BÖLÜM 4

ALTGRUPLAR

Bu bölümü bitirdiğinizde,

- altgrup kavramını
- altgrupların temel özelliklerini
- bir grubun bir alt kümesinin ürettiği grubu
- üreteç kavramını
- devirli grup kavramı ve devirli grupların bazı özelliklerini
- mertebe kavramını
- merkez, merkezleyici,eşlenik kavramalarını

öğrenmiş olabileceksiniz.

BÖLÜM 4

ALTGRUPLAR

Şimdiye kadar verdiğimiz grup örnekleri arasında öyle grup ikilileri var ki bu gruplardan birinin her elemanı diğer grubun elemanıdır ve ikili işlemi de diğer grubun ikili işlemi ile aynıdır. Örneğin, toplamsal gruplar olarak $\mathbb{Z}$ ve $\mathbb{Q}$ bu özelliğe sahiptir; çünkü, $\mathbb{Z} \subseteq \mathbb{Q}$ dur ve $m, n \in \mathbb{Z}$ için $m + n$ toplamı, $\mathbb{Z}$ içinde de $\mathbb{Q}$ içinde de aynı değere sahiptir. $SL(n, \mathbb{R})$ ve $GL(n, \mathbb{R})$ grupları da aynı özelliğe sahiptir. Bu bölümde, çok sık karşımıza çıkan bu durumla ilgili deyim ve gösterimleri sunacağız ve genel sonuçlar elde edeceğiz.

Aşağıdaki tanımla ilgili olarak, bir G grubunun ikili işleminin $G \times G$ den G ye bir fonksiyon olduğunu anımsayınız. Ayrıca, gruplarla ilgili genel tartışmalarımızı çarpımsal gösterim kullanarak yaptığımızı unutmayınız.

Tanım 1. G bir grup ve $H \subseteq G$ olsun. G nin ikili işleminin $H \times H$ ye kısıtlanışı H üzerinde bir ikili işlem oluyorsa, bu takdirde, H altkümesi G nin ikili işlemine göre *kapalı*dır denir. Bu durumda, H üzerinde ortaya çıkan ikili işleme, G den *indirgenmiş ikili işlem* denir. $\square$

Tanım 2. G bir grup ve $H \subseteq G$ olsun. Eğer H, G nin ikili işlemine göre kapalı ve G den indirgenmiş ikili işlem ile bir grup ise, bu takdirde, H ye G nin bir *altgrubu* denir ve $H \leq G$ yazılır. $\square$

Örnek 1. Kolayca görülebilir ki toplamsal grup olarak $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$; çarpımsal grup olarak $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$ ve $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$ dir. Ancak, $\mathbb{Q}^+ \not\leq \mathbb{R}$ dir; çünkü, $\mathbb{Q}^+ \subseteq \mathbb{R}$ ve $\mathbb{Q}^+$, $\mathbb{R}$ nin ikili işlemine (toplamaya) göre kapalı olmakla beraber, $< \mathbb{Q}^+, + >$ bir grup değildir. $\square$

Örnek 2. Toplamsal $\mathbb{Z}$ grubu içinde tüm çift sayılardan oluşan küme, $\mathbb{Z}$ nin bir altgrubudur. Çünkü, çift sayılar kümesi toplama işlemine göre kapalıdır ve (g.1), (g.2), (g.3) koşulları sağlanmaktadır. Bu altgrup, $2\mathbb{Z}$ ile gösterilir. Daha genel olarak, her $m \in \mathbb{Z}$ için

$$m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$$

tanımlanırsa, $m\mathbb{Z} \leq \mathbb{Z}$ olur. Hangi m ler için $m\mathbb{Z} = \mathbb{Z}$ dir? $\square$

Örnek 3. Her G grubu için $G \leq G$ ve $\{e\} \leq G$ dir. Eğer $H \leq G$ fakat $H \neq G$ ise, H ye G nin bir *özaltgrubu* denir ve $H < G$ yazılır. Sadece birim eleman e den oluşan $\{e\}$ grubuna *birim grup* ($trivial grup$) adı verilir. $\square$

Bir grubun bir altkümesinin altgrup olup olmadığı araştırılırken grup tanımındaki bazı koşulların kontrol edilmesi gerekmez; çünkü, bu koşullar kendiliğinden sağlanır. Daha açık bir ifadeyle,

Önerme 1. *G bir grup ve $H \subseteq G$ ise, $H \leq G$ olması için gerek ve yeter koşul,*

$$(i)\ \ e \in H \qquad ve \qquad (ii)\ \ x, y \in H \Longrightarrow xy^{-1} \in H$$

olmasıdır.

