دانشکده علوم

گروه ریاضی

پایان‌نامه دوره کارشناسی ارشد در رشته ریاضی محض گرایش جبر

کراندار بودن رتبه‌های موردل-ویل برخی خم‌های بیضوی و حدسیه لنگ

استاد راهنما:

دکتر علی سرباز جانفدا

نام دانشجو:

رسول دورانی

بهمن ۱۳۹۲


بسم الله الرحمن الرحیم

تقدیم به

پدر و مادر عزیز و مهربانم که معنای زندگی ام هستند

و همسر عزیز و مهربانم، یار و همراه همیشگی زندگیم . . .

سپاس گزاری...

سپاس و ستایش معبود یگانه را که پرتو الطاف بیشمارش بر لحظه لحظه زندگیام ساطع و آشکار است. حمد و ثنا می‌گذارم او را که فکرت و اندیشه را در بستر روحم روان ساخت و بهره‌گیری از خوان گسترده علم و دانش را نصیب و روزی‌ام گردانید.
با لطف و عنایت خداوند منان توانستیم این پایان‌نامه را بعد از یک سال تدوین کنیم. در طول دو سال تحصیل خودم در دانشگاه ارومیه از تجربیات استاد ارجمندم جناب آقای دکتر جانفدا، نه تنها در حیطه پایان‌نامه بلکه در امورات دیگر زندگیم، به کسرت استفاده کردم که جا دارد کمال تشکر وقدردانی را از محضر ایشان داشته باشم.
از محضر اساتید گرامی، آقایان دکتر هوشنگ بهروش و دکتر بهمن رضایی که زحمت خواندن این پایان‌نامه را کشیدند بسیار ممنونم.

همچنین از دوستان گرامی آقای مهندس محمدباقر ولیزاده و آقای اکبر خسروی که در امر تدوین پایان‌نامه مرا یاری نمودند نهایت تقدیر و تشکر را دارم.

رسول دورانی
۱۳۹۲/۱۱/۱۳

چکیده

در این پایان‌نامه نشان خواهیم داد که نوع خاصی از حدسیه لنگ در مورد نقاط گویای روی رویه‌های از نوع کلی ایجاب می‌کند که اگر مختصات x برای n نقطه‌ی گویا با $n \geq ۸$ مشخص باشد، آنگاه تنها تعداد متناهی خم بیضوی با چنین مشخصاتی وجود خواهد داشت.

فهرست مطالب

پیشگفتار

خم‌های بیضوی تاریخچه‌ای بسیار طولانی دارد. تاریخچه مطالعه آن‌ها به زمان دیوفانتس، ریاضیدانی که در سال ۲۵۰ بعد از میلاد مسیح می‌زیسته است، برمی‌گردد. دیوفانتس به دنبال یافتن جواب‌های گویای معادلات ساده‌ای مثل $x^۲ + y^۲ = z^۲$ بود. این معادلات را معادلات دیوفانتی می‌نامند. در آن زمان این معادلات به عنوان شاخه‌ای از نظریه اعداد مطرح بودند.

معادله‌ای به فرم $y^۲ = x^۳ + Ax + B$ را که در آن A و B در یک میدان K قرار دارند، خم بیضوی می‌نامیم. در این‌صورت گوییم خم E روی K تعریف شده و آن را به‌صورت $E|K$ نشان می‌دهیم. بیش از سه دهه است که خم‌های بیضوی نقش مهمی در نظریه اعداد و رمزنگاری بازی می‌کنند. به عنوان نمونه در دهه‌ی ۸۰ خم‌های بیضوی در رمزنگاری مورد استفاده قرار گرفتند. همچنین خم‌های بیضوی کاربرد فراوانی در تجزیه اعداد صحیح بزرگ به عامل‌های اول و آزمون اول بودن[۱] دارند. در دهه‌های ۸۰ و ۹۰ خم‌های بیضوی نقش اساسی در اثبات قضیه آخر فرما داشتند.

فرض کنیم E یک خم بیضوی روی میدان اعداد گویا باشد. موردل-ویل ثابت کرد که با نقاط E به انضمام یک نقطه به نام نقطه در بینهایت، گروهی تعریف می‌شود که آن را با $E(\mathbb{Q})$ نشان داده و آن را گروه موردل-ویل خم بیضوی می‌نامیم. $E(\mathbb{Q})$ یک گروه آبلی با تولید متناهی است ودر نتیجه $E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$ که در آن T زیر گروه تاب خم بوده و r رتبه خم نامیده می‌شود. در سالهای اخیر محاسبه رتبه خم بیضوی با استفاده از روش‌های ۲-کاهشی[۲] انجام شده است.

روش ۲-کاهشی که توسط بیرچ و سوینرتون[۳] برای خم‌های روی $\mathbb{Q}$ مطرح شده بود توسط سرف[۴] برای خم‌های روی میدان‌های عددی مربعی حقیقی با عدد رده‌ای یک توسعه داده شد. سیمون[۵] از توصیف روش کسلز[۶] استفاده کرده و روش ۲-کاهشی را برای خم‌های بیضوی روی میدان‌های عددی دلخواه توسعه داد. روش۲-کاهشی شامل مراحل زیر است:

- تعیین چند جمله‌ای‌های درجه چهارم مربوط به خم E که همه جا به طور موضعی حل پذیرند؛

---

[۱] primality test
[۲] 2-descent
[۳] Birch and Swinnerton
[۴] Serf
[۵] D.Simon
[۶] Cassels

- حذف چند جمله‌ای‌های درجه چهارم معادل؛ یعنی، تعیین گروه رده‌های چند جمله‌ای درجه چهارم مربوط به E که نقطه‌ای روی کامل شده‌ی K دارند؛

-یافتن جواب عمومی این چند جمله‌ای‌های درجه چهارم؛

-تعیین رتبه خم.

