پردیس علوم
دانشکده ریاضی، آمار و علوم کامپیوتر

اعداد اول به فرم $x^2 + ny^2$

نگارنده

نگین شادگار

استاد راهنما: دکتر امیر قادرمرزی

پایان‌نامه برای دریافت درجه کارشناسی
در رشته ریاضیات و کاربردها

مرداد ۱۴۰۲

چکیده

این نوشتار به بررسی مساله‌ای تاریخی در نظریه اعداد می‌پردازد که قدمت آن به حدس‌های فرما می‌رسد.

صورت مساله: فرض کنید عدد صحیح n داده شده است. در این صورت چه اعداد اولی را می‌توان به فرم $x^2 + ny^2$ نوشت که x, y اعدادی صحیح اند؟

ما در این نوشتار از روش‌های متنوعی برای پاسخ دادن به این مساله استفاده می‌کنیم.

ابتدا از روش‌های نظریه مقدماتی اعداد از جمله نزول و تقابل مربعی، نظریه فرم‌های مربعی و نظریه گونا استفاده می‌کنیم. با وجود کارساز بودن این روش‌ها در متناهی حالت خواهیم دید که هریک دارای محدودیت‌هایی در حل مساله در حالت کلی دارند.

با درک این مفاهیم و محدودیت‌هایشان از ابزار نظریه میدان رده‌ای برای بررسی مساله در حالت کلی استفاده می‌کنیم

برای آشنایی با نظریه میدان رده‌ای در ابتدا نظریه میدان رده‌ای هیلبرت را معرفی می‌کنیم و مساله را برای نامتناهی عدد n حل می‌کنیم. سپس با بیان مفاهیم و قضایای نظریه میدان رده‌ای و معرفی حلقه میدان رده‌ای به مساله پاسخی مجرد اما کامل برای هر مقدار n خواهیم داد.

این نوشتار طرحی جامع از تلاش‌های حدودا ۳۰۰ ساله ریاضی‌دانان برای حل مساله بیان شده ارائه می‌کند و در انتها با استفاده از نظریه میدان رده‌ای جوابی برای مساله ارائه می‌کند.

سپاسگزاری

شروع این پروژه از تابستان ۱۴۰۱ (به طور دقیق تر) اوایل مرداد ماه بود. بعد از روخوانی مقدمه چند کتاب به دلیل جذابیت صورت مساله بیان شده در [۷] این کتاب را به عنوان منبع اصلی پروژه کارشناسی‌ام انتخاب کردم.

پیش از واحد پروژه، من چهار درس نظریه اعداد، نظریه جبری اعداد، جبر ۲و ۳ را با دکتر قادرمرزی گذرانده بودم و تا حد خوبی نسبت به سطح علمی و انتظارات ایشون از دانشجویان آشنایی داشتم.

بعد از شروع پروژه، متوجه شدم که تصورات من از سطح علمی دکتر، برخورد ایشون با دانشجویانشون و حمایتی که از دانشجو دارن چه در راستای یادگیری و تحقیق و چه از لحاظ حمایت روانی فراتر از سطح انتظارت من بود.

من هر هفته فرصت این رو داشتم تمام چیزایی رو که اون هفته یاد گرفته بودم و همه سوالاتی رو که داشتم (بعضا سوالای بدیهی و شایدم چرت و پرت) برای دکتر بیان کنم و ایشون واقعا با شکیبایی جواب می‌دادند (شاید هر کس دیگه‌ای بود، اینجوری با صبر جواب سوالات من رو نمی‌داد و ازم می‌خواست خودم برای همشون دنبال جواب باشم).

حتی با شروع شهریور ۱۴۰۱ و تا اواسط آبان که به دلایل شرایط پیش اومده از لحاظ روحی کشش هیچ کاری رو نداشتم، ایشون هیچ انتظاری از من در اون دوره نداشتن و حتی یه بار هم توقع نداشتن که من تو اون دوران کاری در راستای انجام پروژه انجام بدم.

از اوایل آذر ماه ۱۴۰۱ که مجددا شروع به خوندن دوبار کردم؛حدودا میشه گفت که حد خوبی از چیزایی رو که یاد گرفته بودم یادم رفته بود؛ برای همین توی چند جلسه بهم اجازه دادن که هر چی رو که تابستون خونده بودم، دوباره براشون بگم که همه چی مجددا برای من دوره بشه.

این پروژه خوندنش تا حدود اوایل شهریور ۱۴۰۲ طول کشید.

من هر هفته حدود ۲ تا ۳ ساعت از وقت دکتر رو می‌گرفتم و هر از چند گاهی هم هر سوالی که به ذهنم می‌رسید رو ازشون می‌پرسیدم.

حتی در انتهای تایپ پروژه که شاید بگم برای من سخت ترین کار بود؛ ایشون هیچ‌وقت به خاطر کم کاری‌های که من این وسطا انجام دادن عصبانی نشدن و همیشه جوری باهام رفتار کردن که فضا برای من جوری باشه که بتونم بهترین عملکرد خودم رو داشته باشم و هیچ وقت تحت فشار

نباشم.

فقط یه بار مجبور شدم یه ارائه تو قالب عصرانه بدم و الان و حتی همون زمانم برام مشخص بود که انجام این کار مطمئنا به نفع خودمه.

من توی این پروژه واقعا علاوه بر یادگیری کلی مطلب توی رشته مورد علاقه‌ام(نظریه اعداد)، تونستم روش تحقیق کردن و کلی ویژیگی‌های مهم برای کار کردن آکادمیک رو از دکتر قادرمرزی یادبگیرم.

خلاصه شاید نشه هیچ وقت نتونم بابت تمام زحمت‌هایی که دکتر قادرمرزی برام کشیدن که فراتر از وظیفه اشون بوده قدردانی کنم.

صرفا اینجا سعی کردم بگم اگه من و شاید خیلی از دوستانم الان داریم به ریاضی و زندگی آکادمیک فکر می‌کنیم، مدیون زحمات ایشون هستیم.

نگین شادگار
پاییز ۱۴۰۲

پیشگفتار

برخی فرما [1] را به دلیل بیان حدسیات و گزاره هایی که منجر به نظریه‌هایی مهم در نظریه اعداد شده است به عنوان پدر نظریه اعداد مدرن می‌شناسند.

در واقع می‌توان ریشه های تاریخی نظریه میدان رده‌ای [2] را که یکی از مهم‌ترین شاخه‌های نظریه جبری اعداد است را نیز به فرما ارتباط داد. وی در نامه ای به مرسن [3] در تاریخ ۲۵ دسامبر ۱۶۴۰ قضیه زیر را بیان کرد.

قضیه ۱ (قضیه فرما). *فرض کنید p عدد اول است. در این صورت:*

«p را می‌توان به فرم x^2+y^2 برای $x,y\in\mathbb{Z}$ نمایش داد اگر و تنها اگر $p\overset{4}{\equiv}1$.» [4]

قضیه فرما یکی از مقدماتی ترین قضایای نظریه اعداد است؛ که در اکثر کتاب‌های نظریه مقدماتی اعداد یافت می‌شود. فرما در ادامه چند گزاره در ارتباط با نمایش اعداد اول به فرم x^2+ny^2 برای $n>1$ نیز ارائه کرد. این گزاره‌ها منجر به بیان مساله زیر شد:

مساله ۱. *فرض کنید $n\in\mathbb{Z}^{\geq 1}$ داده شده است. در این صورت چه اعداد اولی را می‌توان به صورت*

$$p=x^2+ny^2$$

نمایش داد به طوری که $x,y\in\mathbb{Z}$ باشند؟

در این نوشتار به مساله ذکر شده پاسخ جامعی داده خواهد شد و در طول مسیر ایده‌های متنوعی از نظریه اعداد و نظریه جبری اعداد مورد بررسی قرار خواهد گرفت.

این ایده‌ها که به ترتیب سیر تاریخی در این نوشته گنجانده شده اند هر یک دارای محدودیت هایی برای حل مساله ۱ در حالت کلی اند.

جامع ترین پاسخ به مساله ۱ در بخش سوم و با بیان نظریه میدان رده‌ای صورت می‌گیرد.

---

[1] Fermat

[2] Class Field Theory

[3] Mersenne

[4] از دیدگاه مدرن نظریه جبری اعدادی می‌دانیم که این مساله به نحوه تجزیه عدد اول p در حلقه $\mathbb{Z}[i]$ می پردازد.

هدف نظریه میدان رده‌ای توصیف توسیع‌های گالوای میدان های موضعی و سراسری بر اساس خواص میدان پایه است. برای توسیع های آبلی، این نظریات تقریبا بین سال‌های ۱۸۵۰ تا ۱۹۳۰ توسط کرونکر [۵] ، وبر [۶] ، هیلبرت [۷] ، تاکاگی [۸] ، آرتین [۹] ، هسه [۱۰] و... گسترش یافت.

برای توسیع‌های ناآبلی، اولین اشاره به چگونگی این نظریات در نامه‌ای از لنگندز [۱۱] به ویل [۱۲] در سال ۱۹۶۷ مشاهده می‌شود.

شروع سیر تحول این نظریات از قانون تقابل مربعی بیان شده توسط گاوس است و پیشرفت و توسیع مفاهیم نظریه میدان رده‌ای را می‌توان به عنوان پروژه بلند مدتی در نظریه جبری اعداد در نظر گرفت.

از کاربردهای نظریه میدان رده‌ای می‌توان به اثبات دوگانی آرتین - وردیه [۱۳] و کاربرد آن در شاخه‌هایی از نظریه جبری اعداد از جمله نظریه ایواساوا [۱۴] و نظریه گالوا- مدول‌ها [۱۵] اشاره نمود.

در این نوشتار تلاش می‌شود؛ ضمن بررسی مساله ۱ ، مفاهیم مختلفی در راستای پاسخ به مساله بیان می‌شود.

این نوشته در ۳ بخش تدوین شده است.

تمامی مقدمات مورد نیاز که پیشنیازهای مفاهیم فصل‌های ۲و۳ اند در بخش ۱ گنجانده شده است. با وجود این که سعی شده تا تمامی مفاهیم به طور دقیق بیان، اثبات و یا ارجاع داده شود اما در نگارش این پایان نامه آشنایی با مفاهیم نظریه گروه‌ها، نظریه حلقه‌ها، نظریه میدان‌ها، نظریه مدول‌ها، نظریه مقدماتی اعداد، نظریه جبری اعداد مقدماتی در سطح دروس کارشناسی فرض گرفته شده است.

بخش دوم این نوشتار اختصاص به روش‌های مقدماتی در حل مساله ۱ دارد. این بخش شامل دو فصل است که در هر یک از فصل با رعایت سیر تاریخی، ایده‌های ریاضیدانانی چون اویلر [۱۶] ، گاوس [۱۷] ، لاگرانژ [۱۸] و لژاندر [۱۹] را بررسی می‌کند. در این بخش با ارائه مفاهیم مقدماتی نظریه

---

[5] Kronecker
[6] Weber
[7] HIlbert
[8] Takagi
[9] Artin
[10] Hasse
[11] Langlands
[12] Weil
[13] Artin–Verdier duality
[14] Iwasawa theory
[15] Galois modules theory
[16] Euler
[17] Guass
[18] Lagrange
[19] Legendre

اعدادی (تقابل مربعی [۲۰] و نزول [۲۱])، نظریه فرم‌های مربعی [۲۲] و نظریه گونا [۲۳] سعی به حل مساله ۱ خواهیم داشت. با وجود موثر بودن این روش‌ها در حل مساله ۱ در تعداد متناهی n به دلیل وجود محدودیت‌هایی که این روش‌ها قادر به رفع آن نیستند؛ نیاز به بیان نظریه‌هایی قدرتمند تر می‌باشیم.

در بخش سوم این نوشتار (که بخش اصلی ای پایان نامه محسوب می شود) در ابتدا با بیان نظریه میدان رده‌ای هیلبرت [۲۴] پاسخی به مساله ۱ در نامتناهی مقدار n می‌دهیم. برای ارائه جامع‌ترین پاسخ ملزم به یادگیری مفاهیم و قضایای میدان رده‌ای هستیم در انتها با استفاده از این مفاهیم کامل ترین پاسخ ممکن را برای مساله ۱ می‌دهیم.

بخش چهارم این نوشتار پیوستی در ارتباط با مطالب بخش‌های قبلی است که در سه فصل نگارش شده است. در این بخش سعی شده تا مطالبی اضافه ولی مرتبط با موضوع پروژه و مفاهیم سه بخش قبلی گنجانده شود.

در این نوشتار سعی شده تا علاوه بر بیان مفاهیم و نظریات بیان شده، ارتباطی بین مفاهیم مقدماتی نظریه اعداد و نظریه میدان رده‌ای که یکی از مهم‌ترین شاخه‌های نظریه جبری اعداد است؛ از طریق حل مساله ۱ داده شود.

---

[20] Quadratic Reciprocity
[21] Descent
[22] Theory of Quadratic Forms
[23] Genus Theory
[24] Hilbert Class Field Theory

فهرست مطالب

بخش اول

پیشنیازها

فصل ۱

مروری بر مفاهیم اولیه

در این فصل به به صورت اجمالی به بیان نمادها و مفاهیمی که در فصل‌های آینده از آن‌ها استفاده می‌کنیم؛ می‌پردازیم.

۱.۱ نظریه میدان‌ها

تعریف ۱.۱. *به توسیع‌های میدان $\mathbb{Q}$ میدان عددی می‌گوییم.*

تعریف ۲.۱. *توسیع جبری L/K را نرمال [1] گوییم. اگر برای هر چندجمله‌ای تحویل ناپذیر روی K مانند f که دارای ریشه‌ای در L باشد؛ f را بتوان به صورت عوامل خطی روی $K[x]$ تجزیه کرد.*

تعریف ۳.۱. *توسیع جبری L/K را جدایی پذیر [2] گوییم اگر برای هر $\alpha \in L$ چندجمله‌ای مینیمال α روی K جدایی پذیر باشد.*

تعریف ۴.۱. *توسیع جبری L/K را گالوا [3] گوییم اگر دارای یکی از شرایط زیر باشد:*

- *L/K یک توسیع نرمال و جدایی پذیر باشد.*
- *$|Aut(L/K)| = [L : K]$*
- *L میدان شکافنده چندجمله‌ای های جدایی پذیر روی K باشد.*
- *K دقیقا مجموعه‌ای باشد که توسط تمامی عناصر $Aut(L/K)$ ثابت نگه داشته می‌شود.*

[1] Normal Extension
[2] Separable Extension
[3] Galois Extension

برای مشاهده جزئیات بیشتر به [۱۰ ، فصل ۱۴] رجوع کنید.

تعریف ۵.۱. *میدان عددی $K/\mathbb{Q}$ را مربعی [۴] گوییم اگر $K = \mathbb{Q}\sqrt{N}$ که $N \in \mathbb{Z}$ باشد.*

تعریف ۶.۱. *توسیع L/K را آبلی گوییم اگر $Gal(L/K)$ آبلی باشد.*

[4] Quadratic Extension

۲.۱ حلقه اعداد صحیح جبری

تعریف ۷.۱. *حوزه صحیح R یک حلقه ددکیند [۵] است هرگاه دارای سه شرط زیر باشد:*

- *حلقه R نوتری باشد.*
- *حلقه R صحیح بسته باشد.*
- *ایده‌آل های ماکسیمال و اول R یکی باشند.*

تعریف ۸.۱. *فرض کنید $\alpha \in \mathbb{C}$ است. در این صورت α عدد صحیح جبری است؛ اگر ضرایب چند جمله‌ای مینیمال α اعداد صحیح باشند.*

تعریف ۹.۱. *$K/\mathbb{Q}$ را در نظر بگیرید. در این صورت $\mathcal{O}_K$ را مجموعه همه اعداد صحیح جبری $\mathbb{Q}$ در K در نظر می‌گیریم (در واقع $\mathcal{O}_K$ بستار صحیح $\mathbb{Z}$ در K است).*

$$\begin{array}{ccc} \mathcal{O}_K & \text{——} & K \\ | & & | \\ \mathbb{Z} & \text{——} & \mathbb{Q} \end{array}$$

گزاره ۱۰.۱. *$\mathcal{O}_K$ یک حوزه ددکیند است.*

اثبات. برای اثبات به [۳۰، قضیه ۱.۳] رجوع کنید. □

گزاره ۱۱.۱. *فرض کنید $K/\mathbb{Q}$ است. آنگاه:*

۱. *$\mathcal{O}_K$ زیر حلقه‌ای از $\mathbb{C}$ با میدان کسرهای K است.*

۲. *$\mathcal{O}_K$ یک $\mathbb{Z}$- مدول آزاد از مرتبه $[K : \mathbb{Q}]$ است.*

اثبات. برای اثبات (۱) به [۱، ۲.۲] و برای (۲) به [۳۰، گزاره ۱۰.۲.۱] رجوع کنید. □

لم ۱۲.۱. *فرض کنید K میدان عددی و $\mathfrak{a}$ ایده‌آلی ناصفر از $\mathcal{O}_K$ است. در این صورت حلقه خارج قسمتی $\mathcal{O}_K/\mathfrak{a}$ متناهی است ($|\mathcal{O}_K/\mathfrak{a}|$ را نرم ایده‌آل $\mathfrak{a}$ در نظر می‌گیریم).*

اثبات. برای مشاهده اثبات به [۳۴، ص ۱۱۵ - ۱۱۶] رجوع کنید. □

[5] Dedekind Domain

تعریف ۱۳.۱. *فرض کنید A حوزه صحیح با میدان کسرهای K است. ایده‌آل کسری $\mathfrak{a}$ یک A- مدول متناهیا تولید شده از K است. در واقع $\mathfrak{a}$ به فرم زیر است که $\mathfrak{c}$ ایده‌آل و γ عضوی ناصفر از A است.*

$$\frac{1}{\gamma}\mathfrak{c}$$

ایده‌آل $\mathfrak{a}$ را کسری اصلی گوییم اگر $\mathfrak{c}$ ایده‌آلی اصلی باشد.

قضیه ۱۴.۱. *مجموعه ایده آل های کسری $\mathcal{O}_K$ تشکیل گروهی آبلی می دهند. عنصر همانی $\mathcal{O}_K$ و وارون ایده‌آل کسری $\mathfrak{a}$ ایده‌آل کسری زیر است.*

$$\mathfrak{a}^{-1} = \{x \mid x\mathfrak{a} \subseteq \mathcal{O}_K\}$$

اثبات. برای اثبات به قضیه [۲۲، ص ۱۰۱ - ۱۰۲] رجوع کنید. □

نمادگذاری ۱۵.۱. *حلقه $\mathcal{O}_K$ در نظر بگیرید. در این صورت:*

- *I_K را گروه ایده‌آل‌های کسری $\mathcal{O}_K$ می‌نامیم.*
- *P_K را زیرگروهی از I_K که شامل ایده‌آل‌های کسری اصلی در نظر بگیرید.*
- *گروه خارج قسمتی I_K/P_K را با $C(\mathcal{O}_K)$ نمایش داده و گروه رده‌ای می نامیم.*

گزاره ۱۶.۱. *حلقه $\mathcal{O}_K$ و ایده‌آل کسری ناصفر $\mathfrak{a}$ از $\mathcal{O}_K$ را در نظر بگیرید. در این صورت*

$$\mathfrak{a} = \prod_{i=1}^{r} p_i^{\alpha_i} \qquad (۱.۱)$$

که p_i ها ایده‌آل‌های اول متمایزند و $\alpha_i \in \mathbb{Z}$ است (نمایش (۱.۱) یکتاست).

اثبات. برای مشاهده اثبات به [۳۰، قضیه ۳.۳.۱] رجوع کنید. □

۳.۱ میدان‌های مربعی

میدان مربعی، میدانی به فرم $K = \mathbb{Q}(\sqrt{N})$ که $N \neq ۰, ۱$ عدد صحیح خالی از مربع است. در این صورت مفاهیم زیر را برای میدان K تعریف می‌کنیم.

تعریف ۱۷.۱. *مبین [۶] میدان $K = \mathbb{Q}(\sqrt{N})$ را با d_K نمایش داده و به صورت زیر تعیین می‌کنیم (برای مطالعه جزئیات بیشتر درباره مبین به بخش ۳.۳ [۲۲] رجوع کنید).*

$$d_K = \begin{cases} N & N \equiv ۱ \bmod ۴ \\ ۴N & \text{در غیر این صورت} \end{cases} \qquad (۲.۱)$$

گام بعدی تعیین حلقه اعداد صحیح جبری میدان های مربعی است با استفاده از گزاره زیر می‌توان برای میدان $K = \mathbb{Q}(\sqrt{N})$ حلقه $\mathcal{O}_K$ تعیین کرد.

گزاره ۱۸.۱. *برای $K = \mathbb{Q}(\sqrt{N})$، $\mathcal{O}_K$ به صورت زیر تعیین می‌شود.*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{N}] & N \not\equiv ۱ \bmod ۴ \\ \\ \mathbb{Z}[\frac{۱+\sqrt{N}}{۲}] & N \equiv ۱ \bmod ۴ \end{cases} \qquad (۳.۱)$$

اثبات. برای مشاهده اثبات به [۲۲، گزاره ۳۴.۲] رجوع کنید. □

لم ۱۹.۱. *برای میدان مربعی K می‌توان $\mathcal{O}_K$ را با استفاده از مبین نیز نمایش داد یعنی :*

$$\mathcal{O}_K = \mathbb{Z}[\tfrac{d_K+\sqrt{d_K}}{۲}].$$

اثبات.

$$N \overset{۴}{\not\equiv} ۱ \Rightarrow d_K = ۴N \Rightarrow \mathbb{Z}[\frac{۴N + \sqrt{۴N}}{۲}] = \mathbb{Z}[۲N + \sqrt{N}] = \mathbb{Z}[\sqrt{N}]$$

$$\underbrace{N \overset{۴}{\equiv} ۱}_{N=۴x+۱} \Rightarrow d_K = N \Rightarrow \mathbb{Z}[\frac{۴x + ۱ + \sqrt{N}}{۲}] = \mathbb{Z}[۲x + \frac{۱ + \sqrt{N}}{۲}] = \mathbb{Z}[\frac{۱ + \sqrt{N}}{۲}]$$

□

[6] Discriminant

فصل ۲

نظریه انشعاب

در فصل قبلی اشاره کردیم که ایده‌آل‌های کسری در $\mathcal{O}_K$ دارای تجزیه یکتا به ایده‌آل‌های اول دارند. در این فصل به مطالعه دقیق تجزیه ایده‌آل‌ها در میدان بالاتر می‌پردازیم.
برای اطلاعات بیشتر به [۳۰، فصل ۹.۱] رجوع کنید.

۱.۲ مفاهیم اولیه

در این فصل فرض کنید L/K توسیع جبری و $\mathcal{O}_K$ و $\mathcal{O}_L$ به ترتیب حلقه اعداد صحیح جبری میدان‌های K و L است. ایده‌آل ناصفر و اول $\mathfrak{p}$ از $\mathcal{O}_K$ را در نظر بگیرید. در این صورت با برای ایده‌آل $\mathfrak{p}\mathcal{O}_L$ تجزیه‌ای یکتا به ایده‌آل‌های اول در $\mathcal{O}_L$ دارد (گزاره ۱۶.۱).

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{ei} \qquad (۱.۲)$$

که $\mathfrak{P}_i$ ها ایده‌آل‌های اول متمایز $\mathcal{O}_L$ شامل $\mathfrak{p}$ اند.

تعریف ۱.۲. *با توجه به نمادگذاری بالا مفاهیم زیر را تعریف می‌کنیم.*

- e_i *را که با* $e_{\mathfrak{P}_i|\mathfrak{p}}$ *نیز نمایش می‌دهند؛ اندیس (شاخص) انشعاب* [۱] $\mathfrak{p}$ *در* $\mathfrak{P}_i$ *می‌نامیم.*
- *توسیع* $\mathcal{O}_L/\mathfrak{P}_i$ *روی* $\mathcal{O}_K/\mathfrak{p}$ *را در نظر بگیرید. درجه این توسیع را با* f_i *یا* $f_{\mathfrak{P}_i|\mathfrak{p}}$ *نمایش داده و درجه اینرسی* [۲] $\mathfrak{p}$ *در* $\mathfrak{P}_i$ *می‌نامیم.*

لم ۲.۲. *توسیع* $\mathcal{O}_L/\mathfrak{P}_i$ *روی* $\mathcal{O}_K/\mathfrak{p}$ *توسیع نرمال است. بنابراین این توسیع گالوا است.*

[1] Ramification Index
[2] Inertial Degree

اثبات. برای اثبات نرمال بودن توسیع ذکر شده به [۳۰، قضیه ۴.۹.۱] و برای اثبات گالوا بودن به مفاهیم [۱۰، فصل ۱۴] رجوع کنید. این لم در ادامه و در فصل ۱.۲ اثبات می‌شود. □

تعریف ۳.۲. *با توجه به تعریف بالا داریم:*

- *اگر برای هر* $i \in \{۱, ۲, ..., r\}$ ، $f_i = e_i = ۱$ *باشد؛ می‌گوییم* $\mathfrak{p}$ *در* $\mathcal{O}_L$ *به طور کامل شکافته* [۳] *می‌شود.*
- *اگر* $\exists i \in \{۱, ۲, ..., r\}$ *که* $e_i > ۱$ *باشد؛ می‌گوییم* $\mathfrak{p}$ *در* $\mathcal{O}_L$ *منشعب* [۴] *می‌شود.*
- *اگر* $\mathfrak{p}\mathcal{O}_L$ *ایده‌آل اولی از* $\mathcal{O}_L$ *باشد؛ می‌گوییم* $\mathfrak{p}$ *در* $\mathcal{O}_L$ *اول باقی می‌ماند* [۵] .

با توجه به تعریف بالا توسیع جبری L/K را نامنشعب [۶] می‌نامیم. اگر شاخص انشعاب هر اول ناصفر $\mathfrak{p} \in K$ در L کمتر مساوی ۱ شود.

لم ۴.۲. *تعداد متناهی از اول‌های (ایده‌آل های اول)* K *در* L *منشعب می‌شود.*

اثبات. برای مشاهده اثبات به [۲۷، نتیجه ۳] رجوع کنید. □

قضیه ۵.۲. *فرض کنید* L/K *میدان‌های عددی و* $\mathfrak{p}$ *اول (ایده‌آل اول)* K *است. با توجه به تعریف ۱.۲ و (۱.۲) می‌توان درباره ارتباط* e_i *و* f_i *برای* $i \in \{۱, ۲, ..., r\}$ *گفت:*

$$\sum_{i=۱}^{r} e_i f_i = [L : K]$$

اثبات. برای اثبات به [۲۹، قضیه ۳۴.۳] رجوع کنید. □

لم ۶.۲. *فرض کنید* $K \subset M \subset K$ *میدان های عددی اند.* $\mathfrak{p}$ *ایده‌آل اولی در* $\mathcal{O}_K$ *و*

$$\mathfrak{p} \subset \mathfrak{P} \subset \mathfrak{P}'$$

که $\mathfrak{P}$ *و* $\mathfrak{P}'$ *به ترتیب ایده‌آل‌های اول* $\mathcal{O}_M$ *و* $\mathcal{O}_L$ *اند.*

۱. $e_{\mathfrak{P}'|\mathfrak{p}} = e_{\mathfrak{P}'|\mathfrak{P}} \cdot e_{\mathfrak{P}|\mathfrak{p}}$

۲. $\mathfrak{p}$ *در* L *نامنشعب است اگر و تنها اگر* $\mathfrak{p}$ *در* M *نامشعب و هر ایده‌آل اول* $\mathcal{O}_M$ *شامل* $\mathfrak{p}$ *در* L *نامنشعب باشد.*

---

[3] Splits completely
[4] Ramifies
[5] Inerts
[6] Unramified Extension

۳. *L توسیعی نامنشعب از K است اگر و تنها اگر L روی M و M روی K نامنشعب باشد.*

اثبات. به وضوح قسمت (۲) و (۳) نتیجه قسمت (۱) اند.

برای قسمت (۲) توجه داشته باشید که نامنشعب بودن $\mathfrak{p}$ یعنی شاخص انشعاب در تجزیه به ایده‌آل‌های اول برابر ۱ باشد.

برای قسمت (۳) ، توسیعی را نامنشعب می‌نامیم که شاخص انشعاب هر ایده‌آل در تجزیه به ایده‌آل‌های اول در میدان بالاتر برابر ۱ باشد.

بنابراین با توجه به توضیحات داده شده، کافی است قسمت (۱) را اثبات کنیم:

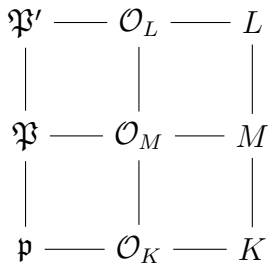
فرض کنید تجزیه $\mathfrak{p}$ در M برابر

$$\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_{\mathfrak{P}_i|\mathfrak{p}}}$$

است. برای سادگی $\mathfrak{P}_1 = \mathfrak{P}$ قرار دهید و سپس تجزیه $\mathfrak{P}$ را در L به صورت

$$\mathfrak{P} = \prod_{i=1}^{r} \mathfrak{P}_i'^{e_{\mathfrak{P}_i'|\mathfrak{P}}}$$

در نظر بگیرید و برای سادگی $\mathfrak{P}_1' = \mathfrak{P}'$ در نظر بگیرید در این صورت با توجه به نمودار زیر و یکتایی تجزیه در حلقه اعداد صحیح جبری داریم:



$$\Rightarrow (\mathfrak{P}'^{e_{\mathfrak{P}'|\mathfrak{P}}})^{e_{\mathfrak{P}|\mathfrak{p}}} = (\mathfrak{P}')^{e_{\mathfrak{P}'|\mathfrak{P}} \cdot e_{\mathfrak{P}|\mathfrak{p}}} \Rightarrow e_{\mathfrak{P}'|\mathfrak{p}} = e_{\mathfrak{P}'|\mathfrak{P}} \cdot e_{\mathfrak{P}|\mathfrak{p}}.$$

□

۲.۲ گروه‌های تجزیه و اینرسی

مساله تجزیه ایده‌آل‌های اول K در L زمانی که L/K گالوا، بسیار مهم است. بنابراین در ادامه فصل L/K را توسیع گالوا در نظر بگیرید [۷].

نمادگذاری ۷.۲. *گروه گالوای L/K را با $Gal(L/K) = G$ نمایش می‌دهیم.*

فرض کنید L/K توسیع گالوا و $\mathcal{O}_K$ و $\mathcal{O}_L$ به ترتیب حلقه اعداد صحیح جبری میدان‌های K و L است. تجزیه ایده‌آل اول ناصفر $\mathfrak{p}$ از $\mathcal{O}_K$ در $\mathcal{O}_L$ را به صورت:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{ei}$$

که $\mathfrak{P}_i$ ها ایده‌آل‌های اول متمایز $\mathcal{O}_L$ شامل $\mathfrak{p}$ اند؛ در نظر بگیرید. $e_i = e_{\mathfrak{P}_i|\mathfrak{p}}$ را اندیس انشعاب و $f_i = f_{\mathfrak{P}_i|\mathfrak{p}}$ را اندیس اینرسی $\mathfrak{p}$ در $\mathfrak{P}_i$ نامیدیم.
حال با توجه به مفاهیم بیان شده می‌توان گزاره‌ها و قضایای زیر را بیان نمود:

قضیه ۸.۲. *فرض کنید L/K توسیع گالوا و p ایده‌آل اول K است.*

۱. *گروه گالوای $Gal(L/K) = G$ به صورت متعددی روی اول‌های L شامل $\mathfrak{p}$ عمل می‌کند (یعنی اگر $\mathfrak{P}$ و $\mathfrak{P}'$ دو اول از L شامل $\mathfrak{p}$ باشند. در این صورت:*

$$.(\exists \sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}'$$

۲. *فرض کنید $\mathfrak{P}_1, ..., \mathfrak{P}_r$ اول‌های L شامل $\mathfrak{p}$ اند، درجه انشعاب و اینرسی $\mathfrak{p}$ در همگی $\mathfrak{P}_i$ ها برابر است (یعنی برای هر $i \in \{1, ..., r\}$ داریم:*

$$.(e_i = e, \quad f_i = f$$

به علاوه طبق قضیه ۵.۲ خواهیم داشت:

$$efr = [L : K].$$

اثبات. برای اثبات قسمت (۱) به [۳۰، گزاره ۱.۹] و برای قسمت (۲) به [۳۰، ص ۵۵] رجوع کنید. □

یادداشت ۹.۲. *با توجه به قضیه بالا میتوان مفاهیم تعریف ۳.۲ برای توسیع گالوای L/K و ایده‌آل اول $\mathfrak{p}$ مجددا نوشت.*

[۷] برای یادآوری توسیع گالوا به ۴.۱ رجوع کنید.

- *اگر* $f = e = ۱$ *باشد؛ می‌گوییم* $\mathfrak{p}$ *در* $\mathcal{O}_L$ *به طور کامل شکافته می‌شود.*
- *اگر* $e > ۱$ *باشد؛ می‌گوییم* $\mathfrak{p}$ *در* $\mathcal{O}_L$ *منشعب می‌شود.*

در ادامه نیازمند مفاهیم گروه تجزیه [۸] و اینرسی [۹] هستیم بدین منظور نمودار زیر را در نظر بگیرید ($\mathfrak{p}$ ایده‌آل اول K و $\mathfrak{P}$ اول L شامل $\mathfrak{p}$ است).

$$\begin{array}{ccccc} \mathfrak{P} & - & \mathcal{O}_L & - & L \\ | & & | & & | \\ \mathfrak{p} & - & \mathcal{O}_K & - & K \end{array}$$

تعریف ۱۰.۲. *گروه زیر را گروه تجزیه* $\mathfrak{P}$ *در* $\mathcal{O}_L$ *می‌نامیم.*

$$G_{\mathfrak{P}} = \{\sigma \in Gal(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

تعریف ۱۱.۲. *گروه زیر را گروه اینرسی* $\mathfrak{P}$ *در* $\mathcal{O}_L$ *می‌نامیم.*

$$I_{\mathfrak{P}} = \{\sigma \in Gal(L/K) \mid \forall \alpha \in \mathcal{O}_L : \sigma(\alpha) \overset{\mathfrak{P}}{\equiv} \alpha\}.$$

برای هر $\sigma \in G_{\mathfrak{P}}$ می‌توان خودریختی ای به $\mathcal{O}_L/\mathfrak{P}$ القا نمود که میدان $\mathcal{O}_K/\mathfrak{p}$ را ثابت نگه دارد. بدین معنا که:

$$\begin{gathered} \tilde{\sigma} : \mathcal{O}_L/\mathfrak{P} \longrightarrow \mathcal{O}_L/\mathfrak{P} \\ a \bmod \mathfrak{P} \mapsto \sigma(a) \bmod \mathfrak{P} \end{gathered}$$

گزاره ۱۲.۲. *بنابر توضیحات بالا می‌توان همریختی پوشا زیر را تعریف کرد.*

$$\begin{gathered} G_{\mathfrak{P}} \longrightarrow \tilde{G} = Gal(\tfrac{\mathcal{O}_L/\mathfrak{P}}{\mathcal{O}_K/\mathfrak{p}}) \\ \sigma \longmapsto \tilde{\sigma} \end{gathered}$$

هسته همریختی بالا $I_{\mathfrak{P}}$ *و بنابراین می‌توان گفت* $G_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \tilde{G}$.

اثبات. برای مشاهده اثبات به [۳۰، ص ۵۶ - ۵۷] رجوع کنید. □

نتیجه ۱۳.۲. $|G_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}$ و $|I_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}}$.

[8] Decomposition Group
[9] Inertia Group

اثبات. $G_{\mathfrak{P}}$ پایدار ساز عمل گروه گالوای L/K روی مجموعه اول‌های L شامل $\mathfrak{p}$ است (این مجموعه را برابر $\{\mathfrak{P}_1, ..., \mathfrak{P}_r\}$ قرار دهید). چون همه این اول‌ها در یک مدار قرار دارند. بنابراین:

$$r = \frac{|Gal(L/K)|}{|G_{\mathfrak{P}}|} \Rightarrow r = \frac{efr}{|G_{\mathfrak{P}}|}$$
$$\Rightarrow |G_{\mathfrak{P}}| = ef$$

باتوجه به گزاره بالا:

$$G_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \tilde{G} \Rightarrow |\frac{G_{\mathfrak{P}}}{I_{\mathfrak{P}}}| = |\tilde{G}| = |Gal(\frac{\mathcal{O}_L/\mathfrak{P}}{\mathcal{O}_K/\mathfrak{p}})|$$
$$\Rightarrow |\frac{ef}{I_{\mathfrak{P}}}| = f \Rightarrow |I_{\mathfrak{P}}| = e$$

□

گزاره ۱۴.۲. *فرض کنید L/K توسیع گالوا باشد. آنگاه $\exists \alpha \in \mathcal{O}_L$ به طوری که $L = K(\alpha)$ و $f(x)$ چند جمله‌ای مینیمال α روی K است ($f(x) \in \mathcal{O}_K[x]$). اگر $\mathfrak{p}$ ایده‌آل اولی در K و $f(x)$ در پیمانه $\mathfrak{p}$ جدایی پذیر باشد. آنگاه:*

۱. *$\mathfrak{p}$ در L نامشعب است.*

۲. *فرض کنید $f(x) \overset{\mathfrak{p}}{\equiv} f_1(x)...f_r(x)$ که $f_i(x)$ ها تکین، متمایز و تحویل ناپذیزند. در این صورت*

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$$

ایده‌آل اولی از $\mathcal{O}_L$ است. اگر $i \neq j$ باشد؛ $\mathfrak{P}_i$ و $\mathfrak{P}_j$ متمایزند. بنابراین:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1...\mathfrak{P}_r$$

به علاوه برای هر $i \in \{1, ..., r\}$ درجه همه‌ی $f_i(x)$ ها برابر و مساوی f است.

۳. *$\mathfrak{p}$ در L کاملا شکافته می‌شود اگر و تنها اگر $f(x) \overset{\mathfrak{p}}{\equiv} 0$ دارای جوابی در $\mathcal{O}_K$ باشد.*

اثبات. برای اثبات قسمت (۲) به [۳۰، گزاره ۳.۸.۱] رجوع کنید. با استفاده از قسمت (۲) دیگر بخش‌ها را اثبات می‌کنیم. در صورتی که درستی قسمت (۲) اثبات شده باشد؛ داریم:

(۱) : از آنجایی که $\mathfrak{P}_i$ ها در تجزیه ارائه شده متمایزند در این صورت با توجه به تعریف $\mathfrak{p}$ نامنشعب است.

