بسم الله الرحمن الرحيم

MRTsoft

دانشگاه ارومیه

رتبه‌های خم‌های بیضوی

سجاد سلامی
دانشکده‌ی علوم
گروه ریاضی

۱۳۸۷ /۳/ ۱۱

پایان‌نامه برای دریافت درجه‌ی کارشناسی ارشد

استاد راهنما:

دکتر علی سرباز جانفدا

پایان نامه سمیرا سلامی به تاریخ ۸۷/۳/۱۱ شماره ۱۵-۱۵۱۰ / ۸۷/۳/۵ مورد پذیرش هیات محترم داوران با رتبه عالی
و نمره ۱۸ قرار گرفت.

۱- استاد راهنما و رئیس هیئت داوران: دکتر ...

۲- استاد مشاور:

۳- داور خارجی: دکتر مرتضی ایزدی

۴- داور داخلی: دکتر رضا سرزیده

۵- نماینده تحصیلات تکمیلی: دکتر ...

۸۷/۳/۱۱

تقدیم به تمامی اعضای خانواده‌ام

پدرم

مادرم

همسرم

برادرها و خواهرهایم

تقدیر و تشکر

سپاس و ستایش معبود یگانه را که پرتو الطاف بی‌شمارش بر لحظه لحظهٔ زندگی‌ام ساطع و آشکار است. حمد و ثنا می‌گزارم او را که فکرت و اندیشه را در بستر روحم روان ساخت و بهره‌گیری از خوان گستردهٔ علم و دانش را نصیب و روزی‌ام گردانید.

با لطف و عنایت خداوند منان توانستیم این پایان‌نامه را بعد از یک سال و چند ماه تدوین کنیم. در طول هفت سال تحصیل خودم در دانشگاه ارومیه از تجربیات استاد ارجمندم جناب آقای دکتر جانفدا، نه تنها در حیطه‌ی پایان نامه بلکه در امورات دیگر زندگیم، به کثرت استفاده کردیم که جا دارد کمال تشکر و قدردانی را در این موضع از محضر ایشان داشته باشم.

همچنین از محضر اساتید محترم آقایان دکتر سزیده و دکتر ایزدی که زحمت مطالعه‌ی این پایان نامه را متقبل شده‌اند، کمال تشکر و قدردانی دارم.

در پایان جا دارد از تمامی اعضای خانواده‌ام تقدیر و تشکر کنم به ویژه از همسرم وحیده فرهنگی به خاطر همیاری و تقویت روحیه‌ی من در طول تدوین این پایان‌نامه تشکر و قدردانی می‌کنم. همچنین از تمامی دوستانی که در طول این پایان‌نامه با همکاری و هم‌فکری‌های خودشان مرا مدیون خویش ساختند، کمال تشکر و قدردانی را به عمل می‌آورم.

چکیده فارسی

در این پایان‌نامه نظریه‌ی عمومی خم‌های بیضوی را روی یک میدان کامل و ساختار گروهی حاصل از خم‌های بیضوی روی میدان‌های $\mathbb{C}$، $\mathbb{R}$، $\mathbb{Q}$، $\mathbb{F}_q$ و $\mathbb{Q}_p$ را به طور مختصر مورد مطالعه قرار داده‌ایم. مطالعه رتبه‌های خم‌های بیضوی روی $\mathbb{Q}$ بخش اصلی پایان‌نامه است. رتبه، اندازه‌ای برای بزرگی مجموعه نقاط گویای روی خم‌های بیضوی می‌باشد. امروزه سوال‌های باز خیلی مهم، شامل حدسیه‌ی بیرچ و اسوینرتون-دایر، درباره‌ی خم‌های بیضوی توسط رتبه‌ها انجام می‌شود. در فصل آخر پایان‌نامه برخی از مسایل باز مهم مرتبط با رتبه‌های خم‌های بیضوی روی $\mathbb{Q}$ را مورد مطالعه قرار داده‌ایم.