در فصل اول پایان‌نامه برخی از مقدمات و تعاریف مربوط به جبر و نظریه جبری اعداد که در طول پایان‌نامه مورد استفاده قرار می‌گیرند، آورده شده است. در فصل دوم مفاهیم مربوط به خم های بیضوی، معرفی گروه سلمر و تیت-شافارویچ و اثبات قضیه موردل-ویل را مورد بررسی قرار داده‌ایم. در فصل سوم که مهمترین فصل پایان‌نامه است حدسیه لنگ را در مورد نقاط گویای روی خم های بیضوی مورد بررسی قرار می‌دهیم. همچنین در این فصل خم های بیضوی با رتبه موردل-ویل بالا به روشی خاص و مشخص ساخته می‌شوند. بر این اساس واریته مشخصی تحت عنوان V_l معرفی شده و نقاط گویای روی V_l مورد بررسی قرار می‌گیرد.

این پایان‌نامه براساس مقاله زیر تهیه و تدوین گردیده است:

- Hizuru Y. *Boundedness of Mordell-Weil ranks of certain elliptic curves and Lang's conjecture*. Journal of Number Theory 100 (2003) 295-306.

فصل ۱

مفاهیم مقدماتی

در این فصل تعاریف و نتایج مقدماتی، که در فصل‌های بعدی این پایان‌نامه مورد استفاده قرار می‌گیرند آورده شده‌اند.

۱.۱ مباحثی از جبر

تعریف ۱.۱.۱. فرض کنیم K یک میدان باشد. میدان L را توسیع[۱] میدان K می‌گوییم هرگاه $K \subseteq L$. در این صورت L یک K-فضای برداری است. بعد این فضای برداری را درجه‌ی توسیع[۲] نامیده و با نماد $[L : K]$ یا $\dim_K L$ نمایش می‌دهیم. توسیع L را یک توسیع متناهی روی K می‌گوییم هرگاه $[L : K] < \infty$.

تعریف ۲.۱.۱. فرض کنیم L یک میدان توسیع از K بوده و $K[X]$ حلقه‌ی چند جمله‌ای‌های باضرایب در K باشد. عنصر $\alpha \in L$ را یک عنصر جبری[۳] روی K می‌گوییم هرگاه ریشه‌ی یک چندجمله‌ای ناصفر در $K[X]$ باشد.

تعریف ۳.۱.۱. توسیع L از میدان K را یک توسیع جبری [۴] می‌گوییم هرگاه تمامی عناصر L روی K جبری باشند.

تعریف ۴.۱.۱. فرض کنیم L یک توسیع میدان K باشد. L را بستار جبری[۵] K می‌نامیم اگر در شرایط زیر صدق کند:

---

[۱] extention
[۲] degree of extention
[۳] algebraic element
[۴] algebraic extention
[۵] algebraic closure

(۱) میدان L روی K جبری باشد؛

(۲) میدان L بسته جبری[۱] باشد؛ یعنی، هر چندجمله‌ای $f(X) \in L[X]$ روی L به عوامل خطی تجزیه شود.

تعریف ۱.۱.۵. فرض کنیم L یک توسیع میدان K باشد و $g(X) \in K[X]$. گوییم g روی L شکافته می‌شود[۲] هرگاه به ازای برخی $a \in K$ ، $\alpha_1, \cdots, \alpha_n \in L$ و $g(X) = a\prod_{i=1}^{n}(X - \alpha_i)$. علاوه بر این هرگاه داشته باشیم $L = K(\alpha_1, \cdots, \alpha_n)$ ، در این صورت L میدان شکافنده‌ی[۳] g روی K نامیده می‌شود.

تعریف ۱.۱.۶. توسیع جبری N از میدان K را یک توسیع نرمال[۴] می‌گوییم هرگاه به ازای هر چندجمله‌ای $p(x) \in K[x]$ که ریشه‌ای در N دارد، همه ریشه‌های $p(x)$ هم در N باشند.

تعریف ۱.۱.۷. فرض کنیم L یک توسیع جبری از میدان K باشد. گوییم عنصر $a \in L$ روی K تفکیک‌پذیر[۵] است، هرگاه ریشه ساده‌ای از چندجمله‌ای مینیمال خود باشد. توسیع L را یک توسیع تفکیک‌پذیر K گوییم هرگاه هر عنصر آن تفکیک‌پذیر باشد.

تعریف ۱.۱.۸. فرض کنیم K یک میدان، L یک توسیع از K و S زیر مجموعه‌ای از L باشد. گوییم S روی K وابسته‌ی جبری[۶] است اگر به ازای یک عدد صحیح مثبت n، یک چندجمله‌ای ناصفر $f \in K[x_1, \cdots, x_n]$ وجود داشته باشد که برای برخی عناصر متمایز $s_1 \cdots s_n$ از S تساوی $f(s_1 \cdots s_n) = 0$ برقرار باشد. هرگاه S روی K وابسته جبری نباشد، می‌گوییم S روی K مستقل جبری[۷] است.

