختلط، تنها چندجمله‌ای‌ها نیستند که نمایشی به صورت سری توانی دارند؛ بلکه هر تابع تمام‌ریخت را می‌توان به صورت یک سری توانی نمایش داد. هنسل، حلقه اعداد صحیح $p-$ای را در تناظر با حلقه توابع تمام‌ریخت تعریف کرد. هم‌چنین هر تابع برخه‌ریخت نیز نمایشی به صورت یک سری توانی با تعدادی متناهی جمله با اندیس منفی (سری لوران) دارد. در تناظر با میدان توابع برخه‌ریخت، هنسل میدان اعداد $p-$ای را معرفی کرد، که در زیربخش بعدی به آن می‌پردازیم.

۲.۱.۲ اعداد $p-$ای

عدد اول p را در مجموعه اعداد صحیح در نظر بگیرید. برای هر $a \in \mathbb{Z}$ ناصفر، بزرگترین توانی از p که a را می‌شمارد، با $v_p(a)$ نمایش می‌دهیم. به علاوه قرار می‌دهیم $v_p(0) = \infty$. می‌توان دامنهٔ تعریف v_p را به اعداد گویا نیز گسترش داد. به فرض $a \in \mathbb{Q}$ در این صورت a را می‌توان به شکل $a = \frac{s}{r}p^m$ نمایش داد که در آن $r, s \in \mathbb{Z}$ و $(rs, p) = 1$. عدد m در این نمایش تنها به a وابسته است. پس قرار می‌دهیم $v_p(a) = m$. این نحوه تعریف v_p با تعریفی که روی اعداد صحیح ارائه شد، سازگار است؛ کافی است قرار دهید $s = a$ و $r = 1$.

به راحتی مشاهده می‌شود که v_p در تعریف ۱.۷. و نامساوی مثلث قوی صدق می‌کند و یک ارزهٔ گسسته ناارشمیدسی است. مطابق مطالب فصل ۱، این ارزه گسسته به ما اجازه می‌دهد تا یک رده از نُرم‌های ناارشمیدسی هم‌ارز را روی $\mathbb{Q}$ تعریف کنیم.

تعریف ۱.۲. *تابع $|\cdot|_p : \mathbb{Q} \to \mathbb{R}^+$ با ضابطه $|x|_p = p^{-v_p(x)}$ یک نُرم روی اعداد گویا تعریف می‌کند که آن را نُرم $p-$ای می‌نامیم.*

هر سری توانی حول p در توپولوژی حاصل از این نُرم، کوشی است. در نتیجه با اضافه کردن حد دنباله‌های کوشی به $\mathbb{Q}$ (نسبت به توپولوژی القا شده از نُرم $p-$ای)، فضای توپولوژیکی به دست می‌آید که هر عضو آن نمایشی (یکتا) به صورت سری لوران دارد. این فضای توپولوژیک که از لحاظ جبری نیز یک میدان است، میدان اعداد $p-$ای نامیده می‌شود. در ادامه به توصیف دقیق‌تر این میدان می‌پردازیم.

تعریف ۲.۲. *میدان F نسبت به نُرم $|\cdot|$ کامل خوانده می‌شود هرگاه برای هر دنباله کوشی نسبت به این نُرم مانند $\{a_n\}_{n\in\mathbb{N}}$، عضوی مانند $a \in F$ باشد به طوری a_n به a همگرا شود؛ یعنی*

$$\lim_{n\to\infty} |a_n - a| = 0.$$

تعریف ۳.۲. *میدان F با نُرم $|\cdot|$ روی آن را در نظر بگیرید. R را حلقهٔ همه دنباله‌های کوشی نسبت به نُرم $|\cdot|$ روی F در نظر بگیرید. در این صورت زیرمجموعه $\mathfrak{m}$ از R شامل همه دنباله‌های همگرا به صفر در R یک ایده‌آل ماکسیمال R است. در این صورت*

$$\hat{F} := R/\mathfrak{m}$$

یک میدان است که آن را کامل‌سازی میدان F نسبت به نُرم $|\cdot|$ می‌نامیم.

مثال ۴.۲. *کامل‌سازی میدان $\mathbb{Q}$ نسبت به نُرم قدر مطلق، میدان اعداد حقیقی است.*

مثال ۵.۲. *کامل‌سازی میدان $\mathbb{Q}(i)$ نسبت به نُرم $|a+bi| = \sqrt{a^2+b^2}$، میدان اعداد مختلط است.*

میدان F به طور طبیعی در $\hat{F}$ می‌نشیند؛ کافی است هر $a \in F$ را به دنباله ثابت $(a, a, a, \cdots)$ در $\hat{F}$ تصویر کنیم.

تعریف ۶.۲. *به ازای عدد اول p، کامل‌سازی میدان اعداد گویا نسبت به نُرم $p-$ای را میدان اعداد $p-$ای می‌نامیم و آن را با $\mathbb{Q}_p$ نمایش می‌دهیم.*

نرم قدر مطلق متداول روی $\mathbb{Q}$ را با $|\cdot|_\infty$ نمایش می‌دهیم. در نتیجه مثال ۴.۲. بیان می‌کند که $\mathbb{Q}_\infty$ همان $\mathbb{R}$ است. به علاوه قضیه‌ای از استروسکی بیان می‌کند که قدر مطلق و نرم‌های $p-$ای تنها نُرم‌های ممکن روی اعداد گویا هستند.

قضیه ۷.۲. *فرض کنید $|\cdot|$ یک نُرم روی $\mathbb{Q}$ باشد. اگر $|\cdot|$ ارشمیدسی باشد، آن‌گاه با $|\cdot|_\infty$ هم‌ارز است و اگر نا‌ارشمیدسی باشد، آن‌گاه به ازای یک و تنها یک عدد اول p، با $|\cdot|_p$ هم‌ارز خواهد بود.*

اثبات. به [۶] صفحه ۱۱۰، قضیه ۱۲.۷. نگاه کنید. ■

تعریف ۸.۲.

$$\mathbb{Z}_{(p)} \coloneqq \{x \in \mathbb{Q} \mid v_p(x) \geq 0\} = \{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z}, p \nmid b\}.$$

مجموعه فوق را می‌توان متناظر با مجموعه توابع تمام‌ریخت در نظریهٔ توابع مختلط دانست.

تعریف ۹.۲. *بستار توپولوژیک $\mathbb{Z}$ نسبت به نُرم $p-$ای را در $\mathbb{Q}_p$، حلقه اعداد صحیح $p-$ای می‌نامیم و آن را با $\mathbb{Z}_p$ نمایش می‌دهیم.*

در واقع $\mathbb{Z}_p$ از افزودن حد دنباله‌های کوشی به $\mathbb{Z}$ نسبت به نُرم $p-$ای حاصل می‌شود. به فرض $\{a_n\}_{n\in\mathbb{N}}$ یک دنباله کوشی در $\mathbb{Z}$ باشد. در این صورت برای هر $\epsilon > 0$ می‌توان $N \in \mathbb{N}$ یافت به طوری که به ازای $n > N$ داشته باشیم $|a_n - a_{n+1}|_p < \epsilon$. به فرض $M \in \mathbb{N}$ بزرگترین عدد طبیعی باشد که $\epsilon \leq \frac{1}{M}$. در این صورت داریم

$$\begin{aligned}
|a_n - a_{n+1}|_p < \epsilon &\implies p^{-v_p(a_n - a_{n+1})} < \epsilon \\
&\implies -v_p(a_n - a_{n+1}) < \log_p \epsilon \\
&\implies v_p(a_n - a_{n+1}) > \log_p \frac{1}{\epsilon} \\
&\implies v_p(a_n - a_{n+1}) > \log_p M \\
&\implies v_p(a_n - a_{n+1}) > \lfloor \log_p M \rfloor \\
&\implies p^{\lfloor \log_p M \rfloor} \mid a_n - a_{n+1} \\
&\implies a_n \equiv a_{n+1} \mod p^{\lfloor \log_p M \rfloor}
\end{aligned}$$

بدین‌ترتیب با کاهش ϵ و در نتیجه آن افزایش M، جملات دنباله از جایی به بعد، به پیمانه توان بزرگتری از p هم‌نهشت می‌شوند. با در نظر گرفتن نمایش جملات دنباله به صورت سری توانی حول p، نتیجه می‌شود که هر دنباله کوشی در $\mathbb{Z}$ زیردنباله‌ای دارد که آن زیردنباله خود دنباله مجموعات جزئی یک سری توانی حول p است. گزاره زیر بیان دقیق‌تر این مشاهده است.

گزاره ۱۰.۲. *$\mathfrak{R}$ را یک دستگاه کامل مانده‌ها به پیمانه p بگیرید به طوری که $0 \in \mathfrak{R}$. در این صورت هر عضو $\mathbb{Z}_p$ را می‌توان به صورت یک سری توانی حول p با ضرایب در $\mathfrak{R}$ نمایش داد.*

گزاره فوق را می‌توان به عنوان حالت خاصی از گزاره زیر در نظر گرفت.

گزاره ۱۱.۲. *$\mathfrak{R}$ را یک دستگاه کامل مانده‌ها به پیمانه p بگیرید به طوری که $0 \in \mathfrak{R}$. در این صورت هر $x \in \mathbb{Q}_p$ را می‌توان به صورت یکتا به شکل*

$$x = p^m(a_0 + a_1 p + a_2 p^2 + \cdots)$$

نمایش داد که در آن $a_i \in \mathfrak{R}$، $a_0 \neq 0$ و $m \in \mathbb{Z}$.

اثبات. برای اثبات این گزاره برای هر میدان کامل ناارشمیدسی به [۷] نگاه کنید. ■

گزاره فوق تناظر میان توابع برخه‌ریخت و اعداد $p-$ای را که هنسل به دنبال آن بود، برقرار می‌سازد. قضیه زیر یکی از کاربردهای اعداد $p-$ای در نظریه اعداد را نشان می‌دهد.

قضیه ۱۲.۲. (هسه - مینکوفسکی) *به فرض $F(X_1, X_2, \cdots, X_n)$ یک فرم مربعی (چندجمله‌ای همگن درجه ۲) با ضرایب در $\mathbb{Q}$ باشد. معادله*

$$F(X_1, X_2, \cdots, X_n) = 0$$

در $\mathbb{Q}$ جواب نابدیهی دارد اگر و تنها اگر برای هر $p \leq \infty$، در $\mathbb{Q}_p$ جواب نابدیهی داشته باشد.

اثبات. به [۹] صفحه ۴۱، قضیه ۸ نگاه کنید. ■

۲.۲ میدان‌های موضعی

پیش از آن که تعریف یک میدان موضعی را ارائه کنیم، ابتدا خواصی از اعداد $p-$ای را بررسی می‌کنیم که در ادامه الهام‌بخش صورت‌بندی ریاضی مفهوم «موضعی بودن» خواهند شد.

