١

[ـ] [ـ] [ـ] [ـ] [ـ] [ـ] [ـ] [ـ]

دانشگاه صنعتی خواجه نصیرالدین طوسی

دانشکده علوم

پایان‌نامه کارشناسی‌ارشد

ریاضی محض، گرایش جبر

موضوع:

ساختار زنجیرهای متمایز اشباع شده

نگارنده:

خدیجه میردار هریجانی

استاد راهنما:

دکتر کمال عقیق

شهریور ۱۳۹۰

ناچیزتر از آن است که تقدیم را شایسته باشد،

ولی به پاس ارج نهادن به زحماتی که جبرانش هرگز برایم میسر نخواهد بود،

تقدیم می‌دارم به **پدر و مادر عزیزم**،

که سایه‌شان بر سرم همه مهر است و نثارم به پایشان همه شرم

و تقدیم به **همسرم**

به پاس تمام همدلی‌ها و مهربانی‌هایش.

اظهارنامه دانشجو

موضوع پایان‌نامه: ساختار زنجیرهای متمایز اشباع شده

استاد راهنما: دکتر کمال عقیق

نام دانشجو: خدیجه میردار هریجانی

شماره‌ی دانشجویی: ۸۸۰۳۲۵۴

اینجانب خدیجه میردار هریجانی دانشجوی کارشناسی ارشد ریاضی محض گرایش جبر دانشکده علوم دانشگاه صنعتی خواجه نصیرالدین طوسی گواهی می‌نمایم که تحقیقات ارائه شده در این پایان‌نامه توسط شخص اینجانب انجام شده و صحت و اصالت مطالب نگارش شده مورد تأیید می‌باشد و در مورد استفاده از کار دیگر محققان به مرجع مورد استفاده اشاره شده است. همچنین گواهی می‌نمایم که مطالب مندرج در پایان‌نامه تاکنون برای دریافت هیچ نوع مدرک یا امتیازی توسط اینجانب یا فرد دیگر در هیچ جا ارائه نشده است و در تدوین متن پایان‌نامه آئین‌نامه مصوب دانشگاه را به‌طور کامل رعایت کرده‌ام.

امضای دانشجو:

تاریخ:

فرم حق طبع و نشر و مالکیت نتایج

سپاس خدایی را که علم را مایه مباهات بشر قرار داده است.

اکنون که به یاری خدا مراحل نگارش و تدوین پایان‌نامه‌ام به اتمام رسیده است، لازم می‌دانم مراتب قدردانی خویش را تقدیم سرورانی نمایم که همواره راهنمایم بوده‌اند.

از استاد محترم و گرانقدرم جناب آقای دکتر کمال عقیق که با الطاف و راهنمایی‌های بی‌دریغشان مرا در به پایان رساندن این پایان‌نامه همراهی فرمودند سپاسگزارم.

همچنین از اساتید بزرگوارم جناب آقای دکتر صمد حاج‌جباری و جناب آقای دکتر شعبان قلندرزاده که زحمت بازخوانی و داوری این پایان‌نامه را بر عهده داشتند نهایت تشکر و قدردانی را دارم.

در نهایت سپاس بی‌پایان تقدیم خانواده عزیز و دلسوزم، آنهایی که بی‌دریغ و بی‌منت حامی و پشتیبان روزهای سخت و دشوارم بوده‌اند.

چکیده

فرض کنیم v یک ارزش هنسلی با رتبه دلخواه از میدان K و $\bar{v}$ (توسیع منحصربه فرد) از v به بستار جبری $\bar{K}$ از K باشد. برای عضو $\alpha \in \bar{K} \setminus K$ زنجیر $\alpha = \alpha_{۰}, \dots, \alpha_r$ از عناصر $\bar{K}$ را یک زنجیر متمایز اشباع شده برای α نسبت به میدان ارزش (K, v) می‌نامیم؛ هرگاه α_i ها از کمترین درجه روی K با این ویژگی که

$$\bar{v}(\alpha_{i-۱} - \alpha_i) = \sup\{\bar{v}(\alpha_{i-۱} - \beta) \mid [K(\beta) : K] < [K(\alpha_{i-۱}) : K], \beta \in \bar{K}\}$$

و $\alpha_r \in K$ باشد.

