GRUP TEORİ

DERS NOTLARI

Dr. Öğr. Üyesi Didem ÖZTÜRK

2024-2025

UYARI

ÖNSÖZ

Grup Teori adlı ders notları, MSGSÜ Fen Edebiyat Fakültesi Matematik Bölümü'nde lisans programında anlattığım MAT477 Grup Teori dersinin konularını kapsamaktadır. Bu çalışmada, öğrencilerin, grup teorisine ait esas teşkil eden teoremleri ve ispatları daha iyi anlayarak, soyut düşünme yetilerinin güçlenmesi amaçlanmıştır.

Bu kaynağın, MAT438 Grupların Gösteriliş Teorisine Giriş, MAT476 Permütasyon Grupları, MAT216 Geometri ve Cebir, yüksek lisans programında anlatmakta olduğum MAT501 Cebir 1 adlı dersler için de yararlı olacağı inancındayım.

İ.Ü Fen Fakültesi Matematik Bölümü'nde henüz bir lisans öğrencisi iken Cebir derslerini kendilerinden aldığım merhum Prof.Dr.Hülya ŞENKON ve akademik yolculuğumun her aşamasında,fikirlerinden yararlandığım Sayın Prof.Dr.Erhan GÜZEL hocalarıma şükranlarımı sunarım.

İstanbul, 2024 Didem ÖZTÜRK

İÇİNDEKİLER

Önsöz

1. Gruplar ve Temel Özellikleri

G boş kümeden farklı bir cümle olmak üzere bir $f: G \times G \rightarrow G$ fonksiyonu verilmiş olsun.

Bu taktirde, f fonksiyonuna, G kümesi üzerinde tanımlanmış bir ikili işlem veya bir **birleşim kuralı** denir.

$x, y \in G$ olmak üzere, (x, y) sırala ikilisinin f fonksiyonu altındaki görüntüsü, x ve y elemanlarının birleşim kuralı altında çarpımı olarak adlandırılır ve $x.y$ $(\boldsymbol{xy})$ ile gösterilir.

Aksi belirtilmedikçe, birleşim kuralı $\boldsymbol{''.''}$ notasyonu ile gösterilecektir. Özel olarak, birleşim kuralı **toplama** ise işlem $"+"$ ile ifade edilir. Bu durumda, (x, y) sıralı ikilisinin f fonksiyonu altındaki görüntüsü, x ve y elemanlarının **toplamıdı**r ve $\boldsymbol{x+y}$ ile belirtilir.

G kümesi ve onun üzerinde tanımlanmış bir $"."$ ikili işleminden oluşan cebirsel yapıyı,

$(G, .)$ ile göstereceğiz. G üzerinde $"."$ işleminin sağladığı özellikler dikkate alınarak,

$(G, .)$ cebirsel yapısı, **yarı grup, monoid, grup** olarak adlandırılır.

Tanım 1.1 G boş olmayan bir küme ve $"."$ bu küme içinde tanımlanmış bir ikili işlem olsun.

Eğer aşağıdaki şartlar sağlanıyorsa $(G, .)$ cebirsel yapısına **grup** denir.

i. **(Kapalılık Özelliği)** $\forall a, b \in G$ için $a.b \in G$ dir.

ii. **(Birleşme Özelliği)** $\forall a, b, c \in G$ için $a.(b.c) = (a.b).c$ dir.

iii. **(Birim Eleman)** $\exists e \in G,\ \forall a \in G$ için $a.e = e.a = a$ dır.

$\boldsymbol{e}$ elemanına grubun birim (etkisiz) elemanı denir.

iv. **(Ters Eleman Özelliği)** $\forall a \in G$ için $\exists b \in G$ vardır öyle ki $b.a = a.b = e$ dir.

b elemanına a nın tersi denir ve $\boldsymbol{b = a^{-1}}$ ile gösterilir.

Birim eleman çoğunlukla **1** ile temsil edilir. Eğer işlem toplama notasyonu ile veriliyorsa birim eleman, sıfır eleman adını alır ve **0** ile gösterilir. Bu durumda, bir a elemanının tersi yerine,

$\boldsymbol{a}$ elemanının zıddı ifadesi kullanılır ve $-\boldsymbol{a}$ ile gösterilir. Çoğu zaman, **"birleşme özelliği"** yerine de **"asosyatif özelliği"** ifadesi kullanılır.

Tanım 1.2: Tanım 1.1 de **i.** ve **ii.** şartları sağlıyorsa $(G,\ .)$ cebirsel yapısına **yarı grup** denir.

Tanım 1.3: Tanım 1.1 de **i.**, **ii.** ve **iii.** şartları sağlıyorsa $(G,\ .)$ cebirsel yapısına **monoid** denir.

Tanım 1.4: $(G,\ .)$ bir grup olmak üzere $\forall a,b \in G$ için $a.b = b.a$ ise bu gruba **değişmeli (komütatif veya abelyen*)* grup** denir.

Örnek 1.1: $(Z,+)$, $(Q,+)$, $(R,+)$, $(C,+)$, $(Q/\{0\},.)$, $(R/\{0\},.)$, $(C/\{0\},.)$ cebirsel yapıları birer abelyen gruptur.

Örnek 1.2: $(Z,\ .)$ cebirsel yapısı monoiddir.

Örnek 1.3: $\boldsymbol{n \in N\ ve\ n > 1}$ olmak üzere, $\forall\ \overline{a},\overline{b} \in \boldsymbol{Z_n}$ için $\overline{a} + \overline{b} = \overline{a+b}$ şeklinde tanımlanan kalan sınıflarının toplama işlemine göre ($\boldsymbol{Z_n}, +$) cebirsel yapısı bir abelyen gruptur.

Örnek 1.4: $\boldsymbol{n \in N\ ve\ n > 1}$ olmak üzere, $\forall\ \overline{a},\overline{b} \in \boldsymbol{Z_n}$ için $\overline{a}\ \boldsymbol{.}\ \overline{b} = \overline{a.b}$ şeklinde tanımlanan kalan sınıflarının çarpımı işlemine göre ($\boldsymbol{Z_n},.$) cebirsel yapısı bir monoiddir, grup değildir.

Örnek 1.5: $\boldsymbol{n \in N\ ve\ n > 1}$ olmak üzere, girdileri reel sayılar olan, n x n boyutlu matrislerin kümesi $\boldsymbol{M_n(R)}$, matrislerin toplama işlemine göre bir gruptur fakat matrislerin çarpımı işlemine göre bir grup değildir; çünkü her matrisin çarpma işlemine göre tersi yoktur.

1.1 Grup Özellikleri

Teorem 1.1.1: $(G,\ .)$ bir grup olsun. Buna göre,

- **i.** G nin birimi tektir.
- **ii.** $\forall a \in G$ için a^{-1} tek türlü belirlidir.
- **iii.** $\forall a,b,c \in G$ için

$a.b = a.c \Rightarrow b = c$ dir. (**sol taraftan kısaltma kuralı)**

$b.a = c.a \Rightarrow b = c$ dir. (**sağ taraftan kısaltma kuralı)**

İspat:

i. G grubunun e_1 ve e_2 gibi iki tane birim elemanının olduğunu varsayalım. O halde,

$$e_1.e_2 = e_2 \qquad \textbf{(1)}$$

e_2 birim eleman olduğundan,

$$e_2.e_1 = e_1 \qquad \textbf{(2)}$$

dir. **(1)** ve **(2)** den dolayı $e_1 = e_2$ elde edilir. Demek ki, G grubunun sadece bir tane birim elemanı vardır.

ii. $a \in G$ olsun. b ve c ise a nın ters elemanları ise,

$$a.b = e \qquad \textbf{(1)} \qquad \text{ve} \qquad c.a = e \qquad \textbf{(2)}$$

eşitlikleri sağlanır. Birleşme özelliği ve **(1), (2)** dikkate alındığında,

$$c = c.e = c.(a.b) = (c.a).b = e.b = b \Rightarrow c = b$$

sonucuna varılır. O halde, a nın tersi tek türlü belirlidir.

iii. $\forall a, b, c \in G$ için $a.b = a.c$ ise eşitliğin her iki tarafı sol taraftan a^{-1} ile çarpıldığında, $a^{-1}.(a.b) = a^{-1}.(a.c)$, $a^{-1}.a = e$ olduğundan,

$$e.b = e.c \quad \text{ve} \quad b = c$$

elde edilir. Sağ taraftan kısaltma kuralı da benzer şekilde ispat edilebilir.

Teorem 1.1.2: $(G, \ .)$ bir grup olsun. $\forall a, b, c, x, y \in G$ için $a.x = b$ ve $y.a = b$ denklemlerinin çözümü tek türlü belirlidir.

İspat:

Öncelikle , $a.x = b$ **(1)** denkleminin her iki tarafı sol taraftan a^{-1} ile çarpılsın. Bu durumda,

$$a^{-1}.(a.x) = a^{-1}.b$$

$$e.x = a^{-1}.b$$

$$x = a^{-1}.b \in G$$

(1) denkleminin çözümüdür.

(1) denkleminin, x_1 ve x_2 gibi iki çözümünün olduğunu kabul edelim. O halde,

$$a.x_1 = b \ , \ a.x_2 = b$$

$$a.x_1 = a.x_2 \quad \textbf{(3)}$$

elde edilir. Sol taraftan kısaltma kuralı gereğince **(3)** den,

$$x_1 = x_2$$

sonucuna varılır. Bu da çözümün tekliğini gösterir.

Tanım 1.1.1 G bir grup, $a_1, a_2, \dots, a_k \in G$; $k \geq 2$ olsun. Bu durumda $k = 2$ için $a_1 . a_2$ çarpımı zaten tanımlanmıştır.

$k > 2$ için $a_1 . a_2 . \dots . a_{k-1}$ çarpımı tanımlanmış ise $a_1 . a_2 . \dots . a_k$ çarpımı

$$a_1 . a_2 . \dots . a_k = (a_1 . a_2 . \dots . a_{k-1}) a_k$$

biçiminde tanımlanır. Böylece tümevarım yöntemiyle her $n \in N$ için $a_1 . a_2 . \dots . a_n$ çarpımı tanımlanmış olur. Burada kısaca, $k \geq 2$

$$a_1 . a_2 . \dots . a_n = \prod_{i=1}^{n} a_i$$

yazılır.

Bu durumda bir grupta alınan herhangi n $(n \geq 3)$ eleman için aşağıdaki **genel birleşme kuralının** geçerli olduğu kolayca (tümevarım yöntemiyle) ispatlanır:

$$a_1 . a_2 . \dots . a_k . a_{\mathrm{k}} . \dots . a_n = (a_1 . a_2 . \dots . a_{k-1})(a_{\mathrm{k}} . a_{k+1} . \dots . a_n) \qquad (1 \leq k \leq n-1)$$

Öte yandan $a_1 . a_2 . \dots . a_n$ $(n \geq 2)$ elemanları ikişer ikişer komütatif elemanlar ise, bunların çarpımında **genel komütatif kuralın** sağlandığı da kolayca (tümevarım yöntemiyle) ispatlanır; yani $1,2,3, \dots, n$ nin herhangi bir permütasyonu $i_1 . i_2 . \dots . i_n$ ise,

$$a_1 . a_2 . \dots . a_n = a_{i_1} . a_{i_2} . \dots . a_{i_n}$$

dir. Buna göre, $a_1 . a_2 . \dots . a_n$ çarpımının çarpanlarını, aşağıdaki gibi istediğimiz sırada ve sayıda paranteze alabiliriz:

$$a_1 . a_2 . \dots . a_n = \left(a_{i_1} . a_{i_2} . \dots . a_{i_n}\right)\left(a_{i_{k+1}} . a_{i_{k+2}} . \dots . a_{i_t}\right) \dots \left(a_{i_m} . a_{i_{m+1}} . \dots . a_{i_n}\right)$$

Teorem 1.1.3: $(G,\ .)$ bir grup ve $a, b\ \in G$ ise $(a.b)^{-1} = b^{-1}.a^{-1}$ dir.

İspat:

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

ve benzer şekilde

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

elde edilir. Bu iki eşitlikten,

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

sonucuna varılır. Öyleyse ters eleman tanımından, $(a.b)$ nin tersinin, $b^{-1}.a^{-1}$ olduğunu söyleyebiliriz;

$$(a.b)^{-1} = b^{-1}.a^{-1}$$

dir.

Genelleştirme 1.1.1: $a_1, a_2, \dots, a_k \in G$ olmak üzere, $(a_1, a_2, \dots, a_k)^{-1} = {a_k}^{-1}. \dots .{a_2}^{-1}.{a_1}^{-1}$ $(k \geq 2)$ dir.

Tanım 1.1.2: $(G,\ .)$ bir grup olmak üzere, $n \in Z^+ \cup \{0\}$ için $a \in G$ nin kuvvetleri,

$$a^n = a.a. \dots .a \qquad \text{(n tane çarpan)}$$

$$a^0 = e$$

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

şeklinde ifade edilir ve $\boldsymbol{a}$ **nın** $\boldsymbol{n}$**.inci kuvveti** olarak adlandırılır.

Not 1.1.1: Tanım 1.1.2 deki ikili işlem toplama işlemi ise,

$$na = a + a + \ldots + a \quad \text{(n tane a nın toplamı)}$$

$$0a = e$$

$$(-n)a = n(-a)$$

şeklinde ifade edilir ve **a nın n katı** olarak adlandırılır.

Teorem 1.1.4: $(G,\ .)$ bir grup, $a \in G$ ve $m, n \in Z$ olmak üzere a nın kuvvetleri için aşağıdaki eşitlikler geçerlidir.

- **i.** $a^m.a^n = a^{m+n} = a^n.a^m$ dir.
- **ii.** $(a^m)^n = a^{m.n} = (a^n)^m$ dir.
- **iii.** $a^{-m} = (a^m)^{-1}$ dir.
- **iv.** $e^m = e$ dir.
- **v.** $a, b \in G$ için $(a.b) = (b.a)$ ise $\forall n \in Z$ için $(a.b)^n = a^n.a^n$ dir.

Genelleştirme 1.1.2: $a^{m_1}.a^{m_2}.\ldots.a^{m_k} = a^{m_1+m_2+\cdots+m_k}$ $(k \geq 2, m_1, m_2, \ldots, m_k \in Z)$ dir.

Genelleştirme 1.1.3: $a_1.a_2.\ldots.a_k$ $(k \geq 2)$ G nin ikişer ikişer komütatif elemanları ise $\forall n \in Z$ için $(a_1.a_2.\ldots.a_k)^n = {a_1}^n.{a_2}^n.\ldots.{a_k}^n$ dir.

Not 1.1.2: Kuvvet tanımı ve özellikleri dikkate alınarak, benzer şekilde kat kavramının temel özelliklerini elde etmek kolaydır.

Alıştırmalar I

1) Bir G grubunda her $a \in G$ için $a^2 = 1_G$ ise G nin komütatif bir grup olduğunu gösteriniz.

2) Mertebesi çift olan bir grupta birimden başka, tersi kendisine eşit olan en az bir elemanın daha bulunduğunu gösteriniz.

3) Bir G grubunda her $a, b \in G$ için $(ab)^2 = a^2 b^2$ ise G nin komütatif bir grup olduğunu gösteriniz.

4) $G = Z \times Z = \{(a, b) \mid a, b \in Z\}$ kümesinin $(a, b).(c, d) = (a + c, (-1)^c(b + d))$ biçiminde tanımlanan "∗" işlemine göre ne tür bir grup olduğunu gösteriniz.

5) a, b, c, d bir G grubunun elemanları olmak üzere,

$a^5 = b^4 = c^6 = 1, ab = ba^3, dc = c^4d \quad ise$

$a^2b = ba, ab^3 = b^3a^2, \ c^3 = 1 \ , cd = dc$ olduğunu gösteriniz.

6) $\omega^3 = 1, \omega \neq 1$ olmak üzere,

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, C = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix},$$

$$D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, E = \begin{pmatrix} 0 & \omega^2 \\ \omega & 0 \end{pmatrix}, F = \begin{pmatrix} 0 & \omega \\ \omega^2 & 0 \end{pmatrix}$$

Matrislerinden oluşan kümenin, matris çarpımına göre bir grup olduğunu gösteriniz.

7) $G = \{3^m 5^n \mid m, n \in Z \}$ kümesinin Q daki çarpma işlemine göre bir grup olduğunu gösteriniz.

2. Alt Gruplar

Tanım 2.1: $(G,\ .)$ bir grup, $H \neq \emptyset$ ve $H \subseteq G$ olsun. H , G de tanımlanan '.' işlemine göre grup ise $(H,\ .)$ cebirsel yapısı, $(G,\ .)$ nin bir **alt grubu**dur denir ve $H \leq G$ ile gösterilir.

Tanım 2.2: G ve $\{1_G\}$ ye G nin triviyal alt grupları denir. G nin triviyal olmayan bir alt grubuna ise bir has alt grubu denir. $\{\mathbf{1_G}\}$ yerine { **e** } gösterimini kullanabileceğimizi biliyoruz, bu şekilde ifade edilen grup, **birim grup** olarak adlandırılır.

Teorem 2.1: $(G,\ .)$ bir grup olsun. $H \neq \emptyset$ ve $H \subseteq G$ olsun. Buna göre $H \leq G$ olması için gerek ve yeter şart,

- **i.** $\forall a, b\ \in H$ için $a.b \in H$,
- **ii.** $\forall a, b\ \in H$ için $a^{-1} \in H$ olmasıdır.

İspat:

(⇒):

$H \leq G$ olsun. Bu durumda, kapalılık ve ters elemanın varlığı aksiyomlarından, **i.** ve **ii.** şartlarının sağlandığı görülür.

(⇐):

Şimdi ise **i.** ve **ii.** şartlarının doğru olduğu kabul edilerek, $(H,\ .)$ nın bir grup olduğu ispat edilecektir; **i**. ve **ii**. şartlarının sağlanması demek, grup aksiyomlarından, kapalılık ve ters elemanın varlığı koşullarının gerçeklenmesi demektir. $(H,\ .)$ nın grup olması için birim elemanı içerdiği ve asosyatif özelliğini sağladığı da görülmelidir. $(G,\ .)$ grup olduğundan, '.' işlemi birleşme özelliğini gerçekler. $H \subseteq G$ ise, H da "." işlemi assosyatifdir.

Öte yandan, **ii.** den $a \in H\ ise\ a^{-1} \in H$ ve **i.** den dolayı,

$$e = a.a^{-1} \in H$$

dır. Bu da, H alt grubunun birim elemanı içerdiği sonucunu ortaya koyar. **Teorem 2.1** de verilen iki şartı birleştirerek, aşağıdaki teoremi yazabiliriz;

Teorem 2.2: $(G,\ .)$ bir grup, $H \neq \emptyset$ ve $H \subseteq G$ olsun. Buna göre $H \leq G$ olması için gerek ve yeter koşul, $\forall a, b\ \in H$ için

$$a.b^{-1} \in H$$

olmasıdır.

İspat:

$(\Rightarrow)$:

$H \leq G$ olsun. $(H,\ .)$ bir grup ise $b \in H$ için $b^{-1} \in H$ dır. Kapalılık aksiyomundan, $a \in H$ ve $b^{-1} \in H$ için

$$a.b^{-1} \in H$$

elde edilir.

$(\Leftarrow)$:

$\forall a, b\ \in H$ için $a.b^{-1} \in H$ olsun. Bu durumda, bir a $\in H$ için $a.a^{-1} = e\ \in H$ dır.

Diğer yandan, $e, b \in H$ için hipotez gereği, $e.b^{-1} = b^{-1} \in H$ elde edilir.

Üstelik, $b^{-1} \in H$ ve $(b^{-1})^{-1} = b$ olduğundan,

$$a.(b^{-1})^{-1} = a.b \in H$$

dır. Dikkat edilirse, **Teorem 2.1** den $H \leq G$ olduğu görülür.

Teorem 2.3: $(G,\ .)$ bir grup, $H \neq \emptyset$ ve H, G nin sonlu bir alt kümesi olsun. Bu durumda, H kümesi, G deki "$.$" işlemine göre kapalı ise $H \leq G$ dir.

İspat:

Kapalılık şartı hipotezde verildiğinden, **Teorem 2.1 i.** şartı sağlanır. O halde, **Teorem 2.1 ii.** şartının da sağlandığı gösterilirse, **Teorem 2.1** gereği $H \leq G$ olur.

Öncelikle, $a \in H$ için $a^{-1} \in H$ olduğu ispat edilmelidir;

Burada iki durum söz konusudur:

i. e birim eleman olmak üzere $a = e$ ise $a^{-1} \in H$ olur ve istenilen sağlanır.

ii. Şimdi $a \neq e$ olduğunu kabul edelim. Hipotezden H daki işlem kapalı olduğundan, a nın bütün pozitif kuvvetleri H da olmak zorundadır. Fakat H sonlu olduğundan $a, a^2, \dots, a^m, \dots$ elemanlarının hepsi birbirinden farklı olamaz.

O halde, $0 < i < j$ tamsayıları için $a^j = a^i$ dir. Grupta kısaltma kuralından,

$a^{j-i} = e$ elde edilir. Öte yandan, $a \neq e$ olarak alındığından, $j - i > 1$ dolayısıyla,

$j - i > 0$ ve $a^{j-i-1} = a^{-1} \in H$ dir.

Böylece, **Teorem 2.1** den , $H \leq G$ sonucuna varılır.

Sonuç 2.1: G bir toplam grubu ise, G grubunun, boş olmayan bir H alt kümesinin, G nin bir alt grubu olması için gerek ve yeter koşul, $\forall a, b \in H$ için a-b ∈ H olmasıdır.

Örnek 2.1: $Z_{11} - \{\overline{0}\}$ de $A = \{\overline{1}, \overline{8}\}$, $B = \{\overline{1}, \overline{10}\}$, $C = \{\overline{1}, \overline{3}, \overline{10}\}$ ve $D = \{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}$ alt kümelerinin çarpma işlemine göre birer alt grup olup olmadıklarını kontrol edelim. Kümeler sonlu olduğundan, sadece çarpma işlemine göre kapalı olup olmadıklarını kontrol etmek yeterlidir.

Buna göre,

$\overline{8}^2 = \overline{9} \notin A$ olduğundan, A kümesi $Z_{11} - \{\overline{0}\}$ in bir alt grubu değildir.

$\overline{10}^2 = \overline{1} \in B$ olduğundan B kümesi $Z_{11} - \{\overline{0}\}$ in bir alt grubudur.

$\overline{3}^2 = \overline{9} \notin C$ olduğundan, C kümesi $Z_{11} - \{\overline{0}\}$ in bir alt grubu değildir.

$\overline{3}^2 = \overline{9} \in D, \overline{3}\,\overline{4} = \overline{1} \in D,\ \overline{3}\,\overline{5} = \overline{4} \in D, \overline{3}\,\overline{9} = \overline{5} \in D, \overline{4}^2 = \overline{5} \in D, \overline{4}\,\overline{5} = \overline{9} \in D, \overline{4}\,\overline{9} = \overline{3} \in D,$

$\overline{5}^2 = \overline{3} \in D, \overline{5}\,\overline{9} = \overline{1} \in D, \overline{9}^2 = \overline{4} \in D$ olduğundan, D kümesi $Z_{11} - \{\overline{0}\}$ in bir alt grubudur.

Örnek 2.2 : $(G,\ .)$ bir grup, $H \leq G$ ve $K \leq G$ ise bu durumda, $H \cap K \leq G$ olduğunu gösterelim;

$a, b \in H \cap K$ ise $a, b \in H$ ve $a, b \in K$ dır. $H \leq G$ olduğundan, $a, b \in H$ için $a.b^{-1} \in H$ dır.

Benzer şekilde, $K \leq G$ olduğundan, $a, b \in K$ için $a.b^{-1} \in K$ elde edilir.

