**T.C.**
**RECEP TAYYİP ERDOĞAN ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**
**MATEMATİK ANABİLİM DALI**

**YÜKSEK LİSANS TEZİ**

# FUZZY CİSİM GENİŞLEMELERİ

**Neslihan YILMAZ**

**TEZ DANIŞMANI**
**Dr. Öğr. Üyesi Ümit DENİZ**
**JÜRİ ÜYELERİ**
**Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU**
**Dr. Öğr. Üyesi Tuncay KÖROĞLU**

**RİZE-2020**

**T.C.**
**RECEP TAYYİP ERDOĞAN ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

**FUZZY CİSİM GENİŞLEMELERİ**

Dr. Öğr. Üyesi Ümit DENİZ danışmanlığında, Neslihan YILMAZ tarafından hazırlanan bu çalışma Enstitü Yönetim Kurulu kararı ile oluşturulan jüri tarafından 29/01/2020 tarihinde Matematik Anabilim Dalı'nda **YÜKSEK LİSANS** tezi olarak kabul edilmiştir.

| **Jüri Üyeleri** | **Unvanı, Adı Soyadı** | **İmza** |
|---|---|---|
| Başkan | : Dr. Öğr. Üyesi Tuncay KÖROĞLU | |
| Üye | : Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU | |
| Üye | : Dr. Öğr. Üyesi Ümit DENİZ | |

**Doç. Dr. Ferhat KALAYCI**
**ENSTİTÜ MÜDÜRÜ**

# ÖNSÖZ

Bu çalışmam esnasında büyük bir sabır ve özveriyle bana yardımcı olan sayın hocam Dr. Öğr. Üyesi Ümit DENİZ'e, tüm hayatım boyunca desteklerini esirgemeyen her zaman yanımda olan tüm başarılarımın temeli olan annem Keziban YILMAZ'a, babam Hasan YILMAZ'a ve kardeşim Cengizhan YILMAZ'a canı gönülden teşekkür ederim.

Yüksek lisans öğrenimim boyunca derslerime göre okul programımı ayarlayan halen görev yapmakta olduğum Rize Anadolu İmam Hatip Lisesi idaresine, Başmüdür yardımcısı Adem AĞZIKARA'ya, tez içindeki düzeltmelerde yardımcı olan değerli meslektaşlarım Sema CERRAH, Hatice BALCI ve Selver ÖNELGE'ye, ingilizce özet konusunda yardımcı olan meslektaşım Selmanur ÖZDEMİR'e ve öğrencilerime teşekkür ederim.

Tabi ki arada bir "Bu gün tezin için ne yaptın?" diyerek beni çalışmaya ve vicdani rahatsızlığa sürükleyen canım arkadaşım Şule Merve ULUDÜZ'e ve güzel arkadaşlarım Elif ŞENCAN ve Şeyma Nur YURTOĞLU'na teşekkür ederim.

Neslihan YILMAZ

## TEZ ETİK BEYANNAMESİ

Tarafımdan hazırlanan "Fuzzy Cisim Genişlemeleri" başlıklı bu tezi, Yükseköğretim Kurulu Bilimsel Araştırma ve Yayın Etiği Yönergesindeki hususlara uygun olarak hazırladığımı ve aksinin ortaya çıkması durumunda her türlü yasal işlemi kabul ettiğimi beyan ederim. 29/01/2020

Neslihan YILMAZ

***Uyarı:*** *Bu tezde kullanılan özgün ve/veya başka kaynaklardan sunulan içeriğin kaynak olarak kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.*

# ÖZET

## FUZZY CİSİM GENİŞLEMELERİ

**Neslihan YILMAZ**

**Recep Tayyip Erdoğan Üniversitesi**
**Fen Bilimleri Enstitüsü**
**Matematik Anabilim Dalı**
**Yüksek Lisans Tezi**
**Danışmanı: Dr. Öğr. Üyesi Ümit DENİZ**

Bu çalışma iki kısımdan oluşmaktadır. Birinci kısımda cisim genişlemelerinin çeşitleri tanım, teorem ve örnekler verilerek araştırılıp derlenmiştir. İkinci kısımda cisim genişlemelerinin fuzzy cebirine uyarlanması araştırılmış ve Ayrılabilir Fuzzy Cisim Genişlemeleri, Tamamen Ayrılamaz Fuzzy Cisim Genişlemeleri ve Lineer Parçalanma konuları ele alınmıştır. Bu başlıklar klasik cebire paralel olarak incelenmiş ve klasik cebirdeki temel tanım ve teoremler bu konular için fuzzy cebire taşınmıştır. Fuzzy cisim genişlemeleri için temel tanım ve teoremler ele alınıp örneklendirilmiştir.

**2020, 136 sayfa**

**Anahtar Kelimeler:** Ayrılabilir Fuzzy Cisim Genişlemeleri, Tamamen Ayrılamaz Fuzzy Cisim Genişlemeleri, Lineer Parçalanma.

## ABSTRACT

### FUZZY FIELDS EXTENSIONS

**Neslihan YILMAZ**

**Recep Tayyip Erdogan University**
**Graduate School of Natural and Applied Sciences**
**Department of Mathematic**
**Master Thesis**
**Supervisor: Asst. Prof. Umit DENIZ**

This study includes two parts. Types of field extensions were analyzed and compiled with definitions, theorem and examples in the first part. The adaptation of field extensions to the fuzzy algebra was analyzed and Seperable Fuzzy Field Extensions, Purely İnseperable Fuzzy Field Extensions and Lineer Discointness were discussed in the second part. These titles were studied parallel to classical algebra and the main definitions and theorems in classical algebra were transferred into fuzzy algebra. Main definitions and theorems for fuzzy field extensions were discussed and examplified.



**2020, 136 pages**

**Keywords:** Seperable Fuzzy Field Extensions, Purely İnseperable Fuzzy Field Extensions, Lineer Discointnes.

# İÇİNDEKİLER

## ŞEKİLLER DİZİNİ

## TABLOLAR DİZİNİ

## SEMBOLLER ve KISALTMALAR DİZİNİ

| | |
|---|---|
| $a\|b$ | $a$ Böler $b$ |
| $a \nmid b$ | $a$ Bölmez $b$ |
| $o(a)$ | $a$'nın Mertebesi |
| $a^{-1}$ | $a$'nın Tersi |
| $\mu_a$ | $a$-Seviye Fuzzy Alt Küme |
| $\subset$ | Alt Kümesi |
| $\subseteq$ | Alt Kümesi veya Eşit |
| $\not\subseteq$ | Alt Kümesi Değil ve Eşit Değil |
| $A/B$ | A, B'nin Fuzzy Cisim Genişlemesi |
| $AB$ | A ve B Kümelerinin Bileşiği |
| $A \times B$ | A ve B Kümelerinin Kartezyen Çarpımı |
| $sup(B)$ | B Kümesinin Supremumu |
| $\inf(B)$ | B Kümesinin İnfimumu |
| $F(s)$ | Basit Cisim Genişlemesi |
| $\exists$ | Bazı |
| $\cup$ | Birleşim |
| $\circ$ | Bileşke |
| $\emptyset$ | Boş Küme |
| $>$ | Büyük |
| $\geq$ | Büyük veya Eşit |
| $\delta_{B^*}$ | $B^*$ ın Karakteristik Fonksiyonu |
| $C\|_{C^*}$ | C'nin $C^*$ ile Kısıtlanışı |
| $\sim$ | Denklik Bağıntısı |
| $\mathbb{Q}(D)$ | D'nin Kesirler Cismi |

| | |
|---|---|
| $D_F$ | D'nin F İçindeki Kesirler Cismi |
| $\phi_u$ | Değer Fonksiyonu |
| $F \leq E$ | E, F'nin Cisim Genişlemesi |
| $[E : F]$ | E'nin F Üzerindeki Boyutu |
| $Aut(E)$ | E'nin Otomorfizma Grubu |
| $G(E/F)$ | E'nin F Üzerindeki Grubu |
| $\Delta(E)$ | E'nin Asal Cismi |
| $\{E : F\}$ | E'nin F Üzerindeki İndeksi |
| $Ara(E/F)$ | E'nin F'yi İçeren Bütün Alt Cisimlerinin Kümesi |
| $\in$ | Elemanı |
| $\notin$ | Elemanı Değil |
| $=$ | Eşit |
| $\neq$ | Eşit Değil |
| $\bar{F}$ | F'nin Cebirsel Kapanışı |
| $\Im$ | F'nin Bütün Fuzzy Alt Cisimlerinin Kümesi |
| $F[S]$ | F'ye S'nin Katılmasıyla Elde Edilen Alt Halka |
| $F(S)$ | F'ye S'nin Katılmasıyla Elde Edilen Alt Cisim |
| $Ker(f)$ | $f$ Fonksiyonunun Çekirdeği |
| $f: A \to B$ | $f$, A'dan B'ye Bir Fonksiyon |
| $\sigma_p$ | Frobenius Otomorfizması |
| $F^*$ | $F \setminus \{0_F\}$ |
| $[0,1]^x$ | Fuzzy Kuvvet Kümesi |
| $\|G\|$ | G Kümesinin Kardinalitesi |
| $B \longrightarrow G(E/B)$ | Galois Eşlemesi |
| $E_H$ | H'nin E İçindeki Sabit Cismi |
| $\forall$ | Her |

| | |
|---|---|
| $\wedge$ | İnfimum |
| $\cong$ | İzomorfizm |
| $\supset$ | Kapsar |
| $\supseteq$ | Kapsar veya Eşit |
| $\not\supseteq$ | Kapsamaz ve Eşit Değil |
| $\cap$ | Kesişim veya Arakesit |
| $<$ | Küçük |
| $\leq$ | Küçük veya Eşit |
| $\mathbb{C}$ | Kompleks Sayılar Kümesi |
| $\langle M \rangle$ | M'nin Ürettiği Alt Grup |
| $\Phi_n(x)$ | $n$-yinci Döngüsel Polinom |
| $e$ | Negatif Olmayan Tam Sayı |
| $\triangleleft$ | Normal Alt Grup |
| $L(P,Q)$ | P ve Q'dan Geçen Doğru |
| $\lvert PQ \rvert$ | PQ Doğrusunun Uzunluğu |
| $C(P,Q)$ | P Merkezli Ve Yarıçapı $\lvert PQ \rvert$ Olan Çember |
| $GF(p^n)$ | $p^n$ Elemanlı Bir Galois Cismi |
| $U(R)$ | R'nin Birimsellerinin Kümesi |
| $Kar(R)$ | R Halkasının Karakteristiği |
| $P(R)$ | R Üzerinde Tanımlı Polinomların Kümesi |
| $\mathbb{R}$ | Reel Sayılar Kümesi |
| $F(X)$ | Rasyonel Fonksiyonlar Cismi |
| $\mathbb{Q}$ | Rasyonel Sayılar Kümesi |
| $(x,y)$ | Sıralı İkili |
| $\vee$ | Supremum |
| $\mathbb{Z}$ | Tam Sayılar Kümesi |

| | |
|---|---|
| $\mathbb{Z}_p$ | Tam Sayılarda $p$ Modülüne Göre Kalan Sınıflarının Kümesi |
| TÇAB | Tek Türlü Çarpanlara Ayırma Bölgesi |
| TÇB | Tek Çarpanlama Bölgesi |
| $\psi_{u,v}$ | Temel İzomorfizma |
| TİB | Temel İdeal Bölgesi |
| K | Tüm Çizilebilir Kompleks Sayıların Kümesi |
| $Sym(U)$ | U Kümesi Üzerindeki Tanımlı Bütün Permütasyonlarının Grubu |
| $der(u,F)$ | $u$'nun F Üzerindeki Derecesi |
| $\dot{I}nd(u,F)$ | $u$'nun F Üzerindeki İndirgenmez Polinomu |
| $\beta$ | X'den X'e Bağıntı |
| $\mu : X \to [0,1]$ | X'den [0,1]'e Tanımlı Fonksiyon |
| $1_Y$ | Y'nin Karakteristik Fonksiyonu |
| $\bar{z}$ | $z$'nin Eşleniği |
| $S_n$ | $\{1,\ 2, \dots, n\}$ Kümesi Üzerindeki Bütün Permütasyonların Kümesi |
| $a_{\{x\}}$ | [0,1]-Fuzzy Singleton |
| $f(\mu)$ | $\mu$'nün $f$'de Fuzzy Görüntü Kümesi |
| $\mu^*$ | $\mu$'nün Destekleyicisi |
| $f^{-1}(v)$ | $v$'nün $f$'de Ters Fuzzy Görüntü Kümesi |
| $F^p$ | $\{a^p : a \in F\}$ |
| $\mathbb{Q}(\sqrt{p})$ | $\{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$ |
| $\mu_*$ | $\{x \in X :\ \mu(x) = \mu(e)\}$ |
| $A_\#$ | $\{x \in F \mid A(x) = 1\}$ |

# 1. GENEL BİLGİLER

## 1.1. Giriş

Lütfi Ali Askerzade Berkeley Üniversitesi Elektrik Elektronik Mühendislik Araştırma Laboratuvarı'nda sürdürdüğü çalışmalar esnasında teknik bir probleme çözüm arayışındaydı. Zadeh, klasik mantığının öznel veya belirsiz fikirleri temsil eden verileri belirleyemediğini gözlemledi, bu nedenle klasik mantığın, insan akıl yürütme sürecine benzer şekilde gri tonları ile veriler arasındaki farkları belirlemesi için bulanık mantık kavramını ortaya attı. Çalışmalarını 1965'te "Information and Control" dergisinde "Fuzzy Sets" başlığıyla yayınlamasıyla bulanık küme kavramını (fuzzy logic) cebire kazandırdı. (Zadeh, 1965)

Klasik mantıkta bir olgu doğruysa "1" yanlışsa "0" denir. Oysa günlük hayatta karşılaştığımız her durum için kesin doğru ya da kesin yanlış ifadelerini kullanamayız. İnsan beyninin algısında sıcakla çok sıcak, soğukla az soğuk, pişmişle az pişmiş, çok pişmiş arasında farklar vardır. Az ve çok gibi zarflarla ortaya belirsizlik çıkmaktadır. Bir kantindeki görevliden az kahve dediğinizde bunu size göre ayarlarken bir makineden çay alırken sadece tuşlara basarak seçeneklerinizi belirlersiniz ve makine dilinde "az" yoktur, bastığınız tuşlar 1 basmadıklarınız 0'dır.

Bulanık küme kavramı uygulamalı ve teorik bilimlerde kullanılmaktadır. Çok sayıda araştırmacı ve bilim adamı cebirsel yapılar üzerinde bulanık(fuzzy) kavramı üzerinde çalışmıştır ve fuzzy kavramı genişletilmiştir. Rosenfeld (1971) fuzzy küme kavramını kullanarak bulanık grup teoriyi geliştirmiştir. Katsonas ve Liu (1977) de ilk olarak fuzzy alt vektör uzayı tanımını vermişlerdir. Fakat Nanda (1986) fuzzy küme kavramını cisim ve lineer uzaylara uyarlamıştır ve fuzzy alt vektör uzayı Nanda'ya göre " bir fuzzy alt cismi üzerinde fuzzy alt vektör uzayı" tanımının özel halidir. Das (1981) seviye alt grupları üzerinde çalışmıştır. Liu (1983) fuzzy grupları kullanarak fuzzy halkalar ve bulanık idealler üzerinde çalışmıştır. Mukherje ve Bhattacharya (1984) fuzzy normal alt grup ve fuzzy yan cümleleri, Mukherjee ve Sen (1987) fuzzy idealleri, Malik ve Mordeson (1990) fuzzy asal idealleri tanımlamışlardır. Dixit ve arkadaşları (1992) fuzzy halkaları, Kuraoka ve Kuroki (1992) fuzzy bölüm halkalarını incelemişlerdir. Mordeson (1992) fuzzy cisim genişlemeleri üzerinde çalışmıştır. De Gang (1998) çalışmasında fuzzy halkalar ve fuzzy bölüm halkalarını araştırmış ve

bunlara ait sonuçlar elde etmiştir. Ersoy (2003) fuzzy alt grupların ve fuzzy ideallerin kartezyen çarpımı üzerine çalışmıştır. Uygulama alanında da çalışmalar olmuştur. Maiers ve Sherief (1985) çalışmalarında bulanık mantığı uygulama alanlarına ayırmış ve her uygulamanın kaynağını da belirterek liste halinde vermişlerdir. Bulanık mantığın uygulama alanlarından bazıları görüntü işleme, bilgi depolama ve yeniden çağırma, bilgi tabanlı sistemler, robotik, ticari elektronik ürünler vb. Denetim sistemleri bulanık mantığın en çok uygulandığı alan olarak günümüze gelmektedir.

Bu tezin amacı cisim genişlemeleri ve fuzzy cisim genişlemeleri hakkında temel özellikleri incelemek ve bu yapılardan elde edilen sonuçları ortaya koymaktır.

Bu kısımdaki Tanım ve Teoremler Taşçı (2010), Asar, Arıkan (2012), Çallıalp (2012, 2013), Karakaş (2008), Gezer, Bizim (2017), Harmancı (1987) ve Fraleigh (2013)'den derlenmiştir.

## 1.2. Grup Tanımı ve Özellikleri

**Tanım 1.2.1**. G boş olmayan bir küme ve üzerinde bir $*$ ikili işlemi tanımlansın. Eğer

(i) Her $a, b, c \in G$ için
$(a * b) * c = a * (b * c)$
ise ($*$ işlemi birleşme özelliğini sağlar);

(ii) Her $a \in G$ için
$a * e = e * a = a$
olacak şekilde bir $e \in G$ varsa ( e'ye G'nin birim elemanı denir);

(iii) Her $a \in G$ için
$a * a' = a' * a = e$
olacak şekilde bir $a' \in G$ varsa ($a'$ ne $a$'nın bir ters elemanı denir)
o zaman $(G,*)$ sıralı ikilisine bir *grup* denir.

Aynı zamanda her $a, b \in G$ için $a * b = b * a$ ise bu gruba *değişmeli* ya da *abelyen grup* denir.

**Tanım 1.2.2.** G bir grup H, G'nin boş olmayan bir alt kümesi olsun. Eğer H, G'deki işlemlere göre kendi başına bir grup ise H'ye G'nin bir alt grubu denir ve $H \leq G$ ile gösterilir.

**Teorem 1.2.3.** G bir grup ve $\emptyset \neq H \subset G$ olsun. H'nin bir alt grup olması için gerek ve yeter şart

*i.* $\forall a, b \in H$ için $ab \in H$

*ii.* $\forall a \in H$ için $a^{-1} \in H$ olmasıdır.

**Tanım 1.2.4.** $M \subset G$ olmak üzere M'yi kapsayan, G'nin bütün alt gruplarının arakesitine M'*nin ürettiği alt grup* denir ve $< M >$ ile gösterilir. M'nin elemanlarına $< M >$ grubunun *üreteçleri* denir.

**Tanım 1.2.5.** Bir G grubu için, $G =< M >$ olacak şekilde bir $M \subset G$ alt kümesi varsa, G'ye M ile *üretilmiş grup* denir. Eğer M sonlu bir küme ise G'ye *sonlu üretilmiş grup* ve $M = \{a\}$ tek elemanlı bir küme ise G'ye $a$ ile üretilmiş *devirli grup* denir ve $G =< a >$ şeklinde gösterilir.

G bir grup ve $a \in G$ olsun. $a$'nın ürettiği grup G çarpımsal grup olarak alınırsa $< a > = \{a^n : n \in \mathbb{Z}\}$, toplamsal grup olarak alınırsa $< a > = \{na : n \in \mathbb{Z}\}$ dir.

**Tanım 1.2.6.** G bir grup ve $a \in G$ olsun. $a$'nın ürettiği $< a >$ devirli grubunun mertebesine $a$ elemanının *mertebesi* denir ve $o(a)$ ile gösterilir.

$o(a) = n,\ a^n = e$ koşulunu sağlayan $n > 0$ tamsayıları arasındaki en küçük olanıdır.

**Sonuç 1.2.7.** $G = \langle a \rangle$ devirli grubu verilsin. Eğer G sonsuz ise G'nin üreteçleri $a$ ve $a^{-1}$ den oluşur. Eğer $|G| = m$ bir sonlu sayı ise $a^s$ nin üreteç olması için gerek ve yeter şart $(s, m) = 1$ olmasıdır.

**Tanım 1.2.8.** G ve H iki grup olmak üzere G'den H'ye $\varphi$ fonksiyonu tanımlansın. Eğer her $a, b \in G$ için

$$\varphi(ab) = \varphi(a)\varphi(b)$$

ise $\varphi$'ye G'den H'ya bir *grup homomorfizması* denir.

Aynı zamanda $\varphi$ bire bir ise $\varphi$'ye bir *grup monomorfizması*; $\varphi$ örten ise $\varphi$'ye bir *grup epimorfizması* ve $\varphi$ hem bire bir ve hem de örten ise $\varphi$'ye bir *grup izomorfizması* denir. $\varphi$ bir izomorfizma ise G, H'ya *izomorftur* denir ve $G \cong H$ ile gösterilir. Ayrıca $G = H$ ve $\varphi$, G'den G'ye bir izomorfizma ise $\varphi$'ye G'nin bir otomorfizması denir.

**Tanım 1.2.9.** $f: G \to H$ bir homomorfizma ise $f^{-1}(e_H) = \{a \in G : f(a) = e_H\}$ kümesine $f$ homomorfizmasının *çekirdeği* denir ve $\text{Ç}ekf$ veya $Kerf$ ile gösterilir.

**Teorem 1.2.10.** *(Birinci izomorfizma Teoremi)* $\varphi: G \to H$ bir grup epimorfizması olmak üzere $G/\,Ker(\varphi) \cong H$ dır.

**Teorem 1.2.11.** G bir grup, $\{e\} = H_0 \leq H_1 \leq \cdots \leq H_n = G$ ve G'nin alt gruplarının bir artan zinciri olsun. Her $0 \leq i < n$ için $H_i, H_{i+1}$ içinde normal ise;

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

ise bu zincire G'nin bir *alt normal serisi* denir. Her $0 \leq i \leq n$ için $H_i \lhd G$ ise seriye *normal seri* denir. Eğer $H = H_0 = H_1 = \cdots = H_n = G$, G'nin altgrupları olmak üzere $H = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$ ise H'ya G'nin bir *alt normal alt grubu* denir.

**Tanım 1.2.12.** G bir grup ve

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

G'nin bir alt normal serisi olsun. Her $0 \leq i < n$ için $H_{i+1}/H_i$ bölüm grubu abelyan ise G'ye *çözülebilir grup* denir.

**Teorem 1.2.13.** G bir çözülebilir grup ise her alt grubu ve her bölüm grubu çözülebilirdir.

**Sonuç 1.2.15.** $n \geq 5$ olsun. $S_n$ permütasyonlarının grubu çözülebilir değildir.

**Teorem 1.2.16.** G bir grup ve N, G'nin normal alt grubu olsun. Eğer N ve $G/N$ çözülebilir ise G çözülebilirdir.

### 1.3. Halka Tanımı ve Özellikleri

**Tanım 1.3.1.** R $\neq \emptyset$ olmak üzere her $a, b \in R$ için

$$+ : (a, b) \to a + b, \quad \cdot : (a, b) \to a \cdot b$$

şeklinde tanımlı ve sırasıyla, toplama ve çarpma işlemleri verilsin. Eğer

(i) $(R, +)$ bir abelyen grup ise,

(ii) $\forall a, b, c \in R$ için $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ise,

(iii) $\forall a, b, c \in R$ için

$a \cdot (b + c) = a \cdot b + a \cdot c$ (soldan dağılma özelliği)

$(a + b) \cdot c = a \cdot c + b \cdot c$ (sağdan dağılma özelliği) ise,

o zaman $(R, +, \cdot)$ sıralı üçlüsüne *halka* denir.

$(R, +, \cdot)$ halka olmak üzere $a, b \in R$ için $a \cdot b = b \cdot a$ ise halkaya bir *değişmeli halka* denir. R'nin toplamsal birimi (sıfırı) $0_R$ ile gösterilir. Eğer her $a \in R$ için $a \cdot 1_R = 1_R \cdot a = a$ olacak şekilde $1_R \in R$ varsa $1_R$ elemanına halkanın *birim elemanı* denir. Halkaya da *birimli halka* denir. $R = \{0_R\}$ halkasının birimi $1_R \neq 0_R$ dir.

Devamında $(R, +, \cdot)$ halkası daha sade olarak R ile $a \cdot b$ çarpımıda $ab$ ile gösterilecektir.

**Tanım 1.3.2.** R bir halka olmak üzere $\forall a, b, c \in R$ ve $a \neq 0_R$ için $ab = ac$ iken $b = c$ ise R içinde *sol sadeleştirme* ve $ba = ca$ iken $b = c$ ise R içinde *sağ sadeleştirme* özellikleri sağlanır.

**Tanım 1.3.3**. R bir halka ve $a, b \in R$ olsun. $a \neq 0_R$ için $ab = 0_R$ olacak şekilde $b \neq 0_R \in R$ varsa $a$'ya bir *sol sıfır böleni*, $a \neq 0_R$ için $ba = 0_R$ olacak şekilde $b \neq 0_R \in R$ varsa $a$'ye bir *sağ sıfır böleni* ve böyle bir b elemanı yoksa $a$ sıfır böleni değildir denir. Ne sol sıfır böleni ne sağ sıfır böleni bulunan bir halkaya da *sıfır bölensiz halka* denir.

**Tanım 1.3.4**. R birimli bir halka ve $0_R \neq a \in R$ olsun. Eğer $ab = 1_R$ olacak biçimde $b \in R$ varsa b'ye $a$'nın *sağ tersi* ve $ca = 1_R$ olacak biçimde $c \in R$ varsa c'ye $a$'nın *sol tersi* denir. $a$'nın sağ ve sol tersi birbirine eşittir; yani $a$'nın tersi tektir. Eğer $d \in R$ olmak üzere $ad = da = 1_R$ ise d'ye $a$'nın bir tersi ve $a$'ya *tersinir (birimsel) eleman* denir. Dolayısıyla $a$'nın tersi, varsa $a^{-1}$ ile gösterilir.

**Tanım 1.3.5.** R birimli değişmeli bir halka ve $1_R \neq 0_R$ olmak üzere R sıfır bölensiz ise R'ye bir *tamlık bölgesi* denir.

**Tanım 1.3.6.** R birimli bir halka ve $1_R \neq 0_R$ olmak üzere R'nin sıfırdan farklı her elemanı tersinir ise R'ye bir *bölme halkası* denir. Değişmeli bir bölme halkasına *cisim* denir.

R birimli bir halka ve $(R,+)$ bir abelyan gruptur. Ancak $(R,\ \cdot)$ bir grup değildir. Fakat R'nin birimsellerinin kümesi $U(R)$ çarpma işlemine göre bir gruptur.

**Tanım 1.3.7.** R bir halka ve $\emptyset \neq A \subset R$ olsun. R'deki işlemlere göre A kümesi kendi başına bu işlemlere göre bir halka ise A'ya R'nin bir *alt halkası* denir.

$\{0_R\}$ ve R'ye R'nin *aşikar alt halkaları* ve R'nin kendisinden farklı her alt halkasına R'nin bir *öz alt halkası* denir.

**Tanım 1.3.8.** R bir halka ve $\emptyset \neq I \subset R$ olsun. Eğer $a,b \in I$ için $a-b \in I$ için her $a \in I$ ve $r \in R$ için $ra \in I$ ise I'ya R'nin bir *sol ideali* ve her $a \in I$ ve $r \in R$ için $ar \in I$ ise I'ya R'nin bir *sağ ideali* denir. Eğer hem sol ideal hem sağ ideal ise I'ya R'nin bir ideali denir.

$\{0_R\}$ ve R, her R halkasının idealleridir. $\{0_R\}$ ve R'ye R'nin *aşikar idealleri* ve R'nin R'den farklı her idealine bir *öz ideali* denir.

**Tanım 1.3.9.** R bir halka ve $X \subseteq R$ olmak üzere R'nin X'i içeren bütün ideallerinin kesişimine *X tarafından üretilen ideal* denir ve $\langle X \rangle$ ile gösterilir. Eğer $X = \{x_1, x_2, \dots, x_n\}$ ise $\langle \{x_1, x_2, \dots, x_n\} \rangle = \langle x_1, x_2, \dots, x_n \rangle$ ile gösterilir ve buna $x_1, x_2, \dots, x_n$ *tarafından üretilen ideal* denir. $n = 1$ için $\langle x_1 \rangle$ idealine $x_1$ tarafından üretilen *temel ideal* denir. Her ideali temel ideal olan bir tamlık bölgesine *temel ideal bölgesi* denir ve TİB ile gösterilir.

**Tanım 1.3.10.** R bir halka ve $M \neq R$ olmak üzere M, R halkasının bir ideali olsun. Eğer R halkasının M idealini bulunduran M ve R'den başka ideali yoksa M'ye R'nin bir *maksimal ideali* denir.

**Tanım 1.3.11.** R değişmeli bir halka, $P \neq R$ ve P, R'nin bir ideali olsun. Eğer her $a,b \in R$ için $ab \in P$ iken $a \in P$ ya da $b \in P$ ise P'ye R'nin bir *asal ideali* denir.

**Tanım 1.3.12.** D bir tamlık bölgesi ve $S = \{(a,b) : a,b \in D \ ve \ b \neq 0_D\}$ olsun. Her $(a,b),\ (c,d) \in S$ olmak üzere S kümesi üzerinde

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc$$

şeklinde bir denklik bağıntısı tanımlıdır. Her $(a,b) \in S$ denklik sınıfı, $\mathbb{Q}$'nun elemanlarına benzemesi için $\frac{a}{b}$ biçiminde gösterilir. Böylece

$\frac{a}{b} = \{(c,d) \in S : ad = bc\}$

dir. Buna bir *biçimsel kesir* denir.

$\mathbb{Q}(D) = \left\{\frac{a}{b} : \ a, b \in D \ ve \ b \neq 0_D\right\}$ olsun. $\mathbb{Q}(D)$ üzerinde tanımlanmış olan toplama ve çarpma işlemleri sırasıyla şu şekildedir: $\frac{a}{b}, \ \frac{c}{d} \in \mathbb{Q}(D)$ olsun.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

ve

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

olsun.

**Lemma 1.3.13.** $\mathbb{Q}(D)$ üzerinde tanımlanan toplama ve çarpma iyi tanımlıdır.

**Teorem 1.3.14.** $\mathbb{Q}(D)$ üzerinde yukarıda tanımlı toplama ve çarpma işlemlerine göre cisimdir.

Belirlenen $\mathbb{Q}(D)$ cismine D'nin *kesirler (bölümler) cismi* denir.

**Teorem 1.3.15.** D tamlık bölgesi F cisminin içinde olsun ve F'nin D'yi içeren en küçük alt cismi $D_F$ olsun. O zaman $\mathbb{Q}(D) \cong D_F$ dir. Özel olarak bir cismin kesirler cismi kendisine izomorftur (Bir D tamlık bölgesinin herhangi iki kesirler cismi izomorftur).

$D_F = \{ab^{-1} : a, b \ \in D \ ve \ b \neq 0_D\}$ cismine D'nin F içindeki *kesirler cismi* denir.

**Tanım 1.3.16.** R birimli bir halka olmak üzere terimleri R'nin elemanları olan $(a_0, a_1, a_2, \dots, a_n, 0_{R,} 0_{R,} \dots)$ biçimindeki bir diziye *R üzerinde bir belirsizin polinomu* denir. R üzerinde tanımlı polinomların kümesi P(R) ile gösterilir.

$f, g \in P(R)$ ve $f = (a_0, a_1, a_2, \dots), \ g = (b_0, b_1, b_2, \dots)$ olsun. $P(R)$ üzerinde tanımlı toplama ve çarpma işlemleri sırasıyla şu şekildedir:

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$$

$k \geq 0$ için $c_k = \sum_{i=0}^{k} a_i b_{k-i} = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 = \sum_{i+j=k} a_i b_j$ olmak üzere

$f.g = (c_0, c_1, c_2, \dots)$

olarak tanımlanır. $k > m+n$ için $a_k + b_k = 0_R$ olacağından $f+g = (a_0+b_0, a_1+b_1, \dots, a_{m+n}+b_{m+n}, 0_R, \dots) \in P(R)$ dir. Ayrıca çarpma işleminin tanımından görüldüğü gibi $k > m+n$ için $c_k = 0_R$ olacağından $f.g = (c_0, c_1, \dots, c_{m+n}, 0_R, \dots) \in P(R)$ dir.

**Teorem 1.3.17.** R birimli bir halka olmak üzere P(R) polinom kümesi yukarıda tanımlanan toplama ve çıkarmaya göre birimli bir halkadır.

$P(R)$ halkasına *R üzerinde bir belirsizin polinom halkası* denir. $x = (0_R, 1_R, 0_R, 0_R, \dots)$ olmak üzere $P(R)$ polinom halkası alışılmış biçimde $R[x]$ ile gösterilecektir. R'den katsayılı polinomlar kümesi $R[x]$ ile gösterilir. $R[x]$ in elemanları, belirsizi de belirtmek amacıyla $f(x), g(x), h(x)$ gibi sembollerle gösterilecektir. Eğer $f \neq 0_{P(R)}$ ise $a_i \neq 0_R$ olan $i$'lerin en büyüğüne *f'nin derecesi* denir.

$f(x) = \sum_{i=0}^{m} a_i x^i$ ve $g(x) = \sum_{j=0}^{n} b_j x^j$ polinomları verilsin. $m \leq n$ alınsın.

$f(x) = (a_0, a_1, a_2, \dots, a_m, 0_R, \dots), \qquad g(x) = (b_0, b_1, b_2, \dots, b_n, 0_R, \dots)$

olduğundan $a_{m+1} = a_{m+2} = a_{m+3} = \cdots = a_n = 0_R$ olarak tanımlanırsa

$f(x) = (a_0, a_1, a_2, \dots, a_n, 0_R, \dots)$ olur. Böylece

$f(x) + g(x) = (a_0+b_0, a_1+b_1, \dots, a_n+b_n, 0_R, \dots)$ olduğundan

$f(x) + g(x) = \sum_{j=0}^{n} (a_i + b_j) x^j$ olur.

Diğer taraftan her $k \geq 0$ için $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ olmak üzere $f(x)$ ile $g(x)$'in çarpımı $f(x)g(x) = (c_0, c_1, c_2, \dots)$ dır. $k > m+n$ için $c_k = 0_R$ olduğundan $f(x)g(x) = (c_0, c_1, \dots, c_{m+n}, 0_R, \dots)$ dir. Böylece

$$f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k, \qquad c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

elde edilir.

$f(x) = \sum_{i=0}^{m} a_i x^i$ polinomunda $a_m \neq 0_R$ olsun. $a_m$ ye *başkatsayı* denir. Eğer $a_m = 1_R$ ise $f(x)$ e *monik polinom* denir.

S birimli bir halka olmak üzere R, S'nin birimli bir alt halkası ve $u \in S$ olsun. $R[x]$ in her $f(x) = a_0x^0 + a_1x + a_2x^2 + \cdots + a_mx^m$ elemanında $x$ yerine $u$ konulursa $f(u) = a_0u^0 + a_1u + a_2u^2 + \cdots + a_mu^m$ elde edilir. S halka olduğundan $f(u) \in S$ dir. Böylece $R[x]$ den S'ye $\phi_u : f(x) \mapsto f(u)$ eşleşmesiyle bir $\phi_u$ fonksiyonu tanımlanır. $\phi_u$ ya bir *değer fonksiyonu* denir.

**Teorem 1.3.18.** S birimli ve değişmeli bir halka ve R, S'nin birimli bir alt halkası olmak üzere her $u \in S$ için $\phi_u$ değer fonksiyonu bir halka homomorfizmasıdır.

$\phi_u\big(f(x)g(x)\big) = \phi_u\big(f(x)\big)\phi_u\big(g(x)\big) = f(u)g(u)$ olur. Böylelikle $\phi_u$ homomorfizmasına bir *değer homomorfizması* denir.

**Tanım 1.3.19.** D bir tamlık bölgesi ve $a, b \in D$ olmak üzere $b = ac$ olacak biçimde $c \in D$ varsa $a, b$'yi *böler* ya da $a,\ b$' nin bir *çarpanıdır* denir ve $a|b$ şeklinde gösterilir.

**Lemma 1.3.20.** D bir tamlık bölgesi $f(x), g(x) \in D[x]$ olmak üzere aşağıdakiler sağlanır.

(i) $der\big(f(x) + g(x)\big) \leq maks\{der\big(f(x),\ g(x)\big)\}$

(ii) $der\big(f(x)g(x)\big) = der\big(f(x)\big) + der\big(g(x)\big)$

**Teorem 1.3.21.** D bir tamlık bölgesi ve $f(x), g(x) \in D[x]$ olsun. Ayrıca $g(x) \neq 0_D$ ve $g(x)$ in baş katsayısı tersinir olsun. O zaman $f(x) = q(x)g(x) + r(x)$ ve $der(r(x)) < der(g(x))$ olacak biçimde $q(x),\ r(x) \in D[x]$ vardır. Ayrıca $q(x)$ ile $r(x)$ tektir.

**Tanım 1.3.22.** $p(x) \in F[x]$ olsun. $p(x)$ sabit olmayan bir polinom olsun. Eğer $p(x)$, $F[x]$ içinde, her birinin derecesi $p(x)$ inkinden daha küçük olan iki polinomun çarpımı olarak yazılamazsa o zaman $p(x)$ e $F[x]$ içinde (F üzerinde) bir *indirgenmez polinom* denir.

Böylece $p(x)$ in indirgenmez olması için gerek ve yeter şart $der(p(x)) \geq 1$ ve $p(x) = r(x)s(x)$ ise $r(x)$ ya da $s(x)$ polinomunun sabit polinom olmasıdır.

**Tanım 1.3.23.** $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ ve $f(x) \neq 0$ olmak üzere $a_0, a_1, \ldots, a_n$ katsayılarının en büyük ortak bölenine $f(x)$ in *içeriği* denir ve $C(f(x))$ ile gösterilir. Eğer $C\big(f(x)\big) = 1$ ise $f(x)$ e bir *ilkel polinom* denir.

**Teorem 1.3.24.** $p$ bir asal sayı ve

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ bir polinom olsun. Eğer

(i) $p|a_0, p|a_1, \ldots, p|a_{n-1}$ fakat $p \nmid a_n$ ve

(ii) $p^2 \nmid a_0$ ise,

$f(x)$, $\mathbb{Q}[x]$ içinde indirgenmezdir. Buna *Einstein İndirgenmezlik Kriteri* denir.

**Teorem 1.3.25.** $F[x]$ in bir I idealinin maksimal olması için gerek ve yeter şart bir indirgenmez polinom tarafından üretilmesidir.

**Lemma 1.3.26.** $p(x)$, $F[x]$ in bir indirgenmez polinomu olsun. Eğer $s(x)$, $t(x) \in F[x]$ olmak üzere $p(x)|s(x)t(x)$ ise $p(x)$, $s(x)$ veya $t(x)$ ten birini böler.

**Teorem 1.3.27.** *(F[x] içinde Tek Türlü Çarpanlara Ayırma)* F bir cisim ve p(x) ∈ F[x] sabit olmayan bir polinom ise

$p(x) = p_1(x) \ldots p_r(x)$

olacak biçimde $p_1(x) \ldots p_r(x)$ indirgemez polinomları vardır. Bu gösterim indirgenmez çarpanların yer değiştirmesi ya da birimsellerle farkıyla tektir.

**Teorem 1.3.28.** D bir TİB ve $a_1, a_2, \ldots, a_n$ D'nin en az biri sıfırdan farklı olan n elemanı olsun. Aşağıdakiler sağlanır.

(i) $a_1, a_2, \ldots, a_n$ nin bir ebobu vardır.

(ii) Eğer $a_1, a_2, \ldots, a_n$ nin bir ebobu $d'$ ise $d' = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ olacak biçimde $x_1, x_2, \ldots, x_n \in D$ vardır.

**Tanım 1.3.29.** D bir tamlık bölgesi olmak üzere eğer;

(i) D'nin sıfır ve birimsel olmayan her elemanı sonlu sayıda indirgenemezin çarpımı ise ve

(ii) $c_1, c_2, \dots, c_m,\ d_1, d_2, \dots, d_n$ D'nin indirgenmez elemanları olmak üzere $c_1 c_2 \dots c_m = d_1 d_2 \dots d_n$ iken $m = n$ ve $d_1, d_2, \dots, d_m$ nin uygun bir indekslenmesinden sonra her $1 \leq i \leq m$ için $c_i$ ile $d_i$ bağdaşık ise,

D'ye bir *tek türlü çarpanlara ayırma bölgesi* (TÇAB) denir.

### 1.4. Cisim Genişlemeleri

**Tanım 1.4.1.** E bir cisim, $F \subset E$ olmak üzere E kendi başına F cismindeki işlemlere göre bir cisim ise F'ye E'nin *alt cismi* denir ve $F \leq E$ ile gösterilir.

**Teorem 1.4.2.** E bir cisim, $F \subseteq E$ olsun. F'nin E'nin alt cismi olması için gerek ve yeter şart F'nin en az iki elemanını içermesi ve her $a, b \in F$ için

(i) $a + b, -a,\ ab \in F$

(ii) $b \neq 0_R$ iken $b^{-1} \in F$

olmasıdır.

**İspat.** Eğer F, E'nin bir alt cismi ise verilen şartların sağlandığı açıktır. Karşıt olarak verilen şartlar sağlansın. Hipotezden $F \neq \emptyset$ dir. $a, b \in F$ olsun. O zaman (i)'den dolayı $a + b, -a, ab \in F$ olduğundan F, E'nin alt halkasıdır. Ayrıca F'nin en az iki elemanı olduğundan $0_R \neq b \in E$ vardır. O zaman (ii)'den dolayı $b^{-1} \in F$ ve $1_R = bb^{-1} \in F$ olduğundan $1_R \in F$ dir. Böylece F, E'nin birimli bir alt halkası ve sıfırdan farklı her elemanın tersi olduğundan E'nin alt cismidir.

**Sonuç 1.4.3.** F, E'nin bir alt cismi ise $0_{\mathrm{E}}$ ve $1_{\mathrm{E}} \in$ F dir.

**Teorem 1.4.4.** E bir cisim ve $\{F_i : i \in I\}$, E'nin alt cisimlerinin boş olmayan bir kümesi olsun. O zaman

$$D = \bigcap_{i \in \mathrm{I}} F_i$$

E'nin bir alt cismidir.

**İspat.** Her $i \in I$ için $F_i$, E'nin alt cismi olduğundan $0_E,\ 1_E \in F_i$ ve buradan $0_E,\ 1_E \in D$'dir. Dolayısıyla D'nin en az iki elemanı vardır. Ayrıca her $i \in I$ için $F_i$ alt halka

olduğundan D, E'nin alt halkasıdır. $0_R \neq b \in D$ olsun. Her $i \in I$ için $b \in F_i$ ve $F_i$ cisim olduğundan $b^{-1} \in F_i$ ve buradan $b^{-1} \in D$ dir. Dolayısıyla D, E'nin bir alt cismidir.

**Tanım 1.4.5.** Kendinden başka hiçbir alt cismi bulunmayan (öz alt cismi yoksa) cisme *asal cisim* denir.

**Örnek 1.4.1.** $\mathbb{Q}$ ve $\mathbb{Z}_p$ (p asal) cisimleri asal cisimdir.

**Tanım 1.4.6.** E bir cisim ve F, E'nin alt cismi olmak üzere E'ye F'nin *cisim genişlemesi* denir ve $F \leq E$ ile gösterilebilir (Şekil 1).


**Şekil 1.** E, F'nin cisim genişlemesi

**Tanım 1.4.7.** E bir cisim ve $\forall\, 0 \leq i < 1$ için $\mathrm{E}_1, \mathrm{E}_2, \ldots, \mathrm{E}_s$, E'nin alt cisimleri olsun. $E_i \leq E_{i+1}$ olmak üzere $E_1 \leq E_2 \leq \cdots \leq E_s$ yükselen zincirine bir *cisim kulesi* denir.

**Örnek 1.4.2.** $\mathbb{R}$, $\mathbb{Q}$'nun $\mathbb{C}$ hem $\mathbb{R}$'nin hem $\mathbb{Q}$'nun birer cisim genişlemesidir ve $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ cisim kulesi elde edilir (Şekil 2).


**Şekil 2.** $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ cisim kulesi

**Örnek 1.4.2.** F bir cisim ve $F[x]$, F üzerinde bir x belirsizinin polinom halkası olmak üzere $F[x]$ in kesirler cismi $F(x)$ ile gösterilir ve şu şekildedir:

$$F(x) = \left\{\frac{f(x)}{g(x)} : f(x), g(x) \in F[x] \; ve \; g(x) \neq 0\right\}.$$

Sabit polinomlar F'nin elemanlarıyla gösterilirse $F \leq F(x)$ dır. F(x) e F üzerindeki *rasyonel fonksiyonlar cismi* denir.

**Lemma 1.4.8.** F bir cisim ve $F \leq E$ olmak üzere E, F üzerinde bir vektör uzayıdır.

**İspat.** E cisim olduğundan $(E, +)$ bir toplamsal abelyan gruptur. E üzerinde F'ye göre skaler çarpım $v \in E$ ve $c \in F$ için $c.v$, E içindeki çarpım şeklinde tanımlansın. E cisim olduğundan $\forall v, w \in E$ ve $c, d \in F$ için aşağıdakiler sağlanır.

i. $c.(v + w) = c.v + c.w$
ii. $(c + d).v = c.v + d.v$
iii. $(cd).v = c.(d.v)$
iv. $1.v = v$

Vektör uzayı tanımı gereğince E, F üzerinde bir vektör uzayıdır.

**Tanım 1.4.9.** F bir cisim ve E, F'nin bir cisim genişlemesi olsun. Bu durumda E, F üzerinde n boyutlu ise o zaman E'ye F üzerinde *n dereceye* sahiptir denir ve $[E : F] = n$ ile gösterilir.

$[E : F]$ sonlu ise *sonlu cisim genişlemesi*, $[E : F]$ sonsuz ise bir *sonsuz cisim genişlemesi* denir.

**Örnek 1.4.4.** $\mathbb{C}$, $\mathbb{R}$'nin bir sonlu cisim genişlemesidir. $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$ ve $\{1, i\}$, $\mathbb{C}$ üzerinde vektör uzayı ve lineer bağımsız olduğundan $[\mathbb{C} : \mathbb{R}] = 2$ dir. $p$ bir asal sayı olmak üzere $\{\sqrt{2}, \sqrt{3}, \ldots, \sqrt{p}\}$ kümesi $\mathbb{Q}$ üzerinde lineer bağımsız olduğundan $\mathbb{R}$, $\mathbb{Q}$'nun sonsuz cisim genişlemesidir.

**Tanım 1.4.10.** F bir cisim ve E, F'nin bir cisim genişlemesi olsun. $u \in E$ olsun. Eğer $F[x]$ in sıfırdan farklı bir $f(x)$ polinomu için $f(u) = 0_F$ ise $u$'ya F üzerinde bir

*cebirsel eleman* denir. Eğer her $0_F \neq f(x) \in F[x]$ için f(u) $\neq 0_F$ ise $u$'ya F üzerinde bir *transandantal eleman* denir.

**Tanım 1.4.11.** $\mathbb{Q}$ üzerinde cebirsel olan bir kompleks sayıya *cebirsel sayı* ve transandantal olan bir kompleks sayıya da *transandantal sayı* denir.

**Örnek 1.4.5.** F bir cisim ve E, F nin bir cisim genişlemesi olmak üzere $u \in E, F$ üzerinde transandant ve $0_F \neq c \in F$ ise $cu$ ve $u^2$ nin F üzerinde transandant olduğu şu şekilde gösterilir:

$u \in E,\ f(u) \neq 0_F,\ \ 0 \leq i \leq n$ ve $c_i \neq 0_F,\ c_i \in F$ olmak üzere $f(u) = c_0 + c_1u + c_2u^2 + \cdots + c_nu^n \neq 0_F$ vardır.

$0_F \neq c \in F$ ise $f(cu) = c_0 + c_1(cu) + c_2(cu)^2 + \cdots + c_n(cu)^n = c_0 + c_1cu + c_2c^2u^2 + \cdots + c_nc^nu^n$ elde edilir. $c_0 = a_0,\ c_1c = a_1,\ c_2c^2 = a_2, \ldots, c_nc^n = a_n$ olarak alınırsa $c,\ c_i \in F$ olduğundan $0_F \neq a_i = c.c_i \in F$ olduğu açıktır.
O halde $f(cu) = a_0 + a_1u + a_2u^2 + \cdots + a_nu^n$ yazılır. $f(u) \neq 0_F$ olduğundan $f(cu) \neq 0_F$ dir. Yani $cu$ transandantır.
$u^2$ için $f(u^2) = c_0 + c_1u^2 + c_2(u^2)^2 + \cdots + c_n(u^2)^n = c_0 + (c_1u)u + (c_2u^2)u^2 + \cdots + (c_nu^n)u^n$ elde edilir. $0_F \neq c_iu^i \in F$ ve $f(u) \neq 0_F$ olduğundan $f(u^2) \neq 0_F$ dir. Yani $u^2$ transandanttır.

**Örnek 1.4.6.** $x^2 - 3$, $x^2 - 5$ ve $x^2 + 1$ polinomlarının kökleri sırasıyla $\sqrt{3}$, $\sqrt{5}$, $i$ sayıları cebirsel sayılardır. $\pi$ ve $e$ sayıları transandantaldır.

**Örnek 1.4.7.** $\sqrt{2} + \sqrt{5}$ bir cebirsel sayıdır. $u = \sqrt{2} + \sqrt{5}$ olsun. O zaman $u^2 = 2 + 2\sqrt{10} + 5 = 7 + 2\sqrt{10}$ olduğundan $(u^2 - 7)^2 = 40$ ve buradan $u^4 - 14u^2 + 9 = 0$ bulunur. O halde $u$ sayısı $f(x) = x^4 - 14x^2 + 9$ polinomunun köküdür.

R bir halka ve $X \subset R$ olmak üzere R halkasının X kümesini içeren alt halkalarının kesişimi de R'nin bir alt halkasıdır ve bu halkaya R içinde X tarafından *üretilen alt halka* denir. F bir cisim ve $X \subseteq F$ olmak üzere F'nin X'i içeren alt cisimlerinin kesişimi F'nin bir alt cismidir ve bu cisme F içinde X tarafından *üretilen alt cisim* denir.

**Tanım 1.4.12.** F bir cisim E, F'nin bir cisim genişlemesi ve $S \subseteq E$ olmak üzere E içinde $F \cup S$ tarafından üretilen alt halkaya F'ye S'nin *katılmasıyla elde edilen alt halka (S*

*tarafından üretilen alt halka)* denir. $F[S]$ ile gösterilir. $F \cup S$ tarafından üretilen alt cisme F'ye S'nin *katılmasıyla elde edilen alt cisim (S tarafından üretilen alt cisim)* denir. $F(S)$ ile gösterilir. $S = \{s_1, s_2, \dots, s_n\}$ $n$ elemanlı bir sonlu küme ise $F[\{s_1, s_2, \dots, s_n\}] = F[s_1, s_2, \dots, s_n]$ ve $F(\{s_1, s_2, \dots, s_n\}) = F(s_1, s_2, \dots, s_n)$ şeklinde gösterilir. $n = 1$ ve $s_1 = s$ ise $F[s]$ ve $F(s)$ ye sırasıyla F'ye s'nin *katılmasıyla elde edilen alt halka* ve *alt cisim* denir. Ayrıca F(s) ye F'nin bir *basit cisim genişlemesi* denir.

**Örnek 1.4.8.** $\mathbb{R} \cup \{i\}$ yi içeren her alt halka $\mathbb{C}$'yi içerdiğinden, $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}(i)$ olduğu açıktır. Benzer şekilde F üzerindeki rasyonel fonksiyonlar cismi $F(x)$, F'ye x'in katılmasıyla elde edilen cisimdir. Aynı biçimde $\mathbb{Q}$ cismini ve $\sqrt{2}$ elemanını içeren her alt halka $\mathbb{Q}(\sqrt{2})$ yi kapsar. O halde $\mathbb{Q}(\sqrt{2})$ cismi de bir basit cisim genişlemesidir.

**Örnek 1.4.9.** $a, b \in \mathbb{Q}^+$ olsun. Eğer $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ ise $b = t^2 a$ olacak biçimde $t \in \mathbb{Q}$ vardır ve şu şekildedir:

$\mathbb{Q}(\sqrt{a}) = \{c + d\sqrt{a} : c,\ d \in \mathbb{Q}\}$ ve $\mathbb{Q}(\sqrt{b}) = \{e + f\sqrt{b} : e,\ f \in \mathbb{Q}\}$

$\sigma: \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}(\sqrt{b})$,

$\sigma(\sqrt{a}) = e + f\sqrt{b}$ , $e, f \in \mathbb{Q}$ vardır.

$\sigma(1) = 1$ ve $\sigma(a) = \sigma(\sqrt{a}.\sqrt{a}) = \sigma(\sqrt{a}).\sigma(\sqrt{a}) = (e + f\sqrt{b})(e + f\sqrt{b}) = e^2 + 2ef\sqrt{b} + f^2 b = a$

$e = 0$ ise $f^2 b = a$ dır. O halde $b = \frac{1}{f^2} a = (\frac{1}{f})^2 a$ dir. $f, \frac{1}{f} = t \in \mathbb{Q}$ olmak üzere $b = t^2 a$ olur.

**Lemma 1.4.13.** F bir cisim E, F'nin bir cisim genişlemesi ve $S \subseteq E$ olmak üzere $F[S]$, E'nin bir alt bölgesi ve $F(S)$, $F[S]$ nin kesirler cismidir.

**İspat.** E bir cisim olduğundan $F[S]$, E'nin değişmeli ve sıfır bölensiz bir alt halkası ve $1_E \in F[S]$ olduğundan bir alt bölgesidir (birimli halkadır). $F[S]$ nin E içindeki kesirler cismi K olsun. O zaman $F \cup S \subseteq K$ olduğundan $F(S) \subseteq K$ dır. Diğer taraftan K, F[S] yi içeren en küçük alt cisim olduğundan $K \subseteq F(S)$ ve böylece $K = F(S)$ dir.

**Teorem 1.4.14.** F bir cisim ve E, F'nin bir cisim genişlemesi ve $u \in E$ olmak üzere $F[u] = \{ f(u): f(x) \in F[x]\}$ ve

$F(u) = \left\{f(u)\left(g(u)\right)^{-1}: f(x), g(x) \in F[x] \text{ ve } g(x) \neq 0_F\right\}$ dir.

