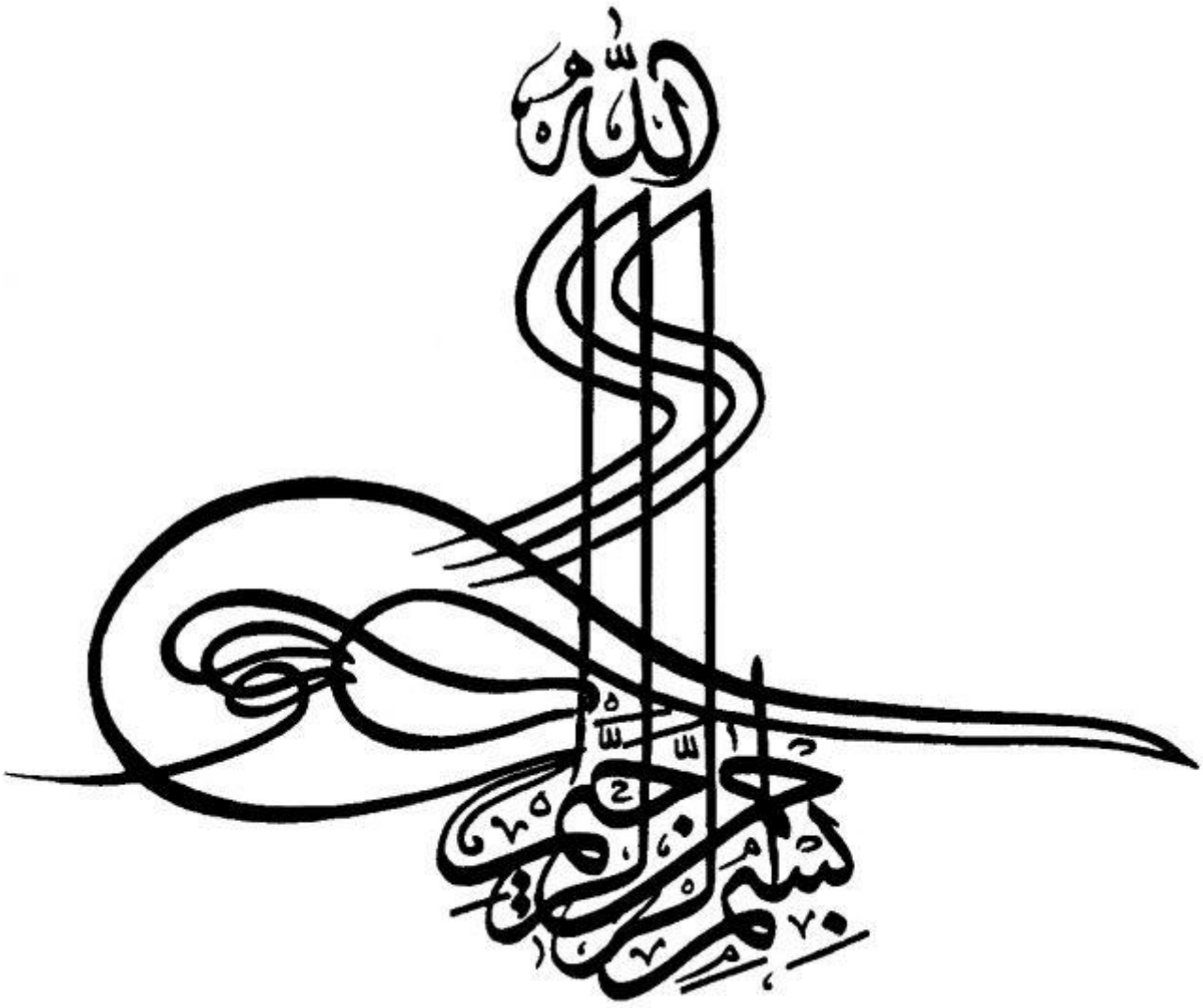
الله
بسم الله الرحمن الرحيم

دانشکده‌ی علوم ریاضی
گروه ریاضیات و کاربردها

پایان‌نامه برای دریافت درجه کارشناسی ارشد
در رشته‌ی ریاضی محض گرایش جبر

عنوان:

بررسی ساختار کدهای خطی و دوری روی حلقه‌های زنجیری

استاد راهنما:

دکتر ناصر زمانی

اساتید مشاور:

دکتر احمد خوجالی بارنجی
دکتر محمد باقر مقیمی

پژوهشگر:

سیده آرزو سیدابراهیمی

شهریور۱۳۹۲

تعهدنامه‌ی اصالت اثر و رعایت حقوق دانشگاه

تمامی حقوق مادی و معنوی مترتب بر نتایج، ابتکارات، اختراعات و نوآوری‌های ناشی از انجام این پژوهش، متعلق به **دانشگاه محقق اردبیلی** می‌باشد. نقل مطلب از این اثر، با رعایت مقررات مربوطه و با ذکر نام دانشگاه محقق اردبیلی، نام استاد راهنما و دانشجو بلامانع است.

اینجانب سیده آرزو سیدابراهیمی دانش‌آموخته مقطع کارشناسی ارشد رشته‌ی ریاضی محض گرایش جبر دانشکده‌ی علوم ریاضی دانشگاه محقق اردبیلی به شماره‌ی دانشجویی ۹۰۲۲۴۱۳۱۱۱ که در تاریخ ۹۲/۰۶/۲۷ از پایان‌نامه‌ی تحصیلی خود تحت عنوان "بررسی ساختار کدهای خطی و دوری روی حلقه‌های زنجیری" دفاع نموده‌ام، متعهد می‌شوم که:

۱) این پایان‌نامه را قبلاً برای دریافت هیچ‌گونه مدرک تحصیلی یا به عنوان هرگونه فعالیت پژوهشی در سایر دانشگاه‌ها و مؤسسات آموزشی و پژوهشی داخل و خارج از کشور ارائه ننموده‌ام.

۲) مسئولیت صحّت و سقم تمامی مندرجات پایان‌نامه‌ی تحصیلی خود را بر عهده می‌گیرم.

۳) این پایان‌نامه، حاصل پژوهش انجام شده توسط اینجانب می‌باشد.

۴) در مواردی که از دستاوردهای علمی و پژوهشی دیگران استفاده نموده‌ام، مطابق ضوابط و مقرّرات مربوطه و با رعایت اصل امانتداری علمی، نام منبع مورد استفاده و سایر مشخصات آن را در متن و فهرست منابع و مآخذ ذکر نموده‌ام.

۵) چنانچه بعد از فراغت از تحصیل، قصد استفاده یا هر گونه بهره‌برداری اعم از نشر کتاب، ثبت اختراع و ... از این پایان‌نامه را داشته باشم، از حوزه‌ی معاونت پژوهشی و فنّاوری دانشگاه محقق اردبیلی، مجوزهای لازم را اخذ نمایم.

۶) در صورت ارائه‌ی مقاله‌ی مستخرج از این پایان‌نامه در همایش‌ها، کنفرانس‌ها، سمینارها، گردهمایی‌ها و انواع مجلات، نام دانشگاه محقق اردبیلی را در کنار نام نویسندگان (دانشجو و اساتید راهنما و مشاور) ذکر نمایم.

۷) چنانچه در هر مقطع زمانی، خلاف موارد فوق ثابت شود، عواقب ناشی از آن (منجمله ابطال مدرک تحصیلی، طرح شکایت توسط دانشگاه و ...) را می‌پذیرم و دانشگاه محقق اردبیلی را مجاز می‌دانم با اینجانب مطابق ضوابط و مقرّرات مربوطه رفتار نماید.

نام و نام‌خانوادگی دانشجو: سیده آرزو سیدابراهیمی

امضا

تاریخ

نام خانوادگی: سیدابراهیمی نام: سیده آرزو

عنوان پایان‌نامه:
بررسی ساختار کدهای خطی و دوری روی حلقه‌های زنجیری

استاد راهنما: دکتر ناصر زمانی
اساتید مشاور: دکتر احمد خوجالی بارنجی، دکتر محمد باقر مقیمی

مقطع تحصیلی: کارشناسی ارشد
رشته: ریاضی محض گرایش: جبر
دانشگاه: محقق‌اردبیلی دانشکده: علوم ریاضی
تاریخ دفاع:۹۲/۰۶/۲۷ تعداد صفحات: ۶۴

