



# CEBİRE GİRİŞ

Doç. Dr. Figen ERYILMAZ

CEBİRE GİRİŞ

Doç. Dr. Figen ERYILMAZ

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

| * | a | b | c | d |
|---|---|---|---|---|
| a | a | b | c | d |
| b | b | c | d | a |
| c | c | d | a | b |
| d | d | a | b | c |



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

$$\begin{aligned}(R, +, \cdot) \\ (R, +) \text{ bir abelyen gruptur} \\ (R, \cdot) \text{ kapalıdır} \\ a(bc) &= (ab)c \\ a(b + c) &= ab + ac \\ (a + b)c &= ac + bc\end{aligned}$$



# CEBİRE GİRİŞ

Doç. Dr. Figen ERYILMAZ

Ondokuz Mayıs Üniversitesi  
Eğitim Fakültesi



## **CEBİRE GİRİŞ**

Doç. Dr. Figen ERYILMAZ

©Ondokuz Mayıs Üniversitesi Yayınları  
Samsun 2026

### **Yayın Yönetmeni**

Doç. Dr. Muhammet MEMİŞ

### **Sayfa Düzeni**

Özlem TEKİNER

### **ISBN**

978-605-5085-58-2

### **Ondokuz Mayıs Üniversitesi Yayınları**

Ondokuz Mayıs Üniversitesi Kurupelit Kampüsü  
Yayın Koordinatörlüğü 55139 Atakum/SAMSUN  
0362 312 19 19  
yayinkoordinatorlugu@omu.edu.tr

Kitapta yer alan bilgilerin tüm sorumluluğu yazara aittir.

# CEBİRE GİRİŞ

Doç. Dr. Figen ERYILMAZ

# ÖNSÖZ

---

Sevgili Okuyucu,

Bu çalışma, Ondokuz Mayıs Üniversitesi Eğitim Fakültesi Matematik Eğitimi Bölümü'nde verilen Cebire Giriş dersinde anlatılan ders notlarından derlenmiş ve düzenlenmiş bir kaynaktır. Yüksek Öğretim Kurumu tarafından yayınlanan Öğretmen Yetiştirme Lisans Programları kapsamında sunulan içeriklerle oluşturulmuş olan bu kitapta, cebirin temel kavramları yer almaktadır. Ayrıca üniversitelerin matematik bölümlerindeki öğrencilere Soyut Cebir dersleri için yardımcı olacak ve temel ders kaynağı oluşturacak niteliktedir. Her bölüm, Ondokuz Mayıs Üniversitesi'nde lisans düzeyinde yürütülmüş olan cebir derslerinden elde edilen bilgileri ve öğretim deneyimini temel alarak oluşturulmuştur.

Hazırlanan bu kitap sadece bir ders materyali olarak değil, aynı zamanda öğrencilerin başvurabileceği bir kaynak olarak da tasarlanmıştır. Bu kaynak, öğrencilerin cebir konusundaki eksikliklerini gidermek, konuya olan ilgisini artırmak ve örneklerle desteklemek için özenle derlenmiştir. Kitap ile cebirin temel kavramlarını ve ilkelerini, lisans düzeyindeki öğrencilere anlaşılır bir şekilde öğretmek amaçlanmaktadır.

Cebir, matematiğin önemli bir kolu olup birçok disiplinde temel bir rol oynamaktadır. Kitap yardımıyla, cebirin temel prensiplerinin kavranması ve ileri seviye cebir konularına sağlam bir temel oluşturulması sağlanacaktır. Bu kitabın, öğrencilerin matematikle olan yolculuklarında bir rehber ve referans kaynağı olması hedeflenmektedir. Her bölüm, basitten karmaşığa doğru ilerleyen adımlarla düzenlenmiş ve okuyucunun konuyu adım adım kavramasına yardımcı olacak örneklerle desteklenmiştir.

Umarım bu kaynak, siz değerli okuyucuların cebir merakını arttırarak matematikle olan yolculuğunuzu daha keyifli hale getirir.

Saygılarımla.

Figen ERYILMAZ

Nisan-2026

# İÇİNDEKİLER

---

|                                         |            |
|-----------------------------------------|------------|
| ÖNSÖZ.....                              | 4          |
| KISALTMALAR.....                        | 6          |
| <b>1. TEMEL BİLGİLER.....</b>           | <b>7</b>   |
| 1.1. Kümeler .....                      | 7          |
| 1.2. Kartezyen Çarpım ve Bağntı .....   | 12         |
| 1.3. Fonksiyonlar .....                 | 17         |
| 1.4. İkili İşlemler.....                | 22         |
| 1.5. Tamsayılarda Bölünebilme .....     | 26         |
| 1.6. Modüler Aritmetik .....            | 39         |
| <b>2. GRUPLAR.....</b>                  | <b>42</b>  |
| 2.1. Grup Aksiyomları .....             | 42         |
| 2.2. Alt Gruplar .....                  | 48         |
| 2.3. Devirli Gruplar.....               | 52         |
| 2.4. Normal Alt Gruplar.....            | 59         |
| 2.5. Grup Homomorfizmaları .....        | 67         |
| 2.6. Simetrik Gruplar .....             | 78         |
| <b>3. HALKALAR .....</b>                | <b>91</b>  |
| 3.1. Halka Kavramı ve Özellikleri ..... | 91         |
| 3.2. Alt Halka ve İdealler .....        | 98         |
| 3.3. Halka Homomorfizmaları .....       | 107        |
| 3.4. Asal ve Maksimal İdealler .....    | 114        |
| <b>4. KAYNAKLAR .....</b>               | <b>118</b> |

## KISALTMALAR

---

|                        |                                                   |
|------------------------|---------------------------------------------------|
| $\mathbb{N}$           | : Doğal sayılar kümesi                            |
| $\mathbb{Z}$           | : Tam sayılar kümesi                              |
| $\mathbb{Z}^+$         | : Pozitif tam sayılar kümesi                      |
| $\mathbb{Q}$           | : Rasyonel sayılar kümesi                         |
| $\mathbb{R}$           | : Reel sayılar kümesi                             |
| $\emptyset$            | : Boş küme                                        |
| $\subset$              | : Alt küme                                        |
| $\subsetneq$           | : Öz alt küme                                     |
| $f _K$                 | : $f$ fonksiyonunun $K$ alt kümesine kısıtlanması |
| $IP$                   | : Asal sayılar kümesi                             |
| $(m, n)$               | : $m$ ile $n$ sayılarının en büyük ortak böleni   |
| $[m, n]$               | : $m$ ile $n$ sayılarının en küçük ortak katı     |
| $\mathbb{Z}_m$         | : $m$ modülüne göre kalan sınıfları kümesi        |
| $\circ (G)$ veya $ G $ | : $G$ grubunun mertebesi                          |
| $<$                    | : Alt grup                                        |
| $\triangleleft$        | : Normal alt grup                                 |
| $\langle M \rangle$    | : $M$ kümesi tarafından üretilen alt grup         |
| $\langle a \rangle$    | : $a$ elemanının ürettiği alt grup                |
| $\circ (a)$            | : $a$ elemanının mertebesi                        |
| $G/N$                  | : $G$ grubunun $N$ alt grubuna göre bölüm grubu   |
| $\text{Çek}(f)$        | : $f$ homomorfizmasının çekirdeği                 |
| $C(a)$                 | : $a$ elemanının eşlenik sınıfı                   |
| $(a)$                  | : $a$ elemanı tarafından üretilen esas ideal      |
| $(A)$                  | : $A$ kümesinin ürettiği ideal                    |
| $R/I$                  | : $R$ halkasının $I$ idealine göre bölüm halkası  |
| $0_R$                  | : $R$ halkasının sıfırı                           |
| $1_R$                  | : $R$ halkasının birimi                           |
| $\text{Gör}(f)$        | : $f$ homomorfizmasının görüntü kümesi            |
| $\cong$                | : İzomorfizma                                     |
| $\forall$              | : Her                                             |
| $\exists$              | : En az                                           |

# BÖLÜM 1

## 1. TEMEL BİLGİLER

### 1.1. KÜMELER

Bu bölümde, matematiğin en temel kavramlarından olan kümeler kuramı aksiyomatik olarak kurulan kümeler kuramı biçiminde değil, ilerideki kısımlarda gerekli olan temel kavramlar ve gösterimler üzerinde durulacaktır. Küme kavramı Cantor (1845-1918) tarafından ortaya konulmuş olup matematiğin her dalında önemli bir yere sahiptir.

**Tanım 1.1.1.** Ayırt edilebilen belirli nesnelerin topluluğuna **küme** denir.

Kümenin içindeki nesnelere de o kümenin **elemanları** denir. Kümeler genellikle  $A, B, C, \dots$  gibi büyük harflerle gösterilir, elemanları ise genellikle küçük harflerle gösterilir.  $a, A$  kümesinin bir elemanı ise bu  $a \in A$  ile ifade edilir. Eğer  $a, A$  kümesinin bir elemanı değilse bu  $a \notin A$  ile ifade edilir.  $A$  kümesinin eleman sayısı  $s(A)$  veya  $n(A)$  ile gösterilir. Kümelerin gösteriminde aşağıdaki gibi üç farklı yol izlenir:

**1) Açık Gösterim (Listeleme Yöntemi).** Kümenin elemanları belli ise bu elemanları  $\{ \}$  parantezler içine yazılarak elde edilen gösterim şeklidir.

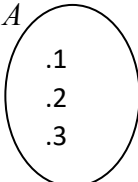
**Örnek.**  $A = \{1,2,5,7\}, B = \{a, b, c, x, y, z\}$ .

**2) Kapalı Gösterim (Ortak Özellik Yöntemiyle Gösterim).** Kümenin elemanları ortak özelliklere sahipse, bu küme elemanları tek tek yazmak yerine ortak özellik belirtilerek ifade edilebilir. Bu gösterim biçiminde küme  $\{x|x \text{ -- in özellikleri}\}$  şeklinde yazılır.

**Örnek.**  $A = \{x|x \in \mathbb{Z} \text{ ve } -5 \leq x < 7\}$  kapalı şekilde gösterilmiştir. Bu kümenin açık gösterimi  $A = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$  olur.  $B = \{x|x \in \mathbb{R} \text{ ve } -5 \leq x < 7\}$  kümesi açık şekilde gösterilemez.

**3) Şematik Gösterim (Venn Şeması).** Kümenin elemanlarının bir kapalı geometrik şekil içine yazılarak elde edilen gösterim biçimidir.

**Örnek.**  $A$

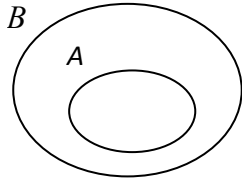


**Tanım 1.1.2.** Hiçbir elemanı olmayan kümeye **boş küme** denir ve  $\emptyset$  ile gösterilir.

**Tanım 1.1.3.** Elemanları aynı olan kümelere **eşit kümeler** denir.  $A$  ve  $B$  kümeleri eşitse bu  $A = B$  ile ifade edilir. Eğer  $A$  kümesi boş küme ise bu  $A = \emptyset$  şeklinde de ifade edilebilir.

**Örnek.**  $A = \{a, b, c, x, y\} = \{x, b, c, a, y\}$ .

**Tanım 1.1.4.**  $A$  ve  $B$  iki küme olsun. Eğer  $A$  nın her elemanı  $B$  nin de bir elemanı ise  $A$  ya,  $B$  nin bir **alt kümesi** denir ve genellikle  $A \subset B$  veya  $B \supset A$  ile ifade edilir. Eğer  $A$  kümesi  $B$  kümesinin bir alt kümesi değil ise, bu durum  $A \not\subset B$  ile gösterilir.



**Not.** Her kümenin, kendisinin bir alt kümesi ve boş kümenin de her kümenin bir alt kümesi olduğu açıktır.

**Tanım 1.1.5.** Bir kümenin, kendisinden ve boş kümeden farklı her alt kümesine bu kümenin bir **öz (has) alt kümesi** denir. Eğer  $A, B$  nin bir öz alt kümesi ise bu genellikle  $A \subsetneq B$ ,  $A \subsetneq B$ ,  $B \supsetneq A$  veya  $B \supsetneq A$  ile gösterilir.

**Tanım 1.1.6.** Elemanları kümeler olan kümeye **kümeler kümesi** veya **kümeler ailesi** denir.

**Örnek.**  $A = \{\emptyset, \{a, b\}, \{a, x, y\}\}$  bir kümeler ailesidir.

**Örnek.**  $A = \{\emptyset, a, b, \{a, b\}, \{a\}, \{a, c\}, x, y\}$  kümesi verilsin.

(i)  $\{a, b\} \in A$  ve  $\{a, b\} \subset A$  dır.

(ii)  $\emptyset \subset A$  ve  $\emptyset \in A$  dır.

(iii)  $\{x, y\} \subset A$  ve  $\{x, y\} \notin A$  dır.

(iv)  $\{a\} \subset A$  ve  $\{a\} \in A$  olur.

(v)  $\{a, c\} \in A$  ve  $\{a, c\} \not\subset A$  dır.

(vi)  $s(A) = 8$  dir.

**Önerme 1.1.7.** Aşağıdaki ifadeler doğrudur.

(i) Her  $A$  kümesi için  $A \subset A$  dır.

(ii)  $A \subset B$  ve  $B \subset C$  ise  $A \subset C$  dir.

(iii)  $A$  ve  $B$  iki küme olmak üzere  $A = B$  olması için gerek ve yeter koşul  $A \subset B$  ve  $B \subset A$  olmasıdır.

**İspat.** (i) Eğer  $A = \emptyset$  ise boş küme her kümenin bir alt kümesi olduğundan  $A \subset A$  olur. Eğer  $A \neq \emptyset$  ise  $A$  nın her elemanı yine  $A$  nın bir elemanı olduğundan yine  $A \subset A$  olur.

(ii)  $A \subset B$  ve  $B \subset C$  olsun.  $A \subset B$  olduğundan tanımdan  $A$  nın her elemanı  $B$  nin bir elemanıdır.  $B \subset C$  olduğundan tanımdan  $B$  nin her elemanı  $C$  nin bir elemanıdır. O halde  $A$  nın her elemanı  $C$  nin bir elemanı olup tanımdan  $A \subset C$  olur.

(iii)  $(\Rightarrow) A = B$  olsun. Bu durumda tanımdan  $A$  ve  $B$  nin elemanları aynı olup  $A$  nın her elemanı  $B$  nin bir elemanı,  $B$  nin her elemanı da  $A$  nın bir elemanı olur. O halde tanımdan  $A \subset B$  ve  $B \subset A$  olup istenen elde edilir.

$(\Leftarrow) A \subset B$  ve  $B \subset A$  olsun.  $A \subset B$  olduğundan tanımdan  $A$  nın her elemanı  $B$  nin bir elemanıdır.  $B \subset A$  olduğundan tanımdan  $B$  nin her elemanı  $A$  nın bir elemanıdır. O halde  $A$  ve  $B$  nin elemanları aynı olup  $A = B$  olur.

**Tanım 1.1.8.** Üzerinde işlem yapılan bütün kümeleri kapsayan bir kümeye **evrensel küme** denir.

**Örnek.**  $A = \{a, b, c, x, y\}$ ,  $B = \{1, 2, x, y\}$  ve  $C = \{a, b, 1, 2, 3\}$  kümeleri verilsin.  $E_1 = \{a, b, c, 1, 2, 3, x, y\}$  kümesi bu kümeler için bir evrensel kümedir.  $E_2 = \{a, b, c, d, 1, 2, 3, x, y, z, t\}$  kümesi de bu kümeler için bir evrensel kümedir.

**Tanım 1.1.9.**  $A$  ve  $B$  iki küme olsun.  $A$  da olup da  $B$  de olmayan elemanların kümesine **fark kümesi** denir ve genellikle  $A - B$  veya  $A \setminus B$  ile gösterilir. Yani

$$A - B = \{x | x \in A \text{ ve } x \notin B\} = \{x | x \in A \wedge x \notin B\}$$

olarak tanımlanır.

**Önerme 1.1.10.**  $A$  bir küme ise  $A - A = \emptyset$  ve  $A - \emptyset = A$  olur.

**İspat.**  $A$  bir küme olsun. Bu durumda tanımdan  $A - A = \{x | x \in A \wedge x \notin A\} = \emptyset$  ve  $A - \emptyset = \{x | x \in A \wedge x \notin \emptyset\} = \{x | x \in A\} = A$  olup istenen elde edilir.

**Tanım 1.1.11.**  $A$  bir küme ve  $E$  evrensel küme olsun.  $E - A$  kümesine  $A$  nın  $E$  evrensel kümesine göre **tümleyeni (tamlayanı)** denir ve genellikle  $\bar{A}$ ,  $A'$ ,  $A^t$  veya  $A^c$  ile gösterilir.

**Önerme 1.1.12.**  $A$  bir küme ve  $E$  evrensel küme olsun. Bu durumda  $(A^t)^t = A$  olur.

**Önerme 1.1.13.**  $E$  evrensel kümesi için  $\emptyset^t = E$  ve  $E^t = \emptyset$  olur.

**Tanım 1.1.14.**  $A$  ve  $B$  iki küme olsun. Hem  $A$  da, hem de  $B$  de bulunan elemanların kümesine  $A$  ve  $B$  nin **kesişimi (arakesiti)** denir ve  $A \cap B$  ile ifade edilir. Yani

$$A \cap B = \{x | x \in A \wedge x \in B\}$$

olarak tanımlanır.

**Önerme 1.1.15.**  $A, B$  ve  $C$  kümeler olmak üzere aşağıdaki ifadeler doğrudur.

- (i)  $A \cap A = A$  dır (Tek kuvvet özelliği).
- (ii)  $A \cap \emptyset = \emptyset$  olur.
- (iii)  $A \cap B = B \cap A$  dır (Değişme özelliği).
- (iv)  $A \cap B \subset A$  ve  $A \cap B \subset B$  dir.
- (v)  $A \cap (B \cap C) = (A \cap B) \cap C$  dir (Birleşme özelliği).

**Tanım 1.1.16.** Kesişimleri boş küme olan kümelere **ayrık kümeler** denir.

**Önerme 1.1.17.**  $A$  ve  $B$  iki küme olsun. Bu takdirde  $A - B = A \cap B^t = B^t - A^t$  olur.

**Tanım 1.1.18.**  $A$  ve  $B$  iki küme olsun.  $A$  veya  $B$  den en az birine ait olan elemanların kümesine  $A$  ve  $B$  nin **birleşimi** denir ve  $A \cup B$  ile gösterilir. Yani

$$A \cup B = \{x | x \in A \vee x \in B\}$$

olarak tanımlanır.

**Önerme 1.1.19.**  $A, B$  ve  $C$  kümeler olmak üzere aşağıdaki ifadeler doğrudur.

- (i)  $A \cup A = A$  dır (Tek kuvvet özelliği).
- (ii)  $A \cup \emptyset = A$  olur.
- (iii)  $A \cup B = B \cup A$  dır (Değişme özelliği).
- (iv)  $A \subset A \cup B$  ve  $B \subset A \cup B$  dir.
- (v)  $A \cup (B \cup C) = (A \cup B) \cup C$  dir (Birleşme özelliği).

**Önerme 1.1.20.**  $A$  ve  $B$  iki küme olmak üzere  $E$  evrensel kümesi verilsin. Bu takdirde aşağıdaki ifadeler doğrudur.

- (i)  $A \cap A^t = \emptyset$  dir.
- (ii)  $A \cup A^t = E$  olur.
- (iii)  $(A \cup B)^t = A^t \cap B^t$  dir (De Morgan kuralı).
- (iv)  $(A \cap B)^t = A^t \cup B^t$  dir (De Morgan kuralı).
- (v)  $A \subset B$  ise  $B^t \subset A^t$  dir.

**Önerme 1.1.21.**  $A, B$  ve  $C$  kümeleri için aşağıdakiler doğrudur.

- (i)  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$  olur ( $\cup$  işleminin  $\cap$  üzerine dağılma özelliği).
- (ii)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$  olur ( $\cap$  işleminin  $\cup$  üzerine dağılma özelliği).

**Tanım 1.1.22.**  $I$  bir küme olsun.  $\forall i \in I$  için  $A_i$  bir küme olmak üzere bütün  $A_i$  kümelerinin oluşturduğu  $\{A_i | i \in I\}$  ailesine  $I$  **indis kümesi ile numaralanmış (damgalanmış) bir aile (kümeler ailesi)** denir ve genellikle  $\{A_i\}_{i \in I}$  şeklinde yazılır.

$\bigcup_{i \in I} A_i = \{x | \text{ en az bir } i \in I \text{ için } x \in A_i\}$  kümesine  $\{A_i | i \in I\}$  **küme ailesinin birleşim kümesi** ve  $\bigcap_{i \in I} A_i = \{x | \text{ her } i \in I \text{ için } x \in A_i\}$  kümesine  $\{A_i | i \in I\}$  **küme ailesinin kesişim kümesi** denir. Ayrıca  $\{A_i | i \in I\}$  küme ailesi için  $I = \emptyset$  ise  $\{A_i | i \in I\}$  ailesine **boş aile** adı verilir.

**Önerme 1.1.23. (Genelleştirilmiş De Morgan Özellikleri)**  $\{A_i\}_{i \in I}$  bir kümeler ailesi ve  $E$  evrensel küme olsun. Bu takdirde,

- (i)  $(\bigcap_{i \in I} A_i)^t = \bigcup_{i \in I} A_i^t$  olur.
- (ii)  $(\bigcup_{i \in I} A_i)^t = \bigcap_{i \in I} A_i^t$  olur.

**Önerme 1.1.24. (Genelleştirilmiş Dağılma Özellikleri)**  $\{A_i\}_{i \in I}$  küme ailesi ve  $B$  kümesi verilsin. Bu takdirde,

- (i)  $B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \cup A_i)$  olur.
- (ii)  $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$  olur.

**Tanım 1.1.25.** Bir  $A$  kümesinin bütün alt kümelerinin oluşturduğu aileye  $A$  nın **kuvvet kümesi** denir ve genellikle  $P(A)$  ile gösterilir.

**Örnek.**  $A = \{a, b, c\}$  ise  $A$  kümesinin kuvvet kümesi

$$P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

olur.

**Tanım 1.1.26.**  $A$  boştan farklı bir küme ve  $\forall i \in I$  için  $A_i$  kümeleri  $A$  nın birtakım alt kümeleri olsunlar. Eğer,

- (i)  $\forall i \in I$  için  $A_i \neq \emptyset$ ,
- (ii)  $i \neq j$  olan  $\forall i, j \in I$  için  $A_i \cap A_j = \emptyset$  ve
- (iii)  $A = \bigcup_{i \in I} A_i$

ise  $\{A_i\}_{i \in I}$  ailesine  $A$  kümesinin **ayrışımı** denir. Burada eğer  $I = \{i\}$  şeklinde tek elemanlı ve  $A_i = A$  ise  $\{A_i\}_{i \in I} = \{A\}$  ailesi  $A$  kümesinin bir **ayrışımı** olarak kabul edilir.

**Örnek.**  $A = \{1, 2, 3, x, a, b\}$  ise  $\{\{1, x\}, \{2\}, \{3, a, b\}\}$  ailesi  $A$  nın bir ayrışımıdır.  $\{\{1, 3, x\}, \{2, a, b\}\}$  kümesi de  $A$  kümesinin bir ayrışımıdır.

**Tanım 1.1.27.**  $A$  ve  $B$  iki küme olmak üzere  $(A \cup B) - (A \cap B)$  kümesine  $A$  ile  $B$  nin **simetrik farkı** denir ve genellikle  $A \Delta B$  ile gösterilir.

**Önerme 1.1.28.**  $A$  ve  $B$  iki küme olsun. Bu takdirde,

- (i)  $A \Delta B = B \Delta A$  olur.
- (ii)  $A \Delta B = (A - B) \cup (B - A)$  olur.

## 1 KARTEZYEN ÇARPIM VE BAĞINTI

**Tanım 1.2.1.** Her ikisi de boş kümeden farklı  $A$  ve  $B$  kümelerinden sırasıyla  $a$  ve  $b$  elemanları alınarak sıra önemli olacak şekilde oluşturulan  $(a, b)$  ifadesine bir **sıralı ikili** denir.

**Tanım 1.2.2.**  $a_1, a_2, \dots, a_n$  elemanları sırasıyla  $A_1, A_2, \dots, A_n$  kümelerine ait olsun. Sıra önemli olmak üzere oluşturulan  $(a_1, a_2, \dots, a_n)$  ifadesine bir **sıralı  $n$  –li** denir. Burada  $1 \leq k \leq n$  olmak üzere  $a_k$  elemanına  $(a_1, a_2, \dots, a_n)$  sıralı  $n$ -lisinin  **$k$ . bileşeni** denir.

**Örnek.**  $(a, b, c, a, c)$  ifadesi bir sıralı beşlidir.  $((a, b, c), (a, c))$  ifadesi bir sıralı ikilidir.  $(a, b, (a, b))$  ifadesi bir sıralı üçlüdür.

**Tanım 1.2.3.**  $a_1, a_2, \dots, a_n, a_1', a_2', \dots, a_n'$  elemanlar olmak üzere  $(a_1, a_2, \dots, a_n) = (a_1', a_2', \dots, a_n') \Leftrightarrow a_1 = a_1', a_2 = a_2', \dots, a_n = a_n'$  olarak tanımlanır.

**Tanım 1.2.4.**  $A$  ve  $B$  iki küme olsun.  $\{(a, b) \mid a \in A \wedge b \in B\}$  kümesine  $A$  nın  $B$  ile **kartezyen (dik) çarpımı** denir ve  $A \times B$  ile gösterilir.

**Tanım 1.2.5.**  $A_1, A_2, \dots, A_n$   $n$  tane küme olsun.  $A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}$  olarak tanımlanır.

**Örnek.**  $A = \{a, b, c\}$ ,  $B = \{x\}$  ve  $C = \{a, x\}$  kümeleri verilsin.

- (i)  $A \times B = \{(a, x), (b, x), (c, x)\}$  olur.
- (ii)  $B \times C = \{(x, a), (x, x)\}$  olur.
- (iii)  $A \times (B \times C) = \{(a, (x, a)), (a, (x, x)), (b, (x, a)), (b, (x, x)), (c, (x, a)), (c, (x, x))\}$  olur.

(iv)  $(A \times B) \times C = \{(a, x), a), ((a, x), x), (b, x), a), ((b, x), x), (c, x), a), ((c, x), x)\}$  olur.

(v)  $A \times B \times C = \{(a, x, a), (a, x, x), (b, x, a), (b, x, x), (c, x, a), (c, x, x)\}$  olur.

(vi)  $B \times A = \{(x, a), (x, b), (x, c)\}$  olur.

(vii)  $A \times A = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$  olur.

Bu örnekten  $A \times (B \times C)$ ,  $(A \times B) \times C$  ve  $A \times B \times C$  kümelerinin birbirinden farklı olduğu anlaşılır.

**Önerme 1.2.6.**  $A$ ,  $B$  ve  $C$  kümeler olmak üzere kartezyen çarpım ile ilgili aşağıdaki özellikler doğrudur.

(i)  $A \times \emptyset = \emptyset \times A = \emptyset$  olur.

(ii) (a)  $A \times (B \cup C) = (A \times B) \cup (A \times C)$  olur.

(b)  $(A \cup B) \times C = (A \times C) \cup (B \times C)$  olur.

(iii) (a)  $A \times (B \cap C) = (A \times B) \cap (A \times C)$  olur.

(b)  $(A \cap B) \times C = (A \times C) \cap (B \times C)$  olur.

(iv)  $A \times (B \times C)$ ,  $(A \times B) \times C$  ve  $A \times B \times C$  kümeleri birbirinden farklıdır.

(v)  $A$  ve  $B$  sonlu elemanlı iseler  $A \times B$  de sonlu elemanlıdır ve  $s(A \times B) = s(A) \cdot s(B)$  olur.

**Tanım 1.2.7.**  $A$  ve  $B$  iki küme olsun.  $A \times B$  nin her alt kümesine  $A$  dan  $B$  ye bir **bağıntı** denir. Bağıntılar genellikle  $\alpha, \beta, \gamma, f, g, h, \dots$  gibi harflerle gösterilir.

$\beta$ ,  $A$  dan  $B$  ye bir bağıntı olsun. Eğer  $(a, b) \in \beta$  ise  **$a$  elemanı  $\beta$  bağıntısı ile  $b$  elemanına bağlıdır** (veya  **$\beta$ ,  $a$  elemanını  $b$  elemanına eşliyor**) denir ve bu durum genellikle  $a\beta b$  ile ifade edilir.

**Örnek.**  $A = \{a, b, c, d\}$  ve  $B = \{a, b, x, y\}$  kümeleri verilsin.

(i)  $\beta = \{(a, a), (a, x), (b, x), (d, x), (d, y)\}$  kümesi  $A$  dan  $B$  ye bir bağıntıdır.

(ii)  $\beta = \{(x, a), (y, c), (y, a)\}$  kümesi  $B$  den  $A$  ya bir bağıntıdır.

(iii)  $\alpha = \{(a, a), (a, b), (b, a)\}$  kümesi hem  $A$  dan  $A$  ya bir bağıntıdır, hem  $A$  dan  $B$  ye bir bağıntıdır, hem  $B$  den  $A$  ya bir bağıntıdır, hem  $B$  den  $B$  ye bir bağıntıdır, hem de  $A \cap B$  den  $A \cap B$  ye bir bağıntıdır.

(iv)  $f = \{(a, x), (b, x), (c, x), (d, x)\}$  kümesi  $A$  dan  $B$  ye bir bağıntıdır.

(v)  $\beta = \{(a, a), (a, b), (a, x), (a, y)\}$  kümesi  $A$  dan  $B$  ye bir bağıntıdır.

**Tanım 1.2.8.**  $A$  boştan farklı bir küme olmak üzere  $A$  dan  $A$  ya bir bağıntıya  **$A$  da bir bağıntı** denir.

**Tanım 1.2.9.**  $\beta$ ,  $A$  dan  $B$  ye bir bağıntı olsun. Bu durumda  $\{(b, a) \mid (a, b) \in \beta\}$  kümesi  $B \times A$  nın boştan farklı bir alt kümesi olup  $B$  den  $A$  ya bir bağıntıdır. Bu bağıntıya  **$\beta$  bağıntısının tersi** denir ve genellikle  $\beta^{-1}$  ile gösterilir.

**Örnek.**  $A = \{-1, 2, a, b\}$  ve  $B = \{-3, 2, x, y\}$  olsun.  $A$  dan  $B$  ye

$$\beta = \{(-1, x), (-1, 2), (2, -3), (a, x), (a, y), (b, y)\}$$

bağıntısının ters bağıntısı

$$\beta^{-1} = \{(x, -1), (2, -1), (-3, 2), (x, a), (y, a), (y, b)\}$$

olur.

**Tanım 1.2. 10.**  $\beta$ ,  $A$  kümesinde bir bağıntı olsun.

- (i)  $\forall a \in A$  için  $(a, a) \in \beta$  ise  $\beta$  ya bir **yansıyan bağıntı** denir, bu özelliğe de  $\beta$  nın **yansıma özelliği** denir.
- (ii)  $(a, b) \in \beta$  olan her  $a, b \in A$  için  $(b, a) \in \beta$  ise  $\beta$  ya bir **simetrik bağıntı** denir, bu özelliğe de  $\beta$  nın **simetri özelliği** denir.
- (iii)  $(a, b), (b, a) \in \beta$  olan her  $a, b \in A$  için  $a = b$  koşulu sağlanıyorsa  $\beta$  ya bir **ters simetrik bağıntı** denir, bu özelliğe de  $\beta$  nın **ters simetri özelliği** denir.
- (iv)  $(a, b), (b, c) \in \beta$  olan her  $a, b, c \in A$  için  $(a, c) \in \beta$  koşulu sağlanıyorsa  $\beta$  ya bir **geçişken bağıntı** denir, bu özelliğe de  $\beta$  nın **geçişme özelliği** denir.

**Örnek.**  $A = \{a, b, c, d, e\}$  kümesi verilsin. Bu kümede,

- (i)  $\beta = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, a)\}$  bağıntısı yansıyandır, simetriktir ve geçişkendir, ancak bu bağıntı ters simetrik değildir.
- (ii)  $\beta = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, a), (a, c), (c, a)\}$  bağıntısı yansıyan ve simetriktir, ancak bu bağıntı ters simetrik değildir.
- (iii)  $\beta = \{(a, b), (c, d), (a, e), (c, e)\}$  bağıntısı ters simetrik ve geçişkendir, ancak bu bağıntı ne yansıyandır, ne de simetriktir.
- (iv)  $\beta = \{(a, a), (a, b), (b, a), (b, c)\}$  bağıntısı ne yansıyandır, ne simetriktir, ne ters simetriktir, ne de geçişkendir.
- (v)  $\beta = \{(a, a), (b, b), (c, c), (d, d), (e, e)\}$  bağıntısı hem yansıyan, hem simetrik, hem ters simetrik, hem de geçişkendir.

**Örnek.**  $\mathbb{R}$  reel sayılar kümesinde  $\beta = \{(x, y) \mid x, y \in \mathbb{R} \wedge x + y = 5\}$  bağıntısı verilsin.  $1 + 1 = 2 \neq 5$  olduğundan  $(1, 1) \notin \beta$  olup bu bağıntı yansıyan değildir.  $(x, y) \in \beta$  olan her  $x, y \in \mathbb{R}$  için  $x + y = 5$  olduğundan  $y + x = 5$  olup  $(y, x) \in \beta$  olur. Dolayısıyla  $\beta$  bağıntısının simetri özelliği vardır.  $2 + 3 = 3 + 2 = 5$  olduğundan  $(2, 3), (3, 2) \in \beta$  olup burada  $2 \neq 3$  olduğundan  $\beta$  bağıntısının ters simetri özelliği yoktur.  $(2, 3), (3, 2) \in \beta$  olduğu halde  $2 + 2 = 4 \neq 5$  olduğundan  $(2, 2) \notin \beta$ dır. Dolayısıyla  $\beta$  bağıntısının geçişme özelliği yoktur.

**Örnek.**  $A = \{1, 2, 3\}$  kümesinde  $\beta = \{(1, 1), (2, 2), (3, 3), (2, 3)\}$  ise  $\beta$  yansıyan, geçişken ve ters simetriktir, ancak simetrik değildir.

**Tanım 1.2.11.**  $\beta$ ,  $A$  kümesinde bir bağıntı olsun. Eğer  $\beta$  nın yansıma, simetri ve geçişme özellikleri varsa  $\beta$  ya bir **denklik bağıntısı** denir.

**Örnek.**  $A = \{a, b, c, d, e\}$  kümesinde

$\beta = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (a, d), (b, a), (b, d), (d, a), (d, b), (c, e), (e, c)\}$  bağıntısı bir denklik bağıntısıdır.

**Tanım 1.2.12.**  $\beta$ ,  $A$  kümesinde bir denklik bağıntısı ve  $a \in A$  olsun.  $\{x \mid x \in A \wedge (a, x) \in \beta\} = \{x \mid x \in A \wedge (x, a) \in \beta\}$  kümesine  $a$  elemanının  $\beta$  bağıntısına göre **denklik sınıfı** denir ve genellikle  $\bar{a}$  ile gösterilir. Yani  $\bar{a} = \{x \mid x \in A \wedge (a, x) \in \beta\} = \{x \mid x \in A \wedge (x, a) \in \beta\}$  olarak tanımlanır.

**Önerme 1.2.13.**  $\beta$ ,  $A$  kümesinde bir denklik bağıntısı olsun. Bu takdirde  $\beta$  nın belirttiği farklı denklik sınıflarının ailesi  $A$  kümesinin bir ayrışımını belirtir.

**Önerme 1.2.14.**  $\{A_i\}_{i \in I}$  ailesi  $A$  kümesinin bir ayrışımı ise bu aile  $A$  da bir denklik bağıntısı belirtir ve bu denklik bağıntısına göre farklı denklik sınıfları  $A_i$  ayrışım kümeleridir.

**Örnek.**  $A = \{a, b, c, x, y, z\}$  kümesinde

$\beta = \{(a, a), (b, b), (c, c), (x, x), (y, y), (z, z), (a, x), (a, y), (x, a), (x, y), (y, a), (y, x), (b, z), (z, b)\}$

bağıntısı bir denklik bağıntısıdır. Bu denklik bağıntısına göre  $\bar{a} = \{a, x, y\}$ ,  $\bar{b} = \{b, z\}$ ,  $\bar{c} = \{c\}$ ,  $\bar{x} = \{a, x, y\}$ ,  $\bar{y} = \{a, x, y\}$  ve  $\bar{z} = \{b, z\}$  olur. Burada  $\bar{a} = \bar{x} = \bar{y}$  ve  $\bar{b} = \bar{z}$  olur.  $\beta$  nın belirttiği farklı denklik sınıflarının ailesi  $\{\bar{a}, \bar{b}, \bar{c}\} = \{\bar{x}, \bar{z}, \bar{c}\}$  olur.

**Örnek.**  $A = \{1, 2, 3, 4, 5\}$  kümesinin bir ayrışımı  $\{\{1\}, \{2, 3\}, \{4, 5\}\}$  olsun. Bu ayrışımın verdiği  $\beta$  denklik bağıntısı şöyle olur:

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

**Tanım 1.2.15.**  $\beta$ ,  $A$  kümesinde bir denklik bağıntısı olsun.  $\beta$  nın  $A$  da belirttiği tüm denklik sınıflarının kümesine  $A$  nın  $\beta$  ya göre **bölüm kümesi** denir ve genellikle  $A/\beta$  ile gösterilir.

$A/\beta$  bölüm kümesinde, her sınıftan bir ve yalnız bir eleman alınarak oluşturulan kümeye bir **tam temsilciler sistemi** denir.

Yukarıdaki örnekte  $\{1,2,4\}$  kümesi  $\beta$  için bir tam temsilciler sistemidir. Bu örnekte  $\{1,3,4\}$  kümesi de  $\beta$  için bir tam temsilciler sistemidir.

**Tanım 1.2.16.**  $\beta$ ,  $A$  kümesinde bir bağıntı olsun. Eğer  $\beta$  nın yansıma, ters simetri ve geçişme özellikleri varsa  $\beta$  ya bir **sıralama** (veya **yarı (kısmi) sıralama**) **bağıntısı** denir.  $\beta$ ,  $A$  da bir sıralama bağıntısı ise  $(A, \beta)$  sıralı ikilisine bir **sıralı küme** denir. Sıralama bağıntıları genellikle  $\leq$  ile gösterilir.

$\leq$ ,  $A$  kümesinde bir sıralama bağıntısı olsun.  $a, b \in A$  olmak üzere eğer  $a \leq b$  ise bu genellikle " **$a, b$  den önce gelir**" veya " **$a, b$  den küçük veya eşittir**" diye okunur.  $a \leq b$  yerine bazen  $b \geq a$  da kullanılır.  $b \geq a$  genellikle " **$b, a$  dan sonra gelir**" veya " **$b, a$  dan büyük veya eşittir**" diye okunur.

**Örnek.** Reel sayılar kümesinde alışılmış  $\leq$  bağıntısı bir sıralama bağıntısıdır. Yani  $\mathbb{R}$  de  $\beta = \{(a, b) \mid a, b \in \mathbb{R} \text{ ve } a \leq b\}$  bağıntısı bir sıralama bağıntısıdır.

**Örnek.** Boştan farklı bir kümeler ailesinde  $\subset$  bağıntısı bir sıralama bağıntısıdır. Yani  $\Omega$  boştan farklı bir aile olmak üzere  $\Omega$  da  $\beta = \{A, B \mid A, B \in \Omega \wedge A \subset B\}$  bağıntısı bir sıralama bağıntısıdır.

**Tanım 1.2.17.**  $\leq$ ,  $A$  kümesinde bir sıralama bağıntısı olsun.  $a, b \in A$  için  $a \leq b$  veya  $b \leq a$  ise  **$a$  ile  $b$  elemanlarına karşılaştırılabilir elemanlar** veya  **$a$  ile  $b$  karşılaştırılabilir** denir.

**Tanım 1.2.18.**  $\leq$ ,  $A$  kümesinde bir sıralama bağıntısı olsun. Eğer  $A$  kümesinde herhangi iki eleman  $\leq$  bağıntısına göre karşılaştırılabilir ise  $\leq$  bağıntısına **tam sıralama bağıntısı** denir.

**Not.**  $\leq$ ,  $A$  kümesinde bir sıralama bağıntısı olsun.  $a, b \in A$  için  $a \leq b$  ve  $a \neq b$  ise bu durum genellikle  $a < b$  (genellikle " **$a, b$  den kesin küçük**" diye okunur) veya  $b > a$  (genellikle " **$b, a$  den kesin büyük**" diye okunur) ile ifade edilir.

**Not.**  $(A, \leq)$  bir sıralı küme ve  $\emptyset \neq B \subset A$  ise,  $B$  de bir sıralı küme olarak düşünülebilir.

**Tanım 1.2.19.** Sıralı bir kümenin tam sıralı bir alt kümesine **zincir** denir.

**Tanım 1.2.20.** Sıralı bir kümenin boştan farklı her alt kümesinin bir en küçük elemanı varsa bu kümeye **iyi sıralı küme** denir.

**Örnek.** Pozitif tam sayılar kümesi, doğal sayılar kümesi alışılmış  $\leq$  bağıntısına göre iyi sıralıdır.

**Zorn Lemması.**  $A$  bir sıralı küme olsun. Eğer  $A$  nın boş olmayan her tam sıralı alt kümesinin yani zincirinin bir üst sınırı varsa  $A$  nın bir maksimal elemanı vardır.

### 1.3. FONKSİYONLAR

**Tanım.1.3.1.**  $A$  ve  $B$  boştan farklı iki küme ve  $f, A$  dan  $B$  ye bir bağıntı olsun. Eğer  $f$  bağıntısı  $A$  nın her elemanını  $B$  nin bir ve yalnız bir elemanına eşliyorsa (yani  $\forall a \in A$  için  $a$  nın  $f$  ile bağlı olduğu  $B$  de bir ve yalnız bir eleman bulunabilirse)  $f$  ye  **$A$  dan  $B$  ye bir fonksiyon** denir. Burada  $A$  ya  $f$  nin **tanım kümesi**,  $B$  ye de **değer kümesi** denir.

**Not.** Eğer  $f, A$  dan  $B$  ye (  $A \rightarrow B$  ) bir fonksiyon ve  $(a, b) \in f$  ise bu genellikle  $f(a) = b$  ile ifade edilir. Buna göre  $f$  fonksiyonu genel olarak

$$\begin{array}{l} f: A \rightarrow B \\ a \rightarrow f(a) \end{array} \text{ veya } f: A \rightarrow B, a \rightarrow f(a)$$

şeklinde de gösterilebilir.

**Not.**  $f$  bağıntısının  $A$  dan  $B$  ye bir fonksiyon olması için,

(i)  $f, A$  nın her elemanını  $B$  nin en az bir elemanına eşlemelidir, yani  $A$  da açıkta eleman kalmamalıdır.

(ii)  $\forall a \in A$  için  $a$  nın  $f$  bağıntısı ile  $B$  de eşlendiği eleman  $a$  ya bağlı olarak tek olmalıdır. Yani  $(a, b_1), (a, b_2) \in f$  ise bu durumda  $b_1 = b_2$  dir.

Bunlardan birincisine  **$f$  nin kapalılığı**, ikincisine de **iyi tanımlılığı** denir.

**Örnek.**  $A = \{a, b, c, d, e\}$  ve  $B = \{x, y, z, k\}$  kümeleri verilsin.

(i)  $f = \{(a, x), (b, k), (c, y), (d, x), (e, k)\}$  kümesi  $A$  dan  $B$  ye bir fonksiyondur.

(ii)  $f = \{(a, y), (b, y), (c, y), (d, y), (e, y)\}$  kümesi  $A$  dan  $B$  ye bir fonksiyondur.

(iii)  $f = \{(a, z), (b, x), (d, y), (e, z)\}$  kümesi  $A$  dan  $B$  ye bir bağıntıdır ancak bir fonksiyon değildir.

- (iv)  $f = \{(a, x), (b, y), (c, x), (d, k), (e, y), (a, y)\}$  kümesi  $A$  dan  $B$  ye bir bağıntıdır, ancak bir fonksiyon değildir.

**Tanım 1.3.2.**  $f$  ve  $g$ ,  $A$  dan  $B$  ye iki fonksiyon olsun. Eğer  $\forall a \in A$  için  $f(a) = g(a)$  ise  $f$  ve  $g$  fonksiyonlarına **eşit fonksiyonlar** denir ve  $f = g$  ile ifade edilir.

**Tanım 1.3.3.**  $f: A \rightarrow B$  bir fonksiyon olsun.

- (i)  $a \in A$  için  $f(a) = b$  ise  $b$  elemanına  $a$  elemanının  **$f$  altındaki görüntüsü** denir.
- (ii)  $T \subset A$  olmak üzere  $\{f(x) \mid x \in T\}$  kümesine  $T$  kümesinin  **$f$  altındaki görüntüsü** denir ve  $f(T)$  ile gösterilir. Yani  $f(T) = \{f(x) \mid x \in T\}$  olarak tanımlanır. Burada  $f(A)$  kümesine  **$f$  nin görüntü kümesi** denir.
- (iii)  $K \subset B$  olmak üzere  $\{x \mid x \in A \wedge f(x) \in K\}$  kümesine  $K$  kümesinin  **$f$  altındaki ters görüntüsü** denir ve  $f^{-1}(K)$  ile gösterilir. Yani  $f^{-1}(K) = \{x \mid x \in A \wedge f(x) \in K\}$  olarak tanımlanır. Burada eğer  $K = \{b\}$  şeklinde tek elemanlı bir küme ise  $f^{-1}(\{b\})$  yerine genellikle  $f^{-1}(b)$  yazılır. Tanımdan  $f^{-1}(B) = A$  olur. Ancak  $f^{-1}(K) = \emptyset$  olabilir.

**Örnek.**  $A = \{a, b, c, d, e\}$  ve  $B = \{1, 2, x, y, z\}$  olmak üzere  $A$  dan  $B$  ye

$$f = \{(a, z), (b, 1), (c, z), (d, y), (e, 1)\}$$

fonksiyonu verilsin.

- (i)  $T = \{a, b, c\}$  ise  $f(T) = \{1, z\}$  olur.
- (ii)  $K = \{1, z\}$  ise  $f^{-1}(K) = \{a, b, c, e\}$  olur.
- (iii)  $f^{-1}(1) = \{b, e\}$ ,  $f^{-1}(z) = \{a, c\}$  ve  $f^{-1}(y) = \{d\}$  olur.
- (iv)  $f^{-1}(2) = \emptyset$ ,  $f^{-1}(x) = \emptyset$  ve  $f^{-1}(\{2, x\}) = \emptyset$  olur.
- (v)  $f(\{a, b, d\}) = \{1, y, z\}$  ve  $f^{-1}(\{1, y, z\}) = \{a, b, c, d, e\} = A$  olur.
- (vi)  $f^{-1}(\{1, x, y\}) = \{b, d, e\}$  ve  $f(\{b, d, e\}) = \{1, y\}$  olur.
- (vii)  $f$  nin görüntü kümesi  $f(A) = \{1, y, z\}$  olur.

**Örnek.**  $\forall m \in \mathbb{Z}$  için  $f(m) = m^2$  ile tanımlı  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  fonksiyonunun görüntü kümesi  $\{m^2 \mid m \in \mathbb{Z}\}$  tam kare tam sayılar kümesidir. Burada  $f^{-1}(4) = \{-2, 2\}$ ,  $f^{-1}(5) = \emptyset$ ,  $f^{-1}(0) = \{0\}$  ve  $f^{-1}(1) = \{-1, 1\}$  olur.  $f$  nin sıralı ikililer yardımıyla gösterimi  $f = \{(x, x^2) \mid x \in \mathbb{Z}\}$  olur. Bu fonksiyon  $f: \mathbb{Z} \rightarrow \mathbb{Z}, m \rightarrow f(m) = m^2$  şeklinde de ifade edilebilir.

**Tanım 1.3.4.**  $f: A \rightarrow B$  bir fonksiyon ise kartezyen koordinat sisteminde  $A \times B$  nin  $\{(a, f(a)) \mid a \in A\}$  alt kümesine  **$f$  nin grafiği** denir.

**Tanım 1.3.5.**  $f: A \rightarrow A, a \rightarrow f(a) = a$  şeklinde tanımlı fonksiyona **birim fonksiyon** veya  **$A$  nın özdeşlik fonksiyonu** denir ve genellikle  $I_A$  ile gösterilir.

**Örnek.**  $A = \{a, b, c, d\}$  olmak üzere özdeşlik fonksiyonu  $I_A = \{(a, a), (b, b), (c, c), (d, d)\}$  olur.

**Tanım 1.3.6.**  $f: A \rightarrow B$  bir fonksiyon olsun. Eğer  $f, A$  nın elemanlarının her birini  $B$  nin sabit bir elemanına eşliyorsa  $f$  ye bir **sabit fonksiyon** denir.

**Örnek.**  $A = \{a, b, c, d\}$  ve  $B = \{x, y, z\}$  olmak üzere  $f = \{(a, y), (b, y), (c, y), (d, y)\}$ ,  $A$  dan  $B$  ye bir sabit fonksiyondur.

**Tanım 1.3.7.**  $f: A \rightarrow B$  bir fonksiyon olsun. Eğer  $a \neq b$  olan  $\forall a, b \in A$  için  $f(a) \neq f(b)$  oluyorsa  $f$  ye **bire-bir (1-1) fonksiyon** denir. Bir başka deyişle,  $\forall a, b \in A$  için  $f(a) = f(b) \Rightarrow a = b$  oluyorsa  $f$  bire-bir (1-1) fonksiyondur.

**Örnek.**  $A = \{a, b, c, d\}$  ve  $B = \{x, y, z, t, k\}$  olmak üzere  $f = \{(a, y), (b, x), (c, t), (d, k)\}$ ,  $A$  dan  $B$  ye bire-bir fonksiyondur.

**Örnek.**  $f: \mathbb{R} \rightarrow \mathbb{R}, x \rightarrow f(x) = x^3 - 2$  fonksiyonu verilsin.  $a, b \in \mathbb{R}$  olmak üzere

$$f(a) = f(b) \Rightarrow a^3 - 2 = b^3 - 2 \Rightarrow a^3 = b^3 \Rightarrow a = b$$

olduğundan  $f$  fonksiyonu bire-birdir.

**Tanım 1.3.8.**  $f: A \rightarrow B$  bir fonksiyon olsun. Eğer  $f(A) = B$  ise  **$f$  ye örten fonksiyon** denir. Bir başka deyişle, eğer  $\forall b \in B$  için  $f(a) = b$  olacak şekilde  $\exists a \in A$  varsa  **$f$  ye örten fonksiyon** denir.

**Örnek.**  $A = \{a, b, c, d, e\}$  ve  $B = \{x, y, z, t\}$  olmak üzere

$$f = \{(a, z), (b, y), (c, t), (d, x), (e, t)\}$$

$A$  dan  $B$  ye örten bir fonksiyondur. Bu fonksiyon bire-bir değildir.

**Örnek.**  $A = \{a, b, c, d\}$  ve  $B = \{x, y, z, t, k\}$  olmak üzere  $A$  dan  $B$  ye

$$f = \{(a, y), (b, x), (c, t), (d, k)\}$$

fonksiyonu bire-birdir, ancak örten değildir.

**Örnek.**  $A = \{a, b, c, d\}$  ve  $B = \{x, y, z, t\}$  olmak üzere  $f = \{(a, z), (b, y), (c, t), (d, x)\}$ ,  $A$  dan  $B$  ye hem bire-bir, hem de örten bir fonksiyondur.

**Örnek.**  $f: \mathbb{R} \rightarrow \mathbb{R}, x \rightarrow f(x) = x^3 - 2$  fonksiyonunun örten olup olmadığını araştıralım.

**Çözüm:** Herhangi  $b \in \mathbb{R}$  alalım.  $a = \sqrt[3]{b+2}$  diyelim. Burada  $a \in \mathbb{R}$  ve  $f(a) = a^3 - 2 = (\sqrt[3]{b+2})^3 - 2 = b + 2 - 2 = b$  olup  $f$  örtendir.

**Önerme 1.3.9.**  $A$  ve  $B$  boştan farklı iki sonlu küme,  $s(A) = s(B)$  ve  $f: A \rightarrow B$  bir fonksiyon olsun. Bu takdirde  $f$  nin bire-bir olması için gerek ve yeter koşul  $f$  nin örten olmasıdır.

**Önerme 1.3.10.**  $f: A \rightarrow B$  bir fonksiyon olsun. Eger  $f$  hem bire-bir, hem de örten ise  $f^{-1}$  bağıntısı  $B$  den  $A$  ya bir fonksiyondur.

**Önerme 1.3.11.**  $f: A \rightarrow B$  bir fonksiyon olsun. Eğer  $f^{-1}$  bağıntısı  $B$  den  $A$  ya bir fonksiyon ise  $f$  hem bire-bir hem de örten olur.

**Tanım 1.3.12.**  $f: A \rightarrow B$  ve  $g: B \rightarrow C$  iki fonksiyon olsun.  $h: A \rightarrow C, a \rightarrow h(a) = g(f(a))$  şeklinde tanımlı fonksiyona **bileşke fonksiyon** denir (  $g$  ve  $f$  nin bileşkesi) ve  $g \circ f$  ile gösterilir. Buna göre  $g \circ f: A \rightarrow C, a \rightarrow (g \circ f)(a) = g(f(a))$  olarak tanımlanır.

**Tanım 1.3.13.**  $f: A \rightarrow B$  bire-bir ve örten bir fonksiyon olsun.  $f \circ f^{-1} = I_B, f^{-1} \circ f = I_A$  koşulunu gerçekleyen  $f^{-1}: B \rightarrow A$  fonksiyonuna  **$f$  fonksiyonunun ters fonksiyonu** denir. Bu durumda  $f$  ye **terslenebilir fonksiyon** denir.

**Örnek.**  $A = \{a, b, c, d\}, B = \{x, y, z, t\}$  ve  $C = \{1, 2, 3\}$  olmak üzere  $A$  dan  $B$  ye  $f = \{(a, z), (b, x), (c, x), (d, z)\}$  ve  $B$  den  $C$  ye  $g = \{(x, 2), (y, 1), (z, 2), (t, 3)\}$  fonksiyonları verilsin. Burada  $g \circ f = \{(a, 2), (b, 2), (c, 2), (d, 2)\}$  olur.

**Önerme 1.3.14.**  $f: A \rightarrow B, g: B \rightarrow C$  ve  $h: C \rightarrow D$  fonksiyonları verilsin. Bu takdirde  $h \circ (g \circ f) = (h \circ g) \circ f$  olur.

**Önerme 1.3.15.**  $f: A \rightarrow B$  ve  $g: B \rightarrow C$  iki fonksiyon olsun.

- (i) Eğer  $f$  ve  $g$  bire-bir ise  $g \circ f$  de bire-birdir.
- (ii) Eğer  $f$  ve  $g$  örten ise  $g \circ f$  de örtendir.

**Önerme 1.3.16.**  $f: A \rightarrow B$  ve  $g: B \rightarrow C$  iki fonksiyon olsun. Eğer  $f$  ve  $g$  terslenebilir fonksiyonlar ise  $g \circ f$  de terslenebilir bir fonksiyondur ve  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$  olur.

**Önerme 1.3.17.**  $f: A \rightarrow B$  bir fonksiyon olsun. Bu takdirde  $f \circ I_A = I_B \circ f = f$  olur.

**Önerme 1.3.18.**  $f: A \rightarrow B$  bir fonksiyon olsun. Eğer  $f$  hem bire-bir, hem de örten ise (dolayısıyla terslenebilirse)

(i)  $f \circ f^{-1} = I_B$  dir.

(ii)  $f^{-1} \circ f = I_A$  dır.

**İspat.**  $f$  fonksiyonu hem bire-bir, hem de örten olsun. Bu durumda bu fonksiyon terslenebilir olup  $f^{-1}: B \rightarrow A$  bir fonksiyon olur.