(۳) : توجه داشته باشید که $deg(f) = [L : K]$ است.
اگر $\mathfrak{p}$ در L کاملا شکافته شود؛ $f = ۱$ و برای هر $i \in \{۱, ..., r\}$ ، $f_i(x)$ خطی خواهد بود بنابراین به وضوح $f(x) \overset{\mathfrak{p}}{\equiv} ۰$ در $\mathcal{O}_K$ جواب دارد.
برای مسیر عکس:
اگر $f(x) \overset{\mathfrak{p}}{\equiv} ۰$ در $\mathcal{O}_K$ ریشه‌ای داشته باشد به دلیل تکین و تحویل ناپذیر بودن $f_i(x)$ ها ،می‌توان گفت حداقل یکی از آن‌ها خطی است. طبق قسمت (۲) می‌دانیم درجه همه $f_i(x)$ ها برابر است و اثبات تکمیل می‌شود.

□

لم ۱۵.۲. *فرض کنید $K \subset M \subset L$ زنجیری از توسیع‌های میدانی است که L/K گالواست. آنگاه ایده‌آل $\mathfrak{p}$ در L کاملا شکافته می‌شود اگر و تنها اگر $\mathfrak{p}$ در M کاملا شکافته شود و ایده‌آلی اول از $\mathcal{O}_M$ شامل $\mathfrak{p}$ در L کاملا شکافته شود.*

اثبات. نمودار زیر را در نظر بگیرید:

$$\begin{array}{ccccc}
\mathfrak{P}' \in \{\mathfrak{P}'_{ij}\}_{۱\le i,j\le r} & \text{———} & \mathcal{O}_L & \text{——} & L \\
\Big| & & \Big| & & \Big| \\
\mathfrak{P} \in \{\mathfrak{P}_i\}_{۱\le i\le r} & \text{———} & \mathcal{O}_M & \text{——} & M \\
\Big| & & \Big| & & \Big| \\
\mathfrak{p} & \text{———————} & \mathcal{O}_K & \text{——} & K
\end{array}$$

که $\{\mathfrak{P}_i\}_{۱\le i\le r}$ اول‌های شامل $\mathfrak{p}$ در $\mathcal{O}_M$ و $\{\mathfrak{P}_{ij}\}_{۱\le i,j\le r}$ اول‌های شامل $\mathfrak{P}_i$ ها در $\mathcal{O}_L$ اند. زنجیر $\mathfrak{P}' \subset \mathfrak{P} \subset \mathfrak{p}$ را در نظر بگیرید. باتوجه به لم ۶.۲ داریم که:

$$e_{\mathfrak{P}'|\mathfrak{p}} = e_{\mathfrak{P}'|\mathfrak{P}} \cdot e_{\mathfrak{P}|\mathfrak{p}}$$

در این صورت برای درجه اینرسی خواهیم داشت:

$$\begin{aligned} f_{\mathfrak{P}|\mathfrak{p}} &= [\mathcal{O}_L/\mathfrak{P}' : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_L/\mathfrak{P}' : \mathcal{O}_M/\mathfrak{P}][\mathcal{O}_M/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] \\ &= f_{\mathfrak{P}'|\mathfrak{P}} \cdot f_{\mathfrak{P}|\mathfrak{p}}. \end{aligned}$$

و درجه اینرسی نیز ضربی خواهد بود.
فرض کنید $\mathfrak{p} \subset \mathcal{O}_K$ کاملا در L شکافته می‌شود بنابراین $[L : K] = r$ ، $e = f = ۱$ است. در این صورت با توجه به ضربی بودن درجه اینرسی و شاخص انشعاب داریم:

$$\begin{aligned} ۱ = e_{\mathfrak{P}'|\mathfrak{p}} &= e_{\mathfrak{P}'|\mathfrak{P}} \cdot e_{\mathfrak{P}|\mathfrak{p}} \\ \Rightarrow e_{\mathfrak{P}'|\mathfrak{P}} &= e_{\mathfrak{P}|\mathfrak{p}} = ۱ \end{aligned}$$

و

$$۱ = f_{\mathfrak{P}'|\mathfrak{p}} = f_{\mathfrak{P}'|\mathfrak{P}} \cdot f_{\mathfrak{P}|\mathfrak{p}}$$
$$\Rightarrow f_{\mathfrak{P}'|\mathfrak{P}} = f_{\mathfrak{P}|\mathfrak{p}} = ۱$$

بنابراین $\mathfrak{p}$ در M کاملا شکافته می‌شود.
برای اثبات عکس:
فرض کنید $\mathfrak{p} \subset \mathcal{O}_K$ در M و ایده‌آل اول $\mathfrak{P} \subset \mathcal{O}_M$ شامل $\mathfrak{p}$ در L کاملا شکافته شود. اگر ایده‌آل $\mathcal{P}' \subset \mathcal{O}_L$ بالا سر $\mathfrak{P}$ باشد. در این صورت با توجه به ضربی بودن درجه اینرسی و شاخص انشعاب داریم:

$$e_{\mathfrak{P}'|\mathfrak{P}} = e_{\mathfrak{P}|\mathfrak{p}} = ۱$$
$$\Rightarrow e_{\mathfrak{P}'|\mathfrak{p}} = e_{\mathfrak{P}'|\mathfrak{P}} \cdot e_{\mathfrak{P}|\mathfrak{p}} = ۱$$

و

$$f_{\mathfrak{P}'|\mathfrak{P}} = f_{\mathfrak{P}|\mathfrak{p}} = ۱$$
$$\Rightarrow f_{\mathfrak{P}'|\mathfrak{p}} = f_{\mathfrak{P}'|\mathfrak{P}} \cdot f_{\mathfrak{P}|\mathfrak{p}} = ۱$$

چون L/K گالوا است بنابراین برای هر اول $\mathfrak{P}'$ در L شامل $\mathfrak{p}$ درجه اینرسی و شاخص انشعاب برابر ۱ است. پس $\mathfrak{p}$ در L کاملا شکافته می‌شود. □

۳.۲ تجزیه اعداد اول در میدان‌های مربعی

بخش ۳.۱ را مرور کنید. به دلیل اهمیت توسیع‌های مربعی در این پروژه مساله تجزیه ایده‌آل‌ها را به طور خاص در این توسیع‌ها مورد بررسی قرار می‌دهیم.

گزاره ۱۶.۲. *فرض کنید K میدان مربعی از مبین d_K است. σ را خودریختی نابدیهی K به $\mathbb{C}$ در نظر بگیرید. برای عدد اول p در $\mathbb{Z}$ داریم:*

۱. *اگر $(d_K/p) = 0$ در این صورت $p\mathcal{O}_K = \mathfrak{p}^2$ ، که $\mathfrak{p}$ اولی در $\mathcal{O}_K$ است.*

۲. *اگر $(d_K/p) = 1$ در این صورت $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ ، که $\mathfrak{p} \neq \mathfrak{p}'$ ایده‌آل‌های اولی در $\mathcal{O}_K$ اند.*

۳. *اگر $(d_K/p) = -1$ در این صورت $p\mathcal{O}_K$ ایده‌آل اولی در $\mathcal{O}_K$ است.*

به علاوه (۱) - (۳) تمامی ایده‌آل‌های اول $\mathcal{O}_K$ را مشخص می‌کند.

اثبات. برای اثبات به [۷، گزاره ۱۶.۵.۲] یا [۲۲، بخش ۹.۵] مراجعه کنید. □

نتیجه ۱۷.۲. *فرض کنید K میدان مربعی از مبین d_K است. عدد اول $p \in \mathbb{Z}$ را در نظر بگیرید. آنگاه:*

۱. *p در K منشعب می‌شود اگر و تنها اگر $p \mid d_K$.*

۲. *p در K کاملا شکافته می‌شود اگر و تنها اگر $(d_K/p) = 1$.*

اثبات. با توجه به گزاره بالا بدیهی است. □

فصل ۳

اردرهای جبری

در گزاره ۱۸.۱ مشاهده کردیم که برای میدان عددی $K = \mathbb{Q}(\sqrt{N})$ ، $\mathbb{Z}[\sqrt{N}]$ همواره حلقه اعداد صحیح جبری میدان K نیست. با این وجود حلقه‌هایی مانند $\mathbb{Z}[\sqrt{N}]$ ویژیگی‌های مهمی داشته و اردر جبری [1] نامیده می‌شوند.

در اردرهای جبری تجزیه یکتا ایده‌آل‌ها به ایده‌آل‌های اول برای ایده‌آل‌هایی که نسبت به کنداکتور [2] اول است وجود دارد.

به علاوه اردهای جبری حوزه صحیح، نوتری و دارای بعد کرول ۱ [3] اند.

در ادامه این بخش به مطالعه جزئیات موارد بیان شده می‌پردازیم.

ابتدا اردرهای جبری را برای میدان دلخواه و سپس برای میدان‌های مربعی تعریف می‌کنیم. در انتها گروه رده‌ای را برای اردر جبری دلخواه تعریف کرده و اندازه آن را براساس اندازه گروه رده‌ای حلقه اعداد صحیح جبری پیدا می‌کنیم.

یکی از دلایل بررسی ویژیگی‌های اردرهای جبری، ساده بودن شناسایی آن‌ها نسبت به حلقه اعداد صحیح جبری است. برای توسیع L/K از درجه n ، شناسایی $\mathcal{O}_K$ وابسته به یافتن پایه‌ای صحیح از مرتبه n است که پایه‌ای برای توسیع L/K به عنوان فضای برداری باشد. الگوریتم‌های شناسایی $\mathcal{O}_K$ ممکن است پیچیده و دارای محاسبات طولانی باشند به همین سبب بررسی اردرهای جبری شامل اهمیت خواهد بود.

در فصل ۸ خواهیم دید که برای بیان پاسخ جامع به مساله ۱ نیاز به مفاهیم اردرهای جبری داریم.

---

[1] Algebraic Order

[2] Conductor

[3] Krull Dimension

۱.۳ مفاهیم اولیه

تعریف ۱.۳. *فرض کنید $K/\mathbb{Q}$ میدانی عددی از درجه n است. اردر $\mathcal{O}$ از میدان K را زیر حلقه‌ای از $\mathcal{O}_K$ در نظر می‌گیریم که دارای پایه ای صحیح از اندازه n است. $\mathcal{O}_K$ را اردر ماکسیمال میدان K می‌نامیم. به بیان دیگر:*

$$\mathcal{O} = \mathbb{Z}[\alpha_1, ..., \alpha_n] \quad \alpha_i \in K$$

که $\alpha_1, ..., \alpha_n$ پایه‌ای برای توسیع زیر به عنوان فضای برداری‌اند.

$$K = \frac{\mathbb{Q}(\alpha_1, ..., \alpha_n)}{\mathbb{Q}}$$

بنابراین $\mathcal{O}$ اردر میدان K است اگر $\mathcal{O} \subset K$ و :

۱. $\mathcal{O}$ زیر حلقه‌ای از K ، شامل ۱ باشد.

۲. $\mathcal{O}$ یک $\mathbb{Z}$ - مدول متناهیا تولید شده باشد.

۳. $\mathcal{O}$ دارای پایه‌ای گویا از K باشد.

گزاره ۲.۳. *اردر $\mathcal{O}$ از میدان K حوزه صحیح، نوتری و از بعد کرول ۱ است.*

اثبات. برای اثبات به [۳۰، گزاره ۲.۱۲.۱] رجوع کنید. □

اردرها لزوما صحیح بسته نیستند. اگر اردر جبری صحیح بسته باشد در این صورت ماکسیمال خواهد بود.

در قضیه ۱۴.۱ دیدیم که ایده‌آل‌های کسری در اردرهای ماکسیمال تشکیل گروه‌آبلی می‌دهند. این گزاره در حالت کلی برای اردرهای جبری برقرار نیست.

تعریف ۳.۳. *ایده‌آل کسری $\mathfrak{a}$ از $\mathcal{O}$ را وارون پذیر گوییم؛ اگر ایده‌آل کسری $\mathfrak{b}$ وجود داشته باشد که $\mathfrak{ab} = \mathcal{O}$.*

ایده‌آل‌های کسری وارون پذیر در اردر جبری تشکیل گروه آبلی می دهند. وارون ایده‌آل $\mathfrak{a}$ مانند حالت حلقه اعداد صحیح جبری به شکل زیر تعریف می‌گردد.

$$\mathfrak{a}^{-1} = \{x \mid x\mathfrak{a} \subseteq \mathcal{O}\}$$

$\mathfrak{a}^{-1}$ را به شکل بالا تعریف می‌کنیم به دلیل اینکه بزرگترین ایده‌آل کسری از $\mathcal{O}$ است که $\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathcal{O}$.

برای مطالعه بیشتر درباره شناسایی ایده‌آل‌های وارون پذیر اردر $\mathcal{O}$ می توانید به [۳۰، گزاره ۴.۱۲.۱] رجوع کنید.

نمادگذاری ۴.۳. *اردر $\mathcal{O}$ در نظر بگیرید. در این صورت:*

- *$I(\mathcal{O})$ را گروه ایده‌آل‌های کسری وارون پذیر $\mathcal{O}$ می‌نامیم.*
- *$P(\mathcal{O})$ را زیرگروهی از $I(\mathcal{O})$ که شامل ایده‌آل‌های کسری اصلی در نظر بگیرید.*

$$P(\mathcal{O}) = \{a\mathcal{O} \mid a \in K^*\}.$$

- *گروه خارج قسمتی $I(\mathcal{O})/P(\mathcal{O})$ را با $C(\mathcal{O})$ یا $Pic(\mathcal{O})$ نمایش داده و گروه پیکارد [۴] می نامیم.*

یادداشت ۵.۳. *تاکنون برای درباره ایده‌آل کسری $\mathfrak{a}$ از اردر $\mathcal{O}$ مشاهده کردیم که:*

- $\mathfrak{a}^{-1} = \{x \mid x\mathfrak{a} \subseteq \mathcal{O}\}$
- *شمول زیر همواره برای ایده‌آل کسری $\mathfrak{a}$ برقرار است:*

$$\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathcal{O}$$

حال اگر $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$ باشد؛ در این صورت $\mathfrak{a}$ در $\mathcal{O}$ وارون پذیر است.

با توجه به وارون پذیر نبودن بعضی از ایده‌آل‌های کسری در اردر $\mathcal{O}$ تجزیه یکتا به ایده‌آل های اول برای همه ایده‌آل‌ها لزوما صورت برقرار نیست.
در ادامه با بیان مفهوم کنداکتور برای اردرهای جبری خواهیم دید که ایده‌آل‌هایی از $\mathcal{O}$ که نسبت به کنداکتور اول‌اند؛ وارون پذیر و دارای تجزیه یکتا به ایده‌آل‌های اول وارون پذیر در $\mathcal{O}$ اند.

تعریف ۶.۳. *کنداکتور اردر جبری $\mathcal{O}$ از میدان عددی K را به شکل زیر تعریف می‌کنیم.*

$$\mathfrak{c} = \mathfrak{c}_{\mathcal{O}} = \{x \in \mathcal{O}_K \mid x\mathcal{O}_K \subset \mathcal{O}\}$$

با توجه به این که $1 \in \mathcal{O}_K$ داریم:

$$\mathfrak{c} = \{x \in \mathcal{O}_K \mid x\mathcal{O}_K \subset \mathcal{O}\} = \{x \in \mathcal{O} \mid x\mathcal{O}_K \subset \mathcal{O}\}$$

در اردر جبری $\mathcal{O}$ دو ایده‌آل $\mathfrak{b}$ و $\mathfrak{b}'$ را نسبت به هم اول گوییم اگر

$$\mathfrak{b} + \mathfrak{b}' =< 1 >= \mathcal{O}$$

باشد. فرض کنید $\beta \in \mathcal{O}$ است. β و ایده‌آل $\mathfrak{b}$ را نسبت به یک‌دیگر اول گوییم اگر ایده‌آل‌های $\beta\mathcal{O}$ و $\mathfrak{b}$ نسبت به هم اول باشند.

[4] Picard Group

قضیه ۷.۳. *فرض کنید $\mathcal{O}$ اردر میدان عددی K و $\mathfrak{c}$ کنداکتور آن است. اگر ایده‌آل ناصفر $\mathfrak{b}$ از $\mathcal{O}$ نسبت به $\mathfrak{c}$ اول باشد در این صورت داریم:*

$$\{x \in K \mid x\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O}.$$

اثبات. برای اثبات به [۵، قضیه ۱.۳] رجوع کنید. □

قضیه بالا وجود وارون را برای ایده‌آل‌های $\mathcal{O}$ که نسبت به کنداکتور اردر($\mathfrak{c}$) اول‌اند را تضمین می‌کند .در ادامه با بیان دو قضیه زیر وجود تجزیه یکتا برای ایده‌آل های $\mathcal{O}$ که نسبت به $\mathfrak{c}$ اول‌اند را اثبات می‌کنیم.

قضیه ۸.۳. *برای ایده‌آل اول ناصفر $\mathfrak{p}$ از $\mathcal{O}$ عبارت‌های زیر معادلند:*

۱. $\mathfrak{p}$ *به عنوان یک $\mathcal{O}$ - ایده‌آل وارون پذیر است.*

۲. $\{x \in K \mid x\mathfrak{p} \subset \mathfrak{p}\} = \mathcal{O}$

اثبات. برای اثبات به [۵، قضیه ۴.۳] رجوع کنید. □

قضیه ۹.۳. *فرض کنید ایده‌آل ناصفر $\mathfrak{b}$ در $\mathcal{O}$ نسبت به $\mathfrak{c}$ کنداکتور $\mathcal{O}$ اول باشد. در این صورت $\mathfrak{b}$ را می توان به صورت حاصل ضرب ایده‌آل های وارون پذیر $\mathcal{O}$ نوشت. به طور خاص، هر ایده‌آل $\mathcal{O}$ که نسبت به کنداکتور اول است وارون پذیر است.*

اثبات. برای اثبات به [۵، قضیه ۶.۳] رجوع کنید. □

بنابر قضایا بالا مشاهده می‌شود که ایده‌آل‌هایی از $\mathcal{O}$ که نسبت به کنداکتور اردر اول‌اند؛ در $\mathcal{O}$ به صورت حاصل ضرب ایده‌آل‌های وارون پذیر نوشته شده و پس دارای وارون اند.
در ادامه با بیان قضیه زیر تناظری یک به یک میان این ایده‌آل‌ها و ایده‌آل‌های $\mathcal{O}_K$ بیان می کنیم.

قضیه ۱۰.۳. *فرض کنید $\mathcal{O}$ اردری از میدان K با کنداکتور $\mathfrak{c}$ است.*

۱. *برای $\mathcal{O}_K$ - ایده‌آل $\mathfrak{a}$ که نسبت به $\mathfrak{c}$ اول است می توان گفت؛ $\mathfrak{a} \cap \mathcal{O}$ یک $\mathcal{O}$ - ایده‌آل نسبت به کنداکتور اول است و همریختی طبیعی*

$$\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \longrightarrow \mathcal{O}_K/\mathfrak{a}$$

یکریختی است.

۲. *برای $\mathcal{O}$ - ایده‌آل $\mathfrak{b}$ که نسبت به $\mathfrak{c}$ اول است می توان گفت؛ $\mathfrak{b}\mathcal{O}_K$ یک $\mathcal{O}_K$ - ایده‌آل نسبت به کنداکتور اول است و همریختی طبیعی*

$$\mathcal{O}/\mathfrak{b} \longrightarrow \mathcal{O}_K/\mathfrak{b}\mathcal{O}_K$$

یکریختی است.

۳. *ایده‌آل‌های ناصفر $\mathcal{O}_K$ و $\mathcal{O}$ که نسبت به $\mathfrak{c}$ اول‌اند در از طریق همریختی‌های $\mathfrak{b} \mapsto \mathfrak{b}\mathcal{O}_K$ و $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ در تناظر با یک به یک یا یک‌دیگرند. به علاوه این تناظر ضربی است:*

$$(\mathfrak{a} \cap \mathcal{O})(\mathfrak{a}' \cap \mathcal{O}) = (\mathfrak{a}\mathfrak{a}' \cap \mathcal{O}), \quad (\mathfrak{b}\mathcal{O}_K)(\mathfrak{b}'\mathcal{O}_K) = (\mathfrak{b}\mathfrak{b}'\mathcal{O}_K)$$

اثبات. برای اثبات این قضیه به [۵، قضیه ۸.۳] رجوع کنید. □

۲.۳ اردر در میدان‌های مربعی

با توجه به اهمیت میدان‌های مربعی در این نوشتار در این بخش به طور خاص به بررسی قضایا و خواص اردرهای جبری در میدان‌های مربعی می‌پردازیم.

۱.۲.۳ تعاریف و مفاهیم اولیه

با توجه به تعریف اردر جبری در بخش قبلی در صورتی که $K = \mathbb{Q}(\sqrt{N})$ باشد. اردر $\mathcal{O} \subset K$ در واقع یک $\mathbb{Z}$ - مدول از رتبه ۲ با میدان کسرهای K است.

مفهوم مبین در میدان‌های مربعی را بیاد آوردید. در بخش ۳.۱ مشاهده کردیم که برای میدان مربعی K اگر مبین میدان برابر d_K باشد؛ می‌توان حلقه اعداد صحیح جبری $\mathcal{O}_K$ را کاملا شناسایی کرد:

$$\mathcal{O}_K = [1, \omega_K], \quad \omega_K = \frac{d_K + \sqrt{d_K}}{2} \tag{۱.۳}$$

در این میدان‌ها می‌توان اردرهای جبری را از طریق لم زیر شناسایی کرد.

لم ۱۱.۳. *فرض کنید $\mathcal{O}$ اردری در میدان مربعی K از مبین d_K است. در این صورت :*

$$[\mathcal{O}_K : \mathcal{O}] < \infty$$

اگر $f = [\mathcal{O}_K : \mathcal{O}]$ باشد؛ خواهیم داشت:

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, f\omega_K]$$

که ω_K همانند (۱.۳) تعریف می‌شود.

اثبات. برای اثبات به [۷، لم ۲.۷.۲] رجوع کنید. □

تعریف ۱۲.۳. *در لم بالا $f = [\mathcal{O}_K : \mathcal{O}]$ را کنداکتور اردر می‌نامیم. مبین اردر $\mathcal{O}$ را باتوجه به کنداکتور می‌توان به شکل $D = f^2 d_K$ تعریف کرد.*

برای مشاهده جزیئات چگونگی محاسبه مبین اردر $\mathcal{O}$ به [۷، ص ۱۲۱] رجوع کنید.

برای اردر $\mathcal{O}$ در میدان K مبین $D = f^2 d_K$ ناورداست (با داشتن مبین یک اردر جبری می‌توان آن اردر را به صورت یکتا تعیین کرد). هم چنین $D \overset{4}{\equiv} 0, 1$ است.

در ادامه هدف مطالعه ایده‌آل‌های اردر $\mathcal{O}$ در میدان مربعی K است.

اگر $\mathfrak{a}$ ایده‌آل ناصفر از $\mathcal{O}$ باشد؛ حلقه خارج قسمتی $\mathcal{O}/\mathfrak{a}$ متناهی است (اثبات متناهی بود اندیس ایده‌آل $\mathfrak{a}$ در $\mathcal{O}$ مشابه ۱۲.۱ است).

$$N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$$

را نرم ایده‌آل $\mathfrak{a}$ می‌نامیم.
مفاهیمی از قبیل ایده‌آل کسری، ایده‌آل وارون پذیر، $I(\mathcal{O}), P(\mathcal{O}), C(\mathcal{O})$ و... برای اردر $\mathcal{O}$ در میدان مربعی K به طور مشابه تعریف می‌گردد.

۲.۲.۳ ایده‌آل‌های نسبت به کنداکتور اول

در ادامه این بخش فرض کنید $\mathcal{O}$ اردری از کنداکتور f در میدان مربعی K است.

مشاهده کردیم ایده‌آل‌های ناصفری که نسبت به کنداکتور اول بودند تجزیه‌ای یکتا به ایده‌آل‌های اول وارون پذیر در $\mathcal{O}$ را دارند و به طور خاص وارون پذیر اند.
با بررسی لم زیر می‌توان درباره خاصیت $\mathcal{O}$ - ایده‌آل‌های نسبت به کنداکتور اول، صحبت کرد.

لم ۱۳.۳. *فرض کنید $\mathcal{O}$ اردری با کنداکتور f در میدان K است.*

۱. *$\mathcal{O}$ - ایده‌آل $\mathfrak{a}$ نسبت به f اول است اگر و تنها اگر $\gcd(N(\alpha), f) = ۱$ باشد.*

۲. *هر $\mathcal{O}$ - ایده‌آل $\mathfrak{a}$ نسبت به f اول، وارون پذیر است.*

اثبات. برای مشاهده اثبات به [۷، لم ۱۸.۷.۲] رجوع کنید. □

در ادامه گروه پیکارد اردر $\mathcal{O}$ را به شکل دیگری تعریف می‌کنیم. در ابتدا نیاز به معرفی دو نماد زیر داریم:

نمادگذاری ۱۴.۳. *مفاهیم $I(\mathcal{O})$ و $P(\mathcal{O})$ را از نمادگذاری ۴.۳ به یاد آورید.*

- *$I(\mathcal{O}, f) \subset I(\mathcal{O})$ را $\mathcal{O}$ - ایده‌آل‌هایی در نظر بگیرید که نسبت به کنداکتور f اول اند.*
- *$P(\mathcal{O}, f)$ را زیرگروهی از $I(\mathcal{O}, f)$ تولید شده توسط ایده‌آل های اصلی $\alpha\mathcal{O}$ در نظر بگیرید که $\alpha \in \mathcal{O}$ و $\gcd(N(\alpha), f) = ۱$ باشد.*

گزاره ۱۵.۳. *شمول $I(\mathcal{O}, f) \subset I(\mathcal{O})$ یکریختی زیر را القا می‌کند.*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I(\mathcal{O})/P(\mathcal{O}) = C(\mathcal{O})$$

اثبات. برای مشاهده اثبات به گزاره [۷، ۱۹.۷.۲] رجوع کنید. □

پیش از مرور ارتباط بین $\mathcal{O}$- ایده‌آل‌ها و $\mathcal{O}_K$- ایده‌آل‌های نسبت به کنداکتور اول نماد گذاری زیر را در نظر بگیرید.

نمادگذاری ۱۶.۳. *فرض کنید $m \in \mathbb{Z}^+$ است. در این صورت:*

- *$I_K(m)$ را تمام $\mathcal{O}_K$ ایده‌آل‌های نسبت به m اول در نظر بگیرید $P_K(m)$ نیز مشابها تعریف می‌گردد.*
- *$P_{K,\mathbb{Z}}(m)$ را زیر گروهی از $I_K(m)$ در نظر بگیرید که توسط ایده‌آل‌های اصلی به فرم $\alpha\mathcal{O}_K$ که $\alpha \in \mathcal{O}_K$ و*

$$\alpha \equiv a \bmod m\mathcal{O}_K, \quad a \in \mathbb{Z}, \quad \gcd(a, m) = 1$$

تولید شده است.

گزاره زیر را برای مرور تناظر بین $\mathcal{O}$ - ایده‌آل‌ها و $\mathcal{O}_K$ - ایده‌آل‌های نسبت به کنداکتور اول مجددا بازگو می‌کنیم.

گزاره ۱۷.۳. *فرض کنید $\mathcal{O}$ از کنداکتور f در میدان مربعی موهومی K است. در این صورت:*

۱. *اگر $\mathfrak{a}$ یک $\mathcal{O}_K$ - ایده‌آل نسبت به f اول باشد در این صورت:*

$$\mathfrak{a} \cap \mathcal{O}$$

یک $\mathcal{O}$ - ایده‌آل نسبت به f اول و از نرم $N(\mathfrak{a})$ است.

۲. *اگر $\mathfrak{b}$ یک $\mathcal{O}$ - ایده‌آل نسبت به f اول باشد در این صورت:*

$$\mathfrak{b}\mathcal{O}_K$$

یک $\mathcal{O}_K$ - ایده‌آل نسبت به f اول و از نرم $N(\mathfrak{b})$ است.

۳. *نگاشت $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ یکریختی $I_K(f) \xrightarrow{\sim} I(\mathcal{O}, f)$ را القا می‌کند. وارون این نگاشت $\mathfrak{b} \mapsto \mathfrak{b}\mathcal{O}_K$ است.*

اثبات. برای اثبات به [۷، گزاره ۲۰.۷.۲] یا قضیه ۱۰.۳ رجوع کنید. □

با توجه به ارتباط بیان شده بین ایده‌آل های $\mathcal{O}$ و $\mathcal{O}_K$ که نسبت به f اول‌اند؛ می‌توان گروه پیکارد $\mathcal{O}$ را بر اساس $\mathcal{O}_K$ - ایده‌آل‌های نسبت به f اول توصیف کرد.

گزاره ۱۸.۳. *فرض کنید $\mathcal{O}$ اردری از کنداکتور f در میدان مربعی موهومی K است. در این صورت یکریختی‌های طبیعی زیر وجود دارند:*

$$C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$$

قبل از اثبات گزاره لم زیر را بررسی می‌کنیم:

لم ۱۹.۳. *فرض کنید $\alpha, \beta \in \mathcal{O}_K$ و $m \in \mathbb{Z}$ است. اگر $\beta \overset{m\mathcal{O}_K}{\equiv} \alpha$ باشد. آنگاه:*

$$N(\alpha) \overset{m}{\equiv} N(\beta)$$

اثبات. در ادامه منظور از $\bar{\alpha}, \bar{\beta}, \bar{x}$ مزدوج مختلط این عناصر است.

$$\alpha \equiv \beta \bmod f\mathcal{O}_K \Rightarrow \begin{cases} \alpha = \beta + mx, x \in \mathcal{O}_K \\ \bar{\alpha} = \bar{\beta} + m\bar{x}, \bar{x} \in \mathcal{O}_K \end{cases} \qquad (۲.۳)$$
$$\Rightarrow N(\alpha) = \alpha\bar{\alpha} = m(\beta\bar{x} + \bar{\beta}x + m\bar{x}x) + N(\beta)$$

□

در ادامه اثبات گزاره ۱۸.۳ را بیان می‌کنیم:

اثبات. یکریختی زیر با توجه به گزاره ۱۵.۳ برقرار است.

$$C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f)$$

با توجه به قسمت (۳) گزاره ۱۷.۳ داریم:

$$I(\mathcal{O}, f) \simeq I_K(f)$$

. حال با توجه به این یکریختی زیر گروه می‌توان گفت

$$P(\mathcal{O}, f) \subset I(\mathcal{O}, f)$$

به زیرگروه $\tilde{P} \subset I_K(f)$ تصویر می‌شود.
بنابراین برای تکمیل اثبات کافی است نشان دهیم $\tilde{P} = P_{K,\mathbb{Z}}(f)$ است.
$P(\mathcal{O}, f)$ توسط ایده‌آل‌های به فرم $\alpha\mathcal{O}$ که $\alpha \in \mathcal{O}$ و $\gcd(N(\alpha), f) = ۱$ باشد؛ تولید شده است.
توسط یکریختی القا شده از قسمت (۳) گزاره ۱۷.۳ داریم:

$$\alpha\mathcal{O} \longmapsto \alpha\mathcal{O}_K \in P_K(f), \quad \gcd(N(\alpha), f) = ۱$$

در ادامه با اثبات ادعای زیر اثبات تکمیل می‌گردد.

$$\alpha \in \mathcal{O}, \gcd(N(\alpha), f) = ۱ \iff \alpha \equiv a \bmod f\mathcal{O}_K, a \in \mathbb{Z}, \gcd(a, f) = ۱$$

برای اثبات مسیر راست به چپ:

$$\alpha \equiv a \bmod f\mathcal{O}_K \overset{\text{نرم را اثر دهید}}{\Longrightarrow} N(\alpha) \equiv N(a) = a^2 \bmod f$$
$$\Rightarrow (N(\alpha), f) = (a^2, f) = 1 \overset{f\mathcal{O}\subset\mathcal{O}}{\Longrightarrow} \alpha \in \mathcal{O}$$

برای اثبات مسیر عکس:

$$\alpha \in \mathcal{O} = [1, f\omega_K], \Rightarrow \exists a, b \in \mathbb{Z} : \alpha = a + bf\omega_K$$
$$\Rightarrow \alpha \equiv a \bmod f\mathbb{O}_K \Rightarrow N(\alpha) \equiv a^2 \bmod f$$

$$\gcd(N(\alpha), f) = 1, N(\alpha) \equiv a^2 \bmod f \Rightarrow \gcd(a, f) = 1$$

□

برای مطالعه بیشتر در رابطه با ارتباط بین ایده‌آل‌های $\mathcal{O}$ و $\mathcal{O}_K$ به [۸، بخش ۸] و [۲۶، بخش ۱.۸] رجوع کنید.

$|\, C(\mathcal{O}) \,| = h(\mathcal{O})$ ۳.۲.۳

یکی از نتایج گزاره ۱۸.۳ محاسبه $h(\mathcal{O})$ بر اساس کنداکتور f و عدد رده‌ای $h(\mathcal{O}_K)$ است.

قضیه ۲۰.۳. *فرض کنید اردر $\mathcal{O}$ از کنداکتور f در میدان مربعی موهومی K است. در این صورت:*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K) f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right)$$

به علاوه، $h(\mathcal{O})$ ضریبی صحیح از $h(\mathcal{O}_K)$ است.

اثبات. برای مشاهده اثبات به [۷، قضیه ۲۴.۷.۲] رجوع شود. □

نتیجه ۲۱.۳. *فرض کنید $D \overset{4}{\equiv} 0, 1$ عددی منفی و $m \in \mathbb{Z}$ در این صورت برای دو عدد رده‌ای $h(D)$ ، $h(m^2 D)$ داریم:*

$$h(m^2 D) = \frac{h(D) m}{[\mathcal{O}^* : \mathcal{O}'^*]} \prod_{p|m} \left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right)$$

که $\mathcal{O}$ و $\mathcal{O}$ اردرهای جبری به ترتیب از مبین‌های D و $m^2 D$ اند.

اثبات. اثبات با استفاده از قضیه بالا و محاسبات ساده صورت می‌گیرد. □

فصل ۴

ارزه

۱.۴ مفاهیم اولیه

تعریف ۱.۴. *برای میدان K تابع $|\cdot| : K \to \mathbb{R}$ که $x \mapsto |x|$ را ارزه ضربی [1] یا ارزه مطلق [2] می‌نامیم؛ اگر برای $x, y \in K$*

۱. $|x| \geq 0$ و تساوی زمانی رخ دهد که $x = 0$.

۲. $|xy| = |x||y|$ ،

۳. $|x + y| \leq |x| + |y|$: *(نامساوی مثلث)*

تابع ارزه ضربی را ناارشمیدسی [3] می‌نامیم اگر به جای شرط (۳) در شرط زیر صدق کند.

$$|x + y| \leq max\{|x|, |y|\}$$

اگر ارزه ناارشمیدسی نباشد، ارشمیدسی است.

تعریف ۲.۴. *برای میدان K تابع $v : K \to \mathbb{Z} \cup \{\infty\}$ را ارزه گسسته (جمعی) می‌نامیم؛ اگر برای هر $x, y \in K$ داشته باشیم:*

۱. $v(x) = 0 \iff x = 0$

۲. $v(xy) = v(x) + v(y)$

[1] Multiplicative Valuation
[2] Absolute Value
[3] Nonarchimedean Absolute Value

۳. $v(x+y) = min(v(x), v(y))$

یادداشت ۳.۴. *فرض کنید v یک ارزه گسسته روی میدان K است. برای $0 < c < 1$ ، $|\cdot|$ یک ارزه ناارشمیدسی است.*

$$|\cdot| : K \longrightarrow \mathbb{R}, \quad x \longmapsto (\frac{1}{c})^{v(x)}$$

مثال ۴.۴. *برای هر میدان عددی K ، نشاندن $\sigma : K \hookrightarrow \mathbb{C}$ یک ارزه مطلق روی K با قرار دادن $|a| = |\sigma a|$ می‌دهد.*

با توجه به تعریف می‌دانیم ارزه‌ای ناارشمیدسی است که برای هر $x, y \in K$ داشته باشیم:

$$|x+y| \leq max\{|x|, |y|\}$$

در این صورت با استفاده از استقرا به راحتی می‌توان نشان داد:

$$|\sum x_i| \leq max\{|x_i|\}$$

بنابر توضیحات بالا می‌توان قضیه زیر را در رابطه با ارزه‌های ناارشمیدسی بیان کرد.

گزاره ۵.۴. *ارزه مطلق $|\cdot|$ ناارشمیدسی است اگر و تنها اگر $|\cdot|$ روی مجموعه*

$$\{m \cdot 1 \mid m \in \mathbb{Z}\}$$

کراندار باشد.

اثبات. برای اثبات به [۲۹، گزاره ۲.۷] رجوع کنید. □

با توجه به قضیه بالا به سادگی مشاهده می‌شود که میدان‌هایی با مشخصه ناصفر $(charK \neq 0)$ فقط دارای ارزه‌های ناارشمیدسی اند. چرا که مجموعه

$$\{m \cdot 1 \mid m \in \mathbb{Z}\}$$

متناهی است.

توجه داشته باشید که هر ارزه مطلق متری روی میدان K معرفی می‌کند که موجب تبدیل K به یک فضای متریک می‌شود. متر القا شده برای $a, b \in K$ به فرم زیر است:

$$d(a,b) = |a-b|$$

با استفاده از این متر می‌توان توپولوژی‌ای به میدان K القا کرد. برای هر $a \in K$ مجموعه‌های

$$U(a,\epsilon) = \{x \in K \mid |x-a| < \epsilon\}, \quad \epsilon > 0$$

پوششی باز برای همسایگی اطراف a تشکیل می‌دهند.

بنابر توضیحات داده شده مجموعه A را باز می‌نامیم اگر و تنها اگر اجتماع مجموعه‌هایی به فرم $U(a,\epsilon)$ باشد.

هدف از بررسی توپولوژی القا شده توسط ارزه $|\cdot|$ ارائه گزاره زیر است که شرایط لازم و کافی را برای معادل بودن دو ارزه

$$|\cdot|_1, \quad |\cdot|_2$$

را بیان می‌کند.

گزاره ۶.۴. *فرض کنید $|\cdot|_1$ و $|\cdot|_2$ دو ارزه مطلق روی میدان K است که $|\cdot|_1$ نابدیهی است. در این صورت گزاره‌های زیر معادل‌اند.*

۱. *$|\cdot|_1$ و $|\cdot|_2$ توپولوژی یکسانی روی K تعریف می‌کنند.*

۲. $|\alpha|_1 < 1 \Rightarrow |\alpha|_2 < 1$.

۳. $\exists a > 0 : |\cdot|_1 = |\cdot|_1^a$

اثبات. برای اثبات به [۲۹، گزاره ۸.۷] رجوع کنید. □

تعریف ۷.۴. *دو ارزه $|\cdot|_1$ و $|\cdot|_2$ را معادل یک‌دیگر گوییم اگر در شرایط گزاره بالا صدق کنند.*

۱.۱.۴ لیست کامل ارزه‌های مطلق روی میدان اعداد گویا

در این بخش با استفاده از با استفاده از قضیه اوستروفسکی [۴] لیست کاملی از ارزه‌های روی میدان $\mathbb{Q}$ ارائه می‌دهیم.