چکیده

در این پایان‌نامه کدهای خطی و دوری روی حلقه‌های زنجیری مورد بررسی قرار می‌گیرند. و چندین نتیجه‌ی اساسی روی حلقه‌های زنجیر متناهی و حلقه‌های گالوا که نمونه‌ای از حلقه‌های زنجیر متناهی هستند ارائه خواهد شد. برای هر کد خطی C روی R برجی از کدهای خطی را ساخته و به وسیله‌ی ماتریس مولد کد C برای کدهای موجود در برج مذکور ماتریس مولد ساخته می‌شود. برای هر کد C روی R مجموعه‌ی منحصر به فرد از چندجمله‌ایهای مولد آن به ماتریس مولد C مرتبط شده و یک مجموعه از مولدهای دوگان C ارائه داده خواهد شد.

کلیدواژه‌ها: حلقه‌ی زنجیر متناهی، حلقه‌ی گالوا، کد خطی، کد دوری

Surname: Seydebrahimi Name: Seyde Arezoo

Title: On the structure of linear and cyclic codes over chain rings

Supervisor: Naser Zamani

Advisors: Ahmad Khojali Baranji, Mohammad Bagher Moghimi

Graduate Degree: M.Sc.

Major: Pure Mathematics Specialty: Algebra

University: Mohaghegh Ardabili Faculty: Mathematics Sciences

Date: September 2013 Number of Pages: 64

Abstract

We generalise structure theorems of Calderbank and Sloane for linear and cyclic codes over $\mathbb{Z}_{\mathbb{P}^\alpha}$ to a finite chain ring. Our results are more detailed and do not use non-trivial results form Commutative Algebra. In this project we study linear and cyclice codes over a finite chain ring. Several main result over chain and Galios ring will be proved. for a linear code over the ring R a tower linear codes and their generator matrix will be presented. the relation bettwen generator matrix and genrator projections are also studied.

Keywords: Cyclic code, finite chain ring, galois ring, linear code

دانشکده‌ی علوم ریاضی
گروه ریاضیات و کاربردها

پایان‌نامه برای دریافت درجه کارشناسی ارشد
در رشته‌ی ریاضی محض گرایش جبر

عنوان:

بررسی ساختار کدهای خطی و دوری روی حلقه‌های زنجیری

پژوهشگر:

سیده آرزو سیدابراهیمی

ارزیابی و تصویب شده‌ی کمیته داوران پایان‌نامه با درجه‌ی .....

نام و نام خانوادگی	مرتبه‌ی علمی	سمت	امضا
ناصر زمانی	استاد راهنما و رئیس کمیته داوران	دانشیار	.....
احمد خوجالی بارنجی	استاد مشاور	استادیار	.....
محمد باقر مقیمی	استاد مشاور	استادیار	.....
عادل کاظمی پیله‌درق	داور	استادیار	.....

شهریور ۱۳۹۲

University of Mohaghegh Ardabili
Faculty of Mathematical Sciences
Department of Mathematics and Applications

Thesis submitted in partial fulfilment of the requirements for the degree of M.Sc. in Pure Mathematics

Title:

On the structure of linear and cyclic codes over chain rings

By:

Seyde Arezoo Seydebrahimi

Evaluated and approved by thesis committee as .....

Name & Famliy	Degree	Responsibility	Signature
Naser Zamani	Assoc. Prof	Supervisor & Chairman	.....
Ahmad Khojali Baranji	Assist. Prof	Advisor	.....
Mohammad Bagher Moghimi	Assist. Prof	Advisor	.....
Adel Kazemi piledargh	Assist. Prof	Referee	.....

September 2013

تقدیم به

پدر و مادر عزیزم

سپاس‌گذاری

به نام خدا

تمام سپاس من از آن کسانیست که تا این مرحله از زندگی همراه و پشتیبانم بوده‌اند و هیچگاه در فراز و نشیبهای آن رهاییم نکرده‌اند. دوست دارم اول از خدای خود تشکر کنم به خاطر تمام مهربانیهایش.

خدایا ...

کاش چشمان حقیر من می‌توانست دستان مهربان تو را ببینند تا به خاطر تمام مهربانیهایت بوسه‌ای بر آن بزنند. اما افسوس که این چشم توان دیدن ندارد پس مهربانم با دیده‌ی دل دستان پر مهرت را بوسه میزنم.