(i)  $f^{-1}: B \rightarrow A$  ve  $f: A \rightarrow B$  birer fonksiyon olduğundan  $f \circ f^{-1}: B \rightarrow B$  bir fonksiyon olur. Ayrıca  $I_B: B \rightarrow B$  bir fonksiyondur. Yani  $f \circ f^{-1}$  ve  $I_B$ ,  $B$  den  $B$  ye birer fonksiyon olur. Herhangi  $y \in B$  alalım.  $f^{-1}(y) = x$  diyelim. Burada  $x \in A$  olup  $f(x) = y$  olur.  $f^{-1}(y) = x$  ve  $f(x) = y$  olduğundan

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

olur. O halde  $f \circ f^{-1} = I_B$  olup istenen elde edilir.

(ii)  $f: A \rightarrow B$  ve  $f^{-1}: B \rightarrow A$  birer fonksiyon olduğundan  $f^{-1} \circ f: A \rightarrow A$  bir fonksiyon olur. Ayrıca  $I_A: A \rightarrow A$  bir fonksiyondur. Yani  $f^{-1} \circ f$  ve  $I_A$ ,  $A$  dan  $A$  ya birer fonksiyon olur. Herhangi  $x \in A$  alalım.  $f(x) = y$  diyelim. Burada  $y \in B$  olup  $f^{-1}(y) = x$  olur.  $f(x) = y$  ve  $f^{-1}(y) = x$  olduğundan

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

olur. O halde  $f^{-1} \circ f = I_A$  olup istenen elde edilir.

**Önerme 1.3.19.**  $f: A \rightarrow B$  bir fonksiyon olsun. Eğer  $f \circ g = I_B$  ve  $g \circ f = I_A$  olacak şekilde  $\exists g: B \rightarrow A$  fonksiyonu varsa  $f$  terslenebilirdir ve  $g = f^{-1}$  olur.

**Tanım 1.3.20.**  $f: A \rightarrow B$  bir fonksiyon ve  $\emptyset \neq K \subset A$  olsun.  $g: K \rightarrow B, x \rightarrow g(x) = f(x)$  şeklinde tanımlı  $g$  fonksiyonuna  **$f$  nin  $K$  alt kümesine kısıtlanması (kısıtlanmış)** denir ve  $f|_K$  ile gösterilir.

**Örnek.**  $A = \{a, b, c, d, e\}$  ve  $B = \{x, y, z, t\}$  olmak üzere  $A$  dan  $B$  ye

$$f = \{(a, y), (b, t), (c, x), (d, y), (e, x)\}$$

fonksiyonu verilsin.

- (i)  $K = \{a, b, c\}$  ise  $f|_K = \{(a, y), (b, t), (c, x)\}$  olur. Burada  $f|_K$  bire-bir olduğu halde  $f$  bire-bir değildir.
- (ii)  $T = \{a, d\}$  ise  $f|_T = \{(a, y), (d, y)\}$  olur.

**Tanım 1.3.21.** İki küme arasında en az bir bire-bir ve örten fonksiyon tanımlanabilirse bu iki kümeye **denk** veya **eş güçlü kümeler** denir.

**Önerme 1.3.22.**  $\Omega$  boştan farklı kümelerin boştan farklı bir ailesi olsun.  $\Omega$  da tanımlanan iki küme arasındaki denk (eş güçlü) olma bağıntısı bir denklik bağıntısıdır.

## 1.4. İKİLİ İŞLEMLER

**Tanım 1.4.1.**  $A$  boştan farklı bir küme olsun.  $A \times A$  dan  $A$  ya bir fonksiyona bir **iç** (veya **ikili**) **işlem** veya sadece **işlem** denir. İşlemler genellikle  $*$ ,  $\blacksquare$ ,  $\Delta$ ,  $\circ$ ,  $+$ ,  $\oplus$ , ... gibi sembollerle gösterilir.

**Not.**  $*, A$  kümesinde bir iç işlem olsun.  $a, b \in A$  olmak üzere  $*(a, b)$  yerine genellikle  $a * b$  yazılır.

**Not.**  $*, A$  kümesinde bir iç işlem olsun. Fonksiyon olma özelliklerinden

(i)  $\forall a, b \in A$  için  $A$  da bir  $a * b$  elemanı vardır.

(ii) Bu  $a * b$  elemanı  $a$  ve  $b$  elemanlarına bağlı olarak tek türdür.

Bu özelliklerden birincisine **işlemin kapalılığı**, ikincisine de **iyi tanımlılığ**ı denir.

**Örnek.**  $\mathbb{Z}$  tam sayılar kümesinde bilinen adi toplama  $+$  ve adi çarpma  $\cdot$  işlemleri birer iç işlemdir.

**Örnek.**  $\mathbb{N}$  doğal sayılar kümesinde bilinen adi toplama  $+$  ve adi çarpma  $\cdot$  işlemleri birer iç işlemdir.  $\mathbb{N}$  de bilinen adi çıkarma  $-$  işlemi,  $\mathbb{N}$  de bir iç işlem değildir.

**Tanım 1.4.2.** Üzerinde en az bir işlem tanımlı boştan farklı bir kümeye bu işlemlerle birlikte **cebirsel (matematiksel) yapı** denir.  $A$  kümesi üzerinde bir  $*$  işlemi tanımlı ise bu cebirsel yapı genellikle  $(A, *)$  ile gösterilir.

**Tanım 1.4.3.**  $*, A$  kümesinde bir iç işlem olsun.

- (i) Eğer  $\forall a, b \in A$  için  $a * b = b * a$  ise bu özelliğe **\* işleminin değişme özelliği** denir. Bu durum genellikle **\* işlemi değişmelidir** şeklinde de ifade edilir.
- (ii) Eğer  $\forall a, b, c \in A$  için  $a * (b * c) = (a * b) * c$  ise bu özelliğe **\* işleminin birleşme özelliği** denir ve bu durum genellikle **\* işlemi birleşmelidir** şeklinde de ifade edilir. Bu durumda  $a * (b * c)$  ve  $(a * b) * c$  yerine genellikle  $a * b * c$  yazılır.
- (iii)  $e \in A$  olmak üzere eğer  $\forall a \in A$  için  $a * e = e * a = a$  ise bu  $e$  elemanına  $A$  kümesinin **\* işlemine göre birim (etkisiz) elemanı** denir.
- (iv)  $A$  kümesi  $*$  işlemine göre bir  $e$  birim elemanna sahip olsun.  $a \in A$  olmak üzere  $a * x = x * a = e$  olacak şekilde  $\exists x \in A$  varsa bu  $x$  elemanına  **$a$  elemanının  $*$  işlemine göre tersi** denir. Eğer  $a$  elemanının  $*$  işlemine göre tersi var ve tek ise bu eleman genellikle  $a^{-1}$  ile gösterilir.
- (v)  $y \in A$  olmak üzere eğer  $\forall a \in A$  için  $a * y = y * a = y$  ise bu  $y$  elemanına  $A$  kümesinin **\* işlemine göre yutan elemanı** denir.

**Örnek.**  $0, \mathbb{Z}$  nin  $+$  işlemine göre birim (etkisiz) elemanıdır.  $\mathbb{Z}$  de bir  $a$  elemanının  $+$  işlemine göre tersi  $-a$  olur.  $0, \mathbb{Z}$  nin  $\cdot$  işlemine göre yutan elemanıdır.

**Örnek.**  $A = \{a, b, c, d, e\}$  kümesinde  $*$  işlemi aşağıdaki tablo ile verilsin.

| $*$ | $a$ | $b$ | $c$ | $d$ | $e$ |
|-----|-----|-----|-----|-----|-----|
| $a$ | $d$ | $c$ | $a$ | $e$ | $c$ |
| $b$ | $c$ | $c$ | $b$ | $e$ | $a$ |
| $c$ | $a$ | $b$ | $c$ | $d$ | $e$ |
| $d$ | $b$ | $a$ | $d$ | $e$ | $c$ |
| $e$ | $c$ | $a$ | $e$ | $e$ | $d$ |

Buna göre  $a * (b * d) = a * e = c$  ve  $(a * b) * d = c * d = d$  olup  $*$  işleminin birleşme özelliği yoktur.  $a * d = e$  ve  $d * a = b$  olduğundan  $*$  işleminin değişme özelliği de yoktur.  $c, A$  nın  $*$  işlemine göre birim elemanı olur.  $b$  ve  $e, a$  elemanının  $*$  işlemine göre birer

tersi olduğundan  $a$  ve  $b$ ,  $b$  elemanının  $*$  işlemine göre birer tersi olur. Ancak  $d$  elemanının  $*$  işlemine göre tersi yoktur.

**Örnek.**  $\mathbb{Z}$  tam sayılar kümesinde  $*$  işlemi  $\forall a, b \in \mathbb{Z}$  için  $a * b = a + b + 4$  olarak tanımlansın.  $\mathbb{Z}$  nin bu işleme göre birim elemanı varsa bulunuz.

**Çözüm.**  $\mathbb{Z}$  nin  $*$  işlemine göre birim elemanını  $e$  olsun.  $a \in \mathbb{Z}$  olmak üzere  $a * e = a \Leftrightarrow a + e + 4 = a \Leftrightarrow e = -4$  denklikleri vardır. Ayrıca  $(-4) * a = -4 + a + 4 = a$  olur. O halde  $e = -4$  elemanı  $\mathbb{Z}$  nin  $*$  işlemine göre birim elemanı olur.

**Örnek.**  $\mathbb{Z}$  tam sayılar kümesinde  $*$  işlemi  $\forall a, b \in \mathbb{Z}$  için  $a * b = a + b + ab$  olarak tanımlansın.  $\mathbb{Z}$  nin bu işleme göre birim elemanı varsa bulunuz.

**Çözüm.**  $\mathbb{Z}$  nin  $*$  işlemine göre birim elemanını  $e$  olsun.  $a \in \mathbb{Z}$  olmak üzere  $a * e = a \Leftrightarrow a + e + ae = a \Leftrightarrow e + ae = 0 \Leftrightarrow e(1 + a) = 0$  eşitliğinde  $e = 0$  olarak alınırsa  $e(1 + a) = 0 \cdot (1 + a) = 0$  olduğundan  $a * e = a$  olur. Ayrıca  $0 * a = 0 + a + 0 \cdot a = a$  olur. O halde  $e = 0$  elemanı  $\mathbb{Z}$  nin  $*$  işlemine göre birim elemanı olur.

**Örnek.**  $\mathbb{Z}$  tam sayılar kümesinde  $*$  işlemi  $\forall a, b \in \mathbb{Z}$  için  $a * b = ab^2$  olarak tanımlansın.  $\mathbb{Z}$  nin bu işleme göre birim elemanı yoktur, ancak yutan elemanı vardır. Gösteriniz.

**Tanım 1.4.4.**  $*$  ve  $\circ$ ,  $A$  kümesinde iki iç işlem olsun.

- (i)  $\forall a, b, c \in A$  için  $a * (b \circ c) = (a * b) \circ (a * c)$  ise bu özelliğe  **$*$  işleminin  $\circ$  işlemi üzerine soldan dağılma özelliği vardır** denir.
- (ii)  $\forall a, b, c \in A$  için  $(a \circ b) * c = (a * c) \circ (b * c)$  ise bu özelliğe  **$*$  işleminin  $\circ$  işlemi üzerine sağdan dağılma özelliği vardır** denir.
- (iii) Eğer  $*$  işleminin  $\circ$  işlemi üzerine hem sağdan hem de soldan dağılma özellikleri varsa  **$*$  işleminin  $\circ$  işlemi üzerine dağılma özelliği vardır** denir.

**Örnek.**  $\mathbb{Z}$  de bilinen adi çarpma  $\cdot$  işleminin bilinen adi toplama  $+$  işlemi üzerine dağılma özelliği vardır.

**Önerme 1.4.5.**  $*$ ,  $A$  kümesinde bir iç işlem olsun.  $A$  kümesinde  $*$  işlemine göre birim eleman varsa tektir.

**İspat.**  $e_1$  ve  $e_2$ ,  $A$  nın  $*$  işlemine göre iki birim elemanı olsun.  $e_1 = e_2$  olduğu gösterilirse istenen elde edilir.  $e_1$ ,  $A$  nın  $*$  işlemine göre birim elemanı ve  $e_2 \in A$  olduğundan  $e_2 * e_1 = e_1 *$

$e_2 = e_2$  olur.  $e_2, A$  nın  $*$  işlemine göre birim elemanı ve  $e_1 \in A$  olduğundan  $e_1 * e_2 = e_2 * e_1 = e_1$  olur.  $e_1 * e_2 = e_1$  ve  $e_1 * e_2 = e_2$  olduğundan  $e_1 = e_2$  olup istenen elde edilir.

**Önerme 1.4.6.**  $*, A$  kümesinde birleşme özelliğine sahip bir iç işlem ve  $A$  bu işleme göre bir  $e$  birim elemanına sahip olsun. Bu takdirde

- (i) Bir  $a \in A$  elemanının  $*$  işlemine göre tersi varsa tektir.
- (ii) Bir  $a \in A$  elemanının  $*$  işlemine göre tersi varsa  $a^{-1}$  elemanının da tersi vardır ve  $(a^{-1})^{-1} = a$  olur.
- (iii)  $a, b \in A$  olmak üzere  $a$  ve  $b$  elemanlarının  $*$  işlemine göre tersleri varsa  $a * b$  elemanının da  $*$  işlemine göre tersi vardır ve  $(a * b)^{-1} = b^{-1} * a^{-1}$  olur.

**İspat.** (i)  $a \in A$  elemanının  $*$  işlemine göre tersinin varlığını kabul edelim.  $x$  ve  $y, a$  nın  $A$  da  $*$  işlemine göre iki tersi olsun.  $x = y$  olduğu gösterilirse istenen elde edilir.  $x, a$  nın  $*$  işlemine göre tersi olduğundan  $a * x = x * a = e$  olur.  $y, a$  nın  $*$  işlemine göre tersi olduğundan  $a * y = y * a = e$  olur. Bu durumda  $*$  işleminin  $A$  da birleşme özelliğinden  $x = x * e = x * (a * y) = (x * a) * y = e * y = y$  olup istenen elde edilir.

(ii)  $a \in A$  elemanının  $*$  işlemine göre tersinin varlığını kabul edelim. (i) şikkından  $a$  elemanının  $*$  işlemine göre tersinin tek olduğu anlaşılır.  $x = a^{-1}$  diyelim. Tanımdan  $a * x = x * a = e$  eşitliğinden  $a$  elemanı da  $x$  elemanının  $A$  da  $*$  işlemine göre tersi olur. Burada (i) şikkı da göz önünde bulundurulursa  $a = x^{-1} = (a^{-1})^{-1}$  olup istenen elde edilir.

(iii)  $a$  ve  $b$  elemanlarının  $A$  da  $*$  işlemine göre terslerinin varlığını kabul edelim. (i) şikkından  $a$  elemanının tersini  $a^{-1}, b$  elemanının tersini de  $b^{-1}$  ile gösterebiliriz. Burada  $a^{-1}, b^{-1} \in A$  ve  $*, A$  da bir iç işlem olduğundan  $b^{-1} * a^{-1} \in A$  olur. Tanımdan  $a * a^{-1} = a^{-1} * a = e$  ve  $b * b^{-1} = b^{-1} * b = e$  olur. Bu durumda  $*$  işleminin  $A$  da birleşme özelliğinden

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

ve

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

olup  $a * b$  elemanının da  $A$  da  $*$  işlemine göre tersi vardır ve (i) şikkından  $(a * b)^{-1} = b^{-1} * a^{-1}$  bulunur.

### 1.5. TAM SAYILARDA BÖLÜNEBİLME

**Tanım 1.5.1.**  $a, b \in \mathbb{Z}$  olsun. Eğer  $b = ac$  olacak şekilde  $\exists c \in \mathbb{Z}$  varsa  **$a$  sayısı  $b$  sayısını böler** denir ve  $a \mid b$  ile ifade edilir. Eğer  $a \mid b$  ise " $a, b$  nin bir bölenidir" veya " $a, b$  nin bir çarpanıdır" ya da " $b, a$  nın bir katıdır" da denir ve  $\frac{b}{a} = c$  olur.

**Not.** Tanımdan  $0 \mid 0$  olduğu anlaşılır.

Tam sayılarda bölünebilmenin özelliklerini aşağıdaki teoremle verebiliriz.

**Teorem 1.5.2.** Bölünebilme ile ilgili aşağıdaki özellikler vardır.

- (i)  $\forall a \in \mathbb{Z}$  için  $1 \mid a, a \mid a$  ve  $a \mid 0$  olur.
- (ii) Sıfır sadece sıfırı böler.
- (iii)  $a \mid b$  ise  $\forall k \in \mathbb{Z}$  için  $a \mid bk$  olur.
- (iv)  $a \mid b$  ve  $b \mid c$  ise  $a \mid c$  olur.
- (v)  $a \mid b$  ve  $a \mid c$  ise  $\forall x, y \in \mathbb{Z}$  için  $a \mid bx + cy$  olur.
- (vi)  $a \mid b$  ve  $b \neq 0$  ise  $|a| \leq |b|$  olur. Burada eğer  $|a| \neq |b|$  ise  $|a| < |b|$  olur.
- (vii)  $a \mid b$  ve  $b \mid a$  ise  $a = \pm b$  olur.
- (viii)  $a \mid b$  ise  $-a \mid b, a \mid -b$  ve  $-a \mid -b$  olur.
- (ix)  $-a \mid b, a \mid -b$  ve  $-a \mid -b$  koşullarından biri sağlanırsa  $a \mid b$  de sağlanır.
- (x)  $a \mid b$  ve  $c \mid d$  ise  $ac \mid bd$  olur.
- (xi)  $a \mid b$  ise  $\forall k \in \mathbb{Z}$  için  $ak \mid bk$  olur.
- (xii)  $a, b, k \in \mathbb{Z}$  ve  $k \neq 0$  olmak üzere  $ak \mid bk$  ise  $a \mid b$  olur.

**İspat.** (i)  $\forall a \in \mathbb{Z}$  için  $a = 1a = a1$  olduğundan tanımdan  $1 \mid a$  ve  $a \mid a$  olur.  $\forall a \in \mathbb{Z}$  için  $0 = a0$  olduğundan tanımdan  $a \mid 0$  olur.

(ii)  $0 = 0 \cdot 0$  olduğundan tanımdan  $0 \mid 0$  olur.  $0 \mid a$  olan herhangi  $a \in \mathbb{Z}$  alalım.  $0 \mid a$  olduğundan tanımdan  $a = 0c$  olacak şekilde  $\exists c \in \mathbb{Z}$  vardır. Burada  $a = 0c = 0$  olur. Yani sıfır sadece sıfırı böler.

(iii)  $a \mid b$  olsun. Bu durumda tanımdan  $b = ac$  olacak şekilde  $\exists c \in \mathbb{Z}$  vardır. Herhangi  $k \in \mathbb{Z}$  alalım.  $b = ac$  olduğundan  $bk = ack$  olup burada  $ck \in \mathbb{Z}$  olduğundan tanımdan  $a \mid bk$  olur.

(iv)  $a \mid b$  ve  $b \mid c$  olsun. Bu durumda tanımdan  $b = ac_1$  ve  $c = bc_2$  olacak şekilde  $\exists c_1, c_2 \in \mathbb{Z}$  vardır. Burada  $c = bc_2 = ac_1c_2$  olup  $c_1c_2 \in \mathbb{Z}$  olduğundan tanımdan  $a \mid c$  olur.

(v)  $a \mid b$  ve  $a \mid c$  olsun. Bu durumda tanımdan  $b = ac_1$  ve  $c = ac_2$  olacak şekilde  $\exists c_1, c_2 \in \mathbb{Z}$  vardır. Herhangi  $x, y \in \mathbb{Z}$  alalım. Burada  $bx + cy = ac_1x + ac_2y = a(c_1x + c_2y)$  olup  $c_1x + c_2y \in \mathbb{Z}$  olduğundan tanımdan  $a \mid bx + cy$  olur.

(vi)  $a \mid b$  ve  $b \neq 0$  olsun.  $a \mid b$  olduğundan tanımdan  $b = ac$  olacak şekilde  $\exists c \in \mathbb{Z}$  vardır.  $b = ac$  ve  $b \neq 0$  olduğundan  $a \neq 0$  ve  $c \neq 0$  olur. Bu durumda  $\frac{b}{a} = c$  olup  $\left| \frac{b}{a} \right| = |c|$  olur. Burada  $c \neq 0$  olduğundan  $|c| > 0$  olup  $|c| \in \mathbb{Z}^+$  olduğundan  $|c| \geq 1$  olur. O halde  $1 \leq |c| = \left| \frac{b}{a} \right| = \frac{|b|}{|a|}$  olup  $|a| \geq 0$  olduğundan  $|a| \leq |b|$  olur. Burada eğer  $|a| \neq |b|$  ise  $|a| < |b|$  olup istenen elde edilir.

(vii)  $a \mid b$  ve  $b \mid a$  olsun. Eğer  $b = 0$  ise  $b \mid a$  olduğundan (ii) şikkından  $a = 0 = \pm 0 = \pm b$  olup istenen elde edilir. Kabul edelim ki  $b \neq 0$  olsun.  $a \mid b$  ve  $b \mid a$  olduğundan tanımdan  $b = ac_1$  ve  $a = bc_2$  olacak şekilde  $\exists c_1, c_2 \in \mathbb{Z}$  vardır. Burada  $b = ac_1 = bc_2c_1$  olup  $b \neq 0$  olduğundan  $1 = c_2c_1$  olur.  $1 = c_2c_1$  ve  $c_1 \in \mathbb{Z}$  olduğundan tanımdan  $c_2 \mid 1$  olup 1 in bölenleri sadece 1 ve -1 olduğundan  $c_2 = \pm 1$  olur. O halde  $a = bc_2 = \pm b$  olup istenen elde edilir.

(viii)  $a \mid b$  olsun. Bu durumda tanımdan  $b = ac$  olacak şekilde  $\exists c \in \mathbb{Z}$  vardır.  $b = ac = (-a)(-c)$  ve  $-c \in \mathbb{Z}$  olduğundan tanımdan  $-a \mid b$  olur. Yine  $b = ac$  olduğundan  $-b = (-a)c = a(-c)$  olup  $-c, c \in \mathbb{Z}$  olduğundan tanımdan  $a \mid -b$  ve  $-a \mid -b$  olur.

(ix)  $-a \mid b$  ise (viii) şikkından  $-(-a) \mid b$  olup  $a \mid b$  olur.  $a \mid -b$  ise (viii) şikkından  $a \mid -(-b)$  olup  $a \mid b$  olur.  $-a \mid -b$  ise (viii) şikkından  $-(-a) \mid -(-b)$  olup yine  $a \mid b$  olur.

(x)  $a \mid b$  ve  $c \mid d$  olsun. Bu durumda tanımdan  $b = ac_1$  ve  $d = cc_2$  olacak şekilde  $\exists c_1, c_2 \in \mathbb{Z}$  vardır.  $b = ac_1$  ve  $d = cc_2$  olduğundan  $bd = ac_1cc_2 = acc_1c_2$  olup  $c_1c_2 \in \mathbb{Z}$  olduğundan tanımdan  $ac \mid bd$  olur.

(xi)  $a \mid b$  olsun. Bu durumda tanımdan  $b = ac$  olacak şekilde  $\exists c \in \mathbb{Z}$  vardır.  $b = ac$  olduğundan  $\forall k \in \mathbb{Z}$  için  $bk = akc$  olup  $c \in \mathbb{Z}$  olduğundan tanımdan  $ak \mid bk$  bulunur.

(xii)  $a, b, k \in \mathbb{Z}$  ve  $k \neq 0$  olmak üzere  $ak \mid bk$  olsun. Bu durumda tanımdan  $bk = akc$  olacak şekilde  $\exists c \in \mathbb{Z}$  vardır.  $bk = akc$  ve  $k \neq 0$  olduğundan  $b = ac$  olup  $c \in \mathbb{Z}$  olduğundan tanımdan  $a \mid b$  olur.

**Tanım 1.5.3.**  $a, b \in \mathbb{Z}$  için  $a \mid b$  ve  $b \mid a$  ise  **$a$  ile  $b$  sayılarına ilgilidir** denir ve  $a \approx b$  ile ifade edilir.

**Not.** Teorem 1.5.2 (vii) den  $a \approx b \Leftrightarrow a = \pm b$  olduğu anlaşılır.

**Tanım 1.5.4.** Pozitif bölenleri sadece 1 ve kendisi olan 1'den büyük tam sayılara asal tam sayılar denir.

**Teorem 1.5.5.** 1 den büyük her tam sayının en az bir asal böleni vardır.

**İspat.**  $a$  birden büyük herhangi bir tam sayı olsun.  $a$  nin en az bir asal böleninin varlığı gösterilirse istenen elde edilir.  $A = \{k \in \mathbb{Z} \mid k > 1 \text{ ve } k \mid a\}$  kümesini tanımlayalım.  $a > 1$  ve  $a \mid a$  olduğundan  $a \in A$  olup  $A \neq \emptyset$  olur. Ayrıca  $A \subset \mathbb{Z}^+$  olduğu da açıktır. Pozitif tam sayılar kümesi iyi sıralı küme olduğundan  $A$  kümesi bir en küçük  $t$  elemanına sahiptir.  $t \in A$  olduğundan  $t > 1$  ve  $t \mid a$  olur. Kabul edelim ki  $t$  asal olmasın. Bu durumda  $t$  nin 1 ve kendisinden farklı en az bir  $c$  pozitif böleni vardır.  $c \mid t$  ve  $t \neq 0$  olduğundan Teorem 1.5.2. (vi) den  $|c| \leq |t|$  olup burada  $c, t \in \mathbb{Z}^+$  olduğundan  $c = |c| \leq |t| = t$  olur.  $c \leq t$  ve  $c \neq t$  olduğundan  $c < t$  olup ayrıca  $c > 1$  olduğundan  $1 < c < t$  olur.  $c \mid t$  ve  $t \mid a$  olduğundan Teorem 1.5.2. (iv) den  $c \mid a$  olup ayrıca  $c > 1$  olduğundan  $c \in A$  olur. Bu ise  $t$  sayısının  $A$  nin en küçük elemanı olmasıyla çelişir. O halde kabulümüz yanlış olup  $t$  asal olur.  $t$  asal ve  $t \mid a$  olduğundan  $a$  sayısının en az bir asal böleni vardır.

**Teorem 1.5.6. (Euclid)** Sonsuz sayıda asal sayı vardır.

**İspat.** İspatı olmayana ergi yöntemi ile yapalım. Kabul edelim ki asal sayılar kümesi  $IP = \{p_1, p_2, p_3, \dots, p_n\}$  sonlu olsun.  $a = p_1 p_2 \dots p_n + 1$  diyelim.  $1 \leq i \leq n$  için  $p_i$  asal olduğundan  $p_i > 1$  olup  $a = p_1 p_2 \dots p_n + 1 > 1$  olur. Bu durumda Teorem 1.5.5 den  $a$  sayısının en az bir  $p$  asal böleni vardır. Burada tüm asal sayıları  $p_1, p_2, \dots, p_n$  olarak kabul ettiğimizden  $p = p_i$  olacak şekilde  $\exists i = 1, 2, \dots, n$  vardır.  $p \mid a$  ve  $p = p_i \mid p_1 p_2 \dots p_n$  olduğundan Teorem 1.5.2.

(v) den  $p \mid a - p_1 p_2 \dots p_n = 1$  olur ki bu da  $p$  nin asal olmasıyla çelişir. O halde kabulümüz yanlış olup asal sayıların kümesi sonlu değildir.

**Teorem 1.5.7.** 1 den büyük her tam sayı sonlu sayıda birtakım asal sayıların çarpımı olarak yazılabilir.

**İspat.** Aksini kabul edelim. Yani sonlu sayıda birtakım asal sayıların çarpımı olarak yazılamayan birden büyük en az bir tam sayının varlığını kabul edelim. Böyle tam sayıların kümesini  $A$  ile gösterelim. Kabulümüzden  $A \neq \emptyset$  olur. Ayrıca  $A \subset \mathbb{Z}^+$  olduğu da açıktır. Pozitif tam sayılar kümesi iyi sıralı küme olduğundan  $A$  kümesi bir en küçük  $t$  elemanına sahiptir.  $t \in A$  olduğundan  $t > 1$  ve  $t$  sayısı sonlu sayıda birtakım asal sayıların çarpımı olarak yazılamaz.  $t > 1$  olduğundan Teorem 1.5.5 gereği  $t$  nin en az bir  $p$  asal böleni vardır.  $p \mid t$  olduğundan tanımdan  $t = pc$  olacak şekilde  $\exists c \in \mathbb{Z}$  vardır. Burada  $t > 0$  ve  $p > 0$  olduğundan  $c > 0$  olur. Ayrıca  $p > 1$  olduğundan  $t = pc > c$  olur.  $t = pc, p$  asal ve  $t$  sonlu sayıda birtakım asal sayıların çarpımı olarak yazılamadığından  $t \neq p$  olup  $c \neq 1$  olur. O halde  $1 < c < t$  olur.  $t = pc, p$  asal ve  $t$  sonlu sayıda birtakım asal sayıların çarpımı olarak yazılamadığından  $c$  de sonlu sayıda birtakım asal sayıların çarpımı olarak yazılamaz. Bu durumda  $c \in A$  olur ki bu da  $t$  sayısının  $A$  nın en küçük elemanı olmasıyla çelişir. O halde kabulümüz yanlış olup birden büyük her tam sayı sonlu sayıda birtakım asal sayıların çarpımı olarak yazılabilir.

**Teorem 1.5.8.** Pozitif  $m$  ve  $n$  tam sayıları verildiğinde  $n = qm + r$  ve  $0 \leq r < m$  olacak şekilde tek türlü  $q$  ve  $r$  tam sayıları bulunabilir.

**İspat.** Önce  $q$  ve  $r$  tam sayılarının varlığını gösterelim. Bunun için  $n$  üzerine tümevarım prensibini uygulayalım.  $n = 1$  olsun. Eğer  $m = 1$  ise  $q = 1$  ve  $r = 0$  olarak alınırsa  $n = 1 = 1 \cdot 1 + 0 = qm + r$  ve  $0 \leq r < m$  olur. Eğer  $m > 1$  ise  $q = 0$  ve  $r = 1$  olarak alınırsa  $n = 1 = 0 \cdot m + 1 = qm + r$  ve  $0 \leq r < m$  olur. Böylece  $n = 1$  için iddia doğru olur.

Şimdi  $k \in \mathbb{Z}^+ - \{1\}$  olmak üzere iddianın  $n < k$  olan her  $n \in \mathbb{Z}^+$  için doğruluğunu kabul edelim. İddianın  $n = k$  doğruluğu gösterilirse istenen elde edilir. Eğer  $m > k$  ise  $q = 0$  ve  $r = k$  olarak alınırsa  $k = 0 \cdot m + k = qm + r$  ve  $0 \leq r < m$  olur. Eğer  $m = k$  ise  $q = 1$  ve  $r = 0$  olarak alınırsa  $k = 1 \cdot k + 0 = qm + r$  ve  $0 \leq r < m$  olur. Kabul edelim ki  $m < k$  olsun. Bu durumda  $0 < k - m < k$  olup iddia  $n < k$  olan her  $n \in \mathbb{Z}^+$  için doğru olduğundan  $k - m = q_1 m + r_1$  ve  $0 \leq r_1 < m$  olacak şekilde  $\exists q_1, r_1 \in \mathbb{Z}$  vardır.  $k - m = q_1 m + r_1$  olduğundan  $k = q_1 m + r_1 + m = (q_1 + 1)m + r_1$  olup burada  $q = q_1 + 1$  ve  $r = r_1$  dersek  $q, r \in \mathbb{Z}$ ,

$k = (q_1 + 1)m + r_1 = qm + r$  ve  $0 \leq r < m$  olur. Böylece iddia  $n = k$  için doğru olup istenen elde edilir.

Şimdi  $q$  ve  $r$  tam sayılarının tekliğini gösterelim.  $n = q_1m + r_1 = q_2m + r_2$  ve  $0 \leq r_1, r_2 < m$  olan herhangi  $q_1, q_2, r_1, r_2 \in \mathbb{Z}$  alalım.  $q_1 = q_2$  ve  $r_1 = r_2$  olduğu gösterilirse istenen elde edilir.  $q_1m + r_1 = q_2m + r_2$  olduğundan  $r_1 - r_2 = m(q_2 - q_1)$  olup tanımdan  $m \mid r_1 - r_2$  olur.  $0 \leq r_1, r_2 < m$  olduğundan  $|r_1 - r_2| < m$  olur. Burada eğer  $r_1 - r_2 \neq 0$  olsa  $m \mid r_1 - r_2$  olduğundan Teorem 1.5.2 (vi) den  $m = |m| \leq |r_1 - r_2|$  olur ki bu da  $|r_1 - r_2| < m$  olmasıyla çelişir. O halde  $r_1 - r_2 = 0$  olup  $r_1 = r_2$  olur.  $r_1 = r_2$  ve  $q_1m + r_1 = q_2m + r_2$  olduğundan  $q_1m = q_2m$  olup burada  $m \neq 0$  olduğundan  $q_1 = q_2$  olur. Yani  $q_1 = q_2$  ve  $r_1 = r_2$  olup istenen elde edilir.

**2. Yol:** Eğer  $m > n$  ise  $q = 0$  ve  $r = n$  olarak alınırsa  $n = 0m + n = qm + r$  ve  $0 \leq r < m$  olur. Kabul edelim ki  $m \leq n$  olsun. Bu durumda  $n - m \geq 0$  olur.  $A = \{n - km \mid k \in \mathbb{Z} \text{ ve } n - km \geq 0\}$  kümesini tanımlayalım.  $n - m \geq 0$  olduğundan  $A$  nın tanımından  $n - m = n - 1m \in A$  olup  $A \neq \emptyset$  olur. Ayrıca  $A \subset \mathbb{Z}^+$  olduğu da açıktır. Pozitif tam sayılar kümesi iyi sıralı küme olduğundan  $A$  kümesi bir en küçük  $r$  elemanına sahiptir.  $r \in A$  olduğundan  $r \geq 0$  olur ve  $r = n - qm$  olacak şekilde  $\exists q \in \mathbb{Z}$  vardır.  $r = n - qm$  olduğundan  $n = qm + r$  olur. Eğer burada  $r \geq m$  olsa  $0 \leq r - m < r$  olup ayrıca

$$r - m = n - qm - m = n - (q + 1)m$$

ve  $q + 1 \in \mathbb{Z}$  olduğundan  $A$  nın tanımından  $r - m \in A$  olur ki bu da  $r$  sayısının  $A$  nın en küçük elemanı olmasıyla çelişir. O halde  $r < m$  olup ayrıca  $r \geq 0$  olduğundan  $0 \leq r < m$  olur. Yani  $n = qm + r$  ve  $0 \leq r < m$  olacak şekilde  $\exists q, r \in \mathbb{Z}$  vardır.

**Sonuç 1.5.9.**  $m \neq 0$  olmak üzere her  $m, n$  tam sayısı için  $n = qm + r$  ve  $0 \leq r < |m|$  olacak şekilde teklikle belirli  $q$  ve  $r$  tam sayıları vardır.

**Tanım 1.5.10.**  $m, n \in \mathbb{Z}$  ve  $m \neq 0$  olsun.  $n$  nin  $n = qm + r, q, r \in \mathbb{Z}, 0 \leq r < |m|$  şeklinde yazılışında  $r$  ye  $n$  nin  $m$  ile bölümünden **kalan**,  $q$  ya ise **bölüm** denir. Burada  $q$  ve  $r$  yi bulma işlemine de  $n$  yi  $m$  ile **kalanlı bölme işlemi** denir.

**Tanım 1.5.11.**  $m$  ve  $n$  sıfırdan farklı iki tam sayı olsun.

- (i)  $d \mid m$  ve  $d \mid n$  olacak şekilde  $d > 0$  tam sayısı varsa  $d$  ye  $m$  ve  $n$  nin bir **ortak böleni** denir.
- (ii)  $d, m$  ve  $n$  nin bir ortak böleni olsun. Eğer  $m$  ile  $n$  nin her ortak  $e$  böleni için  $e \mid d$  ise  $d$  ye

$m$  ve  $n$  nin **en büyük ortak böleni (EBOB)** denir.  $m$  ve  $n$  nin en büyük ortak böleni genellikle  $\text{EBOB}(m, n)$ ,  $\text{OBEB}(m, n)$  veya sadece  $(m, n)$  ile gösterilir.

**Not:** İki tam sayı verildiğinde en büyük ortak bölenleri ilgililik hariç tektir.

**Teorem 1.5.12.** Sıfırdan farklı herhangi iki sayının en büyük ortak böleni vardır ve  $d = (m, n)$  ise  $d = mx + ny$  olacak şekilde  $\exists x, y \in \mathbb{Z}$  vardır.

**İspat.**  $A = \{mx + ny \mid x, y \in \mathbb{Z} \text{ ve } mx + ny > 0\}$  kümesini tanımlayalım.  $m$  ve  $n$  nin tam sayıları için  $m^2 + n^2 > 0$  olup  $x = m$  ve  $y = n$  alınırsa  $A$  nın tanımından  $m^2 + n^2 = mx + ny \in A$  olur. O halde  $A \neq \emptyset$  olup ayrıca  $A \subset \mathbb{Z}^+$  olduğundan pozitif tam sayıların iyi sıralı küme olduğu göz önüne alınırsa  $A$  kümesi bir en küçük  $t$  elemanına sahiptir.  $t \in A$  olduğundan  $t > 0$  olur ve  $t = mx + ny$  olacak şekilde  $\exists x, y \in \mathbb{Z}$  vardır. Şimdi  $d = t$  olduğu gösterilirse istenen elde edilir.  $d = (m, n)$  olduğundan  $d > 0, d \mid m$  ve  $d \mid n$  olur.  $d \mid m$  ve  $d \mid n$  olduğundan Teorem 1.5.2 (v) den  $d \mid mx + ny = t$  olup burada  $d > 0$  ve  $t > 0$  olduğundan  $d \leq t$  olur.  $m$  ile  $t$  ye kalanlı bölme uygulanırsa  $m = qt + r$  ve  $0 \leq r < t$  olacak şekilde  $\exists q, r \in \mathbb{Z}$  vardır.  $m = qt + r$  ve  $t = mx + ny$  eşitliklerinden

$$r = m - qt = m - q(mx + ny) = m(1 - qx) + n(-qy)$$

olur. Eğer burada  $r \neq 0$  olsa  $0 < r < t$  olup  $r = m(1 - qx) + n(-qy)$  ve  $1 - qx, -qy \in \mathbb{Z}$  olduğundan  $A$  nın tanımından  $r \in A$  olur ki bu da  $t$  sayısının  $A$  nın en küçük elemanı olmasıyla çelişir. O halde  $r = 0$  olup  $m = qt + r = qt$  ve  $t \mid m$  olur. Benzer şekilde  $t \mid n$  olduğu da gösterilebilir.  $t \mid m, t \mid n$  ve  $d = (m, n)$  olduğundan  $t \leq d$  olup ayrıca  $d \leq t$  olduğundan  $d = t$  olur.

**Sonuç 1.5.13.**  $m_1, m_2, \dots, m_k$  en az biri sıfırdan farklı tam sayılar olmak üzere  $d = (m_1, m_2, \dots, m_k)$  ise  $d = m_1x_1 + m_2x_2 + \dots + m_kx_k$  olacak şekilde  $\exists x_1, x_2, \dots, x_k \in \mathbb{Z}$  vardır.

**Sonuç 1.5.14.**  $m$  ve  $n$  nin her ortak böleni  $(m, n)$  yi de böler.

**İspat.**  $d = (m, n)$  diyelim. Bu durumda Teorem 1.5.12 den  $d = mx + ny$  olacak şekilde  $\exists x, y \in \mathbb{Z}$  vardır.  $m$  ve  $n$  nin herhangi  $t$  ortak bölenini alalım.  $t \mid m$  ve  $t \mid n$  olduğundan Teorem 1.5.2 (v) den  $t \mid mx + ny = d = (m, n)$  olur. Yani  $m$  ve  $n$  nin her ortak böleni  $(m, n)$  yi de böler.

**Tanım 1.5.15.** İki tam sayının en büyük ortak böleni 1 ise bu iki sayıya **aralarında asal sayılar** denir.

**Önerme 1.5.16.**  $(m, n) = 1$  olması için gerek ve yeter koşul  $mx + ny = 1$  olacak şekilde  $\exists x, y \in \mathbb{Z}$  tam sayılarının mevcut olmasıdır.

**İspat.**  $(\Rightarrow)$   $(m, n) = 1$  olsun. Bu durumda Teorem 1.5.12 den  $mx + ny = 1$  olacak şekilde  $\exists x, y \in \mathbb{Z}$  vardır. O halde istenen elde edilir.

$(\Leftarrow)$   $mx + ny = 1$  olacak şekilde  $x, y \in \mathbb{Z}$  tam sayıları bulunsun.  $d = (m, n)$  diyelim.  $d = (m, n)$  olduğundan  $d > 0, d \mid m$  ve  $d \mid n$  olur.  $d \mid m$  ve  $d \mid n$  olduğundan Teorem 1.5.2 (v) den  $d \mid mx + ny = 1$  olup 1 in pozitif böleni sadece kendisi olduğundan  $d = 1$  olur. O halde  $(m, n) = 1$  olup istenen elde edilir.

**Sonuç 1.5.17.**  $(m, n) = d$  olsun. Bu durumda  $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$  olur.

**İspat.**  $(m, n) = d$  olduğundan Teorem 1.5.12 den  $d = mx + ny$  olacak şekilde  $\exists x, y \in \mathbb{Z}$  vardır.  $d = mx + ny$  olduğundan  $\frac{m}{d}x + \frac{n}{d}y = 1$  olup Önerme 1.5.16 dan  $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$  olur ki bu da istenendir.

**Önerme 1.5.18.**  $(m, n) = d$  olsun. Bu takdirde  $\forall k \in \mathbb{Z}^+$  için  $(mk, nk) = dk$  olur.

**İspat.** Herhangi  $k \in \mathbb{Z}^+$  alalım.  $(mk, nk) = dk$  olduğu gösterilirse istenen elde edilir.  $(mk, nk) = t$  olsun.  $(m, n) = d$  olduğundan  $d > 0, d \mid m$  ve  $d \mid n$  olur.  $d \mid m$  ve  $d \mid n$  olduğundan Teorem 1.5.2 (xi) den  $dk \mid mk$  ve  $dk \mid nk$  olup  $(mk, nk) = t$  olduğundan  $dk \leq t$  olur.  $(m, n) = d$  olduğundan Teorem 1.5.12 den  $d = mx + ny$  olacak şekilde  $\exists x, y \in \mathbb{Z}$  vardır.  $d = mx + ny$  olduğundan  $dk = mkx + nky$  eşitliği elde edilir.  $(mk, nk) = t$  olduğundan  $t > 0, t \mid mk$  ve  $t \mid nk$  olur.  $t \mid mk$  ve  $t \mid nk$  olduğundan Teorem 1.5.2 (v) den  $t \mid mkx + nky = dk$  olup burada  $t > 0$  ve  $dk > 0$  olduğundan  $t \leq dk$  bulunur. Ayrıca  $dk \leq t$  olduğundan  $t = dk$  olup  $(mk, nk) = dk$  olur.

**Önerme 1.5.19.**  $k \in \mathbb{Z}^+$  olmak üzere  $(m, n) = d$  olması için gerek ve yeter koşul  $(mk, nk) = dk$  olmasıdır.

**İspat.**  $(\Rightarrow)$   $k \in \mathbb{Z}^+$  olmak üzere  $(m, n) = d$  olsun. Bu durumda Önerme 1.5.18 den  $(mk, nk) = dk$  olup istenen elde edilir.

$(\Leftarrow) k \in \mathbb{Z}^+$  olmak üzere  $(mk, nk) = dk$  olsun.  $(m, n) = t$  diyelim.  $(m, n) = t$  ve  $k \in \mathbb{Z}^+$  olduğundan Önerme 1.5.18 den  $(mk, nk) = tk$  olup ayrıca  $(mk, nk) = dk$  olduğundan  $tk = dk$  olur. O halde  $k \in \mathbb{Z}^+$  olduğundan  $t = d$  olup  $(m, n) = d$  olur.

**Önerme 1.5.20.**  $p$  asal sayı ve  $a \in \mathbb{Z}$  olsun.  $(a, p) = 1$  olması için gerek ve yeter koşul  $p \nmid a$  olmasıdır.

**İspat.**  $(\Rightarrow) (a, p) = 1$  olsun. Eğer  $p \mid a$  ise ayrıca  $p \mid p$  ve  $(a, p) = 1$  olduğundan  $p \leq 1$  olur ki bu da  $p$  nin bir asal sayı olmasıyla çelişir. O halde  $p \nmid a$  olup istenen elde edilir.

$(\Leftarrow) p \nmid a$  olsun.  $(a, p) = d$  diyelim.  $(a, p) = d$  olduğundan  $d > 0, d \mid a$  ve  $d \mid p$  olur.  $d > 0, d \mid p$  ve  $p$  asal sayı olduğundan  $d = 1$  veya  $d = p$  olur.  $d \mid a$  ve  $p \nmid a$  olduğundan  $d \neq p$  olup  $d = 1$  olur. O halde  $(a, p) = 1$  olup istenen elde edilir.

**Önerme 1.5.21.**  $m$  ve  $a$  sıfırdan farklı iki tam sayı ve  $b$  herhangi bir tam sayı olsun.  $m \mid ab$  ve  $(m, a) = 1$  ise  $m \mid b$  olur.

**İspat.**  $m \mid ab$  ve  $(m, a) = 1$  olsun.  $(m, a) = 1$  olduğundan Teorem 1.5.12 den  $mx + ay = 1$  olacak şekilde  $\exists x, y \in \mathbb{Z}$  vardır.  $mx + ay = 1$  olduğundan  $mbx + aby = b$  olur.  $m \mid m$  ve  $m \mid ab$  olduğundan Teorem 1.5.2 (v) den  $m \mid mbx + aby = b$  olup istenen elde edilir.

**Sonuç 1.5.22.**  $p$  asal sayı ve  $p \mid mn$  ise  $p \mid m$  veya  $p \mid n$  olur.

**Sonuç 1.5.23.**  $p$  asal sayı ve  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  olsun.  $p \mid a_1 a_2 \dots a_n$  ise  $\exists i = 1, 2, \dots, n$  için  $p \mid a_i$  olur.

**Teorem 1.5.24. (Aritmetiğin Temel Teoremi)** Birden büyük her tam sayının asal çarpanlara ayrılışı sıra düşünölmeksizin tek türölüdür.

**İspat.**  $a$  birden büyük herhangi bir tam sayı ve  $p_1, p_2, \dots, p_m, q_1, q_2, \dots, q_n$  asal sayılar olmak üzere  $a = p_1 p_2 \dots p_m$  ve  $a = q_1 q_2 \dots q_n$  olsun.  $m = n$  ve  $p_1, p_2, \dots, p_m$  asal sayıları ile  $q_1, q_2, \dots, q_n$  asal sayılarının aynı olduđu gösterilirse istenen elde edilir.  $a = p_1 p_2 \dots p_m$  ve  $a = q_1 q_2 \dots q_n$  olduğundan  $p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$  olup  $p_1 \mid q_1 q_2 \dots q_n$  olur.  $p_1 \mid q_1 q_2 \dots q_n$  ve  $p_1$  asal sayı olduğundan  $\exists j = 1, 2, \dots, n$  için  $p_1 \mid q_j$  olur. Bu durumda  $p_1$  ve  $q_j$  asal sayılar olduklarından  $p_1 = q_j$  eşitliğı elde edilir. Burada sıra düşünölmediğinden  $p_1 = q_1$  kabul edilebilir.  $p_1 = q_1$  ve  $p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$  olduğundan  $p_2 p_3 \dots p_m = q_2 q_3 \dots q_n$  olup  $p_2 \mid q_2 q_3 \dots q_n$  olur.  $p_2 \mid q_2 q_3 \dots q_n$  ve  $p_2$  asal sayı olduğundan  $\exists j = 2, 3, \dots, n$  için  $p_2 \mid q_j$  olur. Bu

durumda  $p_2$  ve  $q_j$  asal sayılar olduklarından  $p_2 = q_j$  olur. Burada sıra düşünülmediğinden  $p_2 = q_2$  kabul edilebilir. Böyle devam edilirse  $m \leq n$  ve  $p_1, p_2, \dots, p_m$  asal sayılarının  $q_1, q_2, \dots, q_n$  asal sayıları içinde olduğu gösterilebilir. Benzer şekilde  $p_i$  ve  $q_j$  asal sayılarının rolleri değiştirilerek  $n \leq m$  ve  $q_1, q_2, \dots, q_n$  asal sayılarının  $p_1, p_2, \dots, p_m$  asal sayılarından farklı olduğu gösterilebilir. O halde  $m = n$  ve  $p_1, p_2, \dots, p_m$  asal sayıları ile  $q_1, q_2, \dots, q_n$  asal sayıları aynı olup istenen elde edilir.

**Sonuç 1.5.25.** Sıfırdan farklı her  $a$  tam sayısı  $a = (\pm 1)p_1 p_2 \dots p_n$  şeklinde farklı olmaları gerekmeyen birtakım asal sayıların ( $n = 0$  olabilir) çarpımı şeklinde yazılabilir ve bu yazılış sıra düşünülmezsizin tek türüdür. Burada aynı asal sayıların çarpımı üslü şekilde yazılırsa  $a = (\pm 1)p_1 p_2 \dots p_n$  tam sayısı

$$a = (\pm 1)p_{i_1}^{m_{i_1}} p_{i_2}^{m_{i_2}} \dots p_{i_k}^{m_{i_k}} (p_{i_1}, p_{i_2}, \dots, p_{i_k} \text{ farklı asal sayılar } i_1, i_2, \dots, i_k \in \mathbb{Z}^+)$$

biçiminde de ifade edilebilir.

**Önerme 1.5.26.**  $(a, mn) = 1$  olması için gerek ve yeter koşul  $(a, m) = (a, n) = 1$  olmasıdır.

**İspat.**  $(\Rightarrow)(a, mn) = 1$  olsun. Bu durumda Önerme 1.5.16 dan  $ax + mny = 1$  olacak şekilde  $\exists x, y \in \mathbb{Z}$  vardır.  $ax + mny = 1$  ve  $x, ny \in \mathbb{Z}$  olduğundan Önerme 1.5.16 dan  $(a, m) = 1$  olur.  $ax + nmy = ax + mny = 1$  ve  $x, my \in \mathbb{Z}$  olduğundan Önerme 1.5.16 dan  $(a, n) = 1$  olur. Yani  $(a, m) = (a, n) = 1$  olup istenen elde edilir.

$(\Leftarrow)(a, m) = (a, n) = 1$  olsun. Bu durumda Önerme 1.5.16 dan  $ax_1 + my_1 = 1$  ve  $ax_2 + ny_2 = 1$  olacak şekilde  $\exists x_1, x_2, y_1, y_2 \in \mathbb{Z}$  vardır.  $ax_1 + my_1 = 1$  ve  $ax_2 + ny_2 = 1$  olduğundan

$$1 = 1.1 = (ax_1 + my_1)(ax_2 + ny_2) = a(ax_1x_2 + nx_1y_2 + my_1x_2) + mny_1y_2$$

eşitliğinde  $ax_1x_2 + nx_1y_2 + my_1x_2, y_1y_2 \in \mathbb{Z}$  olduğundan Önerme 1.5.16 dan  $(a, mn) = 1$  olur.

**Sonuç 1.5.27.**  $(a, m_1 m_2 \dots m_k) = 1$  olması için gerek ve yeter koşul  $\forall i = 1, 2, \dots, k$  için  $(a, m_i) = 1$  olmasıdır.

**Teorem 1.5.28.**  $a$  ve  $b$  iki pozitif tam sayı,  $a$  ve  $b$  nin farklı asal sayıların kuvvetleriyle birlikte çarpımları şeklinde yazılışları sırasıyla

$$a = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}, b = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} (p_i \text{ ler farklı asal sayılar } m_i, n_i \in \mathbb{N})$$

olsun. Bu durumda

$$(a, b) = p_1^{\min\{m_1, n_1\}} p_2^{\min\{m_2, n_2\}} \dots p_k^{\min\{m_k, n_k\}}$$

olur.

**İspat.**  $d = (a, b) = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$  ( $1 \leq i \leq k$  için  $t_i \in \mathbb{N}$ ) ve

$$c = p_1^{\min\{m_1, n_1\}} p_2^{\min\{m_2, n_2\}} \dots p_k^{\min\{m_k, n_k\}}$$

diyelim.  $1 \leq i \leq k$  için  $\min\{m_i, n_i\} \leq m_i$  ve  $\min\{m_i, n_i\} \leq n_i$  olup  $p_i^{\min\{m_i, n_i\}} \mid p_i^{m_i}$  ve  $p_i^{\min\{m_i, n_i\}} \mid p_i^{n_i}$  olur. Bu durumda Teorem 1.5.2 (x) den

$$c = p_1^{\min\{m_1, n_1\}} p_2^{\min\{m_2, n_2\}} \dots p_k^{\min\{m_k, n_k\}} \mid p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} = a$$

ve

$$c = p_1^{\min\{m_1, n_1\}} p_2^{\min\{m_2, n_2\}} \dots p_k^{\min\{m_k, n_k\}} \mid p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} = b$$

olup  $d = (a, b)$  olduğundan  $c \leq d$  bulunur.  $1 \leq i \leq k$  olan herhangi  $i \in \mathbb{Z}$  alalım.  $d = (a, b)$  olduğundan  $d > 0, d \mid a$  ve  $d \mid b$  olur.  $p_i^{t_i} \mid d, d \mid a$  ve  $d \mid b$  olduğundan Teorem 1.5.2 (iv) den

$$p_i^{t_i} \mid a = p_1^{m_1} \dots p_{i-1}^{m_{i-1}} p_i^{m_i} p_{i+1}^{m_{i+1}} \dots p_k^{m_k}$$

ve

$$p_i^{t_i} \mid b = p_1^{n_1} \dots p_{i-1}^{n_{i-1}} p_i^{n_i} p_{i+1}^{n_{i+1}} \dots p_k^{n_k}$$

dir. Burada  $p_1, p_2, \dots, p_k$  birbirinden farklı asal sayılar olduğundan ikiye ikiye aralarında asal olup  $(p_i^{t_i}, p_1^{m_1} \dots p_{i-1}^{m_{i-1}} p_{i+1}^{m_{i+1}} \dots p_k^{m_k}) = 1$  ve

$$(p_i^{t_i}, p_1^{n_1} \dots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \dots p_k^{n_k}) = 1$$

olur. O halde  $p_i^{t_i} \mid p_i^{m_i}$  ve  $p_i^{t_i} \mid p_i^{n_i}$  olup  $t_i \leq m_i$  ve  $t_i \leq n_i$  olur.  $t_i \leq m_i$  ve  $t_i \leq n_i$  olduğundan  $t_i \leq \min\{m_i, n_i\}$  olup  $p_i > 1$  olduğundan  $p_i^{t_i} \leq p_i^{\min\{m_i, n_i\}}$  olur. Yani  $1 \leq i \leq k$  için  $p_i^{t_i} \leq p_i^{\min\{m_i, n_i\}}$  olup  $d = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k} \leq p_1^{\min\{m_1, n_1\}} p_2^{\min\{m_2, n_2\}} \dots p_k^{\min\{m_k, n_k\}} = c$  eşitliği vardır. Ayrıca  $c \leq d$  olduğundan  $(a, b) = d = c = p_1^{\min\{m_1, n_1\}} p_2^{\min\{m_2, n_2\}} \dots p_k^{\min\{m_k, n_k\}}$  olup istenen elde edilir.

**Sonuç 1.5.29.**  $a$  ve  $b$  nin en büyük ortak böleni,  $a$  ve  $b$  nin asal çarpanlara ayrılışındaki ortak asal sayıların kuvvetleri en küçük olanların kuvvetleriyle birlikte çarpımlarından oluşur.

**Önerme 1.5.30.**  $(a, b) = 1$  olsun.  $k \in \mathbb{Z}$  olmak üzere  $a \mid k$  ve  $b \mid k$  ise  $ab \mid k$  olur.

