بسم الله الرحمن الرحیم

دانشگاه ارومیه

# رتبه خم‌های بیضوی روی میدان‌های عددی

سمیه آسوده آرانی

دانشکده‌ی علوم

گروه ریاضی

زمستان ۱۳۸۷

پایان‌نامه برای دریافت درجه‌ی کارشناسی ارشد

استاد راهنما:

دکتر علی سرباز جانفدا

پایان نامه خانم **سمیه آسوده آرانی** به تاریخ **۱۳۸۷/۱۰/۱۵** شماره ۹۱۱-۲ مورد پذیرش هیات محترم داوران با رتبه **عالي** و نمره ۱۸ (هجده تمام) قرار گرفت.

۱) استاد راهنما و رئیس هیئت داوران: **دکتر علي سرباز جانفدا**

۲) استاد مشاور:

۳) داور خارجي: **دکتر محمد علي اسدي**

۴) داور داخلي: **دکتر هوشنگ بهروش**

۵) نماینده تحصیلات تکمیلي: **دکتر سعید استاد باشي**

# تقدیم به

پدرم اوّلین استاد زندگیم

مادرم مهربان‌ترین و عزیزترینم

خواهرانم که در تلاطم زندگی همیشه همراه و یاورم بودند.

# تقدیر و تشکر

خدایم سپاس، سپاس مر تو را برای همه چیز؛ سپاس بر آنچه به من دادی، سپاس بر آنچه ز من گرفتی. تو خود می‌دانی که تنها پناهم تو بودی، تو هستی. در آن شب‌ها و روزهای سخت که خستگی طاقتم می‌برد و ناامیدی رمقم می‌گرفت تو بودی، تو بودی که توانم دادی و آن تلاش‌های بی‌وقفه و مداوم را ثمر می‌دادی.

در آن تنهایی‌ها تو بودی تنها پناهم، در آن نامهربانی‌ها تو بودی همراه هم‌نوایم، در آن بیچارگی‌ها تو بودی کارساز مشکلاتم. خدایا مباد رهایم کنی که به الطافت ایمان دارم.

اینک که به لطف پروردگار با کوله‌باری از تجربه به پایان تلاش چند ساله نزدیک می‌شوم، به حکم ادب و وظیفه بر خود لازم می‌دانم مراتب قدردانی و تشکّر خود را نسبت به تمام عزیزانی که به نحوی مرا در به انجام رساندن این مسئولیت یاری نمودند، هر چند خیلی کوتاه ابراز دارم.

از استاد راهنمای گرامی جناب آقای دکتر علی سرباز جانفدا که خالصانه مرا از گنجینه گهربار علم و تجربیات خود بهره‌مند ساخته و در نهایت صبر و شکیبایی مرا تشویق و راهنمایی نموده و در تمام مراحل مورد لطف و محبّت خویش قرار دادند، تشکّر می‌کنم.

از اساتید محترم و گرانقدر آقایان دکتر هوشنگ بهروش و دکتر محمدعلی اسدی که زحمت داوری پایان‌نامه را به عهده گرفته و مرا راهنمایی فرمودند، سپاسگزاری می‌نمایم.

از خانواده عزیزم که در تمام مراحل زندگی با من همدل و همراه بودند و پشتوانه عاطفی محکمی برای من بوده و همیشه از دعای خیرشان بهره‌مند بودم، تشکّر و قدردانی می‌نمایم.

از همه‌ی دوستان عزیزم به‌ویژه مستوره مفاخری، سمیه رجاییان، خدیجه شمسی، طیبه سپهوند، نیلوفر صدیقی، سمیه رستمی، فریبا بابایی، زهرا باخدا، سمانه قبادی، بهاره مهرآرا، فاطمه مزرعتی تشکّر و سپاسگزاری می‌کنم.

یاد و خاطره این عزیزان همواره با من خواهد بود.

