

Soyut Cebir

Cebir 1 — Grup Teorisi

Açık Matematik

Açık Matematik — açık kaynaklı, reklamsız Türkçe matematik notları
acik-matematik.com

Bu çalışma [Creative Commons BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/) lisansı ile paylaşılmıştır: kaynak göstererek ve aynı lisansla, ticari olmayan amaçlarla kopyalayabilir, dağıtabilir ve uyarlayabilirsiniz.

Bu sürüm: 20 Eylül 2026

İçindekiler

	Giriş	7
1	İkili İşlem ve Cebirsel Yapılar	9
1.1	İkili İşlem ve Cebirsel Yapı	9
1.2	Asosyatiflik ve Komutatiflik	9
1.3	Birim Eleman	9
1.4	Ters Eleman	10
1.5	Çözümlü Örnekler	11
1.6	Tanıdık Kümelerde Bir Tur	12
2	Yarı Grup, Monoid ve Grup	13
2.1	Yarı Grup ve Monoid	13
2.2	Grup Kavramı	13
2.3	Tanıdık Yapıların Sınıflandırması	14
3	Grup Örnekleri	15
3.1	Bileşenli İşlemle Kurulan Bir Grup	15
3.2	Kompleks Sayıların Çarpma Grubu	15
3.3	Alıştırmalar	17
4	Grup Aksiyomlarının Esnetilmesi	19
4.1	Sol Birim ve Sol Ters Yeterlidir	19
4.2	Denklemlerle Karakterizasyon	20
4.3	Sadeleştirme Kuralları	20
4.4	Sonlu Grup ve Mertebe	21
5	İşlem Tabloları ve Küçük Mertebeli Gruplar	23
5.1	İşlem Tablosu	23
5.2	Mertebesi 1, 2 ve 3 Olan Gruplar	24
5.3	Mertebesi 4 Olan Gruplar	25
6	Kuvvetler ve Katlar	27
6.1	n 'li Çarpım	27
6.2	Tam Sayılı Kuvvetler	27
6.3	Toplamsal Yazış: Katlar	28
7	Alt Grup Kavramı ve Ölçütleri	31
7.1	Alt Grup Tanımı	31

7.2	Üç Alt Grup Ölçütü	31
7.3	Trivial Alt Gruplar	32
8	Alt Grup Örnekleri	33
8.1	Hatırlatma: Kalan Sınıfları	33
8.2	Kompleks Sayılarda Bir Alt Grup	33
8.3	Sonlu Grupta Kapalılık Denetimi	34
8.4	Soyut Örnekler	34
8.5	Alıştırmalar	35
9	Transformasyonlar ve Simetrik Grup	37
9.1	Transformasyonlar Grubu	37
9.2	Substitüsyonlar ve S_n	37
9.3	S_n Komutatif Değildir	38
10	Devreler	41
10.1	Devre Kavramı	41
10.2	Yabancı Devrelere Ayrılış	41
10.3	Devrelerle Hesap Kuralları	42
11	Transpozisyonlar ve Alterne Grup	45
11.1	Transpozisyonlara Ayrılış	45
11.2	Tek ve Çift Substitüsyonlar	45
11.3	Alterne Grup	46
12	Doğurulan Alt Gruplar	49
12.1	Alt Grupların Kesişimi	49
12.2	Doğurulan Alt Grup	49
12.3	İlk Örnekler	50
13	Devresel Gruplar	53
13.1	Tanım ve İlk Özellik	53
13.2	Sonsuz ve Sonlu Devresel Gruplar	53
13.3	Kuvvet Hesabının Aritmetiği	54
14	Bir Elemanın Mertebesi	55
14.1	Tanım	55
14.2	Permütasyonların Mertebesi	56
14.3	Komutatif Elemanların Çarpımı	57
14.4	Alıştırma	57
15	Devresel Grubun Alt Grupları	59
15.1	Her Alt Grup Devreseldir	59
15.2	Mertebe Ayrışımı: $n = \mu\nu$	59
15.3	Doğuraylar ve Euler'in ϕ Fonksiyonu	60

16	Hasse Diyagramları	63
16.1	Alt Gruplar Şeması	63
16.2	Temel Örnekler	63
16.3	Permütasyonlarla İki Büyük Örnek	64
17	Komplekslerle Hesap	67
17.1	Kompleks Kavramı	67
17.2	Alt Grup Ölçütlerinin Kompleks Dili	68
17.3	İki Alt Grubun Çarpımı	68
17.4	Toplamsal Yazış	69
18	Bir Alt Gruba Göre Kalan Sınıfları	71
18.1	Soldan ve Sağdan Eşdeğerlik	71
18.2	Sınıfların Kompleks Biçimi	71
18.3	Bütün Sınıflar Aynı Kuvvettedir	72
18.4	Somut Bir Bölmeleme	72
19	Lagrange Teoremi	75
19.1	Teorem ve İspatı	75
19.2	İndeks	75
19.3	Lagrange Teoreminin Sonuçları	76
19.4	Bir Uygulama: Tersinin Doğru Olmadığı	76
20	Normal Alt Gruplar	79
20.1	Tanım	79
20.2	İndeks 2 Ölçütü	79
20.3	Normallik Geçişken Değildir	80
20.4	Basit Gruplar	80
21	Bölüm Grupları	83
21.1	Çarpma Sınıflara İner	83
21.2	Bölüm Grubunun İnşası	83
21.3	Sonlu Durum ve Komutatif Durum	84
22	Bölüm Grubu Örnekleri	87
22.1	Yapısal Örnekler	87
22.2	S_3/A_3 : İlk Somut Bölüm Grubu	87
22.3	Komutatif Örnekler	88
22.4	Alıştırma	89
23	Homomorfi ve İzomorfi	91
23.1	Tanımlar	91
23.2	Homomorf Resim Grup Yapısını Taşır	92
23.3	Trivial Bölüm Gruplarının Kimliği	93

24	Gruplarda Homomorfi Teoremi	95
24.1	Homomorfi Teoremi	95
24.2	Çekirdek Hesapları	96
24.3	İzomorfi Ölçütü	97
25	Doğal Homomorfi	99
25.1	Doğal Homomorfi	99
25.2	Her Homomorfi Doğal Homomorfiden Geçer	99
25.3	Alıştırmalar	100

Giriş

Matematiğin kalbini oluşturan cebirsel yapıları inceleyen bu kapsamlı seri; grup teorisinden başlayarak halkalara, oradan cisim genişlemelerine ve nihayetinde değişmeli cebirin zirvesi olan modül teorisine uzanan saf matematiksel bir inşadır.

1. İkili İşlem ve Cebirsel Yapılar

Soyut cebir, sayılarla yapageldiğimiz toplama ve çarpma gibi işlemlerin *kendisini* inceleme konusu yapar: bir kümede tanımlı bir işlem hangi kurallara uyarsa hangi yapı ortaya çıkar? Bu ilk bölümde en temel yapı taşlarını kuruyoruz — ikili işlem, cebirsel yapı, asosyatiflik, komutatiflik, birim eleman ve ters eleman. Bölümün iki küçük ama vazgeçilmez teoremi, birim elemanın ve tersin *tek türlü belirli* olduğunu söyler; ilerideki bütün grup teorisi bu iki teklilik üzerine oturur.

1.1 İkili İşlem ve Cebirsel Yapı

Tanım 1.1 (İkili İşlem). $M \neq \emptyset$ bir küme olsun. $M \times M$ kümesini M içine resmeden bir

$$\circ : M \times M \rightarrow M, \quad (a, b) \mapsto c \in M$$

funksiyonu varsa, M 'de bir **ikili işlem** tanımlanmıştır denir; $\circ$ fonksiyonuna M 'de tanımlanmış bir ikili işlem denir. $\circ ((a, b)) = c$ yazımı yerine kısaca

$$a \circ b = c$$

gösterimi kullanılır.

Tanımın gizli ama en önemli parçası, sonucun yine M 'de olmasıdır: işlemin sonucu kümenin dışına çıkıyorsa $\circ$ fonksiyon M 'de bir ikili işlem değildir. Bu koşula kümenin işleme göre **kapalı** olması denir.

Tanım 1.2 (Cebirsel Yapı). İçinde en az bir ikili işlem tanımlanmış, boş olmayan bir kümeye bir **cebirsel yapı** denir. M kümesinde $\circ$ gibi bir ikili işlem tanımlıysa bu cebirsel yapı $\langle M, \circ \rangle$ ile gösterilir.

1.2 Asosyatiflik ve Komutatiflik

Tanım 1.3 (Asosyatif İşlem). $M \neq \emptyset$ kümesinde tanımlı bir $\circ$ ikili işlemi

$$\forall a, b, c \in M \quad (a \circ b) \circ c = a \circ (b \circ c)$$

koşulunu sağlıyorsa $\circ$ işlemine M 'de **asosyatif** (birleşmeli) bir işlem denir; $M, \circ$ işlemine göre asosyatiftir denir.

Tanım 1.4 (Komutatif İşlem). $M \neq \emptyset$ kümesinde tanımlı bir $\circ$ ikili işlemi

$$\forall a, b \in M \quad a \circ b = b \circ a$$

koşulunu sağlıyorsa $\circ$ işlemine M 'de **komutatif** (değişmeli) bir işlem denir.

1.3 Birim Eleman

Birim elemanı tek hamlede tanımlamak yerine, ileride işimize yarayacak daha ince bir ayrımla başlayalım: işlemin yalnızca bir yanında etkisiz kalan elemanlar.

Tanım 1.5 (Sol Birim, Sağ Birim ve Birim Eleman). $\langle M, \circ \rangle$ bir cebirsel yapı olsun.

$$\exists e_1 \in M \text{ öyle ki } \forall a \in M \quad e_1 \circ a = a$$

oluyorsa e_1 'e bir **sol birim elemanı**;

$$\exists e_2 \in M \text{ öyle ki } \forall a \in M \quad a \circ e_2 = a$$

oluyorsa e_2 'ye bir **sağ birim elemanı** denir. Hem sol hem sağ birim olan bir e elemanına, yani

$$\forall a \in M \quad e \circ a = a \circ e = a$$

koşulunu sağlayan $e \in M$ 'ye $\langle M, \circ \rangle$ yapısının bir **birim elemanı** denir.

Teorem 1.1 (Birim Elemanın Tekliği). *Bir $\langle M, \circ \rangle$ cebirsel yapısının birim elemanı varsa tek türdendir.*

İspat.

e ve e' , $\langle M, \circ \rangle$ 'nin iki birim elemanı olsun. e birim eleman olduğundan her elemanı, bu arada e' 'yi de değiştirmez:

$$e \circ e' = e' \circ e = e'$$

Aynı biçimde e' birim eleman olduğundan

$$e \circ e' = e' \circ e = e$$

olur. İki eşitliğin sol tarafları aynı olduğundan $e = e'$ bulunur.

■

1.4 Ters Eleman

Tanım 1.6 (Sol Ters, Sağ Ters ve Ters Eleman). $\langle M, \circ \rangle$ 'nin bir e birim elemanı bulunsun ve $a \in M$ olsun.

$$a^* \circ a = e$$

olacak biçimde bir $a^* \in M$ varsa a^* 'ya a 'nın bir **sol tersi**;

$$a \circ a^{**} = e$$

olacak biçimde bir $a^{**} \in M$ varsa a^{**} 'ya a 'nın bir **sağ tersi** denir. Hem sol hem sağ ters olan bir b elemanına, yani

$$b \circ a = a \circ b = e$$

koşulunu sağlayan $b \in M$ 'ye a 'nın bir **ters elemanı** (kısaca tersi) denir.

Ters elemanın tekliği, birim elemanınkinden farklı olarak bedava gelmez: işlemin asosyatif olması gerekir.

Teorem 1.2 (Ters Elemanın Tekliği). M 'de asosyatif bir $\circ$ ikili işlemi tanımlı ve $\langle M, \circ \rangle$ 'nin birim elemanı e olsun. Herhangi bir $a \in M$ elemanının en çok bir tersi vardır; yani a 'nın tersi varsa tek türdendir.

İspat.

a' ve a'' , a 'nın iki tersi olsun:

$$a' \circ a = a \circ a' = e \quad (1)$$

$$a'' \circ a = a \circ a'' = e \quad (2)$$

(1)'deki $a \circ a' = e$ eşitliğini soldan a'' ile işleme sokalım:

$$a'' \circ (a \circ a') = a'' \circ e = a''$$

(2)'deki $a'' \circ a = e$ eşitliğini sağdan a' ile işleme sokalım:

$$(a'' \circ a) \circ a' = e \circ a' = a'$$

İşlem asosyatif olduğundan iki sol taraf eşittir:

$$a'' \circ (a \circ a') = (a'' \circ a) \circ a'$$

O hâlde $a'' = a'$ olur; ters varsa tektir.

■

1.5 Çözümlü Örnekler

Örnek 1.1 (Birim Elemanı Olmayan Bir Yapı). $\mathbb{Q}$ kümesinde $a \circ b = ab + 1$ işlemi tanımlanıyor. (Her $a, b \in \mathbb{Q}$ için $ab + 1 \in \mathbb{Q}$ olduğundan bu gerçekten bir ikili işlemdir.)

- $\circ$ işlemi $\mathbb{Q}$ 'da asosyatif midir?
- $\circ$ işlemi komutatif midir?
- $\langle \mathbb{Q}, \circ \rangle$ yapısının birim elemanı var mıdır?

Çözüm.

a) İki tarafı ayrı ayrı açalım:

$$(a \circ b) \circ c = (ab + 1) \circ c = (ab + 1)c + 1 = abc + c + 1$$

$$a \circ (b \circ c) = a \circ (bc + 1) = a(bc + 1) + 1 = abc + a + 1$$

$c \neq a$ olduğu her durumda iki sonuç farklıdır; örneğin $a = 1, b = 1, c = 2$ için sol taraf 5, sağ taraf 4 çıkar. İşlem asosyatif **değildir**.

b) $\mathbb{Q}$ 'da çarpma komutatif olduğundan

$$a \circ b = ab + 1 = ba + 1 = b \circ a$$

olur; işlem komutatifdir.

c) Her a için $e \circ a = a$ olacak sabit bir e arıyoruz. $a \in \mathbb{Q} - \{0\}$ alalım:

$$e \circ a = ea + 1 = a \implies e = \frac{a-1}{a}$$

Bulunan değer a 'ya bağlı çıktı; oysa birim elemanın a 'dan bağımsız tek bir eleman olması gerekir. O hâlde $\langle \mathbb{Q}, \circ \rangle$ 'nin birim elemanı **yoktur**.

■

Örnek 1.2 (Birimi ve Tersleri Olan Bir Yapı). $\mathbb{Q}$ kümesinde $a \circ b = \frac{ab}{2}$ işlemi tanımlanıyor.

- $\circ$ asosyatif midir?
- $\circ$ komutatif midir?
- $\langle \mathbb{Q}, \circ \rangle$ 'nin birim elemanı var mıdır?
- 0'ın bu yapıda tersi var mıdır?
- $a \in \mathbb{Q} - \{0\}$ elemanının tersi var mıdır; varsa nedir?

Çözüm.

a) $\mathbb{Q}$ 'da çarpmanın asosyatifliğinden

$$(a \circ b) \circ c = \frac{ab}{2} \circ c = \frac{abc}{4}, \quad a \circ (b \circ c) = a \circ \frac{bc}{2} = \frac{abc}{4}$$

olur; işlem asosyatifdir.

b) $a \circ b = \frac{ab}{2} = \frac{ba}{2} = b \circ a$; işlem komutatifdir.

c) $e \circ a = \frac{ea}{2} = a$ eşitliğini her a için sağlayan tek rasyonel sayı $e = 2$ 'dir ve $2 \in \mathbb{Q}$ 'dur. Birim eleman 2'dir.

d) x 'in 0'ın tersi olması için $x \circ 0 = 2$ olması gerekir. Ama

$$x \circ 0 = \frac{x \cdot 0}{2} = 0 \neq 2$$

olduğundan böyle bir x yoktur: 0'in tersi **yoktur**.

e) $x \circ a = 2$ denkleminde

$$\frac{xa}{2} = 2 \implies x = \frac{4}{a} \in \mathbb{Q} \quad (a \neq 0)$$

bulunur; komutatiflikten $a \circ \frac{4}{a} = 2$ de sağlanır. Sıfırdan farklı her a 'nın tersi $\frac{4}{a}$ 'dır.

■

1.6 Tanıdık Kümelerde Bir Tur

Aşağıdaki gözlemler, tanımları en bildik kümeler üzerinde sınar. $\mathbb{Z}_\epsilon = \{0, \mp 2, \mp 4, \dots\}$ çift tam sayıları, $\mathbb{Z}_t = \{\mp 1, \mp 3, \mp 5, \dots\}$ tek tam sayıları gösterebilir.

1. $M = \{0, 1, 2, \dots\}$ kümesi toplamaya göre kapalıdır; $\langle M, + \rangle$ asosyatif ve komutatif bir cebirsel yapıdır, birimi 0'dır. Ama 0'dan farklı hiçbir elemanın tersi yoktur; 0'in tersi kendisidir.
2. $M = \mathbb{Z} \cup \{\frac{1}{n} : n = 2, 3, \dots\}$ kümesi $\mathbb{Q}$ 'daki çarpmaya göre kapalı **değildir**: 2 ve $\frac{1}{3}$ kümededir ama $2 \cdot \frac{1}{3} = \frac{2}{3}$ kümede değildir.
3. $\mathbb{R}^+$ ve $\mathbb{R}^-$ kümeleri toplamaya göre kapalıdır ve işlem asosyatif ile komutatifdir; fakat 0 bu kümelerde olmadığından $\langle \mathbb{R}^+, + \rangle$ ve $\langle \mathbb{R}^-, + \rangle$ 'nin birim elemanı yoktur.
4. $\mathbb{Z}_t$ toplamaya göre kapalı değildir: iki tek sayının toplamı çifttir.
5. $\langle \mathbb{Z}_\epsilon, + \rangle$ kapalı, asosyatif ve komutatifdir; birimi 0, her a 'nın tersi $-a \in \mathbb{Z}_\epsilon$ 'dir.
6. $\langle \mathbb{R}^+, \cdot \rangle$ kapalı, asosyatif ve komutatifdir; birimi 1, her α 'nın tersi $\frac{1}{\alpha} \in \mathbb{R}^+$ 'dir.
7. $\langle \mathbb{Z}_t, \cdot \rangle$ kapalı, asosyatif ve komutatifdir, birimi 1'dir; ama ∓ 1 dışındaki hiçbir tek sayının tersi yoktur (1 ile -1 kendi kendisinin tersidir).
8. $\langle \mathbb{Z}_\epsilon, \cdot \rangle$ kapalı, asosyatif ve komutatifdir; fakat 1 çift olmadığından birim elemanı yoktur.

Bu tablo şunu gösteriyor: kapalılık, asosyatiflik, birim ve ters birbirinden bağımsız koşullardır — her biri diğerleri sağlanırken tek başına bozulabilir. Bir sonraki bölümde bu koşulların hangi bileşimlerinin hangi yapıları doğurduğunu adlandıracacağız: **yarı grup**, **monoid** ve **grup**.

2. Yarı Grup, Monoid ve Grup

Önceki bölümde kapalılık, asosyatiflik, birim ve ters koşullarının birbirinden bağımsız olduğunu gördük. Şimdi bu koşulları katman katman ekleyerek cebirin temel yapı hiyerarşisini kuruyoruz: yalnız asosyatiflik varsa **yarı grup**, birim de eklenirse **monoid**, her elemanın tersi de varsa **grup**. Bu dersin geri kalanının kahramanı gruptur; yarı grup ve monoid ise grubun hangi koşuldan vazgeçilince nasıl zayıfladığını gösteren ara duraklardır.

2.1 Yarı Grup ve Monoid

Tanım 2.1 (Tek İşlemlili Cebirsel Yapı). İçinde bir tane ikili işlem tanımlanmış cebirsel yapıya **tek işlemlili cebirsel yapı** denir.

Tanım 2.2 (Yarı Grup). İçinde asosyatif bir ikili işlem tanımlanmış tek işlemlili cebirsel yapıya **yarı grup** denir. Yarı grubun işlemi ayrıca komutatif ise yapıya **komutatif (abelyen) yarı grup** denir.

Tanım 2.3 (Monoid). Birim elemanı olan yarı gruba **monoid** denir. Monoidin işlemi komutatif ise yapıya **komutatif (abelyen) monoid** denir.

Tanımları aksiyom listeleri hâlinde yazmak, bir yapıyı denetlerken neyi sırayla kontrol edeceğimizi netleştirir. $M \neq \emptyset$ kümesinde bir $\circ$ işlemi verilsin.

Yarı grup aksiyomları:

$$\text{I. } \forall a, b \in M \quad a \circ b \in M \quad (\text{kapalılık})$$

$$\text{II. } \forall a, b, c \in M \quad (a \circ b) \circ c = a \circ (b \circ c) \quad (\text{asosyatiflik})$$

Monoid aksiyomları: I ve II'ye ek olarak

$$\text{III. } \exists e \in M \text{ öyle ki } \forall a \in M \quad e \circ a = a \circ e = a \quad (\text{birim eleman})$$

Komutatif yapılar için listeye $\forall a, b \in M$ için $a \circ b = b \circ a$ koşulu eklenir; bu durumda III'te tek taraflı $e \circ a = a$ koşulu yeterlidir, çünkü komutatiflik diğer tarafı bedavaya getirir.

2.2 Grup Kavramı

Tanım 2.4 (Grup). $G \neq \emptyset$ kümesinde aşağıdaki dört koşulu sağlayan bir $\circ$ ikili işlemi tanımlanmış olsun:

$$\text{I. } \forall a, b \in G \quad a \circ b \in G$$

$$\text{II. } \forall a, b, c \in G \quad (a \circ b) \circ c = a \circ (b \circ c)$$

$$\text{III. } \exists e \in G \text{ öyle ki } \forall a \in G \quad e \circ a = a \circ e = a$$

$$\text{IV. } \forall a \in G \quad \exists a^* \in G \text{ öyle ki } a^* \circ a = a \circ a^* = e$$

Bu durumda $\langle G, \circ \rangle$ tek işlemlili cebirsel yapısına bir **grup** denir; $G, \circ$ işlemine göre bir gruptur denir.

Tanım 2.5 (Komutatif (Abelyen) Grup). $\langle G, \circ \rangle$ grubundaki $\circ$ işlemi komutatif ise gruba **komutatif grup** veya **abelyen grup** denir.

Grup, birimli ve her elemanı tersinir bir monoiddir: yarı grup $\subset$ monoid $\subset$ grup zinciri, her adımda bir aksiom ekler. Birim elemanın ve terslerin teklik teoremleri önceki bölümde kanıtlandığından, bir grupta e ve her a 'nın tersi otomatik olarak tek türlü belirlidir; bu gerçeğe sık sık başvuracağız.

2.3 Tanıdık Yapıların Sınıflandırması

Örnek 2.1 (Sayı Kümelerinin Sınıflandırması). Aşağıdaki yapıların her birinin yarı grup mu, monoid mi, grup mu olduğunu belirleyiniz. ($\mathbb{N} = \{1, 2, 3, \dots\}$; $\mathbb{Z}_c$ çift, $\mathbb{Z}_t$ tek tam sayılar.)

$$\begin{aligned} &\langle \mathbb{N}, + \rangle, \quad \langle \mathbb{N}, \cdot \rangle, \quad \langle \mathbb{Z}, + \rangle, \quad \langle \mathbb{Z}, \cdot \rangle, \quad \langle \mathbb{Q}, + \rangle, \quad \langle \mathbb{Q} - \{0\}, \cdot \rangle \\ &\langle \mathbb{R}, + \rangle, \quad \langle \mathbb{R} - \{0\}, \cdot \rangle, \quad \langle \mathbb{R}^+, + \rangle, \quad \langle \mathbb{R}^-, + \rangle, \quad \langle \mathbb{R}^+, \cdot \rangle \\ &\langle \mathbb{Z}_c, + \rangle, \quad \langle \mathbb{Z}_t, \cdot \rangle, \quad \langle \mathbb{Z}_c, \cdot \rangle \end{aligned}$$

Çözüm.

Hepsinde işlem, alışılmış toplama ya da çarpma olduğundan asosiyatiflik ve komutatiflik hazır; ayırt edici sorular kapalılık, birim ve terslerdir.

- $\langle \mathbb{N}, + \rangle$: kapalı, ama $0 \notin \mathbb{N}$ olduğundan birim yok — **komutatif yarı grup**. Grup olamaz.
- $\langle \mathbb{N}, \cdot \rangle$: kapalı, birimi 1; ama örneğin $x \cdot 2 = 1$ denkleminin $\mathbb{N}$ 'de çözümü olmadığından 2'nin tersi yok — **komutatif monoid**.
- $\langle \mathbb{Z}, + \rangle$: birimi 0, her a 'nın tersi $-a$ — **komutatif grup**.
- $\langle \mathbb{Z}, \cdot \rangle$: birimi 1; ∓ 1 dışındakilerin tersi yok — **komutatif monoid**.
- $\langle \mathbb{Q}, + \rangle, \langle \mathbb{R}, + \rangle$: **komutatif grup**.
- $\langle \mathbb{Q} - \{0\}, \cdot \rangle, \langle \mathbb{R} - \{0\}, \cdot \rangle$: sıfır atıldığı için her elemanın tersi kümededir — **komutatif grup**. (Sıfırdan farklı iki sayının çarpımı sıfırdan farklı olduğundan kapalılık da korunur.)
- $\langle \mathbb{R}^+, + \rangle$ ve $\langle \mathbb{R}^-, + \rangle$: birim eleman yok — birer **komutatif yarı grup**.
- $\langle \mathbb{R}^+, \cdot \rangle$: birimi 1, tersler $\frac{1}{a}$ — **komutatif grup**.
- $\langle \mathbb{Z}_c, + \rangle$: birimi 0, tersler $-a$ — **komutatif grup**.
- $\langle \mathbb{Z}_t, \cdot \rangle$: birimi 1; ∓ 1 dışında ters yok — **komutatif monoid**.
- $\langle \mathbb{Z}_c, \cdot \rangle$: birim eleman yok (1 çift değildir) — **komutatif yarı grup**.

■

Tablonun dengesine dikkat edin: aynı küme bir işleme göre grupken ($\langle \mathbb{Z}, + \rangle$) öbür işleme göre yalnızca monoid kalabilir ($\langle \mathbb{Z}, \cdot \rangle$). Yapı, kümenin değil *küme ile işlemin birlikte* özelliğidir.

Bir sonraki bölümde soyut tanımın ete kemiğe büründüğü daha zengin örnekleri inceleyeceğiz: üçlüler kümesi üzerinde kurulan gruplar ve sıfırdan farklı kompleks sayıların çarpma grubu — **grup örnekleri**.

3. Grup Örnekleri

Grup tanımı dört maddelik kısa bir listedir; ama bir kümenin grup olduğunu *göstermek*, o listenin her maddesini verilen işlem için tek tek doğrulamak demektir. Bu bölümde iki kapsamlı örnek üzerinde bu denetimin nasıl yürütüldüğünü görüyoruz. İkinci örnek – sıfırdan farklı kompleks sayıların çarpma grubu – ileride alt gruplar ve homomorfiler için ana sahnelerimizden biri olacak.

3.1 Bileşenli İşlemle Kurulan Bir Grup

Örnek 3.1 (Üçlüler Kümesinde Grup). $G = \{(a, b, 2) : a, b \in \mathbb{R} - \{0\}\}$ kümesinde

$$(a, b, 2) \circ (c, d, 2) = (ac, bd, 2)$$

işlemi tanımlanıyor. $\langle G, \circ \rangle$ 'nin komutatif bir grup olduğunu gösteriniz.

Çözüm.

$(1, 1, 2) \in G$ olduğundan $G \neq \emptyset$ 'dir. Aksiyomları sırayla denetleyelim.

Kapalılık. $a, b, c, d \in \mathbb{R} - \{0\}$ ise $ac \neq 0$ ve $bd \neq 0$ olur; dolayısıyla

$$(a, b, 2) \circ (c, d, 2) = (ac, bd, 2) \in G$$

Asosyatiflik. $\mathbb{R}$ 'de çarpma asosyatif olduğundan

$$\begin{aligned} [(a, b, 2) \circ (c, d, 2)] \circ (e, f, 2) &= ((ac)e, (bd)f, 2) \\ &= (a(ce), b(df), 2) = (a, b, 2) \circ [(c, d, 2) \circ (e, f, 2)] \end{aligned}$$

Komutatiflik. $\mathbb{R}$ 'de çarpma komutatif olduğundan

$$(a, b, 2) \circ (c, d, 2) = (ac, bd, 2) = (ca, db, 2) = (c, d, 2) \circ (a, b, 2)$$

Birim eleman. $(x, y, 2) \circ (a, b, 2) = (a, b, 2)$ olması için $xa = a$ ve $yb = b$ gerekir; $a \neq 0, b \neq 0$ olduğundan $x = 1, y = 1$ bulunur. Birim eleman $(1, 1, 2) \in G$ 'dir.

Ters eleman. $(a^\circ, b^\circ, 2) \circ (a, b, 2) = (1, 1, 2)$ denkleminden $a^\circ a = 1, b^\circ b = 1$; yani

$$a^\circ = \frac{1}{a}, \quad b^\circ = \frac{1}{b}$$

$a, b \neq 0$ olduğundan bu değerler $\mathbb{R} - \{0\}$ 'dadır: $(a, b, 2)$ 'nin tersi $(\frac{1}{a}, \frac{1}{b}, 2) \in G$ 'dir.

Beş koşulun tümü sağlandığından $\langle G, \circ \rangle$ komutatif bir gruptur.

■

Üçüncü bileşendeki 2 hiçbir işe karışmıyor; görevi yalnızca kümenin elemanlarını “etiketlemek”. Örnek, grup yapısının kümenin elemanlarının *ne olduğuna* değil, işlemin *nasıl davrandığına* bağlı olduğunu vurguluyor.

3.2 Kompleks Sayıların Çarpma Grubu

Teorem 3.1 (Sıfırdan Farklı Kompleks Sayılar Grubu). $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ ve $0 = 0 + 0i$ olmak üzere $\mathbb{C} - \{0\}$ kümesi,

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

çarpma işlemine göre komutatif bir gruptur.

İspat.

$1 = 1 + 0i \in \mathbb{C} - \{0\}$ olduğundan küme boş değildir.

