CEBİR
DERS NOTLARI

Yrd. Doç. Dr. Yıldıray ÇELİK

Karadeniz Teknik Üniversitesi Fen Fakültesi

Matematik Bölümü

İçindekiler

Bölüm 1

Gruplar Teorisi

Tanım 1.1 G boş olmayan bir küme ve $\cdot$ da G üzerinde tanımlı bir ikili işlem olsun. Eğer aşağıdaki şartlar sağlanıyorsa $(G, \cdot)$ sistemine bir ***grup*** denir.

(i) Her $a, b \in G$ için $a \cdot b \in G$ dir. (Kapalılık özelliği)

(ii) Her $a, b, c \in G$ için $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ dir. (Birleşme özelliği)

(iii) Her $a \in G$ için $a \cdot e = e \cdot a = a$ olacak şekilde bir $e \in G$ vardır. (Birim eleman özelliği)

(iv) Her $a \in G$ için $a \cdot b = b \cdot a = e$ olacak şekilde bir $b \in G$ vardır. (Ters eleman özelliği.)

Burada (iii)'deki e elemanına grubun ***birim (etkisiz) elemanı*** denir. Ayrıca (iv)'deki b elemanına a nın ***tersi*** denir ve $b = a^{-1}$ ile gösterilir. Bu 4 şarta ilaveten eğer

(v) Her $a, b \in G$ için $a \cdot b = b \cdot a$ ise (Değişme özelliği)

bu gruba ***Abelyen***[1] ***(değişmeli) grup*** denir.

Not 1.2 Bu tanımda kullanılan notasyona ***çarpımsal notasyon*** ve $\cdot$ işlemine ***grup çarpması*** denir. Bu yüzden $a \cdot b$ ifadesi "a çarpı b" şeklinde okunur. Bir de, genelde abelyen gruplar için kullanılan, toplamsal notasyon vardır. Bu notasyonda $a \cdot b$ yerine $a + b$ ve a^{-1} yerine de $-a$ yazılır.

Örnek 1.3 $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ birer abelyen gruptur. Ayrıca $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$ birer abelyen gruptur. $(\mathbb{Z}, \cdot)$ bir grup değildir, çünkü $2^{-1} \notin \mathbb{Z}$.

Örnek 1.4 $A = \{1, -1, i, -i\}$ kümesi kompleks sayılardaki bilinen çarpma işlemi ile bir gruptur.

[1] Norveçli matematikçi Niels Henrik Abel (1802-1829).

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Tablodan görüldüğü gibi kapalılık özelliği vardır. Birleşme özelliği kompleks sayıların genelinde vardır. Birim eleman 1 dir. Ayrıca $1^{-1} = 1, (-1)^{-1} = -1, i^{-1} = -i$ ve $(-i)^{-1} = i$ olup her elemanın tersi vardır. Yani $(A, \cdot)$ bir gruptur.

Örnek 1.5 $GL_n(\mathbb{R})$ ile $n \times n$ boyutunda ve tersi olan gerçel haneli matrislerin kümesini gösterelim. Bu küme bilinen matris çarpımı ile bir gruptur. Bu gruba ***n-inci dereceden genel lineer grup*** denir. Benzer şekilde $GL_n(\mathbb{Q}), GL_n(\mathbb{C})$ tanımlanır.

Tanım 1.6 $M \neq \emptyset$ bir küme olsun. M den M ye birebir ve örten bir dönüşüme M nin bir ***permütasyonu*** denir. M nin bütün permütasyonlarının kümesi $P(M)$ ile gösterilir.

Örnek 1.7 $M \neq \emptyset$ olsun. $P(M)$ kümesi bilinen fonksiyon bileşkesi işlemi bir gruptur.
(i) $f, g \in P(M)$ olsun. Birebir ve örten iki dönüşümün bileşkesi birebir ve örten olup $f \circ g \in P(M)$.
(ii) $f, g, h \in P(M)$ ise $f \circ (g \circ h) = (f \circ g) \circ h$ dir.
(iii) $I : M \longrightarrow M$ birim dönüşümü $P(M)$ in birim elemanıdır: $f \circ I = I \circ f = f$.
(iv) $f \in P(M)$ ise f birebir ve örten olup f^{-1} vardır ve 1–1 ve örtendir. $f \circ f^{-1} = f^{-1} \circ f = I$.

Temel Özellikler

Teorem 1.8 $(G, \cdot)$ herhangibir grup olsun.
(i) G nin birim elemanı yegânedir.
(ii) Her elemanın tersi tektir.
(iii) Her $a \in G$ için $(a^{-1})^{-1} = a$ dır.
(iv) Her $a, b \in G$ için $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ dir.
İspat (i): e ve f, G nin iki birim elemanı olsun. e birim eleman olduğu için $e \cdot f = f$ dir. Ayrıca f birim eleman olduğundan $e \cdot f = e$ olup $e = f$ olduğu görülür.
İspat (ii): $a \in G$ olsun. b ve c de a nın tersleri olsun. Yani $a \cdot b = b \cdot a = e$ ve $a \cdot c = c \cdot a = e$ dir. O zaman

$$b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c$$

olup $b = c$ olduğu görülür.
İspat (iii): $x = a^{-1}, y = a$ diyelim. $x \cdot y = y \cdot x = e$ olup $x^{-1} = y$ olur. Yani $(a^{-1})^{-1} = a$ elde edilir.

İspat (iv):

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = e,$$
$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = b^{-1} \cdot e \cdot b = e$$

olup $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ elde edilir. □

Not 1.9 Teoremde **(iii)** ve **(iv)** de ifade edilen özellikler toplamsal notasyonda sırasıyla $-(-a) = a$ ve $-(a+b) = (-b) + (-a)$ şeklini alır.

Not 1.10 Bundan sonra grup işlemi söylenmemişse $\cdot$ kabul edilecek ve grup işlemi $\cdot$ ise kısalık açısından $a \cdot b$ yerine ab yazılacaktır.

Lemma 1.11 G bir grup $a, b \in G$ olsun. G de $ax = b$ ve $ya = b$ denklemini sağlayan sadece bir tane x ve y vardır. Ayrıca

$$ab = ac \Longrightarrow b = c \quad \text{ve} \quad ba = ca \Longrightarrow b = c$$

dir; yani soldan ve sağdan kısaltma kuralları vardır.

İspat:

$$ab = ac \Longrightarrow a^{-1}(ab) = a^{-1}(ac) \Longrightarrow (a^{-1}a)b = (a^{-1}a)c \Longrightarrow b = c,$$
$$ba = ca \Longrightarrow (ba)a^{-1} = (ca)a^{-1} \Longrightarrow b(aa^{-1}) = c(aa^{-1}) \Longrightarrow b = c$$

olup soldan ve sağdan kısaltma kuralı vardır. Şimdi, $ax = b$ denkleminin bir çözümü $x_1 = a^{-1}b$ dir çünkü :

$$a(a^{-1}b) = (aa^{-1})b = eb = b.$$

Bu denklemin başka bir çözümü x_2 olsun. O halde $ax_2 = b$ dir. O zaman $ax_1 = ax_2$, soldan kısaltma kuralı gereğince $x_1 = x_2$ elde edilir. Benzer şekilde $ya = b$ denkleminin çözümü de tektir. □

Not 1.12 Bu Lemma'nın bir sonucu olarak, grup tablosunda bir elemanın bir satırda veya bir sütunda sadece bir defa yer alacağını söyleyebiliriz. (Neden?)

Tanım 1.13 Bir G grubunun elemanlarının sayısına G nin ***mertebesi*** denir ve $|G|$ ile gösterilir.

Örnek 1.14 $M = \{a, b, c\}$ olsun. $P(M)$'in bileşke işlemi ile bir grup olduğunu biliyoruz. Bu gruba S_3 diyelim. $|S_3| = 6$ dır. S_3 ün elemanları:

$$f_1 : \begin{matrix} a \longrightarrow a \\ b \longrightarrow b \\ c \longrightarrow c \end{matrix}, \quad f_2 : \begin{matrix} a \longrightarrow a \\ b \longrightarrow c \\ c \longrightarrow b \end{matrix}, \quad f_3 : \begin{matrix} a \longrightarrow b \\ b \longrightarrow a \\ c \longrightarrow c \end{matrix}, \quad f_4 : \begin{matrix} a \longrightarrow b \\ b \longrightarrow c \\ c \longrightarrow a \end{matrix}, \quad f_5 : \begin{matrix} a \longrightarrow c \\ b \longrightarrow a \\ c \longrightarrow b \end{matrix}, \quad f_6 : \begin{matrix} a \longrightarrow c \\ b \longrightarrow b \\ c \longrightarrow a \end{matrix}.$$

Bu grupta f ile g nin çarpımını (yani bileşkesini) $f \cdot g$ şeklinde gösterelim. Dikkat edilirse $f \cdot g = g \circ f$ şeklinde yazılmalıdır (Neden?). Buna göre grubun çarpım tablosu aşağıdaki gibidir.

$\cdot$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

S_3 grubu değişmeli değildir, çünkü $f_2 f_3 = f_4$ fakat $f_3 f_2 = f_5$.

Tanım 1.15 G bir grup olsun. $a \in G$ olsun.
(i) $a^0 = e$ olarak tanımlanır.
(ii) $1 \leqslant n \in \mathbb{N}$ için $a^n = \underbrace{a \cdot a \dots a}_{n-\text{tane}}$
(iii) $1 \leqslant n \in \mathbb{N}$ için $a^{-n} = (a^{-1})^n$
olarak tanımlanır.

Not 1.16 Toplamsal notasyonda aynı tanımlar, sırasıyla, $0 \cdot a = 0$, $n \cdot a = a + a + \cdots + a$ ve $(-n) \cdot a = (-a) + (-a) + \cdots + (-a)$ şeklinde yazılabilir.

Teorem 1.17 G bir grup ve $a, b \in G$ ve $n, m \in \mathbb{N}$ olsun.
(i) $a^n a^m = a^{n+m}$ dir. ($n, m \in \mathbb{Z}$ için de doğrudur.)
(ii) $(a^n)^m = a^{nm}$ dir. ($n, m \in \mathbb{Z}$ için de doğrudur.)
(iii) $ab = ba$ ise $(ab)^n = a^n b^n$

İspat (i): $a^n a^m = (\underbrace{a \cdot a \cdot \cdots \cdot a}_{n-\text{tane}})(\underbrace{a \cdot a \cdot \cdots \cdot a}_{m-\text{tane}}) = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n+m-\text{tane}} = a^{n+m}$.

İspat (ii): $(a^n)^m = \underbrace{a^n a^n \dots a^n}_{m-\text{tane}} = \underbrace{a \cdot a \dots a}_{nm-\text{tane}} = a^{nm}$.

İspat (iii): $ab = ba$ ise $(ab)^n = \underbrace{(ab)(ab)\dots(ab)}_{n-\text{tane}} = (\underbrace{aa\dots a}_{n-\text{tane}})(\underbrace{bb\dots b}_{n-\text{tane}}) = (a^n)(b^n)$.

Not 1.18 n, m nin tamsayı olması durumundaki ispatlar yapılabilir. Mesela, $n = -2, m = 3$ ise:

$$(a^{-2})^3 = a^{-2}a^{-2}a^{-2} = a^{-1}a^{-1}a^{-1}a^{-1}a^{-1}a^{-1} = (a^{-1})^6 = (a^6)^{-1} = a^{-6}.$$

Tanım 1.19 G bir grup, $a \in G$ olsun. $a^n = e$ olacak şekilde bir en küçük pozitif n doğal sayısı varsa bu sayıya a nın ***derecesi*** denir ve $|a|$ ile gösterilir. Böyle bir n sayısı yoksa $|a| = \infty$ yazılır.

Örnek 1.20 S_3 grubunu ele alalım. Bu grubun birim elemanı f_1 dir. Her grupta birim elemanın derecesi 1 dir. $(f_2)^4 = f_1$ dir fakat f_2 nin derecesi 4 değildir, çünkü $(f_2)^2 = f_1$ olup $|f_2| = 2$ dir. $|f_1| = 1$ ve $|f_4| = 3$ dür.

Örnek 1.21 $(\mathbb{Z},+)$ grubunu ele alalım. 3 ün derecesi sonsuzdur, çünkü $n\cdot 3=0$ olacak şekilde $n\in\mathbb{N}^+$ yoktur. Bu grupta $|0|=1$ dir ve diğer elemanların derecesi sonsuzdur.

Tanım 1.22 G bir grup, $a\in G$ olsun. $\langle a\rangle=\{\,a^n : n\in\mathbb{Z}\,\}$ kümesine a ***tarafından üretilen (doğurulan) grup*** denir. (Toplamsal notasyonda $\langle a\rangle=\{\,na : n\in\mathbb{Z}\,\}$). a elemanına $\langle a\rangle$ grubunun ***üretici elemanı*** denir. Eğer $G=\langle a\rangle$ olacak şekilde bir $a\in G$ elemanı varsa G ye ***devirli grup*** denir.

Not 1.23 Bir grupta $|a|=\infty$ ise

$$\langle a\rangle=\left\{\,\ldots,a^{-3},a^{-2},a^{-1},e,a,a^2,a^3,\ldots\,\right\}.$$

Eğer $|a|=n$ sonlu ise a nın negatif bir kuvveti pozitif bir kuvvetine eşit olacağından

$$\langle a\rangle=\left\{\,e,a,a^2,\ldots,a^{n-1}\,\right\}.$$

yazılabilir.

Örnek 1.24 $A=\{\,1,-1,i,-i\,\}$ grubunu ele alalım.

$$\langle 1\rangle=\{\,1\,\},\quad \langle -1\rangle=\{\,1,-1\,\},\quad \langle i\rangle=\{\,1,-1,i,-i\,\},\quad \langle -i\rangle=\{\,1,-1,i,-i\,\}$$

olup A grubu devirlidir çünkü i ve $-i$ tarafından üretilmiştir. Yani $A=\langle i\rangle=\langle -i\rangle$.

Örnek 1.25 $(\mathbb{Z},+)$ grubunda $\langle 5\rangle=\{\,5n : n\in\mathbb{Z}\,\}=\{\,\ldots,-10,-5,0,5,10,\ldots\,\}=5\mathbb{Z}$ dir. $\mathbb{Z}$ devirlidir, çünkü $\langle -1\rangle=\langle 1\rangle=\mathbb{Z}$ dir.

Sonuç 1.26 Bir G sonlu grubunun devirli olması için gerek ve yeter şart $|G|=|a|$ olacak şekilde en az bir $a\in G$ elemanının olmasıdır.

Teorem 1.27 (Bölme Algoritması) a ve b iki tamsayı, $b\neq 0$ olsun. Bu iki sayı çifti için

$$a=bq+r,\qquad 0\leqslant r<|b|$$

şartını sağlayan sadece bir tane q,r sayı çifti vardır.

