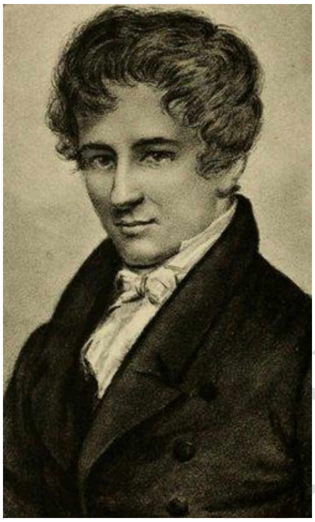
3. BÖLÜM
GRUBA GİRİŞ



Niels Henrik Abel
(05.08.1802, Nedstrand, Norveç – 06.04.1829, Froland Municipality, Norveç)

GRUP KAVRAMI

3.1. Tanım: $A \neq \emptyset$ ve A kümesi üzerinde tanımlı ★ işlemi tanımlansın. Eğer (A, ★) sistemi üzerinde,

G1) ★ işleminin kapalılık özelliği,
G2) ★ işleminin birleşme özelliği,
G3) ★ işlemine göre birim (etkisiz) eleman,
G4) A kümesinin her elemanının ★ işlemine göre tersi,

aksiyomları var ise (A, ★) sistemine grup denir.

Beşinci aksiyom olarak "★" işleminin değişme özelliği varsa (A, ★) sistemine değişmeli grup (Abel grubu) denir.

Bir işlem varsa kapalıdır. Çünkü işlem, fonksiyon üzerinde tanımlıdır. Dolayısıyla işlem mevcutsa kapalılık özelliğine ihtiyaç yoktur. Ama tanımlanan işlem olup olmadığı kapalılık özelliği ile belirlenir. Bu sebepten fonksiyon üzerinde tanımlı gruptan bahsediliyor ve fonksiyon aşikârsa kapalılık özelliğine bakılmaz. Ama fonksiyon olduğu aşikârlık yoksa bu durumda kapalılık özelliği incelenmelidir.

Örnek: $\mathbb{Z}$ tamsayılar kümesi üzerinde Δ işlemi;

$$x \,\Delta\, y = x + y + 3$$

tanımlanıyor, $(\mathbb{Z}, \Delta)$ işlemin değişmeli grup olduğunu gösteriniz.

Çözüm:

G1) Her $x, y \in \mathbb{Z}$ için

$$x \,\Delta\, y = x + y + 3 \in \mathbb{Z}$$

olduğundan kapalılık özelliği vardır.

G2) Her $x, y, z \in \mathbb{Z}$ için

$$x \,\Delta\, (y \,\Delta\, z) = (x \,\Delta\, y) \,\Delta\, z$$
$$x \,\Delta\, (y + z + 3) = (x + y + 3) \,\Delta\, z$$
$$x + (y + z + 3) + 3 = (x + y + 3) + z + 3$$
$$x + y + z + 6 = x + y + z + 6$$

olduğundan birleşme özelliği vardır.

G3) Her $x \in \mathbb{Z}$ için

$$x \,\Delta\, e = e \,\Delta\, x = x$$
$$x + e + 3 = e + x + 3 = x$$
$$e = -3$$

olduğundan Δ işleminin birim (etkisiz) elemanı –3 dür.

G4) Her $x \in \mathbb{Z}$ için

$$x \,\Delta\, x^{-1} = x^{-1} \,\Delta\, x = e$$
$$x + x^{-1} + 3 = x^{-1} + x + 3 = -3$$
$$x^{-1} = -x - 3$$

olduğundan Δ işleminde x^{-1} in ters elemanı $-x - 3 \in \mathbb{Z}$ dir.

G5) Her $x, y \in \mathbb{Z}$ için

$$x \,\Delta\, y = y \,\Delta\, x$$
$$x + y + 3 = y + x + 3$$

olduğundan değişme özelliği vardır.

Görüldüğü gibi G1, G2, G3 ve G4 aksiyomunu sağladığından $(\mathbb{Z}, \Delta)$ sistemi değişmeli (Abel) grubudur.

Örnek: $\mathcal{M}$ kümeler ailesini olmak üzere, kümeler üzerinde tanımlanan birleşme ($\cup$) işleminin bir grup olup–olmadığını araştırınız.

Çözüm: Sadece G4 özelliğini inceleyelim

G4) $A \in \mathcal{M}$ olmak üzere,

$$A \cup A^{-1} = A^{-1} \cup A = \emptyset$$

olacak şekilde her zaman $A^{-1} \in \mathcal{M}$ kümesi bulunamaz. Bu şartın sağlanması için, özel olarak $A = A^{-1} = \emptyset$ olmalıdır. O halde her $A \in \mathcal{M}$ nın ters elemanı yoktur.

Buna göre $(\mathcal{M}, \cup)$ sistemi grup değildir.

Örnek: i) $(\mathbb{N}, +)$ sistemi her elemanın tersi olmadığından grup değildir.

ii) $(\mathbb{Z}, +)$ sistemi değişmeli bir gruptur.

iii) $(\mathbb{N}\backslash\{0\}, .)$ ve $(\mathbb{Z}\backslash\{0\}, .)$ sistemleri her elemanın tersi olmadığından grup değildir.

iv) $(\mathbb{R}, .)$ sistemi grup değildir. Çünkü 0 sayısının tersi yoktur. Fakat $(\mathbb{R}\backslash\{0\}, .)$ sistemi değişmeli bir gruptur.

Bu örneğin çözümü okuyucuya bırakılmıştır.

Örnek: $(\mathbb{Z}_{/5}\{\bar{0}\}, \cdot)$ sisteminin değişmeli bir grup olduğunu gösteriniz.

Çözüm: $\mathbb{Z}_{/5}\{\bar{0}\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ kümesi üzerinde,

$\bullet$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

tablosu oluşturulacaktır. Buna göre,

i) Tabloda bütün elemanların işlemlerinin sonucu mevcut olduğundan kapalılık özelliği vardır.

ii) Çarpma işleminin birleşme özelliği vardır.

iii) Çarpma işleminin birim elemanı $\bar{1}$ dir.

iv) Çarpma işleminin her elemanın tersi vardır.

v) Tablo birinci köşegene göre simetrik olduğundan çarpma işleminin değişme özelliği vardır.