Kapalılık. Çarpımın bileşenleri gerçel olduğundan $(a + bi)(c + di) \in \mathbb{C}$ 'dir; asıl gösterilmesi gereken, çarpımın 0 olamayacağıdır. Tersini varsayalım: $a + bi \neq 0, c + di \neq 0$ iken

$$(ac - bd) + (ad + bc)i = 0 + 0i \implies ac = bd, \quad ad = -bc$$

olsun. $a + bi \neq 0$ olduğundan a ve b 'den en az biri sıfırdan farklıdır; $a \neq 0$ kabul edebiliriz (aksi hâlde $b \neq 0$ ile aynı akıl yürütme simetrik olarak yapılır). Birinci eşitliği c , ikincisini d ile çarpalım:

$$ac^2 = bdc, \quad ad^2 = -bcd$$

Taraf tarafa toplarsak $a(c^2 + d^2) = 0$ olur; $a \neq 0$ olduğundan $c^2 + d^2 = 0$, yani $c = d = 0$ bulunur. Bu, $c + di \neq 0$ varsayımıyla çelişir. Demek ki çarpım sıfır olamaz ve $\mathbb{C} - \{0\}$ çarpıma göre kapalıdır.

Asosyatiflik. İki tarafı bileşenlerine açalım:

$$\begin{aligned} [(a + bi)(c + di)](e + fi) &= (ac - bd)e - (ad + bc)f \\ &\quad + (ac - bd)f + (ad + bc)e \ i \\ (a + bi)[(c + di)(e + fi)] &= a(ce - df) - b(cf + de) \\ &\quad + (a(cf + de) + b(ce - df)) \ i \end{aligned}$$

Parantezler açıldığında iki tarafın gerçel bileşenleri de sanal bileşenleri de $ace - adf - bcf - bde$ ve $acf + ade + bce - bdf$ olarak çakışır; işlem asosyatiftir.

Komutatiflik. $\mathbb{R}$ 'de toplama ve çarpma komutatif olduğundan

$$\begin{aligned} (a + bi)(c + di) &= (ac - bd) + (ad + bc)i \\ &= (ca - db) + (cb + da)i = (c + di)(a + bi) \end{aligned}$$

Birim eleman. $(1 + 0i)(a + bi) = a + bi$ olduğundan birim eleman $1 = 1 + 0i$ 'dir.

Ters eleman. $(a^\circ + b^\circ i)(a + bi) = 1 + 0i$ denklemi, bileşenlere göre

$$aa^\circ - bb^\circ = 1, \quad a^\circ b + b^\circ a = 0$$

sistemini verir. Birinci denklemi a ile, ikincisini b ile çarpıp toplarsak

$$a^\circ(a^2 + b^2) = a$$

birinci denklemi $-b$ ile, ikincisini a ile çarpıp toplarsak

$$b^\circ(a^2 + b^2) = -b$$

bulunur. $a + bi \neq 0$ olduğundan $a^2 + b^2 \neq 0$ 'dır; o hâlde

$$a^\circ = \frac{a}{a^2 + b^2}, \quad b^\circ = \frac{-b}{a^2 + b^2}$$

a ve b 'den en az biri sıfırdan farklı olduğundan a° ile b° 'den de en az biri sıfırdan farklıdır; yani

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \in \mathbb{C} - \{0\}$$

Bütün koşullar sağlandığından $\langle \mathbb{C} - \{0\}, \cdot \rangle$ komutatif bir gruptur.

■

Bu grubu bundan böyle $\mathbb{C}^* = \langle \mathbb{C} - \{0\}, \cdot \rangle$ ile göstereceğiz. Kapalılık adımında kanıtlanan “iki sıfırdan farklı kompleks sayının çarpımı sıfırdan farklıdır” gerçeği, $\mathbb{C}$ 'nin sıfır bölensiz olması demektir; alt grup örneklerinde bu gerçeğe yeniden başvuracağız.

3.3 Alıştırmalar

Alıştırma 3.1 (Bir Yapay İşlem Grubu). $G = \mathbb{R} - \{-1\}$ kümesinde $a * b = a + b + ab$ işlemi tanımlanıyor. $\langle G, * \rangle$ 'nin komutatif bir grup olduğunu gösteriniz.

Çözüm.

Önce kapalılığı görelim: $a * b = a + b + ab = (1 + a)(1 + b) - 1$ 'dir. $a, b \neq -1$ ise $1 + a \neq 0$ ve $1 + b \neq 0$, dolayısıyla $(1 + a)(1 + b) \neq 0$ ve $a * b \neq -1$ olur: işlem G 'de kapalıdır.

Asosyatiflik: Aynı özdeşlikle

$$(a * b) * c = (1 + a * b)(1 + c) - 1 = (1 + a)(1 + b)(1 + c) - 1$$

$$a * (b * c) = (1 + a)(1 + b * c) - 1 = (1 + a)(1 + b)(1 + c) - 1$$

iki taraf eşittir.

Komutatiflik: $a * b = a + b + ab = b + a + ba = b * a$.

Birim eleman: $e * a = a$ için $e + a + ea = a$, yani $e(1 + a) = 0$; $a \neq -1$ olduğundan $e = 0 \in G$ bulunur.

Ters eleman: $a * a = 0$ için $a^*(1 + a) = -a$, yani

$$a^* = \frac{-a}{1 + a}$$

Bu değer -1 olamayacağını görelim: $\frac{-a}{1+a} = -1$ olsaydı $-a = -1 - a$, yani $0 = -1$ çıkardı. O hâlde $a^* \in G$ 'dir ve komutatiflikten iki yanlı ters koşulu sağlanır.

Dört aksiyom ve komutatiflik sağlandığından $\langle G, * \rangle$ komutatif bir gruptur.

■

Alıştırma 3.2 (Bileşenleri Karışık Bir Grup). $G = \{(2a, b) : a \in \mathbb{Z}, b \in \mathbb{Q} - \{0\}\}$ kümesinde

$$(2a, b) \circ (2c, d) = \left(2a + 2c, \frac{bd}{3}\right)$$

işlemi tanımlanıyor. $\langle G, \circ \rangle$ 'nin komutatif bir grup olduğunu gösteriniz.

Çözüm.

Kapalılık: $2a + 2c = 2(a + c)$ çift tam sayıdır ve $b, d \neq 0$ iken $\frac{bd}{3} \in \mathbb{Q} - \{0\}$ 'dir; sonuç G 'dedir.

Asosyatiflik: Birinci bileşen sıradan tam sayı toplaması olduğundan asosyatiftir; ikinci bileşende iki taraf da aynı sonucu verir:

$$\frac{\frac{bd}{3} \cdot f}{3} = \frac{bdf}{9} = \frac{b \cdot \frac{df}{3}}{3}$$

O hâlde işlem asosyatiftir.

Komutatiflik: Her iki bileşendeki işlem de komutatifdir.

Birim eleman: $(2x, y) \circ (2a, b) = (2a, b)$ için $2x + 2a = 2a$ ve $\frac{yb}{3} = b$ gerekir; $x = 0$ ve $y = 3$ bulunur.

Birim eleman $(0, 3) \in G$ 'dir.

Ters eleman: $(2a^\circ, b^\circ) \circ (2a, b) = (0, 3)$ denkleminde $2a^\circ = -2a$ ve $\frac{b^\circ b}{3} = 3$, yani

$$(2a, b)^{-1} = \left(-2a, \frac{9}{b}\right) \in G$$

Hepsi sağlandığından $\langle G, \circ \rangle$ komutatif bir gruptur.

■

Alıştırma 3.3 (Kompleks Sayıların Toplam Grubu). $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ kümesinin

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

toplama işlemine göre komutatif bir grup olduğunu gösteriniz.

Çözüm.

Kapalılık: Bileşenler gerçel sayı toplamları olduğundan sonuç $\mathbb{C}$ 'dedir.

Asosyatiflik ve komutatiflik: Her iki bileşende de $\mathbb{R}$ 'deki toplanmanın asosyatifliği ve komutatifliği kullanılır:

$$\begin{aligned} [(a + bi) + (c + di)] + (e + fi) &= (a + c + e) + (b + d + f)i \\ &= (a + (c + e)) + (b + (d + f))i \end{aligned}$$

ve $(a + c) + (b + d)i = (c + a) + (d + b)i$.

Birim eleman: $0 = 0 + 0i$ için $(0 + 0i) + (a + bi) = a + bi$ 'dir.

Ters eleman: $a + bi$ 'nin tersi $(-a) + (-b)i \in \mathbb{C}$ 'dir:

$$(a + bi) + ((-a) + (-b)i) = 0 + 0i$$

Böylece $\langle \mathbb{C}, + \rangle$ komutatif bir gruptur.

■

Şimdiye dek grup olduğunu gösterdiğimiz her yapıda dört aksiyyomun dördünü de tek tek denetledik. Bir sonraki bölümün konusu tam bu yükü hafifletmek: aksiyyomların bir bölümünü zayıflatıp gerisini *teorem* olarak elde edeceğiz – **grup aksiyyomlarının esnetilmesi**.

4. Grup Aksiyomlarının Esnetilmesi

Grup tanımındaki III ve IV aksiyomları iki yanlıdır: birim eleman her iki yandan etkisiz, ters eleman her iki yandan ters olmalıdır. Bu bölümün ilk sonucu şaşırtıcıdır: yalnızca *sol* birim ve *sol* ters istemek yeterlidir — sağ taraflar kendiliğinden gelir. Ardından aksiyomları bambaşka iki biçimde daha karakterize edeceğiz: denklemlerin çözülebilirliği ve (sonlu kümelerde) sadeleştirme kuralları. Bu ölçütler, bir yapının grup olduğunu göstermenin pratikte en kısa yollarını verir.

4.1 Sol Birim ve Sol Ters Yeterlidir

Teorem 4.1 (Zayıflatılmış Grup Aksiyomları). $G \neq \emptyset$ kümesinde tanımlı bir $\circ$ işlemi şu koşulları sağlasın:

$$\text{I. } \forall a, b \in G \quad a \circ b \in G$$

$$\text{II. } \forall a, b, c \in G \quad (a \circ b) \circ c = a \circ (b \circ c)$$

$$\text{III}^*. \exists e \in G \text{ öyle ki } \forall a \in G \quad e \circ a = a \quad (\text{sol birim})$$

$$\text{IV}^*. \forall a \in G \exists a^* \in G \text{ öyle ki } a^* \circ a = e \quad (\text{sol ters})$$

Bu takdirde $\langle G, \circ \rangle$ bir gruptur.

İspat.

1) **Sol ters aynı zamanda sağ terstir.** $a \in G$ olsun ve IV^* 'daki a^* 'yı alalım: $a^* \circ a = e$. Önce

$$(a^* \circ a) \circ a^* = e \circ a^* = a^*$$

yazalım (III^* kullanıldı); asosyatiflikle bu,

$$a^* \circ (a \circ a^*) = a^*$$

demektir. IV^* 'ı bu kez a^* için kullanalım: $a^{**} \circ a^* = e$ olacak biçimde $a^{**} \in G$ vardır. Son eşitliği soldan a^{**} ile işlemle sokup asosyatifliği uygulayalım:

$$a^{**} \circ [a^* \circ (a \circ a^*)] = a^{**} \circ a^* \implies (a^{**} \circ a^*) \circ (a \circ a^*) = a^{**} \circ a^*$$

$$\implies e \circ (a \circ a^*) = e \implies a \circ a^* = e$$

Son adımda III^* kullanıldı. Demek ki a^* , a 'nın sağ tersi de olur.

2) **Sol birim aynı zamanda sağ birimdir.** Herhangi bir $a \in G$ için IV^* 'dan $a^* \circ a = e$ vardır. O hâlde

$$a \circ e = a \circ (a^* \circ a) = (a \circ a^*) \circ a = e \circ a = a$$

Burada sırasıyla asosyatiflik, 1)'de kanıtlanan $a \circ a^* = e$ ve III^* kullanıldı.

Böylece e iki yanlı birim, her a^* iki yanlı terstir: $\langle G, \circ \rangle$, grup tanımındaki I–IV koşullarının tümünü sağlar. ■

Teoremin iki yan ürünü, ileride sürekli kullanılacak:

- III^* 'daki e , grubun (tek türlü belirli) birim elemanıdır: bir grubun bir ve yalnız bir birim elemanı vardır.
- 1)'den dolayı $a^* \circ a = a \circ a^* = e$ 'dir; işlem asosyatif olduğundan ters tek türlü belirlidir: grubun her elemanının bir ve bir tek tersi vardır.

4.2 Denklemlerle Karakterizasyon

Teorem 4.2 (Çözülebilirlik Aksiyomuyla Grup). $G \neq \emptyset$ kümesinde tanımlı bir $\circ$ işlemi kapalılık (I) ve asosiyatiflik (II) koşullarına ek olarak şunu sağlasın:

$$\text{III}' . \forall a, b \in G \text{ için } a \circ x = b \text{ ve } y \circ a = b \text{ denklemleri } G \text{ 'de çözülebilir.}$$

Bu takdirde $\langle G, \circ \rangle$ bir gruptur.

İspat.

Zayıflatılmış aksiyomlar teoreminden dolayı III* ile IV*'ı türetmek yeterlidir.

Sol birim vardır. Herhangi bir $b \in G$ seçelim. III' 'den $y \circ b = b$ denkleminin bir çözümü vardır; buna e diyelim: $e \circ b = b$. Şimdi bu e 'nin her $a \in G$ için sol birim olduğunu görelim. III' 'den $b \circ x = a$ olacak biçimde bir $x \in G$ vardır; o hâlde

$$e \circ a = e \circ (b \circ x) = (e \circ b) \circ x = b \circ x = a$$

Sol ters vardır. Herhangi bir $a \in G$ için III' 'deki $y \circ a = b$ denkleminde $b = e$ alalım: $a^* \circ a = e$ olacak biçimde $a^* \in G$ vardır.

I, II, III*, IV* sağlandığından $\langle G, \circ \rangle$ gruptur.

■

Grup olduğu bilinen bir yapıda bu denklemlerin çözümleri yalnız var olmakla kalmaz, tek türlü belirlidir:

Teorem 4.3 (Denklemlerin Tek Çözümü). Bir $\langle G, \circ \rangle$ grubunda her $a, b \in G$ çifti için $a \circ x = b$ ve $y \circ a = b$ denklemlerinin çözümleri tek türlü belirlidir ve

$$x = a^{-1} \circ b, \quad y = b \circ a^{-1}$$

ile verilir. (Burada a^{-1} , a 'nın tersidir.)

İspat.

$a \circ x = b$ ise iki tarafı soldan a^{-1} ile işleme sokalım:

$$a^{-1} \circ (a \circ x) = a^{-1} \circ b \implies (a^{-1} \circ a) \circ x = a^{-1} \circ b$$

$$\implies e \circ x = a^{-1} \circ b \implies x = a^{-1} \circ b$$

Demek ki çözüm varsa ancak $a^{-1} \circ b$ olabilir. Tersine bu değer gerçekten çözümdür:

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

$y \circ a = b$ denklemi için tamamen benzer biçimde: $y \circ a = b$ ise sağdan a^{-1} uygulanarak $y = b \circ a^{-1}$ bulunur ve $(b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a) = b$ sağlanır.

■

4.3 Sadeleştirme Kuralları

Teorem 4.4 (Sadeleştirme Kuralları). $\langle G, \circ \rangle$ bir grup ve $a, x, x', y, y' \in G$ olsun. O zaman

$$a \circ x = a \circ x' \implies x = x', \quad y \circ a = y' \circ a \implies y = y'$$

İspat.

Birinci gerektirme için iki tarafı soldan a^{-1} ile işleme sokmak yeterlidir:

$$a^{-1} \circ (a \circ x) = a^{-1} \circ (a \circ x') \implies (a^{-1} \circ a) \circ x = (a^{-1} \circ a) \circ x'$$

$$\implies e \circ x = e \circ x' \implies x = x'$$

İkincisi için sağdan a^{-1} uygulanır:

$$(y \circ a) \circ a^{-1} = (y' \circ a) \circ a^{-1} \implies y \circ (a \circ a^{-1}) = y' \circ (a \circ a^{-1}) \implies y = y'$$

■

Sadeleştirme kurallarına **bölümün tekliği aksiyomu** veya **kısaltma aksiyomu** da denir. Sonsuz kümelerde bu kurallar tek başına grup olmaya yetmez; ama sonlu kümelerde durum bambaşkadır:

Teorem 4.5 (Sonlu Kümelerde Grup Ölçütü). $G \neq \emptyset$ sonlu bir küme olsun. G 'de tanımlı bir $\circ$ işlemi kapalılık (I), asosiyatiflik (II) ve sadeleştirme kurallarını (III') sağlıyorsa $\langle G, \circ \rangle$ bir gruptur.

İspat.

Çözülebilirlik teoreminden dolayı III'ü, yani $a \circ x = b$ ve $y \circ a = b$ denklemlerinin çözülebilirliğini göstermek yeterlidir.

$a, b \in G$ verilsin. $\Psi_a : G \rightarrow G, x \mapsto a \circ x$ fonksiyonunu tanımlayalım (kapalılıktan her x için $a \circ x \in G$ 'dir).

Ψ_a iyi tanımlıdır: $x = x'$ ise $a \circ x = a \circ x'$ 'dir.

Ψ_a birebirdir: $\Psi_a(x) = \Psi_a(x')$ ise $a \circ x = a \circ x'$, sadeleştirme kuralından $x = x'$ olur.

Ψ_a üzerinedir: Sonlu bir kümeyi kendi içine resmeden birebir fonksiyon üzerinedir.

O hâlde $b \in G$ 'ye karşılık $\Psi_a(x) = a \circ x = b$ olacak biçimde bir $x \in G$ vardır: birinci denklem çözülebilir. $y \circ a = b$ denklemi için $\Phi_a : G \rightarrow G, y \mapsto y \circ a$ fonksiyonuyla tamamen benzer akıl yürütme yapılır. III'ü sağlandığından $\langle G, \circ \rangle$ gruptur.

■

⚠ Sonluluk vazgeçilmezdir

Sonlu kümelerde grup ölçütü sonsuz kümelerde geçerli olmak zorunda değildir. Örneğin $\langle \mathbb{N}, \cdot \rangle$ yapısı kapalıdır, asosiyatif ve sadeleştirme kurallarını sağlar ($ax = ax' \Rightarrow x = x'$); ama grup değildir — birimden başka hiçbir elemanın tersi yoktur. İspattaki “sonlu kümede birebir fonksiyon üzerinedir” adımı, sonsuz kümelerde çöker.

4.4 Sonlu Grup ve Mertebe

Tanım 4.1 (Sonlu ve Sonsuz Grup). $\langle G, \circ \rangle$ yapısında G sonlu bir küme ise yapıya **sonlu cebirsel yapı**, sonsuz ise **sonsuz cebirsel yapı** denir. Özel olarak bir grup, sonlu kümeysen **sonlu grup**, sonsuz kümeysen **sonsuz grup** adını alır.

Tanım 4.2 (Grubun Mertebesi). G sonlu bir grup ve eleman sayısı n ise n 'ye G 'nin **mertebe**si denir ve $|G| = n$ yazılır. Sonsuz bir grubun mertebe si sonsuz olarak tanımlanır.

Elimizde artık üç ayrı grup ölçütü var: tanımın kendisi, çözülebilirlik ve — sonlu kümelerde — sadeleştirme. Sıradaki bölümde sonlu grupları somut biçimde *görmenin* aracını tanıyacağız: işlem tabloları. Tablolar bize aynı zamanda küçük mertebeli bütün grupları sınıflandırma imkânı verecek — **işlem tabloları ve küçük mertebeli gruplar**.

5. İşlem Tabloları ve Küçük Mertebeli Gruplar

Sonlu bir grubun işlemi, çarpım tablosu gibi bir tabloya sığar. Bu bölümde önce tabloların hangi özellikleri taşımak zorunda olduğunu görüyor, sonra verilen bir tablonun grup tablosu olup olmadığını denetlemeyi öğreniyoruz. Bölümün ikinci yarısı küçük bir sınıflandırma şaheseri: mertebesi 1, 2, 3 olan gruplar tek tiptir; mertebe 4'te ise tam iki tip vardır ve ikisini de tablolarıyla inşa edeceğiz.

5.1 İşlem Tablosu

Tanım 5.1 (İşlem Tablosu). Elemanları $a_1, a_2, \dots, a_n$ olan sonlu bir grubun işlem sonuçları bir tabloyla gösterilir: satır başına a_i , sütun başına a_j yazılır ve kesişim hücreğine $a_i \circ a_j$ konur. Bu tabloya grubun **işlem tablosu** (Cayley tablosu) denir.

Grupta $a \circ x = b$ ve $y \circ a = b$ denklemlerinin çözümleri tek türlü belirli olduğundan önemli bir kısıt doğar: **grubun her elemanı, tablonun her satırında ve her sütununda tam bir kez yer alır.** Gerçekten a_i satırında b elemanı, $a_i \circ x = b$ denkleminin çözüm sayısı kadar — yani tam bir kez — görünür. Bu kural gerekli ama yeterli değildir: satır-sütun düzeni kusursuz olan bir tablo yine de birim eleman ya da asosiyatiflik yüzünden grup tablosu olmayabilir. Aşağıdaki örnek üç durumu birden sergiliyor.

Örnek 5.1 (Tablo Denetimi). Aşağıdaki tabloların bir grubun işlem tablosu olup olmadığını araştırınız.

	$\circ$	a	b	c	d
	a	b	c	d	a
(1)	b	c	d	a	b
	c	a	b	c	d
	d	d	a	b	b

	$\circ$	a	b	c	d
	a	c	d	a	b
(2)	b	a	b	c	d
	c	d	c	b	a
	d	b	a	d	c

	$\circ$	a	b	c
	a	a	b	c
(3)	b	b	c	a
	c	c	a	b

Çözüm.

(1) Son satırda b iki kez görünüyor: $d \circ c = b$ ve $d \circ d = b$. Bir grup tablosunda her eleman her satırda tam bir kez yer almak zorunda olduğundan bu tablo bir grubun işlem tablosu **olamaz**.

(2) Her eleman her satır ve sütunda tam bir kez yer alıyor; fakat birim eleman yok. Birim elemanın satırı, sütun başlıklarını aynen tekrarlamalıdır: b satırı $a b c d$ veriyor, yani $b \circ x = x$ her x için sağlanıyor — b bir *sol* birimdir. Ama b sütunu d, b, c, a olduğundan $a \circ b = d \neq a$ 'dır: b sağ birim değildir ve başka aday da yoktur. Birim elemanı olmayan yapı grup olamayacağından bu tablo da bir grup tablosu **olamaz**.

(3) Her eleman her satır ve sütunda tam bir kez var; a satırı ve sütunu başlıkları tekrarladığından a birim elemandır. Terslere bakalım: tabloda a 'yı veren hücreler $a \circ a, b \circ c, c \circ b$ 'dir; yani

$$a^{-1} = a, \quad b^{-1} = c, \quad c^{-1} = b$$

Geriye asosiyatiflik kalıyor: her x, y, z için $(x \circ y) \circ z = x \circ (y \circ z)$ denetlenmelidir.

Üçlüde a varsa: a birim olduğundan üç durum da kendiliğinden sağlanır. Örneğin $x = a$ için

$$(a \circ y) \circ z = y \circ z = a \circ (y \circ z)$$

$y = a$ ve $z = a$ durumları da aynı biçimde görülür.

Üçlüde a yoksa: $x, y, z \in \{b, c\}$ olan sekiz üçlüyü tek tek denetleyelim:

$$(b \circ b) \circ b = c \circ b = a, \quad b \circ (b \circ b) = b \circ c = a \quad \checkmark$$

$$(b \circ b) \circ c = c \circ c = b, \quad b \circ (b \circ c) = b \circ a = b \quad \checkmark$$

$$(b \circ c) \circ b = a \circ b = b, \quad b \circ (c \circ b) = b \circ a = b \quad \checkmark$$

$$(b \circ c) \circ c = a \circ c = c, \quad b \circ (c \circ c) = b \circ b = c \quad \checkmark$$

$$(c \circ b) \circ b = a \circ b = b, \quad c \circ (b \circ b) = c \circ c = b \quad \checkmark$$

$$(c \circ b) \circ c = a \circ c = c, \quad c \circ (b \circ c) = c \circ a = c \quad \checkmark$$

$$(c \circ c) \circ b = b \circ b = c, \quad c \circ (c \circ b) = c \circ a = c \quad \checkmark$$

$$(c \circ c) \circ c = b \circ c = a, \quad c \circ (c \circ c) = c \circ b = a \quad \checkmark$$

Bütün üçlülerde eşitlik sağlandığından işlem asosyatiftir: (3) tablosu bir grubun işlem tablosudur.

■

i Çarpımsal yazış

Bundan böyle soyut gruplarda işlemi $\circ$ yerine $\cdot$ ile göstereceğiz ve $\langle G, \cdot \rangle$ yapısına **çarpım grubu** diyeceğiz; $a \cdot b$ yerine çoğu zaman kısaca ab yazılır. Birim eleman 1_G , a 'nın tersi a^{-1} ile gösterilir. Bu yalnız bir gösteriş anlaşmasıdır: işlem, sayıların çarpması olmak zorunda değildir.

5.2 Mertebesi 1, 2 ve 3 Olan Gruplar

Mertebe 1. Grup yalnızca birim elemandan oluşur: $G = \{1_G\}$, $1_G \cdot 1_G = 1_G$. Bu gruba **birim grup** denir.

Mertebe 2. $G = \{1_G, a\}$ olsun. 1_G satır ve sütunu bellidir; geriye yalnız $a \cdot a$ hücresi kalır. $a \cdot a = a$ olamaz, çünkü sadeleştirmeyle $a = 1_G$ çıkardı; o hâlde zorunlu olarak

$$a \cdot a = 1_G, \quad \begin{array}{c|cc} \cdot & 1_G & a \\ \hline 1_G & 1_G & a \\ a & a & 1_G \end{array}$$

Asosyatiflik denetiminde üçlüde 1_G varsa iş kendiliğinden biter; hiçbiri 1_G değilse tek aday $x = y = z = a$ 'dır:

$$(a \cdot a) \cdot a = 1_G \cdot a = a, \quad a \cdot (a \cdot a) = a \cdot 1_G = a$$

Demek ki tablo bir grup verir ve **2. mertebeden tek tip grup vardır**; $a^{-1} = a$ 'dır.

Mertebe 3. $G = \{1_G, a, b\}$ olsun. $a \cdot b$ hücresine bakalım: $b \neq 1_G$ olduğundan $a \cdot b \neq a$ (sadeleştirme), $a \neq 1_G$ olduğundan $a \cdot b \neq b$; tek seçenek

$$a \cdot b = 1_G$$

Aynı akıl yürütmeyeyle $b \cdot a = 1_G$ 'dir; yani $a^{-1} = b$, $b^{-1} = a$. Şimdi $a \cdot a$: tersinin tekliğinden $a^{-1} = b \neq a$ olduğundan $a \cdot a \neq 1_G$; $a \neq 1_G$ olduğundan $a \cdot a \neq a$; geriye

$$a \cdot a = b$$

kalır. Tamamen benzer biçimde $b \cdot b = a$ bulunur:

$$\begin{array}{c|ccc} \cdot & 1_G & a & b \\ \hline 1_G & 1_G & a & b \\ a & a & b & 1_G \\ b & b & 1_G & a \end{array}$$

Asosyatiflik, yukarıdaki (3) tablosundaki gibi (o tablo bu grubun $1_G = a$, $a = b$, $b = c$ adlandırmasıyla aynısıdır) denetlenir. **3. mertebeden tek tip grup vardır.**

5.3 Mertebesi 4 Olan Gruplar

$G = \{1_G, a, b, c\}$ olsun. 1_G ile çarpımlar bellidir; kritik soru terslerin dağılımıdır. Her elemanın tek bir tersi vardır ve ters alma, $\{a, b, c\}$ kümesini kendi içinde eşler. İki olasılık vardır: ya üç eleman da kendi kendisinin tersidir ya da biri kendi kendisinin tersi olup öbür ikisi birbirinin tersidir. (Üçünün de “başkasının tersi” olması imkânsızdır: ters alma eşlemesi üç elemanlı kümede sabit noktasız olamaz.)

Birinci hâl: $a^{-1} = a, b^{-1} = b, c^{-1} = c$. Yani $a^2 = b^2 = c^2 = 1_G$. $a \cdot b$ hücresi: $a^{-1} = a \neq b$ olduğundan $a \cdot b \neq 1_G$; sadeleştirmeden $a \cdot b \neq a$ ve $a \cdot b \neq b$; tek seçenek $a \cdot b = c$. Simetrik akıl yürütmeyle

$$ab = ba = c, \quad ac = ca = b, \quad bc = cb = a$$

$\cdot$	1_G	a	b	c
1_G	1_G	a	b	c
a	a	1_G	c	b
b	b	c	1_G	a
c	c	b	a	1_G

Asosyatifliğin denetimi yine “üçlüde 1_G varsa otomatik; yoksa $\{a, b, c\}$ ’den kurulan üçlüler tek tek” yoluyla yapılır; örneğin

$$(a \cdot a) \cdot b = 1_G \cdot b = b, \quad a \cdot (a \cdot b) = a \cdot c = b \quad \checkmark$$

$$(a \cdot b) \cdot a = c \cdot a = b, \quad a \cdot (b \cdot a) = a \cdot c = b \quad \checkmark$$

Kalan üçlüler de aynı biçimde doğrulanır. Bu gruba **Klein tipi grup** denir; komutatiftir.

İkinci hâl: $a^{-1} = a, b^{-1} = c, c^{-1} = b$. Yani $a^2 = 1_G$ ve $bc = cb = 1_G$. $a \cdot b$: yine $\neq 1_G, a, b$ olduğundan $ab = c$; benzerlikle $ba = c$ ve $ac = ca = b$. $b \cdot b$ hücresi: $b^{-1} = c \neq b$ olduğundan $b^2 \neq 1_G$; $b \neq 1_G$ olduğundan $b^2 \neq b$; $b^2 = c$ olsaydı $b^2 = ab$ ’den sadeleştirmeyeyle $b = a$ çıkardı — o da olamaz. Geriye

$$b^2 = a, \quad \text{benzer biçimde} \quad c^2 = a$$

kalır:

$\cdot$	1_G	a	b	c
1_G	1_G	a	b	c
a	a	1_G	c	b
b	b	c	a	1_G
c	c	b	1_G	a

Asosyatiflik birinci hâldeki gibi denetlenir. Bu grupta $b^2 = a, b^3 = ba = c, b^4 = 1_G$ olduğundan bütün grup b ’nin kuvvetlerinden oluşur; ileride bu tip gruplara **devresel grup** diyeceğiz.