Teorem 1.28 G bir grup $a\in G$ ve $|a|=n$ olsun. $p,q\in\mathbb{Z}$ olsun.

(a) $n<\infty$ ise, $a^p=a^q$ olması için gerek ve yeter şart $p\equiv q \pmod n$ olmasıdır.

(b) $n=\infty$ ise, $a^p=a^q$ olması için gerek ve yeter şart $p=q$ olmasıdır.

İspat (a): $p-q \in \mathbb{Z}$ olup, Bölme Algoritması gereğince, $p-q$ ve n sayı çifti için $p-q = nk_1 + k_2$, $0 \leqslant k_2 < n$ olacak şekilde $k_1, k_2 \in \mathbb{Z}$ vardır.

$$\begin{aligned} a^p = a^q &\Longrightarrow a^{p-q} = e \\ &\Longrightarrow a^{nk_1+k_2} = e \\ &\Longrightarrow (a^n)^{k_1} a^{k_2} = e \\ &\Longrightarrow a^{k_2} = e \end{aligned}$$

olup $k_2 < n$ ve $|a| = n$ olduğundan bu durum sadece $k_2 = 0$ olmasıyla mümkündür. O halde $p - q = nk_1 \Longrightarrow p \equiv q \pmod{n}$. ($p \equiv q \pmod{n} \Longrightarrow a^p = a^q$ olduğunu göstermek kolaydır.)

İspat (b): $p > q$ olsun. $|a| = \infty$ olduğundan her $1 \leqslant k \in \mathbb{N}$ için $a^k \neq e$ dir. $a^p = a^q \Longrightarrow a^{p-q} = e$ dir. $p - q \in \mathbb{N}$ olup $p - q = 0$ olmalıdır. Yani $p = q$ dur. ($p = q \Longrightarrow a^p = a^q$ olduğu açıktır.) □

Not 1.29 $|a| = n < \infty$ olsun.

$$\text{Bir } k \in \mathbb{Z} \text{ için } a^k = e \iff n|k.$$

Teorem 1.30 $G = \langle a \rangle$ ve $|a| = \infty$ olsun. G grubu sadece a ve a^{-1} tarafından üretilir.

İspat: Bir $b \in G$ elemanı G nin üretici elemanı olsun.

$$G = \langle a \rangle = \{ \ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots \}$$

olup bir $m \in \mathbb{Z}$ için $b = a^m$ olmalıdır. Ayrıca, b bir üretici eleman olduğundan her $n \in \mathbb{Z}$ için $a^n = b^x$ olacak şekilde bir $x \in \mathbb{Z}$ vardır. Şimdi, $a^n = a^{mx} \Longrightarrow n = mx$ olup $n = mx$ denkleminin her $n \in \mathbb{Z}$ için çözümünün olması $m = \mp 1$ olmasıyla mümkündür. O halde $b = a$ veya $b = a^{-1}$ dir. □

Teorem 1.31 G sonlu bir grup ve $|G| = m$ olsun. G nin devirli bir grup olması için gerek ve yeter şart G nin abelyen olması ve $x^m = e$ denkleminin en fazla m tane çözümünün olmasıdır.

Çarpımsal Notasyon	Toplamsal Notasyon
$a \cdot b$ veya ab	$a + b$
$a^n = a \cdot a \cdot \cdots \cdot a$	$na = a + a + \cdots + a$
$a_1 a_2 \ldots a_n = \prod_{i=1}^{n} a_i$	$a_1 + a_2 + \cdots + a_n = \sum_{i=1}^{n} a_i$
a nın tersi a^{-1}	a nın tersi $-a$
$\langle a \rangle = \{ a^n : n \in \mathbb{Z} \}$	$\langle a \rangle = \{ na : n \in \mathbb{Z} \}$

Şekil 1.1: Çarpımsal ve Toplamsal Notasyonlar

ALIŞTIRMALAR

1. $\mathbb{Q}^+$ pozitif rasyonel sayılar kümesi üzerinde $x \star y = \dfrac{xy}{2}$ işlemi tanımlanıyor. $(\mathbb{Q}^+, \star)$ bir gruptur, gösterin.

2. $n \in \mathbb{N}$ olmak üzere $G = \{\, nk : k \in \mathbb{Z} \,\}$ kümesi bilinen toplama işlemine göre abelyen bir gruptur, gösterin.

3. $A = \{\, a, b, c \,\}, B = \{\, b, c \,\}, C = \{\, b \,\}$ olsun. $G = \{\, \emptyset, A, B, C \,\}$ alalım. $(G, \cap)$ ve $(G, \cup)$ sistemlerinin birer grup olup olmadığını inceleyin.

4. $M^{2\times 2} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$ kümesi matris toplamı ile bir gruptur. Gösterin.

5. $G = \mathbb{R} \setminus \{\, -1 \,\}$ kümesinde $a \star b = ab + a + b$ işlemi tanımlanıyor. $(G, \star)$ ın bir grup olduğunu gösterip $2 \star x \star 3 = 5$ denkleminin çözümünü bulunuz.

6. $G = \mathbb{Z} \times \mathbb{Z}$ kümesi üzerinde $(a, b) \circ (c, d) = (a + c, (-1)^c b + d)$ işlemi tanımlanıyor. $(G, \circ)$ bir grup olur mu? Abelyen grup olur mu?

7. $\mathbb{Z}_6 = \{\, 0, 1, 2, 3, 4, 5 \,\}$ kümesi modülo 6 toplama işlemine göre bir gruptur. $\mathbb{Z}_6$ devirli midir? Üretici elemanlarını bulunuz.

8. $(\mathbb{Q}, +)$ nın devirli olmadığını gösteriniz.

9. $(\mathbb{Z}, +)$ grubunda 6 elemanının ürettiği grubu bulunuz.

10. $(\mathbb{Q} \setminus \{\, 0 \,\}, \cdot)$ grubunda $\frac{1}{4}$ elemanının ürettiği grubu bulunuz.

11. G bir grup, $x \in G$ olsun. $x^n = e$ olacak şekilde bir $1 < n$ sayısı varsa $x^{-1} = x^m$ olacak şekilde bir $1 \leqslant m$ sayısı vardır. Gösterin.

12. G sonlu bir grup ise her $x \in G$ için $x^n = e$ olacak şekilde bir n pozitif sayısı vardır. Gösterin.

13. Bir G grubunda her $a, b \in G$ için $(ab)^2 = a^2 b^2$ ise G nin abelyen olduğunu gösterin.

14. G bir grup olsun. G de a, a^{-1} ve bab^{-1} elemanlarının derecelerinin aynı olduğunu gösteriniz.

15. G mertebesi çift olan bir grup olsun. G de $a^2 = e$ olacak şekilde e'den farklı bir a elemanının olduğunu gösteriniz.

16. Bir G grubunda her $x \in G$ için $x^2 = e$ ise bu grubun abelyen olduğunu gösterin.

17. G bir grup olsun. $a, b \in G$ için $x^{-1}ax = b$ olacak şekilde bir $x \in G$ varsa a ile b elemanlarına ***eşleniktir*** denir. "Eşlenik" olma bağıntısının bir denklik bağıntısı olduğunu gösteriniz.

Bölüm 2

Altgruplar, Kosetler ve Lagrange Teoremi

Tanım 2.1 G bir grup ve H de G nin boş olmayan bir alt kümesi olsun. Eğer H kümesi G de tanımlanan grup işlemi ile bir grup oluyorsa H ye G nin bir ***altgrubu*** denir ve $H \leqslant G$ yazılır.

Örnek 2.2 $A = \{1, -1, i, -i\}$ grubunda $B = \{1, -1\}$ olsun. B kümesi kapalıdır, birleşme özelliği vardır, $e = 1 \in B$ dir ve $1^{-1} = 1, (-1)^{-1} = -1$ olup her elemanın tersi yine B dedir. O halde $B \leqslant A$ yazılabilir.

Örnek 2.3 $(\mathbb{Q} \setminus \{0\}, \cdot)$ grubu $(\mathbb{R} \setminus \{0\}, \cdot)$ grubunun altgrubudur.

Örnek 2.4 $m \in \mathbb{Z}$ olsun. $(m\mathbb{Z}, +)$ grubu $(\mathbb{Z}, +)$ grubunun altgrubudur.

Örnek 2.5 $(\mathbb{Z}, +)$ grubunda tek tamsayılar kümesi bir altgrup değildir, çünkü $3 + 5 = 8$ çifttir.

Tanım 2.6 Bir G grubunda $\{e\}$ ve G kümeleri her zaman bir altgruptur. Bu altgruplara ***trivial (aşikar) altgruplar*** denir.

Not 2.7 Değişmeli bir grubun bütün altgrupları değişmelidir. Değişmeli olmayan bir grubun değişmeli olan bir altgrubu olabilir.

Teorem 2.8 G bir grup $\emptyset \neq U \subseteq G$ olsun.

(a) U nun altgrup olması için gerek ve yeter şart her $a, b \in U$ için $ab^{-1} \in U$ olmasıdır.

(b) U sonlu ise, U nun altgrup olması için gerek ve yeter şart her $a, b \in U$ için $ab \in U$ olmasıdır.

İspat (a): U bir altgrup olsun. $a, b \in U$ olsun. $b^{-1} \in U$ dur, çünkü U bir gruptur. U kapalı olduğundan $ab^{-1} \in U$ dur. Şimdi U nun boş olmayan bir alt küme olduğunu ve her $a, b \in U$ için $ab^{-1} \in U$ olduğunu kabul edelim. $b = a$ seçersek $aa^{-1} = e \in U$ elde edilir. Şimdi de $a = e$ seçersek her $b \in U$ için $b^{-1} \in U$

elde edilir. $a, b \in U$ olsun. $b^{-1} \in U$ olup $a(b^{-1})^{-1} = ab \in U$ elde edilir, yani U kapalıdır. Birleşme özelliği G de olduğundan U'da da vardır. Sonuç olarak U bir altgruptur.

İspat (b): U bir altgrup olsun. U kapalı olduğundan her $a, b \in U$ için $ab \in U$ olduğu kolayca görülür. Şimdi U nun boş olmayan kapalı bir küme olduğunu kabul edelim. G'de birleşme özelliği olduğundan U da birleşmelidir. $U = \{ a_1, a_2, \ldots, a_n \}$ alalım. $a_k \in U$ olsun. Şimdi

$$a_1 a_k, a_2 a_k, \ldots, a_n a_k$$

elemanlarını düşünelim. U kapalı olduğundan bu elemanların hepsi U nun elemanlarıdır. Bu elemanların hepsi birbirinden farklıdır. Çünkü eğer bir $i \neq j$ için $a_i a_k = a_j a_k$ olsaydı sağdan kısaltma kuralı gereğince $a_i = a_j$ olurdu. $i \neq j$ olup bu mümkün değildir. O halde $U = \{ a_1 a_k, a_2 a_k, \ldots, a_n a_k \}$ dir. $a_k \in U$ olup en az bir $1 \leqslant i \leqslant n$ için $a_k = a_i a_k$ olmalıdır. Yani $a_i = e$ olur ve $e \in U$ dur. Şimdi de, en az bir $1 \leqslant j \leqslant n$ için $a_i = a_j a_k$ olmalıdır. O zaman $(a_k)^{-1} = a_j$ bulunur. k nın seçimi keyfî olduğundan U daki her elemanın tersi vardır. Yani U bir altgruptur. □

Not 2.9 Bir G grubunda sonsuz elemanlı bir U alt kümesinin kapalı olması altgrup olması için yeterli değildir. Mesela $G = (\mathbb{R} \setminus \{ 0 \}, \cdot)$ grubunda $U = \{ 1, 2, 3, \ldots \}$ kümesi kapalıdır fakat bir altgrup değildir.

Örnek 2.10 $G = GL_2(\mathbb{R}), 2 \times 2$ tipinde tersi olan reel matrislerin grubu olsun.

$$H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : ab \neq 0 \right\}$$

olsun. $X = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in H, Y = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in H$ alalım. O zaman $ab \neq 0, cd \neq 0$ dır.

$$Y^{-1} = \begin{bmatrix} \frac{1}{c} & 0 \\ 0 & \frac{1}{d} \end{bmatrix} \text{ olup } XY^{-1} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} \frac{1}{c} & 0 \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} \frac{a}{c} & 0 \\ 0 & \frac{b}{d} \end{bmatrix}.$$

$XY^{-1} \in H$ dir çünkü $ab \neq 0, cd \neq 0$ olup $\frac{a}{c}\frac{b}{d} = \frac{ab}{cd} \neq 0$ dır. Teorem 2.8 gereğince $H \leqslant GL_2(\mathbb{R})$ dir.

Teorem 2.11 Bir G grubunun sonlu sayıdaki altgruplarının kesişimi de G nin bir altgrubudur.

İspat: $H_1, H_2, \ldots, H_n, G$ nin altgrupları olsun.

$$H = H_1 \cap H_2 \cap \cdots \cap H_n = \bigcap_{i=1}^{n} H_i$$

olsun.

$$\begin{aligned} a, b \in H &\Longrightarrow \text{ her } 1 \leqslant i \leqslant n \text{ için } a, b \in H_i \\ &\Longrightarrow \text{ her } 1 \leqslant i \leqslant n \text{ için } ab^{-1} \in H_i \quad (\text{Çünkü } H_i \leqslant G) \\ &\Longrightarrow ab^{-1} \in H_1 \cap H_2 \cap \cdots \cap H_n = H \end{aligned}$$

olup Teorem 2.8 gereğince H bir altgruptur. □

Not 2.12 Altgrupların birleşimi altgrup olmayabilir. Örneğin, $(\mathbb{Z}, +)$ grubunda $2\mathbb{Z}$ ve $3\mathbb{Z}$ altgruplarının birleşimi altgrup değildir, çünkü $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ olup $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ dir. (Yani kapalılık özelliği yoktur.)

Tanım 2.13 G bir grup, H ve K da G'nin boş olmayan iki alt kümesi olsun.

(i) $HK = \{ hk : h \in H, k \in K \}$ kümesine H ile K nın ***çarpımı*** denir. Toplamsal notasyonda ise, $H + K = \{ h + k : h \in H, k \in K \}$ kümesine H ile K nın ***toplamı*** denir. Eğer $H = \{ a \}$ bir elemanlı küme ise $\{ a \} K$ yerine kısaca aK, benzer şekilde $K \{ a \}$ yerine kısaca Ka yazılır.

(ii) $H^{-1} = \left\{ h^{-1} : h \in H \right\}$ kümesine H nin ***ters kümesi*** denir.

Lemma 2.14 G bir grup $A, B, C, D \subseteq G$ olsun. Bu kümeler üzerinde tanımlanan çarpma işlemi aşağıdaki özelliklere sahiptir:

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

(ii) $(AB)^{-1} = B^{-1}A^{-1}$

(iii) $\{ e \} \subseteq AA^{-1}$ dir. Eğer A bir elemanlı ise $AA^{-1} = \{ e \}$.

