

Bölüm 4

DEVİRLİ GRUPLAR

Bu bölümde tek eleman tarafından üretilen grupları inceleyeceğiz. Bir grubun devirli olması halinde üreteçlerinin ve alt gruplarının bulunması ile ilgili yöntemleri vereceğiz.

4.1 Devirli Gruplar

$(\mathbb{Z}, +)$ grubunu gözönüne aldığımızda bu grubun elemanlarından sıfır hariç, diğer bütün elemanlar 1 sayısından elde edilebilir. Yani, $n = (1+1+\dots+1)$ ve $-n = -(1+1+\dots+1)$ şeklinde n tane 1 sayısının toplamıdır. Böylece, 1 sayısı $(\mathbb{Z}, +)$ grubunun üreteçidir. Bir x tamsayısını çarpmaya göre n kez yanyana çarparak x^n şeklinde elde edebiliriz.

Tanım (Devirli Alt Grup): G bir grup ve $g \in G$ olsun.

$$\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \} = \{ \dots, \bar{a}^k, \dots, \bar{a}^{-1}, a^0 = 1_G, a, \dots, a^k, \dots \}$$

alt grubuna a tarafından üretilen alt grup denir. Eğer $H < G$ ve $H = \langle b \rangle$ olacak şekilde $b \in G$ varsa H ya b tarafından üretilen devirli alt grup denir.

Özel olarak $G = \langle a \rangle$ olacak şekilde $a \in G$ varsa G ye a tarafından üretilen devirli grup denir.

Tanım (Üreteç): G bir grup ve $a \in G$ olsun. Eğer $G = \langle a \rangle$ ise a ya G grubunun üreteci denir.

Örnek: $(\mathbb{Z}, +)$ grubu, 1 ve -1 tamsayıları ile üretildiğinden yani; $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ olduğundan devirli bir gruptur.

Örnek: $2\mathbb{Z} = \langle 2 \rangle \subset \mathbb{Z}$ olduğundan çift tamsayıların kümesi, tamsayıların devirli bir alt grubudur.

Benzer şekilde $\forall n \geq 2$ için $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$ kümeleri de $\mathbb{Z}$ nin devirli alt gruplarıdır.

Örnek: $H = \{ \bar{2}, \bar{4}, \bar{6}, \bar{8} \} \subseteq \mathbb{Z}_{10}$ değişmeli grubu,

$\bar{2} + \bar{2} = \bar{4}$, $\bar{2} + \bar{2} + \bar{2} = \bar{6}$, $\bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{8}$ olduğundan $\bar{2}$ ile üretilen bir alt gruptur. Yani; $H = \langle \bar{2} \rangle$ dir.

Teorem: G grubunun bir üretici a ise, G nin diğer bir üretici de a^{-1} dir.

İspat: $x \in G \Rightarrow x = a^k = (a^{-1})^{-k} \in \langle a^{-1} \rangle \Rightarrow G \subset \langle a^{-1} \rangle$ dir. Tersine $x \in \langle a^{-1} \rangle$ olsun. Bu durumda $x = (a^{-1})^k = a^{-k} \in \langle a \rangle \subset \langle a^{-1} \rangle \subset G$ dir. Böylece $G = \langle a^{-1} \rangle$ elde edilir.

Tanım ($\langle a^m \rangle$ Alt Grubu): $G = \langle a \rangle$, $o(G)=n$ ninci mertebeden devirli bir grup ise, her alt grubunun mertebesi n nin bir pozitif bölenidir ve n nin her pozitif k böleni için G kesinlikle k mertebeden bir tek alt gruba sahiptir ve bu alt grup $H = \langle a^{\frac{n}{k}} \rangle = \langle a^m \rangle$ dir.

Örnekler: 1) $(\mathbb{Z}, +)$ grubu, 1 ile üretilmiş sonsuz devirli bir gruptur.

2) $\mathbb{Z}_4$ devirli bir gruptur ve üreteçleri 1 ve 3 dür. $\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4$
 $(k, 4) = 1$ olması g.v.y.k dur.

Önerme 4.1.1 Devirli bir grubun her alt grubu da devirlidir.

İspat: $G = \langle a \rangle$ bir devirli grup ve $H < G$ olsun. i) Eğer $H = \{1_G\}$ veya $H = G$ ise bu aşık alt gruplar da devirlidir. ii) $H \neq \{1_G\}$, G ise: H da en az bir a^m ($m \in \mathbb{Z} - \{0\}$) elemanı vardır. Bir $m > 0$ en küçük tamsayısı için, $a^m \in H$ ve $a^{-m} \in H$ dir. En küçük eleman prensibine göre $a^m \in H$ koşuluna uyan bütün $m \in \mathbb{N}$ lerin μ gibi bir en küçüğü vardır. Şimdi $H = \langle a^\mu \rangle$ olduğunu gösterelim.

H nin herhangi bir $x = a^n \in H$ elemanını gözönüne alalım. n, μ çiftine ait bölme algoritması

$$n = \mu q + r, \quad 0 \leq r < \mu$$
 olduğundan;

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

elde edilir. ($a^\mu \in H$ ve H bir grup olduğundan $(a^\mu)^{-q} \in H$ dir. $a^n \in H$ ve $(a^\mu)^{-q} \in H$ dan $(a^\mu)^{-q} a^n \in H$, yani $a^r \in H$ sonucu çıkar.) Burada $r \neq 0$ olamaz, çünkü aksi halde

$0 \leq r < \mu$ ve $a^r \in H$ olur ki, bu μ nün tanımına aykırıdır. O halde $r = 0$ olmak zorundadır. Buna göre $x = a^n = (a^\mu)^q \in \langle a^\mu \rangle$ elde edilir, yani $H \subset \langle a^\mu \rangle$ (*) dür.

Tersine, $a^\mu \in H$ ve H bir grup olduğundan a^μ nin bütün kuvvetleri de H ya aittir.

O halde $\langle a^\mu \rangle \subset H$ $(**)$ dir.

Böylece $(*)$ ve $(**)$ dan $H = \langle a^\mu \rangle$ elde edilir.

Sonuç: $G = \langle a \rangle$ n. mertebeden bir devirli bir grup ve H da G nin a^μ tarafından üretilmiş alt grubu ise yani, $H = \langle a^\mu \rangle$ ise bir $v \in \mathbb{N}$ için $n = \mu v$ olup, $|H| = v$ dür.

Önerme 4.1.2 $G = \{1_G, a, a^2, \dots, a^{\mu-1}\}$ devirli grubunda aşağıdaki özellikler geçerlidir: $o(G) = \mu$ dir.

i) $s \in \mathbb{Z}$ olmak üzere,

$$a^s = 1_G \Leftrightarrow \mu \mid s \text{ dir.}$$

ii) $m, n \in \mathbb{Z}$ olmak üzere,

$$a^m = a^n \Leftrightarrow m \equiv n \pmod{\mu} \text{ dir.}$$

İspat: i) $\mu \mid s$ ise $s = \mu s'$ ($s' \in \mathbb{Z}$) olup, $a^s = a^{\mu s'} = (a^\mu)^{s'}$ yazılabilir ve $a^\mu = 1_G$ olduğundan buradan $a^s = 1_G$ elde edilir.