O halde $(\mathbb{Z}_{/5} - \{\bar{0}\}, \cdot)$ sisteminin değişmeli bir gruptur. //

Bu örneği genellersek $m \in \mathbb{Z}^+$ olmak üzere $(\mathbb{Z}_{/m}, +)$ sistemi değişmeli bir grup olduğunu gösterir.

3.1. Not: $(A, \star)$ sistemi grup ise "$\star$" işleminin tablosunda, herhangi bir satırı veya sütunda bir elemanın sadece bir kez bulunur.

Örnek: $A = \{1, 2, 3, 4\}$ olmak üzere $\star$ işlemi olarak aşağıda verilen tablo tanımlansın.

$\star$	1	2	3	4
1	2	3	4	1
2	3	a	b	2
3	4	1	2	3
4	1	2	3	c

Bu $(A, \star)$ sisteminin değişmeli gruptur. a, b ve c harflerinin yerinde bulunması gereken elemanları bulalım.

Çözüm: $(A, \star)$ sistemi bir değişmeli grup olduğundan her sütunda her eleman bir kez kullanacağımızdan 2. sütunda $a = 3, b = 1$ ve $c = 4$ dür.

Örnek: $i = \sqrt{-1}$ biçiminde tanımlanan i sayısı Kompleks analiz derslerinde incelenir. Burada $i^2 = -1, i^3 = -i, i^4 = 1$ olduğunu görebilirsiniz. i sayısının detayına Kompleks analiz dersine havale ederek burada $A = \{1, i, -1, -i\}$ kümesini ele alalım. Kompleks sayılardaki i sayısının kuvveti bir gruptur. Gerçekten;

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

i) Tabloda bütün elemanların işlemlerinin sonucu mevcut olduğundan kapalılık özelliği vardır.

ii) Tablodan görüldüğü gibi birleşme özelliği vardır. (Neden?)

iii) Tabloya göre birim eleman 1'dir.

iv) $1^{-1} = 1, (-1)^{-1} = -1, i^{-1} = -i$ ve $(-i)^{-1} = i$ olup her elemanın tersi vardır.

$(A, \cdot)$ bir gruptur.

Örnek: Reel sayılar üzerinde tanımlı bileşke fonksiyonlar birer gruptur. Gerçekten;

i) Fonksiyon olduğu belirli olduğundan kapalılık özelliğine bakmaya gerek yoktur.

ii) Fonksiyonlara giriş konusunda 5.5. teoremde birleşme özelliği gösterilmiştir.

iii) Fonksiyonlara giriş konusunda 5.6. teoremde I birim fonksiyondur.

iv) Fonksiyonlara giriş konusunda 5.7. teoremde ters fonksiyon teoremi verilmiştir.

Buna göre bileşke fonksiyonlar gruptur. Ama bileşke fonksiyonlar değişmeli grup değildir. Değişmeli olmadığına dair bir örnek verelim:

$f(x) = 3x + 5$ ve $g(x) = -x + 2$ ise;
$(g \circ f)(x) = g(3x + 5) = -3x - 5 + 2 = -3x - 3$
$(f \circ g)(x) = f(-x + 2) = 3(-x + 2) + 5 = -3x + 11$

$f \circ g \neq f \circ g$

Şu halde $(\mathbb{R}, f)$ sistemi gruptur. Ama değişme özelliği yoktur.

Örnek: 2×2 boyutundaki matrisler toplama işlemine göre değişmeli gruptur.

Çözüm:

G1) $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ birer matris olsunlar.

$$A + B = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}$$

sonucu da bir matris olduğundan kapalıdır.

G2) $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}, C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$ birer matris olsunlar.

$$\begin{aligned} A + (B + C) &= \left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right) + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \\ &= \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \\ &= \begin{bmatrix} (a_1 + a_2) + a_3 & (b_1 + b_2) + b_3 \\ (c_1 + c_2) + c_3 & (d_1 + d_2) + d_3 \end{bmatrix} \\ &= \begin{bmatrix} a_1 + (a_2 + a_3) & b_1 + (b_2 + b_3) \\ c_1 + (c_2 + c_3) & d_1 + (d_2 + d_3) \end{bmatrix} \\ &= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 + a_3 & b_2 + b_3 \\ c_2 + c_3 & d_2 + d_3 \end{bmatrix} \\ &= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \right) \\ &= A + (B + C) \end{aligned}$$

olup birleşmelidir.

G3) $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ matrisinde

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

olup $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ matrisi toplama işlemine göre birim matrisidir.

G4) $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ matrisinin ters matrisi $-A = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$ dir. Gerçekten;

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

G5) $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ birer matris iseler toplamaya göre değişmeli olduğununu göstemek okuyucuya bırakılmıştır.

Şu halde $(A_{2\times 2}, +)$ değişmeli gruptur.

Örnek: Permütasyon konusunda tanımlanan Permütasyon fonksiyonları P(M) ile gösterirsek P(M) bileşke fonksiyon işlemleri üzerinde gruptur.

Çözüm: $M \neq \varnothing$ bir küme ve $M \rightarrow M$ ye 1-1 ve örten fonksiyon olsunlar.

i) P(M) fonksiyon olduğundan kapalılık özelliğine bakmaya gerek yoktur.

ii) $f, g, h \in P(M)$ ise $f \circ (g \circ h) = (f \circ g) \circ h$ dir.

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

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

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

olmak üzere,

$$\begin{aligned} f \circ (g \circ h) &= \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ (f \circ (g \circ h))(a_1) & (f \circ (g \circ h))(a_2) & \dots & (f \circ (g \circ h))(a_n) \end{pmatrix} \\ &= \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ ((f \circ g) \circ h)(a_1) & ((f \circ g) \circ h)(a_2) & \dots & ((f \circ g) \circ h)(a_n) \end{pmatrix} \\ &= (f \circ g) \circ h \end{aligned}$$

olup bileşke özelliği vardır.

iii) $I_M : M \to M$ birim dönüşümü 1-1 ve örten olup bileşke işleminin birim elemanıdır. Yani her $f \in P(M)$, $f \circ I_M = I_M \circ f$ olacak şekilde $I_M = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ permütasyon fonksiyonu vardır.