Sonuç: **4. mertebeden tam iki tip grup vardır** — Klein tipi ve devresel tip. Her ikisi de komutatiftir; yani mertebesi 4’ü geçmeyen bütün gruplar komutatiftir.

Küçük mertebelerde grupları elle inşa edebildik; ama merteye büyüdükçe tablo kurmak umutsuzlaşır. Bir sonraki bölümde grup elemanlarıyla *cebirsel* hesap yapmanın araçlarını geliştiriyoruz: kuvvetler, katlar ve bunların aritmetiği — **kuvvetler ve katlar**.

6. Kuvvetler ve Katlar

Bir grupta $a \cdot a \cdot a$ gibi çarpımlar yazabilmek için önce ikiden çok elemanın çarpımının parantezlemeden bağımsız olduğunu bilmemiz gerekir. Bu bölümde önce n 'li çarpımı tanımlayıp genel asosyatiflik ve genel komutatiflik kurallarını kaydediyor, sonra bir elemanın tam sayılı kuvvetlerini tanımlayarak lise cebirinden tanıdık kuvvet kurallarının grup ortamındaki karşılıklarını kanıtıyoruz. Bölüm, toplamsal yazıştaki karşılıklar — katlar — ile kapanıyor. Bu aritmetik, devresel gruplar teorisinin tamamının dilidir.

6.1 n 'li Çarpım

Tanım 6.1 (n 'li Çarpım). $\langle G, \cdot \rangle$ bir grup ve $a_1, a_2, \dots, a_n \in G$ olsun ($n \geq 2$). Bu elemanların (bu sıradaki) çarpımı tümevarımla tanımlanır:

- $n = 2$ için $a_1 a_2$ zaten tanımlıdır;
- $n > 2$ için $a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_{n-1}) \cdot a_n$.

Gösteriş: $a_1 a_2 \cdots a_n = \prod_{\nu=1}^n a_\nu$; $n = 1$ için $\prod_{\nu=1}^1 a_\nu = a_1$ olarak tanımlanır.

Teorem 6.1 (Genel Asosyatiflik). Bir grupta herhangi n ($n \geq 3$) elemanın çarpımında çarpanlar, sıraları bozulmadan istenildiği gibi paranteze alınabilir:

$$a_1 \cdots a_k a_{k+1} \cdots a_n = (a_1 \cdots a_k) \cdot (a_{k+1} \cdots a_n) \quad (1 \leq k \leq n-1)$$

Teorem 6.2 (Genel Komutatiflik). $a_1, \dots, a_n$ ($n \geq 2$), bir grubun ikişer ikişer komutatif elemanları olsun ($a_i a_j = a_j a_i$). $i_1, \dots, i_n, 1, \dots, n$ sayılarının herhangi bir permütasyonu olmak üzere

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

İki teorem birlikte şunu söyler: ikişer ikişer komutatif elemanların çarpımında çarpanları istediğimiz sıraya sokabilir ve istediğimiz gibi paranteze alabiliriz. Her iki teorem de n üzerinde tümevarımla kanıtlanır; ispatlar kavramsal bir yenilik içermediğinden ayrıntılarını atlıyoruz.

6.2 Tam Sayılı Kuvvetler

Tanım 6.2 (Bir Elemanın Tam Sayılı Kuvvetleri). $\langle G, \cdot \rangle$ bir grup, $a \in G$ ve $n \in \mathbb{Z}$ olsun. a 'nın n . kuvveti a^n şöyle tanımlanır:

- $n > 0$ için: $a^1 = a$; $n \geq 2$ için $a^n = \underbrace{a \cdot a \cdots a}_{n \text{ tane}}$
- $n = 0$ için: $a^0 = 1_G$
- $n < 0$, $n = -n'$ ($n' > 0$) için: a^{-1} , a 'nın tersi olmak üzere $a^{-n'} = (a^{-1})^{n'} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n' \text{ tane}}$

Teorem 6.3 (Kuvvetlerin Temel Özellikleri). $\langle G, \cdot \rangle$ bir grup, $a, b \in G$ ve $m, n \in \mathbb{Z}$ olsun.

1. $(a^{-1})^{-1} = a$
2. $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$; daha genel olarak $(a_1 a_2 \cdots a_k)^{-1} = a_k^{-1} \cdots a_2^{-1} a_1^{-1}$
3. $a^m \cdot a^n = a^{m+n}$; daha genel olarak $a^{m_1} a^{m_2} \cdots a^{m_k} = a^{m_1+m_2+\cdots+m_k}$
4. $(a^m)^n = a^{mn}$
5. $a \cdot b = b \cdot a$ ise her $n \in \mathbb{Z}$ için $(ab)^n = a^n b^n$; daha genel olarak $a_1, \dots, a_k$ ikişer ikişer komutatif ise $(a_1 \cdots a_k)^n = a_1^n \cdots a_k^n$

İspat.

Kuralların tümü tanımdan tümevarımla çıkar; en öğretici üçünü kanıtlayalım.

1) $a^{-1} \cdot a = a \cdot a^{-1} = 1_G$ eşitliği, ters tanımına göre a 'nın a^{-1} 'in tersi olduğunu söyler; ters tek türlü belirli olduğundan $(a^{-1})^{-1} = a$ 'dır.

2) $x = (ab)^{-1}$ diyelim: $x \cdot (ab) = 1_G$. Asosyatiflikle $(xa)b = 1_G$, yani xa , b 'nin sol tersidir: $xa = b^{-1}$. Buradan sağdan a^{-1} uygulayarak $x = b^{-1}a^{-1}$ bulunur. Genelleştirme k üzerinde tümevarımla yapılır.

5) Üç durumu ayıralım.

$n > 0$: $n = 1$ için eşitlik açıktır. $n \geq 2$ için

$$(ab)^n = \underbrace{(ab)(ab)\cdots(ab)}_n = \underbrace{(aa\cdots a)}_n \underbrace{(bb\cdots b)}_n = a^n b^n$$

Ortak adımda a ile b 'nin komutatifliği sayesinde genel komutatiflik ve genel asosyatiflik kuralları kullanıldı.

$n = 0$: $(ab)^0 = 1_G = 1_G \cdot 1_G = a^0 b^0$.

$n < 0$, $n = -n'$: Önce $ab = ba$ 'dan $(ab)^{-1} = (ba)^{-1}$, yani $b^{-1}a^{-1} = a^{-1}b^{-1}$ olduğunu not edelim: tersler de komutatifdir. O hâlde

$$\begin{aligned} (ab)^{-n'} &= [(ab)^{-1}]^{n'} = (b^{-1}a^{-1})^{n'} = (a^{-1}b^{-1})^{n'} \\ &= (a^{-1})^{n'} (b^{-1})^{n'} = a^{-n'} b^{-n'} = a^n b^n \end{aligned}$$

Ortak adımda pozitif kuvvet durumu ($n' > 0$) uygulandı.

■

⚠ Komutatiflik olmadan 5. kural çöker

$ab \neq ba$ ise $(ab)^n = a^n b^n$ eşitliği genel olarak yanlıştır. Örneğin $(ab)^2 = abab$ 'dir; bunun $a^2 b^2 = aabb$ 'ye eşit olması, ortadaki ba 'nın ab 'ye çevrilebilmesini – yani tam da komutatifliği – gerektirir.

4. kuralın iki kullanışlı özel hâli, $m = -1$ ve $n = -1$ değerleriyle elde edilir:

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

Yani “önce ters alıp sonra kuvvet almak” ile “önce kuvvet alıp sonra ters almak” aynı sonucu verir.

6.3 Toplamsal Yazış: Katlar

Komutatif gruplarda işlem çoğu zaman $+$ ile yazılır; $\langle G, + \rangle$ yapısına **toplam grubu** denir. Bu yazışta birim eleman 0_G ile gösterilir ve **sıfır elemanı** adını alır; a 'nın tersi $-a$ ile gösterilir. Kuvvetin karşılığı ise **kattır**:

Tanım 6.3 (Bir Elemanın Tam Sayılı Katları). $\langle G, + \rangle$ komutatif bir grup, $a \in G$ ve $n \in \mathbb{Z}$ olsun. a 'nın n katı na şöyle tanımlanır:

- $n > 0$ için: $1a = a$; $n \geq 2$ için $na = \underbrace{a + a + \cdots + a}_{n \text{ tane}}$
- $n = 0$ için: $0a = 0_G$
- $n < 0$, $n = -n'$ ($n' > 0$) için: $(-n')a = n'(-a) = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n' \text{ tane}}$

Kuvvet kurallarının katlara çevirisi şöyledir; her biri, çarpımsal kardeşinin birebir kopyasıdır:

- $-(-a) = a$
- $-(a + b) = (-a) + (-b)$; genel olarak $-(a_1 + \cdots + a_k) = (-a_1) + \cdots + (-a_k)$
- $ma + na = (m + n)a$; genel olarak $m_1 a + \cdots + m_k a = (m_1 + \cdots + m_k)a$
- $n(ma) = (nm)a$
- $n(a + b) = na + nb$ (grup komutatif olduğundan bu kural her zaman geçerlidir)

Artık grup elemanlarıyla serbestçe hesap yapabiliyoruz. Sıradaki doğal soru řu: bir grubun *içindeki* hangi alt kümeler, aynı işlemle kendi başlarına grup oluşturur? Bu sorunun yanıtı – alt gruplar – dersin bundan sonraki bütün bölümlerinin zeminidir: [alt gruplar](#).

7. Alt Grup Kavramı ve Ölçütleri

Bir grubun içinde, aynı işlemle kendi başına grup oluşturan alt kümeler yaşar: $\langle \mathbb{Z}, + \rangle$ içindeki çift sayılar, $\langle \mathbb{R} - \{0\}, \cdot \rangle$ içindeki pozitif sayılar gibi. Bu bölümde alt grup kavramını tanımlayıp bir alt kümenin alt grup olduğunu denetlemenin üç pratik ölçütünü kanıtlıyoruz. Ölçütlerin değeri şudur: dört grup aksiyonunu yeniden denetlemek yerine yalnızca bir-iki koşula bakmak yeter — asosyatiflik gibi özellikler büyük gruptan bedavaya miras kalır.

7.1 Alt Grup Tanımı

Tanım 7.1 (Alt Grup). $\langle G, \cdot \rangle$ bir grup ve $\emptyset \neq H \subseteq G$ olsun. H, G 'deki $\cdot$ işlemine göre kendi başına bir grup oluşturuyorsa H 'ye G 'nin bir **alt grubu** denir ve bu durum

$$H \subseteq G$$

a.g.

ile gösterilir.

7.2 Üç Alt Grup Ölçütü

Teorem 7.1 (Alt Grup Ölçütü). $\langle G, \cdot \rangle$ bir grup ve $\emptyset \neq H \subseteq G$ olsun. H 'nin G 'nin bir alt grubu olması için gerek ve yeter koşullar şunlardır:

1. $\forall a, b \in H$ için $a \cdot b \in H$ (kapalılık)
2. $\forall a \in H$ için $a^{-1} \in H$ (terslere kapalılık)

İspat.

Gereklik. H alt grupsa kendisi bir gruptur; grup tanımının I ve IV aksiyomları tam olarak 1) ve 2) koşullarıdır.

Yeterlik. 1) ve 2) sağlansın; H 'nin grup aksiyomlarını taşıdığını görelim.

Kapalılık: 1)'in kendisi.

Asosyatiflik: $(ab)c = a(bc)$ eşitliği G 'nin bütün elemanları için geçerlidir; $H \subseteq G$ olduğundan H 'nin elemanları için de geçerlidir.

Birim eleman: $H \neq \emptyset$ olduğundan bir $a \in H$ seçebiliriz. 2)'den $a^{-1} \in H$; 1)'den

$$a \cdot a^{-1} = 1_G \in H$$

1_G , H 'nin de birim elemanıdır: her $h \in H$ için $1_G h = h 1_G = h$ zaten G 'de sağlanır.

Ters eleman: 2)'nin kendisi.

Dört aksiyom sağlandığından $H \subseteq G$ 'dir.
a.g.

■

İspatın birim eleman adımıından değerli bir yan sonuç çıktı: **alt grubun birimi, büyük grubun birimiyle aynıdır** ($1_H = 1_G$). Benzer biçimde bir elemanın H 'deki tersi, G 'deki tersiyle çakışır. Sonlu gruplarda ikinci koşul bile fazladır:

Teorem 7.2 (Sonlu Gruplarda Alt Grup Ölçütü). $\langle G, \cdot \rangle$ sonlu bir grup ve $\emptyset \neq H \subseteq G$ olsun. H 'nin alt grup olması için gerek ve yeter koşul, H 'nin $\cdot$ işlemine göre kapalı olmasıdır.

İspat.

Gereklik. Alt grup, tanımı gereği kapalıdır.

Yeterlik. H kapalı olsun. G sonlu olduğundan H de sonlu bir kümedir. Sonlu kümelerde grup ölçütünü uygulayalım: kapalılık hipotezdir; asosyatiflik G 'den miras kalır; sadeleştirme kuralları da G 'den miras

kalır — $ax = ax'$ eşitliği G 'de bir grup eşitliği olduğundan $x = x'$ verir. Sonlu küme + kapalılık + asosyatiflik + sadeleştirme, sonlu kümelerde grup ölçütüne göre H 'nin grup olması demektir; o hâlde $H \subseteq G$ 'dir.
a.g.

⚠ Kapalılık sonsuz grupta yetmez

$\langle \mathbb{Z}, + \rangle$ grubunda $\mathbb{N} = \{1, 2, 3, \dots\}$ alt kümesi toplamaya göre kapalıdır; ama alt grup değildir — ne 0 içerir ne de herhangi bir elemanın tersini. Sonlu ölçütündeki sonluluk koşulu gerçekten vazgeçilmezdir.

Üçüncü ölçüt, iki koşulu tek koşulda birleştirir; soyut ispatlarda en sık bu kullanılır:

Teorem 7.3 (Tek Koşullu Alt Grup Ölçütü). $\langle G, \cdot \rangle$ bir grup ve $\emptyset \neq H \subseteq G$ olsun. H 'nin alt grup olması için gerek ve yeter koşul:

$$\forall a, b \in H \quad a \cdot b^{-1} \in H$$

İspat.

Gereklik. H alt grupsa $b \in H$ için $b^{-1} \in H$ ve kapalılıktan $ab^{-1} \in H$ olur.

Yeterlik. Hipotezden alt grup ölçütünün iki koşulunu türetilim.

Terslere kapalılık: Önce $a \in H$ için hipotezi $b = a$ ile kullanalım: $a \cdot a^{-1} = 1_G \in H$. Şimdi $1_G, a \in H$ için hipotez

$$1_G \cdot a^{-1} = a^{-1} \in H$$

verir.

Kapalılık: $a, b \in H$ olsun. Az önce gösterildiği gibi $b^{-1} \in H$ 'dir; hipotezi a ve b^{-1} çiftine uygularsak

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

İki koşul sağlandığından $H \subseteq G$ 'dir.
a.g.

Toplamsal yazıdaki karşılık: $\langle G, + \rangle$ grubunda $\emptyset \neq H \subseteq G$ alt kümesinin alt grup olması için gerek ve yeter koşul, her $a, b \in H$ için

$$a - b = a + (-b) \in H$$

olmasıdır.

7.3 Trivial Alt Gruplar

Teorem 7.4 (Her Grubun Hazır İki Alt Grubu). Her $\langle G, \cdot \rangle$ grubunda $\{1_G\}$ ve G 'nin kendisi birer alt gruptur.

İspat.

$\{1_G\}$ için iki koşullu ölçütü uygulayalım: $1_G \cdot 1_G = 1_G \in \{1_G\}$ ve $1_G^{-1} = 1_G \in \{1_G\}$; küme boş da değildir. G 'nin kendisi ise zaten grup olduğundan alt gruptur.

Tanım 7.2 (Trivial Alt Gruplar). G grubunun G ve $\{1_G\}$ alt gruplarına **trivial alt gruplar** denir.

İlginç olan, elbette trivial olmayan alt gruplardır. Bir sonraki bölümde ölçütlerimizi iş başında göreceğiz: kalan sınıfı halkalarından kompleks sayı çemberlerine uzanan bir örnek galerisi — **alt grup örnekleri**.

8. Alt Grup Örnekleri

Alt grup ölçütlerini elimize aldığımızı göre onları gerçek kümeler üzerinde çalıştırma zamanı. Bu bölümün örnekleri iki kaynaktan geliyor: modüler aritmetiğin $\mathbb{Z}_m$ yapıları ve kompleks sayılar. Aralara serpiştirilmiş soyut örnekler — kare koşuluyla tanımlanan kümeler, bir elemanla değişen elemanların kümesi — ölçütlerin somut hesap olmadan da nasıl işlediğini gösteriyor.

8.1 Hatırlatma: Kalan Sınıfları

Sayılar teorisinden birkaç gerçeği ispatsız kaydedelim; bu yapılar ders boyunca örnek deposu olarak kullanılacak.

$m \geq 2$ bir tam sayı olsun. $a \equiv b \pmod{m}$ bağıntısı ($m \mid a - b$) $\mathbb{Z}$ 'de bir denklik bağıntısıdır ve $\mathbb{Z}$ 'yi

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}, \quad \bar{k} = \{k + qm : q \in \mathbb{Z}\}$$

kalın sınıflarına ayırır. $\mathbb{Z}_m$ 'de toplama ve çarpma, temsilciler üzerinden tanımlanır:

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Bu işlemlerle ilgili kullanacağımız gerçekler şunlardır:

- $\langle \mathbb{Z}_m, + \rangle$ her $m \geq 2$ için komutatif bir gruptur; birimi $\bar{0}$, $\bar{a}$ 'nın tersi $-\bar{a} = \overline{m-a}$ 'dır.
- p asal ise $\bar{0}$ dışındaki sınıflar çarpmaya göre de bir komutatif grup oluşturur; bu grubu $\mathbb{Z}_p^* = \langle \mathbb{Z}_p - \{\bar{0}\}, \cdot \rangle$ ile göstereceğiz. (p asal değilse sıfır bölenler ortaya çıkar ve $\mathbb{Z}_m - \{\bar{0}\}$ çarpmaya göre kapalı bile değildir; örneğin $\mathbb{Z}_{10}$ 'da $\bar{2} \cdot \bar{5} = \bar{0}$.)

Örnek 8.1 (Alt Grup Olmayan Bir Alt Küme). $\langle \mathbb{Z}_{10}, + \rangle$ grubunun $M = \{\bar{0}, \bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ alt kümesi bir alt grup mudur?

Çözüm.

Toplamsal tek koşullu ölçütü deneyelim: $\bar{3}, \bar{1} \in M$ için

$$\bar{3} - \bar{1} = \bar{2} \notin M$$

Ölçüt bozulduğundan $M, \langle \mathbb{Z}_{10}, + \rangle$ 'nin alt grubu **değildir**.

■

8.2 Kompleks Sayılarda Bir Alt Grup

Örnek 8.2 (Bir Çarpma Grubu: $\$a + b \sqrt{5}i \setminus, i\$$). $G = \{a + b\sqrt{5}i : a, b \in \mathbb{R}, a \neq 0 \text{ veya } b \neq 0\}$ kümesinin, $\mathbb{C}$ 'deki çarpma işlemine göre bir grup olduğunu gösteriniz.

Çözüm.

$1 + \sqrt{5}i \in G$ olduğundan $G \neq \emptyset$ 'dir ve G 'nin her elemanı $0 + 0i$ 'den farklı olduğundan $\emptyset \neq G \subseteq \mathbb{C} - \{0\}$ 'dir. $\mathbb{C}^* = \langle \mathbb{C} - \{0\}, \cdot \rangle$ 'in grup olduğunu biliyoruz; G 'nin $\mathbb{C}^*$ 'in bir alt grubu olduğunu göstermek yeterlidir. İki koşullu ölçütü kullanalım.

Kapalılık. $i^2 = -1$ kullanılarak

$$(a + b\sqrt{5}i)(c + d\sqrt{5}i) = (ac - 5bd) + (ad + bc)\sqrt{5}i$$

bulunur; bileşenler gerçeldir, dolayısıyla çarpım yine $x + y\sqrt{5}i$ biçimindedir. Sıfır olamayacağını görmek için $\mathbb{C}$ 'nin sıfır bölensizliğine başvuralım: iki çarpan da 0 'dan farklı olduğundan çarpımları $0 + 0i$ olamaz; yani $ac - 5bd$ ile $ad + bc$ 'den en az biri sıfırdan farklıdır ve çarpım G 'dedir.

Terslere kapalılık. Payda gerçeştirilerek

$$(a + b\sqrt{5}i)^{-1} = \frac{1}{a + b\sqrt{5}i} = \frac{a - b\sqrt{5}i}{a^2 + 5b^2} = \frac{a}{a^2 + 5b^2} + \frac{-b}{a^2 + 5b^2}\sqrt{5}i$$

$a \neq 0$ veya $b \neq 0$ olduğundan $a^2 + 5b^2 \neq 0$ 'dır ve yeni bileşenlerden de en az biri sıfırdan farklıdır; ters, G 'nin bir elemanıdır.

İki koşul sağlandığından $G \subseteq \mathbb{C}^*$ 'dir; alt grup kendi başına grup olduğundan $\langle G, \cdot \rangle$ bir gruptur.

■

8.3 Sonlu Grupta Kapalılık Denetimi

Örnek 8.3 (\$\mathbb{Z}_{11}^*\$ İçinde Alt Küme Arayışı). 11 asal olduğundan $\mathbb{Z}_{11}^* = \langle \mathbb{Z}_{11} - \{0\}, \cdot \rangle$ bir gruptur. Aşağıdaki alt kümelerin $\mathbb{Z}_{11}^*$ 'deki çarpma işlemine göre birer grup olup olmadığını araştırınız:

$$M_1 = \{\bar{1}, \bar{8}\}, \quad M_2 = \{\bar{1}, \bar{10}\}, \quad M_3 = \{\bar{1}, \bar{3}, \bar{10}\}$$

$$M_4 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}\}, \quad M_5 = \{\bar{1}, \bar{3}, \bar{4}, \bar{5}, \bar{9}\}$$

Çözüm.

Hepsi, sonlu $\mathbb{Z}_{11}^*$ grubunun boş olmayan alt kümeleri; sonlu ölçüt gereği yalnızca çarpmaya göre kapalılığı denetlemek gerekli ve yeterlidir.

M_1 : $\bar{8} \cdot \bar{8} = \bar{64} = \bar{9} \notin M_1$. Kapalı değil; grup **değildir**.

M_2 : $\bar{10} \cdot \bar{10} = \bar{100} = \bar{1} \in M_2$ ve $\bar{1}$ ile çarpımlar zaten içeride. Kapalıdır; $M_2 \subseteq \mathbb{Z}_{11}^*$ ve dolayısıyla

gruptur.

M_3 : $\bar{3} \cdot \bar{3} = \bar{9} \notin M_3$. Kapalı değil; grup **değildir**.

M_4 : $\bar{3} \cdot \bar{5} = \bar{15} = \bar{4} \notin M_4$. Kapalı değil; grup **değildir**.

M_5 : Bütün çarpımları denetleyelim ($\bar{1}$ ile çarpımlar açık):

$$\bar{3} \cdot \bar{3} = \bar{9}, \quad \bar{3} \cdot \bar{4} = \bar{12} = \bar{1}, \quad \bar{3} \cdot \bar{5} = \bar{15} = \bar{4}, \quad \bar{3} \cdot \bar{9} = \bar{27} = \bar{5}$$

$$\bar{4} \cdot \bar{4} = \bar{16} = \bar{5}, \quad \bar{4} \cdot \bar{5} = \bar{20} = \bar{9}, \quad \bar{4} \cdot \bar{9} = \bar{36} = \bar{3}$$

$$\bar{5} \cdot \bar{5} = \bar{25} = \bar{3}, \quad \bar{5} \cdot \bar{9} = \bar{45} = \bar{1}, \quad \bar{9} \cdot \bar{9} = \bar{81} = \bar{4}$$

Bütün sonuçlar M_5 'te. Kapalıdır; M_5 bir alt gruptur ve **gruptur**. (Bu küme, $\mathbb{Z}_{11}^*$ 'daki tam kare kalanların kümesidir: $\bar{1} = \bar{1}^2, \bar{3} = \bar{5}^2, \bar{4} = \bar{2}^2, \bar{5} = \bar{4}^2, \bar{9} = \bar{3}^2$.)

■

8.4 Soyut Örnekler

Örnek 8.4 (Karesi Alt Grupta Olanlar). $\langle G, \cdot \rangle$ komutatif bir grup ve $H \subseteq G$ olsun.

a.g.

$$K = \{x \in G : x^2 \in H\}$$

kümesinin G 'nin bir alt grubu olduğunu gösteriniz.

Çözüm.

$1_G^2 = 1_G \in H$ olduğundan (H alt grup, 1_G 'yi içerir) $1_G \in K$ 'dir: $\emptyset \neq K \subseteq G$.

Kapalılık. $x_1, x_2 \in K$ olsun: $x_1^2, x_2^2 \in H$. G komutatif olduğundan

$$(x_1 x_2)^2 = x_1^2 x_2^2$$

ve H kapalı olduğundan $x_1^2 x_2^2 \in H$ 'dir; yani $(x_1 x_2)^2 \in H$, dolayısıyla $x_1 x_2 \in K$.

Terslere kapalılık. $x \in K$ olsun: $x^2 \in H$. H grup olduğundan $(x^2)^{-1} \in H$ ve kuvvet kurallarından $(x^2)^{-1} = (x^{-1})^2$ 'dir. O hâlde $(x^{-1})^2 \in H$, yani $x^{-1} \in K$.

İki koşul sağlandığından $K \subseteq G$ 'dir.

a.g.

■

Örnek 8.5 (Bir Elemanla Değişenler). $\langle G, \cdot \rangle$ bir grup (komutatif olması gerekmiyor) ve $a \in G$ olsun.

$$H = \{x \in G : x \cdot a = a \cdot x\}$$

kümesinin G 'nin bir alt grubu olduğunu gösteriniz.

Çözüm.

$1_G \cdot a = a \cdot 1_G$ olduğundan $1_G \in H$: küme boş değildir.

Kapalılık. $x_1, x_2 \in H$ olsun. Asosyatiflik ve hipotezler art arda kullanılarak

$$(x_1 x_2) a = x_1 (x_2 a) = x_1 (a x_2) = (x_1 a) x_2 = (a x_1) x_2 = a (x_1 x_2)$$

bulunur; $x_1 x_2 \in H$ 'dir.

Terslere kapalılık. $x \in H$, yani $xa = ax$ olsun. Eşitliğin iki yanına soldan ve sağdan x^{-1} uygulayalım:

$$x^{-1}(xa)x^{-1} = x^{-1}(ax)x^{-1} \implies ax^{-1} = x^{-1}a$$

Sol tarafta $x^{-1}(xa)x^{-1} = (x^{-1}x)(ax^{-1}) = ax^{-1}$, sağ tarafta $x^{-1}(ax)x^{-1} = (x^{-1}a)(xx^{-1}) = x^{-1}a$ sadeleşmeleri yapıldı. Demek ki $x^{-1} \in H$ 'dir.

İki koşul sağlandığından $H \subseteq G$ 'dir. (Bu alt gruba a 'nın **merkezleyicisi** denir.)
a.g.

■

8.5 Alıştırmalar

Alıştırma 8.1 (Karesi Birim Olanlar). $\langle G, \cdot \rangle$ komutatif bir grup olsun. $H = \{x \in G : x^2 = 1_G\}$ kümesinin G 'nin bir alt grubu olduğunu gösteriniz.

Çözüm.

$1_G^2 = 1_G$ olduğundan $1_G \in H$: küme boş değildir.

Kapalılık: $x, y \in H$ ise komutatiflikten $(xy)^2 = x^2 y^2 = 1_G \cdot 1_G = 1_G$, yani $xy \in H$.

Terslere kapalılık: $x \in H$ ise $x^2 = 1_G$ eşitliği $x \cdot x = 1_G$ demektir; yani $x^{-1} = x \in H$.

İki koşul sağlandığından $H \subseteq G$ 'dir. (Aslında $x^2 = 1_G$ koşulu $x^{-1} = x$ koşuluyla aynıdır: bu küme, kendi kendisinin tersi olan elemanların kümesidir.)
a.g.

■

Alıştırma 8.2 (Birim Çember Grubu). $G = \{a + bi \in \mathbb{C} : a, b \in \mathbb{R}, |a + bi| = 1\}$ kümesinin (birim çember) $\mathbb{C}$ 'deki çarpma işlemine göre bir grup olduğunu gösteriniz.

Çözüm.

$1 = 1 + 0i$ birim çember üzerindedir: $G \neq \emptyset$. Ayrıca $|z| = 1 \neq 0$ olduğundan $G \subseteq \mathbb{C} - \{0\}$ 'dir; $\mathbb{C}^*$ 'in alt grubu olduğunu gösterelim.

Kapalılık: Mutlak değer çarpımsaldır: $z, w \in G$ için

$$|zw| = |z| |w| = 1 \cdot 1 = 1 \implies zw \in G$$

Terslere kapalılık: $z \in G$ için $|z^{-1}| = \frac{1}{|z|} = 1$, yani $z^{-1} \in G$ 'dir.

İki koşul sağlandığından $G \subseteq \mathbb{C}^*$, dolayısıyla $\langle G, \cdot \rangle$ bir gruptur.
a.g.

■

Alıştırma 8.3 ($\{a + b\sqrt{2} : a, b \in \mathbb{Q}, a \neq 0 \text{ veya } b \neq 0\}$ Sayılarının Çarpma Grubu). $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q}, a \neq 0 \text{ veya } b \neq 0\}$ kümesinin $\mathbb{R}$ 'deki çarpma işlemine göre komutatif bir grup olduğunu gösteriniz.

Çözüm.

$1 = 1 + 0\sqrt{2} \in G$: küme boş değildir. Önce elemanların sıfırdan farklı olduğunu görelim: $a + b\sqrt{2} = 0$ ve $b \neq 0$ olsaydı $\sqrt{2} = -\frac{a}{b}$ rasyonel çıkardı; $b = 0$ ise $a = 0$ olurdu. Her iki durum da G 'nin tanımıyla çelişir; demek ki $\emptyset \neq G \subseteq \mathbb{R} - \{0\}$ ve $(\mathbb{R} - \{0\}, \cdot)$ grubunun alt grubu olduğunu göstermek yeterlidir.