در این پایان‌نامه ابتدا به مطالعه ساختار زنجیرهای متمایز اشباع شده می‌پردازیم و سپس زنجیر متمایز اشباع شده چند جمله‌ای‌ها روی میدان موضعی K را توصیف می‌کنیم و الگوریتمی را برای یافتن این زنجیر از چند جمله‌ای‌ها با در نظر گرفتن چند جمله‌ای تحویل ناپذیر $f(x)$ روی K ارائه می‌کنیم.

فهرست مندرجات

مقدمه

نظریه ارزش اولین بار توسط ریاضیدان مجارستانی جوزف کورشاک [۱] در سال ۱۹۱۲ مطرح شد. امروزه از نظریه ارزش در رشته‌هایی مانند جبر، هندسه، آنالیز و همچنین در نظریه کد گذاری در مخابرات استفاده می‌شود.

اگرچه شکل امروزی تعریف ارزش توسط کورشاک ارائه شد؛ ولی ایده اولیه آن از کورت هنسل [۲] بود و در پیشرفت نظریه ارزش نقش بسزایی داشت از این‌رو هنسل را می‌توان پدر نظریه ارزش نامید. استروسکی [۳]، هیس [۴]، اشمیت [۵] و کرول [۶] با استفاده از ایده هنسل نظریه ارزش را توسعه دادند.

در سال ۱۹۳۱ ولفگانگ کرول به تعمیم نظریه ارزش روی یک میدان دلخواه K پرداخت و نگاشت $v : K \to \Gamma \cup \infty$ که در شرایط زیر صدق می‌کند را یک ارزش نامید:

(۱) $v(0) = \infty$؛

(۲) $v(xy) = v(x) + v(y)$؛

(۳) $v(x+y) \geq \min\{v(x), v(y)\}$؛

این پایان‌نامه شامل چهار فصل است.

در فصل اول به تعاریف و مقدماتی از نظریه جبری اعداد می‌پردازیم و در ادامه آن تعریف و ویژگی‌هایی از قدرمطلق، میدان‌های ارزش، توسیع ارزش‌ها و میدان‌های ارزش هنسلی را خواهیم آورد.

[۱] Josef Kurschak

[۲] Kurt Hensel

[۳] Ostrowski

[۴] Hasse

[۵] Eshmidt

[۶] Krull

مطالعه در مورد چند جمله‌ای‌های تحویل ناپذیر روی یک میدان یک مساله جالب و قدیمی بوده است. از زنجیرهای متمایز اشباع شده جهت به دست آوردن نتایج درباره چند جمله‌ای‌های تحویل ناپذیر روی میدان ارزش گسسته کامل با رتبه یک استفاده می‌شود. همچنین برای یافتن پایه صحیح یک توسیع از میدان کاربرد دارد. و جهت مشخص کردن قوانین مختلف حساب و ثابت‌های متریک وابسته به عناصر بستار میدان ارزش از زنجیر متمایز اشباع شده استفاده می‌شود. بدین منظور در این پروژه این زنجیرها را تعریف و ساختار آن را بررسی می‌کنیم.

در فصل دوم زوج مینیمال و زوج متمایز را روی میدان‌های ارزش معرفی و خواص آن‌ها را مطرح می‌کنیم.

در فصل سوم زنجیر متمایز اشباع شده را تعریف و ساختار آن‌را بررسی می‌کنیم.

در فصل چهارم زنجیر متمایز اشباع شده برای چند جمله‌ای‌ها را روی میدان‌های موضعی تعریف و الگوریتمی را برای یافتن این زنجیرها ارائه می‌کنیم.

محور اصلی این پایان نامه مقالات [۷] و [۲۶] است.

فصل ۱

تعاریف و قضایای مقدماتی

۱.۱ مقدمه‌ای بر نظریه جبری اعداد

در تمامی این بخش فرض می‌کنیم L یک میدان و K زیر میدانی از L باشد؛ دراین صورت L توسیع میدان K خواهد بود و آن‌را با $L|K$ نشان می‌دهیم.