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

Şu halde $(P(M), \circ)$ sistemi gruptur. Bu gruba permütasyon grubu veya simetrik grup adı verilir.

Örnek: $A_1, A_2, \dots, A_n$ gruplar olmak üzere

$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) : 1 \leq i \leq n, a_i \in A_i\}$

kümesi için $A_1 \times A_2 \times \dots \times A_n$ kümesi üzerinde çarpma işlemi her $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in A_1 \times A_2 \times \dots \times A_n$ için

$(a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$

tanımlanırsa $(A_1 \times A_2 \times \dots \times A_n, \cdot)$ Abelyen bir gruptur.

Çözüm: i) her $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in A_1 \times A_2 \times \dots \times A_n$ için

$$(a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n) = (a_1b_1, a_2b_2, \dots, a_nb_1) \in A_1 \times A_2 \times \dots \times A_n$$

olduğundan kapalıdır.

ii) $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n), (c_1, c_2, \dots, c_n) \in A_1 \times A_2 \times \dots \times A_n$ ise

$$\begin{aligned}
&(a_1, a_2, \dots, a_n) \cdot [(b_1, b_2, \dots, b_n) \cdot (c_1, c_2, \dots, c_n)] \\
&= (a_1, a_2, \dots, a_n) \cdot (b_1c_1, b_2c_2, \dots, b_nc_n) \\
&= (a_1(b_1c_1), a_2(b_2c_2), \dots, a_n(b_nc_n)) \\
&= ((a_1b_1)c_1), (a_2b_2)c_2), \dots, (a_nb_n)c_n)) \\
&= [(a_1b_1, a_2b_2, \dots, a_nb_n) \cdot (c_1, c_2, \dots, c_n) \\
&= [(a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n)] \cdot (c_1, c_2, \dots, c_n)
\end{aligned}$$

olduğundan bileşke özelliği vardır.

iii) $(a_1, a_2, \dots, a_n) \in A_1 \times A_2 \times \dots \times A_n$ ise her $1 \leq i \leq n$ için $a_i \in A_i$ grup olup $e_i \in A_i$ vardır.

$(a_1, a_2, \dots, a_n) \cdot (e_1, e_2, \dots, e_n) = (a_1e_1, a_2e_2, \dots, a_ne_n) = (a_1, a_2, \dots, a_n)$ olduğundan $(e_1, e_2, \dots, e_n) \in A_1 \times A_2 \times \dots \times A_n$ birim elemanı vardır.

iv) $(a_1, a_2, \dots, a_n) \in A_1 \times A_2 \times \dots \times A_n$ ise her $1 \leq i \leq n$ için $a_i \in A_i$ grup olup $a_i^{-1} \in A_i$ vardır.

$(a_1, a_2, \dots, a_n) \cdot (a_1^{-1}, a_2^{-1}, \dots, a_n^{-1}) = (a_1a_1^{-1}, a_2a_2^{-1}, \dots, a_na_2^{-1}) = (e_1, e_2, \dots, e_n)$ olduğundan $(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1}) \in A_1 \times A_2 \times \dots \times A_n$ birim elemanı vardır.

v) $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in A_1 \times A_2 \times \dots \times A_n$ ise

$$\begin{aligned}
(a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n) &= (a_1b_1, a_2b_2, \dots, a_nb_n) \\
&= (b_1a_1, b_2a_2, \dots, b_na_n) \\
&= (b_1, b_2, \dots, b_n) \cdot (a_1, a_2, \dots, a_n)
\end{aligned}$$

olduğundan değişme özelliği vardır.

Şu halde $(A_1 \times A_2 \times \dots \times A_n, \ \cdot\ )$ sistemi gruptur.

3.2. Not: Soyut cebirde çarpımsal notasyon tercih edilmektedir. Mesela a^{-1} ile a sayısının tersi gösterilirken, aynı ifade toplamsal notasyonlar içinde geçerlidir. Eğer toplamsal bir denklem kastediliyorsa $-a$ anlaşılmalıdır. Yine a^n gibi bir çarpımsal notasyon kullanıldığında toplamsal notasyonu $a \cdot n$ biçiminde anlaşılmalıdır. Bazen de toplamsal notasyon Σ kullanılırsa çarpımsal noktasyon Π olduğu unutulmamalıdır. Bu durumda çarpımsal notayon Benzer şekilde çarpımsal notasyonlar kullanıldığında toplamsal notasyonları tasvir etmesi veya tersini algılamak okuyucuya bırakılmaktadır.

3.1. Teorem: $(G, \star)$ herhangi bir grup olsun.

i) G'nin birim elemanı tekdir.
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 $e \star f = e$ dir. Ayrıca f birim eleman olduğundan $e \star f = f$ olup $e = f$ dir.

ii) $a \in G$ olsun. b ve c de a'nın tersleri olsun. Buna göre

$$a \star b = b \star a = e \text{ ve } a \star c = c \star a = e$$

dir. O zaman

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

olup $b = c$ olduğu görülür.

iii) $x = a^{-1}, y = a$ diyelim. $x \star y = y \star x = e$ olup $x^{-1} = y$ olur. Buna göre $(a^{-1})^{-1} = a$ elde edilir.

iv) $(a \star b) \star (b^{-1} \star a^{-1}) = a \star (b \star b^{-1}) \star a^{-1} = a \star e \star a^{-1} = e$

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

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

Bu teoremde (iii) ve (iv) de ifade edilen özellikler toplamsal notasyonda sırasıyla $-(-a) = a$ ve $-(a + b) = (-b) + (-a)$ şeklini alır.

3.2. Teorem: Bir G grubunda soldan ve sağdan kısaltma kuralları vardır. Ayrıca $a, b \in G$ ise G'de $a \star x = b$ ve $y \star a = b$ denklemini sağlayan sadece bir tane x ve y vardır.