(iv) $A \subseteq B$ ve $C \subseteq D$ ise $AC \subseteq BD$.

(v) $A \subseteq B$ ise $A^{-1} \subseteq B^{-1}$.

İspat: Alıştırma olarak bırakıyoruz.

Sonuç 2.15 Bir G grubunun boş olmayan bir U alt kümesinin bir altgrup olması için gerek ve yeter şart $UU^{-1} \subseteq U$ olmasıdır. (Eğer U sonlu ise bu şart $UU \subseteq U$ şeklini alır.)

İspat: $UU^{-1} \subseteq U \iff \forall a, b \in U, ab^{-1} \in U$ olduğu açıktır. Bu da Teorem 2.8'in şartıdır. □

Tanım 2.16 G bir grup, $\emptyset \neq K \subseteq G$ olsun. G nin K yı içeren bütün altgruplarının ara kesitine ***K tarafından üretilen altgrup*** denir ve $\langle K \rangle$ ile gösterilir. Yani

$$\langle K \rangle = \bigcap \left\{ H : H \leqslant G, K \subseteq H \right\}.$$

Tanımdan anlaşıldığı gibi, $\langle K \rangle$ altgrubu K'yi içeren en küçük altgruptur. Eğer $\langle K \rangle = G$ ise bu durumda K'ya G'nin ***üretici kümesi*** veya ***doğuray kümesi*** denir.

Lemma 2.17 G bir grup, $\emptyset \neq K \subseteq G$ olsun. $\langle K \rangle$ altgrubu K daki elemanların kuvvetlerinin bütün muhtemel çarpımlarından oluşan kümedir; yani

$$\langle K \rangle = \{ {k_1}^{m_1} {k_2}^{m_2} \dots {k_n}^{m_n} : k_i \in K, m_i \in \mathbb{Z}, n \in \mathbb{N} \}.$$

İspat: $U = \{ k_1{}^{m_1} k_2{}^{m_2} \dots k_n{}^{m_n} : k_i \in K, m_i \in \mathbb{Z}, n \in \mathbb{N} \}$ olsun. K yı içeren her H altgrubu K daki elemanların çarpımlarını da içermelidir. $\langle K \rangle$ ise bu altgrupların kesişimi olduğundan $\langle K \rangle \subseteq U$ olur. K daki elemanların bir takım çarpımları K yı içeren her altgrubun elemanı olacağından $U \subseteq \langle K \rangle$ olur. Yani $U = \langle K \rangle$ dır. □

Not 2.18 Eğer $K = \{ a \}$ bir elemanlı ise $\langle K \rangle = \langle \{ a \} \rangle = \langle a \rangle = \{ a^n : n \in \mathbb{Z} \}$ olup bu tanım "bir eleman tarafından üretilen altgrup" tanımı ile aynı olur. $K = \{ k_1, k_2, \dots, k_n \}$ ise $\langle \{ k_1, k_2, \dots, k_n \} \rangle$ yerine kısaca $\langle k_1, k_2, \dots, k_n \rangle$ yazılabilir.

Örnek 2.19 S_3 grubunda $K = \{ f_3, f_4 \}$ tarafından üretilen altgrubu bulalım. $(f_3)^2 = f_1, (f_4)^2 = f_5$ dir. Ayrıca $f_3 f_4 = f_6$ ve $f_4 f_3 = f_2$ olup f_3 ve f_4 kullanılarak S_3 deki bütün elemanlar elde edilebilir. Yani $\langle f_3, f_4 \rangle = S_3$ olup $\{ f_3, f_4 \}$ kümesi S_3 için bir doğuray kümesidir.

Teorem 2.20 Bir devirli grubun her altgrubu devirlidir. $G = \langle a \rangle$ mertebesi n olan bir devirli grup ise, n yi bölen her m pozitif tam sayısı için mertebesi m olan sadece bir altgrup vardır ve bu altgrup $\langle a^{n/m} \rangle$ dir.

Örnek 2.21 $G = \langle a \rangle$ mertebesi 24 olan bir devirli grup olsun. Yani $G = \{ e, a, a^2, \dots, a^{23} \}$. 24 sayısının bölenleri 1,2,3,4,6,8,12,24 dür. Buna göre G nin n-elemanlı altgrubunu C_n ile gösterirsek bu altgruplar şunlardır:

$$
\begin{aligned}
C_1 &= \left\langle a^{24/1} \right\rangle = \langle e \rangle = \{ e \} \\
C_2 &= \left\langle a^{24/2} \right\rangle = \langle a^{12} \rangle = \{ e, a^{12} \} \\
C_3 &= \left\langle a^{24/3} \right\rangle = \langle a^{8} \rangle = \{ e, a^{8}, a^{16} \} \\
C_4 &= \left\langle a^{24/4} \right\rangle = \langle a^{6} \rangle = \{ e, a^{6}, a^{12}, a^{18} \} \\
C_6 &= \left\langle a^{24/6} \right\rangle = \langle a^{4} \rangle = \{ e, a^{4}, a^{8}, a^{12}, a^{16}, a^{20} \} \\
C_8 &= \left\langle a^{24/8} \right\rangle = \langle a^{3} \rangle = \{ e, a^{3}, a^{6}, a^{9}, a^{12}, a^{15}, a^{18}, a^{21} \} \\
C_{12} &= \left\langle a^{24/12} \right\rangle = \langle a^{2} \rangle = \{ e, a^{2}, a^{4}, a^{6}, a^{8}, a^{10}, a^{12}, a^{14}, a^{16}, a^{18}, a^{20}, a^{22} \} \\
C_{24} &= \left\langle a^{24/24} \right\rangle = \langle a \rangle = \{ e, a, a^{2}, \dots, a^{23} \} = G.
\end{aligned}
$$

Tanım 2.22 G bir grup, $H \leqslant G$ olsun. Bir $a \in G$ için

$$Ha = \{ ha : h \in H \} \qquad \text{ve} \qquad aH = \{ ah : h \in H \}$$

kümelerine sırasıyla H nin G deki ***sağ ve sol kosetleri*** denir. Koset kelimesi yerine ***yansınıf*** veya ***eşküme*** terimleri de kullanılmaktadır.

Örnek 2.23 S_3 grubunda $H = \langle f_2 \rangle = \{ f_1, f_2 \}$ alalım. H nin sağ kosetlerini bulalım.

$$Hf_1 = \{ f_1f_1, f_2f_1 \} = \{ f_1, f_2 \}$$
$$Hf_2 = \{ f_1f_2, f_2f_2 \} = \{ f_2, f_1 \}$$
$$Hf_3 = \{ f_1f_3, f_2f_3 \} = \{ f_3, f_4 \}$$
$$Hf_4 = \{ f_1f_4, f_2f_4 \} = \{ f_4, f_3 \}$$
$$Hf_5 = \{ f_1f_5, f_2f_5 \} = \{ f_5, f_6 \}$$
$$Hf_6 = \{ f_1f_6, f_2f_6 \} = \{ f_6, f_5 \}$$

Burada 3 tane farklı sağ koset vardır. Sağ kosetlerin herbirinde aynı sayıda eleman olup bu sağ kosetler ayrıktırlar. Bunun bir tesadüf olmadığını göstereceğiz. Aslında sağ kosetlerin bir denklik bağıntısının belirlediği denklik sınıfları olduğunu (dolayısıyla ayrık olduğunu) ve iki sağ kosette aynı sayıda eleman olması gerektiğini göstereceğiz.

Tanım 2.24 G bir grup, $H \leqslant G$ olsun. Eğer $a, b \in G$ için $ab^{-1} \in H$ ise ***a elemanı b'ye modülo H eşdeğerdir*** denir ve $a \equiv b \pmod{H}$ yazılır.

Teorem 2.25 Tanım 2.24'de verilen $\equiv \pmod{H}$ bağıntısı bir denklik bağıntısıdır.

İspat: Her $a \in G$ için $aa^{-1} = e \in H$ olup $a \equiv a \pmod{H}$ dir. Yani bağıntı yansıyandır.

$a \equiv b \pmod{H}$ yani $ab^{-1} \in H$ olsun. H bir altgrup olduğundan $(ab^{-1})^{-1} = ba^{-1} \in H$ dir. O halde $b \equiv a \pmod{H}$ olup bağıntı simetriktir.

$a \equiv b \pmod{H}$ ve $b \equiv c \pmod{H}$ olsun. Yani $ab^{-1} \in H$ ve $bc^{-1} \in H$ dir. O zaman $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$ olur. Buradan $a \equiv c \pmod{H}$ olup bağıntı geçişkendir. □

Teorem 2.26 G bir grup $H \leqslant G$ olsun. Her $a \in G$ için $Ha = \{ x \in G : a \equiv x \pmod{H} \}$ dir.

İspat: $A = \{ x \in G : a \equiv x \pmod{H} \}$ diyelim. $Ha = A$ olduğunu göstereceğiz. Önce $Ha \subseteq A$ olduğunu gösterelim. $h \in H$ olmak üzere $ha \in Ha$ alalım. $h^{-1} \in H$ olup,

$$h^{-1} = eh^{-1} = aa^{-1}h^{-1} = a(ha)^{-1} \in H$$

olup $a \equiv ha \pmod{H}$ olur. A'nın tanımından $ha \in A$ olur. Yani $Ha \subseteq A$ dır.

Şimdi $A \subseteq Ha$ olduğunu gösterelim.

$$\begin{aligned} x \in A &\Longrightarrow a \equiv x \pmod{H} \\ &\Longrightarrow ax^{-1} \in H \\ &\Longrightarrow H \text{ bir altgrup olduğundan } (ax^{-1})^{-1} = xa^{-1} \in H \\ &\Longrightarrow \exists\, h \in H, xa^{-1} = h \\ &\Longrightarrow x = ha \in Ha \end{aligned}$$

olup $A \subseteq Ha$ olduğu görülür. Sonuç olarak $A = Ha$ elde edilir. □

Sonuç 2.27 $Ha = H \iff a \in H$. Ayrıca $Ha = Hb \iff ab^{-1} \in H$.

İspat: $Ha = H \Longrightarrow \exists h_1, h_2 \in H, h_1 a = h_2 \Longrightarrow a = {h_1}^{-1} h_2 \in H$. Şimdi $a \in H$ kabul edelim. $ha \in Ha \Longrightarrow h, a \in H$ olup $ha \in H$ dir. $h \in H \Longrightarrow h = ha^{-1}a \in Ha$ dır, çünkü $ha^{-1} \in H$ dir. Sonuç olarak $Ha = H \iff a \in H$ elde edilir. Şimdi

$$Ha = Hb \iff Hab^{-1} = H \iff ab^{-1} \in H.$$

bulunur. □

Not 2.28 Ha sağ kosetindeki elemanların a'ya modülo H eşdeğer olan elemanlar olduğunu gösterdik. Eğer "$a \equiv b \pmod{H}$" olmanın tanımı $a^{-1}b \in H$ şeklinde verilseydi a'ya modülo H eşdeğer olan elemanların kümesi aH sol koseti olurdu. (Gösteriniz.)

Teorem 2.29 G bir grup, $H \leqslant G$ olsun. H nin iki sağ (sol) koseti arasında birebir bir ilişki vardır.

İspat: İspatı sağ koset için yapacağız. $a, b \in G$ ve Ha ve Hb de H'nin iki sağ koseti olsun. $f : Ha \longrightarrow Hb$ dönüşümü $f(ha) = hb$ şeklinde tanımlansın.

$$f(h_1 a) = f(h_2 a) \Longrightarrow h_1 b = h_2 b \Longrightarrow h_1 = h_2 \Longrightarrow h_1 a = h_2 a$$

olup f birebirdir. Şimdi, $hb \in Hb$ verilsin. $x = ha$ seçilirse $f(x) = f(ha) = hb$ olup f örtendir. □

Sonuç 2.30 İki sağ (sol) koset aynı sayıda elemana sahiptir. $H = He$ olup H ile sağ (sol) kosetlerin eleman sayıları aynıdır. Aynı zamanda iki sağ koset ya aynıdır ya da ayrıktır, yani $Ha = Hb$ veya $Ha \cap Hb = \emptyset$. Sağ kosetlerin birleşimi de G yi verir:

$$G = H \cup Ha_1 \cup Ha_2 \cup \cdots \cup Ha_n.$$

Tanım 2.31 G bir grup, $H \leqslant G$ olsun. H nin G deki farklı sağ kosetlerinin sayısına H nin G deki ***indeksi*** denir ve $|G : H|$ şeklinde gösterilir. Örneğin, $|S_3 : \langle f_2 \rangle| = 3$ dür.

Teorem 2.32 (Lagrange[1]) G sonlu bir grup ve $H \leqslant G$ olsun. O zaman H nin mertebesi G nin mertebesini böler; yani $|G| = |G : H|\,|H|$ dir.

İspat: H'nin G'deki indeksi $|G : H| = n$ olsun. Buna göre

$$H, H_{a_1}, H_{a_2}, \ldots, H_{a_{n-1}}$$

kümeleri H nin n tane farklı sağ koseti olsun. Bu kosetler G nin parçalanışını verirler. Ayrıca herbir kosetteki eleman sayısı $|H|$'ye eşittir. O halde

$$G = H \cup H_{a_1} \cup H_{a_2} \cup \cdots \cup H_{a_{n-1}} \Longrightarrow |G| = |H| + |H_{a_1}| + |H_{a_2}| + \cdots + |H_{a_{n-1}}| \Longrightarrow |G| = n \cdot |H|$$

olup $|G| = |G : H|\,|H|$ elde edilir. Buradan $|H| \Big| |G|$ yazılabilir. □

Sonuç 2.33 Eğer G asal mertebeli bir grup ise G nin $\{ e \}$ ve G den başka altgrubu yoktur.

Not 2.34 Eğer $H = \{ e \}$ ise her $a \in G$ için $Ha = \{ a \}$ olup $|G| = |G| = |G : H|\,|H| = |G : H|$ dir.

Örnek 2.35 $\mathbb{Z}_7$ grubunun yegâne altgrupları $\{ 0 \}$ ve $\mathbb{Z}_7$ dir, çünkü $\mathbb{Z}_7$ asal mertebeli bir gruptur.

Örnek 2.36 $(\mathbb{Z}, +)$ grubunda $U = \{ 3k : k \in \mathbb{Z} \}$ altgrubunu ele alalım. Bu altgrup için Lagrange teoremi uygulanamaz, çünkü $\mathbb{Z}$'nin mertebesi sonlu değildir.

Teorem 2.37 G sonlu bir grup ve $a \in G$ olsun. O zaman $|a| \Big| |G|$ dir. Ayrıca $a^{|G|} = e$ dir.