قبل از بیان قضیه نمادگذاری زیر را در نظر بگیرید:

نمادگذاری ۸.۴. *ارزه مطلق $|\cdot|_\infty$ روی $\mathbb{Q}$ را قدر مطلق معمول روی میدان اعداد حقیقی $\mathbb{R}$ در نظر بگیرید.*

قضیه ۹.۴ (قضیه استروفسکی). *فرض کنید $|\cdot|$ ارزه مطلق نابدیهی روی میدان $\mathbb{Q}$ است. در این صورت:*

۱. *اگر $|\cdot|$ ارشمیدسی باشد معادل $|\cdot|_\infty$ است.*

۲. *اگر $|\cdot|$ نارشمیدسی باشد دقیقا یک عدد اول p وجود دارد که $|\cdot|$ معادل $|\cdot|_p$ است.*

اثبات. برای مشاهده اثبات به [۲۹، قضیه ۱۲.۷] رجوع کنید. □

[4] Ostrowski

۲.۴ مکان (اول) های یک میدان عددی

فرض کنید K میدان عددی است. در این صورت مکان [۵] یا اول [۶] از میدان K را به شکل زیر تعریف می‌کنیم:

تعریف ۱۰.۴. *اگر K میدان عددی باشد؛ مجموعه کلاس‌های هم‌ارزی تحت معادل بودن ارزه‌ها را اول یا مکان میدان K می‌نامیم.*

در ادامه با استفاده از قضیه زیر درک درستی از اول‌های میدان عددی K بدست می‌آوریم:

قضیه ۱۱.۴. *میدان عددی K را در نظر بگیرید. در این صورت دقیقا یک اول میدان K برای موارد زیر وجود دارد:*

۱. *برای هر ایده‌آل اول $\mathfrak{p}$ از میدان K.*

۲. *برای هر نشاندن حقیقی میدان K.*

۳. *برای هر جفت نشاندن مزدوج مختلط میدان K.*

اثبات. □

در هر یک از کلاس‌های هم‌ارزی از ارزه‌های مطلق روی میدان K ما ارزه مطلق نرمال شده را به نحوه زیر انتخاب می‌کنیم:

- برای هر ایده‌آل اول $\mathfrak{p}$ از $\mathcal{O}_K$:

$$|a|_{\mathfrak{p}} = \left(\frac{1}{N(\mathfrak{p})}\right)^{ord_{\mathfrak{p}(a)}}$$

- برای هر نشاندن حقیقی $\sigma (\sigma : K \hookrightarrow \mathbb{R})$:

$$|a| = |\sigma a|.$$

- برای هر نشاندن ناحقیقی و مختلط $\sigma (\sigma : K \hookrightarrow \mathbb{C})$:

$$|a| = |\sigma a|^2.$$

حال با استفاده از توضیحات بالا نماد گذاری زیر را در نظر بگیرید:

[5] Place
[6] Prime

نمادگذاری ۱۲.۴. *به صورت معمول ما از نماد v برای اول‌های میدان K استفاده می‌کنیم.*

۱. *اگر v معادل ایده‌آل اول $\mathfrak{p}$ از K باشد. در این صورت v را اول (مکان) متناهی [۷] از K می‌نامیم.*

۲. *اگر v معادل نشاندنی حقیقی یا مختلط از K باشد. در این صورت v را اول (مکان) نامتناهی حقیقی یا مختلط [۸] از K می‌نامیم.*

[7] Finite Primes (Places)
[8] Infinite Real or Complex Primes (Places)

بخش دوم

روش‌های مقدماتی

همان طور که در پیشگفتار بیان شد. هدف ارائه پاسخی در راستای حل مساله ۱ است.

مساله ۱. *فرض کنید $n \in \mathbb{Z}^{\geq 1}$ داده شده است. در این صورت چه اعداد اولی را می‌توان به صورت*

$$p = x^2 + ny^2$$

نمایش داد به طوری که $x, y \in \mathbb{Z}$ باشند؟

هدف ما در این بخش بررسی ایده‌های مقدماتی (ایده‌های نظریه مقدماتی اعداد، نظریه فرم‌های مربعی و نظریه گونا) در راستای حل این مساله است.

ابتدای این بخش را به گزاره‌های ارائه شده توسط فرما برای حالت $n = 1, 2, 3$ می‌پردازیم. در ادامه استراتژی دو مرحله ای اویلر را در حل مساله ۱ برای حالت $n = 1, 2, 3$ را بررسی می‌کنیم.

سپس تمرکز خود را روی کلی کردن استراتژی اویلر برای حل مساله در حالت کلی قرار می‌دهیم.

متاسفانه خواهیم دید که کلی کردن این استراتژی برای هر مقدار n مقدور نیست با بررسی محدودیت‌ها، سعی در رفع آن‌ها داشته و بنابراین با در نظر گرفتن سیر تاریخی حل مساله ۱ نظریه فرم‌های مربعی را تعریف می‌کنیم.

با بیان پیشنیازها و مفاهیم فرم‌های مربعی اهمیت آن‌ها را در حل مساله مذکور بیان می‌کنیم.

با بیان ایده‌های ریاضی‌دانانی چون گاوس، اویلر و لژاندر در توسیع نظریه‌های فرم‌های مربعی این مساله را مورد بررسی قرار داده و در انتهای بخش با استفاده از روش‌های مقدماتی مساله ۱ را برای متناهی حالت n حل می‌کنیم.

سرانجام با درک محدودیت‌ها و بررسی دلایل کار نکردن این روش‌ها این بخش را به پایان می‌رسانیم.

فصل ۵

فرما و اویلر

همانطور که گفته شد، این فصل را با بررسی گزاره‌های زیر شروع می‌کنیم.

$$\begin{aligned} &p = x^۲ + y^۲,\ x, y \in \mathbb{Z} \iff p \equiv ۱ \bmod ۴ \\ &p = x^۲ + ۲y^۲,\ x, y \in \mathbb{Z} \iff p \equiv ۱, ۳ \bmod ۸ \\ &p = x^۲ + ۳y^۲,\ x, y \in \mathbb{Z} \iff p = ۳,\ p \equiv ۱ \bmod ۳ \end{aligned} \qquad (۱.۵)$$

این گزاره‌ها اولین بار توسط فرما [۱] در طی نامه‌هایی به مرسن [۲] و پاسکال [۳] بدون اثبات بیان شد [۱۱] ، شروع می‌کنیم.

سپس تلاش ۴۰ـساله اویلر [۴] در اثبات و تعمیم گزاره‌های فوق را بررسی و نشان خواهیم داد که چگونه استراتژی او در حل گزاره‌های فوق منجر به یافتن قانون تقابل مربعی [۵] شد.

در ادامه چالش‌های موجود در یافتن اعداد p به فرم $x^۲ + ny^۲$ را برای مقادیر دلخواه $n > ۰$ بررسی می‌کنیم.

۱.۵ $n = ۱, ۲, ۳$

در ابتدا، با استفاده از روش‌های مقدماتی نظریه اعدادی اثبات‌هایی برای گزاره (۱.۵) که در واقع صورت سوال برای حالت‌های $n = ۱, ۲, ۳$ اند را بررسی می‌کنیم.

برای حل مساله اصلی در حالت $n = ۱, ۲, ۳$ از استراتژی اویلر کمک می‌گیریم. گزاره زیر با بیان اثبات ارائه شده توسط اویلر جواب مساله ۱ را برای حالت $n = ۳$ می‌دهد.

---

[1] Fermat
[2] Mersenne
[3] Pascal
[4] Euler
[5] Quadratic Reciprocity

توجه داشته باشید که اثبات حالات $n = ۱, ۲$ کاملا مشابه صورت می‌گیرد.

قضیه ۱.۵. *عدد اول فرد p به شکل $x^۲ + ۳y^۲$ است اگر و تنها اگر $p \overset{۳}{\equiv} ۱$ باشد.*

برای اثبات به دو لم زیر نیاز داریم.

لم ۲.۵. *فرض کنید $x, y, z, w, n \in \mathbb{Z}$ اند. آنگاه حاصل ضرب دو عدد به فرم $x^۲ + ny^۲$ و $z^۲ + nw^۲$ نیز به این فرم خواهد بود. یعنی:*

$$(x^۲ + ny^۲)(z^۲ + nw^۲) = (xz \pm nyw)^۲ + n(xw \mp yz)^۲. \qquad (۲.۵)$$

اثبات.

$$\begin{aligned}(x^۲ + ny^۲)(z^۲ + nw^۲) &= x^۲z^۲ \pm ۲nxyzw + n^۲y^۲w^۲ + nx^۲w^۲ \mp ۲nxwyz + ny^۲z^۲ \\ &= x^۲z^۲ + n^۲y^۲w^۲ + nx^۲w^۲ + ny^۲z^۲ \\ &= (xz \pm nyw)^۲ + n(xw \mp yz)^۲.\end{aligned}$$

□

لم ۳.۵. *فرض کنید $N = a^۲ + nb^۲$ که در آن a, b اعداد صحیح نسبت به هم اول اند. اگر q مقسوم علیه اول N به فرم $x^۲ + ny^۲$ باشد. آنگاه N/q نیز به شکل $x_۱^۲ + ny_۱^۲$ است به طوری که $x_۱, y_۱$ اعداد صحیح نسبت به هم اول اند.*

اثبات. می توان به سادگی مشاهده کرد که:

$$q \mid x^۲N - a^۲q = n(xb - ay)(xb + ay).$$

بدون کاستن از کلیت، فرض کنید

$$q \mid xb - ay \quad (*).$$

به وضوح $q \mid xb - ay$ یا $q \mid xb + ay$ آنگاه با تغییر $a \leftrightarrow -a$ می‌توان $(*)$ را برقرار کرد.
بنابراین $\exists d \in \mathbb{Z}$ که $xb - ay = dq$.

$$\begin{aligned}(a + ndy)y &= ay + ndy^۲ = xb - dq + ndy^۲ \\ &= xb - d(q - ny^۲) = xb - dx^۲ = x(b - dx).\end{aligned}$$

از آنجایی که $\gcd(x, y) = ۱$، پس $x \mid a + ndy$ و $\exists c \in \mathbb{Z}$ به طوری که:

$$a + ndy = cx.$$

پس:

$$\Rightarrow a = cx - ndy, \quad b = dx + cy,$$

و داریم:

$$N = a^2 + nb^2 = (cx - ndy)^2 + n(dx + cy)^2$$
$$\overset{(2.5)}{=} \underbrace{(x^2 + ny^2)}_{q}\underbrace{(c^2 + nd^2)}_{N/q}.$$

□

اکنون با استفاده از دو لم بالا ابزار لازم برای اثبات قضیه ۱.۵ را داریم.

اثبات. فرض کنید p عددی اول به فرم $x^2 + 3y^2$ است.
مربع اعداد صحیح در پیمانه ۳، ۰ یا $(\pm 1)^2$ است . پس، $p \overset{3}{\equiv} x^2 \overset{3}{\equiv} 0, 1$ است. بنابراین:

$$p = 3 \text{ یا } p \overset{3}{\equiv} 1.$$

اثبات عکس در دو مرحله صورت می‌گیرد:

۱. **مرحله نزول**[6] **:** اگر $p \mid x^2 + 3y^2$ که $\gcd(x, y) = 1$ باشد، آنگاه p را می‌توان به صورت $x_1^2 + 3y_1^2$ که $x_1, y_1 \in \mathbb{Z}$ نوشت.

۲. **مرحله تقابل**[7] **:** اگر $p \overset{3}{\equiv} 1$ ، آنگاه $x, y \in \mathbb{Z}$ با شرط $\gcd(x, y) = 1$ وجود دارد که:

$$p \mid x^2 + 3y^2.$$

با استفاده از دو مرحله ذکر شده می توان قضیه ۱.۵ را اثبات کرد.
در ابتدا با اثبات مرحله نزول شروع می‌کنیم.
فرض کنید p، مقسوم علیه فرد $N = a^2 + 3b^2$ با شرط $gcd(a, b) = 1$ است. در این صورت بدون کاستن از کلیت می‌توانیم فرض می‌کنیم:

$$|a|, |b| < \frac{1}{2}p \quad (*)$$

(در صورت برقرار نبودن $(*)$ با تغییرات زیر

$$a \mapsto a_1 = a + pk_1, \quad b \mapsto b_1 = b + pk_2$$

[6]Descent Step
[7]Reciprocity Step

و تقسیم بر ۱ < $d = \gcd(a_۱, b_۱)$ شرط را برقرار می‌کنیم).
از آنجایی که $p \nmid d^۲$ ، می‌توانیم فرض کنیم که:

$$p \mid a^۲ + ۳b^۲, \quad \gcd(a, b) = ۱.$$

در این صورت :

$$N < \frac{۱}{۴}p^۲ + \frac{۳}{۴}p^۲ = p^۲ \quad (**).$$

هر مقسوم‌علیه اول N مانند $q \neq p$ از p کمتر است. در غیر این صورت، نابرابری

$$N > pq > p^۲$$

با $(**)$ در تناقض است. به وضوح، p با توان ۱ در تجزیه N ظاهر می‌شود.
حال اگر نتوانیم p را به فرم $x^۲ + ۳y^۲$ بنویسیم در این صورت مقسوم علیه اول q که $q < p$ وجود دارد که q را نیز نتوان به فرم $x^۲ + ۳y^۲$ نوشت.
با استدلالی مشابه درباره q می‌توان دنباله‌ای نامتناهی از مقسوم علیه‌های اول N ساخت که امکان پذیر نیست. بنابراین مقسوم علیه فرد $q < p$ وجود دارد که به فرم $x^۲ + ۳y^۲$ است.

$$p \mid \frac{N}{q}$$

که خود طبق لم **۳.۵** به فرم $c^۲ + ۳d^۲$ است. با تکرار روندی مشابه برای N/q داریم که p نیز به فرم $x^۲ + ۳y^۲$ است.
در ادامه مرحله تقابل را اثبات می‌کنیم. فرض کنید $p \overset{۳}{\equiv} ۱$ است. می‌خواهیم نشان دهیم که

$$\exists x, y \in \mathbb{Z} : \gcd(x, y) = ۱$$

که

$$p \mid x^۲ + ۳y^۲.$$

هنگامی که $p = ۳k + ۱$ گروه $(\mathbb{Z}/p\mathbb{Z})^*$ از مرتبه $۳k$ است. بنابراین برای هر α در $(\mathbb{Z}/p\mathbb{Z})^*$ می‌توان گفت که α ریشه چند جمله ای زیر است.

$$۴(x^{۳k} - ۱) = (x^k - ۱)[(۲x^k + ۱)^۲ + ۳]$$

عامل اول حاصل ضرب سمت راست دارای حداقل k ریشه است، بنابراین عامل دوم باید دارای حداقل $۲k$ ریشه باشد.
فرض کنید $\beta = [b] \in (\mathbb{Z}/p\mathbb{Z})^*$ ریشه‌ای برای عامل دوم است در این صورت:

$$\beta = b + pr$$

بنابراین

$$p \mid (۲b^k + ۱)^۲ + ۳ \qquad و \qquad (۲b^k + ۱)^۲ + ۳ \overset{p}{\equiv} ۰$$

به دلیل این که $\gcd(۲b^k + ۱, ۱) = ۱$ است.
پس مرحله نقابل نیز اثبات می‌شود. □

برای اثبات دو گزاره دیگر ۱.۵ می‌توانیم از استراتژی دو مرحله‌ای اویلر یعنی مرحله نزول و تقابل استفاده کنیم.
برای مطالعه بیشتر به [۷، قضیه ۱.۲.۱] و [۳۵، ص ۱۷۸ - ۱۷۹ ، ۱۹۱ و ۲۱۰ - ۲۱۲] مراجعه کنید.

۲.۵ $n > ۴$

در ادامه مساله $p = x^۲ + ny^۲$ را برای $n > ۴$ در نظر بگیرید. هدف ارائه اثباتی برای مساله در حالت کلی است.

اولین ایده برای ارائه اثبات تعمیم دادن مراحل نزول و تقابل است. همان طور که مشاهده می‌شود برای $n = ۵$،

$$۳ \mid ۲۱ = ۱^۲ + ۵(۲^۲)$$

ولی

$$۳ \neq x^۲ + ۵y^۲$$

بنابراین شرط نزول برای $n = ۵$ کار نمی‌کند.

در فصل بعدی، تعمیم مرحله نزول و دلیل برقرار نبودن آن را برای $n = ۵$ مورد بررسی قرار خواهیم داد.

در ادامه به یافتن شروطی معادل برای مرحله تقابل می‌پردازیم.

اگر $n > ۰$ ایده پیدا کردن هم‌نهشتی‌هایی برای p است به قسمی که درستی $p \mid x^۲ + ny^۲$ تضمین شود.

هم نهشتی‌های ذکر شده در ۱.۵ را می‌توانی با کارکردن در پیمانه $۴n$ معادل کرد. حال شرط معادل، $p \mid x^۲ + ny^۲$ را می توان به شکل زیر بیان کرد:

لم ۴.۵. *فرض کنید $n \in \mathbb{Z}^{>۰}$ و p عدد اول فرد با شرط $\gcd(n,p) = ۱$ است. آنگاه:*

$$\exists x, y \in \mathbb{Z} : p \mid x^۲ + ny^۲, \gcd(x,y) = ۱ \iff \left(\frac{-n}{p}\right) = ۱$$

اثبات. اگر $p \mid x^۲ + ny^۲$ آنگاه (i) $x^۲ + ny^۲ \overset{p}{\equiv} ۰$ از آنجایی که $\gcd(x,y) = ۱$ ، p نسبت به x و y اول خواهد بود. بنابراین y در پیمانه p وارون ضربی دارد.

با ضرب کردن دو طرف رابطه (i) در مربع وارون y (همان $y^{-۱}$) خواهیم داشت:

$$(xy^{-۱})^۲ + n \overset{p}{\equiv} ۰ \Rightarrow \left(\frac{-n}{p}\right) = ۱.$$

برای اثبات میسر عکس داریم:

$$\begin{aligned}(-n/p) = ۱ &\Rightarrow \exists x : x^۲ \equiv -n \bmod p \\ &\Rightarrow x^۲ + n(۱)^۲ \equiv ۰ \bmod p \\ &\Rightarrow p \mid x^۲ + n(۱)^۲.\end{aligned}$$

□

با در نظر گرفتن لم ۴.۵، هدف یافتن هم نهشتی‌هایی روی $p \overset{p}{\equiv} \alpha, \beta, \ldots$ است که $(-n/p) = ۱$ را تضمین کند.
اویلر در سال ۱۷۴۰ به یافتن هم نهشتی‌هایی روی p برای تضمین شرط زیر علاقه مند شد.

$$\left(\frac{-n}{p}\right) = ۱$$

وی با محاسبه برای n های کوچک به نتایج جالب زیر رسید (برای مشاهده جزئیات بیشتر به [۷، ص ۱۳] رجوع کنید).

$$\begin{aligned}
&\left(\frac{۳}{p}\right) \Longleftrightarrow p \equiv \pm ۱ \bmod ۱۲ \\
&\left(\frac{-۳}{p}\right) \Longleftrightarrow p \equiv ۱, ۷ \bmod ۱۲ \\
&\left(\frac{۵}{p}\right) \Longleftrightarrow p \equiv \pm ۱, \pm ۱۱(۳^۲) \bmod ۲۰ \\
&\left(\frac{-۵}{p}\right) \Longleftrightarrow p \equiv ۱, ۳, ۷, ۹ \bmod ۲۰ \qquad (۳.۵) \\
&\left(\frac{۷}{p}\right) \Longleftrightarrow p \equiv \pm ۱, \pm ۳(۵^۲), \pm ۹ \bmod ۲۸ \\
&\left(\frac{-۷}{p}\right) \Longleftrightarrow p \equiv ۱, ۹, ۱۱, ۱۵, ۲۳ \bmod ۲۸ \\
&\left(\frac{۱}{p}\right) \Longleftrightarrow p \equiv \pm ۱, \pm ۵ \bmod ۲۴
\end{aligned}$$

تذکر ۵.۵. *در نظر داشته باشید که ۳.۵ در واقع بیان حدسیات اویلر به زبان مدرن و با استفاده از نماد لژاندر [۸] است.*

با توجه به حدسیات اویلر، می‌توان درباره اعداد اول حدس زیر را بیان کرد.

حدس ۶.۵. *اگر p و q دو عدد اول متمایز باشند آنگاه:*

$$\left(\frac{q}{p}\right) = ۱ \Longleftrightarrow p \equiv \pm \beta^۲ \bmod ۴n$$

که β عدد صحیح فرد است.

[8] Legendre Symbol

حدس ۶.۵ معادل صورت گزاره مهم تقابل مربعی است. بنابراین، می‌توان اویلر را اولین ریاضیدانی در نظر گرفت که قانون تقابل مربعی را کشف کرده است.

گزاره ۷.۵. *اگر p و q دو عدد اول فرد متمایز باشند حدس ۶.۵ معادل گزاره زیر است.*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

اثبات. قرار می دهیم $p^* = (-1)^{\frac{p-1}{2}} p$. با استفاده از خواص نماد لژاندر داریم:

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right) \qquad (۴.۵)$$

در ادامه اثبات می‌کنیم (۴.۵) معادل قانون تقابل مربعی است.
فرض کنید $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$ در این صورت:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) = \begin{cases} 1 & p \text{ یا } q \equiv 1 \bmod 4 \\ -1 & p \equiv q \equiv 3 \bmod 4 \end{cases}$$

پس قانون تقابل مربعی برقرار است. برای اثبات مسیر عکس فرض کنید قانون تقابل مربعی برقرار است، پس:

$$\begin{aligned}\left(\frac{p^*}{q}\right)\left(\frac{q}{p}\right) &= \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \\ &= \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1\end{aligned}$$

بنابراین:

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

در ادامه برای تکمیل اثبات نشان می‌دهیم که حدس ۶.۵ معادل برابری زیر است:

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

از آنجایی که هر دو طرف (۴.۵) برابر ± 1 است، می‌توان تقابل مربعی را به صورت زیر بازنویسی کرد.

$$\left(\frac{q}{p}\right) = 1 \Leftrightarrow \left(\frac{p^*}{q}\right) = 1$$

. با درنظر گرفتن صورت حدس ۶.۵ کافی است ثابت کنیم:

$$\left(\frac{p^*}{q}\right) = ۱ \iff p \overset{۴n}{\equiv} \pm\beta^۲ \ (\beta : \text{فرد}).$$

فرض کنید $\left(\frac{p^*}{q}\right) = ۱$، در این صورت برای اثبات کافی است مساله را در دو حالت زیر بررسی کنیم :

۱. اگر $p \overset{۴}{\equiv} ۱$ در این صورت، $p = p^*$ و داریم $\left(\frac{p}{q}\right) = ۱$ پس:

$$\exists \beta : p \overset{q}{\equiv} \beta^۲ \qquad (۵.۵)$$

با اضافه کردن q به (۵.۵) می‌توانیم مطمئن شویم که β عددی فرد خواهد بود و داریم:

$$p \overset{۴q}{\equiv} \beta^۲.$$

۲. اگر $p \overset{۴}{\equiv} ۳$ در این صورت، $p = -p^*$ و داریم:

$$\left(\frac{-p}{q}\right) = ۱$$

ادامه اثبات این حالت مشابه حالت ۱ است.

برای اثبات عکس نیز مساله را در دو حالت زیر بررسی می‌کنیم:

۱. اگر $p \overset{۴q}{\equiv} \beta^۲$ و β عددی فرد باشد، داریم $p \overset{۴}{\equiv} ۱$ آنگاه $p^* = p$ و $p \overset{q}{\equiv} \beta^۲$ پس:

$$\left(\frac{p}{q}\right) = \left(\frac{p^*}{q}\right) = ۱.$$

۲. اگر $p \overset{۴q}{\equiv} -\beta^۲$ و β عددی فرد باشد، داریم $p \overset{۴}{\equiv} ۳$ آنگاه $p^* = -p$ و با استدلالی مشابه روند حالت ۱ اثبات تکمیل می‌گردد.

□

حدس ۶.۵ و گزاره ۷.۵ تلاش اویلر برای تعمیم دادن مرحله تقابل برای $n > ۴$ است. در صورت علاقه به مشاهده جزئیات بیشتر به [۷، ص ۱۳ - ۱۴] رجوع کنید.
اویلر می‌دانست کار کردن با اعداد اول در واقع حل مساله در حالت خاص است.

لم ۸.۵. *فرض کنید $D \overset{۴}{\equiv} ۰,۱$ عدد صحیح ناصفر است، در این صورت همریختی یکتای زیر وجود دارد.*

$$\chi : \left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^* \longrightarrow \{\pm ۱\}$$

به طوری که برای عدد اول فرد p که D را عاد نکند داریم:

$$\chi([p]) = \left(\frac{D}{p}\right).$$

به علاوه

$$\chi([-۱]) = \begin{cases} ۱ & \text{اگر } D > ۰ \\ -۱ & \text{اگر } D < ۰ \end{cases}$$

اثبات. برای مشاهد اثبات به [۷، لم ۱۴.۱.۱] رجوع کنید. □

نتیجه ۹.۵. *فرض کنید n عددی صحیح و ناصفر است. همریختی زیر را مطابق لم ۸.۵ برای $D = -۴n$ در نظربگیرید.*

$$\chi : \left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^* \longrightarrow \{\pm ۱\}$$

اگر p عدد اول فرد با شرط $p \nmid n$ باشد؛ گزاره‌های زیر با یک‌دیگر معادل‌اند:

۱. *وجود دارد $x, y \in \mathbb{Z}$ به طوری که:*

$$\gcd(x, y) = ۱. \qquad \text{و} \quad p \mid x^۲ + ny^۲$$

۲. $(-n/p) = ۱$

۳. $[p] \in \ker(\chi) \subset (\mathbb{Z}/D\mathbb{Z})^*$

اثبات. قسمت (۱) و (۲) با توجه به لم ۴.۵ معادل‌اند. اثبات معادل بودن قسمت (۲) و (۳) از لم ۸.۵ نتیجه می‌شود. □

فصل ۶

نظریه فرم‌های مربعی

این فصل را نیز با بیان دو حدس از اویلر برای $n = ۵, ۱۴$ شروع می‌کنیم.

۱. $n = ۵$: برای عدد اول فرد $p \neq ۵$ داریم:

$$\begin{aligned} p = x^۲ + ۵y^۲ &\iff p \equiv ۱, ۹ \bmod ۲۰ \\ ۲p = x^۲ + ۵y^۲ &\iff p \equiv ۳, ۷ \bmod ۲۰ \end{aligned} \tag{۱.۶}$$

۲. $n = ۱۴$: برای عدد اول فرد $p \neq ۷$ داریم:

$$\begin{aligned} p = \begin{Bmatrix} x^۲ + ۱۴y^۲ \\ ۲x^۲ + ۷y^۲ \end{Bmatrix} &\iff p \equiv ۱, ۹, ۱۵, ۲۳, ۲۵, ۳۹ \bmod ۵۶ \\ ۳p = x^۲ + ۱۴y^۲ &\iff p \equiv ۳, ۵, ۱۳, ۱۹, ۲۷, ۴۵ \bmod ۵۶ \end{aligned} \tag{۲.۶}$$

در فصل قبل استراتژی اویلر درباره «یافتن اعداد اول p به فرم $x^۲ + ny^۲$» را برای حالت $n = ۱, ۲, ۳$ بررسی کردیم.

در ادامه، دیدیم که مرحله نزول برای $n > ۴$ قابل تعمیم نبود (برای توضیحات بیشتر به **۲.۵** رجوع کنید.) در این فصل با معرفی نظریه فرم‌های مربعی دلیل برقرار نبودن تعمیم مرحله نزول را برای $n > ۴$ دلخواه بررسی می‌کنیم.

۱.۶ تعاریف اولیه

در ابتدا قبل از بیان کردن قضایا و گزاره‌های مربوط به فرم های مربعی و ارتباط آنها با مساله یافتن اعداد اول p به فرم $x^۲ + ny^۲$ موارد زیر را تعریف می‌کنیم.

تعریف ۱.۶. *چندجمله‌ای $f(x,y)=ax^2+bxy+cy^2$ با ضرایب صحیح را فرم مربعی می‌نامند.*

تعریف ۲.۶. *اگر $\gcd(a,b,c)=1$ باشد. فرم $f(x,y)=ax^2+bxy+cy^2$ را اولیه [1] می‌نامند.*

یادداشت ۳.۶. *فرم x^2+ny^2 اولیه است. به همین دلیل بررسی نظریه فرم‌های مربعی در پاسخ به مساله ما موثر خواهد بود.*

توجه کنید که فرم‌های مربعی دارای نمایش ماتریسی‌اند. فرم $f(x,y)=ax^2+bxy+cy^2$ را در نظربگیرید. قرار دهید:

$$C_f := \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$$

در این صورت:

$$2f(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \qquad (۳.۶)$$

تعریف ۴.۶. *در تعریف بالا ماتریس C_f را ماتریس ضرایب فرم می‌نامند.*

تعریف ۵.۶. *عدد صحیح m توسط فرم مربعی $f(x,y)=ax^2+bxy+cy^2$ قابل نمایش [2] است اگر $\exists x,y\in\mathbb{Z}$ به طوریکه $f(x,y)=m$ باشد.*

تعریف ۶.۶. *در تعریف ۵.۶، اگر $\gcd(x,y)=1$ باشد؛ می‌گوییم m به صورت ناسره نمایش داده می‌شود. [3]*

تعریف ۷.۶. *دو فرم مربعی $f(x,y)$ و $g(x,y)$ با یک‌دیگر معادل‌اند [4] ؛ اگر $\exists p,q,r,a\in\mathbb{Z}$ به طوری‌که:*

$$f(x,y)=g(px+qy,rx+sy),\quad ps-qr=\pm 1$$

تذکر ۸.۶. *معادل بدون دو فرم مربعی در تعریف بالا در زبان ماتریسی این گونه است که دترمینان ماتریس تبدیل*

$$M_T=\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

دو فرم f و g برابر ± 1 شود. به عبارتی:

$$M_T=\begin{pmatrix} p & q \\ r & s \end{pmatrix}\in GL_2(\mathbb{Z}).$$

[1] primitive
[2] $f(x,y)=ax^2+bxy+cy^2$ represents m
[3] $f(x,y)=ax^2+bxy+cy^2$ properly represents m
[4] Equivalence

تعریف ۹.۶. *در تعریف ۷.۶، اگر $ps - qr = ۱$ گوییم دو فرم f و g به صورت سره معادل‌اند [۵] . در غیر این صورت به صورت ناسره [۶] با یک‌دیگر معادل‌اند.*

توجه کنید که در تعریف بالا معادل بودن دو فرم به بیان ماتریسی این گونه است که ماتریس تبدیل دارای دترمینان ± ۱ باشد.

مثال ۱۰.۶. *دو فرم $ax^۲ + bxy + cy^۲$ و $ax^۲ - bxy + cy^۲$ با انتقال زیر به صورت ناسره با یک‌دیگر معادل‌اند.*

$$(x, y) \longmapsto (-x, y)$$

لم ۱۱.۶. *فرم $f(x, y)$ عدد صحیح m را به صورت ناسره نمایش می دهد اگر و تنها اگر $f(x, y)$ به صورت سره معادل $mx^۲ + Bxy + Cy^۲$ با $B, C \in \mathbb{Z}$ باشد.*

اثبات. برای مشاهد اثبات به [۷، لم ۳.۲.۱] رجوع کنید. □

تعریف ۱۲.۶. *برای $f(x, y) = ax^۲ + bxy + cy^۲$ مبین فرم را به شکل زیر تعریف کرد.*

$$D = b^۲ - ۴ac$$

دقت کنید که مبین را می‌توان از طریق ماتریس ضرایب نیز بدست آورد:

$$D = -\det(C_f) = -\det\begin{pmatrix} ۲a & b \\ b & ۲c \end{pmatrix} \qquad (۴.۶)$$

لم ۱۳.۶. *فرض کنید دو فرم مربعی $f(x, y)$ و $g(x, y)$ به ترتیب از مبین های D و D' باشند. همچنین اعداد صحیح s و p, q, r وجود دارند به طوری که*

$$f(x, y) = g(px + qy, rx + sy)$$

در این صورت:

$$D = (ps - qr)^۲ D'.$$

اثبات.

$$۲f(x, y) = \begin{pmatrix} x & y \end{pmatrix} C_f \begin{pmatrix} x \\ y \end{pmatrix} \qquad (۵.۶)$$

[5] Properly Equivalent
[6] Improperly Equivalent

و

$$\begin{aligned} ۲g(px+qy, rx+sy) &= \begin{pmatrix} px+qy & rx+sy \end{pmatrix} C_g \begin{pmatrix} px+qy \\ rx+sy \end{pmatrix} \\ &= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix} C_g \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \end{aligned} \tag{۶.۶}$$

چون $f(x,y) = g(px+qy, rx+sy)$ برابر قرار دادن (۵.۶) و (۶.۶) داریم:

$$C_f = \begin{pmatrix} p & r \\ q & s \end{pmatrix} C_g \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

با توجه به رابطه (۴.۶) درباره مبین داریم:

$$\begin{aligned} D &= -\det(C_f) = -\det \begin{pmatrix} p & r \\ q & s \end{pmatrix} \det(C_g) \det \begin{pmatrix} p & q \\ r & s \end{pmatrix} \\ &= -(ps-qr)^۲ \det(C_g) \\ &= (ps-qr)^۲ D' \end{aligned}$$

□

با توجه به لم بالا، دو فرم که به صورت سره یا ناسره با یک‌دیگر معادل‌اند؛ مبین‌های یکسان دارند و با استفاده از لم ۱۱.۶ می‌توان گفت که اعداد یکسانی را، نیز نمایش می‌دهند.

علامت مبین نقش مهمی در علامت اعدادی دارد که توسط فرم نمایش داده می‌شوند.

فرض کنید $f(x,y) = ax^۲ + bxy + cy^۲$ فرم مربعی و D مبین f است. در این صورت:

$$۴af(x,y) = (۲ax+by)^۲ - Dy^۲ \tag{۷.۶}$$

حال وابسته به علامت D مفاهیم زیر را تعریف می‌کنیم:

تعریف ۱۴.۶. *اگر $D > ۰$ در این صورت سمت راست (۷.۶) می تواند مثبت یا منفی باشد و $f(x,y)$ می تواند هم اعداد صحیح مثبت و هم منفی را نمایش دهد. چنین فرمی را، فرم نامعین [۷] می‌نامیم.*

اگر $D < ۰$ در این صورت سمت راست (۷.۶) همواره مثبت است و $f(x,y)$ و a هم علامت خواهند بود.

با توجه به تعریف بالا، تعاریف زیر را داریم:

[7] Indefinite form

تعریف ۱۵.۶. *اگر علامت $f(x,y)$ و a مثبت باشد؛ به فرم $f(x,y)$ مثبت معین* [8] *می‌گوییم.*

تعریف ۱۶.۶. *اگر علامت $f(x,y)$ و a منفی باشد؛ به فرم $f(x,y)$ منفی معین* [9] *می‌گوییم.*

علاوه بر نقش مهم مبین در علامت اعدادی که $f(x,y) = x^۲ + bxy + cy^۲$ نشان می‌دهد، مبین در تعیین زوجیت b نیز نقش دارد. بدین ترتیب که:

$$D = b^۲ - ۴ac \Rightarrow D \equiv b^۲ \bmod ۴ \Rightarrow \begin{cases} b \text{ زوج:} & D \equiv ۰ \bmod ۴ \\ b \text{ فرد:} & D \equiv ۱ \bmod ۴ \end{cases} \qquad (۸.۶)$$

لم ۱۷.۶. *فرض کنید $D \overset{۴}{\equiv} ۰, ۱$ عددی صحیح و m عددی فرد با شرط $\gcd(m, D) = ۱$ است. آنگاه m را می‌توان به صورت سره توسط فرم اولیه‌ای از مبین D نمایش داد، اگر و تنها اگر $(D/m) = ۱$.*

اثبات. برای مشاهد اثبات به [۷، لم ۵.۲.۱] رجوع کنید.

□

نتیجه ۱۸.۶. *فرض کنید n عددی صحیح و p عدد اول فرد است به طوری‌که $p \nmid n$. در این صورت $(-n/p) = ۱$ اگر و تنها اگر p را بتوان توسط فرم اولیه ای از مبین $-۴n$ نمایش داد.*

اثبات. با استفاده از لم ۱۷.۶ برهان بدیهی است. □

نتیجه بالا مربوط به سؤالی است که در فصل ۱ درباره تعمیم مرحله نزول استراتژی اویلر مطرح شد. در واقع هدف یافتن چگونگی نمایش مقسوم علیه های اول $x^۲ + ny^۲$ با شرط $\gcd(x,y) = ۱$ است.

نتیجه ۱۸.۶ پاسخی اولیه به پرسش ما می‌دهد: اعداد اولی که شرط زیر را ارضا می‌کنند.

$$\left(\frac{-۴n}{p}\right) = \left(\frac{-n}{p}\right) = ۱$$

اما مشکل این است که تعداد فرم‌های مربعی از مبین D می‌تواند نامتناهی باشد.

بنابراین در ادامه برای رفع این مشکل اثبات خواهیم کرد که هر فرم با مبین D معادل فرمی کاهش یافته [10] از مبین D است که تعداد این فرم های کاهش یافته متناهی است.

---

[8] Positive definite form

[9] Negative definite form

[10] Reduced Form

۲.۶ فرم‌های کاهش یافته

با توجه به توضیحات بالا در این بخش با معرفی فرم‌های کاهش یافته نشان خواهیم داد که هر فرم مربعی از مبین D به صورت سره با فرم کاهش یافته‌ای معادل خواهد بود.
هم چنین خواهیم دید که تعداد فرم‌های کاهش یافته از مبین D متناهی است.

تعریف ۱۹.۶. *فرم اولیه مثبت معین $f(x,y) = ax^2 + bxy + cy^2$ را کاهش یافته گوییم؛ اگر:*

$$|b| \le a \le c \quad \text{و} \quad b \ge 0 \quad \text{اگر} \quad |b| = a \quad \text{یا} \quad a = c \tag{۹.۶}$$

$x^2 + ny^2$ با توجه به تعریف بالا کاهش یافته است. از این رو بررسی فرم‌های کاهش یافته حائز اهمیت می‌شود.

قضیه ۲۰.۶. *هر فرم مربعی اولیه مثبت معین به صورت یکتا با فرمی کاهش یافته به صورت سره معادل است.*

اثبات. برای مشاهد اثبات به [۳۲، ص ۳۶-۳۸] رجوع کنید. □

یادداشت ۲۱.۶. *فرض کنید $ax^2+bxy+cy^2$ کاهش یافته از مبین $D < 0$ است. در این صورت داریم:*

$$-D = 4ac - b^2 \overset{(۹.۶)}{\ge} 3a^2$$
$$\Rightarrow a \le \frac{\sqrt{(-D)}}{3}.$$

بنابراین برای مبین داده شده D، تعداد مقادیر مختلف برای a متناهی است. همچنین بنابر نامساوی (۹.۶) تعداد مقادیر مختلف برای b نیز متناهی است. بنابر فرمول مبین $D = b^2 - 4ac$ می‌توانیم c را به صورت یکتا تعیین کنیم.