تعریف ۱.۱.۹. میدان K را کامل[۸] می‌گوییم هرگاه هر توسیع جبری K، روی K تفکیک‌پذیر باشد.
فرض کنیم L یک میدان باشد. مجموعه $\mathrm{Aut}(L)$ متشکل از تمام خودریختی‌های $\delta : L \to L$ یک گروه تحت عمل ترکیب توابع تشکیل می‌دهند.

تعریف ۱.۱.۱۰. فرض کنیم E و F توسیع‌هایی از میدان K باشند. نگاشت $\delta : E \to F$ که همریختی میدانی و همچنین همریختی K-مدولی باشد یک K-همریختی نامیده می‌شود.

تعریف ۱.۱.۱۱. فرض کنیم L توسیع میدان K و σ یک خودریختی میدان L باشد و همچنین یک K-همریختی نیز باشد، در این صورت گوییم σ یک K-خودریختی است. در این صورت مجموعه تمام K-خودریختی‌های L را گروه گالوای[۹] L روی K نامیده و با نماد $G_{L/K}$ نمایش می‌دهیم.

[۱] algebraically closed
[۲] splits
[۳] spliting field
[۴] normal extention
[۵] separable
[۶] algebraically dependent
[۷] algebraically independent
[۸] prefect
[۹] galois group

تبصره **۱۲.۱.۱** . به ازای هر زیرگروه H از $G_{L/K}$ قرار می‌دهیم:

$$\mathrm{Fix}(H) = \{x \in K | \forall \sigma \in H : \sigma(x) = x\}$$

به راحتی ثابت می‌شود که مجموعه‌ی $\mathrm{Fix}(H)$ یک زیر میدان K است که آن را میدان ثابتH در L می‌نامیم. تحدید هر نگاشت $\sigma \in G_{L/K}$ به K برابر نگاشت همانی است.

تعریف ۱۳.۱.۱. توسیع جبری (متناهی و یا نامتناهی) L از میدان K را یک توسیع گالوا[۱] می‌گوییم هرگاه $K = \mathrm{Fix}(G_{L/K})$.

تعریف ۱۴.۱.۱. توسیع میدان L از میدان K را دوری می‌گوییم اگر L روی K جبری و گالوا بوده و $G_{L/K}$ یک گروه دوری باشد. هرگاه در این حالت $G_{L/K}$ یک گروه دوری متناهی از مرتبه n باشد، آنگاه می‌گوییم L یک توسیع دوری از درجه n است. پس طبق قضیه اساسی گالوا داریم: $[L : K] = n$.

تبصره **۱۵.۱.۱** . هر توسیع با بعد متناهی از یک میدان متناهی، یک توسیع دوری است.

تعریف ۱۶.۱.۱. فرض کنیم R یک حلقه‌ی جابجایی و یکدار باشد. زیرمجموعه‌ی $S \subset R$ را یک زیرمجموعه بسته ضربی[۲] می‌گوییم هرگاه $۱ \in S$ و S تحت عمل ضرب بسته باشد.
رابطه $\sim$ را روی مجموعه $R \times S$ به صورت زیر تعریف می‌کنیم:

$$(a, s) \sim (b, t) \text{ اگر و تنها اگر } \exists u \in S : (at - bs)u = ۰$$

به راحتی می‌توان نشان داد که $\sim$ یک رابطه هم‌ارزی است. کلاس هم‌ارزی (a, s) را به صورت $\frac{a}{s}$ ومجموعه تمامی کلاس‌ها را با $S^{-۱}R$ نشان می‌دهیم. با تعریف دو عمل جمع و ضرب به صورت زیر،مجموعه‌ی $S^{-۱}R$ به یک حلقه جابجایی و یکدار تبدیل می‌شود:

$$\frac{a}{s} + \frac{b}{t} = \frac{at - bs}{st}, \qquad \frac{a}{s}.\frac{b}{t} = \frac{ab}{st} \quad (a, b \in R, s, t \in S).$$

هرگاه $\mathcal{P}$ ایده‌آل اولی از R باشد آنگاه به راحتی می توان دید که $S = R - p$ یک مجموعه‌ی بسته ضربی است که در این صورت مجموعه $S^{-۱}R$ را به صورت R_p نشان می‌دهیم. همچنین می‌توان نشان داد که حلقه‌ی R_p تنها یک ایده‌آل بیشین دارد؛ یعنی، R_p یک حلقه‌ی موضعی[۳] است. روند رسیدن از R به R_p را موضعی‌سازی[۴] R در p می‌گوییم.

[۱] galois extention
[۲] multiplication closed subset
[۳] local ring
[۴] localization

تعریف ۱.۱.۱۷. فرض کنیم R یک حلقه‌ی جابجایی ویکدار باشد که شامل هیچ مقسوم‌علیه صفر نیست. در این صورت با فرض $S = R - \{0\}$ ، حلقه‌ی $S^{-1}R$ را میدان کسرهای حلقه R می‌نامیم.

۲.۱ مباحثی از نظریه‌ی جبری اعداد

تعریف ۱.۲.۱. میدان عددی[1] عبارت است از زیرمیدانی مثل K از $\mathbb{C}$ به‌طوری که $[K : \mathbb{Q}]$ متناهی است.