İspat: $H = \langle a \rangle$ alalım. a tarafından üretilen altgrubun mertebesi a'nın derecesine eşittir; yani $|\langle a \rangle| = |a|$ dir (Neden?). Lagrange teoremini uygularsak $|a| \Big| |G|$ elde edilir. $|G| = k|a|$ diyelim. O zaman

$$a^{|G|} = a^{|a|k} = (a^{|a|})^k = e^k = e$$

olur ve ispat tamamlanır. □

Örnek 2.38 G en az 2 elemanlı bir grup olsun. G nin trivial olmayan altgrubu yoksa G nin asal mertebeli olduğunu gösteriniz.

Çözüm: G nin trivial olmayan altgrupları olmasın. $|G|$ nin asal olduğunu göstereceğiz. Bir $e \neq a \in G$ için $U = \langle a \rangle$ altgrubunu düşünelim. $U = \{ e \}$ olamaz, o halde $U = G$ olmalıdır. Yani G devirlidir. Devirli grupların, grubun mertebesini bölen her sayıya karşılık bir altgrubu vardır. (bkz. Teorem 2.20). G nin trivial olmayan altgrubu olmadığından $|G|$ asaldır.

[1] Joseph–Louis Lagrange (1736-1813)

Örnek 2.39 G bir grup, $a \in G$ olsun. $a^m = e$ ise $|a| \Big| m$ olduğunu gösterin.
Çözüm: $|a| = n$ olsun. $n \leqslant |m|$ olduğu açıktır. Bölme algoritmasından dolayı m, n sayı çifti için $m = nq + r, 0 \leqslant r < n$ olacak şekilde $q, r \in \mathbb{Z}$ vardır. Şimdi

$$a^m = e \Longrightarrow a^{nq+r} = e \Longrightarrow (a^n)^q a^r = e \Longrightarrow e^q a^r = e \Longrightarrow a^r = e$$

olup $r < n = |a|$ olduğundan $r = 0$ olmalıdır. (Aksi halde bu durum $|a| = n$ olmasıyla çelişirdi.) Yani $m = nq$ olup $n \big| m$ dir.

Teorem 2.40 Asal mertebeli her grup devirlidir.

İspat: G mertebesi asal olan bir grup olsun. $|G| = p$ diyelim. Bir $e \neq a \in G$ için $U = \langle a \rangle$ devirli altgrubunu düşünelim. Lagrange teoreminden dolayı $|U| \Big| p$ olmalıdır. p asal olduğundan $|U| = 1$ veya $|U| = p$ olabilir. $e \neq a$ seçildiğinden $|U| > 1$ dir. O halde $|U| = p$ olmalıdır. Yani $G = U$ olup G devirlidir. □

Tanım 2.41 m ve n iki tamsayı olsun. Eğer m ile n nin en büyük ortak böleni 1 ise bu iki sayıya ***aralarında asaldır*** denir ve $(m, n) = 1$ yazılır.

Lemma 2.42 $(m, n) = 1$ olması için gerek ve yeter şart $mq + nr = 1$ olacak şekilde q, r tamsayılarının var olmasıdır.

Tanım 2.43 n pozitif bir tamsayı olsun. n den küçük ve n ile aralarında asal olan pozitif tamsayıların sayısı $\phi(n)$ ile gösterilir ve ϕ fonksiyonuna ***Euler-ϕ fonksiyonu*** denir. Örneğin, $\phi(10) = 4, \phi(9) = 6$ dır. p asal ise $\phi(p) = p - 1$ olduğu açıktır.

Teorem 2.44 n pozitif bir tamsayı olsun. $\mathbb{Z}_n$'de n ile aralarında asal olan sayılar modülo n çarpımı ile bir abelyen grup oluştururlar. (Bu grubu $\mathbb{Z}_n^*$ ile göstereceğiz.)

İspat: $(a, n) = 1$ ve $(b, n) = 1$ olsun. $(ab, n) = 1$ olduğunu göstermeliyiz. (Burada tabii ki a ile b nin çarpımı modulo n çarpımına göre yapılmıştır.)

$$\begin{aligned}
(a,n) = 1 &\Longrightarrow aq_1 + nr_1 = 1 \text{ olacak şekilde } q_1, r_1 \in \mathbb{Z} \text{ vardır,} \\
(b,n) = 1 &\Longrightarrow bq_2 + nr_2 = 1 \text{ olacak şekilde } q_2, r_2 \in \mathbb{Z} \text{ vardır,} \\
&\Longrightarrow ab(\underbrace{q_1 q_2}_{q}) + n(\underbrace{aq_1 r_2 + bq_2 r_1 + nr_1 r_2}_{r}) = 1 \\
&\Longrightarrow (ab)q + nr = 1 \qquad (q, r \in \mathbb{Z}) \\
&\Longrightarrow (ab, n) = 1
\end{aligned}$$

olup ab ile n aralarında asaldır.

Modülo n çarpmasının birleşme ve değişme özelliği vardır ve 1 sayısı bu grubun birim elemanıdır. Şimdi ters elemanın varlığını gösterelim. $(a,n)=1$ olsun. Bu durumda $aq+nr=1$ olacak şekilde $q,r\in\mathbb{Z}$ vardır. $1\leqslant q<n$ seçilebilir (Neden?). Bu durumda $aq\equiv 1 \pmod{n}$ olup $a^{-1}=q$ olur. □

Örnek 2.45 $\mathbb{Z}_9^*=\{1,2,4,5,7,8\}$ grubunun çarpım tablosunu yazalım.

$\cdot$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Dikkat edilecek olursa, bu grubun mertebesi 6 olduğundan her elemanın 6. kuvveti birim elemana eşit olur. Gerçekten de $1^6=1, 2^6=64, 4^6=4096, 5^6=15625, 7^6=117649, 8^6=262144$ olup bu sayıların hepsi 9'a bölününce 1 kalanı verirler.

Teorem 2.46 (Euler[2]) n pozitif bir tamsayı olsun. $(a,n)=1$ ise $a^{\phi(n)}\equiv 1 \pmod{n}$ dir.

İspat: $G=(\mathbb{Z}_n^*,\cdot)$ grubunu düşünelim. Bu grubun mertebesi $\phi(n)$ dir. Her $a\in G$ için $a^{|G|}=e$ olacağından $a^{\phi(n)}\equiv 1 \pmod{n}$ dir. □

Teorem 2.47 (Fermat[3]) p bir asal sayı ve $a\in\mathbb{Z}$ ise $a^p\equiv a \pmod{p}$ dir.

İspat: $\phi(p)=p-1$ olduğundan Euler teoremi gereğince $a^{p-1}\equiv 1 \pmod{p}$ yani $a^p\equiv a \pmod{p}$ elde edilir. □

Örnek 2.48 $p=7$ alalım. $(-2)^7=-128=(-19)\cdot 7+5$ olup $-128\equiv 5\equiv -2 \pmod{7}$ dir.

Teorem 2.49 G bir grup H ve K, G nin iki altgrubu olsun. HK nın altgrup olması için gerek ve yeter şart $HK=KH$ olmasıdır.

İspat: ($\Longleftarrow$)$HK=KH$ olsun. HK nın altgrup olduğunu göstereceğiz. $x=h_1k_1\in HK$ ve $y=h_2k_2\in$

[2]Leonhard Euler (1707-1783)
[3]Pierre de Fermat (1601-1665)

HK alalım. ($h_i \in H, k_i \in K$ dır.)

$$\begin{aligned} xy^{-1} &= h_1k_1(h_2k_2)^{-1} = h_1\underbrace{k_1{k_2}^{-1}}_{k_3}{h_2}^{-1} \\ &= h_1\ \underbrace{k_3{h_2}^{-1}}_{\in KH=HK} \\ &= \underbrace{h_1h_3}_{\in H}k_4 \\ &= h_4k_4 \in HK \end{aligned}$$

olup Theorem 2.8 den HK altgruptur.

($\Longrightarrow$) Şimdi de HK nın altgrup olduğunu kabul edip $HK = KH$ olduğunu gösterelim.

$$\begin{aligned} x = kh \in KH &\Longrightarrow x^{-1} = h^{-1}k^{-1} \in HK \\ &\Longrightarrow HK \text{ altgrup olduğundan } (x^{-1})^{-1} = x \in HK \\ &\Longrightarrow KH \subseteq HK \end{aligned}$$

Ayrıca,

$$\begin{aligned} x \in HK &\Longrightarrow HK \text{ altgrup olduğundan } x^{-1} \in HK \\ &\Longrightarrow \exists\, h \in H, k \in K \text{ için } x^{-1} = hk \\ &\Longrightarrow x = k^{-1}h^{-1} \in KH \\ &\Longrightarrow HK \subseteq KH. \end{aligned}$$

Sonuç olarak $HK = KH$ elde edilir. □

ALIŞTIRMALAR

1. $(\mathbb{Z}_{10}, +)$ grubunda 5 elemanının derecesini bulunuz. 5'in derecesi grubun mertebesini böler mi? 5'in $(\mathbb{Z}, +)$ daki derecesi kaçtır?

2. G bir abelyen grup olsun. $H = \{\, x \in G : x^2 = e \,\}$ kümesinin G nin bir altgrubu olduğunu gösteriniz.

3. H_1, H_2 bir G grubunun iki altgrubu olsun. $H_1 \cup H_2 \leqslant G \iff H_1 \subseteq H_2$ veya $H_2 \subseteq H_1$. Gösterin.

4. $(\mathbb{Q} \setminus \{\, 0 \,\}, \cdot)$ grubunda $A = \{\, 3, \frac{1}{2} \,\}$ ise $\langle A \rangle$ nedir?

5. G bir grup ve $a \in G$ olsun. $C(a) = \{\, x \in G : ax = xa \,\}$ kümesine ***a'nın merkezleyeni*** denir. ($C(a)$ aslında a elemanı ile değişmeli olan elemanların kümesidir.) Her $a \in G$ için $C(a) \leqslant G$ olduğunu gösterin. Ayrıca $|a| = 5$ ise $C(a) = C(a^3)$ olduğunu gösterin.

6. $G = \{1, -1, i, -i\}$ grubu verilsin. $H = \{1, -1\}$ olsun. H nin G deki bütün farklı sağ kosetlerini ve indeksini bulunuz.

7. H ve K, G nin sonlu altgrupları ise

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

olduğu bilinmektedir. $G = (\mathbb{C} \setminus \{0\}, \cdot)$ ve $H = \{1, -1, i, -i\}, K = \{1, -1\}$ alarak bu eşitliğin doğru olduğunu görünüz. Ayrıca bu eşitliği kullanarak $|H| > \sqrt{|G|}$ ve $|K| > \sqrt{|G|}$ ise $H \cap K \neq \{e\}$ olduğunu gösteriniz.

8. $(\mathbb{Z}, +)$ da $4\mathbb{Z}$ altgrubunun tüm farklı sağ kosetlerini ve indeksini bulunuz.

9. $K = \{a, b, c, d\}$ grubunun çarpım tablosu aşağıda verilmiştir.

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

K değişmeli midir? K nın tüm altgruplarını ve bunların sağ kosetlerini bulunuz. K devirli midir?

10. G bir grup olsun. $\emptyset \neq H \subseteq G$ olsun. H bir altgrup $\Longrightarrow HH = H$ olduğunu gösterin. Eğer H sonsuz elemanlı ise bu önermenin tersinin doğru olmadığını gösterin. (İpucu: Bir ters örnek verin.)

11. G bir grup $H \leqslant G$ olsun. $\theta(xH) = Hx^{-1}$ şeklinde tanımlanan fonksiyonun 1–1 olduğunu gösterin. (Önce iyi tanımlandığını göstermek gereklidir.)

12. G bir grup; $H \leqslant G, K \leqslant G$ olsun. $|H| = 75$ ve $|K| = 57$ ise $H \cap K$ nın devirli olduğunu gösterin.

13. G bir grup $a \in G$ olsun. $H = \{x \in G : \exists\, n \in \mathbb{Z}$ için $x = a^n\}$ kümesi G nin bir altgrubudur, gösterin.

14. $\mathbb{Z}_{14}^*$ grubunun çarpım tablosunu yazınız. Bu grup devirli midir? Bu grubun trivial olmayan bir altgrubunu bulunuz.

15. $(\mathbb{C} \setminus \{0\}, .)$ grubunda $H = \{x + iy : xy \geqslant 0\}$ bir alt grup mudur?

16. Bir G grubunda bir H altgrubunun iki sağ kosetinin aynı ya da ayrık olduğunu gösterin.

Bölüm 3

Normal Altgruplar ve Faktör Grupları

Daha önce S_3 grubunda $H = \{ f_1, f_2 \}$ altgrubunun sağ kosetlerini bulmuştuk. Aynı grubun sol kosetlerini de hesaplayıp karşılaştıralım:

Sol Kosetler	**Sağ Kosetler**
$f_1H = \{ f_1, f_2 \}$	$Hf_1 = \{ f_1, f_2 \}$
$f_2H = \{ f_2, f_1 \}$	$Hf_2 = \{ f_2, f_1 \}$
$f_3H = \{ f_3, f_5 \}$	$Hf_3 = \{ f_3, f_4 \}$
$f_4H = \{ f_4, f_6 \}$	$Hf_4 = \{ f_4, f_3 \}$
$f_5H = \{ f_5, f_3 \}$	$Hf_5 = \{ f_5, f_6 \}$
$f_6H = \{ f_6, f_4 \}$	$Hf_6 = \{ f_6, f_5 \}$

Tablodan görüldüğü gibi sol kosetlere parçalanış ile sağ kosetlere parçalanış birbirinden farklıdır.

Tanım 3.1 G bir grup ve $N \leqslant G$ olsun. Her $g \in G$ ve her $n \in N$ için $gng^{-1} \in N$ ise N ye G nin ***normal altgrubu*** denir ve $N \lhd G$ yazılır. $gNg^{-1} = \{ gng^{-1} : n \in N \}$ olduğundan, "N nin normal altgrup olması için gerek ve yeter şart her $g \in G$ için $gNg^{-1} \subseteq N$ olmasıdır" diyebiliriz.

Not 3.2 $\{ e \}$ ve G, G nin normal altgruplarıdır. (Neden?) G abelyen ise $gng^{-1} = n \in N$ olup abelyen bir grubun her altgrubunun normal olduğu görülür.

Teorem 3.3 G bir grup, $N \leqslant G$ olsun. Aşağıdakiler birbirine denktir.

(i) $N \lhd G$

(ii) Her $g \in G$ için $gNg^{-1} = N$

(iii) Her $g \in G$ için $gN = Ng$

İspat: (**i**$\Longrightarrow$ **ii**) $N \lhd G$ olsun. Tanımdan dolayı $gNg^{-1} \subseteq N$ dir. Şimdi

$$N = g\underbrace{g^{-1}Ng}_{\subseteq N}g^{-1} \subseteq gNg^{-1}$$

olup sonuçta $gNg^{-1} = N$ olduğu görülür.