Böylece, $a.b^{-1} \in H \cap K$ olur ki bu da, **Teorem 2.2** den, $H \cap K \leq G$ sonucunu doğurur.

Sonuç 2.2: $(G,\ .)$ bir grup ve $H_1, H_2, \ldots H_n$, G nin n tane alt grubu olmak üzere,

$$\bigcap_{i=1}^{n} H_i \leq G$$

dir.

Sonuç 2.2 nin ispatı bir sonraki bölümde ayrıntılı olarak ele alınacaktır.

2.1 Kümelerin Çarpımı

Tanım 2.1.1: $(G,\ .)$ bir grup ve $A, B \subset G$ olsun. Bu durumda, $AB = \{ab: a \in A, b \in B\}$ kümesine A ve B **kümelerinin bu sıradaki çarpımı** denir.

Özel olarak, $A = \{a\}$ ise $AB = \{ab: a \in A, b \in B\} = \{a\}B = aB$ ile gösterilir.

Benzer tanımı, A ve B kümelerinin toplamı için $A + B = \{a + b: a \in A, b \in B\}$ şeklinde verebiliriz.

Bir G grubunun, boş kümeden farklı $A, B \subset G$ alt kümelerine, G nin **kompleksleri** adı verilir. Dolayısıyla, **kümelerin çarpımı (toplamı)** yerine, **komplekslerin çarpımı (toplamı)** ifadesi de kullanılabilir.

2.2 Grup ve Mertebe

Tanım 2.2.1: Sonlu sayıda elemanı bulunan bir gruba sonlu bir grup denir. Sonlu olmayan bir gruba sonsuz bir grup denir. G sonlu bir grup ve eleman sayısı n ise n ye G grubunun mertebesi denir ve $|G| = n$ yazılır. Sonsuz bir grubun mertebesi de sonsuz olarak tanımlanır.
e, G nin birim elemanı ve $g \in G$ olmak üzere, $g^n = e$ olacak şekilde $n \in Z^+$ tamsayısı varsa;

g elemanına, **sonlu mertebedendir** denir. $g^n = e$ olacak şekilde $n \in Z^+$ yoksa; g elemanına, **sonsuz mertebedendir** denir. $g \in G$ sonlu mertebeden olmak üzere, $g^n = e$ eşitliğini gerçekleyen en küçük pozitif n tam sayısına, g nin **mertebesi** denir ve $\boldsymbol{O(g)}$ ya da $|\boldsymbol{g}|$ ile gösterilir.

Not 2.1.1: Eğer sözü edilen cebirsel yapı, çarpma işlemine göre değil de toplama işlemine göre bir grup ise $g^n = e$ yerine $ng = e$ olacak şekilde en küçük n pozitif tam sayısı araştırılacaktır.

Örnek 2.2.1: G değişmeli bir grup olsun. G nin sonlu mertebeden elemanlarının kümesinin,

G nin bir alt grubu olduğunu gösterelim;

G nin çarpma işlemine göre bir grup ve H, G nin sonlu mertebeden elemanlarının kümesi olsun.
e, G nin birim elemanı olmak üzere, $H = \{a \in G: a^n = e, n \in Z^+\}$ şeklinde tanımlanır.

$\forall a, b \in H$ için $a^{-1}b \in H$ ise **Teorem 2.2** gereğince $H \leq G$ dir.

Şimdi, a nın mertebesi m ve b nin mertebesinin de n olduğunu kabul edelim.

$O(a) = m$ $(a^m = e)$ ve $O(b) = n$ $(b^n = e)$ yazabiliriz. Bu durumda,

$$
\begin{aligned}
(a.b^{-1})^{mn} &= (ab^{-1})(ab^{-1}) \dots (ab^{-1}) && (mn \text{ tane çarpan}) \\
&= (aa \dots a)(b^{-1}b^{-1} \dots b^{-1}) && (G \text{ değişmeli olduğundan}) \\
&= a^{mn}b^{-mn} \\
&= (a^m)^n(b^n)^{-m} \\
&= e^n.e^{-m} \\
&= e
\end{aligned}
$$

elde edilir. Bu da, ab^{-1} elemanını sonlu mertebeden olduğunu yani $ab^{-1} \in H$ olduğunu gösterir.

Örnek 2.2.2: $< G, . >$ bir grup, $a \in G$ olsun.

a nın herhangi bir kuvvetinin mertebesinin, a nın mertebesinden büyük olamayacağını gösterelim;

$|a| = k, t \in Z$ için a^t= b olsun,

$$b^k = (a^t)^k = (a^k)^t = 1 \Rightarrow |b| \mid k \Rightarrow |a^t| \mid k \Rightarrow |a^t| \leq k$$

elde edilir.

Örnek 2.2.3: $< G, . >$ bir grup $a \in G$ olsun. Bu taktirde, $|a| = |a^{-1}|$ dir.

Yani,

$$|a| = k, |a^{-1}| = t \Rightarrow k = t \text{ dir:}$$

$$(a^{-1})^k = (a^k)^{-1} = 1 \Rightarrow \boldsymbol{t} \mid \boldsymbol{k} \quad \ldots\ldots (*),$$

$$(a^{-1})^k = 1 \Rightarrow at = 1 \Rightarrow \boldsymbol{k} \mid \boldsymbol{t} \quad \ldots\ldots (**) \text{ dir.}$$

$(*)$ ve $(**)$ dan $\mathbf{t} = \mathbf{k}$ elde edilir.

Alıştırmalar II

1) Bir G grubunun bütün elemanlarıyla komütatif olan elemanlarının kümesinin, G nin bir grubu olduğunu gösteriniz.

2) G bir grup ve $a \in G$ olsun. G, a elemanıyla komütatif olan bütün elemanlarının kümesinin, G nin bir alt grubu olduğunu gösteriniz.

3)

i. 2×2 regüler reel girdili matrislerin, matrislerin çarpma işlemine bir grup olduğunu gösteriniz.

ii. $G = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}\}$ kümesinin, 2×2 regüler reel girdili matrislerin çarpım grubunun bir alt grubu olduğunu gösteriniz.

4) $G = \{1, -1, i, -i\}$ kümesinin çarpma işlemine göre komütatif bir grup olduğunu gösteriniz.

5) Mutlak değerleri (modülleri) 1 olan kompleks sayılardan oluşan kümenin, C deki çarpma işlemine göre bir grup olduğunu gösteriniz.

6) *H* ve *K* bir *G* grubunun iki alt grubu ise $H \cup K$ ve $H \cap K$ kümeleri, *G* nin birer alt grubu mudur?.

7) $\boldsymbol{i}$. Bir A kümesinin kendi üzerine (1-1) bütün tasvirlerinin kümesi $S(A)$ nın, tasvirlerin çarpma işlemine göre bir grup olduğunu gösteriniz.

$\boldsymbol{ii}$. Bir $a \epsilon A$ için, $G = \{f \in S(A) | f(a) = a\} < S(A)$ olduğunu gösteriniz.

3.Devresel Gruplar

Teorem 3.1.1: Bir grubun sonlu ya da sonsuz sayıda bir takım alt gruplarının arakesiti de G nin bir alt grubudur.

İspat:

İ sonlu yada sonsuz bir indeks kümesi olmak üzere, G nin H_i $(i \in \text{İ})$ alt gruplarını ele alalım ve

$$K = \bigcap_{i=1} H_i$$

olsun.

Her i için $1_G \in H_i$ olduğundan, $1_G \in K$ dır. Buna göre $K \neq \emptyset$ dır. Öte yandan, her $a, b \in K$ için, arakesit tanımına göre, her $i \in \text{İ}$ için $a, b \in H_i$ dir. Burada her $i \in \text{İ}$ için $H_i \leq G$ olduğundan, her $i \in \text{İ}$ için $ab^{-1} \in H_i$ dir. Böylece, $ab^{-1} \in$ K elde edilir. O halde, $K \leq G$ olmak zorundadır.

Tanım 3.1.1: G bir grup ve M, G nin boş olmayan bir alt kümesi olsun. G nin M yi kapsayan bütün alt gruplarının arakesitine, G nin M tarafından doğurulmuş alt grubu denir ve $< M >$ ile gösterilir. M nin elemanlarına $< M >$ alt grubun **doğurayları** adı verilir. M kümesi sonlu ise $< M >$ **sonlu doğurulmuştur** (**sonlu doğuraylıdır**) denir.

$$< M >= \bigcap_{M \subset H \leq G} H$$

şeklinde ifade edilir. $M = \{a\}$ ise $< M >= < a >$ yazılır. $< M > = G$ ise M nin elemanlarına, G nin **doğurayları** adı verilir ve G grubu M nin elemanları tarafından **doğurulmuştur** denir.

Teorem 3.1.2: $< M >$ alt grubu, G nin M yi kapsayan en küçük alt grubudur.

İspat:

$T < G$ ve $M \subset T$ ise $< M > \subset T$ olmak zorundadır. Bu da ispatı bitirir.

Not 3.1.1: $< M >$ alt grubu, G nin M alt kümesini kapsayan en küçük alt grubu olarak da tanımlanabilir.

Tanım 3.1.2: Bir G grubun $a_1, a_2, \ldots, a_k$ gibi sonlu sayıda elemanı ile oluşturulan, ${a_1}^{m_1}.{a_2}^{m_2}.\ldots.{a_k}^{m_k}$ $(m_1, m_2, \ldots, m_k \in Z)$ biçimindeki bir çarpımına, $a_1, a_2, \ldots, a_k$ elemanlarının bir **kuvvet çarpanı** denir.

Teorem 3.5.3: G nin $< M >$ alt grubu, M nin elemanlarının bütün kuvvet çarpımlarından oluşan kümeye eşittir.

İspat:

M nin elemanlarının bütün kuvvet çarpımlarından oluşan kümeyi K ile gösterelim. Bu durumda, her $\alpha, \beta \in K$, $\alpha = {a_1}^{m_1}.{a_2}^{m_2}.\ldots.{a_k}^{m_k}$, $\beta = {b_1}^{n_1}.{b_2}^{n_2}.\ldots.{b_t}^{n_t}$ için

$$\alpha\beta^{-1} = ({a_1}^{m_1}.{a_2}^{m_2}.\ldots.{a_k}^{m_k}).({b_1}^{n_1}.{b_2}^{n_2}.\ldots.{b_t}^{n_t})^{-1} = {a_1}^{m_1}.{a_2}^{m_2}.\ldots.{a_k}^{m_k}{b_t}^{-n_t}.\ldots.{b_2}^{-n_2}{b_1}^{-n_1} \in K$$

olduğundan, $K \leq G$ dir. Burada M nin her a elemanı, a^1 biçiminde bir kuvvet çarpanı olarak düşünülebileceğinden, $M \subset K$ dır.

Tersine, her $\alpha \in K$, ${a_1}^{m_1}.{a_2}^{m_2}.\ldots.{a_k}^{m_k}$ için $a_1, a_2, \ldots, a_k \in M \subset < M >$ ve $< M >$ bir grup olduğundan, $\alpha = {a_1}^{m_1}.{a_2}^{m_2}.\ldots.{a_k}^{m_k} \in < M >$ yani $K \subset < M >$ dir.

O halde, $< M > = K$ olmak zorundadır.

Tanım 3.1.3: Bir tek eleman tarafından doğurulan bir gruba **devresel grup** denir.

Buna göre, bir a elemanı tarafından doğurulan G devresel grubu,

$$G = < a > = \{\ldots, a^{-n}, \ldots, a^{-1}, a^0 = 1_G, a, \ldots, a^n, \ldots\} = \{a^n \mid n \in Z\}$$

şeklindedir. G bir toplam grubu olarak alınırsa, a nın doğurduğu devresel grup ise,

$< a > = \{na \mid n \in Z\}$ biçimindedir.

Not 3.5.1: Bir grupta, kuvvetlerin temel özellikleri ve Z de toplama işleminin komütatifliği dikkate alındığında, $a^n a^m = a^{n+m} = a^{m+n} = a^m a^n$ olduğundan, **devresel gruplar da komütatifdir**.

Bir $G =< a >$ devresel grubu için iki hal söz konusudur:

i. a nın bütün kuvvetleri birbirinden farklıdır. Bu durumda, G sonsuz bir devresel gruptur.

ii. a nın bazı kuvvetleri aynıdır. Eğer $r > s$ tam sayıları için $a^r = a^s$ ise kısaltma özelliğinden $a^{r-s} = 1_G$ elde edilir. Bu durumda, en küçük eleman prensibine göre, $a^t = 1_G$ koşuluna uyan t doğal sayılarının bir en küçüğü vardır. Bu doğal sayıyı τ ile gösterelim. Bu durumda, $\{1_G, a, a^2, \dots, a^{\tau-1}\}$ kümesinin elemanları birbirinden farklıdır ve $\{1_G, a, a^2, \dots, a^{\tau-1}\} \subset < a >$ dır. Öte yandan, her $a^n \in < a >$ için n, τ çiftine ait bölme algoritmesi

$$n = \tau q + r, 0 \leq r \leq \tau - 1$$

biçiminde ise,

$$a^n = a^{\tau q + r} = (a^\tau)^q a^r = (1_G)^q a^r = a^r, \qquad 0 \leq r \leq \tau - 1$$

elde edilir. Yani

$$< a > \subset \{1_G, a, a^2, \dots, a^{\tau-1}\}$$

dir. Buna göre,

$$< a >= \{1_G, a, a^2, \dots, a^{\tau-1}\}$$

olmak zorundadır.

Örnek 3.1.1: $< Z, + >$ grubunda, $5 \in Z$ nin doğurduğu devresel grup,

$< 5 > = 5Z = \{5k \mid k \in Z\}$ şeklinde ifade edilir.

Tanım 3.1.4: G sonlu bir grup ve $a \in G$ ise, a nın G içinde doğurduğu devresel grubun mertebesine, başka bir değişle $a^t = 1_G$ koşuluna uyan t doğal sayılarının en küçüğüne,

$\boldsymbol{a}$ **elemanının (**$\boldsymbol{G}$ **grubundaki)** mertebesi denir ve $|\boldsymbol{a}|$ (ya da $|\boldsymbol{a_G}|$) şeklinde gösterilir.

Örnek 3.1.3: $< Z, + > = < 1 >$ olduğundan, $< Z, + >$ sonsuz bir devresel gruptur.

Örnek 3.1.4: $Z_{13} - \{\overline{0}\}$ çarpım grubunda,

$$\overline{5}^0 = \overline{1}, \overline{5}^1 = \overline{5}, \overline{5}^2 = \overline{-1},\ \overline{5}^3 = \overline{-5},\ \overline{5}^4 = \overline{1}$$

olduğundan, $\overline{5}$ tarafından doğurulan alt grup, $< \overline{5} > = \{1, \overline{5}, \overline{-1}, \overline{-5}\}$ dir. Öte yandan,

$$\overline{2}^2 = \overline{4}, \overline{2}^3 = \overline{-5}, \overline{2}^4 = \overline{3},\ \overline{2}^5 = \overline{6},\ \overline{2}^6 = \overline{-1},\ \overline{2}^7 = \overline{1},\ \overline{2}^8 = \overline{-4},\ \overline{2}^9 = \overline{5},\ \overline{2}^{10} = \overline{-3},\ \overline{2}^{11} = \overline{-6},\ \overline{2}^{12} = \overline{1}$$

kuvvetleri dikkate alındığında,

$$< \overline{2} > = \{\pm\overline{1}, \pm\overline{2}, \pm\overline{3}, \pm\overline{4}, \pm\overline{5}, \pm\overline{6}\} = Z_{13} - \{\overline{0}\}$$

elde edilir. Yani, $Z_{13} - \{\overline{0}\}$ grubu $\overline{2}$ elemanı tarafından doğurulmuştur. Ancak, Z_{13} toplam grubu $\overline{1}$ tarafından doğurulmuş, 13 elemanlı bir gruptur. Genel olarak, Z_m toplam grubu $\overline{1}$ tarafından doğurulmuş, m elemanlı bir devresel gruptur diyebiliriz.

Örnek 3.1.6: $a\ ve\ b$, herhangi bir grubun mertebeleri sonlu olan elemanları ise ab elemanının mertebesinin sonlu olması gerekmez. Örneğin, reel sayılar üzerinde tanımlı 2×2 regüler matrislerin grubu, komütatif olmayan bir gruptur ve bu gruptan alınan

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

elemanları için, $|A| = |B| = 3$ olmasına rağmen,

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

matrisinin mertebesi sonsuzdur, çünkü her $k \in N$ için

$$(AB)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

dir.

Teorem 3.1.4: Bir $G = \{1_G, a, a^2, \dots, a^{\tau-1}\}$ devresel grubunda aşağıdaki özellikler geçerlidir:

- **i.** $s \in Z$ olmak üzere $a^s = 1_G \Leftrightarrow \tau | s$ dir.
- **ii.** $m, n \in Z$ olmak üzere $a^m = a^n \Leftrightarrow m \equiv n(\tau)$ dır.

İspat:

i.

($\Leftarrow$):

$\tau | s$ ise $s = s'\tau$ $(s' \in Z)$ dir. Burada kuvvetlerin temel özelliklerine göre,

$a^s = a^{\tau s'} = (a^\tau)^{s'}$ yazılabilir ve $a^\tau = 1_G$ olduğundan $a^s = (1_G)^{s'} = 1_G$ elde edilir.

($\Rightarrow$):

$a^s = 1_G$ olsun. s ve τ çiftine ait bölme algoritmesi

$$s = \tau q + r, \;\; 0 \leq r < \tau - 1$$

biçiminde ise kuvvetlerin temel özelliklerine göre, $a^s = (a^\tau)^q a^r = a^r = 1_G$ elde edilir.

Dikkat edilirse, τ nın tanımından dolayı $r \neq 0$ olamaz. Buna göre $s = \tau q$, yani $\tau | s$ dir.

ii.
$m, n \in Z$ olmak üzere,

$$a^m = a^n \Leftrightarrow a^{m-n} \equiv 1_G$$

dir. Öte yandan **i.** ye göre,

$$a^{m-n} = 1_G \Leftrightarrow \tau | m - n$$

dir ve kongrüans tanımına göre ise

$$\tau | m - n \Leftrightarrow m \equiv n(\tau)$$

elde edilir, yani $a^m = a^n \Leftrightarrow m \equiv n(\tau)$ dir.

Teorem 3.1.5: Bir devresel grubun her alt grubu da devreseldir.

İspat:

$G = < a >$ ve $H \leq G$ olsun. $H = \{1_G\}$ ise H devreseldir. $H \neq \{1_G\}$ ise H da en az bir a^m $(m \in Z, m \neq 0)$ elemanı vardır ve $H \leq G$ olduğundan $a^m \in H$ dir. Bu durumda, en küçük eleman prensibine göre, $a^t \in H$ koşuluna uyan $\boldsymbol{t}$ doğal sayılarının bir en küçüğü vardır.

Bu doğal sayı $\boldsymbol{\tau}$ ise, $\boldsymbol{a^\tau} \in H$ dır. Öte yandan $a^s \in H$ herhangi bir eleman ise, s ve τ çiftine ait bölme algoritmesi

$$s = \tau q + r, \ \ 0 \leq r < \tau - 1$$

biçiminde yazılırsa,

$$a^s = (a^\tau)^q a^r \Rightarrow a^r = (a^\tau)^{-q} a^s \in H$$

elde edilir. Fakat $0 \leq r < \tau - 1$ olması, τ nın tanımıyla çelişir. Buna göre, $r = 0$, $s = \tau q$ olmalıdır. Burada $a^s = (a^\tau)^q \in < a >$, yani $H \subset < a^\tau >$ bulunur. O halde, $H = < a^\tau >$ olmak zorundadır.

Teorem 3.1.6:

i. Bir sonsuz devresel grubun $\{1_G\}$ den farklı her alt grubu da bir sonsuz devresel gruptur.

ii. $G = < a >$, s. mertebeden bir devresel grup ve $H = < a^\tau >$ $(\tau > 0)$, G nin bir alt grubu ise uygun bir $q \in N$ ise $s = \tau q$ ve $|H| = q$ ve $|H| \mid |G|$ dır.

İspat:

i. $G = < a >$ bir sonsuz devresel grup ve $H \leq G$; $H \neq \{1_G\}$ olsun. **Teorem 3.1.5** e göre, uygun bir $\tau \in N$ için $H = < a^\tau >$ dır. a nın, dolayısıyla a^τ nun bütün kuvvetleri birbirinden farklı olduğundan H bir sonsuz devresel gruptur.

ii. $G = \{1_G, a, a^2, \dots, a^{s-1}\}$ olsun. $H = < a^\tau >$ olduğundan, **Teorem 3.1.5** e göre τ, $a^t \in H$ koşuluna uyan t doğan sayılarının en küçüğüdür. Burada s ve τ çiftine ait bölme algoritmesi

$$s = \tau q + r, \quad 0 \leq r < \tau - 1$$

biçiminde yazılır.

$$a^s = (a^\tau)^q a^r = 1_G \Rightarrow (a^\tau)^{-q} = a^r \in H$$

elde edilir. Öte yandan, τ nın tanımına göre, $r = 0$ yani $s = \tau q$ olmak zorundadır. Burada s, $a^s = 1_G$ koşuluna uyan en küçük doğal sayı olduğundan, $(a^\tau)^q = 1_G$ koşuluna uyan en küçük doğal sayı da q olmalıdır. Buna göre, $|H| = q$ ve $|H| \mid |G|$ dir.

Teorem 3.1.7: $G = < a >$, s. mertebeden bir devresel grup ise s nin her q bölenine karşılık G nin q. mertebeden bir ve yalnız bir tane alt grubu vardır.

İspat:

$q|s$ ise $s = \tau q$ olacak biçimde τ tam sayısı tek türlü belirlidir. **Teorem 3.1.6** da anlatıldığı gibi $< a^{\tau} >$ alt grubunun mertebesi q dır ve $\tau = \frac{s}{q}$ olarak tek türlü belirlidir.

Buna göre, $< a^{\tau} >$ alt grubu bir ve yalnız bir tanedir.

Teorem 3.1.8: $G =< a >$, s. mertebeden bir devresel grup ise, a^m elemanının, G nin bir doğurayı olabilmesi için gerek ve yeter koşul $(s, m) = 1$ olmasıdır.

İspat:

(⇒):

a^m elemanı G nin bir doğurayı ise $G =< a > =< a^m >$ dir.

O halde, $a \in < a^m > \Rightarrow \mathrm{a} = (a^m)^t$ ($t \in N$) şeklinde yazılabilir.

Buna göre, $a^{mt-1} = 1_G$ olacağından, **Teorem 3.1.4** den $s|mt - 1$ dir. Sonuç olarak, bir $y \in Z$ için $mt - 1 = ys$ ya da $mt - ys = 1$ olduğundan Bezout teoremine göre $(s, m) = 1$ elde edilir.

(⇐):

$(s, m) = 1$ ise $mx + ys = 1$ olacak biçimde $x, y \in Z$ elemanları vardır ve

$$a = (a^m)^x (a^s)^y = (a^m)^x 1_G = (a^m)^x$$

dir. Buna göre, $a \in < a^m >$ olacağından, $G =< a > \subset < a^m >$ dir.

Öte yandan, $< a^m > \subset < a > = G$ olduğundan, $G =< a^m >$ sonucuna varılır.

Sonuç 3.1.1: $G =< a >$, s. mertebeden bir devresel grup ise, G nin doğurayları sayısı $\varphi(s)$ dir.

Örnek 3.1.7: $G =< a >$, 12. mertebeden bir devresel grup olsun. $\tau|12$ ise $\tau = 1, 2, 3, 4, 6, 12$ olabilir. Buna göre G nin alt gruplarını bulalım.

