

**T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

GALOIS HALKALARI

ELİF ALTINAY

**YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI**

**DANIŞMAN
DOÇ. DR. GÜRSEL YEŞİLOT**

İSTANBUL, 2011

T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GALOIS HALKALARI

Elif ALTINAY tarafından hazırlanan tez çalışması 23.06.2011 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Doç. Dr. Gürsel YEŞİLOT
Yıldız Teknik Üniversitesi

Jüri Üyeleri

Doç. Dr. Gürsel YEŞİLOT
Yıldız Teknik Üniversitesi



Prof. Dr. İrfan ŞİAP
Yıldız Teknik Üniversitesi



Doç. Dr. Ünsal TEKİR
Marmara Üniversitesi



ÖNSÖZ

Bütün eğitim hayatım boyunca yanımda olan ve desteklerini hiç eksik etmeyen başta sevgili annem ve babam olmak üzere tüm aileme, dostlarıma; lisans ve yüksek lisans eğitimime katkılarından dolayı saygıdeğer hocalarıma ve ayrıca tez danışmanım olan değerli hocam Doç. Dr. Gürsel Yeşilot'a; yüksek lisans eğitimimi burs vererek destekleyen TÜBİTAK'a teşekkürlerimi sunarım.

Temmuz, 2011

Elif ALTINAY

İÇİNDEKİLER

	Sayfa
SİMGE LİSTESİ.....	Vi
ÖZET.....	Vii
ABSTRACT.....	IX
BÖLÜM 1	
GİRİŞ	1
1.1 Literatür Özeti.....	1
1.2 Tezin Amacı	1
1.3 Hipotez	2
BÖLÜM 2	
ÖN BİLGİLER	3
BÖLÜM 3	
$\mathbb{Z}_{p^s}[x]$ POLİNOM HALKASI.....	8
3.1 $\mathbb{Z}_{p^s}$ Kalan Sınıf Halkası.....	8
3.2 $\mathbb{Z}_{p^s}[x]$ Polinom Halkası ve İdealleri.....	10
3.3 Hensel Yrd. Teoremi ve Temel İndirgenemez Polinomlar	14
BÖLÜM 4	
GALOIS HALKALARI.....	22
4.1 Galois Halkası Tanımı ve Örnekleri	22
4.2 Galois Halkalarının Yapısı	29
4.3 p -adik Gösterim	35
4.4 Galois Halkalarının Birim Grubu.....	41
4.5 Galois Halkalarının Genişlemesi.....	47
4.6 Galois Halkalarının Otomorfizmaları	56

4.7	Genelleştirilmiş İz ve Norm	62
BÖLÜM 5		
	ZİNCİR HALKALAR.....	65
BÖLÜM 6		
	SONUÇ VE ÖNERİLER.....	73
	KAYNAKLAR	74
	ÖZGEÇMİŞ	75

SİMGE LİSTESİ

$\mathbb{F}_q$	q elemanlı sonlu cisim
$\mathbb{Z}_{p^s}$	p^s modülüne göre tamsayılar halkası
$GR(p^s, p^{sm})$	Karakteristiği p^s ve kardinalitesi p^{sm} olan Galois halkası
$\bar{r}$	$r \in R$ nin “-” doğal homomorfizması altındaki görüntüsü
$\bar{f}$	$f \in R[x]$ polinomunun “-” doğal homomorfizması altındaki görüntüsü
ϕ	R' Galois halkasının R Galois halkası üzerindeki genelleştirilmiş Frobenius otomorfizması
$\text{Gal}(R'/R)$	R' halkasının R üzerindeki Galois grubu
$T_{R'/R}(\alpha)$	$\alpha \in R'$ elemanının R halkasına göre genelleştirilmiş izi
$N_{R'/R}(\alpha)$	$\alpha \in R'$ elemanının R halkasına göre genelleştirilmiş normu
$\text{Rad}(R)$	Jacobson Radikali

GALOIS HALKALARI

Elif ALTINAY

Matematik Anabilim Dalı
Yüksek Lisans Tezi

Tez Danışmanı: Doç. Dr. Gürsel YEŞİLOT

Bu tezin temel konusu Galois halkalarının yapısı ve inşa edilmesidir. İlk olarak Bölüm 2’de Galois halkalarını ve sonrasında zincir halkalarını çalışmak için gerekli ön bilgileri verdik. Üçüncü bölümde, $\mathbb{Z}_{p^s}$ Kalan Sınıf halkası, $\mathbb{Z}_{p^s}[x]$ Polinom Halkası ve İdealleri, Hensel Yrd. Teoremi ve Temel İndirgenemez Polinomlar olmak üzere üç başlığı çalıştık. Bu bölümdeki bilgilerin Galois halkalar teorisinde çok önemli yeri vardır. Tezimizin ana bölümü, 4. Bölüm Galois Halkalarıdır. Bu bölümde sırasıyla, Galois halkalarının tanımı ve örnekleri, yapısı, p -adik gösterimi, birimselleri, genişlemeleri, otomorfizmaları, iz ve norm tanımlarını verdik. p bir asal sayı olsun. Birimi 1 olan değişmeli sonlu bir halkada, halkanın sıfırı ve sıfır bölenleri (p) idealini oluşturuyorsa bu halkaya Galois halkası denir. R nin sıfır bölen olmayan elemanları birimseldir. Bu yüzden, R nin tek maksimal ideali (p) dir. R , karakteristiği p^s ve kardinalitesi p^{sm} olan bir Galois halkası ve $h(x) \in \mathbb{Z}_{p^s}[x]$ m . dereceden monik temel indirgenemez bir polinom olmak üzere

$$R \cong \mathbb{Z}_{p^s}[x]/(h(x))$$

izomorfizması vardır. O halde, karakteristikleri ve kardinaliteleri aynı olan Galois halkaları izomorftur. Bu yüzden, karakteristiği p^s ve kardinalitesi p^{sm} olan Galois halkalarını kısaca $GR(p^s, p^{sm})$ ile gösteriyoruz. $h(x)$ polinomunun mertebesi $p^m - 1$ olan bir ξ kökü vardır, ve

$$GR(p^s, p^{sm}) = \mathbb{Z}_{p^s}[\xi] = \{a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1} : a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}_{p^s}\}$$

yazabiliriz. $\tau = \{0, 1, \xi, \xi^2, \dots, \xi^{p^m-2}\}$ olsun. $a_0, a_1, \dots, a_{s-1} \in \tau$ olmak üzere her $c \in GR(p^s, p^{sm})$ elemanını

$$c = a_0 + a_1 p + \dots + a_{s-1} p^{s-1}$$

şeklinde p -adik gösterimle tek türlü ifade edebiliriz. $R = GR(p^s, p^{sm})$, $R' = GR(p^s, p^{sm})$ ve $h(x) \in R[x]$ l . dereceden monik temel indirgenemez bir polinom olmak üzere $R' \cong R[x]/(h(x))$ izomorfizması vardır.

Son bölümde zincir halkalarını inceledik. Bir halkanın bütün idealleri kapsamaya göre lineer sıralı ise yani bir zincir oluşturuyorsa bu halkaya zincir halka denir. Sonlu zincir halkalar, maksimal ideali temel ideal olan yerel halkalardır. R , maksimal ideali M olan sonlu bir zincir halka olsun. p^s : R nin karakteristiği; p^m : $|R/M| = |\mathbb{F}_{p^m}|$; β : M nin nilpotentlik indeksi, $s=1$ iken $t=\beta$ ve $s>1$ iken $1 \leq t \leq k$ olmak üzere $\beta = (s-1)k + t$; k : $p \in M^k$ olacak şekilde β ya eşit veya küçük olan en büyük tamsayı olmak üzere p, s, m, k, t tamsayılarına R nin sabitleri denir. $g(x) \in GR(p^s, p^{sm})[x]$, k . dereceden bir Eisenstein polinomu olsun. p, s, m, k, t sabitlerine sahip her R sonlu zincir halkası için

$$R = GR(p^s, p^{sm})[x]/(g, p^{s-1}x^t)$$

yazabiliriz.

Anahtar Kelimeler: Galois halkaları, sıfır bölen eleman, birimsel eleman, sonlu cisim, polinom halkası, temel indirgenemez polinom, yerel halkalar, zincir halkalar.

ABSTRACT

GALOIS RINGS

Elif ALTINAY

Department of Mathematics
MSc. Thesis

Advisor: Assoc. Prof. Dr. Gursel YESILOT

The main goal of this thesis is exploring the structure of Galois rings and the construction of them. First of all, in Section 2, we give information that is necessary for being able to study Galois rings and then chain rings. In Section 3, we study the residue class ring of $\mathbb{Z}_{p^s}$, the ring of polynomials of $\mathbb{Z}_{p^s}[x]$, Hensel's Lemma and basic irreducible polynomials. The information in this section has a crucial part in The Theory of Galois Rings. Fourth Section is about Galois Rings. In this section, we study the definition of Galois rings, their structure, p -adic representation, units, extension and automorphisms, respectively and give some examples. Let p be a prime. In a finite commutative ring with identity, if the set of zero and zero-divisors form (p) then this ring is called a Galois ring. The non-zero divisors are units in R , so (p) is the unique maximal ideal of R . If $h(x) \in \mathbb{Z}_{p^s}[x]$ is a monic basic irreducible then

$$R \cong \mathbb{Z}_{p^s}[x]/(h(x)).$$

Thus, any two Galois rings of the same characteristic and cardinality are isomorphic. Therefore, we can use the notation $GR(p^s, p^{sm})$ to denote any Galois ring of characteristic p^s and cardinality p^{sm} . Further, there exists a root ξ of $h(x)$ of order $p^m - 1$, and

$$GR(p^s, p^{sm}) = \mathbb{Z}_{p^s}[\xi] = \{a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1} : a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}_{p^s}\}.$$

Let $\tau = \{0, 1, \xi, \xi^2, \dots, \xi^{p^m-2}\}$ and $a_0, a_1, \dots, a_{s-1} \in \tau$. Then, any element $c \in GR(p^s, p^{sm})$ can be written uniquely as

$$c = a_0 + a_1p + \cdots + a_{s-1}p^{s-1}.$$

Let $R = GR(p^s, p^{sm})$ and $R' = GR(p^s, p^{sml})$ be two Galois rings. If $h(x)$ is a monic basic irreducible polynomial of degree l in $R[x]$ then $R' \cong R[x]/(h(x))$.

In the last section, we study chain rings. A ring is called a chain ring if all its ideals form a chain under inclusion. Finite chain rings are precisely finite local rings whose maximal ideal is principal. Let R be a finite chain ring with maximal ideal M . Let p^s : the characteristic of R ; p^m : $|R/M| = |\mathbb{F}_{p^m}|$; β : the nilpotency index of M and $\beta = (s-1)k + t$ such that $t = \beta$ where $s = 1$ and $1 \leq t \leq k$ where $s > 1$; k : the greatest integer that is equal or less than β such that $p \in M^k$. Then the integers p, s, m, k, t are called as the invariants of R . Let $g(x) \in GR(p^s, p^{sm})[x]$ be an Eisenstein polynomial of degree k . Then, any finite chain ring R whose invariants are p, s, m, k, t is

$$R = GR(p^s, p^{sm})[x]/(g, p^{s-1}x^t).$$

Key words: Galois rings, zero divisor, unity, finite field, ring of polynomials, basic irreducible polynomial, local rings, chain rings.

BÖLÜM 1

GİRİŞ

1. 1 Literatür Özeti

Galois Halkaları Teorisi ilk kez 1924 yılında W. Krull tarafından geliştirildi. Daha sonra R. Raghavendran (Composito Math. 21 (1969), 195-229) ve G. Janusz (Seperable Algebras over Commutative Rings Trans. A. M. S. 122 (1966), 461-479) birbirlerinden bağımsız olarak Galois Halkalarının varlığını ve yapısını tekrar keşfettiler. Bernard R. McDonald “Finite Rings with Identity” isimli kitabında $\mathbb{Z}_{p^s}$ halkasının Galois genişlemesini, bu halka üzerinde modülleri ve halkanın birim grubunu çalışmıştır. Aynı kitapta, Galois halkaları ilk kez sonlu halkaların inşa edilmesinde kullanılmıştır. Zincir halkalar, bir Galois halkası üzerinde tanımlı bir polinom halkasının homomorfik görüntüsü olarak karakterize edilmiştir. Galois halkaları ve sonlu cisimlerin yapıları çok benzerlik taşımaktadır ve teorileri paraleldir. Bu yüzden, Zhe-Xian Wan “Lectures on Finite Fields and Galois Rings” isimli kitabında bu yapıları beraber çalışmıştır.

1. 2 Tezin Amacı

Galois halkaları bir çok araştırmacının dikkatini çekmiştir. Bunun en önemli sebebi, Galois halkalarının bilim ve teknolojide cebirsel kodlama teorisi, kriptoloji, cebirsel sistem teorisi gibi geniş bir uygulama alanının olmasıdır. Galois halkalarının inşa edilmesi, elemanlarının tek türlü ifade edilmesi, ideallerinin ve birim grubunun yapısal özellikleri, bir Galois halkasını kapsayan yeni bir Galois halkasının inşa edilmesi, zincir halkaların inşa edilmesi ve bunların örneklendirilmesi amacıyla bu tez çalışması yapılmıştır.

1. 3 Hipotez

Cebirde Kodlama Teorisi, Şifreleme Teorisi gibi bir çok kullanım alanı olan Galois halkaları ve zincir halkaların yapılarının daha somut hale getirilmesi için bir çok örneklendirme yapılabilir.

BÖLÜM 2

ÖN BİLGİLER

Bu bölümde, Galois halkalarını ve sonrasında zincir halkalarını çalışmak için gerekli olan ön bilgileri vereceğiz. Bu bilgiler, grup, halka ve sonlu cisimlerle ilgili temel bazı tanım ve teoremleri içermektedir [1], [2], [3], [4].

Teorem 2. 1 Sonlu elemanlı birimli halkada sıfır bölen olmayan her eleman birimseldir.

İspat: R sonlu bir halka olsun. Sıfır bölen olmayan $0 \neq a \in R$ elemanının tersinin varlığını gösterelim. $R = \{a_1, a_2, \dots, a_n\}$ diyelim ve R nin herhangi bir (sabit) elemanı da a ($a = a_k$) olsun. Her $i = 0, 1, \dots, n$ için

$$f : R \rightarrow R$$

$$a_i \mapsto aa_i$$

fonksiyonunu tanımlayalım. f nin birebir olduğunu gösterelim. $f(a_i) = f(a_j)$ ise $aa_i = aa_j$ dir. Buradan, $a(a_i - a_j) = 0$ olur. a sıfır bölen olmadığından $a_i - a_j = 0$ ve $a_i = a_j$ dir. Bu yüzden, f birebirdir. f birebir olduğundan, $f(R)$ de n elemanlıdır ve dolayısıyla f örtendir. f örten olduğundan $1_R = f(a_i) = aa_i$ olacak şekilde bir a_i elemanı vardır. Yani, a birimseldir.

Teorem 2. 2 R , değişmeli ve birimli bir halka ve I , R nin bir ideali olsun. O halde,

(i)

$$\phi : R \rightarrow R/I$$

$$a \mapsto \bar{a} = a + I$$

bir halka homomorfizmasıdır (ϕ ye doğal homomorfizma denir). $\text{Çek}\phi = I$ ve $\phi(R) \cong R/I$ dır.

(ii) $\phi: R \rightarrow R'$ bir halka homomorfizması olsun. $1_{R'} \in R'$ birimi olmak üzere $\phi(1) = 1_{R'}$ olduğunu kabul edelim. O halde, $\phi(I)$, R' nün bir alt halkasıdır ve $\text{Çek}\phi$, R nin bir idealidir. Ayrıca,

$$\bar{\phi}: R/\text{Çek}\phi \rightarrow \phi(I)$$

$$\bar{a} = a + \text{Çek}\phi \mapsto \phi(a)$$

halka izomorfizmasıdır.

Teorem 2. 3 R ve R' , değişmeli ve birimli halkalar ve $\phi: R \rightarrow R'$ örten halka homomorfizması olsun. O halde,

(i) I , R nin bir ideali (veya bir alt halkası) ise $\phi(I)$, R' halkasının bir idealidir (veya alt halkasıdır).

(ii) I' , R' halkasının bir ideali (veya alt halkası) ise $\phi^{-1}(I')$, R nin bir idealidir (veya bir alt halkasıdır). Ayrıca, $\phi^{-1}(I') \supseteq \text{Çek}\phi$ ve $\phi^{-1}(I')/\text{Çek}\phi \cong I'$ dir.

(iii) I , R nin bir ideali ve $\phi(I) = I'$ ise

$$\varphi: R/I \rightarrow R'/I'$$

$$a + I \mapsto \phi(a) + I'$$

φ bir halka homomorfizmasıdır. $I \supseteq \text{Çek}\phi$ ise $\phi^{-1}(\phi(I)) = I$ dır ve φ izomorfizmadır.

Teorem 2. 4 R değişmeli ve birimli bir halka, R_0 , R nin bir alt halkası, I , R nin bir ideali ve $R_0 + I = \{r_0 + a : r_0 \in R_0, a \in I\}$ olsun. O halde,

(i) $R_0 + I$, R nin homomorfik bir alt halkasıdır; I , $R_0 + I$ halkasının bir idealidir ve $R_0 \cap I$, R_0 halkasının bir idealidir.

(ii)
$$R_0 + I \rightarrow R_0/(R_0 \cap I)$$

$$r_0 + a \mapsto r_0 + (R_0 \cap I)$$

bir halka homomorfizmasıdır ve çekirdeği I dır. Sonuç olarak,

$$(R_0 + I)/I \cong R_0/(R_0 \cap I).$$

Tanım 2. 1 R birimli ve değişmeli bir halka ve Q , R nin bir ideali olsun. $Q \neq R$ ve $ab \in Q$ iken $a \in Q$ veya bir n pozitif tamsayısı için $b^n \in Q$ oluyorsa Q ya asalımsı ideal denir.

Tanım 2. 2 R birimli ve değişmeli bir halka ve I , R nin bir ideali olsun. I nin radikalli $\sqrt{I}$ ile gösterilir ve şu şekilde tanımlanır:

$$\sqrt{I} = \{a \in R : a^n \in I, n \in \mathbb{Z}^+\}$$

Teorem 2. 5 R birimli ve değişmeli bir halka ve I , R nin bir ideali olsun. O halde, $\sqrt{I}$, R nin bir idealidir.

Teorem 2. 6 G , mertebesi n olan sonlu devirli bir grup ise G nin her alt grubunun mertebesi n yi böler, ve n nin pozitif bir d böleni için G nin mertebesi d olan tek bir alt grubu vardır.

Teorem 2. 7 $\mathbb{F}_q$, q elemanlı sonlu bir cisim olsun. $\mathbb{F}_q$ nun $\mathbb{F}_q^*$ çarpımsal grubunun mertebesi $q-1$ dir. $\mathbb{F}_q^*$ in her elemanın mertebesi sonludur ve $q-1$ in bir bölenidir. Bu yüzden, her $a \in \mathbb{F}_q^*$ için $a^{q-1} = 1$ dir.

Teorem 2. 8 Her sonlu cismin çarpımsal grubu devirlidir.

Tanım 2. 3 F bir cisim ve $p(x)$ derecesi 1 den büyük $F[x]$ halkasında bir polinom olsun. $F[x]$ halkasında $p(x)$, derecesi sıfırdan büyük polinomların çarpımı şeklinde yazılamıyorsa $p(x)$ indirgenemezdir.

Teorem 2. 9 (Tek Türlü Çarpanlarına Ayrılma Teoremi) F bir cisim olsun. $F[x]$ halkasında derecesi 1 den büyük olan her $f(x)$ polinomu, $F[x]$ halkasında sonlu sayıda indirgenemez polinomların çarpımı olacak şekilde yazılabilir. Ayrıca, eğer

$$f(x) = p_1(x)p_2(x)...p_r(x) = q_1(x)q_2(x)...q_s(x)$$

olacak şekilde $f(x)$ polinomunun iki türlü çarpanlarına ayrılışı varsa, $r=s$ ve $i=1,2,...,r$ için $c_i \in F$ olmak üzere sıralamaya bakılmaksızın $p_i(x) = c_i q_i(x)$ olur.

Tanım 2. 4 $\alpha \in \mathbb{F}_{q^n}$ olsun. α elemanını kök kabul eden $\mathbb{F}_q[x]$ halkasındaki en küçük dereceli monik polinoma $\alpha \in \mathbb{F}_{q^n}$ elemanının $\mathbb{F}_q$ üzerindeki minimal polinomu denir.

Yrd. Teorem 2. 10 $f(x), \mathbb{F}_q[x]$ halkasında n . dereceden indirgenemez bir polinom olsun. O halde, $f(x) \mid (x^{q^n} - x)$ dir.

Teorem 2. 11 $\mathbb{F}_{p^n}, p^n$ elemanlı sonlu bir cisim ve $\mathbb{F}_p$ de onun asal cismi olsun. $F_0, \mathbb{F}_{p^n}$ cisminin p^m elemanlı bir alt cismi ise $m \mid n$ olmalıdır. Tersine, $m \mid n$ ise $\mathbb{F}_{p^n}$ cisminin p^m elemanlı tek bir alt cismi vardır. Ayrıca, $\mathbb{F}_{p^m}$ ve $\mathbb{F}_{p^{m'}}, \mathbb{F}_{p^n}$ cisminin alt cisimleri ise $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^{m'}}$ olması için gerek ve yeter koşul $m \mid m'$ olmasıdır.

Tanım 2. 5 $\mathbb{F}_q, q$ elemanlı sonlu bir cisim olsun. $\mathbb{F}_q^*$ devirli grubunun üreteçlerine $\mathbb{F}_q$ cisminin ilkel elemanları denir.

Tanım 2. 6 $f(x), \mathbb{F}_q[x]$ halkasında n . dereceden monik bir polinom olsun. Eğer $\mathbb{F}_q$ cisminin herhangi bir ilkel elemanı $f(x)$ polinomunun bir kökü oluyorsa, $f(x)$ polinomuna $\mathbb{F}_q[x]$ halkasında n . dereceden ilkel polinom denir.

Teorem 2. 12 $\alpha, \mathbb{F}_{q^n}$ cisminin herhangi bir elemanı olsun. α elemanının $\mathbb{F}_q$ üzerinde minimal polinomu vardır ve tektir; ayrıca $\mathbb{F}_q[x]$ halkasında indirgenemezdir.

Teorem 2. 13 Her n pozitif tam sayısı için her zaman $\mathbb{F}_q[x]$ halkasında n . dereceden ilkel polinomlar vardır. $\mathbb{F}_q[x]$ halkasında n . dereceden ilkel bir polinomun n tane kökünün hepsi $\mathbb{F}_{q^n}$ cisminin ilkel elemanıdır. $\mathbb{F}_q[x]$ halkasında n . dereceden ilkel polinomlar aynı zamanda indirgenemezdirler.

Tanım 2. 7

$$\sigma : \alpha \mapsto \alpha^q$$

$\mathbb{F}_{q^n}$ cisminin bir otomorfizmasıdır. $\sigma(\alpha) = \alpha^q$ olması için gerek ve yeter koşul $\alpha \in \mathbb{F}_q$ olmasıdır. $\mathbb{F}_q$ cisminin her elemanını sabit bırakan $\mathbb{F}_{q^n}$ cisminin otomorfizmasına, $\mathbb{F}_{q^n}$ cisminin $\mathbb{F}_q$ üzerinde bir otomorfizması denir. $\sigma, \mathbb{F}_{q^n}$ cisminin $\mathbb{F}_q$ üzerinde bir

otomorfizmasıdır ve σ ya, $\mathbb{F}_{q^n}$ cisminin $\mathbb{F}_q$ üzerindeki Frobenius otomorfizması denir.

Yrd. Teorem 2. 14 $\mathbb{F}_q$ sonlu cisminin bir $N = \{x^2 + x : x \in \mathbb{F}_q\}$ alt kümesini tanımlayalım. N , $\mathbb{F}_q$ cisminin indeksi 2 olan toplamsal bir alt grubudur ve $N^2 = N$ dir.

Teorem 2. 15 F bir cisim ve $f(x) \in F$ olsun. $(f(x))$ idealinin $F[x]$ halkasında asal olması için gerek ve yeter koşul $f(x)$ polinomunun asal eleman veya $f(x)=0$ olmasıdır.

BÖLÜM 3

$\mathbb{Z}_{p^s}[x]$ POLİNOM HALKASI

Bu bölüm, Galois Halkaları Bölümü için ön hazırlık niteliğindedir. Bu bölümde, $\mathbb{Z}_{p^s}$ kalan sınıf halkası, $\mathbb{Z}_{p^s}[x]$ polinom halkası, Hensel Yrd. Teoremi ve temel indirgenemez polinomlar gibi Galois halkalar teorisinde çok önemli olan konuları çalışacağız. [1] den yararlanarak bu konuları ele aldık.

3.1 $\mathbb{Z}_{p^s}$ Kalan Sınıf Halkası

Tanım 3.1 R birimli ve değişmeli bir halka ve m , R nin sabit bir elemanı olsun. Herhangi $a, b \in R$ elemanları için,

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b)$$

dır. Yukarıda tanımlanan bağıntı R halkasında bir denklik bağıntısıdır. Bu denklik bağıntısının R de belirttiği denklik sınıflarına, m modülüne göre kalan sınıfları denir. $a \in R$ elemanını kapsayan m modülüne göre kalan sınıfını $\bar{a}$ ile, R deki m modülüne göre kalan sınıflarının kümesini $R/(m)$ ile göstereceğiz.

$a \in R$ olsun. Bu durumda, $\bar{a} \in R/(m)$ dir. Her $b \in R$ için $b \in \bar{a}$ olması için gerek ve yeter koşulun $b \equiv a \pmod{m}$ olduğu açıktır. Diğer bir ifadeyle, bir $r \in R$ için $b = a + rm$ dir. Bu yüzden, $\bar{a} = \{a + rm : r \in R\}$ dir, ve $\bar{a}, \bar{a}' \in R/(m)$ olmak üzere $\bar{a} = \bar{a}'$ olması için gerek ve yeter koşul $\bar{a} \equiv \bar{a}' \pmod{m}$ olmasıdır.

R birimli ve deđiřmeli bir halka ve $m \in R$ olsun. m elemanının tüm katlarının kümesi, R nin toplamsal grubunun bir alt grubunu oluşturur ve bu alt grup (m) ile gösterilir. Yani, $(m) = \{rm : r \in R\}$ dir. Bu durumda, $\bar{a} = a + (m)$ olur. m , R nin sabit bir elemanı ve $\bar{a}, \bar{b} \in R/(m)$ olsun. O halde, ařađıda sırasıyla tanımlanan toplama ve çarpma işlemleriyle, $R/(m)$ halkadır:

$$\bar{a} + \bar{b} = \overline{a + b},$$

$$\overline{ab} = \bar{a}\bar{b}.$$

Tanım 3. 2 R birimli ve deđiřmeli bir halka ve m , R nin sabit bir elemanı olsun. $R/(m)$ halkasına, m modülüne göre R nin kalan sınıf halkası denir.

p bir asal, s pozitif bir tamsayı ve $\mathbb{Z}_{p^s}$, p^s modülüne göre tamsayılar halkası olsun.

$$\mathbb{Z}_{p^s} = \{0, 1, 2, \dots, p^s - 1\}$$

kabul edebiliriz. p ile aralarında asal olan her $a \in \mathbb{Z}_{p^s}$ elemanı, $\mathbb{Z}_{p^s}$ halkasında birim-seldir.

Teorem 3. 1 p bir asal sayı ve $s \geq 1$ bir tam sayı olsun. $s > 1$ ise $\mathbb{Z}_{p^s}$ sıfır bölënli bir halkadır ve her $s \geq 1$ için $\mathbb{Z}_{p^s}/(p)$, $\mathbb{Z}_p$ cismine izomorftur.