İspat: Her $a, b, c \in G$ için:

$$\begin{aligned} a \star b = a \star c &\Rightarrow a^{-1} \star (a \star b) = a^{-1} \star (a \star c) \\ &\Rightarrow (a^{-1} \star a) \star b = (a^{-1} \star a) \star c \\ &\Rightarrow b = c \end{aligned}$$

$$\begin{aligned} b \star a = c \star a &\Rightarrow (b \star a) \star a^{-1} = (c \star a) \star a^{-1} \\ &\Rightarrow b \star (a \star a^{-1}) = c \star (a \star a^{-1}) \\ &\Rightarrow b = c \end{aligned}$$

olup soldan ve sağdan kısaltma kuralı vardır.

Şimdi, $a\bigstar x = b$ denkleminin bir çözümü $x_1 = a^{-1}\bigstar b$ dir. Çünkü:

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

dir.

Bu denklemin başka bir çözümü x_2 olsun. O halde $a\bigstar x_2 = b$ dir. O zaman $a\bigstar x_1 = b\bigstar x_2$ olup soldan kısaltma kuralı gereğince $x_1 = x_2$ elde edilir. Benzer şekilde $ya = b$ denkleminin çözümü de tektir.

3.3. Not: Bu teoremin bir sonucu olarak, grup tablosunda bir elemanın bir satırda veya bir sütunda sadece bir defa yer alacağını söyleyebiliriz.

YARI GRUP

3.2. Tanım: $A \neq \emptyset$ ve A kümesi üzerinde tanımlı $\bigstar$ işlemi tanımlansın. Eğer $\bigstar$ işleminin kapalılık ve birleşme aksiyomu varsa $(A, \bigstar)$ sistemi yarı gruptur denir.

3.3. Teorem: $(G, \bigstar)$ yarı grubunun grup olması için gerek ve yeter şart

i) Her $a \in G$ için $e\bigstar a = a$ olacak şekilde $e \in G$ olmasıdır.

ii) Her $a \in G$ için $b\bigstar a = e$ olacak şekilde $b \in G$ olmasıdır.

İspat: G bir grup ise i ve ii aksiyomlarını sağlanır. Şimdi tersini gösterelim.

$(G, \bigstar)$ yarı grup olup i ve ii şartlarını sağlasın. $a \in G$ alalım. $b\bigstar a = e$, $b \in G$ var (ii) den $b \in G$ için $c\bigstar b = e$, $c \in G$ vardır.

$$a = e\bigstar a = (c\bigstar b)\bigstar a = c\bigstar(b\bigstar a) = c\bigstar e \text{ ve}$$

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

olduğundan (ii) de $ba = e$ olduğuna göre $ab = ba = e$ dir.

$$a\bigstar e = a\bigstar(b\bigstar a) = (a\bigstar b)\bigstar a = e\bigstar a = a$$

olup $(G, \bigstar)$ bir gruptur.

3.4. Teorem: $(G, \bigstar)$ yarı grubunun grup olması için gerek ve yeter şart $\forall a,b \in G$ için her $a,b \in G$ için $a\bigstar x = b$ ve $y\bigstar a = b$ olacak şekilde $\exists x,y \in G$ bulunmasıdır.

İspat: $(G, \bigstar)$ grup ise $x = a^{-1}\bigstar b$, $y = b\bigstar a^{-1}$ alınabilir. Tersine verilen denklemin G'de çözümü olsun. $a \in G$ için $y\bigstar a = a$ denklemini düşünelim

$y = u \in G$ için $u \bigstar a = a$ dır. $b \in G$ için $a \bigstar x = b$ denkleminin $c \in G$ çözümü olsun.

$$u \bigstar b = u \bigstar (a \bigstar c) = (u \bigstar a) \bigstar c = a \bigstar c = b$$

$\forall\, b \in G$ için $u \bigstar b = b$ olup 3.3. teoremin i şıkkı sağlanır. $y \bigstar a = u$ denkleminin $d \in G$ çözüm olsun $d \bigstar a = u$ olur ki 3.3. teoremin ii sağlanır. Dolayısıyla 3.1.4 gereği $(G, \bigstar)$ ikilisi gruptur.

3.5. Teorem: $(G, \bigstar)$ sonlu yarı grubunun grup olması için gerek ve yeter şart $(G, \bigstar)$ da soldan ve sağdan kısaltma özelliklerinin sağlanamasıdır.

İspat: $(G, \bigstar)$ grup ise istenen sağlandığından açıktır. Tersine $(G, \bigstar)$ da kısaltma özellikleri sağlansın. $a, b \in G$ için $a \bigstar x = b$ denklemini düşüneli. Bu denklemin G'de çözümünün olduğunu göstermeliyiz. $G = \{a_1, a_2, \cdots, a_n\}$ olsun. G yarı grup olduğundan $a \in G$ için $a \bigstar a_i \in G$, $i = 1,2, \cdots, n$ dir. Bu takdirde $\{a \bigstar a_1, a \bigstar a_2, \cdots, a \bigstar a_n\} \subseteq G$, $i \neq j$ için $a \bigstar a_i = a \bigstar a_j$ olsun $a_i = a_j$ elde edilir, bu ise çelişkidir. O halde $G = \{a \bigstar a_1, a \bigstar a_2, \cdots, a \bigstar a_n\}$ olur. $b \in G$ için $b = a \bigstar a_k$ oalcak şekilde $a_k \in G$ vardır. Bu da $a \bigstar x = b$ denkleminin G'de çözümünün olması demektir. Benzer şekilde $y \bigstar a = b$ içinde yapılabilir. 3.4. teorem gereği $(G, \bigstar)$ gruptur.

GRUBUN MERTEBE ve DERECELERİ

3.3. Tanım: Bir G grubunun elemanlarının sayısına (eğer G sonlu ise) G'nin mertebesi denir ve $o(G)$ ile gösterilir. Eğer G sonsuz bir küme ise $o(G) = \infty$ yazılır.

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

$$f_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, f_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, f_3 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$
$$f_4 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, f_2 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, f_3 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

Bu grupta f ile g'nin bileşkesinin 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 $f_5f_3 = f_6$ iken $f_3f_5 = f_2$ dir.

