T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SONLU CİSİMLER VE UYGULAMALARI

Ayşe KESKİN

Doç. Dr. Betül GEZER

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

BURSA – 2017

TEZ ONAYI

Ayşe KESKİN tarafından hazırlanan "Sonlu Cisimler ve Uygulamaları" adlı tez çalışması aşağıdaki jüri tarafından oy birliği ile Uludağ Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Doç. Dr. Betül GEZER

Başkan : Prof. Dr. Osman BİZİM
Uludağ Üniversitesi, Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye : Doç. Dr. Betül GEZER
Uludağ Üniversitesi, Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye : Yard. Doç. Dr. Fırat EVİRGEN
Balıkesir Üniversitesi, Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Yukarıdaki sonucu onaylarım

Prof. Dr. Ali Bayram
Enstitü Müdürü
.../.../...

U.Ü. Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

01/06/2017
Ayşe KESKİN

ÖZET

Yüksek Lisans Tezi

SONLU CİSİMLER VE UYGULAMALARI

Ayşe KESKİN

Uludağ Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Doç. Dr. Betül GEZER

Bu çalışmada sonlu cisimlerin özellikleri ele alınmış ve sonlu cisimlerin eliptik eğriler üzerine uygulamaları üzerinde durulmuştur.

Birinci bölümünde çalışmada kullanılacak olan bazı temel kavram ve teoremler verilmiştir.

İkinci bölümde sonlu cisimlerin cebirsel özellikleri ele alınmış, her p asal sayısı ve her $n \in \mathbb{N}$ sayısı için p^n mertebeli bir sonlu cismin var olduğu ve $\mathbb{F}_p[x]$ halkasında istenen her dereceye sahip bir indirgenmez polinomun varlığı ele alınmıştır. Daha sonra indirgenemez polinomların kökleri ele alınarak sonlu cisimlerin Galois grupları ele alınmış ve sonlu cisimler için iz, norm ve baz kavramları ele alınarak ve bunlarla ilgili bazı teoremler verilecektir. Birimin kökleri kavramı incelenerek ve sonlu cisimler üzerinde tanımlı döngüsel polinomlar ele alınmıştır.

Üçüncü bölümde sonlu cisimler üzerinde polinomlar ele alınmıştır. Bu polinomların mertebeleri ve özellikleri üzerinde durulmuş ve ilkel polinom kavramı ele alınmıştır. Daha sonra sonlu cisimler üzerinde tanımlı monik indirgenemez polinomların sayısı bazı özel fonksiyonlar yardımıyla ifade edilmiştir.

Dördüncü bölümde sonlu cisimlerin bir uygulaması olarak sonlu cisimler üzerinde eliptik eğriler ele alınmış ve sonlu cisimler üzerinde tanımlı eliptik eğriler üzerindeki noktaların belirlenmesi üzerinde durulmuştur.

Anahtar Kelimeler: Sonlu cisimler, sonlu cisimler üzerinde tanımlı polinomlar, eliptik eğriler.

2017, vii + 82 sayfa.

ABSTRACT

MSc Thesis

FINITE FIELDS and THEIR APPLICATIONS

Ayşe KESKİN

Uludağ University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Doç. Dr. Betül GEZER

In this work, properties of finite fields and applications of finite fields over elliptic curves are discussed.

In the first chapter, some fundamental definitions and theorems which will be used in the work are given.

In the second chapter, the algebraic properties of the finite fields are discussed. It is proposed that, for every prime p and $n \in \mathbb{N}$ there is an irreducable polynomial over $\mathbb{F}_p[x]$. Then, Galois groups are discussed by analysing the roots of irreducable polynomials. Trace, norm and base terms for finite fields are handled and some theorems are given about these terms. By analysing the roots of unity, cyclotomic polynomials over finite fields are scrutinized.

In the third chapter, polynomials over finite fields are handled. The orders and properties of these polynomials are elaborated and primitive polynomials are discussed. Then, the number of monic irreducible polynomials over finite fields are expressed by the help of some special functions.

In the last chapter, as an application of the finite fields, elliptic curves over finite fields are handled and identification of the points of the elliptic curves over finite fields is emphasized.

Key words: Finite fields, polynomials over finite fields, elliptic curves.

2017, vii + 82 pages.

TEŞEKKÜR

Yüksek lisans çalışmam esnasında sahip olduğu bilgi ve tecrübelerini benimle paylaşan ve her zaman bana destek olan değerli danışman hocam Doç. Dr. Betül GEZER'e teşekkürlerimi sunarım.

Ayşe KESKİN
01/06/2017

İÇİNDEKİLER

Sayfa

SİMGELER DİZİNİ

Simgeler	**Açıklama**
N, Z, Q, R	Doğal sayılar, tamsayılar, rasyonel sayılar, gerçel sayılar kümeleri
$\|A\|$	A kümesinin kardinalitesi
$\text{Ker}(\varphi)$	φ homomorfizminin çekirdeği
$[G : H]$	H alt grubunun G grubu içindeki indeksi
$\text{kar}(R)$	R halkasının karakteristiği
$\text{der}(f)$	f polinomunun derecesi
$\Phi_p(x)$	p. dairesel polinom
$[E : F]$	E cisminin F üzerindeki derecesi

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1. ÖN BİLGİLER

Bu bölümde çalışmada kullanılacak olan bazı kavramlar ve teoremler ele alınacaktır. Kısım 1.1. de gruplar ve halkalarla ilgili bazı temel kavramlar ele alınacak, Kısım 1.2. de ise cisim ve cisim genişlemeleri kavramları üzerinde durulacak ve bazı önemli teoremler verilecektir.

1.1. Gruplar ve Halkalar

G bir grup olmak üzere bir $a \in G$ elemanının tüm kuvvetlerinden oluşan alt gruba a elemanı ile üretilen *devirli alt grup* adı verilir ve bu alt grup $\langle a \rangle$ ile gösterilir. Eğer $\langle a \rangle = G$ ise G grubuna a elemanı ile üretilen *devirli grup* denir. Devirli grupların alt grupları ve elemanların mertebelerini belirlemek oldukça kolaydır. Aşağıda devirli grupların alt gruplarının mertebeleri, elemanları ve üreteçleri ilgili bir teorem verilmektedir.

1.1.1. Teorem. *G*, mertebesi m olan ve $a \in G$ ile üretilen bir sonlu devirli grup olsun. Bu durumda

***i*)** G grubunun a^k elemanının ürettiği alt grubun mertebesi $m/(k, m)$ dir.

***iii*)** k pozitif tamsayısı, m sayısının bir böleni ise G grubunun indeksi k olan sadece bir tek alt grubu vardır. m sayısının herhangi bir pozitif l böleni için G grubunun tam olarak bir tane l mertebeli alt grubu vardır.

***iv*)** k pozitif tamsayısı, m sayısının bir böleni ise G grubunun k mertebeli $\phi(k)$ tane elemanı vardır. Burada $\phi(k)$, Euler ϕ fonksiyonunu belirtmektedir.

***v*)** G grubunun $\phi(m)$ tane üreteci vardır ve bu üreteçler $(r, m) = 1$ olmak üzere a^r elemanının kuvvetleridirler (Fraleigh 2003).

Grup teorisinde işlem koruyan yapılar oldukça önemli bir yere sahiptirler. Hatırlanacağı gibi, G ve H iki grup olmak üzere $f : G \to H$ dönüşümü her $a, b \in G$ için

$$f(ab) = f(a)f(b)$$

eşitliğini gerçekliyor ise f dönüşümüne G grubundan H grubuna bir *homomorfizm* adı verilir. Eğer f örten ise f homomorfizmine bir *epimorfizm*, H grubuna ise G grubunun bir *homomorfik görüntüsü* denir. Bir G grubundan kendi üzerine olan bir homomorfizme

bir *endomorfizm* denir. Eğer f birebir ve örten ise f homomorfizmine bir *izomorfizm* denir, bu halde G ve H *grupları izomortur* denir ve $G \cong H$ ile gösterilir. Bir G grubundan kendi üzerine bir izomorfizme bir *otomorfizm* denir. Bundan başka e', H grubunun etkisiz elemanı olmak üzere

$$\{g \in G \mid f(g) = e'\}$$

kümesine f homomorfizminin *çekirdeği* denir ve Ker(f) ile gösterilir.

Aşağıda grup teorisinin temel teoremlerinden birisi olan Homomorfizmin Temel Teoremi olarak ta bilinen Birinci İzomorfizm Teoremi verilmektedir.

1.1.2. Teorem. G ve H iki grup ve $f : G \to H$ bir homomorfizm ise $G/\text{Ker}(f) \cong f(G)$ dir (Fraleigh 2003).

Şimdi halkalar teorisi ile ilgili bazı temel kavramlar ve teoremler ele alınacaktır. Bu çalışmada bir R halkasının toplama işlemine göre etkisiz elemanı "0" ile çarpma işlemine göre etkisiz elemanı ise "1" ile belirtilecektir. Ayrıca R bir halka, $r \in R$ ve $n \in \mathbb{N}$ olmak üzere $n \cdot r$ çarpımı

$$n \cdot r = \underbrace{r + r + \ldots + r}_{n \text{ tan } e}$$

olduğunu belirtmektedir.

Aşağıda her $r \in R$ için $n \cdot r = 0$ olacak biçimde bir $n \in \mathbb{N}$ sayısının varlığı ile ilgilenilecektir.

1.1.3. Tanım. R bir halka olmak üzere, her $r \in R$ için, $n \cdot r = 0$ olacak biçimde bir n pozitif tamsayısı varsa bu şekildeki pozitif tamsayıların en küçüğüne R halkasının *karakteristiği* denir. Bu şekilde bir pozitif tamsayı yoksa R halkasının karakteristiği 0 olarak alınır.

Bu tanıma göre, $\mathbb{Z}$ ve $\mathbb{Q}$ halkalarının karakteristiği 0, $\mathbb{Z}_p$ halkasının karakteristiği ise p dir. Bu çalışmada bir R halkasının karakteristiği kar(R) ile gösterilecektir.

Aşağıdaki teoremde birim elemanlı, sıfır bölensiz ve karakteristiği bir $n \in \mathbb{N}$ olan halkaların karakteristiğinin bir asal sayı olduğu belirtilmektedir.

1.1.4. Teorem. *R*, sıfır bölensiz birimli ve birimi $1 \neq 0$ olan bir halka olmak üzere *R* halkasının karakteristiği $n > 1$ olsun. Bu durumda *n* bir asal sayıdır (Hungerford 1974).

Bu teoremin bir sonucu olarak her sonlu cismin karakteristiğinin bir asal sayı olduğu elde edilir.

1.1.5. Sonuç. Sonlu bir cismin karakteristiği bir asal sayıdır (Hungerford 1974).

Aşağıda karakteristiği bir asal sayı olan değişmeli halkalarla ilgili oldukça önemli bir teorem verilecektir.

1.1.6. Teorem. *R*, karakteristiği *p* asal sayısı olan değişmeli bir halka olsun. Bu durumda her $a, b \in R$ ve $n \in \mathbb{N}$ için

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

dır (Hungerford 1974).

Halkalar, iki tane ikili işleme sahip olan cebirsel yapılardır ve halkalar teorisinde de grup homomorfizmi gibi işlem koruyan dönüşümler vardır. Halkalar için iki tane ikili işlem tanımlı olduğundan bu işlemlerin ikisi de halka homomorfizmi altında korunur. Buna göre, *R* ve *S* iki halka olmak üzere $f : R \to S$ dönüşümü her $a, b \in R$ için

$$f(a + b) = f(a) + f(b)$$
$$f(ab) = f(a)f(b)$$

eşitliklerini gerçekliyorsa *f* dönüşümüne bir *halka homomorfizmi* denir. Eğer *f* örten bir dönüşüm ise *f* homomorfizmine bir *halka epimorfizmi*, *R* halkasndan kendi üzerine olan bir homomorfizme bir *halka endomorfizmi* denir. Eğer *f*, birebir ve örten ise *f* homomorfizmine bir *halka izomorfizmi* denir. Bir *R* halkasından kendi üzerine bir

izomorfizme ise bir *halka otomorfizmi* denir. Ayrıca, $f : R \to S$ bir halka homomorfizmi olmak üzere

$$\{r \in R \mid f(r) = 0'\}$$

kümesine f homomorfizminin *çekirdeği* denir ve Ker(f) ile gösterilir.

Daha önce gruplar için verilen Birinci İzomorfizm Teoremi halkalar için de verilebilir.

1.1.7. Teorem. R ve S iki halka ve $f : R \to S$ bir halka homomorfizm ise $R/\text{Ker}(f) \cong f(R)$ dir (Fraleigh 2003).

Aşağıdaki teoremde cisim teorisinde önemli bir yere sahip olan adına *Frobenius otomorfizmi* adı verilen özel bir otomorfizminin varlığı belirtilmektedir.

1.1.8. Teorem. F, karakteristiği p olan bir sonlu cisim ve $a \in F$ olmak üzere

$$\phi_p : F \to F, \quad \phi_p(a) = a^p$$

olarak tanımlanan ϕ_p dönüşümü bir otomorfizmdir (Fraleigh 2003).

Halkalar teorisinde özel bir alt halka olan idealler önemli bir yere sahiptir. İdealler yardımıyla yeni halkalar elde edilebilir. Hatırlanacağı gibi, R bir halka ve I, R halkasının boş olmayan bir alt kümesi olmak üzere I kümesi, her $i, j \in I$ ve $r \in R$ için $i - j \in I$, $ri \in I$ ve $ir \in I$ koşullarını gerçekliyor ise I kümesine R halkasının bir *ideali* adı verilir.

Adlarına asal ve maksimal ideal denilen idealler yardımıyla elde edilen bölüm halkaları bir tamlık bölgesi veya bir cisim olabilir. R bir halka, $I \neq R$ ve I, R halkasının bir ideali olsun. Eğer $a, b \in R$ için $ab \in I$ olduğunda $a \in I$ veya $b \in I$ oluyorsa I idealine R halkasının bir *asal ideali* denir. Eğer R halkasının $I \neq R$ idealini bulunduran I ve R ideallerinden başka bir ideali yoksa I idealine R halkasının *maksimal ideali* denir.

Aşağıdaki teoremde maksimal ve asal idealler yardımıyla sırasıyla bir halkadan cisim ve tamlık bölgesi elde edilebileceği görülmektedir.

1.1.9. Teorem. R birimli değişmeli bir halka ve I, R halkasının bir ideali olsun. Bu durumda

***i*)** I idealinin bir maksimal ideal olması için gerek ve yeter koşul R/I halkasının bir cisim olmasıdır,

***ii*)** I idealinin bir asal ideal olması için gerek ve yeter koşul R/I halkasının bir tamlık bölgesi olmasıdır (Gezer ve Bizim 2017).

Hatırlanacağı gibi, bir R tamlık bölgesinin her I ideali bir $a \in I$ elemanı ile üretiliyorsa, yani R tamlık bölgesinin her I ideali için

$$I = \langle a \rangle = \{ra \mid r \in R\}$$

olacak biçimde bir $a \in I$ varsa R tamlık bölgesine *temel ideal bölgesi* adı verilir. F bir cisim olmak üzere $F[x]$ halkası bir temel ideal bölgesidir, yani $F[x]$ halkasının her I ideali için $I = \langle f(x) \rangle$ olacak biçimde tek türlü belirli bir monik $f(x) \in F[x]$ polinomu vardır.

1.1.10. Teorem. F bir cisim olmak üzere $F[x]$ halkasının $\langle f(x) \rangle$ idealinin bir maksimal ideal olması için gerek ve yeter koşul $f(x)$ polinomunun F cismi üzerinde indirgenemez olmasıdır (Gezer ve Bizim 2017).

Bu teoreme dikkat edilirse, F bir cisim olmak üzere $F[x]$ halkasında indirgenemez olan bir $f(x)$ polinomu ile üretilen $\langle f(x) \rangle$ ideali yardımıyla bir cisim elde edilebilir. Örneğin, $x^2 - 2 \in \mathbb{Q}[x]$ polinomu $\mathbb{Q}$ cismi üzerinde indirgenemez olduğundan $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$ bölüm halkası bir cisimdir.

Bu kısımda son olarak bir polinomun bir kökünün katlılığı kavramı ile ilgilenilecektir. F bir cisim, $f(x) \in F[x]$ sabit olmayan bir polinom ve $c \in F$ olmak üzere $f(c) = 0$ ise c elemanına $f(x)$ polinomunun bir *kökü* (*sıfırı*) denir. Eğer $f(c) = 0$ ve $(x - c)^k \mid f(x)$ ancak $(x - c)^{k+1} \nmid f(x)$ ise c elemanına $f(x)$ polinomunun bir *k katlı kökü* denir. Bundan başka $k = 1$ ise c elemanına $f(x)$ polinomunun bir *basit kökü*, $k > 1$ ise c elemanına $f(x)$ polinomunun bir *katlı kökü*dür denir.

1.1.11. Teorem. F bir cisim, $f(x) \in F[x]$ sabit olmayan bir polinom ve $f'(x)$, $f(x)$ polinomunun formal türevi olsun. Bu durumda

i) $c \in F$ elemanının $f(x) \in F[x]$ polinomunun bir kökü olması için gerek ve yeter koşul $(x - c) \mid f(x)$ olmasıdır.

ii) $c \in F$ elemanının $f(x) \in F[x]$ polinomunun bir katlı kökü olması için gerek ve yeter koşul $c \in F$ elemanının $f(x)$ ve $f'(x)$ polinomlarının kökü olmasıdır (Herstein 1999).

1.2 Cisim Genişlemeleri

Hatırlanacağı gibi, E bir cisim ve $F \subset E$ olmak üzere F, E cisminden indirgenen işlemlere göre bir cisim ise F cismine E cisminin bir *alt cismi*, E cismine ise F cisminin bir *cisim genişlemesi* denir ve $F \leq E$ ile gösterilir. Bundan başka E, F cisminin bir cisim genişlemesi ise E, F cismi üzerinde bir vektör uzayıdır ve E cisminin F cismi üzerindeki boyutuna E cisminin F cismi üzerindeki *derecesi* denir, $[E : F]$ ile gösterilir. Eğer $[E : F]$ sonlu ise E cismine F cisminin bir *sonlu cisim genişlemesi*, sonsuz ise bir *sonsuz cisim genişlemesi* denir.

Aşağıdaki teoremde E, F cisminin ve K, E cisminin birer sonlu genişlemesi ise K cisminin F cisminin bir sonlu genişlemesi olduğu verilmektedir.

1.2.1. Teorem. E, F cisminin ve K, E cisminin birer sonlu genişlemesi ise K, F cisminin bir sonlu genişlemesidir. Üstelik

$$[K : F] = [K : E][E : F]$$

dir (Gezer ve Bizim 2017).

F ve E, $F \leq E$ özelliğinde iki cisim olmak üzere E cisminin her elemanı F üzerinde bir cebirsel eleman ise E cismine F cisminin bir *cebirsel cisim genişlemesi* denir. Bundan başka her sonlu cisim genişlemesi bir cebirsel cisim genişlemesidir.

Cisim genişlemesi kavramı, polinomların köklerinin bulunması problemi ile ortaya çıkmıştır. Kronecker Teoremi olarak bilinen aşağıdaki teoreme göre, sabit olmayan her bir polinomun bir kökünün bulunduğu bir cisim genişlemesi vardır.

1.2.2. Teorem (Kronecker Teoremi). F bir cisim ve $f(x) \in F[x]$ sabit olmayan bir polinom ise $f(\alpha) = 0$ ve $\alpha \in E$ olacak biçimde F cisminin bir E cisim genişlemesi vardır (Gezer ve Bizim 2017).

1.2.3. Tanım. F bir cisim ve E, F cisminin bir cisim genişlemesi olmak üzere $\alpha \in E$, F cismi üzerinde bir cebirsel eleman olsun.

$$I = \{f(x) \in F[x] \mid f(\alpha) = 0\}$$

idealini üreten tek türlü belirli monik $f(x) \in F[x]$ polinomuna α elemanının F cismi üzerindeki *minimal polinomu* (*indirgenemez polinomu*), $f(x)$ polinomunun derecesine de α elemanının F cismi üzerindeki *derecesi* denir.

Aşağıdaki teoremde bir cebirsel elemanın minimal polinomunun özellikleri belirtilmektedir.

1.2.4. Teorem. F bir cisim E, F cisminin bir cisim genişlemesi ve $\alpha \in E$, F cismi üzerinde bir cebirsel eleman olmak üzere α elemanının F cismi üzerindeki minimal polinomu $f(x)$ olsun. Bu durumda

i) $f(x)$ polinomu $F[x]$ halkasında indirgenemezdir.

ii) $g(x) \in F[x]$ polinomu için $g(\alpha) = 0$ ise $f(x) \mid g(x)$ dır.

iii) $f(x)$ polinomu $F[x]$ halkasında α elemanını kök olarak bulunduran en küçük dereceli polinomdur (Hungerford 1974)

E, F cisminin bir cisim genişlemesi olmak üzere belli bir $\alpha \in E$ için $E = F(\alpha)$ ise E cismine F cisminin bir *basit genişlemesi* adı verilir. Eğer $\alpha \in E$, F cismi üzerinde bir cebirsel eleman ise $F(\alpha)$ basit cisim genişlemesinin elemanları, α elemanının F cismi üzerindeki indirgenemez polinomunun derecesi kullanılarak ifade edilebilir. Buna göre α elemanının F cismi üzerindeki indirgenemez polinomunun derecesi n ise $E = F(\alpha)$ cisminin her β elemanı $c_i \in F$ olmak üzere

$$\beta = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}$$

olarak ifade edilir.

Cisim teorisinde bir $f(x) \in F[x]$ polinomunun lineer çarpanlarına ayrıldığı halkayı belirlemek oldukça önemlidir.

1.2.5. Tanım. F bir cisim ve $F \leq E$ olmak üzere $f(x)$ polinomu $E[x]$ halkasında lineer çarpanlarına ayrılabiliyorsa $f(x)$ polinomu $E[x]$ halkasında (E cismi üzerinde) *parçalanır* denir. Eğer $f(x)$ polinomu E cismi üzerinde parçalanır ve $\alpha_1, \ldots, \alpha_n \in E$, $f(x)$ polinomunun kökleri olmak üzere $E = F(\alpha_1, \ldots, \alpha_n)$ ise E cismine $f(x)$ polinomunun F cismi üzerindeki *parçalanma cismi* denir.

1.2.6. Uyarı 1. Tanıma dikkat edilirse, bir $f(x)$ polinomunun parçalanma cismi bu polinomun köklerini bulunduran minimal cisimdir. Örneğin, $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ polinomunun kökleri $\sqrt{2}$ ve $-\sqrt{2}$ olduğundan $f(x)$ polinomunun $\mathbb{Q}$ cismi üzerindeki parçalanma cismi $\mathbb{Q}(\sqrt{2})$ dir.

2. Sabit olmayan her polinomun bir parçalanma cismi vardır ve üstelik bir polinomun parçalanma cismi izomorfizme bağlı olarak bir tektir.

Cisim teorisinde, ayrılabilir ve ayrılamaz cisim genişlemeleri de oldukça önemlidir.

1.2.7. Tanım. F bir cisim $f(x) \in F[x]$, F cismi üzerinde indirgenemez polinom olmak üzere $f(x)$ polinomunun parçalanma cismindeki her kökü bir basit kök ise $f(x)$ polinomuna F cismi üzerinde bir *ayrılabilir polinom*, $f(x)$ polinomu ayrılabilir değilse $f(x)$ polinomuna F cismi üzerinde bir *ayrılamaz polinom* denir.

F bir cisim, E, F cisminin bir cisim genişlemesi ve $\alpha \in E$, F cismi üzerinde bir cebirsel eleman olmak üzere α elemanının F cismi üzerindeki minimal polinomu F cismi üzerinde bir ayrılabilir polinom (ayrılamaz polinom) ise α elemanına F cismi üzerinde bir *ayrılabilir eleman* (*ayrılamaz eleman*) denir. Eğer E cisminin her elemanı F cismi üzerinde bir ayrılabilir eleman (ayrılamaz eleman) ise E cismine F cisminin bir *ayrılabilir genişlemesi* (*ayrılamaz genişlemesi*) denir.

Bu tanıma göre, $x^2 - 2 \in \mathbb{Q}[x]$ polinomu $\mathbb{Q}(\sqrt{2})[x]$ halkasında $(x + \sqrt{2})(x - \sqrt{2})$ olarak yazılabildiğinden $x^2 - 2$ bir ayrılabilir polinomdur ve $\mathbb{Q}(\sqrt{2})$ cismi $\mathbb{Q}$ cisminin bir ayrılabilir genişlemesidir.

Bu kısımda son olarak Galois genişlemesi kavramı ele alınacaktır.

1.2.8. Tanım. *F* bir cisim, *E*, *F* cisminin bir cebirsel genişlemesi olmak üzere *E* cisminde bir kökü olan *F*[*x*] halkasındaki her indirgenemez polinom *E* cismi üzerinde parçalanırsa *E* cismine *F* cisminin bir *normal cisim genişlemesi* denir. Eğer *E* cismi *F* cisminin bir sonlu ayrılabilir normal genişlemesi ise *E* cismine *F* cisminin bir *Galois genişlemesi* ve *G*(*E*/*F*) grubuna da *E* cisminin *F* cismi üzerindeki *Galois grubu* denir.

Örneğin, $\mathbb{Q}(\sqrt{2})$ cismi $\mathbb{Q}$ cisminin bir sonlu ayrılabilir normal genişlemesi olduğundan $\mathbb{Q}(\sqrt{2})$ cismi $\mathbb{Q}$ cisminin bir Galois genişlemesidir.

2. SONLU CİSİMLERİN CEBİRSEL YAPISI

Bu bölümde sonlu cisimlerin cebirsel yapısı ve temel özellikleri ele alınacaktır. Kısım 2.1. de sonlu cisimlerin temel özellikleri ile ilgilenilecek ve her p asal sayısı ve her $n \in \mathbb{N}$ sayısı için p^n mertebeli bir sonlu cismin var olduğu görülecektir. Bundan başka, $\mathbb{F}_p[x]$ halkasında istenen her dereceye sahip bir indirgenmez polinomun varlığı ele alınacaktır. Kısım 2.2. de indirgenemez polinomların kökleri ele alınarak sonlu cisimlerin Galois grupları ele alınacak ve bu grupların devirli olduğu ve doğal (kanonik) bir üretecinin olduğu görülecektir. Kısım 2.3. de sonlu cisimler için iz, norm ve baz kavramları ele alınacak ve bunlarla ilgili bazı teoremler verilecektir. Kısım 2.4. de birimin kökleri kavramı incelenecek ve sonlu cisimler üzerinde tanımlı döngüsel polinomlar ele alınacaktır. Kısım 2.5. de sonlu cisimlerin elemanlarının üç farklı gösterimi belirlenecektir.

p bir asal sayı olmak üzere p modülüne göre tamsayıların kümesi $\mathbb{Z}_p$, bilinen en basit sonlu cisimdir. Bununla birlikte $\mathbb{Z}_p$ cisminin birçok özelliği keyfi sonlu cisimlere de genişletilebilir. Daha önceki bölümde $\mathbb{Z}_p$ sonlu cismi ile p mertebeli $\mathbb{F}_p$ Galois cismi özdeşlenmişti. Bu çalışmada, p bir asal sayı olmak üzere p mertebeli bir sonlu cisim $\mathbb{F}_p$ ve q mertebeli bir sonlu cisim $\mathbb{F}_q$ ile gösterilecektir.

2.1 Sonlu Cisimlerin Temel Özellikleri

Bu kısımda ilk olarak polinomlar yardımıyla sonlu cisimler oluşturulacaktır. Hatırlanacağı gibi, F bir cisim ve $p(x) \in F[x]$ olmak üzere $p(x)$ polinomu $F[x]$ halkası üzerinde monik indirgenemez bir polinom ise $F[x]/\langle p(x)\rangle$ bölüm halkası bir cisimdir. O halde derecesi n olan $p(x) \in \mathbb{F}_p[x]$ monik indirgenemez polinomu yardımıyla $q = p^n$ mertebeli $\mathbb{F}_q$ sonlu cismi oluşturulabilir ve üstelik

$$\mathbb{F}_q \cong \mathbb{F}_p[x]/\langle p(x)\rangle$$

dir.