# چکیده

در این پایان‌نامه الگوریتم ۲ـ کاهشی برای محاسبه رتبه‌ی خم بیضوی بدون ۲ـ تاب که روی یک میدان عددی کلّی تعریف شده است، را مورد مطالعه قرار داده‌ایم. روش کلّی الگوریتم شامل ٦ مرحله می‌باشد که عبارتند از: ۱ـ تعریف ریخت ۲ـ کاهش به یک مجموعه‌ی متناهی ۳ـ معادلات لژاندر ۴ـ ساختار چندجمله‌ای درجه چهارم ۵ـ مینیمم‌سازی چندجمله‌ای درجه چهارم ٦ـ بررسی حل‌پذیری چندجمله‌ای درجه چهارم. همچنین به کمک این الگوریتم، رتبه‌ی یک خم بیضوی تعریف شده روی میدان مربعی موهومی را محاسبه نموده‌ایم.

# پیش‌گفتار

خم‌های بیضوی تاریخچه‌ای بسیار طولانی دارند. تاریخچه مطالعه‌ی 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 به‌عنوان شاخه‌ای از نظریه‌ی اعداد مطرح بودند.

معادله‌ای به‌فرم

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

یعنی، معادله دیوفانتی دو متغیره‌ای که حداقل توان یکی از متغیرهای آن بزرگتر مساوی ۳ باشد، را خم بیضوی می‌نامیم. در واقع خم بیضوی یافتن نقاط گویای معادلاتی به‌فرم بالا می‌باشد. بیش از دو یا سه دهه است که خم‌های بیضوی نقش مهمی در نظریه‌ی اعداد و رمزنگاری بازی می‌کنند. مثلاً در دهه‌ی ۱۹۸۰ خم‌های بیضوی در رمزنگاری مورد استفاده قرار گرفتند. همچنین خم‌های بیضوی کاربرد فراوانی در تجزیه‌ی اعداد صحیح بزرگ به عامل‌های اوّل و آزمون اوّل بودن (Primality test) دارند. در دهه‌ی ۱۹۸۰ و ۱۹۹۰ خم‌های بیضوی نقش اساسی در اثبات قضیه آخر فرما داشتند.

فرض کنیم $E$ یک خم بیضوی روی میدان اعداد گویا باشد. گروه $E(\mathbb{Q})$ را گروه موردل- وِیْل خم بیضوی می‌نامیم. محاسبه رتبه‌ی گروه موردل- وِیْل خم $E$ یا همان رتبه‌ی خم، هم‌اکنون به‌صورت یک وظیفه کلاسیک در آمده است. در سال‌های اخیر این کار با استفاده از روش‌های ۲ـ کاهشی (2-descent) انجام شده است. برای خم‌های روی $\mathbb{Q}$، Simath محاسبه رتبه با استفاده از روش‌های ۲ـ کاهشی را پیشنهاد کرد. روش‌های ۲ـ کاهشی بسته به ۲ـ تاب گروه تابی $E(\mathbb{Q})_{tors}$ به سه دسته تقسیم می‌شوند:

(۱) فرض کنیم $E|K$ خم بیضوی روی میدان عددی $K$ باشد. اگر

$$E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

آن‌گاه روش ۲ـ کاهشی کامل را می‌توان به‌کار برد.

(۲) اگر حداقل یک نقطه‌ی تابی غیربدیهی مرتبه ۲ در $K$ وجود داشته باشد، آن‌گاه ۲ـ کاهش مربوط به ۲ـ همگونی را می‌توان به‌کار برد. این دو روش با جزئیات کامل در مرجع [۲۴]، بیان شده‌اند.