**İspat.**  $k \in \mathbb{Z}$  olmak üzere  $a \mid k$  ve  $b \mid k$  olsun.  $b \mid k$  olduğundan  $k = bk_1$  olacak şekilde  $\exists k_1 \in \mathbb{Z}$  vardır.  $a \mid k = bk_1$  ve  $(a, b) = 1$  olduğundan Önerme 1.5.21 den  $a \mid k_1$  olup  $k_1 = ak_2$  olacak şekilde  $\exists k_2 \in \mathbb{Z}$  vardır.  $k = bk_1$  ve  $k_1 = ak_2$  olduğundan  $k = bk_1 = bak_2 = abk_2$  olup  $k_2 \in \mathbb{Z}$  olduğundan  $ab \mid k$  dır.

**Sonuç 1.5.31.**  $m_1, m_2, \dots, m_r$  ikişer ikişer aralarında asal sayılar ve  $k \in \mathbb{Z}$  olmak üzere  $\forall i = 1, 2, \dots, r$  için  $m_i \mid k$  olsun. Bu durumda  $m_1 m_2 \dots m_r \mid k$  olur.

**Tanım 1.5.32.**  $m$  ve  $n$  sıfırdan farklı iki tam sayı olsun.

- (i)  $m \mid k$  ve  $n \mid k$  olacak şekilde  $k > 0$  tam sayısı varsa  $k$  ya  $m$  ve  $n$  nin bir **ortak katı** denir.
- (ii)  $k, m$  ve  $n$  nin bir ortak katı olsun. Eğer  $m$  ile  $n$  nin her ortak  $t$  katı için  $k \mid t$  ise  $k$  ya  $m$  ve  $n$  nin **en küçük ortak katı (EKOK)** denir ve genellikle  $\text{OKEK}(m, n), \text{EKOK}(m, n)$  veya sadece  $[m, n]$  ile ifade edilir.

**Not.** Bu tanım ikiden çok sayılar için de genelleştirilebilir.

**Teorem 1.5.33.**  $a$  ve  $b$  iki pozitif tam sayı,  $a$  ve  $b$  nin farklı asal sayıların kuvvetleriyle birlikte çarpımları şeklinde yazılışları sırasıyla

$$a = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}, b = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} (p_i \text{ ler farklı asal sayılar } m_i, n_i \in \mathbb{N})$$

olsun. Bu durumda

$$[a, b] = p_1^{\max\{m_1, n_1\}} p_2^{\max\{m_2, n_2\}} \dots p_k^{\max\{m_k, n_k\}}$$

olur.

**İspat.**  $s = [a, b] = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$  ( $1 \leq i \leq k$  için  $t_i \in \mathbb{N}$ ) ve

$$c = p_1^{\max\{m_1, n_1\}} p_2^{\max\{m_2, n_2\}} \dots p_k^{\max\{m_k, n_k\}}$$

diyelim.  $1 \leq i \leq k$  için  $m_i \leq \max\{m_i, n_i\}$  ve  $n_i \leq \max\{m_i, n_i\}$  olduğundan  $p_i^{m_i} \mid p_i^{\max\{m_i, n_i\}}$  ve  $p_i^{n_i} \mid p_i^{\max\{m_i, n_i\}}$  olup

$$a = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} \mid p_1^{\max\{m_1, n_1\}} p_2^{\max\{m_2, n_2\}} \dots p_k^{\max\{m_k, n_k\}} = c$$

ve  $b = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} \mid p_1^{\max\{m_1, n_1\}} p_2^{\max\{m_2, n_2\}} \dots p_k^{\max\{m_k, n_k\}} = c$  olur. Ayrıca  $c > 0$  ve  $s = [a, b]$  olduğundan  $s \leq c$  olur.  $1 \leq i \leq k$  olan herhangi  $i \in \mathbb{Z}^+$  alalım.  $s = [a, b]$  olduğundan  $s > 0$ ,  $a \mid s$  ve  $b \mid s$  olur.  $p_i^{m_i} \mid a$ ,  $p_i^{n_i} \mid b$ ,  $a \mid s$  ve  $b \mid s$  olduğundan  $p_i^{m_i} \mid s = p_1^{t_1} \dots p_{i-1}^{t_{i-1}} p_i^{t_i} p_{i+1}^{t_{i+1}} \dots p_k^{t_k}$  ve  $p_i^{n_i} \mid s = p_1^{t_1} \dots p_{i-1}^{t_{i-1}} p_i^{t_i} p_{i+1}^{t_{i+1}} \dots p_k^{t_k}$  olur. Burada  $p_1, p_2, \dots, p_k$  birbirinden farklı asal sayılar olduğundan ikiye ikiye aralarında asal olup  $(p_i^{m_i}, p_1^{t_1} \dots p_{i-1}^{t_{i-1}} p_{i+1}^{t_{i+1}} \dots p_k^{t_k}) = 1$  ve  $(p_i^{n_i}, p_1^{t_1} \dots p_{i-1}^{t_{i-1}} p_{i+1}^{t_{i+1}} \dots p_k^{t_k}) = 1$  olur. Buradan  $p_i^{m_i} \mid p_i^{t_i}$  ve  $p_i^{n_i} \mid p_i^{t_i}$  olup  $p_i^{\max\{m_i, n_i\}} \mid p_i^{t_i}$  olur. Yani  $1 \leq i \leq k$  için

$$c = p_1^{\max\{m_1, n_1\}} p_2^{\max\{m_2, n_2\}} \dots p_k^{\max\{m_k, n_k\}} \mid p_1^{t_1} p_2^{t_2} \dots p_k^{t_k} = s$$

olur.  $c \mid s$  ve  $c, s \in \mathbb{Z}^+$  olduğundan  $c \leq s$  olup ayrıca  $s \leq c$  olduğundan  $[a, b] = p_1^{\max\{m_1, n_1\}} p_2^{\max\{m_2, n_2\}} \dots p_k^{\max\{m_k, n_k\}}$  olur ki bu da istenendir.

**Sonuç 1.5.34.**  $a$  ve  $b$  sıfırdan farklı iki tam sayı ve  $t \in \mathbb{Z}$  olmak üzere  $a \mid t$  ve  $b \mid t$  olsun. Bu durumda  $[a, b] \mid t$  olur.

**İspat.**  $[a, b] = [a, -b] = [-a, b] = [-a, -b]$  olduğu gösterilebilir. O halde ispatı  $a$  ve  $b$  nin pozitif olması durumu için yapmamız yeterlidir.  $a$  ve  $b$  nin birbirinden farklı asal sayıların kuvvetleriyle birlikte çarpımları şeklinde yazılışları sırasıyla

$$a = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}, b = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} \quad (p_i \text{ ler farklı asal sayılar } m_i, n_i \in \mathbb{N})$$

olsun. Bu durumda Teorem 1.5.33 den  $[a, b] = p_1^{\max\{m_1, n_1\}} p_2^{\max\{m_2, n_2\}} \dots p_k^{\max\{m_k, n_k\}}$  olur.  $1 \leq i \leq k$  için  $p_i^{m_i} \mid a$ ,  $p_i^{n_i} \mid b$ ,  $a \mid t$  ve  $b \mid t$  olduğundan  $p_i^{m_i} \mid t$  ve  $p_i^{n_i} \mid t$  olup  $p_i^{\max\{m_i, n_i\}} \mid t$  olur. Burada  $p_1, p_2, \dots, p_k$  birbirinden farklı asal sayılar olduğundan ikiye ikiye aralarında asaldır. Dolayısıyla  $p_1^{\max\{m_1, n_1\}}, p_2^{\max\{m_2, n_2\}}, \dots, p_k^{\max\{m_k, n_k\}}$  sayıları ikiye ikiye aralarında asal olur. Sonuç olarak

$$[a, b] = p_1^{\max\{m_1, n_1\}} p_2^{\max\{m_2, n_2\}} \dots p_k^{\max\{m_k, n_k\}} \mid t$$

olup istenen elde edilir.

**Sonuç 1.5.35.**  $a$  ve  $b$  iki pozitif tam sayı olsun. Bu durumda  $(a, b)[a, b] = ab$  olur.

**İspat.**  $a$  ve  $b$  nin birbirinden farklı asal sayıların kuvvetleriyle birlikte çarpımları şeklinde yazılışları sırasıyla

$$a = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}, b = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} (p_i \text{ ler farklı asal sayılar } m_i, n_i \in \mathbb{N})$$

olsun. Bu durumda Teorem 1.5.28 ve Teorem 1.5.33 gereği  $(a, b) = p_1^{\min\{m_1, n_1\}} p_2^{\min\{m_2, n_2\}} \dots p_k^{\min\{m_k, n_k\}}$  ve  $[a, b] = p_1^{\max\{m_1, n_1\}} p_2^{\max\{m_2, n_2\}} \dots p_k^{\max\{m_k, n_k\}}$  olur.

Burada  $1 \leq i \leq k$  için  $\min\{m_i, n_i\} + \max\{m_i, n_i\} = m_i + n_i$  olduğundan

$$\begin{aligned} (a, b)[a, b] &= p_1^{\min\{m_1, n_1\}} p_2^{\min\{m_2, n_2\}} \dots p_k^{\min\{m_k, n_k\}} p_1^{\max\{m_1, n_1\}} p_2^{\max\{m_2, n_2\}} \dots p_k^{\max\{m_k, n_k\}} \\ &= p_1^{\min\{m_1, n_1\} + \max\{m_1, n_1\}} p_2^{\min\{m_2, n_2\} + \max\{m_2, n_2\}} \dots p_k^{\min\{m_k, n_k\} + \max\{m_k, n_k\}} \\ &= p_1^{m_1 + n_1} p_2^{m_2 + n_2} \dots p_k^{m_k + n_k} = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} \\ &= ab \end{aligned}$$

olup istenen elde edilir.

**Tanım 1.5.36.** Pozitif  $n$  tam sayısı için  $1 \leq a \leq n$  ve  $(a, n) = 1$  olan  $a$  tam sayılarının sayısı genellikle  $\varphi(n)$  ile gösterilir. Bu  $\varphi$  fonksiyonuna **Euler fonksiyonu** denir.

**Teorem 1.5.37.** Euler fonksiyonu ile ilgili aşağıdaki özellikler sağlanır:

(i)  $p \in \mathbb{P}$  ise  $\varphi(p) = p - 1 = p \left(1 - \frac{1}{p}\right)$  olur.

(ii)  $p \in \mathbb{P}$  ve  $k \in \mathbb{Z}^+$  ise  $\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$  olur.

(iii)  $m, n \in \mathbb{Z}^+$  ve  $(m, n) = 1$  ise  $\varphi(mn) = \varphi(m)\varphi(n)$  olur.

(iv)  $p_1, p_2, \dots, p_k$  birbirinden farklı asal sayılar ve  $1 \leq i \leq k$  için  $r_i \in \mathbb{Z}^+$  olmak üzere  $m = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$  ise

$$\varphi(m) = \varphi(p_1^{r_1}) \varphi(p_2^{r_2}) \dots \varphi(p_k^{r_k}) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

olur.

**Örnek.**  $\varphi(1000) = \varphi(2^3 \cdot 5^3) = 1000 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400$ ,

$$\begin{aligned} \varphi(1500) &= \varphi(15 \cdot 10^2) = \varphi(3 \cdot 5 \cdot 2^2 \cdot 5^2) = \varphi(2^2 \cdot 3 \cdot 5^3) \\ &= 1500 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 1500 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 400 \end{aligned}$$

olur.

## 1.6. MODÜLER ARİTMETİK

**Tanım 1.6.1.**  $m$  sıfırdan farklı bir tam sayı ve  $a, b \in \mathbb{Z}$  olsun. Eğer  $m \mid a - b$  ise  $a, b$  ye  $m$  modülüne göre denktir denir ve  $a \equiv b \pmod{m}$  ile ifade edilir.

**Not.**  $m \mid a - b$  ise  $-m \mid a - b$  olduğundan bu bölümde aksi belirtilmedikçe  $a \equiv b \pmod{m}$  denkleğinde  $m > 0$  olarak alınacaktır.

**Örnek:**  $15 \equiv 3 \pmod{4}$ ,  $15 \equiv 11 \pmod{4}$ ,  $15 \equiv -5 \pmod{4}$  olur.

**Önerme 1.6.2.**  $m$  modülüne göre (yukarıda) tanımlanan  $\equiv$  bağıntısı  $\mathbb{Z}$  de bir denklik bağıntısıdır.

**İspat. Yansıma:** Her  $a \in \mathbb{Z}$  için  $m \mid 0 = a - a$  olduğundan  $a \equiv a \pmod{m}$  olup  $\equiv$  bağıntısının yansıma özelliği vardır.

**Simetri:**  $a \equiv b \pmod{m}$  olan herhangi  $a, b \in \mathbb{Z}$  alalım.  $a \equiv b \pmod{m}$  olduğundan tanımdan  $m \mid a - b$  olup Teorem 1.5.2 (viii) gereği  $m \mid -(a - b) = b - a$  olur. O halde tanımdan  $b \equiv a \pmod{m}$  olup  $\equiv$  bağıntısının simetri özelliği vardır.

**Geçişme:**  $a \equiv b \pmod{m}$  ve  $b \equiv c \pmod{m}$  olan herhangi  $a, b, c \in \mathbb{Z}$  alalım.  $a \equiv b \pmod{m}$  ve  $b \equiv c \pmod{m}$  olduğundan tanımdan  $m \mid a - b$  ve  $m \mid b - c$  olup Teorem 1.5.2 (v) gereği  $m \mid a - b + b - c = a - c$  olur. O halde  $a \equiv c \pmod{m}$  olup  $\equiv$  bağıntısının geçişme özelliği vardır.

Böylece  $\equiv$  bağıntısı  $\mathbb{Z}$  de bir denklik bağıntısı olup istenen elde edilir.

**Tanım 1.6.3.**  $\mathbb{Z}$  deki  $m$  modülüne göre tanımlanan  $\equiv$  denklik bağıntısının belirttiği denklik sınıflarına **kalan sınıfları** denir ve  $m$  modülüne göre tüm kalan sınıfları kümesi genellikle  $\mathbb{Z}_m$  ile gösterilir.

**Not.** Tanımdan bir  $a \in \mathbb{Z}$  nin kalan sınıfı  $\bar{a} = \{x \in \mathbb{Z} \mid m \mid a - x\} = \{x \in \mathbb{Z} \mid m \mid x - a\}$  dir.

**Örnek.** 4 modülüne göre

$$\bar{0} = \{\dots - 12, -8, -4, 0, 4, 8, \dots\},$$

$$\bar{1} = \{\dots - 11, -7, -3, 1, 5, 9, \dots\},$$

$$\bar{2} = \{\dots - 10, -6, -2, 2, 6, 10, \dots\}$$

$$\bar{3} = \{\dots - 9, -5, -1, 3, 7, 11, \dots\},$$

$$\bar{4} = \{\dots - 8, -4, 0, 4, 8, 12, \dots\} = \bar{0}$$

ve  $\overline{5} = \overline{1}, \overline{14} = \overline{2}, \overline{-5} = \overline{3}$  olur. Buna göre  $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$  olur.

**Önerme 1.6.4.**  $a \equiv b \pmod{m}$  olması için gerek ve yeter koşul  $a$  ve  $b$  nin  $m$  ile bölümünden elde edilen kalanların aynı olmasıdır.

**İspat.**  $(\Rightarrow) a \equiv b \pmod{m}$  olsun.  $b$  nin  $m$  ile bölümünden kalan  $r$  ve bölüm  $q$  olsun. Bu durumda  $b = qm + r$  ve  $0 \leq r < m$  olur.  $a$  nın da  $m$  ile bölümünden kalan  $r$  olduğu gösterilirse istenen elde edilir.  $a \equiv b \pmod{m}$  olduğundan tanımdan  $m \mid a - b$  olup  $a - b = mk$  olacak şekilde  $\exists k \in \mathbb{Z}$  vardır.  $a - b = mk$  ve  $b = qm + r$  olduğundan  $a = b + mk = qm + r + mk = (q + k)m + r$  olup burada  $q + k \in \mathbb{Z}$  ve  $0 \leq r < m$  olduğundan  $a$  nın  $m$  ile bölümünden kalan  $r$  olur.

$(\Leftarrow)$   $a$  ve  $b$  nin  $m$  ile bölümünden elde edilen kalanlar aynı olsun. Bu kalan sayıya  $r$  denilirse bu durumda  $a = q_1m + r$  ve  $b = q_2m + r$  olacak şekilde  $\exists q_1, q_2 \in \mathbb{Z}$  vardır.  $a = q_1m + r$  ve  $b = q_2m + r$  olduğundan  $a - b = q_1m + r - q_2m - r = (q_1 - q_2)m$  olup  $q_1 - q_2 \in \mathbb{Z}$  olduğundan  $m \mid a - b$  olur. O halde tanımdan  $a \equiv b \pmod{m}$  olup istenen elde edilir.

**Sonuç 1.6.5.**  $a$  nın  $m$  ile bölümünden kalan  $r$  ise  $a \equiv r \pmod{m}$  olur.

**İspat.**  $a$  nın  $m$  ile bölümünden kalan  $r$  olsun. Bu durumda  $a = qm + r$  olacak şekilde  $\exists q \in \mathbb{Z}$  vardır.  $a = qm + r$  olduğundan  $a - r = qm$  olup  $q \in \mathbb{Z}$  olduğundan  $m \mid a - r$  olur. O halde  $a \equiv r \pmod{m}$  olup istenen elde edilir.

**Not.** Bir  $a \in \mathbb{Z}$  nin  $m$  ile bölümünden kalan  $0, 1, 2, \dots, m - 1$  tam sayılarından biri olduğundan  $m$  modülüne göre  $\bar{a}$  sınıfı  $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m - 1}$  sınıflarından biridir. Ayrıca  $m$  modülüne göre  $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m - 1}$  sınıfları birbirinden farklıdır. O halde  $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m - 1}\}$  olup  $m$  elemanlıdır.

**Örnek.**  $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$  ve  $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$  olur.

**Önerme 1.6.6.**  $a \equiv a_1 \pmod{m}$  ve  $b \equiv b_1 \pmod{m}$  olsun. Bu durumda  $a + b \equiv a_1 + b_1 \pmod{m}$  olur.

**İspat.**  $a \equiv a_1 \pmod{m}$  ve  $b \equiv b_1 \pmod{m}$  olduğundan tanımdan  $m \mid a - a_1$  ve  $m \mid b - b_1$  olup Teorem 1.5.2 (v) den  $m \mid a - a_1 + b - b_1 = (a + b) - (a_1 + b_1)$  olur. O halde tanımdan  $a + b \equiv a_1 + b_1 \pmod{m}$  olup istenen elde edilir.

**Tanım 1.6.7.**  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  için  $\bar{a}$  ve  $\bar{b}$  sınıflarının toplamı  $\bar{a} \oplus \bar{b} = \overline{a+b}$  olarak tanımlanır.

**Not.** Önerme 1.6.6 dan  $\oplus$  işleminin  $\mathbb{Z}_m$  de bir iç işlem olduğu anlaşılır.

**Önerme 1.6.8.**  $\mathbb{Z}_m$  de  $\oplus$  işlemi için aşağıdaki özellikler sağlanır:  $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$  için

(i)  $\bar{a} \oplus \bar{b} = \bar{b} \oplus \bar{a}$  olur. (Değişme Özelliği)

(ii)  $\bar{a} \oplus (\bar{b} \oplus \bar{c}) = (\bar{a} \oplus \bar{b}) \oplus \bar{c}$  olur. (Birleşme Özelliği)

(iii)  $\bar{a} \oplus \bar{0} = \bar{0} \oplus \bar{a} = \bar{a}$  olur. ( $\bar{0}$  etkisiz elemandır)

(iv)  $\bar{a} \oplus \bar{x} = \bar{x} \oplus \bar{a} = \bar{0}$  olacak şekilde  $\exists \bar{x} \in \mathbb{Z}_m$  vardır. (Ters eleman)

**İspat.**  $\oplus$  işleminin tanımı kullanılarak ispat kolaylıkla yapılabilir.

**Önerme 1.6.9.**  $a \equiv a_1 \pmod{m}$  ve  $b \equiv b_1 \pmod{m}$  olsun. Bu durumda  $ab \equiv a_1b_1 \pmod{m}$  olur.

**İspat.**  $a \equiv a_1 \pmod{m}$  ve  $b \equiv b_1 \pmod{m}$  olduğundan  $m \mid a - a_1$  ve  $m \mid b - b_1$  olup  $a - a_1 = mk_1$  ve  $b - b_1 = mk_2$  olacak şekilde  $\exists k_1, k_2 \in \mathbb{Z}$  vardır. Burada  $a = a_1 + mk_1$  ve  $b = b_1 + mk_2$  olup  $ab = (a_1 + mk_1)(b_1 + mk_2) = a_1b_1 + m(a_1k_2 + b_1k_1 + mk_1k_2)$  olur.  $ab = a_1b_1 + m(a_1k_2 + b_1k_1 + mk_1k_2)$  eşitliğinden  $ab - a_1b_1 = m(a_1k_2 + b_1k_1 + mk_1k_2)$  olup  $a_1k_2 + b_1k_1 + mk_1k_2 \in \mathbb{Z}$  olduğundan  $m \mid ab - a_1b_1$  olur. O halde tanımdan  $ab \equiv a_1b_1 \pmod{m}$  olup istenen elde edilir.

**Sonuç 1.6.10.**  $a_1 \equiv b_1 \pmod{m}, a_2 \equiv b_2 \pmod{m}, \dots, a_k \equiv b_k \pmod{m}$  olsun. Bu durumda  $a_1a_2 \dots a_k \equiv b_1b_2 \dots b_k \pmod{m}$  olur.

**İspat.**  $a_1 \equiv b_1 \pmod{m}$  ve  $a_2 \equiv b_2 \pmod{m}$  olduğundan Önerme 1.6.9 gereği  $a_1a_2 \equiv b_1b_2 \pmod{m}$  olur.  $a_1a_2 \equiv b_1b_2 \pmod{m}$  ve  $a_3 \equiv b_3 \pmod{m}$  olduğundan yine Önerme 1.6.9 dan  $a_1a_2a_3 \equiv b_1b_2b_3 \pmod{m}$  olur. Böyle devam edilirse  $a_1a_2 \dots a_k \equiv b_1b_2 \dots b_k \pmod{m}$  olduğu gösterilebilir.

**Tanım 1.6.11.**  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  için  $\bar{a}$  ve  $\bar{b}$  sınıflarının çarpımı  $\bar{a} \odot \bar{b} = \overline{ab}$  olarak tanımlanır.

**Not.** Önerme 1.6.9 dan  $\odot$  işleminin  $\mathbb{Z}_m$  de bir iç işlem olduğu anlaşılır.

**Önerme 1.6.12.**  $\mathbb{Z}_m$  de  $\odot$  işlemi için aşağıdaki özellikler sağlanır:  $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$  için

(i)  $\bar{a} \odot \bar{b} = \bar{b} \odot \bar{a}$  olur. (Değişme Özelliği)

(ii)  $\bar{a} \odot (\bar{b} \odot \bar{c}) = (\bar{a} \odot \bar{b}) \odot \bar{c}$  olur. (Birleşme Özelliği)

(iii)  $\bar{a} \odot \bar{1} = \bar{1} \odot \bar{a} = \bar{a}$  olur. ( $\bar{1}$  etkisiz elemandır)

(iv)  $\bar{a} \odot \bar{0} = \bar{0} \odot \bar{a} = \bar{0}$  olur. ( $\bar{0}$  yutan elemandır)

**İspat.**  $\odot$  işleminin tanımı kullanılarak ispat kolaylıkla yapılabilir.

**Önerme 1.6.13.**  $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$  için

$$\bar{a} \odot (\bar{b} \oplus \bar{c}) = (\bar{a} \odot \bar{b}) \oplus (\bar{a} \odot \bar{c})$$

olur. ( $\odot$  işleminin  $\oplus$  işlemi üzerine Dağılma Özelliği)

**İspat.**  $\oplus$  ve  $\odot$  işlemlerinin tanımı kullanılarak ispat kolaylıkla yapılabilir.

Örnek:  $\mathbb{Z}_6$  da  $\bar{2} \cdot \bar{3} = \overline{2 \cdot 3} = \bar{6} = \bar{0}$ ,  $\bar{2} \cdot \bar{5} + \bar{3}^2 = \overline{10 + 9} = \bar{4} + \bar{3} = \bar{7} = \bar{1}$  ve  $\bar{5} \cdot \bar{5} = \overline{25} = \bar{1}$  olur.

## 2. GRUPLAR

### 2.1. GRUP AKSİYOMLARI

**Tanım 2.1.1.**  $G$  boştan farklı bir küme ve  $*$ ,  $G$  de bir ikili (iç) işlem olsun. Eğer  $*$  işlemi aşağıdaki özellikleri sağlarsa  $(G, *)$  cebirsel yapısına bir **grup** denir.

**G1)**  $*$  işleminin  $G$  de birleşme özelliği vardır. Yani  $\forall a, b, c \in G$  için  $a * (b * c) = (a * b) * c$  olur.

**G2)**  $G$  nin  $*$  işlemine göre birim (etkisiz) elemanı vardır. Yani öyle  $e \in G$  elemanı vardır ki  $\forall a \in G$  için  $a * e = e * a = a$  olur.

**G3)**  $G$  deki her elemanın  $*$  işlemine göre tersi vardır. Yani  $\forall a \in G$  için  $a * x = x * a = e$  olacak şekilde  $\exists x \in G$  vardır.

Sadece (G1) özelliğini sağlayan  $(G, *)$  cebirsel yapısına bir **yarı grup**, (G1) ve (G2) özelliklerini sağlayan  $(G, *)$  cebirsel yapısına da **monoid** denir.

**Not.** Önerme 1.4.5 ve Önerme 1.4.6 ya göre, bir grupta birim elemanın ve bir elemanın tersinin teklikle belirli olduğu anlaşılır.

**Tanım 2.1.2.**  $(G, *)$  bir grup olsun. Eğer  $\forall a, b \in G$  için  $a * b = b * a$  ise bu gruba bir **değişmeli grup** veya **Abel Grubu** denir.

**Örnek.**  $\mathbb{Z}$  tam sayılar kümesi bildiğimiz  $+$  işlemine göre değişmeli gruptur.  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{Q} - \{0\}, \cdot)$  ve  $(\mathbb{R} - \{0\}, \cdot)$  cebirsel yapıları birer değişmeli gruptur. Pozitif tam sayılar kümesi bildiğimiz  $\cdot$  işlemine göre hem bir yarı grup hem de bir monoiddir.

**Tanım 2.1.3.**  $(G, *)$  bir grup ve  $G$  sonlu elemanlı ise bu gruba **sonlu grup** denir,  $G$  nin eleman sayısına da **grubun mertebesi** denir ve genellikle  $|G|$  veya  $|G|$  ile gösterilir.

**Not.** Bir  $G$  grubunda işlemin sembolü özel olarak belirtilmemişse bazen bu sembol  $\cdot$  ile gösterilir. Grubun birim elemanı da genellikle  $e_G$  veya sadece  $e$  ile gösterilir. Eğer  $G$  değişmeli grup ise burada işlemin sembolü bazen  $+$  ile de gösterilir. Bu durumda  $\forall a \in G$  için  $a$  elemanının tersi genellikle  $-a$  ile gösterilir, grubun  $+$  işlemine göre birim elemanı da genellikle  $0_G$  veya sadece  $0$  ile gösterilir.

**Önerme 2.1.4.**  $G$  bir grup olsun. Bu durumda  $a, b, c \in G$  olmak üzere

(i)  $ab = ac$  ise  $b = c$  (soldan kısaltma özelliği) ve

(ii)  $ac = bc$  ise  $a = b$  (sağdan kısaltma özelliği) olan kısaltma özellikleri sağlanır.

**İspat.** (i)  $ab = ac$  olsun.  $G$  bir grup olduğundan  $a$  elemanının  $G$  de  $a^{-1}$  tersi vardır.  $ab = ac$  olduğundan  $a^{-1}ab = a^{-1}ac$  olup  $eb = ec$  ve buradan da  $b = c$  elde edilir.

(ii) (i) deki ispat yöntemi kullanılarak görülür.

**Önerme 2.1.5.**  $G$  bir grup olsun. Bu durumda  $\forall a, b \in G$  için

(i)  $ax = b$  olacak şekilde  $\exists x \in G$  vardır ve tektir.

(ii)  $ya = b$  olacak şekilde teklikle belirli bir  $y \in G$  vardır.

**İspat.** Herhangi  $a, b \in G$  alalım.

(i)  $G$  grubunda  $x = a^{-1}b \in G$  elemanı için  $ax = aa^{-1}b = eb = b$  olur. Şimdi bu elemanın tekliğini gösterelim.  $ac = b$  olan herhangi  $c \in G$  alalım.  $c = x$  olduğu gösterilirse istenen elde edilir.  $ax = b$  ve  $ac = b$  olduğundan  $ac = ax$  olup kısaltma özelliğinden  $c = x$  olur.

(ii)  $G$  grubunda  $y = ba^{-1}$  elemanı için  $ya = ba^{-1}a = be = b$  olur. Şimdi bu elemanın tekliğini gösterelim.  $da = b$  olan herhangi  $d \in G$  alalım.  $d = y$  olduğu gösterilirse istenen elde edilir.  $da = b$  ve  $ya = b$  olduğundan  $da = ya$  olup kısaltma özelliğinden  $d = y$  olur.

**Tanım 2.1.5.**  $G$  bir grup,  $a \in G$  ve  $e, G$  nin birim elemanı olsun.  $n \in \mathbb{Z}$  olmak üzere

$$a^n = \begin{cases} \underbrace{aa \dots a}_{n \text{ tane}} & , n > 0 \text{ ise} \\ e & , n = 0 \text{ ise} \\ \underbrace{a^{-1}a^{-1} \dots a^{-1}}_{-n \text{ tane}} & , n < 0 \text{ ise} \end{cases}$$

olarak tanımlanır. Bu  $a^n$  elemanına  **$a$  elemanının  $n$ . kuvveti** denir.

**Örnek.**  $G$  bir grup ve  $a \in G$  olmak üzere  $a^5 = aaaaa$ ,  $a^{-5} = a^{-1}a^{-1}a^{-1}a^{-1}a^{-1}$  ve  $a^0 = e$  olur.

**Önerme 2.1.6.**  $G$  bir grup ve  $a, b \in G$  olsun. Bu takdirde  $\forall m, n \in \mathbb{Z}^+$  için

(i)  $a^m a^n = a^{m+n}$  dir.

(ii)  $(a^m)^n = a^{mn}$  dir.

(iii)  $G$  değişmeli ise  $(ab)^m = a^m b^m$  olur.

**İspat.** Herhangi  $m, n \in \mathbb{Z}^+$  alalım.

(i) Tanımdan  $a^m a^n = \underbrace{aa \dots a}_{m \text{ tane}} \underbrace{aa \dots a}_{n \text{ tane}} = \underbrace{aa \dots a}_{m+n \text{ tane}} = a^{m+n}$  olup istenen elde edilir.

(ii) Tanımdan ve (i) şikkından

$$(a^m)^n = \underbrace{a^m a^m \dots a^m}_{n \text{ tane}} = a^{m+m} \underbrace{a^m a^m \dots a^m}_{n-2 \text{ tane}} = \dots = a^{\underbrace{m+m+\dots+m}_{n \text{ tane}}} = a^{mn}$$

olup istenen elde edilir.

(iii)  $G$  değişmeli olsun. Bu durumda tanımdan

$$\begin{aligned}
(ab)^m &= \underbrace{(ab)(ab) \dots (ab)}_{m \text{ tane}} = (aa)(bb) \underbrace{(ab) \dots (ab)}_{m-2 \text{ tane}} = (aaa)(bbb) \underbrace{(ab) \dots (ab)}_{m-3 \text{ tane}} = \dots = \\
&= \underbrace{aa \dots a}_{m \text{ tane}} \underbrace{bb \dots b}_{m \text{ tane}} = a^m b^m
\end{aligned}$$

elde edilir.

**Sonuç 2.1.7.** Yukarıdaki teorem  $\forall m, n \in \mathbb{Z}$  için de sağlanır. Yani  $G$  bir grup ve  $a, b \in G$  olmak üzere  $\forall m, n \in \mathbb{Z}$  için

(i)  $a^m a^n = a^{m+n}$  dir.

(ii)  $(a^m)^n = a^{mn}$  dir.

(iii)  $G$  değişmeli ise  $(ab)^m = a^m b^m$  olur.

**Not.** Bir  $G$  değişmeli grubundaki işlem  $+$  sembolü ile gösterilmişse  $G$  nin bir  $a$  elemanının  $n$ . kuvveti yerine genellikle kat tanımlanır.

**Tanım 2.1.8.**  $(G, +)$  değişmeli grup ve  $a \in G$  olsun.  $n \in \mathbb{Z}$  olmak üzere

$$na = \begin{cases} \underbrace{a + a + \dots + a}_{n \text{ tane}}, & n > 0 \text{ ise} \\ 0_G, & n = 0 \text{ ise} \\ \underbrace{(-a) + (-a) + \dots + (-a)}_{-n \text{ tane}}, & n < 0 \text{ ise} \end{cases}$$

olarak tanımlanır. Bu  $na$  elemanına  **$a$  elemanının  $n$  katı** denir.

**Önerme 2.1.9.**  $(G, +)$  grup ve  $a, b \in G$  olsun.  $\forall m, n \in \mathbb{Z}$  için

(i)  $ma + na = (m + n)a$  olur.

(ii)  $m(na) = (mn)a$  olur.

(iii)  $n(a + b) = na + nb$  olur.

**Teorem 2.1.10.**  $G$  boştan farklı bir küme ve  $*$ ,  $G$  de bir iç işlem olsun.  $*$  işlemi birleşme aksiyomu ile aşağıdaki koşulları sağlasın.

(i) Öyle  $e \in G$  vardır ki  $\forall a \in G$  için  $e * a = a$  olur (sol birim)

(ii)  $\forall a \in G$  için  $a' * a = e$  olacak şekilde  $\exists a' \in G$  vardır ( $a$  elemanının sol tersi)

Bu durumda  $(G,*)$  bir gruptur.

**İspat.** Herhangi  $a \in G$  alalım. ii) koşulundan  $a' * a = e$  olacak şekilde  $\exists a' \in G$  vardır.  $a' \in G$  olduğundan ii) koşulundan  $a'' * a' = e$  olacak şekilde  $\exists a'' \in G$  vardır. Burada  $*$  işleminin birleşme özelliği ve i) koşulundan  $a = e * a = (a'' * a') * a = a'' * (a' * a) = a'' * e$  olur.  $a = a'' * e$  ve  $e * e = e$  olduğundan  $*$  işleminin birleşme özelliğinden  $a * e = (a'' * e) * e = a'' * (e * e) = a'' * e = a$  olur. Yani  $\forall a \in G$  için  $a * e = e * a = a$  olup  $e$  elemanı  $G$  nin  $*$  işlemine göre birim elemanı olur.

Herhangi  $a \in G$  alalım. ii) koşulundan  $a' * a = e$  olacak şekilde  $\exists a' \in G$  vardır.  $a' \in G$  olduğundan ii) koşulundan  $a'' * a' = e$  olacak şekilde  $\exists a'' \in G$  vardır. Burada  $*$  işleminin birleşme özelliği ve i) koşulundan  $a = e * a = (a'' * a') * a = a'' * (a' * a) = a'' * e$  olur.  $a = a'' * e$  ve  $e, G$  nin  $*$  işlemine göre birim elemanı olduğundan  $a = a'' * e = a''$  olup  $a'' * a' = e$  olduğundan  $a * a' = e$  olur.  $a * a' = a' * a = e$  olduğundan  $a'$  elemanı  $a$  nın  $G$  de  $*$  işlemine göre tersi olur. Yani  $G$  deki her elemanın  $G$  de  $*$  işlemine göre tersi vardır.

Böylece  $(G,*)$  bir grup olup istenen elde edilir.

**Teorem 2.1.11.**  $G$  boştan farklı bir küme ve  $*, G$  de bir iç işlem olsun.  $*$  işlemi birleşme aksiyomu ile aşağıdaki koşulları sağlasın.

- (i) Öyle  $e \in G$  vardır ki  $\forall a \in G$  için  $a * e = a$  olur (sağ birim)
- (ii)  $\forall a \in G$  için  $a * a' = e$  olacak şekilde  $\exists a' \in G$  vardır (  $a$  elemanının sağ tersi)

Bu durumda  $(G,*)$  bir gruptur.

**İspat.** Teorem 2.1.10 daki ispat yöntemi kullanılarak yapılabilir.

**Teorem 2.1.12.**  $G$  boştan farklı bir küme;  $*, G$  de birleşme özelliğine sahip bir iç işlem ve  $\forall a, b \in G$  için  $a * x = b$  ve  $y * a = b$  olacak şekilde  $\exists x, y \in G$  bulunabilsin. Bu durumda  $(G,*)$  bir gruptur.

**İspat.**  $G \neq \emptyset$  olduğundan  $\exists a \in G$  vardır.  $a \in G$  olduğundan hipotezden  $e * a = a$  olacak şekilde bir  $e \in G$  vardır. Herhangi  $b \in G$  alalım.  $a, b \in G$  olduğundan hipotezden  $a * x = b$  olacak şekilde  $\exists x \in G$  vardır. Burada  $*$  işleminin  $G$  de birleşme özelliğinden  $e * b = e * (a * x) = (e * a) * x = a * x = b$  olur. Yani  $\forall b \in G$  için  $e * b = b$  olup  $e$  elemanı  $G$  nin  $*$  işlemine göre sol birim elemanıdır.  $a \in G$  keyfî olsun.  $e \in G$  olduğundan hipotezden  $a' * a =$

$e$  olacak şekilde  $\exists a' \in G$  vardır.  $a' * a = e$  olduğundan  $a'$  elemanı  $a$  nın  $G$  de  $*$  işlemine göre sol tersi olur. Yani  $G$  deki her elemanın  $G$  de  $*$  işlemine göre sol tersi vardır. Böylece Teorem 2.1.10 gereği  $(G, *)$  bir grup olup istenen elde edilir.

**Teorem 2.1.13.**  $G$  boştan farklı sonlu bir küme ve  $*$ ,  $G$  de bir iç işlem olsun.  $*$  işleminin birleşme, sağdan ve soldan kısaltma özellikleri varsa  $(G, *)$  bir gruptur.

**İspat.**  $*$  işleminin  $G$  de, birleşme, sağdan ve soldan kısaltma özelliklerinin varlığını kabul edelim. Herhangi  $a, b \in G$  alalım.

$$f: G \rightarrow G, x \rightarrow f(x) = a * x$$

dönüşümünü tanımlayalım.  $f$  nin bir fonksiyon olduğu açıktır.  $f(x_1) = f(x_2)$  olan herhangi  $x_1, x_2 \in G$  alalım.  $f(x_1) = f(x_2)$  olduğundan  $a * x_1 = a * x_2$  olup  $*$  işleminin soldan kısaltma özelliğinden  $x_1 = x_2$  olur. O halde  $f$  bire-bir olur. Burada  $G$  sonlu elemanlı olduğundan Önerme 1.3.9 gereği  $f$  aynı zamanda örtendir.  $f$  örten ve  $b \in G$  olduğundan  $f(x) = b$  olacak şekilde  $\exists x \in G$  vardır.  $f(x) = b$  olduğundan  $a * x = b$  olur. Benzer şekilde

$$g: G \rightarrow G, y \rightarrow g(y) = y * a$$

dönüşümünü tanımlayarak  $y * a = b$  olacak şekilde  $\exists y \in G$  elemanının varlığı gösterilebilir. O halde Teorem 2.1.12 den  $(G, *)$  bir grup olup istenen elde edilir.

**Teorem 2.1.14.**  $(G_1, \Delta)$  ve  $(G_2, \blacksquare)$  iki grup olsun.  $G_1 \times G_2$  kümesi  $\forall (a_1, b_1), (a_2, b_2) \in G_1 \times G_2$  için  $(a_1, b_1) * (a_2, b_2) = (a_1 \Delta a_2, b_1 \blacksquare b_2)$  ile tanımlı  $*$  işlemine göre bir gruptur. Bu gruba  $G_1$  ve  $G_2$  gruplarının **direkt çarpımı** denir.

**İspat.**  $*$  işleminin  $G_1 \times G_2$  de bir iç işlem olduğu açıktır.  $(G_1, \Delta)$  ve  $(G_2, \blacksquare)$  birer grup olduğundan  $*$  işleminin tanımından  $\forall (a_1, b_1), (a_2, b_2), (a_3, b_3) \in G_1 \times G_2$  için

$$\begin{aligned} (a_1, b_1) * [(a_2, b_2) * (a_3, b_3)] &= (a_1, b_1) * (a_2 \Delta a_3, b_2 \blacksquare b_3) = (a_1 \Delta (a_2 \Delta a_3), b_1 \blacksquare (b_2 \blacksquare b_3)) \\ &= ((a_1 \Delta a_2) \Delta a_3, (b_1 \blacksquare b_2) \blacksquare b_3) = (a_1 \Delta a_2, b_1 \blacksquare b_2) * (a_3, b_3) \\ &= [(a_1, b_1) * (a_2, b_2)] * (a_3, b_3) \end{aligned}$$

olup  $*$  işleminin  $G_1 \times G_2$  de birleşme özelliği vardır.

$G_1$  in  $\Delta$  işlemine göre birim elemanı  $e_1$  ve  $G_2$  nin  $\blacksquare$  işlemine göre birim elemanı  $e_2$  olsun.  $G_1 \times G_2$  nin  $(e_1, e_2)$  elemanını alalım. Burada  $\forall (a, b) \in G_1 \times G_2$  için  $(a, b) * (e_1, e_2) =$

$(a\Delta e_1, b\blacksquare e_2) = (a, b)$  ve  $(e_1, e_2) * (a, b) = (e_1\Delta a, e_2\blacksquare b) = (a, b)$  olup  $(e_1, e_2)$  elemanı  $G_1 \times G_2$  nin  $*$  işlemine göre birim elemanı olur.

Herhangi  $(a, b) \in G_1 \times G_2$  alalım.  $(G_1, \Delta)$  ve  $(G_2, \blacksquare)$  birer grup olduğundan  $a\Delta x = x\Delta a = e_1$  ve  $b\blacksquare y = y\blacksquare b = e_2$  olacak şekilde  $\exists x \in G_1$  ve  $\exists y \in G_2$  vardır.  $G_1 \times G_2$  nin  $(x, y)$  elemanını alalım. Burada  $(a, b) * (x, y) = (a\Delta x, b\blacksquare y) = (e_1, e_2)$  ve  $(x, y) * (a, b) = (x\Delta a, y\blacksquare b) = (e_1, e_2)$  olup  $(x, y)$  elemanı  $(a, b)$  nin  $G_1 \times G_2$  de  $*$  işlemine göre tersi olur. Yani  $G_1 \times G_2$  deki her elemanın  $G_1 \times G_2$  de  $*$  işlemine göre tersi vardır.

Böylece  $G_1 \times G_2$  kümesi  $*$  işlemine göre bir grup olup istenen elde edilir.

## 2.2. ALT GRUPLAR

**Tanım 2.2.1.**  $G$  bir grup ve  $H, G$  nin boştan farklı bir alt kümesi olsun. Eğer  $H, G$  deki işleme göre grup oluyorsa  $H$  ye  $G$  nin bir **alt grubu** denir ve genellikle  $H < G$  ile ifade edilir.

**Not.** Her grup kendisinin bir alt grubudur.  $G$  bir grup ve  $e, G$  nin birim elemanı ise  $\{e\} < G$  olur.

**Tanım 2.2.2.**  $G$  bir grup olsun.  $G$  nin varsa  $\{e\}$  ve  $G$  den farklı alt grubuna  $G$  nin bir **öz (has) alt grubu** denir.

**Örnek.**  $(\mathbb{Q} - \{0\}, \cdot)$  grubu  $(\mathbb{R} - \{0\}, \cdot)$  grubunun bir öz alt grubudur.

**Örnek.**  $G = \{-1, 1, i, -i\}$  kümesi kompleks sayılarda bildiğimiz çarpma işlemine göre 4. mertebeden bir gruptur.  $H = \{-1, 1\}$  kümesi  $G$  nin 2. mertebeden bir öz alt grubudur.

**Teorem 2.2.3.**  $H, G$  nin bir alt grubu ise  $H$  nin birim elemanı ile  $G$  nin birim elemanı aynıdır.

**İspat.**  $H < G$  olsun.  $H$  nin birim elemanına  $e_H$  ve  $G$  nin birim elemanına da  $e_G$  diyelim.  $e_H = e_G$  olduğu gösterilirse istenen elde edilir.  $e_H, H$  nin birim elemanı olduğundan  $e_H e_H = e_H$  olur.  $e_G, G$  nin birim elemanı ve  $e_H \in G$  olduğundan  $e_H e_G = e_H$  olur.  $e_H e_H = e_H$  ve  $e_H e_G = e_H$  olduğundan  $e_H e_H = e_H e_G$  olup burada  $e_H, e_G \in G$  ve  $G$  bir grup olduğundan kısaltma özelliğinden  $e_H = e_G$  elde edilir.

**Sonuç 2.2.4.**  $H < G$  ise  $\forall a \in H$  için  $a$  elemanının  $H$  deki tersi ile  $G$  deki tersi aynıdır.

**Teorem 2.2.5.**  $G$  bir grup ve  $\emptyset \neq H \subset G$  olsun.  $H$  nin bir alt grup olması için gerek ve yeter koşul

(i)  $\forall a, b \in H$  için  $ab \in H$  ve

(ii)  $\forall a \in H$  için  $a^{-1} \in H$  olmasıdır.

**İspat.** ( $\Rightarrow$ )  $H < G$  olsun. Bu durumda  $H, G$  deki işleme göre kendi başına bir grup olup teoremin ifadesindeki (i) ve (ii) koşulları sağlanır.

( $\Leftarrow$ ) Teoremin ifadesindeki (i) ve (ii) koşulları sağlansın. (i) koşulundan  $G$  deki işlemin  $H$  de bir iç işlem olduğu anlaşılır.  $H \subset G$  olduğundan  $\forall a, b, c \in H$  için  $a, b, c \in G$  olup  $G$  deki işlemin birleşme özelliğinden  $a(bc) = (ab)c$  olur. O halde  $G$  deki işlemin  $H$  de birleşme özelliği vardır.  $H \neq \emptyset$  olduğundan  $\exists a \in H$  vardır. (ii) koşulundan  $a^{-1} \in H$  olur.  $a, a^{-1} \in H$  olduğundan (i) koşulundan  $e = aa^{-1} \in H$  olur. Ayrıca  $H \subset G$  olduğundan  $\forall x \in H$  için  $x \in G$  olup  $e, G$  nin birim elemanı olduğundan  $xe = ex = x$  olur. O halde  $e, H$  nin  $G$  deki işleme göre birim elemanı olur. Herhangi  $a \in H$  alalım. (ii) koşulundan  $a^{-1} \in H$  olur. Burada  $aa^{-1} = a^{-1}a = e$  ve  $e, H$  nin  $G$  deki işleme göre birim elemanı olduğundan  $a^{-1}$  elemanı  $a$  nın  $H$  de  $G$  deki işleme göre tersi olur. Yani  $H$  deki her elemanın  $G$  deki işleme göre tersi vardır. Böylece  $H, G$  deki işleme göre bizzat bir grup olup  $H < G$  olur.

**Teorem 2.2.6.**  $G$  bir grup ve  $\emptyset \neq H \subset G$  olsun.  $H$  nin bir alt grup olması için gerek ve yeter koşul  $\forall a, b \in H$  için  $ab^{-1} \in H$  olmasıdır.

**İspat.** ( $\Rightarrow$ )  $H < G$  olsun. Bu durumda  $H, G$  deki işleme göre bizzat bir grup olup  $\forall a, b \in H$  için  $ab^{-1} \in H$  olduğu açıktır.

( $\Leftarrow$ )  $H \neq \emptyset$  olduğundan  $\exists a \in H$  vardır.  $a \in H$  olduğundan hipotezden  $e = aa^{-1} \in H$  olur. Yani  $G$  nin birim elemanı  $H$  nin bir elemanıdır. Herhangi  $c \in H$  alalım.  $e, c \in H$  olduğundan hipotezden  $c^{-1} = ec^{-1} \in H$  olur. Yani  $H$  deki her elemanın  $G$  deki tersi yine  $H$  nin bir elemanıdır. Herhangi  $x, y \in H$  alalım.  $y \in H$  ve  $H$  deki her elemanın  $G$  deki tersi  $H$  nin bir elemanı olduğundan  $y^{-1} \in H$  olur.  $x, y^{-1} \in H$  olduğundan hipotezden  $xy = x(y^{-1})^{-1} \in H$  olur. Yani  $\forall x, y \in H$  için  $xy \in H$  olup  $G$  deki işlem  $H$  de bir iç işlem olur.  $G$  deki işlemin  $H$  de birleşme özelliği de  $G$  den sağlanır. Böylece  $H, G$  deki işleme göre bizzat bir grup olup  $H < G$  olur.

**Teorem 2.2.7.**  $G$  bir grup ve  $\emptyset \neq H \subset G$  olsun.  $H$  nin bir alt grup olması için gerek ve yeter koşul  $\forall a, b \in H$  için  $a^{-1}b \in H$  olmasıdır.

**İspat.** Teorem 2.2.6 nın ispatına benzer şekilde yapılır.

**Teorem 2.2.8.**  $G$  bir grup ve  $H, G$  nin boştan farklı sonlu elemanlı bir alt kümesi olsun. Eğer  $\forall a, b \in H$  için  $ab \in H$  ise  $H < G$  olur.

**İspat.**  $\forall a, b \in H$  için  $ab \in H$  olsun. Herhangi  $x \in H$  alalım.

$$f: H \rightarrow H, x \rightarrow f(x) = ax$$

dönüşümünü tanımlayalım.  $f$  nin bir fonksiyon olduğu açıktır.  $f(x_1) = f(x_2)$  olan herhangi  $x_1, x_2 \in H$  alalım.  $f(x_1) = f(x_2)$  olduğundan  $ax_1 = ax_2$  olup  $G$  deki işlemin soldan kısaltma özelliğinden  $x_1 = x_2$  olur. O halde  $f$  bire-bir olur. Burada  $H$  sonlu elemanlı olduğundan Önerme 1.3.9 gereği  $f$  aynı zamanda örtendir.  $f$  örten ve  $a \in H$  olduğundan  $f(x) = a$  olacak şekilde  $\exists x \in H$  vardır. Burada  $ax = a = ae$  olup kısaltma özelliğinden  $x = e$  olur. O halde  $e \in H$  olur.  $e \in H$  ve  $f$  örten olduğundan  $f(y) = e$  olacak şekilde  $\exists y \in H$  vardır. Burada  $ay = e$  olup  $y = a^{-1}$  olur. O halde  $a^{-1} \in H$  olur. Yani  $\forall a \in H$  için  $a^{-1} \in H$  olup ayrıca  $\forall a, b \in H$  için  $ab \in H$  olduğundan Teorem 2.2.5 den  $H < G$  olur.

**Teorem 2.2.9.** Bir  $G$  grubunun birtakım alt gruplarının kesişimi de  $G$  nin bir alt grubudur.

**İspat.**  $\{H_i\}_{i \in I}, G$  nin alt gruplarının bir ailesi olsun.  $\bigcap_{i \in I} H_i < G$  olduğu gösterilirse istenen elde edilir.  $\forall i \in I$  için  $H_i < G$  olduğundan  $e \in H_i$  olur.  $\forall i \in I$  için  $e \in H_i$  olduğundan  $e \in \bigcap_{i \in I} H_i$  olup  $\bigcap_{i \in I} H_i \neq \emptyset$  olur. Ayrıca  $\bigcap_{i \in I} H_i \subset G$  olduğu da açıktır. Yani  $\emptyset \neq \bigcap_{i \in I} H_i \subset G$  olur. Herhangi  $a, b \in \bigcap_{i \in I} H_i$  alalım.  $a, b \in \bigcap_{i \in I} H_i$  olduğundan  $\forall i \in I$  için  $a, b \in H_i$  olup  $H_i < G$  olduğundan  $ab^{-1} \in H_i$  olur.  $\forall i \in I$  için  $ab^{-1} \in H_i$  olduğundan  $ab^{-1} \in \bigcap_{i \in I} H_i$  olur. Yani  $\forall a, b \in \bigcap_{i \in I} H_i$  için  $ab^{-1} \in \bigcap_{i \in I} H_i$  olup Teorem 2.2.6 dan  $\bigcap_{i \in I} H_i < G$  olur.

**Tanım 2.2.10.**  $G$  bir grup;  $A$  ve  $B, G$  nin iki alt kümesi olsun.  $AB = \{ab \mid a \in A \wedge b \in B\}$  kümesine  **$A$  kümesinin  $B$  kümesine çarpımı** denir. Özel olarak eğer  $A = \{a\}$  şeklinde tek elemanlı ise  $\{a\}B$  yerine genellikle  $aB$  yazılır, eğer  $B = \{b\}$  şeklinde tek elemanlı ise  $A\{b\}$  yerine genellikle  $Ab$  yazılır (hem  $A$ , hem de  $B$  tek elemanlı ise parantez kaldırılmaz, sadece bir tanesinde kaldırılabilir). Benzer tanım toplamsal grup için de yapılabilir.

**Teorem 2.2.11.**  $G$  bir grup,  $H < G$  ve  $K < G$  olsun. Bu durumda  $HK < G$  olması için gerek ve yeter koşul  $HK = KH$  olmasıdır.

**İspat.**  $(\Rightarrow) HK < G$  olsun. Herhangi  $x \in HK$  alalım.  $x \in HK$  ve  $HK < G$  olduğundan  $x^{-1} \in HK$  olup  $x^{-1} = hk$  olacak şekilde  $\exists h \in H$  ve  $\exists k \in K$  vardır.  $x^{-1} = hk$  olduğundan  $x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1}$  olur. Burada  $h \in H$  ve  $H < G$  olduğundan  $h^{-1} \in H$  olur.  $k \in K$

ve  $K < G$  olduğundan  $k^{-1} \in K$  olur. O halde  $x = k^{-1}h^{-1} \in KH$  olur. Yani  $\forall x \in HK$  için  $x \in KH$  olup

$$HK \subset KH \dots (1)$$

olur. Herhangi  $x \in KH$  alalım.  $x \in KH$  olduğundan  $x = kh$  olacak şekilde  $\exists k \in K$  ve  $\exists h \in H$  vardır.  $x = kh$  olduğundan  $x^{-1} = (kh)^{-1} = h^{-1}k^{-1}$  dir. Burada  $h \in H$  ve  $H < G$  olduğundan  $h^{-1} \in H$  dir.  $k \in K$  ve  $K < G$  olduğundan  $k^{-1} \in K$  olur. O halde  $x^{-1} = h^{-1}k^{-1} \in HK$  için  $HK < G$  olduğundan  $x = (x^{-1})^{-1} \in HK$  bulunur. Yani  $\forall x \in KH$  için  $x \in HK$  olup

$$KH \subset HK \dots (2)$$

elde edilir. (1) ve (2) den  $HK = KH$  sağlanır.

( $\Leftarrow$ )  $HK = KH$  olsun.  $\emptyset \neq H \subset G$  ve  $\emptyset \neq K \subset G$  olduğundan  $\emptyset \neq HK \subset G$  olur. Herhangi  $x, y \in HK$  alalım.  $x, y \in HK$  olduğundan  $x = h_1k_1$  ve  $y = h_2k_2$  olacak şekilde  $\exists h_1, h_2 \in H$  ve  $\exists k_1, k_2 \in K$  vardır.  $x = h_1k_1$  ve  $y = h_2k_2$  olduğundan  $xy^{-1} = h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$  olur. Burada  $k_1, k_2 \in K$  ve  $K < G$  olduğundan  $k_1k_2^{-1} \in K$  olur.  $h_2 \in H$  elemanı için  $H < G$  olduğundan  $h_2^{-1} \in H$  dir. O halde  $k_1k_2^{-1}h_2^{-1} \in KH = HK$  olup  $k_1k_2^{-1}h_2^{-1} = h_3k_3$  olacak şekilde  $\exists h_3 \in H$  ve  $\exists k_3 \in K$  vardır.  $k_1k_2^{-1}h_2^{-1} = h_3k_3$  olduğundan  $xy^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h_3k_3$  eşitliği sağlanır. Burada  $h_1, h_3 \in H$  ve  $H < G$  olduğundan  $h_1h_3 \in H$  olup ayrıca  $k_3 \in K$  olduğundan  $xy^{-1} = h_1h_3k_3 \in HK$  olur. Yani  $\forall x, y \in HK$  için  $xy^{-1} \in HK$  olup Teorem 2.2.6 dan  $HK < G$  olur.

