BÖLÜM 9

İZOMORFİZM VE OTOMORFİZMLER

Bu bölümü bitirdiğinizde,

- gruplarda izomorfizm ve otomorfizm kavramları
- işlem koruma özelliği
- Cayley Teoremi
- izomorfizmlerle ilgili temel özellikler
- iç otomorfizmler
- otomorfizmler grubu
- $\mathbb{Z}_n$ nin otomorfizmleri

hakkında bilgi sahibi olabileceksiniz.

BÖLÜM 9

İZOMORFİZM VE OTOMORFİZMLER

İşlem tabloları aşağıda verilmiş olan $G = \{e, a, b\}$ ve $\mathbb{Z}_3 = \{0, 1, 2\}$ gruplarını ele alalım:

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Bu tablolardan ilkinde e, a, b yerine, sırasıyla, $0, 1, 2$ yazarsak ikinci tabloyu elde ederiz. Diğer bir deyişle, $\Phi(e) = 0$, $\Phi(a) = 1$, $\Phi(b) = 2$ ile tanımlanan $\Phi : G \longrightarrow \mathbb{Z}_3$ fonksiyonu bire-bir ve örten olup her $x, y \in G$ için

$$\Phi(xy) = \Phi(x) + \Phi(y)$$

özelliğine sahiptir. Bu nedenle, G ve $\mathbb{Z}_3$ gruplarının esas itibariyle aynı olduğunu, bu gruplardan biri bilindiği takdirde diğerinin de bilindiğini söyleyebiliriz. Gruplar için temel kavramlardan biri olan izomorfizm kavramının çıkış noktası yukarıdaki gibi gözlemlerdir.

Tanım 1. G ve G' iki grup, $\Phi : G \longrightarrow G'$ bir fonksiyon olsun. Aşağıdaki iki koşul sağlanırsa, Φ ye G ile G' arasında bir *izomorfizm* denir:

(`izo.1`) Φ bire-bir ve örtendir.

(`izo.2`) Her $x, y \in G$ için $\Phi(xy) = \Phi(x)\Phi(y)$ dir.

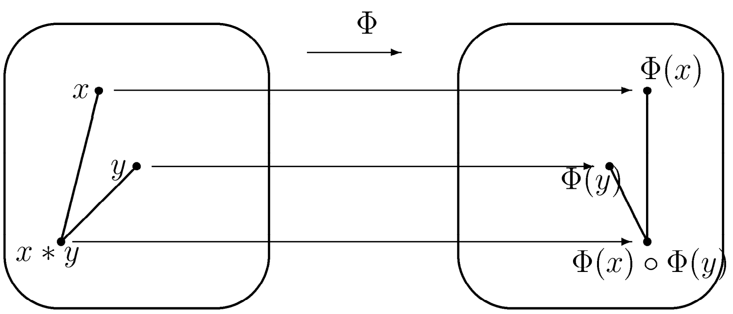
Eğer G ile G' arasında bir izomorfizm varsa, G ile G' *izomorf* gruplardır denir ve $G \cong G'$ yazılır. $\square$

Tanım 1 deki ikinci özelliğe $\Phi : G \longrightarrow G'$ fonksiyonunun *işlem koruma özelliği* denir. Bu tanımda, G ve G' her ikisi de çarpımsal grup olarak düşünülmüştür. G nin veya G' nün ikili işlemi çarpma işlemi değilse, işlem koruma özelliğinin uygun biçimde ifade edilebileceği açıktır. En genel biçimiyle, G nin ikili işlemi $*$ ve G' nün ikli işlemi $\circ$ ise, $\Phi : G \longrightarrow G'$ nün işlem koruma özelliği

$$\forall\ x, y \in G \ \text{ için } \quad \Phi(x * y) = \Phi(x) \circ \Phi(y)$$

olarak ifade edilir.