تعریف ۱.۱.۱ عنصر $x \in L$ را روی K جبری گوییم؛ هرگاه چند جمله‌ای ناصفر f با ضرایب درK وجود داشته باشد به‌طوری که $f(x) = 0$؛ درغیر این‌صورت x را روی K متعالی نامیم.

تعریف ۲.۱.۱ اگر هر عضو از L روی K جبری باشد؛ آنگاه L توسیع جبری K نامیده می‌شود. درغیر این‌صورت L توسیع متعالی از K است.

تعریف ۳.۱.۱ میدان L در حالت خاص یک فضای برداری روی K است. مجموعه $B = \{u_1, u_2, ..., u_n\} \subseteq L$ را یک پایه برای L روی K گوییم، اگر و تنها اگر در ویژگی‌های زیر صدق

کند:

(۱) B روی K مستقل خطی باشد؛ یعنی اگر $a_1, \ldots, a_n \in K$ آنگاه $a_1u_1 + \cdots + a_nu_n = 0$ اگر و تنها اگر برای هر $i \in \{1, \ldots, n\}$، $a_i = 0$.

(۲) B فضای L را تولید کند؛ یعنی اگر $v \in L$؛ برای $a_1, \ldots, a_n \in K$،

$$v = a_1u_1 + \cdots + a_nu_n$$

در این‌صورت، هر عنصر L دارای نمایش یکتایی به عنوان $K-$ترکیب خطی از عضوهای B است؛ و گوییم L روی K دارای بعد n است، که این مطلب را به صورت زیر نمایش می‌دهیم:

$$[L : K] = n$$

تعریف ۴.۱.۱ یک چند جمله‌ای تکین با ضرایب از K و کوچکترین درجه ممکن که $x \in L$ ریشه آن باشد، را چند جمله‌ای مینیمال x روی K نامیم و درجه آن‌را، درجه x روی K گوییم.

تعریف ۵.۱.۱ میدان K را در نظر می‌گیریم؛ میدان $\bar{K}$ با ویژگی‌های زیر وجود دارد:

(۱) $\bar{K}$ توسیع جبری از K است.

(۲) اگر L توسیع جبری $\bar{K}$ باشد، آنگاه $L = \bar{K}$.

(۳) برای هر میدان $\tilde{K}$ که در شرایط (۱) و (۲) صدق می‌کند یک $K-$یکریختی (یکریختی که همه عناصر زیرمیدان K را ثابت نگه می دارد) بین $\bar{K}$ و $\tilde{K}$ وجود دارد.

$\bar{K}$ بستار جبری K نامیده می‌شود.

میدانی را که در شرط (۲) صدق می‌کند میدان به‌طور جبری بسته گوییم.

قضیه ٦.۱.۱ (قضیه اساسی جبر[1]) میدان اعداد مختلط به‌طور جبری بسته است.

[1] Fundemental theorem of algebra

برهان. به [۲۹]، قضیه ۱۹.۳ مراجعه شود. ■

تعریف ۷.۱.۱ فرض کنیم K یک میدان و $\bar{K}$ بستار جبری آن باشد؛ عناصر $x, x' \in \bar{K}$ را روی K مزدوج گوییم هرگاه یکی از شرایط زیر برقرار باشد:

(۱) چند جمله‌ای مینیمال x و x' روی K برابر باشد.

(۲) یک $K-$یکریختی σ از $K(x)$ به $K(x')$ وجود داشته باشد به‌طوری که $\sigma(x) = x'$.

تعریف ۸.۱.۱ گوییم توسیع L روی K نسبت به مزدوج بسته است؛ هرگاه F توسیعی از L و $u \in L$ و $v \in F$ مزدوجی از u روی K باشد آنگاه $v \in L$ باشد.

تعریف ۹.۱.۱ میدان L را یک توسیع نرمال K گوییم هرگاه توسیع L از K نسبت به مزدوج بسته باشد.

مثال ۱۰.۱.۱ $\bar{K}$ توسیع نرمال از K است.

