

SOYUT CEBİR

DERS NOTLARI

Yrd. Doç. Dr. Hüseyin BİLGİÇ

Kahramanmaraş Sütçü İmam Üniversitesi Fen-Edebiyat Fakültesi

Matematik Bölümü

Mart 2013

e-posta: h_bilgic@yahoo.com

İçindekiler

1	Grup Tanımı ve Temel Özellikler	1
2	Altgruplar, Kosetler ve Lagrange Teoremi	15
3	Normal Altgruplar ve Faktör Grupları	29
4	Homomorfizmalar ve İzomorfizmalar	39
5	İzomorfizma Teoremleri	55
6	Permütasyon Grupları	67
6.1	$n \geq 5$ İçin A_n Basit Gruptur	74
7	Halka ve Cisim	79
8	İdealler ve Bölüm Halkaları	98
8.1	İdealler	98
8.2	Bölüm Halkaları	102

Grup Tanımı ve Temel Özellikler

Tanım 1.1 G boş olmayan bir küme ve $\cdot$ (nokta) da G üzerinde tanımlı bir ikili işlem olsun. Eğer aşağıdaki şartlar sağlanıyorsa $(G, \cdot)$ cebirsel yapısına 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 genelde $b = a^{-1}$ 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 **Abelyen¹ (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. Bilinen $+$ işlemine göre grup olan ve sonlu olan tek küme $\{0\}$ kümesidir. Bilinen çarpma işlemine göre: $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$ birer abelyen gruptur. Aynı işleme göre $\{1\}, \{1, -1\}$ kümeleri de gruptur. $(\mathbb{Z}, \cdot)$ bir grup değildir, çünkü $2^{-1} \notin \mathbb{Z}$.

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

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

$\cdot$	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 (determinantı sıfır olmayan) 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) $I_M : M \rightarrow M$ birim dönüşümü $P(M)$ in birim elemanıdır: $\forall f \in P(M), f \circ I_M = I_M \circ f = f$.

(iv) $f \in P(M)$ ise f birebir ve örten olup f^{-1} bağıntısı da 1-1 ve örten bir fonksiyondur. $f \circ f^{-1} = f^{-1} \circ f = I_M$.

Tanım 1.8 n pozitif bir tamsayı olsun. $a, b \in \mathbb{Z}$ için

$$a \equiv b \pmod{n} \iff n \mid (a - b)$$

şekline tanımlanan “ $\equiv \pmod{n}$ ” bağıntısı bir denklik bağıntısıdır. Bu bağıntıya göre olan denklik sınıflarına ***modülo n kalan sınıfları*** denir ve $\mathbb{Z}_n$ ile gösterilir. Bir $n > 0$ tamsayısına göre kalanlar $0, 1, \dots, n-1$ sayılarından birisi olacağından $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ olduğu görülmektedir. $\mathbb{Z}_n$ kümesinde $\oplus$ ve $\odot$ işlemleri

$$\bar{a} \oplus \bar{b} = \overline{a + b} \quad \text{ve} \quad \bar{a} \odot \bar{b} = \overline{a \cdot b}$$

şeklinde tanımlanır. Bu işlemlerin $\bar{a}$ ve $\bar{b}$ temsilci sınıflarından alınan temsilcilere bağlı olmadığı; yani bu işlemlerin iyi tanımlandığı kolaylıkla gösterilebilir. Mesela $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ kümesinde

$$\bar{2} \oplus \bar{5} = \overline{2 + 5} = \bar{7} = \bar{1} \text{ veya } \bar{2} \oplus \bar{5} = \bar{8} \oplus \overline{-7} = \overline{8 - 7} = \bar{1}.$$

Şimdi; $(\mathbb{Z}_n, \oplus)$ bir gruptur fakat; $n \geq 2$ ise $(\mathbb{Z}_n, \odot)$ bir grup değildir. $(\mathbb{Z}_n, \oplus)$ grubuna *modülo n kalan sınıfları grubu* denir ve (işlem adı yazılmadan) kısaca $\mathbb{Z}_n$ ile gösterilebilir.

Örnek 1.9 $(\mathbb{Z}_6, \oplus)$ ve $(\mathbb{Z}_6, \odot)$ sistemlerinin tablosunu yapalım.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Temel Özellikler

Teorem 1.10 $(G, \cdot)$ herhangi bir 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 1.11 Teoremden (iii) ve (iv) de ifade edilen özellikler toplamsal notasyonda sırasıyla $-(-a) = a$ ve $-(a + b) = (-b) + (-a)$ şeklini alır.

Not 1.12 Bundan sonra grup işlemi söylenmemişse $\cdot$ kabul edilecek ve grup işlemi $\cdot$ ise kısalık açısından $a \cdot b$ yerine ab yazılacaktır.

Lemma 1.13 Bir G grubunda soldan ve sağdan kısaltma kuralları vardır. Ayrıca $a, b \in G$ ise G 'de $ax = b$ ve $ya = b$ denklemini sağlayan sadece bir tane x ve y vardır.

İspat: Her $a, b, c \in G$ için:

$$\begin{aligned} ab = ac &\implies a^{-1}(ab) = a^{-1}(ac) \implies (a^{-1}a)b = (a^{-1}a)c \implies b = c, \\ ba = ca &\implies (ba)a^{-1} = (ca)a^{-1} \implies b(aa^{-1}) = c(aa^{-1}) \implies b = c \end{aligned}$$

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 $ax_1 = ax_2$ olup soldan kısaltma kuralı gereğince $x_1 = x_2$ elde edilir. Benzer şekilde $ya = b$ denkleminin çözümü de tektir. $\square$

Not 1.14 Bu Lemma'nın bir sonucu olarak, grup tablosunda bir elemanın bir satırda veya bir sütunda sadece bir defa yer alacağını söyleyebiliriz. (Neden?)

Tanım 1.15 Bir G grubunun elemanlarının sayısına (eğer G sonlu ise) G nin *mertebesi* denir ve $|G|$ ile gösterilir. Eğer G sonsuz bir küme ise $|G| = \infty$ yazılır.

Örnek 1.16 $M = \{a, b, c\}$ olsun. $P(M)$ 'in bileşke işlemi ile bir grup olduğunu biliyoruz. Bu gruba S_3 diyelim. $|S_3| = 6$ dır. S_3 ün elemanları:

$$\begin{array}{cccccc} a \longrightarrow a & a \longrightarrow a & a \longrightarrow b & a \longrightarrow b & a \longrightarrow c & a \longrightarrow c \\ f_1 : b \longrightarrow b, & f_2 : b \longrightarrow c, & f_3 : b \longrightarrow a, & f_4 : b \longrightarrow c, & f_5 : b \longrightarrow a, & f_6 : b \longrightarrow b. \\ c \longrightarrow c & c \longrightarrow b & c \longrightarrow c & c \longrightarrow a & c \longrightarrow b & c \longrightarrow a \end{array}$$

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 1.17 G bir grup ve $a \in G$ olsun.

- (i) $a^0 = e$ olarak tanımlanır.
- (ii) $1 \leq n \in \mathbb{N}$ için $a^n = \underbrace{a \cdot a \cdots a}_{n\text{-tane}}$
- (iii) $1 \leq n \in \mathbb{N}$ için $a^{-n} = (a^{-1})^n$

Not 1.18 Toplamsal notasyonda aynı tanımlar, sırasıyla, $0 \cdot a = e$, $n \cdot a = a + a + \cdots + a$ ve $(-n) \cdot a = (-a) + (-a) + \cdots + (-a)$ şeklinde yazılabilir. Ayrıca, $a^{-n} = (a^n)^{-1}$ olduğu gösterilebilir:

$$(a^n)^{-1} = (a \cdot a \cdots a)^{-1} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n\text{-tane}} = (a^{-1})^n = a^{-n}$$

Teorem 1.19 G bir grup, $a, b \in G$ 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): $a^n a^m = (\underbrace{a \cdots a}_{n\text{-tane}})(\underbrace{a \cdots a}_{m\text{-tane}}) = \underbrace{a \cdots a}_{n+m\text{-tane}} = a^{n+m}.$

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

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

Not 1.20 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 1.21 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 1.22 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 1.23 $(\mathbb{Z}, +)$ 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.

Devirli Gruplar

Tanım 1.24 G bir grup, $a \in G$ olsun. $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ kümesine a *tarafından üretilen (doğru-rulan) 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.

Örnek 1.25 $A = \{1, -1, i, -i\}$ 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 1.26 $(\mathbb{Z}, +)$ grubunda $\langle 5 \rangle = \{5n : n \in \mathbb{Z}\} = \{\dots, -10, -5, 0, 5, 10, \dots\} = 5\mathbb{Z}$ dir. $\mathbb{Z}$ devirlidir, çünkü $\langle -1 \rangle = \langle 1 \rangle = \mathbb{Z}$ dir. $(\mathbb{Z}_n, \oplus)$ grupları devirlidir çünkü her zaman $\bar{1}$ tarafından üretilir. Mesela $\mathbb{Z}_6$ 'da:

$$\langle \bar{1} \rangle = \langle \bar{5} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \mathbb{Z}_6.$$

Örnek 1.27 S_3 devirli değildir, çünkü hiçbir elemanı tarafından üretilemez: S_3 'de

$$\langle f_1 \rangle = \{f_1\}, \langle f_2 \rangle = \{f_1, f_2\}, \langle f_3 \rangle = \{f_1, f_3\}, \langle f_4 \rangle = \langle f_5 \rangle = \{f_1, f_4, f_5\}, \langle f_6 \rangle = \{f_1, f_6\}.$$

S_3 'ün devirli olmamasının sebebi derecesi 6 olan bir eleman olmamasıdır.

Sonuç 1.28 Bir G sonlu grubunun devirli olması için gerek ve yeter şart $|G| = |a|$ olacak şekilde en az bir $a \in G$ elemanının olmasıdır.

Not 1.29 Bir grupta $|a| = \infty$ ise

$$\langle a \rangle = \{\dots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots\}$$

şeklinde yazılır. Fakat eğer $|a| = n$ sonlu ise a nın negatif bir kuvveti pozitif bir kuvvetine eşit olacağından

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$$

şeklinde yazılabilir.

Teorem 1.30 (Bölme Algoritması) a ve b iki tamsayı, $b \neq 0$ olsun. Bu iki sayı çifti için

$$a = bq + r, \quad 0 \leq r < |b|$$

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

Teorem 1.31 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 $p - q = nk_1 + k_2$, $0 \leq k_2 < n$ olacak şekilde $k_1, k_2 \in \mathbb{Z}$ vardır.

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

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

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

Not 1.32 $|a| = n < \infty$ olsun.

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

Teorem 1.33 $G = \langle a \rangle$ ve $|a| = \infty$ olsun. G grubu sadece a ve a^{-1} tarafından üretilir.

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

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

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, $a^n = a^{mx} \implies n = mx$ 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. $\square$

Çarpımsal Notasyon	Toplamsal Notasyon
$a \cdot b$ veya ab	$a + b$
$a^n = a \cdot a \cdots a$	$na = a + a + \cdots + a$
$a_1 a_2 \cdots a_n = \prod_{i=1}^n a_i$	$a_1 + a_2 + \cdots + a_n = \sum_{i=1}^n a_i$
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

ALİŞTIRMALAR

1. $\mathbb{Q}^+$ pozitif rasyonel sayılar kümesi üzerinde $x \star y = \frac{xy}{2}$ 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. $(G, \star)$ in 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. $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$ grubu devirli midir? Üretici elemanlarını bulunuz.
8. $(\mathbb{Q}, +)$ grubunun devirli olmadığını gösteriniz.
9. $(\mathbb{Z}, +)$ grubunda 6 elemanın ürettiği grubu bulunuz.
10. $(\mathbb{Q} \setminus \{0\}, \cdot)$ grubunda $\frac{1}{4}$ elemanın 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 $1 \leq m$ 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.

18. $a, b \in G$ ve $|a| = 5$ olsun. $a^3b = ba^3 \implies ab = ba$ olduğunu gösterin.

ALİŞTIRMALARIN ÇÖZÜMLERİ

ÇÖZÜM 1.

(i) Her $x, y \in \mathbb{Q}^+$ için $x \star y = \frac{xy}{2} \in \mathbb{Q}^+$ olup $\star$ işlemi kapalıdır.

(ii) Her $x, y, z \in \mathbb{Q}^+$ için

$$(x \star y) \star z = \frac{xy}{2} \star z = \frac{xyz}{4} = \frac{x}{2} \frac{yz}{2} = \frac{x}{2} (y \star z) = x \star (y \star z)$$

olup $\star$ işlemi birleşme özelliğine sahiptir.

(iii)

$$\begin{aligned} x \star e = x &\implies \frac{xe}{2} = x \implies e = 2 \text{ olabilir} \\ 2 \star x &= \frac{2x}{2} = x \end{aligned}$$

olup $e = 2$ birim elemandır.

(iv)

$$\begin{aligned} x \star y = 2 &\implies \frac{xy}{2} = 2 \implies y = \frac{4}{x} \text{ olabilir} \\ \frac{4}{x} \star x &= \frac{\frac{4}{x}x}{2} = 2 \end{aligned}$$

olup x in tersi $x^{-1} = \frac{4}{x}$ dir.

ÇÖZÜM 2.

(i) $k_1, k_2 \in \mathbb{Z}$ olsun. $nk_1, nk_2 \in G \implies nk_1 + nk_2 = n(\underbrace{k_1 + k_2}_{\in \mathbb{Z}}) \in G$ olup işlem kapalıdır.

(ii) $nk_1 + (nk_2 + nk_3) = n(k_1 + (k_2 + k_3)) = n((k_1 + k_2) + k_3) = (nk_1 + nk_2) + nk_3$ olup birleşme özelliği vardır.

(iii) $0 = n \cdot 0$ olup $0 \in G$ birim elemandır: $0 + nk = nk + 0 = nk$.

(iv) nk nın tersi $-(nk) = n(-k) = -nk \in G$ dir. $nk + (-nk) = (-nk) + nk = 0$.

(v) $nk_1 + nk_2 = n(k_1 + k_2) = n(k_2 + k_1) = nk_2 + nk_1$ olup değişme özelliği vardır.

ÇÖZÜM 3.

$\cap$	$\emptyset$	A	B	C	$\cup$	$\emptyset$	A	B	C
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	A	B	C
A	$\emptyset$	A	B	C	A	A	A	A	A
B	$\emptyset$	B	B	C	B	B	A	B	B
C	$\emptyset$	C	C	C	C	C	A	B	C

Tablolardan her iki işlemin de kapalılık özelliği vardır. Kesişme ve birleşme işlemleri her zaman değişme ve birleşme özelliğine sahiptir. Tablodan anlaşıldığı gibi $\cap$ ve $\cup$ işlemlerinin birim elemanları sırasıyla A ve $\emptyset$ dir. Fakat her iki işlemde de ters eleman özelliği yoktur, mesela $B \in G$ için

$$B \cap X = A \text{ olacak şekilde } X \in G \text{ yoktur,}$$

$$B \cup X = \emptyset \text{ olacak şekilde } X \in G \text{ yoktur.}$$

Dolayısıyla her iki sistem de grup değildir.

ÇÖZÜM 4.

(i) $a_i, b_i \in \mathbb{R}$ olmak üzere $A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}, B = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \in M^{2 \times 2}$ olsun. $a_i + b_i \in \mathbb{R}$ olup $A + B = \begin{bmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{bmatrix} \in M^{2 \times 2}$ dir.

(ii) $C = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} \in M^{2 \times 2}$ olsun. $a_i + (b_i + c_i) = (a_i + b_i) + c_i$ olduğundan $A + (B + C) = (A + B) + C$ olur.

(iii) $0 \in \mathbb{R}$ olduğundan $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in G$ olup bu matris birim elemandır:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

(iv) $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ matrisinin tersi $-A = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$ matrisidir:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

ÇÖZÜM 5.

(i) $a, b \in G = \mathbb{R} \setminus \{-1\}$ ise $a \star b = ab + a + b \in G$ olur, çünkü

$$ab + a + b = -1 \iff ab + a + b + 1 = 0 \iff (a + 1)(b + 1) = 0 \iff a = -1 \text{ veya } b = -1.$$

Yani $\star$ işlemi kapalıdır.

(ii)

$$\begin{aligned} a \star (b \star c) &= a \star (bc + b + c) = abc + ab + ac + a + bc + b + c, \\ (a \star b) \star c &= (ab + a + b) \star c = abc + ac + bc + ab + a + b + c \end{aligned}$$

olup $a \star (b \star c) = (a \star b) \star c$ olduğu görülür. Yani birleşme özelliği vardır.

(iii) Her $a \in G$ için

$$\begin{aligned} a \star e &= ae + a + e = a \implies ae + a = e(1 + a) = 0 \implies e = 0 \text{ olabilir.} \\ 0 \star a &= 0a + 0 + a = a \end{aligned}$$

olup $e = 0$ birim elemandır.

(iv) Her $a \in G$ için

$$\begin{aligned} a \star b &= ab + a + b = 0 \implies b = -\frac{a}{a+1} \text{ ters eleman olabilir.} \\ \left(\frac{-a}{a+1}\right) \star a &= \frac{-a^2}{a+1} + \frac{-a}{a+1} + \frac{a(a+1)}{a+1} = 0 \end{aligned}$$

olup $a^{-1} = -\frac{a}{a+1}$ elde edilir. $-a/(a+1) = -1$ olsaydı $0 = -1$ çelişkisi elde edilirdi; yani her $a \in G$ için $a^{-1} \in G$ dir.

(v) Şimdi de $2 \star x \star 3 = 5$ denklemini çözelim.

$$\begin{aligned} 2 \star x \star 3 &= 5 \implies 2 \star x = 5 \star 3^{-1} = 5 \star \frac{-3}{4} = \frac{-15}{4} + 5 + \frac{-3}{4} = \frac{1}{2} \\ \implies 2 \star x &= \frac{1}{2} \\ \implies x &= 2^{-1} \star \frac{1}{2} = \frac{-2}{3} \star \frac{1}{2} = \frac{-2}{6} + \frac{-2}{3} + \frac{1}{2} \\ \implies x &= -\frac{1}{2} \end{aligned}$$

ÇÖZÜM 6.

(i) $a, b, c, d \in \mathbb{Z}$ ise $(a, b) \circ (c, d) = (a + c, (-1)^c b + d) \in G$ dir çünkü $a + c \in \mathbb{Z}, (-1)^c b + d \in \mathbb{Z}$ dir.

(ii) $(a, b), (c, d), (e, f) \in G$ olsun.

$$\begin{aligned} [(a, b) \circ (c, d)] \circ (e, f) &= (a + c, (-1)^c b + d) \circ (e, f) = (a + c + e, (-1)^e((-1)^c b + d) + f) \\ &= (a + c + e, (-1)^{e+c} b + (-1)^e d + f). \end{aligned}$$

Ayrıca

$$\begin{aligned}(a, b) \circ [(c, d) \circ (e, f)] &= (a, b) \circ (c + e, (-1)^e d + f) \\ &= (a + c + e, (-1)^{c+e} b + (-1)^e d + f)\end{aligned}$$

olup birleşme özelliğinin olduğu görülür.

(iii) Birim eleman $(0, 0) \in G$ dir çünkü $0 \in \mathbb{Z}$ ve

$$\begin{aligned}(a, b) \circ (0, 0) &= (a + 0, (-1)^0 b + 0) = (a, b), \\ (0, 0) \circ (a, b) &= (0 + a, (-1)^a 0 + b) = (a, b).\end{aligned}$$

(iv) $(a, b) \circ (x, y) = (0, 0) \implies (a + x, (-1)^x b + y) = (0, 0)$ olup buradan $a + x = 0$ ve $(-1)^x b + y = 0$ bulunur. Bu denklemler çözülürse $x = -a$ ve $y = \frac{-b}{(-1)^a}$ bulunur. Ayrıca

$$\left(-a, \frac{-b}{(-1)^a}\right) \circ (a, b) = \left(-a + a, (-1)^a \frac{-b}{(-1)^a} + b\right) = (0, 0)$$

olup $(a, b)^{-1} = \left(-a, -\frac{b}{(-1)^a}\right)$ dir.

(v) Değişme özelliği yoktur, çünkü

$$\begin{aligned}(1, 1) \circ (1, 2) &= (2, (-1)^1 \cdot 1 + 2) = (2, 1), \text{ fakat} \\ (1, 2) \circ (1, 1) &= (2, (-1)^1 \cdot 2 + 1) = (2, -1).\end{aligned}$$

Dolayısıyla Abelyen grup değildir.

ÇÖZÜM 7. $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$ devirlidir, çünkü

$$\langle \bar{1} \rangle = \langle \bar{3} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\} = \mathbb{Z}_8.$$

ÇÖZÜM 8. Bir an için $(\mathbb{Q}, +)$ nın devirli olduğunu kabul edelim. O halde $\mathbb{Q} = \langle q \rangle$ olacak şekilde bir $q \in \mathbb{Q}$ vardır. Yani her $t \in \mathbb{Q}$ için $t = nq$ olacak şekilde bir $n \in \mathbb{Z}$ mevcuttur. $a, b \in \mathbb{Z}$ ve $b \neq 0$ olmak üzere $q = \frac{a}{b}$ şeklinde yazılabilir. Şimdi $t = \frac{1}{2b} \in \mathbb{Q}$ olup $t = nq$ olacak şekilde $n \in \mathbb{Z}$ vardır. O halde

$$\frac{1}{2b} = nq = n \frac{a}{b} \implies 1 = 2na$$

elde edilir. $n, a \in \mathbb{Z}$ olduğundan bu bir çelişkidir. O halde $(\mathbb{Q}, +)$ devirli değildir.

ÇÖZÜM 9. $(\mathbb{Z}, +)$ grubunda $\langle 6 \rangle = \{6k : k \in \mathbb{Z}\} = \{\dots, -18, -12, -6, 0, 6, 12, 18, \dots\} = 6\mathbb{Z}$ dir.

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

$$\left\langle \frac{1}{4} \right\rangle = \left\{ \left(\frac{1}{4} \right)^n : n \in \mathbb{Z} \right\} = \left\{ \dots, \frac{1}{64}, \frac{1}{16}, \frac{1}{4}, 1, 4, 16, 64, \dots \right\}.$$

ÇÖZÜM 11. $x^n = e \implies x^{n-1} = x^{-1}$ olup $m = n - 1$ dersek $m \geq 1$ olur ve $x^m = x^{-1}$ dir.

ÇÖZÜM 12. G sonlu olsun. $x^n = e$ olacak şekilde bir n pozitif tamsayısı olmasın. O halde $A = \{x, x^2, x^3, \dots\}$ kümesindeki elemanların hepsi G nin elemanlarıdır. Ayrıca bu elemanlar birbirinden farklıdır; çünkü en az bir $i \neq j, i > j$ için $x^i = x^j$ olsaydı $x^{i-j} = e$ olurdu. Bu da kabulümüzle çelişirdi çünkü $i - j \in \mathbb{Z}^+$. O halde A sonsuzdur. Şimdi de A sonsuz kümesi G sonlu kümesinin alt kümesi olamaz. O halde $x^n = e$ olacak şekilde en az bir $n \in \mathbb{Z}^+$ vardır.

ÇÖZÜM 13. Her $a, b \in G$ için

$$\begin{aligned} (ab)^2 &= a^2b^2 \implies abab = aabb \\ &\implies bab = abb \quad (\text{soldan } a \text{ kısalır}) \\ &\implies ba = ab \quad (\text{sağdan } b \text{ kısalır}) \end{aligned}$$

olup G abelyendir.

ÇÖZÜM 14. $|a| = n$ olsun. $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$ dir. Fakat bu $|a^{-1}| = n$ anlamına gelmez. Şimdi $1 \leq k < n$ olsun.

$$(a^{-1})^k = e \implies (a^k)^{-1} = e \implies a^k = e^{-1} = e$$

olup bu durum $|a| = n$ olmasıyla çelişir. O halde $|a^{-1}| = n$ dir.

Şimdi,

$$(bab^{-1})^n = \underbrace{(bab^{-1})(bab^{-1}) \cdots (bab^{-1})}_{n\text{-tane}} = ba^n b^{-1} = beb^{-1} = e$$

olur. Şimdi $1 \leq k < n$ olsun.

$$(bab^{-1})^k = e \implies ba^k b^{-1} = e \implies ba^k = b \implies a^k = e$$

olup bu durum $|a| = n$ olmasıyla çelişir. O halde $|bab^{-1}| = n$ dir.

ÇÖZÜM 15. $G = \{e, a_1, a_2, \dots, a_n\}$ olsun. $|G| = n+1$ çift olsun. $f : G \rightarrow G, f(x) = x^{-1}$ dönüşümü 1-1 ve örtendir, çünkü

$$\begin{aligned} f(x) = f(y) &\implies x^{-1} = y^{-1} \implies x = y, \\ y \in G &\implies x = y^{-1} \text{ seçilirse } f(x) = f(y^{-1}) = y \text{ olur.} \end{aligned}$$

Şimdi $f(e) = e$ olduğu aşıkardır. Biz $f(a_i) = a_i$ olacak şekilde $a_i \in G$ olacağını göstereceğiz. $G \setminus \{e\}$ kümesinde $f(x) = y \iff f(y) = x$ olduğundan tersi kendine eşit olmayan elemanlar f altında eşlendiğinde geriye tek tane eleman kalacağı aşıkardır, çünkü $G \setminus \{e\}$ kümesi tek elemanlıdır. Bu da tersi kendine eşlenecek en az bir tane eleman olduğu anlamına gelir. Yani, en az bir i için $f(a_i) = a_i$ olup $(a_i)^{-1} = a_i \implies (a_i)^2 = e$ dir.

ÇÖZÜM 16. Bir G grubunda her $x \in G$ için $x^2 = e$ ise $x = x^{-1}$ dir, yani her elemanın tersi kendisidir. O halde her $a, b \in G$ için $(ab)^2 = e$ olmalıdır. Burada $a^{-1} = a, b^{-1} = b$ olduğu unutulmamalıdır. O halde

$$(ab)^2 = e \implies abab = e \implies aba = b^{-1} \implies ab = b^{-1}a^{-1} = ba$$

olup G nin abelyen olduğu görülür.

ÇÖZÜM 17. Bağıntının yansıyan, simetrik ve geçişken olduğunu göstereceğiz.

(i) Her $a \in G$ için $e^{-1}ae = a$ olup a ile a eşleniktir. Yani bağıntı yansıyandır.

(ii)

$$\begin{aligned} a \text{ ile } b \text{ eşlenik} &\implies \exists x \in G, x^{-1}ax = b \implies ax = xb \\ &\implies xbx^{-1} = a \\ &\implies y = x^{-1} \text{ dersek } y^{-1}by = a \\ &\implies b \text{ ile } a \text{ eşlenik.} \end{aligned}$$

$y = x^{-1} \in G$ olup bağıntımız simetriktir.

(iii)

$$\begin{aligned} a \text{ ile } b \text{ eşlenik} &\implies \exists x \in G, x^{-1}ax = b, \\ b \text{ ile } c \text{ eşlenik} &\implies \exists y \in G, y^{-1}by = c \\ &\implies y^{-1}(x^{-1}ax)y = c \\ &\implies (xy)^{-1}a(xy) = c \\ &\implies z = (xy) \text{ dersek } z^{-1}az = c \\ &\implies a \text{ ile } c \text{ eşlenik.} \end{aligned}$$

$z = xy \in G$ olup bağıntımız geçişkendir.

ÇÖZÜM 18.

$$\begin{aligned} a^3b = ba^3 &\implies a^3(a^3b) = a^3ba^3 \\ &\implies ab = \underbrace{a^3b}_{ba^3} a^3 \\ &\implies ab = ba^3a^3 = ba^6 = ba \end{aligned}$$

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 $H \leq G$ 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 $B \leq A$ yazılabilir.

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

Örnek 2.4 $a \in \mathbb{Z}$ sabit bir tamsayı olmak üzere $(a\mathbb{Z}, +)$ grubu $(\mathbb{Z}, +)$ grubunun alt grubudur.

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 (aşıkâr) 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 sonlu ve kapalı bir altküme olduğunu kabul edelim. G 'de birleşme özelliği olduğundan U da birleşmelidir. $U = \{a_1, a_2, \dots, a_n\}$, n elemanlı bir altküme olsun. $a_k \in U$ olsun. Şimdi

$$a_1 a_k, a_2 a_k, \dots, a_n a_k$$

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 $U = \{a_1 a_k, a_2 a_k, \dots, a_n a_k\}$ dir. $a_k \in U$ olup en az bir $1 \leq i \leq n$ için $a_k = a_i a_k$ olmalıdır. Yani $a_i = e$ olur ve $e \in U$ dur. Şimdi de, en az bir $1 \leq j \leq n$ 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. $\square$

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 $U = \{1, 2, 3, \dots\}$ kümesi kapalıdır fakat bir altgrup değildir.

Örnek 2.10 $G = GL_2(\mathbb{R})$, 2×2 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 $ab \neq 0, cd \neq 0$ dir.

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

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

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

İspat: $H_1, H_2, \dots, H_n, G$ nin altgrupları olsun ve $H = H_1 \cap H_2 \cap \dots \cap H_n = \bigcap_{i=1}^n H_i$ diyelim.

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

olup Teorem 2.8 gereğince H bir altgruptur. $\square$

Not 2.12 Benzer şekilde; sonsuz çokluktaki altgrupların kesişiminin de bir altgrup olduğu gösterilebilir. Altgrupların birleşimi altgrup olmayabilir; mesela, $(\mathbb{Z}, +)$ 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) $H^{-1} = \{h^{-1} : h \in H\}$ 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. $\square$

Teorem 2.16 Bir devirli grubun her altgrubu devirlidir. $G = \langle a \rangle$ mertebesi n olan bir devirli grup ise G 'nin altgruplarının sayısı n 'nin pozitif bölenleri kadardır. 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 2.17 $G = \langle a \rangle$ 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 olup G 'nin 8 tane altgrubu vardır. Buna göre G nin n -elemanlı altgrubunu C_n ile gösterirsek bu altgruplar şunlardır:

$$C_1 = \langle a^{24/1} \rangle = \langle e \rangle = \{e\}$$

$$C_2 = \langle a^{24/2} \rangle = \langle a^{12} \rangle = \{e, a^{12}\}$$

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

Tanım 2.18 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

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

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.

Örnek 2.19 $\mathbb{Z}_{12} = \{ \bar{0}, \bar{1}, \bar{2}, \dots, \bar{11} \}$ grubunda bazı kümeler tarafından üretilen altgruplar sorulmaktadır. Bunun için $\mathbb{Z}_{12}$ 'nin bütün altgrupları hesaplanmalıdır. $\mathbb{Z}_{12}$ devirli olduğundan, bir önceki teoreme göre, bu altgruplar 6 tanedir:

$$H_1 = \{ \bar{0} \}, H_2 = \{ \bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10} \}, H_3 = \{ \bar{0}, \bar{3}, \bar{6}, \bar{9} \}, H_4 = \{ \bar{0}, \bar{4}, \bar{8} \}, H_5 = \{ \bar{0}, \bar{6} \} \text{ ve } H_6 = \mathbb{Z}_{12}.$$

Buna göre K kümeleri ve $\langle K \rangle$ altgrupları şöyle hesaplanır.

$$\begin{aligned}
K &= \{ \bar{6}, \bar{8} \} \implies \langle K \rangle = H_2 \\
K &= \{ \bar{4}, \bar{8} \} \implies \langle K \rangle = H_2 \cap H_4 = H_4 \\
K &= \{ \bar{6} \} \implies \langle K \rangle = H_2 \cap H_3 \cap H_5 = H_5 \\
K &= \{ \bar{3}, \bar{5} \} \implies \langle K \rangle = \mathbb{Z}_{12}.
\end{aligned}$$

Lemma 2.20 G bir grup, $\emptyset \neq K \subseteq G$ olsun. $\langle K \rangle$ altgrubu K daki elemanların tamsayı kuvvetlerinin bütün muhtemel çarpımlarından oluşan kümedir; yani

$$\langle K \rangle = \{ k_1^{a_1} k_2^{a_2} \dots k_n^{a_n} : k_i \in K, a_i \in \mathbb{Z}, n \in \mathbb{N} \}.$$

İspat: $U = \{ k_1^{a_1} k_2^{a_2} \dots k_n^{a_n} : k_i \in K, a_i \in \mathbb{Z}, n \in \mathbb{N} \}$ diyelim ve $U = \langle K \rangle$ olduğunu gösterelim. $u \in U$ alalım. O halde u, K 'daki elemanların çarpımı şeklindedir. K 'yı içeren her H altgrubu K 'daki elemanların çarpımlarını da içereceğinden $u \in H$ olmalıdır. $\langle K \rangle$ ise K 'yı içeren altgrupların kesişimi olduğundan $u \in \langle K \rangle$ olur. Yani $U \subseteq \langle K \rangle$ dir. Şimdi de $x, y \in U$ alalım. O halde

$$x = k_1^{a_1} k_2^{a_2} \dots k_n^{a_n} \quad \text{ve} \quad y = t_1^{b_1} t_2^{b_2} \dots t_m^{b_m}$$

şeklindedir. Şimdi $xy^{-1} = k_1^{a_1} k_2^{a_2} \dots k_n^{a_n} t_m^{-b_m} t_{m-1}^{-b_{m-1}} \dots t_1^{-b_1}$ olup $xy^{-1} \in U$ olduğu açıktır. O halde Teorem 2.8 gereğince $U \leq G$ dir. Ayrıca her $k \in K$ için $k = k^1 \in U$ olup; U, K 'yı içeren bir altgruptur; yani $K \subseteq U \leq G$ dir. Bu durumda $\langle K \rangle$ 'nın tanımından $\langle K \rangle \subseteq U$ olur. $\square$

Not 2.21 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 2.22 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.

Tanım 2.23 G bir grup, $H \leq G$ olsun. Bir $a \in G$ için

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

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

Örnek 2.24 S_3 grubunda $H = \langle f_2 \rangle = \{f_1, f_2\}$ alalım. H nin sağ kosetlerini bulalım.

$$Hf_1 = \{f_1 f_1, f_2 f_1\} = \{f_1, f_2\}$$

$$Hf_2 = \{f_1 f_2, f_2 f_2\} = \{f_2, f_1\}$$

$$Hf_3 = \{f_1 f_3, f_2 f_3\} = \{f_3, f_4\}$$

$$Hf_4 = \{f_1 f_4, f_2 f_4\} = \{f_4, f_3\}$$

$$Hf_5 = \{f_1 f_5, f_2 f_5\} = \{f_5, f_6\}$$

$$Hf_6 = \{f_1 f_6, f_2 f_6\} = \{f_6, f_5\}$$

Burada 3 tane farklı sağ koset vardır. Sağ kosetlerin herbirinde aynı sayıda eleman olup bu sağ kosetler aynı veya ayrıktyrlar. Ayrıca $x \in H \implies Hx = H$ ve $x \notin H \implies Hx \neq H$ olduğuna dikkat edin. Bunların bir tesadüf olmadığını göstereceğiz.