3.4. Tanım: G bir grup ve $a \in G$ olsun. $a^n = e$ olacak şekilde bir en küçük pozitif n doğal sayısı varsa bu sayıya a'nın derecesi denir ve $o(a)$ ile gösterilir. Böyle bir n sayısı yoksa $o(a) = \infty$ yazılır.

Örnek: S_3 permütasyon 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 $o(f_2) = 2$ dir. $o(f_1) = 1$ ve $o(f_4) = 3$ dür.

Örnek: $(\mathbb{Z}, +)$ grubunu ele alalım. 5'in derecesi sonsuzdur, çünkü $n \cdot 5 = 0$ olacak şekilde $m \in \mathbb{N}$ yoktur. Bu grupta $o(0) = 1$ dir ve diğer elemanların derecesi sonsuzdur.

Örnek: Matrislerde çarpma işlemine göre $A = \begin{bmatrix} 1 & 3 \\ 0 & -1 \end{bmatrix}$ matrisinin mertebesini bulunuz.

Çözüm: $A^2 = \begin{bmatrix} 1 & 3 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ olup birim matrisi vermektedir. Şu halde $o(A) = 2$ dir.

3.6. Teorem: $(G, \star)$ bir grup $a \in G$ ve $o(a) = n$ olsun.

i) $m \in \mathbb{Z}^+$ için $a^n = e \Leftrightarrow n \mid m$ dir.

ii) Her $t \in \mathbb{Z}^+$ için $o(a^t) = \dfrac{n}{\text{OBEB}(t,n)}$ dir.

İspat: i) $\Rightarrow$: $m \in \mathbb{Z}^+$ için $a^m = e$ ve $n \nmid m$ olsun. Bu takdirde

$$m = qn + r, \ 0 \le r < n, \ \exists\, q, r \in \mathbb{Z}$$

vardır. $a^n = a^{m-qn} = a^m(a^n)^{-q} = e$ çelişkisi elde edilir. Buna göre $r = 0$ olup $n \mid m$ dir.

$\Leftarrow$: $n \mid m$ ise $a^n = e$ olduğu aşikârdır.

ii) $o(a^t) = k$ olsun $a^{tk} = e$ olup $n \mid tk$ yani $tk = nr, r \in \mathbb{Z}$, $OBEB(t,n) = d$ olsun. $t = du, n = dv$, $OBEB(u,v) = 1, \exists\, u, v \in \mathbb{Z}$ vardır.

$$tk = nr \Leftrightarrow duk = dvr \Leftrightarrow ku = rv \Leftrightarrow v \mid ku \Leftrightarrow v \mid k \Leftrightarrow v = \tfrac{n}{d} \mid k$$

olur.

$(a^t)^{n/d} = a^{tn/d} = a^{ndu/d} = a^{nu} = e^u = e$ ve $o(a^t) = k$ dan $k \mid \frac{n}{d}$ dolayısıyla $k = \frac{n}{d} = \frac{n}{OBEB(t,n)}$ dir.

DEVİRLİ GRUPLAR

3.5. Tanım: G bir grup, $a \in G$ olsun. $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ kümesine a tarafından üretilen (doğurulan) grup denir. 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: $A = \{1, -1, i, -i\}$ grubu verilsin.

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

olup A grubu devirlidir. Çünkü i ve $-i$ nin kuvveti alınarak tarafından üretilmiştir. $A = \langle i \rangle = \langle -i \rangle$ dir.

Örnek: $(\mathbb{Z}, +)$ grubunda

$\langle 5 \rangle = \{5n : n \in \mathbb{Z}\} = \{\cdots, -10, -5, 0, 5, 10, \cdots\} = 5\mathbb{Z}$

dir. $\mathbb{Z}$ devirlidir, çünkü $\langle -1 \rangle = \langle 1 \rangle = \mathbb{Z}$ dir. $(\mathbb{Z}_m, \oplus)$ grupları devirlidir, çünkü her zaman $\bar{1}$ tarafından üretilir. Mesela $\mathbb{Z}_6$ de;

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

dır.

Örnek: $(\mathbb{Q}\backslash\{0\}, +)$ grubunda $\frac{1}{4}$ elemanının ürettiği grubu bulunuz.

Çözüm:

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

Örnek: S_3 permütasyon grubu 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.

3.1. Sonuç: Bir G sonlu grubunun devirli olması için gerek ve yeter şart $o(G) = o(a)$ olacak şekilde en az bir $a \in G$ elemanının olmasıdır.

3.4. Not: Bir grupta $o(a) = \infty$ ise

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

biçiminde yazılır. Fakat eğer $o(a) = n$ sonlu ise a'nın negatif bir kuvveti pozitif bir kuvvetine eşit olacağından

$$\langle a \rangle = \{e, a, a^2, a^3, \cdots\}$$

biçiminde yazılabilir.

3.6. Teorem: G bir grup $a \in G$ ve $o(a) = n$ olsun. $p, q \in \mathbb{Z}$ olsun.

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

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

İspat i) $p - q \in \mathbb{Z}$ olup, "bölme algoritması" gereğince, $p = q$ ve n sayısı için $p - q = nk_1 + k_2, 0 \le k_2 < n$ olacak şekilde $k_1, k_2 \in \mathbb{Z}$ vardır.

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

olup $k_2 < n$ ve $o(a) = n$ olduğundan bu durum sadece $k_2 = 0$ olmasıyla mümkündür. O halde $p - q = nk_1 + k_2 \Leftrightarrow p \equiv q \pmod{n}$ dir.

Tersini göstermek kolaydır.

ii) $p > q$ olsun. $o(a) = \infty$ olduğundan her $1 \leq k \in \mathbb{N}$ için $a^k \neq e$ dir. $a^p = a^q$ ise $a^{p-q} = 0$ dir. $p - q \in \mathbb{N}$ olup $p - q = 0$ olmalıdır. Yani $p = q$ dur.

Tersini göstermek kolaydır.

3.5. Not: $o(a) = n < \infty$ olsun.

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

dir.