پیشگفتار

در طول چند سالی که در دوره‌های کارشناسی و کارشناسی ارشد مشغول به تحصیل در رشته‌ی ریاضیبودم، همیشه این سؤال برایم مطرح بود: " آیا کانونی وجود دارد که گرایش‌های مختلف ریاضی مثل هندسه (جبری، دیفرانسیل و تحلیلی)، آنالیز(حقیقی، مختلط و هارمونیک)، جبر (نظریه‌ی گروهها، حلقه‌ها، میدان‌هاو مدول‌ها) و نظریه‌ی اعداد (جبری و تحلیلی) و غیره ⋯ بتوانند در این کانون نمود پیدا کنند یا نه؟" بالاخره در طول مدت زمانی که برای تدوین این پایان‌نامه صرف کردم، توانستم جوابی برای سؤال خودم پیدا کنم. این کانون چیزی جز نظریه‌ی خم‌های بیضوی نیست.

تاریخچه‌ی خم‌های بیضوی خیلی طولانی است و ریشه در نظریه‌ی معادلات دیوفانتی دارد که شاخه‌ای از نظریه‌ی اعداد بوده و با حل معادلات چندجمله‌ای در اعداد گویا مرتبط است. ساده‌ترین معادله‌های دیوفانتی چندجمله‌ای‌های یک متغیره می‌باشند:

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0 \ (a_i \in \mathbb{Z}).$$

امروزه با استفاده از نظریه‌های جبری موجود، یافتن اعداد گویایی که در چنین معادلاتی صدق می‌کنند کاری نسبتاً راحت و شدنی است.

معادلات دیوفانتی دو متغیّره نیز به صورت چندجمله‌ای‌های $f(x,y) = 0$ هستند که ضرایب آنها اعداد صحیحی می‌باشند. در حالتی که توان‌های x و y بیشتر از ۲ نباشند، چندجمله‌ای $f(x,y)$ معادله‌ی یک خط یا یک مقطع مخروطی خواهد بود. پیدا کردن نقاط گویایی از صفحه که در این معادلات صدق می‌کنند با استفاده از مباحث مربوط به حساب دیفرانسیل معمولی کاری راحت و انجام‌پذیر است. خم‌های بیضوی نیز زمانی مطرح می‌شوند که حداقل توان یکی از متغیّرهای $f(x,y)$ بزرگتر یا مساوی ۳ باشد. در واقع، نظریه‌ی خم‌های

بیضوی با یافتن نقاط گویایی از صفحه آغاز می‌شود که در روابط زیر صدق می‌کنند:

$$y^۲ = x^۳ + ax^۲ + bx + c,\ \ ax^۳ + by^۳ = c, \quad (a, b, c \in \mathbb{Z}).$$

در سال ۱۹۲۲ میلادی، موردل مقاله‌ی [۳۳] را ارائه داد که در آن به مطالعه روی یافتن نقاط گویای روی خم‌های بیضوی پرداخته بود. ایشان در آغاز این مقاله چنین نوشته بود: " تعداد کمی سوال آشنا برای ریاضی‌دانان، همچون یافتن نقاط گویای روی خم‌های بیضوی، وجود دارد که در مدت زمان طولانی کارهای انجام شده روی آن‌ها به نتایج کلی کمی منجر شده است."

هنگامی که توان‌های x و y بیشتر از ۲ باشند، مساله‌ی یافتن نقاط گویایی از صفحه که در چندجمله‌ای‌های $f(x, y)$ صدق می‌کنند، کار چندان راحتی نیست. به عنوان مثال، فرما در قرن شانزده میلادی آخرین قضیه‌ی خودش را به این صورت مطرح کرده بود که به ازای هر عدد صحیح $n \geq ۳$ جوابهای گویای معادله‌ی $x^n + y^n = ۱$ فقط $(\pm ۱, ۰)$ و $(۰, \pm ۱)$ هستند. بالاخره، پروفسور وایلز با فرض درست بودن حدسیه‌ی تانیاما- شیمورا توانست در سال ۱۹۹۵ میلادی این قضیه را اثبات کند به طوری که در این اثبات نظریه‌ی ریاضی خم‌های بیضوی نقشی اساسی داشت [۵۰].