İspat: $s > 1$ olduğunu kabul edelim. $p \neq 0$ ve $p^{s-1} \neq 0$ iken $pp^{s-1} = p^s = 0$ olduğundan $\mathbb{Z}_{p^s}$ sıfır bölënli bir halkadır.

$s \geq 1$ olsun. Herhangi bir $a \in \mathbb{Z}_{p^s}$ elemanını p ile bölerek, $0 \leq r < p$ olmak üzere $a = qp + r$ elde ederiz. Bu yüzden, $\mathbb{Z}_{p^s}/(p)$ halkasında $\bar{a} = \bar{r}$ olur. Yani, $0 \leq r < p$ olmak üzere r elemanını p modülüne göre bir kalan sınıfının temsilcisi seçebiliriz. O halde,

$$\mathbb{Z}_{p^s}/(p) = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p^{s-1}}\}$$

olur. $r \in \mathbb{Z}_{p^s}/(p)$ ve $\bar{r} \neq \bar{0}$, diđer bir ifadeyle $0 < r < p$ olsun. Buradan, $\text{ebob}(r, p) = 1$ dir ve $cr + dp = 1$ olacak şekilde c, d tamsayıları vardır. Bu denklemi $\mathbb{Z}_{p^s}$ halkasında

bir denklem olarak düşünebiliriz. Böylece, $\overline{cr} = \bar{1}$ elde ederiz. $\bar{r}$ elemanının, $\mathbb{Z}_{p^s}/(p)$ halkasında tersi vardır. Bu yüzden, $\mathbb{Z}_{p^s}/(p)$, p elemanlı bir cisimdir ve $\mathbb{Z}_p$ ye izomorfudur.

Teorem 3. 2 $\mathbb{Z}_{p^s}$ halkasının bütün idealleri $(1), (p), (p^2), \dots, (p^{s-1}), (0)$ temel ideallerinden ibarettir. $\mathbb{Z}_{p^s}$ halkasının tek maksimal ideali (p) idealidir, ve $\mathbb{Z}_{p^s}/(p) \cong \mathbb{F}_p$ dir.

İspat: I , $\mathbb{Z}_{p^s}$ halkasının bir ideali olsun. $I \neq (0)$ olduğunu kabul edelim. m , I idealinde bulunan en küçük tamsayı olsun. İlk olarak, $I = (m)$ olduğunu gösterelim. $a \in I$ ve $a \notin (m)$ olsun. Buradan, $a = mk + r$ olacak şekilde $k \in \mathbb{Z}_{p^s}$ ve $0 \leq r < m$ olmak üzere $r \in \mathbb{Z}_{p^s}$ elemanları vardır. $r = a - mk \in I$ olur ve bu da m nin, I idealindeki en küçük tamsayı olmasıyla çelişir. O halde, $I = (m)$ dir. Şimdi m nin, p asalının bir kuvveti olduğunu gösterelim. $a \in \mathbb{Z}$, $a > 0$, $ebob(a, p) = 1$ ve $0 \leq i \leq s-1$ olmak üzere $m = ap^i$ olsun. $ebob(a, p) = 1$ olduğundan $ca + dp^s = 1$ olacak şekilde c , d tamsayılarını bulabiliriz. O halde, $\mathbb{Z}_{p^s}$ halkasında $ca = 1$ dir. Bu yüzden, $p^i = cap^i = cm \in I$ olur. $m = ap^i$, I idealindeki en küçük tamsayı olduğundan $a = 1$ olmak zorundadır. Bu yüzden, $I = (m) = (p^i)$ dir. Böylelikle, ilk iddiamızı ispatlamış olduk.

$(1) \supset (p) \supset (p^2) \supset \dots \supset (p^{s-1}) \supset (0)$ olduğundan $\mathbb{Z}_{p^s}$ halkasının tek maksimal ideali (p) dir. $\mathbb{Z}_{p^s}/(p) \cong \mathbb{F}_p$ olduğunu bir önceki teoremde ispatlamıştık.

3. 2 $\mathbb{Z}_{p^s}[x]$ Polinom Halkası ve İdealleri

Bu bölümde $\mathbb{Z}_{p^s}[x]$ polinom halkasını ve ideallerini çalışacağız. $0 \leq c_i \leq p-1$ olmak üzere $\mathbb{Z}_{p^s}$ halkasının elemanlarını,

$$c_0 + c_1p + \dots + c_{s-1}p^{s-1}$$

şeklinde ifade edebiliriz. Şimdi $\mathbb{Z}_{p^s}$ halkasından $\mathbb{F}_p$ cismine bir dönüşüm tanımlayalım:

$$\mathbb{Z}_{p^s} \rightarrow \mathbb{F}_p$$

$$c_0 + c_1p + \dots + c_{s-1}p^{s-1} \mapsto c_0$$

Bu dönüşüm, çekirdeği (p) olan bir halka homomorfizmasıdır ve bu homomorfizmayı “ $-$ ” ile göstereceğiz. Örneğin, $\overline{c_0 + c_1p + \dots + c_{s-1}p^{s-1}} = c_0$ dir. $- : \mathbb{Z}_{p^s} \rightarrow \mathbb{F}_p$ homomorfizmasını $\mathbb{Z}_{p^s}[x] \rightarrow \mathbb{F}_p[x]$ olacak şekilde polinom halkalarına genişletebiliriz:

$a_0, a_1, \dots, a_n \in \mathbb{Z}_{p^s}$ olmak üzere

$$\mathbb{Z}_{p^s}[x] \rightarrow \mathbb{F}_p[x]$$

$$a_0 + a_1x + \dots + a_nx^n \mapsto \overline{a_0} + \overline{a_1}x + \dots + \overline{a_n}x^n$$

Bu genişletilmiş homomorfizmayı da “ $-$ ” ile göstereceğiz. Örneğin, $f(x) \in \mathbb{Z}_{p^s}[x]$ polinomunun “ $-$ ” altındaki görüntüsü $\overline{f(x)}$ dir. Bu homomorfizmanın çekirdeği de (p) idealidir, ama

$$(p) = \mathbb{Z}_{p^s}[x]p = \left\{ f(x)p \mid f(x) \in \mathbb{Z}_{p^s}[x] \right\}$$

dir. Yani, $\mathbb{Z}_{p^s}[x]$ halkasında p ile üretilen idealdir. Genel olarak, bir $f(x) \in \mathbb{Z}_{p^s}[x]$ polinomu için, $\mathbb{Z}_{p^s}[x]$ halkasında $f(x)$ ile üretilen temel ideal

$$(f(x)) = \mathbb{Z}_{p^s}[x]f(x) = \left\{ g(x)f(x) \mid g(x) \in \mathbb{Z}_{p^s}[x] \right\}$$

şeklindedir.

Teorem 3.3 $(p) = \mathbb{Z}_{p^s}[x]p$ ideali, $\mathbb{Z}_{p^s}[x]$ halkasının asal idealidir; $\mathbb{Z}_{p^s}[x]$ halkasının her asal ideali (p) idealini kapsar; ve $\mathbb{Z}_{p^s}[x]$ halkasının (p) idealini has olarak kapsayan asal idealleri maksimaldir.

İspat: $\mathbb{Z}_{p^s}[x]/(p) \cong \mathbb{F}_p[x]$ ve $\mathbb{F}_p[x]$ tamlık bölgesi olduğundan (p) , $\mathbb{Z}_{p^s}[x]$ halkasının asal idealidir.

$P, \mathbb{Z}_{p^s}[x]$ halkasının bir asal ideali olsun. $pp^{s-1} = p^s = 0 \in P$ olduğundan $p \in P$ veya $p^{s-1} \in P$ dir. $p \in P$ ise $(p) \subseteq P$ olur. Eğer $p^{s-1} \in P$ ve $s > 2$ ise $pp^{s-2} = p^{s-1} \in P$ dir. Buradan, $p \in P$ veya $p^{s-2} \in P$ dir. Bu şekilde ilerleyerek, $p \in P$ ve dolayısıyla $(p) \subseteq P$ elde ederiz.

$P, \mathbb{Z}_{p^s}[x]$ halkasının (p) idealini has olarak kapsayan bir asal ideali olsun. P nin “-” altındaki görüntüsü $\bar{P}$ olsun. $\bar{P}$ nin, $\mathbb{F}_p[x]$ halkasının asal ideali olduğunu iddia ediyoruz. $(p) = \text{Çek} -$ ve $P \supset (p)$ olduğundan, Teorem 2. 2 (iii) den, $\bar{P}$ nin ters görüntüsü P idealidir. Bu yüzden, $\bar{P} \neq \mathbb{F}_p$ dir. $f_0(x)g_0(x) \in \bar{P}$ olacak şekilde $f_0(x), g_0(x) \in \mathbb{F}_p[x]$ olsun. O halde, $\overline{f(x)} = f_0(x), \overline{g(x)} = g_0(x)$ olacak şekilde $f(x), g(x) \in \mathbb{Z}_{p^s}[x]$ polinomları vardır. Buradan, $\overline{f(x)g(x)} \in \bar{P}$ olur. $\bar{P}$ nin ters görüntüsü P olduğundan $f(x)g(x) \in P$ dir. P asal ideal olduğundan $f(x) \in P$ veya $g(x) \in P$ dir. $f(x) \in P$ ise $f_0(x) \in \bar{P}$ dir, ve $g(x) \in P$ ise $g_0(x) \in \bar{P}$ dir. Buradan, $\bar{P}$ $\mathbb{F}_p[x]$ halkasının asal idealidir. $P, (p)$ idealini has olarak kapsadığından $\bar{P} \neq (0)$ olur. $\bar{P}$ nin, $\mathbb{F}_p[x]$ halkasının maksimal idealidir. Dolayısıyla $\mathbb{F}_p[x]/\bar{P}$ bir cisimdir. Teorem 2. 3 (iii) den,

$$\mathbb{Z}_{p^s}[x]/P \cong (\mathbb{Z}_{p^s}[x]/(p)) / (P/(p)) \cong \mathbb{F}_p[x]/\bar{P}$$

dir. Bu yüzden, P ideali $\mathbb{Z}_{p^s}[x]$ halkasının bir maksimal idealidir.

Teorem 3. 4 $Q, \mathbb{Z}_{p^s}[x]$ halkasının bir ideali olsun.

- (i) Q asalımsı ideal ise $\sqrt{Q}$ asal idealdir.
- (ii) $\sqrt{Q} \supseteq (p)$
- (iii) $\sqrt{Q}$ asal ideal ve (p) idealini has olarak kapsıyorsa Q asalımsı idealdir.

İspat: (i) Q asalımsı ideal olsun. $a, b \in \mathbb{Z}_{p^s}[x]$ olmak üzere $ab \in \sqrt{Q}$ olsun. Buradan, bir m pozitif tam sayısı için $(ab)^m \in Q$ olur. Q asalımsı olduğundan, $a^m \in Q$ veya bir

n pozitif tam sayısı için $(b^m)^n \in Q$ dur. $a^m \in Q$ ise $a \in \sqrt{Q}$ dur. Eğer $b^{mn} \in Q$ ise $b \in \sqrt{Q}$ dur. Sonuç olarak, $ab \in \sqrt{Q}$ iken $a \in \sqrt{Q}$ veya $b^{mn} \in Q$ olduğundan $\sqrt{Q}$ asal idealdir.

(ii) $p^s = 0 \in Q$ olduğundan $p \in \sqrt{Q}$ ve dolayısıyla $(p) \subseteq \sqrt{Q}$ dur.

(iii) $\sqrt{Q}$ idealinin asal ideal olduğunu ve (p) idealini has olarak kapsadığını kabul edelim. Teorem 3. 3 ten $\sqrt{Q}$ maksimal idealdir. $\sqrt{Q} \neq \mathbb{Z}_{p^s}[x]$ olduğundan $Q \neq \mathbb{Z}_{p^s}[x]$ olur. $a, b \in \mathbb{Z}_{p^s}[x]$ olmak üzere $ab \in Q$ olsun. Her m pozitif tamsayısı için $b^m \notin Q$ olduğunu kabul edelim. O halde, $b \notin \sqrt{Q}$ dur. $\sqrt{Q}$ maksimal olduğundan, $(b, \sqrt{Q})$ ideali $\mathbb{Z}_{p^s}[x]$ halkasına eşittir. $t \in \mathbb{Z}_{p^s}[x]$ ve $r \in \sqrt{Q}$ olmak üzere $1 \in \mathbb{Z}_{p^s}[x]$ birim elemanını $1 = tb + r$ şeklinde yazabiliriz. $r \in \sqrt{Q}$ olduğundan bir n pozitif tamsayısı için $r^n \in Q$ dur. Bu yüzden, $y \in \mathbb{Z}_{p^s}[x]$ olmak üzere

$$1 = 1^n = (tb + r)^n = yb + r^n$$

dir. Yukarıdaki eşitliği a ile çarparsak, $a = yab + ar^n \in Q$ elde ederiz. Bu da Q idealinin asalımsı olduğunu gösterir.

Tanım 3. 3 R bir halka ve $f(x) \neq 0$ olmak üzere $f(x) \in R[x]$ olsun. $(f(x))$ temel ideali $R[x]$ polinom halkasının asalımsı ideali ise $f(x)$ polinomuna asalımsı polinom denir.

Yrd. Teorem 3. 5 $\mathbb{Z}_{p^s}[x]$ halkasında f bir polinom olsun. $g, \mathbb{F}_p[x]$ halkasında indirgenemez bir polinom ve m pozitif bir tamsayı olmak üzere $\bar{f} = g^m$ olduğunu kabul edelim. O halde, $\mathbb{Z}_{p^s}[x]$ halkasında f asalımsı bir polinomdur.

İspat: (f) idealinin asalımsı olduğunu gösterirsek f nin asalımsı bir polinom olduğunu göstermiş oluruz. Teorem 3. 4 (ii) den $\sqrt{(f)} \supseteq (p)$ dir. $f \in (f) \subseteq \sqrt{(f)}$ ve $\bar{f} \neq 0$ olduğundan $\sqrt{(f)}, (p)$ idealini has olarak kapsar. Teorem 3. 4 (iii) den, (f) idealinin asalımsı olması için $\sqrt{(f)}$ idealinin asal olduğunu göstermemiz yeterlidir.

$1 \notin (f)$ olduğundan $1 \notin \sqrt{(f)}$ dir ve buradan, $\sqrt{(f)} \neq \mathbb{Z}_{p^s}[x]$ olur. $a, b \in \mathbb{Z}_{p^s}[x]$ ve $ab \in \sqrt{(f)}$ olsun. O halde, $(ab)^n \in (f)$ olacak şekilde bir n pozitif tamsayısı vardır. Buradan, $(\overline{ab})^n \in (\overline{f}) = (g^m)$ olur. $\mathbb{F}_p[x]$ halkası için Tek Türlü Çarpanlarına Ayrılma Teoremi'nden, $g|\overline{a}$ ve $g|\overline{b}$ olur. Eğer $g|\overline{a}$ ise $\overline{f}|\overline{a}^m$ dir. $a^m = cf + pd$ olacak şekilde $c, d \in \mathbb{Z}_{p^s}[x]$ polinomları vardır. O halde, $a^{mp^s} = c^{p^s} f^{p^s} \in (f)$ ve böylece, $a \in \sqrt{(f)}$ elde ederiz. Eğer $g|\overline{b}$ ise $b \in \sqrt{(f)}$ olduğunu benzer şekilde gösterebiliriz. Bu yüzden, $\sqrt{(f)}$ ideali asaldır.

3. 3 Hensel Yrd. Teoremi ve Temel İndirgenemez Polinomlar

Tanım 3. 4 f_1 ve $f_2 \in \mathbb{Z}_{p^s}[x]$ olsun. Eğer

$$\lambda_1 f_1 + \lambda_2 f_2 = 1$$

olacak şekilde $\mathbb{Z}_{p^s}[x]$ halkasında λ_1 ve λ_2 polinomları varsa, diğer bir ifadeyle

$$\mathbb{Z}_{p^s}[x]f_1 + \mathbb{Z}_{p^s}[x]f_2 = \mathbb{Z}_{p^s}[x]$$

oluyorsa f_1 ve f_2 aralarında asal, denir.

Aralarında asallık $\mathbb{F}_p[x]$ halkasında da benzer şekilde tanımlanır. Ayrıca, $\mathbb{F}_p[x]$ halkasında iki polinomun aralarında asal olması için gerek ve yeter koşul derecesi 1 veya 1 den büyük ortak bölenlerinin olmamasıdır.

Yrd. Teorem 3. 6 f_1 ve $f_2 \in \mathbb{Z}_{p^s}[x]$ olsun. f_1 ve f_2 polinomlarının, $\mathbb{Z}_{p^s}[x]$ halkasında aralarında asal olması için gerek ve yeter koşul $\overline{f}_1$ ve $\overline{f}_2$ polinomlarının $\mathbb{F}_p[x]$ halkasında aralarında asal olmasıdır.

İspat: $s = 1$ durumu aşikardır. $s > 1$ olsun. $\overline{f}_1$ ve $\overline{f}_2$ polinomlarının $\mathbb{F}_p[x]$ halkasında aralarında asal olduğunu kabul edelim. O halde,

$$\overline{\lambda_1 f_1} + \overline{\lambda_2 f_2} = 1$$

olacak şekilde $\mathbb{F}_p[x]$ halkasında λ_1 ve λ_2 polinomları vardır. Buradan, $k \in \mathbb{Z}_{p^s}[x]$ olmak üzere

$$\lambda_1 f_1 + \lambda_2 f_2 = 1 + pk$$

elde ederiz. $l = \sum_{i=0}^{s-1} (-pk)^i$ olsun. $\lambda_1 f_1 + \lambda_2 f_2 = 1 + pk$ eşitliğini l ile çarparsak,

$$\begin{aligned} l\lambda_1 f_1 + l\lambda_2 f_2 &= \left(\sum_{i=0}^{s-1} (-pk)^i \right) (1 + pk) \\ &= 1 - pk + (pk)^2 - \cdots + (-pk)^{s-1} + pk - (pk)^2 + \cdots - (-pk)^{s-1} + (-pk)^s \\ &= 1 \end{aligned}$$

elde ederiz. Bu yüzden, f_1 ve f_2 polinomları $\mathbb{Z}_{p^s}[x]$ halkasında aralarında asaldır.

İspatın tersi aşıkardır.

Yrd. Teorem 3. 7 (Hensel Yrd. Teoremi) $\mathbb{Z}_{p^s}[x]$ halkasında $f(x)$ monik bir polinom olsun. $\mathbb{F}_p[x]$ halkasında g_1 ve g_2 aralarında asal monik polinomlar olmak üzere $\overline{f} = g_1 g_2 \in \mathbb{F}_p[x]$ olduğunu kabul edelim. O halde,

$$f = f_1 f_2 \in \mathbb{Z}_{p^s}[x] \text{ ve } \overline{f}_1 = g_1, \overline{f}_2 = g_2$$

olacak şekilde $\mathbb{Z}_{p^s}[x]$ halkasında aralarında asal monik f_1 ve f_2 polinomları vardır.

İspat:

$$f = f_1^{(n)} f_2^{(n)} + p^{2^n} k^{(n)} \in \mathbb{Z}_{p^s}[x] \text{ ve } \overline{f_1^{(n)}} = g_1, \overline{f_2^{(n)}} = g_2 \quad (3. 1)$$

olacak şekilde her $n = 0, 1, 2, \dots$ için $\mathbb{Z}_{p^s}[x]$ halkasında $f_1^{(n)}$ ve $f_2^{(n)}$ monik polinomların çiftini ve derecesi f nin derecesinden küçük olan bir $k^{(n)} \in \mathbb{Z}_{p^s}[x]$ polinomunu kullanarak Tümevarım yöntemiyle ispat yapacağız.

$n = 0$ iken $\overline{f_1^{(0)}} = g_1$ ve $\overline{f_2^{(0)}} = g_2$ olacak şekilde $\mathbb{Z}_{p^s}[x]$ halkasında $f_1^{(0)}$ ve $f_2^{(0)}$ monik polinomlar olsun. $f - f_1^{(0)} f_2^{(0)} = pk^{(0)}$ olduğundan $f - f_1^{(0)} f_2^{(0)} \in (p)$ ve

$der(f - f_1^{(0)} f_2^{(0)}) < der(f)$ olur. Böylece, $f = f_1^{(0)} f_2^{(0)} + p k^{(0)}$ ve $der(k^{(0)}) < der(f)$ olacak şekilde $\mathbb{Z}_{p^s}[x]$ halkasında bir $k^{(0)}$ polinomu bulmuş oluruz.

$n \geq 0$ olsun. (3. 1) ifadesini sağlayacak şekilde $\mathbb{Z}_{p^s}[x]$ halkasında $f_1^{(n)}$ ve $f_2^{(n)}$ monik polinomları, ve derecesi f nin derecesinden küçük olan bir $k^{(n)} \in \mathbb{Z}_{p^s}[x]$ polinomunun varlığını kabul edelim. Teoremimizin hipotezinden, $\mathbb{F}_p[x]$ halkasında g_1 ve g_2 polinomlarının aralarında asal monik polinomlar olduğunu biliyoruz. O halde,

$$\lambda_1^{(n)} f_1^{(n)} + \lambda_2^{(n)} f_2^{(n)} = k^{(n)} \quad (3. 2)$$

olacak şekilde $\mathbb{Z}_{p^s}[x]$ halkasında $\lambda_1^{(n)}$ ve $\lambda_2^{(n)}$ polinomları vardır. $\lambda_1^{(n)}$ polinomunu $f_2^{(n)}$ ile bölersek,

$$\lambda_1^{(n)} = q_1^{(n)} f_2^{(n)} + r_1^{(n)} \quad \text{ve} \quad der(r_1^{(n)}) < der(f_2^{(n)}) \quad (3. 3)$$

olacak şekilde $\mathbb{Z}_{p^s}[x]$ halkasında $q_1^{(n)}$ ve $r_1^{(n)}$ polinomlarını bulabiliriz. Benzer şekilde,

$$\lambda_2^{(n)} = q_2^{(n)} f_1^{(n)} + r_2^{(n)} \quad \text{ve} \quad der(r_2^{(n)}) < der(f_1^{(n)}) \quad (3. 4)$$

olacak şekilde $\mathbb{Z}_{p^s}[x]$ halkasında $q_2^{(n)}$ ve $r_2^{(n)}$ polinomlarını bulabiliriz. (3. 3) ve (3. 4) denklemlerini (3. 2) de yerine yazarsak,

$$\begin{aligned} & \left[q_1^{(n)} f_2^{(n)} + r_1^{(n)} \right] f_1^{(n)} + \left[q_2^{(n)} f_1^{(n)} + r_2^{(n)} \right] f_2^{(n)} = k^{(n)} \\ & (q_1^{(n)} + q_2^{(n)}) f_1^{(n)} f_2^{(n)} = k^{(n)} - r_1^{(n)} f_1^{(n)} - r_2^{(n)} f_2^{(n)} \end{aligned} \quad (3. 5)$$

elde ederiz. Eğer $q_1^{(n)} + q_2^{(n)} \neq 0$ ise (3. 5) denkleminin sağ tarafındaki polinomun derecesi f nin derecesinden küçük, ancak sol tarafındaki polinomun derecesi f nin derecesinden büyük olur. O halde, $q_1^{(n)} + q_2^{(n)} = 0$ olmalıdır. Böylece, $r_1^{(n)} f_1^{(n)} + r_2^{(n)} f_2^{(n)} = k^{(n)}$ elde ederiz. $f_1^{(n+1)} = f_1^{(n)} + p^{2^n} r_2^{(n)}$, $f_2^{(n+1)} = f_2^{(n)} + p^{2^n} r_1^{(n)}$, ve $k^{(n+1)} = -r_1^{(n)} r_2^{(n)}$ olsun. O halde, $\mathbb{Z}_{p^s}[x]$ halkasında $f_1^{(n+1)}$ ve $f_2^{(n+1)}$ monik polinomlardır; $k^{(n+1)}$, $\mathbb{Z}_{p^s}[x]$ halkasında derecesi f nin derecesinden küçük bir polinomdur;

$\overline{f_1^{(n+1)}} = \overline{f_1^{(n)}} = g_1$ ve $\overline{f_2^{(n+1)}} = \overline{f_2^{(n)}} = g_2$ dir. Böylece tümevarım tamamlanır.

$2^l \geq s > 2^{l-1}$ olacak şekilde l bir tamsayı olsun. $f_1 = f_1^{(l)}$ ve $f_2 = f_2^{(l)}$ olsun. O halde, $\mathbb{Z}_{p^s}[x]$ halkasında f_1 ve f_2 monik polinomlardır; $f = f_1 f_2 \in \mathbb{Z}_{p^s}[x]$; $\overline{f_1} = \overline{f_1^{(l)}} = g_1$ ve $\overline{f_2} = \overline{f_2^{(l)}} = g_2$ dir. Yrd. Teorem 3. 6 ya göre, $\mathbb{Z}_{p^s}[x]$ halkasında f_1 ve f_2 aralarında asal polinomlardır.

Tümevarımla Yrd. Teorem 3. 7 yi genelleştirebiliriz.

Yrd. Teorem 3. 8 (Hensel Yrd. Teoremi) $f(x)$, $\mathbb{Z}_{p^s}[x]$ halkasında monik bir polinom olsun. $g_1, g_2, \dots, g_r$ polinomları, $\mathbb{F}_p[x]$ halkasında ikişerli aralarında asal monik polinomlar olmak üzere $\overline{f} = g_1 g_2 \dots g_r$ olsun. O halde, $\mathbb{Z}_{p^s}[x]$ halkasında $f = f_1 f_2 \dots f_r$ ve her $i = 1, 2, \dots, r$ için $\overline{f_i} = g_i$ olacak şekilde $\mathbb{Z}_{p^s}[x]$ halkasında ikişerli aralarında asal monik $f_1, f_2, \dots, f_r$ polinomları vardır.

Örnek 3. 1 $\mathbb{Z}_{3^3}[x] = \mathbb{Z}_{27}[x]$ halkasında $f(x) = x^3 + 7x^2 + 11x + 2$ monik polinomunu ele alalım. $\overline{f}(x) = x^3 + x^2 + 2x + 2 = (x^2 + 2x + 1)(x + 2) \in \mathbb{F}_3[x]$ ve $\mathbb{F}_3[x]$ halkasında $g_1(x) = x^2 + 2x + 1$ ve $g_2(x) = x + 2$ aralarında asal monik polinomlardır. Şimdi, Hensel Yrd. Teoremi'nden yararlanarak $f = f_1 f_2 \in \mathbb{Z}_{3^3}[x]$ ve $\overline{f_1} = g_1, \overline{f_2} = g_2$ olacak şekilde $\mathbb{Z}_{3^3}[x]$ halkasında aralarında asal monik f_1 ve f_2 polinomlarını bulalım.

$$f(x) = x^3 + 7x^2 + 11x + 2 = (x^2 + 2x + 1)(x + 2) + 3(x^2 + 2x)$$

şeklinde yazalım. g_1 ve g_2 polinomları, $\mathbb{Z}_{3^3}[x]$ halkasında da aralarında asal olduğundan $f_1^{(0)} = g_1$ ve $f_2^{(0)} = g_2$ alabiliriz ve $1 = (x^2 + 2x + 1) + (26x)(x + 2)$ yazabiliriz. Buradan, $k^{(0)}(x) = x^2 + 2x$ polinomunu,

$$x^2 + 2x = (x^2 + 2x)(x^2 + 2x + 1) + (x^2 + 2x)(26x)(x + 2)$$

şeklinde yazabiliriz. Bu durumda, $\lambda_1(x) = x^2 + 2x$ ve $\lambda_2(x) = 26x^3 + 25x^2$ olur. λ_1 polinomunu $f_1^{(0)}$ ile, λ_2 polinomunu $f_2^{(0)}$ ile bölersek,

$$\lambda_1 = x^2 + 2x = x(x + 2) + 0 \text{ ve } \lambda_2 = 26x^3 + 25x^2 = 26x(x^2 + 2x + 1) + x$$

elde ederiz. Burada, $q_1^{(0)}(x) = x$, $r_1^{(0)}(x) = 0$, $q_2^{(0)}(x) = 26x$, $r_2^{(0)}(x) = x$ ve $q_1^{(0)} + q_2^{(0)} = 0$ dır. $f_1^{(1)} = f_1^{(0)} + 3^{2^0} r_2^{(0)}$ ve $f_2^{(1)} = f_2^{(0)} + 3^{2^0} r_1^{(0)}$ polinomlarını yazalım. $f_1^{(1)}(x) = x^2 + 2x + 1 + 3x = x^2 + 5x + 1$ ve $f_2^{(1)}(x) = x + 2 + 3 \cdot 0 = x + 2$ elde ederiz. Böylece,

$$f_1^{(1)}(x) f_2^{(1)}(x) = (x^2 + 5x + 1)(x + 2) = x^3 + 7x^2 + 11x + 2 = f(x)$$

olur. Ayrıca, $x^2 + 5x + 1$ ve $x + 2$ polinomları $\overline{x^2 + 5x + 1} = x^2 + 2x + 1$ ve $\overline{x + 2} = x + 2$ olacak şekilde $\mathbb{Z}_3[x]$ halkasında aralarında asaldır.