(۳) روش ۲ـ کاهشی عمومی که برای هر خم دلخواه روی میدان عددی $K$ به‌کار می‌رود. این روش که توسط بیرچ و سوینرتون (Birch and Swinnerton) برای خم‌های روی $\mathbb{Q}$ مطرح شده بود، توسط سِرف (Serf) برای خم‌های روی میدان‌های عددی مربعی حقیقی با عدد رده‌ای یک توسعه داده شد. سیمون (D. Simon) از توصیف روش کَسلزْ (Cassels) در مقاله

*The Mordell – Weil Group of Curves of Genus* ۲

استفاده کرده و روش ۲ـ کاهشی عمومی را برای خم‌های بیضوی روی میدان‌های عددی دلخواه توسعه داد. روش ۲ـ کاهشی عمومی شامل مراحل زیر است:

- تعیین چندجمله‌ای‌های درجه چهارم مربوط به خم $E$ که همه جا به‌طور موضعی حل‌پذیر است.
- حذف چندجمله‌ای‌های درجه چهارم معادل؛ یعنی، تعیین گروه رده‌های چندجمله‌ای درجه چهارم مربوط به $E$ که نقطه‌ای روی کامل شده‌ی $K$ دارند.
- یافتن جواب عمومی این چندجمله‌ای‌های درجه چهارم
- تعیین رتبه‌ی خم

در بسیاری از حالت‌ها چندجمله‌ای‌های درجه چهارمی هستند که نقطه‌ی عمومی ندارند. در این‌صورت نمی‌توان اظهار نظر کرد که چندجمله‌ای درجه چهارم جواب عمومی ندارد یا شاید ما به اندازه کافی جستجو نکرده‌ایم. بنابراین روش ۲ـ کاهشی کران بالایی برای رتبه خم می‌دهد.

این پایان‌نامه بر اساس مقاله‌ی [۲۷]، نوشته شده است. در فصل اوّل پایان‌نامه برخی از مقدّمات و تعاریف مربوط به جبر و نظریه‌ی جبری اعداد که در طول پایان‌نامه مورد استفاده قرار می‌گیرند، آورده شده است.

در فصل دوّم مفاهیم مربوط به خم‌های بیضوی، معرفی گروه سِلمِر و تِیْت- شافارویچ و اثبات قضیه موردل- وِیْل را مورد بررسی قرار داده‌ایم.

در فصل سوّم که مهم‌ترین فصل پایان‌نامه است خم بیضوی

$$E : y^۲ = x^۳ + Ax^۲ + Bx + C \quad (A, B, C \in K),$$

را در نظر گرفته و الگوریتم ۲- کاهشی برای محاسبه رتبه این خم را مورد بررسی قرار داده‌ایم. این الگوریتم در ٦ مرحله بیان شده است:

- تعریف ریخت $\mu : E(K) \longrightarrow L^*/L^{*۲}$
- کاهش $\mathrm{Im}\mu$ به یک زیرگروه متناهی $L(S, ۲) \cap \ker\mathcal{N}$ از گروه متناهی $L^*/L^{*۲}$
- بررسی رابطه‌ی شمول $L(S, ۲) \cap \ker\mathcal{N} \subset \mathrm{Im}\mu$ و معرفی معادلات لژاندر
- تشکیل چندجمله‌ای‌های درجه چهارم مربوط به $E$
- مینیمم سازی چندجمله‌ای‌های درجه چهارم
- تعیین حل‌پذیری چندجمله‌ای‌های درجه چهارم و استفاده از جواب‌های این چندجمله‌ای‌های درجه چهارم برای تعیین رتبه‌ی خم

در بخش آخر هم الگوریتم را برای خم بیضوی روی میدان مربعی موهومی اجرا نموده‌ایم.

# فهرست مندرجات

# فصل ۱

# مفاهیم مقدّماتی

در این فصل تعاریف و نتایج مقدّماتی، 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 $K \subseteq L$. $L$ یک $K$ـ 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 چندجمله‌ای‌های با ضرایبی در $K$ باشد. عنصر $a \in L$ را یک عنصر جبری [۳] روی $K$ می‌گوییم هرگاه ریشه‌ی یک چندجمله‌ای ناصفری در $K[X]$ باشد.

تعریف ۳.۱.۱ توسیع $L$ از میدان $K$ را یک توسیع جبری [۴] می‌گوییم هرگاه تمامی عناصر $L$ که متعلق به $K$ نیستند، عناصر جبری روی $K$ باشند.