در چند دهه‌ی اخیر کاربردهای مهیج و جالب توجهی برای خم‌های بیضوی ارائه شده است و روز به روز بر دامنه‌ی تحقیقات برای یافتن کاربردهای دیگر افزوده می‌شود. در [۲۵] و [۳۱]، اولین کاربردهای خم‌های بیضوی در رمزنگاری مورد مطالعه و بررسی قرار گرفته است که امروزه یکی از مهم‌ترین کارها برای امنیت اطلاعات در شبکه‌های اینترنتی می‌باشد. کاربردهای خم‌های بیضوی در نظریه‌ی اعداد نیز خیلی جالب هستند. به عنوان مثال در [۵] و [۱۸]، برای اثبات اول بودن اعداد صحیح خیلی بزرگ و تجزیه اعداد صحیح بزرگ به عامل‌های اول آن شیوه‌هایی با استفاده از خم‌های بیضوی ارائه شده است. هدف از بیان چنین کاربردهایی این است که اهمیت مطالعه و تحقیق درباره‌ی خم‌های بیضوی مشخص شود.

این پایان نامه با محوریت مقاله‌ی [۳۸] تدوین شده است. البته بنابر حجیم بودن مباحث مطرح شده در مقاله و از طرف دیگر محدودیت زمانی موجود، فقط توانستیم بخش‌هایی از این مقاله را مورد بررسی قرار دهیم.

در فصل اول، با ارائه‌ی برخی از مقدمات و تعاریف، خم بیضوی E را روی میدان کامل K در قالب واریته‌ای با گونه‌ی ۱ معرفی کرده و نشان داده‌ایم که هر خم بیضوی با یک رابطه‌ی (تعمیم یافته‌ی وایرشتراس) یکسان است. سپس با تعریف یک عمل جمع هندسی روی مجموعه‌ی نقاط K- گویای E، $E(K)$، نشان داده‌ایم که $E(K)$ یک گروه آبلی است.

در فصل دوم، بدون پرداختن به جزئیات مطالب، ساختار گروه حاصل از خم‌های بیضوی را روی میدان اعداد مختلط، میدان اعداد حقیقی، میدان اعداد p- وار و میدان‌های متناهی مورد بررسی قرار داده‌ایم. به عنوان مثال نشان داده‌ایم که گروه $E(\mathbb{C})$ به ازای هر خم بیضوی E با یک چنبره توپولوژیکی یکریخت است.

در فصل سوم، که اصلی‌ترین فصل این پایان‌نامه است، 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 موردل- ویل این گروه با یک گروه آبلی متناهی مولد یکریخت می‌باشد. رتبه‌ی این گروه آبلی رتبه‌ی هندسی خم بیضوی E گفته می‌شود. در اکثر مقالات و کتاب‌های مربوط به خم‌های بیضوی منظور از رتبه‌ی خم بیضوی E همان رتبه‌ی هندسی آن است ولی چون برای خم بیضوی E یک رتبه‌ی دیگری با عنوان رتبه‌ی تحلیلی نیز تعریف می‌شود، بنابراین در طول پایان نامه بین این دو رتبه تمایز قائل شده‌ایم.

امروزه مسائل باز زیادی در باره‌ی خم‌های بیضوی مطرح می‌باشد که با رتبه‌های خم‌های بیضوی مرتبط است. در فصل سوم به برخی از این مسائل اشاره کرده‌ایم. به عنوان مثال حدسیه‌ی بیرچ و اِسوینرتون- دایر، BSD، یکی از این مسائل می‌باشد که در سال ۲۰۰۰ از طرف موسسه‌ی ریاضیات کلِی، [۵۳]، در لیست هفت مسٔله‌ی یک میلیون دلاری این موسسه قرار گرفت. برای اطلاع از دیگر مسائلِ باز مرتبط با خم‌های بیضوی و هندسه‌ی جبری می‌توان به [۴۱] مراجعه کرد.

