BÖLÜM **6**

DEVİRLİ GRUPLAR

Bu bölümü bitirdiğinizde,

- Devirli grup, devirli grubun üreteci
- Sonlu ve sonsuz devirli gruplar ve bunların üreteçleri
- $\mathbb{Z}$ ve $\mathbb{Z}_n$ devirli grupları ve bunların üreteçleri
- Devirli grubun bir elemanının mertebesi
- Bir devirli grubun altgrupları, altgruplar kafesi

hakkında bilgi sahibi olabileceksiniz.

BÖLÜM **6**

DEVİRLİ GRUPLAR

Bu bölümde, Bölüm 4'te tanımlanmış ve bazı örnekleri sergilenmiş olan devirli grupları tekrar ele almak ve daha ayrıntılı bilgi sunmak istiyoruz. Bu noktada, okuyucunun, Bölüm 4'te devirli gruplarla ilgili olarak sunulan bilgileri, özellikle Teorem 4.2, Teorem 4.3 ve sonuçlarını gözden geçirmesinin yararlı olacağını belirtmek isteriz. Daha önce tanımladığımız üzere, G bir grup, $x \in G$ ve

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

ise, G ye bir *devirli grup*, x elemanına da G nin bir *üreteci* denir.

Tamsayılar grubu $\mathbb{Z}$, bir devirli gruptur; 1 ve -1 her ikisi de $\mathbb{Z}$ nin birer üretecidir(Bak. Örnek 4.6). Teorem 5.1'de, $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ toplamsal grubunun da devirli olduğunu gördük. Bu devirli grubun hangi elemanlarının üreteç olduğunu bu bölümde belirleyeceğiz. $\mathbb{Z}_n^*$ çarpımsal grupları, n nin bazı değerleri için devirli, bazı değerleri için devirli değildir. Örneğin,

$$\mathbb{Z}_{10}^* = < 3 > = < 7 > = \{1, 3, 7, 9\}$$

olduğu kolayca görülebilir. Diğer yandan, $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ grubu içinde,

$$< 1 > = \{1\},\ < 3 > = \{1, 3\},\ < 5 > = \{1, 5\}, < 7 > = \{1, 7\}$$

dir ve sonuç olarak, $\mathbb{Z}_8^*$ devirli değildir.

Eğer G bir devirli grup ve x onun bir üreteci ise, x^{-1} in de o grubun bir üreteci olduğunu biliyoruz. Aşağıdaki teorem, bir devirli grubun herhangi bir elemanının mertebesi ve sonuç olarak da bir devirli grubun üreteçleri hakkında kesin bilgi vermektedir.

Teorem 1. *$G = < x >$ bir devirli grup, $x^k \in G$ olsun. Bu takdirde,*

(i) *G sonsuz ise, G nin, x ve x^{-1} den başka üreteci yoktur;*

(ii) *G sonlu ve $|G| = m$ ise, $|x^k| = \frac{m}{(k,m)}$ dir;*

(iii) *G sonlu ve $|G| = m$ ise, $< x^k > = G \iff (k, m) = 1$ dir(Burada, $(k, m) = obeb(k, m)$ dir).*

Kanıt. *(i)* $G = < x >$ sonsuz ve $k \neq \mp 1$ ise, $n \in \mathbb{Z}$ nasıl seçilirse seçilsin, $(x^k)^n \neq x$ olacağından (Bak. Teorem 4.2), $< x^k > \neq G$ dir. Dolayısıyla, G nin, x ve x^{-1} den başka üreteci yoktur.