---

[۱] Extention
[۲] Degree of Extention
[۳] Algebraic Element
[۴] Algebraic Extention

**تعریف ۴.۱.۱** فرض کنیم $L$ یک توسیع میدان $K$ باشد. $L$ را بستار جبری[۱] $K$ می‌نامیم اگر در شرایط زیر صدق کند:

(۱) میدان $L$ روی $K$ جبری باشد؛

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

**تعریف ۵.۱.۱** فرض کنیم $L$ یک توسیع میدان $K$ باشد و $g(X) \in K[X]$. می‌گوییم $g$ روی $L$ شکافته می‌شود[۳] هرگاه به‌ازای برخی $\alpha_1, ..., \alpha_n \in L$ و $a \in K$، $g(X) = a\prod_{i=1}^{n}(X - \alpha_i)$. علاوه بر این، هرگاه داشته باشیم $L = K(\alpha_1, ..., \alpha_n)$، دراین‌صورت $L$ میدان شکافنده‌ی[۴] $g$ روی $K$ نامیده می‌شود.

**تعریف ۶.۱.۱** توسیع جبری $N$ از میدان $K$ را یک توسیع نرمال[۵] می‌گوییم هرگاه به‌ازای هر چندجمله‌ای $p(x) \in K[x]$ که ریشه‌ای در $N$ دارد، همه ریشه‌های $p(x)$ هم در $N$ باشند.

**تعریف ۷.۱.۱** فرض کنیم $L$ یک توسیع جبری از میدان $K$ باشد. می‌گوییم عنصر $a \in L$ روی $K$ تفکیک‌پذیر[۶] است هرگاه ریشه‌ی ساده‌ای از چندجمله‌ای مینیمال خود باشد. توسیع $L$ را یک توسیع تفکیک‌پذیر $K$ گوییم هرگاه هر عنصر آن تفکیک‌پذیر باشد.

**تعریف ۸.۱.۱** فرض کنیم $K$ یک میدان، $L$ یک توسیع از $K$ و $S$ زیرمجموعه‌ای از $L$ باشد. می‌گوییم $S$ روی $K$ وابسته‌ی جبری[۷] است اگر به‌ازای 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 $K$ وابسته‌ی جبری نباشد، می‌گوییم $S$ روی $K$ مستقل جبری[۸] است.

**تعریف ۹.۱.۱** میدان $K$ را کامل[۹] می‌گوییم هرگاه هر توسیع جبری $K$، روی $K$ تفکیک‌پذیر باشد.

---

[۱] Algebraic Closure
[۲] Algebraically Closed
[۳] Splits
[۴] Spliting Field
[۵] Normal Extention
[۶] Separable
[۷] Algebraically Dependent
[۸] Algebraically Independent
[۹] Perfect

فرض کنیم $L$ یک میدان باشد. مجموعه‌ی $\mathrm{Aut}(L)$ متشکل از تمام خودریختی‌های (میدان) $\sigma : L \longrightarrow L$ یک گروه تحت عمل ترکیب توابع تشکیل می‌دهند.

**تعریف ۱۰.۱.۱** فرض کنیم $E$ و $F$ توسیع‌هایی از میدان $K$ باشند. نگاشت $\sigma : E \to F$ که هم همریختی میدان‌ها و هم همریختی $K$ـ مدول‌ها باشد یک $K$ـ همریختی نامیده می‌شود.

**تعریف ۱۱.۱.۱** فرض کنیم $L$ توسیع میدان $K$ و $\sigma$ یک خودریختی میدان $L$ باشد و در عین حال یک $K$ـ همریختی نیز باشد، دراین‌صورت گوییم $\sigma$ یک $K$ـ خودریختی است. مجموعه‌ی تمام $K$ـ خودریختی‌های $L$ را گروه گالوای [۱] $L$ روی $K$، نامیده و با نماد $G_{L/K}$ نمایش می‌دهیم.

