BÖLÜM 3

GRUPLAR

Bu bölümü bitirdiğinizde,

- grup kavramı
- değişmeli grup(Abel grubu) kavramı
- gruplarla ilgili gösterimler
- bazı grup örnekleri
- gruplarda işlem tablosu ve özellikleri
- grup elemanlarının tamsayı kuvvetleri
- grupların bazı temel özellikleri

konularında bilgi sahibi olabileceksiniz.

BÖLÜM **3**

GRUPLAR

Bir küme üzerinde bir veya daha fazla ikili işlem tanımlanmış ise, bu ikili işlem(ler)le birlikte o kümeye bir *cebirsel yapı* denir.

Soyut cebirin amacı, cebirsel yapıları sınıflandırarak aynı sınıf içindeki cebirsel yapıların, onları oluşturan küme veya ikili işlemlerden bağımsız olarak, ortak özelliklerini bulmak, sergilemek ve bu özelliklerden bazı sonuçlar çıkarmaktır. Matematiğin bu dalının *soyut cebir* olarak adlandırılmasının nedeni budur. Şunu da belirtmek gerekir ki özel bir cebirsel yapıdan söz edilirken o cebirsel yapıyı oluşturan küme ile birlikte o küme üzerindeki ikili işlem(ler)in ne olduğu, kuşkuya yer bırakmayacak biçimde, bilinmelidir.

Bir K kümesi ve onun üzerinde bir $*$ ikili işleminden oluşan cebirsel yapıyı, $< K, * >$ ile göstereceğiz. Eğer K üzerinde ikinci bir ikili işlem, $\circ$, varsa, K ve bu iki ikili işlemden oluşan yapıyı, $< K, *, \circ >$ ile göstereceğiz.

$< K, * >$ cebirsel yapısı ele alındığında, "K üzerinde $*$ ikili işleminin **Ö** özelliği vardır" demek yerine, çoğu zaman, "$< K, * >$ ın **Ö** özelliği vardır" deyimini kullanacağız. Örneğin, "$< K, * >$ ın **birleşme** özelliği var" deyimi, "K üzerinde $*$ işleminin **birleşme** özelliği var" deyimine denktir.

Herhangi bir cebirsel yapıdan söz edilirken o cebirsel yapıyı oluşturan ikili işlemlerin ne olduğu, ayrıca belirtmeye gerek olmayacak biçimde açık ise, gösterim ve yazım kolaylığı sağlamak için, sadece bu cebirsel yapıyı oluşturan kümenin zikredilmesiyle yetinilebilir. Örneğin, ileride görüleceği gibi, " $\mathbb{Z}$ halkası " denince $< \mathbb{Z}, +, . >$ anlaşılır (Burada $+$ ve . , bilinen toplama ve çarpma işlemleridir).

Bu bölümde ele alacağımız grup kavramı, matematiğin değişik alanlarında ortaya çıkan ve uygulanan bir kavramdır. On dokuzuncu yüzyılın ilk yıllarında, E. Galois (1811-1832) ve N. Abel (1802-1829)' in çalışmaları, bir polinom denkleminin çözülebilirliğinin ve köklerinin konumunun anlaşılmasında grup kavramının esas olduğunu göstermiştir. F. Klein (1849-1925)' in geometri konusundaki çalışmalarında da temel kavram grup kavramıdır. Bu örnekler çoğaltılabilir. Günümüzde, grup kavramının uygulama alanı gittikçe genişlemektedir. Teorik fizik ve teorik kimyanın temel problemlerinin çözümünde grup kavramı kullanılmaktadır.

Tanım 1. G bir küme; $*$, G üzerinde bir ikili işlem olsun. Eğer aşağıdaki üç koşul sağlanıyorsa, $< G, * >$ bir *grup*tur denir:

(g.1) $< G, * >$ ın birleşme özelliği vardır.

(g.2) $< G, * >$ ın birim elemanı vardır.

