BÖLÜM **16**

HALKA HOMOMORFİZMLERİ VE İZOMORFİZMLERİ

Bu bölümü bitirdiğinizde,

- halka homomorfizmleri
- izomorfizm ve otomorfizmler
- halkalarda izomorfizm teoremleri
- bir cismin asal altcismi
- bir tamlık bölgesinin kesirler cismi

hakkında bilgi sahibi olabileceksiniz.

BÖLÜM 16

HALKA HOMOMORFİZMLERİ VE İZOMORFİZMLERİ

Gruplar üzerindeki çalışmalarımızda grupların yapılarının benzerliğini incelerken homomorfizm ve izomorfizmlerin ne kadar önemli olduğunu gördük. Bu bölümde, bu kavramların benzerlerini halkalar için tanımlayacağız.

Tanım 1. H ve K halkalar, $\sigma : H \longrightarrow K$ bir fonksiyon olsun. Aşağıdaki iki koşul sağlanıyorsa, σ ya H den K ya bir *halka homomorfizmi* denir:

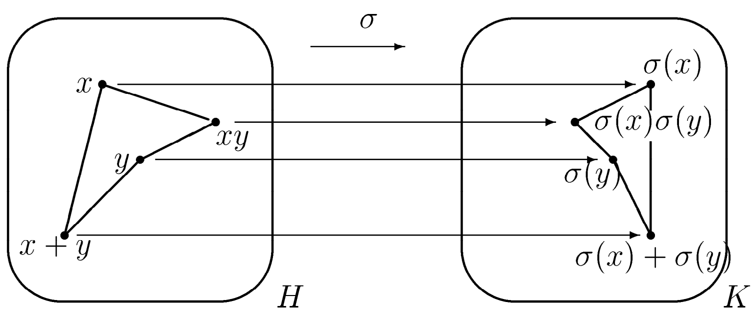
(hh.1) Her $x, y \in H$ için $\sigma(x+y) = \sigma(x) + \sigma(y)$ dir.

(hh.2) Her $x, y \in H$ için $\sigma(xy) = \sigma(x)\sigma(y)$ dir. □

Halka homomorfizmi tanımındaki iki eşitliğin her birinin sol tarafındaki işlem H içinde, sağ tarafındaki işlem ise K içinde işlemlerdir. Daha önce de kullandığımız deyişle, $\sigma : H \longrightarrow K$ nın, H halkasından K halkasına halka homomorfizmi olması için gerek ve yeter koşul, σ nın toplama ve çarpma işlemlerini korumasıdır.

Grup homomorfizmleri gibi, halka homomorfizmlerini de çizelgelerle açıklayabiliriz. Aşağıdaki çizelgede, bir H halkasından K halkasına

σ homomorfizmi ele alınmaktadır. Bu çizelgede kalın çizgiler halka içindeki işlemleri, ince çizgiler ise görüntüleri göstermektedir.



Şimdi bazı halka homomorfizmi örnekleri veriyoruz.

Örnek 1. $\sigma : \mathbb{Z}_{20} \longrightarrow \mathbb{Z}_{30}$, $\sigma(x) = 6x$ fonksiyonunu ele alalım. Burada, kümeler olarak $\mathbb{Z}_{20} \subseteq \mathbb{Z}_{30}$ kabul edilmekte ve $6x$, $\mathbb{Z}_{30}$ içinde, x in 6 katı olarak düşünülmektedir. $\mathbb{Z}_{30}$ içinde $6 \cdot 6 = 6$ olduğu da kullanılarak, her $x, y \in \mathbb{Z}_{20}$ için

(hh.1) $\sigma(x + y) = 6(x + y) = 6x + 6y = \sigma(x) + \sigma(y)$,

(hh.2) $\sigma(xy) = 6(xy) = 6 \cdot 6(xy) = (6x)(6y) = \sigma(x)\sigma(y)$

olur. Böylece, yukarıda verilen σ fonksiyonu, $\mathbb{Z}_{20}$ den $\mathbb{Z}_{30}$ a bir halka homomorfizmidir. □