ابتدا مشاهده می‌کنیم که با توجه به پیوستگی توابع $|\cdot|_p$ و v_p نسبت به توپولوژی $p-$ای، دامنه تعریف این توابع به طور طبیعی به $\mathbb{Q}_p$ گسترش می‌یابد؛ اگر $a \in \mathbb{Q}_p$ و $\{a_n\}_{n\in\mathbb{N}}$ دنباله‌ای کوشی در $\mathbb{Q}$ باشد که به a همگرا است، آن‌گاه

$$|a|_p = \lim_{n\to\infty} |a_n|_p \quad \text{و} \quad v_p(a) = \lim_{n\to\infty} v_p(a_n).$$

در نتیجه، حلقهٔ ارزهٔ $\mathbb{Q}_p$ یعنی

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

یک حلقه موضعی و ایده‌آل ارزهٔ آن

$$\mathfrak{p} := \{x \in \mathbb{Q}_p \mid v_p(x) > 0\} = p\mathbb{Z}_p$$

است. در نتیجه $\mathbb{Z}_p$ یک حلقهٔ ارزهٔ گسسته است که تنها ایده‌آل اول آن $\mathfrak{p}$ است. به همین دلیل مطالعه حلقه‌های اعداد صحیح $p-$ای در برخی موارد از مطالعه حلقه $\mathbb{Z}$ ساده‌تر است؛ زیرا برخلاف $\mathbb{Z}$ که نامتناهی ایده‌آل اول دارد، $\mathbb{Z}_p$ تنها یک ایده‌آل اول دارد که توسط p تولید می‌شود. به علاوه هر عضو $\mathbb{Z}_p$ را می‌توان به صورت یک سری توانی حول p نمایش داد که ضرایب این سری توانی متعلق به یک دستگاه کامل مانده‌ها به پیمانه p اند. متناهی بودن مجموعه ضرایب سری توانی، خاصیتی اساسی برای $\mathbb{Z}_p$ محسوب می‌شود زیرا شرطی اساسی در اثبات موضعاً فشرده بودن $\mathbb{Q}_p$ است. موضعا فشرده بودن یک میدان، منجر به تعریف اندازه هار و سایر مفاهیم آنالیزی روی آن می‌شود. این مفاهیم در مبحث آنالیز $p-$ای مورد مطالعه قرار می‌گیرند که فراتر از اهداف این پایان‌نامه است.

تعریف ۱۳.۲. *یک میدان موضعی عبارت است از یک میدان مانند K همراه با یک نُرم نابدیهی مانند $|\cdot|$ روی آن به طوری که K نسبت به توپولوژی القا شده، موضعاً فشرده باشد.*

از تعریف فوق به سادگی نتیجه می‌شود که هر میدان موضعی، کامل است زیرا در یک فضای موضعاً فشرده، هر دنباله کوشی، همگرا است. در نتیجه تمامی نتایج بخش ۴ از فصل ۱ که درباره میدان‌های کامل که حلقه اعداد صحیح‌شان یک حلقه ارزهٔ گسسته باشد، عیناً برای میدان‌های موضعی نیز صادق است.

قضیه بعد نشان می‌دهد که میدان‌های موضعی را می‌توان به طور کامل طبقه‌بندی کرد.

قضیه ۱۴.۲. *به فرض K یک میدان موضعی باشد.*

آ) اگر نُرم روی K ارشمیدسی باشد، آن‌گاه K با $\mathbb{R}$ یا $\mathbb{C}$ یک‌ریخت است و نُرم روی K نیز با نُرم متداول روی $\mathbb{R}$ یا $\mathbb{C}$ هم‌ارز است.

ب) اگر نرم روی K ناارشمیدسی بوده و K از مشخصه صفر باشد، آن‌گاه K با توسیعی متناهی از میدان $p-$ای یک‌ریخت است و نُرم روی آن نیز با توسیع یکتای نُرم $p-$ای هم‌ارز خواهد بود.

پ) اگر نرم روی K ناارشمیدسی بوده ولی مشخصه K ناصفر باشد، آن‌گاه K با میدان سری‌های لوران صوری $k((X))$ روی میدان متناهی k یک‌ریخت است. میدان سری‌های لوران صوری، کامل‌سازی میدان توابع گویا $k(X)$ نسبت به نُرم حاصل از تابع ارزهٔ گسستهٔ متناظر با ایده‌آل اول $\langle X\rangle$ است.

اثبات. به بخش‌های ۴ و ۵ از فصل دوم کتاب سرر [۱۰] نگاه کنید. ■

از آن‌جایی که هدف نظریهٔ میدان رده‌ای موضعی (و این پایان‌نامه) مطالعه توسیع‌های آبلی میدان‌های موضعی است، از این پس توجه خود را به موارد (ب) و (پ) از قضیه فوق معطوف می‌کنیم زیرا تنها توسیع جبری $\mathbb{R}$، $\mathbb{C}$ است و $\mathbb{C}$ نیز خود بسته جبری است.

اگر L یک توسیع $\mathbb{Q}_p$ از درجه n باشد، آن‌گاه بنا به مطالب بخش ۴ از فصل ۱، میدان رده‌ای مانده‌های آن توسیعی از میدان رده‌ای مانده‌های $\mathbb{Q}_p$ با درجه f خواهد بود. چون میدان رده‌ای مانده‌های $\mathbb{Q}_p$ برابر $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ است، پس در نتیجه $k_L \cong \mathbb{F}_{p^f}$.

از طرف دیگر اگر k یک میدان متناهی باشد، آن‌گاه میدان رده‌ای مانده‌های $L := k((X))$ نیز متناهی خواهد بود زیرا $k_L = k[\![X]\!]/\langle X\rangle \cong k$. بدین ترتیب مشاهده می‌شود موارد (ب) و (پ) از قضیه ۱۳.۲. دقیقا متناظر میدان‌های موضعی با میدان رده‌ای مانده‌های متناهی اند. بنابراین از این پس میدان‌های کامل نسبت به توپولوژی حاصل از یک تابع ارزهٔ گسسته را که میدان رده‌ای مانده‌هایشان متناهی باشد، میدان‌های موضعی (ناارشمیدسی) می‌نامیم.

فصل ۳

گروه‌های صوری

پیش از معرفی گروه‌های صوری لوبین‌ـ تیت و ارتباط آن‌ها به نظریهٔ میدان رده‌ای موضعی لازم است تا برخی تعاریف و مفاهیم مرتبط به گروه‌های صوری در حالت کلی بیان شوند. در بخش اول این فصل یکی از انگیزه‌های مطالعه گروه‌های صوری، یعنی بیان یک قاعدهٔ صریح برای جمع نقاط در خم‌های بیضوی تعریف شده روی میدان‌های موضعی، را شرح داده و سپس در بخش دوم تعریف گروه‌های صوری و برخی مفاهیم مرتبط را بیان می‌کنیم. برای تشریح کامل گروه‌های صوری و کاربردهای آن در جبر، نظریه اعداد و هندسه جبری به [۳] رجوع کنید.

۱.۳ انگیزه؛ گروه‌های صوری و خم‌های بیضوی

به فرض E یک خم بیضوی باشد. در این صورت معادله این خم به فرم وایراشتراس به شکل زیر است:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

حال اگر از تغییر متغیرهای $z = -\frac{x}{y}$ و $w = -\frac{1}{y}$ استفاده کنیم، معادله وایراشتراس این خم به شکل زیر در می‌آید:

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2.$$

اگر عبارت فوق را متوالیا در خودش جایگذاری کنیم، می‌بینیم که می‌توان w را برحسب یک سری توانی با متغیر z نوشت:

$$
\begin{aligned}
w =& z^3 + \left(a_1 z + a_2 z^2\right) w + \left(a_3 + a_4 z\right) w^2 + a_6 w^3 \\
=& z^3 + \left(a_1 z + a_2 z^2\right) \left[z^3 + \left(a_1 z + a_2 z^2\right) w + \left(a_3 + a_4 z\right) w^2 + a_6 w^3\right] \\
&+ \left(a_3 + a_4 z\right) \left[z^3 + \left(a_1 z + a_2 z^2\right) w + \left(a_3 + a_4 z\right) w^2 + a_6 w^3\right]^2 \\
&+ a_6 \left[z^3 + \left(a_1 z + a_2 z^2\right) w + \left(a_3 + a_4 z\right) w^2 + a_6 w^3\right] \\
&\vdots \\
=& z^3 + a_1 z^4 + \left(a_1^2 + a_2\right) z^5 + \left(a_1^3 + 2a_1 a_2 + a_3\right) z^6 \\
&+ \left(a_1^4 + 3a_1^2 a_2 + 3a_1 a_3 + a_2^2 + a_4\right) z^7 + \cdots \\
=& z^3 \left(1 + A_1 z + A_2 z^2 + \cdots\right).
\end{aligned}
$$

به وضوح در سری توانی حاصل هر A_n عضوی از حلقه $\mathbb{Z}[a_1, ..., a_6]$ است. این سری توانی یک سری توانی صوری نامیده می‌شود زیرا آن را صرفا به عنوان یک جمع نامتناهی در نظر می‌گیریم و تشخیص همگرایی یا واگرایی آن برای ما در الویت نیست. اثبات وجود و یکتایی سری توانی حاصل از فرایند فوق، نتیجه‌ای از لم هنسل است. برای اثبات کامل این موضوع به [۱۱] نگاه کنید.

اکنون اگر عکس تغییر متغیر انجام شده را در سری توانی $w(z)$ جایگذاری کنیم، داریم:

$$
\begin{aligned}
x(z) &= \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - \left(a_4 + a_1 a_3\right) z^2 - \cdots, \\
y(z) &= -\frac{1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + \left(a_4 + a_1 a_3\right) z - \cdots.
\end{aligned}
$$

بدین ترتیب می‌توان نقاط روی یک خم بیضوی را به وسیله سری‌های توانی با متغیر z و با ضرایب در $\mathbb{Z}[a_1, ..., a_6]$ نوشت. باید توجه داشت که اگر خم بیضوی E روی میدان K تعریف شده باشد، آن‌گاه لزوما هر سری توانی را نمی‌توان با اعضای میدان متناظر کرد؛ یعنی سری‌های توانی فوق به ازای $z \in K$ لزوما همگرا نیستند. اما اگر K یک میدان موضعی با حلقه اعداد صحیح R و ایده‌آل اول $\mathfrak{p}$ باشد و به علاوه اگر فرض کنیم $a_1, ..., a_6 \in K$، آن‌گاه سری‌های توانی $x(z)$ و $y(z)$ در K لزوما همگرا می‌شوند و در نتیجه نگاشت $z \mapsto (x(z), y(z))$ ایده‌آل $\mathfrak{p}$ را به طور یک‌به‌یک در $E(K)$ می‌نشاند. از این ایده در فصل آینده استفاده خواهیم کرد.