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

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

$\mathrm{Fix}(H)$ را میدان ثابت $H$ در $L$ می‌نامیم. به‌راحتی می‌توان نشان داد که $\mathrm{Fix}(H)$ زیرمیدانی از $K$ است. 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[۲] می‌گوییم هرگاه $K = \mathrm{Fix}(G_{L/K})$.

**گزاره ۱۴.۱.۱** توسیع جبری $L$ از میدان $K$ یک توسیع گالواست اگر و تنها اگر $L$ یک توسیع نرمال و تفکیک‌پذیر از $K$ باشد.

**اثبات:** [۱۳]. □

**تعریف ۱۵.۱.۱** توسیع میدان $L$ از میدان $K$ را دوری (آبلی ) می‌گوییم اگر $L$ روی $K$ جبری و گالوا بوده و $G_{L/K}$ یک گروه دوری (آبلی) باشد. هرگاه در این حالت $G_{L/K}$ یک گروه دوری متناهی از مرتبه $n$ باشد، آنگاه می‌گوییم $L$ یک توسیع دوری از درجه‌ی $n$ است. پس طبق قضیه اساسی گالوا داریم: $[L : K] = n$

**قضیه ۱۶.۱.۱** هرگاه $L$ یک توسیع میدان با بعد متناهی از میدان متناهی $K$ باشد، آن‌گاه $L$ متناهی بوده و روی $K$ گالوا می‌باشد. گروه گالوای $G_{L/K}$، دوری است.

**اثبات:** [۱۳]. □

[۱] Galois Group
[۲] Galois Extention

**تبصره ۱۷.۱.۱** بنابر قضیه ۱۶.۱.۱، هر توسیع با بعد متناهی از یک میدان متناهی، یک توسیع دوری است.

**تعریف ۱۸.۱.۱** فرض کنیم $R$ یک حلقه‌ی جابجایی و یکدار باشد. زیر مجموعه‌ی $S \subset R$ را یک زیر مجموعه‌ی بسته‌ی ضربی[۱] می‌گوییم هرگاه $1 \in S$ و $S$ تحت عمل ضرب بسته باشد. رابطه‌ی $\sim$ را روی مجموعه‌ی $R \times S$ به‌صورت زیر تعریف می‌کنیم:

$$(a,s) \sim (b,t) \text{ اگر و تنها اگر } \exists u \in S \ : \ (at-bs)u = 0.$$

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 زیر مجموعه‌ی $S^{-1}R$ به یک حلقه‌ی جابجایی و یکدار تبدیل می‌شود:

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

هرگاه $\mathfrak{p}$ ایده‌آل اولی از $R$ باشد آن‌گاه به‌راحتی می‌توان دید که $S = R - \mathfrak{p}$ یک مجموعه‌ی بسته‌ی ضربی است که دراین صورت مجموعه‌ی $S^{-1}R$ را به‌صورت $R_{\mathfrak{p}}$ نشان می‌دهیم. همچنین می‌توان نشان داد که حلقه‌ی $R_{\mathfrak{p}}$ تنها یک ایده‌آل بیشین دارد؛ یعنی، $R_{\mathfrak{p}}$ یک حلقه‌ی موضعی[۲] است. روند رسیدن از $R$ به $R_{\mathfrak{p}}$ را موضعی سازی[۳] $R$ در $\mathfrak{p}$ می‌گوییم.

**تعریف ۱۹.۱.۱** هرگاه $R$ یک حلقه‌ی جابجایی و یکداری باشد که شامل هیچ مقسوم علیه‌ی از صفر نیست. دراین‌صورت با فرض $S = R - \{0\}$، حلقه‌ی $S^{-1}R$ را میدان کسرهای حلقه‌ی $R$ می‌نامیم.