Tersine, $a^s = 1_G$ ise ve s, μ çiftine ait bölme algoritması

$$s = \mu q + r, \quad 0 \leq r < \mu$$

şeklinde ise

$$\underbrace{a^s}_{1_G} = a^{\mu q + r} = \underbrace{(a^\mu)^q}_{1_G} a^r = a^r$$

den $a^r = 1_G$ elde edilir. Ancak bu eşitliği sağlayan en küçük pozitif tamsayı μ olduğundan $r = 0$ olmalıdır. Yani, $\mu \mid s$ dir.

ii) $a^m = a^n \Leftrightarrow a^{m-n} = 1_G$ dir. i) ye göre $a^{m-n} = 1_G \Leftrightarrow \mu \mid m - n$ ve kongrüans tanımına göre de

$$\mu \mid m - n \Leftrightarrow m \equiv n \pmod{\mu}$$

dur. Böylece $a^m = a^n \Leftrightarrow m \equiv n \pmod{\mu}$ elde edilir.

Sonuç: Sonlu bir G devirli grubunda her H alt grubunun mertebesi, G nin mertebesini böler.

İspat:

i) $H = \{1_G\}$ ise iddia doğrudur.

ii) $H \neq \{1_G\}$ ise $H = \langle a^\mu \rangle$ olup, $|G| = n$ ve $|H| = v$ olmak üzere, $n = \mu v$ dür, yani $o(H) \mid o(G)$ dir.

Önerme 4.1.3 $G = \langle a \rangle$, n inci mertebeden devirli bir grup olsun. a^s nin G nin bir üretici olması için g.v.y.k $(s, n) = 1$ olmasıdır.

İspat: $G = \{a, a^2, a^3, \dots, a^n = e\}$ ve a^s , G nin bir üretici ise $(s, n) = 1$ dir:
 $G = \langle a \rangle = \langle a^s \rangle$ olduğundan,.

$$a \in \langle a^s \rangle \Rightarrow a = (a^s)^t \text{ olacak şekilde } \exists t \in \mathbb{Z} \text{ vardır. } st \equiv 1 \pmod{n}$$

$$a^{st-1} = e \Rightarrow n \mid st - 1$$

dir. O halde $\exists y \in \mathbb{Z}$ için $st - 1 = ny \Rightarrow st - ny = 1 \Rightarrow (s, n) = 1$ elde edilir.

Tersine, $(s, n) = 1$ olsun. $\exists x, y \in \mathbb{Z}$ için $sx + ny = 1$ yazılır. $a^n = e$ den dolayı

$$a = (a^s)^x \cdot (a^n)^y = a^{sx} \cdot e^y = a^{sx} \cdot e = a^{sx} = (a^s)^x \Rightarrow a \in \langle a^s \rangle$$

elde edilir. $G = \langle a \rangle \subset \langle a^s \rangle$ ve $a^s \in \langle a \rangle \Rightarrow \langle a^s \rangle \subset \langle a \rangle = G$

den $G = \langle a \rangle = \langle a^s \rangle$ elde edilir.

Sonuç: Eğer n inci mertebeden sonlu devirli bir G grubunun üretici a ise, o zaman G nin diğer üreteçleri $(r, n) = 1$ olacak şekilde a^r formundaki elemanlardır.

Önerme 4.1.4 $G = \langle a \rangle$, n inci mertebeden devirli bir grup olsun. d , n nin bir pozitif böleni olsun. Bu durumda G nin d inci mertebeden bir tek H alt grubu vardır.

İspat: $G = \{1_G, a, a^2, a^3, \dots, a^{n-1}\}$ olsun. Eğer $d = 1$ veya $d = n$ ise önermenin doğruluğu açıktır.

$1 < d < n$ olsun. $d \mid n$ ise $n = m d$ olacak şekilde bir $m \in \mathbb{N}$ vardır ve a^m tarafından üretilen H alt grubunun mertebesi d dir.yani; $\langle a^m \rangle$ devirli grubunun mertebesi d dir. Öte yandan, n ve d verilmiş olduğundan H nin üreticinin m üssü, $\frac{n}{d} = m$ olarak tek türlü belirlidir. O halde $H = \langle a^m \rangle$, G nin d . mertebeden tek alt grubudur.

Sonuç: $G = \langle a \mid a^n = e \rangle$ olsun. n nin pozitif bir böleni d olmak üzere G nin bütün farklı alt grupları $\langle a^d \rangle$ şeklindedir.

Önerme 4.1.5 G grubu a tarafından üretilen ve mertebesi n olan devirli bir grup, yani $G = \langle a \mid a^n = e \rangle$ olsun. Herhangi bir $m \in \mathbb{Z}$ için $d = \text{ebob}(m, n)$ olmak üzere $\langle a^d \rangle = \langle a^m \rangle$ dir.

İspat: $d = \text{ebob}(m, n)$ ise $d = m x + n y$ olacak şekilde $x, y \in \mathbb{Z}$ vardır.
 $a^d = a^{mx+ny} = a^{mx} a^{ny} = a^{mx} e = (a^m)^x$ olduğundan $a^d \in \langle a^m \rangle$ ve dolayısıyla $\langle a^d \rangle \subseteq \langle a^m \rangle$ dir.

Tersine $x \in \langle a^m \rangle$ olsun. $d = \text{ebob}(m, n)$ olduğundan $m = d p$ olacak şekilde $p \in \mathbb{Z}$ vardır. $x = (a^m)^k = (a^{dp})^k = (a^d)^{pk}$ yazılabildiğinden $x \in \langle a^d \rangle$ dir. Böylece $\langle a^m \rangle \subseteq \langle a^d \rangle$ olup, $\langle a^d \rangle = \langle a^m \rangle$ elde edilir.

Örnek: $G = \langle a \mid a^{20} = e \rangle$ devirli grubunda $4 = \text{ebob}(8, 20)$ olduğundan $\langle a^4 \rangle = \langle a^8 \rangle$ dür.

Önerme 4.1.6 $G = \langle a \rangle$ sonsuz devirli bir grup ise üreteçleri a ve a^{-1} dir.

İspat: a^s , G nin bir üretici ise $(a^s)^x = a$ olacak şekilde $\exists x \in \mathbb{Z}$ bulunabilir. $G = \langle a \rangle$ sonsuz devirli bir grup olduğundan, $s x = 1 \Rightarrow s = \pm 1$ elde edilir. Dolayısıyla a ve a^{-1} üreteçlerdir.