می‌توان به راحتی مشاهده کرد که به صورت سره معادل بودن رابطه هم‌ارزی است. با توجه به این رابطه هم‌ارزی می‌توان تعریف زیر را بیان کرد:

تعریف ۲۲.۶. *فرم‌های f و g در یک کلاس اند؛ اگر این دو فرم به صورت سره با یک‌دیگر معادل باشند.*

$h(D)$ را برابر تعداد کلاس‌های فرم‌های اولیه مثبت معین از مبین D قرار می‌دهیم.

قضیه ۲۳.۶. *فرض کنید $D < 0$ است. در این صورت $h(D)$ متناهی و برابر با تعداد فرم های کاهش یافته با مبین D است.*

اثبات. اثبات این قضیه با در نظر گرفتن قضیه ۲۰.۶ و یادداشت ۲۱.۶ واضح است. □

یادداشت ۲۴.۶. *توضیحات بالا الگوریتمی برای یافتن تمامی فرم های کاهش یافته از مبین D را بیان می‌کند. برای مطالعه بیشتر درباره وجوه محاسباتی عدد رده‌ای به* [۲] *و* [۳۳] *مراجعه کنید.*

قضیه ۲۵.۶. *فرض کنید $D \in \mathbb{Z}^{<0}$ و $D \overset{4}{\equiv} 0, 1$ است. همریختی زیر را از لم ۸.۵ به یاد آورید.*

$$\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$$

برای عدد فرد اول p به شرطی که $p \nmid D$ خواهیم داشت:
$[p] \in \ker(\chi)$ *اگر و تنها اگر p توسط یکی از $h(D)$ فرم کاهش یافته از مبین D نمایش داده شود.*

اثبات. با استفاده از لم ۸.۵ داریم که:

$$[p] \in \ker(\chi) \iff \left(\frac{D}{p}\right) = 1$$

در این صورت با استفاده از لم ۱۱.۶ داریم : $(D/p) = 1$ معادل نمایش p به صورت سره توسط فرمی اولیه با مبین D است. در انتها با استفاده از قضیه ۲۰.۶ اثبات تکمیل می‌گردد. □

یادداشت ۲۶.۶. *قضیه فوق بینش مهمی را ارائه می‌کند: هم نهشتی های $p \overset{D}{\equiv} \alpha, \beta, \gamma, \ldots$ وجود دارند که می‌توانند شرط لازم و کافی برای نمایش عدد اول فرد p توسط فرم کاهش یافته‌ای از مبین D را بیان کنند.*
این نتیجه محاسباتی است، زیرا می دانیم که چگونه فرم‌های کاهش یافته از مبین D را پیدا کنیم، و تقابل مربعی در یافتن کلاس های هم‌نهشتی $\alpha, \beta, \gamma, \ldots$ در پیمانه D به طوری که

$$\left(\frac{D}{p}\right) = 1$$

شود، کمک می‌کند.

۳.۶ $h(D) = ۱$

لم ۱۷.۶ و نتیجه ۱۸.۶ را به خاطر آورید. اگر $h(-۴n) = ۱$ باشد، $(-۴n/p) = ۱$ تضمین می‌کند که عدد اول فرد p به فرم $x^۲ + ny^۲$ است.

چون $x^۲ + ny^۲$ تنها فرم کاهش یافته از مبین $-۴n$ خواهد بود. قضیه زیر شرط لازم و کافی برای زمانی‌که $h(-۴n) = ۱$ است را بیان می‌کند.

قضیه ۲۷.۶. *فرض کنید n عددی صحیح و مثبت است در این صورت داریم:*

$$h(-۴n) = ۱ \Leftrightarrow n = ۱, ۲, ۳, ۴ \text{ یا } ۷$$

اثبات. فرض کنید $n \in \{۱, ۲, ۳, ۷\}$ است در این صورت با استفاده از الگوریتم بیان شده در یادداشت ۲۱.۶ می‌توان نشان داد که $x^۲ + y^۲$، $x^۲ + ۲y^۲$، $x^۲ + ۳y^۲$ و $x^۲ + ۷y^۲$ به ترتیب تنها فرم‌های کاهش یافته از مبین‌های ۴-، ۸-، ۱۲- و ۲۸- اند.

برای اثبات مسیر عکس فرض کنید عدد صحیح n وجود دارد به طوری که

$$n \notin \{۱, ۲, ۳, ۴, ۷\}$$

و $x^۲ + ny^۲$ تنها فرم کاهش یافته از مبین $-۴n$ است.

ادعا می‌کنیم فرم کاهش یافته دیگری از مبین $-۴n$ وجود دارد (یعنی $h(-۴n) > ۱$ است). فرض کنید $n > ۱$ است. در ادامه حالت‌های زیر را بررسی می‌کنیم:

۱. $n \neq p^r$ برای عدد اول p.

اگر n توان عدد اولی نباشد پس عدد اول p وجود دارد که $n = p^r k$ و $p \nmid k$.

اگر $p^r < k$ بود قرار دهید :

$$a = p^r, \quad c = k$$

و در غیر این صورت قرار دهید:

$$a = k, \quad c = p^r.$$

بنابراین $n = ac$ که

$$۱ < a < c < n \text{ و } \gcd(a, c) = ۱$$

است. فرم $ax^۲ + cy^۲$ با توجه به (۹.۶) کاهش یافته است. مبین این فرم برابر $-۴ac = -۴n$ است. پس $h(-۴n) > ۱$ و حالت (۱) رخ نمی‌دهد.

۲. $n = ۲^r$.

اگر $r = ۱, ۲$ در اینصورت $n = ۲, ۴$. پس $r \geq ۳$.

(آ) $r = ۳$ پس $n = ۸$ است و با استفاده از الگوریتم‌های بیان شده در ۲۱.۶ می توان نشان داد که

$$x^۲ + ۸y^۲, \quad ۳x^۲ + ۲xy + ۳y^۲$$

دو فرم کاهش یافته از مبین **۳۲-** اند.

(ب) $r \geq ۴$: در این صورت فرم زیر را در نظر بگیرید.

$$۴x^۲ + ۴xy + (۲^{r-۲} + ۱)y^۲$$

باتوجه به ضرایب، این فرم اولیه و طبق (۹.۶) کاهش یافته است. مبین این فرم برابر $-۴n$ بوده و به همین سبب در این حالت نیز $h(-۴n) > ۱$ است.

بنابر (آ) و (ب) حالت (۲) نیز رخ نمی‌دهد.

۳. $n = p^r$ برای عدد اول p.

اگر $n = p^r$ به طوری که p عدد فرد اولی باشد پس:

(آ) فرض کنید $n + ۱ = ac$ که

$$۱ < a < c < n + ۱ \text{ و } \gcd(a, c) = ۱$$

در این صورت فرم زیر اولیه و بنابر (۹.۶) کاهش یافته است.

$$ax^۲ + ۲xy + cy^۲$$

به علاوه مبین این فرم $-۴n$ است بنابراین $h(-۴n) > ۱$ است.

(ب) اگر $n + ۱$ به صورت ۲^r باشد (چون n فرد است $\Leftarrow n + ۱$ زوج خواهد بود).

ب.۱: اگر $r \geq ۶$ باشد؛ فرم زیر اولیه و بنابر (۹.۶) کاهش یافته است.

$$۸x^۲ + ۶xy + (۲^{s-۳} + ۱)y^۲$$

مبین این فرم نیز $-۴n$ است و $h(-۴n) > ۱$ خواهد بود.

ب.۲: اگر $r \leq ۵$ باشد. در این صورت

$$n \in \{۱, ۳, ۷, ۱۵, ۳۱\}$$

است و تنها حالت **۱۵** و **۳۱** می‌بایست مورد بررسی قرار گیرد. **۱۵** توان عددی اول نیست پس این حالت رخ نمی‌دهد.

فرض کنید $n = ۳۱$ است با استفاده از الگوریتم بیان شده در یادداشت ۲۱.۶ فرم‌های کاهش یافته از مبین ۱۲۴- برابر دو فرم زیر اند.

$$x^۲ + ۳۱y^۲, \quad ۵x^۲ \pm ۴xy + ۷y^۲$$

در این صورت $h(-۴۰۳۱) = ۳$.

بنابر (آ) و (ب) حالت (۳) نیز رخ نمی‌دهد.

توجه داشته باشید زمانی که $n = ۴$ باشد می‌توان گفت:

$$x^۲ + ۴y^۲ = x^۲ + (۲y)^۲$$

پس مساله برای این حالت نیز بررسی شده است. □

مثال ۲۸.۶. *برای درک بهتر برای $n = ۳$ گزاره ارائه شده توسط فرما (۱.۵) را مجددا اثبات می‌کنیم. اثبات دیگر حالات کاملا مشابه است.*
بنابراین فرض کنید $p > ۳$ است. در این صورت $D = -۴۰۳ = ۱۲ \cdot ۳۰۱^۲ + ۰^۲ = ۳$ و داریم:

$$\begin{aligned}\chi([p]) &= \left(\frac{-۱۲}{p}\right) = \left(\frac{-۱}{p}\right)\left(\frac{۳}{p}\right) \\ &= (-۱)^{\frac{p-۱}{۲}}(-۱)^{\frac{p-۱}{۲}}\left(\frac{p}{۳}\right) \\ &= \left(\frac{۳}{p}\right).\end{aligned}$$

بنابراین p توسط فرم کاهش یافته‌ای از مبین ۱۲- نمایش داده می‌شود اگر p در پیمانه ۳ مانده مربعی باشد ($p \overset{۳}{\equiv} ۱$). تنها فرم کاهش یافته از مبین ۱۲- ، $x^۲ + ۳y^۲$ است.
بنابراین:

$$p = x^۲ + ۳y^۲,\ x, y \in \mathbb{Z} \iff p = ۳,\ p \equiv ۱ \bmod ۳$$

۴.۶ $h(D) > ۱$ و نظریه گونای مقدماتی

مثال ۲۹.۶. *با استفاده از قضیه ۲۵.۶ و نتیجه ۱۸.۶ برای $n = ۵$ داریم:*

$$p \equiv ۱, ۳, ۷, ۹ \bmod ۲۰ \iff \left(\frac{-۵}{p}\right) = ۱$$
$$\iff p = x^۲ + ۵y^۲ \text{ یا } p = ۲x^۲ + ۲xy + ۳y^۲$$

در مثال بالا نیازمند نظریه‌ای هستیم که با استفاده از آن بتوان روشی برای جداسازی اعداد اول نمایش داده شده توسط دو فرم زیر ارائه کرد.

$$x^۲ + ۵y^۲, \quad ۲x^۲ + ۲xy + ۳y^۲$$

لاگرانژ [۱۱] هم‌نهشتی هایی در $(\mathbb{Z}/D\mathbb{Z})^*$ را که توسط یک فرم نمایش داده می‌شوند را در یک گروه قرار می‌داد بنابر ایده وی برای $n = ۵$ داریم:

$x^۲ + ۵y^۲$ ۱ و ۹ را در $(\mathbb{Z}/۲۰\mathbb{Z})^*$ نمایش می دهد.
$x^۲ + ۲xy + ۳y^۲$ ۳ و ۷ را در $(\mathbb{Z}/۲۰\mathbb{Z})^*$ نمایش می دهد.

لاگرانژ در نوشته‌های خود روشی نظامند برای تعیین کلاس‌های هم‌نهشتی در $(\mathbb{Z}/D\mathbb{Z})^*$ که توسط فرم کاهش یافته با مبین D نمایش داده می‌شوند؛ ارائه کرد (برای مطالعه بیشتر به [۲۴، ص ۷۵۹-۷۶۵] رجوع کنید).

تعریف ۳۰.۶. *دو فرم مربعی اولیه مثبت معین با مبین D از یک گونه اند؛ اگر این دو فرم مقادیر یکسانی را در $(\mathbb{Z}/D\mathbb{Z})^*$ نمایش دهند.*

تعریف ۳۱.۶. *برای عدد صحیح $D \overset{۴}{\equiv} ۰, ۱, D < ۰$ فرم اصلی [۱۲] را به شکل زیر تعریف می‌کنیم:*

$$x^۲ - \frac{D}{۴}y^۲, \quad D \equiv ۰ \bmod ۴$$
$$x^۲ + xy + \frac{۱ - D}{۴}y^۲, \quad D \equiv ۱ \bmod ۴$$

توجه کنید که برای $D = -۴n$ فرم مربعی $x^۲ + ny^۲$ اصلی خواهد بود.

[11] Lagrange
[12] Principal Form

لم ۳۲.۶. *فرض کنید $D \not\equiv ۰, ۱ \pmod 4$ منفی است. $\ker(\chi) \subset (\mathbb{Z}/D\mathbb{Z})^*$ را از قضیه ۲۵.۶ به یادآورید. فرض کنید $f(x,y)$ از مبین D است. در این صورت داریم:*

۱. *مقادیر نمایش داده شده در $(\mathbb{Z}/D\mathbb{Z})^*$ توسط فرم اصلی با مبین D تشکیل زیر گروه H از $\ker(\chi)$ را می‌دهند.*

۲. *مقادیر نمایش داده شده توسط فرم $f(x,y)$ همدسته‌ای از H در $(\mathbb{Z}/D\mathbb{Z})^*$ است.*

قبل از اثبات نیاز به لم زیر داریم:

لم ۳۳.۶. *فرم اولیه $f(x,y) = ax^۲ + bxy + cy^۲$ و عدد صحیح M داده شده اند. در این صورت $f(x,y)$ حداقل یک عدد صحیح نسبت به M اول را به صورت سره نمایش می‌دهد.*

اثبات. اثبات را در دو گام کامل می‌کنیم:

۱. اگر $M = p$ اول باشد؛ در این صورت نشان می‌دهیم حداقل یکی از مقادیر زیر نسبت به p اول است.

$$f(۰,۱), \quad f(۱,۰), \quad f(۱,۱)$$

فرض کنید p هر سه مقدار ذکر شده را عاد می‌کند.

$$\begin{array}{l} p \mid f(۱,۰) = a \\ p \mid f(۰,۱) = c \\ p \mid f(۱,۱) = a+b+c \end{array} \Longrightarrow p \mid \gcd(a,b,c) = ۱ \Rightarrow p = ۱.$$

۲. فرض کنید $M = \prod_{i=۱}^{r} p_i^{\alpha_i}$ ؛ بنابر قضیه باقیمانده چینی برای هر p_i می‌توان (x_i, y_i) را به طوری از بین $(۰,۱), (۱,۰)$ و $(۱,۱)$ انتخاب کرد که $p_i \nmid f(x_i, y_i)$. حال :

$$\begin{array}{l} p_۱ \nmid f(x_۱, y_۱) \\ p_۲ \nmid f(x_۲, y_۲) \\ \quad . \\ \quad . \\ \quad . \\ p_r \nmid f(x_r, y_r) \end{array} \Rightarrow \begin{array}{l} \exists x : \forall i \in \{۱,۲,...,r\}\ x \equiv x_i \pmod{p_i} \\ \exists y : \forall i \in \{۱,۲,...,r\}\ y \equiv y_i \pmod{p_i} \end{array}$$

$$\Rightarrow \forall i : f(x,y) \equiv f(x_i, y_i) \not\equiv ۰ \pmod{p_i}$$
$$\Rightarrow \gcd(f(x,y), M) = ۱$$

در صورتی که $\gcd(x,y) = d > ۱$ می‌توان از $f(x/d, y/d)$ استفاده کرد.

□

در ادامه اثبات لم ۳۲.۶ را بررسی می‌کنیم:

اثبات. قبل از اثبات، توجه کنید که اگر $m \in \mathbb{Z}$ و $\gcd(m, D) = ۱$ در این صورت m توسط فرمی از مبین D نمایش داده می‌شود. بنابراین:

$$[m] \in \ker(\chi).$$

$$\exists x, y \in \mathbb{Z} : m = f(x,y) \xrightarrow{\gcd(x,y)=d} m = d^۲ f(x/d, y/d)$$

$$\xrightarrow[y/d := y.]{x/d := x.} m = d^۲ \underbrace{f(x., y.)}_{:= m.}$$

که $m.$ به صورت سره توسط f نمایش داده می‌شود. پس:

$$\chi([m]) = \chi([d^۲ m.]) = \underbrace{\chi([d])^۲}_{=۱} \chi([m.]) = \chi([m.]).$$

بنابراین از ابتدا فرض کنید که m به صورت سره توسط فرمی با مبین D نمایش داده می‌شود.
اگر فرم $f(x,y)$ ، m را به صورت سره نمایش بدهد بنابر لم ۱۱.۶ فرم $g(x,y) = mx^۲ + Bxy + Cy$ وجود دارد که با $f(x,y)$ معادل و از مبین D است.
پس:

$$\chi([m]) = \left(\frac{D}{m}\right) = \left(\frac{B^۲ - ۴mC}{m}\right) = \left(\frac{B^۲}{m}\right) = \left(\frac{B}{m}\right)^۲ = ۱$$

بنابراین:

$$[m] \in \ker(\chi).$$

اثبات را برای حالت $D = -۴n$ ارائه می‌دهیم و روند اثبات $D \overset{۴}{\equiv} ۱$ کاملا مشابه صورت می‌گیرد.

اثبات ۱. $D = -۴n$ است در این صورت فرم های اصلی به صورت $x^۲ + ny^۲$ است و بنابر (۲.۵) مجموعه فرم‌های اصلی نسبت به ضرب دو فرم بسته خواهد بود و $H \subset \ker(\chi)$ زیر گروه است.

اثبات ۲. در لم ۳۳.۶ ، $M = D = -۴n$ قرار دهید؛ پس $a \in \mathbb{Z}$ وجود دارد که توسط $f(x,y)$ نمایش داده شود. با استفاده از لم ۱۱.۶ فرض کنید $f(x,y) = ax^۲ + bxy + cy^۲$ است. بنابراین:

$$\xrightarrow{D \overset{۲}{\equiv} b (۸.۶)} af(x,y) = \underbrace{(ax + \frac{b}{۲}y)^۲ + ny^۲}_{\text{فرم اصلی}} \quad (*).$$

پس مقادیری در $(\mathbb{Z}/D\mathbb{Z})^*$ که توسط $f(x,y)$ نمایش داده می‌شوند در همدسته $[a]^{-1}H$ قرار دارند.

برای $[c] \in [a]^{-1}H$ داریم:

$$\exists z, w : ac \equiv z^2 + nw^2 \bmod 4n (**) \overset{(*)}{\Rightarrow} \exists y. : y. \equiv w \bmod 4n$$
$$\overset{(*),(**)}{\Rightarrow} \exists x. \equiv a^{-1}(z - \frac{b}{2}y.) \bmod D$$
$$\Rightarrow f(x., y.) \equiv c \bmod 4n$$

در این صورت $f(x,y)$ دقیقا اعداد همدسته $[a]^{-1}H$ را نمایش می‌دهد.

□

تعریف ۳۴.۶. *فرض کنید H' همدسته H در $\ker(\chi)$ است (نماد گذاری ۳۲.۶) . در این صورت گونا H' را تمامی فرم‌های کاهش یافته ای از مبین D می‌نامیم که مقادیر H' را نمایش می‌دهد.*

می‌دانیم که همدسته‌های مختلف یک زیرگروه یا کامل مجزا و یا کاملا یکسان‌اند. بنابراین با استفاده از لم ۳۲.۶ می‌توان گفت دو فرم کاهش یافته یا کاملا مقادیری یکسانی در $(\mathbb{Z}/D\mathbb{Z})^*$ را نمایش می‌دهند، یا کاملا مقادیر مجزایی در $(\mathbb{Z}/D\mathbb{Z})^*$ را نمایش می‌دهند.

قضیه ۳۵.۶. *فرض کنید $D \overset{4}{\equiv} 0, 1$ عدد صحیح منفی‌ای است. $H \subset \ker(\chi)$ را از ۳۲.۶ به یاد آورید. اگر H' همدسته H در $\ker(\chi)$ و p عدد اول فرد باشد به طوری که $p \nmid D$:*

$[p] \in \ker(\chi)$ اگر و تنها اگر p را بتوان توسط یکی از فرم‌های مبین D در گونا H' نمایش داد.

اثبات. اثبات با توجه به توضیحات بالا بدیهی است. □

تعریف ۳۶.۶. *گونایی که شامل فرم اصلی است را گونای اصلی می‌نامیم.*

نتیجه ۳۷.۶. *فرض کنید $n \in \mathbb{Z}^+$ و p عدد اول فرد است که $p \nmid n$. آنگاه p را می‌توان توسط فرمی با مبین D در گونای فرم اصلی نمایش داد؛ اگر و تنها اگر عدد صحیح β وجود داشته باشد به طوری که:*

$$p \equiv \beta^2 \text{ یا } \beta^2 + n \bmod 4n$$

اثبات.

$$\exists x, y : p = x^2 + ny^2 \iff \begin{matrix} p \equiv x^2 \bmod D & y : \text{زوج} \\ p \equiv x^2 + n(1)^2 \bmod D & y : \text{فرد} \end{matrix}$$

□

یادداشت ۳۸.۶. *با استفاده از توضیحات بالا زمانی که گونای اصلی تنها شامل یک فرم کاهش یافته است اگر همنهشتی‌هایی برای عدد اول p وجود داشته باشد که تضمین کند p توسط فرمی در گونای اصلی نمایش داده می‌شود می‌توان گفت که در واقع شرط لازم و کافی برای نمایش p به فرم $x^2 + ny^2$ یافته‌ایم.*

۵.۶ ترکیب فرم‌های مربعی و گروه رده ای

در ادامه هدف بررسی نظریه‌های موجود برای زمانی است که دو فرم از مبین یکسان را با یک‌دیگر ترکیب می‌کنیم.

نشان خواهیم داد که در واقع این عمل ترکیب روی فرم‌های کاهش یافته از مبین D سبب القا کردن ساختاری گروهی به مجموعه این فرم‌ها می‌شود.

به علاوه اگر ترکیب رو فرم مربعی f, g را F بنامیم؛ خواهیم دید که F حاصلضرب اعدادی که توسط f و g نمایش داده می‌شود را نمایش می‌دهد.

تعریف ۳۹.۶. *فرض کنید $f(x,y)$، $g(x,y)$ دو فرم اولیه مثبت معین با مبین D اند. در این صورت فرم $F(x,y)$ اولیه و از مبین D را ترکیب این دو می‌نامیم اگر*

$$f(x,y)g(z,w) = F(B_1(x,y;z,w), B_2(x,y;z,w))$$

به طوری که:

$$B_i(x,y;z,w) = a_i xz + b_i xw + c_i yz + d_i yw, i = 1,2$$

فرم های دو خطی صحیح اند.

با توجه به تعریف بالا دو فرم را می‌توان به روش‌های مختلف ترکیب کرد، و فرم‌های به‌دست‌آمده لزوما با یک‌دیگر معادل نیستند.

برای معرفی ترکیب خوش تعربف روی کلاس‌های فرم‌ها باید به نحوی مفهوم ترکیب را محدود کنیم.

گاوس بدین منظور با توجه به داده های ترکیب بالا ثابت کرد که:

$$a_1 b_2 - a_2 b_1 = \pm f(1,0), \quad a_1 c_2 - a_2 c_1 = \pm g(1,0) \qquad (10.6)$$

اثبات. برای اثبات به [۱۴، § ۲۳۵] رجوع کنید. □

تعریف ۴۰.۶. *در (۱۰.۶) اگر هر دو علامت + باشند در این صورت ترکیب را ترکیب مستقیم*[۱۳] *می‌نامیم.*

یادداشت ۴۱.۶. *یکی از مهم ترین نتایج ترکیب مستقیم گاوس روی مجموعه کلاس‌های فرم‌های از مبین D تبدیلشان به گروه آبلی متناهی است.*

برای مشاهده اثبات این موضوع می‌توانید به [۱۴، ۲۴۰ – §۲۳۶, §۲۴۵ و §۲۴۵] رجوع کنید.

[13] Direct Composition

متاسفانه، ترکیب مستقیم مفهوم بسیار پیچیده‌ای برای کارکردن است؛ پس به جای استفاده از ایده گاوس برای ترکیب (ترکیب مستقیم) ما از ترکیب معرفی شده توسط دیریشله [۱۴] برای ترکیب دو فرم استفاده می‌کنیم (برای مشاهده ایده اولیه و جزئیات بیشتر به [۹، Supplement X] مراجعه کنید).

قبل از تعریف ترکیب دیریشله، ترکیب لژاندر را بررسی می‌کنیم.

ترکیب لژاندر در واقع ایده‌ای اولیه برای دیریشله برای معرفی ترکیب خود بوده است و ترکیب دیریشله به گونه‌ای کلی تر کردن ترکیب لژاندر است.

تعریف ۴۲.۶. *فرض کنید*

$$f(x,y) = ax^2 + 2bxy + cy^2$$

و

$$g(x,y) = a'x^2 + 2b'xy + c'y^2$$

دو فرم مربعی از مبین $D = -4n$ اند و $\gcd(a,a') = 1$ (همواره با تغییر فرم ها به معادل‌های سره آنها می‌توان شرط $\gcd(a,a') = 1$ را برقرار کرد).
در این صورت ترکیب لژاندر f و g به شکل زیر است:

$$F(x,y) = aa'x^2 + 2Bxy + \frac{B^2+n}{aa'}y^2 \qquad (۱۱.۶)$$

که B با استفاده از قضیه باقیمانده چینی و از هم‌نهشتی‌های زیر بدست می‌آید.

$$\begin{aligned} B &\equiv \pm b \bmod a \\ B &\equiv \pm b' \bmod a' \end{aligned} \qquad (۱۲.۶)$$

در ادامه برای ترکیب دیریشله دو لم زیر را نیاز داریم:

لم ۴۳.۶. *فرض کنید $\{p_1,...,p_r,q_1,...,q_r,m\} \in \mathbb{Z}$ و $\gcd(p_1,...,p_r,m) = 1$ است. در این صورت عدد یکتای $B \not\equiv 0 \pmod m$ وجود دارد به طوری که:*

$$\forall i \in \{1,..,r\}\ p_iB \equiv q_i \bmod m \Leftrightarrow \forall i,j = 1,...,r:\ p_iq_j \equiv p_jq_i \bmod m$$

اثبات. برای اثبات سمت راست به چپ داریم:

$$\forall i,j \in \{1,..,r\}: \begin{cases} p_iB \equiv q_i \bmod m \\ p_jB \equiv q_j \bmod m \end{cases} \xrightarrow{B^{-1}(\bmod m)} p_iq_j \equiv p_jq_i \bmod m.$$

[14] Dririchlet

برای اثبات مسیر عکس:

$$\gcd(m, p_1, ..., p_r) = 1 \Rightarrow \exists a, a_1, ..., a_r \in \mathbb{Z} : \underbrace{am + \sum_{i=1}^{r} a_i p_i = 1}_{\text{قضیه بزو}}$$

$$\Rightarrow \forall j \in \{1, .., r\} : q_j(\sum_{i=1}^{r} a_i p_i \equiv 1 \bmod m)$$

$$\overset{p_i q_j \equiv p_j q_i \bmod m}{\Longrightarrow} p_j \underbrace{(\sum_{i=1}^{r} a_i q_i)}_{:=B} \equiv q_j \bmod m$$

□

لم ۴۴.۶. *فرض کنید*

$$f(x, y) = ax^2 + bxy + cy^2$$

و

$$g(x, y) = a'x^2 + b'xy + c'y^2$$

دو فرم مربعی از مبین D با شرط زیر اند.

$$\gcd(a, a', (b + b')/2) = 1$$

در این صورت عدد یکتای B در پیمانه $2aa'$ وجود دارد به قسمی که:

$$B \equiv \pm b \bmod 2a \quad (i)$$
$$B \equiv \pm b' \bmod 2a' \quad (ii)$$
$$B^2 \equiv \pm D \bmod 2aa' \quad (iii)$$

اثبات.

$$\exists B \overset{(i),(ii)}{\Longleftrightarrow} (B - b)(B - b') \equiv 0 \bmod 4aa' \Longleftrightarrow B^2 - (b + b')B + bb' \equiv 0 \bmod 4aa' (*)$$

$$\exists B \overset{(iii)}{\Leftrightarrow} B^2 \equiv D \bmod 4aa' \overset{(*)}{\Longleftrightarrow} \frac{D + bb'}{2} \equiv \frac{b + b'}{2} \cdot B \bmod 2aa' (**)$$

$$\overset{(i),(ii),(**)}{\Longrightarrow} \begin{cases} a'B \equiv a'b \bmod 2aa' \\ aB \equiv ab' \bmod 2aa' \\ \frac{b+b'}{2} \cdot B \equiv \frac{D+bb'}{2} \bmod 2aa' \end{cases}$$

و با استفاده از لم ۴۳.۶ ، B به صورت یکتا در پیمانه $2aa'$ مشخص می‌شود. □

با استفاده از لم ۴۳.۶ و ۴۴.۶ می‌توان ترکیب ارائه شده توسط دیریشله را تعریف کرد.

تعریف ۴۵.۶. *فرض کنید*

$$f(x,y) = ax^۲ + ۲bxy + cy^۲$$

و

$$g(x,y) = a'x^۲ + ۲b'xy + c'y^۲$$

دو فرم اولیه و مثبت معین از مبین $D < ۰$ اند شرط زیر برقرار است.

$$\gcd(a, a', (b+b')/۲) = ۱.$$

در این صورت ترکیب دیریشله f و g را به شکل زیر تعریف می‌کنیم:

$$F(x,y) = aa'x^۲ + Bxy + \frac{B^۲ - D}{۴aa'}y^۲ \qquad (۱۳.۶)$$

که B را با استفاده از لم ۴۴.۶ بدست می‌آید.

درباره ترکیب دیریشله می‌توان نکات زیر را بیان کرد:

۱. ترکیب دیریشله به اندازه ترکیب مستقیم تعریف ۴۰.۶ کلی نیست.

۲. در ترکیب دیریشله با قراردادن $D = -۴n$ می‌توان به ترکیب ارائه شده توسط لژاندر در تعریف ۴۲.۶ رسید.

قضیه ۴۶.۶ (خواص ترکیب دیریشله). *$f(x,y)$ و $g(x,y)$ را مانند تعریف بالا در نظر بگیرید و $F(x,y)$ را ترکیب دیریشله مطابق (۱۳.۶) تعریف کنید. آنگاه:*

۱. *$F(x,y)$ فرم اولیه، مثبت معین با مبین D است.*

۲. *$F(x,y)$ ترکیب مستقیم با توجه به تعریف ۴۰.۶ است.*

اثبات. برای اثبات به [۷، گزاره ۸.۳.۱] رجوع کنید. □

نمادگذاری ۴۷.۶. *نمادگذاری‌های زیر را در نظر بگیرید:*

۱. *$C(D)$ را مجموعه کلاس‌های فرم‌های اولیه مثبت معین در نظر می‌گیریم.*

۲. *تعریف ۳۱.۶ را بیادآورید؛ کلاسی که شامل فرم اصلی است را کلاس اصلی می‌گوییم.*

۳. *فرم $ax^۲ - bxy + cy^۲$ را وارون فرم $ax^۲ + bxy + cy^۲$ تعریف می‌کنیم.*

در قضیه بعدی نشان خواهیم داد که با القای ترکیب دیریشله روی $C(D)$ می توان آن را به گروه آبلی متناهیا تولید شده از مرتبه $h(D)$ تبدیل کرد.

قضیه ۴۸.۶. *فرض کنید $D < 0$ و $D \overset{4}{\equiv} 0, 1$، $C(D)$ را مطابق نمادگذاری بالا در نظر بگیرید. آنگاه ترکیب دیریشله روی $C(D)$ عملیات دوتایی خوش تعریفی القا می‌کند که $C(D)$ را به گروه آبلی متناهیا تولید شده از مرتبه $h(D)$ تبدیل می‌کند.*
به علاوه عنصر همانی $C(D)$ کلاس شامل فرم:

$$x^2 - \frac{D}{4}y^2 \quad D \equiv 0 \bmod 4 \text{ اگر}$$
$$x^2 + xy + \frac{1-D}{4}y^2 \quad D \equiv 1 \bmod 4 \text{ اگر}$$

است. وارون کلاس شامل $ax^2 + bxy + cy^2$ را کلاس شامل $ax^2 - bxy + cy^2$ در نظر بگیرید.

اثبات. برای مشاهده بخش خوش تعریفی عملیات القا شده روی مجموعه کلاس‌ها و اثبات کردن آبلی بودن مجموعه $C(D)$ تحت ترکیب دیریشله به [Supplement X، ۹] و یا [§V.2، ۱۲] رجوع کنید. برای مشاهده ادامه اثبات به [۷، قضیه ۹.۳.۱] رجوع کنید. □

۱.۵.۶ کلاس‌های $C(D)$ از مرتبه ≥ 2

در ادامه این فصل خواهیم دید که کلاس‌های گروه $C(D)$ از مرتبه ≥ 2 نقش بسیار مهمی در نظریه گونا و هم‌چنین ترکیب دو فرم ایفا می‌کنند.
علاوه بر این فرم‌های کاهش یافته در این کلاس‌ها به سادگی قابل شناسایی‌اند.

لم ۴۹.۶. *فرم کاهش یافته $f(x,y) = ax^2 + bxy + cy^2$ از مرتبه ۲ است اگر و تنها اگر $f(x,y)$ و $f'(x,y) = ax^2 - bxy + cy^2$ به صورت سره با یک‌دیگر معادل باشند.*

اثبات. برای اثبات به لم ۱۰.۳.۱ [۷] رجوع کنید. □

گزاره ۵۰.۶. *فرض کنید $D < 0$ ، $D \overset{4}{\equiv} 0, 1$ و r تعداد مقسوم علیه‌های فرد D است . μ را مطابق زیر تعریف کنید:*

۱. *زمانی که $D \overset{4}{\equiv} 1$ قرار دهید $\mu = r$.*

۲. *زمانی که $D \overset{4}{\equiv} 0$ و $D = -4n$ ، μ را بر اساس جدول زیر انتخاب کنید:*

μ	n
r	$n \equiv ۳ \bmod ۴$
$r+۱$	$n \equiv ۱, ۲ \bmod ۴$
$r+۱$	$n \equiv ۴ \bmod ۸$
$r+۲$	$n \equiv ۰ \bmod ۸$

آنگاه گروه $C(D)$ شامل دقیقا $۲^{\mu-۱}$ عنصر از مرتبه ≥ ۲ است.

اثبات. برای مشاهده اثبات حالت $D = -۴n$ که $n \overset{۴}{\equiv} ۱$ به گزاره ۱۱.۳.۱ [۷] و برای دیگر حالت‌ها به [۱۲، §V.5] ، [۱۴، ۲۵۷ - §§ ۲۵۸] و یا [۲۸، ص ۱۷۱ - ۱۷۳] مراجعه کنید. □

۶.۶ نظریه گونا

برای معرفی نظریه گونا نیازمند یادآوری موارد زیر هستیم.

۱. دو فرم با مبین D در یک گونا اند اگر در $(\mathbb{Z}/D\mathbb{Z})^*$ مقادیر یکسانی را نمایش دهند.

۲. همریختی χ را برای عدد اول p که $p \nmid D$ را به شکل زیر تعریف کردیم:

$$\begin{aligned} \chi : (\mathbb{Z}/D\mathbb{Z})^* &\longrightarrow (\mathbb{Z}/۲\mathbb{Z}) = \{\pm ۱\} \\ \chi([p]) &\longmapsto \left(\frac{D}{p}\right) \end{aligned}$$

(آ) $\ker(\chi)$ دارای اندیس ۲ در $(\mathbb{Z}/D\mathbb{Z})^*$ است.

(ب) مقادیری که توسط فرم اصلی نمایش داده می‌شوند تشکیل زیرگروه H از $\ker(\chi)$ را می‌دهند.

(ج) مقادیری در $(\mathbb{Z}/D\mathbb{Z})^*$ که توسط f با مبین D نمایش داده می‌شوند همدسته‌ای از H است.

با توجه به توضیحات بالا هدف مرتبط کردن مفاهیم ذکر شده با $C(D)$ است. به همین سبب همریختی [۱۵] زیر را تعریف می کنیم:

$$\Phi : C(D) \longrightarrow \ker(\chi)/H \qquad (۱۴.۶)$$

که برای هر $H' \in \ker(\chi)$ ، $\Phi^{-۱}(H)$ شامل تمامی کلاس‌های در این گونا است. بنابراین تصویر Φ با مجموعه‌ای از گوناها تعریف می‌گردد.

لم ۵۱.۶. *فرض کنید $D \overset{۴}{\equiv} ۰, ۱$ عددی منفی است. آنگاه:*

۱. *هر گونای از فرم‌های با مبین D شامل تعداد مساوی از کلاس‌هاست.*

۲. *تعداد فرم‌های با مبین D هر گونا از توان ۲ است.*

اثبات. برای مشاهده اثبات به نتیجه ۱۴.۳.۱ [۷] رجوع کنید. □

قضیه ۵۲.۶. *فرض کنید $D \overset{۴}{\equiv} ۰, ۱$ عددی منفی است. آنگاه:*

۱. *$۲^{\mu-۱}$ گونا از فرم‌های با مبین D وجود دارد، که μ بر اساس گزاره ۵۰.۶ تعیین می‌گردد.*

[۱۵] برای اثبات همریختی بودن تابع Φ به [۷، لم ۱۳.۳.۱] رجوع کنید.

۲ . *گونای اصلی شامل کلاس‌های* $C(D)$[۲] *است.*

برای اثبات قضیه بالا ابتدا نیاز است تشخیص دهیم چه زمانی دو فرم در یک گونا اند. برای این کار از کاراکترهای خاص [۱۶] استفاده می‌کنیم.

تعریف ۵۳.۶. *فرض کنید* $p_1, ..., p_r$ *مقسوم علیه‌های فرد* D *است. حال توابع زیر را برای* p_i *ها بدین گونه تعریف می‌کنیم:*

$$\chi(a) = \left(\frac{a}{p_i}\right) \qquad \gcd(a, p_i) = 1 : a \text{ برای}$$
$$\delta(a) = (-1)^{(a-1)/2} \qquad a : \text{فرد برای}$$
$$\epsilon(a) = (-1)^{(a-1)/2} \qquad a : \text{فرد برای}$$

به جای استفاده تمامی توابع بالا برای D *تعدادی از آن‌ها را برای* D *اختصاص می‌دهیم.*

۱ . *زمانی که* $D \overset{4}{\equiv} 1$ *است،* $\chi_1, ..., \chi_r$ *را کاراکترهای خاص برای* D *در نظربگیرید.*

۲ . *زمانی که* $D \overset{4}{\equiv} 0$ *و* $D = -4n$ *، کاراکترهای خاص* D *را براساس جدول زیر مشخص کنید:*

کاراکترهای خاص	n
$\chi_1, ..., \chi_r$	$n \equiv 3 \bmod 4$
$\chi_1, ..., \chi_r, \delta$	$n \equiv 1 \bmod 4$
$\chi_1, ..., \chi_r, \delta\epsilon$	$n \equiv 2 \bmod 8$
$\chi_1, ..., \chi_r, \epsilon$	$n \equiv 6 \bmod 8$
$\chi_1, ..., \chi_r, \delta$	$n \equiv 4 \bmod 8$
$\chi_1, ..., \chi_r, \delta, \epsilon$	$n \equiv 0 \bmod 8$

با توجه به جدول بالا و مقایسه آن با گزاره ۵۰.۶ می‌توان مشاهده کرد که تعداد کاراکترهای خاص برای مبین D برابر μ است.

