BÖLÜM 14

TAMLIK BÖLGELERİ VE CİSİMLER

Bu bölümü bitirdiğinizde,

- halkalarda bölenler, sıfır-bölenleri
- tamlık bölgeleri
- kısaltma kuralı
- aykırı cisimler
- cisimler
- kuaterniyonlar
- bir halkanın karakteristiği

hakkında bilgi sahibi olabileceksiniz.

BÖLÜM 14

TAMLIK BÖLGELERİ VE CİSİMLER

Bundan önceki bölümde tanımladığımız halka kavramı, tamsayılar kümesinin cebirsel yapısının soyutlanışı olarak düşünülebilir. Ancak, her soyutlamada olduğu gibi burada da tamsayılar kümesinin bazı temel özelliklerinin kaybolduğu söylenebilir. Başka bir deyişle, halka kavramı, tamsayılar kümesinden çok daha geniş bir cebirsel yapıyı ifade eder. Bu bölümde, tamsayılar kümesi ve rasyonel sayılar kümesine daha yakın cebirsel yapılardan söz edeceğiz: Tamlık bölgeleri ve cisimler.

Tamsayılar için temel kavramlardan biri olan "bölen" kavramı herhangi bir halka için de tanımlanabilir.

Tanım 1. H bir halka; $x, a, b \in H$ olsun. Eğer $ab = x$ ise, a ya x in bir *sol bölen*i, b ye de x in bir *sağ bölen*i denir. Eğer $a \in H$, x in hem sol hem de sağ böleni ise, a ya x in bir *bölen*i denir. □

Değişmeli halkalarda bir eleman için sol bölen, sağ bölen veya bölen kavramlarının çakıştığına dikkat ediniz.

Örnek 1. $\mathbb{R}^{2\times 2}$'de

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

olduğundan, $\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ in sol böleni; $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ de aynı elemanın sağ bölenidir. □

Birimli bir halkada bir elemanın tersinir olması, o elemanın birim eleman 1 in bir böleni olması demektir.

Bir halkada sıfırın bazı bölenleri özel öneme sahiptir.

Tanım 2. H bir halka; $a, b \in H$; $a \neq 0, b \neq 0$ ve $ab = 0$ ise, a ya H nin bir *sol sıfır-böleni*, b ye de H nin bir *sağ sıfır-böleni* denir. Hem sağ hem sol sıfır-böleni olan bir elemana da H nin bir *sıfır-böleni* denir. □

Değişmeli halkalarda yukarıdaki üç kavramın çakıştığı açıktır.

Örnek 2. $\mathbb{R}^{2\times 2}$'de $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, $C = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ alalım.

$$AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad , \quad BC = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

olduğundan, A, bir sol sıfır-böleni; C, bir sağ sıfır-böleni ve B, bir sıfır-bölenidir. □

Önerme 1. *Birimli bir halka içinde tersinir olan bir eleman, o halkanın sol veya sağ sıfır-böleni olamaz.*

Kanıt. H, birimli bir halka; $a \in H$ tersinir bir eleman ve a nın tersi a^{-1} olsun. Eğer $b \in H$ ve $ab = 0$ veya $ba = 0$ ise, bu ifadeler soldan veya sağdan a^{-1} ile çarpılarak $a^{-1}(ab) = b = 0$ veya $(ba)a^{-1} = b = 0$ elde edilir. Bu, a elemanının H nin sol veya sağ sıfır-böleni olamayacağını gösterir. ■

$n \geq 2$ için $\mathbb{Z}_n$ halkasının sıfır-bölenleri nelerdir? Bu sorunun yanıtı aşağıdaki önermede verilmektedir.

Önerme 2. *$n \geq 2$ ve $a \in \mathbb{Z}_n \backslash \{0\}$ ise, aşağıdakiler denktir:*

(i) *a ve n aralarında asaldır.*

(ii) *a, $\mathbb{Z}_n$ içinde tersinir.*

(iii) *a, $\mathbb{Z}_n$ nin sıfır-böleni değildir.*

Kanıt. $(i) \Longrightarrow (ii)$ olduğunu biliyoruz(Bak. Örnek 13.9). Önerme 1 den, $(ii) \Longrightarrow (iii)$. Diğer yandan, eğer a, $\mathbb{Z}_n$ nin sıfır-böleni değilse, a ve n aralarında asal olmak zorundadır. Çünkü, aksi halde a ve n nin bir ortak böleni $c \in \mathbb{Z}_n$ bulunur. $a = ca_1$ ve $n = cn_1$; $a_1, n_1 \in \mathbb{Z}_n \backslash \{0\}$ olsun. O zaman, $an_1 = a_1cn_1 = 0$ olur ki bu, a elemanının $\mathbb{Z}_n$ nin bir sıfır-böleni olduğunu gösterir. Dolayısıyla, $(iii) \Longrightarrow (i)$. ■

Tanım 3. H, birimli değişmeli bir halka; $1_H \neq 0_H$ ve H nin hiç sıfır-böleni yoksa, H ye bir *tamlık bölgesi* denir. □

Bu tanıma göre, $1_H \neq 0_H$ olan birimli değişmeli bir H halkasının tamlık bölgesi olması için gerek ve yeter koşul,

$$a, b \in H,\ ab = 0 \Longrightarrow a = 0 \text{ veya } b = 0$$

olmasıdır.

