بسم الله الرحمن الرحیم

دانشکده علوم
گروه ریاضی
ارومیه – ایران

عنوان:

اعداد همنهشت روی میدان‌های درجه دوّم حقیقی

استاد راهنما:
دکتر علی سرباز جانفدا

دانشجو:
نازیلا واعظ موسوی

پایان نامه
جهت اخذ درجه کارشناسی ارشد

تابستان ۱۳۸۹

پایان نامه خانم : **نازیلا واعظ موسوی** به تاریخ **۱۷ /۸۹/۶** شماره **۱۰۴۹-۲**

مورد پذیرش هیات محترم داوران با رتبه عالی و نمره ۱۸٫۳ (به حروف هیجده [illegible])

قرار گرفت.

۱- استاد راهنما و رئیس هیئت داوران: دکتر علی سرباز جانفدا

۲- داور خارجی: دکتر محسن قاسمی

۳- داور داخلی: دکتر هوشنگ بهروش هوشنگ بهروش

۴- نماینده تحصیلات تکمیلی: دکتر حبیب اذانچیلر اذانچیلر

تقدیم به گنجینه های زندگی ام:

مادر و پدر مهربانم

خواهر و برادر عزیزم

قدردانی و تشکر

خدای مهربان را شاکرم که به اینجانب توفیق داد تا این مقطع تحصیلی را به پایان برسانم که اگر عنایت الهی نبود توان مقابله با مشکلات عدیده دوران تحصیل برایم میسر نبود.
از استاد راهنمای بزرگوارم آقای دکتر علی سربازجانفدا که همواره از حمایت‌های ایشان برخوردار بوده‌ام سپاس‌گذاری می‌کنم.
از جناب آقای دکتر هوشنگ بهروش و آقای دکتر محسن قاسمی که زحمت داوری این پایان نامه را بر عهده داشتند قدردانی می‌کنم.
از خانواده‌ام که همیشه همراهم بوده‌اند تشکر می‌کنم از دوستان و همکلاسی‌های عزیزم‌خانم‌ها و آقایان سپیده حسینی، اهدا حقیقی، رویا قربانی، پریناز ابراهیم‌زاده، زینب میرعلی‌اشرفی، فائزه خراسانی‌کیا، زهرا مرقاتی،الهام ملکی، الهام یوسف‌زاده، محمد احمدپور، صادق محمدی‌خواه، رضابابابیان، تورج صمدی، مصیب ملکی که همیشه مشوق و همراه من بودند نهایت تشکر را دارم.

فهرست مندرجات

چکیده

فرض می‌کنیم $m \neq ۱$ یک عدد صحیح مثبت خالی از مربع باشد. گوییم که یک عدد صحیح مثبت n یک عدد همنهشت روی $\mathbb{Q}(\sqrt{m})$ می‌باشد اگر مساحت یک مثلث قائم‌الزاویه با اضلاع در $\mathbb{Q}(\sqrt{m})$ باشد. قرار می‌دهیم $K = \mathbb{Q}(\sqrt{m})$. اثبات می‌کنیم که اگر $m \neq ۲$، در این صورت n یک عدد همنهشت روی K است اگروتنهااگر $E_n(K)$ دارای یک rank مثبت باشد. که $E_n(K)$ نشان‌دهنده‌ی گروهی از $K-$نقاط گویا روی خم بیضوی E_n که به وسیله‌ی $y^۲ = x^۳ - n^۲x$ تعریف می‌شود.بعلاوه، مثلث‌های قائم‌الزاویه با اضلاع در K و مساحت n را رده‌بندی می‌کنیم.

پیشگفتار

خم‌های بیضوی تاریخچه‌ای بسیار طولانی دارند. تاریخچه مطالعه‌ی آن‌ها به زمان دیوفانتوس، ریاضیدانی که در سال ۲۵۰ بعد از میلاد مسیح می‌زیسته است، برمی‌گردد. دیوفانتوس به‌دنبال یافتن جواب‌های گویای معادلات ساده‌ای مثل $x^۲ + y^۲ = z^۲$ بود. این معادلات را معادلات دیوفانتوسی می‌نامند. در آن زمان این معادلات به‌عنوان شاخه‌ای از نظریه‌ی اعداد مطرح بودند.

