0.1 GRUPLAR

Tanım 1 *A kümesi boştan farklı olmak üzere $\circ$ işlemine göre aşağıdaki koşulları gerçekliyorsa $(A, \circ)$ ikilisine bir Grup denir.*

1. $\circ$ kapalılık özelliğine sahiptir, yani her $x,\ y \in A$ için $x \circ y \in A$ olur.
2. $\circ$ birleşme özelliğine sahiptir, yani her $x,\ y,\ z \in A$ için $(x \circ y) \circ z = x \circ (y \circ z)$ olur.
3. $\circ$ işleminin birim elemanı vardır, yani her $x \in A$ için $x \circ e = e \circ x = x$ olacak şekilde $e \in A$ vardır.
4. $\circ$ işlemine göre her elemanın tersi vardır, yani her $x \in A$ için $x \circ x^{-1} = x^{-1} \circ x = e$ olacak şekilde $x^{-1} \in A$ vardır.

Örnek 2 *$\mathbb{Z}$ tamsayılar kümesi çarpma işlemine göre her elemanın tersi olmadığından, çarpma işlemi altında bir grup değildir. Fakat $\mathbb{Z}$ tamsayılar kümesi toplama işlemine göre bir gruptur.*

Tanım 3 *$(A, \circ)$ grubu değişme özelliğine sahip ise yani her $x,\ y \in A$ için*

$$x \circ y = y \circ x$$

özelliği sağlanıyorsa bu gruba değişmeli grup veya Abelyen grup adı verilir.

Örnek 4 *$A = \{x, y, z, w\}$ olmak üzere aşağıdaki işlem tablasunu göz önüne alalım.*

$\circ$	x	y	z	w
x	x	y	z	w
y	y	w	w	x
z	z	y	x	y
w	w	x	y	z

Bu tablo dikkate alınırsa A kümesinin $\circ$ işlemi altında bir grup olduğu görülür. Bu grubun birim elemanı x dir. Hatta bu grup değişmelidir.

Örnek 5 *$(\mathbb{Z}, +)$ değişmeli bir gruptur.*

Teorem 6 *(Kısaltma Kuralı) Bir $(A, \circ)$ grubunda her $x,\ y,\ z \in A$ için*

$$x \circ y = x \circ z \Longrightarrow y = z$$

ve

$$y \circ x = z \circ x \Longrightarrow y = z$$

özellikleri sağlanır.

İspat: Her $x,\ y,\ z \in A$ için $x \circ y = x \circ z$ olsun. Ters elemanın varlığı birleşme özeeliği nedeniyle

$$\begin{aligned} x^{-1} \circ (x \circ y) &= x^{-1} \circ (x \circ z) \\ \left(x^{-1} \circ x\right) \circ y &= \left(x^{-1} \circ x\right) \circ z \\ e \circ y &= e \circ z \\ y &= z \end{aligned}$$

elde edilir. İspatın ikinci kısmıda benzer düşünce ile yapılır.

Teorem 7 $(A, \circ)$ *bir grup olsun. Bu durumda*
1) Grubun birim elemanı tekdir.
2) Her $x \in A$ *için* $x^{-1} \circ x = x \circ x^{-1} = e$ *eşitliğini sağlayan bir tek* $x^{-1} \in A$ *vardır.*
3) Her $x \in A$ *için* $\left(x^{-1}\right)^{-1} = x$ *dir.*
4) Her $x,\ y \in A$ *için* $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$ *olur.*

İspat: 1) Kabul edelimki $(A, \circ)$ grupunun e den farklı f birim elemanı olsun. Her $x \in A$ için

$$x \circ e = x$$

olduğundan özel olarak $x = f$ alınırsa

$$f \circ e = f \tag{1}$$

bulunur. f bir birim eleman olduğundan her $x \in A$ için

$$f \circ x = x$$

olup $x = e$ alınırsa

$$f \circ e = e \tag{2}$$

bulunur. (1) ve (2) eşitliklerinden

$$f \circ e = f = e$$

elde edilir. Dolayısıyla $e = f$ bulunur.
2) Her $x \in A$ için

$$x^{-1} \circ x = x \circ x^{-1} = e$$

ve

$$x_1^{-1} \circ x = x \circ x_1^{-1} = e$$

olsun. O halde

$$x \circ x_1^{-1} = x \circ x^{-1} = e$$

olup kısaltma kuralından $x_1^{-1} = x^{-1}$ elde edilir.
3) Her $x \in A$ için

$$x^{-1} \circ \left(x^{-1}\right)^{-1} = e = x^{-1} \circ x$$

yazaılabileceğinden ve kısaltma kuralından

$$\left(x^{-1}\right)^{-1} = x$$

elde edillir.
4) Her $x,\ y \in A$ için birleşme özelliğinden

$$\begin{aligned}
(x \circ y) \circ \left(y^{-1} \circ x^{-1}\right) &= x \circ \left(y \circ y^{-1}\right) \circ x^{-1} \\
&= x \circ \left(e \circ x^{-1}\right) \\
&= x \circ x^{-1} \\
&= e
\end{aligned}$$

olduğundan

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1}$$

elde edilir.

Teorem 8 $(A, \circ)$ *bir grup olsun. Bu durumda her* $x,\ y \in A$ *için*

$$x \circ y = a$$

denkleminin bir tek çözümü vardır.

İspat: $x \circ y = a$ denklemini ele alalım. Eşitliğin her iki yanı $x^{-1} \in A$ ile çarpılırsa

$$\begin{aligned}
x^{-1} \circ (x \circ y) &= x^{-1} \circ a \\
\left(x^{-1} \circ x\right) \circ y &= x^{-1} \circ a \\
e \circ y &= x^{-1} \circ a \\
y &= x^{-1} \circ a
\end{aligned}$$

elde edilir. O halde yukarıda verilen denklemin bir çözümü varsa $x^{-1} \circ a$ olmalıdır. Çözümün tekliğini göstermek için

$$x \circ y = a$$

ve

$$x \circ y_1 = a$$

olsun. Bu durumda

$$x \circ y = x \circ y_1$$

olup kısaltma kuralından $y = y_1$ elde edilir.

0.2 n MODÜLÜNE GÖRE TAMSAYILARIN GRUBU

Tanım 9 *a tamsayısı b tamsayısını kalansız bölüyorsa (tam bölüyorsa) bu durumu göstermek için* $a \mid b$ *sembolü kullanılır. Aksine a tamsayısı b tamsayısını kalansız bölmüyorsada bunun için* $a \nmid b$ *sembolü kullanılır.*

Tanım 10 *a ve b iki tamsayı olmak üzere* $a - b$ *farkı sabit bir n pozitif tamsayısına tam bölünüyorsa a ve b tamsayılarına n Modülüne Göre Eşdeğerdir (Denktir) denir. Bu durum*

$$a \equiv b \pmod{n}$$

ile gösterilir.
O halde $a \equiv b \pmod{n}$ *olması için gerek ve yeter şart en az bir* $k \in \mathbb{Z}$ *için* $a - b = kn$ *olmasıdır.*

Örnek 11 $4 \equiv 19$ *(Mod 5);* $-7 \equiv 44 \pmod{3}$

Teorem 12 *n pozitif bir sabit ve a, b, c keyfi sabitler olmak üzere aşağıdaki özellikler sağlanır.*
1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ *ve* $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$
4. $a \equiv b \pmod{n}$ *ve* $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$ *ve* $ac \equiv bd \pmod{n}$
5. $a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n}$

İspat: 1. $a \in \mathbb{Z}$ olmak üzere $a - a = 0n$ olup özellik ağlanır.
2. $a \equiv b \pmod{n}$ ise $a - b = mn$ olacak şekilde bir $m \in \mathbb{Z}$ vardır. O halde

$$b - a = (-m)\,n, \; (-m) \in \mathbb{Z}$$

olduğundan $b \equiv a \pmod{n}$ sağlanır.
3.$a \equiv b \pmod{n}$ ve $b \equiv c \pmod{n}$ olsun. Bu durumda $m, \; p \in \mathbb{Z}$ olmak üzere

$$a - b = mn \text{ ve } b - c = pn$$

olur. Buradan

$$\begin{aligned} a - c &= a - b + b - c \\ &= mn + pn \\ &= (m + p)\,n \end{aligned}$$

yazılır. $(m + p) \in \mathbb{Z}$ olduğundan $a \equiv c \pmod{n}$ bulunur.
4. $a \equiv b \pmod{n}$ ve $c \equiv d \pmod{n}$ olsun. Bu durumda $m, \; p \in \mathbb{Z}$ olmak üzere

$$a - b = mn \text{ ve } c - d = pn$$

olup,

$$\begin{aligned} (a + c) - (b + d) &= (a - b) + (c - d) \\ &= mn + pn \\ &= (m + p)\,n \end{aligned}$$

bulunur. Yani

$$a + c \equiv b + d \pmod{n}$$

elde edilir.

$$\begin{aligned} ac &= (b + mn)(d + pn) \\ &= bd + (bp + md + mpn)\, n \end{aligned}$$

ve $(bp + md + mpn)$ $\in$olduğundan $ac \equiv bd \pmod{n}$ elde edilir.
5. 4. özellikte $c \equiv c \pmod{n}$ olduğu dikkate alınırsa $ac \equiv bc \pmod{n}$ bulunur.
Ayrıca bu özellikler dikkate alınırsa "$\equiv$" (mod n) bir denklik bağıntısıdır.

Tanım 13 *Sabit bir $a \in \mathbb{Z}$ sayısının n modülüne göre eşdeğer olan bütün tamsayıların kümesine a ile tanmlanan denklik sınıfı denir ve $[a]$ ile gösterilir. Buna göre*

$$[a] = \{x \in \mathbb{Z} : x \equiv a \ \ (mod\ n)\}$$

olur.

Örnek 14 *4 modülüne göre denklik sınıflarını bulalım.*

$$\begin{aligned} [0] &= \{x \in \mathbb{Z} : x \equiv 0 \ \ (mod\ 3)\} \\ &= \{..., -12,\ -8,\ -4,\ 0,\ 4,\ 8,\ 12, ...\} \end{aligned}$$

$$\begin{aligned} [1] &= \{x \in \mathbb{Z} : x \equiv 1 \ \ (mod\ 3)\} \\ &= \{..., -11,\ -7,\ -3,\ 1,\ 5,\ 9,\ 13, ...\} \end{aligned}$$

$$\begin{aligned} [2] &= \{x \in \mathbb{Z} : x \equiv 2 \ \ (mod\ 3)\} \\ &= \{..., -10,\ -6,\ -2,\ 2,\ 6,\ 10,\ 14, ...\} \end{aligned}$$

$$\begin{aligned} [3] &= \{x \in \mathbb{Z} : x \equiv 3 \ \ (mod\ 3)\} \\ &= \{..., -9,\ -5,\ -1,\ 3,\ 7,\ 11,\ 15, ...\} \end{aligned}$$

Burada dikkat edilirse her tamsayı bu 4 sınıftan birine aittir.

Şimdi daha genel durumu düşünelim. Bir tamsayı n ile bölünürse kalan 0, 1, 2, ...,n-1 tamsayılarından biridir. Oluşabilen tüm denklik sınıfları

$$\mathbb{Z}_n = \{[0]\,,\ [1]\,,\ [2]\,, ..., [n-1]\}$$

olur. Bu denklik sınıflarına n modülüne göre tamsayı sınıfları denir.

Teorem 15 *$\mathbb{Z}_n$, n modulüne göre tamsayılar kümesi olsun. Bu durumda aşağıdakiler sağlanır.*
1. Her $[a] \in \mathbb{Z}_n$ için $[a] \neq \emptyset$,
2. $[a] \in \mathbb{Z}_n$ ve $b \in [a]$ ise, $[b] = [a]$,
3. Her $[a]\,,\ [b] \in \mathbb{Z}_n$ ve $[b] \neq [a]$ için $[a] \cap [b] = \emptyset$,
4. $\bigcup\limits_{[a] \in \mathbb{Z}_n} [a] = \mathbb{Z}$.

İspat: 1. $a \equiv a \pmod{n}$ olduğundan $a \in [a]$ olmalıdır. O halde $[a] \neq \emptyset$ sağlanır.
2. $b \in [a]$ olsun. Bu durumda $b \equiv a \pmod{n}$ olur. $x \in [b]$ ise $x \equiv b \pmod{n}$ dir. Bu durumda $x \equiv b \pmod{n}$ ve $b \equiv a \pmod{n}$ olup $x \equiv a \pmod{n}$ yani $x \in [a]$ elde edilir. Buna göre $[b] \subset [a]$ elde edilir. Benzer olarak $[a] \subset [b]$ elde edilir. Dolayısıyla $[b] = [a]$ bulunur.
3. Kabul edelimki $[b] \neq [a]$ için $[a] \cap [b] \neq \emptyset$ olsun. Bu durumda $\exists c \in [a] \cap [b]$ vardır. O halde $c \in [a]$ ve $c \in [b]$ olup 2. özellikten $[c] = [a]$ ve $[c] = [b]$ bulunur. Bu ise $[a] = [b]$ oluğundan kabul ile çelişir. O halde $[a] \cap [b] = \emptyset$ olmalıdır.

Tanım 16 *Her $[a]\,,\ [b] \in \mathbb{Z}_n$ olmak üzere $+_n$ işlemini aşağıdaki şekilde tanımlayalım.*

$$[a] +_n [b] = [a+b]$$

Burada tanımlanan işlemin denklik sınıflarından her birinde seçilen eleman değil, denklik sınıfına bağlı olduğunu göstermeliyiz.O halde $[a_1] = [a]$ ve $[b_1] = [b]$ ise

$$[a_1 + b_1] = [a+b]$$

olur.

Örnek 17 $[2]\,,\ [3] \in \mathbb{Z}_4$ *için*

$$[2] +_n [3] = [2+3] = [5] = [1]$$

elde edilir.

Teorem 18 *Her n pozitif tamsayısı için $(\mathbb{Z}_n, +_n)$ matematiksel sistemi, n modülüne göre tamsayılar grubu olarak bilinen bir değişmeli grup (Abelyen) oluşturur.*

İspat: $(\mathbb{Z}_n, +_n)$ matematiksel sisteminin değişmeli grup olduğunu göstermek için birleşmeli, birim elemanlı ve her elemanın tersinin olduğunu gösterip son olarakta değişmeli olduğunu göstermeliyiz. $[a]\,,\ [b]\,,\ [c] \in \mathbb{Z}_n$ olmak üzere

$$\begin{aligned} [a] +_n ([b] +_n [c]) &= [a] +_n [b+c] = [a+(b+c)] \\ &= [(a+b)+c] = [a+b] +_n [c] \\ &= ([a] +_n [b]) +_n [c] \end{aligned}$$

olduğundan $+_n$ işlemi birleşmelidir.

$$[0] +_n [a] = [a] +_n [0] = [a]$$

olduğundan $[0] \in \mathbb{Z}_n$ birim elemandır. $[a] \in \mathbb{Z}_n$ için $[n-a] \in \mathbb{Z}_n$ olduğundan,

$$[a] +_n [n-a] = [a + (n-a)] = [n] = [0]$$

olup

$$[a]^{-1} = [n-a]$$

elde edilir. Bu durumda $(\mathbb{Z}_n, +_n)$ sistemi bir grup oluşturur.

$$[a] +_n [b] = [a+b] = [b+a] = [b] +_n [a]$$

olduğundan grup değişmelidir.

Uyarı 19 *Yukarıda tanımlanan grup işlemi yerine*

$$[a] \odot [b] = [ab]$$

işlemi, iyi tanımış olduğu, birleşmeli olduğu ve birim elemana sahip olduğu görülebilir. Birim eleman [1] *olur. Fakat bu işleme göre her elemanın tersi olmadığından bir grup oluşturmaz.*