Aşağıdaki şekil, işlem koruma özelliğinin daha iyi algılanmasına yardımcı olacaktır:



Örnek 1. Bu bölümün başlangıcında verilen $\Phi : G \longrightarrow \mathbb{Z}_3$ dönüşümü, $G = \{e, a, b\}$ ile $\mathbb{Z}_3$ arasında bir izomorfizmdir. □

Örnek 2. Toplamsal $\mathbb{R}$ grubu ile çarpımsal $\mathbb{R}^+ = \{a \in \mathbb{R} : a > 0\}$ grubu izomorftur. Bunu görmek için, $\Phi : \mathbb{R} \longrightarrow \mathbb{R}^+$, $\Phi(x) = 2^x$ dönüşümünü alalım. Φ nin bire-bir ve örten olduğu bilinmektedir. Ayrıca, her $x, y \in \mathbb{R}$ için

$$\Phi(x + y) = 2^{x+y} = 2^x 2^y = \Phi(x)\Phi(y)$$

dir. Böylece, tanımdaki iki koşul sağlanır; $\mathbb{R} \cong \mathbb{R}^+$ dır. □

Örnek 3. Her sonsuz devirli grup, tamsayılar grubu $\mathbb{Z}$ ile izomorftur. Gerçekten, $G =< x >$ bir sonsuz devirli grup ise,

$$\Phi : \mathbb{Z} \longrightarrow G \quad , \quad \Phi(n) = x^n$$

ile tanımlanan Φ fonksiyonunu düşünelim. Eğer $i, j \in \mathbb{Z}$ ve $i \neq j$ ise, Teorem 4.2 nin ilk sonucuna göre $x^i \neq x^j$ olduğundan, Φ bire-birdir. Φ nin örten olduğu açık ve her $n, m \in \mathbb{Z}$ için

$$\Phi(n+m) = x^{n+m} = x^n x^m = \Phi(n)\Phi(m)$$

dir. Dolayısıyla, $\mathbb{Z} \cong G$ dir. □

Örnek 4. Mertebesi m olan her devirli grup, $\mathbb{Z}_m$ ile izomorftur. Gerçekten, $G = < x >$ ve $|G| = m$ ise, Teorem 4.3 ten $G = \{e, x, x^2, \cdots, x^{m-1}\}$ olduğunu biliyoruz. Bu durumda da,

$$\Phi : \mathbb{Z}_m \longrightarrow G \quad , \quad \Phi(n) = x^n$$

ile verilen dönüşümün bire-bir ve örten olduğu ve işlem koruduğu kolayca görülür. □

Kuşkusuz, herhangi iki grup arasındaki her bire-bir örten dönüşüm işlem koruma özelliğine sahip olmayabilir. Başka bir deyişle, gruplar arasında bire-bir örten olan; ancak, izomorfizm olmayan dönüşümler bulunabilir.

Örnek 5. $\Phi : \mathbb{R} \longrightarrow \mathbb{R}$, $\Phi(x) = x^3$ dönüşümü bire-bir ve örtendir fakat işlem koruma özelliği yoktur, çünkü $(x+y)^3 \neq x^3 + y^3$ tür. □

İki grup verildiğinde, bunların birbiri ile izomorf olup olmadıklarını belirlemek her zaman kolay değildir. Örneğin, toplamsal gruplar olarak $\mathbb{R}$ ve $\mathbb{C}$ nin izomorf oldukları bilinmektedir fakat bunun kanıtı oldukça ince teknikler gerektirir.

A. Cayley (1821-1895)'in aşağıdaki teoremi bir bakıma permütasyon gruplarının önemini ortaya koymaktadır.

Teorem 1 (Cayley) . *Her grup bir permütasyon grubu ile izomorftur.*

Kanıt. G bir grup olsun. Öyle bir G' grubu bulmak istiyoruz ki, G' nün elemanları permütasyonlar olsun ve $G \cong G'$ olsun. Elimizde G den başka bir nesne bulunmadığından, G' nün G den yola çıkılarak bulunacağı açıktır. Her $g \in G$ için

$$\sigma_g : G \longrightarrow G \quad , \quad \sigma_g(x) = gx$$

ile tanımlanan σ_g fonksiyonunun bire-bir ve örten; dolayısıyla, G nin bir permütasyonu olduğu açıktır. $G' = \{\sigma_g : g \in G\}$ kümesi, fonksiyon bileşimi (ya da permütasyon çarpımı) işlemi ile bir grup oluşturur. Gerçekten, bu grubun birim elemanının $\sigma_e = 1_G : G \longrightarrow G$, $1_G(x) = x$ olduğu ve her $g \in G$ için σ_g nin tersinin $\sigma_{g^{-1}}$ olduğu kolayca görülür. Ayrıca, $g, h \in G$ için $\sigma_{gh} = \sigma_g \sigma_h$ dir. Şimdi,

$$\Phi : G \longrightarrow G' \quad , \quad \Phi(g) = \sigma_g$$

dönüşümünün G ile G' arasında bir izomorfizm olduğunu görmek okuyucu için iyi bir alıştırma olacaktır. ∎

Yukarıdaki kanıtta oluşturulan G' grubuna G nin *sol regüler temsili* denir.