$\tau = 1$ için, 1. mertebeden alt grubu $H_1 = \{1_G\}$,

$\tau = 2$ için, 2. mertebeden alt grubu $H_2 =< a^6 >= \{1_G, a^6\}$,

$\tau = 3$ için, 3. mertebeden alt grubu $H_3 =< a^4 >= \{1_G, a^4, a^8\}$,

$\tau = 4$ için, 4. mertebeden alt grubu $H_4 =< a^3 >= \{1_G, a^3, a^6, a^9\}$,

$\tau = 6$ için, 6. mertebeden alt grubu $H_6 =< a^3 >= \{1_G, a^2, a^4, a^8, a^{10}\}$,

$\tau = 12$ için, 12. mertebeden alt grubu $H_{12} = G$ dir.

Öte yandan,

$\varphi(12) = 2^{2-1}.(2-1).3^{1-1}.(3-1) = 2.2 = 4$ ve $(12,1) = (12,5) = (12,7) = (12,11) = 1$

olduğundan, G nin doğurayları a, a^5, a^7, a^{11} dir.

Alıştırmalar III

1) Aşağıdaki iddialar doğru mudur?. Neden?.

- **i.** Her n doğal sayısına karşılık mertebesi n olan bir devresel grup vardır.
- **ii.** 24. mertebeden bir devresel grubun doğurayları sayısı 8 dir.
- **iii.** Bir sonlu devresel grupta her elemanının mertebesi, grubun her doğurayının mertebesini böler.

2) Z_{13} teki asal kalan sınıflar grubunda bütün elemanların mertebelerini bulunuz.

3) G bir grup ve $a \in G$ ise $|a| = |a^{-1}|$ olduğunu gösteriniz.

4) G bir grup ve $a, b \in G$ ise $|a| = |bab^{-1}|$ olduğunu gösteriniz.

5) 36. mertebeden bir devresel grubun bütün doğuraylarını ve alt gruplarını belirleyiniz.

6) $\overline{11}$ kalan sınıfının Z_{18} in asal kalan sınıfları grubundaki mertebesini belirleyiniz.

7) G komütatif bir grup, $a, b \in G$ ve $|a| = m$, $|b| = n$ olsun. $(m, n) = 1 \Rightarrow |ab| = mn$ olduğunu gösteriniz.

4.Kalan Sınıfları ve Lagrange Teoremi

Tanım 4.1: G bir grup ve $H \leq G$ olsun. $a, b \in G$ olmak üzere, G de " $\equiv$ " bağıntısı

$$"a \equiv b\ (H) \Leftrightarrow ab^{-1} \in H" \text{ (ya da } a \equiv b\ (H) \Leftrightarrow a^{-1}b \in H)$$

şeklinde tanımlanır.

Teorem 4.1: **Tanım 4.1** de verilen " $\equiv$ " bağıntısı bir denklik bağıntısıdır.

İspat:

İspat için $a \equiv b\ (H) \Leftrightarrow ab^{-1} \in H$ tanımı kullanılacaktır; $a \equiv b\ (H) \Leftrightarrow a^{-1}b \in H$ tanımı ile de benzer ispat yapılabilir.

1) $a \equiv a\ (H)$ dır, çünkü $H \leq G$ olduğundan, $aa^{-1} = 1_G \in H$ dır.

2) $a \equiv b\ (H)$ ise $b \equiv a\ (H)$ dır, çünkü $a \equiv b\ (H)$ ise $ab^{-1} \in H$ ve $H \leq G$ olduğundan $(ab^{-1})^{-1} = ba^{-1} \in H$ ve $b \equiv a\ (H)$ dır.

3) $a \equiv b\ (H)$, $b \equiv c\ (H)$ ise $a \equiv c\ (H)$ dır; çünkü $a \equiv b\ (H)$, $b \equiv c\ (H)$ olduğuna göre $ab^{-1} \in H$, $bc^{-1} \in H$ ve $H \leq G$ olduğundan $(ab^{-1})(bc^{-1}) = ac^{-1} \in H \Rightarrow a \equiv c\ (H)$ dır.

Tanım 4.2: Tanım 4.1 de verilen denklik bağıntısına göre, $a \in G$ elemanının temsilcisi olduğu denklik sınıfı,

$$Ha = \{b \in G \mid b \equiv a\ (H) \Leftrightarrow ba^{-1} \in H \Leftrightarrow b \in Ha\}$$

$$\text{(ya da } aH = \{b \in G \mid b \equiv a\ (H) \Leftrightarrow a^{-1}b \in H \Leftrightarrow b \in aH\}\text{)}$$

şeklinde tanımlanır.

Burada a nın ait olduğu (a nın temsilcisi olduğu) $\boldsymbol{Ha}$ **denklik sınıfına,** $\boldsymbol{G}$ **nin** $\boldsymbol{H}$ **alt grubuna göre bir sol kalan sınıfı** ve a nın ait olduğu (a nın temsilcisi olduğu) $\boldsymbol{Ha}$ **denklik sınıfına** ise

$\boldsymbol{G}$ **nin** $\boldsymbol{H}$ **alt grubuna göre bir sağ kalan sınıfı** denir.

Not 4.1: $H = 1_G H = H 1_G$ olduğundan, H alt grubunun kendisi, G nin H ya göre hem bir sol,

hem de bir sağ kalan sınıfıdır. Öte yandan, $a, b \in G$ olmak üzere G nin aH, bH (Ha, Hb) alt kümeleri, bir sınıflara ayrılışın iki sol (sağ) kalan sınıfı olduklarından, ya $aH = bH$ $(Ha = Hb)$ ya da $aH \cap bH = \emptyset$ $((Ha \cap Hb) = \emptyset)$ dir.

Teorem 4.2: $a, b \in G$ olmak üzere, aH, bH (Ha, Hb) gibi iki sol (sağ) kalan sınıfı, aynı kuvvettedir.

İspat:

$\boldsymbol{\varphi}: H \to aH$; $\varphi(h) = ah$ tasvirini göz önüne alalım. Her $b \in aH$ için $b = ah$ olacak biçimde bir $h \in H$ bulunduğundan , $\boldsymbol{\varphi}$ tasviri üzerinedir. Öte yandan, G deki kısaltma özelliği kullanıldığında, $ah_1 = ah_2 \Rightarrow h_1 = h_2$ olduğundan, $\boldsymbol{\varphi}$ tasviri $(1-1)$ dir. Sağ kalan sınıfları için de ispat benzer biçimde yapılır.

Teorem 4.3 (Lagrange Teoremi): Sonlu bir grubun her alt grubunun mertebesi grubun mertebesini böler.

İspat:

G sonlu bir grup ve $|G| = n$, $H \leq G$ ve $|H| = m$ olsun. Bu durumda, G nin H ya göre birbirinden farklı sol kalan sınıflarının sayısı da sonludur, çünkü aksi halde, her kalan sınıfından bir temsilci alınarak elde edilen küme, G nin bir sonsuz alt kümesini oluştururdu. G nin H ya göre birbirinden farklı sol kalan sınıflarının, $a_1H, a_2H, \dots, a_rH$ olduğunu varsayalım. Buna göre,

$$G = \bigcup_{i=1}^{r} a_i H$$

G nin bir sınıflara ayrılışı ve her i $(i = 1, 2, \dots, r)$ için $s(a_iH) = |H| = m$ olduğundan $n = rm$ dir. Demek ki, $m|n$ dir.

Sonuç 4.1: Sonlu bir G grubunun bir H alt grubuna göre birbirinden farklı sol kalan sınıflarının sayısı, birbirinden farklı sağ kalan sınıflarının sayısına eşittir.

Tanım 4.3: bir G grubunun bir H alt grubuna göre birbirinden farklı kalan sınıflarının sayısına

H nın G içindeki **indeksi** denir ve bu indeks $[G: H]$ ile gösterilir. Buna göre, $|G| = |H| = [G: H]$ yazılır.

Sonuç 4.2: Sonlu bir G grubunda, her $a \in G$ için $|a| \mid |G|$ ve $a^{|G|} = 1_G$ dir.

Teorem 4.3 e göre, a nın mertebesi, a nın G içinde doğurduğu devresel grubun mertebesi olduğundan, $|a| \mid |G|$ dir. Buna göre, $|G| = |a|.[G:< a >]$ olacağından,

$$a^{|G|} = a^{|a|.[G:<a>]} = (a^{|a|})^{[G:<a>]} = {1_G}^{[G:<a>]} = 1_G$$

dir.

Sonuç 4.3: Mertebesi asal olan grup devreseldir.

İspat:

G bir grup, $|G| = p$ asal ve $a \in G$; $a \neq 1_G$ olsun. **Sonuç 4.2** ye göre $|a|$, p nin bir böleni olacağından $|a| = 1$ ya da $|a| = p$ dir. $a \neq 1_G$ ise $|a| = 1$ olamaz, yani $|a| = p$ dir.

Buna göre, $G = \{1_G, a, a^2, \dots, a^{p-1}\} =< a >$ olarak ifade edilir.

Sonuç 4.4 (Fermat-Euler Teoremi): $m \in N$, $m > 1$, $a \in Z$ ve $(a, m) = 1$ ise,

$$a^{\varphi(m)} \equiv 1 \ (m)$$

dir.

İspat:

Z_m de asal kalan sınıflarının kümesini bir grup oluşturduğunu biliyoruz. Bu grubun mertebesi $\varphi(m)$ dir. Buna göre $a \in Z$ ve $(a, m) = 1$ ise $\bar{a}$ bir asal kalan sınıfıdır ve $\overline{(a)}^{\varphi(m)} = \overline{a^{\varphi(m)}} = \bar{1}$, yani $a^{\varphi(m)} \equiv 1\ (m)$ dir.

Sonuç 4.5 (Küçük Fermat Teoremi): p bir asal sayı ise p bölmez a koşuluna uyan her $a \in Z$ için $a^{p-1} \equiv 1\ (p)$ dir.

Örnek 4.1: 72^{7272} sayısı 41 e bölündüğünde kaç kalanını bırakır? sorusunu yanıtlamak,

$72^{7272} \equiv x\ (41)$ kongrüansını çözmek demektir. Oysa $72 \equiv 31\ (41)$ olduğundan,

$72^{7272} \equiv 31^{7272}\ (41)$ dir. Burada 41 asal ve $41 \nmid 31$ olduğundan **Küçük Fermat Teoremine** göre $31^{40} \equiv 1\ (41)$ dir. O halde,

$31^{7272} \equiv 31^{40.181+32} \equiv (31^{40})^{181} 31^{32} \equiv (-10)^{32} \equiv 10^{32} \equiv (10^2)^{16} \equiv (18)^{32} \equiv (18^2)^8$
$\equiv (-4)^8 \equiv (16^2)^2 \equiv 10^2 \equiv 18$

ve sonuç olarak $72^{7272} \equiv 18\ (41)$ elde edilir.

Örnek 4.2: $(Z_9, +)$ grubunun, $H = \{\bar{0}, \bar{3}, \bar{6}\}$ alt kümesini incelersek

$$(H, +) \leq (Z_9, +)$$

olduğunu görürüz. H nın Z_9 daki sol kalan sınıflarını bulmadan önce, grup işlemi toplama olduğundan, $\bar{a} + H$ gösterimini kullanacağımızı vurgulayalım. Buna göre

$$\bar{a} \in Z_9 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\}$$

olmak üzere,

$$\bar{a} + H = \{\bar{a} + H : h \in H\} \text{ şeklindeki}$$

sol kalan sınıflarının,

$$\bar{0} + H = \{\bar{0} + H : h \in H\} = \{\bar{0}, \bar{3}, \bar{6}, \}$$

$$\bar{1} + H = \{\bar{1} + H : h \in H\} = \{\bar{1}, \bar{4}, \bar{7}\}$$

$$\bar{2} + H = \{\bar{2} + H : h \in H\} = \{\bar{2}, \bar{5}, \bar{8}\}$$

olarak sıralandığına dikkat ediniz.

Örnek 4.3: $(3Z, +) \leq (Z, +)$ olduğuna göre, $3Z$ nin Z deki sol kal kalan sınıflarını bulalım;

$$m + 3Z = \{m + 3k : k \in Z\} \, ,$$

$m = 0$ için

$$0 + 3Z = \{0 + 3k : k \in Z\} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$$

$m = 1$ için

$$1 + 3Z = \{1 + 3k : k \in Z\} = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$$

$m = 2$ için

$$2 + 3Z = \{2 + 3k : k \in Z\} = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$$

$m = 3$ için

$$3 + 3Z = 3Z$$

$m = 4$ için

$$4 + 3Z = 1 + 3Z$$

$m = 5$ için

$$5 + 3Z = 2 + 3Z$$

şeklindedir. Dikkat edilirse sol kalan sınıfları, m yi nasıl seçersek seçelim;

$$3Z, 1 + 3Z, 2 + 3Z$$

olarak sıralanır.

Örnek 4.4: $G = \{ e, a, b \}$ kümesi üzerinde " $*$ " ikili işlemi aşağıdaki tablo yardımıyla tanımlanmış olsun.

$*$	E	a	b
e	E	a	b
a	A	e	b
b	B	a	e

Bu durumda (G, $*$) bir grup değildir. Çünkü ikinci satırda a elemanı iki kere bulunmaktadır.

a * e = a = a * b olduğundan b = e elde edilir. Halbuki $b \neq e$ dir.

Dolayısıyla bir grupta birim eleman olduğundan $G = \{ e, a, b \}$ kümesi $*$ işlemine göre bir grup değildir.

Örnek 4.5: $\boldsymbol{Z_5}$ de $A = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ grubunun elemanları ve kalan sınıfları arasında tanımlanan çarpma işlemi esas alınarak elde edilen grup tablosu aşağıda verilmiştir.

.	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

Bu tabloya göre işlem yapmadan, her elemanın tersini belirlemek,cebirsel yapının komütatifliği hakkında bilgi sahibi olmak kolaydır.

Alıştırmalar IV

1) Aşağıdaki iddialar doğru mudur? Neden?

i. G bir grup ve $H \leq G$ olmak üzere, her $a \in G$ için aH, H ile aynı kuvvettedir.

ii. G bir grup ve $p \in Z$ bir asal sayı olsun. $|G| = p$ olması için gerek ve yeter koşul G nin devresel olmasıdır.

iii. 75. Mertebeden bir grubun indeksi 10 olan 2 alt grubu vardır.

iv. $12^{7272} \equiv 11\ (41)$ dir.

2) Z_{32} nin asal kalan sınıfları grubunun $H = \{\bar{5}\}$ alt grubuna göre sol kalan sınıflarına ayrılışını belirleyiniz.

3) G bir komütatif grup, $|G| = n$ ve bir $k \in N$ için $(k, n) = 1$ ise bir $a \in G$ için $x^k = a$ denkleminin G de kaç çözümü vardır?

4) Aşağıdaki tabloların birer grubun işlem tablosu olup olmadığını belirleyiniz.

.	a	b	c	d
a	b	c	d	a
b	c	d	a	b
c	a	b	c	d
d	d	a	b	b

.	a	b	c	d
a	c	d	a	b
b	a	b	c	d
c	d	c	b	a
d	b	a	d	c

.	a	b
a	a	b
b	b	a

5.Permütasyon Grupları ve Temel Özellikleri

Tanım 5.1: Bir M kümesini kendi üzerine birebir olarak resmeden bir tasvire, M nin bir **transformasyonu** denir. M kümesinin sonlu olması durumunda, **transformasyon** yerine, M nin bir **sübstitüsyonu** ya da **permütasyonu** ifadesi kullanılır. M kümesini kendi üzerine birebir olarak resmeden idantik tasvire (I ile gösterilir) **idantik permütasyon** denir.

M nin bütün transformasyonlarından oluşan kümenin, tasvirlerin çarpım işlemine göre bir grup oluşturduğu kolayca gösterilebilir. Buna göre aşağıdaki tanım verilecektir;

Tanım 5.2: n elemanlı bir kümenin bütün sübstitüsyonlarının (permütasyonlarının) oluşturduğu gruba $\boldsymbol{n}$**. dereceden simetrik grup** ($\boldsymbol{n}$**. dereceden permütasyon grubu**) denir ve $\boldsymbol{S_n}$ ile gösterilir.

S_n, $\{x_1, x_2, \dots, x_n\}$ kümesinin simetrik grubu ve $S \in S_n$ olsun. Burada $i_1, i_2, \dots, i_n$; $1,2,\dots,n$ nin bir sıralanışı olmak üzere, $S(x_k) = x_{i_k}$ $(k = 1,2, \dots n)$ ise,

S permütasyonu, her x_k $(k = 1,2, \dots n)$ elemanının altına görüntüsü yazılmak suretiyle

$$S = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix} = \begin{pmatrix} x_k \\ S(x_{i_k}) \end{pmatrix}$$

biçiminde ya da fonksiyonel olarak

$$S = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} = \begin{pmatrix} k \\ g(i_k) \end{pmatrix}$$

şeklinde gösterilir. Buna göre, $I = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ dir.

$$S = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \ T = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

permütasyonlarının çarpımı

$$ST = \begin{pmatrix} 1 & 2 & \dots & n \\ i_{j_1} & i_{j_2} & \dots & i_{j_n} \end{pmatrix}$$

dir. S nin tersi ise,

$$S^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}$$

dir. Öte yandan $n > 2$ için S_n komütatif değildir. Örneğin S_3 te

$$S = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \; T = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

için

$$ST = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \; T = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

olduğundan $ST \neq TS$ dir.

Not 5.1: S_n grubunun her elemanı, $\{1,2,\dots,n\}$ kümesini kendi üzerine (1-1) olarak resmeden bir tasvir olarak dikkate alındığına göre $S \in S_n$ ise $S(1)$, n tane elemandan biri olabilir. $S(1)$ seçilmiş olduğuna göre $S(2)$, $S(1)$ dışında kalan $n-1$ elemandan biri olabilir. $S(1)$ ve $S(2)$ seçilmiş olduğunda ise $S(3)$, $S(1)$ ve $S(2)$ dışında kalan $n-2$ elemandan biri olabilir.
Bu biçimde devam edilirse, S_n nin

$$n(n-1)(n-2)\dots 1 = n!$$

elemanı olduğu görülür, yani $|S_n| = n!\ dir.$

Örnek 5.1: $S, T \in S_7$; $S = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 1 & 6 & 2 & 4 & 5 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 7 & 5 & 4 & 6 \end{pmatrix}$ için

$$ST = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 7 & 5 & 2 & 6 & 4 \end{pmatrix}, \; TS = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 3 & 4 & 2 & 7 & 5 \end{pmatrix},$$

$$S^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 7 & 4 & 3 & 6 & 2 \end{pmatrix},\ T^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 6 & 5 & 7 & 4 \end{pmatrix},$$

$$S^{-1} = \begin{pmatrix} 7 & 3 & 1 & 6 & 2 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 2 & 6 & 7 & 4 & 1 \end{pmatrix}$$

$$T^{-1} = \begin{pmatrix} 3 & 2 & 1 & 7 & 5 & 4 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 6 & 5 & 7 & 4 \end{pmatrix}$$

dir.

Tanım 5.3: $j_1, j_2, \dots, j_k$ $(k > 1)$ birbirinden farklı doğal sayılar olmak üzere $S \in S_n$ için

$$S(j_1) = j_2, S(j_2) = j_3, \dots, S(j_{k-1}) = j_k, S(j_k) = j_1$$

ise $S = (j_1 j_2 \dots j_k)$ yazılır ve buna ***k* uzunluğunda** bir devre denir. Her j_t $(t = 1,2,\dots)$ için $S(j_t) = j_t$ ise S, 1 uzunluğunda bir devredir.1uzunluğundaki devreler genellikle göz ardı edilirler. Bir devre, saat yönünde yönlendirilerek çember üzerine dizilmiş semboller olarak düşünülebileceğinden,

$j_1, j_2, \dots, j_k$ nın dairesel permütasyonlarını dikkate alarak,

$$S = (j_1 j_2 \dots j_k) = (j_2 j_3 \dots j_k j_1) = (j_3 j_4 \dots j_1 j_2) = \cdots = (j_k j_1 \dots j_{k-2} j_{k-2})$$

yazabiliriz.

Örnek 5.2: $S = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 4 & 6 & 2 & 7 \end{pmatrix}$ permütasyonunda, $S(1) = 3,\ S(3) = 5,\ S(5) = 6,\ S(6) = 2,$ $S(2) = 1$ ve $S(4) = 4$, $S(7) = 7$ olduğundan $S = (13562)$ dir ve aynı zamanda

$S = (35621)(4)(7) = (56213) = (62135) = (21356)$ dir.

Tanım 5.4: Hiçbir ortak rakamları bulunmayan devrelere **yabancı devreler** denir.

Örnek 5.3: $S = (157), T = (2346)$ yabancı devrelerdir.

Teorem 5.1: Yabancı devreler çarpma işlemine göre komütatiftir.

Teorem 5.2: $S \in S_n$, r uzunluğunda bir devre yani $S = (i_1, i_2, \dots, i_r)$ ise $|S| = r$ dir.

Teorem 5.3: Her permütasyon, bir takım yabancı devrelerin çarpımı olarak yazılabilir ve bu yazılış, sıra göz ardı edildiğinde tek türlü belirlidir.

İspat:

$S \in S_n$; $S = \begin{pmatrix} 1 & 2 & \dots & n \\ S(1) & S(2) & \dots & S(n) \end{pmatrix}$ olsun. Burada $S^0(1) = 1, S(1), S^2(1), \dots, S^s(1), \dots$ rakamlarını göz önüne alırsak, bunlar arasında birbirinden farklı olanların sayısı en çok n olduğundan belli bir adımdan sonra tekrar eder. Buna göre $S^k(1) = 1$ koşuluna uyan en küçük bir k doğal sayısı vardır ve 1, $S(1)$, $S^2(1), \dots, S^{k-1}(1)$ rakamları birbirinden farklıdır. Böylece k uzunluğunda bir $(1, S(1), \dots, S^{k-1}(1))$ devresi elde edilir. İşlem bu devrede görünmeyen bir rakamla tekrar edilirse, ilk devreye yabancı bir devre bulunur ve $1,2, \dots n$ rakamları tükeninceye kadar bu işleme devam edildiğinde, ortaya çıkan yabancı devrelerin çarpımı S yi verir. Yabancı devrelerin çarpımı komütatif olduğundan sıra göz ardı edildiğinde, S nin, yabancı devrelerin çarpımı olarak yazılışı tek türlü belirlidir.

Not 5.2: S_n de idantik permütasyonun yabancı devrelerin çarpımı olarak yazılışı (ya da yabancı devrelere ayrılışı) $I = (1)(2) \dots (n)$ biçimindedir.

Örnek 5.4: Örnek 5.1 de verilen S ve T permütasyonlarının ve ST, TS, S^2, T^2, S^{-1}, T^{-1} in yabancı devrelerin çarpımı olarak yazılışları (ya da yabancı devrelere ayrılışları) aşağıdaki gibidir:

$$S = (17523)(46), T = (13)(476), ST = (23745), TS = (16752)$$

$$S^2 = (15372), T^2 = (467), S^{-1} = (13257), T^{-1} = (13)(467)$$

Teorem 5.4: Bir $S \in S_n$ permütasyonunun mertebesi, ayrıldığı yabancı devrelerin uzunluklarının en küçük ortak katıdır.

Örnek 5.5: $S = (34)(125)$ permütasoyonu için $|S| = ekok(2,3) = [2,3] = 6$ ve $T = (346)(1825)(79)$ permütasyonu için $|S| = [2,3,4] = 12$ dir.

Tanım 5.4: Uzunluğu 2 olan, yani (ij) biçimindeki bir devreye bir **transpozisyon** denir.

Teorem 5.5: Her permütasyon birtakım transpozisyonların çarpımı olarak yazılabilir.