Önerme 4.1.7 Her devirli grup abelyendir.

İspat: G devirli bir grup ve $G = \langle a \mid a^n \mid n \in \mathbb{Z} \rangle$ olacak şekilde G nin bir üretici a olsun. Eğer G nin iki elemanı g_1 ve g_2 ise, $g_1 = a^r$ ve $g_2 = a^s$ olacak şekilde r ve s tamsayıları mevcuttur. O zaman,

$$g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1$$

olur. Böylece G abelyen (değişmeli grup) dir.

Tanım (Grubun Üssü veya Eksponenti): sonlu bir G grubunun elemanlarının en küçük üst sınırına grubun üssü (veya eksponenti) denir. Yani; $\forall a \in G$ için $a^t = 1_G$ koşuluna uyan $t \in \mathbb{N}$ lerin en küçüğüne G grubunun eksponenti denir.

Sonuç: G sonlu bir grup ve $|G| = N$ ise $\forall a \in G$ için $a^N = 1_G$ dir.

Önerme 4.1.8 Mertebesi asal olan her grup, devirlidir.

İspat: G bir grup, $|G| = p$ asal ve $a \in G - \{1_G\}$ olsun. Sonlu bir G grubunda her a elemanının mertebesi, G nin mertebesini böldüğünden $|a|$, p nin bir böleni olacağından ya 1 ’ e veya p ye eşittir. $a \neq 1_G$ olduğundan $|a| \neq 1$ dir; şu halde $|a| = p$ olmak zorundadır, yani

$$G = \langle a \rangle = \{1_G, a, \dots, a^{p-1}\}$$

dir.

Önerme 4.1.9 p asal tamsayı ise $Z_p^* = Z_p - \{\bar{0}\}$ bir devirli gruptur.

İspat: $Z_p^* = Z_p - \{\bar{0}\}$ grubunun üssü g olsun. Fermat teoreminden $p \nmid a$ iken $\forall a \in Z_p^*$ için $a^{p-1} \equiv 1 \pmod{p}$ olduğundan, yani, $\bar{a}^{p-1} = \bar{1}$ den $g \leq p-1$ dir. Aynı zamanda $\forall a \in Z_p^*$ için $o(a) \mid g$ dir. Her $a \in Z_p^*$ elemanı için $o(Z_p^*) = p-1$ den $p-1 \leq g$ elde edilir.

Böylece $g = p-1$ ve $Z_p^* = Z_p - \{\bar{0}\}$ grubunda mertebesi $p-1$ olan bir eleman bulunacağından bu grup devirlidir.

Sonuç: p asal tamsayı ise $Z_p^* = Z_p - \{\bar{0}\}$ grubu $p-1$ inci mertebeden bir devirli grupur.

4.2 Devirli Grup Örnekleri

Örnek 1 Z_{10}^* in bir devirli grup olduğunu gösteriniz.

Çözüm: $Z_{10}^* = \{1, 3, 7, 9\}$ elemanlarından oluşan, mertebesi $\Phi(10) = \Phi(2) \cdot \Phi(5) = 4$ olan bir gruptur.

$(a, 10) = 1$ ise $a \equiv 1 \pmod{2}$, $a^4 \equiv 1 \pmod{5}$ ve $a^4 \equiv 1 \pmod{10}$ 'i sağlayan a lar aranır.

$3^1 = 3, 3^2 = 9, 3^3 = 7, 3^4 \equiv 1 \pmod{10}$ sağlandığından üreteç 3 tür.

$\langle 3 \rangle = \{1, 3, 7, 9\} = Z_{10}^*$ dır. Yani devirli bir gruptur.

Örnek 2 Z_{15}^* in bir devirli grup olmadığını gösteriniz.

Çözüm: Z_{15}^* mertebesi $\Phi(15) = \Phi(3) \cdot \Phi(5) = 2 \cdot 4 = 8$ olan bir gruptur.

$Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ elemanlarından oluşur.

$(a, 15) = 1$ ise $a^2 \equiv 1 \pmod{3}$, $a^4 \equiv 1 \pmod{5}$ ve $a^8 \equiv 1 \pmod{15}$ 'i sağlayan a lar aranır.

$2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 \equiv 1 \pmod{15}$ dolayısıyla $2^8 \equiv 1 \pmod{15}$ sağlanmasına rağmen

$\langle 2 \rangle = \{1, 2, 4, 8\} < Z_{15}^*$ dır. Yani tüm elemanlarını içermediğinden bir üreteç değildir.

Dolayısıyla devirli grup değildir.

Örnek 3 $G = \langle a \rangle$, 20. mertebeden bir devirli grup ise bütün üreteçlerini ve alt gruplarını bulunuz.

Çözüm: $o(a) = 20$ olsun. $G = \langle a \rangle$ nın üreteçleri sayısı Euler Φ fonksiyonuna göre $\Phi(n)$ tanedir. Yani; $\Phi(20) = \Phi(4 \cdot 5) = \Phi(2^2) \cdot \Phi(5) = 2 \cdot 4 = 8$ tanedir.

Bunlar, $(r, 20) = 1$ ve $1 \leq r < 20$ olmak üzere a^r ler, yani üreteçler kümesi

$$\{a, a^3, a^7, a^9, a^{11}, a^{13}, a^{17}, a^{19}\}$$

dir. $t = 20$, $t = sq$, $\exists q \in \mathbb{Z}$ olacak şekilde $\langle a^s \rangle$ alt grupları mevcuttur. Bunlar,

$\langle a \rangle$, $\langle a^2 \rangle$, $\langle a^4 \rangle$, $\langle a^5 \rangle$, $\langle a^{10} \rangle$ ve $\langle a^{20} \rangle$ dir.

Örnek 4 20. mertebeden bir devirli grubun tüm alt gruplarını elemanları ile birlikte bulunuz.

Çözüm: $\text{o}(a) = 20$ ve $G = \langle a \rangle$ olsun. $H < G$ olmak üzere $H = \langle a^k \rangle$, $k | n$ den dolayı $k | 20$ olmak üzere $k = 1, 2, 4, 5, 10, 20 | 20$ için

$$\begin{aligned} H = \langle a \rangle &= \{a, a^2, \dots, a^{19}, a^{20} = e\} \\ H = \langle a^2 \rangle &= \{a^2, a^4, \dots, a^{18}, a^{20} = e\} \\ H = \langle a^4 \rangle &= \{a^4, a^8, a^{12}, a^{16}, a^{20} = e\} \\ H = \langle a^5 \rangle &= \{a^5, a^{10}, a^{15}, a^{20} = e\} \\ H = \langle a^{10} \rangle &= \{a^{10}, a^{20} = e\} \\ H = \langle a^{20} \rangle &= \{a^{20} = e\} \end{aligned}$$

elde edilir.