**Örnek 1.**  $S$  boştan farklı bir küme olmak üzere  $S$  kümesinde  $*$  işlemi  $\forall a, b \in S$  için  $a * b = a$  ile tanımlansın.  $*$  işleminin birleşmeli olduğunu gösteriniz.

**Çözüm.**  $*$  işleminin  $S$  de bir iç işlem olduğu açıktır. Burada  $*$  işleminin tanımından  $\forall a, b, c \in S$  için  $a * (b * c) = a$  ve  $(a * b) * c = a * c = a$  olup  $a * (b * c) = a = (a * b) * c$  olur. O halde  $*$  işlemi birleşmeli olup istenen elde edilir.

**Örnek 2.**  $(G, \circ)$  bir grup olsun.  $G$  kümesinde  $*$  işlemi  $\forall a, b \in G$  için  $a * b = b \circ a$  olarak tanımlansın.  $(G, *)$  cebirsel yapısının bir grup olduğunu gösteriniz.

**Çözüm.**  $*$  işleminin  $G$  de bir iç işlem olduğu açıktır.  $*$  işleminin tanımı ve  $\circ$  işleminin birleşme özelliğinden  $\forall a, b, c \in G$  için  $a * (b * c) = a * (c \circ b) = (c \circ b) \circ a = c \circ (b \circ a) = (b \circ a) * c = (a * b) * c$  eşitlikleri sağlandığından  $*$  işleminin  $G$  de birleşme özelliği vardır.

$G$  nin  $\circ$  işlemine göre birim elemanı  $e$  olsun. Bu durumda  $*$  işleminin tanımından  $\forall a \in G$  için  $a * e = e \circ a = a$  ve  $e * a = a \circ e = a$  eşitlikleri sağlandığından  $e$  elemanı  $G$  nin  $*$  işlemine göre de birim elemanıdır.

Herhangi  $a \in G$  alalım.  $(G, \circ)$  bir grup olduğundan  $a$  elemanının  $G$  de  $\circ$  işlemine göre tersi vardır.  $a$  elemanının  $G$  de  $\circ$  işlemine göre tersi  $x$  olsun.  $*$  işleminin tanımından  $a * x = x \circ a = e$  ve  $x * a = a \circ x = e$  olup  $x$  elemanı  $a$  nın  $*$  işlemine göre de tersi olur. Yani  $G$  deki her elemanın  $G$  de  $*$  işlemine göre tersi vardır.

Böylece  $(G, *)$  cebirsel yapısı bir grup olup istenen elde edilir.

**Örnek 3.**  $G$  bir grup  $a, b \in G$  ve  $a^3b = ba^3$  olsun. Eğer  $a^5 = e$  ise  $ab = ba$  olduğunu gösteriniz.

**Çözüm.**  $a^5 = e$  olsun. Bu durumda  $a^6 = a$  olup  $a^3b = ba^3$  olduğundan  $ab = a^6b = a^3a^3b = a^3ba^3 = ba^3a^3 = ba^6 = ba$  olur ki bu da istenendir.

**Ödev.**  $m, n \in \mathbb{Z}^+$  olmak üzere  $m \times n$  tipindeki reel matrisler kümesinin matrislerde toplama işlemine göre değişmeli grup olduğunu gösteriniz.

**Örnek 5.**  $G$  değişmeli grup ve  $n \in \mathbb{Z}^+$  olsun.  $G_n = \{a \in G \mid \exists x \in G \text{ için } a = x^n\}$  kümesinin  $G$  nin bir alt grubu olduğunu gösteriniz.

**Çözüm.**  $e = e^n$  olduğundan  $e \in G_n$  olup  $G_n \neq \emptyset$  olur. Ayrıca  $G_n \subset G$  olduğu da açıktır. Yani  $\emptyset \neq G_n \subset G$  olur. Herhangi  $a, b \in G_n$  alalım.  $a, b \in G_n$  olduğundan  $a = x^n$  ve  $b = y^n$  olacak şekilde  $\exists x, y \in G$  vardır.  $x, y \in G$  ve  $G$  bir grup olduğundan  $xy^{-1} \in G$  olur. Burada  $G$  değişmeli olduğundan  $ab^{-1} = x^n(y^n)^{-1} = x^n y^{-n} = x^n (y^{-1})^n = (xy^{-1})^n$  olup  $xy^{-1} \in G$  olduğundan  $G_n$  nin tanımından  $ab^{-1} \in G_n$  olur. Yani  $\forall a, b \in G_n$  için  $ab^{-1} \in G_n$  olup Teorem 2.2.6 dan  $G_n < G$  olur.

## 2.3. DEVİRLİ GRUPLAR

**Tanım 2.3.1.**  $G$  bir grup ve  $M$ ,  $G$  nin bir alt kümesi olsun.  $G$  nin  $M$  yi kapsayan bütün alt gruplarının kesişimine  **$M$  nin ürettiği (doğurduğu) alt grup** denir ve genellikle  $\langle M \rangle$  ile ifade edilir.  $M$  nin elemanlarına da  $\langle M \rangle$  grubunun **üreteçleri (doğurayları)** denir.

**Not.**  $H < G$  ve  $M \subset H$  ise tanımdan  $\langle M \rangle \subset H$  olduğu anlaşılır. Dolayısıyla  $\langle M \rangle$ ,  $G$  nin  $M$  yi kapsayan en küçük alt grubudur.

**Not.**  $G$  bir grup ve  $M = \emptyset$  ise  $\langle M \rangle = \{e\}$  dir.

**Teorem 2.3.2.**  $G$  bir grup ve  $\emptyset \neq M \subset G$  olsun. Bu durumda

$$\langle M \rangle = \{a_1^{n_1} a_2^{n_2} \dots a_r^{n_r} \mid r \in \mathbb{Z}^+, n_1, n_2, \dots, n_r \in \mathbb{Z}, a_1, a_2, \dots, a_r \in M\} \text{ olur.}$$

**İspat.**  $A = \{a_1^{n_1} a_2^{n_2} \dots a_r^{n_r} \mid r \in \mathbb{Z}^+, n_1, n_2, \dots, n_r \in \mathbb{Z}, a_1, a_2, \dots, a_r \in M\}$  diyelim.  $\forall a \in M$  için  $a = a^1 \in A$  olup  $M \subset A$  olur. Burada  $M \neq \emptyset$  olduğundan  $A \neq \emptyset$  olur. Ayrıca  $A \subset G$  olduğu da açıktır. Yani  $\emptyset \neq A \subset G$  olur.

Herhangi  $x, y \in A$  alalım.  $x, y \in A$  olduğundan  $x = a_1^{n_1} a_2^{n_2} \dots a_r^{n_r}$  ve  $y = b_1^{m_1} b_2^{m_2} \dots b_s^{m_s}$  olacak şekilde  $\exists r, s \in \mathbb{Z}^+, \exists n_1, n_2, \dots, n_r, m_1, m_2, \dots, m_s \in \mathbb{Z}$  ve  $\exists a_1, a_2, \dots, a_r, b_1, b_2, \dots, b_s \in M$  vardır.  $x = a_1^{n_1} a_2^{n_2} \dots a_r^{n_r}$  ve  $y = b_1^{m_1} b_2^{m_2} \dots b_s^{m_s}$  olduğundan

$$xy^{-1} = a_1^{n_1} a_2^{n_2} \dots a_r^{n_r} (b_1^{m_1} b_2^{m_2} \dots b_s^{m_s})^{-1} = a_1^{n_1} a_2^{n_2} \dots a_r^{n_r} b_s^{-m_s} b_{s-1}^{-m_{s-1}} \dots b_1^{-m_1}$$

olup burada  $n_1, n_2, \dots, n_r, -m_s, -m_{s-1}, \dots, -m_1 \in \mathbb{Z}$  ve  $a_1, a_2, \dots, a_r, b_s, b_{s-1}, \dots, b_1 \in M$  olduğundan  $A$  nın tanımından

$$xy^{-1} = a_1^{n_1} a_2^{n_2} \dots a_r^{n_r} b_s^{-m_s} b_{s-1}^{-m_{s-1}} \dots b_1^{-m_1} \in A$$

olur. Yani  $\forall x, y \in A$  için  $xy^{-1} \in A$  olup Teorem 2.2.6 dan  $A < G$  olur.  $M \subset A$  ve  $A < G$  olduğundan  $\langle M \rangle \subset A$  olur.

Herhangi  $x \in A$  alalım.  $x \in A$  olduğundan  $x = a_1^{n_1} a_2^{n_2} \dots a_r^{n_r}$  olacak şekilde  $\exists r \in \mathbb{Z}^+, \exists n_1, n_2, \dots, n_r \in \mathbb{Z}$  ve  $\exists a_1, a_2, \dots, a_r \in M$  vardır. Burada  $a_1, a_2, \dots, a_r \in M$  ve  $M \subset \langle M \rangle$  olduğundan  $a_1, a_2, \dots, a_r \in \langle M \rangle$  olup  $\langle M \rangle < G$  olduğundan  $x = a_1^{n_1} a_2^{n_2} \dots a_r^{n_r} \in \langle M \rangle$  olur. Yani  $\forall x \in A$  için  $x \in \langle M \rangle$  olup  $A \subset \langle M \rangle$  olur. Ayrıca  $\langle M \rangle \subset A$  olduğundan  $\langle M \rangle = A = \{a_1^{n_1} a_2^{n_2} \dots a_r^{n_r} \mid r \in \mathbb{Z}^+, n_1, n_2, \dots, n_r \in \mathbb{Z}, a_1, a_2, \dots, a_r \in M\}$  olup istenen elde edilir.

**Tanım 2.3.3.**  $G$  bir grup ve  $M \subset G$  olmak üzere  $G = \langle M \rangle$  ise  $G$  ye  **$M$  ile üretilmiş grup** denir.  $G = \langle M \rangle$  olacak şekilde  $G$  nin sonlu elemanlı bir  $M$  alt kümesi varsa  $G$  ye **sonlu üretilmiş grup** denir. Eğer  $G = \langle \{a\} \rangle$  olacak şekilde  $\exists a \in G$  varsa  $G$  ye  **$a$  elemanı ile üretilmiş devirli grup** denir ve genellikle  $G = \langle a \rangle$  olarak yazılır.

**Not.** Teorem 2.3.2 den  $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$  olur. Eğer burada  $G$  toplamsal grup olarak alınırsa  $a$  elemanının ürettiği devirli grup  $\langle a \rangle = \{na | n \in \mathbb{Z}\}$  olur.

**Teorem 2.3.4.**  $G = \langle a \rangle$  devirli bir grup olsun. Bu takdirde  $G$  nin mertebesinin sonlu olması için gerek ve yeter koşul  $a$  nın bazı farklı pozitif tam sayı kuvvetlerinin aynı olmasıdır.

**İspat.** ( $\Rightarrow$ )  $G$  nin mertebesi sonlu olsun. Eğer  $a$  nın bütün pozitif tam sayı kuvvetleri birbirinden farklı olsa  $a, a^2, a^3, \dots, a^n, \dots$  elemanlarının hepsi birbirinden farklı olup bunların sayısı sonlu olmadığından ve bu elemanların hepsi  $G$  nin elemanları olduğundan bu durum  $G$  nin mertebesinin sonlu olmasıyla çelişir. O halde  $a$  nın bazı farklı pozitif tam sayı kuvvetleri eşit olup istenen elde edilir.

( $\Leftarrow$ )  $a$  nın bazı farklı pozitif tam sayı kuvvetleri eşit olsun. Bu durumda  $a^{m_1} = a^{m_2}$  ve  $m_1 \neq m_2$  olacak şekilde  $\exists m_1, m_2 \in \mathbb{Z}^+$  vardır.  $m_1 \neq m_2$  olduğundan  $|m_1 - m_2| \in \mathbb{Z}^+$  olur.  $a^{m_1} = a^{m_2}$  olduğundan  $a^{m_1 - m_2} = e$  ve  $a^{m_2 - m_1} = e$  olup  $a^{|m_1 - m_2|} = e$  olur.  $A = \{k \in \mathbb{Z}^+ | a^k = e\}$  kümesini tanımlayalım.  $|m_1 - m_2| \in \mathbb{Z}^+$  ve  $a^{|m_1 - m_2|} = e$  olduğundan  $A$  nın tanımından  $|m_1 - m_2| \in A$  olup  $A \neq \emptyset$  bulunur. Ayrıca  $A \subset \mathbb{Z}^+$  olduğu da açıktır. O halde  $A$  kümesi bir en küçük  $t$  elemanına sahiptir (Çünkü pozitif tam sayılar kümesi iyi sıralıdır).  $t \in A$  olduğundan  $t \in \mathbb{Z}^+$  ve  $a^t = e$  olur.  $G$  nin  $a, a^2, \dots, a^t = e$  elemanlarını göz önüne alalım.  $s_1, s_2 \in \mathbb{Z}^+$  ve  $1 \leq s_1, s_2 \leq t$  olmak üzere  $a^{s_1} = a^{s_2}$  olsun.  $a^{s_1} = a^{s_2}$  olduğundan  $a^{s_1 - s_2} = e$  ve  $a^{s_2 - s_1} = e$  olup  $a^{|s_1 - s_2|} = e$  bulunur.  $1 \leq s_1, s_2 \leq t$  olduğundan  $|s_1 - s_2| < t$  olur. Eğer burada  $|s_1 - s_2| \neq 0$  olsa  $|s_1 - s_2| \in \mathbb{Z}^+$  olup ayrıca  $a^{|s_1 - s_2|} = e$  olduğundan  $|s_1 - s_2| \in A$  olur ki bu da  $t$  sayısının  $A$  nın en küçük elemanı olmasıyla çelişir. O halde  $|s_1 - s_2| = 0$  olup  $s_1 = s_2$  elde edilir. Böylece  $a, a^2, \dots, a^t = e$  elemanları birbirinden farklı olur. Şimdi  $H = \{a, a^2, \dots, a^t = e\}$  diyelim. Burada  $H \subset G$  olduğu açıktır. Herhangi  $x \in G$  alalım.  $x \in G = \langle a \rangle$  olduğundan  $x = a^n$  olacak şekilde  $\exists n \in \mathbb{Z}$  vardır. Burada  $t > 0$  olduğundan  $n$  ile  $t$  ye kalanlı bölme uygulanırsa bu durumda  $n = qt + r$  ve  $0 \leq r < t$  olacak şekilde  $\exists q, r \in \mathbb{Z}$  vardır.  $a^t = e$  olduğundan  $x = a^n = a^{qt+r} = a^{qt} a^r = (a^t)^q a^r = e^q a^r = a^r$  olur. Burada eğer  $r = 0$  olsa  $x = a^r = a^0 = e = a^t \in H$  olur. Eğer  $r \neq 0$  olsa ayrıca  $0 \leq r < t$  olduğundan  $1 \leq r < t$  olup yine  $x = a^r \in H = \{a, a^2, \dots, a^t = e\}$  olur. Yani  $\forall x \in G$  için  $x \in H$  olup  $G \subset H$  olur. Ayrıca  $H \subset G$  olduğundan  $G = H = \{a, a^2, \dots, a^t = e\}$  olup  $G$  nin mertebesi sonlu ( $\circ(G) = t$ ) olur.

**Sonuç 2.3.5.**  $G = \langle a \rangle, t$ . mertebeden devirli bir grup olsun. Bu durumda  $t, a^k = e$  olan  $k$  pozitif tam sayıların en küçüğüdür. Ayrıca  $G = \{a, a^2, \dots, a^t = e\}$  olur.

**Teorem 2.3.6.** Devirli bir grubun her alt grubu da devirlidir.

**İspat.**  $G = \langle a \rangle$  devirli bir grup ve  $H < G$  olsun.  $H$  nin de devirli olduğu gösterilirse istenen elde edilir. Eğer burada  $H = \{e\}$  ise  $H = \langle e \rangle$  olup devirlidir. Kabul edelim ki  $H \neq \{e\}$  olsun.  $H \neq \{e\}$  olduğundan  $\exists e \neq x \in H$  vardır.  $x \in H$  ve  $H < G$  olduğundan  $x \in G = \langle a \rangle$  olup  $x = a^s$  olacak şekilde  $\exists s \in \mathbb{Z}$  vardır. Burada  $x \neq e$  olduğundan  $s \neq 0$  olur.  $a^s = x \in H$  ve  $H < G$  olduğundan  $a^{-s} = x^{-1} \in H$  olur.  $a^s, a^{-s} \in H$  olduğundan  $a^{|s|} \in H$  olur.  $s \neq 0$  olduğundan  $|s| \in \mathbb{Z}^+$  olur.  $A = \{k \in \mathbb{Z}^+ \mid a^k \in H\}$  kümesini tanımlayalım.  $|s| \in \mathbb{Z}^+$  ve  $a^{|s|} \in H$  olduğundan  $|s| \in A$  olup  $A \neq \emptyset$  olur. Ayrıca  $A \subset \mathbb{Z}^+$  olduğu da açıktır. O halde  $A$  kümesi bir en küçük  $t$  elemanına sahiptir.  $t \in A$  olduğundan  $t \in \mathbb{Z}^+$  ve  $a^t \in H$  olur.  $a^t \in H$  ve  $H < G$  olduğundan  $\langle a^t \rangle \subset H$  kapsaması elde edilir. Herhangi  $x \in H$  alalım.  $x \in H < G = \langle a \rangle$  olduğundan  $x = a^n$  olacak şekilde  $\exists n \in \mathbb{Z}$  vardır.  $t \in \mathbb{Z}^+$  olduğundan  $n$  sayısı ile  $t$  ye kalanlı bölme uygulanırsa bu durumda  $n = qt + r$  ve  $0 \leq r < t$  olacak şekilde  $\exists q, r \in \mathbb{Z}$  vardır. Burada  $x = a^n = a^{qt+r} = (a^t)^q a^r$  olup  $a^r = (a^t)^{-q} x$  eşitliği sağlanır.  $a^t, x \in H$  ve  $H < G$  olduğundan  $a^r = (a^t)^{-q} x \in H$  bulunur. Burada eğer  $r \neq 0$  olsa  $0 < r < t$  olup  $a^r \in H$  olduğundan  $A$  nın tanımından  $r \in A$  olur ki bu da  $t$  sayısının  $A$  nın en küçük elemanı olmasıyla çelişir. O halde  $r = 0$  olup  $n = qt + r = qt$  ve  $x = a^n = a^{qt} = (a^t)^q \in \langle a^t \rangle$  dir. Yani  $\forall x \in H$  için  $x \in \langle a^t \rangle$  olup  $H \subset \langle a^t \rangle$  olur. Ayrıca  $\langle a^t \rangle \subset H$  olduğundan  $H = \langle a^t \rangle$  olup  $H$  devirlidir.

**Teorem 2.3.7.**  $G = \langle a \rangle$  sonsuz devirli bir grup ise  $G$  nin  $\{e\}$  den farklı her alt grubu da sonsuz devirli bir gruptur.

**İspat.**  $G = \langle a \rangle$  sonsuz devirli bir grup,  $H < G$  ve  $H \neq \{e\}$  olsun. Teorem 2.3.6 dan  $H$  de devirli olup  $H = \langle b \rangle$  olacak şekilde  $\exists b \in H$  vardır. Şimdi  $H$  nin mertebesinin sonlu olmadığı gösterilirse istenen elde edilir. Aksini kabul edelim. Yani  $H$  nin mertebesinin sonlu olduğunu kabul edelim. Bu durumda Teorem 2.3.4 den  $b^{s_1} = b^{s_2}$  ve  $s_1 \neq s_2$  olacak şekilde  $\exists s_1, s_2 \in \mathbb{Z}$  vardır.  $H = \langle b \rangle$  ve  $H \neq \{e\}$  olduğundan  $b \neq e$  olur.  $b \in H < G = \langle a \rangle$  olduğundan  $b = a^n$  olacak şekilde  $\exists n \in \mathbb{Z}$  vardır.  $b = a^n$  ve  $b \neq e$  olduğundan  $n \neq 0$  olur.  $s_1 \neq s_2$  ve  $n \neq 0$  olduğundan  $ns_1 \neq ns_2$  olur.  $b = a^n$  ve  $b^{s_1} = b^{s_2}$  olduğundan  $a^{ns_1} = (a^n)^{s_1} = b^{s_1} = b^{s_2} = (a^n)^{s_2} = a^{ns_2}$  olup  $ns_1 \neq ns_2$  ve  $G = \langle a \rangle$  olduğundan Teorem 2.3.4 gereği  $G$  nin mertebesi sonlu olur ki bu da  $G$  nin sonsuz devirli grup olmasıyla çelişir. O halde kabulümüz yanlış olup  $H$  nin mertebesi sonlu değildir.

**Teorem 2.3.8.**  $G = \langle a \rangle$ ,  $n$ . mertebeden devirli bir grup ise  $G$  nin her alt grubunun mertebesi  $n$  yi böler ve  $n$  nin her pozitif  $q$  böleni için  $G$  nin mertebesi  $q$  olan bir ve yalnız bir tane alt grubu vardır. Eğer burada  $s \in \mathbb{Z}^+$  olmak üzere  $n = sq$  ise bu mertebesi  $q$  olan alt grup  $\langle a^s \rangle$  olur.

**İspat.**  $G$  nin herhangi  $A$  alt grubunu alalım. Teorem 2.3.6 dan  $A$  da devirli olup  $A = \langle a^x \rangle$  olacak şekilde  $\exists x \in \mathbb{Z}$  vardır.  $\circ(A) = m$  diyelim.  $\circ(A) = m$  olduğundan  $m$  sayısı  $a^{xk} = (a^x)^k = e$  koşuluna uyan  $k$  pozitif tam sayıların en küçüğüdür.  $\circ(G) = n$  olduğundan Sonuç 2.3.5 gereği  $n$  sayısı  $a^k = e$  koşuluna uyan  $k$  pozitif tam sayıların en küçüğüdür.  $m \in \mathbb{Z}^+$  olduğundan  $n$  sayısı ile  $m$  ye kalanlı bölme uygulanırsa bu durumda  $n = qm + r$  ve  $0 \leq r < m$  olacak şekilde  $\exists q, r \in \mathbb{Z}$  vardır. Burada  $e = e^x = (a^n)^x = a^{xn} = a^{x(qm+r)} = (a^{xm})^q a^{xr} = e^q a^{xr} = a^{xr}$  olur.  $a^{xr} = e$ ,  $0 \leq r < m$  ve  $m$  sayısı  $a^{xk} = e$  koşuluna uyan  $k$  pozitif tam sayıların en küçüğü olduğundan  $r = 0$  olup  $n = qm + r = qm$  ve buradan da  $\circ(A) = m | n$  elde edilir. Yani  $G$  nin her alt grubunun mertebesi  $n$  yi böler.

Şimdi  $n$  nin herhangi  $q$  pozitif bölenini alalım.  $s \in \mathbb{Z}^+$  olmak üzere  $n = sq$  olsun.  $H = \langle a^s \rangle$  ve  $\circ(H) = t$  diyelim.  $\circ(G) = n$  olduğundan Sonuç 2.3.5 den  $n$  sayısı  $a^k = e$  koşuluna uyan  $k$  pozitif tam sayıların en küçüğüdür.  $\circ(H) = t$  olduğundan  $t$  sayısı  $a^{sk} = (a^s)^k = e$  koşuluna uyan  $k$  pozitif tam sayıların en küçüğü olup  $q \in \mathbb{Z}^+$  ve  $a^{sq} = a^n = e$  olduğundan  $t \leq q$  olur.  $a^{st} = e$ ,  $st \in \mathbb{Z}^+$  ve  $n$  sayısı  $a^k = e$  koşuluna uyan  $k$  pozitif tam sayıların en küçüğü olduğundan  $sq = n \leq st$  olup burada  $s \in \mathbb{Z}^+$  olduğundan  $q \leq t$  olur.  $t \leq q$  ve  $q \leq t$  olduğundan  $\circ(H) = t = q$  olur. Son olarak  $G$  nin mertebesi  $q$  olan herhangi  $K$  alt grubunu alalım.  $K = H$  olduğu gösterilirse istenen elde edilir.  $K < G = \langle a \rangle$  olduğundan Teorem 2.3.6 dan  $K$  da devirli olup  $K = \langle a^y \rangle$  olacak şekilde  $\exists y \in \mathbb{Z}$  vardır.  $s \in \mathbb{Z}^+$  olduğundan  $y$  sayısı ile  $s$  ye kalanlı bölme uygulanırsa bu durumda  $y = ps + r$  ve  $0 \leq r < s$  olacak şekilde  $\exists p, r \in \mathbb{Z}$  vardır.  $\circ(K) = q$  olduğundan  $a^{yq} = (a^y)^q = e$  olup  $y = ps + r$  ve  $a^{sq} = a^n = e$  olduğundan  $e = a^{yq} = a^{(ps+r)q} = a^{psq} a^{rq} = (a^{sq})^p a^{rq} = e^p a^{rq} = a^{rq}$  eşitliği sağlanır. Eğer burada  $r \neq 0$  olsa  $0 < r < s$  olup  $q > 0$  olduğundan  $0 < rq < sq = n$  bulunur. Burada  $a^{rq} = e$  olduğundan bu durum  $n$  sayısının  $a^k = e$  koşuluna uyan  $k$  pozitif tam sayıların en küçüğü olmasıyla çelişir. O halde  $r = 0$  olup  $y = ps + r = ps + 0 = ps$  dir. Bu durumda  $a^y = a^{ps} = (a^s)^p \in \langle a^s \rangle = H$  olup  $H < G$  olduğundan  $K = \langle a^y \rangle \subset H$  olur.  $K \subset H$  ve  $\circ(K) = \circ(H) = q$  olduğu göz önüne alınırsa  $K = H$  olup istenen elde edilir.

**Tanım 2.3.9.**  $G$  bir grup ve  $a \in G$  olsun.  $a$  elemanının ürettiği  $\langle a \rangle$  devirli grubunun mertebesine  **$a$  elemanının mertebesi** denir ve genellikle  $\circ(a)$  ile gösterilir.

**Not.** O halde  $\circ(a)$ ,  $a^n = e$  koşulunu sağlayan  $n > 0$  tam sayılarının arasında en küçüğüdür. Toplamsal gruplarda  $\circ(a)$ ,  $na = e$  koşulunu sağlayan  $n > 0$  tam sayılarının en küçüğüdür.

**Teorem 2.3.10.**  $G$  bir grup,  $a \in G$  ve  $\circ(a) = n$  olsun.  $m \in \mathbb{Z}$  olmak üzere  $a^m = e$  olması için gerek ve yeter koşul  $n|m$  olmasıdır.

**İspat.**  $(\Rightarrow)$   $a^m = e$  olsun.  $\circ(a) = n$  olduğundan  $n$  sayısı  $a^k = e$  olan  $k$  pozitif tam sayıların en küçüğüdür.  $n \in \mathbb{Z}^+$  olduğundan  $m$  sayısı  $n$  ile kalanlı olarak bölünebilir. Bu durumda  $m = qn + r$  ve  $0 \leq r < n$  olacak şekilde  $\exists q, r \in \mathbb{Z}$  vardır.  $a^m = a^n = e$  ve  $m = qn + r$  olduğundan  $e = a^m = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r$  olur. Eğer burada  $r \neq 0$  olsa  $0 < r < n$  olup  $a^r = e$  olduğundan bu durum  $n$  sayısının  $a^k = e$  olan  $k$  pozitif tam sayıların en küçüğü olmasıyla çelişir. O halde  $r = 0$  olup  $m = qn + r = qn$  ve buradan da  $n|m$  elde edilir.

$(\Leftarrow)$   $n|m$  olsun. Bu durumda  $m = nc$  olacak şekilde  $\exists c \in \mathbb{Z}$  vardır.  $\circ(a) = n$  olduğundan  $a^n = e$  olur. Bu durumda  $m = nc$  olduğundan  $a^m = a^{nc} = (a^n)^c = e^c = e$  olup istenen elde edilir.

**Teorem 2.3.11.**  $G = \langle a \rangle, n$ . mertebeden devirli bir grup olsun.  $s \in \mathbb{Z}$  olmak üzere  $a^s$  elemanının  $G$  nin bir üretici (yani  $G = \langle a^s \rangle$ ) olması için gerek ve yeter koşul  $(s, n) = 1$  olmasıdır.

**İspat.**  $(\Rightarrow)$   $s \in \mathbb{Z}$  olmak üzere  $G = \langle a^s \rangle$  olsun.  $a \in G = \langle a^s \rangle$  olduğundan  $a = (a^s)^x = a^{sx}$  olacak şekilde  $\exists x \in \mathbb{Z}$  vardır.  $a = a^{sx}$  olduğundan  $a^{1-sx} = e$  olup  $\circ(a) = \circ(G) = n$  olduğundan Teorem 2.3.10 dan  $n|1-sx$  olur.  $n|1-sx$  olduğundan  $1-sx = ny$  olacak şekilde  $\exists y \in \mathbb{Z}$  vardır.  $1-sx = ny$  olduğundan  $sx + ny = 1$  olup burada  $x, y \in \mathbb{Z}$  olduğundan Önerme 1.5.16 dan  $(s, n) = 1$  bulunur.

$(\Leftarrow)$   $(s, n) = 1$  olsun. Bu durumda Önerme 1.5.16 dan  $sx + ny = 1$  olacak şekilde  $\exists x, y \in \mathbb{Z}$  vardır.  $\circ(a) = \circ(G) = n$  olduğundan  $a^n = e$  bulunur. O halde  $a = a^1 = a^{sx+ny} = (a^s)^x (a^n)^y = (a^s)^x e^y = (a^s)^x \in \langle a^s \rangle$  olup  $\langle a^s \rangle < G$  olduğundan  $G = \langle a \rangle \subset \langle a^s \rangle$  kapsamı elde edilir. Ayrıca  $\langle a^s \rangle \subset G$  olduğundan  $G = \langle a^s \rangle$  bulunur. Böylece  $a^s$  elemanının  $G$  nin üretici olduğu görülür.

**Teorem 2.3.12.**  $G = \langle a \rangle$  sonsuz devirli bir grup ise üreticileri sadece  $a$  ve  $a^{-1}$  olur.

**İspat.**  $G = \langle a \rangle$  sonsuz devirli bir grup olsun.  $a = (a^{-1})^{-1} \in \langle a^{-1} \rangle$  ve  $\langle a^{-1} \rangle < G$  olduğundan  $G = \langle a \rangle \subset \langle a^{-1} \rangle$  olup ayrıca  $\langle a^{-1} \rangle \subset G$  olduğundan  $G = \langle a^{-1} \rangle$  eşitliği elde edilir. Şimdi  $s \in \mathbb{Z}$  olmak üzere  $G = \langle a^s \rangle$  olsun.  $s = 1$  veya  $s = -1$  olduğu gösterilirse istenen elde edilir.  $a \in G = \langle a^s \rangle$  olduğundan  $a = (a^s)^x = a^{sx}$  olacak şekilde  $\exists x \in \mathbb{Z}$  vardır. Eğer burada  $1 \neq sx$  olsa  $a^1 = a = a^{sx}$  ve  $G = \langle a \rangle$  olduğundan Teorem 2.3.4 den  $G$  nin mertebesi sonlu olur ki bu da

$G = \langle a \rangle$  nın sonsuz devirli grup olmasıyla çelişir. O halde  $1 = sx$  iken  $s|1$  olur.  $s|1$  ve 1 in bölenleri sadece 1 ve  $-1$  olduğundan  $s = 1$  veya  $s = -1$  olup istenen elde edilir.

**Örnek.**  $\mathbb{Z}$  tam sayılar kümesi bildiğimiz  $+$  işlemine göre 1 ile üretilmiş sonsuz devirli gruptur.

**Örnek.**  $G = \{1, -1, i, -i\}$  kümesi kompleks sayılarda bildiğimiz çarpma işlemine göre  $i$  elemanı ile üretilmiş 4. mertebeden devirli bir gruptur.

**Örnek.**  $(\mathbb{Z}, +)$  grubunun her alt grubu devirli olduğundan  $(\mathbb{Z}, +)$  grubunun alt grupları  $m \in \mathbb{Z}$  olmak üzere  $\langle m \rangle = m\mathbb{Z} = \{mk | k \in \mathbb{Z}\}$  şeklindedir.

**Örnek.**  $G = \langle a \rangle, 20$ . mertebeden devirli bir grup olsun. Bu grubun

(i) Alt gruplarını belirtiniz.

(ii) Mertebesi 4 olan elemanlarını bulunuz.

(iii) Mertebesi 5 olan elemanlarını bulunuz.

**Çözüm.** (i)  $G = \langle a \rangle, 20$ . mertebeden devirli grup olduğundan Teorem 2.3.8 den  $G$  nin her alt grubunun mertebesi 20 sayısını böler ve 20 nin her pozitif  $q$  böleni için  $G$  nin mertebesi  $q$  olan bir ve yalnız bir alt grubu vardır. Burada  $s \in \mathbb{Z}^+$  olmak üzere  $20 = sq$  ise bu mertebesi  $q$  olan alt grup  $\langle a^s \rangle$  olur. 20 nin pozitif bölenleri 1, 2, 4, 5, 10 ve 20 sayılarıdır. Buna göre,

$20 = 20 \cdot 1$  olduğundan  $G$  nin mertebesi 1 olan alt grubu  $\langle a^{20} \rangle = \{e\}$  ve mertebesi 20 olan alt grubu  $\langle a^1 \rangle = G$  olur,

$20 = 10 \cdot 2$  olduğundan  $G$  nin mertebesi 2 olan alt grubu  $\langle a^{10} \rangle = \{a^{10}, a^{20} = e\}$  ve mertebesi 10 olan alt grubu  $\langle a^2 \rangle = \{a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18}, a^{20} = e\}$  olur,

$20 = 5 \cdot 4$  olduğundan  $G$  nin mertebesi 4 olan alt grubu  $\langle a^5 \rangle = \{a^5, a^{10}, a^{15}, a^{20} = e\}$  ve mertebesi 5 olan alt grubu  $\langle a^4 \rangle = \{a^4, a^8, a^{12}, a^{16}, a^{20} = e\}$  olur.

Sonuç olarak  $G$  nin alt grupları  $\langle a^1 \rangle = G, \langle a^2 \rangle, \langle a^4 \rangle, \langle a^5 \rangle, \langle a^{10} \rangle$  ve  $\langle a^{20} \rangle = \{e\}$  olur.

(ii)  $20 = 5 \cdot 4$  olduğundan Teorem 2.3.8 den  $G$  nin mertebesi 4 olan tek alt grubu  $\langle a^5 \rangle = \{a^5, a^{10}, a^{15}, a^{20} = e\}$  olur. Teorem 2.3.11 gereği  $\langle a^5 \rangle = \{a^5, a^{10}, a^{15}, a^{20} = e\}$  grubunun üreteçleri  $s \in \mathbb{Z}, 1 \leq s \leq 4$  ve  $(s, 4) = 1$  olmak üzere  $(a^5)^s = a^{5s}$  şeklindedir. Burada  $1 \leq s \leq 4$  ve  $(s, 4) = 1$  koşuluna uyan  $s$  tam sayıları 1 ve 3 olduğundan  $G$  nin mertebesi 4 olan elemanları  $a^{5 \cdot 1} = a^5$  ve  $a^{5 \cdot 3} = a^{15}$  olur.

(iii)  $20 = 4 \cdot 5$  olduğundan Teorem 2.3.8 den  $G$  nin mertebesi 5 olan tek alt grubu  $\langle a^4 \rangle = \{a^4, a^8, a^{12}, a^{16}, a^{20} = e\}$  olur. Teorem 2.3.11 gereği  $\langle a^4 \rangle = \{a^4, a^8, a^{12}, a^{16}, a^{20} = e\}$

grubunun üreteçleri  $s \in \mathbb{Z}$ ,  $1 \leq s \leq 5$  ve  $(s, 5) = 1$  olmak üzere  $(a^4)^s = a^{4s}$  şeklindedir. Burada  $1 \leq s \leq 5$  ve  $(s, 5) = 1$  koşuluna uyan  $s$  tam sayıları 1, 2, 3 ve 4 olduğundan  $G$  nin mertebesi 5 olan elemanları  $a^{4 \cdot 1} = a^4$ ,  $a^{4 \cdot 2} = a^8$ ,  $a^{4 \cdot 3} = a^{12}$  ve  $a^{4 \cdot 4} = a^{16}$  olur.

**Not.**  $G = \langle a \rangle$ ,  $n$ . mertebeden devirli bir grup olsun. Bu durumda

- (i)  $G$  nin alt grupları sayısı  $n$  nin pozitif bölenleri sayısıdır.
- (ii)  $G$  nin üreteçleri sayısı  $\varphi(n)$  olur.
- (iii)  $q$ ,  $n$  nin bir pozitif böleni olmak üzere  $G$  nin mertebesi  $q$  olan elemanları sayısı  $\varphi(q)$  olur.

## 2.4. NORMAL ALT GRUPLAR

**Teorem 2.4.1.**  $G$  bir grup ve  $H < G$  olsun.  $G$  de  $\equiv$  bağıntısını  $a, b \in G$  olmak üzere  $a \equiv_R b \pmod{H} \Leftrightarrow ab^{-1} \in H$  ile tanımlayalım. Bu takdirde  $\equiv$  bağıntısı  $G$  de bir denklik bağıntısıdır.

**İspat. Yansıma:**  $\forall a \in G$  için  $aa^{-1} = e \in H$  olduğundan  $a \equiv a \pmod{H}$  olup  $\equiv$  bağıntısının yansıma özelliği vardır.

**Simetri:**  $a \equiv b \pmod{H}$  olan herhangi  $a, b \in G$  alalım.  $a \equiv b \pmod{H}$  olduğundan  $ab^{-1} \in H$  olup  $H < G$  olduğundan  $ba^{-1} = (b^{-1})^{-1}a^{-1} = (ab^{-1})^{-1} \in H$  olur. O halde  $b \equiv a \pmod{H}$  olup  $\equiv$  bağıntısının simetri özelliği vardır.

**Geçişme:**  $a \equiv b \pmod{H}$  ve  $b \equiv c \pmod{H}$  olan herhangi  $a, b, c \in G$  alalım.  $a \equiv b \pmod{H}$  ve  $b \equiv c \pmod{H}$  olduğundan  $ab^{-1}, bc^{-1} \in H$  olup  $H < G$  olduğundan  $ac^{-1} = ab^{-1}bc^{-1} \in H$  olur. O halde  $a \equiv c \pmod{H}$  olup  $\equiv$  bağıntısının geçişme özelliği vardır.

Böylece  $\equiv$  bağıntısı  $G$  de bir denklik bağıntısı olup istenen elde edilir.

**Teorem 2.4.2.** Yukarıdaki  $\equiv$  denklik bağıntısına göre bir  $a \in G$  elemanının denklik sınıfı  $G$  nin  $\bar{a} = Ha = \{ha | h \in H\}$  alt kümesidir.

**İspat.** Herhangi  $x \in \bar{a}$  alalım.  $x \in \bar{a}$  olduğundan  $x \equiv a \pmod{H}$  olup  $xa^{-1} \in H$  olur. Burada  $xa^{-1} = h$  denilirse  $h \in H$  olur.  $xa^{-1} = h$  olduğundan  $x = ha$  olup  $h \in H$  olduğundan  $x = ha \in Ha$  bulunur. O halde

$$\bar{a} \subset Ha \quad (1)$$

kapsaması bulunur. Herhangi  $x \in Ha$  alalım.  $x \in Ha$  olduğundan  $x = ha$  olacak şekilde  $\exists h \in H$  vardır.  $x = ha$  olduğundan  $xa^{-1} = h \in H$  olup  $x \equiv a \pmod{H}$  denkliği sağlanır. O halde  $x \in \bar{a}$  olup

$$Ha \subset \bar{a} \quad (2)$$

kapsaması elde edilir. (1) ve (2) den  $\bar{a} = Ha = \{ha|h \in H\}$  olup  $\bar{a} = Ha$  eşitliği sağlanır.

**Teorem 2.4.3.**  $G$  bir grup ve  $H < G$  olsun.  $G$  de  $\equiv_L$  bağıntısı  $a, b \in G$  olmak üzere

$$a \equiv_L b \pmod{H} \Leftrightarrow a^{-1}b \in H$$

ile tanımlansın. Bu takdirde  $\equiv_L$  bağıntısı  $G$  de bir denklik bağıntısıdır ve bu bağıntıya göre bir  $a \in G$  elemanının denklik sınıfı  $G$  nin  $\bar{a} = aH = \{ah|h \in H\}$  alt kümesidir.

**İspat.** Teorem 2.4.1 ve Teorem 2.4.2 nin ispatlarına benzer şekilde yapılır.

Yukarıdaki teoremlerin ifadelerinde geçen  $Ha$  ya  $a$  elemanının  $H$  alt grubuna göre **sağ denklik sınıfı**,  $aH$  ye de  $a$  elemanının  $H$  alt grubuna göre **sol denklik sınıfı** denir.

**Teorem 2.4.4.**  $G$  bir grup,  $H < G$  ve  $H$  sonlu elemanlı olsun. Bu durumda  $H$  alt grubuna göre bütün sağ ve sol denklik sınıflarında sonlu sayıda eleman olup her birinde aynı sayıda eleman bulunur.

**İspat.** Herhangi  $a \in G$  alalım.

$$f: H \rightarrow Ha, x \rightarrow f(x) = xa$$

dönüşümünü tanımlayalım.  $f$  nin bir fonksiyon olduğu açıktır.  $f(x_1) = f(x_2)$  olan herhangi  $x_1, x_2 \in H$  alalım.  $f(x_1) = f(x_2)$  olduğundan  $x_1a = x_2a$  olup kısaltma özelliğinden  $x_1 = x_2$  olur. O halde  $f$  bire-bir olur. Herhangi  $y \in Ha$  alalım.  $y \in Ha$  olduğundan  $y = xa$  olacak şekilde  $\exists x \in H$  vardır. Burada  $f$  nin tanımından  $f(x) = xa = y$  olup  $f$  örtendir.  $f: H \rightarrow Ha$  bire-bir ve örten bir fonksiyon ve  $H$  sonlu elemanlı olduğundan  $Ha$  da sonlu elemanlı ve  $s(Ha) = s(H) = \circ(H)$  olur. Benzer şekilde

$$g: H \rightarrow aH, x \rightarrow g(x) = ax$$

dönüşümünü tanımlayarak  $aH$  kümesinin de sonlu elemanlı ve  $s(aH) = s(H) = \circ(H)$  olduğu benzer şekilde gösterilir. Yani  $H$  alt grubuna göre bütün sağ ve sol denklik sınıflarında sonlu sayıda eleman olup aynı sayıda eleman bulunur.

**Not.**  $H < G$  ise  $He = eH = H$  olduğundan  $H$ ,  $e$  elemanının  $H$  ye göre hem sağ, hem de sol denklik sınıfıdır.

**Teorem 2.4.5 (Lagrange Teoremi).** Sonlu bir grubun her alt grubunun mertebesi grubun mertebesini böler.

**İspat.**  $G$  sonlu bir grup ve  $H < G$  olsun.  $\circ(G) = n$  ve  $\circ(H) = k$  diyelim.  $k|n$  olduğu gösterilirse istenen elde edilir.  $G$  sonlu bir grup olduğundan  $G$  de  $H$  ye göre sağ denklik sınıflarının sayısı da sonludur. Kabul edelim ki  $G$  de  $H$  ye göre birbirinden farklı sağ denklik sınıflarının ailesi  $\{Ha_1, Ha_2, \dots, Ha_t\}$  olsun. Burada  $a_1, a_2, \dots, a_t \in G, t \in \mathbb{Z}^+$  dir. Bu durumda  $\{Ha_1, Ha_2, \dots, Ha_t\}$  ailesi  $G$  nin bir ayrışımıdır. Bir küme üzerindeki denklik bağıntısına göre oluşan denklik sınıfları,  $\circ$  kümenin bir ayrışımını verdiği için  $n = s(G) = s(Ha_1) + s(Ha_2) + \dots + s(Ha_t)$  yazılır. Diğer taraftan Teorem 2.4.4 den  $1 \leq i \leq t$  için  $s(Ha_i) = \circ(H) = k$  olur. O halde  $n = s(Ha_1) + s(Ha_2) + \dots + s(Ha_t) = \underbrace{k + k + \dots + k}_{t \text{ tane}} = kt$  eşitliğinden  $k|n$  olur ki bu da istenendir.

**Sonuç 2.4.6.**  $G$  sonlu bir grup ve  $H < G$  ise  $G$  de  $H$  alt grubuna göre sağ ve sol denklik sınıflarının sayısı aynıdır. Bu sayıya  $H$  alt grubunun  $G$  içindeki **indeksi** denir ve genellikle  $(G:H)$  ile gösterilir. Ayrıca  $(G:H) = \frac{\circ(G)}{\circ(H)}$  olur.

**İspat.**  $G = \bigcup_{i=1}^t Ha_i$  ve her sağ denklik sınıfında aynı sayıda,  $\circ(H)$  eleman olduğundan istenen elde edilir.

**Sonuç 2.4.7.**  $G$  sonlu grup ve  $\circ(G) = n$  ise  $\forall a \in G$  için  $\circ(a)|n$  dir. Böylece  $a^n = e$  olur.

**İspat.**  $a \in G$  ve  $H = \langle a \rangle < G$  olsun. Lagrange Teoremine göre  $m = \circ(H) = \circ(a) | \circ(G) = n$  olur. Bölünebilme tanımı gereği  $n = mt$  olacak şekilde  $t \in \mathbb{Z}$  vardır. Dolayısıyla  $a^n = (a^m)^t = e$  bulunur.

**Teorem 2.4.8.**  $N < G$  olsun. Aşağıdaki ifadeler birbirine denktir:

(i)  $\forall a \in G$  ve  $\forall x \in N$  için  $axa^{-1} \in N$  dir.

(ii)  $\forall a \in G$  için  $aNa^{-1} \subset N$  dir.

(iii)  $\forall a \in G$  için  $aNa^{-1} = N$  dir.

(iv)  $\forall a \in G$  için  $aN = Na$  dir.

**İspat.** (i)  $\Rightarrow$  (ii)  $\forall a \in G$  ve  $\forall x \in N$  için  $axa^{-1} \in N$  olsun. Bu durumda  $\forall a \in G$  için  $aNa^{-1} = \{axa^{-1} | x \in N\} \subset N$  olup istenen elde edilir.

(ii)  $\Rightarrow$  (iii)  $\forall a \in G$  için  $aNa^{-1} \subset N$  olsun. Herhangi  $a \in G$  alalım. Hipotezden  $aNa^{-1} \subset N$  olur.  $a^{-1} \in G$  olduğundan hipotezden  $a^{-1}Na = a^{-1}N(a^{-1})^{-1} \subset N$  olur. Herhangi  $x \in N$

alalım.  $y = a^{-1}xa$  diyelim. Burada  $y = a^{-1}xa \in a^{-1}Na$  için  $a^{-1}Na \subset N$  olduğundan  $y \in N$  olur. Bu durumda  $x = aa^{-1}xaa^{-1} = aya^{-1} \in aNa^{-1}$  olduğundan  $N \subset aNa^{-1}$  kapsaması bulunur. Ayrıca  $aNa^{-1} \subset N$  olduğundan  $aNa^{-1} = N$  eşitliği elde edilir. Yani  $\forall a \in G$  için  $aNa^{-1} = N$  olup istenen elde edilir.

(iii)  $\Rightarrow$  (iv)  $\forall a \in G$  için  $aNa^{-1} = N$  olsun. Herhangi  $a \in G$  alalım.  $aN = Na$  olduğu gösterilirse istenen elde edilir. Hipotezden  $aNa^{-1} = N$  olur. Herhangi  $x \in aN$  alalım.  $x \in aN$  olduğundan  $x = an$  olacak şekilde  $\exists n \in N$  vardır.  $x = an$  olduğundan  $xa^{-1} = ana^{-1} \in aNa^{-1} = N$  iken  $m = xa^{-1}$  denilirse  $m \in N$  olur. O halde  $x = xa^{-1}a = ma \in Na$  olup

$$aN \subset Na \dots (1)$$

kapsaması bulunur. Herhangi  $x \in Na$  alalım.  $x \in Na$  olduğundan  $x = na$  olacak şekilde  $\exists n \in N$  vardır.  $x = na$  olduğundan  $xa^{-1} = n \in N = aNa^{-1}$  olup  $xa^{-1} = ata^{-1}$  olacak şekilde  $\exists t \in N$  vardır.  $xa^{-1} = ata^{-1}$  eşitliğinde kısaltma özelliğinden  $x = at \in aN$  olup

$$Na \subset aN \dots (2)$$

kapsaması bulunur. (1) ve (2) den  $aN = Na$  olup istenen elde edilir.

(iv)  $\Rightarrow$  (i)  $\forall a \in G$  için  $aN = Na$  olsun. Herhangi  $a \in G$  ve herhangi  $x \in N$  alalım. Hipotezden  $aN = Na$  olur.  $a \in G$  ve  $x \in N$  olduğundan  $ax \in aN = Na$  olup  $ax = na$  olacak şekilde  $\exists n \in N$  vardır.  $ax = na$  olduğundan  $axa^{-1} = n \in N$  olur. Yani  $\forall a \in G$  ve  $\forall x \in N$  için  $axa^{-1} \in N$  olup istenen elde edilir.

**Tanım 2.4.9.** Teorem 2.4.8 in denk koşullarından birini sağlayan  $G$  nin  $N$  alt grubuna **normal alt grup** denir ve  $N \triangleleft G$  ile ifade edilir.

**Not.**  $G$  bir grup ise  $G \triangleleft G$  ve  $\{e\} \triangleleft G$  olur.

**Not.**  $G$  değişmeli grup ise  $G$  nin her alt grubu normaldir.

**Not.**  $N \triangleleft G$  ise  $N$  ye göre tanımlanan sağ ve sol denklik sınıfları aynıdır.

**Teorem 2.4.10.**  $G$  bir grup olsun.  $G$  nin birtakım normal alt gruplarının kesişimi de bir normal alt gruptur.

**İspat.**  $\{N_i\}_{i \in I}$ ,  $G$  nin normal alt gruplarının bir ailesi olsun.  $\bigcap_{i \in I} N_i \triangleleft G$  olduğu gösterilirse istenen elde edilir.  $\forall i \in I$  için  $N_i \triangleleft G$  olduğundan  $N_i < G$  olup Teorem 2.2.9 dan  $\bigcap_{i \in I} N_i < G$  olur. Herhangi  $a \in G$  ve herhangi  $x \in \bigcap_{i \in I} N_i$  alalım.  $x \in \bigcap_{i \in I} N_i$  olduğundan  $\forall i \in I$  için  $x \in N_i$  olup  $N_i \triangleleft G$  olduğundan normal alt grup tanımı gereği  $axa^{-1} \in N_i$  olur.  $\forall i \in I$  için

$axa^{-1} \in N_i$  olduğundan  $axa^{-1} \in \bigcap_{i \in I} N_i$  olur. Yani  $\forall a \in G$  ve  $\forall x \in \bigcap_{i \in I} N_i$  için  $axa^{-1} \in \bigcap_{i \in I} N_i$  olup tanımdan  $\bigcap_{i \in I} N_i \triangleleft G$  olur.

**Not.**  $N \triangleleft G$  olsun.  $G$  de  $N$  ye göre sol (veya sağ) denklik sınıflarının kümesi  $G/N$  ile gösterilir. Yani  $G/N = \{aN | a \in G\} = \{Na | a \in G\}$  olarak tanımlanır.

**Teorem 2.4.11.**  $N \triangleleft G$  ise  $a, b \in G$  olmak üzere  $\forall aN, bN \in G/N$  için

$$(aN)(bN) = (ab)N \text{ olur.}$$

**İspat.**  $N \triangleleft G$  olsun.  $a, b \in G$  olmak üzere herhangi  $aN, bN \in G/N$  alalım.  $(aN)(bN) = (ab)N$  olduğu gösterilirse istenen elde edilir. Herhangi  $x \in (aN)(bN)$  alalım.  $x \in (aN)(bN)$  olduğundan  $x = x_1x_2$  olacak şekilde  $\exists x_1 \in aN$  ve  $\exists x_2 \in bN$  vardır.  $x_1 \in aN$  ve  $x_2 \in bN$  olduğundan  $x_1 = an_1$  ve  $x_2 = bn_2$  olacak şekilde  $\exists n_1, n_2 \in N$  vardır. Burada  $x = x_1x_2 = an_1bn_2$  olur.  $n_1 \in N$  olduğundan  $n_1b \in Nb$  olur.  $N \triangleleft G$  olduğundan  $Nb = bN$  olup  $n_1b \in Nb = bN$  dir. O halde  $n_1b = bn_3$  olacak şekilde  $\exists n_3 \in N$  vardır. Bu durumda  $x = an_1bn_2 = abn_3n_2$  olur. Burada  $n_3, n_2 \in N$  ve  $N \triangleleft G$  olduğundan  $n_3n_2 \in N$  olup  $x = abn_3n_2 \in (ab)N$  olur. Böylece  $\forall x \in (aN)(bN)$  için  $x \in (ab)N$  olup

$$(aN)(bN) \subset (ab)N \quad (1)$$

kapsaması bulunur. Herhangi  $x \in (ab)N$  alalım.  $x \in (ab)N$  olduğundan  $x = abn$  olacak şekilde  $\exists n \in N$  vardır. Burada  $x = abn = aebn$  olur.  $e, n \in N$  olduğundan  $ae \in aN$  ve  $bn \in bN$  olur. O halde  $x = aebn \in (aN)(bN)$  olup

$$(ab)N \subset (aN)(bN) \quad (2)$$

kapsaması bulunur. (1) ve (2) den  $(aN)(bN) = (ab)N$  olup istenen elde edilir.

**Teorem 2.4.12.**  $N \triangleleft G$  ise  $G/N$ ,  $a, b \in G$  olmak üzere  $\forall aN, bN \in G/N$  için  $(aN) * (bN) = (aN)(bN)$  ile tanımlı  $*$  işlemine göre bir gruptur.

**İspat.**  $N \triangleleft G$  olsun.  $G \neq \emptyset$  olduğundan  $G/N \neq \emptyset$  olur. Teorem 2.4.11 den  $a, b \in G$  olmak üzere  $\forall aN, bN \in G/N$  için  $(aN) * (bN) = (aN)(bN) = (ab)N \in G/N$  olup  $*$  işlemi  $G/N$  de bir iç işlem olur.

$*$  işleminin tanımı ve Teorem 2.4.11 den  $a, b, c \in G$  olmak üzere  $\forall aN, bN, cN \in G/N$  için

$$\begin{aligned} (aN) * [(bN) * (cN)] &= (aN) * [(bc)N] = (a(bc))N = ((ab)c)N \\ &= [(ab)N] * (cN) = [(aN) * (bN)] * (cN) \end{aligned}$$

olup  $*$  işleminin  $G/N$  de birleşme özelliği vardır.

$G/N$  nin  $eN = N$  elemanını alalım.  $*$  işleminin tanımı ve Teorem 2.4.11 den  $a \in G$  olmak üzere  $\forall aN \in G/N$  için  $(aN) * (eN) = (ae)N = aN$  ve  $(eN) * (aN) = (ea)N = aN$  olup  $eN = N$  elemanı  $G/N$  nin  $*$  işlemine göre birim elemanı olur.

$a \in G$  olmak üzere herhangi  $aN \in G/N$  alalım.  $G/N$  nin  $a^{-1}N$  elemanını alırsak  $*$  işleminin tanımı ve Teorem 2.4.11 den  $(aN) * (a^{-1}N) = (aa^{-1})N = eN = N$  ve  $(a^{-1}N) * (aN) = (a^{-1}a)N = eN = N$  olup  $a^{-1}N$  elemanı  $aN$  elemanının  $G/N$  de  $*$  işlemine göre tersi olur. Yani  $G/N$  deki her elemanın  $G/N$  de  $*$  işlemine göre tersi vardır.

Böylece  $G/N$  kümesi  $*$  işlemine göre bir grup olup istenen elde edilir.