Aşağıdaki teoremde $p(x) \in \mathsf{F}_p[x]$ derecesi n olan monik indirgenemez polinomu yardımıyla oluşturulan $\mathsf{F}_p[x]/\langle p(x)\rangle$ cisminin $q = p^n$ mertebeli bir sonlu cisim olduğu görülmektedir.

2.1.1 Teorem. p bir asal sayı, $p(x) \in \mathsf{F}_p[x]$ derecesi n olan monik indirgenemez bir polinom olsun. Bu durumda $\mathsf{F}_p[x]/\langle p(x)\rangle$ bölüm halkası $q = p^n$ mertebeli sonlu bir cisimdir (Conrad 2013).

İspat. $\mathsf{F}_p[x]/\langle p(x)\rangle$ bölüm halkasının elemanları $\mathsf{F}_p[x]$ de

$$\text{“}f(x) \equiv g(x) \pmod{\langle p(x)\rangle} \Leftrightarrow f(x) - g(x) \in \pmod{\langle p(x)\rangle}\text{”}$$

ile tanımlanan denklik sınıflarıdır. Ayrıca

“$f(x) \equiv g(x) \pmod{\langle p(x)\rangle} \Leftrightarrow f(x)$ ve $g(x)$, $p(x)$ ile bölündüğünde kalanlar aynıdır”

olduğundan $\mathsf{F}_p[x]/\langle p(x)\rangle$ in her elemanı derecesi $p(x)$ den daha küçük olan bir polinom bulundurur, böylece $a_0, a_1, ..., a_{n-1} \in \mathsf{F}_p$ olmak üzere $\mathsf{F}_p[x]/\langle p(x)\rangle$ bölüm halkasının farklı elemanları kesin olarak

$$a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + \langle p(x)\rangle$$

biçimindedir. Üstelik her bir a_i katsayısı için p farklı seçim söz konusu olduğundan bu özellikteki elemanların sayısı p^n dir. Diğer yandan $p(x) \in \mathsf{F}_p[x]$ monik indirgenemez bir polinom olduğundan $\langle p(x)\rangle$ ideali maksimal idealdir ve böylece $\mathsf{F}_p[x]/\langle p(x)\rangle$ bir cisimdir. Dolayıyla $\mathsf{F}_p[x]/\langle p(x)\rangle$, p^n mertebeli bir sonlu cisimdir.

2.1.2 Uyarı. Yukarıdaki teoreme göre derecesi n olan $p(x) \in \mathsf{F}_p[x]$ monik indirgenemez polinomu yardımıyla $q = p^n$ mertebeli sonlu bir cisim oluşturulabilir, daha sonra her sonlu cismin belli bir p asal sayısı ve belli bir monik indirgenmez $p(x)$ polinomu için $\mathsf{F}_p[x]/\langle p(x)\rangle$ ye izomorf olduğu görülecektir. Dolayısıyla bu izomorfizm yardımıyla herhangi bir sonlu cisim yapısı çalışılabilir. Bununla birlikte her sonlu cismin $\mathsf{F}_p[x]/\langle p(x)\rangle$ biçiminde olmadığı da açıktır. Örneğin, $\mathsf{Z}[i]/\langle 7\rangle$ bölüm halkası $\mathsf{Z}_7[x]/\langle x^2 + 1\rangle$ cismine izomorf 49 elemanlı bir cisimdir.

2.1.3 Örnek. $p(x) = x^2 + x + 1 \in \mathsf{Z}_2[x]$ polinomu $\mathsf{Z}_2[x]$ halkası üzerinde indirgenemezdir. Gerçekten de $p(0)$, $p(1) \neq 0$ dır. Böylece $\mathsf{Z}_2[x]/\langle x^2 + x + 1\rangle$ bölüm halkası bir cisimdir ve $I = \langle x^2 + x + 1\rangle$ olmak üzere

$$\mathsf{Z}_2[x]/\langle x^2 + x + 1\rangle = \{a_0 + a_1x + I \mid a_0, a_1 \in \mathsf{Z}_2\}$$

biçimindedir. O halde $\mathsf{Z}_2[x]/\langle x^2 + x + 1\rangle$ in elemanları I, $1 + I$, $x + I$, $1 + x + I$ dır. Bu cismin cisim tabloları aşağıda görülmektedir.

Çizelge 2.1. $\mathsf{Z}_2[x]/\langle x^2 + x + 1\rangle$ cisminin işlem tablosu

+	I	$1 + I$	$x + I$	$1 + x + I$
I	I	$1 + I$	$x + I$	$1 + x + I$
$1 + I$	$1 + I$	I	$1 + x+I$	$X + I$
$x + I$	$x + I$	$1 + x + I$	I	$1 + I$
$1 + x + I$	$1 + x + I$	$x + I$	$1 + I$	I

·	I	$1 + I$	$x + I$	$1 + x + I$
I	I	I	I	I
$1 + I$	I	$1 + I$	$x + I$	$x + 1 + I$
$x + I$	I	$x + I$	$x + 1 + I$	$1 + I$
$1 + x + I$	I	$x + 1 + I$	$1 + I$	$x + I$

Bu tabloya göre, örneğin,

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

ve

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

dir.

Bu kısımda ilk olarak her sonlu cismin mertebesinin bir asal sayının kuvveti olduğu görülecektir. Hatırlanacağı gibi, F bir cisim ve $\text{kar}(F) = n$ ise $n = 0$ veya p bir asal sayı olmak üzere $n = p$ dir. Diğer yandan, $\text{kar}(F) = 0$ ise F cisminin Z halkasına izomorf bir

alt halkası ve dolayısıyla $\mathbb{Q}$ cismine izomorf bir alt cismi vardır. Eğer kar(F) = p ise F cisminin $\mathbb{F}_p$ cismine izomorf bir alt cismi vardır. Gerçektende

$$\phi : \mathbb{Z} \to F,\ \phi(x) = x \cdot 1_F$$

olarak tanımlanan ϕ dönüşümü bir halka homomorfizmidir. Üstelik bu dönüşümün çekirdeği, kar(F) = 0 ise

$$\text{Ker}(\phi) = \{x \in \mathbb{Z} | \phi(x) = 0_F\} = \{0\}$$

ve kar(F) = p ise

$$\text{Ker}(\phi) = \{x \in \mathbb{Z} | \phi(x) = 0_F\} = \{x \in \mathbb{Z} |\ x \cdot 1_F = 0_F\} = \{x \in \mathbb{Z} |\ x = pt,\ t \in \mathbb{Z}\} = p\mathbb{Z}$$

dır. O halde Birinci İzomorfizm Teoremi gereği, sırasıyla

$$\mathbb{Z}/\{0\} \cong \phi(\mathbb{Z}) \text{ ve } \mathbb{Z}/p\mathbb{Z} \cong \phi(\mathbb{Z})$$

dir. O halde kar(F) = 0 özelliğindeki cisimler $\mathbb{Z}$ ye izomorf bir alt halka ve dolayısıyla $\mathbb{Q}$ cismine izomorf bir alt cisim, kar(F) = p özelliğindeki cisimler ise $\mathbb{F}_p$ cismine izomorf bir alt halka ve dolayısıyla $\mathbb{F}_p$ cismine izomorf bir alt cisim bulundurur. Dolayısıyla her bir sonlu cisim, $\mathbb{F}_p$ cisminin bir cisim genişlemesi olarak düşünülebilir. Bu sonuç ile birlikte, her sonlu cismin mertebesinin bir asal sayının kuvveti olduğu görülebilir.

2.1.4. Teorem. F bir sonlu cisim ve kar(F) = p ise F cisminin mertebesi belli bir $n \in \mathbb{N}$ sayısı için $q = p^n$ dir (Fraleigh 2003).

İspat. F bir sonlu cisim olduğundan F cisminin $\mathbb{F}_p$ cismine izomorf bir K asal alt cismi vardır. Üstelik F cismi sonlu olduğundan, F, K alt cismi üzerinde sonlu boyutlu bir vektör uzayıdır. O halde [F : K] = n olacak biçimde belli bir $n \in \mathbb{N}$ sayısı vardır. Eğer F cisminin bir K-bazı $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ ise $c_1, c_2, \ldots, c_n \in K$ olmak üzere her $\beta \in F$ elemanı

$$\beta = c_1\alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n$$

biçiminde tek türlü yazılabilir. Ayrıca K cismi $\mathbb{F}_p$ cismine izomorf olduğundan K cisminin p tane elemanı vardır. Dolayısıyla $1 \le i \le n$ olmak üzere her bir c_i için p farklı seçim olduğundan F nin eleman sayısı p^n dir.

2.1.5. Teorem. F_q sonlu bir cisim ise $\mathsf{F}_q^* = \mathsf{F}_q \setminus \{0\}$ çarpımsal grubu devirli bir gruptur (Conrad 2013).

İspat. m, F_q^* abelyen grubundaki elemanların mertebelerinin en büyüğü olsun. Bir sonlu abelyen grupta tüm elemanların mertebesi en büyük mertebeli elemanın mertebesini böleceğinden her $t \in \mathsf{F}_q^*$ için $t^m = 1$ dir. Böylece F_q^* grubunun tüm elemanları $x^m - 1$ polinomunun birer köküdür. Bir cisimde bir polinomun en fazla derecesi kadar kökü var olduğundan $x^m - 1$ polinomunun F_q cisminde $q - 1$ tane kökü vardır. Dolayısıyla $m \geq q - 1$ dir. Diğer yandan m, F_q^* grubundaki bir elemanın mertebesi olduğundan m, F_q^* grubunun mertebesi olan $q - 1$ sayısını böler. O halde $m \leq q - 1$ dir. Böylece $m = q - 1$ olduğu sonucu elde edilir. Bu ise F_q^* grubunda $q - 1$ mertebeli elemanların var olduğunu gösterir, yani F_q^* grubu devirlidir.

Sonlu cisimlerin bu özelliği özellikle sonlu cisimlerin uygulamalarında oldukça önemlidir. Aşağıda F_q^*, devirli grubunun üretecine özel bir isim verilecektir.

2.1.6. Tanım. F_q^* devirli grubunu üreten $\zeta \in \mathsf{F}_q^*$ elemanına F_q sonlu cisminin bir *ilkel elemanı* denir.

ζ, F_q sonlu cisminin bir ilkel elemanı olsun. Bu durumda $\zeta^k \in \mathsf{F}_q^*$ elemanının bir ilkel eleman olması için gerek ve yeter koşul $(k, q - 1) = 1$ olmasıdır. Dolayısıyla ϕ, Euler fonksiyonunu olmak üzere F_q cisminde $\phi(q - 1)$ tane ilkel eleman vardır.

Teorem 2.1.5. in bir sonucu olarak, bir sonlu cismin her sonlu cisim genişlemesinin bir basit genişleme olduğu görülebilir.

2.1.7. Sonuç. Bir sonlu cismin her sonlu genişlemesi bir basit genişlemedir (Asar ve ark. 2009).

İspat. F bir sonlu cisim E, F cisminin bir sonlu cisim genişlemesi ise $[E : F] = n$ olacak biçimde belli bir $n \geq 1$ tamsayısı vardır. F sonlu olduğun Teorem 2.1.4. gereği, $|E| = |F|^n$

dir. Dolayısıyla E cismi de sonludur. Diğer yandan E^* çarpımsal grubu devirli olduğundan $E^* = \langle\zeta\rangle$ olacak şekilde bir $\zeta \in E^*$ ilkel elemanı vardır. Dolayısıyla $F(\zeta) \subset E$ dır. Bundan başka, $F(\zeta)$, 0 elemanını ve ζ elemanlarının tüm kuvvetlerini bulundurduğundan E cisminin tüm elemanlarını bulundurur, yani,

$$E = E^* \cup \{0\} \subset F(\zeta)$$

dir. Dolayısıyla $E = F(\zeta)$ dır. Bu ise E cisminin F cisminin bir basit cisim genişlemesi olduğunu gösterir.

Teorem 2.1.5. in bir diğer önemli sonucu ise q elemanlı sonlu F cismindeki her $\alpha \in F$ elemanı için $\alpha^q = \alpha$ olmasıdır.

2.1.8. Sonuç. F, q elemanlı bir sonlu cisim ise her $\alpha \in F$ elemanı için $\alpha^q = \alpha$ dır (Lidl ve Neiderreiter 1986).

İspat. $\alpha = 0$ için eşitlik gerçeklenir. Diğer yandan $F^* = F\backslash\{0\}$ grubu, $q - 1$ mertebeli devirli bir grup olduğundan her $\alpha \in F^*$ için $\alpha^{q-1} = 1$ dir. Bu eşitliğin her iki yanı α ile çarpılırsa $\alpha^q = \alpha$ olduğu elde edilir.

Aşağıdaki teorem, $q = p^n$ mertebeli bir sonlu cisim var ise, bu sonlu cisim $p(x) \in \mathsf{F}_p[x]$ derecesi n olan monik indirgenmez bir polinom olmak üzere $\mathsf{F}_p[x]/\langle p(x)\rangle$ halkasına izomorf olduğunu göstermektedir.

2.1.9. Teorem. Her sonlu cisim belli bir p asal sayısı ve belli bir monik indirgenmez $p(x)$ polinomu için $\mathsf{F}_p[x]/\langle p(x)\rangle$ halkasına izomorftur (Conrad 2013).

İspat. F bir sonlu cisim olsun. Bu durumda F^* devirli bir gruptur, bu grubun bir üreteci $\alpha \in F^*$ olsun. Her $f(x) \in \mathsf{F}_p[x]$ ve her $a \in \mathsf{F}_p$ için

$$\phi_\alpha : \mathsf{F}_p[x] \to F,\ \phi_\alpha(a) = a \text{ ve } \phi_\alpha(f(x)) = f(\alpha)$$

olarak tanımlanan değer homomorfizmi örtendir. Gerçektende $\phi_\alpha(a) = a$ veya $r \geq 0$ için $\alpha^r \in F$ alınırsa $\alpha^r = \phi_\alpha(x^r)$ olacak şekilde bir x^r polinomu vardır, yani F cismindeki her eleman ya 0 dır ya da α nın bir kuvvetidir. ϕ_α örten olduğundan $\phi_\alpha(\mathsf{F}_p[x]) = F$ dir. O

halde halkalar için Birinci İzomorfizm Teoremi gereği, $\mathsf{F}_p[x]/\mathrm{Ker}(\phi_\alpha) \cong F$ olur. Bu ise $\mathrm{Ker}(\phi_\alpha)$ nın $\mathsf{F}_p[x]$ halkasının maksimal ideali olduğunu gösterir. $\mathsf{F}_p[x]$ halkasının bu maksimal ideali ise belli bir monik indirgenmez $p(x)$ polinomu ile üretilen $\langle p(x)\rangle$ idealidir, dolayısıyla $\mathsf{F}_p[x]/\langle p(x)\rangle \cong F$ olur.

2.1.10. Uyarı. Yukarıdaki teoremde geçen $\phi_\alpha : \mathsf{F}_p[x] \to F$ değer homomorfizmi dikkate alınırsa $\mathsf{F}_p[x]/\mathrm{Ker}(\phi_\alpha) \cong \phi_\alpha(\mathsf{F}_p[x])$ ve ϕ_α dönüşümü örten olduğundan $\phi_\alpha(\mathsf{F}_p[x]) = \mathsf{F}_p[\alpha] = F$ olduğu elde edilir. Üstelik F bir cisim olduğundan $\mathsf{F}_p[\alpha]$ halkası da bir cisimdir ve $\mathsf{F}_p[\alpha] = \mathsf{F}_p(\alpha)$ dır. Diğer yandan $\mathrm{Ker}(\phi_\alpha)$, $\mathsf{F}_p[x]$ halkasının maksimal ideali olduğundan bu ideal $p(\alpha) = 0$ olacak biçimdeki bir $p(x) \in \mathsf{F}_p[x]$ monik indirgenemez polinomu ile üretilen idealdir. Dolayısıyla $\mathsf{F}_p[x]/\langle p(x)\rangle \cong \mathsf{F}_p(\alpha)$ olduğu elde edilir.

Teorem 2.1.9. mertebesi bir asalın kuvveti olan tüm sonlu cisimlerin varlığını, yani p bir asal sayı ve $n \in \mathsf{N}$ olmak üzere p^n mertebeli bir sonlu cismin her zaman var olduğunu garanti etmez. Bu teorem, eğer p^n mertebeli bir sonlu cisim var ise, $p(x) \in \mathsf{F}_p[x]$ derecesi n olan monik indirgenmez bir polinom olmak üzere bu sonlu cismin $\mathsf{F}_p[x]/\langle p(x)\rangle$ bölüm halkasına izomorf olduğunu belirtir.

Herhangi bir sonlu cisim, eleman sayısına bağlı olarak bir polinomun parçalanma cismi olarak ifade edilebilir.

2.1.11. Teorem. $q = p^n$ mertebeli herhangi bir sonlu cisim, $x^q - x \in \mathsf{F}_p[x]$ polinomunun F_p cismi üzerindeki parçalanma cismidir (Conrad 2013).

İspat. F, $q = p^n$ mertebeli sonlu bir cisim olsun. Bu durumda F cisminin F_p cismine izomorf olan bir asal alt cismi vardır. F^*, $q - 1$ mertebeli devirli bir grup olduğundan her $\alpha \in F^*$ için $\alpha^{q-1} = 1$ ve böylece $\alpha^q = \alpha$ olur. Bu F cisminin her elemanının $x^q - x$ polinomunun bir kökü olduğunu gösterir. F bir cisim olduğundan bu polinomun en çok q tane kökü vardır. O halde F, $x^q - x$ polinomunun F_p üzerindeki parçalanma cismidir.

Hatırlanacağı gibi, F bir cisim olmak üzere F cisminin her sonlu genişlemesi bir ayrılabilir genişleme ise F cismine *mükemmel cisim* denir. Teorem 2.1.11. kullanılarak her sonlu cismin bir mükemmel cisim olduğu görülebilir.

2.1.12. Sonuç. Her sonlu cisim mükemmeldir (Asar ve ark. 2009).

İspat. F bir sonlu cisim ve kar(F) = p olmak üzere $\mathsf{F}_p \leq F$ olsun. Bu durumda F cisminin mertebesi $q = p^n$ olacak biçimde belli bir $n \geq 1$ tamsayısı vardır. Eğer E, F cisminin sonlu bir cisim genişlemesi ise $[E : F] = r$ olacak biçimde belli bir $r \geq 1$ tamsayısı vardır. O halde E cisminin mertebesi q^r dir. Diğer yandan Teorem 2.1.5. gereği, E cisminin her elemanı $x^{q^r} - x \in \mathsf{F}_p[x]$ polinomunun bir sıfırıdır. Diğer yandan

$$(x^{q^r} - x)' = q^r x^{q^r-1} - 1 = -1$$

olduğundan $x^{q^r} - x$ polinomunun tüm köklerinin katlılığı 1 dir ve dolayısıyla F_p üzerinde ayrılabilirdir. Böylece E cisminin her elemanı F üzerinde ayrılabilir olduğundan E, F cisminin bir ayrılabilir genişlemesidir.

Aşağıdaki teoremde parçalanma cisimleri kullanılarak her p asal sayısı ve her $n \in \mathsf{N}$ için $q = p^n$ mertebeli sonlu cisimlerin var olduğu gösterilmektedir.

2.1.13. Teorem. Her p asal sayısı ve her $n \in \mathsf{N}$ için $q = p^n$ mertebeli bir sonlu cisim vardır (Conrad 2013).

İspat. $p(x) = x^{p^n} - x \in \mathsf{F}_p[x]$ polinomunun parçalanma cismi F ve $p(x)$ polinomunun F cismindeki tüm köklerinin kümesi $S = \{\alpha \in F : \alpha^{p^n} = \alpha\}$ olsun. $x^{p^n} - x$ ayrılabilirdir, yani $x^{p^n} - x$ polinomunun parçalanma cismindeki her kökü basit köktür. Gerçektende $p'(x) = p^n x^{p^n-1} - 1 = -1$, yani $(p(x), p'(x)) = 1$ dir. Dolayısıyla $|S| = p^n$ dir. Şimdi S kümesinin F cisminin bir alt cismi olduğunu gösterelim. Bunun için, $\alpha, \beta \in S$ olmak üzere $\alpha + \beta$, $\alpha \cdot \beta$, $-\alpha$ ve $\alpha \neq 0$ olmak üzere $1/\alpha$ elemanlarının S kümesinde olduğunu göstermek yeterlidir. α ve β, $p(x)$ polinomunun kökleri olduğundan $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$ ve üstelik Kar(F) = p olduğundan her $n \geq 1$ için

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha+\beta \in S \quad \text{ve} \quad (\alpha\cdot\beta)^{p^n} = \alpha^{p^n}\cdot\beta^{p^n} = \alpha\cdot\beta \in S$$

dir. $(-\alpha)^{p^n} = (-1)^{p^n}\cdot\alpha^{p^n} = (-1)^{p^n}\cdot\alpha$, eğer p tek bir asal sayı ise $(-1)^{p^n} = -1$ ve $p = 2$ ise $(-1)^{p^n} = 1$ dir. Böylece her iki halde de $(-\alpha)^{p^n} = -\alpha$, yani $-\alpha \in S$ dir. $\alpha \neq 0$ olmak üzere $(1/\alpha)^{p^n} = 1/\alpha^{p^n} = 1/\alpha$ olduğundan $1/\alpha \in S$ dir. Bundan başka $0, 1 \in S$ olduğu açıktır. O halde S, p^n mertebeli sonlu bir cisimdir. Üstelik $S = F$ dir, gerçekten $\mathsf{F}_p < S$, yani S, F_p üzerinde $p(x)$ polinomunun parçalanma cismidir ve dolayısıyla $S = F$ dir.

Bu teoremin bir sonucu olarak $\mathsf{F}_p[x]$ halkasında istenen her dereceye sahip bir indirgenmez polinomun varlığı ele alınacaktır. Daha sonra bu $p(x)$ polinomunun bir tek olduğu görülecektir.

2.1.14. Sonuç. Her $q = p^n$ asal kuvveti ve her $n \in \mathsf{N}$ sayısı için $\mathsf{F}_p[x]$ halkasında derecesi n olan bir monik indirgenmez $p(x)$ polinomu vardır ve bu $p(x)$ polinomu, $\mathsf{F}_p[x]/\langle p(x)\rangle$ halkasının sıfırdan farklı olan her bir elemanı x in bir kuvvetine denk olacak biçimde seçilebilir (Conrad 2013).

İspat. Teorem 2.1.13 gereği, $q = p^n$ mertebeli sonlu bir cisim vardır. O halde yukarıdaki teorem gereği, $\mathsf{F}_p[x]$ halkasında derecesi n olan bir monik indirgenmez $p(x)$ polinomu vardır. Diğer yandan $\mathsf{F}_p[x]/\langle p(x)\rangle \cong \mathsf{F}_p(\alpha)$ izomorfizmi kullanılarak $\mathsf{F}_p[x]/\langle p(x)\rangle$ halkasının $x + \langle p(x)\rangle$ elemanı ile $p(x)$ polinomunun F cismindeki kökü olan α elemanı, yani F^* devirli bir grubunun üreteci ile eşlenir. O halde $\mathsf{F}_p[x]/\langle p(x)\rangle$ halkasının sıfırdan farklı olan her bir elemanı x in bir kuvvetine denk olarak alınabilir.

2.1.15. Örnek. 9 elemanlı bir cisim oluşturmak için $\mathsf{F}_3[x]$ halkasında derecesi 2 olan monik indirgenemez polinomlar dikkate alınabilir. $\mathsf{F}_3[x]$ halkasında derecesi 2 olan monik indirgenmez polinomlar

$$x^2 + 1,\ x^2 + x + 2 \text{ ve } x^2 + 2x + 2$$

polinomları olduğundan

$$\mathsf{F}_3[x]/\langle x^2+1\rangle, \quad \mathsf{F}_3[x]/\langle x^2+x+2\rangle, \quad \mathsf{F}_3[x]/\langle x^2+2x+2\rangle$$

bölüm halkalarının her biri 9 mertebeli bir cisimdir.

2.1.16. Teorem. $q = p^n$ mertebeli her sonlu cisim $x^q - x$ polinomunun F_p cismi üzerindeki parçalanma cismine izomorftur (Conrad 2013).

İspat. F, $q = p^n$ elemanlı sonlu bir cisim ise F cisminin karakteristiği p dir. Dolayısıyla F cismi, F_p cismine izomorf bir asal alt cisim bulundurur. O halde Teorem 2.1.11. gereği, F cismi $x^q - x$ polinomunun F_p cismi üzerinde parçalanma cismidir. Üstelik cisim teoriden, bir polinomun bir cisim üzerindeki parçalanma cisimlerinin izomorf olduğu bilinmektedir. Dolayısıyla p^n mertebeli her sonlu cisim, $x^q - x$ polinomunun F_p cismi üzerindeki parçalanma cismine izomorftur.

2.1.17. Uyarı 1. Teorem 2.1.16., q mertebeli her sonlu cismin $x^q - x$ polinomunun F_p cismi üzerindeki parçalanma cismine izomorf olduğunu ve dolayısıyla aynı mertebeye sahip herhangi iki sonlu cismin birbirine izomorf olduğunu belirtmektedir. O halde verilen bir mertebeye sahip sonlu bir cisim izomorfizme bağlı olarak bir tektir.

2. Benzer bir sonuç sonlu grup ve sonlu halkalar için geçerli değildir, yani mertebeleri aynı olan iki sonlu grup veya halka birbirlerine izomorf olmak zorunda değillerdir. Örneğin 4 elemanlı devirli bir grup ve 4 elemanlı Klein-4 grubu izomorf değildir, benzer şekilde $\mathsf{Z}_2 \times \mathsf{Z}_2$ ve Z_4 halkaları da izomorf değildir.

2.1.18. Örnek. $\mathsf{F}_5[x]$ halkası üzerinde $p(x) = x^3 + x + 1$, $q(x) = x^3 + x^2 + 1$ polinomlarını dikkate alalım.

$$p(0) = 1,\ p(1) = 3,\ p(2) = 1,\ p(3) = 1,\ p(4) = 4$$

ve

$$q(0) = 1,\ q(1) = 3,\ q(2) = 1,\ q(3) = 1,\ q(4) = 4$$

olduğundan $p(x)$ ve $q(x)$ polinomlarının F_5 cisminde bir sıfırı yoktur. Dolayısıyla $p(x)$ ve $q(x)$ polinomlarının birer lineer çarpanı yoktur. O halde $p(x)$ ve $q(x)$ polinomları $\mathsf{F}_5[x]$ halkası üzerinde indirgenemezdir. Diğer yandan $p(x)$ ve $q(x)$ polinomlarının F_5 cisminin

birer genişlemesindeki kökleri, sırasıyla, α, β ve $E = \mathsf{F}_3(\alpha)$, $F = \mathsf{F}_5(\beta)$ olmak üzere $p(x)$ ve $q(x)$ polinomları, $\mathsf{F}_5[x]$ halkası üzerinde indirgenemez olduğundan $[E : \mathsf{F}_5] = [F : \mathsf{F}_5] = 3$ ve dolayısıyla $|E| = |F| = 5^3 = 125$ dir ve üstelik Teorem 2.1.16 gereği, $E \cong F$ dir.

2.1.19. Teorem. F_q, $q = p^n$ mertebeli bir sonlu cisim ise F_q cisminin her alt cisminin mertebesi, $d \mid n$ olmak üzere p^d dir. Üstelik bu özellikteki her bir d için p^d mertebeli bir tek alt cisim vardır (Conrad 2013).