Örnek 2. H bir halka ve A onun bir ideali ise,

$$\delta \;:\; H \longrightarrow H/A \;\;,\;\; \delta(x) \;=\; x + A$$

dönüşümü H den H/A ya bir örten halka homomorfizmidir. δ ya H den H/A ya *doğal homomorfizm* denir. □

Örnek 3. Eğer H değişmeli halka ve H nin karakteristiği 2 ise, bu takdirde, $\sigma : H \longrightarrow H$, $\sigma(x) = x^2$, H den H ye bir halka homomorfizmidir. □

Tanım 2. Eğer $\sigma : H \longrightarrow K$ bire-bir ve örten bir halka homomorfizmi ise, σ ya H den K ya bir *halka izomorfizmi* denir. $\sigma : H \longrightarrow K$ bir halka izomorfizmi ise, H ve K *izomorf* halkalardır denir ve $H \cong K$ yazılır. $\square$

İzomorf gruplar ve izomorf halkalar için aynı gösterim kullanılmakla birlikte, hangisinin kastedildiği konunun akışından anlaşılacaktır.

Tanım 3. Bir halkadan kendi üzerine bir izomorfizme, gruplarda olduğu gibi, bir halka *otomorfizmi* denir. $\square$

Örnek 4. Her $z = x + iy \in \mathbb{C}$ için $\overline{z} = x - iy$ olduğunu ve $\overline{z}$ ye z nin eşleniği dendiğini anımsayınız. $\sigma : \mathbb{C} \longrightarrow \mathbb{C},\ \ \sigma(z) = \overline{z}$ fonksiyonu, $\mathbb{C}$ nin bir otomorfizmidir. Çünkü, her $z_1, z_2 \in \mathbb{C}$ için

(`hh.1`) $\sigma(z_1 + z_2) = \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} = \sigma(z_1) + \sigma(z_2)$,

(`hh.2`) $\sigma(z_1 z_2) = \overline{z_1 z_2} = \overline{z_1}\ \overline{z_2} = \sigma(z_1)\sigma(z_2)$

olup σ, bire-bir ve örtendir. $\square$

Örnek 5. F, karakteristiği $p > 0$ olan bir sonlu cisim ise,

$$\varphi_p : F \longrightarrow F \quad , \quad \varphi_p(x) = x^p$$

fonksiyonu, F nin bir otomorfizmi olur. Gerçekten, her $x, y \in F$ için

(`hh.1`) $\varphi_p(x + y) = (x + y)^p = x^p + y^p = \varphi_p(x) + \varphi_p(y)$,

(`hh.2`) $\varphi_p(xy) = (xy)^p = x^p y^p = \varphi_p(x)\varphi_p(y)$

olduğundan, φ_p, bir cisim homomorfizmidir. Diğer yandan,

$$\varphi_p(x) = \varphi_p(y) \Longrightarrow x^p = y^p \Longrightarrow (x - y)^p = 0 \Longrightarrow x = y$$

olduğundan, φ_p, bire-birdir. F sonlu olduğundan da φ_p, örtendir. Sonuç olarak, φ_p, F nin bir otomorfizmidir. φ_p ye F nin *Frobenius otomorfizmi* denir. $\square$

Her halka homomorfizmi $\sigma : H \longrightarrow K$ nın, $< H, + >$ dan $< K, + >$ ya bir toplamsal grup homomorfizmi olduğuna dikkat ediniz. Bu bağlamda biliyoruz ki σ nın çekirdeği, *çek* (σ), H nin bir toplamsal altgrubudur. Aşağıdaki teoremde görüleceği üzere; *çek* (σ), H nin sadece bir toplamsal altgrubu değil, bir idealidir.

Teorem 1. *$\sigma : H \longrightarrow K$, H den K ya bir halka homomorfizmi, $x \in H$ olsun. Ayrıca, A, H nin bir althalkası ve B, K nın bir ideali olsun. Bu takdirde,*

(i) Her $n \in \mathbb{N}$ için, $\sigma(nx) = n\sigma(x)$ ve $\sigma(x^n) = (\sigma(x))^n$ dir.

