
بسم الله الرحمن الرحيم

دانشکدهٔ علوم پایه
گروه آموزشی ریاضی

پایان نامه برای دریافت درجه کارشناسی ارشد در رشته ریاضی محض گرایش جبر

عنوان:

کدهای دوری از طول p^k روی $GR(p^2, m)$

استاد راهنما:
دکتر کریم سامعی

نگارش:
حسن طبیبانی

۲۹ بهمن ۱۳۹۳

کلیه امتیازهای این پایان‌نامه به دانشگاه بوعلی سینا تعلق دارد. در صورت استفاده از تمام یا بخشی از مطالب این پایان‌نامه در مجلات، کنفرانس‌ها و یا سخنرانی‌ها، باید نام دانشگاه بوعلی سینا یا استاد راهنمای پایان‌نامه و نام دانشجو با ذکر مأخذ و ضمن کسب مجوز کتبی از دفتر تحصیلات تکمیلی دانشگاه ثبت شود. در غیر این صورت مورد پیگرد قانونی قرار خواهد گرفت. درج آدرس‌های ذیل در کلیه مقالات خارجی و داخلی مستخرج از تمام یا بخشی از مطالب این پایان‌نامه در مجلات، کنفرانس‌ها و یا سخنرانی‌ها الزلمی می‌باشد.

مقالات خارجی

……..……, **Bu-Ali Sina University, Hamedan, Iran.**

مقالات داخلی

.....، .....، گروه .....، دانشکده .....، دانشگاه بوعلی سینا، همدان.

باسمه تعالی

صورت‌جلسه دفاع از پایان‌نامه کارشناسی ارشد

پایان‌نامه کارشناسی ارشد رشته ریاضی محض گرایش جبر

با عنوان:

کدهای دوری از طول p^k روی $GR(p^2,m)$

جلسه دفاع از پایان‌نامه آقای **حسن طبیبانی** به ارزش ۶ واحد در روز **چهارشنبه** مورخ ۱۳۹۳/۱۱/۲۹ ساعت ۱۱ در محل **آمفی تئاتر ۱** دانشکده **علوم پایه** در حضور هیأت داوران برگزار گردید که پس از بررسی‌های لازم، پایان‌نامه نامبرده با نمره به عدد **۱۹/۰۰** به حروف **نوزده تمام** و با درجه **عالی** مورد ارزیابی قرار گرفت.

ردیف	نام و نام خانوادگی	سمت	مرتبه علمی	امضاء
۱	دکتر کریم سامعی	استاد راهنما	دانشیار	
۲	دکتر اشرف دانشخواه	داور داخلی	دانشیار	
۳	دکتر غلامرضا صفاکیش همدانی	داور داخلی	استادیار	
۴	دکتر بهروز رفیعی	★ مسئول تحصیلات تکمیلی دانشکده	دانشیار	

★ بدون حق رأی

تقدیم به

پدر و مادر مهربانم

خدایا... [1] به من زیستنی عطا کن که در لحظه مرگ، بر بی‌ثمری لحظه‌ای که برای زیستن گذشته است، حسرت نخورم و مُردنی عطا کن که بر بیهودگیش، سوگوار نباشم. بگذار تا آن را، خود انتخاب کنم، اما آنچنان که تو دوست می‌داری. تو می‌دانی و همه می‌دانند که شکنجه دیدن بخاطر تو، زندانی کشیدن بخاطر تو و رنج بردن به پای تو تنها لذت بزرگ زندگی من است، از شادی توست که من در دل می‌خندم، از امید رهایی توست که برق امید در چشمان خسته‌ام می‌درخشد و از خوشبختی توست که هوای پاک سعادت را در ریه‌هایم احساس می‌کنم. نمی‌توانم خوب حرف بزنم. نیروی شگفتی را که در زیر کلمات ساده و جمله‌های ضعیف و افتاده، پنهان کرده‌ام دریاب، دریاب.

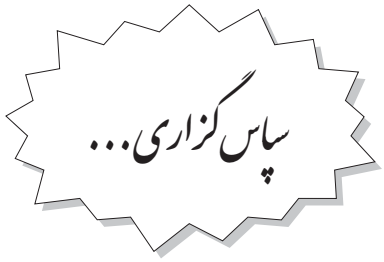
تو می‌دانی و همه می‌دانند که زندگی از تحمیل لبخندی بر لبان من، از آوردن برق امیدی در نگاه من، از برانگیختن موج شعفی در دل من، عاجز است.

تو، چگونه زیستن را به من بیاموز، چگونه مردن را خود خواهم آموخت.

به من توفیق تلاش در شکست، صبر در نومیدی، رفتن بی‌همراه، جهاد بی‌سلاح، کار بی‌پاداش، فداکاری در سکوت، دین بی‌دنیا، مذهب بی‌عوام، عظمت بی‌نام، خدمت بی‌نان، ایمان بی‌ریا، خوبی بی‌نمود، گستاخی بی‌خامی، قناعت بی‌غرور، عشق بی‌هوس، تنهایی در انبوه جمعیت، و دوست داشتن بی‌آنکه دوست بداند، روزی کن.