Örnek 5 $(Z_{11}^*, \cdot)$ grubunun alt gruplarını ve üreteçlerini bulalım.

$$Z_{11}^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}\} = \{1, 2, 3, 4, 5, -5, -4, -3, -2, -1\} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$$

$$\begin{aligned} 2^1 &= 2, 2^2 = 4, 2^3 = 8 = -3, 2^4 = 16 = 5, 2^5 = 10 = -1, 2^6 = 9 = -2, 2^7 = 7 = -4, \\ 2^8 &= 3, 2^{10} = 6 = -5, 2^{11} = 1 \Rightarrow \langle 2 \rangle = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\} \end{aligned}$$

$$3^1 = 3, 3^2 = 9 = -2, 3^3 = 5, 3^4 = 4, 3^5 = 1 \Rightarrow \langle 3 \rangle = \{1, 3, 4, 5, 9\}$$

$$4^1 = 4, 4^2 = 5, 4^3 = 9 = -2, 4^4 = 3, 4^5 = 1 \Rightarrow \langle 4 \rangle = \{1, 3, 4, 5, 9\}$$

$$5^1 = 5, 5^2 = 3, 5^3 = 4, 5^4 = 9 = -2, 5^5 = 1 \Rightarrow \langle 5 \rangle = \{1, 3, 4, 5, 9\}$$

$$\begin{aligned} 6^1 &= 6 = -5, 6^2 = 3, 6^3 = 7 = -4, 6^4 = -2, 6^5 = -1, 6^6 = -6 = 5, 6^7 = 8 = -3, \\ 6^8 &= 4, 6^9 = 2, 6^{10} = 1 \Rightarrow \langle 6 \rangle = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\} \end{aligned}$$

$$\begin{aligned} 7^1 &= 7 = -4, 7^2 = 5, 7^3 = 2, 7^4 = 3, 7^5 = -1, 7^6 = 4, 7^7 = 6 = -5, \\ 7^8 &= -2, 7^9 = -3, 7^{10} = 1 \Rightarrow \langle 7 \rangle = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\} \end{aligned}$$

$$\begin{aligned} 8^1 &= 8 = -3, 8^2 = -2, 8^3 = -5, 8^4 = 4, 8^5 = -1, 8^6 = 3, 8^7 = 2, 8^8 = 5, 8^9 = -4, 8^{10} = 1 \\ \langle 8 \rangle &= \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\} \end{aligned}$$

$$9^1 = 9 = -2, 9^2 = 4, 9^3 = 3, 9^4 = 5, 9^5 = 1 \Rightarrow \langle 9 \rangle = \{1, 3, 4, 5, 9\}$$

$$10^1 = -1, 10^2 = 1 \Rightarrow \langle 10 \rangle = \{\pm 1\}$$

O halde üreteçleri $Z_{11}^* = \langle 2 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 8 \rangle$ bulunur.

$o(Z_{11}^*) = 10$ olduğundan, alt grupları $d \mid 10$ olmak üzere, $\langle 2^d \rangle$ şeklindedir. Yani; $d = 1, 2, 5, 10$ olmak üzere Z_{11}^* in alt grupları $\langle 2^1 \rangle, \langle 2^2 \rangle, \langle 2^5 \rangle, \langle 2^{10} \rangle$, $\langle 6^1 \rangle, \langle 6^2 \rangle, \langle 6^5 \rangle, \langle 6^{10} \rangle$, $\langle 7^1 \rangle, \langle 7^2 \rangle, \langle 7^5 \rangle, \langle 7^{10} \rangle$ ve $\langle 8^1 \rangle, \langle 8^2 \rangle, \langle 8^5 \rangle, \langle 8^{10} \rangle$ şeklindedir.

Örnek 6 20. mertebeden bir devirli grubun tüm üreteçlerini bulunuz.

Çözüm: $o(a) = 20$ ve $G = \langle a \rangle$ devirli bir grup olsun. a^k elemanının G nin bir üreteci olması için g.v.y.k. $(k, n) = 1$ olmalıdır. O halde G nin üreteçleri $(k, 20) = 1$ olmak üzere a^k elemanlarıdır. O zaman G nin üreteçleri

$$\{a, a^3, a^7, a^{11}, a^{13}, a^{17}, a^{19}\}$$

elemanlarıdır.

Örnek 7 $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ kuaterniyonlar grubunun bütün üreteçlerini bulunuz.

Çözüm:

$$o(1) = 1$$

$$o(i) = o(j) = o(k) = 4$$

$$o(-1) = 2$$

$$o(-i) = o(-j) = o(-k) = 4$$

olup, Q_8 grubunun mertebesi 8 olan elemanı olmadığından bu grup devirli değildir.

Örnek 8 $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ kuaterniyonlar grubunun üreteci $Q_8 = \langle i, j \rangle$ midir?

Çözüm:

$$1 = i^4 = j^4 \quad -1 = i^2$$

$$i = i \quad -i = i^3$$

$$j = j \quad -j = j^3$$

$$k = ij \quad -k = ji$$

olduğundan $Q_8 = \langle i, j \rangle$ dir. Aynı zamanda $Q_8 = \langle i, k \rangle$ ve $Q_8 = \langle j, k \rangle$ dir.

Örnek 9 $Z_{20}^* = \{ x \in Z_{20} \mid (x, 20) = 1 \}$ çarpım grubunun biri devirli diğeri devirli olmayan 4 ncü mertebeden iki alt grubunu bulunuz.

Çözüm: $Z_{20}^* = \{ x \in Z_{20} \mid (x, 20) = 1 \} = \{ 1, 3, 7, 9, 11, 13, 17, 19 \} = \{ \pm 1, \pm 3, \pm 7, \pm 9 \}$

$$3^1 = 3, 3^2 = 9, 3^3 = 7, 3^4 = 1 \Rightarrow \langle 3 \rangle = \{ 1, 3, 7, 9 \}$$

$$7^1 = 7, 7^2 = 9, 7^3 = 3, 7^4 = 1 \Rightarrow \langle 7 \rangle = \{ 1, 3, 7, 9 \}$$

$$9^1 = 9, 9^2 = 1 \Rightarrow \langle 9 \rangle = \{ 1, 9 \}$$

olduğundan, bu grup üretece sahip değildir. Çünkü 20 asal sayı değildir. Fakat devirli alt grupları olabilir.

$H = \langle 3 \rangle = \{ 1, 3, 7, 9 \}$ 4-elemanlı bir alt grup olup, devirlidir.

$K = \{ -1, -9, 1, 9 \}$ ise 4-elemanlı bir alt grup olup, devirli değildir.

Örnek 10 $H = \langle a \rangle$ ve $K = \langle b \rangle$ grupları $(m, n) = 1$ olmak üzere sırasıyla m inci ve n inci mertebeden devirli gruplar olsun. $H \times K = \langle a, b \rangle$ grubunun mn inci mertebeden devirli bir grup olduğunu gösteriniz.