**İspat.** $\phi_u$, $u$'ya karşılık gelen değer homomorfizması olmak üzere $\phi_u(F[x]) = \{f(u): f(x) \in F[x]\}$, $E$'nin alt halkasıdır. $S = \phi_u(F[x])$ olmak üzere $S = F[u]$ olduğu gösterilmelidir. $F \cup \{u\} \subseteq S$ ise $F[u] \subseteq S$ dir. $f(u) \in S$ olmak üzere $f(u) = c_0 + c_1u + \cdots + c_nu^n$ olacak şekilde $c_0, c_1, \ldots, c_n \in F$ vardır. Ancak $F[u]$ alt halka olduğundan $f(u) \in F[u]$ ve buradan $S \subseteq F[u]$ dur. O halde $F[u] = S$ dir. Lemma 1.4.13'den ve bir özel cismin kesirler cismi kendisine izomorf olduğundan dolayı

$$F(u) = \left\{f(u)\left(g(u)\right)^{-1}: f(u), g(u) \in F[u] ve\ g(u) \neq 0_F\right\}$$

$$= \left\{f(u)\left(g(u)\right)^{-1}: f(x), g(x) \in F[x] ve\ g(x) \neq 0_F\right\} \text{ dir.}$$

Teorem 1.4.14'den $F[u] = \phi_u(F[x])$, $u$'nun F üzerindeki polinomlarının "*çok terimlilerinin*" kümesidir.

Genel olarak $u_1, u_2 \ldots, u_n \in E$ olsun. Yukarıdaki ispata benzer şekilde gösterilebileceği gibi

$$F[u_1, u_2 \ldots, u_n] = \{f(u_1, u_2 \ldots, u_n): f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]\}$$

$$F(u_1, u_2 \ldots, u_n) =$$
$$\{f(u_1, u_2 \ldots, u_n)\left(g(u_1, u_2 \ldots, u_n)\right)^{-1}: f(x_1, x_2, \ldots, x_n), g(x_1, x_2, \ldots, x_n) \in$$
$F[x_1, x_2, \ldots, x_n]$ ve $g(x_1, x_2, \ldots, x_n) \neq 0_F\}$ dir.

**Teorem 1.4.15.** F bir cisim E, F'nin bir cisim genişlemesi ve $u \in E$ olmak üzere $u$'nun F üzerinde transandant olması için gerek ve yeter şart $F[x] \cong F[u]$ olmasıdır.

**İspat.** $\phi_u: F[x] \to E$ değer homomorfizması olmak üzere $u$'nun F üzerinde transandant olması için gerek ve yeter şart sıfırdan farklı her $f(x) \in F[x]$ için $f(u) \neq 0_E$ olmasıdır, bunun için gerek ve yeter şart $Ker(\phi_u) = \{0_F\}$ ve böylece $F[x] = \phi_u(F[x])$ olmasıdır. $F[u] = \phi_u(F[x])$ olduğundan u'nun F üzerinde transandant olması için gerek ve yeter şart $F[x] \cong F[u]$ olmasıdır.

**Teorem 1.4.16.** F bir cisim ve $p(x) \in F[x]$ bir indirgenemez polinom olmak üzere F'nin öyle bir cisim genişlemesi E vardır ki $p(x)$ in E içinde bir kökü vardır.

**İspat.** F[x] bir temel ideal bölgesi ve p(x) indirgenemez olduğundan $\langle p(x)\rangle$ maksimal idealdir. Böylece $F[x]/\langle p(x)\rangle$ bölüm halkası cisimdir. $E = F[x]/\langle p(x)\rangle$ olsun.

$\mu: F[x] \to F[x]/\langle p(x)\rangle, \qquad f(x) \mapsto f(x) + \langle p(x)\rangle$

biçiminde kanonik epimorfizma tanımlansın. $\mu_1 = \mu|_F$ olsun. $\mu_1(F) \neq \{0_E\}$ olduğundan $F \cong \mu_1(F)$ dir. $\mu_1(F) = \{a + \langle p(x)\rangle : a \in F\}$ olduğundan E içinde $a + \langle p(x)\rangle$ yerine $a$ yazılırsa F, E'nin bir alt cismi ve E, F'nin bir cisim genişlemesi olur. $F[x] \subseteq E[x]$ olduğundan $p(x) \in E[x]$ dir. $u = x + \langle p(x)\rangle$ ve $p(x) = c_0 + c_1x + \ldots + c_nx^n$ olmak üzere $u \in E$ olduğundan

$p(u) = c_0 + c_1u + \ldots + c_nu^n$

$= c_0 + c_1(x + \langle p(x)\rangle) + \ldots + c_n(x + \langle p(x)\rangle)^n$

$= c_0 + c_1(x + \langle p(x)\rangle) + \ldots + c_n(x^n + \langle p(x)\rangle)$

$= c_0 + c_1x + \ldots + c_nx^n + \langle p(x)\rangle$

$= p(x) + \langle p(x)\rangle$

$= 0_E$

ve böylece $p(u) = 0_E$ dir.

**Sonuç 1.4.17.** $f(x) \in F[x]$ sabit olmayan bir polinom olmak üzere F'nin içinde $f(x)$ in kökü olan bir cisim genişlemesi E vardır.

**İspat.** $f(x)$ sabit olmadığından $F[x]$ içinde $p(x)$ gibi bir indirgenmez çarpanı vardır. Teorem 1.4.16'dan bir $u \in E$ için $p(u) = 0_F$ dir. Bu durumda, açıkça görüldüğü gibi $f(u) = 0$'dır.

Teorem 1.4.16'da inşa edilen E cismi için $E = F[x]/\langle p(x)\rangle = \{f(x) + \langle p(x)\rangle : f(x) \in F[x]\}$ tir. $f(x) \in F[x]$ olsun. $f(x) + \langle p(x)\rangle$ te $u = x + \langle p(x)\rangle$ yerine yazılırsa $f(x) + \langle p(x)\rangle = f(u)$ elde edilir. Böylelikle $E = \{f(u): f(x) \in F[x]\}$ dir. Teorem 1.4.14'den $E = F[u]$ dur. $E = F(u)$, F'ye $u$'nun katılmasıyla elde edilen basit cisim genişlemesidir.

**Örnek 1.4.10.** $p(x) = x^3 + 2x + 3 \in \mathbb{Q}[x]$ olsun. $p(x)$, $\mathbb{Q}$ üzerinde indirgenemez olduğundan $E = \mathbb{Q}[x]/\langle p(x)\rangle$ bir cisimdir. $\mathbb{Q} \leq E$ olduğu kabul edilirse E, $\mathbb{Q}$'nun bir cisim genişlemesi ve $p(x) \in E[x]$ olur. Şimdi

$$p(\, x + \langle p(x)\rangle) = (\, x + \langle p(x)\rangle\,)^3 + 2(\, x + \langle p(x)\rangle) + 3 = x^3 + 2x + 3 + \langle p(x)\rangle$$
$$= p(x) + \langle p(x)\rangle = 0$$

olduğundan $p(\, x + \langle p(x)\rangle) = 0$ dır.

**Lemma 1.4.18.** F bir cisim E, F'nin bir cisim genişlemesi ve $u \in E$, $F$ üzerinde cebirsel olmak üzere öyle bir monik ve indirgenmez $p(x) \in F[x]$ vardır ki $p(u) = 0_F$ dır. p(x) tektir ve $g(u) = 0_F$ olan her $g(x) \in F[x]$ in bir bölenidir.

**İspat.** $\phi_u : F[x] \to E$ değer homomorfizması dikkate alınırsa $F[x]$ bir temel ideal bölgesi olduğundan $Ker(\phi_u) = \langle p(x)\rangle$ olacak şekilde bir $p(x) \in F[x]$ vardır. $u$, F üzerinde cebirsel olduğundan $f(u) = 0_F$ olacak şekilde sabit olmayan bir $f(x) \in F[x]$ vardır. $p(x) \in Ker(\phi_u)$ olduğundan $p(x)$ sabit değildir. Eğer $p(x)$ indirgenmez olmazsa dereceleri $p(x)$ in derecesinden daha küçük olan $s(x)$, $t(x) \in F[x]$ vardır ve $p(x) = s(x)t(x)$ tir. Eşitliğin iki tarafına da $\phi_u$ uygulanırsa $0_F = p(u) = s(u)t(u)$ elde edilir. E cisim olduğundan $s(u) = 0_F$ ya da $t(u) = 0_F$ olmalıdır. Eğer $s(u) = 0_F$ ise $s(x) \in \langle p(x)\rangle$ ve $p(x)|s(x)$ elde edilir. Fakat $s(x)|p(x)$ olduğundan $s(x) = ap(x)$ olacak biçimde $0_F \neq a \in F$ vardır. Yerine yazılırsa $at(x) = 1_F$ ve buradan $t(x) = a^{-1}$ bulunur. Dolayısıyla $t(x)$ birimseldir. Benzer şekilde $t(u) = 0_F$ ise $s(x)$ birimsel olur. Dolayısıyla $p(x)$ indirgenmezdir. Bazı durumlar için $p(x)$'i başkatsayısının tersiyle çarparak $p(x)$ in monik olduğu kabul edilebilir.

$q(x) \in F[x]$ monik ve $q(u) = 0_F$ olmak üzere $q(x) \in Ker(\phi_u)$ olduğundan yukarıdaki gibi, $q(x) = ap(x)$ olacak şekilde $0_F \neq a \in F$ vardır. Aynı zamanda $q(x)$ monik olduğundan $a = 1_E$ ve böylece $q(x) = p(x)$ bulunur.

Son olarak $q(x) \in F[x]$ ve $q(u) = 0_F$ olmak üzere $q(x) \in \langle p(x)\rangle$ olduğundan $p(x)|q(x)$ tir.

**Tanım 1.4.19.** F bir cisim E, F'nin bir cisim genişlemesi ve $u \in E, F$ üzerinde cebirsel olsun. Lemma 1.4.18'de tanımlı ve tek türlü belirli olan monik ve indirgenmez (derecesi kendisinden küçük olan iki polinomun çarpımı şeklinde yazılamıyorsa) $p(x)$

polinomuna $u$'nun F üzerindeki *indirgenmez polinomu*, $der\big(p(x)\big)$ e $p(x)$ polinomunun *derecesi* denir ve $p(x) = \text{İ}nd(u,F)$ ve $der\big(p(x)\big) = der(u,F)$ ile gösterilir.

**Örnek 1.4.11.** $\sqrt{5}$, $\sqrt{7}$, $\sqrt[3]{4}$, $i$ sayılarının $\mathbb{Q}$ üzerindeki indirgenmez polinomları sırasıyla $x^2-5$, $x^2-7$, $x^3-4$ ve $x^2+1$ dir.

**Örnek 1.4.12.** $1+\sqrt{5}$ elemanının $\mathbb{Q}$ cismi üzerindeki indirgenmez polinomu aşağıdaki gibidir.

$1+\sqrt{5}=u$ olsun. $\sqrt{5}=u-1$ ve $5=u^2-2u+1$ bulunur. Buradan $u^2-2u-4=0$ yani $f(x)=x^2-2x-4$ elde edilir. $1+\sqrt{5}$ sayısı $f(x)=x^2-2x-4$ in bir köküdür. $f(1)=-5$, $f(-1)=-1$, $f(2)=-4$ ve $f(-2)=4\neq 0$ olduğundan $f(x)$ in rasyonel kökü yoktur. $f(x)$ in birinci dereceden çarpanları bulunsun. O zaman

$$x^2-2x-4=(x+a)(x+b)$$

olacak biçimde $a$, $b$ tam sayıları vardır. Buradan $a+b=-2$, $ab=-4$ eşitlikleri elde edilir. Buradan $a=-b-2$ yerine konulursa $(-b-2)b=-4$ ve buradan $b^2+2b-4=0$ elde edilir. b tam sayı olduğundan çelişki elde edilir. $ind(u,\mathbb{Q})=x^2-2x-4$ indirgenmez polinomudur.

**Örnek 1.4.13.** $3+5i$ elemanın $\mathbb{Q}$ cisim üzerinde cebirseldir ve indirgenmez polinomu aşağıdaki gibidir.

$3+5i=u$ olsun. $u-3=5i$ ve $u^2-6u+9=-25$ olduğundan $u^2-6u+34=0$ bulunur. Dolayısıyla u sayısı $f(x)=x^2-6x+34$ polinomunun bir köküdür.

**Teorem 1.4.20.** F bir cisim E, F'nin bir cisim genişlemesi ve $u\in E$, $F$ üzerinde cebirsel, $\text{İ}nd(u,F)=p(x)$ ve $der\big(p(x)\big)=n$ olmak üzere aşağıdakiler sağlanır.

(i) $F(u)=F[u]$ ve $F(u)\cong F[x]/\langle p(x)\rangle$

(ii) $\{1,u,\dots,u^{n-1}\}$, $F(u)$ nun bir F-bazıdır.

(iii) $[F(u):F]=n$

**İspat.** (i) $\phi_u: F[x]\to E$ değer homomorfizması olmak üzere $F[x]/Ker(\phi_u)\cong \phi_u(F[x])$ tir. Teorem 1.4.14'den $\phi_u(F[x])=F[u]$ ve Lemma 1.4.18'den $Ker(\phi_u)=\langle p(x)\rangle$ olduğundan bu değerler yerine yazılırsa $F[u]\cong F[x]/\langle p(x)\rangle$ elde edilir. Diğer

taraftan Teorem 1.4.16'nın ispatında olduğu gibi $F[x]/\langle p(x)\rangle$ cisim olduğundan $F[u]$ bir cisimdir. Aynı zamanda $F(u)$, $F[u]$ yu içeren en küçük cisim olduğundan $F[u] = F(u)$ bulunur.

(ii) $f(u) \in F[u]$ ve $f(x) = q(x)p(x) + r(x)$ ve $der(r(x)) < n$ olacak şekilde $q(x)$, $r(x) \in F[x]$ vardır. Eşitliğin iki tarafına $\phi_u$ uygulanırsa $f(u) = q(u)p(u) + r(u) = q(u)0_F + r(u) = r(u)$ bulunur. O halde $\{1, u, \dots, u^{n-1}\}$ kümesi $F[u]$ yu F-uzayı olarak gerer. $c_0, c_1, \dots, c_{n-1} \in F$ olmak üzere $c_0 + c_1u + \dots + c_{n-1}u^{n-1} = 0_F$ olsun. $s(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ olarak tanımlansın. $s(u) = 0_F$ olduğundan Lemma 1.4.12'den dolayı $p(x)|s(x)$ dır. Fakat $der\big(s(x)\big) \leq n-1$ olduğundan $s(u) = 0_F$ dir. Buradan $c_0 = c_1 = \dots = c_{n-1} = 0_F$ elde edilir. Dolayısıyla $1, u, \dots, u^{n-1}$ elemanları F üzerinde lineer bağımsızdır ve böylece $\{1, u, \dots, u^{n-1}\}$, $F(u)$ nun bir F-bazıdır.

(iii) Tanım 1.4.9 ve (ii)'nin sonucudur.

**Sonuç 1.4.21.** F bir cisim ve E, F'nin bir cisim genişlemesi olsun. $u_1, u_2, \dots, u_k \in E$, $F$ üzerinde cebirsel olmak üzere $E = F(u_1, u_2, \dots, u_k)$ olsun. O halde E'nin elemanları $m_1, m_2, \dots, m_k$ doğal sayılar ve $c_{m_1,m_2,\dots,m_k}u_1^{m_1} \dots u_k^{m_k}$ tipindeki elemanların sonlu toplamlarından oluşur.

**İspat.** $F_0 = F$ ve her $0 \leq i < k$ için $F_{i+1} = F_i(u_{i+1})$ olmak üzere $F = F_0 \leq F_1 \leq \dots \leq F_k = E$ cisim kulesi elde edilir. $0 \leq i \leq k$ olmak üzere $i$ üzerine tümevarım uygulanır. $i = 0$ için $F_1 = F(u_1)$ olduğundan Teorem 1.4.20'den $F_1 = F[u_1]$ dir. Kabul edilsin ki $0 \leq i < k$ için iddia sağlansın ve $F_{i+1}$ için sağlandığı gösterilsin. $u_{i+1}$, F üzerinde cebirsel olduğundan $F_i$ üzerinde cebirseldir ve $y \in F_{i+1}$ olsun. Teorem 1.4.20(i)'den $F_{i+1} = F_i[u_{i+1}]$ olduğundan $b_0, b_1, \dots, b_t \in F_i$ olmak üzere $y = b_0 + b_1u_{i+1} + \dots + b_tu_{i+1}^t$'dir. Tümevarımdan her $b_j, d_{s_1,\dots,s_i} \in F$ olmak üzere $d_{s_1,\dots,s_i}u_1^{s_1}u_2^{s_2} \dots u_i^{s_i}$ tipindeki monomlarının bir sonlu toplamı olduğundan, yerine yazılırsa y elemanı $u_1^{m_1}u_2^{m_2} \dots u_{i+1}^{s_{m_{i+1}}}$ monomlarının bir F lineer kombinasyonu olur. Böylece tümevarım ve ispat tamamlanır.

**Örnek 1.4.14.** $p(x) = x^2 + 1$ polinomu $\mathbb{R}$'de indirgenmezdir ve $\langle p(x)\rangle$ $\mathbb{R}[x]$ de maksimal idealdir. O halde ve $E = \mathbb{R}[x]/\langle p(x)\rangle$ bir cisimdir ve $\mathbb{R} \leq E$ olsun. Teorem

1.4.16'nın ispatında görüldüğü gibi $u = x + \langle p(x)\rangle$ yazılırsa $\text{İ}nd(u, E) = x^2 + 1$ olduğundan Teorem 1.4.20(i)'den dolayı $\mathbb{R}(u) \cong \mathbb{R}[x]/\langle x^2 + 1\rangle$ ve $\mathbb{R}(u) = \{a + bu : a,\ b\ \in \mathbb{R}\}$ dir. $a + bu, c + du \in \mathbb{R}(u)$ olsun. $u^2 = -1$ olduğundan

$$(a + bu) + (c + du) = (a + c) + (b + d)u$$

$$(a + bu)(c + du) = (ac - bd) + (ad + bc)u$$

dur. Açıkça görüldüğü gibi $\mathbb{R}$(u) daki toplama ve çarpma $\mathbb{C}$'dekinin aynısıdır. $u, \mathbb{C}$ içindeki $i$'nin özelliğine sahiptir. $a + bu \mapsto a + bi$ eşleşmesi vardır ve $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$ dir.

**Örnek 1.4.15.** $\mathbb{Z}_2$ cismi üzerinde $f(x) = x^2 + x + 2$ polinomu verilsin. Buna göre $\mathbb{Z}_2[x]/\langle f(x)\rangle$ halkasının bir cisminin toplam ve çarpım tabloları aşağıdaki gibidir:

$f(x) = x^2 + x + 2 = \left(x + \frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\left(x + \frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$ olduğundan $f(x)$ polinomu $\mathbb{Z}_2$ üzerinde indirgenmezdir. Bu nedenle $\mathbb{Z}_2[x]/\langle x^2 + x + 2\rangle$ halkası bir cisimdir. Bu cismin elemanları $\mathbb{Z}_2[x]\ /\langle x^2 + x + 2\rangle = \{0, 1, \propto, \propto +1\}$ dir. Burada $P = \langle x^2 + x + 2\rangle$ olup $\propto = x + P \in \mathbb{Z}_2[x]\ /\langle x^2 + x + 2\rangle$ dir. Buna göre $0 = 0 + P$ ve $1 = 1 + P$ olmak üzere $\mathbb{Z}_2[x]/\ \langle f(x)\rangle = \{0, 1, \propto, \propto +1\}$ dir.

Bu cisim için toplama ve çarpma tabloları sırası ile aşağıdaki gibidir:

**Tablo 1.** Cisme göre elemanlarının toplama tablosu

| + | 0 | 1 | $\propto$ | $\propto +1$ |
|---|---|---|---|---|
| 0 | 0 | 1 | $\propto$ | $\propto +1$ |
| 1 | 1 | 0 | $\propto +1$ | $\propto$ |
| $\propto$ | $\propto$ | $\propto +1$ | 0 | 1 |
| $\propto +1$ | $\propto +1$ | $\propto$ | 1 | 0 |

**Tablo 2.** Cisme göre elemanlarının çarpma tablosu

| · | 0 | 1 | $\propto$ | $\propto +1$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | $\propto$ | $\propto +1$ |
| $\propto$ | 0 | $\propto$ | $\propto +1$ | 1 |
| $\propto +1$ | 0 | $\propto +1$ | 1 | $\propto$ |

**Örnek 1.4.16.** $\mathbb{Q}(\sqrt{2})$ cismi $İnd\left(\sqrt{2},\mathbb{Q}\right)=x^2-2$ olduğundan $\mathbb{Q}(\sqrt{2})$ in bir $\mathbb{Q}$-bazı $\left\{1,\sqrt{2}\right\}$ den oluşur. O halde $\mathbb{Q}\left(\sqrt{2}\right)=\{a+b\sqrt{2}:a,b\in\mathbb{Q}\}$ ve $[F:\mathbb{Q}]=2$ dir. Toplama ve çarpma işlemleri de

$$\left(a+b\sqrt{2}\right)+\left(c+d\sqrt{2}\right)=(a+c)+(b+d)\sqrt{2}$$

$$\left(a+b\sqrt{2}\right).\left(c+d\sqrt{2}\right)=(ac+2bd)+(ad+bc)\sqrt{2}$$

şeklindedir.

$\sqrt{5}\notin\mathbb{Q}(\sqrt{2})$ olduğu şu şekilde gösterilir: $f(x)=x^2-5$ fonksiyonunun bir kökü $\sqrt{5}$ tir. $\sqrt{5}\in\mathbb{Q}(\sqrt{2})$ ise $\sqrt{5}=a+b\sqrt{2}$ yerine yazılırsa $(a+b\sqrt{2})^2-5=0$, $a^2+2ab\sqrt{2}+2b^2-5=0$ elde edilir. $a=0$ ise $2b^2=5$ yani $b=\sqrt{5/2}\notin\mathbb{Q}$ çelişkisi elde edilir. $b=0$ ise $a=\sqrt{5}\notin\mathbb{Q}$ çelişkisi elde edilir. O halde $\sqrt{5}\notin\mathbb{Q}\left(\sqrt{2}\right)$ dir.

**Örnek 1.4.17.** $\mathbb{Q}\left(\sqrt[3]{2},\ \mathbb{Q}\right)$ cismi için $İnd\left(\mathbb{Q}\left(\sqrt[3]{2}\right),\ \mathbb{Q}\right)=x^3-2$ olduğundan $\mathbb{Q}\left(\sqrt[3]{2}\right)$ nin bir $\mathbb{Q}$-bazı $\left\{1,\ \sqrt[3]{2},\ \sqrt[3]{4}\right\}$ ten oluşur. O halde $\mathbb{Q}\left(\sqrt[3]{2}\right)=\{a+b\sqrt[3]{2}+c\sqrt[3]{4}:a,\ b,\ c\in\mathbb{Q}\}$ dur. $w=\frac{1}{2}(-1+i\sqrt{3})$ olmak üzere $x^3-2=0$ denkleminin bütün kökleri $\sqrt[3]{2},\ \sqrt[3]{2}w,\ \sqrt[3]{2}w^2$ dir. Teorem 1.4.20(i)'den dolayı $\mathbb{Q}\left(\sqrt[3]{2}\right)\cong\mathbb{Q}\left(\sqrt[3]{2}w\right)\cong\mathbb{Q}\left(\sqrt[3]{2}w^2\right)$ dur.

## 1.5. Cebirsel Genişlemeleri

**Tanım 1.5.1.** $F\leq E$ olmak üzere eğer E'deki her eleman F üzerinde cebirsel ise o zaman E'ye F'nin bir *cebirsel genişlemesi* denir.

**Not 1.5.2.** E, F cisminin bir sonlu genişlemesi ise bu durumda $[\,E:F\,]=1\Leftrightarrow E=F\ (1)=F$ olmasıdır.

**Teorem 1.5.3.** E, F cisminin sonlu bir cisim genişlemesi ise o zaman E, F'nin bir cebirsel genişlemesidir.

**İspat.** E, F cismi üzerinde derecesi $n$ (sonlu) olan bir cisim genişlemesi ve $\alpha\in E$ olmak üzere $K=\{1,\alpha,\alpha^2,\ldots,\alpha^n\}$ kümesi dikkate alınırsa K kümesi $n+1$ tane elemana sahip olduğundan K kümesi lineer bağımlı olup

$c_0 1 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0$

olacak biçimde en az birisi sıfırdan farklı olan $c_0, c_1, \ldots, c_n \in F$ vardır. O halde buradan $\alpha \in E$ elemanının

$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n \in F[x]$

Sıfırdan farklı polinomunun kökü olduğu sonucu elde edilir. Bu da $\alpha \in E$'nin F üzerinde cebirsel olmasını gerektirir.

**Not 1.5.4.** Teorem 1.5.3'ün karşıtı her zaman doğru değildir. Örneğin $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$ cismi $\mathbb{Q}$'nun bir cebirsel genişlemesi olmasına rağmen $\mathbb{Q}$'nun bir sonlu genişlemesi değildir.

**Sonuç 1.5.5.** E, F cisminin bir cisim genişlemesi ve $\alpha \in E$ olmak üzere $\alpha$, F üzerinde cebirsel ise $F(\alpha)$ nın her elemanı F üzerinde cebirseldir. Başka bir ifadeyle $F(\alpha)$, F'nin bir cebirsel genişlemesidir.

**İspat.** Pozitif bir n tam sayısı için Tanım 1.4.9'dan $[F(\alpha) : F] = n$ yazılabilir. Böylece istenilen sonuç Teorem 1.5.3'den elde edilir.

**Örnek 1.5.1.** Sonuç 1.5.5'den $\mathbb{Q}(\sqrt{3})$ ün her elemanı $\mathbb{Q}$ üzerinde cebirseldir. Eğer $a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ ise $a + b\sqrt{3}$ ,

$$f(x) = \left(x - a + b\sqrt{3}\right)\left(x - a - b\sqrt{3}\right) = (x-a)^2 - 3b^2 = x^2 - 2ax + (a^2 - 3b^2)$$

polinomunun bir köküdür ve f(x), $\mathbb{Q}$[x] de bir polinomdur.

**Teorem 1.5.6.** E, F'nin ve K'da E'nin bir sonlu cisim genişlemesi ise K, F'nin bir sonlu cisim genişlemesidir ve [ K : F] = [K : E][E : F] dir.

**İspat.** $A = \{x_1,\ x_2, \ldots, x_n\}$ E cismi üzerinde K için bir baz ve $B = \{y_1,\ y_2, \ldots, y_n\}$ F üzerinde E için bir baz olmak üzere $BA = \{y_j x_i : 1 \le j \le m\ , 1 \le i \le n\}$ kümesinin F üzerinde K için bir baz olduğu gösterilirse ispat tamamlanır. Yani BA kümesinin F üzerinde K'yı gerdiği ve lineer bağımsız olduğu gösterilmelidir. Buna göre eğer $\alpha \in K$ ise $a = b_1 x_1 + b_2 x_2 + \cdots + b_n x_n$ olacak biçimde E cismine ait $b_1,\ b_2, \ldots, b_n$ elemanları vardır ve bu yazılış tek türlüdür. Öte taraftan $b_i = c_{i1} y_1 + c_{i2} y_2 + \cdots + c_{im} y_m$ olacak şekilde $i = 1, 2, \ldots, n$ için $c_{i1},\ c_{i2}, \ldots ,\ c_{im} \in F$ vardır. Böylece

$$a = \sum_{i=1}^{n} b_i x_i = \sum_{i=1}^{n} \left( \sum_{j=1}^{m} c_{ij} y_j \right) x_i = \sum_{i,j} c_{ij}(y_j x_i)$$

yazılabilir. O halde BA kümesi F üzerinde K'yı gerer. BA kümesinin F cismi üzerinde lineer bağımsız olduğu gösterilsin.

$c_{ij} \in F$ olmak üzere

$$0 = \sum_{i,j} c_{ij}(y_j x_i) = \sum_{i} \sum_{j} (c_{ij} y_j) x_i$$

olduğu kabul edilsin. O zaman $c_{ij} y_j \in E$ ve A, E üzerinde K için bir baz olduğundan her $i$ için

$$\sum_{j} c_{ij} y_j = 0$$

yazılabilir. Fakat $c_{ij} \in F$ ve B, F üzerinde E için bir baz olduğundan buradan her $c_{ij}$ elemanı sıfır olur. O halde BA kümesi F üzerinde K'yı gerdiğinden ve yine F üzerinde lineer bağımsız olduğundan F üzerinde K için bir baz olur.

**Örnek 1.5.2.** $\{1, \sqrt{2}\}$, $\mathbb{Q}(\sqrt{3})$ üzerinde $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ için bir bazdır. Yine $\{1, \sqrt{3}\}$, $\mathbb{Q}$ üzerinde $\mathbb{Q}(\sqrt{3})$ için bir bazdır. O halde Teorem 1.5.6'nın ispatından $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ kümesi $\mathbb{Q}$ üzerinde $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ için bir bazdır.

E, F cisminin bir cisim genişlemesi ve $\alpha_1, \alpha_2, \dots, \alpha_n \in E$ olsun. $F[\alpha_1] \subseteq F(\alpha_1)$ olacak şekilde en küçük $F(\alpha_1)$ cismini elde etmek için $\alpha_1$, F'ye eklenebilir. $F \subseteq F[\alpha_1]$ olduğundan $F \subseteq F(\alpha_1) \subseteq E$'dır. Aynı şekilde $\alpha_2$ , $F(\alpha_1)[\alpha_2]$'yi kapsayan $F(\alpha_1)(\alpha_2) = F(\alpha_1, \alpha_2)$ en küçük cismini elde etmek için $F(\alpha_1)$ e eklenebilir.

$F(\alpha_1) \subseteq F(\alpha_1)[\alpha_2]$ olduğundan $F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2)$ yazılabilir. Bu işleme devam edilirse F cisminin cisim genişlemelerinin kulesi ya da zinciri denilen

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq F(\alpha_1, \alpha_2, \alpha_3) \subseteq \cdots \subseteq F(\alpha_1, \alpha_2, \dots, \alpha_n)$$

elde edilir.

$$F(\alpha_1, \alpha_2, \dots, \alpha_n) = F(\alpha_1, \alpha_2, \dots, \alpha_{n-1})(\alpha_n)$$

olup $F(\alpha_1, \alpha_2, \dots, \alpha_n)$, F'ye $\alpha_1,\ \alpha_2, \dots,\ \alpha_n \in E$ elemanlarının katılmasıyla F'den elde edilen cisimdir.

**Örnek 1.5.3.** $f(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$ polinomunun kökleri $\sqrt{2},\ -\sqrt{2},\ i,\ -i$ olup bunların hepsi $\mathbb{Q}$ üzerinde cebirseldir. $f(x)$ in kökleri

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, -\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, -\sqrt{2}, i) \subseteq \mathbb{Q}(\sqrt{2}, -\sqrt{2}, i, -i)$$

cisim kulesini oluşturur. $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ olduğundan $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ ve $\mathbb{Q}(\sqrt{2},\ -\sqrt{2},\ i) \subseteq \mathbb{Q}(\sqrt{2},\ i),\quad i \in \mathbb{Q}(\sqrt{2},\ i)$ olduğundan $\mathbb{Q}(\sqrt{2}, -\sqrt{2},\ i,\ -i) = \mathbb{Q}(\sqrt{2},\ i)$ olup bundan dolayı cisim genişlemelerinin kulesi $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, i)$ şeklinde yazılır.

**Örnek 1.5.4.** $\mathbb{Q}(\sqrt{3},\ \sqrt[3]{3}) = \mathbb{Q}(\sqrt[6]{3})$ olduğu gösterilsin. $\sqrt[3]{3},\ x^3 - 3 = 0$ indirgenmez polinomunun kökü olduğundan $\left[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}\right] = 3,\ \sqrt{3},\ x^2 - 3 = 0$ indirgenmez polinomunun kökü olduğundan $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ ve $(3,2) = 1$ olduğundan $\left[\mathbb{Q}(\sqrt{3},\ \sqrt[3]{3}) : \mathbb{Q}\right] = 3.2 = 6$ dır. $\sqrt[6]{3}, x^6 - 3 = 0$ indirgenmez polinomunun kökü olduğundan $\left[\mathbb{Q}(\sqrt[6]{3}) : \mathbb{Q}\right] = 6$ dır.

$\sqrt{3},\ \sqrt[6]{3} \in \mathbb{Q}(\sqrt{3},\ \sqrt[3]{3})$ ise $\sqrt{3}.\frac{1}{\sqrt[6]{3}} = \sqrt[6]{3} \in \mathbb{Q}(\sqrt{3},\ \sqrt[3]{3})$.

$\sqrt[6]{3} \in \mathbb{Q}(\sqrt[6]{3})$ olduğundan $\mathbb{Q}(\sqrt{3},\ \sqrt[3]{3}) \subset \mathbb{Q}(\sqrt[6]{3})$ dir.

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[6]{3}) \subset \mathbb{Q}(\sqrt{3},\ \sqrt[3]{3})$ olduğundan $\mathbb{Q}(\sqrt{3},\ \sqrt[3]{3}) = \mathbb{Q}(\sqrt[6]{3})$ dir.

**Not 1.5.7.** Eğer $\alpha$, F üzerinde cebirsel ise F'nin her cisim genişlemesi üzerinde cebirseldir. $\alpha$, F[x] deki sıfırdan farklı bir polinomun kökü olmak üzere E, F'nin herhangi bir cisim genişlemesi ise $F \subseteq E$ olursa $F[x] \subseteq E[x]$ olmalıdır. Dolayısıyla $\alpha$, $E[x]$ deki sıfırdan farklı bir polinomunun köküdür. Böylece $\alpha_1, \alpha_2, \dots, \alpha_n$ elemanlarının her biri $k = 1,2, \dots, n$ için $F(\alpha_1, \alpha_2, \dots, \alpha_k)$ üzerinde cebirseldir.

**Teorem 1.5.8.** $\alpha_1, \alpha_2, \dots, \alpha_n$ elemanlarının her biri F cismi üzerinde cebirsel ise bu durumda $F(\alpha_1, \alpha_2, \dots, \alpha_n)$, F nin bir cebirsel cisim genişlemesidir.

**İspat.** $\alpha_1, \alpha_2, \dots, \alpha_n$ elemanlarının F üzerinde cebirsel olduğu kabul edilsin ve

$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq F(\alpha_1, \alpha_2, \alpha_3) \subseteq \cdots \subseteq F(\alpha_1, \alpha_2, \ldots, \alpha_n)$

cisim kulesi kolaylık açısından

$F_0 = F, F_1 = F(\alpha_1), \ldots, F_n = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$

şeklinde gösterilsin. Bu durumda

$F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$

olacağı açıktır. Öte yandan $\alpha_i$, $F_{i-1}$ cismi üzerinde cebirsel olduğundan Teorem 1.4.20'den $[F_i : F_{i-1}]$ in $\alpha_i$ nin $F_{i-1}[x]$ deki minimal polinomunun derecesi ile belirlenir. $i = 1,2, \ldots, n$ için $[F_i : F_{i-1}]$ sonludur. Buna göre Teorem 1.5.6'dan

$[F_2 : F_0] = [F_2 : F_1][F_1 : F_0]$

yazılabilir. Bu son eşitliğin her iki tarafını $[F_3 : F_2]$ ile çarparak ve Teorem 1.5.6 tekrar kullanılırsa

$[F_3 : F_0] = [F_3 : F_2][F_2 : F_0] = [F_3 : F_2][F_2 : F_1][F_1 : F_0]$

yazılabilir. Benzer şekilde bu defa da son eşitliği $[F_4 : F_3]$ ile çarpılırsa

$[F_4 : F_0] = [F_4 : F_3][F_3 : F_0] = [F_4 : F_3][F_3 : F_2][F_2 : F_1][F_1 : F_0]$.

Bu işlemin n. adımda

$[F_n : F_0] = [F_n : F_{n-1}] \ldots [F_3 : F_2][F_2 : F_1][F_1 : F_0]$

eşitliği elde edilir. Bu son denklemin sağ tarafındaki her çarpan bir pozitif tamsayı olduğundan $[F_n : F_0]$ dolayısı ile $[F_n : F]$ pozitif bir tamsayı olmak zorundadır. O halde Teorem 1.5.3'den $F_n$ , F cisminin bir cebirsel genişlemesidir denilebilir.

**Sonuç 1.5.9.** $\alpha_1, \alpha_2, \ldots, \alpha_n$ elemanları F üzerinde cebirsel ve

$[F_n : F_0] = [F_n : F_{n-1}] \ldots [F_3 : F_2][F_2 : F_1][F_1 : F_0]$

olduğunda $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, F'nin bir sonlu boyutlu cisim genişlemesidir.

**Teorem 1.5.10.** Eğer K, E'nin ve E'de F'nin cebirsel cisim genişlemeleri ise K'da F'nin bir cebirsel cisim genişlemesidir.

**İspat.** $\alpha \in K$ ve $\alpha$, E üzerinde cebirsel olmak üzere $E[x]$ de $f(\alpha) = 0$ olacak şekilde bir

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

polinomu vardır. $F(\alpha_0, \alpha_1, \dots, \alpha_n)$ cismi için $\alpha_1, \alpha_2, \dots, \alpha_n \in A$ F üzerinde cebirsel olduğundan Sonuç 1.5.9'dan $F(\alpha_1, \alpha_2, \dots, \alpha_n)$, F'nin bir sonlu boyutlu cisim genişlemesidir. $\alpha$, $f(x) \in F(\alpha_0, \alpha_1, \dots, \alpha_n)[x]$ polinomunun bir kökü olduğundan $F(\alpha_0, \alpha_1, \dots, \alpha_n)$ cismi üzerinde cebirseldir. $F(\alpha_0, \alpha_1, \dots, \alpha_n, \propto) = F(\alpha_0, \alpha_1, \dots, \alpha_n)(\propto)$, $F(\alpha_0, \alpha_1, \dots, \alpha_n)$ nin ve $F(\alpha_0, \alpha_1, \dots, \alpha_n)$, F nin sonlu bir cisim genişlemesidir. Fakat

$$[F(\alpha_0, \alpha_1, \dots, \alpha_n, \propto): F] = [F(\alpha_0, \alpha_1, \dots, \alpha_n, \propto): F(\alpha_0, \alpha_1, \dots, \alpha_n)].[F(\alpha_0, \alpha_1, \dots, \alpha_n): F]$$

ve bu eşitliğin sağ tarafındaki her iki çarpan da pozitif tamsayılardır. Bundan dolayı $F(\alpha_0, \alpha_1, \dots, \alpha_n, \propto)$, F nin bir sonlu cisim genişlemesi olup Teorem 2.1.3'den bir cebirsel cisim genişlemesidir. $\propto \in F(\alpha_0, \alpha_1, \dots, \alpha_n, \propto)$ olduğundan $a$, F üzerinde cebirseldir. $\propto$ elemanı keyfi seçildiğinden K F'nin cisminin bir cebirsel cisim genişlemesidir.

**Örnek 1.5.5.** $f(x) = x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$ in indirgenmez olduğu aşağıda verilmiştir. $\mathbb{Z}_3(\propto)$ nın bütün elemanları ve $\propto^2 + \propto + 2$ elemanının çarpımsal tersi aşağıdaki gibidir. $f(0) = 1$, $f(1) = 1$ ve $f(2) = 2$ olduğundan $f(x) = x^3 + 2x^2 + 1$ polinomu $\mathbb{Z}_3$ cismi üzerinde kökü yoktur ve indirgenemezdir. $f(x) = x^3 + 2x^2 + 1$ polinomunun bir kökü $\propto$ ise $f(\propto) = \propto^3 + 2\propto^2 + 1 = 0$ yazılır. Bu $\propto$ kökünü $\mathbb{Z}_3$'e ilave ederek elde edilen $\mathbb{Z}_3(\propto)$ cisminin elemanları şunlardır:

$0, 1, 2, \propto, \propto + 1, \propto + 2, 2\propto, 2\propto + 1, 2\propto + 2, \propto^2, \propto^2 + 1,$
$\propto^2 + 2, 2\propto^2, 2\propto^2 + 1, 2\propto^2 + 2, \propto^2 + \propto, \propto^2 + \propto + 1,$
$\propto^2 + \propto + 2, 2\propto^2 + \propto, 2\propto^2 + \propto + 1, 2\propto^2 + \propto + 2, 2\propto^2 + 2\propto,$
$2\propto^2 + 2\propto + 1, 2\propto^2 + 2\propto + 2$

$F(\propto)$ nın verilen $\propto^2 + \propto + 2$ polinomunun çarpmaya göre tersi $\propto + 1$ dir. Yani $(\propto^2 + \propto + 2)^{-1} = \propto + 1$ dir.

$(\propto^2 + \propto + 2)(\propto + 1) = \propto^3 + 2\propto^2 + 3\propto + 2$
olup $f(\propto) = \propto^3 + 2\propto^2 + 1 = 0$ dolayısıyla $\propto^3 + 2\propto^2 = -1$ ve $\mathbb{Z}_3$'de $3\propto = 0$ olduğundan

$(\propto^2 + \propto + 2)(\propto + 1) = -1 + 2 = 1$

yazılır.

**Tanım 1.5.11.** F bir cisim ve E, F'nin bir cisim genişlemesi ve $f(x) \in F[x]$ sabit olmayan bir polinom olmak üzere eğer $f(x)$, $E[x]$ deki lineer çarpanların bir çarpımı olarak yazılırsa $f(x)$ polinomuna E'de parçalanışa sahiptir denir. $f(x)$ polinomu E'de parçalanışa sahip fakat E'nin öz alt cisimlerinde parçalanışa sahip olmayan bir polinom ise o zaman E'ye F üzerinde $f(x)$ için *parçalanış cismi* denir.

**Teorem 1.5.12.** E, F cisminin bir cisim genişlemesi ve $f(x) \in F[x]$ derecesi n olan ve sabit olmayan bir polinom olmak üzere $f(x)$ polinomu E cismi üzerinde

$f(x) = \propto (x - \propto_1)(x - \propto_2) \dots (x - \propto_n)$

olacak biçimde bir parçalanışa sahip ise $F(\propto_1, \propto_2, \dots, \propto_n)$ cismi $f(x)$ polinomu için bir parçalanış cismidir.

**İspat.** $\propto_1, \propto_2, \dots, \propto_n \in F(\propto_1, \propto_2, \dots, \propto_n)$, $f(x)$ in kökleri olduğundan $f(x)$ polinomu $F(\propto_1, \propto_2, \dots, \propto_n)$ üzerinde parçalanışa sahiptir.

$$F \subseteq F' \subseteq F(\propto_1, \propto_2, \dots, \propto_n) \qquad (1)$$

ve $f(x)$ polinomu $F'$ üzerinde parçalanışa sahip olsun. $E[x]$ bir Tek Çarpanlama Bölgesi (TÇB) ve $F'[x] \subseteq E[x]$ olduğundan $f(x)$, $F'$ üzerinde

$f(x) = \propto (x - \propto_1)(x - \propto_2) \dots (x - \propto_n)$

şeklinde bir parçalanışa sahiptir. $\propto_1, \propto_2, \dots, \propto_n \in F'$ olup bundan dolayı $F(\propto_1, \propto_2, \dots, \propto_n)$, $f(x)$ in bütün köklerinin kapsayan E'nin en küçük alt cismi olduğundan

$$F(\propto_1, \propto_2, \dots, \propto_n) \subseteq F' \qquad (2)$$

Dolayısıyla (1) ve (2)'den $F' = F(\propto_1, \propto_2, \dots, \propto_n)$ yazılır. Böylece $F(\propto_1, \propto_2, \dots, \propto_n)$, $f(x)$ için bir parçalanış cismidir.

**Tanım 1.5.13.** F bir cisim olmak üzere eğer $F[x]$ deki sabit olmayan her polinom F cisminde bir köke sahipse F cismine *cebirsel olarak kapalıdır* denir.

**Tanım 1.5.14.** F bir cisim ve E, F'nin bir cisim genişlemesi olsun. E cebirsel olarak kapalı ve E, F'nin bir cebirsel cisim genişlemesi ise E'ye F'nin bir *cebirsel kapanışı* denir ve $\bar{F} = E$ ile gösterilir.

**Teorem 1.5.15.** Bir F cismi için aşağıdaki önermeler denktir:

a) F cebirsel olarak kapalıdır.
b) $\forall f(x) \in F[x]$ indirgenemez polinomu için $der\big(f(x)\big) = 1$ dir.
c) $\propto \in F$ olmak üzere$F[x]$ deki sabit olmayan her polinom $x-\propto$ formunda lineer çarpanlar ve polinomun başkatsayısının çarpımı şeklinde bir parçalanışa sahiptir.
d) Eğer E, F cisminin bir cebirsel cisim genişlemesi ise E = F dir.

**İspat.** (a) ⇒ (b) F cisminin cebirsel olarak kapalı ve $f(x)$ polinomunun $F[x]$ de indirgenmez olsun. F cebirsel olarak kapalı olduğundan $f(x)$ polinomu bir $\propto \in F$ köküne sahiptir. Böylece $f(x)$ polinomu $g(x) \in F[x]$ olmak üzere $f(x) = (x-\propto)g(x)$ şeklinde yazılır. Kabulden $f(x)$, $F[x]$ de indirgenemez $g(x) = a$ olacak şekilde bir $0 \neq a \in F$ vardır. O halde $f(x) = a(x-\propto)$ olup buradan $der\big(f(x)\big) = 1$ dir.

(b) ⇒ (c) $\forall f(x) \in F[x]$ indirgenemez polinomu için $der\big(f(x)\big) = 1$ olsun. $F[x]$ bir TÇB olduğundan $\forall f_i(x)$ polinomu $F[x]$ de indirgenemez olmak üzere $f(x) = f_1(x)f_2(x) \dots f_n(n)$ şeklinde yazılır. Kabulden her $f_i(x)$ in derecesi 1 olduğundan $i = 1,2, \dots, n$ için $a_i, \propto_i \in F$ olmak üzere $f_i(x) = a_i(x - \propto_i)$ şeklinde yazılır. $a = a_1a_2 \dots a_n$, $f(x)$ polinomunun başkatsayısı olmak üzere

$f(x) = a(x - \propto_1)(x - \propto_2) \dots (x - \propto_n)$.

(c) ⇒ (d) E'nin F cisminin bir cebirsel genişlemesi olsun. Eğer $\propto \in E$ ise $\propto$, $F$ cismi üzerinde cebirseldir. Diğer yandan $\propto$'nın $F[x]$ de minimal polinomunun $m(x)$ olsun. O halde $m(x)$, $F[x]$ de indirgenemez olduğundan (c) şıkkından $der\big(m(x)\big) = 1$ olmalıdır. Eğer $a \in F$ için $m(x) = x + a$ şeklinde ise $0 = m(\propto) = \propto + a$ ya da $\propto = -a \in F$ olup buradan $F \subseteq E$ olduğundan $F = E$ dir.

(d) ⇒ (a) $f(x) \in F[x]$ sabit olmayan bir polinom olmak üzere Kronecker Teoreminin sonucundan $E$, $f(x)$ polinomunun bir $\propto$ kökünü kapsayacak şekilde F nin bir cebirsel genişlemesidir. Teorem 1.5.3'ün sonucundan $F(\propto)$, $F$'nin bir cebirsel cisim

genişlemesidir. (d) şıkkından $F(\propto) = F$ olup buradan $\propto \in F$ dir. O halde F cebirsel olarak kapalıdır.

**Örnek 1.5.6.** $\mathbb{C}$ kompleks sayılar cismi $\mathbb{R}$ reel sayılar cisminin bir cebirsel kapanışıdır. Cebirin Esas Teoreminden eğer $f(x) \in \mathbb{C}(x)$ pozitif dereceli bir polinom ise $f(x)$ polinomunun $\mathbb{C}$'de bir kökü vardır. Bu teoremden dolayı $\mathbb{C}$ cebirsel olarak kapalıdır. $\mathbb{C}$, $\mathbb{R}$'nin bir cebirsel genişlemesidir. Çünkü $z = a + bi \in \mathbb{C}$ ise bu durumda $z$,

$f(x) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$

polinomunun bir köküdür. O halde $\mathbb{C}$, $\mathbb{R}$'in cebirsel kapanışıdır.

**Not 1.5.16.** $\mathbb{C}$ kompleks sayılar cismi, alt cisimlerinin her birinin cebirsel kapanışını kapsar.

## 1.6. Geometrik Cisimler

Eski Mısır ve Yunanlılara kadar geriye giden matematikçiler "Verilen bir açı derecesiz pergel ve derecesiz cetvelle üç eşit parçaya bölünebilir mi?", "Verilen bir küpün hacminin iki katına eşit hacimli bir küp derecesiz pergel ve derecesiz cetvelle çizilebilir mi?" ve "Verilen bir dairenin alanına eşit alanlı bir kare derecesiz pergel ve derecesiz cetvelle çizilebilir mi?" problemlerine çözüm aramışlardır. 18. ve 19. Yüzyıllarda modern cebirin gelişmesiyle bu problemlerin çözümleri olumsuz olarak elde edilebilmiştir. Bu bölümde ispatlarıyla gösterilecektir.

Burada cetvel ve pergel denildiğinde üzerinde hiç bir işaret bulunmayan pergel ve cetvel kastedilmektedir.

Bir düzlemde P ve Q noktaları verilsin. Uç noktaları P ve Q olan doğru parçası PQ ve uzunluğu $|PQ|$ ile gösterilir. P ve Q 'dan geçen doğru $L(P, Q)$ ve merkezi P ve yarıçapı $|PQ|$ olan çember $C(P, Q)$ ile gösterilir.

Bir düzlemde kartezyen koordinat sistemi verilsin. x ekseni üzerinde $A(-1,0)$ ve $B(1,0)$ noktaları belirlensin.

**Tanım 1.6.1.** Düzlemde birbirinden farklı E, F, G, H noktaları ve Z herhangi bir nokta olsun.

(i) $Z \in L(E,F) \cap L(G,H)$ , $L(E,F) \neq L(G,H)$ ya da

(ii) $Z \in L(E,F) \cap C(G,H)$ ya da

(iii) $Z \in C(E,F) \cap C(G,H), C(E,F) \neq C(G,H)$

ise Z'ye E, F, G, H noktaları yardımıyla *çizilebilir nokta* denir. Eğer Z = A ya da Z = B ise ya da $n \geq 1$ için $P_1, P_2, \dots, P_n$ düzlemin noktaları olmak üzere

(iv) $P_0 \in \{A,B\}$ ve her $0 \leq j < n$ için $P_{j+1}$ noktası $\{A, B, P_1, P_2, \dots, P_j\}$ kümesinin noktaları yardımıyla çizilebilirse ve

(v) $Z = P_n$ ise o zaman Z'ye *çizilebilir nokta* denir.

A ve B noktaları çizilebilir noktalardır.

**Örnek 1.6.1.** $\{A,B\}$ yardımıyla $(-2,0)$, $(2,0)$, $(0,-\sqrt{2})$ ve $(0,\sqrt{2})$ noktaları çizilebilirdir.

$C(A,B)$ ve $C(B,A)$ çemberlerinin birbiriyle ve $L(A,B)$ ile kesim noktaları aranan noktalardır.

**Örnek 1.6.2.** $O = (0,0)$ noktası $\{A, B, (0,-\sqrt{2}), (0,\sqrt{2})\}$ kümesi yardımıyla çizilebilir. $O \in L(A,B) \cap L((0,-\sqrt{2}) \cup (0,\sqrt{2}))$ dir.

$(cos\theta, sin\theta)$ noktası çizilebilirse θ açısına *çizilebilir açı* denir. Her açı iki eşit parçaya bölünebilir olduğundan, eğer $(cos\theta, sin\theta)$ noktası çizilebilirse $(cos\frac{\theta}{2}, sin\frac{\theta}{2})$ noktası ve dolayısıyla $\frac{\theta}{2}$ açısı çizilebilirdir. Bir doğruya paralel doğrular ve üzerindeki bir noktada dik olan bir doğru pergel ve cetvel yardımıyla çizilebilir.

**Tanım 1.6.2.** $(a,b)$ noktası çizilebilirse $z = a + ib$ kompleks sayısına *çizilebilir sayı* denir. Özel olarak $(a,0)$ noktası çizilebilirse $a$ reel sayısına çizilebilir sayı denir.

$(0,0)$, $(1,0)$, $(-1,0)$, $(0,-1)$, $(0,1)$, $(0,-\sqrt{2})$ ve $(0,\sqrt{2})$ noktaları çizilebilir olduğundan $0,1,-1,-i,i,-\sqrt{2}i,\sqrt{2}i$ sayıları çizilebilirdir. O halde bütün tamsayılar ve bütün rasyonel sayılar çizilebilirdir.

**Lemma 1.6.3.** $z = a + ib$ kompleks sayısının çizilebilir olması için gerek ve yeter şart reel kısmının ve imajiner kısmının çizilebilir olmasıdır.

**İspat.** z çizilebilir olmak üzere $Z = (a, b)$ noktası çizilebilirdir. Z noktasından x-eksenine dik olan bir doğru çizilebilir. C(Z,O), x-eksenini O ve R $\neq 0$ noktalarında keser. C(O,Z) ve C(R,Z) nin kesim noktaları Z ve $Z'$ dür. L$(Z, Z')$ doğrusu x-eksenine diktir ve bu doğrunun x eksenini kestiği nokta $(a, 0)$ olduğundan $a$ sayısı çizilebilirdir. Benzer şekilde b sayısı çizilebilirdir. Tersine $a$ ve b sayıları çizilebilir ise $(a, 0)$ ve $(b, 0)$ noktaları çizilebilirdir. O zaman $(0, b)$ noktasının da çizilebilir olduğu açıktır. Şimdi $(a, 0)$ ve $(0, b)$ noktalarında sırasıyla x ve y eksenlerine çıkılan dik doğruların kesin noktası $Z = (a, b)$ olduğundan $z = a + ib$ çizilebilirdir.

Tüm çizilebilir kompleks sayıların kümesine K denirse $\mathbb{Q}$ cismi $\mathbb{R}$'nin en küçük alt cismi olduğundan aynı zamanda K'nın da alt cismidir.

**Lemma 1.6.4.** Aşağıdakiler sağlanır.

(i) $K \cap \mathbb{R}$ cisim ise K, $\mathbb{C}$'nin bir alt cismidir.

(ii) $K \cap \mathbb{R} \leq \mathbb{R}$ olmak üzere $\forall a \in K \cap \mathbb{R}$ ve $a > 0$ için $\sqrt{a} \in K \cap \mathbb{R}$ ise $\forall z \in K$ için $\sqrt{z} \in K$ dır.

**İspat.** (i) $K \cap \mathbb{R}$ cisim ve $z = a + ib, w = c + id$ çizilebilir sayılar olmak üzere Lemma 1.6.3'ten $a, b, c, d \in K \cap \mathbb{R}$ ve $a \pm c,\ b \pm d \in K \cap \mathbb{R}$ dir. O halde $z \pm w = (a \pm c) + i(b \pm d) \in K$ dir. Aynı şekilde $zw \in K$'dir. $z \neq 0$ ise $z\bar{z} = a^2 + b^2 \neq 0$ olduğundan

$$z^{-1} = \frac{\bar{z}}{a^2 + b^2} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}.$$

Ayrıca $K \cap \mathbb{R}$ cisim olduğundan $\frac{a}{a^2+b^2}$ ve $\frac{b}{a^2+b^2}$ elemanlarını kapsar ve Lemma 1.6.3'ten $z^{-1} \in K$ olur. Böylelikle K cisimdir.

(ii) $K \cap \mathbb{R}$ cisim, karekök alma işlemine göre kapalı ve $z = a + ib$ çizilebilir olsun. Lemma 1.6.3'ten $a, b \in K \cap \mathbb{R}$ dir. $r = \sqrt{a^2 + b^2} \in K \cap \mathbb{R}$ olmak üzere z'nin kutupsal biçimi $z = re^{i\theta}$ şeklindedir. Yani

$$\sqrt{z} = \sqrt{r}\left(\cos\left(\frac{\theta}{2} + k\pi\right) + i\sin\left(\frac{\theta}{2} + k\pi\right)\right); \qquad k = 0,1\,.$$

$r \geq 0$ olduğundan $\sqrt{r} \in K \cap \mathbb{R}$ dir. θ çizilebilir olduğundan $\frac{\theta}{2}$ ve $\frac{\theta}{2} + k\pi$ çizilebilirdir. O halde $\left(\cos\left(\frac{\theta}{2} + k\pi\right) + i \sin\left(\frac{\theta}{2} + k\pi\right)\right)$ noktası çizilebilirdir. $\sqrt{z}$ çizilebilirdir ve $\sqrt{z} \in K$ dır.

**Örnek 1.6.3.** $z = e^{\frac{2\pi}{5}} = \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5}$ olmak üzere

a) $\text{İ}nd(z, \mathbb{Q}) = x^4 + x^3 + x^2 + x + 1$

b) $z + \bar{z} = 2\cos\frac{2\pi}{5}$

c) $(z + \bar{z})^2 + (z + \bar{z}) - 1 = 0$

d) $\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$

aşağıdaki gibidir.

(a) $f(x) = x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$, $p(x) = x - 1$ ve $q(x) = x^4 + x^3 + x^2 + x + 1$ şeklinde tanımlansın. $x^5 - 1$ denkleminin kökleri $z_k = \cos\frac{2k\pi}{5} + i \sin\frac{2k\pi}{5}$, $k = 0,\ 1,\ 2,\ 3,\ 4$ şeklindedir. $w = z_1 = \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5}$ denklemin bir köküdür; yani, $f(w) = 0$ ise $p(w) \neq 0$ olduğundan $q(w) = 0$ dır. O halde $w$, $q(x)$ in köküdür ve $\mathbb{Q}$ üzerinde indirgenmezdir. O halde $\text{İ}nd(z, \mathbb{Q}) = x^4 + x^3 + x^2 + x + 1$ dir.

(b) $\bar{z} = \cos\frac{2\pi}{5} - i \sin\frac{2\pi}{5}$ dir. $z + \bar{z} = \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5} + \cos\frac{2\pi}{5} - i \sin\frac{2\pi}{5} = 2\cos\frac{2\pi}{5}$

(c) $z + \bar{z} = 2\cos\frac{2\pi}{5}$ yerine yazılırsa $(2\cos\frac{2\pi}{5})^2 + \left(2\cos\frac{2\pi}{5}\right) - 1 = 0$ denkleminde değişken değiştirme yöntemi kullanılarak $2\cos\frac{2\pi}{5} = a$ alınırsa $a^2 + a - 1 = 0$ denkleminin kökleri $a_{1,2} = \frac{-1\pm\sqrt{5}}{2}$ dir.

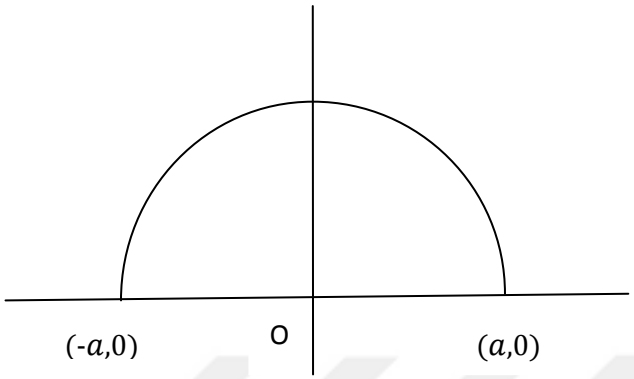
(d) (c)'den $2\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{2}$ olduğundan $\cos\frac{2\pi}{5} = \frac{-1\pm\sqrt{5}}{4}$ tür.

**Teorem 1.6.5.** K, $\mathbb{C}$'nin alt cismi olmak üzere karekök ve eşlenik alma işlemlerine göre kapalıdır.

**İspat.** $K \cap \mathbb{R}$ nin ve Lemma 1.6.4(i)'den K'nin cisim olduğu gösterilir. $a, b \in K \cap \mathbb{R}$ için $a + b, -a, ab$ ve $b \neq 0$ iken $b^{-1} \in K \cap \mathbb{R}$ olduğu gösterilmelidir.

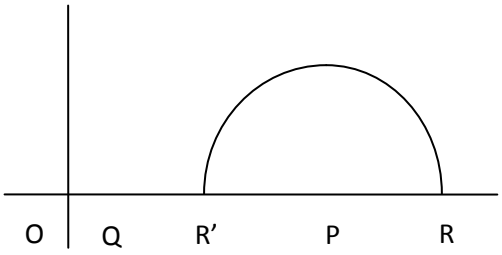
(i) $-a$ sayısı çizilebilirdir.

$P = (a, 0)$ noktası çizilebilirdir ve $\mathrm{C}(\mathrm{O}, \mathrm{P})$ çemberinin x eksenini kestiği noktalar $P = (a, 0)$ ve $P' = (-a, 0)$ olduğundan $-a \in K \cap \mathbb{R}$ dir (Şekil 3).




**Şekil 3.** $-a$ sayısının çizilebilir olduğunu gösteren koordinat düzlemi

(ii) $a + b$, $a - b$ sayıları çizilebilirdir. $a \neq 0$ ve $b \neq 0$ ve $a \geq b$ için $a \geq b > 0$ olmak üzere $P = (a, 0)$ ve $Q = (b, 0)$ olsun. Merkezi P ve yarıçapı b olan çember çizilir ve bu çember x eksenini $R = (a + b, 0)$ ve $R' = (a - b, 0)$ noktalarında keser. O halde $a + b$ ve $a - b \in K \cap \mathbb{R}$ dir (Şekil 4).

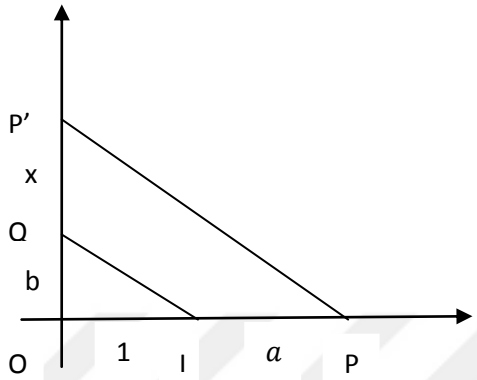



**Şekil 4.** $a + b$ ve $a - b$ sayılarının çizilebilir olduğunu gösteren koordinat düzlemi

Benzer şekilde $a > 0 > b$ ve $0 > a > b$ içinde aynı sonuç elde edilir.

(iii) $ab$ sayısı çizilebilirdir. $a > 0,\ b > 0$ ve $I = (1,0),\ P = (1+a, 0), Q = (0, b)$ olsun.

Şekil 5'te IQ ∥ $PP'$, QOI ve $P'OP$ üçgenleri benzer olduğundan $\frac{|OI|}{|OP|} = \frac{|OQ|}{|OP'|}$ dir.

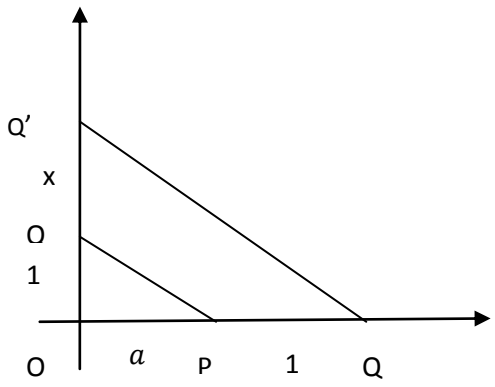



**Şekil 5.** $ab$ sayısının çizilebilir olduğunu gösteren koordinat düzlemi

$|OI| = 1,\ |OP| = 1 + a,\ |OQ| = b,\ |OP'| = b + x$ olduğundan $\frac{1}{1+a} = \frac{b}{b+x}$ eşitliğinden $x = ab$ elde edilir. O halde $ab \in K \cap \mathbb{R}$ dir.

(iv) $a \neq 0$ olmak üzere $\frac{1}{a}$ sayısı çizilebilirdir.

$a > 0$ ve $P = (a, 0),\ Q = (a+1, 0)$ ve $I = (0,1)$ olsun. Şekil 6'da $PI \parallel QQ'$, IOP ve $Q'OQ$ üçgenleri benzer olduğundan

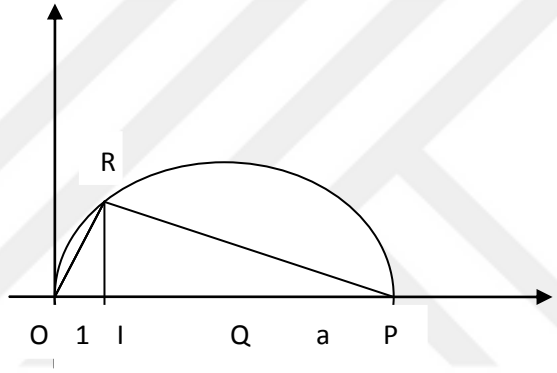



**Şekil 6.** $1, a$ sayısının çizilebilir olduğunu gösteren koordinat düzlemi

$\frac{1}{1+x} = \frac{a}{a+1}$ eşitliğinden $x = \frac{1}{a}$ bulunur.

Böylece (i), (ii), (iii) ve (iv)'ten görüldüğü gibi $K \cap \mathbb{R}$, $\mathbb{R}$'nin alt cismidir.

(v) $a \in K \cap \mathbb{R}$ ve $a \geq 0$ için $\sqrt{a}$ sayısı çizilebilirdir.
$a > 0$ ve $I = (1,0)$, $P = (a+1,0)$ ve OP doğru parçasının orta noktası Q olsun. $C(Q,O)$ çemberi çizilsin ve I noktasından x eksenine çıkılan dikmenin çemberi kestiği nokta R olsun. ROI ve RIP üçgenleri benzer olduğundan $\frac{|RI|}{|QP|} = \frac{|QI|}{|RI|} = \frac{|RI|}{a} = \frac{1}{|RI|}$ eşitliğinden $|RI|^2 = a$ elde edilir. O halde $|RI| = \sqrt{a} \in K \cap \mathbb{R}$ dir (Şekil 7).




**Şekil 7.** $\sqrt{a}$ sayısının çizilebilir olduğunu gösteren koordinat düzlemi

(vi) $z = a + ib \in K$ ve Lemma 1.6.3'ten $a, b \in K \cap \mathbb{R}$ dir. $-b \in K \cap \mathbb{R}$ olduğundan $z = a - ib \in K$ dir.

**Sonuç 1.6.6.** $a, b, c \in K$ olmak üzere $ax^2 + bx + c = 0$ ikinci derece denklemin kökleri K'dedir.

**İspat.** $a, b, c \in K$ olduğundan $b \neq 0$ ise $a/b$ ve $a/c \in K$ dir. $a = 1$ alınırsa

$$x^2 + bx + c = (x + \frac{b}{2})^2 + (4c - b^2)/4$$

olduğundan $(x+\frac{b}{2})^2+\frac{4c-b^2}{4}=0$ ve $(x+\frac{b}{2})^2=(b^2-4c)/4$ bulunur. $D=b^2-4ac$ olmak üzere $D\in K$ dir. Teorem 1.6.5'ten K bir cisim ve $\sqrt{D}\in K$ dir. $(x+\frac{b}{2})^2=(\sqrt{D})^2/4$ olduğundan $x_1=-\frac{b}{2}-\frac{\sqrt{D}}{2}, x_2=-\frac{b}{2}+\frac{\sqrt{D}}{2}$ ve $x_1,x_2\in K$ dir.

**Lemma 1.6.7.** F, $\mathbb{C}$'nin bir alt cismi ve eşleniklemeye göre kapalı olmak üzere $i\in F$ olsun. P, Q, R, S çizilebilir sayılarının koordinatları F'de ve $w=u+iv\in\mathbb{C}$ olsun. Eğer

(i) Birbirinden farklı iki doğru bir noktada kesişirse ya da
(ii) Bir çember ve bir doğru bir noktada kesişirse ya da
(iii) Birbirinden farklı iki çember kesişirse

$[F(w):F]\leq 2$ dir.

**İspat.** (i) için $L(P,Q)$ ve $L(R,S)$ x eksenine dik olmayan birbirinden farklı iki doğru ve

$L(P,Q):y=mx+q;\qquad m,q\in F\cap\mathbb{R}$

$L(R,S):y=m'x+q';\qquad m',q'\in F\cap\mathbb{R}$

olmak üzere $w\in L(P,Q)\cap L(R,S)$ olsun. $w=(u,v)$ için $mu+q=m'u+q'$ ve $(m-m')u=q'-q$ elde edilir. Ayrıca $m\neq m'$ olduğundan her iki taraf $m-m'$ ile bölünürse

$u=\frac{q-q'}{m-m'}$ ve $v=\frac{q-q'}{m-m'}m+q$

elde edilir. $m,m',q,q'\in F\cap\mathbb{R}$ olduğundan $u,v\in F\cap\mathbb{R}$ ve $i\in F$ olduğundan $w=u+iv\in F$ ve $[F(w):F]=1$ dir. Diğer koşullarda da aynı sonuca ulaşılır.

(ii) için $L(P,Q)$ bir doğru ve $C(R,S)$ bir çember olmak üzere

$L(P,Q):y=mx+q;\qquad m,q\in F\cap\mathbb{R},$

$C(R,S):(x-a)^2+(y-b)^2=r^2$ ve $r^2=(c-a)^2+(d-b)^2\in F\cap\mathbb{R}$

ve $w\in L(P,Q)\cap C(R,S)$ olsun. $w=(u,v)$ için $v=mu+q$ ve $(u-a)^2+(v-b)^2=r^2$ yazılır. $v$'nin değeri ikinci eşitlikte yerine yazılırsa ikinci dereceden $Au^2+Bu+C=0$ eşitliği elde edilir. $A=1+m^2,\ B=2(mq-mb-a),\ C=a^2+$

$(q-b)^2-r^2$ dir. O halde $f(u)=Au^2+Bu+C=0$ dir ve $\text{İ}nd(u,F)|f(x)$ olduğundan $[F(u):F]\leq 2$ dir. $v=mu+q\in F(u)$ ve $i\in F$ olduğundan $w\in F(u)$ ve $[F(w):F]\leq 2$ dir. Gerçekten $f(x)$ in kökleri

$$x_{1,2}=\frac{-B\pm D}{2A} \text{ ve } D=B^2-4AC$$

olduğundan $F(u)=F(\sqrt{D})$ dir. D, F içinde bir tam kare ise $|F(u):F|=1$ ve tam kare değilse $[F(u):F]=2$ dir.

(iii) için $C(P,Q)$ ve $C(R,S)$ birbirinden farklı iki çember olmak üzere bu çemberler ya teğettir ya da farklı iki noktada kesişir. O halde (ii) haline dönüştürülerek iddia sağlanır.

**Sonuç 1.6.8.** Tüm çizilebilir kompleks sayıların cismi K olmak üzere katsayıları K'den seçilmiş olan doğrular ve çemberlerin kesişimleri belli bir $z\in K$ için $K\left(\sqrt{z}\right)$ cismindedir.

**Teorem 1.6.9.** Bir z kompleks sayısının çizilebilir olması için gerek ve yeter şart her $0\leq i<s$ tamsayısı için $[L_{i+1}:L_i]\in\{1,2\}$ ve $z\in L_s$ olacak şekilde bir $\mathbb{Q}=L_0\leq L_1\leq\cdots\leq L_s$ cisim kulesinin olmasıdır.

**İspat.** z çizilebilir olmak üzere $n\geq 1$ için öyle bir $-1,1,z_1,z_2,\dots,z_n=z$ çizilebilir sayıları vardır ki her $1\leq j\leq n$ için $z_j$ sayısı $\{-1,1,z_1,z_2,\dots,z_{j-1}\}$ kümesiyle çizilebilir. $z_0\in\{-1,1\}$ olmak üzere $i$ çizilebilir olduğundan $z_1=i$ olarak alınır. $\forall j\geq 1$ için her $0\leq i<s(j)$ için, $[L_{i+1}:L_i]\leq 2$ dir ve $-1,1,z_1,z_2,\dots,z_j\in L_{s(j)}$, eşlenik almaya göre kapalıdır şartlarını sağlayan

$$\mathbb{Q}=L_0\leq L_1\leq\cdots\leq L_{s(j)} \qquad (*)$$

cisim kulesi inşa edilir. $j=1$ için $L_{s(1)}=L_1=\mathbb{Q}(i)$ olarak alınırsa $[\mathbb{Q}(i):\mathbb{Q}]=2$ olacağından (*) sağlanır. Tümevarımdan $j\geq 1$ için iddia sağlansın ve $j+1$ için doğru olduğu gösterilsin. $z_{j+1}$ sayısı $-1,1,z_1,z_2,\dots,z_j$ sayılarıyla çizildiğinden bu noktalara karşılık gelen öyle P, Q, R, S noktaları vardır ki aşağıdakilerden biri sağlanır.

(i) $z_{j+1}\in L(P,Q)\cap L(R,S)$; $\quad L(P,Q)\neq L(R,S)$ ya da

(ii) $z_{j+1}\in L(P,Q)\cap C(R,S)$

$L_{s(j)}$, $i$'yi içerir ve eşlenik almaya kapalıdır. Lemma 1.6.8 gereğince $[L_{s(j)}(z_{j+1}) : L_{s(j)}] \leq 2$ dir ve $L_{s(j+1)} = L_{s(j)}(z_j + 1)$ olsun. Eğer $L_{s(j)}$ in eşlenik almaya göre kapalı olduğu gösterilirse (*) kulesine $L_{s(j+1)}$ eklenmesiyle elde edilen kule (1) ve (2) şartlarını sağlar ve tümevarım tamamlanır. $z_{j+1} \in L_{s(j)}$ ise $L_{s(j+1)} = L_{s(j)}$ olduğundan $L_{s(j+1)}$ eşlenik almaya göre kapalıdır $z_{j+1} \notin L_{s(j)}$ olmak üzere Lemma 1.6.7'nin ispatından öyle bir $D \geq 0$ reel sayısı vardır ki; $L_{s(j)}(z_{j+1}) = L_{s(j)}(\sqrt{D})$'dir. $w \in L_{s(j)}(\sqrt{D})$ ve $w = u + v\sqrt{D}$ olacak şekilde $u, v \in L_{s(j)}$ vardır ve $\bar{w} = \bar{u} + \bar{v}\sqrt{D}$ bulunur. $\bar{u}, \bar{v} \in L_{s(j)}$ olduğundan $\bar{w} \in L_{s(j)}(\sqrt{D})$ ve $L_{s(j)}(\sqrt{D})$ eşlenik almaya göre kapalıdır.

Tersine $\forall 0 \leq j < s$ için $[L_{i+1} : L_i] \leq 2$ ve $z \in L_s$ olacak şekilde bir $\mathbb{Q} = L_0 \leq L_1 \leq \cdots \leq L_s$ cisim kulesi verilsin. $\forall j \geq 0$ için $L_j$ nin elemanlarının çizilebilir olduğu gösterilmelidir. $j = 0$ için $\mathbb{Q}$'nun elemanları çizilebilir olduğundan iddia doğrudur. $j \geq 0$ için iddia sağlansın ve $j + 1$ için doğruluğu gösterilsin. $[L_{i+1} : L_i] = 1$ ise iddia açıktır. O halde $[L_{i+1} : L_i] = 2$ ve $w \in L_{j+1}/L_j$ olmak üzere $L_{j+1} = L_j(w)$ dir. $p(x) = \text{İnd}(w, L_j)$ olsun. $p(x) = x^2 + bx + c$ olacak şekilde $b, c \in L_j$ vardır. Sonuç 1.6.6'dan $p(x)$ in kökleri çizilebilir olduğundan w çizilebilirdir ve Lemma 1.3.4 gereğince $L_j(w)$ nun her elemanı çizilebilirdir.

**Sonuç 1.6.10.** Bir $z \in \mathbb{C}$ çizilebilirse $s \geq 0$ tamsayısı için $[\mathbb{Q}(z): \mathbb{Q}] = 2^s$ dır.

**İspat.** Teorem 1.6.9'dan $\mathbb{Q} = L_0 \leq L_1 \leq \cdots \leq L_s$ cisim kulesi için her $0 \leq j < s$ olmak üzere $[L_{i+1} : L_i] \leq 2$ ve $z \in L_s$'dir. Sonuç 1.2.4'ten dolayı,

$$[L_s : \mathbb{Q}] = [L_s : L_{s-1}][L_{s-1} : L_{s-2}] \ldots [L_1 : L_0]$$

olduğundan $[L_s : \mathbb{Q}] = 2^t$ olacak biçimde $t \geq 0$ tamsayısı vardır. Diğer taraftan $[L_s : \mathbb{Q}] = [L_s : L(z)].[L(z) : \mathbb{Q}]$ olduğundan $[L(z) : \mathbb{Q}] / 2^t$ dir. O halde $[L(z) : \mathbb{Q}] = 2^S$ olacak şekilde bir $s \geq 0$ vardır.

**Teorem 1.6.11.** Verilen bir açı derecesiz pergel ve derecesiz cetvelle üç eşit parçaya her zaman bölünemez.

**İspat.** Bir θ açısının çizilebilir olması için $(cos\theta, sin\theta)$ noktası çizilebilir olmalıdır. θ açısının üç eşit parçaya bölünebilmesi için $(cos\frac{\theta}{3}, sin\frac{\theta}{3})$ noktasının çizilebilir olması gerekir. Özel olarak $cos\frac{\theta}{3}$ çizilebilir ise θ açısı çizilebilirdir.

**Örnek 1.6.3.** 6° ve 15° lik açıların üçe bölünemez. Yani bir 6°'lik açının çizilebilir olması demek $(cos6°, sin6°)$ noktasının çizilebilir olması demektir. Dolayısıyla 6° lik açının üç eşit parçaya bölünebilmesi için $(cos2°, sin2°)$ noktasının çizilebilir olması gerekir. Özel olarak $cos2°$ çizilebilir değildir. O halde 6° lik açı üçe bölünemez.

Benzer şekilde bir 15° lik açının çizilebilir olması demek $(cos15°,\ sin15°)$ noktasının çizilebilir olması demektir. Dolayısıyla 15° lik açının üç eşit parçaya bölünebilmesi için $(cos5°,\ sin5°)$ noktasının çizilebilir olması gerekir. Özel olarak $cos5°$ çizilebilir değildir. O halde 15° lik açı üçe bölünemez.

**Örnek 1.6.4.** Derecesiz pergel ve derecesiz cetvel kullanarak 45° lik açının üç eşit parçaya bölünebilir. 45° lik açının çizilebilir olması demek $(cos45,\ sin45)$ noktasının çizilebilir olması demektir. Dolayısıyla 45° lik açının üç eşit parçaya bölünebilmesi için $(cos15,\ sin15)$ noktasının çizilebilir olması gerekir. Özel olarak $cos15$ çizilebilirdir.

$$cos3\theta = \cos(\theta + 2\theta) = cos\theta cos2\theta - sin\theta sin2 = cos\theta(2cos^2\theta - 1) - 2sin^2\theta cos\theta$$

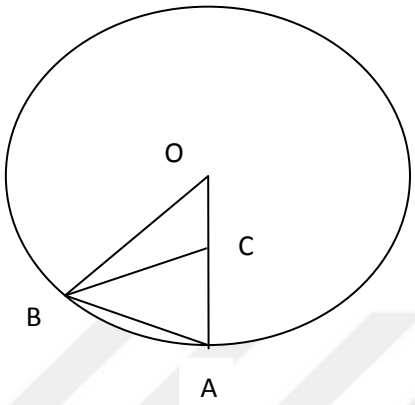
$$= 2cos^3\theta - cos\theta - 2cos\theta + 2cos^3\theta = 4cos^3\theta - 3cos\theta$$

olduğundan $cos3\theta = 4cos^3\theta - 3cos\theta$ dır. Burada $3\theta = 45$ konulursa $\frac{\sqrt{2}}{2} = 4cos^320 - 3cos20$ ve buradan $8cos^315 - 6cos15 - \sqrt{2} = 0$ bulunur. Dolayısıyla $cos15°$ sayısı $p(x) = 8x^3 - 6x - \sqrt{2}$ polinomunun bir köküdür. Ancak bu polinom $\mathbb{Q}$ üzerinde rasyonel kökü $cos15° = \frac{\sqrt{6}-\sqrt{2}}{4}$ sayısı çizilebilirdir.

**Not 1.6.12.** $n \geq 3$ olmak üzere düzgün bir n-genin çizilebilir olması için gerek ve yeter şart $\cos\frac{2\pi}{n}$ sayısının çizilebilir olmasıdır.

**Örnek 1.6.5.** 36° lik açıların çizilebildiğini ve buradan yararlanarak düzgün ongen aşağıdaki gibi çizilebilir.

$m(\widehat{AOB}) = a,\ m(\widehat{ABC}) = m(\widehat{BAO}) = \beta,\ |AB| = |OB| = |OC|$ dir. $m(\widehat{BCA}) = 2\beta = a$ dır. ABC üçgeninin iç açıları toplamı 180 dir; yani, $5a = 180°,\ a = 36°$ dir. $[AB]$ kirişine benzer şekilde 10 tane eşit uzunlukta kiriş çizilerek düzgün ongen elde edilir. Köşeleri bir atlayarak birleştirilirse düzgün beşgen elde edilir. (Şekil 8)




**Şekil 8.** Düzgün ongen çizimi

**Teorem 1.6.13.** Verilen bir küpün hacminin iki katına eşit hacimli bir küp derecesiz pergel ve derecesiz cetvelle çizilemez.

**İspat.** Bir kenarının uzunluğu 1 birim olan bir küp çizilebilir olsun. Bu küpün hacmi 1 birim küptür. Hacmi 2 birim küp olan bir küpün bir kenarının uzunluğu $\sqrt[3]{2}$ dir. $\sqrt[3]{2}$ çizilebilir değildir. $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ olduğundan Sonuç 1.3.10'dan bir çelişki elde edilir.

**Teorem 1.6.14.** Verilen bir dairenin alanına eşit alanlı bir kare derecesiz pergel ve derecesiz cetvelle çizilemez.

**İspat.** Yarıçapı 1 birim olan bir daire çizilebilirdir ve bu dairenin alanı $\pi$ birim karedir. Alanının ölçüsü $\pi$ birim kare olan bir karenin bir kenarının uzunluğu $\sqrt{\pi}$ dir. $\pi$ transandant olduğundan $\sqrt{\pi}$ çizilemezdir. Çelişki elde edilir.

## 1.7. İzomorfizmaların Genişletimesi ve Otomorfizma Grupları

Bu bölümde E, F'nin cebirsel genişlemesi ve $\alpha,\ \beta \in E$ elemanları minimal bir polinomun sıfırları olmak üzere F cisminin her bir elemanını kendisine ve $F(\alpha)$ dan $F(\beta)$ ye tanımlı izomorfizmalar verilecektir ve bu izomorfizmalar E'nin F'yi sabit bırakan otomorfizmalarının belirlenmesinde yardımcı olacaktır. E'nin F'yi sabit bırakan tüm otomorfizmalarının kümesinin E'nin tüm otomorfizmalarının grubunun bir alt grubu olduğu gösterilecektir.

**Tanım 1.7.1.** F bir cisim E, F'nin bir cebirsel genişlemesi ve $u, v \in E$ olmak üzere $\text{İ}nd(u,F) = \text{İ}nd(v,F)$ ise $u$ ile $v$, F *üzerinde eşleniktir* denir.

**Örnek 1.7.1.** $a, b$ reel sayılar olmak üzere $z = a + ib$ ve $z \in \mathbb{C}$ olsun. Eğer $b = 0$ ise $z = a$ ve $z = a$ dır. $b \neq 0$ ise $p(x) = (x - z)(x - z) = x^2 - 2ax + (a^2 + b^2)$ olsun. $p(x)$ in kökleri $z, z$ reel olmadığından $p(x), \mathbb{R}$ üzerinde indirgenmezdir. O halde z'nin eşlenikleri $z, z$ dir.

**Örnek 1.7.2.** $\mathbb{Q}$ üzerinde $\sqrt{2} + i$ nin eşleniği $-\sqrt{2} + i$, $\sqrt{i}$ nin eşleniği $\sqrt{i}$, $\sqrt{7}$ nin eşleniği $-\sqrt{7}$, $\sqrt[3]{8} = 2$ olduğundan eşleniği kendisidir ve $\sqrt{3+\sqrt{2}}$ nin eşlenikleri $\sqrt{7}\left(\sqrt{3-\sqrt{2}}\right), -\sqrt{7}\left(\sqrt{3-\sqrt{2}}\right)$ dir.

**Tanım 1.7.2.** $\varphi : R \to S$ bir halka homomorfizması ve A, R'nin bir alt halkası olmak üzere $\forall a \in A$ için $\varphi(a) = a$ ise $\varphi$, A'yı *sabit bırakır* denir. $\sigma : A \to S$ bir halka homomorfizması olmak üzere $\varphi|A = \sigma$ ise $\sigma$'ya $\varphi$'nin A'ya *kısıtlanışı* ve $\varphi$'ye $\sigma$'nun R'den S'ye bir *genişlemesi* denir.

**Lemma 1.7.3.** $\sigma : F \to F'$ bir cisim izomorfizması olmak üzere

$$\sigma^* : (a_0 + a_1x + \dots a_nx^n) \to \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$$

olarak tanımlı $\sigma^*$ bir halka homomorfizmasıdır. $p(x) \in F[x],\ F$ üzerinde indirgenmez ise $\sigma^*\big(p(x)\big),\ F'$ üzerinde indirgenmezdir.

**İspat.** $p(x) \in F[x],\ F$ üzerinde indirgenmez olsun. $s(x), t(x) \in F'[x]$ olmak üzere $\sigma^*\big(p(x)\big) = s(x)t(x)$ olarak alınsın. $\sigma^*$ örten olduğundan $s(x) = \sigma^*\big(a(x)\big),\ t(x) = \sigma^*(b(x))$ olacak şekilde $a(x),\ b(x) \in F[x]$ vardır. Yerlerine yazılırsa $\sigma^*\big(p(x)\big) =$

$\sigma^*(a(x))\sigma^*(b(x)) = \sigma^*(a(x)b(x))$ ve $p(x) = a(x)b(x)$ elde edilir. $p(x)$, $F$ üzerinde indirgenmez olduğundan $a(x) \in F$ ya da $b(x) \in F$ dir. $s(x) \in F'$ ya da $t(x) \in F'$ çelişkisi elde edilir. $\sigma^*(p(x))$, $F'$ üzerinde indirgenmezdir.

**Teorem 1.7.4.** $E = F(u)$ ve $E' = F'(v)$ basit cebirsel genişlemeler ve $\sigma : F \to F'$ bir cisim izomorfizması olmak üzere $p(x) = İnd(u, F)$ ve $\sigma^*(p(x)) = İnd(v, F')$ olsun. $\tau : E \to E'$ cisim homomorfizması için $\tau(u) = v$ ve $\tau|F = \sigma$ dir. (Şekil 9)

**İspat.** Teorem 1.2.14(i)'den dolayı

$$\begin{array}{ccc} F(u) & \overset{\tau}{\to} & F'(v) \\ | & & | \\ F & \overset{\sigma}{\to} & F' \end{array}$$

**Şekil 9.** Teorem 1.7.4'te verilen $\tau$ ve $\tau|F = \sigma$ homomorfizmaları

$E = \{f(u) : f(x) \in F[x]\}$ ve $E' = \{h(v) : h(x) \in F'[x]\}$ tir. $\forall f(x) \in F[x]$ için $\sigma^*(f(x)) = f^*(x)$ olsun. $\tau : E \to E'$ fonksiyonu $\tau : f(u) \to f^*(v)$ olarak tanımlanır. $\forall a \in F$ için $\tau(a) = \sigma(a)$ ve $\tau(u) = v$ dir.

(i) $f(u)$, $g(u) \in F(u)$, $u$ ve $v$'ye karşılık gelen değer homomorfizmaları $\phi_u$ ve $\phi_v$ olmak üzere

$f(u) = g(u) \Leftrightarrow \phi_u(f(x)) = \phi_u(g(x))$

$\Leftrightarrow \phi_u(f(x) - g(x)) = 0_F$

$\Leftrightarrow f(x) - g(x) \in Ker(\phi_u)$

$\Leftrightarrow f(x) - g(x) \in \langle p(x) \rangle$

$\Leftrightarrow p(x) | (f(x) - g(x))$

$\Leftrightarrow \sigma^*(p(x)) | \sigma^*(f(x) - g(x))$

$\Leftrightarrow p^*(x)|\big(f^*(x)-g^*(x)\big)$

$\Leftrightarrow f^*(x)-g^*(x)\in Ker(\phi_u)$

$\Leftrightarrow f^*(v)-g^*(v)=0_{F'}$

$\Leftrightarrow f^*(v)=g^*(v)$

olduğundan $\tau$ iyi tanımlı ve bire birdir.

(ii) $f(u)=\sum_{i=0}^{m}a_iu^i$ ve $g(u)=\sum_{j=0}^{n}b_ju^j$ olmak üzere $m\le n$ alınsın. $m<n$ iken $a_{m+2}=\cdots=a_n=0_F$ olarak alınırsa $f(u)=\sum_{i=0}^{n}a_iu^i$ şeklinde yazılır. O halde $\tau(f(u))=\sum_{i=0}^{n}\sigma(a_i)v^i$ ve $\tau(g(u))=\sum_{j=0}^{n}\sigma(b_j)v^j$ dir.

$$\tau\left(\sum_{i=0}^{n}a_iu^i+\sum_{j=0}^{n}b_ju^j\right)=\tau\left(\sum_{i=0}^{n}a_iu^i+\sum_{i=0}^{n}b_iu^i\right)$$

$$=\tau\left(\sum_{i=0}^{n}(a_i+b_i)u^i\right)$$

$$=\sum_{i=0}^{n}\sigma(a_i+b_i)v^i$$

$$=\sum_{i=0}^{n}\sigma(a_i)v^i+\sum_{j=0}^{n}\sigma(b_j)v^j$$

$$=\tau\left(\sum_{i=0}^{n}a_iu^i\right)+\tau\left(\sum_{j=0}^{n}b_ju^j\right)$$

olduğundan $\tau\big(f(u)+g(u)\big)=\tau\big(f(u)\big)+\tau(g(u))$ dur.

$$\left(\sum\nolimits_{i=0}^{n}a_iu^i\sum\nolimits_{j=0}^{n}b_ju^j\right)=\sum\nolimits_{k=0}^{m+n}c_ku^k,\ \ c_k=\sum\nolimits_{i=0}^{k}a_ib_{k-i}$$

olduğunda

$$\tau\big(f(u)g(u)\big) = \sum_{k=0}^{m+n} \sigma(c_k)v^k\,, \qquad \sigma(c_k) = \sum_{i=0}^{m+n} \sigma(a_i)\,\sigma(b_{k-i}).$$

Diğer taraftan

$$\tau\big(f(u)\big)\tau\big(g(u)\big) = \left(\sum_{i=0}^{m}\big(\sigma(a_i)v^i\big)\right)\left(\sum_{j=0}^{n}\sigma(b_j)v^j\right) = \sum_{k=0}^{m+n} d_k v^k,$$

$$d_k = \sum_{i=0}^{k} \sigma(a_i)\sigma(b_{k-i}).$$

$\forall k \geq 0$ için $\sigma(c_k) = d_k$ olduğundan

$$\tau\big(f(u)g(u)\big) = \tau\big(f(u)\big)\tau\big(g(u)\big).$$

$\tau$ bir halka homomorfizmasıdır ve tanımdan dolayı $\tau$ örten olduğundan bir halka izomorfizmasıdır.

Teorem 1.7.4'te $F = F'$, $E = E'$ ve $\sigma = \iota$ ise $\tau : F(u) \to F(v)$ izomorfizması, $\psi_{u,v}$ ile gösterilir ve buna *temel izomorfizma (monomorfizma)* denir.

**Sonuç 1.7.5.** $F$ ve $F'$ iki cisim ve sırasıyla, $E$ ve $E'$ bunların birer cebirsel genişlemeleri olsun. $\sigma : F \to F'$ bir cisim izomorfizması olmak üzere $p(x) \in F[x]$ bir indirgenmez polinom ve $p(x)$ in E içindeki bir kökü $u$ olsun. $\sigma$'nun $F(u)$ dan $E'$ içine tanımlı her genişlemesi $u$'yu $\sigma^*(p(x))$ in bir köküne götürür. O halde bu genişlemelerinin sayısı $\sigma^*(p(x))$ in $E'$ içindeki köklerinin sayısına eşittir.

**İspat.** Teorem 1.7.4'ten $\sigma^*(p(x))$ in $E'$ içindeki her kökü $v$ için öyle bir $\tau : F(u) \to F'(v)$ izomorfizması vardır ki, $\tau|F = \sigma$ ve $\tau(u) = v$ dir. Bir polinomun bir cisimdeki sıfırları sayısı sonlu olduğundan $\tau$ izomorfizmasının genişlemelerinin sayısı da sonludur.

Tersine $\tau$, $F(u)$ dan $E'$ içine bir cisim homomorfizması olmak üzere $\tau|F = \sigma$ olsun. $p(x) = a_0 + a_1x + \cdots + a_nx^n$ olsun. $p(u) = 0_F$ olduğundan $a_0 + a_1u + \cdots + a_nu^n = 0_F$ dir. Eşitliğin iki tarafına $\tau$ uygulanırsa

$\tau(a_0 + a_1u + \cdots + a_nu^n) = \tau(a_0) + \tau(a_1)\tau(u) + \cdots + \tau(a_n)\tau(u^n) = \sigma(a_0) + \sigma(a_1)\tau(u) + \cdots + \sigma(a_n)\tau(u)^n = 0_F$,

Diğer taraftan $\sigma^*\big(p(x)\big) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$ olduğundan $\tau^*\left(p\big(\tau(u)\big)\right) = 0_F$, olur. O halde $\tau(u)$, $\sigma^*(p(x))$ in bir köküdür. $\sigma$'nun $\sigma^*(p(x))$ in farklı köklerine karşılık gelen genişlemeleri de farklıdır. O zaman $\sigma$'nun $F(u)$ dan $E'$ içine olan genişlemelerinin sayısı $\sigma^*(p(x))$ in $E'$ içindeki köklerinin sayısına eşittir.

**Sonuç 1.7.6.** $E = F(u)$, $F$'nin bir basit cebirsel genişlemesi, $p(x) = \text{İ}nd(u, F)$ ve $der\big(p(x)\big) = n$ olmak üzere E'nin F'yi sabit bırakan otomorfizmalarının sayısı $p(x)$ in E içindeki köklerinin sayısına eşittir.

**İspat.** $\tau|F = \iota_F$ olduğundan Sonuç 1.7.5'ten $p(x)$ in E içinde öyle bir kökü $v$ vardır ki, $\tau(u) = v$ ve $\tau|F = \iota_F$; yani, $\tau = \psi_{u,v}$ dir. Böylece Teorem 1.6.4'ten $\tau, F(u)$ dan $F(v)$ üzerine bir izomorfizmadır. $\tau$'nun E nin otomorfizması olduğu gösterilir. $\text{İ}nd(u, F) = p(x) = \text{İ}nd(v, F)$ olduğundan $[F(u) : F] = [F(v) : F]$ dir. $[E : F] = [F(u) : F] = [E : F(v)][F(v) : F]$ olduğundan $[E : F(v)] = 1$ ve $boy_{F(v)}(E) = 1$ dir. O halde E'nin bir $F(v)$-bazı $\{1_F\}$ olduğundan $E = F(v)1_F = F(v)$ dir ve $\tau$, $E$'nin F'yi sabit bırakan bir otomorfizmasıdır. E'nin F'yi sabit bırakan bütün otomorfizmaları $v, p(x)$ in E içindeki kökleri üzerinde değişmek üzere $\psi_{u,v}$ temel otomorfizmalarından oluşur.

$b \in E$ olsun. Teorem 1.2.14'ten $c_0, c_1, \ldots, c_{n-1} \in F$ olmak üzere

$b = c_0 + c_1u + \cdots + c_{n-1}u^{n-1}$

ve

$\tau(b) = \psi_{u,v}(b) = \psi_{u,v}(c_0 + c_1u + \cdots + c_{n-1}u^{n-1}) = c_0 + c_1v + \cdots + c_{n-1}v^{n-1}$

şeklindedir.

**Teorem 1.7.7.** $f(x) \in \mathbb{R}$[x]'in $\mathbb{R}$ üzerinde indirgenmez olması için gerek ve yeter şart $f(x)$ in derecesinin 1 olması ya da $f(x) = ax^2 + bx + c$ ve $b^2 - 4ac < 0$ olmasıdır.

**İspat.** $der\big(f(x)\big) = 1$ ise ya da $f(x) = ax^2 + bx + c$ ve $b^2 - 4ac < 0$ ise $f(x)$ in $\mathbb{R}$ üzerinde indirgenmez olduğu açıktır. O halde $f(x)$ in indirgenmez ve $der(f(x)) \geq 2$ olarak alınır. $\mathbb{C}$ cebirsel kapalı olduğundan $f(x)$ in bir kompleks kökü z vardır ve

$f(\bar{z}) = 0$ dır. $f(x), \mathbb{R}$ üzerinde indirgenmez olduğundan $\bar{z} = z$ dir. Teorem 1.5.13 gereğince $f(x) = (x - z)(x - \bar{z})f_1(x)$ olacak şekilde $f_1(x) \in \mathbb{R}[x]$ vardır. $(x - z)(x - \bar{z}) = x^2 - 2(z + \bar{z}) + z\bar{z} \in \mathbb{R}[x]$ ve $f(x), \mathbb{R}$ üzerinde indirgenmez olduğundan $f_1(x) = c$ olacak şekilde bir $c \in \mathbb{R}$ vardır ve $der\big(f(x)\big) = 2$ dir.

**Örnek 1.7.3.** $E = \mathbb{Q}(\sqrt{3})$ cisminden $\mathbb{C}$'ye tanımlı bütün $\mathbb{Q}$ monomorfizmaları aşağıdaki gibidir.

$\text{İ}nd\big(\sqrt{3}, \mathbb{Q}\big) = x^2 - 3$ olduğundan $\sqrt{3}$ nin $\mathbb{Q}$ üzerindeki eşlenikleri $-\sqrt{3}$, $\sqrt{3}$ dir ve Sonuç 1.7.6 gereğince E'nin $\mathbb{Q}$'yu sabit bırakan bütün monomorfizmaları $\psi_{\sqrt{3},\sqrt{3}}$ ve $\psi_{\sqrt{3},-\sqrt{3}}$ dir. $a, b \in \mathbb{Q}$ olmak üzere $a + b\sqrt{3} \in E$ şeklindedir ve $\psi_{\sqrt{3},-\sqrt{3}}\big(a + b\sqrt{3}\big) = a - b\sqrt{3}$ dir.

**Tanım 1.7.8.** Bir cismin kendi üzerine tanımlı bir izomorfizmasına o cismin *otomorfizması* denir ve bir E cisminin bütün otomorfizmalarının kümesi $Aut(E)$ veya $Oto(E)$ ile gösterilir.

**Teorem 1.7.9.** E bir cisim olmak üzere Aut(E) bileşke işlemine göre bir gruptur.

**İspat.** $\iota_E : E \to E$ birim fonksiyonu otomorfizma olduğundan $\iota_E \in$ Aut(E) ve $Aut(E) \neq \emptyset$ dir. $\sigma, \tau \in Aut(E)$ ve $a, b \in E$ olsun. $\sigma \circ \tau = \sigma\tau$ olmak üzere

$$\sigma\tau(a + b) = \sigma\big(\tau(a + b)\big) = \sigma\big(\tau(a) + \tau(b)\big) = \sigma\tau(a) + \sigma\tau(b)$$

ve benzer şekilde $\sigma\tau(ab) = (\sigma(\tau(a))(\sigma(\tau(b))$ olduğundan $\sigma\tau$, halka homomorfizmasıdır. $\sigma$ ve $\tau$ bire bir eşleme olduğundan $\sigma\tau$, $E$'nin bir otomorfizmasıdır ve $\sigma\tau \in Aut(E)$ dir. Bileşke işlemi birleşme özelliğini sağlar ve $\iota_E$ bu işleme göre birim elemandır. $\sigma \in Aut(E)$ için $\sigma^{-1} \in Aut(E)$ olduğu gösterilsin. $\sigma$ bire bir ve örten olduğundan $\sigma^{-1}$ bire bir ve örtendir. $a, b \in E$ olsun. $\sigma(c) = a, \sigma(d) = b$ olacak şekilde $c, d \in E$ vardır. Buradan $\sigma^{-1}(a) = c, \sigma^{-1}(b) = d$ bulunur.

$\sigma(c + d) = \sigma(c) + \sigma(d) = a + b$ olduğundan $\sigma^{-1}(a + b) = c + d = \sigma^{-1}(a) + \sigma^{-1}(b)$ dir. Benzer şekilde $\sigma^{-1}(ab) = \sigma^{-1}(a)\sigma^{-1}(b)$ olduğundan $\sigma^{-1} \in Aut(E)$ dir. O halde $Aut(E)$ bileşke işlemine göre bir gruptur.

$Aut(E)$ ye E'nin *otomorfizma grubu* denir.

**Tanım 1.7.10.** E bir cisim F, E'nin bir alt cismi ve H, $Aut(E)$ nin bir altgrubu olmak üzere E'nin F'yi sabit bırakan bütün otomorfizmalarının kümesi G(E/F) ile E'nin H tarafından sabit bırakılan elemanlarının kümesi $E_H$ ile gösterilir.

$G(E/F) = \{\sigma \in Aut(E) : \text{her } a \in F \text{ için } \sigma(a) = a\}$

ve

$E_H = \{a \in E \ : \ \text{her } \sigma \in H \text{ için } \sigma(a) = a\}$.

**Teorem 1.7.11.** E bir cisim ve H, $Aut(E)$ nin bir altgrubu olmak üzere $E_H$ kümesi E'nin alt cismidir.

**İspat.** $\forall \sigma \in H$ için $\sigma(0_E) = 0_E$ ve $\sigma(1_E) = 1_E$ olduğundan $0_E,\ 1_E \in E_H$ ve $|E_H| \geq 2$ dir. $a, b \in E_H$ olmak üzere Teorem 1.4.4'ten $a + b, -a,\ ab \in E_H$ ve $b \neq 0_E$ iken $b^{-1} \in E_H$ olduğunun gösterilmesi yeterlidir. $\sigma \in H$ olmak üzere

$\sigma(a + b) = \sigma(a) + \sigma(b) = a + b,\ \ \sigma(-a) = -\sigma(a) = -a,$

$\sigma(ab) = \sigma(a)\sigma(b) = ab$

olduğundan $a + b, -a,\ ab \in E_H$ dır. $b \neq 0_E$ olmak üzere $bb^{-1} = 1_E$ olduğundan $\sigma(bb^{-1}) = \sigma(b)\sigma(b^{-1}) = 1_R$ dir. Buradan, $\sigma(b^{-1}) = \sigma(b)^{-1} = b^{-1}$ olduğundan $b^{-1} \in E_H$ dır. O halde $E_H$, E'nin alt cismidir.

$E_H$ cismine H'nın E içindeki *sabit cismi* denir.

**Sonuç 1.7.12.** E, F'nin bir cisim genişlemesi olmak üzere G(E/F) kümesi $Aut(E)$ nin bir alt grubudur.

**İspat.** $\iota_E \in G(E/F)$ olduğundan $G(E/F) \neq \emptyset$ dir. $\sigma, \tau \in G(E/F)$ olmak üzere $\forall a \in F$ için $\sigma\tau(a) = \sigma\big(\tau(a)\big) = \sigma(a) = a$ ve $\sigma^{-1}(a) = a$ olduğundan $\sigma\tau, \sigma^{-1} \in G(E/F)$ ve Teorem 1.2.3 gereğince, $G(E/F)$, $Aut(E)$ 'nin altgrubudur.

E'nin F *üzerindeki grubu* (E'nin F'yi *sabit bırakan otomorfizmalarının grubu*) $G(E/F)$ dir.

Teorem 1.4.4'ten E'nin bütün alt cisimlerinin kesişimi E'nin bir alt cismidir ve buna E'nin *asal cismi* denir. $\Delta(E)$ ile gösterilir. Diğer taraftan, Teorem 1.7.11'den,

$H = Aut(E)$ için $E_H$, E'nin bir alt cismidir ve $\Delta(E) \subseteq E_H$ dır. $E_H$ nın her elemanı E'nin her otomorfizması tarafından sabit bırakıldığından, $\Delta(E)$ nin her elemanı da E'nin her otomorfizması tarafından sabit bırakılır. O halde $Aut(E) = G(E/\Delta(E))$ dir. $kar(E)$ nin 0 ise $\Delta(E)$, $\mathbb{Q}$'ya ya da bir p asal sayısı ise $\mathbb{Z}_p$ ye izomorftur.

**Teorem 1.7.13.** F bir cisim, E, F'nin bir cebirsel cisim genişlemesi ve $E = F(u_1, u_2, \dots, u_k)$ olmak üzere $G(E/F)$ nin her $\sigma$ elemanı $u_1, u_2, \dots, u_k$ deki değerleriyle tam olarak belirlenir. $G(E/F)$ nin her $\sigma$ elemanı için $\sigma(\{u_1, u_2, \dots, u_k\}) \subseteq \{u_1, u_2, \dots, u_s\}$ ise $G(E/F)$, $Sym(\{u_1, u_2, \dots, u_k\})$ nin bir alt grubuna izomorftur.

**İspat.** $\sigma \in G(E/F)$, $y \in E$ ve Sonuç 1.4.21'den $\forall i \geq 0$ için $c_{m_{i1},\dots,m_{ik}} \in F$ olmak üzere $y$ elemanı $c_{m_{i1},\dots,m_{ik}} u_1^{m_{i1}} \dots u_k^{m_{ik}}$ tipindeki monomların bir sonlu toplamıdır.

$\sigma\left(c_{m_{i1},\dots,m_{ik}} u_1^{m_{i1}} \dots u_k^{m_{ik}}\right)$

$= \sigma\left(c_{m_{i1},\dots,m_{ik}}\right)\sigma(u_1)^{m_{i1}} \dots \sigma(u_k)^{m_{ik}}$

$= c_{m_{i1},\dots,m_{ik}}\sigma(u_1)^{m_{i1}} \dots \sigma(u_k)^{m_{ik}}$

olduğundan $\sigma$; $\sigma(u_1)$, $\sigma(u_2), \dots, \sigma(u_k)$ değerleriyle tam olarak belirlenir.

$U = \{u_1, u_2, \dots, u_k\}$, her $\sigma \in G(E/F)$ için $\sigma(U) \subseteq U$ ve $\bar{\sigma} = \sigma|U$ olsun. $\sigma$ bire bir olduğundan $\bar{\sigma}$ de bire bir ve örtendir. O halde $\bar{\sigma} \in Sym(U)$ dır. $\sigma \to \bar{\sigma}$ eşlemesi $G(E/F)$ den $Sym(U)$ ye bir monomorfizma olduğu açıktır.

**Sonuç 1.7.14.** F bir cisim, E, F'nin bir cebirsel genişlemesi ve $E = F(u_1, u_2, \dots, u_k)$ olmak üzere $\forall \sigma \in G(E/F)$ için $\sigma(\{(u_1, u_2, \dots, u_k)\}) \subseteq \{u_1, u_2, \dots, u_k\}$ olsun. $G(E/F)$, $S_k$ nın bir alt grubuna izomorftur ve böylece $|G(E/F)||k!$ dir.

**İspat.** $U = \{u_1, u_2, \dots, u_k\}$ ve Teorem 1.7.14'ten $G(E/F)$, $Sym(U)$ nun bir alt grubuna izomorftur. $Sym(U) \cong S_k$ olduğundan $G(E/F)$, $S_k$ nın bir alt grubuna izomorftur ve Lagrange teoreminden dolayı $|G(E/F)||k!$ dir.

**Örnek 1.7.4.** $E = \mathbb{Q}(\sqrt{3})$ olmak üzere $G(E/\mathbb{Q})$ şu şekilde belirlenir: Örnek 1.7.3'ten dolayı $G(E/\mathbb{Q}) = \{\psi_{\sqrt{3},\sqrt{3}}, \psi_{\sqrt{3},-\sqrt{3}}\}$ dir. O halde $G(E/\mathbb{Q})$, mertebesi iki olan devirli gruptur ve $E_{G(E/\mathbb{Q})} = \mathbb{Q}$ dur. E'nin $\mathbb{Q}$ ve kendisinden başka alt cismi ve $G(E/\mathbb{Q})$ nun birim ve kendisinden başka altgrubu yoktur.

**Örnek 1.7.5.** $E = \mathbb{Q}(\sqrt{3}\,,\ \sqrt{5})$ olmak üzere $G(E/\mathbb{Q})$ aşağıdaki gibi belirlenir.

$E = \mathbb{Q}(\sqrt{3}\,)(\sqrt{5})$ tür. $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$ olduğundan $\text{İnd}\left(\sqrt{5}, \mathbb{Q}\left(\sqrt{3}\,\right)\right) = x^2 - 5$ dir. $\sqrt{5}$ nin $\mathbb{Q}(\sqrt{5}\,)$ üzerindeki eşlenikleri $\sqrt{5}, -\sqrt{5}$ olduğundan $\mathbb{Q}(\sqrt{3}\,)$ yi sabit bırakan $\psi_{\sqrt{5},\sqrt{5}}\,, \psi_{\sqrt{5},-\sqrt{5}}$ otomorfizmaları vardır.

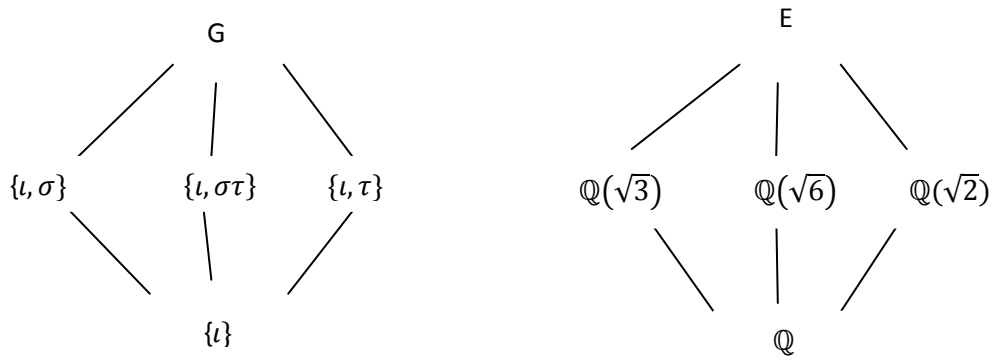
$\psi_{\sqrt{3},\sqrt{3}}\,, \psi_{\sqrt{3},-\sqrt{3}}, \psi_{\sqrt{5},\sqrt{5}}\,, \psi_{\sqrt{5},-\sqrt{5}}$

otomorfizmaları elde edilir. $\sigma_2 = \psi_{\sqrt{3},-\sqrt{3}}$ ve $\sigma_3 = \psi_{\sqrt{5},-\sqrt{5}}$ olsun. İki otomorfizmanın bileşkesi de otomorfizma olduğundan $\sigma_2\sigma_3$ bir otomorfizmadır.

$\{\iota_E, \sigma_2, \sigma_3, \sigma_2\sigma_3\} \subseteq G(E/\mathbb{Q})$ ..

$\sigma \in G(E/\mathbb{Q})$ olsun. Teorem 1.7.14'ten $\sigma$, $\sigma(\sqrt{2})$ ve $\sigma(\sqrt{3})$ değerleriyle tam olarak belirlenir. Sonuç 1.7.6'dan, $\sigma\left(\sqrt{2}\right) \in \{\sqrt{2}, -\sqrt{2}\}$ ve $\sigma\left(\sqrt{3}\right) \in \{\sqrt{3}, -\sqrt{3}\}$ olduğundan $\sigma$ dört farklı biçimde seçilebilir ve $G(E/\mathbb{Q}) = \{\iota_E, \sigma_2, \sigma_3, \sigma_2\sigma_3\}$ dir. Burada $\sigma = \sigma_2$ ve $\tau = \sigma_3$ konulursa $G(E/\mathbb{Q}) = \{\iota, \sigma, \tau, \sigma\tau\}$ olur. Üstelik $\sigma^2 = \tau^2 = \iota$ ve $\sigma\tau = \tau\sigma$ olduğundan dolayı $G(E/\mathbb{Q})$, mertebesi dört olan bir abelyan gruptur.

**Örnek 1.7.6.** Örnek 1.7.5'deki $G(E/\mathbb{Q})$ grubunun alt grupları ve bunların sabit cisimleri şu şekilde belirlenir: $G = G(E/\mathbb{Q})$ olsun. $G = \{\iota, \sigma, \tau, \sigma\tau\}$, $\sigma^2 = \tau^2 = \iota_E$ ve $\sigma\tau = \tau\sigma$ olduğundan G'nin alt grupları $G = \langle\iota\rangle$, $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\sigma\tau\rangle$ dur. $E_G = \mathbb{Q}$ ve $E_\iota = E$ dir. $\sigma\left(\sqrt{5}\right) = \sqrt{5}$ olduğundan $\mathbb{Q}(\sqrt{5}) \subseteq E_\sigma$ dır. Ayrıca $2 = \left[E : \mathbb{Q}\left(\sqrt{5}\right)\right] = [E : E_\sigma][E_\sigma : \mathbb{Q}\left(\sqrt{5}\right)]$ olduğundan $[E : E_\sigma] = 1$ ya da $[E : E_\sigma] = 2$ olmalıdır. Birinci durumda $E = E_\sigma$ olur. Fakat $\sigma\left(\sqrt{2}\right) = -\sqrt{2} \neq \sqrt{2}$ olduğundan bu çelişkidir. O halde $[E : E_\sigma] = 2$ olmalıdır. Buradan $\left[E_\sigma : \mathbb{Q}\left(\sqrt{3}\right)\right] = 1$ ve $E_\sigma = \mathbb{Q}\left(\sqrt{3}\right)$ bulunur. Benzer şekilde $E_\tau = \mathbb{Q}\left(\sqrt{2}\right)$ dir. $E_{\sigma\tau}$ için $\sigma\tau\left(\sqrt{6}\right) = \sigma\left(\tau\left(\sqrt{6}\right)\right) = \sigma\left(-\sqrt{6}\right) = \sqrt{6}$ olduğundan $\sqrt{6} \in E_{\sigma\tau}$ ve $\mathbb{Q}(\sqrt{6}) \subseteq E_{\sigma\tau}$ olur. $\left[E : \mathbb{Q}\left(\sqrt{6}\right)\right] = 2$ olduğundan $E_\sigma$ 'nın belirlenmesinde olduğu gibi, $\mathbb{Q}\left(\sqrt{6}\right) = E_{\sigma\tau}$ bulunur (Şekil 10(a-b)).




**(a)** **(b)**

**Şekil 10:** G'nin alt grup kafesi (a), E'nin alt cisim kafesi (b)

**Örnek 1.7.7.** $E = \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ cisminin aşağıdaki temel otomorfizmaları veriliyor.

$\psi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{3},\sqrt{5})(\sqrt{2}) \to \mathbb{Q}(\sqrt{3},\sqrt{5})(-\sqrt{2})$

$\psi_{\sqrt{3},-\sqrt{3}} : \mathbb{Q}(\sqrt{2},\sqrt{5})(\sqrt{3}) \to \mathbb{Q}(\sqrt{2},\sqrt{5})(-\sqrt{3})$

$\psi_{\sqrt{5},-\sqrt{5}} : \mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5}) \to \mathbb{Q}(\sqrt{2},\sqrt{3})(-\sqrt{5})$

$\tau_2 = \psi_{\sqrt{2},-\sqrt{2}}$, $\tau_3 = \psi_{\sqrt{3},-\sqrt{3}}$ ve $\tau_5 = \psi_{\sqrt{5},-\sqrt{5}}$ olmak üzere E'nin aşağıdaki elemanları aşağıdaki gibi hesaplanır.

(a) $\tau_2\tau_3(\sqrt{3}+\sqrt{10}) = \tau_2(\sqrt{3}-\sqrt{10}) = -\sqrt{3}-\sqrt{10}$

(b) $\tau_3[\tau_5(\sqrt{6}-\sqrt{15}) + \tau_2\tau_5(\sqrt{30}) = \tau_3[\sqrt{6}+\sqrt{15}+\tau_2(-\sqrt{30})] = \tau_3[\sqrt{6}+\sqrt{15}+\sqrt{30}] = -\sqrt{6}-\sqrt{15}-\sqrt{30}$

**Örnek 1.7.8.** Örnek 1.7.7'de verilen E cismi için $G(E/\mathbb{Q})$ grubu şu şekilde belirlenir: $E = \mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5})$ tür. $\sqrt{5} \notin \mathbb{Q}(\sqrt{2},\sqrt{3})$ olduğundan $\text{İnd}\left(\sqrt{5},\mathbb{Q}(\sqrt{2},\sqrt{3})\right) = x^2 - 5$ dir. $\sqrt{5}$ in $\mathbb{Q}(\sqrt{2},\sqrt{3})$ üzerinde eşlenikleri $\sqrt{5},-\sqrt{5}$ olduğundan $\mathbb{Q}(\sqrt{2},\sqrt{3})$ ü sabit bırakan $\psi_{\sqrt{5},\sqrt{5}}$, $\psi_{\sqrt{5},-\sqrt{5}}$ otomorfizmaları vardır. Örnek 1.7.7'de olduğu gibi $\mathbb{Q}(\sqrt{3})$ ü sabit bırakan $\psi_{\sqrt{2},\sqrt{2}}, \psi_{\sqrt{2},-\sqrt{2}}$, $\mathbb{Q}(\sqrt{2})$ ü sabit bırakan $\psi_{\sqrt{3},\sqrt{3}}$, $\psi_{\sqrt{3},-\sqrt{3}}$ otomorfizmaları vardır.

$\psi_{\sqrt{2},\sqrt{2}}, \psi_{\sqrt{2},-\sqrt{2}}, \psi_{\sqrt{3},\sqrt{3}}$, $\psi_{\sqrt{3},-\sqrt{3}}, \psi_{\sqrt{5},\sqrt{5}}, \psi_{\sqrt{5},-\sqrt{5}}$

otomorfizmaları elde edilir. $\tau_2 = \psi_{\sqrt{2},-\sqrt{2}},\ \tau_3 = \psi_{\sqrt{3},-\sqrt{3}}$ ve $\tau_5 = \psi_{\sqrt{5},-\sqrt{5}}$ olsun.

$G(E/\mathbb{Q}) = \{\iota_F, \tau_2, \tau_3, \tau_5, \tau_2\,\tau_3, \tau_2\tau_5, \tau_3\tau_5, \tau_2\tau_3\tau_5\}$

şeklinde bulunur.

**Örnek 1.7.9.** Örnek 1.7.7'de verilen E cismi için $\tau_2, \tau_3, \tau_2\tau_3\tau_5$ in sabit cisimleri şu şekilde belirlenir: $\tau_2$, $\mathbb{Q}(\sqrt{3},\sqrt{5})$ cismini sabit bırakır, $\tau_3$, $\mathbb{Q}(\sqrt{2},\sqrt{5})$ cismini sabit bırakır ve $\tau_2\tau_3\tau_5$, $\mathbb{Q}$ cismini sabit bırakır.

R değişmeli ve birimli bir halka olmak üzere binom teoremi sağlanır. $\forall a, b \in R$ ve $\forall n \geq 1$ için

$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{i}a^{n-i}b^i + \cdots + b^n.$

$n = p$ bir asal sayı ve $kar(R) = p$ olmak üzere $1 \leq i < p$ için

$\binom{p}{i} = \frac{p!}{i!(p-i)!}$

sayısı p ile bölünür; çünkü $i!$ ve $(p-i)!$ sayılarının çarpanları $< p$ olduğundan bu sayının paydası p ile bölünmez fakat payı p ile bölünür. $1 \leq i < p$ ve $r \in R$ için

$\binom{p}{i}r = 0_R$

Böylece $kar(R) = p$ iken binom teoreminden $(a+b)^p = a^p + b^p$ elde edilir.

**Teorem 1.7.16.** F bir cisim ve $kar(F) = p$ olmak üzere $\sigma_p : F \to F, a \longmapsto a^p$ şeklinde tanımlanan $\sigma_p$ fonksiyonu monomorfizmadır ve $\sigma_p$ nin sabit cismi $\mathbb{Z}_p$ ye izomorftur. F sonlu ise $\sigma_p$ bir otomorfizmadır.

**İspat.** Teoremden önceki açıklamadan dolayı $a, b \in F$ olmak üzere

$(a+b)^p = a^p + b^p$ ve $(ab)^p = a^p b^p$

olduğundan $\sigma_p$ halka homomorfizmasıdır. $a \in F$ için $a^p = 0_F$ olmak üzere F sıfır bölensiz olduğundan $a = 0_F$ ve $\sigma_p$ bire birdir. F sonlu ise $\sigma_p$ örten olduğundan bir otomorfizmadır. $\sigma_p$ nin sabit cismi E ve $a \in E$ olsun. $a^p = a$ olduğundan $a$ elemanı $1_F x^p - 1_F x = 0_F$ denkleminin bir köküdür. F cisim olduğundan bu denklemin F içinde

en çok p kökü vardır. Fermat teoreminden, her $0 \leq t < p$ için $t^p \equiv t(mod p)$ olduğundan F içinde, $t^p 1_F = t1_F$ dir. O halde $0.1_F,\ 1.1_F, \dots,\ (p-1).1_F,\ 1_F x^p - 1_F x = 0_F$ denkeleminin birbirinden farklı p kökü vardır. $E = \{0_F,\ 1.1_F, \dots,\ (p-1).1_F\}$ dir. $\varphi : \mathbb{Z} \to F, z \mapsto z1_F$ eşlemesi bir halka izomorfizmasıdır ve Ker(φ = pℤ dir. $\varphi(\mathbb{Z}) = E$ olduğundan $\mathbb{Z}/p\mathbb{Z} \cong E$ dir.

Teorem 1.7.16'da F cismi sonlu iken tanımlı $\sigma_p$ otomorfizmasına *Frobenius otomorfizması* denir.

**Örnek 1.7.10.** $p(x) = x^3 - x + \bar{1} \in \mathbb{Z}_3[x]$ polinomunun $\mathbb{Z}_3$ ün bir cebirsel genişlemesi içindeki bir kökü $u$ ve $E = \mathbb{Z}_3[u]$ olsun. $G(E/\mathbb{Z}_3) = \langle\sigma_3\rangle$ olduğu ve $w = \bar{1} + u + \bar{2}u^2$ elemanlarının bütün eşlenikleri aşağıda verilmiştir.

$p(x)$ in $\mathbb{Z}_3$ içinde hiçbir kökü olmadığından $\mathbb{Z}_3$ üzerinde indirgenmez ve $[E : \mathbb{Z}_3] = 3$ tür. $kar(\mathbb{Z}_3) = 3$ olduğundan E'nin $\sigma_3$ Frobenius otomorfizması tanımlıdır.

$\sigma_3(u) = u^3 - u + \bar{1} = \bar{0}, \sigma_3(u) = \ u^3 = u - \bar{1}$

$\sigma_3^2(u) = \sigma_3(u - \bar{1}) = u - \bar{1} - \bar{1} = u - \bar{2}$

$\sigma_3^3(u) = \sigma_3(u - \bar{2}) = u - \bar{2} - \bar{1} = u - \bar{3} = u - \bar{0} = u,\ \ \sigma_3^3(u) = u$

$\sigma_3$ nun mertebesi 3 tür ve $u$'nun eşlenikleri $u, u - \bar{1}, u\ - \bar{2}$ olup E'ye aittir. Dolayısıyla Sonuç 1.7.4 gereğince, E'nin bütün otomorfizmaları $\sigma_3$ ün kuvvetlerinden oluşur ve $G(E/\mathbb{Z}_3) = \langle\sigma_3\rangle$ dir.

$w = \bar{1} + u + \bar{2}u^2$ için;

$\sigma_3(w) = w - \bar{1} = \bar{1} + u + \bar{2}u^2 - \bar{1} = u + \bar{2}u^2$

$\sigma_3^2(w) = \sigma_3(w - \bar{1}) = w - \bar{2} = \bar{1} + u + \bar{2}u^2 - \bar{2} = u + \bar{2}u^2 - \bar{1}$

$\sigma_3^3(w) = w = \bar{1} + u + \bar{2}u^2$

olduğundan $w = \bar{1} + u + \bar{2}u^2$'nin bütün eşlenikleri $\bar{1} + u + \bar{2}u^2, u + \bar{2}u^2, u + \bar{2}u^2 - \bar{1}$ dir.

## 1.8. Parçalanma Cisimleri ve Normal Genişlemeler

**Tanım 1.8.1.** F bir cisim, $f(x) \in F[x]$ sabit olmayan bir polinom ve $F \leq E$ olsun. $f(x)$, $E[x]$ içinde lineer çarpanlarına ayrılırsa; yani $a \in F$ ve $u_1, u_2, \dots, u_n \in E$ olmak üzere

$$f(x) = a(x-u_1)(x-u_2)\dots(x-u_n)$$

olarak yazılabilirse $f(x)$, *E üzerinde parçalanır* denir. $F(u_1, u_2, \dots, u_n) = K$ ise K'ya, $f(x)$ in F *üzerinde bir parçalanma cismi* denir.

**Örnek 1.8.1.** $\mathbb{Q}(\sqrt{3})$, $x^2-3 \in \mathbb{Q}[x]$ ve $\mathbb{C} = \mathbb{R}(i)$, $x^2+1 \in \mathbb{Q}[x]$ polinomunun $\mathbb{Q}$ üzerinde ki parçalanma cismidir.

**Örnek 1.8.2.** $\mathbb{Q}(\sqrt{2},\sqrt{3})$ cisminin $x^4+2x^3-8x^2-6x-1$ polinomunun $\mathbb{Q}$ üzerindeki parçalanma cismi şu şekilde gösterilir: $x^4+2x^3-8x^2-6x-1$ in kökleri $\pm\sqrt{2}$, $\pm\sqrt{3}$ olursa polinomun $\mathbb{Q}$ üzerindeki parçalanma cismi $\mathbb{Q}(\sqrt{2},\sqrt{3})$ olur.

$$\begin{aligned} x^4+2x^3-8x^2-6x-1 &= (ax^2+bx+c)(dx^2+ex+f) \\ &= adx^4+(ae+bd)x^3+(af+dc+be)x^2+(bf+ce)x+cf \end{aligned}$$

$ad=1, ae+bd=2, af+dc+be=-8, bf+ce=-6, cf=-1$ eşitlikleri elde edilir. Buradan $a=d=c=1, f=-1, b=4$ ve $e=-2$ bulunur.

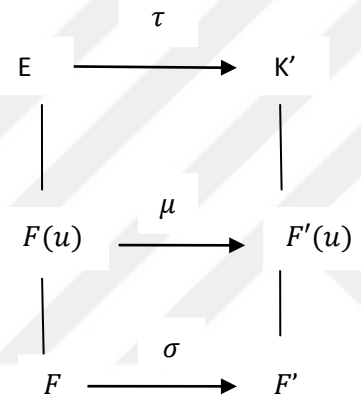
$x^4+2x^3-8x^2-6x-1 = (x^2+4x+1)(x^2-2x-1)$ olarak çarpanlarına ayrılır. $x^2+4x+1$'nin kökleri $1\pm\sqrt{2}$, $x^2-2x-1$ nin kökleri $-2\pm\sqrt{6}$ ve $1\pm\sqrt{2}$, $-2\pm\sqrt{6} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ olduğundan $\mathbb{Q}(\sqrt{2},\sqrt{3})$ parçalanma cismidir.

**Teorem 1.8.2.** $f(x) \in F[x]$ sabit olmayan bir polinom olmak üzere $f(x)$ in F üzerinde bir parçalanma cismi K vardır ve $[K : F] \leq n!$ dir.

**İspat.** $der\big(f(x)\big) = n$ üzerine tümevarım uygulanır. $n=1$ ise $f(x)$ in tek kökü vardır ve F'ye aittir ve $K=F$ dir. $1 \leq k < n$ dereceli polinomlar için sağlansın. Teorem 1.4.16 ve Teorem 1.3.27'den F'nin $p(x)$ in bir kökü olan $F(u)$ genişlemesi vardır ve $f(x) = (x-u)g(x)$ olacak biçimde $g(x) \in F(u)[x]$ vardır ve $der\big(g(x)\big) \leq n-1$'dir. Tümevarım $g(x)$ in $F(u)$ üzerinde bir parçalanma cismi K vardır ve $[K :$

$F(u)] \leq (n-1)!$ dir. $c \in F(u), u_1,\ u_2, \dots, u_{n-1} \in K$ olmak üzere $g(x) = c(x-u_1)(x-u_2)\dots(x-u_{n-1})$ dir. $g(x)$ in değeri $f(x)$ te yerine K üzerinde parçalanır. $K = F(u)(u_1,\ u_2, \dots, u_{n-1}) = f(u, u_1,\ u_2, \dots, u_{n-1})$ olduğundan K, $f(x)$ in F üzerindeki bir parçalanma cismidir. $[F(u) : F] \leq der(u, F) \leq n$ olduğundan $[K : F] = [K : F(u)][F(u) : F] \leq (n-1)!\, n = n!$ dir.

**Teorem 1.8.3.** $\sigma : F \to F'$ bir cisim izomorfizması ve $f(x) \in F[x]$ sabit olmayan bir polinom olmak üzere $f(x)$ in F üzerindeki bir parçalanma cismi K ve $\sigma^*\big(f(x)\big)$ in $F'$ üzerindeki bir parçalanma cismi $K'$ olsun. $\sigma$, K'dan $K'$ ne bir $\tau$ izomorfizmasına genişler.




**Şekil 11.** Teorem 1.8.3'te tanımlı izomorfizma genişlemesi

**İspat.** $der\big(f(x)\big) = n$ üzerinde tümevarım uygulanır. $n = 1$ olursa $f(x)$ ve $\sigma^*\big(f(x)\big)$ lineer polinomlar olduğundan $f(x)$ in parçalanma cismi F ve $\sigma^*\big(f(x)\big)$ 'in parçalanma cismi $F'$ dür ve $\sigma = \tau$ dir. Şimdi ise $1 < k < n$ dereceli polinomlar için doğru olsun. Teorem 1.3.27'den ve Lemma 1.7.3'ten dolayı $\sigma^*\big(f(x)\big), F'$ üzerinde indirgenmezdir ve $\sigma^*\big(f(x)\big)$ in bir çarpanıdır. $f(x)$, K üzerinde parçalandığından, K içindeki bir kökü $u$ ve $\sigma^*\big(f(x)\big)$ in $K'$ içindeki bir kökü $v$ olsun. Teorem 1.7.4'ten $F(u)$ dan $F'(v)$ ye $u$'yu $v$'ye götüren bir $\mu$ izomorfizması vardır. $\mu(u) = v$ ve $\mu|_F = \sigma$ dır (Şekil 11). Diğer taraftan $f(x) = (x-u)t(x)$ olacak şekilde $t(x) \in F(u)[x]$ vardır. Bu eşitliğe $\mu^*\big(f(x)\big) = (x-v)\mu^*\big(t(x)\big)$ olur.

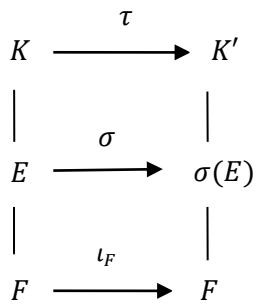
$K$ ve $K'$, sırasıyla, $t(x)$ ve $\mu^*\big(t(x)\big)$ in $F(u)$ ve $F(v)$ üzerindeki parçalanma cisimleridir ve $der\big(t(x)\big) = der\left(\mu^*\big(t(x)\big)\right) = n-1$ dir. O halde $\tau : K \to K'$ izomorfizması için $\tau|_{F(u)} = \mu$ dur ve $\mu|_F = \sigma$ olduğundan $\tau|_F = \sigma$ dır.

**Sonuç 1.8.4.** $f(x) \in F[x]$ sabit olmayan bir polinom olmak üzere $f(x)$'in F üzerinde tanımlı olan herhangi iki parçalanma cismi F'yi sabit bırakan izomorfizma adı altında izomorftur.

**İspat.** $f(x)$ in F üzerinde iki parçalanma cismi $K, K'$ ve $\iota_E$, $F$'nin birim otomorfizması olsun. Teorem 1.8.3'te $F = F'$ ve $\iota_F = \sigma$ yazılırsa $K', \iota_F^*\big(f(x)\big) = f(x)$ in $\iota_F(F) = F$ üzerindeki parçalanma cismi olacağından öyle bir $\tau : K \to K'$ izomorfizması vardır ki $\tau|_F = \iota_F$ dir.

**Sonuç 1.8.5.** $F \leq E \leq K$ bir cisim kulesi ve K, bir $f(x) \in F[x]$ polinomunun F üzerindeki parçalanma cismi olmak üzere E'den K içine tanımlı her F monomorfizması K'nın bir otomorfizmasına genişler.

**İspat.** $\sigma : E \to K$ bir F monomorfizması olsun. $\sigma : E \to \sigma(E)$ bir izomorfizma olduğundan $\sigma(E)$, K nın bir alt cismidir ve $\sigma|_F = \iota_F$ olduğundan $F \leq \sigma(E)$ dir. Bu durumda $f(x) = \iota_F^*\big(f(x)\big) = \sigma^*\big(f(x)\big)$ olduğundan K, $f(x)$ in E ve $\sigma(E)$ üzerindeki parçalanma cismidir. Sonuç 1.8.4'den öyle bir $\tau : K \to K$ otomorfizması vardır ki $\tau|_E = \sigma$ dır. $\tau|_F = \sigma|_E = \iota_F$ olduğundan $\tau$, F'yi sabit bırakır (Şekil 12).




**Şekil 12.** Sonuç 1.8.5'te tanımlı otomorfizma genişlemesi

**Teorem 1.8.6.** $F \leq K \leq L$ bir cisim kulesi ve $f(x) \in F[x]$ polinomunun F üzerindeki parçalanma cismi K olmak üzere K'den L'ye tanımlı ve F'yi sabit bırakan her monomorfizma K'nin bir otomorfizmasıdır.

**İspat.** $f(x)$ in K içindeki bütün kökleri $u_1,\ u_2, \dots, u_n$ olmak üzere $K = F(u_1,\ u_2, \dots, u_n)$ ve $a \in K$ için

$f(x) = a(x - u_1)(x - u_2) \dots (x - u_n)$.

$\tau : K \to L$ bir monomorfizma ve $\tau|_F = \iota_F$ olmak üzere $\tau^*\big(f(x)\big) = f(x)$ ve

$\tau^*\big(f(x)\big) = \tau(a)(x - \tau(u_1))\big(x - \tau(u_2)\big) \dots (x - \tau(u_n))$

olduğundan $\tau(u_1), \tau(u_2), \dots, \tau(u_n)$ $f(x)$'in kökleridir. $u_i \neq u_j$ iken $\tau(u_i) \neq \tau(u_j)$ dir. O halde $\{\tau(u_1), \tau(u_2), \dots, \tau(u_n)\} = \{u_1,\ u_2, \dots, u_n\}$ ve $K = F(u_1,\ u_2, \dots, u_n) \leq \tau(K)$ dır. Diğer taraftan $\tau$ bir cisim otomorfizması ve $\tau|_F = \iota_F$ olduğundan bir vektör uzayı izomorfizmasıdır. O halde $boy_F(K) = boy_F\tau(K)$; yani $[K : F] = [\tau(K) : F]$ dir. $[\tau(K) : F] = [\tau(K) : K][K : F]$ ve $[K : F] < \infty$ olduğundan $[\tau(K) : K] = 1$ ve $\tau(K) = K$ bulunur.

**Teorem 1.8.7.** F bir cisim ve $f(x) \in F[x]$ sabit olmayan polinomunun parçalanma cismi K olsun. $f(x)$ in K içindeki birbirinden farklı kökleri $u_1,\ u_2, \dots, u_k$ olmak üzere $G(K/F)$, $Sym(\{u_1,\ u_2, \dots, u_k\})$ nın bir alt grubuna izomorftur ve $|G(K/F)|\big|k!$ dir.

**İspat.** $c \in F$ ve $m_1,\ m_2, \dots, m_k$ pozitif tam sayılar olmak üzere $f(x) = c(x - u_1)^{m_1}(x - u_2)^{m_2} \dots (x - u_k)^{m_k}$ olsun. $\sigma \in G(E/F)$ olmak üzere $\sigma^*\big(f(x)\big) = c(x - \sigma(u_1))^{m_1}(x - \sigma(u_2))^{m_2} \dots (x - \sigma(u_k))^{m_k}$ olduğundan $\sigma(u_1),\ \sigma(u_2), \dots, \sigma(u_k)$ elemanları da $f(x)$ in K içindeki birbirinden farklı kökleridir. O halde $\{\sigma(u_1), \sigma(u_2), \dots, \sigma(u_k)\} = \{u_1,\ u_2, \dots, u_k\}$ dır. Teorem 1.7.14 ve Sonuç 1.8.15 gereğince $G(K/F),\ Sym(u_1,\ u_2, \dots, u_k)$ nın bir alt grubuna izomorftur ve $|G(K/F)|\big|k!$ dir.

**Örnek 1.8.3.** $(x^2 - 5)(x^2 - 7)$ polinomunun $\mathbb{Q}$ üzerindeki parçalanma cismi K ve $G(K/\mathbb{Q})$ aşağıdaki gibi belirlenir.

$(x^2 - 5)(x^2 - 7) \in \mathbb{Q}[x]$ polinomunun $\mathbb{Q}$ üzerindeki parçalanma cismi $\mathbb{Q}\big(\sqrt{5}, \sqrt{7}\big)$ dir. $\mathbb{Q}\big(\sqrt{5}, \sqrt{7}\big) = K$ dır. $İnd\big(\sqrt{5}, \mathbb{Q}\big) = x^2 - 5$ olduğundan $\mathbb{Q}\big(\sqrt{5}\big)$ nin bir $\mathbb{Q}$-bazı

$\{1, \sqrt{5}\}$, $\text{İnd}(\sqrt{7}, \mathbb{Q}) = x^2 - 7$ olduğundan $\mathbb{Q}(\sqrt{7})$ nin bir $\mathbb{Q}$-bazı $\{1, \sqrt{7}\}$ dir. Dolayısıyla K'nın bir $\mathbb{Q}$-bazı $\{1, \sqrt{5}, \sqrt{7}, \sqrt{35}\}$ ve buradan $[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = [K : \mathbb{Q}] = 4$ tür. Örnek 1.7.7'den dolayı $\mathbb{Q}(\sqrt{5})$ i sabit bırakan $\psi_{\sqrt{7},\sqrt{7}}$, $\sigma_2 = \psi_{\sqrt{7},-\sqrt{7}}$, $\mathbb{Q}(\sqrt{7})$ i sabit bırakan $\psi_{\sqrt{5},\sqrt{5}}$, $\sigma_3 = \psi_{\sqrt{5},-\sqrt{5}}$ otomorfizmaları vardır. O halde $G(K/\mathbb{Q}) = \{\iota_E, \sigma_2, \sigma_3, \sigma_2\sigma_3\}$ dir.

**Örnek 1.8.4.** $x^4 - 1$ polinomunun $\mathbb{Q}$ üzerindeki parçalanma cismi K ve $G(K/\mathbb{Q})$ aşağıdaki gibi belirlenir.

$x^4 - 1 \in \mathbb{Q}[x]$ denkleminin kökleri $z_k = \cos\frac{2\pi k}{4} + i \sin\frac{2\pi k}{4}, k = 0, 1, 2, 3$ eşitlikleriyle verilir. $w = z_1$ olsun. O zaman her $k \geq 0$ için $w^k = z_k$ olacağından $K = \mathbb{Q}(w)$ dir. $x^4 - 1 = (x-1)(x+1)(x^2+1), \phi_4(x) = (x^2+1)$ indirgenmez olduğundan $\text{İnd}(w, \mathbb{Q}) = x^2 + 1 = \phi_4(x)$ dir. Dolayısıyla $[K : \mathbb{Q}] = 2$ dir ve $w$'nun $\mathbb{Q}$ eşlenikleri $w^2$, $w^3$, $w^4$ tür. Bütün otomorfizmalar $\iota_\phi, \psi_{w,w^2}, \psi_{w,w^3}, \psi_{w,w^4}$ temel otomorfizmalarından oluşur. $\psi_{w,w^2} = \sigma, \sigma(w) = w^2, \sigma^2(w) = w^4, \sigma^3(w) = w^3$ olduğundan $o(\sigma) = 4$, $G(K/\mathbb{Q}) = \langle\sigma\rangle$ ve $|G(K/\mathbb{Q})| = 4$ tür. $|G(K/\mathbb{Q})| \neq [K : \mathbb{Q}]$ dır.

**Teorem 1.8.8.** F bir cisim $f(x) \in F[x]$ olmak üzere $f(x)$ in F üzerindeki bir parçalanma cismi K ve $p(x)$, $F[x]$ in bir indirgenmez polinomu olsun. $p(x)$ in K içinde bir sıfırı varsa $p(x)$, K üzerinde parçalanır.

**İspat.** $p(x)$ in K içindeki bir kökü $u$ ve $F \leq K$ olduğundan $p(x) \in K[x]$ tir. $p(x)$ in K üzerindeki bir parçalanma cismi L ve L içindeki herhangi bir kökü $v$ olmak üzere Sonuç 1.7.6'dan $\psi_{u,v} : F(u) \to F(v)$ temel izomorfizması vardır. $\tau = \psi_{u,v}$ ve $\tau(u) = v$ ve $\tau|_F = \iota_F$ dir. Diğer taraftan K, F üzerinde $f(x)$ in parçalanma cismi olduğundan $K(u)$, $F(u)$ üzerinde ve $K(v)$, $F(v)$ üzerinde $f(x)$ in parçalanma cismidir. $\tau^*(f(x)) = f(x)$ olduğundan $K(v)$, $F(v)$ üzerinde $f(x)$ in parçalanma cismidir. O halde Teorem 1.8.3'den $\tau$, $K(u)$ dan $K(v)$ ye bir $\mu$ izomorfizmasına genişler. Ayrıca $\mu|_F = \tau|_F = \iota_F$ olduğundan $\mu$, F yi sabit bırakır ve $\mu$, K'dan L'ye bir F monomorfizması olduğundan Teorem 1.8.6'dan $\mu|_K$, K'nın bir F-otomorfizmasıdır. Buradan $v = \tau(u) = \mu(u) \in K$ ve $v \in K$ olur. O halde $p(x)$, K üzerinde parçalanır.

**Tanım 1.8.9.** F bir cisim ve E, F'nin bir cebirsel genişlemesi olmak üzere E içinde bir kökü olan her $p(x) \in F[x]$ indirgenmez polinomu E üzerinde parçalanırsa E'ye F'nin bir *normal genişlemesi* denir.

**Teorem 1.8.10.** F bir cisim ve E, F'nin bir cebirsel cisim genişlemesi olmak üzere E'nin F'nin bir normal genişlemesi olması için gerek ve yeter şart E'nin F üzerinde bir $f(x) \in F[x]$ polinomunun parçalanma cismi olmasıdır.

**İspat.** E, F üzerinde bir $f(x) \in F[x]$ polinomunun parçalanma cismi olsun. Teorem 1.8.8'den $F[x]$ in E içinde bir kökü olan her indirgenemez polinomu E üzerinde parçalandığından E, F'nin bir normal genişlemesidir.

Tersine E, F'nin bir normal genişlemesi olsun. $[E : F]$ sonlu olduğundan Teorem 1.5.6'dan $E = F(u_1, u_2, \dots, u_r)$ olacak şekilde E'nin $u_1, u_2, \dots, u_r$ cebirsel elemanları vardır. $\forall i = 1, 2, \dots, r$ için $p_i(x) = \text{İ}nd(u_i, F)$ ve $f(x) = p_1(x)p_2(x) \dots p_r(x)$ ve $f(x) \in F[x]$ tir. E, F'nin bir normal genişlemesi ve $\forall i = 1, 2, \dots, r$ için $p_i(u_i) = 0_F$ olduğundan $p_i(x)$, E üzerinde parçalanır. O halde $f(x)$, E üzerinde parçalanır. $f(x)$ in E içindeki parçalanma cismi K olsun. $F \cup \{u_1, u_2, \dots, u_r\} \subseteq K$ olduğundan $E = F(u_1, u_2, \dots, u_r) \subseteq K$ dır, yani $E = K$ dır.

**Teorem 1.8.11.** $F \leq E \leq K$ bir cisim kulesi ve K, F'nin bir sonlu normal genişlemesi olsmak üzere E'den K içine tanımlı F monomorfizmalarının sayısı $\leq [E : F]$ dir. Bu monomorfizmaların sayısı yalnız E ve F'ye bağlıdır.

**İspat.** E'den K'ya tanımlı F monomorfizmalarının sayısının $\leq [E : F]$ için $[K : F] = n$ olacak şekilde bir $n \geq 1$ tamsayısı vardır ve Teorem 1.8.10'dan K, F üzerinde bir $f(x) \in F[x]$ polinomunun parçalanma cismidir. n üzerine tümevarım uygulanır. $n = 1$ için iddia açıktır. $1 < k < n$ dereceli olan normal genişlemeler için sağlansın. $u \in E/F$ olmak üzere $[F(u):F] \geq 2$ olduğundan $[E : F(u)] < n$ dir. Ayrıca K, $F(u)$ nun bir normal genişlemesi olduğundan, hipotezden dolayı, E'den K'ya tanımlı $F(u)$ monomorfizmalarının sayısı $\leq [E : F(u)]$ dur.

$F(u)$ dan K içine tanımlı bir F-monomorfizması $\sigma$ ve $\tau_1, \tau_2, \dots, \tau_s, \sigma$'nun E'den K'ya tanımlı s genişlemesi olsun. Sonuç 1.8.5'ten $\forall \tau_i$, K'nın bir $\overline{\tau_\iota}$ otomorfizmasına genişler. $\forall 1 \leq i \leq s$ için K'nın $(\overline{\tau_1})^{-1}\overline{\tau_\iota}$ otomotrifzması dikkate alınırsa $\overline{\tau_1}|_{F(u)} = \sigma$ ve $\overline{\tau_\iota}|_{F(u)} = \sigma$ olduğundan $\overline{\tau_1}(u) = \overline{\tau_\iota}(u)$ ve buradan

$(\overline{\tau_1})^{-1}\overline{\tau_i}(u) = u$ 'dur. $(\overline{\tau_1})^{-1}\overline{\tau_i}|_E$ , E'den K'ya tanımlı ve $F(u)$ yu sabit bırakan bir monomorfizmadır. Ayrıca $i \neq j$ için $\tau_i \neq \tau_j$ olduğundan $(\overline{\tau_1})^{-1}\overline{\tau_i}|_E$ monomorfizmalarının sayısı s dir. İddia $F(u) \leq E$ genişlemesi için doğru olduğundan, $s \leq [E : F(u)]$ dur. O halde $\sigma$'nun E'den K'ya tanımlı genişlemelerinin sayısı $\leq [E : F(u)]$ dur.

Sonuç 1.7.5'ten, $F(u)$ dan K içine tanımlı F monomorfizmalarının sayısı $\leq [F(u) : F]$ olduğundan $F(u)$ dan K'ya tanımlı F monomorfizmalarının E'ye genişlemelerinin sayısı $\leq [E : F(u)][F(u) : F] = [\, E : F]$ dir. E'den K'ya tanımlı her F monomorfizmasının $F(u)$ dan K'ya tanımlı bir F monomorfizmasının E'ye genişlemesidir. O halde E'den K'ya tanımlı F-monomorfizmalarının sayısı $[\, E : F]$ den küçük veya eşittir.

L, F'nin bir sonlu normal genişlemesi ve $F \leq E \leq L$ olmak üzere L, F üzerinde bir $g(x) \in F[x]$ in parçalanma cismidir. $h(x) = f(x)g(x)$ ve $h(x)$ in F üzerindeki bir parçalanma cismi M olsun. M içinde $f(x)$ in ve $g(x)$ in parçalanma cisimleri, sırasıyla, $K'$ ve $L'$ olsun. Teorem 1.8.3'ten K'dan $K'$ ne ve L'den $L'$ ne birer F izomorfizması tanımlıdır. O halde $K = K'$ ve $L = L'$ olsun. E'den K'ya tanımlı bir F monomorfizması $\sigma$ olsun. Sonuç 1.8.5'ten $\sigma$, M'nin bir $\tau$ otomorfizmasına genişler. Teorem 1.8.6'dan $\tau|_L$, L'nin bir F otomorfizması olduğundan $\tau|_E = \sigma$, E'den L'ye bir F monomorfizmasıdır. O halde E'den K'ya tanımlı F monomorfizmalarının sayısı E'den L'ye tanımlı F monomorfizmalarının sayısından küçük veya eşittir. K yerine L alınırsa bunun karşıtı da doğru olur ve eşitlik sağlanır. O halde E'den K'ya tanımlı F monomorfizmalarının sayısı yalnız F ve E'ye bağlıdır (K'dan bağımsızdır).

**Tanım 1.8.12.** $F \leq E \leq K$ bir cisim kulesi ve K, F'nin bir sonlu normal genişlemesi olmak üzere E'den K'ya tanımlı F-monomorfizmalarının sayısına E'nin F üzerindeki *indeksi* denir ve $\{E : F\}$ ile gösterilir.

**Teorem 1.8.13.** K, F'nin bir sonlu cisim genişlemesi ve $F \leq E \leq K$ olmak üzere $\{K : E\}\{E : F\} = \{K : F\}$ dir.

**İspat.** F'nin K'yı içeren bir sonlu normal genişlemesi L olmak üzere Teorem 1.8.11'den E'den L'ye tanımlı F monomorfizmalarının sayısı sonludur ve bu monomorfizmalar $\sigma_1,\ \sigma_2, \dots ,\ \sigma_s$ olsun. Benzer şekilde K'dan L'ye tanımlı E monomorfizmalarının sayısı

da sonludur, bu monomorfizmalar da $\tau_1,\ \tau_2, \dots ,\ \tau_t$ olsun. Tanım 1.8.12'den $\{E : F\} = s$ ve $\{K : E\} = t$ dir. Sonuç 1.8.4'ten her $\sigma_i$, L'nin bir F otomorfizması $\overline{\sigma_i}$ ye ve her $\tau_j$, L'nin bir E-otomorfizması $\overline{\tau_j}$ ye genişler. Her $1 \le i \le s$ ve her $1 \le j \le t$ için $\overline{\varphi_{ij}} = \overline{\sigma_i} \circ \overline{\tau_j}$ olsun. $\overline{\varphi_{ij}}$ , L'nin bir F-otomorfizması olduğundan $\varphi_{ij} = \overline{\varphi_{ij}}\big|_K$, K'dan L içine tanımlı bir F-monomorfizmasdır. $\varphi_{ij}$ lerin sayısının $st$ olduğu gösterilir. $1 \le i,\ u \le s$ ve $1 \le j,\ v \le t$ için $\varphi_{ij} = \varphi_{uv}$ olmak üzere

$$\overline{\varphi_{ij}}\big|_K = \overline{\varphi_{uv}}|_K \Longrightarrow \overline{\sigma_i} \circ \overline{\tau_j}\big|_K = \overline{\sigma_u} \circ \overline{\tau_v}|_K$$
$$\Longrightarrow \overline{\sigma_i} \circ \overline{\tau_j}\big|_E = \overline{\sigma_u} \circ \overline{\tau_v}|_E$$
$$\Longrightarrow \sigma_i = \sigma_u$$
$$\Longrightarrow i = u$$

dur; $\overline{\tau_j}\big|_E = \overline{\tau_v}|_E = \iota|_E$ dir. $\overline{\sigma_i} = \overline{\sigma_u}$ ve $\overline{\sigma_i}$ ler birebir olduğundan

$$\overline{\sigma_i} \circ \overline{\tau_j}\big|_K = \overline{\sigma_i} \circ \overline{\tau_v}|_K \Longrightarrow \overline{\tau_j}\big|_K = \overline{\tau_v}|_K \Longrightarrow \tau_j = \tau_v \Longrightarrow j = v$$

dir. O halde $(i,j) \neq (u,v)$ iken $\varphi_{ij} \neq \varphi_{uv}$ dir ve $\varphi_{ij}$ lerin sayısı $st$ olduğundan $st \le \{K : F\}$ dir.

Tersine $\varphi : K \to L$ bir F-monomorfizması ise $\varphi$'nin bir $\varphi_{ij}$ 'ye eşit olduğu gösterilir ve $\{K : F\} \le st$ olduğundan $\{K : F\} = st$ olur ve ispat tamamlanır.

**Teorem 1.8.14.** F bir cisim ve E, F'nin bir sonlu cisim genişlemesi olmak üzere E, F'nin bir normal genişlemesi olması için gerek ve yeter şart $\{E : F\} = |G(E/F)|$ dir.

**İspat.** E, F'nin bir sonlu normal genişlemesi olduğundan Tanım 1.8.12 gereğince, E'den E'ye tanımlı F monomorfizmalarının sayısı $\{E : F\}$ dir. Diğer taraftan Teorem 1.8.6'dan, E'den E'ye tanımlı her F monomorfizması E'nin bir F otomorfizması olduğundan $\{E : F\} = |G(E/F)|$ dir.

Tersine $\{E : F\} = |G(E/F)|$ ve E, F'nin bir normal genişlemesi olmasın. E, F'nin bir sonlu genişlemesi olduğundan E'nin F'yi içeren bir sonlu normal genişlemesi L vardır ve $E \neq L$ dir. Teorem 1.8.8 ve Teorem 1.8.10'dan öyle bir $u \in E/F$ vardır ki, $\text{İ}nd(u,F)$, E üzerinde parçalanmaz. $\text{İ}nd(u,F)$, L üzerinde parçalandığından $u$'nun $L/E$ içinde eşleneği vardır. Bu eşlenik $v$ olsun. Sonuç 1.7.5'ten dolayı $F(u)$ dan $F(v)$ ye,

$u$'yu $v$'ye eşleyen bir $\psi_{u,v}$ değer homomorfizması tanımlıdır. Sonuç 1.8.5'ten $\psi_{u,v}$ , L'nin bir $\mu$ otomorfizmasına genişler ve $\mu|_E$, E'den L içine tanımlı bir F-monomorfizmasıdır. $\{E : F\} = |G(E/F)|$ olduğundan $\mu|_E$, E'nin bir otomorfizmasıdır ve $\mu(u) \in E$ dir. Ancak $\mu(u) = \psi_{u,v}(u) = v$ olduğundan $v \in E$ olur ki, bu bir çelişkidir. O halde $E = L$ ve E, F'nin bir normal genişlemesidir.

**Örnek 1.8.5.** $K = \mathbb{Q}(\sqrt[3]{2},\ \sqrt{3}, i)$ nin $\mathbb{Q}$ üzerinde bir parçalanma cismidir. $E = \mathbb{Q}(\sqrt[3]{2}, i)$ olduğuna göre $\{E : \mathbb{Q}\}$ ve $\{K : E\}$ indekslerini aşağıdaki gibi belirlenir.

$x^3 - 2 \in \mathbb{Q}[x]$ in $\mathbb{Q}$ üzerindeki parçalanma cismi $\mathbb{Q}(\sqrt[3]{2})$, $x^2 - 3 \in \mathbb{Q}[x]$ in $\mathbb{Q}$ üzerindeki parçalanma cismi $\mathbb{Q}(\sqrt{3})$, $x^2 + 1 \in \mathbb{Q}[x]$ in $\mathbb{Q}$ üzerindeki parçalanma cismi $\mathbb{Q}(i)$ olmak üzere $(x^3 - 2)(x^2 - 3)(x^2 + 1) \in \mathbb{Q}[x]$ polinomunun kökleri $\pm i, \pm\sqrt{3}, \pm\sqrt[3]{2}$ olduğundan $\mathbb{Q}(\pm i, \pm\sqrt{3}, \pm\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2},\ \sqrt{3}, i)$ parçalanma cismidir.

E, $\mathbb{Q}$ üzerinde parçalanma cismi olduğundan E, $\mathbb{Q}$'nun normal genişlemesidir. $F = \mathbb{Q}(\sqrt[3]{2})$ olsun. $\{E : \mathbb{Q}\} = \{E : F\}\{F : \mathbb{Q}\}$ dır. $\{E : F\} = 2$ ve $\{F : \mathbb{Q}\} = 3$ dür. O halde $\{E : \mathbb{Q}\} = 2 \times 3 = 6$ dır. K, $\mathbb{Q}$ üzerinde parçalanma cismi olduğundan K, $\mathbb{Q}$'nun normal genişlemesidir. $\{K : \mathbb{Q}\} = \{K : E\}\{E : \mathbb{Q}\}$ ve $\{K : \mathbb{Q}\} = 12$ olduğundan $12 = \{K : E\} \times 6$ ise $\{K : E\} = 2$ dir.

## 1.9. Ayrılabilir Genişlemeler

**Tanım 1.9.1.** $f(x) \in F[x]$ olsun. $f(u) = 0$ olacak şekilde bir $u$ elemanı vardır. $(x - u)^s$, $f(x)$ in bir çarpanı olacak şekilde s en büyük tamsayı ise $u, f(x)$ in çok katlı bir sıfırıdır.

**Teorem 1.9.2.** $f(x) \in F[x]$ ve $f(u) = 0$ olacak şekilde bir $u$ elemanı vardır. $u$'nun çok katlı kök olması için gerek ve yeter şart $f'(x)$ in bir kökü olmasıdır.

**İspat.** K, $f(x)$ in $u$'yu içeren bir parçalanma cismi olsun.

$u, f(x)$ in çok katlı bir kökü olmak üzere

$$f(x) = (x - u)^s g(x)$$

olacak şekilde $g(x) \in K[x]$ ve $s \geq 2$ tamsayısı vardır. İki tarafa türev uygulandığında

$f'(x) = s(x-u)^{s-1}g(x) + (x-u)^s g'(x).$

İki tarafa da değer homomorfizması $\phi_u$ uygulandığında

$f'(u) = s(u-u)^{s-1}g(u) + (u-u)^s g'(u) = 0_F.$

Tersine $f(x)$ ve $f'(x)$ in ortak kökü $u$ olsun. $f(x) = (x-u)h(x)$ olacak şekilde $h(x) \in K[x]$ vardır. Her iki tarafa türev uygulanırsa

$f'(x) = h(x) + (x-u)h'(x).$

Buradan $f'(u) = 0_F$ olduğundan

$0_F = h(u) + (u-u)h'(u) = h(u).$

$h(x) = (x-u)t(x)$ olacak şekilde $t(x) \in K[x]$ vardır. Yerine yazıldığında $f(x) = (x-u)^2 t(x)$ olduğundan $u$ çokkatlı köktür.

**Teorem 1.9.3.** K, $p(x) \in F[x]$ indirgenmez polinomunun F üzerindeki parçalanma cismi olmak üzere

(i) $kar(F) = 0_F$ ise $p(x)$ in K içindeki her kökü basit köktür.

(ii) $kar(F) = p$ ise $p(x)$ in çok katlı kök olması için gerek ve yeter şart $p(x) = q(x^p)$ olacak şeklinde bir $q(x) \in F[x]$ olmasıdır.

**İspat.** $u \in K$, $p(x)$ in çok katlı kökü olmak üzere Teorem 1.9.2'den $u$, $p'(x)$ in bir kökü olduğundan $(x-u)$ hem $p(x)$ i ve hem de $p'(x)$ i böler. Teorem 1.3.28'den dolayı $p(x)$ ile $p'(x)$ in $K[x]$ içinde bir ebobu $d(x)$ olmak üzere $(x-u)|d(x)$ olduğundan $der(d(x)) \geq 1$ dir. $d(x)|p(x)$ ve $p(x)$ indirgenmez olduğundan $d(x)$ ile $p(x)$ bağdaşıktır ve $d(x)|p'(x)$ olduğundan $p(x)|p'(x)$'tir. $der\big(p'(x)\big) < der\big(p(x)\big)$ olduğundan $p'(x) = 0_F$ olmalıdır.

$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

olmak üzere

$p'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$

olduğundan $p'(x) = 0_F$ olması için gerek ve yeter şart her $1 \leq i \leq n$ için $ia_i = 0_F$ dır.

(i) $kar(F) = 0$ olsun. $\forall 1 \leq i \leq n$ için $ia_i = 0_F$ iken $a_i = 0_F$ olduğundan $p(x) = a_0$ olur $p(x)$ indirgenmez olduğundan çelişki elde edilir. O halde $p(x)$ in her kökü basit köktür.

(ii) $kar(F) = p > 0$ olsun. $\forall 1 \leq i \leq n$ için ya $a_i = 0_F$ ya da $p|i$ olması gerekir. $p|i$ olan $i$'ler $k_1,\ k_2, \dots, k_r$ olsun. $p \nmid i$ iken $a_i = 0_F$ olduğundan

$$p(x) = a_{k_r}x^{k_r} + \cdots + a_{k_1}x^{k_1} + a_0.$$

$\forall 1 \leq i \leq r$ için $k_i = ps_i, a_{k_i} = b_{s_i}$ ve $a_0 = b_0$ olsun. Yerine yazılırsa

$$p(x) = b_{s_r}x^{ps_r} + \cdots + b_{s_1}x^{ps_1} + b_0x^0.$$

$$q(x) = b_{s_r}x^{s_r} + \cdots + b_{s_1}x^{s_1} + b_0x^0$$

olarak tanımlanırsa $p(x) = q(x^p)$ dır.

Tersine $kar(F) = p$ ve $p(x) = b_{s_r}x^{ps_r} + \cdots + b_{s_1}x^{ps_1} + b_0$ olmak üzere $p'(x) = ps_rb_{s_r}x^{ps_r-1} + \cdots + ps_1b_{s_1}x^{ps_1-1} = 0_F$

olduğundan Teorem 1.9.2 gereğince $p(x)$ in çok katlı kökü vardır.

**Tanım 1.9.4.** $f(x) \in F[x]$ sabit olmayan bir polinom olmak üzere $f(x)$ in her indirgenmez çarpanı F üzerinde ayrılabilir ise $f(x)$ e F üzerinde bir *ayrılabilir polinom* denir.

**Sonuç 1.9.5.** F bir cisim olmak üzere $kar(F) = 0$ ise F üzerinde tanımlı her indirgenmez polinom ayrılabilir polinomdur. Ancak $kar(F) = p$ ise F üzerinde tanımlı bir indirgenmez polinomun ayrılabilir olması için gerek ve yeter şart $x^p$ nin bir polinomu olarak yazılamamasıdır.

**İspat.** $p(x) \in F[x]$ bir indirgenmez polinom olsun. Teorem 1.9.3'ten $kar(F) = 0$ için $p(x)$ in her kökü basit kök olacağından $p(x)$, F üzerinde ayrılabilirdir. $kar(F) = p$ ise $p(x)$ in ayrılabilir olması için gerek ve yeter şart $p(x) = q(x^p)$ olacak şekilde $q(x) \in F[x]$ olmamasıdır.

**Tanım 1.9.6.** F bir cisim E, F'nin bir cebirsel genişlemesi ve $u \in E$ olmak üzere $\text{İ}nd(u, F)$ ayrılabilir polinom ise $u$'ya F üzerinde bir *ayrılabilir eleman* denir. E'nin her elemanı F üzerinde ayrılabilir ise E'ye F'nin bir *ayrılabilir cisim genişlemesi* denir.

**Lemma 1.9.7.** K, E cisminin, E de F cisminin birer sonlu genişlemesi olsun. Bu durumda K'nin F cisminin ayrılabilir genişlemesi olması için gerek ve yeter şart K, E'nin bir ayrılabilir cisim genişlemesidir.

**İspat.** K'nin her elemanı F üzerinde ayrılabilir olduğundan E'nin her elemanı da F üzerinde ayrılabilirdir. O halde E, F'nin bir ayrılabilir genişlemesidir. $u \in K$, $\text{İ}nd(u,F) = p(x)$ ve $\text{İ}nd(u,E) = q(x)$ olsun. $q(x)|p(x)$ ve $p(x)$ ayrılabilir polinom olduğundan $q(x)$ ayrılabilir polinomdur. Böylelikle $u$, E üzerinde ayrılabilirdir ve $u$, K'den keyfi alındığından K, E'nin bir ayrılabilir genişlemesidir.

**Teorem 1.9.8.** F bir cisim ve $kar(F) = 0$ olmak üzere F'nin her cebirsel genişlemesi ayrılabilir genişlemedir.

**İspat.** E, F'nin bir cebirsel genişlemesi ve $u \in E$ olsun. $kar(F) = 0$ olduğundan Sonuç 1.9.5'ten $\text{İ}nd(u,F)$, F üzerinde ayrılabilir polinomdur. O halde $u$, F üzerinde ayrılabilirdir ve $u$, E'den keyfi seçildiğinden E, F'nin bir ayrılabilir genişlemesidir.

**Örnek 1.9.1.** $\mathbb{Q}$'nun her cebirsel genişlemesi ayrılabilir genişlemedir. $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, ... gibi.

**Teorem 1.9.9.** F bir cisim ve E, F'nin bir sonlu cisim genişlemesi olsun. E, F'nin bir ayrılabilir genişlemesi olması için gerek ve yeter şart $\{E : F\} = [E : F]$ dir.

**İspat.** E, F'nin bir ayrılabilir genişlemesi olsun. $[E : F] = n$ ve F'nin E'yi içeren bir sonlu normal genişlemesi L olmak üzere $n$ üzerine tümevarım uygulanır. $n = 1$ için iddia doğrudur. $n > 1$ ve $\leq n - 1$ dereceli polinomlar için iddia doğru olsun. $n > 1$ olduğundan $E \neq F$ dir. $u \in E/F$ ve $\text{İ}nd(u,F) = p(x)$ olsun. Teorem 1.5.3 ve Teorem 1.8.13'ten $[E : F] = [E : F(u)][F(u) : F]$ ve $\{E : F\} = \{E : F(u)\}\{F(u) : F\}$ olduğundan $[E : F(u)] = \{E : F(u)\}$ ve $[F(u) : F] = \{F(u) : F\}$ olduğu gösterilmelidir. $[F(u) : F] = der(p(x)) > 1$ olduğundan $[E : F(u)] \leq n - 1$ dir. Lemma 1.9.7'den dolayı, $[E : F(u)] = \{E : F(u)\}$ dur.

$[F(u) : F] = \{F(u) : F\}$ için $\{F(u) : F\} = der(p(x))$ olduğunun gösterilmelidir. Sonuç 1.7.5'ten $F(u)$ dan L içine tanımlı her F monomorfizması $u$'yu F üzerindeki bir eşleniğe götürdüğünden $\{F(u) : F\}$ sayısı, L içinde $p(x)$ in sıfırlarının sayısına eşittir. $u$, F üzerinde ayrılabilir olduğundan ve $p(x)$, L üzerinde parçalandığından $u$'nun F

üzerindeki eşleniklerinin sayısı $der(p(x))$ e eşittir. O halde $\{F(u):F\} = der\big(p(x)\big)$ dir.

Tersine $\{E:F\} = [E:F]$ olsun. $E \neq F$, $u \in E/F$ ve $\text{İ}nd(u,F) = p(x)$ olsun. $u$'nun F üzerinde ayrılabilir olduğu gösterilmelidir. $[F(u):F] = der(p(x))$ tir. $[E:F] = [E:F(u)][F(u):F]$ ve $\{E:F\} = \{E:F(u)\}\{F(u):F\}$ tir. Teorem 1.8.11'den $\{E:F(u)\} \leq [E:F(u)]$ ve $\{F(u):F\} \leq [F(u):F]$ olmalıdır. $\{F(u):F\} = der(p(x))$ olarak bulunur. Tanımdan $\{F(u):F\}$, $F(u)$ dan L içine tanımlı F monomorfizmalarının sayısıdır ve Sonuç 1.7.5'ten $p(x)$ in L içindeki sıfırlarının sayısına eşittir. O halde $p(x)$ in her kökü tek katlı köktür ve $u$, F üzerinde ayrılabilirdir.

**Sonuç 1.9.10.** K, E'nin, E, F'nin sonlu bir genişlemesi olmak üzere E, F'nin ve K, E'nin ayrılabilir genişlemeleri ise K, F'nin bir ayrılabilir genişlemesidir.

**İspat.** E, F'nin ve K, E'nin ayrılabilir genişlemeleri ise Teorem 1.9.9(ii)'den $\{E:F\} = [E:F]$ ve $\{K:E\} = [K:E]$ dir. Teorem 1.5.6 ve Teorem 1.8.13'ten $[K:F] = [K:E][E:F]$ ve $\{K:F\} = \{K:E\}\{E:F\}$ olduğundan yerine yazıldığında $[K:F] = \{K:F\}$ elde edilir. Teorem 1.9.9(i)'den K, F'nin ayrılabilir genişlemesidir.

**Sonuç 1.9.11.** F bir cisim E, F'nin bir sonlu cisim genişlemesi ve $E = F(u_1, u_2, \dots, u_n)$ olsun. $u_1, u_2, \dots, u_n \in E$, F üzerinde ayrılabilir ise E, F'nin bir ayrılabilir genişlemesidir.

**İspat.** $u = u_1$ ve $\text{İ}nd(u,F) = p(x)$ olmak üzere $[F(u):F] = der\big(p(x)\big)$ tir. $u$, $F$ üzerinde ayrılabilir olduğundan $p(x)$ bir ayrılabilir polinom ve $\{F(u):F\} = der\big(p(x)\big)$ dir. $[F(u):F] = \{F(u):F\}$ olduğundan Teorem 1.9.9'dan, $F(u)$, F'nin bir ayrılabilir genişlemesidir. n üzerine tümevarım uygulanarak genel hali gösterilir.

**Tanım 1.9.12.** F bir cisim olmak üzere F cisminin her sonlu genişlemesi ayrılabilir genişleme ise F cismine bir *mükemmel cisim* denir.

**Sonuç 1.9.13.** Karakteristiği sıfır olan her cisim mükemmeldir.

**İspat.** Teorem 1.9.8 ve Teorem 1.9.11 gereğince ispat açıktır.

**Teorem 1.9.14.** F bir cisim ve $kar(F) = p$ olmak üzere F cisminin mükemmel olması için gerek ve yeter şart $F = F^p$ olmasıdır. $F^p = \{a^p : a \in F\}$ dir.

**İspat.** $F \neq F^p$ olarak kabul edilsin. $a \in F/F^p$ ve $f(x) = x^p - a$ olsun. $f(x)$ in F üzerindeki parçalanma cismi K ve K içindeki bir kökü $u$ olmak üzere $u^p - a = 0$ ve $u^p = a$ olduğundan $f(x) = x^p - u^p = (x-u)^p$ olur. $p(x) = \text{İnd}(u, F)$ ve $p(x)|f(x)$ olduğundan $p(x) = (x-u)^t$ olacak şekilde $t \geq 1$ tam sayısı vardır. $t = 1$ ise $u \in F$ ve $u^p = a \in F^p$ çelişkisi elde edilir. O halde $t > 1$ ve $u$, $p(x)$ in çok katlı bir köküdür. $F(u)$, F'nin bir ayrılabilir genişlemesi değildir.

Tersine F mükemmel olmasın. F cisminin ayrılabilir olmayan bir sonlu genişlemesi E vardır. $u \in E$, F üzerinde ayrılabilir olmasın ve $p(x) = \text{İnd}(u, F)$ olsun. Teorem 1.9.3(ii) gereğince

$$p(x) = b_r(x^p)^r + b_{r-1}(x^p)^{r-1} + \cdots + b_1(x^p) + b_0$$

olacak şekilde $b_0, b_1, \ldots, b_r \in F$ vardır. $\forall 0 \leq i \leq r$ için $b_i = c_i^p$ olacak şekilde $c_i \in F$ varsa

$$p(x) = c_r^p x^{pr} + c_{r-1}^p x^{pr-1} + \cdots + c_1^p x^p + c_0^p = (c_r x^r + c_{r-1}x^{r-1} + \cdots + c_1 x + c_0)^p$$

elde edilir. Ancak $c_r x^r + c_{r-1}x^{r-1} + \cdots + c_1 x + c_0 \in F[x]$ ve $p(x)$ indirgenmez olmasıyla çelişir. O halde kabul yanlıştır ve $\exists 0 \leq i \leq r$ için $b_i \notin F^p$ olduğundan $F \neq F^p$ dir.

**Sonuç 1.9.15.** Her sonlu cisim mükemmeldir.

**İspat.** F sonlu bir cisim olsun. p asal sayısı olmak üzere $kar(F) = p$ dır. Teorem 1.7.16'dan, $F = F^p$ olduğundan Teorem 1.9.14 gereğince F mükemmeldir.

**Örnek 1.9.2.** F bir cisim ve $kar(F) = 0$ olsun. $f(x) \in F[x]$ ve $f'(x) = 0_F$ ise $f(x) = c$ olacak biçimde bir $c \in F$ vardır. Eğer $kar(F) \neq 0$ ise bu sonucun yanlış olabileceği $\mathbb{Z}_3[x]$ den bir örnekle aşağıdaki gibi gösterilir.

$kar(F) = 0$ ise $f(x) = x^n + d$ olacak biçimde $f(x)$ polinomu tanımlansın. $f'(x) = nx^{n-1} = 0_F$, $n = 0$ alınırsa $f'(x) = 0_F$ olur. $f(x) = x^0 + d = 1 + d = c$ olacak biçimde $c \in F$ vardır. $kar(F) \neq 0$ için $f(x) = x^3 \in F[x]$, $f'(x) = 3x^2 = 0_F$ fakat $f(x) = x^3 \neq c$ olduğundan bu ifade yanlıştır.

**Tanım 1.9.17.** F bir cisim ve E, F'nin bir cisim genişlemesi olsun. Eğer $E = F(u)$ olacak biçimde bir $u \in E$ varsa $u$'ya E'nin F üzerinde bir *ilkel elemanı* denir.

**Teorem 1.9.18.** *(İlkel Eleman Teoremi)* F bir sonsuz cisim ve E, F cisminin bir sonlu ayrılabilir cisim genişlemesi ise E, F'nin bir basit genişlemesidir.

**İspat.** $[E : F]$ sonlu olduğundan $E = F(u_1, u_2, \dots, u_n)$ olacak şekilde $u_1, u_2, \dots, u_n \in E$ vardır. n üzerine tümevarım uygulanır. $n = 1$ için $E = F(u_1)$, F'nin bir basit genişlemesidir. $1 < k \leq n-1$ için iddia doğru olsun. Tümevarımdan dolayı $F(u_1, u_2, \dots, u_{n-1}) = F(v)$ olacak şekilde bir $v \in E$ vardır ve $E = F(v, u_n)$ olur. $u_n = w$ olsun. F'nin E'yi içeren bir sonlu normal genişlemesi L, $\text{İ}nd(v, F) = p(x)$ ve $\text{İ}nd(w, F) = q(x)$ olsun. $u, v \in L$ olduğundan Teorem 1.8.7'den dolayı $p(x)$ ve $q(x)$, L üzerinde parçalanır ve kökler basit köktür. $p(x)$ ve $q(x)$ in L içindeki birbirinden farklı kökleri, sırasıyla $v = v_1, v_2, \dots, v_m, w = w_1, w_2, \dots, w_n$ olsun. $\forall 1 \leq i \leq m$ ve $\forall 1 < j \leq n$ için $v + xw = v_i + xw_j$ eşitliğini sağlayan bir tek $x \in F$ vardır. $(i, j)$ ikililerinin sayısı sonlu ve F sonsuz olduğundan öyle bir $a \in F$ vardır ki, her $1 \leq i \leq m$, her $1 \leq j \leq n$ ve $(1,1) \neq (i, j)$ için $v + aw \neq v_i + aw_j$; yani $a \neq \frac{v - v_i}{w_j - w}$ dir. $t = v + aw$ olsun. $v = t - aw$ olduğundan $p(t - aw) = 0_F$ olsun. $p(t - ax) = h(x)$ olsun. $h(x) \in F(t)[x]$ ve $h(w) = 0_F$ dir. Bir $j > 1$ için $h(w_j) = 0_F$ olsun. O zaman $p(t - aw_j) = 0$ olduğundan bir $1 \leq i \leq m$ için $t - aw_j = v_i$ ve buradan $t = v_i + aw_j$ çelişkisi elde edilir. O halde $h(x)$ ile $q(x)$ in bir tek ortak kökü vardır. $F(t)[x]$ içinde $h(x)$ ile $q(x)$ in $w$'dan başka kökü olmayan bir en büyük ortak böleni $d(x)$ olsun. $q(x)$, L içinde parçalandığında $d(x)$ te parçalanır. Fakat $d(x)$ in her kökü $q(x)$ in bir kökü olduğundan $d(x)$ bir lineer polinom olmalıdır. Böylece $0_F \neq b, c \in F(t)$ olmak üzere $d(x) = bx + c$ dır. $0_F = d(w) = bw + c$ olduğundan $w = -c/b \in F(t)$ olur. $t \in F(t)$ olduğundan $v \in F(t)$ ve $F(v, w) \leq F(t)$ olur. $F(t) \subseteq F(v, w)$ olduğundan $F(v, w) = F(t)$ dir.

**Sonuç 1.9.18.** F bir cisim ve $kar(F) = 0$ olsun. O zaman F'nin her sonlu genişlemesi F'nin bir basit genişlemesidir.

**İspat.** E, F'nin bir sonlu cisim genişlemesi olsun. $kar(F) = 0$ olduğundan F sonsuzdur. Ayrıca Sonuç 1.9.13'ten dolayı E, F'nin bir ayrılabilir genişlemesi olduğundan Teorem 1.9.16 gereğince, E, F'nin bir basit genişlemesidir.

**Örnek 1.9.3.** $f(x) = (x^2 + 2)(x^3 - 3)$ polinomunun $\mathbb{Q}$ üzerindeki parçalanma cismi K olsun. $K = \mathbb{Q}(u)$ olacak biçimde $u \in \mathbb{C}$ vardır. Yani $f(x) = (x^2 + 2)(x^3 - 3)$ polinomunun $\mathbb{Q}$ üzerindeki parçalanma cismi $\mathbb{Q}(\sqrt{3}, i\sqrt{2})$ dir. Polinomunun kökleri $\pm i\sqrt{2},\ \pm\sqrt{3}$ olduğundan $\mathbb{Q}(\pm i\sqrt{2},\ \pm\sqrt{3}) = \mathbb{Q}(\sqrt{3},\ i\sqrt{2})$ dir.

## 1.10. Tamamen Ayrılamaz Genişlemeler

**Tanım 1.10.1.** E, F cisminin sonlu bir genişlemesi ve $\{E : F\} = 1 < [E : F]$ ise E'ye F'nin *tamamen ayrılamaz genişlemesi* denir. $\bar{F}$ nin bir $\alpha$ elemanı $F(\alpha)$, F üzerinde tamamen ayrılamaz ise F üzerinde tamamen ayrılamazdır.

**Örnek 1.10.1.** $\mathbb{Z}_p(y),\ \mathbb{Z}_p(y^p)$ üzerinde tamamen ayrılamazdır.

**Teorem 1.10.2.** K, E'nin bir sonlu genişlemesi ve E, F'nin bir sonlu genişlemesi ve $F < K < E$ ise o zaman K, F üzerinde tamamen ayrılamaz olması için gerek ve yeter şart K, E üzerinde tamamen ayrılamaz ve E, F üzerinde tamamen ayrılamaz olmasıdır.

**İspat.** $F < K < E$ ise $[K : E] > 1$ ve $[E : F] > 1$ dir. Kabul edelim ki K, F üzerinde tamamen ayrılamaz olsun. O zaman $\{K : F\} = 1$ ve $\{K : F\} = \{K : E\}\{E : F\}$ dir. Dolayısıyla

$\{K : E\} = 1 < [K : E]$ ve $\{E : F\} = 1 < [E : F]$

olmalıdır. Böylece K, E üzerinde tamamen ayrılamazdır ve E, F üzerinde tamamen ayrılamazdır.

Tersine K, E üzerinde tamamen ayrılamaz ve E, F üzerinde tamamen ayrılamaz ise

$\{K : F\} = \{K : E\}\{E : F\} = (1)(1) = 1$ ve $[K : F] > 1$.

O halde K, F üzerinde tamamen ayrılamazdır.

Teorem 1.10.2 sonlu genişlemelerin herhangi bir sonlu cisim kulesine tümevarımla genişletilebilir. Cisim kulesindeki en üst cisim en alttaki cisim tamamen ayrılamaz olması için her bir cisim hemen altındakinin bir tamamen ayrılamaz genişlemesi olmalıdır.

**Sonuç 1.10.3.** E, F'nin bir sonlu genişlemesi ise E'nin F üzerinde tamamen ayrılamaz olması için gerek ve yeter şart E'deki her bir $\alpha \in E - F$, F üzerinde tamamen ayrılamazdır.

**İspat.** E, F üzerinde tamamen ayrılamaz ve $\alpha \in E - F$ olsun. O zaman $F < F(\alpha) < E$ dir. $F(\alpha) = E$ ise sonuçtan önceki açıklamadan dolayı $\alpha$, F üzerinde tamamen ayrılamazdır. $F < F(\alpha) < E$ ise o zaman Teorem 1.10.2 ve E, F üzerinde tamamen ayrılamaz olmasından dolayı $F(\alpha)$, F üzerinde tamamen ayrılamazdır.

Tersine her $\alpha \in E - F$ için $\alpha$, F üzerinde tamamen ayrılamaz olsun. E, F üzerinde sonlu olduğundan

$$F < F(\alpha_1) < F(\alpha_1, \alpha_2) < \cdots < E = F(\alpha_1, \dots, \alpha_n)$$

olacak şekilde $\alpha_1, \dots, \alpha_n$ vardır. Şimdi $\alpha_i$, F üzerinde tamamen ayrılamaz olduğu için $\alpha_i$, $F(\alpha_1, \dots, \alpha_{i-1})$ üzerinde tamamen ayrılamazdır. Çünkü $q(x) = ind\big(\alpha_i, F(\alpha_1, \dots, \alpha_{i-1})\big)$, $ind(\alpha_i, F)$'yi böler. Buna göre $\alpha_i$, $q(x)$ in tek sıfırıdır ve çok katlıdır. Böylece $F(\alpha_1, \dots, \alpha_i)$ tümevarımla genişletilmiş Teorem 1.10.2 sayesinde $F(\alpha_1, \dots, \alpha_{i-1})$ üzerinde tamamen ayrılamazdır.

### 1.11. Sonlu Cisimler ve Galois Genişlemeleri

Bu kısımda eleman sayısı sonlu olan cisimler ve bu cisimlerin özellikleri araştırılacaktır. Sonlu cisimler ilk kez Evariste Galois (1811-1832) tarafından çalışıldığından bunlara *Galois cisimleri* de denir.

**Teorem 1.11.1.** F bir sonlu cisim ve $kar(F) = p$ olmak üzere bir $n \geq 1$ için F, $p^n$ elemanlı bir cisimdir.

**İspat.** $\Delta\,(F)$, F'nin asal cismi ve F, $\Delta\,(F)$ üzerinde vektör uzayı olduğundan $[F : \Delta\,(F)] = n$ olacak biçimde bir $n \geq 1$ vardır. F'nin bir $\Delta\,(F)$-bazı $\{v_1, v_2, \dots, v_n\}$ olsun. F'nin her elemanı $u, c_1, c_2, \dots, c_n \in \Delta\,(F)$ olmak üzere,

$$u = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n$$

olacak şekilde tek türlü yazılabilir. $\Delta\,(F) \cong \mathbb{Z}_p$, olduğundan $|\Delta\,(F)| = p$ dir. $\forall c_i$, $p$ farklı şekilde seçilebildiğinden F cisminin elemanlarının sayısı $p^n$ dir.

**Teorem 1.11.2.** F bir sonlu cisim olmak üzere $F^* = F/\{0_F\}$ çarpımsal grubunun her sonlu alt grubu devirlidir.

**İspat.** G, $F^*$ nin bir sonlu altgrubu ve $|G| = n$ olsun. $n = 1$ için $G = \{1_F\}$ devirlidir. $n > 1$ için G'nin mertebesi maksimal olan bir elemanı $a$ ve $o(a) = m$ olsun. $m = n$ ise $G = \langle a \rangle$ dır. $m < n$ olsun. $\forall c \in \langle a \rangle$ için $c^m = 1_F$ olduğundan $\langle a \rangle$ nın elemanları $x^m - 1_F$ polinomunun m farklı kökünü oluşturur. Polinomun derecesi m ise polinomun F içindeki köklerinin sayısı en çok m'dir. Bu polinomun F içinde en çok m kökü olduğundan bütün kökler $\langle a \rangle$'nın elemanlarıdır. $b \in G/\langle a \rangle$ ve $o(b) = s$ olsun. $b^m \neq 1_F$ olduğundan $s \nmid m$ ve $s < m$'dir. $d = (m, s)$ için $d < m$ ve $d < s$ dir. $o(a^d) = \frac{m}{d}$ ve $o(b^d) = \frac{s}{d}$ dir. $\left(\frac{m}{d}, \frac{s}{d}\right) = 1$ olduğundan $o((ab)^d) = o(a^d b^d) = \left(\frac{m}{d}\right)\left(\frac{s}{d}\right)$ dir. Buradan $o(ab) = d\left(\frac{m}{d}\right)\left(\frac{s}{d}\right) = m\left(\frac{s}{d}\right) > m$ çelişkisi elde edilir. O halde $G = \langle a \rangle$ olduğundan G devirlidir.

**Sonuç 1.11.3.** Bir sonlu cismin her sonlu genişlemesi bir basit genişlemedir.

**İspat.** F bir sonlu cisim ve E, F'nin bir sonlu cisim genişlemesi olmak üzere $[E : F] = n$ olsun. F sonlu olduğundan $|E| = |F|^n$ dir. E sonludur ve Teorem 1.11.2'den $E^* = \langle a \rangle$ olacak şekilde $a \in E$ vardır. $E = F(a)$ olacağı açıktır.

**Teorem 1.11.4.** F, $p^n$ elemanlı bir cisim ise $1_F x^{p^n} - 1_F x \in \Delta(F)[x]$ polinomunun $\Delta(F)$ üzerindeki bir parçalanma cismi ve $p^n$ elemanlı herhangi iki cisim birbirine izomorftur.

**İspat.** $f(x) = 1_F x^{p^n} - 1_F x$ olsun. F sonlu olduğundan Teorem 1.11.2'den $F^* = \langle a \rangle$ olacak şekilde $0_F \neq a \in F$ vardır. $|F^*| = p^n - 1$ olduğundan $a^{p^n} = a$ dır. $\forall 1 \leq i \leq p^n$ için $(a^i)^{p^n} = (a^{p^n})^i = a^i$ olduğundan F cisminin her elemanı $f(x)$ in bir köküdür. O halde $f(x)$ in F içinde $p^n$ kökü vardır. $f(x)$ in köklerinin sayısı $\leq p^n$ olduğundan F üzerinde lineer çarpanlarına ayrılır. O halde F, $f(x)$ in $\Delta(F)$ üzerindeki bir parçalanma cismidir.

$p^n$ elemanlı başka bir cisim E, $1_E x^{p^n} - 1_E x$ polinomunun $\Delta(E)$ üzerindeki parçalanma cismidir. Öte yandan, $\Delta(F) \cong \mathbb{Z}_p$ ve $\Delta(E) \cong \mathbb{Z}_p$ olduğundan $\Delta(F)$ den $\Delta(E)$ ye bir $\sigma$ izomorfizması tanımlıdır. $\sigma^*$, $\Delta(F)[x]$ ten $\Delta(E)[x]$ e $\sigma$'nun

eşlemesiyle tanımlı izomorfizma olmak üzere $\sigma^*(1_F x^{p^n} - 1_F x) = 1_E x^{p^n} - 1_E x$ olduğundan Teorem 1.7.3'ten dolayı $\sigma$, F'den E'ye bir izomorfizmaya genişler.

Çoğunlukla $p^n$ elemanlı bir cismin daima $\mathbb{Z}_p$ yi içerdiği kabul edilecektir.

**Örnek 1.11.1.** F bir sonlu cisim ve $|F| = p^n$ olsun. F'nin sıfırdan farklı her $a$ elemanının bir tek p. kökü şu şekilde gösterilir: $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ olsun. Kabul edilsin ki $a \in F$ için $b \neq c$ olmak üzere $a = b^n$ ve $a = c^n$olacak şekilde $b,\ c \in F$ vardır. $f(a) = a^{p^n} - a = 0_F$, $a = b^n$ ve $a = c^n$ için sırasıyla $(b^n)^{p^n} - b^n = 0_F$ ve $(c^n)^{p^n} - c^n = 0_F$ eşitlikleri elde edilir. $(b^n)^{p^n} - b^n = (c^n)^{p^n} - c^n \Rightarrow (b^n)^{p^n} - (c^n)^{p^n} = b^n - c^n \Rightarrow (b^n - c^n)^{p^n} = (b^n - c^n)^1 \Rightarrow (b^n - c^n)^{p^n - 1} = 0_F$ eşitliği elde edilir. O halde $b^n = c^n$ den $b = c$ dir. Kabulle çelişir. F'nin sıfırdan farklı her $a$ elemanının bir tek p. kökü vardır.

**Teorem 1.11.5.** Her p asal sayısı ve her $n \geq 1$ için $p^n$ elemanlı bir cisim vardır.

**İspat.** $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ olsun. Teorem 1.8.2'den K, $\mathbb{Z}_p$ üzerinde $f(x)$ in bir parçalanma cismi olmak üzere $f(x)$ in K içindeki bütün köklerinin kümesi S olsun.

$$f'(x) = \overline{p^n} x^{p^n - 1} - \overline{1} = -\overline{1}$$

olduğundan $f'(x)$ in hiçbir kökü yoktur. O halde Teorem 1.9.2'den $f(x)$ in her kökü basit köktür ve $|S| = p^n$ dir.

$|S| \geq 2$ olduğu açıktır. $a, b \in S$ olsun. Teorem 1.4.2'den $a + b$, $-b$, $ab$ ve $(b \neq \bar{0})$ $b^{-1} \in S$ olduğu gösterilmelidir. $a$, $b$, $f(x)$ in kökleri olduğundan $a^{p^n} = a$ ve $b^{p^n} = b$ dir. $\forall k \geq 0$ için

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

olduğu gösterilir. $k = 0$ için aşikardır. $k = 1$ hali Frobenius otomorfizmasının açıklamasında gösterilmiştir. $k > 0$ ve $k - 1$ için iddia sağlansın. Tümevarımdan dolayı, $(a + b)^{p^{k-1}} = a^{p^{k-1}} + b^{p^{k-1}}$ olduğundan

$$(a + b)^{p^k} = [(a + b)^{p^{k-1}}]^p = (a^{p^{k-1}} + b^{p^{k-1}})^p = a^{p^k} + b^{p^k}.$$

$k = n$ için $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$'dir. Aynı zamanda $(-a)^{p^n} = -a^{p^n} = -a$, $ab^{p^n} = a^{p^n}b^{p^n} = ab$ ve $b \neq 0$ iken $(b^{-1})^{p^n} = b^{-1}$ olduğundan $a+b$, $-b$, $ab$, $b^{-1}$ $(b \neq \bar{0}) \in S$ dir. O halde S bir cisimdir. $\mathbb{Z}_p \leq S$ olduğu açıktır. O halde S, $\mathbb{Z}_p$ üzerinde $f(x)$ in parçalanma cismi olduğundan S = K dır.

**Tanım 1.11.6.** $\mathbb{Z}_p$ yi içeren $p^n$ elemanlı bir cisim $GF(p^n)$ ile gösterilir ve bu cisme $p^n$ elemanlı bir *Galois cismi* denir.

**Teorem 1.11.7.** F bir sonlu cisim olmak üzere $\forall n \geq 1$ için $F[x]$ içinde derecesi n olan bir indirgenmez polinom vardır.

**İspat.** $kar(F) = p$, $F = GF(p^r)$ ve $f(x) = x^{p^{rn}} - x \in \mathbb{Z}_p[x]$ olmak üzere $\mathbb{Z}_p \leq F$ olduğundan $f(x) \in F[x]$ tir. K, $f(x)$ in F üzerindeki parçalanma cismi ve S, $f(x)$ in K içindeki köklerinin kümesi olsun. Teorem 1.11.6'nın ispatında görüldüğü gibi S, K'nin bir alt cismi ve $|S| = p^{nr}$ dir. Öte yandan $\mathbb{Z}_p$, K'nin asal cismi olduğundan S'nin bir alt cismidir. $f(x) \in \mathbb{Z}_p[x]$ olduğundan hem K ve hem de S, K içinde $f(x)$ in $\mathbb{Z}_p$ üzerindeki parçalanma cisimleridir ve $S = K$ dir. Özel olarak $|K| = p^{rn}$ dir. $F \leq K$ ve $|F| = p^r$ olduğundan $[K : F] = n$ dir. Sonuç 1.10.4'ten bir $u \in K$ için $K = F(u)$ olduğundan $[K : F] = der\big(\text{İnd}(u, F)\big)$ ve $der\big(\text{İnd}(u, F)\big) = n$ bulunur.

**Sonuç 1.11.8.** $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ polinomu birbirinden farklı monik indirgenmez polinomların çarpımı ve bir indirgenmez polinomun $f(x)$ i bölmesi için gerek ve yeter şart derecesinin $n$'yi bölmesidir.

**İspat.** $f'(x) = \overline{p^n}x^{p^n-1} - \bar{1} = -\bar{1}$ olduğundan $f(x)$ in her kökü tek katlıdır. Yani birbirinden farklı monik indirgenmez polinomların çarpımıdır.

$p(x) \in \mathbb{Z}_p[x]$ indirgenmez ve $der\big(p(x)\big) = d$ olmak üzere $f(x)$ in $\mathbb{Z}_p$ üzerindeki parçalanma cismi K olsun. Teorem 1.11.6'dan K, $f(x)$ in bütün köklerinin kümesidir ve $|K| = p^n$ dir. O halde $\big[K : \mathbb{Z}_p\big] = n$ dir. $p(x)|f(x)$ olsun. K, $f(x)$ in bütün kökleri olduğundan $p(u) = \bar{0}$ olacak şekilde bir $u \in K$ vardır. Bu durumda $\big[\mathbb{Z}_p(u) : \mathbb{Z}_p\big] = d$ dir. Ayrıca

$$n = \big[K : \mathbb{Z}_p\big] = \big[K : \mathbb{Z}_p(u)\big]\big[\mathbb{Z}_p(u) : \mathbb{Z}_p\big] = \big[K : \mathbb{Z}_p(u)\big]d$$

olduğundan $d|n$ dir.

Tersine $d|n$ için $p(x) \in \mathbb{Z}_p[x] \subseteq K[x]$ olduğundan $p(x) \in K[x]$ tir. $p(x)$ in K üzerinde bir parçalanma cismi L ve $p(x)$ in L içindeki bir kökü $v$ olsun. Eğer $v \in K$ ise Teorem 1.11.6'nın ispatından $f(u) = \bar{0}$ ve $p(x)|f(x)$ tir. $v \notin K$ olursa $\mathbb{Z}_p \leq K$ olduğundan $\mathbb{Z}_p(v) \leq K(v)$ dir. Ayrıca $\left[\mathbb{Z}_p(v) : \mathbb{Z}_p\right] = d$ olduğundan $\left|\mathbb{Z}_p(v)\right| = p^d$ ve $\left|\mathbb{Z}_p(v)\right|^* = p^d - 1$ dir. $v \neq 0$ olduğundan $v^{p^d-1} = 1$ ve $v,\ x^{p^d-1} - 1$ in bir köküdür. Öte yandan $d|n$ olduğundan $p^d - 1|p^n - 1$ ve $x^{p^d-1} - 1 \Big| x^{p^n-1} - 1$ dir. O halde $v^{p^n-1} = 1$ ve $v^{p^n} = v$ bulunur. $v,\ p(x)$ in L içindeki bir köküdür ve $v \in K$ çelişkisi elde edilir.

**Örnek 1.11.2.** $p(x) = x^4 + x + \bar{1}$ polinomu için $\mathbb{Z}_2$ üzerinde $p(\bar{0}) = \bar{1}$ ve $p(\bar{1}) = \bar{1}$ olduğundan kökü yoktur. O halde $p(x) = x^4 + x + \bar{1}$ polinomu $\mathbb{Z}_2$ üzerinde indirgenmezdir.

**Tanım 1.11.9.** F bir cisim ve E, F'nin bir sonlu cisim genişlemesi olmak üzere E, F'nin bir ayrılabilir normal genişlemesi ise E'ye F'nin bir *galois genişlemesi* ve $G(E/F)$ grubuna *galois grubu* denir.

**Örnek 1.11.3.** $x^4 - 2$ polinomunun $\mathbb{Q}$ üzerindeki parçalanış cisminin galois grubu şu şekildedir: $x^4 - 2$ polinomunun kökleri $\pm\sqrt[4]{2},\ \pm i\sqrt[4]{2}$ olup $\mathbb{Q}$ üzerindeki parçalanma cismi $K = \mathbb{Q}(\sqrt[4]{2}, i)$ dir. $\mathbb{Q}\left(\sqrt[4]{2}\right)$ yi sabit bırakan otomorfizmaları $\psi_{i,-i},\ \psi_{i,i},\ \psi_{\sqrt[4]{2},\sqrt[4]{2}},\ \psi_{\sqrt[4]{2},-\sqrt[4]{2}}$ dir. $\psi_{i,-i} = \tau$ ve $\psi_{\sqrt[4]{2},-\sqrt[4]{2}} = \sigma$ dur. $G(K/\mathbb{Q}) = \langle\sigma,\ \tau\rangle = \{\iota,\ \sigma, \tau, \sigma\tau\}$ dir.

**Teorem 1.11.10.** F bir cisim ve E, F'nin bir sonlu cisim genişlemesi olmak üzere E'nin F üzerinde galois olması için gerek ve yeter şart $|G(E/F)| = [E : F]$ dir.

**İspat.** E, F üzerinde galois ise Tanım 1.11.9'den E, F'nin bir ayrılabilir normal genişlemesidir. Teorem 1.8.14 ve Teorem 1.9.9 gereğince $\{E : F\} = |G(E/F)|$ ve $\{E : F\} = [E : F]$ olduğundan $|G(E/F)| = [E : F]$ dir.

Tersine $|G(E/F)| = [E : F]$ olsun. $\{E : F\}$ nin tanımından $|G(E/F)| \leq \{E : F\}$ olduğu açıktır. Teorem 1.8.11'den $\{E : F\} \leq [E : F]$ dır. Böylelikle $|G(E/F)| = \{E : F\} = [E : F]$ elde edilir. Teorem 1.8.14 ve Teorem 1.9.9 uygulanır E, F üzerinde galoistir.

**Lemma 1.11.11.** F bir cisim olmak üzere E, F'nin bir galois genişlemesi ve $F \leq B \leq E$ ise E, B'nin bir galois genişlemesidir.

**İspat.** E, F'nin bir sonlu ayrılabilir normal genişlemesi olduğundan Lemma 1.9.7'den E, B'nin bir ayrılabilir genişlemesidir. E, F üzerinde parçalanma cismi olduğundan B üzerinde de parçalanma cismidir. Yani B'nin bir normal genişlemesidir. O halde E, B'nin üzerinde galoisdir.

**Lemma 1.11.12.** F bir cisim E, F'nin bir galois genişlemesi ve $F \leq B \leq E$ ise $E_{G(E/B)} = B$ dir.

**İspat.** Tanım 1.11.9'dan

$$E_{G(E/B)} = \{u \in E : \sigma(u) = u, \ \forall \sigma \in G(E/B) \text{ için}\}.$$

O halde $B \leq E_{G(E/B)}$ dir. Varsayalım ki, $E_{G(E/B)} \neq B$ olsun. $u \in E_{G(E/B)} \setminus B$ ve $p(x) = \text{İ}nd(u, B)$ olsun. Lemma 1.11.12'den E, B üzerinde galois olduğundan B'nin bir normal genişlemesidir. O halde $p(x)$, E üzerinde parçalanır. Ayrıca $u, p(x)$ in bir basit kökü ve $der(\big(p(x)\big) > 1$ olduğundan $p(x)$ in E içinde $u$'dan farklı bir kökü $v$ vardır. $\psi_{u,v} : B(u) \to B(v)$ temel izomorfizması göz önüne alınırsa Teorem 1.8.3'ten $\psi_{u,v}$, E'nin bir $\theta$ otomorfizmasına genişler ve $\theta \in G(E/B)$ dir. Ancak $u \in E_{G(E/B)}$ olduğundan $v = \psi_{u,v}(u) = \theta(u) = u \in G(E/B)$ çelişkisi elde edilir. O halde $E_{G(E/B)} = B$ dir.

**Lemma 1.11.13.** F bir cisim olsun. E, F'nin bir galois genişlemesi, $G = G(E/F)$ ve H, G'nin bir alt grubu ise $G(E/E_H) = H$ dır.

**İspat.** $|H| = n$ ve $H = \{\sigma_1, \sigma_2, \ldots \sigma_n\}$ olsun. E, F'nin bir ayrılabilir cisim genişlemesi olduğundan Teorem 1.9.16 ve Sonuç 1.11.3'ten $E = F(u)$ olacak şekilde bir $u \in E$ vardır.

$$f(x) = \big(x - \sigma_1(x)\big)\big(x - \sigma_2(x)\big) \ldots \big(x - \sigma_n(x)\big)$$

$f(x)$ polinomu tanımlansın. $1 \leq j \leq n$ için $\sigma$'nun etkisiyle tanımlanan $\sigma_j^* : E[x] \to E[x]$ otomorfizması göz önüne alınırsa

$$\sigma_j^*\big(f(x)\big) = \Big(x - \sigma_j\sigma_1(x)\Big)\Big(x - \sigma_j\sigma_2(x)\Big) \ldots \Big(x - \sigma_j\sigma_n(x)\Big).$$

H grup olduğundan $\sigma_i$, H'nin bütün elemanları üzerinde değişirken $\sigma_j\sigma_i$'de H'nin bütün elemanları üzerinde değişir. $\sigma_j^*\big(f(x)\big) = f(x)$ ve $f(x)$ in katsayıları $\sigma_j$ altında sabit kalır. Burada $\sigma_j$ keyfi seçildiğinden, $f(x) \in E_H[x]$ tir. O halde E, $f(x)$ in $E_H$ üzerindeki bir parçalanma cismidir. $p(x) = \text{İ}nd(u, E_H)$ ve $\sigma_1 = \iota_G$ olsun. $(x-u)|f(x)$ olduğundan $f(u) = 0_F$ ve $p(x)|f(x)$ tir. Bu durumda $der\big(p(x)\big) \leq n$ olduğundan $[E : E_H] \leq n$ dir. Ayrıca Teorem 1.8.11'den $|G(E/E_H)| \leq [E : E_H]$ olduğundan $|H| = [E : E_H]$ elde edilir.

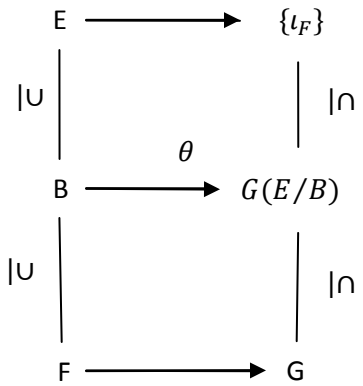
**Teorem 1.11.14.** *(Galois Teorisinin Temel Teoremi)* F bir cisim E, F'nin bir Galois genişlemesi ve $G = G(E/F)$ olsun. E'nin F'yi içeren bütün alt cisimlerinin kümesi $Ara(E/F)$ ve G'nin bütün alt gruplarının kümesi $Alt(G)$ olmak üzere $\forall B \in Ara(E/F)$ için $\theta : B \to G(E/B)$ eşlemesi $Ara(E/F)$ den $Alt(G)$ üzerine bire bir eşlemedir (Şekil 13). Aşağıdakiler sağlanır.

(i) $\forall B \in Ara(E/F)$ için $B = E_{G(E/E_B)}$

(ii) $\forall H \in Alt(G)$ için $H = G(E/E_H)$

(iii) $[E : B] = |G(E/B)|$ve $[B : F] = |G(E/F) : G(E/B)|$

(iv) B'nin F'nin bir galois genişlemesi olması için gerek ve yeter şart $G(E/B) \lhd G(E/F)$ olmasıdır. Bu durumda $G(B/F) \cong G(E/F)/G(E/B)$ dir.




**Şekil 13.** Galois Teorisinin Temel Teoremi

(i) $B \in Ara(E/F)$ olmak üzere E, F üzerinde Galois olduğundan Lemma 1.11.13'den $B = E_{G(E/E_B)}$ dir.

(ii) $H \in Alt(G)$ olmak üzere E, F üzerinde Galois olduğundan Lemma 1.11.13'den $H = G(E/E_H)$ dir.

$B', B \in Ara(E/F)$ olmak üzere $\theta(B) = \theta(B')$ ise $G(E/B) = G(E/B')$ olduğundan, $E_{G(E/B)} = E_{G(E/B')}$ dir. (i)'den $B = E_{G(E/E_B)}$ ve $B' = E_{G(E/B')}$ olduğundan $B = B'$ olur.

$H \in Alt(G)$ olmak üzere $\theta(E_H) = G(E/E_H)$ dır. Fakat (ii)'den dolayı $G(E/E_H) = H$ olduğundan, $\theta$ örtendir. O halde $\theta$ bire bir eşlemedir.

(iii) $B \in Ara(E/F)$ olmak üzere E, B üzerinde galois olduğundan $[E : B] = |G(E/B)|$ dir.

$G(E/F)$ Galois olduğundan

$$|G| = [E : F] = [E : B][B : F] = |G(E/B)|[B : F]$$

böylelikle

$$[B : F] = \frac{|G|}{|G(E/B)|} = |G : G(E/B)|$$

bulunur.

(iv) $B \in Ara(E/F)$ olmak üzere B, F'nin bir galois genişlemesi olsun. $\sigma \in G(E/B)$ ve $\sigma \in G$ olsun. $\theta|_B$, B'den E içine bir F monomorfizmasıdır. B, F üzerinde normal olduğundan Teorem 1.8.6'den B'nin bir otomorfizmasıdır. O halde $\theta(B) \subseteq B$'dir. $\forall b \in B$ için $\theta(b) \in B$ olduğundan $\theta^{-1}\sigma\theta(b) = \theta^{-1}\sigma\big(\theta(b)\big) = \theta^{-1}\big(\theta(b)\big) = b$ dir. Dolayısıyla $\theta^{-1}\sigma\theta \in G(E/B)$ ve $G(E/B) \lhd G$ dir.

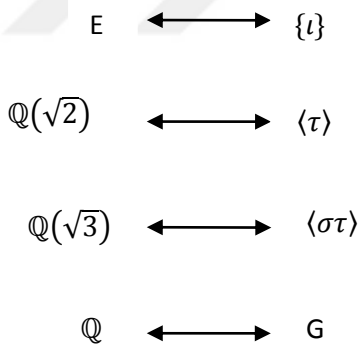
Tersine $G(E/B) \lhd G$ olsun. Varsayalım ki B, F üzerinde galois olmasın. E, F üzerinde galois olduğundan Lemma 1.9.7'den B, F üzerinde ayrılabilirdir; dolayısıyla normal genişleme olamaz. Öyleyse bir $u \in B$ vardır ki $\text{İ}nd(u, F)$, B üzerinde parçalanmaz. $\text{İ}nd(u, F)$ nin $E/B$ içindeki bir kökü $v$ olsun. $\psi_{u,v} : F(u) \to F(v)$ değer izomorfizması, Sonuç 1.8.5'ten E'nin bir $\tau$ otomorfizmasına genişler. $\sigma \in G(E/B)$ olsun. Kabulden $\tau^{-1}\sigma\tau \in G(E/B)$ dir. Buradan $(\tau^{-1}\sigma\tau)(u) = u$ olduğundan

$\sigma\big(\tau(u)\big) = \tau(u)$ dur. $\sigma, G(E/B)$ den keyfi seçildiğinden, $\tau(u) = E_{G(E/B)}$ olur. Lemma 1.11.13'ten dolayı, $E_{G(E/B)} = B$ olduğundan $\tau(u) \in B$ çelişkisi elde edilir. O halde B, F üzerine galoistir.

Teorem 1.11.15'daki $B \to G(E/B)$ eşlemesine *galois eşlemesi* denir. Bu teorem bir $E/F$ Galois genişlemesinde ara cisimlerin sayısının $G(E/F)$ Galois grubunun alt gruplarının sayısına eşit olduğunun ve $G(E/F)$ sonlu olduğundan, B ara cisimlerinin sayısının sonlu olduğunu göstermektedir.

**Örnek 1.11.4.** $E = \mathbb{Q}\big(\sqrt{3}, \sqrt{5}\big)$ ve $G = G(E/\mathbb{Q})$ olsun. E'nin bütün ara cisimleri aşağıdaki gibi belirlenir.

E, $\mathbb{Q}$ üzerinde galois ve ara cisimler alt grupların sabit cisimlerinden oluşur. $\sigma = \psi_{\sqrt{3},-\sqrt{3}}$ ve $\tau = \psi_{\sqrt{5},-\sqrt{5}}$ olmak üzere $G = \{\iota, \sigma, \tau, \sigma\tau\}$ ve G'nin elemanter abelyan grup olduğu gösterildi ve G'nin alt grupları ile bunların sabit cisimleri belirlendi.



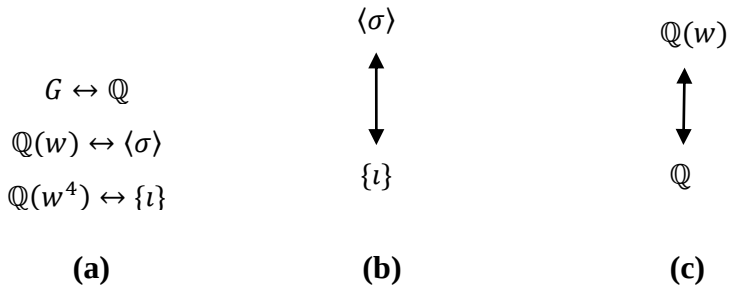

**Şekil 14.** E'nin alt cisimleri ile G'nin alt grupları arasındaki eşleme

**Örnek 1.11.5.** $x^4 - 1$ polinomunun $\mathbb{Q}$ üzerindeki parçalanma cismi K ve $G = G(K/\mathbb{Q})$ olsun. K'nın $\mathbb{Q}$'nun galois genişlemesidir. galois eşlemesi, alt grup ve alt cisim kafesleri aşağıda gösterilmiştir.

$K = \mathbb{Q}(w)$ ve $G = G(K/\mathbb{Q}) = \langle\sigma\rangle = \{\iota_F,\ \psi_{w,w^2},\ \psi_{w,w^3},\ \psi_{w,w^4}\}$ dır.

$\psi_{w,w^2} = \sigma, \psi_{w,w^3} = \sigma^2, \psi_{w,w^4} = \sigma^3, \iota_F = \sigma^4$

K, $\mathbb{Q}$'nun ayrılabilir normal genişlemesi olduğundan K, $\mathbb{Q}$'nun galois genişlemesidir.




**Şekil 15:** Galois eşlemesi (a), Alt grup kafesi (b), Alt cisim kafesi (c)

F bir cisim, $f(x) \in F[x]$ F üzerinde bir ayrılabilir polinom ve $f(x)$ polinomunun F üzerindeki parçalanma cismi K ise K, F cismi üzerinde bir ayrılabilir genişlemesidir. Üstelik K, F'nin bir normal genişlemesi olduğundan galoistir. Bu durumda $G(K/F)$ grubuna $f(x)$ *polinomunun F üzerindeki galois grubu* denir.

**Teorem 1.11.15.** $F = GF(p^r)$ ve E, F'nin bir sonlu cisim genişlemesi olmak üzere $[E : F] = n$ ise E, F'nin bir Galois genişlemesidir.

$\sigma_{p^r} : E \to E,\ u \mapsto u^{p^r}$

şeklinde tanımlı $\sigma_{p^r}$ fonksiyonu E'nin F'yi sabit bırakan bir otomorfizmasıdır ve $G(E/F) = \langle\sigma_{p^r}\rangle$ dir.

**İspat.** $[E : F] = n$ olduğundan $|E| = p^{nr}$ ve Teorem 1.11.4 gereğince E, $x^{p^{nr}} - x \in F[x]$ polinomunun F üzerindeki parçalanma cismidir. $x^{p^{nr}} - x$ in her kökü tek katlı olduğundan E, F üzerinde galoistir. Teorem 1.11.10'den $|G(E/F)| = n$ dir.

$a, b \in E$ olsun. $kar(F) = p$ olduğundan $(a+b)^{p^r} = a^{p^r} + b^{p^r}$, $(ab)^{p^r} = a^{p^r} b^{p^r}$ dır.

O halde $\sigma_{p^r}$ bir halka homomorfizmasıdır. $\sigma_{p^r}(1_F) = 1_F \neq 0_F$ olduğundan $\sigma_{p^r}$ bire birdir. E sonlu olduğundan $\sigma_{p^r}$ otomorfizmadır. Öte yandan $u \in E$ için $\sigma^{p^r}(u) = u$ demek $u^{p^r} = u$ olduğundan u, $x^{p^{nr}} - x$ in bir köküdür. $x^{p^{nr}} - x$ in köklerinin kümesi F olduğundan $\sigma^{p^r}$, F'yi sabit bırakır ve $G(E/F)$ ye aittir. $|G(E/F)| = n$ olduğundan

$o(\sigma_{p^r}) = n$ olduğu gösterilirse eşitlik sağlanır. $\theta = \sigma_{p^r}$ ve $o(\theta) = s$ olsun. $\forall u \in E$ ve $k \geq 1$ için $\theta^k(u) = u^{p^{kr}}$ olduğu tümevarımla gösterilir. $k = 1$, $\theta$ tanımının sonucudur. $k \geq 1$ için iddia doğru olsun ve $k + 1$ için doğruluğu gösterilsin.

$$\theta^{k+1}(u) = \theta\left((u)^{p^{kr}}\right) = (\theta(u))^{p^{kr}} = \left(u^{p^r}\right)^{p^{kr}} = u^{p^{(k+1)r}}.$$

$k = n$ için $\theta^n(u) = u^{p^m} = u$ olduğundan, $\theta^n = \iota$ ve buradan $s|n$ dir. Öte yandan $\forall u \in E$ için $\theta^s(u) = (u)^{p^{rs}} = \iota(u) = u$ olduğundan $u$ elemanı $x^{p^{rs}} - x$ polinomunun bir köküdür. Buradan $|E| \leq p^{rs}$ ve böylece $p^m \leq p^{rs}$ olur. Buradan $rn \leq rs$ olduğundan $n \leq s$ bulunur. $s \leq n$ olduğundan $s = n$ dir.

**Örnek 1.11.6.** $GF(729)/GF(9)$ galois genişlemesinin galois grubu devirlidir. $GF(9) \leq B \leq GF(729)$ olan B ara cisimlerinin sayısını aşağıda verilmiştir.

$E = GF(729) = GF(3^6)$ Teorem 1.11.15'den dolayı $\mathbb{Z}_3$ üzerinde Galois olduğundan $[E : \mathbb{Z}_3] = 3^6$ dır. Her $u \in E$ için $\sigma_3 : u \to u^3$ biçiminde tanımlı $\sigma_3$ fonksiyonu E'nin bir otomorfizmasıdır ve $G(E/\mathbb{Z}_3) = \langle\sigma_3\rangle$ tür. Benzer şekilde $F = GF(9) = \langle\sigma_3\rangle$ tür. O halde $GF(729)/GF(9)$ genişlemesi devirlidir. E'nin bütün alt grupları $1 \leq k \leq 12$ ve $k|12$ olmak üzere $\langle\sigma_3^k\rangle$ lardan oluşur ve Örnek 1.11.5 'deki gibi $E_k \leftrightarrow GF(3^k)$ eşlemesi elde edilir. $GF(3^6)$ nin alt grupları $\langle\sigma_3\rangle$, $\langle\sigma_3^3\rangle$, $\langle\sigma_3^{3^2}\rangle$, $\langle\sigma_3^{3^3}\rangle$, $\langle\sigma_3^{3^4}\rangle$, $\langle\sigma_3^{3^6}\rangle$, $\langle\sigma_3^{3^{12}}\rangle$ ve $GF(3^6)$ nin alt cisimleri $GF(3)$, $GF(3^2), GF(3^3)$, $GF(3^4)$, $GF(3^6)$, $GF(3^{12})$ dir. Benzer şekilde $GF(9)$'nin altgrupları $\langle\sigma_3\rangle$, $\langle\sigma_3^3\rangle$, $\langle\sigma_3^{3^2}\rangle$ ve $GF(9)$ nin alt cisimleri $GF(3), GF(3^3), GF(3^9)$ dır. O halde $GF(9) \leq B \leq GF(729)$ olacak şekilde B ara cisimleri $GF(3^2)$, $GF(3^6)$ dir.

**Lemma 1.11.16.** $s, t \in \mathbb{C}$ için $f(x) = x^2 + sx + t$ olmak üzere $f(x), \mathbb{C}$ üzerinde parçalanır.

**İspat.** $x^2 + sx + t = (x - s/2)^2 + (4t - s^2)/4$ tür. $(x - s/2)^2 + (4t - s^2)/4 = 0$ olsun. Buradan $(x - s/2)^2 = (s^2 - 4t)/4$ bulunur. $(s^2 - 4t)/4$ ün karekökleri aşağıdaki şekilde bulunabilir.

$a, b \in \mathbb{R}$ olmak üzere $(s^2 - 4t)/4 = a + ib$ ve $a + ib$ nin bir karekökü $x + yi$ olmak üzere $a + ib = (x + yi)^2$ eşitliğinden $x^2 - y^2 = a$ ve $2xy = b$ elde edilir. $y = b/2x$ birinci eşitlikte yerine yazılırsa $x^4 - ax^2 - \frac{b^2}{4} = 0$ denklemi elde edilir. Buradan

$$(x^2)_{1,2} = \frac{a \pm \sqrt{a^2 + b^2}}{2}$$

bulunur.

**Örnek 1.11.7.** $5z^2 + 2z + 10 = 0$ denklemi Lemma 1.11.16'daki ikinci yöntem uygalanırsa şu şekilde çözülür:

$z^2 + 2/5z + 2 = 0$ Lemma 1.11.16'den $s = 2/5,\ t = 2$ dir.

$$z^2 + \frac{2}{5z} + 2 = \left(z - \frac{2}{10}\right)^2 + \frac{\frac{8-4}{25}}{4}$$

$$\left(z - \frac{2}{10}\right)^2 = -\frac{\frac{8-4}{25}}{4}$$

$$\sqrt{\left(z - \frac{2}{10}\right)^2} = \sqrt{-\frac{\frac{8-4}{25}}{4}}, \qquad z_1 = \frac{2}{10} + \frac{6\sqrt{6}}{10}i, \qquad z_2 = \frac{2}{10} - \frac{6\sqrt{6}}{10}i$$

**Lemma 1.11.17.** $f(x) \in \mathbb{R}[x]$ ve $der\big(f(x)\big) = n$ bir tek tamsayı olmak üzere $f(x)$ in bir reel kökü vardır.

**İspat.** $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{R}[x]$ ve $t = 1 + \sum_{i=1}^{n-1}|a_i|$ olsun. Her $0 \le i \le n - 1$ için $a_i \le t - 1$ dir. Buradan

$$|a_0 + a_1t + \cdots + a_{n-1}t^{n-1}| \le (t-1)(1 + t + \cdots + t^{n-1}) = t^n - 1 < t^n$$

elde edilir. O halde

$$f(t) = a_0 + a_1t + \cdots + a_{n-1}t^{n-1} + t^n \ge t^n - |a_0 + a_1t + \cdots + a_{n-1}t^{n-1}| > t^n - t^n$$

$$= 0.$$

Öte yandan $\forall a_i \le t$ olduğundan

$$f(-t) = a_0 + a_1(-t) + \cdots + a_{n-1}(-t)^{n-1} + (-t)^n$$
$$\leq t[1 + (-t) + \cdots + (-t)^{n-1}] + (-t)^n$$
$$= t[(t^n + 1)/(t + 1)] - t^n < 0.$$

O halde $f(t) > 0$ ve $f(-t) < 0$ ve $f(x)$, fonksiyon olarak sürekli olduğundan bir $c \in (-t, t)$ için $f(c) = 0$ olur.

**Teorem 1.11.18.** *(Cebirin Temel Teoremi)* $\mathbb{C}[x]$ in sabit olmayan her polinomu $\mathbb{C}$ üzerinde parçalanır.

**İspat.** $f(x) \in \mathbb{C}[x]$ ve $der(f(x)) > 0$ olsun. $f(x)$ polinomunda katsayıları yerine eşlenikleri konularak elde edilen polinom $\bar{f}(x)$ olsun. $f(x)\bar{f}(x)$ in her katsayısı reeldir. Bazı durumlarda $f(x)$ yerine bu polinom alınırsa katsayılarının reel olduğu kabul edilebilir. $f(x)$ in $\mathbb{C}$ üzerindeki parçalanma cismi K olmak üzere K, $f(x)(x^2 + 1)$ in $\mathbb{R}$ üzerindeki bir parçalanma cismidir. $kar(\mathbb{R}) = 0$ olduğundan K, $\mathbb{R}$ üzerinde ayrılabilir ve galoistir. $[K : \mathbb{R}] = [K : \mathbb{C}][\mathbb{C}: \mathbb{R}]$ ve $[\mathbb{C}: \mathbb{R}] = 2$ olduğundan $[K : \mathbb{R}]$ bir çift tam sayıdır. Yani $[K : \mathbb{R}] = 2^s t$ ve $(2, t) = 1$ olacak şekilde $s \geq 1, t \geq 1$ tam sayıları vardır. $G = G(K/\mathbb{R})$ olsun. K, $\mathbb{R}$ üzerinde galois olduğundan $|G| = 2^s t$ dir. G'nin bir Sylow 2 alt grubu P olsun. $|P| = 2^s$ dir. $E = K_P$ olsun. Teorem 1.11.14(iii)'den $[K : E] = |P| = 2^s$ dir. Buradan $[E: \mathbb{R}] = t$ bulunur. $u \in E$ ve $p(x) = \text{İ}nd(u, \mathbb{R})$ olsun. $[\mathbb{R}[u] : \mathbb{R}] = der(p(x))$ olduğundan $der(p(x))|t$ ve t bir tek tamsayı olduğundan Lemma 1.11.17'dan $p(x)$ in bir reel kökü vardır. Fakat $p(x)$, $\mathbb{R}$ üzerinde indirgenmez olduğundan, $der\big(p(x)\big) = 1$ ve $u \in \mathbb{R}$ dir. Buradan $E = \mathbb{R}$ bulunur. Böylece $|G| = 2^s$ ve $G = P$ dir. $H = G(K/\mathbb{C})$ olsun. $|H| = 2^{s-1}$ dir. $s - 1 \geq 1$ olmak üzere H'nin öyle bir alt grubu N vardır ki, $|H : N| = 2$ dir. $U = K_N$ olsun. $N \lhd H$ olduğundan Teorem 1.11.15 (iv) gereğince $U, \mathbb{C}$'nin bir galois genişlemesidir ve

$$[U : \mathbb{C}] = \frac{|G(K/\mathbb{C})|}{|G(K/U)|} = 2$$

dir. $\forall u \in U$ için $a, b, c \in \mathbb{C}$ olmak üzere bir $ax^2 + bx + c$ polinomunun köküdür. Ancak Lemma 1.11.15'den $x^2 + bx + c$'nin her kökü $\mathbb{C}$'nin içinde olduğundan $u \in \mathbb{C}$ buradan $U \subseteq \mathbb{C}$ olur, bu da çelişkidir. O halde $s - 1 = 0, s = 1$ ve $K = \mathbb{C}$ bulunur. Böylelikle $f(x)$ in $\mathbb{C}$ üzerindeki parçalanma cismi $\mathbb{C}$'dir.

## 1.12. Döngüsel Genişlemeler

Bu bölümde birimin bazı köklerinin F'ye eklenerek elde edilen bir F cisim genişlemeleri incelenecektir. Bulunan sonuçlar yardımıyla bir düzgün n-genin çizilebilir olması için gerek ve yeter şart verilecektir.

**Tanım 1.12.1.** F bir cisim ve $n \geq 1$ bir tamsayı olmak üzere $f(x) = x^n - 1_F \in F[x]$ olsun. $f(x)$ in F üzerindeki parçalanma cismi K ve $a \in K$ olmak üzere $a$, $f(x)$ in bir kökü ise $a$'ya F üzerinde *birimin bir n. kökü* denir. $a^n = 1_F$ ancak $\forall k | n$ için $a^k \neq 1_F$ ise $a$'ya F üzerinde *birimin bir ilkel n. kökü* denir.

$a \in K$ bir ilkel n. kök olmak üzere $H = \langle a \rangle$ ise $|H| = n$ dir. O halde H'nın elemanları $x^n - 1_F \in F[x]$ polinomunun bütün kökleridir. Böylece $b \in K$ bir ilkel n yinci kök ise $b^n - 1_F = 0_F$ olacağından $b \in H$ olup H devirli grubunun bir üretecidir. O halde ilkel n. kökler, Sonuç 1.2.7'den dolayı, $1 \leq k \leq n$ ve $(k, n) = 1$ olmak üzere $a^k$ lardan oluşur ve bunların sayısı $\phi(n)$ dir.

**Tanım 1.12.2.** $x^n - 1_F \in F[x]$ polinomunun F üzerinde parçalanış cismine F'nin *n. döngüsel genişlemesi* denir.

$kar(F) = 0$ ise ya da $kar(F) = p$ ve $p \nmid n$ ise F üzerinde ilkel n-yinci kökler vardır. Fakat $p | n$ ise F üzerinde ilkel n-yinci kök yoktur.

F bir cisim E, F'nin bir n. döngüsel genişlemesi, $n \in \mathbb{N}$ ve F cisminin karakteristiği $p > 0$ ise $p \nmid n$ olsun. $f(x) = x^n - 1_F$ polinomunun E içindeki her kökünün katlılığı birdir ve bu polinomun E içinde n tane kökü vardır. Böylelikle E içinde birimin n. köklerinin oluşturduğu devirli grup $U_n$ in mertebesi $n$'dir. Mertebesi n olan bir devirli grubun $\varphi(n)$ tane üreteci vardır. $\varphi(n)$, birimin n. ilkel köklerinin sayısıdır. $U_n = \{w_k : 0 \leq k \leq n-1\}$ n. ilkel köklerinin kümesidir.

$kar(F) > 0$ ve $p \nmid n$ olduğunda E, F üzerinde parçalanış cismidir ve $f(x)$, F üzerinde ayrılabilir olduğundan Sonuç 1.9.11 gereğince E, F cisminin bir ayrılabilir genişlemesidir; yani E bir normal genişlemedir. O halde $[E : F] = \{E : F\} = |G(E/F)|$ dir.

$G(E/F)$, $U(\mathbb{Z}_n)$ nin bir alt grubuna izomorftur. O halde $G(E/F)$ abelyandır ve mertebesi $\phi(n)$ yi böler.

Bundan sonra $kar(F) \nmid n$ olarak kabul edilecektir. Teorem 1.12.3(i)'den dolayı F üzerinde birimin ilkel n. kökleri vardır ve $w$ bir ilkel kök olmak üzere bütün ilkel kökler $1 \leq k \leq$ n ve $(k, n) = 1$ olmak üzere $w^k$ biçimindedir.

**Örnek 1.12.1.** $w \in \mathbb{C}$ bir ilkel dokuzuncu kök olsun. $z^9 - 1$ denkleminin dokuzuncu kökleri $z_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, $k = 0, 1, \dots, n-1$ şeklindedir. $U_n = \{1, z_1, z_2, \dots, z_n\}$ birimin dokuzuncu köklerinin kümesidir. İlkel n. kökler $1 \leq k \leq n$ ve $(k, n) = 1$ olmak üzere $w^k$ lardan oluşur; yani, $w^1$, $w^2$, $w^4$, $w^5$, $w^7$, $w^8$ dir ve $\phi(9) = 6$ dır.

**Tanım 1.12.3.** F cisminin bir n. dairesel genişlemesi E olsun. E içinde birimin bütün n. ilkel kökleri $w_i, 1 \leq i \leq \phi(n)$ olmak üzere

$\Phi_n(x) = \prod_{i=1}^{\phi(n)}(x - w_i)$

polinomuna F üzerinde *n. döngüsel polinom* denir.

**Teorem 1.12.4.** $\Phi_n(x) \in F[x]$ tir.

**İspat.** $\Phi_n(x)$ polinomunun katsayıları, F cisminin asal cisminin elemanlarıdır. Özel olarak F cisminin asal cismi $\mathbb{Q}$ ise $\Phi_n(x)$ polinomunun katsayıları $\mathbb{Z}$ halkasındadır; yani $\Phi_n(x) \in \mathbb{Z}$[x] tir.

**Teorem 1.12.6.** $\Phi_n(x)$, $F[x]$'in bir monik polinomudur.

**İspat.** $U_n$, E içinde birimin bütün n. köklerinin çarpımsal grubu olmak üzere $u \in U_n$ ise $u^n - 1 = 0$ olacağından $d|n$ için $o(u) = d$ dir. O halde $u$ birimin bir ilkel $d.$ köküdür ve $(x - u)|\Phi_d(x)$ tir. Tersine $d|n$ olmak üzere $u$ birimin bir ilkel d. kökü ise $u^n = 1$ olacağından $u \in U_n$ dir. O halde $\Phi_d(x)|(x^n - 1)$ dir. $e|n$ ve $d \neq e$ ise $\Phi_d(x)$ ile $\Phi_e(x)$ in hiçbir ortak kökü olamaz. Böylelikle

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

n üzerine tümevarım uygulanır ve ispat biter. $n = 1$ ise $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$ tir. $n > 1$ ve $\forall 1 \leq d < n$ için $\Phi_d(x),\ \mathbb{Z}[x]$ in bir monik polinomu olsun.

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

olarak alınırsa tümevarımdan $g(x) \in \mathbb{Z}[x]$ ve $x^n - 1 = g(x)\Phi_n(x)$ tir. $x^n - 1$ ve $g(x)$ monik olduğundan $x^n - 1 = q(x)g(x) + r(x)$ ve $der(r(x)) < der\big(g(x)\big)$ olacak şekilde $q(x),\ r(x) \in \mathbb{Z}[x]$ vardır ve $q(x)$ moniktir. Buradan

$$q(x)g(x) + r(x) = g(x)\Phi_n(x)$$

ve

$$r(x) = g(x)[\Phi_n(x) - q(x)]$$

$g(x) \neq 0$ ve $der(r(x)) \geq der\big(g(x)\big)$ olduğundan $[\Phi_n(x) - q(x)] \neq 0$ ise $r(x) \neq 0$ çelişkisi elde edilir. O halde $\Phi_n(x) - q(x) = 0$ ve $\Phi_n(x) = q(x) \in \mathbb{Z}[x]$ tir. $q(x)$ monik olduğundan $\Phi_n(x)$ de moniktir.

$x^n - 1 = \prod_{d|n} \Phi_d(x)$ eşitliğinden d'nin küçük değerleri için $\Phi_d(x)$ ifadeleri yazılabilir:

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

$$\Phi_2(x) = \frac{x^2 - 1}{x - 1} = x + 1$$

$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1$$

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

$$\Phi_5(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$$

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

$$\Phi_7(x) = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

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

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

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

**Teorem 1.12.6.** $\Phi_n(x)$ döngüsel polinomu $F = \mathbb{Q}$ için F üzerinde indirgenmezdir.

**İspat.** $f(x) = \Phi_n(x)$ ve Teorem 1.12.6'dan $f(x) \in \mathbb{Z}[x]$ tir. Varsayalım ki $f(x), \mathbb{Q}[x]$ içinde indirgenmez olsun. $f(x)$ in bir indirgenmez çarpanı $g(x)$ olmak üzere $der(g(x)) < \phi(n)$ dir. $f(x) = g(x)h(x)$ olacak şeklinde bir $h(x) \in \mathbb{Q}[x]$ vardır. $g(x), h(x) \in \mathbb{Z}[x]$ ve $f(x)$ monik olduğundan $g(x)$ ve $h(x)$ in de moniktir denebilir. $w$ bir n. ilkel kök olmak üzere $g(w) = 0$ olsun. $1 < p \leq n$ ve $p \nmid n$ olan her p asal sayısı için $g(w^p) = 0$ olduğu gösterilirse $g(x) = f(x)$ olur.

$p \nmid n$ olan bir p asal sayısı için $g(w^p) \neq 0$ olmak üzere $h(w^p) = 0$ olduğundan $w$, $h(x^p)$ nin bir köküdür ve $g(w) = 0$ olduğundan $(x - w)$, $g(x)$ ve $h(x^p)$ yi böler. $g(x)$ indirgenmez olduğundan $g(x)|h(x^p)$ dir. Öte yandan $g(x)$ monik olduğundan, $h(x^p) = g(x)t(x)$ olacak biçimde $t(x) \in \mathbb{Z}[x]$ vardır. $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x], \varphi\big(f(x)\big) = \bar{f}(x)$ şeklinde bir epimorfizma tanımlanırsa $\mathbb{Z}_p[x]$ içinde $\bar{h}(x^p) = \bar{g}(x)\bar{t}(x)$ olur. $\bar{g}(x)$ in $\mathbb{Z}_p[x]$ içinde bir indirgenmez çarpanı $\bar{d}(x)$ ise $\bar{d}(x)\big|\bar{h}(x^p)$ tir. $\bar{h}(x^p) = (\bar{h}(x))^p$ olduğundan $\bar{d}(x)\big|\bar{h}(x)$ olur. Öte yandan $f(x)|(x^n - 1)$ olduğundan $g(x)h(x)|(x^n - 1)$ ve $\bar{g}(x)\bar{h}(x)|(x^n - \bar{1})$ bulunur. Böylelikle $\overline{(d}(x))^2|(x^n - \bar{1})$ olur. O halde $(x^n - \bar{1})$ in en az iki katlı bir kökü vardır. Ancak $(x^n - \bar{1})' = nx^{n-1}$ ve $p \nmid n$ olduğundan $n\bar{1} \neq \bar{0}$ dır. Bu durumda $(x^n - \bar{1})'$ ın tek kökü $x = \bar{0}$ olduğundan $(x^n - \bar{1})'$ ile ortak kökü yoktur. Teorem 1.9.2 gereğince $x^n - \bar{1}$ in çok katlı kökü olamayacağından bu bir çelişkidir ve $g(w^p) = 0$ olmalıdır.

**Teorem 1.12.7.** $G(\mathbb{Q}(w)/\mathbb{Q})$ galois grubunun mertebesi $\phi(n)$ ve $G(\mathbb{Q}(w)/\mathbb{Q}) \cong U(\mathbb{Z}_n)$ dir.

**İspat.** $w$, $\mathbb{Q}$ üzerinde bir n. ilkel kök ise $\mathbb{Q}$'nun n. döngüsel genişlemesi $\mathbb{Q}(w)$'ye eşittir ve $\mathbb{Q}(w)$, $\mathbb{Q}$ cisminin bir galois genişlemesi olduğundan Teorem 1.12.6'dan dolayı $[\mathbb{Q}(w) : \mathbb{Q}] = |G(\mathbb{Q}(w)/\mathbb{Q})| = \phi(n)$ ve $G(\mathbb{Q}(w)/\mathbb{Q}) \cong U(\mathbb{Z}_n)$ dir.

**Sonuç 1.12.8.** $p$ bir asal sayı olsun. $\mathbb{Q}$'nun $p$. döngüsel genişlemesinin galois grubu, mertebesi $p-1$ olan bir devirli gruptur.

**İspat.** $\mathbb{Q}$'nun $p$. döngüsel genişlemesinin galois grubu G olmak üzere Teorem 1.12.7'den $|G(\mathbb{Q}(w)/\mathbb{Q})| = p-1$ ve $G(\mathbb{Q}(w)/\mathbb{Q}) \cong U(\mathbb{Z}_p)$ olduğundan $G(\mathbb{Q}(w)/\mathbb{Q})$ devirlidir.

$p$ bir asal tek sayı olmak üzere ancak $n = 1, 2, 4, p^r, 2p^r$ için n. ilkel kök vardır ve n'nin bu değerleri için $U(\mathbb{Z}_n)$ devirlidir.

**Tanım 1.12.9.** k negatif olmayan bir tam sayı olmak üzere $2^{2^k}+1$ biçimindeki bir asal sayıya *Fermat asal sayısı* denir.

**Örnek 1.12.2.** Euler $k = 0, 1, 2, 3, 4$ için $2^{2^k}+1$ biçimindeki sayıların asal sayı olduklarını göstermiştir. Bilinen Fermat asal sayıları $3, 5, 17, 257, 65537$ dir.

**Teorem 1.12.10.** $n \geq 1$ bir tam sayı olmak üzere $\phi(n)$ sayısı 2 nin bir kuvveti ise $k, t \geq 0$ ve $p_1,\ p_2, \dots, p_t$ birbirinden farklı fermat asal sayıları olmak üzere $n = 2^k p_1 p_2 \dots p_t$ dir.

**İspat.** Aritmetiğin temel teoremi gereği $k, t \geq 0$ ve $p_1,\ p_2, \dots, p_t$ birbirinden farklı asal sayılar ve $s_1, s_2, \dots, s_t \geq 1$ olmak üzere $n = 2^k p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$ şeklinde yazılabilir. Eşitliğin her iki yanına Euler fonksiyonu uygulanır:

$$\phi(n) = 2^{k-1} p_1^{s_1-1} p_2^{s_2-1} \dots p_t^{s_t-1}(p_1-1)(p_2-1)\dots(p_t-1).$$

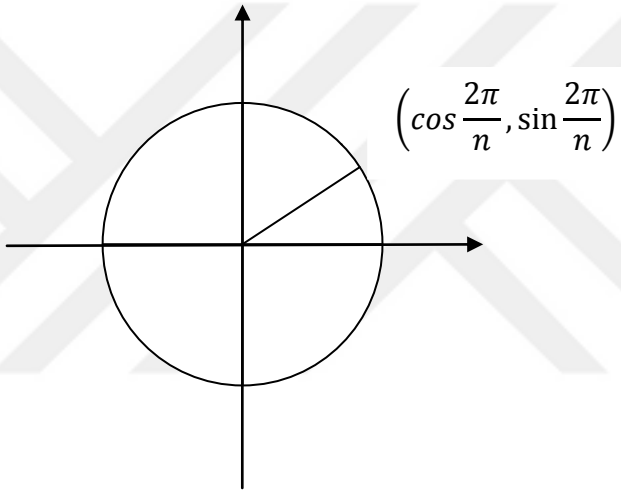
$\phi(n)$ sayısı 2 nin bir kuvveti olduğundan ve buradan $i = 1, \dots, t$ için $s_i = 1$ dir. $1 \leq i \leq t$ için $p_i - 1, 2$ nin bir kuvveti olduğundan $p_i - 1 = 2^m$ ve $p_i = 2^m + 1$ olacak şekilde $m \geq 1$ vardır. Eğer m sayısını bölen q asal tek sayısı varsa $m = qu$ olacak şekilde $u \geq 1$ tam sayısı vardır.

$$p_i = 2^m + 1 = 2^{qu} + 1 = (2^u)^q + 1 = (2^u + 1)[(2^u)^{q-1} + \dots + 2^u + 1]$$

$p_i$ nin asal olması ile çelişir. O halde $p = 2^m + 1$ in asal olması için $m = 2^a,\ a \geq 0$ ve $2^{2^a} + 1$ olmalıdır. O halde $p_i$ bir fermat asal sayısıdır.

**Teorem 1.12.11.** $n \geq 3$ bir tam sayı olmak üzere düzgün n-genin pergel ve cetvelle çizilebilmesi için gerek ve yeter şart $\varphi(n)$ in 2 sayısının bir kuvveti olmasıdır.

**İspat.** Düzgün n-genin çizilebilir olması için $\left(cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}\right)$ noktasının yani $w = cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ kompleks sayısının çizilebilir olması gerekir (Şekil 16).




**Şekil 16.** $w = cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ kompleks sayısının çizilebilir olduğunu gösteren koordinat düzlemi

Sonuç 1.6.10'dan $[\mathbb{Q}(w) : \mathbb{Q}] = 2^s$ olacak şekilde bir $s \geq 1$ tam sayısı vardır. Öte yandan Teorem 1.12.8'den dolayı $[\mathbb{Q}(w) : \mathbb{Q}] = \phi(n)$ olduğundan $\phi(n) = 2^s$ dir. Teorem 1.12.10'dan $k \geq 0$ ve $p_1,\ p_2, \dots, p_t$ birbirinden farklı fermat asal sayıları olmak üzere $n = 2^k p_1 p_2 \dots p_t$ dir.

Tersine $k \geq 0$ ve $p_1,\ p_2, \dots, p_t$ birbirinden farklı fermat asal sayıları olmak üzere $n = 2^k p_1 p_2 \dots p_t$ ise $\phi(n) = 2^s$ olacak şekilde bir $s \geq 1$ tam sayısı vardır. $E = \mathbb{Q}(w)$ ve $G = G(\mathbb{Q}(w)/\mathbb{Q}$ olsun. Teorem 1.12.8'den dolayı $[\mathbb{Q}(w) : \mathbb{Q}] = |G| = 2^s$ ve $G \cong U(\mathbb{Z}_n)$ dir. O halde G bir abelyan 2 grubudur. G bir 2-grubu olduğundan $o(a) = 2$

olacak şekilde bir $a \in G$ vardır. $G = \langle a \rangle$ ve $|H_1| = 2$ dir. $|G/H_1| = 2^{s-1}$ olduğundan, $G/H_1$ in mertebesi 2 olan bir alt grubu $H_2/H_1$ vardır. Aynı şekilde devam edilirse G'nin bir normal serisi

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_s = G$$

elde edilir; öyle ki, $\forall 0 \leq i < s$ için $|H_{i+1}/H_i| = 2$ dir. $\forall 0 \leq i < s$ için $E_i = E_{H_i}$ olmak üzere $E = E_0 > E_1 > \cdots > E_s = \mathbb{Q}$ cisim kulesi elde edilir. $\forall 0 \leq i < s$ için $E_i, \mathbb{Q}$ üzerinde galois olduğundan Teorem 1.11.6(iii)'den

$$[E_{i+1} : E_i] = [E : E_i]/[E : E_{i+1}] = |H_i/H_{i+1}| = 2.$$

$i$ üzerine tümevarım uygulanır. $\forall 0 \leq i < s$ için $E_i$ nin elemanlarının çizilebilir olduğu gösterilir. $i = 0$ için $\mathbb{Q}$'nun elemanları çizilebilirdir. $i \geq 0$ olmak üzere $E_i$ nin elemanlarının çizilebilir ve $u \in E_{i+1}$ olsun. $[E_{i+1} : E_i] = 2$ olduğundan $E_{i+1} = E_i(u)$ ve $\text{İnd}(u, E_1) = x^2 + bx + c$ olacak şekilde $b, c \in E_i$ vardır. Aynı zamanda $b, c$ çizilebilir olduğundan Sonuç 1.6.6'dan $u$ çizilebilirdir. O halde $E_{i+1}$ in her elemanı çizilebilirdir. Özel olarak $i = s$ için $E = E_s$ nin her elemanı çizilebilir olduğundan $w = cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$ çizilebilirdir.

**Örnek 1.12.3.** 17 fermat sal sayısı olduğundan Teorem 1.12.11 gereğince düzgün 17-gen derecesiz pergel ve derecesiz cetvelle çizilebilir.

**Örnek 1.12.4.** $\cos 72° + i \sin 72°$ birimin bir onuncu ilkel kökü değildir. $z^n - 1$ denkleminin kökleri $z_k = \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}$ şeklindedir. $n > 10$ olsun. $w^k = z_k$ için $k = 10$ alınırsa $z_{10} = \cos\frac{20\pi}{n} + i \sin\frac{20\pi}{n}$ bir ilkel kök olur. $\frac{20\pi}{n} = 72$ ise $n = 50$ olur. $w^{10} = z_{10} = 1_F$ birimin ilkel onuncu kökü olması için $10|50$ ve $w^{50} \neq 1_F$ olmalıdır. $w^{50} = (w^{10})^5 = (1_F)^5 = 1_F$ çelişkisi elde edilir.

**Örnek 1.12.5.** k bir pozitif tamsayı ve p bir asal sayı olsun. $\Phi_{p^k}(x) = \Phi_p\left(x^{p^{k-1}}\right)$ olduğu aşağıda gösterilmiştir.

$\Phi_{p^k}(x) = \prod_{i=1}^{\phi(p^k)}(x - w_i) = (x - w_1)(x - w_2) \ldots (x - w_{p-1})$ ve

$\Phi_p\left(x^{p^{k-1}}\right) = \prod_{i=1}^{\phi(p)}(x^{p^{k-1}} - w_i) = \left(x^{p^{k-1}} - w_1\right)\left(x^{p^{k-1}} - w_2\right)\ldots(x^{p^{k-1}} - w_{p-1})$

dır. Her $a_i$ bir $p^k$-yıncı ilkel kök olduğundan $a_i^{p^{k-1}}$ de bir p-yinci ilkel köktür. Dolayısıyla $\Phi_p\left(a_i^{p^{k-1}}\right) = 0$ dır. Böylece $a_i$ ler $\Phi_p\left(x^{p^{k-1}}\right)$ in birbirinden farklı $p^{k-1}(p-1)$ köküdür. Aynı zamanda $\Phi_{p^k}(x)$'ninde köküdür. O halde $\Phi_{p^k}(x)$ ve $\Phi_p\left(a_i^{p^{k-1}}\right)$ dereceleri aynı olan monik polinomlardır ve birbirine eşittir. Bu eşitlik kullanılarak $\Phi_{25}(x)$ şu şekilde hesaplanır:

$\Phi_{25}(x) = \Phi_{5^2}(x) = \Phi_5\left(x^{5^1}\right) = \Phi_5(x^5) = x^{20} + x^{15} + x^{10} + x^5 + 1.$

**Örnek 1.12.6.** m ve n aralarında asal pozitif tamsayılar olsun. $x^{mn} - 1$ in $\mathbb{Q}$ üzerindeki parçalanma cisminin $(x^m - 1)(x^n - 1)$ parçalanma cismine eşittir. Örnek olarak $n = 2$ ve $m = 3$ alınsın. $(3,2) = 1$ dir. $x^6 - 1$ 'nin kökleri $z_k = \cos\frac{2k\pi}{6} + i\sin\frac{2k\pi}{6}$ şeklindedir. $z_1 = \frac{1}{2}\left(1 + \sqrt{3}i\right)$, $z_2 = \frac{1}{2}\left(-1 + \sqrt{3}i\right)$, $z_3 = -1$, $z_4 = -\frac{1}{2}\left(1 + \sqrt{3}i\right)$, $z_5 = \frac{1}{2}\left(1 - \sqrt{3}i\right)$, $z_0 = 1$ denklemin kökleridir. $\frac{1}{2}\left(1 + \sqrt{3}i\right) \in \mathbb{Q}(\sqrt{3}, i)$ olduğundan parçalanma cismi $\mathbb{Q}(\sqrt{3}, i)$ dir. $x^2 - 1$ denkleminin kökleri $\pm 1$ dir ve parçalanma cismi $\mathbb{Q}$'dur. $x^3 - 1$ denkleminin kökleri $z_1 = \frac{1}{2}\left(-1 + \sqrt{3}i\right), z_2 = -\frac{1}{2}\left(1 + \sqrt{3}i\right), z_0 = 1$ dir ve parçalanma cismi $\mathbb{Q}(\sqrt{3}, i)$ dir. O halde $(x^2 - 1)(x^3 - 1)$ 'in parçalanma cismi $\mathbb{Q}(\sqrt{3}, i)$ dir.

**Örnek 1.12.7.** $n > 1$ bir tek tamsayı olsun. $\Phi_{2n}(x) = \Phi_n(-x)$ olduğu aşağıda gösterilmiştir.

n üzerine tümevarım uygulanır. $n = 3$ için $\Phi_3(-x) = (-x)^2 + (-x) + 1 = x^2 - x + 1$ ve $\Phi_6(x) = x^2 - x + 1$ doğrudur. $n = k$ için doğru olsun. $\Phi_k(-x) = \frac{(-x)^k - 1}{\Phi_1(-x)\Phi_{s_1}(-x)\ldots\Phi_{s_i}(-x)}$, $i \geq 1$ $k = s_1 \ldots s_i$ olacak şekilde $s_1 \ldots s_i$ asal sayıları vardır. $\Phi_{2k}(x) = \frac{x^{2k} - 1}{\Phi_1(x)\Phi_2(x)\Phi_{s_1}(x)\ldots\Phi_{s_i}(x)}$ dir.

$\Phi_k(-x) = \Phi_{2k}(x)$

$$\Rightarrow \frac{(-x)^k - 1}{\Phi_1(-x)\Phi_{s_1}(-x)\ldots\Phi_{s_i}(-x)} = \frac{x^{2k} - 1}{\Phi_1(x)\Phi_2(x)\Phi_{s_1}(x)\ldots\Phi_{s_i}(x)} = \frac{-(x^k - 1)((-x)^k - 1)}{\Phi_1(x)\Phi_2(x)\Phi_{s_1}(x)\ldots\Phi_{s_i}(x)}$$

sadeleştirmeler yapılırsa

$\frac{-(x^k-1)}{\Phi_2(x)} = 1$

olduğundan $-(x^k - 1) = \Phi_2(x)$ dir.

$n = k + 2$ için

$$\Phi_{k+2}(-x) = \frac{(-x)^{k+2}-1}{\Phi_1(-x)\Phi_{t_1}(-x)\dots\Phi_{t_j}(-x)}, j \geq 1 \;\; k+2 = t_1 \dots t_j$$

olacak şekilde $t_1 \dots t_j$ asal sayıları vardır.

$$\Phi_{2k+4}(x) = \frac{x^{2k+4}-1}{\Phi_1(x)\Phi_2(x)\Phi_{s_1}(x)\dots\Phi_{s_i}(x)}$$

$$\frac{(-x)^{k+2}-1}{\Phi_1(-x)\Phi_{t_1}(-x)\dots\Phi_{t_j}(-x)} = \frac{x^{2k+4}-1}{\Phi_1(x)\Phi_2(x)\Phi_{s_1}(x)\dots\Phi_{s_i}(x)}$$

için $-(x^{k+2} - 1) = \Phi_2(x)$ olduğundan $\Phi_{k+2}(-x) = \Phi_{2k+4}(x)$ dir.

### 1.13. Köklerle Çözülebilirlik

Bu bölümde n. dereceden rasyonel cisim katsayılı $a_n x^n + \dots + a_1 x + a_0 = 0$ polinom denkleminin hangi şartlar altından köklerle çözümünün mümkün olduğu incelenecektir.

*2. ve 3. dereceden polinom denklemlerin köklerle çözümü* için formüller sırasıyla aşağıda belirtilmiştir.

(a) $ax^2 + bx + c = 0,\ a, b, c \in \mathbb{Q}$ ve $a \neq 0$ olsun. $a = 1$ alınır ve $x^2 + bx + c = 0$ denkleminde $x = y - \frac{b}{2}$ yerine yazılırsa

$$\left(y - \frac{b}{2}\right)^2 + b\left(y - \frac{b}{2}\right) + c = y^2 - by + \frac{b^2}{4} + by - \frac{b^2}{2} + c = y^2 - \frac{b^2}{4} + c = 0.$$

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

polinomun kökleridir. $b^2 - 4c \geq 0$ ise kökler reel, $b^2 - 4c < 0$ ise komplekstir.

(b) $a, b, c \in \mathbb{Q}$ olmak üzere $x^3 + ax^2 + bx + c = 0$ olsun. Bu denklemde $x = y - \frac{a}{3}$ yerine yazılırsa gerekli işlemlerden sonra

$$y^3 + \left(-\frac{a^2}{3} + b\right)y + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right) = 0$$

bulunur. $p = -\frac{a^2}{3} + b,\ q = \frac{2a^3}{27} - \frac{ab}{3} + c$ yazılırsa,

$$y^3 = (u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = u^3 + v^3 + 3uvy$$

Önceki denklemde yerine yazılırsa

$$u^3 + v^3 + (3uv + p)y + q = 0$$

$3uv + p = 0$ ve $uv = -\frac{p}{3}$ olmak üzere

$u^3 + v^3 = -q$ ve $u^3v^3 = -\frac{p^3}{27}$

O halde $u^3$ ve $v^3$

$$x^2 + qx - \frac{p^3}{27} = 0$$

ikinci dereceden denklemin kökleridir.

$$u^3 = \frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right),\ \ v^3 = \frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right).$$

$u^3v^3 = -\frac{p^3}{27}$ denkleminin kökleri $(u, v)$ sıralı ikilisi bir kök olmak üzere $(u, v)$, $(u, wv), (u, w^2v), (wu, v), (wu,\ wv),\ (wu, w^2v), (w^2u, wv),\ (w^2, wv), (w^2u,\ w^2v)$ dir. $w = \frac{-1+i\sqrt{3}}{2}$ olmak üzere bileşenleri çarpımı $-\frac{p}{3}$ e eşit olanlar $(u, v), (wu, w^2v)$ ve $(w^2u,\ wv)$ dir. $y^3 + py + q = 0$ denkleminin kökleri $u + v, wu + w^2v, w^2u + wv$ dir. üçüncü dereceden denklemin kökleri

$$x_1 = u + v - \frac{a}{3},\ \ x_2 = wu + w^2v - \frac{a}{3},\ \ \ x_3 = w^2u + wv - \frac{a}{3}$$

Bu formüllere *CardanoFormülleri* denir.

**Örnek 1.13.1.** $x^3 - 3x + 1$ polinomunun köklerini Cardano formülleriyle çözümü aşağıdaki gibi bulunur.

$p = -3$ ve $q = 1$ dir. Bu değerler

$$u = \left[\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)\right]^{1/3}, v = \left[\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)\right]^{1/3}$$

Eşitliklerinde yerine yazılırsa $u = \left[\frac{1}{2}\left(-1 + \sqrt{1^2 + \frac{4(-3)^3}{27}}\right)\right]^{1/3} = [\frac{1}{2}(-1 + i\sqrt{3})]^{1/3}$ ve $v = [\frac{1}{2}(-1 - i\sqrt{3})]^{1/3}$ olarak bulunur. Dolayısıyla f$(x)$'in kökleri $w = \frac{-1+i\sqrt{3}}{2}$ olmak üzere,

$$x_1 = \sqrt[3]{\frac{1}{2}(-1 + i\sqrt{3})} + \sqrt[3]{\frac{1}{2}(-1 - i\sqrt{3})}$$

$$x_2 = \sqrt[3]{\frac{1}{2}(-1 + i\sqrt{3}w)} + \sqrt[3]{\frac{1}{2}(-1 - i\sqrt{3}w^2)}$$

$$x_3 = \sqrt[3]{\frac{1}{2}(-1 + i\sqrt{3}w^2)} + \sqrt[3]{\frac{1}{2}(-1 - i\sqrt{3}w)}$$

olarak bulunur. $\frac{1}{2}(-1 + i\sqrt{3}) = \cos\frac{2\pi}{3} + isin\ \frac{2\pi}{3}$ sayısının bir küp kökü, $t = \cos\frac{2\pi}{9} + isin\ \frac{2\pi}{9}$ olduğundan $\sqrt[3]{u} = t$ ve $\sqrt[3]{v} = \bar{t}$ dır. Buradan

$$\sqrt[3]{u} + \sqrt[3]{v} = t + \bar{t} = 2\cos\frac{2\pi}{9},$$

$$\left(\cos\frac{\pi}{3} + isin\ \frac{\pi}{3}\right)\left(\cos\frac{2\pi}{9} + isin\ \frac{2\pi}{9}\right) = \cos\frac{8\pi}{9} + isin\ \frac{8\pi}{9}$$

olduğundan

$$\sqrt[3]{u}w + \sqrt[3]{v}w^2 = \left(\cos\frac{8\pi}{9} + isin\ \frac{8\pi}{9}\right) + \left(\cos\frac{8\pi}{9} - isin\ \frac{8\pi}{9}\right) = 2\cos\frac{8\pi}{9}$$

ve

$$\left(\cos\frac{\pi}{3} - isin\ \frac{\pi}{3}\right)\left(\cos\frac{2\pi}{9} + isin\ \frac{2\pi}{9}\right) = \cos\left(-\frac{\pi}{9}\right) + isin\ \left(-\frac{\pi}{9}\right)$$

olduğundan

$$\sqrt[3]{u}w^2 + \sqrt[3]{v}w = \left(\cos\frac{\pi}{9} - isin\ \frac{\pi}{9}\right) + \left(\cos\frac{\pi}{9} + isin\ \frac{\pi}{9}\right) = 2\cos\frac{5\pi}{9}$$

bulunur. O halde denklemin bütün kökleri

$$x_1 = 2\cos\frac{2\pi}{9}\ ,\quad x_2 = 2\cos\frac{8\pi}{9}\ ,\qquad x_3 = 2\cos\frac{\pi}{9}$$

olup kökler reeldir.

**Tanım 1.13.1.** F bir cisim ve E, F'nin sonlu cisim genişlemesi olsun. $n_1 \in \mathbb{N}$ olmak üzere $a_1$, $p_1(x) = x^{n_1} - {a_1}^{n_1} \in F[x]$ polinomunun $i = 2, \dots, r$ için $n_i \in \mathbb{N}$ olmak üzere $a_i$, $p_i(x) = x^{n_i} - {a_i}^{n_i} \in F(a_1, \dots, a_{i-1})[x]$ polinomunun bir kökü ve $1 \le i \le r$ için $F_i = F_{i-1}(a_i)$ olmak üzere $F_1, \dots, F_r$ cisim genişlemelerinin $F = F_0 \le F_1 \le \cdots \le F_r = E$ özelliğinde bir cisim kulesi varsa bu kuleye *kök kulesi,* E'ye de F cisminin bir *kök genişlemesi* denir.

**Tanım 1.13.2.** F bir cisim, $der(f(x)) \ge 1$ ve K, $f(x)$ in F üzerindeki bir parçalanma cismi olsun. Eğer F cisminin bir K kök genişlemesi varsa $f(x) = 0_F$ denklemi *F cismi üzerinde köklerle çözülebilir* denir.

Tanım 1.13.1'den $\forall 1 \le i < t$ için $u_i^{n_i} = a_i$ konulursa $u_i, x^{n_i} - a_i = 0$'ın bir çözümü olur. Burada $u_i = \sqrt[n_i]{a_i}$ yazılırsa $E = F\left(\sqrt[n_1]{a_1},\ \sqrt[n_2]{a_2}, \dots, \sqrt[n_t]{a_t}\right)$ dır. $f(x) = 0_F$ denkleminin E içindeki çözümleri $\sqrt[n_1]{a_1},\ \sqrt[n_2]{a_2}, \dots, \sqrt[n_t]{a_t}$ köklerinin monomlarının F lineer kombinasyonları olur.

**Örnek 1.13.2.** $x^6 - 1 \in \mathbb{Q}[x]$ polinomunun parçalanma cismi K olsun. birimin bir ilkel beşinci kökü $w$ olmak üzere K = $\mathbb{Q}$(w), $\mathbb{Q}$'nun K'yı içeren bir kök genişlemesi ve bu polinomun köklerle çözülebilir olduğu aşağıda gösterilmiştir.

$w \in K$ bir ilkel altıncı kök olsun. $z^6 = 1$ denkleminin kökleri $z_k = \cos\frac{2k\pi}{6} + i\sin\frac{2k\pi}{6}, k = 0, \dots, 5$ ile bulunur. $w^k = z_k$ olmak üzere $w = z_1 = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6} = \frac{1}{2}\left(1 + i\sqrt{3}\right)$ olarak bulunur. K = $\mathbb{Q}$(w) = $\mathbb{Q}\left(\sqrt{3}, i\right)$ dir. Tanım 1.13.1 den $F_0 = \mathbb{Q}$, $F_1 =$

$F_0(z_1) = \mathbb{Q}(\sqrt{3}, i) = K$ bulunur. $F_0 = \mathbb{Q} \leq F_1 = F_0(z_1) = \mathbb{Q}(\sqrt{3}, i) = K$ cisim kulesi elde edilir. K'ya F'nin bir kök genişlemesi denir. $w \in K, f(w) = w^6 - 1 = 0$ ve denklemin bütün kökleri K içinde olduğundan $\mathbb{Q}$ üzerinde köklerle çözülebilirdir.

**Örnek 1.13.3.** $x^5 + 32 \in \mathbb{Q}[x]$ polinomunun $\mathbb{Q}$ üzerindeki galois grubu ve bu polinomun $\mathbb{Q}$ üzerinde köklerle çözülebilir olduğu aşağıda gösterilmiştir.

$x^5 + 32 \in \mathbb{Q}[x]$ polinomunun bir kökü $-2$ olduğundan $w$ bir ilkel kök olmak üzere bütün kökler $-2, -2w, -2w^2, -2w^3, -2w^4$ ve böylece $\mathbb{Q}(w)$ parçalanma cismi ve $\mathbb{Q}$'nun bir kök genişlemesidir. Dolayısıyla $x^5 + 32 = 0$ denklemi köklerle çözülebilirdir. $\sigma(w) = -2w$ olarak tanımlansın. Lemma 1.13.5'ten $o(\sigma) = 4$ ve $G(\mathbb{Q}(w)/\mathbb{Q}) = \langle w \rangle$ dir. Galois grubu devirlidir.

**Lemma 1.13.3.** $F \leq B \leq L$ bir cisim kulesi, F sıfır karakteristikli bir cisim ve L, F'nin bir sonlu cisim genişlemesi ve B, F'nin bir normal genişlemesi olsun. $v \in L$ ve $k \geq 1$ için $L = B(v)$ ve $v^k \in B$ olmak üzere L'nin öyle bir cisim genişlemesi N vardır ki B'nin bir kök genişlemesi ve F'nin bir normal genişlemesidir.

**İspat.** Teorem 1.8.10'dan B, F üzerinde bir $g(x) \in F[x]$ in parçalanma cismidir. $p(x) = \text{İ}nd(v, F)$ ve N, $g(x)p(x)$ in F üzerindeki bir parçalanma cismi olsun. Teorem 1.8.10'dan N, F üzerinde normaldir ve $B \leq L \leq N$ dir. $p(x)$ in N içindeki bütün kökleri $v = v_1, .., v_k$ olsun. $\forall 1 \leq i \leq k$ için $\psi_{v_1, v_i} : F(v_1) \to F(v_i)$ temel izomorfizması Sonuç 1.8.5'ten N'nin bir $\tau_i$ otomorfizmasına genişler. Böylece $\tau_i$, F'yi sabit bırakır, $\tau_i(v) = v_i$ dir ve B, F üzerinde parçalanma cismi olduğunan Teorem 1.9.6'dan $\tau_i(B) = B$ dir.

$$B = B_0 \leq B(v_1) \leq B(v_1, v_2) \leq \cdots \leq B(v_1, .., v_t) = N$$

cisim kulesi $\forall 1 \leq i \leq t$ için $v_i^k = \tau_i(v_1)^k = \tau_i(v_1^k) \in B \leq B_{i-1}$ olduğundan bir kök kulesi olduğundan N, B'nin bir kök genişlemesidir.

**Lemma 1.13.4.** F karakteristiği sıfır olan bir cisim ve $der(f(x)) \geq 1$ olsun. $f(x) = 0_F$ denklemi F üzerinde köklerle çözülebilir ise F cisminin öyle bir normal kök genişlemesi N vardır ki N, $f(x)$ in F üzerindeki bir parçalanma cismini içerir.

**İspat.** K, $f(x)$ polinomunun F üzerinde bir parçalanma cismi olsun. Hipotezden F'nin K'yı içeren bir kök genişlemesi E vardır. E, F'nin bir kök genişlemesi olduğundan E'nin öyle $u_1, u_2, \dots, u_t$ elemanları ve öyle $n_1, n_2, \dots, n_t$ pozitif tamsayıları vardır ki, $F_0 = F$ ve $\forall 1 \leq i \leq t$ için $F_i = F_{i-1}(u_i)$ olmak üzere $u_i^{n_i} \in F_{i-1}$'dır. $F = F_0 \leq F_1 \leq \cdots \leq F_t = E$ bir kök kulesidir.

Lemma 1.13.3'te $B = F$ ve $L = F_1$ alınırsa F'nin $F_i$ i içeren bir normal kök genişlemesi $N_1$ ve $u_2^{n_2} \in F_1 \leq N_1$ dir. Öte yandan $F_1(u_2)$ tanımlı olduğundan $N_1(u_2)$ tanımlıdır ve $F_2 = F_1(u_2) \leq N_1(u_2)$ dir. Lemma 1.13.3'te $B = N_1$ ve $L = N_1(u_2)$ alınırsa F'nin $N_1(u_2)$ yi içeren öyle bir normal genişlemesi $N_2$ bulunur ki; $N_2$, $N_1$ in, dolayısıyla F'nin, bir kök genişlemesidir. Aynı biçimde F'nin $F_t$ yi içeren bir normal kök genişlemesi $N_t$ ve $K \leq F_t$ olduğundan $K \leq N_t$ dir.

**Lemma 1.13.5.** F, $kar(F) = 0$ olan bir cisim olsun ve birimin bir ilkel n-yinci kökünü kapsasın ve $a \in F$ olmak üzere $x^n - a$ polinomunun F'nin bir cisim genişlemesi içindeki bir kökü $u$ olsun. Aşağıdakiler sağlanır.

(i) $F(u)$, F'nin bir galois genişlemesidir.
(ii) $G(F(u)/F)$ galois grubu devirlidir.

**İspat.**

(i) F içinde birimin bir ilkel n-yinci kökü $w$ olsun. $x^n - a$'nın bir kökü $u$ olduğundan bütün kökler $u, wu, \dots, w^{n-1}u$'dur. $F(u, wu, \dots, w^{n-1}u) = F(u)$ olduğundan $F(u)$, F üzerinde $x^n - a$ nın bir parçalanma cismidir. Karakteristiği sıfır olduğundan $F(u)$, F üzerinde Galois genişlemesidir.

(ii) $G = G(F(u)/F)$ ve $\sigma \in G$ olsun. $\sigma(u), f(x)$ in bir kökü olduğundan, $\sigma(u) = w^k u$ olacak şekilde $0 \leq k < n$ vardır ve $\sigma = \sigma_k$ yazılabilir. $\psi : G \to \langle w \rangle, \sigma_k \mapsto w^k$ şekilde bir fonksiyon tanımlansın. $0 \leq s, t < n$ olmak üzere $\sigma_s$, $\sigma_t \in G$ olsun. $s + t \equiv r(mod\ n)$ olacak şekilde $0 \leq r < n$ vardır.

$(\sigma_s \sigma_t)(u) = w^s w^t u = w^{s+t} u = w^r u = \sigma_r(u)$

olduğundan $\sigma_s \sigma_t = \sigma_r$ dir. $\psi(\sigma_s \sigma_t) = \psi(\sigma_r) = w^r$ ve $\psi(\sigma_s)\psi(\sigma_t) = w^s w^t = w^r$ olduğundan $\psi(\sigma_s \sigma_t) = \psi(\sigma_s)\psi(\sigma_t)$ dir. O halde $\psi$ bir grup homomorfizmasıdır. Aynı şekilde $\psi$ birebirdir. G, $\langle w \rangle$ nun bir alt grubuna izomorf olduğundan devirlidir.

**Teorem 1.13.6.** F, $kar(F) = 0$ olan bir cisim ve E, F'nin bir normal kök genişlemesi ise $G(E/F)$ galois grubu çözülebilirdir.

**İspat.** Hipotezden E, bir $g(x) \in F[x]$ in F üzerindeki parçalanma cismidir ve $u_1, u_2, \dots, u_t \in E$ ve $n_1, n_2, \dots, n_t \in \mathbb{Z}^+$ vardır. $F_0 = F$ ve $\forall 1 \leq i \leq t$ için $F_i = F_{i-1}(u_i)$ ise $\forall 1 \leq i \leq t$ için $u_i^{n_i} \in F_{i-1}$ ve $F = F_0 \leq F_1 \leq \cdots \leq F_t = E$ bir kök genişlemesidir.

$n_1, n_2, \dots, n_t$ pozitif tamsayılarının ekoku $n$ ve F üzerinde birimin bir ilkel n-yinci kökü $w$ olsun. $\forall 1 \leq i \leq t$ için $L_i = F_i(w)$ olmak üzere $\forall 1 \leq i \leq t$ için $L_i = F_i(w) = F_{i-1}(u_i)(w) = F_{i-1}(u_i, w) = F_{i-1}(w)(u_i) = L_{i-1}(u_i)$, $u_i^{n_i} \in F_{i-1} \leq L_{i-1}$ ve $w^n \in F$ olduğundan $F \leq L_0 \leq L_1 \leq \cdots \leq L_t = L$, F'nin bir kök genişlemesidir. $L_0 = F(w), x^n - 1_F$ nin F üzerindeki bir parçalanma cismi olduğundan L, $g(x)(x^n - 1_F)$ in F üzerindeki bir parçalanma cismidir. $kar(F) = 0$ olduğundan L, F'nin bir galois genişlemesidir.

$$G(L/F) \geq G(L/L_0) \geq \cdots \geq G(L/L_t) = \{1\}$$

azalan grup zinciri göz önüne alınırsa $\forall 1 \leq i < t$ için $G(L/L_{i+1}) \lhd G(L/L_i)$ ve $G(L/L_i)/G(L/L_{i+1})$ bölümünün grubunun devirli olduğu gösterilir.

Teorem 1.12.3(ii)'den $L_0 = F(w)$, F'nin bir Galois genişlemesidir ve $\forall 1 \leq i < t$ için için $n_i | n$ olduğundan birimin bir ilkel $n_i$-yinci kökünü içerir. Teorem 1.13.5'ten $\forall 1 \leq i < t$ için $L_{i+1}, L_i$ nin bir galois genişlemesidir ve $G(L_{i+1}/L_i)$ devirlidir. Bu durumda Teorem 1.11.6(iv)'den $G(L/L_{i+1}) \lhd G(L/L_i)$ ve $G(L_{i+1}/L_i) \cong G(L/L_i)/G(L/L_{i+1})$ dır. Ayrıca her $1 \leq i < t$ için $G(L_{i+1}/L_i)$ devirli olduğundan $G(L/L_i)/G(L/L_{i+1})$ de devirlidir. O halde Tanım 1.2.11 gereğince $G(L/L_0)$ çözülebilirdir. Öte yandan $L_0 = F(w)$, F üzerinde bir n-yinci dairesel genişleme olduğundan Teorem 1.12.3 gereğince $L_0$, F'nin bir Galois genişlemesidir ve $G(L_0/F)$ abelyandır. Bu durumda $G(L_0/F) \cong G(L/F)/G(L/L_0)$ ve $G(L/L_0)$ çözülebilir olduğundan Teorem 1.2.16 gereğince $G(L/F)$ çözülebilirdir.

**Teorem 1.13.7.** F karakteristiği sıfır olan bir cisim, $der(f(x)) \geq 1$ ve K, $f(x)$ polinomunun F üzerindeki bir parçalanma cismi olsun. $f(x) = 0_F$ denklemi F üzerinde köklerle çözülebilir ise $G(K/F)$ galois grubu çözülebilirdir.

**İspat.** $f(x) = 0_F$ denklemi F üzerinde köklerle çözülebilir olduğu kabul edilsin. Lemma 1.13.4'ten F cisminin öyle bir normal kök genişlemesi N vardır ki, $K \leq N$ dir. Teorem 1.13.6'dan $G(N/F)$ Galois grubu çözülebilirdir. Öte yandan karakteristiği sıfır olduğundan K, F cisminin bir galois genişlemesidir. Bu durumda Teorem 1.11.6(iv)'den $G(K/F) \cong G(N/F)/G(N/K)$ olduğundan Teorem 1.2.13 gereğince $G(K/F)$ çözülebilirdir.

**Teorem 1.13.8.** F karakteristiği sıfır olan bir cisim ve E, F'nin bir galois genişlemesi olmak üzere $G(E/F)$ grubu çözülebilir ise F cisminin E cismini içeren bir kök genişlemesi vardır.

**Teorem 1.13.9.** *(Abel-Ruffini)* Beşinci dereceden köklerle çözülemeyen bir $f(x) \in \mathbb{Q}[x]$ polinomu vardır.

**İspat.** $f(x) = x^5 - 6x + 3$ polinomunun $\mathbb{Q}$ üzerinde köklerle çözülebilir olmadığı aşağıda gösterilmiştir.

$x^5 - 6x + 3$, $\mathbb{Q}$ üzerinde indirgenmezdir. Gerçekten $p = 5$ için Eisenstein indirgenmezlik kriterine göre $f(x)$ indirgenmezdir.

$f(x)$'in üç reel kökü ve iki reel olmayan kompleks kökü vardır. $f(x)$ in türevi alınırsa $f'(x) = 5x^4 - 6 = 0 \Rightarrow 5x^4 = 6 \Longrightarrow x = \sqrt[4]{6/5}$, $x = -\sqrt[4]{6/5}$ bulunur. $f$ fonksiyonu, $(-\infty, -\sqrt[4]{6/5}]$ aralığında artan, $\left[-\sqrt[4]{6/5}, \sqrt[4]{6/5}\right]$ aralığında azalan ve $\left[\sqrt[4]{6/5}, \infty\right)$ aralığında artandır. $f(-2) = -17 < 0$ ve $f\left(-\sqrt[4]{6/5}\right) > 0$ olduğundan bir $a_1 \in \left(-2, -\sqrt[4]{6/5}\right)$ için $f(a_1) = 0$ dır. $f\left(-\sqrt[4]{6/5}\right) > 0$ ve $f\left(\sqrt[4]{6/5}\right) < 0$ olduğundan bir $a_2 \in \left(-\sqrt[4]{6/5}, \sqrt[4]{6/5}\right)$ için $f(a_2) = 0$ dır. Son olarak $f\left(\sqrt[4]{6/5}\right) < 0$ ve $f(2) > 0$ olduğundan bir $a_3 \in \left(\sqrt[4]{6/5}, 2\right)$ için $f(a_3) = 0$ dır. Böylece $f(x)$ in bütün reel kökleri $a_1$, $a_2$ ve $a_3$ tür. $f(x)$ in reel olmayan kompleks kökleri $b_1$ ve $b_2$ olsun. O zaman $f(x)$ in parçalanma cismi $K = \mathbb{Q}(a_1, a_2, a_3, b_1, b_2)$ olur. Eğer G'nin çözülebilir olmadığı gösterilirse Teorem 1.13.7'den dolayı, $f(x)$ köklerle çözülemez.

$G \cong S_5$ bulunur. $S_5$ çözülebilir olmadığından G de çözülebilir değildir. O halde Teorem 1.13.7 gereğince $f(x)$ polinomu $\mathbb{Q}$ üzerinde köklerle çözülemez.

**Örnek 1.13.4.** $F$ bir cisim ve $kar(F) \neq 2$ olsun. $ax^2 + bx + c, a \neq 0_F$ polinomunun parçalanma cismi $F\left(\sqrt{b^2 - 4ac}\right)$ bir kök genişlemesi olduğu aşağıda gösterilmiştir.

$f(x) = ax^2 + bx + c, a$ ile bölünürse $\frac{f(x)}{a} = x^2 + px + q, p = \frac{b}{a}, q = \frac{c}{a}$ olacak şekilde $\frac{f(x)}{a} = g(x)$ polinomu tanımlansın. $g(x)$ in kökleri $x_{1,2} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$ şeklindedir. $p$ ve $q$ yerine yazılırsa $x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ elde edilir. $F \leq F\left(\sqrt{b^2 - 4ac}\right)$ ve $(\sqrt{b^2 - 4ac})^2 = b^2 - 4ac \in F$ olduğundan $\left(\sqrt{b^2 - 4ac}\right)$, F'nin bir kök genişlemesidir ve $x_1, x_2 \in F\left(\sqrt{b^2 - 4ac}\right)$ olduğundan $\frac{f(x)}{a} = g(x)$ denklemi F üzerinde köklerle çözülebilirdir.

## 1.14. Simetrik Fonksiyonlar

**Tanım 1.14.1.** $\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \in F(x_1, x_2, \ldots, x_n)$ ve her $\sigma \in S_n$ olmak üzere

$$\bar{\sigma}\left(\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}\right) = \frac{f\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right)}{g\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right)} = \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}$$

ise $\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}$ ye *F üzerinde* $x_1, \ldots, x_n$ *nin bir simetrik fonksiyonu* denir.

Bütün simetrik fonksiyonlar $\overline{S_n}$ nin $F(x_1, x_2, \ldots, x_n)$ içindeki sabit cismini oluşturur ve bu cisim K olsun.

$F(x_1, x_2, \ldots, x_n)$ üzerinde bir $t$ belirsizinin polinom halkası $F(x_1, x_2, \ldots, x_n)[t]$ ve

$$f(t) = \prod_{i=1}^{n}(t - x_i)$$

$\bar{\sigma} \in \overline{S_n}$ ve $\bar{\sigma}$'nin $F(x_1, x_2, \ldots, x_n)[t]$ ye genişlemesi $\bar{\sigma}_t$ olmak üzere

$$\bar{\sigma}_t\big(f(t)\big) = \bar{\sigma}_t\left(\prod_{i=1}^{n}(t - x_i)\right) = \prod_{i=1}^{n}\left(t - x_{\sigma(i)}\right) = \prod_{i=1}^{n}(t - x_i) = f(t)$$

olduğundan $\bar{\sigma}_t$, $f(t)$ nin katsayılarını sabit bırakır ve $f(t) \in K[t]$ bulunur. Öte yandan $f(t)$ nin sağ yanı açılır ve $t$'nin kuvvetlerine göre yazılırsa $s_1 = \sum_{i=1}^{n} x_i$ ve $\forall i \geq 2$ için $s_j = \sum_{1 \leq i_1 < \cdots < i_j} x_{i_1} \ldots x_{i_j}$ olmak üzere $f(t) = t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n$ dır. Her $\bar{\sigma} \in \overline{S_n}$ ve $1 \leq i \leq n$ için $\bar{\sigma}(s_i) = s_i$ olduğundan $s_i \in K$ dir.

**Tanım 1.14.2.** $\forall 1 \leq i \leq n$ için $s_i$, $x_1, \ldots, x_n$ *nin i-ninci elemanter simetrik fonksiyonu* denir.$s_1 = x_1 + x_2 + \cdots + x_n$ ve $s_n = x_1 x_2 \ldots x_n$ dir.

$E = F(s_1, s_2, \ldots, s_n)$ olmak üzere $E \leq K$ dır. $f(t) \in E[t]$ olduğundan $F(x_1, x_2, \ldots, x_n), f(t)$'nin E üzerindeki bir parçalanma cismidir ve $f(t)$ nin bütün kökleri birbirinden farklı olduğundan E'nin bir ayrılabilir genişlemesidir. O halde $F(x_1, x_2, \ldots, x_n)$, E üzerinde galoistir. $G = G(F(x_1, x_2, \ldots, x_n)/E)$ olmak üzere $[F(x_1, x_2, \ldots, x_n) : E] = |G|$ dir. $E \leq K \leq F(x_1, x_2, \ldots, x_n)$ olduğundan $F(x_1, x_2, \ldots, x_n)$, $K$'nın bir Galois genişlemesidir. $\overline{S_n} \leq G(F(x_1, x_2, \ldots, x_n)/K)$ ve Teorem 1.8.2'den $[F(x_1, x_2, \ldots, x_n) : K] \leq n!$ olduğundan $[F(x_1, x_2, \ldots, x_n) : K] = |\overline{S_n}| = n!$ ve $|G| \geq n!$ dir. $F(x_1, x_2, \ldots, x_n)$, F üzerinde $f(t)$ nin bir parçalanma cismi olduğundan Teorem 1.8.7'den $|G| \leq n!$ ve $|G| = n!$ olduğundan $G = \overline{S_n}$ olur. Özel olarak $G \cong S_n$ dir. Öte yandan $[F(x_1, x_2, \ldots, x_n) : K] = |\overline{S_n}|$ olduğundan $K = E$ dir.

**Teorem 1.14.3.** F bir cisim ve $x_1, x_2, \ldots, x_n$, F üzerinde $n$ tane belirsiz olmak üzere $x_1, x_2, \ldots, x_n$ üzerinde tanımlı elemanter simetrik fonksiyonlar $s_1$, $s_2, \ldots, s_n$ olsun. $F(s_1, s_2, \ldots, s_n)$ bütün simetrik fonksiyonların kümesidir. $F(x_1, x_2, \ldots, x_n)$, $F(s_1, s_2, \ldots, s_n)$ nin bir galois genişlemesidir ve şu şekilde gösterilir:

$G(F(x_1, x_2, \ldots, x_n)/F(s_1, s_2, \ldots, s_n)) \cong S_n$ .

F bir cisim, F üzerinde $n$ tane $x_1, x_2, \ldots, x_n$ belirsizinin rasyonel fonksiyonlar cismi $F(x_1, x_2, \ldots, x_n)$ ve $F(x_1, x_2, \ldots, x_n)$ üzerinde bir belirsiz $t$ olsun. O zaman

$$g_n(t) = t^n - x_1 t^{n-1} + \cdots + (-1)^n x_n$$

polinomuna *F üzerinde n. dereceden bir genel polinom* denir. $F[t]$ içinde n. dereceden her monik polinom, $x_1, x_2, \ldots, x_n$ yerine F'nin uygun elemanları seçilerek $g_n(t)$ den elde edilebilir. Gerçekten $f(t) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in F[t]$ olmak üzere $x_i$ yerine $a_i$ yazılarak tanımlanan $\phi_{a_1, a_2, \ldots, a_n} : F(x_1, x_2, \ldots, x_n) \to F[t]$ değer homomorfizması altında $g_n(t)$ nin görüntüsü $f(t)$ dir. $g_n(t) = 0$ polinom denkleminin

çözümleri için $x_1, x_2, \dots, x_n$ cinsinden formül varsa bu formülde $x_1, x_2, \dots, x_n$ yerine $a_1, a_2, \dots, a_n$ konularak $f(t) = 0$ polinom denkleminin çözümleri elde edilir.

**Teorem 1.14.4.** F bir cisim, F üzerinde tanımlı bir genel polinom $g_n(t) = t^n - x_1 t^{n-1} + \cdots + (-1)^n x_n$ ve K, $g_n(t)$ nin $F(x_1, x_2, \dots, x_n)$ üzerindeki parçalanma cismi ve $F(x_1, x_2, \dots, x_n)$ üzerinde galoistir. $G(K/F(x_1, x_2, \dots, x_n)) \cong S_n$ dir.

**İspat.** $u_1, u_2, \dots, u_n \in K$ olmak üzere $g_n(t) = (t - u_1) \dots (t - u_n)$'dir. Buradan,

$$x_1 = \sum_{i=1}^{n} u_i = s_1(u_1, u_2, \dots, u_n)$$

ve $\forall i \geq 2$ için

$$x_j = \sum_{1 \leq i_1 < \cdots < i_j} u_{i_1} \dots u_{i_j} = s_i(u_1, u_2, \dots, u_n)$$

$y_1, y_2, \dots, y_n$ belirsizleri $x_1, x_2, \dots, x_n, t$ den farklı olmak üzere $F[y_1, y_2, \dots, y_n]$ polinom halkası vardır. $y_1, y_2, \dots, y_n$ nin elemanter simetrik fonksiyonları $s_1 = \sum_{i=1}^{n} y_i$ ve $i \geq 2$ için $s_j = \sum_{1 \leq i_1 < \cdots < i_j} y_{i_1} \dots y_{i_j}$ olmak üzere $x_1 = s_1(u_1, \dots, u_n), \dots, x_n = s_n(u_1, \dots, u_n)$ olur. Teorem 1.14.3'te $F(y_1, y_2, \dots, y_n)$, $F(s_1, s_2, \dots, s_n)$ üzerinde galoistir ve $G(F(y_1, y_2, \dots, y_n)/F(s_1, s_2, \dots, s_n)) \cong S_n$ dir. O halde K'nın $F(x_1, x_2, \dots, x_n)$ üzerinde galois ve $G(K/F(x_1, \dots, x_n)) \cong S_n$ dir.

$F[y_1, \dots, y_n]$, $n$ tane $y_1, \dots, y_n$ belirsizinin polinom halkası olduğundan

$\tau : F[y_1, \dots, y_n] \to F[u_1, \dots, u_n]$, $\tau(y_i) = u_i$ ve $\tau|_F = \iota_F$

şekilde tanımlı bir $\tau$ değer homomorfizması vardır. Benzer şekilde $\sigma : F[x_1, \dots, x_n] \to F[s_1, s_2, \dots, s_n]$, $\sigma(x_i) = s_i$ ve $\sigma|_F = \iota_F$

şekilde tanımlı bir $\sigma$ değer homomorfizması vardır. $\tau\sigma : F[x_1, \dots, x_n] \to F[u_1, \dots, u_n]$ homomorfizması elde edilir. $1 \leq i \leq n$ için

$$\tau\sigma(x_i) = \tau(s_i) = \tau\big(s_i(y_1, \dots, y_n)\big) = s_i(u_1, \dots, u_n) = x_i \text{ ve } \tau\sigma|_F = \iota_F$$

olduğundan $\tau\sigma$, $F[x_1, \dots, x_n]$ in birim otomorfizmasıdır. Öyleyse $\sigma$'nun bir monomorfizma olduğu açıktır. $\sigma$ örten olduğundan bir F izomorfizmasıdır. O halde $\sigma$,

Sonuç 1.8.5'ten dolayı, $F(x_1, x_2, \dots, x_n)$ den $F(s_1, s_2, \dots, s_n)$ ye bir $\bar{\sigma}$ izomorfizmasına genişler. $\bar{\sigma}$ nin $F(x_1, x_2, \dots, x_n)[t]$ ye genişlemesi $\overline{\sigma_t}$ olmak üzere $\overline{\sigma_t}(t) = t$ olduğundan

$$\overline{\sigma_t}\big(g_n(t)\big) = \overline{\sigma_t}(t^n - x_1 t^{n-1} + \cdots + (-1)^n x_n) = t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n = f(t)$$

olur. K, $g_n(t)$ nin $F(x_1, x_2, \dots, x_n)$ üzerinde ve $F(y_1, y_2, \dots, y_n)$ de $f(t) = \prod_{i=1}^{n}(t - y_i)$ nin $F(s_1, s_2, \dots, s_n)$ üzerinde parçalanma cisimleri olduğundan Teorem 1.8.3'ten $\bar{\sigma}$, K'dan $F(y_1, y_2, \dots, y_n)$ ye bir $\theta$ otomorfizmasına genişler. $F(y_1, y_2, \dots, y_n)$, $F(s_1, s_2, \dots, s_n)$ üzerinde Galois olduğundan K, $F(x_1, x_2, \dots, x_n)$ üzerinde Galois'tir. $\theta$ yardımıyla $G(K/F(x_1, x_2, \dots, x_n))$ den $G(F(y_1, y_2, \dots, y_n)/\, F(s_1, s_2, \dots, s_n))$ ye bir izomorfizma tanımlanabilir. $G(F(y_1, y_2, \dots, y_n)/\, F(s_1, s_2, \dots, s_n)) \cong S_n$ olduğundan $G(K/F(x_1, x_2, \dots, x_n)) \cong S_n$ dir.

**Sonuç 1.14.5.** F cisim ve $kar(F) = 0$ olmak üzere $n \geq 5$ için $n$. dereceden bir genel polinom $g_n(t) = t^n - x_1 t^{n-1} + \cdots + (-1)^n x_n$, $F(x_1, x_2, \dots, x_n)$ üzerindeki köklerle çözülemez.

**İspat.** $g_n(t)$ nin $F(x_1, x_2, \dots, x_n)$ üzerindeki parçalanma cismi K ve $G = G(K/F(x_1, \dots, x_n))$ olsun. Teorem 1.14.4'ten $G \cong S_n$ dir. Sonuç 1.2.15'ten $n \geq 5$ için $S_n$ çözülebilir olmadığından Teorem 1.13.7'den $g_n(t), F(x_1, x_2, \dots, x_n)$ üzerinde köklerle çözülemez.

**Örnek 1.14.1.** $x^3 - 4x^2 + 6x - 2 \in \mathbb{Q}[x]$ polinomunun kökleri $\frac{1}{u_1}, \frac{1}{u_2}, \frac{1}{u_3}$ olan n. dereceden denklemi şu şekilde gösterilir: $s_1 = u_1 + u_2 + u_3 = -4$, $s_2 = u_1u_2 + u_1u_3 + u_2u_3 = 6$, $s_3 = u_1u_2u_3 = -2$ olmak üzere

$$\left(x - \frac{1}{u_1}\right)\left(x - \frac{1}{u_2}\right)\left(x - \frac{1}{u_3}\right)$$

$$= x^3 - \left(\frac{1}{u_1} + \frac{1}{u_2} + \frac{1}{u_3}\right)x^2 - \left(\frac{1}{u_{1u_3}} + \frac{1}{u_2u_3} + \frac{1}{u_2u_3}\right)x - \frac{1}{u_1u_2u_3}$$

$$= x^3 - \left(\frac{s_2}{s_3}\right)x^2 - \left(\frac{s_1}{s_3}\right)x - \left(\frac{1}{s_3}\right) = x^3 + 3x^2 - 2x + \frac{1}{2}$$

## 1.15. Bağıntılar ve Kafes

**Tanım 1.15.1.** $\beta \subset X \times X$ olmak üzere

(i) $\forall x \in X$ için $(x,x) \in \beta$ ise $\beta$'ya *yansıyan bağıntı*,

(ii) $\forall (x,y) \in \beta$ için $(y,x) \in \beta$ ise $\beta$'ya *simetrik bağıntı*,

(iii) $\forall (x,y) \in \beta$ için $(y,x) \notin \beta$ ise $\beta$'ya *ters simetrik bağıntı*,

(iv) $\forall (x,y),(y,z) \in \beta$ için $(x,z) \in \beta$ ise $\beta$'ya *geçişken bağıntı*

denir.

**Tanım 1.15.2.** X boş kümeden farklı bir küme olmak üzere üzerindeki bir $\beta$ bağıntısı aynı zamandan yansıyan, simetri ve geçişme bağıntısı ise bu bağıntıya *denklik bağıntısı* denir.

**Tanım 1.15.3.** X boş kümeden farklı bir küme olmak üzere üzerindeki bir $\beta$ bağıntısı aynı zamandan yansıyan, ters simetri ve geçişme bağıntısı ise bu bağıntıya *kısmi sıralama bağıntısı* denir. "$\leq$" ile gösterilir.

**Tanım 1.15.4.** Bir X kümesi üzerinde tanımlanan kısmi sıralama bağıntısı varsa $(X, \leq)$ ikilisine *kısmi sıralı küme* denir.

**Tanım 1.15.5.** $(X, \leq)$ kısmi sıralı bir küme ve $x, y \in X$ olmak üzere $(x,y) \in \beta$ veya $(y,x) \in \beta$ oluyorsa $x$ ve $y$ elemalarına *karşılaştırılabilir (ilişkili) elemanlar,* olmuyorsa *karşılaştırılamaz (ilişkisiz) elemanlar* denir.

**Tanım 1.15.6.** X boş kümeden farklı bir küme olmak üzere üzerindeki bir $\beta$ kısmi sıralama bağıntısı verilsin. $\forall x, y \in X$ için $(x,y) \in \beta$ veya $(y,x) \in \beta$ oluyorsa $\beta$'ya X üzerinde bir *tam sıralama bağıntısı* denir. $(A, \beta)$ iklisine de *tam sıralı küme* denir.

**Tanım 1.15.7.** $(X, \leq)$ bir kısmi sıralı küme ve $B \subset X$ olsun. Eğer $(B, \leq)$ bir tam sıralı küme oluyorsa B alt kümesine X kümesinin bir *zinciri* denir.

**Tanım 1.15.8.** $(X, \leq)$ kısmi sıralı küme olsun.

(i) $\forall x \in X$ için $x \leq M$ olacak biçimde bir $M \in X$ varsa $M$'ye A kümesinin *en büyük elemanı* denir.

(ii) $\forall x \in X$ için $M \leq x$ olacak biçimde bir $M \in X$ varsa $M$'ye A kümesinin *en küçük elemanı* denir.

(iii) $M^* \in X$ için X kümesinde $M^*$ dan büyük eleman yoksa $M^*$ ya *maksimal eleman* denir ve $\max(X)$ ile gösterilir.

(iv) $M^* \in X$ için X kümesinde $M^*$ dan küçük eleman yoksa $M^*$ ya *minimal eleman* denir ve $\min(X)$ ile gösterilir.

**Not 1.15.9.** Sıralı bir kümede en büyük ve en küçük eleman tektir ve maksimal ve minimal eleman birden fazla olabilir.

**Tanım 1.15.10.** X kümesi üzerinde bir sıralama bağıntısı olsun. Eğer bu bağıntı bir kısmi sıralama bağıntısı ve $X$ kümesinin boştan farklı her alt kümesinin bir en küçük elemanı varsa $(X, \leq)$ ya *iyi sıralı küme* denir.

**Tanım 1.15.11.** $(X, \leq)$ kısmi sıralı küme ve $B \subset X$ olsun.

I. $\forall y \in B$ için $y \leq M$ olacak biçimde $M \in X$ varsa M'ye B kümesinin bir *üst sınırı* denir ve $\text{üst}(B) = \{ a | \ a, \ B$ kümesinin bir üst sınırı$\}$ şeklinde gösterilir.

II. $\forall y \in B$ için $M \leq y$ olacak biçimde $M \in X$ varsa M'ye B kümesinin bir *alt sınırı* denir ve $alt(B) = \{ a | \ a, \ B$ kümesinin bir alt sınırı$\}$ şeklinde gösterilir.

**Tanım 1.15.12.** $(X, \leq)$ kısmi sıralı küme ve $B \subset X$ olsun.

I. B alt kümesinin üst sınırlarının en küçük elemanına B kümesinin *en küçük üst sınırı veya supremumu* denir ve $\sup(B)$ ile gösterilir.

II. B alt kümesinin üst sınırlarının en büyük elemanına B kümesinin *en büyük alt sınırı veya infimumu* denir ve $\inf(B)$ ile gösterilir.

**Tanım 1.15.13.** $(X, \leq)$ kısmi sıralı küme olmak üzere $\forall x, y \in X$ için $\inf(x, y) = x \wedge y$ varsa $(X, \leq, \wedge)$ sistemine *yarı kafes* denir.

**Tanım 1.15.14.** $(X, \leq)$ kısmi sıralı küme olmak üzere $\forall x, y \in X$ için $\inf(x, y) = x \vee y$ ve $\sup(x, y) = x \vee y$ varsa $(X, \leq, \wedge, \vee)$ sistemine *kafes* denir.

**Not 1.15.15.** Bir kafeste en büyük ve en küçük eleman varsa sırasıyla 1 ve 0 ile gösterilirler.

**Tanım 1.15.16.** $\forall x \in X$ için $x \wedge x' = 0$ ve $x \vee x' = 1$ eşitliklerini sağlayan $x'$ elemanına $x$ *elemanın tamlayanı* denir.

## 2. YAPILAN ÇALIŞMALAR

Bu kısımdaki tanım ve teoremler Mordeson ve Malik (1998), Mordeson (1992) ve Mordeson ve Malik (1991) çalışmalarından derlenmiştir.

### 2.1. Fuzzy Alt Küme

**Tanım 2.1.1.** X herhangi bir küme olsun. $\mu : X \to [0,1]$ şeklinde tanımlanan fonksiyona X kümesinin *fuzzy alt kümesi* denir. X kümesinin bütün fuzzy alt kümelerinin oluşturduğu kümeye *fuzzy kuvvet kümesi* denir ve $[0,1]^X$ ile gösterilir.

**Tanım 2.1.2.** $\mu \in [0,1]^X$ olmak üzere $\{\mu(x) | x \in X\} = \mu(X)$ kümesine *görüntü kümesi* denir ve $Im(X)$ ile gösterilir.

**Tanım 2.1.3.** $\mu \in [0,1]^X$ olmak üzere $\mu^* = \{x \in X | \, \mu(x) > 0 \}$ kümesine $\mu$'nün *destekleyicisi* denir. $\mu^*$ sonlu bir küme ise $\mu$' ye *sonlu fuzzy küme*, $\mu^*$ sonsuz bir küme ise $\mu$' ye *sonsuz fuzzy küme* denir. Ayrıca $1 \in \mu(X)$ ise $\mu$' ye X kümesinin *birimli fuzzy alt kümesi* denir.

**Tanım 2.1.4.** $Y \subset X$ ve $a \in [0,1]$ olsun. $a_Y \in [0,1]^X$ şu şekilde tanımlanır:

$$a_Y(x) = \begin{cases} a; \ x \in Y \\ 0; \ x \notin Y \end{cases}$$

Eğer $Y = \{x\}$ olacak şekilde tek elemanlı bir küme ise $a_Y = a_{\{x\}}$ şeklinde gösterilir ve $[0,1]$- *fuzzy singleton* veya $[0,1]$- *fuzzy nokta* denir.

$a = 1$ ise

$$1_Y = \begin{cases} 1; x \in Y \\ 0; x \notin Y \end{cases}$$

fonksiyonuna *Y'nin karakteristik fonksiyonu* denir. (Kaufmann, 1975)

**Tanım 2.1.5.** $\mu, v \in [0,1]^X$ olsun. $\forall x \in X$ için $\mu(x) \leq v(x)$ ise $\mu$, $v$'nün fuzzy alt kümesidir denir. Eğer $\mu \subseteq v$ ve $\mu \neq v$ ise *kesin içindedir* denir.

**Tanım 2.1.6.** $\mu, v \in [0,1]^X$ olsun. $\mu \cap v$, $\mu \cup v \in [0,1]^X$ sırasıyla kümeleri şeklinde tanımlanır:

$(\mu \cap \nu)(x) = \mu(x) \wedge \nu(x)$

$(\mu \cup \nu)(x) = \mu(x) \vee \nu(x)$

$\mu \cap \nu$ ve $\mu \cup \nu$'ye sırasıyla $\mu$ ve $\nu$'nün kesişimi ve birleşimi denir.

**Tanım 2.1.7.** $\mu \in [0,1]^X$ ve $a \in [0,1]$ olmak üzere $\mu_a = \{x | x \in X,\ \mu(x) \geq a\}$ kümesine $\mu$'nün $a$ *-seviye kümesi* denir.

**Tanım 2.1.8.** $I \neq \emptyset$ ve $\{X_i | i \in I\}$ boş olmayan bir kümeler ailesi olsun. Bu kümelerin kartezyen çarpımı

$$X = \prod_{i \in I} X_i = \{(x_i)_{i \in I} | x_i \in X, i \in I\}$$

biçiminde tanımlanır.

$\forall i \in I$ için $\mu_i \in [0,1]^{X_i}$ olsun. Her $(x_i)_{i \in I} \in X$ için $\mu(x) = \bigwedge_{i \in I} \mu_i(x_i)$ şeklinde $\mu \in [0,1]^X$ fuzzy kümesine $\mu_i$ lerin *tam direkt çarpımı* denir ve şu şekilde gösterilir:

$$\mu = \tilde{\prod_{i \in I}} \mu_i$$

**Tanım 2.1.9.** X ve Y herhangi iki küme olmak üzere $\mu \in [0,1]^X$, $\nu \in [0,1]^Y$ ve $f: X \to Y$ bir fonksiyon olsun. $\forall y \in Y$ için $f(\mu) \in [0,1]^Y$ $\mu$'nün $f$'de fuzzy görüntü kümesi

$$f(\mu)(y) = \begin{cases} \vee \{\mu(x): x \in X\};\ f^{-1}(x) \neq \emptyset \\ 0 \qquad\qquad\quad ;\ f^{-1}(x) = \emptyset \end{cases}$$

ve $f^{-1}(\nu) \in [0,1]^X$ $\nu$'nün $f$'de ters fuzzy görüntüsü $f^{-1}(\nu)(x) = \nu\big(f(x)\big)$ şeklinde tanımlanır.

## 2.2. Fuzzy Alt Gruplar ve Fuzzy Normal Alt Gruplar

**Tanım 2.1.1.** X bir grup ve $\forall \mu, \nu \in [0,1]^X$ fuzzy kümeleri olmak üzere $\forall x \in X$ için

$$(\mu \circ \nu)(x) = \bigvee \{\mu(y) \wedge \nu(z): y, z \in X, yz = x\}$$

$\mu^{-1}(x) = \mu(x^{-1})$

şeklinde tanımlanır. $\mu \circ \nu$'ye $\mu$ ve $\nu$'nün çarpımı, $\mu^{-1}$ ye $\mu$ fuzzy kümesinin tersi denir.

**Tanım 2.2.2.** X bir grup ve $\mu \in [0,1]^X$ olmak üzere $\mu$

(i) $\forall x, y \in X$ için $\mu(xy) \geq \mu(x) \wedge \mu(y)$

(ii)

(iii) $\forall x \in X$ için $\mu(x^{-1}) \geq \mu(x)$

şartlarını sağlarsa $\mu$'ye X'in *fuzzy alt grubu* denir.

**Tanım 2.2.3.** X bir grup ve $\mu$, X'in fuzzy alt grubu olsun. $e$, X'nin fuzzy alt grubu olmak üzere $\mu_* = \{x \in X: \mu(x) = \mu(e)\}$ dir.

**Tanım 2.2.4.** $\mu$ sonlu bir X grubunun fuzzy alt grubu olmak üzere $\mu_*$ G'nin değişmeli alt grubu ise $\mu$'ye *değişmeli fuzzy alt grup* denir.

**Önerme 2.2.5.** X bir grup olmak üzere $\mu$, X'in fuzzy alt kümesi olması için gerek ve yeter şart $\forall x, y \in X$ için $\mu(xy^{-1}) \geq \mu(x) \wedge \mu(y)$ dır.

**Teorem 2.2.6.** X bir grup $\mu$, X'in fuzzy alt kümesi olmak üzere $\forall x, y \in X$ için aşağıdakiler denktir.

(i) $\mu(xy) = \mu(yx)$ (Bu durumda $\mu$'ye abelian (değişmeli) fuzzy alt küme denir)

(ii) $\mu(xyx^{-1}) = \mu(y)$

(iii) $\mu(xyx^{-1}) \geq \mu(y)$

(iv) $\mu(xyx^{-1}) \leq \mu(y)$

(v) $\forall \nu \in [0,1]^x$ için $\mu \circ \nu = \nu \circ \mu$

**Tanım 2.2.7.** Teorem 2.2.6'daki şartlardan en az birini sağlayan $\mu$'ye *fuzzy normal alt grup* denir.

**Tanım 2.2.8.** X bir grup ve $\mu$, X'in fuzzy alt grubu ve $x \in X$ olmak üzere $\mu(e)_{\{x\}} \circ \mu$ , $\mu \circ \mu(e)_{\{x\}}$ ye sırasıyla $\mu$'nün x'e göre *sol koseti* ve *sağ koseti* denir ve sırasıyla $x\mu$ ve $\mu x$ ile gösterilir.

Eğer $\mu$, X grubunun fuzzy normal alt grubu ise $x\mu = \mu x$ dir.

**Önerme 2.2.9.** $f: G \to H$ grup izomorfizması olsun. $v$, H grubunun fuzzy normal alt grubu ise $f^{-1}(v)$, G grubunun fuzzy normal alt grubudur.

## 2.3. Fuzzy Alt Halka ve Fuzzy İdealler

**Tanım 2.3.1.** R bir halka $\mu$ ve $v$, R halkasının fuzzy alt kümeleri olsun. $\mu + v$, $-\mu$, $\mu - v \in [0,1]^x$ aşağıdaki şekilde tanımlanır. $\forall x, y, z \in R$ için,

i)$(\mu + v)(x) = \vee_{x=y+z} \{\mu(y) \wedge v(z)\}$

ii) $(-\mu)(x) = \mu(-x)$

iii) $(\mu - v)(x) = \vee_{x=y-z} \{\mu(y) \wedge v(z)\}$

$\mu + v$ ve $\mu - v$'ye sırasıyla $\mu$ ve $v$'nün toplamı ve farkı, $-\mu$'ye $\mu$'nün tersi denir.

**Tanım 2.3.2.** R bir halka ve μ, R'nin bir fuzzy alt kümesi olsun. Eğer $\forall\ x, y \in R$ için,
(i) $\mu(x - y) \geq \mu(x) \wedge \mu(y)$

(ii) $\mu(xy) \geq \mu(x) \wedge \mu(y)$

ise μ'ye R'nin bir fuzzy alt halkası denir. (Liu,1982)

**Tanım 2.3.3.** μ, R'nin fuzzy alt kümesi olmak üzere $\forall x, y \in R$ için,

(i) $\mu(x - y) \geq \mu(x) \wedge \mu(y)$

(ii) $\mu(xy) \geq \mu(x)$ ise μ'ye R halkasının bir fuzzy sağ ideali,

(iii) $\mu(xy) \geq \mu(y)$ ise μ'ye R halkasının bir fuzzy sol ideali denir.

Eğer $\mu$, R halkasının hem sol fuzzy hem sağ fuzzy ideali ise μ'ye R halkasının fuzzy ideali denir. (Gupta ve Kantroo, 2001)

## 2.4. Fuzzy Alt Cisim, Fuzzy Alt Uzay ve Fuzzy Cisim Genişlemeleri

Bu kısımda F cisim olarak alınacaktır. Pozitif tam sayılar kümesi N ile gösterilecektir.

**Tanım 2.4.1.** F bir cisim, $A: F \to [0,1]$ fuzzy alt küme olsun. Eğer $A(0) = 1 = A(1)$ ve $\forall x, y \in F$ için

i. $A(x - y) \geq A(x) \wedge A(y)$
ii. $A(xy^{-1}) \geq A(x) \wedge A(y)\ \ y \neq 0$

oluyorsa A'ya *fuzzy alt cisim* denir.

F cisminin bütün fuzzy alt cisimlerinin kümesi $\mathfrak{F}$ ile gösterilecektir. Eğer $A \in \mathfrak{F}$ ise bu durumda $\forall x \in F$ için $x \neq 0, A(x) = A(-x) = A(x^{-1})$ olduğu açıktır.

**Tanım 2.4.2.** A ve B, F'nin fuzzy alt cisimleri olsun. Eğer $A \supseteq B$ ise $A/B$ ye *fuzzy cisim genişlemesi* denir. $C \in \mathfrak{F}$ ve $A \supseteq C \supseteq B$ olduğunda C'ye $A/B$ nin *fuzzy ara cismi* denir.

$A \in \mathfrak{F}$ olsun. $A_{\#} = \{x \in F | A(x) = 1\}$ şeklinde tanımlanır.

**Önerme 2.4.3.** $A : F \to [0,1]$ fuzzy alt cisim olmak üzere $A_{\#}$ ve $A^*$, F'nin alt cismidir.

**İspat.** $A_{\#}$ için $x, y \in A_{\#}$ olsun. O halde $A(x) = 1$ ve $A(y) = 1$ dir.

(i) $A(x + y) \geq A(x) \wedge A(y) = 1 \wedge 1 = 1$ ise $A(x + y) = 1$ dir. Böylece $x + y \in A_{\#}$ dir.
(ii) A, fuzzy alt cisim olduğundan $A(x) = A(-x) = A(x^{-1}) = 1$ dir. Böylece $-x, x^{-1} \in A_{\#}$ dir.
(iii) $A(xy) \geq A(x) \wedge A(y^{-1}) = 1 \wedge 1 = 1$ ise $A(xy) = 1$ dir. Böylece $xy \in A_{\#}$ dir.

(i), (ii) ve (iii)'den $A_{\#}$, F'nin alt cismidir.

$A^*$ için $x, y \in A^*$ olsun. O halde $A(x) > 0$ ve $A(y) > 0$ dır.

(i) $A(x + y) \geq A(x) \wedge A(y) > 0$ ise $A(x + y) > 0$ dır. Böylece $x + y \in A^*$ dir.
(ii) A, fuzzy alt cisim olduğundan $A(x) = A(-x) = A(x^{-1}) > 0$ dir. Böylece $-x, x^{-1} \in A^*$ dir.
(iii) $A(xy) \geq A(x) \wedge A(y^{-1}) > 0$ ise $A(xy) > 0$ dır. Böylece $xy \in A^*$ dır.

(i), (ii) ve (iii)'den $A^*$, F'nin alt cismidir.

**Önerme 2.4.4.** $A/B$ bir fuzzy cisim genişlemesi olmak üzere $A_{\#} \supseteq B_{\#}$ ve $A^* \supseteq B^*$ dır.

**İspat.** $A/B$ bir fuzzy cisim genişlemesi olduğundan $A \supseteq B$ dir.

$x \in B_{\#}$ olsun. $B(x) = 1$ ve $A \supseteq B$ olduğundan $\forall x \in F$ için $A(x) \geq B(x) = 1$ dir. O halde $A(x) \geq 1$ olduğundan $x \in A_{\#}$ dir. Böylelikle $A_{\#} \supseteq B_{\#}$ dir.

$x \in B^*$ olsun. $B(x) > 0$ ve $A \supseteq B$ olduğundan $\forall x \in F$ için $A(x) \geq B(x) > 0$ dir. O halde $A(x) > 0$ olduğundan $x \in A^*$ dir. Böylelikle $A^* \supseteq B^*$ dır.

**Tanım 2.4.5.** $A, B \in \mathfrak{F}$ olsun. $\forall x \in F$ için F'nin $A \circ B$ fuzzy alt kümesi şu şekilde tanımlanır:

$(A \circ B)(x) = \wedge\{C(x) | C \in \mathfrak{F},\ B \subseteq C,\ A \subseteq C\}$.

Açıkça görüldüğü gibi $A \circ B$, A ve B'yi kapsayan F'nin en küçük fuzzy alt cismidir.

**Tanım 2.4.6.** $A, B \in \mathfrak{F}$ olsun. $\forall x \in F$ için

$$(AB)(x) = \bigvee \left\{ \bigwedge \{\{A(y_i) \wedge B(z_i)\} | i = 1, \dots, n\} \middle| x = \sum_{i=1}^{n} y_i z_i, \qquad n \in N \right\}.$$

şeklinde tanımlanan $AB$ fuzzy kümesine A ve B'nin *bileşiği* denir.

A, F'nin fuzzy alt halkası olmak üzere A, F'nin bir fuzzy alt kümesidir öyle ki $\forall x, y \in F$ için $A(x - y) \wedge A(xy) \geq A(x) \wedge A(y)$ dır.

**Teorem 2.4.7.** $A, B \in \mathfrak{F}$ olsun. Bu durumda

(i) $A \circ B \supseteq AB \supseteq A, B$

(ii) $AB$, F'nin bir fuzzy alt halkasıdır.

**İspat.**

(i) $C \supseteq B$ ve $C \supseteq A$ olacak şekilde $C \in \mathfrak{F}$ olsun. $x \in F$ ve $x = \sum_{i=1}^{n} y_i z_i$ olsun. Bu durumda

$C(x) \geq \wedge \{C(y_i z_i) | i = 1, \dots, n\} \geq \wedge \{\{C(y_i) \wedge C(z_i)\} \ | i = 1, \dots, n\}$

$\geq \wedge \{\{A(y_i) \wedge B(z_i)\} | i = 1, \dots, n\}$

Dolayısıyla $C(x) \geq A(x)B(x)$ dir. Böylelikle $A \circ B \supseteq AB$ dir. Şimdi $x \neq 0$ ise $(AB)(x) \geq A(x) \wedge B(1) = A(x)$ ve $(AB)(0) \geq A(0) \wedge B(0) = A(0)$ dır.

(ii) $x, x' \in F$ olsun.

$(AB)(x) \wedge (AB)(x') =$

$$\wedge\left\{\vee\left\{\wedge\{\{A(y_i) \wedge B(z_i)\} | i = 1, \dots, n\} \middle| x = \sum_{i=1}^{n} y_i z_i, n \in N\right\},\right.$$

$$\left.\vee\left\{\wedge\{\{A(u_j) \wedge B(v_j)\} | j = 1, \dots, m\} \middle| x' = \sum_{j=1}^{m} u_j v_j, m \in N\right\}\right\}$$

$$= \vee\left\{\wedge\{\wedge\{A(y_i), A(u_j), B(z_i), B(v_j)\} | i = 1, \dots, n, j = 1, \dots, m\} \middle| x = \sum_{i=1}^{n} y_i z_i, x' = \sum_{j=1}^{m} u_j v_j, n, m \in N\right\}$$

Son ifadede eşitliğin her iki tarafı daha da azaltılırsa

$$\vee\left\{\wedge\{\{A(t_k) \wedge B(w_k)\} | k = 1, \dots, q\} \middle| x + x' = \sum_{k=1}^{q} t_k w_k, q \in N\right\}$$

ve

$$\vee\left\{\wedge\{\{A(r_h) \wedge B(s_h)\} | h = 1, \dots, p\} \middle| xx' = \sum_{h=1}^{p} r_h s_h, p \in N\right\}.$$

$x = \sum_{i=1}^{n} y_i z_i$ ve $x' = \sum_{j=1}^{m} u_j v_j$ olarak yazıldığında

$$x + x' = \sum_{i=1}^{n} y_i z_i + \sum_{j=1}^{m} u_j v_j, xx' = \sum_{i=1}^{n} \sum_{j=1}^{m} (y_i u_j)(z_i v_j)$$

ve bundan dolayı

$A(y_i u_j) \geq A(y_i) \wedge A(u_j)$ ve $B(z_i v_j) \geq B(z_i) \wedge B(v_j)$.

Bu durumda

$(AB)(x + x') \geq (AB)(x) \wedge (AB)(x') \leq (AB)(xx')$.

Şimdi

$$(AB)(-x) = \bigvee\left\{\wedge\{\{A(y_i) \wedge B(z_i)\}|i = 1, \dots, n\}\middle| -x = \sum_{i=1}^{n} y_i z_i, n \in N\right\}$$

$$= \bigvee\left\{\wedge\{\{A(y_i) \wedge B(z_i)\}|i = 1, \dots, n\}\middle| x = \sum_{i=1}^{n} (-y_i) z_i, n \in N\right\}$$

$$= \bigvee\left\{\wedge\{\{A(-y_i) \wedge B(z_i)\}|i = 1, \dots, n\}\middle| x = \sum_{i=1}^{n} (-y_i) z_i, n \in N\right\}$$

$$= (AB)(x).$$

Teorem 2. 4. 5'ten

$$(AB)(1) = \bigvee\left\{\wedge\{\{A(y_i) \wedge B(z_i)\}|i = 1, \dots, n\}\middle| 1 = \sum_{i=1}^{n} y_i z_i, n \in N\right\}$$

$$= A(1) \wedge B(1) = 1.$$

**Önerme 2.4.8.** $A, B \in \mathfrak{F}$ olsun. Bu durumda

(i) $A_{\#} \cap B_{\#} = (A \cap B)_{\#}$

(ii) $(AB)_{\#} \supseteq A_{\#}B_{\#}$; A ve B sonlu olduğunda $A_{\#}B_{\#} = (AB)_{\#}$ dir.

**İspat.**

(i) $x \in A_{\#} \cap B_{\#}$ olsun.

$= A(x) = 1 \ \wedge B(x) = 1$

$= A(x) \wedge B(x) = 1$

$= (A \cap B)(x) = 1$

O halde $x \in (A \cap B)_{\#}$ dir. $A_{\#} \cap B_{\#} \subseteq (A \cap B)_{\#}$ dir.

$x \in (A \cap B)_{\#}$ olsun.

$= (A \cap B)(x) = 1$

$= A(x) \wedge B(x) = 1$

$= A(x) = 1 \wedge B(x) = 1$

$= x \in A_{\#}$ ve $x \in B_{\#}$

O halde $x \in A_{\#} \cap B_{\#}$ dir. $(A \cap B)_{\#} \subseteq A_{\#} \cap B_{\#}$ dir.

$A_{\#} \cap B_{\#} \subseteq (A \cap B)_{\#}$ ve $(A \cap B)_{\#} \subseteq A_{\#} \cap B_{\#}$ olduğundan $(A \cap B)_{\#} = A_{\#} \cap B_{\#}$ dir.

(ii) $AB \supseteq A, B$ dir. Böylece $(AB)_{\#} \supseteq A_{\#}, B_{\#}$ dir. Dolayısıyla $(AB)_{\#} \supseteq A_{\#}B_{\#}$ dir. $x \in (AB)_{\#}$ olsun. O halde

$$1 = (AB)(x) = \bigvee \left\{ \wedge \{\{A(y_i) \wedge B(z_i)\} | i = 1, \dots, n\} \middle| 1 = \sum_{i=1}^{n} y_i z_i , n \in N \right\}.$$

Dolayısıyla $i = 1, \dots, n$ için $\exists y_i \in A_{\#}, z_i \in B_{\#}$ için $x = \sum_{i=1}^{n} y_i z_i$ dir. Böylelikle $x \in A_{\#}B_{\#}$ dir. O halde $A_{\#}B_{\#} \supseteq (AB)_{\#}$ dir.

**Önerme 2.4.9.** $A, B \in \mathfrak{F}$ olsun. Bu durumda aşağıdakiler sağlanır.

(i) $A^* \cap B^* = (A \cap B)^*$

(ii) $(AB)^* = A^* B^*$

**İspat.**

(i) $x \in A^* \cap B^*$ olsun.

$A^* \cap B^* \Leftrightarrow A(x) > 0 \wedge B(x) > 0$

$\Leftrightarrow A(x) \wedge B(x) > 0$

$\Leftrightarrow (A \cap B)(x) > 0$

$\Leftrightarrow x \in (A \cap B)^*$

O halde $A^* \cap B^* = (A \cap B)^*$ dir.

**Teorem 2.4.10.** $F/K$ bir cebirsel cisim genişlemesi olsun. A, F'nin fuzzy alt halkası öyle ki $\wedge\{A(k) | k \in K\} \geq \vee\{A(c) | c \in F - K\}$ ve P, K'nın asal alt cismi olmak üzere A, $K - P$ üzerinde sabit olsun.

(i) $kar(K) = 0$ ve A, $P - \{0\}$ üzerinde sabit olduğunda A, F'nin bir fuzzy alt cismidir.

(ii) $kar(K) = p > 0$ olduğunda A, $P - \{0\}$ üzerinde sabittir.

**İspat.** $kar(K) = p > 0$ olduğunda A, $P - \{0\}$ üzerinde sabittir. $x \in F$ ve $x \notin K$ olsun. O halde $i = 0, \dots, n$ için bazı $k_i \in K$ için $x^{-1} = \sum_{i=1}^{n} k_i\, x^i$ dir. Böylelikle

$$A(x^{-1}) \geq \wedge\{A(k_i x^i) | i = 0, \dots, n\} \geq \wedge\{\{A(k_i) \wedge A(x^i)\} | i = 0, \dots, n\} = A(x).$$

Benzer şekilde $A(x) = A((x^{-1})^{-1}) \geq A(x^{-1})$ dir. Dolayısıyla $A(x) = A(x^{-1})$ dir. $x \in K - \{0\}$ ise $A(x) = A(x^{-1})$ olduğundan A, $K - P$ ve $P - \{0\}$ üzerinde sabittir.

Teorem 2.4.10'da $A \supseteq \delta_K$ ise $A_\# \supseteq K$ dır. Ayrıca $A_\# \supseteq K$ olması için gerek ve yeter şart A, $K - \{0\}$ üzerinde sabittir. Eğer $A_\# \supseteq K$ ise böylece $\wedge\{A(k) | k \in K\} \geq \vee\{A(c) | c \in F - K\}$ dır.

**Sonuç 2.4.11.** $F/K$ bir cebirsel cisim genişlemesi olsun. $A_\# \supseteq K$ ve $B_\# \supseteq K$ olacak şekilde $A, B \in \mathfrak{F}$ olsun. Bu durumda AB, F'nin fuzzy alt cismidir.

**İspat.** $k \in K$ olsun. Öyleyse

$$(AB)(k) \geq A(k) \wedge B(1) = A(1) \wedge B(1) = 1.$$

Böylelikle $(AB)_\# \supseteq K$ dır.

**Sonuç 2.4.12.** $F = A_\# B_\#$ ve $A_\#/(A_\# \cap B_\#)$ cebirsel olacak şekilde $A, B \in \mathfrak{F}$ olsun. O halde AB, F'nin bir fuzzy alt cismidir.

**İspat.** Önerme 2.4.6 dan $F/B_\#$ cebirseldir ve $(AB)_\# \supseteq B_\#$ dir.

**Tanım 2.4.13.** V, K cismi üzerinde bir vektör uzayı olsun. A, V'nin bir fuzzy alt kümesi ve C, K'nın bir fuzzy alt cismi olsun. Bu durumda A, C üzerinde V'nin bir fuzzy alt uzayı olması için gerek ve yeter şart her $x, y \in V$ ve her $c \in K$ için

i. $A(0) = 1$
ii. $A(x - y) \geq A(x) \wedge A(y)$
iii. $A(cx) \geq C(c) \wedge A(x)$ dır.

C, K'nın alt cismi ise Tanım 2.4.11(iii) şartı $A(cx) \geq A(x)$ şeklinde yazılır. (Mordeson ve Malik, 1991)

$\mathcal{A}_K$, V üzerinde $K \in \mathfrak{F}$ nın bütün fuzzy alt uzaylarının kümesi şeklinde tanımlanır.

**Önerme 2.4.14.** $A/C$ bir fuzzy cisim genişlemesi olsun. Bu durumda

(i) A, C üzerinde F'nin fuzzy alt uzayıdır.

(ii) A, $C|_{C^*}$ üzerinde F'nin fuzzy alt uzayıdır.

**İspat.** $c, x \in F$ olsun. Bu durumda $A(cx) \geq A(c) \wedge A(x) \geq C(c) \wedge A(x)$ dır.

(i) Tanım 2.4.13'de K yerine F alınırsa V ile C tanımlanır.

(ii) K yerine F alınırsa V ve $C^*$ tanımlanır.

**Önerme 2.4.15.** $A/C$ ve $B/C$ fuzzy cisim genişlemeleri olsun. Bu durumda

(i) AB, B ve C üzerinde F'nin bir fuzzy alt uzayıdır.

(ii) AB, $C|_{C^*}$ ve $B|_{B^*}$ üzerinde F'nin bir fuzzy alt uzayıdır.

**İspat.** $c, x \in F$ olsun. Bu durumda

$(AB)(x) \geq (AB)(c) \wedge (AB)(x) \geq B(c) \wedge (AB)(x) \geq C(c) \wedge (AB)(x)$.

(i) Tanım 2.4.13'de K yerine F alınırsa V ile C tanımlanır.

(ii) K yerine F alınırsa V ve $C^*$ tanımlanır. Böylece $B^*$ da tanımlanır.

**Tanım 2.4.16.** $A \in \mathcal{A}_K$ ve X, V'nin bir fuzzy alt kümesidir öyle ki $X \subseteq A$ olsun. $\langle X \rangle$, K üzerinde V'nin X'i kapsayan ve A'nın kapsadığı bütün fuzzy alt uzaylarının kesişimidir. Bu durumda $\langle X \rangle$ e X'den A'ya *fuzzily üretilmiş fuzzy alt uzayı* denir.

**Tanım 2.4.17.** $x, y \in F$ için $X - x$ , F'nin fuzzy alt kümesi olmak üzere

$$(X - x)(y) = \begin{cases} X(y) & x \neq y \\ 0 & x = y \end{cases}$$

şeklinde tanımlanır.

**Tanım 2.4.18.** $A \in \mathcal{A}_K$ ve X, V'nin bir fuzzy alt kümesidir öyle ki $X \subseteq A$ olsun.

(i) Eğer $\langle X \rangle = A$ ise X'e K üzerinde A'dan *üretilmiş bir fuzzy sistemi* denir.

(ii) $\lambda = X(x)$, $x_\lambda \notin \langle X - x \rangle$ olan her $x_\lambda \subseteq X$ için X, K üzerinde *fuzzy bağımsızdır* denir.

(iii) X, A'nın üreticisinin fuzzy sistemi ise X, A için bir *fuzzy bazıdır* denir.

(iv) $\xi$, V'nin fuzzy singletonlarının bir kümesidir öyle ki $x_\lambda,\ x_k \in \xi$; böylece $\lambda = k$ ve $x_\lambda \subseteq A$ dır. Bu durumda eğer $\langle \xi \rangle = A$ ise $\xi$'ye K üzerinde A'nın üreticisinin *fuzzy singleton sistemi* denir.

(v) Eğer $\forall x_\lambda \in \xi$ için $x_\lambda \notin \langle \xi - \{x_\lambda\} \rangle$ ise $\xi$, K'da *fuzzy bağımsızdır* denir.

(vi) Eğer $\xi$, A'nın üreticisinin bir fuzzy singleton sistemi ise ve fuzzy bağımsız ise $\xi$'ye A için *singletonların bir fuzzy bazıdır* denir.

$\forall x \in F$ için $x_\lambda \in \xi$ ise $X(\xi)(x) = \lambda$ ve diğer durumlarda $X(\xi)(x) = 0$ dır. Ayrıca $\langle \xi \rangle = \langle X(\xi) \rangle$ olarak alınır. X, F'nin bir fuzzy alt kümesi olsun.

$$\xi(X) = \{x_\lambda | x \in F, \qquad X(x) = \lambda > 0\}$$

şeklinde tanımlanır. Bu durumda $X(\xi)(x) = x$ ve $\xi\big(X(\xi)\big) = \xi$ dır.

**Teorem 2.4.19.** $A \in \mathcal{A}_K$ ve $\xi \subseteq \{x_\lambda | x \in A^*,\ 0 < \lambda \leq A(x)\}$ öyle ki $x_\lambda,\ x_k \in \xi$ olsun. Bu durumda $\lambda = k$ ve $X = \{x |\ x_\lambda \in \xi\}$ dır. Kabul edelim ki $\bigwedge\{K(c) | c \in F\} \geq \bigvee\{A(x) | x \in V - \{0\}\}$ olsun. Bu durumda $\xi$, K üzerinde fuzzy bağımsız olması için gerek ve yeter şart X, F'de lineer bağımsızdır. (Malik and Mordeson, 1991)

**Teorem 2.4.20.** $A, B \in \mathfrak{F}$ olsun. X, F'nin bir fuzzy alt kümesidir öyle ki $X \subseteq A$ dır. Bu durumda X, $\delta_{B^*}$ üzerinde bağımsız olması için gerek ve yeter şart $X^*$, $B^*$ üzerinde lineer bağımsızdır.

**Tanım 2.4.21.** $A, B \in \mathfrak{F}$, $A/C$ ve $B/C$ fuzzy cisim genişlemeleri olsun. Bu durumda A ve B, C üzerinde *lineer parçalanış* olması için gerek ve yeter şart $A \cap B = C$ ve X, F'nin herhangi bir fuzzy alt kümesidir öyle ki $A \supseteq X$ olsun. X, $\delta_{C^*}$ üzerinde bağımsız ise $\delta_{B^*}$ üzerinde de bağımsızdır.

**Teorem 2.4.22.** $A/C$ ve $B/C$ fuzzy cisim genişlemeleri olsun. Bu durumda A ve B, C üzerinde lineer parçalanış olması için gerek ve yeter şart $A \cap B = C$ ve $A^*$ ve $B^*$, $C^*$ üzerinde lineer parçalanıştır.

**İspat.** Kabul edelim ki A ve B, C üzerinde lineer parçalanış olsun. $A^*,\ C^* \supseteq S$ üzerinde lineer bağımsız olsun. X, F'nin fuzzy alt kümesi tanımından $x \in S$ ise $X(x) = A(x)$ diğer durumlarda $X(x) = 0$ alınır. Bu durumda Teorem 2.4.20'den X, $\delta_{C^*}$ üzerinde bağımsızdır. Böylelikle X, $\delta_{B^*}$ üzerinde bağımsızdır. Dolayısıyla S, $B^*$ üzerinde lineer bağımsızdır. Böylece Teorem 2.4.20'den $A^*$ ve $B^*$, $C^*$ üzerinde lineer parçalanıştır.

Tersine varsayalım ki $A^*$ ve $B^*$, $C^*$ üzerinde lineer parçalanış olsun. X, F'nin bir fuzzy alt kümesi öyle ki $A \supseteq X$ ve X, $\delta_{C^*}$ üzerinde bağımsızdır. O halde X, $C^*$ üzerinde ve böylelikle $B^*$ üzerinde lineer bağımsızdır. Öyleyse X, $\delta_{B^*}$ üzerinde bağımsızdır.

**Örnek 2.4.23.** G ve H, F'nin alt cismi olsun öyle ki $G \cap H \supset P$ olduğunda P, F'nin asal alt cismidir. Kabul edelim ki G ve H, $G \cap H$ üzerinde lineer parçalanıştır. $A = \delta_G$ ve $B = \delta_H$ olsun. C, F'nin fuzzy alt cismi olmak üzere $x \in P$ için $C(x) = 1$, $x \in G \cap H$ için $C(x) = 1/2$, diğer durumlarda $C(x) = 0$ olarak tanımlanır. O halde $A^*$ ve $B^*$, $C^* = A^* \cap B^* = (A \cap B)^*$ üzerinde lineer parçalanabilir. Aynı zamanda $A \cap B = \delta_{C^*} \supset C$ dir. Böylelikle A ve B, C üzerinde lineer parçalanış değildir. Teorem 2.4.16'dan A ve B, $A \cap B$ üzerinde lineer parçalanıştır.

**Teorem 2.4.24.** $A/B$, $B/C$ ve $D/C$ fuzzy cisim genişlemeleridir öyle ki BD, F'nin bir fuzzy alt cismidir. Eğer A ve D, C $(= A \cap D)$ üzerinde lineer parçalanış ise bu durumda

(i) A ve BD, $A \cap BD$ üzerinde lineer parçalanıştır,
(ii) B ve D, C üzerinde lineer parçalanıştır.

Tersine eğer (i), (ii) ve $A \cap BD = B$ alınırsa o zaman A ve D, C üzerinde lineer parçalanıştır.

**İspat.** Kabul edelim ki A ve D, C üzerinde lineer parçalanış olsun.

(i) Önerme 2.4.9 ve 2.4.8'den $A^*$ ve $D^*$, $A^* \cap D^* = (A \cap D)^* = C^*$ üzerinde lineer parçalanıştır. Böylelikle Önerme 2.4.9'dan $,A^*$ ve $(BD)^* = B^*D^*$, $A^* \cap (BD)^* = (A \cap BD)^*$ üzerinde lineer parçalanıştır. Dolayısıyla A ve BD, $A \cap BD$ üzerinde lineer parçalanıştır. (Jacobson,1964)

(ii) $C \subseteq B \cap D \subseteq A \cap D = C$ olsun. Buradan $B \cap D = C$ dir. Şimdi $A^* \cap D^*$, $C^*$ üzerinde lineer parçalanıştır. Böylece $B^*$ ve $D^*$, $C^*$ üzerinde lineer parçalanıştır. Dolayısıyla B ve D, C üzerinde lineer parçalanıştır.

Karşıtı için $A^*$ ve $(BD)^* = B^*D^*$, $B^*$ üzerinde lineer parçalanış ve $B^*$ ve $D^*, C^*$ üzerinde lineer parçalanıştır. Dolayısıyla $A^*$ ve $D^*$, $C^*$ üzerinde lineer parçalanış olur. Şimdi $A \cap D = A \cap BD \cap D = B \cap D = C$ dir. Böylelikle Teorem 2.4.23'ten istenen sonuç elde edilir.

**Örnek 2.4.25.** $A/B$, $B/C$ ve $D/C$ fuzzy cisim genişlemeleridir öyle ki A ve D, C üzerinde lineer parçalanış, $A \cap BD \neq B$ ve $A \neq B$ olmasına rağmen $BD = AD$ dır.

$K = P(t)$ ve P karakteristiği sıfırdan büyük mükemmel bir cisim $F = K(\theta, t^{p-1})$ olduğunda $t$, $P$ üzerinde transandantal ve $\theta$, $K$ üzerinde $x^p + tx + t$ polinomunun bir köküdür. O halde Eisenstein kriterinden $x^p + tx + t$, K üzerinde indirgenmezdir. Dolayısıyla $K(\theta)/K$ cebirsel ayrılabilirdir. F'de A, B, C ve D fuzzy alt kümeleri tanımlansın. $A = \delta_s$ alındığında $S = K(\theta)$; $B(z) = 1$ ise $z \in P(\theta^p)$, $B(z) = \frac{1}{2}$ ise $z \in S - P(\theta^p)$, diğer durumlarda $B(z) = 0$; $C(z) = 1$ ise $z \in P$, $C(z) = \frac{1}{2}$ ise $z \in K - P$, diğer durumlarda $C(z) = 0$; $J = K(t^{p-1})$ olduğunda $D = \delta_J$ dir. O halde A, B, C ve D, F'nin fuzzy alt cisimleri ve $A^* = S = B^*$, $C^* = K$ ve $D^* = J$ dir. Teorem 2.4.10'dan her $k \in K$ için $D(k) = 1 \leq BD(k) \leq 1$ den dolayı BD, F'nin fuzzy alt cismidir. Ayrıca $\theta = \theta^p(-t^{-1}) - 1$ dir. Böylelikle

$$(BD)(\theta) \geq B(\theta^p) \wedge D(-t^{-1}) \wedge (BD)(-1) = 1.$$

Dolayısıyla $(BD)(\theta) = 1 = A(\theta)$ dır. Aynı zamanda $B(\theta) = \frac{1}{2}$ dir. Böylelikle $A \cap BD \neq B$ dir. Dolayısıyla A ve BD, B üzerinde lineer parçalanış değildir. $z \in F$ olsun. Bu durumda $c_r \in J$ olduğunda $z = \sum_{r=0}^{p-1} c_r \theta^r$ dır. Şimdi $J$ üstünde $BD \subseteq D$'den dolayı $BD = 1$ ve $J$ üstünde $D = 1$ dir. Böylelikle

$$(BD)(z) \geq \wedge\{(BD)(c_r\theta^r) | r = 0, .., p-1\}$$

$$\geq \wedge\{(BD)(c_r) \wedge (BD)(\theta^r) | r = 0, .., p-1\} = 1.$$

Dolayısıyla $BD = \delta_F = AD$ dir. Ayrıca kanıt olarak $B(\theta) = \frac{1}{2}$ den dolayı B ve BD, $B^*$ üstünde eşit değildir.

**Teorem 2.4.26.** $A/C$, $B/C$ ve $D/C$ fuzzy cisim genişlemeleri öyle ki A ve D, C $(= A \cap D)$ üzerinde lineer parçalanış ve BD, F'nin bir fuzzy alt cismidir. Bu durumda aşağıdaki maddeler için (i), (ii)'yi ve (ii), (iii)'yi sağlar.

(i) $C^* \subseteq B_{\#}$

(ii) $B^*$ üzerinde $B = BD$

(iii) $A \cap BD = B$

**İspat.** $(i) \Rightarrow (ii)$: $x \in B^*$ olsun. $B^*$ ve $D^*$, $C^*$ üzerinde lineer parçalanış olduğundan dolayı $i = 1, \dots, n$ için $y_i \in B^*, z_i \in D^*$ olduğunda $x = \sum_{i=1}^{n} y_i \otimes z_i$ dir. $1 = t_1, t_2, \dots, t_r \in D^*$, $C^*$ üzerinde lineer bağımsızdır ve $i = 1, \dots, n$, $j = 1, .., r$ için $z_i = \sum_{j=1}^{r} k_{ij} t_j$, $k_{ij} \in C^*$ dır. Bu durumda

$x \otimes 1 = \sum_{i=1}^{n} y_i \otimes \sum_{j=1}^{r} k_{ij} t_j = \sum_{j=1}^{r} \sum_{i=1}^{n} k_{ij} y_i \otimes t_j$ ve bu yüzden , j=2,..,r için

$\sum_{i=1}^{n} k_{ij} y_i = 0$ ve $\sum_{i=1}^{n} k_{i1} y_i = x.$

Şimdi

$B(x) \geq \wedge\{B(k_{i1}, y_i) | i = 1, \dots, n\} \geq \wedge\{B(k_{i1}) \wedge B(y_i) | i = 1, .., n\}$

$= \wedge\{B(y_i) | i = 1, \dots, n\}.$

Böylelikle $B(x) \geq \wedge\{B(y_i) \wedge D(z_i) | i = 1, \dots, n\}$ dır. Dolayısıyla $B(x) \geq (BD)(x)$ ve bu yüzden $B(x) = (BD)(x)$ dir. Buradan (ii) sağlanır.

$(ii) \Rightarrow (iii)$: $(A \cap BD)^* = A^* \cap B^* D^* = B^*$ dır. Şimdi $A \supseteq B$ ve $B^*$ de $BD = B$ dir. Böylelikle $B^*$ de $A \cap BD = B$ dir. Bundan dolayı $(A \cap BD)^* = B^*$, $A \cap BD = B$ dir.

**Sonuç 2.4.27.** $A/B$, $B/C$ ve $D/C$ fuzzy cisim genişlemeleri olsun. Öyle ki AD ve BD, F'nin fuzzy alt cisimleri ve A ve D, C$(= A \cap D)$ üzerinde lineer parçalanıştır. $C^* \subseteq B_{\#}$ olduğunda $A \neq B$ ise $AD \neq BD$ demektir.

**İspat.** Teorem 2.4.2'den $A^*$ ve $D^*$, $C^*$ üzerinde lineer parçalanıştır. Eğer $A^* \neq B^*$, o zaman $(AD)^* = A^* D^* \neq B^* D^* = (BD)^*$ ve bu yüzden $AD \neq BD$ dır. Kabul edelim ki $A^* = B^*$ olsun. $A(x) > B(x)$ olacak şekilde $x \in A^*$ olsun. Teorem 2.4.6'dan, $(AD)(x) = A(x)$ ve $(BD)(x) = B(x)$ dir. Dolayısıyla $AD \neq BD$ dir.

**Tanım 2.4.28.** $A/B$ fuzzy cisim genişlemesi olsun. $A/B$ nin boyutu $[A : B]$ şeklinde yazılır ve $\delta_{B^*}$ üzerinde A'ya göre F'nin maksimal bağımsız alt kümelerinin kardinalitesi ile tanımlanır. $A/B$ için $[A : B] < \infty$ ise sonlu boyutludur denir.

Teorem 2.4.28'den $[A : B] = [A^* : B^*]$ dir.

**Önerme 2.4.29.** $A/B$ ve $B/C$ fuzzy cisim genişlemeleri olsun. Bu durumda aşağıdakiler sağlanır.

(i) $[A:C] = [A:B][B:C]$

(ii) $[A:B] = 1 \Leftrightarrow A^* = B^*$

**İspat.**

(i) $[A:C] = [A^*:C^*] = [A^*:B^*][B^*:C^*] = [A:B][B:C]$

(ii) $[A:B] = 1 \Leftrightarrow [A^*:B^*] = 1 \Leftrightarrow A^* = B^*$ dir.

## 2.5. Tamamen Ayrılamaz Fuzzy Cisim Genişlemeleri

Bu bölümde F cisminin karakteristiği $p > 0$ olarak alınacaktır.

**Tanım 2.5.1.** $A/B$ fuzzy cisim genişlemesi olsun. O halde $A/B$ tamamen ayrılamazdır denir ancak ve ancak her $x_\lambda \subseteq A$ için $x_\lambda^{p^e} \subseteq B$ olacak şekilde $e$ negatif olmayan tam sayısı bulunabilmesidir.

**Önerme 2.5.2.** $A/B$ fuzzy cisim genişlemesi olsun. Bu durumda $A/B$ tamamen ayrılamaz olması için gerek ve yeter şart her $x \in F$ için $A(x) \leq B\left(x^{p^e}\right)$ olacak şekilde $e$ negatif olmayan tam sayısı olmasıdır.

**İspat.** Kabul edelim ki $A/B$ tamamen ayrılamaz olsun. $A(x) = \lambda$ olduğunda $x_\lambda \subseteq A$ dır. Böylece $e$ vardır öyle ki $A(x) \leq B\left(x^{p^e}\right)$ den dolayı $x_\lambda^{p^e} \subseteq B$ dir. Karşıtı için kabul edelim ki $x_\lambda \subseteq A$ olsun. O halde $\lambda \leq A(x) \leq B(x^{pe})$ bu yüzden $x_\lambda^{p^e} \subseteq B$ dir.

Eğer $A \in \mathfrak{F}$ alınırsa $A/A$ tamamen ayrılamazdır.

Kabul edelim ki B, F'nin alt cismi olsun. O halde $B\left(x^{p^e}\right) \leq B\left(x^{p^{e+1}}\right)$ dır. Dolayısıyla bazı $e$ için $x_\lambda^{p^e} \subseteq B$, öyleyse $x_\lambda^{p^{e+1}} \subseteq B$ dır.

Eğer bazı $e$ için $x_\lambda^{p^e} \subseteq B$, öyleyse en küçük $e$'ye B üzerinde $x_\lambda$ nın üssü denir ve $x_\lambda$ ya B üzerinde tamamen ayrılamaz denir. Eğer $e$ negatif olmayan tam sayı olsun öyle ki her $x_\lambda$ için $x_\lambda \subseteq A$ ile $x_\lambda^{p^e} \subseteq B$, o halde en küçük $e$, $A/B$ nin üssü olarak adlandırılır.

**Önerme 2.5.3.** $A/B$ tamamen ayrılamaz fuzzy cisim genişlemesi olsun. Bu durumda

(i) $A_{\#}/B_{\#}$ tamamen ayrılamazdır;

(ii) $A^*/B^*$ tamamen ayrılamazdır.

**İspat.**

(i) $x \in A_{\#}$ olsun. Öyleyse $e \geq 0$ vardır öyle ki $B\left(x^{p^e}\right) \geq A(x) = 1$ dır. Böylece $x^{p^e} \in B_{\#}$ dir.

(ii) $x \in A^*$ olsun. Öyleyse $e \geq 0$ vardır öyle ki $B\left(x^{p^e}\right) \geq A(x) \geq 0$ dır. Böylece $x^{p^e} \in B^*$ dir.

**Örnek 2.5.4.** K, karakteristiği $p > 0$ olan bir cisim olmak üzere $F = K(\theta)$ olsun ve $\theta$, K üzerinde cebirsel ayrılabilir olsun. F'nin A ve B fuzzy alt cisimleri eğer $z \in K$ ise $A(z) = B(z) = 1$ ve diğer durumlarda $A(z) = \frac{1}{2}$, $B(z) = \frac{1}{4}$ şeklinde tanımlanır. O halde $A_{\#} = K = B_{\#}$ ve $A^* = F = B^*$ dır. Dolayısıyla $A_{\#}/B_{\#}$ ve $A^*/B^*$ tamamen ayrılamazdır. Aynı zamanda her $e \geq 0$ için $B\left(\theta^{p^e}\right) = 1/4 < A(\theta)$ olduğunda $A/B$ tamamen ayrılamaz değildir.

**Önerme 2.5.5.** $F/K$ bir cisim genişlemesi olsun. O halde $F/K$ nın tamamen ayrılamaz olması için gerek ve yeter şart $\delta_F/\delta_K$ nın tamamen ayrılamaz olmasıdır.

**Teorem 2.5.6.** $A/B$ ve $B/C$ fuzzy cisim genişlemeleri olsun. Bu durumda $A/C$ nin tamamen ayrılamaz olması için gerek ve yeter şart $A/B$ ve $B/C$ tamamen ayrılamaz olmasıdır.

**İspat.** Kabul edelim ki $A/C$ tamamen ayrılamaz ve $x \in F$ olsun. O halde $e \geq 0$ vardır öyle ki $C\left(x^{p^e}\right) \geq A(x)$ dır. Dolayısıyla $B\left(x^{p^e}\right) \geq C\left(x^{p^e}\right) \geq A(x) \geq B(x)$ dır. Dolayısıyla $A/B$ ve $B/C$ tamamen ayrılamaz olur. Aksini kabul edelim. $A/B$ ve $B/C$ tamamen ayrılamaz ve $x \in F$ olsun. O halde $e \geq 0$ ve $f \geq 0$ vardır öyle ki $B\left(x^{p^e}\right) \geq A(x)$ ve $C\left(\left(x^{p^e}\right)^{p^f}\right) \geq B\left(x^{p^e}\right)$ dir. Böylelikle $C\left(x^{p^{e+f}}\right) \geq A(x)$ dır. Dolayısıyla $A/C$ tamamen ayrılamaz olur.

**Tanım 2.5.7.** A, F'nin bir fuzzy alt kümesi ve $i$ negatif olmayan bir tam sayı olsun. $A^{p^i}$ F'nin fuzzy alt kümesi olmak üzere her $x \in F$ için $A^{p^i}\left(x^{p^i}\right) = A(x)$ ve $x \notin F^{p^i}$ için $A^{p^i}(x) = 0$ şeklinde tanımlanır.

**Teorem 2.5.8.** Eğer A, F'nin alt cismi ise bu durumda $A^{p^i}$, F'nin fuzzy alt cismidir.

**İspat.** $x, y \in F$ olsun. Bu durumda

$$A^{p^i}\left(x^{p^i} - y^{p^i}\right) = A^{p^i}\left((x-y)^{p^i}\right) = A(x-y)$$
$$\geq A(x) \wedge A(y) = A^{p^i}\left(x^{p^i}\right) \wedge A^{p^i}(y^{p^i}).$$

Kabul edelim ki $x - y \in F^{p^i}$ ve $x \notin F^{p^i}$, $y \notin F^{p^i}$ olsun. Bu durumda $A^{p^i}(x-y) \geq 0 = A^{p^i}(x) \wedge A^{p^i}(y)$ dır. Kabul edelim ki $x - y \neq F^{p^i}$ olsun. Bu durumda ya $x \notin F^{p^i}$ ya da $y \notin F^{p^i}$ dır. O halde $A^{p^i}(x-y) = 0 = A^{p^i}(x) \wedge A^{p^i}(y)$ dır. Benzer şekilde $A^{p^i}(xy^{-1}) \geq A^{p^i}(x) \wedge A^{p^i}(y)$, $y \neq 0$ dır.

**Önerme 2.5.9.** A, F'nin fuzzy alt kümesi ve $i$ ve $j$ negatif olmayan birer tam sayı olsun. Bu durumda $(A^{p^i})^{p^j} = A^{p^{i+j}}$ dir.

**İspat.** $x \in F$ olsun. Bu durumda

$$\left(A^{p^i}\right)^{p^j}\left(x^{p^{i+j}}\right) = \left(A^{p^i}\right)^{p^j}\left(\left(x^{p^i}\right)^{p^j}\right) = A^{p^i}\left(x^{p^i}\right) = A(x) = A^{p^{i+j}}\left(x^{p^{i+j}}\right).$$

$x \notin F^{p^i}$ kabul edilsin. En büyük negatif olmayan $k$ tam sayısı vardır öyle ki $\exists y \in F$ için $x = y^{p^k}$ dır. O halde $k < i + j$ dir. Eğer $k < j$ ise bu durumda $\left(A^{p^i}\right)^{p^j}(x) = 0$ dır. $k \geq j$ kabul edilsin. Bu durumda $\exists m \geq 0$ ve $m < i$ için $k = j + m$ dir. Böylelikle $\left(A^{p^i}\right)^{p^j}(x) = \left(A^{p^i}\right)^{p^j}\left(\left(y^{p^m}\right)^{p^j}\right) = A^{p^i}\left(y^{p^m}\right) = 0$ dır. En sade haliyle $A^{p^{i+j}}(x) = 0$ dır. Böylelikle $(A^{p^i})^{p^j} = A^{p^{i+j}}$ dir.

**Önerme 2.5.10.** $A/B$ bir fuzzy cisim genişlemesi ve $e$ negatif olmayan bir tam sayı olsun. Bu durumda $A^{p^e} \subseteq B$ olması için gerek ve yeter şart her $x_\lambda \subseteq A$ için, $x_\lambda^{p^e} \subseteq B$ dir.

**İspat.** Kabul edelim ki $A^{p^e} \subseteq B$ ve $x_\lambda \subseteq A$ olsun. O halde $\lambda \leq A(x) = A^{p^e}(x^{p^e}) \leq B(x^{p^e})$ dir. Böylelikle $x_\lambda^{p^e} \subseteq B$ dir. Tersine $x_\lambda \subseteq A$ kabul edilsin. O halde $x_\lambda^{p^e} \subseteq B$ dir. $x \notin F^{p^e}$ kabul edilsin. Bu durumda $A^{p^e}(x) = 0 \leq B(x)$ dir. $A(x) = \lambda$ olsun. Bu durumda $x_\lambda \subseteq A$ bu yüzden $x_\lambda^{p^e} \subseteq B$ dir yani; $A^{p^e}\left(x^{p^e}\right) = A(x) = \lambda \leq B(x^{p^e})$ dir. Böylelikle $A^{p^e} \subseteq B$ dir.

Önerme 2.5.10'da $A/B$ bir fuzzy cisim genişlemesi ve $\exists e \geq 0$ için $A^{p^e} \subseteq B$ dır bu durumda $A/B$ tamamen ayrılamaz ve en küçük $e$ kuvveti için $A/B$ önceden tanımlanmıştır.

**Önerme 2.5.11.** $A \in \mathfrak{F}$ olsun. Bu durumda $i = 1,2, \ldots$ için

(i) $(A_\#)^{p^i} = (A^{p^i})_\#$

(ii) $(A^*)^{p^i} = (A^{p^i})^*$

**İspat.** Önerme 2.5.9'dan $i = 1$ için sonucunu göstermek yeterlidir.

(i) $x^p \in (A_\#)^p \Leftrightarrow x \in A_\# \Leftrightarrow A(x) = 1 \Leftrightarrow A^p(x^p) = 1 \Leftrightarrow x^p \in (A^p)_\#$ dir. Eğer $y \in (A^p)_\#$ ise bu durumda $\exists x \in F$ için $x^p = y$ dir.

(ii) $x^p \in (A^*)^p \Leftrightarrow x \in A^* \Leftrightarrow A(x) > 0 \Leftrightarrow A^p(x^p) > 0 \Leftrightarrow x^p \in (A^p)^*$ dır.

**Önerme 2.5.12.** $A, B \in \mathfrak{F}$ olsun. Bu durumda $i = 1,2, \ldots$ için $(AB)^{p^i} = A^{p^i}B^{p^i}$ dir.

**İspat.** Önerme 2.5.9'dan $i = 1$ için sonucunu göstermek yeterlidir. $x \in F$ olsun. Bu durumda

$$(A^pB^p)(x^p) = \bigvee\left\{\wedge\{A^p(y_i)\wedge B^p(z_i)|i = 1, \ldots, n\}\,|x^p = \sum_{i=1}^{n} y_i z_i\,, n \in N\right\}$$

$$= \bigvee\left\{\wedge\left\{A^p\left(u_i^p\right)\wedge B^p\left(v_i^p\right)|i = 1, \ldots, n\right\}\middle|x^p = \sum_{i=1}^{n} u_i^p v_i^p\,, u_i^p \in (A^p)^* = (A^*)^p,\right.$$

$$\left. v_i^p \in (B^p)^* = (B^*)^p, n \in N\right\}$$

$$= \bigvee\left\{\wedge\{A(u_i) \wedge B(v_i)|i = 1, \ldots, n\}\,|x = \sum_{i=1}^{n} u_i v_i\,, u_i \in A^*, \quad v_i \in B^* n \in N\right\}$$

$= (AB)(x) = (AB)^p(x)^p.$

Şimdi $A^pB^p \subseteq (AB)^p$ ve $x \notin F^p$ olduğundan $(A^pB^p)(x) = 0$ dır. Öyleyse $A^pB^p = (AB)^p$ dir.

**Tanım 2.5.13.** $B \in \mathfrak{F}$ ve X, F'nin bir fuzzy alt kümesi olsun. Her $x \in F$ için F'nin $B(X)$ fuzzy alt kümesi

$B(X)(x) = \wedge \{C(x) | C \in \mathfrak{F}, B \subseteq C \text{ ve } X \subseteq C\}$

şeklinde gösterilir.

Kolayca görüldüğü gibi $B(X)$, C ve X'i kapsayan F'nin en küçük fuzzy alt cismidir.

**Önerme 2.5.14.** $A/B$ bir fuzzy cisim genişlemesi ve X, F'nin bir fuzzy alt kümesi olsun. Bu durumda $(A \circ B)(x) = B(X)$ dır.

**İspat.** $C \in \mathfrak{F}$ olsun. Bu durumda $C \supseteq A$ ve $C \supseteq B(X)$ olması için gerek ve yeter şart $C \supseteq A$ ve $C \supseteq X$ dir.

**Önerme 2.5.15.** $B \in \mathfrak{F}$ ve X, F nin bir fuzzy alt kümesi olsun. Bu durumda $i = 1,2, \ldots$ için $(B(X))^{p^i} = B^{p^i}\left(x^{p^i}\right)$ dir.

**İspat.** $z \in F$ olsun.

$\big(B(X)\big)^p(z^p) = \big(B(X)\big)(z) = \wedge\{C(z) | C \in \mathfrak{F}, \quad C \supseteq B, \quad C \supseteq X\}$

$= \wedge\{C^p(z^p) |\ C \in \mathfrak{F}, \quad C^p \supseteq B^p, \quad C^p \supseteq X^p\}$

$\geq \wedge\{D(z^p) |\ D \in \mathfrak{F},\ D \supseteq B^p,\ D \supseteq X^p\} = \big(B^p(X^p)\big)(z^p).$

$D \in \mathfrak{F}$ vardır öyle ki $D \supseteq B^p$ ve $D \supseteq X^p$ dir. C, F'nin fuzzy alt kümesi her $z \in F$ için $C(z) = D(z^p)$ şeklindedir. O halde $C \in \mathfrak{F}$ olsun. Şimdi $C^p(z^p) = C(z) = D(z^p) \geq B^p(z^p)$, $X^p(z^p)$ dir. O halde $C^p \supseteq B^p$ ve $C^p \supseteq X^p$ dir. $F^p$ üstünde $C^p = D$ olduğundan $\big(B(X)\big)^p(z^p) = \big(B^p(X^p)\big)(z^p)$ dir Dolayısıyla $\big(B(X)\big)^p = \big(B^p(X^p)\big)$ dir.

**Sonuç 2.5.16.** $B \in \mathfrak{F}$ ve X, F'nin fuzzy alt kümesi olsun öyle ki bazı negatif olmayan $e$ sayısı için $X^{p^e} \subseteq B$ dir. Bu durumda $(B(X))^{p^e} \subseteq B$ dir.

**İspat.** Önerme 2.5.15'ten $(B(X))^{p^e} = B^{p^e}(X^{p^e})$ dir.

**Önerme 2.5.17.** $A/B$ bir fuzzy cisim genişlemesi olsun. Kabul edelim ki $\vee\{A(z)|z \in A^* - B^*\} \leq \wedge\{B(z)|z \in B^*\}$ ve $B^*$ üstünde $A = B$ olsun. Bu durumda $A/B$ nin tamamen ayrılamaz olması için gerek ve yeter şart $A^*/B^*$ tamamen ayrılamazdır.

**İspat.** $A^*/B^*$ tamamen ayrılamaz kabul edilsin. $x \in F$ olsun. Eğer $x \notin A^*$ ise, bu durumda $\forall e \geq 0$ için $A(x) = 0 \leq B(x^{p^e})$ dir. $x \in A^* - B^*$ kabul edilsin. Bu durumda $\exists e \geq 0$ için $x^{p^e} \in B^*$ dir. Dolayısıyla hipotezden $B(x^{p^e}) \geq A(x)$ dir. $x \in B^*$ kabul edilsin. Bu durumda $A(x) = B(x)$ dir. Tersi Önerme 2.5.3'ten elde edilir.

**Sonuç 2.5.18.** $F/K$ bir cisim genişlemesi olsun. Bu durumda $F/K$ nın tamamen ayrılamaz olması için gerek ve yeter şart $\delta_F/\delta_K$ tamamen ayrılamaz olmasıdır.

**Örnek 2.5.19.** $F = P(x)(x^{p^{-1}}, \dots, x^{p^{-i}}, \dots)$ olduğunda P mükemmel cisminin karakteristiği $p > 0$ ve x, P üzerinde transandantal olsun. B, F'nin fuzzy alt kümesi eğer $z \in P$ ise $B(z) = 1,\ i = 0,1, \dots\ z \in P\left(x^{p^i}\right) - P\left(x^{p^{i+1}}\right)$ ise $B(z) = i/(i+1)$ ve $z \in F - P(x)$ ise $B(z) = 0$ şeklinde tanımlanır. Bu durumda $B \in \mathfrak{F}$ (Malik ve Mordeson 1990) ve $B^* = P(x^p)$ dir. X, F'nin fuzzy alt kümesi $i = 1,2, \dots$ için $X\left(x^{p^{-i}}\right) = i/(i+1)$ ve eğer $z \neq x^{p^{-i}}$ $(i = 1,2, \dots)$ ise $X(z) = 0$ dır. Bu durumda her $(x^{p^{-i}})_{i/(i+1)} \subseteq X$ için $e = 2i$ olduğunda $i/(i+1) \leq B((x^{p^{-i}})^{p^e})$ dır. $i = 1,2, \dots$ için $(x^{p^{-i}})_{i/(i+1)}$, B üzerinde tamamen ayrılamazdır. Aynı zamanda şimdi $B(x)/B$ nin tamamen ayrılamaz olduğu gösterilecektir. $C \in \mathcal{F}$ vardır öyle ki $C \supseteq B$ ve $C \supseteq X$ dir. Bu durumda $i = 1,2, \dots$ için $C(x) = C\left((x^{p^{-i}})^{p^i}\right) \geq C\left((x^{p^{-i}}\right) \geq X\left((x^{p^{-i}})\right) = i/(i+1)$ dir. Öyleyse $C(x) = 1$ dir. Dolayısıyla $B(X)(x) = 1$ dir. Öyleyse $x_1 \subseteq B(X)$, fakat $x_1^{p^e} \subseteq B$ olacak şekilde $e > 0$ yoktur. Dolayısıyla $x_1$, B üzerinde tamamen ayrılamaz değildir. Ayrıca Sonuç 2.5.16 dan $X' \subseteq X$ ve $x_1 \subseteq B(X')$ olacak şekilde F'nin sonlu fuzzy alt kümesi $X'$ yoktur. Aynı zamanda eğer $X_i$, F'nin fuzzy alt kümesi ise $j = 1,2, \dots, i$ için $X_i(x^{p^{-j}}) = j/(j+1)$ ve diğer durumlarda $X_i(z) = 0$ şeklindedir, o halde $i = 1,2, \dots$ için $x_1 \not\subseteq B(x_i)$ dır.

## 2.6 Ayrılabilir Fuzzy Cisim Genişlemeleri

Bu bölümün tamamında F'nin karakteristiği $p > 0$ alınacaktır.

**Tanım 2.6.1.** $A/B$ bir fuzzy cisim genişlemesi olsun. Bu durumda eğer B ve $A^p$, $B^p(= B \cap A^p)$ üzerinde lineer parçalanış ise $A/B$ ayrılabilir denir.

**Örnek 2.6.2.** $F = P(x)$ olduğunda P mükemmel cisminin karakteristiği $p > 0$ ve x, P üzerinde transandantal olsun. F'nin A ve B fuzzy alt cisimleri $A = \delta_F$ ve $z \in F^p$ için $B(z) = 1$ ve diğer durumlarda $B(z) = {}^1\!/_2$ şeklindedir. Bu durumda $A^p = \delta_{F^p}$ dır. $z \in F$ olsun. Bu durumda $z \notin F^p$ ise $(B \cap A^p)(z) = B(z) \wedge A^p(z) = 0, z \in F^p$ ise 1 dir. Şimdi $z \notin F^p$ ise $B^p(z) = 0, z \in F^p - F^{p^2}$ ise ${}^1\!/_2$, $z \in F^{p^2}$ ise 1 dir. Böylelikle $B \cap A^p \neq B^p$ dir. O halde $A/B$ ayrılabilir değildir. Aynı zamanda $A^* = B^*$ dir ve bu yüzden $A^*/B^*$ ayrılabilirdir.

**Önerme 2.6.3.** $A/B$ bir fuzzy cisim genişlemesi olsun. Bu durumda $A/B$ ayrılabilir olması için gerek ve yeter şart $A^*/B^*$ ayrılabilirdir ve $B^p = B \cap A^p$ dir.

**İspat.** B ve $A^p$ , $B^p$ üzerinde lineer parçalanış olması için gerek ve yeter şart $B^*$ ve $(A^p)^* = (A^*)^p$ , $(B^p)^* = (B^*)^p$ üzerinde lineer parçalanıştır ve Teorem 2.4.16 ve Önerme 2.5.11'den $B^p = B \cap A^p$ dir.

**Önerme 2.6.4.** $A/B$ ve $B/C$ fuzzy cisim genişlemeleri olsun.

(i) Eğer $A/C$ ayrılabilir ise bu durumda $B/C$ ayrılabilirdir.
(ii) Eğer $A/B$ ve $B/C$ ayrılabilir ise bu durumda $A/C$ ayrılabilirdir.

**İspat.**

(i) $A^*/C^*$ ve bu yüzden $B^*/C^*$ ayrılabilirdir. Şimdi $C^p = C \cap A^p \supseteq C \cap B^p \supseteq C^p$ dir. Böylelikle Önerme 2.6.3'ten $B/C$ ayrılabilirdir.
(ii) $A^*/B^*$ ve $B^*/C^*$ ayrılabilir bu yüzden $A^*/C^*$ ayrılabilirdir. Şimdi $C \cap A^p \subseteq B \cap A^p = B^p$ dir. Öyleyse $C \cap A^p \subseteq C \cap B^p = C^p$ dir. Dolayısıyla $C \cap A^p = C^p$ ve Önerme 2.6.3'ten $A/C$ ayrılabilirdir.

**Önerme 2.6.5.** $F/K$ bir fuzzy cisim genişlemesi olsun. Bu durumda $F/K$ ayrılabilir olması için gerek ve yeter şart $\delta_F/\delta_K$ ayrılabilirdir.

**İspat.** $(\delta_F)^* = F$ ve $(\delta_K)^* = K$ dır. Dolayısıyla Önerme 2.6.3'ten $F/K$ ayrılabilir olması için $\delta_K \cap (\delta_F)^p = (\delta_K)^p$ olduğunu göstermek yeterlidir. Önerme 2.6.3'ün ispatı tekrar uygulanarak gösterilir.

Eğer $F/K$ cisim genişlemesi ise bu durumda $F/K$ cebirsel ayrılabilir olması için gerek ve yeter şart $F/K$ nın her L ara cismi için $x^p \in L$ demek $x \in L$ demektir.

**Tanım 2.6.6.** $A/B$ bir fuzzy cisim genişlemesi olsun. Bu durumda her $x_\lambda \subseteq A$ ve $A/B$ nin her fuzzy ara cismi D için $x_\lambda^p \subseteq D$ yani $x_\lambda \subseteq D$ ise $A/B$ cebirsel ayrılabilirdir denir.

**Teorem 2.6.7.** $A/B$ bir fuzzy cisim genişlemesi olsun. Bu durumda $A/B$ cebirsel ayrılabilir olması için gerek ve yeter şart her $x \in F$ için ve $A/B$ nin her fuzzy ara cismi D için ya $D(x) = x^p$ ya da $D(x) = A(x)$ alınır.

**İspat.** Kabul edelim ki $A/B$ cebirsel ayrılabilir olsun. $x \in F$ ve D, $A/B$'nin bir fuzzy ara cismi olsun. $D(x^p) \leq A(x)$ kabul edilsin. Bu durumda $x_\lambda \subseteq A$ ve $x_\lambda^p \subseteq D$ olduğundan $\lambda = D(x^p)$ yani $x_\lambda \subseteq D$ dir. Böylece $D(x^p) \leq D(x)$ dir. Dolayısıyla $D(x^p) = D(x)$ dir. $D(x^p) > A(x)$ kabul edilsin. $\lambda = A(x)$ olsun. Bu durumda $x_\lambda^p \subseteq D$ ve bu yüzden $x_\lambda \subseteq D$ dir. Benzer şekilde $A(x) \leq D(x)$ dir. Dolayısıyla $A(x) = D(x)$ dir. Tersine her x ve D için ya $D(x^p) = D(x)$ ya da $D(x) = A(x)$ kabul edilsin. $x_\lambda \subseteq A$ ve $x_\lambda^p \subseteq D$ kabul edilsin. Eğer $D(x^p) = D(x)$ ise bu durumda $D(x) \geq \lambda$ dır. Benzer şekilde $x_\lambda \subseteq D$ dir. Eğer $A(x) = D(x)$ ise bu durumda $D(x) \geq \lambda$ benzer şekilde $x_\lambda \subseteq D$ dir. Öyleyse $A/B$ cebirsel ayrılabilirdir.

Eğer A, F'nin fuzzy alt cismi ise bu durumda $A/A$ cebirsel ayrılabilirdir.

Kabul edelim ki $A/B$ fuzzy cisim genişlemesi cebirsel ayrılabilir ve tamamen ayrılamaz olsun. $x \in F$ ve $\lambda = A(x)$ olsun. Bu durumda $e \geq 0$ vardır öyle ki $x_\lambda^{p^e} \subseteq B$ olduğunda $A/B$ tamamen ayrılamazdır. Eğer $e = 0$ ise bu durumda $A(x) \leq B(x)$ ve bu yüzden $A(x) = B(x)$ dir. $e$ en küçük pozitif tam sayıyı olmak üzere $e > 0$ kabul edilsin. $A/B$ cebirsel ayrılabilir olduğundan $x_\lambda^{p^{e-1}} \subseteq B$ dir ve böylece $e - 1 = 0$ dır. Bu $x_\lambda \subseteq B$ ve böylece $A(x) = B(x)$ dir. O halde $A = B$ dir.

**Önerme 2.6.8.** $A/B$ bir cebirsel ayrılabilir fuzzy cisim genişlemesi olsun. Bu durumda

(i) $A_\#/B_\#$ cebirsel ayrılabilirdir.

(ii) $A^*/B^*$ cebirsel ayrılabilirdir.

**İspat.**

(i) $x \in A_\#$ ve L, $A_\#/B_\#$'nin bir ara cismi olsun. $x^p \in L$ kabul edilsin. D, F'nin fuzzy alt kümesi $z \in L$ ise $D(z) = 1$ ve $z \notin L$ ise $D(z) = B(z)$ şeklindedir. Bu durumda D, $A/B$ nin fuzzy ara cismidir öyle ki $D_\# = L$ dir. Şimdi $D(x) \leq D(x^p) = 1 = A(x)$ dir. Öyleyse Teorem 2.6.7'den $D(x) = 1$ dir. Dolayısıyla $x \in L$ dir. O halde $A_\#/B_\#$ cebirsel ayrılabilirdir.

(ii) $x \in A^*$ ve L, $A^*/B^*$ nin ara cismi olsun. $x^p \in L$ kabul edilsin. D, F'nin fuzzy alt kümesi $z \in L$ ise $D(z) = A(z)$ ve diğer durumlarda $D(z) = 0$ şeklindedir. Bu durumda D, $A/B$'nin bir fuzzy ara cismidir ve $D^* = L$ dir. Teorem 2.6.7'den, $D(x^p) = D(x)$ ya da $D(x) = A(x)$ dir. Öyleyse $D(x) > 0$ ve böylece $x \in D^* = L$ dir. Dolayısıyla $A^*/B^*$ cebirsel ayrılabilirdir.

**Önerme 2.6.9.** $A/B$ bir fuzzy cisim genişlemesi olsun. Eğer $A/B$ cebirsel ayrılabilir ise bu durumda $A/B$ ayrılabilirdir.

**İspat.** $A^*/B^*$ ayrılabilir olduğundan Önerme 2.6.3'ten $B^p = B \cap A^p$ olduğunu göstermek yeterlidir. $x \in F$ olsun. Bu durumda $x \notin F^p$ ise

$(B \cap A^p)(\mathrm{x}) = \mathrm{B}(\mathrm{x}) \wedge A^p(\mathrm{x}) = 0 = B^p(x)$.

$\exists z \in F$ için $x = z^p$ kabul edilsin. Bu durumda

$(B \cap A^p)(\mathrm{x}) = \mathrm{B}(z^p) \wedge A^p(z^p) = \mathrm{B}(z^p) \wedge \mathrm{A}(\mathrm{z}) = \mathrm{B}(\mathrm{z}) = B^p(z^p)$

Teorem 2.6.7'den $\mathrm{B}(z^p) = B(z)$ ise $B^p(x)$ ve $\mathrm{B}(z^p) > B(z)$ ise $A(z) = B(z) = B^p(x)$ dir. Böylece $B^p = B \cap A^p$ dir.

**Örnek 2.6.10.** P mükemmel cisminin karakteristiği $p > 0$, $F = P(x)$ ve x, P üstünde transandantal olsun. F'nin A ve B fuzzy alt kümeleri $z \in P$ ise $A(z) = 1 = B(z)$ ve $z \in F - P$ ise $A(z) = \frac{3}{4}$, $B(z) = \frac{1}{4}$ dür. Bu durumda $A/B$ bir fuzzy cisim genişlemesidir öyle ki $A_\# = B_\#$ ve $A^* = B^*$ dır. Böylece $A_\#/B_\#$ ve $A^*/B^*$ cebirsel ayrılabilirdir. D, F'nin fuzzy alt kümesi $z \in P$ ise $D(z) = 1$, $z \in P(x^p) - P$ ise $D(z) = \frac{1}{2}$ ve diğer durumlarda $D(z) = \frac{1}{4}$ şeklindedir. Bu durumda D, $A/B$ nin fuzzy ara

cismidir. Şimdi $A(x) = \frac{3}{4} \neq \frac{1}{4} = D(x) \neq D(x^p)$ dir. Böylelikle Teorem 2.6.7'den $A/B$ cebirsel ayrılabilir değildir.

**Önerme 2.6.11.** $F/K$ bir cisim genişlemesi olsun. Bu durumda $F/K$ cebirsel ayrılabilir olması için gerek ve yeter şart $\delta_F/\delta_K$ cebirsel ayrılabilirdir.

**İspat.** Kabul edelim ki $F/K$ cebirsel ayrılabilir olsun. D, $\delta_F/\delta_K$ nin fuzzy ara cismi olsun. Eğer $x \in K$ ise bu durumda $D(x) = 1 = D(x^p)$ dir. $x \notin K$ kabul edilsin. Bu durumda $K(x) = K(x^p)$ ve böylece $\exists k_i \in K, i = 0,1, \dots, n$ için $x = \sum_{i=0}^{n} k_i (x^p)^i$ dır. Böylelikle

$D(x) \geq \wedge\{D(k_i) \wedge D(x^{pi}) | i = 0,1, \dots, n\} = D(x^p)$.

Dolayısıyla $D(x) = D(x^p)$ dir. Böylece $\delta_F/\delta_K$ cebirsel ayrılabilirdir. Karşıt olarak, $\delta_F/\delta_K$ cebirsel ayrılabilir kabul edilsin. Bu durumda Önerme 2.6.8'den $F = (\delta_F)^*$ ve $K = (\delta_K)^*$ alındığında istenilen sonuç elde edilir.

**Önerme 2.6.12.** $A/B$ ve $B/C$ fuzzy cisim genişlemeleri olsun. Eğer $A/C$ cebirsel ayrılabilir ise bu durumda $A/B$ ve $B/C$ cebirsel ayrılabilirdir.

**İspat.** $x \in F$ olsun. D, $A/B$ nin fuzzy ara cismi olsun. Bu durumda D, $A/C$ nin fuzzy ara cismidir. Dolayısıyla ya $D(x) = D(x^p)$ ya da $D(x) = A(x)$ alınır. D, $B/C$ nin fuzzy ara cismi olsun. Eğer $D(x) = D(x^p)$ ise bu durumda istenilen sonuç elde edilir. $D(x) \neq D(x^p)$ kabul edilsin. Bu durumda $D(x) = A(x)$ dir. Dolayısıyla $D \subseteq B \subseteq A$ olduğunda $D(x) = B(x)$ dir.

**Önerme 2.6.13.** Eğer $A/B$ bir cebirsel ayrılabilir fuzzy cisim genişlemesi ise bu durumda $A = B \circ A^p$ dir.

**İspat.** Önerme 2.5.11'den $A/B \circ A^p$ tamamen ayrılamazdır. Önerme 2.6.12'den $A/B \circ A^p$ cebirsel ayrılabilirdir. Böylelikle Teorem 2.6.7'den göz önüne alınırsa $A = B \circ A^p$ dir.

**Örnek 2.6.14.** K cisminin karakteristiği $p > 0$, $F = K(\theta)$ ve $\theta$, K üstünde cebirsel ayrılabilir olsun. B, $\delta_K$ dan F'ye fuzzy alt cismi olsun. X, F'nin fuzzy alt kümesi $i = 1,2, \dots$ için $X\left(\theta^{p^i}\right) = i/(i+1)$ ve diğer durumlarda $X(z) = 0$ dır. C, X'den F'ye

herhangi bir alt fuzzy alt kümesidir öyle ki $B \subseteq C$ ve $X \subseteq C$ dir. Şimdi $i = 1,2, \ldots$ için $k_{ij} \in K$ alınırsa $\theta = \sum_{j=0}^{n} k_{ij}(\theta^{p^i})^j$ dır. Böylelikle $i = 1,2, \ldots$ için

$$C(\theta) \geq \wedge\left\{C\left(k_{ij}\left(\theta^{p^i}\right)^j\right) | j = 0,1, \ldots, n\right\} \geq \wedge\{C\left(k_{ij}\right) \wedge\ C((\theta^{p^i})^j) | j = 0,1, \ldots, n\}$$

$$= C\left(\theta^{p^i}\right) \geq X\left(\theta^{p^i}\right) = i/(i+1).$$

Böylece $C(\theta) = 1$ dir. Dolayısıyla $\big(B(X)\big)(0) = 1$ dir. Gerçekten $B(X) = \delta_F$ dir. Böylelikle $B(X)/B$ cebirsel ayrılabilirdir.

$X_i$ den F'ye fuzzy alt kümeleri $j = 1, .., i$ için $X_i\left(\theta^{p^i}\right) = j/(j+1)$ ve diğer durumlarda $i = 1,2, \ldots$ için $X_i(z) = 0$ şeklindedir. Bu durumda $\theta_1 \subseteq B(X)$ fakat $\theta_1 \nsubseteq B(X_i)$ dır. Dolayısıyla $X'$ den F'ye bir sonlu fuzzy alt kümesi yoktur öyle ki $X' \subseteq X$ ve $\theta_1 \subseteq B(X')$ dır.

## 3. TARTIŞMA VE SONUÇLAR

Bu çalışmada klasik cebir ve fuzzy cebir için bazı cisim genişlemeleri karşılaştırılmıştır. Cebirdeki bazı temel kavramların fuzzy cebirdeki halleri verilmektedir. Örneğin alt cisim ile fuzzy alt cisim, vektör uzayı ile fuzzy vektör uzayı, alt küme ile fuzzy alt küme, ara cisim ile fuzzy ara cisim, alt halka ile fuzzy alt halka arasında uyarlamalar ve karşılaştırmalar yapılmıştır. Bu yüzden çalışma iki kısımdan oluşmaktadır.

İlk aşamasında cebirsel tanım ve teoremler ele alınarak klasik cebirdeki cisim genişlemeleri ve bazı çeşitleri incelenmiştir. Cisim genişlemelerinin çeşitleri literatürde taranmıştır. Cisim genişlemeleri, Cebirsel Cisim Genişlemeleri, Geometrik Çizimler, İzomorfizmaların Genişletilmesi ve Otomorfizma Grupları, Parçalanma Cisimleri ve Normal Genişlemeler, Ayrılabilir Genişlemeleri, Tamamen Ayrılamaz Genişlemeler, Sonlu Genişlemeler ve Galois Genişlemeleri, Döngüsel Genişlemeler, Köklerle Çözülebilirlik, Simetrik Fonksiyonlar incelenmiş ve örneklendirilerek ele alınmıştır.

İkinci kısımda ise fuzzy cebir incelenmiş mevcut literatür taraması yapılmış ve klasik cebirdeki cisim genişlemelerinin karşılıkları fuzzy de aranmıştır. Fuzzy Cisim Genişlemeleri, Ayrılabilir Fuzzy Cisim Genişlemeleri ve Tamamen Ayrılamaz Fuzzy Cisim Genişlemeleri başlıkları ayrıntılı olarak ele alınmış ve klasik cebirdeki tanım ve teoremler fuzzy cebire taşınmış ve bu başlıklar için çeşitli örneklendirmeler yapılmıştır.

Bu çalışma klasik cebirdeki cisim genişlemeleriyle fuzzy cisim genişlemelerinin karşılaştırılması ve uyarlanması için bir örnektir.

# 4. ÖNERİLER

Bu çalışmada klasik cebirdeki cisim genişlemelerinden yola çıkarak fuzzy cisim genişlemelerinin ele alındığı görülmektedir. Örneğin "Ayrılabilir Cisim Genişlemeleri" fuzzy cebire uyarlanarak "Ayrılabilir Fuzzy Cisim Genişlemeleri" elde edilmiştir.

Benzer şekilde klasik cebirdeki birçok cebirsel tanım ve teorem fuzzy cebire uyarlanabilir. Diğer cisim genişlemeleri çeşitlerinin fuzzy cebirdeki karşılığı araştırılabilir.

## KAYNAKLAR


Asar, A.O., Arıkan, A. ve Arıkan, A. (2012). Cebir. Gazi Yayınları, 2. Baskı, ISBN: 978-605-344-002-4, 381s.

Çallıalp, F. (2013). Örneklerle Soyut Cebir. Birsen Yayınları, 1. Baskı, ISBN: 978-975-511-350-9, 343s.

Çallıalp, F. (2012). Soyut Matematik. Birsen Yayınları, 1. Baskı, ISBN: 978-975-511-417-3, 217s.

Das, P.S. (1981). Fuzzy groups and level subgroups. *Journal of Mathematical Analysis and Aplications*, 84, 264-269.

De-Gang, C. and Su-Yun, L. (1998). Fuzzy factor rings. *Fuzzy Sets and Systems,* 94, 125-127.

Dixit, V.N., Kumar, R. and Ajmal, N. (1992). On fuzzy rings. *Fuzzy Sets and Systems*, 49, 205-213.

Ersoy, B.A. (2003). A generalization of cartesian product of fuzzy subgroups and ideals. *Pakistan Journal of Applied Sciences*, 3(2), 100-102.

Fraleigh, J.B. (2013). Soyut Cebire Giriş 7. Baskıdan Çeviri. Palme Yayınları, 1. Baskı, ISBN: 978-605-355-127-0, 512, Terziler, M. ve Öner, T.( Ç. Ed.), 265-512.

Harmancı, A. (1987). Cebir 2. Hacettepe Üniversitesi Fen Fakültesi Yayınları, 77-103s.

Gezer, B. ve Bizim, O. (2017). Soyut Cebir. Dora Yayınları, 1. Baskı, ISBN: 9786059666756, 662 s.

Jacobson, N. (1964). Lectures in Abstract Algebra, Vol. III: Theory of fields and galois theory, Van Nostrand, Princeton University, New Jersey, USA.

Kara, G. (2014). Bulanık Kümelerin Halka ve İdeal Yapılarına Uygulanması. Yüksek Lisans Tezi. Ordu Üniversitesi, Fen Bilimleri Enstitüsü, Ordu, Türkiye, 57 s.

Karakaş, H.İ. (2008). Cebir Dersleri. Tüba Yayınları, 1. Baskı, ISBN: 9789944252232,420s, BİL, F.Ç, 281-388.

Katsaras, A.K. and Liu, D.B., (1977). Fuzzy vector spaces and fuzzy topological spaces. *Journal of Mathematical Analysis and Applications*, 58, 135-146.

Liu, W.J. (1982). Fuzzy invariant subgroups and fuzzy ideals. *Fuzzy Sets and Systems*, 8, 133-139.

Liu, W.J. (1983). Operations on fuzzy ideals. *Fuzzy Sets Systems,* 11, 31 -41.

Maiers, J. and Sherif, Y.S. (1985). Applications of fuzzy set theory. Institute of Electrical and Electronics Engineers Transactions on Systems, Man, and Cybernetics, Vol. SMC- 15, No. 1, 175- 189.

Mordeson, J.N. (1992). Fuzzy field extensions. *Fuzzy Sets and Systems*, 47, 253-264.

Mordeson, J.N. and Malik, D.S. (1990). Fuzzy subfields. *Fuzzy Sets and Systems*, 37, 383-388.

Mordeson, J.N. and Malik, D.S. (1991). Fuzzy vector spaces. *Information Sciences*, 55, 271-281.

Mordeson, J.N. and Malik, D.S. (1998). Fuzzy Commutative Algebra. World Scientific Publising, 1. Baskı, ISBN: 981-02-3628-X.

Mukherjee, N. and Bhattacharya, P. (1984). Fuzzy normal subgroups and fuzzy cosets. *Information Science*, 34, 225-239.

Nanda, S. (1986). Fuzzy fields and linear spaces. *Fuzzy Sets and Systems*, 19, 89-94.

Rosenfeld, A. (1971). Fuzzy groups. *Journal of Mathematical Analysis and Applications*, 35, 512-517.

Taşçı, D. (2010). Soyut Cebir. Gazi Yayınları, 2. Baskı, ISBN: 978-605-61746-0-5,665s.

Zadeh, L.A. (1965). Fuzzy sets. *Information and Control*, 8, 338-353.

# ÖZGEÇMİŞ

Neslihan YILMAZ, 1993 yılında Rize (Merkez)'de doğdu. Ortaöğretimini 2011 yılında Rize Güneysu Şehit Kemal Mutlu Anadolu Öğretmen Lisesi'nde tamamladı. 2011 tarihinde başladığı lisans eğitimini 2016 tarihinde Gazi Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde tamamladı. 2017 yılında Recep Tayyip Erdoğan Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda başladığı tezli yüksek lisans öğrenimini halen devam ettirmektedir. Rize Anadolu İmam Hatip Lisesi Kurumunda Öğretmen olarak 2016 yılı itibariyle görev yapmaktadır.