فهرست مندرجات

چکیده فارسی ii

پیشگفتار iii

۱ مقدمات و پیش نیازها ۱

۱.۱ مباحثی از جبر ۱

۲.۱ مباحثی از هندسه‌ی جبری ۷
۱.۲.۱ واریته‌های جبری ۷
۲.۲.۱ خم‌های جبری ۱۹

۳.۱ روابط وایرشتراس و خم‌های بیضوی ۲۶
۱.۳.۱ روابط وایرشتراس ۲۶
۲.۳.۱ خم‌های بیضوی ۳۸

۲ خم‌های بیضوی روی برخی از میدانها ۴۲

۱.۲ خم‌های بیضوی روی $\mathbb{C}$ ۴۲
۱.۱.۲ مشبکه‌ها و رابطه‌ی آنها با گروه $E(\mathbb{C})$ ۴۳
۲.۱.۲ توابع مدولی و فرم‌های مدولی ۴۸

۲.۲ خم‌های بیضوی روی $\mathbb{R}$ ۵۵

۳.۲ خم‌های بیضوی روی $\mathbb{F}_q$ ۵۶

۴.۲ خم‌های بیضوی روی $\mathbb{Q}_p$ ۵۹
۱.۴.۲ مقدمه‌ای بر میدان اعداد pـ وار ۵۹
۲.۴.۲ خم‌های بیضوی روی $\mathbb{Q}_p$ ۶۴

۳ خم‌های بیضوی روی میدان اعداد گویا ۶۶

۱.۳ چند قضیه‌ی اساسی ۶۶
۱.۱.۳ محاسبه‌ی زیر گروه $E(\mathbb{Q})_{tors}$ ۶۸
۲.۱.۳ یافتن رتبه‌ی هندسی خم بیضوی E ۷۵
۳.۱.۳ منظم کننده‌ی خم‌های بیضوی ۷۸
۴.۱.۳ اثبات قضیه‌ی موردل- ویل در حالت خاص ۷۹

۲.۳ گروه تِیْت- شافارویچ ۸۱

۳.۳ Lـ سری خم‌های بیضوی ۹۰
۱.۳.۳ کاهش خم‌های بیضوی تعریف شده روی $\mathbb{Q}$ ۹۰
۲.۳.۳ تابع زتا و فرضیه‌ی ریمان ۹۴
۳.۳.۳ Lـ تابع مختلط هَس- وِیْل ۹۷

۴.۳ حدسیه‌ی BSD ۱۰۴
۱.۴.۳ معرفی حدسیه‌ی BSD ۱۰۴
۲.۴.۳ کارهای اخیر ۱۱۰

کتاب‌نامه ۱۱۳

لیست اشکال

۱.۱ نموداری از یک خم هموار و خم‌هایی شامل یک نقطه‌ی گره یا بازگشت ۳۰

۲.۱ قانون جمع هندسی ۳۲

۱.۲ جهت‌دهی مثبتی از یک مشبکه ۴۴

۲.۲ برخی از همسایگی‌ها در $\mathcal{H}^*$ ۵۲

۳.۲ خم‌های بیضوی با تعداد مولفه‌های همبندی متفاوت ۵۶

۱.۳ نمودار $y^۲ = x^۳ - x + ۱$ به همراه عمل جمعی از آن ۶۷

۲.۳ داده‌های بیرچ و اسوینرتون- دایر برای $y^۲ = x^۳ - d^۲x$ ۱۰۵

لیست جداول

۱.۱ ضرایب حاصل از تغییر متغیرهای $x = u^۲x' + r$ و $y = u^۳y' + u^۲sx' + t$ ۲۸

۱.۲ نقاط خم بیضوی $y^۲ = x^۳ - x + ۱$ روی $\mathbb{F}_۳$ ۵۷

۱.۳ دسته بندی خم‌های بیضوی بر اساس زیر گروه تابی ۷۲

۲.۳ بزرگترین رتبه‌های ثبت شده ۷۷

۳.۳ کاهش خم E به پیمانه‌ی عدد اول p $(\neq ۲,۳)$ ۹۳

فصل ۱

مقدمات و پیش نیازها

در این فصل مقدماتی از مباحث جبری، هندسه‌ی جبری و همچنین نظریه‌ی خم‌های بیضوی را ارائه می‌کنیم. تا حد امکان سعی کرده‌ایم که مطالب مختصر بوده و برای درک بهتر مطالب فصل‌های بعدی مفید باشند بنابراین از ارائه‌ی اکثر اثبات‌ها خودداری نموده‌ایم.