---

Multiplication Closed Subset[۱]
Local Ring[۲]
Localization[۳]

## ۲.۱ مباحثی از نظریه‌ی جبری اعداد

**تعریف ۱.۲.۱** میدان عددی[۱] عبارت است از زیر میدانی مثل $K$ از $\mathbb{C}$ به‌طوری‌که $[K:\mathbb{Q}]$ متناهی است.

واضح است که اگر $K$ میدان عددی باشد، آن‌گاه $K=\mathbb{Q}(\alpha_{۱},...,\alpha_n)$ که در آن $\alpha_{۱}$،...،$\alpha_n$ اعداد جبری روی $\mathbb{Q}$ هستند. همچنین $\alpha$ عدد جبری است اگر و تنها اگر $[\mathbb{Q}(\alpha):\mathbb{Q}]$ متناهی باشد.

**قضیه ۲.۲.۱** اگر $K$ میدان عددی باشد، آن‌گاه عدد جبری $\theta$ موجود است به‌طوری‌که

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

**اثبات:** [[۲۸]، قضیه 2.2]. □

**قضیه ۳.۲.۱** فرض کنیم $K=\mathbb{Q}(\theta)$ یک میدان عددی از درجه $n$ باشد. دراین‌صورت دقیقاً $n$ تکریختی (همریختی یک‌به‌یک) متمایز $\sigma_i:K\longrightarrow\mathbb{C}$ $(i=۱,...,n)$ وجود دارد. عناصر $\sigma_i(\theta)=\theta_i$ ریشه‌های متمایز چندجمله‌ای مینیمال $\theta$ روی $\mathbb{Q}$ هستند.

**اثبات:** [[۲۸]، قضیه 2.4]. □

**تعریف ۴.۲.۱** فرض کنیم $K=\mathbb{Q}(\theta)$ میدان عددی از درجه‌ی $n$ باشد. مجموعه‌ی $\{\alpha_{۱},...,\alpha_n\}$ را پایه‌ای برای $K$ به‌عنوان فضای برداری روی $\mathbb{Q}$ در نظر می‌گیریم. مبیّن[۲] این پایه به‌صورت زیر تعریف می‌شود:

$$\Delta[\alpha_{۱},...,\alpha_n]=\left\{det(\sigma_i(\alpha_j))\right\}^{۲}.$$

**تعریف ۵.۲.۱** عدد مختلط $\theta$ را صحیح جبری می‌گوییم اگر چندجمله‌ای تکین $f(t)\in\mathbb{Z}[t]$ وجود داشته باشد به‌طوری‌که $f(\theta)=۰$.

**نمادگذاری ۶.۲.۱** مجموعه اعداد صحیح جبری را با نماد $\mathbf{B}$ نمایش می‌دهیم.

**تعریف ۷.۲.۱** فرض کنیم $K$ میدان عددی باشد. دراین‌صورت $\mathfrak{O}=K\cap\mathbf{B}$ زیر حلقه‌ای از میدان $K$ می‌باشد و آن‌را حلقه‌ی اعداد صحیح $K$ می‌نامیم.

**تبصره ۸.۲.۱** واضح است $\mathbb{Z}\subseteq\mathbb{Q}\subseteq K$ و $\mathbb{Z}\subseteq\mathbf{B}$، بنابراین $\mathbb{Z}\subseteq\mathfrak{O}$.

[۱] Number Field
[۲] Discriminant

قرارداد ۹.۲.۱ تعریف فوق بر اساس مرجع [۲۸]، بیان شده است. امّا در اکثر کتاب‌ها و مقالات حلقه‌ی اعداد صحیح $K$ را با نماد $\mathbb{Z}_K$ نمایش می‌دهند. ازاین‌رو در سرتاسر 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 دقیقاً به‌فرم $\mathbb{Q}(\sqrt{d})$ هستند که در آن $d$ آزاد از مربع می‌باشد.