---

[1] مناجاتی از دکتر علی شریعتی.



زندگی یک جاده است. وقتی دلت هوای رفتن می کند.

یک آسمان آبی است، وقتی هوای پریدن می کنی. وقتی هوای به اوج رسیدن، در سلول سلول بدنت جا باز می کند.

زندگی یک درخت است وقتی هوای نشستن داری هوای آرامیدن، هوای نفس تازه کردن.

زندگی دیروز است. فردا است. همه وقت است.

وقتی است که کسی صدایت می زند، یا کسی در خاطرت است.

یک آواز بلند از سر شوق است.

زندگی، پدر است وقتی روبرویت از خستگی کار می نشیند و می پرسد: «خوبی؟» و تو خوب می شوی.

زندگی، مادر است وقتی بی تاب آمدنت است و شال دستانش را دور گردنت می اندازد و تو از سرمای همه زمستان ها، همه تنهایی ها، گرم می شوی.

زندگی این واژه هاست:

پرنده

آسمان

رسیدن و...

همین واژه‌ی سپاس.

پس به نام یک بی‌پایان به یاد همه‌ی خوبی‌ها سپاسگزاری می‌کنم از:
پدر و مادر عزیزم،
استاد ارجمندم،
برادر عزیزم و
دوست صمیمی‌ام...

ابتدا وظیفه خود می‌دانم از آموزش‌ها و زحمات بی‌دریغ استاد راهنمای فرهیخته و فرزانه علمی و اخلاقی خود، جناب آقای دکتر کریم سامعی [۲] صمیمانه تشکر و قدردانی کنم که با صبر فراوان و صرف وقت زیاد، همواره راهنما و راه‌گشای بنده در طول تحصیل و تکمیل این رساله بوده است. از خانم دکتر اشرف دانشخواه و جناب آقای دکتر غلامرضا صفاکیش همدانی که زحمت مطالعه این پایان نامه را تقبل فرمودند و نکته‌های ارزنده خودشان را نسبت به بنده در دوران تحصیل روا داشتند، کمال امتنان و تشکر را دارم.

حسن طبیبانی
همدان- ایران

[۲] Samei@ipm.ir

دانشگاه بوعلی سینا

مشخصات رساله/پایان نامه تحصیلی

عنوان:

کدهای دوری از طول p^k روی $GR(p^2,m)$

نام نویسنده: حسن طبیبانی

نام استاد/اساتید راهنما: دکتر کریم سامعی

نام استاد/اساتید مشاور: -

دانشکده: علوم پایه	**گروه آموزشی: ریاضی**	
رشته تحصیلی: ریاضی محض	**گرایش تحصیلی: جبر**	**مقطع تحصیلی: کارشناسی ارشد**
تاریخ تصویب پروپوزال:۱۳۹۲/۰۷/۱۵	**تاریخ دفاع: ۱۳۹۳/۱۱/۲۹**	**تعداد صفحات: ۷۰**

چکیده:

در این پایان نامه کدهای دوری به طول p^k روی حلقه گالوای $GR(p^2,m)$ (یا به طور معادل، ایده آل های حلقه $GR(p^2,m)[u]/\langle u^{p^k}-1\rangle$) مطالعه می شوند، که در آن m,k اعداد صحیح مثبت و p عددی اول است. برای هر ایده آل $GR(p^k,m)[u]/\langle u^{p^k}-1\rangle$ یک مولد یکتا ارائه می شود؛ که هر عضو آن ایده آل، به صورت ترکیبی یکتا از مولدها با ضرایب در میدان تیخ مولر متناظر نوشته می شود. همچنین دوگان های این حلقه، مورد تجزیه و تحلیل قرار گرفته و کدهای خود دوگان به طور کامل مشخص می گردد.

واژه‌های کلیدی: کدهای دوری، حلقه گالوا

فهرست مطالب

مقدمه

با پیشرفت الکترونیک و تکنولوژی کامپیوتر و میسر شدن ارتباطات از فواصل بسیار دور از طریق ماهواره، ارتباطات که در قدیم مطلقاً به صورت مکالمه حضوری یا از طریق مکاتبه انجام می‌گرفت، به‌طور کلی دگرگون شد و ارتباطات صوتی و تصویری نیز مطرح گردیده و در نتیجه ارتباطات از حساسیت بسیار برخوردار شد و در این راستا مشکلات جدیدی نیز مطرح شدند.