۱.۱ مباحثی از جبر

تعریف ۱.۱.۱ فرض می‌کنیم R یک حلقه‌ی جابجایی و یکدار باشد. زیر مجموعه‌ی $S \subset R$ را یک زیر مجموعه‌ی بسته‌ی ضربی [1] می‌گوییم هرگاه $1 \in S$ و S تحت عمل ضرب بسته باشد. رابطه‌ی $\sim$ را روی مجموعه‌ی $R \times S$ به صورت زیر تعریف می‌کنیم:

$$(a,s) \sim (b,t) \Longleftrightarrow \exists u \in S \ : \ (at - bs)u = 0.$$

به راحتی می‌توان نشان داد که $\sim$ یک رابطه‌ی هم‌ارزی است. کلاس هم‌ارزی (a,s) را به صورت $\frac{a}{s}$ و مجموعه‌ی تمامی کلاس‌ها را با $S^{-1}R$ نشان می‌دهیم. با تعریف دو عمل جمع و ضرب به صورت 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 I ایده‌آل اولی از R باشد آنگاه به راحتی می‌توان دید که $S = R - I$ یک مجموعه‌ی بسته‌ی ضربی است که در این صورت مجموعه‌ی $S^{-1}R$ را به صورت R_I نشان می‌دهیم.

[1] multiplication closed subset

همچنین می‌توان نشان داد که حلقه‌ی R_I تنها یک ایده‌ال بیشین دارد یعنی R_I یک حلقه‌ی موضعی[۱] است. روند رسیدن از R به R_I را موضعی سازی[۲] R در I می‌گوییم.

تعریف ۲.۱.۱ هرگاه R یک حلقه‌ی جابجایی و یکداری باشد که شامل هیچ مقسوم علیه‌ی از صفر نیست، در این صورت با فرض $S = R - \{0\}$، حلقه‌ی $S^{-1}R$ را میدان کسرهای حلقه‌ی R می‌گوییم.

قضیه ۳.۱.۱ (پایه‌ی هیلبرت)[۳] فرض کنیم R یک حلقه‌ی جابجایی و یکدار بوده و تمامی ایده‌ال‌های آن متناهی مولد باشند. در این صورت حلقه‌ی $R[x_1, \cdots, x_n]$ جابجایی و یکدار بوده و تمامی ایده‌ال‌های آن متناهی مولد هستند.

اثبات: [[۲۳]، بخش 7.9]. □

تعریف ۴.۱.۱ فرض کنیم K یک میدان باشد. منظور از یک توسیع[۴] K، میدانی مثل L است که $K \subseteq L$. به راحتی می‌توان دید که L یک Kـ فضای برداری است. بعد این فضای برداری را درجه‌ی توسیع[۵] گفته و به صورت $[L : K]$ نشان می‌دهیم. هرگاه $[L : K] < \infty$، می‌گوییم L یک توسیع متناهی روی K است.

تعریف ۵.۱.۱ فرض کنیم L یک توسیع از K بوده و $A = \{a_1, \cdots, a_n\} \subseteq L$. کوچکترین میدان شامل K و A را توسیع تولید شده[۶] توسط A گفته و به صورت $K(A) = K(a_1, \cdots, a_n)$ نشان می‌دهیم.

تعریف ۶.۱.۱ فرض کنیم L یک توسیع از K بوده و $K[X]$ حلقه‌ی چندجمله‌ایهای با ضرایبی در K باشد. عنصر $a \in L$ را یک عنصر جبری[۷] روی K می‌گوییم هرگاه ریشه‌ی یک چندجمله‌ای ناصفری در $K[X]$ باشد. در غیر این صورت عنصر a را یک عنصر متعالی[۸] روی K می‌گوییم.

تعریف ۷.۱.۱ توسیع L از میدان K را یک توسیع جبری[۹] می‌گوییم هرگاه تمامی عناصر $a \in L - K$ روی K عناصر جبری باشند. همچنین هرگاه $a_1, \cdots, a_n \in L$ عناصری جبری

[۱] local ring
[۲] localization
[۳] Hilbert Basis Theorem
[۴] extention
[۵] degree of extention
[۶] extention generated by A
[۷] algebraic element
[۸] transcendental element
[۹] algebraic extention

روی K باشند در این صورت $K(a_1, \cdots, a_n)$ را توسیع جبری متناهی تولید شده[۱] توسط عناصر a_1، $\cdots$، a_n می‌گوییم.