İspat:

Her permütasyon, bir takım yabancı devrelerin çarpımı olarak yazılabildiğinden, her devrenin birtakım transpozisyonların çarpımı olarak yazılabildiğini göstermek yeterlidir. Burada

$$(i_1 i_2 \dots i_r) = (i_1 i_r) \dots (i_1 i_3)(i_1 i_2)$$

olduğundan, istenen elde edilmiş olur.

Not 5.3: Bir permütasyonun birtakım transpozisyonların çarpımı olarak gösterilişi tek türlü değildir. Çünkü $(ij)^2 = I$ olduğundan çarpımın herhangi bir yerine keyfi bir transpozisyonun karesi yazılabilir. Örneğin $S = (12487)(536)$ permütasyonunun bir transpozisyonların çarpımı olarak yazılışı $S = (17)(18)(14)(12)(56)(53)$, ikinci bir yazılışı ise $S = (17)(18)(13)(13)(14)(12)(56)(53)$ biçimindedir.

Tanım 5.5: Tek (çift) sayıda transpozisyonun çarpımı olarak yazılan bir permütasyona **tek (çift) permütasyon** denir.

Örnek 5.6: $I = (ij)^2$ olduğundan, I çift permütasyondur.

$$S = (1534)(26879) = (14)(13)(15)(29)(27)(28)(26)$$

olduğundan S tek permütasyondur.

$$T = (1357)(2468) = (17)(15)(13)(18)(16)(24)$$

olduğundan T çift permütasyondur.

Teorem 5.6: S_n deki tek ve çift permütasyonlar aynı sayıdadır.

İspat:

S_n deki bütün çift permütasyonlarının kümesi $\{S_1, S_2, \dots, S_k\}$ olsun. Bu kümenin her elemanını bir (ij) transpozisyonu ile çarparsak, **tek** permütasyonlardan oluşan $\{(ij)S_1, (ij)S_2, \dots, (ij)S_k\}$ kümesi elde edilir. S_n de bunlar dışında tek permütasyon yoktur, çünkü T bir tek permütasyon ise $(ij)T \in \{S_1, S_2, \dots, S_k\}$ dır. Buna göre,

$$(ij)T = S_r; 1 \leq r \leq k \Rightarrow T = (ij)S_r; 1 \leq r \leq k$$

yani

$$T \in \{(ij)S_1, (ij)S_2, \dots, (ij)S_k\}$$

olmak zorundadır. Bu da ispatı bitirir.

Tanım 5.6: S_n deki bütün çift permütasyonlarının kümesini A_n ile gösterirsek, S_n bir sonlu grup olduğundan $A_n < S_n$ dir ve **Teorem 5.6** gereği,

$$|A_n| = \frac{n!}{2}$$

dir. S_n in $\boldsymbol{A_n}$ alt grubuna $\boldsymbol{n}$**. dereceden alterne grup** denir.

Örnek 5.7: $n = 2, 3, 4$ için S_n ve A_n grupları aşağıdaki gibidir.

$S_2 = \{I, (12)\}, A_2 = \{I\}$

$S_3 = \{I, (12), (13), (23), (123), (132)\}, A_3 = \{I, (123), (132)\}$

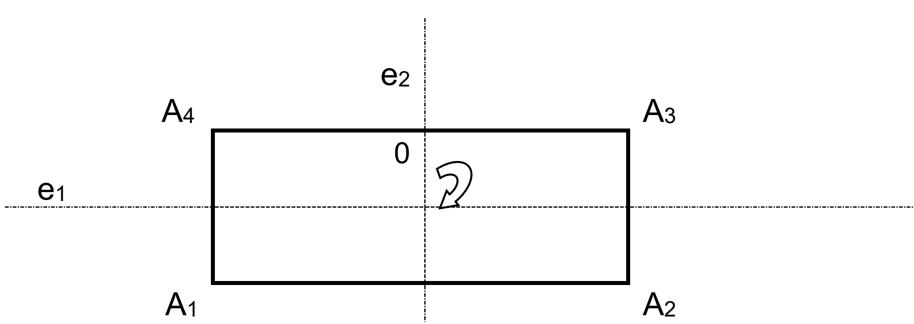
$S_4 =$
$\{I, (12), (13), (14), (23), (24), (34), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34),$
$(13)(24), (14)(23), (1234), (1432), (1243), (1342), (1324), (1423)\}$

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

Teorem 5.7: S_n grubu $(1j); j = 2, 3, \dots, n;$ biçimindeki transpozisyonlar tarafından doğurulur.

Teorem 5.8: $n \geq 3$ olmak üzere A_n grubu $(12j)\ ; j = 3, 4, \dots n$ devreleri tarafından doğurulur.

Örnek 5.8: Bir dikdörtgeni kendi üzerine dönüştüren bütün dönme ve simetrilerini göz önüne alalım.



Dikdörtgeni D ile gösterirsek, D nin kendi üzerine bütün dönme ve simetrileri aşağıdaki gibidir:

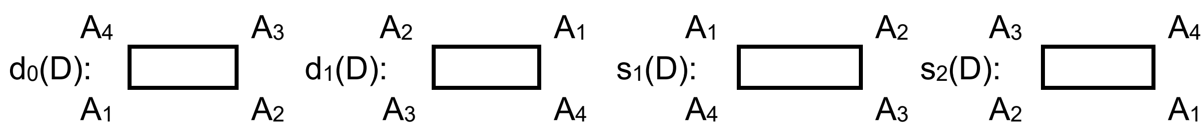
d_0: 0 etrafında (ok yönünde) 0 lık (2π lik) dönme,

d_1: 0 etrafında π lik dönme,

s_1: e_1 eksenine göre simetri,

s_2: e_2 eksenine göre simetri,

Bu dört dönüşüm D dikdörtgenini aşağıdaki biçimde değiştirir.



Burada $G = \{d_0, d_1, s_1, s_2\}$ kümesinin grup aksiyomlarını gerçeklediğini gösterelim. Bunu çarpım tablosunu yaparak görebiliriz.

.	d_0	d_1	s_1	s_2
d_0	d_0	d_1	s_1	s_2
d_1	d_1	d_0	s_2	s_1
s_1	s_1	s_2	d_0	d_1
s_2	s_2	s_1	d_1	d_0

i. G tasvirlerin çarpma işlemine göre kapalıdır.

ii. Genel olarak tasvir çarpımı asosyatif olduğundan, G de asosyatiflik geçerlidir.

iii. Çarpım tablosu esas köşegene göre simetrik olduğundan G komütatiftir.

iv. d_0, G nin birimidir.

v. ${d_0}^{-1} = d_0$, ${d_1}^{-1} = d_1$, ${s_1}^{-1} = s_1$, ${s_2}^{-1} = s_2$

O halde, G, gerçekten bir gruptur. Bu gruba **dikdörtgenin grubu** denir. Burada A_1, A_2, A_3, A_4 yerine sırasıyla $1, 2, 3, 4$ yazarsak, G nin her elemanı dikdörtgenin köşeleri üzerinde yaptığı etki ile tamamen belirlendiğine göre, bu elemanların her birine aşağıda verildiği gibi, S_4 ün bir elemanı kaşı gelir:

$$d_0 \rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = I$$

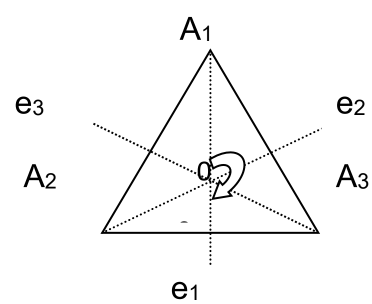
$$d_1 \rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$

$$s_1 \rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$$

$$s_2 \rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$

Bu tasvir bir izomorfidir, yani G grubu S_4 ün $V_4 = \{I, (13)(24), (14)(23), (12)(34)\}$ alt grubuna izomorftur. V_4 grubuna **Klein'in dörtlü grubu** denir.

Örnek 5.9: Bir eşkenar üçgeni kendi üzerine dönüştüren bütün dönme ve simetrilerini göz önüne alalım.



Eşkenar üçgeni E ile gösterirsek, E nin kendi üzerine bütün dönme ve simetrileri aşağıdaki gibidir:

d_0: 0 etrafında (ok yönünde) 0 lık (2π lik) dönme,

d_1: 0 etrafında $\frac{2\pi}{3}$ lik dönme,

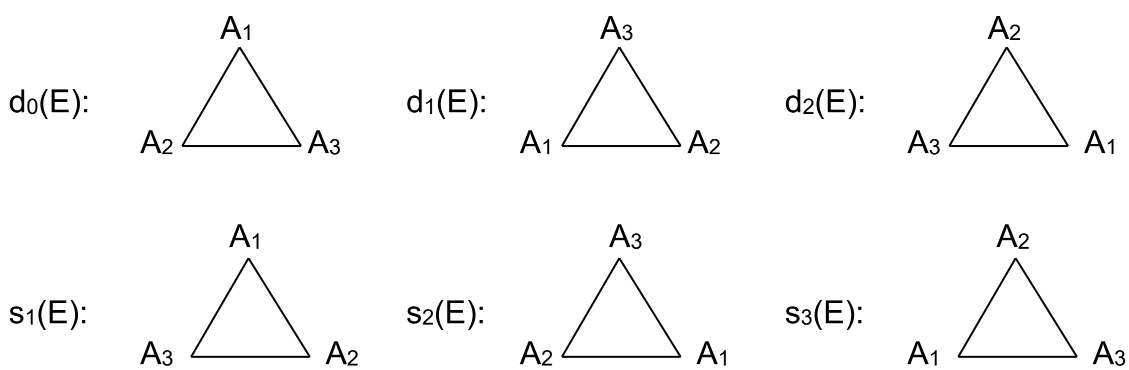
d_2: 0 etrafında $\frac{4\pi}{3}$ lik dönme,

s_1: e_1 eksenine göre simetri,

s_2: e_2 eksenine göre simetri,

s_3: e_3 eksenine göre simetri,

Bu altı dönüşüm E eşkenar üçgenini aşağıdaki biçimde değiştirir:



Burada $G = \{d_0, d_1, d_2, s_1, s_2, s_3\}$ kümesinin grup aksiyomlarını gerçeklediğini gösterelim. Bunu çarpım tablosunu yaparak görebiliriz;

.	d_0	d_1	d_2	s_1	s_2	s_3
d_0	d_0	d_1	d_2	s_1	s_2	s_3
d_1	d_1	d_2	d_0	s_3	s_1	s_2
d_2	d_2	d_0	d_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	d_0	d_1	d_2
s_2	s_2	s_3	s_1	d_2	d_0	d_1
s_3	s_3	s_1	s_2	d_1	d_2	d_0

Tablodan görüleceği gibi $1_G = d_0$ ve

$$d_0^{-1} = d_0,\ d_1^{-1} = d_2,\ d_2^{-1} = d_1,\ s_1^{-1} = s_1,\ s_2^{-1} = s_2,\ s_3^{-1} = s_2$$

olduğundan G bir gruptur. Bu gruba **eşkenar üçgenin grubu** denir. Çarpım tablosu esas köşegene göre simetrik olmadığından G komütatif değildir. Öte yandan G grubunun elemanlarına karşı gelen 3. dereceden permütasyonlar aşağıdaki gibidir:

$$d_0 \rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$$

$$d_1 \rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$$

$$d_2 \rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$$

$$s_1 \rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$$

$$s_2 \to \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$$

$$s_3 \to \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$$

Buna göre G grubu S_3 simetrik grubuna izomorftur, yani $G \cong S_3$ yazabiliriz ve eşkenar üçgenin grubu olarak S_3 alabiliriz.

6. Normal Alt Gruplar, Eşlenikler ve Bölüm Grupları

6.1 Normal Alt Gruplar

Tanım 6.1.1: G grubunun, a, x elemanları için axa^{-1} (ya da $a^{-1}xa$) elemanına,

x in a ile dönüşmüşü (x elemanının eşleniği ya da konjügesi) denir; $b = axa^{-1}$ ise **a ile b eşleniktir** denir.

Tanım 6.1.2: G bir grup, $N \leq G$, a $\in G$ ise $aNa^{-1} \leq G$ ye **N alt grubunun a ile eşleniği** denir.

$M = aNa^{-1}$ ise **N ile M eşleniktir** denir.

Sonuç 6.1.1: G grubu üzerinde aşağıdaki biçimde tanımlanan $\sim$ bağıntısı bir denklik bağıntısıdır:

$$"\forall\ g, f \in G \text{ için } g \sim f \Leftrightarm a \in G; f = aga^{-1}" \text{ dir.}$$

$\sim$ bağıntısının G üzerinde belirlediği sınıflara, G nin eşlenik eleman sınıfları denir.

Herhangi bir $g \in G$ elemanının ait olduğu eşlenik eleman sınıfı

$$[g] = \{aga^{-1} |\ a \in G\}$$

dir. G komütatif ise doğal olarak $[g] = \{g\}$ dir.

Sonlu bir G grubunun birbirinden farklı eşlenik eleman sınıfları $[g_1], [g_2], \dots, [g_r]$ ve bunların eleman sayıları sırasıyla $t_1, t_2, \dots, t_r$ ise

$$G = \bigcup_{i=1}^{r} [g_i] \ ve\ |G| = \sum_{i=1}^{r} t_i$$

yazılır. Buradaki birinci eşitlik G nin bir sınıflara ayrılışıdır ve ikinci eşitliğe G nin **sınıf denklemi** denir. Sınıf denklemi, ilerleyen paragraflarda etki kavramı ile yeniden ele alınacaktır.

Teorem 6.1.1: G bir grup ve N, G nin bir alt grubu ise aşağıdaki ifadeler birbirine denktir:

- **i.** Her $a \in G$, her $x \in N$ için $axa^{-1} \in N$ dir.
- **ii.** Her $a \in G$ için $aNa^{-1} \subset N$ dir.
- **iii.** Her $a \in G$ için $aNa^{-1} = N$ dir.
- **iv.** Her $a \in G$ için $aN = Na$ dir.

Tanım 6.1.3: G bir grup, N de G nin bir alt grubu olsun. Eğer her $a \in G$ için $aN = Na$ ise N ye G nin bir **normal alt grubu** denir ve N ($N \neq G$ ise $N \lhd G$) yazılır.

G nin bir normal alt grubu, **Teorem 6.1.1** de verilen **iii.** koşulunu gerçekleyen bir alt gruptur. Buna göre G nin bir normal alt grubu, **Teorem 6.1.1** de verilen birbirine denk koşullardan birini gerçekleyen bir alt grup olarak tanımlanabilir; **iv.** koşulunu gerçekleyen N alt grubuna, G nin bir **invaryant alt grubu** denir. Buna göre **"invaryant alt grup"** ve **"normal alt grup"** kavramları birbiriyle çakışır.

Burada $aN = Na$ olması, her $x \in N$ için $ax = xa$ olmasını gerektirmez. Ancak, her $x \in N$ elemanına karşılık $ax = ya$ olacak biçimde bir $y \in N$ vardır.

$N \lhd G$ olması halinde, G grubunun N alt grubuna göre sağ ve sol kalan sınıfları aynıdır.

Örnek 6.1.1: G grubunun triviyal alt grupları olan G ve $\{1_G\}$ grupları, G nin triviyal normal alt gruplarıdır. G komütatif ise her alt grubu normaldir.

Örnek 6.1.2: S_3 ün $N = \{I, (12)\}$ alt grubuna göre sol ve sağ kalan sınıfları dikkate alındığında, $(13)N \neq N(13)$ olduğundan N, G nin bir normal alt grubu değildir.

Teorem 6.1.2: Bir grubun indeksi iki olan alt grubu bir normal alt gruptur.

İspat:

G bir grup ve $N < G$; $[G:N] = 2$ olsun. Bu durumda her $a \in G - N$ için ayrık birleşim olarak

$$G = N \cup aN = N \cup Na$$

olacağından, $aN = Na = G - N$ dir. Sonuç olarak, her $a \in G$ için $aN = Na$, yani $N \lhd G$ dir.

Sonuç 6.1.2: $An \lhd Sn$ dir.

Tanım 5.6 da, $|A_n| = \frac{n!}{2}$ olduğu verilmişti. Buna göre, $[Sn: An] = 2$, yani $An \lhd Sn$ dir.

Not 6.1.1: G bir grup ve $K < H < G$ olsun. $K \lhd G$ ise $K \lhd H$ dır, çünkü her a∈G için $aK = Ka$ ise $H \subset G$ olduğundan aynı zamanda her $a \in H$ için $aK = Ka$ dır. Fakat $K \lhd H$ ise $K \lhd G$ olması gerekmez.

$$G = \{I, (13), (24), (13)(24), (14)(23), (12)(34), (1234), (1432)\}$$

alınması durumunda, H= $\{I, (13), (24), (13)(24)\}$ ve $K = \{I, (13)\}$ için
$K < H < G$ ve $[H: K] = 2$ dir. Buna göre $K \lhd H$ olmasına rağmen, K, G nin normal alt grubu değildir; çünkü $(13)(24)K \neq K(12)(34)$ dır.

6.2 Bölüm Grubu

Teorem 6.2.1: $N \lhd G$ olsun, G nin N ye göre sol (ya da sağ) kalan sınıflarından oluşan kümeyi G/N ile gösterelim ve $G/N = \{aN \mid a \in G\}$ kümesi üzerinde çarpma işlemini her $aN, bN \in G/N$ için $(aN)(bN) = abN$ biçiminde tanımlayalım. Bu durumda aşağıdaki iddialar doğrudur:

i. Bu çarpım, kalan sınıfların temsilcileri olan a, b elemanlarından bağımsızdır.

ii. G/N kümesi bu çarpma işlemine göre bir gruptur.

iii. G bir sonlu grup ise, $|G/N| = \frac{|G|}{|N|}$ dir.

Tanım 6.2.1: G/N grubuna, G grubunun N normal alt grubuna göre bölüm grubu denir.

Komütatif bir grubun her alt grubu bir normal alt grup olacağından, komütatif bir grubun her alt grubuna göre bölüm grubu oluşturulabilir; üstelik bu bölüm grubu da komütatiftir.

Öte yandan, G bir toplam grubu ise G komütatiftir ve herhangi bir N alt grubuna göre

$\forall\, a + N, b + N \in G/N$ için $(a + N) + (b + N) = (a + b) + N$ dir.

Örnek 6.2.1: $G = \{I, (13), (24), (13)(24), (14)(23), (12)(34), (1234), (1432)\}$,

$$N = V_4 = \{I, (13), (24), (13)(24)\}$$

için G/N bölüm grubu oluşturulabilir. Buna göre $G = V_4 \cup (13)V_4$ olduğundan,

$G/V_4 = \{V_4, (13)V_4\}$ dır.

Teorem 6.2.2: Bir devresel grubun her bölüm grubu da devreseldir.

G bir devresel grup ve $|G| = n$ ise n in her k bölenine karşılık, G nin k. mertebeden bir tek bölüm grubu vardır. Çünkü $n = kq$ ise G nin q mertebeden bir tek H alt grubu vardır ve G nin H alt grubuna göre bölüm grubunun mertebesi k olmak zorundadır. Buna göre sonlu devresel gruplar için Lagrange teoreminin karşıtı doğrudur.

Tanım 6.2.2: Triviyal normal alt gruplarından başka normal alt grubu bulunmayan bir gruba **basit grup** denir.

Örnek 6.2.2: S_4 bir basit grup değildir.

Tanım 6.2.3: G bir grup M, G nin, G den farklı bir normal alt grubu olsun. G nin M yi bir has alt küme olarak kabul eden ve G den farklı hiçbir normal alt grubu yoksa, M ye G nin bir **maksimal normal alt grubu denir.** Bu tanım aşağıdaki biçimde de ifade edilebilir:

$M \lhd G, M \neq G$ bir maksimal normal alt grup $\Leftrightarrow$ $\forall N$ normal alt grup için $M \lhd N \lhd G$ ise $M = N$ dir.

Teorem 6.2.3: M nin G grubunun bir maksimal normal alt grubu olması için gerek ve yeter koşul G/M nin basit olmasıdır.

İspat:

($\Rightarrow$):

M, G nin bir maksimal normal alt grubu olsun. G/M nin normal alt grupları K/M biçimindedir. M maksimal olduğundan $K = G$ olmak zorundadır. O halde G/M nin triviyal normal alt gruplarından başka normal alt grubu yoktur, yani G/M basittir.

($\Leftarrow$):

G/M basit olsun. G nin M yi kapsayan ve G den başka hiçbir normal alt grubu yoktur, yani

M maksimaldir.

Örnek 6.2.3. Mertebesi asal olan gruplar basittir. Çünkü, p bir asal sayı ve $|G| = p$ için $K \lhd G$ ise $|K| = 1$ ya da $|K| = p$ yani $K = \{1_G\}$ ya da $K = G$ olmak zorundadır.

6.3 Normalizatör, Merkez, Komütatör

Teorem 6.3.1: G grubunun herhangi bir g elemanıyla komütatif olan bütün elemanlarının kümesi G nin bir alt grubudur.

İspat:

$g \in G$ için göz önüne alınan kümeyi $N(g)$ ile gösterirsek,

$N(g) = \{a \in G \mid ag = ga\} \leq G$ olduğunu ispat edeceğiz. $1_G \in N(g)$ olduğundan $N(g) \neq \emptyset$ dir.

Öte yandan, $\forall a, b \in N(g)$ için $ag = ga$ ve $bg = gb$ olduğundan asosyatif özellik kullanılırsa,

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab) \Rightarrow ab \in N(g)$$

ve $\forall a \in N(g)$ için

$$ag = ga \Rightarrow a^{-1}(ag)a^{-1} = a^{-1}(ga)a^{-1} \Rightarrow ga^{-1} = a^{-1}g \Rightarrow a^{-1} \in N(g)$$

olduğundan $N(g) \leq G$ dir.

Tanım 6.3.1: Teorem 6.3.1 de verilen $N(g)$ alt grubuna, g elemanının G içindeki n**ormalizatörü** denir.

Tanım 6.3.2: G grubunun herhangi bir boş olmayan T alt kümesi ile komütatif olan bütün elemanlarının kümesini $N(T)$ ile gösterelim. $N(T) = \{a \in G \mid aT = Ta\}$ ye ***T* nin *G* içindeki normalizatörü** denir. Kolayca görüleceği gibi $N(T) \leq G$ ve $T \trianglelefteq N(T)$ dir.

Teorem 6.3.2: G bir grup, $T \leq G$ ise $N(T), G$ nin , T yi normal alt grup olarak kabul eden en büyük alt grubudur.

İspat:

$T \trianglelefteq G$ ise doğal olarak $N(T) = G$ dir. $T \leq G$ ise $T \trianglelefteq N(T) \leq G$ olduğunu gördük.

Eğer $T \lhd K < G$ olacak biçimde bir K alt grubu var olsa, her $k \in K$ için $kT = Tk$ olacağından, $k \in N(T)$ yani $K < N(T)$ elde edilir. O halde $N(T), G$ nin T yi normal alt grup olarak kabul eden enbüyük alt grubudur.

Tanım 6.3.3: G grubunun bütün elemanlarıyla komütatif olan elemanlarından oluşan alt kümeye G grubunun **merkezi** denir ve $M(G)$ ya da $Z(G), M_G$ sembolleriyle gösterilir. Buna göre,

$$M(G) = \{\ g \in G \ \mid \ ag = ga\ , (\forall a \in G\ için)\}$$

yazılır.

Teorem 6.3.3:

$$M(G) = \bigcap_{a \in G} N_G(a)$$

dır ve $M(G) \trianglelefteq G$ olduğu gibi $M(G)$ nin her normal alt grubu G de de normaldir.