İspat: (**ii**$\Longrightarrow$ **iii**) $gNg^{-1} = N \Longrightarrow gNg^{-1}g = Ng \Longrightarrow gN = Ng$

İspat: (**iii**$\Longrightarrow$ **i**) $gN = Ng \Longrightarrow gNg^{-1} = N \Longrightarrow gNg^{-1} \subseteq N \Longrightarrow N \lhd G$. □

Örnek 3.4 S_3'de $H = \{ f_1, f_2 \}$ olsun. $Hf_3 \neq f_3H$ olup H nin normal olmadığı görülür. Şimdi $N = \langle f_4 \rangle = \{ f_1, f_4, f_5 \}$ olsun.

$$Nf_1 = f_1N = Nf_4 = f_4N = Nf_5 = f_5N = \{ f_1, f_4, f_5 \}$$
$$Nf_2 = f_2N = Nf_3 = f_3N = Nf_6 = f_6N = \{ f_2, f_3, f_6 \}$$

olup $N \lhd G$ dir.

Bu bölümde bir G grubunun H altgrubunun sağ kosetleri arasında $(Ha) \cdot (Hb) = H(ab)$ şeklinde bir işlem tanımlamak istiyoruz. Ancak eğer H normal değilse bu işlem iyi tanımlanmamıştır. Yani $Ha_1 = Ha_2$ ve $Hb_1 = Hb_2$ ise $H(a_1b_1) \neq H(a_2b_2)$ olabilir. Mesela $G = S_3$ ve $H = \{ f_1, f_2 \}$ ise $Hf_3 = Hf_4$ ve $Hf_5 = Hf_6$ olup $H(f_3f_5) = Hf_2 = \{ f_1, f_2 \}$ dir, fakat $H(f_4f_6) = Hf_3 = \{ f_3, f_4 \}$ dir. Ayrıca iki sağ kosetin çarpımı başka bir sağ kosete eşit olmayabilir; mesela

$$(Hf_3)(Hf_5) = \{ f_3, f_4 \} \cdot \{ f_5, f_6 \} = \{ f_2, f_4, f_1, f_3 \}$$

olup bu küme bir sağ koset değildir.

Teorem 3.5 G bir grup $H \leqslant G$ olsun. $Ha = Hx$ ve $Hb = Hy$ eşitliklerinden her zaman $H(ab) = H(xy)$ elde edilmesi için gerek ve yeter şart $H \lhd G$ olmasıdır.

İspat:($\Longrightarrow$) Her $a, b, x, y \in G$ için $Ha = Hx$ ve $Hb = Hy \Longrightarrow H(ab) = H(xy)$ olduğunu kabul edelim. Şimdi her $g \in G$ için $Hg = Hg$ ve her $h \in H$ için $He = Hh$ olduğunu biliyoruz. O halde

$$Hg = Hg, He = Hh \Longrightarrow Hg = H(gh) \Longrightarrow H = H(ghg^{-1}) \Longrightarrow ghg^{-1} \in H$$

olup H nin normal olduğu görülür.

($\Longleftarrow$) Şimdi de H nin normal olduğunu kabul edelim.

$$\begin{aligned} Ha = Hx, Hb = Hy &\Longrightarrow a^{-1}x \in H, b^{-1}y \in H \\ &\Longrightarrow a^{-1}xy \in Hy = Hb = bH \text{ (Çünkü } H \text{ normal)} \\ &\Longrightarrow b^{-1}a^{-1}xy \in H \\ &\Longrightarrow (ab)^{-1}(xy) \in H \\ &\Longrightarrow H(ab) = H(xy). \end{aligned}$$

□

Teorem 3.6 G bir grup, $H \leqslant G$ olsun. H nin iki sağ kosetinin çarpımının yine bir sağ koset olması için gerek ve yeter şart $H \lhd G$ olmasıdır.

İspat: ($\Longleftarrow$) $H \lhd G$ olsun. Ha, Hb iki sağ koset olsun.

$$(Ha)(Hb) = H(aH)b = H(Ha)b = (HH)ab = H(ab)$$

olup iki sağ kosetin çarpımı başka bir sağ kosettir.

($\Longrightarrow$) Şimdi her Ha, Hb sağ koseti için $(Ha)(Hb) = Hc$ olacak şekilde bir $c \in G$ olsun. $b = a^{-1}$ seçilirse:

$$\begin{aligned} HaHa^{-1} = Hc &\Longrightarrow eaea^{-1} = e = h_1 c \text{ olacak şekilde bir } h_1 \in H \text{ vardır} \\ &\Longrightarrow c = {h_1}^{-1} \in H \text{ olup } Hc = H \\ &\Longrightarrow HaHa^{-1} = H \\ &\Longrightarrow \forall\ h \in H \text{ için } haha^{-1} = h_2 \text{ olacak şekilde bir } h_2 \in H \text{ vardır} \\ &\Longrightarrow aha^{-1} = h^{-1}h_2 \in H \\ &\Longrightarrow aHa^{-1} \subseteq H \\ &\Longrightarrow H \lhd G \end{aligned}$$

□

Böylece H normal ise H nin sağ kosetleri üzerindeki çarpma işleminin iyi tanımlandığını ve kapalı olduğunu gösterdik.

Tanım 3.7 G bir grup, $N \lhd G$ olsun. N nin G deki farklı sağ kosetlerinin kümesini $G/N = \{\, Ng : g \in G \,\}$ ile gösterelim. Bu küme üzerinde

$$Na, Nb \in G/N \text{ için } (Na) \cdot (Nb) = N(ab)$$

şeklinde bir işlem tanımlayalım. Bu işlemin iyi tanımlandığını Teorem 3.5'de gösterdik. $(G/N, \cdot)$'nın bir grup olduğunu göstereceğiz. Bu gruba G nin N ile olan ***faktör grubu*** denir. (Faktör grubu yerine ***bölüm grubu*** terimi de kullanılmaktadır.)

Teorem 3.8 G bir grup, $N \lhd G$ olsun. G/N yukardaki tanımda verilen işlemle bir gruptur.

İspat: $(Na)(Nb) = N(ab)$ olup iki sağ kosetin çarpımı bir sağ kosettir.

$$\begin{aligned} Na(NbNc) &= NaN(bc) = N(a(bc)) \\ &= N((ab)c) = N(ab)Nc \\ &= (NaNb)Nc \end{aligned}$$

olup birleşme özelliği vardır. Her $Na \in G/N$ için

$$NaNe = Na \qquad \text{ve} \qquad NeNa = Na$$

olup $Ne = N$ bu grubun birim elemanıdır. Na'nın tersi $(Na)^{-1} = Na^{-1}$ dir, çünkü

$$NaNa^{-1} = Ne = N \qquad \text{ve} \qquad Na^{-1}Na = Ne = N.$$

Sonuç olarak G/N bir gruptur. □

Not 3.9 Lagrange Teoremi gereğince eğer $|G|$ sonlu ise $|G/N| = \dfrac{|G|}{|N|}$ dir.

Örnek 3.10 $G = (\mathbb{Z}, +)$ grubunda $U = 4\mathbb{Z}$ altgrubunu ele alalım. G abelyen olduğundan her altgrubu normaldir. U nun G deki farklı sağ kosetleri $G/U = \{\, U, U+1, U+2, U+3 \,\}$ şeklinde yazılabilir. Bu grubun tablosu şöyledir.

$+$	U	$U+1$	$U+2$	$U+3$
U	U	$U+1$	$U+2$	$U+3$
$U+1$	$U+1$	$U+2$	$U+3$	U
$U+2$	$U+2$	$U+3$	U	$U+1$
$U+3$	$U+3$	U	$U+1$	$U+2$

Burada, mesela $(U+2)+(U+3) = U+5 = U+1$ şeklinde hesaplanır.

Örnek 3.11 G bir grup olsun. $Z(G) = \{\, g \in G : \text{ her } x \in G \text{ için } gx = xg \,\}$ kümesine G nin ***merkezi*** denir. Bir grubun merkezi, gruptaki bütün elemanlarla değişmeli olan elemanların kümesidir. $Z(G) \lhd G$ olduğunu gösterin.

Çözüm: Önce $Z(G) \leqslant G$ olduğunu göstermeliyiz. $g, h \in Z(G)$ alalım. O halde her $x \in G$ için $gx = xg, hx = xh$ dir. Şimdi

$$hx = xh \Longrightarrow x = h^{-1}xh \Longrightarrow xh^{-1} = h^{-1}x$$

olur ve

$$(gh^{-1})x = g(h^{-1}x) = g(xh^{-1}) = (gx)h^{-1} = (xg)h^{-1} = x(gh^{-1})$$

olup $gh^{-1} \in Z(G)$ elde edilir. Teorem 2.8 den $Z(G) \leqslant G$ olur. Şimdi $z \in Z(G)$ ve $g \in G$ alalım. $gzg^{-1} \in Z(G)$ olduğunu göstermeliyiz. z elemanı gruptaki bütün elemanlarla değişmeli olduğundan $gzg^{-1} = z \in Z(G)$ olup $Z(G) \lhd G$ dir.

Tanım 3.12 En az 2 elemanlı bir G grubunun $\{ e \}$ ve G'den başka normal altgrubu yoksa G'ye ***basit grup*** denir.

Örnek 3.13 $\mathbb{Z}_5 = \{ 0, 1, 2, 3, 4 \}$ grubunun altgrupları (dolayısıyla normal altgrupları) $\{ 0 \}$ ve kendisidir. O halde $\mathbb{Z}_5$ basit gruptur.

Teorem 3.14 Bir abelyen grubun basit olması için gerek ve yeter şart asal mertebeli olmasıdır.

İspat: ($\Longrightarrow$) G abelyen ve basit bir grup olsun. Bir $e \neq a \in G$ için $|a| = n$ sonludur. Eğer n sonlu olmasaydı $\langle a \rangle$ devirli altgrubu da sonlu olmayıp G nin normal altgrubu olurdu. Eğer $\langle a \rangle = G$ olsaydı G sonsuz devirli grup olurdu ve G nin trivial olmayan altgrubu (yani normal altgrubu) olurdu (Neden?). O halde n sonludur. Öyleyse bir p asal böleni vardır. Buna göre $\left\langle a^{n/p} \right\rangle$ altgrubu mertebesi p olan bir normal altgruptur. G basit olduğundan $G = \left\langle a^{n/p} \right\rangle$ olmalıdır. O halde $|G| = p$ dir.

($\Longleftarrow$) p bir asal sayı olmak üzere $|G| = p$ olsun. $U \lhd G$ bir olsun. Lagrange teoremi gereğince $|U| \Big| p$ dir. p asal olduğundan $|U| = 1$ veya $|U| = p$ dir. O halde $U = \{ e \}$ veya $U = G$ olabilir. Yani G basittir.$\square$

Örnek 3.15 G bir grup ve H de indeksi 2 olan bir altgrup olsun. $H \lhd G$ olduğunu gösterin.
Çözüm: H nin G de iki farklı sağ koseti vardır. Bunlar H ve Ha dir. Burada $a \in G \setminus H$ olduğu açıktır. ($Ha = H \iff a \in H$ olduğunu hatırlayın.) Benzer şekilde iki farklı sol koseti H ve aH dir. Bunlar G nin parçalanışıdır. Şimdi $g \in G$ verilsin. $g \in H$ ise $Hg = gH = H$ dir. $g \in G \setminus H$ ise $Hg = gH = G \setminus H$ olup sağ koset sol kosete eşittir. O halde $H \lhd G$ dir.

Örnek 3.16 İki normal altgrubun kesişiminin de normal olduğunu gösteriniz.
Çözüm: G bir grup $H \lhd G$ ve $K \lhd G$ olsun. $H \cap K \leqslant G$ olduğunu biliyoruz. Şimdi her $g \in G$ ve her $x \in H \cap K$ için

$$\begin{aligned} x \in H \cap K &\Longrightarrow x \in H \text{ ve } x \in K \\ &\Longrightarrow H \lhd G, K \lhd G \text{ olduğundan } gxg^{-1} \in H, gxg^{-1} \in K \\ &\Longrightarrow gxg^{-1} \in H \cap K \\ &\Longrightarrow H \cap K \lhd G. \end{aligned}$$

Örnek 3.17 $H \leqslant G$ ve $N \lhd G$ ise $HN \leqslant G$ olduğunu gösterin.
Çözüm: $x = h_1 n_1 \in HN$ ve $y = h_2 n_2 \in HN$ alalım.

$$\begin{aligned} xy^{-1} &= h_1 \underbrace{n_1 {n_2}^{-1}}_{\in N} {h_2}^{-1} \\ &= h_1 n_3 {h_2}^{-1} \\ &= \underbrace{h_1 {h_2}^{-1}}_{\in H} \underbrace{h_2 n_3 {h_2}^{-1}}_{\in h_2 N {h_2}^{-1} = N} \\ &= h_3 n_4 \in HN \end{aligned}$$

olup Teorem 2.8 gereğince $HN \leqslant G$ dir.

Örnek 3.18 $H \lhd G$ ve $K \lhd G$ ise $HK \lhd G$ olduğunu gösterin.
Çözüm: $x = h_1 k_1 \in HK$ ve $y = h_2 k_2 \in HK$ olsun. O zaman

$$\begin{aligned} xy^{-1} &= h_1 \underbrace{k_1 {k_2}^{-1}}_{\in K} {h_2}^{-1} \\ &= h_1 k_3 {h_2}^{-1} \\ &= \underbrace{h_1 {h_2}^{-1}}_{\in H} \underbrace{h_2 k_3 {h_2}^{-1}}_{\in h_2 K {h_2}^{-1} = K} \\ &= h_3 k_4 \in HK \end{aligned}$$

olup Teorem 2.8 gereğince $HK \leqslant G$ dir. Şimdi $HK \lhd G$ olduğunu gösterelim. $H \lhd G, K \lhd G$ olduğundan her $g \in G$ için $Hg = gH$ ve $Kg = gK$ dır. $g^{-1} \in G$ olduğundan $g^{-1}K = Kg^{-1}$ dir. O halde:

$$\begin{aligned} g(HK)g^{-1} &= (gH)(Kg^{-1}) \\ &= (Hg)(g^{-1}K) \\ &= H(gg^{-1})K \\ &= HK \end{aligned}$$

olup $HK \lhd G$ olduğu görülür.