Kanıt. $H \leq G$ ise, (i) ve (ii) koşullarının sağlanacağı açıktır. Karşıt olarak, (i) ve (ii) sağlanıyor ise, her $y \in H$ için ($e \in H$ olduğundan, (ii) uygulanarak) $ey^{-1} = y^{-1} \in H$ olduğu; sonra da her $x, y \in H$ için ($y^{-1} \in H$ olduğundan, yine (ii) uygulanarak) $x(y^{-1})^{-1} = xy \in H$ olduğu görülür. Böylece, H, G nin ikili işlemine göre kapalıdır ve (g.2), (g.3) koşulları sağlanmaktadır. (g.1) koşulu da kendiliğinden sağlandığından, $H \leq G$ dir. $\blacksquare$

Soyut cebire yeni başlamış öğrencilerden çoğu, Önerme 1 yerine aşağıdaki önermeyi tercih ederler.

Önerme 2. *G bir grup ve $H \subseteq G$ ise, $H \leq G$ olması için gerek ve yeter koşul,*

$$(i)\ H \neq \emptyset, \quad (ii)\ x, y \in H \Longrightarrow xy \in H \ \text{ ve } \ (iii)\ x \in H \Longrightarrow x^{-1} \in H$$

olmasıdır.

Kanıt. $H \leq G$ ise, (i) , (ii) ve (iii) nin sağlandığı açıktır. Karşıt olarak, (i) , (ii) ve (iii) sağlanıyorsa, (i) den H içinde en az bir x elemanı bulunduğu; (iii) den, $x^{-1} \in H$ ve (ii) den, $xx^{-1} = e \in H$ olduğu görülür. Şimdi her $x, y \in H$ için, (iii) den, $y^{-1} \in H$ ve (ii) den, $xy^{-1} \in H$ olduğu görülür. Böylece, Önerme 1 e göre $H \leq G$ dir. ∎

Eğer altgrup adayı olan H altkümesi, G grubunun bir sonlu altkümesi ise, aşağıdaki önermeden görüleceği gibi, H nin altgrup olup olmadığını araştırırken yapılacak iş daha da kolaydır.

Önerme 3. *G bir grup, $H \subseteq G$ ve H sonlu ise, $H \leq G$ olması için gerek ve yeter koşul,*

$$(i) \quad H \neq \emptyset \qquad \text{ve} \qquad (ii) \quad x, y \in H \Longrightarrow xy \in H$$

olmasıdır.

Kanıt. Gereklilik açık olduğu için sadece yeterliliği kanıtlayalım. Bunun için, Önerme 2 ye göre sadece her $x \in H$ için $x^{-1} \in H$ olduğunu kanıtlamak yeter. $H = \{a_1, a_2, \ldots, a_n\}$ ve $x \in H$ olsun. Bu takdirde, her $i = 1, \ldots, n$ için $xa_i \in H$ dir ve ayrıca

$$xa_i = xa_j \Longrightarrow a_i = a_j \Longrightarrow i = j$$

olacağından, $i \neq j$ için $xa_i \neq xa_j$ dir. Böylece,

$$H = \{xa_1, xa_2, \ldots, xa_n\}$$

olmalıdır. O halde, uygun bir k için, $xa_k = e$ dir ve $x^{-1} = a_k \in H$ olduğu görülür. ∎

Önerme 4. *$\mathcal{A}$, bir G grubunun altgruplarından oluşan, boş ol-*

mayan bir aile olsun. Bu takdirde, $\bar{H} = \bigcap_{H \in \mathcal{A}} H$ *de* G *nin bir altgrubudur.*

Kanıt. Her $H \in \mathcal{A}$ için $H \leq G$ olduğundan, $e \in H$ dir. O halde, $e \in \bar{H}$ dir. Ayrıca, $x, y \in \bar{H}$ verildiğinde, her $H \in \mathcal{A}$ için $x, y \in H$ ve dolayısıyla, $xy^{-1} \in H$ olacağından, $xy^{-1} \in \bar{H}$ olur. Önerme 1 e göre, $\bar{H} \leq G$ dir. ∎