(g.3) G nin her elemanı, $*$ a göre tersinir.

Eğer ek olarak

(g.4) $< G, * >$ ın değişme özelliği vardır.

koşulu sağlanıyorsa, $< G, * >$, *değişmeli grup* (ya da *N. Abel*'e atfen *Abel grubu*) adını alır. $\square$

$< G, * >$ bir grup ise, bu durumu bazen, "G kümesi, $*$ işlemine göre bir gruptur " deyimi ile ifade edeceğiz; eğer, bu bölümün başında da belirtildiği gibi, $*$ işleminin ne olduğu açıksa, "$< G, * >$, bir gruptur" deyimi yerine "G, bir gruptur " deyimi kullanılacaktır. Bir grubun elemanları denince, o grubu oluşturan kümenin elemanları anlaşılır.

(g.2) koşulu, bir grubun birim elemanının varlığını ifade eder. Böyle bir elemanın, tek türlü belirli olduğunu hatırlayınız(Bak. Teorem 2.2). (g.3) koşulu ise bir grubun her bir elemanının tersinir olduğunu ifade eder; tersinir bir elemanın tersinin, tek türlü belirli olduğunu hatırlayınız(Bak. Teorem 2.3).

Örnek 1. $G = \{e, a\}$ kümesi üzerinde yandaki tablo ile tanımlanan ikili işlemi düşünelim. Tanım 1 deki (g.1), (g.2), (g.3) ve (g.4) koşullarının $< G, * >$ için tümüyle sağlandığı kolayca görülebilir.

$*$	e	a
e	e	a
a	a	e

Örneğin, $< G, * >$ ın birim elemanı e dir; a nın tersi, yine a dır. Böylece, $< G, * >$, bir değişmeli gruptur. □

Örnek 2. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ kümelerinin her biri, bilinen toplama işlemine göre; $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ ve $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ kümelerinden her biri, bilinen çarpma işlemine göre, bir değişmeli gruptur. $< \mathbb{N}, + >$, $< \mathbb{Z}, . >$ veya $< \mathbb{Z}\backslash\{0\}, . >$ dan hiçbiri grup değildir (Neden ?). □

Örnek 3. m ve n pozitif tamsayılar olmak üzere, girdileri $\mathbb{R}$ içinde olan $m \times n$ matrislerden oluşan $\mathbb{R}^{m\times n}$ kümesi, matris toplama işlemine göre bir değişmeli gruptur. Benzer biçimde, $\mathbb{Z}^{m\times n}$, $\mathbb{Q}^{m\times n}$, $\mathbb{C}^{m\times n}$ de matris toplama işlemine göre Abel gruplarıdır. Matrisler üzerinde çarpma işlemi de tanımlı olduğu için, çarpımsal matris grupları bulunabileceğini düşünmek doğaldır. Matris çarpımının, en azından girdileri reel veya karmaşık sayılar olan matrisler için, birleşme özelliğine ve birim elemanına sahip olduğu bilinmektedir. Ancak, tersinir olmayan matrisler vardır. $\mathbb{R}^{n\times n}$ içinde bir matrisin tersinir olması için gerek ve yeter koşul, o matrisin determinantının sıfırdan farklı olmasıdır. Her $n \geq 1$ için

$$GL(n, \mathbb{R}) = \{A \in \mathbb{R}^{n\times n} : \; det\ A \neq 0\},$$

$$SL(n, \mathbb{R}) = \{A \in \mathbb{R}^{n\times n} : \; det\ A = 1\}$$

olarak tanımlanır. $GL(n, \mathbb{R})$ ve $SL(n, \mathbb{R})$ den her biri, matris çarpma işlemine göre bir gruptur. Matris çarpımı değişme özelliğine sahip olmadığından, $GL(n, \mathbb{R})$ ve $SL(n, \mathbb{R})$ *değişmeli olmayan* gruplardır. $GL(n, \mathbb{Q})$, $GL(n, \mathbb{C})$, $SL(n, \mathbb{Q})$ ve $SL(n, \mathbb{C})$, için de benzer tanımlar verilir. □