(ii) $G = < x >$ sonlu, $|G| = m$ olsun. Bu durumda,

$$G = \{e, x, \cdots, x^{m-1}\}$$

olacağından (Bak. Teorem 4.3), iddianın kanıtı için $0 < k < m$ olduğunu kabul edebiliriz. ($k = 0$ için $|x^0| = |e| = 1 = \frac{m}{(0,m)}$ dir). $|x^k| = t$ olsun. Ayrıca, $(k, m) = d$; $k = dr$, $m = ds$; $r, s \in \mathbb{N}$ olsun. Bu takdirde, $t > 1$, $(r, s) = 1$ dir ve

$$(x^k)^s = (x^{dr})^s = (x^{ds})^r = (x^m)^r = e$$

olur. Böylece, Teorem 4.3(ii) den, $t \mid s$ olduğu görülür. Diğer yandan,

$$(x^k)^t = x^{kt} = e \quad \text{ve} \quad |x| = m$$

olduğundan $m = ds \mid kt = drt$ ve buradan, $s \mid rt$ olduğu görülür. s ve r aralarında asal olduğundan, $s \mid t$ olmalıdır. Sonuç olarak; $t \mid s$ ve $s \mid t$ den $t = s$, yani

$$|x^k| = t = s = \frac{m}{d} = \frac{m}{(k, m)}$$

elde edilir.

(iii) $G = < x >$ sonlu, $|G| = m$, $(k, m) = d$ olsun. Eğer $< x^k > = G$ ise, $|x^k| = |G| = m$ olması gerekir. Bu durumda, (ii) den, $(k, m) = d = 1$ olduğu sonucu çıkar. Karşıt olarak, $(k, m) = 1$

olsun. Bu takdirde, yine (ii) den, $|x^k| = m = |G|$ dir. $< x^k > \subseteq G$ olduğundan, $G =< x^k >$ dir. O halde, x^k, G yi üretir. ∎

Teorem 1 e göre, $G =< x >$ devirli grubu sonsuz ise, G nin tam iki tane üreteci vardır: x ve x^{-1}. Eğer $G =< x >$ devirli grubu sonlu ve $|G| = m$ ise, G nin üreteçleri

$$\{\ x^k\ :\ k \in \mathbb{Z},\ 1 < k < m,\ (k, m) = 1\ \}$$

kümesinin elemanlarıdır; dolayısıyla, bu durumda G nin tam $\varphi(m)$ tane üreteci vardır.

Sonuç 1. *Mertebesi m olan bir devirli grubun tam $\varphi(m)$ tane üreteci vardır.* ∎

Sonuç 2. (i) *$\mathbb{Z}$ devirli grubunun üreteçleri, 1 ve -1 den ibarettir.*

(ii) *$k \in \mathbb{Z}_n$ nin bir üreteç olması için gerek ve yeter koşul, $(k, n) = 1$ olması; yani $k \in \mathbb{Z}_n^*$ olmasıdır.*

Kanıt. (i) $\mathbb{Z} =< 1 >$ alınırsa, Teorem $1(i)$ den, $\mathbb{Z}$ nin, sadece 1 veya -1 tarafından üretildiği görülür.

(ii) $\mathbb{Z}_n =< 1 >$ alalım ve Teorem $1(iii)$ ü toplamsal gösterimde uygulayalım: $k \in \mathbb{Z}_n$ için

$$\mathbb{Z}_n =< k > \iff (k, n) = 1 \iff k \in \mathbb{Z}_n^*$$

olduğu görülür. ∎

Bu sonuçlardan hareketle şu hususu vurgulayalım ki bir devirli grubun üreteçleri araştırılırken üreteçlerden biri biliniyorsa, diğer üreteçler, grubun tüm elemanlarına bakılmadan, bilinen üreteç yardımıyla belirlenebilir.

Örnek 1. $\mathbb{Z}_{50}^*$ ın mertebesi 20 olan bir çarpımsal devirli grup olduğu ve $\mathbb{Z}_{50}^* =< 3 >$ olduğu görülebilir. Yukarıdaki sonuçlara göre $\mathbb{Z}_{50}^*$ ın $\varphi(20) = 8$ üreteci vardır ve bunlar

$$3^1 = 3, 3^3 = 27, 3^7 = 37, 3^9 = 33, 3^{11} = 47, 3^{13} = 23, 3^{17} = 13, 3^{19} = 17$$

den ibarettir. □

Bir grup verildiğinde, o grubun alt gruplarının neler olduğunu bilmek çok önemlidir. Çünkü, grubun altgrupları o grubun yapısı hakkında önemli bilgiler verir. Herhangi bir grubun tüm altgruplarını belirlemek kolay değildir. Ancak, devirli gruplar için durum biraz farklıdır.