حال مجددا خم‌های بیضوی روی میدان‌های دلخواه را در نظر می‌گیریم و تلاش می‌کنیم تا قاعده جمع نقاط روی یک خم بیضوی را به کمک سری‌های توانی صوری بیان کنیم. به فرض z_1 و z_2 دو متغیر مستقل باشند. تعریف می‌کنیم $w_1 = w(z_1)$ و $w_2 = w(z_2)$. برای یافتن جمع دو نقطه (z_1, w_1) و (z_2, w_2) روی خم بیضوی E در صفحه (z, w)، کافی است که محل تقاطع خط

واصل نقاط (z_1, w_1) و (z_2, w_2) با خم E را در نظر گرفته و وارون آن را بیابیم. نقطه حاصل برابر مجموع مورد نظر خواهد بود. محل برخورد سوم خط واصل دو نقطه با خم را با (z_3, w_3) نمایش می‌دهیم. اگر λ برابر شیب خط واصل بین (z_1, w_1) و (z_2, w_2) باشد و همچنین اگر تعریف کنیم $\nu = w_1 - \lambda z_1$، آن‌گاه داریم:

$$\begin{aligned} z_3 &= z_3(z_1, z_2) \\ &= -z_1 - z_2 + \frac{a_1\lambda + a_3\lambda^2 - a_2 y - 2a_4\lambda\nu - 3a_6\lambda^2\nu}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3} \\ &\in \mathbb{Z}[a_1, \ldots, a_6][\![z_1, z_2]\!]. \end{aligned}$$

با جایگذاری عبارت فوق در رابطه $w_3 = \lambda z_3 + \mu$ می‌توان w_3 را نیز بر حسب λ و μ نوشت. فرمول یافتن نقاط روی یک خم بیضوی در صفحه (z, w) به صورت زیر است:

$$i(z) = \frac{x(z)}{y(z) + a_1 x(z) + a_3} = \frac{z^{-2} - a_1 z^{-1} - \cdots}{-z^{-3} + 2a_1 z^{-2} + \cdots} \in \mathbb{Z}[a_1, \ldots, a_6][\![z]\!],$$

در نتیجه اگر $F(z_1, z_2)$ بیانگر مولفهٔ روی محور z دو نقطهٔ (z_1, w_1) و (z_2, w_2) باشد، آن‌گاه داریم:

$$\begin{aligned} F(z_1, z_2) =& i(z_3(z_1, z_2)) \\ =& z_1 + z_2 - a_1 z_1 z_2 - a_2\left(z_1^2 z_2 + z_1 z_2^2\right) \\ &+ \left(2a_3 z_1^3 z_2 + (a_1 a_2 - 3a_3) z_1^2 z_2^2 + 2a_3 z_1 z_2^3\right) + \cdots \\ &\in \mathbb{Z}[a_1, \ldots, a_6][\![z_1, z_2]\!]. \end{aligned}$$

بدین ترتیب گروه آبلی نقاط روی یک خم بیضوی را می‌توان به صورت یک سری توانی دو متغیره نمایش داد. باید توجه داشت که سری توانی فوق خواص عمل جمع یک گروه آبلی را دارا است. به طور دقیق‌تر F در روابط زیر صدق می‌کند:

$$\begin{aligned} F(z_1, z_2) &= F(z_2, z_1) && \text{(جابه‌جایی)} \\ F(z_1, F(z_2, z)) &= F(F(z_1, z_2), z) && \text{(شرکت‌پذیری)} \\ F(z, i(z)) &= 0 && \text{(وارون‌پذیری)}. \end{aligned}$$

بدین ترتیب سری‌های توانی دومتغیره با خواص فوق (یا خواصی مشابه) متناظر قواعد گروهی گروه‌هایی اند که اعضایشان مشخص نیست. به عنوان مثال اگر K و L دو میدان موضعی باشند و $F(z_1, z_2)$ سری توانی متناظر جمع نقاط روی یک خم بیضوی E باشد، آن‌گاه ایده‌آل‌های اول $\mathfrak{p}_K$ و $\mathfrak{p}_L$ هر دو تحت قاعده F تبدیل به گروه آبلی می‌شوند در حالی که اعضای $\mathfrak{p}_K$ و $\mathfrak{p}_L$ می‌توانند کاملا از یکدیگر متفاوت باشند. چنین سری‌های توانی را قواعد گروهی صوری می‌نامیم. در بخش بعد به تعریف و خواص اولیه این قواعد می‌پردازیم.

۲.۳ تعاریف و نتایج اولیه

فرض کنید A یک حلقهٔ جابه‌جایی و یک‌دار باشد.

تعریف ۱.۳. *یک سری توانی با ضرایب در A یک دنباله نامتناهی به شکل*

$$f = (a_0, a_1, a_2, \ldots), \quad a_i \in A, \quad i \in \mathbb{N}$$

است. جمع و ضرب سری‌های توانی نیز به شکل زیر تعریف می‌شوند:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots),$$
$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = \left(a_0 b_0, \ldots, \sum_{i+j=k} a_i b_j, \ldots \right).$$

بدین ترتیب سری‌های توانی با ضرایب در A تشکیل یک حلقه جابه‌جایی می‌دهند که آن را با $A[\![T]\!]$ نمایش می‌دهیم.

علت استفاده از نماد $A[\![T]\!]$ برای حلقه سری‌های توانی با ضرایب در A این است که می‌توان هر عضو $A[\![T]\!]$ مانند $f = (a_0, a_1, a_2, \ldots)$ را به صورت زیر در نظر گرفت که در آن T یک متغیر صوری است:

$$\sum_{i=0}^{\infty} a_i T^i$$

در نتیجه می‌توان دید که تعریف داده شده از سری توانی با ضرایب در A بر تعریف متداول سری توانی منطبق است. سری‌های توانی با بیش از یک متغیر نیز به شکل مشابه قابل تعریف اند.

تعریف ۲.۳. *یک قاعده گروهی صوری جابه‌جایی عبارت است از یک سری توانی دومتغیره در A مانند $F \in A[\![X, Y]\!]$ به طوری که*

۱) $F(X, Y) = X + Y +$ *عبارت‌های از درجه ۲ یا بالاتر*،

۲) $F(X, F(Y, Z)) = F(F(X, Y), Z)$،

۳) $F(X, Y) = F(Y, X)$.

مورد ۲ و ۳ به ترتیب بیان‌گر خواص شرکت‌پذیری و جابه‌جایی قاعده گروهی صوری اند. برای آن که یک قاعده گروهی صوری بتواند در عمل نیز یک قاعده گروهی باشد، لازم است که دارای

خاصیت وارون‌پذیری نیز باشد. خوشبختانه این خاصیت از تعریف فوق نتیجه می‌شود و می‌توان برای X سری توانی یکتای

$$i_F(X) = -X + \sum_{i=2}^{\infty} b_i X^i \qquad b_i \in A$$

را یافت که

$$F(X, i_F(X)) = 0.$$

برای اثبات این موضوع به [۳] نگاه کنید.

تعریف ۳.۳. *به فرض $F(X,Y)$ و $G(X,Y)$ دو قاعده گروهی صوری باشند. یک هم‌ریختی $F \to G$ عبارت است از یک سری توانی مانند $h \in TA[\![T]\!]$ به طوری که*

$$h(F(X,Y)) = G(h(X), h(Y)).$$

اگر هم‌ریختی h وارون داشته باشد، آن را یک یک‌ریختی می‌نامیم. همچنین یک هم‌ریختی $F \to F$ را یک خودریختی F می‌نامیم.

مثال ۴.۳. *قاعده گروهی صوری $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$ را در نظر بگیرید. اگر $\mathfrak{p}$ ایده‌آل اول میدان موضعی K باشد، آن‌گاه بنا به مطالب بخش اول این فصل $(\mathfrak{p}, +_F)$ یک گروه آبلی است. ادعا می‌کنیم که گروه یکه‌های اصلی میدان موضعی K تحت عمل ضرب با گروه $(\mathfrak{p}, +_F)$ یک‌ریخت است. نگاشت $\phi : \mathfrak{p} \to U^{(1)}$ را با ضابطه $z \mapsto 1 + z$ در نظر بگیرید. ϕ به وضوح یک نگاشت دوسویی است. همچنین*

$$\begin{aligned}\phi(z_1 +_F z_2) &= \phi(F(z_1, z_2)) = \phi(z_1 z_2 + z_1 + z_2) \\ &= z_1 z_2 + z_1 + z_2 + 1 = (z_1 + 1)(z_2 + 1) = \phi(z_1)\phi(z_2).\end{aligned}$$

لذا ϕ یک یک‌ریختی است.

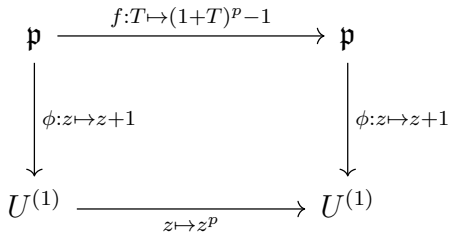
مثال ۵.۳. *قاعده گروهی صوری F در مثال قبل را در نظر بگیرید. در این صورت سری توانی (در واقع چندجمله‌ای) $f(T) = (1+T)^p - 1$ یک خودریختی F است زیرا:*

$$\begin{aligned}F(f(X), f(Y)) &= F((1+X)^p - 1, (1+Y)^p - 1) \\ &= (1+X)^p (1+Y)^p - 1 \\ &= f(F(X,Y)).\end{aligned}$$

حال چون بنا به مثال قبل $(\mathfrak{p}, +_F)$ و $U^{(1)}$ یک‌ریخت اند، پس نگاشت $\phi \circ f \circ \phi^{-1}$ یک خودریختی $U^{(1)}$ است. به طور دقیق‌تر داریم:

$$\phi \circ f \circ \phi^{-1}(z) = \phi \circ f(z-1) = \phi(z^p - 1) = z^p.$$

در نتیجه نمودار زیر جابه‌جایی است:



گزاره زیر به ساختار جبری موجود بر هم‌ریختی‌های گروه‌های صوری می‌پردازد:

گزاره ۶.۳. آ) *برای قواعد گروهی صوری دلخواه F و G ، مجموعه $Hom(F,G)$ متشکل از هم‌ریختی‌های $F \to G$ تحت عمل جمع $+_G$ یک گروه آبلی است.*
ب) *برای قاعده گروهی صوری دلخواه F، گروه آبلی $End(F)$ متشکل از خودریختی‌های F تحت عمل ترکیب خودریختی‌ها تبدیل به یک حلقه می‌شود.*

اثبات.
صفحه ۳۱، لم ۸.۲. از [۵] را ببینید.