**Not.** Teoremdeki  $*$  sembolü yerine de genellikle  $\cdot$  sembolü kullanılacaktır. Ayrıca  $(aN)(bN)$  ve  $(ab)N$  gibi ifadelerde parantezler konulmayacaktır.

**Tanım 2.4.13.**  $N \triangleleft G$  ise  $G/N$  grubuna,  $G$  nin  $N$  ye göre **bölüm grubu** denir.

**Teorem 2.4.14.**  $G$  sonlu bir grup ve  $N \triangleleft G$  olsun. Bu durumda  $G/N$  de sonlu bir gruptur ve  $\circ\left(\frac{G}{N}\right) = \frac{\circ(G)}{\circ(N)}$  olur.

**İspat.**  $G/N = \{aN | a \in G\}$  ve  $G$  sonlu elemanlı olduğundan  $G/N$  de sonlu elemanlı olur. Ayrıca  $G/N$  nin tanımı ve Sonuç 2.4.6 gereği  $\circ(G/N) = (G:N) = \frac{\circ(G)}{\circ(N)}$  olup istenen elde edilir.

**Not.**  $G$  abel grup ise toplamsal değişmeli olduğundan her alt grubu normal olur. O halde  $G$  nin her alt grubuna göre bölüm grubu tanımlanabilir. Burada bölüm grubundaki işlem de genellikle  $+$  ile ifade edilir.  $N < G$  ve  $a \in G$  ise  $a$  nın denklik sınıfı  $\bar{a} = a + N = \{a + x | x \in N\}$  olur.

**Teorem 2.4.15.** Bir grubun indeksi 2 olan her alt grubu bir normal alt gruptur.

**İspat.**  $G$  bir grup ve  $N$ ,  $G$  nin  $G$  içindeki indeksi 2 olan bir alt grubu olsun.  $N \triangleleft G$  olduğu gösterilirse istenen elde edilir.  $x \in G$  olmak üzere

$$x \in N \Leftrightarrow e^{-1}x \in N \Leftrightarrow e \equiv_L x(\text{mod } N) \Leftrightarrow N = eN = xN$$

ve

$$x \in N \Leftrightarrow xe^{-1} \in N \Leftrightarrow x \equiv e(\text{mod } N) \Leftrightarrow Nx = Ne = N$$

denklikleri vardır. Herhangi  $a \in G$  alalım. Eğer  $a \in N$  ise yukarıdaki denkliklerden  $aN = N$  ve  $Na = N$  olup  $aN = Na$  olur. Kabul edelim ki  $a \notin N$  olsun. Bu durumda yine yukarıdaki denkliklerden  $aN \neq N$  ve  $Na \neq N$  olur.  $aN \neq N$  ve  $(G:N) = 2$  olduğundan  $G$  de  $N$  ye göre sol denklik sınıflarının ailesi  $\{aN, N\}$  olup bu aile  $G$  nin bir ayrışımı olduğundan  $G = aN \cup N$  ve  $aN \cap N = \emptyset$  olur. Bu durumda  $aN = G - N$  olur.  $Na \neq N$  ve  $(G:N) = 2$  olduğundan  $G$  de

$N$  ye göre sağ denklik sınıflarının ailesi  $\{Na, N\}$  olup bu aile  $G$  nin bir ayrışımı olduğundan  $G = Na \cup N$  ve  $Na \cap N = \emptyset$  olur. Bu durumda da  $Na = G - N$  olur.  $aN = G - N$  ve  $Na = G - N$  olduğundan  $aN = Na$  olur. Yani  $\forall a \in G$  için  $aN = Na$  olup tanımdan  $N \triangleleft G$  olur.

**Teorem 2.4.16.**  $N \triangleleft G$  olsun.  $N < K < G$  ise  $N \triangleleft K$  ve  $K/N < G/N$  olur. Eğer ayrıca  $N < K \triangleleft G$  ise  $K/N \triangleleft G/N$  olur. Tersine,  $G/N$  nin alt grupları  $N < T < G$  olmak üzere  $T/N$  şeklinde ve normal alt grupları da  $N < T \triangleleft G$  olmak üzere  $T/N$  şeklindedir.

**İspat.**  $N < K < G$  olsun. Herhangi  $a \in K$  ve herhangi  $x \in N$  alalım.  $a \in K$  ve  $K < G$  olduğundan  $a \in G$  olur. Ayrıca  $x \in N$  ve  $N \triangleleft G$  olduğundan  $axa^{-1} \in N$  olur. Yani  $\forall a \in K$  ve  $\forall x \in N$  için  $axa^{-1} \in N$  olup ayrıca  $N < K$  olduğundan normal alt grup tanımı gereği  $N \triangleleft K$  olur.  $N \triangleleft K$  olduğundan  $K/N$  bölüm grubu anlamlıdır. Ayrıca  $K/N \subset G/N$  ve  $K/N$  bölüm grubundaki iç işlem  $G/N$  grubundaki iç işlem olduğundan  $K/N < G/N$  olur. Şimdi kabul edelim ki  $N < K \triangleleft G$  olsun. Herhangi  $a \in G$  için  $aN \in G/N$  ve herhangi  $x \in K$  için  $xN \in K/N$  elemanlarını alalım.  $a \in G$ ,  $x \in K$  ve  $K \triangleleft G$  olduğundan tanımdan  $axa^{-1} \in K$  olup  $aNxN(aN)^{-1} = axNa^{-1}N = axa^{-1}N \in K/N$  olur. Yani her  $aN \in G/N$  ve her  $xN \in K/N$  için  $aNxN(aN)^{-1} \in K/N$  olup ayrıca  $K/N < G/N$  olduğundan tanımdan  $K/N \triangleleft G/N$  olur.

Tersine,  $G/N$  nin herhangi  $\bar{T}$  alt grubunu alalım.  $T = \{c \in G \mid cN \in \bar{T}\}$  kümesini tanımlayalım.  $\forall x \in N$  için  $e^{-1}x = x \in N$  olduğundan  $e \equiv_L x \pmod{N}$  olup  $xN = eN = N = e_{G/N} \in \bar{T}$  ve buradan da  $x \in T$  elde edilir. O halde  $N \subset T$  olur. Burada  $N \neq \emptyset$  olduğundan  $T \neq \emptyset$  olur. Ayrıca  $T \subset G$  olduğu da açıktır. Yani  $\emptyset \neq T \subset G$  olur. Herhangi  $a, b \in T$  alalım.  $a, b \in T$  olduğundan  $aN, bN \in \bar{T}$  olup  $\bar{T} < G/N$  olduğundan  $ab^{-1}N = aNb^{-1}N = aN(bN)^{-1} \in \bar{T}$  olur. O halde  $T$  nin tanımından  $ab^{-1} \in T$  olup Teorem 2.2.6 dan  $T < G$  olur. Ayrıca  $N \subset T$  olduğundan  $N < T < G$  olur.  $N \triangleleft G$  ve  $N < T < G$  olduğundan  $N \triangleleft T$  ve  $T/N < G/N$  olur. Herhangi  $\bar{x} \in T/N$  alalım.  $\bar{x} \in T/N$  olduğundan  $\bar{x} = xN$  olacak şekilde  $\exists x \in T$  vardır.  $x \in T$  ve  $T = \{c \in G \mid cN \in \bar{T}\}$  olduğundan  $\bar{x} = xN \in \bar{T}$  bulunur. Yani  $\forall \bar{x} \in T/N$  için  $\bar{x} \in \bar{T}$  olup

$$\frac{T}{N} \subset \bar{T} \quad (1)$$

kapsaması elde edilir. Herhangi  $\bar{x} \in \bar{T}$  alalım.  $\bar{x} \in \bar{T}$  ve  $\bar{T} < G/N$  olduğundan  $\bar{x} \in G/N$  olup  $\bar{x} = xN$  olacak şekilde  $\exists x \in G$  vardır.  $xN = \bar{x} \in \bar{T}$  olduğundan  $T$  nin tanımından  $x \in T$  olup  $\bar{x} = xN \in T/N$  olur. Yani  $\forall \bar{x} \in \bar{T}$  için  $\bar{x} \in T/N$  olup

$$\bar{T} \subset \frac{T}{N} \quad (2)$$

kapsaması bulunur. (1) ve (2) den  $\bar{T} = T/N$  elde edilir. Son olarak, kabul edelim ki  $\bar{T} \triangleleft G/N$  olsun.  $T \triangleleft G$  olduğu gösterilirse istenen elde edilir. Herhangi  $a \in G$  ve herhangi  $x \in T$  alalım.  $a \in G$  ve  $x \in T$  olduğundan  $aN \in G/N$  ve  $xN \in T/N = \bar{T}$  olup  $\bar{T} \triangleleft G/N$  olduğundan  $axa^{-1}N = aNxNa^{-1}N = aNxN(aN)^{-1} \in \bar{T}$  olur.  $axa^{-1}N \in \bar{T}$  olduğundan  $T$  nin tanımından  $axa^{-1} \in T$  dir. Yani  $\forall a \in G$  ve  $\forall x \in T$  için  $axa^{-1} \in T$  olup ayrıca  $T < G$  olduğundan tanımdan  $T \triangleleft G$  bulunur.

**Teorem 2.4.17.**  $G$  bir grup,  $N \triangleleft G$ ,  $N < K < G$  ve  $N < T < G$  olsun. Bu durumda  $K/N = T/N$  olması için gerek ve yeter koşul  $K = T$  olmasıdır.

**İspat.** ( $\Rightarrow$ )  $K/N = T/N$  olsun. Herhangi  $x \in K$  alalım.  $x \in K$  olduğundan  $xN \in K/N = T/N$  olup  $xN = yN$  olacak şekilde  $\exists y \in T$  vardır.  $yN = xN$  olduğundan  $y \equiv_L x(\text{mod } N)$  olup  $y^{-1}x \in N$  olur.  $y^{-1}x \in N$  ve  $N \subset T$  olduğundan  $y^{-1}x \in T$  olup ayrıca  $y \in T$  ve  $T < G$  olduğundan  $x = ey = yy^{-1}x \in T$  olur. Yani  $\forall x \in K$  için  $x \in T$  olup

$$K \subset T \quad (1)$$

kapsaması bulunur. Herhangi  $x \in T$  alalım.  $x \in T$  olduğundan  $xN \in T/N = K/N$  olup  $xN = yN$  olacak şekilde  $\exists y \in K$  vardır.  $yN = xN$  olduğundan  $y \equiv_L x(\text{mod } N)$  olup  $y^{-1}x \in N$  olur.  $y^{-1}x \in N$  ve  $N \subset K$  olduğundan  $y^{-1}x \in K$  olup ayrıca  $y \in K$  ve  $K < G$  olduğundan  $x = ey = yy^{-1}x \in K$  bulunur. Yani  $\forall x \in T$  için  $x \in K$  olup

$$T \subset K \quad (2)$$

kapsaması elde edilir. (1) ve (2) den  $K = T$  olup istenen elde edilir.

( $\Leftarrow$ ) Açıktır.

**Tanım 2.4.18.** Bir  $G$  grubunun  $\{e\}$  ve  $G$  den başka bir normal alt grubu yoksa  $G$  ye **basit grup** denir.

**Örnek.** Mertebesi bir asal sayı olan her grup basittir.

**Tanım 2.4.19.**  $G$  bir grup,  $M \triangleleft G$  ve  $M \neq G$  olsun.  $G$  nin  $M$  yi kapsayan  $M$  ve  $G$  den başka bir normal alt grubu yoksa  $M$  ye  $G$  nin **maksimal normal alt grubu** denir.

**Teorem 2.4.20.**  $G$  bir grup,  $M \triangleleft G$  ve  $M \neq G$  olsun. Bu takdirde  $M$  nin maksimal normal alt grup olması için gerek ve yeter koşul  $G/M$  nin basit grup olmasıdır.

**İspat.** ( $\Rightarrow$ )  $M \triangleleft G$  maksimal olsun.  $G/M$  nin herhangi  $\bar{T}$  normal alt grubunu alalım. Teorem 2.4.16 dan  $M < T \triangleleft G$  ve  $\bar{T} = T/M$  olacak şekilde  $G$  nin bir  $T$  alt grubu vardır.  $M < T \triangleleft G$  ve

$M$  maksimal olduğundan  $T = M$  veya  $T = G$  olmalıdır. Eğer burada  $T = M$  ise  $\forall a \in T$  için  $ae^{-1} = a \in T = M$  olup  $a \equiv e \pmod{M}$  ve buradan da  $Ma = Me = M = \{e_{G/M}\}$  bulunur. Bu durumda  $\bar{T} = T/M = \{aM | a \in T\} = \{Ma | a \in T\} = \{e_{G/M}\}$  olur. Eğer  $T = G$  ise  $\bar{T} = T/M = G/M$  olur. Yani  $G/M$  nin  $\{e_{G/M}\}$  ve  $G/M$  den farklı bir normal alt grubu yoktur. O halde tanımdan  $G/M$  basit grup olup istenen elde edilir.

( $\Leftarrow$ )  $G/M$  basit grup olsun.  $G$  nin  $M$  yi kapsayan herhangi  $T$  normal alt grubunu alalım.  $M < T \triangleleft G$  olduğundan Teorem 2.4.16 dan  $T/M \triangleleft G/M$  olup  $G/M$  basit grup olduğundan  $T/M = \{e_{G/M}\}$  veya  $T/M = G/M$  olmalıdır. Eğer burada  $T/M = \{e_{G/M}\}$  ise  $\forall a \in T$  için  $aM \in T/M = \{e_{G/M}\}$  olup  $aM = e_{G/M} = M = eM$  eşitliğinden  $e \equiv_L a \pmod{M}$  bulunur. Böylece  $a = e^{-1}a \in M$  elde edilir. Bu durumda  $T \subset M$  olup ayrıca  $M \subset T$  olduğundan  $T = M$  olur. Eğer  $T/M = G/M$  ise Teorem 2.4.17 den  $T = G$  olur. Yani  $G$  nin  $M$  yi kapsayan  $M$  ve  $G$  den farklı bir normal alt grubu yoktur. O halde  $M$ ,  $G$  nin bir maksimal normal alt grubu olup istenen elde edilir.

## 2.5. GRUP HOMOMORFİZMALARI

Bu bölümde, gruplar arasında grupların cebirsel yapısını koruyan fonksiyonlar üzerinde duracağız.

**Tanım 2.5.1.**  $(G, *)$  ve  $(H, \blacksquare)$  iki grup ve  $f: G \rightarrow H$  bir fonksiyon olsun. Eğer  $\forall a, b \in G$  için  $f(a * b) = f(a) \blacksquare f(b)$  ise  $f$  fonksiyonuna  $G$  den  $H$  ye bir **homomorfizma (grup homomorfizması)** denir.

**Not.**  $f: G \rightarrow H$ ,  $\forall a \in G$  için  $f(a) = e_H$  ile tanımlı  $f$  fonksiyonu bir homomorfizmadır. Bu homomorfizmaya **aşık homomorfizma** denir.

**Örnek.**  $f: (\mathbb{R}, +) \rightarrow (\mathbb{R} - \{0\}, \cdot), x \mapsto f(x) = 5^x$  ile tanımlı  $f$  fonksiyonu verilsin.  $\forall x, y \in \mathbb{R}$  için  $f(x + y) = 5^{x+y} = 5^x \cdot 5^y = f(x) \cdot f(y)$  olduğundan  $f$  bir homomorfizmadır.

**Örnek.**  $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_n, +), a \mapsto f(a) = \bar{a}$  ile tanımlı  $f$  fonksiyonu verilsin.  $\forall x, y \in \mathbb{Z}$  için  $f(x + y) = \overline{x + y} = \bar{x} + \bar{y} = f(x) + f(y)$  olduğundan  $f$  bir homomorfizmadır.

**Teorem 2.5.2.**  $f: G \rightarrow H$  bir homomorfizma olsun. Bu takdirde

- (i)  $f(e_G) = e_H$  ve
- (ii)  $\forall a \in G$  için  $f(a^{-1}) = f(a)^{-1}$  olur.

**İspat.** (i)  $e_G = e_G e_G$  olduğundan  $f(e_G) = f(e_G e_G)$  olup  $f$  bir homomorfizma olduğundan  $f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$  olur.  $f(e_G)f(e_G) = f(e_G) = f(e_G)e_H$  olduğundan kısaltma özelliğinden  $f(e_G) = e_H$  olup istenen elde edilir.

(ii) Herhangi  $a \in G$  alalım.  $aa^{-1} = e_G$  olduğundan  $f(aa^{-1}) = f(e_G)$  olup  $f$  bir homomorfizma olduğundan  $f(e_G) = f(aa^{-1}) = f(a)f(a^{-1})$  olur. (i) şikkından  $f(e_G) = e_H$  olur. O halde  $f(a)f(a^{-1}) = f(e_G) = e_H$  olup  $f(a)^{-1}f(a)f(a^{-1}) = f(a)^{-1}e_H = f(a)^{-1}$  olur. Burada  $f(a)^{-1}f(a) = e_H$  olup  $e_H f(a^{-1}) = f(a)^{-1}$  eşitliğinden  $f(a^{-1}) = f(a)^{-1}$  bulunur. Yani  $\forall a \in G$  için  $f(a^{-1}) = f(a)^{-1}$  olup istenen elde edilir.

**Teorem 2.5.3.**  $f: G \rightarrow H$  bir homomorfizma olsun. Bu takdirde

- (i)  $G$  nin her alt grubunun  $f$  altındaki görüntüsü  $H$  nin bir alt grubudur.
- (ii)  $H$  nin her alt grubunun  $f$  altındaki ters görüntüsü  $G$  nin bir alt grubudur.

**İspat.** (i)  $G$  nin herhangi  $K$  alt grubunu alalım.  $f(K) < H$  olduğu gösterilirse istenen elde edilir.  $K < G$  olduğundan  $\emptyset \neq K \subset G$  olup  $\emptyset \neq f(K) \subset H$  olur. Herhangi  $x, y \in f(K)$  alalım.  $x, y \in f(K)$  olduğundan  $x = f(a)$  ve  $y = f(b)$  olacak şekilde  $\exists a, b \in K$  vardır.  $a, b \in K$  ve  $K < G$  olduğundan  $ab^{-1} \in K$  olup  $f(ab^{-1}) \in f(K)$  olur. Diğer taraftan  $f$  bir homomorfizma olduğundan Teorem 2.5.2 (ii) gereği  $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = xy^{-1}$  olur. O halde  $xy^{-1} \in f(K)$  olup Teorem 2.2.6 dan  $f(K) < H$  olur.

(ii)  $H$  nin herhangi  $T$  alt grubunu alalım.  $f^{-1}(T) < G$  olduğu gösterilirse istenen elde edilir.  $f: G \rightarrow H$  bir homomorfizma olduğundan Teorem 2.5.2 (i) gereği  $f(e_G) = e_H \in T$  olup  $e_G \in f^{-1}(T)$  olur. O halde  $f^{-1}(T) \neq \emptyset$  olur. Ayrıca  $f^{-1}(T) \subset G$  olduğu da açıktır. Yani  $\emptyset \neq f^{-1}(T) \subset G$  olur. Herhangi  $a, b \in f^{-1}(T)$  alalım.  $a, b \in f^{-1}(T)$  olduğundan  $f(a), f(b) \in T$  olup  $T < H$  olduğundan  $f(a)f(b)^{-1} \in T$  olur. Diğer taraftan  $f$  bir homomorfizma olduğundan Teorem 2.5.2 (ii) gereği  $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1}$  olur. O halde  $f(ab^{-1}) \in T$  olup  $ab^{-1} \in f^{-1}(T)$  olur. Yani  $\forall a, b \in f^{-1}(T)$  için  $ab^{-1} \in f^{-1}(T)$  olup Teorem 2.2.6 dan  $f^{-1}(T) < G$  olur.

**Sonuç 2.5.4.**  $f: G \rightarrow H$  bir homomorfizma olsun. Bu durumda  $f(G) < H$  olur.

**İspat.**  $G \leq G$  olduğundan Teorem 2.5.3 ün (i) şikkından  $f(G) < H$  olup istenen elde edilir.

**Teorem 2.5.5.**  $f: G \rightarrow H$  bir homomorfizma olsun. Bu takdirde

- (i)  $H$  nin her normal alt grubunun  $f$  altındaki ters görüntüsü  $G$  nin bir normal alt grubudur.
- (ii)  $f$  örten ise  $G$  nin her normal alt grubunun  $f$  altındaki görüntüsü  $H$  nin bir normal alt grubudur.

**İspat.** (i)  $H$  nin herhangi  $T$  normal alt grubunu alalım.  $f^{-1}(T) \triangleleft G$  olduğu gösterilirse istenen elde edilir.  $T \triangleleft H$  olduğundan  $T < H$  olup Teorem 2.5.3 (ii) den  $f^{-1}(T) < G$  olur. Herhangi  $a \in G$  ve herhangi  $x \in f^{-1}(T)$  alalım.  $a \in G$  ve  $x \in f^{-1}(T)$  olduğundan  $f(a) \in H$  ve  $f(x) \in T$  olup  $T \triangleleft H$  olduğundan  $f(a)f(x)f(a)^{-1} \in T$  olur. Diğer taraftan  $f$  bir homomorfizma olduğundan  $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)f(x)f(a)^{-1}$  olur. O halde  $f(axa^{-1}) \in T$  olup  $axa^{-1} \in f^{-1}(T)$  olur. Yani  $\forall a \in G$  ve  $\forall x \in f^{-1}(T)$  için  $axa^{-1} \in f^{-1}(T)$  olup normal alt grup tanımından  $f^{-1}(T) \triangleleft G$  olur.

(ii)  $f$  örten olsun.  $G$  nin herhangi  $K$  normal alt grubunu alalım.  $f(K) \triangleleft H$  olduğu gösterilirse istenen elde edilir.  $K \triangleleft G$  olduğundan  $K < G$  olup Teorem 2.5.3 (i) den  $f(K) < H$  olur. Herhangi  $a \in H$  ve herhangi  $x \in f(K)$  alalım.  $a \in H$  ve  $f$  örten olduğundan  $f(b) = a$  olacak şekilde  $\exists b \in G$  vardır.  $x \in f(K)$  olduğundan  $x = f(y)$  olacak şekilde  $\exists y \in K$  vardır.  $b \in G$ ,  $y \in K$  ve  $K \triangleleft G$  olduğundan  $byb^{-1} \in K$  olup  $f(byb^{-1}) \in f(K)$  olur. Diğer taraftan  $f: G \rightarrow H$  bir homomorfizma olduğundan Teorem 2.5.2 (ii) gereği  $f(byb^{-1}) = f(b)f(y)f(b^{-1}) = f(b)f(y)f(b)^{-1} = axa^{-1}$  olur. O halde  $axa^{-1} \in f(K)$  olup ayrıca  $f(K) < H$  olduğundan tanımdan  $f(K) \triangleleft H$  olur.

**Tanım 2.5.6.**  $f: G \rightarrow H$  bir homomorfizma olsun.  $f^{-1}(e_H) = \{a \in G | f(a) = e_H\}$  kümesine  $f$  homomorfizmasının **çekirdeği** denir ve genellikle  $\text{Çek}f$  ile gösterilir.

**Önerme 2.5.7.**  $f: G \rightarrow H$  bir homomorfizma olsun. Bu takdirde  $f$  nin bire-bir olması için gerek ve yeter koşul  $\text{Çek}f = \{e_G\}$  olmasıdır.

**İspat.**  $(\Rightarrow)$   $f$  bire-bir olsun.  $f: G \rightarrow H$  bir homomorfizma olduğundan Teorem 2.5.2 (i) gereği  $f(e_G) = e_H$  olup  $e_G \in f^{-1}(e_H) = \text{Çek}f$  olur. Herhangi  $x \in \text{Çek}f$  alalım.  $x \in \text{Çek}f$  olduğundan  $f(x) = e_H = f(e_G)$  olup  $f$  bire-bir olduğundan  $x = e_G$  olur. O halde  $\text{Çek}f = \{e_G\}$  bulunur.

$(\Leftarrow)$   $\text{Çek}f = \{e_G\}$  olsun.  $f(x) = f(y)$  olan herhangi  $x, y \in G$  alalım.  $f(x) = f(y)$  olduğundan  $f(x)f(y)^{-1} = e_H$  eşitliği bulunur. Diğer taraftan  $f$  bir homomorfizma olduğundan Teorem 2.5.2 (ii) gereği  $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1}$  olur. O halde  $f(xy^{-1}) = e_H$  olup  $xy^{-1} \in f^{-1}(e_H) = \text{Çek}f = \{e_G\}$  olur. Bu durumda  $xy^{-1} = e_G$  olup  $x = y$  olur. Böylece  $f$  bire-birdir.

**Tanım 2.5.8.** Bire-bir ve örten bir homomorfizmaya **izomorfizma (grup izomorfizması)** denir. Eğer  $G$  ve  $H$  grupları arasında en az bir izomorfizma varsa bu gruplara **izomorf gruplar** denir ve genellikle  $G \cong H$  ile ifade edilir.

**Not:** İzomorf gruplar arasında bire-bir bir eşleme var ve grup yapıları da bu eşleme altında bozulmadığı için izomorfizma bir eşitlik gibi düşünülebilir.

**Örnek.**  $f: G \rightarrow H$  bir izomorfizma ise  $f^{-1}: H \rightarrow G$  dönüşümü de bir izomorfizmadır.

**Çözüm.** İzomorfizma bire-bir ve örten bir fonksiyon olduğundan, ters fonksiyonu da bire-bir ve örtendir.  $f: G \rightarrow H$  bir izomorfizma olsun. Bu durumda  $\forall x, y \in H$  için  $x = f(a)$  ve  $y = f(b)$  olacak şekilde  $\exists a, b \in G$  vardır. Buradan  $f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x)f^{-1}(y)$  olup  $f^{-1}: H \rightarrow G$  dönüşümü de bir izomorfizmadır.

**Teorem 2.5.9.**  $G$  bir grup ve  $N \triangleleft G$  olsun. Bu takdirde  $\forall x \in G$  için  $\varphi(x) = Nx$  ile tanımlı  $\varphi: G \rightarrow G/N$  dönüşümü örten bir homomorfizmadır. Ayrıca  $\text{Çek}\varphi = N$  dir.

**İspat.**  $\varphi$  nin bir fonksiyon olduğu açıktır.  $N \triangleleft G$  olduğundan  $\varphi$  nin tanımından  $\forall a, b \in G$  için  $\varphi(ab) = Nab = abN = aNbN = NaNb = \varphi(a)\varphi(b)$  olup  $\varphi$  bir homomorfizma olur. Herhangi  $\bar{a} \in G/N$  alalım.  $\bar{a} \in G/N$  olduğundan  $\bar{a} = aN = Na$  olacak şekilde  $\exists a \in G$  vardır. Burada  $\varphi$  nin tanımından  $\varphi(a) = Na = \bar{a}$  olup  $\varphi$  örten olur.

$x \in G$  olmak üzere

$$x \in \text{Çek}\varphi \Leftrightarrow \varphi(x) = e_{G/N} \Leftrightarrow Nx = N = Ne \Leftrightarrow x \equiv e \pmod{N} \Leftrightarrow x = xe^{-1} \in N$$

denkliklerinden  $\text{Çek}\varphi = N$  elde edilir.

**Not.**  $G$  bir grup ve  $N \triangleleft G$  ise çekirdeği  $N$  olan en az bir homomorfizma vardır. Gerçekten yukarıda tanımlanan  $\varphi: G \rightarrow G/N$  homomorfizması alınabilir.

**Teorem 2.5.10.(Homomorfizma Teoremi)**  $f: G \rightarrow H$  bir homomorfizma ve  $\text{Çek}f = N$  olsun.

Bu durumda

(i)  $N \triangleleft G$  dir.

(ii)  $h \in H$  ve bir  $a \in G$  için  $f(a) = h$  ise  $f^{-1}(h) = aN$  dir.

(iii)  $G/N \cong f(G)$  dir.

**İspat.** (i)  $f: G \rightarrow H$  bir homomorfizma ve  $\{e_H\} \triangleleft H$  olduğundan Teorem 2.5.5 (i) gereği  $N = \text{Çek}f = f^{-1}(e_H) \triangleleft G$  olup istenen elde edilir.

(ii)  $h \in H$  ve bir  $a \in G$  için  $f(a) = h$  olsun. Herhangi  $x \in f^{-1}(h)$  alalım.  $x \in f^{-1}(h)$  olduğundan  $f(x) = h = f(a)$  olup  $f(a)^{-1}f(x) = e_H$  eşitliği vardır. Ayrıca  $f$  bir homomorfizma olduğundan  $f(a^{-1}x) = f(a)^{-1}f(x) = e_H$  olup  $a^{-1}x \in \text{Çek}f = N$  dir. Bu durumda  $x = aa^{-1}x \in aN$  olup

$$f^{-1}(h) \subset aN \tag{1}$$

kapsaması bulunur. Herhangi  $x \in aN$  alalım.  $x \in aN$  olduğundan  $x = an$  olacak şekilde  $\exists n \in N$  vardır.  $n \in N = \text{Çekf}$  olduğundan  $f(n) = e_H$  dir.  $f$  bir homomorfizma olduğundan  $f(x) = f(an) = f(a)f(n) = f(a)e_H = f(a) = h$  olur. O halde  $x \in f^{-1}(h)$  olup

$$aN \subset f^{-1}(h) \quad (2)$$

olur. (1) ve (2) den  $f^{-1}(h) = aN$  olup istenen elde edilir.

(iii)  $N \triangleleft G$  olduğundan  $G/N$  bölüm grubu anlamlıdır.

$$\bar{f}: G/N \rightarrow f(G), xN \rightarrow \bar{f}(xN) = f(x)$$

dönüşümünü tanımlayalım.  $\bar{f}$  nin kapalı olduğu açıktır.  $xN = yN$  olan herhangi  $x, y \in G$  alalım.  $x = xe \in xN = yN$  olduğundan  $x = yn$  olacak şekilde  $\exists n \in N$  vardır.  $n \in N = \text{Çekf}$  olduğundan  $f(n) = e_H$  olup  $f$  bir homomorfizma olduğundan  $f(x) = f(yn) = f(y)f(n) = f(y)e_H = f(y)$  olur. O halde  $\bar{f}$  iyi tanımlıdır. Böylece  $\bar{f}$  bir fonksiyon olur.  $f$  homomorfizma olduğundan  $\bar{f}$  nin tanımından  $\forall aN, bN \in G/N$  için  $\bar{f}(aNbN) = \bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN)$  olup  $\bar{f}$  bir homomorfizmadır. Herhangi  $xN \in \text{Çekf}$  alalım.  $xN \in \text{Çekf}$  olduğundan  $f(x) = \bar{f}(xN) = e_H$  olup  $x \in f^{-1}(e_H) = \text{Çekf} = N$  olur.  $e^{-1}x = x \in N$  olduğundan  $e \equiv_L x(\text{mod}N)$  olup  $xN = eN = N = \{e_{G/N}\}$  bulunur. O halde  $\text{Çekf} = \{e_{G/N}\}$  olup Önerme 2.5.7 den  $\bar{f}$  bire-birdir. Herhangi  $y \in f(G)$  alalım.  $y \in f(G)$  olduğundan  $y = f(x)$  olacak şekilde  $\exists x \in G$  vardır. Burada  $xN \in G/N$  elemanı alınırsa  $\bar{f}$  nin tanımından  $\bar{f}(xN) = f(x) = y$  olup  $\bar{f}$  örten bulunur.  $\bar{f}: G/N \rightarrow f(G)$  bire-bir ve örten bir homomorfizma olduğundan tanımdan  $\bar{f}$  bir izomorfizma olup  $G/N \cong f(G)$  izomorfizması vardır.

**Sonuç 2.5.11.**  $f: G \rightarrow H$  örten homomorfizma ise  $N = \text{Çekf}$  olmak üzere  $\varphi: G \rightarrow G/N, a \rightarrow \varphi(a) = aN$  ve  $\bar{f}: G/N \rightarrow f(G) = H, aN \rightarrow \bar{f}(aN) = f(a)$  fonksiyonları için  $f = \bar{f} \circ \varphi$  dir. Burada  $\varphi$  örten homomorfizmasına **doğal homomorfizma** ve  $f$  nin böyle yazılışına da **doğal ayrışım** denir.

**Teorem 2.5.12. (İzomorfizma Teoremi)**  $f: G \rightarrow \bar{G}$  örten homomorfizma,  $\text{Çekf} = K, \bar{N} \triangleleft \bar{G}$  ve  $N = f^{-1}(\bar{N})$  olsun. Bu takdirde  $G/N \cong \bar{G}/\bar{N} \cong \frac{G/K}{N/K}$  olur.

**İspat.**  $\bar{N} \triangleleft \bar{G}$  olduğundan  $\bar{G}/\bar{N}$  bölüm grubu anlamlıdır.  $\bar{N} \triangleleft \bar{G}$  olduğundan Teorem 2.5.5 (i) den  $N = f^{-1}(\bar{N}) \triangleleft G$  olup  $G/N$  bölüm grubu anlamlıdır. Ayrıca Homomorfizma Teoreminden  $K = \text{Çekf} \triangleleft G$  olduğundan  $G/K$  bölüm grubu anlamlıdır.  $\forall x \in K = \text{Çekf}$  için

$f(x) = e_{\bar{G}} \in \bar{N}$  olduğundan  $x \in f^{-1}(\bar{N}) = N$  olup  $K \subset N$  olur.  $K \triangleleft G$  ve  $K < N < G$  olduğundan Teorem 2.4.16 dan  $K \triangleleft N$  olup  $N/K$  bölüm grubu anlamlıdır.  $K < N \triangleleft G$  olduğundan Teorem 2.4.16 dan  $N/K \triangleleft G/K$  olup  $\frac{G/K}{N/K}$  bölüm grubu anlamlıdır.

$$g: G \rightarrow \bar{G}/\bar{N}, x \rightarrow g(x) = f(x)\bar{N}$$

dönüşümünü tanımlayalım.  $g$  nin fonksiyon olduğu açıktır. Ayrıca  $f: G \rightarrow \bar{G}$  homomorfizma olduğundan  $g$  nin tanımından  $\forall x, y \in G$  için  $g(xy) = f(xy)\bar{N} = f(x)f(y)\bar{N} = f(x)\bar{N}f(y)\bar{N} = g(x)g(y)$  eşitliği yardımıyla  $g$  nin bir homomorfizma olduğu görülür. Herhangi  $y\bar{N} \in \bar{G}/\bar{N}$  ( $y \in \bar{G}$ ) alalım.  $y \in \bar{G}$  ve  $f$  örten olduğundan  $f(x) = y$  olacak şekilde  $\exists x \in G$  vardır. Burada  $g$  nin tanımından  $g(x) = f(x)\bar{N} = y\bar{N}$  olup  $g$  örten ve dolayısıyla da  $g(G) = \bar{G}/\bar{N}$  olur.  $x \in G$  olmak üzere

$$\begin{aligned} x \in \text{Çekg} &\Leftrightarrow g(x) = e_{\bar{G}/\bar{N}} \Leftrightarrow f(x)\bar{N} = \bar{N} = e_{\bar{G}}\bar{N} \Leftrightarrow e_{\bar{G}} \equiv_L f(x)(\text{mod}\bar{N}) \Leftrightarrow \\ &\Leftrightarrow f(x) = e_{\bar{G}}^{-1}f(x) \in \bar{N} \Leftrightarrow x \in f^{-1}(\bar{N}) = N \end{aligned}$$

denkliklerinden  $\text{Çekg} = N$  elde edilir. O halde Homomorfizma Teoreminden  $G/N \cong g(G) = \bar{G}/\bar{N}$  olur. Şimdi

$$h: G/K \rightarrow G/N, \quad xK \rightarrow h(xK) = xN$$

dönüşümünü tanımlayalım.  $h$  nin kapalı olduğu açıktır.  $xK = yK$  olan herhangi  $x, y \in G$  alalım.  $xK = yK$  olduğundan  $x \equiv_L y(\text{mod}K)$  iken  $x^{-1}y \in K$  sağlanır. Ayrıca  $x^{-1}y \in K$  ve  $K \subset N$  olduğundan  $x^{-1}y \in N$  iken  $x \equiv_L y(\text{mod}N)$  bulunur. O halde  $xN = yN$  olup  $h$  iyi tanımlıdır. Böylece  $h: G/K \rightarrow G/N$  bir fonksiyondur.  $h$  nin tanımından  $\forall xK, yK \in G/K$  ( $x, y \in G$ ) için  $h(xKyK) = h(xyK) = xyN = xNyN = h(xK)h(yK)$  olup  $h: G/K \rightarrow G/N$  bir homomorfizmadır. Her  $xN \in G/N$  ( $x \in G$ ) için  $G/K$  nin  $xK$  elemanı alınırsa  $h$  nin tanımından  $h(xK) = xN$  olup  $h$  örtendir. Dolayısıyla da  $h(G/K) = G/N$  olur. Herhangi  $\bar{x} \in \text{Çek}h$  alalım.  $\bar{x} \in \text{Çek}h$  ve  $\text{Çek}h \subset G/K$  olduğundan  $\bar{x} \in G/K$  olup  $\bar{x} = xK$  olacak şekilde  $\exists x \in G$  vardır. Burada  $e_G N = N = \{e_{G/N}\} = h(\bar{x}) = h(xK) = xN$  olup  $e_G \equiv_L x(\text{mod}N)$  olur. Bu durumda  $x = e_G^{-1}x \in N$  olup  $\bar{x} = xK \in N/K$  dir. Yani  $\forall \bar{x} \in \text{Çek}h$  için  $\bar{x} \in N/K$  olup

$$\text{Çek}h \subset N/K \tag{1}$$

kapsaması bulunur. Herhangi  $\bar{x} \in N/K$  alalım.  $\bar{x} \in N/K$  olduğundan  $\bar{x} = xK$  olacak şekilde  $\exists x \in N$  vardır.  $e_G^{-1}x = x \in N$  olduğundan  $e_G \equiv_L x(\text{mod}N)$  olup  $\{e_{G/N}\} = e_G N = xN$  olur.

Ayrıca  $h$  nin tanımından  $h(\bar{x}) = h(xK) = xN$  olur. O halde  $h(\bar{x}) = e_{G/N}$  olup  $\bar{x} \in \text{Çekh}$  olur. Yani  $\forall \bar{x} \in N/K$  için  $\bar{x} \in \text{Çekh}$  olup

$$N/K \subset \text{Çekh} \quad (2)$$

kapsaması elde edilir. (1) ve (2) den  $\text{Çekh} = N/K$  bulunur. O halde Homomorfizma Teoreminden  $\frac{G/K}{N/K} \cong h(G/K) = G/N$  elde edilir. Dolayısıyla  $\frac{G/K}{N/K} \cong G/N$  ve  $G/N \cong \overline{G}/\overline{N}$  iken  $G/N \cong \overline{G}/\overline{N} \cong \frac{G/K}{N/K}$  olup istenen elde edilir.

**Teorem 2.5.13. (2. İzomorfizma Teoremi)**  $G$  bir grup,  $H < K$  ve  $K \triangleleft G$  olsun. Bu takdirde  $HK = KH < G$  ve  $H \cap K \triangleleft H$  olup  $HK/K \cong H/H \cap K$  izomorfizması vardır.

**İspat.**  $\emptyset \neq HK \subset G$  olduğu açıktır. Herhangi  $x, y \in HK$  alalım.  $x, y \in HK$  olduğundan  $x = h_1k_1$  ve  $y = h_2k_2$  olacak şekilde  $\exists h_1, h_2 \in H$  ve  $\exists k_1, k_2 \in K$  vardır.  $x = h_1k_1$  ve  $y = h_2k_2$  olduğundan  $xy^{-1} = h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h_2^{-1}h_2k_1k_2^{-1}h_2^{-1}$  olur. Burada  $h_1, h_2 \in H$  ve  $H < G$  olduğundan  $h_1h_2^{-1} \in H$  dir.  $k_1, k_2 \in K$  ve  $K < G$  olduğundan  $k_1k_2^{-1} \in K$  olur.  $h_2 \in H$  ve  $H \subset G$  olduğundan  $h_2 \in G$  olup ayrıca  $k_1k_2^{-1} \in K$  ve  $K \triangleleft G$  olduğu için  $h_2k_1k_2^{-1}h_2^{-1} \in K$  olur.  $h_1h_2^{-1} \in H$  ve  $h_2k_1k_2^{-1}h_2^{-1} \in K$  iken

$$xy^{-1} = h_1h_2^{-1}h_2k_1k_2^{-1}h_2^{-1} \in HK$$

olur. Yani  $\forall x, y \in HK$  için  $xy^{-1} \in HK$  olup Teorem 2.2.6 gereği  $HK < G$  bulunur. Bu durumda Teorem 2.2.11 gereği  $HK = KH < G$  olur. Burada  $e \in H$  olduğundan  $\forall k \in K$  için  $k = ek \in HK$  olup  $K \subset HK$  kapsamı elde edilir.  $K \triangleleft G$  ve  $K < HK < G$  olduğundan Teorem 2.4.16 dan  $K \triangleleft HK$  ve  $HK/K < G/K$  olur.

$H < G$  ve  $K < G$  olduğundan Teorem 2.2.9 dan  $H \cap K < G$  olup  $H \cap K \subset H$  için  $H \cap K < H$  dir. Herhangi  $a \in H$  ve herhangi  $x \in H \cap K$  alalım.  $x \in H \cap K$  olduğundan  $x \in H$  ve  $x \in K$  olur.  $a \in H$  ve  $H < G$  olduğundan  $a \in G$  olup ayrıca  $x \in K$  ve  $K \triangleleft G$  olduğundan tanımdan  $axa^{-1} \in K$  bulunur. Diğer taraftan  $a, x \in H$  ve  $H < G$  olduğundan  $axa^{-1} \in H$  olur. O halde  $axa^{-1} \in H \cap K$  olur. Böylece  $\forall a \in H$  ve  $\forall x \in H \cap K$  için  $axa^{-1} \in H \cap K$  olup ayrıca  $H \cap K < H$  olduğundan tanımdan  $H \cap K \triangleleft H$  olur.

$$f: H \rightarrow HK/K, x \rightarrow f(x) = xK$$

dönüşümünü tanımlayalım.  $e \in K$  olduğundan  $\forall x \in H$  için  $x = xe \in HK$  olup  $xK \in HK/K$  olur. O halde  $f$  kapalıdır.  $f$  nin iyi tanımlı olduğu da açıktır. Yani  $f$  bir fonksiyondur.  $f$  nin tanımından  $\forall x, y \in H$  için  $f(xy) = xyK = xKyK = f(x)f(y)$  olup  $f$  homomorfizmadır. Herhangi  $\bar{x} \in HK/K$  alalım.  $\bar{x} \in HK/K$  olduğundan  $\bar{x} = xK$  olacak şekilde  $\exists x \in HK$  vardır.

$x \in HK$  olduğundan  $x = hk$  olacak şekilde  $\exists h \in H$  ve  $\exists k \in K$  vardır.  $x = hk$  olduğundan  $h^{-1}x = k \in K$  için  $h \equiv_L x(\text{mod}K)$  ve buradan da  $hK = xK = \bar{x}$  elde edilir. Burada  $f$  nin tanımından  $f(h) = hK = \bar{x}$  olup  $f$  örten olur.  $y \in H$  olmak üzere

$y \in \text{Çek}f \Leftrightarrow f(y) = e_{G/K} \Leftrightarrow yK = eK \Leftrightarrow e \equiv_L y(\text{mod}K) \Leftrightarrow y = e^{-1}y \in K \Leftrightarrow y \in H \cap K$  denkliklerinden  $\text{Çek}f = H \cap K$  olduğu anlaşılır. O halde Homomorfizma Teoreminden  $H \cap K \triangleleft H$  ve  $H/H \cap K \cong f(H) = HK/K$  izomorfizmasından  $HK/K \cong H/H \cap K$  elde edilir.

**Teorem 2.5.14.** Boştan farklı bir  $A$  kümesinden  $A$  ya bire-bir ve örten fonksiyonlar kümesini  $S(A)$  ile gösterelim. Bu takdirde  $S(A)$  kümesi fonksiyonlarda bileşke işlemine göre bir gruptur.

**İspat.**  $I_A: A \rightarrow A$  özdeşlik fonksiyonu bire-bir ve örten olduğundan  $I_A \in S(A)$  olup  $S(A) \neq \emptyset$  dir.  $\forall f, g \in S(A)$  için  $f$  ve  $g$ ,  $A$  kümesinden  $A$  ya bire-bir ve örten fonksiyonlar olduğundan  $f \circ g: A \rightarrow A$  bire-bir ve örten bir fonksiyondur. Böylece  $f \circ g \in S(A)$  olur. O halde fonksiyonlarda bileşke işlemi  $S(A)$  da bir iç işlem olur.

$\forall f, g, h \in S(A)$  için  $f \circ (g \circ h) = (f \circ g) \circ h$  olup fonksiyonlarda bileşke işleminin  $S(A)$  da birleşme özelliği vardır.

$\forall f \in S(A)$  için  $f \circ I_A = I_A \circ f = f$  olup  $I_A$ ,  $S(A)$  kümesinin fonksiyonlarda bileşke işlemine göre birim elemanıdır.

Herhangi  $f \in S(A)$  alalım.  $f \in S(A)$  olduğundan  $f: A \rightarrow A$  bire-bir ve örten bir fonksiyon olup  $f$  fonksiyonunun ters fonksiyonu da  $f^{-1}: A \rightarrow A$  bire-bir ve örtendir. O halde  $f^{-1} \in S(A)$  olur. Ayrıca  $f \circ f^{-1} = f^{-1} \circ f = I_A$  olup  $f^{-1}$ ,  $f$  nin  $S(A)$  da fonksiyonlarda bileşke işlemine göre tersi olur. Yani  $S(A)$ daki her elemanın  $S(A)$ da fonksiyonlarda bileşke işlemine göre tersi vardır.

Böylece  $S(A)$  kümesi fonksiyonlarda bileşke işlemine göre bir gruptur.

**Tanım 2.5.15.**  $S(A)$  nın alt grubuna **dönüşüm grubu** denir.

**Teorem 2.5.16. (Cayley Teoremi)** Her grup bir dönüşüm grubuna izomorftur.

**İspat.**  $G$  bir grup olsun.  $G$  nin bir dönüşüm grubuna izomorf olduğu gösterilirse istenen elde edilir.  $a \in G$  olmak üzere

$$T_a: G \rightarrow G, x \rightarrow T_a(x) = ax$$

dönüşümünü tanımlayalım.  $T_a$  nın bir fonksiyon olduğu açıktır.  $T_a(x_1) = T_a(x_2)$  olan herhangi  $x_1, x_2 \in G$  alalım.  $T_a(x_1) = T_a(x_2)$  olduğundan  $ax_1 = ax_2$  olup kısaltma özelliğinden  $x_1 = x_2$  olur. O halde  $T_a$  bire-birdir. Herhangi  $y \in G$  alalım.  $x = a^{-1}y$  diyelim. Burada  $x \in G$  ve  $T_a(x) = ax = aa^{-1}y = y$  olup  $T_a$  örtendir.  $T_a: G \rightarrow G$  bire-bir ve örten bir fonksiyon olduğundan  $T_a \in S(G)$  olur. Şimdi

$$\varphi: G \rightarrow S(G), a \rightarrow \varphi(a) = T_a$$

dönüşümünü tanımlayalım.  $\varphi$  nin bir fonksiyon olduğu açıktır. Herhangi  $a, b \in G$  alalım.  $T_a$ ,  $T_b$  ve  $T_{ab}$  nin tanımından  $\forall x \in G$  için  $T_{ab}(x) = abx = aT_b(x) = T_a(T_b(x)) = (T_a \circ T_b)(x)$  olup  $T_{ab} = T_a \circ T_b$  eşitliği sağlanır. O halde  $\varphi$  nin tanımından  $\varphi(ab) = T_{ab} = T_a \circ T_b = \varphi(a) \circ \varphi(b)$  olup  $\varphi$  bir homomorfizma olur. Buradan  $\varphi(G) < S(G)$  olur.  $\varphi(a_1) = \varphi(a_2)$  olan herhangi  $a_1, a_2 \in G$  alalım.  $\varphi(a_1) = \varphi(a_2)$  olduğundan  $T_{a_1} = T_{a_2}$  olup  $T_{a_1}(e) = T_{a_2}(e)$  olur. Bu durumda  $a_1e = a_2e$  olup  $a_1 = a_2$  olur. O halde  $\varphi$  bire-bir olup  $G \cong \varphi(G)$  izomorfizması elde edilir. Böylece  $G$  bir dönüşüm grubuna izomorf olup istenen elde edilir.

## ÖRNEKLER:

**Örnek 1.**  $m, n \in \mathbb{Z}^+$  olmak üzere  $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$  grubunun devirli olması için gerek ve yeter koşul  $(m, n) = \text{OBEB}(m, n) = 1$  olduğunu gösteriniz.

**Çözüm.**  $(\Rightarrow)$   $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$  grubu devirli olsun. Bu durumda  $\mathbb{Z}_m \times \mathbb{Z}_n = \langle (\bar{a}, \bar{b}) \rangle$  olacak şekilde  $\exists (\bar{a}, \bar{b}) \in \mathbb{Z}_m \times \mathbb{Z}_n$  vardır. Burada  $\circ((\bar{a}, \bar{b})) = s(\mathbb{Z}_m \times \mathbb{Z}_n) = mn$  olur.  $k = \text{OKEK}(m, n)$  diyelim. Burada  $m|k$  ve  $n|k$  olup hem  $m$  modülüne göre, hem de  $n$  modülüne göre  $\bar{k} = \bar{0}$  olur. O halde

$$\begin{aligned} k(\bar{a}, \bar{b}) &= \underbrace{(\bar{a}, \bar{b}) + (\bar{a}, \bar{b}) + \cdots + (\bar{a}, \bar{b})}_{k \text{ tane}} = \left( \underbrace{\bar{a} + \bar{a} + \cdots + \bar{a}}_{k \text{ tane}}, \underbrace{\bar{b} + \bar{b} + \cdots + \bar{b}}_{k \text{ tane}} \right) \\ &= \left( \underbrace{\bar{a} + \bar{a} + \cdots + \bar{a}}_{k \text{ tane}}, \underbrace{\bar{b} + \bar{b} + \cdots + \bar{b}}_{k \text{ tane}} \right) \\ &= (\overline{ka}, \overline{kb}) = (\overline{k\bar{a}}, \overline{k\bar{b}}) = (\overline{0\bar{a}}, \overline{0\bar{b}}) = (\bar{0}, \bar{0}) \end{aligned}$$

olup  $\circ((\bar{a}, \bar{b})) = mn$  olduğundan Teorem 2.3.10 dan  $mn|k$  olur. Diğer taraftan  $k = \text{OKEK}(m, n)|mn$  olup  $mn|k$ ,  $k|mn$  ve  $k, mn \in \mathbb{Z}^+$  olduğundan  $\text{OKEK}(m, n) = k = mn$  olur. Ayrıca Sonuç 1.5.35 gereği  $\text{OBEB}(m, n)\text{OKEK}(m, n) = mn$  olur. O halde  $\text{OBEB}(m, n)mn = mn$  olup  $(m, n) = \text{OBEB}(m, n) = 1$  bulunur.

$(\Leftarrow)$   $(m, n) = \text{OBEB}(m, n) = 1$  olsun.  $\mathbb{Z}_m \times \mathbb{Z}_n$  nin  $(\bar{1}, \bar{1})$  elemanını alalım. Herhangi  $(\bar{a}, \bar{b}) \in \mathbb{Z}_m \times \mathbb{Z}_n$  alalım.  $(m, n) = \text{OBEB}(m, n) = 1$  olduğundan Önerme 1.5.16 dan  $mx + ny = 1$  olacak şekilde  $\exists x, y \in \mathbb{Z}$  vardır.  $k = mxb + nya$  diyelim. Burada  $k \in \mathbb{Z}$  ve

$$\begin{aligned} k(\bar{1}, \bar{1}) &= (k\bar{1}, k\bar{1}) = (\bar{k}, \bar{k}) = (\overline{mxb + nya}, \overline{mxb + nya}) = (\overline{mxb} + \overline{nya}, \overline{mxb} + \overline{nya}) \\ &= (\bar{0} + \overline{(1 - mx)\bar{a}}, \overline{(1 - ny)\bar{b}} + \bar{0}) = ((\bar{1} - \overline{mx})\bar{a}, (\bar{1} - \overline{ny})\bar{b}) \end{aligned}$$

$$= ((\bar{1} - \bar{0})\bar{a}, (\bar{1} - \bar{0})\bar{b}) = (\bar{1}\bar{a}, \bar{1}\bar{b}) = (\bar{a}, \bar{b})$$

olup  $(\bar{a}, \bar{b}) = k(\bar{1}, \bar{1}) \in \langle (\bar{1}, \bar{1}) \rangle$  olur. O halde  $\mathbb{Z}_m \times \mathbb{Z}_n \subset \langle (\bar{1}, \bar{1}) \rangle$  olup ayrıca  $\langle (\bar{1}, \bar{1}) \rangle \subset \mathbb{Z}_m \times \mathbb{Z}_n$  olduğundan  $\mathbb{Z}_m \times \mathbb{Z}_n = \langle (\bar{1}, \bar{1}) \rangle$  olur. Böylece  $\mathbb{Z}_m \times \mathbb{Z}_n$  devirli olup istenen elde edilir.

**Örnek 2.**  $G$  bir grup ve  $a, b \in G$  olsun.  $\circ(a) = 5$  ve  $aba^{-1} = b^2$  ise  $\circ(b)$  yi bulunuz.

**Çözüm.**  $\circ(a) = 5$  ve  $aba^{-1} = b^2$  olsun.  $aba^{-1} = b^2$  olduğundan

$$b^4 = b^2 b^2 = aba^{-1} aba^{-1} = ab^2 a^{-1} = aaba^{-1} a^{-1} = a^2 b a^{-2}$$

olup

$$b^8 = b^4 b^4 = a^2 b a^{-2} a^2 b a^{-2} = a^2 b^2 a^{-2} = a^2 a b a^{-1} a^{-2} = a^3 b a^{-3}$$

bulunur.  $b^8 = a^3 b a^{-3}$  ve  $b^2 = aba^{-1}$  olduğundan

$$b^{16} = b^8 b^8 = a^3 b a^{-3} a^3 b a^{-3} = a^3 b^2 a^{-3} = a^3 a b a^{-1} a^{-3} = a^4 b a^{-4}$$

olup

$$b^{32} = b^{16} b^{16} = a^4 b a^{-4} a^4 b a^{-4} = a^4 b^2 a^{-4} = a^4 a b a^{-1} a^{-4} = a^5 b a^{-5}$$

eşitliği sağlanır. Burada  $\circ(a) = 5$  olduğundan  $a^5 = a^{-5} = e$  olup  $b^{32} = a^5 b a^{-5} = e b e = b$  bulunur.  $b^{32} = b$  olduğundan  $b^{31} = e$  olup Teorem 2.3.10 dan  $\circ(b) | 31$  olur.  $\circ(b) | 31$  ve 31 bir asal tam sayı olduğundan  $\circ(b) = 1$  veya  $\circ(b) = 31$  olur.

**Örnek 3.**  $G$  bir grup ve  $a, b \in G$  olsun.  $a$  ve  $bab^{-1}$  elemanlarının mertebeleri sonlu ise  $\circ(a) = \circ(bab^{-1})$  olduğunu gösteriniz.

**Çözüm.**  $a$  ve  $bab^{-1}$  elemanlarının mertebeleri sonlu olsun.  $\circ(a) = m$  ve  $\circ(bab^{-1}) = n$  diyelim.  $\circ(a) = m$  olduğundan  $a^m = e$  olup

$$\begin{aligned} (bab^{-1})^m &= \underbrace{(bab^{-1})(bab^{-1}) \dots (bab^{-1})}_{m \text{ tane}} = b \underbrace{aa \dots a}_{m \text{ tane}} b^{-1} \\ &= ba^m b^{-1} = beb^{-1} = bb^{-1} = e \end{aligned}$$

olur. Bu durumda  $m \in \mathbb{Z}^+$  ve  $\circ(bab^{-1}) = n$  olduğundan  $n \leq m$  olur.  $\circ(bab^{-1}) = n$  olduğundan

$$e = (bab^{-1})^n = \underbrace{(bab^{-1})(bab^{-1}) \dots (bab^{-1})}_{n \text{ tane}} = b \underbrace{aa \dots a}_{n \text{ tane}} b^{-1} = ba^n b^{-1}$$

olup  $a^n = b^{-1} ba^n b^{-1} b = b^{-1} e b = e$  sağlanır. Bu durumda  $n \in \mathbb{Z}^+$  ve  $\circ(a) = m$  olduğundan  $m \leq n$  olur.  $m \leq n$  ve  $n \leq m$  olduğundan  $m = n$  olup  $\circ(a) = \circ(bab^{-1})$  eşitliği elde edilir.