میخواهم از خانواده عزیزم به خاطر زحمات بی دریغ و حمایتهای همیشگی‌شان کمال تشکر را داشته باشم و بگوییم بدون وجود عزیزشان هیچ نیستم.

بر خود لازم می دانم که از تمامی اساتید دوران تحصیلم به ویژه استاد ارجمند جناب آقای دکتر ناصر زمانی به خاطر تمامی زحمات بی دریغشان کمال تشکر را داشته باشم. و امیدوارم که بار دیگر سعادت شاگردی ایشان شامل حال بنده گردد، با این امید که لیاقت شاگردی ایشان را داشته باشم.

و در پایان از تمامی دوستان عزیزی که از ابتدا تا به امروز همراه و مشوق من بوده‌اند کمال سپاسگذاری را دارم.

سیده آرزو سیدابراهیمی

تابستان۱۳۹۲

فهرست مطالب

مقدمه

«نظریه‌ی کدگذاری» شاخه‌ای از ریاضیات است که روش‌های کنترل خطاهای به وجود آمده در انتقال اطلاعات را بررسی می‌کند. این نظریه با وجود جوان بودن یکی از شاخه‌های پر کاربرد در ریاضیات محسوب می‌شود که به سرعت در حال گسترش است. نظریه‌ی کدگذاری با مقاله‌ای کلاسیک از شانون در سال ۱۹۴۸ متولد شد که در آن ثابت کرد ساختارهایی وجود دارد که با استفاده از آنها می‌توان اثر خطاهای به وجود آمده در انتقال اطلاعات را به دلخواه کم کرد. از آنجا که قضیه‌ی او به هیچ پرسشی در مورد نحوه‌ی ساخت این ساختارها پاسخ نمی‌داد مطالعه در مورد کدهای کنترل کننده‌ی خطا به یک شاخه‌ی فعال تحقیق به نام «نظریه‌ی کدگذاری» منجر شد. این نظریه مثال بسیار جالبی از قدرت کاربردی شاخه‌های گوناگون ریاضیات مانند جبر، ترکیبیات و هندسه است که مورد توجه ریاضیدانان، متخصصان علوم کامپیوتر و مهندسان است. نظریه‌ی کدگذاری با استفاده از ابزارهای جبری و همچنین ریاضیات ترکیبی در صدد ایجاد ساختارهایی برای تبادل اطلاعات می‌باشد. مبحث اصلی این نظریه مطالعه‌ی روشهایی برای انتقال اطلاعات به صورت دقیق و کارآمد از محلی به محل دیگر است. چنین روشهایی می‌توانند کاربردهای بسیار متنوعی داشته باشند. انتقال اطلاعات از یک کامپیوتر به کامپیوتر دیگر یا از حافظه به پردازشگر مرکزی و ارسال تصاویر و اطلاعات از فضا تنها چند نمونه از این کاربردها هستند. این انتقال می‌تواند در زمان صورت گیرد، مانند زمانی که بخواهیم داده‌ای را ذخیره کنیم. بنابراین، کدگذاری در ذخیره‌ی داده‌ی روی دیسک‌های فشرده و DVDها انجام می‌شود به طوری که حتی اگر خراشی روی دیسک به وجود آید بتوان از آن استفاده کرد. کدهای خطی و دوری که در این پایانامه مورد بررسی قرار می‌گیرند کدهای تصحیح وخطا هستند که دارای سه پارامتر $[n, k, d]$ می‌باشند، که n طول کد، k بعد کد و d حداقل فاصله‌ی بین عناصر آن می‌باشد. به طور کلی، کد روی یک مجموعه‌ی متناهی بنام الفبای کد تعریف می‌شود . اما هدف اصلی این پایان‌نامه بررسی ساختاری از کدهای خطی و دوری روی یک حلقه‌ی زنجیر متناهی می‌باشد. برای رسیدن به این هدف این پایان‌نامه در ۴ فصل تنظیم شده است. در فصل اول به ذکر تعاریف و مقدماتی راجع به الفبای کد، کد به عنوان فضای برداری روی حلقه‌های زنجیر متناهی، کدهای خطی و دوری و کد