تعریف ۱۱.۱.۱ چند جمله‌ای $f \in K[x]$ را در نظر می‌گیریم؛ آنگاه f روی L شکافته می‌شود؛ اگر و تنها اگر عنصر $c \in K$ و عناصر $u_۱, u_۲, \ldots, u_n \in L$ موجود باشند به‌طوری که

$$f(x) = c(x - u_۱)(x - u_۲) \cdots (x - u_n)$$

در این حالت، هر u_i $(۱ \leq i \leq n)$ ریشه‌ای از چند جمله‌ای f است.

مثال ۱۲.۱.۱ $f(x) = x^۲ - ۲ \in \mathbb{Q}[X]$ روی میدان $L = \mathbb{Q}(\sqrt{۲})$ و همچنین روی هر توسیع L شکافته می‌شود.

تعریف ۱۳.۱.۱ چند جمله‌ای $f \in K[x]$ را در نظر می‌گیریم. در این‌صورت L میدان شکافنده f روی K است اگر و تنها اگر در ویژگی‌های زیر صدق کند:

(۱) چند جمله‌ای f روی L شکافته شود.

(۲) اگر $E|K$ و $L|E$ و f روی E شکافته شوند؛ آنگاه $E = L$.

قضیه ۱۴.۱.۱ فرض کنیم $L|K$ یک توسیع متناهی میدان باشد؛ در این صورت شرایط زیر معادلند:

(۱) L روی K نرمال است.

(۲) L میدان شکافنده چند جمله‌ای $g(x) \in K[x]$ روی K است.

(۳) به ازای هر میدان $E \supseteq L$ تمام $K-$یکریختی‌ها از L به‌توی E، میدان L را به‌روی L می‌نگارند، یعنی $L-$ یکریختی های L می‌باشند.

برهان. به[۲۸]، قضیه ۳.۱.۲۴ مراجعه شود. ■

نتیجه ۱۵.۱.۱ هر توسیع میدان از درجه دو نرمال است.

برهان. اگر $L|K$ و $[L:K] = ۲$ باشد. $a \in L \setminus K$ را در نظر می‌گیریم؛ چون:

$$[L:K] = [L:K(a)][K(a):K] = ۲$$

و $a \notin K$ پس $[K(a):K] = ۲$.

فرض کنیم $f(x)$ چند جمله‌ای مینیمال a روی K باشد؛ در این‌صورت:

$$[K(a):K] = \deg f(x) = ۲$$

حال برای چند جمله‌ای $h(x) \in L[x]$، $f(x) = (x-a)h(x)$؛ بنابراین $\deg h(x) = ۱$. فرض کنیم به‌ازای $c, d \in L$، $h(x) = cx + d$، که در آن $c \neq ۰$. در این صورت $-c^{-۱}d \in L$ ریشه $h(x)$ است.

بنابراین $-c^{-1}d$ ریشه $f(x)$ است. از این‌رو، هر دو ریشه $f(x)$ در L قرار دارند؛ بنابراین L میدان شکافنده‌ی $f(x)$ روی K است؛ در نتیجه، L توسیع نرمال K می‌باشد. ■

تعریف ۱.۱.۱۶ فرض کنیم $K \subseteq L \subseteq \bar{K}$، که $[L:K] < \infty$؛ گوییم L روی K جدایی پذیر است هرگاه تعداد $K-$یکریختی‌های مجزا از L به $\bar{K}$ برابر با درجه $[L:K]$ باشد.

به‌طور کلی اگر L یک میدان باشد و$K \subseteq L \subseteq \bar{K}$ گوییم L روی K جدایی پذیر است اگر هر زیر میدان F از L که شامل K است و $[F:K] < \infty$ روی K جدایی پذیر باشد.

در حالت خاص توسیع جبری $L = K(x)$ روی K را جدایی پذیر نامیم هرگاه x دارای $n = [L:K]$ مزدوج روی K باشد؛ در این حالت گوییم x عنصر جدایی پذیر روی K است.

تعریف ۱.۱.۱۷ مجموعه

$$K^{sep} = \{\alpha \in \bar{K} \mid \text{روی } K \text{ جدایی پذیر است } \alpha\}$$

را بستار جدایی پذیر K گوییم.

گزاره ۱.۱.۱۸ هر توسیع جبری از میدان با مشخصه صفر جدایی پذیر است.