در اواسط جنگ جهانی دوم چند ریاضیدان بزرگ و در راس آن‌ها کلود شانون[۳] بررسی جامعی را درباره اصول ارتباطات شروع کردند. حاصل این بررسی در سال ۱۹۴۸ طی چند مقاله منتشر شده و انقلابی را در علم ارتباطات پدید آورد، به‌طوری‌که از آن زمان تا به حال ارتباطات بر مبنای نظریات شانون پیشرفت‌های عظیمی کرده است. بررسی شانون چند جنبه داشت، شاید مهمترین جنبه کار او یک بررسی عمیق درباره تعریف مفوم «اطلاعات» و روش‌های اندازه‌گیری آن بود. یکی دیگر از جنبه‌های کار او را می‌توان در این جمله خلاصه کرد: «مساله اصلی ارتباطات بازسازی دقیق یا تقریبی پیامی است که در نقطه‌ای دیگر انتخاب شده است.»

یکی از کاربردهای عمده میدان‌های متناهی، نظریه کدگذاری است. ابداع این نظریه نیز به قضیه معروفی از شانون بر می‌گردد که وجود کدهایی را تضمین می‌کند که می‌توانند اطلاعات را به میزانی نزدیک به حداکثر ظرفیت کانال ارتباطی و با احتمال خطایی به اندازه کوچک انتقال دهند. یکی از هدف‌های نظریه جبری کدگذاری، یعنی نظریه کدهای آشکارساز و تصحیح کننده خطا، ابداع روش‌هایی برای ساخت چنین کدهایی است. در خلال دو دهه اخیر ابزارهای مجرد جبری بیشتر و بیشتری مانند نظریه میدان‌های متناهی و نظریه چندجمله‌ای‌های روی میدان‌های متناهی در کدگذاری اثر گذاشته‌اند. به‌ویژه، توصیف کدهای افزونه به‌وسیله چندجمله‌ای‌ها روی $\mathbb{F}_q$ نقطه عطفی در این تاثیرگذاری بوده است. این نکته که می‌توان ثبات‌های تغییر مکان را در کدگذاری و کدگشایی به کار برد، رابطه بین این مبحث و دنباله‌های بازگشتی خطی برقرار می‌کند. در مبحث از نظریه جبری کدگذاری، هیچ یک از مساله‌های عملی یا تکنیکی به کارگیری کدها را مطرح نمی‌کنیم، بلکه به مطالعه ویژگی‌های بنیادی کدهای بلوکی و توصیف برخی از رده‌های جالب کدهای بلوکی اکتفا می‌کنیم.

مسئله مخابره اطلاعات به‌ویژه کدگذاری و کدگشایی اطلاعات با هدف انتقال بی‌خطای آن‌ها از طریق

[۳] shannon

کانالی نوفه‌دار، امروزه اهمیت بسیاری دارد. مساله از این نوع است که می‌خواهیم پیامی متشکل از دنباله‌ای متناهی از نمادها را، که عضوهای الفبایی متناهی‌اند، منتقل کنیم. به‌عنوان مثال اگر الفبا تنها از ۰ و ۱ تشکیل شده باشد، پیام را می‌توان به صورت عددی دودویی توصیف کرد. معمولا فرض بر این است که الفبا میدانی متناهی است. یکی از شگردهای اساسی در نظریه کدگذاری جبری، انتقال اطلاعات افزونه به انضمام پیامی است که قرار بر انتقال آن است، یعنی تبدیل دنباله نمادهای پیام به‌طور روشمند به دنباله‌ای درازتر. فرض می‌کنیم نمادهای پیام و نمادهای پیام کدگذاری شده عضوهایی از میدان‌های متناهی یکسانی هستند. منظور از کدگذاری متناظر سازی بلوک متشکل از k حرف پیام مثلا $a_1a_2\cdots a_k$ که $a_i \in \mathbb{F}_q$ با کد واژه‌ای مثلا $c_1c_2\cdots c_n$ که $n \geq k$ متشکل از n نماد $c_j \in \mathbb{F}_q$ است. کدواژه را به صورت بردار سطری n بعدی cای در $\mathbb{F}_q^n$ در نظر می‌گیریم. بنابراین، f تابعی از $\mathbb{F}_q^k$ به $\mathbb{F}_q^n$ است، که آن را طرح کدگذاری[۴] و $g : \mathbb{F}_q^n \to \mathbb{F}_q^k$ را طرح کدگشایی[۵] می‌نامیم.

گونه به‌ویژه جالبی از کدهای خطی، کد دوری است، یعنی کدی خطی که تحت تغییر مکان‌های دوری ناورداست. بعبارتی کدهای دوری یک دسته از کدهایی هستند که از دیدگاه نظری و عملی مهم هستند. در گذشته کدهای دوری روی میدان‌های متناهی مطالعه شده است. در حالی که بعضی کدهای غیر خطی روی $\mathbb{Z}_2$ هستند که می توان آن ها را به صورت تصویری از یک نگاشت خطی از کدهای دوری روی $\mathbb{Z}_4$ نمایش داد. این موضوع ما را به مطالعه کدهای دوری روی حلقه‌های متناهی سوق داد. روش توصیف کدهای دوری از طول N روی یک حلقه R ، شبیه یک میدان متناهی، و در واقع، آن‌ها ایده‌آل‌های حلقه‌های چندجمله‌ای می‌باشند. بنابراین برای توصیف کدهای دوری روی $\mathbb{Z}_{p^e}$ ، همان ایده‌آل‌های حلقه بررسی می‌شوند.