İspat. F, $\mathsf{F}_p < F < \mathsf{F}_q = \mathsf{F}_{p^n}$ özelliğinde bir sonlu cisim ve $[F : \mathsf{F}_p] = d$ ise $|F| = p^d$ dir. Diğer yandan $n = [\mathsf{F}_{p^n} : \mathsf{F}_p] = [\mathsf{F}_{p^n} : F] \cdot [F : \mathsf{F}_p]$ olduğundan $d|n$ olmalıdır. Bundan başka F^* çarpımsal grubunun mertebesi $p^d - 1$ olduğundan her $t \in F^*$ için $t^{p^d-1} = 1$ yani $t^{p^d} = t$ olur ve üstelik bu son eşitlik $t = 0$ için de gerçeklenir. $x^{p^d} - x$ polinomunun F_{p^n} cisminde en fazla p^d tane kökü vardır. Böylece F, p^d tane farklı kökten oluşan bir küme olur, yani

$$F = \{t \in \mathsf{F}_{p^n} \mid t^{p^d} = t\}$$

dir. Bu ise F_{p^n} cisminin en fazla p^d mertebeli bir alt cismin olduğunu gösterir. Her $d \mid n$ için p^d mertebeli bir alt cismin var olduğunu göstermek için

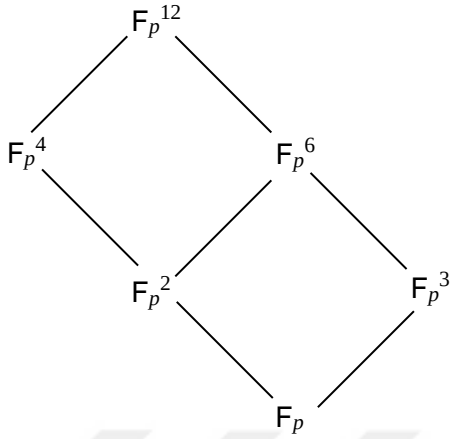
$$\{t \in \mathsf{F}_{p^n} \mid t^{p^d} = t\}$$

kümesini göz önüne alalım. Bu kümenin bir cisim olduğu Teorem 2.1.13. ün ispatındaki S kümesinin bir cisim olduğunun gösterilmesine benzer biçimde görülebilir. Şimdi bu kümenin eleman sayısının p^d olduğunu göstermek için F_{p^n} cisminde $t^{p^d-1} = 1$ eşitliğini gerçekleyen $p^d - 1$ tane sıfırdan farklı eleman olduğunu göstermek yeterlidir. γ, $\mathsf{F}_{p^n} \setminus \{0\}$ grubunun bir üreteci ise γ elemanının meretebesi $p^n - 1$ dir. Ayrıca $d \mid n$ olduğundan $(p^d - 1) \mid (p^n - 1)$ dir. Eğer

$$\alpha = \gamma^{(p^n-1)/(p^d-1)}$$

olarak alınırsa α nın mertebesi $p^d - 1$ olur. $0 \le k \le p^d - 2$ için α^k lar $t^{p^d-1} = 1$ eşitliğini gerçekler. Böylece F, p^d mertebeli bir cisim olur.

2.1.20. Örnek. Aşağıda F_p^{12} cisminin alt cisimleri verilmiştir, burada d = 1, 2, 3, 4, 6, 12 dir.



Şekil 2.1. F_p^{12} cisminin alt cisimleri

2.2. İndirgenemez Polinomların Kökleri

Bu kısımda sonlu cisimleri elde ederken kullanılan indirgenemez polinomların kökleri ve bu köklerin özellikleri üzerinde durulacaktır. Sonuç 2.1.14. gereği, her $n \in \mathbb{N}$ sayısı ve her $q = p^n$ asal kuvveti ve için $F_p[x]$ halkasında derecesi n olan bir monik indirgenemez $p(x)$ polinomu vardır ve üstelik

$$F_p[x]/\langle p(x)\rangle \cong F_p(\alpha)$$

dir.

2.2.1. Örnek. $p(x) = x^2 + x + 1 \in F_2[x]$ polinomu $F_2[x]$ halkası üzerinde indirgenemezdir. Kronecker Teoremi gereği, $p(x)$ polinomunun bir α kökünü bulunduran F_2 cisminin bir cisim genişlemesi vardır. α, $p(x)$ polinomunun F_2 cisminin bir genişlemesindeki bir kökü olmak üzere $\alpha^2 + \alpha + 1 = 0$ ve böylece $\alpha^2 = -(1 + \alpha) = 1 + \alpha$ dir. $F_2(\alpha)$ cismi

$$\{a + b\alpha \mid a, b \in F_2\}$$

biçimindedir ve bu cismin elemanları 0, 1, α ve $1 + \alpha$ dır. Bundan başka F_4, $F_2(\alpha)$ cismine izomorftur. Üstelik α, bu cismin bir ilkel elemanı olduğundan

$$\alpha^1 = \alpha,\ \alpha^2 = 1 + \alpha \text{ ve } \alpha^3 = 1$$

dir.

Çizelge 2.2. $F_2(\alpha)$ cisminin işlem tabloları

+	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

·	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

2.2.2. Örnek. $p(x) = x^2 + x + 2 \in F_3[x]$ polinomunun F_3 cisminde kökü olmadığından $F_3[x]$ halkasında indirgenemez bir polinomdur. Kronecker Teoremi gereği, $p(x)$ polinomunun bir α kökünü bulunduran F_2 cisminin bir cisim genişlemesi vardır. α, $p(x)$ polinomunun F_3 cisminin bir genişlemesindeki bir kökü olmak üzere

$$\alpha^2 + \alpha + 2 = 0$$

ve böylece

$$\alpha^2 = -\alpha - 2 = 2\alpha + 1$$

dir. $F_3(\alpha)$ cismi, F_3 cismi üzerinde 2 boyutlu bir vektör uzayı olduğundan

$$F_3(\alpha) = \{a + b\alpha \mid a, b \in F_3\}$$

dır. Bundan başka F_9, $F_3(\alpha)$ cismine izomorftur. Bu cismin toplam ve çarpım tablolarını oluşturmak için küçük hesaplamalar yapılabilir. Örneğin,

$$2\alpha(\alpha + 2) = 2\alpha^2 + 4\alpha = 2(2\alpha + 1) + \alpha = 2\alpha + 2$$

dir. Elde edilen çarpım tablosu yardımıyla α elemanının F_9^* grubundaki mertebesinin 8 olduğu görülür. Dolayısıyla α, F_9 cisminin ilkel bir elemanıdır.

Çizelge 2.3. $F_3(\alpha)$ cisminin işlem tabloları

+	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
1	1	2	0	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α
2	2	0	1	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$
α	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$	0	1	2
$\alpha+1$	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α	1	2	1
$\alpha+2$	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$	2	0	0
2α	2α	$2\alpha+1$	$2\alpha+2$	0	1	2	α	$\alpha+1$	$\alpha+2$
$2\alpha+1$	$2\alpha+1$	$2\alpha+2$	2α	1	2	1	$\alpha+1$	$\alpha+2$	α
$2\alpha+2$	$2\alpha+2$	2α	$2\alpha+1$	2	0	0	$\alpha+2$	α	$\alpha+1$

.	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	$2\alpha+1$	1	$\alpha+1$	$\alpha+2$	$2\alpha+2$	2
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	1	$\alpha+2$	2α	2	α	$2\alpha+1$
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$\alpha+1$	2α	2	$2\alpha+2$	1	α
2α	0	2α	α	$\alpha+2$	2	$2\alpha+2$	$2\alpha+1$	$\alpha+1$	1
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$2\alpha+2$	α	1	$\alpha+1$	2	2α
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	2	$2\alpha+1$	α	1	2α	$\alpha+2$

Yukarıdaki örneklerde ele alınan indirgenemez polinomun kökleri sonlu cisimler teorisinde oldukça önemlidir. Bu kısımda sonlu bir cisim üzerinde tanımlı olan indirgenemez bir polinomun köklerinin kümesi incelenecektir.

2.2.3. Teorem. $p(x) \in \mathsf{F}_q[x]$, F_q cismi üzerinde bir indirgenemez polinom ve α, $p(x)$ polinomunun F_q cisminin bir cisim genişlemesindeki bir kökü olsun. Bu durumda bir $h(x) \in \mathsf{F}_q[x]$ polinomu için $h(x) = 0$ olması için gerek ve yeter koşul $p(x)$ polinomunun $h(x)$ polinomunu bölmesidir (Lidl ve Neiderreiter 1986).

İspat. $a \in \mathsf{F}_q$, $p(x)$ polinomunun başkatsayısı ve $g(x) = a^{-1}p(x)$ olsun. Bu durumda $g(x)$ polinomu $\mathsf{F}_q[x]$ halkasında monik indirgenemez bir polinomdur ve $g(\alpha) = 0$ dır. Böylece $g(x)$ polinomu, α elemanının F_q cismi üzerindeki minimal polinomudur. İspatın devamı Teorem 1.2.4. den elde edilir.

2.2.4. Teorem. $p(x) \in \mathsf{F}_q[x]$ polinomu derecesi m olan F_q cismi üzerinde indirgenemez bir polinom olsun. Bu durumda $p(x)$ polinomunun $x^{q^n} - x$ polinomunu bölmesi için gerek ve yeter koşul m nin n yi bölmesidir (Lidl ve Neiderreiter 1986).

İspat. $p(x) \mid x^{q^n} - x$ olsun. Eğer α, $p(x)$ polinomunun F_q cismi üzerindeki parçalanma cismindeki bir kökü ise $\alpha^{q^n} = \alpha$ ve dolayısıyla $\alpha \in \mathsf{F}_{q^n}$ dir. Bu ise $\mathsf{F}_q(\alpha)$ cisminin F_{q^n} cisminin bir alt cismi olduğunu gösterir. O halde $\mathsf{F}_q < \mathsf{F}_q(\alpha) < \mathsf{F}_{q^n}$ dir. Dolayısıyla Teorem 1.2.1. gereği,

$$[\mathsf{F}_{q^n} : \mathsf{F}_q] = [\mathsf{F}_{q^n} : \mathsf{F}_q(\alpha)]\,[\mathsf{F}_q(\alpha) : \mathsf{F}_q]$$

dir. Diğer yandan $[\mathsf{F}_q(\alpha) : \mathsf{F}_p] = m$ ve $[\mathsf{F}_{q^n} : \mathsf{F}_q] = n$ olduğundan $m \mid n$ dir.

Tersine $m|n$ ise Teorem 2.1.19. gereği, F_{q^m}, F_{q^n} cisminin bir alt cismidir. Eğer α, $p(x)$ polinomunun F_q cismi üzerindeki parçalanma cisminindeki bir kökü ise $[\mathsf{F}_q(\alpha) : \mathsf{F}_q] = m$ ve böylece $\mathsf{F}_q(\alpha) = \mathsf{F}_{q^m}$ olur. O halde $\alpha \in \mathsf{F}_{q^n}$ ve dolayısıyla $\alpha^{q^n} = \alpha$ dir. Bu ise α nın $x^{q^n} - x \in \mathsf{F}_q[x]$ polinomunun bir kökü olduğunu gösterir. Dolayısıyla yukarıdaki teorem gereği, $p(x) \mid x^{p^n} - x$ dir.

2.2.5. Örnek. $\mathsf{F}_2[x]$ halkasında $x^{2^n} - x$ polinomunu, $n = 1, 2, 3, 4$ için indirgenmezlerin çarpımı biçiminde aşağıdaki gibi yazılabilir;

$$x^2 - x = x(x - 1),$$

$x^4 - x = x(x-1)(x^2 + x + 1)$,

$x^8 - x = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$,

$x^{16} - x = x(x-1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$.

2.2.6. Teorem. $p(x) \in \mathsf{F}_q[x]$, F_q cismi üzerinde m dereceli indirgenemez bir polinom olsun. Bu durumda $p(x)$ polinomunun $\mathsf{F}_q{}^m$ cisminde bir α kökü vardır. Üstelik $p(x)$ polinomunun tüm kökleri basit köktür ve bu kökler, $\mathsf{F}_q{}^m$ cisminin birbirinden farklı olan $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ elemanlarıdır (Lidl ve Neiderreiter 1986).

İspat. α, $p(x)$ polinomunun F_q cismi üzerindeki parçalanma cismindeki bir kökü ise $[\mathsf{F}_q(\alpha) : \mathsf{F}_q] = m$ ve dolayısıyla $\mathsf{F}_q(\alpha) = \mathsf{F}_q{}^m$ dır. Bu ise $\alpha \in \mathsf{F}_q{}^m$ olduğunu gösterir. Şimdi $\beta \in \mathsf{F}_q{}^m$ elemanı $p(x)$ polinomunun bir kökü ise β^q elemanının da $p(x)$ polinomunun bir kökü olduğunu gösterelim. $0 \le i \le m$ için $a_i \in \mathsf{F}_q$ olmak üzere

$$p(x) = a_m x^m + ... + a_1 x + a_0$$

polinomunu alalım. $a_i^q = a_i$ ve F_q cisminin karakteristiği p olduğundan

$$\begin{aligned} p(\beta^q) &= a_m \beta^{qm} + ... + a_1 \beta^q + a_0 \\ &= a_m^q \beta^{qm} + ... + a_1^q \beta^q + a_0^q \\ &= (a_m \beta^m + ... + a_1 \beta + a_0)^q \\ &= p(\beta)^q = 0 \end{aligned}$$

olur. Dolayısıyla $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ elemanları $p(x)$ polinomunun kökleridir. Şimdi bu köklerin birbirinden farklı olduğunu gösterelim. Tersine j ve k, $0 \le j \le k \le m-1$ özelliğinde iki tamsayı olmak üzere $\alpha^{q^j} = \alpha^{q^k}$ olsun. Bu eşitliğin her iki yanı q^{m-k} ile çarpılırsa

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha$$

eşitliği elde edilir. Dolayısıyla Teorem 2.2.3 gereği, $p(x) \mid (x^{q^{m-k+j}} - x)$ olmalıdır. Bu ise m sayısının $m - k + j$ sayısını bölmesiyle mümkündür, ancak $0 < m - k + j < m$ olduğundan bu imkansızdır.

2.2.7. Sonuç. $p(x) \in \mathsf{F}_q[x]$ derecesi m olan indirgenemez bir polinom ise $p(x)$ polinomunun F_q cismi üzerindeki parçalanma cismi $\mathsf{F}_q{}^m$ cismidir (Lidl ve Neiderreiter 1986).

İspat. Bir önceki teorem gereği $p(x)$ polinomu $\mathsf{F}_q{}^m$ cisminde parçalanır. Üstelik $p(x)$ polinomunun $\mathsf{F}_q{}^m$ cismindeki bir α kökü için

$$\mathsf{F}_q(\alpha,\ \alpha^q, \alpha^{q^2}, ...,\ \alpha^{q^{m-1}}) = \mathsf{F}_q(\alpha) = \mathsf{F}_q{}^m$$

dir.

2.2.8. Sonuç. $\mathsf{F}_q[x]$ halkasında aynı dereceli herhangi iki indirgenemez polinomun parçalanma cisimleri izomorftur (Lidl ve Neiderreiter 1986).

Şimdi yukarıdaki teoremde geçen $p(x)$ indirgenemez polinomun kökleri olan $\alpha,\ \alpha^q,\ \alpha^{q^2}, ...,\ \alpha^{q^{m-1}}$ elemanlarına özel bir isim verilecektir.

2.2.9. Tanım. F_q bir sonlu cisim ve $\mathsf{F}_q{}^m$, F_q cisminin bir cisim genişlemesi olmak üzere $\alpha \in \mathsf{F}_q{}^m$ olsun. $\alpha,\ \alpha^q, \alpha^{q^2}, ...,\ \alpha^{q^{m-1}}$ elemanlarına α elemanının F_q cismine göre *eşlenikleri* denir.

2.2.10. Uyarı. $\alpha \in \mathsf{F}_q{}^m$ elemanının F_q cismi üzerindeki minimal polinomunun derecesi $d = m$ ise α elemanının F_q cismine göre eşlenikleri $\alpha,\ \alpha^q,\ \alpha^{q^2},\ ...,\ \alpha^{q^{m-1}}$ birbirinden farklıdır. Eğer $m \neq d$ ise d, m nin bir has bölenidir ve her bir eşlenik eleman m/d kez tekrarlanır.

2.2.11. Teorem. $\alpha \in \mathsf{F}_q{}^*$ elemanının, F_q cisminin herhangi bir alt cismine göre eşleniklerinin $\mathsf{F}_q{}^*$ grubundaki mertebeleri aynıdır (Lidl ve Neiderreiter 1986).

İspat. $\mathsf{F}_q{}^*$ devirli bir grup olduğundan teoremin ispatı Teorem 1.1.1 ve F_q cisminin karakteristiği olan p asal sayısının tüm kuvvetleri $\mathsf{F}_q{}^*$ grubunun mertebesi olan $q - 1$ ile aralarında asal olduğu gerçeği kullanılarak elde edilir.

2.2.12. Sonuç. α, F_q cisminin bir ilkel elemanı ise α elemanının tüm eşlenikleri de F_q cisminin herhangi bir alt cismine göre ilkel elemandır (Lidl ve Neiderreiter 1986).

2.2.13. Örnek 1. $\alpha \in \mathsf{F}_{16}$, $p(x) = x^4 + x + 1 \in \mathsf{F}_2[x]$ polinomunun bir kökü olsun. Bu durumda α elemanının F_2 cismine göre eşlenikleri

$$\alpha,\ \alpha^2,\ \alpha^4 = \alpha + 1 \text{ ve } \alpha^8 = \alpha^2 + 1$$

biçimindedir ve bu eşleniklerin her biri F_{16} cisminin ilkel elemanlarıdır. α elemanının F_4 cismine göre eşlenikleri ise α ve $\alpha^4 = \alpha + 1$ dir.

2. $\alpha \in \mathsf{F}_{27}$, $p(x) = x^3 - x + 1 \in \mathsf{F}_3[x]$ polinomunun bir kökü olsun. Bu durumda α elemanının F_3 cismine göre eşlenikleri

$$\alpha, \qquad \alpha^3 = \alpha + 2 \qquad \text{ve } \alpha^9 = \alpha + 1$$

biçimindedir ve bu eşleniklerin her biri F_{27} cisminin ilkel elemanlarıdır.

2.2.14. Uyarı. Bir sonlu cismin belli otomorfizmleri ve eşlenik elemanlar arasında yakın bir ilişki vardır. $\mathsf{F}_q{}^m$, F_q cisminin bir cisim genişlemesi olsun. Bundan sonra $\mathsf{F}_q{}^m$ cisminin F_q cismi üzerindeki bir otomorfizmi denildiğinde $\alpha \in \mathsf{F}_q{}^m$ elemanını F_q cismine göre eşleniğine resmeden ve F_q cisminin elemanlarını sabit bırakan $\mathsf{F}_q{}^m$ cisminin bir otomorfizmi anlaşılacaktır.

2.2.15. Teorem. $\mathsf{F}_q{}^m$ cisminin F_q cismi üzerindeki farklı otomorfizmleri $\alpha \in \mathsf{F}_q{}^m$ ve $0 \le j \le m - 1$ için $\sigma_j(\alpha) = \alpha^{q^j}$ olarak tanımlanan $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ dönüşümleridir (Lidl ve Neiderreiter 1986).

İspat. Her bir σ_j dönüşümü ve her $\alpha, \beta \in \mathsf{F}_q{}^m$ için $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$ olduğu açıktır. Diğer yandan $\mathsf{F}_q{}^m$ cisminin karakteristiği p olduğundan $\sigma_j(\alpha + \beta) = \sigma_j(\alpha) + \sigma_j(\beta)$ dır. Dolayısıyla σ_j dönüşümü $\mathsf{F}_q{}^m$ cisminin bir endomorfizmidir. Ayrıca $\sigma_j(\alpha) = 0$ olması için gerek ve yeter koşul $\alpha = 0$ olmasıdır. Bu ise σ_j dönüşümünün birebir olduğunu gösterir. Son olarak $\mathsf{F}_q{}^m$ cismi sonlu olduğundan σ_j bir epimorfizm ve dolayısıyla $\mathsf{F}_q{}^m$ cisminin bir

otomorfizmdir. Üstelik Sonuç 2.1.8. gereği, her $a \in \mathsf{F}_q$ için $\sigma_j(a) = a$ olduğundan her σ_j dönüşümü, $\mathsf{F}_q{}^m$ cisminin F_q cismi üzerinde bir otomorfizmidir.

Diğer yandan $\sigma_0, \sigma_1, ..., \sigma_{m-1}$ dönüşümleri altında $\mathsf{F}_q{}^m$ cisminin bir ilkel elemanı farklı değerler aldığından bu dönüşümler birbirinden farklıdır.

Şimdi σ, $\mathsf{F}_q{}^m$ cisminin F_q cismi üzerinde herhangi bir otomorfizmi olmak üzere β, $\mathsf{F}_q{}^m$ cisminin bir ilkel elemanı ve $p(x) = x^m + a_{m-1}x^{m-1} + ... + a_0 \in \mathsf{F}_q[x]$ polinomu β elemanın F_q cismi üzerindeki minimal polinomu ise

$$\begin{aligned} 0 &= \sigma(\beta^m + a_{m-1}\beta^{m-1} + ... + a_0) \\ &= \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + ... + a_0 \end{aligned}$$

olarak yazılabileceğinden $\sigma(\beta)$, $p(x)$ polinomunun $\mathsf{F}_q{}^m$ cismindeki bir köküdür. O halde Teorem 2.2.6. gereği, $0 \le j \le m-1$ özelliğindeki belli bir j sayısı için $\sigma(\beta) = \beta^{q^j}$ dir. σ, bir homomorfizm olduğundan her $\alpha \in \mathsf{F}_q{}^m$ için $\sigma(\alpha) = \alpha^{q^j}$ dir.

2.2.16. Uyarı 1. $\mathsf{F}_q{}^m$ cisminin F_q cismi üzerindeki tüm otomorfizmlerinin kümesi fonksiyonların bileşke işlemine göre bir gruptur. Bu gruba $\mathsf{F}_q{}^m$ cisminin F_q cismi üzerindeki *Galois grubu* adı verilir. Üstelik yukarıdaki teorem gereği, bu grup $\alpha \in \mathsf{F}_q{}^m$ olmak üzere

$$\sigma_1 : \mathsf{F}_q{}^m \to \mathsf{F}_q{}^m,\ \sigma_1(\alpha) = \alpha^q$$

Frobenius otomorfizmi ile üretilen m mertebeli devirli bir gruptur.

2. F_q cisminin elemanları $x^q - x$ polinomunun tüm kökleri olduğundan F_q, F_p üzerinde bu polinomun parçalanma cismidir. Diğer yandan F_q, F_p cisminin sonlu bir genişlemesi olduğundan mükemmel ve dolayısıyla da ayrılabilirdir. O halde F_q, F_p cisminin bir Galois genişlemesidir.

Aşağıdaki teoremde sonlu cisimlerin Galois gruplarının devirli olduğu ve doğal bir üretecinin olduğu görülecektir.

2.2.17. Teorem. Gal($\mathbb{F}_q^m/\mathbb{F}_q$) Galois grubu devirlidir ve bu grubun üreteci

$$\sigma_1 : \mathbb{F}_q^m \to \mathbb{F}_q^m,\ \sigma_1(\alpha) = \alpha^q$$

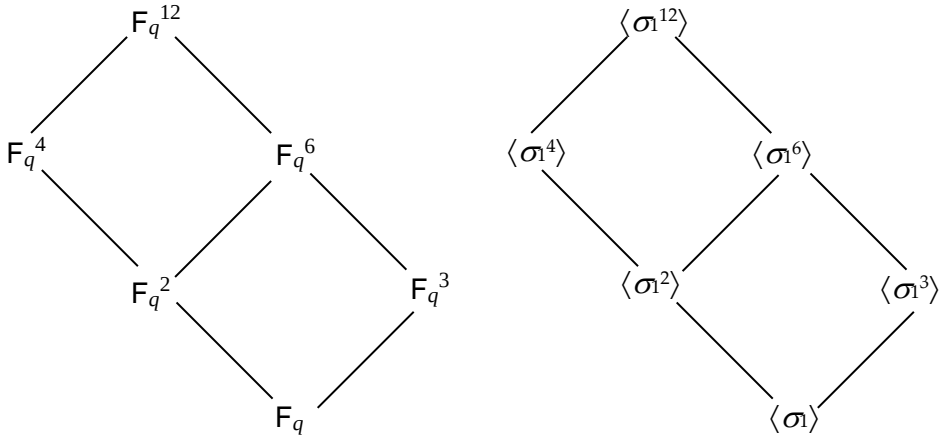
Frobenius otomorfizmidir (Conrad 2013).

İspat. Her $\alpha \in \mathbb{F}_q$ için $\sigma_1(\alpha) = \alpha^q = \alpha$ olduğundan σ_1 dönüşümü $\mathbb{F}_q$ cismini sabit bırakır. Ayrıca σ_1 dönüşümü bir cisim homomorfizmidir ve birebirdir. $\mathbb{F}_q$ cismi sonlu olduğundan σ_1 örtendir. Dolayısıyla $\sigma_1 \in$ Gal($\mathbb{F}_q^m/\mathbb{F}_q$) dir.

Diğer yandan Gal($\mathbb{F}_q^m/\mathbb{F}_q$) grubunun mertebesi $[\mathbb{F}_q^m : \mathbb{F}_q] = m$ dir. σ_1 otomorfizminin mertebesinin m olduğunu, yani bu grubun bir üreteci olduğunu gösterelim. $r \geq 1$ ve $\alpha \in \mathbb{F}_q^m$ için $\sigma_1^r(\alpha) = \alpha^{q^r}$ dir Dolayısıyla σ_1^r özdeşlik dönüşüm ise her $\alpha \in \mathbb{F}_q^m$ için $\alpha^{q^r} = \alpha$ ve böylece $\alpha^{q^r} - \alpha = 0$ dır. $x^{q^r} - x$ polinomunun derecesi q^r olduğundan bu polinomun bir cisimde en fazla q^r tane kökü vardır. O halde $q^m \leq q^r$ ve böylece $m \leq r$ dir. Bu ise σ_1 dönüşümünün Gal($\mathbb{F}_q^m/\mathbb{F}_q$) grubundaki mertebesinin en az m olduğunu gösterir. Gal($\mathbb{F}_q^m/\mathbb{F}_q$) Galois grubunun mertebesi m olduğundan σ_1 otomorfizminin mertebesi m olmak zorundadır, yani σ_1 bu grubun bir üretecidir.

Galois teorisi gereği, Gal($\mathbb{F}_q^m/\mathbb{F}_q$) Galois grubunun alt grup diyagramı ile $\mathbb{F}_q^m$ cisminin $\mathbb{F}_q$ üzerindeki ara cisim diyagramları birbirinin ters dönmüş halidir. Buna göre $\mathbb{F}_q^m$ cisiminin $\mathbb{F}_q$ cismi üzerindeki d dereceli tek alt cismi, Gal($\mathbb{F}_q^m/\mathbb{F}_q$) Galois grubunun indeksi d olan tek alt grubuna karşılık gelir.

2.2.18. Örnek. $\mathbb{F}_q$ cisminin $\mathbb{F}_q^{12}$ cisim genişlemesinin derecesi $[\mathbb{F}_q^{12} : \mathbb{F}_q] = 12$ olduğundan $\mathbb{F}_q^{12}$ cisminin $\mathbb{F}_q$ üzerindeki Galois grubu Gal($\mathbb{F}_q^{12}/\mathbb{F}_q$) $= \langle\sigma_1\rangle \cong \mathbb{Z}_{12}$ dir. Aşağıda diyagramlarda $\mathbb{F}_q^{12}$ cisminin $\mathbb{F}_q$ üzerindeki ara cisim cisimleri ve bunlara karşılık gelen Gal($\mathbb{F}_q^{12}/\mathbb{F}_q$) grubunun alt grupları üreteçleri yardımıyla verilmiştir.



Şekil 2.2. $\mathbb{F}_q^{12}$ cisminin $\mathbb{F}_q$ üzerindeki alt cisim diyagramı ve $\mathrm{Gal}(\mathbb{F}_q^{12}/\mathbb{F}_q)$ grubunun alt grup diyagramı

2.3. İz, Norm ve Baz

$K = \mathbb{F}_q$ bir sonlu cisim ve $F = \mathbb{F}_q^m$, K cisminin bir sonlu genişlemesi ise F, K cismi üzerinde m boyutlu bir vektör uzayıdır. Eğer $\{\alpha_1, \alpha_2, ..., \alpha_m\}$ kümesi, F cisminin bir K bazı ise $1 \le j \le m$ için $c_j \in K$ olmak üzere her $\beta \in F$ elemanı

$$\beta = c_1\alpha_1 + ... + c_m\alpha_m$$

şeklinde tek türlü yazılabilir.