Tanım 3. G bir grup, $S \subseteq G$ olsun. G nin S yi kapsayan altgruplarından oluşan

$$\mathcal{A} = \{\ H : H \leq G,\ S \subseteq H\ \}$$

ailesini alalım ve

$$< S >= \bigcap_{H \in \mathcal{A}} H$$

tanımlayalım. $< S >$ altgrubuna, S nin G *içinde ürettiği altgrup* ve S kümesine de bu altgrubun bir *üreteç kümesi* denir. Eğer $G =< S >$ ise, G grubu, S *tarafından üretilmiştir* denir; $G =< S >$ ve S kümesi sonlu ise, G bir *sonlu üretilmiş* gruptur denir. S sonlu ve $S = \{x_1, \ldots, x_n\}$ ise, $< S >=< x_1, \ldots, x_n >$ yazılır. $S = \{x\}$ ise, $< S >=< x >$ altgrubuna G nin x tarafından üretilen *devirli* altgrubu (veya G içinde x in ürettiği *devirli altgrup*); x elemanına da bu devirli altgrubun bir *üreteci* denir. □

Bir grup içinde bir altkümenin ürettiği altgrup veya bir elemanın ürettiği devirli altgrup aşağıdaki gibi de tasvir edilebilir.

Teorem 1. *G bir grup, $S \subseteq G$ ve $x \in G$ olsun. Bu takdirde,*

(i) $< \emptyset >= \{e\}$,

(ii) $S \neq \emptyset$ *ise,* $< S >= \{s_1^{n_1} s_2^{n_2} \cdots s_r^{n_r} : r \in \mathbb{N}, n_i \in \mathbb{Z}, s_i \in S\}$,

(iii) $< x >= \{x^n : n \in \mathbb{Z}\}$

dir.

Kanıt. *(i)* $\emptyset \subseteq \{e\}$ dir ve G nin her altgrubu, $\{e\}$ yi kapsar. Bu nedenle, $< \emptyset >= \{e\}$ dir.

(ii) $S \neq \emptyset$ olsun. $K = \{s_1^{n_1} \cdots s_r^{n_r} : r \in \mathbb{N}, n_i \in \mathbb{Z}, s_i \in S\}$ alalım. $S \subseteq K$ olduğu açıktır. Diğer yandan, $H \leq G$ ve $S \subseteq H$ ise, $K \subseteq H$ olacağından, iddianın kanıtı için, $K \leq G$ olduğunu göstermek yeter. Gerçekten, $S \neq \emptyset$ olduğundan, en az bir s $\in S$ vardır ve dolayısıyla, $e = s^0 \in K$ dır. Ayrıca, K nın

$$x = s_1^{n_1} \cdots s_r^{n_r} \quad , \quad y = t_1^{m_1} \cdots t_k^{m_k}$$

gibi iki elemanı verildiğinde

$$xy^{-1} = s_1^{n_1} \cdots s_r^{n_r} t_k^{-m_k} \cdots t_1^{-m_1}$$

yine K nın bir elemanıdır. Böylece, Önerme 1 den, $K \leq G$ dir. (iii) nin kanıtını okuyucuya alıştırma olarak bırakıyoruz. ∎

Örnek 4. $S = \{6, 15\} \subseteq \mathbb{Q}^*$ için,

$$< S >= \{ \ 2^m 3^{m+n} 5^n \ : \ m, n \in \mathbb{Z} \ \}$$

dir. □

Uyarı 1. Daha önce de belirttiğimiz gibi, okuyucunun, çarpımsal gösterimde verilmiş olan tüm önerme, sonuç ve tanımların toplamsal gösterimde karşılıklarını düşünmesi ve ifade etmesi çok yerinde olacaktır. Örneğin, G

bir toplamsal grup, $x \in G$ ve $\emptyset \neq S \subseteq G$ ise,

$$< S >= \{n_1 s_1 + \cdots + n_r s_r : \quad r \in \mathbb{N}, n_i \in \mathbb{Z}, s_i \in S\},$$

$$< x > = \ \{nx : \ n \in \mathbb{Z}\}$$

olacaktır. □

Örnek 5. $T = \{6, 15\} \subseteq \mathbb{Z}$ için, $< T >=< 3 >= 3\mathbb{Z}$ dir. Bunu görmek için, $(-2) \cdot 6 + (1) \cdot 15 = 3$ ve $6 = 2 \cdot 3$, $15 = 3 \cdot 5$ olduğuna dikkat etmek yeter. □

Tanım 4. Bir G grubunun $< x >= G$ olacak biçimde bir x elemanı varsa, G ye bir *devirli grup*; x elemanına G nin bir *üreteci* denir. □