Teorem 2.25 $H \leq G$ olsun. $Ha = H \iff a \in H$. Ayrıca $Ha = Hb \iff ab^{-1} \in H$.

İspat: Önce $Ha = H$ olduğunu kabul edelim. O zaman $\exists h_1, h_2 \in H$ için $h_1 a = h_2$ olup H altgrup olduğundan $a = h_1^{-1} h_2 \in H$.

Şimdi $a \in H$ kabul edelim ve $Ha = H$ olduğunu gösterelim. $x \in Ha$ alalım. O halde $\exists h \in H$ için $x = ha$ şeklindedir. $h, a \in H$ olup H kapalı olduğundan $x = ha \in H$ olduğu açıktır. Yani $Ha \subseteq H$ dir. Şimdi de $x \in H$ alalım. $x = (xa^{-1})a \in Ha$ dir, çünkü H altgrup olduğundan $xa^{-1} \in H$ dir. Yani $H \subseteq Ha$ dir. O halde $Ha = H$ elde edilir.

Sonuç olarak “ $Ha = H \iff a \in H$ ” önermesi ispatlanmıştır. Son olarak

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

bulunur. □

Teorem 2.26 Bir G grubunda bir H alt grubunun iki sağ koseti aynı ya da ayrıktır.

İspat: Ha ve Hb iki sağ koset olsun. $Ha \cap Hb = \emptyset$ ise ispat yapılmış olur. $Ha \cap Hb \neq \emptyset$ olsun. O zaman $x \in Ha \cap Hb$ alalım. Bu durumda $\exists h_1, h_2 \in H$ için $x = h_1a$ ve $x = h_2b$ şeklindedir. O zaman

$$h_1a = h_2b \implies a = h_1^{-1}h_2b \implies ab^{-1} = h_1^{-1}h_2 \in H \implies Hab^{-1} = H \implies Ha = Hb$$

olup Ha ile Hb ya aynıdır ya da ayrıktır.

Teorem 2.27 G bir grup, $H \leq G$ 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. $f : Ha \rightarrow Hb$ dönüşümü $f(ha) = hb$ şeklinde tanımlansın.

$$f(h_1a) = f(h_2a) \implies h_1b = h_2b \implies h_1 = h_2 \implies h_1a = h_2a$$

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

Sonuç 2.28 Eğer G sonlu ise H ’nin iki sağ (sol) koseti 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:

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

Tanım 2.29 G bir grup, $H \leq G$ 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 2.30 (Lagrange¹) G sonlu bir grup ve $H \leq G$ 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

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

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

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

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

¹Joseph–Louis Lagrange (1736-1813)

Sonuç 2.31 Eğer G asal mertebeli bir grup ise G nin $\{e\}$ ve G den başka altgrubu yoktur.

Not 2.32 Eğer $H = \{e\}$ ise her $a \in G$ için $Ha = \{a\}$ olup $|G| = |G| = |G : H| |H| = |G : H|$ dir.

Örnek 2.33 $\mathbb{Z}_7$ grubunun altgrupları sadece $\{\bar{0}\}$ ve $\mathbb{Z}_7$ dir, çünkü $\mathbb{Z}_7$ asal mertebeli bir gruptur.

Örnek 2.34 $(\mathbb{Z}, +)$ grubunda $U = \{3k : k \in \mathbb{Z}\}$ altgrubunu ele alalım. Bu altgrup için Lagrange teoremi uygulanamaz, çünkü $\mathbb{Z}$ 'nin mertebesi sonlu değildir.

Teorem 2.35 G sonlu bir grup ve $a \in G$ olsun. O zaman $|a| \mid |G|$ 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 $|a| \mid |G|$ elde edilir. $|G| = k|a|$ diyelim. O zaman

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

olur ve ispat tamamlanır. $\square$

Örnek 2.36 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 2.16). G nin trivial olmayan altgrubu olmadığından $|G|$ asaldır.

Örnek 2.37 G bir grup, $a \in G$ olsun. $0 \neq m$ için $a^m = e$ ise $|a| \mid m$ olduğunu gösterin.

Çözüm: $|a| = n$ olsun. $n \leq m$ olduğu açıktır. Bölme algoritmasından dolayı m, n sayı çifti için $m = nq + r, 0 \leq r < n$ olacak şekilde $q, r \in \mathbb{Z}$ vardır. Şimdi

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

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

Teorem 2.38 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 $|U| \mid p$ 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. $\square$

Tanım 2.39 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 2.40 $(m, n) = 1$ olması için gerek ve yeter şart $mq + nr = 1$ olacak şekilde q, r tamsayılarının var olmasıdır.

Tanım 2.41 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, $\phi(10) = 4, \phi(9) = 6$ dir. p asal ise $\phi(p) = p - 1$ olduğu açıktır.

Teorem 2.42 n pozitif bir tamsayı olsun. $\mathbb{Z}_n$ 'de n ile aralarında asal olan sayıların kalan sınıfları modülo n çarpımı ile bir abelyen grup oluştururlar. (Bu grubu $\mathbb{Z}_n^*$ ile göstereceğiz.)

İspat: $\bar{a}, \bar{b} \in \mathbb{Z}_n^*$ alalım. O halde $(a, n) = 1$ ve $(b, n) = 1$ dir. $\bar{a} \odot \bar{b} \in \mathbb{Z}_n^*$ olduğunu yani $(ab, n) = 1$ olduğunu göstermeliyiz.

$$\begin{aligned} (a, n) = 1 &\implies aq_1 + nr_1 = 1 \text{ olacak şekilde } q_1, r_1 \in \mathbb{Z} \text{ vardır,} \\ (b, n) = 1 &\implies bq_2 + nr_2 = 1 \text{ olacak şekilde } q_2, r_2 \in \mathbb{Z} \text{ vardır,} \\ &\implies ab(\underbrace{q_1q_2}_q) + n(\underbrace{aq_1r_2 + bq_2r_1 + nr_1r_2}_r) = 1 \\ &\implies (ab)q + nr = 1 \quad (q, r \in \mathbb{Z}) \\ &\implies (ab, n) = 1 \end{aligned}$$

olup ab ile n aralarında asaldır.

Modülo n çarpmasının birleşme ve değişme özelliği vardır ve $\bar{1}$ bu grubun birim elemanıdır. (Her $n \in \mathbb{Z}^+$ için $(1, n) = 1$ dir.) Şimdi ters elemanın varlığını gösterelim. $\bar{a} \in \mathbb{Z}_n^*$ alalım. O zaman $(a, n) = 1$ olur. Bu durumda $aq + nr = 1$ olacak şekilde $q, r \in \mathbb{Z}$ vardır. Bu durumda $aq \equiv 1 \pmod{n}$ olup $(\bar{a})^{-1} = \bar{q}$ olur. $(q, n) = 1$ olduğundan $\bar{q} \in \mathbb{Z}_n^*$ dir. $\square$

Örnek 2.43 $\mathbb{Z}_9^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ grubunun çarpım tablosunu yazalım.

$\odot$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$	$\bar{8}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$	$\bar{8}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\bar{1}$	$\bar{5}$	$\bar{7}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{7}$	$\bar{2}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\bar{2}$	$\bar{7}$	$\bar{8}$	$\bar{4}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{1}$	$\bar{8}$	$\bar{4}$	$\bar{2}$
$\bar{8}$	$\bar{8}$	$\bar{7}$	$\bar{5}$	$\bar{4}$	$\bar{2}$	$\bar{1}$

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 2.44 (Euler²) n pozitif bir tamsayı olsun. $(a, n) = 1$ ise $a^{\phi(n)} \equiv 1 \pmod{n}$ dir.

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

Teorem 2.45 (Fermat³) 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. $(a, p) \neq 1$ ise a, p 'nin katı olup $a^p \equiv a \equiv 0 \pmod{p}$ olur. $\square$

Örnek 2.46 $p = 7$ alalım. $(-2)^7 = -128 = (-19) \cdot 7 + 5$ olup $-128 \equiv 5 \equiv -2 \pmod{7}$ dir.

Teorem 2.47 G bir grup H ve K , G nin iki altgrubu olsun. HK nin altgrup olması için gerek ve yeter şart $HK = KH$ olmasıdır.

İspat: $(\Leftarrow) HK = KH$ olsun. HK nin altgrup olduğunu göstereceğiz. $x = h_1 k_1 \in HK$ ve $y = h_2 k_2 \in HK$ alalım. ($h_i \in H, k_i \in K$ dir.)

$$\begin{aligned} xy^{-1} &= h_1 k_1 (h_2 k_2)^{-1} = h_1 \underbrace{k_1 k_2^{-1}}_{k_3} h_2^{-1} \\ &= h_1 \underbrace{(k_3 h_2^{-1})}_{\in KH=HK} = h_1 (h_3 k_4) = \underbrace{(h_1 h_3)}_{\in H} k_4 \\ &= h_4 k_4 \in HK \end{aligned}$$

olup Teorem 2.8 den HK altgruptur.

$(\Rightarrow)$ Şimdi de HK nin altgrup olduğunu kabul edip $HK = KH$ olduğunu gösterelim.

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

Ayrıca,

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

Sonuç olarak $HK = KH$ elde edilir. $\square$

²Leonhard Euler (1707-1783)

³Pierre de Fermat (1601-1665)

ALİŞTIRMALAR

1. $(\mathbb{Z}_{10}, \oplus)$ grubunda $\bar{5}$ elemanının derecesini bulunuz. $\bar{5}$ 'in derecesi grubun mertebesini böler mi? $\bar{5}$ '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. $H_1 \cup H_2 \leq G \iff H_1 \subseteq H_2$ 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 $C(a) \leq G$ 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 $\implies HH = H$ olduğunu gösterin. Eğer H sonsuz elemanlı ise bu önermenin tersinin doğru olmadığını gösterin. (İpucu: Bir ters örnek verin.)
11. G bir grup $H \leq G$ olsun. $\theta(xH) = Hx^{-1}$ şeklinde tanımlanan fonksiyonun 1-1 olduğunu gösterin. (Önce iyi tanımlandığını göstermek gereklidir.)

12. G bir grup; $H \leq G, K \leq G$ olsun. $|H| = 75$ ve $|K| = 57$ ise $H \cap K$ nın devirli olduğunu gösterin.
13. G bir grup $a \in G$ olsun. $H = \{x \in G : \exists n \in \mathbb{Z} \text{ için } x = a^n\}$ kümesi G nin bir alt grubudur, gösterin.
14. $\mathbb{Z}_{14}^*$ grubunun çarpım tablosunu yazınız. Bu grup devirli midir? Bu grubun trivial olmayan bir alt grubunu bulunuz.
15. $(\mathbb{C} \setminus \{0\}, \cdot)$ grubunda $H = \{x + iy : x, y \in \mathbb{R}, xy \geq 0\}$ bir alt grup mudur?

ALİŞTIRMALARIN ÇÖZÜMLERİ

ÇÖZÜM 1. $\mathbb{Z}_{10}$ da $\bar{5} \oplus \bar{5} = \bar{0}$ olup $|\bar{5}| = 2$ dir. $2 \mid 10$ olup $\bar{5}$ 'in derecesi grubun mertebesini böler. $\bar{5}$ 'in $\mathbb{Z}$ deki derecesi sonsuzdur, çünkü $n \cdot 5 = 0$ olacak şekilde $n \in \mathbb{N}^+$ yoktur.

ÇÖZÜM 2. $x, y \in H$ olsun. O halde $x^2 = y^2 = e$ dir.

$$\begin{aligned} (xy^{-1})^2 &= xy^{-1}xy^{-1} \\ &= x^2(y^{-1})^2 \quad (G \text{ değişmeli olduğundan}) \\ &= e(y^2)^{-1} \\ &= e^{-1} = e \end{aligned}$$

olup $xy^{-1} \in H$ dir. O halde Teorem 2.8 gereğince H bir altgruptur.

ÇÖZÜM 3. $(\Leftarrow)$ $H_1 \subseteq H_2$ veya $H_2 \subseteq H_1 \implies H_1 \cup H_2 = H_1 \leq G$ veya $H_1 \cup H_2 = H_2 \leq G$ olup her iki halde de $H_1 \cup H_2$ bir altgruptur.

$(\implies)$ Şimdi $H_1 \cup H_2 \leq G$ olduğunu kabul edelim. $H_1 \subseteq H_2$ veya $H_2 \subseteq H_1$ olduğunu göstereceğiz. Aksini kabul edelim. Yani $H_1 \not\subseteq H_2$ ve $H_2 \not\subseteq H_1$ olsun. (Bu iki küme ayrık olamazlar, çünkü $e \in H_1 \cap H_2$ dir.) Şimdi

$$\begin{aligned} a \in H_1 \setminus H_2 &\implies a \in H_1 \text{ fakat } a \notin H_2 \\ b \in H_2 \setminus H_1 &\implies b \in H_2 \text{ fakat } b \notin H_1. \end{aligned}$$

Bu durumda $a, b \in H_1 \cup H_2$ olup $ab \in H_1 \cup H_2$ dir. $ab \in H_1$ olabilir, fakat

$$ab \in H_1 \implies \underbrace{a^{-1}}_{\in H_1}(ab) = b \in H_1$$

çelişkisi elde edilir. O halde $ab \in H_2$ olmalıdır, fakat

$$ab \in H_2 \implies (ab) \underbrace{b^{-1}}_{\in H_2} = a \in H_2$$

çelişkisi elde edilir. Bu da $H_1 \cup H_2$ nin altgrup olmasıyla çelişir. O halde $H_1 \subseteq H_2$ veya $H_2 \subseteq H_1$ olmalıdır.

ÇÖZÜM 4. $(\mathbb{Q} \setminus \{0\}, \cdot)$ grubunda $\langle 3, \frac{1}{2} \rangle = \{ 3^n \cdot \frac{1}{2^m} : n, m \in \mathbb{Z} \}$ kümesidir. Bazı elemanlarını yazalım:

$$\left\langle 3, \frac{1}{2} \right\rangle = \left\{ \dots, \frac{1}{24}, \frac{1}{12}, \frac{1}{8}, \frac{1}{4}, \frac{3}{4}, \frac{2}{9}, \dots, 2, 3, 6, 18, \dots \right\}.$$

ÇÖZÜM 5. $C(a) = \{ x \in G : ax = xa \}$. $x, y \in C(a)$ alalım. O halde $ax = xa$ ve $ay = ya$ dır.

$$ay = ya \implies a = yay^{-1} \implies y^{-1}a = ay^{-1} \implies y^{-1} \in C(a).$$

Şimdi $xy^{-1} \in C(a)$ olduğunu gösterelim:

$$(xy^{-1})a = x(y^{-1}a) = x(ay^{-1}) = (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1})$$

olup $xy^{-1} \in C(a)$ dır. Teorem 2.8 gereğince $C(a)$ bir altgruptur.

Şimdi de $|a| = 5$ olsun.

$$x \in C(a) \implies xa = ax \implies xa^3 = axa^2 = a(xa)a = a(ax)a = a^2(xa) = a^2(ax) = a^3x$$

$$\implies x \in C(a^3),$$

$$x \in C(a^3) \implies xa^3 = a^3x \implies xa^6 = a^3xa^3 = a^3(xa^3) = a^3(a^3x)$$

$$\implies xa = a^6x = ax$$

$$\implies x \in C(a)$$

olup $C(a) = C(a^3)$ olduğu görülür.

ÇÖZÜM 6. Farklı sağ kosetler

$$H1 = H(-1) = \{ 1, -1 \}$$

$$Hi = H(-i) = \{ i, -i \}$$

ÇÖZÜM 7. $HK = \{ 1, -1, i, -i \}$ ve $H \cap K = \{ 1, -1 \}$ olur. Bu durumda

$$|HK| = 4 \quad \text{ve} \quad \frac{|H||K|}{|H \cap K|} = \frac{4 \cdot 2}{2} = 4$$

olup eşitlik sağlanır. Şimdi $|H| > \sqrt{|G|}$ ve $|K| > \sqrt{|G|}$ olduğunu kabul edelim. Bu durumda

$$|G| = \sqrt{|G|}\sqrt{|G|} < |H||K| = |H \cap K||HK|.$$

Şimdi, $H \cap K = \{ e \}$ ise $|G| < |HK|$ olur. $HK \subseteq G$ olduğundan bu bir çelişki olur. O halde $|H \cap K| \neq \{ e \}$ dir; yani $H \cap K$ en az iki elemanlıdır.

ÇÖZÜM 8. $(\mathbb{Z}, +)$ da $4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, \dots\}$ altgrubunun farklı sağ kosetleri:

$$4\mathbb{Z} + 0 = \{\dots, -8, -4, 0, 4, 8, \dots\}$$

$$4\mathbb{Z} + 1 = \{\dots, -7, -3, 1, 5, 9, \dots\}$$

$$4\mathbb{Z} + 2 = \{\dots, -6, -2, 2, 6, 10, \dots\}$$

$$4\mathbb{Z} + 3 = \{\dots, -5, -1, 3, 7, 11, \dots\}$$

olup $|\mathbb{Z} : 4\mathbb{Z}| = 4$ dür.

ÇÖZÜM 9. K nın grup tablosu ana diyagonale göre simetrik olduğundan K abelyen bir gruptur. Birim eleman a dır. K nın altgrupları:

$$H = \langle a \rangle = \{a\}, \quad G = \langle b \rangle = \{a, b\}, \quad K = \langle c \rangle = \{a, c, b, d\}.$$

Ayrıca $\langle d \rangle = \{a, d, b, c\} = K$ olur. Buradan K nın devirli olduğu söylenebilir. H nin farklı sağ kosetleri 4 tanedir:

$$Ha = \{a\}, \quad Hb = \{b\}, \quad Hc = \{c\}, \quad Hd = \{d\}.$$

$G = \{a, b\}$ nin farklı sağ kosetleri 2 tanedir:

$$Ga = Gb = \{a, b\}, \quad Gc = Gd = \{c, d\}.$$

$K = \{a, b, c, d\}$ nin sağ koseti bir tanedir:

$$Ka = Kb = Kc = Kd = \{a, b, c, d\}.$$

ÇÖZÜM 10.

$$x \in HH \implies \exists h_1, h_2 \in H, x = h_1 h_2 \in H \text{ (Çünkü } H \leq G) \implies HH \subseteq H$$

$$x \in H \implies x = \underbrace{x}_{\in H} \cdot \underbrace{e}_{\in H} \in HH \implies H \subseteq HH$$

olup $HH = H$ olduğu görülür.

Şimdi $G = (\mathbb{Z}, +)$ ve $H = \{0, 1, 2, 3, \dots\}$ olsun. $H + H = H$ dir fakat H bir altgrup değildir. Böylece “ $H + H = H \implies H$ altgruptur” önermesinin doğru olmadığı gösterilmiş olur.

ÇÖZÜM 11. θ nın iyi tanımlı olduğunu göstermek için $xH = yH \implies Hx^{-1} = Hy^{-1}$ önermesi ispatlanmalıdır.

$$xH = yH \implies y^{-1}xH = H \implies y^{-1}x \in H \implies Hy^{-1}x = H \implies Hy^{-1} = Hx^{-1}$$

olup θ iyi tanımlanmıştır. Ayrıca

$$\theta(xH) = \theta(yH) \implies Hx^{-1} = Hy^{-1} \implies Hx^{-1}y = H \implies x^{-1}y \in H \implies H = x^{-1}yH \implies xH = yH$$

olup θ nın 1-1 olduğu görülür.

ÇÖZÜM 12. $|H| = 75 = 3 \cdot 5^2$ ve $|K| = 57 = 3 \cdot 19$ olup $H \cap K \leq H$ ve $H \cap K \leq K$ olacağından Lagrange Teoremi gereğince $|H \cap K|$ hem 75'i hem de 57'yi bölmelidir. Bunu sağlayan sadece 1 ve 3 sayıları vardır. $|H \cap K| = 1$ ise $H \cap K$ trivial grup olup devirlidir. $|H \cap K| = 3$ ise 3 asal olup $H \cap K$ devirlidir.

ÇÖZÜM 13.

$$\begin{aligned} x, y \in H &\implies \exists n, m \in \mathbb{Z}, x = a^n, y = a^m \\ &\implies xy^{-1} = a^n a^{-m} = a^{n-m} \\ &\implies xy^{-1} \in H \quad (\text{Çünkü } n - m \in \mathbb{Z}) \end{aligned}$$

olup Teorem 2.8 gereğince $H \leq G$ dir.

ÇÖZÜM 14. $\mathbb{Z}_{14}^* = \{ \bar{1}, \bar{3}, \bar{5}, \bar{9}, \bar{11}, \bar{13} \}$ dır. Bu grubun çarpım tablosu:

$\odot$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{9}$	$\bar{11}$	$\bar{13}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{9}$	$\bar{11}$	$\bar{13}$
$\bar{3}$	$\bar{3}$	$\bar{9}$	$\bar{1}$	$\bar{13}$	$\bar{5}$	$\bar{11}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\bar{11}$	$\bar{3}$	$\bar{13}$	$\bar{9}$
$\bar{9}$	$\bar{9}$	$\bar{13}$	$\bar{3}$	$\bar{11}$	$\bar{1}$	$\bar{5}$
$\bar{11}$	$\bar{11}$	$\bar{5}$	$\bar{13}$	$\bar{1}$	$\bar{9}$	$\bar{3}$
$\bar{13}$	$\bar{13}$	$\bar{11}$	$\bar{9}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

Şimdi $\langle \bar{3} \rangle = \{ \bar{1}, \bar{3}, \bar{9}, \bar{13}, \bar{11}, \bar{5} \} = \mathbb{Z}_{14}^*$ olup grup devirlidir. $\langle \bar{9} \rangle = \{ \bar{1}, \bar{9}, \bar{11} \}$ bu grubun trivial olmayan bir altgrubudur.

ÇÖZÜM 15. $z_1 = 1 + i, z_2 = 0 + 5i$ olsun. $z_1, z_2 \in H$ olduğu açıktır. Şimdi $z_1 z_2 = -5 + 5i \notin H$ dir çünkü $(-5)5 < 0$ dir. Yani; H kümesi kapalı olmadığından bir altgrup değildir.

Normal Altgruplar ve Faktör Grupları

Daha önce S_3 grubunda $H = \{ f_1, f_2 \}$ alt grubunun 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. Eğer S_3 abelyen olsaydı sol kosetler ile sağ kosetler eşit olurdu. Acaba; sol kosetler ile sağ kosetlerin eşit olduğu başka altgruplar var mıdır?

Tanım 3.1 G bir grup ve $N \leq G$ olsun. Her $g \in G$ ve her $n \in N$ için $gng^{-1} \in N$ ise N ye G nin **normal alt grubu** denir ve $N \triangleleft G$ 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 alt gruplarıdır. (Neden?) G abelyen ise $gng^{-1} = n \in N$ olup abelyen bir grubun her alt grubunun normal olduğu görülür.

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

- (i) $N \triangleleft G$
- (ii) Her $g \in G$ için $gNg^{-1} = N$
- (iii) Her $g \in G$ için $gN = Ng$

İspat: (i $\implies$ ii) $N \triangleleft G$ 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 $\implies$ iii) $gNg^{-1} = N \implies gNg^{-1}g = Ng \implies gN = Ng$

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

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.

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

olup $N \triangleleft G$ dir.

Normal Altgrup Kullanarak Faktör Grubu Elde Edilmesi

Bu bölümde bir G grubunun bir H altgrubunun sağ kosetleri arasında $(Ha) * (Hb) = H(ab)$ şeklinde bir $*$ işlemi tanımlamak istiyoruz. Ancak eğer H normal değilse bu $*$ işlemi iyi tanımlanmamıştır. Yani $Ha = Hx$ ve $Hb = Hy$ iken $H(ab) \neq H(xy)$ 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 $(Ha) * (Hb)$ ile $(Ha) \cdot (Hb)$ çarpımının aynı sonucu vermesini istiyoruz. Yani Ha kümesi ile Hb kümesinin çarpımının $H(ab)$ 'ye eşit olmasını istiyoruz. Fakat; H normal değilse iki sağ kosetin çarpımı başka bir sağ kosete eşit olmayabilir; mesela S_3 grubunda $H = \{f_1, f_2\}$ alınırsa:

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

olup bu küme bir sağ koset değildir.

Teorem 3.5 G bir grup ve $N \triangleleft G$ olsun. $Na = Nx$ ve $Nb = Ny$ eşitliklerinden her zaman $N(ab) = N(xy)$ elde edilir.

İspat: $Na = Nx$ ve $Nb = Ny$ olsun.

$$N(ab) = (Na)b = (Nx)b = (xN)b = x(Nb) = x(Ny) = x(yN) = (xy)N = N(xy) \quad \square$$

Teorem 3.6 G bir grup ve $N \triangleleft G$ ise N nin iki sağ kosetinin çarpımı yine bir sağ kosettir.

İspat: Na, Nb iki sağ koset olsun.

$$(Na)(Nb) = N(aN)b = N(Na)b = (NN)ab = N(ab)$$

olup iki sağ kosetin çarpımı başka bir sağ kosettir. $\square$

Böylece, N normal ise N nin sağ kosetleri üzerindeki çarpma işleminin iyi tanımlandığını ve $*$ ile $\cdot$ işlemlerinin aynı olduğunu gösterdik.

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

$$(Na) * (Nb) = N(ab)$$

şeklinde bir işlem tanımlayalım. Bu işlemin iyi tanımlandığını Teorem 3.5’de gösterdik. $(G/N, *)$ cebirsel yapısının bir grup olduğunu göstereceğiz. Bu gruba G nin N ile olan **faktör grubu** denir. (Faktör grubu yerine **bölüm grubu** terimi de kullanılmaktadır.) Ayrıca; Teorem 3.6’nın ispatında görüldüğü gibi, $*$ yerine $\cdot$ kullanılmasında bir sakınca yoktur. Bu yüzden G grubunun işlem sembolü ile G/N faktör grubunun işlem sembolü aynı olacaktır.

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

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

$$Na(NbNc) = NaN(bc) = N(a(bc)) = N((ab)c) = N(ab)Nc = (NaNb)Nc$$

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

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

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

$$NaN a^{-1} = Ne = N \quad \text{ve} \quad Na^{-1}Na = Ne = N.$$

Sonuç olarak G/N bir gruptur. $\square$

Not 3.9 Lagrange Teoremi gereğince eğer $|G|$ sonlu ise $|G/N| = \frac{|G|}{|N|}$ 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 $G/U = \{U + 0, U + 1, U + 2, U + 3\}$ şeklinde yazılabilir. Bu grubun tablosu şöyledir.

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

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. $e \in Z(G)$ olup $Z(G) \neq \emptyset$ dir. $Z(G) \triangleleft G$ olduğunu gösterin.

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

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

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 $Z(G) \leq G$ 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 $Z(G) \triangleleft G$ 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 $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ grubunun altgrupları (dolayısıyla normal altgrupları) $\{\bar{0}\}$ ve kendisidir. O halde $\mathbb{Z}_5$ basit gruptur. Aslında asal mertebeli her grubun basit olduğunu Lagrange Teoreminden söyleyebiliriz. Acaba bunun tersi doğru mudur? Yani; basit her grup asal mertebeli midir? Bunun cevabı olumsuzdur. Fakat; basit ve abelyen her grup asal mertebelidir.

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

İspat: ($\implies$) G abelyen ve basit bir grup olsun. O halde $|G| \geq 2$ dir. Bir $e \neq a \in G$ seçelim. $|a| = n$ sonludur. Çünkü eğer $|a| = \infty$ olsaydı $\langle a \rangle$ devirli altgrubu da sonlu olmayıp G nin (en az 2 elemanlı) normal altgrubu olurdu. G basit olduğundan $\langle a \rangle = G$ olmalıdır. Bu durumda G sonsuz devirli grup olurdu. Bu durumda G 'nin trivial olmayan bir altgrubu (yani normal altgrubu) olurdu (Mesela $\langle a^2 \rangle$ gibi). O halde n sonludur. Öyleyse bir p asal böleni vardır. Buna göre $\langle a^{n/p} \rangle$ altgrubu mertebesi p olan bir normal altgruptur. G basit olduğundan $G = \langle a^{n/p} \rangle$ olmalıdır. O halde $|G| = p$ dir; yani G asal mertebelidir.

($\impliedby$) p bir asal sayı olmak üzere $|G| = p$ olsun. $U \triangleleft G$ olsun. Lagrange teoremi gereğince $|U| \mid p$ 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. $H \triangleleft G$ 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 $H \triangleleft G$ dir.

Örnek 3.16 İki normal alt grubun kesişiminin de normal olduğunu gösteriniz.

Çözüm: G bir grup $H \triangleleft G$ ve $K \triangleleft G$ olsun. $H \cap K \leq G$ olduğunu biliyoruz. Şimdi her $g \in G$ ve her $x \in H \cap K$ için

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

Örnek 3.17 $H \leq G$ ve $N \triangleleft G$ ise $HN \leq G$ olduğunu gösterin.

Çözüm: $x = h_1n_1 \in HN$ ve $y = h_2n_2 \in HN$ alalım.

$$\begin{aligned} xy^{-1} &= h_1 \underbrace{n_1n_2^{-1}}_{\in N} h_2^{-1} \quad (\text{Çünkü } N \leq G) \\ &= h_1n_3h_2^{-1} \\ &= \underbrace{(h_1h_2^{-1})}_{\in H} \underbrace{(h_2n_3h_2^{-1})}_{\in N} \quad (\text{Çünkü } H \leq G \text{ ve } N \triangleleft G) \\ &= h_3n_4 \in HN \end{aligned}$$

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

Örnek 3.18 $H \triangleleft G$ ve $N \triangleleft G$ ise $HN \triangleleft G$ olduğunu gösterin.

Çözüm: $HN \leq G$ olduğu bir önceki örnekte gösterilmiştir. Şimdi $HN \triangleleft G$ olduğunu gösterelim. $H \triangleleft G, N \triangleleft G$ olduğundan her $g \in G$ için $Hg = gH$ ve $Ng = gN$ dir. O halde:

$$g(HN) = (gH)N = (Hg)N = H(gN) = H(Ng) = (HN)g$$

olup $HN \triangleleft G$ olduğu görülür.

Örnek 3.19 $M = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z} \right\}$ 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 alt grubudur, gösterin. M/H yi oluşturunuz.

Çözüm:

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

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

Örnek 3.20 $\mathbb{Z}_{12}$ 'de $H = \langle \bar{6} \rangle$ altgrubunu bulunuz. $\mathbb{Z}_{12}/H$ yi yazınız. Bu gruptaki elemanların derecelerini bulunuz.

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

$$\begin{aligned} H \oplus \bar{0} &= \{ \bar{0}, \bar{6} \} = H \oplus \bar{6} \\ H \oplus \bar{1} &= \{ \bar{1}, \bar{7} \} = H \oplus \bar{7} \\ H \oplus \bar{2} &= \{ \bar{2}, \bar{8} \} = H \oplus \bar{8} \\ H \oplus \bar{3} &= \{ \bar{3}, \bar{9} \} = H \oplus \bar{9} \\ H \oplus \bar{4} &= \{ \bar{4}, \bar{10} \} = H \oplus \bar{10} \\ H \oplus \bar{5} &= \{ \bar{5}, \bar{11} \} = H \oplus \bar{11} \end{aligned}$$

O halde $\mathbb{Z}_{12}/H = \{ H \oplus \bar{0}, H \oplus \bar{1}, H \oplus \bar{2}, H \oplus \bar{3}, H \oplus \bar{4}, H \oplus \bar{5} \}$ dir. Bu elemanların dereceleri:

$$|H \oplus \bar{0}| = 1, \quad |H \oplus \bar{1}| = 6, \quad |H \oplus \bar{2}| = 3, \quad |H \oplus \bar{3}| = 2, \quad |H \oplus \bar{4}| = 3, \quad |H \oplus \bar{5}| = 6.$$

Örnek 3.21 G bir grup ve $H = \langle a \rangle$ sonlu devirli altgrubu G de normal olsun. Eğer $K \leq H$ ise $K \triangleleft G$ olduğunu gösterin.

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

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

Şimdi K sonlu olduğundan $|k| = m$ sonludur. Ayrıca $|gkg^{-1}| = m$ dir (Bölüm 1, Alıştırma 14).

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

olur. Ayrıca $\langle k \rangle \leq K \leq H$ ve $\langle gkg^{-1} \rangle \leq H$ olup $\langle k \rangle$ ve $\langle gkg^{-1} \rangle$ altgrupları, H nin mertebeleri eşit olan iki altgrubu olur. Devirli bir grubun mertebesi eşit olan iki altgrubu eşit olacağından $\langle k \rangle = \langle gkg^{-1} \rangle$ olmalıdır. O halde $\langle gkg^{-1} \rangle \leq K$ olup $gkg^{-1} \in K$ dir. Yani $K \triangleleft G$ olur.

ALIŞTIRMALAR

1. $G = \{e, a, a^2, a^3\}$ 4-üncü mertebeden devirli grup ve $H = \{e, a^2\}$ onun altgrubu olsun. $H \triangleleft G$ 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. $H \triangleleft G$ olduğunu gösterin.
5. G abelyen bir grup ve $N \triangleleft G$ olsun. G/N nin abelyen olduğunu gösterin.
6. G bir grup, $H \leq G$ ve $K \triangleleft G$ ise $H \cap K \triangleleft H$ olduğunu gösterin.
7. G bir grup ve $H \leq G$ olsun. $N_G(H) = \{x \in G : xHx^{-1} = H\}$ kümesine H nin G deki **normalleyeni** denir. $N_G(H) \leq G$ ve $H \triangleleft N_G(H)$ 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. $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$ 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. $H \leq G$ alt grubu “her $x \in G$ için $x^2 \in H$ ” özelliğine sahip olsun. $H \triangleleft G$ olduğunu gösterin. (İpucu: $xhx^{-1} = (xh)^2h^{-1}(x^{-1})^2$) Ayrıca G/H nin abelyen olduğunu gösterin.

ALIŞTIRMALARIN ÇÖZÜMLERİ

ÇÖZÜM 1. G abelyen ve H altgrup olduğundan $H \triangleleft G$ 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 $x \in G$ için $xh = hx$ yani $xhx^{-1} = h$ olduğunu göstermeliyiz. $H \triangleleft G$ olduğundan $xhx^{-1} \in H$ dir. O halde ya

$xhx^{-1} = e$ ya da $xhx^{-1} = h$ dir. $xhx^{-1} = e \implies xh = x \implies h = e$ olamaz. O halde $xhx^{-1} = h$ olup ispat tamamlanır.

ÇÖZÜM 3. $e \neq a \in G$ derecesi 2 olan tek eleman olsun. Her $x \in G$ için $ax = xa$ yani $x^{-1}ax = a$ olduğunu göstereceğiz.

$$(x^{-1}ax)^2 = (x^{-1}ax)(x^{-1}ax) = x^{-1}a^2x = x^{-1}x = e$$

olup $(x^{-1}ax)$ 'in derecesi 2 dir. ($x^{-1}ax = e$ olsaydı $a = e$ olurdu). O halde $x^{-1}ax = a$ olmalıdır.

ÇÖZÜM 4. $g \in G, h \in H$ olsun. $ghg^{-1} = hgg^{-1} = h \in H$ dir, çünkü $h \in H \subseteq Z(G)$ olup h elemanı merkezededir; yani her elemanla değişmelidir.