**Örnek 4.**  $G$  bir değişmeli grup ve  $a, b \in G$  olsun.  $\circ(a) = m$ ,  $\circ(b) = n$  ve  $(m, n) = \text{OBEB}(m, n) = 1$  ise  $\circ(ab) = mn$  olduğunu gösteriniz.

**Çözüm.**  $\circ(a) = m$ ,  $\circ(b) = n$  ve  $(m, n) = \text{OBEB}(m, n) = 1$  olsun.  $\circ(a) = m$  ve  $\circ(b) = n$  olduğundan  $a^m = b^n = e$  olup  $G$  değişmeli olduğundan  $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e^n e^m = e$  olur.  $\circ(ab) = k$  diyelim.  $(ab)^{mn} = e$ ,  $mn \in \mathbb{Z}^+$  ve  $\circ(ab) = k$  olduğundan  $k \leq mn$  olur.  $\circ(ab) = k$  olduğundan  $(ab)^k = e$  olup  $G$  değişmeli olduğundan  $e = (ab)^k = a^k b^k$  olur.  $a^k b^k = e$  olduğundan  $a^k = b^{-k}$  olup  $a^{nk} = (a^k)^n = (b^{-k})^n = b^{-kn} = (b^n)^{-k} = e^{-k} = e$  olur.  $\circ(a) = m$  ve  $a^{nk} = e$  olduğundan Teorem 2.3.10 gereği  $m|nk$  olup  $(m, n) = \text{OBEB}(m, n) = 1$  olduğundan Önerme 1.5.21 gereği  $m|k$  olur.  $a^k b^k = e$  olduğundan  $b^k = a^{-k}$  olup  $b^{mk} = (b^k)^m = (a^{-k})^m = a^{-km} = (a^m)^{-k} = e^{-k} = e$  olur.  $\circ(b) = n$  ve  $b^{mk} = e$  olduğundan Teorem 2.3.10 dan  $n|mk$  olup  $(m, n) = \text{OBEB}(m, n) = 1$  olduğundan Önerme 1.5.21 den  $n|k$  olur.  $m|k$ ,  $n|k$  ve  $(m, n) = \text{OBEB}(m, n) = 1$  olduğundan  $mn|k$  olur.  $mn|k$  ve  $mn, k \in \mathbb{Z}^+$  olduğundan  $mn \leq k$  olup ayrıca  $k \leq mn$  olduğundan  $\circ(ab) = k = mn$  olur ki bu da istenendir.

**Ödev.**  $m \in \mathbb{Z}^+$  olmak üzere  $\mathbb{Z}_m$  kümesinin  $+$  işlemine göre değişmeli bir grup olduğunu gösteriniz.

**Örnek 5.**  $\mathbb{Z}_4 \times \mathbb{Z}_6$  direkt çarpım grubunun devirli olup olmadığını araştırınız.

**Çözüm.**  $\text{OBEB}(4, 6) \neq 1$  olduğundan  $\mathbb{Z}_4 \times \mathbb{Z}_6$  direkt çarpım grubu devirli değildir.

**Örnek 6.**  $f: G \rightarrow H$  örten bir homomorfizma olsun. Eğer  $\text{Çekf}$ ,  $G$  nin bir maksimal normal alt grubu ise  $H$  nin basit grup olduğunu gösteriniz.

**Çözüm.**  $\text{Çekf}$ ,  $G$  nin bir maksimal normal alt grubu olsun. Bu durumda Teorem 2.4.20 den  $G/\text{Çekf}$  bölüm grubu basittir. Diğer taraftan  $f: G \rightarrow H$  örten homomorfizma olduğundan Homomorfizma Teoreminden  $G/\text{Çekf} \cong f(G) = H$  olur. O halde  $H$  basit olup istenen elde edilir.

**Örnek 7.**  $f: G \rightarrow H$  bir homomorfizma olsun. Eğer  $G$  basit grup ise  $f$  nin ya bire-bir ya da  $\forall a \in G$  için  $f(a) = e_H$  olduğunu gösteriniz.

**Çözüm.**  $G$  basit grup olsun. Homomorfizma Teoreminden  $\text{Çekf} \triangleleft G$  olur.  $G$  basit ve  $\text{Çekf} \triangleleft G$  olduğundan  $\text{Çekf} = \{e_G\}$  veya  $\text{Çekf} = G$  olur. Eğer burada  $\text{Çekf} = \{e_G\}$  ise Önerme 2.5.7 gereği  $f$  bire-birdir. Eğer  $\text{Çekf} = G$  ise her  $a \in G$  için  $a \in \text{Çekf}$  olup  $f(a) = e_H$  olur.

**Örnek 8.**  $m \in \mathbb{Z}^+$  olmak üzere  $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_m, +), a \rightarrow f(a) = \bar{a}$  ile tanımlı  $f$  dönüşümünün bir homomorfizma olduğunu gösteriniz ve  $\text{Çek}f$  yi bulunuz.

**Çözüm.**  $f$  nin fonksiyon olduğu açıktır. Ayrıca  $f$  nin tanımından  $\forall x, y \in \mathbb{Z}$  için  $f(x + y) = \overline{x + y} = \bar{x} + \bar{y} = f(x) + f(y)$  olup  $f$  bir homomorfizmadır.  $x \in \mathbb{Z}$  olmak üzere

$$\begin{aligned} x \in \text{Çek}f &\Leftrightarrow f(x) = \bar{0} \Leftrightarrow \bar{x} = \bar{0} \Leftrightarrow x \equiv 0 \pmod{m} \Leftrightarrow m|x - 0 = x \Leftrightarrow x \in m\mathbb{Z} \\ &= \{mk | k \in \mathbb{Z}\} \end{aligned}$$

denkliklerinden  $\text{Çek}f = m\mathbb{Z} = \{mk | k \in \mathbb{Z}\}$  elde edilir.

## 2.6. SİMETRİK GRUPLAR

**Tanım 2.6.1.**  $n \in \mathbb{Z}^+$  olmak üzere  $n$  elemanlı bir kümenin kendi üzerine bire-bir bir fonksiyonuna bu kümenin bir **permütasyonu** denir.

**Not.**  $n$  elemanlı bir kümenin her permütasyonu bu kümenin elemanlarının bir sıralanışını belirtir. Tersine  $n$  elemanlı bir kümenin elemanlarının her sıralanışı bu kümenin bir permütasyonunu belirtir.  $n$  elemanlı bir kümenin tüm permütasyonları kümesinin fonksiyonlarda bileşke işlemine göre bir grup olduğu Teorem 2.5.14 de gösterilmişti. Bu gruba **simetrik grup** veya **permütasyon grubu** denir.

**Teorem 2.6.2.**  $n$  elemanlı bir kümenin tüm permütasyonları sayısı  $n!$  dir.

**İspat.**  $n$  elemanlı herhangi  $A = \{a_1, a_2, \dots, a_n\}$  kümesini alalım.  $A = \{a_1, a_2, \dots, a_n\}$  kümesinin elemanlarını sıraladığımızda birinci sıraya  $n$  tane farklı eleman, bunların her birinde ikinci sıraya  $n - 1$  tane farklı eleman, bunların her birinde üçüncü sıraya  $n - 2$  farklı eleman, ..., bunların her birinde  $n$ . sıraya  $n - (n - 1) = 1$  farklı eleman yazabiliriz. Böylece  $A = \{a_1, a_2, \dots, a_n\}$  kümesinin elemanlarının farklı sıralanışları sayısı  $n(n - 1)(n - 2) \dots 1 = n!$  olup  $n$  elemanlı bir kümenin tüm permütasyonlarının sayısı  $n!$  olur.

**Not.**  $\sigma, L = \{x_1, x_2, \dots, x_n\}$  kümesinin bir permütasyonu ve

$$\sigma(x_1) = x_{i_1}, \sigma(x_2) = x_{i_2}, \dots, \sigma(x_n) = x_{i_n}$$

ise bu permütasyon genellikle  $\sigma = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix}$  şeklinde de gösterilir.  $M = \{1, 2, \dots, n\}$  kümesinin tüm permütasyonları kümesi genellikle  $S_n$  ile gösterilir.

**Teorem 2.6.3.**  $L = \{x_1, x_2, \dots, x_n\}$  kümesinin tüm permütasyonları kümesi  $T_n$  olsun. Bu durumda

$\varphi: T_n \rightarrow S_n, \sigma = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix} \rightarrow \varphi(\sigma) = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$  ile tanımlı  $\varphi$  dönüşümü bir grup izomorfizmasıdır.

**İspat.**  $\varphi$  nin bir fonksiyon olduğu açıktır. Herhangi  $\sigma_1, \sigma_2 \in T_n$  alalım.  $\sigma_1 = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix}$  ve  $\sigma_2 = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{j_1} & x_{j_2} & \dots & x_{j_n} \end{pmatrix}$  olsun. Bu durumda  $\sigma_1 \circ \sigma_2 = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_{j_1}} & x_{i_{j_2}} & \dots & x_{i_{j_n}} \end{pmatrix}$  olur.  $\varphi$  nin tanımından  $\varphi(\sigma_1) = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ ,  $\varphi(\sigma_2) = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$  ve  $\varphi(\sigma_1 \circ \sigma_2) = \begin{pmatrix} 1 & 2 & \dots & n \\ i_{j_1} & i_{j_2} & \dots & i_{j_n} \end{pmatrix}$  olur. Burada

$$\varphi(\sigma_1) \circ \varphi(\sigma_2) = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ i_{j_1} & i_{j_2} & \dots & i_{j_n} \end{pmatrix}$$

olup  $\varphi(\sigma_1 \circ \sigma_2) = \varphi(\sigma_1) \circ \varphi(\sigma_2)$  olur. O halde  $\varphi$  bir grup homomorfizmasıdır.  $\varphi(\sigma_1) = \varphi(\sigma_2)$  olan herhangi  $\sigma_1, \sigma_2 \in T_n$  alalım. Kabul edelim ki  $\sigma_1 = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix}$  ve  $\sigma_2 = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{j_1} & x_{j_2} & \dots & x_{j_n} \end{pmatrix}$  olsun.  $\varphi$  nin tanımından

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} = \varphi(\sigma_1) = \varphi(\sigma_2) = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

olup  $i_1 = j_1, i_2 = j_2, \dots, i_n = j_n$  eşitliği sağlanır. O halde  $\sigma_1 = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{j_1} & x_{j_2} & \dots & x_{j_n} \end{pmatrix} = \sigma_2$  dir. Böylece  $\varphi$  bire-birdir. Burada  $T_n$  ve  $S_n$  sonlu elemanlı ve  $s(T_n) = s(S_n) = n!$  olduğundan Önerme 1.3.9 gereği  $\varphi$  aynı zamanda örtendir. Böylece  $\varphi: T_n \rightarrow S_n$  bir grup izomorfizması olup istenen elde edilir.

**Not.** Teoremdaki izomorfizmadan dolayı bundan sonra simetrik grup denildiğinde  $S_n$  grubu, permütasyon denildiğinde  $S_n$  nin elemanları anlaşılacaktır.  $S_n$  deki  $\circ$  işlemi yerine de genellikle  $\cdot$  kullanılacaktır.

**Tanım 2.6.4.**  $f: M = \{1, 2, \dots, n\}$  kümesinin bir permütasyonu olmak üzere eğer birbirinden farklı  $j_1, j_2, \dots, j_k \in M$  ( $k > 1$ ) elemanları için  $f(j_1) = j_2, f(j_2) = j_3, \dots, f(j_{k-1}) = j_k, f(j_k) = j_1$  ve  $\forall x \in M - \{j_1, j_2, \dots, j_k\}$  için  $f(x) = x$  ise  $f$  permütasyonuna  **$k$  uzunluğunda bir devir** denir ve genellikle  $f = (j_1 \ j_2 \ \dots \ j_k)$  ile ifade edilir. 1 uzunluğundaki bir devir özdeşlik fonksiyonu olarak alınır. 2 uzunluğundaki devirlere **transpozisyon** denir.

**Not.**  $f = (j_1 \ j_2 \ \dots \ j_k)$  bir devir ise tanımdan  $f = (j_1 \ j_2 \ \dots \ j_k) = (j_2 \ j_3 \ \dots \ j_k \ j_1) = (j_3 \ \dots \ j_k \ j_1 \ j_2) = \dots = (j_k \ j_1 \ \dots \ j_{k-2} \ j_{k-1})$  olduğu anlaşılır.  $f = (j_1 \ j_2 \ \dots \ j_k)$  ise  $f$  devirinin tersi  $f^{-1} = (j_k \ j_{k-1} \ \dots \ j_2 \ j_1) = (j_1 \ j_k \ j_{k-1} \ \dots \ j_2)$  olur.

**Örnek.**  $(1 \ 3 \ 4) \in S_5$  deviri  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \in S_5$  permütasyonudur.

**Örnek.**  $(2 \ 4 \ 1 \ 3) \in S_6$  deviri için  $(2 \ 4 \ 1 \ 3) = (4 \ 1 \ 3 \ 2) = (1 \ 3 \ 2 \ 4) = (3 \ 2 \ 4 \ 1)$  olur. Bu devirin açık şekilde yazılışı  $(2 \ 4 \ 1 \ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 1 & 5 & 6 \end{pmatrix}$  formundadır.

**Not.** İki permütasyonun çarpımı (bileşkesi) değişmeli olmayabilir. Fakat iki devir ortak eleman bulundurmuyorsa, yani ayrık devirler ise çarpımları değişmelidir.

**Teorem 2.6.5.** Ayrık iki devirin çarpımı değişmelidir.

**İspat.**  $f = (i_1 \ i_2 \ \dots \ i_k)$ ,  $g = (j_1 \ j_2 \ \dots \ j_s) \in S_n$  iki ayrık devir olsun.  $fg = gf$  olduğu gösterilirse istenen elde edilir. Herhangi  $x \in M = \{1, 2, \dots, n\}$  alalım. Eğer  $x \notin \{i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_s\}$  ise  $f(x) = x$  ve  $g(x) = x$  olup  $(fg)(x) = f(g(x)) = f(x) = x = g(x) = g(f(x)) = (gf)(x)$  eşitliği sağlanır. Kabul edelim ki  $x \in \{i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_s\}$  olsun. Bu durumda  $x \in \{i_1, i_2, \dots, i_k\}$  veya  $x \in \{j_1, j_2, \dots, j_s\}$  dir. Eğer  $x \in \{i_1, i_2, \dots, i_k\}$  ise  $f(x) \in \{i_1, i_2, \dots, i_k\}$  olup  $x \notin \{j_1, j_2, \dots, j_s\}$  ve  $f(x) \notin \{j_1, j_2, \dots, j_s\}$  olduğundan  $g(x) = x$  ve  $g(f(x)) = f(x)$  bulunur. Bu durumda  $(gf)(x) = g(f(x)) = f(x)$  ve  $(fg)(x) = f(g(x)) = f(x)$  olup  $(fg)(x) = (gf)(x)$  eşitliği sağlanır. Eğer  $x \in \{j_1, j_2, \dots, j_s\}$  ise  $g(x) \in \{j_1, j_2, \dots, j_s\}$  olup  $x \notin \{i_1, i_2, \dots, i_k\}$  ve  $g(x) \notin \{i_1, i_2, \dots, i_k\}$  olduğundan  $f(x) = x$  ve  $f(g(x)) = g(x)$  dir. Bu durumda da  $(gf)(x) = g(f(x)) = g(x)$  ve  $(fg)(x) = f(g(x)) = g(x)$  olup  $(fg)(x) = (gf)(x)$  olur. Yani  $\forall x \in M = \{1, 2, \dots, n\}$  için  $(fg)(x) = (gf)(x)$  olup  $fg = gf$  elde edilir.

**Teorem 2.6.6.**  $r$  uzunluğundaki bir devirin mertebesi  $r$  olur.

**İspat.**  $f = (i_1 \ i_2 \ \dots \ i_r) \in S_n$   $r$  uzunluğunda bir devir ve  $M = \{1, 2, \dots, n\}$  olsun.  $\circ (f) = r$  olduğu gösterilirse istenen elde edilir.  $1 \leq j, k \leq r$  için  $j + k \leq r$  ise  $f^k(i_j) = f(f(\dots f(i_j))) = f(f(\dots f(i_{j+1}))) = \dots = i_{j+k}$  ve  $j + k > r$  ise  $f^k(i_j) = i_{j+k-r}$  olur. Bu durumda  $1 \leq j \leq r$  için  $j + r > r$  olduğundan  $f^r(i_j) = i_{j+r-r} = i_j$  olup  $f^r = I_M$

olur. Ayrıca  $1 \leq t < r$  için  $1 + t \leq r$  olduğundan  $f^t(i_1) = i_{1+t} \neq i_1$  olup  $f^t \neq I_M$  sağlanır. O halde  $\circ(f) = r$  olup istenen elde edilir.

**Teorem 2.6.7.**  $S_n$  deki her permütasyon ayrık devirlerin çarpımı olarak yazılabilir ve bu yazılış birim ve sıra düşünülme-sizin tek tür-lüdür.

**İspat.** Herhangi  $f \in S_n$  alalım.  $f$  nin mertebesi sonlu olduğundan  $f^k(1) = 1$  olacak şekilde  $\exists k \in \mathbb{Z}^+$  vardır. Bu şekildeki  $k$  pozitif tam sayılarının en küçüğüne  $t$  denilirse  $f(1), f^2(1), \dots, f^t(1) = 1$  elemanları birbirinden farklı olur. Böylece  $t$  uzunluğundaki  $(f(1) \ f^2(1) \ \dots \ f^t(1))$  deviri elde edilir. İşleme 1 yerine bu devirde gözükmeyen başka bir sayı alarak devam edilirse elde ettiğimiz devirler ayrık ve çarpımları  $f$  yi verir. Böylece  $f$  ayrık devirlerin çarpımı olarak yazılabilir.

Şimdi bu yazılışın birim ve sıra düşünülme-sizin tek tür-lü olduğunu gösterelim. Eğer  $f$  birim permütasyon ise birim düşünülmediğinden istenen elde edilir. Kabul edelim ki  $f$  birimden farklı olsun.  $f$  nin birimden farklı ayrık devirlerin çarpımı şeklinde  $f = f_1 f_2 \dots f_s$  ve  $f = g_1 g_2 \dots g_t$  yazılışlarını alalım.  $s = t$  ve  $f_1, f_2, \dots, f_s$  devirleri ile  $g_1, g_2, \dots, g_t$  devirlerinin aynı olduğunu gösterelim.  $1 \leq k \leq s$  olan herhangi  $k \in \mathbb{Z}$  alalım.  $f_k = (i_1 \ i_2 \ \dots \ i_r)$  diyelim.  $f = f_1 f_2 \dots f_s$  ve  $f_1, f_2, \dots, f_s$  devirleri ayrık olduğundan  $f(i_1) = i_2, f(i_2) = i_3, \dots, f(i_{r-1}) = i_r$  ve  $f(i_r) = i_1$  olup  $f = g_1 g_2 \dots g_t$  ve  $g_1, g_2, \dots, g_t$  devirleri ayrık olduğundan  $\exists j = 1, 2, \dots, t$  için  $g_j(i_1) = i_2, g_j(i_2) = i_3, \dots, g_j(i_{r-1}) = i_r$  ve  $g_j(i_k) = i_1$  olur. Buradan  $f_k = (i_1 \ i_2 \ \dots \ i_r) = g_j$  olduğu anlaşılır. Böylece  $s \leq t$  ve  $f_1, f_2, \dots, f_s$  devirlerinin  $g_1, g_2, \dots, g_t$  devirleri içinde olduğu anlaşılır. Benzer şekilde  $f_k$  ve  $g_j$  devirlerinin rolleri değiştirilerek  $t \leq s$  ve  $g_1, g_2, \dots, g_t$  devirlerinin de  $f_1, f_2, \dots, f_s$  devirleri içinde olduğu gösterilebilir. Böylece  $s = t$  ve  $f_1, f_2, \dots, f_s$  devirleri ile  $g_1, g_2, \dots, g_t$  devirleri aynı olup istenen elde edilir.

**Örnek.**  $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$  permütasyonunun ayrık devirlerin çarpımı şeklinde yazılışı  $f = (1 \ 5 \ 2 \ 3)(4 \ 6)$ ,  $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 3 & 6 \end{pmatrix}$  permütasyonunun ayrık devirlerin çarpımı şeklinde yazılışı  $g = (1 \ 4 \ 2)(3 \ 5)$ ,  $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix}$  permütasyonunun ayrık devirlerin çarpımı şeklinde yazılışı  $h = (1 \ 3 \ 5)(2 \ 6 \ 4)$  olur.

**Teorem 2.6.8.**  $G$  bir grup,  $a, b \in G$  ve  $ab = ba$  olsun. Bu durumda  $\forall t \in \mathbb{Z}^+$  için  $(ab)^t = a^t b^t$  olur.

**İspat.**  $ab = ba$  olduğundan  $\forall t \in \mathbb{Z}^+$  için

$$(ab)^t = \underbrace{(ab)(ab)\dots(ab)}_{t \text{ tane}} = (aa)(bb) \underbrace{(ab)(ab)\dots(ab)}_{t-2 \text{ tane}} = \dots = \underbrace{aa\dots a}_{t \text{ tane}} \underbrace{bb\dots b}_{t \text{ tane}} = a^t b^t$$

olup istenen elde edilir.

**Sonuç 2.6.9.**  $G$  bir grup,  $a_1, a_2, \dots, a_n \in G$  ve  $a_1, a_2, \dots, a_n$  elemanları kendi aralarında değişmeli olsun. Bu durumda  $\forall t \in \mathbb{Z}^+$  için  $(a_1 a_2 \dots a_n)^t = a_1^t a_2^t \dots a_n^t$  olur.

**İspat.**  $a_1, a_2, \dots, a_n$  elemanları kendi aralarında değişmeli olduğundan  $\forall t \in \mathbb{Z}^+$  için

$$(a_1 a_2 \dots a_n)^t = a_1^t (a_2 a_3 \dots a_n)^t = a_1^t a_2^t (a_3 \dots a_n)^t = \dots = a_1^t a_2^t \dots a_n^t$$

olup istenen elde edilir.

**Teorem 2.6.10.** Bir  $f \in S_n$  permütasyonunun mertebesi ayrıldığı ayrık devirlerin uzunluklarının en küçük ortak katıdır.

**İspat.**  $f$  nin ayrık devirlerin çarpımı şeklinde yazılışı  $f = f_1 f_2 \dots f_t$  olsun. Kabul edelim ki  $\circ(f) = m$  ve  $1 \leq i \leq t$  için  $\circ(f_i) = m_i$  olsun.  $k = [m_1, m_2, \dots, m_t] = \text{OKEK}(m_1, m_2, \dots, m_t)$  ve  $M = \{1, 2, \dots, n\}$  diyelim.  $m = k$  olduğu gösterilirse istenen elde edilir.  $1 \leq i \leq t$  için  $m_i | k$  olduğundan  $f_i^k = I_M$  olur. Bu durumda  $f_1, f_2, \dots, f_t$  elemanları kendi aralarında değişmeli olduğundan  $f^k = (f_1 f_2 \dots f_t)^k = f_1^k f_2^k \dots f_t^k = I_M$  olup  $\circ(f) = m$  olduğundan  $m \leq k$  olur.

$1 \leq i \leq t$  olan herhangi  $i \in \mathbb{Z}$  alalım.  $f_i = (j_1 \ j_2 \ \dots \ j_{m_i})$  diyelim.  $f^m = I_M$  ve  $f_1, f_2, \dots, f_t$  devirleri ayrık olduğundan  $1 \leq s \leq m_i$  için  $f_i^m(j_s) = f^m(j_s) = j_s$  olup ayrıca varsa  $\forall x \in M - \{j_1, j_2, \dots, j_{m_i}\}$  için  $f_i^m(x) = x$  olduğundan  $f_i^m = I_M$  olur. Bu durumda  $\circ(f_i) = m_i$  olduğundan Teorem 2.3.10 gereği  $m_i | m$  olur. Yani  $1 \leq i \leq t$  için  $m_i | m$  olup  $m > 0$  ve  $k = [m_1, m_2, \dots, m_t] = \text{OKEK}(m_1, m_2, \dots, m_t)$  olduğundan  $k \leq m$  bulunur.  $m \leq k$  ve  $k \leq m$  olduğundan  $m = k$  olup istenen elde edilir.

**Örnek.**  $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix}$  permütasyonunun ayrık devirlerin çarpımı şeklinde yazılışı  $f = (1 \ 6 \ 3)(2 \ 5)$  olduğundan Teorem 2.6.10 dan  $\circ(f) = [3, 2] = 6$  olur.

**Sonuç 2.6.11.** Her devir sonlu sayıda ikili devirlerin (transpozisyonların) bir çarpımı olarak yazılabilir.

**İspat.**  $(i_1 \ i_2 \ \dots \ i_k) \in S_n$  deviri verilsin.  $(i_1 \ i_2 \ \dots \ i_k) = (i_1 \ i_k)(i_1 \ i_{k-1}) \dots (i_1 \ i_2)$  olduğundan bu devir sonlu sayıda ikili devirlerin çarpımı olarak yazılabilir. Yani her devir sonlu sayıda ikili devirlerin çarpımı olarak yazılabilir.

**Tanım 2.6.12.** Bir permütasyon çift sayıda ikili devirlerin çarpımı ise bu permütasyona bir **çift permütasyon**, tek sayıda ikili devirlerin çarpımı ise bu permütasyona bir **tek permütasyon** denir.  $S_n$  deki tüm çift permütasyonlar kümesi  $A_n$  ile gösterilir.

**Not.** Bir devirin ikili devirlerin çarpımı olarak yazılışı tek türlü değildir. Ancak bir permütasyonun ayrıldığı ikili devirlerin sayısının teklik ve çiftliği değişmez. Her transpozisyonun mertebesi 2 olduğundan her permütasyon transpozisyonların çarpımı biçiminde tek türlü olarak ifade edilmeyebilir.

**Örnek.**  $f = (1 \ 4 \ 5 \ 2) \in S_5$  deviri için

$$f = (1 \ 4 \ 5 \ 2) = (1 \ 2)(1 \ 5)(1 \ 4) = (1 \ 2)(1 \ 5)(1 \ 4)(2 \ 3)(2 \ 3) \text{ olur.}$$

**Teorem 2.6.13.**  $n \geq 2$  olmak üzere  $S_n$  deki tüm çift permütasyonlar kümesi  $A_n$ ,  $S_n$  nin  $n!/2$  elemanlı bir alt grubudur. Bu alt gruba  **$n$ . alterne grup** denir.

**İspat.**  $M = \{1, 2, \dots, n\}$  diyelim.  $a, b \in M$  ve  $a \neq b$  olmak üzere  $I_M = (a \ b)(a \ b)$  olduğundan  $I_M \in A_n$  olup  $\emptyset \neq A_n \subset S_n$  olur. Herhangi  $f, g \in A_n$  alalım.  $f, g \in A_n$  olduğundan  $f$  ve  $g$  permütasyonları çift sayıda ikili devirlerin çarpımı olup  $fg$  de çift sayıda ikili devirlerin çarpımı olur. O halde  $fg \in A_n$  olup ayrıca  $S_n$  sonlu grup olduğundan  $A_n < S_n$  olur.

Şimdi  $S_n$  deki çift permütasyonların sayısı ile tek permütasyonların sayısının eşit olduğu gösterilirse  $\circ(S_n) = n!$  olduğundan istenen elde edilir.  $S_n$  de çift permütasyonların sayısı  $n_1$  ve tek permütasyonların sayısı da  $n_2$  olsun.  $n \geq 2$  olduğundan  $a \neq b$  olacak şekilde  $\exists a, b \in M$  vardır.  $S_n$  deki her  $f$  çift permütasyonu için  $(a \ b)f$  bir tek permütasyondur. Bu şekilde birbirinden farklı çift permütasyonlardan birbirinden farklı tek permütasyonlar elde edilir. O halde  $n_1 \leq n_2$  olur. Tersine,  $S_n$  deki her  $g$  tek permütasyonu için  $(a \ b)g$  bir çift permütasyondur. Bu şekilde birbirinden farklı tek permütasyonlardan, birbirinden farklı çift permütasyonlar elde edilir. O halde  $n_2 \leq n_1$  olur.  $n_1 \leq n_2$  ve  $n_2 \leq n_1$  olduğundan  $n_1 = n_2$  olup istenen elde edilir.

**Sonuç 2.6.14.**  $n \geq 2$  olmak üzere  $A_n$ ,  $S_n$  nin indeksi 2 olan normal alt grubudur.

**İspat.** Teorem 2.4.15 gereği  $(S_n : A_n) = \frac{n!}{n!/2} = 2$  ve  $A_n \triangleleft S_n$  olup istenen elde edilir.

**Örnek.**  $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} \in S_5$  permütasyonu için

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

ve  $(3 \ 5)f = (3 \ 5) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$  olur.

**Tanım 2.6.15.**  $G$  bir grup ve  $a, b \in G$  olsun. Eğer  $b = xax^{-1}$  olacak şekilde  $\exists x \in G$  varsa  $b$  elemanına  $a$  nın ( $x$  ile) **eşleniği** denir ve bu durum  $a \approx b$  ile ifade edilir.

**Teorem 2.6.16.** Yukarıda tanımlanan  $\approx$  eşlenik olma bağıntısı  $G$  de bir denklik bağıntısıdır.

**İspat. Yansıma:**  $\forall a \in G$  için  $a = eae^{-1}$  olduğundan  $a \approx a$  olup  $\approx$  bağıntısının yansıma özelliği vardır.

**Simetri:**  $a \approx b$  olan herhangi  $a, b \in G$  alalım.  $a \approx b$  olduğundan  $b = xax^{-1}$  olacak şekilde  $\exists x \in G$  vardır.  $b = xax^{-1}$  olduğundan  $a = x^{-1}bx = x^{-1}b(x^{-1})^{-1}$  olup  $x^{-1} = y$  alınırsa  $y \in G$  ve  $a = yby^{-1}$  olur. O halde  $b \approx a$  olup  $\approx$  bağıntısının simetri özelliği vardır.

**Geçişme:**  $a \approx b$  ve  $b \approx c$  olan herhangi  $a, b, c \in G$  alalım.  $a \approx b$  olduğundan  $b = xax^{-1}$  olacak şekilde  $\exists x \in G$  vardır.  $b \approx c$  olduğundan  $c = yby^{-1}$  olacak şekilde  $\exists y \in G$  vardır. Burada  $c = yby^{-1} = yxax^{-1}y^{-1} = yxa(yx)^{-1}$  olup  $z = yx$  alınırsa  $z \in G$  ve  $c = zaz^{-1}$  olur. O halde  $a \approx c$  olup  $\approx$  bağıntısının geçişme özelliği vardır.

Böylece  $\approx$  bağıntısı bir denklik bağıntısı olup istenen elde edilir.

**Tanım 2.6.17.**  $G$  de  $\approx$  denklik bağıntısının belirttiği denklik sınıflarına **eşlenik sınıfları** denir. Bir  $a \in G$  nin belirttiği eşlenik sınıfı  $C(a)$  ile gösterilir. Burada  $C(a) = \{x \in G | a \approx x\}$  olur.

**Not.** Denklik sınıfları kümenin ayrışımını belirttiğinden  $G$  sonlu bir grup ise grubun mertebesi birbirinden farklı eşlenik sınıflarındaki elemanların sayıları toplamıdır.  $a \in G$  olmak üzere  $C(a)$  eşlenik sınıfının eleman sayısı genellikle  $c_a$  ile gösterilir. Burada  $c_a$ ,  $G$  de  $a$  ile eşlenik olan elemanların sayısıdır. Eğer  $G$  de birbirinden farklı tüm eşlenik sınıflarının kümesi  $a_1, a_2, \dots, a_k \in G$  olmak üzere  $\{C(a_1), C(a_2), \dots, C(a_k)\}$  ise  $G$  nin eşlenik sınıflarına ayrışımı  $G = C(a_1) \cup C(a_2) \cup \dots \cup C(a_k)$  olup  $o(G) = c_{a_1} + c_{a_2} + \dots + c_{a_k}$  olur.

Şimdi  $S_n$ deki bir elemanın eşleniklerini ve  $S_n$  nin eşlenik sınıflarına ayrışımını inceleyelim.

**Teorem 2.6.18.** Bir  $\sigma \in S_n$  için  $\sigma(i_1 \ i_2 \ \dots \ i_r)\sigma^{-1} = (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r))$  olur.

**İspat.** Herhangi  $x \in M = \{1, 2, \dots, n\}$  alalım. Eğer  $x \notin \{\sigma(i_1), \sigma(i_2), \dots, \sigma(i_r)\}$  ise  $\sigma^{-1}(x) \notin \{i_1, i_2, \dots, i_r\}$  olur. Bu durumda  $(\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r))(x) = x$  ve

$$(\sigma(i_1 \ i_2 \ \dots \ i_r)\sigma^{-1})(x) = \sigma\left((i_1 \ i_2 \ \dots \ i_r)(\sigma^{-1}(x))\right) = \sigma(\sigma^{-1}(x)) = x$$

olup  $(\sigma(i_1 \ i_2 \ \dots \ i_r)\sigma^{-1})(x) = (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r))(x)$  sağlanır. Kabul edelim ki  $x \in \{\sigma(i_1), \sigma(i_2), \dots, \sigma(i_r)\}$  olsun. Bu durumda  $\exists k = 1, 2, \dots, r$  için  $x = \sigma(i_k)$  olur.  $x = \sigma(i_k)$  olduğundan  $\sigma^{-1}(x) = i_k$  dir. Eğer  $k < r$  ise

$$(\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r))(x) = (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r))(\sigma(i_k)) = \sigma(i_{k+1})$$

ve

$$\begin{aligned} (\sigma(i_1 \ i_2 \ \dots \ i_r)\sigma^{-1})(x) &= \sigma\left((i_1 \ i_2 \ \dots \ i_r)(\sigma^{-1}(x))\right) \\ &= \sigma((i_1 \ i_2 \ \dots \ i_r)(i_k)) = \sigma(i_{k+1}) \end{aligned}$$

olup  $(\sigma(i_1 \ i_2 \ \dots \ i_r)\sigma^{-1})(x) = (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r))(x)$  bulunur. Eğer  $k = r$  ise

$$(\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r))(x) = (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r))(\sigma(i_r)) = \sigma(i_1)$$

ve

$$\begin{aligned} (\sigma(i_1 \ i_2 \ \dots \ i_r)\sigma^{-1})(x) &= \sigma\left((i_1 \ i_2 \ \dots \ i_r)(\sigma^{-1}(x))\right) \\ &= \sigma((i_1 \ i_2 \ \dots \ i_r)(i_r)) = \sigma(i_1) \end{aligned}$$

olup yine  $(\sigma(i_1 \ i_2 \ \dots \ i_r)\sigma^{-1})(x) = (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r))(x)$  eşitliği elde edilir.

Yani  $\forall x \in M = \{1, 2, \dots, n\}$  için

$$(\sigma(i_1 \ i_2 \ \dots \ i_r)\sigma^{-1})(x) = (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r))(x)$$

olup  $\sigma(i_1 \ i_2 \ \dots \ i_r)\sigma^{-1} = (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r))$  bulunur.

**Sonuç 2.6.19.** İki devirin eşlenik olması için gerek ve yeter koşul bu iki devirin aynı uzunluklara sahip olmalarıdır.

**İspat.**  $(\Rightarrow)$  Teorem 2.6.18 den açıktır.

$(\Leftarrow)$   $S_n$  de uzunlukları eşit herhangi iki  $(i_1 \ i_2 \ \dots \ i_r)$  ve  $(j_1 \ j_2 \ \dots \ j_r)$  devirleri verilsin. Bu devirlerin eşlenik olduğu gösterilirse istenen elde edilir.  $1 \leq k \leq r$  için  $j_k$  elemanını  $i_k$  nin altına ve  $M = \{1, 2, \dots, n\}$  kümesinin varsa  $j_1, j_2, \dots, j_r$  dışındaki elemanlarını da bu kümenin  $i_1, i_2, \dots, i_r$  elemanları dışındaki elemanlarının altına yazarak bir  $\sigma$  permütasyonu oluşturulabilir.  $1 \leq k \leq r$  için  $\sigma(i_k) = j_k$  olduğundan Teorem 2.6.18 gereği

$$(j_1 \ j_2 \ \dots \ j_r) = (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_r)) = \sigma(i_1 \ i_2 \ \dots \ i_r)\sigma^{-1}$$

olup  $(i_1 \ i_2 \ \dots \ i_r)$  ve  $(j_1 \ j_2 \ \dots \ j_r)$  devirleri eşleniktir.

**Teorem 2.6.20.**  $S_n$  deki iki permütasyonun eşlenik olması için gerek ve yeter koşul bu permütasyonların ayrık devirlere ayrılışındaki devirlerin sayısının ve uzunluklarının aynı olmasıdır.

**İspat.** ( $\Rightarrow$ )  $S_n$  de eşlenik herhangi iki  $f$  ve  $g$  permütasyonlarını alalım.  $f$  ve  $g$  nin ayrık devirlere ayrılışındaki devirlerin sayısının ve uzunluklarının aynı olduğu gösterilirse istenen elde edilir.  $f$  nin ayrık devirlerin çarpımı şeklinde yazılışı  $f = f_1 f_2 \dots f_r$  olsun.  $f \approx g$  olduğundan  $g = \sigma f \sigma^{-1}$  olacak şekilde  $\exists \sigma \in S_n$  vardır. Burada  $g = \sigma f \sigma^{-1} = \sigma f_1 f_2 \dots f_r \sigma^{-1} = \sigma f_1 \sigma^{-1} \sigma f_2 \sigma^{-1} \dots \sigma f_r \sigma^{-1}$  olup  $1 \leq i \leq r$  için  $g_i = \sigma f_i \sigma^{-1}$  alınır.  $g$  nin ayrık devirlere ayrılışı  $g = g_1 g_2 \dots g_r$  biçimindedir. Ayrıca  $1 \leq i \leq r$  için  $g_i = \sigma f_i \sigma^{-1}$  olduğundan  $f_i$  ile  $g_i$  devirlerinin uzunlukları aynı olup istenen elde edilir.

( $\Leftarrow$ )  $f, g \in S_n$  için  $f$  ve  $g$  nin ayrık devirlere ayrılışı sırasıyla  $f = f_1 f_2 \dots f_r$  ve  $g = g_1 g_2 \dots g_r$  olmak üzere kabul edelim ki  $1 \leq i \leq r$  için  $f_i$  ile  $g_i$  devirlerinin uzunlukları aynı olsun.  $f \approx g$  olduğu gösterilirse istenen elde edilir. Burada  $1 \leq i \leq r$  için  $g_i$  devirinin elemanlarını  $f_i$  devirinin aynı sıradaki elemanlarının altına ve  $M = \{1, 2, \dots, n\}$  kümesinin varsa  $g_1, g_2, \dots, g_r$  devirlerinin elemanları dışındaki elemanlarını da bu kümenin  $f_1, f_2, \dots, f_r$  devirlerinin elemanları dışındaki elemanlarının altına yazarak bir  $\sigma$  permütasyonu oluşturulabilir. Bu durumda  $1 \leq i \leq r$  için  $g_i = \sigma f_i \sigma^{-1}$  olup  $g = g_1 g_2 \dots g_r = \sigma f_1 \sigma^{-1} \sigma f_2 \sigma^{-1} \dots \sigma f_r \sigma^{-1} = \sigma f \sigma^{-1}$  olur. Buradan  $f \approx g$  bulunur.

**Örnek.**  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix} \in S_6$  permütasyonu için

$\sigma(2 \ 1 \ 3 \ 4) \sigma^{-1} = (\sigma(2) \ \sigma(1) \ \sigma(3) \ \sigma(4)) = (5 \ 6 \ 1 \ 4)$  olur.

**Örnek.**  $S_6$  da  $(2 \ 1 \ 5)$  ile  $(4 \ 2 \ 3)$  devirleri birbirine denktir. Şimdi  $S_6$  da  $\sigma(2 \ 1 \ 5) \sigma^{-1} = (4 \ 2 \ 3)$  şartını sağlayan  $\sigma$  permütasyonlarının kümesini bulalım. Bunun için  $(\sigma(2) \ \sigma(1) \ \sigma(5)) = (4 \ 2 \ 3)$  şartını sağlayan permütasyonlar bulunmalıdır. Bu permütasyonlar

$$\begin{aligned} \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 3 & 6 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 6 & 3 & 5 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}, \\ \sigma_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 6 & 3 & 1 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 3 & 1 \end{pmatrix}, \\ \sigma_7 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 5 & 2 & 6 \end{pmatrix}, \sigma_8 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix}, \sigma_9 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix}, \\ \sigma_{10} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 6 & 2 & 1 \end{pmatrix}, \sigma_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 2 & 5 \end{pmatrix}, \sigma_{12} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 5 & 2 & 1 \end{pmatrix} \end{aligned}$$

$$\sigma_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 4 & 6 \end{pmatrix}, \sigma_{14} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 4 & 5 \end{pmatrix}, \sigma_{15} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix},$$

$$\sigma_{16} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 6 & 4 & 1 \end{pmatrix}, \sigma_{17} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 4 & 5 \end{pmatrix}, \sigma_{18} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 5 & 4 & 1 \end{pmatrix}$$

olup yukarıdaki şartı sağlayan  $\sigma$  permütasyonlarının kümesi

$$\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}, \sigma_{16}, \sigma_{17}, \sigma_{18}\}$$

kümesidir.

**Örnek.**  $S_6$  da  $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix}$  permütasyonunun  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 6 & 2 & 5 \end{pmatrix}$  permütasyonu ile eşleniğini bulalım.

**Çözüm.**  $f$  nin ayırık devirlerin çarpımı şeklinde yazılışı  $f = (1 \ 4 \ 3)(2 \ 6)$ dır. O halde  $f$  nin  $\sigma$  permütasyonu ile eşleniği

$$\begin{aligned} \sigma f \sigma^{-1} &= \sigma(1 \ 4 \ 3)(2 \ 6)\sigma^{-1} = \sigma(1 \ 4 \ 3)\sigma^{-1}\sigma(2 \ 6)\sigma^{-1} \\ &= (\sigma(1) \ \sigma(4) \ \sigma(3))(\sigma(2) \ \sigma(6)) = (3 \ 6 \ 4)(1 \ 5) \end{aligned}$$

olur.

**Tanım 2.6.21.**  $n \in \mathbb{Z}^+$  olsun.  $n_1 \leq n_2 \leq \dots \leq n_r$  ve  $n = n_1 + n_2 + \dots + n_r$  koşullarını sağlayan bir  $n_1, n_2, \dots, n_r$  pozitif tam sayılar dizisine  **$n$  nin bir ayrışımı** denir.  $n$  nin tüm ayrışimleri sayısı  $p(n)$  ile gösterilir.

**Örnek.** 1 in ayrışımı sadece  $1=1$  olduğundan  $p(1) = 1$  olur.

2 nin ayrışimleri  $2=2$  ve  $2=1+1$  olduğundan  $p(2) = 2$  olur.

3 ün ayrışimleri  $3=3$ ,  $3=1+2$  ve  $3=1+1+1$  olduğundan  $p(3) = 3$  olur.

4 ün ayrışimleri  $4=4$ ,  $4=1+3$ ,  $4=1+1+2$ ,  $4=1+1+1+1$  ve  $4=2+2$  olduğundan  $p(4) = 5$  olur.

**Teorem 2.6.22.**  $S_n$  deki farklı eşlenik sınıflarının sayısı  $p(n)$  olur.

**İspat.** Teorem 2.6.18 den bir eşlenik sınıfındaki tüm permütasyonların ayırık devirlere ayrılışındaki devirlerin sayısı ve bu devirlerin uzunlukları aynıdır.  $S_n$  de bir permütasyonu ayırık devirlere ayrıldığında bu devirlere  $M = \{1, 2, \dots, n\}$  kümesinin bu devirlerdeki elemanlar dışındaki eleman sayısı kadar 1 uzunluğunda devirler ilave edildiğinde elde edilen devirlerin uzunlukları toplamı  $n$  yi verir. Yani  $S_n$  deki her permütasyona  $n$  nin bir ayrışımı karşılık gelir. Tersine,  $n$  nin her  $n = n_1 + n_2 + \dots + n_r$  ( $0 < n_1 \leq n_2 \leq \dots \leq n_r$ ) ayrışımına karşılık uzunlukları sırasıyla  $n_1, n_2, \dots, n_r$  olan  $f_1, f_2, \dots, f_r$  devirleri ve bunların çarpımı olan  $f = f_1 f_2 \dots f_r \in S_n$  permütasyonu vardır. O halde  $S_n$  deki farklı eşlenik sınıflarının sayısı  $p(n)$  olup istenen elde edilir.

**Örnek.**  $p(4) = 5$  olduğundan  $S_4$  de farklı eşlenik sınıflarının sayısı 5 olur. Bu sınıflar aşağıdakilerdir:

$$\begin{aligned} C_1 &= \{I\}, \\ C_2 &= \{(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}, \\ C_3 &= \{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)\}, \\ C_4 &= \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, \\ C_5 &= \{(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\}. \end{aligned}$$

**Teorem 2.6.23.**  $A_n$ , tüm üçlü devirlerin kümesi ile üretilmiştir.

**İspat.**  $S_n$  nin tüm üçlü devirlerinin ürettiği alt grubuna  $T$  diyelim.  $T = A_n$  olduğu gösterilirse istenen elde edilir. Herhangi  $f = (i_1\ i_2\ i_3)$  üçlü devirini alalım.  $f = (i_1\ i_2\ i_3) = (i_1\ i_3)(i_1\ i_2)$  olduğundan  $f \in A_n$  olur. O halde  $T \subset A_n$  olur. Şimdi ters kapsamayı gösterelim. Bunun için  $S_n$  de her  $(a\ b)$  ve  $(c\ d)$  transpozisyonları için  $(a\ b)(c\ d) \in T$  olduğunu göstermemiz yeterlidir.  $S_n$  de herhangi  $(a\ b)$  ve  $(c\ d)$  transpozisyonları verilsin. Eğer  $(a\ b) = (c\ d)$  ise  $(a\ b)(c\ d) = I_M \in T$  olur. Eğer  $b = c$  ve  $a \neq d$  ise  $(a\ b)(c\ d) = (a\ b)(b\ d) = (a\ b\ d) \in T$  dir. Eğer  $a, b, c, d$  sayıları birbirinden farklı ise yine  $(a\ b)(c\ d) = (a\ b\ c)(b\ c\ d) \in T$  bulunur. Böylece  $A_n \subset T$  olup ayrıca  $T \subset A_n$  olduğundan  $T = A_n$  olur.

**Teorem 2.6.24.**  $n \geq 5$  ve  $N \triangleleft A_n$  olsun. Eğer  $N$  bir üçlü devir kapsarsa  $N = A_n$  olur.

**İspat.**  $N$  bir üçlü  $(i_1\ i_2\ i_3)$  devirini kapsasın.  $N$  nin bütün üçlü devirleri kapsadığı gösterilirse istenen elde edilir.  $n \geq 5$  olduğundan  $S_n$  de  $(i_1\ i_2\ i_3)$  deviri ile ayrık en az bir  $(a\ b)$  transpozisyonu vardır. Herhangi  $(j_1\ j_2\ j_3)$  üçlü devirini alalım. Sonuç 2.6.19 dan  $(i_1\ i_2\ i_3)$  ile  $(j_1\ j_2\ j_3)$  devirleri eşlenik olup  $(j_1\ j_2\ j_3) = \sigma(i_1\ i_2\ i_3)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \sigma(i_3))$  olacak şekilde  $\exists \sigma \in S_n$  vardır. Eğer burada  $\sigma \in A_n$  ise  $(i_1\ i_2\ i_3) \in N$  ve  $N \triangleleft A_n$  olduğundan  $(j_1\ j_2\ j_3) = \sigma(i_1\ i_2\ i_3)\sigma^{-1} \in N$  sağlanır.  $\sigma \notin A_n$  olsun. Bu durumda  $f = \sigma(a\ b)$  alınırsa  $f \in A_n$  olur. Burada  $(i_1\ i_2\ i_3)$  deviri ile  $(a\ b)$  deviri ayrık olduğundan  $f(i_1) = \sigma(i_1)$ ,  $f(i_2) = \sigma(i_2)$  ve  $f(i_3) = \sigma(i_3)$  olup

$(j_1\ j_2\ j_3) = (\sigma(i_1)\ \sigma(i_2)\ \sigma(i_3)) = (f(i_1)\ f(i_2)\ f(i_3)) = f(i_1\ i_2\ i_3)f^{-1}$  sağlanır. Bu durumda yine  $N \triangleleft A_n$  olduğundan  $(j_1\ j_2\ j_3) = f(i_1\ i_2\ i_3)f^{-1} \in N$  bulunur. Yani  $N$  bütün üçlü devirleri kapsar.

**Teorem 2.6.25.**  $A_n$  alterne grubunun basit grup olması için gerek ve yeter koşul  $n \neq 4$  olmasıdır.

**İspat.**  $(\Rightarrow)$   $A_n$  alterne grubu basit grup olsun. Eğer  $n = 4$  ise  $A_4$  ün  $V_4 = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$  alt grubu için  $V_4 \triangleleft A_4$  olur. Dahası,  $V_4 \triangleleft S_4$

olur. Çünkü  $V_4$  deki her elemanın her  $\sigma \in S_4$  ile eşleniği yine  $V_4$  ün bir elemanı olur. Ayrıca  $V_4 \neq \{I\}$  ve  $V_4 \neq A_4$  olduğundan  $A_4$  basit grup değildir. O halde  $n \neq 4$  olup istenen elde edilir. ( $\Leftarrow$ )  $n \neq 4$  olsun. Eğer  $n = 2$  ise  $s(A_2) = \frac{2!}{2} = 1$  olduğundan  $A_2 = \{I\}$  olup basit gruptur. Eğer  $n = 3$  ise  $s(A_3) = \frac{3!}{2} = 3$  ve 3 bir asal sayı olduğundan  $A_3$  grubu da basittir. Kabul edelim ki  $n \geq 5$  olsun.  $A_n$  nin  $\{I_M\}$  den farklı herhangi  $N$  normal alt grubunu alalım.  $N = A_n$  olduğu gösterilirse istenen elde edilir. Bunun için ispatı aşağıdaki altı durumda yapmak yeterlidir.

**1. durum:** Eğer  $N$  normal alt grubu bir üçlü devir kapsarsa, Teorem 2.6.24 den  $N = A_n$  olur.

**2. durum:**  $N$  normal alt grubu  $r \geq 4$  olmak üzere, ayırık devirlere ayrılışında  $r$  uzunluğunda en az bir  $(i_1 \ i_2 \ \dots \ i_r)$  deviri bulunan bir  $\sigma$  permütasyonunu kapsasın. Burada  $\sigma$  nın ayırık devirlere ayrılışındaki (varsa)  $(i_1 \ i_2 \ \dots \ i_r)$  deviri dışındaki devirlerin çarpımına  $f$  denilirse  $\sigma = (i_1 \ i_2 \ \dots \ i_r)f$  şeklinde olur.  $g = (i_1 \ i_2 \ i_3) \in A_n$  elemanı alınırsa  $\sigma \in N$  ve  $N \triangleleft A_n$  olduğundan  $g\sigma g^{-1} \in N$  olup ayrıca  $\sigma^{-1} \in N$  olduğundan  $\sigma^{-1}g\sigma g^{-1} \in N$  olur. Diğer taraftan

$$\begin{aligned} \sigma^{-1}g\sigma g^{-1} &= f^{-1}(i_r \ i_{r-1} \ \dots \ i_1)(i_1 \ i_2 \ i_3)(i_1 \ i_2 \ \dots \ i_r)f(i_3 \ i_2 \ i_1) = \\ &= f^{-1}f(i_r \ i_{r-1} \ \dots \ i_1)(i_1 \ i_2 \ i_3)(i_1 \ i_2 \ \dots \ i_r)(i_3 \ i_2 \ i_1) = (i_1 \ i_3 \ i_r) \end{aligned}$$

olur. O halde  $(i_1 \ i_3 \ i_r) \in N$  olup 1. durumdan  $N = A_n$  olur.

**3. durum:**  $N$  normal alt grubu, ayırık devirlere ayrılışında iki tane ayırık  $(i_1 \ i_2 \ i_3)$  ve  $(i_4 \ i_5 \ i_6)$  devirleri bulunan bir  $\sigma$  permütasyonunu kapsasın. Burada  $\sigma$  nın ayırık devirlere ayrılışındaki (varsa)  $(i_1 \ i_2 \ i_3)$  ve  $(i_4 \ i_5 \ i_6)$  devirleri dışındaki devirlerin çarpımına  $f$  denilirse  $\sigma = (i_1 \ i_2 \ i_3)(i_4 \ i_5 \ i_6)f$  biçiminde bulunur.  $g = (i_1 \ i_2 \ i_4) \in A_n$  elemanı alınırsa  $\sigma \in N$  ve  $N \triangleleft A_n$  olduğundan  $g\sigma g^{-1} \in N$  olup ayrıca  $\sigma^{-1} \in N$  olduğundan  $\sigma^{-1}g\sigma g^{-1} \in N$  olur. Diğer taraftan

$$\begin{aligned} \sigma^{-1}g\sigma g^{-1} &= f^{-1}(i_6 \ i_5 \ i_4)(i_3 \ i_2 \ i_1)(i_1 \ i_2 \ i_4)(i_1 \ i_2 \ i_3)(i_4 \ i_5 \ i_6)f(i_4 \ i_2 \ i_1) \\ &= f^{-1}f(i_6 \ i_5 \ i_4)(i_3 \ i_2 \ i_1)(i_1 \ i_2 \ i_4)(i_1 \ i_2 \ i_3)(i_4 \ i_5 \ i_6)(i_4 \ i_2 \ i_1) \\ &= (i_1 \ i_4 \ i_2 \ i_6 \ i_3) \end{aligned}$$

biçimindedir. O halde  $(i_1 \ i_4 \ i_2 \ i_6 \ i_3) \in N$  olup 2. durumdan  $N = A_n$  olur.

**4. durum:**  $N$  normal alt grubu, ayırık devirlere ayrılışında bir tane  $(i_1 \ i_2 \ i_3)$  üçlü deviri ve diğerleri ikili devirler olan bir  $\sigma$  permütasyonunu kapsasın. Burada ikili devirlerin çarpımına  $f$  denilirse  $\sigma = (i_1 \ i_2 \ i_3)f$  bulunur.  $N \triangleleft A_n$  olduğundan  $\sigma^2 \in N$  olur. Burada  $f$  ayırık transpozisyonların çarpımı olduğundan  $f^2 = I_M$  olup

$$\sigma^2 = (i_1 \ i_2 \ i_3)^2 f^2 = (i_1 \ i_2 \ i_3)(i_1 \ i_2 \ i_3) = (i_1 \ i_3 \ i_2)$$

elde edilir. O halde  $(i_1 \ i_3 \ i_2) \in N$  olup 1. durumdan  $N = A_n$  bulunur.