Örnek 3.19 G abelyen bir grup, $H, K \leqslant G$ olsun. Ayrıca $|H| = m, |K| = n$ ve $H \cap K = \{ e \}$ olsun. $HK \leqslant G$ ve $|HK| = mn$ olduğunu gösterin.
İspat:

$$x = h_1 k_1 \in HK, y = h_2 k_2 \in HK \Longrightarrow xy^{-1} = h_1 k_1 {k_2}^{-1} {h_2}^{-1} = (h_1 {h_2}^{-1})(k_1 {k_2}^{-1}) \in HK$$

olup $HK \leqslant G$ dir. Ayrıca

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = |H|\,|K| = mn.$$

Örnek 3.20 $M = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z} \right\}$ kümesi bilinen matris toplamı ile bir gruptur. $H = \left\{ \begin{bmatrix} a & b \\ c & -a \end{bmatrix} : a,b,c \in \mathbb{Z} \right\}$ kümesi M nin normal altgrubudur, gösterin. M/H yi oluşturunuz.

Çözüm:

$$X = \begin{bmatrix} a & b \\ c & -a \end{bmatrix}, Y = \begin{bmatrix} d & e \\ f & -d \end{bmatrix} \in H \Longrightarrow X + (-Y) = \begin{bmatrix} a-d & b-e \\ c-f & -(a-d) \end{bmatrix} \in H$$

dir. Teorem 2.8 gereğince $H \leqslant M$ dir. Matrislerdeki toplama işlemi değişmeli olduğundan M bir abelyen gruptur. O halde $H \lhd M$ dir. $M/H = \{ H + X : X \in M \}$ şeklinde yazılabilir.

Örnek 3.21 $\mathbb{Z}_{12}$'de $H = \langle 6 \rangle$ altgrubunu bulunuz. $\mathbb{Z}_{12}/H$ yi yazınız. Bu gruptaki elemanların derecelerini bulunuz.

Çözüm: $H = \langle 6 \rangle = \{ 0, 6 \}$ dır. H nin farklı sağ kosetleri:

$$H + 0 = \{ 0, 6 \} = H + 6$$
$$H + 1 = \{ 1, 7 \} = H + 7$$
$$H + 2 = \{ 2, 8 \} = H + 8$$
$$H + 3 = \{ 3, 9 \} = H + 9$$
$$H + 4 = \{ 4, 10 \} = H + 10$$
$$H + 5 = \{ 5, 11 \} = H + 11$$

O halde $\mathbb{Z}_{12}/H = \{ H, H+1, H+2, H+3, H+4, H+5 \}$ dir. Bu elemanların dereceleri:

$$|H| = 1, \quad |H+1| = 6, \quad |H+2| = 3, \quad |H+3| = 2, \quad |H+4| = 3, \quad |H+5| = 6.$$

Örnek 3.22 G bir grup ve $H = \langle a \rangle$ sonlu devirli altgrubu G de normal olsun. Eğer $K \leqslant H$ ise $K \lhd G$ olduğunu gösterin.

Çözüm: $\langle a \rangle = H \lhd G$ ve $K \leqslant H$ olduğu veriliyor. $K \lhd G$ olduğunu göstereceğiz. $K \leqslant H$ ve $H \leqslant G$ olduğundan $K \leqslant G$ olduğu açıktır. Şimdi $k \in K, g \in G$ verilsin.

$$k \in K \Longrightarrow k \in H \Longrightarrow H \lhd G \text{ olduğundan } gkg^{-1} \in H.$$

Şimdi K sonlu olduğundan $|k| = m$ sonludur. $|gkg^{-1}| = m$ dir, çünkü:

$$(gkg^{-1})^m = \underbrace{(gkg^{-1})(gkg^{-1}) \ldots (gkg^{-1})}_{m-\text{tane}} = gk^m g^{-1} = gg^{-1} = e$$

olur. Ayrıca gkg^{-1} in daha küçük bir kuvveti e ye eşit olamaz. (Neden?)

$$|gkg^{-1}| = m \Longrightarrow |\langle gkg^{-1} \rangle| = m \quad \text{ve} \quad |k| = m \Longrightarrow |\langle k \rangle| = m$$

olur. Ayrıca $\langle k \rangle \leqslant K \leqslant H$ ve $\langle gkg^{-1} \rangle \leqslant H$ olup $\langle k \rangle$ ve $\langle gkg^{-1} \rangle$ altgrupları H nin mertebeleri aynı iki altgrubu olur. H devirli olduğundan ve devirli bir grubun mertebesi aynı olan iki altgrubu eşit olacağından $\langle k \rangle = \langle gkg^{-1} \rangle$ olmalıdır. O halde $\langle gkg^{-1} \rangle \leqslant K$ olup $gkg^{-1} \in K$ dır. Yani $K \lhd G$ olur.

ALIŞTIRMALAR

1. $G = \{ e, a, a^2, a^3 \}$ 4-üncü mertebeden devirli grup ve $H = \{ e, a^2 \}$ onun altgrubu olsun. $H \lhd G$ olduğunu gösterip G/H yi yazınız.

2. G bir grup ve H de onun iki elemanlı normal bir altgrubu ise $H \subseteq Z(G)$ olduğunu gösterin.

3. Bir grupta derecesi 2 olan sadece bir tane eleman varsa bu elemanın grubun merkezinde olduğunu gösterin.

4. G bir grup ve H de $Z(G)$ nin alt kümesi olan bir altgrup olsun. $H \lhd G$ olduğunu gösterin.

5. G abelyen bir grup ve $N \lhd G$ olsun. G/N nin abelyen olduğunu gösterin.

6. G bir grup, $H \leqslant G$ ve $K \lhd G$ ise $H \cap K \lhd H$ olduğunu gösterin.

7. G bir grup ve $H \leqslant G$ olsun. $N_G(H) = \{ x \in G : xHx^{-1} = H \}$ kümesine H nin G deki ***normalleyeni*** denir. $N_G(H) \leqslant G$ ve $H \lhd N_G(H)$ olduğunu gösterin.

8. $Q_8 = \{ 1, -1, i, -i, j, -j, k, -k \}$ olsun. $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i, ki = j$ ve $ji = -k, kj = -i, ik = -j$ kuralları verilsin. Q_8 in grup tablosunu yazınız. Bu gruba ***quaternionlar grubu*** denir. Q_8 in merkezini bulunuz. $\{ i, j \}$ kümesi tarafından doğurulan alt grubu bulunuz. Q_8'in bütün altgruplarının normal olduğunu gösterin. (Q_8, bütün altgrupları normal olup da abelyen olmayan bir grup örneğidir.)

9. $SL_n(\mathbb{R})$ ile $n \times n$ tipinde ve determinantı 1 olan matrislerin kümesini gösterelim. $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$ olduğunu gösterin.

10. H ve K bir G grubunun normal altgrupları ve $H \cap K = \{ e \}$ olsun. Her $h \in H$ ve $k \in K$ için $hk = kh$ olduğunu gösterin.

11. G abelyen olmayan bir grup ve Z de onun merkezi olsun. O zaman G/Z devirli grup olamaz.

12. G bir grup olsun. $H \leqslant G$ alt grubu "her $x \in G$ için $x^2 \in H$" özelliğine sahip olsun. $H \lhd G$ olduğunu gösterin. (İpucu: $xhx^{-1} = (xh)^2 h^{-1} (x^{-1})^2$) Ayrıca G/H nin abelyen olduğunu gösterin.

ALIŞTIRMALARIN ÇÖZÜMLERİ

ÇÖZÜM 1. G abelyen ve H altgrup olduğundan $H \lhd G$ dir. $G/H = \{ H, Ha \}$ olur.

ÇÖZÜM 2. $H = \{ e, h \}$ olsun. $e \in Z(G)$ olduğu açıktır. Biz $h \in Z(G)$ olduğunu yani her $x \in G$

Bölüm 4

Homomorfizmalar ve İzomorfizmalar

Tanım 4.1 $(G,\cdot)$ ve $(H,\star)$ iki grup olsun. $f: G \longrightarrow H$ bir fonksiyon olsun. Eğer f fonksiyonu "grup işlemini koruyorsa"; yani her $a,b \in G$ için

$$f(a\cdot b) = f(a)\star f(b)$$

ise f ye G den H ye bir ***grup homomorfizması*** veya kısaca ***homomorfizma*** denir.

$\cdot$	$\dots$	$\dots$	b	$\dots$
$\vdots$			$\vdots$	
$\vdots$			$\vdots$	
a	$\dots$	$\dots$	$a\cdot b$	
$\vdots$				

$\star$	$\dots$	$\dots$	$f(b)$	$\dots$
$\vdots$			$\vdots$	
$\vdots$			$\vdots$	
$f(a)$	$\dots$	$\dots$	$f(a)\star f(b) = f(a\cdot b)$	$\dots$
$\vdots$				

Örnek 4.2 $I: G \longrightarrow G$ birim dönüşümü G'nin bir homomorfizmasıdır, çünkü $I(xy) = xy = I(x)I(y)$.

Örnek 4.3 $G = (\mathbb{Z},+)$ ve $n \in \mathbb{Z}$ olsun. $f: G \longrightarrow G$ dönüşümü her $x \in \mathbb{Z}$ için $f(x) = nx$ şeklinde tanımlansın. f bir homomorfizmadır, çünkü

$$f(x+y) = n(x+y) = nx + ny = f(x) + f(y).$$

Örnek 4.4 $G = (\mathbb{R},+)$ ve $H = (\mathbb{R}^+,\cdot)$ olsun. $f: G \longrightarrow H, f(x) = e^x$ şeklinde tanımlansın. Her $x,y \in \mathbb{R}$ için

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x)\cdot f(y)$$

olup f bir grup homomorfizması olur. Burada $g: H \longrightarrow G, g(x) = \ln x$ de bir homomorfizmadır.

Örnek 4.5 $G = (\mathbb{Z}, +)$ ve $H = (\mathbb{Z}_n, +)$ olsun. H deki $+$ işlemi modülo n'e göre yapılmaktadır. Buna göre $f : G \longrightarrow H, f(x) = x \pmod{n}$ şeklinde tanımlanan dönüşüm bir homomorfizmadır, çünkü her $x, y \in \mathbb{Z}$ için

$$f(x+y) = (x+y) \pmod{n} = (x \pmod{n}) + (y \pmod{n}) = f(x) + f(y).$$

Örnek 4.6 $G = GL_n(\mathbb{R}), H = (\mathbb{R} \setminus \{0\}, \cdot)$ olsun. $f : G \longrightarrow H, f(X) = \det(X)$ olsun. f bir homorfizmadır, çünkü her $X, Y \in GL_n(\mathbb{R})$ için

$$f(X \cdot Y) = \det(X \cdot Y) = \det(X) \cdot \det(Y) = f(X) \cdot f(Y).$$

Örnek 4.7 G bir grup, $N \lhd G$ olsun. $f : G \longrightarrow G/N$ her $x \in G$ için $f(x) = Nx$ şeklinde tanımlanan dönüşüm örten bir homomorfizmadır. Bu dönüşüme G den G/N üzerine olan ***kanonik (doğal) homomorfizma*** denir. Her $x, y \in G$ için

$$f(xy) = N(xy) = (Nx)(Ny) = f(x)f(y)$$

olup f bir homomorfizmadır. Her $Y = Nx \in G/N$ için $f(x) = Nx = Y$ olup f nin örten olduğu görülür.

Teorem 4.8 G ve H iki grup ve $f : G \longrightarrow H$ bir homomorfizma olsun.

(i) e, G'nin ve e_0 da H nin birim elemanı ise $f(e) = e_0$

(ii) Her $a \in G$ için $f(a^{-1}) = [f(a)]^{-1}$

(iii) $f(G) \leqslant H$

(iv) G abelyen ve f örten ise H de abelyendir.

(v) G devirli ve f örten ise H de devirlidir.

İspat (i) Her $g \in G$ için

$$\begin{aligned} f(g) = f(ge) = f(g)f(e) &\Longrightarrow f(g) = f(g)f(e) \\ &\Longrightarrow f(g)^{-1}f(g) = f(g)^{-1}f(g)f(e) \\ &\Longrightarrow e_0 = e_0 f(e) \\ &\Longrightarrow f(e) = e_0 \end{aligned}$$

İspat (ii) Her $a \in G$ için

$$\begin{aligned} f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e_0, \\ f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e_0 \end{aligned}$$

olup $[f(a)]^{-1} = f(a^{-1})$ dir.

İspat (iii) $x, y \in f(G)$ alalım.

$$\begin{aligned} x, y \in f(G) &\Longrightarrow f(a) = x, f(b) = y \text{ olacak şekilde } \exists\ a, b \in G \text{ vardır} \\ &\Longrightarrow ab^{-1} \in G \text{ olup } f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} = xy^{-1} \\ &\Longrightarrow xy^{-1} \in f(G) \\ &\Longrightarrow \text{ Teorem 2.8 gereğince } f(G) \leqslant H. \end{aligned}$$

İspat (iv) G abelyen ve f örten olsun. $x, y \in H$ olsun.

$$\begin{aligned} x, y \in H &\Longrightarrow f \text{ örten olduğundan } \exists\ a, b \in G \text{ için } f(a) = x, f(b) = y. \\ &\Longrightarrow xy = f(a)f(b) = f(ab) = f(ba) \ (G \text{ abelyen olduğundan } ab = ba) \\ &\Longrightarrow xy = f(ba) = f(b)f(a) = yx \\ &\Longrightarrow H \text{ abelyen gruptur.} \end{aligned}$$

İspat (v) $G = \langle a \rangle$ devirli ve f örten olsun. f örten olduğundan $f(G) = H$ yazalım. $G = \{\, a^n : n \in \mathbb{Z} \,\}$ olup $f(G) = \{\, f(a^n) : n \in \mathbb{Z} \,\}$ dir. Şimdi $n \geqslant 1$ ise

$$f(a^n) = f(\underbrace{a \cdot a \cdots a}_{n-tane}) = \underbrace{f(a)f(a)\cdots f(a)}_{n-tane} = f(a)^n.$$

Benzer şekilde $n < 0$ ise

$$\begin{aligned} f(a^n) = f((a^{-1})^{-n}) &= \underbrace{f(a^{-1})f(a^{-1})\cdots f(a^{-1})}_{(-n)-tane} \\ &= \underbrace{f(a)^{-1}f(a)^{-1}\cdots f(a)^{-1}}_{(-n)-tane} \\ &= [f(a)^{-1}]^{-n} \\ &= f(a)^n \end{aligned}$$

Ayrıca $n = 0$ ise $f(a^0) = f(e) = e_0 = f(a)^0$ dır. Sonuç olarak her $n \in \mathbb{Z}$ için $f(a^n) = f(a)^n$. O halde

$$H = f(G) = \{\, f(a^n) : n \in \mathbb{Z} \,\} = \{\, f(a)^n : n \in \mathbb{Z} \,\} = \langle f(a) \rangle$$

olup H de devirlidir. □

Not 4.9 $f : G \longrightarrow H$ bir homomorfizma olsun. $x, y \in G$ için

$$\beta = \{\, (x, y) : f(x) = f(y) \,\}$$

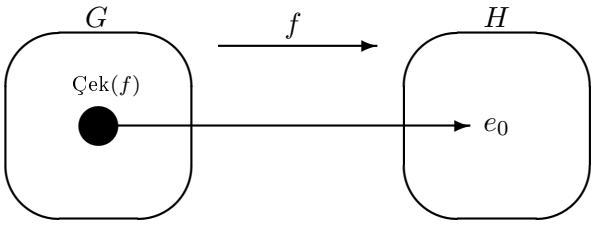
kümesi G de bir denklik bağıntısıdır. Bu bağıntıya göre bir $x \in G$ elemanının denklik sınıfı $\overline{x} = \{\, y \in G : f(x) = f(y) \,\}$ dir. Özel olarak e nin denklik sınıfı

$$\bar{e} = \{\, x \in G : f(x) = f(e) \,\} = \{\, x \in G : f(x) = e_0 \,\}$$

kümesine özel bir isim vereceğiz.