ÇÖZÜM 5. $Na, Nb \in G/N$ alalım. G abelyen olduğundan $ab = ba$ dir. O halde

$$NaNb = N(ab) = N(ba) = NbNa$$

olup G/N nin abelyen olduğu görülür.

ÇÖZÜM 6. İki altgrubun kesişimi altgrup olduğundan $H \cap K \leq H$ olur. Şimdi $x \in H \cap K$ ve $h \in H$ alalım. H bir alt grup ve $x \in H$ olduğundan $h x h^{-1} \in H$ dir. Ayrıca $h \in G, x \in K$ ve $K \triangleleft G$ olduğundan $h x h^{-1} \in K$ dir. Bu durumda $h x h^{-1} \in H \cap K$ olur; yani $H \cap K \triangleleft H$ olur.

ÇÖZÜM 7. $N_G(H) = \{x \in G : Hx = xH\}$ şeklinde yazılabilir. Önce

$$y \in N_G(H) \implies Hy = yH \implies y^{-1}Hy = H \implies y^{-1}H = Hy^{-1} \implies y^{-1} \in N_G(H)$$

sonucunu elde edelim. Şimdi

$$\begin{aligned} x, y \in N_G(H) &\implies (xy^{-1})H = x(y^{-1}H) = x(Hy^{-1}) = (xH)y^{-1} = (Hx)y^{-1} = H(xy^{-1}) \\ &\implies xy^{-1} \in N_G(H) \end{aligned}$$

olup Teorem 2.8 gereğince $N_G(H) \leq G$ dir.

Şimdi $h \in H \implies Hh = hH = H$ olup $H \subseteq N_G(H)$ dir. H bir altgrup olduğundan $H \leq N_G(H)$ yazabiliriz. Şimdi $h \in H, x \in N_G(H)$ alalım.

$$(x^{-1}hx)H = x^{-1}h(xH) = x^{-1}h(Hx) = x^{-1}(hH)x = x^{-1}Hx = H$$

olup " $aH = H \iff a \in H$ " önermesi hatırlanırsa $x^{-1}hx \in H$ elde edilir. O halde $H \triangleleft N_G(H)$ dir.

ÇÖZÜM 8. Q_8 in grup tablosu:

$\cdot$	1	-1	i	j	k	-i	-j	-k
1	1	-1	i	j	k	-i	-j	-k
-1	-1	1	-i	-j	-k	i	j	k
i	i	-i	-1	k	-j	1	-k	j
j	j	-j	-k	-1	i	k	1	-i
k	k	-k	j	-i	-1	-j	i	1
-i	-i	i	1	-k	j	-1	k	-j
-j	-j	j	k	1	-i	-k	-1	i
-k	-k	k	-j	i	1	j	-i	-1

Bütün elemanlarla değişmeli olan elemanlar 1 ve -1 dir; yani $Z(Q_8) = \{1, -1\}$ dir.

Şimdi $i \cdot i = -1, i \cdot j = k$ olduğundan gruptaki bütün elemanlar i ve j kullanılarak bulunur. Mesela, $-k = (i \cdot i)(i \cdot j)$ dir. O halde $\langle i, j \rangle = Q_8$ dir. Q_8 in altgrupları:

$$\begin{aligned} H_1 &= \{1\} & H_2 &= \{1, -1\} \\ H_3 &= \{1, -1, i, -i\} & H_4 &= \{1, -1, j, -j\} \\ H_5 &= \{1, -1, k, -k\} & H_6 &= Q_8 \end{aligned}$$

H_1 ve H_6 trivial altgruplar olduğundan normaldirler. H_2 grubun merkezi olduğundan normaldir. H_3, H_4 ve H_5 de indeksleri 2 olduğundan normaldir.

ÇÖZÜM 9.

$$\begin{aligned} GL_n(\mathbb{R}) &= \{A : A, n \times n \text{ reel matris ve } \det(A) \neq 0\} \\ SL_n(\mathbb{R}) &= \{A : A, n \times n \text{ reel matris ve } \det(A) = 1\}. \end{aligned}$$

Şimdi $A, B \in SL_n(\mathbb{R})$ alalım. O halde $\det(A) = \det(B) = 1$ dir.

$$\det(AB^{-1}) = \det(A) \det(B^{-1}) = \det(A) \frac{1}{\det(B)} = 1$$

olup $AB^{-1} \in SL_n(\mathbb{R})$ dir. Teorem 2.8'den $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ dir. Şimdi $A \in SL_n(\mathbb{R})$ ve $X \in GL_n(\mathbb{R})$ alalım. Yani $\det(A) = 1, \det(X) \neq 0$ dir.

$$\det(XAX^{-1}) = \det(X) \det(A) \det(X^{-1}) = \det(X) \det(A) \frac{1}{\det(X)} = \det(A) = 1$$

olup $XAX^{-1} \in SL_n(\mathbb{R})$ dir; yani $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$ dir.

ÇÖZÜM 10. $hkh^{-1}k^{-1}$ elemanına bakalım. H normal olduğundan $kh^{-1}k^{-1} \in H$ ve K normal

olduğundan $hkh^{-1} \in K$ dır. O halde:

$$\begin{aligned} hkh^{-1}k^{-1} &= h(\underbrace{kh^{-1}k^{-1}}_{\in H}) = hh_2 \in H \\ hkh^{-1}k^{-1} &= (\underbrace{hkh^{-1}}_{\in K})k^{-1} = k_2k^{-1} \in K \end{aligned}$$

olup $hkh^{-1}k^{-1} \in H \cap K = \{e\} \implies hkh^{-1}k^{-1} = e \implies hk = kh$.

ÇÖZÜM 11. G/Z nin devirli olduğunu kabul edelim. O zaman $G/Z = \langle Zt \rangle$ olacak şekilde $t \in G$ vardır. Yani Z nin her koseti bir $i \in \mathbb{Z}$ için $(Zt)^i = Zt^i$ şeklindedir. Şimdi $x, y \in G$ alalım. Bu iki eleman Z nin iki sağ kosetine ait olmalıdır. $x \in Zt^m$ ve $y \in Zt^n$ olsun ($m, n \in \mathbb{Z}$). O halde $\exists z_1, z_2 \in Z$ için $x = z_1t^m, y = z_2t^n$ dir. Şimdi

$$\begin{aligned} xy &= z_1t^m z_2t^n = t^{m+n} z_1 z_2, \\ yx &= z_2t^n z_1t^m = t^{m+n} z_1 z_2 \end{aligned}$$

olup $xy = yx$ dir. x, y nin seçimi keyfî olduğundan G abelyendir. Bu da G nin abelyen olmadığı kabülü ile çelişir. O halde G/Z devirli değildir.

ÇÖZÜM 12. $h \in H$ ve $x \in G$ alalım.

$$xhx^{-1} = (\underbrace{xh}_H)^2 h^{-1} (\underbrace{x^{-1}}_H)^2 = h_2 h^{-1} h_3 \in H$$

olup $H \triangleleft G$ olduğu görülür. $G/H = \{Ha : a \in G\}$ yazalım. Önce her $a \in G$ için

$$(Ha)^2 = Ha^2 = H \quad (\text{Çünkü } a^2 \in H) \implies Ha = Ha^{-1}$$

olduğunu görelim. O halde her $a, b \in G$ için

$$(Hab)^2 = H \implies Habab = H \implies Haba = Hb^{-1} \implies Hab = Hb^{-1}a^{-1} = (Hb^{-1})(Ha^{-1}) = HbHa$$

olup $HaHb = HbHa$ elde edilir. Yani G/H abelyendir.

Homomorfizmalar ve İzomorfizmalar

Tanım 4.1 (G, Δ) 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

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

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

Δ	...	...	b	...
$\vdots$			$\vdots$	
$\vdots$			$\vdots$	
a	...	...	$a\Delta b$	
$\vdots$				

$\star$	...	...	$f(b)$	...
$\vdots$			$\vdots$	
$\vdots$			$\vdots$	
$f(a)$	...	...	$f(a) \star f(b) = f(a\Delta b)$	...
$\vdots$				

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

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 $H = (\mathbb{Z}_n, \oplus)$ olsun. Buna göre $f : G \longrightarrow H, f(x) = \bar{x}$ şeklinde tanımlanan dönüşüm bir homomorfizmadır, çünkü her $x, y \in \mathbb{Z}$ için

$$f(x + y) = \overline{x + y} = \bar{x} \oplus \bar{y} = f(x) \oplus f(y).$$

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 homomorfizmadır, 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, $N \triangleleft G$ 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) $f(G) \leq H$ dir.

(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

$$\begin{aligned} f(g) &= f(ge) = f(g)f(e) \implies f(g) = f(g)f(e) \\ &\implies f(g)^{-1}f(g) = f(g)^{-1}f(g)f(e) \\ &\implies e_0 = e_0f(e) \\ &\implies f(e) = e_0 \end{aligned}$$

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.

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

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

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

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 $n \geq 1$ ise

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

Benzer şekilde $n < 0$ ise

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

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

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

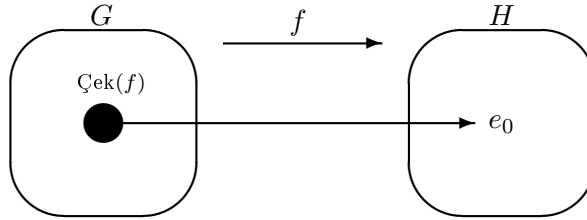
olup H de devirlidir. □

Bir Grup Homomorfizmasının Çekirdeği

Tanım 4.9 G, H iki grup $f : G \longrightarrow H$ bir homomorfizma ve H nin birim elemanı e_0 olsun. f nin **çekirdeği** şöyle tanımlanır:

$$\text{Çek}(f) = \{ x \in G : f(x) = e_0 \} = f^{-1}(e_0).$$

$\text{Çek}(f)$ boş küme olamaz, çünkü $f(e) = e_0$ olduğundan $e \in \text{Çek}(f)$ olmalıdır.



Teorem 4.10 $f : G \longrightarrow H$ bir grup homomorfizması ise $\text{Çek}(f) \triangleleft G$ dir.

İspat:

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

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

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

Tanım 4.11 $f : G \longrightarrow H$ 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 $\text{Çek}(f)$ nin bir sol koseti (veya sağ koseti) olduğunu göreceğiz.

Teorem 4.12 $f : G \rightarrow H$ bir homomorfizma, $h \in H$ ve $x \in f^{-1}(h)$ olsun. Bu durumda $f^{-1}(h) = x \cdot \text{Çek}(f)$ dir.

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

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

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

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

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

Sonuç 4.13 $h \in H$ elemanının bütün ters görüntüleri $x \in f^{-1}(h)$ olmak üzere $x \cdot \text{Çek}(f)$ kümesidir.

Tanım 4.14 $f : G \rightarrow H$ grup homomorfizması birebir ve örten ise f ye bir **izomorfizma** denir. Eğer G den H ye bir izomorfizma (yani birebir ve örten bir homomorfizma) varsa G ile H gruplarına **izomorfiktirler** veya **eş yapılıdırlar** denir ve $G \cong H$ yazılır.

Not 4.15 Birebir homomorfizmalara **monomorfizma**; örten homomorfizmalara da **epimorfizma** denmektedir.

Not 4.16 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 4.17 $A = \{1, -1, i, -i\}$ kümesi çarpma işlemi ile bir gruptur. $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ alalım. $f : \mathbb{Z}_4 \rightarrow A$ dönüşümünü

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

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

$$f(\bar{1} \oplus \bar{2}) = f(\bar{3}) = -i \quad \text{ve} \quad f(\bar{1})f(\bar{2}) = i(-1) = -i.$$

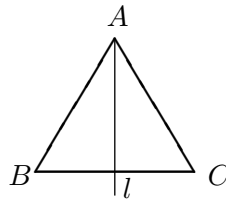
Bütün kontroller yapıldıktan sonra $A \cong \mathbb{Z}_4$ yazabiliriz. Şimdi grup tablolarının (elemanları f de verilen sırada yazdığımızda) aslında aynı olduğunu görelim.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\cdot$	1	i	-1	$-i$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	1	1	i	-1	$-i$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	i	i	-1	$-i$	1
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	-1	-1	$-i$	1	i
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$-i$	$-i$	1	i	-1

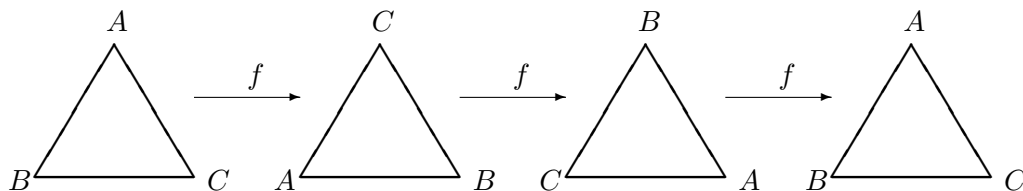
Benzer şekilde $G = \langle a \rangle = \{e, a, a^2, a^3\}$ 4-üncü mertebeden devirli grup ise $A \cong G$ dir. Bu şekildeki tüm grupların sınıfına 4-üncü mertebeden devirli grup denir ve hepsi de C_4 ile gösterilir. Genel olarak n -inci mertebeden devirli gruplar C_n ile gösterilir. Bu durumda $\mathbb{Z}_n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

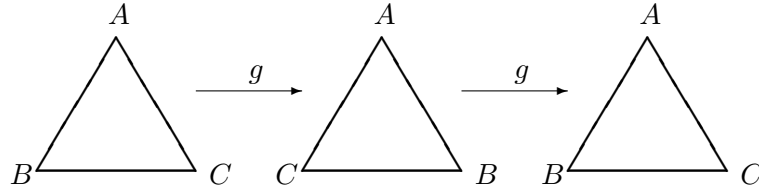
Not: 4 elemanlı olup da C_4 'e izomorfik olmayan bir grup vardır. Bu grupta, birim eleman hariç, bütün elemanların dereceleri 2'dir; yani her elemanın tersi kendisidir. Bu gruba **Klein-4 grubu** denir. Mesela, $\mathbb{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ bir Klein-4 grubudur.

Örnek 4.18 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 (yani e) olarak üçgenin orjinal hali anlaşılmaktadır.





Bu şekilde elde edeceğimiz bütün farklı dönmelerin kümesi $\{e, f, f^2, g, fg, f^2g\}$ 'dir. Bu şekilde elde ettiğimiz gruba **eşkenar üçgenin dihedral grubu** denir ve D_3 ile gösterilir. Benzer şekilde eşkenar n -genler kullanılarak elde edilen gruplar sınıfına **dihedral gruplar** denir ve bu gruplar D_n ile gösterilir. $|D_n| = 2n$ dir. Şimdi, $D_3 = \{e, f, f^2, g, fg, f^2g\}$ grubundan S_3 grubuna ϕ dönüşümünü

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

şeklinde tanımlarsak bir izomorfizma elde ederiz. O halde $D_3 \cong S_3$. Tablodaki boşlukları doldurun. (**İpucu:** $gf = f^2g$ eşitliğini kullanın)

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

Teorem 4.19 $f : G \longrightarrow H$ homomorfizmasının birebir olması için gerek ve yeter şart $\text{Çek}(f) = \{e\}$ olmasıdır.

İspat: ($\implies$) f birebir olsun. $f(x) = e_0$ 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.

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

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

olup f nin 1-1 olduğu gösterilmiş olur. □

Teorem 4.20 G, H, K birer grup olsun.

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

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

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

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 $g \circ f$ bir izomorfizmadır. □

Sonuç 4.21 G den G ye I_G birim dönüşümü bir izomorfizmadır. O halde her grup kendine izomorftir. Yukardaki teoremden $G \cong H \implies H \cong G$ ve $G \cong H, H \cong K \implies G \cong K$ olduğu gösterilmiştir. O halde gruplar üzerinde tanımlanan izomorfik olma bağıntısı bir denklik bağıntısıdır. Bu bağıntıya göre farklı gruplar (ilk 10 merteye için) Tablo 4.1'de verilmiştir.

Mertebe	Abelyen Gruplar	Abelyen Olmayan Gruplar	Toplam
1	C_1	–	1
2	C_2	–	1
3	C_3	–	1
4	C_4 ve $C_2 \times C_2$ (Klein-4)	–	2
5	C_5	–	1
6	C_6	S_3	2
7	C_7	–	1
8	$C_8, C_4 \times C_2$ ve $C_2 \times C_2 \times C_2$	Q_8 ve D_4	5
9	C_9 ve $C_3 \times C_3$	–	2
10	C_{10}	D_5	2
C_n : n -inci mertebeden devirli grup		D_n : eşkenar n -genin dihedral grubu	
Q_8 : Quaternionlar (Alıştırma 3.8)		S_3 : Permütasyon grubu (Örnek 1.16)	
$G \times H$: G ile H gruplarının “direkt çarpımı” (bu notlarda anlatılmamıştır)			

Tablo 4.1: İzomorfik olma bağıntısına göre 10. mertebeye kadar olan farklı gruplar.

Teorem 4.22 İki devirli grubun izomorfik olması için gerek ve yeter şart bu iki grubun mertebelerinin aynı olmasıdır.

İspat: ($\implies$) 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.)

($\impliedby$) 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.

$f(a^k) = f(a^t) \implies b^k = b^t$ 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 1.31). 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. $\square$

Tanım 4.23 Bir G grubundan kendi üzerine olan bir izomorfizmaya G nin bir **otomorfizması** denir. G nin bir $a \in G$ elemanı için $f_a : G \rightarrow G$, $f_a(x) = axa^{-1}$ 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 $\text{Oto}(G)$ nin bileşke işlemi ile bir grup olduğunu göstereceğiz. Bu gruba G nin **otomorfizmalar grubu** denir. Yani

$$\text{Oto}(G) = \{ f : G \rightarrow G \mid f, 1-1, \text{ örten bir homomorfizma } \}.$$

Teorem 4.24 G nin otomorfizmalarını kümesi $\text{Oto}(G)$ bileşke işlemi ile bir gruptur.

İspat: Teorem 4.20 gereğince iki otomorfizmanın bileşkesi bir otomorfizmadır. Ayrıca $f \in \text{Oto}(G) \implies f^{-1} \in \text{Oto}(G)$ dir. Birim dönüşüm bir otomorfizma olup $\text{Oto}(G)$ nin birim elemanıdır. Fonksiyonlardaki bileşke işleminin birleşme özelliği olup $\text{Oto}(G)$ bir grup olur. $\square$

Örnek 4.25 $A = \{ 1, -1, i, -i \}$ grubunun bütün otomorfizmalarını bulalım. I_A birim dönüşümü bir otomorfizmadır. $f \in \text{Oto}(A)$ 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

$$\begin{aligned} f(-1) &= f(ii) = f(i)f(i) = (-i)(-i) = -1 \\ f(-i) &= f(-1)f(i) = (-1)(-i) = i \end{aligned}$$

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

$\circ$	I_A	f
I_A	I_A	f
f	f	I_A

Örnek 4.26 G bir grup olsun. Bir $a \in G$ için $f_a : G \rightarrow G$, $f_a(x) = axa^{-1}$ 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

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

olup f_a birebirdir. Şimdi 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 $f_a \in \text{Oto}(G)$.

Teorem 4.27 $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$, n -inci mertebeden devirli grup olsun. $f_k : G \rightarrow G$, $f_k(a) = a^k$ olmak üzere

$$\text{Oto}(G) = \{f_k \mid 1 \leq k < n, (k, n) = 1\}.$$

İspat: $f \in \text{Oto}(G)$ olsun. $f(a) = a^k$ olsun. G nin üretici elemanları $1 \leq m < n$ 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 $f_k \in \text{Oto}(G)$ dir. Sonuç: $\text{Oto}(G) = \{f_k \mid 1 \leq k < n, (k, n) = 1\}$. $\square$

Örnek 4.28 $\mathbb{Z}_8$ 'in otomorfizmalar grubu olan $\text{Oto}(\mathbb{Z}_8)$ 'i belirleyiniz.

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

$f_1(\bar{0}) = 1 \cdot \bar{0} = \bar{0}$	$f_3(\bar{0}) = 3 \cdot \bar{0} = \bar{0}$	$f_5(\bar{0}) = 5 \cdot \bar{0} = \bar{0}$	$f_7(\bar{0}) = 7 \cdot \bar{0} = \bar{0}$
$f_1(\bar{1}) = 1 \cdot \bar{1} = \bar{1}$	$f_3(\bar{1}) = 3 \cdot \bar{1} = \bar{3}$	$f_5(\bar{1}) = 5 \cdot \bar{1} = \bar{5}$	$f_7(\bar{1}) = 7 \cdot \bar{1} = \bar{7}$
$f_1(\bar{2}) = 1 \cdot \bar{2} = \bar{2}$	$f_3(\bar{2}) = 3 \cdot \bar{2} = \bar{6}$	$f_5(\bar{2}) = 5 \cdot \bar{2} = \bar{2}$	$f_7(\bar{2}) = 7 \cdot \bar{2} = \bar{6}$
$f_1(\bar{3}) = 1 \cdot \bar{3} = \bar{3}$	$f_3(\bar{3}) = 3 \cdot \bar{3} = \bar{1}$	$f_5(\bar{3}) = 5 \cdot \bar{3} = \bar{7}$	$f_7(\bar{3}) = 7 \cdot \bar{3} = \bar{5}$
$f_1(\bar{4}) = 1 \cdot \bar{4} = \bar{4}$	$f_3(\bar{4}) = 3 \cdot \bar{4} = \bar{4}$	$f_5(\bar{4}) = 5 \cdot \bar{4} = \bar{4}$	$f_7(\bar{4}) = 7 \cdot \bar{4} = \bar{4}$
$f_1(\bar{5}) = 1 \cdot \bar{5} = \bar{5}$	$f_3(\bar{5}) = 3 \cdot \bar{5} = \bar{7}$	$f_5(\bar{5}) = 5 \cdot \bar{5} = \bar{1}$	$f_7(\bar{5}) = 7 \cdot \bar{5} = \bar{3}$
$f_1(\bar{6}) = 1 \cdot \bar{6} = \bar{6}$	$f_3(\bar{6}) = 3 \cdot \bar{6} = \bar{2}$	$f_5(\bar{6}) = 5 \cdot \bar{6} = \bar{6}$	$f_7(\bar{6}) = 7 \cdot \bar{6} = \bar{2}$
$f_1(\bar{7}) = 1 \cdot \bar{7} = \bar{7}$	$f_3(\bar{7}) = 3 \cdot \bar{7} = \bar{5}$	$f_5(\bar{7}) = 5 \cdot \bar{7} = \bar{3}$	$f_7(\bar{7}) = 7 \cdot \bar{7} = \bar{1}$

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

Örnek 4.29 Abelyen bir G grubunun iç otomorfizmalar kümesi $I(G)$ 'yi belirleyin.

Çözüm: G abelyen olduğundan, her $a \in G$ için $f_a : G \rightarrow G$, $f_a(x) = axa^{-1} = x$ olup $f_a = I_G$ özdeşlik dönüşümü olduğu görülür. O halde G abelyen ise $I(G) = \{I_G\}$ dir.

Teorem 4.30 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: $C_n = \{e, a, a^2, \dots, a^{n-1}\}$ olsun. $f : C_n \rightarrow \mathbb{Z}_n$ dönüşümünü her $k \in \mathbb{Z}$ için $f(a^k) = \bar{k}$ olarak tanımlayalım. Her $\bar{k} \in \mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ için $f(a^k) = \bar{k}$ olup f örtendir. ($a^0 = e$ kabul edildi.)

$$f(a^k) = f(a^m) \implies \bar{k} = \bar{m} \implies k \equiv m \pmod{n} \implies a^k = a^m$$

olup f 1-1 dir. Ayrıca

$$f(a^k a^m) = f(a^{k+m}) = \overline{k+m} = \bar{k} \oplus \bar{m} = f(a^k) \oplus f(a^m)$$

olup f bir homomorfizmadır. Sonuç olarak f bir izomorfizma olup $C_n \cong \mathbb{Z}_n$ dir.

Şimdi de $f : C_\infty \rightarrow \mathbb{Z}$ dönüşümünü her $k \in \mathbb{Z}$ için $f(a^k) = k$ şeklinde tanımlayalım.

$$f(a^n a^m) = f(a^{n+m}) = n + m = f(a^n) + f(a^m)$$

olup f bir homomorfizmadır. Ayrıca $f(a^n) = f(a^m) \implies n = m \implies a^n = a^m$ olduğu açıktır. Yani f 1-1 dir. Verilen her $y \in \mathbb{Z}$ için $x = a^y$ seçilirse $f(x) = y$ olacağından f örtendir. O halde $C_\infty \cong \mathbb{Z}$. $\square$

Örnek 4.31 G devirli ve mertebesi sonsuz olsun. Bu durumda G nin otomorfizmalar grubunu belirleyiniz.

Çözüm: G devirli olduğundan bir $a \in G$ için $G = \langle a \rangle$ dir. $f : G \rightarrow G$ bir $k \in \mathbb{Z}$ için $f(a) = a^k$ dir. 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.

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

elde edilir. $k = 1$ olduğunda $f(a) = a \implies f = I_G$ bulunur. $k = -1$ olduğunda $f(a) = a^{-1}$ dir. Yani

$$\text{Oto}(G) = \{I_G, f \mid \forall a \in G, f(a) = a^{-1}\}.$$

Örnek 4.32 $f : G \rightarrow S$ bir grup homomorfizması ve $\text{Çek}(f) = \{e\}$ 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. Şimdi $[f(a)]^n = e_0$ olacak şekilde $1 \leq n < m$ doğal sayısı olduğunu kabul edelim. O zaman $\implies [f(a)]^n = f(a^n) = e_0$ olup $\text{Çek}(f) = \{e\}$ olduğundan $a^n = e$ olur. Bu da $|a| = m$ olması ile çelişir. Buradan $|f(a)| = m$ elde edilir.

ALİŞTIRMALAR

1. $G = (\mathbb{Q} \setminus \{0\}, \cdot)$ olsun. $f : G \rightarrow G, f(x) = |x|$ şeklinde tanımlansın. f nin bir grup homomorfizması olduğunu gösterip $\text{Çek}(f)$ yi bulunuz ve $G/\text{Çek}(f)$ 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. $f : M^{2 \times 2} \rightarrow (\mathbb{R}, +)$ dönüşümü

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

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

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

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

6. $f : G \rightarrow H$ bir homomorfizma olsun. O zaman $N \leq G$ ise $f(N) \leq H$ dir. Ayrıca f örten ve $N \triangleleft G$ ise $f(N) \triangleleft H$ dir. Gösteriniz.

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

8. $f : G \rightarrow H$ bir grup homomorfizması olsun. $K \leq H$ ise $f^{-1}(K) \leq G$ olduğunu; daha sonra $K \triangleleft H$ ise $f^{-1}(K) \triangleleft G$ olduğunu gösterin.

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

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

ALİŞTIRMALARIN 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

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

ÇÖZÜM 2. $a_i, b_i, c_i, d_i \in \mathbb{R}$ olsun.

$$\begin{aligned} f\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right) &= f\left(\begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}\right) \\ &= (a_1 + a_2) + (d_1 + d_2) \\ &= (a_1 + d_1) + (a_2 + d_2) \\ &= f\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\right) + f\left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right) \end{aligned}$$

olup f bir homomorfizmadır.

$$\text{Çek}(f) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M^{2 \times 2} : a + d = 0 \right\} = \left\{ \begin{bmatrix} a & b \\ c & -a \end{bmatrix} : a, b, c \in \mathbb{R} \right\}$$

olur ve

$$M^{2 \times 2} / \text{Çek}(f) = \{ \text{Çek}(f) + A : A \in M^{2 \times 2} \}.$$

ÇÖZÜM 3. f bir grup homomorfizması olsun. Her $a, b \in G$ için

$$\begin{aligned} f(ab) = f(a)f(b) &\implies (ab)^{-1} = a^{-1}b^{-1} \\ &\implies (ab)^{-1} = (ba)^{-1} \\ &\implies ab = ba \end{aligned}$$

olup G nin abelyen olduğu görülür. Şimdi de G nin abelyen olduğunu kabul edip f nin homomorfizma olduğunu gösterelim.

$$f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b)$$

olup f bir homomorfizmadır.

ÇÖZÜM 4.

I.Durum: G sonlu ise f bir fonksiyon olmayabilir. Mesela $G = \langle x \rangle$ 6-ncı mertebeden devirli grup ise $x^2 = x^8$ dir fakat $f(x^8) = 8$ olup $f(x^2) = 2$ olur.

II.Durum: $G = \langle x \rangle$ sonsuz devirli grup ise

$$f(x^n x^m) = f(x^{n+m}) = n + m = f(x^n) + f(x^m)$$

olup f bir homomorfizmadır. $(\mathbb{Z}, +)$ nın birim elemanı 0 olup

$$\text{Çek}(f) = \{ x^n : f(x^n) = n = 0 \} = \{ x^0 \} = \{ e \}.$$

ÇÖZÜM 5. $z_1 = a + bi, z_2 = c + di$ iki kompleks sayı olsun.

$$\begin{aligned}
 \phi(z_1) = \phi(z_2) &\implies \phi(a + bi) = \phi(c + di) \\
 &\implies a - bi = c - di \\
 &\implies a = c, -b = -d \\
 &\implies a = c, b = d \\
 &\implies a + bi = c + di \\
 &\implies z_1 = z_2
 \end{aligned}$$

olup ϕ 'nin 1-1 olduğu gösterilmiş olur. Verilen her $z = a + bi \in \mathbb{C}$ için $w = a - bi$ seçilirse

$$\phi(w) = \phi(a - bi) = a + bi = z$$

olup ϕ örtendir. Şimdi de

$$\phi(z_1 + z_2) = \phi((a + c) + (b + d)i) = a + c - (b + d)i = (a - bi) + (c - di) = \phi(z_1) + \phi(z_2)$$

olup ϕ bir homomorfizmadır. Sonuç olarak ϕ bir otomorfizmadır.

ÇÖZÜM 6.

$$\begin{aligned}
 x, y \in f(N) &\implies \exists a, b \in N \text{ için } f(a) = x, f(b) = y \\
 &\implies ab^{-1} \in N \text{ olup } f(ab^{-1}) = f(a)f(b)^{-1} = xy^{-1} \\
 &\implies xy^{-1} \in f(N) \\
 &\implies \text{Teorem 2.8 den } f(N) \leq H.
 \end{aligned}$$

$$\begin{aligned}
 x \in f(N) &\implies \exists n \in N \text{ için } f(n) = x, \\
 h \in H &\implies f \text{ örten olduğundan } \exists g \in G \text{ için } f(g) = h \\
 &\implies f(\underbrace{gng^{-1}}_{\in N}) = f(g)f(n)f(g)^{-1} = h x h^{-1} \\
 &\implies h x h^{-1} \in f(N) \\
 &\implies f(N) \triangleleft H.
 \end{aligned}$$

ÇÖZÜM 7.

$$\phi((a + bi)(c + di)) = \phi(ac - bd + i(ad + bc)) = \begin{bmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{bmatrix},$$

$$\phi(a + bi)\phi(c + di) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{bmatrix}$$

olup ϕ nin bir homomorfizma olduğu görülür. ϕ örten değildir, çünkü $A = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}$ ise $\phi(a + bi) = A$ olacak şekilde $a + bi \in \mathbb{C}$ yoktur. O halde ϕ dönüşümü G ile H yi izomorfik yapamaz.

ÇÖZÜM 8. Önce $K \leq H \implies f^{-1}(K) \leq G$ olduğunu gösterelim.

$$\begin{aligned} x, y \in f^{-1}(K) &\implies \exists a, b \in K \text{ için } f(x) = a, f(y) = b \\ &\implies f(xy^{-1}) = f(x)f(y)^{-1} = ab^{-1} \in K \quad (\text{çünkü } K \leq H) \\ &\implies xy^{-1} \in f^{-1}(K) \\ &\implies \text{Teorem 2.8 den } f^{-1}(K) \leq G. \end{aligned}$$

Şimdi $x \in f^{-1}(K)$ ve $g \in G$ alalım. O halde en az bir $k \in K$ için $f(x) = k$ olmalıdır. Şimdi $f(g) \in H$ ve $K \triangleleft H$ olduğundan

$$\begin{aligned} f(g)kf(g)^{-1} \in K &\implies f(g)f(x)f(g)^{-1} \in K \\ &\implies f(gxg^{-1}) \in K \\ &\implies gxg^{-1} \in f^{-1}(K) \end{aligned}$$

olup $f^{-1}(K) \triangleleft G$ olduğu gösterilmiş olur.

ÇÖZÜM 9. $z_1 = x + iy, z_2 = a + bi$ iki kompleks sayı olsun.

$$\begin{aligned} \phi(z_1 z_2) &= \phi((ax - by) + i(ay + xb)) \\ &= |(ax - by) + i(ay + xb)| \\ &= \sqrt{(ax - by)^2 + (ay + xb)^2} \\ &= \sqrt{a^2x^2 + y^2b^2 - 2axyb + a^2y^2 + x^2b^2 + 2ayxb} \\ &= \sqrt{a^2(x^2 + y^2) + b^2(x^2 + y^2)} \\ &= \sqrt{a^2 + b^2} \sqrt{x^2 + y^2} \\ &= \phi(z_1)\phi(z_2) \end{aligned}$$

olup ϕ bir homomorfizmadır. ϕ 1-1 değildir, çünkü $z_1 = 3 + 4i$ ve $z_2 = 3 - 4i$ seçilirse $|z_1| = |z_2| = 5$, yani $\phi(z_1) = \phi(z_2)$ olup $z_1 \neq z_2$ dir. Yani bu dönüşüm G ile H yi izomorfik yapamaz.

ÇÖZÜM 10. Her $x, y \in \mathbb{R}$ için $f(x + y) = 5^{x+y} = 5^x 5^y = f(x)f(y)$ olup f homomorfizmadır. $f(x) = 1 \implies 5^x = 1 \implies x = 0$ olup $\text{Çek}(f) = \{0\}$ bulunur. Teorem 4.19 gereği f 1-1 dir. $y = -1 \in \mathbb{R}^*$ için $f(x) = 5^x = -1$ olacak şekilde $x \in \mathbb{R}$ olmadığından f örten değildir.

$$\mathbb{R}/\text{Çek}(f) = \{\text{Çek}(f) + a : a \in \mathbb{R}\} = \{\{a\} : a \in \mathbb{R}\}.$$

İzomorfizma Teoremleri

G bir grup olsun. Bir $N \triangleleft G$ için $f : G \longrightarrow G/N$ homomorfizmasının varlığını göstermiştik. Acaba bunun tersi de doğru mudur? Yani; G ve H birer grup olmak üzere $G/N \cong H$ olacak şekilde bir $N \triangleleft G$ normal alt grubu var mıdır?

Teorem 5.1 (1. İzomorfizma Teoremi) $f : G \longrightarrow H$ örten bir homomorfizma olsun. O zaman $G/\text{Çek}(f) \cong H$ dır.

İspat: İspat boyunca $K = \text{Çek}(f)$ diyelim.