Şimdi bu özellikteki F ve K cisimleri için F cisminden K cismine tanımlı önemli bir dönüşüm verilecektir.

2.3.1. Tanım. $K = \mathbb{F}_q$ ve $F = \mathbb{F}_q^m$ sonlu cisimler ve $\alpha \in F$ olmak üzere

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + ... + \alpha^{q^{m-1}}$$

toplamına α elemanının K cismi üzerindeki *izi* denir. Eğer K, F cisminin asal cismi ise $\mathrm{Tr}_{F/K}(\alpha)$ ya α elemanının *mutlak izi* denir ve $\mathrm{Tr}_F(\alpha)$ şeklinde gösterilir.

Tanıma dikkat edilirse, α elemanının K cismi üzerindeki izi, α elemanının K cismine göre eşleniklerinin toplamıdır. α elemanının K cismi üzerindeki izi tanımı şu sekilde de verilebilir: $p(x) \in K[x]$, α elemanının K cismi üzerindeki minimal polinomu ise $p(x)$

polinomunun derecesi d, m nin bir bölenidir. $g(x) = p(x)^{m/d} \in K[x]$ polinomuna α elemanının K cismi üzerindeki *karakteristik polinomu* denir. Teorem 2.2.3. gereği, $p(x)$ polinomunun F cismindeki kökleri α, α^q, ..., $\alpha^{q^{d-1}}$ dir. Tanım 2.2.6. gereği, $g(x)$ polinomunun F cismindeki kökleri tam olarak α elemanının K cismine göre eşlenikleridir. Dolayısıyla

$$g(x) = x^m + a_{m-1}x^{m-1} + ... + a_0 = (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{m-1}}) \quad (2.1)$$

dir ve bu iki polinomun eşitliğinden

$$\mathrm{Tr}_{F/K}(\alpha) = -a_{m-1} \quad (2.2)$$

elde edilir. Böylece $\mathrm{Tr}_{F/K}(\alpha)$ her zaman K cisminin bir elemanıdır.

2.3.2. Teorem. $K = \mathbb{F}_q$ ve $F = \mathbb{F}_q^m$ olsun. Bu durumda iz fonksiyonu $\mathrm{Tr}_{F/K}$ aşağıdaki özellikleri gerçekler:

i) Her $\alpha, \beta \in F$ için $\mathrm{Tr}_{F/K}(\alpha + \beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta)$ dır.

ii) Her $c \in K$ ve $\alpha \in F$ için $\mathrm{Tr}_{F/K}(c\alpha) = c\mathrm{Tr}_{F/K}(\alpha)$ dır.

iii) F ve K, K cismi üzerinde birer vektör uzayı olarak alınırsa $\mathrm{Tr}_{F/K}$, F cisminden K cismi üzerine bir lineer dönüşümdür.

iv) Her $a \in K$ için $\mathrm{Tr}_{F/K}(a) = ma$ dır.

v) Her $\alpha \in F$ için $\mathrm{Tr}_{F/K}(\alpha^q) = \mathrm{Tr}_{F/K}(\alpha)$ dır (Lidl ve Neiderreiter 1986).

İspat. *i)* F cisminin karakteristiği p olduğundan $\alpha, \beta \in F$ için

$$\begin{aligned}\mathrm{Tr}_{F/K}(\alpha + \beta) &= \alpha + \beta + (\alpha + \beta)^q + ... + (\alpha + \beta)^{q^{m-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + ... + \alpha^{q^{m-1}} + \beta^{q^{m-1}} \\ &= \alpha + \alpha^q + ... + \alpha^{q^{m-1}} + \beta + \beta^q + ... + \beta^{q^{m-1}} \\ &= \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta)\end{aligned}$$

ii) $c \in K$ olmak üzere Sonuç 2.1.8. gereği, her $j \geq 0$ sayısı için $c^{q^j} = c$ dir. Buradan her $\alpha \in F$ için

$$\begin{aligned}\mathrm{Tr}_{F/K}(c\alpha) &= c\alpha + c^q\alpha^q + ... + c^{q^{m-1}}\alpha^{q^{m-1}} \\ &= c\alpha + c\alpha^q + ... + c\alpha^{q^{m-1}} \\ &= c(\alpha + \alpha^q + ... + \alpha^{q^{m-1}}) \\ &= c\mathrm{Tr}_{F/K}(\alpha)\end{aligned}$$

***iii*)** Her $\alpha \in F$ için $\mathrm{Tr}_{F/K}(\alpha) \in K$ olduğundan (*i*) ve (*ii*) özellikleri gereği $\mathrm{Tr}_{F/K}$ dönüşümü F cisminden K cismi içine bir lineer dönüşümdür. Bu dönüşümün üzerine olduğunu göstermek için $\mathrm{Tr}_{F/K}(\alpha) \neq 0$ olacak şekilde bir $\alpha \in F$ nin var olduğunu göstermek yeterlidir. $\mathrm{Tr}_{F/K}(\alpha) = 0$ olması için gerek ve yeter koşul $\alpha \in F$ elemanının

$$x^{q^{m-1}} + \ldots + x^q + x \in K[x]$$

polinomunun bir kökü olmasıdır. Bu polinomun F cisminde en fazla q^{m-1} tane kökü olduğundan ve F cisminin q^m tane elemanı olduğundan istenilen şekilde bir α elemanı vardır.

***iv*)** Her $a \in K$ için Sonuç 2.1.8. gereği, $a^{q^m} = a$ olduğundan iz fonksiyonunun tanımı da göz önüne alınırsa istenilen elde edilir.

***v*)** Her $\alpha \in F$ için Sonuç 2.1.8. gereği, $\alpha^{q^m} = \alpha$ olduğundan

$$\mathrm{Tr}_{F/K}(\alpha^q) = \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^m} = \mathrm{Tr}_{F/K}(\alpha)$$

eşitliği elde edilir.

F cisminden K cismi üzerine tanımlı olan tek lineer dönüşüm iz fonksiyonu değildir. Ayrıca iz fonksiyonu seçilen bazdan bağımsız olduğundan F cismi üzerindeki diğer lineer dönüşümlerin bulunmasında kullanılabilir.

2.3.3. Teorem. *K* bir sonlu cisim ve *F*, *K* cisminin bir sonlu genişlemesi, yani *K* ve *F* cisimleri, *K* cismi üzerinde birer vektör uzayı olsun. Bu durumda *F* cisminden *K* cismi içine tanımlı lineer dönüşümler tam olarak $\beta \in F$ olmak üzere her $\alpha \in F$ için

$$L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$$

özelliğindeki L_β lineer dönüşümleridir. Üstelik β ve γ, *F* cisminin birbirinden farklı elemanları ise $L_\beta \neq L_\gamma$ dır (Lidl ve Neiderreiter 1986).

İspat. Teorem 2.3.2. (*iii*) gereği, her bir L_β dönüşümü *F* cisminden *K* cismi içine tanımlı bir lineer dönüşümdür. $\beta \neq \gamma$ olmak üzere $\beta, \gamma \in F$ ve $0 \neq \alpha \in F$ için $\mathrm{Tr}_{F/K}$ dönüşümü *F* cisminden *K* cismi üzerine bir dönüşüm olduğundan

$$L_\beta(\alpha) - L_\gamma(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha) - \mathrm{Tr}_{F/K}(\gamma\alpha) = \mathrm{Tr}_{F/K}((\beta - \gamma)\ \alpha) \neq 0$$

dır. Dolayısıyla $L_\beta \neq L_\gamma$ dır.

$K = \mathsf{F}_q$ ve $F = \mathsf{F}_q{}^m$ ise bu durumda L_β dönüşümleri, *F* cisminden *K* cismi içine tanımlı q^m tane farklı lineer dönüşüm verir. Diğer yandan *F* cisminden *K* cismi içine her lineer

dönüşüm, F cisminin bir K bazındaki m tane elemanıyla belirlenir. Bu işlem için q^m tane farklı seçim yapılabileceğinden L_β dönüşümü F cisminden K cismi içine olabilecek tüm lineer dönüşümleri verir.

2.3.4. Teorem. F, $K = \mathsf{F}_q$ cisminin bir sonlu genişlemesi olsun. Bu durumda $\alpha \in F$ için $\mathrm{Tr}_{F/K}(\alpha) = 0$ olması için gerek ve yeter koşul belli bir $\beta \in F$ için $\alpha = \beta^q - \beta$ olmasıdır (Lidl ve Neiderreiter 1986).

İspat. Bir $\beta \in F$ için $\alpha = \beta^q - \beta$ ise Teorem 2.3.2 nin (i), (ii) ve (v) şıkları gereği,

$$\mathrm{Tr}_{F/K}(\alpha) = \mathrm{Tr}_{F/K}(\beta^q - \beta) = \mathrm{Tr}_{F/K}(\beta^q) - \mathrm{Tr}_{F/K}(\beta)$$
$$= \mathrm{Tr}_{F/K}(\beta) - \mathrm{Tr}_{F/K}(\beta) = 0$$

olduğu görülür. Tersine $\mathrm{Tr}_{F/K}(\alpha) = 0$ özelliğinde bir $\alpha \in F = \mathsf{F}_q{}^m$ alalım ve β, $x^q - x - \alpha$ polinomunun F cisminin bir genişlemesindeki kökü olsun. Bu durumda $\beta^q - \beta = \alpha$ dır ve

$$0 = \mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}$$
$$= (\beta^q - \beta) + (\beta^q - \beta)^q + \ldots + (\beta^q - \beta)^{q^{m-1}}$$
$$= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \ldots + (\beta^{q^m} - \beta^{q^{m-1}})$$
$$= \beta^{q^m} - \beta$$

olduğundan $\beta^{q^m} = \beta$ ve böylece $\beta \in F$ dir.

Cisim genişlemelerinin zinciri göz önüne alınırsa, iz fonksiyonlarının bileşkesi basit bir kuralla bulunabilir.

2.3.5. Teorem. K bir sonlu cisim, F, K cisminin bir sonlu genişlemesi ve E cismi de F cisminin bir sonlu genişlemesi yani $K \le F \le E$ olsun. Bu durumda her $\alpha \in E$ için

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha))$$

dır (Lidl ve Neiderreiter 1986).

İspat. $K = \mathsf{F}_q$, $[F : K] = m$ ve $[E : F] = n$ ise Teorem 1.2.1. gereği, $[E : K] = mn$ dir. O halde $\alpha \in E$ için

$$\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)) = \sum_{i=0}^{m-1} \mathrm{Tr}_{E/F}(\alpha)^{q^i} = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{q^{jm}}\right)^{q^j}$$

$$= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \alpha^{jm+i} = \sum_{k=0}^{mn-1} \alpha^{k^q} = \mathrm{Tr}_{E/K}(\alpha)$$

olur.

Bir sonlu cisimden bu cismin alt cismine tanımlanan bir başka fonksiyon, o cismin bir elemanının alt cismine göre eşleniklerinin çarpımıyla aşağıdaki gibi elde edilir.

2.3.6. Tanım. $K = \mathsf{F}_q$ ve $F = \mathsf{F}_q{}^m$ sonlu cisimler ve $\alpha \in F$ olmak üzere

$$N_{F/K}(\alpha) = \alpha\alpha^q \cdots \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}$$

çarpımına α elemanının K cismi üzerindeki *normu* denir (Lidl ve Neiderreiter 1986).

(2.1) eşitliğindeki sabit terimler dikkate alınırsa $N_{F/K}(\alpha)$, α elemanının K cismi üzerindeki karakteristik polinomu $g(x)$ yardımıyla bulunabilir, yani

$N_{F/K}(\alpha) = (-1)^m a_0$ (2.3)

dır. Dolayısıyla $N_{F/K}(\alpha)$ her zaman K cisminin bir elemanıdır.

2.3.7. Teorem. $K = \mathsf{F}_q$ ve $F = \mathsf{F}_q{}^m$ olsun. Bu durumda $N_{F/K}$ norm fonksiyonu, aşağıdaki özellikleri gerçekler:

***i*)** Her $\alpha, \beta \in F$ için $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta)$ dır.

***ii*)** $N_{F/K}$ dönüşümü, F cismini K cismi üzerine ve F^* grubunu K^* grubuna resmeden bir dönüşümdür.

***iii*)** Her $a \in K$ için $N_{F/K}(a) = a^m$ dir.

***iv*)** Her $\alpha \in F$ için $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)$ dır (Lidl ve Neiderreiter 1986).

İspat. *i*) Norm tanımından

$$N_{F/K}(\alpha\beta) = \alpha\beta(\alpha\beta)^q \cdots (\alpha\beta)^{q^{m-1}}$$

$$= (\alpha\alpha^q \cdots \alpha^{q^{m-1}})(\beta\beta^q \cdots \beta^{q^{m-1}})$$

$$= N_{F/K}(\alpha)N_{F/K}(\beta)$$

olarak elde edilir.

***ii*)** $N_{F/K}$ dönüşümü F cismini K cismine resmeden bir dönüşümdür. Diğer yandan $N_{F/K}(\alpha) = 0$ olması için gerek ve yeter koşul $\alpha = 0$ olmasıdır. Dolayısıyla $N_{F/K}$ dönüşümü, F^* grubunu K^* grubu içine bir dönüşümdür. (i) deki bu işlem koruma özelliğiyle birlikte $N_{F/K}$ dönüşümü, bu çarpımsal gruplar arasında tanımlı bir homomorfizmdir. $N_{F/K}$ homomorfizminin çekirdeği tam olarak $x^{(q^m-1)/(q-1)} - 1 \in K[x]$ polinomunun F cismindeki köklerinden oluştuğundan $N_{F/K}$ homomorfizminin çekirdeğinin mertebesi d,

$$d \leq (q^m - 1)/(q - 1)$$

eşitsizliğini gerçekler. $N_{F/K}$ dönüşümünün görüntü kümesinin mertebesi ise $(q^m - 1)/d$ dir ve $(q^m - 1)/d \geq q - 1$ dir. O halde $N_{F/K}$ dönüşümü, F^* grubundan K^* grubuna tanımlı bir dönüşümdür.

***iii*)** Bir $a \in K$ için a elemanının K cismine göre tüm eşlenikleri kendisine eşit olduğundan norm fonksiyonun tanımı gereği $N_{F/K}(a) = a^m$ dir.

***iv*)** $N_{F/K}(\alpha)$, K cisminin bir elemanı olduğundan (i) özelliği gereği,

$$\begin{aligned} N_{F/K}(\alpha^q) &= N_{F/K}(\underbrace{\alpha \cdots \alpha}_{q \text{ tane}}) \\ &= N_{F/K}(\alpha) \cdots N_{F/K}(\alpha) = N_{F/K}(\alpha)^q \\ &= N_{F/K}(\alpha) \end{aligned}$$

dır.

2.3.8. Teorem. K bir sonlu cisim, F, K cisminin bir sonlu genişlemesi ve E cismi de F cisminin bir sonlu genişlemesi olsun. Bu durumda her $\alpha \in F$ için

$$N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha))$$

dır (Lidl ve Neiderreiter 1986).

İspat. Bir $\alpha \in E$ için

$$\begin{aligned} N_{F/K}(N_{E/F}(\alpha)) &= N_{F/K}(\alpha^{(q^{mn}-1)/(q^m-1)}) \\ &= (\alpha^{(q^{mn}-1)/(q^m-1)})^{(q^m-1)(q-1)} \\ &= \alpha^{(q^{mn}-1)/(q-1)} \\ &= N_{E/K}(\alpha) \end{aligned}$$

dir.

$\{\alpha_1, ..., \alpha_m\}$ kümesi, F cisminin bir K bazı ise bir $\alpha \in F$ elemanı $1 \leq j \leq m$ için $c_j \in K$ olmak üzere

$$\alpha = c_1(\alpha)\alpha_1 + ... + c_m(\alpha)\alpha_m \quad (2.4)$$

biçiminde tek türlü yazılabilir. Bu eşitlikteki c_j katsayıları belirlenmek istenirse, F cisminden K cismi içine tanımlı $c_j : \alpha \mapsto c_j(\alpha)$ lineer dönüşümü dikkate alınabilir. Bu dönüşüm bir lineer dönüşüm olduğundan Teorem 2.3.3 gereği, her $\alpha \in F$ için

$$c_j(\alpha) = \mathrm{Tr}_{F/K}(\beta_j\alpha)$$

olacak şekilde bir $\beta_j \in F$ vardır. $1 \leq i \leq m$ olmak üzere $\alpha = \alpha_i$ yazılırsa $i = j$ için $\mathrm{Tr}_{F/K}(\beta_j\alpha_i) = 1$ ve $i \neq j$ için $\mathrm{Tr}_{F/K}(\beta_j\alpha_i) = 0$ olduğu görülür. Üstelik $1 \leq i \leq m$ için $d_i \in K$ olmak üzere

$$d_1\beta_1 + ... + d_m\beta_m = 0$$

ise bu eşitliğin her iki tarafı belli bir $\alpha_i \in K$ ile çarpılır ve iz fonksiyonu uygulanırsa $d_i = 0$ olur. Dolayısıyla $\{\beta_1, ... , \beta_m\}$ kümesi, F cisminin bir K bazı olur.

2.3.9. Tanım. K bir sonlu cisim ve F, K cisminin bir sonlu genişlemesi olsun. Bu durumda F cisminin iki K bazı $\{\alpha_1, ..., \alpha_m\}$ ve $\{\beta_1, ..., \beta_m\}$ olmak üzere $1 \leq i, j \leq m$ için

$$\mathrm{Tr}_{F/K}(\alpha_i\beta_j) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

ise $\{\alpha_1, ..., \alpha_m\}$ ve $\{\beta_1, ..., \beta_m\}$ bazlarına *dual bazlar* denir (Lidl ve Neiderreiter 1986).

Buradan hareketle F cisminin K üzerindeki her bir $\{\alpha_1, ..., \alpha_m\}$ bazı için $\{\beta_1, ..., \beta_m\}$ şeklinde bir dual bazının var olduğu söylenebilir. (2.4) eşitliğindeki c_j katsayıları her $\alpha \in F$ için $c_j(\alpha) = \mathrm{Tr}_{F/K}(\beta_j\alpha)$ eşitliğini gerçeklediğinden dual baz tek türlü tanımlıdır ve Teorem 2.3.3. gereği, β_j elemanı c_j lineer dönüşümüyle tek türlü belirlidir.

2.3.10. Örnek. $\alpha \in \mathsf{F}_8$, $x^3 + x^2 + 1 \in \mathsf{F}_2[x]$ indirgenemez polinomunun bir kökü olsun. Bu durumda $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$, F_8 cisminin bir F_2 bazıdır. Bu bazın tek türlü tanımlı dual bazının yine $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ olduğu kolayca görülebilir. Bunun gibi dual bazı kendisine eşit olan baza *kendi dual baz* denir. $\alpha^5 \in \mathsf{F}_8$ elemanı, $c_1, c_2, c_3 \in \mathsf{F}_2$ olmak üzere

$$\alpha^5 = c_1\alpha + c_2\alpha^2 + c_3(1 + \alpha + \alpha^2)$$

şeklindedir ve c_1, c_2 ve c_3 katsayıları

$$c_1 = \mathrm{Tr}_{F_8}(\alpha\,\alpha^5) = \mathrm{Tr}_{F_8}(\alpha^6) = \alpha^6 + \alpha^{12} + \alpha^{24} = \alpha^6 + \alpha^8\alpha^4 + (\alpha^8)^3$$

$$= \alpha^6 + \alpha^5 + \alpha^3 = 1 + \alpha^4 + \alpha^2 + \alpha^4 + 1 + \alpha^2 = 0,$$

$$c_2 = \mathrm{Tr}_{F_8}(\alpha^2\,\alpha^5) = \mathrm{Tr}_{F_8}(\alpha^7) = \alpha^7 + \alpha^{14} + \alpha^{28} = \alpha^7 + (\alpha^7)^2 + (\alpha^7)^4 = 1,$$

$$c_3 = \mathrm{Tr}_{F_8}((1 + \alpha + \alpha^2)\alpha^5) = \mathrm{Tr}_{F_8}(\alpha^5 + \alpha^6 + \alpha^7)$$

$$= \mathrm{Tr}_{F_8}(\alpha^5) + \mathrm{Tr}_{F_8}(\alpha^6) + \mathrm{Tr}_{F_8}(\alpha^7)$$

$$= \alpha^5 + \alpha^{10} + \alpha^{20} + 0 + 1 = \alpha^5 + \alpha^8\,\alpha^2 + (\alpha^8)^2\alpha^4 + 1 = \alpha^5 + \alpha^3 + \alpha^6 + 1$$

$$= \alpha^2 + \alpha^4 + \alpha^3 + 1 + \alpha^4 + 1 = \alpha^3 + \alpha^2 + 1 + 1 = 1$$

olduğundan

$$\alpha^5 = \alpha^2 + (1 + \alpha + \alpha^2)$$

dir (Lidl ve Neiderreiter 1986).

Benzer şekilde hareket edilirse $\alpha^6 \in F_8$ elemanı, d_1, d_2, $d_3 \in F_2$ olmak üzere $\alpha^6 = d_1\alpha + d_2\alpha^2 + d_3(1 + \alpha + \alpha^2)$ biçimindedir. Burada d_1, d_2, d_3 katsayıları,

$$d_1 = \mathrm{Tr}_{F_8}(\alpha\alpha^6) = \mathrm{Tr}_{F_8}(\alpha^7) = \alpha^7 + \alpha^{14} + \alpha^{28} = \alpha^7 + (\alpha^7)^2 + (\alpha^7)^4 = 1,$$

$$d_2 = \mathrm{Tr}_{F_8}(\alpha^2\,\alpha^6) = \mathrm{Tr}_{F_8}(\alpha^8) = \alpha^8 + \alpha^{16} + \alpha^{32} = \alpha + \alpha^2 + \alpha^4 = \alpha + \alpha^2 + \alpha^3 + \alpha$$

$$= \alpha^2 + 1 + \alpha^2 = 1,$$

$$d_3 = \mathrm{Tr}_{F_8}((1 + \alpha + \alpha^2)\alpha^6) = \mathrm{Tr}_{F_8}(\alpha^6 + \alpha^7 + \alpha^8)$$

$$= \mathrm{Tr}_{F_8}(\alpha^6) + \mathrm{Tr}_{F_8}(\alpha^7) + \mathrm{Tr}_{F_8}(\alpha^8) = 0 + 1 + 1 = 0$$

biçiminde olduğundan

$$\alpha^6 = \alpha + \alpha\alpha^2 = \alpha + \alpha^3$$

dır.

F cisminin farklı *K* bazlarının sayısı oldukça fazladır, ancak bunlardan iki tanesi özel bir öneme sahiptir. Bunlardan ilki *F* cisminin *K* cismi üzerindeki bir α üretecinin kuvvetlerinden oluşan $\{1, \alpha, \alpha^2, ..., \alpha^{m-1}\}$ şeklindeki *polinom baz*dır. α elemanı genellikle *F* cisminin bir ilkel elemanı olarak alınır. Diğer tip baz ise *F* cisminin uygun bir elemanı ile oluşturulan *normal baz*dır.

2.3.11. Tanım. $K = \mathsf{F}_q$ ve $F = \mathsf{F}_q{}^m$ olmak üzere belli bir $\alpha \in F$ elemanı ve α elemanının K cismine göre eşleniklerinden oluşan $\{\alpha, \alpha^q, ..., \alpha^{q^{m-1}}\}$ kümesine F cisminin K üzerinde bir *normal bazı* denir (Lidl ve Neiderreiter 1986).

Örnek 2.3.10. göz önüne alınırsa $1 + \alpha + \alpha^2 = \alpha^4$ olduğundan $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ kümesi F_8 cisminin F_2 üzerindeki normal bazıdır.

2.3.12. Teorem (Artin Lemması). F bir cisim ve $\psi_1, ..., \psi_m$ bir G grubundan F^* çarpımsal grubuna tanımlı farklı homomorfizmler olmak üzere $a_1, ..., a_m$, F cisminin hepsi birden sıfır olmayan elemanları olsun. Bu durumda belli $g \in G$ elemanı için

$$a_1\psi_1(g) + ... + a_m\psi_m(g) \neq 0$$

dır (Lidl ve Neiderreiter 1986).

İspat. Bunu göstermek için m üzerine tümevarım uygulanırsa $m = 1$ için $a_1\psi_1(g) \neq 0$ olduğu açıktır. $m > 1$ olsun. $m - 1$ farklı homomorfizm teoremin hipotezini gerçeklesin. Teoremde belirtilen şekilde $\psi_1, ..., \psi_m$ homomorfizmleri ve $a_1, ..., a_m \in F$ alalım. Eğer $a_1 = 0$ için teoremin hipotezi gerçeklenir. O halde $a_1 \neq 0$ ve her $g \in G$ için

$$a_1\psi_1(g) + ... + a_m\psi_m(g) = 0 \qquad (2.5)$$

olsun. $\psi_1 \neq \psi_m$ olduğundan $a_1\psi_1(h) \neq a_m\psi_m(h)$ olacak şekilde bir $h \in G$ vardır. Bu durumda (2.5) eşitliğindeki g yerine hg yazılırsa her $g \in G$ için

$$a_1\psi_1(h)\psi_1(g) + ... + a_m\psi_m(h)\psi_m(g) = 0$$

elde edilir. Eşitliğin her iki tarafı $\psi_m(h)^{-1}$ ile çarpılırsa $1 \leq i \leq m - 1$ ve her $g \in G$ için $b_i = a_i\psi_i(h)\ \psi_m(h)^{-1}$ olmak üzere

$$b_1\psi_1(g) + ... + b_{m-1}\psi_{m-1}(g) + a_m\psi_m(g) = 0$$

elde edilir. (2.5) eşitliğinden bu son eşitlik çıkartılırsa $1 \leq i \leq m - 1$ ve her $g \in G$ için $c_i = a_i - b_i$ olmak üzere

$$c_1\psi_1(g) + ... + c_{m-1}\psi_{m-1}(g) = 0$$

olur. Bu ise $c_1 = a_1 - a_1\psi_1(h)\psi_m(h)^{-1} \neq 0$ olmasıyla çelişir.

2.3.13. Tanım. V, herhangi bir K cismi üzerinde tanımlı sonlu boyutlu bir vektör uzayı T, V üzerinde tanımlı bir lineer dönüşüm olmak üzere

$$f(x) = a_nx^n + ... + a_1x + a_0 \in K[x]$$

olsun. I ve 0, V üzerinde sırasıyla özdeşlik ve sıfır dönüşüm olmak üzere T lineer dönüşümü

$$a_nT^n + ... + a_1T + a_0I = 0$$

eşitliğini gerçekliyorsa $f(x)$ polinomuna T dönüşümünde *sıfırlanan polinom* denir. Bu özelliğe sahip olan en küçük dereceli monik polinom bir tektir ve bu polinoma T *dönüşümü için minimal polinom* denir.

Eğer $K[x]$ halkasında T dönüşümünü sıfırlayan bir başka $g(x) \in K[x]$ polinomu var ise $g(x) \mid f(x)$ dir. Özel olarak, Cayley-Hamilton Teoremi gereği, T dönüşümünün minimal polinomu T dönüşümünün $g(x)$ karakteristik polinomunu da böler. Burada $g(x) = det(xI - T)$ polinomudur ve bu polinom monik ve derecesi V vektör uzayının derecesine eşittir.

2.3.14. Tanım. V, herhangi bir K cismi üzerinde tanımlı sonlu boyutlu bir vektör uzayı olmak üzere T, V üzerinde tanımlı bir lineer dönüşüm olsun. $k = 0, 1, ...$ için $T^k\alpha$ vektörleri V uzayını geriyorsa $\alpha \in V$ vektörüne T dönüşümü için *devirli vektör* denir.