İspat:

$g \in M(G) \Leftrightarrow \forall a \in G$ için $ag = ga \Leftrightarrow \forall a \in G$ için $g \in Na$ olduğundan,

$$M(G) = \bigcap_{a \in G} N_G(a)$$

dır ve her $a \in G$ için $N_a \leq G$ olduğundan $M(G) \leq G$ dir. Öte yandan, her $a \in G$ ve her $g \in M(G)$ için $ag = ga$ olduğundan $aM(G) = M(G)a$ yani $M(G) \trianglelefteq G$ dir. Ayrıca, $H < M(G)$ ise $\forall h \in H$ için $h \in M(G)$ ve $H \lhd G$ dir.

Tanım 6.3.4: *G* bir grup ve *a, b* ∈ *G* olmak üzere *a ve b* elemanlarının komütatörü [*a,b*] ile gösterilir,

$$[a,b] = aba^{-1}b^{-1}$$

olarak tanımlanır.

Örnek 6.3.1: *A* ve *B* aynı mertebeli, reel girdili tersi olan kare matrisler olmak üzere*, A* ve *B* matrislerinin komütatörü,

$$[A, B\,] = ABA^{-1}B^{-1}$$

şeklindedir. Burada hemen hatırlatalım ki tersi olan, aynı mertebeli, reel girdili bütün kare matrislerin kümesi, matrislerin çarpım işlemine göre bir gruptur.

Teorem 6.3.4: Bir *G* grubunun değişmeli olması için gerek ve yeter şart ∀*a, b* ∈ *G* için *e, G* nin birim elemanı olmak üzere,

$$[a, b] = e$$

olmasıdır.

İspat:

(⇒):

G değişmeli bir grup olsun. Yani, ∀*a, b* ∈ *G* için

$$ab = ba \qquad (*)$$

olsun. (*) eşitliğinin her iki tarafını önce sağ taraftan, a^{-1} ile ve daha sonra tekrar sağ taraftan b^{-1} ile çarpalım. Bu durumda,

$$aba^{-1}b^{-1} = e$$

elde edilir. Komütatör tanımı hatırlandığında,

$$[a, b] = e$$

sonucuna varılır.

(⇐):

$\forall a, b \in G$ için $[a, b] = e$ olsun. Komütatör tanımından,

$$aba^{-1}b^{-1} = e$$

dır. Bir sonraki adımda, eşitliğin her iki tarafını sağ taraftan, önce *b* ile sonra da *a* ile çarparsak,

$$ab = ba$$

olur. Yani, *G* grubu değişmelidir.

Teorem 6.3.5: Bir komütatörün tersi de yine bir komütatördür.

İspat:

G bir grup ve $a, b \in G$ elemanlarının komütatörü $[a, b]$ olsun. O halde,

$$[a, b] = aba^{-1}b^{-1}$$

ve $[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a]$ elde edilir. Bu da, $[b, a]$ nın dolayısıyla $[a,b]^{-1}$ nin de komütatör olduğunu gösterir.

Teorem 6.3.6: G grubunun, sonlu sayıda komütatörlerinin çarpımlarından oluşan kümeyi, $[G, G]$ ile gösterelim. Yani,

$$[G,G] = \left\{\prod_{i=1}^{n}[a_i b_i] : a_i, b_i \in G\right\}$$

olsun. Bu durumda,

$$[G, G] \lhd G \quad \text{dir.}$$

Örnek 6.3.2: S_4 de (123) , $(13)(24)$ ün komütatörü,

$$[(123),(13)(24)] = (123)(13)(24)(123)^{-1}\left((13)(24)\right)^{-1}$$

$$= (21)(34)\,(13)(24) = (14)(23) \text{ dir.}$$

Alıştırmalar VI

1) Bir grubun bir takım normal alt gruplarının arakesitinin de bir normal alt grup olduğunu gösteriniz.

2) G bir grup, $H \lhd G,\ K \lhd G$ ve $H \cap K = \{1_G\}$ ise her $h \in H$ ve $H \cap K=\{1_G\}$ ise her $h \in H$ ve her $k \in K$ için $hk = kh$ olduğunu gösteriniz.

3) G bir grup ve $H \leq G, K \leq G$ olsun.

i. $H \lhd G$ ise $HK \leq G$ olduğunu gösteriniz.

ii. $H \lhd G, K \lhd G$ ise $HK \lhd G$ olduğunu gösteriniz.

4) $G = \{1, -1, i, -i\}$ çarpım grubunun $G = \{1, -1\}$ alt grubuna göre bölüm grubunu bulunuz.

5) **i.** G bir grup ise $M = \{g \in G \mid \forall a \in G$ için $ag = ga\}$ için $M \lhd G$ olduğunu gösteriniz

ii. G/M devresel ise G nin komütatif olduğunu gösteriniz.

6) G bir grup ve $H \leq G$ ise $K = \bigcap_{g \in G} gHg^{-1}$ $için$ $K \lhd G$ olduğunu gösteriniz.

7) G bir grup ve $a \in G$ için $< a > \leq N_G(a)$ olduğunu gösteriniz.

7. Gruplarda Homomorfizma ve İzomorfizma Teoremleri

Bu bölüme geçmeden önce, temel tanım ve teoremleri hatırlayalım;

K ve K' gibi iki cebirsel yapı (her ikisi de tek ya da her ikisi de çift işlemli) verilmiş olsun. K yı K' içine resmeden ve işlemlerin sonucunu koruyan (K nın iki elemanının toplamını bunların resimlerinin toplamına, çarpımını bunların resimlerinin çarpımına götüren) bir φ tasvirine içine bir homomorfi denir. Doğal olarak, φ homomorfisi K yı K' içine resmeder. K nın elemanlarının, φ homomorfisindeki resimlerinin kümesi olan $\varphi(K)$ ya K nın homomorf resmi adı verilir.

Buna göre φ homomorfisi, K yı $\varphi(K)$ üzerine resmeder.

φ, tek işlemli $< K, \mathrm{o} >$ cebirsel yapısını, tek işlemli $< K,* >$ cebirsel yapısı içine resmeden bir homomorfi ise her $a, b \in K$ için

$$\varphi: K \to K'$$

$$a \to \varphi(a)$$

$$b \to \varphi(b)$$

$$a\mathrm{o}b \to \varphi(a\mathrm{o}b) = \varphi(a) * \varphi(b) \text{ dır.}$$

φ, bir K cebirsel yapısından bir K' cebirsel yapısına bir homomorfi olsun.

φ üzerine bir tasvir ise, φ ye K dan K' ye bir **üzerine homomorfi** denir.

Bu durumda K', K nın homomorf resmidir, yani $\varphi(K) = K'$ dir. φ bir birebir tasvir ise φ ye

K dan K' ye bir **içine izomorfi**, φ üzerine ve birebir bir tasvir ise φ ye, K dan K' ye bir **izomorfi** denir. K dan K' içine bir izomorfi varsa, K, K' **içine yatırılmış** denir. K dan K' ye bir izomorfi varsa, K ve K' cebirsel yapıları **birbirine izomorftur** denir ve $K \cong K'$ yazılır. K dan kendi içine bir homomorfiye bir **endomorfi** (ya da ***K* nın bir endomorfisi**) denir. K nın kendi üzerine bir izomorfisine bir **otomorfi** (ya da K nın bir **otomorfisi**) denir.

Teorem 7.1: A ve B, tek işlemli iki cebirsel yapı ve $\varphi: A \rightarrow B$ bir homomorfi olsun. φ nin üzerine olması halinde, A bir grup ise B de bir gruptur.

İspat:

i. **Kapalılık:**

Her $b_1, b_2 \in B$ için $b_1 b_2 \in B$ dir:

φ üzerine olduğundan, $\varphi(a_1) = b_1$, $\varphi(a_2) = b_2$ olacak biçimde $a_1, a_2 \in A$ elemanları vardır.

A bir grup olduğundan $a_1 a_2 \in A$ dır. $\varphi(a_1 a_2) \in B$ ve φ bir homomorfi olduğundan $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2) = b_1 b_2 \in B$ dir.

ii. **Asosyatiflik:**

Her $b_1, b_2, b_3 \in B$ için $b_1(b_2 b_3) = (b_1 b_2) b_3$ dir:

φ üzerine olduğundan, $\varphi(a_1) = b_1$, $\varphi(a_2) = b_2$, $\varphi(a_3) = b_3$ olacak biçimde $a_1, a_2, a_3 \in A$ elemanları vardır ve A bir grup olduğundan $a_1(a_2 a_3) = (a_1 a_2) a_3$ dir.

Buna göre,

$$\varphi(a_1(a_2 a_3)) = \varphi((a_1 a_2) a_3) \Rightarrow \varphi(a_1)\varphi(a_2 a_3) = \varphi(a_1 a_2) a_3 \Rightarrow \varphi(a_1)\big(\varphi(a_2)\varphi(a_3)\big)$$
$$= \big(\varphi(a_1)\varphi(a_2)\big)\varphi(a_3) \Rightarrow b_1(b_2 b_3) = (b_1 b_2) b_3$$

elde edilir.

iii. **Birim Eleman:**

Her $b \in B$ için $b 1_B = 1_B b = b$ olacak şekilde $1_B \in B$ vardır:

φ üzerine olduğundan, her $b \in B$ için $\varphi(a) = b$ olacak biçimde $a \in A$ elemanı vardır ve $1_A \in A$ için $\varphi(1_A) \in B$ ve $a 1_A = 1_A a = a$ olduğundan

$$\varphi(a 1_A) = \varphi(1_A a) = \varphi(a) \Rightarrow \varphi(a)\varphi(1_A) = \varphi(1_A)\varphi(a) = \varphi(a) \Rightarrow b\varphi(1_A) = \varphi(.1_A) b = b$$

yani $\varphi(1_A) = 1_B$ dir.

iv. Ters Eleman:

Her $b \in B$ için $bb^{-1} = b^{-1}b = 1_B$ olacak biçimde $b^{-1} \in B$ vardır:

$a \in A$ için $\varphi(a) = b$ olsun. $a^{-1} \in A$ için $\varphi(a^{-1}) \in B$ ve $aa^{-1} = a^{-1}a = 1_A$ olduğundan, $b\varphi(a^{-1}) = \varphi(a^{-1})b = 1_A \Rightarrow b^{-1} = \varphi(a^{-1})$, yani her $a \in A$ için $\varphi\left(a^{-1}\right) = \varphi(a)^{-1}$ dir.

Böylece A bir grup ise B nin de bir grup olduğu gösterilmiş olur.

Not 7.1: φ homomorfisi üzerine olmasa da, her $a \in A$ için $\varphi\left(a^{-1}\right) = \varphi(a)^{-1}$ dir.

Sonuç 7.1: A, B iki grup ve $\varphi\colon A \to B$ bir homomorfi olsun. $H \leq A$ ise $\varphi(H) \leq B$ dir.

İspat:

Her $b_1, b_2 \in \varphi(H)$ için, $\varphi(a_1) = b_1$, $\varphi(a_2) = b_2$ olacak biçimde $a_1, a_2 \in H$ elemanları vardır ve $a_1, {a_2}^{-1} \in H$ olduğundan $\varphi(a_1, {a_2}^{-1}) \in \varphi(H)$ dır.

$$\varphi(a_1 {a_2}^{-1}) = \varphi(a_1)\varphi({a_2}^{-1}) = \varphi(a_1)\varphi(a_2)^{-1} = b_1 {b_2}^{-1} \in \varphi(H)$$

olduğundan $H \leq A$ ise $\varphi(H) \leq B$ dir.

Teorem 7.2 (Cayley Teoremi): Her grup uygun bir transformasyon grubuna izomorftur.

İspat:

G bir grup ve $a \in G$ belirli bir eleman olsun. $\varphi_a\colon G \to G$; $\varphi_a(g) = ga$ tasvirini göz önüne alalım;

Her $x \in G$ için $x = ga$ olacak biçimde bir $g \in G$ bulunabileceğinden, φ_a üzerinedir ve $g, h \in G$ olmak üzere $ag = ah \Rightarrow g = h$ olacağından φ_a $(1-1)$ dir.

Buna göre φ_a, G nin bir transformasyonudur. G nin bu tip bütün transformasyonları kümesi T_r ile gösterilirse, $T_r(G) = \{\varphi_a \mid a \in G\}$ dir ve $\varphi_a, \varphi_b \in T_r(G)$ olmak üzere, her $g \in G$ için

$$(\varphi_a \varphi_b)(g) = \varphi_a\left(\varphi_b(g)\right) = \varphi_a(bg) = a(bg) = (ab)g$$

yani $\varphi_a \varphi_b = \varphi_{ab}$ dir. Buna göre $T_r(G)$ kümesi çarpma işlemine göre kapalıdır.

G yi $T_r(G)$ içine resmeden $\varphi_a: G \to T_r(G)$; $\varphi(a) = \varphi_a$ tasvirini ele alalım;

Doğal olarak φ tasviri üzerinedir ve $a, b \in G$ olmak üzere $a \neq b$ için $\varphi_a = \varphi_b$ olsa, her $g \in G$ için $ag = bg \Rightarrow a = b$ çelişkisi ortaya çıkar, yani φ $(1-1)$ dir. Üstelik, her $a, b \in G$ için

$$\varphi(ab) = \varphi_{ab} = \varphi_a \varphi_b = \varphi(a)\varphi(b)$$

olduğundan φ işlemi korur. O halde, φ bir izomorfidir. **Teorem7.1** e göre G bir grup olduğundan $T_r(G)$ de bir gruptur.

Sonuç 7.2: G sonlu bir grup ve $G = \{a_1, a_2, \dots, a_n\}$ ise bir $T = \{\varphi_a \mid a \in G\}$ permütasyon grubudur ve her $a \in G$ için

$$\varphi_a = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ aa_1 & aa_2 & \dots & aa_n \end{pmatrix}$$

biçimindedir.

Örnek 7.1: $\mathbb{Z}_5^* = \mathbb{Z}_5 - \{\bar{0}\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ çarpım grubu için

$$\varphi_1 = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \overline{1.1} & \overline{1.2} & \overline{1.3} & \overline{1.4} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{1} & \bar{2} & \bar{3} & \bar{4} \end{pmatrix}$$

$$\varphi_2 = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \overline{2.1} & \overline{2.2} & \overline{2.3} & \overline{2.4} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{2} & \bar{4} & \bar{1} & \bar{3} \end{pmatrix}$$

$$\varphi_3 = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \overline{3.1} & \overline{3.2} & \overline{3.3} & \overline{3.4} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{3} & \bar{1} & \bar{4} & \bar{2} \end{pmatrix}$$

$$\varphi_4 = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \overline{4.1} & \overline{4.2} & \overline{4.3} & \overline{4.4} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{4} & \bar{3} & \bar{2} & \bar{1} \end{pmatrix}$$

olacağından, Cayley teoreminden dolayı,

$$\varphi(\bar{1}) = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{1} & \bar{2} & \bar{3} & \bar{4} \end{pmatrix},$$

$$\varphi(\bar{2}) = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{2} & \bar{4} & \bar{1} & \bar{3} \end{pmatrix},$$

$$\varphi(\bar{3}) = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{3} & \bar{1} & \bar{4} & \bar{2} \end{pmatrix},$$

$$\varphi(\bar{4}) = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{4} & \bar{3} & \bar{2} & \bar{1} \end{pmatrix}$$

dir. Buna göre $\mathbb{Z}_5^*$ grubu, $\{I, (1243), (1342), (14)(23)\}$ permütasyon grubuna izomorftur.

Teorem 7.3: G bir grup ve $a \in G$ belirli bir elemanı olmak üzere,

$$\Psi_a : G \to G;\ \Psi_a(g) = aga^{-1}$$

tasviri bir otomorfidir.

İspat:

i. Ψ_a tasviri üzerinedir: $x \in G$ için $x = aga^{-1}$ olacak biçimde bir $g \in G$ vardır ve $g = a^{-1}xa$ dır.

ii. Ψ_a tasviri $(1-1)$ dir: Her $g, h \in G$ için $aga^{-1} = aha^{-1} \Rightarrow g = h$ dır.

iii. Ψ_a tasviri işlemi korur: Her $g, h \in G$ için

$$\Psi_a(gh) = agha^{-1} = ag(\underbrace{aa^{-1}}_{1_G})ha^{-1} = (aga^{-1})(aha^{-1}) = \Psi_a(g)\Psi_a(h)$$

dır.

Tanım 7.2: $\Psi_a: G \to G;\ \Psi_a(g) = aga^{-1}$ otomorfisine G nin bir **iç otomorfisi** denir.

Teorem 7.4: Bir G grubunun bütün iç otomorfileri kümesi tasvir çarpımına göre bir gruptur.

Not 7.2: G grubu komütatif ise her $a \in G$ ve her $g \in G$ için aga^{-1} olacağından G nin tek iç otomorfisi I_G idantik otomorfisidir ve $I(G) = \{I_G\}$ şeklinde ifade edilir.

Örnek 7.2: $S_{13} = \{I, (12), (13), (23), (123), (132)\}$ grubunun Ψ_1 dışındaki iç otomorfileri aşağıdaki gibidir:

$\Psi_{(12)}: S_3 \to S_3$	$\Psi_{(13)}: S_3 \to S_3$	$\Psi_{(23)}: S_3 \to S_3$
$(12) \to (12)$	$(12) \to (23)$	$(12) \to (13)$
$(13) \to (23)$	$(13) \to (13)$	$(13) \to (12)$
$(23) \to (13)$	$(23) \to (12)$	$(23) \to (23)$
$(123) \to (132)$	$(123) \to (132)$	$(123) \to (132)$
$(132) \to (123)$	$(132) \to (123)$	$(132) \to (123)$

$\Psi_{(123)}: S_3 \to S_3$
$(12) \to (23)$
$(13) \to (12)$
$(23) \to (13)$
$(123) \to (123)$
$(132) \to (132)$

$\Psi_{(132)}: S_3 \to S_3$
$(12) \to (13)$
$(13) \to (23)$
$(23) \to (12)$
$(123) \to (132)$
$(132) \to (123)$

Teorem 7.5: A, B iki grup ve $\varphi: A \to B$ bir homomorfi ise aşağıdaki iddialar doğrudur:

i. 1_B nin φ deki tam orijinaller kümesi, A nın N gibi bir normal alt grubudur. $(N \trianglelefteq A)$

ii. B nin herhangi bir a' elemanının φ deki tam orijinaller kümesi boş değilse, N nin A içindeki uygun bir kalan sınıfıdır.

iii. φ üzerine ise, A/N bölüm grubu B grubuna izomorftur. $(A/N \cong B$)

İspat:

i. $\varphi^{-1}(1_B) = N$ olsun. Bu durumda $N = \{a \in A \mid \varphi(a) = 1_B\}$ yazılır.
Burada, her $a, b \in N$ için

$$\varphi(a) = \varphi(b) = 1_B$$

ve φ çarpımı koruduğu için

$$\varphi(ab) = \varphi(a)\varphi(b) = 1_B 1_B = 1_B \text{ dir.}$$

O halde, $a.b \in N$ elde edilir.

Her $a \in N$ için,

$$\varphi(a) = \varphi(a^{-1}) = \varphi(a)^{-1} = 1_{B^{-1}} = 1_B$$

olduğundan $a^{-1} \in N$ dir.

Buna göre, **i.** ve **ii.** den $N \leq A$ elde edilir.

Her $a \in A$ ve her $n \in N$ için,

$$\varphi(ana^{-1}) = \varphi(a)\varphi(n)\varphi(a^{-1}) = \varphi(a)1_B\varphi(a)^{-1} = 1_B$$

olduğundan, $ana^{-1} \in N$ ve dolayısıyla $N \trianglelefteq A$ dir.

ii.B nin herhangi bir a' elemanının φ deki tam orijinaller kümesi $\varphi(a') = M_{a'}$ olsun. $M_{a'} \neq \emptyset$ olduğundan, $\varphi(a) = a'$ olacak biçimde bir $a \in A$ vardır. aN kalan sınıfını göz önüne alalım.

Her $b \in aN$ için, $b = an$ olacak biçimde bir $n \in N$ vardır. Buna göre,

$$\varphi(b) = \varphi(an) = \varphi(a)\varphi(n) = a'1_B = a'$$

olduğundan $b \in M_{a'}$ yani $aN \subset M_{a'}$ dür. Öte yandan, her $d \in M_{a'}$ için $M_{a'} \subset aN$ dir.

Sonuç olarak, $aN = M_a$ olduğu ortaya çıkar.

iii. A/N bölüm grubunu B içine resmeden $\Psi: aN \to \varphi(a)$ tasvirinin göz önüne alalım.

1) Ψ iyi tanımlıdır: Çünkü $aN = bN$ ise

$$(a^{-1}b)N = N \Rightarrow a^{-1}b \in N$$

dir. Buna göre $\varphi(a^{-1}b) = 1_B$, yani $\varphi(a^{-1})\varphi(b) = \varphi(a)^{-1}\varphi(b) = 1_B$ dir.

O halde, $\varphi(a) = \varphi(b)$ dir.

2) Ψ üzerinedir: Çünkü φ üzerine olduğundan her $b' \in B$ elemanına karşılık, $\varphi(b) = b'$ olacak biçimde bir $b \in B$ elemanı vardır ve $\Psi(bN) = \varphi(b) = b'$ dir.

3) Ψ $(1-1)$ dir: Çünkü herhangi iki aN, bN kalan sınıfı için $aN \neq bN$ iken $\Psi(a) = \Psi(b)$ ise

$$\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) = \varphi(b)^{-1}\varphi(b) = 1_B$$

olur ki, buradan $a^{-1}b \in N$ dolayısıyla $b \in aN$ ve $b \in aN \cap bN$ elde edilir.

Oysa $aN \neq bN$ olduğundan $aN \cap bN = \emptyset$ dir.

4) Ψ çarpımı korur: Çünkü,

$$\Psi(aNbN) = \Psi\big((ab)N\big) = \varphi(ab) = \varphi(a)\varphi(b) = \Psi(aN)\Psi(bN) \text{ dir.}$$

O halde $A/N \cong B$ dir.

Tanım 7.3: Teorem 7.5 de ifade edilen N normal alt grubuna φ **homomorfisinin çekirdeği** denir ve $\boldsymbol{Ker\varphi}$ ile gösterilir. Buna göre $\varphi: A \to B$ bir grup homomorfisi ise

$$Ker\varphi = \{a \in A;\ \varphi(a) = 1_B\}$$

yazılır.

Örnek 7.3: A bir komütatif grup ise $\varphi: G \to G;\ \varphi(g) = g^n\ (n \in N)$ tasvirini göz önüne alalım,

$$\forall g, h \in G \text{ için } \varphi(gh) = (gh)^n = g^n h^n = \varphi(g)\varphi(g)$$

olduğundan φ bir homomorfidir ve $g \in G$ için

$$\varphi(g) = 1_G \Leftrightarrow g^n = 1_G \Leftrightarrow |g| \mid n$$

olduğundan $Ker\varphi = \{g \in G \mid |g| \mid n\}$ dir.

Sonuç 7.3: $\varphi: A \to B$ grup homomorfisinin bir izomorfi olabilmesi için gerek ve yeter koşul $Ker\varphi = \{1_A\}$ olmasıdır.

Teorem 7.6: G bir grup ve $N \trianglelefteq G$ ise $\mu: a \to aN$ tasviri G nin G/N üzerine bir homomorfisidir ve $N < H < G$ ise $\mu(H) = H/N < G/N$ olduğu gibi $\bar{H} < G/N$ ise $H = \{g \mid gN \in \bar{H}\}$ için $H < G$ dir.

Tanım 7.4: $\mu: a \to aN$ homomorfisine, G nin N normal alt grubuna göre **doğal (kanonik) homomorfisi** denir.

Teorem 7.7 (Birinci İzomorfi Teoremi): φ, A grubunun B grubu içine bir homomorfisi ise $Ker\varphi$, A nın bir normal alt grubudur ve $\Psi: aN \to \varphi(a)$ tasviri $A/Ker\varphi$ bölüm grubunun B nin $\varphi(A)$ alt grubuna bir izomorfisidir.