در سال ۲۰۰۳ بلکفورد[۶] در مرجع [۵] وقتی که کدهای دوری از طول $2n$ (که n فرد باشد)، روی $\mathbb{Z}_4$ را مطالعه می‌کرد، حلقه چندجمله‌ای $\mathbb{Z}_4[X]/\langle X^4 - 1\rangle$ را در نظر گرفت و کدهای دوری با طول $2n$ روی $\mathbb{Z}_4$ را شناسایی کرد. در ادامه همین مقاله سال ۲۰۰۶ دوگرتی[۷] و لینگ [۸] در مرجع [۶] نتایج بیشتری از کدهای دوری روی $\mathbb{Z}_4$ با طول زوج را به دست آوردند و توانستند دوگان های آن‌ها را بنویسند. اما سال ۲۰۰۷ دوگرتی و پارک [۹] در مرجع [۷] یک نتیجه کلیدی را ثابت کردند که حلقه $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ با جمع مستقیم حلقه‌هایی به شکل $GR(p^e, m)[u]/\langle u^{p^k} - 1\rangle$ یکریخت است که در آن $GR(p^e, m)$ نمایش حلقه گالوا از مشخصه p^e با $(p^e)^m$ عضو می‌باشد و k بزرگترین عدد صحیح است به طوری‌که p^k ، N را می شمارد. از این رو کافیست ایده‌آل‌های حلقه $GR(p^e, m)[u]/\langle u^{p^k} - 1\rangle$، مورد مطالعه قرار گیرند.

این پایانامه در ۳ فصل تهیه و تنظیم شده است و مطالب آن عمدتاً از مراجع [۵، ۶، ۱۱] و [۸] که

[۴] Coding scheme
[۵] Decoding scheme
[۶] T. Blackford
[۷] S.T. Dougherty
[۸] S. Ling
[۹] Y.H. Park

مرجع اصلی ماست، استفاده شده است:

فصل ۱ تعاریف و مفاهیم مقدماتی از نظریه حلقه‌ها و میدان‌های متناهی و نظریه جبری کدگذاری بیان شده است.

فصل ۲ در این فصل حلقه‌های گالوا و توسیع آن‌ها به طور کامل شرح داده می‌شوند، و همچنین ارتباط حلقه‌های گالوا با نظریه کدگذاری، از مشخصه ۴، بیان می‌گردند.

فصل ۳ در این فصل ابتدا کدهای تابدار و مانده‌ای معرفی می‌شوند، سپس نمایش یکتایی از مولدها برای ایده‌آل‌های $GR(p^2, m)[u]/\langle u^{p^k}-1\rangle$ اثبات و همچنین همه ایده‌آل‌های حلقه $GR(p^e, m)[u]/\langle u^{p^k}-1\rangle$ با نمایش جدیدی، بیان می‌شوند. و در ادامه، شکل دوگان این ایده‌آل‌ها، مشخص و محاسبه می گردند.

فصل ۱
مقدماتی از نظریه حلقه‌ها و میدان‌های متناهی

در این فصل مفاهیم بنیادی جبری را مرور خواهیم کرد. هدف ما علاوه بر یادآوری، فراهم آوردن اصطلاحات، علامت‌ها و مقدماتی است که در فصل‌های آتی مورد نیاز خواهند بود، می‌باشد. بخش اول به تعریف‌ها و نتایج مقدماتی از مراجع [۱، ۲] اختصاص دارد. در بخش دوم مفاهیمی از نظریه جبری کدگذاری از مراجع [۲، ۹] بیان خواهد شد. توجه کنید، در کل این پایان‌نامه حلقه‌ها جابه‌جایی و یکدار می‌باشند.

۱.۱ مقدماتی از جبر

تعریف ۱.۱.۱. فرض کنید R یک حلقه جابه‌جایی و $q \in R$، در این صورت q عضو تحویل‌ناپذیر است هرگاه:

الف) q ناصفر و غیر یکه باشد،

ب) اگر q به صورت $q = ab$ با $a, b \in R$ نوشته شود، آنگاه یا a یا b یک عضو یکه در R باشد.

قضیه ۲.۱.۱. *فرض کنید R یک حلقه جابه‌جایی باشد و $a \in R$. در این صورت a عضو وارون‌پذیر R است اگر وتنها اگر به ازای هر ایده‌آل ماکسیمال $\mathfrak{m}$ از R داشته باشیم $a \notin \mathfrak{m}$، یعنی اگر و تنها اگر a بیرون از هر ایده‌آل ماکسیمال R واقع باشد.*

برهان. قضیه ۱۱.۳ در مرجع [۱] را ببینید. ■

تعریف ۳.۱.۱. هر حلقه جابه‌جایی R که دقیقاً یک ایده‌آل ماکسیمال چون $\mathfrak{m}$ دارد، شبه موضعی نامیده می‌شود.
در این حالت، میدان $K = \frac{R}{\mathfrak{m}}$، را میدان‌مانده‌ای R می‌گوییم.