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[۲] 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 وابسته‌ی جبری نباشد، می‌گوییم S روی K مستقل جبری[۳] است.

تعریف **۹.۱.۱** فرض کنیم L توسیعی از میدان K باشد. منظور از یک پایه‌ی متعالی[۴] L روی K، زیر مجموعه‌ی مستقل جبری S از L است که عنصر بیشین (نسبت به رابطه‌ی شمول) گردایه‌ی زیر مجموعه‌های مستقل جبری L روی K می‌باشد. وجود یک چنین مجموعه‌ی را می‌توان با لم زرن اثبات کرد. عدد کاردینال مجموعه‌ی S را درجه‌ی تعالی[۵] توسیع L روی K می‌گوییم.

تعریف **۱۰.۱.۱** توسیع جبری N از میدان K را یک توسیع نرمال[۶] می‌گوییم هرگاه به ازای هر چندجمله‌ای $p(x) \in K[x]$ با ریشه‌ای در N، تمامی ریشه‌های $p(x)$ در N باشند.

تعریف **۱۱.۱.۱** فرض کنیم L یک توسیع از K باشد. مجموعه‌ی تمامی یکریختی‌های حلقه‌ای $\sigma : L \longrightarrow L$ که عناصر K را ثابت نگه می‌دارند، گروه گالوای[۷] توسیع L روی K گفته و به صورت $G_{L/K}$ نشان می‌دهیم. به ازای هر زیرگروه H از $G_{L/K}$ قرار می‌دهیم:

$$Fix(H) = \{x \in L | \forall \sigma \in H : \sigma(x) = x\},$$

به راحتی می‌توان نشان داد که $Fix(H)$ زیرمیدانی از L است.

تعریف **۱۲.۱.۱** میدان K را بسته‌ی جبری[۸] می‌گوییم هرگاه تمامی چندجمله‌ایهای غیر ثابت موجود در $K[X]$ دارای ریشه‌هایی در K باشند. کوچکترین (نسبت به رابطه‌ی شمول) توسیع جبری میدان K را بستار جبری[۹] K می‌گوییم.

[۱] finitely generated algebraic extention
[۲] algebraically dependent
[۳] algebraically independent
[۴] transcendence basis
[۵] transcendence degree
[۶] normal extention
[۷] Galois Group
[۸] algebarically closed
[۹] algebraic closur

تعریف ۱۳.۱.۱ فرض کنیم L یک توسیع جبری از میدان K باشد. می‌گوییم عنصر $a \in L$ روی K تفکیک پذیر[۱] است هرگاه ریشه‌ی ساده‌ای از چندجمله‌ای مینیمال خود باشد. توسیع L را یک توسیع تفکیک پذیر K گوییم اگر هر عنصر آن تفکیک پذیر باشند.

فرض کنیم K میدانی با مشخصه‌ی $char(K) = p$ باشد. همریختی فروبنیوس $F : K \longrightarrow K$ به صورت $F(x) = x^p$ تعریف می‌شود. هرگاه این همریختی یک‌به‌یک باشد به راحتی می‌توان دید که $F(K) = K^p$ یک زیر میدان از K است.

تعریف ۱۴.۱.۱ میدان K را یک میدان کامل[۲] می‌گوییم هرگاه $char(K) = \circ$ و یا در صورتی که $char(K) = p$، داشته باشیم $K = K^p$. به عنوان مثال میدان $\mathbb{Q}$ و تمامی میدان‌های متناهی کامل هستند.

گزاره ۱۵.۱.۱ میدان K کامل است اگر و تنها اگر هر توسیع جبری آن تفکیک‌پذیر باشد.

اثبات: [[۱۷]، گزاره‌ی 15.5]. □

تعریف ۱۶.۱.۱ توسیع جبری (متناهی و یا نا متناهی) L از میدان K را یک توسیع گالوا[۳] می‌گوییم هرگاه $K = Fix(G_{L/K})$.

گزاره ۱۷.۱.۱ توسیع جبری L از میدان K یک توسیع گالواست اگر و تنها اگر L یک توسیع نرمال و تفکیک‌پذیر از K باشد.