واضح است که اگر K میدان عددی باشد، آنگاه $K = \mathbb{Q}(\alpha_1, ..., \alpha_n)$، که در آن α_1 ، ... ، α_n اعداد جبری روی $\mathbb{Q}$ هستند. همچنین α عدد جبری است اگر و تنها اگر $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ متناهی باشد.

قضیه ۱.۲.۲. *اگر K میدان عددی باشد، آنگاه عدد جبری θ موجود است به طوری‌که $K = \mathbb{Q}(\theta)$.*

برهان. به $\left[[3]\right.$ ، قضیه ۲.۲$\left.\right]$ مراجعه شود. □

قضیه ۱.۲.۳. *فرض کنیم $K = \mathbb{Q}(\theta)$ یک میدان عددی از درجه n باشد. در این صورت دقیقاً n تکریختی متمایز $\sigma_i : K \to \mathbb{C}(i = 1, ..., n)$ وجود دارد. عناصر $\theta_i = \delta_i(\theta)$ ریشه‌های متمایز چندجمله‌ای مینیمال θ روی $\mathbb{Q}$ هستند.*

برهان. به $\left[[3]\right.$ ، قضیه ۲.۲$\left.\right]$ مراجعه شود. □

تعریف ۱.۲.۴. فرض کنیم $K = \mathbb{Q}(\theta)$ میدان عددی از درجه n باشد. مجموعه $\{\alpha_1, ..., \alpha_n\}$ را پایه‌ای برای K به عنوان فضای برداری روی $\mathbb{Q}$ در نظر می‌گیریم. مبیّن[2] این پایه به صورت زیر تعریف می‌شود:

$$\Delta[\alpha_1, ..., \alpha_n] = \{det(\sigma_i(\alpha_j))\}^2 \quad (i, j = 1, ..., n).$$

تعریف ۱.۲.۵. عدد مختلط θ را صحیح جبری می‌گوییم اگر چندجمله‌ای تکین $f(t) \in \mathbb{Z}[t]$ وجود داشته باشد به طوری‌که $f(\theta) = 0$.

نماد گذاری ۱.۲.۶. مجموعه اعداد صحیح جبری را با نماد $\mathcal{B}$ نمایش می‌دهیم.

تعریف ۱.۲.۷. فرض کنیم K میدان عددی باشد. در این صورت $\mathfrak{O} = K \cap \mathcal{B}$ زیر حلقه‌ای از میدان K می‌باشد و آن را حلقه‌ی اعداد صحیح K می‌نامیم.

[1] number field
[2] discriminant

تبصره ۸.۲.۱. واضح است $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$ و $\mathbb{Z} \subseteq \mathcal{B}$ ، بنابراین $\mathbb{Z} \subseteq \mathfrak{D}$.

قرارداد ۹.۲.۱. در اکثر کتاب‌ها و مقالات حلقه‌ی اعداد صحیح K را با نماد $\mathbb{Z}_K$ نمایش می‌دهند. از این‌رو در سراسر این پایان‌نامه، از نماد $\mathbb{Z}_K$ برای نمایش حلقه‌ی اعداد صحیح K استفاده خواهیم نمود.

تعریف ۱۰.۲.۱. میدان عددی K را میدان مربعی [۱] می‌نامیم اگر $[K : \mathbb{Q}] = ۲$.

گزاره ۱۱.۲.۱. *میدان‌های مربعی به فرم $\mathbb{Q}(\sqrt{d})$ هستند که در آن d آزاد از مربع می‌باشد.*

برهان. به [۳] ، قضیه ۳.۱ مراجعه شود. □

تعریف ۱۲.۲.۱. میدان مربعی K را یک میدان مربعی موهومی [۲] می‌گوییم هرگاه $K = \mathbb{Q}(\theta)$ به طوری‌که θ یک عدد مختلط محض باشد.

تعریف ۱۳.۲.۱. فرض کنیم K میدان عددی از درجه n باشد و $\sigma_۱$ ، ...، σ_n تکریختی‌های $K \to \mathbb{C}$ باشند. برای هر $\alpha \in K$ نرم[۳] α را به صورت زیر تعریف می‌کنیم:

$$N_K(\alpha) = \prod_{i=۱}^{n} \sigma_i(\alpha).$$

گزاره ۱۴.۲.۱. *فرض کنیم K میدان عددی و θ چندجمله‌ای مینیمال p از درجه n باشد. مبیّن[۴] پایه‌ی $\{۱, \theta, ..., \theta^{n-۱}\}$ به صورت زیر است:*

$$\Delta[۱, \theta, ..., \theta^{n-۱}] = (-۱)^{n(n-۱)/۲} N(D_p(\theta)),$$

که در آن D_p مشتق صوری p است.

برهان. به [۳] ، قضیه ۲.۱۸ مراجعه شود. □

تعریف ۱۵.۲.۱. فرض کنیم R یک دامنه‌ی صحیح باشد. گوییم R نوتری [۵] است اگر هر زنجیر صعودی از ایده‌آل‌های R متناهی باشد، یا به‌طور معادل اگر هر ایده‌آل R با تولید متناهی باشد.

تعریف ۱۶.۲.۱. فرض کنیم L میدانی شامل حلقه R باشد. $\alpha \in L$ را صحیح [۶] روی R می‌گوییم اگر α ریشه چندجمله‌ای تکین f باشد به‌طوری که $f(x) \in R[x]$.