با توجه به نحوه تعریف کاراکترهای خاص می‌توان همریختی زیر را تعریف کرد:

$$\Psi : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}^\mu \qquad (۱۵.۶)$$

با استفاده از همریختی بالا می‌توان لم زیر را بیان کرد:

لم ۵۴.۶. *همریختی* Ψ *پوشا است.*

$$\Psi : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}^\mu$$

[16] Assigned Character

هسته آن زیر گروه H از مقادیری است که توسط فرم اصلی نمایش داده می‌شود.
بنابراین Ψ یکریختی زیر را القا می‌کند:

$$(\mathbb{Z}/D\mathbb{Z})^*/H \xrightarrow{\sim} \{\pm 1\}^{\mu}$$

اثبات. برای اثبات به [۷، قضیه ۱۷.۳.۱] رجوع کنید. □

کاراکترهای خاص روشی مناسب برای تعیین این که آیا دو فرم در یک گونا اند یا نه ارائه می‌کنند.
برای اثبات قضیه ۵۲.۶ به [۷، ص ۵۱] رجوع کنید.

۷.۶ گونای ۱: تلاقی کار اویلر و گاوس

به یادداشت ۳۸.۶ رجوع کنید. با توجه به توضیحات بخش‌های قبل می‌دانیم که فرم‌های کاهش یافته‌ای از مبین D که در یک گونا قرار دارند مقادیر یکسانی از $(\mathbb{Z}/D\mathbb{Z})^*$ را نمایش می‌دهند.

بنابراین اگر برای مبین $D = -۴n$ هر گونا شامل ۱ کلاس از فرم‌های کاهش یافته باشد؛ در این صورت با ارائه هم‌نهشتی های مناسب مانند $\alpha, \beta, \gamma, \ldots$ در پیمانه $۴n$ می‌توان تضمین کرد که اگر

$$p \overset{۴n}{\equiv} \alpha, \beta, \gamma, \ldots$$

باشد، p را بتوان به فرم $x^۲ + ny^۲$ نمایش داد.

با استفاده از نظریه گونا و توضیحات بخش‌های قبل می‌توان قضیه زیر را بیان کرد.

قضیه ۵۵.۶. *فرض کنید $n \in \mathbb{Z}^+$ است. در این صورت گزاره‌های زیر معادل اند:*

۱. *هر گونا از فرم‌های با مبین $D = -۴n$ شامل یک کلاس است.*

۲. *اگر $ax^۲ + bxy + cy^۲$ فرم کاهش یافته باشد در این صورت یا $b = ۰$ ، $a = b$ ، یا $a = c$ است.*

۳. *دو فرم مربعی معادل‌اند اگر و تنها اگر به صورت سره معادل باشند.*

۴. *عدد صحیح m وجود دارد به طوری که:*

$$C(-۴n) \cong (\mathbb{Z}/۲\mathbb{Z})^m.$$

۵. $h(-۴n) = ۲^{\mu - ۱}$ *(μ براساس گزاره ۵۰.۶ است).*

اثبات. برای مشاهده اثبات به [۷، قضیه ۲۲.۳.۱] رجوع کنید. □

این قضیه به زیبایی با بهره‌گیری تمامی مفاهیم قبلی از جمله نظریه گونا، فرم‌های کاهش یافته، گروه رده‌ای و اندازه آن و ارتباط بین معادل بودن دو فرم به صورت سره روشی برای یافتن مبین‌هایی که هر گونای آن‌ها شامل یک فرم کاهش یافته (یا یک کلاس) است ارائه می‌کند.

گاوس در [۱۴، §۵] لیستی ۶۵ تایی از مبین‌ها ارائه کرد که در قضیه ۵۵.۶ صدق می کنند

. ([§۳۰۳ ،۱۴])

(۱۶.۶)

$h(-۴n)$	n هایی که شامل یک‌فرم در هر گونا هستند
۱	۱, ۲, ۳, ۴, ۷
۲	۵, ۶, ۸, ۹, ۱۰, ۱۲, ۱۳, ۱۵, ۱۶, ۱۸, ۲۲, ۲۵, ۲۸, ۳۷, ۵۸
۴	۲۱, ۲۴, ۳۰, ۳۳, ۴۰, ۴۲, ۴۵, ۴۸, ۵۷, ۶۰, ۷۰, ۷۲, ۷۸, ۸۵, ۸۸, ۹۳, ۱۰۲, ۱۱۲ ۱۳۰, ۱۳۳, ۱۷۷, ۱۹۰, ۲۳۲, ۲۵۳
۸	۱۰۵, ۱۲۰, ۱۶۵, ۱۶۸, ۲۱۰, ۲۴۰, ۲۷۳, ۲۸۰, ۳۱۲, ۳۳۰, ۳۴۵, ۳۵۷, ۳۸۵ ۴۰۸, ۴۶۲, ۵۲۰, ۷۶۰
۱۶	۸۴۰, ۱۳۲۰, ۱۳۶۵, ۱۸۴۸

دلیل اصلی علاقه گاوس به این ۶۵ مبین، تلاقی کار وی با اویلر بود. بدین معنا که اویلر پیش از او این لیست ۶۵تایی را برای هدف دیگری کشف کرده بود.

در زمان اویلر یافتن اعداد اول کار چندان ساده‌ای نبود. اویلر با معرفی اعداد آسوده [۱۷] توانست اعداد اول بزرگی را کشف کند.

ابتدا اعداد آسوده را تعریف کرده و سپس ارتباط کار اویلر و گاوس را در قالب قضیه‌ای شرح می‌دهیم.

تعریف ۵۶.۶. *فرض کنید m عددی فرد و نسبت به n اول است؛ به طوری که m را می‌توان به صورت سره توسط فرم $x^۲ + ny^۲$ نمایش داد.*

اگر معادله $m = x^۲ + ny^۲$ تنها یک جواب با شرط $x, y \geq ۰$ داشته باشد؛ در این صورت m اول است و n را عدد آسوده می‌نامیم. [۱۸]

مثال ۵۷.۶. *فرض کنید $n = ۱۸۴۸$ در این صورت اویلر توانست نشان دهد که عدد زیر اول است.*

$$۱۸,۵۱۸,۸۰۹ = ۱۹۷^۲ + ۱۸۴۸\times۱۰۰^۲$$

در ادامه با بیان قضیه زیر که توسط گاوس بیان شد نحوه ارتباط کار گاوس و اویلر را شرح می‌دهیم.

قضیه ۵۸.۶. *فرض کنید $n \in \mathbb{Z}^+$ است. در این صورت n ، عدد آسوده است اگر و تنها اگر برای فرم‌های با مبین $-۴n$ ، هر گونا شامل یک کلاس باشد.*

اثبات. برای اثبات به [۷، گزاره ۲۴.۳.۱] رجوع کنید. □

[17] Convenient Numbers: Numerus Idoneus

[۱۸] برای مطالعه بیشتر درباره اعداد آسوده به [۱۳] یا [۳۵، ص ۲۱۹ - ۲۲۶] رجوع کنید.

مساله‌ای که در انتها مطرح می‌شود مربوط به کامل بودن یا نبودن لیست ۶۵ تایی ارائه شده توسط گاوس و اویلر است.

گاوس ادعا می‌کرد که این لیست کامل است و یا با اضافه کردن یک n کامل می‌شود (برای مشاهده جزئیات بیشتر به [۱۴، §§۳۰۳] رجوع کنید) .

در سال ۱۹۳۴، چاولا ([۳، ص ۳۰۴-۳۰۷]) اثبات کرد که تعداد مبین‌هایی که در قضیه ۵۵.۶ صدق می‌کنند متناهی است و در سال ۱۹۷۳ اثبات شد که لیست ۱۶.۶ کامل است و یا تنها با اضافه کردن یک عدد تکمیل می‌گردد [۳۶].

مساله وجود این یک مبین اضافی برای تکمیل لیست هنوز مساله‌ای باز است.

۸.۶ نکات پایانی

ابتدای فصل را با بیان دو حدس از اویلر شروع کردیم و در ادامه با شرح نظریه فرم‌های مربعی و نظریه گونا توانستیم شرط لازم و کافی برای متناهی عدد n بدست آوریم که عدد اول p را بتوان به فرم $x^۲ + ny^۲$ نوشت.

در واقع نشان دادیم اگر در هر گونا تنها یک کلاس فرم باشد؛ در این صورت اعدادی در $(\mathbb{Z}/D\mathbb{Z})^*$ که توسط گونای اصلی نمایش داده می‌شوند؛ جواب‌های مساله ۱ اند.

در ادامه با بررسی مثال $n = ۵$ کاربرد این نظریات مقدماتی را به طور روشن تری مشاهده کردیم.

ولی همان طور که در ابتدای فصل مشاهده کردیم؛ در حالت $n = ۱۴$ (۲.۶) به دلیل اینکه در گونای اصلی دو فرم کاهش یافته داریم، نظریه گونا نمی توانست تمایزی در اعداد نمایش داده شده برای دو فرم زیر ارائه کند.

$$x^۲ + ۱۴y^۲, \quad ۲x^۲ + ۷y^۲$$

بنابراین نیازمند تئوری قوی‌تری برای حالت $n = ۱۴$ هستیم.

به طور کلی می‌توان گفت اگر برای عدد صحیح مثبت n هر گونا شامل بیش از یک فرم کاهش یافته باشد در این صورت روش‌های مقدماتی (نظریه فرم‌های مربعی و نظریه گونا) قادر به حل مساله نخواهند بود. با توجه به این محدودیت نیازمند معرفی تئوری‌ای قوی تر برای حل مساله اصلی هستیم.

بخش سوم

نظریه میدان رده‌ای

نظریه میدان رده‌ای [۱۹] توصیف توسیع‌های آبلی موضعی [۲۰] و سراسری [۲۱] است. اصطلاح «میدان رده‌ای» به توسیع میدانی اشاره دارد که شرطی وابسته به گروه رده‌ای را ارضا کند.

یکی از قضایای اساسی نظریه میدان‌های رده‌ای بیان می‌کند که میدان‌های رده‌ای با توسیع‌های آبلی معادل اند.

در پایان قرن نوزدهم میلادی سه موضوع در نظریه اعداد منجر به کشف نظریه میدان‌های رده‌ای شد:

- رابطه بین توسیع‌های آبلی و گروه رده‌های ایده‌آلی ،
- قضایای (چگالی) اعداد اول [۲۲] (و تابع - L) [۲۳] و
- قوانین تقابل [۲۴]

برای مطالعه بیشتر درباره نظریه میدان‌های رده‌ای به [۱۶] ، [۱۷] ، [۱۹] ، [۲۰]، [۲۳] و ابتدای بخش دوم [۲۵] رجوع کنید.

با توجه به محدودیت‌های روش های مقدماتی در روند حل مساله ۱ در این بخش با معرفی میدان رده‌ای هیلبرت و نظریه میدان رده‌ای سعی در پاسخ دادن به مساله در کلی‌ترین حالت ممکن داریم.

[19] Class Field Theory
[20] Local extensions
[21] Global extensions
[22] Density Theorems for Primes or Prime Number Theorem
[23] L-Function
[24] Reciprocity Laws

فصل ۷

میدان رده‌ای هیلبرت

ایده هیلبرت درباره توسیع‌های آبلی میدان‌های عددی از طریق مطالعه دقیق سه دسته مثال زیر شکل گرفت:

۱. توسیع‌های مربعی (درجه دوم)

۲. میدان‌های دایره بر

۳. توسیع‌های کومر [۱] میدان‌های دایره بر.

در ادامه این فصل با معرفی مفاهیم مورد نیاز سنگ بنای بررسی میدان رده‌ای هیلبرت را می‌گذاریم و مساله ۱ را برای تعداد نامتناهی n حل می‌کنیم.

۱.۷ نماد و نگاشت آرتین

برای درک دقیق میدان رده‌ای هیلبرت در ابتدا باید نماد آرتین [۲] (فروبینیوس) [۳] و نگاشت آرتین را تعریف کنیم. در ادامه این بخش، از نماد گذاری زیر استفاده می‌کنیم:
توسیع L/K گالوا و آبلی است و $\mathcal{O}_L$ و $\mathcal{O}_K$ به ترتیب حلقه اعداد صحیح جبری L و K اند.
$\mathfrak{p}$ را اولی نامشعب از K و $\mathfrak{P}$ را اولی از $\mathcal{O}_L$ شامل $\mathfrak{p}$ در نظر بگیرید.

$$G_{\mathfrak{P}} = \{\sigma \in Gal(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

$$I_{\mathfrak{P}} = \{\sigma \in Gal(L/K) \mid \forall \alpha \in \mathcal{O}_L : \sigma(\alpha) \overset{\mathfrak{P}}{\equiv} \alpha\}$$

[1] Kummer Extensions of Cyclotomic Fields
[2] Artin
[3] Frobenius

به ترتیب گروه تجزیه و اینرسی $\mathfrak{P}$ در $\mathcal{O}_L$ اند (برای مشاهده جزئیات بیشتر درباره $G_{\mathfrak{P}}$ و $I_{\mathfrak{P}}$ به بخش ۲.۲ رجوع کنید).

با یادآوری جزئیات ذکر شده این بخش را با لم زیر شروع می‌کنیم:

لم ۱.۷. *فرض کنید L/K توسیع گالوا و $\mathfrak{p}$ اولی نامنشعب از $\mathcal{O}_K$ در L است. اگر $\mathfrak{P}$ اولی از L شامل $\mathfrak{p}$ باشد. در این صورت $\sigma \in Gal(L/K)$ به صورت یکتا وجود دارد که برای هر $\alpha \in \mathcal{O}_L$:*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$$

که $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ نرم ایده‌آل $\mathfrak{p}$ است.

قبل از اثبات لم درباره توسیع و گروه گالوای $\tilde{G}$ توضیح می‌دهیم.

$$\tilde{G} = \frac{\mathcal{O}_L/\mathfrak{P}}{\mathcal{O}_K/\mathfrak{p}}$$

نمادگذاری ۲.۷. *میدان $\mathcal{O}_L/\mathfrak{P}$ و $\mathcal{O}_K/\mathfrak{p}$ را از این پس به ترتیب با $\kappa(\mathfrak{P})$ و $\kappa(\mathfrak{p})$ نمایش می‌دهیم.*

لم ۲.۲ را بیاد آورید. می‌خواهیم اثبات کنیم توسیع $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ گالواست.

اثبات. درجه توسیع $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ برابر f (درجه اینرسی) است. اگر $|\kappa(\mathfrak{p})| = p^n$ که p عددی اول و n درجه توسیع L/K باشد؛ داریم:

$$|\kappa(\mathfrak{P})| = p^{nf}.$$

گروه $Aut(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ را در نظر بگیرید، عضوی مانند $\sigma \in Aut(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ وجود دارد که

$$x \longmapsto x^{|\kappa(\mathfrak{p})|}.$$

چون اگر

$$|\kappa(\mathfrak{p})| = q = p^n$$

در این صورت:

$$(xy)^q \equiv x^q y^q \bmod p$$
$$(x+y)^q = x^q + qx^{q-1}y + \ldots + y^q \bmod p$$

می‌دانیم گروه $\kappa(\mathfrak{P})^*$ دوری است. پس عنصری $a \in \kappa(\mathfrak{P})^*$ وجود دارد که از مرتبه $p^{nf} - 1$ است.

عضو $\text{Frob}_{\mathfrak{P}} \in Aut(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ را این گونه تعریف کنید:

$$x \longmapsto x^q$$

آنگاه:

$$\begin{aligned}\text{Frob}_{\mathfrak{P}}(a)^m = a^{q^m} = a &\Leftrightarrow p^{nf} - ۱ \mid p^{mn} - ۱ \\ &\Leftrightarrow f \mid m\end{aligned}$$

بنابراین مرتبه $\text{Frob}_{\mathfrak{P}}$ ، f است.
اندازه گروه خود ریختی‌ها همواره از درجه توسیع کمتر یا مساوی است. در این حالت

$$Aut(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) = |\kappa(\mathfrak{P})/\kappa(\mathfrak{p})|$$

است. بنابراین توسیع $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ گالواست و گروه گالوای این توسیع، دوری و از مرتبه f است. □

در ادامه لم ۱.۷ را اثبات می‌کنیم.

اثبات. چون $\mathfrak{p}$ در L نامنشعب است؛ $e = ۱$ (اندیس انشعاب) خواهد بود. بنابراین $|I_{\mathfrak{P}}| = ۱$ است و طبق گزاره ۱۲.۲ داریم :

$$G_{\mathfrak{P}} \simeq \tilde{G} = Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})).$$

باتوجه به اثبات قبلی می‌دانیم که $\tilde{G} = Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ دوری و توسط مولد $\text{Frob}_{\mathfrak{P}}$ تولید می‌گردد.
برای هر اول $\mathfrak{P}$ ، عضو $\text{Frob}_{\mathfrak{P}} \in G_{\mathfrak{P}}$ به صورت یکتا وجود دارد که:

$$\forall a \in \mathcal{O}_K : \text{Frob}_{\mathfrak{P}}(a) \overset{\mathfrak{p}}{\equiv} a^q$$

یکتایی از یکریختی بین $G_{\mathfrak{P}} \simeq \tilde{G} = Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ نتیجه می‌شود. چون $\text{Frob}_{\mathfrak{P}}(۰) \overset{\mathfrak{p}}{\equiv} ۰$ است. پس $\mathfrak{P} \overset{\mathfrak{p}}{\equiv} \text{Frob}_{\mathfrak{P}}(\mathfrak{P})$ خواهد بود. □

تعریف ۳.۷. *عنصر یکتای σ در لم ۱.۷ را نماد آرتین (فروبینیوس) می‌نامیم و با نماد زیر نمایش می‌دهیم:*

$$\left[\frac{L/K}{\mathfrak{P}}\right]$$

با توجه به لم ۱.۷ برای نماد آرتین داریم:

$$\forall \alpha \in \mathcal{O}_L : \left[\frac{L/K}{\mathfrak{P}}\right](\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P} \qquad (۱.۷)$$

که $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.

نتیجه ۴.۷ (خواص نماد آرتین). *فرض کنید L/K توسیع گالوا و $\mathfrak{p}$ ایده‌آلی اول و نامنشعب از K است. برای ایده‌آل اول $\mathfrak{P}$ در L که شامل $\mathfrak{p}$ است؛ داریم:*

۱. *اگر $\sigma \in Gal(L/K)$ آنگاه :*

$$\left[\frac{L/K}{\sigma(\mathfrak{P})}\right] = \sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1}$$

.

۲. *مرتبه $[(L/K)/\mathfrak{P}]$ برابر درجه اینرسی ($f = f_{\mathfrak{P}|\mathfrak{p}}$) است.*

۳. *$\mathfrak{p}$ در L کاملا شکافته می‌شود $\iff [(L/K)/\mathfrak{P}] = 1$.*

اثبات. برای اثبات به [۷، نتیجه ۲۱.۵.۲] رجوع کنید. □

یادداشت ۵.۷. *برای توسیع گالوای L/K نماد آرتین $[(L/K)/\mathfrak{P}]$ تنها وابسته به ایده‌آل اول $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ است.*

دلیل. *فرض کنید $\mathfrak{P}'$ ایده‌آل اول دیگری در L شامل $\mathfrak{p}$ است. در این صورت با توجه به قضیه ۸.۲ داریم:*

$$\begin{aligned}\exists \sigma \in Gal(L/K) : \mathfrak{P}' = \sigma(\mathfrak{P}) \overset{(۴.۷)}{\Longrightarrow} \left[\frac{L/K}{\mathfrak{P}'}\right] &= \left[\frac{L/K}{\sigma(\mathfrak{P})}\right] \\ &= \sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1} \\ &= \left[\frac{L/K}{\mathfrak{P}}\right]\end{aligned}$$

بنابراین زمانی که توسیع L/K گالواست؛ می‌توان نماد آرتین را وابسته به ایده‌آل $\mathfrak{p}$ نوشت. یعنی:

$$\left[\frac{L/K}{\mathfrak{p}}\right].$$

علاوه بر ایده‌آل‌های اول می‌توان نماد آرتین را برای هر ایده‌آل $\mathfrak{a} \in I_K$ تعریف کرد.

تعریف ۶.۷. *فرض کنید L/K توسیعی آبلی و نامنشعب است. با توجه به توضیحات داده شده درباره نماد آرتین، $\left[\frac{L/K}{\mathfrak{p}}\right]$ برای هر ایده‌آل اول $\mathfrak{p} \in K$ تعریف شده است.*

گزاره ۱۶.۱ را درباره تجزیه یکتا به ایده‌آل‌ها در $\mathcal{O}_K$ به یاد آورید:

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}, \quad \alpha_i \in \mathbb{Z}$$

که $\mathfrak{p}_i$ ها ایده‌آل‌های اول در $\mathcal{O}_K$ اند. در این صورت نماد آرتین $\left[(L/K)/\mathfrak{a}\right]$ ، را به شکل زیر تعریف می‌کنیم:

$$\left[\frac{L/K}{\mathfrak{a}}\right] = \prod_{i=1}^{r} \left[\frac{L/K}{\mathfrak{p}_i}\right]^{\alpha_i}$$

تعریف ۷.۷. با توجه به تعریف نماد آرتین برای ایده‌آل‌های کسری، می‌توان همریختی ای از I_K به گروه گالوای $G = Gal(L/K)$ تعریف کرد.

$$\left[\frac{L/K}{\cdot}\right] : I_K \longrightarrow Gal(L/K)$$

به این همریختی نگاشت آرتین [۴] می‌گوییم.

توجه کنید که اگر L/K توسیعی منشعب باشد؛ نمی‌توان نگاشت آرتین را برای تمامی ایده‌آل‌های I_K تعریف کرد به همین دلیل صورت قضایای اصلی میدان رده‌ای در حالت کلی دارای پیچیدگی هایی اند.

[4] Artin Map

۲.۷ میدان رده‌ای هیلبرت

در این بخش با معرفی میدان رده‌ای هیلبرت [۵] و بیان قضیه تقابل آرتین [۶] برای این دسته از میدان ها ارتباط بین توسیع‌های گالوای آبلی میدان K و $C(\mathcal{O}_K)$ [۷] را شرح می‌دهیم.

قضیه ۸.۷. *برای میدان K ، توسیع گالوای متناهی مانند L وجود دارد که:*

۱. *L توسیع نامنشعب آبلی از K است.*

۲. *هر توسیع نامنشعب آبلی از K در L است (L توسیع نامشعب آبلی ماکسیمال K است).*

اثبات. برای اثبات این قضیه نیارمند معرفی نظریه میدان رده‌ای هستیم. برای مشاهده اثبات به ۲.۳.۸ رجوع کنید. □

تعریف ۹.۷. *میدان L در قضیه قبل را میدان رده‌ای هیلبرت K می‌نامیم.*

قضیه ۱۰.۷ (قضیه تقابل آرتین). *فرض کنید L میدان رده‌ای هیلبرت K است در این صورت نگاشت آرتین پوشاست.*

$$\left[\frac{L/K}{\cdot}\right] : I_K \longrightarrow Gal(L/K)$$

هسته نگاست آرتین دقیقا مجموعه ایده‌آل‌های کسری اصلی (P_K) است. بنابراین نگاشت آرتین یکریختی زیر را القا می‌کند

$$C(\mathcal{O}_K) \xrightarrow{\sim} Gal(L/K).$$

اثبات. اثبات این قضیه یکی از نتایج نظریه میدان رده‌ای است. برای مشاهده اثبات به قضیه ۸.۸ رجوع کنید. □

نتیجه ۱۱.۷ (نظریه میدان رده‌ای برای توسیع های آبلی نامنشعب). *برای میدان عددی K تناظری یک به یک بین توسیع های آبلی نامشعب M/K و زیرگروه‌های، گروه رده‌ای $C(\mathcal{O}_K)$ وجود دارد.*
به علاوه اگر تناظری بین توسیع M/K و $H \subset C(\mathcal{O}_K)$ وجود داشته باشد در این صورت نگاشت آرتین یکریختی زیر را القا می‌کند:

$$C(\mathcal{O}_K)/H \xrightarrow{\sim} Gal(M/K).$$

اثبات. برای اثبات [۳۱، فصل ۴ قضیه ۱.۷] رجوع کنید. □

[5] Hilbert Class Field
[6] Artin Reciprocity Theorem
[۷] گروه رده‌ای میدان K

نتیجه ۱۲.۷. *فرض کنید L میدان رده‌ای هیلبرت K و $\mathfrak{p}$ ایده‌آلی اول از K است. در این صورت:*

$\mathfrak{p}$ در L کاملا شکافته می‌شود $\iff$ $\mathfrak{p}$ ایده‌آل اصلی باشد.

اثبات. برای مشاهده اثبات به [۷، نتیجه ۲۵.۲.۲] رجوع کنید. □

حال به مساله اصلی باز می‌گردیم. هدف ما یافتن اعداد اول p به فرم $x^2 + ny^2$ برای $n > 0$ دلخواه بود. با استفاده از میدان رده‌ای هیلبرت می‌توان جواب سوال را برای دسته نامتناهی از n ها بدست آورد.

قضیه ۱۳.۷. *فرض کنید $K = \mathbb{Q}(\sqrt{-n})$ که $n \in \mathbb{Z}^+$ است. τ را مزدوج مختلط در نظر بگیرید در این صورت برای توسیع گالوای L/K داریم:*

۱. *$\tau(L) = L \iff$ توسیع $L/\mathbb{Q}$ گالوا است.*

۲. *فرض کنید توسیع $L/\mathbb{Q}$ گالوا است. آنگاه:*

$$[L \cap \mathbb{R} : \mathbb{Q}] = [L : K] \quad (آ)$$

(ب) *برای $\alpha \in L \cap \mathbb{R}$:*

$$L \cap \mathbb{R} = \mathbb{Q}(\alpha) \iff L = K(\alpha)$$

اثبات. ۱. فرض کنید $\tau(L) = L$ بنابراین $\tau \in Gal(L/\mathbb{Q})$ است. چون L/K گالواست طبق تعریف ۴.۱ داریم:

$$|Gal(L : K)| = \underbrace{[L : K]}_{:=n}$$

پس:

$$|L/\mathbb{Q}| < \infty \Rightarrow |Gal(L/\mathbb{Q})| \mid [L/\mathbb{Q}] = 2n$$
$$\Rightarrow |Gal(L/\mathbb{Q})| = \begin{cases} [L : \mathbb{Q}] \text{ یا} \\ [L : K] \quad (*) \end{cases}$$

حالت $(*)$ به دلیل این که $\tau(K) \neq K$ است؛ رخ نخواهد داد. پس :

$$|Gal(L/\mathbb{Q})| = [L : \mathbb{Q}].$$

بنابر تعریف ۴.۱ توسیع $L/\mathbb{Q}$ خواهد بود.
برای اثبات مسیر عکس، فرض کنید $L/\mathbb{Q}$ گالواست. هر توسیع جبری $\mathbb{Q}$ ساده است. بنابراین $\alpha \in L$ وجود دارد به طوری که $L = \mathbb{Q}(\alpha)$ شود.

نشاندن‌های L به داخل $\mathbb{C}$ ، α را به دیگر ریشه‌های چندجمله‌ای مینیمالش ($f(x)$) تصویر می‌کند. بدین معنا که:

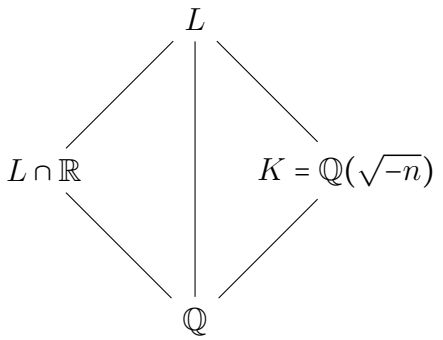
$$\tau(\alpha) \longmapsto \bar{\alpha}$$

که $f(\alpha) = f(\bar{\alpha}) = ۰$ است. چون $L/\mathbb{Q}$ گالواست بنابراین طبق تعریف ۴.۱ ، $\bar{\alpha} \in L$ و در این صورت $\tau(L) \subset L$ است.

با بررسی درجه توسیع L و $\tau(L)$ روی $\mathbb{Q}$ تساوی $\tau(L) = L$ نتیجه می‌شود.

۲. باتوجه به قسمت (۱) می‌دانیم که توسیع $L/\mathbb{Q}$ گالو است اگر و تنها اگر $\tau(L) = L$ باشد. در این صورت گروه ایجاد شده توسط τ از مرتبه ۲ است ($| < \tau > | = ۲$). بنابراین داریم:

(آ) نمودار زیر را در نظر بگیرید:

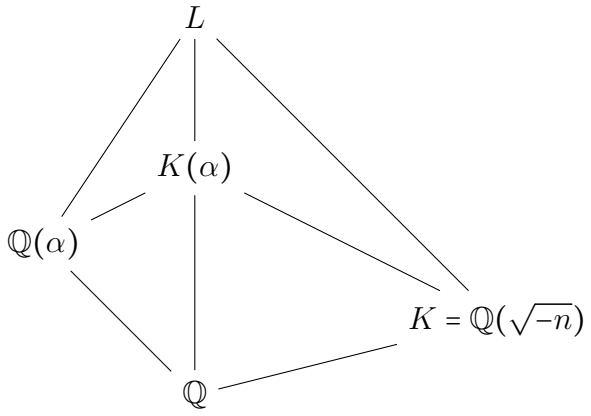


می‌دانیم $[L : L \cap \mathbb{R}] = [L : \mathcal{F}(< \tau >)] = | < \tau > | = ۲$.[۸]

$$[L : \mathbb{Q}] = \begin{cases} \underbrace{[L : L \cap \mathbb{R}]}_{۲}[L \cap \mathbb{R} : \mathbb{Q}] \\ [L : K]\underbrace{[K : \mathbb{Q}]}_{۲} \end{cases} \Rightarrow [L \cap \mathbb{R} : \mathbb{Q}] = [L : K].$$

(ب) برای $\alpha \in L \cap \mathbb{R}$ فرض کنید $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$ در این صورت با استفاده از نمودار زیر داریم:

[۸] $\mathcal{F}(< \tau >)$ را میدان ثابت شده توسط عضو τ در نظر بگیرید.

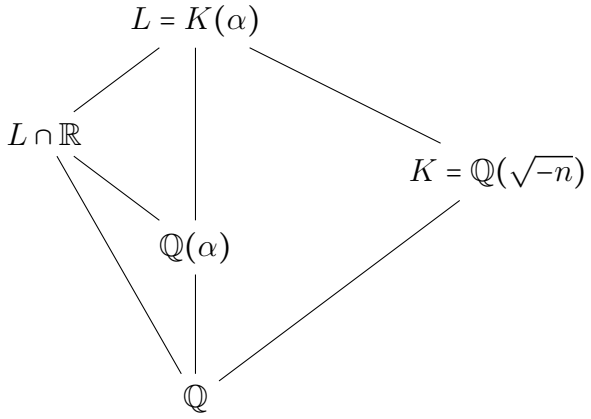


اگر $[L : K] = n$ باشد در این صورت داریم:

$$[L : \mathbb{Q}] = \underbrace{[L : K]}_{n} \cdot \underbrace{[K : \mathbb{Q}]}_{۲} \Rightarrow ۲ \mid [L : K(\alpha)] \Rightarrow \begin{cases} L = K(\alpha) \text{ یا} \\ [L : K(\alpha)] = ۲ \end{cases}$$

اگر $[L : K(\alpha)] = ۲$ باشد؛ چون $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \underbrace{[L : \mathbb{Q}(\alpha)]}_{۲}[\mathbb{Q}(\alpha) : \mathbb{Q}]$ پس $\underbrace{[L : \mathbb{Q}]}_{n}$

$K(\alpha) = \mathbb{Q}(\alpha)$ است.
اما $\sqrt{-n} \notin \mathbb{Q}(\alpha)$. در نتیجه این حالت رخ نخواهد داد و $L = K(\alpha)$ است.
برای اثبات عکس نمودار زیر را در نظر بگیرید:



اگر $[L : K] = n$ باشد در اینصورت داریم:

$$[L : \mathbb{Q}] = \underbrace{[L : K]}_{n}\underbrace{[K : \mathbb{Q}]}_{۲}$$

حال خواهیم داشت:

$$[L:\mathbb{Q}] = ۲n = \underbrace{[L:L\cap\mathbb{R}]}_{۲}[L\cap\mathbb{R}:\mathbb{Q}] \Rightarrow [L\cap\mathbb{R}:\mathbb{Q}] = n$$

$$[L:\mathbb{Q}] = ۲n = \underbrace{[L:\mathbb{Q}(\alpha)]}_{۲}[\mathbb{Q}(\alpha):\mathbb{Q}] \Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] = n$$

پس $L\cap\mathbb{R} = \mathbb{Q}(\alpha)$ خواهد بود.

□

نتیجه ۱۴.۷. *فرض کنید L میدان رده‌ای هیلبرت میدان عددی موهومی $K = \mathbb{Q}(\sqrt{-n})$ است. τ را مزدوج مختلط قرار دهید. در این صورت $\tau(L) = L$ و بنابر قضیه بالا $L/\mathbb{Q}$ گالواست.*

اثبات. چون $\tau(L)$ توسیعی نامنشعب از $\tau(K) = K$ است بنابر تعریف میدان رده‌ای هیلبرت $\tau(L) \subset L$ است. چون درجه توسیع L و $\tau(L)$ روی K برابر است در این صورت $\tau(L) = L$ و بنابر قضیه بالا $L/\mathbb{Q}$ گالوا خواهد بود. □

قضیه ۱۵.۷. *فرض کنید L میدان رده‌ای هیلبرت میدان عددی $K = \mathbb{Q}(\sqrt{-n})$ که n خالی از مربع و $n \overset{۴}{\not\equiv} ۳$ است. آنگاه :*

$$p \text{ در } L \text{ کاملا شکافته شود.} \iff p = x^۲ + ny^۲$$

اثبات. چون $n \overset{۴}{\not\equiv} ۳$ و خالی از مربع است بنابراین $d_K = -۴n$ و $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$ خواهد بود. فرض کنید $p \nmid d_K$ در این صورت p با توجه به نتیجه ۱۷.۲ در K نامنشعب است.

$$\begin{aligned} p + x^۲ + ny^۲ &\overset{(۱)}{\iff} p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}}, \text{ } \mathfrak{p} \text{ در } \mathcal{O}_K \text{ اصلی است} \\ &\overset{(۲)}{\iff} p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}}, \text{ } \mathfrak{p} \text{ در } L \text{ کاملا شکافته می‌شود} \\ &\overset{(۳)}{\iff} p \text{ در } L \text{ کاملا شکافته می‌شود} \end{aligned} \qquad (۲.۷)$$

(۱) • فرض کنید $p = x^۲ + ny^۲$ در این صورت:

$$p = x^۲ + ny^۲ = (x + \sqrt{-n}y)(x - \sqrt{-n}y) \Rightarrow \begin{cases} \mathfrak{p} = (x + \sqrt{-n}y)\mathcal{O}_K \\ \bar{\mathfrak{p}} = (x - \sqrt{-n}y)\mathcal{O}_K \end{cases}$$

چون $\mathfrak{p}$ در K نامنشعب است در این صورت $\mathfrak{p} \neq \bar{\mathfrak{p}}$.

- برای اثبات مسیر عکس فرض کنید $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ که $\mathfrak{p} \neq \bar{\mathfrak{p}}$ و $\mathfrak{p}$ اصلی است. چون $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$ در این صورت

$$\exists x, y \in \mathbb{Z} : \mathfrak{p} = (x + \sqrt{-n}y) \Rightarrow p = (x^2 + ny^2)\mathcal{O}_K \Rightarrow p = x^2 + ny^2.$$

(۲) معادل بودن قسمت (۲) دقیقا صورت نتیجه ۱۲.۷ است.

(۳) اثبات معادل بودن قسمت (۳) از نتیجه ۱۴.۷ و لم ۱۵.۲ نتیجه می‌شود.

□

گزاره ۱۶.۷. *فرض کنید $K = \mathbb{Q}(\sqrt{-n})$ میدان موهومی و L توسیع متناهی از K است که $L/\mathbb{Q}$ گالوا است. آنگاه:*

۱. *عدد جبری $\alpha \in \mathbb{R}$ وجود دارد که $L = K(\alpha)$.*

۲. *$f(x) \in \mathbb{Z}[x]$ را چند جمله‌ای مینیمال α معرفی شده در قسمت (۱) در نظر بگیرید. فرض کنید عدد اول p ، مبین $f(x)$ را عاد نمی‌کند ($p \nmid d(f(x))$) . در این صورت:*

$$p \text{ در } L \text{ کاملا شکافته می‌شود.} \iff \begin{cases} \left(\frac{d_K}{p}\right) = ۱ \\ f_n(x) \overset{p}{\equiv} ۰ \text{ دارای جواب صحیح باشد.} \end{cases}$$

اثبات. برای اثبات به قضیه ۱۳.۷ و [۷، گزاره ۲۹.۵.۲] رجوع کنید. □

قضیه ۱۷.۷. *فرض کنید $n > ۰$ شروط زیر را ارضا می‌کند:*

$$n \text{ خالی از مربع} \quad n \not\equiv ۳ \bmod ۴ \tag{۳.۷}$$

در این صورت چندجمله‌ای تکین و تحویل ناپذیر $f_n(x) \in \mathbb{Z}[x]$ از درجه $h(-۴n)$ وجود دارد که برای هر عدد اول p که n و $d(f_n(x))$ [۹] را عاد نکند؛ داریم:

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{-n}{p}\right) = ۱ \\ f_n(x) \overset{p}{\equiv} ۰ \text{ دارای جواب صحیح باشد.} \end{cases}$$

به علاوه $f_n(x)$ را می‌توان چند جمله‌ای مینیمال عدد جبری حقیقی α در نظر گرفت که $L = K(\alpha)$ میدان رده‌ای $K = \mathbb{Q}(\sqrt{-n})$ است.

[۹] منظور از $d(f_n(x))$ مبین چندجمله‌ای $f_n(x)$ است.

اثبات. اثبات این قضیه از گزاره، لم‌ها و قضایای این بخش نتیجه می‌شود. برای مشاهده جزئیات بیشتر به [۷، ص ۱۰۰] رجوع کنید. □

یادداشت ۱۸.۷. *چند جمله‌ای $f_n(x)$ در قضیه بالا یکتا نیست (تعداد عناصر اولیه α که می‌توانند در شروط قضیه صدق کنند، متعدد است).*
در ادامه مشاهده خواهیم کرد که دانستن چند جمله‌ای $f_n(x)$ در واقع معادل دانستن میدان رده‌ای هیلبرت است.