(ii) $\sigma(A) = \{\sigma(a) : a \in A\}$, K nın bir althalkasıdır.

(iii) A, H nin bir ideali ise, $\sigma(A)$ da $\sigma(H)$ nin bir idealidir.

(iv) $\sigma^{-1}(B) = \{a \in H : \sigma(a) \in B\}$, H nin bir idealidir.

(v) çek (σ), H nin bir idealidir.

(vi) H değişmeli halka ise, $\sigma(H)$ de değişmeli halkadır.

(vii) H birimli halka ve σ örten ise, K da birimlidir ve $\sigma(1_H) = 1_K$ dır.

$(viii)$ σ bire-bir $\Longleftrightarrow$ çek $(\sigma) = \{0\}$.

(ix) $\sigma : H \longrightarrow K$ halka izomorfizmi ise, $\sigma^{-1} : K \longrightarrow H$ de halka izomorfizmidir.

Kanıt. Alıştırma. ∎

Örnek 6. $n > 1$ verilmiş olsun. Grup homomorfizmlerine örnek olmak üzere Örnek 12.3'te tanımlanan $(mod\ n)$ indirgeme homomorfizmi

$$\sigma_n \ : \ \mathbb{Z} \ \longrightarrow \ \mathbb{Z}_n \ \ , \ \ \sigma_n(x) \ = \ k,$$

bir örten halka homomorfizmidir. $(mod\ n)$ indirgeme homomorfizmleri, elemanter sayılar teorisinde *Diofant* denklemleri olarak bilinen denklemlerin tamsayı çözümleri araştırılırken büyük kolaylık sağlar. Örneğin,

$$a^2 + b^2 = 3c^2$$

denklemini sağlayan tüm (a, b, c) tamsayı üçlüleri araştırılırken şu yol izlenebilir: Verilen denklemi sağlayan bir tamsayı üçlüsü (a, b, c) bulunduğunu kabul edelim. Bu takdirde, a, b ve c nin ortak çarpanı bulunmadığını kabul edebiliriz. Çünkü, eğer ortak çarpan varsa, bu sayıların her biri o ortak çarpana bölününce elde edilen tamsayı üçlüsü de denklemin bir çözümü olur. Şimdi, $(mod\ 4)$ indirgeme homomorfizmini düşünelim. $a^2 + b^2 = 3c^2$ ye, $(mod\ 4)$ indirgeme homomorfizmi uygulanırsa, $\sigma(a)^2 + \sigma(b)^2 = 3\sigma(c)^2$ elde edilir. Dolayısıyla, $(\sigma(a), \sigma(b), \sigma(c))$ üçlüsü de aynı denklemi ($\mathbb{Z}_4$'te) sağlar. $\mathbb{Z}_4$ ün her u elemanı için, ya $u^2 = 0$ ya da $u^2 = 1$ olduğu göz önüne alınınca, $\sigma(a)^2 + \sigma(b)^2 = 3\sigma(c)^2$ denkleminin sağlanması için, $\mathbb{Z}_4$'te, $\sigma(a)^2 = \sigma(b)^2 = \sigma(c)^2 = 0$ olmalıdır. Bu, a, b ve c tamsayılarının her birinin çift olmasıyla mümkündür. a, b ve c tamsayılarının ortak çarpanı bulunmadığını varsaydığımızdan, bu mümkün değildir. Demek ki söz konusu denklemin hiç tamsayı çözümü yoktur. □