[۱] quadratic field
[۲] imaginary quadretic field
[۳] norm
[۴] discriminant
[۵] noetherian
[۶] integral

تعریف ۱.۲.۱۷. گوییم R به‌طور صحیح بسته [۱] است اگر هر عنصر متعلق به حلقه‌ی کسرهای R، متعلق به R باشد.

تعریف ۱.۲.۱۸. حوزه صحیح R را قلمرو ددکیند [۲] گوییم اگر در شرایط زیر صدق کند:

(۱) R نوتری باشد؛

(۲) R به‌طور صحیح بسته باشد؛

(۳) هر ایده‌آل اوّل ناصفرش، ماکسیمال باشد.

گزاره ۱.۲.۱۹. *اگر K میدان عددی باشد، حلقه‌ی کسرهای میدان K، $\mathbb{Z}_K$، یک دامنه‌ی ددکیند است.*

برهان. به $\big[$[۳]، قضیه ۵.۳$\big]$ مراجعه شود. □

تعریف ۱.۲.۲۰. فرض کنیم K یک میدان عددی باشد. تابع ارزیابی گسسته [۳] روی K یک همریختی ناصفر مانند $v : K^* = K - \{0\} \to \mathbb{Z}$ با خواص زیر است:

(۱) $v(xy) = v(x) + v(y)$ ؛

(۲) $v(x+y) \geq min\{v(x), v(Y)\}$.

همچنین v همریختی صفر نبوده و تصویر v زیرگروه ناصفری از $\mathbb{Z}$ است و به ازای هر $m \in \mathbb{Z}$، به فرم $m\mathbb{Z}$ می‌باشد.

تعریف ۱.۲.۲۱. اگر در تعریف فوق قرار دهیم $m = 1$، آنگاه $v : K^* = K - \{0\} \to \mathbb{Z}$ پوشاست؛ یعنی، $v(K^*) = \mathbb{Z}$. در این حالت v را نرمال شده [۴] می‌گوییم. در غیر این صورت $x \mapsto m^{-1} \cdot v(x)$ یک ارزیابی گسسته نرمال شده خواهد بود.

تبصره ۱.۲.۲۲. با قرارداد $v(0) = \infty$ می‌توان $v : K \to \mathbb{Z}$ را نیز تعریف کرد. همچنین داریم: $v(1) = v(1 \times 1) = v(1) + v(1)$، در نتیجه $v(1) = 0$.

تعریف ۱.۲.۲۳. برای یک ارزیابی v از K ، تعریف می‌کنیم:

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

چون $v(1) = 0$، پس $1 \in \mathcal{O}_v$. اگر $x, y \in \mathcal{O}_v$، آنگاه طبق تعریف داریم:

$$x + y \in \mathcal{O}_v, xy \in \mathcal{O}_v$$

[۱] integrally closed
[۲] dedekind
[۳] discrete valuation
[۴] normalized

از این رو $\mathcal{O}_v$ یک حلقه است. به $\mathcal{O}_v$ حلقه ارزیابی[۱] v در K می‌گوییم.

تعریف ۲۴.۲.۱. دامنه‌ی صحیح R را یک حلقه ارزیابی گسسته[۲] ، DVR، گوییم هرگاه یک تابع ارزیابی گسسته v از میدان کسرهای R موجود باشد به‌طوری که

$$R = \{x \in K | v(x) \geq ۰\}$$

تبصره ۲۵.۲.۱ . چون یک DVR، یک حلقه ارزیابی است پس یک حلقه موضعی است. حال فرض کنیم ایده‌آل ماکسیمال R برابر m باشد. همچنین فرض کنیم $x \in R$ وارون‌پذیر باشد. بنابراین $x^{-۱} \in R$ و داریم:

$$۰ = v(۱) = v(xx^{-۱}) = v(x) + v(x^{-۱})$$

حال چون طبق تعریف $v(x) \geq ۰$، پس رابطه فوق معادل با $v(x) = ۰$ می‌باشد. از این رو m برابر است با مجموعه عناصر وارون ناپذیر R و داریم

$$\begin{aligned} m &= \{x \in K \mid v(x) \geq ۰\}, \\ &= \{x \in R \mid v(x) \geq ۰\}. \end{aligned}$$

حال قرار می‌دهیم $P_v = \{x \in K | v(x) > ۰\}$. این مجموعه یک $\mathcal{O}_v$-ایده‌آل است. به‌علاوه ایده‌آل سره نیز می‌باشد. چون $۱ \in \mathcal{O}_V$ و $۱ \notin P_v$. به عبارت دیگر، P_v ناصفر است. چون V پوشاست پس می‌توان $x \in K$ پیدا کرد که $v(x) = ۱$.

تعریف ۲۶.۲.۱. P_v معرفی شده در ۲۵.۲.۱ را ایده‌آل ارزیابی[۳] v می‌نامیم.

حال فرض کنیم $x, y \in \mathcal{O}_v$. اگر $xy \in P_v$ ، آنگاه $v(xy) = v(x) + v(y) > ۰$. پس $v(x) \geq ۰$، $v(y) \geq ۰$. بنابراین $v(x) > ۰$ یا $v(y) > ۰$. پس $x \in P_v$ یا $y \in P_v$. در نتیجه P_v یک ایده‌آل اول است.