Teorem 7.8 (İkinci İzomorfi Teoremi): G bir grup, $N \trianglelefteq G\ ve\ H \leq G$ ise,

$H \cap N \trianglelefteq H, HN \leq G\ ve\ H/H \cap N \cong HN/N\ dir.$

İspat: Burada $HN = \{ab \mid a \in H, b \in N\} \subset G$ olduğunu biliyoruz.

$n \in H \cap N\ ve\ h \in H\ ise\ N \trianglelefteq G\ olduğundan\ h^{-1}nh \in H$ dir.

Dolayısıyla $h^{-1}nh \in H \cap N$ yani $H \cap N \trianglelefteq H\ dır.$

$HN \neq \emptyset$ olduğu açıktır. Üstelik her $x, y \in HN$ için, $x = ab, y = cd$ $(a, c \in H, b, d \in N)$ ise

$xy^{-1} = (ab)(cd)^{-1} = abd^{-1}c^{-1}$, $t = bd^{-1} \in N \Rightarrow xy^{-1} = atc^{-1}$, $c^{-1}\ c = 1_G$

olduğundan,

$$xy^{-1} = a\,c^{-1}.ctc^{-1}, ac^{-1} \in H\ ve\ N \trianglelefteq G \Rightarrow c\,tc^{-1} \in N \Rightarrow xy^{-1} \in HN$$

$$HN \leq G$$

elde edilir.

$\varphi : H \to HN/N$; $\varphi(h) = hN$ tasviri iyi tanımlı ve üzerine bir tasvirdir. Gerçektende,

$$\varphi(h_1h_2) = h_1h_2N = h_1\,N\,h_2N = \varphi(h_1)\,\varphi(h_2)$$

olduğundan φ bir üzerine homomorfidir. Üstelik $xN = N\ ise\ x \in N$ olduğundan,

$$Ker\varphi = \{x \mid x \in H\ ve\ x \in N\} = H \cap N$$

dir. Birinci izomorfi teoremine göre $H/H \cap N \cong HN/N$ olmak zorundadır.

Şimdi, gruplarda homomorfi ve izomorfi teoremlerinden elde edilebilen aşağıdaki sonuçlara bakalım.

Sonuç 7.4: Bir devresel grubun her homomorf resmi de bir devresel gruptur.

İspat: $A = < a >$ devresel grubunu göz önüne alalım ve B de A nın bir φ homomorfisindeki resmi olsun. Bu taktirde **Teorem 7.1** den, B de bir gruptur.

$\varphi(a) = b$ olarak alındığında, her $x \in B$ için $\varphi(a^k) = x$ olacak biçimde bir $a^k \in A$,$(k \in Z)$ vardır. Buna göre,

$$\varphi(a^k) = x \Rightarrow \varphi(a)^k = x \Rightarrow x = b^k \Rightarrow B = < b > = < \varphi(a) > \text{ dir.}$$

Sonuç 7.5: Sonlu bir devresel grubun her homomorf resmi de sonlu bir devresel gruptur.

İspat: $A \; =< a > , n.$ mertebeden bir devresel grup ve $B \; de \; A$ nın bir φ homomorfisindeki resmi ise $B =< \; \varphi(a) > =< b >$ dir. Öte yandan, $a^n = 1_A$olduğundan,

$$\varphi(a^n) = \varphi(1_A) = \varphi(a\,)^n = 1_B \Rightarrow \; b^n = 1_B$$

elde edilir.Yani, B nin mertebesi n in bir bölenidir; B sonludur.

Sonuç 7.6:

i. Sonsuz bir devresel grubun her izomorf resmi de sonsuz bir devresel gruptur.

ii. n. mertebeden bir devresel grubun her izomorf resmi de n. mertebeden bir devresel gruptur.

İspat:

$A \; =< a >$ bir devresel grup ve B de A nın bir φ izomorfisindeki resmi ise

$$B \; =< \; \varphi(a) > =< b > \; \text{dir.}$$

i. A sonsuz olsun. Şimdi, $k \neq t \; (k, t \in Z) için \;\; b^k = b^t$ olduğunu varsayalım.

$\varphi(a)^k \; = \; \varphi(a)^t \; \Rightarrow \; \varphi(a^k) = \; \varphi(a^t)$ ise φ , $(1-1)$ olduğundan $a^k = a^t$ elde edilir.

Oysa A sonsuz olduğundan, $her \; k \neq t \; (k, t \in Z)$ için $a^t \; \neq a^k$ dir. O halde B de sonsuzdur.

ii. $|\mathrm{A}| = \mathrm{n}$ olsun. Bu durumda, $b^n = 1_B$ dir. Öte yandan, $1 \leq t \leq n \; (t \in Z)$ için $b^t = 1_B$olsa $\varphi(a)^t = \varphi(1_A) \Rightarrow \varphi(a^t) = \varphi(1_A)$ elde edilir.

φ, $(1-1)$ olduğundan $a^t = 1_A$ sonucuna varılır. Bu ise a nın mertebesinin *n* olmasıyla çelişir.

O halde, $A = \{1_A, a, \dots, a^{n-1}\}$ ise $B = \{1_B, b, \dots, b^{n-1}\}$ dir.

Sonsuz bir devresel grubun her homomorf resminin de sonsuz bir devresel grup olması gerekmez. Örneğin, $Z = < 1 >$ sonsuz devresel toplam grubu ve $\{0\}$ toplam grubu için $\varphi: Z \to \{0\}\,;\ \varphi(t) = 0$ tasviri bir üzerine homomorfidir.

Teorem 7.9: G bir grup, $N \trianglelefteq G$ ve $N \leq K \leq G$ ise $N \trianglelefteq K$ ve $K/N \leq G/N$ dir. Ayrıca $N \leq K \trianglelefteq G$ ise K/N ⊴ G/N dir. Tersine G/N nin alt grupları, $N \leq K \leq G$ olmak üzere K/N biçiminde ve normal alt grupları $N \leq K \trianglelefteq G$ olmak üzere K/N biçimindedir.

İspat: $N \trianglelefteq G$ ve $N \leq K \leq G$ ise $N \trianglelefteq K$ dır ve K/N in her kN $(k \in K)$ elemanı için $k \in G$ olacağından $K/N \leq G/N$ dır. K⊲G ise her $g \in G$ ve her $k \in K$ için $gkg^{-1} \in K$ dır. Buna göre her $gN \in G/N$ ve $kN \in K/N$ için $(gN)(kN)(gN)^{-1} = (gkg^{-1})N$ kalan sınıfı, K/N bölüm grubuna ait olacağından, $K/N \trianglelefteq G/N$ dir.

Tersine $[K] \leq G/N$ olması halinde $K = \{ g \in G \mid gN \in [K] \}$ alınabilir. Burada her $a, b \in K$ için $(aN)(bN)^{-1} = (ab^{-1})N \in [K]$ olduğundan, K nın tanımına göre $ab^{-1} \in K$ olmak zorundadır. Buna göre $K \leq G$ dir. Öte yandan, her $x \in N$ için $xN = N\ ve\ N \in [K]$ olduğundan $N \leq K$ dır. $[K] \trianglelefteq G/N$ ve $g \in G\,, k \in K\ için\ (gkg^{-1})N = (gN)(kN)(gN)^{-1} \in [K]$ dikkate alındığında, $gkg^{-1} \in K$ yani K ⊴ G dir.

Teorem 7.10 (Üçüncü İzomorfi Teoremi): G bir grup, $T \trianglelefteq G$ ve G/Tbölüm grubunun K/T gibi bir normal alt grubu olduğunu varsayalım. Bu durumda $K \trianglelefteq G$ ve $G/K \cong (G/T)/(K/T)$ dir.

İspat: $\varphi: G \to G/T$ ve $\delta: G/K \to (G/K)/(K/T)$ doğal homomorfilerinin göz önüne alalım.

φ ve δ üzerine olduklarından $\theta = \delta\varphi$: $g \to (gT)(K/T)$ bileşke tasviri G nin $(G/T)/(K/T)$ üzerine bir homomorfisidir. Burada $g \in Ker\theta$ ise

$$\theta(g) = K/T \Rightarrow (gT)(K/T) = K/T \Rightarrow gT \in K/T \Rightarrow \exists k \in K;\ gT = kT$$

dir. Yani bir $t \in T$ için $g = kt$ dir ve $T \subseteq K$ olduğundan,

$$g \in K \Rightarrow Ker\theta \subseteq K$$

dır. Öte yandan $g \in K$ ise $gT \in K/T$ olacağından, $\theta(g) = (gT)(K/T) = K/T$ yani

$$g \in Ker\theta \Rightarrow K \subseteq Ker\theta$$

elde edilir. Sonuç olarak $Ker\theta = K$ olduğu görülür. Buna göre, $K \trianglelefteq G$ ve $G/K \cong (G/T)/(K/T)$ dir.

Örnek 7.4:

$G = \mathbb{Z}_{24}$, $H = <\bar{4}>$ ve $K =<\bar{8}>$ ise

$$G/H = \mathbb{Z}_{24}/<\bar{4}>= \{<\bar{4}>, \bar{1}+<\bar{4}>, \bar{2}+<\bar{4}>, \bar{3}+<\bar{4}>\} \cong \mathbb{Z}_4$$

ve

$$G/K = \mathbb{Z}_{24}/<\bar{8}>= \{<\bar{8}>, \bar{1}+<\bar{8}>, \bar{2}+<\bar{8}>, \bar{3}+<\bar{8}>, \bar{4}+<\bar{8}>, \bar{5}+<\bar{8}>, \bar{6}+<\bar{8}>, 7+<\bar{8}>\} \cong \mathbb{Z}_8$$

dir, bundan başka

$$H/K =<\bar{4}>/<\bar{8}>= \{<\bar{8}>, \bar{4}+<\bar{8}>\} \cong \mathbb{Z}_2$$

dir.

Böylece,

$$(G/K)/(H/K) \cong G/H \cong \mathbb{Z}_4$$

elde edilir.

Örnek 7.5:

$G = \mathbb{Z}$ grubu ve $H = 2\mathbb{Z}$ ve $K = 8\mathbb{Z}$ alt grupları dikkate alındığında

$$G/H = \mathbb{Z}/2\mathbb{Z} = \{2\mathbb{Z}, 1 + 2\mathbb{Z}\} \cong \mathbb{Z}_2,$$

$G/K = \mathbb{Z}/8\mathbb{Z} = \{8\mathbb{Z}, 1 + 8\mathbb{Z}, 2 + 8\mathbb{Z}, 3 + 8\mathbb{Z}, 4 + 8\mathbb{Z}, 5 + 8\mathbb{Z}, 6 + 8\mathbb{Z}, 7 + 8\mathbb{Z}\} \cong \mathbb{Z}_4$ dir.

Üstelik

$$H/K = 2\mathbb{Z}/8\mathbb{Z} = \{8\mathbb{Z}, 2 + 8\mathbb{Z}, 4 + 8\mathbb{Z}, 6 + 8\mathbb{Z}\} \cong \mathbb{Z}_4$$

olduğundan

$$(G/K)/(H/K) \cong G/H \cong \mathbb{Z}_2$$

dir.

7.1 Direkt Çarpımlar

Verilen gruplardan yeni gruplar elde etmek için bu grupların kartezyen çarpımları dikkate alınabilir. Bu yöntem abelyen gruplara uygulanırsa; abelyen grupların tüm yapısal özelliklerini bulunduran daha geniş bir sınıf elde edilir.

Teorem 7.1.1: H ve K iki grup olmak üzere, $H \times K = \{(x, y) \mid x \in H, y \in K\}$ kümesi,

$$(x, y), (u, v) \in H \times K \text{ için } (x, y).(u, v) = (xu, yv)$$

şeklinde tanımlanan " $\cdot$ " işlemine göre bir gruptur.

İspat: $(1_H, 1_K) \in H \times K$ olduğundan, $H \times K$ nın boş kümeden farklı olduğunu görmek kolaydır. Öte yandan,

1) $\forall (x, y), (u, v) \in H \times K$ için $(x, y).(u, v) = (\underbrace{xu}_{\in H}, \underbrace{yv}_{\in K}) \in H \times K$ dır.

2) $\forall (x, y), (u, v), (k, r) \in H \times K$ için

$$(x, y)[(u, v).(k, r)] = (x, y)(uk, vr) = \big(x(uk), y(vr)\big) = \big((xu)k, (yv)r\big) = (xu, yv).(k, r) = [(x, y).(u, v)].(k, r) \text{ dir.}$$

$\forall (x, y) \in H \times K \quad (1_H, 1_K).(x, y) = (x, y).(1_H, 1_K) = (x, y)$ dir.

3) $\forall (x, y) \in H \times K$ için $(x, y).(x^{-1}, y^{-1}) = (x^{-1}, y^{-1})(x, y) = (1_H, 1_K)$ dir.

Sonuç olarak, $< H \times K, \cdot >$ cebirsel yapısının grup olduğunu söyleyebiliriz.

$H \times K$ grubuna, H ve K gruplarının **dolaysız çarpımı** ya da **direkt çarpımı** denir. Üstelik, $|H \times K| = |H|.|K|$ dir.

Genelleştirme: $G_1, G_2, \dots, G_n$ birer grup ve

$$G = \prod_{i=1}^{n} G_i$$

olmak üzere $< G, \cdot >$ grubuna $G_1, G_2, \dots, G_n$ gruplarının direkt çarpımı denir. Üstelik,

$$|G_1 \times G_2 \times \ldots \times G_n \,| = |G_1|.\,|G_1| \ldots |G_n|$$

dir.

Tanım 7.1.1: $G_1, G_2, \ldots, G_n$ grupları birer toplamsal grup ise

$G = \bigoplus_{i=1}^{n} G_i$ toplamsal grubuna $G_1, G_2, \ldots, G_n$ gruplarının direkt toplamı denir.

$$G = \bigoplus_{i=1}^{n} G_i$$

gösterimi yerine

$$G = \prod_{i=1}^{n} G_i$$

sembolü kullanılır.

Örnek 7.1.1: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1})\}$ mertebesi 4 olan bir abelyen gruptur.

$(\bar{0},\bar{0})$ nin dışında her elemanın mertebesi 2 olduğundan, $\mathbb{Z}_2 \times \mathbb{Z}_2$ grubuna izomorf değildir.

$\mathbb{Z}_3 \times \mathbb{Z}_3$ grubunun da devresel olmadığını başka ifadeyle, $\mathbb{Z}_9$ a izomorf olmadığını görmek kolaydır.

Not 7.1.1: G_1 ve G_2 gruplarının direkt çarpımı $G = G_1 \times G_2$, ${G_1}^*$ ve ${G_2}^*$ gruplarının direkt çarpımı da $G^* = {G_1}^* \times {G_2}^*$ olsun.

$G_1 \cong {G_1}^*$ ve $G_2 \cong {G_2}^*$ ise $G \cong G^*$ dır. Gerçektende, $G_1 \cong {G_1}^*$ ve $G_2 \cong {G_2}^*$ olduğundan $\Phi_1: G_1 \to {G_1}^*$ ve $\Phi_2: G_2 \to {G_2}^*$ izomorfileri yardımıyla, $\Phi: G \to G^*$, her $g = (g_1, g_2) \in G$ için $\Phi\big((g_1, g_2)\big) = \Phi(g) = \Phi(\Phi_1(g_1), \Phi_2(g_2))$ olarak tanımlanan Φ dönüşümü bir izomorfidir.

$G_1, \dots, G_n$ birer grup ve

$$G = \prod_{i=1}^{n} G_i$$

olmak üzere $g = (g_1, \dots, g_n) \in G$ sonlu mertebeli ise her $1 \le i \le n$ için $g_i \in G$ sonlu mertebelidir. Gerçektende, $g \in G$ elemanının mertebesi k ise $g^k = 1_G = ({g_1}^k, \dots, {g_n}^k)$ ve $1_G = (1_{G_1}, \dots, 1_{G_n})$ olduğundan her $1 \le i \le n$ için ${g_i}^k = 1_{G_i} \in G_i$ ve dolayısıyla her $1 \le i \le n$ için $g_i \in G_i$ sonlu mertebelidir.

Tersine, her $1 \le i \le n$ için $g_i \in G_i$ elemanı sonlu mertebeli ise $g \in G$ de sonlu mertebelidir.

Teorem 7.1.2: Her $i = 1,2, \dots, n$ için G_i birer grup ve

$$G = \prod_{i=1}^{n} G_i$$

olmak üzere $g = (g_1, g_2, \dots, g_n) \in G$ olsun. Her i için $g_i \in G_i$ elemanlarının mertebesi sonlu ve mertebeleri m_i ise g elemanlarının mertebesi sonludur ve üstelik $|g| = [m_1, m_2, \dots, m_n]$ dir.

Teorem 7.1.3: $m, n \in \mathbb{Z}$ olmak üzere $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ olması için gerek ve yeter koşul

$(m, n) = 1$ olmasıdır.

İspat:

$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ olmak üzere, tersine $(m, n) = d > 1$ olsun. $(m, n) = d$ ise $d|m$ ve $d|n$ dir.

$d|m$ ve $d|n \Rightarrow \exists u, v \in \mathbb{Z} \ni m = d.u$ ve $n = d.v \Rightarrow \frac{mn}{d} = \frac{d.u.d.v}{d} = d(u.v)$

$d.u.v = m.v = n.u \Rightarrow m|\frac{mn}{d}$ ve $n|\frac{mn}{d}$ dir.

O halde, her $(\bar{x}, \bar{y}) \in \mathbb{Z}_m \times \mathbb{Z}_n$ için $(\bar{x}, \bar{y}) \underbrace{+ \cdots +}_{\frac{mn}{d}\, tane} (\bar{x}, \bar{y}) = (\bar{0}, \bar{0})$ dir.

Dolayısıyla, $\mathbb{Z}_m \times \mathbb{Z}_n$ grubunun hiçbir $(\bar{x}, \bar{y})$ elemanı $\mathbb{Z}_m \times \mathbb{Z}_n$ grubunu üretemez. Bu da $\mathbb{Z}_m \times \mathbb{Z}_n$ grubunun devirli olmasıyla çelişir. Dolayısıyla, $(m, n) = 1$ dir.

Diğer yandan, $(m, n) = 1$ olsun;

$[m, n] = mn,\ \mathbb{Z}_m =< \bar{x} >, \mathbb{Z}_n =< \bar{y} >$ ve $|\bar{x}| = o(\bar{x}), |\bar{y}| = o(\bar{y})$ ise,

$O\big((\bar{x}, \bar{y})\big) = [O(\bar{x}), O(\bar{y})] = [m, n] = mn$ olduğundan $(\bar{x}, \bar{y})$ elemanı $\mathbb{Z}_m \times \mathbb{Z}_n$ grubunu üretir. $\mathbb{Z}_m \times \mathbb{Z}_n$ grubu devirlidir. $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$ ve $\mathbb{Z}_m \times \mathbb{Z}_n$ devirli ise $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ dir.

Sonuç 7.1.1:

$$\prod_{i=1}^{n} \mathbb{Z}_{m_i} \cong \mathbb{Z}_{m_1 m_2 \dots m_n}$$

olması için gerek ve yeter koşul $i = 1,2, \dots, n$ için m_i sayılarının ikişer ikişer aralarında asal olmasıdır.

Sonuç 7.1.2: $G_1, G_2, \dots, G_n$ sonlu devirli gruplar olmak üzere, $G_1, \times G_2 \times \dots \times G_n$ grubunun devirli olması için gerek ve yeter koşul $\big(O(G_1), O(G_2), \dots, O(G_n)\big) = 1$ olmasıdır.

Sonuç 7.1.3: $p_1, p_2, \dots, p_n$ birbirinden farklı asal sayılar, m= ${p_1}^{\propto_1}, {p_2}^{\propto_2}, \dots, {p_n}^{\propto_n}$ şeklinde yazılmış olsun.

$$\mathbb{Z}_{{p_1}^{\propto_1}} \times \mathbb{Z}_{{p_2}^{\propto_2}} \times \dots \times \mathbb{Z}_{{p_n}^{\propto_n}} \cong \mathbb{Z}_{{p_1}^{\propto_1} . {p_2}^{\propto_2} \dots {p_n}^{\propto_n}} = \mathbb{Z}_m$$

dir.

Örnek 7.1.2: $\mathbb{Z}_{10} \times \mathbb{Z}_{40} \times \mathbb{Z}_{36}$ grubunda, $(\bar{4}, \bar{7}, \bar{3})$ elemanının mertebesini belirleyiniz.

$|\bar{4}|_{\mathbb{Z}_{10}} = 5,\ |\bar{7}|_{\mathbb{Z}_{40}} = 40,\ |\bar{3}|_{\mathbb{Z}_{36}} = 12$ ise

$[5,40,12] = 120$ olduğundan, $|(\bar{4}, \bar{7}, \bar{3})|_{\mathbb{Z}_{10} \times \mathbb{Z}_{40} \times \mathbb{Z}_{36}} = 120$ dir.

Tanım 7.1.2: G bir grup, $H_1, \dots, H_n \trianglelefteq G$ olsun. Eğer, $H_1, \dots, H_n \trianglelefteq G$ alt grupları,

i. $G = H_1 . H_2 \dots . H_n$

ii. $1 \leq i, j \leq n$ olmak üzere, $i \neq j$ için $H_i \cap H_1 \dots H_{i-1} H_{i+1} \dots H_n = \{1_G\}$

koşullarını gerçekliyorsa, G grubuna, $H_1, \dots, H_n$ alt gruplarının iç direkt çarpımı denir.

Teorem 7.1.4: G bir grup, $H_1, \dots, H_n \trianglelefteq G$ olmak üzere, G, $H_1, \dots, H_n$ alt gruplarının iç direkt çarpımı olsun. Bu durumda, $G \cong H_1 \times \dots \times H_n$ dir.

İspat: G, $H_1, \dots, H_n$ alt gruplarının iç direkt çarpımı olduğuna göre, her $1 \leq i \leq n$ için $h_i \in H_i$ olmak üzere bir $g \in G$, $g = h_1, h_2, \dots, h_n$ şeklinde tek türlü yazılabilir. O halde,

$$\emptyset : G \to H_1 \times \dots \times H_n$$

$$g \to (h_1, h_2, \dots, h_n)$$

eşlemesi iyi tanımlıdır. Şimdi, $\emptyset$ nin bir izomorfi olduğunu gösterelim;

$g = h_1, h_2, \dots, h_n, k = k_1, k_2, \dots, k_n \in G$ için $1 \leq i, j \leq n$ olmak üzere, $i \neq j$ için

$H_i \cap H_1 \dots H_{i-1} H_{i+1} \dots H_n = \{1_G\}$ ve $H_i \trianglelefteq G$ olduğundan, $h_i k_i = k_i h_i$dir.

$\emptyset(gk) = \emptyset((h_1, h_2, \dots, h_n)(k_1, k_2, \dots, k_n)) = \emptyset((h_1 k_1) \dots (h_n k_n)) = (h_1 k_1, \dots, h_n k_n) = (h_1, h_2, \dots, h_n).(k_1, k_2, \dots, k_n) = \emptyset(g)\emptyset(k)$ dir.

Öte yandan, $\emptyset$ nin üzerine olduğunu görmek kolaydır. Sonuç olarak, $\emptyset$ tasvirinin bir üzerine homomorfi ve $Ker\emptyset = \{g \in G \mid \emptyset(g) = (1_G, \dots, 1_G)\}$ ile birlikte $g = h_1 h_2 \dots h_n$ olduğu düşünülürse,

$$\emptyset(g) = (h_1, h_2, \dots, h_n) = (1_G, \dots, 1_G)$$

dolayısıyla, $h_1 = h_2 = \cdots = h_n = 1_G$, $g = 1_G$ elde edilir. Demek ki, $Ker\emptyset = \{1_G\}$ dir.