Çözüm: $o(H) = m$, $o(K) = n$ ve $(a, b) \in H \times K$, $(e, e') \in (H \times K)$, $o(H \times K) = d$ olsun.

$$(a, b)^{mn} = (a^{mn}, b^{mn}) = ((a^m)^n, (b^n)^m) = (e, e') \Rightarrow d \mid mn$$

$$(e, e') = (a, b)^d = (a^d, b^d) \Rightarrow m \mid d \text{ ve } n \mid d, (m, n) = 1 \Rightarrow mn \mid d$$

Buradan $(m, n) = d$ elde edilir. Böylece $H \times K = \langle a, b \rangle$ nin mertebesi $o(H \times K) = mn$ dir.

Örnek 11 n inci mertebeden bir devirli grubun üreteçlerinin sayısının tam $\Phi(n)$ tane olduğunu gösteriniz.

Çözüm: $G = \langle a \rangle$ grubu n. mertebeden bir devirli grup olsun. a^k elemanının G nin üreteci olması için g.v.y.k. $(k, n) = 1$ olmasından dolayı böyle k ların sayısı yani G nin üreteçlerinin sayısı tam $\Phi(n)$ tanedir. Çünkü, $\Phi(n)$, $n \in \mathbb{Z}^+$ olmak üzere 1 ile n arasındaki (1 dahil) n ile aralarında asal olan sayıların sayısıdır.

Örnek 12 $n = 4, 6, 8, 12, 24$ için n. mertebeden devirli grubunun bütün üreteçlerini bulunuz ve alt gruplar şemasını yapınız.

Çözüm: 1) $n=4$ için $G = \{1_G, a, a^2, a^3\}$, $H < G \Rightarrow H = \langle a^\mu \rangle$, $4 = \mu v$, $|H| = v$

$$v|4 \Rightarrow v=1, 2, 4$$

$$v=1: H_1 = \{1_G\}$$

$$v=2: \mu=2, H_2 = \langle a^2 \rangle = \{1_G, a^2\}$$

$$v=4: \mu=1, H_4 = \langle a \rangle = \{1_G, a, a^2, a^3\} = G$$

G nin üreteçleri : a, a^3

2) $n=6$ için $G = \{1_G, a, a^2, a^3, a^4, a^5\}$, $H < G \Rightarrow H = \langle a^\mu \rangle$, $6 = \mu v$, $|H| = v$

$$v|6 \Rightarrow v=1, 2, 3, 6$$

$$v=1: H_1 = \{1_G\}$$

$$v=2: \mu=3, H_2 = \langle a^3 \rangle = \{1_G, a^3\}$$

$$v=3: \mu=2, H_3 = \langle a^2 \rangle = \{1_G, a^2, a^4\}$$

$$v=6: H_6 = \langle a \rangle = \{1_G, a, a^2, a^3, a^4, a^5\} = G$$

G nin üreteçleri : a, a^5

3) $n=8$ için $G = \{1_G, a, a^2, a^3, a^4, a^5, a^6, a^7\}$, $H = \langle a^\mu \rangle$, $8 = \mu v$, $|H| = v$

$$v|8 \Rightarrow v=1, 2, 4, 8$$

$$v=1: H_1 = \{1_G\}$$

$$v=2: \mu=4, H_2 = \langle a^4 \rangle = \{1_G, a^4\}$$

$$v=4: \mu=2, H_4 = \langle a^2 \rangle = \{1_G, a^2, a^4, a^6\}$$

$$v=8: H_8 = \langle a \rangle = \{1_G, a, a^2, a^3, a^4, a^5, a^6, a^7\} = G$$

G nin üreteçleri : a, a^3, a^5, a^7

4) $n=12$ için $G = \{1_G, a, a^2, a^3, a^4, \dots, a^{11}\}$, $H = \langle a^\mu \rangle$, $12 = \mu v$, $|H| = v$

$$v|12 \Rightarrow v=1, 2, 3, 4, 6, 12$$

$$v=1: H_1 = \{1_G\}$$

$$\begin{aligned}
v=2 : \mu=6, H_2 = \langle a^6 \rangle &= \{1_G, a^6\} \\
v=3 : \mu=4, H_3 = \langle a^4 \rangle &= \{1_G, a^4, a^8\} \\
v=4 : \mu=3, H_4 = \langle a^3 \rangle &= \{1_G, a^3, a^6, a^9\} \\
v=6 : \mu=2, H_6 = \langle a^2 \rangle &= \{1_G, a^2, a^4, a^6, a^8, a^{10}\} \\
v=12 : H_{12} = \langle a \rangle &= \{1_G, a, a^2, a^3, a^4, \dots, a^{11}\} = G
\end{aligned}$$

G nin üreteçleri : a, a^5, a^7, a^{11}

$$5) \quad n=24 \text{ için } G = \{1_G, a, a^2, a^3, a^4, \dots, a^{23}\}, H = \langle a^\mu \rangle, 24 = \mu v, |H| = v$$

$$v | 24 \Rightarrow v = 1, 2, 3, 4, 6, 8, 12, 24$$

$$\begin{aligned}
v=1 : H_1 &= \{1_G\} \\
v=2 : \mu=12, H_2 = \langle a^{12} \rangle &= \{1_G, a^{12}\} \\
v=3 : \mu=8, H_3 = \langle a^8 \rangle &= \{1_G, a^8, a^{16}\} \\
v=4 : \mu=6, H_4 = \langle a^6 \rangle &= \{1_G, a^6, a^{12}, a^{18}\} \\
v=6 : \mu=4, H_6 = \langle a^4 \rangle &= \{1_G, a^4, a^8, a^{12}, a^{16}, a^{20}\} \\
v=8 : \mu=3, H_8 = \langle a^3 \rangle &= \{1_G, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}\} \\
v=12 : \mu=2, H_{12} = \langle a^2 \rangle &= \{1_G, a^2, a^4, a^6, a^8, a^{10}, a^{12}, \dots, a^{22}\} \\
v=24 : H_{24} = \langle a \rangle &= \{1_G, a, a^2, a^3, a^4, \dots, a^{23}\} = G
\end{aligned}$$

$$2 | 4, 6, 8, 12 \Rightarrow H_2 \subset H_4, H_6, H_8, H_{12}$$

$$3 | 6 | 12 \Rightarrow H_3 \subset H_6 \subset H_{12}$$

$$4 | 8, 12 \Rightarrow H_4 \subset H_8 \subset H_{12}$$

G nin üreteçleri : $a, a^5, a^7, a^{11}, a^{13}, a^{17}, a^{19}, a^{23}$

Örnek 13 G değişmeli bir grup ve $a, b \in G$ olsun.