Teorem 3. 9 (Tek Türlü Çarpanlarına Ayrılma Teoremi) $f(x)$, $\mathbb{Z}_{p^s}[x]$ halkasında monik bir polinom ve $\text{der}(f) \geq 1$ olsun. O halde,

(i) r pozitif bir tamsayı ve her $i = 1, 2, \dots, r$ için $\overline{f_i}$, $\mathbb{F}_p[x]$ halkasında monik indirgenemez bir polinomun bir kuvveti olmak üzere f , $\mathbb{Z}_{p^s}[x]$ halkasında $f = f_1 f_2 \dots f_r$ olacak şekilde ikişerli aralarında asal monik asalımsı $f_1, f_2, \dots, f_r$ polinomlarının çarpımı şeklinde yazılabilir.

$$(ii) f = f_1 f_2 \dots f_r = h_1 h_2 \dots h_t \quad (3. 6)$$

$\mathbb{Z}_{p^s}[x]$ halkasında ikişerli aralarında asal monik asalımsı polinomların çarpımı olacak şekilde f polinomunun iki türlü yazılışı olsun. O halde, $r = t$ dir ve sıralamaya bakılmaksızın $i = 1, 2, \dots, r$ için $f_i = h_i$ dir.

İspat: (i) $\mathbb{F}_p[x]$ halkası için tek türlü çarpanlarına ayırma teoreminden, $\mathbb{F}_p[x]$ halkasında $g_1, g_2, \dots, g_r$ farklı monik indirgenemez polinomlar ve $e_1, e_2, \dots, e_r$ pozitif tamsayılar olmak üzere $\overline{f} = g_1^{e_1} g_2^{e_2} \dots g_r^{e_r}$ yazabiliriz. Hensel Yrd. Teoremi'nden, $f = f_1 f_2 \dots f_r$ ve $i = 1, 2, \dots, r$ için $\overline{f_i} = g_i^{e_i}$ olacak şekilde $\mathbb{Z}_{p^s}[x]$ halkasında ikişerli aralarında asal monik $f_1, f_2, \dots, f_r$ polinomları vardır. Yrd. Teorem 3. 5 ten, $i = 1, 2, \dots, r$ için $f_i \in \mathbb{Z}_{p^s}[x]$ polinomları asalımsıdır.

(ii) (3. 6) eşitliğinden, her $i = 1, 2, \dots, t$ için $f_1 f_2 \dots f_r \in (h_i)$ olduğunu söyleyebiliriz. h_i asalımsı olduğundan (h_i) asalımsı idealdir. O halde, $f_{k_i}^{n_i} \in (h_i)$ olacak şekilde bir n_i pozitif tamsayısı ve $1 \leq k_i \leq r$ olmak üzere bir k_i tamsayısı vardır. k_i tamsayısının tek türlü belirlendiğini iddia ediyoruz. $f_{k_i'}^{n_i'} \in (h_i)$ olacak şekilde farklı bir $k_i' \neq k_i$ tamsayısı ve n_i' pozitif tamsayısı olsun. f_{k_i} ve $f_{k_i'}$ polinomları $\mathbb{Z}_{p^s}[x]$ halkasında aralarında asal polinomlar olduğundan $1 = af_{k_i} + bf_{k_i'}$ olacak şekilde $a, b \in \mathbb{Z}_{p^s}[x]$ polinomları vardır. O halde,

$$1 = 1^{n_i + n_i' - 1} = \left(af_{k_i} + bf_{k_i'} \right)^{n_i + n_i' - 1} \in (h_i)$$

olur. Bu ise (h_i) idealinin asalımsı olmasıyla çelişir.

Benzer şekilde, her $j = 1, 2, \dots, r$ için $h_{l_j}^{m_j} \in (f_j)$ olacak şekilde bir m_j pozitif tamsayısı ve $1 \leq l_j \leq t$ olmak üzere tek türlü belirli bir l_j tamsayısı vardır. Her $j = 1, 2, \dots, r$ için $h_{l_j}^{m_j} \in (f_j)$ ve her $1 \leq k_i \leq r$ için $f_{k_i}^{n_i} \in (h_i)$ olduğundan her $i = 1, 2, \dots, t$ için $h_{l_{k_i}}^{m_{k_i} n_i} \in (h_i)$ olur. Buradan, $\bar{h}_{l_{k_i}}^{m_{k_i} n_i} \in (\bar{h}_i)$ dir. $i \neq j$ için hem h_i ve h_j polinomları hem de $\bar{h}_i$ ve $\bar{h}_j$ polinomları aralarında asal olduğundan her $i = 1, 2, \dots, t$ için $l_{k_i} = i$ olmak zorundadır. Buradan,

$$\{1, 2, \dots, t\} \rightarrow \{1, 2, \dots, r\}$$

$$i \mapsto k_i$$

iyi tanımlı birebir dönüşümünü yazabiliriz. Bu yüzden, $t \leq r$ dir. Benzer şekilde, $r \leq t$ olduğundan $r = t$ elde ederiz. Sıralamayı yeniden yaptıktan sonra her $i = 1, 2, \dots, r$ için $k_i = i$ kabul edebiliriz. O halde, her $i = 1, 2, \dots, r$ için $l_i = i$ dir. Buradan, her $i = 1, 2, \dots, r$ için $f_i^{n_i} \in (h_i)$ ve $h_i^{m_i} \in (f_i)$ olur.

$j \neq 1$ için, f_j ve f_1 aralarında asal polinomlardır. $\bar{f}_j$ ve $\bar{f}_1$ polinomlarının da aralarında asal olduğunu Yrd. Teorem 3. 6 dan biliyoruz. $\bar{f}_j$ ve $\bar{f}_1^{n_1}$ aralarında asaldır.

Bu yüzden, $\bar{f}_2 \bar{f}_3 \dots \bar{f}_r$ ve $\bar{f}_1^{n_1}$ polinomları da aralarında asaldır. Yrd. Teorem 3. 6 dan,

$f_2 f_3 \dots f_r$ ve $f_1^{n_1}$ polinomları aralarında asaldır. $f_1^{n_1} \in (h_1)$ olduğundan $f_2 f_3 \dots f_r$ ve h_1 aralarında asaldır. O halde,

$$cf_2 f_3 \dots f_r + dh_1 = 1$$

olacak şekilde $c, d \in \mathbb{Z}_{p^s}[x]$ polinomları vardır. Yukarıdaki eşitliğin her iki tarafını f_1 ile çarparsak,

$$f_1 = cf_1 f_2 \dots f_r + df_1 h_1 = ch_1 h_2 \dots h_r + df_1 h_1$$

elde ederiz. Bu da $h_1 \mid f_1$ olmasını gerektirir. Benzer şekilde, $f_1 \mid h_1$ elde edebiliriz. f_1 ve h_1 polinomlarının ikisi de monik olduğundan $f_1 = h_1$ dir. Benzer şekilde, her $i = 2, \dots, r$ için de $f_i = h_i$ yazabiliriz.

Tanım 3. 6 $f(x)$, $\mathbb{Z}_{p^s}[x]$ halkasında monik bir polinom ve $\text{der}(f(x)) = m \geq 1$ olsun. $\overline{f}(x)$ polinomu, $\mathbb{F}_p[x]$ halkasında indirgenemez (veya ilkel) ise $f(x)$ polinomuna $\mathbb{Z}_{p^s}[x]$ halkasında monik temel indirgenemez (veya monik temel ilkel) polinom denir. $\mathbb{Z}_{p^s}[x]$ halkasında monik temel ilkel polinomlar monik temel indirgenemezdir.

Örnek 3. 1 $\mathbb{Z}_4[x]$ halkasında 2. dereceden $h(x) = x^2 + 3x + 3$ monik polinomunu ele alalım. $\overline{h}(x) = \overline{x^2 + 3x + 3} = x^2 + \overline{3}x + \overline{3} = x^2 + x + 1$ $\mathbb{F}_2[x]$ halkasında indirgenemez olduğundan $h(x)$, $\mathbb{Z}_4[x]$ halkasında monik temel indirgenemez bir polinomdur.

Teorem 3. 10 Her $m \geq 1$ tam sayısı için $\mathbb{Z}_{p^s}[x]$ halkasında $x^{p^m-1} - 1$ polinomunu bölen m . dereceden monik temel indirgenemez (ve monik temel ilkel) polinomlar vardır.

İspat: $\mathbb{F}_p[x]$ halkasında m . dereceden monik indirgenemez polinomların varlığını Teorem 2. 12 den; m . dereceden monik temel ilkel polinomların varlığını Teorem 2. 13 ten biliyoruz. Yrd. Teorem 2. 10 dan bu polinomlar $\mathbb{F}_p[x]$ halkasında $x^{p^m-1} - 1$ i böler.

Bu polinomlardan birine $f_p(x)$ diyelim ve $g_p(x) = (x^{p^m-1} - 1) / f_p(x)$ olsun. Buradan,

$$x^{p^m-1} - 1 = f_p(x)g_p(x) \in \mathbb{F}_p[x]$$

olur. $x^{p^m-1} - 1$ polinomunun katlı kökü olmadığından $f_p(x)$ ve $g_p(x)$ $\mathbb{F}_p[x]$ halkasında aralarında asal polinomlardır. Hensel Yrd. Teoremi'nden dolayı,

$$x^{p^m-1} - 1 = f(x)g(x) \in \mathbb{Z}_{p^s}[x] \quad \text{ve} \quad \overline{f}(x) = f_p(x), \overline{g}(x) = g_p(x)$$

olacak şekilde $\mathbb{Z}_{p^s}[x]$ halkasında $f(x)$ ve $g(x)$ monik polinomları vardır. Buradan, $\text{der}(f(x)) = \text{der}(f_p(x)) = m$ olur. Bu yüzden, $f(x)$ polinomu $\mathbb{Z}_{p^s}[x]$ halkasında m . dereceden monik temel indirgenemezdir (monik temel ilkeldir) ve $\mathbb{Z}_{p^s}[x]$ halkasında $x^{p^m-1} - 1$ i böler.

BÖLÜM 4

GALOIS HALKALARI

Bu bölümde, son zamanlarda başta Kodlama Teorisi olmak üzere bir çok uygulama alanı olan ve akademisyenlerin dikkatini çeken Galois halkalarını çalışacağız. Sırasıyla, Galois halkalarının tanımı ve örnekleri, yapısı, p -adik gösterimi, birimselleri, genişlemeleri, otomorfizmaları ve son olarak iz ve norm tanımlarını vereceğiz. Galois Halkaları Bölümü'nü oluştururken [1], [3], [4] ten yararlanarak derleme niteliğinde bir çalışma yaptık ve ayrıca çalışmalarımızı daha somut hale getirmek için örneklere yer verdik.

4. 1 Galois Halkası Tanımı ve Örnekleri

Tanım 4. 1 p bir asal sayı olsun. Birimi 1 olan değişmeli sonlu bir halkada, halkanın sıfırı ve sıfır bölenleri (p) idealini oluşturuyorsa bu halkaya Galois halkası denir.

$$p1 = \underbrace{1 + 1 + \dots + 1}_{p \text{ tane}}.$$

Örnek 4. 1 p bir asal sayı ve s pozitif bir tamsayı olmak üzere $\mathbb{Z}_{p^s}$ halkası bir Galois halkasıdır.

$1 \in \mathbb{Z}_{p^s}$ ve $\mathbb{Z}_{p^s}$ sonlu bir halkadır. $\mathbb{Z}_{p^s}$ halkasının sıfırı ve sıfır bölenlerinin (p) idealini oluşturduğunu gösterelim. $\mathbb{Z}_{p^s}$ halkasının sıfır bölenlerinin kümesini Ω ile gösterelim.

$$\begin{aligned}\Omega &= \{a \in \mathbb{Z}_{p^s} \mid (a, p^s) \neq 1\} \\ &= \{a \in \mathbb{Z}_{p^s} \mid (a, p) \neq 1\}\end{aligned}$$

$$= \{a \in \mathbb{Z}_{p^s} \mid p \mid a\}.$$

Buradan, $\Omega \subseteq (p)$ olur. Şimdi ters kapsamayı gösterelim:

$0 \neq a \in (p)$ olsun. $a = pk$ olacak şekilde en az bir tane $k \in \mathbb{Z}$ vardır. $p^{s-1}a = p^s k = 0$ olduğundan $a \in \mathbb{Z}_{p^s}$ sıfır bölendir. O halde, $(p) \subseteq \Omega$ dır. Sonuç olarak, $\mathbb{Z}_{p^s}$ halkasının sıfırı ve sıfır bölenleri (p) idealini oluşturduğundan $\mathbb{Z}_{p^s}$ bir Galois halkasıdır.

Teorem 3. 2 den $\mathbb{Z}_{p^s}$ halkasının tek maksimal idealinin (p) olduğunu biliyoruz. $s = 1$ iken $\mathbb{Z}_{p^s} = \mathbb{F}_p$, p elemanlı cisim ve $(p) = 0$ olur.

Örnek 4. 2 $\mathbb{Z}_{2^3} = \mathbb{Z}_8$ halkasını ele alalım. $\mathbb{Z}_8$ halkasının sıfır bölenleri $\{2, 4, 6\}$ dır. $(2) = \{0, 2, 4, 6\}$ olduğundan $\mathbb{Z}_8$ bir Galois halkasıdır.

Örnek 4. 3 $h(x)$, $\mathbb{Z}_{p^s}[x]$ halkasında m . dereceden monik temel indirgenemez bir polinom olsun. $\mathbb{Z}_{p^s}[x]/(h(x))$ bölüm halkası bir Galois halkasıdır.

$$\mathbb{Z}_{p^s}[x]/(h(x)) = \{a_0 + a_1x + \dots + a_{m-1}x^{m-1} + (h(x)) \mid a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}_{p^s}\}$$

oldüğundan $|\mathbb{Z}_{p^s}[x]/(h(x))| = p^{sm}$ dir. $1 + (h(x)) \in \mathbb{Z}_{p^s}[x]$ halkanın birimi ve $0 + (h(x))$ halkanın sıfırıdır. Yani, $\mathbb{Z}_{p^s}[x]/(h(x))$ sonlu ve birimli bir halkadır. Galois halkası tanımından,

$$p(1 + (h(x))) = \underbrace{1 + (h(x)) + \dots + 1 + (h(x))}_{p \text{ tane}} = \underbrace{1 + \dots + 1}_{p \text{ tane}} + (h(x)) = p + (h(x))$$

oldüğundan $(p(1 + (h(x)))) = (p + (h(x)))$ dir.

$\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının sıfırı ve sıfır bölenlerinin $(p + (h(x)))$ idealini oluşturduğunu gösterelim:

$$[a_0 + a_1x + \dots + a_{m-1}x^{m-1} + (h(x))][p + (h(x))] \in (p + (h(x)))$$

$(p + (h(x)))$ idealinin herhangi bir elemanını alalım.

$$\underbrace{\left[p^{s-1} + (h(x)) \right]}_{\neq 0} \underbrace{\left[a_0 + a_1x + \dots + a_{m-1}x^{m-1} + (h(x)) \right]}_{\neq 0} \left[p + (h(x)) \right] = (h(x))$$

olduğundan $(p + (h(x)))$ idealinin sıfırdan farklı bütün elemanları $\mathbb{Z}_{p^s}[x]/(h(x))$ hal-
kasının sıfır bölenidir.

$0 \leq c_i \leq p-1$ olmak üzere

$$- : \mathbb{Z}_{p^s} \rightarrow \mathbb{F}_p$$

$$c_0 + c_1p + \dots + c_{s-1}p^{s-1} \mapsto c_0$$

homomorfizmasını daha önce tanımlamıştık ve $\text{çek}-(p)$ olduğunu biliyoruz. Daha
sonra, $a_0, a_1, \dots, a_n \in \mathbb{Z}_{p^s}$ olmak üzere

$$- : \mathbb{Z}_{p^s}[x] \rightarrow \mathbb{F}_p[x]$$

$$a_0 + a_1x + \dots + a_nx^n \mapsto \overline{a_0} + \overline{a_1}x + \dots + \overline{a_n}x^n,$$

genişletilmiş homomorfizmasını elde etmiştik ve $\text{çek}-(p)$ nin, $\mathbb{Z}_{p^s}[x]$ halkasında p
ile üretilen temel ideal olduğunu söylemiştik. $(h(x))$ idealinin görüntüsü $(\overline{h}(x))$ ideali-
dir. $a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}_{p^s}$ olmak üzere

$$- : \mathbb{Z}_{p^s}[x]/(h(x)) \rightarrow \mathbb{F}_p[x]/(\overline{h}(x)) \quad (4.1)$$

$$a_0 + \dots + a_{m-1}x^{m-1} + (h(x)) \mapsto \overline{a_0} + \dots + \overline{a_{m-1}}x^{m-1} + (\overline{h}(x))$$

bir halka homomorfizmasıdır. Bu homomorfizmanın çekirdeği $(p + (h(x)))$ idealidir.
Halkalar için Temel Homomorfizma Teoremi'nden,

$$\mathbb{Z}_{p^s}[x]/(h(x))/(p + (h(x))) \cong \mathbb{F}_p[x]/(\overline{h}(x))$$

dir. $h(x)$, $\mathbb{Z}_{p^s}[x]$ halkasında monik temel indirgenemez bir polinom olduğundan $\overline{h}(x)$,

$\mathbb{F}_p[x]$ halkasında m . dereceden monik indirgenemez bir polinomdur ve $\mathbb{F}_p[x]/(\overline{h}(x))$

bir $\mathbb{F}_{p^m}$ Galois cismidir. Bu yüzden, $p + (h(x))$ ile üretilen $(p + (h(x)))$ temel ideali

$\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının bir maksimal idealidir.

Şimdi $\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının sıfır bölenlerinin $(p+(h(x)))$ idealinin elemanları olduğunu gösterelim:

$a(x)+(h(x)) \in \mathbb{Z}_{p^s}[x]/(h(x))$ sıfır bölen olsun. $a(x)+(h(x)) \notin (p+(h(x)))$ olduğunu kabul edelim. $(p+(h(x)))$, $\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının maksimal idealidir. Buradan, $(a(x)+(h(x)), p+(h(x))) = \mathbb{Z}_{p^s}[x]/(h(x))$ dir. O halde,

$$1+(h(x)) = [b(x)+(h(x))][a(x)+(h(x))] + [c(x)+(h(x))][p+(h(x))]$$

olacak şekilde $b(x)+(h(x))$ ve $c(x)+(h(x)) \in \mathbb{Z}_{p^s}[x]/(h(x))$ elemanları vardır. Sonra,

$$1+(h(x)) = b(x)a(x) + pc(x) + (h(x))$$

elde ederiz. $1+(h(x)), \mathbb{Z}_{p^s}[x]/(h(x))$ halkasının birimi olduğu için $c_1(x) \in \mathbb{Z}_{p^s}[x]$ olmak üzere

$$1+(h(x)) = [1+(h(x))]^p = [b(x)a(x)]^p + p^2c_1(x) + (h(x))$$

olur. Benzer şekilde, $c_2(x) \in \mathbb{Z}_{p^s}[x]$ olmak üzere

$$1+(h(x)) = [1+(h(x))]^{p^2} = [b(x)a(x)]^{p^2} + p^3c_2(x) + (h(x))$$

olur. Bu şekilde devam ederek, $(s-1)$. adımda, $c_{s-1}(x) \in \mathbb{Z}_{p^s}[x]$ olmak üzere

$$\begin{aligned} 1+(h(x)) &= [1+(h(x))]^{p^{s-1}} = [b(x)a(x)]^{p^{s-1}} + p^s c_{s-1}(x) + (h(x)) \\ &= [b(x)a(x)]^{p^{s-1}} + (h(x)) \\ &= [a(x)+(h(x))][b(x)^{p^{s-1}}a(x)^{p^{s-1}-1} + (h(x))] \end{aligned}$$

elde ederiz. Buradan, $a(x)+(h(x))$ birimsel olur. Bu ise $a(x)+(h(x))$ elemanının sıfır bölen olması ile çelişir. Çelişki $a(x)+(h(x)) \notin (p+(h(x)))$ kabul ettiğimizden oluştu. Sonuç olarak, $\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının sıfırı ve sıfır bölenleri $(p+(h(x)))$ idealini oluşturduğundan, $\mathbb{Z}_{p^s}[x]/(h(x))$ bir Galois halkasıdır. $\mathbb{Z}_{p^s}[x]/(h(x)) \setminus (p+(h(x)))$

deki her eleman birimsel olduğundan $(p + (h(x)))$ ideali, $\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının tek maksimal idealidir.

$\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının, $a \in \mathbb{Z}_{p^s}$ olmak üzere $a + (h(x))$ şeklindeki elemanlarından oluşan bir R_0 alt halkası vardır.

$$\mathbb{Z}_{p^s} \rightarrow R_0$$

$$a \mapsto a + (h(x))$$

dönüşümü bir izomorfizmadır. Bu yüzden, $\mathbb{Z}_{p^s}$ halkasının her a elemanını, $\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının $a + (h(x))$ elemanı olarak düşünebiliriz ve $\mathbb{Z}_{p^s}$ yi, $\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının bir alt halkası olarak alabiliriz. $(p + (h(x)))$ idealini de (p) şeklinde yazabiliriz.

$\xi = x + (h(x))$ yazalım. O halde, $\xi = \xi + (h(\xi))$ ve dolayısıyla $h(\xi) = 0$ olur. Buradan,

$$a_0 + a_1x + \dots + a_{m-1}x^{m-1} + (h(x)) = a_0 + a_1\xi + \dots + a_{m-1}\xi^{m-1}$$

olacağından $\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının her elemanını

$$a_0 + a_1\xi + \dots + a_{m-1}\xi^{m-1}, \quad a_i \in \mathbb{Z}_{p^s} \quad a_i \in \mathbb{Z}_{p^s} (i = 0, 1, \dots, m-1) \quad (4.2)$$

şeklinde tek türlü ifade edebiliriz. O halde,

$$\mathbb{Z}_{p^s}[x]/(h(x)) = \mathbb{Z}_{p^s}[\xi] = \{a_0 + a_1\xi + \dots + a_{m-1}\xi^{m-1}, a_i \in \mathbb{Z}_{p^s} (i = 0, 1, \dots, m-1)\}$$

şeklinde gösterebiliriz, ve $\mathbb{Z}_{p^s}[\xi]$ halkasının bir Galois halkası olduğunu söyleyebiliriz.

$\mathbb{Z}_{p^s}[\xi]$ halkasının elemanlarının bu tek tek türlü yazılımına toplamsal gösterim denir.

$\mathbb{Z}_{p^s}[\xi]$ Galois halkasındaki toplama ve çarpma işlemleri şu şekilde tanımlanır:

$a(\xi), b(\xi) \in \mathbb{Z}_{p^s}[\xi]$ olmak üzere

$$a(\xi) = a_0 + a_1\xi + \dots + a_{m-1}\xi^{m-1}, b(\xi) = b_0 + b_1\xi + \dots + b_{m-1}\xi^{m-1}$$

olsun. $\mathbb{Z}_{p^s}[x]$ halkasında $a(x)b(x)$ polinomunun $h(x)$ ile bölümünden kalan $r(x)$ olsun.

$$a(\xi) + b(\xi) = (a_0 + b_0) + (a_1 + b_1)\xi + \cdots + (a_{m-1} + b_{m-1})\xi^{m-1} \quad \text{ve} \quad a(\xi)b(\xi) = r(\xi)$$

$\xi = x + (h(x))$ elemanın (4. 1) homomorfizması altındaki görüntüsü $\bar{\xi}$ olsun. Buradan, $\bar{\xi} = x + (\bar{h}(x))$ ve $\bar{h}(\bar{\xi}) = 0$ olur. Yani, $\mathbb{F}_p[x]$ halkasında $\bar{\xi}$ monik indirgenemez $\bar{h}(x)$ polinomunun bir köküdür. O halde,

$$\mathbb{F}_p[x]/(\bar{h}(x)) = \mathbb{F}_p[\bar{\xi}] \cong \mathbb{F}_{p^m}$$

dir. Ayrıca (4. 1) homomorfizmasını şu şekilde de yazabiliriz:

$$-: \mathbb{Z}_{p^s}[\xi] \rightarrow \mathbb{F}_p[\bar{\xi}]$$

$$a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1} + (h(x)) \mapsto \bar{a}_0 + \bar{a}_1\bar{\xi} + \cdots + \bar{a}_{m-1}\bar{\xi}^{m-1} \quad (4. 3)$$

O halde, aşağıdaki değişmeli diyagramı yazabiliriz:

$$\begin{array}{ccc} \mathbb{Z}_{p^s}[x] & \xrightarrow{-} & \mathbb{F}_p[x] \\ \downarrow & & \downarrow \\ \mathbb{Z}_{p^s}[\xi] & \xrightarrow{-} & \mathbb{F}_p[\bar{\xi}] \end{array}$$

Eğer monik temel indirgenemez $h(x)$ polinomunun derecesi 1 ise $\mathbb{Z}_{p^s}[x]/(h(x)) = \mathbb{Z}_{p^s}$ dir. Eğer $s = 1$ ve $\deg(h(x)) = m$ ise $\mathbb{Z}_{p^s}[x]/(h(x)) = \mathbb{F}_p[x]/(h(x)) \cong \mathbb{F}_{p^m}$ dir.

Örnek 4. 4 $h(x) = x^2 + 3x + 3 \in \mathbb{Z}_2[x]$ polinom halkasında 2. dereceden monik temel indirgenemez bir polinom olduğunu daha önce söylemiştik. Şimdi $\mathbb{Z}_2[x]/(x^2 + 3x + 3)$ halkasının Galois halkası olduğunu gösterelim.

$$\mathbb{Z}_2[x]/(x^2 + 3x + 3) = \left\{ \begin{array}{l} 0 + (x^2 + 3x + 3), \dots, 3 + (x^2 + 3x + 3), \\ x + (x^2 + 3x + 3), \dots, x + 3 + (x^2 + 3x + 3), \\ 2x + (x^2 + 3x + 3), \dots, 2x + 3 + (x^2 + 3x + 3), \\ 3x + (x^2 + 3x + 3), \dots, 3x + 3 + (x^2 + 3x + 3) \end{array} \right\}$$

ve $|\mathbb{Z}_2[x]/(x^2 + 3x + 3)| = 2^{2.2} = 16$ dir.

$\mathbb{Z}_2[x]/(x^2 + 3x + 3)$ halkasının sıfırı $0 + (x^2 + 3x + 3)$; sıfır bölenleri $2 + (x^2 + 3x + 3)$,

$2x + (x^2 + 3x + 3)$ ve $2x + 2 + (x^2 + 3x + 3)$ elemanlarıdır.