3.7. Teorem: $G = \langle a \rangle$ ve $o(a) = \infty$ olsun. G grubu sadece a ve a^{-1} tarafından üretilir.

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

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

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,

$$a^n = a^{mx} \Leftrightarrow n = mx$$

olup $n = mx$ denkleminin her $n \in \mathbb{Z}$ için çözümünün olması $m = \pm 1$ olmasıyla mümkündür. O halde $b = a$veya $b = a^{-1}$ dir.

ÇÖZÜMLÜ ALIŞTIRMALAR

Grup Tanımı

1. $\mathbb{Q}^+$ pozitif rasyonel sayılar kümesi üzerinde $x \ast y = \frac{xy}{2}$ işlemi tanımlanıyor. $(\mathbb{Q}^+, \ast)$ bir grup olduğunu gösteriniz.

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

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

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

olup $\ast$ işlemi birleşme özelliğine sahiptir.

iii) $x \ast e = x$ ve $e \ast x = x$

$$\frac{xe}{2} = x \text{ ve } \frac{ex}{2} = x$$

$$x = 2$$

olup e = 2 birim elemandır.

iv) $x \star x^{-1} = e$ ve $x^{-1} \star x = e$

$$\frac{xx^{-1}}{2} = 2 \text{ ve } \frac{x^{-1}x}{2} = 2$$

$$x^{-1} = \frac{4}{x}$$

dir.

2. $n \in \mathbb{N}$ olmak üzere $G = \{nk : n \in \mathbb{Z}\}$ kümesi toplama işlemine göre Abelyen bir grup olduğunu gösteriniz.

Çözüm:

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

ii)
$$\begin{aligned} nk_1 + (nk_2 + nk_3) &= n(k_1 + (k_2 + k_2)) \\ &= n((k_1 + k_2) + k_2) \\ &= (nk_1 + nk_2) + nk_2 \end{aligned}$$
olup birleşme özelliği vardır.

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

iv) nk sayısının tersi $-(nk) = n(-k) = -nk \in G$ dir. Bu durumda;
$$nk + (-nk) = (-nk) + nk = 0$$
dır.

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

3. $A = \{a, b, c\}, B = \{b, c\}, C = \{b\}$ olsun. $G = \{\emptyset, A, B, C\}$ alalım. $(G, \cap)$ sisteminin grup olup olmadığını inceleyiniz.

Çözüm: Birim eleman $\emptyset$ olduğu rahatlıkla görülür. Ters eleman özelliğine bakmamız gerekir.

$A \cap A^{-1} = \emptyset$ olması ancak $A^{-1} = \emptyset$ olmasıyla mümkündür. Şu halde, ters eleman özelliği yoktur. Buna göre $(G, \cap)$ sisteminin grup değildir.

4. $G=\mathbb{Z}\times\mathbb{Z}$ kümesi üzerinde $(a;\ b)\circ(c;\ d)=(a+c;\ (-1)^c b+\ d)$ işlemi tanımlanıyor. $(G;\circ)$ Abelyen grup olup olmadığını araştırınız.

Çözüm: i) $(a;\ b),(c;\ d)\in G$ 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.

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

olup birleşme özelliğinin olduğu görülür.

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

$(a;\ b)\circ(0;\ 0)=(a+0;\ (-1)^0 b+0)=(a;b)$

$(0;\ 0)\circ(a;\ b)=(0+a;\ (-1)^0 0+b)=(a;b)$

olur.

iv) $(a;\ b),(a^{-1};\ b^{-1})\in G$ olsun.

$(a;\ b)\circ(a^{-1};\ b^{-1})=(0;\ 0)$

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

$a+a^{-1}=0$ ve $(-1)^{a^{-1}} b+b^{-1}=0$

$a^{-1}=-a$ ve $b^{-1}=-\dfrac{b}{(-1)^a}$

$$(a^{-1};\ b^{-1})=\left(-a;-\frac{b}{(-1)^a}\right)$$

olur.

v) Değişme özelliği yoktur, çünkü

$(1;\ 2)\circ(3;\ 4)=(1+3;\ (-1)^3 2+4)=(4;2)$

$(3;\ 4)\circ(1;\ 2)=(3+1;\ (-1)^1 4+\ 2)=(4;\ -2)$

dir. Buna göre $(\mathbb{Z}\times\mathbb{Z},\ \circ)$ sistemi gruptur, ama Abelyen grup değildir.

5.

★	1	2	3	4

1	1	2	x	4
2	2	1	4	y
3	3	z	1	
4	4			1

(G, ★) değişmeli grubunda G = {e, a, b, c} birim eleman e ise verilen tabloda $x + y + z$ sayılarının sonucu ne olur?

Çözüm: (G, o) değişmeli grup olacak şekilde, aynı satır ve sütunda bir elamanın iki kez kullanacağı dikkate alınarak tablo şu şekilde çizilir:

★	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Bu tabloya göre $x + y + z = 3 + 3 + 4 = 10$ olur.

6. (G, ⊙) grubu verilsin. $\forall\, x,y \in G$, için $x \ast y = x \odot a \odot y$ biçiminde ikinci bir $\ast$ işlem tanımlanıyor. (G, $\ast$) işlemine göre birim elemanı aşağıdakilerden hangisidir?

Çözüm: $x \ast e = x$ ve $e \ast x = x$

$x \odot a \odot e = x$ ve $e \odot a \odot x = x$

$x^{-1} \odot x \odot a = x^{-1} \odot x$

$e \odot a = e$

$a = e$

olduğundan (G, $\ast$) işleminin e birim elemandır.

7. (G, ♥) grubunun tablosu aşağıdaki gibidir.

♥	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

$c^2 ♥ e^{-2}$

işleminin sonucu aşağıdakilerden hangisidir?

Çözüm: Her $x \in G$ için

$b ♥ e = e ♥ b = a$ olduğundan $e^{-1} = b$ $e^{-1} = b$ dir.

$$c^2 ♥ e^{-2} = c^2 ♥ b^2 = (c♥c) ♥ (b♥b) = e♥c = b$$

Cevap: B

8. Bir (G, Δ) grubunda her $a, b \in G$ için $(a \,\Delta\, b)^2 = a^2 \,\Delta\, b^2$ eşitliği varsa G, abelyen grup olduğunu gösteriniz.