Şimdi de analizden bir örnek sunuyoruz:

Örnek 4. Bir $[a, b]$ aralığı üzerinde sürekli olan tüm (reel değerli) fonksiyonların kümesi, $\mathcal{S}[a,b]$ ile gösterilsin. $f,g \in \mathcal{S}[a,b]$ için $f+g$,

$$(f+g)(x) = f(x) + g(x)\ ,\ x \in [a,b]$$

ile tanımlanırsa, $\mathcal{S}[a,b]$ üzerinde bir ikili işlem elde edilir. Bu ikili işlemle birlikte, $\mathcal{S}[a,b]$, bir değişmeli gruptur. Bu grupta birim eleman,

$$0(x) = 0\ ,\ x \in [a,b]$$

ile tanımlanan sıfır fonksiyonu; $f \in \mathcal{S}[a,b]$ nin tersi,

$$(-f)(x) = -(f(x))\ ,\ x \in [a,b]$$

olarak tanımlanan $-f$ fonksiyonudur. □

Bir grubun ikili işlemi için $*$ gösterimini kullanmak çoğu durumlarda elverişli olmamaktadır. Bu nedenle, gruplar hakkındaki genel tartışmalarda, ikili işlem için çarpımsal gösterim kullanmak adettendir. Böylece, G üzerinde ikili işlem olarak çarpma işlemi düşünülür; $a,b \in G$ için (a,b) sıralı ikilisine karşılık gelen eleman, $a \cdot b$ veya ab ile gösterilir ve a ile b nin *çarpımı* olarak adlandırılır. İkili işlemi çarpma işlemi olan bir gruba *çarpımsal grup* denir; bir çarpımsal grubun birim elemanı, 1 veya e ile, bir x elemanının tersi, x^{-1} ile gösterilir.

Her ne kadar genel tartışmalarımızda çarpımsal gösterim kullanılacaksa da okuyucunun çarpımsal gösterimde ifade edilmiş sonuçları kolaylıkla top- lamsal gösterime veya $*$ gösterimine çevirebileceğini varsayıyoruz. Aslında, okuyucunun gruplar üzerindeki çalışmalarının başlarında bu doğrultudaki becerisini geliştirmek için çaba göstermesi çok yerinde olur. Örneğin, okuyucu; $x,y \in G$ için x in tersi, çarpımsal gösterimde x^{-1}, toplamsal gösterimde $(-x)$ ve $*$ gösteriminde x' ile gösterildiğine göre; çarpımsal gösterimde

$$(xy)^{-1} = y^{-1}x^{-1}$$

ifadesinin, toplamsal gösterimde

$$-(x+y) = (-y) + (-x),$$

ve $*$ gösteriminde ise

$$(x * y)' = y' * x'$$

biçimini alacağını görebilmelidir.

Bu bölümün geri kalan kısmında, grupların bazı temel özelliklerini vereceğiz.

Önerme 1. *G bir grup; $x, y, a, b \in G$ olsun. Bu takdirde,*

(i) $ax = b \Longleftrightarrow x = a^{-1}b$ $\qquad$ (ii) $ya = b \Longleftrightarrow y = ba^{-1}$

(iii) $ax = ay \Longrightarrow x = y$ $\qquad$ (iv) $xb = yb \Longrightarrow x = y$

dir.

Kanıt. (i) Grup tanımındaki (g.1), (g.2) ve (g.3) kullanılarak,

$$ax = b \Longrightarrow a^{-1}ax = a^{-1}b \Longrightarrow ex = a^{-1}b \Longrightarrow x = a^{-1}b.$$

Benzer biçimde,

$$x = a^{-1}b \Longrightarrow ax = aa^{-1}b \Longrightarrow ax = eb \Longrightarrow ax = b.$$

(iii) Burada da (i), (g.1), (g.2) ve (g.3) kullanılarak,

$$ax = ay \Longleftrightarrow x = a^{-1}ay \Longleftrightarrow x = ey \Longleftrightarrow x = y.$$

(ii) ve (iv) ün kanıtını, okuyucuya alıştırma olarak bırakıyoruz. ■

G bir grup; $x, y \in G$ olsun. $x^{-1} = y$ olduğunu söyleyebilmek için, tanıma göre, hem $xy = e$ hem de $yx = e$ olduğunu bilmek gerekir. Ancak, yukarıda kanıtladığımız önerme, bu eşitliklerden birinin yeterli olduğu sonucunu verir.

Sonuç 1. *G bir grup; $x, y \in G$ olsun. Eğer $xy = e$ veya $yx = e$ ise, $x^{-1} = y$ dir.*

Kanıt. $xy = e$ ise, Önerme 1(i) den $y = x^{-1}e = x^{-1}$; $yx = e$ ise, Önerme 1(ii) den $y = ex^{-1} = x^{-1}$ dir. ■

Sonuç 2. *Bir G grubunda birim elemanın tersi kendisidir, yani*

$e^{-1} = e$ *dir.*

Kanıt. $ee = e$ ye Sonuç 1 uygulanırsa, $e = e^{-1}$ elde edilir. ∎

Sonuç 3. *G bir grup; $x \in G$ ise, $(x^{-1})^{-1} = x$ tir.*

Kanıt. $xx^{-1} = e$ ye Sonuç 1 uygulanırsa, $(x^{-1})^{-1} = x$ elde edilir. ∎

Sonuç 4. *G bir grup; $x, y \in G$ ise, $(xy)^{-1} = y^{-1}x^{-1}$ dir.*

Kanıt. $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$, yani $(xy)(y^{-1}x^{-1}) = e$ dir. Sonuç 1 e göre $(xy)^{-1} = (y^{-1}x^{-1})$ dir. ∎

Sonuç 5. *G bir grup; $x_1, x_2, \ldots, x_n \in G$, $n \geq 2$ olsun. Bu takdirde*

$$(x_1 x_2 \cdots x_n)^{-1} = x_n^{-1} \cdots x_2^{-1} x_1^{-1}$$

dir.

Kanıt. Sonuç 4 ve tümevarım. ∎

Sonuç 6. *G bir grup ise, her $x \in G$ ve $n \in \mathbb{N}$ için $(x^n)^{-1} = (x^{-1})^n$ dir.*

Kanıt. Sonuç 5'te $x = x_1 = x_2 = \cdots = x_n$ alınırsa, iddia edilen eşitlik elde edilir. ∎

Sonuç 7. *G bir sonlu grup (yani sonlu sayıda elemanı olan bir grup) ise, G nin her bir elemanı, G nin işlem tablosunun her bir satırında ve her bir sütununda tam bir kez bulunur.*

Kanıt. $G = \{a_1, a_2, \ldots, a_n\}$ olsun. G nin işlem tablosunun bir satırı, $a \in G$ olmak üzere

$$aa_1 \ , \ aa_2 \ , \ \ldots \ , \ aa_n$$

elemanlarından oluşur. Şimdi, Önerme 1(iii) ye göre

$$aa_i = aa_j \Longrightarrow a_i = a_j$$

olduğundan, G nin her bir elemanı bu satırda en çok bir kez bulunur. Diğer yandan, her $a_i \in G$ için $a^{-1}a_i \in G$ ve

$$a_i = a(a^{-1}a_i)$$

olduğundan, G nin her bir elemanı her bir satırda en az bir kez bulunur. Böylece, her bir eleman her bir satırda tam bir kez bulunur. Sütunlarla ilgili iddia da benzer biçimde kanıtlanır. ■

Bu bölümü, bir çarpımsal grubun elemanlarının tamsayı kuvvetlerini tanımlayarak kapatacağız. İkili işlemi çarpma işlemi olan ve birleşme özelliğine sahip olan herhangi bir cebirsel yapı içinde bir elemanın pozitif kuvvetlerini Gözlem 1.1'de tanımlamıştık. Dolayısıyla, G bir (çarpımsal) grup; $x \in G$ ve $n \in \mathbb{N}$ ise,

$$x^n = \prod_{j=1}^{n} x = \overbrace{x \cdots x}^{n\ tane}$$

tir. n tane elemanın çarpımının tanımına dönülürse, kuvvetlerin de tümevarımsal olarak $x^1 = x$ ve $x^n = (x^{n-1})x$ olarak tanımlandığı görülür. Pozitif tamsayılar için verilmiş olan bu tanım tüm tamsayılara şöyle genişletilebilir: $x^0 = e$ tanımlanır ve eğer $m \in \mathbb{Z}$, $m < 0$ ise,

$$x^m = (x^{-1})^{-m}$$

olarak tanımlanır.

Önerme 2. *G bir çarpımsal grup ise, her $x \in G$ ve $m, n \in \mathbb{Z}$ için*

(i) $(x^{-1})^m = (x^m)^{-1} = x^{-m}$,

(ii) $x^m x^n = x^{m+n}$,

(iii) $(x^m)^n = x^{mn}$ *dir.*

Kanıt. *(i)* $m = 0$ için iddianın doğru olduğu aşikârdır. $m > 0$ ise, önce yukarıdaki tanım ve sonra Önerme 1 in altıncı sonucu kullanılarak, her $x \in G$ için $x^{-m} = (x^{-1})^m = (x^m)^{-1}$ olduğu görülür. $m < 0$ ise, $-m > 0$ olup tanımdan ve kanıtın ilk kısmından, $x^m = (x^{-1})^{-m} = (x^{-m})^{-1}$, dolayısıyla, $(x^m)^{-1} = x^{-m}$ ve benzer şekilde, $(x^{-1})^m = (x^{-1})^{-1})^{-m} = x^{-m}$ dir. Böylece, $(x^m)^{-1} = ((x^{-1})^m = x^{-m}$ olduğu görülür.

(ii) $m > 0$ ve $n > 0$ için iddianın doğruluğu, Gözlem 2.1 den hemen görülür. $m = 0$ veya $n = 0$ ise, iddianın doğru olduğu aşikârdır. Eğer $m > 0$, $n < 0$ ve $m + n > 0$ ise, $-n > 0$ olup (i) kullanılarak

$$x^m x^n = (x^{m+n} x^{-n}) x^n = x^{m+n}(x^{-n} x^n) = x^{m+n}.$$

Eğer $m > 0$, $n < 0$ ve $m+n < 0$ ise, $-(m+n) > 0$ olup (i) kullanılarak

$$x^{-(m+n)}(x^m x^n) = (x^{-(m+n)} x^m) x^n = x^{-n} x^n = 1 \Longrightarrow x^m x^n = x^{m+n}.$$

$m < 0$, $n > 0$ olması durumunda, iddia, $m > 0, n < 0$ durumuna benzer biçimde kanıtlanır. Eğer $m < 0$, $n < 0$ ise,

$$x^m x^n = (x^{-1})^{-m} (x^{-1})^{-n} = (x^{-1})^{-(m+n)} = x^{m+n}.$$

(iii) nin kanıtını okuyucuya alıştırma olarak bırakıyoruz. ■

G bir toplamsal grup ise, G nin birim elemanı genellikle 0 ile gösterilir. Bu durumda, $x \in G$ için x in tamsayı katları

$$0x = 0 \quad , \quad 1x = x;$$

her $n \geq 2$ için

$$nx = (n-1)x + x$$

ve her $m < 0$ için

$$mx = -m(-x)$$

olarak tanımlanır.