$(2 + (x^2 + 3x + 3)) = \{0 + (x^2 + 3x + 3), 2 + (x^2 + 3x + 3), 2x + (x^2 + 3x + 3), 2x + 2 + (x^2 + 3x + 3)\}$ ideali $\mathbb{Z}_2[x]/(x^2 + 3x + 3)$ halkasının sıfırı ve sıfır bölenlerinden oluştuğundan $\mathbb{Z}_2[x]/(x^2 + 3x + 3)$ bir Galois halkasıdır.

$$\begin{array}{ccc} \mathbb{Z}_4[x] & \xrightarrow{\quad} & \mathbb{F}_2[x] \\ \downarrow & & \downarrow \\ \mathbb{Z}_4[\xi] & \xrightarrow{\quad} & \mathbb{F}_2[\bar{\xi}] \end{array}$$

Tanım 4. 2 Değişmeli ve birimli bir halkada, halkanın biriminin toplamsal gruptaki mertebesine halkanın karakteristiği denir.

$\mathbb{Z}_{p^s}$ halkasının karakteristiği p^s dir. $h(x)$, $\mathbb{Z}_{p^s}[x]$ halkasında monik temel indirgenemez bir polinom olmak üzere $\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının karakteristiği p^s dir.

Karakteristiği p^s ve kardinalitesi p^{sm} olmak üzere, $\mathbb{Z}_{p^s}[x]/(h(x))$ Galois halkasını $GR(p^s, p^{sm})$ ile göstereceğiz. Özel olarak, $\mathbb{Z}_{p^s}$ Galois halkasını $GR(p^s, p^s)$ ile göstereceğiz.

Şimdi Örnek 4. 3 ten elde ettiğimiz sonuçları aşağıdaki teoremle özetleyelim.

Teorem 4. 1 $h(x)$, $\mathbb{Z}_{p^s}[x]$ halkasında m . dereceden monik temel indirgenemez bir polinom olsun. O halde, $\mathbb{Z}_{p^s}[x]/(h(x))$ kalan sınıf halkası, karakteristiği p^s ve kardinalitesi p^{sm} olan bir Galois halkasıdır; ve $GR(p^s, p^{sm})$ ile gösterilir. $\mathbb{Z}_{p^s}$, $\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının bir alt halkasıdır. $\xi = x + (h(x))$ için $h(\xi) = 0$ dir ve $\mathbb{Z}_{p^s}[x]/(h(x))$ halkasının her elemanını, (4. 2) de gösterdiğimiz şekilde tek türlü ifade edebiliriz. $\mathbb{Z}_{p^s}[\xi]$ halkasının (p) ideali, $\mathbb{Z}_{p^s}[\xi]$ halkasının sıfırı ve bütün sıfır bölenlerinden oluşur. (p) , $\mathbb{Z}_{p^s}[\xi]$ halkasının tek maksimal idealidir. $\xi = x + (h(x))$ elemanının (4. 1) homomorfizması altındaki görüntüsü $\bar{\xi}$ ile gösterirsek, $\bar{\xi} = x + (\bar{h}(x))$

ve $\bar{h}(\bar{\xi}) = 0$ dır. Bu yüzden, $\mathbb{F}_p[x]/(\bar{h}(x)) = \mathbb{F}_p[\bar{\xi}] = \mathbb{F}_{p^m}$ dir ve (4. 1) homorfizmasını (4. 3) deki gibi yazabiliriz. Son olarak, aşağıdaki değişmeli diyagramı yazabiliriz.

$$\begin{array}{ccc} \mathbb{Z}_{p^s}[x] & \xrightarrow{\quad \bar{\quad} \quad} & \mathbb{F}_p[x] \\ \downarrow & & \downarrow \\ \mathbb{Z}_{p^s}[\xi] & \xrightarrow{\quad \bar{\quad} \quad} & \mathbb{F}_p[\bar{\xi}] \end{array}$$

4. 2 Galois Halkalarının Yapısı

Yrd. Teorem 4. 2 R bir Galois halkası olsun. R nin sıfırı ve sıfır bölenlerinin oluşturduğu ideal, bir p asalı için $(p1)$ idealini oluştursun. O halde, $(p1)$ ideali R nin tek maksimal idealidir; $R/(p1)$, bir $m \in \mathbb{Z}^+$ için $\mathbb{F}_{p^m}$ Galois cismidir; ve R nin karakteristiği p nin bir kuvvetidir.

İspat: $(p1) \subset I \subseteq R$ olacak şekilde R nin bir I idealini alalım. $a \notin (p1)$ olacak şekilde $\exists a \in I$ vardır. $a \notin (p1)$ ise a sıfır bölen değildir. Sonlu halkada sıfır bölen olmayan sıfırdan farklı her eleman birimseldir. $a \in I$ birimselse $I = R$ dir. Bu yüzden, $(p1)$ ideali R nin tek maksimal idealidir. $(p1)$ maksimal ideal olduğundan, $R/(p1)$ cisimdir.

$$\begin{aligned} - : R &\rightarrow R/(p1) \\ r &\mapsto \bar{r} \end{aligned}$$

doğal homomorfizmasını göz önüne alalım. $a \in R$ veya $a \in R/(p1)$ için, $\underbrace{a + a + \dots + a}_n$ toplamını na ile gösterirsek $p\bar{1} = \overline{p1} = \bar{0}$ olduğundan $R/(p1)$ cisminin karakteristiği p dir. Sonuç olarak, $R/(p1)$ karakterisitiği p olan sonlu bir cisimdir.

R nin karakteristiği k olsun. Buradan, $k1 = 0$ dır.

$$k\bar{1} = k(1 + (p1)) = k1 + (p1) = 0 + (p1) = \bar{0}$$

ve $R/(p1)$ nin karakteristiği p olduğundan $p|k$ dır. Bu durumda, $k = p^s l$ ve $(p, l) = 1$ olacak şekilde s ve l poizitif tamsayıları vardır. Eğer $l > 1$ ise $a = p^s 1$ ve $b = l1$, R nin

sıfırdan farklı elemanlarıdır ve $ab = p^s 1l = k1 = 0$ dir. Buradan, $l1$ sıfır bölen ve dolayısıyla $l1 \in (p1)$ olur. O halde, $\bar{l}1 = \bar{0} = \bar{l}1$ dir. $R/(p1)$ cisminin karakteristiği p olduğundan $p|l$ dir. Bu ise $(p, l) = 1$ olması ile çelişir. Bu yüzden, $l = 1$ ve $k = p^s$ dir.

Örnek 4. 5 $\mathbb{Z}_{16}$ bir Galois halkasıdır ve (2) , $\mathbb{Z}_{16}$ halkasının tek maksimal idealidir. $3, 5, 7, 9, 11, 13, 15$ birimsel olduklarından $(3) = (5) = (7) = (9) = (11) = (13) = (15) = \mathbb{Z}_{16}$ dir. Sıfır bölenleri $2, 4, 6, 8, 10, 12, 14$ olduğundan $(2) = \{0, 2, 4, 6, 8, 10, 12, 14\}$ dir. Yrd. Teorem 4. 2 ye göre, $\mathbb{Z}_{16}$ halkasının tek maksimal idealidir. Gerçekten, $\mathbb{Z}_{16}$ halkasının has idealleri $(2) = (6), (4) = (10), (8) = (12) = (14)$ ve $(8) \subset (4) \subset (2)$ olduğundan (2) , $\mathbb{Z}_{16}$ halkasının tek maksimal idealidir. Buradan, $\mathbb{Z}_{16}/(2)$ bir cisimdir ve

$$\mathbb{Z}_{16}/(2) = \{0 + (2), 1 + (2)\}$$

oldüğundan $\mathbb{Z}_{16}/(2) \cong \mathbb{F}_2$ dir. $16 \cdot \bar{1} = \bar{0}$ ve bu eşitliği sağlayan en küçük pozitif tamsayı 16 olduğundan $\mathbb{Z}_{16}$ halkasının karakteristiği $2^4 = 16$ dir.

Yrd. Teorem 4. 3 p bir asal olmak üzere, R karakteristiği p^s olan bir Galois halkası olsun ve $1 \in R$ halkanın birimi olsun. O halde, R nin sıfırı ve sıfır bölenleri $(p1)$ idealini oluşturur; $\{r1 : r \in \mathbb{Z}_{p^s}\}$, R nin bir alt halkasıdır ve $\mathbb{Z}_{p^s}$ halkasına izomorftur.

İspat: Galois halkasının tanımından, R nin sıfırı ve sıfır bölenleri bir q asalı için $(q1)$ idealini oluşturur. Yrd. Teorem 4. 2 den, R nin karakteristiğinin q nun bir kuvveti olduğunu biliyoruz. Buradan, $q = p$ dir.

$$\mathbb{Z}_{p^s} \rightarrow R$$

$$r \mapsto r1$$

homomorfizması, $\mathbb{Z}_{p^s}$ halkasından R nin içine bir izomorfizmadır ve görüntüsü

$$\{r1 : r \in \mathbb{Z}_{p^s}\} \text{ dir.}$$

R , karakteristiği p^s olan bir Galois halkası olsun. Her $r \in \mathbb{Z}_{p^s}$ için, r elemanını $r1 \in R$ olarak alırsak $\mathbb{Z}_{p^s}$ halkasını, R nin bir alt halkası olarak düşünebiliriz. Özel

olarak, $p1$ yerine $p \in \mathbb{Z}_{p^s}$ alırsak, $(p1)$ ideali yerine (p) yazabiliriz.

Yrd. Teorem 4. 4 p bir asal sayı olmak üzere, R karakteristiği p^s olan bir Galois halkası olsun ve R nin sıfırı ve sıfır bölenlerinin oluşturduğu ideal (p) olsun. O halde, bir $m \in \mathbb{Z}^+$ için $R/(p) \cong \mathbb{F}_{p^m}$ dir; $0 \leq i \leq s$ için (p^i) idealinin kardinalitesi $p^{(s-i)m}$ dir; ve özel olarak $|R| = p^{sm}$ dir.

İspat: (p) , R nin tek maksimal ideali olduğu için bir $m \in \mathbb{Z}^+$ için $R/(p) \cong \mathbb{F}_{p^m}$ dir. R yi toplamsal grup olarak düşünürsek, (p^i) idealleri R nin alt grupları olur ve aşağıdaki grup homomorfizmasını tanımlayabiliriz:

$$\begin{aligned}\phi: R &\rightarrow (p^i)/(p^{i+1}) \\ r &\mapsto p^i r + (p^{i+1})\end{aligned}$$

ϕ örten grup homomorfizmasıdır ve $\text{çek}\phi$, (p) idealini kapsar. Ancak $\text{çek}\phi$, R nin bir ideali ve $1 \notin \text{çek}\phi$ olduğundan $(p) \subseteq \text{çek}\phi \subseteq R$ dir. (p) , R nin maksimal ideali olduğundan $(p) = \text{çek}\phi$ dir. Gruplar için temel homomorfizma teoreminden,

$$R/(p) \cong (p^i)/(p^{i+1}), \text{ ve}$$

$$|R/(p)| = |(p)/(p^2)| = \dots = |(p^{s-2})/(p^{s-1})| = |(p^{s-1})|$$

yazabiliriz. Ancak $R/(p) \cong \mathbb{F}_{p^m}$ olduğundan $|R/(p)| = p^m$ dir. Buradan,

$$|(p^i)| = |(p^i)/(p^{i+1})| |(p^{i+1})/(p^{i+2})| \dots = |(p^{s-1})| = |(p^{(s-i)m})|$$

olur. Özel olarak, $|R| = |(1)| = |(p^0)| = p^{sm}$ dir.

Örnek 4. 6 $\mathbb{Z}_{16}$ halkasının bir Galois halkası ve $\mathbb{Z}_{16}/(2) \cong \mathbb{F}_2$ olduğunu daha önceki örnekten biliyoruz. $|\mathbb{Z}_{16}| = 2^{4.1} = 16$ dir. Y. Teorem 4. 4 e göre, $0 \leq i \leq 4$ için

$$|(2^i)| = |(2^0)| = |\mathbb{Z}_{16}| = 2^{4-0} = 16,$$

$$|(2^i)| = |(2)| = 2^{4-1} = 8,$$

$$\left| (2^i) \right| = \left| (2^2) \right| = \left| (4) \right| = 2^{4-2} = 4,$$

$$\left| (2^i) \right| = \left| (2^3) \right| = \left| (8) \right| = 2^{4-3} = 2, \text{ ve}$$

$$\left| (2^i) \right| = \left| (2^4) \right| = \left| (0) \right| = 1$$

R karakteristiği p^s olan bir Galois halkası olsun.

$$- : R \rightarrow R/(p)$$

$$r \mapsto \bar{r}$$

doğal homomorfizmasını aşağıdaki halka homomorfizmasına genişletebiliriz:

$$- : R[x] \rightarrow R/(p)[x]$$

$$f = a_0 + a_1x + \dots + a_nx^n \mapsto \bar{f} = \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n \quad (a_0, a_1, \dots, a_n \in R)$$

Örneğin,

$$- : \mathbb{Z}_{16} \rightarrow \mathbb{Z}_{16}/(2)$$

$$r \mapsto \bar{r} = r + (2)$$

doğal homomorfizmasını şu şekilde genişletebiliriz:

$$- : \mathbb{Z}_{16}[x] \rightarrow \mathbb{Z}_{16}/(2)[x]$$

$$f = a_0 + a_1x + \dots + a_nx^n \mapsto \bar{f} = \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n, (a_0, a_1, \dots, a_n \in \mathbb{Z}_{16})$$

$f(x) = 12x^3 + 9x^2 + 15x + 8 \in \mathbb{Z}_{16}[x]$ polinomunun “-” doğal homomorfizması altındaki görüntüsü $\bar{f}(x) = \bar{12}x^3 + \bar{9}x^2 + \bar{8} = x^2 \in \mathbb{Z}_{16}/(2)[x]$ olur.

Yrd. Teorem 4. 5 p bir asal sayı, s ve m pozitif tamsayılar olmak üzere R , karakteristiği p^s ve kardinalitesi p^{sm} olan bir Galois halkası olsun. $f(x) \in \mathbb{Z}_{p^s}[x]$ olsun. $\bar{f}(x)$ polinomunun $R/(p) \cong \mathbb{F}_{p^m}$ cismindeki kökünün $\bar{\beta}$ ve $\bar{f}'(\bar{\beta}) \neq 0$ olduğunu kabul edelim. O halde, $\bar{\alpha} = \bar{\beta}$ olacak şekilde $f(x)$ polinomunun R de tek bir α kökü vardır.

İspat: $-: R \rightarrow R/(p)$ homomorfizması altında β elemanının görüntüsü $\bar{\beta}$ olsun. $i = 0, 1, \dots, s-1$ için $\bar{\alpha}_i = \bar{\beta}$ ve $f(\alpha_i) \in (p^{i+1})$ olacak şekilde $\alpha_0, \alpha_1, \dots, \alpha_{s-1} \in R$ elemanlarından oluşan bir dizi inşa edelim. İlk olarak, $\alpha_0 = \beta$ olsun. Buradan, $\bar{\alpha}_0 = \bar{\beta}$ olur. $\bar{f}(\bar{\beta}) = 0$ olduğundan $f(\alpha_0) = f(\beta) \in (p)$ dir. α_i elemanının zaten varolduğunu ve, $\bar{\alpha}_i = \bar{\beta}$ ve $f(\alpha_i) \in (p^{i+1})$ koşullarını sağladığını kabul edelim. $\bar{f}'(\bar{\alpha}_i) = \bar{f}'(\bar{\beta}) \neq 0$ olduğundan $f'(\alpha_i) \notin (p)$ dir. Bu yüzden, $f'(\alpha_i)$ elemanı R halkasının birimselidir. $\alpha_{i+1} = \alpha_i - f'(\alpha_i)^{-1} f(\alpha_i) \in R$ olsun. $f'(\alpha_i)^{-1} f(\alpha_i) \in (p^{i+1}) \subset (p)$ olduğundan $\bar{\alpha}_{i+1} = \bar{\alpha}_i = \bar{\beta}$ dir. Taylor formülünü kullanarak,

$$f(\alpha_{i+1}) = f(\alpha_i) + \frac{f'(\alpha_i)}{1!} (-f'(\alpha_i)^{-1} f(\alpha_i)) + \frac{f''(\alpha_i)}{2!} (-f'(\alpha_i)^{-1} f(\alpha_i))^2 + \dots$$

eşitliğini yazabiliriz. Buradan, $f(\alpha_{i+1}) \in (p^{i+2})$ olur. Tümevarımla, $\bar{\alpha}_{s-1} = \bar{\beta}$ ve $f(\alpha_{s-1}) \in (p^s) = (0)$, yani $f(\alpha_{s-1}) = 0$ koşullarını sağlayan $\alpha_{s-1} \in R$ elemanını elde etmiş olduk. $\alpha = \alpha_{s-1}$ alırsak, $f(\alpha) = 0$ ve $\bar{\alpha} = \bar{\beta}$ olur.

Şimdi, α nın tekliğini gösterelim. $\bar{\alpha}' = \bar{\beta}$ olacak şekilde $f(x)$ polinomunun herhangi bir kökü α' olsun. O halde, $\bar{\alpha}' = \bar{\alpha}$ dir. Eğer $\alpha' \neq \alpha$ ise $\alpha' = \alpha + p^i r$ ve $p^i r \notin (p^{i+1})$ olacak şekilde $1 \leq i \leq s-1$ aralığında bir i tamsayısı ve bir $r \in R$ elemanı vardır. Taylor formülünü kullanarak,

$$f(\alpha') = f(\alpha) + \frac{f'(\alpha)}{1!} (p^i r) + \frac{f''(\alpha)}{2!} (p^i r)^2 + \dots$$

eşitliğini yazabiliriz. $f(\alpha') = f(\alpha) = 0$ olduğundan $f'(\alpha) p^i r \in (p^{2i}) \subseteq (p^{i+1})$ elde ederiz. Ancak $\bar{f}'(\bar{\alpha}) = \bar{f}'(\bar{\beta}) \neq 0$ olduğundan $f'(\alpha) \notin (p)$ dir, yani $f'(\alpha)$ elemanı R nin birimselidir. Buradan, $p^i r \in (p^{i+1})$ olur. Ancak i tamsayısını ve $r \in R$ elemanını $p^i r \notin (p^{i+1})$ olacak şekilde seçmiştik. O halde, $\bar{\alpha} = \bar{\beta}$ olacak şekilde $f(x)$ polinomunun R de tek bir α kökü vardır.

Örnek 4. 7 $R = \mathbb{Z}_{3^2} = GR(3^2, 3^2)$ ve $f(x) = x^3 + 5x + 3 \in \mathbb{Z}_{3^2}[x]$ alalım. Bu durumda, $\mathbb{Z}_{3^2}/(3) \cong \mathbb{F}_3$ ve $\bar{f}(x) = x^3 + 2x \in \mathbb{F}_3[x]$ olur. $\bar{f}'(\bar{\beta}) \neq 0$ olacak şekilde $\bar{f}(x)$ polinomunun $\mathbb{F}_3$ cismindeki kökleri 0, 1, 2 dir. $\bar{\beta} = 0$ seçelim. $f(x) = x^3 + 5x + 3$ ün $\mathbb{Z}_{3^2}$ halkasındaki kökleri 1, 3, 5 tir. $\bar{1} = 1, \bar{3} = 0, \bar{5} = 2$ olduğundan sadece $\bar{3} = \bar{\beta}$ dir.

Teorem 4. 6 p bir asal sayı ve s, m pozitif tamsayılar olmak üzere R , karakteristiği p^s ve kardinalitesi p^{sm} olan bir Galois halkası olsun. O halde, her m . dereceden monik temel indirgenemez $h(x)$ polinomu için

$$R \cong \mathbb{Z}_{p^s}[x]/(h(x))$$

izomorfizması vardır.

İspat: $h(x) \in \mathbb{Z}_{p^s}[x]$, m . dereceden monik temel indirgenemez bir polinom olsun. O halde, $\mathbb{F}_p[x]$ halkasında $\bar{h}(x)$ monik indirgenemezdir; $\text{der}(\bar{h}(x)) = m$, ve $\bar{h}(x)$ polinomunun $\mathbb{F}_{p^m}$ halkasında bir kökü vardır. Yrd. Teorem 4. 4 ten, $R/(p) \cong \mathbb{F}_{p^m}$ olduğundan $\bar{h}(x)$ polinomunun $R/(p)$ cisminde bir kökü vardır. Bu kök $\bar{\beta}$ olsun. $\bar{h}(\bar{\beta}) = 0$ dir. $\bar{h}(x)$ indirgenemez olduğundan $\bar{h}(x)$ polinomunun katlı kökü yoktur. Bu yüzden, $\bar{h}'(\bar{\beta}) \neq 0$ dir. Yrd. Teorem 4. 5 ten, $h(x)$ polinomunun $\bar{\alpha} = \bar{\beta}$ olacak şekilde R de tek bir α kökü vardır.

$$\phi: \mathbb{Z}_{p^s}[x]/(h(x)) \rightarrow R$$

$$a_0 + a_1x + \dots + a_{m-1}x^{m-1} + (h(x)) \mapsto a_0 + a_1\alpha + \dots + a_{m-1}\alpha^{m-1}, \left(a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}_{p^s} \right)$$

ϕ iyi tanımlı bir halka homomorfizmasıdır. ϕ nin birebir olduğunu gösterelim. Bunun için $\ker \phi = \{0\}$ olduğunu göstermemiz yeterlidir. $a_0 + \dots + a_{m-1}\alpha^{m-1} = 0$ olsun. Buradan, $\bar{a}_0 + \dots + \bar{a}_{m-1}\bar{\alpha}^{m-1} = 0$ dir. $\bar{\alpha} = \bar{\beta}$ olduğundan $\bar{a}_0 + \dots + \bar{a}_{m-1}\bar{\beta}^{m-1} = 0$ dir ve böylece, $\bar{\beta}$ $m-1$. dereceden polinomun kökü olur. Ama $\bar{\beta}$, m . dereceden indirgenemez $\bar{h}(x)$ polinomunun köküydü. Bu yüzden, $\bar{a}_0 = \bar{a}_1 = \dots = \bar{a}_{m-1} = 0$ olmalıdır. $i = 0, 1, \dots, m-1$ için $b_i^{(1)} \in R$ olmak üzere $a_i = pb_i^{(1)}$ yazabiliriz. $p(b_0^{(1)} + b_1^{(1)}\alpha + \dots + b_{m-1}^{(1)}\alpha^{m-1}) = 0$ dir.

Buradan, $b_0^{(1)} + b_1^{(1)}\alpha + \dots + b_{m-1}^{(1)}\alpha^{m-1}$ elemanı ya sıfırdır yada sıfır bölendir. Yani, $b_0^{(1)} + b_1^{(1)}\alpha + \dots + b_{m-1}^{(1)}\alpha^{m-1} \in (p)$ dir ve dolayısıyla $\overline{b_0^{(1)}} + \overline{b_1^{(1)}}\overline{\alpha} + \dots + \overline{b_{m-1}^{(1)}}\overline{\alpha}^{m-1} = 0$ dır. Benzer şekilde, $\overline{\alpha}$, $m-1$. dereceden bir polinomun kökü olur ama $\overline{\alpha}$, m . dereceden indirgenemez $\overline{h(x)}$ polinomunun kökü olduğundan $\overline{b_0^{(1)}} = \overline{b_1^{(1)}} = \dots = \overline{b_{m-1}^{(1)}} = 0$ olmalıdır. $i = 0, 1, \dots, m-1$ için $b_i^{(2)} \in R$ olmak üzere $b_i^{(1)} = pb_i^{(2)}$ yazabiliriz. Bu şekilde ilerleyerek, $j = 0, 1, \dots, m-1$ için $b_i^{(j)}, b_i^{(j+1)} \in R$ olmak üzere $b_i^{(j)} = pb_i^{(j+1)}$ elde ederiz. Buradan, $i = 0, 1, \dots, m-1$ için

$$a_i = pb_i^{(1)} = p^2b_i^{(2)} = \dots = p^sb_i^{(s)} = 0$$

olur. $a_0 = a_1 = \dots = a_{m-1} = 0$ ve böylece $\phi = \{0\}$ olur.

Teorem 4. 1 den $|\mathbb{Z}_{p^s}[x]/(h(x))| = p^{sm}$ ve teoremimizin hipotezinden $|R| = p^{sm}$ olduğundan ϕ örtendir. Sonuç olarak, $R \cong \mathbb{Z}_{p^s}[x]/(h(x))$ elde ederiz.

Sonuç 4. 7 Karakteristikleri ve kardinaliteleri aynı olan Galois halkaları birbirine izomorftur. Bu yüzden, karakteristiği p^s ve kardinalitesi p^{sm} olan bütün Galois halkalarını $GR(p^s, p^{sm})$ ile gösterebiliriz.

4. 3 p -adik Gösterim

Teorem 4. 8 (i) $h(x) \in \mathbb{Z}_{p^s}[x]$, m . dereceden monik temel indirgenemez ve $\mathbb{Z}_{p^s}[x]$ halkasında $x^{p^m-1} - 1$ i bölen bir polinom olsun. O halde,

(i) $GR(p^s, p^{sm})$ Galois halkasında, $h(x)$ polinomunun mertebesi $p^m - 1$ olan bir ξ kökü vardır, ve

$$GR(p^s, p^{sm}) = \mathbb{Z}_{p^s}[\xi] = \{a_0 + a_1\xi + \dots + a_{m-1}\xi^{m-1} : a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}_{p^s}\}$$

dir. Ayrıca, $h(x)$ derecesi m veya m den küçük olan ve ξ yi kök kabul eden $\mathbb{Z}_{p^s}[x]$ halkasındaki tek polinomdur.

(ii) $\tau = \{0, 1, \xi, \xi^2, \dots, \xi^{p^m-2}\}$ olsun. $a_0, a_1, \dots, a_{s-1} \in \tau$ olmak üzere her $c \in GR(p^s, p^{sm})$

$$c = a_0 + a_1 p + \dots + a_{s-1} p^{s-1}$$

şeklinde tek türlü yazılabilir. Ayrıca, c nin birimsel olması için gerek ve yeter koşul $a_0 \neq 0$ olmasıdır. c nin sıfır veya sıfır bölen olması için, yani $c \in (p)$ olması için gerek ve yeter koşul $a_0 = 0$ olmasıdır.

İspat: (i) Teorem 4. 10 dan m . dereceden monik temel indirgenemez ve $\mathbb{Z}_{p^s}[x]$ halkasında $x^{p^m-1} - 1$ i bölen bir $h(x) \in \mathbb{Z}_{p^s}[x]$ polinomu vardır. Buradan, $\bar{h}(x)$ de $\mathbb{F}_p$ sonlu cisminde m . dereceden monik ilkel bir polinomdur. $\xi_p \in \mathbb{F}_{p^m}$, $h(x)$ polinomunun bir kökü olsun. Bu yüzden, ξ_p , $\mathbb{F}_{p^m}$ cisminin ilkel elemanıdır. Yrd. Teorem 4. 5 ten, $h(x)$ polinomunun $\bar{\xi} = \xi_p$ olacak şekilde tek bir $\xi \in GR(p^s, p^{sm})$ kökü vardır. $h(x)$, $x^{p^m-1} - 1$ polinomunu böldüğünden $\xi^{p^m-1} - 1 = 0$ dir. ξ_p , $\mathbb{F}_{p^m}$ cisminin ilkel elemanı olduğundan mertebesi $p^m - 1$ dir. $\bar{\xi} = \xi_p$ ve $\xi^{p^m-1} = 1$ olduğundan ξ nin mertebesi de $p^m - 1$ dir.