■

فصل ۴

قانون تقابل موضعی

در این فصل به بیان و اثبات قانون تقابل موضعی خواهیم پرداخت. قانون تقابل موضعی بیان می‌کند که برای هر میدان موضعی مانند K، هم‌ریختی یکتای

$$\phi_K : K^\times \to Gal(K^{ab}/K)$$

که به نگاشت تقابل موضعی یا نگاشت آرتین معروف است، با ویژگی‌های زیر وجود دارد:

آ) برای هر عنصر اول K و برای هر توسیع متناهی غیر منشعب L از K، $\phi_K(\pi)$ همان نگاشت $Frob_{L/K}$ است.

ب) برای هر توسیع متناهی آبلی L از K، هسته هم‌ریختی $a \mapsto \phi_K(a)|_L$ شامل $N_{L/K}(L^\times)$ است و در نتیجه ϕ_K یک‌ریختی زیر را القا می‌کند:

$$\phi_{L/K} : K^\times/N_{L/K}(L^\times) \to Gal(L/K).$$

قانون تقابل موضعی تا به امروز به روش‌های متفاوتی اثبات شده است. اثباتی که در ادامه به آن پرداخته خواهد شد، اثباتی است که جاناتان لوبین و جان تیت در سال ۱۹۶۵ در مقاله خود [۴] منتشر کردند. آن‌ها توانستند با الهام از نظریهٔ ضرب مختلط روی خم‌های بیضوی، که منجر به توصیف توسیع‌های متناهی $\mathbb{Q}(i)$ می‌شود، و به کمک نظریه گروه‌های صوری، توسیع آبلی کاملا منشعب ماکسیمال K_π را بسازند و عمل نگاشت آرتین روی این توسیع را به طور صریح مشخص کنند. در بخش اول این فصل، گروه‌های صوری لوبین‌ـتیت را معرفی می‌کنیم. در بخش دوم به کمک این گروه‌ها، توسیع آبلی کاملا منشعب K_π از K را خواهیم ساخت و در نهایت در بخش سوم خواص نگاشت آرتین را بررسی خواهیم کرد.

۱.۴ گروه‌های صوری لوبین-تیت

فرض کنید R حلقهٔ اعداد صحیح میدان موضعی نا‌ارشمیدسی K باشد. π را یک عنصر اول R و q را تعداد اعضای میدان رده‌ای مانده‌ها در نظر می‌گیریم.

تعریف ۱.۴. *مجموعه $\mathcal{F}_\pi$ را مجموعه متشکل از سری‌های توانی صوری $f(X) \in R[\![X]\!]$ در نظر بگیرید به طوری که*

آ) $f(X) = \pi X + (\text{جملات از درجه حداقل ۲})$،

ب) $f(X) \equiv X^q \pmod{\pi}$.

لم زیر که منسوب به لوبین و تیت [۴] است، نقشی اساسی در اثبات گزاره‌های این بخش خواهد داشت.

لم ۲.۴. *فرض کنید $f, g \in \mathcal{F}_\pi$ و $l(X_1, \cdots, X_n)$ یک فرم خطی (چندجمله‌ای همگن از درجه یک) با ضرایب در R باشد. در این صورت، $\phi \in R[\![X_1, \cdots, X_n]\!]$ یکتایی وجود دارد به طوری که*

آ) $\phi(X_1, \cdots, X_n) = l(X_1, \cdots, X_n) + (\text{جملات از درجه حداقل ۲})$،

ب) $f(\phi(X_1, \cdots, X_n)) = \phi(g(X_1), \cdots, g(X_n))$.

اثبات. برای اثبات وجود و یکتایی سری توانی ϕ ابتدا به کمک استقرا دنباله‌ی $\{\phi_r\}_{r=1}^{\infty}$ از چندجمله‌ای‌ها را با خواص زیر را می‌سازیم:

$\phi_r(X_1, \cdots, X_n) = l(X_1, \cdots, X_n) + (\text{جملات از درجه حداقل ۲})$,
$f(\phi_r(X_1, \cdots, X_n)) = \phi_r(g(X_1), \cdots, g(X_n)) + (\text{جملات از درجه حداقل } r+1)$.

این دنباله را می‌توان به طریق زیر و به طور یکتا تعریف کرد:

$$\phi_1(X_1, \cdots, X_n) = l(X_1, \cdots, X_n),$$
$$\phi_{r+1}(X_1, \cdots, X_n)) = \phi_r(X_1, \cdots, X_n) + Q_r(X_1, \cdots, X_n).$$

که در آن هر Q_r چندجمله‌ای همگنی از درجه $r+1$ است که با توجه به خواص مورد انتظار از ϕ_r به طور یکتا تعیین می‌شود. در نهایت با تعریف کردن ϕ به عنوان حد دنباله $\{\phi_r\}_{r=1}^{\infty}$ حکم ثابت می‌شود. برای مشاهده اثبات کامل به [۴] یا [۵] نگاه کنید. ■

گزاره ۳.۴. *به ازای هر $f \in \mathcal{F}_\pi$ قاعده گروهی صوری یکتای F_f با ضرایب در R وجود دارد به طوری که f یک خودریختی F_f باشد.*

اثبات. اگر فرم خطی $l(X,Y) = X + Y$ را در نظر بگیریم، آن‌گاه لم ۲.۴. وجود و یکتایی سری توانی صوری $F_f = X+Y+(\text{جملات از درجه حداقل } ۲) \in R[\![X,Y]\!]$ را نتیجه می‌دهد. بنابراین کافی است نشان دهیم که F_f خواص جابه‌جایی و شرکت‌پذیری را نیز دارد.

برای اثبات جابه‌جایی بودن F_f تعریف می‌کنیم $G(X,Y) := F_f(Y,X)$. در این صورت داریم:

$$G(X,Y) = X + Y + (\text{جملات از درجه حداقل } ۲)$$

و

$$f(G(X,Y)) = f(F_f(Y,X)) = F_f(f(Y),f(X)) = G(f(X),f(Y)).$$

پس بنا به لم ۲.۴.، $G(X,Y) = F_f(X,Y)$ و در نتیجه F_f جابه‌جایی است.

برای اثبات شرکت‌پذیر بودن F_f تعریف می‌کنیم $G_1(X,Y,Z) := F_f(X,F_f(Y,Z))$ و $G_2(X,Y,Z) := F_f(F_f(X,Y),Z)$. در این صورت برای هر دوی G_1 و G_2 داریم:

$$G_i(X,Y,Z) = X + Y + Z + (\text{جملات از درجه حداقل } ۲)$$

و

$$G_i(f(X),f(Y),f(Z)) = f(G_i(X,Y,Z)).$$

از لم ۲.۴. می‌دانیم که یک و فقط یک سری توانی در شروط فوق صدق می‌کند. در نتیجه $G_1(X,Y,Z) = G_2(X,Y,Z)$ و لذا F_f شرکت‌پذیر است. ■

گروه‌های فرمال F_f را گروه‌های صوری لوبین‌ـتیت می‌نامیم. ویژگی مهم این گروه‌های صوری که در آینده از آن استفاده خواهیم کرد این است که سری توانی $f \in \mathcal{F}_\pi$ یک خودریختی برای آنان است. به عبارت دیگر، گروه‌های صوری لوبین‌ـتیت آن دسته از گروه‌های صوری اند که یک خودریختی با ویژگی‌های زیر دارند:

آ) مشتق آن در مبدا برابر یک یکنواخت‌ساز می‌شود.

ب) روی میدان رده‌ای مانده‌ها به شکل نگاشت فروبنیوس عمل می‌کند.

اکنون وجود رده‌ای از سری‌های توانی را اثبات می‌کنیم که به ما اجازه می‌دهد تا در ادامه مدول‌های لوبین‌ـتیت را تعریف کنیم.

گزاره ۴.۴. *برای هر $f,g \in \mathcal{F}_\pi$ و هر $a \in R$، سری توانی یکتای $[a]_{g,f} \in R[\![X]\!]$ وجود دارد به طوری که*

آ) $[a]_{g,f}(X) = aX + (\text{جملات از درجه حداقل } ۲)$،

ب) $g \circ [a]_{g,f} = [a]_{g,f} \circ f$.

در نتیجه $[a]_{g,f} : F_f \to F_g$ *یک هم‌ریختی است.*

اثبات. وجود و یکتایی $[a]_{g,f}$ به وضوح از لم ۲.۴. نتیجه می‌شود. کافی است که نشان دهیم که $[a]_{g,f} : F_f \to F_g$ یک هم‌ریختی است. برای این کار باید تساوی زیر را ثابت کنیم:

$$[a]_{g,f}(F_f(X,Y)) = F_g([a]_{g,f}(X), [a]_{g,f}(Y)).$$

اولاً هر دو طرف تساوی فوق به پیمانه جملات از درجه حداقل ۲، به شکل $aX + aY$ اند. دوماً،

$$\begin{aligned}[a]_{g,f}(F_f(f(X), f(Y))) = [a]_{g,f} \circ f(F_f(X,Y)) = g \circ [a]_{g,f}(F_f(X,Y)) \\ \implies ([a]_{g,f} \circ F_f) \circ f = g \circ ([a]_{g,f} \circ F_f)\end{aligned}$$

و

$$\begin{aligned}F_g([a]_{g,f}(f(X), f(Y))) = F_g(g \circ [a]_{g,f}(X,Y)) = g \circ F_g([a]_{g,f}(X,Y)) \\ \implies (F_g \circ [a]_{g,f}) \circ f = g \circ (F_g \circ [a]_{g,f}).\end{aligned}$$

در نتیجه بنا به لم ۲.۴. ثابت می‌شود که

$$[a]_{g,f} \circ F_f = F_g \circ [a]_{g,f}$$

و لذا $[a]_{g,f} : F_f \to F_g$ یک هم‌ریختی است. ■

نتیجه ۵.۴. *برای هر* $f, g \in \mathcal{F}_\pi$، *داریم* $F_f \cong F_g$.

اثبات. $[1]_{g,f} : F_f \to F_g$ یک‌ریختی است. ■

از گزاره ۶.۳. می‌دانیم که $Hom(F_f, F_g)$ با عمل F_g یک گروه است. گزاره ۴.۴. نیز نگاشت $a \mapsto [a]_{g,f} : R \to Hom(F_f, F_g)$ را معرفی می‌کند. گزاره بعد نشان می‌دهد که این نگاشت در واقع یک هم‌ریختی گروهی است.