Tanım 4.10 G, H iki grup $f : G \longrightarrow H$ bir homomorfizma ve H nin birim elemanı e_0 olsun. f nin ***çekirdeği*** şöyle tanımlanır:

$$\text{Çek}(f) = \{\, x \in G : f(x) = e_0 \,\}$$



Teorem 4.11 $f : G \longrightarrow H$ bir grup homomorfizması ise $\text{Çek}(f) \lhd G$ dir.

İspat:

$$\begin{aligned} a, b \in \text{Çek}(f) &\Longrightarrow f(a) = f(b) = e_0 \\ &\Longrightarrow f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \\ &\Longrightarrow f(ab^{-1}) = e_0(e_0)^{-1} = e_0 \\ &\Longrightarrow ab^{-1} \in \text{Çek}(f) \\ &\Longrightarrow \text{ Teorem 2.8 gereğince } \text{Çek}(f) \leqslant G. \end{aligned}$$

$$\begin{aligned} g \in G, a \in \text{Çek}(f) &\Longrightarrow f(gag^{-1}) = f(g)f(a)f(g^{-1}) \\ &\Longrightarrow f(gag^{-1}) = f(g)f(a)f(g)^{-1} = f(g)e_0f(g)^{-1} \\ &\Longrightarrow f(gag^{-1}) = e_0 \\ &\Longrightarrow gag^{-1} \in \text{Çek}(f) \end{aligned}$$

olup $\text{Çek}(f) \lhd G$ olduğu görülür. □

Tanım 4.12 $f : G \longrightarrow H$ bir homomorfizma olsun. Bir $h \in H$ için $f(x) = h$ ise $x \in G$ elemanına h nin ***ters görüntüsü*** denir. h nin birden fazla ters görüntüsü olabilir. h nin ***ters görüntülerinin kümesi***

$$f^{-1}(h) = \{\, x \in G : f(x) = h \,\}$$

şeklinde ifade edilebilir. Şimdi bir $h \in H$ nin ters görüntü kümesinin Çek(f) nin bir sol koseti (veya sağ koseti) olduğunu göreceğiz.

Teorem 4.13 $f : G \longrightarrow H$ bir homomorfizma, $h \in H$ ve $x \in f^{-1}(h)$ olsun. Bu durumda $f^{-1}(h) = x \cdot$ Çek(f) dir.

İspat: Önce $f^{-1}(h) \subseteq x \cdot$ Çek(f) olduğunu gösterelim. $x \in f^{-1}(h)$ ise $f(x) = h$ dir.

$$\begin{aligned} b \in f^{-1}(h) &\Longrightarrow f(b) = h \\ &\Longrightarrow f(x) = f(b) \Longrightarrow f(x)^{-1}f(x) = f(x)^{-1}f(b) \\ &\Longrightarrow e_0 = f(x^{-1})f(b) = f(x^{-1}b) \\ &\Longrightarrow x^{-1}b \in \text{Çek}(f) \\ &\Longrightarrow \exists\ k \in \text{Çek}(f) \text{ için } x^{-1}b = k \\ &\Longrightarrow b = xk \in x \cdot \text{Çek}(f) \end{aligned}$$

olup $f^{-1}(h) \subseteq x \cdot$ Çek(f) elde edilir. Şimdi de

$$\begin{aligned} b \in x \cdot \text{Çek}(f) &\Longrightarrow \exists\ k \in \text{Çek}(f) \text{ için } b = xk \\ &\Longrightarrow f(b) = f(xk) = f(x)f(k) = f(x)e_0 = f(x) = h \\ &\Longrightarrow f(b) = h \text{ olup } b \in f^{-1}(h) \end{aligned}$$

olur ve $x \cdot$ Çek$(f) \subseteq f^{-1}(h)$ dir. Sonuç olarak $f^{-1}(h) = x \cdot$ Çek(f) dir. □

Sonuç 4.14 $h \in H$ elemanının bütün ters görüntüleri $x \in f^{-1}(h)$ olmak üzere $x \cdot$ Çek(f) kümesidir.

Tanım 4.15 $f : G \longrightarrow H$ grup homomorfizması birebir ise f ye bir ***izomorfizma*** denir. Eğer G den H ye örten bir izomorfizma (yani birebir ve örten bir homomorfizma) varsa G ile H gruplarına ***izomorfiktirler*** veya ***eş yapılıdırlar*** denir ve $G \cong H$ yazılır.

Not 4.16 Bazı yazarlar izomorfizmayı "birebir ve örten homomorfizma" olarak tanımlamaktadır. Bu durumda da $G \cong H$ olması "G den H ye bir izomorfizma vardır" şeklinde tanımlanır.

Not 4.17 Gruplar arasındaki "izomorfik (eş yapılı) olma" bağıntısının bir denklik bağıntısı olduğunu göstereceğiz. Bu yüzden cebirciler iki izomorfik grup arasında fark gözetmezler. İki izomorfik grubun yapıları aynıdır; sadece elemanları farklıdır. Bu yüzden, mesela, elemanlar arasında uygun eşleme yapıldığında grup tablolarının aynı olduğu görülür.

Örnek 4.18 $A = \{1, -1, i, -i\}$ kümesi çarpma işlemi ile bir gruptur. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ alalım. $f : \mathbb{Z}_4 \longrightarrow A$ dönüşümünü

$$f(0) = 1, \quad f(1) = i, \quad f(2) = -1, \quad f(3) = -i$$

şeklinde tanımlayalım. f nin 1–1 ve örten olduğu açıktır. f nin homomorfizma olduğu kontrol edilebilir. Mesela

$$f(1+2) = f(3) = -i \qquad \text{ve} \qquad f(1)f(2) = i(-1) = -i.$$

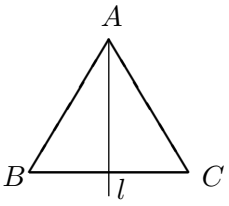
Bütün kontroller yapıldıktan sonra $A \cong \mathbb{Z}_4$ yazabiliriz. Şimdi grup tablolarının (elemanları f de verilen sırada yazdığımızda) aslında aynı olduğunu görelim.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

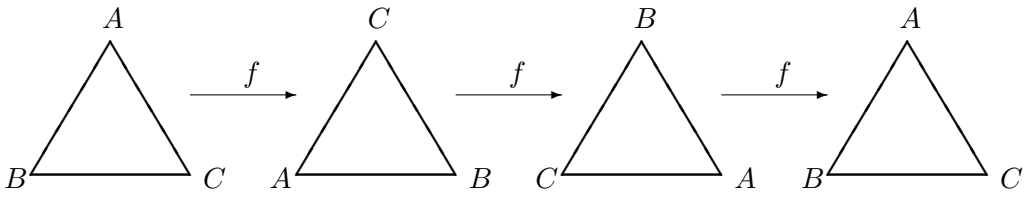
$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

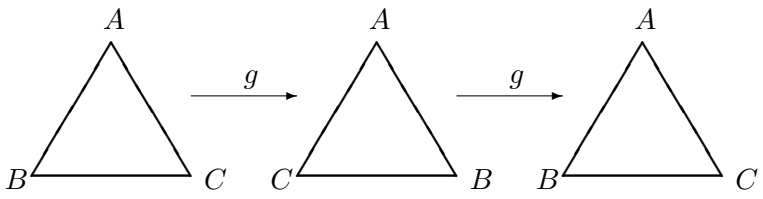
Benzer şekilde $G = \langle a \rangle = \{ e, a, a^2, a^3 \}$ 4-üncü mertebeden devirli grup ise $A \cong G$ dir. Bu şekildeki tüm grupların sınıfına 4-üncü mertebeden devirli grup denir ve hepsi de C_4 ile gösterilir. Genel olarak $n-$inci mertebeden devirli gruplar C_n ile gösterilir. Bu durumda $\mathbb{Z}_n \cong C_n$ olduğu açıktır.

Örnek 4.19 Şimdi şekildeki ABC eşkenar üçgenini düşünelim.



Bu üçgeni tam ortasından ve düzleme dik bir eksen etrafında 120° saatin ters yönünde döndürme işlemine f diyelim. l doğrusu etrafında 180° döndürmeye g diyelim. Bu durumda $f^3 = e$ ve $g^2 = e$ dir. Birim dönüşüm olarak üçgenin orjinal hali anlaşılmaktadır.





Bu şekilde elde edeceğimiz bütün farklı dönmeler : e, f, f^2, g, fg, f^2g fonksiyonlarıdır. Bu şekilde elde ettiğimiz gruba ***dihedral grup*** denir ve D_3 ile gösterilir. Benzer şekilde eşkenar n-gen kullanılarak elde edilen grup da D_n ile gösterilir ve $|D_n| = 2n$ dir. $D_3 = \{ e, f, f^2, g, fg, f^2g \}$ grubundan S_3 grubuna ϕ dönüşümünü

$$\phi : \begin{array}{c} e \longrightarrow f_1 \\ f \longrightarrow f_5 \\ f^2 \longrightarrow f_4 \\ fg \longrightarrow f_6 \\ g \longrightarrow f_2 \\ f^2g \longrightarrow f_3 \end{array}$$

şeklinde tanımlarsak bir örten izomorfizma elde ederiz. O halde $D_3 \cong S_3$. Tablodaki boşlukları doldurun.

$\cdot$	e	f	f^2	g	fg	f^2g
e	e	f	f^2	g	fg	f^2g
f	f	f^2	e	fg	f^2g	g
f^2	f^2	e	f	f^2g	g	fg
g	g	f^2g	fg	e	f	f^2
fg	fg					
f^2g	f^2g					

Teorem 4.20 $f : G \longrightarrow H$ homomorfizmasının bir izomorfizma olması için gerek ve yeter şart $\text{Çek}(f) = \{ e \}$ olmasıdır.

İspat: ($\Longrightarrow$) f bir izomorfizma olsun. O halde f birebirdir. $f(x) = e_0$ olsun. $f(e) = e_0$ olup f 1–1 olduğundan $x = e$ olmalıdır. O halde $f(x) = e_0$ olacak şekildeki tek eleman $x = e$ dir. Yani $\text{Çek}(f) = \{ e \}$ olur.

($\Longleftarrow$) Çek$(f) = \{\, e \,\}$ olsun. Her $x, y \in G$ için

$$\begin{aligned} f(x) = f(y) &\Longrightarrow f(x)f(y)^{-1} = e_0 \\ &\Longrightarrow f(xy^{-1}) = e_0 \\ &\Longrightarrow xy^{-1} \in \text{Çek}(f) = \{\, e \,\} \\ &\Longrightarrow xy^{-1} = e \\ &\Longrightarrow x = y \end{aligned}$$

olup f nin 1–1 olduğu, yani izomorfizma olduğu gösterilmiş olur. □

Teorem 4.21 G, H, K birer grup olsun.

(i) $f : G \longrightarrow H$ örten izomorfizma ise $f^{-1} : H \longrightarrow G$ de örten izomorfizmadır.

(ii) $f : G \longrightarrow H, g : H \longrightarrow K$ örten izomorfizma ise $g_\circ f : G \longrightarrow K$ örten izomorfizmadır.

İspat (i) Birebir ve örten bir dönüşümün tersi de 1–1 ve örten olacağından f^{-1} de 1–1 ve örtendir. O halde f^{-1} in homomorfizma olduğunu göstermemiz yeterlidir. $h_1, h_2 \in H$ olsun. f 1–1 ve örten olduğundan $f(g_1) = h_1, f(g_2) = h_2$ olacak şekilde sadece bir tane $g_1, g_2 \in G$ eleman çifti vardır. Şimdi

$$f(g_1g_2) = f(g_1)f(g_2) = h_1h_2 \Longrightarrow f^{-1}(h_1h_2) = g_1g_2 = f^{-1}(h_1)f^{-1}(h_2)$$

olup f^{-1} bir homomorfizmadır.

İspat (ii) Birebir ve örten iki dönüşümün bileşkesi 1–1 ve örten olacağından $g_\circ f$ 1–1 ve örtendir. O halde $g_\circ f$'nin bir homomorfizma olduğunu göstermemiz yeterlidir. $x, y \in G$ olsun.

$$\begin{aligned} (g_\circ f)(xy) &= g(f(xy)) \\ &= g(f(x)f(y)) \quad (f \text{ hom. olduğundan}) \\ &= g(f(x)) \cdot g(f(y)) \quad (g \text{ hom. olduğundan}) \\ &= (g_\circ f)(x) \cdot (g_\circ f)(y) \end{aligned}$$

olup $g_\circ f$ bir homomorfizmadır. O halde örten izomorfizmadır. □

Sonuç 4.22 G den G ye I birim dönüşümü örten bir izomorfizmadır. O halde her grup kendine izomorfiktir. Yukardaki teoremde $G \cong H \Longrightarrow H \cong G$ ve $G \cong H, H \cong K \Longrightarrow G \cong K$ olduğu gösterilmiştir. O halde gruplar üzerinde tanımlanan izomorfik olma bağıntısı bir denklik bağıntısıdır.

Teorem 4.23 İki devirli grubun izomorfik olması için gerek ve yeter şart bu iki grubun mertebelerinin aynı olmasıdır.

İspat: ($\Longrightarrow$) G ve H iki devirli grup olsun. $G \cong H$ ise $f : G \longrightarrow H$ homomorfizması 1–1 ve örten olduğundan $|G| = |H|$ olmalıdır. (Bu sonuç G ve H devirli olmasa da doğrudur.)

($\Longleftarrow$) Şimdi $G = \langle a \rangle, H = \langle b \rangle$ iki devirli grup ve $|G| = |H| = n$ olsun. $f : G \longrightarrow H$ dönüşümü her $k \in \mathbb{Z}$ için $f(a^k) = b^k$ şeklinde tanımlansın. f nin 1–1 ve örten bir homomorfizma olduğunu göstereceğiz.