معادله‌ای به فرم

$$y^۲ = x^۳ + Ax + B \quad (A, B \in \mathbb{Z})$$

یعنی، معادله دیوفانتوسی دو متغیره‌ای که حداقل توان یکی از متغیرهای آن بزرگتر مساوی ۳ باشد، را خم بیضوی می‌نامیم. بیش از دو یا سه دهه است که خم‌های بیضوی در رمزنگاری مورد استفاده قرار گرفته‌اند. در این پایان‌نامه می‌خواهیم ارتباط بین خم‌های بیضوی و اعداد همنهشت را بیان کنیم. این پایان‌نامه در پنج فصل تدوین شده است که به‌صورت زیر می‌باشند.

در فصل اول، مباحثی از جبرپیشرفته و نظریه اعداد بیان شده است. در فصل دوم و سوم، خم بیضوی E را روی میدان اعداد گویا در نظر گرفته و ساختار $E(\mathbb{Q})$ را مورد بررسی و مطالعه قرار داده‌ایم. بنابر قضیه‌ی موردِل—وِیل این گروه با یک گروه آبلی با تولید متناهی یکریخت می‌باشد. در فصل چهارم، فرض می‌کنیم n یک عدد صحیح مثبت و خالی از مربع باشد. در این صورت n یک عدد همنهشت نامیده می‌شود هرگاه n برابر با مساحت یک مثلث قائم‌الزاویه با اضلاع گویا باشد در

غیر این صورت n عددی ناهمنهشت خواهد بود. و ثابت می‌کنیم که n یک عدد همنهشت روی $K=\mathbb{Q}(\sqrt{m})$ است اگر و تنها اگر $E_n(K)$ یک نقطه از مرتبه‌ی نامتناهی داشته باشد. به عبارت دیگر، n یک عدد همنهشت روی $K=\mathbb{Q}(\sqrt{m})$ است اگر و تنها اگر $\operatorname{rank}\big(E_n(K)\big) > 0$.

در فصل پنج، به بیان قضیه‌ای برای رده‌بندی مثلث‌های قائم‌الزاویه می‌پردازیم و سپس مثال‌های در این مورد ارائه می‌کنیم.

فصل ۱

مقدمات و پیش نیازها

۱.۱ مباحثی از جبر

در این فصل هدف یادآوری برخی از تعاریف، قضایا و مفاهیم اساسی و مورد نیاز در این پایان‌نامه، نظیر تعاریف و قضایایی در مورد توسیع میدان‌ها و نظریهٔ گالوا می‌باشد.

تعریف ۱.۱.۱. میدان E را یک توسیع میدان[۱] F می‌نامیم و می‌نویسیم E/F، هرگاه $F \subseteq E$. بنابراین هر میدان شامل F یک توسیع میدان F نامیده می‌شود.

تعریف ۲.۱.۱ فرض می‌کنیم E/F یک توسیع میدان است. بعد E به‌عنوان فضای برداری روی F را درجهٔ توسیع می‌نامیم و با $[E:F]$ نمایش می‌دهیم. درواقع داریم $[E:F] = \dim_F E$ که اگر متناهی باشد توسیع E/F را یک توسیع متناهی می‌نامیم، در غیر اینصورت توسیع را نامتناهی می‌نامیم.

تعریف ۳.۱.۱ فرض می‌کنیم E/F یک توسیع میدان و X زیر مجموعه‌ای از E است. اشتراک تمام زیر میدانهای E را که شامل $F \cup X$ باشد با $F(X)$ نمایش می‌دهیم و آن را توسیع F تولید شده توسط X می‌نامیم.

---

[۱] field extension

درحالتی که $X = \{a_1, \ldots, a_n\}$ یک مجموعهٔ متناهی باشد قرار می‌دهیم $F(X) = F(a_1, a_2, \ldots, a_n)$ و آن را یک توسیع به طور متناهی تولید شده F می‌نامیم.