تعریف ۴.۱.۱. هر حلقه جابه‌جایی R، موضعی نامیده می‌شود، هرگاه نوتری و شبه‌موضعی باشد.

لم ۱.۱.۵. *فرض کنید a یک عضو پوچ‌توان از حلقه جابه‌جایی R باشد، در این صورت $1+a$ یک عضو وارون‌پذیر R است. همچنین به ازای هر عضو یکه u از R، $u+a$ یک عضو وارون‌پذیر R است.*

برهان. فرض کنید a پوچ‌توان باشد، پس $n \in \mathbb{N}$ وجود دارد که $a^n = 0$. در این صورت

$$1 = 1 + (-1)^n a^n = (1+a)(1 - a + a^2 + \cdots + (-1)^{n-1}a^{n-1})$$

لذا $1+a$ یکه است.

حال اگر u یکه و a پوچ‌توان باشد، آنگاه $u^{-1}a$ نیز پوچ‌توان است، زیرا

$$(u^{-1}a)^n = (u^{-1})^n a^n = 0$$

لذا از قسمت اول $1 + u^{-1}a$ یکه است و با توجه به یکه بودن u، عنصر $u + a = u(1 + u^{-1}a)$ نیز یکه است. ■

گزاره ۱.۱.۶. *فرض کنید R حلقه‌ای جابه‌جایی و X مجهول است و*

$$f = r_0 + r_1 X + \ldots + r_n X^n \in R[X]$$

الف) f یک عضو وارون‌پذیر $R[X]$ است اگر وتنها اگر r_0 یک عضو وارون‌پذیر R باشد و $r_1, \ldots, r_n$ همه پوچ‌توان باشند.

ب) f پوچ‌توان است اگر وتنها اگر $r_0, r_1, \ldots, r_n$ پوچ‌توان باشند.

پ) f در $R[X]$ مقسوم‌علیه صفر است اگر و تنها اگر عضوی چون $c \in R$ وجود داشته باشد که $c \neq 0$ ولی $cf = 0$.

برهان. گزاره ۳۶.۱ در مرجع [۱] را ببینید. ■

لم ۱.۱.۷. *فرض کنید $f : R \to S$ همریختی پوشای حلقه‌ها و برای هر ایده‌آل I از R که $I \supseteq kerf$ باشد، در این صورت داریم:*

$$\frac{R}{I} \simeq \frac{S}{I^e}$$

که در آن $I^e = \langle f(I) \rangle$ ایده‌آل توسیع[۱] نامیده می‌شود.

برهان. لم ۷.۴ در مرجع [۱] را ببینید. ■

تعریف ۱.۱.۸. فرض کنید I و J ایده‌آل‌های حلقه جابه‌جایی R باشند. حاصل تقسیم یا خارج قسمت $(I : J)$ بصورت $(I : J) = \{a \in R \ : \ aJ \subseteq I\}$ تعریف می شود. که ایده‌آل R است و $I \subseteq (I : J)$.

در حالت خاص $I = 0$، حاصل تقسیم

[۱] extension

$$Ann(J) = (\circ : J) = \{a \in R \ : \ aJ = \circ\} = \{a \in R \ : \ ab = \circ, b \in J\}$$

را پوچساز J می‌نامیم.

قضیه ۹.۱.۱. *هر دامنه ایده‌آل اصلی، دامنه تجزیه یکتاست.*

برهان. لم ۳۹.۳ در مرجع [۱] را ببینید. ■

گزاره ۱۰.۱.۱. *اگر K میدان باشد، آنگاه $K[X]$ یک دامنه ایده‌آل اصلی است.*

برهان. قضیه ۵۴.۱ در مرجع [۲] را ببینید. ■

لم ۱۱.۱.۱. *تمام ایده‌آل‌های ماکسیمال حلقه $K[X]$ که در آن K میدان است، به صورت مجموعه زیر می باشد:*

$$Max(K[X]) = \{\langle f\rangle \ : \ f \in K[X], \quad f \text{ تحویل‌ناپذیر است}\}.$$

برهان. لم ۳۴.۳ در مرجع [۱] را ببینید. ■

تبصره ۱۲.۱.۱. *در حلقه رده‌مانده‌ای $\frac{\mathbb{F}[X]}{\langle f\rangle}$ که در آن $\mathbb{F}$ میدان، $f \in \mathbb{F}[X]$ و $deg(f) = n$ است، داریم:*

$$\frac{\mathbb{F}[X]}{\langle f\rangle} = \{a_\circ + a_1 X + \cdots + a_{n-1}X^{n-1} + \langle f\rangle \ : \ a_i \in \mathbb{F}; \circ < \forall i < n-1\}.$$

زیرا

$$\frac{\mathbb{F}[X]}{\langle f\rangle} = \{g + \langle f\rangle \ : \ g \in \mathbb{F}[X]\}$$