تعریف ۲۷.۲.۱. فضای متری A را تام[۴] می‌گوییم هرگاه هر دنباله‌ی کوشی در A همگرا باشد. هرگاه A تام نباشد با افزودن حد همه‌ی دنباله‌های کوشی به آن یک فضای تام به دست می‌آید که کامل شده‌ی[۵]

[۱] valuation ring
[۲] discrete valuation ring
[۳] valuation ideal
[۴] complete
[۵] completion

A یا متمم سازی A نام دارد.

با توجه به تعریف، کامل شده‌ی یک فضای متری بستگی به متری دارد که در نظر می‌گیریم. به عنوان مثال، اگر $\mathbb{Q}$ را با متر متعارف در نظر بگیریم، کامل شده‌ی آن برابر $\mathbb{R}$ است. در حالی که با در نظر گرفتن متر p-ای، که در ادامه معرفی می‌شود، کامل شده‌ی آن برابر میدان $\mathbb{Q}_p$ است.

تعریف ۲۸.۲.۱. فرض کنیم p یک عدد اول ثابتی بوده و $\alpha \in \mathbb{Q}^*$ دلخواه باشد. در این صورت به طور منحصر به فردی می‌توان نوشت:

$$a = p^r \frac{m}{n}, \quad r \in \mathbb{Z},\ m, n \in \mathbb{Z}, \quad p \nmid m,\ p \nmid n.$$

نگاشت‌های $||.||_p : \mathbb{Q} \to \mathbb{R}^+, v_p : \mathbb{Q} \to \mathbb{Z}$ را به صورت زیر تعریف می‌کنیم:

$$v_p(a) = r,\ v_p(۰) = \infty,\ v_p(\infty) = ۰,$$

$$||a||_p = p^{-v_p(a)},\ ||۰||_p = ۰,\ ||\infty||_p = \infty.$$

به عنوان مثال می‌توان نوشت:

$$v_۷(\frac{۶۸۶}{۱۵}) = ۳ \quad , \quad v_۵(\frac{۲۱}{۱۴۰}) = -۱,$$

$$||\frac{۶۸۶}{۱۵}||_۷ = \frac{۱}{۳۴۳} \quad , \quad ||\frac{۲۱}{۱۴۰}||_۵ = ۵.$$

لم ۲۹.۲.۱. *به ازای هر عدد ثابت p، نگاشت $||.||_p$ در خواص زیر صدق می‌کند:*

(۱) $||a||_p = ۰, ||-a||_p = ||a||_p$ *اگر و تنها اگر* $a = ۰$؛

(۲) *به ازای هر* $a, b \in \mathbb{Q}$، $||ab||_p = ||a||_p||b||_p$؛

(۳) *به ازای هر* $a, b \in \mathbb{Q}$، $||a+b||_p \leq \max\{||a||_p, ||b||_p\}$؛

(۴) *نگاشت* $d_p(a,b) = ||a-b||_p$ *یک متر روی* $\mathbb{Q}$ *می‌باشد.*

برهان. در حالتی که $p = \infty$، تمامی عبارات از خواص قدر مطلق معمولی نتیجه می‌شود. بنابراین فرض کنیم $p < \infty$ یک عدد اوّل باشد. در این صورت قسمت (۱) از تعریف نگاشت $||.||_p$ نتیجه

می‌شود. فرض کنیم $a, b \in \mathbb{Q}$ دارای نمایش‌های زیر باشند:

$$a = p^r \frac{m}{n}, \quad r \in \mathbb{Z}, \quad m, n \in \mathbb{Z}, \quad p \nmid m, p \nmid n,$$
$$b = p^s \frac{u}{w}, \quad s \in \mathbb{Z}, \quad u, w \in \mathbb{Z}, \quad p \nmid u, p \nmid w.$$

در این صورت نتیجه می‌شود:

$$ab = p^{r+s} \frac{mu}{nw}, \quad v_p(ab) = r + s = v_p(a) + v_p(b),$$
$$||ab||_p = P^{-v_p(ab)} = p^{-[v_p(a)+v_p(b)]} = p^{-v_p(a)} p^{-v_p(b)} = ||a||_p ||b||_p.$$

بنابراین قسمت (۲) اثبات می‌شود.
حال فرض کنیم $s \geq r$؛ یعنی، $||a||_p \leq ||b||_p$. به راحتی می‌توان دید:

$$a + b = p^r \frac{mw + p^{s-r} nu}{bnw},$$

در این صورت $p \nmid nw$. چون در غیر این صورت $p \nmid n$ یا $p \nmid w$ که هریک، به ترتیب، متناقض با تعریف $||a||_p$ و $||b||_p$ می‌باشند. صورت کسر $\frac{mw+p^{s-r}nu}{bnw}$ یک عدد صحیح است اما احتمالاً برای حالت $s = r$ بر p بخش‌پذیر باشد. پس نتیجه می‌شود $||a + b||_p \leq p^{-r} = ||a||_p$. به طور مشابه می‌توان دید $||a+b||_p \leq p^{-s} = ||b||_p$. بنابراین نامساوی قسمت (۳) نتیجه می‌شود. متر بودن نگاشت d_p را می‌توان از قسمت‌های قبل نتیجه گرفت. □

تعریف ۳۰.۲.۱. نگاشت $||.||_p$ را ارزیابی p-ای[۱] روی $\mathbb{Q}$ می‌نامیم.

تعریف ۳۱.۲.۱. کامل شده‌ی میدان $\mathbb{Q}$ توسط متر d_p را میدان اعداد p-ای[۲] گفته و به صورت $\mathbb{Q}_p$ نشان می‌دهیم.