اگر $X = a$ آنگاه $F(X) = F(a)$ یک توسیع ساده F نامیده می‌شود. در این حالت a یک عنصر اولیهٔ $F(a)$ نامیده می‌شود. $F(X)$ کوچک‌ترین زیر میدان E شامل F و X است. همچنین داریم $F(a_1, \ldots, a_n) = F(a_1, \ldots, a_{n-1})(a_n)$.

تعریف ۴.۱.۱ فرض می‌کنیم E/F یک توسیع میدان است. گوییم $a \in E$ روی F جبری است، هرگاه چندجمله‌ای $0 \neq f(x) \in F(x)$ وجود داشته باشد، به‌طوریکه $f(a) = 0$. اگر $a \in E$ روی F جبری نباشد گوییم a روی F متعالی است. توسیع E/F را یک توسیع جبری نامیم هرگاه هر عضو E روی F جبری باشد.

تعریف ۵.۱.۱ گوییم $\alpha \in \mathbb{Q}$ یک عدد جبری است، هرگاه α یک عدد جبری روی $\mathbb{Q}$ باشد؛ یعنی، $0 \neq f(x) \in \mathbb{Q}[x]$ وجود داشته‌باشد، به‌طوریکه $f(\alpha) = 0$. در غیر اینصورت α یک عدد متعالی نامیده می‌شود. هرگاه $0 \neq f(x) \in \mathbb{Z}[x]$ تکین وجود داشته باشد، به‌طوری‌که $f(\alpha) = 0$، آن‌گاه گوییم α یک عدد صحیح جبری است. هر توسیع متناهی $\mathbb{Q}$ را یک میدان جبری حسابی می‌نامیم.

تعریف ۶.۱.۱ فرض می‌کنیم E/F و K/F توسیع میدان هستند. یک F–همریختی عبارت است از همریختی ناصفر $\sigma : E \to K$ به‌طوری‌که برای هر $a \in F$ داشته باشیم $\sigma(a) = a$. چون σ ناصفر فرض شده است، پس یک نشاندن E در K است، که آنرا نشاندن E در K، روی F می‌نامیم.

تعریف ۷.۱.۱ فرض می‌کنیم F یک میدان و $f(x) \in F[x]$ یک چند جمله‌ای از درجهٔ حداقل یک باشد. توسیع E/F یک میدان شکافنده[۲] $f(x)$ روی F نامیده می‌شود هرگاه شرایط زیر برقرار

[۲] splitting field

باشد:

(۱) $f(x) = a(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$ که در آن $a \in F$ و به‌ازای هر $i = 1, \dots, n$، $\alpha_i \in E$.

(۲) $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

تعریف ۸.۱.۱ مجموعهٔ تمام F–خودریختی‌های میدان E را با $\mathrm{Gal}(E/F)$ نمایش می‌دهیم؛ یعنی،

$$\mathrm{Gal}(E/F) = \{\sigma \in \mathrm{Aut}(E) | \sigma(a) = a, \forall a \in F\}.$$

ادعا می‌کنیم که مجموعهٔ فوق زیرگروهی از $\mathrm{Aut}(E)$ است. فرض می‌کنیم $\sigma \in \mathrm{Aut}(E)$ آن‌گاه باید داشته باشیم:

$$\sigma(a+b) = \sigma(a) + \sigma(b),$$

$$\sigma(ab) = \sigma(a)\sigma(b) \quad \forall a, b \in E.$$

چون نگاشت همانی روی E یک F–خودریختی از E است پس $\mathrm{Gal}(E/F)$ زیر مجموعه‌ای ناتهی از $\mathrm{Aut}(E)$ می‌باشد. اکنون اگر $\sigma, \tau \in \mathrm{Gal}(E/F)$، آنگاه $\sigma, \tau \in \mathrm{Aut}(E)$ و $\sigma(a) = a$ و $\tau(a) = a$ برای هر $a \in F$. در نتیجه $\sigma^{-1}(a) = \sigma^{-1}(\tau(a)) = \sigma^{-1}\tau(a)$. پس $\sigma^{-1}\tau \in \mathrm{Gal}(E/F)$ که ثابت می‌کند $\mathrm{Gal}(E/F) \leq \mathrm{Aut}(E)$.