$f(a^k) = f(a^t) \Longrightarrow b^k = b^t$ olup $n = \infty$ ise $k = t$ olup $a^k = a^t$ olur ve f birebir olur. Eğer $n < \infty$ ise $k \equiv t \pmod{n}$ olduğunu hatırlayın (bkz. Teorem 1.28). O halde $m, t \in \mathbb{Z}$ olmak üzere $k = t + mn$ dir. Şimdi

$$\begin{aligned} a^k &= a^{t+mn} \\ &= a^t a^{mn} = a^t (a^n)^m \\ &= a^t \end{aligned}$$

olup f bu durumda da birebirdir.

Şimdi $h \in H$ verilsin. Bir $k \in \mathbb{Z}$ için $h = b^k$ şeklindedir. O halde $f(a^k) = b^k = h$ olup f örtendir.

$x = a^k \in G$ ve $y = a^t \in G$ olsun.

$$f(xy) = f(a^k a^t) = f(a^{k+t}) = b^{k+t} = b^k b^t = f(a^k) f(a^t) = f(x) f(y)$$

olup f bir homomorfizmadır. Sonuç olarak $G \cong H$ dir. □

Tanım 4.24 Bir G grubundan kendi üzerine olan bir izomorfizmaya G nin bir ***otomorfizması*** denir. G nin bir $a \in G$ elemanı için $f_a : G \longrightarrow G$, $f_a(x) = axa^{-1}$ şeklinde tanımlanan f_a dönüşümü her zaman bir otomorfizmadır (Neden?). Bu tür bir otomorfizmaya G nin bir ***iç otomorfizması*** denir. G nin iç otomorfizmalarının kümesi $I(G)$ ile gösterilir. G nin bütün otomorfizmalarının kümesi $O(G)$ nin bileşke işlemi ile bir grup olduğunu göstereceğiz. Bu gruba G nin ***otomorfizmalar grubu*** denir. Yani

$$O(G) = \{\, f : G \longrightarrow G \mid f,\ \text{1–1, örten bir homomorfizma} \,\}.$$

Teorem 4.25 G nin otomorfizmalarını kümesi $O(G)$ bileşke işlemi ile bir gruptur.

İspat: Teorem 4.21 gereğince iki otomorfizmanın bileşkesi bir otomorfizmadır. Ayrıca $f \in O(G) \Longrightarrow f^{-1} \in O(G)$ dir. Birim dönüşüm bir otomorfizma olup $O(G)$ nin birim elemanıdır. Fonksiyonlardaki bileşke işleminin birleşme özelliği olup $O(G)$ bir grup olur. □

Örnek 4.26 $A = \{\, 1, -1, i, -i \,\}$ grubunun bütün otomorfizmalarını bulalım. I birim dönüşümü bir otomorfizmadır. $f \in O(G)$ olsun. $f(1) = 1$ olmak zorundadır. $f(i) = -1$ diyelim. O halde $f(ii) = f(i)f(i)$ yani $f(-1) = (-1)(-1) = 1$ olmalıdır. Bu da f nin 1–1 olmadığı anlamına gelir. Şimdi de

$f(i) = -i$ seçelim. Buradan

$$f(-1) = f(ii) = f(i)f(i) = (-i)(-i) = -1$$
$$f(-i) = f(-1)f(i) = (-1)(-i) = i$$

seçilmelidir. f 1–1 ve örten olup diğer bir otomorfizmadır. Bu grubun başka otomorfizması yoktur. O halde $O(A) = \{ I, f \}$ dir. Otomorfizma grubunun tablosu şöyledir:

$\circ$	I	f
I	I	f
f	f	I

Örnek 4.27 G bir grup olsun. Bir $a \in G$ için $f_a : G \longrightarrow G$, $f_a(x) = axa^{-1}$ şeklinde tanımlanan dönüşümün G nin bir otomorfizması olduğunu gösterin.

Çözüm: $x, y \in G$ olsun.

$$f_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = f_a(x)f_a(y)$$

olup f_a bir homomorfizmadır. Ayrıca

$$f_a(x) = f_a(y) \Longrightarrow axa^{-1} = aya^{-1} \Longrightarrow x = y$$

olup f_a birebirdir. Şimgi verilen her $g \in G$ için $x = a^{-1}ga$ seçersek

$$f_a(x) = axa^{-1} = a(a^{-1}ga)a^{-1} = g$$

olup f_a nın örten olduğu görülür. Yani $f_a \in O(G)$.

Teorem 4.28 $G = \langle a \rangle = \left\{ e, a, a^2, \ldots, a^{n-1} \right\}$ ise $f_k : G \longrightarrow G, f_k(a) = a^k$ olmak üzere

$$O(G) = \{ f_k \mid 1 \leqslant k < n, (k, n) = 1 \}.$$

İspat: $f \in O(G)$ olsun. $f(a) = a^k$ olsun. G nin üretici elemanları $1 \leqslant m < n$ ve $(m, n) = 1$ olmak üzere a^m şeklindedir. O halde $(n, k) = 1$ dir. Tersine $(k, n) = 1$ olmak üzere f_k dönüşümünü düşünelim. $f_k(a) = a^k$, G nin üretici elemanı olup f_k örtendir. Ayrıca f_k 1–1 bir homomorfizmadır. Yani $f_k \in O(G)$ dir. Sonuç: $O(G) = \{ f_k \mid 1 \leqslant k < n, (n, k) = 1 \}$. □

Örnek 4.29 $\mathbb{Z}_6$ nın otomorfizmalar grubunu belirleyiniz.
Çözüm:

$|\mathbb{Z}_6| = 6$. $O(\mathbb{Z}_6) = \{ f_k \mid 0 < k < 6, (k,6) = 1 \} = \{ f_1, f_5 \}$ dir.

$$f_1(0) = 1 \cdot 0 = 0 \qquad f_5(0) = 5 \cdot 0 = 0$$
$$f_1(1) = 1 \cdot 1 = 1 \qquad f_5(1) = 5 \cdot 1 = 5$$
$$f_1(2) = 1 \cdot 2 = 2 \qquad f_5(2) = 5 \cdot 2 = 4$$
$$f_1(3) = 1 \cdot 3 = 3 \qquad f_5(3) = 5 \cdot 3 = 3$$
$$f_1(4) = 1 \cdot 4 = 4 \qquad f_5(4) = 5 \cdot 4 = 2$$
$$f_1(5) = 1 \cdot 5 = 5 \qquad f_5(5) = 5 \cdot 5 = 1$$

Ödev: $\mathbb{Z}_{11}$ in otomorfizmalar grubunu belirleyiniz.

Örnek 4.30 G bir grup olsun. $|O(G)| = 1$ ise G nin bir abelyen grup olduğunu gösteriniz.
Çözüm:
$O(G) = \{ f \mid f : G \longrightarrow G$ otomorfizma $\}$. $|O(G)| = 1 \Longrightarrow G \longrightarrow G$ bir tek otomorfizma vardır, o da I_G dir. O zaman G nin eleman sayısı 1 veya 2 dir. Yani G abelyendir.

Teorem 4.31 C_n, n. mertebeden devirli grup ise $C_n \cong \mathbb{Z}_n$ dir. C_∞ sonsuz devirli grup ise $C_\infty \cong \mathbb{Z}$ dir.
İspat:
$C_n = \{ e, a, a^2, \ldots, a^{n-1} \}$ olsun. $f : C_n \longrightarrow \mathbb{Z}_n$ dönüşümünü $0 \leqslant k \leqslant n-1$ olmak üzere $f(a^k) = k$ olarak tanımlayalım.

Her $k \in \mathbb{Z}_n = \{ 0, 1, \ldots, n-1 \}$ için $f(a^k) = k$ olup f örtendir. ($a^0 = e$ kabul edildi.)

$f(a^k) = f(a^m) \Longrightarrow k = m \Longrightarrow a^k = a^m$ olup f 1–1 dir.

$f(a^k a^m) = f(a^t)$ [burada $t \equiv k + m \pmod n$] $= t = k + m \pmod n = f(a^k) + f(a^m)$
$\Longrightarrow f$ bir homomorfizmadır.
$\Longrightarrow f$ bir izomorfizma olup $C_n \cong \mathbb{Z}_n$ dir.

Şimdi $f : C_\infty \longrightarrow \mathbb{Z}$ dönüşümünü $f(a^k) = k$ şeklinde tanımlayalım.

$f(a^n a^m) = f(a^{n+m}) = n + m = f(a^n) + f(a^m)$ olup f bir homomorfizmadır.

$f(a^n) = f(a^m) \Longrightarrow C_\infty$ sonsuz devirli olduğundan $n = m$ dir.

C_∞ sonsuz devirli grup olduğundan her $n \in \mathbb{Z}$ için $a^n \in C_\infty$ ve $f(a^n) = n$ olup f örtendir. O halde $C_\infty \cong \mathbb{Z}$. □

Örnek 4.32 $\mathbb{Z}_8$'in otomorfizmalar grubu olan $O(\mathbb{Z}_8)$'i belirleyiniz.
Çözüm:

8 ile aralarında asal olan sayılar 1,3,5 ve 7 dir. O halde $O(\mathbb{Z}_8) = \{ f_1, f_3, f_5, f_7 \}$ dir. Mesela f_3 elemanını yazalım.

$$f_3(0) = 3 \cdot 0 = 0 \qquad f_3(4) = 3 \cdot 4 = 4$$
$$f_3(1) = 3 \cdot 1 = 3 \qquad f_3(5) = 3 \cdot 5 = 7$$
$$f_3(2) = 3 \cdot 2 = 6 \qquad f_3(6) = 3 \cdot 6 = 2$$
$$f_3(3) = 3 \cdot 3 = 1 \qquad f_3(7) = 3 \cdot 7 = 5$$

Örnek 4.33 G devirli ve mertebesi sonsuz olsun. Bu durumda G nin otomorfizmalar grubunu belirleyiniz.

Çözüm:

G devirli olduğundan bir $a \in G$ için $G = \langle a \rangle$ dır. $f : G \longrightarrow G$ bir $k \in \mathbb{Z}$ için $f(a) = a^k$ dır. f otomorfizma olduğundan örtendir. O halde $a \in G$ için öyle bir $b \in G$ vardır ki $f(b) = a$ olur. G devirli olduğundan bir $r \in \mathbb{Z}$ için $b = a^r$ olmalıdır.

$f(b) = f(a^r) = a \Longrightarrow (a^r)^k = a \Longrightarrow a^{rk} = a \Longrightarrow k = \mp 1$.

$k = 1$ olduğunda $f(a) = a \Longrightarrow f = I$,

$k = -1$ olduğunda $f(a) = a^{-1}$.

Yani $O(G) = \left\{ I, f \mid f(a) = a^{-1} \right\}$.

Örnek 4.34 $f : G \longrightarrow S$ bir grup homomorfizması ve Çek$(f) = \{ e \}$ olsun. Her $a \in G$ için a ile $f(a)$ nın derecelerinin aynı olduğunu gösteriniz.

Çözüm:

$|a| = m$ olsun. $[f(a)]^m = f(a^m) = f(e) = e_0$ olur. Acaba $[f(a)]^n = e_0$ olacak şekilde $n < m$ doğal sayısı var mıdır? Olduğunu kabul edelim $\Longrightarrow [f(a)]^n = f(a^n) = e_0$ olup Çek$(f) = \{ e \}$ olduğundan $a^n = e$ olur. Bu da $|a| = m$ olması ile çelişir. Buradan $|f(a)| = m$ elde edilir.

ALIŞTIRMALAR

1. $G = (\mathbb{Q} \setminus \{ 0 \}, \cdot)$ olsun. $f : G \longrightarrow G, f(x) = |x|$ şeklinde tanımlansın. f nin bir grup homomorfizması olduğunu gösterip Çek(f) yi bulunuz ve $G/$ Çek(f) yi yazınız.

2. $M^{2\times 2} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$ kümesi bilinen matris toplamı ile bir gruptur. $f : M^{2\times 2} \longrightarrow (\mathbb{R}, +)$ dönüşümü

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = a + d$$

şeklinde tanımlanıyor. f nin bir grup homomorfizması olduğunu gösterip Çek(f) yi bulunuz ve $M^{2\times 2}/$ Çek(f) yi yazınız.

3. $f : G \longrightarrow G$ dönüşümü her $a \in G$ için $f(a) = a^{-1}$ şeklinde tanımlansın. f nin bir grup homomorfizması olması için gerek ve yeter şart G nin abelyen olmasıdır. Gösterin.

4. $G = \langle x \rangle$ herhangibir devirli grup olsun. $f : G \longrightarrow (\mathbb{Z}, +)$ dönüşümü $f(x^n) = n$ şeklinde tanımlansın. f bir homomorfizma olur mu? Eğer olursa Çek(f) yi yazınız.

5. $\phi : \mathbb{C} \longrightarrow \mathbb{C}, \phi(x + iy) = x - iy$ dönüşümü toplamsal $\mathbb{C}$ grubunun bir otomorfizmasıdır. Gösteriniz.

6. $f : G \longrightarrow H$ örten bir izomorfizma olsun. $N \lhd G$ ise $f(N) \lhd H$ olduğunu gösteriniz.

7. $G = \mathbb{C} \setminus \{0\}$ çarpma işlemi ile bir gruptur. $H = \{\, 2 \times 2$ tersi olan reel matrisler $\}$ de bilinen matris çarpımı ile bir gruptur. $\phi : G \longrightarrow H, \phi(a + ib) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ ile tanımlanan dönüşüm bir grup homomorfizması mıdır? Bu dönüşüm G ile H yi izomorfik yapar mı?

8. $f : G \longrightarrow H$ bir grup homomorfizması olsun. $K \lhd H$ ise $f^{-1}(K) \lhd G$ olduğunu gösterin.

9. $G = (\mathbb{C} \setminus \{\, 0 \,\}, \cdot)$ ve $H = (\mathbb{R}^+, \cdot)$ olsun. $z = x + iy$ için $\phi : G \longrightarrow H, \phi(z) = |z| = \sqrt{x^2 + y^2}$ olarak tanımlanan dönüşüm bir homomorfizma mıdır? G ile H yi izomorfik yapar mı?

10. $\mathbb{R}^\star = \mathbb{R} \setminus \{0\}$ olmak üzere $f : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^\star, \cdot), f(x) = 5^x$ olsun. f nin grup homomorfizması olduğunu gösteriniz. Çek(f) yi bulunuz. f 1–1 ve örten midir? $\mathbb{R}/$ Çek(f) yi yazınız.

ALIŞTIRMALARIN ÇÖZÜMLERİ

ÇÖZÜM 1. $x, y \in G$ için

$$f(xy) = |xy| = |x|\ |y| = f(x)f(y)$$

olup f bir homomorfizmadır.

$$\text{Çek}(f) = \{\, x \in G : f(x) = |x| = 1 \,\} = \{\, 1, -1 \,\}$$

olup

$$G/\,\text{Çek}(f) = \{\, \text{Çek}(f) \cdot x : x \in G \,\} = \{\, \{\, x, -x \,\} : x \in G \,\} \text{ dir.}$$