Örnek 7. $\mathbb{Z}_{20}$ den $\mathbb{Z}_{30}$ a tanımlı tüm halka homomorfizmlerini bulalım. $\mathbb{Z}_{20}$ den $\mathbb{Z}_{30}$ a grup homomorfizmlerinin, $\sigma(1)$ ile tamamen belirlendiğini biliyoruz. $\mathbb{Z}_{20}$'de $20 \cdot 1 = 0$ olduğundan $\mathbb{Z}_{30}$ içinde $20 \cdot \sigma(1) = 0$ olmalıdır. Diğer yandan, $\mathbb{Z}_{30}$ içinde $30 \cdot \sigma(1) = 0$ olduğundan, $10 \cdot \sigma(1) = 0$ olması gerekir. Ayrıca, $\mathbb{Z}_{20}$'de $1 \cdot 1 = 1$ olduğundan, $\mathbb{Z}_{30}$ içinde de $\sigma(1) \cdot \sigma(1) = \sigma(1)$ olmalıdır. $\mathbb{Z}_{30}$ un bu koşulları sağlayan elemanları

$$0\ ,\ 6\ ,\ 15\ ,\ 21$$

den ibarettir ve bunlardan her biri, $\sigma(1)$ olarak seçilebilir. Böylece, $\mathbb{Z}_{20}$ den $\mathbb{Z}_{30}$ a halka homomorfizmleri

$$\sigma_0(x) = 0\ ,\ \sigma_1(x) = 6x\ ,\ \sigma_2(x) = 15x\ ,\ \sigma_3(x) = 21x$$

ile tanımlanan fonksiyonlardan ibarettir. □

Grup homomorfizmleri gibi, halka homomorfizmlerinin bileşkeleri de yine halka homomorfizmidir.

Teorem 2. *$\sigma : H \longrightarrow K$ ve $\gamma : K \longrightarrow L$, halka homomorfizmleri ise, $\gamma \circ \sigma$ bileşkesi de H den L ye bir halka homomorfizmidir.*

Kanıt. $\gamma \circ \sigma$ bileşkesinin çarpma işlemini koruduğunu göstermek yeter(Neden?). $x, y \in H$ için

$$\sigma(xy) = \sigma(x)\sigma(y) \quad \text{ve} \quad \gamma(\sigma(x)\sigma(y)) = (\gamma(\sigma(x)))(\gamma(\sigma(y)))$$

olduğundan

$$\gamma \circ \sigma(xy) = \gamma(\sigma(xy)) = \gamma(\sigma(x)\sigma(y)) = \\ (\gamma(\sigma(x)))(\gamma(\sigma(y))) = (\gamma \circ \sigma(x))(\gamma \circ \sigma(y))$$

olduğu görülür ki bu, $\gamma \circ \sigma$ nın çarpma işlemini koruduğunu gösterir. ∎

Gruplar için ifade edilen izomorfizm teoremlerinin benzerleri halkalar için de geçerlidir. Bunlardan birincisini ifade ediyoruz; kanıtını okuyucuya alıştırma olarak bırakıyoruz.

Teorem 3 (Halkalarda Birinci İzomorfizm Teoremi). $\sigma : H \longrightarrow K$ *bir halka homomorfizmi, çek* $(\sigma) = A$ *ise,* $\overline{\sigma}(x + A) = \sigma(x)$ *ile tanımlanan* $\overline{\sigma} : H/A \longrightarrow \sigma(H)$ *fonksiyonu bir halka izomorfizmidir.*

Kanıt. Alıştırma. ∎

Örnek 8. Örnek 6'da verilen, $\mathbb{Z}$ den $\mathbb{Z}_n$ ye, $(mod\ n)$ indirgeme homomorfizmi σ_n için, $\sigma_n(\mathbb{Z}) = \mathbb{Z}_n$ ve *çek* $(\sigma_n) = n\mathbb{Z}$ dir. Dolayısıyla, Teorem 3 uygulanarak, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ olduğu görülür. □

Birimli bir H halkasının karakteristiği, $\mathbb{Z}$ den H ye tanımlanan özel bir homomorfizmle çok yakından ilişkilidir.

Teorem 4. *H, birim elemanı 1 olan bir halka ise,*

$$\sigma : \mathbb{Z} \longrightarrow H \quad , \quad \sigma(x) = x \cdot 1 = 1 \ in\ x - katı$$

ile tanımlanan σ, $\mathbb{Z}$ den H ye bir halka homomorfizmi olur. H nin karekteristiğinin n olması için gerek ve yeter koşul, bu homomorfizmin çekirdeğinin, çek $(\sigma) = n\mathbb{Z}$ olmasıdır.