برهان. اگر K یک میدان از مشخصه صفر باشد، ادعا می‌کنیم همه ریشه‌های هر چند جمله‌ای مینیمال تحویل ناپذیر f روی K متمایزند؛ لذا K جدایی پذیر است.

(اثبات ادعا) فرض کنیم چنین نباشد یعنی $u \in L$ وجود داشته باشد؛ به‌طوری که ریشه چندگانه f باشد. چون K دارای مشخصه صفر و درجه f بزرگتر از یک است، بنابراین $0 < \deg f' < \deg f$. حال چون $f'(u) = 0$ و f چند جمله‌ای مینیمال u روی K است، پس $f|f'$. اما نتیجه به دست آمده از این مطلب، کمتر یا مساوی بودن درجه‌ی f با درجه f' است که با این مطلب که f دارای درجه بیشتر از درجه f' است در تناقض است. ■

مثال ۱.۱.۱۹ هر توسیع جبری از $\mathbb{Q}$ جدایی پذیر است.

تعریف ۲۰.۱.۱ اگر L یک توسیع جدایی پذیر از درجه متناهی از میدان K باشد؛ آنگاه مولفه t در L وجود دارد به‌طوری که $L = K(t)$؛ t را عنصر اولیه L روی K گوییم.

تعریف ۲۱.۱.۱ توسیع جبری L از K را توسیع گالوا[۲] نامیم هرگاه L نرمال و جدایی پذیر روی K باشد.

تعریف ۲۲.۱.۱ مجموعه همه K−خودریختی‌ها از یک توسیع گالوا L روی K را گروه گالوای[۳] L روی K نامیم؛ و آن‌را با $\mathrm{Gal(L|K)}$ نمایش می‌دهیم.

اگر $[L : K] = n$ آنگاه $\mathrm{Gal(L|K)}$ دقیقا n عضو دارد.

تعریف ۲۳.۱.۱ توسیع $L|K$ و $G = \mathrm{Gal(L|K)}$ را در نظر می‌گیریم. برای هر زیر گروه H از G، فرض کنیم

$$H' = \{u \in L \mid \sigma(u) = u, \sigma \in H\}$$

H' را میدان ثابت H نسبت به L روی K می‌نامیم.

قضیه ۲۴.۱.۱ توسیع $L|K$ و $G = \mathrm{Gal(L|K)}$ را در نظر می‌گیریم. برای هر زیر گروه H از G، فرض کنیم H' میدان ثابت H نسبت به L روی K باشد؛ موارد زیر برقرار است:

(۱) $\langle i_L \rangle' = L$ (i_L همانی L است).

(۲) اگر $H \subseteq J$ زیر گروه‌های G باشند؛ آنگاه $H'|J'$.

(۳) اگر H زیر گروهی از G باشد، آنگاه $H'|K$ و $L|H'$ (H' یک میدان میانی L روی K است).

---

[۲] Galois extension

[۳] Galois group

برهان. به[۲۷]، قضیه ۴.۱ مراجعه شود. ■

تعریف ۲۵.۱.۱ فرض کنیم K یک میدان و L توسیع جدایی پذیر از درجه n باشد بنابراین n، $K-$یکریختی مجزای $\sigma_۱ = \varepsilon, \sigma_۲, \cdots, \sigma_n$ از L بتوی بستار جبری $\bar{K}$ از K وجود دارد (متذکر می‌شویم ε نمایش نگاشت همانی است).

اگر $x \in L$ اثر x به صورت زیر تعریف می‌شود:

$$Tr_{L|K}(x) = \sum_{i=۱}^{n} \sigma_i(x)$$

ونرم x برابر است با:

$$N_{L|K}(x) = \prod_{i=۱}^{n} \sigma_i(x)$$

توجه داریم که

$$Tr_{L|K}(x+y) = Tr_{L|K}(x) + Tr_{L|K}(y)$$

و

$$N_{L|K}(xy) = N_{L|K}(x) \cdot N_{L|K}(y)$$

اگر $K \subseteq L \subseteq L'$ میدان باشند و L' روی K جدایی پذیر باشد؛ خاصیت تعدی برای اثر و نرم به صورت زیر برقرار است