Lineer cebir teorisinden bundan sonraki çalışmalarda kullanılacak aşağıdaki teoremi hatırlatmakta fayda vardır.

2.3.15. Teorem. T, sonlu boyutlu bir V vektör uzayında bir lineer dönüşüm olsun. Bu durumda T dönüşümünün devirli bir vektöre sahip olması için gerek ve yeter koşul T dönüşümü için karakteristik ve minimal polinomlarının eşit olmasıdır (Lidl ve Neiderreiter 1986).

2.3.16. Teorem (Normal Baz Teoremi). K, herhangi bir sonlu cisim ve F, K cisminin herhangi bir sonlu genişlemesi ise F cisminin K cismi üzerinde bir normal bazı vardır (Neiderreiter 1986).

İspat. $m \geq 2$ olmak üzere $K = \mathbb{F}_q$ ve $F = \mathbb{F}_q{}^m$ ise Teorem 2.2.15. ve Uyarı 2.2.16. gereği, F cisminin K cismi üzerindeki farklı otomorfizmleri ι özdeşlik dönüşüm olmak üzere $\alpha \in \mathbb{F}_q{}^m$ için $\sigma(\alpha) = \alpha^q$ olarak tanımlanan $\iota, \sigma, \sigma^2, ..., \sigma^{m-1}$ dönüşümleridir. $\alpha, \beta \in F$ ve $c \in K$ için

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) \text{ ve } \sigma(c\alpha) = \sigma(c)\sigma(\alpha) = c\sigma(\alpha)$$

olduğundan F, K cismi üzerinde bir vektör uzayı olarak alınırsa σ dönüşümü F cismi üzerinde bir lineer dönüşüm olarak düşünülebilir. $\sigma^m = \iota$ olduğundan $x^m - 1 \in K[x]$ polinomu σ dönüşümünü sıfırlar. Eğer ι, σ, σ^2, ..., σ^{m-1} dönüşümleri F^* grubunun endomorfizmleri olarak düşünülür ve Artin Lemması uygulanırsa $K[x]$ halkasındaki derecesi m den küçük ve sıfırdan farklı hiçbir polinom σ dönüşümünü sıfırlamaz. Sonuç olarak, $x^m - 1$ polinomu, σ dönüşümünün minimal polinomudur.

σ dönüşümünün karakteristik polinomu derecesi m olan ve σ dönüşümünün minimal polinomu tarafından bölünebilen bir monik polinom olduğundan $x^m - 1$ polinomu aynı zamanda σ dönüşümünün karakteristik polinomudur. Lemma 2.3.13 gereği, α, $\sigma(\alpha)$, $\sigma^2(\alpha)$, ... F cismini gerecek şekilde bir $\alpha \in F$ vardır. Tekrar eden elemanlar atılırsa α, $\sigma(\alpha)$, $\sigma^2(\alpha)$, ..., $\sigma^{m-1}(\alpha)$ dönüşümleri F cismini gerer ve böylece F cisminin bir K bazı olur. Bu baz, α ve α nın K cismine göre eşleniklerinden oluştuğundan F nin K üzerindeki normal bazıdır.

Şimdi verilen bir kümenin bir cisim genişlemesi için bir baz olup olmadığının belirlenmesi için bir yöntem verilecektir.

2.3.17. Tanım. K bir sonlu cisim ve F, K cisminin derecesi m olan bir cisim genişlemesi olsun. Bu durumda α_1, ..., $\alpha_m \in F$ *elemanlarının diskriminantı* $\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ ile gösterilir ve

$$\Delta_{F/K}(\alpha_1, ..., \alpha_m) = \begin{vmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_m) \\ \mathrm{Tr}_{F/K}(\alpha_2\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_2\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}_{F/K}(\alpha_m\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_m\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_m\alpha_m) \end{vmatrix}$$

biçimindeki m mertebeli determinat olarak tanımlanır.

Tanıma dikkat edilirse $\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ her zaman K cisminin bir elemanıdır.

2.3.18. Teorem. K bir sonlu cisim, F, K cisminin derecesi m olan bir cisim genişlemesi ve $\alpha_1, ..., \alpha_m \in F$ olsun. Bu durumda $\{\alpha_1, ..., \alpha_m\}$ kümesinin F cisminin bir K bazı olması için gerek ve yeter koşul $\Delta_{F/K}(\alpha_1, ..., \alpha_m) \neq 0$ olmasıdır (Lidl ve Neiderreiter 1986)

İspat. $\{\alpha_1, ..., \alpha_m\}$ kümesi F cisminin bir K bazı olsun. $\Delta_{F/K}(\alpha_1, ..., \alpha_m) \neq 0$ olduğunu göstermek için diskriminant tanımındaki satır vektörlerinin lineer bağımsız olduğunu gösterilmelidir. $c_1, ..., c_m \in K$ olmak üzere $1 \leq j \leq m$ için

$$c_1 \mathrm{Tr}_{F/K}(\alpha_1\alpha_j) + ... + c_m \mathrm{Tr}_{F/K}(\alpha_m\alpha_j) = 0$$

olduğunu varsayalım. Bu durumda

$$\beta = c_1\alpha_1 + ... + c_m\alpha_m$$

olmak üzere $\alpha_1, ..., \alpha_m$ elemanları F cismini gerdiğinden $1 \leq j \leq m$ için $\mathrm{Tr}_{F/K}(\beta\alpha_j) = 0$ dır. Böylece her $\alpha \in F$ için $\mathrm{Tr}_{F/K}(\beta\alpha) = 0$ olur. Bu ise sadece $\beta = 0$ olması ile mümkün olduğundan $c_1\alpha_1 + ...+ c_m\alpha_m = 0$ olması $c_1 = \cdots = c_m = 0$ olmasını gerektirir.

Tersine $\Delta_{F/K}(\alpha_1, ..., \alpha_m) \neq 0$ ve belli $c_1, ..., c_m \in K$ için $c_1\alpha_1 + ... + c_m\alpha_m = 0$ olduğu varsayalım. Bu durumda $1 \leq j \leq m$ için

$$c_1\alpha_1\alpha_j + ... + c_m\alpha_m\alpha_j = 0$$

olur. Bu son eşitliğe iz fonksiyonu uygulanırsa $1 \leq j \leq m$ için

$$c_1 \mathrm{Tr}_{F/K}(\alpha_1\alpha_j) + ... + c_m \mathrm{Tr}_{F/K}(\alpha_m\alpha_j) = 0$$

eşitliği elde edilir. Ancak diskriminant tanımındaki satır vektörleri lineer bağımsız olduğundan $c_1 = \cdots = c_m = 0$ olmaldır. Dolayısıyla $\alpha_1, ..., \alpha_m$ elemanları, K cismi üzerinde lineer bağımsızdır.

$\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ diskriminantı ile aynı işlevi gören m mertebeli başka bir determinant ise F cisminin bir genişlemesinin elemanları ile oluşturulan determinanttır. q, K cisminin eleman sayısı olmak üzere, $\alpha_1, ..., \alpha_m \in F$ için A matrisi, i. satır ve j. sütunu $\alpha_j^{q^{i-1}}$ şeklinde olan $m \times m$ lik bir matris olsun. A^T, A matrisinin transpozu ve B matrisi, i. satır ve j. sütunu $\mathrm{Tr}_{F/K}(\alpha_i\alpha_j)$ olan $m \times m$ lik bir matris olmak üzere $A^TA = B$ dir. Eşitliğin her iki tarafının determinantı alınırsa

$$\Delta_{F/K}(\alpha_1, ..., \alpha_m) = \det(A)^2$$

eşitliği elde edilir.

Aşağıda Teorem 2.3.18. nin bir sonucu verilmektedir. Bu sonuç normal bazın belirlenmesinde kolaylık sağlar.

2.3.19. Sonuç. $\alpha_1, ..., \alpha_m \in \mathsf{F}_q{}^m$ olsun. Bu durumda $\{\alpha_1, ..., \alpha_m\}$ kümesinin $\mathsf{F}_q{}^m$ cisminin bir F_q bazı olması için gerek ve yeter koşul

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_m^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \cdots & \alpha_m^{q^{m-1}} \end{vmatrix} \neq 0$$

olmasıdır (Lidl ve Neiderreiter 1986) .

Şimdi $\alpha \in \mathsf{F}_q{}^m$ için $\{\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}\}$ kümesinin $\mathsf{F}_q{}^m$ cisminin F_q cismi üzerindeki bir normal bazı olması için gerek ve yeter koşul verilecektir. Bunun için verilecek teoremin ispatında kullanılacak olan iki polinomun bileşkesi kavramını hatırlayalım: F bir cisim, $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n \in K[x]$ ve $g(x) = b_0x^m + b_1x^{m-1} + ... + b_m \in K[x]$ dereceleri sırasıyla n ve m olan iki polinom olmak üzere $f(x)$ ve $g(x)$ polinomunlarının bileşkesi $R(f, g)$ ile gösterilir ve

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_n & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_n \end{vmatrix} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} m\ satir \\ \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} n\ satir \end{matrix}$$

biçimindeki $m + n$ mertebeli determinant olarak tanımlanır.

2.3.20. Teorem. $\alpha \in \mathsf{F}_q{}^m$ olmak üzere $\{\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}\}$ kümesinin $\mathsf{F}_q{}^m$ cisminin F_q üzerindeki bir normal bazı olması için gerek ve yeter koşul

$$x^m - 1 \in \mathsf{F}_q{}^m[x] \quad \text{ve} \quad \alpha x^{m-1} + \alpha^q x^{m-2} + ... + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}} \in \mathsf{F}_q{}^m[x]$$

polinomlarının aralarında asal olmasıdır (Lidl ve Neiderreiter 1986).

İspat. $\alpha_1 = \alpha, \alpha_2 = \alpha^q, ..., \alpha_m = \alpha^{q^{m-1}}$ alınır ve Sonuç 2.3.20. deki determinatın satırları yeniden düzenlenirse

$$\pm\begin{vmatrix} \alpha & \alpha^{q} & \alpha^{q^2} & \cdots & \alpha^{q^{m-1}} \\ \alpha^{q^{m-1}} & \alpha & \alpha^{q} & \cdots & \alpha^{q^{m-2}} \\ \alpha^{q^{m-2}} & \alpha^{q^{m-1}} & \alpha & \cdots & \alpha^{q^{m-3}} \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha^{q} & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha \end{vmatrix}$$

determinantı elde edilir. $f(x) = x^m - 1$ ve $g(x) = \alpha x^{m-1} + \alpha^q x^{m-2} + \ldots + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}}$ sırasıyla dereceleri m ve $m - 1$ olan polinomlar olmak üzere bu polinomların bileşkesi $R(f, g)$, mertebesi $2m - 1$ olan bir determinanttır. Bu determinanttaki $(m + 1)$. sütun birinci sütuna, $(m + 2)$. sütun ikinci sütuna eklenip bu şekilde devam edilir ve son olarak $(2m - 1)$. sütun $(m - 1)$. sütuna eklenirse bileşke determinant, yukarıdaki determinantla birlikte esas köşegeni -1 lerden oluşan $m - 1$ mertebeli köşegen matrislere ayrılır. Dolayısıyla $R(f, g)$ determinantı işaretten bağımsız olarak yukarıdaki determinanta eşittir. Teoremin ispatı Sonuç 2.3.20. den ve "$R(f, g) \neq 0$ olması için gerek ve yeter koşul f ve g polinomlarının aralarında asal olmasıdır" gerçeği kullanılarak tamamlanır.

Bir önceki teoreme dayanarak normal baz teoreminin geliştirilmiş hali ispatsız verilebilir.

2.3.21. Teorem. *K*, herhangi bir sonlu cisim ve *F*, *K* cisminin herhangi bir sonlu genişlemesi ise *F* cisminin *K* cismi üzerinde *F* cisminin ilkel elemanlarından oluşan bir normal bazı vardır (Lidl ve Neiderreiter 1986).

2.4. Birimin Kökleri ve Döngüsel Polinomlar

Bu kısımda *n*, pozitif bir tamsayı olmak üzere $x^n - 1$ polinomunun herhangi bir *K* cismi üzerindeki parçalanma cismi incelenecek ve birimin *kökleri* kavramı genelleştirilecektir. *K* cisminin herhangi bir cisim olması durumunda birimin *n.* köklerinin temel özellikleri incelenecektir. Bu nedenle teoremlerde karakteristiği *p* olan bir *K* cismi için $p = 0$ olması hali de söz konusu olacaktır.

2.4.1. Tanım. n bir pozitif tamsayı ve K bir cisim olsun. $p(x) = x^n - 1 \in K[x]$ polinomunun K cismi üzerindeki parçalanma cismine *K cismi üzerinde n. döngüsel cisim* (veya *K cisminin n. döngüsel genişlemesi*) denir ve $K^{(n)}$ ile gösterilir.

$x^n - 1 \in K[x]$ polinomunun $K^{(n)}$ cismindeki köklerine de *K cismi üzerinde birimin n. kökleri* denir ve tüm bu köklerin kümesi de $E^{(n)}$ ile gösterilir.

Aşağıdaki teoremde, $E^{(n)}$ kümesinin yapısı, n pozitif tamsayısı ile K cisminin karakteristiği arasındaki ilişki ile belirlenecek ve üstelik $K^{(n)}$ cisminin K cisminin bir Galois genişlemesi olduğu görülecektir.

2.4.2. Teorem. n bir pozitif tamsayı ve K, karakteristiği p olan bir cisim olsun. Bu durumda

i) $kar(K) \nmid n$ ise $E^{(n)}$ kümesi, $K^{(n)}$ cisminden indirgenen çarpma işlemine göre mertebesi n olan devirli bir gruptur.

ii) $kar(K) \mid n$ ise m ve e birer pozitif tamsayı, $p \nmid m$ olmak üzere $n = mp^e$ olsun. Bu durumda

$$K^{(n)} = K^{(m)} \text{ ve } E^{(n)} = E^{(m)}$$

dir ve $x^n - 1$ polinomunun $K^{(n)}$ cismindeki kökleri, $E^{(m)}$ kümesinin katlılığı p^e olan m tane elemanlarıdır.

iii) $K^{(n)}$ cismi, K cisminin bir Galois genişlemesidir (Lidl ve Neiderreiter 1986).

İspat. *i)* $p(x) = x^n - 1$ olsun. Eğer $n = 1$ ise $E^{(1)} = \{1\}$ olduğundan teorem doğrudur. O halde $n > 1$ olsun. Bu durumda $p(x) = x^n - 1$ polinomunun türevi olan $p'(x) = nx^{n-1}$ polinomunun $K^{(n)}$ cismindeki tek kökü 0 olduğundan $p(x)$ ve $p'(x)$ polinomlarının ortak kökü yoktur. Böylece Teorem 1.1.11. gereği, $x^n - 1$ polinomunun katlı kökü yoktur ve dolayısıyla $E^{(n)}$ kümesinin n tane elemanı vardır. Şimdi $\theta, \eta \in E^{(n)}$ olmak üzere

$$(\theta\eta^{-1})^n = \theta^n(\eta^n)^{-1} = 1$$

olduğundan $\theta\eta^{-1} \in E^{(n)}$ dir. Dolayısıyla $E^{(n)}$ kümesi, $K^{(n)}$ cisminden indirgenen çarpma işlemine göre n mertebeli bir çarpımsal gruptur. n tamsayısının asal çarpanlarına ayrımı

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

olsun. Bu durumda $1 \le i \le t$ özelligindeki her i için $x^{n/p_i} - 1$ polinomunun bir kökü olmayan bir $\alpha_i \in E^{(n)}$ elemanı vardır. Böylece $\beta_i = \alpha_i^{n/p^{e_i}}$ elemanlarının mertebesi $p_i^{e_i}$ dir ve dolayısıyla $E^{(n)}$, $\zeta = \beta_1\beta_2 \cdots \beta_t$ üreteçli devirli bir gruptur.

ii) $p(x) = x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}$ eşitliğinden ve (i) özelliğinden kolayca görülebilir.

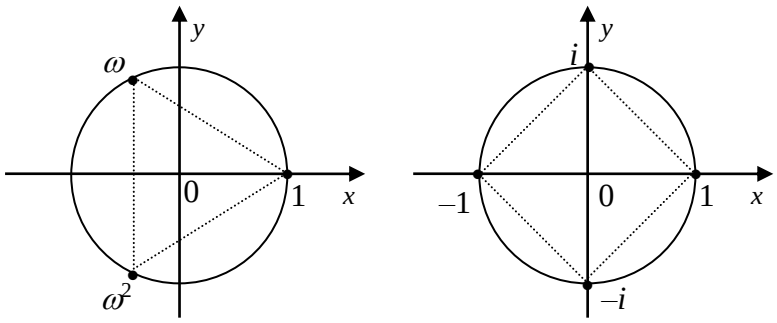
iii) Tanım 2.4.1. gereği, $K^{(n)}$ cismi $p(x)$ polinomunun K cismi üzerinde parçalanma cismidir. Bundan başka, $p(x)$ polinomu K cismi üzerinde ayrılabilir bir polinom olduğudan $K^{(n)}$ cismi K cisminin bir ayrılabilir cisim genişlemesidir. Dolayısıyla $K^{(n)}$ cismi, K cisminin bir Galois genişlemesidir.

2.4.3. Örnek. $p(x) = x^3 - 1 \in \mathbb{Q}[x]$ polinomunun $\mathbb{Q}$ cismi üzerindeki parçalanma cismi $\mathbb{Q}^{(3)} = \mathbb{Q}(\omega)$ dır. Gerçektende $p(x)$ polinomu $\mathbb{Q}(\omega)$ cismi üzerinde

$$p(x) = (x - 1)(x - \omega)(x - \omega^2)$$

biçiminde lineer çarpanlarına ayrılabilir ve üstelik $\mathbb{Q}(\omega)$ cismi $p(x)$ polinomunun tüm sıfırlarını ve $\mathbb{Q}$ cismini bulunduran $\overline{\mathbb{Q}}$ cisminin en küçük alt cisimdir. Benzer biçimde $q(x) = x^4 - 1 \in \mathbb{Q}[x]$ polinomunun $\mathbb{Q}$ cismi üzerindeki parçalanma cismi $\mathbb{Q}^{(4)} = \mathbb{Q}(i)$ dir.

2.4.4. Uyarı. Birimin n. kökleri düzlemde birim çember üzerinde bulunurlar ve bir köşesi 1 de bulunan n-kenarlı düzgün çokgen oluştururlar. Aşağıdaki şekilde birimin üçüncü köklerinin bir eşkenar üçgen ve birimin dördüncü köklerinin bir kare üzerindeki dağılımı görülmektedir.



Şekil 2.3. Birimin üçüncü ve dördüncü kökleri.

2.4.5. Tanım. K karakteristiği p olan bir cisim ve n, $p \nmid n$ özelliğinde bir tamsayı olsun. Bu durumda $E^{(n)}$ devirli grubunun bir üretecine *birimin K cismi üzerinde n. ilkel kökü* denir.

Yukarıdaki tanıma dikkat edilirse K cismi üzerinde birimin farklı n. ilkel köklerinin sayısı tam olarak $\phi(n)$ tane olduğu görülür. Eğer ζ, birimin bir n. ilkel kökü ise $1 \leq k \leq n$ ve $(k, n) = 1$ olmak üzere birimin tüm n. ilkel kökleri ζ^k elemanlarıdır, yani birimin tüm n. ilkel köklerinin kümesi

$$\{\zeta^k \mid 1 \leq k \leq n, (k, n) = 1\}$$

dır.

2.4.6. Örnek 1. $K = \mathbb{Q}$ cismi için birimin 3. ilkel kökleri ω ve ω^2 ve birimin 4. ilkel kökleri i ve $-i$ dir.

2. $K = \mathbb{Z}_7$ olarak alalım. Teorem 2.1.5. gereği, $\mathbb{Z}_7^*$ grubu devirlidir ve bu grubun mertebesi 6 dır. Dolayısıyla Lagrange Teoremi gereği, $5 \in \mathbb{Z}_7^*$ elemanının mertebesi 6 sayısını böler. O halde 5 elemanının mertebesi 2, 3 veya 6 olabilir. Bundan başka,

$$5^2 = 4, \quad 5^3 = 6$$

olduğundan 5 elemanının mertebesi 2 ve 3 olamaz. O halde $5^6 = 1$ olduğundan 5 elemanı $\mathbb{Z}_7$ cisminde birimin 6. ilkel köküdür. Diğer ilkel kökler ise $(k, 6) = 1$ olacak şekildeki k tamsayıları için 5^k biçiminde olduğundan bu eleman $5^5 = 3$ tür.

3. $K = \mathbb{Z}_{11}$ olarak alalım. Teorem 2.1.5. gereği, $\mathbb{Z}_{11}^*$ grubu devirlidir ve bu grubun mertebesi 10 dur. Dolayısıyla, Lagrange Teoremi gereği, $2 \in \mathbb{Z}_{11}^*$ elemanının mertebesi 10 sayısını böler. O halde 2 elemanının mertebesi 2, 5 veya 10 olabilir. Diger yandan

$$2^2 = 4, \quad 2^4 = 5, \quad 2^5 = (2)(5) = 10 = -1$$

olduğundan 2 elemanının mertebesi 2 ve 5 olamaz. Diğer yandan $2^{10} = 1$ olduğundan 2 elemanı $\mathbb{Z}_{11}$ cisminde birimin 10. ilkel köküdür. Diğer ilkel kökler ise $(k, 10) = 1$ olacak şekildeki k tamsayıları için 2^k biçiminde olduğundan bu elemanlar

$$2^1 = 2, \quad 2^3 = 8, \quad 2^7 = 7, \quad 2^9 = 6$$

dır (Fraleigh 2003).

2.4.7. Tanım. *K* karakteristiği *p* olan bir cisim, *n*, $p \nmid n$ özelliğinde bir tamsayı ve ζ, *K* cismi üzerinde birimin *n*. ilkel kökü olmak üzere

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n} (x - \zeta^k)$$

polinomuna *K* cismi üzerinde *n*. *döngüsel polinom* denir.

2.4.8. Uyarı 1. Tanıma dikkat edilirse, $\Phi_n(x)$ polinomu ζ elemanının seçiminden bağımsızdır ve $\Phi_n(x)$ polinomunun derecesi $\phi(n)$ dir.

2. $\Phi_n(x)$ polinomunun katsayıları, *K* cismi üzerinde *n*. döngüsel cisim yani, $K^{(n)}$ cisminin elemanlarıdır. Aşağıdaki teoremde gerçekte $\Phi_n(x)$ polinomunun katsayılarının *K* cisminin asal cisminin elemanları olduğu görülecektir.

3. Bundan sonra, *n* ve *d* birer pozitif tamsayı olmak üzere $d \mid n$ özelliğindeki tüm *d* sayıları alınarak yapılacak çarpımı göstermek için $\prod_{d|n}$ sembolü kullanılacaktır.

2.4.9. Teorem. *K*, karakteristiği *p* olan bir cisim ve *n*, $p \nmid n$ olacak şekilde bir tamsayı olsun. Bu durumda;

i) $x^n - 1 = \prod_{d|n} \Phi_d(x)$ dir.

ii) $\Phi_n(x)$ polinomunun katsayıları, *K* cisminin asal cisminin elemanlarıdır. Eğer *K* cisminin asal cismi $\mathbb{Q}$ ise $\Phi_n(x)$ polinomunun katsayıları $\mathbb{Z}$ halkasına aittir. (Lidl ve Neiderreiter 1986)

İspat *i)* *K* cismi üzerindeki birimin her bir *n*. kökü, *n* sayısının tam olarak bir pozitif *d* böleni için *K* cismi üzerinde birimin *d*. ilkel köküdür. Eğer ζ, *K* cismi üzerinde birimin *n*. ilkel kökü ve ζ^k, *K* cismi üzerinde birimin keyfi bir *n*. kökü ise $d = \frac{n}{(k,n)}$ dir, yani *d* sayısı ζ^k elemanının $E^{(n)}$ grubundaki mertebesidir.

$$x^n - 1 = \prod_{k=1}^{n} (x - \zeta^k)$$

olduğundan ζ^k, K cismi üzerinde birimin d. ilkel kökü olmak üzere $x - \zeta^k$ çarpanları düzenlenerek

$$x^n - 1 = x^n - 1 = \prod_{d|n} \Phi_d(x)$$

eşitliği elde edilir.

***ii*)** Bunu göstermek için n sayısı üzerine tümevarım uygulamak yeterlidir. Dikkat edilirse $\Phi_n(x)$ polinomu bir monik polinomdur. $n = 1$ için $\Phi_1(x) = x - 1$ olduğundan iddia doğrudur. O halde $n > 1$ ve $1 \leq d < n$ olmak üzere önerme tüm $\Phi_d(x)$ polinomları için doğru olsun. Bu durumda (*i*) özelliğinden, $p(x) = \prod_{d|n,\, d<n} \Phi_d(x)$ olmak üzere

$$\Phi_n(x) = \frac{x^n - 1}{p(x)}$$

tir. Tümevarım hipotezi gereği, $p(x)$ polinomunun katsayıları K cisminin asal cisminin elemanları veya $K = \mathbb{Q}$ ise $\mathbb{Z}$ halkasının elemanlarıdır. O halde, $x^n - 1$ polinomu $p(x)$ polinomu ile uzun bölme işlemi yapılırsa, $\Phi_n(x)$ polinomunun katsayılarının sırasıyla, K cismine ait asal cisme veya $\mathbb{Z}$ halkasına ait olduğu görülmüş olur.

2.4.10. Örnek 1. r bir asal sayı ve $k \in \mathbb{N}$ olsun. Bu durumda

$$\Phi_{r^k}(x) = \frac{x^{r^k} - 1}{\Phi_1(x)\Phi_r(x)\cdots\Phi_{r^{k-1}}(x)} = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}$$

olduğundan Teorem 2.4.9 (*i*) gereği,

$$\Phi_{r^k}(x) = x^{(r-1)r^{k-1}} + x^{(r-2)r^{k-1}} + \cdots + 1$$

dir. O halde, $k = 1$ için

$$\Phi_r(x) = x^{r-1} + x^{r-2} + \cdots + x + 1$$

olduğu elde edilir. Dolayısıyla $r = 2$, 3, 5 ve 7 için $\Phi_r(x)$ polinomları sırasıyla,

$\Phi_2(x) = x + 1$,

$\Phi_3(x) = x^2 + x + 1$,

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$,

$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

biçimindedir.

2. r sayısının asal olmadığı durumlarda $\Phi_r(x)$ polinomları uzun bölme işlemi yapılarak bulunabilir. Dolayısıyla r = 1, 4, 6, 9 ve 10 için $\Phi_r(x)$ polinomları sırasıyla,

$$\Phi_1(x) = x - 1,$$

$$\Phi_4(x) = \frac{x^4 - 1}{(x-1)(x+1)} = x^2 + 1,$$

$$\Phi_6(x) = \frac{x^6 - 1}{(x-1)(x+1)(x^2 + x + 1)} = x^2 - x + 1,$$

$$\Phi_8(x) = \frac{x^8 - 1}{(x-1)(x+1)(x^2 + 1)} = x^4 + 1,$$

$$\Phi_9(x) = \frac{x^9 - 1}{(x-1)(x^2 + x + 1)} = x^6 + x^3 + 1,$$

ve

$$\Phi_{10}(x) = \frac{x^{10} - 1}{(x-1)(x+1)(x^4 + x^3 + x^2 + x + 1)} = x^4 - x^3 + x^2 - x + 1$$

biçimindedir.

2.4.11. Teorem. $K^{(n)}$ cismi döngüsel cismi, K cisminin bir basit cebirsel genişlemesidir. Bundan başka, $(q, n) = 1$ olmak üzere $K = \mathsf{F}_q$ ise $\Phi_n(x)$ döngüsel polinomu $K[x]$ halkasında $\phi(n)/d$ sayıda, dereceleri d olan farklı monik indirgenemez polinomların çarpımı şeklinde yazılabilir. $K^{(n)}$ cismi bu indirgenemez çarpanların K cismi üzerindeki parçalanma cismidir. Üstelik d, $q^d \equiv 1 \pmod{n}$ olacak şekildeki en küçük pozitif tamsayı olmak üzere $[K^{(n)} : K] = d$ dir (Lidl ve Neiderreiter 1986).