Kapalılık:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

Bileşenler rasyoneldir; çarpım, sıfırdan farklı iki gerçel sayının çarpımı olduğundan sıfır değildir, dolayısıyla bileşenlerinden en az biri sıfırdan farklıdır ve sonuç G 'dedir.

Terslere kapalılık: Payda, eşlenikle rasyonelleştirilir:

$$(a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

Payda sıfır olamaz: $a^2 = 2b^2$ ve $b \neq 0$ olsaydı $\sqrt{2} = |a/b|$ rasyonel olurdu; $b = 0$ ise $a = 0$ gerekirdi. Bileşenler rasyoneldir ve en az biri sıfırdan farklıdır; ters G 'dedir.

Alt grup ölçütü sağlandığından $(G, \cdot)$ bir gruptur; komutatiflik $\mathbb{R}$ 'deki çarpımdan miras kalır.

■

Alt gruplar elimizdeyken sıra, soyut cebirin en somut gruplarına geliyor: bir kümenin kendi üzerine birebir eşlemelerinden kurulan permütasyon grupları. Grup kavramının tarihsel doğum yeri de orasıdır – [permütasyon grupları](#).

9. Transformasyonlar ve Simetrik Grup

Soyut grup kavramı tarihte önce permütasyonlarla ortaya çıktı: bir kümenin elemanlarını kendi aralarında yeniden dizen eşlemeler, bileşke işlemiyle doğal bir grup oluşturur. Bu bölümde önce keyfi bir kümenin transformasyonlar grubunu kuruyor, sonra sonlu kümelerle inerek n . dereceden simetrik grup S_n 'yi tanımlıyoruz. S_n , bu dersin en çok iş görecek örnek grubudur: komutatif olmayan ilk gruplarımız da buradan çıkacak.

9.1 Transformasyonlar Grubu

Tanım 9.1 (Transformasyon). $M \neq \emptyset$ bir küme olsun. M 'yi kendi üzerine birebir resmeden bir fonksiyona M 'nin bir **transformasyonu** denir.

Teorem 9.1 (Transformasyonlar Grubu). $M \neq \emptyset$ kümesinin bütün transformasyonlarından oluşan $\tilde{M}$ kümesi, fonksiyonların bileşke işlemine göre bir gruptur.

İspat.

$I_M : M \rightarrow M, m \mapsto m$ identik fonksiyonu M 'yi kendi üzerine birebir resmettiğinden $I_M \in \tilde{M}$: küme boş değildir.

Kapalılık. $f, g \in \tilde{M}$ ise fg (önce g , sonra f) yine birebir ve üzerinedir: birebirlik, $f(g(x)) = f(g(y))$ eşitliğinden önce f 'nin sonra g 'nin birebirliğiyle $x = y$ çıkmasından; üzerinelik, her $z \in M$ için önce $f(u) = z$ olan u 'nun, sonra $g(x) = u$ olan x 'in bulunmasından görülür.

Asosyatiflik. Her $m \in M$ için

$$((fg)h)(m) = (fg)(h(m)) = f(g(h(m))) = f((gh)(m)) = (f(gh))(m)$$

İki fonksiyon her noktada çakıştığından eşittir.

Birim eleman. Her m için $(I_M f)(m) = I_M(f(m)) = f(m)$ ve $(f I_M)(m) = f(m)$; birim eleman I_M 'dir.

Ters eleman. $f \in \tilde{M}$ birebir ve üzerine olduğundan ters fonksiyonu f^{-1} vardır ve f^{-1} de M 'yi kendi üzerine birebir resmeder: $f^{-1} \in \tilde{M}$. Her m için

$$(f^{-1}f)(m) = f^{-1}(f(m)) = m = I_M(m)$$

ve benzer biçimde $ff^{-1} = I_M$ 'dir.

O hâlde $\langle \tilde{M}, \cdot \rangle$ bir gruptur.

■

Tanım 9.2 (Transformasyonlar Grubu). Yukarıdaki $\tilde{M}$ grubuna M kümesinin **transformasyonlar grubu** denir.

9.2 Substitüsyonlar ve S_n

Tanım 9.3 (Substitüsyon (Permütasyon)). M sonlu bir küme ise transformasyon sözcüğü yerine **substitüsyon** veya **permütasyon** sözcüğü kullanılır. n elemanlı bir kümenin bir transformasyonuna **n . dereceden bir substitüsyon** denir.

Elemanları $1, 2, \dots, n$ ile numaralayalım. j 'yi i_j 'ye götüren S substitüsyonu iki satırlı biçimde yazılır:

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

Üst satırda argümanlar, alt satırda resimleri durur: $S(j) = i_j$.

Tanım 9.4 (Simetrik Grup). Bütün n . dereceden substitüsyonların (transformasyonlar grubu teoremine göre) bileşkeye göre oluşturdıkları gruba **n . dereceden simetrik grup** denir ve S_n ile gösterilir.

S_n ile hesap yaparken şu kurallar geçerlidir:

- **Birim:** $I = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$
- **Çarpım:** ST bileşkesi “önce T , sonra S ” demektir: $(ST)(m) = S(T(m))$.
- **Ters:** S 'nin satırları yer değiştirilir (ve istenirse sütunlar üst satıra göre yeniden sıralanır):

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

- **Mertebe:** $|S_n| = n!$ 'dir; çünkü alt satır, $1, \dots, n$ 'nin $n!$ permütasyonundan herhangi biri olabilir.
- Bir substitüsyon $n!$ ayrı biçimde yazılabilir: sütunların sırası önemsizdir, örneğin $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

Örnek 9.1 (İlk Üç Simetrik Grup). $|S_1| = 1! = 1$: $S_1 = \{I\}$.

$|S_2| = 2! = 2$: $S_2 = \left\{ I, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$.

$|S_3| = 3! = 6$:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

9.3 S_n Komutatif Değildir

$n > 2$ için S_n komutatif değildir. Bunu S_3 'te bir çiftle görelim:

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

ST için önce T , sonra S uygulanır: $1 \mapsto 2 \mapsto 3$, $2 \mapsto 3 \mapsto 2$, $3 \mapsto 1 \mapsto 1$; TS için önce S : $1 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 1$, $3 \mapsto 2 \mapsto 3$. Yani

$$ST = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = TS$$

$n \geq 3$ için aynı çift $(1, 2, 3)$ üzerinde çalışan, gerisini sabit bırakan iki substitüsyon) her S_n 'de komutatıflığı bozar.

Örnek 9.2 (\$S_7\$'de Hesap Pratiği). S_7 'de

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

veriliyor. $ST, TS, S^2, T^2, S^{-1}, T^{-1}$ substitüsyonlarını bulunuz.

Çözüm.

ST : Her m için önce T , sonra S : $1 \mapsto 3 \mapsto 1$, $2 \mapsto 2 \mapsto 3$, $3 \mapsto 1 \mapsto 7$, $4 \mapsto 7 \mapsto 5$, $5 \mapsto 5 \mapsto 2$, $6 \mapsto 4 \mapsto 6$, $7 \mapsto 6 \mapsto 4$:

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

TS : Önce S , sonra T : $1 \mapsto 7 \mapsto 6, 2 \mapsto 3 \mapsto 1, 3 \mapsto 1 \mapsto 3, 4 \mapsto 6 \mapsto 4, 5 \mapsto 2 \mapsto 2, 6 \mapsto 4 \mapsto 7, 7 \mapsto 5 \mapsto 5$:

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

($ST \neq TS$ olduğuna dikkat edin.)

S^2 : S 'yi iki kez uygula: $1 \mapsto 7 \mapsto 5, 2 \mapsto 3 \mapsto 1, 3 \mapsto 1 \mapsto 7, 4 \mapsto 6 \mapsto 4, 5 \mapsto 2 \mapsto 3, 6 \mapsto 4 \mapsto 6, 7 \mapsto 5 \mapsto 2$:

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

T^2 : $1 \mapsto 3 \mapsto 1, 2 \mapsto 2, 3 \mapsto 1 \mapsto 3, 4 \mapsto 7 \mapsto 6, 5 \mapsto 5, 6 \mapsto 4 \mapsto 7, 7 \mapsto 6 \mapsto 4$:

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

S^{-1} : Satırları yer değiştirip sütunları sırala: S 'de $7 \mapsto 5$ olduğundan S^{-1} 'de $5 \mapsto 7$ olur, vb.:

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

T^{-1} :

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

■

İki satırlı gösterim hesap için işlevsel ama hantal: yedi sütunun dördü yerinde saymış olabilir. Bir sonraki bölümde substitüsyonların gerçek anatomisini açığa çıkaran çok daha ekonomik bir dil kuracağız: [devreler](#).

10. Devreler

İki satırlı gösterim, bir substitüsyonun ne yaptığını satır satır söyler ama *nasıl bir hareket* olduğunu göstermez. Bu bölümün ana fikri, her substitüsyonun elemanları halkalar hâlinde döndürdüğüdür: $2 \rightarrow 4 \rightarrow 6 \rightarrow 2$ gibi kapalı yörüngeler. Bu yörüngelere devre diyeceğiz ve her substitüsyonun ortak elemanı olmayan devrelerin çarpımı olarak *tek türlü* yazılabildiğini göreceğiz. Devre dili, çarpım, kuvvet ve ters hesaplarını birkaç satırlık işe indirger.

10.1 Devre Kavramı

Tanım 10.1 (Devre). $S \in S_n$ ve a , S 'nin yerinden oynattığı bir eleman olsun. S ; a 'yı $S(a)$ 'ya, $S(a)$ 'yı $S^2(a)$ 'ya, ... götürür. Uygun bir $k \in \mathbb{N}$ için

$$S^k(a) = a$$

oluyorsa (böyle en küçük k 'yı alalım) ve S ; $a, S(a), S^2(a), \dots, S^{k-1}(a)$ dışındaki elemanların hepsini sabit bırakıyorsa, S 'ye **k uzunluğunda bir devre** denir ve

$$S = (a, S(a), S^2(a), \dots, S^{k-1}(a))$$

ile gösterilir: parantezdeki her eleman bir sağındakine, sonuncusu da baştakine gider.

Gösterimle ilgili iki not:

- Devre, elemanlarının dairesel kaydırılmasıyla değişmez: $(2\ 4\ 6\ 7\ 3) = (4\ 6\ 7\ 3\ 2) = (6\ 7\ 3\ 2\ 4) = \dots$ Hangi elemandan başladığımız önemsizdir; önemli olan dönüş sırasıdır.
- Uzunluğu 1 olan “devreler” — yani $S(a) = a$ diyen (a) parantezleri — devre sayılmaz; sabit elemanlar yazılmaz.

Örnek 10.1 (Devre Tanıma). $S = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 2 & 6 & 5 & 7 & 3 & 8 \end{pmatrix} \in S_8$ substitüsyonuna bakalım. 1, 5, 8 sabittir; öbür elemanlar tek bir yörünge çizer:

$$2 \mapsto 4 \mapsto 6 \mapsto 7 \mapsto 3 \mapsto 2$$

O hâlde S , 5 uzunluğunda bir devredir:

$$S = (2\ 4\ 6\ 7\ 3) = (4\ 6\ 7\ 3\ 2) = (6\ 7\ 3\ 2\ 4) = (7\ 3\ 2\ 4\ 6) = (3\ 2\ 4\ 6\ 7)$$

10.2 Yabancı Devrelere Ayrılış

Tanım 10.2 (Yabancı Devreler). Hiçbir ortak elemanı bulunmayan devrelere **yabancı devreler** denir. Örneğin $(1\ 2\ 3)$ ile $(4\ 7\ 6\ 5)$ yabancıdır.

Teorem 10.1 (Yabancı Devrelere Ayrılış). Her substitüsyon, bir takım yabancı devrelerin çarpımı olarak gösterilebilir; devrelerin sırasından vazgeçildiği takdirde bu gösteriliş tek türlü belirlidir.

İspatın fikri, uygulamadaki tarifi kendisidir: yerinden oynayan bir elemandan başlayıp yörüngesi kapana dek izleyin — bu bir devredir; sonra henüz kullanılmamış bir elemandan yeni bir yörünge başlatın. Yörüngeler ya çakışır ya hiç kesişmez; bu da tekliği verir.

Örnek 10.2 (Ayrılış Örnekleri).

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 7 & 2 & 5 & 1 & 8 \end{pmatrix} = (1347)(265)$$

çünkü $1 \mapsto 3 \mapsto 4 \mapsto 7 \mapsto 1$ ve $2 \mapsto 6 \mapsto 5 \mapsto 2$; 8 sabittir. Benzer biçimde

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 8 & 3 & 6 & 1 & 7 \end{pmatrix} = (1487)(253)$$

İdentik substitüsyon hiçbir elemanı oynatmadığından ayrılığı boş çarpımdır; S_n 'de $I = (1)(2)\dots(n)$ diye yazılır.

10.3 Devrelerle Hesap Kuralları

Yabancı ayrılışın gücü, dört pratik kuraldan gelir:

1. **Yabancı devreler komutatiftir:** $D_1 D_2 = D_2 D_1$ — her biri diğerinin elemanlarını sabit bıraktığından sıra fark etmez. (Yabancı *olmayan* devrelerin çarpımı genel olarak komutatif değildir.)
2. **Kuvvet, devre içinde öteleme demektir:** yabancı devrelere ayrılmış S 'nin k . kuvvetini almak için her devrenin içinde her elemanı k adım ileri götürmek yeterlidir; devreler birbirine karışmaz:

$$S = D_1 D_2 \dots D_r \implies S^k = D_1^k D_2^k \dots D_r^k$$

3. **m uzunluğundaki devrenin m . kuvveti birimdir:** $(a_1 a_2 \dots a_m)^m = I$; her eleman tam tur atar.

4. **Ters, devreyi tersten okumaktır:**

$$(a_1 a_2 a_3 \dots a_k)^{-1} = (a_1 a_k a_{k-1} \dots a_2)$$

ve yabancı devrelerin komutatıflığı sayesinde $S = D_1 \dots D_r$ için $S^{-1} = D_1^{-1} \dots D_r^{-1}$ 'dir.

Örnek 10.3 (Bir Devrenin Bütün Kuvvetleri). $(123456) \in S_6$ devresinin kuvvetlerini hesaplayalım; k . kuvvet, her elemanı devre içinde k adım öteler:

$$(123456)^2 = (135)(246), \quad (123456)^3 = (14)(25)(36)$$

$$(123456)^4 = (153)(264), \quad (123456)^5 = (165432), \quad (123456)^6 = I$$

Uzunluk 6 çift olduğundan ara kuvvetlerde devre küçük parçalara kırılıyor; 5. kuvvet ise tersten okunmuş devredir: $(123456)^5 = (123456)^{-1}$.

Örnek 10.4 (\$S_8\$'de Devrelerle Hesap). S_8 'de

$$S = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 7 & 1 & 6 & 2 & 8 & 5 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 7 & 6 & 1 & 3 & 4 & 2 \end{pmatrix}$$

substitüsyonlarının, ayrıca S^{-1} , T^{-1} , ST ve TS 'nin yabancı devrelere ayrılışlarını bulunuz; S^2 ile T^3 'ü hesaplayınız.

Çözüm.

S : $1 \mapsto 3 \mapsto 7 \mapsto 8 \mapsto 5 \mapsto 6 \mapsto 2 \mapsto 4 \mapsto 1$ — tek büyük yörünge:

$$S = (13785624)$$

T : $1 \mapsto 8 \mapsto 2 \mapsto 5 \mapsto 1$ ve $3 \mapsto 7 \mapsto 4 \mapsto 6 \mapsto 3$:

$$T = (1825)(3746)$$

Tersler: Devreler tersten okunur:

$$S^{-1} = (14265873), \quad T^{-1} = (1528)(3647)$$

ST (önce T , sonra S): $1 \mapsto 8 \mapsto 5, 5 \mapsto 1 \mapsto 3, 3 \mapsto 7 \mapsto 8, 8 \mapsto 2 \mapsto 4, 4 \mapsto 6 \mapsto 2, 2 \mapsto 5 \mapsto 6, 6 \mapsto 3 \mapsto 7, 7 \mapsto 4 \mapsto 1$:

$$ST = (1\ 5\ 3\ 8\ 4\ 2\ 6\ 7)$$

TS (önce S , sonra T): $1 \mapsto 3 \mapsto 7, 7 \mapsto 8 \mapsto 2, 2 \mapsto 4 \mapsto 6, 6 \mapsto 2 \mapsto 5, 5 \mapsto 6 \mapsto 3, 3 \mapsto 7 \mapsto 4, 4 \mapsto 1 \mapsto 8, 8 \mapsto 5 \mapsto 1$:

$$TS = (1\ 7\ 2\ 6\ 5\ 3\ 4\ 8)$$

S^2 : 8'li devrede herkes iki adım ilerler; sıra 1, 3, 7, 8, 5, 6, 2, 4 olduğundan

$$S^2 = (1\ 7\ 5\ 2)(3\ 8\ 6\ 4)$$

T^3 : 4 uzunluğundaki devrenin küpü, tersidir ($D^3 = D^{-1}$, çünkü $D^4 = I$):

$$T^3 = (1\ 8\ 2\ 5)^3(3\ 7\ 4\ 6)^3 = (1\ 5\ 2\ 8)(3\ 6\ 4\ 7)$$

■

Örnek 10.5 (\$S_6\$'da Devrelerle Hesap). S_6 'da

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

için $S, T, ST, TS, S^2, T^2, S^{-1}, T^{-1}, (ST)^{-1}, (TS)^{-1}$ 'in yabancı devrelere ayrılışlarını bulunuz.

Çözüm.

$S = (2\ 6)(3\ 5)$ (1 ve 4 sabit); $T = (1\ 5\ 4\ 2\ 3\ 6)$.

ST (önce T): $1 \mapsto 5 \mapsto 3, 3 \mapsto 6 \mapsto 2, 2 \mapsto 3 \mapsto 5, 5 \mapsto 4 \mapsto 4, 4 \mapsto 2 \mapsto 6, 6 \mapsto 1 \mapsto 1$:

$$ST = (1\ 3\ 2\ 5\ 4\ 6)$$

TS (önce S): $1 \mapsto 1 \mapsto 5, 5 \mapsto 3 \mapsto 6, 6 \mapsto 2 \mapsto 3, 3 \mapsto 5 \mapsto 4, 4 \mapsto 4 \mapsto 2, 2 \mapsto 6 \mapsto 1$:

$$TS = (1\ 5\ 6\ 3\ 4\ 2)$$

Kuvvetler: Transpozisyonların karesi birimdir:

$$S^2 = (2\ 6)^2(3\ 5)^2 = I$$

T^2 'de altılı devrenin herkesi iki adım ilerler; sıra 1, 5, 4, 2, 3, 6:

$$T^2 = (1\ 4\ 3)(5\ 2\ 6) = (1\ 4\ 3)(2\ 6\ 5)$$

Tersler: $S^{-1} = (2\ 6)(3\ 5) = S$; öbürleri devrenin tersten okunuşudur:

$$T^{-1} = (1\ 6\ 3\ 2\ 4\ 5), \quad (ST)^{-1} = (1\ 6\ 4\ 5\ 2\ 3), \quad (TS)^{-1} = (1\ 2\ 4\ 3\ 6\ 5)$$

■

Devre dili elimizde: artık her substitüsyon, yapısını açık eden standart bir biçimde yazılabiliyor. Sıradaki adım, devreleri de en küçük parçalarına — iki elemanlı takaslara — kırmak. Bu kırılım, substitüsyonların “tek” ve “çift” diye ikiye ayrılmasını ve S_n 'nin en ünlü alt grubunu getirecek: [transpozisyonlar ve alterne grup](#).

11. Transpozisyonlar ve Alterne Grup

Devreler substitüsyonun anatomisini verdi; şimdi devreleri de en küçük yapı taşına indiriyoruz: yalnızca iki elemanı takas eden **transpozisyonlar**. Her substitüsyon transpozisyonların çarpımıdır — ama bu ayrış tek türlü değildir. Bölümün derin sonucu, yine de değişmeyen bir şeyin olduğudur: kullanılan transpozisyon sayısının *tek mi çift mi* olduğu. Bu görünmez imza, S_n 'yi tam ortadan ikiye böler ve yarısından A_n alterne grubunu çıkarır.

11.1 Transpozisyonlara Ayrış

Tanım 11.1 (Transpozisyon). Uzunluğu 2 olan $(i j)$ devresine bir **transpozisyon** denir: i ile j yer değiştirir, geri kalan her şey sabit kalır.

Teorem 11.1 (Transpozisyonlara Ayrış). Her substitüsyon, bir takım transpozisyonların çarpımı olarak gösterilebilir.

İspat.

Her substitüsyon yabancı devrelerin çarpımı olduğundan, her devrenin transpozisyonlara ayrılabilirdiğini göstermek yeterlidir. Doğrudan doğrulanabilen özdeşlik şudur:

$$(a_1 a_2 a_3 \dots a_{k-1} a_k) = (a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_3)(a_1 a_2)$$

Sağ tarafta önce en sağdaki çarpan uygulanır: $a_1 \mapsto a_2$ ve sonraki transpozisyonlar a_2 'ye dokunmaz; $a_2 \mapsto a_1 \mapsto a_3$ ve sonrakiler a_3 'e dokunmaz; böyle sürer ve $a_k \mapsto a_1$ ile devre kapanır. k uzunluğundaki devre böylece $k - 1$ transpozisyonun çarpımıdır.

■

Bu gösteriliş tek türlü **değildir**: $(i j)^2 = I$ olduğundan çarpımın herhangi bir yerine bir transpozisyonun karesi sokulabilir. Örneğin S_7 'de

$$S = (1\ 4\ 3)(2\ 6\ 5\ 7) = (1\ 3)(1\ 4)(2\ 7)(2\ 5)(2\ 6) = (1\ 3)(1\ 4)(2\ 3)(2\ 3)(2\ 7)(2\ 5)(2\ 6)$$

Beş transpozisyonluk yazılış yedi transpozisyonluğa uzatıldı — ama dikkat: 5 de 7 de *tek* sayı. Bu bir rastlantı değildir.

11.2 Tek ve Çift Substitüsyonlar

Teorem 11.2 (Tekliğin-Çiftliğin Değişmezliği). Bir substitüsyon ne şekilde transpozisyonların çarpımı olarak gösterilirse gösterilsin, çarpımdaki transpozisyonların sayısı ya daima tektir ya daima çifttir.

Tanım 11.2 (Tek ve Çift Substitüsyon). Çift (tek) sayıda transpozisyonun çarpımı olarak gösterilebilen substitüsyona **çift (tek) substitüsyon** denir.

Tanımın hemen görülen sonuçları:

- $I = (1\ 2)(1\ 2)$ olduğundan identik substitüsyon çifttir.
- k uzunluğundaki devre $k - 1$ transpozisyonun çarpımı olduğundan, **uzunluğu çift olan devre tek, uzunluğu tek olan devre çift substitüsyondur.**
- Çarpımda sayılar toplanır: iki çift ya da iki tek substitüsyonun çarpımı çift; bir tekle bir çiftin çarpımı tektir.

Örnek 11.1 (Teklik-Çiftlik Belirleme). S_7 'de aşağıdaki substitüsyonları yabancı devrelere ayırıp tek mi çift mi olduklarını belirleyiniz:

$$S = (1\ 2\ 3\ 4)(5\ 6\ 7)(2\ 6\ 1)(4\ 7), \quad T = (1\ 2\ 3\ 4\ 5)(6\ 7)(1\ 3\ 5\ 7)(1\ 6)$$

$$U = (1\ 4)(1\ 2\ 3)(4\ 5)(1\ 4)$$

Çözüm.

S: Çarpımı sağdan sola izleyerek (önce en sağdaki çarpan) her elemanın yörüngesini çıkaralım: $1 \mapsto 3, 3 \mapsto 4, 4 \mapsto 5, 5 \mapsto 6, 6 \mapsto 2, 2 \mapsto 7, 7 \mapsto 1$. Yani

$$S = (1\ 3\ 4\ 5\ 6\ 2\ 7)$$

Uzunluğu 7 (tek sayı) olan devre **çift** substitüsyondur (6 transpozisyon).

T: Aynı yöntemle $1 \mapsto 7, 7 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$ ve $4 \mapsto 5, 5 \mapsto 6, 6 \mapsto 4$:

$$T = (1\ 7\ 2\ 3)(4\ 5\ 6)$$

Dörtlü devre tek (3 transpozisyon), üçlü devre çifttir (2 transpozisyon); çarpım **tek** substitüsyondur.

U: Çarpanları yine sağdan sola uygulayalım. 1: en sağdaki $(1\ 4)$ ile $1 \mapsto 4$, sonra $(4\ 5)$ ile $4 \mapsto 5$, kalan çarpanlar 5'e dokunmaz — $1 \mapsto 5$. 5: $(4\ 5)$ ile $5 \mapsto 4$, en soldaki $(1\ 4)$ ile $4 \mapsto 1 - 5 \mapsto 1$. 2: yalnız $(1\ 2\ 3)$ dokunur — $2 \mapsto 3$. 3: $(1\ 2\ 3)$ ile $3 \mapsto 1$, sonra $(1\ 4)$ ile $1 \mapsto 4 - 3 \mapsto 4$. 4: en sağdaki $(1\ 4)$ ile $4 \mapsto 1$, $(1\ 2\ 3)$ ile $1 \mapsto 2 - 4 \mapsto 2$. Yani

$$U = (1\ 5)(2\ 3\ 4)$$

Transpozisyon tek, üçlü devre çift; çarpım **tek** substitüsyondur.

Aynı sonuçlara yabancı ayrılış yapmadan da ulaşılabilirdi: verilen çarpanların her birinin tekliği-çiftliği bellidir. S için tek-çift-çift-tek = çift; T için çift-tek-tek-tek = tek; U için tek-çift-tek-tek = tek.

■

11.3 Alterne Grup

Teorem 11.3 (Çift Substitüsyonlar Alt Grup Oluşturur). S_n 'nin bütün çift substitüsyonlarından oluşan A_n kümesi, S_n 'nin bir alt grubudur.

İspat.

I çift olduğundan $A_n \neq \emptyset$ 'dir. İki çift substitüsyonun çarpımı çift olduğundan A_n çarpmaya göre kapalıdır. S_n sonlu bir grup olduğundan, sonlu grupta alt grup ölçütü gereği kapalılık yeterlidir: $A_n \subseteq S_n$.

■

Tanım 11.3 (Alterne Grup). S_n 'nin çift substitüsyonlardan oluşan A_n alt grubuna n . **dereceden alterne grup** denir.

Teorem 11.4 (Tek ve Çift Substitüsyonlar Eşit Sayıdadır). $n > 1$ için S_n 'deki tek ve çift substitüsyonlar aynı sayıdadır; dolayısıyla

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

İspat.

$S = (1\ 2)$ sabit bir transpozisyon (tek substitüsyon) olsun ve

$$f : A_n \rightarrow S_n - A_n, \quad f(T) = ST$$

fonksiyonunu tanımlayalım. T çiftken ST tektir; yani f gerçekten $S_n - A_n$ 'ye gider ve iyi tanımlıdır.

f birebirdir: $ST_1 = ST_2$ ise grupta sadeleştirmeyle $T_1 = T_2$.

f üzerinedir: U tek bir substitüsyon olsun. $T = SU$ çift substitüsyondur (tek · tek) ve $S^2 = I$ olduğundan

$$f(T) = S(SU) = S^2U = U$$

Sonlu A_n kümesini $S_n - A_n$ üzerine birebir resmeden fonksiyon bulduğumuzdan iki küme aynı sayıda elemana sahiptir; toplamı $n!$ olduğundan her biri $\frac{n!}{2}$ elemanlıdır.

■

Örnek 11.2 (Küçük Alterne Gruplar). $A_2 = \{I\}$.

$S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ içinde üçlü devreler çift, transpozisyonlar tektir:

$$A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}, \quad |A_3| = \frac{3!}{2} = 3$$

S_4 'ün 24 elemanından çift olanlar: identik, sekiz üçlü devre ve üç ikili-ikili çarpım:

$$A_4 = \{I, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), \\ (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

$|A_4| = \frac{4!}{2} = 12$ 'dir. (Transpozisyonlar ve dörtlü devreler tektir; $S_4 - A_4$ 'ü onlar oluşturur.)

İ Klein'in dörtlü grubu

A_4 'ün içindeki

$$V = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

alt kümesi çarpmaya göre kapalıdır (iki farklı çift-transpozisyonun çarpımı üçüncüsünü verir) ve dolayısıyla A_4 'ün bir alt grubudur. Birimden farklı her elemanın karesi birimdir; yani V , dördüncü mertebeden iki grup tipinden birincisinin – **Klein tipi** grubun – somut bir örneğidir ve **Klein'in dörtlü grubu** diye anılır. V komutatiftir.

Simetrik ve alterne gruplar, sonlu grup teorisinin ana laboratuvarıdır; ilerleyen bölümlerin örneklerinde sürekli onlara döneceğiz. Şimdi yönümüzü yeniden genel teoriye çeviriyoruz: bir grubun bir elemanının ürettiği en küçük alt grup nedir ve tek elemanla üretilen gruplar nasıl sınıflandırılır? – **doğurulan alt gruplar**.

12. Doğurulan Alt Gruplar

Bir grubun içinde belli elemanları — diyelim tek bir a elemanını — kapsayan *en küçük* alt grup hangisidir? Bu sorunun temiz yanıtı iki adımda kurulur: önce alt grupların kesişiminin yine alt grup olduğu gösterilir, sonra “verilen kümeyi kapsayan bütün alt grupların kesişimi” alınır. Bu bölümde bu inşayı yapıyor ve doğurulan alt grubun somut betimlemesini kanıtlıyoruz: o, doğurayların bütün kuvvet çarpımlarının kümesidir.

12.1 Alt Grupların Kesişimi

Teorem 12.1 (Alt Grupların Kesişimi Alt Gruptur). *Bir G grubunun sonlu ya da sonsuz sayıda alt grubunun kesişimi de G ’nin bir alt grubudur.*

İspat.

I bir indis kümesi ve her $i \in I$ için $H_i \subseteq G$ olsun. Her alt grup 1_G ’yi içerdiğinden

$$1_G \in \bigcap_{i \in I} H_i$$

ve kesişim boş değildir. Şimdi $a, b \in \bigcap_{i \in I} H_i$ alalım: her i için $a, b \in H_i$ ’dir ve H_i alt grup olduğundan tek koşullu ölçüt gereği $ab^{-1} \in H_i$ olur. Bu her i için doğru olduğundan

$$ab^{-1} \in \bigcap_{i \in I} H_i$$

Tek koşullu alt grup ölçütüne göre kesişim G ’nin bir alt grubudur.