$o(a) = m, o(b) = n$ ve $(m, n) = 1$ ise $o(ab) = mn$ olduğunu gösteriniz.

$$\text{Çözüm: } (ab)^{mn} = a^{mn} b^{mn} = e \Rightarrow o(ab) = k | mn$$

$$e = (ab)^{kn} = a^{kn} b^{kn} = a^{kn} \Rightarrow o(a) = m | kn \Rightarrow m | k$$

$$e = (ab)^{km} = a^{km} b^{km} = b^{km} \Rightarrow o(b) = n | km \Rightarrow n | k$$

eşitliklerinden $k = mn$ elde edilir.

Örnek 14 G bir grup ve $a \in G$ ise $o(a) = o(a^{-1})$ olduğunu gösteriniz.

Çözüm: $a \in G$, $o(a) = n$ ve $o(a^{-1}) = m$ olsun. Önerme 1.5.2 ye göre

$$\begin{aligned} o(a) = n &\Rightarrow a^n = e \Rightarrow (a^n)^{-1} = a^{-n} = (a^{-1})^n = e \Rightarrow m = o(a^{-1}) | n \\ o(a^{-1}) = m &\Rightarrow a^{-m} = e \Rightarrow (a^{-m})^{-1} = a^m = e \Rightarrow n = o(a) | m \end{aligned}$$

olur. O halde $m = n$ dir.

Bölüm 5

HOMOMORFİZMALAR VE İZOMORFİZMALAR

Bu bölümde verilen iki grubun cebirsel yapılarını karşılaştıracacağız. Eş yapıda olmasını gerektiren koşulları inceleyeceğiz.

5.1 HOMOMORFİZMALAR

Tanım: (G, o) ve (H, o) iki grup olsun. Her $a, b \in G$ elemanları için $f(aob) = f(a)of(b)$ oluyorsa, $f: (G, o) \rightarrow (H, o)$ dönüşümüne **grup morfizması** denir.

Tanım (Homomorfizma): Eğer her iki grup üzerindeki işlemler farklı ise yani, $(G, *)$ ve (H, o) iki grup ve her $a, b \in G$ için $f(a * b) = f(a)of(b)$ oluyorsa, $f: (G, *) \rightarrow (H, o)$ dönüşümüne de **homomorfizma** denir.

$f: (G, *) \rightarrow (H, o)$ **homomorfizmasının** oluşumu aşağıdaki diagramda gösterilmiştir.

$$\begin{array}{ccc} (a, b) & \xrightarrow{*} & a * b \\ \downarrow & & \downarrow \\ f & & f \\ \downarrow & & \downarrow \\ f(a), f(b) & \xrightarrow{o} & f(a) \circ f(b) = f(a * b) \end{array}$$

Önerme 5.1.1 $f: G \rightarrow H$ dönüşümü bir grup morfizması olsun. O zaman,

- i) G ve H gruplarının birim elemanları e_G ve e_H ise, $f(e_G) = e_H$
- ii) $\forall a \in G$ elemanları için $f(a^{-1}) = [f(a)]^{-1}$ dir.

İspat:

i) $f: G \rightarrow H$ dönüşümü bir grup morfizması olduğundan,

$$f(a) = f(a \circ e_G) = f(a) \circ f(e_G) \quad \text{ve} \quad f(a) = f(e_G \circ a) = f(e_G) \circ f(a) \quad \text{den}$$

$$f(a) \circ f(e_G) = f(e_G) \circ f(a) = f(a)$$

elde edilir. Bu da, birim eleman tanımından $f(e_G)$ nin H grubunun birim elemanı olmasını gerektirir. Bir grubun birim elemanının tek olması gerektiğinden H nin birim elemanı e_H olduğundan

$$e_H = f(e_G)$$

elde edilir.

ii) $\forall a \in G$ elemanları için,

$$f(a) \circ f(a^{-1}) = f(a \circ a^{-1}) = f(e_G) = e_H$$

yazılır. $f(a)$ elemanının tek olan tersi $f(a^{-1})$ olduğundan,

$$f(a^{-1}) = [f(a)]^{-1}$$

sonucu elde edilir.

Önerme 5.1.2 $f : (G, *) \rightarrow (H, o)$ bir homomorfizma olsun.

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

İspat: i) $N < G$ olsun. $f(N) = \{f(a) \in H \mid a \in N\} < H$ olduğunu gösterelim:
 $a, b \in N$ olmak üzere $f(a), f(b) \in f(N)$ olsun.

$$f(a) \circ f(b)^{-1} = f(a) \circ f(b^{-1}) = f(\underbrace{a * b^{-1}}_{\in N}) \in f(N)$$

olur. Buradan $f(N) < H$ elde edilir.

ii) $K < H$ olsun. $f^{-1}(K) = \{a \in G \mid f(a) \in K\} < G$ olduğunu gösterelim:
 $\forall a, b \in f^{-1}(K)$ için $f(a), f(b) \in K$ ve $K < H$ olduğundan,

$$f(a) \circ f(b)^{-1} = f(a) \circ f(b^{-1}) = f(\underbrace{a * b^{-1}}_{\in f^{-1}(K)}) \in K$$

olur. Buradan $f^{-1}(K) < G$ elde edilir.

Tanım (Çekirdek): $f : (G, *) \rightarrow (H, o)$ dönüşümü bir homomorfizma olsun.

$K = \text{Ker}(f) = \{x \in G \mid f(x) = e_H\} = f^{-1}(e_H)$ kümesine, f dönüşümünün çekirdeği denir ve çekf veya Kerf şeklinde gösterilir.

Önerme 5.1.3 $f : (G, *) \rightarrow (H, o)$ dönüşümünün 1-1 olması için gerek ve yeter koşul $\text{Kerf} = \{e_G\}$ olmasıdır.

İspat: Eğer f dönüşümü 1-1 ise, $e_H \in H$ elemanına dönüşecek bir tek $e_G \in G$ elemanı vardır. Öyleyse $\text{Kerf} = \{e_G\}$ olur.

Tersine, $\text{Kerf} = \{e_G\}$ olsun ve $f(a) = f(b)$ olarak alınsın. Bu halde,

$$f(a * b^{-1}) = f(a) o [f(b)]^{-1} = f(a) o [f(a)]^{-1} = e_H \text{ ve } a * b^{-1} \in \text{Kerf} = \{e_G\}$$

olur. Böylece, $a = b$ elde edilir. Bu da $f : (G, *) \rightarrow (H, o)$ dönüşümünün 1-1 olduğunun ispatıdır.

Önerme 5.1.4 H , G nin bir normal alt grubu olsun. $f : G \rightarrow G/H$ dönüşümü $f(a) = aH$ şeklinde tanımlandığında H çekirdeği ile bir homomorfizmadır.

İspat: $a, b \in G$ olsun. O zaman,

$$f(ab) = (ab)H = (aH)(bH) = f(a)f(b)$$

dir. Yani, f bir homomorfizmadır. $a \in H$ ise $aH = H$ olduğundan, f nin çekirdeğinin H nın içinde olduğunu görürüz.