با توجه به قضیه ۱۷.۷ جواب مساله:

«عدد اول p چه رمانی می‌توان به فرم $x^2 + ny^2$ نمایش داد؟»

برای نامتناهی n که در شرایط (۳.۷) صدق می‌کنند داده می شود.
برای پاسخ دادن به مساله در کلی ترین حالت نیازمند بیان قضایای بیشتری از نظریه میدان رده‌ای هستیم.

۱.۲.۷ $p = x^2 + 14y^2$

قسمت آخر این بخش را به ارائه مثالی از میدان رده‌ای هیلبرت ارائه می‌دهیم. با توجه به قضیه ۱۷.۷ چند جمله‌ای $f_{14}(x)$ وجود دارد به قسمی که:

$$p = x^2 + 14y^2 \iff \begin{cases} \left(\frac{-14}{p}\right) = 1 \\ f_{14}(x) \overset{p}{\equiv} 0 \text{ دارای جواب صحیح باشد.} \end{cases}$$

ولی همان طور که در بخش قبلی اشاره کردیم به دلیل تعدد عناصر اولیه تنها موردی که درباره $f_{14}(x)$ می دانیم اندازه درجه آن است که برابر ۴ است. $K = \mathbb{Q}(\sqrt{-14})$ و با محاسبه گروه رده‌ای داریم :

$$C(\mathcal{O}_K) \simeq \mathbb{Z}/4\mathbb{Z} \Rightarrow |C(\mathcal{O}_K)| = 4$$

. در ادامه برای محاسبه $f_{14}(x)$ از چند لم و گزاره زیر استفاده می‌کنیم:

لم ۱۹.۷. *فرض کنید $L = K(\sqrt{\theta})$ توسیعی درجه دو است که $\theta \in \mathcal{O}_K$. $\mathfrak{p}$ را ایده‌آل اولی از $\mathcal{O}_K$ در نظر بگیرید. آنگاه:*

۱. *اگر $2\theta \notin \mathfrak{p}$ ، در این صورت $\mathfrak{p}$ در L نامنشعب است.*

۲. *اگر $2 \in \mathfrak{p}$ ، $\theta \notin \mathfrak{p}$ و $c \in \mathcal{O}_K$, که $\theta = b^2 - 4ac$ باشد. در این صورت $\mathfrak{p}$ در L نامنشعب است.*

اثبات. برای مشاهده اثبات به [۷، لم ۳۲.۵.۲] رجوع کنید. □

گزاره ۲۰.۷. *میدان رده‌ای هیلبرت میدان* $K = \mathbb{Q}(\sqrt{-۱۴})$ *برابر* $L = K(\alpha)$ *است که*

$$\alpha = \sqrt{۲\sqrt{۲} - ۱}.$$

اثبات. برای مشاهده اثبات به لم ۱۵.۲ و [۷، گزاره ۳۱.۵.۲] رجوع کنید. □

با توجه به موارد ذکر شده می‌توان شرط لازم و کافی برای زمانی که عدد اول p به فرم $x^۲ + ۱۴y^۲$ است ارائه نمود:

قضیه ۲۱.۷. *اگر* $p \neq ۷$ *عدد اول فرد باشد. آنگاه:*

$$p = x^۲ + ۱۴y^۲ \iff \begin{cases} \left(\frac{-۱۴}{p}\right) = ۱ \\ (x^۲ + ۱)^۲ \overset{p}{\equiv} ۸ \text{ دارای جواب صحیح باشد.} \end{cases} \qquad (۴.۷)$$

اثبات. به راحتی می‌توان مشاهده کرد که چند جمله‌ای مینیمال $\alpha = \sqrt{۲\sqrt{۲} - ۱}$ برابر

$$(x^۲ + ۱)^۲ - ۸$$

است. به همین سبب می‌توان آن را به عنوان $f_{۱۴}(x)$ در قضیه ۱۷.۷ انتخاب کرد.
مبین این چند جمله‌ای از فرمول

$$\prod_{۱ \leq i < j \leq ۴} (\theta_i - \theta_j)^۲$$

که $\theta_۱, ..., \theta_۴$ ریشه‌های چند جمله‌ای $f_{۱۴}(x)$ اند؛ بدست می‌آید.
با محاسباتی ساده می‌توان نشان داد که مبین $d(f_{۱۴}(x))$ برابر مقدار زیر است.

$$d(f_{۱۴}(x)) = -۲^{۱۴} \cdot ۷$$

. پس (۴.۷) برای هر عدد اولی به جز $p = ۲, ۷$ کار می‌کند. ادامه اثبات به کمک استفاده از قضیه ۱۷.۷ نتیجه می‌شود. □

تذکر ۲۲.۷. *توجه داشته باشید که در قضیه بالا می‌توان با تغییر عنصر اولیه* α *، و در واقع تغییر مبین چند جمله ای* $f_{۱۴}(x)$ *می‌توان کاری کرد که* $d(f_{۱۴}(x)) \neq ۷$ *در این صورت شرایط* (۴.۷) *را برای* $p = ۷$ *نیز، می‌توان بررسی نمود.*
با استفاده از روش بیان شده در این بخش می‌توان میدان رده‌ای هیلبرت را در دیگر مثال ها نیاز بدست آورد برای مشاهده مثال و جزئیات بیشتر به [۱۸] *و بخش ۴ جزوه* [۴] *رجوع کنید.*

فصل ۸

قضایای اساسی نظریه میدان رده‌ای

این فصل را با معرفی مفهوم هنگ [۱] شروع می‌کنیم. با کلی کردن مفهوم نماد و نگاشت آرتین نسبت به هنگ $\mathfrak{m}$ به بیان سه قضیه مهم در نظریه میدان رده‌ای (قانون تقابل آرتین [۲] ، قضیه وجودی [۳] و قضیه کنداکتور [۴]) می‌پردازیم.

همان گونه که در مقدمه این بخش اشاره کردیم، نظریه میدان رده‌ای روشی برای توصیف توسیع‌های آبلی موضعی و سراسری است.

تیجی تاکاگی [۵] در قضیه وجودی خود بیان می‌کند که هر توسیع آبلی متناهی میدان عددی داده شده K را می‌توان توسط گروه رده‌ای تعمیم یافته‌ای [۶] توصیف کرد.

هم چنین برای هر توسیع آبلی داده شده L/K می‌توان یکریختی زیر را اثبات نمود:

$$Gal(L/K) \simeq I_K(\mathfrak{m})/H_{\mathfrak{m}} \qquad (۱.۸)$$

که $H_{\mathfrak{m}}$ زیر گروه هم نهشتی [۷] وابسته به هنگ $\mathfrak{m}$ و متناظر با توسیع L/K است. اگر چه تاکاگی موفق به ارائه نگاشت صریحی برای یکریختی ذکر شده نشد؛ امیل آرتین [۸] در قضیه تقابل آرتین توانست با معرفی دقیق این نگاشت، زیر گروه هم‌نهشتی $H_{\mathfrak{m}}$ را شناسایی و یکریختی (۱.۸) را اثبات کند.

---

[1] Modulus
[2] Artin Reciprocity Theorem
[3] Existence Theorem
[4] Conductor Theorem
[5] Teiji Takagi
[6] Generalized ideal class group
[7] Congruence Subgroup
[8] Emil Artin

در این فصل ابتدا به بیان قضیه قانون تقابل آرتین، قضیه کنداکتور و قضیه وجودی می‌پردازیم و در انتها با استفاده از قضایای ذکر شده، دو قضیه مهم کرونکر - وبر [9] و میدان رده‌ای هیلبرت را با استفاده از قضایای میدان رده‌ای اثبات می‌کنیم.

۱.۸ مفاهیم اولیه

تعریف ۱.۸. *برای میدان عددی K ، هنگ $\mathfrak{m}$ را که حاصل ضرب صوری روی همه اول‌های (متناهی یا نامتناهی) $\mathfrak{p}$ میدان K است؛ به شکل زیر تعریف می‌کنیم:*

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

که $n_{\mathfrak{p}} \in \mathbb{Z}^{\geq 0}$ در شرایط زیر صدق می‌کند:

۱. $n_{\mathfrak{p}} > 0$ *برای تعداد متناهی $\mathfrak{p}$ رخ می‌دهد.*

۲. $n_{\mathfrak{p}} = 0$ *اگر $\mathfrak{p}$ اول نامتناهی مختلط باشد.*

۳. $n_{\mathfrak{p}} = 1$ *اگر $\mathfrak{p}$ اول نامتناهی حقیقی باشد.*

یادداشت ۲.۸. *هنگ $\mathfrak{m}$ را می‌توان حاصل ضرب $\mathfrak{m}.\mathfrak{m}_\infty$ در نظر گرفت که:*

- *$\mathfrak{m}.$ حاصل ضرب اول‌های متناهی با توان ۱ در $\mathfrak{m}$ است. بنابراین $\mathfrak{m}.$ یک $\mathcal{O}_K$ - ایده‌آل است.*
- *$\mathfrak{m}_\infty$ حاصل‌ضرب اول‌های نامتناهی حقیقی متمایز K است.*

اگر تمامی $n_{\mathfrak{p}}$ ها برابر صفر باشند؛ $\mathfrak{m} = 1$ قرار می‌دهیم.

تذکر ۳.۸. *برای میدان‌های کاملا موهومی (میدان‌هایی که ما بیشتر با آن‌ها سر و کار داریم) هنگ را می‌توان ایده‌آلی از $\mathcal{O}_K$ در نظر گرفت.*

نمادگذاری ۴.۸. *برای هنگ $\mathfrak{m}$ نمادهای زیر را تعریف می‌کنیم:*

- *$I_K(\mathfrak{m})$ را گروه $\mathcal{O}_K$ ایده‌آل‌های کسری نسبت به $\mathfrak{m}.$ می‌نامیم.*
- *$P_{K,1}(\mathfrak{m})$ را زیر گروهی از $I_K(\mathfrak{m})$ در نظر بگیرید که توسط ایده‌آل های اصلی $\alpha\mathcal{O}_K$ که $\alpha \in \mathcal{O}_K$ تولید شده است و α در شرایط زیر صدق می‌کند:*

[9] Kronecker - Weber

۱. $\alpha \equiv 1 \bmod \mathfrak{m}$.

۲. برای هر اول نامتناهی حقیقی که $\mathfrak{m}$. را عاد می‌کند $\sigma(\alpha) > 0$ باشد.

$P_{K,1}(\mathfrak{m})$ را شعاع به پیمانه $\mathfrak{m}$ [10] می‌نامیم.

تعریف ۵.۸. زیر گروه $H \subset I_K(\mathfrak{m})$ را برای هنگ $\mathfrak{m}$ زیر گروه هم‌نهشتی می‌نامیم اگر در شرط

$$P_{K,1}(\mathfrak{m}) \subset H_{\mathfrak{m}} \subset I_K(\mathfrak{m})$$

صدق کند. به گروه خارج قسمتی $I_K(\mathfrak{m})/H_{\mathfrak{m}}$ گروه رده‌ای (ایده‌آلی) تعمیم یافته می‌گوییم.
به طور خاص، به گروه آبلی متناهی $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ [11] گروه رده‌ای شعاعی هنگ $\mathfrak{m}$ [12] می‌گوییم.

مثال ۶.۸. با در نظر گرفتن تعاریف بالا داریم:

۱. اگر $\mathfrak{m} = 1$ باشد؛ در این صورت $P_{K,1}(\mathfrak{m}) = P_K$ زیر گروه هم‌نهشتی است و

$$C(\mathcal{O}_K) = I_K/P_K$$

گروه ایده‌آلی تعمیم یافته است.

۲. فرض کنید $\mathcal{O}$ اردری از کنداکتور f در میدان مربعی موهومی K است. در این صورت با قرار دادن $\mathfrak{m} = f$ داریم:

$$P_{K,1}(f\mathcal{O}_K) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f) = I_K(f\mathcal{O}_K)$$

بنابراین $P_{K,\mathbb{Z}}(f)$ یک زیر گروه هم نهشتی است . با توجه به قضیه ۱۸.۳

$$C(\mathcal{O}) = I_K(f)/P_{K,\mathbb{Z}}(f)$$

پس $C(\mathcal{O})$ نیز یک گروه رده‌ای تعمیم یافته می‌شود.

در بخش ۱.۷ با نماد و نگاشت آرتین آشنا شدیم. برای توسیع گالوای آبلی L/K نماد آرتین را وابسته به ایده‌آل های اول K و با نماد زیر تعریف کردیم.

$$\left[\frac{L/K}{\mathfrak{p}}\right]$$

در ادامه و با استفاده از خاصیت ضربی این نماد و تجزیه یکتای ایده‌آل‌های کسری در $\mathcal{O}_K$ به ایده‌آل‌های اول، نماد آرتین را برای ایده‌آل‌های کسری نیز معرفی کردیم.
حال با استفاده از خاصیت ضربی این نماد و نگاشت را برای هنگ $\mathfrak{m}$ نیز تعریف می‌کنیم.

---

[10] Ray mod $\mathfrak{m}$

[11] گروه $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ متناهی است. برای مشاهده اثبات به نتیجه ۳.۱.۴ [۲۱] رجوع کنید.

[12] Ray Class Group mod $\mathfrak{m}$

تعریف ۷.۸. *فرض کنید توسیع L/K آبلی است و هنگ $\mathfrak{m}$ توسط تمامی اول‌های منشعب شده $\mathfrak{p}$ عاد می‌شود. در این صورت برای اول $\mathfrak{p}$ که $\mathfrak{m}$ را عاد نکند؛ می توان نماد آرتین را مطابق بخش ۱.۷ تعریف کرد.*

$$\left[\frac{L/K}{\mathfrak{p}}\right] \in Gal(L/K)$$

هم چنین مشابه قضیه ۱۰.۷ می‌توان نگاشت آرتین وابسته به توسیع L/K و هنگ $\mathfrak{m}$ را به شکل زیر تعریف کرد:

$$\Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$$

توجه داشته باشید در صورت مشخص بودن توسیع L/K از نماد $\Phi_{\mathfrak{m}}$ به جای $\Phi_{L/K,\mathfrak{m}}$ استفاده می‌کنیم.

۲.۸ سه قضیه اساسی نظریه میدان رده‌ای

همانطور که در ابتدای فصل اشاره کردیم تاکاگی با بیان قضیه وجودی سعی در بیان تناظری بین توسیع‌های آبلی متناهی یک میدان عددی و گروه رده‌ای تعمیم یافته داشت.
در ادامه با بیان قضیه تقابل آرتین و قضیه وجودی این تناظر را به طور دقیق مورد بررسی قرار می‌دهیم. هم چنین با بیان قضیه کنداکتور هنگی یکتا برای هر توسیع آبلی در نظر می‌گیریم.
با بررسی قضیه تقابل آرتین شروع می‌کنیم:

قضیه ۸.۸ (قضیه تقابل آرتین). *فرض کنید L/K توسیعی گالوا و آبلی است. هنگ $\mathfrak{m}$ را در میدان K طوری در نظر بگیرید که توسط تمامی اول‌های K (متناهی و نامتناهی) که در L منشعب می‌شود؛ عاد شود هم چنین توان تمام مقسوم علیه‌های اول $\mathfrak{m}$ به اندازه کافی بزرگ است. در این صورت درباره نگاشت آرتین زیر می‌توان گفت:*

$$\Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$$

۱. $\Phi_{L/K,\mathfrak{m}}$ *پوشاست.*

۲. $\ker(\Phi_{L/K,\mathfrak{m}})$ *زیر گروه هم‌نهشتی برای* $\mathfrak{m}$ *است. یعنی:*

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}}) \subset I_K(\mathfrak{m})$$

و بنابراین یکریختی

$$I_K(\mathfrak{m})/\ker(\Phi_{L/K,\mathfrak{m}}) \xrightarrow{\sim} Gal(L/K)$$

القا می‌شود و $Gal(L/k)$ گروه رده‌ای تعمیم یافته‌ای برای $\mathfrak{m}$ خواهد بود.

اثبات. برای مشاهده اثبات به [۲۱، قضیه ۷.۵.۵] رجوع کنید. □

تناظر آرتین یکی از مهم‌ترین قضایای میدان‌رده‌ای است. این قضیه به زیبایی یک طرف از تناظر بین توسیع‌های آبلی میدان عددی داده شده K و گروه‌های رده‌ای تعمیم یافته را شرح می‌دهد. بدین معنا که برای هنگ $\mathfrak{m}$ می‌توان زیرگروه هم‌نهشتی $H_{\mathfrak{m}}$ را به طور دقیق پیدا کرد به گونه‌ای که یکریختی

$$I_K(\mathfrak{m})/\ker(\Phi_{L/K,\mathfrak{m}}) \xrightarrow{\sim} Gal(L/K)$$

القا شود. این گروه هم‌نهشتی که هسته نگاشت آرتین است را می‌توان به صورت دقیقی توسط تابع نرم

$$N_{L/K} : I_L(\mathfrak{m}) \longrightarrow I_K(\mathfrak{m})$$

شناسایی کرد. بدین معنا که:

$$\ker(\Phi_{\mathfrak{m}}) = P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$$

خواهد بود. برای مطالعه بیشتر به [۲۱، *قضیه ۷.۵.۵*] *رجوع کنید.*
مورد بعدی درباره قضیه تقابل آرتین یکتا نبودن هنگ $\mathfrak{m}$ *است. با توجه به لم زیر برای هر* $\mathfrak{n}$ *که* $\mathfrak{m} \mid \mathfrak{n}$ *می‌توان نشان داد که* $\ker(\Phi_{\mathfrak{n}})$ *زیر گروه هم‌نهشتی است. یعنی:*

$$P_{K,1}(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{n}}) \subset I_K(\mathfrak{n}).$$

و گروه رده‌ای تعمیم یافته وابسته به هنگ $\mathfrak{n}$ *نیز یکریخت با* $Gal(L/K)$ *می‌شود.*

لم ۹.۸. *فرض کنید توسیع* L/K *آبلی است. هنگ* $\mathfrak{m}$ *را طوری در نظر بگیرید که نگاشت آرتین* $\Phi_{\mathfrak{m}}$ *تعریف شود. اگر* $\mathfrak{n}$ *هنگ دیگری برای* K *باشد به طوری که* $\mathfrak{m} \mid \mathfrak{n}$ *در این صورت:*

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}}) \Rightarrow P_{K,1}(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{n}})$$

به علاوه اگر $Gal(L/K)$ *گروه رده‌ای تعمیم یافته برای* $\mathfrak{m}$ *باشد. در این صورت* $Gal(L/K)$ *گروه رده‌ای تعمیم یافته برای* $\mathfrak{n}$ *نیز است.*

اثبات. از آنجایی که نگاشت آرتین برای $\mathfrak{m}$ تعریف شده است و $\mathfrak{m} \mid \mathfrak{n}$ بنابراین هر ایده‌آلی که نسبت به $\mathfrak{n}$ اول باشد نسبت به $\mathfrak{m}$ نیز اول است در این صورت:

$$\Rightarrow I_K(\mathfrak{n}) \subset I_K(\mathfrak{m}).$$

حال می‌توان نگاشت آرتین را برای هنگ $\mathfrak{n}$ از طریق تحدید نگاشت $\Phi_{\mathfrak{m}}$ به مجموعه $I_K(\mathfrak{n})$ تعریف کرد. بنابراین:

$$\Phi_{\mathfrak{m}}|_{I_K(\mathfrak{n})} = \Phi_{\mathfrak{n}} : I_K(\mathfrak{n}) \longrightarrow Gal(L/K)$$

حال اگر $\alpha\mathcal{O}_K \in P_{K,1}(\mathfrak{n})$ باشد؛ در این صورت با توجه به تعریف:

$$\alpha \equiv 1 \bmod \mathfrak{n}., \quad \sigma(\alpha) > 0 \text{ برای هر اول نامتناهی حقیقی } \sigma \mid \mathfrak{n}.$$
$$\xrightarrow{\mathfrak{m}|\mathfrak{n}} \alpha \equiv 1 \bmod \mathfrak{m}., \quad \sigma(\alpha) > 0 \text{ برای هر اول نامتناهی حقیقی } \sigma \mid \mathfrak{m}.$$

با توجه به تعریف نماد آرتین داریم:

$$\begin{aligned}
&\Phi_{\mathfrak{n}}(\alpha\mathcal{O}_K) = \Phi_{\mathfrak{m}}(\alpha\mathcal{O}_K) = 1_{Gal(L/K)} \\
&\Rightarrow P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}}) \\
&\Rightarrow P_{K,1}(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{n}}).
\end{aligned}$$

□

بنابراین هدف در ادامه معرفی هنگی یکتا برای توسیع L/K است. با توجه به لم بالا، ایده یافتن بزرگ‌ترین مضرب مشترک هنگ‌هایی که در شرایط قضیه تقابل آرتین صدق می‌کنند.

قضیه ۱۰.۸ (قضیه کنداکتور). *فرض کنید L/K توسیع آبلی است. در این صورت هنگ $\mathfrak{f} = \mathfrak{f}(L/K)$ وجود دارد به طوری که:*

۱. *یک اول K (متناهی یا نا متناهی) در L منشعب می‌شود اگر و تنها اگر $\mathfrak{p}$ را عاد کند.*

۲. *فرض کنید $\mathfrak{m}$ توسط تمامی اول‌های K که در L منشعب می‌شود، عاد می شود. در این صورت $\ker(\Phi_{L/K,\mathfrak{m}})$ یک زیر گروه هم‌نهشتی برای $\mathfrak{m}$ است اگر و تنها اگر $\mathfrak{f} \mid \mathfrak{m}$.*

اثبات. برای مشاهده اثبات به [۲۱، قضیه ۱۱.۱۱.۵] رجوع کنید. □

بنابر قضیه بالا هنگ $\mathfrak{f}(L/K)$ توسط توسیع L/K به طور یکتا مشخص می‌شود و در واقع کوچک‌ترین هنگی است که یکریختی ذکر شده در قضیه تقابل آرتین (قضیه ۸.۸) را برقرار می‌سازد. $\mathfrak{f}$ را کنداکتور توسیع L/K می‌نامیم.

تاکنون با استفاده از قضیه تقابل آرتین (قضیه ۸.۸) و قضیه کنداکتور (قضیه ۱۰.۸) می‌توان برای توسیع آبلی داده شده L/K اطلاعات زیادی درباره گروه گالوای $Gal(L/K)$ به همراه هنگی یکتا (کنداکتور توسیع) که موجب القای یکریختی بین گروه رده‌ای تعمیم یافته و $Gal(L/K)$ می‌شود؛ داد.
در ادامه سمت دیگر تناظر را اثبات می‌کنیم یعنی برای هر زیر گروه هم‌نهشتی $H_{\mathfrak{m}}$ از هنگ $\mathfrak{m}$ توسیع آبلی L/K را به گونه‌ای پیدا می‌کنیم که گروه رده‌ای تعمیم یافته زیر

$$I_K(\mathfrak{m})/H_{\mathfrak{m}}$$

یکریخت با گروه گالوای $Gal(L/K)$ شود و زیر گروه هم‌نهشتی، هسته نگاشت آرتین $\Phi_{L/K,\mathfrak{m}}$ باشد.

قضیه ۱۱.۸ (قضیه وجودی). *فرض کنید $\mathfrak{m}$ هنگی برای میدان K و $H_{\mathfrak{m}}$ زیر گروه هم‌نهشتی برای $\mathfrak{m}$ است. در این صورت توسیع L/K به صورت یکتا وجود دارد که در شرایط زیر صدق کند:*

۱. *L/K آبلی است.*

۲. *تمامی اول های K (متناهی و نامتناهی) که در L منشعب می‌شوند؛ $\mathfrak{m}$ را عاد می‌کنند به طوری که*

$$\Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$$

نگاشت آرتین L/K و $H_{\mathfrak{m}} = \ker(\Phi_{L/K,\mathfrak{m}})$ است.

اثبات. برای مشاهده اثبات به [۲۱، قضیه ۱۶.۹.۴] رجوع کنید. □

با توجه به قضایای بیان شده می‌توان به راحتی تناظر یک به یک بین گروه‌های رده‌ای تعمیم یافته و توسیع‌های آبلی میدان عددی K را مشاهده کرد.
با توجه به قضیه وجودی برای هنگ $\mathfrak{m}$ ، توسیع یکتای آبلی $K_{\mathfrak{m}}$ از K وجود دارد که

$$P_{K,1}(\mathfrak{m}) = \ker(\Phi_{K_{\mathfrak{m}}/K,\mathfrak{m}})$$

شود.

تعریف ۱۲.۸. *به توسیع آبلی $K_{\mathfrak{m}}$ میدان رده‌ای شعاعی پیمانه $\mathfrak{m}$ [۱۳] می‌گوییم.*

به طور خاص، اگر $\mathfrak{m} = 1$ ، در این صورت $K_{\mathfrak{m}}$ همان میدان رده‌ای هیلبرت که در بخش ۲.۷ تعریف کردیم؛ خواهد بود.

نتیجه ۱۳.۸. *فرض کنید M و L توسیع‌های آبلی از K اند. در این صورت $L \subset M$ است اگر و تنها اگر هنگ $\mathfrak{m}$ به گونه‌ای وجود داشته باشد که توسط تمامی اول‌های K (متناهی و نامتناهی) که در L و M منشعب می‌شود، عاد شود. هم چنین:*

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$$

باشد.

اثبات. برای مشاهده اثبات به [۷، نتیجه ۷.۸.۲] رجوع کنید. □

[13] Ray Class Field mod $\mathfrak{m}$

۳.۸ کاربرد قضایای میدان رده‌ای

در ادامه با استفاده از قضایای میدان رده‌ای دو قضیه بسیار مهم را به زیبایی اثبات می‌کنیم.

۱.۳.۸ قضیه کرونکر - وبر

پیش از بیان و اثبات قضیه کرونکر - وبر در ارتباط با رده بندی کردن تمامی توسیع‌های آبلی میدان $\mathbb{Q}$ نیاز است به بیان چند لم و قضیه درباره میدان‌های دایره بر بپردازیم.
در ادامه فرض کنید $K = \mathbb{Q}(\zeta_m)$ که ζ_m ریشه m - ام اولیه واحد است ($\zeta_m = e^{2\pi i/m}$) . در این صورت حلقه اعداد صحیح جبری K برابر $\mathbb{Z}[\zeta_m]$ خواهد بود (برای مشاهده اثبات به قضیه ۱۳.۹ [۲۲] رجوع کنید) .

لم ۱۴.۸. *فرض کنید $K = \mathbb{Q}(\zeta_m)$ که $\zeta_m = e^{2\pi i/m}$ است. هنگ $\mathfrak{m}$ را برابر m_∞ قرار دهید (∞ اول‌های نامتناهی حقیقی از $\mathbb{Q}$ است) .*
در این صورت نگاشت آرتین Φ_{m_∞} به شکل زیر قابل تعریف است .

$$\Phi_{m_\infty} : I_{\mathbb{Q}}(m_\infty) \longrightarrow Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$$

که برای

$$\frac{a}{b}\mathbb{Z} \in I_{\mathbb{Q}}(m_\infty)$$

به شرطی که $a/b > 0$ و $\gcd(a,m) = \gcd(b,m) = 1$:

$$\Phi_{m_\infty}(\frac{a}{b}\mathbb{Z}) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^*$$

هم چنین داریم:

$$\ker(\Phi_{m_\infty}) = P_{\mathbb{Q},1}(m_\infty)$$

اثبات. با توجه به [۳۰، نتیجه ۱۴.۱۰.۱] هر اول متناهی که در $\mathbb{Q}(\zeta_m)$ منشعب شود؛ m را عاد می‌کند. پس نگاشت Φ_{m_∞} قابل تعریف است. بنابر [۶، قضیه ۵.۲] داریم:

$$Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*.$$

بنابراین می‌توان گفت:

$$\Phi_{m_\infty} : I_{\mathbb{Q}}(m_\infty) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*, \quad p\mathbb{Z} \longmapsto [p]$$

پس

$$\begin{aligned}\frac{a}{b}\mathbb{Z} \in I_{\mathbb{Q}}(m_\infty) \xrightarrow{\Phi_{m_\infty}} \Phi_{m_\infty}(\frac{a}{b}\mathbb{Z}) &= \Phi_{m_\infty}(a\mathbb{Z})\Phi_{m_\infty}(a\mathbb{Z})^{-1} \\ &= [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^*\end{aligned}$$

در ادامه برای اثبات مرحله آخر خواهیم داشت:

$$\frac{a}{b}\mathbb{Z} \in P_{\mathbb{Q},1}(m_\infty) \text{ که } a,b \overset{m}{\equiv} 1 \Rightarrow [a][b]^{-1} = [1] \in (\mathbb{Z}/m\mathbb{Z})^*$$
$$\Rightarrow \frac{a}{b}\mathbb{Z} \in \ker(\Phi_{m_\infty})$$
$$\Rightarrow P_{\mathbb{Q},1}(m_\infty) \subseteq \ker(\Phi_{m_\infty})(*)$$

$$\frac{a}{b}\mathbb{Z} \in \ker(\Phi_{m_\infty}) \Rightarrow [a][b]^{-1} = [1] \in (\mathbb{Z}/m\mathbb{Z})^* \Rightarrow [a] = [b] \in (\mathbb{Z}/m\mathbb{Z})^*$$
$$\Rightarrow a \overset{m}{\equiv} b \overset{\exists d>0}{\Longrightarrow} ad, bd \overset{m}{\equiv} 1 \Rightarrow \frac{a}{b}\mathbb{Z} = \frac{ad}{bd}\mathbb{Z} \Rightarrow \frac{a}{b}\mathbb{Z} \in P_{\mathbb{Q},1}(m)$$
$$\Rightarrow P_{\mathbb{Q},1}(m_\infty) \subseteq \ker(\Phi_{m_\infty})(**)$$
$$(*),(**) \Rightarrow \ker(\Phi_{m_\infty}) = P_{\mathbb{Q},1}(m_\infty)$$

□

قضیه ۱۵.۸ (کرونکر - وبر). *فرض کنید L توسیعی آبلی از $\mathbb{Q}$ است. آنگاه:*

$$\exists m \in \mathbb{Z}^{>0} : L \subset \mathbb{Q}(\zeta_m), \quad \zeta_m = e^{2\pi i/m}.$$

اثبات. بنا بر قضیه تقابل آرتین (قضیه ۸.۸) می‌دانیم هنگ $\mathfrak{m}$ وجود دارد به طوری‌که

$$P_{\mathbb{Q},1}(\mathfrak{m}) \subset \ker(\Phi_L/\mathbb{Q}, \mathfrak{m}).$$

با توجه به لم بالا می‌دانیم با برابر قرار دادن $\mathfrak{m} = m_\infty$ خواهیم داشت:

$$P_{\mathbb{Q},1}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}, \mathfrak{m}) \Rightarrow P_{\mathbb{Q},1}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}, \mathfrak{m}) \subset \ker(\Phi_L/\mathbb{Q}, \mathfrak{m})$$

و با توجه به نتیجه ۱۳.۸ $L \subset \mathbb{Q}(\zeta_m)$ خواهد بود. □

لازم به ذکر است این قضیه بدون استفاده از نظریه میدان رده‌ای نیز اثبات می‌گردد. برای مشاهده جزئیات بیشتر به [۲۷، مسائل ۲۹ - ۳۶ فصل ۴] رجوع کنید.

۲.۳.۸ قضیه میدان رده‌ای هیلبرت

در بخش ۲.۷ مشاهده کردیم که وجود میدان رده‌ای هیلبرت در روند حل مساله ما نقش بسزایی دارند و مساله را برای نامتناهی مقدار n حل می‌کند.
در ادامه با استفاده از نظریه میدان رده‌ای می‌توان وجود میدان رده‌ای هیلبرت را برای میدان عددی K اثبات نمود.

قضیه ۱۶.۸. *برای میدان K ، توسیع گالوای متناهی مانند L وجود دارد که:*

۱. *L توسیع نامنشعب آبلی از K است.*

۲. *هر توسیع نامنشعب آبلی از K در L است (L توسیع نامشعب آبلی ماکسیمال K است).*

اثبات. بخش ۲.۷ و قسمت (۱) مثال ۶.۸ را مرور کنید. به وضوح با مساوی قرار دادن هنگ $\mathfrak{m} = ۱$ و استفاده از قضیه وجودی (قضیه ۱۱.۸) می‌توان گفت که توسیع آبلی یکتای L/K وجود دارد که نامنشعب است (چون $\mathfrak{m} = ۱$ است بنابراین تمامی اول‌های K (متناهی و نامتناهی) در L نامنشعب اند).

هم چنین نگاشت آرتین $\Phi_{L/K,۱}$ یکریختی زیر را القا می‌کند:

$$C(\mathcal{O}_K) = I_K/P_K \xrightarrow{\sim} Gal(L/K)$$

برای تکمیل اثبات، باید نشان دهیم توسیع L ماکسیمال است.

اگر M توسیع نامنشعب آبلی از میدان K باشد؛ بنابر قضیه کنداکتور (قضیه ۱۰.۸) داریم:

$$\mathfrak{f}(M/K) = ۱$$

و $\ker(\Phi_{M/K,۱})$ یک زیر گروه هم‌نهشتی برای هنگ ۱ است.

حال طبق تعریف میدان رده‌ای هیلبرت داریم:

$$P_K = \ker(\Phi_{L/K,۱}) \subset \ker(\Phi_{M/K,۱})$$

با استفاده از نتیجه ۱۳.۸ ، $M \subset L$ خواهد بود. □

فصل ۹

اعداد اول به فرم $p = x^۲ + ny^۲$

فصل آخر...
در این فصل با استفاده از مفاهیم و قضایای بیان شده در فصل قبلی (نظریه میدان رده‌ای) پاسخی کامل به مساله ۱ می‌دهیم.

۱.۹ مفاهیم اولیه

این بخش را با معرفی نماد چگالی دیریشله شروع می‌کنیم. برای میدان عددی K مجموعه $\mathcal{P}_K$ را تمامی اول‌های متناهی میدان K در نظر بگیرید.
حال برای زیر مجموعه $\mathcal{S} \subset \mathcal{P}_K$ چگالی دیریشله را به صورت زیر تعریف می‌کنیم:

$$\delta(\mathcal{S}) = \lim_{s \to ۱^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}}{-\log(s-۱)} \qquad (۱.۹)$$

پیش از بیان خواص چگالی دیریشله، تابع ζ- دیریشله $\zeta_K(s)$ از میدان K را به شکل زیر تعریف می‌کنیم:

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} N(\mathfrak{a})^{-s} = \prod_{\mathfrak{p} \in \mathcal{P}_K} (۱ - N(\mathfrak{p})^{-s})^{-۱} \qquad (۲.۹)$$

لم ۱.۹ (خواص $\zeta_{\mathbf{K}}(\mathbf{s})$). *اگر $Re(s) > ۱$ و $\mathcal{S} \subset \mathcal{P}_K$ باشد. در این صورت:*

- *$\zeta_K(s)$ به صورت یکنواخت همگراست.*
- *$\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}$ به صورت یکنواخت همگرا است.*

- $\zeta_K(s)$ *قطب ساده در* $s = ۱$ *دارد بنابراین:*

$$۱ = \lim_{s\to ۱^+} \frac{\log(\zeta_K(s))}{-\log(s-۱)}$$
$$= \lim_{s\to ۱^+} \frac{\sum_{\mathfrak{p}\in\mathcal{S}} N(\mathfrak{p})^{-s}}{-\log(s-۱)}$$

اثبات. برای مشاهده اثبات به [۳۱، قضیه ۲.۲.۵] رجوع کنید. □

گزاره ۲.۹ (خواص چگالی دیریشله). *فرض کنید* $\mathcal{T},\mathcal{S} \subset \mathcal{P}_K$ *و حد* $\delta(\mathcal{S}),\delta(\mathcal{T})$ *وجود دارند. در این صورت:*

۱. $\delta(\mathcal{P}_K) = ۱$

۲. *اگر* $\mathcal{S} \subset \mathcal{T}$ *باشد. در این صورت* $\delta(\mathcal{S}) \le \delta(\mathcal{T})$ *است.*

۳. $۰ \le \delta(\mathcal{S}) \le ۱$

۴. *اگر* $\mathcal{S}$ *و* $\mathcal{T}$ *دو مجموعه‌ی مجزا باشند. در این صورت* $\delta(\mathcal{S}\cup\mathcal{T}) = \delta(\mathcal{S}) + \delta(\mathcal{T})$ *است.*

۵. *اگر* $\mathcal{S}$ *متناهی باشد. آنگاه* $\delta(\mathcal{S}) = ۰$ *است.*

۶. *اگر دو مجموعه* $\mathcal{S}$ *و* $\mathcal{T}$ *در تعداد متناهی عنصر با یک‌دیگر تمایز داشته باشند. در این صورت* $\delta(\mathcal{S}) = \delta(\mathcal{T})$ *است.*

در ادامه با معرفی مجموعه اول‌های درجه ۱ ارتباطی بین چگالی دیریشله و نماد آرتین برقرار می‌کنیم.

تعریف ۳.۹. *مجموعه زیر را مجموعه اول‌های درجه ۱ در میدان* K *می‌نامیم.*

$$\mathcal{P}_{K,۱} = \{\mathfrak{p} \in \mathcal{P}_K \mid N(\mathfrak{p}) : \text{عددی اول است.}\}$$

حال برای مجموعه $\mathcal{S} \subset \mathcal{P}_K$ *در صورت وجود* $\delta(\mathcal{S})$ *داریم:*

$$\delta(\mathcal{S}) = \delta(\mathcal{S} \cap \mathcal{P}_{K,۱})$$

اگر L/K *توسیع گالوا و* $\mathfrak{p}$ *ایده‌آلی اول و نامنشعب از* K *باشد در نتیجه ۴.۷ ثابت کردیم که برای ایده‌آل اول* $\mathfrak{P}$ *در* L *که شامل* $\mathfrak{p}$ *و عضو* $\sigma \in Gal(L/K)$ *داریم:*

$$\left[\frac{L/K}{\sigma(\mathfrak{P})}\right] = \sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-۱}$$

با توجه به مورد ذکر شده لم زیر را بیان می‌کنیم:

لم ۴.۹. *فرض کنید توسیع L/K گالوا و ایده‌آل اول $\mathfrak{p}$ از میدان K در L نامنشعب است. در این صورت مجموعه*

$$\left\{\left[\frac{L/K}{\mathfrak{P}}\right] \mid \mathfrak{P} \text{ ایده‌آل اولی از } L \text{ شامل } \mathfrak{p} \text{ است.}\right\}$$

یک کلاس تزویجی از $Gal(L/K)$ است.

اثبات. برای هر $\sigma \in Gal(L/K)$ می‌دانیم که با عمل دادن σ روی ایده‌آل‌های اول از L که شامل $\mathfrak{p}$ اند؛ هر کدام را به دیگری تصویر می‌کنیم. با توجه به

$$\left[\frac{L/K}{\sigma(\mathfrak{P})}\right] = \sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1}$$

و تراگذر بودن عمل گروه گالوای $Gal(L/K)$ روی مجموعه اول‌های شامل $\mathfrak{p}$ در L می‌توان نتیجه گرفت که تمامی اعضای مجموعه

$$\left\{\left[\frac{L/K}{\mathfrak{P}}\right] \mid \mathfrak{P} \text{ ایده‌آل اولی از } L \text{ شامل } \mathfrak{p} \text{ است.}\right\}$$

مزدوج یک‌دیگرند و اثبات کامل می‌گردد.