■

12.2 Doğurulan Alt Grup

Tanım 12.1 (Doğurulan Alt Grup ve Doğuraylar). G bir grup ve $\emptyset \neq M \subseteq G$ olsun. G ’nin M ’yi kapsayan bütün alt gruplarının kesişimine G ’nin M tarafından doğurulan alt grubu denir:

$$G(M) = \bigcap_{\substack{M \subseteq H \subseteq G \\ \text{a.g.}}} H$$

M ’nin elemanlarına $G(M)$ ’nin **doğurayları** denir. $M = \{a\}$ tek elemanlıysa $G(\{a\})$ yerine kısaca $G(a)$ yazılır.

$G(M) = G$ oluyorsa “ G grubu M tarafından doğurulmuştur” denir; M ayrıca sonluysa G ’ye **sonlu doğuraylı grup** denir.

Tanım gereği $G(M)$; M ’yi kapsayan alt grupların *en küçüğüdür*: hem kendisi böyle bir alt gruptur (kesişim teoremi) hem de M ’yi kapsayan her alt grup, kesişimin bir çarpanı olduğundan $G(M)$ ’yi kapsar. Kesişim tanımı zarif ama hesaba elverişsiz; elemanları tek tek betimleyen ikinci bir tanıma ihtiyacımız var.

Tanım 12.2 (Kuvvet Çarpımı). G grubunun $a_1, a_2, \dots, a_k$ gibi sonlu sayıda elemanı ile kurulan

$$a_1^{m_1} a_2^{m_2} \dots a_k^{m_k} \quad (m_i \in \mathbb{Z})$$

biçimindeki çarpıma, bu elemanların bir **kuvvet çarpımı** denir. (Elemanlar tekrarlanabilir; kuvvetler negatif ya da sıfır olabilir.)

Teorem 12.2 (Doğurulan Alt Grubun Betimlenmesi). $G(M)$; M 'nin elemanlarının bütün kuvvet çarpımlarından oluşan küme ile çakışır.

İspat.

M 'nin elemanlarının bütün kuvvet çarpımlarının kümesine K diyelim; $G(M) = K$ olduğunu iki kapsama ile göstereyim.

$K \subseteq G(M)$: $a_1^{m_1} \dots a_k^{m_k} \in K$ olsun ($a_i \in M$). $M \subseteq G(M)$ ve $G(M)$ bir gruptur; grup, elemanlarının terslerini ve çarpımlarını içerdiğinden her $a_i^{m_i}$ 'yi, dolayısıyla bunların çarpımını da içerir:

$$a_1^{m_1} \dots a_k^{m_k} \in G(M)$$

$G(M) \subseteq K$: Önce $M \subseteq K$ 'dir: her $a \in M$ için $a = a^1$ bir kuvvet çarpımıdır. Şimdi K 'nin bir alt grup olduğunu görelim: $K \neq \emptyset$ ve $K \subseteq G$ 'dir; iki kuvvet çarpımı için

$$(a_1^{m_1} \dots a_k^{m_k}) (b_1^{n_1} \dots b_l^{n_l})^{-1} = a_1^{m_1} \dots a_k^{m_k} b_l^{-n_l} \dots b_2^{-n_2} b_1^{-n_1}$$

sağ taraf yine M 'nin elemanlarının bir kuvvet çarpımıdır, yani K 'dedir. Tek koşullu ölçüt gereği $K \subseteq_{\text{a.g.}} G$ 'dir. M 'yi kapsayan bir alt grup bulduk; $G(M)$, böyle alt grupların kesişimi olduğundan

$$G(M) \subseteq K$$

İki kapsama birlikte $G(M) = K$ verir.

■

12.3 İlk Örnekler

Örnek 12.1 ($\mathbb{Z}_{13}^*$ 'da Doğurulan Alt Gruplar). 13 asal olduğundan $\mathbb{Z}_{13}^* = \langle \mathbb{Z}_{13} - \{0\}, \cdot \rangle$ bir gruptur; elemanlarını $\{\mp 1, \mp 2, \dots, \mp 6\}$ biçiminde yazmak hesabı kısaltır ($\overline{12} = -1$ gibi).

- $\overline{4}$ tarafından doğurulan alt grubu bulunuz.
- $\overline{2}$ tarafından doğurulan alt grubu bulunuz.

Çözüm.

Tek elemanla doğurulan alt grup, o elemanın bütün kuvvetlerinin kümesidir.

a) Kuvvetleri sırayla hesaplayalım:

$$\overline{4}^0 = \overline{1}, \quad \overline{4}^1 = \overline{4}, \quad \overline{4}^2 = \overline{16} = \overline{3}, \quad \overline{4}^3 = \overline{4} \cdot \overline{3} = \overline{12} = -\overline{1}$$

$-\overline{1}$ 'e ulaştık; sonraki üç kuvvet öncekilerin işaretlisidir:

$$\overline{4}^4 = -\overline{4}, \quad \overline{4}^5 = -\overline{3}, \quad \overline{4}^6 = \overline{1}$$

Kuvvetler bundan sonra dönmeye başlar (negatif kuvvetler de aynı kümede kalır: $\overline{4}^{-1} = \overline{4}^5$). O hâlde

$$\mathbb{Z}_{13}^*(\overline{4}) = \{\mp 1, \mp 3, \mp 4\}$$

altı elemanlı bir alt gruptur.

b) Aynı hesap:

$$\overline{2}^1 = \overline{2}, \quad \overline{2}^2 = \overline{4}, \quad \overline{2}^3 = \overline{8} = -\overline{5}, \quad \overline{2}^4 = \overline{16} = \overline{3}, \quad \overline{2}^5 = \overline{6}, \quad \overline{2}^6 = \overline{12} = -\overline{1}$$

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

On iki kuvvet, grubun on iki elemanının tamamını verdi:

$$\mathbb{Z}_{13}^*(\overline{2}) = \mathbb{Z}_{13}^*$$

Yani $\mathbb{Z}_{13}^*$ grubu $\overline{2}$ tarafından doğurulmuştur.

■

Örnek 12.2 (\$S_3\$'te Bir Transpozisyonun Doğurdukları). S_3 'te $(1\ 2)$ tarafından doğurulan alt grup:

$$(1\ 2)^0 = I, \quad (1\ 2)^1 = (1\ 2), \quad (1\ 2)^2 = I$$

Kuvvetler iki değer arasında salınır:

$$S_3 \langle (1\ 2) \rangle = \{I, (1\ 2)\}$$

Aynı grupta bir eleman bütün grubu doğurabiliyor ($\bar{2}$), bir başkası küçük bir alt grupta takılıp kalabiliyor (4 ya da $(1\ 2)$). Tek elemanla doğurulan bu gruplar o kadar temel ki kendilerine ayrılmış bir ada ve ayrıntılı bir teoriye sahipler: [devresel gruplar](#).

13. Devresel Gruplar

Tek bir eleman tarafından doğurulan gruplar, grup dünyasının en yalın üyeleridir: bütün grup, a 'nın kuvvetlerinden ibarettir. Bu bölümde devresel grupları tanımlıyor, her devresel grubun komutatif olduğunu görüyor ve temel ikiliği kuruyoruz: kuvvetlerin hepsi birbirinden farklıysa grup sonsuzdur; iki kuvvet çakışıyorsa grup sonludur ve çok düzenli bir biçimi vardır – $\{1_G, a, a^2, \dots, a^{\tau-1}\}$.

13.1 Tanım ve İlk Özellik

Tanım 13.1 (Devresel Grup). Bir tek elemanı tarafından doğurulan gruba **devresel grup** denir. G devresel grubu $a \in G$ tarafından doğuruluyorsa

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, 1_G, a, a^2, \dots\}$$

yazılır; a 'ya G 'nin bir **doğurayı** denir.

(Kuvvet çarpımı betimlemesi tek doğurayda kuvvet kümesine indirgenir: $a^{m_1}a^{m_2}\dots a^{m_k} = a^{m_1+\dots+m_k}$.)

Teorem 13.1 (Devresel Gruplar Komutatifdir). Her devresel grup komutatifdir.

İspat.

$G = \langle a \rangle$ olsun. G 'nin herhangi iki elemanı a^m ve a^n biçimindedir; kuvvet kuralları ve $\mathbb{Z}$ 'de toplanmanın komutatifliğiyle

$$a^m \cdot a^n = a^{m+n} = a^{n+m} = a^n \cdot a^m$$

■

Bu basit teorem sık sık *ters yönde* iş görür: komutatif olmayan bir grup (S_3 gibi) devresel olamaz.

13.2 Sonsuz ve Sonlu Devresel Gruplar

$\langle a \rangle$ devresel grubunda iki durum söz konusudur.

Birinci durum: $m \neq n$ olan her $m, n \in \mathbb{Z}$ çifti için $a^m \neq a^n$ 'dir. Kuvvetlerin hepsi birbirinden farklı olduğundan grup sonsuzdur; $\langle a \rangle$ 'ya **sonsuz devresel grup** denir. Örnek: $\langle \mathbb{Z}, + \rangle = \langle 1 \rangle$ (toplamsal yazışta kuvvetlerin yerini katlar alır: $n \cdot 1 = n$).

İkinci durum: $a^m = a^n$ olacak biçimde $m > n$ tam sayıları vardır. O zaman

$$a^m \cdot a^{-n} = a^n \cdot a^{-n} \implies a^{m-n} = 1_G, \quad m - n \in \mathbb{N}$$

Yani $a^t = 1_G$ koşulunu sağlayan en az bir doğal sayı t vardır. Bu doğal sayıların en küçüğüne τ diyelim. Aşağıdaki teorem, grubun tamamını τ ile betimler.

Teorem 13.2 (Sonlu Devresel Grubun Yapısı). $\langle a \rangle$ devresel grubunda $a^t = 1_G$ koşulunu sağlayan doğal sayılar bulunsun ve bunların en küçüğü τ olsun. Bu takdirde

$$\langle a \rangle = \{1_G, a, a^2, \dots, a^{\tau-1}\}$$

ve sağdaki τ eleman birbirinden farklıdır; yani $\langle a \rangle$ sonludur ve mertebesi τ 'dur.

İspat.

Her kuvvet listeye düşer. $a^n \in \langle a \rangle$ olsun ($n \in \mathbb{Z}$ herhangi bir tam sayı). n 'yi τ 'ya bölelim: bölme algoritmasına göre

$$n = \tau q + r, \quad 0 \leq r < \tau$$

olacak biçimde q, r tam sayıları tek türlü belirlidir. O hâlde

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

yani $a^n \in \{1_G, a, \dots, a^{\tau-1}\}$ 'dir. Ters kapsama açıktır.

Listedekiler birbirinden farklıdır. $0 \leq r < s < \tau$ için $a^r = a^s$ olsaydı

$$a^{s-r} = 1_G, \quad 0 < s - r < \tau$$

olurdu; bu, τ 'nın en küçük seçilmesiyle çelişir.

İki gözlem birlikte $|\langle a \rangle| = \tau$ verir.

■

Örnek 13.1 (Dördüncü Mertebeden Devresel Grup). S_4 'te $S = (1\ 2\ 3\ 4)$ alalım:

$$S^2 = (1\ 3)(2\ 4), \quad S^3 = (1\ 4\ 3\ 2), \quad S^4 = I$$

O hâlde $\langle S \rangle = \{I, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$ dördüncü mertebeden devresel bir gruptur. Küçük gruplar sınıflandırmamızdaki iki tipten devresel olanın somut örneğidir.

Grubun ikinci bir doğurayı $(1\ 4\ 3\ 2) = S^3 = S^{-1}$ 'dir: tersinin kuvvetleri de aynı kümeyi tarar. Buna karşılık $T = (1\ 3)(2\ 4)$ doğuray olamaz; çünkü $T^2 = I$ olduğundan $\langle T \rangle = \{I, T\}$ iki elemanda kapanır.

13.3 Kuvvet Hesabının Aritmetiği

Sonlu devresel grupta kuvvet hesabı, τ modülüne göre aritmetiğe dönüşür:

Teorem 13.3 (Kuvvetler ve Bölünebilme). $G = \langle a \rangle$, mertebesi τ olan sonlu devresel grup olsun.

1. $s \in \mathbb{Z}$ için: $a^s = 1_G \Leftrightarrow \tau \mid s$
2. $m, n \in \mathbb{Z}$ için: $a^m = a^n \Leftrightarrow m \equiv n \pmod{\tau}$

İspat.

1) $(\Leftarrow) \tau \mid s$ ise $s = \tau s'$ yazılır ve

$$a^s = (a^\tau)^{s'} = 1_G^{s'} = 1_G$$

$(\Rightarrow) a^s = 1_G$ olsun. Bölme algoritmasıyla $s = \tau q + r$, $0 \leq r < \tau$ yazalım:

$$1_G = a^s = (a^\tau)^q \cdot a^r = a^r$$

$r \neq 0$ olsaydı, $a^r = 1_G$ ve $0 < r < \tau$ birlikte τ 'nın en küçüklüğüyle çelişirdi. O hâlde $r = 0$, yani $\tau \mid s$ 'dir.

2) $a^m = a^n \Leftrightarrow a^{m-n} = 1_G \Leftrightarrow \tau \mid (m-n) \Leftrightarrow m \equiv n \pmod{\tau}$; ortadaki adımda 1) kullanıldı.

■

Bu teorem, sonlu devresel grupla $\langle \mathbb{Z}_\tau, + \rangle$ arasındaki derin benzerliğin ilk işaretidir: kuvvetlerin üsleri, τ modülüne göre kalan sınıfları gibi davranır.

Sonlu devresel grubun mertebesi τ , doğurayın kendine has bir niceliğidir: $a^\tau = 1_G$ yapan en küçük doğal sayı. Bu sayı yalnız devresel gruplarda değil, herhangi bir grubun herhangi bir elemanı için tanımlanabilir ve grup teorisinin en çok kullanılan kavramlarından biridir: **bir elemanın mertebesi**.

14. Bir Elemanın Mertebesi

Sonlu devresel grup teorisi bize her elemana iliştilirebilen bir sayı armağan etti: elemanın kuvvetlerinin birime ilk döndüğü an. Bu bölümde eleman mertebesini tanımlayıp kalan sınıfı gruplarında ve permütasyon gruplarında hesaplıyoruz. Permütasyonlar için sonuç zarif bir formüle dönüşür: mertebe, yabancı devre uzunluklarının en küçük ortak katıdır. Yüksek kuvvet hesapları – S^{3045} gibi – bu formülle birkaç satıra iner.

14.1 Tanım

Tanım 14.1 (Bir Elemanın Mertebesi). G bir grup ve $a \in G$ olsun. a 'nın doğurduğu $\langle a \rangle$ devresel alt grubu sonluysa bu alt grubun mertebesine – eşdeğer biçimde, $a^t = 1_G$ koşulunu sağlayan doğal sayıların en küçüğüne – **a elemanın $(G$ grubundaki) mertebesi** denir ve $|a|_G$ veya kısaca $|a|$ ile gösterilir. $\langle a \rangle$ sonsuz devresel grup ise a 'nın mertebesi sonsuzdur denir.

Sonlu bir grupta her elemanın mertebesi sonludur: kuvvetler sonlu kümede sonsuza dek farklı kalmaz. Sonsuz bir grupta ise iki tür eleman bir arada yaşayabilir; örneğin $\langle \mathbb{R} - \{0\}, \cdot \rangle$ grubunda $|-1| = 2$ sonlu, $|2|$ sonsuzdur.

Örnek 14.1 (\$S_4\$'te İki Mertebe). $S = (1\ 2)(3\ 4)$ için $S^2 = (1\ 2)^2(3\ 4)^2 = I$ ve $S \neq I$ olduğundan $|S| = 2$ 'dir. $T = (1\ 2\ 3)$ için $T^2 = (1\ 3\ 2) \neq I$ ve $T^3 = I$ olduğundan $|T| = 3$ 'tür.

Örnek 14.2 ($\mathbb{Z}_{17}^*$ 'da Mertebeler). $\mathbb{Z}_{17}^* = \langle \mathbb{Z}_{17} - \{0\}, \cdot \rangle$ grubunun mertebesi 16'dır; elemanları $\{\bar{1}, \dots, \bar{16}\}$ olarak yazalım. $\bar{5}$, $\bar{4}$ ve $\bar{2}$ 'nin mertebelerini bulunuz.

Çözüm.

$\bar{5}$: Kuvvetleri izleyelim (17'ye göre kalanlarla):

$$\bar{5}^2 = \bar{25} = \bar{8}, \quad \bar{5}^3 = \bar{5} \cdot \bar{8} = \bar{40} = \bar{6}, \quad \bar{5}^4 = \bar{5} \cdot \bar{6} = \bar{30} = -\bar{4}$$

$$\bar{5}^8 = (\bar{5}^4)^2 = (-\bar{4})^2 = \bar{16} = -\bar{1}$$

$\bar{5}^8 = -\bar{1} \neq \bar{1}$ olduğundan mertebe 8'i böler ama 8 olamaz; $\bar{5}^{16} = (-\bar{1})^2 = \bar{1}$ 'dir. Mertebe 16'nın bir böleni olup 1, 2, 4, 8 olamayacağından (ilk kuvvetler $\bar{1}$ vermedi) $|\bar{5}| = 16$ 'dır. Mertebesi grubun mertebesine eşit olduğundan $\bar{5}$ bir doğuraydır:

$$\mathbb{Z}_{17}^* = \langle \bar{5} \rangle$$

$\bar{4}$: $\bar{4}^2 = \bar{16} = -\bar{1}$, dolayısıyla $\bar{4}^4 = \bar{1}$; daha küçük kuvvetler birim vermediğinden $|\bar{4}| = 4$.

$\bar{2}$: $\bar{2}^4 = \bar{16} = -\bar{1}$, dolayısıyla $\bar{2}^8 = \bar{1}$; 1, 2, 4. kuvvetler birim vermediğinden $|\bar{2}| = 8$.

■

Toplamsal gruplarda mertebe, $na = 0_G$ yapan en küçük $n \in \mathbb{N}$ 'dir:

Örnek 14.3 ($\mathbb{Z}_{25}$ 'da Bir Doğuray). $\langle \mathbb{Z}_{25}, + \rangle$ 'da $\bar{11}$ 'in mertebesini bulunuz.

Çözüm.

$n \cdot \bar{11} = \bar{11n} = \bar{0}$ olması, $25 \mid 11n$ demektir. 25 ile 11 aralarında asal olduğundan $25 \mid n$ gerekir; bunun en küçük doğal çözümü $n = 25$ 'tir:

$$|\overline{11}| = 25$$

Mertebe grubun mertebesine eşit olduğundan $\mathbb{Z}_{25} = \langle \overline{11} \rangle$ 'dir: $\overline{11}$ bir doğuraydır. (Katları sırayla yazarak da görülebilir: $\overline{11}, \overline{22}, \overline{8}, \overline{19}, \dots$ dizisi 25 adımda bütün sınıfları dolaşır.)

■

14.2 Permütasyonların Mertebesi

Teorem 14.1 (Devrenin Mertebesi). S_n 'de k uzunluğundaki bir devrenin mertebesi k 'dır.

İspat.

$D = (a_1 a_2 \dots a_k)$ olsun. D^j kuvveti her a_i 'yi devre içinde j adım öteler; $0 < j < k$ için $a_1 \mapsto a_{j+1} \neq a_1$ olduğundan $D^j \neq I$ 'dir. $j = k$ 'de ise her eleman tam tur atar: $D^k = I$. En küçük doğal kuvvet k olduğundan $|D| = k$ 'dir.

■

Teorem 14.2 (Mertebe EKOK Kuralı). S_n 'de bir S substitüsyonunun mertebesi, S 'nin ayrıldığı yabancı devrelerin uzunluklarının en küçük ortak katına eşittir:

$$S = D_1 D_2 \dots D_r, \quad |D_i| = k_i \implies |S| = [k_1, k_2, \dots, k_r]$$

İspat.

$m = [k_1, \dots, k_r]$ diyelim.

$S^m = I$: Her i için $k_i \mid m$, diyelim $m = k_i t_i$; o hâlde

$$D_i^m = (D_i^{k_i})^{t_i} = I$$

Yabancı devreler ikişer ikişer komutatif olduğundan kuvvet, çarpanlara dağıtılabilir:

$$S^m = (D_1 \dots D_r)^m = D_1^m \dots D_r^m = I$$

m en küçüktür: $\ell \in \mathbb{N}$, $S^\ell = I$ olsun:

$$I = S^\ell = D_1^\ell D_2^\ell \dots D_r^\ell$$

$D_1^\ell, \dots, D_r^\ell$ substitüsyonları da ikişer ikişer yabancıdır (her biri kendi devresinin elemanlarını oynatır). Yabancı substitüsyonların çarpımı birimse her biri birim olmak zorundadır; çünkü biri bir elemanı oynatsaydı, öbürleri o elemana dokunamayacağından çarpım da onu oynatırdı. O hâlde her i için $D_i^\ell = I$, kuvvet aritmetiği teoremiyle $k_i \mid \ell$ 'dir. Bütün k_i 'lerin ortak katı olan ℓ , EKOK tanımı gereği m 'ye bölünür: $m \mid \ell$, özel olarak $m \leq \ell$. Demek ki $|S| = m$ 'dir.

■

Örnek 14.4 (Hızlı Mertebe Okuma). S_8 'de $S = (25)(137)(468)$ için uzunluklar 2, 3, 3'tür:

$$|S| = [2, 3, 3] = 6$$

Örnek 14.5 (Yüksek Kuvvet Hesabı). S_8 'de $S = (1273)(64)(38745)$ substitüsyonu veriliyor (devreler yabancı değildir). S^{3045} 'in yabancı devrelere ayrılışını bulunuz.

Çözüm.

Önce S 'nin kendisini yabancı devrelere ayıralım; çarpanlar sağdan sola uygulanır. Yörüngeleri izleyince

$$S = (127645)(38)$$

bulunur. (Denetim örneği: en sağdaki devre $3 \mapsto 8$ der, kalan çarpanlar 8'e dokunmaz — $S(3) = 8$; yine sağdaki devre $8 \mapsto 7$, soldaki devre $7 \mapsto 3$ der — $S(8) = 3$.)
Uzunluklar 6 ve 2 olduğundan

$$|S| = [6, 2] = 6, \quad S^6 = I$$

3045'i 6'ya bölelim: $3045 = 6 \cdot 507 + 3$. O hâlde

$$S^{3045} = (S^6)^{507} \cdot S^3 = S^3 = (1\ 2\ 7\ 6\ 4\ 5)^3 (3\ 8)^3$$

Altılı devrenin küpü, her elemanı üç adım ötelere ve devreyi transpozisyonlara kırar; $(3\ 8)^3 = (3\ 8)$ 'dir:

$$S^{3045} = (1\ 6)(2\ 4)(7\ 5)(3\ 8)$$

■

14.3 Komutatif Elemanların Çarpımı

Teorem 14.3 (Komutatif Çarpımın Mertebesi). a ve b , bir grubun **komutatif** iki elemanı olsun ($ab = ba$). $|a| = m$, $|b| = n$ ve $(m, n) = 1$ (aralarında asal) ise

$$|a \cdot b| = m \cdot n$$

Daha genel olarak $a_1, \dots, a_k$ *ikişer ikişer komutatif*, mertebeleri $n_1, \dots, n_k$ *ikişer ikişer aralarında asal* ise $|a_1 a_2 \dots a_k| = n_1 n_2 \dots n_k$ 'dır.

EKOK kuralı bu teoremin permütasyonlardaki yansımasıdır: yabancı devreler komutatif ve uzunlukları aralarında asalsa $[k_1, \dots, k_r] = k_1 \dots k_r$ olur.

14.4 Alıştırma

Alıştırma 14.1 (Yüksek Kuvvet). S_9 'da $S = (1\ 3\ 8)(2\ 7)(4\ 9\ 6\ 5)$ substitüsyonu için S^{1012} 'nin yabancı devrelere ayrılışını bulunuz.

Çözüm.

Devreler zaten yabancısıdır; uzunluklar 3, 2, 4:

$$|S| = [3, 2, 4] = 12, \quad S^{12} = I$$

1012 = 12 · 84 + 4 olduğundan

$$S^{1012} = S^4 = (1\ 3\ 8)^4 (2\ 7)^4 (4\ 9\ 6\ 5)^4 = (1\ 3\ 8) \cdot I \cdot I = (1\ 3\ 8)$$

Üçlü devrenin dördüncü kuvveti kendisidir ($D^4 = D^3 D = D$); transpozisyonun ve dörtlü devrenin dördüncü kuvvetleri birimdir.

■

Eleman mertebesi, devresel alt grupların boyunu ölçüyor. Sıradaki soru yapısal: bir devresel grubun *bütün* alt grupları nasıl görünür? Yanıt şaşırtıcı ölçüde eksiksizdir — hepsi devreseldir ve mertebeleri, grup mertebesinin bölenleriyle birebir eşleşir: **devresel grubun alt grupları**.

15. Devresel Grubun Alt Grupları

Devresel gruplar yalnız kendileri düzenli değildir; alt grup dünyaları da tamamen şeffaftır. Bu bölümün dört sonucu, sonlu devresel grubun alt grup teorisini eksiksiz kapatır: her alt grup devreseldir, her alt grubun mertebesi grup mertebesini böler, her bölene karşılık *tam bir* alt grup vardır ve doğuraylar $(m, n) = 1$ koşuluyla belirlenir. Bölümün sonunda doğuray sayısını Euler'in φ fonksiyonuyla sayacağız.

15.1 Her Alt Grup Devreseldir

Teorem 15.1 (Devresel Grubun Alt Grupları Devreseldir). *Bir devresel grubun her alt grubu da devreseldir.*

İspat.

$G = \langle a \rangle$ ve $H \subseteq G$ olsun. İki durum vardır.

$H = \{1_G\}$ ise $H = \langle 1_G \rangle$ devreseldir.

$H \neq \{1_G\}$ olsun. H 'de 1_G 'den farklı bir eleman, yani $m \neq 0$ için bir a^m vardır. H grup olduğundan a^m ile birlikte $(a^m)^{-1} = a^{-m}$ 'yi de içerir; m ile $-m$ 'den biri pozitif olduğundan, $a^m \in H$ koşulunu sağlayan en az bir doğal sayı m vardır. Bu doğal sayıların en küçüğüne μ diyelim.

İddia: $H = \langle a^\mu \rangle$.

$H \subseteq \langle a^\mu \rangle$: $a^n \in H$ olsun. Bölme algoritmasıyla $n = \mu q + r$, $0 \leq r < \mu$ yazalım:

$$a^r = a^{n-\mu q} = (a^\mu)^{-q} \cdot a^n \in H$$

çünkü sağdaki iki çarpan da H 'dedir. $0 < r < \mu$ olsaydı μ 'nün en küçüklüğü bozulurdu; o hâlde $r = 0$ ve

$$a^n = (a^\mu)^q \in \langle a^\mu \rangle$$

$\langle a^\mu \rangle \subseteq H$: $a^\mu \in H$ ve H grup olduğundan a^μ 'nün bütün kuvvetleri H 'dedir.

İki kapsama birlikte $H = \langle a^\mu \rangle$ verir: H devreseldir.

■

Sonuç 15.1 (Sonsuz Devresel Grubun Alt Grupları). *Sonsuz devresel bir grubun $\{1_G\}$ 'den farklı her alt grubu da sonsuz devreseldir.*

İspat.

$G = \langle a \rangle$ sonsuz devresel, $H \neq \{1_G\}$ bir alt grup olsun. Teoremden $H = \langle a^\mu \rangle$ 'dür ($\mu \in \mathbb{N}$). $m \neq n$ tam sayıları için $\mu m \neq \mu n$ ve G sonsuz devresel olduğundan

$$(a^\mu)^m = a^{\mu m} \neq a^{\mu n} = (a^\mu)^n$$

a^μ 'nün kuvvetleri birbirinden farklıdır: H sonsuz devreseldir.

■

15.2 Mertebe Ayrışımı: $n = \mu\nu$

Teorem 15.2 (Alt Grubun Mertebesi). $G = \langle a \rangle$, n . mertebeden devresel bir grup ve H , G 'nin a^μ tarafından doğurulan alt grubu olsun ($\mu, a^\mu \in H$ koşulunu sağlayan doğal sayıların en küçüğü). Bu takdirde

$$n = \mu\nu \quad \text{ve} \quad |H| = \nu$$

olacak biçimde bir $\nu \in \mathbb{N}$ vardır ve tek türlü belirlidir.

İspat.

$\mu \mid n$: n 'yi μ 'ye bölelim: $n = \mu\nu + r$, $0 \leq r < \mu$. O zaman

$$a^r = a^{n-\mu\nu} = a^n \cdot (a^\mu)^{-\nu} = 1_G \cdot (a^\mu)^{-\nu} \in H$$

$0 < r < \mu$, μ 'nin en küçüklüğüyle çelişeceğinden $r = 0$ 'dır: $n = \mu\nu$.

$|H| = \nu$: Önce H 'nin listesini çıkaralım:

$$H = \langle a^\mu \rangle = \{1_G, a^\mu, (a^\mu)^2, \dots, (a^\mu)^{\nu-1}\}$$

Gerçekten herhangi bir $(a^\mu)^k$ için $k = \nu q + r'$, $0 \leq r' < \nu$ yazılırsa

$$(a^\mu)^k = ((a^\mu)^\nu)^q (a^\mu)^{r'} = (a^{\mu\nu})^q (a^\mu)^{r'} = (a^n)^q (a^\mu)^{r'} = (a^\mu)^{r'}$$

listeye düşer. Listedekiler birbirinden farklıdır: $0 \leq r_1 < r_2 < \nu$ için $(a^\mu)^{r_1} = (a^\mu)^{r_2}$ olsaydı $a^{\mu(r_2-r_1)} = 1_G$ olur, kuvvet aritmetiğinden $n = \mu\nu \mid \mu(r_2 - r_1)$, yani $\nu \mid (r_2 - r_1)$ çıkardı; oysa $0 < r_2 - r_1 < \nu$ 'dür. O hâlde $|H| = \nu$ 'dür.

■

Sonuç 15.2 (Alt Grup Mertebesi Grup Mertebesini Böler). Sonlu devresel bir grubun her alt grubunun mertebesi, grubun mertebesini böler.

İspat.