لم ۶.۴. *برای هر* $a, b \in R$،

$$[a+b]_{g,f} = [a]_{g,f} +_{F_g} [b]_{g,f}$$

و

$$[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}.$$

اثبات. برای اثبات این گزاره نیز مجددا از لم ۲.۴. استفاده می‌کنیم. نخست مشاهده می‌کنیم که هر دو عبارت $[a+b]_{g,f}$ و $[a]_{g,f} +_{F_g} [b]_{g,f}$ به پیمانه جملات از درجه حداقل ۲، با $aX+bX$ هم‌نهشت اند. همچنین

$$\begin{aligned}([a]_{g,f} +_{F_g} [b]_{g,f}) \circ f(X) &= F_g([a]_{g,f} \circ f(X), [b]_{g,f} \circ f(X)) \\ &= F_g(g \circ [a]_{g,f}(X), g \circ [b]_{g,f}(X)) \\ &= g \circ F_g([a]_{g,f}(X), [b]_{g,f}(X)) \\ &= g \circ ([a]_{g,f} +_{F_g} [b]_{g,f})(X).\end{aligned}$$

از طرف دیگر بنا به گزاره ۴.۴. داریم

$$[a+b]_{g,f} \circ f = g \circ [a+b]_{g,f}.$$

در نتیجه از لم ۲.۴. نتیجه می‌شود که

$$[a+b]_{g,f} = [a]_{g,f} +_{F_g} [b]_{g,f}.$$

با استدلالی کاملاً مشابه به دست می‌آید که

$$[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}.$$

■

نتیجه ۷.۴. *برای هر $u \in R^\times$، هم‌ریختی‌های $[u]_{g,f}$ و $[u^{-1}]_{g,f}$ وارون یک‌دیگر اند و لذا یک‌ریختی اند.*

نتیجه ۸.۴. *برای هر $a \in R$، خودریختی یکتای $[a]_f : F_f \to F_f$ هست به طوری که $[a]_f = aX + (\text{جملات از درجه حداقل } ۲)$ و $f \circ [a]_f = [a]_f \circ f$. همچنین نگاشت*

$$a \mapsto [a]_f : R \to End(F_f)$$

یک هم‌ریختی حلقه‌ای یک‌به‌یک است.

اثبات. تنها ادعای یک‌به‌یکی را اثبات می‌کنیم. باقی ادعاها همگی مستقیماً از گزاره‌های قبل نتیجه می‌شوند.

فرض کنید $[a]_f = [b]_f$. در نتیجه

$$\begin{aligned}aX + (\text{جملات از درجه حداقل } ۲) &= bX + (\text{جملات از درجه حداقل } ۲) \\ \implies aX &= bX \\ \implies a &= b.\end{aligned}$$

■

نتیجه ۹.۴. *برای هر $f \in \mathcal{F}_\pi$، داریم $[\pi]_f = f$.*

اثبات. از یکتایی $[a]_f$ برای هر $a \in R$ نتیجه می‌شود. ■

۲.۴ K_π

در این بخش K را یک میدان موضعی ناارشمیدسی، R را حلقه اعداد صحیح آن، $\mathfrak{p}$ را ایده‌آل اول یکتای آن، k را میدان رده‌ای مانده‌های آن و $\pi \in K$ را یک عنصر اول آن در نظر بگیرید. هدف ما ساخت توسیع آبلی و کاملاً منشعب K_π از K است.

فرض کنید K^{al} توسیع جبری جدایی‌پذیر K باشد. از گزاره ۲۹.۱.، می‌دانیم که نُرم روی K به طور یکتا به هر توسیع متناهی آن توسعه می‌یابد. بنابراین به هر عضو K^{al} می‌توان نُرم نسبت داد. حال فرض کنید $f \in \mathcal{F}_\pi$، $\alpha, \beta \in K^{al}$ و $|\alpha|, |\beta| < 1$. در نتیجه سری‌های $F_f(\alpha, \beta)$ و $[a]_f(\alpha)$ به ازای هر $a \in R$ همگرا می‌شوند.

تعریف ۱۰.۴. *$f \in \mathcal{F}_\pi$ را در نظر بگیرید. مجموعهٔ*

$$\Lambda_f := \{\alpha \in K^{al} \mid |\alpha| < 1\}$$

با عمل جمع $\alpha +_{\Lambda_f} \beta := F_f(\alpha, \beta)$ و ضرب اسکالر $a * \alpha := [a]_f(\alpha)$، تشکیل یک $R-$مدول می‌دهد. این مدول را، یک مدول لوبین‌ـ تیت می‌نامیم.

باید توجه داشت که انتخاب f در تعریف فوق تاثیری بر ساختار جبری مدول Λ_f ندارد زیرا مطابق مطالب بخش اول این فصل، برای هر $g \in \mathcal{F}_\pi$، یک‌ریختی کانونی $[1]_{g,f} : F_f \to F_g$ یک یک‌ریختی $R-$مدولی $\Lambda_f \to \Lambda_g$ القا می‌کند. در نتیجه برای عنصر اول π، همه مدول‌های لوبین‌ـ تیت یک‌ریخت اند.

تعریف ۱۱.۴. *برای هر n صحیح مثبت، $\Lambda_{f,n}$ را زیرمدولی از Λ_f بگیرید که توسط π^n پوچ می‌شود:*

$$\Lambda_{f,n} := \{\alpha \in \Lambda_f \mid \pi^n * \alpha = 0\} = \{\alpha \in \Lambda_f \mid [\pi^n]_f(\alpha) = 0\}.$$

بنا به لم ۶.۴.، داریم

$$\begin{aligned} \pi^n * \alpha = 0 &\iff [\pi^n]_f(\alpha) = 0 \\ &\iff [\pi]_f \circ \cdots \circ [\pi]_f(\alpha) = 0 \\ &\iff f \circ \cdots \circ f(\alpha) = 0 \\ &\iff f^{(n)}(\alpha) = 0. \end{aligned}$$

پس $\Lambda_{f,n}$ را می‌توان مجموعه ریشه‌های چندجمله‌ای $f^{(n)}(X)$ در نظر گرفت که دارای نُرم کمتر از یک اند. زیرمدول بودن $\Lambda_{f,n}$ با این تعریف نیز به سادگی نتیجه می‌شود؛ چون f با F_f و $[a]_f$ جابه‌جا می‌شود، پس $\Lambda_{f,n}$ تحت جمع و ضرب اسکالر بسته است.

گزاره ۱۲.۴. *$\Lambda_{f,n}$ به عنوان یک $R-$مدول با $R/\langle \pi^n \rangle$ یک‌ریخت است.*

اثبات. از آن‌جایی که ساختار جبری Λ_f مستقل از انتخاب f است، می‌توان فرض کرد که $f(X) = \pi X + X^q$. در این صورت واضح است که $f(X) \in \mathcal{F}_\pi$.

چون هر $\Lambda_{f,n}$ متناهی است (زیرا مجموعه ریشه‌های یک چندجمله‌ای است) و به علاوه R یک دامنه ایده‌آل اصلی است، پس بنا به قضیه ساختاری مدول‌های متناهیاً تولید شده بر روی دامنه‌های ایده‌آل اصلی، $\Lambda_{f,n}$ به صورت یکتایی به حاصل‌ضرب مدول‌های دوری دارد. به عبارت دیگر $d_1 \leq d_2 \leq \cdots \leq d_r$ یافت می‌شوند به طوری که

$$\Lambda_{f,n} = R/\langle \pi^{d_1} \rangle \times R/\langle \pi^{d_2} \rangle \times \cdots \times R/\langle \pi^{d_r} \rangle.$$

حال حکم را به استقرا روی n اثبات می‌کنیم. می‌دانیم که $\Lambda_{f,1}$ مجموعه ریشه‌های f است. f دارای q ریشهٔ مجزا در K^{al} است. چون $f(X) = X(X^{q-1} + \pi)$، و $X^{q-1} + \pi$ تحویل‌ناپذیر است (چون آیزنشتاین است)، پس ریشه‌های ناصفر f همگی مزدوج اند و بنا به نتیجه ۳۲.۱. ارزهٔ برابر دارند. از طرف دیگر حاصل ضرب ریشه‌های ناصفر $X^{q-1} + \pi$ برابر π است و چون ارزهٔ π برابر یک است (چون عنصر اول است)، نتیجه می‌شود که ریشه‌های ناصفر f همگی دارای ارزهٔ مثبت اند. پس نُرم همگی از یک کمتر بوده و لذا همه آن‌ها مشمول در Λ_f اند. پس زیرمدول $\Lambda_{f,1}$ دقیقا q عضو دارد. چون $q = \#k = [R : \langle \pi \rangle]$، پس لزوما $\Lambda_{f,1} \cong R/\langle \pi \rangle$.

برای $n > 1$ فرض کنید که حکم برای $\Lambda_{f,n-1}$ برقرار باشد. دنبالهٔ دقیق زیر را در نظر بگیرید:

$$0 \longrightarrow \Lambda_{f,1} \longrightarrow \Lambda_{f,n} \xrightarrow{\pi} \Lambda_{f,n-1} \longrightarrow 0$$

اگر نگاشت $\alpha \mapsto \pi * \alpha : \Lambda_{f,n} \to \Lambda_{f,n-1}$ پوشا باشد، آن‌گاه با توجه به دنباله فوق $\Lambda_{f,n} = \Lambda_{f,1} \times \Lambda_{f,n-1}$ و لذا حکم نتیجه می‌شود. برای اثبات پوشایی نگاشت $\pi : \Lambda_{f,1} \times \Lambda_{f,n-1}$، نشان می‌دهیم که نگاشت

$$\pi : \Lambda_f \times \Lambda_f$$

پوشا است. فرض کنید $\alpha \in \Lambda_f$. حاصل‌ضرب ریشه‌های چندجمله‌ای $f(X) - \alpha = X^q + \pi X - \alpha$ برابر $-\alpha$ است و لذا ارزهٔ ریشه‌های این چندجمله‌ای همگی مثبت اند. در نتیجه ریشه‌های این چندجمله‌ای همگی در Λ_f هستند. اگر β یکی از ریشه‌های آن باشد، آن‌گاه $\pi * \beta = f(\beta) = \alpha$ و حکم ثابت می‌شود. ■

نتیجه ۱۳.۴. $End(\Lambda_{f,n}) \cong R/\langle \pi^n \rangle$ و $Aut(\Lambda_{f,n}) \cong (R/\langle \pi^n \rangle)^\times$.

برای اثبات قضیه اصلی این بخش، به لم زیر نیاز خواهیم داشت.