Teorem 2. *G, G', G'' gruplar, $\Phi : G \longrightarrow G'$ ve $\Psi : G' \longrightarrow G''$ izomorfizmler olsun. Bu takdirde,*

(i) $\Phi^{-1} : G' \longrightarrow G$ *bir izomorfizmdir.*

(ii) $\Psi \circ \Phi : G \longrightarrow G''$ *bir izomorfizmdir.*

Kanıt. (i) Φ, bire-bir ve örten olduğundan, Φ^{-1} tanımlıdır ve o da bire-bir ve örtendir. $a,\ b \in G'$; $\Phi^{-1}(a) = x$, $\Phi^{-1}(b) = y$ olsun. Bu takdirde, $\Phi(x) = a$, $\Phi(y) = b$ ve $\Phi(xy) = ab$; buradan da

$$\Phi^{-1}(ab) = xy = \Phi^{-1}(a)\Phi^{-1}(b)$$

olur. Böylece, $\Phi^{-1} : G' \longrightarrow G$ bir izomorfizmdir.

(ii) Varsayıma göre Φ ve Ψ her ikisi de bire-bir ve örten olduğundan, $\Psi \circ \Phi$ de bire-bir ve örtendir. Diğer yandan, her $x, y \in G$ için $(\Psi \circ \Phi)(xy) = \Psi(\Phi(xy)) = \Psi(\Phi(x))\Psi(\Phi(y)) = [(\Psi \circ \Phi)(x)][(\Psi \circ \Phi)(y)]$ dir. Böylece, $\Psi \circ \Phi$ bir izomorfizmdir. ∎

Yukarıdaki teoreme ek olarak, her G grubu için 1_G birim dönüşümünün G den G ye bir izomorfizm olduğu da gözlenirse, $\cong$ ile gösterilen *izomorf olma* bağıntısının tüm gruplardan oluşan küme üzerinde bir denklik bağıntısı olduğu görülür. Cebirciler, bu denklik bağıntısına göre aynı denklik sınıfında olan, yani izomorf olan iki grup arasında pek fark gözetmezler ve bu denklik sınıflarından birinin bir temsilcisini bildikleri takdirde o sınıfın tüm elemanlarını bildiklerini düşünürler. Aşağıdaki teorem cebircilerin neden böyle düşündüğünü aydınlatmada yardımcı olabilir.

Teorem 3. $\Phi : G \longrightarrow G'$ *bir izomorfizm olsun. Bu takdirde,*

(i) *G nin birim elemanının Φ altındaki görüntüsü, G' nün birim elemanıdır.*

(ii) *Her $x \in G$ ve $n \in \mathbb{Z}$ için $\Phi(x^n) = (\Phi(x))^n$ dir.*

(iii) *$x, y \in G$ için, $xy = yx \Longleftrightarrow \Phi(x)\Phi(y) = \Phi(y)\Phi(x)$ dir.*

(iv) *G Abel grubu ise, G' de Abel grubudur.*

(v) *$|G| = |G'|$ dür.*

(vi) *Her $x \in G$ için $|x| = |\Phi(x)|$ dir.*

(vii) *G devirli ise, G' de devirlidir.*

$(viii)$ *$a \in G$ ve $k \in \mathbb{Z}$ verildiğinde; G nin, $x^k = a$ denklemini sağlayan kaç elemanı varsa, G' nün de $x^k = \Phi(a)$ denklemini sağlayan o kadar elemanı vardır.*