Teorem 4. 6 nın ispatında,

$$\phi: \mathbb{Z}_{p^s}[x]/(h(x)) \rightarrow GR(p^s, p^{sm})$$

$$a_0 + a_1 x + \dots + a_{m-1} x^{m-1} + (h(x)) \mapsto a_0 + a_1 \xi + \dots + a_{m-1} \xi^{m-1}, \quad (a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}_{p^s})$$

homomorfizmasının izomorfizma olduğunu göstermiştik. Buradan,

$$GR(p^s, p^{sm}) = \mathbb{Z}_{p^s}[\xi] = \{a_0 + a_1 \xi + \dots + a_{m-1} \xi^{m-1} : a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}_{p^s}\}$$

yazabiliriz. Şimdi $h(x)$ polinomunun tekliliğini gösterelim:

$f(x) \in \mathbb{Z}_{p^s}[x]$, derecesi m veya m den küçük olan olan ve ξ yi kök kabul eden monik bir polinom olsun. $\deg(f(x)) < m$ ise $\phi(f(x) + (h(x))) = f(\xi) = 0$ olur. Bu yüzden, $f(x) + (h(x)) \in \ker \phi = \{0\}$, yani $f(x) + (h(x)) = 0$ dir. Buradan, $f(x) \in (h(x))$ olur. Bu ise $\deg(f(x)) < m$ olmasıyla çelişir. Eğer $\deg(f(x)) = m$ ise $\deg(f(x) - h(x)) < m$ olur. $\phi((f(x) - h(x)) + (h(x))) = f(\xi) - h(\xi) = 0$ olduğundan $f(x) - h(x) \in \ker \phi = \{0\}$ dir. Bu yüzden, $f(x) = h(x)$ olur.

(ii) $i = 0, 1, \dots, p^m - 2$ için $\xi^i \xi^{p^m-1-i} = 1$ dir. Bu yüzden, her $0 \leq i \leq p^m - 2$ için ξ^i elemanları $GR(p^s, p^{sm})$ halkasında birimseldir. Ayrıca, her $0 < j < p^m - 2$ için $1 - \xi^j$ elemanları da $GR(p^s, p^{sm})$ Galois halkasında birimseldir. Eğer $1 - \xi^j \in (p)$ olsaydı $\overline{1 - \xi^j} = 1 - \overline{\xi^j} = 0$, yani $\overline{\xi^j} = 1$ olurdu. Bu ise $\overline{\xi}$ elemanının mertebesinin $p^m - 1$ olmasıyla çelişir. O halde, $0 < j < p^m - 2$ için $1 - \xi^j$ elemanları sıfır veya sıfır bölen olamaz. Sonuç olarak, her $0 \leq i < j \leq p^m - 2$ için $\xi^i - \xi^j = \xi^i (1 - \xi^{j-i})$ olduğundan $\xi^i - \xi^j$ elemaları $GR(p^s, p^{sm})$ halkasında birimseldir.

$|GR(p^s, p^{sm})| = p^{sm}$ olduğunu biliyoruz. Eğer $c = a_0 + a_1 p + \dots + a_{s-1} p^{s-1}$ şeklinde yazdığımız p^{sm} tane elemanın birbirinden farklı olduğunu gösterirsek (ii) nin ilk ifadesini ispatlamış oluruz. $a_0, a_1, \dots, a_{s-1}, a'_0, a'_1, \dots, a'_{s-1} \in \tau$ olmak üzere

$$a_0 + a_1 p + \dots + a_{s-1} p^{s-1} = a'_0 + a'_1 p + \dots + a'_{s-1} p^{s-1}$$

olduğunu kabul edelim. Bu eşitliği p^{s-1} ile çarparsak, $a_0 p^{s-1} = a'_0 p^{s-1}$ elde ederiz. $a_0 = 0$ olması için gerek ve yeter koşul $a'_0 = 0$ olmasıdır. $a_0 \neq 0$ ve $a'_0 \neq 0$ olduğunu kabul edelim. $(a_0 - a'_0) p^{s-1} = 0$ olur. Eğer $a_0 - a'_0 \neq 0$ ise $a_0 - a'_0$, $GR(p^s, p^{sm})$ halkasının birimsel elemanıdır. Çünkü $a_0, a'_0 \in \tau$, yani ξ nin kuvvetleridir ve (i) de $\xi^i - \xi^j$ elemanının birimsel olduğunu göstermiştik. O halde, $(a_0 - a'_0) p^{s-1} = 0$ eşitliğini, $a_0 - a'_0$ elemanının tersi ile çarparsak $p^{s-1} = 0$ elde ederiz ki bu mümkün değildir. Bu yüzden, $a_0 = a'_0$ dir. Buradan,

$$a_1 p + \dots + a_{s-1} p^{s-1} = a'_1 p + \dots + a'_{s-1} p^{s-1}$$

elde ederiz. Bu eşitliği p^{s-2} ile çarparsak, $a_1 p^{s-1} = a'_1 p^{s-1}$ olur. Yukarıda yaptığımız şekilde devam edersek $a_1 = a'_1$ olur, ve

$$a_2 p^2 + \dots + a_{s-1} p^{s-1} = a'_2 p^2 + \dots + a'_{s-1} p^{s-1}$$

elde ederiz. Benzer şekilde ilerlersek en sonunda $a_2 = a'_2, \dots, a_{s-1} = a'_{s-1}$ elde ederiz.

Son olarak, $c = a_0 + a_1p + \dots + a_{s-1}p^{s-1} \in GR(p^s, p^{sm})$ elemanının (p) idealinde olması için gerek ve yeter koşulun $a_0 = 0$ olduğunu gösterelim. $c \in (p)$ olsun. Buradan, $a_0 \in (p)$ olur. Yani, a_0 elemanı ya sıfırdır yada sıfır bölendir. Ancak $a_0 \in \tau = \{0, 1, \xi, \xi^2, \dots, \xi^{p^m-2}\}$ ve $0 \leq i \leq p^m-2$ için ξ^i elemanlarının birimsel olduklarını biliyoruz. Bu yüzden $a_0 = 0$ olmalıdır. Tersî açıktır. Sonuç olarak, $c \in GR(p^s, p^{sm})$ elemanının birimsel olması için gerek ve yeter koşul $a_0 \neq 0$ olmasıdır.

Tanım 4. 3 $\tau = \{0, 1, \xi, \xi^2, \dots, \xi^{p^m-2}\}$ ve $a_0, a_1, \dots, a_{s-1} \in \tau$ olsun. $GR(p^s, p^{sm})$ Galois halkasının bir c elemanının

$$c = a_0 + a_1p + \dots + a_{s-1}p^{s-1}$$

şeklindeki yazılımına c nin p -adik gösterimi denir.

Örnek 4. 8 $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$, 2. dereceden monik temel indirgenemez bir polinomdur ve $x^{2^2-1} - 1 = x^3 - 1$ i böler. O halde, Teorem 4. 8 e göre $GR(2^2, 2^4)$ Galois halkasında $h(x)$ polinomunun mertebesi $2^2 - 1 = 3$ olan bir ξ kökü vardır. Bu yüzden, $\xi^2 + \xi = 3$ ve $\xi^3 = 1$ dir. ξ nin mertbesinin 3 olduğunu şu şekilde de söyleyebiliriz:

$$\xi^2 = 3\xi + 3$$

$$\xi^3 = 3\xi^2 + 3\xi$$

$$\xi^3 = 3\xi^2 + 3\xi = 3(3\xi + 3) + 3\xi = 12\xi + 9$$

$$\xi^3 = 1$$

$$\phi: \mathbb{Z}_4[x] / (x^2 + x + 1) \rightarrow GR(2^2, 2^4)$$

$$a_0 + a_1x + (x^2 + x + 1) \mapsto a_0 + a_1\xi$$

izomorfizmasından dolayı

$$GR(2^2, 2^4) = \left\{ \begin{array}{l} 0, 1, 2, 3, \xi, \xi + 1, \xi + 2, \xi + 3, \\ 2\xi, 2\xi + 1, 2\xi + 2, 2\xi + 3, \\ 3\xi, 3\xi + 1, 3\xi + 2, 3\xi + 3 \end{array} \right\} = \mathbb{Z}_4[\xi]$$

elde ederiz. $\xi^2 + \xi = 3$ ve $\xi^3 = 1$ eşitliklerini kullanarak da aynı elemanları yazabiliriz.

$\tau = \{0, 1, \xi, \xi^2\}$ olsun. $a_0, a_1 \in \tau$ olmak üzere her $c \in GR(2^2, 2^4)$ elemanını $c = a_0 + a_1 2$ şeklinde yazabiliriz.

$$GR(2^2, 2^4) = \left\{ \begin{array}{l} 0, 1, \xi, \xi^2, 2, \xi 2, \xi^2 2, \\ 1+2, 1+\xi 2, 1+\xi^2 2, \\ \xi+2, \xi+\xi 2, \xi+\xi^2 2 \\ \xi^2+2, \xi^2+\xi 2, \xi^2+\xi^2 2 \end{array} \right\}$$

Örneğin, $3\xi + 2 \in GR(2^2, 2^4)$ elemanını şu şekilde p -adik gösterimle ifade edebiliriz:

$$\begin{aligned} 3\xi + 2 &= 1 + \xi^2 + 2 \\ &= \xi^2 + 3 = \xi^2 + \xi^2 + \xi \\ &= \xi + \xi^2 2 \end{aligned}$$

Teorem 4. 8 e göre $GR(2^2, 2^4) = \mathbb{Z}_4[\xi]$ halkasının birimsel elemanları $a_0 \neq 0$ olmak üzere $c = a_0 + a_1 2$ şeklindeki elemanlardır. O halde, $GR(2^2, 2^4) = \mathbb{Z}_4[\xi]$ halkasının

$$1, \xi, \xi^2, 1+2, 1+\xi 2, 1+\xi^2 2, \xi+2, \xi+\xi 2, \xi+\xi^2 2, \xi^2+2, \xi^2+\xi 2, \xi^2+\xi^2 2$$

elemanları birimseldir. $GR(2^2, 2^4) = \mathbb{Z}_4[\xi]$ halkasının sıfır bölenleri $2, \xi 2, \xi^2 2$ elemanlarıdır ve $GR(2^2, 2^4)$ Galois halkasında $(2) = \{0, 2, \xi 2, \xi^2 2\}$ dir.

Sonuç 4. 9 $a_0, a_1, \dots, a_{s-1} \in \tau$ olmak üzere her $c \in GR(p^s, p^{sm})$ elemanı

$$c = a_0 + a_1 p + \dots + a_{s-1} p^{s-1}$$

şeklinde ifade edilsin. O halde,

(i) $a_0 \neq 0$ olan bütün $c \in GR(p^s, p^{sm})$ elemanları birimseldir ve bu elemanlar mertebesi $(p^m - 1)p^{(s-1)m}$ olan $\langle \xi \rangle \times \varepsilon$ çarpımsal grubunu oluşturur. Burada, $\langle \xi \rangle$, ξ ile üretilen mertebesi $p^m - 1$ olan devirli grup ve $\varepsilon = \{1 + \pi : \pi \in (p)\}$, mertebesi $p^{(s-1)m}$ olan bir grup olmak üzere $\langle \xi \rangle \times \varepsilon$ çarpımsal grubu direk çarpımdır.

(ii) $0 \leq i \leq p^m - 2$ olmak üzere ξ^i elemanının mertebesi $p^m - 1$ in bir bölenidir, ve $\pi \in (p)$ olmak üzere $1 + \pi$ elemanının mertebesi p^{s-1} in bir bölenidir. Mertebesi $p^m - 1$ in bir böleni olan $GR(p^s, p^{sm})$ halkasının bir elemanı, $0 \leq i \leq p^m - 2$ olmak üzere ξ^i şeklindedir. Özel olarak, mertebesi $p^m - 1$ olan bir eleman, $0 \leq i \leq p^m - 2$ ve $ebob(i, p^{m-1}) = 1$ olmak üzere ξ^i şeklindedir, ve $\mathbb{Z}_{p^s}[x]$ halkasında $x^{p^m-1} - 1$ i bölen m . dereceden temel indirgenemez bir polinomun köküdür.

(iii) $a_0 = 0$ olan bütün $c \in GR(p^s, p^{sm})$ elemanları ya sıfır yada sıfır bölendir. Bu elemanlar $GR(p^s, p^{sm})$ halkasının (p) idealini oluştururlar.

Örnek 4. 9 Bir önceki örnekte

$$\mathbb{Z}_4[\xi] = GR(2^2, 2^4) = \left\{ \begin{array}{l} 0, 1, \xi, \xi^2, 2, \xi 2, \xi^2 2, \\ 1 + 2, 1 + \xi 2, 1 + \xi^2 2, \\ \xi + 2, \xi + \xi 2, \xi + \xi^2 2 \\ \xi^2 + 2, \xi^2 + \xi 2, \xi^2 + \xi^2 2 \end{array} \right\}$$

Galois halkasını ele almıştık. $\mathbb{Z}_4[\xi] = GR(2^2, 2^4)$ halkasının birimselleri, $a_0 \neq 0$ olmak üzere $c = a_0 + a_1 2$ şeklinde olduğunu söylemiş ve

$$1, \xi, \xi^2, 1 + 2, 1 + \xi 2, 1 + \xi^2 2, \xi + 2, \xi + \xi 2, \xi + \xi^2 2, \xi^2 + 2, \xi^2 + \xi 2, \xi^2 + \xi^2 2$$

birimsel elemanlarını bulmuştuk. $\xi^3 = 1$ olduğundan, ξ ile üretilen devirli grup

$$\langle \xi \rangle = \{1, \xi, \xi^2\}$$

ve mertebesi $2^2 - 1 = 3$ tür. $(2) = \{0, 2, \xi 2, \xi^2 2\}$ ise

$$\mathcal{E} = \{1 + \pi : \pi \in (2)\} = \{1, 3, 1 + \xi 2, 1 + \xi^2 2\}$$

mertebesi $2^2 = 4$ olan bir gruptur. O halde, $\langle \xi \rangle \times \mathcal{E}$ direk çarpımı,

$$\langle \xi \rangle \times \mathcal{E} = \{1, \xi, \xi^2, 1 + 2, 1 + \xi 2, 1 + \xi^2 2, \xi + \xi 2, \xi + \xi^2 2, \xi + 2, \xi^2 + 2, \xi^2 + \xi 2, \xi^2 + \xi^2 2\}$$

mertebesi $3 \cdot 4 = 12$ olan bir gruptur ve $\mathbb{Z}_4[\xi] = GR(2^2, 2^4)$ halkasının birimsel elemanlarından oluşur.

4. 4 Galois Halkalarının Birim Grubu

$R = GR(p^s, p^{sm})$ olsun ve R nin birimsellerinin grubunu R^* ile gösterelim. G_1 , ξ ile üretilen mertebesi $p^m - 1$ olan bir devirli grup ve $G_2 = \{1 + \pi : \pi \in (p)\}$, mertebesi $p^{(s-1)m}$ olan bir grup olmak üzere $R^* = G_1 \times G_2$ olduğunu Sonuç 4. 9 (i) den biliyoruz. Bu bölümde G_2 grubunun yapısını belirleyeceğiz.

Yrd. Teorem 4. 10 X bir bilinmeyen, p bir asal ve tek tamsayı ve a_t, b_t, c_t sırasıyla $(1 + pX)^N$, $(1 + 2X)^N$, $(1 + 4X)^N$ ifadelerinin açılımlarındaki X^t teriminin katsayıları olsun. O halde, aşağıdaki ifadeler doğrudur.

- (i) $p^e | N$ ise $p^{e+1} | a_1$ ve $t \geq 2$ için $p^{e+2} | a_t$ dir.
- (ii) $p^{2e} | N$ ise $t = 1, 2$ için $2^{e+1} | b_t$ ve $t \geq 3$ için $2^{e+2} | b_t$ dir.
- (iii) $p^{2e} | N$ ise $2^{e+2} | c_1$ ve $t \geq 2$ için $2^{e+3} | c_t$ dir.
- (iv) $t \geq 1$ için $4 | c_t$ dir.

İspat: (i) $a_1 = Np$ dir. Teoremimizin hipotezinden, $p^e | N$ olduğundan $p^{e+1} | a_1$ dir. Şimdi $t \geq 2$ olsun. O halde,

$$a_t = \binom{N}{t} p^t = \frac{N}{t} \binom{N-1}{t-1} p^t$$

dir. $\binom{N}{t}$ ve $\binom{N-1}{t-1}$ ifadelerinin ikisi de tamsayıdır. $p^f | t$ olduğunu kabul edelim.

Hipotezimizden $p^e | N$ olduğundan

$$p^{e-f} \left| \binom{N}{t} \right|$$

dir. Buradan, $p^{e-f+t} | a_t$ olur. $f = 0$ ise $t \geq f + 2$ olduğu açıktır. Eğer $f > 0$ ise

$p^f \geq f + 2$ ve böylece, $t \geq p^f \geq f + 2$ olur. Her iki durumda da, $-f + t \geq 2$ dir ve bu yüzden, $p^{e+2} | p^{e-f+t}$ dir. Sonuç olarak, $p^{e+2} | a_t$ dir.

(ii) ve (iii) benzer şekilde ispatlanabilir.

(iv) aşıkardır.

Teorem 4. 11 $R = GR(p^s, p^{sm})$ olsun. R nin birimsel elemanlarının grubunu R^* ile gösterelim. O halde, $R^* = G_1 \times G_2$ direk çarpımındaki G_1 , mertebesi $p^m - 1$ olan devirli bir grup ve G_2 , mertebesi $p^{(s-1)m}$ olan ve aşağıdaki özellikleri sağlayan bir gruptur:

- (i) p tek ise G_2 , mertebesi p^{s-1} olan m tane devirli grubun direk çarpımıdır.
- (ii) $p = 2$ ve $s \leq 2$ ise G_2 , mertebesi p^{s-1} olan m tane devirli grubun direk çarpımıdır.
- (iii) $p = 2$ ve $s \geq 3$ ise G_2 , mertebesi 2 olan bir devirli grup ve mertebesi 2^{s-2} olan bir devirli grubun, mertebesi 2^{s-1} olan $m-1$ tane devirli grup ile direk çarpımıdır.

İspat: $s = 1$ olduğunda $R = GR(p, p^m) = \mathbb{F}_{p^m}$ dir. ξ , $\mathbb{F}_{p^m}$ cisminin ilkel elemanı olmak üzere $R^* = \langle \xi \rangle$ grubunun mertebesi $p^m - 1$ olan bir devirli grup olduğunu Teorem 2. 8 den biliyoruz. Bu durumda, $G_1 = R^*$ ve $G_2 = 1$ dir.

Şimdi $s \geq 2$ olduğu durumu düşünelim. $h(x) \in \mathbb{Z}_{p^s}[x]$, m . dereceden monik temel indirgenemez ve $\mathbb{Z}_{p^s}[x]$ halkasında $x^{p^{m-1}} - 1$ i bölen bir polinom; $\xi \in R$, mertebesi p^{m-1} olan $h(x)$ polinomunun bir kökü olmak üzere $R = \mathbb{Z}_{p^s}[\xi]$ olduğunu Teorem 4. 8 den biliyoruz. G_1 , mertebesi $p^m - 1$ olan ξ ile üretilen devirli grup ve $G_2 = \{1 + \pi : \pi \in (p)\}$, mertebesi $p^{(s-1)m}$ olan bir grup olmak üzere $R^* = G_1 \times G_2$ olduğunu Sonuç 4. 9 (i) den biliyoruz. Şimdi aşağıdaki farklı durumlar için G_2 grubunun yapısını belirleyelim.

1. Durum : p asalı tek tamsayı olsun. $G_2 = \{1 + \pi : \pi \in (p)\}$ olduğundan $1 + p\xi^i \in G_2$ dir. $i = 0, 1, \dots, m-1$ ve $t \geq 1$ için $(1 + p\xi^i)^{p^{s-1}}$ ifadesinin açılımındaki $(\xi^i)^t$ teriminin kat sayısı a^t olsun. Yrd. Teorem 4. 10 (i) ye göre, $p^{s-2} \mid p^{s-1}$ olduğundan $p^s \mid a^t$ dir. R nin karakteristiği p^s olduğundan, $t \geq 1$ için $a^t (\xi^i)^t = 0$ olur. Yani, $i = 0, 1, \dots, m-1$ için $(1 + p\xi^i)^{p^{s-1}} = 1$ dir. İddiamız: $n_0, n_1, \dots, n_{m-1} \leq p^{s-1}$ olacak şekilde pozitif tamsayılar ol-

mak üzere her $i = 0, 1, \dots, m-1$ için $\prod_{i=0}^{m-1} (1 + p\xi^i)^{n_i} = 1$ ise $n_i = p^{s-1}$ dir. Şimdi iddiamızı

ispatlayalım. $\prod_{i=0}^{m-1} (1 + p\xi^i)^{n_i} = 1$ ifadesini açarsak, bir $a \in R$ için

$$p \left(\sum_{i=0}^{m-1} n_i \xi^i + pa \right) = 0$$

elde ederiz. $\sum_{i=0}^{m-1} n_i \xi^i + pa$ sıfır bölen olduğundan $\sum_{i=0}^{m-1} n_i \xi^i + pa \in (p)$ olur. Buradan,

$$\sum_{i=0}^{m-1} \overline{n_i} \overline{\xi}^i = 0$$

olur. $\overline{\xi} \in \mathbb{F}_{p^m}$ sonlu cisminin ilkel elemanı olduğundan, $\overline{\xi}$ elemanının $\mathbb{F}_p[x]$ halkasındaki minimal polinomunun derecesi m dir ve $1, \overline{\xi}, \dots, \overline{\xi}^{m-1}$ elemanları, $\mathbb{F}_p$ üzerinde lineer bağımsızdır. Bu yüzden, $i = 0, 1, \dots, m-1$ için $\overline{n_i} = 0$ olur. Yani, $i = 0, 1, \dots, m-1$ için $p \mid n_i$ dir. $0 \leq e \leq s-2$ olmak üzere $n_0, n_1, \dots, n_{m-1}$ elemanlarının hepsini bölen p nin en büyük kuvveti p^{e+1} olsun. $e = s-2$ olduğunu göstermek istiyoruz. $i = 0, 1, \dots, m-1$ için $n_i = p^{e+1} r_i$ olsun. O halde, $r_0, r_1, \dots, r_{m-1}$ elemanlarından en az biri p ile bölünemez.

$\prod_{i=0}^{m-1} (1 + p\xi^i)^{n_i} = 1$ ifadesi açarak ve Yrd. Teorem 4. 10 (i) yi kullanarak, bir $c \in R$ için

$$p^{e+2} \left(\sum_{i=0}^{m-1} r_i \xi^i + pc \right) = 0$$

elde ederiz. Eğer $e+2 < s$ ise $\sum_{i=0}^{m-1} r_i \xi^i + pc \in (p)$ olur. Buradan,

$$\sum_{i=0}^{m-1} r_i \overline{\xi}^i = 0$$

olur. $1, \overline{\xi}, \dots, \overline{\xi}^{m-1}$ elemanları, $\mathbb{F}_p$ üzerinde lineer bağımsız olduğundan $i = 0, 1, \dots, m-1$ için $\overline{r_i} = 0$ olur. Yani, $i = 0, 1, \dots, m-1$ için $p \mid r_i$ dir. Ancak $r_0, r_1, \dots, r_{m-1}$ elemanlarından en az biri p ile bölünemez olduğundan çelişki oluşur. O halde, $e = s-2$ dir. İddiamızı ispatlamış olduk.

$i = 0, 1, \dots, m-1$ için $H_i = \langle 1 + p\xi^i \rangle$ olsun. Her $i = 0, 1, \dots, m-1$ için H_i grubunun mertebesi p^{s-1} dir. $H_0 \times H_1 \times \dots \times H_{m-1}$, H_i gruplarının direk çarpımıdır; mertebesi $p^{(s-1)m}$ dir ve $G_2 = H_0 \times H_1 \times \dots \times H_{m-1}$ elde ederiz.

2. Durum : $p = 2$ ve $s = 2$ olsun. Bu durumda, G_2 grubunun her elemanının karesi 1 dir. Bu yüzden, G_2 mertebesi 2 olan m tane devirli grubun direk çarpımıdır.

3. Durum : $p = 2$ ve $s \geq 3$ olsun. Yrd. Teorem 2. 14 ten $N = \left\{ \bar{a}^{-2} + \bar{a} : \bar{a} \in \mathbb{F}_{2^m} \right\}$, $\mathbb{F}_{2^m}$ cisminin indeksi 2 olan bir alt grubudur. Bu yüzden, bir $\bar{b} \in \mathbb{F}_{2^m} \setminus N$ elemanı bulabiliriz. “-” homomorfizması altında $\bar{b}$, $b \in R$ elemanının görüntüsü olsun. Teorem 4. 1 den R nin her elemanını $i = 0, 1, \dots, m-1$ için $a_i \in \mathbb{Z}_{p^s}$ olmak üzere $a_0 + a_1\xi + \dots + a_{m-1}\xi^{m-1}$ şeklinde tek türlü yazılabilir. $G_2 = \{1 + \pi : \pi \in (p)\}$ olduğundan $1 + 2 + 2^2 + \dots + 2^{s-2}$, $i = 0, 1, \dots, m-1$ için $1 + 2\xi^i$, ve $1 + 4b$ elemanlarının hepsi G_2 grubunun elemanıdır. Ayrıca,

$$(1 + 2 + 2^2 + \dots + 2^{s-2})^2 = \left(\sum_{i=0}^{s-2} 2^i \right)^2 = \left(\frac{1 - 2^{s-1}}{1 - 2} \right)^2 = (1 - 2^{s-1})^2 = 1$$

$$(1 + 2\xi^i)^{2^{s-1}} = \sum_{r=0}^{2^{s-1}-1} \binom{2^{s-1}}{r} (2\xi^i)^r = 1$$

$$(1 + 4b)^{2^{s-2}} = \sum_{r=0}^{2^{s-2}-1} \binom{2^{s-2}}{r} (4b)^r = 1$$

eşitlikleri sağlanır. İddiamız: $n_1, \dots, n_{m-1} \leq 2^{s-1}$, $n \leq 2^{s-2}$, $n_0 \leq 2$ ve $n_0, n_1, n_2, \dots, n_{m-1}, n$ pozitif tamsayılar olmak üzere her $i = 0, 1, \dots, m-1$ için

$$(1 + 2 + 2^2 + \dots + 2^{s-2})^{n_0} \prod_{i=1}^{m-1} (1 + 2\xi^i)^{n_i} (1 + 4b)^n = 1 \quad (4. 4)$$

ise $n_0 = 2$, $n_1 = n_2 = \dots = n_{m-1} = 2^{s-1}$ ve $n = 2^{s-2}$ dir. Şimdi iddiamızı ispatlayalım:

$n_0 = 1$ olduğunu kabul edelim. (4. 4) ifadesini açarak ve Yrd. Teorem 4. 10 (ii) yi kullanarak, bir $a \in R$ için

$$2 \left(1 + \sum_{i=1}^{m-1} n_i \xi^i + 2a \right) = 0$$

elde ederiz. Buradan, $1 + \sum_{i=1}^{m-1} n_i \xi^i + 2a \in (2)$ olur. O halde, $1 + \sum_{i=1}^{m-1} \bar{n}_i \bar{\xi}^i = 0$ dır. Ancak bu

$\mathbb{F}_{2^m}$ cisminin $1, \bar{\xi}, \dots, \bar{\xi}^{m-1}$ elemanlarının, $\mathbb{F}_p$ üzerinde lineer bağımsız olmasıyla çelişir.