$$Tr_{L|K}(Tr_{L'|L}(x)) = Tr_{L'|K}(x)$$

و

$$N_{L|K}(N_{L'|L}(x)) = N_{L'|K}(x)$$

تعریف ۲۶.۱.۱ فرض کنیم K یک میدان و L توسیع جدایی پذیر از درجه n باشد، و $(x_1, \ldots, x_n)$، یک n−تایی از عناصر L باشد؛ مبین آن‌را به صورت زیر تعریف می‌کنیم:

$$\mathrm{discr}_{L|K}(x_1, \ldots, x_n) = \det(Tr_{L|K}(x_i x_j))$$

که در واقع دترمینان ماتریسی است که به ازای $i, j = 1, \ldots, n$ درایه (i,j)ام آن برابر $Tr_{L|K}(x_i x_j)$ است.

بیان دیگری از تعریف مبین با توجه به K−یکریختی‌های $\sigma_1, \ldots, \sigma_n$ از L به‌صورت زیر به دست می آید:

$$\mathrm{discr}_{L|K}(x_1, \ldots, x_n) = (\det(\sigma_i(x_j)))^2$$

تعریف ۲۷.۱.۱ اگر $f(x) \in K[x]$ یک چند جمله‌ای از درجه n با ریشه‌های $x_1, \ldots, x_n$ و ضریب پیشرو a_0 باشد؛ مبین آن‌را به صورت زیر تعریف می‌کنیم:

$$\mathrm{discr}(f) = a_0^{2n-2} \prod_{i<j} (x_i - x_j)^2 = (-1)^{n(n-1)/2} a_0^{2n-2} \prod_{i \neq j} (x_i - x_j)$$

بنابراین $\mathrm{discr}(f) \in K$ و $\mathrm{discr}(f) \neq 0$ اگر و تنها اگر ریشه‌های f مجزا باشد.

محاسبه مبین یک چند جمله‌ای تحویل ناپذیر $f = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ بدون دانستن ریشه‌های آن اهمیت دارد.

فرض کنیم به ازای $k = 0, 1, 2, \ldots$، $p_k = x_1^k + \cdots + x_n^k$ باشد (که $x_1, \ldots, x_n$ ریشه‌های f می‌باشند)؛ در این‌صورت $p_0 = n$ و $p_1 = \frac{-a_1}{a_0}$ و به همین ترتیب p_2 و p_3 و... به‌طور بازگشتی با

استفاده از فرمول نیوتن[۴] محاسبه می‌شود. آنگاه:

$$discr(f) = a_0^{2n-2}\begin{vmatrix} p_0 & p_1 & \cdots & p_{n-1} \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & \cdots & p_{2n-2} \end{vmatrix}$$

در این‌جا منظور از علامت | |، دترمینان ماتریس است.

گاهی اوقات محاسبه دترمینان فوق مشکل است؛ بنابراین از رابطه زیر استفاده می‌کنیم

$$\mathrm{discr(f) = (-1)^{n(n-1)/2}a_0^{n-2}N_{K(x)|K}(f'(x))}$$

که x ریشه‌ای از f و f' نمایش مشتق f است.

تعریف ۲۸.۱.۱ دو چند جمله‌ای

$$f = a_0x^m + a_1x^{m-1} + \cdots + a_m$$

و

$$g = b_0x^n + b_1x^{n-1} + \cdots + b_n$$

که $a_i, b_j \in K$ و $a_0b_0 \neq 0$ و $m, n > 0$ را در نظر می‌گیریم. برایند f و g به صورت زیر تعریف می‌شود:

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \cdots & a_m & 0 & 0 & \cdots & 0 & 0 & \cdots \\ 0 & a_0 & \cdots & a_{m-1} & a_m & 0 & \cdots & 0 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ b_0 & b_1 & \cdots & \cdots & \cdots & \cdots & \cdots & b_n & 0 & \cdots \\ 0 & b_0 & \cdots & \cdots & \cdots & \cdots & \cdots & b_{n-1} & b_n & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{vmatrix}$$

---

[۴] Newton formulas