$|G| = n$ olsun. $H = \{1_G\}$ için $|H| = 1 \mid n$ 'dir. $H \neq \{1_G\}$ ise $H = \langle a^\mu \rangle$ ve mertebe ayrışımı teoreminden $|H| = \nu$ ile $n = \mu\nu$; yani $\nu \mid n$ 'dir.

■

Bu sonuç, ileride her sonlu grup için kanıtlayacağımız Lagrange teoreminin devresel öncüsüdür. Devresel gruplarda tersi de doğrudur:

Teorem 15.3 (Her Bölüne Karşılık Tek Alt Grup). $G = \langle a \rangle$, n . mertebeden devresel bir grup olsun. n 'nin her ν doğal bölenine karşılık G 'nin ν . mertebeden bir ve yalnız bir alt grubu vardır; bu alt grup $\langle a^{n/\nu} \rangle$ 'dür.

İspat.

Varlık. $\nu \mid n$ olsun ve $\mu = n/\nu$ yazalım. Mertebe ayrışımı teoreminin hesabı, $\langle a^\mu \rangle$ alt grubunun tam ν elemanlı olduğunu gösterir.

Teklik. H , ν . mertebeden herhangi bir alt grup olsun. Alt gruplar devreseldir: $H = \langle a^{\mu'} \rangle$, μ' en küçük üs. Mertebe ayrışımından $n = \mu' \cdot |H| = \mu' \nu$; yani $\mu' = n/\nu = \mu$ tek türlü belirlidir ve $H = \langle a^{n/\nu} \rangle$ 'dür.

■

15.3 Doğuraylar ve Euler'in ϕ Fonksiyonu

Teorem 15.4 (Doğuray Ölçütü). $G = \langle a \rangle$, n . mertebeden devresel bir grup olsun. a^m ($m \in \mathbb{Z}$) elemanının G 'nin bir doğurayı olması için gerek ve yeter koşul $(m, n) = 1$ olmasıdır.

İspat.

Bézout teoremini hatırlayalım: m ile n 'nin aralarında asal olması, $km + \ell n = 1$ olacak biçimde k, ℓ tam sayılarının varlığına denktir.

Gereklik. $G = \langle a^m \rangle$ olsun. $a \in G$ olduğundan $a = (a^m)^u = a^{mu}$ olacak bir $u \in \mathbb{Z}$ vardır; kuvvet aritmetiğinden

$$1 \equiv mu \pmod{n} \implies 1 - mu = vn \implies mu + vn = 1$$

olacak bir $v \in \mathbb{Z}$ bulunur: $(m, n) = 1$ 'dir.

Yeterlik. $(m, n) = 1$ olsun: $km + \ell n = 1$ yazalım. O zaman

$$a = a^{km+\ell n} = (a^m)^k \cdot (a^n)^\ell = (a^m)^k \cdot 1_G = (a^m)^k \in \langle a^m \rangle$$

a 'nın bütün kuvvetleri de $\langle a^m \rangle$ 'de olduğundan $G = \langle a \rangle \subseteq \langle a^m \rangle \subseteq G$; yani $G = \langle a^m \rangle$ ve a^m doğuraydır. ■

Sonuç 15.3 (Doğuray Sayısı). n . mertebeden devresel bir grubun doğuraylarının sayısı $\varphi(n)$ 'dir; burada φ , **Euler'in φ fonksiyonudur**: $\varphi(n)$, n 'yi aşmayan ve n ile aralarında asal olan doğal sayıların sayısıdır. $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ asal çarpanlara ayrılışıyla

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Örnek 15.1 (Mertebesi 12 Olan Devresel Grubun Envanteri). $G = \langle a \rangle$, $|G| = 12$ olsun. Bütün alt gruplarını ve doğuraylarını bulunuz.

Çözüm.

12'nin bölenleri 1, 2, 3, 4, 6, 12'dir; her bölene karşılık tam bir alt grup vardır ve ν mertebeli alt grup $\mu = 12/\nu$ ile $\langle a^\mu \rangle$ 'dür:

$$H_1 = \{1_G\}, \quad H_2 = \langle a^6 \rangle = \{1_G, a^6\}, \quad H_3 = \langle a^4 \rangle = \{1_G, a^4, a^8\}$$

$$H_4 = \langle a^3 \rangle = \{1_G, a^3, a^6, a^9\}$$

$$H_6 = \langle a^2 \rangle = \{1_G, a^2, a^4, a^6, a^8, a^{10}\}, \quad H_{12} = G$$

Doğuraylar, 12 ile aralarında asal üslü kuvvetlerdir:

$$a, \quad a^5, \quad a^7, \quad a^{11}; \quad \varphi(12) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 4$$

■

Alt grup envanteri elimizde; ama altı alt grubun *birbiriyle ilişkisi* — hangisi hangisinin içinde? — listeden okunmuyor. Bu ilişkiyi tek bakışta gösteren bir çizim tekniği var: [Hasse diyagramları](#).

16. Hasse Diyagramları

Devresel grubun alt grup envanterini tam olarak çıkarabiliyoruz; şimdi bu envanteri *görselleştireceğiz*. Hasse diyagramı, alt grupları kapsama ilişkisine göre katlara dizen bir şemadır: kapsanan aşağıda, kapsayan yukarıda, arada bir çizgi. Devresel gruplarda diyagramın tamamı tek bir aritmetik gözlemle çizilir — alt grupların kapsama ilişkisi, mertebelerin bölünebilme ilişkisinin kopyasıdır.

16.1 Alt Gruplar Şeması

Tanım 16.1 (Hasse Diyagramı). Sonlu sayıda alt grubu bulunan bir G grubu verilsin. $H_1 \subseteq H_2$ olan iki alt gruptan H_1, H_2 'nin altında bir hizaya yerleştirilip iki alt grup bir çizgiyle birleştirilir; biri diğerinin içinde olmayan iki alt grup ise aynı hizaya veya (çizgi çekilmeksizin) farklı hizalara yerleştirilir. Bütün alt grupların bu biçimde yerleştirilmesiyle elde edilen şemaya G 'nin **Hasse diyagramı** (alt gruplar şeması) denir.

(Şema çizilirken zincirleme kapsamaların ara çizgileri atlanır: $H_1 \subseteq H_2 \subseteq H_3$ durumunda $H_1 - H_3$ çizgisi çizilmez; o ilişki iki basamaktan zaten okunur. Yerleştirmeyi olabildiğince simetrik yapmak şemayı okunur kılar.)

Devresel gruplarda şemayı çizen anahtar gözlem şudur. $G = \langle a \rangle$, n . mertebeden ve $H_\nu = \langle a^{n/\nu} \rangle$, ν mertebeli alt grup olsun:

$$H_{\nu_1} \subseteq H_{\nu_2} \Leftrightarrow \nu_1 \mid \nu_2$$

Gerçekten $H_{\nu_1} \subseteq H_{\nu_2}$ ise, alt grup mertebesi kapsayan alt grubun mertebesini bölmek zorundadır (devresel gruplarda bunu kanıtladık). Tersine $\nu_1 \mid \nu_2$ ise $\mu_1 = n/\nu_1, \mu_2 = n/\nu_2$ için $\mu_2 \mid \mu_1$ olur; a^{μ_1}, a^{μ_2} 'nin bir kuvvetidir ve $H_{\nu_1} = \langle a^{\mu_1} \rangle \subseteq \langle a^{\mu_2} \rangle = H_{\nu_2}$ çıkar. **Yani devresel grubun Hasse diyagramı, n 'nin bölenlerinin bölünebilme diyagramının aynısıdır.**

16.2 Temel Örnekler

Örnek 16.1 (Mertebe Asal: En Yalın Şema). p asal ve $G = \langle a \rangle$, p . mertebeden olsun. Alt grup mertebeleri p 'nin bölenleridir: yalnız 1 ve p . Yani alt gruplar yalnızca trivial olanlardır ve şema tek çizgidir:

$$\begin{array}{c} G \\ | \\ \{1_G\} \end{array}$$

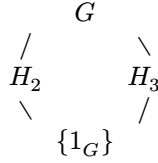
Doğuraylar: $a, a^2, \dots, a^{p-1}$ — birimden farklı her eleman; sayıları $\varphi(p) = p - 1$.

Örnek 16.2 (Mertebe 4, 6 ve 8). $n = 4$: Bölenler 1, 2, 4. Şema bir zincirdir:

$$\begin{array}{c} G \\ | \\ H_2 = \langle a^2 \rangle \\ | \\ \{1_G\} \end{array}$$

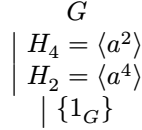
Doğuraylar a, a^3 ; $\varphi(4) = 2$.

$n = 6$: Bölenler 1, 2, 3, 6. $H_2 = \langle a^3 \rangle$ ile $H_3 = \langle a^2 \rangle$ birbirini kapsamaz ($2 \nmid 3$); şema bir eşkenar dörtgendir:



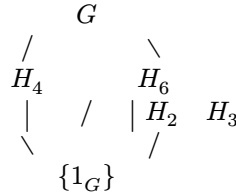
Doğuraylar $a, a^5; \varphi(6) = 2$.

$n = 8$: Bölenler 1, 2, 4, 8 zincir oluşturur ($1 \mid 2 \mid 4 \mid 8$):



Doğuraylar $a, a^3, a^5, a^7; \varphi(8) = 4$.

Örnek 16.3 (Mertebe 12). $n = 12$ 'nin bölenleri 1, 2, 3, 4, 6, 12'dir; alt gruplar önceki bölümde listelenmişti. Bölünebilme ilişkileri: $2 \mid 4, 2 \mid 6, 3 \mid 6, 4 \mid 12$ ile 6'nın üstünde yalnız 12 vardır. Şema:



(Ortadaki çapraz çizgi $H_2 \subseteq H_6$ kapsamasıdır; $H_2 \subseteq H_4$ ve $H_3 \subseteq H_6$ dikey çizgilerle gösterildi.) Doğuraylar $a, a^5, a^7, a^{11}; \varphi(12) = 4$.

16.3 Permütasyonlarla İki Büyük Örnek

Örnek 16.4 (Mertebesi 24 Olan Devresel Grup). S_{11} 'de, elemanları $a, b, \dots, k$ harfleriyle yazılmış

$$S = (a c g h e f b d)(a h b e)(c g d f)(i j k)$$

substitüsyonu tarafından doğurulan devresel grubun alt gruplar şemasını çiziniz.

Çözüm.

Önce S 'yi yabancı devrelere ayırılım (çarpanlar sağdan sola uygulanır). Yörüngeler izlenince

$$S = (a e c h d b f g)(i j k)$$

bulunur: sekizli ve üçlü yabancı devreler. Mertebe, EKOK kuralından

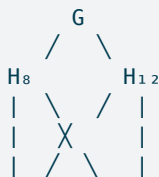
$$|S| = [8, 3] = 24$$

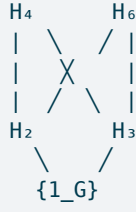
ve $G = \langle S \rangle = \{I, S, S^2, \dots, S^{23}\}$ 'tür.

24'ün bölenleri 1, 2, 3, 4, 6, 8, 12, 24; her ν bölenine karşılık $H_\nu = \langle S^{24/\nu} \rangle$ alt grubu vardır:

$$H_2 = \langle S^{12} \rangle, \quad H_3 = \langle S^8 \rangle, \quad H_4 = \langle S^6 \rangle, \quad H_6 = \langle S^4 \rangle, \quad H_8 = \langle S^3 \rangle, \quad H_{12} = \langle S^2 \rangle$$

Kapsamalar bölünebilmeyi izler: $2 \mid 4, 6, 8, 12; 3 \mid 6 \mid 12; 4 \mid 8, 12$. Şema:





Buradaki çizgiler: $G-H_8, G-H_{12}; H_8-H_4, H_{12}-H_4, H_{12}-H_6; H_4-H_2, H_6-H_2, H_6-H_3; H_2-\{1_G\}, H_3-\{1_G\}$.

Doğuraylar, 24 ile aralarında asal üslerdir:

$$S, S^5, S^7, S^{11}, S^{13}, S^{17}, S^{19}, S^{23}; \quad \varphi(24) = 24 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 8$$

■

Örnek 16.5 (Mertebesi 42 Olan Devresel Grup). S_{20} 'de, elemanları yirmi harften oluşan

$$S = (a u p b i s)(k m o b h)(d t e f n j)(g r u v c)$$

substitüsüyonu tarafından doğurulan devresel grubun alt gruplar şemasını çiziniz.

Çözüm.

Devreler yabancı değildir (b ile u iki devrede geçiyor); yörüngeleri izleyerek yabancı ayrılışı çıkaralım:

$$S = (a u v c g r p b h k m o i s)(d t e f n j)$$

on dörtlü ve altılı yabancı devreler. Mertebe:

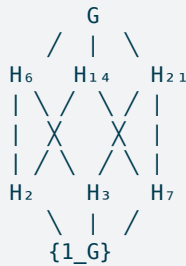
$$|S| = [14, 6] = 42, \quad G = \langle S \rangle = \{I, S, \dots, S^{41}\}$$

$42 = 2 \cdot 3 \cdot 7$ 'nin bölenleri 1, 2, 3, 6, 7, 14, 21, 42'dir; alt gruplar $H_\nu = \langle S^{42/\nu} \rangle$:

$$H_2 = \langle S^{21} \rangle, \quad H_3 = \langle S^{14} \rangle, \quad H_6 = \langle S^7 \rangle$$

$$H_7 = \langle S^6 \rangle, \quad H_{14} = \langle S^3 \rangle, \quad H_{21} = \langle S^2 \rangle$$

Kapsamalar: $2 \mid 6, 14; 3 \mid 6, 21; 7 \mid 14, 21$. Şema, küpün köşelerine yerleşmiş gibi tam simetrik çıkar (bölenler $2^{\epsilon_1} 3^{\epsilon_2} 7^{\epsilon_3}, \epsilon_i \in \{0, 1\}$ biçimindedir):



Çizgiler: $G-H_6, G-H_{14}, G-H_{21}; H_6-H_2, H_6-H_3; H_{14}-H_2, H_{14}-H_3; H_{21}-H_2, H_{21}-H_3; H_2, H_3, H_7-\{1_G\}$.

Doğuray sayısı:

$$\varphi(42) = 42 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{7}\right) = 12$$

Doğuraylar: $S, S^5, S^{11}, S^{13}, S^{17}, S^{19}, S^{23}, S^{25}, S^{29}, S^{31}, S^{37}, S^{41}$.



Devresel grupların dünyası artık baştan sona haritalanmış durumda. Genel gruplara dönme vakti: bir alt grup, kendisini kapsayan grubu nasıl dilimler? Bu sorunun aygıtı — alt kümelerle çarpma — bir sonraki bölümün konusudur: [komplekslerle hesap](#).

17. Komplekslerle Hesap

Grup teorisinin bundan sonraki büyük adımları — kalan sınıfları, Lagrange teoremi, bölüm grupları — elemanlarla değil *elemanlardan oluşan kümelerle* hesap yapmayı gerektirir. Bu bölümde o hesabın gramerini kuruyoruz: iki alt kümenin çarpımı, bir alt kümenin tersi ve bu işlemlerin cebiri. Bölümün yıldız sonucu, iki alt grubun çarpımının ne zaman yine alt grup olduğunu söyleyen $HK = KH$ ölçütüdür.

17.1 Kompleks Kavramı

Tanım 17.1 (Kompleks). Bir G grubunun boş olmayan bir alt kümesine G 'nin bir **kompleksi** denir.

Tanım 17.2 (Komplekslerin Çarpımı). A ve B , $\langle G, \cdot \rangle$ grubunun iki kompleksi olsun. A ile B 'nin (bu sıradaki) çarpımı

$$A \cdot B = \{a \cdot b \in G : a \in A, b \in B\} \subseteq G$$

kompleksdir. $A = \{a\}$ tek elemanlıysa $\{a\}B$ yerine kısaca aB ; $B = \{b\}$ tek elemanlıysa Ab yazılır:

$$aB = \{a \cdot b : b \in B\}, \quad Ab = \{a \cdot b : a \in A\}$$

Kompleks çarpımının temel dil bilgisi:

- **Asosyatiflik:** $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ — çünkü elemanlar düzeyinde $(ab)c = a(bc)$ 'dir.
- **Komutatif grupta:** $A \cdot B = B \cdot A$ — her ab çarpımı ba olarak da yazılır.
- **Komutatif olmayan grupta** genel olarak $A \cdot B \neq B \cdot A$ 'dır; ama eşitlik *bazı* çiftlerde yine de sağlanabilir. Örneğin S_3 'te $A = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$ ve $B = \{(1\ 2), (1\ 3)\}$ alınırsa çarpımlar tek tek hesaplandığında

$$A \cdot B = \{(1\ 2), (1\ 3), (2\ 3)\} = B \cdot A$$

bulunur — iki çarpım da S_3 'ün bütün transpozisyonlarının kümesidir. Önemli nokta: $AB = BA$ eşitliği, *eleman eleman* değişme demek değildir; iki kümenin küme olarak çıkışması demektir.

Tanım 17.3 (Kompleksin Tersi). A kompleksinin bütün elemanlarının terslerinden oluşan komplekse A 'nın **tersi** denir:

$$A^{-1} = \{a^{-1} \in G : a \in A\}$$

⚠ $A \cdot A^{-1}$ birim kompleks değildir

A en az iki elemanlıysa $A \cdot A^{-1} \neq \{1_G\}$ 'dir: çarpım kümesinde $aa^{-1} = 1_G$ 'lerin yanı sıra $a \neq b$ için $ab^{-1} \neq 1_G$ çarpımları da bulunur. Kompleks tersi, eleman tersinin bire bir kopyası değildir.

Teorem 17.1 (Kompleks Tersinin Kuralları). A, B , bir G grubunun kompleksleri olsun.

1. $(A^{-1})^{-1} = A$
2. $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$

İspat.

İki kural da eleman düzeyindeki $(a^{-1})^{-1} = a$ ve $(ab)^{-1} = b^{-1}a^{-1}$ kurallarının kümelere yansımalarıdır. Örneğin 2) için: $(AB)^{-1}$ 'in tipik elemanı $(ab)^{-1} = b^{-1}a^{-1}$ 'dir ve $b^{-1} \in B^{-1}$, $a^{-1} \in A^{-1}$ olduğundan bu eleman $B^{-1}A^{-1}$ 'dedir; tersine $B^{-1}A^{-1}$ 'in tipik elemanı $b^{-1}a^{-1} = (ab)^{-1} \in (AB)^{-1}$ 'dir.

■

17.2 Alt Grup Ölçütlerinin Kompleks Dili

Alt grup ölçütlerimiz kompleks diliyle tek satırlık koşullara dönüşür. H, G 'nin bir kompleksi olsun:

- H alt gruptur $\Leftrightarrow H \cdot H \subseteq H$ ve $H^{-1} \subseteq H$.
- G sonlu ise: H alt gruptur $\Leftrightarrow H \cdot H \subseteq H$.
- H alt gruptur $\Leftrightarrow H \cdot H^{-1} \subseteq H$.

Bunlar sırasıyla iki koşullu, sonlu ve tek koşullu ölçütlerin yeniden yazılışıdır. Alt gruplar için kapsamalar aslında eşitliğe döner:

Örnek 17.1 (Alt Gruplarda $H^{-1} = H$ ve $H \cdot H = H$). $\langle G, \cdot \rangle$ bir grup olsun. $G^{-1} = G$ ve $G \cdot G = G$ olduğunu gösteriniz. (Aynı akıl yürütme her H alt grubu için $H^{-1} = H$ ve $H \cdot H = H$ verir.)

Çözüm.

$G^{-1} = G$: Her g^{-1} yine G 'de olduğundan $G^{-1} \subseteq G$ 'dir. Tersine her $g \in G$ için $g = (g^{-1})^{-1}$ yazılabilir ve $g^{-1} \in G$ olduğundan $g \in G^{-1}$ 'dir: $G \subseteq G^{-1}$.

$G \cdot G = G$: Kapalılıktan $G \cdot G \subseteq G$ 'dir. Tersine her $g \in G$ için $g = g \cdot 1_G \in G \cdot G$ 'dir: $G \subseteq G \cdot G$.

■

17.3 İki Alt Grubun Çarpımı

Teorem 17.2 (HK Ne Zaman Alt Gruptur?). H ve K , bir G grubunun iki alt grubu olsun. $H \cdot K$ kompleksinin G 'nin bir alt grubu olması için gerek ve yeter koşul

$$H \cdot K = K \cdot H$$

olmasıdır.

İspat.

Gereklik. HK alt grup olsun. Alt gruplar kendi terslerine eşit olduğundan ve kompleks tersi kuralıyla

$$HK = (HK)^{-1} = K^{-1}H^{-1} = KH$$

Son adımda H ile K 'nin alt grup olarak $H^{-1} = H$, $K^{-1} = K$ eşitlikleri kullanıldı.

Yeterlik. $HK = KH$ olsun; iki koşullu kompleks ölçütünü denetleyelim.

Çarpıma kapalılık:

$$(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$$

Ortadaki adımda hipotez, sonrakinde asosyatiflik ve $HH = H$, $KK = K$ eşitlikleri kullanıldı; sonuç $\subseteq$ yerine doğrudan eşitlik verdi.

Terslere kapalılık:

$$(HK)^{-1} = K^{-1}H^{-1} = KH = HK$$

İki koşul sağlandığından $HK \subseteq G$ 'dir.
a.g.

■

Komutatif gruplarda $HK = KH$ bedava sağlandığından *iki alt grubun çarpımı daima alt gruptur*. Komutatif olmayan gruplarda ise koşul gerçekten kısıtlayıcıdır; örneğin S_3 'te $H = \{I, (12)\}$ ve $K = \{I, (13)\}$ için

$$HK = \{I, (13), (12), (132)\}$$

dört elemanlıdır; ama $4 \nmid 6$ olduğundan (bir sonraki bölümlerde kanıtlayacağımız Lagrange teoremi gereği) S_3 'ün dört elemanlı alt grubu olamaz – nitekim $KH = \{I, (12), (13), (123)\} \neq HK$ 'dir.

17.4 Toplamsal Yazış

$\langle G, + \rangle$ komutatif grubunda kompleks işlemleri toplamsal yazılır:

$$A + B = \{a + b : a \in A, b \in B\}, \quad -A = \{-a : a \in A\}$$

ve kurallar aynen taşınır: $(A + B) + C = A + (B + C)$; $A + B = B + A$; $-(-A) = A$; $-(A + B) = (-A) + (-B)$. Alt grup ölçütü: H alt gruptur $\Leftrightarrow H + (-H) \subseteq H$.

Son bir gözlem, ileride sık kullanılacak: $A = B$ ise her $g \in G$ için $gA = gB$ ve $Ag = Bg$ 'dir; $A \subseteq B$ ise $gA \subseteq gB$ ve $Ag \subseteq Bg$ 'dir. (Elemanlara g ile çarpma uygulamak kümeleri aynı biçimde dönüştürür.)

Kompleks hesabı kurulduğuna göre onu asıl amacına koşabiliriz: bir alt grubun aH biçimindeki ötelemeleri, grubu birbirine denk parçalara diler. Bu dilimleme — kalan sınıfları — sonlu grup teorisinin en güçlü teoremine götüren yoldur: [kalan sınıfları](#).

18. Bir Alt Gruba Göre Kalan Sınıfları

Modüler aritmetikte $\mathbb{Z}$ 'yi m 'nin katlarına göre sınıflara ayırmıştık: $a \equiv b \pmod{m}$, yani $a - b$ kümesi $m\mathbb{Z}$ alt grubunda. Bu bölüm aynı fikri keyfi bir gruba taşır: H alt grubu verilince " $a^{-1}b \in H$ " bağıntısı G 'yi **kalan sınıflarına** böler. Sınıfların iki altın özelliği — ya çakışır ya ayrıkırlar, ve hepsi aynı büyüklüktedir — bir sonraki bölümde Lagrange teoremini tek hamlede verecek.

18.1 Soldan ve Sağdan Eşdeğerlik

Tanım 18.1 (Soldan ve Sağdan Eşdeğerlik). $\langle G, \cdot \rangle$ bir grup, $H \subseteq G$ ve $a, b \in G$ olsun.

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

ise " a, b 'ye H alt grubuna göre **soldan eşdeğerdir**" denir ve $a \sim_{\text{sol}} b (H)$ yazılır;

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

ise " a, b 'ye H 'ye göre **sağdan eşdeğerdir**" denir ve $a \sim_{\text{sağ}} b (H)$ yazılır.

Teorem 18.1 (Eşdeğerlikler Denklik Bağıntısıdır). $\sim_{\text{sol}}$ ve $\sim_{\text{sağ}}$ bağıntıları G 'de birer eşdeğerlik (denklik) bağıntısıdır.

İspat.

Soldan eşdeğerlik için üç koşulu denetleyelim; sağdan eşdeğerlik tamamen benzerdir.

Yansıma: H alt grup olduğundan $1_G \in H$ 'dir; her a için $a^{-1}a = 1_G \in H$, yani $a \sim a$.

Simetri: $a \sim b$ ise $a^{-1}b \in H$ 'dir; H terslere kapalı olduğundan

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

Geçişme: $a \sim b$ ve $b \sim c$ ise $a^{-1}b \in H$ ve $b^{-1}c \in H$ 'dir; H çarpmaya kapalı olduğundan

$$(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}c \in H \implies a \sim c$$

■

Tanım 18.2 (Kalan Sınıfları). $\sim_{\text{sol}}$ eşdeğerlik bağıntısının G 'de belirttiği denklik sınıflarına G 'nin H alt grubuna göre **sol kalan sınıfları**; $\sim_{\text{sağ}}$ 'in belirttiği sınıflara **sağ kalan sınıfları** denir.

18.2 Sınıfların Kompleks Biçimi

Soyut denklik sınıfları, kompleks çarpımıyla son derece somut bir biçim alır:

Teorem 18.2 (Sol Kalan Sınıfı aH). G 'nin H 'ye göre bir sol kalan sınıfı, a bu sınıfın herhangi bir elemanı olmak üzere, G 'nin aH kompleksi ile çakışır.

İspat.

$K_a = \{b \in G : b \sim_{\text{sol}} a\}$, a 'nın sınıfı olsun. Simetriden $b \sim a \Leftrightarrow a \sim b$ olduğuna dikkat ederek

$$b \in K_a \Leftrightarrow a^{-1}b \in H \Leftrightarrow \exists h \in H : a^{-1}b = h$$

$$\Leftrightarrow \exists h \in H : b = ah \Leftrightarrow b \in aH$$

O hâlde $K_a = aH$ 'dir.

■

Teorem 18.3 (Sağ Kalan Sınıfı $= H a$). Benzer biçimde, a 'nın sağ kalan sınıfı Ha kompleksi ile çıkarılır:
 $b \underset{\text{sağ}}{\sim} a \Leftrightarrow ba^{-1} \in H \Leftrightarrow b \in Ha$.

İki hızlı gözlem:

- H 'nin kendisi hem bir sol hem bir sağ kalan sınıfıdır: $H = 1_G H = H 1_G$.
- $a \in aH$ 'dir ($a = a \cdot 1_G$); her eleman kendi sınıfının içindedir.

Sonuç 18.1 (Sınıflar Ya Eşit Ya Ayrıktır). aH ve bH gibi iki sol kalan sınıfı ya birbirinin aynısıdır ya da tamamen ayrıktır:

$$aH = bH \quad \text{veya} \quad aH \cap bH = \emptyset$$

Aynısı sağ kalan sınıfları için de geçerlidir.

İspat.

Kalan sınıfları bir denklik bağıntısının sınıflarıdır; denklik sınıfları kümeyi ayrık parçalara böler.

■

18.3 Bütün Sınıflar Aynı Kuvvettedir

Teorem 18.4 (Sınıfların Eş Kuvvetliliği). aH ve bH gibi iki sol kalan sınıfı aynı kuvvettedir (aralarında birebir ve üzerine bir eşleme vardır); aynısı sağ kalan sınıfları için de geçerlidir.

İspat.

Önce her sınıfın H ile eş kuvvette olduğunu görelim:

$$\varphi_a : H \rightarrow aH, \quad h \mapsto ah$$

İyi tanımlıdır: $h_1 = h_2 \Rightarrow ah_1 = ah_2$. Üzerinedir: aH 'nin tipik elemanı zaten ah biçimindedir. Birebirdir: $ah_1 = ah_2$ ise grupta sadeleştirmeyle $h_1 = h_2$.

O hâlde H ile aH eş kuvvettedir ve $\varphi_a^{-1} : aH \rightarrow H, ah \mapsto h$ de birebir-üzerinedir. İki sınıf için

$$\varphi_b \circ \varphi_a^{-1} : aH \rightarrow bH, \quad ah \mapsto bh$$

bileşkesi, birebir-üzerine iki fonksiyonun bileşkesi olarak birebir ve üzerinedir: aH ile bH eş kuvvettedir.

■

Sonuç 18.2 (Sonlu Durumda Eleman Sayısı). $|H| = n$ ise her aH sol kalan sınıfının ve her Ha sağ kalan sınıfının eleman sayısı da n 'dir.

18.4 Somut Bir Bölmeleme

Örnek 18.1 (S_3 'ün $\{I, (1\ 2)\}$ 'ye Göre Sınıfları). S_3 'ün $H = \{I, (1\ 2)\}$ alt grubuna göre sol ve sağ kalan sınıflarını bulunuz.

Çözüm.

Sol sınıflar. H 'nin kendisi bir sınıftır. H 'de olmayan $(1\ 3)$ ile

$$(1\ 3)H = \{(1\ 3), (1\ 3)(1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\}$$

$((1\ 3)(1\ 2))$: önce $(1\ 2)$, sonra $(1\ 3)$ uygulanır $- 1 \mapsto 2, 2 \mapsto 1 \mapsto 3, 3 \mapsto 1$; sonuç $(1\ 2\ 3)$.) Henüz sınıfı çıkmamış $(2\ 3)$ ile

$$(23)H = \{(23), (23)(12)\} = \{(23), (132)\}$$

Altı eleman üçe bölündü:

$$S_3 = H \cup (13)H \cup (23)H$$

Sağ sınıflar. Aynı temsilcilerle

$$H(13) = \{(13), (12)(13)\} = \{(13), (132)\}$$

$$H(23) = \{(23), (12)(23)\} = \{(23), (123)\}$$

$$S_3 = H \cup H(13) \cup H(23)$$

Dikkat: $(13)H \neq H(13)$ 'tür — sol ve sağ bölmelemeler *farklı* parçalamalardır. (Sınıf sayıları yine de eşit çıktı; bunun bir rastlantı olmadığını bir sonraki bölümde göreceğiz.)