قرارداد ۳۲.۲.۱. در حالتی که $p = \infty$، کامل شده‌ی $\mathbb{Q}$ میدان اعداد حقیقی $\mathbb{R}$ می‌باشد. بنابراین قرارداد می‌کنیم که $\mathbb{Q}_\infty = \mathbb{R}$.

تعریف ۳۳.۲.۱. به ازای هر عدد اوّل p، $\mathbb{Z}_p$ راحلقه‌ی اعداد صحیح p-ای[۳] و گروه ضربی $\mathbb{Z}_p^*$ را گروه یکه‌های p-ای[۴] حلقه‌ی $\mathbb{Z}_p$ می‌گوییم.

[۱] p-adic valution
[۲] p-adic numbers field
[۳] p-adic integers
[۴] p-adic units

تعریف ۳۴.۲.۱. هر ایده‌آل $\mathcal{I}$ از حلقه $\mathbb{Z}_p$ را به صورت یکتا می‌توان به حاصل‌ضرب ایده‌آل‌های اوّل از آن حلقه تجزیه نمود. به عبارت دیگر،

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

که حاصل‌ضرب روی مجموعه‌ی متناهی از ایده‌آل‌های اوّل تعریف شده است و توان‌های $v_{\mathfrak{p}}(\mathcal{I})$ متعلق به $\mathbb{Z}$ هستند. مقدار $v_{\mathfrak{p}}(\mathcal{I})$ را ارزیابی $\mathfrak{p}$-ای[۱] می‌گوییم هرگاه در شرایط زیر صدق کند:

(۱)به ازای هر ایده‌آل $\mathcal{I}, \mathcal{J}$، $v_{\mathfrak{p}}(\mathcal{I}\mathcal{J}) = v_{\mathfrak{p}}(\mathcal{I}) + v_{\mathfrak{p}}(\mathcal{J})$؛

(۲) $v_{\mathfrak{p}}(\mathcal{I} + \mathcal{J}) = min(v_{\mathfrak{p}}(\mathcal{I}), v_{\mathfrak{p}}(\mathcal{J}))$.

تعریف ۳۵.۲.۱. فرض کنیم R دامنه‌ی صحیح و K میدان کسرهای آن باشد. یک R- زیر مدول $\mathfrak{a}$ از میدان K را ایده‌آل کسری[۲] R می‌نامیم اگر عنصر ناصفر $c \in R$ وجود داشته باشد به‌طوری‌که $c\mathfrak{a} \subset R$. به عبارت دیگر، $\mathfrak{b} = c\mathfrak{a}$ یک ایده‌آل از R است و $\mathfrak{a} = c^{-1}\mathfrak{b}$.

تعریف ۳۶.۲.۱. اگر در تعریف فوق قرار دهیم $c = 1$، ایده‌آل کسری، یک ایده‌آل معمولی است و آن را ایده‌ال صحیح[۳] می‌نامیم.

در حالت کلّی یک ایده‌آل به وضوح یک ایده‌آل کسری است و برعکس، یک ایده‌آل کسری $\mathfrak{a}$ ایده‌آل است اگر و تنها اگر $\mathfrak{a} \subset R$. حاصل‌ضرب ایده‌آل‌های کسری، یک ایده‌آل کسری است. ضرب ایده‌آل‌های کسری جابه‌جایی و شرکت‌پذیر است و عنصر همانی آن R می‌باشد. در نتیجه قضیه زیر را داریم:

قضیه ۳۷.۲.۱. *ایده‌آل‌های کسری R تشکیل گروه آبلی تحت عمل ضرب ایده‌آل‌ها می‌دهند.*

برهان. به [۳]، قضیه ۵.۵ مراجعه شود. □

تعریف ۳۸.۲.۱. فرض کنیم K میدان عددی و $\mathbb{Z}_K$ حلقه‌ی اعداد صحیح K باشد. یک ایده‌آل کسری $\mathbb{Z}_K$ را اصلی[۴] می‌گوییم هرگاه به فرم $c^{-1}\mathfrak{a}$ باشد که در آن $0 \neq c \in \mathbb{Z}_K$ و $\mathfrak{a}$ یک ایده‌آل اصلی $\mathbb{Z}_K$ است.

تعریف ۳۹.۲.۱. فرض کنیم K یک میدان عددی و $\mathbb{Z}_K$ حلقه‌ی اعداد صحیح آن باشد. برای هر ایده‌آل $\mathfrak{a}$ از $\mathbb{Z}_K$، وارون یک ایده‌آل[۵] را به صورت زیر تعریف می‌کنیم:

$$\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subseteq \mathbb{Z}_k\}$$

[۱] p-adic valuation
[۲] fractional ideal
[۳] integral ideal
[۴] principal
[۵] inverse of ideal

. واضح است که $\mathfrak{a}^{-1}$[۱] یک $\mathbb{Z}_K$ ـ زیر مدول است.

تعریف ۴۰.۲.۱. فرض کنیم $\mathfrak{a}$ ایده‌آل کسری دامنه‌ی صحیح R باشد. گوییم $\mathfrak{a}$ ایده‌آل وارون‌پذیر[۱] است اگر یک ایده‌آل کسری $\mathfrak{b}$ از R وجود داشته باشد به طوری‌که $R = \mathfrak{ab}$. ایده‌آل کسری $\mathfrak{b}$ را وارون ایده‌آل $\mathfrak{a}$ می‌نامیم.