Uyarı 2. G bir grup, $x \in G$ olsun. Her ne kadar

$$\ldots,\ x^{-2},\ x^{-1},\ x^{0},\ x^{1},\ x^{2},\ \ldots$$

sonsuz bir dizi ise de, $< x >= \{x^n : n \in \mathbb{Z}\}$ devirli grubunun eleman sayısı sonlu olabilir (Neden ?). Ayrıca, $x^m x^n = x^{m+n} = x^{n+m} = x^n x^m$ olduğundan her devirli grup bir Abel grubudur. □

Örnek 6. $\mathbb{C}^*$ çarpımsal grubu içinde $< i >= \{1, i, -1, -i\}$; $\mathbb{R}^*$ içinde

$$< \pi >= \{\pi^n : n \in \mathbb{Z}\}, \quad < -1 >= \{1, -1\};$$

ve toplamsal grup $\mathbb{Z}$ içinde

$$< 2 >= \{2n : n \in \mathbb{Z}\} = 2\mathbb{Z} \quad , \quad < -1 >= \{-n : n \in \mathbb{Z}\} = \mathbb{Z} =< 1 >$$

dir. Böylece, $\mathbb{Z}$ nin bir devirli grup olduğunu görüyoruz. □

Tanım 5. G bir grup, $x \in G$ olsun. G kümesinin kardinalitesine G grubunun *mertebesi* denir. Mertebesi sonlu olan bir gruba *sonlu grup*, mertebesi sonsuz olan bir gruba *sonsuz grup* denir. G içinde x tarafından üretilen devirli altgrubun mertebesine x in *mertebesi* denir. G nin mertebesi, $|G|$ ile; $x \in G$ nin mertebesi, $|x|$ ile gösterilir. □

Bölüm 3'te verilen örneklerin çoğunluğu sonsuz grup olmasına rağmen, Örnek 3.1'de, mertebesi 2 olan bir grup örneği vardır. Örnek 6'da, $\mathbb{C}^*$ grubunun i elemanının mertebesinin 4 olduğu; $\mathbb{R}^*$ ın π elemanının mertebesinin sonsuz, -1 elemanının mertebesinin ise 2 olduğu; toplamsal $\mathbb{Z}$ grubunda 1 ve -1 in her ikisinin de mertebesinin sonsuz olduğu görülmektedir. Bir grubun birim elemanının mertebesi 1 dir ve grup içinde mertebesi 1 olan başka eleman yoktur. Grup elemanlarının mertebelerinin sonlu veya sonsuz oluşu şöyle de belirlenebilir:

Teorem 2. *G bir grup, $x \in G$ ise, aşağıdaki koşullar denktir:*

(i) *x in mertebesi sonludur.*

(*ii*) $x^i = x^j$ *olacak şekilde farklı* $i, j \in \mathbb{Z}$ *vardır.*

(*iii*) $x^r = e$ *olacak şekilde bir* $r \in \mathbb{N}$ *vardır.*

Kanıt. $(i) \Longrightarrow (ii)$ x in mertebesi sonlu ise, $< x >= \{x^n : n \in \mathbb{Z}\}$ sonlu olduğundan, $x^i = x^j$ olacak biçimde $i \neq j$ tamsayıları vardır.

$(ii) \Longrightarrow (iii)$ $x^i = x^j$; $i, j \in \mathbb{Z}$ ve $i > j$ olsun. Bu takdirde, $r = i - j \in \mathbb{N}$ ve $x^r = x^{i-j} = x^i x^{-j} = x^j x^{-j} = x^0 = e$ olur.

$(iii) \Longrightarrow (i)$ $x^r = e$ olan en küçük $r \in \mathbb{N}$ sayısının seçildiğini varsayalım ve her $n \in \mathbb{Z}$ için bölme algoritması ile

$$n = qr + k \quad ; \quad q, k \in \mathbb{Z} \ ; \ 0 \leq k \leq r - 1$$

yazalım. O zaman,

$$x^n = x^{qr+k} = (x^r)^q x^k = x^k$$

ve sonuç olarak,

$$< x >= \{ \ x^n : n \in \mathbb{Z} \ \} = \{ \ x^k : 0 \leq k \leq r - 1 \ \}$$

elde edilir ki bu, x in mertebesinin sonlu olduğunu gösterir. ∎

Teorem 2 nin aşağıdaki iki sonucunu kanıtsız olarak ifade ediyoruz:

Sonuç 1. *G bir grup, $x \in G$ olsun. x in mertebesinin sonsuz olması için gerek ve yeter koşul, her $i, j \in \mathbb{Z}$, $i \neq j$ için $x^i \neq x^j$ olmasıdır.* ∎

Sonuç 2. *G bir grup, $x \in G$, $m \in \mathbb{N}$ olsun. Bu takdirde, $|x| = m$ olması için gerek ve yeter koşul, $x^m = e$ olması ve m nin bu özelliğe sahip en küçük doğal sayı olmasıdır.* ∎

Teorem 3. *G bir grup, $|x| = m$ olsun. Bu takdirde,*

(*i*) $< x >= \{e, x, x^2, \ldots, x^{m-1}\}$,

(*ii*) $r \in \mathbb{Z}$ *için,* $x^r = e \Longleftrightarrow m \mid r$,

(*iii*) $i, j \in \mathbb{Z}$ *için,* $x^i = x^j \Longleftrightarrow m \mid (i - j)$.

Kanıt. Sadece (ii) yi kanıtlayıp diğer kısımların kanıtını okuyucuya bırakıyoruz. $r \in \mathbb{Z}$; $x^r = e$ olsun. Bölme algoritması ile

$$r = mq + k \; ; \; q, k \in \mathbb{Z} \quad , \quad 0 \leq k < m$$

yazalım. Bu durumda, $e = x^r = x^{mq+k} = (x^m)^q x^k = x^k$, $0 \leq k < m$ olacağından, Teorem 2 nin ikinci sonucuna göre, $k = 0$ ve $m \mid r$. Karşıt olarak, $m \mid r$ ve $r = mq$ olsun. O zaman, $x^r = x^{mq} = (x^m)^q = e$ olur. ▪

Bu bölümü bazı standart altgrup örnekleri içeren önermelerle kapatıyoruz.

Önerme 5. *Her G grubu için*

$$M(G) = \{ \; x \in G : \quad \textit{her } y \in G \textit{ için } xy = yx \; \}$$

kümesi G nin bir altgrubudur.

Kanıt. Alıştırma. Önerme 1 i kullanınız. ▪

Tanım 6. Bir G grubu için Önerme 5'te tanımlanan $M(G)$ altgrubuna G nin *merkezi* denir. □

Gerçekte, her G için $M(G)$ bir Abel grubudur. G grubunun Abel grubu olması, $M(G) = G$ olması için gerek ve yeter koşuldur.

Önerme 6. *G bir grup, $x \in G$ ve $H \leq G$ ise, aşağıdaki kümelerden her biri G nin bir altgrubudur:*

$$M_G(x) = \{y \in G : xy = yx\} \quad , \quad x^{-1}Hx = \{x^{-1}hx : h \in H\}.$$

Kanıt. $ex = xe = x$ olduğundan, $e \in M_G(x)$ tir. Her $y, z \in M_G(x)$ için $xy = yx$, $xz = zx$ olduğundan,

$$x(yz) = (xy)z = (yx)z = y(xz) = y(zx) = (yz)x$$

ve buradan, $yz \in M_G(x)$. Ayrıca, her $y \in M_G(x)$ için $xy = yx$ olduğundan,

$$\begin{aligned} xy^{-1} &= e(xy^{-1}) = (y^{-1}y)(xy^{-1}) = y^{-1}(yx)y^{-1} \\ &= y^{-1}(xy)y^{-1} = (y^{-1}x)(yy^{-1}) = (y^{-1}x)e = y^{-1}x \end{aligned}$$

ve buradan, $y^{-1} \in M_G(x)$. Böylece, $M_G(x) \leq G$ dir. $x^{-1}Hx \leq G$ olduğunu kanıtlamak için aşağıdaki gözlemler yeterlidir:

$$e \in H \text{ olduğundan } x^{-1}ex = e \in x^{-1}Hx,$$

$$x^{-1}ax, x^{-1}bx \in x^{-1}Hx \Longrightarrow (x^{-1}ax)(x^{-1}bx) = x^{-1}abx \in x^{-1}Hx,$$

$$x^{-1}ax \in x^{-1}Hx \Longrightarrow (x^{-1}ax)^{-1} = x^{-1}a^{-1}x \in x^{-1}Hx.$$

■

Tanım 7. Önerme 6'da tanımlanan $M_G(x)$ altgrubuna x elemanının G içindeki *merkezleyicisi*, $x^{-1}Hx$ e de H nin (G içinde) x e göre *eşleniği* denir. □