Çözüm: Her $a, b \in G$ için

$$(a \,\Delta\, b)^2 = a^2 \,\Delta\, b^2 \Leftrightarrow a \,\Delta\, b \,\Delta\, a \,\Delta\, b = a \,\Delta\, a \,\Delta\, b \,\Delta\, b$$
$$\Leftrightarrow a \,\Delta\, b \,\Delta\, a = a \,\Delta\, a \,\Delta\, b \quad \text{(soldan a kısalır)}$$
$$\Leftrightarrow b \,\Delta\, a = a \,\Delta\, b \quad \text{(sağdan a kısalır)}$$

olduğundan G, Abelyen grup olur.

Devirli Grup

9. $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$ grubu devirli midir? Üretici elemanlarını bulunuz.

Çözüm: $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$ = devirlidir, Gerçekten

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

dir.

10. $(\mathbb{Q}, +)$ grubunun devirli grup olmadığını gösteriniz.

Çözüm: Kabul edelim ki $(\mathbb{Q}, +)$ 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 $q = \frac{a}{b}$ biçiminde yazılabilir. Şimdi $t = \frac{1}{2b} \in \mathbb{Q}$ olup $t = nq$ olacak şekilde $n \in \mathbb{Z}$ vardır. O halde

$$\frac{1}{2b} = nq = n\frac{a}{b} \Leftrightarrow \frac{1}{2} = na \in \mathbb{Z}$$

olur ki bu bir çelişkidir. O halde $(\mathbb{Q}, +)$ devirli değildir.

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

Çözüm: $(\mathbb{Z}, +)$ grubunda

$$\langle \bar{6} \rangle = \{6k : k \in \mathbb{Z}\} = \{\cdots, -18, -12, -6, 0, 6, 12, 18, \cdots\} = 6\mathbb{Z}$$

dir.

12. $(\mathbb{Q}\backslash\{0\},+)$ grubunda $\frac{1}{3}$ elemanının ürettiği grubu bulunuz.

Çözüm:
$$\langle\overline{\tfrac{1}{3}}\rangle=\left\{\left(\frac{1}{3}\right)^{n}:n\in\mathbb{Z}\right\}=\left\{\cdots,\frac{1}{27},\frac{1}{9},\frac{1}{3},1,3,9,27,\cdots\right\}$$

Grubun Mertebe ve Dereceleri

13. 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 olduğunu gösteriniz.

Çözüm: $x^{n}=e$ ise $x^{n-1}=x^{-1}$ olup $m=n-1$ dersek $m>1$ olur ve $x^{-1}=x^{m}$ elde edilir.

14. G sonlu bir grup ise her $x\in G$ için $x^{n}=e$ olacak şekilde bir n pozitif sayısı olduğunu gösteriniz.

Çözüm: G sonlu olsun. $x^{n}=e$ olacak şekilde bir n pozitif tamsayısı olmasın. O halde $A=\{x,x^{2},x^{3},\cdots\}$ kümesindeki elemanların hepsi G'nin elemanlarıdır. Ayrıca bu elemanlar birbirinden farklıdır. Gerçekten en az bir $i\neq j, i>j$ için $x^{i}=x^{j}$ olsaydı $x^{i-j}=e$ olurdu. Bu da kabulümüzle çelişirdi. 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.

15. $(G,\star)$ bir grup olsun. G'de a,a^{-1} ve $b\star a\star b^{-1}$ elemanlarının derecelerinin aynı olduğunu gösteriniz.

Çözüm: $o(a)=n$ olsun. $(a^{-1})^{n}=(a^{n})^{-1}=e^{-1}=e$ dir. Fakat bu $o(a^{-1})=n$ anlamına gelmez. $1\leq k<n$ olsun.
$$(a^{-1})^{k}=e\Leftrightarrow(a^{k})^{-1}=e\Leftrightarrow a^{k}=e^{-1}=e$$
olup bu durum $o(a)=n$ olmasıyla çelişir. O halde $o(a^{-1})=n$ dir.
$$\begin{aligned}(b\star a\star b^{-1})^{n}&=\underbrace{(b\star a\star b^{-1})(b\star a\star b^{-1})\cdots(b\star a\star b^{-1})}_{\text{n tane}}\\&=b\star a^{n}\star b^{-1}\\&=b\star e\star b^{-1}\\&=e\end{aligned}$$
olur. Burada $1\leq k<n$ olsun.

$$(b\star a\star b^{-1})^n = e \Leftrightarrow b\star a^k\star b^{-1} = e \Leftrightarrow b\star a^k = b \Leftrightarrow a^k = e$$

olup bu durum $o(a) = n$ olmasıyla çelişir. O halde $o(b\star a\star b^{-1}) = n$ dir.

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

Çözüm: $G = \{e, a_1, a_2, \cdots, a_n\}$ olsun. $o(G) = n + 1$ çift olsun. $f: G \to G$, $f(x) = x^{-1}$ için

$$f(x) = f(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow x = y$$
$$y \in G \Rightarrow x = y^{-1} \text{ alınırsa } f(x) = f(y^{-1}) = y$$

dönüşümü 1–1 ve örtendir.

Buna göre $f(e) = e$ olduğu aşikârdır. Biz $f(a_i) = a_i$ olacak şekilde $a_i \in G$ olacağını göstereceğiz. $G\backslash\{e\}$ kümesinde $f(x) = y \Leftrightarrow f(y) = x$ olduğundan tersi kendine eşit olmayan elemanlar f altında eşlendiğinde geriye tek tane eleman kalacağı aşikardır, çünkü $G\backslash\{e\}$ kümesi tek elemanlıdır. Bu da tersi kendine eşlenecek en az bir tane eleman olduğu anlamına gelir. O halde en az bir i için $f(a_i) = a_i$ olup $(a_i)^{-1} = a_i$ bu da $(a_i)^2 = e$ dir.