Kanıt. $x, y \in \mathbb{Z}$ için $\sigma(x+y) = (x+y)\cdot 1 = x\cdot 1 + y\cdot 1 = \sigma(x) + \sigma(y)$ ve $\sigma(xy) = (xy) \cdot 1 = (x \cdot 1)(y \cdot 1) = \sigma(x)\sigma(y)$ olduğundan, σ bir homomorfizmdir. H nin karakteristiği 0 ise, her $n \neq 0$ için $\sigma(n) = n \cdot 1 \neq 0$ olacağından, *çek* $(\sigma) = \{0\} = 0\mathbb{Z}$ dir. Karşıt olarak, eğer *çek* $(\sigma) = \{0\}$ ise, her $n \neq 0$ tamsayısı için $n \cdot 1 = \sigma(n) \neq 0$ olacağından, H nin karakteristiği sıfırdır. Son olarak, H nin karakteristiğinin $n \geq 1$ olması için gerek ve yeter koşul, $n \cdot 1 = 0$ olması ve n nin bu özelliğe sahip en küçük pozitif tamsayı olmasıdır ki bu, *çek* $(\sigma) = n\mathbb{Z}$ olmasına denktir. ∎

Sonuç 1. *Her birimli halka, ya* $\mathbb{Z}$ *ya da uygun bir* $n \geq 1$ *için* $\mathbb{Z}_n$ *ye izomorf bir althalka içerir.*

Kanıt. $\sigma : \mathbb{Z} \longrightarrow H$, Teorem 4 teki gibi olsun. O zaman, Teorem 4 ten, $\sigma(\mathbb{Z}) \cong \mathbb{Z}/\text{çek}\,(\sigma)$ dır. Ya *çek* $(\sigma) = \{0\}$ ya da *çek* $(\sigma) = n\mathbb{Z}$, $n \geq 1$, olduğundan, $\sigma(\mathbb{Z}) \cong \mathbb{Z}$ veya $\sigma(\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ dir. ∎

Sonuç 2. *Karakteristiği* 0 (*sıfır*) *olan her cismin,* $\mathbb{Q}$ *ya izomorf bir altcismi; karakteristiği* $p > 1$ *olan her cismin,* $\mathbb{Z}_p$ *ye izomorf bir altcismi vardır.*

Kanıt. Sonuç 1 e göre, eğer F cisminin karakteristiği 0 ise, F nin $\mathbb{Z}$ ye izomorf bir althalkası H vardır. Bu durumda,

$$K = \{xy^{-1} : \ x, y \in H, \ y \neq 0\}$$

F nin $\mathbb{Q}$ ya izomorf bir altcismi olur. Eğer F nin karakteristiği $p > 0$ ise, Sonuç 1 e göre, F nin, $\mathbb{Z}_p$ ye izomorf olan bir altcismi vardır. ∎

Şimdi, F herhangi bir cisim olsun. Eğer F nin karakteristiği 0 (sıfır) ise, F nin her altcismi, $\mathbb{Q}$ ya izomorf olan bir altcisim içerir; bu altcisim, F nin tüm altcisimlerinin kesişimidir. Eğer F nin karakteristiği $p > 0$ ise, bu durumda da F nin her alt cismi, $\mathbb{Z}_p$ ye izomorf olan bir altcisim içerir; bu altcisim, F nin tüm altcisimlerinin kesişimidir.

Bir cismin tüm altcisimlerinin kesişimine, o cismin *asal altcismi* denir. Bir cismin asal altcismi, o cismin (küme kapsama bağıntısına göre) en küçük altcismidir. Sonuç 2 ye göre, karakteristiği sıfır olan bir cismin asal altcismi $\mathbb{Q}$ ya, karakteristiği $p > 1$ olan cismin asal altcismi de $\mathbb{Z}_p$ ye izomorftur. Her iki durumda da asal altcismi izomorf olduğu cisim ile özdeşleyerek, karakteristiği sıfır olan bir cismin $\mathbb{Q}$ yu, karakteristiği $p > 0$ olan bir cismin de $\mathbb{Z}_p$ yi altcisim olarak kapsadığını varsayabiliriz.