تعریف ۴۱.۲.۱. فرض کنیم K میدان عددی و $\mathbb{Z}_K$ حلقه اعداد صحیح آن باشد. فرض کنیم $\mathfrak{a}$ ایده‌آل کسری $\mathbb{Z}_K$ باشد. نرم ایده‌آل[۲] $\mathfrak{a}$ را به صورت زیر تعریف می‌کنیم:

$$N(\mathfrak{a}) = \left|\frac{\mathbb{Z}_K}{\mathfrak{a}}\right|$$

$N(\mathfrak{a})$ یک عدد صحیح مثبت است.

قضیه ۴۲.۲.۱. (۱) *هر ایده‌آل $\mathfrak{a}$ از $\mathbb{Z}_K$ با $\mathfrak{a} \neq 0$، $\mathbb{Z}$ـ پایه $\{\alpha_1, ..., \alpha_n\}$ دارد که در آن n درجه میدان K می‌باشد.*

(۲) *داریم:*

$$N(\mathfrak{a}) = \left|\frac{\Delta[\alpha_1, ..., \alpha_n]}{\Delta}\right|^{1/2}$$

که Δ مبیّن میدان K است.

نتیجه زیر ارتباط بین نرم ایده‌آل حلقه و نرم عضو حلقه را بیان می کند.

نتیجه ۴۳.۲.۱. *اگر $\mathfrak{a} =< a >$ یک ایده آل اصلی باشد، آن‌گاه $N(\mathfrak{a}) = |N(a)|$.*

تعریف ۴۴.۲.۱. فرض کنیم K یک میدان عددی باشد. یک مرتبه[۳] R در K، زیر حلقه‌ای از K می‌باشد که به‌عنوان یک $\mathbb{Z}$ ـ مدول، با تولید متناهی بوده و از رتبه‌ی بیشین $n = deg(K)$ می‌باشد.

تعریف ۴۵.۲.۱. فرض کنیم $\mathcal{I}_K$ مجموعه‌ی ایده‌آل‌های کسری K و $\mathcal{P}_K$ مجموعه‌ی ایده‌آل‌های کسری اصلی K باشد. گروه رده‌ای[۴] K را به‌صورت زیر تعریف می‌کنیم:

$$cl(K) = \frac{\mathcal{I}_K}{\mathcal{P}_K}$$

[۱] invertible ideal
[۲] ideal norm
[۳] order
[۴] class group

مرتبه‌ی این گروه را عدد رده‌ای[۱] نامیده و با نماد $h(K)$ نمایش می‌دهیم. گروه رده‌ای را می‌توان به روشی دیگر هم تعریف نمود. در ادامه این روش را بیان می‌کنیم.

تعریف ۱.۲.۴۶. فرض کنیم $\mathcal{I}_K$ مجموعه‌ی ایده‌آل‌های کسری K باشد. رابطه هم‌ارزی $\sim$ را به صورت زیر تعریف می‌کنیم:

$\xi \sim \eta$ اگر و تنها اگر ایده‌آل‌های اصلی $\mathfrak{b}$ و $\mathfrak{c}$ وجود داشته باشند به‌طوری‌که $\xi b = \eta c$

مجموعه‌ی رده‌های هم‌ارزی $[\xi]$ با عمل $[\xi][\eta] = [\xi\eta]$ تشکیل یک گروه می‌دهند. این گروه را گروه رده‌ای نامیده و با نماد $\mathrm{cl}(K)$ نمایش می‌دهیم.

قضیه ۱.۲.۴۷. *برای میدان عددی K، گروه رده‌ای $\mathrm{cl}(K)$ یک گروه آبلی متناهی است.*

برهان. به [۳]، قضیه ۹.۷ مراجعه شود. □

قضیه ۱.۲.۴۸. *$\mathbb{Z}_K$ یک دامنه‌ی تجزیه‌ي یکتا است اگر و تنها اگر $h(K) = ۱$.*

برهان. به [۳]، قضیه ۹.۷ مراجعه شود. □

تبصره ۱.۲.۴۹. اگر $\mathcal{I}_K$ مجموعه‌ی ایده آل‌های کسری K و $\mathcal{P}_K$ مجموعه‌ی ایده‌آل‌های کسری اصلی K باشد، به وضوح دنباله‌ی دقیق زیر را داریم:

$$۱ \to \mathcal{P}_K \to \mathcal{I}_K \to cl(K) \to ۱$$

همچنین می‌توان گروه رده‌ای را برای یک مرتبه R در K که مرتبه بیشین نیست، هم تعریف نمود.

تعریف ۱.۲.۵۰. فرض کنیم R یک مرتبه در K باشد که لزوماً بیشین نیست. مجموعه‌ی همه رده‌های هم‌ارزی از ایده‌آل‌های وارون‌پذیر R را گروه رده‌ای R نامیده و با نماد $\mathrm{cl}(R)$ نمایش می‌دهیم.

فرض کنیم $f(x) = a_۰ + a_۱x + ... + a_nx^n$ چندجمله‌ای متعلق به $F[x]$ باشد. برای هر چندجمله‌ای ناصفر، میدان Lی وجود دارد که بستار جبری F یا میدان شکافنده f روی F است. بنابراین در $L[x]$ داریم:

$$f(x) = c\prod_{j=۱}^{n}(x - \alpha_j) \quad (c \neq ۰).$$

[۱] class number