Bu yüzden, $n_0 = 2$ olmalıdır. O halde, (4. 4) denklemi

$$\prod_{i=1}^{m-1} (1 + 2\xi^i)^{n_i} (1 + 4b)^n = 1 \quad (4. 5)$$

şeklini alır. (4. 5) ifadesini açarak ve Yrd. Teorem 4. 10 (ii) yi kullanarak, bir $a' \in R$

için $2 \left(\sum_{i=1}^{m-1} n_i \xi^i + 2a' \right) = 0$ buluruz. $\sum_{i=1}^{m-1} n_i \xi^i + 2a' \in (2)$ ve buradan, $i = 0, 1, \dots, m-1$ için

$n_i \in (2)$ olur. Yani, $i = 0, 1, \dots, m-1$ için her n_i çift tamsayıdır. $0 \leq e \leq s-2$ olmak üzere

$2n, n_1, n_2, \dots, n_{m-1}$ elemanlarının hepsini bölen 2 nin en büyük kuvveti 2^{e+1} olsun.

$e = s-2$ olduğunu göstermek istiyoruz. $i = 0, 1, \dots, m-1$ için $n = 2^e r$ ve $n_i = 2^{e+1} r_i$

olsun. O halde, $r, r_1, r_2, \dots, r_{m-1}$ elemanlarından en az biri tek tamsayıdır. (4. 5) ifadesini

açarak ve Yrd. Teorem 4. 10 (ii) yi kullanarak (e yerine $e+1$ alarak), bir $c \in R$ için

$$2^{e+2} \left(\sum_{i=0}^{m-1} \left(r_i \xi^i + r_i (r_i 2^{e+1} - 1) \xi^{2i} \right) + rb + 2c \right) = 0$$

elde ederiz. Eğer $e+2 < s$ ise $\sum_{i=0}^{m-1} \left(r_i \xi^i + r_i (r_i 2^{e+1} - 1) \xi^{2i} \right) + rb + 2c \in (p)$ olur. Buradan,

$$\sum_{i=0}^{m-1} \left(r_i \bar{\xi}^i + r_i \bar{\xi}^{2i} \right) + r\bar{b} = \bar{0}$$

elde ederiz. $r_i \bar{\xi}^i + r_i \bar{\xi}^{2i} \in N$ ve $\bar{b} \in \mathbb{F}_{2^m} \setminus N$ olduğundan r çift tamsayı olmak zorundadır.

$$\sum_{i=0}^{m-1} \left(r_i \bar{\xi}^i + r_i \bar{\xi}^{2i} \right) = \bar{0}$$

olur. $r, r_1, r_2, \dots, r_{m-1}$ elemanlarından en az birinin tek tamsayı olduğunu daha önce

söylemiştik. O halde, r çift tamsayı olduğuna göre $r_1, r_2, \dots, r_{m-1}$ elemanlarından en az biri

tek olmak zorundadır. Bu yüzden, $\sum_{i=0}^{m-1} r_i \bar{\xi}^i = \bar{0}$ veya $\sum_{i=0}^{m-1} r_i \bar{\xi}^i = \bar{1}$ olmak zorundadır. Ancak iki durumda da çelişki oluşur. O halde, $e = s - 2$ dir. İddiamızı ispatlamış olduk.

$$H_0 = \langle 1 + 2 + 2^2 + \dots + 2^{s-2} \rangle,$$

$$H_i = \langle 1 + 2\xi^i \rangle \quad i = 0, 1, \dots, m-1 \text{ ve}$$

$$H_r = \langle 1 + 4b \rangle$$

olsun. O halde, $H_0, i = 0, 1, \dots, m-1$ olmak üzere H_i ve H_r mertebeleri sırasıyla $2, 2^{n-1}$ ve 2^{n-2} olan devirli gruplardır. $H_0 \times H_1 \times \dots \times H_{m-1} \times H_r, G_2$ nin alt gruplarının bir direk çarpımıdır ve $|H_0 \times H_1 \times \dots \times H_{m-1} \times H_r| = |G_2|$ olduğundan $G_2 = H_0 \times H_1 \times \dots \times H_{m-1} \times H_r$ elde ederiz.

Örnek 4. 10 Örnek 3. 9 da $R = \mathbb{Z}_4[\xi] = GR(2^2, 2^4)$ Galois halkasının birimsel elemanlarını belirlemiştik. $G_1 = \langle \xi \rangle = \{1, \xi, \xi^2\}$ ve $G_2 = \{1 + \pi : \pi \in (2)\} = \{1, 3, 1 + \xi 2, 1 + \xi^2 2\}$ olmak üzere

$$R^* = G_1 \times G_2 = \{1, \xi, \xi^2, 1 + 2, 1 + \xi 2, 1 + \xi^2 2, \xi + \xi 2, \xi + \xi^2 2, \xi + 2, \xi^2, \xi^2 + \xi^2 2, \xi^2 + 2, \}$$

olduğunu biliyoruz. Şimdi G_2 grubunun yapısını belirleyelim. Teorem 4. 11 (ii) ye göre $p = 2$ ve $s = 2$ iken G_2 grubunun her elemanının karesi 1 olduğundan $G_2, m = 2$ tane mertebesi $2^{2-1} = 2$ olan devirli grupların direk çarpımı olacak şekilde mertebesi $2^{(2-1)^2} = 4$ olan bir gruptur. $G_2 = H_1 \times H_2$ olacak şekilde H_1, H_2 devirli gruplarını bulalım.

$$\mathbb{Z}_4[\xi] \text{ halkasında } 3^2 = 9 = 1 \text{ olduğundan } H_1 = \langle 3 \rangle = \{1, 3\} \text{ ve}$$

$$\mathbb{Z}_4[\xi] \text{ de } (1 + \xi 2)^2 = 1 \text{ olduğundan } H_2 = \langle 1 + \xi 2 \rangle = \{1, 1 + \xi 2\} \text{ olsun. Bu durumda,}$$

$$G_2 = H_1 \times H_2 = \langle 3 \rangle \times \langle 1 + \xi 2 \rangle = \{1, 3, 1 + \xi 2, 3(1 + \xi 2)\} = \{1, 3, 1 + \xi 2, 3 + \xi 2\}$$

$$3 + \xi 2 = 1 + \xi^2 2 \text{ olduğunu gösterirsek } G_2 = H_1 \times H_2 \text{ olduğunu göstermiş oluruz.}$$

$$\begin{aligned} 3 + \xi 2 &= \xi^2 + \xi + \xi 2 = \xi^2 + \xi 3 \\ &= \xi^2 + 1 + \xi^2 = 1 + \xi^2 2 \end{aligned}$$

Sonuç olarak, $G_2 = \{1 + \pi : \pi \in (2)\} = \{1, 3, 1 + \xi 2, 1 + \xi^2 2\} = \langle 3 \rangle \times \langle 1 + \xi 2 \rangle$ dir.

Sonuç 4. 12 p bir asal ve s pozitif bir tamsayı olsun. O halde, $\mathbb{Z}_{p^s}^* = G_1 \times G_2$ direk çarpımındaki G_1 , mertebesi $p-1$ olan devirli bir grup ve G_2 , mertebesi $p^{(s-1)}$ olan ve aşağıdaki özellikleri sağlayan bir gruptur:

- (i) p tek ise G_2 , mertebesi p^{s-1} olan devirli bir gruptur.
- (ii) $p = 2$ ve $s \leq 2$ ise G_2 , mertebesi p^{s-1} olan devirli bir gruptur.
- (iii) $p = 2$ ve $s \geq 3$ ise G_2 , mertebesi 2 olan devirli bir grup ile mertebesi 2^{s-2} olan devirli bir grubun direk çarpımıdır.

Örnek 4. 11 $\mathbb{Z}_{3^2}$ halkasını ele alalım. $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ dir. $\mathbb{Z}_9^* = G_1 \times G_2$ olacak şekilde G_1 ve G_2 gruplarını belirleyelim. Sonuç 4. 12 (i) den, $p = 3$ olduğunda G_1 , mertebesi $p-1 = 3-1 = 2$ olan devirli bir gruptur. $\mathbb{Z}_9$ halkasında $8^2 = 1$ olduğundan $G_1 = \langle 8 \rangle = \{1, 8\}$ dir.

$G_2 = \{1 + \pi : \pi \in (3)\} = \{1, 4, 7\}$, mertebesi $p^s - 1 = 2^2 - 1 = 3$ olan devirli bir gruptur. $\mathbb{Z}_9$ halkasında $4^2 = 16 = 7$ ve $4^3 = 28 = 1$ olduğundan $G_2 = \langle 4 \rangle$ elde ederiz. Sonuç olarak, $\mathbb{Z}_9^* = \langle 8 \rangle \times \langle 4 \rangle$ tür.

4. 5 Galois Halkalarının Genişlemesi

Teorem 4. 13 $R = GR(p^s, p^{sm})$ ve $R' = GR(p^s, p^{sn})$ olsun. Eğer R' , R nin genişletilmiş halkası ise $m|n$ dir.

İspat:

$$- : R' \rightarrow \overline{R'} = R'/R'p \cong \mathbb{F}_{p^n}$$

homomorfizmasını ele alalım. Bu homomorfizmanın çekirdeği $R'p$ dir. $R + R'p$, R' halkasının bir alt halkasıdır ve $R'p$, $R + R'p$ halkasının bir idealidir. Bu yüzden, $(R + R'p)/R'p$, $R'/R'p$ bölüm halkasının bir alt halkasıdır. Buradan,

$$(R + R'p)/R'p \subseteq \overline{R'} = R'/R'p \cong \mathbb{F}_{p^n}$$

olur. Şimdi $R \cap R'p = Rp$ olduğunu gösterelim. $R \cap R'p \supseteq Rp$ olduğu aşıkardır. $r \in R \cap R'p$ olsun. $r \in R$ ve $r \in R'p$ olur. $r = r'p$ olacak şekilde bir $r' \in R'$ elemanı vardır. O halde, $rp^{s-1} = r'p^s = 0$ olur. Buradan, r sıfırdır veya sıfır bölendir. Bu da $r \in Rp$ olmasını gerektirir. Böylece, $R \cap R'p \subseteq Rp$ olur. Teorem 2. 4 ten,

$$(R + R'p)/R'p \cong R/R \cap R'p$$

olduğunu biliyoruz.

$$(R + R'p)/R'p \cong R/Rp \cong \mathbb{F}_{p^m}$$

olduğundan $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ elde ederiz. Teorem 2. 11 den $m|n$ dir.

Not: Aşağıdaki değişmeli diyagram vardır. “ $\uparrow$ ” kapsamayı göstermektedir.

$$\begin{array}{ccc} - : GR(p^s, p^{sn}) & \rightarrow & \mathbb{F}_p^n \\ \uparrow & & \uparrow \\ - : GR(p^s, p^{sm}) & \rightarrow & \mathbb{F}_p^m \end{array}$$

Şimdi Teorem 4. 13 in tersinin de var olduğunu gösterelim.

Teorem 4. 14 $R = GR(p^s, p^{sm})$ ve $m|n$ olsun. O halde, R yi alt halka kabul eden bir $R' = GR(p^s, p^{sn})$ Galois halkası vardır.

Teorem 4. 14 ü ispatlamak için $\mathbb{Z}_{p^s}$ halkasından Galois halkası elde etmek için yaptığımız halka genişlemesini $R = GR(p^s, p^{sm})$ Galois halkasına genelleştirmemiz gerekiyor. Aşağıda vereceğimiz teoremlerin ispatları $\mathbb{Z}_{p^s}$ için yaptıklarımıza benzer olduğu için tekrar yapmayacağız. Bu teoremlerdeki $R = GR(p^s, p^{sm})$ dir. $R \rightarrow R/Rp$ doğal homomorfizmasını “ $-$ ” ile göstereceğiz ve $\overline{R} = R/Rp \cong \mathbb{F}_{p^m}$ dir.

Teorem 4. 15 $R = GR(p^s, p^{sm})$ halkasının bütün idealleri $(1), (p), (p^2), \dots, (p^{s-1}), (0)$ temel idealleridir. R nin tek maksimal ideali (p) idealidir, ve $R/(p) \cong \mathbb{F}_{p^m}$ dir.

Teorem 4. 16 $(p) = R[x]p$ ideali, $R[x]$ halkasının asal idealidir; $R[x]$ halkasının her asal ideali (p) idealini kapsar; ve $R[x]$ halkasının (p) idealini has olarak kapsayan asal idealleri maksimaldir.

Teorem 4. 17 Q , $R[x]$ halkasının bir ideali olsun.

(i) Q asalımsı ideal ise $\sqrt{Q}$ asal idealdir.

(ii) $\sqrt{Q} \supseteq (p)$

(iii) $\sqrt{Q}$ asal ideal ve (p) idealini has olarak kapsıyorsa Q asalımsı idealdir.

$R[x]$ halkasındaki polinomlar için de aralarında asallık tanımını yapabiliriz.

Tanım 4. 4 $f, g \in R[x]$ olsun. $R[x]f + R[x]g = R[x]$ ise f ve g aralarında asaldır, denir.

Yrd. Teorem 4. 18 f_1 ve $f_2 \in R[x]$ olsun. f_1 ve f_2 polinomlarının $R[x]$ halkasında aralarında asal olması için gerek ve yeter koşul $\overline{f_1}$ ve $\overline{f_2}$ polinomlarının $\mathbb{F}_{p^m}[x]$ halkasında aralarında asal olmasıdır.

Yrd. Teorem 4. 19 (Hensel Yrd. Teoremi) $R[x]$ halkasında f monik bir polinom olsun. $g_1, g_2, \dots, g_r$ polinomları, $\overline{R[x]}$ halkasında ikişerli aralarında asal monik polinomlar olmak üzere $\overline{f} = g_1 g_2 \dots g_r$ olsun. O halde, $R[x]$ halkasında $f = f_1 f_2 \dots f_r$ ve $i = 1, 2, \dots, r$ için $\overline{f_i} = g_i$ olacak şekilde $R[x]$ halkasında ikişerli aralarında asal monik $f_1, f_2, \dots, f_r$ polinomları vardır.

Teorem 4. 20 (Tek Türlü Çarpanlarına Ayrılma Teoremi) $R[x]$ halkasında $f(x)$ monik bir polinom ve $\deg(f) \geq 1$ olsun. O halde,

(i) r pozitif bir tamsayı ve her $i = 1, 2, \dots, r$ için $\overline{f_i} \in \mathbb{F}_{p^m}[x]$ halkasında monik indirgenemez bir polinomun bir kuvveti olmak üzere $f \in R[x]$ halkasında $f = f_1 f_2 \dots f_r$ olacak şekilde ikişerli aralarında asal monik asalımsı $f_1, f_2, \dots, f_r$ polinomlarının çarpımı şeklinde yazılabilir.

$$(ii) f = f_1 f_2 \dots f_r = h_1 h_2 \dots h_t$$

$R[x]$ halkasında ikişerli aralarında asal monik asalımsı polinomların çarpımı olacak şekilde f polinomunun iki türlü çarpanlarına ayrılışı olsun. O halde, $r=t$ dir ve sıralamaya bakılmaksızın $i=1,2,\dots,r$ için $f_i = h_i$ dir.

Tanım 4. 5 $f \in R[x]$ monik bir polinom ve $der(f)=l \geq 1$ olsun. Eğer $\bar{f}, \bar{R}[x]$ halkasında indirgenemez (veya ilkel) ise f polinomuna $R[x]$ halkasında monik temel indirgenemez (veya monik temel indirgenemez) polinom denir. $R[x]$ halkasında monik temel ilkel polinomlar monik temel indirgenemezdir.

Örnek 4. 12 $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$, 2. dereceden monik temel indirgenemez bir polinom ve ξ , $h(x)$ polinomunun $2^2 - 1 = 3$ mertebeli bir kökü olmak üzere

$$\begin{aligned} R = GR(2^2, 2^{2.2}) &= \mathbb{Z}_{2^2}[x] / (x^2 + x + 1) \\ &= \mathbb{Z}_{2^2}[\xi] = \{a_0 + a_1 \xi : a_0, a_1 \in \mathbb{Z}_{2^2}\} \\ &= \{a_0 + a_1 2 : a_0, a_1 \in \tau = \{0, 1, \xi, \xi^2\}\} \end{aligned}$$

Galois halkasını ele alalım. O halde,

$$\begin{aligned} \bar{R} = R/Rp &= GR(2^2, 2^{2.2}) / (2) = \{a_0 + a_1 2 + (2) : a_0, a_1 \in \tau\} \\ &= \{a_0 + (2) : a_0 \in \tau\} = \{0 + (2), 1 + (2), \xi + (2), \xi^2 + (2)\} \end{aligned}$$

olur. Buradan,

$$\bar{R} = GR(2^2, 2^{2.2}) / (2) \cong \mathbb{F}_{2^2} = \{0, 1, \xi, \xi^2\}$$

olur. Şimdi $f(x) = x^2 + \xi x + 1 \in R[x]$ polinomunun temel indirgenemez olduğunu gösterelim. $\bar{f}(x) = x^2 + \xi x + 1 \in \bar{R}[x]$ polinomunun $\bar{R} \cong \mathbb{F}_{2^2}$ sonlu cisminde hiç kökü bulunmadığından, $\bar{f}(x) \in \bar{R}$ indirgenemezdir. Bu yüzden, $f(x) \in R[x]$ monik temel indirgenemez bir polinomdur.

Teorem 4. 21 Her $l \geq 1$ tamsayısı için, $R[x]$ polinom halkasında $x^{p^{ml}-1} - 1$ i bölen l . dereceden monik temel indirgenemez (ve monik temel ilkel) polinomlar vardır.

Örnek 4. 13 $R = GR(2^2, 2^{2.2}) = \mathbb{Z}_{2^2}[x]/(x^2 + x + 1) = \mathbb{Z}_{2^2}[\xi]$ Galois halkasını ele alalım. $R[x]$ halkasında $f(x) = x^2 + (1 + 2\xi^2)x + \xi^2$ temel indirgenemez bir polinomdur. Çünkü $\bar{f}(x) = x^2 + x + \xi^2 \in \bar{R}[x]$ polinomunun $\bar{R} \cong \mathbb{F}_{2^2}$ cisminde hiç kökü yoktur. Ayrıca, $f(x)$ polinomu $R[x]$ halkasında $x^{2^{2.2}-1} - 1 = x^{15} - 1$ i böler.

Teorem 4. 22 $h(x) \in R[x]$, l . dereceden monik temel indirgenemez bir polinom olsun. $R[x]/(h(x))$, karakteristiği p^s ve kardinalitesi p^{sm} olan ve R yi alt halka kabul eden bir Galois halkasıdır. Buradan,

$$R[x]/(h(x)) = GR(p^s, p^{sm})$$

diyebiliriz. $\xi' = x + (h(x))$ yazalım. O halde, $\xi' = \xi' + (h(\xi'))$ ve dolayısıyla $h(\xi') = 0$ olur. Buradan,

$$a_0 + a_1x + \dots + a_{l-1}x^{l-1} + (h(x)) = a_0 + a_1\xi' + \dots + a_{l-1}\xi'^{l-1}$$

olacağından $R[x]/(h(x))$ halkasının her elemanını

$$a_0 + a_1\xi' + \dots + a_{l-1}\xi'^{l-1}, \quad a_i \in R \quad (i = 0, 1, \dots, l-1)$$

şeklinde tek türlü ifade edebiliriz. O halde,

$$R[x]/(h(x)) = R[\xi'] = \{a_0 + a_1\xi' + \dots + a_{l-1}\xi'^{l-1}, a_i \in R \quad (i = 0, 1, \dots, l-1)\}$$

şeklinde yazabiliriz.

Örnek 4. 14 $R = GR(2^2, 2^{2.2}) = \mathbb{Z}_{2^2}[x]/(x^2 + x + 1) = \mathbb{Z}_{2^2}[\xi]$ halkasını ele alalım. $R[x]$ halkasında $h(x) = x^2 + (1 + 2\xi^2)x + \xi^2$ polinomunun 2. dereceden monik temel indirgenemez olduğunu biliyoruz. O halde, Teorem 4. 22 ye göre,

$$\begin{aligned} R[x]/(h(x)) &= GR(2^2, 2^{2.2})[x]/(x^2 + (1 + 2\xi^2)x + \xi^2) \\ &= \{a_0 + a_1x + (x^2 + (1 + 2\xi^2)x + \xi^2) : a_0, a_1 \in GR(2^2, 2^{2.2})\} \end{aligned}$$

halkası karakteristiği 2^2 ve kardinalitesi $2^{2.2.2}$ olan bir Galois halkasıdır, ve

$$GR(2^2, 2^{2.2})[x]/(x^2 + (1 + 2\xi^2)x + \xi^2) = GR(2^2, 2^{2.2.2})$$

diyebiliriz. $\xi' = x + (h(x))$ yazalım. Buradan, $\xi' = \xi' + (h(\xi'))$ ve $h(\xi') = 0$ olur.

$$a_0 + a_1x + (x^2 + (1 + 2\xi^2)x + \xi^2) = a_0 + a_1\xi'$$

olacağından $GR(2^2, 2^{2.2})[x]/(x^2 + (1 + 2\xi^2)x + \xi^2)$ Galois halkasının her elemanını

$a_0, a_1 \in GR(2^2, 2^{2.2})$ olmak üzere $a_0 + a_1\xi'$ şeklinde tek türlü ifade edebiliriz. O halde,

$$GR(2^2, 2^{2.2})[x]/(x^2 + (1 + 2\xi^2)x + \xi^2) = GR(2^2, 2^{2.2})[\xi']$$

yazabiliriz.

Teorem 4. 14 ün İspatı: Teorem 4. 21 ve Teorem 4. 22 den elde edilir.

Teorem 4. 23 $R' = GR(p^s, p^{sn})$ ve m, n nin pozitif bir böleni olsun. O halde, R' karakteristiği p^s ve kardinalitesi p^{sm} olan tek bir Galois halkasını alt halkası olarak kapsar.

İspat: $R = GR(p^s, p^{sm})$, karakteristiği p^s ve kardinalitesi p^{sm} olan bir Galois halkası olsun. $n = ml$ olsun. Teorem 4. 14 ten R yi alt halka kabul eden bir $R' = GR(p^s, p^{sml})$ Galois halkası vardır. Ancak $GR(p^s, p^{sml}) \cong GR(p^s, p^{sn})$ olur. Bu izomorfizma altında, $GR(p^s, p^{sml})$ Galois halkasının bir $R = GR(p^s, p^{sm})$ alt halkası, R' Galois halkasının bir $R_0 = GR(p^s, p^{sm})$ alt halkasına karşılık gelir.

Şimdi $R_0 = GR(p^s, p^{sm})$ alt halkasının tekliğini ispatlayalım. $\mathbb{Z}_{p^s}[x]$ halkasında m . dereceden monik temel indirgenemez ve $x^{p^{m-1}} - 1$ i bölen bir polinomun, R_0 Galois halkasında mertebesi p^{m-1} olan bir η kökünün varlığını, ve ayrıca $\tau_0 = \{0, 1, \eta, \eta^2, \dots, \eta^{p^{m-2}}\}$ olmak üzere

$$R_0 = \{a_0 + a_1p + \dots + a_{s-1}p^{s-1} : a_0, a_1, \dots, a_{s-1} \in \tau_0\}$$

olduğunu Teorem 4. 8 den biliyoruz. R_1 , karakteristiği p^s ve kardinalitesi p^{sm} olan bir Galois halkası ve R' halkasının bir alt halkası olsun. $\mathbb{Z}_{p^s}[x]$ halkasında m . dereceden

monik temel indirgenemez ve $x^{p^m-1}-1$ i bölen bir polinomun, R_1 halkasında mertebesi p^{m-1} olan bir ζ kökü vardır. $\tau_1 = \{0, 1, \zeta, \zeta^2, \dots, \zeta^{p^m-2}\}$ olmak üzere

$$R_1 = \{a_0 + a_1 p + \dots + a_{s-1} p^{s-1} : a_0, a_1, \dots, a_{s-1} \in \tau_1\}$$

dir. Teorem 4. 11 den, R^* birim grubunun mertebesi $p^n - 1$ olan tek bir G_1 alt grubu vardır, ve Teorem 2. 6 dan, G_1 grubunun mertebesi $p^m - 1$ olan tek bir alt grubu vardır. $\langle \eta \rangle$ ve $\langle \zeta \rangle$, G_1 grubunun mertebesi $p^m - 1$ olan iki alt grubu olduğundan $\langle \eta \rangle = \langle \zeta \rangle$ olmalıdır. O halde, $p^m - 1$ sayısı ile aralarında asal bir i pozitif tamsayısı için $\zeta = \eta^i$ dir. Buradan, $\tau_1 = \tau_0$ ve $R_1 = R_0$ olur.

Şimdi Yrd. Teorem 4. 5, Teorem 4. 6 ve Teorem 4. 8 ifadelerini Galois halkalarına genelleştirerek tekrar verelim.

Yrd. Teorem 4. 24 $R = GR(p^s, p^{sm})$, $R' = GR(p^s, p^{sml})$ ve R , R' halkasının bir alt halkası ve $f(x) \in R[x]$ olsun. $\overline{f}(x)$ polinomunun $\overline{R'} \cong \mathbb{F}_{p^{ml}}$ cismindeki kökünün $\overline{\beta}$ ve $\overline{f}(\overline{\beta}) \neq 0$ olduğunu kabul edelim. O halde, $\overline{\alpha} = \overline{\beta}$ olacak şekilde $f(x)$ polinomunun R' halkasında tek bir α kökü vardır.

Teorem 4. 25 p bir asal ve s, m, l pozitif tamsayılar olmak üzere $R' = GR(p^s, p^{sml})$ ve $R = GR(p^s, p^{sm})$ olsun. O halde, $R[x]$ halkasının l . dereceden monik temel indirgenemez her $h(x)$ polinomu için $R' \cong R[x]/(h(x))$ olur.

Teorem 4. 26 $R = GR(p^s, p^{sm})$ olsun. $h(x) \in R[x]$, l . dereceden monik temel indirgenemez ve $R[x]$ halkasında $x^{p^{ml}-1}-1$ i bölen bir polinom olsun. O halde,

(i) $GR(p^s, p^{sml})$ Galois halkasında $h(x)$ polinomunun mertebesi $p^{ml}-1$ olan bir ξ kökü vardır, ve

$$GR(p^s, p^{sml}) = GR(p^s, p^{sm})[\xi] = \{a_0 + a_1 \xi + \dots + a_{l-1} \xi^{l-1} : a_0, a_1, \dots, a_{l-1} \in GR(p^s, p^{sm})\}$$

dir. Ayrıca, $h(x) \in R[x]$ derecesi l veya l den küçük olan ve ξ yi kök kabul eden tek polinomdur.

(ii) $\tau = \{0, 1, \xi, \xi^2, \dots, \xi^{p^{ml}-2}\}$ olsun. $a_0, a_1, \dots, a_{s-1} \in \tau$ olmak üzere, her $c \in GR(p^s, p^{sml})$

$$c = a_0 + a_1 p + \dots + a_{s-1} p^{s-1}$$

şeklinde tek türlü yazılabilir. Ayrıca, c nin birimsel olması için gerek ve yeter koşul $a_0 \neq 0$ olmasıdır. c nin sıfır veya sıfır bölen olması için, yani $c \in (p)$ olması için gerek ve yeter koşul $a_0 = 0$ olmasıdır.