Her $g \in G$ için $r(Kg) = f(g)$ şeklinde bir $r : G/K \longrightarrow H$ dönüşümü tanımlayalım. r 'nin bir izomorfizma olduğunu göstereceğiz.

i) r iyi tanımlanmıştır

Yani $X = Ka$ ve $X = Kb$ şeklinde yazıldığında $r(X) = f(a)$ ve $r(X) = f(b)$ olur. Bu durumda $f(a) = f(b)$ olduğunu göstermeliyiz. Şimdi K altgrup ve f homomorfizma olduğundan:

$$\begin{aligned}
 Ka = Kb &\implies Kab^{-1} = K \\
 &\implies ab^{-1} \in K = \text{Çek}(f) \\
 &\implies f(ab^{-1}) = e_H \\
 &\implies f(a)f(b)^{-1} = e_H \implies f(a) = f(b).
 \end{aligned}$$

ii) r homomorfizmadır

Her $X, Y \in G/K$ için $r(XY) = r(X)r(Y)$ olduğunu göstereceğiz. $X = Ka$ ve $Y = Kb$ şeklinde olsun.

$$\begin{aligned}
 r(XY) &= r(Ka \cdot Kb) \\
 &= r(Kab) \quad (\text{Çünkü } K \triangleleft G) \\
 &= f(ab) \\
 &= f(a)f(b) \quad (\text{Çünkü } f \text{ homomorfizma}) \\
 &= r(Ka)r(Kb) \\
 &= r(X)r(Y)
 \end{aligned}$$

olup r bir homomorfizmadır.

iii) r örtendir

Her $h \in H$ için $r(X) = h$ olacak şekilde bir $X \in G/K$ bulmalıyız. $h \in H$ verilsin. f örten olduğundan bir $a \in G$ için $h = f(a)$ dır. Şimdi $X = Ka$ seçersek, $r(X) = r(Ka) = f(a) = h$ olur. Yani r örtendir.

iv) r 1-1 dir

r nin çekirdeğinde sadece G/K nın birim elemanı olduğunu, yani $\text{Çek}(r) = \{K\}$ olduğunu gösterirsek r 1-1 olur. (İlgili teoremden). $X \in \text{Çek}(r)$ alalım $\implies X = Kg$ şeklindedir $\implies r(X) = e_H \implies r(Kg) = e_H \implies f(g) = e_H \implies g \in \text{Çek}(f) = K \implies X = Kg = K \implies \text{Çek}(r) = \{K\}$.

Sonuç olarak $G/K \cong H$ yazabiliriz.

Not 5.2 Bazı kaynaklarda aynı teorem “ $f : G \longrightarrow H$ bir homomorfizma ise $G/\text{Çek}(f) \cong f(G)$ ” şeklinde ifade edilmektedir. Bu ifade bizim ifademizin genel halidir; çünkü eğer f örten ise $f(G) = H$ olup aynı ifade elde edilir.

Örnek 5.3 $G = (\mathbb{Z}, +)$, $H = (\mathbb{Q} \setminus \{0\}, \cdot)$ ve $f : G \longrightarrow H$ dönüşümü her $x \in G$ için

$$f(x) = \begin{cases} 1, & x \text{ çift ise} \\ -1, & x \text{ tek ise} \end{cases}$$

şeklinde tanımlansın. $f : G \longrightarrow f(G)$ örten bir fonksiyondur. f nin bir homomorfizma olduğunu gösterelim. $x, y \in \mathbb{Z}$ verilsin.

Durum 1: x ve y çift $\implies f(x+y) = 1$ ve $f(x)f(y) = 1 \cdot 1 = 1$

Durum 2: x ve y tek $\implies f(x+y) = 1$ ve $f(x)f(y) = (-1) \cdot (-1) = 1$

Durum 3: x ve y nin biri tek biri çift $\implies f(x+y) = -1$ ve $f(x)f(y) = -1$.

Yani f bir homomorfizmadır.

$K = \text{Çek}(f) = \{x \in \mathbb{Z} \mid f(x) = 1\} = \{x \in \mathbb{Z} \mid x \text{ çift sayı}\} = 2\mathbb{Z}$ dir. K nın farklı sağ kosetleri

$$\{K + 0, K + 1\} \text{ olup } G/K = \{K + 0, K + 1\}.$$

$$\begin{array}{ccc} G & \xrightarrow{f} & f(G) = \{-1, 1\} \\ & \nearrow \psi & \\ & G/K & \end{array}$$

$\psi : G/K \rightarrow f(G)$ dönüşümünü $\psi(K+0) = 1, \psi(K+1) = -1$ şeklinde tanımlayalım. ψ bir izomorfizma olup $G/K \cong f(G)$ dir.

Örnek 5.4 G ve K herhangi iki grup olsun. $f : G \rightarrow K$ bir grup homomorfizması ve $|G|$ sonlu ise $|f(G)| \mid |G|$ dir, gösteriniz.

Çözüm:

$$\begin{array}{ccc} G & \xrightarrow{f \text{ hom.}} & f(G) \subseteq K \\ & \searrow & \nearrow \psi \\ & G/\text{Çek}(f) & \end{array}$$

Birinci İzomorfizma Teoremi'nden $G/\text{Çek}(f) \cong f(G)$ dir. G sonlu olduğundan $G/\text{Çek}(f)$ de sonludur. O halde $|G/\text{Çek}(f)| = |f(G)|$ olup Lagrange Teoremi'nden:

$$\frac{|G|}{|\text{Çek}(f)|} = |f(G)| \implies \frac{|G|}{|f(G)|} = |\text{Çek}(f)| \implies |f(G)| \mid |G|.$$

Örnek 5.5 $\mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \cdot)$ grubu olmak üzere $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$ olduğunu gösterin.

Çözüm: $G = GL_n(\mathbb{R})$ olsun. G 'nin matris çarpımına göre bir grup olduğunu biliyoruz. $f : G \rightarrow \mathbb{R}^*, f(X) = \det(X)$ şeklinde determinant fonksiyonu tanımlayalım.

$$X, Y \in G \implies f(XY) = \det(XY) = \det(X) \det(Y) = f(X)f(Y)$$

olup f bir homomorfizmadır.

$$\text{Çek}(f) = \{X \in G \mid f(X) = \det(X) = 1\} = SL_n(\mathbb{R})$$

elde ederiz. Ayrıca f örtendir, çünkü determinanti verilen bir reel sayı olan bir matris her zaman yazılabilir. O halde Birinci İzomorfizma Teoreminden

$$GL_n(\mathbb{R})/\text{Çek}(f) \cong \mathbb{R}^* \quad \text{yani} \quad GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*.$$

Teorem 5.6 (2. İzomorfizma Teoremi) G bir grup, $H \leq G$ ve $N \triangleleft G$ olsun. $H \cap N \triangleleft H$ ve $HN \leq G$ dir. Ayrıca $H/(H \cap N) \cong HN/N$ dir.

İspat:

$HN \leq G$ dir. $x = h_1n_1, y = h_2n_2 \in HN$ alalım.

$$\begin{aligned} xy^{-1} &= (h_1n_1)(h_2n_2)^{-1} = h_1 \underbrace{n_1n_2^{-1}}_{\in N} h_2^{-1} = h_1n_3h_2^{-1} \\ &= \underbrace{(h_1h_2^{-1})}_{\in H} \underbrace{(h_2n_3h_2^{-1})}_{\in N} \quad (\text{Çünkü } N \triangleleft G) \\ &= h_3n_4 \in HN \end{aligned}$$

olup Teorem 2.8'den $HN \leq G$ dir.

HN/N faktör grubunu oluşturmak için $N \triangleleft HN$ olduğunun gösterilmesi gerekir:

$N \triangleleft HN$ dir

Her $n \in N$ için $n = e \cdot n \in HN$ olduğundan $N \subseteq HN$ olduğu görülür. N ve HN her ikisi de altgrup olduğundan $N \leq HN$ dir. Şimdi $x \in N$ ve $hn \in HN$ alalım.

$$(hn) \cdot x \cdot (hn)^{-1} = h \underbrace{(n x n^{-1})}_{\in N} h^{-1} = h n_1 h^{-1} \in N \quad (\text{Çünkü } N \triangleleft G)$$

olduğundan $N \triangleleft HN$.

Şimdi $f : H \rightarrow HN/N$ dönüşümü her $h \in H$ için $f(h) = Nh$ şeklinde tanımlansın. **İddia:** f örten homomorfizmadır.

f örtendir:

$Nhn \in HN/N$ verilsin. $N \triangleleft G$ olduğundan $Nhn = hNn = hN = Nh = f(h)$ olup f örtendir.

f homomorfizmadır: Her $h_1, h_2 \in H$ için

$$\begin{aligned} f(h_1h_2) &= Nh_1h_2 = Nh_1Nh_2 \quad (N \triangleleft G \text{ olduğundan}) \\ &= f(h_1)f(h_2) \end{aligned}$$

olup f bir homomorfizmadır.

O halde Birinci İzomorfizma Teoremi'nden $H/\text{Çek}(f) \cong HN/N$ dir.

$\text{Çek}(f) = H \cap N$ dir

HN/N grubunun birim elemanı N dir.

$$\begin{aligned} \text{Çek}(f) &= \{x \in H \mid f(x) = N\} \\ &= \{x \in H \mid Nx = N\} \\ &= \{x \in H \mid x \in N\} \quad (Nx = N \iff x \in N) \\ &= H \cap N. \end{aligned}$$

Bir homomorfizmanın çekirdeği her zaman normal altgrup olduğundan $H \cap N \triangleleft H$ elde edilir.

Sonuç: $H/(H \cap N) \cong HN/N$

Teorem 5.7 (3. İzomorfizma Teoremi) G bir grup ve H ile K da G 'nin normal altgrupları ve ayrıca $K \leq H$ olsun. O zaman $H/K \triangleleft G/K$ dır ve

$$\frac{G/K}{H/K} \cong G/H.$$

İspat: Her $h \in H, k \in K$ için $hkh^{-1} \in K$ dır, çünkü $h \in G$ ve $K \triangleleft G$ dir. O halde $K \triangleleft H$ dir. Şimdi

$$\psi : G/K \longrightarrow G/H, \text{ her } Kg \in G/K \text{ için } \psi(Kg) = Hg$$

şeklinde tanımlayalım.

ψ iyi tanımlıdır: $Ka = Kb \implies ab^{-1} \in K \implies ab^{-1} \in H \implies Ha = Hb \implies \psi(Ka) = \psi(Kb)$.

ψ homomorfizmadır: $\psi(KaKb) = \psi(Kab) = Hab = HaHb = \psi(Ka)\psi(Kb)$.

ψ örtendir: Verilen her $Y = Ha \in G/H$ için $X = Ka \in G/K$ seçilirse $\psi(X) = \psi(Ka) = Ha = Y$ olur.

$\text{Çek}(\psi) = H/K$: G/H grubunun birim elemanı H dir. O halde

$$\begin{aligned} \text{Çek}(\psi) &= \{ Kx \in G/K : \psi(Kx) = Hx = H \} \\ &= \{ Kx \in G/K : x \in H \} \\ &= H/K \end{aligned}$$

bulunur. Bir homomorfizmanın çekirdeği her zaman normal altgrup olduğundan $H/K \triangleleft G/K$ elde edilir. Ayrıca, Birinci İzomorfizma Teoreminden

$$(G/K)/\text{Çek}(\psi) \cong G/H \quad \text{yani} \quad \frac{G/K}{H/K} \cong G/H. \quad \square$$

Şimdi, bir sonraki teoremde bazı maddeleri kullanılacak olan ve altgrupların görüntü ve ters görüntüleri ile ilgili sonuçları özetleyen bir lemmayı veriyoruz.

Lemma 5.8 $f : G \longrightarrow H$ bir homomorfizma, $A \leq G$ ve $B \leq H$ olsun.

- | | |
|---|-------------------------------|
| (a) $f(A) \leq H$ | (İspat: Bölüm 4, Alıştırma 6) |
| (b) $f^{-1}(B) \leq G$ | (İspat: Bölüm 4, Alıştırma 8) |
| (c) f örten ve $A \triangleleft G$ ise $f(A) \triangleleft H$ | (İspat: Bölüm 4, Alıştırma 6) |
| (d) $B \triangleleft H$ ise $f^{-1}(B) \triangleleft G$ | (İspat: Bölüm 4, Alıştırma 8) |

Teorem 5.9 (Eşleme Teoremi) $f : G \longrightarrow H$ örten bir grup homomorfizması olsun. O zaman G nin $\text{Çek}(f)$ yi içeren altgrupları ile H nin altgrupları arasındaki $A \longmapsto f(A)$ eşlemesi birebir ve örten bir eşlemedir. Ayrıca, bu eşleme normal altgrupları normal altgruplara eşler.

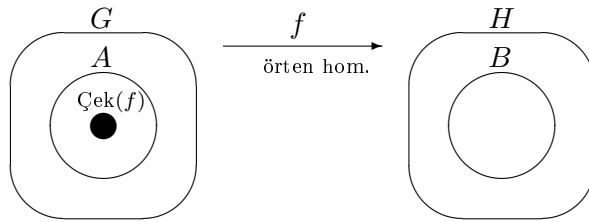
İspat: $A \leq G$ ve $\text{Çek}(f) \leq A$ olsun. Bu durumda $B = f(A) \leq H$ dir (Lemma 5.8.a). Bu eşlemenin birebir olduğunu gösterelim. Çekirdeği içeren başka bir $A_1 \leq G$ için $f(A_1) = B$ olsun. $A = A_1$ olduğunu gösterelim.

$$\begin{aligned} x \in A &\implies f(x) \in B \\ &\implies \exists y \in A_1, f(y) = f(x) \text{ (Çünkü } f(A_1) = B) \\ &\implies xy^{-1} \in \text{Çek}(f) \implies xy^{-1} \in A_1 \\ &\implies \exists u \in A_1, xy^{-1} = u \implies x = uy \in A_1 \end{aligned}$$

olup $A \subseteq A_1$ olduğu görülür. Benzer şekilde $A_1 \subseteq A$ olduğu ispatlanır. O halde bu eşleme 1-1 dir. Şimdi de bu eşlemenin örten olduğunu görelim. $B \leq H$ verilsin. $f^{-1}(B) \leq G$ dir (Lemma 5.8.b). $\text{Çek}(f) \subseteq f^{-1}(B)$ olduğu kolaylıkla görülür, çünkü:

$$k \in \text{Çek}(f) \implies f(k) = e_o \in B \implies k \in f^{-1}(B).$$

O halde verilen her $B \leq H$ altgrubu için $A = f^{-1}(B)$ seçersek, A kümesi, çekirdeği içeren bir altgrup olur ve $f(A) = f(f^{-1}(B)) = B$ olur. (Çünkü f örten olduğundan bir altkümenin ters görüntüsünün görüntüsü kendisidir.)



Buradan, bu eşlemenin tersi olan $B \longmapsto f^{-1}(B)$ eşlemesinin de 1-1 ve örten olduğunu söyleriz.

Şimdi, $A \triangleleft G \implies f(A) \triangleleft H$ olduğundan (Lemma 5.8.c) ve $B \triangleleft H \implies f^{-1}(B) \triangleleft G$ olduğundan (Lemma 5.8.d) bu eşlemenin normal altgrupları normal altgruplara eşlediği söylenebilir. $\square$

Örnek 5.10 $G = (\mathbb{Z}, +)$, $H = (\mathbb{Z}_6, \oplus)$ ve $f : G \longrightarrow H$, her $x \in \mathbb{Z}$ için $f(x) = \bar{x}$ şeklinde tanımlansın. f 'nin örten bir homomorfizma olduğu kolaylıkla gösterilebilir. $\text{Çek}(f) = 6\mathbb{Z}$ olup,

$$\begin{aligned} G\text{'nin } \text{Çek}(f)\text{'yi içeren altgrupları} & : A_1 = 6\mathbb{Z}, \quad A_2 = 2\mathbb{Z}, \quad A_3 = 3\mathbb{Z}, \quad A_4 = \mathbb{Z}. \\ \mathbb{Z}_6\text{'nın bütün altgrupları} & : B_1 = \{\bar{0}\}, \quad B_2 = \{\bar{0}, \bar{2}, \bar{4}\}, \quad B_3 = \{\bar{0}, \bar{3}\} \quad B_4 = \mathbb{Z}_6. \end{aligned}$$

Bütün altgruplar normal olup $i = 1, 2, 3, 4$ için $B_i = f(A_i)$ eşlemesinin 1-1 ve örten olduğu görülür.

Teorem 5.11 (4. İzomorfizma Teoremi) G bir grup ve $N \triangleleft G$ olsun. O zaman G 'nin N 'yi içeren altgruplarının kümesi ile G/N 'nin altgruplarının kümesi arasında $A \mapsto A/N$ eşlemesi 1-1 ve örtendir. Bu eşleme altında G 'nin normal altgrupları G/N 'nin normal altgrupları ile eşlenir.

İspat: $\psi : G \longrightarrow G/N, \psi(x) = Nx$ şeklinde tanımlanan kanonik homomorfizmayı düşünelim. Bu fonksiyonun; çekirdeği N olan örten bir homomorfizma olduğunu biliyoruz (Örnek 4.7).

$$\psi(A) = \{ \psi(a) : a \in A \} = \{ Na : a \in A \} = A/N$$

olup; Eşleme Teoreminde $H = G/N$ ve $f = \psi$ alırsak sonuç ortaya çıkar. $\square$

Teorem 5.12 $f : G \longrightarrow H$ örten homomorfizma olsun. $T \triangleleft H$ ve $S = \{ x \in G \mid f(x) \in T \}$ olsun. O zaman $G/S \cong H/T$ ve $G/S \cong (G/\text{Çek}(f))/(S/\text{Çek}(f))$.

İspat:

$$\begin{array}{ccc} f:G & \xrightarrow{\text{örten}} & H \\ & \searrow & \nearrow \\ & H/T & \end{array} \qquad \begin{array}{ccc} g & \xrightarrow{f} & f(g) \\ \psi \searrow & & \nearrow \eta \\ & Th= Tf(g) & \end{array}$$

$T \triangleleft H$ olduğundan $H \longrightarrow H/T$ bir η kanonik (doğal) homomorfizması vardır öyle ki $\eta(h) = Th$ dır. Şimdi $\psi : G \longrightarrow H/T$ dönüşümünü $\psi(g) = Tf(g)$ şeklinde tanımlayalım. **İddia:** ψ örten homomorfizmadır.

ψ örtendir:

$Th \in H/T$ verilsin. f örten olduğundan $\exists g' \in G$ için $f(g') = h$ dır. $\psi(g') = Tf(g') = Th$ olup ψ örtendir.

ψ homomorfizmadır: Her $g_1, g_2 \in G$ için,

$$\begin{aligned} \psi(g_1g_2) &= Tf(g_1g_2) \\ &= Tf(g_1)f(g_2) \\ &= Tf(g_1)Tf(g_2) \quad (T \triangleleft H \text{ olduğundan}) \\ &= \psi(g_1)\psi(g_2) \end{aligned}$$

olup ψ bir homomorfizmadır. Birinci İzomorfizma Teoremi'nden $G/\text{Çek}(\psi) \cong H/T$ dir.

$\text{Çek}(\psi) = S$ dir. H/T nin birim elemanı T olduğundan:

$$\text{Çek}(\psi) = \{ x \in G : \psi(x) = T \} = \{ x \in G : Tf(x) = T \} = \{ x \in G : f(x) \in T \} = S$$

olup $S = \text{Çek}(\psi)$ elde edilir.

Sonuç: $G/S \cong H/T$

Şimdi $S \triangleleft G$ ve $\text{Çek}(f) \triangleleft G$ dir. Ayrıca $\text{Çek}(f) \leq S$ olduğundan, Üçüncü İzomorfizma Teoreminden

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

elde edilir. □

Örnek 5.13 G bir grup ve $I(G), G$ nin iç otomorfizmalar grubu olsun. $I(G) \triangleleft \text{Oto}(G)$ ve $G/Z(G) \cong I(G)$ dir. ($Z(G) : G$ nin merkezi.)

Çözüm: $I(G) = \{t_a \mid a \in G, t_a : G \longrightarrow G, t_a(x) = axa^{-1}\}$ kümesi olduğunu hatırlayalım.

$I(G) \leq \text{Oto}(G)$ dir:

$t_a, t_b \in I(G)$ alalım. t_b otomorfizmasının tersi $t_{b^{-1}}$ dir. Çünkü:

$$t_b(t_{b^{-1}}(x)) = b(b^{-1}xb)b^{-1} = x \quad \text{ve} \quad t_{b^{-1}}(t_b(x)) = b^{-1}(bxb^{-1})b = x.$$

Şimdi:

$$\begin{aligned} [t_a(t_b)^{-1}](x) &= t_a[(t_b)^{-1}(x)] = t_a[t_{b^{-1}}(x)] \\ &= at_{b^{-1}}(x)a^{-1} = a(b^{-1}xb)a^{-1} \\ &= (ab^{-1})x(ba^{-1}) = cxc^{-1} \quad (c = ab^{-1} \text{ dersek}) \\ &= t_c(x) \end{aligned}$$

$\implies t_a(t_b)^{-1} \in I(G)$ olup, Teorem 2.8'den, $I(G) \leq \text{Oto}(G)$ dir.

$I(G) \triangleleft \text{Oto}(G)$ dir

Her $f \in \text{Oto}(G)$ ve $t_a \in I(G)$ için $ft_af^{-1} \in I(G)$ dir. Çünkü

$$\begin{aligned} (ft_af^{-1})(x) &= f(t_a(f^{-1}(x))) \\ &= f(a \cdot f^{-1}(x) \cdot a^{-1}) \\ &= f(a) \cdot f(f^{-1}(x)) \cdot f(a^{-1}) \\ &= f(a) \cdot x \cdot f(a)^{-1} \quad (\text{Çünkü } f \text{ hom., 1-1 ve örten}) \\ &= t_{f(a)}(x). \end{aligned}$$

$G/Z(G) \cong I(G)$ dir: $f : G \longrightarrow I(G), f(g) = t_g$ olarak tanımlayalım. **İddia:** f örten homomorfizmadır.

f örtendir: $t_g \in I(G)$ verilsin. $f(g) = t_g$ olup f örtendir.

f homomorfizmadır:

$$t_{ab}(x) = abxb^{-1}a^{-1} = t_a(bxb^{-1}) = t_a(t_b(x)) = [t_at_b](x)$$

olup $t_{ab} = t_at_b$ dir. Yani $f(ab) = t_{ab} = t_at_b = f(a)f(b)$ olur ve f bir homomorfizmadır. O halde Birinci İzomorfizma Teoremi'nden dolayı $G/\text{Çek}(f) \cong I(G)$ dir.

$\text{Çek}(f) = Z(G)$ dir. $I(G)$ 'nin birim elemanı, G 'nin birim dönüşümü olan I_G birim fonksiyonudur.

$$\begin{aligned}
 \text{Çek}(f) &= \{ a \in G : f(a) = t_a = I_G \} \\
 &= \{ a \in G : \forall x \in G, t_a(x) = I_G(x) \} \\
 &= \{ a \in G : \forall x \in G, axa^{-1} = x \} \\
 &= \{ a \in G : \forall x \in G, ax = xa \} \\
 &= Z(G)
 \end{aligned}$$

Sonuç: $G/Z(G) \cong I(G)$.

Ödev: $\psi : G/Z(G) \longrightarrow I(G), \psi(Z(G) \cdot g) = t_g$ dönüşümünün iyi tanımlı olduğunu ve izomorfizma olduğunu gösterip yukardaki örneği diğer bir yolla (Birinci İzomorfizma Teoremini kullanmadan) çözünüz.

ALIŞTIRMALAR

1. $\phi : \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_3$ örten homomorfizması $\phi(\bar{1}) = \bar{2}$ şeklinde veriliyor. **a)** $K = \text{Çek}(\phi)$ alt grubunu bulunuz. **b)** $\mathbb{Z}_{12}/K$ grubunu bulunuz. **c)** $\psi : \mathbb{Z}_{12}/K \longrightarrow \mathbb{Z}_3$ bir izomorfizma bulunuz.
2. $G = \mathbb{Z}_{24}$ olsun. $H = \langle \bar{4} \rangle \leq \mathbb{Z}_{24}$ ve $N = \langle \bar{6} \rangle \triangleleft \mathbb{Z}_{24}$ olarak verilsin. Bu durumda **(a)** $H \oplus N \leq \mathbb{Z}_{24}$, **(b)** $N \triangleleft (H \oplus N)$, **(c)** $H/(H \cap N) \cong (H \oplus N)/N$ olduğunu gösteriniz.
3. $G = \mathbb{Z}_{24}$ olsun. $H = \langle \bar{4} \rangle$ ve $K = \langle \bar{8} \rangle$ altgrupları verilsin. $G/H, G/K$ ve H/K faktör gruplarını yazın. $(G/K)/(H/K)$ faktör grubunu yazıp G/H 'a izomorfik olduğunu gösterin.
4. $G = \mathbb{Z}_{12}, H = \mathbb{Z}_4$ olsun. $f : G \longrightarrow H, f(\bar{1}) = \bar{1}$ olacak şekilde örten bir homomorfizma verilsin. $T = \langle \bar{2} \rangle \triangleleft \mathbb{Z}_4$ ve $S = \{ x : f(x) \in T \}$ olsun. $G/S \cong H/T$ olduğunu gösteriniz.
5. Abelyen olmayan bir grubun en az iki tane iç otomorfizmasının olduğunu ispatlayın.
6. $\phi : \mathbb{Z}_{18} \longrightarrow \mathbb{Z}_{18}, \phi(\bar{1}) = \bar{10}$ şeklinde bir homomorfizma veriliyor. $\text{Çek}(\phi)$ yi bulup Birinci İzomorfizma Teoremini uygulayın.

ALİŞTIRMALARIN ÇÖZÜMLERİ

ÇÖZÜM 1. $\phi(\bar{1}) = \bar{2}$ eşitliği verildiğinden, diğer elemanların görüntüleri $\phi(a \oplus b) = \phi(a) \oplus \phi(b)$ kuralıyla şöyle bulunur:

$$\phi : \begin{cases} \bar{0} \mapsto \bar{0} & \bar{6} \mapsto \bar{0} \\ \bar{1} \mapsto \bar{2} & \bar{7} \mapsto \bar{2} \\ \bar{2} \mapsto \bar{1} & \bar{8} \mapsto \bar{1} \\ \bar{3} \mapsto \bar{0} & \bar{9} \mapsto \bar{0} \\ \bar{4} \mapsto \bar{2} & \bar{10} \mapsto \bar{2} \\ \bar{5} \mapsto \bar{1} & \bar{11} \mapsto \bar{1} \end{cases}$$

a) $K = \text{Çek}(\phi) = \{x \in \mathbb{Z}_{12} \mid \phi(x) = \bar{0}\} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$

b) $K \oplus \bar{1} = \{\bar{1}, \bar{4}, \bar{7}, \bar{10}\}$, $K \oplus \bar{2} = \{\bar{2}, \bar{5}, \bar{8}, \bar{11}\}$ ve $K \oplus \bar{0} = K$ farklı sağ kosetlerdir. Yani

$$\mathbb{Z}_{12}/K = \{K, K \oplus \bar{1}, K \oplus \bar{2}\}.$$

c)

$$\begin{array}{ccc} \mathbb{Z}_{12} & \xrightarrow{\phi} & \mathbb{Z}_3 \\ & \searrow \psi & \nearrow \\ & \mathbb{Z}_{12}/K & \end{array}$$

$\psi(K \oplus \bar{0}) = \phi(\bar{0}) = \bar{0}$, $\psi(K \oplus \bar{1}) = \phi(\bar{1}) = \bar{2}$, $\psi(K \oplus \bar{2}) = \phi(\bar{2}) = \bar{1}$ şeklinde tanımlayalım. Birinci İzomorfizma Teoreminden, ψ iyi tanımlanmış 1-1 ve örten bir homomorfizmadır.

ÇÖZÜM 2. a) $H = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}, \bar{12}, \bar{16}, \bar{20}\}$ ve $N = \langle \bar{6} \rangle = \{\bar{0}, \bar{6}, \bar{12}, \bar{18}\}$ bulunur.

$$H \oplus N = \{h \oplus n \mid h \in H, n \in N\} = \{\bar{0}, \bar{6}, \bar{12}, \bar{18}, \bar{4}, \bar{10}, \bar{16}, \bar{22}, \bar{8}, \bar{14}, \bar{20}, \bar{2}\}$$

elde edilir. Bu küme kapalı olduğundan $(H \oplus N) \leq \mathbb{Z}_{24}$ dir.

Çözüm: b) $N \subseteq (H \oplus N)$ olduğu açıktır. Her ikisi de grup olduğundan $N \leq (H \oplus N)$ dir ve $H \oplus N$ abelyen olduğundan $N \triangleleft (H \oplus N)$ elde edilir.

Çözüm: c) $(H \oplus N)/N = \{N \oplus m \mid m \in H \oplus N\} = \{N, N \oplus \bar{4}, N \oplus \bar{8}\}$ bölüm grubudur. Şimdi

$$f : H \longrightarrow (H \oplus N)/N, \quad f(h) = N \oplus h$$

şeklinde tanımlayalım. f örten bir homomorfizmadır. (İkinci İzomorfizma Teoreminden). $f(\bar{0}) = f(\bar{12}) = N$, $f(\bar{4}) = f(\bar{16}) = N \oplus \bar{4}$, $f(\bar{8}) = f(\bar{20}) = N \oplus \bar{8}$ dir. $\text{Çek}(f) = \{h \in H \mid f(h) = N\} = \{\bar{0}, \bar{12}\}$ olur. Yani $\text{Çek}(f) = H \cap N$ elde edilir. Birinci İzomorfizma Teoreminden:

$$H/\text{Çek}(f) \cong (H \oplus N)/N \text{ yani } H/(H \cap N) \cong (H \oplus N)/N.$$

ÇÖZÜM 3. $G = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{23}\}$, $H = \{\bar{0}, \bar{4}, \bar{8}, \bar{12}, \bar{16}, \bar{20}\}$, $K = \{\bar{0}, \bar{8}, \bar{16}\}$ bulunur. İstenen faktör grupları:

$$\begin{aligned} G/H &= \{H \oplus \bar{0}, H \oplus \bar{1}, H \oplus \bar{2}, H \oplus \bar{3}\} \\ G/K &= \{K \oplus \bar{0}, K \oplus \bar{1}, K \oplus \bar{2}, K \oplus \bar{3}, K \oplus \bar{4}, K \oplus \bar{5}, K \oplus \bar{6}, K \oplus \bar{7}\} \\ H/K &= \{K \oplus \bar{0}, K \oplus \bar{4}\}. \end{aligned}$$

Şimdi $H/K \triangleleft G/K$ olduğundan

$$\begin{aligned} (G/K)/(H/K) &= \{(H/K) \oplus X : X \in G/K\} \\ &= \{(H/K) \oplus (K \oplus \bar{0}), (H/K) \oplus (K \oplus \bar{1}), (H/K) \oplus (K \oplus \bar{2}), (H/K) \oplus (K \oplus \bar{3})\}. \end{aligned}$$

Şimdi $\psi : G/K \longrightarrow G/H$, her $K \oplus g \in G/K$ için $\psi(K \oplus g) = H \oplus g$ şeklinde tanımlayalım. Şimdi ψ fonksiyonunu bulalım.

$$\psi : \begin{cases} K \oplus \bar{0} \mapsto H \oplus \bar{0} & K \oplus \bar{4} \mapsto H \oplus \bar{4} = H \oplus \bar{0} \\ K \oplus \bar{1} \mapsto H \oplus \bar{1} & K \oplus \bar{5} \mapsto H \oplus \bar{5} = H \oplus \bar{1} \\ K \oplus \bar{2} \mapsto H \oplus \bar{2} & K \oplus \bar{6} \mapsto H \oplus \bar{6} = H \oplus \bar{2} \\ K \oplus \bar{3} \mapsto H \oplus \bar{3} & K \oplus \bar{7} \mapsto H \oplus \bar{7} = H \oplus \bar{3} \end{cases}$$

Üçüncü İzomorfizma Teoremine göre ψ iyi tanımlıdır ve örten bir homomorfizmadır. O halde Birinci İzomorfizma Teoreminden $(G/K)/\text{Çek}(\psi) \cong G/H$ dır. G/H nin birim elemanı $H = H \oplus \bar{0}$ olduğundan

$$\text{Çek}(\psi) = \{X \in G/K : \psi(X) = H \oplus \bar{0}\} = \{K \oplus \bar{0}, K \oplus \bar{4}\} = H/K$$

olup $(G/K)/(H/K) \cong G/H$ elde edilir.

ÇÖZÜM 4.

$T = \{\bar{0}, \bar{2}\}$ olup $H/T = \{T \oplus \bar{0}, T \oplus \bar{1}\}$ dir. $\psi : G \longrightarrow H/T = \mathbb{Z}_4/\langle \bar{2} \rangle$ dönüşümünü

$$\psi(g) = T \oplus f(g)$$

şeklinde tanımlayalım. Önce f yi bulalım:

$$\begin{aligned} f(\bar{0}) &= f(\bar{4}) = f(\bar{8}) = \bar{0}, & f(\bar{1}) &= f(\bar{5}) = f(\bar{9}) = \bar{1}, \\ f(\bar{2}) &= f(\bar{6}) = f(\bar{10}) = \bar{2}, & f(\bar{3}) &= f(\bar{7}) = f(\bar{11}) = \bar{3}. \end{aligned}$$

Şimdi ψ yi bulalım.

$$\psi : \begin{cases} \bar{0} \mapsto T \oplus \bar{0} & \bar{4} \mapsto T \oplus \bar{0} & \bar{8} \mapsto T \oplus \bar{0} \\ \bar{1} \mapsto T \oplus \bar{1} & \bar{5} \mapsto T \oplus \bar{1} & \bar{9} \mapsto T \oplus \bar{1} \\ \bar{2} \mapsto T \oplus \bar{0} & \bar{6} \mapsto T \oplus \bar{0} & \bar{10} \mapsto T \oplus \bar{0} \\ \bar{3} \mapsto T \oplus \bar{1} & \bar{7} \mapsto T \oplus \bar{1} & \bar{11} \mapsto T \oplus \bar{1} \end{cases}$$

Teorem 5.12'den ψ örten bir homomorfizmadır.

$$\text{Çek}(\psi) = \{x \in \mathbb{Z}_{12} \mid \psi(x) = T\} = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\} = S$$

bulunur.

$$\begin{array}{ccc}
G & \xrightarrow{\psi} & H/T \\
& \searrow & \nearrow \\
& G/S &
\end{array}$$

Birinci İzomorfizma Teoremi'nden $G/S \cong H/T = \mathbb{Z}_4 / \langle \bar{2} \rangle$ elde edilir.

ÇÖZÜM 5. G abelyen olmayan bir grup olsun. O zaman $G \neq Z(G)$ olup $G/Z(G)$ en az iki elemanlı bir gruptur. $G/Z(G) \cong I(G)$ olduğundan $I(G)$ iç otomorfizmalar grubu da en az iki elemalıdır. O halde G nin en az iki tane iç otomorfizması vardır.