Örnek: $f : G \rightarrow H$ ve $g : H \rightarrow K$ iki homomorfizma olduğuna göre $gof : G \rightarrow K$ in de bir homomorfizma olduğunu gösteriniz.

Çözüm:

$$\begin{aligned} \forall a, b \in G \text{ için } gof(ab) &= g(f(ab)) = g(f(a)f(b)) \\ &= g(f(a))g(f(b)) = (gof)(a)(gof)(b) \end{aligned}$$

oldüğundan gof bir homomorfizmadır.

Örnek: $f : G \rightarrow G$ $f(x) = x^{-1}$ şeklinde tanımlansın. G grubu değişmeli ise f in bir homomorfizma olduğunu gösteriniz.

Çözüm: G değişmeli grup olsun. $\forall x, y \in G$ için $xy = yx$ dir. f nin bir homomorfizma olduğunu göstermeliyiz.

$$f(xy) = (xy)^{-1} = y^{-1}x^{-1}$$

oldüğundan, G nin değişmeli olduğunu kullanarak

$$f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$$

elde edilir.

Örnek: $(\mathbb{R}^+, \cdot)$ çarpımsal grubu ve $(\mathbb{R}, +)$ toplamsal grubu için $f(x) = \log x$ şeklinde tanımlı $f : \mathbb{R}^+ \rightarrow \mathbb{R}$ fonksiyonunun bir homomorfizma olduğunu gösteriniz ve $\text{Ker} f$ 'i bulunuz.

Çözüm: $x, y \in \mathbb{R}^+$ için $f(xy) = \log xy = \log x + \log y = f(x) + f(y)$ olduğundan $f : \mathbb{R}^+ \rightarrow \mathbb{R}$ fonksiyonu bir homomorfizmadır. f nin çekirdeği,

$$\text{Ker} f = \{x \in \mathbb{R}^+ : \log x = 0\} = \{1\}$$

dir.

Örnek: $f : \mathbb{Z} \rightarrow 4\mathbb{Z}$, $f(n) = 4n$ şeklinde tanımlı fonksiyonun bir homomorfizma olduğunu gösteriniz ve $\text{Ker} f$ 'i bulunuz. Çekirdek kaç elemanlıdır?

Çözüm: $n, m \in \mathbb{Z}$ için $f(n + m) = 4(n + m) = 4n + 4m = f(n) + f(m)$ olduğundan bir homomorfizmadır. Aynı zamanda f fonksiyonu 1-1 ve örtendir. Yani bir izomorfizmadır. f nin çekirdeği,

$$\text{Ker} f = \{n \in \mathbb{Z} : f(n) = 4n = 0\} = \{0\}$$

olup, çekirdek tek elemanlıdır.

Örnek: $f : (\mathbb{R}, +) \rightarrow (\mathbb{C} - \{0\}, \cdot)$, $f(t) = \cos t + i \sin t$ şeklinde tanımlı fonksiyonun bir homomorfizma olduğunu gösteriniz ve $\text{Ker} f$ 'i bulunuz.

Çözüm:

$$\begin{aligned} f(t + u) &= \cos(t + u) + i \sin(t + u) \\ &= \cos t \cos u - \sin t \sin u + i \sin t \cos u + i \cos t \sin u \\ &= (\cos t + i \sin t)(\cos u + i \sin u) \\ &= f(t) \cdot f(u) \end{aligned}$$

olup, f bir homomorfizmadır.

$$\text{Ker} f = \{t \in \mathbb{R} : f(t) = \cos t + i \sin t = 1\} = \{t = 2k\pi, k \in \mathbb{Z}\}$$

dir.

Örnek: $f : (Z, +) \rightarrow (Z_4, +)$, $f(n) = \bar{n}$ şeklinde tanımlı fonksiyonun bir homomorfizma olduğunu gösteriniz ve $\text{Ker} f$ 'i bulunuz. Çekirdek kaç elemanlıdır?

Çözüm:

$$f(n_1 + n_2) = \overline{n_1 + n_2} = \overline{n_1} + \overline{n_2} = f(n_1) + f(n_2)$$

olup, f bir homomorfizmadır.

$$\text{Ker} f = \{ n \in Z : f(n) = \bar{n} = \bar{0} \} = 4Z$$

dir. Çekirdeğin mertebesi sonsuzdur.

Örnek: $f : G \rightarrow H$ bir homomorfizma olsun.

$$\text{Im} f = \{ y \in H : y = f(x), \text{ belli bir } x \in G \text{ için} \}$$

kümesinin H nın bir alt grubu olduğunu gösteriniz.

Çözüm: $y_1, y_2 \in \text{Im} f$ olsun. $y_1 = f(x_1)$ ve $y_2 = f(x_2)$ olacak şekilde x_1 ve x_2 elemanları vardır. $y_1 y_2^{-1} \in \text{Im} f$ olduğunu göstermeliyiz.

Öyle bir x elemanı bulmalıyız ki $x = x_1 x_2^{-1} \in G$ olmak üzere $f(x) = y_1 y_2^{-1}$ olsun. f homomorfizma olduğundan,

$$f(x_1) f(x_2^{-1}) = f(x_1) f(x_2)^{-1} = y_1 y_2^{-1} = f(x_1 x_2^{-1}) \in H$$

dır. Buradan $y_1 y_2^{-1} \in \text{Im} f < H$ elde edilir.

Örnek: G ve H iki grup ve $f : G \rightarrow H$ ve $g : H \rightarrow K$ iki homomorfizma olsun. H değişmeli ise $h(a) = f(a) * g(a)$ şeklinde tanımlanan $h : G \rightarrow K$ fonksiyonunun bir homomorfizma olduğunu gösteriniz.

Çözüm:

$$\begin{aligned} \forall a, b \in G \text{ için } h(ab) &= f(ab) * g(ab) = f(a) * f(b) * g(a) * g(b) \\ &= [f(a) * g(a)] * [f(b) * g(b)] = h(a) * h(b) \end{aligned}$$

olup, h bir homomorfizmadır.

Örnek: Mutlak değer fonksiyonunun bir homomorfizma olduğunu gösteriniz. Çekirdeğini bulunuz.

Çözüm: $f : \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}^+$, $f(a) = |a|$ şeklinde tanımlandığından

$$\forall a, b \in \mathbb{R} \setminus \{0\} \text{ için } f(ab) = |ab| = |a| \cdot |b| = f(a) \cdot f(b)$$

homomorfizma olduğu görülür. Çekirdek tanımı gereği $f(a) = |a| = 1 \Rightarrow \ker f = \{-1, 1\}$ dir.

Örnek: İşaret (sgn) fonksiyonunun bir homomorfizma olduğunu gösteriniz.