طبق قضیه الگوریتم تقسیم، وجود دارد $q, r \in \mathbb{F}[X]$ که $g = fq + r$ و $deg(r) < deg(f) = n$

لذا $g + \langle f\rangle = fq + r + \langle f\rangle = r + \langle f\rangle$ و در نتیجه

$$\frac{\mathbb{F}[X]}{\langle f\rangle} = \{r + \langle f\rangle \ : \ r \in \mathbb{F}[X] \ , \ deg(r) < n\}$$

اکنون اگر $f(X) = X^n$ آنگاه

$$\frac{\mathbb{F}[X]}{\langle X^n\rangle} = \{a_\circ + a_1 X + \cdots + a_{n-1}X^{n-1} + \langle X^n\rangle \ : \ a_i \in \mathbb{F} \ ; \ \circ < \forall i < n-1\}$$

و اگر قرار دهیم $x = X + \langle X^n\rangle$ آنگاه

$$\frac{\mathbb{F}[X]}{\langle X^n\rangle} = \{a_\circ + a_1 x + \cdots + a_{n-1}x^{n-1} \ : \ a_i \in \mathbb{F} \ ; \ \circ < \forall i < n-1, x^n = \circ\}$$

چون که $x^n = (X + \langle X^n\rangle)^n = X^n + \langle X^n\rangle = \circ_{\mathbb{F}[X]/\langle X^n\rangle}$.

تعریف ۱.۱.۱۳. فرض کنید p عددی اول، $\mathbb{F}_p$ مجموعه $\{0,1,...,p-1\}$ و نگاشت $\varphi : \frac{\mathbb{Z}}{\langle p\rangle} \to \mathbb{F}_p$ با ضابطه $\varphi([a]) = a$ برای هر $0 \le a \le p-1$ باشد. در این صورت φ یک یکریختی است و $\mathbb{F}_p$ با ساختار میدانی که توسط φ القا می‌شود، میدانی متناهی است و آن را میدان گالوای[۲] مرتبه p می‌نامیم.

تعریف ۱.۱.۱۴. فرض کنید K زیر میدان $\mathbb{F}$ و $\theta \in \mathbb{F}$. اگر θ در معادله چندجمله‌ای غیر بدیهی با ضریب‌های واقع در K صدق کند، یعنی اگر $a_n\theta^n + \cdots + a_1\theta + a_0 = 0$ که $a_i \in K$ آنگاه θ روی K جبری است.

تعریف ۱.۱.۱۵. اگر عضو $\theta \in \mathbb{F}$ روی میدان K جبری باشد، چندجمله‌ای تکین یکتای مولد ایده‌آل $J = \{f \in K[X] : f(\theta) = 0\}$ را چندجمله‌ای مینیمال یا چندجمله‌ای تحویل‌ناپذیر θ روی K می‌نامیم.

تعریف ۱.۱.۱۶. فرض کنید درجه $f \in K[X]$ مثبت و $\mathbb{F}$ توسیعی از میدان K باشد. می‌گوییم f در $\mathbb{F}$ تجزیه می‌شود اگر بتوان f را به صورت حاصل‌ضرب عامل‌های خطی از $\mathbb{F}[X]$ نوشت. یعنی اگر عضوهایی مثل $a_1, a_2, \ldots, a_n \in \mathbb{F}$ وجود داشته باشند به طوری که

$$f(X) = a(X - a_1)(X - a_2)\cdots(X - a_n)$$

که در آن a ضریب پیشرو f است. میدان $\mathbb{F}$ را میدان تجزیه f روی K می‌نامیم.

لم ۱.۱.۱۷. *اگر $\mathbb{F}$ میدانی متناهی با q عضو و K زیر میدانی از $\mathbb{F}$ باشد، آنگاه چندجمله‌ای $X^q - X \in K[X]$ در $\mathbb{F}$ به صورت*

$$X^q - X = \prod_{a\in\mathbb{F}}(X - a)$$

تجزیه می‌شود و $\mathbb{F}$ میدان تجزیه یا شکافنده $X^q - X$ روی K نامیده می‌شود.

برهان. لم ۴.۲ در مرجع [۲] را ببینید. ■

قضیه ۱.۱.۱۸. *به ازای هر میدان متناهی $\mathbb{F}_p$ گروه ضربی $\mathbb{F}_p^*$ متشکل از عضوهای مخالف صفر $\mathbb{F}_p$، دوری است.*

برهان. قضیه ۸.۲ در مرجع [۲] را ببینید. ■

تعریف ۱.۱.۱۹. هر مولد گروه دوری $\mathbb{F}_p^*$ را عضو اولیه $\mathbb{F}_p$ می‌نامیم.

قضیه ۱.۱.۲۰. *فرض کنید $\mathbb{F}_q$ میدان متناهی و $\mathbb{F}_r$ توسیعی متناهی از $\mathbb{F}_q$ باشد. در این صورت $\mathbb{F}_r$ توسیع جبری ساده‌ای از $\mathbb{F}_q$ است و هر عضو اولیه $\mathbb{F}_r$ عضو تعریف کننده $\mathbb{F}_r$ روی $\mathbb{F}_q$ است.*

[۲] Galois Field

برهان. قضیه ۱۰.۲ در مرجع [۲] را ببینید. ■

قضیه ۲۱.۱.۱. *اگر f چندجمله‌ای تحویل‌ناپذیری با درجه m روی $\mathbb{F}_q[X]$ باشد، آنگاه $f(X)$ ریشه‌ای مثل a در $\mathbb{F}_{q^m}$ دارد. بعلاوه، همه ریشه‌های f ساده‌اند و عبارت‌اند از m عضو متمایز $a, a^q, a^{q^2}, ..., a^{q^{m-1}}$ متعلق به $\mathbb{F}_{q^m}$.*

برهان. قضیه ۱۴.۲ در مرجع [۲] را ببینید. ■

نتیجه ۲۲.۱.۱. *اگر f چندجمله‌ای تحویل‌ناپذیری با درجه m روی $\mathbb{F}_q[X]$ باشد، آنگاه $\mathbb{F}_{q^m}$ میدان تجزیه f روی $\mathbb{F}_q$ است.*

برهان. نتیجه ۱۵.۲ در مرجع [۲] را ببینید. ■

قضیه ۲۳.۱.۱. *اگر درجه چندجمله‌ای $f \in \mathbb{F}_q[X]$، برابر m باشد که $m \geq 1$ و $f(0) \neq 0$، آنگاه عدد صحیح مثبتی چون e نابزرگتر از $q^m - 1$ وجود دارد به گونه‌ای که $f(X)$، چندجمله‌ای $X^e - 1$ را بشمارد.*

برهان. لم ۱.۳ در مرجع [۲] را ببینید. ■

تعریف ۲۴.۱.۱. چندجمله‌ای $f \in \mathbb{F}[X]$ با درجه m، که $m \geq 1$، چندجمله‌ای اولیه روی $\mathbb{F}_q$ نامیده می‌شود، اگر چندجمله‌ای مینیمال عضو اولیه‌ای از $\mathbb{F}_{q^m}$ روی $\mathbb{F}_q$ باشد. یا بعبارت دیگر چندجمله‌ای درجه m اولیه روی $\mathbb{F}_q$ چندجمله‌ای تکینی است که روی $\mathbb{F}_q$ تحویل‌ناپذیر است و ریشه αای در $\mathbb{F}_{q^m}$ دارد که گروه ضربی $\mathbb{F}_{q^m}$ را تولید می‌کند.

تعریف ۲۵.۱.۱. اگر چندجمله‌ای $f(X) = a_0 + a_1X + \cdots + a_{n-1}X + a_nX^n \in \mathbb{F}[X]$ و $a_n \neq 0$ آنگاه چندجمله‌ای معکوسه f را با f^* نشان می‌دهیم و به صورت زیر تعریف می‌کنیم:

$$f^*(X) = X^n f(\frac{1}{X}) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n.$$

قضیه ۲۶.۱.۱. *فرض کنید R حلقه جابه‌جایی و متناهی باشد، در این صورت R به طور یکتا با جمع مستقیم از حلقه‌های موضعی متناهی یکریخت است.*

برهان. قضیه ۶.۲ در مرجع [۱۰] را ببینید. ■

۲.۱ مقدماتی از نظریه جبری کدگذاری

۱.۲.۱ کدهای خطی

تعریف ۱.۲.۱. یک کد C به طول n روی حلقه R یک زیر مجموعه از R^n است. اگر کد C یک R-زیرمدول باشد، کد C را یک کدخطی می‌نامیم.

تعریف ۲.۲.۱. مجموعه $C^\perp = \{v \in R^n \ : \ v.w = 0, \forall w \in C\}$ را کد دوگان یا قائم بر کد C می‌نامیم. (که در آن « . » همان ضرب مولفه‌ای است.)

قضیه ۳.۲.۱. *فرض کنید C یک کد خطی با طول n روی $\mathbb{F}_p$ باشد. بعد C بعنوان فضای برداری روی F_q^n را با $dim(C)$ نشان می‌دهیم. در این صورت*

الف) $|C| = p^{dim(C)}$

ب) *$C^\perp$ یک کد خطی و $dim(C) + dim(C^\perp) = n$.*

برهان. قضیه ۴.۲.۴ در مرجع [۹] را ببینید. ■

تعریف ۴.۲.۱. فرض کنید C یک کد خطی باشد.

الف) اگر $C \subseteq C^\perp$ آنگاه کد C را کد خود متعامد می‌نامیم.

ب) اگر $C = C^\perp$ آنگاه کد C را کد خوددوگان می‌نامیم.

تعریف ۵.۲.۱. فرض کنید H ماتریس $(n-k) \times n$ با رتبه $n-k$ و درایه‌های متعلق به $\mathbb{F}_q$ باشد. مجموعه C متشکل از همه بردارهای n بعدی $c \in \mathbb{F}_q^n$ که به ازای آن‌ها $Hc^T = 0$ باشد را (n,k)-کد خطی روی $\mathbb{F}_q$ می‌گوییم، که n طول کد و k بعد کد می‌باشد. و ماتریس H را ماتریس توازن‌سنجی می‌نامیم. بویژه اگر H به صورت $[A, I_{n-k}]$ که در آن A ماتریس $(n-k) \times k$ و I ماتریس همانی است، باشد. آنگاه ماتریس H را ماتریس توازن‌سنجی استاندارد می‌نامیم.

تعریف ۶.۲.۱. ماتریس $G = [I_k, -A^T]_{k \times n}$ را ماتریس مولد استاندارد (n,k)-کد خطی با ماتریس توازن‌سنجی $H = [A, I_{n-k}]$ می‌گوییم.

لم ۷.۲.۱. *فرض کنید C یک (n,k)-کدخطی روی $\mathbb{F}_q$ با ماتریس مولد G باشد. در این صورت $v \in \mathbb{F}_q^n$ متعلق به $C^\perp$ است، اگر و تنها اگر v عمود بر هر سطر G باشد، (یعنی $vG^T = 0 \Leftrightarrow v \in C^\perp$).*
بویژه ماتریس $H_{(n-k)\times n}$ ماتریس توازن‌سنجی برای G است اگر و تنها اگر سطرهای H مستقل خطی و $HG^T = 0$.

برهان. لم ۴.۵.۴ در مرجع [۹] را ببینید. ■

تعریف ۸.۲.۱. فرض کنید X, Y دو بردار در $\mathbb{F}_q^n$ باشند. در این صورت:
الف) فاصله همینگ میان X, Y که با $d(X,Y)$ نشان داده می‌شود، تعداد مولفه‌های متفاوت X, Y است،
ب) وزن (همینگ) X که با $Wt(X)$ نشان داده می‌شود، تعداد مولفه‌های مخالف صفر X است.

لم ۹.۲.۱. *اگر X, Y دو بردار در $\mathbb{F}_q^n$ آنگاه $Wt(X) = d(X, ۰)$ و $d(X,Y) = Wt(X-Y)$.*

برهان. لم ۴.۳.۳ در مرجع [۹] را ببینید. ■

قضیه ۱۰.۲.۱. *فرض کنید C یک کدخطی روی $\mathbb{F}_q$ باشد. در این صورت $d(C) = Wt(C)$.*

برهان. لم ۴.۳.۸ در مرجع [۹] را ببینید. ■

لم ۱۱.۲.۱. *اگر R یک حلقه جابه‌جایی باشد، آنگاه نگاشت*

$$\varphi : R^n \to \frac{R[X]}{\langle X^n \rangle}$$
$$\varphi(a_۰, a_۱, \cdots, a_{n-۱}) = a_۰ + a_۱x + \cdots + a_{n-۱}x^{n-۱}$$

یک R- یکریختی است. که در آن $x = X + \langle X^n - ۱ \rangle$ و $x^n = ۰$ می‌باشد.

نتیجه ۱۲.۲.۱. *اگر $C \subseteq R^n$ یک کد خطی روی حلقه R باشد، آنگاه می‌توان اعضای آن را با یک چندجمله‌ای از درجه $n-۱$، از مدول $\frac{R[X]}{\langle X^n \rangle}$ یکی در نظر گرفت.*

۲.۲.۱ کدهای دوری

تعریف ۱۳.۲.۱. (n,k)-کدخطی C روی $\mathbb{F}_q$ دوری نامیده می‌شود اگر گزاره $(a_۰, a_۱, \ldots, a_{n-۱}) \in C$، گزاره $(a_{n-۱}, a_۰, \ldots, a_{n-۲}) \in C$ را ایجاب کند.

لم ۱۴.۲.۱. *فرض کنید $gcd(n,q) = ۱$ و $\langle X^n - ۱ \rangle$ ایده‌آل تولید شده توسط $X^n - ۱ \in \mathbb{F}_q[X]$ باشد. در این صورت همه عضوهای $\frac{\mathbb{F}_q[X]}{\langle X^n - ۱ \rangle}$ را می‌توان به صورت چندجمله‌ای‌های با درجه کمتر از n نشان داد که این حلقه رده‌مانده‌ای به عنوان فضای برداری روی $\mathbb{F}_q$ با $\mathbb{F}_q^n$ به صورت*

$$\varphi : \mathbb{F}_q^n \to \frac{\mathbb{F}_q[X]}{\langle X^n - ۱ \rangle}$$
$$\varphi(a_۰, a_۱, ..., a_{n-۱}) = a_۰ + a_۱x + ... + a_{n-۱}x^{n-۱}$$

یکریخت است. که در آن $x = X + \langle X^n - ۱ \rangle$ و $x^n = ۱$ می‌باشد.