ÇÖZÜM 6. ϕ homomorfizmasının aşağıdaki gibi eşleme yaptığı görülür:

$$\phi : \begin{cases} \bar{0} \mapsto \bar{0} & \bar{6} \mapsto \bar{6} & \bar{12} \mapsto \bar{12} \\ \bar{1} \mapsto \bar{10} & \bar{7} \mapsto \bar{16} & \bar{13} \mapsto \bar{4} \\ \bar{2} \mapsto \bar{2} & \bar{8} \mapsto \bar{8} & \bar{14} \mapsto \bar{14} \\ \bar{3} \mapsto \bar{12} & \bar{9} \mapsto \bar{0} & \bar{15} \mapsto \bar{6} \\ \bar{4} \mapsto \bar{4} & \bar{10} \mapsto \bar{10} & \bar{16} \mapsto \bar{16} \\ \bar{5} \mapsto \bar{14} & \bar{11} \mapsto \bar{2} & \bar{17} \mapsto \bar{8} \end{cases}$$

Burada ϕ örten olmadığından $\mathbb{Z}_{18}/\text{Çek}(\phi) \cong \phi(\mathbb{Z}_{18})$ olduğu gösterilecektir.

$$K = \text{Çek}(\phi) = \{x \in \mathbb{Z}_{18} : \phi(x) = \bar{0}\} = \{\bar{0}, \bar{9}\}$$

bulunur. Ayrıca bölüm grubu

$$\mathbb{Z}_{18}/K = \{K \oplus \bar{0}, K \oplus \bar{1}, K \oplus \bar{2}, K \oplus \bar{3}, K \oplus \bar{4}, K \oplus \bar{5}, K \oplus \bar{6}, K \oplus \bar{7}, K \oplus \bar{8}\}$$

olarak bulunur. $r : \mathbb{Z}_{18}/K \longrightarrow \phi(\mathbb{Z}_{18})$ fonksiyonu $r(K \oplus x) = \phi(x)$ şeklinde tanımlanır. r fonksiyonunun aşağıdaki gibi eşleme yaptığı görülür:

$$r : \begin{cases} K \oplus \bar{0} \mapsto \bar{0} & K \oplus \bar{3} \mapsto \bar{12} & K \oplus \bar{6} \mapsto \bar{6} \\ K \oplus \bar{1} \mapsto \bar{10} & K \oplus \bar{4} \mapsto \bar{4} & K \oplus \bar{7} \mapsto \bar{16} \\ K \oplus \bar{2} \mapsto \bar{2} & K \oplus \bar{5} \mapsto \bar{14} & K \oplus \bar{8} \mapsto \bar{8} \end{cases}$$

Tablodan, r nin 1-1 ve örten olduğu görülmektedir. Birinci İzomorfizma Teoreminden dolayı r bir izomorfizma olup $\mathbb{Z}_{18}/K \cong \phi(\mathbb{Z}_{18})$ dir.

Permütasyon Grupları

Tanım 6.1 $M \neq \emptyset$ bir küme olsun. $P(M)$ ile M nin tüm permütasyonlarının (M den M ye 1-1 ve örten fonksiyonların) kümesini gösterelim. $P(M)$ bileşke işlemi ile bir gruptur. Çünkü:

- i) $f, g \in P(M)$ ise $f \circ g \in P(M)$ dir; çünkü 1-1 ve örten iki fonksiyonun bileşkesi 1-1 ve örtendir.
- ii) Fonksiyonlardaki bileşke işleminin birleşme özelliği vardır.
- iii) $I_M : M \longrightarrow M$ birim dönüşümü 1-1 ve örten olup bileşke işleminin birim elemanıdır.
- iv) $f \in P(M)$ ise, 1-1 ve örten bir fonksiyonunu tersi de 1-1 ve örten olduğundan $f^{-1} \in P(M)$ dir.

Eğer $|M| = n$ sonlu ise $P(M) = S_n$ ile gösterilir ve S_n grubuna n -inci dereceden **simetrik grup** denir. S_n in bir alt grubuna da bir **permütasyon grubu** denir. $|S_n| = n!$ olduğu açıktır.

$M = \{a_1, a_2, \dots, a_n\}$ diyelim. $f \in S_n$ elemanını 2 satırlı ve n sütunlu bir matris halinde aşağıdaki gibi göstereceğiz:

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ f(a_1) & f(a_2) & \dots & f(a_n) \end{pmatrix}.$$

O zaman, mesela,

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}.$$

permütasyonu I_M birim permütasyonudur.

Permütasyon grupları gruplar teorisinin önemli konularındandır, çünkü her G sonlu grubunun aslında bir permütasyon grubuna izomorfik olduğu 1878'de Arthur Cayley (1821-1895) tarafından gösterilmiştir.

Teorem 6.2 (Cayley) Her G grubu $P(G)$ permütasyonlar grubunun bir altgrubuna izomorfiktir. Özel

olarak; n elemanlı bir grup S_n in bir altgrubuna izomorftir.

İspat: Her $a \in G$ için $h_a : G \rightarrow G$ dönüşümünü $h_a(x) = ax$ şeklinde tanımlayalım. (Yani h_a dönüşümü “soldan a ile çarpmak” dönüşümüdür.) h_a dönüşümü G nin bir permütasyonudur, çünkü:

$$\begin{aligned} h_a(x) = h_a(y) &\implies ax = ay \implies x = y \implies h_a \text{ birebirdir.} \\ y \in G &\implies x = a^{-1}y \text{ seçilirse } h_a(x) = a(a^{-1}y) = y \implies h_a \text{ örtendir.} \end{aligned}$$

Şimdi $f : G \rightarrow P(G)$ dönüşümünü her $a \in G$ için $f(a) = h_a$ şeklinde tanımlayalım. f nin 1-1 homomorfizma olduğunu göstereceğiz. f birebirdir, çünkü $a, b \in G$ için

$$\begin{aligned} f(a) = f(b) &\implies h_a = h_b \\ &\implies \forall x \in G, h_a(x) = h_b(x) \\ &\implies \forall x \in G, ax = bx \\ &\implies a = b. \end{aligned}$$

f bir homomorfizmadır, çünkü $a, b \in G$ ise her $x \in G$ için

$$\begin{aligned} [f(ab)](x) &= h_{ab}(x) = (ab)x \\ &= a(bx) = h_a(bx) \\ &= h_a(h_b(x)) = (h_a h_b)(x) \\ &= [f(a)f(b)](x) \end{aligned}$$

olup $f(ab) = f(a)f(b)$ dir. Sonuç olarak $f : G \rightarrow P(G)$ birebir homomorfizmadır. $f : G \rightarrow f(G)$ izomorfizma ve $f(G) \leq P(G)$ olduğundan $G \cong f(G)$ olur. Yani G grubu $P(G)$ nin bir alt grubuna izomorftir. $\square$

Örnek 6.3 $G = \{1, -1, i, -i\}$ çarpma işlemi ile bir gruptur. Buna göre

$$\begin{aligned} h_1 &= \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix}, h_{(-1)} = \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix} \\ h_i &= \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix}, h_{(-i)} = \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix} \end{aligned}$$

permütasyonlarını yazalım. Bunlar $P(G)$ nin $4! = 24$ permütasyonundan 4 tanesidir. Bu permütasyonlar $P(G)$ nin bir alt grubunu oluştururlar, çünkü çarpım (bileşke) tablosu kapalıdır:

$\cdot$	h_1	$h_{(-1)}$	h_i	$h_{(-i)}$
h_1	h_1	$h_{(-1)}$	h_i	$h_{(-i)}$
$h_{(-1)}$	$h_{(-1)}$	h_1	$h_{(-i)}$	h_i
h_i	h_i	$h_{(-i)}$	$h_{(-1)}$	h_1
$h_{(-i)}$	$h_{(-i)}$	h_i	h_1	$h_{(-1)}$

Bu grup tablosunda h sembollerini sildiğimizde aslında G nin grup tablosunu elde ederiz. Başka bir deyişle $f : G \rightarrow f(G), f(a) = h_a$ dönüşümü bir izomorfizmadır.

Permütasyonların Devirsel Gösterimi

Bu kısımda permütasyonları daha kısa bir şekilde göstermenin bir şeklini göreceğiz. Bilindiği gibi S_n, n elemanlı bir M kümesinin bütün permütasyonlarının grubudur. Burada, aslında M nin elemanlarının ne olduğu değil de eleman sayısı önemli olduğundan genelde $M = \{1, 2, \dots, n\}$ alınır.

$\alpha \in S_n$ olsun. Eğer α permütasyonu

$$\alpha = \begin{pmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_2 & a_3 & \dots & a_n & a_1 \end{pmatrix}$$

şeklinde ise α ya **uzunluğu n olan bir devir** (veya kısaca **n -li devir**) denir ve $\alpha = (a_1, a_2, \dots, a_n)$ şeklinde gösterilir. Dikkat edilecek olursa α permütasyonu yazılırken a_1 den başlanmak zorunda değildir; mesela

$$\alpha = \begin{pmatrix} a_2 & a_3 & \dots & a_{n-1} & a_n & a_1 \\ a_3 & a_4 & \dots & a_n & a_1 & a_2 \end{pmatrix}$$

olup $\alpha = (a_2, a_3, \dots, a_n, a_1)$ şeklinde de yazılabilir. O halde, n -li bir devirin n farklı yazılışı vardır. Mesela aşağıdaki $\sigma \in S_5$ permütasyonu 5 değişik şekilde yazılabilir:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = (1, 3, 4, 2, 5) = (3, 4, 2, 5, 1) = (4, 2, 5, 1, 3) = (2, 5, 1, 3, 4) = (5, 1, 3, 4, 2).$$

Genelde bir $f \in S_n$ permütasyonu bir n -li devir değildir. Bu durumda f birden fazla “devir” den oluşmaktadır. O halde “devir” tanımının verilmesi gerekmektedir:

Tanım 6.4 $f \in S_n$ olsun ve $M = \{1, 2, \dots, n\}$ alalım. Herhangi bir $a \in M$ alalım. M sonlu olduğundan $f^m(a) = a$ şartını sağlayan bir en küçük $m \in \mathbb{Z}^+$ vardır. Bu durumda

$$(a, f(a), f^2(a), \dots, f^{m-1}(a))$$

sıralı kümesine f nin bir **devri** denir. Bu devir yazılırken a dan başlanması gerekmez. f permütasyonu bu şekilde bir veya daha fazla ayrık devirlerden oluşmaktadır. Bu ayrık devirler yanyana yazılarak elde edilen gösterime f ’nin **devirsel gösterimi** denir.

Örnek 6.5 Aşağıdaki S_9 un elemanı olan σ permütasyonunu ele alalım.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 4 & 9 & 2 & 1 & 7 & 6 & 3 \end{pmatrix}$$

Şimdi σ permütasyonunda 4 farklı devir vardır:

$$\begin{array}{llll} a = 1 \text{ alınır} & m = 3 \text{ bulunur} & \text{ve } (1, 8, 6) & \text{devri elde edilir} \\ a = 2 \text{ alınır} & m = 2 \text{ bulunur} & \text{ve } (2, 5) & \text{devri elde edilir} \\ a = 3 \text{ alınır} & m = 3 \text{ bulunur} & \text{ve } (3, 4, 9) & \text{devri elde edilir} \\ a = 7 \text{ alınır} & m = 1 \text{ bulunur} & \text{ve } (7) & \text{devri elde edilir} \end{array}$$

Eğer $a = 4$ alınsaydı $(4, 9, 3)$ devri bulunurdu; ki bu da $(3, 4, 9)$ devrine eşittir. O halde σ nın devirsel gösterimi şöyledir:

$$\sigma = (1, 8, 6)(2, 5)(3, 4, 9)(7).$$

Bu gösterim tek türlü değildir. Devirler yazılırken sıraları değişebilir. Ayrıca, mesela, $(1, 8, 6)$ devri $(8, 6, 1)$ veya $(6, 1, 8)$ şeklinde 3 türlü yazılabilir. Bu durumda σ toplamda, $(3 \cdot 2 \cdot 3) \cdot 4! = 432$ farklı şekilde yazılabilir. Bunlardan bazıları:

$$\sigma = (5, 2)(8, 6, 1)(7)(4, 9, 3) = (7)(6, 1, 8)(9, 3, 4)(2, 5) = (3, 4, 9)(2, 5)(7)(8, 6, 1) = \dots$$

Not 6.6 Bir permütasyonu devirsel gösterimde yazarken, uzunluğu 1 olan devirler yazılmayabilir; ancak bu durumda bu permütasyonun hangi simetrik grubun elemanı olduğunun belirtilmemesi (veya bilinmemesi) karışıklığa yol açabilir. Mesela $(1, 2, 3)$ permütasyonu aşağıdaki 3 farklı permütasyona eşit olabilir.

$$(1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ veya } (1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \text{ veya } (1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}.$$

S_n deki birim eleman sadece 1-li devirlerden oluştuğu için bu 1-li devirlerin hiçbirinin yazılmaması olmaz. Bu yüzden birim elemanı göstermek için $(1) \in S_n$ sembolünü kullanacağız. Aslında her $k \in \{1, 2, \dots, n\}$ için (k) birim elemanı ifade eder. Ayrıca devirsel gösterimde, eğer bir karışıklığa yol açmayacaksa, semboller arasında virgül kullanılmayabilir.

Örnek 6.7 $f = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_2 & a_1 & a_3 & \dots & a_n \end{pmatrix}$ permütasyonu sadece a_1 ve a_2 elemanlarını değiştirip diğerlerini sabit bırakır. Bu durumda $f = (a_1, a_2)$ yazılır.

Örnek 6.8 $\alpha = \begin{pmatrix} a & b & c & d & e & f \\ b & a & c & d & f & e \end{pmatrix} = (ab)(ef)$

$$\beta = \begin{pmatrix} a & b & c & d & e & f \\ b & a & c & e & f & d \end{pmatrix} = (ab)(def)$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{pmatrix} = (16)(243)$$

Not 6.9 Permütasyonların çarpımı soldan sağa doğru yapılmaktadır. Örneğin, $(1\ 2)$ ile $(1\ 3)$ permütasyonunun çarpımı $(1\ 2\ 3)$ dür:

$$(1\ 2) \cdot (1\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$

Bazı yazarlar fonksiyonlardaki bileşke alma işlemindeki sırayı takip edip bu çarpımı sağdan sola doğru yapmaktadır. Yani $(1\ 2) \circ (1\ 3) = (1\ 3\ 2)$ şeklinde. Buna göre f ve g iki permütasyon ise bir x elemanın f ile g nin çarpımındaki (bileşkesindeki) değeri $(fg)(i) = g(f(i))$ şeklinde hesaplanır. Bir x elemanın bir f fonksiyonundaki değerini $f(x)$ yerine xf şeklinde gösterenler için permütasyonları soldan sağa doğru çarpmak daha kolaydır: $x(fg) = (xf)g$.

Örnek 6.10

$$\begin{aligned} (1\ 2) \cdot (1\ 4\ 5\ 3) &= (1\ 2\ 4\ 5\ 3) \\ (2\ 6\ 3\ 4) \cdot (1\ 2\ 5) &= (1\ 2\ 6\ 3\ 4\ 5) \\ (1\ 2) \cdot (2\ 5) \cdot (5\ 1) &= (1)(2\ 5)(3)(4) = (2\ 5) \\ (1\ 6) \cdot (2\ 4\ 5\ 3) \cdot (1\ 2\ 4\ 9) &= (1\ 6\ 2\ 9)(3\ 4\ 5)(7)(8) = (1\ 6\ 2\ 9)(3\ 4\ 5) \\ (1\ 2\ 3\ 4\ 5) \cdot (5\ 4\ 3\ 2\ 1) &= (1)(2)(3)(4)(5) = (1) \end{aligned}$$

Lemma 6.11

a) $f = (a_1, a_2, \dots, a_r) \implies f^{-1} = (a_r, a_{r-1}, \dots, a_2, a_1)$

b) Ayırık devirlerin çarpımı değişmelidir. Yani $\{a_1, a_2, \dots, a_r\}$ ve $\{b_1, b_2, \dots, b_s\}$ kümeleri ayırık ise

$$(a_1, a_2, \dots, a_r)(b_1, b_2, \dots, b_s) = (b_1, b_2, \dots, b_s)(a_1, a_2, \dots, a_r).$$

c) Bir n -li devirin derecesi n dir.

d) Bir m -li devir ile n -li ayırık devirin çarpımının derecesi $\text{OKEK}(m, n)$ dir.

Teorem 6.12 Her permütasyon devirlerinin çarpımına eşittir.

İspat: Bir $f \in S_n$ permütasyonunun bir deviri $(a, f(a), f^2(a), \dots, f^{m-1}(a))$ şeklindedir. Devirler ayırık olduklarından çarpımlarının a üzerindeki etkisi ile f nin a üzerindeki etkisi aynıdır. O halde f kendi devirlerinin çarpımına eşittir. $\square$

Teorem 6.13 $n \geq 2$ ise her $f \in S_n$ permütasyonu 2-li devirlerin (uzunluğu 2 olan devirlerin) bir çarpımı olarak yazılabilir.

İspat: f nin bir deviri $(a, f(a), f^2(a), \dots, f^{m-1}(a))$ şeklindedir. Bu deviri

$$(a, f(a)) \cdot (a, f^2(a)) \dots (a, f^{m-1}(a))$$

şekline 2–li devirlerin çarpımı olarak yazabiliriz. f nin bütün devirlerini bu şekilde yazabileceğimizden iddia açıktır. $\square$

Örnek 6.14 $\alpha = (15436)(798) \in S_9$ elemanına bakalım.

$$\alpha = (15)(14)(13)(16)(79)(78)$$

şeklinde 2–li devirlerin çarpımı olarak yazılabilir. $n \geq 2$ ise S_n deki birim eleman $(1) = (12)(12)$ şeklinde yazılabilir.

Tek ve Çift Permütasyonlar

Tanım 6.15 Bir 2–li devire bir *transpozisyon* denir. Bir permütasyon ikili devirlerin çarpımı olarak birden fazla şekilde yazılabilir. Mesela;

$$(12345) = (12)(13)(14)(15) = (41)(32)(14)(51)(52)(54).$$

Ancak bu yazılıştaki transpozisyonların sayısı ya hep çifttir ya da hep tektir. Çift sayıda transpozisyonun çarpımı olarak yazılabilen permütasyona *çift permütasyon* denir. Aksi halde *tek permütasyon* denir. Ayrıca aşağıdaki kurallar geçerlidir.

$$\boxed{\text{TEK} \times \text{TEK} = \text{ÇİFT}}$$

$$\boxed{\text{TEK} \times \text{ÇİFT} = \text{TEK}}$$

$$\boxed{\text{ÇİFT} \times \text{ÇİFT} = \text{ÇİFT}}$$

Tanım 6.16 S_n de çift permütasyonların kümesini A_n ile gösterelim. İki çift permütasyonun çarpımı çift olduğundan A_n sonlu ve kapalı bir alt kümedir. O halde Teorem 2.8 den A_n bir gruptur. Bu gruba n –inci dereceden *alterne grup* denir.

Örnek 6.17 Alterne grupların ilk 4 tanesi:

$$A_1 \cong A_2 = \{ (1) \},$$

$$A_3 = \{ (1), (123), (132) \},$$

$$A_4 = \{ (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23) \}.$$

Teorem 6.18 $A_n \triangleleft S_n$ dir ve $n \geq 2$ için $|A_n| = \frac{n!}{2}$ dir.

İspat: A_1 trivial grup olup $A_1 \triangleleft S_1$ olduğu açıktır. $n \geq 2$ olsun. $\{1, -1\}$ kümesi çarpma işlemi ile bir gruptur. Şimdi $\phi : S_n \rightarrow \{1, -1\}$ dönüşümünü

$$\phi(\sigma) = \begin{cases} 1, & \sigma \text{ çift ise;} \\ -1, & \sigma \text{ tek ise.} \end{cases}$$

şeklinde tanımlayalım. $\alpha, \beta \in S_n$ alalım. Toplam 4 durum vardır:

$$\alpha, \beta \text{ tek} \implies \phi(\alpha\beta) = +1 = (-1) \cdot (-1) = \phi(\alpha)\phi(\beta)$$

$$\alpha, \beta \text{ çift} \implies \phi(\alpha\beta) = +1 = (+1) \cdot (+1) = \phi(\alpha)\phi(\beta)$$

$$\alpha \text{ tek}, \beta \text{ çift} \implies \phi(\alpha\beta) = -1 = (-1) \cdot (+1) = \phi(\alpha)\phi(\beta)$$

$$\alpha \text{ çift}, \beta \text{ tek} \implies \phi(\alpha\beta) = -1 = (+1) \cdot (-1) = \phi(\alpha)\phi(\beta)$$

Yani ϕ bir homomorfizmadır. $n \geq 2$ olduğundan S_n 'de hem çift hem de tek permütasyonlar vardır. (Örneğin, $(1, 2)$ tek; (1) çifttir.) O halde ϕ örtendir. $\text{Çek}(\phi) = A_n$ olup bir grup homomorfizmasının çekirdeği her zaman normal altgrup olduğundan $A_n \triangleleft S_n$ dir (Teorem 4.10). Ayrıca, Birinci İzomorfizma Teoreminden $S_n/A_n \cong \{1, -1\}$ dir. Lagrange Teoremi'nden $|A_n| = n!/2$ elde edilir. $\square$

Lemma 6.19 $\sigma \in S_n$ ayrık devirlerin çarpımı şeklinde yazılsın. $\beta^{-1}\sigma\beta$ permütasyonu σ ile aynı şekle sahiptir ve σ 'daki sembollerin yerine onların β 'daki görüntülerinin yazılması ile elde edilir.

İspat: (İspat boyunca fonksiyonların sağa, elemanların sola yazıldığı gösterim tarzını kullanacağız. Yani $\sigma(i)$ yerine $i\sigma$ yazacağız.) σ nın i sembolünü j ye taşıdığını, yani $i\sigma = j$ olduğunu farzedelim. $\beta^{-1}\sigma\beta$ permütasyonunun $i\beta$ sembolünü $j\beta$ ya taşıdığını göstermemiz yeterlidir.

$$i\beta(\beta^{-1}\sigma\beta) = i(\sigma\beta) = (i\sigma)\beta = j\beta$$

olup ispat tamamlanır. $\square$

Örnek 6.20 $\sigma = (1, 5, 6)(2, 3)$ ve $\beta = (1, 4, 3)$ ise $\beta^{-1}\sigma\beta = (4, 5, 6)(2, 1)$ bulunur.

Teorem 6.21 $\alpha, \beta \in S_n$ ayrık devirlerin çarpımı şeklinde yazılmış iki permütasyon olsun. α ile β nın eşlenik olması için gerek ve yeter şart bu iki permütasyonun aynı devir yapısına sahip olmalarıdır.

İspat: ($\implies$) α ile β eşlenik olsun. O halde $\tau^{-1}\alpha\tau = \beta$ olacak şekilde $\tau \in S_n$ vardır. Bir önceki Lemmaya göre $\tau^{-1}\alpha\tau$ permütasyonu α daki i sembolünün yerine $i\tau$ yazılmasıyla elde edilir. O halde α ile β aynı devir yapısına sahiptir.

($\impliedby$) Şimdi de α ile β aynı devir yapısına sahip olsun. α 'yı β 'nın üzerine, aynı uzunluktaki devirler (uzunluğu 1 olanlar dahil) alt alta gelecek şekilde yazalım. Yukarıdaki sembolleri aşağıdaki sembollere eşleyen permütasyona τ dersek, $\tau^{-1}\alpha\tau = \beta$ olduğu açıktır. O halde α ile β eşleniktir. $\square$

Örnek 6.22 S_8 de $\alpha = (1, 3, 4)(2, 6)(5, 7)$ ile $\beta = (1, 8)(2, 5, 7)(3, 4)$ permütasyonları eşleniktir. Çünkü

$$\alpha = (1, 3, 4)(2, 6)(5, 7)(8)$$

$$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$$

$$\beta = (2, 5, 7)(3, 4)(1, 8)(6)$$

yazılırsa $\tau = (1, 2, 3, 5)(4, 7, 8, 6)$ seçilirse $\tau^{-1}\alpha\tau = \beta$ olur. Bunu sağlayan daha fazla τ bulmak için β 'nın yazılışı değiştirilebilir, mesela $\beta = (5, 7, 2)(1, 8)(4, 3)(6)$ yazılabilir.

6.1 $n \geq 5$ İçin A_n Basit Gruptur

A_1 ve A_2 trivial grup olduklarından basit değildir. A_3 'ün mertebesi 3 asal olduğundan A_3 basittir. A_4 grubu basit değildir, çünkü 4 elemanlı bir normal altgrubu vardır:

$$V = \{ (1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \} \triangleleft A_4.$$

Bu kısımda $n \geq 5$ için A_n grubunun basit olduğunu ispatlayacağız. Yani, eğer $H \triangleleft A_n$ ve $H \neq \{ (1) \}$ ise $H = A_n$ olduğunu göstereceğiz. Bu amaçla 3 tane Lemma veriyoruz.

Lemma 6.23 $n \geq 5$ için A_n 'in her elemanı 3-lü devirlerin bir çarpımıdır.

İspat: A_n in her elemanı (yani her çift permütasyon) çift sayıda transpozisyonun çarpımıdır. O halde iki transpozisyonun çarpımının, 3-lü devirlerin bir çarpımı şeklinde yazıldığını göstermek yeterlidir. Şimdi $(a_1, a_2)(b_1, b_2)$ çarpımını düşünelim. Bu dört sayının birbirinden farklı olduğunu kabul edebiliriz, çünkü öyle olmasaydı, aşağıda iki durum halinde açıklandığı gibi, bu çarpım ya birim elemana ya da bir 3-lü devire eşit olurdu. ($n \geq 3$ ise, birim eleman 3-lü devirlerin bir çarpımı olarak yazılabilir.)

$$\textbf{Durum 1: } a_1 = b_1, a_2 \neq b_2 \text{ ise: } (a_1, a_2)(b_1, b_2) = (a_1, a_2)(a_1, b_2) = (a_1, a_2, b_2)$$

$$\textbf{Durum 2: } a_1 = b_1, a_2 = b_2 \text{ ise: } (a_1, a_2)(b_1, b_2) = (a_1, a_2)(a_1, a_2) = (a_1)$$

Şimdi, $n \geq 5$ olduğundan $1 \leq e \leq n$ olacak şekilde bu dört sayıdan farklı bir e sayısı vardır. Böylece;

$$(a_1, a_2)(b_1, b_2) = (e, a_1, a_2)(e, a_1, b_1)(e, b_2, b_1)$$

olup iddia doğrudur. □

Lemma 6.24 $H \triangleleft A_n$ olsun. Eğer H bir 3-lü devir içeriyorsa o zaman $H = A_n$ dir.

İspat: $(a, b, c) \in H$ olsun. $x, y, z \in \{1, 2, \dots, n\}$ olsun ve x, y, z birbirinden farklı olsunlar. $\theta \in S_n$ elemanı a 'yı x 'e, b 'yi y 'ye ve c 'yi z 'ye eşleyen bir eleman ise $\theta^{-1}(a, b, c)\theta = (x, y, z)$ dir. Eğer θ çift ise $H \triangleleft A_n$ olduğundan $(x, y, z) \in H$ dir. Eğer θ tek ise $n \geq 5$ olduğundan a, b, c den farklı e, f sayıları vardır. O zaman $\Psi = (e, f)\theta$ çifttir.

$$\begin{aligned} \Psi^{-1}(a, b, c)\Psi &= \theta^{-1}(e, f)(a, b, c)(e, f)\theta \\ &= \theta^{-1}(a, b, c)\theta \\ &= (x, y, z) \end{aligned}$$

olup normallikten dolayı $(x, y, z) \in H$ olur. x, y, z nin seçimi keyfî olduğundan H , S_n deki bütün 3-lü devirleri içerir ve Lemma 6.23 den dolayı $H = A_n$ dir. □

Lemma 6.25 $H \triangleleft A_n$ olsun. Eğer H , iki ayrık transpozisyonun çarpımını içeriyorsa $H = A_n$ dir.

İspat: $\alpha = (a_1, a_2)(a_3, a_4) \in H$ iki ayrık transpozisyonun çarpımı olsun. $n \geq 5$ olduğundan bu dört sayıdan farklı $e \in \{1, 2, \dots, n\}$ sayısı vardır. $\theta = (a_1, a_2, e)$ olsun. $\theta \in A_n$ olup normallikten dolayı $\theta^{-1}\alpha\theta = (a_2, e)(a_3, a_4) \in H$ dir. Şimdi,

$$\begin{aligned}\alpha^{-1}(\theta^{-1}\alpha\theta) &= (a_1, a_2)(a_3, a_4)(a_2, e)(a_3, a_4) \\ &= (a_1, a_2)(a_2, e) \\ &= (a_1, e, a_2) \in H\end{aligned}$$

olup H bir 3-lü devir içerir. Lemma 6.24 den dolayı $H = A_n$ dir. $\square$

Teorem 6.26 $n \geq 5$ için A_n basit gruptur.

İspat: $H \triangleleft A_n$ ve $H \neq \{(1)\}$ olsun. O zaman $(1) \neq \alpha \in H$ vardır. $\alpha_1, \alpha_2 \dots \alpha_k$ ayrık devirler olmak üzere $\alpha = \alpha_1 \alpha_2 \dots \alpha_k$ olsun. Ayrık devirler değişmeli olduğundan $\alpha_1, \alpha_2 \dots \alpha_k$ ların uzunluklarına göre büyükten küçüğe sıralandığını; yani $i = 1, 2, \dots, k-1$ için “ α_i nin uzunluğu” $\geq$ “ α_{i+1} in uzunluğu” olduğunu varsayabiliriz.

Durum 1: $\alpha_1 = (a_1, a_2, \dots, a_m)$ ve $m \geq 4$ olsun.

$\sigma = (a_1, a_2, a_3)$ olsun. $\sigma \in A_n$ olduğu ve σ nın $\alpha_2, \alpha_3, \dots, \alpha_k$ ile değişmeli olduğu açıktır. $\sigma^{-1} \in A_n$ ve $H \triangleleft A_n$ olduğundan

$$\begin{aligned}\beta &= \alpha^{-1}(\sigma^{-1}\alpha\sigma) \\ &= \alpha_k^{-1} \dots \alpha_1^{-1}(a_2, a_3, a_1, a_4, \dots, a_m)\alpha_2 \dots \alpha_k \\ &= \alpha_1^{-1}(a_2, a_3, a_1, a_4, \dots, a_m) \\ &= (a_m, a_{m-1}, \dots, a_2, a_1)(a_2, a_3, a_1, a_4, \dots, a_m) \\ &= (a_1, a_2, a_4)\end{aligned}$$

olup $\beta \in H$ dir. Lemma 6.24 den sonuç ortaya çıkar.

Durum 2: $m = 3$ olsun ve α_2 de bir 3-lü devir olsun.

$\alpha_1 = (a_1, a_2, a_3)$ ve $\alpha_2 = (a_4, a_5, a_6)$ diyelim. $\sigma = (a_2, a_3, a_4) \in A_n$ olsun. Şimdi

$$\begin{aligned}\alpha^{-1}(\sigma^{-1}\alpha\sigma) &= \alpha_1^{-1}\alpha_2^{-1} \dots \alpha_k^{-1}(a_1, a_3, a_4)(a_2, a_5, a_6)\alpha_3\alpha_4 \dots \alpha_k \\ &= \alpha_1^{-1}\alpha_2^{-1}(a_1, a_3, a_4)(a_2, a_5, a_6) \\ &= (a_1, a_3, a_2)(a_4, a_6, a_5)(a_1, a_3, a_4)(a_2, a_5, a_6) \\ &= (a_1, a_4, a_2, a_3, a_5) \in H\end{aligned}$$

olup Durum 1’den dolayı sonuç elde edilir.

Durum 3: $m = 3$ ve $\alpha_2, \dots, \alpha_k$ ların hepsi transpozisyon olsun.

$\alpha_1 = (a_1, a_2, a_3)$ olsun. $\alpha^2 = (a_1, a_2, a_3)^2 = (a_1, a_3, a_2) \in H$ olup sonuç Lemma 6.24 den ortaya çıkar.

Durum 4: Bütün α_i ler transpozisyon olsun.

$\alpha_1 = (a_1, a_2), \alpha_2 = (a_3, a_4)$ olsun. $\sigma = (a_2, a_3, a_4)$ diyelim. Şimdi

$$\begin{aligned} (\sigma^{-1}\alpha\sigma)\alpha^{-1} &= (a_1, a_3)(a_4, a_2)\alpha_3 \dots \alpha_k \alpha_k^{-1} \dots \alpha_1^{-1} \\ &= (a_1, a_3)(a_4, a_2)(a_1, a_2)(a_3, a_4) \\ &= (a_1, a_4)(a_2, a_3) \in H \end{aligned}$$

olup Lemma 6.25 den sonuç ortaya çıkar. □

ALİŞTIRMALAR

1. $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 6 & 1 & 2 & 8 & 4 \end{pmatrix}$ permütasyonu verilsin. θ yı önce ayrık devirlerin sonra da 2-li devirlerin bir çarpımı şeklinde yazınız. θ çift midir, tek midir?
2. S_3 de $A = \langle (1, 2) \rangle$ ve $B = \langle (1, 3) \rangle$ alt grupları verilsin. AB çarpımı S_3 ün bir alt grubu mudur?
3. $\hat{S}_n = \{ f \in S_n \mid f(n) = n \}$ kümesinin S_n in bir altgrubu olduğunu ve S_{n-1} 'e izomorfik olduğunu gösteriniz.
4. Bir G grubunun normal bir altgrubunun normal bir altgrubu G 'de normal olmayabilir. Bir örnek vererek gösterin. (**İpucu:** A_4 grubunu ele alın.)
5. $n \geq 3$ için S_n abelyen değildir. Gösterin.
6. $H \leq S_n$ bir altgrup olsun. Ya H nin tüm elemanları çifttir ya da yarısı tek yarısı çifttir. Gösterin.
7. S_5 de $\alpha = (1, 2, 3)(4, 5)$ permütasyonunun merkezleyenini bulunuz.
8. A_3 'ün grup tablosunu yazınız.
9. $A_n = S_n$ ise $n = 1$ olduğunu gösterin.

ALİŞTIRMALARIN ÇÖZÜMLERİ

ÇÖZÜM 1. $\theta = (1, 3, 5)(2, 7, 8, 4, 6) = (1, 3)(1, 5)(2, 7)(2, 8)(2, 4)(2, 6)$ olup θ permütasyonu 6 tane transpozisyonun çarpımıdır, yani çifttir.

ÇÖZÜM 2. $A = \{(1), (1, 2)\}$, $B = \{(1), (1, 3)\}$ ve $AB = \{(1), (1, 2), (1, 3), (1, 2, 3)\}$ olur. Buradan $(1, 3)(1, 2) = (1, 3, 2) \notin AB$ olup AB bir alt grup değildir.