اثبات: [[۱۷]، گزاره‌ی 15.6.2]. □

تعریف ۱۸.۱.۱ بزرگترین توسیع گالوای میدان K را بستار تفکیک‌پذیر[۴] K گفته و با K_s نشان می‌دهیم. در واقع، K_s زیر میدانی از بستار جبری $\bar{K}$ می‌باشد که شامل تمامی عناصر تفکیک‌پذیر روی K است. از تعریف میدان کامل و گزاره‌های ۱۵.۱.۱ و ۱۷.۱.۱ نتیجه می‌شود که $K_s = \bar{K}$ هرگاه $char(K) = \circ$.

تعریف ۱۹.۱.۱ فرض کنیم I یک مجموعه‌ی اندیس‌گذار جزأ مرتب بوده و A مجموعه‌ی گروه‌ها باشد. گردایه‌ی $\{A_i, \phi_{ij}\}$ از گروه‌ها و همریختی‌های گروهی را یک دستگاه معکوس[۵] می‌گوییم هرگاه برای هر $i, j \in I$ با فرض $i \leq j$ همریختی ϕ_{ji} از A_j به A_i تعریف

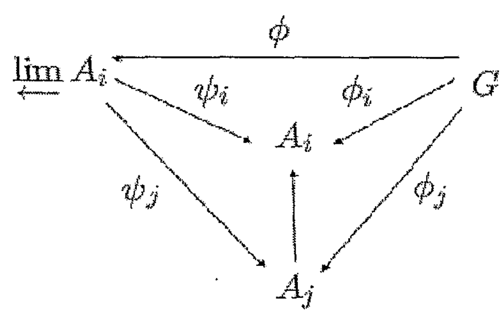
[۱] separable
[۲] perfect field
[۳] Galois extention
[۴] Galois extention
[۵] invers system

شده و در شرایط زیر صدق کنند:

(۱) ϕ_{ii} همریختی همانی روی A_i است؛

(۲) هرگاه $i \leq \ell \leq j$، آنگاه $\phi_{ji} = \phi_{\ell i}\phi_{j\ell}$.

تعریف ۲۰.۱.۱ فرض کنیم گردایه‌ی $\{A_i, \phi_{ij}\}$ یک دستگاه معکوس از گروه‌ها باشد. حد معکوس[۱] این دستگاه را به صورت $\varprojlim A_i$ نشان داده و برابر با گروهی تعریف می‌کنیم که به ازای هر $i \in I$، یک همریختی گروهی $\psi_i : \varprojlim A_i \longrightarrow A_i$ با خاصیت $\psi_i = \phi_{ji}\psi_j$ موجود باشد. همچنین به ازای هر $i \leq j$، اگر G یک گروه و $\phi_i : G \longrightarrow A_i$ و $\phi_j : G \longrightarrow A_j$ همریختی‌هایی باشند که $\phi_i = \phi_{ij}\phi_j$، آنگاه همریختی منحصر به فرد $\phi : G \longrightarrow \varprojlim A_i$ موجود باشد به طوری که نمودار زیر را جابجایی کند



تبصره ۲۱.۱.۱ فرض کنیم I یک مجموعه‌ی جزأً مرتب بوده و $i, j \in I$ دلخواه باشند. می‌توان نشان داد که حد معکوس هر دستگاه معکوس $\{A_i, \phi_{ji}\}$ از گروه ها و همریختی‌های گروهی با مجموعه‌ی عناصر (a_i) از فضای حاصل‌ضربی $\prod A_i$ برابر است به طوری که به ازای هر $i, j \in I$ با فرض $i \leq j$ داریم $\phi_{ji}a_j = a_i$. همچنین می‌توان نشان داد که این مجموعه یک گروه است. چون هر یک از گروه‌های A_i دارای توپولوژی گسسته هستند بنابراین یک توپولوژی روی $\prod A_i$ القا می‌کنند که آن را توپولوژی فرامتناهی[۲] می‌گوییم. بنابراین حد معکوس دستگاه $\{A_i, \phi_{ij}\}$ نیز به عنوان زیر فضایی از $\prod A_i$ دارای توپولوژی فرامتناهی است.