Tamsayılar halkası $\mathbb{Z}$, tamlık bölgesi olmasına rağmen cisim değildir; ancak $\mathbb{Z}$ yi kapsayan bir en küçük cisim vardır: Rasyonel sayılar cismi $\mathbb{Q}$. Bu bölümde son olarak, her tamlık bölgesi için de o tamlık bölgesini kapsayan bir en küçük cisim bulunduğunu göreceğiz. Böyle bir cismin inşasının, tamsayılardan rasyonel sayıların elde edilişine ne kadar çok benzediğine dikkat ediniz.

Bir tamlık bölgesi T verilmiş olsun ve

$$S = \{(a,b) : \ a,b \in T, \ b \neq 0\}$$

kümesini ele alalım. Bu küme üzerinde, $(a,b),(c,d) \in S$ için

$$(a,b)\beta(c,d) \Longleftrightarrow ad - bc = 0$$

ile tanımlanan β bağıntısının bir denklik bağıntısı olduğunu görmek kolaydır. Gerçekten, yansıma ve simetri özellikleri çok açık olup, geçişme özelliği şöyle görülebilir:

$$(a,b)\beta(c,d); \ (c,d)\beta(e,f) \Longrightarrow \left\{ \begin{array}{l} ad - bc = 0 \\ cf - de = 0 \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} adf - bcf = 0 \\ bcf - bde = 0 \end{array} \right.$$

$$\Longrightarrow \ adf - bde = 0 \ \Longrightarrow \ af - be = 0 \ \Longrightarrow \ (a,b)\beta(e,f).$$

Şimdi, $(a,b) \in S$ için (a,b) nin temsil ettiği denklik sınıfını, $\frac{a}{b}$ ile gösterelim:

$$[(a,b)]_\beta = \tfrac{a}{b} \quad ; \quad \tfrac{a}{b} = \tfrac{c}{d} \Longleftrightarrow ad - bc = 0.$$

S içinde β ya göre denklik sınıflarının oluşturduğu kümeyi, $Kes(T)$ ile gösterelim:

$$Kes(T) = S/\beta = \{\tfrac{a}{b} : \ a,b \in T, \ b \neq 0\}.$$

Kolayca görülebileceği gibi; $\frac{a}{b}, \frac{c}{d} \in Kes(T)$ için

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad , \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

tanımlanırsa, $Kes(T)$ içinde, iyi tanımlı ikili işlemler, toplama ve çarpma işlemleri, elde edilir. $Kes(T)$, yukarıdaki işlemlerle birlikte, bir cisimdir (Bak. Alıştırma 13). $Kes(T)$ nin sıfır elemanı $\frac{0}{1}$, birim elemanı $\frac{1}{1}$ dir. Ayrıca,

$$\sigma : T \longrightarrow Kes(T) \ , \ \sigma(a) = \frac{a}{1}$$

dönüşümü, T den $Kes(T)$ ye bire-bir bir halka homomorfizmidir. Başka bir deyişle, $\sigma(T)$ görüntüsü, $Kes(T)$ nin T ye izomorf olan bir althalkasıdır (Bak. Alıştırma 14).

Tanım 4. $Kes(T)$ ye T nin *kesirler cismi* denir. □

Örnek 9. $\mathbb{Z}$ nin kesirler cismi, $\mathbb{Q}$ dur. Kompleks sayılar cisminin bir alt halkası olan $T = \mathbb{Z}[i] = \{a + bi : \ a, b \in \mathbb{Z}\}$ tamlık bölgesinin kesirler cismi,

$$Kes(T) = \{c + di : \ c, d \in \mathbb{Q}\}$$

dur ve bu cisim, $\mathbb{Q}(i)$ ile gösterilir. □