لم ۱۴.۴. *فرض کنید L یک توسیع گالوای متناهی از میدان موضعی K باشد. R را حلقه اعداد صحیح K و $\mathfrak{p}_L$ را ایده‌آل اول L در نظر بگیرید. برای هر $F \in R[\![X_1, \cdots, X_n]\!]$ و $\alpha_1, \cdots, \alpha_n \in \mathfrak{p}_L$ دلخواه، داریم*

$$F(\tau(\alpha_1), \cdots, \tau(\alpha_n)) = \tau(F(\alpha_1, \cdots, \alpha_n)), \quad \forall \tau \in Gal(L/K).$$

اثبات. اگر F یک چندجمله‌ای باشد، آن‌گاه چون $\tau \in Gal(L/K)$ ضرایب F را تغییر نمی‌دهد، $F(\tau(X_1), \cdots, \tau(X_n)) = \tau(F(X_1, \cdots, X_n))$. اکنون فرض کنید که $F(X)$ یک سری توانی باشد. می‌توان نوشت: (جملات از درجه حداقل $m+1$) $F(X) = F_m(X)$ که در آن $F_m(X)$ یک چندجمله‌ای از درجه حداکثر m است. پس می‌توان نوشت $F(X_1, \cdots, X_n) = \lim_{m\to\infty} F_m(X_1, \cdots, X_n)$. از طرف دیگر، چون برای هر $\tau \in Gal(L/K)$ و هر $\alpha \in L$ داریم $|\tau(\alpha)| = |\alpha|$، پس τ روی L پیوسته است. بنابراین

$$\begin{aligned}\tau(F(\alpha_1, \cdots, \alpha_n)) &= \tau(\lim_{m\to\infty} F_m(\alpha_1, \cdots, \alpha_n)) \\ &= \lim_{m\to\infty} \tau(F_m(\alpha_1, \cdots, \alpha_n)) \\ &= \lim_{m\to\infty} F_m(\tau(\alpha_1), \cdots, \tau(\alpha_n)) \\ &= F(\tau(\alpha_1), \cdots, \tau(\alpha_n))\end{aligned}$$

و حکم ثابت می‌شود. ■

عدد صحیح مثبت n را در نظر بگیرید. زیرمیدان $K[\Lambda_{f,n}]$ از K^{al} را که با افزودن اعضای $\Lambda_{f,n}$ به K ساخته می‌شود را با $K_{\pi,n}$ نمایش می‌دهیم. باید توجه داشت که $K_{\pi,n}$ به انتخاب f وابسته نیست؛ زیرا $R-$مدول‌های $\Lambda_{f,n}$ به ازای هر $f \in \mathcal{F}_\pi$ یک‌ریخت اند و هر توسیع $K[\Lambda_{f,n}]/K$ یک توسیع گالوا است (زیرا میدان شکافنده چندجمله‌ای $f^{(n)}$ است). پس همه میدان‌های $K_{\pi,n}$ حاصل از انتخاب‌های مختلف $f \in \mathcal{F}_\pi$، با یک‌دیگر $K-$یک‌ریخت اند.

قضیه ۱۵.۴.

آ) *برای هر n صحیح مثبت، $K_{\pi,n}/K$ یک توسیع کاملا منشعب از درجه $(q-1)q^{n-1}$ است.*

ب) *عمل R روی Λ_n یک یک‌ریختی $(R/\langle\pi^n\rangle)^\times \to Gal(K_{\pi,n}/K)$ تعریف می‌کند.*

پ) *برای هر n صحیح مثبت، π یک نُرم از $K_{\pi,n}$ به K است.*

اثبات. برای سادگی فرض می‌کنیم $f(X) = X^q + \pi X$. π_1 را یک ریشه ناصفر $f(X)$ در نظر بگیرید. $\pi_2, \cdots, \pi_n$ را به صورت استقرایی این گونه تعریف می‌کنیم که هر π_i یک ریشه چندجمله‌ای $f(X) - \pi_{i-1}$ باشد. بدین‌ترتیب هر π_i یک ریشه $f^{(i)}(X)$ است ولی ریشه $f^{(i-1)}(X)$ نیست. بدین ترتیب می‌توان زنجیره زیر از توسیع‌های میدانی را به دست آورد:

$$K \subset K(\pi_1) \subset K(\pi_2) \subset \cdots \subset K(\pi_n) \subset K[\Lambda_{f,n}].$$

برای $i = 1, 2, \cdots, n$ هر کدام از توسیع‌های $K(\pi_i)/K(\pi_{i-1})$ آیزنشتاین از درجه q اند. توسیع $K(\pi_1)/K$ نیز آیزنشتاین و از درجه $q-1$ است. در نتیجه بنا به گزاره ۴۰.۱.، $K(\pi_n)/K$ یک توسیع کاملا منشعب از درجه $(q-1)q^{n-1}$ است.

برای اثبات (ب)، توجه می‌کنیم که چون $K[\Lambda_{f,n}]$ میدان شکافنده چندجمله‌ای $f^{(n)}(X)$ است، پس گروه $Gal(L/K)$ با زیرگروهی از گروه جایگشت‌های $\Lambda_{f,n}$ یک‌ریخت خواهد بود. از طرف دیگر لم ۱۴.۴. نتیجه می‌دهد که هر $\tau \in Gal(L/K)$ با جمع و ضرب اسکالر روی مدول Λ_f جابه‌جا می‌شود و لذا $Gal(L/K)$ با زیرگروهی از گروه $Aut(\Lambda_{f,n}) \cong (R/\langle\pi^n\rangle)^\times$ یک‌ریخت خواهد بود. بنابراین

$$\begin{aligned}(q-1)q^{n-1} &= \#Aut(\Lambda_{f,n}) \\ &\geq \#Gal(K[\Lambda_{f,n}]/K) \\ &= [K[\Lambda_{f,n}] : K] \\ &\geq [K(\pi_n) : K] \\ &= (q-1)q^{n-1}.\end{aligned}$$

با توجه به برابری ابتدا و انتهای عبارت فوق، نامساوی‌ها لزوما باید تساوی باشند. در نتیجه

$$Gal(K[\Lambda_{f,n}]/K) \cong (R/\langle\pi^n\rangle)^\times$$

و

$$K[\Lambda_{f,n}] = K(\pi_n).$$

برای اثبات قسمت (پ)، ابتدا چندجمله‌ای مینیمال π_n را معرفی می‌کنیم. تعریف کنید $f^{[n]}(X) = (\frac{1}{X}f) \circ f^{(n-1)}(X)$. در این صورت $f^{[n]}(X) = \pi + X^{(q-1)q^{n-1}}$. این چندجمله‌ای، چندجمله‌ای مینیمال π_n است زیرا

$$f^{[n]}(\pi_n) = f^{[n-1]}(\pi_{n-1}) = \cdots = f(\pi_1) = 0$$

و درجه آن با درجه توسیع $K(\pi_n)/K$ برابر است. بنابراین

$$N_{K_{\pi,n}/K}(\pi_n) = (-1)^{(q-1)q^{n-1}}\pi.$$

بنا به عبارت فوق، نُرم π_n همواره برابر π است مگر وقتی که $q = 2$ و $n = 1$. اما در این حالت داریم $K_{\pi,1} = K$ و به وضوح $N_{K_{\pi,1}/K}(\pi) = \pi$. پس همواره π یک نُرم است. ■

اکنون تعریف می‌کنیم

$$K_\pi := \bigcup_{n=1}^{\infty} K_{\pi,n}.$$

چون هر زیرمیدان متناهی K_π، کاملاً منشعب است، پس K_π یک توسیع کاملاً منشعب از K خواهد بود. همچنین چون برای هر n داریم $Gal(K_{\pi,n}/K) \cong (R/\langle\pi^n\rangle)^\times$، با حد معکوس گرفتن از طرفین نتیجه می‌شود که

$$Gal(K_\pi/K) = \varprojlim_n Gal(K_{\pi,n}/K) \cong \varprojlim_n (R/\langle\pi^n\rangle)^\times = R^\times.$$

اکنون به کمک مطالب این بخش، مثال‌های ۴.۳. و ۵.۳. از فصل قبل را گسترش می‌دهیم.

مثال ۱۶.۴. *میدان موضعی نا‌ارشمیدسی $\mathbb{Q}_p$ را در نظر بگیرید. p یک یک‌نواخت‌ساز برای این میدان موضعی است. چندجمله‌ای $f(X) = (1+X)^p - 1 = X^p + \cdots + pX \in \mathbb{Q}_p[X]$ به پیمانه p برابر X^p است و مشتق آن در مبدا نیز برابر p است. در نتیجه $f(X) \in \mathcal{F}_p$. می‌توان به سادگی دید که گروه صوری لوبین‌ـ تیت $F(X,Y) = X + Y + XY$، f را به عنوان یک خودریختی می‌پذیرد. در نتیجه بنا به گزاره ۳.۴. داریم $F_f = F$. در مثال ۵.۳. دیدیم که $[a]_f(X) = (1+X)^a - 1$. در نتیجه $f^{(n)}(X) = [\pi^n]_f(X) = (1+X)^{p^n}$. در این صورت*

$$\Lambda_n = \{a \in \mathbb{Q}_p^{\mathrm{ab}} \mid (\alpha+1)^{p^n} = 1\} \cong \mu_{p^n}.$$

یک‌ریختی فوق، یک‌ریختی $\alpha \mapsto \alpha + 1$ میان دو $\mathbb{Z}_p-$مدول است.
اکنون با توجه به اثبات قضیه ۱۵.۴. می‌توان دید که

$$(\mathbb{Q}_p)_{p,n} = \mathbb{Q}_p[\Lambda_n] = \mathbb{Q}_p(\mu_{p^n}).$$

به علاوه

$$Gal((\mathbb{Q}_p)_{p,n}/\mathbb{Q}_p) \cong (\mathbb{Z}_p/\langle p^n\rangle)^\times.$$

۳.۴ قانون تقابل موضعی

در بخش قبل توسیع آبلی کاملاً منشعب K_π از میدان موضعی K را ساختیم و گروه گالوای آن را نیز شناسایی کردیم. در این بخش، پیش از آن که به قانون تقابل موضعی بپردازیم، توسیع آبلی غیرمنشعب ماکسیمال K^{un} از K را توصیف خواهیم کرد.