(ix) *$H \leq G$ ise, $\Phi(H) \leq G'$ dür.*

(x) *$N \trianglelefteq G$ ise, $\Phi(N) \trianglelefteq G'$ dür.*

Kanıt. Bu özelliklerin çoğu kanıt gerektirmeyecek kadar açık özelliklerdir. Bunları bir arada toplu olarak ifade etmemizin nedenlerinden biri, izomorf olma bağıntısının ne kadar güçlü olduğunu sergilemektir. Burada, sadece (i), (vi) ve (x) i kanıtlayacağız ve diğer şıkların kanıtını okuyucuya bırakacağız. G ve G' nün birim elemanları, sırasıyla, e ve e' olsun. $ee = e$ olduğundan, $\Phi(e)\Phi(e) = \Phi(ee) = \Phi(e) = \Phi(e)e'$

dür. Böylece, $\Phi(e) = e'$ olduğu görülür. Dolayısıyla, $\Phi(e)$, G' nün birim elemanıdır. Bu, (i) yi kanıtlar. (vi) nin kanıtı için G nin bir x elemanını alalım. $x^n = e \Leftrightarrow \Phi(x)^n = e'$ dür. Buradan, x in mertebesi sonsuz ise, $\Phi(x)$ in mertebesi de sonsuz; $|x| = n$ ise, $|\Phi(x)| = n$ olduğu görülür. Son olarak, $N \trianglelefteq G$ ise, $\Phi(N) \leq G'$ olduğu kolayca görülür ve ayrıca, $a \in G'$, $b \in \Phi(N)$ için $\Phi(x) = a$, $\Phi(y) = b$ olacak biçimde $x \in G$, $y \in N$ vardır. Bu durumda, $N \trianglelefteq G$ olduğundan, $xyx^{-1} \in N$ dir ve dolayısıyla,

$$aba^{-1} = \Phi(x)\Phi(y)\Phi(x^{-1}) = \Phi(xyx^{-1}) \in \Phi(N)$$

dir. O halde, her $a \in G'$ için $a\Phi(N)a^{-1} \subseteq \Phi(N)$ dir ve böylece, $\Phi(N) \trianglelefteq G'$ dür. ∎

Daha önce, verilen iki grubun izomorf olup olmadıklarını belirlemenin her zaman kolay olmadığını belirtmiştik. Bu bağlamda, Teorem 3 ün, verilen iki grubun izomorf olmadıklarını gösterirken kullanılabileceğine dikkat ediniz. Örneğin, Teorem 3 (iv) den bir Abel grubunun Abel olmayan bir gruba, Teorem 3 (vii) den bir devirli grubun devirli olmayan bir gruba izomorf olması mümkün değildir. Benzer biçimde, Teorem 3 $(viii)$ ye göre $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$ ve $\mathbb{C}^* = \mathbb{C}\setminus\{0\}$ çarpımsal grupları izomorf olamazlar; çünkü, $\mathbb{R}^*$ içinde $x^4 = 1$ denklemini sağlayan iki eleman olduğu halde, $\mathbb{C}^*$ içinde (Φ ne olursa olsun) $x^4 = \Phi(1) = 1$ denklemini sağlayan tam dört eleman vardır.

Her G grubu için 1_G nin G den G ye bir izomorfizm olduğunu belirtmiştik; ancak, G den G ye 1_G den başka izomorfizmler de bulunabilir ve bunları ele alıp incelemek soyut cebirin ilginç konularından birini oluşturur.

Tanım 2. G bir grup olsun. G den G ye bir izomorfizme G nin bir *otomorfizm*i denir. □

Örnek 6. $\Phi : \mathbb{C} \longrightarrow \mathbb{C}$, $\Phi(a + bi) = a - bi$ dönüşümü, toplamsal $\mathbb{C}$ grubunun bir otomorfizmidir. □

Örnek 7. G bir Abel grubu ise, $\Phi : G \longrightarrow G$, $\Phi(x) = x^{-1}$ ile tanımlanan dönüşüm, G nin bir otomorfizmidir. Gerçekten, $x, y \in G$ için

$$\Phi(x) = \Phi(y) \Longrightarrow x^{-1} = y^{-1} \Longrightarrow x = y,\ \Phi(y^{-1}) = y$$

olduğundan, Φ, bire-bir ve örtendir. Ayrıca,

$$\Phi(xy) = (xy)^{-1} = (yx)^{-1} = x^{-1}y^{-1} = \Phi(x)\Phi(y)$$

dir. □

Bir G grubunun tüm otomorfizmlerinden oluşan küme, fonksiyon bileşkesi ile, bir gruptur. Bu grubu $Oto(G)$ ile göstereceğiz. $g \in G$ için

$$i_g : G \longrightarrow G \quad , \quad i_g(x) = gxg^{-1}$$

ile tanımlanan i_g dönüşümü, G nin bir otomorfizmidir. Gerçekten, $x, y \in G$ için $i_g(x) = i_g(y) \Longrightarrow gxg^{-1} = gyg^{-1} \Longrightarrow x = y$ olduğundan, i_g, bire-birdir. $y = g(g^{-1}yg)g^{-1} = i_g(g^{-1}yg)$ olduğundan, i_g, örtendir ve ayrıca, $i_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = i_g(x)i_g(y)$ olduğundan da işlem korur.