اثبات: [[۲۸]، قضیه 3.1]. □

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

تعریف ۱۳.۲.۱ فرض کنیم $K$ میدان عددی از درجه $n$ باشد و $\sigma_۱,\dots,\sigma_n$ تکریختی‌هایی از $K\longrightarrow\mathbb{C}$ باشند. برای هر $\alpha\in K$ نرم [۳] $\alpha$ را به‌صورت زیر تعریف می‌کنیم:

$$\mathcal{N}_K(\alpha)=\prod_{i=۱}^{n}\sigma_i(\alpha).$$

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

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

که در آن $D_p$ مشتق صوری $p$ است.

اثبات: [[۲۸]، قضیه 2.18]. □

تعریف ۱۵.۲.۱ فرض کنیم $R$ یک دامنه‌ی صحیح باشد؛ یعنی، حلقه‌ی جابجایی و یکدار و بدون مقسم صفر 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.

[۱] Quadratic Field
[۲] Imaginary Quadretic Field
[۳] Norm
[۴] Discriminant
[۵] Noetherian

**تعریف ۱۶.۲.۱** فرض کنیم $L$ میدانی شامل حلقه، $R$ باشد. $\alpha \in L$ را صحیح[1] روی $R$ می‌گوییم اگر $\alpha$ ریشه‌ی چندجمله‌ای تکین $f$ باشد به‌طوری‌که $f(x) \in R[x]$.

**تعریف ۱۷.۲.۱** گوییم $R$ به‌طور صحیح بسته[2] است اگر هر عنصر متعلق به حلقه‌ی کسرهای $R$، متعلق به $R$ باشد.

**تعریف ۱۸.۲.۱** حوزه‌ی صحیح $R$ را قلمرو ددکیند[3] 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 ۱۹.۲.۱** اگر $K$ میدان عددی باشد، حلقه‌ی کسرهای، $\mathbb{Z}_K$، میدان $K$ یک دامنه‌ی ددکیند است.

اثبات: [[۲۸]، قضیه 5.3]. $\square$

**تعریف ۲۰.۲.۱** فرض کنیم $K$ یک میدان عددی باشد. تابع ارزیابی گسسته[4] روی $K$ یک همریختی ناصفر مانند $v : K^* = K - \{\circ\} \to \mathbb{Z}$ 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 تصویرش زیرگروه ناصفری از $\mathbb{Z}$ است و به‌ازای هر $m \in \mathbb{Z}$، به‌فرم $m\mathbb{Z}$ می‌باشد.

**تعریف ۲۱.۲.۱** اگر در تعریف فوق قرار دهیم $m = ۱$، آن‌گاه $v : K^* = K - \{\circ\} \to \mathbb{Z}$ پوشاست؛ یعنی، $v(K^*) = \mathbb{Z}$. در این حالت $v$ را نرمال شده[5] می‌گوییم. در غیر این‌صورت $x \mapsto m^{-۱}.v(x)$ یک ارزیابی گسسته نرمال شده خواهد بود.

**تبصره ۲۲.۲.۱** با قرارداد $v(\circ) = \infty$ می‌توان $v : K \to \mathbb{Z}$ را نیز تعریف کرد. همچنین داریم: $v(۱) = v(۱ \times ۱) = v(۱) + v(۱)$، درنتیجه $v(۱) = \circ$.

[1] Integral
[2] Integrally Closed
[3] Dedekind
[4] Discrete Valuation
[5] Normalized

تعریف ۲۳.۲.۱ برای ارزیابی از $K$، مثل $v$، تعریف می‌کنیم: $\mathcal{O}_v = \{x \in K \mid v(x) \geq \circ\}$.
چون $v(\text{۱}) = \circ$ پس $\text{۱} \in \mathcal{O}_v$. اگر $x, y \in \mathcal{O}_v$، آن‌گاه طبق تعریف داریم: $xy \in \mathcal{O}_v$ و $x + y \in \mathcal{O}_v$. ازاین‌رو $\mathcal{O}_v$ یک حلقه است. به $\mathcal{O}_v$ حلقه‌ی ارزیابی[۱] $v$ در $K$ می‌گوییم.