Bu ise dönüşümün birebir olduğunu gösterir. Yani, $\emptyset$ bir izomorfidir ve $G \cong H_1 \times \ldots \times H_n$ dir.

7.2 Sonlu Abelyen Gruplar ve Temel Teoremi

Tanım 7.2.1: G bir grup, $\{g_i\colon \mid\ g \in G,\ i \in I\} \subseteq G$ olsun. Bu kümeyi kapsayan G grubunun tüm altgruplarının arakesiti, g_i elemanları tarafından üretilen alt grup olarak tanımlanmıştır. Eğer bu alt grup, G grubunun kendisi ise G grubuna, g_i elemanları tarafından üretilen grup denir. $\{g_i\colon \mid\ g \in G,\ i \in I\}$ sonlu bir küme ise G grubuna da sonlu üreteçli bir grup dendiğini biliyoruz.

$\mathbb{Z}, \mathbb{Z} \times \mathbb{Z}_n$ gruplarının sonlu olmadığı halde sonlu üreteçli gruplar olduğu aşikardır.

Öte yandan Q grubu sonlu üreteçli bir grup değildir.

Teorem 7.2.1: G bir grup, H, G grubunun $\{g_i\colon \mid\ g \in G,\ i \in I\}$ kümesiyle üretilmiş bir alt grup olsun. g_{i_k} birbirinden farklı olması gerekmeyen elemanlar olmak üzere, H nın her elemanı, $k_1, \ldots, k_n \in \mathbb{Z}$ için $h = {g_{i_1}}^{k_1} \ldots {g_{i_n}}^{k_n}$ biçimde yazılabilir.

Yani H altgrunun sözü edilen yukarıdaki alt kümenin kuvvet çarpımlarından oluşan cümle ile çakışır.

İspat: $K = \{{g_{i_1}}^{k_1} \ldots {g_{i_n}}^{k_n} \mid g_{i_1}, \ldots, g_{i_n} \in G, k_1, k_2, \ldots, k_n \in \mathbb{Z}\}$ kümesini göz önüne alalım. ${g_{i_k}}^0 = 1_G$ olduğundan, $K \neq \emptyset\ dir. H,$ bu kümeyi kapsayan en küçük altküme olduğuna göre

g_{i_k} elemanlarını ve bunların tüm mümkün kuvvet çarpımlarını da içermelidir

Kuvvet alma işlemleri dikkate alındığında, K kümesi kapalıdır:

$({g_{i_1}}^{k_1} \ldots {g_{i_n}}^{k_n})^{-1} = ({g_{i_n}}^{k_n})^{-1} \ldots \left({g_{i_n}}^{k_n}\right)^{-1} = {g_{i_n}}^{-k_n} \ldots {g_{i_1}}^{-k_1} \in$ K olduğundan,

$K \leq G$ dir. Diğer yandan H alt grubu g_i elemanını içeren en küçük alt grup olduğuna göre $K = H$ olmalıdır.

Bu bölümde her sonlu abelyen grubunun ya bir devirli gruba ya da bir takım devirli grupların direkt çarpımına izomorf olduğunu göstermeye çalışacağız. Bunun için bir sonraki bölümde detaylı biçimde incelenecek olan p-gruplarından kısaca bahsedelim;

p bir asal sayı olmak üzere, her elemanının mertebesi, p sayısının bir kuvveti olan gruplar ile ilgileneceğiz.

Teorem 7.2.2: p bir asal olmak üzere G sonlu bir abelyen grubu olsun. Bu durumda G grubu bir takım p-gruplarının iç direkt çarpımına izomorftur.

İspat: $|G|$ = 1 olması halinde teoremin ispatı açıktır.

$|G| > 1$ olsun. O halde;

$|G| = p_1^{r_1} \dots p_n^{r_n}$; $p_1, \dots, p_n$ asal sayılar, $r_1, \dots, r_n \in \mathbb{N}$ ve $k \in \mathbb{Z}$, $1 \le i \le n$ için

$G_i = \{g \in G \mid g^{p_i^k} = 1_G\}$ olacak şekilde alt kümeleri ele alalım.

$1_G^{p_i^k} = 1_G$ olduğundan, $1_G \in G_i$ dir. O halde, $1 \le i \le n$ için $G_i \neq \emptyset$ dir.

Öte yandan, $1 \le i \le n$ ve $g_1, g_2 \in G_i$ için $(g_1.g_2)^{p_i^k} = g_1^{p_i^k}.g_2^{p_i^k} = 1_G.1_G = 1_G, g_1.g_2 \in G_i$ elde edilir.

$1 \le i \le n$ ve $g_1 \in G_i$ için $g_1^{p_i^k} = 1_G, (g_1^{p_i^k})^{-1} = 1_G$, $g_1^{-1} \in G_i$ dir.

Sonuç olarak, $G_i \le G$ dir. Şimdi, G grubunun G_i alt gruplarının iç direkt çarpımı olduğunu göstermeye çalışacağız. Bunun için G_i ye ait elemanları, notasyonda kolaylık sağlamak amacıyla g_{p_i} ile temsil ederek, $g \in G$ nın, $g = g_{p_1} \dots g_{p_n}$ şeklindeki yazılımın tek olduğunu göstermek yeterli olacaktır.

$g \in G, |g| \mid |G| \Rightarrow |g| = p_1^{m_1} \dots p_n^{m_n}$ olacak şekilde $\exists$ $m_1, m_2, \dots m_n \in \mathbb{N}$

Öte yandan aşağıdaki gibi $\begin{matrix} 1 \le i, j \le n \\ (i, j \in \mathbb{N}) \end{matrix}$ için $a_i = \frac{|g|}{p_i^{m_i}}$ sayıları dikkate alınırsa, $i \neq j$ için

$(a_i, a_j) = 1$ olacaktır. O halde, $\exists$ $b_1, b_2, \dots, b_n \in \mathbb{Z}$ $\ni$ $a_1b_1 + a_2b_2 + \dots + a_nb_n = 1$ ve

$g^1 = g^{a_1b_1 + a_2b_2 + \dots + a_nb_n} = g^{a_1b_1} \dots g^{a_nb_n}$ dir.

Diğer yandan, her $1 \le i \le n$ için $(g^{a_ib_i})^{p_i^m} = g^{b_i|g|} = 1_G$ $1 \le i \le n$ $(i \in \mathbb{N})$ olduğundan,

$g^{a_ib_i} \in G_i$ dir. O halde, $g^{a_ib_i} = g_i$ alınırsa $g = g_1g_2 \dots g_n$, $1 \le i, j \le n$ ve $i \neq j$ için

$G_i \cap G_j = \{1_G\}$ dir.

Bu yazılımın tek türlü olduğunu görmeye çalışalım;

$1 \leq i \leq n$ için $g_i, h_i \in G_i$ olmak üzere, $g = g_1 \dots g_n$, $g = h_1 \dots h_n$, şeklinde verildiğinde,

$1_G = g.g^{-1} = (g_1 \dots g_n)(h_1 \dots h_n)^{-1} = g_1 \dots g_n . {h_1}^{-1} \dots {h_n}^{-1} = g_1 {h_1}^{-1} \dots g_n {h_n}^{-1}$

eşitliğinden, $g_{1=} h_1 \dots g_{n=} h_n$ sonucuna ulaşılır. Dolayısıyla, yazılım tek türlüdür.

Teorem 7.2.3: G bir sonlu abelyen p-grubu ve $g \in G$, G nin, mertebesi en büyük elemanı olmak üzere belli bir $H \leq G$ için $G \cong < g > \times H$ dir.

Teorem 7.2.4: (Sonlu Abelyen Gruplarının Temel Teoremi)

Her sonlu abelyen G grubu, $p_i$sayıları birbirinden farklı olması gerekmeyen asal sayılar olmak üzere, r_i pozitif tam sayıları için $\mathbb{Z}_{{p_1}^{r_1}} \times \mathbb{Z}_{{p_2}^{r_2}} \times \dots \times \mathbb{Z}_{{p_n}^{r_n}}$ biçiminde devirli grupların direkt çarpımına izomorftur.

İspat: G sonlu bir abelyen grubu $g \in G$, G grubunun mertebesi en büyük elemanı göstersin. Eğer $G = < g >$ ise ispat tamamlanır. Aksi halde, **Teorem 7.2.3** ve her sonlu abel grubunun,

bir takım p-gruplarının direkt çarpımı olduğu hatırlanırsa, belirli bir $H \leq G$ için $G \cong \mathbb{Z}_{|g|} \times H$ dır.$|H| < |G|$ olduğundan, $|G|$ üzerine tümevarım prensibini uygulayarak teoremin ispatı elde edilir.

Örnek 7.2.1: p bir asal olmak üzere, izomorfizme bağlı olararak;

i. Mertebesi p^2 olan tüm abelyen gruplar:

$\mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{Z}_{p^2}$ dir.

ii. Mertebesi p^3 olan tüm abelyen gruplar:

$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$, $\mathbb{Z}_{p^3}$ dir.

iii. Mertebesi p^4 olan tüm abelyen gruplar:

$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2}$, $\mathbb{Z}_p \times \mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$, $\mathbb{Z}_{p^4}$ dir.

Örnek 7.2.2: $|G| = 540 = 2^2.3^3.5$ olduğu dikkate alınırsa, izomorfizme bağlı olarak tüm abelyen G grupları;

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$$

$$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \text{ ve } \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$$

şeklinde sıralanabilir.

Örnek 7.2.3: Z_6 grubu K = { $\overline{0}$, $\overline{2}, \overline{4}$ } ve L = { $\overline{0}$, $\overline{3}$ } alt gruplarının direkt çarpımıdır.

Gerçektende, Z_6 komütatif bir grup olduğundan, K$\trianglelefteq$ Z_6, L $\trianglelefteq$ Z_6 dir.

Öte yandan, K∩L = $\{\overline{0}\}$ ve Z_6= KL dir. **Teorem 7.1.4** den, $Z_6 \cong$ K × L yazabiliriz.

Teorem 7.2.5: G mertebesi n olan bir sonlu abelyen grup ve m, n sayısının bir pozitif böleni ise G grubunun mertebesi m olan bir alt grubu vardır.

İspat:

Teorem 7.2.4 den, p_i sayıları birbirinden farklı olmaları gerekmeyen asal sayılar ve r_i sayıları da pozitif tam sayılar olmak üzere,

$$G \cong \mathbb{Z}_{{p_1}^{r_1}} \times \mathbb{Z}_{{p_2}^{r_2}} \times \ldots \times \mathbb{Z}_{{p_n}^{r_n}} \text{ dir.}$$

$m \mid |G|$, $|G| = {p_1}^{r_1}.{p_2}^{r_2} \ldots {p_n}^{r_n}$ olduğundan $0 \leq s_i \leq r_i$ olmak üzere, $m = {p_1}^{s_1}.{p_2}^{s_2} \ldots {p_n}^{s_n}$

biçiminde ifade edilebilir. Öte yandan, $\overline{{p_\iota}^{r_\iota - s_\iota}}$ elemanı, $\mathbb{Z}_{{p_i}^{r_i}}$ grubunun $\frac{{p_i}^{r_i}}{({p_i}^{r_i - s_i}, {p_i}^{r_i})} = p^{s_i}$ mertebeli bir devirli alt grubunu doğurur. O halde, G grubunun

$$< \overline{{p_1}^{r_1 - s_1}} > \times < \overline{{p_2}^{r_2 - s_2}} > \times \ldots \times < \overline{{p_n}^{r_n - s_n}} >$$

alt grubuna izomorftur. Yani, G nin m-inci mertebeden bir alt grubu vardır.

7.3 Serbest Abelyen Gruplar

G herhangi bir grup olmak üzere,

$\emptyset: \mathbb{Z} \to G,\ g \in G$ olarak tanımlanan tasvir bir homomorfidir.

$n \mapsto g^n$

Herhangi bir $n \in \mathbb{Z}$ için $\emptyset(n)$ değerinin, $\emptyset(1)$ değerine bağlı olarak belirlenebileceğine dikkat edelim;

$$\emptyset(n) = \emptyset(n.1) = \emptyset\left(\underbrace{1 + 1 + \cdots + 1}_{n\ tane}\right) = \emptyset(1) \cdot \emptyset(1) \cdot\ \ldots \cdot \emptyset(1) = g \cdot \ldots \cdot g = g^n$$

Benzer şekilde negatif sayılar için de kat kavramı kullanılarak aynı sonuca ulaşılır.

Öte yandan, $\mathbb{Z} \times \mathbb{Z}$ grubunda, $\forall (m, n) \in \mathbb{Z} \times \mathbb{Z}$ için $m(1{,}0) + n(0{,}1) = (m, n)$ olduğundan,

bir $\emptyset: \mathbb{Z} \times \mathbb{Z} \to G$ homomorfisi için $\emptyset\big((m, n)\big) = \emptyset\big(m(1{,}0) + n.(0{,}1)\big) = \big(\emptyset(1{,}0)\big)^m + (\emptyset(0{,}1))^n$

yazılabilir, yani her $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ için $\emptyset\big((m, n)\big)$ değeri, $\emptyset((1{,}0))$ ve $\emptyset((0{,}1))$ değerleri ile belirlenir.

Dikkat edilecek olursa, $e_1 = (1{,}0)$, $e_2 = (0{,}1)$ elemanları $\mathbb{Z} \times \mathbb{Z}$ için özel elemanlardır.

Nitekim $\mathbb{Z} \times \mathbb{Z}$ grubunu elemanları, $\{e_1, e_2\}$ kümesinin elemanları kullanılarak tanımlanmaktadır.

Tanım 7.3.1: H bir grup, I bir indis kümesi ve $\{e_i \in H \mid i \in I\}$ olmak üzere, her $h \in H$ için

$$h = \sum_{i \in I} h_i e_i$$

şeklinde yazılabiliyorsa bu kümeye bir üreteç kümesi denir.

Tanım 7.3.2: H bir grup, $I\ bir$ indis kümesi olmak üzere, $\{e_i \in H \mid i \in I\}$ kümesi aşağıdaki koşulu gerçekliyorsa, H grubunun lineer bağımsız bir alt kümesidir denir.

$$"h = \sum_{i \in I} t_i e_i = 0 \Leftrightarrow \forall i \in I\,, t_i = 0"$$

Tanım 7.3.3: $B = \{e_i \in H \mid i \in I\}$ kümesi, H grubu için bir üreteç kümesi ve üstelik lineer bağımsız ise B kümesine, H grubunun bir bazı denir.

Örnek 7.3.1: Her grubun bir bazı olması gerekmez. $\mathbb{Z}_n$ grubunun hiçbir alt kümesi, $\mathbb{Z}_n$ grubu için bir baz teşkil etmez.

Dikkat: $\mathbb{Z}$ de $\{1\}$ ve $\{-1\}$ kümelerinin birer baz olduğu aşikardır. Bir grubun bazının bir tek olması gerekmez. Öte yandan her üreteç kümesi de bir baz teşkil etmez.

$\mathbb{Z}$ de $\{1,3\}$ kümesi bir üreteçtir fakat $3.1 + (-1).3 = 0$ eşitliğinden dolayı, bir baz değildir.

Tanım 7.3.4: G bir abelyen grup olmak üzere G nin bir bazı varsa G ye **serbest abelyen grup**

denir. $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ birer serbest abelyen gruptur. Sırasıyla,

$\{1\}, \{(1,0), (0,1)\}, \{(1,0,0), (0,1,0), (0,0,1)\}$ kümeleri, yukarıda ifade edilen gruplar için birer baz cümleleridir.

Teorem 7.3.1: G, aşikar olmayan r elemanlı bir bazı olan serbest abelyen grup ise

$$G \cong \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{r\ tane}$$

dir.

İspat:

G, aşikar olmayan r elemanlı bir bazı $B = \{e_1, e_2, \dots, e_r\}$ olan bir serbest abelyen bir grup olsun.

Bu durumda, $\forall g \in G$ için $g = n_1.e_1 + n_2.e_2 + \cdots + n_r.e_r$ yazılışında $n_1, n_2, \dots n_r$ değerleri tek türlü belirlidir. Sonuç olarak,

$$\emptyset: G \to \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{r\ tane}$$

$$g \to (n_1, \dots, n_r)$$

şeklinde tanımlanan $\emptyset$ tasvirinin bir izomorfizma olduğu kolayca gösterilir.

Not 7.3.1: Eğer serbest abelyen grubu tek bir elemandan oluşuyorsa devreseldir.

Not 7.3.2: Bir grubun bazının sonlu olması gerekmez. Eğer bir grubun bazı sonlu ise bu grup sonlu doğuraylı grup olarak adlandırılır. Üstelik, herhangi iki bazı aynı sayıda eleman içerir.

Tanım 7.3.5: G bir serbest abelyen grup olmak üzere, G grubunun bir bazının kardinalitesine G grubunun **rankı** denir.

Teorem 7.3.2: Her sonlu üreteçli abelyen grup, bir sonlu üreteçli serbest abelyen grubunun homomorfik görüntüsüdür.

İspat:

G bir sonlu üreteçli abelyen grup olmak üzere, $B = \{a_1, a_2, \dots, a_r\}$, G grubunun bir üreteçler kümesi olsun.

$$\emptyset: \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{r\ tane} \to G$$

$$(n_1, \dots, n_r) \to n_1\, a_1 + \cdots + n_r a_r$$

tasvirinin bir üzerine homomorfi olduğunu görmek kolaydır. **Teorem 7.3.1** dikkate alındığında,ispat tamamlanır.

Alıştırmalar VII

1) Cayley teoremi yardımıyla, $\mathbb{Z}_{15}$ in asal kalan sınıfları grubunun, S_8 in

$\{I, (1235)(4876), (1532)(4678), (1734)(2658), (1437)(2856), (13)(25)(47)(68),$
$(16)(24)(38)(57), (18)(24)(38)(57)\}$

alt grubuna izomorf olup olmadığını araştırınız.

2) Bir G grubunun bütün otomorfileri grubu $Aut(G)$ ile gösterilir. Buna göre $I(G) \lhd Aut(G)$ olduğunu ispat ediniz.

3) $\varphi: A \to B$ bir grup homomorfisi olsun.

i. $H \lhd A$ ise $\varphi(H) \lhd B$ olduğunu gösteriniz.

ii. $K \lhd B$ ise $\varphi^{-1}(K) \lhd A$ olduğunu gösteriniz.

4) Aşağıdaki iddialar doğru mudur? Neden?

i. $\varphi: A \to B$ bir grup homomorfisi ise B nin herhangi bir a' elemanının φ deki tam orijinaller kümesi A nın bir alt grubudur.

ii. $\varphi: A \to B$ bir grup homomorfisi ve $N \lhd A$ ise $A/N \cong B$ dir.

iii. $\varphi: A \to B$ bir üzerine grup homomorfisi ise $A/Ker\varphi \cong B$ dir.

5) G', G nin komütatör grubu olduğuna göre, G nin her φ otomorfizması için

$\varphi(G') = G'$ olup olmadığını araştırınız.

6) G, H, n mertebeli sonlu abelyen gruplar olsunlar; $G \cong H$ olup olmadığını araştırınız.

7) $\mathbb{Z}_n$, $n \in N, n > 1$ serbest abelyen grup olmadığını gösteriniz.

8) Q serbest abelyen grup mudur? Neden?

9) $14, 28, 25$ ve 29 mertebeli kaç tane farklı abelyen grup vardır?

10) $\mathbb{Z}_{10} \times \mathbb{Z}_{12}$ grubunun izomorfizma bağlı olarak 8.mertebeden bir alt grubunu belirleyiniz.

11) p, q farklı asal sayılar olmak üzere, izomorfizme bağlı olarak, mertebesi pq olan kaç tane abelyen grup vardır?

12) G sonlu üreteçli serbest bir abelyen grup ise G grubunun herhangi iki bazının aynı sayıda eleman içerdiğini gösteriniz.

8. p-Grup, Sylow Teoremleri

Teorem 8.1: G grubunun bir g elemanının G içindeki birbirinden farklı eşleniklerinin sayısı, g nin normalizatörü $N_G(g)$ nin G içindeki indeksine eşittir.

İspat:

$[G: N_G(g)] = k$ olduğunu ve G nin $N_G(g)$ alt grubuna göre sol kalan sınıflara ayrılışının

$$G = a_0N_G(g) + a_1N_G(g) + \cdots + a_{k-1}N_G(g) \ , \quad (a_0 = 1_G)$$

olduğunu varsayalım. Bir $h \in$ G için $h \in N_G(g)$ ise $hg = gh$ yani $hgh^{-1} = g$ dir.
$h \in a_iN_G(g)$ $(1 \leq i \leq k-1)$ ise $h = a_in$ olacak biçimde bir $n \in N_G(g)$ vardır ve buna göre

$$hgh^{-1} = (a_in)g(a_in)^{-1} = a_i(ngn^{-1}){a_i}^{-1} = a_iga_i{}^{-1}$$

dir. Yani, g nin $a_iN_G(g)$ deki bütün eşlenikleri $a_i$ile eşleniğine eşittir. O halde g nin k tane eşleniği vardır ve bunlar $g, a_1ga_1{}^{-1}, \ldots, a_{k-1}ga_{k-1}{}^{-1}$ dır. Öte yandan $(1 \leq i, j \leq k-1)$ ve $i \neq j$ olmak üzere $a_iga_i{}^{-1} = a_jga_j{}^{-1}$ olsa

$$a_i{}^{-1}(a_iga_i{}^{-1})a_j = a_i{}^{-1}(a_jga_j{}^{-1})a_j \Rightarrow g(a_i{}^{-1}a_j) = (a_i{}^{-1}a_j)g \Rightarrow a_i{}^{-1}a_j \in N_G(g) \Rightarrow a_j \in a_iN_G(g)$$

çelişkisi elde edilir. Çünkü $a_iN_G(g) \cap a_iN_G(g) = \emptyset$ dir. O halde g nin G içindeki birbirinden farklı eşleniklerinin sayısı k dır.

Not 8.1: Bu teorem dikkate alındığında bir $g \in G$ elemanının ait olduğu $[g]$ eşlenik eleman sınıfının eleman sayısının $[G: N_G(g)]$ olduğunu söyleyebiliriz. Buna göre sonlu bir G grubunun sınıf denklemi

$$|G| = \sum_{i=1}^{r} |[g_i]| = \sum_{i=1}^{r} [G: N_G(g)]$$

şeklinde yazılır.

Not 8.2: G grubunun herhangi bir boş olmayan T alt kümesi ile komütatif olan bütün elemanlarının kümesini $N_G(T)$ ile gösterildiğini, $N_G(T) = \{a \in G \mid aT = Ta\}$ nin $\boldsymbol{T}$ **nin** $\boldsymbol{G}$ **içindeki normalizatörü** olarak adlandırıldığını biliyoruz.

Not 8.: Yukarıda verilen bilgiler ışığında $N_G(T) \leq G$ ve $T \trianglelefteq N_G(T)$ olduğunu hatırlayalım.

Öte yandan, T alt kümesinin G içindeki birbirinden farklı eşleniklerinin sayısı T nin normalizatörü $N_G(T)$ nin G içindeki indeksine eşittir.

Şimdi, sonlu bir grubun sınıf denkleminin farklı bir yöntemle nasıl elde edilebileceğini göreceğiz.

Bunun için, **bir grubun bir küme üzerindeki etkisi ve uygulamalarından** bahsedeceğiz.

8.1 Bir Grubun Bir Küme Üzerine Etkisi

Tanım 8.1.1: X boş kümeden farklı bir cümle, G bir grup olsun. G nin, X kümesi üzerindeki bir etkisi**,**

$$\cdot\ : G \times X \to X$$

$$(g, x) \to g.x$$

şeklinde tanımlanan, aşağıdaki koşulları gerçekleyen bir fonksiyondur;

- **i.** $\forall g \in G,\ \forall x \in G$ için $g.x \in X$ dir.
- **ii.** $\forall g_1, g_2 \in G,\ \forall x \in X$ için $(g_1, g_2).x = g_1.(g_2.x)$ dir.
- **iii.** $\forall x \in X$ için $1_G.x = x$ dir.