□

در ادامه، به بررسی قضیه چگالی چبوتارف [1] نیاز داریم. بدین منظور نیازمند برقراری ارتباطی بین چگالی دیریشله و نماد آرتین ایم.

فرض کنید توسیع L/K گالوا (ولی نه لزوما آبلی) است. در این صورت برای $\sigma \in Gal(L/K)$ مجموعه $\mathcal{P}_{L/K}(\sigma)$ را به شکل زیر تعریف کنید:

$$\mathcal{P}_{L/K}(\sigma) = \{\mathfrak{p} \in \mathcal{P}_K \mid \left[\frac{L/K}{\mathfrak{P}}\right] = \sigma \text{ و } \mathfrak{P} \in L \text{ نا منشعب و } L \text{ در } \mathfrak{p}\}$$

با توجه به لم ۴.۹ به سادگی می‌توان نتیجه گرفت که برای $\sigma \in Gal(L/K)$ مجموعه $\mathcal{P}_{L/K}(\sigma)$ تنها به کلاس تزویجی $< \sigma >$ وابسته است.

اگر $\tau, \sigma \in Gal(L/K)$ دو عضو متمایز باشند. در این صورت:

$$\mathcal{P}_{L/K}(\sigma) \cap \mathcal{P}_{L/K}(\tau) = \varnothing.$$

در ادامه با بیان قضیه چبوتارف به سوال زیر پاسخ می‌دهیم.

[1] Čebotarev Density Theorem

«چگالی مجموعه $\mathcal{P}_{L/K}(\sigma)$ چقدر است؟»

قضیه ۵.۹ (قضیه چگالی چبوتاروف). *فرض کنید L/K توسیع گالوا و $\sigma > < \sigma$ کلاس مزدوج عضو $\sigma \in Gal(L/K)$ است. در این صورت مجموعه $\mathcal{P}_{L/K}(\sigma)$ دارای چگالی دیریشله*

$$\delta(\mathcal{P}_{L/K}(\sigma)) = \frac{|\langle\sigma\rangle|}{|\mathrm{Gal}(L/K)|} = \frac{|\langle\sigma\rangle|}{[L:K]}$$

است.

اثبات. برای اثبات به [۳۱، قضیه ۴.۶.۵] رجوع کنید. □

توجه کنید که $\delta(\mathcal{P}_{L/K}(\sigma)) > ۰$ است و طبق خواص چگالی دیریشله می‌توان نتیجه گرفت که مجموعه $\mathcal{P}_{L/K}(\sigma)$ نامتناهی است.

با توجه به قضیه چگالی چبوتارف و رفتار نماد آرتین در توسیع های آبلی می‌توان نتیجه زیر را بیان کرد:

نتیجه ۶.۹. *فرض کنید توسیع L/K آبلی است و هنگ $\mathfrak{m}$ توسط تمامی ایده‌آل‌های اول K که در L منشعب می‌شوند؛ عاد شود. در این صورت برای هر $\sigma \in Gal(L/K)$ مجموعه اول‌های $\mathfrak{p}$ که هنگ $\mathfrak{m}$ را عاد نکرد و*

$$\left[\frac{L/K}{\mathfrak{p}}\right] = \sigma$$

شود دارای چگالی $۱/[L:K]$ است و بنابراین نامتناهی است.

یادداشت ۷.۹. *یکی از کاربردهای قضایای چگالی توسیع L/K در ارتباط با ایده‌آل‌های اولی از K است که کاملا در L شکافته می‌شوند.*

بدین معنا که توسیع گالوای L/K را در نظر بگیرید. کلاس تزویجی عضو همانی گروه $Gal(L/K)$ که

$$\left[\frac{L/K}{\mathfrak{p}}\right] = ۱$$

می‌شود دارای چگالی دیریشله

$$\frac{۱}{[L:K]}$$

است.

با توجه به خواص نماد آرتین می‌دانیم $\mathfrak{p}$ در L کاملا شکافته می‌شود اگر و تنها اگر $\left[\frac{L/K}{\mathfrak{P}}\right] = ۱$ باشد [۲].

[۲] برای مشاهده جزئیات بیشتر به ۴.۷ رجوع کنید.

بنابراین تعداد ایده‌آل‌های اول K که در L کاملا شکافته می‌شوند نامتناهی است. چون

$$\frac{1}{[L:K]} > 0$$

است در این صورت بنابر خواص دیریشله نامتناهی بودن نتیجه می‌شود.

نکته جالب درباره ایده‌آل‌های اول K که در L کاملا شکافته می‌شوند این است که این ایده‌ال‌ها توسیع L/K را به طور یکتا مشخص می‌کنند.
برای واضح تر کردن توضیح بیان شده در ارتباط با جمله بالا به مفاهیم زیر احتیاج داریم:

نمادگذاری ۸.۹. دو مجموعه داده شده $\mathcal{S}$ و $\mathcal{T}$ را در نظر بگیرید. در این صورت:

- $\mathcal{S} \dot{\subset} \mathcal{T}$ یعنی:

$$\mathcal{S} \subset \mathcal{T} \cup \sum$$

که $\sum$ مجموعه‌ای متناهی است.

- $\mathcal{S} \doteq \mathcal{T}$ یعنی:

$$\mathcal{S} \dot{\subset} \mathcal{T}, \quad \mathcal{T} \dot{\subset} \mathcal{S}.$$

- فرض کنید توسیع L/K متناهی است در این صورت:

$$\mathcal{S}_{L/K} = \{\mathfrak{p} \in \mathcal{P}_K \mid \mathfrak{p} \text{ در } L \text{ کاملا شکافته شود}\}$$

$$\tilde{\mathcal{S}}_{L/K} = \{\mathfrak{p} \in \mathcal{P}_K \mid f_{\mathfrak{P}|\mathfrak{p}} = 1 \text{ داریم } \mathfrak{P} \text{ برای ایده‌آل اول } \mathfrak{p} \text{ در } L \text{ نامنشعب و}\}$$

با توجه به نماد گذاری بالا می‌توان ارتباطی برای توسیع‌های جبری میدان K بیان کرد.

قضیه ۹.۹. فرض کنید M و L توسیع‌های جبری از میدان K است. آنگاه:

۱. اگر M/K گالوا باشد. در این صورت:

$$L \subset M \iff \mathcal{S}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$$

۲. اگر L روی K گالوا باشد. در این صورت:

$$L \subset M \iff \tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$$

اثبات. برای مشاهده اثبات به [۷، قضیه ۲۰.۸.۲] رجوع کنید. □

با توجه به قضیه بالا به طور خاص می‌توان درباره توسیع‌های گالوای L و M روی میدان K گفت:

نتیجه ۱۰.۹. *فرض کنید فرض کنید M و L توسیع‌های گالوا از میدان K است. آنگاه:*

$$L \subset M \iff \mathcal{S}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$$

و به طور خاص:

$$L = M \iff \mathcal{S}_{M/K} \doteq \mathcal{S}_{L/K}$$

۲.۹ سرانجام مساله ی اصلی

در این بخش با ارائه قضیه ۱۵.۹ به مساله زیر پاسخ کاملی می‌دهیم:
فرض کنید $n \in \mathbb{Z}^{\geq 1}$ داده شده است. در این صورت چه اعداد اولی را می‌توان به صورت

$$p = x^2 + ny^2$$

نمایش داد به طوری که $x, y \in \mathbb{Z}$ باشند؟
برای تعریف مفهوم حلقه میدان رده‌ای نیاز به یادآوری مفاهیم زیر داریم:
برای میدان عددی K مفهومی به نام هنگ $\mathfrak{m}$ را معرفی کردیم (در میدان‌های موهومی می‌توان هنگ را ایده‌آلی از $\mathcal{O}_K$ در نظر گرفت).
گروه های $I_K(\mathfrak{m})$ و $P_{K,1}(\mathfrak{m})$ را از نمادگذاری ۴.۸ به یاد آورید. حال برای اردر $\mathcal{O}$ از کنداکتور $f(f\mathcal{O}_K)$ در میدان موهومی K بنابر قضیه ۱۸.۳

$$C(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$$

خواهد بود. هم چنین با توجه به تعاریف فصل قبل به دلیل شمول زیر $P_{K,\mathbb{Z}}(f)$ یک زیرگروه هم‌نهشتی برای کنداکتور $f(f\mathcal{O}_K)$ است و $C(\mathcal{O})$ گروه رده‌ای تعمیم یافته برای هنگ (ایده‌آل) $f(f\mathcal{O}_K)$ خواهد بود.

$$P_{K,1}(f) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f)$$

قضیه وجودی را به یاد آورید (قضیه ۱۱.۸).
با توجه به این قضیه توسیع آبلی متناهی یکتای L/K برای هنگ $f\mathcal{O}_K$ وجود دارد که تمامی اول‌های K که در L منشعب می‌شوند؛ f را عاد کنند و نگاشت آرتین $\Phi_{L/K,f}$ یکریختی

$$C(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbb{Z}}(f) \simeq Gal(L/K)$$

را القا می‌کند و به طور خاص $[L : K] = h(\mathcal{O})$ است.

تعریف ۱۱.۹. *توسیع آبلی یکتای L را حلقه میدان رده‌ای می‌نامیم.*

قبل از بیان اساسی ترین قضیه این پروژه (قضیه ۱۵.۹) چند لم و گزاره در این راستا بیان می‌کنیم.

لم ۱۲.۹. *فرض کنید $\mathcal{O}$ اردری از کنداکتور f در میدان موهومی K است. میدان L را حلقه میدان رده‌ای اردر L در نظر بگیرید. اگر هنگ $\mathfrak{m} = f\mathcal{O}_K$ و τ مزدوج مختلط باشد؛ داریم:*

۱. $\tau(\mathfrak{m}) = \mathfrak{m}$ و در این صورت $\tau(P_{K,\mathbb{Z}}(f)) = P_{K,\mathbb{Z}}(f)$ است.

۲. $\ker(\Phi_{\tau(L)/K,\mathfrak{m}}) = \tau(\ker(\Phi_{L/K,\mathfrak{m}}))$

۳. *با استفاده از برابر بودن* $\ker(\Phi_{L/K,\mathfrak{m}}) = P_{K,\mathbb{Z}}(f)$ *داریم:*

$$\ker(\Phi_{\tau(L)/K,\mathfrak{m}}) = \ker(\Phi_{L/K,\mathfrak{m}}).$$

گزاره ۱۳.۹. *فرض کنید میدان* L *حلقه میدان رده‌ای اردر* $\mathcal{O}$ *از کنداکتور* $f\mathcal{O}_K$ *در میدان مربعی موهومی* K *است. در این صورت توسیع* $L/\mathbb{Q}$ *گالوا است و گروه گالوای* $Gal(L/\mathbb{Q})$ *را می‌توان به صورت حاصل ضرب نیم‌مستقیم زیر نوشت:*

$$Gal(L/\mathbb{Q}) \simeq Gal(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$$

که عضو نابدیهی $(\mathbb{Z}/2\mathbb{Z})$ *روی گروه* $Gal(L/K)$ *با* $\sigma \mapsto \sigma^{-1}$ *عمل می‌کند.*

اثبات. برای اثبات به [۷، لم ۳.۹.۲] رجوع کنید. □

حال با بیان قضیه زیر شرط لازم و کافی برای نمایش p *به فرم* $x^2 + ny^2$ *را براساس نحوه تجزیه* p *در میدان* L *که حلقه میدان رده‌ای اردر* $\mathbb{Z}[\sqrt{-n}]$ *در میدان مربعی موهومی* $K = \mathbb{Q}(\sqrt{-n})$ *است؛ معادل می‌کنیم.*

قضیه ۱۴.۹. *فرض کنید* L *حلقه میدان رده‌ای اردر* $\mathbb{Z}[\sqrt{-n}]$ *در میدان موهومی* $K = \mathbb{Q}(\sqrt{-n})$ *است. برای عدد اول فرد* p *که* $p \nmid n$ *داریم:*

$$p \iff p = x^2 + ny^2 \text{ در } L \text{ کاملا شکافته شود.}$$

اثبات. مبین میدان K را برابر d_K قرار دهید. مبین اردر $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ برابر $h(-4n) = f^2 d_K$ است که f کنداتور اردر $\mathcal{O}$ است.

$$\begin{cases} p \nmid n \\ h(-4n) = f^2 d_K = -4n \end{cases} \xrightarrow{p \text{ فرد}} p \nmid f^2 d_K \Rightarrow p \text{ در } K \text{ نامنشعب است}$$

با استفاده از گزاره‌های معادل زیر حکم را اثبات می‌کنیم:

$$\begin{aligned} p + x^2 + ny^2 &\overset{(1)}{\iff} p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p} \neq \bar{\mathfrak{p}},\ \mathfrak{p} = \alpha\mathcal{O}_K, \alpha \in \mathcal{O} \\ &\overset{(2)}{\iff} p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p} \neq \bar{\mathfrak{p}},\ \mathfrak{p} \in P_{K,\mathbb{Z}}(f) \\ &\overset{(3)}{\iff} p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p} \neq \bar{\mathfrak{p}},\ \left[\frac{L/K}{\mathfrak{p}}\right] = 1 \qquad (۳.۹) \\ &\overset{(4)}{\iff} p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p} \neq \bar{\mathfrak{p}},\ \mathfrak{p} \text{ در } L \text{ کاملا شکافته می‌شود} \\ &\overset{(5)}{\iff} p \text{ در } L \text{ کاملا شکافته می‌شود} \end{aligned}$$

(۱) • فرض کنید $p = x^۲ + ny^۲$ در این صورت:

$$p = x^۲ + ny^۲ = (x + \sqrt{-n}y)(x - \sqrt{-n}y) \Rightarrow \begin{cases} \mathfrak{p} := (x + \sqrt{-n}y)\mathcal{O}_K \\ \bar{\mathfrak{p}} := (x - \sqrt{-n}y)\mathcal{O}_K \end{cases}$$

چون $\mathfrak{p}$ در K نامنشعب است در این صورت $\mathfrak{p} \neq \bar{\mathfrak{p}}$ و هم چنین $\underbrace{(x + \sqrt{-n}y)}_{:=\alpha\mathcal{O}_K} \in \mathcal{O}$ است.

• برای اثبات مسیر عکس فرض کنید $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ که $\mathfrak{p} \neq \bar{\mathfrak{p}}$ و $\mathfrak{p} = \alpha\mathcal{O}_K$ که $\alpha \in \mathcal{O}$ است. چون $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ در این صورت

$$\exists x, y \in \mathbb{Z} : \mathfrak{p} = (x + \sqrt{-n}y)\mathcal{O}_K \Rightarrow p = x^۲ + ny^۲.$$

(۲) مطابق گزاره ۱۸.۳ می‌دانیم:

$$C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$$

هم چنین $p \nmid f$ در این صورت معادل بودن قسمت (۲) نتیجه می‌شود.

(۳) با توجه به یکریختی القا شده توسط نگاشت آرتین $\Phi_{L/K,f}$ داریم:

$$Gal(L/K) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$$

که $P_{K,\mathbb{Z}}(f) = \ker(\Phi_{L/K,f})$ است. در این صورت معادل بود قسمت (۳) نیز به سادگی نتیجه می‌شود.

(۴) مطابق نتیجه ۱۲.۷ داریم:

$\mathfrak{p}$ در L کاملا شکافته می‌شود $\Longleftrightarrow$ $\mathfrak{p}$ ایده‌آل اصلی باشد.

بنابراین با توجه به قسمت (۳) نیز اثبات نتیجه می‌شود.

(۵) با توجه به گزاره ۱۳.۹ توسیع $L/\mathbb{Q}$ گالوا است. در این صورت بر اساس لم ۱۵.۲ می‌دانیم p در L کاملا شکافته می‌وشد اگر و تنها اگر p در K و ایده‌آل اولی از K شامل p در L کاملا شکافته شود. بنابراین قسمت (۵) نیز اثبات می‌شود.

□

بر اساس گزاره ۱۳.۹ می‌دانیم در صورتی که L حلقه میدان رده‌ای برای اردر $\mathbb{Z}[\sqrt{-n}]$ در میدان مربعی موهومی $K = \mathbb{Q}(\sqrt{-n})$ باشد. توسیع $L/\mathbb{Q}$ گالواست.

در این صورت با استفاده از قضیه ۱۳.۷ می‌توان عدد حقیقی جبری α را به گونه‌ای یافت که: $L = K(\alpha)$.

فرض کنید $f_n(x) \in \mathbb{Z}[x]$ چند جمله‌ای مینیمال α روی K است. در این صورت درجه چند جمله‌ای $f_n(x)$ برابر $[L : K] = h(\mathcal{O})$ است. اکنون بر اساس گزاره ۱۶.۷ می‌دانیم اگر $p \nmid d(f_n(x)), n$ در این صورت خواهیم داشت:

$$p \text{ در } L \text{ کاملا شکافته می‌شود.} \iff \begin{cases} \left(\frac{-n}{p}\right) = ۱ \\ f_n(x) \overset{p}{\equiv} ۰ \text{ دارای جواب صحیح باشد.} \end{cases}$$

بنابراین می‌توان با توجه به تمامی توضیحات بالا قضیه زیر را بیان کرد:

قضیه ۱۵.۹. *فرض کنید $n > ۰$ عددی صحیح است. در این صورت چندجمله‌ای تکین و تجویل ناپذیر $f_n(x) \in \mathbb{Z}[x]$ از درجه $h(-۴n)$ وجود دارد که برای هر عدد اول p که n و $d(f_n(x))$ [۳] را عاد نکند؛ داریم:*

$$p = x^۲ + ny^۲ \iff \begin{cases} \left(\frac{-n}{p}\right) = ۱ \\ f_n(x) \overset{p}{\equiv} ۰ \text{ دارای جواب صحیح باشد.} \end{cases}$$

به علاوه $f_n(x)$ را می‌توان چند جمله‌ای مینیمال عدد جبری حقیقی α در نظر گرفت که $L = K(\alpha)$ حلقه میدان رده‌ای اردر $\mathbb{Z}[\sqrt{-n}]$ در میدان $K = \mathbb{Q}(\sqrt{-n})$ است.

در نهایت، برای هر $f_n(x) \in \mathbb{Z}[x]$ تکین از درجه $h(-۴n)$ که در شرایط بالا صدق کند؛ می‌توان گفت که $f_n(x)$ روی $\mathbb{Z}$ تحویل ناپذیر است. هم چنین $f_n(x)$ چند جمله‌ای مینیمال عنصر اولیه حلقه میدان رده‌ای معرفی شده L است.

اثبات. تمامی قسمت‌های این قضیه بجز قسمت «یکتایی $f_n(x)$» در این بخش اثبات گردیده است.

برای تکمیل اثبات می‌بایست نشان دهیم برای چند جمله‌ای تکین $f_n(x) \in \mathbb{Z}[x]$ از درجه $h(-۴n)$ که در شرایط قضیه صدق کند؛ اگر $g(x) \in K[x]$ عاملی تحویل ناپذیر از $f_n(x)$ باشد؛ $L = M$ خواهد بود.

اگر $M = K(\alpha)$ که α ریشه چند جمله‌ای $g(x)$ باشد.

$$g(x) \mid f_n(x) \Rightarrow \alpha \in L \Rightarrow M = K(\alpha) \subset L$$

[۳] منظور از $d(f_n(x))$ مبین چندجمله‌ای $f_n(x)$ است.

پس باید نشان دهیم که $L \subset M$ است. می‌دانیم $L/\mathbb{Q}$ گالوا است در این صورت طبق گزاره ۹.۹ می دانیم:

$$L \subset M \iff \tilde{\mathcal{S}}_{M/\mathcal{Q}} \doteq \mathcal{S}_{L/\mathcal{Q}} \qquad (۴.۹)$$

بنابراین کافی است ثابت کنیم:

$$\tilde{\mathcal{S}}_{M/\mathbb{Q}} \doteq \mathcal{S}_{L/\mathbb{Q}}$$

برای مشاهده ادامه اثبات به [۷، ص ۱۶۵ - ۱۶۶] رجوع کنید. □

۱.۲.۹ $p = x^۲ + ۲۷y^۲$

برای درک بهتر قضایا و مفاهیم این بخش، مساله نمایش عدد اول p به فرم $x^۲ + ۲۷y^۲$ را حل می‌کنیم. توجه داشته باشید که اگر $n = ۲۷$ باشد. در این صورت مبین فرم برابر ۱۰۸ - است. حال با توجه به الگوریتم‌های بیان شده در بخش دوم می‌توان فرم‌های کاهش یافته از این مبین را یافت.

$$x^۲ + ۲۷y^۲, \quad ۴x^۲ \pm ۲xy + ۷y^۲$$

با بهره‌گیری از ایده‌های مقدماتی می‌توان نشان داد که این سه فرم مربعی هر سه در گونای اصلی اند. بنابراین ایده‌های مقدماتی برای حل مساله کمکی نمی‌کنند.

در ادامه با توجه به شرایط قضیه میدان رده‌ای هیلبرت بر روی عدد n نمی‌توان از قضیه ۱۷.۷ نیز استفاده کرد. به دلیل این که ۲۷ خالی از مربع نیست. حال از قضیه ۱۵.۹ برای حل مساله کمک می‌گیریم.

با توجه به مفاهیم بیان شده می‌دانیم برای یافتن عدد های اولی که به فرم $x^۲ + ۲۷y^۲$ اند؛ می‌بایست حلقه میدان رده‌ای اردر $\mathbb{Z}[\sqrt{-۲۷}]$ را پیدا کنیم.

قضیه زیر حلقه میدان رده‌ای را برای اردر $\mathbb{Z}[\sqrt{-۲۷}]$ بیان می‌کند.

گزاره ۱۶.۹. *حلقه میدان رده‌ای اردر $\mathbb{Z}[\sqrt{-۲۷}]$ در میدان موهومی $K = \mathbb{Q}(\sqrt{-۲۷})$ برابر L است.*

$$L = K(\sqrt[۳]{۲}).$$

اثبات. برای مشاهده اثبات به [۷، گزاره ۵.۹.۲] رجوع کنید. □

در ادامه با یافتن چند جمله‌ای مینمال $f_{۲۷}(x)$ می‌توان قضیه ۱۵.۹ را برای $n = ۲۷$ به شکل زیر بازنویسی کرد:

قضیه ۱۷.۹. *اگر $p > ۳$ عددی اول باشد. آنگاه:*

$$p = x^۲ + ۲۷y^۲ \iff \begin{cases} p \equiv ۱ \bmod ۳ \\ x^۳ \overset{p}{\equiv} ۲ \text{ دارای جواب صحیح باشد.} \end{cases}$$

اثبات. برای مشاهده اثبات به [۷، قضیه ۸.۹.۲] رجوع کنید. □

بخش چهارم

پیوست

فصل ۱۰

گروه رده‌ای و فرم‌های مربعی

در نظریه جبری اعداد و پیشنیازها با مفهوم گروه رده ای و گروه پیکارد آشنا شدیم. در ادامه در بخش روش های مقدماتی با معرفی نظریه فرم‌های مربعی با گروه تولید شده توسط فرم‌های کاهش یافته از مبین D آشنا شدیم. در این بخش ارتباط بین این دو گروه را بیان می‌کنیم.

برای بیان قضیه ارتباط بین گروه رده‌ای ایده‌آلی و گروه رده‌ای فرم‌های کاهش یافته نماد گذاری‌های زیر را بیاد آورید.

قضیه ۱.۱۰. *فرض کنید $\mathcal{O}$ اردر از مبین D در میدان مربعی موهومی K است. در این صورت:*

۱. *اگر $f(x,y) = ax^۲ + bxy + cy^۲$ فرم مثبت معین اولیه از مبین D باشد. آنگاه:*

$$< a, \frac{-b + \sqrt{d_K}}{۲} >$$

ایده‌آل وارون پذیر است.

۲. *نگاشت زیر یکریختی بین $C(\mathcal{O})$ و $C(D)$ القا می‌کند.*

$$f(x,y) \longmapsto < a, \frac{-b + \sqrt{D}}{۲} >$$

۳. *فرض کنید $m \in \mathbb{Z}^+$ است. m توسط $f(x,y)$ به صورت سره نمایش داده می‌شود اگر و تنها اگر m نرم ایده‌آل $\mathfrak{a}$ در کلاس متناظر در $C(\mathcal{O})$ باشد.*

نتیجه ۲.۱۰. *فرض کنید $\mathcal{O}$ اردر در میدان مربعی موهومی K است. برای $M \in \mathbb{Z}^{+۰}$ می‌توان گفت هر کلاس در $C(\mathcal{O})$ شامل $\mathcal{O}$ - ایده‌آل وارون پذیر $\mathfrak{a}$ است که $\gcd(N(\mathfrak{a}), M) = ۱$ باشد.*

اثبات. برای اثبات به نتیجه ۱۷.۷.۲ [۷] رجوع کنید. □

نتیجه ۳.۱۰. *فرض کنید K میدان مربعی موهومی از مبین $d_K < 0$ است. در این صورت:*

۱. *اگر $f(x,y) = ax^2 + bxy + cy^2$ فرم مثبت معین اولیه از مبین d_K باشد. آنگاه:*

$$< a, \frac{-b + \sqrt{d_K}}{2} >$$

یک $\mathcal{O}_K$ - ایده‌آل است.

۲. *نگاشت زیر یکریختی بین $C(\mathcal{O}_K)$ و $C(d_K)$ القا می‌کند.*

$$f(x,y) \longmapsto < a, \frac{-b + \sqrt{d_K}}{2} >$$

فصل ۱۱

اعداد اول به فرم $ax^۲ + bxy + cy^۲$

فرض کنید $f(x,y) = ax^۲ + bxy + cy^۲$ فرم مربعی اولیه مثبت معین از مبین D است. در ادامه نشان خواهیم داد که این فرم نامتناهی عدد اول را نمایش می‌دهد.

ایده اصلی بررسی چگالی دیریشله اعداد اولی است که توسط f نمایش داده می‌شوند. زمانی که نشان دهیم این چگالی مثبت است، با استفاده از خواص چگالی دیریشله ثابت خواهد شد که تعداد اعداد اولی که توسط f نمایش داده می‌شود نامتناهی است.

قضیه زیر به طور دقیق توضیحات بالا را خلاصه می‌کند:

قضیه ۱.۱۱. *فرض کنید $f(x,y) = ax^۲ + bxy + cy^۲$ فرم مربعی اولیه مثبت معین از مبین $D < ۰$ است. $\mathcal{S}$ را برابر مجموعه اعداد اول نمایش داده شده توسط f قرار دهید. در این صورت چگالی دیریشله $\delta(\mathcal{S})$ وجود دارد و از طریق روابط زیر بدست می‌آید.*

$$\delta(\mathcal{S}) = \begin{cases} \frac{۱}{۲h(D)} & \text{اگر } f \text{ به صورت سره با وارونش معادل باشد.} \\ \frac{۱}{h(D)} & \text{در غیر این صورت} \end{cases} \qquad (۱.۱۱)$$

پیش از اثبات این قضیه، قضیه زیر را بررسی می‌کنیم:

قضیه ۲.۱۱. *فرض کنید H آبلی و $G = H \rtimes \mathbb{Z}/۲\mathbb{Z}$ است؛ به طوری که $۱ \in \mathbb{Z}/۲\mathbb{Z}$ روی گروه H به شکل $h = h^{-۱}$ عمل می‌کند. در این صورت کلاس تزویجی در G برای هر $h \in H$ برابر $\{h, h^{-۱}\}$ است؛ عنصر $h \in H$ را با استفاده از تصویر $(h, ۰) \in G$ شناسایی می‌کنیم.*

اثبات. هر عنصر $g \in G$ را می‌توان به صورت یکتا به شکل (h, a) نمایش داد به طوری که $h \in H$ و $a \in \mathbb{Z}/۲\mathbb{Z}$ است.

با توجه به خواص نیم ضرب مستقیم می‌دانیم برای دو عنصر زیر

$$(h_۱, a_۱), (h_۲, a_۲) \in G = H \rtimes \mathbb{Z}/۲\mathbb{Z}$$

ضرب به شکل زیر تعریف می‌گردد:

$$(h_۱, a_۱) \cdot (h_۲, a_۲) = (h_۱(a_۱ \cdot h_۲), a_۱ + a_۲)$$

می‌دانیم $(h, ۰)^{-۱} = (h^{-۱}, ۰)$ و از آنجایی که

$$(h, ۱)(h, ۱) = (h(۱ \cdot h), ۰) = (hh^{-۱}) = (۱, ۰)$$

داریم:

$$(h, ۱)^{-۱} = (h, ۱)$$

بنابراین برای $h = (h, ۰) \in H \subset G$ و $k \in H$ با توجه به آبلی بودن H خواهیم داشت:

$$(k, ۰)h(k, ۰)^{-۱} = (k, ۰)(h, ۰)(k^{-۱}, ۰) = (kh, ۰)(k^{-۱}, ۰) = (khk^{-۱}, ۰) = (h, ۰) = h$$

$$(k, ۱)h(k, ۱)^{-۱} = (k, ۱)(h, ۰)(k, ۱) = (kh^{-۱}k^{-۱}, ۰) = (h^{-۱}, ۰) = h^{-۱}$$

بنابراین کلاس تزویجی h برابر $\{h, h^{-۱}\}$ است. □

در ادامه به بررسی اثبات قضیه ۱.۱۱ می‌پردازیم:

اثبات. فرض کنید $\mathcal{O}$ اردر جبری از مبین D و $K = \mathbb{Q}(\sqrt{D})$ است. می‌دانیم $D = f^۲ d_K$ است که f کنداکتور میدان K و d_K مبین میدان است.
مطابق صورت قضیه مجموعه $\mathcal{S}$ را به شکل زیر تعریف می‌کنیم:

$$\mathcal{S} = \{\text{اول } p : p = ax^۲ + bxy + cy^۲\}$$

در این صورت هدف محاسبه چگالی دیریشله مجموعه $\mathcal{S}$ است.
اثبات در چندین گام صورت می‌گیرد.

ابتدا مجموعه $\mathcal{S}$ را به گروه رده‌ای تعمیم یافته $I_K(f)/P_{K,\mathbb{Z}}$ نسبت می‌دهیم. با توجه به قضیه ۱.۱۰ داریم:

$$C(\mathcal{O}) \simeq C(D)$$

بنابراین کلاس $[ax^۲ + bxy + cy^۲] \in C(D)$ متناظر ایده‌آل $\mathfrak{a}. \in C(\mathcal{O})$ است به طوری که $\mathfrak{a}.$ یک $\mathcal{O}$ ـ‌ایده‌آل وارون پذیر است.
بنابراین، طبق قسمت سوم قضیه ۱.۱۰ داریم:

$$\mathcal{S} = \{\text{اول } p : p = N(\mathfrak{b}), \mathfrak{b} \in [\mathfrak{a}.])\}$$

گام بعدی در روند اثبات بازنویسی مجموعه $\mathcal{S}$ بر اساس اردر ماکسیمال یا $\mathcal{O}_K$ است.
بنابر گزاره ۱۷.۳ می‌توان ایده‌آل $\mathfrak{a}.$ را نسبت به کنداکتور f اول فرض کرد. در ادامه تنها اول‌هایی مانند p را در نظر می‌گیریم که کنداکتور را عاد نکنند.

مطابق تناظر بیان شده در گزاره ۱۷.۳ و گزاره ۱۸.۳ خواهیم داشت:

$$\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K \Rightarrow \mathfrak{b} \in [\mathfrak{a}.] \in C(\mathcal{O}) \mapsto \mathfrak{b}\mathcal{O}_K \in [\mathfrak{a}.\mathcal{O}_K] \in I_K(f)/P_{K,\mathbb{Z}}(f)$$

براساس گزاره ۱۷.۳ می‌دانیم $\mathfrak{b}$ و $\tilde{\mathfrak{b}} = \mathfrak{b}\mathcal{O}_K$ چون نسبت به f اول اند؛ دارای نرم‌های یکسانی اند.
بنابراین می‌توان محموعه $\mathcal{S}$ را به شکل زیر بازنویسی کرد:

$$\mathcal{S} \doteq \{\text{اول } p : p \nmid f, p = N(\tilde{\mathfrak{b}}), \tilde{\mathfrak{b}} \in [\mathfrak{a}.\mathcal{O}_K]\}$$

با توجه به اول بودن p، ایده‌آل $\tilde{\mathfrak{b}}$ نیز اول خواهد بود. بنابراین مجموعه $\mathcal{S}$ را می‌توان به شکل زیر بازنویسی کرد:

$$\mathcal{S} \doteq \{\text{اول } p : p \nmid f, p = N(\mathfrak{b}), \text{اول } \mathfrak{p}, \mathfrak{p} \in [\mathfrak{a}.\mathcal{O}_K]\}$$

حال اگر L حلقه میدان رده‌ای اردر $\mathcal{O}$ باشد؛ بنابر تقابل آرتین یکریختی زیر برقرار است:

$$I_K(f)/P_{K,\mathbb{Z}}(f) \simeq Gal(L/K)$$

با توجه به یکریختی بالا کلاس $\mathfrak{a}.\mathcal{O}_K$ به عضو $\sigma. \in Gal(L/K)$ تصویر می‌شود.
بدون کاستن از کلیت و باتوجه به گالوا بودن توسیع $L/\mathbb{Q}$ می‌توان $\sigma.$ را عضوی از $Gal(L/\mathbb{Q})$ نیز در نظر گرفت.
اگر $<\sigma.>$ کلاس تزویجی این عضو در گروه $Gal(L/\mathbb{Q})$ باشد؛ ادعا می‌کنیم که مجموعه $\mathcal{S}$ را می‌توان به شکل زیر بازنویسی کرد:

$$\mathcal{S} \doteq \{\text{اول } p : L \text{ در نامنشعب } p, \left[\frac{L/\mathbb{Q}}{p}\right] = <\sigma.>\}$$

برای اثبات ادعا قرار دهید:

$$\mathcal{R} = \{\text{اول } p : L \text{ در نامنشعب } p, \left[\frac{L/\mathbb{Q}}{p}\right] = <\sigma.>\}$$

در این صورت هدف نسان دادن $\mathcal{S} \doteq \mathcal{R}$ است.
ابتدا اثبات می‌کنیم که $\mathcal{R} \dot{\subset} \mathcal{S}$ است.
فرض کنید $p \in \mathcal{R}$ در این صورت برای ایده‌آل اول $\mathfrak{P}$ در L که شامل p است؛ داریم:

$$\left[\frac{L/\mathbb{Q}}{p}\right] = <\sigma.> \Rightarrow \left[\frac{L/\mathbb{Q}}{\mathfrak{P}}\right] = <\sigma.>$$

ایده‌آل $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ ایده‌آل اولی از K شامل p است که $p = N(\mathfrak{p})$ است.
چون برای هر $\alpha \in \mathcal{O}_L$ ، $\sigma. = [(L/\mathbb{Q})/\mathfrak{P}]$ است. بنابراین:

$$\sigma.(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}$$

از آنجایی که $\sigma_{\mathfrak{a}} \in Gal(L/K)$ نیز است. می‌توان برای هر $\alpha \in \mathcal{O}_K$ هم‌نهشتی بالا را مجددا به شکل زیر بازنویسی نمود:

$$\alpha \equiv \alpha^p \pmod{\mathfrak{p}}$$

با توجه به هم نهشتی بالا می‌توان گفت:

$$\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z} \Longrightarrow N(\mathfrak{p}) = p.$$

پس $\sigma_{\mathfrak{a}}$ نماد آرتین $[(L/K)/\mathfrak{p}]$ است.
با توجه به یکریختی القا شده توسط نگاشت آرتین بین $I_K(f)/P_{K,\mathbb{Z}}$ و $Gal(L/K)$ و تناظر بین $[\mathfrak{a}.\mathcal{O}_K]$ و $\sigma_{\mathfrak{a}}$ می‌توان گفت که $\mathfrak{p}$ در کلاس $[\mathfrak{a}.\mathcal{O}_K]$ است و بنابراین $p \in \mathcal{S}$ است .
در ادامه می‌خواهیم نشان دهیم که $\mathcal{S} \dot{\subset} \mathcal{R}$ است.
برای این منظور کافی است نشان دهیم:

$$\{p \text{ اول} : p \nmid f, p = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \in [\mathfrak{a}.\mathcal{O}_K]\} \dot{\subset} \mathcal{R}$$

عدد اول p را برای $[\mathfrak{a}.\mathcal{O}_K] \in I_K(f)/P_{K,\mathbb{Z}} \simeq C(\mathcal{O})$ به گونه ای انتخاب کنید که $p \nmid f$ و $p = \mathfrak{p}\bar{\mathfrak{p}} = N(\mathfrak{p})$ برقرار باشد.
در این صورت با توجه به یکریختی $C(\mathcal{O}) \simeq Gal(L/K)$، کلاس $[\mathfrak{a}.]$ به $\sigma_{\mathfrak{a}} \in Gal(L/K)$ تصویر می‌شود.
بدون کاستن از کلیت می‌توان فرض کرد که عدد اول p در L نامنشعب است (تعداد متناهی از اول‌های K در L منشعب می‌شوند).
ایده‌آل اول $\mathfrak{P} \in \mathcal{O}_L$ را شامل ایده‌آل $\mathfrak{p}$ در نظر بگیرید. چون $N(\mathfrak{p}) = p$ طبق تعریف نماد آرتین برای هر $\alpha \in \mathcal{O}_L$ خواهیم داشت:

$$\left[\frac{L/K}{\mathfrak{P}}\right](\alpha) \equiv \alpha^{N(\mathfrak{p})} \equiv \alpha^p \pmod{\mathfrak{P}}$$

با توجه به این که $\mathfrak{p} \in [\mathfrak{a}.\mathcal{O}_K]$ پس $\sigma_{\mathfrak{a}} = [(L/K)/\mathfrak{P}]$.
با استفاده از همین استدلال داریم:

$$\left[\frac{L/\mathbb{Q}}{\mathfrak{P}}\right](\alpha) \equiv \alpha^{N_{\mathbb{Q}/\mathbb{Q}}(\mathfrak{p})} \equiv \alpha^p \pmod{\mathfrak{P}}$$

بنابراین:

$$\left[\frac{L/\mathbb{Q}}{\mathfrak{P}}\right] = \left[\frac{L/K}{\mathfrak{P}}\right] = \sigma_{\mathfrak{a}}$$

که $\sigma_{\mathfrak{a}}$ عضوی از $Gal(L/K)$ و $Gal(L/\mathbb{Q})$ است.