تعریف ۹.۱.۱ فرض می‌کنیم E/F توسیع میدان است. در این صورت $\mathrm{Gal}(E/F)$ را گروه گالوای[۳] E روی F می‌نامیم. اگر $f(x) \in F[x]$ و E میدان شکافندهٔ $f(x)$ روی F باشد آن‌گاه گروه گالوای معادله $f(x) = 0$ که با G_f نمایش می‌دهیم عبارتست از گروه گالوای E روی F.

قضیه ۱۰.۱.۱ فرض می‌کنیم F یک میدان و $f(x) \in F[x]$ یک چندجمله‌ای تفکیک‌پذیر باشد. اگر E میدان شکافنده $f(x)$ روی F فرض شود، آن‌گاه داریم $|\mathrm{Gal}(E/F)| = [E:F]$. در

[۳] galois group

واقع $\mathrm{Gal}(E/F)$ بنابه تعریف، گروه گالوای $f(x)$ روی F است.

اثبات : به [۱، فصل دوازده، نتیجهٔ ۶.۲]، مراجعه شود. □

قضیه ۱۱.۱.۱ فرض می‌کنیم p یک عدد اول است و

$$g(x) = 1 + x + \ldots + x^{p-1}.$$

دراین‌صورت $g(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

اثبات : به [۱]، مراجعه کنید. □

قضیه ۱۲.۱.۱ فرض می‌کنیم p یک عدد اول است و قرار می‌دهیم $\alpha = e^{\frac{2\pi i}{p}}$. آنگاه

$$\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}_{p-1}.$$

اثبات : چون $\alpha = e^{\frac{2\pi i}{p}}$ بنابراین داریم $\alpha^p = 1$. بنابراین α یک ریشهٔ $x^p - 1$ است. از طرفی $x^p - 1 = (x-1)f(x)$ که $f(x) = x^{p-1} + \ldots + x + 1$ است و بنابه قضیهٔ ۱۱.۱.۱، $f(x)$ تحویل‌ناپذیر است. لذا به‌ازای هر $n = 1, 2, \ldots, p-1$،

$$\alpha^n = \cos(\tfrac{2\pi n}{p}) + i\sin(\tfrac{2\pi n}{p}),$$

ریشه‌های $f(x)$ هستند. خودریختی σ_n در $\mathbb{Q}(\alpha)$ را به‌ازای هر $n = 1, 2, \ldots, p-1$، چنین تعریف می‌کنیم $\sigma_n(\alpha) = \alpha^n$. بدیهی است که این خودریختی‌ها متمایزو متعلق به $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ هستند. چون بنابر قضیهٔ ۱۰.۱.۱،

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = p - 1,$$

σ_i ها همگی در $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ هستند. چون α مولد گروه گالوا است، لذا $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}_{p-1}$.

□

تعریف ۱۳.۱.۱ فرض می‌کنیم R یک حلقه‌ی جابجایی و یکدار باشد. زیرمجموعه‌ی

$S \subset R$ را یک زیرمجموعه‌ی بسته‌ی ضربی[۴] می‌گوییم. هرگاه $S \ni 1$ و S تحت عمل ضرب بسته باشد. رابطه‌ی $\sim$ را روی مجموعه‌ی $R \times S$ به صورت زیر تعریف می‌کنیم:

$$(a,s) \sim (b,t) \quad \text{اگروتنهااگر} \quad \exists \quad u \in S: \quad (at-bs)u = 0$$