Tanım 3. G bir grup ve $g \in G$ olsun. Her $x \in G$ için $i_g(x) = gxg^{-1}$ ile tanımlanan i_g ye G nin g tarafından belirlenen <u>*iç otomorfizmi*</u> denir. G nin tüm iç otomorfizmlerinden oluşan küme, $\dot{I}\c{c}(G)$ ile gösterilir. □

Her G grubu için $Oto(G)$ nin birim elemanı, $1_G = i_e$, bir iç otomorfizmdir. Her $g \in M(G)$ için de $i_g = 1_G$ dir. Ek olarak, $g, h \in G$ ve $\sigma \in Oto(G)$ için

$$i_g i_h = i_{gh} \quad , \quad (i_g)^{-1} = i_{g^{-1}} \quad , \quad \sigma i_g \sigma^{-1} = i_{\sigma(g)}$$

olduğu görülebilir (Bak. Alıştırma 6 , 7). Böylece, $\dot{I}\c{c}(G) \trianglelefteq Oto(G)$ dir.

Örnek 8. $\dot{I}\c{c}(\mathcal{D}_4)$ ü belirleyelim. $M(\mathcal{D}_4) = \{d_0, d_2\}$ olduğundan, $i_{d0} = i_{d2}$, $Oto(\mathcal{D}_4)$ ün birim elemanıdır. Diğer yandan, $d_3 = d_1d_2$ olduğundan, $i_{d_3} = i_{d_1}$; $t_1d_2 = t_2$ olduğundan, $i_{t_1} = i_{t_2}$ ve $k_1d_2 = k_2$ olduğundan, $i_{k_1} = i_{k_2}$ dir. Ayrıca, i_{d_0}, i_{d_1}, i_{t_1} ve i_{k_1} in birbirinden farklı olduğu; böylece, $\dot{I}\c{c}(\mathcal{D}_4) = \{i_{d_0}, i_{d_1}, i_{t_1}, i_{k_1}\}$ olduğu görülür. □

Bu bölümü, $Oto(\mathbb{Z}_n)$ yi belirleyerek kapatalım.

Teorem 4. *Her $n > 1$ için $Oto(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$ dir.*

Kanıt. $Oto(\mathbb{Z}_n)$ nin her Φ elemanı, $\Phi(1)$ ile tamamen belirlenir. Çünkü, her $k \in \mathbb{Z}_n$ için $\Phi(k) = k\Phi(1)$ dir. Ayrıca, Φ bir otomorfizm (örten) olduğundan, $\Phi(1) \in \mathbb{Z}_n^*$ dır. Şimdi, $\sigma : Oto(\mathbb{Z}_n) \longrightarrow \mathbb{Z}_n^*$, $\sigma(\Phi) = \Phi(1)$ ile tanımlanan dönüşümü ele alalım. $\Phi_1,\ \Phi_2 \in Oto(\mathbb{Z}_n)$ için

$$\begin{aligned}\sigma(\Phi_1) = \sigma(\Phi_2) &\implies \Phi_1(1) = \Phi_2(1)\\ &\implies \Phi_1(x) = \Phi_2(x)\ \ \forall x \in \mathbb{Z}_n \implies \Phi_1 = \Phi_2\end{aligned}$$

olduğundan, σ, bire-birdir. $b \in \mathbb{Z}_n^*$ nin x katı olan xb elemanı $\mathbb{Z}_n$'de hesaplanmak üzere, $\Phi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, $\Phi(x) = xb$ dönüşümü, $\mathbb{Z}_n$ nin bir otomorfizmi olur ve $\sigma(\Phi) = \Phi(1) = b$ dir. Dolayısıyla, σ örtendir. σ, işlem koruyan bir dönüşümdür; çünkü,

$$\sigma(\Phi_1 \circ \Phi_2) = \Phi_1(\Phi_2(1)) = \Phi_1(1)\Phi_2(1) = \sigma(\Phi_1)\sigma(\Phi_2). \qquad \blacksquare$$