عوض کردن $\mathfrak{P}$ با $\sigma(\mathfrak{P})$ برای $\sigma \in Gal(L/K)$ عناصر کلاس تزویجی $< \sigma. >$ را می‌دهد. بنابراین:

$$\left[\frac{L/\mathbb{Q}}{p}\right] =< \sigma. > \Longrightarrow p \in \mathcal{R} \Longrightarrow \mathcal{S} \dot{\subset} \mathcal{R}$$

بنابر قضیه چگالی چبوتارف، چگالی مجموعه $\mathcal{S}$ را می‌توان به از طریق رابطه زیر بدست آورد:

$$\delta(\mathcal{S}) = \frac{|< \sigma. >|}{[L : \mathbb{Q}]}$$

با توجه به گزاره ۱۳.۹ و قضیه ۲.۱۱ می‌توان گفت:

$$< \sigma. >= \{\sigma., \sigma_.^{-1}\}.$$

چون $[L : \mathbb{Q}] = 2h(D)$ داریم:

$$\delta(\mathcal{S}) = \begin{cases} \frac{1}{2h(D)} & \text{اگر } \sigma. \text{ دارای مرتبه } \geq 2 \\ \frac{1}{h(D)} & \text{در غیر این صورت} \end{cases} \qquad (2.11)$$

با توجه به مطالب بالا مرتبه $\sigma. \geq 2$ است اگر و تنها اگر مرتبه فرم مربعی $ax^2 + bxy + cy^2 \geq 2$ باشد.

با توجه به قضایای فرم‌های مربعی می‌دانیم مرتبه یک فرم ≥ 2 است اگر و تنها اگر با وارونش به صورت سره معادل باشد.

بنابراین اثبات کامل می‌شود. □

فصل ۱۲

تقابل ضعیف و قوی

همانطور که در بخش‌های قبلی بیان شد، نظریه میدان رده‌ای یکی از مهم ترین شاخه‌های نظریه جبری اعداد است که با به کار گیری آن می‌توان قضایای مهمی از جمله قضیه کرونکر- وبر و وجود میدان رده‌ای هیلبرت، را اثبات نمود.

در این بخش با بیان قضایای تقابل ضعیف [۱] و تقابل قوی [۲] نقش مهم نظریه میدان رده‌ای را در شکل گیری این دو قضیه بررسی می‌کنیم.

۱.۱۲ مفاهیم اولیه

در این فصل به بررسی قوانین تقابل برای نماد لژاندار از مرتبه n می‌پردازیم که با نماد زیر نشان می‌دهیم (در نظریه مقدماتی اعداد با نماد لژاندر از مرتبه دوم آشنا شدیم) .

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n$$

ابتدا با یادآوری مفاهیم مانده و نامانده مربعی در پیمانه عدد اول p تعریف نماد لژاندر (از مرتبه ۲) را مرور می‌کنیم.

یادآوری ۱.۱۲ (مانده و نامانده مربعی)**.** *p عددی اول و فرد و a عدد صحیح و نسبت به p اول است. اگر معادله هم‌نهشتی $x^2 \overset{p}{\equiv} a$ جواب داشته باشد، آنگاه عدد a در پیمانه p مانده مربعی و در غیر این‌صورت نامانده مربعی می‌گوییم.*

حال تعریف نماد لژاندر از مرتبه دو را مجددا بیان می‌کنیم:

[1] Weak Reciprocity
[2] Strong Reciprocity

یادآوری ۲.۱۲ (نماد لژاندر (مرتبه ۲))**.** *اگر p عدد اول و فرد و a عدد صحیح باشد که $\gcd(a,p)=1$ است. در این صورت تابع لژاندر را با نماد زیر تعریف می‌کنیم:*

$$\left(\frac{a}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow \{\pm 1\}$$

که

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{اگر } a \text{ در پیمانه } p \text{ مانده مربعی باشد.} \\ -1 & \text{در غیر این صورت} \end{cases}$$

در ادامه نماد $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ را تعریف می‌کنیم.

فرض کنید K میدان عددی شامل $\zeta = e^{\frac{2\pi i}{n}}$ (nـامین ریشه اولیه واحد) است. $\mathfrak{p}$ را ایده‌آل اولی از $\mathcal{O}_K$ در نظر بگیرید. در این صورت برای هر $\alpha \in \mathcal{O}_K$ که نسبت به ایده‌آل $\mathfrak{p}$ اول باشد؛ طبق قضیه کوچک فرما خواهیم داشت:

$$\alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$$

هم چنین لم زیر نیز برقرار است.

لم ۳.۱۲. *فرض کنید K میدان عددی شامل ζ ، n ـامین ریشه اولیه واحد است. اگر $a \in \mathcal{O}_K$ و $\mathfrak{p}$ ایده‌آل اولی از $\mathcal{O}_K$ باشد؛ به طوری‌که $na \notin \mathfrak{p}$. در این صورت موارد زیر برقرار است:*

۱. *$1, \zeta, ..., \zeta^{n-1}$ در پیمانه $\mathfrak{p}$ متمایزند.*

۲. $n \mid N(\mathfrak{p}) - 1$.

۳. *$a^{(N(\mathfrak{p})-1)/n}$ در پیمانه $\mathfrak{p}$ همنهشت تنها یکی از nـامین ریشه اولیه واحد است.*

اثبات. ۱. با توجه به این‌که $n \notin \mathfrak{p}$ است؛ پس دو چندجمله $f(x) = x^n - 1$ و $f'(x) = nx^{n-1}$ در پیمانه $\mathfrak{p}$ صفر نخواهند بود. بنابراین چندجمله‌ای $f(x)$ در پیمانه $\mathfrak{p}$ جدایی پذیر است.

با توجه به این‌که چند جمله ای مینمال nـامین ریشه‌های اولیه واحد، $p(x)$، $f(x)$ را عاد می‌کند؛ می‌توان گفت که $p(x)$ نیز جدایی پذیر بوده و به همین دلیل ریشه‌های $p(x)$ ($1, \zeta, ..., \zeta^{n-1}$) در پیمانه $\mathfrak{p}$ متمایزند.

۲. طبق قسمت قبل می‌دانیم $1, \zeta, ..., \zeta^{n-1}$ در پیمانه $\mathfrak{p}$ متمایزند؛ این ریشه ها در پیمانه $\mathfrak{p}$ تشکیل گروهی ضربی می‌دهند؛ نام این گروه را H بنامید. به وضوح H زیر گروهی از $(\mathcal{O}_K/\mathfrak{p})^*$ است. باتوجه به قضیه لاگرانژ در ارتباط با اندازه زیرگروه‌ها داریم:

$$|H| \mid |(\mathcal{O}_K/\mathfrak{p})^*| \Rightarrow n \mid N(\mathfrak{p}) - 1$$

۳. اثبات این قسمت باتوجه به دو قسمت قبلی بدیهی است. توجه داشته باشید که a ریشه‌ای برای چندجمله‌ای $x^n - ۱$ خواهد بود.

□

حال با استفاده از یکتایی قسمت سوم در لم بالا می‌توان نماد لژاندر از مرتبه n را تعریف کرد.

تعریف ۴.۱۲. *فرض کنید K میدان عددی شامل n- امین ریشه اولیه واحد، ζ است. $\mathfrak{p}$ را ایده‌آل اولی از $\mathcal{O}_K$ در نظر بگیرید که برای عضو $a \in \mathcal{O}_K$ ، $na \notin \mathfrak{p}$ باشد. در این صورت مطابق لم ۳.۱۲*

$$\exists! i \in \{۰, ..., n-۱\} : a^{\frac{N(\mathfrak{p})-۱}{n}} \equiv \zeta^i \pmod{\mathfrak{p}}$$

حال نماد لژاندر از مرتبه n را به شکل زیر تعریف می‌کنیم:

$$a^{\frac{N(\mathfrak{p})-۱}{n}} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}}$$

با توجه به لم ۳.۱۲ و تعریف بالا، نتیجه زیر برقرار است:

نتیجه ۵.۱۲. *$\left(\frac{a}{\mathfrak{p}}\right)_n = ۱$ اگر و تنها اگر a ، مانده توانی [3] از مرتبه n در پیمانه $\mathfrak{p}$ باشد.*

اثبات. اثبات این نتیجه با در نظر گرفتن لم ۳.۱۲ بدیهی است. □

با توجه به تعریف بالا و یکتایی تجزیه ایده‌آل‌ها به ایده‌آل‌های اول در $\mathcal{O}_K$ می‌توان نماد لژاندر از مرتبه n را برای ایده‌آل $\mathfrak{a}$ از $\mathcal{O}_K$ نیز تعریف کرد.
بدین معنا که اگر تجزیه ایده‌آل $\mathfrak{a}$ در $\mathcal{O}_K$ برابر $\mathfrak{a} = \mathfrak{p}_۱ ... \mathfrak{p}_r$ باشد که $\mathfrak{p}_i$ ها ایده‌آل‌های اول در $\mathcal{O}_K$ اند. داریم:

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n = \prod_{i=۱}^{r} \left(\frac{\alpha}{\mathfrak{p}_i}\right)_n$$

در ادامه فرض کنید هنگ $\mathfrak{m}$ از میدان K و $\alpha \in \mathcal{O}_K$ است؛ که هر اول $\mathfrak{p}$ با شرط $n\alpha \in \mathfrak{p}$ هنگ $\mathfrak{m}$ را عاد کند، $\mathfrak{p} \mid \mathfrak{m}$.
در این صورت نماد لژاندر از مرتبه n همریختی گروهی زیر را القا می‌کند:

$$\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m}) \longrightarrow \mu_n$$

که $\mu_n \subset \mathbb{C}^*$ گروه شامل nـامین ریشه‌های اولیه واحد است.

[3] Power Residue

۲.۱۲ قضایای تقابل ضعیف و قوی

در ادامه این فصل قضایای تقابل ضعیف و قوی را مورد بررسی قرار می‌دهیم. قبل از بررسی قضایای ذکر شده نیازمند بررسی قضیه زیر از نظریه گالوا هستیم.

قضیه ۶.۱۲. *فرض کنید K میدان عددی شامل n- امین ریشه اولیه واحد است. در این صورت برای هر $\alpha \in K$ توسیع میدان $K \subset L = K(\sqrt[n]{\alpha})$ گالواست.*
به علاوه برای هر $\sigma \in Gal(L/K)$ داریم:

$$\sigma(\sqrt[n]{\alpha}) = \zeta \sqrt[n]{\alpha}$$

که ζ یکی از n- امین ریشه اولیه واحد است.

اثبات. اثبات با استفاده از مفاهیم نظریه گالوا بدیهی است. برای اثبات کافی است به چند جمله‌ای مینمال α دقت کنید، میدان شکافنده این چند جمله‌ای برابر L خواهد بود(توجه داشته باشید که توسیع L/K، توسیعی نرمال و جدایی پذیر است).
هم‌چنین چون هر یک از عناصر گروه گالوا ریشه‌های چند جمله‌ای مینمال را به یک دیگر تصویر می‌کنند، پس $\sigma(\sqrt[n]{\alpha}) = \zeta \sqrt[n]{\alpha}$ نیز نتیجه می‌شود. □

با توجه به قضیه بالا و نگاشت $\sigma \mapsto \zeta$ می‌توان همریختی یک به یک زیر را تعریف نمود:

$$Gal(L/K) \hookrightarrow \mu_n$$

در ادامه با در نظر گرفتن مفاهیم و قضایای بالا دو قضیه تقابل ضعیف و قوی را بیان می‌کنیم:

قضیه ۷.۱۲ (تقابل ضعیف)**.** *فرض کنید K میدان عددی شامل n- امین ریشه اولیه واحد است. برای عضو ناصفر $\alpha \in \mathcal{O}_K$ ، $L = K(\sqrt[n]{\alpha})$ قرار دهید.*
فرض کنید هنگ $\mathfrak{m}$ توسط تمامی اول‌های میدان K که شامل $n\alpha$ اند، شمرده می‌شود. به علاوه $\ker(\Phi_{L/K,\mathfrak{m}})$ گروه همنهشتی به پیمانه $\mathfrak{m}$ است. در این صورت نمودار زیر جابجایی است:

$$\begin{array}{ccc} I_K(\mathfrak{m}) & \xrightarrow{\Phi_{L/K,\mathfrak{m}}} & Gal(L/K) \\ & \searrow^{\left(\frac{\alpha}{\cdot}\right)_n} & \downarrow \\ & & \mu_n \end{array}$$

که $Gal(L/K) \hookrightarrow \mu_n$ نگاشت یک به یک طبیعی است.
بنابراین اگر G تصویر $Gal(L/K)$ در μ_n باشد، نماد لژاندر مرتبه n- ام $\left(\left(\frac{\alpha}{\mathfrak{a}}\right)_n\right)$ همریختی پوشای زیر را القا می‌کند:

$$\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \longrightarrow G \subset \mu_n$$

اثبات. برای مشاهده اثبات به [۷، قضیه ۱۱.۸] رجوع کنید. □

به این دلیل قضیه بالا را قضیه تقابل ضعیف می‌نامیم که این قضیه تنها همریختی بین دو گروه $I_K(\mathfrak{m})$ و μ_n را بیان می‌کند و فرمولی برای محاسبه $(\alpha/\mathfrak{a})_n$ ارائه نمی‌کند. ولی با این وجود این قضیه ابزاری بسیار قدرتمند است، برای نمونه با به کارگیری این قضیه می‌توان قضیه تقابل مربعی را اثبات نمود(برای مشاهده جزئیات بیشتر به [۷، قضیه ۱۲.۸] رجوع کنید).

پیش از بیان قضیه تقابل قوی نماد گذاری زیر ار در نظر بگیرید. فرض کنید $\alpha, \beta \in \mathcal{O}_K$ اند. در این صورت برای سادگی $(\alpha/\beta\mathcal{O}_K)_n$ را با $(\alpha/\beta)_n$ نمایش می‌دهیم.

قضیه ۸.۱۲ (تقابل قوی)**.** *فرض کنید K میدان عددی شامل n- امین ریشه اولیه واحد است و $\alpha, \beta \in \mathcal{O}_K$ دو عضو نسبت به هم و n اولند. در این صورت داریم:*

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{p}|n_\infty} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n$$

که $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_n$ نماد هیلبرت [۴] [۵] از مرتبه n- ام و ∞ حاصلضرب اول‌های حقیقی نامتناهی از K است (تنها زمانی که $n = 2$ رخ می‌دهد).

اثبات. برای مشاهده اثبات به [۷، قضیه ۱۴.۸] رجوع کنید. □

[4] Hilbert Symbol

[۵] نماد هیلبرت از مرتبه n- ام با استفاده از نظریه میدان رده‌ای میدان‌های موضعی تعریف می‌گردد. از آنجایی که در این نوشتار به روش‌های موضعی نظریه میدان رده‌ای اشاره نشده است، نمی‌توان تعریف دقیقی از این نماد را بیان کرد.

علاقه مندان مطالعه جزئیات بیشتر در رابطه با نماد هیلبرت می‌توانند به [۱۵، بخش دوم، ص ۵۳-۶۴] و [۳۱، ص ۵۰-۵۵ و ۱۱۰-۱۱۲] مراجعه کنند.

جدول زمانی نظریه میدان رده‌ای

جدول زیر به طور خلاصه سیر تاریخی تحول نظریه میدان رده‌ای را بیان می‌کند.

تاریخ	رویداد
۱۸۰۱	اثبات قانون تقابل مربعی توسط گاوس
۱۸۲۹	آبل گسترش میدانی از $\mathbb{Q}(i)$ ارائه کرد.
۱۸۳۷	بیان قضیه دیریشله روی تصاعدهای حسابی توسط دیریشله [۶]
۱۸۵۳	بیان قضیه کرونکر- وبر توسط کرونکر
۱۸۸۰	کرونکر Jugendtraum [۷] خود را در ارتباط با توسیع‌های آبلی میدان‌های مربعی موهومی بیان کرد.
۱۸۸۶	وبر اثباتی برای قضیه کرونکر- وبر ارائه می‌دهد. [۸]
۱۸۹۶	هیلبرت اولین اثبات کامل را برای قضیه کرونکر- وبر ارائه داد.
۱۸۹۷	وبر گروه رده‌ای شعاعی و گروه رده‌ای تعمیم یافته را معرفی کردند.
۱۸۹۷	هیلبرت قانون تقابل مربعی را به صورت حاصل‌ضربی برای نماد هیلبرت بازنویسی کرد.
۱۸۹۷	معرفی اعداد پی‌ادیک [۹] توسط هنسل [۱۰]
۱۸۹۸	هیلبرت حدس خود را در ارتباط با وجود و خاصیت‌های میدان رده‌ای هیلبرت بیان کرد. هم‌چنین این موارد را برای حالت خاصی که عدد رده‌ای برابر ۲ است، اثبات کرد.
۱۹۰۷	فیلیپ فورتوانگلر [۱۱] اثباتی در ارتباط با وجود میدان رده‌ای هیلبرت و خواص ابندایی آن ارائه کرد.
۱۹۰۸	وبر میدان رده‌ای یک گروه رده‌ای تعمیم یافته را تعریف کرد.
۱۹۲۰	تاکایاگی با ارائه اثباتی نشان داد که توسیع‌های آبلی یک میدان عددی دقیقا همان میدان‌های رده‌ای گروه رده‌ای اند.
۱۹۲۲	تاکایاگی نشریه‌ای درباره قوانین تقابل چاپ کرد.
۱۹۲۳	آرتین قضیه تقابل آرتین را حدس زد. [۱۲]
۱۹۲۴	آرتین توابع L- آرتین را معرفی کرد.
۱۹۲۶	چبوتارف قضیه چگالی خود را اثبات کرد. [۱۳]

۱۹۲۷	آرتین قضیه تقابل خود را اثبات کرد. اثبات این قضیه یکریختی طبیعی بین گروه گالوا و گروه رده‌ای ایده‌آلی ارائه می‌دهد.
۱۹۳۰	فورتوانگلر و آرتین اثباتی برای قضیه ایده‌آل اصلی ارائه دادند. [۱۴]
۱۹۳۰	هسه نظریه میدان رده‌ای موضعی [۱۵] را معرفی کرد.
۱۹۳۱	هسه قضیه نرم [۱۶] خود را اثبات کرد. و جبرهای ساده [۱۷] برای روی میدان‌های موضعی را رده بندی کرد.
۱۹۳۱	قضیه آلبرت- باوئر- هسه- نوتر [۱۸] اثباتی برای قانون هسه در ارتباط با جبرهای ساده بر روی میدان‌های سراسری ارائه داد.
۱۹۳۳	هسه جبرهای ساده روی میدان‌های سراسری را رده بندی کرد.
۱۹۳۴	مکس دیورینگ [۱۹] و امی نوتر [۲۰] نظریه میدان رده‌ای با استفاده از جبر گسترش دادند.
۱۹۳۶	کلود شوالی [۲۱] مفهومی به نام ایدل [۲۲] را معرفی کرد.
۱۹۴۰	شوالی با استفاده از ایدل اثباتی در ارتباط با نامساوی دوم توسیع‌های آبلی ارائه کرد.
۱۹۵۰	تیت در رساله خود با استفاده از آنالیز روی حلقه‌های ایدل توابع ζ را مطالعه کرد.
۱۹۵۱	آندره ویل [۲۳] گروه‌های ویل [۲۴] را معرفی کرد.
۱۹۵۲	آرتین و تیت مفهومی به نام Class Formation را در نوشتار خود در ارتباط با نظریه میدان رده‌ای معرفی کردند.
۱۹۵۲	گرهارد هوچیلد [۲۵] و تاداشی ناکایاما [۲۶] از کوهمولوژی گروه‌ها در نظریه میدان رده‌ای استفاده کردند.
۱۹۵۲	تیت، کوهمولوژی گروه‌های تیت [۲۷] را معرفی کرد.
۱۹۶۴	اوگنی گولود [۲۸] و ایگور شافارویچ [۲۹] اثبات کردند که برج میدان رده‌ای [۳۰] می‌تواند نامتناهی باشد.
۱۹۶۵	جاناتان لوبین [۳۱] و تیت با استفاده Lubin–Tate Formal Group Law، توسیع‌های آبلی منشعب از میدان‌های موضعی ساختند.

جدول ارائه شده به طور خلاصه روندی از تحول نظریه میدان رده‌ای را بیان می‌کند.
باتوجه به این جدول، همان گونه که در بخش‌های قبلی نیز بیان شد، نظریه میدان رده‌ای را می‌توان توصیفی برای توسیع‌های آبلی موضعی و سراسری دانست.

---

۶ Dirichlet's Theorem on Arithmetic Progression
۷ Jugendtraum کلمه‌ای آلمانی است، ترجمه این کلمه به معنای رویای جوانی است.
۸ اثبات ارائه شده توسط وبر شامل نقص‌هایی بوده است.
۹ Numbers P-adic
۱۰ Hensel
۱۱ Furtwängler Philipp
۱۲ این حدس در این نوشتار در قالب قضیه تقابل آرتین بیان شده است.
۱۳ این قضیه در این نوشتار در قالب قضیه چگالی چبوتارف بیان شده است.
۱۴ Principal Ideal Theorem
۱۵ Local Class Field Theory
۱۶ Hasse Norm Theorem
۱۷ Simple Algebras
۱۸ Albert-Bauer-Hasse-Noether Theorem
۱۹ Max Deuring
۲۰ Emmy Noether
۲۱ Claude Chevalley
۲۲ Idele
۲۳ Andre Weil
۲۴ Weil's Group
۲۵ Gerhard Hochschild
۲۶ Tadashi Nakayama
۲۷ Tate Cohomology Groups
۲۸ Evgeny Golod
۲۹ Igor Shafarevich
۳۰ Class Field Tower
۳۱ Jonathan Lubin

واژه‌نامه فارسی به انگلیسی

الف

آبلی ..... Abelian
nـامین ریشه اولیه واحد ..... n^{th} root of unity
اردر ..... Order
اردر جبری ..... Algebraic Order
ارزه ضربی ..... Multiplicative Valuation
ارزه مطلق ..... Absolute Value
ارزه ناارشمیدسی ..... Non-Archimedean Absolute Value
اصلی ..... Principal
اول ..... Prime
اول‌های متناهی ..... Finite Primes
اول‌های نامتناهی حقیقی ..... Infinite Real Primes
اول‌های نامتناهی مختلط ..... Infinite Complex Primes
اول‌های درجه ۱ ..... Primes of Degree 1
اولیه ..... Primitive
ایده‌آل ..... Ideal
ایده‌آل کسری ..... Fractional Ideal

ب

باقی‌ماندن ..... Inert
بعد کرول ..... Krull Dimension
به صورت سره معادل بودن ..... Properly Equivalent
به صورت سره نمایش دادن ..... Properly Represent
به صورت ناسره معادل بودن ..... Properly Equivalent
به صورت یکنواخت همگرا ..... Absolutely Converge
به طور صحیح بسته ..... Algebraically Closed

ت

تابع ال ..... L- Function
ترکیب ..... Composition
ترکیب مستقیم ..... Direct Composition
تقابل ..... Reciprocity
تقابل ضعیف ..... Weak Reciprocity
تقابل قوی ..... Strong Reciprocity
تقابل مربعی ..... Quadratic Reciprocity
توسیع جدایی پذیر ..... Separable Extension
توسیع ..... Extension
توسیع سراسری ..... Global Extension
توسیع کومر ..... Kummer Extension
توسیع گالوا ..... Galois Extension
توسیع موضعی ..... Local Extension
توسیع نامنشعب ..... Unramified Extension
توسیع نرمال ..... Normal Extension

ج

جمعی ..... Additive

چ

چگالی ..... Density
چند جمله‌ای مینیمال ..... Minimal Polynomial

ح

حلقه اعداد صحیح جبری ..... Ring of Algebraic Integers
حوزه ددکنید ..... Dedekind Domain

خ

خارج قسمت ..... Quotient

د

دترمینان ..... Determinant
درجه ..... Degree
درجه اینرسی ..... Inertia Degree

ر

رابطه هم ارزی ..... Equivalence Relation

ش

شاخص انشعاب ..... Ramification Index
شعاع به پیمانه $\mathfrak{m}$ ..... Ray mod $\mathfrak{m}$

ص

صوری ..... Formal

ط

طبیعی ..... Canonical

ف

فرم اصلی ..... Principal Form
فرم کاهش یافته ..... Reduced Form
فرم مثبت معین ..... Positive Definite Form
فرم مربعی ..... Quadratic Form
فرم نامعین ..... Indefinite Form

ق

قضیه تقابل آرتین ..... Artin Reciprocity
قضیه چگالی چبوتارف ..... Cebotarev Density Theorem
قضیه کنداکتور ..... Conductor Theorem
قضیه وجودی ..... Existence Theorem
قطب ساده ..... Simple Pole
قوانین تقابل ..... Reciprocity Laws

ک

کاراکترهای نسبت داده شده ... Assigned Characters
کاملا شکافته شدن ... Splits Compeletly
کلاس ... Class
کلاس تزویجی ... Conjugacy Class
کنداکتور ... Conductor

گ

گروه اینرسی ... Inertia Group
گروه پیکارد ... Picard Group
گروه تجزیه ... Decomposition Group
گروه رده‌ای (ایده‌آلی) ... Ideal Class Group
گروه رده‌ای تعمیم یافته ... Generalized Ideal Class Group
گروه رده‌ای شعاعی به پیمانه $\mathfrak{m}$ ... Ray Class Field mod $\mathfrak{m}$
گروه همنهشتی ... Congruent Subgroup
گروه رده‌ای ... Class Group
گسسته ... Additive
گونا ... Genra

م

ماتریس ضرائب ... Coefficient Matrix
ماکسیمال ... Maximal
مانده توانی ... Power Residue
مانده مربعی ... Quadratic Residue
مبین ... Discriminant
مدول ... Module
مرتبه ... Rank
مزدوج ... Conjugate
مکان ... Place
معادل ... Equivalent
منشعب شدن ... Ramifies
میدان ... Field
میدان ثابت شده ... Fix Field
میدان رده‌ای شعاعی به پیمانه $\mathfrak{m}$ ... Ray Class Field mod $\mathfrak{m}$

میدان رده‌ای هیلبرت ..... Hilbert Class Field
میدان شکافنده ..... Spiting Field
میدان عددی ..... Number Field
میدان کسرها ..... Fractional Field
میدان مربعی ..... Quadratic Field
میدان مربعی موهومی ..... Imaginary Quadratic Field
میدان دایره بر ..... Cyclotomic Field

ن

نامانده مربعی ..... Nonquadratic Residue
نرمال شده ..... Normalized
نزول ..... Descent
نظریه انشعاب ..... Ramification Theory
نظریه فرم‌های مربعی ..... Theory of Quadratic Forms
نظریه گونا ..... Genus Theory
نظریه میدان رده‌ای ..... Class Field Theory
نظریه میدان‌ها ..... Field Theory
نماد آرتین ..... Artin Symbol
نماد فروبینیوس ..... Frobineus Symbol
نماد کرونکر ..... Kronecker Symbol
نماد لژاندر ..... Legendre Symbol
نمایش دادن ..... Represent
نوتری ..... Noetherian

ه

هم‌ارز ..... Equivalent
همریختی ..... Homomorphism
همگرا ..... Convergent
همنهشت ..... Congruent
فرم منفی نامعین ..... Negative Definite Form

و

وارون پذیر ..... Invertible

ی

یک ریختی ..... Isomorphism

واژه‌نامه انگلیسی به فارسی

A

Abelian ..... آبلی
Absolutely Converge ..... به صورت یکنواخت همگرا
Absolute Value ..... ارزه مطلق
Additive ..... جمعی
Algebraic Order ..... اردر جبری
Algebraically Closed ..... به طور صحیح بسته
Artin Reciprocity Theorem ..... قضیه تقابل آرتین
Artin Symbol ..... نماد آرتین
Assigned Character ..... کاراکترهای نسبت داده شده

C

Cebotarev Density Theorem ..... قضیه چگالی چبوتارف
Class ..... کلاس
Class Field Theory ..... نظریه میدان رده‌ای
Class Group ..... گروه رده‌ای
Coefficient Matrix ..... ماتریس ضرایب
Composition ..... ترکیب
Conductor ..... کنداکتور
Conductor Theorem ..... قضیه کنداکتور
Congruence Subgroup ..... گروه همنهشتی
Congruent ..... همنهشت
Conjugate ..... مزدوج
Conjugacy Class ..... کلاس تزویجی
Canonical ..... طبیعی
Converge ..... همگرا

Cyclotomic Field ..... میدان دایره بر

D

Decomposition Group ..... گروه تجزیه
Dedekind Domain ..... حوزه ددکنید
Degree ..... درجه
Density ..... چگالی
Descent ..... نزول
Determinant ..... دترمینان
Direct Composition ..... ترکیب مستقیم
Discrete ..... گسسته
Discriminant ..... مبین

E

Equivalence ..... معادل - هم‌ارز
Equivalence Relation ..... رابطه هم‌ارزی
Existence Theorem ..... قضیه وجودی
Extension ..... توسیع

F

Field ..... میدان
Field Theory ..... نظریه میدان‌ها
Finite Primes ..... اول‌های متناهی
Fix Field ..... میدان ثابت شده
Frobenuis Symbol ..... نماد فروبینیوس
Formal ..... صوری
Fraction Field ..... میدان کسرها
Fractional Ideal ..... ایده‌آل کسری

G

Galois Extension ..... توسیع گالوا
Generalized Ideal Class Group ..... گروه رده‌ای تعمیم یافته

Genra ..... گونا
Genus Theory ..... نظریه گونا
Global Extension ..... توسیع سراسری

H

Hilbert Class Field ..... میدان رده‌ای هیلبرت
Homomorphism ..... همریختی

I

Ideal ..... ایده‌آل
Ideal Class Group ..... گروه رده‌ای (ایده‌آلی)
Imaginary Quadratic Form ..... میدان مربعی موهومی
Improperly Equivalent ..... به صورت ناسره معادل
Indefinite form ..... فرم نامعین
Inert ..... باقی ماندن
Inertia Group ..... گروه اینرسی
Inertial Degree ..... درجه اینرسی
Infinite Complex Primes ..... اول‌های نامتناهی مختلط
Infinite Real Primes ..... اول‌های نامتناهی حقیقی
Invertible ..... وارون پذیر
Isomorphism ..... یکریختی

K

Kronecker Symbol ..... نماد کرونکر
Krull Dimension ..... بعد کرول
Kummer Extension ..... توسیع کومر

L

L- Function ..... تابع- L
Legendre Symbol ..... نماد لژاندر
Local Extension ..... توسیع موضعی
Localization ..... موضعی سازی

M

Maximal ..... ماکسیمال
Minimal Polynomial ..... چندجمله‌ای مینیمال
Module ..... مدول
Modulus ..... هنگ
Multiplicative Valuation ..... ارزه ضربی

N

Negative Definite Form ..... فرم منفی معین
n^{th} root of unity ..... nـامین ریشه اولیه واحد
Noetherian ..... نوتری
Non-Archimedean Absolute Value ..... ارزه ناارشمیدسی
Non-quadratic Residue ..... نامانده مربعی
Normal Extension ..... توسیع نرمال
Normalized ..... نرمال شده
Number Field ..... میدان عددی

O

Order ..... اردر

P

Picard Group ..... گروه پیکارد
Place ..... مکان
Positive Definite Form ..... فرم مثبت معین
Power Residue ..... مانده توانی
Prime ..... اول
Primes of Degree 1 ..... اول‌های درجه ۱
Primitive ..... اولیه
Principal ..... اصلی
Principal Form ..... فرم اصلی
Properly Equivalent ..... به صورت سره معادل بودن
Properly Represent ..... به صورت سره نمایش دادن

Q

Quadratic Field ..... میدان مربعی
Quadratic Forms ..... فرم مربعی
Quadratic Reciprocity ..... تقابل مربعی
Quadratic Residue ..... مانده مربعی
Quotient ..... خارج قسمت

R

Ramification Index ..... شاخص انشعاب
Ramification Theory ..... نظریه انشعاب
Ramifies ..... منشعب شدن
Rank ..... مرتبه
Ray Class Field mod $\mathfrak{m}$ ..... گروه رده‌ای شعاعی پیمانه $\mathfrak{m}$
Ray Class Group mod $\mathfrak{m}$ ..... خارج قسمت
Ray mod $\mathfrak{m}$ ..... شعاع به پیمانه $\mathfrak{m}$
Reciprocity Laws ..... قوانین تقابل
Reciprocity ..... تقابل
Reduced Forms ..... فرم کاهش یافته
Represent ..... نمایش دادن
Ring of Algebraic Integers ..... حلقه اعداد صحیح جبری

S

Separable Extension ..... توسیع حدایی پذیر
Simple Pole ..... قطب ساده
Splits Completely ..... کاملا شکافته شدن
Splitting Field ..... میدان شکافنده
Strong Reciprocity ..... تقابل قوی

T

Theory of Quadratic Forms ..... نظریه فرم‌های مربعی

U

Unramified Extension ..... توسیع نامنشعب

W

Weak Reciprocity ..... تقابل ضعیف

کتاب‌نامه

[1] Z. I. Borevich and I. R. Shafarevich, Number theory, Pure and Applied Mathematics, Vol.20, Academic Press, New York-London, 1966. Translated from the Russian by Newcomb Greenleaf.

[2] Duncan A. Buell, Class groups of quadratic fields I, II, Math. Comp. 30 (1976), no. 135, 610–623, ibid 48 (1987), 85–93, DOI 10.2307/2005330.

[3] S. Chowla, An extension of Heilbronn's class number theorem, Quarterly J. Math. 5 (1934).

[4] Keith Conard, History of Class Field Theory, Available at kconrad.math.uconn.edu/blurbs/gradnumthy/cfthistory.pdf

[5] Keith Conard, The Conductor Ideal of an Order, Available at kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf

[6] Keith Conard, Cyclotomic Extensions, Available at kconrad.math.uconn.edu/blurbs/galoistheory/cyclotomic.pdf

[7] David A. Cox, Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication, 2nd Edition.

[8] M. Deuring, Die Klassenkorper der komplexen Multiplikation (German), Enzyklopadie dermathematischen Wissenschaften mit Einschluss ihrer Anwendungen, Band I 2, Heft 10, Teil II (Article I 2, vol. 23, B. G. Teubner Verlagsgesellschaft, Stuttgart, 1958.

[9] P. G. L. Dirichlet, Zahlentheorie, 4th edition, Vieweg, Braunschweig, 1894.

[10] David S. Dummit & Richard M. Foote, Abstract Algebra, 3rd edition.

[11] P. de Fermat, Oeuvres, Gauthier-Villars, Paris, 1891–1896.

[12] Daniel E. Flath, Introduction to number theory, A Wiley-Interscience Publication, John Wiley Sons, Inc., New York, 1989.

[13] Gunther Frei, On the development of the genus of quadratic forms (English, with French summary), Ann. Sci. Math. Quebec 3 (1979), no. 1, 5–62.

[14] C. F. Gauss, Disquisitiones Arithmeticae, Leipzig, 1801. Republished in 1863 as Volume I of Werke (see [42]). French translation, Recherches Arithm´etiques, Paris, 1807. (Reprint by Hermann, Paris, 1910.) German translation, Untersuchungen uber Hohere Arithmetik,Berlin, 1889. (Reprint by Chelsea, New York, 1965.) English Translation, Yale, New Haven, 1966. (Reprint by Springer-Verlag, Berlin, Heidelberg, and New York, 1986.

[15] H. Hasse,Bericht uber neuere Untersuchungen und Probleme aus der Theorie def algebraischen Zahlkorper, I, Ia and II, Jahresber. Deutch. Math. Verein 35 (1926), pp. 1–55, 36 (1927), pp. 233–311, and Erg. Bd. 6 (1930), pp. 1–201. (Reprint by Physica-Verlag,Wurzburg Vienna, 1965.)

[16] H. Hasse, History of Class Field Theory, in “Algebraic Number Theory,” J. W. S. Cassels and A. Frohlich (ed.), Academic Press, New York, 1967, 266–279.

[17] H. Hasse, “Class Field Theory,” Lecture Notes 11, Dept. Math. Univ. Laval, Quebec, 1973.

[18] C. S. Herz, Construction of class fields, in Seminar on Complex Multiplication, Lecture Notes in Math. 21, Springer-Verlag, Berlin, Heidelberg, and New York, 1966, pp. VII-1 to VII-21.

[19] S. Iyanaga, “The Theory of Numbers,” North-Holland, Amsterdam, 1975.

[20] S. Iyanaga, Travaux de Claude Chevalley sur la theorie du corps de classes: Introduction, Japan. J. Math.1 (2006), 25–85.

[21] Gerald J. Janusz, Algebraic number fields, Pure and Applied Mathematics, Vol. 55, Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1973.

[22] Frazer Jarvis, Algebraic Number Theory, Springer Cham Heidelberg New York Dordrecht London.

[23] M. Katsuya, The Establishment of the Takagi–Artin Class Field Theory, in "The Intersection of History and Mathematics," (C. Sasaki, M. Sugiura, J. W. Dauben ed.), Birkhauser, Boston, 1995, 109–128.

[24] J. L. Lagrange, Oeuvres, Vol. 3, Gauthier-Villars, Paris, 1869.

[25] S. Lang, "Algebraic Number Theory," 2nd ed., Springer-Verlag, New York, 1994.

[26] S. Lang, Elliptic Functions, 2nd edition, Springer-Verlag, Berlin, Heidelberg, and New York, 1987.

[27] Daniel A. Marcus, Number fields, Universitext, Springer-Verlag, New York-Heidelberg, 1977.

[28] G. B. Mathews, Theory of numbers, Chelsea Publishing Co., New York, 1961. 2nd ed.

[29] J.S. Milne, Algebraic Number Theory, (v3.08), Available at www.jmilne.org/math/

[30] Jürgen Neukirch, Algebraic.Number.Theory, Springer-Verlag Berlin Heidelberg 1999.

[31] Jürgen Neukirch, Class Field Theory, Springer-Verlag Berlin Heidelberg New York Tokyo.

[32] Winfried Scharlau and Hans Opolka, From Fermat to Minkowski, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1985. Lectures on the theory of numbers and its historical development; Translated from the German by Walter K. Buhler and Gary Cornell, DOI 10.1007/978-1-4757-1867-6.]

[33] Daniel Shanks, Class number, a theory of factorization, and genera, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 415–440.

[34] Ian Stewart & David Hall, Algebraic Number Theory and Fermat's Last Theorem, 3rd edition.

[35] Andre Weil, Number theory: An approach through history; From Hammurapi to Legendre, Birkhauser Boston, Inc., Boston, MA, 1984, DOI 10.1007/978-0-8176-4571-7.

[36] P. J. Weinberger, Exponents of the class groups of complex quadratic fields, Acta Arith. **22** (1973), 117–124, DOI 10.4064/aa-22-2-117-124.

Abstract

This thesis delves into a mathematical problem that has been challenging since the era of Fermat:

Given an integer n, find all prime numbers in the form of x^2+ny^2 with $x, y \in \mathbb{Z}$.

We explore various elementary techniques to tackle the problem, descent and reciprocity (suggested by Euler), quadratic forms, and Genus theory. However, each approach has its limitations.

Class field theory is required to make further progress, which provides an abstract solution to the problem. The Hilbert class field is introduced first to solve the problem for infinite values of n, followed by using the ring class field to solve the problem for all values of n.

This thesis provides a comprehensive overview of the techniques used to solve this longstanding mathematical problem and presents a promising solution using class field theory.

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

Primes of the Form $x^2 + ny^2$

Negin Shadgar

Supervisor: Dr. Amir Ghadermarzi

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

2023