دوگان می‌پردازیم. در فصل دوم به بررسی حلقه‌های زنجیر متناهی و نمونه‌ای از آن یعنی حلقه‌های گالوا پرداخته و چندین نتیجه‌ی پایه‌ای ارائه می‌شوند. به ویژه نشان داده می‌شود که به‌ازای هر عدد اول p و هر عدد صحیح $a \geq ۱$، حلقه‌ی $\mathbb{Z}_{p^a}$ یک حلقه‌ی زنجیر متناهی و موضعی است. در فصل سوم نتایج ارائه شده برای کدهای خطی به حلقه‌های زنجیر متناهی محدود شده و قضایا تعمیم داده می‌شوند. برای هر کد خطی C روی R برجی از کدهایی خطی به صورت زیر

$$\bar{C} = \overline{(C : \gamma^{۰})} \subseteq \ldots \subseteq \overline{(C : \gamma^{i})} \subseteq \ldots \subseteq \overline{(C : \gamma^{\nu-۱})}$$

داریم. از آنجایی که $(C : r)$ نشاندهنده‌ی زیر مدول خارج قسمتی از C به وسیله‌ی $r \in R$ می‌باشد تعریف ۱.۲.۳ را داریم و بوسیله‌ی ماتریس مولد کد C، برای کدهای موجود در برج مذکور ماتریس مولد می‌سازیم. در فصل چهارم مفهومی از مجموعه مولدی در شکل استاندارد ارائه خواهد شد و به هر کد دوری و دوگان آن یک مجموعه مولد منحصر به فرد در شکل استاندارد نسبت داده می‌شود و چندین قضیه‌ی اساسی را ثابت می‌کنیم. لازم به ذکر است که مقاله‌ی اصلی برای نگارش این پایان‌نامه مرجع (نورتون و سالاجین [۱]، ۲۰۰۰) می‌باشد.

[۱] Norton, Salagean

فصل ۱
مقدمات و مفاهیم اولیه

۱.۱ مقدمات و مفاهیم اولیه

در این فصل برخی مفاهیم و قضایایی را که در فصل‌های بعدی مورد استفاده قرار می‌گیرند، مرور می‌کنیم.

تعریف ۱.۱.۱. فرض کنیم $A = \{a_۱, \ldots, a_q\}$ یک مجموعه‌ی q عضوی باشد. مجموعه‌ی A را مجموعه الفبای کد و عناصر A را نمادهای کد می‌نامیم.

۱. یک کلمه یا بردار به طول n روی A عبارتست از دنباله‌ی $\mathbf{w} = w_۱ \ldots . w_n$ که برای هر i، $w_i \in A$.

۲. یک کد بلوکی $q-$نمادی به طول n روی A عبارتست از مجموعه‌ی ناتهی C از کلمات به طول n روی A. هر عضو C را یک کدواژه نامیده، تعداد عناصر C را با نماد $|C|$ نشان داده و آنرا اندازه‌ی کد C می‌نامیم.

۳. اگر C یک کد به طول n باشد، آنگاه $\log_۲ \frac{|C|}{n}$ را نرخ اطلاعات [۱] می‌نامیم.

۴. یک کد بلوکی $q-$نمادی به طول n و اندازه‌ی M را به صورت $(n, M)_q-$کد نمایش می‌دهیم.

تعریف ۱.۱.۲. میدانی که تعداد عناصر آن متناهی باشد را یک میدان متناهی و تعداد عناصر آنرا مرتبه آن می‌نامیم.

تعریف ۱.۱.۳. یک میدان متناهی از مرتبه‌ی q که در آن q توانی از یک عدد اول است، را میدان گالوا از مرتبه‌ی q و آنرا با $GF(q)$ یا $\mathbb{F}_q$ نشان می‌دهیم.

قرارداد ۱.۱.۱. معمولاً مجموعه‌ی $\mathbb{Z}_q = \{۰, ۱, \ldots, q-۱\}$ را به عنوان الفبای کد انتخاب کرده و اگر $q = p^h$ توان صحیح مثبتی از عدد اول p باشد، آنگاه میدان متناهی q عضوی $\mathbb{F}_q$ الفبای کد خواهد بود.

[۱] information rate

مثال ۱.۱.۱.