Teorem 2. *Bir devirli grubun her altgrubu devirlidir. $G =< x >$, mertebesi m olan bir devirli grup ise, G nin her altgrubunun mertebesi, m yi böler. Ayrıca, m nin her pozitif böleni d için, G nin, mertebesi d olan bir ve yalnız bir altgrubu vardır ve o da $< x^{m/d} >$ dir.*

Kanıt. $G = < x >$, $H \leq G$ olsun. H nin devirli olduğunu göstereceğiz. $H = \{e\}$ ise, H devirli, $H = < e >$ dir. O nedenle, $H \neq \{e\}$ olsun. $x^n \in H \backslash \{e\}$ alalım. $(x^n)^{-1} = x^{-n} \in H$ olduğundan $n > 0$ kabul edebiliriz. Başka bir deyişle, $\{n \in \mathbb{N} : x^n \in H\}$ kümesi boş değildir. Bu kümenin en küçük elemanı t olsun. İddia ediyoruz ki, $< x^t > = H$ dir. $x^t \in H$ olduğundan, $< x^t > \subseteq H$ olduğu açıktır. Eğer $x^r \in H$ ise, bölme algoritması ile,

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

yazalım. O zaman, $x^{tq} = (x^t)^q \in H$ olduğundan

$$x^r = x^{tq+k} = x^{tq} \cdot x^k \quad , \quad x^k = x^{-tq} \cdot x^r \in H$$

olur. t nin seçiminden dolayı

$$0 \leq k < t \quad \text{ve} \quad x^k \in H$$

olması ancak $k = 0$ olunca mümkündür. Böylece, $r = tq$ ve

$$x^r = x^{tq} = (x^t)^q \in < x^t >;$$

dolayısıyla, $H \subseteq < x^t >$ olduğu görülür. O halde, $H = < x^t >$ dir. Bu, ilk önermeyi, yani bir devirli grubun her altgrubunun da devirli olduğunu kanıtlar.

Teoremin ikinci kısmının kanıtı için $G =< x >$; $|G| = m$ ve $H \leq G$ alalım. Kanıtın yukarıdaki kısmından, $H =< x^t >$, $t \geq 0$ dır. Şimdi Teorem 1 den,

$$|H| = |x^t| = \frac{m}{(t,m)} \quad , \quad m = (t,m) \cdot |H|$$

ve böylece, $|H|$, m yi böler. Son olarak, m nin bir pozitif böleni d olsun ve $r = m/d$ alalım. Bu takdirde, Teorem $1(ii)$ den

$$|x^r| = \frac{m}{(r,m)} = \frac{m}{r} = d$$

ve dolayısıyla, $< x^r >$, mertebesi d olan bir altgruptur. Diğer yandan, G nin, mertebesi d olan herhangi bir altgrubu K ise, kanıtın ilk kısmından, $x^k \in K$ olan en küçük pozitif tamsayı k olmak üzere, $K =< x^k >$ dır ve Teorem $1(ii)$ den

$$d = |K| = \frac{m}{(k,m)}$$

dir. Son ifadeden, $(k,m) = \frac{m}{d} = r$ dir ve dolayısıyla, $r \mid k$ dır. $k = rq$ olsun. O zaman, $x^k = x^{rq} = (x^r)^q \in < x^r >$ ve bu nedenle, $K \subseteq < x^r >$ dir. $|K| = | < x^r > | = d$ olduğundan, $K =< x^r >$ dir. O halde, m nin her pozitif böleni d için $|H| = d$ olan bir ve yalnız bir altgrup $H \leq G$ vardır ve o da $H =< x^{m/d} >$ dir. ∎

Teorem 2 nin sonucu olarak, mertebesi m olan bir devirli grup $< x >$ in altgrupları, $r \mid m$ olmak üzere, $< x^r >$ lerden ibarettir. Eğer $r \mid m$, $m = rd$ ise, $| < x^r > | = d$ dir ve $< x^r >=< x^{m/d} >$, $< x >$ in, mertebesi d olan yegane altgrubudur.