■

Elimizde artık kusursuz bir dilimleme var: G , her biri $|H|$ elemanlı, ikişer ikişer ayrık sınıfların birleşimidir. Sonlu gruplar için bunun tek satırlık ama çığır açıcı bir sonucu vardır: [Lagrange teoremi](#).

19. Lagrange Teoremi

Sonlu grup teorisinin ilk büyük teoremine geldik. Kalan sınıfları G 'yi eşit boyutlu ayırık parçalara böldüğüne göre, G 'nin mertebesi parça boyutunun tam katı olmalıdır: **alt grubun mertebesi, grubun mertebesini böler**. Bu tek cümle, sonlu grupların iskeletini belirler — hangi mertebeden alt grup ya da eleman *olamayacağını* hesap yapmadan söyler. Bölümün sonunda teoremin dört klasik sonucunu çıkarıyoruz; asal mertebeli grupların tam sınıflandırması bunlardan biridir.

19.1 Teorem ve İspatı

Teorem 19.1 (Lagrange Teoremi). Sonlu bir G grubunun her H alt grubunun mertebesi, G 'nin mertebesini böler:

$$|H| \mid |G|$$

İspat.

$|G| = N$ ve $|H| = n$ olsun. G sonlu olduğundan H 'ye göre birbirinden farklı sol kalan sınıflarının sayısı da sonludur; bu sayıya j diyelim ve her sınıftan birer temsilci $a_1, a_2, \dots, a_j$ seçelim. Her eleman bir sınıfta bulunduğu ve farklı sınıflar ayırık olduğundan

$$G = a_1H \cup a_2H \cup \dots \cup a_jH, \quad a_{i_1}H \cap a_{i_2}H = \emptyset \ (i_1 \neq i_2)$$

Ayrık birleşimin eleman sayısı, parçaların eleman sayılarının toplamıdır; her sınıf $|H| = n$ elemanlı olduğundan

$$N = \underbrace{n + n + \dots + n}_{j \text{ tane}} = j \cdot n$$

O hâlde $n \mid N$ 'dir.

■

19.2 İndeks

İspattaki j sayısı kendi başına önemlidir:

Teorem 19.2 (Sol ve Sağ Sınıf Sayıları Eşittir). Sonlu G grubunun H 'ye göre birbirinden farklı sol kalan sınıflarının sayısı, birbirinden farklı sağ kalan sınıflarının sayısına eşittir.

İspat.

Lagrange ispatındaki sayma soldan $N = jn$ verdi; aynı sayma sağ sınıflarla yapılırsa $N = j'n$ bulunur. İkisinden $j = j' = N/n$ çıkar.

■

Tanım 19.1 (İndeks). G 'nin H 'ye göre birbirinden farklı sol (eşdeğer olarak sağ) kalan sınıflarının sayısına H 'nin G içindeki indeksi denir ve $[G : H]$ ile gösterilir. Sonlu grupta

$$|G| = [G : H] \cdot |H|, \quad [G : H] = \frac{|G|}{|H|}$$

Ayrıca bölmelemedeki temsilcilerden biri her zaman 1_G seçilebilir: $G = H \cup a_2H \cup \dots \cup a_jH$.

Örnek 19.1 (\$S_3\$'te İndeks). Önceki bölümde S_3 'ü $H = \{I, (1\ 2)\}$ 'ye göre bölmelemiştik: üç sol sınıf, üç sağ sınıf. Gerçekten

$$[S_3 : H] = \frac{|S_3|}{|H|} = \frac{6}{2} = 3$$

19.3 Lagrange Teoreminin Sonuçları

Sonuç 19.1 (Eleman Mertebesi Grup Mertebesini Böler). Sonlu bir G grubunun her a elemanının mertebesi, G 'nin mertebesini böler.

İspat.

$|a| = n$ olsun. Eleman mertebesi tanımı gereği $|\langle a \rangle| = n$ 'dir ve $\langle a \rangle \subseteq G$ 'dir; Lagrange teoreminden $n \mid |G|$.

■

Sonuç 19.2 ($a^{|G|} = 1_G$). G sonlu bir grup ve $|G| = N$ ise her $a \in G$ için $a^N = 1_G$ 'dir.

İspat.

$|a| = n$ diyelim; önceki sonuçtan $n \mid N$, yani $N = nt$ olacak bir $t \in \mathbb{N}$ vardır. $a^n = 1_G$ olduğundan

$$a^N = a^{nt} = (a^n)^t = 1_G^t = 1_G$$

■

i Sayılar teorisiyle bağ

$G = \mathbb{Z}_p^*$ (p asal) alınırsa $|G| = p - 1$ ve son sonuç, sayılar teorisinden tanıdık **Fermat'nın küçük teoremi** olur: $p \nmid a$ için $a^{p-1} \equiv 1 \pmod{p}$. Grup teorisi, bu teoremi tek satırlık bir özel duruma indirger.

Sonuç 19.3 (Asal Mertebeli Gruplar Devreseldir). Mertebesi asal olan her grup devreseldir.

İspat.

$|G| = p$ asal ve $a \in G - \{1_G\}$ olsun. $|a|$, p 'yi böler: $|a| = 1$ veya $|a| = p$. $a \neq 1_G$ olduğundan $|a| \neq 1$ 'dir; o hâlde $|a| = p$ ve

$$\langle a \rangle \subseteq G, \quad |\langle a \rangle| = p = |G| \implies G = \langle a \rangle = \{1_G, a, a^2, \dots, a^{p-1}\}$$

G devreseldir; üstelik birimden farklı her elemanı bir doğuraydır.

■

Bu sonuç, küçük mertebeli grupların sınıflandırmasındaki gözlemlerimizi açıklar ve genişletir: mertebesi 2, 3, 5, 7, ... olan gruplar zorunlu olarak devreseldir – mertebe 4'te iki tip çıkmasının nedeni, 4'ün asal olmamasıdır.

19.4 Bir Uygulama: Tersinin Doğru Olmadığı

Örnek 19.2 (Alt Grupları Devresel Olan Grup Devresel Olmayabilir). “Devresel grubun her alt grubu devreseldir” teoreminin tersi doğru mudur? Yani kendisinden farklı bütün alt grupları devresel olan bir grup devresel olmak zorunda mıdır?

Çözüm.

Hayır. S_3 bir karşı örnektir. $H \subseteq_{\text{a.g.}} S_3$ ve $H \neq S_3$ olsun. Lagrange teoreminden $|H| \in \{1, 2, 3\}$ 'tür:

- $|H| = 1$ ise $H = \{I\} = \langle I \rangle$ devreseldir.
- $|H| = 2$ veya 3 ise mertebe asaldır; asal mertebeli her grup devreseldir.

Demek ki S_3 'ün kendisinden farklı her alt grubu devreseldir. Ama S_3 devresel değildir: devresel gruplar komutatiftir, oysa

$$(1\ 2)(1\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 3)(1\ 2)$$

■

Lagrange teoremi “alt grup mertebesi böler” der; ama *tersini söylemez*: $|G|$ 'nin her böleni için o mertebeden bir alt grup bulunacağını garantiyi yoktur. (Devresel gruplarda bu garanti vardı; genel gruplarda örneğin A_4 'ün mertebesi 12 olduğu hâlde 6. mertebeden alt grubu yoktur.)

Kalan sınıflarının hikâyesi burada bitmiyor. S_3 örneğinde sol ve sağ bölmelemelerin *farklı* çıktığını gördük; bazı alt gruplar içinse ikisi çakışır. Bu özel alt gruplar — normal alt gruplar — kalan sınıflarının kendilerinin bir grup oluşturmalarına izin verir ve bizi bölüm gruplarına götürür: [normal alt gruplar](#).

20. Normal Alt Gruplar

Sol ve sağ kalan sınıflarının çakıştığı alt gruplar, grup teorisinde ayrıcalıklı bir role sahiptir: yalnız onların kalan sınıfları üzerinde tutarlı bir çarpma tanımlanabilir. Bu bölümde normal alt grubu tanımlıyor, en kullanışlı normallik ölçütünü — indeksin 2 olmasını — kanıtlıyor ve iki uyarı örneği veriyoruz: normal olmayan alt gruplar gerçekten vardır ve normallik zincirleme aktarılmaz.

20.1 Tanım

Tanım 20.1 (Normal Alt Grup). $\langle G, \cdot \rangle$ bir grup ve H, G 'nin bir alt grubu olsun. Her $a \in G$ için

$$aH = Ha$$

oluyorsa H 'ye G 'nin bir **normal alt grubu** denir ve $H \trianglelefteq G$ ile gösterilir.

⚠ $aH = Ha$ ne demek değildir

$aH = Ha$ eşitliği, her $h \in H$ için $ah = ha$ olması demek **değildir**; iki kümenin çakışması demektir. Yani her $h \in H$ 'ye karşılık $ah = h'a$ olacak biçimde bir $h' \in H$ vardır — ama h', h 'den farklı olabilir. Normallik, eleman eleman değişmeden çok daha zayıf bir koşuldur.

Örnek 20.1 (Trivial Alt Gruplar Normaldir). Her G grubunda iki trivial alt grup da normaldir:

- $G \trianglelefteq G$: her a için $aG = G = Ga$ 'dır ($aG = G$ eşitliği için: kapalılıktan $aG \subseteq G$; tersine her $g \in G, g = a(a^{-1}g) \in aG$ yazılır).
- $\{1_G\} \trianglelefteq G$: her a için $a\{1_G\} = \{a\} = \{1_G\}a$ 'dır.

Örnek 20.2 (Normal Olmayan Bir Alt Grup). S_3 'ün $H = \{I, (2\ 3)\}$ alt grubu normal değildir: $(1\ 2) \in S_3$ için

$$(1\ 2)H = \{(1\ 2), (1\ 2)(2\ 3)\} = \{(1\ 2), (1\ 2\ 3)\}$$

$$H(1\ 2) = \{(1\ 2), (2\ 3)(1\ 2)\} = \{(1\ 2), (1\ 3\ 2)\}$$

$(1\ 2)H \neq H(1\ 2)$ olduğundan $H \not\trianglelefteq S_3$ 'tür. (Aynı biçimde $\{I, (1\ 2)\}$ ve $\{I, (1\ 3)\}$ de normal değildir.)

Komutatif gruplarda bu sorunu hiç doğmaz: $aH = \{ah\} = \{ha\} = Ha$ her zaman sağlanır. **Komutatif bir grubun her alt grubu normaldir.**

20.2 İndeks 2 Ölçütü

Teorem 20.1 (İndeksi 2 Olan Alt Gruplar Normaldir). Bir grupta indeksi 2 olan her alt grup normaldir.

İspat.

$H \subseteq G$ ve $[G : H] = 2$ olsun.

a.g.
 $a \in G - H$ alalım. Sol bölmelemede yalnız iki sınıf vardır ve biri H 'dir; $a \notin H$ olduğundan ikinci sınıf aH 'dir ve

$$G = H \cup aH, \quad H \cap aH = \emptyset \implies aH = G - H$$

Aynı akıl yürütme sağ bölmeleme için $Ha = G - H$ verir. O hâlde

$$aH = G - H = Ha \quad (a \in G - H)$$

$a \in H$ için ise $aH = H = Ha$ zaten sağlanır. Her iki durumda da $aH = Ha$ olduğundan $H \trianglelefteq G$ 'dir.

■

Sonuç 20.1 (S_n lt.tri.eq S_n). *Alterne grup, simetrik grubun normal alt grubudur.*

İspat.

$$[S_n : A_n] = \frac{|S_n|}{|A_n|} = \frac{n!}{n!/2} = 2$$

olduğundan indeks 2 ölçütü uygulanır.

■

20.3 Normallik Geçişken Değildir

Normallikğin iki incelikli davranışını kaydedelim. Birincisi zararsızdır:

Örnek 20.3 (Normallik Ara Alt Gruba İner). $K \subseteq H \subseteq G$ ve $K \trianglelefteq G$ ise $K \trianglelefteq H$ 'dir.

Çözüm.

$K \trianglelefteq G$ olduğundan her $a \in G$ için $aK = Ka$ 'dır; özel olarak her $a \in H \subseteq G$ için de $aK = Ka$ sağlanır. K, H 'nin alt grubu olduğundan $K \trianglelefteq H$ çıkar.

■

İkincisi bir tuzaktır: $K \trianglelefteq H$ ve $H \trianglelefteq G$ olsa bile $K \trianglelefteq G$ gerekmez.

Örnek 20.4 (Normallik Zincirleme Aktarılmaz). S_4 içinde şu üç kümeye bakalım:

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

$$H = \{I, (13), (24), (13)(24)\}, \quad K = \{I, (13)\}$$

G, S_4 'ün 8 elemanlı bir alt grubudur (bir karenin simetri grubu) ve $K \subseteq H \subseteq G$ 'dir. $K \trianglelefteq H$ olduğu hâlde $K \not\trianglelefteq G$ olduğunu gösteriniz.

Çözüm.

$[H : K] = \frac{|H|}{|K|} = \frac{4}{2} = 2$ olduğundan indeks 2 ölçütüyle $K \trianglelefteq H$ 'dir.

Öte yandan $(12)(34) \in G$ için sol ve sağ sınıfları karşılaştıralım:

$$(12)(34)K = \{(12)(34), (12)(34)(13)\} = \{(12)(34), (1432)\}$$

$$K(12)(34) = \{(12)(34), (13)(12)(34)\} = \{(12)(34), (1234)\}$$

(Birinci çarpımda önce (13) , sonra $(12)(34)$ uygulanır: $1 \mapsto 3 \mapsto 4, 4 \mapsto 4 \mapsto 3, 3 \mapsto 1 \mapsto 2, 2 \mapsto 2 \mapsto 1$; sonuç (1432) . İkincisinde önce $(12)(34)$: $1 \mapsto 2 \mapsto 2, 2 \mapsto 1 \mapsto 3, 3 \mapsto 4 \mapsto 4, 4 \mapsto 3 \mapsto 1$; sonuç (1234) .)

İki küme farklı olduğundan K, G 'nin normal alt grubu **değildir**: normallik geçişken değildir.

■

20.4 Basit Gruplar

Tanım 20.2 (Basit Grup). Trivial alt gruplarından başka hiçbir **normal** alt grubu bulunmayan gruba **basit grup** denir.

Örnek 20.5 (Asal Mertebeli Gruplar Basittir). Mertebesi asal olan her grup basittir: $|G| = p$ asalsa Lagrange teoreminden her alt grubun mertebesi 1 veya p 'dir; yani G 'nin trivial olanlardan başka alt grubu — normal olsun olmasın — yoktur.

Basit gruplar, sonlu grup teorisinin “asal sayılarıdır”: her sonlu grup, basit gruplardan katmanlar hâlinde kurulur. Bu katmanların harcını da tam olarak normal alt gruplar sağlar — bir normal alt grup, kalan sınıflarından yeni ve daha küçük bir grup üretmeye izin verir. Bu inşa, dersin dönüm noktalarından biridir: [bölüm grupları](#).

21. Bölüm Grupları

Normal alt grubun asıl ödülü bu bölümdedir: $H \trianglelefteq G$ ise kalan sınıflarının kümesi üzerinde $aH \cdot bH = (ab)H$ kuralıyla bir çarpma tanımlanabilir ve sınıflar bu çarpmayla *yeni bir grup* oluşturur — bölüm grubu G/H . İnşanın kalbi bir iyi tanımlılık meselesidir: çarpım, sınıflardan seçilen temsilcilere bağlı kalmamalıdır; bunu garanti eden şey tam olarak normalliktir.

21.1 Çarpma Sınıflara İner

Teorem 21.1 (Eşdeğerlik Çarpmayla Uyumludur). $\langle G, \cdot \rangle$ bir grup ve $H \trianglelefteq G$ olsun. $x, x', y, y' \in G$ olmak üzere

$$x \sim_{\text{sol}} x' (H), \quad y \sim_{\text{sol}} y' (H) \implies x \cdot y \sim_{\text{sol}} x' \cdot y' (H)$$

İspat.

$x \sim x'$ demek, ikisinin aynı aH sınıfında olması demektir: $x = ah_1, x' = ah_2$ olacak biçimde $h_1, h_2 \in H$ vardır. Benzer biçimde $y = bh_3, y' = bh_4$ olacak biçimde bir bH sınıfı ve $h_3, h_4 \in H$ vardır. Çarpımları yazalım:

$$xy = (ah_1)(bh_3) = a(h_1b)h_3, \quad x'y' = (ah_2)(bh_4) = a(h_2b)h_4$$

H normal olduğundan $bH = Hb$ 'dir; yani $h_1b = bh'_1$ ve $h_2b = bh'_2$ olacak biçimde $h'_1, h'_2 \in H$ vardır. Yerine koyalım:

$$xy = a(bh'_1)h_3 = (ab)(h'_1h_3) \in (ab)H$$

$$x'y' = a(bh'_2)h_4 = (ab)(h'_2h_4) \in (ab)H$$

xy ile $x'y'$ aynı $(ab)H$ sol kalan sınıfına düştüğünden $xy \sim x'y'$ olur.

■

(Sağdan eşdeğerlik için aynı sonuç tamamen benzer biçimde kanıtlanır. Ayrıca $H \trianglelefteq G$ iken her a için $aH = Ha$ olduğundan soldan ve sağdan eşdeğerlik bağıntıları G 'yi aynı sınıflara ayırır: iki bağıntı birbiriyle çakışır ve “sol/sağ” ayrımı ortadan kalkar — kısaca *kalan sınıflarından* söz edebiliriz.)

21.2 Bölüm Grubunun İnşası

Teorem 21.2 (Kalan Sınıfları Grubu). $\langle G, \cdot \rangle$ bir grup ve $H \trianglelefteq G$ olsun. Kalan sınıflarının kümesi

$$\bar{G} = \{aH : a \in G\}$$

üzerinde

$$aH \circ bH = (a \cdot b)H$$

işlemi tanımlanabilir ve $\langle \bar{G}, \circ \rangle$ bir gruptur.

İspat.

İşlemin iyi tanımlı olduğu — yani sonucun temsilci seçimine bağlı olmadığı — bir önceki teoremin içerdiği: $aH = a'H$ ve $bH = b'H$ ise $a \sim a', b \sim b'$ olur; uyum teoremi $ab \sim a'b'$, yani $(ab)H = (a'b')H$ verir.

$1_G H = H \in \bar{G}$ olduğundan $\bar{G} \neq \emptyset$ 'dir. Aksiyomları denetleyelim.

Kapalılık. $a, b \in G$ için $ab \in G$ olduğundan $aH \circ bH = (ab)H \in \bar{G}$ 'dir.

Asosyatiflik. G 'deki asosyatiflikten

$$(aH \circ bH) \circ cH = ((ab)c)H = (a(bc))H = aH \circ (bH \circ cH)$$

Birim eleman. $H = 1_G H$ sınıfı birimdir:

$$1_G H \circ aH = (1_G \cdot a)H = aH, \quad aH \circ 1_G H = aH$$

Ters eleman. aH 'nin tersi $a^{-1}H$ 'dir:

$$a^{-1}H \circ aH = (a^{-1}a)H = 1_G H = H, \quad aH \circ a^{-1}H = H$$

Dört aksiyom sağlandığından $\langle \bar{G}, \circ \rangle$ bir gruptur.

■

Tanım 21.1 (Bölüm Grubu). $\langle \bar{G}, \circ \rangle$ grubuna G 'nin H normal alt grubuna göre bölüm grubu denir ve G/H ile gösterilir.

Teorem 21.3 (Sınıf Çarpımı, Kompleks Çarpımıdır). $H \trianglelefteq G$ iken $aH \circ bH$ çarpımı, aH ile bH komplekslerinin kompleks çarpımı anlamındaki $aH \cdot bH$ ile aynıdır.

İspat.

Kompleks çarpımının asosyatifliği, normallik ($Hb = bH$) ve $H \cdot H = H$ eşitliğiyle

$$aH \cdot bH = a(Hb)H = a(bH)H = (ab)(H \cdot H) = (ab)H$$

■

Bu uyum sayesinde $\circ$ işareti için ayrı bir sembol taşımaya gerek kalmaz; bundan böyle bölüm grubunda da çarpımı $\cdot$ ile (ya da yan yana yazarak) göstereceğiz.

21.3 Sonlu Durum ve Komutatif Durum

Üç pratik not:

1. **Mertebe.** G sonlu ve $H \trianglelefteq G$ ise bölüm grubunun mertebesi indekstir:

$$|G/H| = [G : H] = \frac{|G|}{|H|}$$

2. **Komutatif grupta her alt grup bölüm grubu verir.** Komutatif grubun her alt grubu normal olduğundan her H alt grubuna göre G/H kurulabilir; üstelik G/H de komutatifdir:

$$aH \cdot bH = (ab)H = (ba)H = bH \cdot aH$$

3. **Toplamsal yazış.** $\langle G, + \rangle$ komutatif grubunda kalan sınıfları $a + H = \{a + h : h \in H\}$ biçimini alır ve

$$G/H = \{a + H : a \in G\}, \quad (a + H) + (b + H) = (a + b) + H$$

toplamasıyla bir toplamsal gruptur.

Örnek 21.1 (En Tanıdık Bölüm Grubu: $\mathbb{Z}/m\mathbb{Z}$). $\langle \mathbb{Z}, + \rangle$ grubunda $H = m\mathbb{Z} = \{0, \mp m, \mp 2m, \dots\}$ alt grubunu alalım ($m \geq 2$). Grup komutatif olduğundan H normaldir ve kalan sınıfları tam olarak modüler aritmetiğin sınıflarıdır:

$$k + m\mathbb{Z} = \bar{k}, \quad \mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$$

Sınıflar üzerindeki toplama ($\bar{a} + \bar{b} = \overline{a+b}$), bölüm grubu toplamasının kendisidir: $\langle \mathbb{Z}_m, + \rangle$, ilk günden beri kullandığımız yapı, aslında bir bölüm grubudur — $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$.

Bölüm grubu inşası soyut görünebilir; gücünü örneklerde gösterir. Bir sonraki bölüm baştan sona örneklerle ayrılmıştır: S_3/A_3 'ten kompleks sayı gruplarına, alt grup çarpımlarının normallüğinden $\mathbb{Z}_{15}$ 'in çarpımsal yapısına — [bölüm grubu örnekleri](#).

22. Bölüm Grubu Örnekleri

Bölüm grubu makinesi kuruldu; şimdi onu çalıştırıyoruz. Bu bölümde önce normal alt gruplarla ilgili iki yapısal sonuç kanıtıyoruz — $N \trianglelefteq G$ iken NH çarpımının alt grup, iki normal alt grubun çarpımının normal alt grup olması — sonra üç somut bölüm grubunu elemanlarına kadar hesaplıyoruz: $S_3/A_3, \mathbb{Z}_{15}$ 'in çarpımsal grubunun bir bölümü ve dördüncü birim köklerinin $\{1, -1\}$ 'e göre bölümü.

22.1 Yapısal Örnekler

Örnek 22.1 (\$N\$ It.tri.eq \$G\$ İse \$NH\$ Alt Gruptur). $\langle G, \cdot \rangle$ bir grup, $N \trianglelefteq G$ ve $H \subseteq G$ olsun. NH kompleksinin G 'nin bir alt grubu olduğunu gösteriniz. a.g.

Çözüm.

$NH = \{nh : n \in N, h \in H\} \subseteq G$ ve $1_G = 1_G \cdot 1_G \in NH$ olduğundan küme boş değildir. İki koşullu ölçütü denetleyelim.

Kapalılık. $n_1h_1, n_2h_2 \in NH$ olsun:

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2)h_2$$

N normal olduğundan $h_1N = Nh_1$ 'dir; yani $h_1n_2 = n_2'h_1$ olacak biçimde bir $n_2' \in N$ vardır. Yerine koyunca

$$(n_1h_1)(n_2h_2) = n_1(n_2'h_1)h_2 = (n_1n_2')(h_1h_2) \in NH$$

çünkü $n_1n_2' \in N$ ve $h_1h_2 \in H$ 'dir.

Terslere kapalılık. $(nh)^{-1} = h^{-1}n^{-1}$ 'dir. N normal olduğundan $h^{-1}N = Nh^{-1}$, yani $h^{-1}n^{-1} = t h^{-1}$ olacak biçimde bir $t \in N$ vardır:

$$(nh)^{-1} = t h^{-1} \in NH$$

İki koşul sağlandığından $NH \subseteq G$ 'dir. a.g.

■

Bu, komplekslerle hesap bölümündeki $HK = KH$ ölçütünün iş başındaki hâlidir: normallik, $NH = HN$ eşitliğini garanti eder.

Örnek 22.2 (İki Normal Alt Grubun Çarpımı Normaldir). $\langle G, \cdot \rangle$ bir grup, $N \trianglelefteq G$ ve $H \trianglelefteq G$ olsun. $NH \trianglelefteq G$ olduğunu gösteriniz.

Çözüm.

Önceki örnekten NH bir alt gruptur. Normalliği kompleks hesabıyla görelim: herhangi $a \in G$ için

$$a(NH) = (aN)H = (Na)H = N(aH) = N(Ha) = (NH)a$$

Birinci ve dördüncü adımda kompleks çarpımının asosyatifliği, ikinci adımda $N \trianglelefteq G$, dördüncü adımda $H \trianglelefteq G$ kullanıldı. Her a için $a(NH) = (NH)a$ olduğundan $NH \trianglelefteq G$ 'dir.

■

22.2 S_3/A_3 : İlk Somut Bölüm Grubu

Örnek 22.3 (\$S_3\$'ün \$A_3\$'e Göre Bölüm Grubu). S_3 'ün A_3 alt grubuna göre bölüm grubunu oluşturunuz.

Çözüm.

$A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$, üçüncü mertebeden devresel bir gruptur: $A_3 = \langle (1\ 2\ 3) \rangle = \langle (1\ 3\ 2) \rangle$.

$$[S_3 : A_3] = \frac{6}{3} = 2$$

olduğundan indeks 2 ölçütüyle $A_3 \trianglelefteq S_3$ tür ve bölüm grubu iki elemanlıdır. Sınıfları yazalım:

$$A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$$

$$(2\ 3)A_3 = \{(2\ 3), (2\ 3)(1\ 2\ 3), (2\ 3)(1\ 3\ 2)\} = \{(2\ 3), (1\ 3), (1\ 2)\}$$

Yani sınıflardan biri çift substitüsyonlar, öbürü tek substitüsyonlardır:

$$S_3 = A_3 \cup (2\ 3)A_3, \quad S_3/A_3 = \{A_3, (2\ 3)A_3\}$$

İkinci mertebeden bu grup, “çift · çift = çift, tek · tek = çift, tek · çift = tek” kurallarının grup hâline getirilmiştir.

■

22.3 Komutatif Örnekler

Örnek 22.4 (\$\mathbb{Z}_{15}\$'in Çarpımsal Grubunda Bölüm). $\mathbb{Z}_{15}$ 'te, 15 ile aralarında asal kalan sınıflarının kümesi

$$A = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\} = \{\mp\bar{1}, \mp\bar{2}, \mp\bar{4}, \mp\bar{7}\}$$

çarpma işlemine göre komutatif bir gruptur. $H = \{\bar{1}, \bar{4}\}$ kümesinin $\langle A, \cdot \rangle$ 'nin bir alt grubu olduğunu görüp A/H bölüm grubunu oluşturunuz.

Çözüm.

$\bar{4} \cdot \bar{4} = \bar{16} = \bar{1}$ olduğundan H çarpmaya kapalıdır; A sonlu grup olduğundan kapalılık, alt grup olmaya yeter: $H \subseteq A$. A komutatif olduğundan $H \trianglelefteq A$ 'dır ve bölüm grubu kurulabilir:

a.g.

$$[A : H] = \frac{|A|}{|H|} = \frac{8}{2} = 4$$

Dört kalan sınıfını temsilcileriyle yazalım:

$$H = \{\bar{1}, \bar{4}\}, \quad -H = \{-\bar{1}, -\bar{4}\}$$

$$\bar{2}H = \{\bar{2}, \bar{8}\} = \{\bar{2}, -\bar{7}\}, \quad -\bar{2}H = \{-\bar{2}, \bar{7}\}$$

O hâlde

$$A/H = \{H, -H, \bar{2}H, -\bar{2}H\}$$

dördüncü mertebeden bir gruptur. Tipini de belirleyebiliriz: $(\bar{2}H)^2 = \bar{4}H = H$, $(-H)^2 = H$, $(-\bar{2}H)^2 = \bar{4}H = H$ — birimden farklı her elemanın karesi birimdir; A/H , Klein tipindedir.

■

Örnek 22.5 (Dördüncü Birim Köklerinde Bölüm). $G = \{1, -1, i, -i\}$ kümesi $\mathbb{C}$ 'deki çarpma işlemine göre bir gruptur.

a) G 'nin devresel olduğunu gösteriniz.

b) $H = \{1, -1\}$ alt grubuna göre G/H bölüm grubunu oluşturunuz.

Çözüm.

a) i 'nin kuvvetlerini yazalım:

$$i^1 = i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = 1$$

Dört kuvvet grubun dört elemanını verdi: $G = \langle i \rangle$, dördüncü mertebeden devresel gruptur. (Kapalılık, asosyatiflik, birim ve tersler $\mathbb{C}^*$ 'dan miras kalır; $G, \mathbb{C}^*$ 'ın sonlu ve çarpmaya kapalı bir alt kümesi olarak alt gruptur.)

b) $H = \{1, -1\}$, çarpmaya kapalı ve sonludur: $H \subseteq G$. G komutatif olduğundan $H \trianglelefteq G$ dir: a.g.

$$|G/H| = [G : H] = \frac{4}{2} = 2$$

Sınıflar:

$$H = \{1, -1\}, \quad iH = \{i, -i\}, \quad G = H \cup iH$$

$$G/H = \{H, iH\}$$

İkinci mertebeden gruptur; $iH \cdot iH = i^2H = -H = H$ eşitliği tabloyu tamamlar.

■

22.4 Alıştırma

Alıştırma 22.1 (Normallik Denetimi). $H = \{I, (1\ 2)\}$ kümesi S_3 'ün bir normal alt grubu mudur?

Çözüm.

H , çarpmaya kapalı ($((1\ 2))^2 = I$) ve sonlu olduğundan S_3 'ün bir alt grubudur. Normallik için bir eleman deneyelim: $(2\ 3) \in S_3$ için

$$(2\ 3)H = \{(2\ 3), (2\ 3)(1\ 2)\} = \{(2\ 3), (1\ 3\ 2)\}$$

$$H(2\ 3) = \{(2\ 3), (1\ 2)(2\ 3)\} = \{(2\ 3), (1\ 2\ 3)\}$$

$(2\ 3)H \neq H(2\ 3)$ olduğundan H , S_3 'ün normal alt grubu **değildir**; S_3/H diye bir bölüm grubu kurulamaz.