۱. یک کد روی مجموعه‌ی $\mathbb{F}_۲ = \{۰,۱\}$ را کد دودویی (باینری [۱]) می‌نامیم که در آن عناصر ۰,۱ نمادهای کد هستند. در زیر دو نمونه از کدهای دوتایی آورده شده‌اند.

(آ) مجموعه‌ی $C_۱ = \{۰۰, ۰۱, ۱۰, ۱۱\}$ یک $(۲, ۴)_۲$–کد می‌باشد که طول کد برابر ۲ و اندازه‌ی آن برابر ۴ است.

(ب) مجموعه‌ی $C_۲ = \{۰۰۱۱, ۰۱۰۱, ۱۰۱۰, ۱۱۰۰, ۱۰۰۱, ۰۱۱۰\}$ یک $(۴, ۶)_۲$–کد می‌باشد که طول کد برابر ۴ و اندازه‌ی آن برابر ۶ است.

۲. یک کد روی مجموعه‌ی $\mathbb{F}_۳ = \{۰, ۱, ۲\}$ را کد سه‌سه‌ای می‌نامیم که عناصر ۰, ۱, ۲ نمادهای کد هستند. در زیر نمونه‌ای از کدهای سه‌سه‌ای را آورده‌ایم.

مجموعه‌ی $C_۳ = \{۰۰۰, ۱۱۱, ۲۲۲\}$ یک $(۳, ۳)_۳$–کد می‌باشد که طول و اندازه‌ی آن برابر ۳ است.

تبصره ۱.۱.۱. در تعریف ۱.۱.۱ ملاحظه شد که کد C روی مجموعه‌ی متناهی $\mathbb{F}_q$ تعریف می‌شود. بنابراین، الفبای کد یک مجموعه‌ی متناهی است. برای نیل به نتایج اصیل در مورد کدها، فرض می‌کنیم $\mathbb{F}_q$ صرفاً یک مجموعه نبوده و دارای ساختار جبری نیز می‌باشد. معمولاً در تعاریف اولیه از کد، $\mathbb{F}_q$ را یک میدان متناهی در نظر می‌گیریم.

تعریف ۴.۱.۱. فرض کنیم R یک حلقه باشد. در این صورت، کوچکترین عدد طبیعی مانند p که در شرط $p \cdot ۱ = ۰$ صدق کند، را مشخصه‌ی حلقه گفته (۱، عضو همانی ضربی R است) و آنرا با $char(R)$ نمایش می‌دهیم. اگر چنین pای موجود نباشد، مشخصه‌ی حلقه را صفر می‌گیریم.

مثال ۲.۱.۱. حلقه‌ی $\mathbb{Z}_n$ دارای مشخصه‌ی n است، ولی $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ دارای مشخصه‌ی صفر می‌باشند.

[۱] Binary

۲.۱ حلقه‌ی چندجمله‌ایها

فرض کنیم R یک حلقه بوده و $R[X] := \{a_۰ + a_۱X + \ldots + a_nX^n \mid a_i \in R, n \geqslant ۰\}$ حلقه‌ی چندجمله‌ایها روی X با ضرایب در R باشد. در ادامه تمام حلقه‌ها جابجایی و یکدار فرض می‌شوند.

تعریف ۱.۲.۱. فرض کنیم R یک حلقه و M یک $R-$مدول باشد. عنصر $r \in R$ را $M-$منظم می‌گوییم اگر به ازای هر $m \in M$ که $rm = ۰$، آنگاه $m = ۰$.

تعریف ۲.۲.۱. هر حلقه‌ی جابجایی R را که دقیقاً یک ایده‌آل ماکسیمال چون $\mathbf{M}$ دارد را موضعی می‌نامیم.

تبصره ۱.۲.۱. اگر R یک حلقه‌ی جابجایی موضعی متناهی بوده و $\mathbf{m}$ یک ایده‌آل ماکسیمال آن باشد، آنگاه میدان $K = \frac{R}{\mathbf{m}}$ را میدان مانده می‌گوییم. نگاشت طبیعی $\mu : R[X] \longrightarrow K[X]$ با ضابطه‌ی

$$\mu(a_۰ + a_۱X + \cdots + a_nX^n) = (a_۰ + \mathbf{m}) + (a_۱ + \mathbf{m})X + \cdots + (a_n + \mathbf{m})X^n$$

یک هومومرفیسم حلقه است.