ÇÖZÜM 3. $S = \{1, 2, \dots, n-1, n\}$ olsun. $\widehat{S}_n$ aslında son elemanı sabit bırakan permütasyonların kümesidir. $f, g \in \widehat{S}_n$ olsun. Bu durumda $g^{-1} \in \widehat{S}_n$ olduğu açıktır. Şimdi,

$$[fg^{-1}](n) = g^{-1}(f(n)) = g^{-1}(n) = n$$

olup $fg^{-1} \in \widehat{S}_n$ olduğu görülür. Teorem 2.8'den $\widehat{S}_n \leq S_n$. Şimdi $\widehat{S}_n \cong S_{n-1}$ olduğunu gösterelim. $\psi : S_{n-1} \rightarrow \widehat{S}_n$ dönüşümünü her $g \in S_{n-1}$ için $\psi(g) = g \cdot (n)$ şeklinde tanımlayalım. Yani g ye (n) permütasyonu ilave edelim. ψ bir izomorfizmadır, çünkü:

ψ 1-1 dir: $\psi(f) = \psi(g) \implies f \cdot (n) = g \cdot (n) \implies f = g$.

ψ homomorfizmadır: $\psi(fg) = fg \cdot (n) = f \cdot (n) \cdot g \cdot (n) = \psi(f)\psi(g)$.

ψ örtendir: $g' \in \widehat{S}_n$ alalım. Bu durumda $g' = g \cdot (n)$ şeklinde olup burada $g \in S_{n-1}$ dir. O zaman $\psi(g) = g'$ olduğu açıktır.

ÇÖZÜM 4. $G = A_4$ alalım. $V = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \triangleleft A_4$ olduğu açıktır, çünkü ayrık iki transpozisyonun çarpımı şeklindeki bütün permütasyonlar V de olup her $\alpha \in A_4$ ve her $\beta \in V$ için $\alpha^{-1}\beta\alpha$ permütasyonu β ile aynı şekle sahiptir; yani birim elemandır ya da ayrık iki transpozisyonun çarpımıdır. O halde $\alpha^{-1}\beta\alpha \in V$ dir. Şimdi $U = \{(1), (1\ 2)(3\ 4)\}$ dersek $U \triangleleft V$ olur, çünkü bu alt grubun indeksi 2 dir. Ancak U, A_4 'ün normal alt grubu değildir, çünkü $(1\ 2\ 3) \in A_4$ için

$$(1\ 2\ 3)^{-1} \cdot (1\ 2)(3\ 4) \cdot (1\ 2\ 3) = (2\ 3)(1\ 4) \notin U.$$

ÇÖZÜM 5. $n \geq 3$ ise $\alpha = (1, 2) \in S_n$ ve $\beta = (1, 3) \in S_n$ alalım $\alpha\beta = (1, 2, 3)$ fakat $\beta\alpha = (1, 3, 2)$ olup S_n abelyen değildir.

ÇÖZÜM 6. $H \leq S_n$ olsun. H nin tüm elemanları çift olmasın. $\sigma \in H$ tek olsun. $H\sigma = H$ olup H yi σ ile çarpmak H deki bütün çift elemanları tek; tek elemanları da çift yapar. O halde H deki elemanların yarısı çift yarısı tektir.

ÇÖZÜM 7. $C_\alpha = \{\tau \in S_5 : \tau^{-1}\alpha\tau = \alpha\}$ kümesidir. Başka bir deyişle bu küme α yı α 'ya eşlenik yapan permütasyonların kümesidir. Teorem 6.21'de izah edildiği gibi bu permütasyonları bulmak için α nın altına α yazılıp üstteki sembolleri alttakilere eşleyen permütasyonlar yazılır. O halde

$$C_\alpha = \{(1), (1, 2, 3), (1, 3, 2), (1, 2, 3)(4, 5), (1, 3, 2)(4, 5), (4, 5)\}.$$

ÇÖZÜM 8. $A_3 = \{(1), (123), (132)\}$ grubunun tablosu aşağıdadır:

$\cdot$	(1)	(123)	(132)
(1)	(1)	(123)	(132)
(123)	(123)	(132)	(1)
(132)	(132)	(1)	(123)

ÇÖZÜM 9. $n > 1$ ise S_n grubu 1 ile 2 yi yer değiştirip diğer bütün elemanları sabit bırakan $\alpha = (1, 2)$ permütasyonunu içerir. α tek permütasyon olduğundan $A_n \neq S_n$ dir. $A_1 = S_1$ olduğundan $A_n = S_n \implies n = 1$ dir.

Tanım 7.1 $R \neq \emptyset$ bir küme olsun. R de adına “toplama” ve “çarpma” denilen ve sırasıyla “+” ve “.” sembolleri ile gösterilen iki işlem tanımlanmış olsun. Eğer aşağıdaki 3 şart sağlanıyorsa $(R, +, \cdot)$ iki işlemli cebirsel yapısına bir ***halka*** denir.

1. $(R, +)$ bir abelyen (değişmeli) gruptur.
2. Her $a, b, c \in R$ için $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ dir. (Yani $(R, \cdot)$ bir yarıgruptur.)
3. Her $a, b, c \in R$ için:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ (Soldan dağılma özelliği),}$$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \text{ (Sağdan dağılma özelliği).}$$

Bunlara ek olarak;

4. Her $a, b \in R$ için $a \cdot b = b \cdot a$ ise (yani $\cdot$ işlemi değişmeli ise) R ye ***değişimli halka*** denir.
5. Her $a \in R$ için $a \cdot e = e \cdot a = a$ olacak şekilde bir $e \in R$ var ise e ye ***birim eleman***; R ye de ***birim elemanlı halka*** denir.

Not: Aksi belirtilmedikçe çarpma işleminin toplama işlemine göre işlem önceliği olduğu kabul edilecektir. Bu yüzden 3. özellikte eşitliğin sağındaki parentezler kullanılmayabilir. Ayrıca $a \cdot b$ yerine kısaca ab yazılabilir. Halkadaki toplama işleminde (birinci işlemde) toplamsal gösterim tarzı; çarpma işleminde (ikinci işlemde) çarpımsal gösterim tarzı kullanılır.

Not: Bir R birim elemanlı halkasında birim eleman genelde 1_R veya kısaca 1 ile gösterilir. Bazı yazarlar 5. özelliği bir halkanın sahip olması gereken bir özellik olarak kabul ederler.

Örnek 7.2 $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sistemleri birer halkadır.

Örnek 7.3 $S = \{x + y\sqrt{2} \mid x, y \in \mathbb{Z}\}$ kümesi bilinen $+$ ve $\cdot$ işlemleri ile bir halkadır.

Örnek 7.4 $T = \{u + v\sqrt[3]{2} + w\sqrt[3]{4} \mid u, v, w \in \mathbb{Q}\}$ kümesi bilinen $+$ ve $\cdot$ işlemleri ile bir halkadır.

Örnek 7.5 $(\mathbb{Z}_n, \oplus, \odot)$ bir halkadır. Her $\bar{a}, \bar{b} \in \mathbb{Z}_n$ için $\oplus$ ve $\odot$ işlemleri şöyle tanımlanmaktadır:

$$\bar{a} \oplus \bar{b} = \overline{a + b} \quad \text{ve} \quad \bar{a} \odot \bar{b} = \overline{a \cdot b}$$

Örnek 7.6 $T = \{0, e\}$ kümesinde toplama ve çarpma şöyle tanımlansın:

$$\begin{array}{c|cc} + & 0 & e \\ \hline 0 & 0 & e \\ e & e & 0 \end{array} \quad \begin{array}{c|cc} \cdot & 0 & e \\ \hline 0 & 0 & 0 \\ e & 0 & e \end{array}$$

Buna göre $(T, +, \cdot)$ bir halkadır.

Tanım 7.7 $(R, +, \cdot)$ halkasında toplama işlemine göre olan birim elemana halkanın **sıfırı** denir ve 0_R veya kısaca 0 ile gösterilir. Bir a elemanının $+$ işlemine göre tersi $-a$ ile gösterilir ve $a + (-b)$ yerine kısaca $a - b$ yazılır.

Örnek 7.8 $L = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} = \{(a, b, c) \mid a, b, c \in \mathbb{Z}\}$ kümesinde toplama ve çarpma işlemleri şöyle tanımlansın:

$$(a, b, c) + (d, e, f) = (a + d, b + e, c + f), \quad (a, b, c)(d, e, f) = (ad, bd + ce, cf).$$

$(L, +, \cdot)$ cebirsel yapısının bir halka olduğunu gösterelim.

i) $(L, +)$ değişmeli gruptur. Çünkü kapalıdır, birleşimlidir, birim eleman $(0, 0, 0)$ dır, (a, b, c) nin tersi $-(a, b, c) = (-a, -b, -c)$ dir ve değişme özelliği vardır.

ii)

$$\begin{aligned} (a, b, c)[(d, e, f)(g, h, i)] &= (a, b, c)[(dg, eg + fh, fi)] \\ &= (adg, bdg + ceg + cfh, cfi) \\ &= (ad, bd + ce, cf)(g, h, i) \\ &= [(a, b, c)(d, e, f)](g, h, i) \quad \text{bulunur.} \end{aligned}$$

iii)

$$\begin{aligned} (a, b, c)[(d, e, f) + (g, h, i)] &= (a, b, c)[(d + g, e + h, f + i)] \\ &= (ad + ag, bd + bg + ce + ch, cf + ci) \\ &= (a, b, c)(d, e, f) + (a, b, c)(g, h, i) \quad \text{olduğu görülür.} \end{aligned}$$

Sağdan dağılma özelliğini ödev olarak bırakıyoruz. Sonuç: $(L, +, \cdot)$ bir halkadır.

iv) Birim elemanı bulalım:

$$\begin{aligned}(a, b, c)(x, y, z) &= (a, b, c) \implies (ax, bx + cy, cz) = (a, b, c) \\ \implies ax &= a, bx + cy = b, cz = c \\ \implies x &= 1, z = 1, y = 0\end{aligned}$$

olur. Ayrıca $(1, 0, 1)(a, b, c) = (a, b, c)$ olup $(1, 0, 1)$ birim elemandır. Yani $(L, +, \cdot)$ birim elemanlı bir halkadır.

v) $(1, 0, 0)(0, 1, 0) = (0, 0, 0)$ fakat $(0, 1, 0)(1, 0, 0) = (0, 1, 0)$ olup çarpmanın değişme özelliği yoktur. $(L, +, \cdot)$ değişmeli halka değildir.

Not: Bir halkada $\cdot$ işleminin $+$ üzerine soldan dağılma özelliği varsa ve bu halka değişmeli ise $\cdot$ işleminin $+$ üzerine sağdan dağılma özelliği de vardır, çünkü:

$$(a + b) \cdot c = c \cdot (a + b) = c \cdot a + c \cdot b = a \cdot c + b \cdot c.$$

Teorem 7.9 Bir halkanın sıfırı tektir.

İspat: (Gruplar teorisindeki ispatın aynısıdır.) 0 ve $0'$, R nin iki farklı sıfırı olsun. 0 bir sıfır olduğundan $0 + 0' = 0'$ olur. Ayrıca, $0'$ bir sıfır olduğundan $0 + 0' = 0$ olur. Bu iki eşitlikten $0 = 0'$ elde edilir. $\square$

Teorem 7.10 R bir halka ve $a, b, c \in R$ olsun.

1. $a + c = b + c$ ise $a = b$ dir (Sağdan kısaltma).
2. $c + a = c + b$ ise $a = b$ dir (Soldan kısaltma).
3. Toplamaya göre ters eleman tektir.
4. $a + x = b$ denkleminin tek çözümü $x = b - a$ dır.
5. R nin birim elemanı (varsa) tektir.
6. a nın çarpmaya göre tersi (varsa) tektir.

İspat: Grup teorisindeki gibidir. $\square$

Tanım 7.11 $(R, +, \cdot)$ bir halka olsun. Eğer $(R \setminus \{0\}, \cdot)$ bir abelyen grup ise $(R, +, \cdot)$ sistemine bir *cisim* denir.

Not: Bir R cisminde $R \setminus \{0\}$ kümesi bir grup olacağından $R = \{0\}$ halkası bir cisim olamaz. O halde “bir cisim en az 2 elemanlıdır” diyebiliriz.

Örnek 7.12 $(\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Q}, +, \cdot)$ birer cisimdir, fakat $(\mathbb{Z}, +, \cdot)$ bir cisim değildir.

Teorem 7.13 R bir halka olsun. Her $a, b \in R$ için:

1. $a0 = 0a = 0$
2. $(-a)b = a(-b) = -(ab)$
3. $(-a)(-b) = ab$

İspat 1. $a0 = a(0 + 0) = a0 + a0$ olur, veya $0 + a0 = a0 + a0$ yazabiliriz. Sağdan kısaltma kuralını kullanırsak $0 = a0$ elde edilir. Benzer şekilde $0a = 0$ olduğu gösterilebilir.

İspat 2. $(-a)b + ab = (-a + a)b = 0b = 0$ olduğundan $-(ab) = (-a)b$ olur. Benzer şekilde $a(-b) = -(ab)$ gösterilebilir.

İspat 3. Eğer $(-a)b = a(-b)$ eşitliğinde b yerine $(-b)$ yazarsak, $(-a)(-b) = a(-(-b)) = ab$. $\square$

Not 7.14 Birim elemanlı bir halkanın sıfırı ile birim elemanı eşit olabilir mi? Yani $0_R = 1_R$ olabilir mi? Cevap: Bu durum sadece $R = \{0\}$ halkasında görülür. (Bu halkaya *trivial halka* veya *sıfır halkası* denir.) Bunu şöyle ispatlayabiliriz: Bir R halkasında $0_R = 1_R$ olduğunu kabul edelim. Her $a \in R$ için $0 = 0 \cdot a = 1 \cdot a = a$ olup $R = \{0\}$ olduğu görülür.

Tanım 7.15 R bir halka ve $\emptyset \neq S \subseteq R$ olsun. Eğer S, R deki işlemlerle birlikte bir halka oluyorsa S 'ye R 'nin bir *alt halkası* denir.

Örnek 7.16 $\mathbb{Z}$ halkası $\mathbb{Q}$ nun; $\mathbb{Q}$ halkası da $\mathbb{R}$ nin alt halkasıdır. $2\mathbb{Z}$ halkası $\mathbb{Z}$ nin alt halkasıdır.

Teorem 7.17 R bir halka ve $\emptyset \neq S \subseteq R$ olsun. S 'nin alt halka olması için gerek ve yeter şartlar:

- 1.) Her $a, b \in S$ için $a - b \in S$
- 2.) Her $a, b \in S$ için $ab \in S$

İspat: ($\implies$) S bir alt halka ve $a, b \in S$ olsun. $(S, +)$ grubu $(R, +)$ grubunun alt grubu olduğundan, Teorem 2.8'den, $a - b \in S$ dir. Ayrıca S bir halka olduğundan $ab \in S$ dir.

($\impliedby$) $S \neq \emptyset$ ve her $a, b \in S$ için $a - b, ab \in S$ olsun. Teorem 2.8'den $(S, +)$ grubu $(R, +)$ grubunun alt grubudur. $S \subseteq R$ olduğundan $+$ işlemi S 'de de değişmelidir. Yine, $S \subseteq R$ olduğundan çarpma işlemi S 'de de birleşmelidir ve $\cdot$ işleminin $+$ üzerine soldan ve sağdan dağılma özelliği S 'de de vardır. O halde S bir alt halkadır. $\square$

Not 7.18 Bu teoremin uygulanması için S nin boş olmadığından emin olmak gerekir. O yüzden bazı kaynaklarda bir S altkümesinin (boş veya değil) alt halka olması için gerek ve yeter şartlar 3 tane verilmiştir. Bu üç şart, yukardaki 2 şartla birlikte, $0 \in S$ şartıdır. Eğer S boş değilse, $0 \in S$ olduğu Teorem 7.17'de $b = a$ alınarak 1.) şartı uygulanırsa elde edilir.

Tanım 7.19 $(R, +, \cdot)$ ve $(S, \oplus, \odot)$ iki halka ve $\theta : R \longrightarrow S$ bir fonksiyon olsun. Eğer θ toplama ve çarpma işlemlerini koruyorsa; yani

$$(i) \text{ her } a, b \in R \text{ için } \theta(a + b) = \theta(a) \oplus \theta(b),$$

$$(ii) \text{ her } a, b \in R \text{ için } \theta(a \cdot b) = \theta(a) \odot \theta(b)$$

ise θ ya bir **halka homomorfizması** denir. Bu durumda $\theta : (R, +) \longrightarrow (S, \oplus)$ bir grup homomorfizması olduğu açıktır. O halde grup homomorfizmalarındaki sonuçlar geçerlidir. Mesela;

$$(i) \quad \theta(0_R) = 0_S,$$

$$(ii) \quad \theta(-a) = -\theta(a),$$

$$(iii) \quad \theta(a - b) = \theta(a + (-b)) = \theta(a) \oplus \theta(-b) = \theta(a) \oplus (-\theta(b)) = \theta(a) - \theta(b).$$

Örnek 7.20 $\theta : \mathbb{Z}_{20} \longrightarrow \mathbb{Z}_{30}$, $\theta(\bar{x}) = 6\bar{x}$ şeklinde tanımlansın. $\bar{x}, \bar{y} \in \mathbb{Z}_{20}$ için $\bar{x} \oplus \bar{y} = \bar{r}$ ve $\bar{x} \odot \bar{y} = \bar{s}$ ise $\mathbb{Z}$ 'de $x + y = 20q + r$ ve $xy = 20t + s$ dir ($q, t \in \mathbb{Z}$ ve $0 \leq r, s < 20$.) Bu durumda $\mathbb{Z}$ 'de

$$6x + 6y = 6(x + y) = 120q + 6r \quad \text{ve} \quad 6(xy) = 120t + 6s$$

olur. $\mathbb{Z}_{30}$ 'da ise

$$\theta(\bar{x} \oplus \bar{y}) = 6(\bar{x} \oplus \bar{y}) = 6\bar{r} = 6\bar{x} \oplus 6\bar{y} = \theta(\bar{x}) \oplus \theta(\bar{y}),$$

$$\theta(\bar{x} \odot \bar{y}) = 6(\bar{x} \odot \bar{y}) = 6\bar{s} = (6 \cdot 6)\bar{s} = 6 \cdot 6(\bar{x} \odot \bar{y}) = (6\bar{x}) \odot (6\bar{y}) = \theta(\bar{x}) \odot \theta(\bar{y})$$

olur ve böylece θ bir halka homomorfizmasıdır.

Örnek 7.21 $\theta : \mathbb{Z}_5 \longrightarrow \mathbb{Z}_{10}$, $\theta(\bar{x}) = 5\bar{x}$ şeklinde tanımlansın. θ bir halka homomorfizması değildir, çünkü

$$\theta(\bar{3} \odot \bar{3}) = \theta(\bar{4}) = \bar{0}, \quad \text{fakat} \quad \theta(\bar{3}) \odot \theta(\bar{3}) = \bar{5} \odot \bar{5} = \bar{5}.$$

Ayrıca, $\theta : (\mathbb{Z}_5, \oplus) \longrightarrow (\mathbb{Z}_{10}, \oplus)$ grup homomorfizması da değildir, çünkü

$$\theta(\bar{4} \oplus \bar{4}) = \theta(\bar{3}) = \bar{5}, \quad \text{fakat} \quad \theta(\bar{4}) \oplus \theta(\bar{4}) = \bar{0} \oplus \bar{0} = \bar{0}.$$

Örnek 7.22 $R = (\mathbb{Z}, +, \cdot)$, $S = (2\mathbb{Z}, +, \cdot)$ olsun. $\theta : R \longrightarrow S$, $\theta(x) = 2x$ olarak tanımlansın.

$$\theta(x + y) = 2(x + y) = 2x + 2y = \theta(x) + \theta(y)$$

olup θ bir grup homomorfizmasıdır. Fakat genelde $\theta(xy) = 2xy \neq 2x2y = \theta(x)\theta(y)$ olup θ bir halka homomorfizması değildir.

Tanım 7.23 $\theta : R \longrightarrow S$ bir halka homomorfizması olsun. θ birebir ve örten ise θ 'ya bir **halka izomorfizması** denir. Eğer R 'den S 'ye bir halka izomorfizması var ise R ve S halkalarına **izomorftir** denir. $\theta : R \longrightarrow R$ izomorfizma ise θ 'ya bir **halka otomorfizması** denir.

Örnek 7.24 $H = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ bilinen matris toplamı ve çarpımı ile bir halkadır. $\phi : \mathbb{C} \longrightarrow H, \phi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ bir halka homomorfizması mıdır? ϕ dönüşümü $\mathbb{C}$ ile H yi izomorfik yapar mı?

Çözüm: $a, b, c, d \in \mathbb{R}$ olmak üzere $z = a + bi \in \mathbb{C}$ ve $w = c + di \in \mathbb{C}$ alalım.

$$\begin{aligned}
 \phi(z + w) &= \phi((a + c) + (b + d)i) \\
 &= \begin{pmatrix} a + c & b + d \\ -b - d & a + c \end{pmatrix} \\
 &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\
 &= \phi(z) + \phi(w), \\
 \phi(zw) &= \phi((ac - bd) + (ad + bc)i) \\
 &= \begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{pmatrix} \\
 &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\
 &= \phi(z)\phi(w).
 \end{aligned}$$

Yani ϕ bir halka homomorfizmasıdır.

$$\phi(z) = \phi(w) \implies \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \implies a = c, b = d \implies a + bi = c + di \implies z = w$$

olup ϕ 1-1 dir. Şimdi verilen her $Y = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in H$ matrisi için $X = a + bi \in \mathbb{C}$ seçilirse $\phi(X) = Y$ olup ϕ nin örten olduğu görülür. Yani $\mathbb{C}$ ile H izomorfiktir.

Tanım 7.25 R birim elemanlı bir halka olsun. Bir $u \in R$ elemanının çarpmaya göre tersi varsa u ya bir **birim** (unit) denir. Bir halkadaki bütün birimlerin kümesi $U(R)$ ile gösterilir. $(U(R), \cdot)$ cebirsel yapısı bir gruptur.

Dikkat: “Birim eleman” ile “birim” kavramlarını karıştırmayınız.

Örnek 7.26 $U(\mathbb{Z}) = \{1, -1\}, U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}, U(\mathbb{C}) = \mathbb{C} \setminus \{0\}, U(\mathbb{Z}_6) = \{\bar{1}, \bar{5}\}.$

Tanım 7.27 R bir halka olsun. Bir $a \in R$ için $a^n = 0$ olacak şekilde bir $n \in \mathbb{Z}^+$ varsa a ya *nilpotent* denir. Mesela;

$\mathbb{Z}$ halkasındaki nilpotent elemanlar: $\{0\}$

$\mathbb{Q}$ halkasındaki nilpotent elemanlar: $\{0\}$

$\mathbb{Z}_8$ halkasındaki nilpotent elemanlar: $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$

$\mathbb{Z}_9$ halkasındaki nilpotent elemanlar: $\{\bar{0}, \bar{3}, \bar{6}\}$

Örnek 7.28 H birim elemanlı bir halka olsun. $x \in H$ nilpotent ise $(1 - x)$ in ve $(1 + x)$ in bir birim olduğunu gösteriniz.

Çözüm: $x \in H$ nilpotent olsun. O halde $\exists n \in \mathbb{Z}^+$ için $x^n = 0$ dır.

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

olup $(1 - x)$ in tersi vardır. Yani $1 - x$ birimdir. Ayrıca

$$(1 + x)(1 - x + x^2 - \cdots \mp x^{n-1}) = \begin{cases} 1 + x^n, & n \text{ tek ise;} \\ 1 - x^n, & n \text{ çift ise.} \end{cases}$$

Her iki durumda da $1 \mp x^n = 1$ olup $1 + x$ in birim olduğu görülür.

Tanım 7.29 Birim elemanlı (ve trivial olmayan) bir halkanın, 0 hariç bütün elemanları birim ise bu halkaya *çarpık cisim* (skew field) veya *bölüm halkası* (division ring) denir. (Her cisim bir çarpık cisimdir fakat bir çarpık cismin cisim olması gerekmez.)

Örnek 7.30 $(\mathbb{Z}, +, \cdot)$ halkası çarpık cisim değildir, çünkü 2 elemanı birim değildir. $(\mathbb{Q}, +, \cdot)$ halkasının 0 hariç her elemanı birim olduğundan bu halka bir çarpık cisimdir. $\mathbb{Z}_7$ bir bölüm halkasıdır çünkü $1^{-1} = 1, 2^{-1} = 4, 3^{-1} = 5, 4^{-1} = 2, 5^{-1} = 3, 6^{-1} = 6$ dır.

Örnek 7.31 Çarpık cisim olup cisim olmayan bir halka örneği, kompleks sayıları da içeren *Hamilton¹ sayılarıdır* (*dördeyler* veya *quaterniyonlar halkası* da denir) ve

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{R}\}$$

kümesi olarak tanımlanır. $z_1 = a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}$ ve $z_2 = a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}$ ise toplama ve çarpma işlemi şöyle tanımlanır:

$$\begin{aligned} z_1 + z_2 &= (a_1 + a_2) + (b_1 + b_2)\mathbf{i} + (c_1 + c_2)\mathbf{j} + (d_1 + d_2)\mathbf{k}, \\ z_1 \cdot z_2 &= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)\mathbf{i} \\ &\quad + (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)\mathbf{j} + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\mathbf{k} \end{aligned}$$

¹İrlandalı matematikçi, fizikçi ve astronom Sir William Rowan Hamilton (4 Ağustos 1805-2 Eylül 1865)

Bu işlemlerle $(\mathbb{H}, +, \cdot)$ birim elemanı 1 olan bir halkadır. $z = a + bi + cj + dk$ ise z 'nin **uzunluğu** ve **eşleniği**

$$|z| = \sqrt{a^2 + b^2 + c^2 + d^2}, \quad \bar{z} = a - bi - cj - dk$$

şeklinde tanımlanır. O zaman $z \neq 0$ ise

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$$

olup çarpma işlemine göre 0 hariç her elemanın tersi vardır. Fakat bu halka değişmeli değildir (mesela $\mathbf{k} = \mathbf{ij} \neq \mathbf{ji} = -\mathbf{k}$); yani cisim olmayan bir çarpık cisimdir.

Tanım 7.32 R bir halka, $a, b \in R$ ve $a \neq 0, b \neq 0$ olsun. Eğer $a \cdot b = 0$ ise a ve b ye R nin **sıfır bölenleri** denir. a ya **sol sıfır bölen**, b ye **sağ sıfır bölen** denir. R halkası değişmeli ise sol (sağ) sıfır bölen aynı zamanda sağ (sol) sıfır bölendir.

Örnek 7.33 $(\mathbb{Z}_{12}, \oplus, \odot)$ halkasının sıfır bölenlerini bulalım:

$$\bar{2} \odot \bar{6} = \bar{0}, \quad \bar{3} \odot \bar{4} = \bar{0}, \quad \bar{8} \odot \bar{9} = \bar{0}, \quad \bar{6} \odot \bar{10} = \bar{0}$$

olduğundan, sıfır bölenlerin kümesi: $\{\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{10}\}$.

Teorem 7.34 $\mathbb{Z}_n$ halkasının sıfır bölenleri, m ile n ile aralarında asal olmamak üzere $\bar{m}$ şeklindedir.

İspat: $\bar{m} \in \mathbb{Z}_n$ ve m ile n aralarında asal olmasın. Yani $\text{EBOB}\{m, n\} = (m, n) = d \geq 2$ olsun. Bu durumda

$$m \left(\frac{n}{d} \right) = \left(\frac{m}{d} \right) n \equiv 0 \pmod{n}$$

olur. Burada $\bar{m} \neq \bar{0}$ ve $\overline{\left(\frac{n}{d} \right)} \neq \bar{0}$ olduğundan $\bar{m}$ bir sıfır bölendir. □

Sonuç 7.35 p asal ise $\mathbb{Z}_p$ nin sıfır bölenleri yoktur.

Tanım 7.36 Birim elemanlı, değişmeli ve sıfır böleni olmayan en az 2 elemanlı bir halkaya **tamlık bölgesi** denir.

Örnek 7.37 $\mathbb{Z}_p$ bir tamlık bölgesidir. Ayrıca $(\mathbb{Q}, +, \cdot), (\mathbb{Z}, +, \cdot)$ ve $(\mathbb{R}, +, \cdot)$ birer tamlık bölgesidir. $(\mathbb{H}, +, \cdot)$ halkası sıfır bölensizdir fakat değişmeli olmadığından bir tamlık bölgesi değildir.

Teorem 7.38 Her F cismi bir tamlık bölgesidir.

İspat: $a, b \in F, a \neq 0, ab = 0$ olsun. $b = 0$ olduğunu göstermemiz yeterlidir. F bir cisim olduğundan $a^{-1} \in F$ vardır.

$$ab = 0 \implies a^{-1}(ab) = a^{-1}0 \implies (a^{-1}a)b = 0 \implies 1 \cdot b = 0 \implies b = 0.$$

Teorem 7.39 Her sonlu tamlık bölgesi bir cisimdir.

İspat: $F = \{0, 1, a_1, a_2, \dots, a_n\}$, $n + 2$ elemanlı sonlu bir tamlık bölgesi olsun. $F^* = F \setminus \{0\}$ diyelim. Her $x \in F^*$ ın çarpma işlemine göre bir tersinin olduğunu göstermemiz yeterlidir. 1'in tersi 1'dir. a_1 in tersinin olduğunu gösterelim. (Diğerlerinin tersinin olduğu da aynı yöntemle gösterilir.) $a_1 F^* = \{a_1, a_1 a_1, a_1 a_2, \dots, a_1 a_n\}$ kümesine bakalım. Çarpma işlemi kapalı olduğundan ve F tamlık bölgesi olduğundan bu kümedeki elemanların hepsi F^* ın elemanlarıdır. Ayrıca bu elemanların hepsi birbirinden farklıdır. Çünkü:

- 1.) $\exists i$ için $a_1 = a_1 a_i$ olsaydı $a_i = 1$ olurdu.
- 2.) $\exists i, j$ ve $i \neq j$ için $a_1 a_i = a_1 a_j$ olsaydı $a_1 a_i - a_1 a_j = 0$ yani $a_1(a_i - a_j) = 0$ olurdu. F bir tamlık bölgesi olduğundan $a_i - a_j = 0$ yani $a_i = a_j$ olurdu.

Sonuç olarak, her iki küme de $n + 1$ elemanlı olduğundan, $a_1 F^* = F^*$ bulunur. $1 \in F^*$ olduğundan $\exists j$ için $a_1 a_j = 1$ olmalıdır ki bu da $(a_1)^{-1} = a_j \in F$ olduğunu gösterir. $\square$

Örnek 7.40 $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ sonlu bir tamlık bölgesi olup bir cisimdir. Daha genel olarak p asal ise $\mathbb{Z}_p$ bir cisimdir, aksi halde değildir.

Tanım 7.41 R bir halka olsun. Her $a \in R$ için $na = 0$ olacak şekildeki en küçük n pozitif tamsayısına R halkasının **karakteristiği** denir ve $\text{kar}(R)$ ile gösterilir. Eğer böyle bir n sayısı yoksa “halkanın karakteristiği sıfırdır” denir.

Örnek 7.42 $\text{kar}(\mathbb{Q}) = \text{kar}(\mathbb{Z}) = 0$ dir. $\text{kar}(\mathbb{Z}_8) = 8$ dir. Ayrıca $\text{kar}(2\mathbb{Z}) = 0$. Karakteristiği 1 olan tek halka $R = \{0\}$ halkasıdır.

Teorem 7.43 R birim elemanı e ve karakteristiği n olan bir halkadır $\iff n$ sayısı $ne = 0$ olacak şekildeki en küçük pozitif tamsayıdır.

İspat: ($\implies$) Her $a \in R$ için $na = 0$ olup $e \in R$ için de $ne = 0$ dir.

($\impliedby$) n sayısı $ne = 0$ olacak şekildeki en küçük pozitif tamsayı olsun. Her $a \in R$ için:

$$\begin{aligned} na &= \underbrace{a + a + \dots + a}_{n\text{-tane}} = \underbrace{ae + ae + \dots + ae}_{n\text{-tane}} = a \underbrace{(e + e + \dots + e)}_{n\text{-tane}} \\ &= a(ne) = a \cdot 0 = 0 \end{aligned}$$

olup ispat tamamlanır.

Teorem 7.44 Bir tamlık bölgesinin karakteristiği 0 veya asal bir sayıdır.

İspat: D bir tamlık bölgesi olsun. $\text{kar}(D) = 0$ ise ispat biter. $\text{kar}(D) = 1$ olamaz çünkü o zaman $D = \{0\}$ olurdu ve $\{0\}$ bir tamlık bölgesi değildir. $\text{kar}(D) = n \geq 2$ olsun. n nin asal olduğunu

Özellik / Cebirsel Yapı	Halka	Tamlık Bölgesi	Çarpık Cisim (Bölüm Halkası)	Cisim
$(R, +)$ abelyen grup	✓	✓	✓	✓
$(R, \cdot)$ yarı grup	✓	✓	✓	✓
Dağılma özellikleri var	✓	✓	✓	✓
Birim elemanlı		✓	✓	✓
Değişmeli		✓		✓
0 hariç her elemanın tersi var			✓	✓
Sıfır bölensiz		✓	✓	✓
$(R \setminus \{0\}, \cdot)$ grup			✓	✓
$(R \setminus \{0\}, \cdot)$ abelyen grup				✓
En az 2 elemanlı		✓	✓	✓

Tablo 7.1: Bir $(R, +, \cdot)$ cebirsel yapısının sağlaması gereken özellikler tablosu.

göstereceğiz. Aksini kabul edelim; yani n asal olmasın. O halde $1 < n_1, n_2 < n$ olmak üzere $n = n_1 n_2$ şeklinde yazılabilir. $e \in D$ için $ne = 0$ dır. Şimdi:

$$ne = 0 \implies \underbrace{e + e + \cdots + e}_{n\text{-tane}} = 0 \implies \underbrace{(e + \cdots + e)}_{n_1\text{-tane}} \underbrace{(e + \cdots + e)}_{n_2\text{-tane}} = 0 \implies (n_1 e)(n_2 e) = 0$$

olup D tamlık bölgesi olduğundan $n_1 e = 0$ veya $n_2 e = 0$ olmalıdır. Ancak bu durum n 'nin $ne = 0$ olacak şekilde en küçük pozitif tamsayı olması ile çelişir. O halde n asaldır. $\square$

Örnek 7.45 Birim elemanlı bir R halkasının birim elemanı ile onun en az 2 elemanlı bir S alt halkasının birim elemanı farklı olabilir. Gösteriniz.

Çözüm: $R = \mathbb{Z}_6$ ve $S = \{\bar{0}, \bar{3}\}$ alalım. Bu durumda R nin birim elemanı $\bar{1}$ dir, fakat S nin birim elemanı $\bar{3}$ dür. Ayrıca $T = \{\bar{0}, \bar{2}, \bar{4}\}$ alt halkasının birim elemanı $\bar{4}$ dür.