تعریف ۲۴.۲.۱ دامنه‌ی صحیح $R$ را یک حلقه‌ی ارزیابی گسسته[۲]، $DVR$، گوییم هرگاه یک تابع ارزیابی گسسته $v$ از میدان کسرهای $R$ موجود باشد به‌طوری‌که

$$R = \{x \in K \mid v(x) \geq \circ\}.$$

تبصره ۲۵.۲.۱ چون یک $DVR$، یک حلقه‌ی ارزیابی است پس یک حلقه‌ی موضعی است. حال فرض کنیم ایده‌آل بیشین $R$ برابر $\mathfrak{m}$ باشد. همچنین فرض کنیم $x \in R$ وارون‌پذیر باشد. بنابراین $x^{-\text{۱}} \in R$ و داریم: $\circ = v(\text{۱}) = v(xx^{-\text{۱}}) = v(x) + (x^{-\text{۱}})$. حال چون طبق تعریف $v(x) \geq \circ$، پس رابطه‌ی فوق معادل با $v(x) = \circ$ می‌باشد. ازاین‌رو

$$\mathfrak{m} = \{\text{مجموعه‌ی عناصر وارون‌ناپذیر } R\}$$

$$= \{x \in K \mid v(x) \geq \circ\}$$

$$= \{x \in R \mid v(x) \geq \circ\}.$$

حال قرار می‌دهیم $\mathcal{P}_v = \{x \in K \mid v(x) > \circ\}$. این مجموعه یک $\mathcal{O}_v$ـ ایده‌آل است. به‌علاوه ایده‌آل سره نیز می‌باشد. چون $\text{۱} \in \mathcal{O}_v$ و $\text{۱} \notin \mathcal{P}_v$. به‌عبارت دیگر، $\mathcal{P}_v$ ناصفر است. چون $v$ پوشاست پس می‌توان $x \in K$ پیدا کرد که $v(x) = \text{۱}$.

تعریف ۲۶.۲.۱ $\mathcal{P}_v$ معرّفی شده در ۲۵.۲.۱ را ایده‌آل ارزیابی[۳] $v$ می‌نامیم.

حال فرض کنیم $x, y \in \mathcal{O}_v$. اگر $xy \in \mathcal{P}_v$، آن‌گاه $v(xy) = v(x) + v(y) > \circ$. پس $v(x) \geq \circ$، $v(y) \geq \circ$. بنابراین $v(x) > \circ$ یا $v(y) > \circ$. پس $x \in \mathcal{P}_v$ یا $y \in \mathcal{P}_v$. درنتیجه $\mathcal{P}_v$ یک ایده‌آل اوّل 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 حدّ همه‌ی دنباله‌های کوشی به آن یک فضای تام به‌دست می‌آید که کامل شده‌ی[۵] یا متمم‌سازی $A$ نام دارد.

---

Valuation Ring[۱]
discrete valuation ring[۲]
Valuation Ideal[۳]
Complete[۴]
Completion[۵]

با توجّه به تعریف، کامل شده‌ی یک فضای متری بستگی به متری دارد که در نظر می‌گیریم. به‌عنوان مثال، اگر $\mathbb{Q}$ را با متر متعارف درنظر بگیریم، کامل شده‌ی آن برابر $\mathbb{R}$ است. درحالی‌که 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 $a \in \mathbb{Q}^*$ دلخواه باشد. دراین‌صورت به‌طور منحصربه‌فردی می‌توان نوشت:

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

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

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

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

به‌عنوان مثال می‌توان نوشت:

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

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

**قرارداد ۲۹.۲.۱** مجموعه‌ی تمامی اعداد اوّل و $\infty$ را با $\mathbf{P}$ نشان می‌دهیم. همچنین نگاشت $\|.\|_\infty$ را قدر مطلق معمولی در نظر می‌گیریم.

**لم ۳۰.۲.۱** به‌ازای هر $p \in \mathbf{P}$، نگاشت $\|.\|_p$ در خواص زیر صدق می‌کند:

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

(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.