Örnek 4. 15 $R = GR(2^2, 2^{2.2}) = \mathbb{Z}_{2^2}[x]/(x^2 + x + 1) = \mathbb{Z}_{2^2}[\xi]$ Galois halkasını ele alalım. $h(x) = x^2 + (1 + 2\xi^2)x + \xi^2 \in R[x]$ polinomunun temel indirgenemez olduğunu ve $R[x]$ halkasında $x^{2^{2.2}-1} - 1 = x^{15} - 1$ i böldüğünü biliyoruz. Yukarıdaki teoreme göre, $GR(2^2, 2^8)$ Galois halkasında $h(x)$ polinomunun mertebesi 15 olan bir ξ' kökü vardır, ve $GR(2^2, 2^8) = GR(2^2, 2^4)[\xi'] = \{a_0 + a_1 \xi' : a_0, a_1 \in GR(2^2, 2^4)\}$ dir. O halde,

$$GR(2^2, 2^8) = \left\{ \begin{array}{l} 0, 1, 2, 3, \xi, \xi + 1, \xi + 2, \xi + 3, 2\xi, 2\xi + 1, 2\xi + 2, 2\xi + 3, 3\xi, 3\xi + 1, 3\xi + 2, 3\xi + 3 \\ \xi', 1 + \xi', 2 + \xi', \dots, 3\xi' + 3 + \xi' \\ 2\xi', 1 + 2\xi', 2 + 2\xi', \dots, 3\xi' + 3 + 2\xi' \\ 3\xi', 1 + 3\xi', 2 + 3\xi', \dots, 3\xi' + 3 + 3\xi' \\ \xi\xi', 1 + \xi\xi', 2 + \xi\xi', \dots, 3\xi' + 3 + \xi\xi' \\ (\xi + 1)\xi', 1 + (\xi + 1)\xi', 2 + (\xi + 1)\xi', \dots, 3\xi' + 3 + (\xi + 1)\xi' \\ (\xi + 2)\xi', 1 + (\xi + 2)\xi', 2 + (\xi + 2)\xi', \dots, 3\xi' + 3 + (\xi + 2)\xi' \\ (\xi + 3)\xi', 1 + (\xi + 3)\xi', 2 + (\xi + 3)\xi', \dots, 3\xi' + 3 + (\xi + 3)\xi' \\ 2\xi\xi', 1 + 2\xi\xi', 2 + 2\xi\xi', \dots, 3\xi' + 3 + 2\xi\xi' \\ (2\xi + 1)\xi', 1 + (2\xi + 1)\xi', 2 + (2\xi + 1)\xi', \dots, 3\xi' + 3 + (2\xi + 1)\xi' \\ (2\xi + 2)\xi', 1 + (2\xi + 2)\xi', 2 + (2\xi + 2)\xi', \dots, 3\xi' + 3 + (2\xi + 2)\xi' \\ (2\xi + 3)\xi', 1 + (2\xi + 3)\xi', 2 + (2\xi + 3)\xi', \dots, 3\xi' + 3 + (2\xi + 3)\xi' \\ 3\xi\xi', 1 + 3\xi\xi', 2 + 3\xi\xi', \dots, 3\xi' + 3 + 3\xi\xi' \\ (3\xi + 1)\xi', 1 + (3\xi + 1)\xi', 2 + (3\xi + 1)\xi', \dots, 3\xi' + 3 + (3\xi + 1)\xi' \\ (3\xi + 2)\xi', 1 + (3\xi + 2)\xi', 2 + (3\xi + 2)\xi', \dots, 3\xi' + 3 + (3\xi + 2)\xi' \\ (3\xi + 3)\xi', 1 + (3\xi + 3)\xi', 2 + (3\xi + 3)\xi', \dots, 3\xi' + 3 + (3\xi + 3)\xi' \end{array} \right\}$$

$$= \mathbb{Z}_4[\xi, \xi'] = \{a_0 + a_1 \xi + a_2 \xi' + a_3 \xi\xi' : a_0, a_1, a_2, a_3 \in \mathbb{Z}_4\}$$

yazabiliriz.

$\tau' = \{0, 1, \xi', \xi'^2, \dots, \xi'^{2^{2^2}-2} = \xi'^{14}\}$ olsun. $a_0, a_1 \in \tau'$ olmak üzere her $c \in GR(2^2, 2^8)$ elemanını $c = a_0 + a_1 2$ şeklinde tek türlü gösterebiliriz.

Sonuç 4. 27 $R = GR(p^s, p^{sm})$ olsun. $h(x) \in R[x]$, l . dereceden monik temel indirgenemez ve $R[x]$ halkasında $x^{p^{ml}-1} - 1$ i bölen bir polinom, ve $\eta = \xi'^{(p^{ml}-1)/(p^m-1)}$ olsun. O halde, η nün mertebesi $p^m - 1$ dir. $\tau'' = \{0, 1, \eta, \eta^2, \dots, \eta^{p^m-2}\}$ olsun. O halde, $a_0, a_1, \dots, a_{s-1} \in \tau''$ olmak üzere $c = a_0 + a_1 p + \dots + a_{s-1} p^{s-1}$ şeklindeki elemanlar $GR(p^s, p^{sm})$ Galois halkasını oluşturur.

İspat: Teorem 4. 23 te, alt halkanın tekliğinin ispatına benzer bir ispat yapacağız. ξ' elemanının mertebesi $p^{ml} - 1$ olduğundan η nün mertebesi de $p^m - 1$ dir. Teorem 4. 11 den, R^* in mertebesi $p^m - 1$ olan tek bir G_1 alt grubu vardır, ve Teorem 2. 6 dan, G_1 in mertebesi $p^m - 1$ olan tek bir alt grubu vardır. $R = GR(p^s, p^{sm}) = \mathbb{Z}_{p^s}[\xi]$ olmak üzere $\langle \xi \rangle$ devirli grubunun, G_1 in mertebesi $p^m - 1$ olan bir alt grubu olduğunu daha önce söylemiştik. $\langle \eta \rangle$ ve $\langle \xi \rangle$, G_1 in mertebesi $p^m - 1$ olan iki alt grubu olduğundan $\langle \eta \rangle = \langle \xi \rangle$ olmalıdır. O halde, $p^m - 1$ sayısı ile aralarında asal bir i pozitif tamsayısı için $\xi = \eta^i$ dir. Buradan, $\tau = \tau''$ olur.

Örnek 4. 16 $R = GR(2^2, 2^{2.2}) = \mathbb{Z}_{2^2}[x]/(x^2 + x + 1) = \{a_0 + a_1 2 : a_0, a_1 \in \tau = \{0, 1, \xi, \xi^2\}\}$ halkasını alalım. $h(x) = x^2 + (1 + 2\xi^2)x + \xi^2 \in R[x]$ polinomunun temel indirgenemez olduğunu ve $R[x]$ halkasında $x^{2^{2.2}-1} - 1 = x^{15} - 1$ polinomunu böldüğünü biliyoruz. $\xi'^{(p^{ml}-1)/(p^m-1)} = \xi'^{(2^{2.2}-1)/(2^2-1)} = \xi'^5$ olur. $\xi^2 + \xi + 1 = 0$ ve $\xi'^2 + (1 + 2\xi^2)\xi' + \xi^2 = 0$ eşitliklerini kullanarak ξ'^5 elemanını, $a_0, a_1 \in R$ olmak üzere $a_0 + a_1 \xi'$ şeklinde yazalım:

$$\xi'^2 = (3 + 2\xi^2)\xi' + 3\xi^2$$

$$\xi'^3 = (3 + 2\xi^2)[(3 + 2\xi^2)\xi' + 3\xi^2] + 3\xi^2\xi'$$

$$= \xi' + \xi^2 + 2\xi + 3\xi^2\xi'$$

$$\xi'^4 = (3 + 2\xi^2)\xi' + 3\xi^2 + \xi^2\xi' + 2\xi\xi' + 3\xi^2(3 + 2\xi^2)\xi' + 3\xi^2$$

$$= 3\xi' + 4\xi^2\xi' + 4\xi\xi' + 3\xi^2 + \xi$$

$$= 3\xi' + 3\xi^2 + \xi$$

$$\xi'^5 = 3[(3 + 2\xi^2)\xi' + 3\xi^2] + 3\xi^2\xi' + \xi\xi'$$

$$= \xi' + 2\xi^2\xi' + \xi^2 + 3\xi^2\xi' + \xi\xi'$$

$$= \xi' + \xi^2\xi' + \xi^2 + \xi\xi' = \xi' + (3\xi + 3)\xi' + \xi^2 + \xi\xi' = 4\xi' + 4\xi\xi' + \xi^2$$

$$\xi'^5 = \xi^2$$

elde ederiz. O halde, $\xi'^5 = \xi^2$ ve $\tau = \{0, 1, \xi^2, (\xi^2)^2 = \xi\} = \tau = \{0, 1, \xi, \xi^2\}$

4. 6 Galois Halkalarının Otomorfizmaları

$R = GR(p^s, p^{sm})$, $R' = GR(p^s, p^{sn})$ ve R , R' Galois halkasının bir alt halkası olsun.

$R[x]$ halkasında $x^{p^{ml}-1} - 1$ i bölen l . dereceden monik temel indirgenemez $h(x)$ polinomunun, R' halkasında mertebesi $p^{ml} - 1$ olan sıfırdan farklı bir ξ' kökünün varlığını ve $R' = R[\xi']$ olduğunu Teorem 4. 26 dan biliyoruz.

İlk önce aşağıdaki yardımcı teoremi ispatlayalım.

Yrd. Teorem 4. 28 R , R' Galois halkasının bir alt halkası olsun. $h(x)$, l . dereceden monik temel indirgenemez ve $R[x]$ halkasında $x^{p^{ml}-1} - 1$ i bölen bir polinom olsun. ξ' , $h(x)$ polinomunun bir kökü ve R' halkasının mertebesi $p^{ml} - 1$ olan sıfırdan farklı bir elemanı olmak üzere $R' = R[\xi']$ olsun. O halde, $\xi', \xi'^{p^m}, \dots, \xi'^{p^{m(l-1)}}$ elemanlarının hepsi $h(x)$ polinomunun köküdür. Böylece, $h(x) = (\xi' - x)(\xi'^{p^m} - x) \dots (\xi'^{p^{m(l-1)}} - x)$ olur.

İspat: $h(x)$, l . dereceden monik temel indirgenemez bir polinom ve ξ , $h(x)$ polinomunun bir kökü olduğundan $\bar{h}(x)$ de $\bar{R}[x] = \mathbb{F}_{p^m}[x]$ halkasında l . dereceden monik temel ilkel bir polinomdur ve $\bar{\xi} \in \mathbb{F}_{p^m}$, $\bar{h}(x)$ polinomunun köklerinden biridir. Bu

yüzden, $\overline{\xi}$ elemanının mertebesi $p^{ml} - 1$ dir ve $\overline{\xi}, \overline{\xi}^{p^m}, \dots, \overline{\xi}^{p^{m(l-1)}}$ elemanlarının hepsi $\overline{h(x)}$ polinomunun $\overline{R} = \mathbb{F}_{p^m}$ cismindeki kökleridir. $0 \leq i \leq l-1$ olmak üzere her $\overline{\xi}^{p^{mi}}$ için $\overline{\alpha_i} = \overline{\xi}^{p^{mi}}$ olacak şekilde $h(x)$ polinomunun tek bir $\alpha_i \in R'$ kökünün olduğunu Yrd. Teorem 4. 5 ten biliyoruz. α_i , $h(x)$ polinomunun bir kökü ve $h(x) \Big|_{x^{p^{ml}-1}-1}$ olduğundan $\alpha_i^{p^{ml}-1} - 1 = 0$ dir ve böylece $\alpha_i^{p^{ml}} = \alpha_i$ olur. Sonuç 4. 9 (ii) den, $0 \leq l_i \leq p^{ml} - 2$ olmak üzere bir l_i tamsayısı için $\alpha_i = \xi^{l_i}$ dir. Buradan, $\overline{\alpha_i} = \overline{\xi}^{l_i}$ dir. Yukarıda $\overline{\alpha_i} = \overline{\xi}^{p^{mi}}$ olduğunu bulmuştuk. Böylece, $l_i = p^{mi}$ ve $\alpha_i = \xi^{l_i} = \xi^{p^{mi}}$ olur. Bu yüzden, $\xi, \xi^{p^m}, \dots, \xi^{p^{m(l-1)}}$ elemanlarının hepsi $h(x)$ polinomunun $R' = R[\xi]$ halkasındaki l tane köküdür. Tek Türlü Çarpanlarına Ayrılma Teoremi'nden, $h(x)$ polinomunun bütün kökleri bu elemanlardan ibarettir.

Örnek 4. 17 $R = GR(2^2, 2^{2.2}) = \mathbb{Z}_{2^2}[x]/(x^2 + x + 1)$ Galois halkasını ele alalım. $R[x]$ halkasında $h(x) = x^2 + (1 + 2\xi^2)x + \xi^2$ polinomunun temel indirgenemez olduğunu ve $R[x]$ halkasında $x^{2^{2.2}-1} - 1 = x^{15} - 1$ i böldüğünü biliyoruz. ξ' , $h(x)$ polinomunun bir kökü ve R' halkasının mertebesi 15 olan sıfırdan farklı bir elemanı olmak üzere $R' = R[\xi']$ olsun. Yukarıdaki Yrd. Teoreme göre, $\xi'^{12^2} = \xi'^4$ elemanı da $h(x)$ polinomunun bir köküdür. ξ'^4 elemanını $h(x)$ polinomunda yerine yazarsak, $h(\xi'^4) = (\xi'^4)^2 + (1 + 2\xi^2)\xi'^4 + \xi^2$ olur. Örnek 4. 16 da $\xi'^4 = 3\xi' + 3\xi^2 + \xi$ olduğunu bulmuştuk. Bu eşitliği kullanarak,

$$\begin{aligned}
 h(\xi'^4) &= (\xi'^4)^2 + (1 + 2\xi^2)\xi'^4 + \xi^2 \\
 &= (3\xi' + 3\xi^2 + \xi)^2 + (1 + 2\xi^2)(3\xi' + 3\xi^2 + \xi) + \xi^2 \\
 &= \xi'^2 + \xi^2 + 3\xi' + 4\xi + 4\xi^2\xi' + 2\xi\xi' + 4 \\
 &= \xi'^2 + \xi^2 + 3\xi' + 2\xi\xi' \\
 &= (3 + 2\xi^2)\xi' + 3\xi^2 + \xi^2 + 3\xi' + 2\xi\xi' = 2\xi' + 2\xi^2\xi' + 2\xi\xi' \\
 &= 2\xi' + 2(3\xi + 3)\xi' + 2\xi\xi' = 4\xi' + 4\xi\xi' \\
 &= 0
 \end{aligned}$$

olduğunu gösterebiliriz. O halde, ξ' ve ξ'^4 , $h(x) = x^2 + (1 + 2\xi'^2)x + \xi'^2$ polinomunun kökleridir. Böylece, $h(x) = x^2 + (1 + 2\xi'^2)x + \xi'^2 = (x - \xi'^2)(\xi'^4 - x)$ olur.

Teorem 4. 29 $R = GR(p^s, p^{sm})$, $R' = GR(p^s, p^{sml})$ Galois halkasının bir alt halkası olsun. $\xi' \in R'$ mertebesi $p^{ml} - 1$ olan sıfırdan farklı bir eleman ve $R[x]$ halkasında $x^{p^{ml}-1} - 1$ i bölen l . dereceden monik temel indirgenemez $h(x)$ polinomunun bir kökü olmak üzere $R' = R[\xi']$ olsun. Bütün $a_0, a_1, \dots, a_{l-1} \in R$ için, $\phi: R' \rightarrow R'$ dönüşümünü şu şekilde tanımlayalım:

$$\phi(a_0 + a_1\xi' + \dots + a_{l-1}\xi'^{l-1}) = a_0 + a_1\xi'^{p^m} + \dots + a_{l-1}\xi'^{(l-1)p^m}$$

O halde, ϕ , R nin elemanlarını sabit bırakan R' halkasının bir otomorfizmasıdır. Ayrıca, $\alpha \in R'$ olmak üzere $\phi(\alpha) = \alpha$ olması için gerek ve yeter koşul $\alpha \in R$ olmasıdır.

İspat: ϕ nin, R deki elemanları sabit bıraktığı açıktır. ϕ nin, R' halkasının bir otomorfizması olduğunu gösterelim. Yrd. Teorem 4. 28 den, ξ' ve ξ'^{p^m} , $h(x)$ polinomunun kökleridir. $a_0, a_1, \dots, a_{l-1} \in R$ olmak üzere

$$R[x]/(h(x)) \rightarrow R[\xi']$$

$$a_0 + a_1x + \dots + a_{l-1}x^{l-1} + (h(x)) \mapsto a_0 + a_1\xi' + \dots + a_{l-1}\xi'^{l-1}$$

ve

$$R[x]/(h(x)) \rightarrow R[\xi'^{p^m}] \subseteq R[\xi']$$

$$a_0 + a_1x + \dots + a_{l-1}x^{l-1} + (h(x)) \mapsto a_0 + a_1\xi'^{p^m} + \dots + a_{l-1}\xi'^{(l-1)p^m}$$

dönüşümlerinin ikisinin de halka izomorfizması olduğunu Teorem 4. 6 nın ispatından söyleyebiliriz. Buradan, $a_0, a_1, \dots, a_{l-1} \in R$ olmak üzere

$$\phi: R[\xi'] \rightarrow R[\xi'^{p^m}] \subseteq R[\xi']$$

$$a_0 + a_1\xi' + \dots + a_{l-1}\xi'^{l-1} \mapsto a_0 + a_1\xi'^{p^m} + \dots + a_{l-1}\xi'^{(l-1)p^m}$$

halka homomorfizması da izomorfizmadır. Ancak $\left| R[\xi^{p^m}] \right| = p^{sm}$ olduğundan

$$R[\xi^{p^m}] = R[\xi'] \text{ ve } \phi, R' = R[\xi'] \text{ halkasının bir otomorfizması olur.}$$

$\alpha \in R'$ ve $\phi(\alpha) = \alpha$ olsun. $\tau = \{0, 1, \xi', \xi'^2, \dots, \xi'^{p^m-2}\}$ ve $a_0, a_1, \dots, a_{l-1} \in \tau$ olmak üzere

$$\alpha = a_0 + a_1 p + \dots + a_{l-1} p^{l-1}$$

şeklinde α yı, p -adik gösterimle ifade edelim. $\phi(\xi') = \xi'^{p^m}$ olduğundan,

$$\phi(\alpha) = a_0^{p^m} + a_1^{p^m} p + \dots + a_{l-1}^{p^m} p^{l-1}$$

dir. Bu yüzden, $\phi(\alpha) = \alpha$ olması için gerek ve yeter koşul $i = 0, 1, \dots, l-1$ için $a_i^{p^m} = a_i$

olmasıdır. $a_i \in \tau$ olduğundan $a_i = 0$ olması için gerek ve yeter koşul $a_i^{p^m} = 0$ olmasıdır.

Eğer $a_i \neq 0$ ise $j = 0, 1, \dots, p^m-2$ olacak şekilde bir j için $a_i = \xi'^j$ dir. Buradan,

$$\xi'^{jp^m} = \xi'^j \text{ ve } \xi'^{j(p^m-1)} = 1 \text{ olur. } a_i, \langle \xi' \rangle \text{ devirli grubunun mertebesi } p^m-1 \text{ olan bir}$$

$\langle \xi'^j \rangle$ alt grubunun elemanıdır. Ancak, $\langle \xi' \rangle$ devirli grubunun mertebesi p^m-1 olan tek

bir alt grubu vardır ve bu alt grup $\langle \xi'^{(p^m-1)/(p^m-1)} \rangle$ devirli grubudur. Bu yüzden,

$$a_i \in \langle \xi'^{(p^m-1)/(p^m-1)} \rangle \text{ olur. } \eta = \xi'^{(p^m-1)/(p^m-1)} \text{ alırsak, } \tau' = \{0, 1, \eta, \eta^2, \dots, \eta^{p^m-2}\} \text{ olmak üzere}$$

$a_i \in \tau'$ olur. Sonuç 4. 27 den $\alpha \in R$ dir.

Tanım 4. 6 R nin her elemanını sabit bırakan R' halkasının otomorfizmasına, R' halkasının R üzerindeki bir otomorfizması denir. Örneğin, Teorem 4. 29 da tanımladığımız ϕ , R' halkasının R üzerindeki bir otomorfizmasıdır. ϕ otomorfizmasına, R' halkasının R üzerindeki genelleştirilmiş Frobenius otomorfizması denir. R' halkasının birim otomorfizmasını 1 ile gösterelim ve,

$$\phi^0 = 1 \text{ ve } \phi^{i+1} = \phi^i \circ \phi, \quad i = 1, 2, \dots$$

tanımlarını yapalım. Bu durumda, $i = 0, 1, 2, \dots$ için bütün ϕ^i homomorfizmaları, R' halkasının R üzerindeki otomorfizmalarıdır. Her $a_0, a_1, \dots, a_{l-1} \in R$ için

$$\phi(a_0 + a_1 \xi' + \dots + a_{l-1} \xi'^{l-1}) = a_0 + a_1 \xi'^{p^m} + \dots + a_{l-1} \xi'^{(l-1)p^m}$$

$$\phi^2(a_0 + a_1 \xi^{p^1} + \dots + a_{l-1} \xi^{p^{l-1}}) = \phi(a_0 + a_1 (\xi^{p^1})^{p^m} + \dots + a_{l-1} (\xi^{p^{l-1}})^{p^m}) = a_0 + a_1 \xi^{p^{2m}} + \dots + a_{l-1} \xi^{p^{2m} p^{l-1}}$$

$$\vdots$$

$$\phi^i(a_0 + a_1 \xi^{p^1} + \dots + a_{l-1} \xi^{p^{l-1}}) = a_0 + a_1 \xi^{p^{mi}} + \dots + a_{l-1} \xi^{p^{mi} p^{l-1}}$$

olur. ξ^{p^l} elemanın mertebesi $p^{ml} - 1$ olduğundan $\phi^l = 1$ eşitliğini sağlayan en küçük pozitif tamsayı l dir. O halde, $\phi^0 = 1, \phi, \phi^2, \dots, \phi^{l-1}$ otomorfizmaları ϕ ile üretilen mertebesi l olan $\langle \phi \rangle$ devirli grubunu oluşturur.

R' halkasının R üzerindeki otomorfizmaları, bileşke işlemine göre bir grup oluştururlar. Bu gruba R' halkasının R üzerindeki Galois grubu denir ve $\text{Gal}(R'/R)$ ile gösterilir.

Yrd. Teorem 4. 30 $\tau \in \text{Gal}(R'/R)$ olsun. $\overline{R'} \cong \mathbb{F}_{p^{ml}}$ sonlu cisminin bir $\overline{\tau}$ indirgenmiş otomorfizmasını şu şekilde tanımlıyoruz: Her $a \in \mathbb{F}_{p^{ml}}$ için, $\overline{\alpha} = a$ olacak şekilde bir $\alpha \in R'$ vardır.

$$\overline{\tau} : \mathbb{F}_{p^{ml}} \rightarrow \mathbb{F}_{p^{ml}}$$

$$a \mapsto \overline{\tau}(a) = \overline{\tau(\alpha)}$$

dönüşümünü tanımlayalım. O halde, $\overline{\tau}$ iyi tanımlıdır ve $\overline{\tau} \in \text{Gal}(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m})$ dir.

İspat: Öncelikle $\overline{\tau}$ dönüşümünün iyi tanımlı olduğunu gösterelim. $\overline{\alpha} = \overline{\alpha'} = a$ olacak şekilde $\alpha, \alpha' \in R'$ olsun. $\overline{\alpha - \alpha'} = 0$ olduğundan bir $\pi \in R'$ için $\alpha - \alpha' = p\pi$ dir. Buradan, $\overline{\tau(\alpha)} - \overline{\tau(\alpha')} = \overline{\tau(\alpha - \alpha')} = \overline{\tau(p\pi)} = \overline{p\tau(\pi)} = 0$ ve $\overline{\tau(\alpha)} = \overline{\tau(\alpha')}$ olur. Bu yüzden, $\overline{\tau}$ iyi tanımlıdır. Şimdi, $\overline{\tau}$ dönüşümünün halka homomorfizması olduğunu gösterelim. Her $a, b \in \mathbb{F}_{p^{ml}}$ için, $\overline{\alpha} = a, \overline{\beta} = b$ olacak şekilde $\alpha, \beta \in R'$ elemanları vardır. $\overline{\alpha + \beta} = a + b$ ve $\overline{\alpha\beta} = ab$ dir.

$$\overline{\tau(a+b)} = \overline{\tau(\alpha + \beta)} = \overline{\tau(\alpha) + \tau(\beta)} = \overline{\tau(\alpha)} + \overline{\tau(\beta)} = \overline{\tau(a)} + \overline{\tau(b)}, \text{ ve}$$

$$\overline{\tau(ab)} = \overline{\tau(\alpha\beta)} = \overline{\tau(\alpha)\tau(\beta)} = \overline{\tau(\alpha)}\overline{\tau(\beta)} = \overline{\tau(a)}\overline{\tau(b)}$$

olduğundan $\bar{\tau}$ bir halka homomorfizmasıdır. $\bar{\tau}(a) = 0$ olduğunu kabul edelim. $\overline{\tau(\alpha)} = 0$ dır. Yani, bir $\pi \in R'$ için $\tau(\alpha) = p\pi$ dir. Buradan, $\tau(\alpha^s) = \tau(\alpha)^s = (p\pi)^s = 0$ olur. $\tau \in \text{Gal}(R'/R)$ olduğundan $\alpha^s = 0$ dır. Bu da $\alpha \in (p)$ ve $a = \bar{\alpha} = \bar{0}$ olmasını gerektirir. Bu yüzden, $\text{Çek}\bar{\tau} = \{\bar{0}\}$ ve $\bar{\tau}, \mathbb{F}_{p^{ml}}$ cisminin bir otomorfizmasıdır. Her $a \in \mathbb{F}_{p^m}$ için $\bar{\alpha} = a$ olacak şekilde bir $\alpha \in R$ vardır. $\bar{\tau}(a) = \overline{\tau(\alpha)} = \bar{\alpha} = a$ dır. Buradan, $\bar{\tau} \in \text{Gal}(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m})$ olur.

Teorem 4. 31 ϕ, R' halkasının R üzerindeki genelleştirilmiş Frobenius otomorfizması olsun. O halde, $\bar{\phi}$ de $\mathbb{F}_{p^{ml}}$ cisminin $\mathbb{F}_{p^m}$ üzerindeki Frobenius otomorfizmasıdır. Ayrıca, $\text{Gal}(R'/R) = \langle \phi \rangle$ dir ve

$$\text{Gal}(R'/R) \rightarrow \text{Gal}(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m})$$

$$\tau \mapsto \bar{\tau}$$

bir grup izomorfizmasıdır.

İspat: Yrd. Teorem 4. 30 dan, $\bar{\phi} \in \text{Gal}(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m})$ dir. ϕ nin tanımı gereği $\phi(\xi') = \xi'^{p^m}$ olur. Buradan, $\bar{\phi}(\bar{\xi}') = \overline{\phi(\xi')} = \overline{\xi'^{p^m}} = \bar{\xi}'^{p^m} = \sigma(\bar{\xi}')$ ve dolayısıyla $\bar{\phi} = \sigma$ dır.

$\tau \in \text{Gal}(R'/R)$ olsun. O halde, $0 \leq j \leq p^{ml} - 2$ ve $\text{ebob}(j, p^{ml} - 1) = 1$ olmak üzere $\tau(\xi') = \xi'^j$ dir. Buradan, $\bar{\tau}(\bar{\xi}') = \overline{\tau(\xi')} = \overline{\xi'^j} = \bar{\xi}'^j$ olur. Yrd. Teorem 4. 30 dan, $\bar{\tau} \in \text{Gal}(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m})$ olduğunu biliyoruz. $\text{Gal}(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m}) = \langle \sigma \rangle$ olduğundan $\bar{\tau} = \sigma^i$ kabul edebiliriz. O halde, $\bar{\tau}(\bar{\xi}') = \sigma^i(\bar{\xi}') = \bar{\xi}'^{p^{mi}}$ dir. Bu yüzden, $j = p^{mi}$ ve $\tau(\xi') = \xi'^j = \xi'^{p^{mi}}$ dir. Yani $\tau = \phi^i$ dir.