به‌راحتی می‌توان نشان داد که $\sim$ یک رابطه‌ی هم‌ارزی است. کلاس هم‌ارزی (a,s) را به‌صورت $\frac{a}{s}$ و مجموعه‌ی تمامی کلاس‌ها را با $S^{-1}R$ نشان می‌دهیم. با تعریف دو عمل جمع و ضرب به‌صورت زیرمجموعه‌ی $S^{-1}R$ به یک حلقه‌ی جابجایی و یکدار تبدیل می‌شود:

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

هرگاه p ایده‌آل اول از R باشد آن‌گاه به‌راحتی می‌توان دید که $S = R - p$ یک مجموعه‌ی بسته‌ی ضربی است که دراین‌صورت مجموعه‌ی $S^{-1}R$ را به‌صورت R_p نشان می‌دهیم. همچنین می‌توان نشان داد که حلقه‌ی R_p تنها یک ایده‌آل بیشین دارد؛ یعنی، R_p یک حلقه‌ی موضعی[۵] است. روند رسیدن ازR به R_p را موضعی‌سازی[۶] R در p می‌گوییم.

تعریف ۱۴.۱.۱ هرگاه R یک حلقه‌ی جابجایی و یکداری باشد که شامل هیچ مقسوم‌علیه‌ی از صفر نیست. دراین‌صورت با فرض $S = R - \{0\}$، حلقه‌ی $S^{-1}R$ را میدان کسرهای حلقه‌ی R می‌نامیم.

---

[۴] multiplication closed subset

[۵] local Ring

[۶] localization

۲.۱ مباحثی از نظریه‌ی جبری اعداد

تعریف ۱.۲.۱ میدان عددی [۷] عبارت است از زیر میدانی مثل K از $\mathbb{C}$ به طوریکه $[K:\mathbb{Q}]$ متناهی است.

قضیه ۲.۲.۱ اگر K میدان عددی باشد، آن گاه عدد جبری θ موجود است به طوریکه

$$K = \mathbb{Q}(\theta)$$

اثبات : به [۱، قضیه‌ی ۲.۲]، مراجعه شود. □

قضیه ۳.۲.۱ فرض می‌کنیم $K = \mathbb{Q}(\theta)$ یک میدان عددی از درجه n باشد. در این‌صورت دقیقاً n تکریختی (همریختی یک به یک) متمایز $\sigma_i : K \longrightarrow \mathbb{C}$ $(i = 1, ..., n)$ وجود دارد. عناصر $\sigma_i(\theta) = \theta_i$ ریشه‌های متمایز چندجمله‌ای مینیمال θ روی $\mathbb{Q}$ هستند.

اثبات : به [۱، قضیه‌ی ۴.۲]، مراجعه شود. □

تعریف ۴.۲.۱ فرض می‌کنیم $K = \mathbb{Q}(\theta)$ میدان عددی از درجه n باشد. مجموعه‌ی $\{\alpha_1, ..., \alpha_n\}$ را پایه‌ای برای K به عنوان فضای برداری روی $\mathbb{Q}$ در نظر می‌گیریم. مبیّن [۸] این پایه به صورت زیر تعریف می شود:

$$\Delta[\alpha_1, ..., \alpha_n] = \{det(\sigma_i(\alpha_j))\}^2$$

تعریف ۵.۲.۱ عدد مختلط θ را صحیح جبری می‌گوییم اگر چندجمله‌ای تکین $f(t) \in \mathbb{Z}[t]$ وجود داشته باشد به‌طوریکه $f(\theta) = 0$. مجموعه اعداد صحیح جبری را با نماد B نمایش می‌دهیم .

تعریف ۶.۲.۱ فرض می‌کنیم K میدان عددی باشد. در این‌صورت $\Im = K \cap B$ زیرحلقه‌ای از میدان K می‌باشد و آن را حلقه‌ی اعداد صحیح K می‌نامیم.

---
[۷] number Field
[۸] discriminant

تبصره ۷.۲.۱ واضح است $K \subseteq \mathbb{Q} \subseteq \mathbb{Z}$ و $B \subseteq \mathbb{Z}$، بنابراین $\Im \subseteq \mathbb{Z}$.