**5. durum:**  $N$  normal alt grubu, iki ayrık  $(i_1 \ i_2)$  ve  $(i_3 \ i_4)$  devirlerinin çarpımı olan bir  $\sigma$  permütasyonunu kapsasın.  $n \geq 5$  olduğundan  $\exists i_5 \in \{1, 2, \dots, n\} - \{i_1, i_2, i_3, i_4\}$  vardır.  $g = (i_1 \ i_3 \ i_5) \in A_n$  elemanı alınırsa  $\sigma \in N$  ve  $N \triangleleft A_n$  olduğundan  $g\sigma g^{-1} \in N$  olup ayrıca  $\sigma^{-1} \in N$  olduğundan  $\sigma^{-1}g\sigma g^{-1} \in N$  olur. Diğer taraftan

$$\begin{aligned}\sigma^{-1}g\sigma g^{-1} &= (i_1 \ i_2)(i_3 \ i_4)(i_1 \ i_3 \ i_5)(i_1 \ i_2)(i_3 \ i_4)(i_5 \ i_3 \ i_1) \\ &= (i_1 \ i_2 \ i_4 \ i_5 \ i_3)\end{aligned}$$

eşitliği vardır. O halde  $(i_1 \ i_2 \ i_4 \ i_5 \ i_3) \in N$  olup 2. durumdan  $N = A_n$  olur.

**6. durum:**  $N$  normal alt grubu, ikiden fazla ayrık transpozisyonların çarpımı olan bir  $\sigma$  permütasyonunu kapsasın. Buradaki transpozisyonların ilk üçü  $(i_1 \ i_2)$ ,  $(i_3 \ i_4)$  ve  $(i_5 \ i_6)$  ise diğerlerinin çarpımına  $f$  denilirse  $\sigma = (i_1 \ i_2)(i_3 \ i_4)(i_5 \ i_6)f$  olur.  $g = (i_1 \ i_3 \ i_5) \in A_n$  elemanı alınırsa  $\sigma \in N$  ve  $N \triangleleft A_n$  olduğundan  $g\sigma g^{-1} \in N$  bulunur. Ayrıca  $\sigma^{-1} \in N$  olduğundan  $\sigma^{-1}g\sigma g^{-1} \in N$  olur. Diğer taraftan

$$\begin{aligned}\sigma^{-1}g\sigma g^{-1} &= f^{-1}(i_1 \ i_2)(i_3 \ i_4)(i_5 \ i_6)(i_1 \ i_3 \ i_5)(i_1 \ i_2)(i_3 \ i_4)(i_5 \ i_6)f(i_5 \ i_3 \ i_1) \\ &= f^{-1}f(i_1 \ i_2)(i_3 \ i_4)(i_5 \ i_6)(i_1 \ i_3 \ i_5)(i_1 \ i_2)(i_3 \ i_4)(i_5 \ i_6)(i_5 \ i_3 \ i_1) \\ &= (i_1 \ i_5 \ i_3)(i_2 \ i_4 \ i_6)\end{aligned}$$

olur. O halde  $(i_1 \ i_5 \ i_3)(i_2 \ i_4 \ i_6) \in N$  olup 3. durumdan  $N = A_n$  olur.

Sonuç olarak  $N = A_n$  olup istenen elde edilir.

**Tanım 2.6.26.** Teorem 2.6.25 in ispatında geçen  $V_4$  grubuna **Klein'in 4-lü grubu** denir.  $V_4$  devirli olmayan değişmeli bir gruptur.

**Tanım 2.6.27.**  $G$  bir grup ve  $p$  bir asal tam sayı olsun. Eğer  $G$  nin her elemanının mertebesi  $p$  nin bir kuvveti ise  $G$  ye bir  **$p$ -grup** denir.  $G$  nin  $H$  alt grubu bir  $p$ -grup ise  $H$  ye  $G$  nin  **$p$ -alt grubu** denir.

**Teorem 2.6.28.**  $G$  sonlu, değişmeli bir grup ve  $p$  bir asal tam sayı olsun.  $G$  grubunun mertebesi  $p$  nin bir kuvveti olan elemanlarının oluşturduğu

$$G_p = \{a \in G \mid \exists k \in \mathbb{N} \text{ için } a^k = 1\}$$

alt kümesi  $G$  nin bir alt grubudur.  $G_p$  ye  $G$  nin **maksimal  $p$ -alt grubu** veya **Sylow  $p$ -alt grubu** denir.

**İspat.**  $a^p = 1 = 1^0$  olduğundan  $a \in G_p$  olup  $G_p \neq \emptyset$  olur. Ayrıca  $G_p \subset G$  olduğu da açıktır. Yani  $\emptyset \neq G_p \subset G$  olur. Herhangi  $a, b \in G_p$  alalım.  $a, b \in G_p$  olduğundan  $a^p = 1$  ve  $b^p = 1$

$(b) = p^t$  olacak şekilde  $\exists k, t \in \mathbb{N}$  vardır.  $s = \max\{k, t\}$  diyelim. Burada  $p^k | p^s$  ve  $p^t | p^s$  olup Teorem 2.3.10 dan  $a^{p^s} = e$  ve  $b^{p^s} = e$  olur. Bu durumda  $G$  değişmeli olduğundan  $(ab^{-1})^{p^s} = a^{p^s} b^{-p^s} = e(b^{p^s})^{-1} = ee^{-1} = e$  olup  $(ab^{-1}) | p^s$  olur.  $(ab^{-1}) | p^s$  olduğundan  $(ab^{-1})$ ,  $p$  nin bir kuvveti olup  $G_p$  nin tanımından  $ab^{-1} \in G_p$  olur. Yani  $\forall a, b \in G_p$  için  $ab^{-1} \in G_p$  olup Teorem 2.2.6 gereği  $G_p < G$  olur.

**Örnek.** Mertebesi  $p$  asal tam sayısının kuvveti olan grup bir  $p$ -gruptur.

**Örnek.** Klein'in 4-lü grubu bir 2-gruptur.

**Örnek.**  $(\mathbb{Z}_{12}, +)$  grubunu göz önüne alalım. Bu grup bir  $p$ -grup değildir. Bu grubun 2-alt grupları  $K = \{\overline{0}\}$ ,  $H = \{\overline{0}, \overline{6}\}$  ve  $G_2 = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ , 3-alt grupları  $K = \{\overline{0}\}$  ve  $G_3 = \{\overline{0}, \overline{4}, \overline{8}\}$ , 5-alt grubu  $G_5 = K = \{\overline{0}\}$  olur.

;

### 3. HALKALAR

#### 3.1. HALKA KAVRAMI VE ÖZELLİKLERİ

**Tanım 3.1.1.**  $R$  boştan farklı bir küme,  $\oplus$  ve  $\odot$ ,  $R$  de iki iç işlem olsun. Aşağıdaki aksiyomlar (özellikler) sağlanırsa  $(R, \oplus, \odot)$  cebirsel yapısına bir **halka** denir.

**R1)**  $(R, \oplus)$  bir değişmeli gruptur.

**R2)**  $\odot$  işleminin  $R$  de birleşme özelliği vardır. Yani  $\forall a, b, c \in R$  için  $(a \odot b) \odot c = a \odot (b \odot c)$  dir.

**R3)**  $\odot$  işleminin  $\oplus$  işlemi üzerine sağdan ve soldan dağılma özellikleri vardır. Yani  $\forall a, b, c \in R$  için  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$  ve  $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$  olur.

**Not.** Tanımda geçen  $\oplus$  sembolü yerine genellikle  $+$ ,  $\odot$  sembolü yerine de genellikle  $\cdot$  kullanılacaktır.

**Örnek.**  $(\mathbb{Z}, +, \cdot)$  bir halkadır.

**Örnek.**  $(5\mathbb{Z}, +, \cdot)$  bir halkadır.

**Not.**  $(R, +, \cdot)$  bir halka olsun.  $R$  nin  $+$  işlemine göre birim elemanına **halkanın sıfır elemanı** veya **sıfırı** denir ve genellikle  $0_R$  veya sadece 0 ile gösterilir.  $R$  nin  $\cdot$  işlemine göre birim elemanı olmayabilir. Eğer  $\cdot$  işlemine göre de birim elemanı varsa bu elemana **halkanın birim**

**elemanı** veya **birimi** denir ve genellikle  $1_R$  veya sadece 1 ile gösterilir, böyle bir halkaya da **birimli halka** denir. Halka ikinci işleme göre değişme özelliğine sahipse bu halkaya **değişmeli halka** denir.

**Not.** Gruplarda olduğu gibi halkalarda da iki eleman için tanımlı  $+$  ve  $\cdot$  işlemleri sonlu sayıda eleman için de tanımlıdır. Bu durumda genel birleşme ve genel dağılma özellikleri de sağlanır.

Yani  $R$  bir halka olmak üzere  $\forall a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m \in R$  için

(i)  $1 \leq k < n$  olmak üzere  $(\sum_{i=1}^k a_i) + (\sum_{i=k+1}^n a_i) = \sum_{i=1}^n a_i$  olur.

(ii)  $1 \leq k < n$  olmak üzere  $(\prod_{i=1}^k a_i) \cdot (\prod_{i=k+1}^n a_i) = \prod_{i=1}^n a_i$  olur.

(iii)  $(\sum_{i=1}^n a_i) \cdot (\sum_{j=1}^m b_j) = \sum_{i=1}^n (\sum_{j=1}^m a_i b_j) = \sum_{j=1}^m (\sum_{i=1}^n a_i b_j) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j = \sum_{j=1}^m \sum_{i=1}^n a_i b_j$  olur.

**Teorem 3.1.2.**  $R$  bir halka olsun. Bu durumda aşağıdaki eşitlikler vardır.

(i)  $\forall a \in R$  için  $a0_R = 0_R a = 0_R$ .

(ii)  $\forall a, b \in R$  için  $a(-b) = (-a)b = -(ab)$ .

(iii)  $\forall a, b \in R$  için  $(-a)(-b) = ab$ .

(iv)  $R$  birimli ise  $\forall a \in R$  için  $(-1_R)a = a(-1_R) = -a$ .

(v)  $R$  birimli ise  $(-1_R)(-1_R) = 1_R$  olur.

**İspat:** (i) Herhangi  $a \in R$  alalım.  $0_R + 0_R = 0_R$  olduğundan  $a(0_R + 0_R) = a0_R$  sağlanır.  $R$  bir halka olduğundan  $a0_R + a0_R = a(0_R + 0_R) = a0_R$  bulunur. Bu durumda  $a0_R + a0_R + (-(a0_R)) = a0_R + (-(a0_R))$  olup  $a0_R + (-(a0_R)) = 0_R$  elde edilir. Böylece  $a0_R + 0_R = 0_R$  olup  $a0_R = 0_R$  elde edilir.  $0_R a = 0_R$  olduğu da benzer şekilde gösterilebilir.

(ii) Herhangi  $a, b \in R$  alalım.  $b + (-b) = (-b) + b = 0_R$  ve  $R$  bir halka olduğundan (i) şikkından  $ab + a(-b) = a(b + (-b)) = a0_R = 0_R$  ve  $a(-b) + ab = a(-b + b) = a0_R = 0_R$  olup  $a(-b)$  elemanı  $ab$  elemanının  $R$  de  $+$  işlemine göre tersi olur. O halde  $a(-b) = -(ab)$  olur.  $(-a)b = -(ab)$  olduğu da benzer şekilde gösterilebilir.

(iii)  $R$  deki bir elemanın  $+$  işlemine göre tersinin tersi kendisine eşit olduğundan (ii) şikkından  $\forall a, b \in R$  için  $(-a)(-b) = (-(-a))b = ab$  olup istenen elde edilir.

(iv)  $R$  birimli olsun. Bu durumda (ii) şikkından  $\forall a \in R$  için  $(-1_R)a = -(1_R a) = -a$  ve  $a(-1_R) = -(a1_R) = -a$  olup  $(-1_R)a = a(-1_R) = -a$  olur.

(v)  $R$  birimli olsun. Bu durumda (iii) şikkından  $(-1_R)(-1_R) = 1_R 1_R = 1_R$  olup istenen elde edilir.

**Not.**  $R$  bir halka olmak üzere  $\forall a, b \in R$  için  $a(-b) = (-a)b = -(ab)$  olduğundan  $-(ab)$  yerine  $-ab$  yazılacaktır.

**Tanım 3.1.3.**  $R$  bir halka ve  $a \in R$  olsun.  $-a$  ya  $a$  elemanının **toplamsal tersi** denir,  $a$  elemanının varsa  $\cdot$  işlemine göre tersine de  $a$  elemanının **tersi** denir ve genellikle  $a^{-1}$  ile gösterilir.

**Örnek.** Birimli bir  $R$  halkasında, tersi mevcut olan elemanların oluşturduğu küme çarpımsal bir gruptur. Bu grubun elemanlarına **birimsel eleman**, bu gruba da **birim grup** denir ve  $U_R$  ile gösterilir.

**Çözüm.**  $U_R = \{a \in R \mid \exists a^{-1} \in R\}$  olmak üzere  $1_R \in U_R$  ve  $U_R \subset R$  olduğu açıktır.  $\cdot$  işleminin  $U_R$  de birleşme özelliği ve tanıma göre,  $U_R$  deki her elemanın da tersi vardır. O halde  $U_R$  nin bir grup olduğunu göstermek için kapalılığı göstermek yeterlidir.  $a, b \in U_R$  alalım. Bu durumda  $a^{-1}, b^{-1} \in R$  elemanları vardır. Buradan  $(ab)^{-1} = b^{-1}a^{-1} \in R$  olup  $ab \in U_R$  bulunur.

**Tanım 3.1.4.**  $R = \{0_R\}$  tek elemanlı bir halkadır. Bu halkaya **sıfır halka** veya **aşık halka** denir. Genel olarak halka sıfır halkadan farklı kabul edilir.

**Teorem 3.1.5.** Birimli bir halkada birim ve sıfır elemanlar birbirinden farklıdır.

**İspat.**  $R$  birimli bir halka olsun.  $1_R \neq 0_R$  olduğu gösterilirse istenen elde edilir. Eğer  $1_R = 0_R$  ise  $\forall a \in R$  için  $a = a1_R = a0_R = 0_R$  olup  $R = \{0_R\}$  olur ki bu da halkanın sıfır halkadan farklı kabul edilmesiyle çelişir. O halde  $1_R \neq 0_R$  olup istenen elde edilir.

**Tanım 3.1.6.** Bir  $R$  halkasında sıfırdan farklı bir  $a$  elemanı için  $ab = 0_R$  veya  $ba = 0_R$  olacak şekilde  $\exists 0_R \neq b \in R$  bulunabilirse  $a$  elemanına halkanın **sıfır bölen elemanı** denir. Eğer böyle  $b$  elemanı yoksa  $a$  elemanına halkanın **sıfır bölen olmayan elemanı** denir.

**Not.** Tanımdan  $0_R$  ne sıfır bölendir, ne de sıfır bölen olmayan elemandır.

**Örnek.**  $\mathbb{Z}_6$  da  $\bar{2}, \bar{3}$  ve  $\bar{4}$  sıfır bölen elemanlardır.

**Tanım 3.1.7.** Sıfır bölensiz (sıfırdan farklı her elemanı sıfır bölen olmayan) bir halkaya **tam halka** denir. Birimli, değişmeli ve sıfır bölensiz bir halkaya **tamlık bölgesi** denir.

**Örnek.**  $(\mathbb{Z}, +, \cdot)$  halkası bir tamlık bölgesidir.  $(3\mathbb{Z}, +, \cdot)$  tamlık bölgesi değildir.

**Örnek.**  $2 \times 2$  tipindeki reel matrisler kümesi matrislerde toplama ve çarpma işlemlerine göre bir halkadır. Bu halka birimlidir, ancak değişmeli değildir. Ayrıca bu halka bir tam halka da değildir.

**Teorem 3.1.8.**  $R$  bir halka ve  $0_R \neq c \in R$  sıfır bölen olmayan eleman olsun. Bu takdirde  $a, b \in R$  için

$$ac = bc \text{ (} ca = cb \text{) ise } a = b \text{ sağdan (soldan) kısaltma özelliği sağlanır.}$$

**İspat.**  $ac = bc$  ( $ca = cb$ ) olsun. Bu durumda  $ac - bc = 0_R$  ( $ca - cb = 0_R$ ) olup  $R$  bir halka olduğundan  $(a - b)c = ac - bc = 0_R$  ( $c(a - b) = ca - cb = 0_R$ ) olur. Bu durumda  $c$ ,  $R$  nin bir sıfır bölen olmayan elemanı olduğundan  $a - b = 0_R$  olup  $a = b$  bulunur.

**Sonuç 3.1.9.**  $R$  bir tam halka ise  $0_R \neq a \in R$  ve  $b \in R$  için  $ax = b$  olacak şekilde  $\exists x \in R$  varsa tektir. Ancak böyle bir  $x$  elemanı bulunmayabilir.

**İspat.**  $x_1, x_2 \in R$  olmak üzere  $ax_1 = b$  ve  $ax_2 = b$  olsun. Bu durumda  $ax_1 = b = ax_2$  olur.  $R$  bir tam halka ve  $0_R \neq a \in R$  olduğundan  $a$  bir sıfır bölen olmayan elemandır. O halde Teorem 3.1.8 gereği  $x_1 = x_2$  olur. Yani  $ax = b$  olacak şekilde  $\exists x \in R$  varsa tektir.

Şimdi böyle bir  $x$  elemanının bulunmayabileceğine dair bir örnek verelim.  $(\mathbb{Z}, +, \cdot)$  tamlık bölgesinde  $3x = 2$  olacak şekilde hiçbir  $x$  elemanı mevcut değildir.

**Tanım 3.1.10.**  $R$  birimli ve değişmeli bir halka ve  $R^* = R - \{0\}$ , ikinci işlem  $\cdot$  ya göre bir grup ise yada sıfırdan farklı her elemanın  $\cdot$  işlemine göre tersi varsa  $R$  halkasına bir **cisim** denir.

**Örnek.**  $(\mathbb{Q}, +, \cdot)$  ve  $(\mathbb{R}, +, \cdot)$  cebirsel yapıları birer cisimdir. Fakat  $(\mathbb{Z}, +, \cdot)$  bir cisim değildir.

**Teorem 3.1.11.** Sonlu elemanlı tamlık bölgesi bir cisimdir.

**İspat.**  $K$  sonlu elemanlı bir tamlık bölgesi olsun.  $K$  nın bir cisim olduğu gösterilirse istenen elde edilir.  $0_K \neq a \in K$  olsun.  $K$  bir tamlık bölgesi olduğundan  $a$  bir sıfır bölen olmayan elemandır.  $f: K \rightarrow K, x \rightarrow f(x) = ax$  dönüşümünü tanımlayalım.  $f$  nin bir fonksiyon olduğu açıktır.  $f(x_1) = f(x_2)$  olan herhangi  $x_1, x_2 \in K$  alalım.  $f(x_1) = f(x_2)$  olduğundan  $ax_1 = ax_2$  olup  $a$  bir sıfır bölen olmayan eleman olduğundan Teorem 3.1.8 den  $x_1 = x_2$  olur. O halde  $f$  bire-bir olup ayrıca  $K$  sonlu elemanlı olduğundan Önerme 1.3.9 gereği  $f$  aynı zamanda örtendir.  $f$  örten ve  $1_K \in K$  olduğundan  $f(x) = 1_K$  olacak şekilde  $\exists x \in K$  vardır.  $f(x) = 1_K$  olduğundan  $ax = 1_K$  olur. Ayrıca  $K$  değişmeli olduğundan  $ax = xa = 1_K$  olup  $x$  elemanı  $a$  nın  $K$  da  $\cdot$  işlemine göre tersidir. Yani  $K$  nın sıfırdan farklı her elemanının  $K$  da  $\cdot$  işlemine göre tersi mevcuttur. Böylece  $K$  bir cisim olup istenen elde edilir.

**Örnek.**  $p$  bir asal tam sayı ise  $\mathbb{Z}_p$ ,  $p$  elemanlı bir cisimdir.

Yukarıdaki teoremden sonluluk ifadesi kaldırılırsa, iddia yanlış olur.  $(\mathbb{Z}, +, \cdot)$  bir tamlık bölgesidir, fakat bir cisim değildir.

**Not.** Gruplarda olduğu gibi halkalarda da bir elemanın  $n$  katı ve  $n$ . kuvveti ( $n \in \mathbb{Z}$ ) tanımlıdır.

**Teorem 3.1.12.**  $R$  bir halka olsun. Bu durumda  $\forall a, b \in R$  ve  $\forall m, n \in \mathbb{Z}$  için

$$(i) \quad ma + na = (m + n)a$$

$$(ii) \quad m(na) = (mn)a$$

$$(iii) \quad n(a + b) = na + nb$$

$$(iv) \quad (-m)a = m(-a) = -(ma)$$

$$(v) \quad (ma)b = a(mb) = m(ab)$$

$$(vi) \quad (ma)(nb) = (mn)(ab)$$

**İspat.** Herhangi  $a, b \in R$  ve herhangi  $m, n \in \mathbb{Z}$  alalım.  $(R, +)$  değişmeli bir grup olduğundan (i), (ii) ve (iii) gruplardaki kat özelliklerinden sağlanır.

(iv) Kat tanımından  $\forall x \in R$  için  $(-1)x = -x$  olur. Bu durumda (ii) şikkından  $(-m)a = ((-1)m)a = (-1)(ma) = -(ma)$  ve  $m(-a) = m((-1)a) = (m(-1))a = ((-1)m)a = (-1)(ma) = -(ma)$  olup  $(-m)a = m(-a) = -(ma)$  olur.

(v) Eğer  $m > 0$  ise  $(ma)b = \left( \underbrace{a + a + \dots + a}_{m \text{ tane}} \right) b = \underbrace{ab + ab + \dots + ab}_{m \text{ tane}} = m(ab)$  ve  $a(mb) =$

$a \left( \underbrace{b + b + \dots + b}_{m \text{ tane}} \right) = \underbrace{ab + ab + \dots + ab}_{m \text{ tane}} = m(ab)$  olup  $(ma)b = a(mb) = m(ab)$  olur. Eğer

$m = 0$  ise her  $x \in R$  için  $0x = 0_R$  olduğundan  $(ma)b = (0a)b = 0_R b = 0_R = 0(ab) = m(ab)$  ve  $a(mb) = a(0b) = a0_R = 0_R = 0(ab) = m(ab)$  olup  $(ma)b = a(mb) = m(ab)$  eşitliği sağlanır. Eğer  $m < 0$  ise  $-m > 0$  ve  $(-m)(-a) = ma$  olduğundan

$$\begin{aligned} (ma)b &= \left( \underbrace{(-a) + (-a) + \dots + (-a)}_{-m \text{ tane}} \right) b = \underbrace{(-a)b + (-a)b + \dots + (-a)b}_{-m \text{ tane}} \\ &= \underbrace{(-ab) + (-ab) + \dots + (-ab)}_{-m \text{ tane}} = m(ab) \end{aligned}$$

ve

$$\begin{aligned} a(mb) &= a \left( \underbrace{(-b) + (-b) + \dots + (-b)}_{-m \text{ tane}} \right) = \underbrace{a(-b) + a(-b) + \dots + a(-b)}_{-m \text{ tane}} \\ &= \underbrace{(-ab) + (-ab) + \dots + (-ab)}_{-m \text{ tane}} = m(ab) \end{aligned}$$

olup yine  $(ma)b = a(mb) = m(ab)$  olur.

(vi) (ii) ve (v) şıklarından  $(ma)(nb) = m(a(nb)) = m(n(ab)) = (mn)(ab)$  olup istenen elde edilir.

**Not.**  $R$  bir halka olsun.  $\forall a \in R$  ve  $\forall m, n \in \mathbb{Z}$  için  $m(na) = (mn)a$  olduğundan  $m(na)$  ve  $(mn)a$  yerine  $mna$  yazılacaktır.  $\forall a, b \in R$  ve  $\forall m \in \mathbb{Z}$  için  $(ma)b = a(mb) = m(ab)$  olduğundan  $(ma)b$ ,  $a(mb)$  ve  $m(ab)$  yerine  $mab$  yazılır.  $\forall m \in \mathbb{Z}$  ve  $\forall a \in R$  için  $(-m)a = m(-a) = -(ma)$  olduğundan  $(-m)a$ ,  $m(-a)$  ve  $-(ma)$  yerine  $-ma$  yazılır.

**Tanım 3.1.13.**  $R$  birimli bir halka olsun.  $m1_R = 0_R$  olacak şekilde bir  $m > 0$  tam sayısı varsa böyle  $m$  pozitif tam sayılarının en küçüğüne  $R$  halkasının **karakteristiği** denir. Eğer bu koşulu sağlayan bir  $m$  pozitif tam sayısı yoksa  $R$  halkasının **karakteristiği sıfırdır** denir.

**Teorem 3.1.14.** Bir tamlık bölgesinin karakteristiği sıfır değilse bir asal sayıdır.

**İspat.**  $R$  bir tamlık bölgesi ve  $R$  nin karakteristiği sıfırdan farklı olsun. Kabul edelim ki  $R$  nin karakteristiği  $m > 0$  tam sayısı olsun.  $m$  nin asal olduğu gösterilirse istenen elde edilir.  $m1_R = 0_R$  ve  $1_R \neq 0_R$  olduğundan  $m \neq 1$  dir. Dolayısıyla  $m > 1$  olur.  $m$  nin 1 den farklı herhangi  $n$  pozitif bölenini alalım.  $n|m$  olduğundan  $m = nt$  olacak şekilde  $\exists t \in \mathbb{Z}$  vardır. Burada  $m > 0$  ve  $n > 1$  olduğundan  $0 < t < m$  olur.  $m$  tam sayısı  $R$  nin karakteristiği olduğundan  $m1_R = 0_R$  olup  $0_R = m1_R = (nt)(1_R1_R) = (n1_R)(t1_R)$  eşitliğinde  $R$  nin sıfır bölensiz oluşu kullanılarak  $n1_R = 0_R$  veya  $t1_R = 0_R$  olduğu görülür.  $R$  nin karakteristiği  $m$  olduğundan ve  $0 < t < m$  eşitsizliğinden  $t1_R \neq 0_R$  olur. Bu durumda  $n1_R = 0_R$  olup  $n > 0$  dir.  $R$  nin karakteristiği  $m$  olduğundan  $m \leq n$  olmalıdır. Ayrıca  $n|m$  ve  $m, n \in \mathbb{Z}^+$  olduğundan  $n \leq m$  dir. O halde  $n = m$  olur. Yani  $m$  nin 1 ve kendisinden farklı hiçbir pozitif böleni yoktur. O halde  $m$  asal olup istenen elde edilir.

**Teorem 3.1.15.**  $R$  bir tamlık bölgesi olsun.

(i)  $R$  nin karakteristiği sıfır ise  $\forall 0_R \neq a \in R$  için  $|a| = \infty$  dur.

(ii)  $R$  nin karakteristiği  $m$  ise  $\forall 0_R \neq a \in R$  için  $|a| = m$  dir.

**İspat.** (i)  $R$  nin karakteristiği sıfır olsun. Sıfırdan farklı herhangi  $a \in R$  alalım. Eğer  $a$  nın toplamsal mertebesi sonlu ve  $m$  ise  $ma = 0_R$  olup  $0_R = ma = m(1_Ra) = (m1_R)a$  olur. Bu durumda  $R$  nin sıfır bölensizliği ve  $a \neq 0_R$  oluşu kullanılarak  $m1_R = 0_R$  bulunur. Bu ise  $R$  nin karakteristiğinin sıfır olmasıyla çelişir. O halde  $a$  nın toplamsal mertebesi sonlu değildir. Yani  $R$  nin karakteristiğinin sıfır olması durumunda  $R$  nin sıfırdan farklı her elemanının toplamsal mertebesi sonlu değildir.

(ii) Kabul edelim ki  $R$  nin karakteristiği  $m > 0$  tam sayısı olsun. Sıfırdan farklı herhangi  $a \in R$  alalım.  $m > 0$  tam sayısı  $R$  nin karakteristiği olduğundan  $m1_R = 0_R$  olup  $ma = m1_R a = 0_R a = 0_R$  olur. O halde  $a$  nın toplamsal mertebesi sonlu ve bu mertebeye  $n$  denilirse  $n \leq m$  olur.  $n$  tam sayısı  $a$  nın toplamsal mertebesi olduğundan  $na = 0_R$  olup  $0_R = na = (n1_R)a$  olur. Bu durumda  $R$  nin sıfır bölensizliği ve  $a \neq 0$  oluşu kullanılarak  $n1_R = 0_R$  bulunur. Ancak  $R$  nin karakteristiği  $m$  ve  $n > 0$  olduğundan  $m \leq n$  olmalıdır. Böylece  $n \leq m$  ve  $m \leq n$  olduğundan  $n = m$  olup  $a$  nın toplamsal mertebesi  $m$  olur. Yani  $R$  nin karakteristiğinin  $m > 0$  tam sayısı olması durumunda  $R$  nin sıfırdan farklı her elemanının toplamsal mertebesi  $m$  olur.

**Teorem 3.1.16.**  $R$  ve  $S$  iki halka olsun. Bu takdirde  $R \times S$  kümesi  $\forall (r_1, s_1), (r_2, s_2) \in R \times S$  için  $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$  ve  $(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$  ile tanımlı  $+$  ve  $\cdot$  işlemlerine göre bir halkadır. Bu halkaya  $R$  ile  $S$  nin **direkt çarpımı** denir ve genellikle  $R \oplus S$  ile ifade edilir.

**İspat.** Teoremin ifadesindeki  $+$  ve  $\cdot$  işlemlerinin  $R \times S$  de bir iç işlem olduğu açıktır. Şimdi bu işlemlerin halka tanımındaki koşulları sağladığını gösterelim.

**R1)** Teorem 2.1.14 den  $R \times S$  kümesi  $+$  işlemine göre bir gruptur. Ayrıca  $(R, +)$  ve  $(S, +)$  birer değişmeli grup olduğundan  $R \times S$  deki  $+$  işleminin tanımından  $\forall (r_1, s_1), (r_2, s_2) \in R \times S$  için

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) = (r_2 + r_1, s_2 + s_1) = (r_2, s_2) + (r_1, s_1)$$

olup  $R \times S$  kümesi  $+$  işlemine göre değişmeli bir grup olur.

**R2)**  $R$  ve  $S$  deki  $\cdot$  işleminin birleşme özelliği ve  $R \times S$  de  $\cdot$  işleminin tanımından  $\forall (r_1, s_1), (r_2, s_2), (r_3, s_3) \in R \times S$  için

$$\begin{aligned} (r_1, s_1)[(r_2, s_2)(r_3, s_3)] &= (r_1, s_1)(r_2 r_3, s_2 s_3) = (r_1(r_2 r_3), s_1(s_2 s_3)) \\ &= ((r_1 r_2) r_3, (s_1 s_2) s_3) = (r_1 r_2, s_1 s_2)(r_3, s_3) \\ &= [(r_1, s_1)(r_2, s_2)](r_3, s_3) \end{aligned}$$

eşitliği sağlanır. Böylece  $R \times S$  de  $\cdot$  işleminin birleşme özelliği vardır.

**R3)**  $R$  ve  $S$  de  $\cdot$  işleminin  $+$  işlemi üzerine sağdan ve soldan dağılma özellikleri ve  $R \times S$  de  $+$  ve  $\cdot$  işlemlerinin tanımlarından  $\forall (r_1, s_1), (r_2, s_2), (r_3, s_3) \in R \times S$  için

$$\begin{aligned} (r_1, s_1)[(r_2, s_2) + (r_3, s_3)] &= (r_1, s_1)(r_2 + r_3, s_2 + s_3) \\ &= (r_1(r_2 + r_3), s_1(s_2 + s_3)) = (r_1 r_2 + r_1 r_3, s_1 s_2 + s_1 s_3) \\ &= (r_1 r_2, s_1 s_2) + (r_1 r_3, s_1 s_3) = (r_1, s_1)(r_2, s_2) + (r_1, s_1)(r_3, s_3) \end{aligned}$$

ve

$$\begin{aligned}
[(r_1, s_1) + (r_2, s_2)](r_3, s_3) &= (r_1 + r_2, s_1 + s_2)(r_3, s_3) = ((r_1 + r_2)r_3, (s_1 + s_2)s_3) \\
&= (r_1r_3 + r_2r_3, s_1s_3 + s_2s_3) = (r_1r_3, s_1s_3) + (r_2r_3, s_2s_3) \\
&= (r_1, s_1)(r_3, s_3) + (r_2, s_2)(r_3, s_3)
\end{aligned}$$

eşitlikleri sağlanır. O halde  $R \times S$  de  $\cdot$  işleminin  $+$  işlemi üzerine sağdan ve soldan dağılma özellikleri vardır.

Böylece  $R \times S$  kartezyen çarpım kümesi üzerinde tanımlanan  $+$  ve  $\cdot$  iç işlemlerine göre bir halka olup istenen elde edilir.

## 3.2. ALT HALKA VE İDEALLER

**Tanım 3.2.1.**  $R$  bir halka ve  $\emptyset \neq S \subset R$  olsun. Eğer  $S$  kümesi  $R$  deki işlemlere göre bizzat bir halka ise  $S$  ye  $R$  nin bir **alt halkası** denir.

**Not.**  $R$  bir halka olsun. Bu durumda  $\{0_R\}$  ve  $R$ ,  $R$  nin birer alt halkasıdır. Bu alt halkalara  $R$  nin **aşık alt halkaları** denir.  $R$  nin varsa  $\{0_R\}$  ve  $R$  den farklı alt halkalarına **öz alt halkaları** denir.

**Örnek.**  $\mathbb{Z}, \mathbb{Q}$  nun bir öz alt halkasıdır.  $\mathbb{Q}, \mathbb{R}$  nin bir öz alt halkasıdır.

**Örnek.**  $4\mathbb{Z}, (\mathbb{Z}, +, \cdot)$  halkasının bir öz alt halkasıdır. Burada  $\mathbb{Z}$  halkası birimli olduğu halde  $4\mathbb{Z}$  halkası birimli değildir.

**Örnek.**  $(\mathbb{Z}_6, +, \cdot)$  halkasını göz önüne alalım.  $\{\bar{0}, \bar{3}\}$  kümesi bu halkanın birim elemanı  $\bar{3}$  olan birimli bir alt halkasıdır. Burada  $\bar{1}$  elemanı da  $(\mathbb{Z}_6, +, \cdot)$  halkasının birim elemanıdır ve  $\bar{3} \neq \bar{1}$  dir.

**Teorem 3.2.2.**  $R$  bir halka ve  $\emptyset \neq S \subset R$  olsun. Bu takdirde  $S$  nin bir alt halka olması için gerek ve yeter koşul  $\forall a, b \in S$  için  $a - b \in S$  ve  $ab \in S$  olmasıdır.

**İspat.**  $(\Rightarrow)$   $S$ ,  $R$  nin bir alt halkası olsun. Bu durumda  $S$ ,  $R$  deki işlemlere göre kendi başına bir halka olup  $\forall a, b \in S$  için  $a - b \in S$  ve  $ab \in S$  olur.

$(\Leftarrow)$   $\forall a, b \in S$  için  $a - b \in S$  ve  $ab \in S$  olsun.  $\emptyset \neq S \subset R$  ve  $\forall a, b \in S$  için  $a - b \in S$  olduğundan Teorem 2.2.6 gereği  $S$ ,  $+$  işlemine göre  $R$  nin bir alt grubu olur. Ayrıca  $S \subset R$  olduğundan  $\forall a, b \in S$  için  $a, b \in R$  olup  $(R, +)$  bir değişmeli grup olduğundan  $a + b = b + a$  olur. O halde  $(S, +)$  cebirsel yapısı değişmeli bir grup olur.

$\forall a, b \in S$  için  $ab \in S$  olduğundan  $R$  deki  $\cdot$  işlemi  $S$  de bir iç işlem olur. Ayrıca  $S \subset R$  olduğundan  $\forall a, b, c \in S$  için  $a, b, c \in R$  olup  $(R, +, \cdot)$  bir halka olduğundan  $(ab)c = a(bc)$ ,  $a(b + c) = ab + ac$  ve  $(a + b)c = ac + bc$  olur.

Böylece  $S, R$  deki işlemlere göre bizzat bir halka olduğundan  $R$  nin bir alt halkasıdır.

**Teorem 3.2.3.** Bir halkanın birtakım alt halkalarının kesişimi de bir alt halkadır.

**İspat.**  $R$  bir halka ve  $\{S_i\}_{i \in I}$ ,  $R$  nin alt halkalarının bir ailesi olsun.  $\bigcap_{i \in I} S_i$  kümesinin  $R$  nin bir alt halkası olduğu gösterilirse istenen elde edilir. Her  $i \in I$  için  $S_i$ ,  $R$  nin bir alt halkası olduğundan  $(S_i, +)$  grubu  $(R, +)$  grubunun bir alt grubu olup  $0_R \in S_i$  olur. Her  $i \in I$  için  $0_R \in S_i$  olduğundan  $0_R \in \bigcap_{i \in I} S_i$  dir. Buradan  $\bigcap_{i \in I} S_i \neq \emptyset$  olur. Ayrıca  $\bigcap_{i \in I} S_i \subset R$  olduğu da açıktır. Yani  $\emptyset \neq \bigcap_{i \in I} S_i \subset R$  olur. Herhangi  $a, b \in \bigcap_{i \in I} S_i$  alalım.  $a, b \in \bigcap_{i \in I} S_i$  olduğundan her  $i \in I$  için  $a, b \in S_i$  olup  $S_i$ ,  $R$  nin bir alt halkası olduğundan  $a - b \in S_i$  ve  $ab \in S_i$  olur. Her  $i \in I$  için  $a - b \in S_i$  ve  $ab \in S_i$  olduğundan  $a - b \in \bigcap_{i \in I} S_i$  ve  $ab \in \bigcap_{i \in I} S_i$  bulunur. Yani  $\forall a, b \in \bigcap_{i \in I} S_i$  için  $a - b \in \bigcap_{i \in I} S_i$  ve  $ab \in \bigcap_{i \in I} S_i$  olup Teorem 3.2.2 gereği  $\bigcap_{i \in I} S_i$ ,  $R$  nin bir alt halkasıdır.

**Tanım 3.2.4.**  $R$  bir halka ve  $A \subset R$  olsun.  $R$  nin  $A$  yı kapsayan bütün alt halkalarının kesişimine  $A$  nın **ürettiği alt halka** denir ve genellikle  $\langle A \rangle$  ile ifade edilir. Burada  $A$  nın elemanlarına da  $\langle A \rangle$  halkasının **üretecileri** denir.

**Not.**  $A \subset T$  ve  $T, R$  nin bir alt halkası ise  $\langle A \rangle$  nın tanımından  $\langle A \rangle \subset T$  olur. Böylece  $\langle A \rangle$ ,  $R$  nin  $A$  yı kapsayan en küçük alt halkası olur. Eğer  $A = \emptyset$  ise  $\langle A \rangle = \{0_R\}$  olur.

**Tanım 3.2.5.**  $R$  bir halka ve  $\emptyset \neq I \subset R$  olsun. Eğer

- (i)  $\forall a, b \in I$  için  $a - b \in I$  ve
- (ii)  $\forall a \in I$  ve  $\forall r \in R$  için  $ra \in I$  ( $ar \in I$ )

ise  $I$  ya  $R$  nin bir **sol (sağ) ideali** denir. Hem sol, hem de sağ ideale **iki taraflı ideal** veya kısaca **ideal** denir.

**Not.** Her sol (sağ) ideal bir alt halkadır, fakat her alt halka bir ideal olmayabilir.

**Örnek.**  $\mathbb{Z}, \mathbb{Q}$  nun bir alt halkasıdır, ancak bir ideali değildir.

**Not.**  $R$  halkası değişmeli ise  $R$  nin her sol ideali bir sağ ideal, her sağ ideali de bir sol ideal olur. Dolayısıyla değişmeli halkalarda her sol (sağ) ideal bir idealdir.

**Tanım 3.2.6.**  $\{0_R\}$  ve  $R$ ,  $R$  halkasının idealleri olup bu ideallere  $R$  nin **aşık idealleri** denir.  $R$  nin varsa  $\{0_R\}$  ve  $R$  den farklı ideallerine de **öz idealleri** denir.

**Teorem 3.2.7.** Bir  $R$  halkasının birtakım sol (sağ) ideallerinin kesişimi de  $R$  nin bir sol (sağ) idealidir.

**İspat.**  $\{S_i\}_{i \in I}$ ,  $R$  nin sol (sağ) ideallerinin bir ailesi olsun.  $\cap_{i \in I} S_i$  kümesinin  $R$  nin bir sol (sağ) ideali olduğu gösterilirse istenen elde edilir. Her  $i \in I$  için  $S_i$ ,  $R$  nin bir sol (sağ) ideali olduğundan  $(S_i, +)$  grubu  $(R, +)$  grubunun bir alt grubudur. Böylece  $0_R \in S_i$  olduğu açıktır. Buradan  $\forall i \in I$  için  $0_R \in S_i$  olduğundan  $0_R \in \cap_{i \in I} S_i$  olup  $\cap_{i \in I} S_i \neq \emptyset$  olur. Ayrıca  $\cap_{i \in I} S_i \subset R$  olduğu da açıktır. Yani  $\emptyset \neq \cap_{i \in I} S_i \subset R$  olur. Herhangi  $a, b \in \cap_{i \in I} S_i$  ve herhangi  $r \in R$  alalım.  $a, b \in \cap_{i \in I} S_i$  olduğundan  $\forall i \in I$  için  $a, b \in S_i$  olup  $S_i$ ,  $R$  nin bir sol (sağ) ideali olduğundan  $a - b \in S_i$  ve  $ra \in S_i$  ( $ar \in S_i$ ) olur. Her  $i \in I$  için  $a - b \in S_i$  ve  $ra \in S_i$  ( $ar \in S_i$ ) olduğundan  $a - b \in \cap_{i \in I} S_i$  ve  $ra \in \cap_{i \in I} S_i$  ( $ar \in \cap_{i \in I} S_i$ ) olur. Yani  $\forall a, b \in \cap_{i \in I} S_i$  ve  $\forall r \in R$  için  $a - b \in \cap_{i \in I} S_i$  ve  $ra \in \cap_{i \in I} S_i$  ( $ar \in \cap_{i \in I} S_i$ ) olup ideal tanımı gereği  $\cap_{i \in I} S_i$ ,  $R$  nin bir sol (sağ) idealidir.

**Tanım 3.2.8.**  $R$  bir halka ve  $A \subset R$  olsun.  $R$  nin  $A$  yı kapsayan bütün ideallerinin kesişimine  $A$  nın **ürettiği ideal** denir ve genellikle  $(A)$  ile ifade edilir. Eğer  $A = \{a\}$  şeklinde tek elemanlı ise  $A$  nın ürettiği ideale **temel (esas) ideal** denir ve genellikle  $(a)$  ile ifade edilir.

**Not.** Boş kümenin ürettiği ideal sıfır idealidir.  $(A)$  nın tanımından  $(A)$ ,  $R$  nin  $A$  yı kapsayan en küçük idealidir.

**Teorem 3.2.9.**  $R$  bir halka ve  $\emptyset \neq A \subset R$  olsun. Bu durumda

$$(A) = \left\{ \sum_{i=1}^n r_i a_i + \sum_{j=1}^m a'_j r'_j + \sum_{k=1}^s r''_k a''_k r'''_k + \sum_{u=1}^t n_u c_u \mid \begin{array}{l} r_i, r'_j, r''_k, r'''_k \in R, \\ a_i, a'_j, a''_k, c_u \in A, \\ n_u \in \mathbb{Z}, n, m, s, t \in \mathbb{Z}^+ \end{array} \right\}$$

olur.

**İspat.**

$$M = \left\{ \sum_{i=1}^n r_i a_i + \sum_{j=1}^m a'_j r'_j + \sum_{k=1}^s r''_k a''_k r'''_k + \sum_{u=1}^t n_u c_u \mid \begin{array}{l} r_i, r'_j, r''_k, r'''_k \in R \\ a_i, a'_j, a''_k, c_u \in A \\ n_u \in \mathbb{Z}, n, m, s, t \in \mathbb{Z}^+ \end{array} \right\}$$

diyelim. Her  $a \in A$  için  $a = 1a \in M$  olup  $A \subset M$  olur. Burada  $A \neq \emptyset$  olduğundan  $M \neq \emptyset$  olur. Ayrıca  $M \subset R$  olduğu da açıktır. O halde  $\emptyset \neq M \subset R$  olur. Herhangi  $a, b \in M$  ve herhangi  $r \in R$  alalım.  $a, b \in M$  olduğundan

$$a = \sum_{i=1}^n r_i a_i + \sum_{j=1}^m a'_j r'_j + \sum_{k=1}^s r''_k a''_k r'''_k + \sum_{u=1}^t n_u c_u$$

ve

$$b = \sum_{i=1}^{n'} q_i b_i + \sum_{j=1}^{m'} b'_j q'_j + \sum_{k=1}^{s'} q''_k b''_k q'''_k + \sum_{u=1}^{t'} n'_u d_u$$

olacak şekilde  $\exists n, m, s, t, n', m', s', t' \in \mathbb{Z}^+$ ,  $\exists r_i, r'_j, r''_k, r'''_k, q_i, q'_j, q''_k, q'''_k \in R$ ,  
 $\exists a_i, a'_j, a''_k, c_u, b_i, b'_j, b''_k, d_u \in A$  ve  $\exists n_u, n'_u \in \mathbb{Z}$  vardır. Burada

$$\begin{aligned} a - b &= \sum_{i=1}^n r_i a_i + \sum_{i=1}^{n'} (-q_i) b_i + \sum_{j=1}^m a'_j r'_j + \sum_{j=1}^{m'} b'_j (-q'_j) + \sum_{k=1}^s r''_k a''_k r'''_k + \sum_{k=1}^{s'} (-q''_k) b''_k q'''_k \\ &\quad + \sum_{u=1}^t n_u c_u + \sum_{u=1}^{t'} (-n'_u) d_u \in M, \\ ra &= \sum_{i=1}^n (rr_i) a_i + \sum_{u=1}^t (n_u r) c_u + \sum_{j=1}^m r a'_j r'_j + \sum_{k=1}^s (r r''_k) a''_k r'''_k \in M \end{aligned}$$

ve

$$ar = \sum_{j=1}^m a'_j (r'_j r) + \sum_{u=1}^t c_u (n_u r) + \sum_{i=1}^n r_i a_i r + \sum_{k=1}^s r''_k a''_k (r'''_k r) \in M$$

olup  $M, R$  nin bir ideali olur. Ayrıca  $A \subset M$  olduğundan

$$(A) \subset M \quad (1)$$

kapsaması bulunur. Herhangi  $a \in M$  alalım.  $a \in M$  olduğundan

$$a = \sum_{i=1}^n r_i a_i + \sum_{j=1}^m a'_j r'_j + \sum_{k=1}^s r''_k a''_k r'''_k + \sum_{u=1}^t n_u c_u$$

olacak şekilde  $\exists n, m, s, t \in \mathbb{Z}^+$ ,  $\exists r_i, r'_j, r''_k, r'''_k \in R$ ,  $\exists a_i, a'_j, a''_k, c_u \in A$  ve  $\exists n_u \in \mathbb{Z}$  vardır.

Burada  $a_i, a'_j, a''_k, c_u \in A$  ve  $A \subset (A)$  olduğundan  $a_i, a'_j, a''_k, c_u \in (A)$  olup  $(A)$ ,  $R$  nin bir ideali olduğundan

$$a = \sum_{i=1}^n r_i a_i + \sum_{j=1}^m a'_j r'_j + \sum_{k=1}^s r''_k a''_k r'''_k + \sum_{u=1}^t n_u c_u \in (A)$$

olur. Yani  $\forall a \in M$  için  $a \in (A)$  olup

$$M \subset (A) \quad (2)$$

kapsaması elde edilir. (1) ve (2) den

$$(A) = M = \left\{ \sum_{i=1}^n r_i a_i + \sum_{j=1}^m a'_j r'_j + \sum_{k=1}^s r''_k a''_k r'''_k + \sum_{u=1}^t n_u c_u \left| \begin{array}{l} r_i, r'_j, r''_k, r'''_k \in R \\ a_i, a'_j, a''_k, c_u \in A \\ n_u \in \mathbb{Z}, n, m, s, t \in \mathbb{Z}^+ \end{array} \right. \right\}$$

olup istenen elde edilir.

**Sonuç 3.2.10.**  $R$  değişmeli bir halka ve  $\emptyset \neq A \subset R$  olsun. Bu durumda

$$(A) = \left\{ \sum_{i=1}^n r_i a_i + \sum_{u=1}^t n_u c_u \mid r_i \in R, a_i, c_u \in A, n_u \in \mathbb{Z}, n, t \in \mathbb{Z}^+ \right\}$$

olur.

**İspat.**

$$T = \left\{ \sum_{i=1}^n r_i a_i + \sum_{u=1}^t n_u c_u \mid r_i \in R, a_i, c_u \in A, n_u \in \mathbb{Z}, n, t \in \mathbb{Z}^+ \right\}$$

diyelim.  $T \subset (A)$  olduğu açıktır. Herhangi  $a \in (A)$  alalım. Teorem 3.2.9 dan

$$a = \sum_{i=1}^n r_i a_i + \sum_{j=1}^m a'_j r'_j + \sum_{k=1}^s r''_k a''_k r'''_k + \sum_{u=1}^t n_u c_u$$

olacak şekilde  $\exists n, m, s, t \in \mathbb{Z}^+, \exists r_i, r'_j, r''_k, r'''_k \in R, \exists a_i, a'_j, a''_k, c_u \in A$  ve  $\exists n_u \in \mathbb{Z}$  vardır.

Burada  $R$  değişmeli olduğundan

$$\begin{aligned} a &= \sum_{i=1}^n r_i a_i + \sum_{j=1}^m a'_j r'_j + \sum_{k=1}^s r''_k a''_k r'''_k + \sum_{u=1}^t n_u c_u \\ &= \sum_{i=1}^n r_i a_i + \sum_{j=1}^m r'_j a'_j + \sum_{k=1}^s (r''_k r'''_k) a''_k + \sum_{u=1}^t n_u c_u \in T \end{aligned}$$

olur. Yani  $\forall a \in (A)$  için  $a \in T$  olup  $(A) \subset T$  olur. Ayrıca  $T \subset (A)$  olduğundan

$$(A) = T = \left\{ \sum_{i=1}^n r_i a_i + \sum_{u=1}^t n_u c_u \mid r_i \in R, a_i, c_u \in A, n_u \in \mathbb{Z}, n, t \in \mathbb{Z}^+ \right\}$$

olup istenen elde edilir.

**Sonuç 3.2.11.**  $R$  birimli ve değişmeli bir halka ve  $\emptyset \neq A \subset R$  olsun. Bu durumda

$$(A) = \left\{ \sum_{i=1}^n r_i a_i \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+ \right\} \text{ olur.}$$

**İspat.**  $R$  değişmeli halka olduğundan Sonuç 3.2.10 gereği

$$(A) = \left\{ \sum_{i=1}^n r_i a_i + \sum_{u=1}^t n_u c_u \mid r_i \in R, a_i, c_u \in A, n_u \in \mathbb{Z}, n, t \in \mathbb{Z}^+ \right\}$$

olur.  $K = \{ \sum_{i=1}^n r_i a_i \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+ \}$  diyelim.  $K \subset (A)$  olduğu açıktır. Herhangi  $a \in (A)$  için

$$(A) = \left\{ \sum_{i=1}^n r_i a_i + \sum_{u=1}^t n_u c_u \mid r_i \in R, a_i, c_u \in A, n_u \in \mathbb{Z}, n, t \in \mathbb{Z}^+ \right\}$$

olduğundan  $a = \sum_{i=1}^n r_i a_i + \sum_{u=1}^t n_u c_u$  olacak şekilde  $\exists n, t \in \mathbb{Z}^+, \exists r_i \in R, \exists a_i, c_u \in A$  ve  $\exists n_u \in \mathbb{Z}$  vardır. Burada  $R$  birimli olduğundan

$$a = \sum_{i=1}^n r_i a_i + \sum_{u=1}^t n_u c_u = \sum_{i=1}^n r_i a_i + \sum_{u=1}^t (n_u 1_R) c_u \in K$$

olur. Yani  $\forall a \in (A)$  için  $a \in K$  olup  $(A) \subset K$  olur. Ayrıca  $K \subset (A)$  olduğundan

$$(A) = K = \left\{ \sum_{i=1}^n r_i a_i \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+ \right\}$$

olup istenen elde edilir.

**Sonuç 3.2.12.**  $R$  bir halka ve  $a \in R$  olsun. Bu durumda

$$(a) = \left\{ ra + ar' + \sum_{i=1}^n r_i'' ar_i''' + ta \mid r, r', r_i'', r_i''' \in R, t \in \mathbb{Z}, n \in \mathbb{Z}^+ \right\}$$

olur.

**Sonuç 3.2.13.**  $R$  değişmeli bir halka ve  $a \in R$  olsun. Bu durumda

$$(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$$

olur.

**Sonuç 3.2.14.**  $R$  birimli ve değişmeli bir halka ve  $a \in R$  olsun. Bu durumda

$$(a) = Ra = \{ra \mid r \in R\}$$

olur.

**Tanım 3.2.15.** Her ideali temel ideal olan tamlık bölgesine **temel ideal bölgesi** denir ve kısaca TİB ile ifade edilir.

**Teorem 3.2.16.**  $(\mathbb{Z}, +, \cdot)$  halkası bir TİB dir.

**İspat.**  $I, \mathbb{Z}$  nin herhangi bir ideali olsun.  $I$  idealinin bir temel ideal olduğu gösterilirse istenen elde edilir. Eğer  $I = \{0\}$  ise  $I = (0)$  olup  $I$  bir temel ideal olur. Kabul edelim ki  $I \neq \{0\}$  olsun. Bu durumda  $\exists 0 \neq a \in I$  vardır.  $I, \mathbb{Z}$  nin bir ideali ve  $a \in I$  olduğundan  $-a = (-1)a \in I$  olur.  $-a, a \in I$  olduğundan  $|a| \in I$  olur.  $A = \{x \in I \mid x > 0\}$  kümesini tanımlayalım.  $|a| \in I$  ve  $|a| > 0$  olduğundan  $|a| \in A$  olup  $A \neq \emptyset$  olur. Ayrıca  $A \subset \mathbb{Z}^+$  ve pozitif tam sayılar kümesi iyi sıralı küme olduğundan pozitif tam sayılar kümesinin boştan farklı her  $A$  alt kümesi bir en küçük elemana sahiptir. Bu elemana  $t$  diyelim.  $t \in A$  olduğundan  $t \in I$  ve  $t > 0$  olur. Herhangi  $b \in I$  alalım.  $t > 0$  olduğundan  $b$  tam sayısını  $t$  tam sayısına kalanlı olarak bölebiliriz. Bu durumda  $b = qt + r$  ve  $0 \leq r < t$  olacak şekilde  $\exists q, r \in \mathbb{Z}$  vardır.  $b = qt + r$  olduğundan  $r = b - qt$  olup  $b, t \in I$  ve  $I, \mathbb{Z}$  nin bir ideali olduğundan  $r = b - qt \in I$  olur. Burada eğer  $r \neq 0$  olsa  $0 < r < t$  olup  $r \in A$  olur ki bu da  $t$  sayısının  $A$  nın en küçük elemanı olmasıyla çelişir. O halde

$r = 0$  olup  $b = qt \in (t)$  olur. Yani  $\forall b \in I$  için  $b \in (t)$  olup  $I \subset (t)$  olur. Ayrıca  $t \in I$  ve  $I, \mathbb{Z}$  nin bir ideali olduğundan  $(t) \subset I$  olur. O halde  $I = (t)$  olup  $I, R$  nin bir temel idealidir.

**Teorem 3.2.17.**  $a_1, a_2, \dots, a_n \in \mathbb{Z} - \{0\}$  ve  $k = [a_1, a_2, \dots, a_n] = OKEK(a_1, a_2, \dots, a_n)$  olsun. Bu durumda  $\cap_{i=1}^n (a_i) = (k)$  olur.

**İspat.** Teorem 3.2.7 gereği  $\cap_{i=1}^n (a_i)$  bir ideal ve Teorem 3.2.16 gereği  $\cap_{i=1}^n (a_i) = (k)$  bir temel idealdir.  $x \in \cap_{i=1}^n (a_i) \Rightarrow \forall i = 1, 2, \dots, n$  için  $x \in (a_i) \Rightarrow \forall i = 1, 2, \dots, n$  için  $a_i | x \Rightarrow k | x$  olduğundan  $x, a_i$  lerin bir ortak katı olur. Eğer  $y, a_i$  lerin herhangi bir ortak katı ise  $\forall i = 1, 2, \dots, n$  için  $a_i | y \Rightarrow y \in (a_i) \Rightarrow i = 1, 2, \dots, n$  için  $y \in \cap_{i=1}^n (a_i) = (k) \Rightarrow k | y$  olur. O halde  $\cap_{i=1}^n (a_i) = (k)$  olup istenen elde edilir.