۱.۳.۴ توسیع غیرمنشعب ماکسیمال

از نظریهٔ میدان‌ها می‌دانیم که هر میدان متناهی k از مشخصه p، دقیقا یک توسیع جبری از درجه n دارد که از افزودن ریشه‌های $m-$ام واحد به k حاصل می‌شود که در آن m بزرگترین مقسوم‌علیه مثبت $p^n - 1$ است. از طرف دیگر از گزاره ۳۴.۱. می‌دانیم که هر توسیع غیرمنشعب یک میدان

موضعی نا‌ارشمیدسی متناظر توسیعی از میدان رده‌ای مانده‌های آن است. در نتیجه هر توسیع متناهی غیرمنشعب از K، با افزودن برخی از ریشه‌های واحد به K تولید می‌شود. به طور دقیق‌تر، فرض کنید μ_m مجموعهٔ ریشه‌های $m-$ام واحد در K^{al} باشد؛ به عبارت دیگر μ_mرا مجموعهٔ ریشه‌های چندجمله‌ای $X^m - 1$ بگیرید. اگر m بر p بخش‌پذیر نباشد، آن‌گاه توسیع $K[\mu_m]$ یک توسیع غیرمنشعب K از درجه n است که n کوچک‌ترین عدد صحیح مثبتی است که $m \mid p^n - 1$. همچنین داریم

$$Gal(K[\mu_m]/K) \cong \mathbb{Z}/n\mathbb{Z}.$$

اکنون اگر تعریف کنیم

$$K^{\mathrm{un}} := \bigcup_{p\nmid m} K[\mu_m]$$

آن‌گاه K^{un} یک توسیع غیرمنشعب از K خواهد بود میدان رده‌ای مانده‌های آن دقیقا برابر بستار جبری (جدایی‌پذیر) میدان رده‌ای مانده‌های K خواهد بود. اکنون با توجه به گزاره ۳۴.۱. نتیجه می‌گیریم که K^{un} توسیع غیرمنشعب ماکسیمال K است. پس هر توسیع غیرمنشعب K، زیرمیدانی از K^{un} خواهد بود. به علاوه به کمک حد معکوس، می‌توان گروه گالوای K^{un} را نیز مشخص کرد:

$$Gal(K^{\mathrm{un}}/K) = \varprojlim_m Gal(K[\mu_m]/K) \cong \varprojlim_m \mathbb{Z}/m\mathbb{Z} = \hat{\mathbb{Z}}.$$

با توجه به مثال ۳۷.۱.، مولد گروه گالوای هر توسیع غیرمنشعب متناهی L/K، نگاشت فروبنیوس $Frob_K$ است. بنابراین یک‌ریختی $\hat{\mathbb{Z}} \to Gal(K^{\mathrm{un}}/K)$ را می‌توان به صورت

$$a \mapsto {Frob_K}^a$$

توصیف کرد که در آن نگاشت $Frob_K$ برای هر $\zeta \in \mu_m$ به شکل

$$Frob_K(\zeta) = \zeta^{a_0}$$

تعریف می‌شود. در این‌جا a_0 می‌تواند هر عضو یک همسایگی a در $\hat{\mathbb{Z}}$ باشد که شعاع این همسایگی تابعی از m است.

۲.۳.۴ نگاشت تقابل موضعی

حال برای میدان موضعی K و عنصر اول π در آن تعریف کنید $L_\pi := K_\pi \cdot K^{\mathrm{un}}$. چون $K_\pi \cap K^{\mathrm{un}} = K$، داریم

$$Gal(L_\pi/K) \cong Gal(K_\pi/K) \times Gal(K^{\mathrm{un}}/K).$$

بنابراین برای توصیف عمل $Gal(L_\pi/K)$ روی اعضای L_π، کافی است نحوه عمل هر $\sigma \in Gal(L_\pi/K)$ را به طور مجزا روی K_π و K^{un} بررسی کنیم. در نتیجه برای تعریف یک هم‌ریختی

$$K^\times \to Gal(L_\pi/K)$$

کافی است برای هر $a \in K^\times$، اثر تصویر a تحت این هم‌ریختی را به طور جداگانه بر K_π و K^{un} تعریف کرد. از طرف دیگر نیز می‌دانیم که هر $a \in K$ را می‌توان به طور یکتا به شکل $a = u\pi^n$ نوشت که $u \in R^\times$ و $n = v_\pi(x)$. در نتیجه یک‌ریختی گروهی زیر وجود دارد:

$$K^\times \cong R^\times \times \mathbb{Z}.$$

اکنون هم‌ریختی

$$\phi_\pi : K^\times \to Gal(L_\pi/K)$$

را این‌گونه تعریف می‌کنیم که برای $a = u\pi^n \in K^\times$،

$$\phi_\pi(a)|_{K_\pi} \coloneqq Frob^n$$

و

$$\phi_\pi(a)|_{K^{\mathrm{un}}} \coloneqq [u^{-1}]_f.$$

به طور معادل، ϕ_π را می‌توان به شکل ترکیب هم‌ریختی‌های زیر نیز توصیف کرد:

$$K^\times \longrightarrow R^\times \times \mathbb{Z} \longrightarrow Gal(K_\pi/K) \times Gal(K^{\mathrm{un}}/K) \longrightarrow Gal(L_\pi/K)$$

$$u\pi^n \mapsto (u, n) \mapsto ([u^{-1}]_f, Frob^n) \mapsto \phi_\pi(u\pi^n)$$

اکنون اثبات خواهیم کرد L_π و ϕ_π هر دو مستقل از انتخاب π اند. بدین ترتیب نشان می‌دهیم که هم‌ریختی تعریف شده در بالا، از جهت آن که از هر انتخابی مستقل است، کانونی است.

فرض کنید π و $\omega = u\pi$ دو عنصر اول میدان موضعی K باشند. به علاوه $f \in \mathcal{F}_\pi$ و $g \in \mathcal{F}_\omega$، دلخواه را نیز در نظر بگیرید. برای آن که نشان دهیم L_π و L_ω یک‌ریخت اند، نشان خواهیم داد که برای هر n، میدان‌های $K_{\pi,n} \cdot K^{\mathrm{un}}$ و $K_{\omega,n} \cdot K^{\mathrm{un}}$ یکسان اند. بدین منظور کافی است نشان دهیم که F_f و F_g به عنوان قواعد جمعی $R^{\mathrm{un}}-$مدول‌های $\Lambda_{n,f}$ و $\Lambda_{n,g}$ یک‌ریخت اند که در این‌جا R^{un} حلقه اعداد صحیح K^{un} است.

میدان K^{un} اگر چه اجتماع دنباله‌ای صعودی از میدان‌های کامل است اما خود کامل نیست. در نتیجه سری‌های توانی تعریف شده روی این میدان ممکن است همگرا نشوند. به همین دلیل کامل‌سازی $\hat{K}^{\mathrm{un}}$ از K^{un} در نظر می‌گیریم و حلقهٔ اعداد صحیح آن را نیز با $\hat{R}^{\mathrm{un}}$ نمایش می‌دهیم.

گزاره ۱۷.۴.۵ *F_f و F_g روی $\hat{R}^{\mathrm{un}}$، $R-$یک‌ریخت اند. به طور دقیق‌تر، $\epsilon \in \hat{R}^{\mathrm{un}\times}$ وجود دارد که برای $Frob_K \in Gal(K^{\mathrm{un}}/K)$ داشته باشیم $Frob_K(\epsilon) = \epsilon u$. هم‌چنین $\theta(X) \in \hat{R}^{\mathrm{un}}[\![X]\!]$ وجود دارد به طوری که*

آ) $\theta(X) = \epsilon X +$ (*جملات از درجه حداقل ۲*)،

ب) $Frob_K \circ \theta = \theta \circ [u]_f$،

پ) $\theta(F_f(X,Y)) = F_g(\theta(X), \theta(Y))$،

ت) $\theta \circ [a]_f = [a]_g \circ \theta$.

اثبات. [۴] را ببینید. ■

موارد (پ) و (ت) از گزاره فوق نشان می‌دهند که θ یک $R-$هم‌ریختی میان F_f و F_g است و چون ϵ یکه است، مورد (آ) یک‌ریختی بودن θ را نتیجه می‌دهد.

لم ۱۸.۴. *هر زیرمیدان L از K^{al} که شامل K باشد، از لحاظ توپولوژیکی بسته است.*

اثبات. قرار دهید $H := Gal(K^{\mathrm{al}}/L)$. آن‌گاه H هر عضو L را ثابت نگه می‌دارد. قبلا نشان دادیم که عمل گروه گالوا پیوسته است، پس H هر عضو بستار توپولوژیک L را نیز ثابت نگه می‌دارد. اما H فقط اعضای L را ثابت نگه می‌دارد؛ در نتیجه بستار توپولوژیک L با L برابر است و لذا L بسته است. ■

قضیه ۱۹.۴. *L_π و ϕ_π مستقل از انتخاب π اند.*

اثبات. فرض کنید π و $\omega = u\pi$ دو عنصر اول K باشند. از گزاره ۱۷.۴. داریم

$$(Frob_K \circ \theta) \circ [\pi]_f = \theta \circ [u]_f \circ [\pi_f] = \theta \circ [\omega]_f = [\omega]_g \circ \theta$$

و در نتیجه

$$(Frob_K \circ \theta)(f(X)) = g(\theta(X)).$$

لذا برای هر $\alpha \in K^{\mathrm{al}}$ داریم

$$f(\alpha) = 0 \Rightarrow g(\theta(\alpha)) = 0$$

و

$$g(\alpha) = 0 \Rightarrow f\left(\theta^{-1}(\alpha)\right) = 0.$$

در نتیجه θ یک تناظر یک به یک میان $\Lambda_{f,1}$ و $\Lambda_{g,1}$ برقرار می‌سازد. بنابراین می‌توان نوشت

$$\hat{K}^{\mathrm{un}}[\Lambda_{g,1}] = \hat{K}^{\mathrm{un}}[\theta(\Lambda_{f,1})] \subset \hat{K}^{\mathrm{un}}[\Lambda_{f,1}] = \hat{K}^{\mathrm{un}}\left[\theta^{-1}(\Lambda_{g,1})\right] \subset \hat{K}^{\mathrm{un}}[\Lambda_{g,1}].$$

از عبارت فوق نتیجه می‌شود که $\hat{K}^{\mathrm{un}}[\Lambda_{g,1}] = \hat{K}^{\mathrm{un}}[\Lambda_{f,1}]$. حال به کمک لم ۱۸.۴. می‌توان نتیجه گرفت که

$$\hat{K}^{\mathrm{un}}[\Lambda_{g,1}] \cap K^{\mathrm{al}} = K^{\mathrm{un}}[\Lambda_{g,1}]$$

و

$$\hat{K}^{\mathrm{un}}[\Lambda_{f,1}] \cap K^{\mathrm{al}} = K^{\mathrm{un}}[\Lambda_{f,1}].$$

بدین ترتیب ثابت می‌شود که $K^{\mathrm{un}}[\Lambda_{g,1}] = K^{\mathrm{un}}[\Lambda_{f,1}]$.

به طریق مشابه برای هر n می‌توان نشان داد که $K^{un}[\Lambda_{g,n}] = K^{\mathrm{un}}[\Lambda_{f,n}]$. در نتیجه ثابت می‌شود که $K^{\mathrm{un}} \cdot K_\omega = K^{\mathrm{un}} \cdot K_\pi$. پس L_π مستقل از انتخاب π است.

برای آن که نشان دهیم ϕ_π مستقل از انتخاب π است، نشان می‌دهیم که برای هر دو عنصر اول π و ω، $\phi_\pi(\omega) = \phi_\omega(\omega)$. از آن‌جایی که π دلخواه است، برای هر عنصر اول دیگر مانند π' داریم

$$\phi'_\pi(\omega) = \phi_\pi(\omega) = \phi_\omega(\omega).$$

هم‌چنین چون ω نیز دلخواه است و عناصر اول مولد گروه ضربی $K^\times$ اند، پس $\phi_\pi = \phi'_\pi$. لذا کافی است که نشان دهیم $\phi_\pi(\omega) = \phi_\omega(\omega)$.