Çözüm: $f : \mathbb{R} \setminus \{0\} \rightarrow \{-1, 1\}$, $x \rightarrow \begin{cases} 1, & x > 0 \\ -1, & x < 0 \end{cases}$ şeklinde tanımlandığından

$$f(xy) = \begin{cases} 1, & xy > 0 \\ -1, & xy < 0 \end{cases} = f(x) \cdot f(y) \text{ olup, bir homomorfizmadır.}$$

5.2 İzomorfizmalar

Tanım: Eğer $f : (G, *) \rightarrow (H, o)$ homomorfizması 1-1 ve örten bir dönüşüm ise, bu dönüşüme de **izomorfizma** adı verilir. Bu halde, $(G, *)$ ve (H, o) gruplarına birbirlerine **izomorftur** denir ve bu yapı $(G, *) \cong (H, o)$ sembolü ile gösterilir.

Eğer iki grubun yapıları aynı ise, bu iki gruba izomorftur denir. Örneğin, (C_4, o) grubu ile $(\{1, -1, i, -i\}, \cdot)$ grubu izomorftur.

Önerme 5.2.1 $f : (G, *) \rightarrow (H, o)$ dönüşümü bir izomorfizma olsun. e_G , G grubunun birim elemanı ise,

- i) $f(e_G) = e_H$ ve e_H H grubunun birim elemanıdır.
- ii) $\forall a \in G$ elemanları için $f(a^{-1}) = [f(a)]^{-1}$ dir.

İspat: i) $y \in H$ olsun. f dönüşümü örten olduğu için, $f(x) = y$ olacak şekilde en az bir $x \in G$ elemanı vardır. Buna göre,

$$y = f(x) = f(e_G * x) = f(e_G) o f(x) = f(e_G) o y \quad \text{ve}$$

$$y = f(x) = f(x * e_G) = f(x) o f(e_G) = y o f(e_G)$$

yazılır. Buradan $f(e_G) = e_H$ olmak zorundadır.

ii) $\forall a \in G$ elemanları için,

$$e_H = f(a^{-1} * a) = f(a^{-1}) \circ f(a)$$

ve

$$e_H = f(a * a^{-1}) = f(a) \circ f(a^{-1})$$

olduğundan, $f(a)$ elemanının tersi $f(a^{-1})$ olur. Böylece,

$$f(a^{-1}) = [f(a)]^{-1}$$

elde edilir.

Önerme 5.2.2 Aynı mertebeden devirli gruplar izomorftur.

İspat: G ve H sırasıyla g ve h elemanları tarafından üretilen devirli iki grup olsun. Eğer her iki grup da aynı mertebeden ise, r tamsayısı için $f : (G, *) \rightarrow (H, \circ)$ dönüşümü $f(g^r) = h^r$ şeklinde tanımlanır. Bu tanıma göre, f dönüşümü G ve H grupları arasında 1-1 ve örtendir. Aynı zamanda,

$$f(g^r * g^s) = f(g^{r+s}) = h^{r+s} = h^r * h^s = f(g^r) \circ f(g^s)$$

yazılabilir. Bu da f dönüşümünün bir grup izomorfizması olduğunu gösterir.

Örnek: $G \cong H$ olmak üzere, G ve H aynı mertebeden devirli gruplar olsun. $\forall a \in G$ için $o(a) = o(f(a))$ olduğunu gösteriniz.

Çözüm: $o(a) = m$ ve $o(f(a)) = n$ olsun.

$$a^m = e \Rightarrow f(a^m) = f(a)^m = f(e) = e \Rightarrow o(f(a)) = n \mid m$$

$$(f(a))^n = e \Rightarrow f(a^n) = e = f(e) \Rightarrow a^n = e, \Rightarrow o(a) = m \mid n$$

olduğundan, $m = n$ bulunur.

Örnek: G ve H iki grup olmak üzere $G \times H \cong H \times G$ olduğunu gösteriniz.

Çözüm: Bir $f : G \times H \rightarrow H \times G$ fonksiyonunu $f((a, b)) = (b, a)$ şeklinde tanımlayalım.

$\forall (a_1, b_1), (a_2, b_2) \in G \times H$ için

$$\begin{aligned} f[(a_1, b_1)(a_2, b_2)] &= f(a_1 a_2, b_1 b_2) = (b_1 b_2, a_1 a_2) \\ &= (b_1, a_1)(b_2, a_2) = f(a_1, b_1)f(a_2, b_2) \end{aligned}$$

olup, f bir homomorfizmadır.

1-1 olduğunu gösterelim: $f(a_1, b_1) = f(a_2, b_2) \Leftrightarrow (a_1, b_1) = (a_2, b_2)$ olmalıdır.

$f(a_1, b_1) = f(a_2, b_2) \Rightarrow (b_1, a_1) = (b_2, a_2) \Rightarrow b_1 = b_2$ ve $a_1 = a_2$ olduğundan 1-1 dir.

Örten olduğunu gösterelim:

$\forall (b, a) \in H \times G$ için $f(a, b) = (b, a)$ olacak şekilde $\exists (a, b) \in G \times H$ mevcuttur. f örtendir.

O halde f bir izomorfizmadır. Yani; $G \times H \cong H \times G$ dır.

Önerme 5.2.3 $f : (G, *) \rightarrow (H, o)$ bir izomorfizmasının tersi de bir izomorfizmadır.

İspat: $f^{-1} : (H, o) \rightarrow (G, *)$ ters dönüşümü $\forall a, b \in H$ için $f^{-1}(a) = a_1$, $f^{-1}(b) = b_1$ şeklinde tanımlansın. Burada $f(a_1) = a$ ve $f(b_1) = b$ dir.

$$f^{-1}(a o b) = f^{-1}[f(a_1) o f(b_1)] = f^{-1}(f(a_1 * b_1)) = a_1 * b_1 = f^{-1}(a) * f^{-1}(b)$$

olduğundan f^{-1} bir homomorfizmdir. Aynı zamanda ters dönüşümünün 1-1 ve örten olması nedeniyle f^{-1} bir izomorfizma olur.

Örnek: Her sonsuz devirli grubun $(\mathbb{Z}, +)$ grubu ile izomorf olduğunu gösteriniz.

Çözüm: $G = \langle a \rangle$ sonsuz devirli bir grup olsun. $\forall a^k \in G$ için $f(a^k) = k$ ile $f : G \rightarrow \mathbb{Z}$ fonksiyonunu tanımlayalım.

$$\forall a^s, a^t \in G \text{ için } f(a^s a^t) = f(a^{s+t}) = s + t = f(a^s) + f(a^t)$$

olduğundan, f bir homomorfizmadır.

$$f(a^s) = f(a^t) \Rightarrow s = t \Rightarrow a^s = a^t$$

olduğundan, f 1-1 dir.

$$\forall k \in \mathbb{Z} \text{ için } f(a^k) = k \text{ ve } a^k \in G \text{ olduğundan, } f \text{ örtendir.}$$