تعریف فوق براساس مرجع [۱]، بیان شده است. امّا در اکثر کتاب ها و مقالات حلقه‌ی اعداد صحیح K را با نماد $\mathbb{Z}_K$ نمایش می دهند. از این رو در سرتاسر این پایان نامه، از نماد $\mathbb{Z}_K$ برای نمایش حلقه‌ی صحیح K استفاده خواهیم نمود.

تعریف ۸.۲.۱ میدان عددی K را میدان مربعی [۹] می‌نامیم اگر $[K:\mathbb{Q}] = ۲$.

گزاره ۹.۲.۱ میدان‌های مربعی دقیقاً به فرم $\mathbb{Q}(\sqrt{d})$ هستند که در آن d آزاد از مربع می‌باشد.

اثبات : به [٦]، قضیه‌ی ٦.٣]، مراجعه شود. $\square$

تعریف ۱۰.۲.۱ میدان مربعی K را یک میدان مربعی موهومی [۱۰] می‌گوییم هرگاه $K = \mathbb{Q}(\theta)$، به‌طوریکه θ یک عدد مختلط باشد.

تعریف ۱۱.۲.۱ فرض می‌کنیم K میدان عددی از درجه‌ی n باشد و σ_1،...،σ_n تکریختی‌هایی از K به $\mathbb{C}$ باشند. برای هر $\alpha \in K$ نرم [۱۱] را به صورت زیر تعریف می‌کنیم :

$$N_K(\alpha) = \Pi_{i=1}^{n} \sigma_i(\alpha).$$

گزاره ۱۲.۲.۱ فرض می‌کنیم K میدان عددی و θ چندجمله‌ای مینیمال p از درجه n باشد. مبیّن [۱۲] پایه‌ی $\{1, \theta, ..., \theta^{n-1}\}$ به صورت زیر است:

$$\Delta[1, \theta, ..., \theta^{n-1}] = (-1)^{n(n-1)/2} N(D_p(\theta)),$$

که در آن D_p مشتق صوری p است.

اثبات : به [۴، قضیه‌ی ۲.۱۸]، مراجعه شود. $\square$

---

quadratic Field [۹]
imaginary Quadretic Field [۱۰]
norm [۱۱]
discriminant [۱۲]

تعریف ۱۳.۲.۱ فرض می‌کنیم L میدانی شامل حلقه‌ی R باشد. $\alpha \in L$ راصحیح [۱۳] روی R می‌گوییم اگر α ریشه‌ی چند جمله‌ای تکین f باشد به‌طوریکه $f(x) \in R[x]$.

تعریف ۱۴.۲.۱ گوییم R به طور صحیح بسته [۱۴] است اگر هر عنصر متعلق به حلقه‌ی کسرهای R، متعلق به R باشد.

تعریف ۱۵.۲.۱ فضای متری A را تام [۱۵] می‌گوییم هرگاه هر دنباله‌ی کوشی در A همگرا باشد. هرگاه A تام نباشد با افزودن حدّ همه‌ی دنباله‌های کوشی به آن یک فضای تام به‌دست می آید که کامل شده‌ی [۱۶] یا متم‌سازی A نام دارد. با توجّه به تعریف، کامل شده‌ی یک فضای متری بستگی به متری دارد که درنظر می‌گیریم. به‌عنوان مثال، اگر $\mathbb{Q}$ را با متر متعارف درنظر 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 $\mathbb{R}$ برابر میدان $\mathbb{Q}_p$ است.

تعریف ۱۶.۲.۱ فرض کنیم p یک عدد اوّل ثابتی بوده و $a \in \mathbb{Q}^*$ دلخواه باشد. دراین‌صورت به‌طور منحصربه‌فردی می‌توان نوشت:

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

نگاشت‌های $v_p : \mathbb{Q} \longrightarrow \mathbb{Z}$ و $\| \cdot \|_p : \mathbb{Q} \longrightarrow \mathbb{R}^+$ را به‌صورت زیر تعریف می‌کنیم:

$$v_p(a) = r, \quad v_p(0) = \infty, \quad v_p(\infty) = 0$$

$$\| a \|_p = p^{-v_p(a)}, \quad \| 0 \|_p = 0, \quad \| \infty \|_p = \infty.$$

به‌عنوان مثال می‌توان نوشت :

$$v_5(\frac{۲۱}{۱۴۰}) = -۱, \quad v_7(\frac{۶۸۶}{۱۵}) = ۳$$

---

[۱۳] integral
[۱۴] integrally closed
[۱۵] complete
[۱۶] completion

$$\| \frac{۶۸۶}{۱۵} \|_{۷}= \frac{۱}{۳۴۳}, \quad \| \frac{۲۱}{۱۴۰} \|_{۵}= ۵$$

قرارداد ۱۷.۲.۱ مجموعه‌ی تمامی اعداد اوّل و ∞ را با P نشان می‌دهیم. همچنین نگاشت $\| . \|_\infty$ را قدرمطلق معمولی درنظر می‌گیریم.

لم ۱۸.۲.۱ به‌ازای هر $p \in P$، نگاشت $\| . \|_p$ در خواص زیر صدق می‌کند:

(۱) به‌ازای هر $a \in \mathbb{Q}$، $\| a \|_p = \| -a \|_p$ و $\| a \|_p = ۰$ اگروتنهااگر $a = ۰$؛

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

(۳) به‌ازای 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.

اثبات : در حالتی که $p = \infty$، تمامی عبارات از خواص قدرمطلق معمولی نتیجه می‌شود. بنابراین فرض می‌کنیم $p < \infty$ یک عدد اوّل باشد. در این صورت قسمت (۱) از تعریف نگاشت $\| . \|_p$ نتیجه می شود. فرض کنیم $a, b \in \mathbb{Q}$ دارای نمایش‌های زیر باشند:

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

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

دراین‌صورت 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، $\| b \|_p \leq \| a \|_p$. به‌راحتی می‌توان دید:

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

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

تعریف ۱۹.۲.۱ کامل شده‌ی میدان $\mathbb{Q}$ توسط متر d_p رامیدان اعداد pــای[۱۷] گفته و به‌صورت $\mathbb{Q}_p$ نشان می‌دهیم .

قرارداد ۲۰.۲.۱ در حالتی که $p = \infty$، کامل شده‌ی $\mathbb{Q}$ میدان اعداد حقیقی $\mathbb{R}$ می‌باشد. بنابراین قرارداد می‌کنیم که $\mathbb{Q}_\infty = \mathbb{R}$.

قضیه ۲۱.۲.۱ به‌ازای هر عدد اوّل p مجموعه‌های زیر را درنظر می گیریم:

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p : \| a \|_p \leq 1\} = \{a \in \mathbb{Q}_p : v_p(a) \geq 0\},$$

$$\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p : \| a \|_p = 1\} = \{a \in \mathbb{Z}_p : v_p(a) = 0\},$$

$$M = \{a \in \mathbb{Z}_p : \| a \|_p < 1\} = \{a \in \mathbb{Z}_p : v_p(a) > 0\}.$$

دراین صورت $\mathbb{Z}_p$ یک حلقه‌ی یکدار و $\mathbb{Z}_p^*$ یک گروه ضربی بوده و M نیز یک ایده‌آل بیشین، درنتیجه یک ایده‌آل اوّل، از $\mathbb{Z}_p$ می‌باشد.

اثبات : به [۱، قضیه‌ی ۲.۳]، مراجعه شود. □

تعریف ۲۲.۲.۱ به ازای هر عدد اوّل p، حلقه‌ی $\mathbb{Z}_p$ را حلقه‌ی اعداد صحیح pــای و گروه ضربی $\mathbb{Z}_p^*$ را گروه یکه‌های pــای[۱۸] حلقه‌ی $\mathbb{Z}_p$ می گوییم.

در واقع حلقه‌ی اعداد صحیح pــای، حلقه‌ی ارزیابی میدان اعداد گویای pــای می‌باشد.

[۱۷] p-adic numbers field
[۱۸] p-Adic Units