عمل هر دوی $\phi_\pi(\omega)$ و $\phi_\omega(\omega)$ بر روی K^{un} برابر عنصر فروبنیوس است. ثابت می‌کنیم که عمل این دو روی K_ω نیز یکسان است.

فرض کنید θ یک‌ریختی $F_f \to F_g$ تعریف شده در گزاره ۱۷.۴. باشد. این یک‌ریختی، برای هر n نیز یک یک‌ریختی $\Lambda_{f,n} \to \Lambda_{g,n}$ القا می‌کند. برای هر $\lambda \in \Lambda_{f,n}$ نشان می‌دهیم که

$$\phi_\pi(\omega)(\theta(\lambda)) = \theta(\lambda).$$

با این کار حکم ثابت می‌شود زیرا بنا به تعریف می‌دانیم که عمل $\phi_\omega(\omega)$ روی K_ω همانی است و $K_{\omega,n}$ توسط $\theta(\lambda)$ها تولید می‌شود. مطابق قبل فرض کنید $\omega = u\pi$. در این صورت داریم $\phi_\pi(\omega) = \phi_\pi(u) \circ \phi_\pi(\pi)$. چون ضرایب θ اعضای $\hat{R}^{\mathrm{un}}$ اند، پس $\phi_\pi(u)$ روی ضرایب θ تاثیری نمی‌گذارد. همچنین $\phi_\pi(\pi)$ روی λ تاثیری نمی‌گذارد. در نتیجه داریم

$$\begin{aligned}
\phi_\pi(\omega)(\theta(\lambda)) &= \phi_\pi(u) \circ \phi_\pi(\pi)(\theta(\lambda)) \\
&= Frob_K \circ \theta([u^{-1}]_f(\lambda)) \\
&= \theta \circ [u]_f \circ [u^{-1}]_f(\lambda) \\
&= \theta(\lambda).
\end{aligned}$$

■

قضیه زیر نشان می‌دهد که هم‌ریختی کانونی $\phi_\pi : K^\times Gal(L_\pi/K)$، همان نگاشت آرتین است. این قضیه که به قضیه کرونکر–وبر موضعی معروف است، به روش‌های مختلفی اثبات شده است که در اینجا ما از اثبات این قضیه صرف نظر می‌کنیم. علت این که این قضیه به

قضیه کرونکر–وبر موضعی معروف است، این است که این قضیه را می‌توان نسخه موضعی قضیه کرونکر–وبر دانست که بیان می‌کند هر توسیع آبلی میدان اعداد گویا، زیرمیدانی از یک توسیع دایره‌بُر است.

قضیه ۲۰.۴. ***(قضیه کرونکر–وبر موضعی)*** $L_\pi = K^{\mathrm{ab}}$.

اثبات. بخش ۴ از فصل اول [۵] را ببینید. ■

بدین ترتیب قسمت اثبات وجود و یکتایی نگاشت تقابل موضعی از قضیه زیر کامل می‌شود.

قضیه ۲۱.۴. ***(قضیه تقابل موضعی)*** *برای هر میدان موضعی نا‌ارشمیدسی K، هم‌ریختی یکتای*

$$\phi_K : K^\times \to Gal(K^{\mathrm{ab}}/K)$$

با ویژگی‌های زیر وجود دارد:

آ) *برای هر عنصر اول K و برای هر توسیع متناهی غیر منشعب L از K، $\phi_K(\pi)$ همان نگاشت $Frob_{L/K}$ است.*

ب) *برای هر توسیع متناهی آبلی L از K، هسته هم‌ریختی $a \mapsto \phi_K(a)|_L$ شامل $N_{L/K}(L^\times)$ است و در نتیجه ϕ_K یک‌ریختی زیر را القا می‌کند:*

$$\phi_{L/K} : K^\times/N_{L/K}(L^\times) \to Gal(L/K).$$

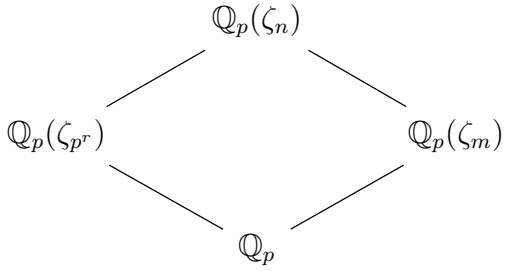
مثال ۲۲.۴. *در این مثال نگاشت تقابل موضعی را برای توسیع $L = \mathbb{Q}_p(\zeta_n)$ از میدان موضعی نا‌ارشمیدسی $\mathbb{Q}_p$ که در آن ζ_n یک ریشه اولیه $n-$ام واحد است، توصیف خواهیم کرد.*
فرض کنید $n = mp^r$ که در آن m نسبت به p اول است. در این صورت داریم

$$\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_{p^r}) \cdot \mathbb{Q}_p(\zeta_m)$$

و به علاوه $\mathbb{Q}_p(\zeta_{p^r}) \cap \mathbb{Q}_p(\zeta_m) = \mathbb{Q}_p$. پس داریم

$$Gal(L/\mathbb{Q}_p) \cong Gal(\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p) \times Gal(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p).$$

در نتیجه برای توصیف نگاشت تقابل موضعی، کافی است اثر آن را روی $\mathbb{Q}_p(\zeta_{p^r})$ و $\mathbb{Q}_p(\zeta_m)$ توصیف کنیم.



فرض کنید $a = up^t \in \mathbb{Z}_p^\times$ که در آن u یک عنصر وارون‌پذیر $\mathbb{Z}_p$ است. در این صورت $\phi_{\mathbb{Q}_p}(a)$ روی توسیع غیرمنشعب $\mathbb{Q}_p(\zeta_m)$ به شکل توان t نگاشت فروبنیوس یعنی $\zeta_m \mapsto \zeta_m^t$ و روی توسیع کاملا منشعب $\mathbb{Q}_p(\zeta_{p^r})$ به شکل $[u^{-1}]_f$ یعنی $\zeta_{p^n} \mapsto \zeta_{p^n}^{u_0^{-1}}$ عمل می‌کند که u_0 در اینجا یک عدد صحیح است که به پیمانه p^r با u هم‌نهشت است.

به علاوه از قضیه تقابل موضعی داریم:

$$Gal(L/\mathbb{Q}_p) \cong \mathbb{Q}_p^\times / N_{L/\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_n)).$$

واژه‌نامه

ارشمیدسی ..... Archimedean
ارزه ..... Valuation
اسکالر ..... Scalar
اعداد $p-$ای ..... p-adic Numbers
انشعاب ..... Ramification
ایده‌آل کسری ..... Fractional Ideal
برخه‌ریخت ..... Meromorphic
بستار جبری ..... Algebraic Closure
بستار صحیح ..... Integral Closure
تمام‌ریخت ..... Meromorphic
توسیع جدایی‌پذیر ..... Separable Extension
جمع‌وند ..... Summand
حد معکوس ..... Inverse Limit
چندجمله‌ای آیزنشتاین ..... Eisenstein Polynomial
حلقهٔ ارزهٔ گسسته ..... Discrete Valuation Ring
حلقه نوتری ..... Noetherian Ring
خم بیضوی ..... Elliptic Curve
خودریختی ..... Endomorphism
دامنه ایده‌آل اصلی ..... Princinpal Ideal Domain
دامنه ددکیند ..... Dedekind Domain
دایره‌بُر ..... Cyclotomic
دنباله دقیق ..... Exact Sequence
دنباله کوشی ..... Cauchy Sequence
دوسویی ..... Bijection
سری لوران ..... Laurent Series
غیرمنشعب ..... Non-ramified
فضای برداری ..... Vector Space
قانون تقابل موضعی ..... Local Reciprocity Law

کامل‌سازی ..... Completion
کاملا منشعب ..... Totally Ramified
کانونی ..... Canonical
گروه آبلی ..... Abelian Group
گروه صوری ..... Formal Group
گروه گالوا ..... Galois Group
گروه یکه‌های اصلی ..... Group of Principal Units
لم هنسل ..... Hensel's Lemma
ماکسیمال ..... Maximal
مدول ..... Module
موضعی‌سازی ..... Localization
میدان توابع ..... Function Field
میدان رده‌ای مانده‌ها ..... Residue Class Field
میدان شکافنده ..... Splitting Field
میدان موضعی ..... Local Field
ناارشمیدسی ..... Non-Archimedean
نُرم ..... Norm
نظریه میدان رده‌ای ..... Class Field Theory
نگاشت فروبنیوس ..... Frobenius Map
هم‌ریختی ..... Homomorphism
یک‌ریختی ..... Isomorphism
یکنواخت‌ساز ..... Uniformizer

کتاب‌نامه

[1] Cassels, J. and Fröhlich, A., eds., *Algebraic Number Theory*, Academic Press, San Diego, 1967.

[2] Gouvêa, F. Q., *p-adic Numbers, An Introduction*, Springer Nature Switzerland, 2010.

[3] Hazewinkel, M., *Formal Groups and Applications*, Academic Press, New York, 1978.

[4] Lubin, J. and Tate, J., *Formal Complex Multiplication in Local Fields*, Annals of Mathematics 81, 1965, 380-387.

[5] Milne, J., *Class Field Theory*, http://www.milne.org/math, 2020.

[6] Milne, J., *Algebraic Number Theory*, http://www.milne.org/math, 2020.

[7] Neukirch, J., *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften 322, Springer-Verlag, Berlin, Heidelberg, 1999.

[8] Riehl, E., *Lubin-Tate Formal Groups and Local Class Field Theory*, Senior Thesis, Harvard University, 2006.

[9] Serre, J-P., *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag, New York, 1973.

[10] Serre, J-P., *Local Fields*, Graduate Texts in Mathematics 67, Springer-Verlag, New York, 1979.

[11] Silverman, J., *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer, New York, 2009.

Abstract

Local class field theory is a branch of algebraic number theory that describes and classifies Galois extensions of local fields. One of the most important results of this theory is the local reciprocity law which describing it is the main purpose of this thesis. To do so, after mentioning some definitions and theorems about Dedekind domains, local field, and formal groups, we introduce Lubin-Tate formal groups and we use them to prove the existence, uniqueness, and some properties of the local reciprocity map.

College of Science
School of Mathematics, Statistics, and Computer Science

Lubin-Tate Fromal Groups and Local Class Field Theory

Mohammad Masoud Ahmadi

Supervisor:
Dr. Amir Ghadermarzi

A thesis submitted in partial fulfillment of the requirements for the degree of B.Sc. in Pure Mathematics

July 2022