Teorem 7.46 D birim elemanı e olan bir tamlık bölgesi, R de D nin en az iki elemanlı bir alt halkası olsun. R birim elemanlı ise $e \in R$ dir ve e, R nin de birim elemanıdır.

İspat: $f \in R$ birim eleman olsun. Şimdi $f(fe - e) = f^2 e - fe = fe - fe = 0$ elde edilir. D bir tamlık bölgesi olduğundan $f = 0$ veya $fe - e = 0$ olur. Ancak R en az 2 elemanlı olduğundan $f \neq 0$ dır. O halde $fe - e = 0$; yani $fe = e$ bulunur. Ayrıca e, D nin birim elemanı olduğundan $fe = f$ olup $e = f$ elde edilir. $\square$

Örnek 7.47 Elemanları bir R halkasından seçilen $n \times n$ tipindeki matrislerin kümesi, matrislerdeki

bilinen toplama ve çarpma işlemi ile bir halkadır. Bu halka $M_n(R)$ ile gösterilir.

$$M_n(\mathbb{Z}) = \{ n \times n \text{ tamsayı haneli matrisler} \}$$

$$M_n(\mathbb{R}) = \{ n \times n \text{ reel haneli matrisler} \}$$

$$M_n(\mathbb{C}) = \{ n \times n \text{ kompleks haneli matrisler} \}$$

gibi. Benzer şekilde $M_n(\mathbb{Z}_7)$ ve $M_n(3\mathbb{Z})$ de tanımlıdır. $n \geq 2$ için bu halkalar değişmeli değildir. Eğer R birim elemanlı ise $M_n(R)$ de birim elemanlıdır ve birim elemanı, köşegeni 1_R olan skaler matristir. Ayrıca bu halkalar sıfır bölendirdir; mesela $M_2(\mathbb{R})$ halkasında:

$$\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} \begin{pmatrix} 8 & -2 \\ -4 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

ALİŞTIRMALAR

1. $H = \{ f \mid f : \mathbb{R} \rightarrow \mathbb{R} \text{ bir fonksiyon} \}$ kümesi üzerinde $f, g \in H$ için

$$(f + g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

işlemleri tanımlansın. $(H, +, \cdot)$ sisteminin bir halka olduğunu gösterin. $(H, +, \cdot)$ bir tamlık bölgesi midir?

2. $\mathbb{Z}$ üzerinde $a \oplus b = a + b - 1$ ve $a \odot b = a + b - ab$ işlemleri tanımlanıyor. $(\mathbb{Z}, \oplus, \odot)$ sisteminin değişmeli ve birim elemanlı bir halka olduğunu gösterin. $(\mathbb{Z}, \oplus, \odot)$ bir tamlık bölgesi midir? Bir cisim midir?

3. H bir halka, $a \in H$ olsun. $I_a = \{ x \in H \mid ax = 0 \}$ kümesi H nin bir alt halkasıdır, gösterin.

4. R birim elemanı 1 olan bir halka ve bir $a \in R$ için $a^2 = 1$ olsun. $H = \{ axa : x \in R \}$ kümesinin R nin bir alt halkası olduğunu gösteriniz.

5. $\mathbb{Z}[\sqrt{2}] = \{ x + y\sqrt{2} : x, y \in \mathbb{Z} \}$ halkası verilsin. $f : \mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}[\sqrt{2}]$ fonksiyonu $f(x + y\sqrt{2}) = x - y\sqrt{2}$ ile tanımlansın. f nin $\mathbb{Z}[\sqrt{2}]$ halkasının bir otomorfizması olduğunu gösteriniz.

6. Bir H halkasında $\forall x \in H$ için $x^2 = x$ dir. Buna göre $\forall x \in H$ için $x = -x$ olduğunu gösteriniz. (İpucu: $(x + x)$ in karesine bakınız.) Ayrıca H nin değişmeli olduğunu gösteriniz.

7. U boş olmayan bir küme ve R de U nun bütün alt kümelerinin kümesi olsun. R 'de toplama ve çarpma, $A + B = (A \cup B) \setminus (A \cap B)$ ve $A \cdot B = A \cap B$ olarak tanımlansın. $(R, +, \cdot)$ bir halka mıdır? Birim elemanlı mıdır? Değişmeli midir? Gösterin. (NOT: $+$ işlemi birleşmelidir.)

8. Bir tamlık bölgesinde karesi kendisine eşit olan elemanların sadece 0 ve 1 olduğunu gösterin.

9. R en az iki elemanlı bir halka olsun. Her $a \in R$ için $a^2 = a$ ise R 'nin karakteristiğinin 2 olduğunu gösterin. (İpucu: $(a + a)$ nin karesine bakın.)
10. $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ kümesinin bilinen kompleks sayı toplaması ve çarpması ile bir tamlık bölgesi olduğunu gösterin. Bu halkaya **Gauss² tamsayılar halkası** denir. $\mathbb{Z}[i]$ bir cisim midir?
11. $T = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$ kümesi $(\mathbb{R}, +, \cdot)$ halkasının bir alt halkası mıdır? Gösterin.
12. $A = \{a + b\sqrt[4]{5} : a, b \in \mathbb{Q}\}$ kümesi $(\mathbb{R}, +, \cdot)$ halkasının bir alt halkası mıdır?
13. R ve H iki halka olsun. $f : R \rightarrow H$ dönüşümü her $x \in R$ için $f(x) = 0_H$ olarak tanımlansın. f nin bir halka homomorfizması olduğunu gösterin. (Bu homomorfizmaya **sıfır homomorfizması** denir.)
14. R ve H iki halka $\theta : R \rightarrow H$ bir halka homomorfizması olsun.
- (i) I , R nin bir alt halkası ise $\theta(I)$ da H nin bir alt halkasıdır.
 - (ii) $\text{Çek}(\theta) = \{x \in R : \theta(x) = 0_H\}$ kümesi R nin bir alt halkasıdır.
 - (iii) R birim elemanlı halka, $H \neq \{0\}$ ve θ örten ise H da birim elemanlıdır ve $\theta(1_R) = 1_H$ dir.
15. D bir tamlık bölgesi olsun. $x \in D$ için " $x^2 = 1 \implies x = 1$ veya $x = -1$ " olduğunu gösterin. Bunun sonucu olarak, eğer D sonlu sayıda birime sahipse bu birimlerin çarpımının -1 olduğunu gösterin. Buradan, her p asal sayısı için $(p-1)! \equiv -1 \pmod{p}$ olduğunu gösterin. (Bu sonuç sayılar teorisinde Wilson Teoremi olarak bilinmektedir.)

ALİŞTIRMALARIN ÇÖZÜMLERİ

ÇÖZÜM 1. $f, g, h \in H$ olsun.

- (i) $(f + g)(x) = f(x) + g(x) \in \mathbb{R}$ olup $f + g \in H$.
- (ii) $(f + g) + h = f + (g + h)$ dir, çünkü $[f(x) + g(x)] + h(x) = f(x) + [g(x) + h(x)]$.
- (iii) $f + g = g + f$ dir, çünkü $f(x) + g(x) = g(x) + f(x)$.
- (iv) Her $x \in \mathbb{R}$ için $O(x) = 0$ şeklinde tanımlanan sıfır fonksiyonu bu halkanın sıfırıdır.
- (v) f nin $+$ işlemine göre tersi $(-f)(x) = -f(x)$ şeklinde tanımlanan fonksiyondur. Çünkü

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0 = O(x).$$

- (vi) $f \cdot g \in H$ çünkü $f(x) \cdot g(x) \in \mathbb{R}$.

²Carl Friedrich Gauss (1777-1855)

$$(vii) f(gh) = (fg)h, \text{ çünkü } f(x)[g(x)h(x)] = [f(x)h(x)]g(x).$$

$$(vii) f(g+h) = fg + fh, \text{ çünkü } f(x)[g(x) + h(x)] = f(x)g(x) + f(x)h(x). \text{ Benzer şekilde, } (f+g)h = fh + gh, \text{ çünkü } [f(x) + g(x)]h(x) = f(x)h(x) + g(x)h(x).$$

Sonuç olarak, H bir halkadır. H bir tamlık bölgesi değildir, çünkü

$$f(x) = \begin{cases} 0, & x \geq 1 \\ e^x, & x < 1 \end{cases} \quad \text{ve} \quad g(x) = \begin{cases} \cos x, & x \geq 1 \\ 0, & x < 1 \end{cases}$$

şeklinde tanımlanırsa $f \neq 0, g \neq 0$ fakat $fg = 0$ olur.

ÇÖZÜM 2. $a, b, c \in \mathbb{Z}$ olsun.

$$(i) a \oplus b = a + b - 1 \in \mathbb{Z}.$$

$$(ii) (a \oplus b) \oplus c = (a + b - 1) \oplus c = a + b + c - 2 = a \oplus (b + c - 1) = a \oplus (b \oplus c).$$

$$(iii) a \oplus b = a + b - 1 = b + a - 1 = b \oplus a.$$

$$(iv) a \oplus 1 = 1 \oplus a = a + 1 - 1 = a \text{ olup halkanın sıfırı } 1 \text{ dir.}$$

$$(v) a \oplus (2 - a) = a + 2 - a - 1 = 1 \text{ olup } a \text{ nın tersi } 2 - a \text{ dır.}$$

$$(vi) a \odot b = a + b - ab \in \mathbb{Z}.$$

(vii)

$$(a \odot b) \odot c = (a + b - ab) \odot c = a + b - ab + c - ac - bc + abc,$$

$$a \odot (b \odot c) = a \odot (b + c - bc) = a + b + c - bc - ab - ac + abc$$

olup çarpma işlemi birleşmelidir.

$$(viii) a \odot b = a + b - ab = b + a - ba = b \odot a.$$

(ix)

$$a \odot (b \oplus c) = a \odot (b + c - 1) = a + b + c - 1 - ab - ac + a = 2a + b + c - ab - ac - 1,$$

$$(a \odot b) \oplus (a \odot c) = (a + b - ab) \oplus (a + c - ac) = 2a + b + c - ab - ac - 1$$

olup $\odot$ işlemi $\oplus$ üzerine soldan dağılma özelliğine sahiptir. $\odot$ işlemi değişme özelliğine sahip olduğundan sağdan dağılma özelliği de vardır.

$$(x) a \odot 0 = 0 \odot a = a + 0 - a \cdot 0 = a \text{ olup halkanın birim elemanı } 0 \text{ dır.}$$

Sonuç olarak, $(\mathbb{Z}, \oplus, \odot)$ birim elemanlı ve değişmeli bir halkadır.

(xi) Sıfır bölen olmadığını gösterelim. Halkanın sıfırı 1, birim elemanı da 0 dır. $a \odot b = 1$ olsun. $a \neq 1$ olsun. $b = 1$ olduğunu göstereceğiz.

$$a \odot b = 1 \implies a + b - ab = 1 \implies a + b - ab - 1 = 0 \implies (a - 1)(1 - b) = 0$$

olup $a \neq 1$ olduğundan $b = 1$ olmalıdır.

Yani, $(\mathbb{Z}, \oplus, \odot)$ bir tamlık bölgesidir.

$(\mathbb{Z}, \oplus, \odot)$ bir cisim değildir, çünkü 3'ün $\odot$ işlemine göre tersine x dersek

$$x \odot 3 = 0 \implies x + 3 - 3x = 0 \implies x = \frac{3}{2} \notin \mathbb{Z}$$

olur.

ÇÖZÜM 3. $x, y \in I_a$ alalım. O zaman $ax = ay = 0$ dır

(i) $a(x - y) = a(x + (-y)) = ax + a(-y) = ax + -(ay) = ax - ay = 0 - 0 = 0$ olup $x - y \in I_a$ dır.

(ii) $a(xy) = (ax)y = 0y = 0$ olup $xy \in I_a$ dır.

Teorem 7.17 gereği I_a bir alt halkadır.

ÇÖZÜM 4. $axa, aya \in H$ alalım.

(i) $axa - aya = a(xa - ya) = a(x - y)a \in H$ dir, çünkü $x - y \in R$.

(ii) $(axa)(aya) = axa^2ya = ax1ya = a(xy)a \in H$ dir, çünkü $xy \in R$

Teorem 7.17 gereği H bir alt halkadır.

ÇÖZÜM 5.

$$\begin{aligned} f\left((a + b\sqrt{2}) + (c + d\sqrt{2})\right) &= f\left((a + c) + (b + d)\sqrt{2}\right) \\ &= (a + c) - (b + d)\sqrt{2} \\ &= (a - b\sqrt{2}) + (c - d\sqrt{2}) \\ &= f(a + b\sqrt{2}) + f(c + d\sqrt{2}). \end{aligned}$$

Ayrıca,

$$\begin{aligned} f\left((a + b\sqrt{2})(c + d\sqrt{2})\right) &= f\left((ac + 2bd) + (ad + bc)\sqrt{2}\right) \\ &= (ac + 2bd) - (ad + bc)\sqrt{2} \\ &= (a - b\sqrt{2})(c - d\sqrt{2}) \\ &= f(a + b\sqrt{2})f(c + d\sqrt{2}). \end{aligned}$$

olup f bir halka homomorfizmasıdır.

$$\begin{aligned}
 f(a + b\sqrt{2}) = f(c + d\sqrt{2}) &\implies a - b\sqrt{2} = c - d\sqrt{2} \\
 &\implies a = c \text{ ve } -b = -d \text{ (Çünkü } a, b, c, d \in \mathbb{Z}) \\
 &\implies a = c \text{ ve } b = d \\
 &\implies a + b\sqrt{2} = c + d\sqrt{2} \\
 &\implies f \text{ birebirdir.}
 \end{aligned}$$

Şimdi f nin örten olduğunu gösterelim. $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ verilsin. $a = x$ ve $b = -y$ seçilirse $f(a + b\sqrt{2}) = f(x - y\sqrt{2}) = x + y\sqrt{2}$ olup f nin örten olduğu görülür.

Sonuç olarak, f bir otomorfizmadır.

ÇÖZÜM 6. Her $x \in H$ için $(x+x)^2 = (x+x)$ olmalıdır. O halde $x^2 + x^2 + x^2 + x^2 = x + x + x + x = x + x$ ve buradan $x + x = 0$ yani $x = -x$ bulunur. Ayrıca, her $a, b \in H$ için $(a+b)^2 = a+b$ olmalıdır. Yani $a^2 + ab + ba + b^2 = a+b$ dir. $a^2 = a$ ve $b^2 = b$ olduğundan $ab + ba = 0$ yani $ab = -(ba)$ dir. $-(ba) = ba$ olacağından $ab = ba$ bulunur. Yani halka değişmelidir.

ÇÖZÜM 7.

- (i) $A, B \in R \implies A + B = A \triangle B = (A \cup B) \setminus (A \cap B) \in R$ dir.
- (ii) $(A + B) + C = (A \triangle B) \triangle C = A \triangle (B \triangle C) = A + (B + C)$ olduğunu biliyoruz.
- (iii) $A \triangle B = B \triangle A$ olduğundan $A + B = B + A$ dir.
- (iv) $A \triangle \emptyset = A$ olduğundan halkanın sıfırı boşkümedir.
- (v) $A \triangle A = \emptyset$ olduğundan $-A = A$ dir.
- (vi) $A, B \in R \implies A \cdot B = A \cap B \in R$ dir.
- (vii) $(A \cdot B) \cdot C = (A \cap B) \cap C = A \cap (B \cap C) = A \cdot (B \cdot C)$.
- (viii) $A \cdot B = A \cap B = B \cap A = B \cdot A$
- (ix) $A \cdot (B + C) = A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C) = A \cdot B + A \cdot C$ olduğu gösterilebilir. Çarpma işlemi değişmeli olduğundan sağdan dağılma özelliği de vardır.
- (x) Her $A \in R$ için $A \cdot U = A$ olup U bu halkanın birim elemanıdır.

Sonuç: R birim elemanlı ve değişmeli bir halkadır. U en az iki elemanlı ise R bir cisim değildir. Çünkü her $\emptyset \neq A \in R$ için $A \cdot X = A \cap X = U$ olacak şekilde bir $X \in R$ bulunamaz (mesela A bir elemanlı ise.)

ÇÖZÜM 8. D bir tamlık bölgesi ve $x \in D$ olsun.

$$\begin{aligned} x^2 = x &\implies x^2 - x = 0 \implies x(x - 1) = 0 \\ &\implies D \text{ bir tamlık bölgesi olduğundan } x = 0 \text{ veya } x - 1 = 0 \\ &\implies x = 0 \text{ veya } x = 1 \end{aligned}$$

ÇÖZÜM 9. $(a + a)^2 = a^2 + a^2 + a^2 + a^2$ yani $a + a = a + a + a + a$ bulunur. Buradan $2a = 0$ elde edilir. R en az 2 elemanlı olduğundan $\text{kar}(R) \neq 1$ dir. O halde $\text{kar}(R) = 2$ dir.

ÇÖZÜM 10. $a, b, c, d, e, f \in \mathbb{Z}$ olmak üzere $z = a + bi, w = c + di, t = e + fi$ olsun.

- (i) $z + w = (a + c) + (b + d)i \in \mathbb{Z}[i]$, çünkü $a + c, b + d \in \mathbb{Z}$
- (ii) $(z + w) + t = z + (w + t) = (a + c + e) + (b + d + f)i$
- (iii) $z + w = (a + c) + (b + d)i = (c + a) + (b + d)i = w + z$
- (iv) $z + (0 + 0i) = (0 + 0i) + z = a + bi$ olup $0_{\mathbb{Z}[i]} = 0 + 0i \in \mathbb{Z}[i]$ dir, çünkü $0 \in \mathbb{Z}$.
- (v) $-z = (-a) + (-b)i \in \mathbb{Z}[i]$, çünkü $-a, -b \in \mathbb{Z}$.
- (vi) $zw = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i]$, çünkü $ac - bd, ad + bc \in \mathbb{Z}$.
- (vii)

$$\begin{aligned} (zw)t &= [(ac - bd) + (ad + bc)i](e + fi) \\ &= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i \\ &= (a + bi)[(ce - df) + (cf + de)i] \\ &= z(wt) \end{aligned}$$

olup çarpma işlemi birleşmelidir.

(viii) $zw = (ac - bd) + (ad + bc)i = (ca - db) + (cb + da)i = wz$ olup çarpma işlemi değişmelidir.

(ix)

$$\begin{aligned} z(w + t) &= (a + bi)[(c + e) + (d + f)i] \\ &= (ac + ae - bd - bf) + (ad + af + bc + be)i \\ &= (ac - bd) + (ad + bc)i + (ae - bf) + (af + be)i \\ &= zw + zt \end{aligned}$$

olup çarpma işlemi toplama üzerine soldan dağılma özelliğine sahiptir. Çarpma işlemi değişmeli olduğundan sağdan dağılma özelliği de vardır.

(x) $(a + bi)(1 + 0i) = (1 + 0i)(a + bi) = a + bi$ olup halkanın birim elemanı $1 = 1 + 0i \in \mathbb{Z}[i]$ dir, çünkü $1, 0 \in \mathbb{Z}$ dir.

Şimdi, $\mathbb{Z}[i]$ nin sıfır bölenleri olmadığını gösterelim.

(xi) $zw = 0$ olsun ve $z \neq 0$ olsun. Bu durumda $a \neq 0$ veya $b \neq 0$ dir. $w = 0$ olduğunu, yani $c = d = 0$

olduğunu göstereceğiz. Aşağıdaki denklem sistemini çözeceğiz:

$$ac - bd = 0$$

$$ad + bc = 0$$

Durum 1: $a \neq 0$

1. denklemi c , 2. denklemi d ile çarpıp toplarsak $a(c^2 + d^2) = 0$ bulunur. $a \neq 0$ olup $c^2 + d^2 = 0 \implies c = 0, d = 0$ elde edilir.

Durum 2: $b \neq 0$

1. denklemi $-d$, 2. denklemi c ile çarpıp toplarsak $b(c^2 + d^2) = 0$ bulunur. $b \neq 0$ olup $c^2 + d^2 = 0 \implies c = 0, d = 0$ elde edilir.

Sonuç olarak, $\mathbb{Z}[i]$ bir tamlık bölgesidir. $\mathbb{Z}[i]$ bir cisim değildir, çünkü $1 + i$ sayısının çarpma işlemine göre tersi $\frac{1}{2} - \frac{1}{2}i \notin \mathbb{Z}[i]$ dir, çünkü $\frac{1}{2} \notin \mathbb{Z}$.

ÇÖZÜM 11. $a, b, c, d, e, f \in \mathbb{Q}$ ve $x = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in T, y = d + e\sqrt[3]{2} + f\sqrt[3]{4} \in T$ olsun.

$$x - y = (a - d) + (b - e)\sqrt[3]{2} + (c - f)\sqrt[3]{4} \in T$$

olur çünkü $a - d, b - e, c - f \in \mathbb{Q}$ dur.

$$\begin{aligned} xy &= ad + ae\sqrt[3]{2} + af\sqrt[3]{4} + bd\sqrt[3]{2} + be\sqrt[3]{4} + bf\sqrt[3]{8} + cd\sqrt[3]{4} + ce\sqrt[3]{8} + cf\sqrt[3]{16} \\ &= (ad + 2bf + 2ce) + (ae + bd + 2cf)\sqrt[3]{2} + (af + be + cd)\sqrt[3]{4} \in T \end{aligned}$$

olur, çünkü bütün katsayılar rasyoneldir. Teorem 7.17 gereği T bir alt halkadır.

ÇÖZÜM 12. $x = \sqrt[4]{5} \in A$ ve $y = \sqrt[4]{5} \in A$ alalım. $xy = \sqrt[4]{25} \notin A$ olur. Yani A bir alt halka değildir.

ÇÖZÜM 13. Her $x, y \in R$ için

$$f(x + y) = 0_H = 0_H + 0_H = f(x) + f(y),$$

$$f(x \cdot y) = 0_H = 0_H \cdot 0_H = f(x) \cdot f(y)$$

olup f bir halka homomorfizmasıdır.

ÇÖZÜM 14. (i)

$$\begin{aligned} x, y \in \theta(I) &\implies \exists a, b \in I \text{ için } \theta(a) = x, \theta(b) = y \\ &\implies \underbrace{\theta(a - b)}_{\in I} = \theta(a) - \theta(b) = x - y \quad (\text{Çünkü } \theta \text{ grup hom.}) \\ &\implies x - y \in \theta(I). \end{aligned}$$

Ayrıca

$$\underbrace{\theta(a \cdot b)}_{\in I} = \theta(a) \cdot \theta(b) = x \cdot y$$

olup $x \cdot y \in \theta(I)$ dır. Teorem 7.17 gereği $\theta(I), H$ nin alt halkasıdır.

(ii)

$$\begin{aligned} a, b \in \text{Çek}(\theta) &\implies \theta(a) = 0_H, \theta(b) = 0_H \\ &\implies \theta(a - b) = \theta(a) - \theta(b) = 0_H - 0_H = 0_H \quad (\text{Çünkü } \theta \text{ grup hom.}) \\ &\implies a - b \in \text{Çek}(\theta). \end{aligned}$$

Ayrıca

$$\theta(a \cdot b) = \theta(a) \cdot \theta(b) = 0_H \cdot 0_H = 0_H$$

olup $a \cdot b \in \text{Çek}(\theta)$ dır. Teorem 7.17 gereği $\text{Çek}(\theta), R$ nin alt halkasıdır.

(iii) θ örten olduğundan her $h \in H$ için $\exists r \in R$ vardır öyle ki $\theta(r) = h$ dir. Şimdi, her $h \in H$ için

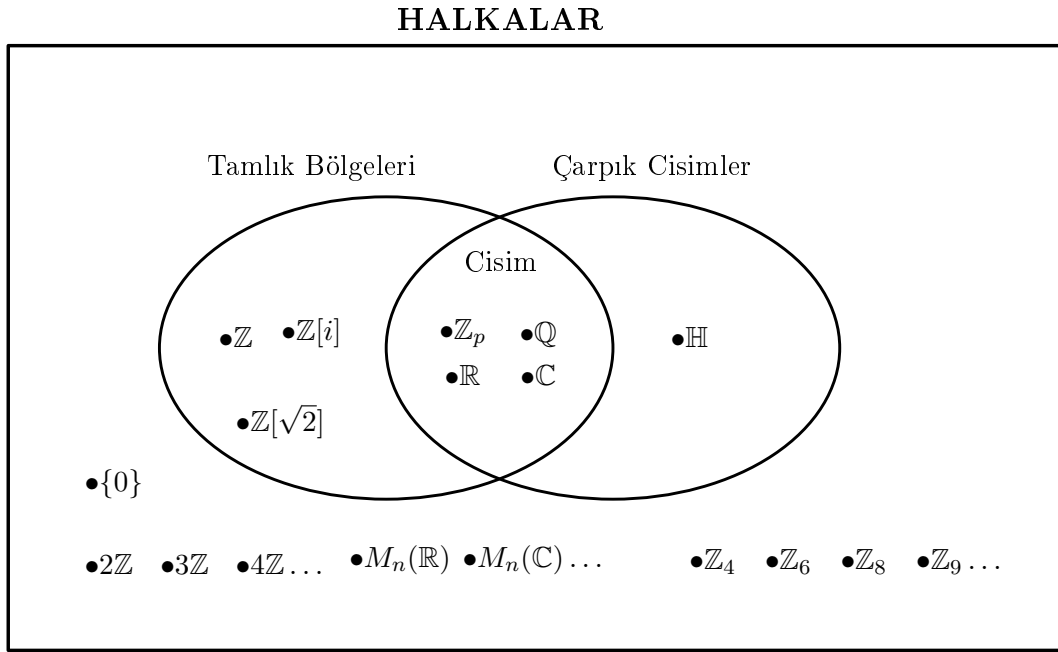
$$\begin{aligned} h &= \theta(r) = \theta(1_R \cdot r) = \theta(1_R) \cdot \theta(r) = \theta(1_R) \cdot h, \\ h &= \theta(r) = \theta(r \cdot 1_R) = \theta(r) \cdot \theta(1_R) = h \cdot \theta(1_R) \end{aligned}$$

olup H nin birim elemanlı olduğu ve $\theta(1_R) = 1_H$ olduğu görülür.

ÇÖZÜM 15. $x^2 = 1 \implies x^2 - 1 = 0 \implies (x - 1)(x + 1) = 0 \implies D$ bir tamlık bölgesi olduğundan $x - 1 = 0$ veya $x + 1 = 0 \implies x = 1$ veya $x = -1$.

D deki bütün birimler $U = \{1, -1, u_1, u_2, \dots, u_n\}$ olsun. $x \in U$ için $x^{-1} = x \iff x^2 = 1$ olup tersi kendine eşit olan elemanların sadece 1 ve -1 olduğu görülür. $u = (-1)u_1u_2 \dots u_n$ dersek u_i lerin tersi kendisi olmadığından bu çarpımın sonucu -1 dir.

Bu sonucu $\mathbb{Z}_p$ tamlık bölgesine uygularsak; $\mathbb{Z}_p$ bir cisim olduğundan $U(\mathbb{Z}_p) = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$ dir. Buradan $\overline{1 \cdot 2 \cdots (p-1)} = \overline{-1}$ yani $(p-1)! \equiv -1 \pmod{p}$ bulunur.



Şekil 7.1: Halka çeşitlerini gösteren bir şekil.

8.1 İdealler

Şimdi gruptaki normal altgrup kavramına benzer bir kavram olan “ideal” kavramını vereceğiz.

Tanım 8.1 R bir halka, I da R nin bir alt halkası olsun. Eğer her $r \in R$ için $rI \subseteq I$ ise I ya bir *sol ideal*; $Ir \subseteq I$ ise I ya bir *sağ ideal* denir. Başka bir deyişle:

$$\forall r \in R, \forall x \in I \text{ için } rx \in I \iff I \text{ sol ideal}$$

$$\forall r \in R, \forall x \in I \text{ için } xr \in I \iff I \text{ sağ ideal}$$

Eğer I hem sağ hem de sol ideal ise I ya kısaca bir *ideal* denir.

Örnek 8.2 $(\mathbb{Z}, +, \cdot)$ halkasında her $n \in \mathbb{Z}$ için $I = n\mathbb{Z}$ alt halkası bir idealdir. Çünkü, $r \in \mathbb{Z}$ ve $x \in I$ seçelim. O zaman $\exists k \in \mathbb{Z}$ için $x = nk$ dır. Bu durumda $rx = r(nk) = n(rk) \in I$ ve $xr = (nk)r = n(kr) \in I$ olup I nın bir ideal olduğu görülür.

Örnek 8.3 $(\mathbb{Z}, +, \cdot)$ halkası $(\mathbb{Q}, +, \cdot)$ halkasının bir ideali değildir. Çünkü $x = 2 \in \mathbb{Z}$ ve $r = \frac{1}{5} \in \mathbb{Q}$ seçilirse $rx = \frac{2}{5} \notin \mathbb{Z}$ olur.

Örnek 8.4 $W = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}$ halkası verilsin. $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ kümesi

W nun alt halkasıdır. (Neden?) $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in W$ ve $X = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \in I$ seçelim.

$$AX = \begin{pmatrix} ax & ay \\ cx & cy \end{pmatrix} \text{ ve } XA = \begin{pmatrix} xa + yc & xb + yd \\ 0 & 0 \end{pmatrix}$$

olup genelde $AX \notin I$ ve $XA \in I$ olduğu görülür. Yani I bir sağ idealdir ama sol ideal değildir.

Ödev: Sol ideal olup sağ ideal olmayan bir örnek bulunuz.

Örnek 8.5 A ve B bir R halkasının iki ideali olsun. $A + B = \{a + b : a \in A, b \in B\}$ kümesine A ile B nin **toplamı** denir. $A + B$ nin R nin bir ideali olduğunu gösterelim. $A + B$ nin alt halka olduğu kolayca gösterilebilir (Alıştırma 11). Şimdi $r \in R$ ve $a + b \in A + B$ alalım. A ve B ideal olduğundan $ra, ar \in A$ ve $rb, br \in B$ olur. O zaman

$$r(a + b) = ra + rb \in A + B \quad \text{ve} \quad (a + b)r = ar + br \in A + B$$

olup $A + B$ nin ideal olduğu görülür.

Örnek 8.6 Bir R halkasında $\{0\}$ ve R her zaman birer idealdir. Bunlara sırasıyla **sıfır ideali** (veya **trivial ideal**) ve **öz olmayan** ideal denir. Eğer $I \neq R$ ideal ise I ya bir **özideal** denir.

Teorem 8.7 R bir halka $U \subseteq R$ olsun. U nun bir ideal olması için gerek ve yeter şartlar:

- (i) $0 \in U$
- (ii) Her $u, v \in U$ için $u - v \in U$
- (iii) Her $u \in U$ ve $r \in R$ için $ur \in U$ ve $ru \in U$.

İspat: ($\implies$) U bir ideal olsun. U bir alt halka olduğundan $0 \in U$ dur. Ayrıca $(U, +)$ grubu $(R, +)$ grubunun altgrubu olduğundan $u, v \in U \implies u - v \in U$ olduğu açıktır (Teorem 2.8). U bir ideal olduğundan, tanımdan dolayı, (iii) sağlanır.

($\impliedby$) Şimdi (i), (ii) ve (iii) doğru olsun. $0 \in U$ olduğundan $U \neq \emptyset$ dir. $u, v \in U$ olsun. (ii) den dolayı $u - v \in U$ olduğu açıktır. $u \in R$ ve $v \in U$ olup (iii) den dolayı $uv \in U$ olur. Böylece; Teorem 7.17'den; U nun bir alt halka olduğu görülür. Ayrıca, (iii) den dolayı da U bir idealdir. $\square$

Teorem 8.8 R birim elemanlı bir halka, N de onun bir ideali olsun. Eğer N bir birim ($\cdot$ işlemine göre tersi olan bir eleman) içeriyor ise $N = R$ dir.

İspat: $u \in N$ bir birim olsun. $u^{-1} \in R$ olup N ideal olduğundan $uu^{-1} = 1_R \in N$ olur. Yine N ideal olduğundan her $r \in R$ için $r \cdot 1_R \in N$ olmalıdır. Yani her $r \in R$ için $r \in N$ olup $N = R$ elde edilir. $\square$

Sonuç 8.9 Bir F cisminin idealleri sadece $\{0\}$ ve F dir.

İspat: F nin 0 hariç her elemanı birim olduğundan sonuç açıktır. $\square$

Örnek 8.10 $(H, +, \cdot), \mathbb{R}$ den $\mathbb{R}$ ye bütün fonksiyonların halkası olsun. $I = \{f \in H : f(\frac{1}{2}) = 0\}$ kümesi H nin bir ideali midir?

Çözüm: (i) Bu halkanın sıfırı O ile gösterilen “sıfır” fonksiyonudur (Bölüm 7, Alıştırma 1). $O(\frac{1}{2}) = 0$ olduğundan $O \in I$ dır.

(ii) $f, g \in I$ ise $f(\frac{1}{2}) = g(\frac{1}{2}) = 0$ olup $(f - g)(\frac{1}{2}) = f(\frac{1}{2}) - g(\frac{1}{2}) = 0 - 0 = 0$ olup $f - g \in I$ dir.

(iii) Şimdi $h \in H$ ve $f \in I$ alalım. O halde $f(\frac{1}{2}) = 0$ dir.

$$(h \cdot f)(1/2) = h(1/2)f(1/2) = h(1/2) \cdot 0 = 0 \quad \text{ve} \quad (f \cdot h)(1/2) = f(1/2)h(1/2) = 0 \cdot h(1/2) = 0$$

olup $h \cdot f, f \cdot h \in I$ olur ve Teorem 8.7'den I bir idealdir.

Örnek 8.11 R halkası birim elemanlı ve değişmeli olsun. Eğer R nin sadece iki tane ideali var ise (yani $\{0\}$ ve R), R 'nin bir cisim olduğunu gösteriniz.

Çözüm: Her $0 \neq a \in R$ için $ba = 1$ olacak şekilde bir $b \in R$ elemanının varlığını göstermeliyiz. $0 \neq a \in R$ verilsin. $Ra = \{xa : x \in R\}$ kümesini düşünelim. Ra nın bir ideal olduğunu gösterelim:

(i) $0 \cdot a = 0$ olup $0 \in Ra$ dir. ($x = 0$ alınırsa)

(ii) $xa, ya \in Ra \implies xa - ya = \underbrace{(x - y)}_{\in R} a \in Ra$, çünkü $x - y \in R$.

(iii) $xa \in Ra$ ve $r \in R$ alalım. $r(xa) = (rx)a \in Ra$ dir, çünkü $rx \in R$ dir. Ayrıca R değişmeli olduğundan $(xa)r \in Ra$ dir.

Teorem 8.7 den dolayı Ra bir idealdir. O zaman $Ra = \{0\}$ veya $Ra = R$ olmalıdır. $Ra = \{0\}$ olamaz çünkü $1 \cdot a = a \in Ra$ ve $a \neq 0$ seçilmişti. O zaman $Ra = R$ olur. $1 \in R$ olduğundan $\exists b \in R$ için $ba = 1$ olmalıdır. O zaman $a^{-1} = b \in R$ olur.