İspat. ζ, birimin K cismi üzerinde n.ilkel kökü olmak üzere $K^{(n)} = K(\zeta)$ dır, yani $K^{(n)}$ cismi K cisminin bir basit cebirsel genişlemesidir.

η, F_q cismi üzerinde birimin n. ilkel kökü olsun. Bu durumda $\eta \in \mathsf{F}_q{}^k$ olması için gerek ve yeter koşul $\eta^{q^k} = \eta$ olmasıdır. Bu ise $q^k \equiv 1 \pmod{n}$ olduğunu gösterir. Bu özellikteki en küçük pozitif tamsayı $k = d$ olduğundan $\eta \in \mathsf{F}_q{}^d$ dir. Bununla birlikte, η, $\mathsf{F}_q{}^d$ cisminin hiçbir has alt cisminde bulunmaz. Bundan dolayı η elemanının F_q cismi üzerindeki minimal polinomunun derecesi d dir ve η, Φ_n polinomunun herhangi bir kökü olduğundan istenen elde edilir.

2.4.12. Örnek. $K = \mathsf{F}_{11}$ olmak üzere $\Phi_{12}(x) = x^4 - x^2 + 1 \in \mathsf{F}_{11}[x]$ polinomunu $\mathsf{F}_{11}[x]$ halkasında indirgenemez polinomların çarpımı olarak

$$\Phi_{12}(x) = (x^2 + 5x + 1)(x^2 - 5x + 1)$$

biçiminde çarpanlarına ayrılabilir. Böylece, $K^{(12)} = \mathsf{F}_{121}$ dir.

Döngüsel polinomlar ve sonlu cisimler arasındaki bir başka ilişki aşağıdaki teoremde verilmiştir.

2.4.13. Teorem. F_q sonlu cismi, kendisinin herhangi bir alt cismi üzerinde $(q - 1)$. döngüsel cismidir.

İspat. F_q cisminin sıfırdan farklı tüm elemanları, $x^{q-1} - 1$ polinomunun kökleri olduğundan $x^{q-1} - 1$ polinomu F_q cismi üzerinde parçalanır. Üstelik bu polinom F_q cisminin hiç bir has alt cismi üzerinde parçalanmadığından F_q cismi, $x^{q-1} - 1$ polinomunun kendisinin herhangi bir alt cismi üzerindeki parçalanma cismidir. F_q^*, $q - 1$ mertebeli devirli bir gruptur. O halde Teorem 1.1.1. gereği, $n \mid (q - 1)$ olacak biçimdeki n pozitif sayısı için F_q^* grubunun n mertebeli bir $\{1, \alpha, ..., \alpha^{n-1}\}$ alt grubu vardır. Bu alt grubun tüm elemanları F_q cisminin herhangi bir alt cismi üzerinde birimin n. kökleridir ve α üreteci, F_q cisminin herhangi bir alt cismi üzerinde birimin n. ilkel köküdür.

2.4.14. Teorem. n, bir pozitif tamsayı ve $1 \leq d < n$ olmak üzere $d \mid n$ ise $\Phi_n(x)$ polinomu $\frac{x^n - 1}{x^d - 1}$ polinomunu böler (Lidl ve Neiderreiter 1986).

İspat. Teorem 2.4.9. gereği, $\Phi_n(x)$ polinomu

$$x^n - 1 = (x^d - 1)\frac{x^n - 1}{x^d - 1}$$

polinomunu böler. d sayısı, n tamsayısının bir has böleni olduğundan $\Phi_n(x)$ ve $x^d - 1$ polinomlarının ortak kökü yoktur, yani $(\Phi_n(x), x^d - 1) = 1$ dir. Dolayısıyla $\Phi_n(x)$ polinomu $\frac{x^n - 1}{x^d - 1}$ polinomunu böler.

2.5. Sonlu Cisimlerin Elemanlarının Gösterimi

Bu kısımda, F_q karakteristiği p olan ve $q = p^n$ elemanlı sonlu bir cisim olmak üzere, F_q cisminin elemanlarının üç farklı gösterimi belirlenecektir.

Sonuç 2.1.7. gereği, F_q, F_p cisminin bir basit cebirsel genişlemesidir. Gerçekten de, $f(x)$ polinomu, $\mathsf{F}_p[x]$ halkasında n. dereceden indirgenemez bir polinom ise Teorem 2.1.6. gereği $f(x)$ polinomunun bir $\alpha \in \mathsf{F}_q$ kökü vardır. Dolayısıyla $\mathsf{F}_q = \mathsf{F}_p(\alpha)$ tir. Böylece F_q cisminin her β elemanı $0 \leq i \leq n$ için $c_i \in \mathsf{F}_p$ olmak üzere

$$\beta = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}$$

biçimde tek türlü ifade edilebilir.

2.5.1. Örnek. $f(x) = x^2 + 1 \in \mathsf{F}_3[x]$, bir monik indirgenemez polinomdur. α, $f(x)$ polinomunun F_3 cisminin bir cisim genişlemesindeki bir kökü olmak üzere, F_9 cismi, F_3 cismine α elemanını katarak elde edilen $\mathsf{F}_3(\alpha)$ cismi olarak düşünülebilir. Diğer yandan F_9 cismi, F_3 cismi üzerinde 2 boyutlu bir vektör uzayı ve $f(\alpha) = \alpha^2 + 1 = 0$ olduğundan ve F_9 cisminin 9 elemanı $a_0, a_1 \in \mathsf{F}_3$ olmak üzere $a_0 + a_1\alpha$ formundadır, yani

$$\mathsf{F}_9 = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\}$$

dır. F_9 cisminin işlem tablosu daha önce verilmişti.

F_q cisminin elemanlarının başka bir gösterimi de döngüsel polinomlar yardımıyla elde edilebilir. F_q, F_p cismi üzerinde $(q - 1)$. döngüsel cisim olduğundan F_q cismi $(q - 1)$. döngüsel polinom yani, $\Phi_{q-1} \in \mathsf{F}_p[x]$ polinomunun $\mathsf{F}_p[x]$ halkasında aynı dereceli indirgenemez polinomların çarpımı şeklinde yazılmasıyla oluşturulabilir. Bu durumda indirgenemez çarpanlardan herhangi birinin bir kökü aynı zamanda F_p cismi üzerinde birimin $(q - 1)$. ilkel kökü olacağından F_q cisminin de bir ilkel elemanı olur. Böylece F_q cismi, 0 elemanı ve bu ilkel elemanın uygun kuvvetlerinden oluşur.

2.5.2. Örnek. F_9 cismi, F_3 cismi üzerinde 8. döngüsel cisim olduğundan $\mathsf{F}_9 = \mathsf{F}_3^{(8)}$ olarak yazılabilir. $\Phi_8 = x^4 + 1 \in \mathsf{F}_3[x]$ polinomu $\mathsf{F}_3[x]$ halkasında

$$\Phi_8 = (x^2 + x + 2)(x^2 + 2x + 2)$$

biçiminde indirgenemez polinomların çarpımı biçiminde yazılabilir. Eğer ζ, $x^2 + x + 2$ polinomunun bir kökü ise ζ, F_3 cismi üzerinde birimin 8. ilkel köküdür. Böylece F_9 cisminin sıfırdan farklı tüm elemanları, ζ elemanının kuvvetleri şeklinde yazılabilir. Dolayısıyla

$$\mathsf{F}_9 = \{0, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^7, \zeta^8\}$$

dir. Örnek 2.5.1. deki gösterimle ilişkilendirilecek olursa, $x^2 + x + 2 \in \mathsf{F}_3[x]$ polinomunun bir kökü $\zeta = 1 + \alpha$ elemanıdır. Böylece F_9 cisminin sıfırdan farklı elemanları, ζ elemanının kuvvetlerine göre indeks tablosunda şu şekilde gösterilebilir;

Çizelge 2.4. ζ elemanının kuvvetlerine göre indeks tablosu

i	1	2	3	4	5	6	7	8
ζ^i	$1 + \alpha$	2α	$1 + 2\alpha$	2	$2 + 2\alpha$	α	$2 + \alpha$	1

Yukarıdaki tabloya dikkat edilirse Örnek 2.5.1. deki aynı elemanlar elde edilmiştir.

F_q cisminin elemanlarının üçüncü bir gösterimi de matrislerle elde edilir. Sabit olmayan n dereceli monik bir $f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + x^n$ polinomunun $n \times n$ lik eş matrisi

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

biçimindedir. Bundan başka A matrisi, I, $n \times n$ lik birim matris olmak üzere $f(A) = 0$ eşitliğini gerçekler, yani,

$$a_0I + a_1A + ... + a_{n-1}A^{n-1} + A^n = 0$$

dır. Böylece, A, F_p cismi üzerinde derecesi n olan monik indirgenemez bir polinomun eş matrisi ise $f(A) = 0$ dır. Burada A matrisi, $f(x)$ polinomunun bir kökü gibi hareket eder. A matrisinin içindeki derecesi n sayısından küçük diğer polinomlar, F_q cisminin elemanlarının gösterimlerini verir.

2.5.3. Örnek. $f(x) = x^2 + 1 \in \mathsf{F}_3[x]$ polinomunun eş matrisi,

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

dır. Böylece F_9 cismi, $\mathsf{F}_9 = \{0, I, 2I, A, I + A, 2I + A, 2A, I + 2A, 2I + 2A\}$ biçiminde ifade edilebilir. Burada

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad 2I = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},$$

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \qquad I + A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \qquad 2I + A = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix},$$

$$2A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \qquad I + 2A = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \qquad 2I + 2A = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$$

dir. Bu şekilde verilen F_9 cisminde yapılacak matris işlemleri genel matrislerle aynı özelliklere sahiptir. Örneğin,

$$(2I + A)(I + 2A) = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} = 2A$$

dır.

Aynı şekilde, Φ_{q-1} döngüsel polinomunun $\mathsf{F}_p[x]$ halkasında çarpanlarına ayrılması yöntemi F_q cisminin elemanlarının matrisler yadımıyla gösterimi için de uygulanabilir.

2.5.4. Örnek. Hatırlanacağı gibi $p(x) = x^2 + x + 2 \in \mathsf{F}_3[x]$ polinomu, $\Phi_8 \in \mathsf{F}_3[x]$ polinomunun bir indirgenemez çarpanıdır. Bundan başka $p(x)$ polinomunun eş matrisi

$$C = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$$

dir. Böylece F_9 cismi

$$\{0, C, C^2, C^3, C^4, C^5, C^6, C^7, C^8\}$$

biçiminde ifade edilebilir. Burada

$$0=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix},\quad C=\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix},\quad C^2=\begin{pmatrix}1 & 2\\ 2 & 2\end{pmatrix}$$

$$C^3=\begin{pmatrix}2 & 2\\ 2 & 0\end{pmatrix},\quad C^4=\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix},\quad C^5=\begin{pmatrix}0 & 2\\ 2 & 1\end{pmatrix}$$

$$C^6=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix},\quad C^7=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix},\quad C^8=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

dir. Buradaki matris işlemleri, genel matris işlemleri gibidir. Örneğin,

$$C^6+C=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}+\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}=\begin{pmatrix}2 & 2\\ 2 & 0\end{pmatrix}=C^3$$

dır.

3. SONLU CİSİMLER ÜZERİNDE POLİNOMLAR

Bu bölümde sonlu cisimler üzerinde polinomlar ele alınacaktır. Kısım 3.1. de polinomların mertebeleri ve ilkel polinom kavramı ele alınacaktır. Daha sonra bir polinomun indirgenemezliği kavramı ve verilen bir polinomun bir cisim genişlemesindeki minimal polinomunun belirlenmesi üzerinde durulacaktır. Kısım 3.2. de sonlu cisimler üzerinde tanımlı monik indirgenemez polinomların sayısı bazı özel fonksiyonlar yardımıyla ifade edilecektir.

3.1. Polinomların Mertebeleri ve İlkel Polinomlar

Bu kısımda ilk olarak bir polinomun mertebesi kavramı ele alınacak daha sonra ilkel elemanların minimal polinomları ve verilen bir derece için olabilecek en yüksek mertebeli polinomlar arasındaki ilişkiler incelenecektir. Ayrıca, bir polinomun indirgenemezliği ve verilen bir polinomun bir cisim genişlemesindeki minimal polinomunun bulunması ele alınacaktır.

Sonlu bir cisim üzerindeı sıfırdan farklı bir polinomun mertebesini belirlemek oldukça önemlidir. Bu sayının belirlenmesi için aşağıdaki teoreme ihtiyaç vardır.

3.1.1. Teorem. $p(x) \in \mathsf{F}_q[x]$, $m \geq 1$ dereceli bir polinom olmak üzere $p(0) \neq 0$ olsun. Bu durumda $p(x) \mid (x^e - 1)$ olacak biçimde bir $e \leq q^m - 1$ pozitif tamsayısı vardır (Lidl ve Neiderreiter 1986).

İspat. $\mathsf{F}_q[x]/\langle p(x)\rangle$ bölüm halkasının elemanları $j = 0, 1, 2, \ldots, q^m - 1$ için $x^j + \langle p(x)\rangle$ şeklindeki sıfırdan farklı q^m kalan sınıflarıdır. Dolayısıyla $0 \leq r \leq s \leq q^m - 1$ olmak üzere $x^s \equiv x^r \pmod{p(x)}$ olacak şekilde r ve s tamsayıları vardır. x ve $p(x)$ polinomları aralarında asal olduğundan $x^{s-r} \equiv 1 \pmod{p(x)}$ tir. Böylece $0 < s - r \leq q^m - 1$ olmak üzere $p(x) \mid (x^{s-r} - 1)$ dir. $e = s - r$ alınırsa istenilen elde edilmiş olur.

3.1.2. Tanım. $p(x) \in \mathsf{F}_q[x]$ sıfırdan farklı bir polinom olsun. Eğer $p(0) \neq 0$ ise

$$p(x) \mid (x^e - 1)$$

olacak şekildeki en küçük pozitif e tamsayısına $p(x)$ *polinomunun mertebesi* denir ve ord(p) veya ord($p(x)$) şeklinde gösterilir. Eğer $p(0) = 0$ ise $p(x) = x^h r(x)$ ve $r(0) \neq 0$ olacak biçimde tek türlü belirli $h \in \mathbb{N}$ ve $r(x) \in \mathbb{F}_q[x]$ vardır ve bu durumda ord(p) = ord(r) dir.

Bir $p(x)$ polinomunun mertebesine $p(x)$ polinomunun *periyodu* veya *eksponenti* denir. Aşağıdaki teoremde indirgenemez bir $p(x)$ polinomunun mertebesi belirlenecektir.

3.1.3. Teorem. $p(x) \in \mathbb{F}_q[x]$ polinomu $\mathbb{F}_q$ cismi üzerinde derecesi m olan indirgenemez bir polinom ve $p(0) \neq 0$ olsun. Bu durumda $p(x)$ polinomunun mertebesi polinomun herhangi bir kökünün $\mathbb{F}_{q^m}^*$ çarpımsal grubundaki mertebesine eşittir (Lidl ve Neiderreiter 1986).

İspat. Sonuç 2.2.7. gereği, $\mathbb{F}_q{}^m$ cismi $p(x)$ polinomunun $\mathbb{F}_q$ cismi üzerinde parçalanma cismidir. Teorem 2.2.11. gereği, $p(x)$ polinomunun köklerinin mertebeleri, bu köklerin $\mathbb{F}_{q^m}^*$ grubundaki mertebeleri ile aynıdır. $\alpha \in \mathbb{F}_{q^m}^*$ elemanı $p(x)$ polinomunun bir kökü olsun. Bu durumda Teorem 2.2.3. gereği, $\alpha^e = 1$ olması için gerek ve yeter koşul $p(x) \mid (x^e - 1)$ olmasıdır. Böylece ord(p) ve α elemanının $\mathbb{F}_{q^m}^*$ grubundaki mertebesi tanımlarından sonuç elde edilir.

3.1.4. Sonuç. $p(x) \in \mathbb{F}_q[x]$ polinomu $\mathbb{F}_q$ cismi üzerinde derecesi m olan indirgenemez bir polinom ise ord(p) $\mid (q^m - 1)$ dir (Lidl ve Neiderreiter 1986).

İspat. $c \in \mathbb{F}_q{}^*$ olmak üzere $p(x) = cx$ şeklinde ise ord(p) = 1 dir ve sonuç açıktır. Diğer yandan bir önceki teorem gereği, ord(p), $p(x)$ polinomunun herhangi bir kökünün $\mathbb{F}_{q^m}^*$ grubundaki mertebesine eşittir. $\mathbb{F}_{q^m}^*$ grubunun mertebesi de $q^m - 1$ olduğundan ord(p) $\mid (q^m - 1)$ dir.

3.1.5. Örnek. $p(x) = x^3 + x^2 + 1 \in \mathsf{F}_2[x]$ polinomu için $q = 2$ ve $m = 3$ tür. Bu durumda, Teorem 3.1.4. gereği, $\text{ord}(p) \mid (2^3 - 1) = 7$ dir. Diğer yandan $\mathsf{F}_2[x]$ halkasında

$$x^7 - 1 = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + 1)$$

şeklinde yazılabildiğinden mertebe tanımı gereği $\text{ord}(p) = 7$ dir.

İndirgenebilir polinomlar için yukarıdaki sonuç her zaman doğru değildir. Örneğin; $p(x) = x^{10} + x^9 + x^3 + x^2 + 1 \in \mathsf{F}_2[x]$ indirgenebilir polinomu için $\text{ord}(p) = 60$ olduğu görülecektir, ancak $60 \nmid 2^{10} - 1$ dir.

Aşağıdaki teoremde, Teorem 3.1.3. kullanılarak verilen bir derece ve mertebeye sahip monik indirgenemez polinomların sayısını veren bir formül elde edilecektir.

3.1.6. Teorem. $\mathsf{F}_q[x]$ halkasındaki m dereceli, e mertebeli monik indirgenemez polinomların sayısı; $e \geq 2$ ve m, q sayısının e modülüne göre çarpımsal mertebesi ise ϕ, Euler fonksiyonu olmak üzere $\frac{\phi(e)}{m}$ dir, $m = e = 1$ ise 2 dir ve diğer durumlarda 0 dır. Özel olarak, $\mathsf{F}_q[x]$ halkasındaki e mertebeli bir indirgenemez polinomun derecesi q sayısının e modülüne göre çarpımsal mertebesine eşittir (Lidl ve Neiderreiter 1986).

İspat. $p(x) \in \mathsf{F}_q[x]$, $p(0) \neq 0$ özelliğinde bir indirgenemez polinom olsun. Bu durumda Teorem 3.1.3 gereği, $\text{ord}(p) = e$ olması için gerek ve yeter koşul $p(x)$ polinomunun tüm köklerinin F_q cismi üzerinde birimin e. ilkel kökü olmasıdır. Diğer bir ifade ile $\text{ord}(p) = e$ olması için gerek ve yeter koşul $p(x) \mid \Phi_e$ olmasıdır. Teorem 2.4.11. gereği, Φ_e polinomunun herhangi bir monik indirgenemez çarpanının derecesi $q^m \equiv 1 \pmod{e}$ olacak şekildeki en küçük pozitif m tamsayısı ile aynıdır ve üstelik bu çarpanların sayısı $\phi(e)/m$ dir. $m = e = 1$ durumu $p(x) = x$ alınarak elde edilir.

Hatırlanacağı gibi, pozitif dereceli her polinom indirgenemez polinomların çarpımı biçiminde yazılabilir. Dolayısıyla indirgenemez bir polinomun bir kuvvetinin mertebesi ve ikişerli aralarında asal polinomların çarpımlarının mertebesi belirlenerek her polinomun mertebesi hesaplanabilir. Bunun için aşağıdaki teoreme ihtiyaç vardır.

3.1.7. Teorem. c, bir pozitif tamsayı olmak üzere $p(x) \in \mathsf{F}_q[x]$ polinomu $p(0) \neq 0$ özelliğinde bir polinom olsun. Bu durumda $p(x) \mid (x^c - 1)$ olması için gerek ve yeter koşul $\text{ord}(p) \mid c$ olmasıdır (Lidl ve Neiderreiter 1986).

İspat. $e = \text{ord}(p) \mid c$ ise $p(x) \mid (x^e - 1)$ ve $(x^e - 1) \mid (x^c - 1)$ dir. Bu ise $p(x) \mid (x^c - 1)$ olduğunu gösterir. Tersine, $p(x) \mid (x^c - 1)$ olsun. Bu durumda $c \geq e$ dir ve $m \in \mathsf{N}$, $0 \leq r < e$ olmak üzere $c = me + r$ biçiminde yazılabilir. $x^c - 1 = (x^{me} - 1)x^r + x^r - 1$ olarak düzenlenirse $p(x) \mid (x^r - 1)$ olmalıdır. Bu ise ancak $r = 0$ olması durumunda mümkündür. O halde $e \mid c$ dir.

3.1.8. Sonuç. e_1 ve e_2 pozitif tamsayılar olsun. Bu durumda d, e_1 ve e_2 sayılarının en büyük ortak böleni olmak üzere $x^{e_1} - 1$ ve $x^{e_2} - 1$ polinomlarının $\mathsf{F}_q[x]$ halkasındaki en büyük ortak böleni $x^d - 1$ polinomudur (Lidl ve Neiderreiter 1986).

İspat. $p(x)$ polinomu, $x^{e_1} - 1$ ve $x^{e_2} - 1$ polinomlarının monik en büyük ortak böleni olsun. $i = 1, 2$ için $x^d - 1$ polinomu $x^{e_i} - 1$ polinomlarının bir ortak böleni olduğundan $(x^d - 1) \mid p(x)$ dir. Diğer yandan $i = 1, 2$ için $p(x)$ polinomu $x^{e_i} - 1$ polinomlarının bir ortak böleni olduğundan Teorem 3.1.7. gereği, $\text{ord}(p)$, e_1 ve e_2 sayılarını böler. Dolayısıyla, $\text{ord}(p) \mid d$ dir ve böylece Teorem 3.1.7. gereği, $p(x) \mid (x^d - 1)$ dir. O halde $p(x) = x^d - 1$ dir.

3.1.9. Teorem. $g(x) \in \mathsf{F}_q[x]$ polinomu $g(0) \neq 0$ ve $\text{ord}(g) = e$ özelliğinde bir polinom ve b, $f(x) = g(x)^b$ özelliğinde bir pozitif tamsayı olsun. p, F_q cisminin karakteristiği olmak üzere t, $p^t \geq b$ olacak şekildeki en küçük tamsayı olsun. Bu durumda $\text{ord}(f) = ep^t$ dir (Lidl ve Neiderreiter 1986).

İspat. $c = \text{ord}(f)$ olsun. Bu durumda $f(x) \mid (x^c - 1)$ olduğundan $g(x) \mid (x^c - 1)$ dir. Böylece, Teorem 3.1.7 gereği, $e \mid c$ elde edilir. Üstelik, $g(x) \mid (x^e - 1)$ ve dolayısıyla $f(x) \mid (x^e - 1)^b$ dir. $f(x) \mid (x^e - 1)^{p^t} = x^{ep^t} - 1$ dir. Böylece Teorem 3.1.7. gereği, $c \mid ep^t$ dir. O halde $0 \leq u \leq t$ olmak üzere $c = ep^u$ şeklindedir. Sonuç 3.1.4. gereği, $p \nmid e$ olduğundan, $x^e - 1$ polinomunun kökleri birer basit köktür. Dolayısıyla, $x^{ep^u} - 1 = (x^e - 1)^{p^u}$ polinomunun tüm köklerinin katlılığı p^u dur. Diğer yandan $g(x)^b$ ve $x^{ep^u} - 1$ polinomlarının köklerinin

katlılıkları karşılaştırıldığında $p^u \geq b$ olduğundan $g(x)^b \mid (x^{ep^u} - 1)$ dir. O halde $u \geq t$ ve böylece $u = t$ ve $c = ep^t$ dir.

3.1.10. Teorem. $g_1(x)$, ..., $g_k(x)$, F_q cismi üzerinde ikişerli aralarında asal sıfırdan farklı polinomlar olmak üzere $f(x) = g_1(x) \cdots g_k(x)$ olsun. Bu durumda

$$\text{ord}(f) = [\text{ord}(g_1), ..., \text{ord}(g_k)]$$

dir (Lidl ve Neiderreiter 1986).

İspat. Bunu göstermek için, $1 \leq i \leq k$ için $g_i(0) \neq 0$ olması halini dikkate almak yeterlidir. $e = \text{ord}(f)$ ve $1 \leq i \leq k$ için $e_i = \text{ord}(g_i)$ olmak üzere $c = [e_1, ..., e_k]$ olsun. Bu durumda $1 \leq i \leq k$ için her bir $g_i(x)$ polinomu $x^{e_i} - 1$ polinomunu böler. Böylece $g_i(x) \mid x^c - 1$ dir. $g_1(x)$, ... $g_k(x)$ polinomları ikişerli aralarında asal olduğundan $f(x) \mid (x^c - 1)$ dir. Böylece Teorem 3.1.7. gereği $e \mid c$ dir. Diğer yandan, $f(x) \mid (x^e - 1)$ olduğundan $1 \leq i \leq k$ için her bir g_i polinomu, $(x^e - 1)$ polinomunu böler. Teorem 3.1.7. gereği, her $1 \leq i \leq k$ için $e_i \mid e$ dir. Dolayısıyla $c \mid e$ dir. Böylece $e = c$ dir.

Yukarıdaki teoremle birlikte, sonlu sayıda sıfırdan farklı polinomun en küçük ortak katının mertebesinin bu polinomların mertebelerinin en küçük ortak katına eşit olduğu söylenebilir.

3.1.11. Örnek 1. $f(x) = (x^2 + x + 1)(x^3 + x^2 + 1) \in \mathsf{F}_2[x]$ polinomu için $g_1(x) = x^2 + x + 1$ ve $g_2(x) = x^3 + x^2 + 1$ dir. $\text{ord}(g_1) = 3$ ve $\text{ord}(g_2) = 7$ olduğundan $\text{ord}(f) = 21$ dir.

2. $f(x) = x^{10} + x^9 + x^3 + x^2 + 1 \in \mathsf{F}_2[x]$ polinomu $\mathsf{F}_2[x]$ halkasında

$$f(x) = (x^2 + x + 1)^3(x^4 + x + 1)$$

biçiminde yazılabilir. $\text{ord}(x^2 + x + 1) = 3$ olduğundan Teorem 3.1.9 gereği, $\text{ord}((x^2 + x + 1)^3) = 3 \cdot 2^2 = 12$ dir, üstelik $\text{ord}(x^4 + x + 1) = 15$ olduğundan Teorem 3.1.10 gereği, $\text{ord}(f) = [12, 15] = 60$ dır (Lidl ve Neiderreiter 1986).

Teorem 3.1.10. aşağıdaki gibi genelleştirilebilir.

3.1.12. Teorem. F_q, karakteristiği p olan sonlu bir cisim ve $f(x) \in \mathsf{F}_q[x]$ polinomu, $f(0) \neq 0$ özelliğinde pozitif dereceli bir polinom olsun. $a \in \mathsf{F}_q$, $b_1, ..., b_k \in \mathsf{N}$ ve $f_1(x), ..., f_k(x) \in \mathsf{F}_q[x]$ farklı monik indirgenemez polinomlar olmak üzere $f(x)$ polinomunun $\mathsf{F}_q[x]$ halkasındaki çarpanlaması $f(x) = a f_1^{b_1}(x) \cdots f_k^{b_k}(x)$ olsun. Bu durumda $e = [\text{ord}(f_1), ..., \text{ord}(f_k)]$ ve t, $p^t \geq \text{maks}\{b_1, ..., b_k\}$ olacak biçimdeki en küçük tamsayı olmak üzere $\text{ord}(f) = ep^t$ dir (Lidl ve Neiderreiter 1986).