Teorem 2 yi $\mathbb{Z}_n =< 1 >$ e uygularsak şu sonucu elde ederiz:

Sonuç 1. *$n \in \mathbb{N}$, $n \geq 2$ verilmiş olsun. n nin her pozitif böleni d için $\mathbb{Z}_n$ nin, mertebesi d olan bir ve yalnız bir altgrubu vardır; $d = 1$ için bu altgrup $< 0 >$ dır ve $d > 1$ için $< n/d >$ dir. Ayrıca, $\mathbb{Z}_n$ nin tüm altgrupları bunlardan ibarettir (Böylece, $\mathbb{Z}_n$ nin altgruplarının sayısı, n nin pozitif bölenlerinin sayısına eşittir).* ∎

Örnek 2. $G =< x >$, mertebesi 30 olan bir grup ise, 30 un pozitif bölenlerinin kümesi $\{1,\ 2,\ 3,\ 5,\ 6,\ 10,\ 15,\ 30\}$ olduğundan, G nin altgrupları şunlardır:

$$\begin{aligned}
< x^1 > &= < x > = \{e, x, x^2, \cdots, x^{29}\}, & |x| &= 30.\\
< x^2 > &= \{e, x^2, x^4, \cdots, x^{28}\}, & |x^2| &= 15.\\
< x^3 > &= \{e, x^3, x^6, \cdots, x^{27}\}, & |x^3| &= 10.\\
< x^5 > &= \{e, x^5, x^{10}, x^{15}, x^{20}, x^{25}\}, & |x^5| &= 6.\\
< x^6 > &= \{e, x^6, x^{12}, x^{18}, x^{24}\}, & |x^6| &= 5.\\
< x^{10} > &= \{e, x^{10}, x^{20}\}, & |x^{10}| &= 3.\\
< x^{15} > &= \{e, x^{15}\}, & |x^{15}| &= 2.\\
< x^{30} > &= \{e\}, & |x^{30}| &= 1.
\end{aligned}$$

□

Örnek 3. Önceki örnekteki düşüncelerle, $\mathbb{Z}_{30}$ un tüm altgrupları şöyle listelenebilir:

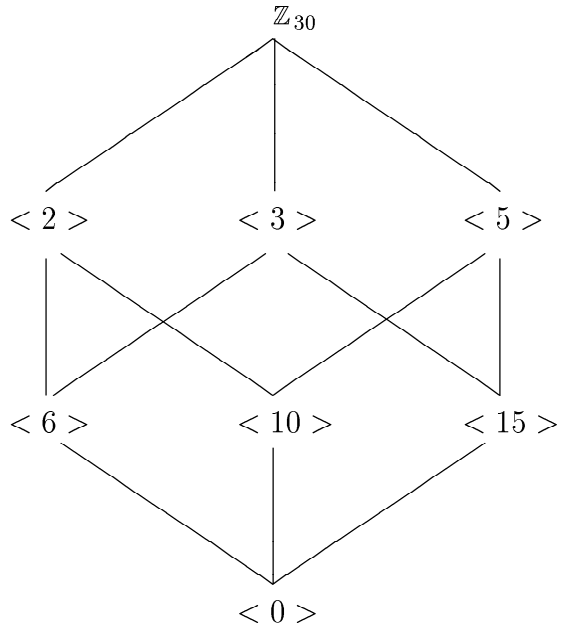
$$\begin{aligned}
< 1 > &= \{0, 1, 2, \cdots, 29\}, & &\text{mertebesi } 30.\\
< 2 > &= \{0, 2, 4, \cdots, 28\}, & &\text{mertebesi } 15.\\
< 3 > &= \{0, 3, 6, \cdots, 27\}, & &\text{mertebesi } 10.\\
< 5 > &= \{0, 5, 10, \cdots, 25\}, & &\text{mertebesi } 6.\\
< 6 > &= \{0, 6, 12, 18, 24\}, & &\text{mertebesi } 5.\\
< 10 > &= \{0, 10, 20\}, & &\text{mertebesi } 3.\\
< 15 > &= \{0, 15\}, & &\text{mertebesi } 2.\\
< 0 > &= \{0\}, & &\text{mertebesi } 1.
\end{aligned}$$