Örnek 8.12 $\phi : H \longrightarrow K$ bir halka homomorfizması olsun. Aşağıdakileri ispatlayınız.

(i) $\text{Çek}(\phi), H$ nin bir idealidir.

(ii) A, H nin bir ideali ise $\phi(A)$ da $\phi(H)$ nin bir idealidir.

(iii) B, K nın bir ideali ise $\phi^{-1}(B)$ de H nin bir idealidir.

Çözüm (i): $\text{Çek}(\phi)$ bir alt halkadır. (Bölüm 7, Alıştırma 14). Şimdi $x \in \text{Çek}(\phi), h \in H$ alalım.

$$\phi(xh) = \phi(x)\phi(h) = 0_K\phi(h) = 0_K \quad \text{ve} \quad \phi(hx) = \phi(h)\phi(x) = \phi(h)0_K = 0_K$$

olup $xh, hx \in \text{Çek}(\phi)$ olur. Yani $\text{Çek}(\phi)$ bir idealdir.

Çözüm (ii): A bir alt halka olup $\phi(A)$ da bir alt halkadır (Bölüm 7, Alıştırma 14). Şimdi, $x \in \phi(A)$ ve $k \in \phi(H)$ alalım. Bu durumda $\exists a \in A$ için $\phi(a) = x$ ve $\exists h \in H$ için $\phi(h) = k$ dir. A bir ideal olduğundan $ah, ha \in A$ dir. O zaman

$$\phi(ah) = \phi(a)\phi(h) = xk, \phi(ha) = \phi(h)\phi(a) = kx \implies xk, kx \in \phi(A)$$

olup $\phi(A)$ bir idealdir.

Çözüm (iii): B, K nın bir ideali olsun. $\phi^{-1}(B) = \{x \in H \mid \phi(x) \in B\}$ kümesidir.

a.) $\phi : (H, +) \longrightarrow (K, +)$ grup hom. olduğundan $\phi(0_H) = 0_K$ dır ve B ideal olduğundan $0_K \in B$ dir. O halde $0_H \in \phi^{-1}(B)$ dir.

b.) $x, y \in \phi^{-1}(B) \implies \phi(x), \phi(y) \in B$ olup B bir ideal olduğundan $\phi(x) - \phi(y) \in B$ yani $\phi(x - y) \in B$ olup $x - y \in \phi^{-1}(B)$ bulunur.

c.) $x \in \phi^{-1}(B)$ ve $h \in H$ alalım. $\phi(x) \in B$ ve $\phi(h) \in K$ olup B ideal olduğundan

$$\phi(xh) = \phi(x)\phi(h) \in B \quad \text{ve} \quad \phi(hx) = \phi(h)\phi(x) \in B$$

olur. Yani $xh, hx \in \phi^{-1}(B)$ dir.

Teorem 8.7 den dolayı $\phi^{-1}(B)$ bir ideal olur.

Örnek 8.13 F bir cisim, R bir halka ve $\phi : F \longrightarrow R$ bir halka homomorfizması olsun. ϕ nin ya sıfır homomorfizması ya da 1-1 olduğunu gösterin.

Çözüm: $\text{Çek}(\phi)$ nin F nin ideali olduğunu biliyoruz. F bir cisim olduğundan idealleri sadece $\{0\}$ ve F dir. $\text{Çek}(\phi) = \{0\}$ ise ϕ 1-1 dir (Neden?). $\text{Çek}(\phi) = F$ ise ϕ sıfır homomorfizmasıdır.

Örnek 8.14 Değişmeli bir R halkasında nilpotent elemanların oluşturduğu küme bir idealdir, gösterin.

Çözüm: $N = \{x \in R : \exists n \in \mathbb{Z}^+, x^n = 0\}$ kümesi nilpotent elemanların kümesi olsun. $0 \in N$ dir, çünkü $0^1 = 0$ dir. $x \in N, r \in R$ alalım. O zaman $x^n = 0$ olacak şekilde $n \in \mathbb{Z}^+$ vardır. R değişmeli olduğundan

$$(rx)^n = (xr)^n = x^n r^n = 0 r^n = 0$$

olup $xr, rx \in N$ dir. Şimdi $x, y \in N$ olsun. O halde $x^m = 0$ ve $y^n = 0$ dir ($m, n \in \mathbb{Z}^+$). R değişmeli olduğundan binom formülü geçerlidir. Yani

$$(x - y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^{n+m-i} (-1)^i y^i.$$

Bu toplamdaki herbir terimde ya $n + m - i \geq m$ ya da $i \geq n$ dir. Yani toplamdaki herbir terim 0 dir. O halde $(x - y)^{n+m} = 0$ olup $x - y \in N$ dir. Teorem 8.7 den dolayı N bir idealdir.

Tanım 8.15 R değişmeli bir halka ve $I \neq R$ bir ideal olsun. Eğer her $a, b \in R$ için “ $ab \in I \implies a \in I$ veya $b \in I$ ” önermesi doğru ise I ya **asal ideal** denir.

Örnek 8.16 Bir R tamlık bölgesinde $\{0_R\}$ bir asal idealdir, çünkü $ab = 0 \implies a = 0$ veya $b = 0$ dir.

Lemma 8.17 $\mathbb{Z}$ halkasında $1 < n \in \mathbb{Z}$ verilsin. $P = n\mathbb{Z}$ ideali asal idealdir $\iff n$ asaldır.

İspat: ($\Leftarrow$) n asal olsun. $a, b \in \mathbb{Z}$ ve $ab \in P = n\mathbb{Z}$ olsun. O zaman $n|(ab)$ demektir. n asal olduğundan $n|a$ veya $n|b$ dir. O zaman $a \in n\mathbb{Z} = P$ veya $b \in n\mathbb{Z} = P$ olur. O halde P asal idealdir.

($\Rightarrow$) Tersine, $P = n\mathbb{Z}$ bir asal ideal olsun. n nin asal olduğunu gösterelim. n asal olmasın. O halde $n = ab$ ve $a, b > 1$ dir. $ab \in P = n\mathbb{Z}$ olup P asal ideal olduğundan $a \in n\mathbb{Z}$ veya $b \in n\mathbb{Z}$ dir. Yani $n|a$ veya $n|b$ dir. Bu bir çelişkidir, çünkü $1 < a, b < n$ verilmişti. O halde n asaldır. $\square$

Tanım 8.18 R bir halka, $M \neq R$ de onun bir ideali olsun. Eğer R nin $M \subsetneq I$ olacak şekilde başka bir I özideali yoksa M ye **maksimal ideal** denir.

Örnek 8.19 $(\mathbb{Z}, +, \cdot)$ halkasında $6\mathbb{Z}$ ideali maksimal değildir, çünkü $6\mathbb{Z} \subsetneq 3\mathbb{Z} \subsetneq \mathbb{Z}$ olup $3\mathbb{Z}$ de bir idealdir.

Örnek 8.20 $(\mathbb{Z}, +, \cdot)$ da $M = 3\mathbb{Z}$ idealinin maksimal olduğunu gösterelim. $M \subsetneq I$ olacak şekilde bir I ideali olduğunu kabul edelim. Bu durumda I da olup $3\mathbb{Z}$ de bulunmayan bir t elemanı vardır. O halde $t, 3$ 'ün katı olmadığından $t = 3k + \alpha$ şeklindedir ($k \in \mathbb{Z}, 1 \leq \alpha \leq 2$). $t - \alpha = 3k$ olup $t - \alpha \in M$ yani $t - \alpha \in I$ dir. I ideal olduğundan $t - (t - \alpha) = \alpha \in I$ dir.

$$\alpha = 1 \implies 1 \in I \implies I = \mathbb{Z} \text{ (Teorem 8.8 den)}$$

$$\alpha = 2 \implies 3 \in I, 2 \in I \implies 3 - 2 = 1 \in I \implies I = \mathbb{Z} \text{ (Teorem 8.8 den)}$$

Her iki halde de $I = \mathbb{Z}$ olup M nin maksimal ideal olduğu görülür.

Örnek 8.21 $(\mathbb{Z}, +, \cdot)$ da p asal olmak üzere $p\mathbb{Z}$ ideali maksimaldir. Çünkü $p\mathbb{Z} \subsetneq I$ olacak şekilde bir I ideali varsa $I = n\mathbb{Z}$ olacak şekilde pozitif bir n tamsayısı vardır. $p\mathbb{Z} \subsetneq n\mathbb{Z}$ olduğundan $n|p$ olmalıdır. $n \neq p$ ve p asal olduğundan $n = 1$ olmalıdır. O halde $I = 1\mathbb{Z} = \mathbb{Z}$ dir.

8.2 Bölüm Halkaları

Gruplar teorisindeki faktör grubu kavramına benzer bir kavramı halkalar için vereceğiz.

Tanım 8.22 $(R, +, \cdot)$ bir halka ve I da onun bir ideali olsun.

$$R/I = \{ I + x : x \in R \}$$

kümesinin aşağıda tanımlanan işlemlerle bir halka olduğu gösterilecektir.

$$\text{Toplama: } (I + x) \oplus (I + y) = I + (x + y)$$

$$\text{Çarpma: } (I + x) \odot (I + y) = I + (xy)$$

$(R/I, \oplus, \odot)$ halkasına R ile I nin **bölüm halkası** denir. ($\oplus$ ve $\odot$ yerine $+$ ve $\cdot$ kullanılacaktır)

Not: R/I kümesinin bu işlemlerle bir halka olduğunu göstermeden önce bu işlemlerin iyi tanımlandığını göstermeliyiz: $(I, +)$ grubu $(R, +)$ abelyen grubunun altgrubu olduğundan $I \triangleleft R$ dir. O halde toplama işlemi iyi tanımlanmıştır. (Grup teorisindeki gibi.) Şimdi çarpma işleminin iyi tanımlandığını gösterebiliriz. Yani

$$I + x = I + a \text{ ve } I + y = I + b \implies I + xy = I + ab$$

olduğunu göstermeliyiz. $I + a = I + b \iff a - b \in I$ (veya $b - a \in I$) olduğunu hatırlayalım. Buradan

$$I + x = I + a \implies x - a \in I \quad \text{ve} \quad I + y = I + b \implies y - b \in I$$

yazabiliriz. I bir ideal olduğundan $(x-a)y \in I$ ve $a(y-b) \in I$ dir. O halde $(x-a)y + a(y-b) = xy - ab \in I$ elde edilir. Yani $I + xy = I + ab$ bulunur; o halde çarpma işlemi de iyi tanımlıdır.

Not: Eğer I, R 'nin bir alt halkası olsaydı fakat bir ideali olmasaydı, çarpma işlemi iyi tanımlı olmayabilirdi. Bunu bir örnek ile açıklayalım: $\mathbb{Z}$ halkası $\mathbb{Q}$ 'nun bir alt halkasıdır, fakat ideali değildir. Şimdi

$$\mathbb{Z} + (1/2) = \mathbb{Z} + (3/2) \quad \text{ve} \quad \mathbb{Z} + (1/3) = \mathbb{Z} + (4/3) \text{ olup}$$

$$(\mathbb{Z} + (\frac{1}{2})) \cdot (\mathbb{Z} + (\frac{1}{3})) = \mathbb{Z} + (\frac{1}{6}) \text{ fakat } (\mathbb{Z} + (\frac{3}{2})) \cdot (\mathbb{Z} + (\frac{4}{3})) = \mathbb{Z} + (\frac{4}{2}) = \mathbb{Z} + 0 \text{ dir.}$$

Teorem 8.23 R bir halka ve I da onun bir ideali olsun.

- a) R/I yukarıda tanımlanan işlemlerle bir halkadır.
- b) R değişmeli halka ise R/I da değişmeli halkadır.
- c) R birim elemanlı halka ise R/I da birim elemanlıdır ve birim elemanı $I + 1_R$ dir.

İspat: a) $I + a, I + b, I + c \in R/I$ verilsin.

- (i) $(I + a) + (I + b) = I + (a + b) \in R/I$, çünkü $a + b \in R$
- (ii) $[(I + a) + (I + b)] + (I + c) = I + (a + b + c) = (I + a) + [(I + b) + (I + c)]$
- (iii) $(I + a) + (I + b) = I + (a + b) = I + (b + a) = (I + b) + (I + a)$
- (iv) $I + 0 = I$ birim eleman, çünkü $(I + a) + (I + 0) = I + (a + 0) = I + a$
- (v) $(I + a) + (I + (-a)) = I + 0$ olup $-(I + a) = I + (-a)$ dir.
- (vi) $(I + a)(I + b) = I + (ab) \in R/I$, çünkü $ab \in R$
- (vii) $[(I + a)(I + b)](I + c) = I + ((ab)c) = I + (a(bc)) = (I + a)[(I + b)(I + c)]$
- (viii) $(I + a)[(I + b) + (I + c)] = (I + a)(I + (b + c)) = I + (ab + ac) = (I + a)(I + b) + (I + a)(I + c)$ olup çarpma işleminin toplama üzerine soldan dağılma özelliği vardır. Benzer şekilde sağdan dağılma özelliği de gösterilebilir.

İspat: b) R halkası değişmeli ve $a, b \in R$ olsun. R/I da değişmelidir, çünkü:

$$(I + a)(I + b) = I + ab = I + ba = (I + b)(I + a).$$

İspat: c) $I + a \in R/I$ olsun.

$$(I + a)(I + 1_R) = I + (a \cdot 1_R) = I + a \quad \text{ve} \quad (I + 1_R)(I + a) = I + (1_R \cdot a) = I + a$$

olup $I + 1_R$ birim elemandır. $\square$

Örnek 8.24 $R = \mathbb{Z}$ halkasında $I = 4\mathbb{Z}$ idealini ele alalım. $R/I = \{I + 0, I + 1, I + 2, I + 3\}$ bölüm halkasını elde ederiz. Bu halkanın işlem tabloları şöyledir:

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

$\cdot$	$I + 0$	$I + 1$	$I + 2$	$I + 3$
$I + 0$	$I + 0$	$I + 0$	$I + 0$	$I + 0$
$I + 1$	$I + 0$	$I + 1$	$I + 2$	$I + 3$
$I + 2$	$I + 0$	$I + 2$	$I + 0$	$I + 2$
$I + 3$	$I + 0$	$I + 3$	$I + 2$	$I + 1$

Bu tablolar $\mathbb{Z}_4$ halkasının tablolarına çok benzemektedir. Aslında $\mathbb{Z}/4\mathbb{Z}$ halkası ile $\mathbb{Z}_4$ halkası izomorftir. Genel olarak $\mathbb{Z}/n\mathbb{Z}$ halkası ile $\mathbb{Z}_n$ halkası izomorftir.

Teorem 8.25 R bir halka, I da R nin bir ideali olsun. $\phi : R \longrightarrow R/I$, $\phi(x) = I + x$ şeklinde tanımlanan dönüşüm, çekirdeği I olan, örten bir homomorfizmadır. Bu homomorfizmaya R den R/I ya **doğal homomorfizma** denir.

İspat: $I + x \in R/I$ verilsin. $\phi(x) = I + x$ olup ϕ örtendir. Ayrıca $x, y \in R$ için

$$\phi(x + y) = I + (x + y) = (I + x) + (I + y) = \phi(x) + \phi(y),$$

$$\phi(xy) = I + (xy) = (I + x)(I + y) = \phi(x)\phi(y)$$

olup ϕ bir homomorfizmadır. Şimdi

$$k \in \text{Çek}(\phi) \iff \phi(k) = I + 0 = I \iff I + k = I \iff k \in I$$

olup $\text{Çek}(\phi) = I$ olduğu görülür. $\square$

Örnek 8.26 R bir halka I da onun bir ideali olsun. R/I nın değişmeli olması için gerek ve yeter şart her $x, y \in R$ için $xy - yx \in I$ olmasıdır. Gösteriniz.

Çözüm:

$$\begin{aligned}
R/I \text{ değişmeli} &\iff \forall x, y \in R \text{ için } (I + x)(I + y) = (I + y)(I + x) \\
&\iff \forall x, y \in R \text{ için } I + xy = I + yx \\
&\iff \forall x, y \in R \text{ için } I + (xy - yx) = I \\
&\iff \forall x, y \in R \text{ için } xy - yx \in I
\end{aligned}$$

Teorem 8.27 R değişmeli ve birim elemanlı bir halka ve $I \subseteq R$ bir ideal olsun. I asal idealdir $\iff R/I$ tamlık bölgesidir.

İspat: ($\implies$) I asal ideal olsun. $I \neq R$ olup R/I en az 2 elemanlıdır. $I + x, I + y \in R/I$ alalım ve R/I nin sıfırının I olduğunu hatırlayalım.

$$\begin{aligned} (I + x)(I + y) = I &\implies I + xy = I \\ &\implies xy \in I \\ &\implies x \in I \text{ veya } y \in I \quad (\text{Çünkü } I \text{ asal ideal}) \\ &\implies I + x = I \text{ veya } I + y = I \end{aligned}$$

olup R/I sıfır bölensizdir. R birim elemanlı ve değişmeli olup R/I da birim elemanlı ve değişmelidir, yani tamlık bölgesidir.

($\impliedby$) R/I bir tamlık bölgesi olsun. R/I en az 2 elemanlı olup $I \neq R$ dir. $x, y \in R$ olsun.

$$\begin{aligned} xy \in I &\implies I + xy = I \\ &\implies (I + x)(I + y) = I \\ &\implies I + x = I \text{ veya } I + y = I \quad (\text{Çünkü } R/I \text{ tamlık bölgesi}) \\ &\implies x \in I \text{ veya } y \in I \end{aligned}$$

olup I nin asal ideal olduğu gösterilmiş olur. □

Teorem 8.28 R değişmeli ve birim elemanlı bir halka, M de onun bir ideali olsun. M maksimal idealdir $\iff R/M$ cisimdir.

İspat: ($\implies$) M, R nin maksimal ideali olsun. O halde $M \neq R$ olup R/M en az iki elemanlı bir halkadır. Ayrıca; R değişmeli ve birim elemanlı olduğundan R/M de değişmeli ve birim elemanlıdır (bkz Teorem 8.23). R/M nin cisim olduğunu göstermek için sıfır hariç (yani $M + 0$ hariç) her elemanın çarpma işlemine göre tersinin olduğunu göstermeliyiz. R/M halkasının sıfırı $M + 0 = M$ olduğundan $M \neq M + x \in R/M$ elemanını seçelim. Bu durumda $x \notin M$ olur. Şimdi

$$I = \{ m + rx : m \in M, r \in R \}$$

kümesini düşünelim. Bu kümenin bir ideal olduğu kolaylıkla gösterilebilir (Alıştırma 12). Her $m \in M$ için $m = m + 0x \in I$ olduğundan ve $x = 0 + 1x \in I$ fakat $x \notin M$ olduğundan $M \subsetneq I$ şartının sağlandığı görülür. M maksimal olduğundan $I = R$ olmalıdır. $1 \in R$ olduğundan $1 = m + ax$ olacak şekilde $m \in M, a \in R$ vardır. Yani $1 - ax \in M$ dir. Buradan

$$(M + a)(M + x) = M + ax = M + 1$$

sonucu bulunur. O halde $M + x$ in çarpma işlemine göre tersi $M + a$ dır.

($\Leftarrow$) M, R nin bir ideali ve R/M bir cisim olsun. Bir cismin sıfırı ile birim elemanı farklı olduğundan $M \neq M + 1$ olup $1 \notin M$ dir. O halde $M \neq R$ dir. $M \subsetneq I \subseteq R$ olacak şekilde bir I idealinin olduğunu kabul edelim. $x \in I \setminus M$ alalım. $x \notin M$ olduğundan $M + x \neq M$ olup $M + x$ in R/M içerisinde çarpma işlemine göre tersi vardır. $M + x$ in tersine $M + a$ diyelim. O halde

$$(M + x)(M + a) = M + xa = M + 1$$

olup $1 - xa \in M \subsetneq I$ olur. $x \in I$ ve I ideal olduğundan $xa \in I$ dır. Bu yüzden

$$1 = (1 - xa) + xa \in I$$

olur. Bu ise $I = R$ olduğunu gösterir (bkz. Teorem 8.8). Yani M maksimal idealdir. $\square$

ALIŞTIRMALAR

1. $R = \mathbb{Z}_{12}$ halkasının bütün ideallerini, bölüm halkalarını, asal ve maksimal ideallerini belirleyiniz.

2. İki idealin kesişiminin de bir ideal olduğunu gösteriniz.

3. A ve B bir R halkasının iki ideali olsun.

$$A \cdot B = \left\{ \sum_{i=1}^n a_i b_i : a_i \in A, b_i \in B, n \in \mathbb{Z}^+ \right\}$$

kümesine A ile B nin **çarpımı** denir. $A \cdot B$ nin R nin bir ideali olduğunu gösteriniz.

4. A ve B bir R halkasının iki ideali ise $A \cdot B \subseteq A \cap B$ olduğunu gösteriniz.

5. R değişimli bir halka, $a \in R$ olsun. $I_a = \{x \in R \mid ax = 0\}$ kümesi R nin bir idealidir, gösteriniz.

6. R değişmeli bir halka ve N de onun bir ideali olsun.

$$\sqrt{N} = \{a \in R : \text{Bir } n \in \mathbb{Z}^+ \text{ için } a^n \in N\}$$

kümesine N nin **radikali** denir. $\sqrt{N}$ nin R nin bir ideali olduğunu ve $\sqrt{\sqrt{N}} = \sqrt{N}$ olduğunu gösterin.

7. R değişmeli bir halka, $K \subseteq R$ olsun. $\text{Ann}(K) = \{a \in R : \text{Her } x \in K \text{ için } ax = 0\}$ kümesinin R nin bir ideali olduğunu gösterin. Bu kümeye K nin **sıfırlayıcısı** veya **annihilatörü** denir.

8. $\mathbb{Z}_{12}$ de $\text{Ann}(\{\bar{3}\})$, $\text{Ann}(\{\bar{4}\})$ ve $\text{Ann}(\{\bar{3}, \bar{4}\})$ ideallerini bulunuz.

9. A ve B değişmeli bir R halkasının iki ideali olsun. $A:B = \{x \in R : \text{Her } b \in B \text{ için } xb \in A\}$ kümesinin R nin bir ideali olduğunu gösterin.

10. A ve B bir R halkasının iki ideali ve $A \cap B = \{0\}$ olsun. Her $a \in A$ ve her $b \in B$ için $ab = 0$ olduğunu gösterin.

11. A ve B bir R halkasının iki ideali ise $A + B$ 'nin bir alt halka olduğunu gösterin.

12. Teorem 8.28'nin ispatında geçen I kümesinin bir ideal olduğunu gösterin.

ALİŞTIRMALARIN ÇÖZÜMLERİ

ÇÖZÜM 1. $\mathbb{Z}_{12}$ nin 6 tane ideali vardır.

$I = \{0\}$	$R/I = \{I, I \oplus \bar{1}, I \oplus \bar{2}, \dots, I \oplus \bar{11}\}$
$J = \{0, \bar{6}\}$	$R/J = \{J, J \oplus \bar{1}, J \oplus \bar{2}, J \oplus \bar{3}, J \oplus \bar{4}, J \oplus \bar{5}\}$
$K = \{0, \bar{3}, \bar{6}, \bar{9}\}$	$R/K = \{K, K \oplus \bar{1}, K \oplus \bar{2}\}$
$L = \{0, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$	$R/L = \{L, L \oplus \bar{1}\}$
$M = \{0, \bar{4}, \bar{8}\}$	$R/M = \{M, M \oplus \bar{1}, M \oplus \bar{2}, M \oplus \bar{3}\}$
$N = \mathbb{Z}_{12}$	$R/N = \{N\}$
Asal idealler :	K, L
Maksimal idealler :	K, L

ÇÖZÜM 2. I ve J bir R halkasının iki ideali olsun.

(i) I ve J ideal olduklarından $0 \in I$ ve $0 \in J$ olup $0 \in I \cap J$ dir.

(ii) $x, y \in I \cap J \implies x, y \in I$ ve $x, y \in J \implies I$ ideal olduğundan $x - y \in I$ ve J ideal olduğundan $x - y \in J \implies x - y \in I \cap J$.

(iii) Şimdi $r \in R$ ve $x \in I \cap J$ alalım. O zaman $x \in I$ ve $x \in J$ olur.

$$\left. \begin{array}{l} rx, xr \in I \text{ çünkü } r \in R, x \in I \text{ ve } I \text{ ideal} \\ rx, xr \in J \text{ çünkü } r \in R, x \in J \text{ ve } J \text{ ideal} \end{array} \right\} \implies rx, xr \in I \cap J$$

Teorem 8.7'den $I \cap J$ bir idealdir.

ÇÖZÜM 3. $A \cdot B$ kümesi A 'daki elemanlar ile B 'deki elemanların ikili çarpımlarının sonlu toplamından oluşmaktadır. Buna göre:

(i) $0 \in A, 0 \in B$ olup $0 = 0 \cdot 0$ olup $0 \in A \cdot B$ olur. ($a_1 = b_1 = 0$ ve $n = 1$ alınır.)

(ii) $x = a_1b_1 + \dots + a_nb_n \in AB$ ve $y = c_1d_1 + \dots + c_md_m \in AB$ olsun. ($m, n \in \mathbb{Z}^+; a_i, c_i \in A; b_i, d_i \in B$).

$$\begin{aligned} x - y &= a_1b_1 + \dots + a_nb_n - (c_1d_1 + \dots + c_md_m) \\ &= a_1b_1 + \dots + a_nb_n + (-c_1)d_1 + \dots + (-c_m)d_m \end{aligned}$$

olup A ideal olduğundan $(-c_i) \in A$ dır ve $m + n \in \mathbb{Z}^+$ olduğundan $x - y \in AB$ olur.

(iii) $x = a_1b_1 + \cdots + a_nb_n \in AB$ ve $r \in R$ alalım. A ideal olduğundan $i = 1, \dots, n$ için $ra_i \in A$ olup

$$rx = r(a_1b_1 + \cdots + a_nb_n) = (ra_1)b_1 + \cdots + (ra_n)b_n \in AB.$$

Benzer şekilde B ideal olduğundan $i = 1, \dots, n$ için $b_ir \in B$ olup

$$xr = (a_1b_1 + \cdots + a_nb_n)r = a_1(b_1r) + \cdots + a_n(b_nr) \in AB.$$

Teorem 8.7 den dolayı AB bir ideal olur.

ÇÖZÜM 4. $a_i \in A$ ve $b_i \in B$ olmak üzere $x = a_1b_1 + \cdots + a_nb_n \in AB$ alalım. Şimdi A bir ideal ve $i = 1, 2, \dots, n$ için $b_i \in R$ olduğundan $a_1b_1, \dots, a_nb_n \in A$ dir. O halde $x = a_1b_1 + \cdots + a_nb_n \in A$ dir. Benzer şekilde, B bir ideal ve $i = 1, 2, \dots, n$ için $a_i \in R$ olduğundan $a_1b_1, \dots, a_nb_n \in B$ dir. O halde $x = a_1b_1 + \cdots + a_nb_n \in B$ olur. Yani $x \in A \cap B$ dir. $AB \subseteq A \cap B$ elde edilmiş olur.

ÇÖZÜM 5.

(i) $0 \in I_a$ dır çünkü $a \cdot 0 = 0$

(ii) $x, y \in I_a$ olsun. $a(x - y) = ax - ay = 0 - 0 = 0$ olup $x - y \in I_a$

(iii) $x \in I_a, r \in R$ olsun. $a(xr) = (ax)r = 0r = 0$ olup $xr \in I_a$ dır. Ayrıca $a(rx) = a(xr)$ (çünkü R değişmeli) $= (ax)r = 0r = 0$ olup $rx \in I_a$ elde edilir.

Teorem 8.7 den dolayı I_a bir ideal olur.

ÇÖZÜM 6.

(i) N ideal olduğundan $0 \in N$ dir. $0^1 = 0 \in N$ olup $1 \in \mathbb{Z}^+$ olduğundan $0 \in \sqrt{N}$ dir.

(ii) $x, y \in \sqrt{N}$ yani $x^m \in N, y^n \in N$ olsun ($m, n \in \mathbb{Z}^+$). R değişmeli olduğundan binom formülü geçerlidir; yani

$$(x - y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^{n+m-i} (-1)^i y^i.$$

Burada ya “ $(x$ in kuvveti) $\geq m$ ” ya da “ $(y$ nin kuvveti) $\geq n$ ” önermesi doğru olup, her bir terimde N nin bir elemanı çarpım durumundadır. N bir ideal olduğundan her bir terim N nin bir elemanıdır. O halde $(x - y)^{m+n} \in N$ olup $m + n \in \mathbb{Z}^+$ olacağından $x - y \in \sqrt{N}$ dir.

(iii) $r \in R$ ve $x \in \sqrt{N}$ olsun. En az bir $n \in \mathbb{Z}^+$ için $x^n \in N$ olsun. R değişmeli olduğundan ve N ideal olduğundan

$$(rx)^n = (xr)^n = \underbrace{x^n}_{\in N} \underbrace{r^n}_{\in R} \in N$$

olup $rx, xr \in \sqrt{N}$ dir.

Teorem 8.7 den dolayı $\sqrt{N}$ bir ideal olur.

(iv) Şimdi de $\sqrt{\sqrt{N}} = \sqrt{N}$ olduğunu gösterelim. $n, m \in \mathbb{Z}^+$ ise $nm \in \mathbb{Z}^+$ olduğu ve $1 \in \mathbb{Z}^+$ olduğu hatırlanırsa;

$$\begin{aligned} x \in \sqrt{\sqrt{N}} &\implies \exists n \in \mathbb{Z}^+, x^n \in \sqrt{N} \\ &\implies \exists m \in \mathbb{Z}^+, (x^n)^m \in N \\ &\implies x^{nm} \in N \\ &\implies x \in \sqrt{N}. \end{aligned}$$

Ayrıca, $x \in \sqrt{N} \implies x^1 \in \sqrt{N} \implies x \in \sqrt{\sqrt{N}}$, olup $\sqrt{\sqrt{N}} = \sqrt{N}$ elde edilir.

ÇÖZÜM 7.

(i) Her $x \in K$ için $0 \cdot x = 0$ olup $0 \in \text{Ann}(K)$ dir.

(ii) $a, b \in \text{Ann}(K)$ ise her $x \in K$ için $ax = bx = 0$ olup $(a - b)x = ax - bx = 0$ olduğundan $a - b \in \text{Ann}(K)$ dir.

(iii) $r \in R, a \in \text{Ann}(K)$ olsun. O halde her $x \in K$ için $ax = 0$ dir. R değişmeli olduğundan, her $x \in K$ için

$$(ra)x = r(ax) = r \cdot 0 = 0 \quad \text{ve} \quad (ar)x = (ra)x = r(ax) = 0$$

olup $ra, ar \in \text{Ann}(K)$ dir.

Teorem 8.7 den dolayı $\text{Ann}(K)$ bir ideal olur.

ÇÖZÜM 8.

$$\begin{aligned} \text{Ann}(\{\bar{3}\}) &= \{a \in \mathbb{Z}_{12} : \bar{3} \odot a = \bar{0}\} = \{\bar{0}, \bar{4}, \bar{8}\} \\ \text{Ann}(\{\bar{4}\}) &= \{a \in \mathbb{Z}_{12} : \bar{4} \odot a = \bar{0}\} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} \\ \text{Ann}(\{\bar{3}, \bar{4}\}) &= \{a \in \mathbb{Z}_{12} : \bar{3} \odot a = \bar{0} \text{ ve } \bar{4} \odot a = \bar{0}\} = \{\bar{0}\} \end{aligned}$$

ÇÖZÜM 9.

(i) Her $b \in B$ için $0 \cdot b = 0 \in A$ olup $0 \in A:B$ dir.

(ii) $x, y \in A:B$ ise her $b \in B$ için $xb, yb \in A$ dir. $(x - y)b = xb - yb \in A$ olup $x - y \in A:B$ dir.

(iii) $x \in A:B$ ve $r \in R$ alalım. Her $b \in B$ için $xb \in A$, R değişmeli ve A ideal olduğundan

$$(xr)b = (rx)b = r(\underbrace{xb}_{\in A}) \in A$$

olur. O halde $rx, xr \in A:B$ dir.

Teorem 8.7 den dolayı $A:B$ bir idealdir.

ÇÖZÜM 10.

$$\begin{aligned} a \in A, b \in B &\implies a \in A, b \in R \text{ ve } A \text{ ideal olup } ab \in A, \\ a \in A, b \in B &\implies a \in R, b \in B \text{ ve } B \text{ ideal olup } ab \in B. \end{aligned}$$

Yani $ab \in A \cap B = \{0\}$ dir. O halde $ab = 0$ dir.

ÇÖZÜM 11. $x = a_1 + b_1 \in A + B$ ve $y = a_2 + b_2 \in A + B$ alalım.

(i) $x - y = (a_1 - a_2) + (b_1 - b_2) \in A + B$ dir, çünkü A alt halka olduğundan $(a_1 - a_2) \in A$ ve B alt halka olduğundan $(b_1 - b_2) \in B$ dir (Teorem 7.17) .

(ii) $xy = a_1a_2 + a_1b_2 + b_1a_2 + b_1b_2$ elde edilir. Şimdi bu toplamdaki terimlere teker teker bakalım:

$$\begin{aligned} a_1a_2 &\in A, \text{ çünkü } A \text{ alt halka} \\ a_1b_2 &\in A, \text{ çünkü } A \text{ ideal ve } b_2 \in R \\ b_1a_2 &\in B, \text{ çünkü } B \text{ ideal ve } a_2 \in R \\ b_1b_2 &\in B, \text{ çünkü } B \text{ alt halka} \end{aligned}$$

O halde, A ve B alt halka olduklarından $(a_1a_2 + a_1b_2) \in A$ ve $(b_1a_2 + b_1b_2) \in B$ olup $xy \in A + B$ elde edilir.

Teorem 7.17 gereği $A + B$ bir alt halkadır.

ÇÖZÜM 12. $I = \{m + rx : m \in M, r \in R\}$ kümesini ele alıyoruz.

(i) $m = r = 0$ alınırsa $0 + 0x = 0 \in I$ olduğu görülür. (M ideal olduğundan $0 \in M$ dir.)

(ii) $m_1, m_2 \in M$ ve $r_1, r_2 \in R$ olmak üzere $a = m_1 + r_1x \in I$ ve $b = m_2 + r_2x \in I$ alalım. M ideal olduğundan $m_1 - m_2 \in M$ dir ve R halka olduğundan $r_1 - r_2 \in R$ dir. O halde

$$a - b = \underbrace{(m_1 - m_2)}_{\in M} + \underbrace{(r_1 - r_2)}_{\in R} x \in I.$$

(iii) $m \in M$ ve $r \in R$ olmak üzere $a = m + rx \in I$ ve $y \in R$ alalım. M ideal olduğundan $ym \in M$ dir. O halde

$$ya = y(m + rx) = ym + y(rx) = \underbrace{ym}_{\in M} + \underbrace{(yr)}_{\in R} x \in I$$

elde edilir. Ayrıca, R değişmeli olduğundan $ay \in I$ dir.

Teorem 8.7 den dolayı I bir idealdir.