Bu durumda, X bir $\boldsymbol{G}$**-kümesidir** denir.

Örnek 8.1.1: X sonlu bir küme, $H \leq S_X$ olsun.

$$\cdot\ : H \times X \to X$$

$$(\alpha, x) \to \alpha . x = \alpha(x)$$

şeklinde tanımlanan " · " fonksiyonunun bir etki olduğunu gösterelim;

Dikkat edilecek olursa, yukarıdaki tasvir, α permütasyonunun, x noktasını eşlediği değer yardımıyla tanımlanmıştır. Şimdi etki şartlarının sağlanıp, sağlanmadığını inceleyeceğiz.

i. $\forall \alpha \in H,\ \forall x \in H$ için $\alpha . x = \alpha(x) \in X$ dir.

ii. $\forall \alpha, \beta \in H, \forall x \in H$ için $(\alpha\beta)x = (\alpha\beta)(x) = \alpha\big(\beta(x)\big) = \alpha(\beta . x) = \alpha . (\beta . x)$ dir.

iii. $\forall x \in X$, $1_{S_X} . x = I(x) = x$ dir.

Şu halde, X bir H- kümesidir.

Örnek 8.1.2: G bir grup olmak üzere,

$$\cdot\ : G \times G \to G$$

$$(g, x) \to g . x = gx$$

şeklinde tanımlanan " · " tasviri, G nin kendi üzerinde bir etkisidir. Gerçektende;

i. $\forall g, x \in G$ için $g . x = gx \in G$ dir.

ii. $\forall g_1, g_2 \in G$ için $g_1 . (g_2 . x) = g_1 . (g_2 . x) = g_1(g_2 x) = (g_1 g_2)x = (g_1 g_2) . x$ dir.

iii. $\forall x \in G$ için $1_G.x = 1_G x = x$ dir.

Örnek 8.1.3: G bir grup olmak üzere,

$$\cdot\ : G \times G \to G$$

$$(x, g) \to x.g = xgx^{-1}$$

şeklinde tanımlanan " · " tasvirinin, G nin kendi üzerinde bir etki olduğunu gösterelim.

i. $\forall x, g \in G$ için $x.g = xgx^{-1} \in G$ dir.

ii. $\forall x_1, x_2, g \in G$ için $x_1(x_2.g) = x_1.(x_2 g x_2{}^{-1}) = x_1(x_2 g x_2{}^{-1})x_1{}^{-1} = (x_1x_2)g(x_2{}^{-1}x_1{}^{-1}) = (x_1x_2)g(x_1x_2)^{-1} = (x_1x_2)g$ dir.

iii. $1_G.g = 1_G.g1_G{}^{-1} = g$ dir.

O halde " · " bir etkidir. G nin kendi üzerinde **eşlenik etkisi** olarak adlandırılır.

Örnek 8.1.4: G bir grup, $H \leq G$ ve $1_H = \{xH \mid x \in G\}$ olarak verilsin.

$$\cdot\ : G \times L_H \to L_H$$

$$(g, xH) \to g.(xH) = (gx)H$$

şeklinde tanımlanan bir " · " fonksiyonu bir etkidir.O halde, G grubunun, H altgrubuna göre sol kalan sınıfları üzerinde bir etki tanımlabileceğini söyleyebiliriz. Aynı etki tanımını, H nın G grubu içindeki sağ kalan sınıfları üzerinde de vermek mümkündür.

Tanım 8.1.2: X bir G-kümesi, $x \in X$ ve $g \in G$ olsun.

$X_g = \{x \in X \mid g.x = x\}$ kümesine, $g \in G$ nin X kümesindeki sabit nokta kümesi denir.

Tanım 8.1.3: X bir G-kümesi, $x \in X$ ve $g \in G$ olsun.

$G_x = \{u \in G \mid u.x = x\}$ kümesine, $x \in G$ nin sabitleyici alt grubu denir.

Teorem 8.1.1: X bir G-kümesi, $x_1, x_2 \in X$ olsun;

$x_1 \sim x_2 \Rightarrow \exists g \in G \ni g.x_1 = x_2$ şeklinde tanımlanan "$\sim$" bağıntısı bir denklik bağıntısıdır.

İspat:

i. $\forall x \in X$, $1_G.x = x$ olduğundan $x \sim x$ dir.

ii. $x_1, x_2 \in X$ $x_1 \sim x_2 \Rightarrow g.\ x_1 = x_2 \Rightarrow g^{-1}(g.\ x_1) = g^{-1}x_2 \Rightarrow (g^{-1}g)\ x_1 = g^{-1}.x_2 \Rightarrow$

$x_1 = g^{-1}.x_2 \Rightarrow x_2 \sim x_1$ dir.

iii. $x_1, x_2, x_3 \in X$ için $x_1 \sim x_2$ ve $x_2 \sim x_3 \Rightarrow \exists g_1, g_2 \in G \ni g_1.x_1 = x_2$ ve $g_2.x_2 = x_3 \Rightarrow$

$x_1 = (g_1.g_2)^{-1}.x_3 \Rightarrow x_1 \sim x_3$ dir.

O halde, "$\sim$" bağıntısı bir denklik bağıntısıdır. Bu bağıntının, X kümesi üzerinde belirlediği denklik sınıflarının her birine, **yörünge (orbit)** adı verilir; $x \in X$ için

$Gx = \{ y \in X \mid g.x = y, g \in G \}$ kümesi ile temsil edilir.

Not 8.1.1: X bir G-kümesi ve $x \in X$ olsun. O halde $x_1 \in Gx \Rightarrow x \sim x_1 \Rightarrow \exists g_1 \in G \ni g_1 x = x_1$ dir.

$$\emptyset: Gx \to L_{G_x}$$
$$x_1 \to g_1 Gx$$

tasviri yardımıyla, $S(Gx) = [G: G_x]$ olduğu kolaylıkla görülür.

Tanım 8.1.4: X sonlu bir küme, G sonlu bir grup, X bir G-kümesi olmak üzere,

$X_G = \{x \in X \mid \forall g \in G$ için $gx = x\}$ kümesine, G grubu tarafından sabit bırakılan, $x \in X$ elemanlarının kümesi denir.

Dolayısıyla, $x \in X_G \Leftrightarrow Gx = \{x\}$ dir.

$X = \{x_1, x_2, \dots, x_n\}$, $X_G = \{x_1, x_2, \dots, x_{k-1}\}$ olmak üzere,

$$\boldsymbol{S(X) = S(X_G) + \sum_{i=k}^{n} S(Gx_i)}$$

yazılabilir.

Öte yandan, etki olarak sonlu bir G grubunun kendi üzerinde tanımlı **eşlenik etkisi** alındığında,

$$\boldsymbol{S(X) = S(X_G) + \sum_{i=k}^{n} S(Gx_i)}$$

denklemi, G grubunun sınıf denklemini verecektir.

Şimdi, bir grubun alt gruplarını belirleme problemine çözüm getirmeye çalışacağız;

Lagrange teoremine göre, sonlu bir gurubun her alt grubunun mertebesinin grubun mertebesini böldüğünün biliyoruz. Burada akla şu soru geliyor:

G, mertebesi k olan bir sonlu grup olmak üzere k nın herhangi bir t bölenine karşılık, G nin mertebesi t olan bir alt grubu var mıdır?

Bu sorunun yanıtı genel olarak olumsuzdur. Çünkü bilindiği gibi 4 üncü dereceden simetrik grup S_4 ün normal alt gurubu olan 4 üncü dereceden alterne grup A_4, mertebesi 12 olan bir gruptur ve A_4 ün mertebesi 6 olan bir alt gurubu yoktur.

Ancak p bir asal sayı olmak üzere p^m $(m \geq 1)$ G nin mertebesini bölüyorsa, G nin, mertebesi p^m olan bir alt gurubunun var olduğu Norveçli matematikçi Sylow (Peter Ludwig Mejdell Sylow) tarafından 1872 yılında ispat edilmiştir.

8.2 Grup Serileri

Tanım 8.2.1: G bir grup, $m > 0$ bir tam sayı ve $H_0, H_1, \dots, H_m \leq G$ olsun. Her $0 \leq i \leq m$ için $H_i \trianglelefteq H_{i+1}$ ise $\{1_G\} = H_0 \leq H_1 \leq \cdots \leq H_m = G$ sonlu alt grup zincirine G grubunun bir **alt normal serisi** denir ve bu seri $\{H_i \mid 0 \leq i \leq m\}$ veya $\{H_i\}$ ile gösterilir.

Her $0 \leq i \leq m$ için $H_i \lhd G$ ise $\{H_i\}$ zincirine G grubunun bir **normal serisi** denir.

Not 8.2.1: Bir normal serinin aynı zamanda bir alt normal seri olduğu açıktır.

Fakat bir alt normal serinin normal seri olması gerekmez.

Not 8.2.2: G bir abelyen grup ise G grubunun her alt grubu normal olduğundan, grubun alt normal ve normal serileri çakışıktır.

Örnek 8.2.1: D_4 grubunun,

$\{(1)\} \leq \{(1), (24)\} \leq \{(1), (13)(24), (24), (13)\} \leq D_4$ serisi, bir alt normal seridir. Dikkat edilirse, $\{(1), (24)\}$ alt grubu D_4 grubunun bir normal alt grubu değildir. Dolayısıyla, bu seri bir normal seri değildir. Öte yandan,

$\{(1)\} \leq \{(1), (13)(24)\} \leq D_4$, D_4 grubunun bir normal serisidir.

Tanım 8.2.2: G bir grup, $\{H_i\}$ ve $\{K_i\}$, G grubunun iki alt normal (veya normal) serisi olsun. Eğer $\{H_i\} \subset \{K_i\}$ sa $\{K_i\}$ alt normal (veya normal) serisine $\{H_i\}$ alt normal (veya normal) serisinin bir **inceltilmiş serisi** denir.

Örnek 8.2.2: $\{0\} \subset 48\mathbb{Z} \subset 12\mathbb{Z} \subset 6\mathbb{Z} \subset \mathbb{Z}$ serisinin bir inceltilmiş serisi, $\{0\} \subset 48\mathbb{Z} \subset 12\mathbb{Z} \subset 6\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$ serisidir.

Tanım 8.2.3: Bir G grubunun, $i = 0,1, \dots n-1$ için H_i/H_{i+1} bölüm grubu komütatif olacak şekilde bir $H_n = \{1_G\} \leq H_{n-1} \leq \cdots \leq H_2 \leq H_1 \leq H_0 = G$ alt normal seri varsa, G grubu **çözülebilirdir** denir. Her komütatif grup çözülebilirdir.

Örnek 8.2.3: $\{I\} \leq \{I,(123),(132)\} \leq S_3$ ve

$\{I\} \leq \{I,(12)(34)\} \leq \{I,(12)(34),(13)(24),(14)(23)\} \leq A_4 \leq S_4$ olduğuna göre $S_3,\ S_4, A_4$ grupları çözülebilirdir.

Öte yandan S_1 ve S_2 grupları komütatif olduğundan çözülebilirdir.

Sonuç 8.2.1: $n \in N, n \leq 4$ için S_n grupları çözülebilirdir.

Tanım 8.2.4: G bir sonlu grup ve p bir asal sayı olmak üzere $|G| = p^n$ $(n \geq 0)$ ise G ye bir $\boldsymbol{p}$**-grup** denir.

G bir sonlu grup ve $H \leq G$ olsun H bir p-grup ise H ya bir **p-alt grup** denir.

G bir sonlu grup ve H, G nin bir p-alt gurubu olsun. $|H| = p^m$ ve p asal sayısının G nin mertebesini bölen en büyük kuvveti m ise **(** $\boldsymbol{p^m \mid |G|\ ;\ p^{m+1} \nmid |G|}$ **)** H alt gurubuna, G nin bir

p-Sylow alt gurubu denir.

Örnek 8.2.4: $S_3 = \{I,(12),(13),(23),(123),(132)\}$; $|S_3| = 6 = 2.3$ olduğundan,

$p = 2$ için 2-Sylow alt grupları $\{I,(12)\},\{I,(13)\},\{I,(23)\}$

$p = 3$ için 3-Sylow alt grubu $\{I,(123),(132)\ \}$ dir.

Teorem 8.2.1: G mertebesi n olan komütatif bir grup ve p, n yi bölen bir asal sayı ise G nin mertebesi p olan bir elemanı vardır.

İspat:

G nin mertebesine göre indüksiyonla ispat yapacağız. $|G| = 1$ ise ispat edilecek bir şey yoktur; $n > 1$ olmak üzere, mertebesi n den küçük olan bütün gruplar için iddianın doğru olduğunu varsayalım. Burada G bir devresel grup ise $|G|$ nin her bölenine karşılık bu böleni mertebe olarak kabul eden bir alt gurubun var olduğunu biliyoruz. Buna göre, G devresel ise iddia doğrudur.

Öte yandan n asal ise G devresel olacağından, n nin asal olmadığını varsayabiliriz.

$h \in G$ ve $|h| = m$ $(m \neq 0)$ olsun. G devresel olmadığından, $m < n$ olmak zorundadır.

$H =< h >$ devresel grubunu göz önüne alalım. H, G nin bir has alt gurubu olmak zorundadır.

Bu durumda,

$p|m$ ise H, mertebesi p olan bir elemana sahiptir. Dolayısıyla G de mertebesi p olan bir elemana sahiptir.

$p \nmid m$ ise komütatif bir gurubun her alt gurubu normal olduğundan G/H bölüm grubunu göz önüne alabiliriz.

$$|H| > 1, |G/H| < |G| \text{ ve } |G/H| = |G|/|H|$$

olduğundan $p \mid |G/H|$ dir. Dolayısıyla indüksiyon kabulüne göre G/H gurubunun mertebesi p olan gH bir elemanı vardır. Burada $\varphi: G \to G/H$ doğal homomorfisini göz önüne alalım ve $\varphi(g) = gH$ olduğunu düşünelim. Bu durumda,

$$\varphi(g^p) = (gH)^p = g^p H = H$$

olmak zorundadır. Buna göre, $g^p \in H$ dır. $|H| = m$ olduğundan, $(g^m)^p = (g^p)^m = 1_G$ dir.

O halde, ya $|g^m| = p$ ya da $g^m = 1_G$ dir. $|g^m| = p$ ise ispat tamamdır. $g^m = 1_G$ ise $\varphi(g^m) = (gH)^m = g^m H = H$ olmak zorundadır ve $|gH| = p$ olduğundan, $p|m$ çelişkisi elde edilir. Dolayısıyla g^m, G nin mertebesi p olan bir elemanıdır.

Teorem 8.2.2:

i. G bir p-grup ve $G \neq \{1_G\}$ ise $M_G \neq \{1_G\}$ dir.

ii. G bir p-grup ve $G \neq \{1_G\}$ ise G gurubunun,

$$\{1_G\} = G_0 \subset G_1 \subset \cdots \subset G_{t-1} \subset G_t = G$$

biçiminde bir alt gruplar dizisi vardır. Burada her i $(0 \leq i \leq t-1)$ için $G_i \trianglelefteq G_{i+1}$ ve G_{i+1}/G_i mertebesi p olan devresel bir gruptur.

İspat:

i. G nin sınıf formülünü göz önüne alalım.

$$|G| = |M_G| + \sum_{i=s+1}^{r} [G: N_G(g_i)]$$

Yukarıdaki eşitliğin sağ tarafında yer alan toplamda, her i $(s+1 \leq i \leq r)$ için $g_i \notin M_G$dir. Dolayısıyla her i $(s+1 \leq i \leq r)$ için $[G: N_G(g_i)] \neq 1$ dir ve $|G| = p^r$ ise $p \mid [G: N_G(g_i)]$ olmak zorundadır. O halde,

$$p \mid \sum_{i=s+1}^{r} [G: N_G(g_i)]$$

ve

$$p \mid |G| \Rightarrow p \mid |M_G|$$

yani $M_G \neq \{1_G\}$ dir.

ii. $|G| = p^r; r \geq 1$ alalım; r ye göre indüksiyon yapacağız. $r = 1$ halinde, $|G| = p$ olduğunda,

G bir devresel gruptur ve doğal olarak bir alt gruplar dizisi vardır. İddia, $1 < k < r$ olmak üzere, mertebeleri p^k olan gruplar için doğru olsun. Teoremin **i.** şıkkına göre $M_G \neq \{1_G\}$ dir. M_G komütatif olduğundan

$$\exists a \in M_G \; ; \; |a| = p$$

dir. Bu durumda, $< a >= H$ devresel gurubu için $H < M_G$ olduğundan $H \trianglelefteq G$ dir. Ayrıca, $|G/H| = p^{r-1}$ olduğundan iddia G/H için doğrudur. Buna göre, G nin bir alt gruplar dizisinin var olduğu ortaya çıkar.

Sonuç 8.2.2: G bir p-grup ve $|G| = p^r;\ r \geq 1$ ise G nin mertebesi p^{r-1} olan bir normal alt grubu vardır.

Sonuç 8.2.3: p bir asal sayı olmak üzere, mertebesi p^2 olan gruplar komütatiftir.

İspat: Bir G grubunun komütatif olması için gerek yeter koşulun $M_G = G$ olduğunu biliyoruz.

O halde, $|G| = p^2$ için $M_G \neq \{1_G\}$ dir. Burada, $|M_G| \mid p^2$ olacağından $|M_G| = p$ ya da p^2 dir. $|M_G| = p$ olsun. $g \notin M_G$ koşulunu sağlayan bir $g \in G$ elemanı için $M_G < N_G(g)$ ve

$M_G \neq N_G(g)$ olacağından $|N_G(g)| > p$ dir. Öte yandan, Lagrange teoremine göre

$$|N_G(g)| \mid p^2 \Rightarrow |N_G(g)| = p^2$$

yani $N_G(g) = G$ elde edilir. Oysa, $N_G(g) = G \Leftrightarrow g \in M_G$ olduğundan bu durum, $g \notin M_G$ ile çelişir. O halde $|M_G| = p$ olamaz. Buna göre $M_G = G$ dir. Sonuç olarak, G komütatiftir.

Teorem 8.2.3 (Birinci Sylow Teoremi): G bir sonlu grup ve $p \mid |G|$ ise G nin bir p-Sylow alt grubu vardır.

Örnek 8.2.5 : G bir grup ve $H \subset G$ ise her $g \in G$ için $gHg^{-1} = \{gHg^{-1} \mid h \in H\}$ biçimindedir. $\varphi: H \to gHg^{-1}$; $\varphi(h) = gHg^{-1}$ tasviri üzerine ve birebir olduğundan $|gHg^{-1}| = |H|$ dir.

Öte yandan, $H \leq G$ ise $gHg^{-1} \leq G$ dir. Buna göre G sonlu bir grup ve H, G nin bir p-Sylow alt gurubu ise gHg^{-1} de bir p-Sylow alt gurubudur.

Örnek 8.2.6: G bir sonlu grup ve H, G nin tek p-Sylow alt gurubu ise $g \in G$ için gHg^{-1} de bir p-Sylow alt gurubu olduğundan $gHg^{-1} = H$ yani $H \trianglelefteq G$ dir.

Teorem 8.2.4: G bir sonlu grup ve P, G nin bir p-Sylow alt gurubu olsun. H, G nin bir p-alt gurubu ise $N_H(P) = \{h \in H \mid hP = Ph\}$ (P nin H alt gurubu içindeki normalizatörü) olmak üzere $N_H(P) = H \cap P$ dir.

Teorem 8.2.5 (İkinci Sylow Teoremi): G bir sonlu grup, $H \leq G$ ve P, g nin bir p-Sylow alt gurubu olsun. Bu durumda H bir p-grup ise bir $g \in G$ için $H \subseteq gPg^{-1}$ dir.

Teorem 8.2.6 (Üçüncü Sylow Teoremi):

i. P ve R, G sonlu gurubunun iki p-Sylow alt gurubu ise bir $g \in G$ için $R = gPg^{-1}$ dir, yani herhangi iki p-Sylow alt gurubu G de eşleniktir.

ii. G nin birbirinden farklı p-Sylow alt grupları sayısı s_p ise $s_p \equiv 1 \ (mod\ p)$ dir.

iii. $s_p \mid |G|$ dir.

Örnek 8.2.7: G bir grup ve $|G| = 20$ olsun. $20 = 2.5^2$ olduğundan 20 sayısının asal bölenleri 2 ve 5 tir.Yani G nin 2-Sylow ve 5-Sylow alt grupları vardır. G nin 5-Sylow alt gruplarının sayısı $s_5$ise Üçüncü Sylow Teoremine göre, $s_5 \mid 20$ ve $s_5 \equiv 1 \ (mod\ 5)$ dir;

20 nin bölenleri 1, 2, 4, 5, 10, 20 arasında bu koşulları gerçekleyen sayı sadece 1 dir. Buna göre, G nin tek 5-Sylow alt gurubu vardır ve bu alt grup normal olmak zorundadır. O halde mertebesi 20 olan grup, basit olamaz.

Örnek 8.2.8: Mertebesi 5 ya da daha küçük gruplar komütatiftir. Çünkü, mertebenin 1 olması hali triviyal haldir; mertebelerin 2,3 olması halinde ise mertebe asal olduğundan devresel gruplar söz konusudur ve devresel gruplar komütatiftir. Mertebenin 4 olması halinde $4 = 2^2$ nedeniyle, grup komütatiftir. Komütatif olmayan en küçük mertebeli sonlu grup 6. mertebedendir

Gerçekten de, 3.dereceden simetrik grup,

$$S_3 = \{I, (12), (13), (23), (123), (132)\}$$

ve $(12)(123) = (13)$, $(123)(12) = (23)$ olduğundan, S_3 komütatif değildir.

Alıştırmalar VIII

1) Aşağıdaki iddialar doğru mudur? Neden?

i) G mertebesi n olan bir grup ve k, n yi bölen bir sayı ise G nin mertebesi k olan bir elemanı vardır.

ii) Mertebesi 42 olan grup basit basittir.

iii) 559. mertebeden komütatif olmayan grup yoktur.

iv) 2772. mertebeden bir grubun 5-Sylow alt grubu vardır.

2) A_4 grubunun 2-Sylow ve 3-Sylow alt gruplarını belirleyiniz.

3) Mertebesi 30 olan grubun basit olmadığını gösteriniz.

4) P, G grubunun bir p-Sylow alt grubu, $|G| = p^r m$ $(r \geq 1)$ ve $p \mid m$ olsun. H bir p-grup ve $P \leq H \leq G$ ise $H = P$ olduğunu gösteriniz.

5) P, G nin bir p-Sylow alt grubu ve bir $a \in G$ için $|a| = p^k$ olsun. Bu durumda

$$aPa^{-1} = P \Rightarrow a \in P$$

olduğunu gösteriniz.

KAYNAKÇA

1.FRALEIGH, J.B., A FIRST COURSE IN ABSTRACT ALGEBRA,

ADDISON - WESLEY PUBLISHING COMPANY, 2003.

2.ŞENKON HÜLYA., SOYUT CEBİR DERSLERİ CİLT II,

İSTANBUL ÜNİVERSİTESİ FEN FAKÜLTESİ YAYINLARI, 1998.

3. WALTER-LEDERMAN, A.J., WEIR., INTRODUCTION TO GROUP THEORY, LONGMAN, 1996.

4.D. DUMMIT, RICHARD M. FOOTE., ABSTRACT ALGEBRA,

JOHN WILEY AND SONS, 2003.

5.GEZER BETÜL, BİZİM OSMAN., SOYUT CEBİR, DORA YAYINLARI, 2017.