□

Bir grubun altgrupları arasındaki ilişkiler, bu altgrupları düzlemde bazı noktalarla temsil edip biri diğerinin özaltgrubu olan gruplara karşılık gelen noktaları doğru parçaları ile birbirlerine bağlamak suretiyle elde edilen çizelgede görülebilir. Bu çizelgeye, sözü edilen grubun *altgruplar kafesi* denir.

Altgrup kafeslerini çeşitli biçimlerde yapmak mümkündür; kuşkusuz,

göze hoş görünen çizelgeler tercih edilir. $\mathbb{Z}_{30}$ un altgruplar kafesi aşağıdaki gibi yapılabilir:



Teorem 1 ve Teorem 2 yi birleştirerek bir devirli grupta belli bir mertebeden elemanların sayısını belirleyebiliriz.

Sonuç 2. *Mertebesi m olan bir devirli grubun mertebesi d olan elemanlarının sayısı, $d \mid m$ ise $\varphi(d)$; aksi halde,* 0 *dır.*

Kanıt. $G = < x >$, $|G| = m$ ve $d \mid m$ olsun. G nin bir elemanının mertebesinin d olması demek, o elemanın ürettiği devirli altgrubun mertebesinin d olması demektir. G nin, mertebesi d olan tam bir tane altgrubu bulunduğuna ve bunun üreteçlerinin sayısı $\varphi(d)$ olduğuna göre, G nin, mertebesi d olan elemanlarının sayısı da $\varphi(d)$ dir. d, m yi bölmüyorsa, G içinde mertebesi d olan eleman yoktur. ∎

Teorem 2, *devirli grupların temel teoremi* diye adlandırılabilir. Bu teoremin önemi, $\mathbb{Z}_{30}$ un altgruplarının belirlenmesi; örneğin, altgruplar

kafesinin yapılması ile, aynı işin $\mathbb{Z}_{30}^*$ veya $\mathcal{D}_{30}$ için yapılması karşılaştırıldığı zaman anlaşılır. Oysa, $\mathcal{D}_{30}$ ve diğer dihedral gruplar devirli olmayan gruplar arasında en basit yapıya sahip gruplardır.

İleride, Teorem 2 nin bir kısmının, devirli olmayan gruplar için de doğru olduğunu göreceğiz. Örneğin, bu bölümü izleyen bölümde göreceğiz ki bir sonlu grubun her altgrubunun mertebesi o grubun mertebesini böler. Bununla beraber, Teorem 2 nin önemli bir kısmı, devirli olmayan gruplar için geçerli değildir. Örneğin, öyle m doğal sayıları vardır ki, mertebesi m olan bir grup, m nin bazı pozitif bölenleri için hiç altgruba sahip olmayıp m nin bazı pozitif bölenleri için birden çok alt gruba sahip olabilir.

Son olarak şunu da belirtelim ki tüm gruplar içinde çok küçük bir sınıf oluşturmalarına karşın, devirli gruplar, sonlu Abel grupları için, aynen asal sayıların tamsayılara yapıtaşı rolü oynadıkları gibi, yapıtaşı rolü oynarlar.