**Teorem 3.2.18.**  $I_1, I_2, \dots, I_n$  bir  $R$  halkasının idealleri olsun. Bu durumda  $I = \{\sum_{k=1}^n a_k = a_1 + a_2 + \dots + a_n | a_1 \in I_1, a_2 \in I_2, \dots, a_n \in I_n\}$  kümesi  $R$  nin bir idealidir. Ayrıca  $1 \leq k \leq n$  için  $I_k \subset I$  olur.

**İspat.**  $1 \leq k \leq n$  olan herhangi  $k \in \mathbb{Z}$  ve herhangi  $a_k \in I_k$  verilsin. Burada  $1 \leq j \leq n$  ve  $j \neq k$  için  $a_j = 0_R$  alınırsa  $a_j \in I_j$  ve  $a_k = a_1 + a_2 + \dots + a_n \in I$  bulunur. O halde  $I_k \subset I$  olur. Yani  $1 \leq k \leq n$  için  $I_k \subset I$  olur. Burada  $1 \leq k \leq n$  için  $I_k \neq \emptyset$  olduğundan  $I \neq \emptyset$  olur. Ayrıca  $I \subset R$  olduğu da açıktır. Böylece  $\emptyset \neq I \subset R$  dir.

Herhangi  $a, b \in I$  ve herhangi  $r \in R$  için  $a, b \in I$  olduğundan  $a = \sum_{k=1}^n a_k$  ve  $b = \sum_{k=1}^n b_k$  olacak şekilde  $\exists a_k, b_k \in I_k$  ( $1 \leq k \leq n$ ) vardır. Burada  $1 \leq k \leq n$  için  $a_k, b_k \in I_k$  ve  $I_k, R$  nin bir ideali olduğundan  $a_k - b_k, ra_k, a_k r \in I_k$  olup  $a - b = \sum_{k=1}^n a_k - \sum_{k=1}^n b_k = \sum_{k=1}^n (a_k - b_k) \in I, ra = r \sum_{k=1}^n a_k = \sum_{k=1}^n ra_k \in I$  ve  $ar = (\sum_{k=1}^n a_k)r = \sum_{k=1}^n a_k r \in I$  bulunur. O halde  $I, R$  nin bir ideali olup istenen elde edilir.

**Tanım 3.2.19.** Teorem 3.2.18 deki  $I$  idealine  $I_1, I_2, \dots, I_n$  ideallerinin **toplamı** denir ve genellikle  $I = \sum_{k=1}^n I_k = I_1 + I_2 + \dots + I_n$  ile ifade edilir.

**Teorem 3.2.20.**  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  ve  $d = (a_1, a_2, \dots, a_n) = OBEB(a_1, a_2, \dots, a_n)$  olsun. Bu durumda  $\sum_{i=1}^n (a_i) = (d)$  olur.

**İspat.**  $d = (a_1, a_2, \dots, a_n) = OBEB(a_1, a_2, \dots, a_n)$  olduğundan  $1 \leq i \leq n$  için  $d | a_i$  olup  $a_i \in (d)$  olur. Bu durumda  $(d), \mathbb{Z}$  nin bir ideali olduğundan  $1 \leq i \leq n$  için  $(a_i) \subset (d)$  olup

$$\sum_{i=1}^n (a_i) \subset (d) \quad (1)$$

kapsaması bulunur.  $d = (a_1, a_2, \dots, a_n) = OBEB(a_1, a_2, \dots, a_n)$  olduğundan Teorem 1.5.12 den  $d = a_1 x_1 + a_2 x_2 + \dots + a_n x_n$  olacak şekilde  $\exists x_1, x_2, \dots, x_n \in \mathbb{Z}$  vardır. Burada  $1 \leq i \leq n$

için  $a_i x_i \in (a_i)$  olup  $d = a_1 x_1 + a_2 x_2 + \dots + a_n x_n \in \sum_{i=1}^n (a_i)$  bulunur.  $d \in \sum_{i=1}^n (a_i)$  ve  $\sum_{i=1}^n (a_i)$ ,  $\mathbb{Z}$  nin bir ideali olduğundan

$$(d) \subset \sum_{i=1}^n (a_i) \quad (2)$$

kapsaması elde edilir. (1) ve (2) den  $\sum_{i=1}^n (a_i) = (d)$  olup istenen elde edilir.

**Not.**  $I$ ,  $R$  halkasının bir ideali ise  $(I, +)$  grubu  $(R, +)$  değişmeli grubunun bir normal alt grubu olup  $(R/I, +)$  bölüm grubu anlamlıdır. Ayrıca  $(R, +)$  grubu değişmeli olduğundan  $(R/I, +)$  grubu da değişmelidir. Burada  $(R/I, +)$  grubunun elemanları  $a \in R$  olmak üzere  $\bar{a} = a + I = \{a + x \mid x \in I\}$  şeklindedir. Ayrıca  $\forall a, b \in R$  için  $\bar{a} + \bar{b} = a + I + b + I = a + b + I = \overline{a + b}$  olur.

**Teorem 3.2.21.**  $R$  bir halka ve  $I, R$  nin bir ideali olsun. Bu durumda  $R/I$  kümesi  $\forall a + I, b + I \in R/I$  için  $(a + I) + (b + I) = (a + b) + I$  ve  $(a + I) \cdot (b + I) = ab + I$  ile tanımlı  $+$  ve  $\cdot$  işlemlerine göre bir halkadır. Bu halkaya  $R$  nin  $I$  idealine göre **bölüm halkası** denir.

**İspat.** Teoremin ifadesindeki  $+$  işleminin  $R/I$  da bir iç işlem ve  $\cdot$  işleminin kapalı olduğu açıktır.  $a + I = x + I$  ve  $b + I = y + I$  olan herhangi  $a, b, x, y \in R$  için  $a - x \in I$  ve  $b - y \in I$  olur.  $a - x \in I$ ,  $b \in R$  ve  $I, R$  nin bir ideali olduğundan  $ab - xb = (a - x)b \in I$  olur.  $b - y \in I$ ,  $x \in R$  ve  $I, R$  nin bir ideali olduğundan  $xb - xy = x(b - y) \in I$  bulunur. O halde  $ab - xy = ab - xb + xb - xy \in I$  olup  $ab + I = xy + I$  eşitliği elde edilir. Böylece  $\cdot$  işlemi iyi tanımlı olup ayrıca kapalı olduğundan  $\cdot$  işlemi de  $R/I$  da bir iç işlemdir.

Şimdi bu işlemlerin halka tanımındaki koşulları sağladığını gösterelim.

**R1)**  $(R/I, +)$  cebirsel yapısının bir değişmeli grup olduğu yukarıdaki işlemlerden açıktır.

**R2)**  $R$  deki  $\cdot$  işleminin birleşme özelliği ve  $R/I$  daki  $\cdot$  işleminin tanımından  $\forall a + I, b + I, c + I \in R/I$  için

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

olup  $R/I$  daki  $\cdot$  işleminin birleşme özelliği vardır.

**R3)**  $R$  deki  $\cdot$  işleminin  $+$  işlemi üzerine sağdan, soldan dağılma özelliği ve  $R/I$  daki  $+$ ,  $\cdot$  işlemlerinin tanımından  $\forall a + I, b + I, c + I \in R/I$  için

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

ve

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

olup  $R/I$  da  $\cdot$  işleminin  $+$  işlemi üzerine sağdan ve soldan dağılma özellikleri vardır.

Böylece  $R/I$  kümesi teoremin ifadesinde tanımlanan  $+$  ve  $\cdot$  işlemlerine göre bir halka olup istenen elde edilir.

**Teorem 3.2.22.**  $R$  bir halka ve  $I, R$  nin bir ideali olsun. Bu durumda

- (i)  $R$  birimli ise  $R/I$  da birimlidir.
- (ii)  $R$  değişmeli ise  $R/I$  da değişmelidir.

**İspat.** (i)  $R$  birimli olsun.  $R/I$  halkasının  $1_R + I$  elemanını alalım. Burada  $\forall a \in R$  için  $a1_R = 1_R a = a$  olduğundan  $(a + I)(1_R + I) = a1_R + I = a + I$  ve  $(1_R + I)(a + I) = 1_R a + I = a + I$  olup  $1_R + I$  elemanı  $R/I$  halkasının birim elemanıdır. Böylece  $R/I$  birimli halka olup istenen elde edilir.

(ii)  $R$  değişmeli olsun. Her  $a + I, b + I \in R/I$  elemanları için  $a, b \in R$  olup  $R$  değişmeli olduğundan  $ab = ba$  bulunur. Buradan  $(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I)$  eşitliği sağlandığından  $R/I$  halkası değişmelidir.

**Teorem 3.2.23.**  $R$  bir halka ve  $I, R$  nin bir ideali olsun.  $S, R$  nin  $I$  yı kapsayan bir alt halkası ise  $I, S$  nin de bir ideali ve  $S/I, R/I$  nin bir alt halkası olur. Tersine,  $R/I$  nin her alt halkası  $T, R$  nin  $I$  yı kapsayan bir alt halkası olmak üzere  $T/I$  şeklindedir.

**İspat.**  $\emptyset \neq I \subset S$  olduğu açıktır. Herhangi  $a, b \in I$  ve herhangi  $r \in S$  alalım.  $r \in S$  ve  $S \subset R$  olduğundan  $r \in R$  dir.  $I, R$  nin bir ideali olduğundan  $a - b, ra, ar \in I$  olur. O halde  $I, S$  nin bir ideali olup  $S/I$  bölüm halkası anlamlıdır. Burada  $S/I \subset R/I$  ve her iki bölüm halkasındaki iç işlemler aynı olduğundan  $S/I, R/I$  nin bir alt halkası olur.

Tersine,  $R/I$  nin herhangi  $\bar{T}$  alt halkasını alalım.  $\bar{T}, R/I$  nin bir alt halkası olduğundan  $(\bar{T}, +)$  grubu  $(R/I, +)$  grubunun bir alt grubu olup Teorem 2.4.16 dan  $I \subset T$  ve  $\bar{T} = T/I$  olacak şekilde  $(R, +)$  grubunun bir  $T$  alt grubu vardır. Şimdi  $T$  kümesinin  $R$  nin bir alt halkası olduğunu göstereyim. Herhangi  $a, b \in T$  alalım.  $T, (R, +)$  grubunun bir alt grubu olduğundan  $a - b \in T$  bulunur.  $a, b \in T$  olduğundan  $a + I, b + I \in T/I = \bar{T}$  olup  $\bar{T}, R/I$  nin bir alt halkası olduğundan  $ab + I = (a + I)(b + I) \in \bar{T} = T/I$  eşitliği sağlanır. Bu durumda  $ab + I = t + I$  olacak şekilde  $\exists t \in T$  vardır.  $ab + I = t + I$  olduğundan  $ab - t \in I$  olup  $I \subset T$  olduğundan  $ab - t \in T$  dir. Bu durumda ayrıca  $t \in T$  ve  $T, (R, +)$  grubunun bir alt grubu olduğundan  $ab =$

$ab - t + t \in T$  dir. Dolayısıyla  $\forall a, b \in T$  için  $a - b \in T$  ve  $ab \in T$  olup Teorem 3.2.2 den  $T, R$  nin bir alt halkasıdır.

**Teorem 3.2.24.**  $R$  bir halka ve  $I, R$  nin bir ideali olsun.  $S, R$  nin  $I$  yı kapsayan bir ideali ise  $I, S$  nin de bir ideali ve  $S/I, R/I$  nin bir ideali olur. Tersine,  $R/I$  nin her ideali  $S, R$  nin  $I$  yı kapsayan bir ideali olmak üzere  $S/I$  şeklindedir.

**İspat.** Teorem 3.2.23 in ispatına benzer şekilde yapılır.

**Teorem 3.2.25.**  $R$  bir halka ve  $I, R$  nin bir ideali;  $S$  ve  $T, R$  nin birer alt halkası,  $I \subset S$  ve  $I \subset T$  olsun. Bu durumda  $S/I = T/I$  olması için gerek ve yeter koşul  $S = T$  olmasıdır.

**İspat.**  $(\Rightarrow) S/I = T/I$  olsun. Herhangi  $x \in S$  alalım.  $x \in S$  olduğundan  $x + I \in S/I = T/I$  olup  $x + I = y + I$  olacak şekilde  $\exists y \in T$  vardır.  $x + I = y + I$  olduğundan  $x - y \in I$  olur.  $x - y \in I$  ve  $I \subset T$  olduğundan  $x - y \in T$  olup ayrıca  $y \in T$  ve  $T, R$  nin bir alt halkası olduğundan  $x = x - y + y \in T$  olur. Yani  $\forall x \in S$  için  $x \in T$  olup

$$S \subset T \quad (1)$$

kapsaması bulunur. Herhangi  $x \in T$  alalım.  $x \in T$  olduğundan  $x + I \in T/I = S/I$  olup  $x + I = y + I$  olacak şekilde  $\exists y \in S$  vardır.  $x + I = y + I$  olduğundan  $x - y \in I$  olur.  $x - y \in I$  ve  $I \subset S$  olduğundan  $x - y \in S$  dir. Ayrıca  $y \in S$  ve  $S, R$  nin bir alt halkası olduğundan  $x = x - y + y \in S$  dir. Yani  $\forall x \in T$  için  $x \in S$  olup

$$T \subset S \quad (2)$$

kapsaması elde edilir. (1) ve (2) den  $S = T$  olup istenen elde edilir.

$(\Leftarrow)$  Açıktır.

### 3.3. HALKA HOMOMORFİZMALARI

**Tanım 3.3.1.**  $R$  ve  $S$  iki halka ve  $f: R \rightarrow S$  bir fonksiyon olsun. Eğer  $\forall a, b \in R$  için  $f(a + b) = f(a) + f(b)$  ve  $f(ab) = f(a)f(b)$  ise  $f$  ye,  $R$  den  $S$  ye bir **halka homomorfizması** denir.

**Not.**  $f: R \rightarrow S$  bir halka homomorfizması ise tanımdan  $f: (R, +) \rightarrow (S, +)$  bir grup homomorfizması olduğu anlaşılır. O halde grup homomorfizmasındaki özellikler burada da sağlanır. Aşağıdaki teorem grup homomorfizmalarındaki Teorem 2.5.2 den sağlanır.

**Teorem 3.3.2.**  $f: R \rightarrow S$  bir halka homomorfizması olsun. Bu durumda

(i)  $f(0_R) = 0_S$  olur.

(ii)  $\forall a \in R$  için  $f(-a) = -f(a)$  olur.

**Örnek.**  $R$  ve  $S$  iki halka olmak üzere  $\forall a \in R$  için  $f(a) = 0_S$  ile tanımlı  $f: R \rightarrow S$  dönüşümü bir halka homomorfizmasıdır. Gerçekten de  $\forall a, b \in R$  için  $f(a) = f(b) = f(a + b) = f(ab) = 0_S$  olup  $f(a + b) = 0_S = 0_S + 0_S = f(a) + f(b)$  ve  $f(ab) = 0_S = 0_S 0_S = f(a)f(b)$  sağlanır.

**Örnek.**  $n \in \mathbb{Z}^+$  olmak üzere  $f: \mathbb{Z} \rightarrow \mathbb{Z}_n, x \rightarrow f(x) = \bar{x}$  fonksiyonunu göz önüne alalım.  $\forall x, y \in \mathbb{Z}$  için  $f(x + y) = \overline{x + y} = \bar{x} + \bar{y} = f(x) + f(y)$  ve  $f(xy) = \overline{xy} = \bar{x} \cdot \bar{y} = f(x)f(y)$  olduğundan  $f$  bir halka homomorfizması olur. Ayrıca  $\forall \bar{x} \in \mathbb{Z}_n$  için  $f(x) = \bar{x}$  olduğundan  $f$  örtendir.

**Teorem 3.3.3.**  $f: R \rightarrow S$  bir halka homomorfizması olsun. Bu durumda

- (i)  $R$  nin her alt halkasının  $f$  altındaki görüntüsü  $S$  nin bir alt halkasıdır.
- (ii)  $S$  nin her alt halkasının  $f$  altındaki ters görüntüsü  $R$  nin bir alt halkasıdır.
- (iii)  $S$  nin her idealinin  $f$  altındaki ters görüntüsü  $R$  nin bir idealidir.

**İspat.** (i)  $R$  nin herhangi  $K$  alt halkasını alalım.  $f(K)$  kümesinin  $S$  nin bir alt halkası olduğu gösterilirse istenen elde edilir.  $K$ ,  $R$  nin bir alt halkası olduğundan  $\emptyset \neq K \subset R$  olup  $\emptyset \neq f(K) \subset S$  olur. Herhangi  $x, y \in f(K)$  alalım.  $x, y \in f(K)$  olduğundan  $x = f(a)$  ve  $y = f(b)$  olacak şekilde  $\exists a, b \in K$  vardır.  $a, b \in K$  ve  $K, R$  nin bir alt halkası olduğundan  $a - b \in K$  ve  $ab \in K$  iken  $f(a - b) \in f(K)$  ve  $f(ab) \in f(K)$  olur. Diğer taraftan  $f$  bir halka homomorfizması olduğundan  $f(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b) = x - y$  ve  $f(ab) = f(a)f(b) = xy$  sağlanır. O halde  $x - y \in f(K)$  ve  $xy \in f(K)$  olur. Yani  $\forall x, y \in f(K)$  için  $x - y \in f(K)$  ve  $xy \in f(K)$  olup Teorem 3.2.2 den  $f(K)$  kümesi  $S$  nin bir alt halkasıdır.

(ii)  $S$  nin herhangi  $T$  alt halkasını alalım.  $f^{-1}(T)$  kümesinin  $R$  nin bir alt halkası olduğu gösterilirse istenen elde edilir.  $f: R \rightarrow S$  bir halka homomorfizması olduğundan Teorem 3.3.2 den  $f(0_R) = 0_S \in T$  olup  $0_R \in f^{-1}(T)$  bulunur. O halde  $f^{-1}(T) \neq \emptyset$  olur. Ayrıca  $f^{-1}(T) \subset R$  dir. Böylece  $\emptyset \neq f^{-1}(T) \subset R$  olur. Herhangi  $a, b \in f^{-1}(T)$  alalım.  $a, b \in f^{-1}(T)$  olduğundan  $f(a), f(b) \in T$  olup  $T, S$  nin bir alt halkası olduğundan  $f(a) - f(b) \in T$  ve  $f(a)f(b) \in T$  dir. Diğer taraftan  $f: R \rightarrow S$  bir halka homomorfizması olduğundan  $f(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b)$  ve  $f(ab) = f(a)f(b)$  eşitlikleri sağlanır. O halde  $f(a - b) \in T$  ve  $f(ab) \in T$  olup  $a - b \in f^{-1}(T)$  ve  $ab \in f^{-1}(T)$  olur. Yani  $\forall a, b \in$

$f^{-1}(T)$  için  $a - b \in f^{-1}(T)$  ve  $ab \in f^{-1}(T)$  olup Teorem 3.2.2 den  $f^{-1}(T)$  kümesi  $R$  nin bir alt halkasıdır.

(iii)  $S$  nin herhangi  $J$  idealini alalım.  $f^{-1}(J)$  kümesinin  $R$  nin bir ideali olduğu gösterilirse istenen elde edilir.  $f: R \rightarrow S$  bir halka homomorfizması olduğundan Teorem 3.3.2 den  $f(0_R) = 0_S \in J$  olup  $0_R \in f^{-1}(J)$  olur. O halde  $f^{-1}(J) \neq \emptyset$  olur. Ayrıca  $f^{-1}(J) \subset R$  dir. Böylece  $\emptyset \neq f^{-1}(J) \subset R$  olur. Herhangi  $a, b \in f^{-1}(J)$  ve herhangi  $r \in R$  için  $f(a), f(b) \in J$  ve  $f(r) \in S$  dir.  $J, S$  nin bir ideali olduğundan  $f(a) - f(b) \in J, f(r)f(a) \in J$  ve  $f(a)f(r) \in J$  eşitlikleri sağlanır. Diğer taraftan  $f: R \rightarrow S$  nin bir halka homomorfizması olduğu göz önüne alınırsa  $f(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b), f(ra) = f(r)f(a)$  ve  $f(ar) = f(a)f(r)$  eşitlikleri sağlanır. O halde  $f(a - b) \in J, f(ra) \in J$  ve  $f(ar) \in J$  olup  $a - b \in f^{-1}(J), ra \in f^{-1}(J)$  ve  $ar \in f^{-1}(J)$  bulunur. Yani  $\forall a, b \in f^{-1}(J)$  ve  $\forall r \in R$  için  $a - b \in f^{-1}(J), ra \in f^{-1}(J)$  ve  $ar \in f^{-1}(J)$  olup tanımdan  $f^{-1}(J)$  kümesi  $R$  nin bir idealidir.

**Teorem 3.3.4.**  $f: R \rightarrow S$  örten bir halka homomorfizması olsun. Bu durumda

(i)  $R$  nin her idealinin  $f$  altındaki görüntüsü  $S$  nin bir idealidir.

(ii)  $R$  birimli ise  $S$  de birimlidir.

(iii)  $R$  değişmeli ise  $S$  de değişmelidir.

**İspat.** (i)  $R$  nin herhangi  $I$  idealini alalım.  $f(I)$  kümesinin  $S$  nin bir ideali olduğu gösterilirse istenen elde edilir.  $I, R$  nin bir ideali olduğundan  $\emptyset \neq I \subset R$  olup  $\emptyset \neq f(I) \subset S$  olur. Herhangi  $x, y \in f(I)$  ve herhangi  $s \in S$  için  $x, y \in f(I)$  olduğundan  $x = f(a)$  ve  $y = f(b)$  olacak şekilde  $\exists a, b \in I$  vardır.  $s \in S$  ve  $f$  örten olduğundan  $f(r) = s$  olacak şekilde  $\exists r \in R$  vardır.  $I, R$  nin bir ideali olduğundan  $a - b \in I, ra \in I$  ve  $ar \in I$  olup  $f(a - b) \in f(I), f(ra) \in f(I)$  ve  $f(ar) \in f(I)$  bulunur. Diğer taraftan  $f$  bir halka homomorfizması olduğundan  $f(a - b) = f(a) - f(b) = x - y, f(ra) = f(r)f(a) = sx$  ve  $f(ar) = f(a)f(r) = xs$  olur. O halde  $x - y \in f(I), sx \in f(I)$  ve  $xs \in f(I)$  olur. Yani  $\forall x, y \in f(I)$  ve  $\forall s \in S$  için  $x - y \in f(I), sx \in f(I)$  ve  $xs \in f(I)$  olup tanımdan  $f(I)$  kümesi  $S$  nin bir idealidir.

(ii)  $R$  birimli olsun. Herhangi  $x \in S$  alalım.  $x \in S$  ve  $f$  örten olduğundan  $f(a) = x$  olacak şekilde  $\exists a \in R$  vardır.  $a \in R$  ve  $1_R, R$  nin birim elemanı olduğundan  $a1_R = 1_R a = a$  olup  $f(a1_R) = f(1_R a) = f(a) = x$  olur. Diğer taraftan  $f$  bir halka homomorfizması olduğundan  $f(a1_R) = f(a)f(1_R) = xf(1_R)$  ve  $f(1_R a) = f(1_R)f(a) = f(1_R)x$  olup  $xf(1_R) = f(1_R)x = x$  eşitliği sağlanır. Yani  $\forall x \in S$  için  $xf(1_R) = f(1_R)x = x$  olup  $f(1_R)$  elemanı  $S$  nin birim elemanıdır.

(iii)  $R$  değişmeli olsun. Herhangi  $x, y \in S$  için  $f$  örten olduğundan  $x = f(a)$  ve  $y = f(b)$  olacak şekilde  $\exists a, b \in R$  vardır.  $a, b \in R$  ve  $R$  değişmeli olduğundan  $ab = ba$  olup  $f(ab) = f(ba)$  olur. Diğer taraftan  $f$  bir halka homomorfizması olduğundan  $f(ab) = f(a)f(b) = xy$  ve  $f(ba) = f(b)f(a) = yx$  olur. Yani  $\forall x, y \in S$  için  $xy = yx$  olup  $S$  değişmeli olur.

**Tanım 3.3.5.**  $f: R \rightarrow S$  bir halka homomorfizması olsun. Eğer  $f$  hem bire-bir, hem de örten ise  $f$  ye bir **halka izomorfizması** denir. Bu durumda  $R$  ve  $S$  halkaları **izomorfikler** denir ve genellikle  $R \cong S$  ile ifade edilir.

**Tanım 3.3.6.**  $f: R \rightarrow S$  bir halka homomorfizması olsun.  $f^{-1}(0_S) = \{x \in R \mid f(x) = 0_S\}$  kümesine  $f$  nin **çekirdeği** denir ve genellikle  $\text{Çek}f$  ile ifade edilir. Yani  $\text{Çek}f = f^{-1}(0_S) = \{x \in R \mid f(x) = 0_S\}$  olarak tanımlanır.

**Teorem 3.3.7.**  $f: R \rightarrow S$  bir halka homomorfizması olsun. Bu durumda  $f$  nin bire-bir olması için gerek ve yeter koşul  $\text{Çek}f = \{0_R\}$  olmasıdır.

**İspat.** Önerme 2.5.7 nin ispatına benzer şekilde yapılabilir.

**Örnek.**  $n \in \mathbb{Z}^+$  olmak üzere  $f: \mathbb{Z} \rightarrow \mathbb{Z}_n, x \rightarrow f(x) = \bar{x}$  örten halka homomorfizmasının çekirdeğini bulalım.  $x \in \mathbb{Z}$  olmak üzere

$$x \in \text{Çek}f \Leftrightarrow f(x) = \bar{0} \Leftrightarrow \bar{x} = \bar{0} \Leftrightarrow x \equiv 0 \pmod{n} \Leftrightarrow n \mid x \Leftrightarrow x \in n\mathbb{Z} = (n)$$

denkliklerinden  $\text{Çek}f = n\mathbb{Z} = (n)$  olduğu anlaşılır.

**Teorem 3.3.8.**  $R$  bir halka ve  $I, R$  nin bir ideali olsun. Bu durumda  $\varphi: R \rightarrow R/I, r \rightarrow \varphi(r) = r + I$  ile tanımlı  $\varphi$  dönüşümü örten bir halka homomorfizmasıdır. Ayrıca  $\text{Çek}\varphi = I$  dir. Bu halka homomorfizmasına **doğal halka homomorfizması** denir.

**İspat.**  $\varphi$  nin bir fonksiyon olduğu açıktır. Ayrıca  $\varphi$  nin tanımından  $\forall x, y \in R$  için  $\varphi(x + y) = x + y + I = x + I + y + I = \varphi(x) + \varphi(y)$ ,  $\varphi(xy) = xy + I = (x + I)(y + I) = \varphi(x)\varphi(y)$  olup  $\varphi$  bir halka homomorfizmasıdır. Burada yine  $\varphi$  nin tanımından  $\forall r + I \in R/I$  için  $\varphi(r) = r + I$  olup  $\varphi$  örtendir. Ayrıca  $x \in R$  için  $x \in \text{Çek}\varphi \Leftrightarrow \varphi(x) = 0_{R/I} \Leftrightarrow x + I = I \Leftrightarrow x \in I$  denkliklerinden  $\text{Çek}\varphi = I$  olduğu anlaşılır.

**Teorem 3.3.9.(Homomorfizma Teoremi)**  $f: R \rightarrow S$  bir halka homomorfizması ve  $\text{Çek}f = K$  olsun. Bu durumda

(i)  $K, R$  nin bir idealidir.

(ii)  $R/K \cong f(R)$  olur.

**İspat.** (i)  $0_R \in \text{Çekf} = K$  olduğundan  $K \neq \emptyset$  dir. Böylece  $\emptyset \neq K \subset R$  olur. Herhangi  $a, b \in K$  ve herhangi  $r \in R$  alalım.  $a, b \in K = \text{Çekf}$  olduğundan  $f(a) = f(b) = 0_S$  olup  $f$  bir halka homomorfizması olduğundan  $f(a - b) = f(a) - f(b) = 0_S$ ,  $f(ra) = f(r)f(a) = f(r)0_S = 0_S$  ve  $f(ar) = f(a)f(r) = 0_S f(r) = 0_S$  dir. O halde  $a - b \in \text{Çekf} = K$ ,  $ra \in \text{Çekf} = K$  ve  $ar \in \text{Çekf} = K$  olup  $K, R$  nin bir idealidir.

(ii)  $\bar{f}: R/K \rightarrow f(R), r + K \rightarrow \bar{f}(r + K) = f(r)$  dönüşümünü tanımlayalım.  $\bar{f}$  nin kapalı olduğu açıktır.  $x + K = y + K$  olan herhangi  $x, y \in R$  alalım.  $x + K = y + K$  olduğundan  $x - y \in K = \text{Çekf}$  olup  $f(x) - f(y) = f(x - y) = 0_S$  olur. O halde  $f(x) = f(y)$  olup  $\bar{f}$  iyi tanımlıdır. Ayrıca  $f$  bir halka homomorfizması olduğundan  $\bar{f}$  nin tanımından  $\forall x + K, y + K \in R/K$  için

$$\bar{f}(x + K + y + K) = \bar{f}(x + y + K) = f(x + y) = f(x) + f(y) = \bar{f}(x + K) + \bar{f}(y + K)$$

ve

$$\bar{f}((x + K)(y + K)) = \bar{f}(xy + K) = f(xy) = f(x)f(y) = \bar{f}(x + K)\bar{f}(y + K)$$

olup  $\bar{f}$  bir halka homomorfizmasıdır.

$\bar{f}(x + K) = \bar{f}(y + K)$  olan herhangi  $x + K, y + K \in R/K$  için  $f(x) = \bar{f}(x + K) = \bar{f}(y + K) = f(y)$  eşitliğinden  $f(x - y) = f(x) - f(y) = 0_S$  olur. Bu durumda  $x - y \in \text{Çekf} = K$  olup  $x + K = y + K$  bulunur. O halde  $\bar{f}$  bire-birdir. Herhangi  $a \in f(R)$  için  $a \in f(R)$  olduğundan  $f(x) = a$  olacak şekilde  $\exists x \in R$  vardır. Burada  $\bar{f}$  nin tanımından  $\bar{f}(x + K) = f(x) = a$  olup  $\bar{f}$  örtendir.

$\bar{f}: R/K \rightarrow f(R)$  bire-bir ve örten bir halka homomorfizması olduğundan bir halka izomorfizması olup  $R/K \cong f(R)$  olur.

**Sonuç 3.3.10.**  $f: R \rightarrow S$  örten bir halka homomorfizması ve  $\text{Çekf} = K$  ise  $\varphi: R \rightarrow R/K$  doğal halka homomorfizması ve  $\bar{f}: R/K \rightarrow f(R) = S, r + K \rightarrow \bar{f}(r + K) = f(r)$  ile tanımlı halka homomorfizması olmak üzere  $f = \bar{f} \circ \varphi$  olur. Burada  $f$  nin böyle yazılışına **doğal ayrışım** denir.

**Sonuç 3.3.11.**  $f: R \rightarrow S$  bir halka homomorfizması ve  $\text{Çekf} = K$  ise  $\varphi: R \rightarrow R/K$  doğal halka homomorfizması,  $\bar{f}: R/K \rightarrow f(R), r + K \rightarrow \bar{f}(r + K) = f(r)$  ile tanımlı halka homomorfizması ve  $i: f(R) \rightarrow S, x \rightarrow i(x) = x$  ile tanımlı halka homomorfizması olmak üzere  $f = i \circ \bar{f} \circ \varphi$  eşitliği sağlanır. Buradaki  $i$  bire-bir homomorfizmasına **gömme homomorfizması**,  $f$  nin böyle yazılışına da **doğal ayrışım** denir.

**Teorem 3.3.12. (1. İzomorfizma Teoremi)**  $R$  bir halka,  $S, R$  nin bir alt halkası ve  $I, R$  nin bir ideali olsun. Bu durumda  $S + I = \{s + a \mid s \in S \text{ ve } a \in I\}$  kümesi  $R$  nin  $I$  idealini kapsayan bir alt halkası olur. Ayrıca  $S \cap I$  kümesi  $S$  nin bir ideali ve  $(S + I)/I \cong S/(S \cap I)$  olur.

**İspat.**  $0_R \in S$  olduğundan  $\forall x \in I$  için  $x = 0_R + x \in S + I$  olup  $I \subset S + I$  olur. Burada  $I \neq \emptyset$  olduğundan  $S + I \neq \emptyset$  dir. Böylece  $\emptyset \neq S + I \subset R$  olduğu görülür. Herhangi  $x, y \in S + I$  için  $x, y \in S + I$  olduğundan  $x = s_1 + a_1$  ve  $y = s_2 + a_2$  olacak şekilde  $\exists s_1, s_2 \in S$  ve  $\exists a_1, a_2 \in I$  vardır.  $x = s_1 + a_1$  ve  $y = s_2 + a_2$  olduğundan  $x - y = s_1 - s_2 + a_1 - a_2$  ve  $xy = s_1s_2 + s_1a_2 + a_1s_2 + a_1a_2$  olur. Burada  $s_1, s_2 \in S$  ve  $S, R$  nin bir alt halkası olduğundan  $s_1 - s_2 \in S$  ve  $s_1s_2 \in S$  olur.  $a_1, a_2 \in I$  ve  $I, R$  nin bir ideali olduğundan  $a_1 - a_2 \in I$  olur. Ayrıca  $s_1a_2, a_1s_2, a_1a_2 \in I$  için  $s_1a_2 + a_1s_2 + a_1a_2 \in I$  olduğu açıktır. O halde  $x - y = s_1 - s_2 + a_1 - a_2 \in S + I$  ve  $xy = s_1s_2 + s_1a_2 + a_1s_2 + a_1a_2 \in S + I$  olup Teorem 3.2.2 den  $S + I$  kümesi  $R$  nin bir alt halkasıdır. Üstelik  $I \subset S + I$  olduğundan  $I, S + I$  nin bir ideali olup  $(S + I)/I, R/I$  nin bir alt halkasıdır. Üstelik

$$f: S \rightarrow (S + I)/I, \quad x \mapsto f(x) = x + I$$

dönüşümünü tanımlayalım.  $0_R \in I$  olduğundan  $\forall x \in S$  için  $x = x + 0_R \in S + I$  olup  $f$  kapalıdır.  $f$  nin iyi tanımlı olduğu da açıktır. Yani  $f$  bir fonksiyondur. Her  $x, y \in S$  için  $f(x + y) = x + y + I = x + I + y + I = f(x) + f(y)$  ve  $f(xy) = xy + I = (x + I)(y + I) = f(x)f(y)$  olup  $f$  bir halka homomorfizmasıdır. Herhangi  $\bar{y} \in (S + I)/I$  için  $\bar{y} \in (S + I)/I$  olduğundan  $\bar{y} = y + I$  olacak şekilde  $\exists y \in S + I$  vardır.  $y \in S + I$  olduğundan  $y = s + a$  olacak şekilde  $\exists s \in S$  ve  $\exists a \in I$  vardır.  $y = s + a$  olduğundan  $y - s = a \in I$  olup  $y + I = s + I$  bulunur. Burada  $s \in S$  için  $f$  nin tanımından  $f(s) = s + I = y + I = \bar{y}$  olup  $f$  örtendir.  $x \in S$  olmak üzere

$$x \in \text{Çek}f \Leftrightarrow f(x) = 0_{R/I} \Leftrightarrow x + I = I \Leftrightarrow x \in I \Leftrightarrow x \in S \cap I$$

denkliklerinden  $\text{Çek}f = S \cap I$  olduğu anlaşılır. O halde Homomorfizma Teoreminden  $(S + I)/I \cong S/(S \cap I)$  izomorfizması elde edilir.

**Teorem 3.3.13. (2. İzomorfizma Teoremi)**  $f: R \rightarrow S$  örten bir halka homomorfizması ve  $\text{Çek}f = K$  olsun. Bu durumda  $S$  nin idealleri ile  $R$  nin  $K$  yı kapsayan idealleri arasında  $I \rightarrow f^{-1}(I)$  şeklinde bire-bir ve örten bir eşleme yapılabilir. Burada  $S$  nin bir  $I$  ideali verildiğinde  $J = f^{-1}(I)$  olmak üzere  $R/J \cong S/I$  olur.

**İspat.** Teorem 3.3.3 (iii) den  $S$  nin her  $I$  ideali için  $f^{-1}(I), R$  nin bir ideali olur. Ayrıca  $0_S \in I$  olduğundan  $\text{Çek}f = f^{-1}(0_S) \subset f^{-1}(I)$  kapsaması vardır.  $f: R \rightarrow S$  örten bir fonksiyon olduğundan  $S$  nin her  $T$  alt kümesi için  $f(f^{-1}(T)) = T$  olduğu kolayca gösterilebilir. O halde

$S$  nin  $f^{-1}(I_1) = f^{-1}(I_2)$  olan her  $I_1$  ve  $I_2$  idealleri için  $f(f^{-1}(I_1)) = f(f^{-1}(I_2))$  olup  $f(f^{-1}(I_1)) = I_1$  ve  $f(f^{-1}(I_2)) = I_2$  olduğundan  $I_1 = I_2$  eşitliği sağlanır.  $R$  nin  $K$  yı kapsayan herhangi  $T$  ideali için  $f(T) = L$  diyelim.  $f$  örten olduğundan Teorem 3.3.4 (i) den  $L$ ,  $S$  nin bir idealidir. Herhangi  $t \in T$  için  $f(t) \in f(T) = L$  olup  $t \in f^{-1}(L)$  bulunur. O halde  $T \subset f^{-1}(L)$  dir. Herhangi  $x \in f^{-1}(L)$  için  $f(x) \in L = f(T)$  dir. Böylece  $f(x) = f(t)$  olacak şekilde  $\exists t \in T$  vardır.  $f(x) = f(t)$  ve  $f$  bir halka homomorfizması olduğundan  $f(x - t) = f(x) - f(t) = 0_S$  olup  $x - t \in \text{Çek}f = K$  bulunur.  $x - t \in K$  ve  $K \subset T$  olduğundan  $x - t \in T$  dir. Üstelik  $t \in T$  ve  $T$ ,  $R$  nin bir ideali olduğundan  $x = x - t + t \in T$  olur. O halde  $f^{-1}(L) \subset T$  olup  $T \subset f^{-1}(L)$  kapsamasından  $f^{-1}(L) = T$  bulunur. Böylece  $S$  nin idealleri ile  $R$  nin  $K$  yı kapsayan idealleri arasında  $I \rightarrow f^{-1}(I)$  şeklinde bire-bir bir eşleme yapılabilir.

Şimdi  $I$ ,  $S$  nin bir ideali ve  $J = f^{-1}(I)$  olsun.  $R/J \cong S/I$  olduğu gösterilirse istenen elde edilir.

$$h: R \rightarrow S/I, \quad x \rightarrow h(x) = f(x) + I$$

dönüşümünü tanımlayalım.  $h$  nin bir fonksiyon olduğu açıktır. Ayrıca  $f$  bir halka homomorfizması olduğundan  $\forall x, y \in R$  için

$$h(x + y) = f(x + y) + I = f(x) + f(y) + I = f(x) + I + f(y) + I = h(x) + h(y)$$

ve

$$h(xy) = f(xy) + I = f(x)f(y) + I = (f(x) + I)(f(y) + I) = h(x)h(y)$$

olup  $h$  bir halka homomorfizmasıdır. Herhangi  $y + I \in S/I$  için  $y \in S$  ve  $f$  örten olduğundan  $f(x) = y$  olacak şekilde  $\exists x \in R$  vardır. Burada  $h$  nin tanımından  $h(x) = f(x) + I = y + I$  olup  $h$  örtendir. Diğer taraftan  $x \in R$  olmak üzere

$$x \in \text{Çek}h \Leftrightarrow h(x) = 0_{S/I} \Leftrightarrow f(x) + I = I \Leftrightarrow f(x) \in I \Leftrightarrow x \in f^{-1}(I) = J$$

denkliklerinden  $\text{Çek}h = J$  olduğu anlaşılır. O halde Homomorfizma Teoreminden  $R/J \cong h(R) = S/I$  izomorfizması elde edilir.

**Sonuç 3.3.14.**  $R$  bir halka ve  $I$ ,  $R$  nin bir ideali olsun. Bu takdirde  $R$  nin  $I$  yı kapsayan idealleri ile  $R/I$  nin idealleri arasında  $K \rightarrow K/I$  şeklinde bire-bir bir eşleme yapılabilir.

**İspat.**  $\varphi: R \rightarrow R/I, x \rightarrow \varphi(x) = x + I$  doğal homomorfizması için Teorem 3.3.13 de  $f = \varphi$  alınarak istenen elde edilir.

**Örnek.**  $f: \mathbb{Z} \rightarrow \mathbb{Z}_{10}, x \rightarrow f(x) = \bar{x}$  örten halka homomorfizmasından yararlanarak  $\mathbb{Z}_{10}$  halkasının ideallerini bulalım. Bir önceki örnekten  $\text{Çek}f = 10\mathbb{Z} = (10)$  olduğunu biliyoruz. O halde  $\mathbb{Z}_{10}$  halkasının idealleri  $m \in \mathbb{Z}^+$  ve  $(10) \subset m\mathbb{Z} = (m)$  olmak üzere  $f(m\mathbb{Z}) = (\overline{m})$  şeklindedir. Burada  $(10) \subset m\mathbb{Z} = (m) \Leftrightarrow m|10$  denkliği vardır.  $m|10$  koşulunu sağlayan

pozitif tam sayılar 1, 2, 5 ve 10 tam sayılarıdır. O halde  $\mathbb{Z}_{10}$  halkasının idealleri  $(\overline{1})$ ,  $(\overline{2})$ ,  $(\overline{5})$  ve  $(\overline{10}) = (\overline{0})$  idealleridir.

**Tanım 3.3.15.** Birimli bir halkada, biriminin ürettiği alt halkaya bu halkanın **asal alt halkası** denir.

Tanımdan birimli bir halkanın asal alt halkasının o halkanın birimini kapsayan en küçük alt halkası olduğu anlaşılır.

**Örnek.** Bir tamlık bölgesi; karakteristiği sıfır olan bir asal alt halkaya sahip ise  $\mathbb{Z}$  ye, karakteristiği  $p$  asal tam sayısı olan bir asal alt halkaya sahip ise  $\mathbb{Z}_p$  ye izomorf bir alt halka kapsar.

**Çözüm.**  $R$  bir tamlık bölgesi olsun. Her  $n \in \mathbb{Z}$  için  $f(n) = n1_R$  ile tanımlı  $f: \mathbb{Z} \rightarrow R$  fonksiyonu bir homomorfizmadır. Eğer  $R$  nin karakteristiği sıfır ise  $\text{Çek}(f) = (0)$  olacağından,  $f$  bire-bir ve dolayısıyla  $\mathbb{Z} \cong f(R) \subset R$  dir. Eğer  $R$  nin karakteristiği  $p$  asal tam sayısı ise,  $\text{Çek}(f) = (p)$  olup Homomorfizma Teoremine göre  $\mathbb{Z}/(p) = \mathbb{Z}_p \cong f(R) \subset R$  olur.

### 3.4. ASAL VE MAKSİMAL İDEALLER

**Tanım 3.4.1.**  $R$  değişmeli bir halka ve  $P$  de  $R$  nin kendisinden farklı bir ideali olsun. Eğer  $ab \in P$  olan her  $a, b \in R$  için  $a \in P$  veya  $b \in P$  ise  $P$  ye  $R$  nin bir **asal ideali** denir.

**Örnek.**  $p$  bir asal tam sayı olmak üzere  $(p)$  ideali  $\mathbb{Z}$  nin bir asal idealidir.

**Tanım 3.4.2.**  $R$  bir tamlık bölgesi,  $\pi \in R, \pi \notin U_R$  ve  $\pi \neq 0_R$  olsun.  $a, b \in R$  için,  $\pi|ab$  olmak üzere  $\pi|a$  veya  $\pi|b$  ise  $\pi \in R$  elemanına **asal eleman** denir.

**Örnek.**  $R$  bir tamlık bölgesi ve  $\pi$ ,  $R$  nin bir asal elemanı olsun.  $R$  nin  $I = (\pi) = \pi R = R\pi$  idealini alalım. Burada  $I = (\pi) = \{\pi x | x \in R\} = \{y \in R | \exists x \in R \text{ için } y = \pi x\} = \{y | y \in R \text{ ve } \pi|y\}$  olur.  $a, b \in R$  olmak üzere  $ab \in I = \pi R$  ise  $\pi|ab$  olup  $\pi, R$  nin asal elemanı olduğundan  $\pi|a$  veya  $\pi|b$  olur. Bu durumda  $a \in I$  veya  $b \in I$  olup  $I, R$  nin bir asal ideali olur.

**Örnek.**  $\mathbb{Z}$  nin  $(8) = 8\mathbb{Z}$  ideali asal değildir. Çünkü  $4 \cdot 2 = 8 \in (8)$  olduğu halde  $4 \notin (8)$  ve  $2 \notin (8)$  dir.

**Teorem 3.4.3.**  $R$  bir TİB olsun. Bu durumda  $R$  nin bir  $P$  idealinin asal ideal olması için gerek ve yeter koşul  $\pi \in R$  asal veya sıfır olmak üzere  $P = (\pi)$  şeklinde olmasıdır.

**İspat.**  $(\Rightarrow)$   $P$  ideali asal olsun.  $R$  bir TİB olduğundan  $P = (\pi)$  olacak şekilde  $\exists \pi \in R$  vardır. Eğer  $\pi = 0_R$  ise istenen elde edilir. Kabul edelim ki  $\pi \neq 0_R$  olsun.  $P$  ideali asal olduğundan  $P \neq R$  olup  $\pi \notin U_R$  olur.  $\pi|ab$  olan herhangi  $a, b \in R$  alalım.  $\pi|ab$  olduğundan  $ab \in R\pi = (\pi) = P$  olup  $P$  ideali asal olduğundan  $a \in P$  veya  $b \in P$  olur. Eğer  $a \in P = R\pi$  ise  $\pi|a$  olur. Eğer  $b \in P = R\pi$  ise bu durumda da  $\pi|b$  olur. O halde  $\pi$  asal olup istenen elde edilir.

$(\Leftarrow)$   $\pi \in R$  asal veya sıfır olmak üzere  $P = (\pi)$  şeklinde olsun. Eğer  $\pi$  asal ise bu bölümdeki ikinci örnekten  $P = (\pi)$  ideali asaldır. Kabul edelim ki  $\pi = 0_R$  olsun. Bu durumda  $P = (\pi) = 0$  olur. Burada  $ab \in P = 0$  olan her  $a, b \in R$  için  $ab = 0_R$  olup  $R$  nin sıfır bölensizliği gereğince  $a = 0_R \in P$  veya  $b = 0_R \in P$  olur. O halde  $P$  ideali asal olup istenen elde edilir.

**Teorem 3.4.4.**  $R$  birimli ve değişmeli bir halka ve  $I, R$  nin  $R$  den farklı bir ideali olsun. Bu durumda  $I$  nin asal ideal olması için gerek ve yeter koşul  $R/I$  bölüm halkasının bir tamlık bölgesi olmasıdır.

**İspat.**  $(\Rightarrow)$   $I$  ideali asal olsun.  $R$  halkası birimli ve değişmeli olduğundan Teorem 3.2.22 den  $R/I$  bölüm halkası da birimli ve değişmeli olur. Sıfırdan farklı herhangi  $a + I \in R/I$  ve  $(a + I)(b + I) = 0_{R/I} = I$  olan herhangi  $b + I \in R/I$  için  $a + I \neq 0_{R/I} = I$  olduğundan  $a \notin I$  olur.  $ab + I = (a + I)(b + I) = I$  olduğundan  $ab \in I$  olup  $I, R$  nin asal ideali olduğundan  $a \in I$  veya  $b \in I$  olur. Burada  $a \notin I$  olduğundan  $b \in I$  olup  $b + I = I = 0_{R/I}$  bulunur. O halde  $a + I$  elemanı  $R/I$  nin bir sıfır bölen olmayan elemanı olur. Yani  $R/I$  nin sıfırdan farklı her elemanı bir sıfır bölen değildir. O halde  $R/I$  sıfır bölensiz olup ayrıca birimli ve değişmeli olduğundan  $R/I$  halkası bir tamlık bölgesi olur.

$(\Leftarrow)$   $R/I$  bölüm halkası bir tamlık bölgesi olsun.  $ab \in I$  olan herhangi  $a, b \in I$  alalım.  $ab \in I$  olduğundan  $(a + I)(b + I) = ab + I = 0_{R/I} = I$  olup  $R/I$  bölüm halkası sıfır bölensiz olduğundan  $a + I = 0_{R/I} = I$  veya  $b + I = 0_{R/I} = I$  olur. Bu durumda  $a \in I$  veya  $b \in I$  olup  $I, R$  nin asal idealidir.

**Tanım 3.4.5.**  $R$  değişmeli bir halka ve  $M, R$  nin  $R$  den farklı bir ideali olsun. Eğer  $R$  nin  $M$  yi kapsayan  $M$  ve  $R$  den başka hiçbir ideali yoksa  $M$  ye  $R$  nin bir **maksimal ideali** denir.

**Teorem 3.4.6.**  $R$  bir halka ve  $M, R$  nin  $R$  den farklı bir ideali olsun. Bu durumda  $M$  nin maksimal ideal olması için gerek ve yeter koşul her  $x \in R - M$  için  $M + (x) = R$  olmasıdır.

**İspat:** ( $\Rightarrow$ )  $M, R$  nin maksimal ideali olsun. Herhangi  $x \in R - M$  alalım.  $x \in R - M$  olduğundan  $x \in R$  ve  $x \notin M$  olur.  $x \notin M$  olduğundan  $M \neq M + (x)$  olur. Ayrıca  $M \subset M + (x)$  ve  $M, R$  nin bir maksimal ideali olduğundan  $M + (x) = R$  olup istenen elde edilir.

( $\Leftarrow$ ) Herhangi bir  $x \in R - M$  için  $M + (x) = R$  olsun.  $R$  nin  $M$  yi kapsayan  $M$  den farklı herhangi  $K$  idealini alalım.  $K = R$  olduğu gösterilirse istenen elde edilir.  $M \subset K$  ve  $M \neq K$  olduğundan  $\exists x \in K - M$  vardır.  $x \in K - M$  olduğundan  $x \in R - M$  olup hipotezden  $M + (x) = R$  olur. Burada  $M \subset K$  ve  $x \in K$  olduğundan  $R = M + (x) \subset K$  olur. Ayrıca  $K \subset R$  olduğundan  $K = R$  olup istenen elde edilir.

**Teorem 3.4.7.**  $R$  birimli ve değişmeli bir halka ve  $M, R$  nin  $R$  den farklı bir ideali olsun. Bu durumda  $M$  idealinin maksimal ideal olması için gerek ve yeter koşul  $R/M$  bölüm halkasının bir cisim olmasıdır.

**İspat.** ( $\Rightarrow$ )  $M, R$  nin maksimal ideali olsun.  $M \neq R$  olduğundan  $R/M \neq 0$  olur.  $R$  halkası birimli ve değişmeli olduğundan Teorem 3.2.22 den  $R/M$  bölüm halkası da birimli ve değişmelidir. Herhangi  $x + M \neq 0_{R/M} = M$  için  $x \notin M$  olup  $x \in R - M$  dir. Bu durumda  $M$  maksimal olduğundan Teorem 3.4.6 gereği  $M + (x) = R$  olup  $1_R \in M + (x)$  bulunur.  $1_R \in M + (x) = M + Rx$  olduğundan  $1_R = m + rx$  olacak şekilde  $\exists m \in M$  ve  $\exists r \in R$  vardır.

Burada  $1_R + M = m + rx + M = rx + M = (r + M)(x + M)$  olup ayrıca  $R/M$  değişmeli olduğundan  $(x + M)(r + M) = (r + M)(x + M) = 1_R + M$  dir. O halde  $r + M$  eleman  $x + M$  elemanının  $R/M$  de tersidir. Yani  $R/M$  nin sıfırdan farklı her elemanının  $\cdot$  işlemine göre tersi vardır. O halde  $R/M$  bölüm halkası bir cisimdir.

( $\Leftarrow$ )  $R/M$  bölüm halkası bir cisim olsun. Herhangi  $x \in R - M$  için  $x \in R$  ve  $x \notin M$  olup  $x + M \neq M = 0_{R/M}$  dir.  $R/M$  bir cisim olduğundan  $(r + M)(x + M) = (x + M)(r + M) = 1_R + M$  olacak şekilde  $\exists r + M \in R/M$  vardır.  $rx + M = (r + M)(x + M) = 1_R + M$  olduğundan  $rx - 1_R \in M$  olup  $rx - 1_R = m$  olacak şekilde  $\exists m \in M$  vardır.  $rx - 1_R = m$  olduğundan  $rx - m = 1_R$  eşitliği sağlanır. Her  $y \in R$  için  $y = y1_R = y(rx - m) = y(-m) + yrx \in M + Rx = M + (x)$  olur. O halde  $R \subset M + (x)$  olup ayrıca  $M + (x) \subset R$  olduğundan  $M + (x) = R$  olur. Böylece Teorem 3.4.6 gereği  $M, R$  nin maksimal idealidir.

**Sonuç 3.4.8.** Birimli ve değişmeli bir  $R$  halkasının her maksimal ideali bir asal idealdir.

**İspat.**  $M, R$  nin bir maksimal ideali ise  $R/M$  bölüm halkası bir cisim olup tamlık bölgesi olur. O halde  $M$  ideali asal ideal olup istenen elde edilir.

**Örnek.**  $\mathbb{Z}$  tam sayılar halkası bir TİB olduğundan her  $p$  asal tam sayısı için  $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$  halkası bir cisimdir.

**Örnek.** Birim elemanlı olmayan  $2\mathbb{Z}$  çift tam sayılar halkasında  $4\mathbb{Z}$  idealini göz önüne alalım.  $2 \cdot 2 \in 4\mathbb{Z}$  iken  $2 \notin 4\mathbb{Z}$  olduğundan  $2\mathbb{Z}$  çift tam sayılar halkasında  $4\mathbb{Z}$  ideali bir asal ideal değildir. Ayrıca  $4\mathbb{Z} \subsetneq m\mathbb{Z} \subsetneq 2\mathbb{Z}$  olacak şekilde  $m \in 2\mathbb{Z}$  mevcut olmadığından  $4\mathbb{Z}$  yi öz olarak içeren  $2\mathbb{Z}$  den farklı  $2\mathbb{Z}$  nin  $m\mathbb{Z}$  ideali mevcut değildir. Dolayısıyla  $4\mathbb{Z}$ ,  $2\mathbb{Z}$  nin bir maksimal idealidir.

## KAYNAKÇA

---

- Cohn, Paul Moritz. Basic algebra: groups, rings and fields. Springer Science & Business Media, 2012.
- Çallıalp, Fethi. Cebir. Sakarya Üniversitesi, 1994.
- Çallıalp, Fethi, Lineer Cebir, Birsen Yayınevi, 2009.
- Çallıalp, Fethi, Soyut Matematik, Birsen Yayınevi, 2009.
- Çallıalp, Fethi, Örneklerle Soyut Cebir, Birsen Yayınevi, 2011.
- Durbin, John R. Modern algebra: An introduction. John Wiley & Sons, 2008.
- Fraleigh, John B. A first course in abstract algebra. Pearson Education India, 2003.
- Herstein, Israel N. Topics in algebra. John Wiley & Sons, 1991.
- Hungerford, Thomas W. Algebra. Vol. 73. Springer Science & Business Media, 2012.
- Malik, Davender S., John N. Mordeson, and M. K. Sen. Fundamentals of abstract algebra. McGraw-Hill, 1997.
- Patterson EM. A First Course in Rings and Ideals. By David M. Burton. Pp. viii, 309. 1970. (Addison-Wesley.).
- The Mathematical Gazette. 1972;56(396):170-171. doi:10.2307/3615330.
- Taşçı, Dursun, Soyut Cebir, Gazi Kitabevi, 2018.
- Türkmen Nişancı Burcu, Türkmen Ergül, Grup Teorisi I, Amasya Üniversitesi, 2021.