تعریف ۳.۲.۱. فرض کنیم $f, g \in R[X]$ در اینصورت

۱. f را پوچتوان می‌گوییم اگر عدد صحیح n موجود باشد به طوری که $f^n = ۰$.

۲. f را یکال می‌گوییم اگر چندجمله‌ای h موجود باشد به طوری که $fh = ۱$.

قضیه ۱.۲.۱. فرض کنیم $f = a_۰ + a_۱X + \ldots + a_nX^n$ یک چندجمله‌ای روی حلقه‌ی R باشد. در اینصورت گزاره‌های زیر معادل اند.

۱. f یکال است.

۲. μf یکال است.

۳. $a_۰$ یکال و $a_۱, \ldots, a_n$ پوچتوان هستند.

قضیه ۲.۲.۱. فرض کنیم $f = a_۰ + a_۱X + \ldots + a_nX^n$ یک چندجمله‌ای روی حلقه‌ی R باشد. در اینصورت گزاره‌های زیر معادل اند.

۱. f پوچتوان است.

۲. $\mu f = ۰$.

۳. $a_۰, \ldots, a_n$ پوچتوان هستند.

۴. f مقسوم‌علیه صفر است.

۵. عضو غیر صفری مانند $a \in R$ موجود است که $af = ۰$.

قضیه ۳.۲.۱. فرض کنیم $f = a_۰ + a_۱X + \ldots + a_nX^n$ یک چندجمله‌ای روی حلقه‌ی R باشد. در اینصورت گزاره‌های زیر معادل اند.

۱. f منظم است.

۲. $(a_۰, \ldots, a_n) = R$.

۳. a_i برای هر i، $۰ \leqslant i \leqslant n$، یکال است.

۴. $\mu f \neq ۰$.

برهان. برای دیدن اثبات سه قضیه‌ی فوق به قضیه‌ی ۱۳۰۲ از(مک دونالد [۱]، ۱۹۷۴) مراجعه شود. □

تعریف ۴.۲.۱. چندجمله‌ای غیر ثابت $f(x)$ را تحویل‌پذیر می‌گوییم اگر دو چندجمله‌ای $g(x)$ و $h(x)$ موجود باشند به طوری که $f(x) = g(x)h(x)$ و $\deg h(x), \deg g(x) < \deg f(x)$. در غیر اینصورت، $f(x)$ را تحویل‌ناپذیر می‌گوییم.

[۱] McDonald

مثال ۱.۲.۱. چندجمله‌ای غیر ثابت $g(x) = ۱ + x + x^۲ \in \mathbb{Z}_۲[X]$ یک چندجمله‌ای تحویل‌ناپذیر است. زیرا در غیر اینصورت دارای عامل‌های خطی x یا $x+۱$ می‌باشد. به عبارت دیگر، ۰ یا ۱ ریشه‌ای برای $g(x)$ است. در حالیکه $g(۰) = g(۱) = ۱$ که یک تناقض است.

تعریف ۵.۲.۱. چندجمله‌ای f در $R[X]$ را تحویل‌ناپذیر اساسی می‌گوییم اگر $\mu(f)$ در $K[X]$ تحویل‌ناپذیر باشد.

تعریف ۶.۲.۱. ایده‌آل I در حلقه‌ی R را اولیه می‌گوییم اگر $I \neq R$ و به ازای هر $x, y \in R$ از $xy \in I$ و $x \notin I$ نتیجه شود که به ازای یک مقدار صحیح و مثبت n، $y^n \in I$.

تعریف ۷.۲.۱. چندجمله‌ای $f \in R[X]$ را اولیه می‌گوییم اگر (f) یعنی ایده‌آل تعریف شده به وسیله‌ی f ایده‌آلی اولیه باشد.

تعریف ۸.۲.۱. چندجمله‌ای منظم $f \in R[X]$ را اولیه می‌گوییم اگر و فقط اگر μf در $K[X]$ اولیه باشد.

گزاره ۱.۲.۱. عنصر غیر یکال $f \in R[X]$ اولیه است اگر و فقط اگر $f = \delta g^h + \beta$ ، که در آن δ یکال، g تحویل‌ناپذیر اساسی، $h \geqslant ۱$ و $\beta \in \mathbf{m}\ [X]$.