3.1.13. Tanım. $a_n \neq 0$ olmak üzere $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathsf{F}_q[x]$ olsun. Bu durumda f polinomunun karşı (reciprocal) polinomu f^* ile gösterilir ve

$$f^*(x) = x^n f(1/x) = a_0 x^n + a_1 x^{n-1} + ... + a_{n-1}x + a_n$$

olarak tanımlanır.

3.1.14. Teorem. $f(x) \in \mathsf{F}_q[x]$ sıfırdan farklı bir polinom ve $f^*(x)$, $f(x)$ polinomunun karşı polinomu olsun. Bu durumda $\text{ord}(f) = \text{ord}(f^*)$ dir (Lidl ve Neiderreiter 1986).

İspat. İlk olarak $f(0) \neq 0$ olsun. Bu durumda $f(x) \mid (x^e - 1)$ olması için gerek ve yeter koşul $f^*(x) \mid (x^e - 1)$ olmasıdır. Böylece istenilen elde edilir. $f(0) = 0$ olsun. Bu durumda $h \in \mathsf{N}$ ve $g(x) \in \mathsf{F}_q[x]$, $g(0) \neq 0$ özelliğinde bir polinom olmak üzere $f(x) = x^h g(x)$ olarak yazılırsa $g^*(x) = f^*(x)$ olduğundan $\text{ord}(f) = \text{ord}(g) = \text{ord}(g^*) = \text{ord}(f^*)$ dır.

$f(x)$ ve $f(-x)$ polinomlarının mertebeleri arasında yakın bir ilişki vardır. Karakteristiği 2 olan bir cisim için $f(x) = f(-x)$ olduğundan karakteristiği tek sayı olan cisimler ele alınacaktır.

3.1.15. Teorem. q bir tek sayı, $f(x) \in \mathsf{F}_q[x]$, $f(0) \neq 0$ özelliğinde pozitif dereceli bir polinom olsun. Bu durumda $e = \text{ord}(f(x))$ ve $E = \text{ord}(f(-x))$ olmak üzere

i) $e = 4k$, $k \in \mathsf{Z}$ ise $E = e$ dir,

ii) e, tek sayı ise $E = 2e$ dir,

iii) e, bir tek sayının 2 katı ve $f(x)$ polinomunun tüm indirgenemez çarpanlarının mertebesi çift sayı ise $E = e/2$ dir,

iv) diğer durumlarda $E = e$ dir (Lidl ve Neiderreiter 1986).

İspat. ord($f(x)$) = e olduğundan $f(x) \mid (x^{2e} - 1)$ dir. Benzer biçimde $f(-x) \mid ((-x)^{2e} - 1) = x^{2e} - 1$ dir. Böylece, Teorem 3.1.7. gereği, $E \mid 2e$ dir. Benzer biçimde hareket edilirse $e \mid 2E$ olduğu sonucu elde edilir. O halde E sayısı $2e$, e veya $e/2$ olabilir. $k \in \mathbb{Z}$ olmak üzere $e = 4k$ ise e ve E sayıları çifttir. $f(x) \mid (x^e - 1)$ ve $f(-x) \mid ((-x)^e - 1) = x^e - 1$ olduğundan $E \mid e$ dir. Benzer şekilde $e \mid E$ olduğu elde edilir. Böylece $E = e$ dir. Eğer e, tek sayı ise $f(-x) \mid ((-x)^e - 1) = -x^e - 1$ ve böylece $f(-x) \mid (x^e + 1)$ dir. Ancak bu durumda $f(-x) \nmid (x^e - 1)$ dir. Böylece $E = 2e$ olmalıdır.

h, tek tamsayı olmak üzere $e = 2h$ ve $f(x)$ polinomu $\mathbb{F}_q[x]$ halkasındaki bir indirgenemez polinomun bir kuvveti olsun. Bu durumda ord(f) = $2h$ olduğundan $f(x) \mid (x^h - 1)(x^h + 1)$ ve $f(x) \nmid (x^h - 1)$ dir. Diğer yandan $x^h - 1$ ve $x^h + 1$ polinomları aralarında asal olduğundan $f(x) \mid (x^h + 1)$ dir. Sonuç olarak, $f(-x)$ polinomu, $(-x)^h + 1 = -x^h + 1$ polinomunu, dolayısıyla $x^h - 1$ polinomunu böler. Böylece $E = e/2$ dir. Teorem 3.1.9. gereği, bir indirgenemez polinomun kuvvetinin mertebesinin çift olması için gerek ve yeter koşul indirgenemez polinomun kendisinin çift mertebeli olmasıdır.

Her bir $g_i(x)$ bir indirgenemez polinomun kuvveti ve $g_1(x)$, ..., $g_k(x)$ ikişerli aralarında asal polinomlar olmak üzere $f(x) = g_1(x) \cdots g_k(x)$ biçiminde bir polinom olsun. Teorem 3.1.10. gereği, $2h$ = [ord(g_1), ..., ord(g_k)] dir. $1 \le i \le k$ için h_i sayıları birer tek tamsayı olmak üzere $[h_1, ..., h_k] = h$ olsun. Şimdi $g_i(x)$ çarpan polinomlarını, $1 \le i \le m$ için ord(g_i) = $2h_i$ ve $m + 1 \le i \le k$ için ord(g_i) = h_i olacak biçimde yeniden sıralıyalım. Böylece $1 \le i \le m$ için ord($g_i(-x)$) = h_i ve $m + 1 \le i \le k$ için ord($g_i(-x)$) = $2h_i$ olur. Dolayısıyla Teorem 3.1.10 gereği, $E = [h_1, ..., h_m, 2h_{m+1}, ..., 2h_k]$ dir ve $m = k$ ise $E = h = e/2$ ve $m < k$ ise $E = 2h = e$ dir.

Hatırlanacağı gibi, $\mathbb{F}_q$ cismi üzerinde $m \ge 1$ dereceli bir polinomun mertebesi en fazla $q^m - 1$ dir. Mertebesi bu üst sınır, yani $q^m - 1$ olan polinomlar ilkel polinomlar olarak adlandırılır. Şimdi, Tanım 2.1.6. da bahsedilen ilkel eleman kavramı kullanılarak ilkel polinom tanımı verilebilir.

3.1.16. Tanım. $f(x) \in \mathsf{F}_q[x]$, $m \geq 1$ dereceli bir polinom olsun. Eğer $f(x)$, $\mathsf{F}_q{}^m$ cisminin bir ilkel elemanının F_q cismi üzerindeki minimal polinomu ise $f(x)$ polinomuna F_q cismi üzerinde bir *ilkel polinom* denir (Lidl ve Neiderreiter 1986).

F_q cismi üzerinde m dereceli bir ilkel polinom F_q cismi üzerinde $\mathsf{F}_q{}^m$ çarpımsal grubunu üreten bir $\alpha \in \mathsf{F}_q{}^m$ elemanını kök kabul eden monik indirgenemez bir polinom olarak tanımlanabilir. İlkel polinomlar aşağıdaki gibi karakterize edilebilirler.

3.1.17. Teorem. $f(x) \in \mathsf{F}_q[x]$ polinomunun $m \geq 1$ dereceli bir ilkel polinom olması için gerek ve yeter koşul $f(x)$ polinomunun $f(0) \neq 0$ ve $\text{ord}(f) = q^m - 1$ özelliğinde bir monik polinom olmasıdır (Lidl ve Neiderreiter 1986).

İspat. $f(x)$ polinomu F_q cismi üzerinde bir ilkel polinom ise $f(x)$ moniktir ve $f(0) \neq 0$ dır. $f(x)$ polinomu F_q cismi üzerinde bir indirgenemez polinom olduğundan Teorem 3.1.3 gereği ve üstelik $f(x)$, F_q cisminin bir ilkel elemanını kök olarak bulundurduğundan $\text{ord}(f) = q^m - 1$ dir.

Tersine, $\text{ord}(f) = q^m - 1$ ise $m \geq 1$ dir. $f(x)$ polinomu F_q cismi üzerinde indirgenemezdir. Tersine $f(x)$ polinomu F_q cismi üzerinde indirgebilir olsaydı $f(x)$ polinomu ya indirgenemez bir polinomun bir kuvveti ya da aralarında asal pozitif dereceli iki polinomun çarpımı şeklinde yazılabilirdi. İlk halde $g(x) \in \mathsf{F}_q[x]$ polinomu F_q cismi üzerinde indirgenemez $g(0) \neq 0$ özelliğinde bir polinom ve $b \geq 2$ olmak üzere $f(x) = g^b(x)$ dir. Bu durumda Teorem 3.1.9. gereği, $\text{ord}(f)$, F_q cisminin karakteristiği ile bölünür ancak $q^m - 1$ sayısı ile bölünmez. Bu ise bir çelişkidir. İkinci halde, $g_1(x)$, $g_2(x) \in \mathsf{F}_q[x]$ polinomları pozitif m_1 ve m_2 dereceli, aralarında asal, monik polinomlar olmak üzere $f(x) = g_1(x)g_2(x)$ dir. $i = 1, 2$ için $e_i = \text{ord}(g_i)$ ise Teorem 3.1.10. gereği, $\text{ord}(f) \leq e_1e_2$ dir. Üstelik Teorem 3.1.1. gereği, $i = 1, 2$ için $e_i \leq q^{m_i} - 1$ olduğundan

$$\text{ord}(f) \leq (q^{m_1} - 1)(q^{m_2} - 1) < q^{m_1+m_2} - 1 = q^m - 1$$

dir. Bu ise $\text{ord}(f) = q^m - 1$ olması ile çelişkidir. Her iki halde de çelişki elde edildiğinden $f(x)$ polinomu, F_q cismi üzerinde indirgenemezdir ve böylece Teorem 3.1.3. gereği, $f(x)$, F_q cismi üzerinde ilkel bir polinomdur.

3.1.18. Teorem. $f(x) \in \mathsf{F}_q[x]$, pozitif dereceli ve $f(0) \neq 0$ özelliğinde bir polinom ve r, $a \in \mathsf{F}_q^*$ olmak üzere

$$x^r \equiv a \pmod{(f(x))}$$

olacak biçimdeki en küçük pozitif tamsayı olsun. Bu durumda h, $a \in \mathsf{F}_q^*$ elemanının F_q^* devirli grubundaki mertebesi olmak üzere ord(f) = hr dir (Lidl ve Neiderreiter 1986).

İspat. ord(f) = e olsun. $x^e \equiv 1 \pmod{(f(x))}$ olduğundan $e \geq r$ dir. Böylece $s \in \mathsf{N}$ ve $0 \leq t < r$ olmak üzere $e = sr + t$ biçiminde yazılabilir. O halde

$$1 \equiv x^e \equiv x^{sr+t} \equiv a^s x^t \pmod{(f(x))}$$

dir ve böylece $x^t \equiv a^{-s} \pmod{(f(x))}$ dir. r sayısının tanımı gereği bu ancak $t = 0$ için gerçeklenir. Bu durumda yukarıdaki denklik $a^s \equiv 1 \pmod{(f(x))}$ halini alır. Böylece $a^s = 1$ ve dolayısıyla $s \geq h$ ve $e \geq hr$ dir. Diğer yandan $x^{hr} \equiv a^h \equiv 1 \pmod{(f(x))}$ dir ve dolayısıyla $e = hr$ dir.

3.1.19. Teorem. $m \geq 1$ dereceli $f(x) \in \mathsf{F}_q[x]$ monik polinomunun F_q üzerinde bir ilkel polinom olması için gerek ve yeter koşul $(-1)^m f(0)$ nın F_q cisminin bir ilkel elemanı olması ve x^r nin $f(x)$ modülüne göre F_q cisminin belli bir elemanına denk olacak biçimdeki en küçük pozitif r tamsayısının $r = (q^m - 1)/(q - 1)$ olmasıdır. $f(x)$ polinomu F_q cismi üzerinde bir ilkel polinom ise $x^r \equiv (-1)^m f(0) \pmod{f(x)}$ dir (Lidl ve Neiderreiter 1986).

İspat. $f(x)$ polinomu F_q cismi üzerinde bir ilkel polinom ise $\alpha \in \mathsf{F}_q{}^m$ bir ilkel eleman olmak üzere α, $f(x)$ polinomunun bir köküdür. $f(x)$ polinomunun α elemanının F_q cismi üzerindeki karakteristik polinomu olduğu dikkate alınır, norm tanımı ve (2.3) eşitliği kullanılarak $N_{\mathsf{F}_q{}^m/\mathsf{F}_q}(\alpha)$ normu hesaplanırsa

$$(-1)^m f(0) = \alpha^{(q^m-1)/(q-1)}$$

eşitliği elde edilir. Böylece $(-1)^m f(0)$ elemanının F_q^* grubundaki mertebesi $q - 1$ dir, yani, $(-1)^m f(0)$, F_q cisminin bir ilkel elemanıdır. $f(x)$ polinomu α elemanının F_q cismi üzerindeki minimal polinomu olduğundan yukarıdaki eşitlikten

$$x^{(q^m-1)/(q-1)} \equiv (-1)^m f(0) \pmod{f(x)}$$

denkliği elde edilir. Böylece $r \le (q^m - 1)/(q - 1)$ dir. Ancak, Teorem 3.1.17. ve Teorem 3.1.18. gereği, $q^m - 1 = \text{ord}(f) \le (q - 1)r$ dir. Dolayısıyla $r = (q^m - 1)/(q - 1)$ dir.

Tersine, teoremin koşulları gerçeklensin. $r = (q^m - 1)/(q - 1)$ eşitliği ve Teorem 3.1.18. gereği, ord(f) ve q aralarında asaldır. Bu durumda Teorem 3.1.12. gereği, $f_i(x)$ polinomları, F_q cismi üzerinde farklı monik indirgenemez polinomlar olmak üzere $f(x) = f_1(x) \cdots f_k(x)$ biçiminde çarpanlarına ayrılabilir. Eğer $m_i = \text{der}(f_i)$ olarak alınırsa $1 \le i \le k$ için $\text{ord}(f_i) \mid (q^{m_i} - 1)$ dir. Böylece $d = (q^{m_1} - 1) \cdots (q^{m_1 k} - 1)/(q - 1)^{k-1}$ olmak üzere $(q^{m_i} - 1) \mid d$ dir. Dolayısıyla $1 \le i \le k$ için $\text{ord}(f_i) \mid d$ dir. Sonuç 3.1.4 gereği, $1 \le i \le k$ için $f_i(x) \mid (x^d - 1)$ ve böylece $f(x) \mid (x^d - 1)$ dir. Eğer $k \ge 2$ ise

$$d < (q^{m_1 + \ldots + m_k} - 1)/(q - 1) = (q^m - 1)/(q - 1) = r$$

olur, bu ise r sayısının tanımı ile çelişkidir. O halde $k = 1$ dir ve $f(x)$ polinomu F_q cismi üzerinde bir indirgenemez polinomdur.

Eğer $\beta \in \mathsf{F}_q{}^m$, $f(x)$ polinomunun bir kökü ise $\beta^r = (-1)^m f(0)$ dir ve böylece $x^r = (-1)^m f(0) \pmod{f(x)}$ dir. $(-1)^m f(0)$ nın $\mathsf{F}_q{}^*$ grubundaki mertebesi $q - 1$ olduğundan Teorem 3.1.18. gereği, $\text{ord}(f) = q^m - 1$ dir ve dolayısıyla Teorem 3.1.17. gereği, $f(x)$ polinomu F_q cismi üzerinde bir ilkel polinomdur.

3.1.20 Örnek. $f(x) = x^4 + x^3 + x^2 + 2x + 2 \in \mathsf{F}_3[x]$ polinomu F_3 cismi üzerinde bir indirgenemez polinom olduğundan $\text{ord}(f) = 80 = 3^4 - 1$ dir. O halde Teorem 3.1.17. gereği, $f(x)$ polinomu F_3 cismi üzerinde bir ilkel polinomdur. Üstelik $x^{40} \equiv 2 \pmod{f(x)}$ dir (Lidl ve Neiderreiter 1986).

3.2. İndirgenemez Polinomlar

Bu kısımda sonlu cisimler üzerinde tanımlı indirgenemez polinomların sayısı bazı özel fonksiyonlar yardımıyla ifade edilecektir. Hatırlanacağı gibi, pozitif dereceli bir $f(x) \in \mathsf{F}_q[x]$ polinomunun $\mathsf{F}_q[x]$ halkasındaki her çarpanlaması bir sabit polinom içeriyorsa $f(x)$ polinomu F_q cismi üzerinde bir indirgenemez polinomdur.

3.2.1. Teorem. Her sonlu F_q cismi ve her $n \in \mathsf{N}$ sayısı için F_q cismi üzerindeki derecesi n sayısını bölen tüm monik indirgenemez polinomların çarpımı $x^{q^n} - x$ polinomuna eşittir (Lidl ve Neiderreiter 1986).

İspat. Teorem 2.2.4. gereği, F_q cismi üzerindeki monik indirgenemez polinomlar, $g(x) = x^{q^n} - x$ polinomunun $\mathsf{F}_q[x]$ halkasındaki doğal çarpanlamasından elde edilen ve dereceleri n sayısını bölen polinomlardır. $g'(x) = -1$ olduğundan Teorem 1.1.11. gereği, $g(x)$ polinomunun F_q cismi üzerindeki parçalanma cisminde hiç katlı kökü yoktur. Dolayısıyla F_q cismi üzerindeki derecesi n sayısını bölen her bir monik indirgenemez polinom $g(x)$ polinomunun $\mathsf{F}_q[x]$ halkasındaki doğal çarpanlamasında tam olarak bir kez bulunur.

3.2.2. Sonuç. $N_q(d)$, $\mathsf{F}_q[x]$ halkasında derecesi d olan monik indirgenemez polinomların sayısı olmak üzere her $n \in \mathsf{N}$ için

$$q^n = \sum_{d|n} dN_q(d) \tag{3.1}$$

dir. Bu toplam, n sayısının tüm pozitif d bölenlerine genişletilebilir (Lidl ve Neiderreiter 1986).

İspat. (3.1) eşitliği, Teorem 3.1.1 yardımıyla $g(x) = x^{q^n} - x$ polinomunun derecesi ve $g(x)$ polinomunun doğal çarpanlamasındaki toplam derecesi karşılaştırılarak elde edilir.

(3.1) eşitliği ve sayılar teorisi kullanılarak, $\mathsf{F}_q[x]$ halkasındaki belli bir dereceye sahip monik indirgenemez polinomların sayısı için daha açık bir formül verilebilir. Bunun için aşağıda verilecek olan Möbius fonksiyonu kullanılacaktır.

3.2.3. Tanım. Möbius fonksiyonu μ ile gösterilir ve $n \in \mathsf{N}$ olmak üzere

$$\mu(n) = \begin{cases} 1, & n = 1 \text{ ise} \\ (-1)^k, & n, k \text{ farklı asal sayının çarpımı ise} \\ 0, & n, \text{ bir asal sayının karesi ile bölünebiliyorsa} \end{cases}$$

olarak tanımlanır.

Bundan sonra (3.1) eşitliğindeki gibi, $n \in \mathbb{N}$ sayısının tüm pozitif d bölenleri üzerinden toplamı için $\Sigma_{d|n}$ sembolü kullanılacaktır. Benzer bir gösterim $\Pi_{d|n}$ çarpım sembolü için de kullanılacaktır.

3.2.4. Teorem. Her $n \in \mathbb{N}$ için

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \text{ ise} \\ 0, & n > 1 \text{ ise} \end{cases}$$

dir (Lidl ve Neiderreiter 1986).

İspat. $n = 1$ hali açıktır. $n > 1$ için $\mu(d) \neq 0$ olacak biçimdeki n sayısının pozitif d bölenleri dikkate alınmalıdır, yani $d = 1$ dir veya d sayısı farklı asalların çarpımı olarak alınmalıdır. Böylece $p_1, p_2, ..., p_k$ sayıları n sayısının farklı asal bölenleri olmak üzere

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \le i_1 < i_2 \le k} \mu(p_{i_1} p_{i_2}) + ... + \mu(p_1 p_2 ... p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + ... + \binom{k}{k}(-1)^k \\ &= (1 + (-1))^k = 0 \end{aligned}$$

elde edilir.

3.2.5. Teorem (Möbius İnversiyon Formülü).

i) Toplamsal durum: h ve H fonksiyonları, $\mathbb{N}$ kümesinden bir toplamsal G abelyen grubuna tanımlı iki fonksiyon olsun. Bu durumda her $n \in \mathbb{N}$ sayısı için

$$H(n) = \sum_{d|n} h(d) \tag{3.2}$$

olması için gerek ve yeter koşul her $n \in \mathbb{N}$ sayısı için

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) \tag{3.3}$$

olmasıdır.

ii) Çarpımsal durum: h ve H fonksiyonları, $\mathbb{N}$ kümesinden bir çarpımsal G abelyen grubuna tanımlı iki fonksiyon olsun. Bu durumda her $n \in \mathbb{N}$ sayısı için

$$H(n) = \prod_{d|n} h(d) \tag{3.4}$$

olması için gerek ve yeter koşul her $n \in \mathbb{N}$ sayısı için

$$h(n) = \prod_{d|n} H(d)^{\mu(n/d)} = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} \tag{3.5}$$

olmasıdır (Lidl ve Neiderreiter 1986).

İspat. (3.2) eşitliği dikkate alınır ve Teorem 3.2.4. kullanılırsa her $n \in \mathbb{N}$ sayısı için

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{c|n/d} h(c)$$

$$= \sum_{c|n} \sum_{d|n/c} \mu(d) h(c) = \sum_{c|n} h(c) \sum_{d|n/c} \mu(d) = h(n)$$

olduğu elde edilir. Benzer bir hesaplama ile önermenin tersi gösterilebilir. (*ii*) kısmının ispatı için (*i*) kısmının ispatındaki toplamlar yerine çarpım, katlar yerine kuvvet alınırsa istenilen elde edilmiş olur.

3.2.6. Teorem. $N_q(n)$, $\mathbb{F}_q[x]$ halkasında derecesi n olan monik indirgenemez polinomların sayısı olmak üzere

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d|n} \mu(d)\, q^{n/d}$$

dir (Lidl ve Neiderreiter 1986).

İspat. Teoremin ispatı için Möbius inversiyon formülünün toplamsal halini $G = \mathbb{Z}$ grubuna uygulayalım. Her $n \in \mathbb{N}$ sayısı için $h(n) = nN_q(n)$ ve $H(n) = q^n$ olsun. Bu durumda, (3.1) eşitliğinden (3.2) eşitliği gerçeklenir ve böylece (3.5) eşitliği ile istenilen formül elde edilmiş olur.

3.2.7. Örnek. $\mathbb{F}_q[x]$ halkasında derecesi 20 olan monik indirgenemez polinomların sayısı

$$N_q(20) = \frac{1}{20} (\mu(1)q^{20} + \mu(2)q^{10} + \mu(4)q^5 + \mu(5)q^4 + \mu(10)q^2 + \mu(20)q)$$

$$= \frac{1}{20} (q^{20} - q^{10} - q^4 + q^2)$$

dir.

Teorem 3.2.6. dikkate alındığında "her $n \in \mathbb{N}$ sayısı ve her sonlu $\mathbb{F}_q$ cismi için $\mathbb{F}_q[x]$ halkasında n dereceli bir indirgenemez polinom vardır" sonucu yeniden elde edilmiş olur. O halde $\mu(1) = 1$ ve her $d \in \mathbb{N}$ için $\mu(d) \geq -1$ olduğu kullanılarak

$$N_q(n) \geq \frac{1}{n}(q^n - q^{n-1} - q^{n-2} - \ldots - q) = \frac{1}{n}(q^n - \frac{q^n - q}{q-1}) > 0$$

olduğu elde edilir.

Aşağıda, Möbius inversiyon formülünün bir diğer uygulaması olarak, n. döngüsel polinomu Φ_n için açık bir formül verilecektir.

3.2.8. Teorem. K, karakteristiği p olan bir cisim ve $p \nmid n$ olmak üzere bir $n \in \mathbb{N}$ sayısı için K cismi üzerindeki n. döngüsel polinom Φ_n,

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)} = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$$

eşitliğini gerçekler (Lidl ve Neiderreiter 1986).

İspat. Teoremin ispatı için Möbius inversiyon formülünün çarpımsal halini G grubunu K cismi üzerindeki sıfırdan farklı rasyonel fonksiyonların çarpımsal grubu alarak uygulayalım. Her $n \in \mathbb{N}$ için $h(n) = \Phi_n(x)$ ve $H(n) = x^n - 1$ olsun. Bu durumda Teorem 2.4.9. (*i*) gereği, (3.4) eşitliği gerçeklenir ve böylece (3.3) eşitliği ile istenilen sonuç elde edilmiş olur.

Teoremde verilen formül döngüsel polinomların temel özelliklerini belirlemek için kullanılabilir.

3.2.9. Örnek. Φ_{12} polinomunun tanımlı olduğu K cisimleri için

$$\begin{aligned}\Phi_{12}(x) &= \prod_{d|12}(x^{12/d} - 1)^{\mu(d)} \\ &= (x^{12} - 1)^{\mu(1)}(x^6 - 1)^{\mu(2)}(x^4 - 1)^{\mu(3)}(x^3 - 1)^{\mu(4)}(x^2 - 1)^{\mu(6)}(x - 1)^{\mu(12)} \\ &= \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = x^4 - x^2 - 1\end{aligned}$$

dir (Lidl ve Neiderreiter 1986).

Teorem 3.2.6.'da $\mathsf{F}_q[x]$ halkasında belli dereceye sahip monik indirgenemez polinomların sayısı belirlenmişti. Şimdi $\mathsf{F}_q[x]$ halkasında belli dereceye sahip monik indirgenemez polinomların çarpımı belirlenecektir.

3.2.10. Teorem. $\mathsf{F}_q[x]$ halkasında derecesi n olan tüm monik indirgenemez polinomların çarpımı $I(q, n; x)$,

$$I(q, n; x) = \prod_{d|n} (x^{q^d} - x)^{\mu(n/d)} = \prod_{d|n} (x^{q^{n/d}} - x)^{\mu(d)}$$

biçimindedir (Lidl ve Neiderreiter 1986).

İspat. Teorem 3.2.1. gereği,

$$x^{q^n} - x = \prod_{d|n} I(q, d; x)$$

dir. Teoremin ispatı için Möbius inversiyon formülünün çarpımsal halini G grubunu F_q cismi üzerindeki sıfırdan farklı rasyonel fonksiyonların çarpımsal grubu alarak uygulamak yeterlidir. Möbius inversiyon formülünün çarpımsal halinde her $n \in \mathsf{N}$ için $h(n) = I(q, n; x)$ ve $H(n) = x^{q^n} - x$ olarak alınırsa istenilen formül elde edilmiş olur.

3.2.11. Örnek. $q = 2$ ve $n = 4$ için

$$I(2, 4; x) = (x^{16} - x)^{\mu(1)}(x^4 - x)^{\mu(2)}(x^2 - x)^{\mu(4)}$$

$$= \frac{x^{16} - x}{x^4 - x} = \frac{x^{15} - 1}{x^3 - 1}$$

$$= x^{12} + x^9 + x^6 + x^3 + 1$$

dir (Lidl ve Neiderreiter 1986).

$\mathsf{F}_q[x]$ halkasında derecesi n olan tüm monik indirgenemez polinomlar $I(q, n; x)$ polinomunun çarpanlamasıyla belirlenebilir. Bunun için aşağıdaki sonuç kullanılarak $I(q, n; x)$ çarpımını kısmen çarpanlarına ayırmak daha kullanışlıdır.

3.2.12. Teorem. $\Phi_m(x)$, F_q cismi üzerinde n. döngüsel polinom ve $I(q,n; x)$ polinomu Teorem 3.2.10 daki gibi olmak üzere her $n > 1$ için

$$I(q, n; x) = \prod_{m} \Phi_m(x) \tag{3.6}$$

dir. Burada n sayısı q nun m modülüne göre mertebesi olmak üzere çarpım $q^n - 1$ nin tüm pozitif m bölenleri üzerinden alınmaktadır (Lidl ve Neiderreiter 1986).