17. Bir $(G, \star)$ grubunda her $x \in G$ için $x^2 = e$ ise bu grubun Abelyen olduğunu gösteriniz.

Çözüm: Bir G grubunda her $x \in G$ için $x^2 = e$ ise $x = x^{-1}$ dir. O halde her elemanın tersi kendisidir. Buna göre her $a, b \in G$ için $(a\star b)^2 = e$ olmalıdır. Burada $a = a^{-1}$, $b = b^{-1}$ olacağından

$$\begin{aligned}(a\star b)^2 = e &\Rightarrow a\star b\star a\star b = e\\ &\Rightarrow a\star b\star a = b^{-1}\\ &\Rightarrow a\star b = b^{-1}\star a^{-1} = b\star a\end{aligned}$$

olup G'nin Abelyen olduğu görülür.

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

Çözüm: Bağıntının yansıyan, simetrik ve geçişken olduğunu göstereceğiz.

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

ii) a ile b eşlenik ise $\exists\, x \in G$,

$$x^{-1} \star a \star x = b \Rightarrow a \star x = x \star b$$
$$\Rightarrow a \star x \star x^{-1} = x \star b \star x^{-1}$$
$$\Rightarrow a = x \star b \star x^{-1}$$

Burada $y = x^{-1}$ dersek $a = y \star b \star y^{-1}$ olur. Yani, b ile a eşleniktir. $y = x^{-1} \in G$ olup bağıntımız simetriktir.

iii) a ile b eşlenik ise $\exists\, x \in G, x^{-1} \star a \star x = b$

b ile c eşlenik ise $\exists\, y \in G, y^{-1} \star b \star y = c$

$$y^{-1} \star (x^{-1} \star a \star x) \star y = c$$
$$(x \star y)^{-1} \star a \star (x \star y) = c$$
$$z^{-1} \star a \star z = c, \ (z = x \star y)$$

Buna göre a ile c bağıntımız geçişkendir.

19. $a, b \in G$ ve $o(a) = 5$ olsun. $a^3 \star b = b \star a^3$ ise $a \star b = b \star a$ olduğunu gösterin.

Çözüm: $c = b \star a^3$

$$a^3 \star (a^3 \star b) = a^3 \star (b \star a^3)$$
$$(a^3 \star a^3) \star b = (a^3 \star b) \star a^3$$
$$a \star b = b \star a^3 \star a^3$$
$$a \star b = b \star a$$

20. $(G, \star)$ bir grup $a, b \in G$ olsun. $a \star b = b \star a^{-1}$ ve $b \star a = a \star b^{-1}$ ise $a^4 = b^4 = e$ olduğunu gösteriniz.

Çözüm:

$a \star b = b \star a^{-1}$ ise $a = b \star a^{-1} \star b^{-1}$

$b \star a = a \star b^{-1}$ ise $b = a \star b^{-1} \star a^{-1}$

olduğundan

$$b \star a = a \star b^{-1} = (b \star a^{-1} \star b^{-1}) \star b^{-1} = b \star a^{-1} \star b^{-2}$$

$b \star a = b \star a^{-1} \star b^{-2}$ ise $a^2 = b^{-2}$

$$a^4 = a^2 \star a^2 = a^2 \star b^{-2} = a \star a \star b^{-1} \star b^{-1} = a \star b^{-1} \star a \star b^{-1}$$
$$= b \star a^{-1} \star a \star b^{-1} = b \star e \star b^{-1} = e$$

ve

$$a^2 = b^{-2} \Rightarrow a^4 = b^{-4}$$

$$\Rightarrow b^4 \star a^4 = b^4 \star b^{-4}$$
$$\Rightarrow b^4 \star e = e$$
$$\Rightarrow b^4 = e$$

elde edilir.

21. (G,·) bir grup ve $a,b \in G$ olsun. $a \cdot b$ nin mertebesinin $b \cdot a$ nin mertebesine eşit olduğunu gösteriniz.

Çözüm: Mertebe tanımına göre a'nın mertebesi $o(a)$ ile gösterilir ve pozitif tamsayıdır.

$o(a \cdot b) = m$ ve $o(b \cdot a) = n$ olsun. $m \mid n$ ve $n \mid m$ olduğunu göstermeliyiz.

$$\begin{aligned} o(a \cdot b) = m &\Leftrightarrow (a \cdot b)^m = e \\ &\Leftrightarrow \underbrace{(a \cdot b) \cdot (a \cdot b) \ldots (a \cdot b)}_{m \text{ tane}} = e \\ &\Leftrightarrow a^{-1} \cdot (a \cdot b)(a \cdot b) \ldots (a \cdot b) = a^{-1} \cdot e \\ &\Leftrightarrow (a^{-1} \cdot a) \cdot (b \cdot a) \ldots (b \cdot a) \cdot b = a^{-1} \cdot e \\ &\Leftrightarrow (b \cdot a)^{m-1} \cdot b = a^{-1} \\ &\Leftrightarrow (b \cdot a)^{m-1} \cdot b \cdot a = a^{-1} \cdot a \\ &\Leftrightarrow (b \cdot a)^m = e \end{aligned}$$

olup $n \mid m$ dir. Benzer şekilde $m \mid n$ de gösterilir.

KAYNAKÇA

1. Prof. Dr. Fethi ÇALLIALP, Soyut Cebir, 2011, İstanbul.
2. Yrd. Doç. Dr. Hüseyin BİLGİÇ, Soyut Cebir Ders Notları, Kahramanmaraş Sütçü İmam Üniversitesi, 2012, Kahramanmaraş.
3. Prof. Dr. Şenol Eren, Soyut Cebir, Ondokuz Mayıs Üniversitesi Dijital Ders Platformu, 2021, Samsun.
4. Prof. Dr. Sait Halıcıoğlu, Doç. Dr. Burcu Üngör, Cebir, Açık ders, Ankara Üniversitesi, 2021, Ankara.
5. Doç. Dr. Sebahattin BALCI, Modern Cebire Giriş, Ankara Üniversitesi, Fen Fakültesi Döner Sermaye İşletmeleri Yayınları: 15, 1993, ANKARA.
6. Doç. Dr. Mustafa Bayraktar, Soyut Cebir ve Sayılar Teorisi, Atatürk Üniversitesi Basımevi, 1988, Erzurum.
7. Prof. Dr. H.İbrahim Karataş, Soyut Cebir, TÜBA, 2010, Ankara.