برهان. به برهان گزاره‌ی ۱۲ ۰ ۱۳ از(مک دونالد، ۱۹۷۴) مراجعه شود. □

تعریف ۹.۲.۱. فرض کنیم $g(X), f(X) \in R[X]$ دو چندجمله‌ای غیر صفر باشند. بزرگترین مقسوم‌علیه مشترک $g(X)$ و $f(X)$ با نماد $\mathbf{gcd}\ (f(X), g(X))$ [۱] برابر است با چندجمله‌ای منحصربه فرد با بیشترین درجه به طوری که $f(X)$ و $g(X)$ را عاد کند. اگر $\mathbf{gcd}(f(X), g(X)) = ۱$، آنگاه $f(X)$ و $g(X)$ را نسبت به هم اول می‌نامیم. و کوچکترین مضرب مشترک $f(X)$ و $g(X)$ با نماد $\mathbf{lcm}\ (f(X), g(X))$ [۲] برابر است با چندجمله‌ای منحصربه فرد با کمترین درجه به طوری که هر دوی $f(X)$ و $g(X)$ آن را عاد می‌کنند.

[۱] greatest common divisor
[۲] least common multiple

تعریف ۱۰.۲.۱. فرض کنیم N مجموعه‌ای از اعداد صحیح نامنفی و R حلقه‌ای تحویل‌پذیر باشد R را حلقه‌ی اقلیدسی می‌گوییم هرگاه تابعی مانند $\varphi : R - \{۰\} \longrightarrow N$ موجود باشد به طوری که

۱. اگر $a, b \in R$ و $ab \neq ۰$، آنگاه $\varphi(a) \leq \varphi(ab)$.

۲. اگر $a, b \in R$ و $b \neq ۰$، آنگاه $r, q \in R$ موجودند به طوری که $a = qb + r$ که در آن $\varphi(r) < \varphi(b)$.

مثال ۲.۲.۱. هرگاه $\mathbb{F}$ یک میدان باشد، آنگاه $\mathbb{F}[X]$ یک حوزه‌ی اقلیدسی است.

قضیه ۴.۲.۱. فرض کنیم f یک چندجمله‌ای منظم در $R[X]$ باشد. در اینصورت چندجمله‌ای تکین f^* موجود است به طوری که $\mu f = \mu f^*$ و برای هر $a \in R$، $f(a) = ۰$ اگر و فقط اگر $f^*(a) = ۰$. به علاوه، عنصر یکال $v \in R[X]$ موجود است به طوری که $vf = f^*$.

برهان. به قضیه‌ی ۱۳۰۶ از(مک دونالد، ۱۹۷۴) مراجعه شود. □

قضیه ۵.۲.۱. (لم هنسل[۱]) فرض کنیم $f \in R[X]$ و به ازای $۱ \leq i \leq n$، $\bar{g}_i \in K[X]$ به طوری که $\mu f = \bar{g}_۱ \ldots . \bar{g}_n$ و $\bar{g}_۱, \ldots, \bar{g}_n$ دو به دو نسبت به هم اول اند. در اینصورت $g_۱, \ldots, g_n \in R[X]$ وجود دارند به طوری که

۱. $g_۱, \ldots, g_n$ دو به دو نسبت به هم اول اند،

۲. $\mu g_i = \bar{g}_i$، $, ۱ \leqslant i \leqslant n$

۳. $f = g_۱ \ldots . g_n$.

برهان. با استقراء روی n حکم را ثابت می‌کنیم. برای $n = ۲$ داریم $f = h_۱ h_۲ + \nu$ که $\mu h_۱ = \bar{g}_۱$ و $\mu h_۲ = \bar{g}_۲$ و $\nu \in \mathbf{m}\ [X]$. در اینصورت $\bar{g}_۱, \bar{g}_۲$ نسبت به هم اول اند اگر و فقط اگر $h_۱, h_۲$ نسبت به هم اول باشند. پس $\lambda_۱, \lambda_۲ \in R[X]$ موجود اند که $\lambda_۱ h_۱ + \lambda_۲ h_۲ = ۱$. قرار می‌دهیم $h_{۱۱} = h_۱ + \lambda_۲ \nu$،

[۱] Hensel Lemma