Sonuç 4. 32 $n = mld$ ve $\phi, R' = GR(p^s, p^{sn})$ halkasının $R = GR(p^s, p^{sm})$ üzerindeki Frobenius otomorfizması olsun. O halde,

(i) $\phi^d, R' = GR(p^s, p^{sn})$ halkasının $R'' = GR(p^s, p^{smd})$ üzerindeki Frobenius otomorfizmasıdır ve $\text{Gal}(R'/R'') = \langle \phi^d \rangle$, mertebesi l olan devirli gruptur.

(ii) Her $\alpha \in R''$ için, $\phi(\alpha) \in R''$ dir. ϕ nin R'' halkasına kısıtlanışını $\phi|_{R''}$ ile gösterelim. O halde,

$$\phi|_{R''} : R'' \rightarrow R''$$

$$\alpha \mapsto \phi(\alpha)$$

dönüşümü iyi tanımlıdır. $\phi|_{R''}$, R'' halkasının R üzerindeki Frobenius otomorfizmasıdır ve $\text{Gal}(R''/R) = \langle \phi|_{R''} \rangle$, mertebesi d olan devirli bir gruptur.

4. 7 Genelleştirilmiş İz ve Norm

Tanım 4. 8 $R = GR(p^s, p^{sm})$, $R' = GR(p^s, p^{sml})$ Galois halkasının bir alt halkası ve ϕ , R' halkasının R üzerindeki genelleştirilmiş Frobenius otomorfizması olsun. $\alpha \in R'$ elemanının R halkasına göre genelleştirilmiş izi,

$$T_{R'/R}(\alpha) = \alpha + \phi(\alpha) + \cdots + \phi^{l-1}(\alpha)$$

şeklinde tanımlanır.

$\alpha \in R'$ elemanının R halkasına göre genelleştirilmiş normu,

$$N_{R'/R}(\alpha) = \alpha \phi(\alpha) \cdots \phi^{l-1}(\alpha)$$

şeklinde tanımlanır.

Eğer R ve R' halkalarını biliyorsak $T_{R'/R}$ ve $N_{R'/R}$ yerine sırasıyla T ve N yazabiliriz.

Teorem 4. 33 $\alpha, \beta \in R'$ ve $a \in R$ için aşağıdaki ifadeler doğrudur:

$$(i) \quad T(\alpha) \in R;$$

$$(i') \quad N(\alpha) \in R;$$

$$(ii) \quad T(\alpha + \beta) = T(\alpha) + T(\beta);$$

$$(ii') \quad N(\alpha\beta) = N(\alpha)N(\beta);$$

$$(iii) \quad T(a\alpha) = aT(\alpha) \text{ ve,}$$

$$(iii') \quad N(a\alpha) = a^l N(\alpha) \text{ ve,}$$

$$\text{özel olarak, } T(a) = la;$$

$$\text{özel olarak, } T(a) = a^l;$$

$$(iv) \quad T(\phi(\alpha)) = T(\alpha);$$

$$(iv') \quad N(\phi(\alpha)) = N(\alpha).$$

İspat: Yukarıdaki ifadelerin ispatları iz ve norm için benzer olduklarından sadece iz için ispat yapacağız.

$$(i) \phi(T(\alpha)) = \phi(\alpha + \phi(\alpha) + \dots + \phi^{l-1}(\alpha)) = \phi(\alpha) + \phi^2(\alpha) + \dots + \phi^{l-1}(\alpha) + \alpha = T(\alpha)$$

olduğundan $T(\alpha) \in R$ dir.

$$(ii) T(\alpha + \beta) = \alpha + \beta + \phi(\alpha + \beta) + \dots + \phi^{l-1}(\alpha + \beta) \\ = \alpha + \phi(\alpha) + \dots + \phi^{l-1}(\alpha) + \beta + \phi(\beta) + \dots + \phi^{l-1}(\beta) = T(\alpha) + T(\beta)$$

$$(iii) T(a\alpha) = a\alpha + \phi(a\alpha) + \dots + \phi^{l-1}(a\alpha) \\ = a(\alpha + \phi(\alpha) + \dots + \phi^{l-1}(\alpha)) = aT(\alpha)$$

$a \in R$ olduğundan $T(a) = a + \phi(a) + \dots + \phi^{l-1}(a) = a + a + \dots + a = la$ dir.

$$(iv) T(\phi(\alpha)) = \phi(\alpha) + \phi(\phi(\alpha)) + \dots + \phi^{l-1}(\phi(\alpha)) \\ = \phi(\alpha) + \phi^2(\alpha) + \dots + \phi^{l-1}(\alpha) + \alpha = T(\alpha)$$

Teorem 4. 34 $R = GR(p^s, p^{sm})$, $R' = GR(p^s, p^{sml})$ Galois halkasının alt halkası ve $R' = GR(p^s, p^{sml})$, $R'' = GR(p^s, p^{smld})$ Galois halkasının bir alt halkası olsun. O halde, her $\alpha \in R''$ için

$$T_{R''/R}(\alpha) = T_{R'/R}(T_{R''/R'}(\alpha)) \quad \text{ve} \quad N_{R''/R}(\alpha) = N_{R'/R}(N_{R''/R'}(\alpha))$$

eşitlikleri vardır.

İspat: Yukarıdaki eşitliklerin ispatları iz ve norm için benzer olduğundan sadece iz için yapacağız. Sonuç 4. 32 ye göre ϕ , $R' = GR(p^s, p^{sml})$ halkasının $R = GR(p^s, p^{sm})$ üzerindeki Frobenius otomorfizması olmak üzere ϕ^l , $R'' = GR(p^s, p^{smld})$ halkasının $R' = GR(p^s, p^{sml})$ üzerindeki Frobenius otomorfizmasıdır ve $\text{Gal}(R''/R') = \langle \phi^l \rangle$, mertebesi d olan devirli bir gruptur. Her $\alpha \in R'$ için, $\phi(\alpha) \in R'$ dür. ϕ nin R' halkasına kısıtlanışını $\phi|_{R'}$ ile gösterelim. O halde,

$$\phi|_{R'} : R' \rightarrow R'$$

$$\alpha \mapsto \phi(\alpha)$$

dönüşümü iyi tanımlıdır. $\phi|_{R'}$, R' halkasının R üzerindeki Frobenius otomorfizmasıdır ve $\text{Gal}(R'/R) = \langle \phi|_{R'} \rangle$, mertebesi l olan devirli gruptur.

Teorem 4. 33 ten $T_{R''/R'}(\alpha) \in R'$ olduğunu biliyoruz. O halde, $T_{R'/R}(T_{R''/R'}(\alpha))$ iyi tanımlıdır.

$$\begin{aligned} T_{R'/R}(T_{R''/R'}(\alpha)) &= \sum_{i=0}^{l-1} \phi^i(T_{R''/R'}(\alpha)) \\ &= \sum_{i=0}^{l-1} \phi^i \left(\sum_{j=0}^{d-1} \phi^{lj}(\alpha) \right) = \sum_{i=0}^{l-1} \phi^i \left(\alpha + \phi^l(\alpha) + \phi^{2l}(\alpha) + \dots + \phi^{l(d-1)}(\alpha) \right) \\ &= \phi^0 \left(\alpha + \phi^l(\alpha) + \phi^{2l}(\alpha) + \dots + \phi^{l(d-1)}(\alpha) \right) + \phi \left(\alpha + \phi^l(\alpha) + \phi^{2l}(\alpha) + \dots + \phi^{l(d-1)}(\alpha) \right) + \dots + \\ &\quad \phi^{l-1} \left(\alpha + \phi^l(\alpha) + \phi^{2l}(\alpha) + \dots + \phi^{l(d-1)}(\alpha) \right) \\ &= \alpha + \phi^l(\alpha) + \phi^{2l}(\alpha) + \dots + \phi^{l(d-1)}(\alpha) + \phi(\alpha) + \phi^{l+1}(\alpha) + \phi^{2l+1}(\alpha) + \dots + \phi^{l(d-1)+1}(\alpha) + \dots + \\ &\quad \phi^{l-1}(\alpha) + \phi^{l+l-1}(\alpha) + \phi^{2l+l-1}(\alpha) + \dots + \phi^{l(d-1)+l-1}(\alpha) \\ &= \sum_{i=0}^{ld-1} \phi^i(\alpha) = T_{R''/R}(\alpha) \end{aligned}$$

elde ederiz.

BÖLÜM 5

ZİNCİR HALKALAR

Bu bölümde, ilk olarak yerel halkaların ve daha sonra zincir halkaların tanım ve örneklerini vereceğiz. Bölümün amacı, herhangi bir zincir halkanın Galois halkaları kullanılarak nasıl inşa edildiğini göstermek ve sonrasında örneklendirme yapmaktır. [6], [7], [8], [9], [10], [11] i inceledikten sonra bu kaynaklardaki ilgili tanım ve teoremleri bir araya getirmek suretiyle Zincir Halkalar Bölümü'nü oluşturduk.

Tanım 5. 1 R bir halka olsun. R nin bütün maksimal sağ ideallerinin kesişimine Jacobson Radikali denir, ve $Rad(R)$ ile gösterilir.

Önerme 5. 1 R bir halka olsun. $Rad(R)$, R nin bütün maksimal sol ideallerinin kesişimine de eşittir ve R nin bir idealidir.

Yrd. Teorem 5. 2 R sonlu ve birimli bir halka olsun. $a, b \in R$ ve $ab = 1$ ise $ba = 1$ dir.

İspat: $bR \supseteq b^2R \supseteq \dots \supseteq b^nR \supseteq b^{n+1}R \supseteq \dots$

sonlu zincirini düşünelim. $b^nR \neq 0$ dir. Çünkü $b^nR = 0$ olsaydı $b^na = 0$ ve bunu a^n ile çarptığımızda $a = 0$ olurdu. O halde, $b^nR = b^{n+1}R \neq 0$ dir. Buradan, $b^{n+1}x = b^n$ olur. Her iki tarafı a^n ile çarptığımızda $bx = 1$ olur. $x = 1x = (ab)x = a(bx) = a$ ve $ba = 1$ elde ederiz.

Önerme 5. 3 R sonlu ve birimli bir halka olsun. O halde,

$$Rad(R) = \{r \in R : \forall s \in R \text{ için } 1 - rs \text{ birimsel eleman} \}.$$

İspat: $r \in Rad(R)$ olsun. O halde, R nin her M maksimal ideali için $r \in M$ dir. Buradan, $1 \notin M + rR$ olur. Tersine, R nin her M maksimal ideali için $1 \notin M + rR$ ise

$M \subseteq M + rR$ dir. M maksimal olduğundan $r \in M$ ve dolayısıyla, $r \in \text{Rad}(R)$ olur. Bu yüzden, $r \in \text{Rad}(R)$ olması, her M maksimal ideali ve $s \in R$ için $1 - rs \notin M$ olmasıyla denktir. O halde, $1 - rs$ sağ birimseldir. Yrd. Teorem 5. 2 ye göre $1 - rs$ birimseldir.

Önerme 5. 4 $\text{Rad}(R)$, R nin nilpotent idealidir.

Tanım 5. 4 R bir halka, $m \geq 1$ bir tamsayı ve $\text{Rad}(R) = M$ olsun. Eğer $M^m = \{0\}$ ve $M^{m-1} \neq \{0\}$ ise m tamsayısına M nin nilpotentlik indeksi denir.

Tanım 5. 2 R sonlu ve birimli bir halka olsun. $R/\text{Rad}(R)$ sonlu bir cisim ise R ye yerel halka denir.

Teorem 5. 5 Aşağıdaki ifadeler birbirine denktir:

- (i) R bir yerel halkadır.
- (ii) R nin tam bir tane maksimal sağ (veya sol) ideali vardır.
- (iii) R nin birimsel olmayan elemanları, R nin bir has idealinin içindedir.
- (iv) R nin birimsel olmayan elemanları, R nin bir sağ (veya sol) idealini oluşturur.
- (v) R nin birimsel olmayan elemanları, toplamsal Abelian grup oluşturur.
- (vi) Her $r \in R$ için, r veya $1 + r$ birimseldir.

İspat: (i) $\Leftrightarrow$ (ii) R bir yerel halka olsun. O halde, $R/\text{Rad}(R)$ sonlu bir cisim ve $\text{Rad}(R)$ maksimal idealdir. $\text{Rad}(R)$, R nin bütün maksimal idealleri tarafından kapsandığından R nin tek bir maksimal ideali olmak zorundadır.

(ii) $\Rightarrow$ (iii) R nin tek maksimal sağ ideali M olsun. $r \in R$, R nin birimsel olmayan bir elemanı olsun. O halde, $rR \subseteq R$ olur. R nin her has ideali bir maksimal ideal tarafından kapsandığından $rR \subseteq M$, yani $r \in M$ dir. Bu yüzden, R nin birimsel olmayan bütün elemanları M maksimal idealinin içindedir.

(iii) $\Rightarrow$ (iv) R nin birimsel olmayan elemanları, R nin bir I has idealinin içinde olsun. I has ideal olduğundan hiçbir elemanı birimsel olamaz. Bu yüzden, I nin bütün elemanları birimsellerden ibarettir.

(v) $\Rightarrow$ (vi) R nin birimsel olmayan elemanları, toplamsal G Abelian grubunu oluştursun. $r \notin G$ ise r birimseldir. $r \in G$ ise $1+r$, G nin elemanı olamaz. Çünkü $1+r \in G$ olsaydı $1+r-r=1 \in G$ olurdu. Bu yüzden, $1+r$ birimseldir.

(vi) $\Rightarrow$ (ii) Her $r \in R$ için, r veya $1+r$ birimsel olsun. R nin $M_1 \neq M_2$ olmak üzere iki tane M_1 , M_2 maksimal ideali olduğunu kabul edelim. $M_1 \neq M_2$ ise en az bir tane $m_1 \in M_1 \setminus M_2$ vardır. M_2 , R nin maksimal ideali olduğundan $M_2 + m_1 R = R$ dir. O halde, $m_2 + m_1 r = 1$ olacak şekilde $m_2 \in M_2$ ve $r \in R$ vardır. $m_1 r = 1 - m_2 \in M_1$ ve $1 - m_2$ birimseldir. Bu ise M_1 in maksimal ideal olmasıyla çelişir. Bu yüzden, R nin tek maksimal ideali vardır.

Örnek 5. 1 Sonlu cisimler yerel halkadır.

Örnek 5. 2 Galois halkaları yerel halkadır.

Teorem 5. 6 R bir yerel halka ve maksimal ideali M olsun. O halde, aşağıdaki ifadeler birbirine denktir:

- (i) Her sağ (sol) ideali temel idealdir.
- (ii) M temel idealdir.

Tanım 5. 3 Bir halkanın bütün sol idealleri kapsamaya göre lineer sıralı ise yani bir zincir oluşturuyorsa bu halkaya sol zincir halka denir. Benzer şekilde, sağ zincir halka tanımını da yapabiliriz.

Bu tanımdan zincir halkaların tek bir maksimal ideali olduğunu söyleyebiliriz. O halde, bütün zincir halkalar yerel halkadır.

Teorem 5. 7 R sonlu ve birimli bir halka olsun. $Rad(R) = M$ olsun. O halde, aşağıdaki ifadeler birbirine denktir:

- (i) R bir sol zincir halkadır.
- (ii) R nin temel sol idealleri bir zincir oluşturur.
- (iii) R bir yerel halkadır ve $M = R\theta$ sol temel idealdir.
- (iv) R bir sağ zincir halkadır.

Ayrıca, R halkası yukarıdaki koşulları sağlarsa, i pozitif bir tamsayı olmak üzere R nin her has ideali,

$$M^i = R\theta^i = \theta^i R$$

şeklindedir.

İspat: $M = \{0\}$ ise $R \cong \mathbb{F}_q$ olacağından (i)-(iv) koşulları sağlanır. $M \neq \{0\}$ alalım. Bu durumda, $M^2 \subsetneq M$ olur.

(i) $\Leftrightarrow$ (ii) R bir sol zincir halka ise R nin sol idealleri kapsamaya göre lineer sıralıdır. O halde, R nin tek bir sol maksimal ideali vardır. Yani, R yerel halkadır. Tersî, sol zincir halkanın tanımı gereği vardır.

(i) $\Rightarrow$ (iii) R bir sol zincir halka olsun. R nin yerel halka olduğunu yukarıda söyledik. $V = M/M^2$ bölüm modülünü ele alalım. $MV = VM = 0$ dır. Buradan, V , $R/M \cong \mathbb{F}_q$ üzerinde hem sol hem de sağ vektör uzayı olur. M ve M^2 arasında kalan idealler V nin alt uzaylarına denk gelir. R nin sol idealleri sıralı olduğundan $\text{boy} V = 1$ olmalıdır. $\theta \in M \setminus M^2$ olsun. $R\theta \subseteq M$ ve $R\theta \not\subseteq M^2$ olduğundan $R\theta = M$ elde ederiz.

(iii) $\Rightarrow$ (i), (iv) R bir yerel halkadır ve $M = R\theta$ sol temel ideal olsun. Burada önemli olan $M = \theta R$ olduğunu göstermektir. $M = R\theta$ ise $\text{boy}_{R/M} V = 1$ dir ve $\theta \in M \setminus M^2$ olduğundan $M = \theta R + M^2$ dir. Buradan,

$$\begin{aligned} M &= \theta R + M^2 = \theta R + (\theta R + M^2)M \\ &= \theta R + M^3 = \dots = \theta R + M^m = \theta R \end{aligned}$$

olur. $i = 1, 2, \dots$ için $M^i = R\theta^i = \theta^i R$ elde ederiz. Böylece,

$$R = M^0 \supsetneq M \supsetneq M^2 \supsetneq \dots \supsetneq M^{m-1} \supsetneq M^m = \{0\} \quad (5.1)$$

iki taraflı ideallerin bir zincirini elde etmiş olduk. Şimdi, $0 \neq a \in R$ alalım. $a \in M^i \setminus M^{i+1} = R\theta^i \setminus R\theta^{i+1}$ olacak şekilde $i \in \{0, 1, \dots, m-1\}$ tamsayısı vardır. Yani, $u \in R \setminus M$ birimsel olmak üzere $a = u\theta^i$ dir. O halde, $Ra = R\theta^i$ olur. Dolayısıyla, R nin her sol ideali (5.1) zincirine aittir. (iii) $\Leftrightarrow$ (iv) olduğunu yukarıda yaptıklarımızdan söyleyebiliriz.

Sonuç 5. 8 Bir yerel halkanın maksimal ideali temel ideal ise bu halka sonlu zincir halkadır.

Sonuç 5. 9 Sonlu zincir halkaların her ideali temel idealdir. Dolayısıyla, her sonlu zincir halka temel ideal halkasıdır.

İspat: Sonlu bir R zincir halkasında $Rad(R) = M$ nin temel ideal olduğunu Teorem 5. 7 den biliyoruz. Teorem 5. 6 dan, R nin bütün sol (sağ) idealleri temel idealdir.

Örnek 5. 3 Galois halkaları zincir halkadır. $R = GR(p^s, p^{sm})$ Galois halkasının bütün ideallerinin $(1), (p), (p^2), \dots, (p^{s-1}), (0)$ olduğunu Bölüm 4 ten biliyoruz. R nin idealleri

$$(1) \supset (p) \supset (p^2) \supset \dots \supset (p^{s-1}) \supset (0)$$

şeklinde bir zincir oluşturduğundan $R = GR(p^s, p^{sm})$ bir zincir halkadır.

Tanım 5. 5 R bir Galois halkası olsun. $a_0 \in R$ birimsel olmak üzere

$$g(x) = x^k + p(a_{k-1}x^{k-1} + \dots + a_1x + a_0) \in R[x]$$

polinomuna R üzerinde k . dereceden Eisenstein polinomu denir. $R[x]/(g(x))$ kalan sınıf halkasına R nin Eisenstein genişlemesi denir.

Tanım 5. 6 R , maksimal ideali M olan sonlu bir zincir halka olsun.

p^s : R nin karakteristiği

$$p^m : |R/M| = |\mathbb{F}_{p^m}|$$

β : M nin nilpotentlik indeksi

$$s = 1 \text{ iken } t = \beta \text{ ve } s > 1 \text{ iken } 1 \leq t \leq k \text{ olmak üzere } \beta = (s-1)k + t$$

k : $p \in M^k$ olacak şekilde β ya eşit veya küçük olan en büyük tamsayı

olmak üzere p, s, m, k, t tamsayılarına R nin sabitleri denir.

Teorem 5. 10 $g(x) \in GR(p^s, p^{sm})[x]$, k . dereceden bir Eisenstein polinomu olsun. p, s, m, k, t sabitlerine sahip her R sonlu zincir halkası

$$R = GR(p^s, p^{sm})[x]/(g, p^{s-1}x^t) \quad (5. 2)$$

şeklinde yazılabilir.

Örnek 5. 4 $\mathbb{Z}_{2^2} = \mathbb{Z}_4 = GR(2^2, 2^2)$ Galois halkasını ele alalım. Teorem 5. 9 a göre,

$$R = GR(2^2, 2^2)[x]/(x^2 + 2, 2x^2) = GR(2^2, 2^2)[x]/(x^2 + 2) = \mathbb{Z}_4[x]/(x^2 + 2)$$

$p = 2$, $s = 2$, $m = 1$, $k = 2$, $t = 2$ sabitlerine sahip bir zincir halkadır.

$$\begin{aligned} R &= \mathbb{Z}_4[x]/(x^2 + 2) = \{a + bx + (x^2 + 2) : a, b \in \mathbb{Z}_4\} \\ &= \{a + bx : x^2 = 2 \text{ ve } a, b \in \mathbb{Z}_4\} \\ &= \{0, 1, 2, 3, x, 1+x, 2+x, 3+x, 2x, 1+2x, 2+2x, 3+2x, 3x, 1+3x, 2+3x, 3+3x\} \end{aligned}$$

Sonuç 5. 9 dan, sonlu zincir halkaların her idealinin temel ideal olduğunu biliyoruz.

Şimdi R nin ideallerini belirleyelim:

$$\{0\}$$

$$1R = R$$

$$2R = \{0, 2, 2x, 2+2x\}$$

$$3R = R$$

$$xR = \{0, x, 2x, 3x, 2, 2+x, 2+2x, 2+3x\}$$

$$(1+x)R = \{0, 1+x, 2+2x, 3+3x, 3+2x, 1\} = R$$

$$(2+x)R = \{0, 2+x, 2x, 2+3x, 2+2x, 3x, 2, x\}$$

$$(3+x)R = \{0, 3+x, 2+2x, 1+3x, 2+3x, 1\} = R$$

$$2xR = \{0, 2x\}$$

$$(1+2x)R = \{0, 1+2x, 2, 3+2x, x, 2x, 1\} = R$$

$$(2+2x)R = \{0, 2+2x, 2x, 2\}$$

$$(3+2x)R = \{0, 3+2x, 2, 2x, 3\} = R$$

$$3xR = \{0, 3x, 2x, x, 2, 3x+2, 2x+2\}$$

$$(1+3x)R = \{0, 1+3x, 2+2x, 3+x, x+2, 1\} = R$$

$$(2+3x)R = \{0, 2+3x, 2x, 2+x, 2+2x, 2, x, 3x\}$$

$$(3+3x)R = \{0, 3+3x, 2+2x, 1+x, 2+3x, 1+2x, 1\} = R$$

R nin has idealleri:

$$xR = \{0, x, 2x, 3x, 2, x+2, 2+2x, 2+3x\}$$

$$(2+x)R = \{0, 2+x, 2x, 2+3x, 2+2x, 3x, 2, x\}$$

$$2xR = \{0, 2x\}$$

$$(2+2x)R = \{0, 2+2x, 2x, 2\}$$

$$3xR = \{0, 3x, 2x, x, 2, 3x+2, 2x+2\}$$

$$(2+3x)R = \{0, 2+3x, 2x, 2+x, 2+2x, 2, x, 3x\}$$

olup

$$xR = (2+x)R = 3xR = (2+3x)R$$

$$2R = (2+2x)R$$

elde ederiz. O halde, R nin bütün idealleri $R, xR, 2R, 2xR, \{0\}$ temel idealleridir ve

$$R \supset xR \supset 2R \supset 2xR \supset \{0\}$$

sonlu zincirini oluştururlar. Bu durumda, R nin tek maksimal ideali xR olur. Teorem 5. 7 ye göre, R nin tek maksimal ideali M olmak üzere $M = \theta R$ ve R nin her has idealinin $M^i = \theta^i R$ şeklinde olduğunu biliyoruz. O halde, bu örnekte

$$M = xR$$

$$M^2 = x^2 R = 2R$$

$$M^3 = x^3 R = 2xR$$

$$M^4 = x^4 R = 2^2 R = \{0\}$$

olur. $M^4 = \{0\}$ ve $M^3 \neq \{0\}$ olduğundan M nin nilpotentlik indeksi 4 tür. Ayrıca, M nin nilpotentlik indeksinin 4 olduğunu Tanım 5. 6 dan da söyleyebiliriz. Tanıma göre, $s > 1$ iken $1 \leq t \leq k$ olmak üzere $\beta = (s-1)k + t$ dir. Bu örnekte, $s = 2 > 1$ ve $1 < t = k = 2$ olduğundan $\beta = (2-1)2 + 2 = 4$ tür.

Zincir halkaların yerel halka olduğunu biliyoruz ve Teorem 5. 5 ten bir yerel halkada birimsel olmayan elemanların, halkanın tek maksimal idealini oluşturduğunu biliyoruz. O halde, R nin tek maksimal ideali $M = xR$ olduğundan R nin birimsel olmayan

elemanları $M = xR$ idealini oluşturur. Bu durumda, R nin birimsel elemanlarının kümesi $R \setminus xR$ olur ve $1, 3, 1+x, 3+x, 1+2x, 3+2x, 1+3x, 3+3x$ elemanlarından oluşur.

BÖLÜM 6

SONUÇ VE ÖNERİLER

Bu çalışmada, Galois ve zincir halkalarına örneklendirmeler yapılarak bu halkaların yapısı ve özellikleri tanıtıldı. Daha ileri seviyede bu halkaları baz alarak, verilen örnekleri de dikkate almak suretiyle Kodlama Teorisinde kullanılacak şekilde yeni çalışmalar yapılabilir.

KAYNAKLAR

- [1] Wan, Z. X. , (2003). Lectures on Finite Fields and Galois Rings, World Scientific.
- [2] Agargun, G. A. ,Aygör, N. K. , Ersoy, B. ve Alan, M., (2002). Soyut Cebir Cilt 2, Yıldız Teknik Üniversitesi Vakfı Yayınları, İstanbul.
- [3] Çallıalp, F. ve Tekir Ü., (2009). Değişmeli Halkalar ve Modüller, Birsan Yayınevi, İstanbul.
- [4] Çallıalp, F. ,(2001). Örneklerle Soyut Cebir, Birsan Yayınevi, İstanbul.
- [5] Wan, Z. X. , (1997). Quaternary Codes, World Scientific.
- [6] McDonald, B. R. , (1974). Finite Rings with Identity, Marcel Dekker, New York.
- [7] Raghavendran R. (1969)Finite associative rings.Compositio Mathematica, 21:195– 229.
- [8] Hou, X., (2001). “Finite Commutative Chain Rings”, Finite Fields and Their Applications, 7:382-396.
- [9] Hou, X., Leungh K. H. ve Ma, S. L. , (2003). “On the groups of units of finite commutative chain rings”, Finite Fields and Their Applications, 9: 20–38.
- [10] Olayan, H., (2001). The Structure Of Chain Rings, Doktora Tezi, College of Science, King Saud University, Riyadh.
- [11] Janusz, G. J., (1966). “Separable algebras over commutative rings”, Transactions of the American Mathematical Society,122:461–479.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı :Elif ALTINAY
Doğum Tarihi ve Yeri :28/05/1985 – Safranbolu
Yabancı Dili :İngilizce
E-posta :altinay.elif@gmail.com

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Y. Lisans	Matematik	Yıldız Teknik Üniversitesi	2011
Lisans	Matematik	Yıldız Teknik Üniversitesi	2009
Lise		İbrahim Turhan Lisesi	2003