تبصره ۲۲.۱.۱ فرض کنیم I یک مجموعه‌ی جزأً مرتب و $i \leq j \in I$ باشد. هرگاه K یک میدان و L_i و L_j توسیع‌های متناهی گالوا از میدان K باشند که $K \subset L_i \subset L_j$، در این

[۱] invers limit

[۲] profinite topology

صورت یک همریختی پوشا مثل ϕ_{ij} از گروه گالوای $G_{L_j/K}$ به گروه گالوای $G_{L_i/K}$ وجود دارد. بنابراین گردایه‌ی $\{G_{L_i/K}, \phi_{ij}\}$ یک دستگاه معکوس تشکیل می‌دهد. به راحتی می‌توان نشان داد که $\varprojlim G_{L_i/K}$ حد معکوس این دستگاه یک گروه گالوای میدان K است.

قضیه ۲۳.۱.۱ (کرول[۱]) به ازای هر میدان K، گروه گالوای $G_{K_s/K}$ با حد معکوس دستگاه $\{G_{L_i/K}, \phi_{ij}\}$ یکریخت می‌باشد.

اثبات: [[۴۸]، قضیه‌ی 6.11.1]. □

تعریف ۲۴.۱.۱ منظور از یک ارزیابی گسسته[۲] روی میدان K تابعی مثل $v : K \longrightarrow \mathbb{Z}$ است به طوری که به ازای هر $x, y \in K$،

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

به عنوان قرارداد فرض می‌کنیم $v(\circ) = -\infty$. همچنین به راحتی می‌توان نشان داد مجموعه‌ی

$$R_v = \{x \in K : v(x) \geq \circ\} \subseteq K,$$

یک حلقه است که آن را حلقه‌ی ارزیابی گسسته[۳] K می‌گوییم.

در ادامه‌ی این فصل فرض می‌کنیم K یک میدان کامل، $\bar{K}$ یک بستار جبری ثابت از K و $G_{\bar{K}/K}$ گروه گالوای $\bar{K}/K$ هستند مگر این که خلاف آنها به صراحت بیان گردد.

[۱] Krull's Theorem
[۲] discrete valution
[۳] discrete valution ring

۲.۱ مباحثی از هندسه‌ی جبری

از آنجا که مبحث خم‌های بیضوی با مباحث هندسه‌ی جبری [۱] ارتباط نزدیکی دارد، در این بخش، مختصری از مباحث هندسه‌ی جبری را مطرح می‌کنیم تا بتوانیم خم‌های بیضوی را تحت عنوان یکی از ابزارهای مهم در مباحث هندسه‌ی جبری، یعنی واریته [۲]، معرفی کرده و برخی از خواص اساسی آن را مورد مطالعه قرار دهیم.

۱.۲.۱ واریته‌های جبری

تعریف ۱.۲.۱ مجموعه‌ی تمامی n - تایی‌های واقع در $\bar{K}$ یعنی مجموعه‌ی

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{(x_1, \cdots, x_n) : x_i \in \bar{K}\},$$

را n - فضای آفینی (دکارتی) [۳] روی K می‌گوییم. همچنین مجموعه‌ی

$$\mathbb{A}^n(K) = \{(x_1, \cdots, x_n) : x_i \in K\},$$

را نقاط K- گویای [۴] $\mathbb{A}^n$ می‌گوییم.

تبصره ۲.۲.۱ به راحتی می‌توان بررسی کرد که گروه گالوای $G_{\bar{K}/K}$ روی $\mathbb{A}^n$ به صورت

$$\forall \left(\sigma \in G_{\bar{K}/K}\ ,\ P \in \mathbb{A}^n\right) : P^\sigma = (x_0^\sigma, \cdots, x_n^\sigma),$$

عمل می‌کند. بنابراین می‌توان نوشت :

$$\mathbb{A}^n(K) = \left\{P \in \mathbb{A}^n | \forall\ \sigma \in G_{\bar{K}/K} : P^\sigma = P\right\}.$$

تعریف ۳.۲.۱ میدان K و عمل‌های دوتایی زیر را در نظر می‌گیریم:

$$\begin{array}{lcl} K \times K \longrightarrow K & , & K^* \times K^* \longrightarrow K^* \\ (x,y) \mapsto x+y & & (x,y) \mapsto xy \end{array}$$

[۱] algebric geometry
[۲] variety
[۳] affine (Cartesian) n-space
[۴] K-rational points