İspat. $n > 1$ için S, F_q cismi üzerinde derecesi n olan F_{q^n} cisminin elemanlarının kümesi olsun. Bu durumda, her $\alpha \in S$ elemanının F_q cismi üzerinde derecesi n olan bir minimal polinomu vardır ve böylece $\alpha \in S$, $I(q, n; x)$ polinomunun bir köküdür. Diğer yandan β, $I(q, n; x)$ polinomunun bir kökü ise β, $\mathsf{F}_q[x]$ halkasında n. dereceden belli bir monik indirgenemez polinomun köküdür ve böylece $\beta \in S$ dir. Dolayısıyla

$$I(q, n; x) = \prod_{\alpha \in S} (x - \alpha)$$

dır.

$\alpha \in S$ ise $\alpha \in \mathsf{F}_{q^n}^*$ dır, dolayısıyla α elemanının bu çarpımsal gruptaki mertebesi, $q^n - 1$ sayısının bir bölenidir. Dikkat edilirse $\gamma \in \mathsf{F}_{q^n}^*$ elemanının F_{q^n} cisminin bir has alt cismi olan F_{q^d} cisminin bir elemanı olması için gerek ve yeter koşul $\gamma^{q^d} = \gamma$ olmasıdır, yani γ elemanının mertebesinin $q^d - 1$ sayısını bölmesidir. Böylece S kümesinin bir α elemanının mertebesi olan m, $q^n \equiv 1 \pmod{m}$ olacak biçimdeki en küçük pozitif tamsayıdır, yani bu özellikteki n sayısı q sayısının m modülüne göre çarpımsal mertebesidir. $q^n - 1$ sayısının bu özellikteki bir pozitif m böleni için S_m, S kümesindeki mertebesi m olan elemanların kümesi olsun. Bu durumda, S kümesi, S_m alt kümelerinin ayrık birleşimi olduğundan

$$I(q, n; x) = \prod_{m} \prod_{\alpha \in S_m} (x - \alpha)$$

olarak yazılabilir. Böylece S_m kümesi tam olarak, $\mathsf{F}_{q^n}^*$ grubunun m mertebeli tüm elemanlarını bulundurur. Diğer bir ifade ile S_m kümesi, F_q cismi üzerindeki birimin m. ilkel köklerinin kümesidir. Döngüsel polinomların tanımı gereği,

$$\prod_{\alpha \in S_m} (x - \alpha) = \Phi_m(x)$$

olduğundan (3.6) eşitliği elde edilmiş olur.

3.2.13. Örnek. $\mathsf{F}_2[x]$ halkasında derecesi 4 olan tüm monik indirgenemez polinomları belirleyelim. (3.6) eşitliğinden

$$I(2, 4; x) = \Phi_5(x)\Phi_{15}(x)$$

dir. Teorem 2.4.11. (*ii*) özelliği gereği, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ polinomu $\mathsf{F}_2[x]$ halkasında indirgenemezdir. Benzer şekilde $\Phi_{15}(x)$ polinomu $\mathsf{F}_2[x]$ halkasında dereceleri 4 olan iki indirgenemez polinomun çarpımı biçiminde yazılabilir. $\Phi_5(x + 1) = x^4 + x^3 + 1$ polinomu $\mathsf{F}_2[x]$ halkasında indirgenemez olduğundan bu polinom $\Phi_{15}(x)$ polinomunu bölmelidir ve böylece

$$\Phi_{15}(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 = (x^4 + x^3 + 1)(x^4 + x + 1)$$

dir. Dolayısıyla $\mathsf{F}_2[x]$ halkasında derecesi 4 olan monik indirgenemez polinomlar

$$x^4 + x^3 + x^2 + x + 1,\ x^4 + x^3 + 1 \text{ ve } x^4 + x + 1$$

biçimindedir (Lidl ve Neiderreiter 1986).

İndirgenemez polinomlar, çoğu kez bir cisim genişlemesindeki elemanların minimal polinomu olarak ortaya çıkarlar. Daha önce minimal polinomlar ve temel özellikleri ele alınmıştı. Aşağıdaki teoremde de sonlu cisimler kullanılarak minimal polinomlarla ilgili bazı özellikler ele alınacaktır.

3.2.14. Teorem. α, F_q cisminin $\mathsf{F}_q{}^m$ cisim genişlemesindeki bir elemanı olmak üzere α elemanının F_q cismi üzerindeki derecesi d ve minimal polinomu $g(x) \in \mathsf{F}_q[x]$ olsun. Bu durumda

i) $g(x)$ polinomu F_q cismi üzerinde indirgenemezdir ve $d \mid m$ dir.

ii) $f(x) \in \mathsf{F}_q[x]$ polinomunun $f(\alpha) = 0$ eşitliğini gerçeklemesi için gerek ve yeter koşul $g(x) \mid f(x)$ olmasıdır.

iii) $f(x)$ polinomu $\mathsf{F}_q[x]$ halkasında $f(\alpha) = 0$ özelliğinde monik indirgenemez bir polinom ise $f(x) = g(x)$ dir.

iv) $g(x) \mid (x^{q^d} - x)$ ve $g(x) \mid (x^{q^m} - x)$ dir.

v) $g(x)$ polinomunun kökleri $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ dir ve $g(x)$ polinomu tüm bu elemanların F_q cismi üzerindeki minimal polinomudur.

vi) $\alpha \neq 0$ ise ord(g), α elemanının $\mathsf{F}_{q^m}^*$ çarpımsal grubundaki mertebesine eşittir.

vii) $g(x)$ polinomunun F_q cismi üzerinde bir ilkel polinom olması için gerek ve yeter koşul α elemanının $\mathsf{F}_{q^m}^*$ çarpımsal grubunda $q^d - 1$ mertebeli bir elemanı olmasıdır (Lidl ve Neiderreiter 1986).

İspat. *i)* Teorem 1.2.4. (i) gereği, $g(x)$ polinomu F_q cismi üzerinde indirgenemezdir. Diğer yandan $d \mid [\mathsf{F}_q : \mathsf{F}_q{}^m] = m$ olduğu açıktır.

ii) Teorem 1.2.4. (ii) yardımıyla elde edilir.

iii) (ii) özelliğinin bir sonucudur.

iv) (i) özelliği ve Teorem 2.2.4. yardımıyla görülebilir.

v) İspatın ilk kısmı (i) den ve Teorem 2.2.6. yardımıyla, ikinci kısmı (iii) den görülebilir.

vi) $\alpha \in \mathsf{F}_{q^d}^*$ ve $\mathsf{F}_{q^d}^*$, $\mathsf{F}_{q^m}^*$ grubunun bir alt grubu olduğundan Teorem 3.1.3. gereği, istenilen elde edilmiş olur.

vii) $g(x)$, F_q cismi üzerinde ilkel bir polinom ise ord(g) = $q^d - 1$ dir ve böylece (vi) gereği, α elemanı $\mathsf{F}_{q^m}^*$ çarpımsal grubunun $q^d - 1$ mertebeli bir elemanıdır. Tersine α, $\mathsf{F}_{q^m}^*$ çarpımsal grubunun $q^d - 1$ mertebeli bir elemanı ise $\mathsf{F}_{q^d}^*$ grubunda da $q^d - 1$ mertebelidir. Böylece α, $\mathsf{F}_q{}^d$ cisminin bir ilkel elemanıdır ve dolayısıyla Tanım 3.1.16 gereği, $g(x)$ polinomu da F_q cismi üzerinde ilkel bir polinomdur.

Bu kısımda son olarak bir indirgenemez polinomun mertebesi veren bir algoritma verilecektir.

3.2.15. Algoritma (Bir indirgenemez polinomun mertebesi).

Input. Katsayıları F_q cisminden alınan ve derecesi n olan $f(x)$ polinomu ve $q^n - 1$ sayısının $q_1^{e1} \ldots q_k^{ek}$ biçimindeki çarpanlaması.

Output. $f(x)$ polinomunun mertebesi.

1. for $i = 1$ **to** k **do**

2. $f(x) \mid (x^{q_1^{e1} \ldots q_i^{e_i} \ldots q_k^{ek}} - 1)$ olacak biçimdeki en küçük negatif olmayan e_i sayısını bul.

3. end for

4. return $q_1^{e1} \ldots q_k^{ek}$. (Mullen ve Panario 2013).

4. SONLU CİSİMLER ÜZERİNDE ELİPTİK EĞRİLER

Bu bölümde, sonlu cisimlerin bir uygulaması olarak sonlu cisimler üzerinde eliptik eğriler ele alınacak ve sonlu cisimler üzerinde tanımlı eliptik eğriler üzerindeki noktaların belirlenmesi ile ilgili olarak bazı algoritmalar verilecektir. Bunun için ilk olarak Kısım 4.1. de eliptik eğriler ile ilgili bazı önemli tanım ve teoremler ele alınacaktır. Kısım 4.2. de ise sonlu cisimler üzerinde tanımlı eliptik eğriler ele alınacaktır.

4.1. Eliptik Eğriler

Eliptik eğriler, sayılar teorisi, bilgisayar bilimleri gibi bir çok alanda uygulamalara sahip olan önemli bir araştırma konusudur. Eliptik eğriler özellikle Fermat'nın son teoreminin ispatında oldukça önemli bir rol oynamışlardır.

4.1.1. Tanım. F bir cisim ve $a_1, a_2, a_3, a_4, a_6 \in F$ olmak üzere

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

biçimindeki denkleme *uzun Weierstrass normal form* denir. Bu denklemin *Tate değerleri*

$$b_2 = a_1^2 + 4a_2$$

$$b_4 = a_1a_3 + 2a_4$$

$$b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4^2$$

$$c_4 = b_2^2 - 24b_4$$

biçimindedir. Bundan başka *diskriminantı*

$$\Delta(E) = -\, b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6$$

ve *j-değişmezi*

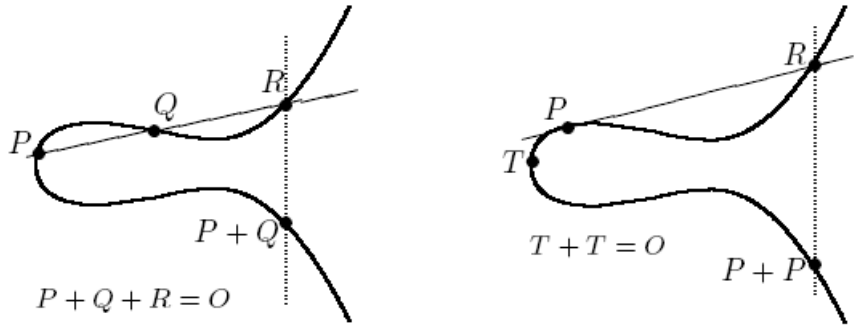
$$j = \frac{c_4^3}{\Delta}$$

olarak tanımlanır.

Bir F cismi üzerinde tanımlı uzun Weierstrass normal formda verilen ve diskriminantı sıfırdan farklı olan bir eğriye üzerindeki $\boldsymbol{O}$ noktasıyla birlikte F cismi üzerinde bir *eliptik eğri* denir.

Tanımda geçen $\boldsymbol{O}$ noktası, sonsuzdaki nokta olarak adlandırılır ve üstelik bu nokta x-eksenine dik olan tüm doğruların kesiştikleri noktadır. Bir eliptik eğri üzerindeki noktaların kümesi üzerinde tanımlanan özel bir toplama işlemine göre bir grup oluşturur. Eliptik eğri üzerinde olduğu varsayılan bu $\boldsymbol{O}$ noktası ise daha sonra da görüleceği gibi bu grubun etkisiz elemanıdır.

Şimdi eliptik eğri üzerindeki noktaların toplama işlemini tanımlayalım: P ve Q, bir E eliptik eğrisi üzerinde farklı iki nokta ise P ve Q noktalarından geçen l doğrusu E eliptik eğrisini, bu noktalardan farklı bir üçüncü noktada keser. Eğer bu noktaya R' denirse P ve Q noktalarının toplamı R' noktasının x eksenine göre simetriği olarak tanımlanır. Eğer $P = Q$ ise, yani E eliptik eğrisi üzerindeki bir nokta kendisi ile toplanmak istenirse bu noktadan geçen teğet doğru dikkate alınır.



Şekil 4.1. Eliptik eğri üzerindeki noktaların toplama işlemi.

Eğer E, F cismi üzerinde tanımlı bir eliptik eğri ise E üzerindeki noktaların kümesi $E(F)$ ile gösterilir ve $E(F)$ kümesi üzerinde yukarıda tanımlanan toplama işlemine göre bir gruptur.

4.1.2. Teorem. E, F cismi üzerinde tanımlı bir eliptik eğri ise $E(F)$ kümesi $\boldsymbol{O}$ noktası ile bir gruptur.

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ olmak üzere belirtilen toplama işlemi aşağıdaki gibi ifade edilebilir:

***i*)** Her $P \in E(F)$ için $P + \boldsymbol{O} = \boldsymbol{O} + P = P$ dir.

***ii*)** P_1 noktasının tersi $-P_1$ ile gösterilir ve $P_1 = (x_1, y_1)$ ise $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$ dir.

***iii*)** $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ olmak üzere $x_1 = x_2$ ve $y_1 + y_2 + a_1x_2 + a_3 = 0$ ise $P_1 + P_2 = \boldsymbol{O}$ dur.

***iv*)** $P_1 \neq -P_2$ olmak üzere $x_1 \neq x_2$ ise

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \mu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} = y_1 - \lambda x_1$$

ve $x_1 = x_2$ ise

$$\lambda = \frac{3y_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \mu = \frac{-3x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} = y_1 - \lambda x_1$$

olsun. Bu durumda $P_1 + P_2 = P_3 = (x_3, y_3)$ olmak üzere

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \quad \text{ve} \quad y_3 = -(\lambda + a_1)x_3 - \mu - a_3$$

dir.

4.2. Sonlu Cisimler Üzerinde Eliptik Eğriler

E, p bir asal sayı, $n \in \mathbb{N}$ ve $q = p^n$ olmak üzere bir $\mathbb{F}_q$ sonlu cismi üzerinde tanımlı bir eliptik eğri ise $E(\mathbb{F}_q)$ sonlu bir abelyen gruptur. Sonlu cisimler üzerindeki eliptik eğriler ile ilgili olarak yapılan çalışmaların çoğu bu eğriler üzerindeki noktaların sayılarının belirlenmesi ile ilgilidir.

4.2.1. Tanım. E, $\mathbb{F}_q$ sonlu cismi üzerinde tanımlı bir eliptik eğri olsun. Her $(x, y) \in E(\overline{\mathbb{F}}_q)$ için

$$\varphi_q : E(\overline{\mathsf{F}}_q) \to E(\overline{\mathsf{F}}_q),\ \varphi_q(x, y) = (x^q, y^q) \text{ ve } \varphi_q(\boldsymbol{O}) = \boldsymbol{O}$$

olarak tanımlanan φ_q endomorfizmine E eliptik eğrisinin *q-Frobenius endomorfizmi* denir.

4.2.2. Teorem. E, F_q sonlu cismi üzerinde tanımlı bir eliptik eğri ve φ_q, E eliptik eğrisinin q-Frobenius endomorfizmi olsun. Bu durumda aşağıdakiler gerçeklenir:

***i*)** $P \in E(\mathsf{F}_q)$ olması için gerek ve yeter koşul $\varphi_q(P) = P$ olmasıdır.

***ii*)** φ_q endomorfizmi tamamıyla ayrılamazdır.

***iii*)** $der(\varphi_q) = q$ dur.

***iv*)** $\varphi_q^2 - a\varphi_q + q = 0$ eşitliğini gerçekleyen bir tek a tamsayısı vardır, diğer bir ifade ile her $P \in E(\mathsf{F}_q)$ için

$$\varphi_q^2(P) - a\varphi_q(P) + qP = \boldsymbol{O}$$

eşitliğini gerçekleyen bir tek a tamsayısı vardır (Schmitt ve Zimmer 2003).

İspat. *i*) φ_q , $\overline{\mathsf{F}}_q$ sonlu cisminin q-Frobenius otomorfizmi olmak üzere "$x \in \mathsf{F}_q$ olması için gerek ve yeter koşul $\varphi_q(x) \in \mathsf{F}_q$ olmasıdır" gerçeğinden elde edilir.

***ii*)** $\mathsf{F}_q(E)$ fonksiyon cismi olmak üzere q-Frobenius endomorfizmi yardımıyla bu fonksiyon cismi üzerinde tanımlanan bir φ_q* endomorfizmi vardır. Şimdi $F/G \in \mathsf{F}_q(E)$ ise her $x \in \mathsf{F}_q$ için $x^q = x$ olduğundan

$$\varphi_q * \left(\frac{F}{G}\right) = \frac{F(X^q, Y^q)}{G(X^q, Y^q)} = \frac{F(X, Y)^q}{G(X, Y)^q}$$

dur. O halde φ_q*($\mathsf{F}_q(E)$) = $\mathsf{F}_q(E)^q$ ve böylece $\mathsf{F}_q(E)$ cisminin $\mathsf{F}_q(E)^q$ cisim genişlemesi tamamıyla ayrılamaz bir cisim genişlemesidir.

***iii*)** $\mathsf{F}_q(E)$ cisminin $\mathsf{F}_q(E)^q$ cisim genişlemesinin derecesinin q olduğundan açıktır.

***iv*)** φ_q Frobenius endomorfizminin duali

$$\hat{\varphi}_q : E(\overline{\mathsf{F}}_q) \to E(\overline{\mathsf{F}}_q),\ \hat{\varphi}_q(x, y) = \frac{der(\varphi_q)}{\varphi_q(x, y)}$$

olmak üzere $\varphi_q - 1$ endomorfizmi dikkate alınırsa

$$der(\varphi_q - 1) = (\varphi_q - 1)(\hat{\varphi}_q - 1)$$

$$= \varphi_q \hat{\varphi}_q - (\varphi_q + \hat{\varphi}_q) + 1$$

$$= der(\varphi_q) - (\varphi_q + \hat{\varphi}_q) + 1$$

dir. Diğer yandan $der(\varphi_q) = q$ olduğundan

$$a = \mathrm{tr}(\varphi_q) = \varphi_q + \hat{\varphi}_q = q + 1 - der(\varphi_q - 1)$$

dir. Şimdi $\varphi_q^2 - a\varphi_q + q = 0$ eşitliğini gerçekleyen bir tek a tamsayısı var olduğunu görelim. q-Frobenius endomorfizminin izi $\mathrm{tr}(\varphi_q)$ ve normu $N(\varphi_q)$, sırasıyla,

$$\mathrm{tr}(\varphi_q) = \varphi_q + \hat{\varphi}_q$$

ve

$$N(\varphi_q) = \varphi_q \hat{\varphi}_q = der(\varphi_q) = \#\mathrm{Ker}(\varphi_q) = q$$

olduğundan

$$0 = (\varphi_q - \varphi_q)(\varphi_q - \hat{\varphi}_q) = \varphi_q^2 - (\varphi_q + \hat{\varphi}_q)\varphi_q + \varphi_q \hat{\varphi}_q) = \varphi_q^2 - \mathrm{tr}(\varphi_q)\varphi_q + N(\varphi_q)$$

dır ve böylece $\varphi_q^2 - a\varphi_q + q = 0$ dır.

4.2.3. Teorem. E, F_q sonlu cismi üzerinde tanımlı bir eliptik eğri ve φ_q, q-Frobenius endomorfizminin izi a olmak üzere

$$\# E(\mathsf{F}_q) = q + 1 - a$$

dir (Schmitt ve Zimmer 2003).

İspat. Teorem 4.2.2. nin ispatında da görüldüğü gibi

$$der(\varphi_q - 1) = \#(\mathrm{Ker}(\varphi_q - 1)) = \#E(\mathsf{F}_q)$$

dir. Böylece

$$a = \mathrm{tr}(\varphi_q) = \varphi_q + \hat{\varphi}_q = q + 1 - \#E(\mathsf{F}_q)$$

dir.

Frobenius endomorfizminin izi için bir üst sınır Hasse tarafından ispat edilmiştir:

4.2.4. Teorem (Hasse Teoremi). E, F_q sonlu cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda a, q-Frobenius endomorfizminin izi olmak üzere

$$|\# E(\mathsf{F}_q) - (q + 1)| = |a| \leq 2\sqrt{q}$$

dır (Silverman 2009).

4.3. Sonlu Cisimler Üzerinde Tanımlı Eliptik Eğriler Üzerindeki Noktaların Sayısının Belirlenmesi

Bu kısımda sonlu bir F_q cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktalarının sayısını belirlemek için bazı algoritmalar verilecek ve naive sayma, Legendre sembolü methodu ve Schoof'un algoritmaları dikkate alınacaktır.

İlk olarak naive sayma için algoritma verilecektir. Bunun için verilen bir F_q sonlu cismi için bir R_q temsil sistemi bulunur ve bu temsil sisteminden alınan her bir elemanın eliptik eğri üzerindeki bir noktanın x-koordinatı olup olmadığı belirlenir. Eğer belirlenen bu elemanın mertebesi 2 ise eliptik eğri üzerinde bir nokta, mertebesi 2 den büyük ise eliptik eğri üzerinde iki farklı nokta olduğu dikkate alınır. Bununla ilgili algoritma aşağıdaki gibi ifade edilir.

4.3.1. Algoritma (Naive Sayma)

Input: q sayısı ve F_q cismi üzerinde tanımlı katsayıları a_1, a_2, a_3, a_4 ve a_6 olan E eliptik eğrisi.

Output: $\#E(\mathsf{F}_q)$ sayısı.

1. $n \leftarrow 1$. /****O*** */

2. F_q cismi için bir R_q temsil sistemi bul.

3. For her $x \in R_q$ **do** :

4. **If** $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ olacak biçimde $y \in R_q$ bulunabilirse **then do:**

5. **If** $y = -y_1 - a_1x_1 - a_3$ **then** $n \leftarrow n + 1$.

else $n \leftarrow n + 2$.

6. Return n. (Schmitt ve Zimmer 2003).

F_q sonlu cisminin karakteristiğinin 2 den farklı olması durumunda aşağıdaki algoritma dikkate alınarak $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ eliptik eğrisi üzerindeki noktaların sayısı belirlenebilir. Doğal olarak bu halde F_q cismindeki kareler belirlenmelidir.

4.3.2. Algoritma (Naive Sayma, kar(F_q) ≠ 2)

Input: q sayısı ve F_q cismi üzerinde tanımlı katsayıları a_2, a_4, a_6 olan E eliptik eğrisi.

Output: $\#E(\mathsf{F}_q)$ sayısı.

1. $n \leftarrow 1$. /****O*** */

2. F_q cismi için bir R_q temsil sistemi bul.

3. F_q cismindeki karelerin kümesini S_q al.

4. For her $x \in R_q$ **do** :

5. **If** $x^3 + a_2x^2 + a_4x + a_6 \in S_q$ **then do:**

6. **If** $x^3 + a_2x^2 + a_4x + a_6 = 0$ **then** $n \leftarrow n + 1$,

7. **else** $n \leftarrow n + 2$.

6. Return n. (Schmitt ve Zimmer 2003).

Legendre sembolünü kullanarak bir sonlu cisim üzerinde tanımlı eliptik eğri üzerindeki noktaların sayısı belirlenenilir.

4.3.3. Teorem. $p > 2$ olmak üzere $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$, F_p sonlu cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda

$$\#E(\mathsf{F}_p) = p + 1 + \sum_{x=0}^{p-1}\left(\frac{x^3 + a_2x^2 + a_4x + a_6}{p}\right)$$

dir. Burada $\left(\frac{\cdot}{p}\right)$ simgesi Legendre sembolünü belirtmektedir (Silverman 2009).

Yukarıdaki teorem kullanılarak eğri üzerindeki noktaların sayısını belirleyen Legendre algoritması verilecektir.

4.3.4. Algoritma (Legendre Sembolü Methodu)

Input: p asal sayısı ve F_p cismi üzerinde tanımlı katsayıları a_2, a_4, a_6 olan E eliptik eğrisi.

Output: $\#E(\mathsf{F}_p)$ sayısı.

1. $n \leftarrow p + 1$.

2. For $x = 0$ to $p - 1$ **do** $n \leftarrow n + \left(\dfrac{x^3 + a_2 x^2 + a_4 x + a_6}{p} \right)$.

3. Return n. (Schmitt ve Zimmer 2003).

Aşağıda özellikle eliptik eğri kriptololojisinde uygulamaları bulunan Schoof'un algoritması verilecektir. Bu algoritmada Çinli Kalan Teoremi ve q-Frobenius endomorfizmi kullanılmaktadır. Algoritmada geçen P kümesi asal sayıların kümesini belirtmektedir.

4.3.5. Algoritma (Schoof).

Input: $q = p^k$ asal kuvveti ve F_q cismi üzerinde tanımlı E eliptik eğrisi.

Output: $a = q + 1 - \#E(\mathsf{F}_q)$ sayısı.

1. $l_{maks} \leftarrow \min\{p \in \mathsf{P} \mid \prod_{l \in P, l \le p} l > 4\sqrt{q}\}$.

2. If $2 \mid q$ **then do**:

3. **If** $j(E) = 0$ **then** $a_2 \leftarrow 1$, **else** $a_2 \leftarrow 0$,

4. else do:

5. **If** $\#E(\mathsf{F}_q)[2] = 1$ **then** $a_2 \leftarrow 1$, **else** $a_2 \leftarrow 0$.

6. For her $l \in \mathsf{P}$, $3 \le l \le l_{maks}$, **do:**

7. Keyfi bir $P \in E[l] \backslash \{\boldsymbol{O}\}$ noktası al.

8. $0 \le q_l < l$, $q_l \equiv q \pmod{l}$ için $\varphi_q^2(P) + q_l P$ değerini hesapla.

9. **For** $t = 0$ **to** l **do:**

10. $t\varphi_q(P)$ değerini hesapla.

11. **If** $t\varphi_q(P) = \varphi_q^2(P) + q_l P$ **then do**:

12. $a_l \leftarrow t$.

13. 6. adımdaki bir sonraki asala git.

14. Her $l \in \mathsf{P}$, $2 \leq l \leq l_{maks}$ için $|a| \leq 2\sqrt{q}$ ve $a \equiv a_l \pmod{l}$ özelliğindeki a sayısını belirmek için Çinli Kalan Teoremini kullan.

15. Return a. (Schmitt ve Zimmer 2003).

KAYNAKLAR

Asar, A. O., Arıkan, A., Arıkan, A. 2009. Cebir. Eflatun Yayınları, Ankara, 528 s.

Conrad, K. 2013. www.math.uconn.edu/~kconrad/blurbs/galoistheory/finitefields.pdf - (Erişim tarihi: 31.03.2017)

Fraleigh, J. B. 2003. A first course in abstract algebra. Addison-Wesley, 513 pp.

Gezer, B., Bizim, O. 2017. Soyut cebir. Dora Yayıncılık, Bursa, 662 s.

Herstein, I.N. 1999. Abstract algebra. Prentice-Hall, Inc., New Jersey, 249 pp.

Hungerford, T. W. 1974. Algebra. Springer - Verlag New York Inc., USA, 493 pp.

Lidl, R., Neiderreiter, H. 1986. Introduction to finite fields and their applications. Cambridge University Press, USA, 401 pp.

Mullen, G., Panario, D. 2013. Hand book of finite fields. Crc Press, USA, 1033 pp.

Schmitt, S., Zimmer, H. G. 2003. Elliptic curves. Walter de Gruyter GmbH & Co., Berlin, Germany, 367 pp.

Silverman, J.S. 2009. The arithmetic of elliptic curves. Springer Science+Business Media, New York, USA, 513 pp.

ÖZGEÇMİŞ

Adı Soyadı	: Ayşe Keskin
Doğum Yeri ve Tarihi	: Bozkır, 08.10.1987
Yabancı Dili	: İngilizce
Eğitim Durumu (Kurum ve Yıl)	
Lise	: Küçükyalı Halit Armay Lisesi, 2005
Lisans	: İstanbul Üniversitesi Fen - Edebiyat Fakültesi Matematik Bölümü, 2011
Yüksek Lisans	: Uludağ Üniversitesi Fen Bilimleri Enstitüsü, 2017
Çalıştığı Kurum/Kurumlar ve Yıl	:
İletişim (e-posta)	: eskinay@yahoo.com
Yayınları	: