SOYUT CEBİR NOTLARI

İ. H. Denizler

18 Haziran 2015

İçindekiler

1 Giriş **3**
1.1 Temel Bilgiler 3

2 Grup **6**
2.1 YarıGrup, Monoid ve Grup 6
2.2 Homomorfizma ve Altgruplar 9
2.3 Devirli Gruplar 11
2.4 Yankümeler (Eşkümeler) 15
2.5 Normallik ve Bölüm Altgrupları 17
2.6 Simetri, Alterne ve Dihedral Gruplar 20

3 Grup Yapıları **23**
3.1 Sonlu Gerilmiş Abel Gruplar 23
3.2 Grup Etkileri 26
3.3 Sylow Teoremleri 29
3.4 Sonlu Grupların Sınıflandırması 31

4 Halka kavramı **32**
4.1 Halkalar 32
4.2 İdealler ve Homomorfizmalar 35
4.3 Tek Türlü Çarpanlama Bölgesi ve Euclid (Öklid) Bölgesi . . . 41
4.4 TÇB de Polinom Halkaları 43

5 Cisim Genişlemeleri **44**
5.1 İndirgenemez Polinomlar 44
5.2 Köklerin Katılması 46
5.3 Cebirsel Genişlemeler 48
5.4 Cebirsel KapalıCisimler 50

6 Normal ve Ayrılabilir Genişlemeler **51**
6.1 Açılım (Parçalanış) Cisimleri 51
6.2 Normal Genişlemeler 53
6.3 KatlıKökler 54
6.4 Sonlu Cisimler 56
6.5 Ayrılabilir Genişlemeler 57

Bölüm 1

Giriş

1.1 Temel Bilgiler

Bu alt bölümde bazı temel bilgilerin bir hatırlatmasını vereceğiz. Bununla birlikte bazı temel analiz ve soyut matematik bigilerinin okuyucu tarafından bilindiğini varsayıyoruz. Bu sebeple, mutad olan sembolleri, neyi temsil ettğini belirtmeden doğrudan kullanacağız. Mesela $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N}$ gibi.

Tanım 1.1.1 *Belirli nesnelerin kolleksiyonuna* küme*, her bir nesneye de bu kümenin bir* elemanı *denir. Elemanı olmayan kümeye ise* boş küme *denir ve* ϕ *ile veya* $\{\}$ *ile gösterilir.*

A bir küme ve a da bu kümenin bir elemanı ise bu, $a \in A$ ile gösterilir. $a, b \in A$ için $(a, b) = \{\{a\}, \{a, b\}\}$ ye bir **sıralı ikili** denir. $a, b, c, d \in A$ için, $(a, b) = (c, d)$ olması için gerek ve yeter şart $a = c, b = d$ olmasıdır.

Tanım 1.1.2 *Boş olmayan A ve B kümeleri verilsin. Elemanları sıralı ikililer olan*

$$A \times B = \{(x, y) | x \in A, y \in B\}$$

kümesine A ve B nin karteziyen çarpımı denir.

Buna göre $\mathbb{R} \times \mathbb{R}$, düzlemdeki bütün noktalara karşılık gelen tüm ikililerin kümesidir.

Tanım 1.1.3 *A ve B verilmiş kümeler olsun. A nın her elemanı B nin de bir elemanı ise A ya B nin bir altkümesidir denir ve $A \subseteq B$ ile gösterilir.*

Tanım 1.1.4 *A ve B kümeleri verilsin. $A \times B$ nin bir $\mathcal{R}$ alt kümesine A dan B ye bir bağıntı denir. $A = B$ ise $\mathcal{R}$ ye A da bir bağıntıdır denir.*

Tanım 1.1.5 *$\mathcal{R}$, A da bir bağıntı ve $a, b, c, \in A$ olsun. Şayet $\mathcal{R}$,*

(i) $(a, a) \in \mathcal{R}$, $\forall a \in A$ *(yansıma öz.)*

(ii) $(a, b) \in \mathcal{R} \Rightarrow (b, a) \in \mathcal{R}$ *(simetri öz.);*

(iii) $(a, b) \in \mathcal{R}$ *ve* $(b, c) \in \mathcal{R}$ *iken* $(a, c) \in \mathcal{R}$*(geçişme öz.);*

(iv) $(a, b) \in \mathcal{R}$ *ve* $(b, a) \in \mathcal{R}$ *ise* $a = b$ *(ters simetri öz.).*

özelliklerinden ilk üçünü sağlıyorsa bir denklik bağıntısı, i, iii ve iv özelliklerini sağlıyorsa bir sıralama bağıntısıdır.

Tanım 1.1.6 *A bir küme ve $\mathcal{R}$, A da bir sıralama bağıntısı olsun. Bu durumda A ya ($\mathcal{R}$ altında) kısmi sıralı bir küme denir.*

Örnekler :

a. X, elemanları kümeler olan bir küme olsun. X, $\subseteq$ bağıntısı altında bir kısmi sıralı kümedir.

b. $\leqslant$, $\mathbb{R}$ reeel sayılar kümesi üzerinde bir sıralama bağıntısı oluşturur.

c. $x \equiv y(\mathrm{mod\ n})$, modül n ye göre kalan sınıflarını oluşturma $\mathbb{Z}$ üzerinde bir denklik bağıntısıdır. $(x \equiv y(\mathrm{mod\ n}) \Leftrightarrow n \mid x - y)$

Tanım 1.1.7 *A bir küme, $\mathcal{R}$, A da bir denklik bağıntısı ve $a, b \in A$ olsun. $a \in A$ ya denk olan elemanların $\{x \in A : (x, a) \in \mathcal{R}\}$ kümesine a nın denklik sınıfı denir ve $[a]$ veya $\bar{a}$ ile gösterilir. $(a, b) \in \mathcal{R}$ ise, simetri özelliğinden dolayı, $\bar{a} = \bar{b}$ dir.*

$\mathcal{R}$ nin A da oluşturduğu denklik sınıflarının kümesini $A/\mathcal{R}$ ile gösteririz. Buna göre; $\forall a \in A$ için $\bar{a} \neq \emptyset$ ve

$$\bigcup_{a \in A} \bar{a} = A = \bigcup_{\bar{a} \in A/\mathcal{R}} \bar{a}$$

dir. Üstelik, $a, b \in A$ için $\bar{a} \bigcap \bar{b} = \emptyset$ veya $\bar{a} = \bar{b}$ dir.

Tanım 1.1.8 *A bir küme ve $\{A_i | i \in I\}$, A nın altkümelerinin bir ailesi olsun. Bu durumda*

(i) $\forall\, i \in I$ *için* $A_i \neq \emptyset$*;*

(ii) $\bigcup_{i\in I} A_i = A$*;*

(iii) $A_i \bigcap A_j = \emptyset$, $\forall i \neq j \in I$*;*

sağlıyorsa $\{A_i | i \in I\}$ ya A nın bir parçalanışı (ayrşımı) denir.

Teorem 1.1.9 *A bir küme ve $\mathcal{R}$, A da bir denklik bağıntısı olsun. Bu durumda $A/\mathcal{R}$, A nın bir parçalanışını verir. Tersine, P, A nın bir parçalanışı olsun. Bu durumda A da (yalnız) bir $\mathcal{R}$ bağıntısı vardır öyleki $A/\mathcal{R} = P$ dir. (*Gösteriniz.*)*

Bu teoremin bir sonucu olarak:

Sonuç 1.1.10 *A, boş olmayan bir küme olsun. Bu durumda $E(A)$ ve $Q(A)$, sırasıyla, A daki tüm denklik bağıntılarını ve A nın tüm parçalanışlarını göstermek üzere;*

$$\begin{array}{rccc} \psi: & E(A) & \longrightarrow & Q(A) \\ & \mathcal{R} & \longmapsto & A/\mathcal{R} \end{array}$$

fonksiyonu birebir örten bir dönüşümdür. (bak[5])

Tanım 1.1.11 *G boştan farklı bir küme olsun. $(a, b) \longmapsto a\star b$ ile tanımlanan $\star : G \times G \longrightarrow G$ fonksiyonuna bir ikili işlem denir ($a \star b \in G$). Burada $\star$, verilen tarife göre, çarpma, toplama ya da değişik bir işlem olabilir. Genel olarak $a \star b$ yerine ab kullanılır.*

Bölüm 2

Grup

2.1 Yarı Grup, Monoid ve Grup

Tanım 2.1.1 *Boş olmayan bir G kümesi üzerinde*

$$\begin{aligned} * : \ G \times G &\longrightarrow G \\ (a,b) &\longmapsto a * b \end{aligned}$$

ikili işlemi tanımlansın. Bu durumda G,

(i) $\forall a,b,c, \in G$ *için* $(a*b)*c = a*(b*c)$, *(*birleşme öz.*)*

(ii) $\exists\, e \in G$ *öyleki* $\forall a \in G$ *için* $a*e = e*a = a$, *(*birim eleman öz.*)*

(iii) $\forall\, a \in G$ *için* $\exists b \in G$ *öyleki* $a*b = b*a = e$, $b := a^{-1}$ *(*ters eleman öz.*)*

(iv) $\forall\, a,b \in G$ *için* $a*b = b*a$, *(*değişme öz.*)*

özelliklerinden, sırasıyla, i sağlanıyorsa **yarı grup**, *i ve ii sağlanıyorsa* **monoid**, *i,ii ve iii sağlanıyorsa* **grup**, *i, ii, iii ve iv sağlanıyorsa* **Abel grup** *veya* **değişmeli grup** *adını alır.*

Not : Bazı yazarlar $*$ ikili işleminin tanımlı olmasını, yani $\forall\, a,b \in G$ için $a*b \in G$ sağlamasını ayrı bir özellik (kapalılık) olarak vermekte olup, buna göre, yarı grup, monoid, grup ve Abel grup kapalılık özelliğini sağlayan yapılardır.

Tanım 2.1.2 *Bir G grubunun elaman sayısına G nin mertebesi denir ve $|G|$ ile göstrilir. Şayet $|G| < \infty$ ise G ye sonlu, aksi takdirde sonsuz grup denir.*

Notasyon: G bir grup ve $*$, G de tanımlı ikili işlem olsun. Üzerinde tanımlı işlemin belirtilmesi gerektiğinde G grubu $(G,*)$ ile gösterilir. Üstelik, $\forall\, a \in G$ ve $\forall\, n \in \mathbb{N}$ için $a^n = \underbrace{a * a * \ldots * a}_{\text{n-tane}}$ ve $a^{-n} = \underbrace{a^{-1} * a^{-1} * \ldots * a^{-1}}_{\text{n-tane}}$ ile tanımlıdır. $n = 0$ için $a^n = e$ dir. İşlem belirtilmedikce $a, b \in G$ için $a * b$ yerine ab kullanacağız.

Teorem 2.1.3 *G bir grup olsun. Bu durumda:*

(i) $\exists! e \in G$ *(*birim eleman tektir.*);*

(ii) $a \in G$ *için* $a^2 = a$ *ise* $a = e$ *dir. (*idempotent eleman yalnız e*);*

(iii) $\forall a, b, c \in G$ *için* $ab = ac$ *veya* $ba = ca$ *ise* $b = c$ *dir. (*sırasıyla, soldan ve sağdan kısaltma*)*

(iv) $\forall a \in G$ *için* $\exists! a^{-1} \in G$ *(*her elemanın tersi var ve tek*);*

(v) $\forall a \in G$ *için* $(a^{-1})^{-1} = a$*;*

(vi) $\forall a, b \in G$ *için* $(ab)^{-1} = b^{-1}a^{-1}$*;*

dir.

Teorem 2.1.4 *G bir grup ve $a, b \in G$ verilsin. $ax = b$ ve $ya = b$ eşitlikleri G de yalnız bir çözüme sahiptir.*

Örnek 2.1.5 *G, H birer grup olsun. $G \times H = \{(g,h) | g \in G$ ve $h \in H\}$ karteziyen çarpımı üzerinde $*$ işlemi, $(g_1, h_1) * (g_2, h_2) = (g_1 g_2, h_1 h_2)$ ile tanımlansın. Bu durumda $(G \times H, *)$ bir gruptur (*gösteriniz*). Bu gruba G ile H ın* direkt çarpım grubu *denir. Bu grubun birimi (e_G, e_H) ve $(g,h)^{-1} = (g^{-1}, h^{-1})$ dir (burada e_G ve e_H, sırasıyla, G ve H ın birimleri).*

Örnek 2.1.6 *$X \neq \emptyset$ olmak üzere $S_X = \{f | f : X \longrightarrow X$* bire-bir ve örten*$\}$ fonksiyonlar kümesi üzerinde "o" bileşke işlemi iyi tanımlı olup (S_X, o) bir gruptur* (gösteriniz)*. Bu gruba* **permütasyon grubu** *denir. özel olarak $X = \{1, 2, \ldots, n\}$ için S_X* **Simetrik grup** *adını alır ve* $\mathbf{S_n}$ *ile gösterilir.*

Örnek 2.1.7 *Bir düzlemde düzgün çokgenin (n-gen) simetrik hareketlerinin oluşturduğu kümeyi D_n ile gösterelim. Sabit nokta etrafında saatin aksi yönünde $2\pi/n$ radyanlık dönüşü σ, sabit nokta ile ilk köşeden geçen eksene göre yansımayı τ ile gösterelim. Buna göre, bu hareketlerin bileşkesi altında D_n bir grup oluşturur ($n = 4$* için gösteriniz*). Bu grup $n = 4$ için $D_4 = \{\iota, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$ olup $|D_4| = 8$ dir (ι, birim dön.).*

Teorem 2.1.8 *G bir yarı grup olsun. Şayet G nin sağ birimi ve G deki her elemanın sağ tersi varsa G bir grup olur.*

Uyarı: Yukarıdaki teorem, sol birim ve sol ters için de sağlar fakat, çapraz durumda, yani, sağ birim ve sol ters veya sol birim ve sağ ters varlığı durumunda sağlamak zorunda değildir.

Örnek 2.1.9 $G = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{R} \right\} \setminus \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, *$2\times 2$-tipli üst satır matrislerin kümesi matris çarpımı işlemi altında bir yarıgruptur.*
$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ *ve* $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ *olup,*
$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ *sol birim fakat sağ birim değil. Öte yandan $a \neq 0$ için*
$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1/a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ *ve* $\begin{bmatrix} 1/a & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & b/a \\ 0 & 0 \end{bmatrix}$ *olup,*
$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ *nin sağ tersi var fakat sol tersi yok. Dolayısıyla G bir grup değildir.*

Önerme 2.1.10 *G bir yarı grup olsun. Bu durumda G nin bir grup olması için gerek ve yeter şart, her $a, b \in G$ için $ax = b$ ve $ya = b$ eşitliklerinin G de bir çözümünün olmasıdır.*

Önerme 2.1.11 *G bir grup olsun. Aşağıdaki şartlardan birini sağladığı takdirde G bir Abel gruptur:*

(i) $\forall a, b \in G$ *için* $(ab)^2 = a^2b^2$*;*

(ii) $\forall a, b \in G$ *için* $(ab)^{-1} = a^{-1}b^{-1}$*;*

(iii) $\forall a \in G$ *için* $a^2 = e$*;*

(iv) $\forall a, b \in G$ *ve* $\forall n \in \mathbb{Z}^+$ *için* $(ab)^n = a^n b^n$, $(ab)^{n+1} = a^{n+1}b^{n+1}$ *ve* $(ab)^{n+2} = a^{n+2}b^{n+2}, (n > 2)$*;*

NOT: yukarıdaki *iv.* özellik ardışık üç sayı için sağlamadığında G Abel olmayabilir.

Örnek 2.1.12 $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ *kuaternion-8 grubu Abel değildir* (gösteriniz).

2.2 Homomorfizma ve Altgruplar

Tanım 2.2.1 *G ve H birer yarı grup olsunlar. $\forall a, b \in G$ için $f(ab) = f(a)f(b)$ sağlayan $f : G \longrightarrow H$ fonksiyonuna bir* homomorfizma *veya* homomorfizm *denir. Bu durumda f, bire-bir ise bir* monomorfizma*, örten ise bir* epimorfizma*, bire-bir ve örten ise bir* izomorfizma *dır. f in bir izomorfizma olması $G \cong H$ ile gösterilir. $f : G \longrightarrow G$ homomorfizmasına bir* endomorfizma *denir. Bu durumda, bire-bir örten olması halinde f bir* otomorfizma *adını alır. $f : G \longrightarrow H$ ve $g : H \longrightarrow K$ iki yarıgrup homomorfizması olsun. Bu durumda $gf : G \longrightarrow K$ da bir homomorfizma olup f ve g nin ortak yapılarına (monomorfizma, epimorfizma, izomorfizma gibi) sahiptir.*

Önerme 2.2.2 *$f : G \longrightarrow H$ bir grup homomorfizması olsun. (G ve H birer grup, f, homomorfizma.) Bu durumda $f(e_G) = e_H$ ve $\forall a \in G$ için $f(a^{-1}) = (f(a))^{-1}$ dir. (Bu özellikler yarı-gruplar için sağlamayabilir.)*

Örnek 2.2.3 $f : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}_m \\ n & \longmapsto & \bar{n} \end{array}$ *dönüşümü bir grup epimorfizmasıdır.*

Örnek 2.2.4 *G bir Abel grup olsun. Bu durumda:*

(i) $a \mapsto a^{-1}$ ile tanımlı $f : G \longrightarrow G$ dönüşümü bir grup otomorfizmasıdır ($a \in G$).

(ii) $a \mapsto a^2$ ile tanımlı $f : G \longrightarrow G$ dönüşümü bir grup endomorfizmasıdır ($a \in G$).

Tanım 2.2.5 *$f : G \longrightarrow H$ bir grup homomorfizması olsun. Bu durumda:*

(i) Çek$(f) = \{a \in G | f(a) = e_H\}$ ye f in çekirdeği *denir;*

(ii) $A \subseteq G$ olmak üzere $f(A) = \{b \in H | b = f(a),\ \exists a \in A\}$ kümesine A nın f altında görüntüsü *denir, $A = G$ halinde bu küme $\mathrm{Im}(f)$ ile gösterilir;*

(iii) $B \subseteq H$ olmak üzere $f^{-1}(B) = \{a \in G | f(a) \in B\}$ kümesine B nin f altında ters görüntüsü *veya* öngörüntüsü *denir.*

Tanım 2.2.6 *G bir grup $H \subseteq G$ boş olmayan bir küme olsun. H, G de tanımlı işlem altında bir grup oluşturuyorsa H ye G nin bir altgrubudur denir ve $H \leqslant G$ ile gösterilir.*

Yukarıdaki tanıma örnek olarak, $G \leqslant G$ ve $\{e\} \leqslant G$ birer alt gruptur. Bunlardan ikincisine özel olarak *aşikâr altgrup* denir. Bu ikisinin dışında, $H \leqslant G$ sağlayan her H altgrubuna G nin *öz altgrubu* ya da *has altgrubu* denir, $H < G$ ile gösterilir.

Teorem 2.2.7 *H bir G grubunun altkümesi olsun. Bu durumda:*

$$H \leqslant G \Leftrightarrow \forall a, b \in H \text{ için } ab^{-1} \in H$$

dir.

Teorem 2.2.8 *$f : G \longrightarrow H$ bir grup homomorfizması olsun. Bu durumda:*

(i) $\text{Çek}(f) = \{a \in G | f(a) = e_H\} \leqslant G$;

(ii) $A \leqslant G$ *ise* $f(A) = \{b \in H | b = f(a),\ \exists a \in A\} \leqslant H$;

(iii) $B \leqslant H$ *ise* $f^{-1}(B) = \{a \in G | f(a) \in B\} \leqslant G$ *dir.*

Teorem 2.2.9 *$f : G \longrightarrow H$ bir grup homomorfizması olsun. Bu durumda:*

(i) *f bir monomorfizma* $\Leftrightarrow \text{Çek}(f) = \{e_G\}$;

(ii) *f bir izomorfizma* $\Leftrightarrow \exists f^{-1} : H \longrightarrow G$ *(grup homomor.) öyleki* $fof^{-1} = 1_H$ & $f^{-1}of = 1_G$.

Örnek 2.2.10 $n\mathbb{Z} = \{nz : n \in \mathbb{Z} \quad \text{sabit}, z \in \mathbb{Z}\}$, $(\mathbb{Z}, +)$ *nin bir altgrubudur.* (gösteriniz).

Ödev 2.2.11 *G bir grup ve $H_1, H_2 \leqslant G$ olsun. Bu durmda $H_1 \cap H_2 \leqslant G$ dir, gösteriniz. Daha genel olarak; G nin altgruplarının bir $\{H_i : i \in I\}$ ailesi için, $\bigcap_{i \in I} H_i \leqslant G$ dir, gösteriniz.*

Tanım 2.2.12 *G bir grup, X, G nin bir altkümesi ve $\{H_i : i \in I\}$ de X i barındıran bütün H_i altgruplarının ailesi olsun. Bu durumda $\bigcap_{i \in I} H_i$ ye G de X in gerdiği (doğurduğu-ürettiği) altgrup denir ve $< X >$ ile gösterilir. Şayet $X = \{a_1, \ldots, a_t\}$ sonlu bir küme ise bu durmda $< X > = < a_1, \ldots, a_t >$ yazarız, $a_i \in G$. Eğer $G = < a_1, \ldots, a_t >$ ise G ye sonlu gerilmiştir denir (G nin kendisi sonlu olmak zorunda değil).*

Yukarıdaki tanıma göre $X \subseteq G$ için $< X >$ altgrubunun elemanları $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ sonlu çarpımından oluşur $(a_i \in X, n_i \in \mathbb{Z})$.

Tanım 2.2.13 *G bir grup olsun. $C = \{a \in G | ax = xa,\ \forall x \in G\}$ kümesine G nin* merkezi *denir ve $Z(G)$ ile gösterilir.*

Ödev 2.2.14 *$Z(G) \leqslant G$ dir, gösteriniz.*

2.3 Devirli Gruplar

Tanım 2.3.1 *G bir grup ve $a \in G$ olsun. $G =< a >$ ise G ye bir devirli grup denir. Şayet $G = \{a^m | m \in \mathbb{Z}\} = \{\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\}$ ise G ye sonsuz devirli grup, $G =< a : a^n = 1, \exists\, n \in \mathbb{N}^+ >= \{a, a^2, \ldots, a^{n-1}, a^n = 1\}$ ise G ye n-mertebeli (sonlu) devirli grup denir (Burada 1, birimi temsil etmekte).*

Devirli grubun temel özellikleri: $G =< a >$ verilsin. Bu durumda:

(i) $|G|$ sonsuz ise;

  (a) $a^k = 1 \Leftrightarrow k = 0$;

  (b) $i \neq j$ için $a^i \neq a^j$, tüm elemanlar biribirinden farklı.

(ii) $|G| = n$ (G, n-mertebeli) ise;

  (a) $a^n = 1$ yapan en küçük pozitif tam sayı n dir;

  (b) $G = \{a, a^2, \ldots, a^{n-1}, a^n = 1\}$ biribirinden farklı n-elemandan oluşur.

Teorem 2.3.2 *$\mathbb{Z}$ toplamsal grubunun her H alt grubu devirlidir. Üstelik $H =< 0 >$ veya $\exists\, m \in \mathbb{Z} : H =< m >$ ve $|H|$ sonsuz, burada $m \in H$ ve m, H ta barınan en küçük pozitif tam sayı.*

Teorem 2.3.3 *G, n-mertebeli bir devirli grup ve $G =< a >$ olsun. Bu durumda:*

(i) $a^k = 1 \Leftrightarrow n \mid k$ *($k \in \mathbb{N}$);*

(ii) $a^r = a^s \Leftrightarrow r \equiv s \,(\mathrm{mod\ n})$ *($r, s \in \mathbb{Z}$);*

(iii) *$k \mid n$ ise $|a^k| = n/k$ dir.*

Teorem 2.3.4 *(i) Her sonsuz devirli grup, $\mathbb{Z}$ toplamsal grubuna, ve*

(ii) n-mertebeli devirli grup, $\mathbb{Z}_n$ toplamsal grubuna izomorftur.

Teorem 2.3.5 *Bir G devirli grubunun her altgrubu da devirlidir.*

Devirli Gruplarda Üreteçler

I-Sonsuz devirli gruplarda üreteçler: $\mathbb{Z}$ de belirlenecek her eleman izomorfizma yoluyla diğer sonsuz gruplara taşınacağından $\mathbb{Z}$ deki üreteçleri belirlememiz yeterli olacaktır. Bir $m \in \mathbb{Z}$ için $< m >= \mathbb{Z}$ olsun. $< 1 >= \mathbb{Z}$ olup $1 \in < m >$ dir. O halde;

$$1 \in < mk : k \in \mathbb{Z} > \Rightarrow 1 = mk,\ \exists\, k \in \mathbb{Z} \Rightarrow m = 1/k \Rightarrow k = \pm 1 \Rightarrow m = \pm 1$$

Böylece $\mathbb{Z} =< 1 >=< -1 >$. Yani sonsuz devirli grupların yalnız iki üreteci vardır. Buna göre, bir G sonsuz devirli grubu için $G =< a >=< a^{-1} >$ dir $(a \in G)$.

II-Sonlu devirli gruplarda üreteçler: $\mathbb{Z}_n$ de belirlenecek her eleman izomorfizma yoluyla n-mertebeli başka gruplara taşınabileceğinden $\mathbb{Z}_n$ deki üreteçleri bulmamız yeterlidir. $\bar{k} \in \mathbb{Z}_n$ ve $< \bar{k} >= \mathbb{Z}_n$ olsun. $< \bar{1} >= \mathbb{Z}_n$ olup $\bar{1} \in < \bar{k} >$ olmalıdır. Bu da

$$\bar{1} \in < \bar{k} > \Leftrightarrow \bar{1} \in < \bar{k}m : m \in \mathbb{Z} > \Leftrightarrow 1 \equiv mk(\text{mod n}) \Leftrightarrow 1 = mk+nq \Leftrightarrow (k,n) = 1$$

$(q \in \mathbb{Z})$. Buna göre $G =< a : a^n = 1 >$ için $G =< a^k > \Leftrightarrow (k,n) = 1$.

Ödev 2.3.6 *$\mathcal{U}(\mathbb{Z}_n)$ üreteçler kümesi çarpma işlemi altında $\Phi(n)$ (Euler fonk.) mertebeli bir grup oluşturur. (*Bunu bazen $\mathbb{Z}_n^\star$ ile de gösteririz.*)*

Teorem 2.3.7 *$f : G \longrightarrow H$ bir grup homomorfizması, $a \in G$ ve $|a| = n$ olsun.*

(i) $|f(a)| \Big| |a|$;

(ii) $G \cong_f H$ *ise* $|f(a)| = |a|$.

Teorem 2.3.8 *Her devirli grup Abeldir.*

Önerme 2.3.9 *G bir grup, $H \leqslant G$ ve $K \leqslant G$ olsun. Bu durmda*

$$H \cup K \leqslant G \Leftrightarrow H \subseteq K \text{ veya } K \subseteq H\ .$$

Ödev 2.3.10 *G_1 ve G_2 iki sonlu devirli grup olsun. $G_1 \times G_2$ çarpım grubu hangi şartlar altında devirli olur, gösteriniz.*

Sonuç 2.3.11 *Yukarıdaki ödevin bir sonucu olarak:*

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \Leftrightarrow (m,n) = 1 \ .$$

Yani $\mathbb{Z}_m \times \mathbb{Z}_n$ *nin devirli olması için gerek ve yeter şart* $(m,n) = 1$ *olmasıdır.*

Teorem 2.3.12 $G =< x >$ *devirli grubu verilsin. Bu durumda:*

(i) $H \leqslant G$ *ise* $H =< x^l >$ *veya* $H =< e >$ *dir. Burada* l, $x^l \in H$ *sağlayan en küçük pozitif tam sayıdır. Şayet* $m = |G| < \infty$ *ise* $l \mid m$ *ve* $|H| = m/l$ *dir.* $|G| = \infty$ *ise* $|H| = \infty$ *ya da* $|H| =< e >$ *dir;*

(ii) Tersine, $|G| = m$ *ve* $l \mid m$ $(l \in \mathbb{Z}^+)$, *ise* $| < x^l > | = m/l$ *dir, yani* $q \in \mathbb{Z}^+$, $q|m \Rightarrow \exists\, S \leqslant G : |S| = q$ *;*

(iii) $H_i \leqslant G$ *sağlayan biribirinden farklı* H_i *alt gruplarının sayısı,* $m = |G|$ *sayısının farklı pozitif bölenlerinin sayısı kadardır* $(m < \infty)$*;*

(iv) Sonlu bir G *devirli grubunun herhangi bir mertebeden* $(\leqslant |G|)$ *en çok bir altgrubu vardır.*

Ödev 2.3.13 $m, n \in \mathbb{Z}$, $m\mathbb{Z} \leqslant \mathbb{Z}$, $n\mathbb{Z} \leqslant \mathbb{Z}$ *verilsin.* $m\mathbb{Z} + n\mathbb{Z} =?$ *Yani* $H = \{ms + nr : s, r \in \mathbb{Z}\} =?$ *(Burada* $m\mathbb{Z} + n\mathbb{Z} =< m\mathbb{Z} \cup n\mathbb{Z} >$ *dir)*

Teorem 2.3.14 (Bölme Algoritması) *Sıfırdan farklı her* $a, b \in \mathbb{Z}$ *sayısı için* $q, r \in \mathbb{Z}$ *sayıları vardır öyleki* $a = b\,q + r$ *ve* $0 \leqslant r < |b|$, q *ve* r *tekdir.*

Önteorem 2.3.15 $d = (a, b)$ *ise* $\exists\, m, n \in \mathbb{Z} : d = ma + nb$, $(a, b, d \in \mathbb{Z})$.

Yukarıdaki önteoremde verilen $m, n \in \mathbb{Z}$ ler tek değildir. Nitekim $\forall\, k \in \mathbb{N}$ için, $(a, b) = m\,a + n\,b = (m + k\,b)a + (n - k\,a)b$ dir.

Örnek 2.3.16 $(726, 275) = d$ *ise* $d = a\,726 + b\,275$ *yapan* a, b, d *sayılarını bulunuz.*

Tanım 2.3.17 $(a, b) = 1$ *yapan* $a, b \in \mathbb{Z}^+$ *sayılarına aralarında asaldır denir.*

Teorem 2.3.18 $G =< a >$ *ve* $|G| = n$ *verilsin.* $b \in G$, $a^s = b$ *ve* $(n, s) = d$ *olsun. Bu durumda* $H =< b >$ *için* $|H| = n/d$ *dir.*

Teorem 2.3.19 (Fermat) *Bir $a \in \mathbb{Z}$ tam sayısı ve $p \in \mathbb{N}$ asal sayısı için;*

$$\begin{aligned} p \nmid a &\Rightarrow p \mid a^{p-1} - 1 \\ &\Rightarrow a^{p-1} \equiv 1 (\mathrm{mod}\, p) \\ &\Rightarrow a^{p} \equiv a (\mathrm{mod}\, p) \end{aligned}$$

Teorem 2.3.20 (Euler) *Bir $a \in \mathbb{Z}$ tam sayısı ve $n \in \mathbb{N}$ doğal sayısı için;*

$$\begin{aligned} (a,n) = 1 &\Rightarrow n \mid a^{\Phi(n)} - 1 \\ &\Rightarrow a^{\Phi(n)} \equiv 1 (\mathrm{mod}\, n) \end{aligned}$$

Tanım 2.3.21 (Euler Φ fonksiyonu) *Bir $n \in \mathbb{Z}^+$ için $1 \leqslant a \leqslant n$ ve $(a,n) = 1$ yapan $a \in \mathbb{Z}$ lerin sayısı $\Phi(n)$ fonksiyonuyla gösterilir ve buna Euler Φ fonksiyonu denir.*

Özellikleri: $p \in \mathbb{Z}$ bir asal sayı olsun. Bu durumda;

E1: $\Phi(p) = p - 1 = p(1 - \frac{1}{p})$;

E2: $s \in \mathbb{N}$ için $\Phi(p^s) = p^s - p^{s-1} = p^s(1 - \frac{1}{p})$;

E3: $(m,n) = 1 \Rightarrow \Phi(mn) = \Phi(m)\Phi(n)$ dir;

E4: $m = p_1^{s_1} p_2^{s_2} p_3^{s_3} \cdots p_r^{s_r}$, öyleki p_i ler asal sayı ve $s_i \in \mathbb{Z}^+$, $1 \leqslant i \leqslant r$ ise

$$\begin{aligned} \Phi(m) &= \Phi(p_1^{s_1} p_2^{s_2} p_3^{s_3} \cdots p_r^{s_r}) \\ &= \Phi(p_1^{s_1})\Phi(p_2^{s_2})\Phi(p_3^{s_3}) \cdots \Phi(p_r^{s_r}) \\ &= p_1^{s_1} p_2^{s_2} p_3^{s_3} \cdots p_r^{s_r} (1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \cdots (1 - \frac{1}{p_r}) \\ &= m \left((1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \cdots (1 - \frac{1}{p_r}) \right) \end{aligned}$$

2.4 Yankümeler (Eşkümeler)

Tanım 2.4.1 *G bir grup $H \leqslant G$, $a, b \in G$ olsun. Şayet $ab^{-1} \in H$ oluyorsa a, $(\mathrm{mod\ H})$ a göre b ye sağ denktir denir. Bu, $a \equiv_r b\,(\mathrm{mod\ H})$ ile gösterilir. Eğer a, b ye sol denk ise $a^{-1}b \in H$ ve $a \equiv_l b\,(\mathrm{mod\ H})$ dir.*

Yukarıdaki tanıma göre G Abel ise sağ ve sol denklik aynıdır. Bunun tersi doğru değildir, yani, sağ ve sol denkliğin aynı olması grubun Abel olmasını gerektirmez.

Teorem 2.4.2 *G bir grup, $H \leqslant G$ olsun. Bu durumda,*

(i) G de $(\mathrm{mod\ H})$ a göre sağ (sol) denklik bir denklik bağıntısıdır;

(ii) Bir $a \in G$ nin yukarıdaki bağıntıya göre denklik sınıfı, sağ ve sol denklik için, sırasıyla: $Ha = \{ha : h \in H\}$ ve $aH = \{ah : h \in H\}$ dir;

(iii) $\forall\, a \in G$ için $|Ha| = |H| = |aH|$, (eleman sayısı olarak).

Tanım 2.4.3 *Theorem 2.4.2 de verilen Ha ve aH denklik sınıflarına H alt-gubunun, sırasıyla, bir sağ yankümesi (sağ eş-kümesi) ve bir sol yankümesi (sol eş-kümesi) denir.*

Sonuç 2.4.4 *G bir grup, $H \leqslant G$ olsun.*

(i) $G = \bigcup_{a \in G} Ha$; yani G, H ın sağ (sol) yankümelerinin bir birleşimidir;

(ii) H ın G deki herhangi iki sağ (sol) yankümesi ayrık ya da aynıdır.

(iii) $a, b \in G$ için $Ha = Hb \Leftrightarrow ab^{-1} \in H$ ve $aH = bH \Leftrightarrow a^{-1}b \in H$ dır;

(iv) H ın G deki sol ve sağ yankümelerinin sayısı eşittir.

Toplamsal Notasyon: G bir toplamsal grup ise

$$a \equiv_r b\,(\mathrm{mod\ H}) \Leftrightarrow a - b \in H, \qquad (H \leqslant G)$$

olarak tanımlanır. Buna göre sağ yankümeler $H + a = \{h + a : h \in H\}$ şeklindedir.

Tanım 2.4.5 *G bir grup ve $H \leqslant G$ olsun. H ın G deki tüm sol (veya sağ) yankümelerinin sayısına H ın G deki indeksi denir ve $[G : H]$ ile gösterilir.*

$|G|$ ve $|H|$ sonsuz iken $[G : H]$ sonlu olabilir. Nitekim $\mathbb{Z}$ toplamsal grubu için, $G = \mathbb{Z}$, $H = 3\mathbb{Z}$ olsun. Bu durumda H ın sol yankümeleri $0+3\mathbb{Z}$, $1+3\mathbb{Z}$, $2+3\mathbb{Z}$ olup $[\mathbb{Z} : 3\mathbb{Z}] = 3$ tür. Oysa $\mathbb{Z}$ ve $3\mathbb{Z}$ sonsuz mertebeden gruplardır. Şayet $H =< e >$ ise, her a elemanı için $Ha = \{a\}$ olup, $[G : H] = |G|$ dir. Herbir Ha_i yan kümesinin a_i temsili elemanlarından oluşan $\{a_i\}_{i\in I}$ kümesi $[G : H]$ tane elamandan oluşur ($a_i \in Ha_i$). Önceki örneğe göre $\{a_i\}_{i\in I} = \{0, 1, 2\}$ olur.

Teorem 2.4.6 *G bir grup, $H \leqslant G$, $K \leqslant H$ olsun. Bu durumda $[G : K] = [G : H][H : K]$ dır.*

Teorem 2.4.7 (Lagrange) *G bir grup ve $H \leqslant G$ olsun. Bu durumda $|G| = [G : H]|H|$. G sonlu ise, $a \in G$ için $|a|\Big||G|$ dir.*

Teorem 2.4.8 *G bir grup, $H \leqslant G$, $K \leqslant G$ sonlu alt gruplar olsun. Bu durumda $|HK| = |H|\,|K|/|H \cap K|$ dır.*

Burada $HK = \{ab|\, a \in H,\ b \in K\}$. Üstelik HK nın bir altgrup olması gerekmez.

Önerme 2.4.9 *G bir grup, $H \leqslant G$ ve $K \leqslant G$ olsun. Bu durumda $[H : H \cap K] \leqslant [G : K]$. Şayet $[G : K] < \infty$ ise*

$$[H : H \cap K] = [G : K] \Leftrightarrow G = HK$$

dır.

Önerme 2.4.10 *G bir grup, H ve K, G de sonlu indeksli altgruplar olsun. Bu durumda $[G : H \cap K] < \infty$ ve $[G : H \cap K] \leqslant [G : H][G : K]$. Üstelik $[G : H \cap K] = [G : H][G : K] \Leftrightarrow G = HK$ dır.*

Ödev 2.4.11 *G bir grup, $H \leqslant G$ ve $K \leqslant G$ olsun. Bu durumda*

$$HK \leqslant G \Leftrightarrow HK = KH$$

dır, gösteriniz.

2.5 Normallik ve Bölüm Altgrupları

Tanım 2.5.1 *G bir grup ve $N \leqslant G$ olsun. $\forall x \in G$ için $xNx^{-1} \subseteq N$ oluyorsa N, G de normaldir denir ve $N \lhd G$ ile gösterilir.*

Teorem 2.5.2 *G bir grup ve $N \leqslant G$ olsun. Bu durumda aşağıdakiler biribirine denktir.*

(i) $N \lhd G$;

(ii) $\forall x \in G$ *için* $xNx^{-1} = N$;

(iii) $\forall x \in G$ *için* $xN = Nx$;

(iv) $\forall x, y \in G$ *için* $(xN)(yN) = xyN$.

Bu teoremin bir sonucu olarak, Abel grupların her altgrubu normaldir.

Ödev 2.5.3 *G bir grup ve $N \leqslant G$ olsun. Şayet $[G : N] = 2$ oluyorsa $N \lhd G$ dir, gösteriniz.*

Ödev 2.5.4 *Bir G grubu için, $H \lhd G$ ve $K \lhd G$ ise $(H \cap K) \lhd G$ dir, gösteriniz.*

G bir grup, $N \leqslant G$ ve $M \leqslant G$ olsun öyleki $N \lhd M$ ve $M \lhd G$. Bu durumda $N \lhd G$ olması gerekmez. Fakat bunun tersi doğrudur; yani, $N \lhd G$ ise $\forall\, N \subset M$ yapan $M \leqslant G$ için $N \lhd M$ dir.

Teorem 2.5.5 *G bir grup, $K \leqslant G$ ve $N \lhd G$ olsun. Bu durumda*

(i) $N \cap K \lhd K$;

(ii) $N \lhd N \vee K$, *(Burada* $N \vee K =< N \cup K >$*)*;

(iii) $NK = N \vee K = KN$;

(iv) Şayet $K \lhd G$ *ve* $K \cap N =< e >$ *ise* $\forall k \in K$ *ve* $\forall n \in N$ *için* $kn = nk$;

dir.

Teorem 2.5.6 *G bir grup, $N \lhd G$ ve G/N, N nin G deki tüm (sol) yankümelerinin kümesi olsun. Bu durumda G/N kümesi $(aN)(bN) = abN$ işlemi altında $[G : N]$ mertebeli bir gruptur.*

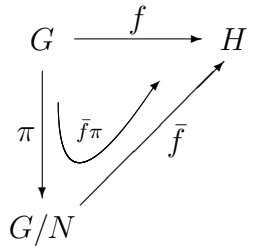
Yukarıdaki teoremde verilen G/N grubuna (G nin N ye) **bölüm grubu** denir. Toplama notasyonunda G/N deki işlem $(a+N)+(b+N) = (a+b)+N$ şeklindedir.
İHTAR $m > 1$ bir tam sayı ve $k \in \mathbb{Z}$ (mod m) denkliği altında $\bar{k}$ sınıfı $< m >$ nin k yı barındıran yankümesidir. $\bar{k}$ nın temsil elemanı $\bar{k}$ daki negatif olmayan en küçük tam sayı alındığında $i+ < m >$ lerin $\mathbb{Z} \,/\, < m >$ kümesi aslında $\mathbb{Z}_m$ nin kendisidir. $\mathbb{Z} \,/\, < m >= \mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{(m-1)}\}$ $\bar{k} = k+ < m >= \{k + mt : t \in \mathbb{Z}\}$.

Teorem 2.5.7 *$f : G \to H$ bir grup homomorfizmi olsun. Bu durumda $K =$ Çek$(f) \lhd G$. Tersine, şayet $N \lhd G$ ise $\pi(a) = aN$ ile tarifli $\pi : G \to G/N$ dönüşümü bir epimorfizm ve Çek$(\pi) = N$ dir.*

Yukarıdaki teoremde verilen π dönüşümüne özel olarak kanonik (doğal) epimorfizm ya da projeksiyon denir.

Teorem 2.5.8 *$f : G \to H$ grup homomorfizmi, $N \lhd G$ ve $N \subseteq$ Çek(f) olsun. Bu durumda $\forall a \in G$ için $\bar{f}(aN) = f(a)$ yapan yalnız bir $\bar{f} : G/N \to H$ homomorfizmi vardır;* $\mathrm{Im}(f) = \mathrm{Im}(\bar{f})$ *ve* Çek$(\bar{f}) =$ Çek$(f)/N$. *Üstelik, $\bar{f}$ nin bir izomorfizm olması için gerek ve yeter şart f in bir epimorfizm ve* Çek$(f) = N$ *olmasıdır.*

Bu teoremdeki ilk ifade



diagramını tutarlı kılan ($\bar{f}\pi = f$) yalnız bir $\bar{f}$ homomorfizmi vardır şeklinde ifade edilir.

Teorem 2.5.9 (Birinci İzomorfizma Teoremi) *$f : G \to H$ bir grup homomorfizmi olsun. Bu durumda f,*

$$G/\text{ Çek}(f) \cong \mathrm{Im}(f)$$

izomorfizması doğurur.

Sonuç 2.5.10 *$f : G \to H$ bir grup homomorfizmi, $N \lhd G$, $M \lhd H$ ve $f(N) < M$ olsun. Bu durumda f,*

$$\begin{aligned} \bar{f} : \ G/N &\to H/M \\ aN &\mapsto f(a)M \end{aligned}$$

homomorfizni doğurur. Üstelik $\bar{f}$ in bir izomorfizm olması için gerek ve yeter şart $\mathrm{Im}(f) \vee M = H$ ve $f^{-1}(M) \subset N$ olmasıdır. Özellikle, f, $f(N) = M$ ve $Çek(f) \subset N$ sağlayan bir epimorfizma ise $\bar{f}$ bir izomorfizmadır.

Sonuç 2.5.11 (İkinci İzomorfizma Teoremi) *G bir grup, $K, N \leqslant G$ ve $N \lhd G$ olsun. Bu durumda $K/(N \cap K) \cong (NK)/N$ dir.*

Sonuç 2.5.12 (Üçüncü İzomorfizma Teoremi) *G bir grup, $H, K \lhd G$ ve $K < H$ olsun. Bu durumda $H/K \lhd G/K$ ve $(G/K)/(H/K) \cong G/H$ dir.*

Teorem 2.5.13 *$f : G \to H$ bir grup epimorfizmi olsun. Bu durumda G nin $Çek(f)$ çekirdeğini barındıran bütün K altgruplarının $S_f(G)$ kümesinden H ın bütün altgruplarının $S(H)$ kümesine $K \mapsto f(K)$ ile tanımlı dönüşümü bire-birdir. Bu dönüşüm altında normal altgruplar normal altgruplara gider.*

Önerme 2.5.14 *$f : G \to H$ bir homomorfizim $N = Çek(f)$ ve $K < G$ olsun. Bu durumda $f^{-1}(f(K)) = KN$ ve böylece; $f^{-1}(f(K)) = K \Leftrightarrow N < K$ dır.*

Sonuç 2.5.15 *G bir grup ve $N \lhd G$ olsun. Bu durumda $N \subseteq K$ yapan $K < G$ ler için G/N nin her alt grubu K/N formundadır. Üstelik,*

$$K/N \lhd G/N \Leftrightarrow K \lhd G\,.$$

2.6 Simetri, Alterne ve Dihedral Gruplar

Tanım 2.6.1 *$i_1, \ldots, i_r$ ($r \leqslant n$) ler $I_n = \{1, 2, 3, \ldots, n\}$ kümesinin biribirinden farklı elemanları olsun. Bu durumda $(i_1\, i_2 \cdots i_r)$, $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_{r-1} \mapsto i_r$, $i_r \mapsto i_1$ götüren, I_n in diğer elemanlarını ise kendine götüren permütasyonu gösterir. Bu permütasyona r-uzunlukta bir devir ya da r-devir denir. Özel olarak, 2-devirlere transpozisyon adı verilir.*

Tanımdan anlaşılacağı gibi bir $\tau \in S_n$ permütasyonunun bir devir olarak ifadesi tek değildir. Üstelik, bir r-devirin ($r \leqslant n$) S_n in bir elemanı olduğu herhangi bir şekilde belirtilmelidir. $k \leqslant n$ için $(k) \in S_n$ 1-deviri herzaman birim permütasyonu gösterir. $\tau \in S_n$ ve $\tau(x) \neq x$ için τ deviri,
$\tau = (x\ \tau(x)\ \tau^2(x) \cdots \tau^d(x))$, $(d \geqslant 1)$ dir. Bu durumda $(i_1\, i_2 \cdots i_r)$ devirinin tersi $(i_r\, i_{r-1} \cdots i_2\, i_1) = (i_1\, i_r\, i_{r-1} \cdots i_2)$ dir (gösteriniz).

Örnek 2.6.2 *S_5 te $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}$ bir 4-devirdir. Bu, $\tau = (1432) = (4321) = (3214) = (2143)$ şeklinde de ifade ediliebilir. Şayet $\sigma = (125)$, S_5 te bir 3-devir ise $\sigma\tau = (125)(1432) = (1435) \neq (2543) = (1432)(125) = \tau\sigma$ yani $\sigma\tau \neq \tau\sigma$*

Tanım 2.6.3 *σ_1, σ_2, $\ldots$, σ_r ler S_n in elemanları olsun. Her $1 \leqslant i \leqslant r$ ve her $k \in I_n$ için $\sigma_i(k) \neq k$ olması $\sigma_j(k) = k$ $(\forall\, j \neq i)$ olmasını gerektiriyorsa σ_i lere ayrıktır denir $(i = 1, 2, 3, \ldots, r)$.*

Bu tanıma göre σ_i lerin ayrık olması için gerek ve yeter şart I_n in hiç bir elemanının σ_i lerin birden fazlası tarafından I_n in başka elemanına taşınmaz olmasıdır. Buna göre $\sigma, \tau \in S_n$ ayrık ise $\sigma\tau = \tau\sigma$ dır. Yani ayrık devirlerin çarpımı değişmelidir. Mesela $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1\,3\,6)(2\,8)(4\,7\,5)$ olup σ, üç ayrık devirin çarpımı olarak ifade edilebilir. Bu devirler sırasıyla τ_1, τ_2, τ_3 olsun. $\sigma = \tau_1\tau_2\tau_3 = \tau_1\tau_3\tau_2 = \tau_2\tau_1\tau_3 = \tau_2\tau_3\tau_1 = \tau_3\tau_2\tau_1 = \tau_3\tau_1\tau_2$ altı farklı sıralama ile ifade edilebilir.

Tanım 2.6.4 *$\sigma \in S_n$ ve $x, y \in I_n$ için "$x \sim y \Leftrightarrow \exists\ m \in \mathbb{Z} : y = \sigma^m(x)$" bir denklik bağıntısıdır (gösteriniz). Bu bağıntı I_n kümesini B_i denklik sınıflarına ayırır ki her bir $B_i = \{u : x \sim u\} = \{\sigma^m(x) : m \in \mathbb{Z}\}$ kümesine bir* **yörünge** *denir.*

Teorem 2.6.5 *S_n de birimden farklı her permütasyon, uzunluğu en az iki olan ayrık devirlerin çarpımı olarak, sıralama hariç, tek türlü yazılır.*

Sonuç 2.6.6 *$\sigma \in S_n$ permütasyonunun mertebesi σ nın ayrık devirlerinin mertebelerinin en küçük ortak katıdır.*

Sonuç 2.6.7 *S_n deki her permütasyon, ayrık olmaları gerekmeyen transpozisyonların çarpımı olarak ifade edilebilir.*

Tanım 2.6.8 *Bir $\tau \in S_n$ permütasyonu, şayet çift sayıda transpozisyonun çarpımı olarak ifade edilebiliyorsa* çift*, tek sayıda transpozisyonun çarpımı olarak ifade edilebiliyorsa* tek *dir denir. $\tau \in S_n$ in* $\operatorname{sgn}(\tau)$ *işareti, τ çift ise 1, tek ise -1 olarak tanımlanır.*

Teorem 2.6.9 *S_n de bir permütasyon hem çift hem de tek olamaz ($n \geqslant 2$).*

Tanım 2.6.10 *S_n n-simetri grubundaki tüm çift permütasyonların oluşturduğu altkümeye* **n-alterna grup** *denir ve A_n ile gösterilir ($n \geqslant 2$).*

Önteorem 2.6.11 *$I_n = \{1, 2, 3, \ldots, n\}$ ve $r, s \in I_n$ farklı elemanlar olsun. Bu durumda $n \geqslant 3$ için A_n, $\{(r\, s\, k) | 1 \leqslant k \leqslant n, \quad k \neq r, s\}$ 3-devirleri tarafından üretilir.*

Teorem 2.6.12 *$n \geqslant 2$ için, $A_n \lhd S_n$, $[S_n : A_n] = 2$ ve $|A_n| = |S_n|/2 = n!/2$. Üstelik A_n, S_n de indeksi 2 olan tek altgruptur .*

Tanım 2.6.13 *Has normal altgrup barındırmayan bir gruba* **basit***tir denir.*

Teorem 2.6.14 *A_n alterne grubunun basit olması için gerek ve yeter şart $n \neq 4$ olmasıdır.*

Önteorem 2.6.15 *$N \lhd A_n$, $n \geqslant 3$ ve N bir 3-devir barındırsın. Bu durumda $N = A_n$ dir.*

S_n in $n \geqslant 3$ için önemli bir altgrubu da a ve b tarafından üretilen D_n dir;

$$a = (1\, 2\, 3 \ldots n), \quad b = \begin{pmatrix} 1 & 2 & 3 & \ldots & i & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & n+2-i & \ldots & 3 & 2 \end{pmatrix} = \prod_{2 \leqslant i < n+2-i} (i \;\; n+2-i)$$

D_n, n-inci dereceden Dihedral grup diye adlandırılır, düzgün n-gen in simetrilerinin oluşturduğu grup olarak bilinir.

Teorem 2.6.16 *Her $n \geqslant 3$ için D_n dihedral grubu $2n$ mertebelidir. Üstelik a, b gerenleri*

(i) $a^n = (1) = b^2$*;* $0 < k < n$ *için* $a^k \neq (1)$*;*

(ii) $ba = a^{-1}b$*;*

sağlar. Bununla beraber $a, b \in G$ tarafından gerilen ve (i),(ii) sağlayan herhangi bir G grubu D_n e izomorftur $(n \geqslant 3)$.

Teorem 2.6.17 (Cayley) *Her grup bir permütasyon grubuna izomorftur.*

Bölüm 3

Grup Yapıları

3.1 Sonlu Gerilmiş Abel Gruplar

Teorem 3.1.1 *G bir grup, $H_1, \ldots, H_n$ ler G nin birer altgrubu ve $H = H_1 H_2 \cdots H_n$ olsun. Bu durumda aşağıdaki ifadeler biribirine denktir;*

(i) $\begin{array}{rl} f : H_1 \times H_2 \times \cdots \times H_n & \longrightarrow H \\ (x_1, x_2, \ldots x_n) & \longmapsto x_1 x_2 \cdots x_n \end{array}$ *bir izomorfizmdir;*

(ii) $H_i \lhd H$ *ve* $\forall\, x \in H$ *için* $x = x_1 x_2 \cdots x_n$ *şeklinde tek türlü ifade edilir* $(x_i \in H_i)$*;*

(iii) $H_i \lhd H$ *ve şayet* $x_1 x_2 \cdots x_n = e$ *ise* $\forall\, i$ *için* $x_i = e$ *dir ;*

(iv) $H_i \lhd H$ *ve* $H_i \cap (H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{e\}$, $1 \leqslant i \leqslant n$.

Yukarıdaki teoremde verilen biribirine denk ifadelerden herhangi birinin sağlaması durmunda H a $H_1, \ldots, H_n$ lerin bir **iç direkt çarpımı** denir. Şayet verilen grup toplamsal ise G nin $H_1, \ldots, H_n$ alt gruplarının direkt çarpımına $H_1, \ldots, H_n$ altgruplarının direkt toplamı denir ve $H_1 \oplus H_2 \oplus \cdots \oplus H_n$ ile gösterilir. Her bir H_i ye de **direkt toplanan** denir $(1 \leqslant i \leqslant n)$.

Teorem 3.1.2 (Sonlu Gerilmiş Abel Grupların Temel Teoremi) *Her sonlu gerilmiş Abel grup sonlu sayıda devirli grubun bir direkt toplamına izomorftur. Bu toplamda, şayet varsa, mertebeleri sonlu $m_1, \ldots, m_t$ olan $(m_1 > 1)$ direkt toplananlar için $m_1 \mid m_2 \mid \cdots \mid m_{t-1} \mid m_t$ sağlar.*

Bundan sonra yukarıdaki teorem için SATT kısaltmasını kullanacağız. Şunu belirtelim ki bu teorem değişik kaynaklarda farklı şekillerde ifade edilmekle birlikte esasta aynıdırlar. Bir başka ifadeyle SATT;

Teorem 3.1.3 (SATT) *Sonlu gerilmiş her G Abel grubu, herbiri, mertebesi sonsuz ya da bir asal sayının kuvveti olan sonlu sayıda devirli grubun sonlu bir direkt toplamına izomorftur. Yani $\exists p_i, r_i \in \mathbb{Z}$, p_i asal $(1 \leqslant i \leqslant k)$;*

$$G \cong \mathbb{Z}_{{p_1}^{r_1}} \oplus \mathbb{Z}_{{p_2}^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{{p_k}^{r_k}} \oplus \mathbb{Z} \oplus \mathbb{Z} \cdots \oplus \mathbb{Z}\,.$$

Bu diziliş izomorfizim farkıyla tektir.

Bu teoremde verilen son ifadede $\mathbb{Z}$ direkt toplananlarının sayısına G nin Betti sayısı ya da rankı denir. Bu sayı G için bir *sabit*tir.

Örnek 3.1.4 *İzomorfizm farkıyla, mertebesi 360 olan tüm Abel grupları SATT'a göre ifade edelim.* $360 = 2^3 3^2 5$ *olduğu gözönünde tutulursa aranan gruplar*

(i) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

(ii) $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

(iii) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$

(iv) $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$

(v) $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

(vi) $\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$

lerden birine izomorf olacaktır.

Önteorem 3.1.5 *Bir m pozitif tamsayısı, $m = {p_1}^{n_1}{p_2}^{n_2}\cdots{p_t}^{n_t}$ sağlasın (burada $p_1, \ldots, p_t$ ler biribirinden farklı asallar ve $n_i > 0$). Bu durumda $\mathbb{Z}_m \cong \mathbb{Z}_{{p_1}^{n_1}} \oplus \mathbb{Z}_{{p_2}^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{{p_t}^{n_t}}$ dir.*

Sonuç 3.1.6 *G, n mertebeli bir sonlu Abel grup olsun. Bu durumda G, n yi bölen her pozitif m tamsayısı için, mertebesi m olan bir altgruba sahiptir.*

Not: Bu sonuç, Abel olmayan gruplar için sağlamayabilir.

Önteorem 3.1.7 *G bir Abel grup, $p, m \in \mathbb{Z}$ ve p asal olsun. Bu drumda;*

(i) $mG = \{mu : u \in G\} \leqslant G$;

(ii) $G[m] = \{u \in G : mu = 0\} \leqslant G$;

(iii) $G(p) = \{u \in G : |u| = p^n \ (\exists n \geqslant 0)\} \leqslant G$;

(iv) $G_t = \{u \in G : |u| < \infty\} \leqslant G$;

(v) $\mathbb{Z}_{p^n}[p] \cong \mathbb{Z}_p \ (n \geqslant 1)$ *ve* $p^m\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{n-m}} \ (m < n)$;

(vi) $G_i \ (i \in I)$ *ler Abel grup olsun. Şayet* $g : G \longrightarrow \sum_{i\in I} G_i$ *bir izomorfizm ise, g nin mG ve $G[m]$ kısıtlamaları, sırasıyla,* $mG \cong \sum_{i\in I} mG_i$ *ve* $G[m] \cong \sum_{i\in I} G_i[m]$ *izomorfizmlerini verir;*

(vii) H, Abel grup ve $f : G \longrightarrow H$ bir izomorfizm ise f in G_t ve $G(p)$ ye kısıtlanması, sırasıyla, $G_t \cong H_t$ *ve* $G(p) \cong H(p)$ *izomorfizmalarını verir.*

Bir G Abel grubu için bu önteoremde verilen G_t altgrubuna G nin *burulmalı (torsion) altgrubu* denir. Şayet $G = G_t$ ise G ye *burulmalı (torsion) grup* denir. $G_t = 0$ ise G ye *burulmasız grup* denir. G sonlu gerilmiş ise Teorem 3.1.2 de verilen ve G tarafından tektürlü belirlenen $m_1, \ldots, m_t$ sayılarına G nin **sabit bölenleri** denir. Yani bu sayılar G nin invariantları (sabitleri) dir. Teorem 3.1.3 de verilen ve G tarafından tektürlü belirlenen $p_i^{r_i}$ asal kuvetlerine de G nin **esas bölenleri** denir.

Sonuç 3.1.8 *Sonlu gerilmiş iki G ve H Abel gruplarının izomorf olması için gerek ve yeter şart G/G_t ve H/H_t bölüm gruplarının aynı ranka, G ve H ın aynı sabit bölenlere (sırasıyla, aynı esas bölenlere) sahip olmasıdır.*

3.2 Grup Etkileri

Tanım 3.2.1 *Bir G grubunun bir S kümesine etkisi*

$$\begin{array}{ccc} G \times S & \to & S \\ (g, x) & \mapsto & g \cdot x \end{array}$$

fonksiyonudur öyleki $\forall x \in S$ ve $g_1, g_2 \in G$ için

(i) $e \cdot x = x$ *; ve*

(ii) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$

sağlar. Bu durumda, G grubu S kümesine etkir denir.

Örnek 3.2.2 $(\sigma, x) \mapsto \sigma(x)$ *ile verilen $S_n \times I_n \to I_n$ fonksiyonu, S_n simetri grubunun $I_n = \{1, 2, 3, \ldots, n\}$ kümesine bir etkisidir (gösteriniz).*

Örnek 3.2.3 *G bir grup ve $H \leqslant G$ olsun. $H \times G \to G$,: $(h, x) \mapsto hx$ fonksiyonu bir grup etkisidir. Burada $h \in H$ elemanının G üzerindeki etkisine (sol) öteleme denir. Şayet $K \leqslant G$ başka bir altgrup ve S, K nın G deki bütün sol yankümelerin kümesi ise H, $H \times S \to S$,: $(h, xK) \mapsto hxK$ ötelemesiyle S ye etkir (gösteriniz).*

Örnek 3.2.4 *G bir grup ve $H \leqslant G$ olsun. $(h, x) \mapsto hxh^{-1}$, H ın G ye bir etkisidir. h ın bu etkisine eşlenik etki, hxh^{-1} elemanına da x in eşleniği denir. Şayet K, G nin herhangi bir altgrubu ve $h \in H$ ise, bu durumda hKh^{-1}, G nin K ya izomorf bir altgrubudur. Böylece H, $(h, K) \mapsto hKh^{-1}$ eşlenik etkisiyle G nin tüm altgruplarının S kümesine etkir. Burada hKh^{-1} altgrubuna K nın eşleniği denir.*

Teorem 3.2.5 *G, bir S kümesine etkiyen bir grup olsun. Bu durmumda:*

(i) S de "$x \sim y \Leftrightarrow g \cdot x = y$ " $(\exists g \in G)$ bir denklik bağıntısı;

(ii) Her bir $x \in S$ için $G_x = \{g \in G : g \cdot x = x\} \leqslant G$.

Bu teoremin (i) kısmında verilen denklik bağıntısının oluşturacağı $x \in S$ in $\bar{x} = \{y \in S : g \cdot x = y,\ g \in G\} = \{g \cdot x : g \in G\}$ denklik sınıflarına G nin S deki **yörünge**leri denir. $G_x \leqslant G$ altgrubuna da x in **izotropi grubu** (sabitleyen altgrubu, dengeleyeni) denir.

Örnek 3.2.6 *Bir G grubu eşlenik etkiyle kendine etkisin. Bu durumda $x \in G$ nin $\{gxg^{-1} : g \in G\}$ yörüngesine x in eşlenik sınıfı denir. Bir $H \leqslant G$ altgrubu eşlenik etkiyle G grubuna etkisin. Bu durumda $H_x = \{h \in H : hxh^{-1} = x\} = \{h \in H : hx = xh\}$ izotropi grubuna x in H ta merkezleyeni denir ve $C_H(x)$ ile gösterilir. $H = G$ için $C_G(x)$ e sadece x in merkezleyeni denir. H, G nin tüm altgruplarının S kümesine eşlenik etkiyle etkisin. Bu durumda $K \in S$ yi sabitleyen, H ın $\{h \in H : hKh^{-1} = K\}$ altgrubuna K nın H ta normalleyeni denir ve $N_H(K)$ ile gösterilir. $N_G(K)$ grubuna da, sadece, K nın normalleyeni denir. Açıkca, K nın her altgrubu $N_G(K)$ da normaldir. Üstelik, K nın G de normal olması için gerek ve yeter şart $N_G(K) = G$ olmasıdır.*

Teorem 3.2.7 *Bir G grubu bir S kümesine etkisin. Bu durumda $x \in S$ yörüngesinin kardinal sayısı $[G : G_x]$ indeksidir.*

Sonuç 3.2.8 *G bir sonlu grup ve $H \leqslant G$ olsun. Bu durumda;*

(i) $x \in G$ nin eşlenik sınıfındaki elemanların sayısı $[G : C_G(x)]$ dir ki bu sayı $|G|$ yi böler;

(ii) $\bar{x}_1, \ldots, \bar{x}_n$, $(x_i \in G)$ G nin farklı eşlenik sınıfları olsun. Bu durumda, $|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$;

(iii) G nin K ya eşlenik altgruplarının sayısı $[G : N_G(K)]$ dir ki bu sayı $|G|$ yi böler.

Bu sonuçta verilen $|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$ eşitliğine sonlu G grubunun **sınıf denklemi** denir.

Teorem 3.2.9 *Bir G grubunun bir S kümesine etkisi bir $G \to A(S)$ homomorfizmi doğurur (burada $A(S)$, S in tüm permütasyonlarının grubu).*

Sonuç 3.2.10 (Cayley) *G bir grup olsun. Bu durumda bir $G \to A(G)$ monomorfizmi vardır. Böylece, her grup bir permütasyon grubuna izomorftur. Özellikle, her sonlu grup S_n in bir altgrubuna izomorftur ($n = |G|$).*

Sonuç 3.2.11 *G bir grup olsun. Bu durumda:*

(i) Her $g \in G$ için, g ile eşlenik alma, G nin bir otomorfizmasını doğurur;

(ii) Çekirdeği $C(G) = \{g \in G : gx = xg\,,\ \forall\, x \in G\}$ olan bir $G \to \mathrm{Aut}(G)$ homomorfizmi vardır (burada $\mathrm{Aut}(G)$, G nin tüm otomorfizmalarının fonksiyon bileşgesi işlemi altında oluşturduğu grup).

Önerme 3.2.12 *G bir grup, $H \leqslant G$ ve G, H ın G deki tüm sol yankümelerinin S kümesine sol ötelemeyle etkisin. Bu durumda $G \to A(S)$ homomorfizminin çekirdeği H ta kapsanır.*

Sonuç 3.2.13 *G bir grup, $H \leqslant G$, H ın G deki indeksi n ve H, G nin aşikâr olmayan hiçbir normal altgrubunu kapsamasın. Bu durumda G, S_n in bir altgrubuna izomorftur.*

Sonuç 3.2.14 *G bir sonlu grup, $H \leqslant G$, H ın G deki indeksi p ve p, G nin mertebesini bölen en küçük asal olsun. Bu durumda $H \lhd G$ dir.*

Teorem 3.2.15 (Cauchy-Frobenius-Burnside) *Sonlu bir G grubu sonlu bir X kümesine etkisin. Bu durumda X in G etkisi altındaki yörüngelerinin sayısı k ise,*

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

dir. Burada $X_g = \{x \in X | g \cdot x = x\} \subseteq X$, g nin sabit kümesi.

3.3 Sylow Teoremleri

G, mertebesi n olan bir Abel grup olsun. m|n ler için mertebesi m olan bir $H \leqslant G$ altgrubunun varlığını biliyoruz (Sonuç 3.1.6). G keyfi bir grup ise hangi şartlar altında böyle bir H alt grubu vardır? Bu kısımda bu soruya cevap arayacağız.

Önteorem 3.3.1 *G bir grup, p bir asal sayı ve $|G| = p^n$ olsun ($n \in \mathbb{Z}$). G, sonlu bir S kümesine etkisin ve $S_0 = \{x \in S : g \cdot x = x,\ \forall g \in G\}$ olsun. Bu durumda $|S| \equiv |S_0| (\text{mod p})$ dir.*

Teorem 3.3.2 (Cauchy) *G, sonlu bir grup, p bir asal sayı ve $p \Big| |G|$ olsun. Bu durumda G nin, mertebesi p olan bir elemanı vardır.*

Tanım 3.3.3 *G, her elemanı, mertebesi sabit bir p asalının bir kuvveti ($\geqslant 0$) olan bir grup olsun. Bu durumda G ye bir* p-grup *denir. $H \leqslant G$ ise H, bir* p-altgrup *adını alır. $| < e > | = 1 = p^0$ olacağından, $< e >$ bir p-altgruptur.*

Sonuç 3.3.4 *Sonlu bir G grubunun bir p-grup olması için gerek ve yeter şart, bir $t \in \mathbb{Z}^+$ için, $|G| = p^t$ olmasıdır.*

Sonuç 3.3.5 *Aşikâr olmayan, sonlu bir G p-grubunun $C(G)$ merkezi, birden fazla eleman barındırır.*

Önteorem 3.3.6 *H, sonlu bir G grubunun bir p-altgrubu olsun. Bu durumda $[N_G(H) : H] \equiv [G : H] (\text{mod p})$ dir.*

Sonuç 3.3.7 *H, $p \Big| [G : H]$ olacak şekilde, sonlu bir G grubunun p-altgrubu olsun. Bu durumda $N_G(H) \neq H$ dir.*

Teorem 3.3.8 (1. Sylow Teoremi) *G bir grup, $n \geqslant 1$ ve $|G| = p^n m$, p bir asal ve $(p, m) = 1$ olsun. Bu durumda $1 \leqslant i \leqslant n$ olan her i için G, mertebesi p^i olan bir altgruba sahiptir. Üstelik, G nin, mertebesi p^i olan her altgrubu ($i < n$), mertebesi p^{i+1} olan bazı altgruplar içinde normaldir.*

Tanım 3.3.9 *G bir grup ve $P \leqslant G$ olsun. Şayet P, G de maksimal p-altgrup ise, yani, bir H p-altgrubu için $P \leqslant H < G$ olması $H = P$ gerektiriyorsa, P ye bir Sylow p-altgrubu denir (p, asal).*

Sonuç 3.3.10 *G bir grup, $n \geqslant 1$ ve $|G| = p^n m$, p bir asal ve $(p, m) = 1$ olsun. H, G nin bir p-altgrubu olarak verilsin. Bu drumda;*

(i) H ın, G nin bir Sylow p-altgup olması için gerek ve yeter şart $|H| = p^n$ olmasıdır;

(ii) Bir Sylow p-altgubun her eşleniği yine bir Sylow p-altgrubudur.

(iii) G, sadece bir P Sylow p-altgrubuna sahip olsun. Bu durumda $P \lhd G$ dir.

Teorem 3.3.11 (2. Sylow Teoremi) *G bir sonlu grup, H, G nin bir p-altgrubu ve P, G nin herhangi bir Sylow p-altgrubu olsun. Bu durumda $H < xPx^{-1}$ yapan bir $x \in G$ vardır. Özellikle, G nin herhangi iki Sylow p-altgrubu eşleniktir.*

Teorem 3.3.12 (3. Sylow Teoremi) *G bir sonlu grup ve p bir asal olsun. Bu durmda G nin Sylow p-altgruplarının sayısı, bazı $k \geqslant 0$ lar için, $kp + 1$ formunda olup G nin $|G|$ mertebesini böler.*

Teorem 3.3.13 *G, sonlu bir grup ve P, G nin bir Sylow p-altgrubu olsun. Bu durumda $N_G(N_G(P)) = N_G(P)$ dir.*

3.4 Sonlu Grupların Sınıflandırması

Bu alt bölümde, mertebesi, 15 ten küçük olan ve pq formunda yazılabilen grupları, izomorfizm farkıyla sınıflandıracağız (p ve q birer asal).

Önerme 3.4.1 *p ve q birer asal ve $p > q$ olsun. Şayet $q \nmid (p-1)$ ise bu durumda mertebesi pq olan her grup $\mathbb{Z}_{pq}$ devirli grubuna izomorftur. Şayet $q \mid (p-1)$ ise, bu durumda, mertebesi pq yapan (izomorfizm farkıyla) sadece iki farklı grup vardır; $\mathbb{Z}_{pq}$ ve abel olmayan K grubu. Burada K,*

$$K =< c, d : |c| = p,\ |d| = q,\ dc = c^s d >$$

ve $s \not\equiv 1(\text{mod p})$, $s^q \equiv 1(\text{mod p})$ dir.

Sonuç 3.4.2 *p, çift olmayan bir asal sayı ($p \neq 2$) olsun. Bu durumda, mertebesi $2p$ olan her grup ya $\mathbb{Z}_{2p}$ devirli grubuna ya da D_p Dihedral grubuna izomorftur.*

Önerme 3.4.3 *Mertebesi 8 olan (izomorfizm farkıyla) farklı yalnız iki abel olmayan grup vardır. Bunlar D_4 Dihedral grubu ile Q_8 Queternion grubudur.*

Önerme 3.4.4 *Mertebesi 12 olan (izomorfizm farkıyla) farklı yalnız üç abel olmayan grup vardır. Bunlar D_6 Dihedral grubu, A_4 Alterne grup ve $|a| = 6$, $b^2 = a^3$ ve $ba = a^{-1}b$ yapan a ve b nin gerdiği T gruptur.*

Aşağıda, mertebesi 16 dan küçük ve (izomorfizm farkıyla) farklı olan grupların bir tablosu verilmiştir, inceleyiniz.

Mertebe	*Farklı grup*	*Mertebe*	*Farklı grup*
1	$< e >$	*9*	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
2	$\mathbb{Z}_2$	*10*	$\mathbb{Z}_{10},\ D_5$
3	$\mathbb{Z}_3$	*11*	$\mathbb{Z}_{11}$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$	*12*	$\mathbb{Z}_2 \oplus \mathbb{Z}_6,\ \mathbb{Z}_{12},\ A_4,\ D_6,\ T$
5	$\mathbb{Z}_5$	*13*	$\mathbb{Z}_{13}$
6	$\mathbb{Z}_6,\ D_3$	*14*	$\mathbb{Z}_{14},\ D_7$
7	$\mathbb{Z}_7$	*15*	$\mathbb{Z}_{15}$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_2 \oplus \mathbb{Z}_4$ $\mathbb{Z}_8,\ Q_8,\ D_4$		

Bölüm 4

Halka kavramı

4.1 Halkalar

Tanım 4.1.1 *$R \neq \emptyset$ bir küme, $+, \cdot$ (sırasıyla, toplama ve çarpma) R de iyi tanımlı işlemler olsun. Bu durumda*

(i) $(R, +)$ *sistemi bir Abel grup;*

(ii) $(R, \cdot)$ *sistemi bir yarı grup;*

(iii) Çarpma işleminin toplama işlemi üzerine sağdan ve soldan dağılma özelliği mevcut, yani; $a, b, c \in R$ *için*
$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c)$

sağlanması halinde $(R, +, \cdot)$ *sistemi bir halkadır denir (ya da sadece,* R *bir halkadır deriz).*

Bu tanımda verilen $a \cdot b$ *çarpımını kısaca* ab *ile göstereceğiz.* $(R, +)$ *nin birimi* 0 *olup, bu eleman* halkanın sıfırı *olarakta adlandırılır. Şayet* $(R \backslash \{0\}, \cdot)$ *sistemi bir grup ise* R *ye bir* **bölümlü halka** *(division ring), üstelik* $(R, \cdot)$ *sistemi Abel ise* R *ye bir* **cisim** *denir.*
$(R, \cdot)$ *sistemi Abel ise* R *ye bir* **değişmeli halka**, $(R, \cdot)$ *sistemi birim elemanına sahip ise* R *ye bir* **birimli halka** *denir.*
O halde, değişmeli ve birimli bir bölümlü halka bir cisimdir. Buna göre $\mathbb{Z}$ *bir değişmeli birimli bir halka,* $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ *birer cisim örneğidir.*

Meselâ; $[0,1]$ *aralığından* $\mathbb{R}$ *ye sürekli fonksiyonlar kümesi, fonksiyonların toplamı ve çarpımı işlemleri altında bir halka oluşturur. Yine, boştan farklı bir* X *kümesinden* $\mathbb{R}$ *ye tüm fonksiyonların* $\mathbb{R}^*$ *kümesi de bir halka oluşturur.*

Halkanın Temel Özellikleri: *R bir halka, $a, b, c \in R$ olsun.*

(i) $a0 = 0 = 0a$;

(ii) $a(-b) = -(ab) = (-a)b$;

(iii) $a(b-c) = ab - ac$, $(a-b)c = ac - bc$

dir, gösteriniz.

Tanım 4.1.2 *R (değişmeli, birimli) bir halka, $x, y \in R$ olsun. Şayet $xy = 0$ olması $x = 0$ ya da $y = 0$ olmasını gerektiriyorsa R ye bir Tamlık Bölgesi (TB) denir.*

Meselâ; $\mathbb{Z}$ *tamsayılar halkası bir TB dir. Yine, her cisim ve her bölümlü halka bir TB dir.*

Tanım 4.1.3 *R bir halka ve $x \in R$ olsun. $yx = 0$ (ya da $xy = 0$) yapan bir $y \in R$ ($y \neq 0$) varsa x elemanına R nin bir sağ (ya da, sol) sıfır böleni denir.*

Hem sağ sıfır böleni hem de sol sıfır böleni olan bir elemana sedece bir sıfır böleni *denir.*

O halde, bir R halkasının bir TB olması için gerek ve yeter şart R nin 0 dan başka sıfır bölenin olmamasıdır.

Tanım 4.1.4 *$(R, +, \cdot)$ bir halka ve $S \subseteq R$ olsun ($S \neq \emptyset$). Bu durumda $(S, +, \cdot)$ da bir halka oluyorsa S ye R nin bir althalkası denir.*

Bu tanıma göre, R bir bölümlü halka ise S de bir bölümlü althalkadır. Her bir R halkası için, R nin kendisi ve (0) birer althalkadır. Bunlardan (0) althalkasına aşikâr althalka denir. Birimli bir R halkasının bir S althalkası birimli olmak zorunda olmadığı gibi, R ile aynı birime sahip olamak zorunda da değildir. Meselâ, $\mathbb{Z}_{10}$ halkasının $S = \{0, 2, 4, 6, 8\}$ althalkası $\mathbb{Z}_{10}$ dan farklı bir birime sahiptir.

Teorem 4.1.5 *R bir halka, $S \neq \emptyset$ ve $S \subseteq R$ olsun. S nin, R nin bir althalkası olması için gerek ve yeter şart $\forall a, b \in S$ için $a - b \in S$ ve $ab \in S$ olmasıdır.*

Tanım 4.1.6 *R bir halka olsun. $Z(R) = \{a \in R \mid xa = ax,\ \forall x \in R\}$ kümesine R nin merkezi denir.*

Teorem 4.1.7 *Bir R halkasının $Z(R)$ merkezi bir althalkadır.*

Tanım 4.1.8 *R bir halka ve $S \subseteq R$ olsun. R nin S yi barndıran en küçük alt halkasına S nin gerdiği althalka denir.*

Tanım 4.1.9 *R bir halka olsun. Her $a \in R$ için $na = 0$ yapan pozitif n tam sayılarının en küçüğüne R nin karekteristiği denir,* $\mathrm{kar}(R)$ *ile gösterilir. Şayet böyle bir n sayısı yoksa R nin karekteristiği sıfır olarak tanımlanır.*

Teorem 4.1.10 *F bir cisim olsun. F in* $\mathrm{kar}(F)$ *karekteristiği ya bir p asalı ya da sıfırdır.*

Tanım 4.1.11 *R bir halka, $a \in R$ ve $\exists n \in \mathbb{Z}^+$ için $a^n = 0$ olsun. Bu durumda $a \in R$ ye nilpotent eleman denir.*

Tanım 4.1.12 *R bir halka ve $a \in R$ olsun. Şayet $a^2 = a$ sağlıyorsa $a \in R$ ye idempotent eleman denir.*

*(*Birimli bir halka için 0 ve 1 birer idempotentdir.*)*

Tanım 4.1.13 *R bir halka ve F bir cisim olsun.* $\begin{array}{ccc} F \times R & \longrightarrow & R \\ (\alpha, x) & \longmapsto & \alpha x \end{array}$ *dönüşümü aşağıdaki şartları sağladığı takdirde R ye F üzerinde bir cebirdir denir; α, $\beta \in F$, x,$y \in R$ için,*

(i) $(\alpha + \beta)x = \alpha x + \beta x$;

(ii) $\alpha(x + y) = \alpha x + \alpha y$;

(iii) $(\alpha\beta)x = \alpha(\beta x)$;

(iv) $1x = x$;

(v) $\alpha(xy) = (\alpha x)y = x(\alpha y)$.

(Burada αx çarpımına α ve x in skaler çarpımı denir.)

Tanım 4.1.14 *R, birimli bir halka ve $a \in R$ olsun. Şayet $au = ua = 1_R$ yapan bir $u \in R$ varsa $a \in R$ ye bir birimsel (ünit eleman) denir. Bu durumda u, a nın çarpımsal tersidir ($u = a^{-1}$).*

4.2 İdealler ve Homomorfizmalar

Gruplar için normal altgrup ne ise, halkalar için idealler aynıdır, aynı rolü üstlenir.

Tanım 4.2.1 *R bir halka, $S \neq \emptyset$ ve $S \subseteq R$ olsun. Aşağıdaki şartların sağlaması halinde S ye R nin bir* ideal*i denir;*

(i) $a, b \in S$ ise $a - b \in S$;

(ii) $a \in S$ ve $r \in R$ ise $ar \in S$ ve $ra \in S$.

Tanım 4.2.2 *R bir halka, $S \neq \emptyset$ ve $S \subseteq R$ olsun. S ye R nin bir* sağ ideal*i (ya da,* sol ideal*i) denir şayet*

(i) $a, b \in S$ ise $a - b \in S$;

(ii) $a \in S$ ve $r \in R$ ise $ar \in S$ (ya da $ra \in S$).

Hem sağ hem de sol ideal şartlarını taşıyan bir I idealine ikiyanlı ideal *yada* çift yanlı ideal *denir. Şayet halka değişmeli ise her ideali ikiyanlıdır. Bir R halkasının bir I ideali, açıkça bir althalkadır. Her althalkanın bir ideal olması gerekmez. Öte yandan, (0) ve R, R nin aşikâr idealidir.*

Teorem 4.2.3 *R birimli bir halka, R_n de, girdileri R den alınan $n \times n$ tipli matrisler halkası olsun. I, R nin bir ideali olmak üzere, I_n ile, girdileri I dan alınan $n \times n$ tipli matrisler kümesini gösterelim. Bu durumda R_n in her ideali I_n formundadır.*

Sonuç 4.2.4 *D bir bölümlü halka olsun. Bu durumda $R = D_n$ halkasının idealleri yalnızca (0) ve R dir.*

Teorem 4.2.5 *R bir halka ve $(I_i)_{i \in \Lambda}$, R de sağ(sol) ideallerin bir ailesi olsun. Bu durumda $\bigcap_{i \in \Lambda} I_i$ de R nin bir sağ(sol) idealidir.*

R bir halka $S \subseteq R$ olsun. $\mathcal{A} = \{\mathcal{A} | \, \mathcal{A}$ bir sağ ideal ve $\mathcal{S} \subseteq \mathcal{A}\}$. Bu durumda $\mathcal{A} \neq \emptyset$, $(R \in \mathcal{A})$. $I = \bigcap_{A \in \mathcal{A}} A$ olsun. Bu durumda I, R nin S yi barındıran en küçük sağ idealidir. Bunu $(S)_r$ ile gösterelim. $(S)_r$ ye S nin gerdiği sağ ideal denir. Şayet $S = \{a_1, \ldots, a_m\}$ ise, yani S sonlu bir küme ise bunu $(S)_r = (a_1, \ldots, a_m)$ ile gösteririz. Benzer şekilde $(S)_l$ de S nin gerdiği sol ideal olacaktır. $(S)_l = (S)_r$ olması durumunda bu ideal (S) ile gösterilir.

Tanım 4.2.6 *R bir halka, I, R nin bir sağ ideali olsun. Şayet* $I = (a_1, \ldots, a_m)_r$ *yapan* $a_i \in R \quad (1 \leqslant i \leqslant m)$ *varsa, I ya sonlu gerilmiştir denir.*

Tanım 4.2.7 *R bir halka ve I, R nin bir sağ ideali olsun. Bazı* $a \in R$ *ler için* $I = (a)_r$ *ise I ya bir sağ* temel ideal *(*esas ideal*) denir. (Benzer tanım sol idealler için de geçerlidir.)*

Tanım 4.2.8 *Her ideali bir sağ(sol) temel ideal olan bir R halkasına bir sağ(sol) temel (esas) ideal halkası (Tİ H) denir. Üstelik R, değişmeli ve birimli bir TB ise, bu durumda R ye bir Temel İdeal Bölgesi (Tİ B) denir.*

Meselâ; F bir cisim olmak üzere, $F[x]$ *ve* $\mathbb{Z}$ *halkası birer Tİ B dir.*

R bir halka ve I, R nin bir ideali olsun. R üzerinde, $a, b \in R$ *için* " $a \equiv b \pmod{I} \Longleftrightarrow a - b \in I$ " *bir denklik bağıntısı oluşturur.* $a \in R$ *için* $\bar{a}$*, a nın denklik sınıfını göstermek üzere,* $\bar{a} + \bar{b} = \overline{a+b}$ *ve* $\bar{a}\bar{b} = \overline{ab}$*, toplama ve çarpma işlemleri altında, denklik sınflarının* R/I *kümesi bir halka oluştur.*

Tanım 4.2.9 *R bir halka ve I, R nin bir ideali olsun.* $(R/I, +, \cdot)$ *halkasına (R nin I modülüne)* bölüm halkası *denir.*

Tanım 4.2.10 *R ve S birer halka,* $f : R \longrightarrow S$ *bir dönüşüm olsun.* $a, b \in R$ *için*

(i) $f(a + b) = f(a) + f(b)$*;*

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

oluyorsa f ye bir halka homomorfizmi denir.

Teorem 4.2.11 *Bir* $f : R \longrightarrow S$ *halka homomorfizmi olsun. Bu durumda;*

(i) $0 \in R$ için, $f(0) = 0 \in S$*;*

(ii) $a \in R$ için, $f(-a) = -f(a)$*;*

(iii) $\operatorname{Im} f = f(R) = \{f(a) : a \in R\}$ homomorfik görüntüsü S nin bir althalkasıdır*;*

(iv) $f^{-1}(0) = \text{Çek}\, f = \{a \in R : f(a) = 0\}$, f in çekirdeği, R nin bir idealidir*;*

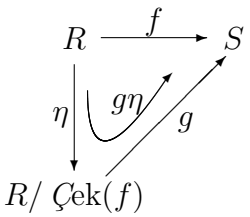
(v) $1_R \in R$ ise, $f(1_R) = 1_{f(R)}$, $f(R)$ nın birimidir*;*

(vi) R değişmeli ise $f(R)$ de değişmelidir.

Teorem 4.2.12 *$f : R \longrightarrow S$ halka homomorfizmi olsun. Bu durumda; " f birebir $\Longleftrightarrow$ Çek$(f) = \{0\}$ " dır.*

Teorem 4.2.13 (Homomorfizmin Esas Teoremi) *$f : R \longrightarrow S$ bir halka homomorfizmi ve $N =$ Çek(f) olsun. Bu durumda $R/N \cong \mathrm{Im}(f)$ dir.*

Teorem 4.2.14 *$f : R \longrightarrow S$ bir halka homomorfizmi olsun. Bu durumda aşağıdaki diagramı tutarlı $(f = g\eta)$ yapacak şekilde bir $g : R/$ Çek$(f) \longrightarrow S$ injektif (bire-bir) homomorfizmi vardır.*



Teorem 4.2.15 (Tekabûl Teoremi) *$f : R \longrightarrow S$ bir örten halka homomorfizmi ve $N =$ Çek(f) olsun. Bu durmda R nin N yi barındıran ideallerinin kümesinden S nin idealleri kümesine tanımlı $F : A \mapsto f(A)$ örten dönüşümü bire-bir dönüşüm sağlar. Bu dönüşüm altküme olma açısından sıralamayı korur. Yani $A \subset B \Longleftrightarrow f(A) \subset f(B)$ dir.*

Teorem 4.2.16 *K, R halkasının bir (sağ ya da sol) ideal olsun. Bu durumda R/K halkasının her bir (sağ ya da sol) ideali, bazı $A \leqslant R$ ve $K \subseteq A$ (sağ ya da sol) idealleri için, A/K şeklindedir.*

Tanım 4.2.17 *R ve S birer halka olsun. Şayet her $x, y \in R$ için*

(i) $f(x + y) = f(x) + f(y)$*;*

(ii) $f(xy) = f(y)f(x)$

oluyorsa $f : R \longrightarrow S$ ye bir antihomomorfizm denir.

Tanım 4.2.18 *$(R,+,\cdot)$ bir halka olsun. Bu durumda $\forall x,y \in R$ için $xoy = y \cdot x$ sağlayan bir $(R,+,o)$ sistemine R nin tersi (oposit) denir ve R^{op} ile gösterilir.*

R^{op} bir halkadır, gösteriniz.

Tanım 4.2.19 *$A_1, A_2, \ldots, A_n$ bir R halkasının sağ idealler ailesi olsun. $1 \leqslant i \leqslant n$ yapan her i için A_i leri barındıran en küçük sağ ideal $A_1, A_2 \ldots, A_n$ ailesinin toplamı olarak tarif edilir. Yani A_i ailesi toplamı, her i için tüm A_i leri barındıran ideallerin arakesitidir. Bu toplam $\sum_{i=1}^{n} A_i$ ile gösterilir.*

Teorem 4.2.20 *$S := \sum_{i=1}^{n} A_i$, A_i sağ ideallerin toplamı olsun. Bu durumda $S = \{a_1 + a_2 + \ldots + a_n |\ a_i \in A_i,\ i = 1, 2, \ldots, n\}$.*

Tanım 4.2.21 *A, A_i sağ (sol) idealler ailesinin $\sum_{i=1}^{n} A_i$ toplamı olsun. Her bir $a \in A$, $a = \sum_{i=1}^{n} a_i$ formunda yalnız bir şekilde ifade edilebiliyorsa A ya A_i lerin bir direkt toplamı denir ve $A = \bigoplus_{i=1}^{n} A_i$ ile gösterilir.*

Teorem 4.2.22 *$A_1, \ldots, A_n$ ler bir R halkasının sağ(sol) idealleri olsun. Bu durumda aşağıdaki ifadeler biribirine denktir;*

(i) $A = \sum_{i=1}^{n} A_i$ *toplamı direkttir;*

(ii) $0 = \sum_{i=1}^{n} a_i$, $a_i \in A_i$ *ise* $\forall i = 1, 2, \ldots, n$ *için* $a_i = 0$ *dır;*

(iii) $$A_i \bigcap \sum_{\substack{j=1 \\ j \neq i}}^{n} A_j = (0), \quad i = 1, 2, \ldots, n.$$

Teorem 4.2.23 *$R_1, \ldots, R_n$ bir halka ailesi, $R = R_1 \times R_2 \times \ldots \times R_n$, bu halkaların direkt çarpımı olsun. $R_i^{\star} = \{(0, 0, \ldots, 0, a_i, 0, \ldots, 0) |\ a_i \in R_i\}$. Bu durumda $R = \bigoplus_{i=1}^{n} R_i^{\star}$. R, $R_i^{\star}$ ideallerinin bir direkt toplamı ve bir halka olarak $R_i^{\star} \cong R_i$ dir . Diğer yandan $R = \bigoplus_{i=1}^{n} A_i$, ideallerin bir direkt toplamı ise aynı zamanda, $R = A_1 \times A_2 \times \ldots \times A_n$, A_i ideallerinin direkt çarpımından oluşan halkadır.*

Tanım 4.2.24 *R bir halka, I, R nin bir sağ(sol) ideali olsun. Aşağıdaki şartların sağlaması durumunda I ya bir minimal sağ(sol) ideal denir ;*

(i) $I \neq (0)$ *;*

(ii) eğer J, R nin $J \neq (0)$ sağlayan bir sağ(sol) ideali ve $J \subseteq I$ ise $I = J$ dir

Tanım 4.2.25 *R bir halka, A, B iki ideal olsun. $A + B = R$ oluyorsa A ve B eşmaksimaldir denir.*

Tanım 4.2.26 *Bir R halkasının bir A idealine, aşağıdaki şartları sağlaması durumunda, maksimal ideal denir;*

(i) $A \neq R$;

(ii) $A \subseteq B$ sağlayan bir B ideali için $B = A$ ya da $B = R$ dir.

Teorem 4.2.27 *R bir halka $A \neq R$ bir ideal olsun. Bu durumda aşağıdaki ifadeler biribirine eşittir;*

(i) A, maksimal;

(ii) R/A bölüm halkası aşikar olmayan ideale sahip değildir;

(iii) $x \notin A$ sağlayan $x \in R$ için $A + (x) = R$ dir.

Tanım 4.2.28 *Kendisi ve (0) dan başka ideali olmayan bir R halkasına Basit Halka denir.*

Meselâ*, bir F cismi basit halkadır. Değişmeli birimli bir R basit halkası bir cisimdir. Değişmeli olmayan bir basit halkaya örnek ise F cismi üzerinde alınan $n \times n$ tipli matrislerin F_n halkasıdır $(n > 1)$.*

Teorem 4.2.29 *$R \neq 0$ birimli, değişmeli bir halka ve $M \leqslant R$ bir ideal olsun. Bu durmda M nin R de maksimal olması için gerek ve yeter şart R/M nin bir cisim olmasıdır.*

Tanım 4.2.30 *R bir halka, A ve B, R nin sağ(sol) idealleri olsun. Bu durumda $\{\sum_{\substack{i \in \Lambda \\ \Lambda \text{sonlu}}} a_i b_i |\ a_i \in A, b_i \in B\}$ kümesine A ve B nin çarpımı denir ve AB ile gösterilir.(*AB nin yine bir sağ(sol) ideal olacağına dikkat ediniz*)*

Teorem 4.2.31 *R bir halka, A, B ve C bu halkanın birer ideali olsun. Bu durumda*

(i) $(AB)C = A(BC)$;

(ii) $A(B+C) = AB + AC$ *ve* $(B+C)A = BA + CA$ *dır.*

Tanım 4.2.32 *A, B ve P, bir R halkasının idealleri olsun. Bu durumda "*$AB \subseteq P$ ise $A \subseteq P$ ya da $B \subseteq P$ *" sağlıyorsa P ye bir asal ideal denir.*

Teorem 4.2.33 *R birimli bir halka olsun. Bu durumda* $I \leqslant R$ *maksimal ise asaldır.*

Teorem 4.2.34 *R değişmeli bir halka olsun. Bu durumda, bir P ideali için,* $a, b \in R$ *olmak üzere*

$$\text{" } P \leqslant R \text{ asal ideal } \iff ab \in P \text{ ise } a \in P \text{ veya } b \in P \text{ "}$$

dir.

Teorem 4.2.35 *R, (değişmeli birimli) bir TIB olsun. Bu durumda* $P \neq R$, $P \neq (0)$ *için*

$$\text{" } P \text{ asal } \iff P \text{ maksimal "}$$

dır.

Tanım 4.2.36 *R bir halka,* $A \leqslant R$ *bir sağ(sol) ideal olsun. Bazı* $n \in \mathbb{Z}^+$ *için* $A^n = (0)$ *oluyorsa, A ya* nilpotent ideal *denir.*

Tanım 4.2.37 *Bir R halkasının, her elemanı nilpotent olan bir A sağ(sol) idealine* nil ideal *denir.*

Zorn Lemması: *Bir* $S \neq \emptyset$ *kümesi üzerinde "*$\leqslant$*" bir sıralama bağıntısı oluştursun. Bu durumda* $(S, \leqslant)$ *sistemine kısmı sıralıdır denir. Bir* $C \subseteq S$ *kümesi* $\forall a, b \in C$ *için* $a \leqslant b$ *veya* $b \leqslant a$ *oluyorsa C kümesine S de bir zincirdir denir. Her* $a \in C$ *için* $a \leqslant u$ *yapan* $u \in S$ *ye C nin bir üst sınırı denir. Bir* $m \in S$, $m \leqslant a$ *yapan her* $a \in S$ *için* $m = a$ *oluyorsa m ye* $(S, \leqslant)$ *sisteminin bir maksimal elemanı denir.*

Önteorem 4.2.38 (Zorn Lemması) *Bir* $(S, \leqslant)$ *kismi sıralı sisteminde her C zinciri S de bir üst sınıra sahip oluyorsa,*$(S, \leqslant)$ *sisteminin bir maksimal elemanı vardır.*

Teorem 4.2.39 $R \neq \emptyset$ *birmli bir halka ve* $I < R$ *bir ideal olsun. Bu durumda* $I \subseteq M$ *sağlayan bir M maksimal ideali vardır.*

4.3 Tek Türlü Çarpanlama Bölgesi ve Euclid (Öklid) Bölgesi

R, birimli değişmeli bir TB, $a, b \in R$ olsun. $a = bc$ yapan bir $c \in R$ varsa, b, a yı böler ya da a, b ye bölünür denir ve bu, $b \mid a$ ile ya da $a \equiv 0(\text{mod b})$ gösterilir. Bu durumda a ya b nin bir çarpanıdır da denir. Buna göre bir $u \in R$ nin birimsel olması için gerek ve yeter şart $u \in R$ nin 1 in bir böleni olmasıdır. Diğer yandan, $a = ub$ yapan bir $u \in R$ birimseli varsa $a, b \in R$ elemanlarına ortak elemanlar denir. Bu durumda $b = va$ $(v = u^{-1})$ olup, a ve b ortak elemanlar ise $a \mid b$ ve $b \mid a$ dir.
R, değişmeli bir TB olup, bunun aksine, $a \mid b$ ve $b \mid a$ ise a ve b ortak elemanlardır. Çünkü: $b = ax$ ve $a = by$ olsun. Bu durumda $b = byx$ sağlar. R, birimli bir TB olup $xy = 1$ sağlar. Dolayısıyla x ve y birimsel, yani a ve b ortak elemanlardır.

Tanım 4.3.1 *R birimli bir TB, $0 \neq a \in R$ olsun.*

(i) $a \in R$ birimsel değil;

(ii) $a = bc$ ise b ya da c, R nin birimselidir $(b, c \in R)$,

sağlıyorsa $a \in R$ ye indirgenemez eleman denir.

Tanım 4.3.2 *Birimli bir R TB nin bir $p \in R$ elemanına, aşağıdaki şartları sağlaması halinde, asaldır denir;*

(i) $p \neq 0$, ve p birimsel değil ;

(ii) $p \mid ab$ ise $p \mid a$ ya da $p \mid b$, $(a, b \in R)$.

Teorem 4.3.3 *R, birimli ve değişmeli bir TİB ve $p \in R$ olsun. Bu durumda, p indirgenemez ise asaldır.*

Tanım 4.3.4 *R, birimli değişmeli bir TB olsun. Aşağıdaki şartların sağlaması durumunda R ye bir Tek Türlü Çarpanlama Bölgesi (kısaca, TÇB) denir;*

(i) R nin birimsel olmayan her elemanı, sonlu sayıda, indirgenemez elemanların bir çarpımıdır;

(ii) R nin indirgenemez her elemanı asaldır.

Teorem 4.3.5 *R bir TÇB olsun. Bu durumda bir $a \in R$ nin indirgenemez elemanların bir çarpımı olarak ifadesi, sıralama ve birimsellerle çarpımı hariç, tek türlüdür*

Tanım 4.3.6 *R, birimli ve değişmeli bir TB olsun. Bu durumda, $a, b \in R$ için;*

(i) $d \mid a$ *ve* $d \mid b$ *;*

(ii) $c \in R$ *için* $c \mid a$ *ve* $c \mid b$ *ise* $c \mid d$*,*

sağlayan bir $d \in R$ ye a ve b nin en büyük ortak böleni denir ve $(a, b) = d$ ile gösterilir.

Teorem 4.3.7 *R bir TÇB ve $a, b \in R$ olsun. Bu durumda a ve b nin bir en büyük ortak böleni vardır. Bu bölen (birimsellerle farklı çarpımı hariç) tek türlü seçilir.*

Tanım 4.3.8 *R bir TÇB, $a, b \in R$ olsun. Şayet $(a, b) = 1$ oluyorsa a ve b ye aralarında asaldır denir.*

Teorem 4.3.9 *Her TİB bir TÇB dir (*Bu ifadenin tersi doğru olmak zorunda değildir*).*

Tanım 4.3.10 *E, değişmeli ve birimli bir TB olsun. $\phi : E \to \mathbb{Z}$ fonksiyonunun aşağıdaki şartları sağlaması durumunda E ye bir Öklid (Euclid) bölgesi (kısaca, ÖB) denir;*

(i) $a, b \in E^\star = E \setminus \{0\}$ *ve* $b \mid a \Rightarrow \phi(b) \leqslant \phi(a)$*;*

(ii) Her bir $a, b \quad (b \neq 0)$ *çifti için* $\exists\ q, r \in E : a = bq + r,\ \phi(r) < \phi(b)$*.*

Teorem 4.3.11 *Her Öklid bölgesi bir Temel İdeal Bölgesidir.*

Sonuç 4.3.12 *Her Öklid Bölgesi bir Tek Türlü Çarpanlama Bölgesidir*

4.4 TÇB de Polinom Halkaları

R bir halka olmak üzere, $R[x]$ ile, katsayıları R den alınan x - tek değişkenli $f(x)$ polinomlarının halkası gösterilir. $f(x) = \sum_{i=0}^{n} a_i x^i$ polinomu $(a_1, \ldots, a_n)$ dizisi olarak veya (a_i) olarak da ifade edilir. Burada, $a_n \neq 0$ olması durumunda f in $\mathrm{der}(f)$ derecesi n dir. Burada a_n'e lider katsayı denir. Şayet $a_n = 1$ ise $f(x)$'e monik denir. Yani bir monik, lider katsayısı 1 olan polinomdur. Sıfır polinomunun derecesi $-\infty$ olarak tanımlanır. Diğer yandan $a \mapsto (a, 0, 0, \ldots, 0)$ ile tanımlanan $R \to R[x]$ dönüşümü bir homomorfizma olup R de a ya $R[x]$ de $(a, 0, 0, \ldots, 0)$ yı karşılık getirir. Bu durumda R, $R[x]$ in bir alt halkasıdır. $S = R[x]$ için $S[y] = R[x, y]$ çift değişkenli polinom olup tipik bir elemanı $\sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} x^i y^j, \quad (a_{ij} \in R)$ formundadır.

Teorem 4.4.1 *F, değişmeli bir TB ve $R = F[x]$ polinom halkası olsun. $F[x]$ de $f(x)$ ve $g(x) \neq 0$ sırasıyla, dereceleri m ve n olan polinomlar, $k = \mathrm{maks}(m - n + 1, 0)$ ve a, $g(x)$ in lider katsayısı olsun. Bu durumda*

$$\exists\ !\ q(x),\ r(x) \in F[x] : a^k f(x) = q(x)g(x) + r(x)$$

öyleki $r(x) = 0 \quad$ veya $\quad \mathrm{der}(r(x)) < \mathrm{der}(g(x))$.

Tanım 4.4.2 *R bir TÇB olsun. Bu durumda, katsayılarının ebob'u birimsel olan $f(x) \in R[x]$ polinomuna ilkel (primitif) polinom denir.*

*Herhangi bir $f \neq 0, \quad f(x) \in R[x]$ polinomunu, $f_1(x) \in R[x]$ ilkel ve $c \in R$, $f(x)$ in katsayılarının ebob'u olmak üzere, $f = cf_1$ formunda yazabiliriz. Bu durumda $c \in R$ ye $f(x)$ in **kontent**'i denir ve $c(f)$ ile gösterilir.*

Önteorem 4.4.3 (Gauss) *R bir TÇB, $f(x), g(x) \in R[x]$ olsun. Bu durumda $c \in R$ için $c(fg) = c(f)c(g)$ dir. Özellikle, iki ilkel polinomun çarpımı yine ilkeldir.*

Teorem 4.4.4 *R bir TÇB olsun. Bu durumda $R[x]$ polinom halkası da bir TÇB dir.*

Sonuç 4.4.5 *R bir TÇB ise $R[x_1, \ldots, x_n]$ çok değişkenli polinomlar halkası da bir TÇB dir.*

Bölüm 5

Cisim Genişlemeleri

5.1 İndirgenemez Polinomlar

F bir cisim ve $F[x]$ polinomlar halkası olsun. Bu durumda $F[x]$ birimli bir TB ve $F \subseteq F[x]$ bir alt halkadır. Burada $f(x) \in F[x]$ polinomu,

(i) $\text{der}(f(x)) \geqslant 1$ *;*

(ii) $f(x) = g(x)h(x)$ *ise* $g(x) \in F$ *veya* $h(x) \in F$*,*

$(g(x), h(x) \in F[x])$ *sağlıyorsa* $f(x)$*'e* indirgenemez polinom *denir. İndirgenemez olmayan bir* $g(x)$ *polinomuna da* indirgenebilir polinom *denir.*
$f(x) \in F[x]$ polinomunun indirgenemezliği çoğu zaman F cismine bağlı olarak değişir. Meselâ, $f(x) = x^2 + 1$ polinomu $\mathbb{R}$ reel sayılar cismi üzerinde indirgenemez iken $\mathbb{C}$ kompleks sayılar cismi üzerinde indirgenebilir (gösteriniz).

$F[x]$ ***halkasının bazı özellikleri:*** *F bir cisim olmak üzere;*

(i) $F[x]$, bölme algoroitmasını sağlar. Yani $f(x), g(x) \in F[x], g(x) \neq 0$ için,

$$\exists\ !\ q(x),\ r(x) \in F[x] : f(x) = q(x)g(x) + r(x)$$

öyleki $r(x) = 0$ *veya* $\text{der}(r(x)) < \text{der}(g(x))$*;*

(ii) $F[x]$ bir TİB dir;

(iii) $F[x]$ bir TÇB dir;

(iv) $F[x]$ in birimsellerinin $(\mathcal{U}(F[x]))$ kümesi $F\backslash\{0\}$ dır;

(v) $p(x) \in F[x]$ *indirgenemez olsun. Bu durumda* $F[x]/(p(x))$ *bölüm halkası bir cisimdir. (Bu ifadenin tersi de doğrudur).*

Önerme 5.1.1 *F bir cisim,* $f(x) \in F[x]$ *ve* $\mathrm{der}(f(x)) > 1$ *olsun. Bu durmda bazı* $\alpha \in F$ *için* $f(\alpha) = 0$ *oluyorsa* $f(x)$*, F üzerinde indirgenebilirdir.*

Tanım 5.1.2 *E ve F birer cisim ve* $F \subseteq E$ *olsun.* $f(x) \in F[x]$ *alalım. Bir* $\alpha \in E$ *elemanına,* $f(\alpha) = 0$ *yapıyorsa,* $f(x)$ *in bir sıfırı ya da kökü denir. (Burada* $f(x) = a_0 + a_1x + \ldots + a_nx^n$ *ise* $f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$ *ve* $f(\alpha) \in E$ *dir.)*

Önerme 5.1.3 *F bir cisim,* $f(x) \in F[x]$, $\mathrm{der}(f(x)) = 2$ *veya* $\mathrm{der}(f(x)) = 3$ *olsun. Bu durumda* $f(x)$ *in indirgenebilir olması için gerek ve yeter şart* $f(x)$ *in F de bir kökünün olmasıdır.*

Tanım 5.1.4 *Bir R halkası üzerinde tanımlı bir* $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n$ *polinomuna,* $a_n = 1$ *ise, bir monik denir.*

Önerme 5.1.5 (Gauss) $f(x) \in \mathbb{Z}[x]$ *bir ilkel polinom olsun. Bu durumda* $f(x)$ *in* $\mathbb{Q}$ *üzerinde indirgenebilir olması için gerek ve yeter şart* $f(x)$ *in* $\mathbb{Z}$ *üzerinde indirgenebilir olmasıdır.*

Sonuç 5.1.6 $f(x) \in \mathbb{Z}[x]$ *polinomu* $\mathbb{Q}[x]$ *de indirgenebilir ise* $\mathbb{Z}[x]$ *de de indirgenebilirdir.*

Teorem 5.1.7 $f(x) = \sum_{i=0}^{n} a_ix^i \in \mathbb{Z}[x]$ *polinomu bir monik olsun. Şayet* $f(x)$ *in* $\mathbb{Q}$ *da bir a kökü var ise* $a \in \mathbb{Z}$ *ve* $a \mid a_0$ *dır.*

Teorem 5.1.8 (Eisenstein Kriteri) $f(x) = a_0+a_1x+a_2x^2+a_3x^3+\ldots+a_nx^n \in \mathbb{Z}[x]$ *ve* $n \geqslant 1$ *olsun.* $i = 0, 1, 2, \ldots, (n-1)$ *için* $p \mid a_i$, $p \nmid a_n$, *ve* $p^2 \nmid a_0$ *yapan bir* $p \in \mathbb{Z}$ *asal sayısı varsa* $f(x)$*,* $\mathbb{Q}$ *üzerinde indirgenemezdir.*

Tanım 5.1.9 *F bir cisim* $f(x)$, $g(x) \in F[x]$ *(sıfır olmayan) polinomlar olsun. Aşağıdaki şartları sağlayan bir*
$d(x) \in F[x]$ *monik polimonuna* $f(x)$ *ve* $g(x)$ *in* **en büyük ortak böleni** *denir:*

i. $d(x)|f(x)$ *ve* $d(x)|g(x)$*;*

ii. *Şayet* $c(x)|f(x)$ *ve* $c(x)|g(x)$ *ise* $c(x)|d(x)$.

5.2 Köklerin Katılması

Tanım 5.2.1 *E bir cisim, F, E nin bir altcismi olsun. Bu durmda E ye F cisminin bir genişlemesi denir, $F \leqslant E$ ile gösterilir.*

E, F cisminin bir genişlemesi ise E, F üzerinde bir vektör uzayı oluşturur. Bu uzayın boyutu $[E : F]$ ile gösterilir.

Tanım 5.2.2 *E, F cismi üzerinde bir cisim genişlemesi olsun. Bu durumda, F üzerinde bir vektör uzayı olarak E nin boyutu F üzerinde E nin (genişleme) derecesi olarak adlandırılır. $[E : F] = n < \infty$ ise E, F nin bir sonlu genişlemesi (veya kısaca E, F üzerinde sonlu), aksi halde E, F nin bir sonsuz genişlemesidir denir.*

Teorem 5.2.3 *$F \subseteq E \subseteq K$ cisimler olsun. $[K : E] < \infty$ ve $[E : F] < \infty$ ise;*

(i) $[K : F] < \infty$;

(ii) $[K : F] = [K : E][E : F]$

Tanım 5.2.4 *Bir F cisminden bir E cismine 1-1 bir f homomorfizmine F in E ye bir yerleşimi (embedding) denir.*

Önteorem 5.2.5 *E ve F birer cisim, $\sigma : F \to E$, F nin E içine bir yerleşimi olsun. Bu durumda bir K cismi vardır öyleki, F, K nın bir alt cismi ve σ, K dan E ye bir izomorfizmaya genişletilebilir (yükseltilebilir).*

Sonuç 5.2.6 *E ve F cisimler arasında bir $F \to E$ yerleşimi varsa E, F nin bir genişlemesidir.*

Teorem 5.2.7 *F bir cisim, $F[x]$ polinomlar halkası ve $p(x) \in F[x]$ indirgenemez bir polinom olsun. Bu durumda F nin $p(x)$ in bir kökünü barındıran E genişlemesi vardır.*

Sonuç 5.2.8 (Kronecker Teoremi) *F bir cisim, $f(x) \in F[x]$, $f(x) \notin F$ olsun. Bu durumda F nin $f(x)$ in bir kökünü barındıran bir E genişlemesi vardır.*

Teorem 5.2.9 *F bir cisim, $p(x) \in F[x]$ indirgenemez polinom, E, F nin bir genişlemesi ve $u \in E$, $p(x)$ in E de bir bir kökü olsun. Bu durumda*

(i) $F(u)$, *E nin F ve u tarafından gerilen alt cismi olmak üzere,*

$$F[u] = \{b_0 + b_1u + \ldots + b_mu^m \in E \mid b_0 + b_1x + \ldots + b_mx^m \in F[x]\};$$

(ii) $\mathrm{der}(p(x)) = n$ *ise* $(1, u, u^2, \ldots, u^{n-1})$, $F(u)$ *nun* F *üzerinde bir tabanıdır. Yani* $\alpha \in F(u)$ *için* $\exists\ !\ c_i \in F : c_0 + c_1u \ldots + c_{n-1}u^{n-1} = \alpha$, $(i = 0, 1, 2, \ldots, (n-1))$ *ve* $[F(u) : F] = n$.

5.3 Cebirsel Genişlemeler

Tanım 5.3.1 *F bir cisim, E, F nin bir genişlemesi ve $\alpha \in E$ olsun. Şayet $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$ olacak şekilde, hepsi birden sıfır olmayan $a_0, a_1, a_2, \ldots, a_n \in F$, $(n \geqslant 1)$ elemanları varsa $\alpha \in E$ elemanına F üzerinde cebirsel (ya da F-cebirsel) dir denir.*

Yani,"$\alpha \in E, \quad F - cebirsel \iff \exists\, p(x) \in F[x],\ p(x) \notin F : p(\alpha) = 0$"

Teorem 5.3.2 *F bir cisim,E, F nin bir genişlemesi ve $u \in E$, F-cebirsel olsun. $p(x) \in F[x]$, $p(u) = 0$ sağlayan en küçük dereceli polinom olsun. Bu durumda;*

(i) $p(x)$, F üzerinde indirgenemezdir;

(ii) $g(x) \in F[x]$ polinomu $g(u) = 0$ yapıyorsa, $p(x) \mid g(x)$ dir;

(iii) $p(u) = 0$ yapan en küçük dereceli yalnız bir $p(x) \in F[x]$ monik polinomu vardır.

Tanım 5.3.3 *F bir cisim ve $F[x]$ polinomlar halkası olsun. F in bir E cisim genişlemesi için, $u \in E$ elemanını kök kabul eden monik, indirgenemez bir $p(x) \in F[x]$ polinomuna u nun F üzerindeki minimal polinomu denir ve $min_F(u, x)$ ile gösterilir.*

Tanım 5.3.4 *F bir cisim, E, F nin bir genişlemesi olsun. Şayet her $u \in E$, F üzerinde cebirsel (F-cebirsel) ise E ye F nin bir cebirsel genişlemesi denir. Bir genişleme, cebirsel değilse* aşkın *(transandant) genişlemedir denir.*

Teorem 5.3.5 *E, F nin bir sonlu genişlemesi ($[E : F] < \infty$) olsun. Bu durumda E, F nın bir cebirsel genişlemesidir.*

Teorem 5.3.6 *F bir cisim, E, F nin bir genişlemesi ve $u \in E$, F-cebirsel olsun. Bu durumda $F(u)$, F nin bir cebirsel genişlemesidir.*

Tanım 5.3.7 *F bir cisim ve E, F nin bir genişlemesi olsun. Şayet E nin $u_1, u_2, \ldots, u_r$ sonlu tane elemanı için E nin F ve $\{u_1, u_2, \ldots, u_r\}$ kümesini barındıran en küçük alt cismi kendisi ise E ye sonlu gerilmiş (üretilmiş) denir ve $E = F(u_1, \ldots, u_r)$ yazılır.*

Teorem 5.3.8 *F bir cisim ve $E = F(u_1, \ldots, u_r)$, her bir $i = 1, 2, 3, \ldots, r$ için u_i, F-cebirsel olacak şekilde, F in sonlu gerilmiş bir genişlemesi olsun. Bu durumda E, F üzerinde sonlu ve dolayısıyla da F in bir cebirsel genişlemesidir.*

Teorem 5.3.9 *F bir cisim ve E, F nin bir genişlemesi olsun. K, E nin tüm F-cebirsel elemanlarının kümesi, yani, $K = \{a \in E : a,\ F$ üzerinde cebirsel$\}$ olsun. Bu durumda K, E nin bir altcismi ve F nin bir cebirsel genişlemesidir.*

Tanım 5.3.10 *F bir cisim, K ve L, F nin birer genişlemesi olsun. Bu durumda, her $a \in F$ için, $\sigma(a) = a$ ile tanımlı $0 \neq \sigma : K \to L$ homomorfizmine K dan L ye bir F-homomorfizmi veya K dan L ye F üzerinde bir yerleşme denir.*

Teorem 5.3.11 *F bir cisim olsun. E, F nin bir cebirsel genişlemesi ve $\sigma : E \to E$, E nin kendi içine bir F-yerleşimi olsun. Bu durumda σ, örten olup bir otomorfizmadır.*

5.4 Cebirsel Kapalı Cisimler

Tanım 5.4.1 *Kendisinden daha geniş cebirsel genişlemesi olmayan bir K cismine* Cebirsel Kapalı Cisim *denir. (Bu durumda K nın her cebirsel genişlemesi K ile çakışır.)*

Teorem 5.4.2 *Bir K cismi için aşağıdaki ifadeler biribirine denktir;*

(i) *K cebirsel kapalı;*

(ii) *$K[x]$ de indirgenemez her polinomun derecesi 1 dir;*

(iii) *$K[x]$ de sabit olmayan her $f(x)$ polinomu ($\mathrm{der}(f(x)) \geqslant 1$) $K[x]$ de lineer çarpanlarına ayrılır;*

(iv) *Pozitif dereceli her $f(x) \in K[x]$ polinomu K da en az bir köke sahiptir.*

Tanım 5.4.3 *E bir cisim, F, E nin bir altcismi olsun. Şayet E, F nin bir cebirsel genişlemesi ve E cebirsel kapalı ise E ye F nin bir cebirsel kapanışı denir ve $\overline{F}$ ile gösterilir.*

Önteorem 5.4.4 *F bir cisim, L cebirsel kapalı bir cisim ve $\sigma : F \to L$, F nin L ye yerleşimi olsun. $E = F(\alpha)$, F nin bir cebirsel genişlemesi ise σ, $\eta : E \to L$ yerleşimine genişletilebilir (yükseltilebilir) ve bu genişletmelerin sayısı α nın minimal polinomunun farklı köklerinin sayısı kadardır.*

Teorem 5.4.5 *F bir cisim, E, F in bir cebirsel genişlemesi ve $\sigma : F \to L$, F in cebirsel kapalı L cismine bir yerleşimi olsun. Bu durumda σ, $\eta : E \to L$ yerleşimine genişletilebilir (yükseltilebilir).*

Teorem 5.4.6 *F bir cisim, K ve K' ler F in cebirsel kapanışları olsun. Bu durumda $K \cong K'$ dir.*

Teorem 5.4.7 *F bir cisim olsun. Bu durumda F yi bir alt cisim olarak barındıran cebirsel kapalı K cismi vardır.*

Teorem 5.4.8 *F bir cisim olsun. Bu durumda F üzerinde cebirsel, cebirsel kapalı bir $\overline{F}$ genişlemesi vardır. Yani, herbir cisim bir cebirsel kapanışa sahiptir.*

Bölüm 6

Normal ve Ayrılabilir Genişlemeler

6.1 Açılım (Parçalanış) Cisimleri

Tanım 6.1.1 *F bir cisim, $f(x) \in F[x]$ ve $\mathrm{der}(f(x)) \geqslant 1$ olsun. F in bir K genişlemesi için;*

(i) $f(x)$, $K[x]$ de lineer çarpanlarına ayrılır, yani $\alpha_i \in K$ için
$f(x) = c(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n), \quad i = 1, 2, \dots, n$

(ii) $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ yani K, F üzerinde $f(x)$ in K daki $\alpha_1, \alpha_2, \dots, \alpha_n$ kökleri tarafından üretilir

sağlanması durumunda K ya f(x) in F üzerinde bir açılım cismi denir.

Not: Bir $f(x) \in F[x]$ polinomunun daima bir açılım cismi vardır: $\overline{F}$, F nin bir cebirsel kapanışı ise $f(x)$ in $\overline{F}$ deki kökleri tarafından üretilen $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ cismi açılım cismidir.

Teorem 6.1.2 *K, $f(x) \in F[x]$ in F üzerinde bir açılım cismi ise, K, F in bir sonlu genişlemesi, dolayısıyla bir cebirsel genişlemesidir.*

Teorem 6.1.3 *K, $f(x) \in F[x]$ in F üzerinde bir açılım cismi olsun. E, $f(x)$ in F üzerinde başka bir açılım cismi ise bu durumda F de birim olan bir $\sigma : E \to K$ izomorfizmi vardır.*

Yukarıdaki teoremin bir sonucu olarak, verilen bir cisim üzerinde bir polinomun açılım cismi (varsa) izomorfizm farkıyla tektir. Ancak, her F cismi, F üzerindeki tüm polinomların köklerini barındıran bir $\overline{F}$ cebirsel kapanışına sahiptir. O halde $\overline{F}$ nin, verilen bir $f(x) \in F[x]$ polinomunun tüm köklerini barındıran tüm alt cisimlerinin arakesiti, $f(x)$ in F üzerindeki açılım cismidir.

6.2 Normal Genişlemeler

F bir cisim ve $(f_i(x))_{i\in\Lambda}$, F cismi üzerinde $\text{der}(f_i(x)) \geqslant 1$ yapan polinomlar ailesi olsun. Her bir $i \in \Lambda$ için, F üzerinde, $f_i(x)$ polinomlarının tüm kökleri tarafından üretilen F in E genişlemesine, her bir $f_i(x)$ polinomunun $E[x]$ de lineer çarpanlarına ayrışması durumunda $(f_i(x))_{i\in\Lambda}$ ailesinin bir açılım cismi denir. Şayet Λ sonlu ve polinomlar $f_1(x),\ f_2(x), \ldots, f_n(x)$ ise bu polinomların açılım cismi $f(x) = f_1(x)f_2(x)\ldots f_n(x)$ çarpım polinomunun açılılm cismidir. Bu durumda bir polinomun açılım cisminin (izmorfizm farkıyla) tekliğinin ispatı, verilen bir cisim üzerinde polinomlar ailesinin açılım cisminin (izomorfizm farkıyla) tekliğinin ispatına dönüşür.

Teorem 6.2.1 *E, bir F cisminin, $\overline{F}$ kapanışınca kapsanan bir cebirsel genişlemesi olsun. Bu durumda aşağıdaki ifadeler biribirine denktir:*

(i) E de bir köke sahip her $f(x) \in F[x]$ indirgenemez polinomu E de lineer çarpanlarına ayrışır;

(ii) E, $F[x]$ de bir polinomlar ailesinin açılım cismidir;

(iii) F nin her elemanını sabit bırakan bir $\sigma : E \to \overline{F}$ yerleşimi E yi E üzerine dönüştürür. Yani σ , E nin bir otomorfizmasına dönüşür.

Tanım 6.2.2 *F cisminin bir E genişlemesine, yukarıdaki 6.2.1 Teorem'in denk ifadelerinden herhangi birini sağlaması durumunda, Normal Genişleme denir.*

6.3 Katlı Kökler

F bir cisim ve $f(x) \in F[x]$ bir polinom olsun. $f(x) = \sum_{i=0}^{n} a_i x^i$ polinomunun $f'(x)$ türevi diye $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$ polinomuna deriz. Burada $f'(x) = 0$ olması $f(x) \in F$ (yani f bir sabit polinom) olmasını gerektirmez. Meselâ F, karekteristiği 5 olan bir cisim olmak üzere, F üzerinde $f(x) = x^5$ polinomu için $f'(x) = 5x^4 = 0$ dır. Bununla birlikte türevin geri kalan tüm özellikleri Analiz bilgileriyle aynıdır.. Öte yandan, türev alma bir lineer dönüşümdür. Yani;

Teorem 6.3.1 *F bir cismi ve $a, b \in F$ olmak üzere $F[x]$ de ;*

$$(af(x) + b\,g(x))' = af'(x) + bg'(x).$$

Teorem 6.3.2 *F bir cisim olmak üzere F üzerinde*

$$(f(x)\,g(x))' = f'(x)\,g(x) + f(x)\,g'(x)\ .$$

K bir $f(x) \in F[x]$ polinomunun açılım cismi ve α, $f(x)$ in bir kökü olsun. Bu durumda $K[x]$ de $(x-\alpha)|f(x)$. Şayet $K[x]$ de $(x-\alpha)$ nın $f(x)$ polinomunu bölen en büyük kuvveti s ise, yani $(x-\alpha)^s|f(x)$, $(x-\alpha)^{s+1} \not| f(x)$ oluyorsa s sayısına α nın katlığı denir. Eğer $s = 1$ ise α ya bir basit kök, $s > 1$ ise α ya bir katlı kök denir.

Teorem 6.3.3 *F bir cisim, $f(x) \in F[x]$, $\deg(f(x)) \geqslant 1$ ve α, $f(x)$ in bir kökü olsun. Bu durumda α nın $f(x)$ in bir katlı kökü olması için gerek ve yeter şart $f'(\alpha) = 0$ olmasıdır.*

Sonuç 6.3.4 *F bir cisim ve $f(x) \in F[x]$ indirgenemez olsun. Bu durumda $f(x)$ in bir katlı kökü olması için gerek ve yeter şart $f'(x) = 0$ olmasıdır.*

Sonuç 6.3.5 *F, karekteristiği sıfır olan bir cisim ve $f(x) \in F[x]$ indirgenemez bir polinom olsun. Bu durumda $f(x)$ in kökleri basittir. Buna rağmen: F, karekteristiği bir p asalı olan bir cisim olsun. $f(x) \in F[x]$ indirgenemez polinomunun bir katlı köke sahip olması için gerek ve yerter şart $f(x) = g(x^p)$ yapan bir $g(x) \in F[x]$ olmasıdır.*

Teorem 6.3.6 *F bir cisim, $f(x) \in F[x]$ indirgenemez olsun. Bu durumda $f(x)$ in tüm kökleri aynı katlığa sahiptir.*

Sonuç 6.3.7 *F bir cisim, $f(x) \in F[x]$ indirgenemez olsun. Bu durumda α_i ler $f(x)$ in, F üzerinde $f(x)$ in açılım cismindeki kökleri olmak üzere*

$$f(x) = a(x-\alpha_1)^k(x-\alpha_2)^k \dots (x-\alpha_r)^k = a\prod_{i=1}^{r}(x-\alpha_i)^k$$

dır.

6.4 Sonlu Cisimler

Tanım 6.4.1 *Özalt cismi olmayan bir F cismine asal cisim denir.*

Bu tanımdan da anlaşılacağı gibi her bir F cismi bir asal cisim barındırır; F in tüm altcisimlerinin arakesiti. Meselâ $\mathbb{Q}$ ve bir p asalı için $\mathbb{Z}/(p)$ asal cisimlerdir. İki değişik tip asal cisim vardır;

Teorem 6.4.2 *Bir F cisminin asal cismi ya $\mathbb{Q}$ cismine ya da, bir p asalı için, $\mathbb{Z}_p$ cismine izomorftur.*

Teorem 6.4.3 *F bir sonlu cisim olsun. Bu durumda;*

(i) $\mathrm{kar}(F) = p$, *(p asal) ve F nin $F_p \cong \mathbb{Z}/(p)$ yapan bir F_p alt cismi vardır.*

(ii) $\exists\, n \in \mathbb{N} : |F| = p^n$.

Not: Sonlu bir cisme Galois (galua) cismi de denir. Bu cisim p^n elemanlı ise, $GF(p^n)$ ile gösterilir.

Teorem 6.4.4 *Pozitif bir n tamsayısı ve p asalı için, p^n elemanlı bir F cismi, $x^{p^n} - x \in F_p[x]$ polinomunun açılım cismi olup, p^n elemanlı sonlu cisimler izomorftur (F_p, F nin asal cismi).*

Teorem 6.4.5 *Her bir p asal sayısı ve bir $n \geqslant 1$ pozitif tam sayısı için $(x^{p^n} - x) \in \mathbb{Z}_p[x]$ in $\mathbb{Z}_p$ üzerindeki açılım cismindeki köklerinin tümü farklı olup, bu kökler p^n elemanlı bir F cismi oluştururlar. Ayrıca F, $(x^{p^n} - x)$ in $\mathbb{Z}_p$ üzerindeki açılım cismidir.*

Sıradaki teorem, her sonlu cismin verilen bir sonlu dereceden bir genişlemesinin varlığını gösterir, yani;

Teorem 6.4.6 *F, p^n elemanlı bir sonlu cisim ve $m \in \mathbb{Z}^+$ olsun. Bu durumda F nin $[E : F] = m$ yapan bir E genişlemesi var ve F nin bu şekildeki tüm genişlemeleri biribirine izomorftur.*

Teorem 6.4.7 *Sonlu bir F cismi için $(F^*, \cdot)$ çarpımsal grubu devirlidir.*

Sonuç 6.4.8 *F bir sonlu cisim ve E, F nin bir sonlu genişlemesi $([E : F] < \infty)$ olsun. Bu durumda $\exists\, \alpha \in E : E = F(\alpha)$.*

Teorem 6.4.9 *F bir sonlu cisim olsun. Bu durumda F üzerinde, verilen her $n \in \mathbb{Z}^+$ dereceden bir indirgenemez polinom vardır.*

6.5 Ayrılabilir Genişlemeler

Tanım 6.5.1 *Tüm kökleri basit olan bir $f(x) \in F[x]$ indirgenemez polinomuna ayrılabilir polinom, tüm indirgenemez çarpanları ayrılabilir olan $f(x) \in F[x]$ polinomuna da ayrılabilirdir denir. Ayrılabilir olmayan bir polinomada ayrılamaz polinom denir.*

Tanım 6.5.2 *F bir cisim, E, F nin bir genişlemesi ve $\alpha \in E$ elemanı F-cebirsel olsun. Şayet α nın F üzerindeki $\min_F(\alpha, x)$ minimal polinomu ayrılabilir ise α, F üzerinde ayrılabilirdir denir. F nin bir E cebirsel genişlemesi için; E nin her elemanı F üzerinde ayrılabilir ise E ye F nin bir ayrılabilir genişlemesi denir.*

Not:

(i) 6.3.5 Sonuç'tan, sıfır karekteristikli bir cisim üzerindeki her polinom ayrılabilirdir. Dolayısıyla F, karekteristiği sıfır olan bir cisim ise F in her cebirsel genişlemesi ayrılabilirdir;

(ii) Sonlu bir cisim üzerindeki indirgenemez polinomların kökleri farklıdır. Buna göre; bir sonlu cismin her cebirsel genişlemesi ayrılabilirdir;

(iii) $K = F(x)$, $\text{kar}(F) = 3$ yapan bir F cismi üzerindeki rasyonel fonksiyonlar cismi ise $(y^3 - x) \in K[y]$ polinomu K üzerinde indirgenemezdir. Üstelik $(y^3 - x)$ polinomunun tüm kökleri eşittir, buna α diyelim; bu durumda $K(\alpha)$, K nın bir ayrılabilir genişlemesi değildir.

Tanım 6.5.3 *Tüm cebirsel genişlemeleri ayrılabilir olan bir F cismine mükemmel (perfect) cisim denir.*

Meselâ, sonlu cisimler ve sıfır karekteristikli cisimler mükemmel cisimlerdir. Buna rağmen, $\text{kar}(F) = p > 0$ olan sonsuz cisimler ayrılamaz genişlemelere sahip olup, böyle cisimler genelde mükemmel değillerdir.

Tanım 6.5.4 *F bir cisim ve E, F in bir genişlemesi olsun. Bu durumda, $\exists\, \alpha \in E : E = F(\alpha)$ oluyorsa, E ye F in bir basit genişlemesi denir.*

Teorem 6.5.5 *E, bir F cisminin bir sonlu ayrılabilir genişlemesi olsun. Bu durumda E, F in bir basit genişlemesidir.*

Teorem 6.5.6 *E bir F cisminin sonlu genişlemesi olsun. Bu durumda aşağıdaki ifadeler biribirine denktir:*

(i) Bazı $\alpha \in E$ ler için $E = F(\alpha)$;

(ii) F ile E arasında yalnızca sonlu tane aracisim vardır.

Kaynaklar

[1] P.B.BHATTACHARYA, S.K.JAIN and S.R.NAGPAUL, Basic Abstract Algebra *(Cambridge Uni. Press), 1986.*

[2] T.S.BLYTH and E.F. ROBERTSON, Algebra Through Practice *(Cambridge Uni. Prs.), Vol:3,5,6. 1984.*

[3] J.B.FRALEIGH, A First Course in Abstrac Algerbra *(Adisson-Wesley), 1989.*

[4] I.N.HERSTEIN, Topics in Algebra *(WILEY), 1975.*

[5] T.W.HUNGERFORD, Algebra *(Springer-Verlag 73), 1974.*

[6] S.LANG Algebra *(Addiso Wesley), 1993.*

[7] D.J.S.ROBINSON, A Course in Theory of Groups*(Springer,GTM-80),1996.*

[8] K.SPINDLER, Abstract Algebra with Applications *(M Dekker), 1994.*