■

Bölüm grubu, büyük bir gruptan sistematik biçimde küçük gruplar üretiyor. Ama bu üretimin doğal dili henüz eksik: iki grup arasında “yapıyı koruyan fonksiyon” kavramı. Bölüm grubunun gerçek anlamı — büyük grubun *homomorf resmi* olması — ancak o dille söylenebilir: **homomorfi** ve **izomorfi**.

23. Homomorfi ve İzomorfi

Cebirsel yapılar arasında önemli olan fonksiyonlar, işlemi işleme taşıyanlardır: $\varphi(a \circ b) = \varphi(a) * \varphi(b)$. Böyle bir fonksiyon iki yapının cebirini birbirine bağlar; birebirse iki yapı cebirsel bakımdan *aynıdır* – yalnız elemanlarının adları değişmiştir. Bu bölümde homomorfi, izomorfi ve otomorfi kavramlarını tanımlıyor, klasik logaritma örneğini işliyor ve ilk yapısal teoremleri kanıtlıyoruz: grup olma özelliği ve alt grup olma özelliği, üzerine homomorfilerle resme taşınır.

23.1 Tanımlar

Tanım 23.1 (Homomorfi). $\langle M, \circ \rangle$ ve $\langle M', * \rangle$ tek işlemli iki cebirsel yapı olsun. M 'den M' üzerine, işlemi koruyan – yani her $a, b \in M$ için

$$\varphi(a \circ b) = \varphi(a) * \varphi(b)$$

koşulunu sağlayan – bir $\varphi : M \rightarrow M'$ fonksiyonu varsa φ 'ye M 'den M' üzerine bir **homomorfi**, M' 'ye M 'nin bir **homomorf resmi** denir ve “ M , M' 'ye homomorftur” denir. (φ üzerine olduğundan $\varphi(M) = \{\varphi(a) : a \in M\} = M'$ 'dür.)

Tanım 23.2 (İzomorfi). Homomorfi tanımındaki φ üstelik birebir ise φ 'ye M 'den M' üzerine bir **izomorfi**, M' 'ye M 'nin bir **izomorf resmi** denir; bu durum

$$M \cong M'$$

ile gösterilir ve “ M , M' 'ye izomorftur” denir.

Tanım 23.3 (Otomorfi). Bir M cebirsel yapısının kendi üzerine bir izomorfisine M 'nin bir **otomorfi** denir. Örneğin $I_M : M \rightarrow M$, $m \mapsto m$ identik fonksiyonu her yapının bir otomorfisidir (**identik otomorfi**).

İzomorf yapılar, cebirin gözünde ayırt edilemez: birinde geçerli her işlem tablosu, eleman adları φ ile çevrilerek öbürüne taşınır.

Örnek 23.1 (Klasik Örnek: Logaritma). $\varphi : \langle \mathbb{R}^+, \cdot \rangle \rightarrow \langle \mathbb{R}, + \rangle$, $x \mapsto \log x$ fonksiyonunun bir izomorfi olduğunu gösteriniz.

Çözüm.

İki yapı da birer komutatif gruptur. Dört koşulu denetleyelim.

İyi tanımlılık: $x_1 = x_2 \implies \log x_1 = \log x_2$.

Üzerinelik: Her $y \in \mathbb{R}$ için $e^y \in \mathbb{R}^+$ ve

$$\varphi(e^y) = \log e^y = y$$

Birebirlik: $\varphi(x) = \varphi(y)$ ise $\log x = \log y$; üstel fonksiyon uygulanınca

$$e^{\log x} = e^{\log y} \implies x = y$$

İşlemi koruma: Logaritmanın temel özelliğiyle

$$\varphi(x \cdot y) = \log(xy) = \log x + \log y = \varphi(x) + \varphi(y)$$

O hâlde φ bir izomorfidir: $\langle \mathbb{R}^+, \cdot \rangle \cong \langle \mathbb{R}, + \rangle$. (Logaritma cetvellerinin çalışma ilkesi de budur: çarpma sorusu, izomorfiyle toplama sorusuna çevrilir.)

■

23.2 Homomorf Resim Grup Yapısını Taşır

Teorem 23.1 (Grubun Homomorf Resmi Gruptur). G ve G' tek işlemli iki cebirsel yapı ve $\varphi : G \rightarrow G'$ bir üzerine homomorfi olsun. G , içinde tanımlanmış ikili işleme göre bir grup ise G' de kendi işlemine göre bir gruptur.

İspat.

Yazıyı kolaylaştırmak için iki yapının işlemini $\cdot$ ile gösterelim. $1_G \in G$ olduğundan $\varphi(1_G) \in G'$ ve $G' \neq \emptyset$ 'dür.

Kapalılık. G' bir cebirsel yapı olduğundan işlemi kapalıdır (hipotez).

Asosyatiflik. $a', b', c' \in G'$ olsun. φ üzerine olduğundan $\varphi(a) = a'$, $\varphi(b) = b'$, $\varphi(c) = c'$ olacak biçimde $a, b, c \in G$ vardır. G 'de $(ab)c = a(bc)$ olduğundan iki tarafın resmi alınıp homomorfi koşulu iki kez uygulanınca

$$(\varphi(a)\varphi(b))\varphi(c) = \varphi(a)(\varphi(b)\varphi(c)) \implies (a'b')c' = a'(b'c')$$

Birim eleman. $a' \in G'$ ve $\varphi(a) = a'$ olsun. $1_G a = a 1_G = a$ eşitliklerinin resmi:

$$\varphi(1_G) a' = a' \varphi(1_G) = a'$$

a' keyfi olduğundan $\varphi(1_G)$, G' 'nin birim elemanıdır:

$$1_{G'} = \varphi(1_G)$$

Ters eleman. $a' = \varphi(a)$ için $a^{-1}a = aa^{-1} = 1_G$ eşitliklerinin resmi:

$$\varphi(a^{-1}) a' = a' \varphi(a^{-1}) = \varphi(1_G) = 1_{G'}$$

Yani $\varphi(a^{-1})$, a' 'nin tersidir:

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

Dört aksiyom sağlandığından G' bir gruptur. ■

İspat, iki taşınabilir formül bıraktı; sürekli kullanacağız:

$$1_{G'} = \varphi(1_G), \quad (\varphi(a))^{-1} = \varphi(a^{-1})$$

Teorem 23.2 (Alt Grubun Resmi Alt Gruptur). G bir grup, G' tek işlemli bir cebirsel yapı ve $\varphi : G \rightarrow G'$ üzerine bir homomorfi olsun. G 'nin herhangi bir H alt grubunun $\varphi(H) = \{\varphi(h) : h \in H\}$ resmi, G' 'nin bir alt grubudur.

İspat.

Önceki teoremden G' bir gruptur. $1_G \in H$ olduğundan $\varphi(1_G) \in \varphi(H)$: küme boş değildir. İki koşullu ölçütü denetleyelim.

Kapalılık. $a', b' \in \varphi(H)$ olsun: $\varphi(a) = a'$, $\varphi(b) = b'$ olacak biçimde $a, b \in H$ vardır. H alt grup olduğundan $ab \in H$ ve

$$a'b' = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(H)$$

Terslere kapalılık. $a' = \varphi(a) \in \varphi(H)$ ($a \in H$) olsun. $a^{-1} \in H$ ve

$$(a')^{-1} = (\varphi(a))^{-1} = \varphi(a^{-1}) \in \varphi(H)$$

İki koşul sağlandığından $\varphi(H) \subseteq G'$ 'dür.
a.g. ■

23.3 Trivial Bölüm Gruplarının Kimliği

Bölüm grubu inşasının en uç iki örneği, izomorfi diliyle kimliklerine kavuşur.

Örnek 23.2 ($G \vee G \text{ tilde.equiv } 1_G$). G/G bölüm grubu tek elemanlıdır: her a için $aG = G$ olduğundan

$$G/G = \{aG : a \in G\} = \{G\}$$

$\varphi : G/G \rightarrow \{1_G\}$, $G \mapsto 1_G$ fonksiyonu üzerine ve birebirdir; işlemi de korur:

$$\varphi(G \cdot G) = \varphi(G) = 1_G = 1_G \cdot 1_G = \varphi(G) \varphi(G)$$

O hâlde $G/G \cong \{1_G\}$: bütün grubu “bölmek”, birim grubu bırakır.

Örnek 23.3 ($G \vee 1_G \text{ tilde.equiv } G$). $\{1_G\}$ ’ye göre her kalan sınıfı tek elemanlıdır: $a\{1_G\} = \{a\}$. O hâlde

$$G/\{1_G\} = \{\{a\} : a \in G\}$$

$\psi : G/\{1_G\} \rightarrow G$, $\{a\} \mapsto a$ fonksiyonu iyi tanımlı, üzerine ve birebirdir; işlemi korur:

$$\psi(\{a\} \cdot \{b\}) = \psi(\{ab\}) = ab = \psi(\{a\}) \psi(\{b\})$$

O hâlde $G/\{1_G\} \cong G$: birim grupla “bölmek” hiçbir şeyi değiştirmez.

İki uç örnek arasında asıl ilginç olanlar duruyor: G ’nin *özsel* normal alt gruplarına göre bölümleri. Bir sonraki bölümün ana teoremi, bu bölümlerin tam olarak G ’nin homomorf resimleri olduğunu söyleyecek – grup teorisinin en temel köprülerinden biri: [gruplarda homomorfi teoremi](#).

24. Gruplarda Homomorfi Teoremi

Bölüm grupları ile homomorfiler arasındaki köprüye geldik. Bir üzerine homomorfinin birime giden elemanları — çekirdeği — her zaman bir normal alt gruptur; aynı değere giden elemanlar tam olarak çekirdeğin kalan sınıflarını doldurur; ve bölüm grubu, resmin kendisine izomorftur: $G / \text{Ker } \varphi \cong G'$. Tek bir teoremden toplanan bu üç olgu, “bölüm grubu” ile “homomorf resim” kavramlarının aynı şeyin iki dili olduğunu söyler.

24.1 Homomorfi Teoremi

Teorem 24.1 (Gruplarda Homomorfi Teoremi). G bir grup, G' tek işlemli bir cebirsel yapı ve $\varphi : G \rightarrow G'$ üzerine bir homomorfi olsun ($\varphi(G) = G'$; homomorf resim teoreminden G' bir gruptur). Bu takdirde:

1. $N = \{a \in G : \varphi(a) = 1_{G'}\}$ kümesi G 'nin bir **normal** alt grubudur.
2. a', G' 'nin herhangi bir elemanı olmak üzere $M_{a'} = \{b \in G : \varphi(b) = a'\}$ kümesi, N 'nin G içindeki uygun bir kalan sınıfıdır.
3. $G/N \cong G'$.

İspat.

1) $\varphi(1_G) = 1_{G'}$ olduğundan $1_G \in N$: küme boş değildir.

Alt gruptur: $a, b \in N$ için

$$\varphi(ab) = \varphi(a)\varphi(b) = 1_{G'} \cdot 1_{G'} = 1_{G'} \implies ab \in N$$

$$\varphi(a^{-1}) = (\varphi(a))^{-1} = 1_{G'}^{-1} = 1_{G'} \implies a^{-1} \in N$$

İki koşullu ölçütle $N \subseteq G$ 'dir.

Normaldir: $aN = Na$ eşitliği, $aNa^{-1} = N$ eşitliğine denktir; bunu iki kapsamayla görelim. Bir $aca^{-1} \in aNa^{-1}$ alalım ($c \in N$):

$$\varphi(aca^{-1}) = \varphi(a)\varphi(c)\varphi(a^{-1}) = \varphi(a) \cdot 1_{G'} \cdot (\varphi(a))^{-1} = 1_{G'}$$

Yani $aca^{-1} \in N$: $aNa^{-1} \subseteq N$. Bu kapsama her $a \in G$ için geçerli olduğundan a yerine a^{-1} konarak $a^{-1}Na \subseteq N$, yani $N \subseteq aNa^{-1}$ de elde edilir. İki kapsama birlikte $aNa^{-1} = N$, dolayısıyla $aN = Na$ verir: $N \trianglelefteq G$.

2) $a' \in G'$ olsun. φ üzerine olduğundan $\varphi(a) = a'$ olacak bir $a \in G$ vardır; $a \in M_{a'}$, yani $M_{a'} \neq \emptyset$ 'dir.

İddia: $M_{a'} = aN$.

$aN \subseteq M_{a'}$: $c \in N$ için

$$\varphi(ac) = \varphi(a)\varphi(c) = a' \cdot 1_{G'} = a' \implies ac \in M_{a'}$$

$M_{a'} \subseteq aN$: $b \in M_{a'}$ olsun:

$$\varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = (a')^{-1}a' = 1_{G'} \implies a^{-1}b \in N \implies b \in aN$$

O hâlde $M_{a'} = aN$: “ a' değerini alan elemanlar”, N 'nin bir kalan sınıfıdır.

3) $\psi : G/N \rightarrow G'$, $aN \mapsto \varphi(a)$ fonksiyonunu tanımlayalım.

İyi tanımlıdır: $aN = bN$ ise $a^{-1}b \in N$, yani $\varphi(a^{-1}b) = 1_{G'}$; açılırsa $(\varphi(a))^{-1}\varphi(b) = 1_{G'}$, yani $\varphi(a) = \varphi(b)$ ve $\psi(aN) = \psi(bN)$.

Üzerinedir: Her $b' \in G'$ için $\varphi(b) = b'$ olan $b \in G$ vardır ve $\psi(bN) = b'$.

Birebirdir: $\psi(aN) = \psi(bN)$ olsun: $\varphi(a) = \varphi(b)$ 'den

$$\varphi(a^{-1}b) = (\varphi(a))^{-1}\varphi(b) = 1_{G'} \implies a^{-1}b \in N \implies b \in aN$$

$b \in bN$ de olduğundan $aN \cap bN \neq \emptyset$; sınıflar ya eşit ya ayrık olduğundan $aN = bN$ 'dir.

İşlemi korur:

$$\psi(aN \cdot bN) = \psi((ab)N) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aN)\psi(bN)$$

Dört özellik birlikte $G/N \cong G'$ verir.

■

Tanım 24.1 (Çekirdek). Homomorfi teoremindeki N normal alt grubuna φ **homomorfisinin çekirdeği** denir ve $\text{Ker } \varphi$ ile gösterilir:

$$\text{Ker } \varphi = \{a \in G : \varphi(a) = 1_{G'}\}$$

Teoremin özeti tek satıra sığar:

$$G / \text{Ker } \varphi \cong \varphi(G)$$

24.2 Çekirdek Hesapları

Örnek 24.1 (Mutlak Değer Homomorfisi). $\varphi : \langle \mathbb{R} - \{0\}, \cdot \rangle \rightarrow \langle \mathbb{R}^+, \cdot \rangle$, $\alpha \mapsto |\alpha|$ fonksiyonunun üzerine bir homomorfi olduğunu gösterip çekirdeğini bulunuz.

Çözüm.

İyi tanımlılık: $\alpha = \beta \implies |\alpha| = |\beta|$.

Üzerinelik: $y \in \mathbb{R}^+$ için $\varphi(y) = |y| = y$.

İşlemi koruma: Mutlak değer çarpımsaldır:

$$\varphi(\alpha\beta) = |\alpha\beta| = |\alpha| |\beta| = \varphi(\alpha)\varphi(\beta)$$

O hâlde φ üzerine bir homomorfidir. $\langle \mathbb{R}^+, \cdot \rangle$ 'nin birimi 1 olduğundan

$$\text{Ker } \varphi = \{\alpha \in \mathbb{R} - \{0\} : |\alpha| = 1\} = \{-1, 1\}$$

Homomorfi teoremi ayrıca $\langle \mathbb{R} - \{0\}, \cdot \rangle / \{-1, 1\} \cong \langle \mathbb{R}^+, \cdot \rangle$ der: her pozitif sayı, $\{\alpha, -\alpha\}$ biçimindeki bir kalan sınıfının etiketi gibidir.

■

Örnek 24.2 (Ters Alma Otomorfisi). $\varphi : \langle \mathbb{R} - \{0\}, \cdot \rangle \rightarrow \langle \mathbb{R} - \{0\}, \cdot \rangle$, $\alpha \mapsto \frac{1}{\alpha}$ fonksiyonunun bir otomorfi olduğunu gösterip çekirdeğini bulunuz.

Çözüm.

İyi tanımlılık: $\alpha = \beta \implies \frac{1}{\alpha} = \frac{1}{\beta}$.

Üzerinelik: $y \neq 0$ için $\frac{1}{\frac{1}{y}} \neq 0$ ve $\varphi\left(\frac{1}{y}\right) = y$.

Birebirlik: $\alpha \neq \beta \implies \frac{1}{\alpha} \neq \frac{1}{\beta}$.

İşlemi koruma:

$$\varphi(\alpha\beta) = \frac{1}{\alpha\beta} = \frac{1}{\alpha} \cdot \frac{1}{\beta} = \varphi(\alpha)\varphi(\beta)$$

Kendi üzerine izomorfi, yani otomorfidir. Çekirdek:

$$\text{Ker } \varphi = \left\{ \alpha : \frac{1}{\alpha} = 1 \right\} = \{1\}$$

■

Örnek 24.3 (Kompleks Eşlenik Otomorfisi). $\varphi : \langle \mathbb{C}, + \rangle \rightarrow \langle \mathbb{C}, + \rangle$, $a + bi \mapsto a - bi$ fonksiyonunun bir otomorfi olduğunu gösterip çekirdeğini bulunuz.

Çözüm.

İyi tanımlılık ve birebirlik: $a + bi = c + di \Leftrightarrow a = c, b = d \Leftrightarrow a - bi = c - di$; iki yön birden hem iyi tanımlılığı hem birebirliği verir.

Üzerinelik: Her $x + yi$ için $\varphi(x - yi) = x + yi$ 'dir.

İşlemi koruma:

$$\begin{aligned}\varphi((a + bi) + (c + di)) &= \varphi((a + c) + (b + d)i) = (a + c) - (b + d)i \\ &= (a - bi) + (c - di) = \varphi(a + bi) + \varphi(c + di)\end{aligned}$$

O hâlde $\varphi, \langle \mathbb{C}, + \rangle$ 'nin bir otomorfisidir. Toplam grubunun birimi $0 = 0 + 0i$ olduğundan

$$\text{Ker } \varphi = \{a + bi : a - bi = 0 + 0i\} = \{0\}$$

■

24.3 İzomorfi Ölçütü

Son iki örnekte çekirdek trivial çıktı ve fonksiyonlar birebirdi; ilkinde çekirdek iki elemanlıydı ve fonksiyon birebir değildi. Bu bir rastlantı değildir:

Teorem 24.2 (İzomorfi Ölçütü). $\varphi : G \rightarrow G'$ üzerine bir grup homomorfisi olsun. φ 'nin bir izomorfi olması için gerek ve yeter koşul

$$\text{Ker } \varphi = \{1_G\}$$

olmasıdır.

İspat.

Gereklik. φ izomorfi, yani birebir olsun. $\varphi(1_G) = 1_{G'}$ olduğundan $1_G \in \text{Ker } \varphi$ 'dir; birebirlik, $1_{G'}$ değerini alan başka eleman bırakmaz: $\text{Ker } \varphi = \{1_G\}$.

Yeterlik. $\text{Ker } \varphi = \{1_G\}$ olsun ve $\varphi(a) = \varphi(b)$ alalım:

$$(\varphi(a))^{-1}\varphi(b) = 1_{G'} \implies \varphi(a^{-1}b) = 1_{G'} \implies a^{-1}b \in \text{Ker } \varphi = \{1_G\}$$

O hâlde $a^{-1}b = 1_G$, yani $a = b$ 'dir: φ birebirdir ve üzerine homomorfi olduğundan izomorfidir.

■

Bu ölçüt, homomorfi teoremiyle birlikte okunmalıdır: çekirdek, homomorfinin birebirlikten “ne kadar uzak” olduğunun tam ölçüsüdür — $\text{Ker } \varphi$ ne kadar büyükse φ o kadar çok elemanı aynı değere yapıştırır ve $G/\text{Ker } \varphi$ yapışmadan arta kalan yapıyı kaydeder.

Teorem, her homomorfidenden bir normal alt grup üretti. Peki tersi? Her normal alt grup bir homomorfiden mi gelir? Yanıt evettir ve bunu kuran fonksiyon son derece doğaldır: her elemanı kendi kalan sınıfına gönderin — **doğal homomorfi**.

25. Doğal Homomorfi

Homomorfi teoremi, her üzerine homomorfinin çekirdeğinin normal alt grup olduğunu söyledi. Bu bölümde madalyonun öbür yüzünü kanıtlıyoruz: her normal alt grup da bir homomorfinin çekirdeğidir – elemanı kendi kalan sınıfına gönderen *doğal homomorfinin*. Böylece normal alt gruplar ile homomorfiler arasında tam bir karşılıklık kurulur ve her homomorfi, “önce doğal homomorfi, sonra izomorfi” biçiminde çarpanlara ayrılır: $\varphi = \psi\chi$.

25.1 Doğal Homomorfi

Teorem 25.1 (Doğal Homomorfi). $\langle G, \cdot \rangle$ bir grup ve $H \trianglelefteq G$ olsun.

$$\chi : G \rightarrow G/H, \quad a \mapsto aH$$

fonksiyonu, G 'nin G/H üzerine bir homomorfisidir.

İspat.

İyi tanımlıdır: $a = b \implies aH = bH \implies \chi(a) = \chi(b)$.

Üzerinedir: G/H 'nin tipik elemanı aH 'dir ve $\chi(a) = aH$ 'dir.

İşlemi korur: Bölüm grubundaki çarpmanın tanımıyla

$$\chi(a \cdot b) = (ab)H = aH \cdot bH = \chi(a) \cdot \chi(b)$$

■

Tanım 25.1 (Doğal (Kanonik) Homomorfi). Yukarıdaki χ homomorfisine G 'nin H normal alt grubuna göre doğal (kanonik) homomorfisi denir.

χ 'nin çekirdeği tam olarak H 'dir: $\chi(a) = aH$ sınıfının birim olması, $aH = H$, yani $a \in H$ demektir. Böylece:

Sonuç 25.1 (Normal Alt Gruplar ile Homomorfiler Arasındaki Karşılıklık). Bir G grubunun her üzerine homomorfisi (çekirdeği aracılığıyla) G 'nin bir normal alt grubunu belirler; karışt olarak G 'nin her normal alt grubu da (doğal homomorfi aracılığıyla) G 'nin bir üzerine homomorfisini belirler.

İspat.

Birinci yön homomorfi teoreminin 1) maddesidir. İkinci yön: verilen $H \trianglelefteq G$ için doğal homomorfi $\chi : G \rightarrow G/H$ bir üzerine homomorfidir ve $\text{Ker } \chi = H$ 'dir.

■

25.2 Her Homomorfi Doğal Homomorfiden Geçer

Teorem 25.2 ($\varphi = \psi\chi$ Ayrışımı). G bir grup ve $\varphi : G \rightarrow G'$ üzerine bir homomorfi olsun; $N = \text{Ker } \varphi$ diyelim. $\chi : G \rightarrow G/N$ doğal homomorfi ve $\psi : G/N \rightarrow G'$, $aN \mapsto \varphi(a)$ homomorfi teoremindeki izomorfi olmak üzere

$$\varphi = \psi\chi$$

İspat.

$\psi\chi : G \rightarrow G'$ bileşkesini herhangi bir $a \in G$ 'de hesaplayalım:

$$(\psi\chi)(a) = \psi(\chi(a)) = \psi(aN) = \varphi(a)$$

İki fonksiyon her noktada çakıştığından eşittir.

■

Bu ayrışımın söylediği şudur: bir homomorfinin yaptığı iş iki katmana ayrılır — önce χ elemanları çekirdeğin sınıflarına *yapıştırır* (bilgi kaybı tamamen buradadır), sonra ψ sınıfları hedefe *birebir* taşır (hiçbir bilgi kaybetmez). Homomorfinin bütün “kayıplı” kısmı, bir bölüm grubuna geçişten ibarettir.

25.3 Alıştırmalar

Alıştırma 25.1 (Üçlüler Grubundan $\mathbb{bb}(\mathbb{Z})$ 'ye). $G = \{(a, b, 3) : a, b \in \mathbb{Z}\}$ kümesinde $(a, b, 3) * (c, d, 3) = (a + c, b + d, 3)$ işlemi tanımlanıyor.

- a) $\langle G, * \rangle$ 'nin komutatif bir grup olduğunu gösteriniz.
- b) $\varphi : \langle G, * \rangle \rightarrow \langle \mathbb{Z}, + \rangle$, $(a, b, 3) \mapsto a + b$ fonksiyonunun üzerine bir homomorfi olduğunu gösterip çekirdeğini bulunuz.

Çözüm.

a) İlk iki bileşendeki işlem, tam sayıların toplamasıdır.

Kapalılık: $a + c, b + d \in \mathbb{Z}$ olduğundan sonuç G 'dedir.

Asosyatiflik ve komutatiflik: Bileşen bileşen, $\mathbb{Z}$ 'deki toplamının asosyatifliği ve komutatifliğinden gelir.

Birim eleman: $(0, 0, 3) \in G$ için $(0, 0, 3) * (a, b, 3) = (a, b, 3)$ 'tür.

Ters eleman: $(a, b, 3)$ 'ün tersi $(-a, -b, 3) \in G$ 'dir.

O hâlde $\langle G, * \rangle$ komutatif bir gruptur.

b) *İyi tanımlılık:* Aynı üçlü aynı $a + b$ toplamını verir.

Üzerinelik: Her $n \in \mathbb{Z}$ için $(n, 0, 3) \in G$ ve $\varphi((n, 0, 3)) = n$ 'dir.

İşlemi koruma:

$$\begin{aligned} \varphi((a, b, 3) * (c, d, 3)) &= \varphi((a + c, b + d, 3)) = (a + c) + (b + d) \\ &= (a + b) + (c + d) = \varphi((a, b, 3)) + \varphi((c, d, 3)) \end{aligned}$$

Demek ki φ üzerine bir homomorfidir. $\langle \mathbb{Z}, + \rangle$ 'nin birimi 0 olduğundan

$$\text{Ker } \varphi = \{(a, b, 3) \in G : a + b = 0\} = \{(a, -a, 3) : a \in \mathbb{Z}\}$$

Homomorfi teoremi ayrıca $G / \text{Ker } \varphi \cong \langle \mathbb{Z}, + \rangle$ olduğunu söyler.

■

Alıştırma 25.2 (Bir Sayı Kümesinden $\mathbb{bb}(\mathbb{Z})$ 'ye). $H = \{3a + b\sqrt{3}i : a, b \in \mathbb{Z}, a \equiv b \pmod{2}\}$ kümesi veriliyor.

- a) H 'nin $\mathbb{C}$ 'deki toplama işlemine göre bir grup olduğunu gösteriniz.
- b) $\varphi : \langle H, + \rangle \rightarrow \langle \mathbb{Z}, + \rangle$, $3a + b\sqrt{3}i \mapsto \frac{3a-b}{2}$ fonksiyonunun üzerine bir homomorfi olduğunu gösterip çekirdeğini bulunuz.

Çözüm.

a) $0 = 3 \cdot 0 + 0\sqrt{3}i \in H$ ($0 \equiv 0$) olduğundan $\emptyset \neq H \subseteq \mathbb{C}$ 'dir; $\langle \mathbb{C}, + \rangle$ grubunun alt grubu olduğunu gösterelim. Toplamsal tek koşullu ölçütü kullanalım: $3a + b\sqrt{3}i, 3c + d\sqrt{3}i \in H$ için

$$(3a + b\sqrt{3}i) - (3c + d\sqrt{3}i) = 3(a - c) + (b - d)\sqrt{3}i$$

Bileşen katsayıları $a - c, b - d \in \mathbb{Z}$ 'dir; ayrıca $a \equiv b$ ve $c \equiv d \pmod{2}$ olduğundan

$$a - c \equiv b - d \pmod{2}$$

sağlanır: fark yine H 'dedir. O hâlde $H \subseteq \langle \mathbb{C}, + \rangle$ ve $\langle H, + \rangle$ bir gruptur.

a.g.

b) İyi tanımlılık: $a \equiv b \pmod{2}$ koşulu $3a - b = 3a - b$ 'nin çift olmasını garanti eder: $3a - b \equiv 3a - a = 2a \equiv 0 \pmod{2}$. Yani $\frac{3a-b}{2}$ gerçekten bir tam sayıdır ve gösterim (a, b) çifti tarafından tek türlü belirlendiğinden fonksiyon iyi tanımlıdır.

Üzerinelik: $n \in \mathbb{Z}$ verilsin. $a = n, b = n$ seçersek $a \equiv b$ sağlanır ve

$$\varphi(3n + n\sqrt{3}i) = \frac{3n - n}{2} = n$$

İşlemi koruma:

$$\begin{aligned} \varphi((3a + b\sqrt{3}i) + (3c + d\sqrt{3}i)) &= \varphi(3(a + c) + (b + d)\sqrt{3}i) \\ &= \frac{3(a + c) - (b + d)}{2} \\ &= \frac{3a - b}{2} + \frac{3c - d}{2} = \varphi(3a + b\sqrt{3}i) + \varphi(3c + d\sqrt{3}i) \end{aligned}$$

Demek ki φ üzerine bir homomorfidir.

Çekirdek: $\varphi(3a + b\sqrt{3}i) = 0$ olması $3a = b$ demektir ($a \equiv 3a \pmod{2}$) otomatik sağlanır):

$$\text{Ker } \varphi = \{3a + 3a\sqrt{3}i : a \in \mathbb{Z}\} = \{3a(1 + \sqrt{3}i) : a \in \mathbb{Z}\}$$

■

Cebir 1'in yolculuğu burada tamamlanıyor. İkili işlem tanımıyla başladık; grup aksiyomlarını esnettik, permütasyonları ve devresel grupları sınıflandırdık, Lagrange teoremiyle sonlu grupların iskeletini çıkardık ve bölüm grubu ile homomorfi teoreminde iki büyük fikrin aynı şey olduğunu gördük. Serinin devamı olan Cebir 2, aynı soruları *iki* işlemli yapılara – halkalara ve ideallere – taşıyacak; müfredatı [ana sayfada](#) bulabilirsiniz.