Örnek 3. Şimdiye kadar tanıdığımız halkalardan $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Q}[x]$ ten her biri bir tamlık bölgesidir. Eğer p asal sayı ise, $\mathbb{Z}_p$ nin bir tamlık bölgesi olduğunu görmek zor değildir. □

Örnek 4. $2\mathbb{Z}$ halkası, birim elemanı bulunmadığından; $\mathbb{R}^{n\times n}$, değişmeli olmadığından veya sıfır-bölenleri bulunduğundan; asal olmayan her $n > 1$ için $\mathbb{Z}_n$, sıfır-bölenleri bulunduğundan, tamlık bölgesi değildir. □

Bir tamlık bölgesi, çarpma işlemine göre bir grup oluşturmasa da çarpımsal grupların sahip olduğu bir özelliğe sahiptir: *Kısaltma kuralı.*

Önerme 3. *H bir tamlık bölgesi; $x, y, z \in H$ olsun. Eğer $x \neq 0$ ve $xy = xz$ ise, $y = z$ dir.*

Kanıt. $xy = xz$ ise, $x(y-z) = 0$ olur. $x \neq 0$ olduğundan, $y - z = 0$

ve böylece, $y = z$ dir. ∎

Tamsayılar halkası $\mathbb{Z}$ ve rasyonel sayılar halkası $\mathbb{Q}$, her ikisi de tamlık bölgesi olmalarına karşın, bunların farklı cebirsel yapılar oluşturdukları açıktır. Bu farklılığı yansıtan cebirsel yapılar için yeni bir isim verilmesi yerinde olacaktır.

Tanım 4. Birimli bir H halkasında $1_H \neq 0_H$ ise ve H nin sıfırdan farklı her elemanı tersinir ise, H ye bir *aykırı cisim* denir. □

Yukarıdaki tanımdan da görüleceği üzere, $1_H \neq 0_H$ olan bir H halkasının aykırı cisim olması için gerek ve yeter koşul, $H^* = H\backslash\{0\}$ olmasıdır. Şimdiye kadar ele aldığımız halkalar arasında $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ve p asal olmak üzere $\mathbb{Z}_p$, aykırı cisim örnekleridir. Bu aykırı cisimlerde çarpma işlemi değişme özelliğine sahiptir. Aykırı cisim tanımında çarpma işleminin değişme özelliğine sahip olması koşulu yoktur. Çarpma işlemi değişme özelliğine sahip olmayan aykırı cisimlerin standart örneği *kuaterniyonlar* aykırı cismidir.

Örnek 5. $K = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$ toplamsal Abel grubunu ele alalım. K nın toplama işleminin, $\mathbb{R}$ deki toplama işlemi yardımıyla, bileşenlere göre tanımlandığını anımsayınız. K üzerinde bir de çarpma işlemi tanımlayıp K ya bir halka yapısı kazandırmak istiyoruz. Bunu, K nın aşağıdaki elemanlarını kullanarak gerçekleştireceğiz:

$$\mathbf{1} = (1,0,0,0),\ \mathbf{i} = (0,1,0,0),\ \mathbf{j} = (0,0,1,0),\ \mathbf{k} = (0,0,0,1)$$

Her $x_1, x_2, x_3, x_4 \in \mathbb{R}$ için

$$x_1 = (x_1,0,0,0),\ x_2\mathbf{i} = (0,x_2,0,0),\ x_3\mathbf{j} = (0,0,x_3,0),\ x_4\mathbf{k} = (0,0,0,x_4)$$

olsun. Bu durumda her $(x_1, x_2, x_3, x_4) \in K$ için

$$(x_1, x_2, x_3, x_4) = x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k}$$

olur ve K içindeki toplama işlemi

$$\begin{aligned}(x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k}) &+ (y_1 + y_2\mathbf{i} + y_3\mathbf{j} + y_4\mathbf{k}) \\ &= (x_1 + y_1) + (x_2 + y_2)\mathbf{i} + (x_3 + y_3)\mathbf{j} + (x_4 + y_4)\mathbf{k}\end{aligned}$$

olarak ifade edilebilir. Çarpma işleminin tanımına, $\mathbf{i}$, $\mathbf{j}$ ve $\mathbf{k}$ nın birbirleriyle çarpımını tanımlayarak başlıyoruz:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1,\ \mathbf{ij} = \mathbf{k},\ \mathbf{jk} = \mathbf{i},\ \mathbf{ki} = \mathbf{j},\ \mathbf{ji} = -\mathbf{k},\ \mathbf{kj} = -\mathbf{i},\ \mathbf{ik} = -\mathbf{j}.$$

Bu çarpımları anımsamanın bir yolu, Fraleigh'in işaret ettiği gibi,

$$\mathbf{i},\ \mathbf{j},\ \mathbf{k},\ \mathbf{i},\ \mathbf{j},\ \mathbf{k}$$

dizisinde ardışık iki terimin sağa doğru çarpımını bunların sağındaki ilk eleman, sola doğru çarpımını ise, bunların solundaki ilk elemanın eksi işaretlisi olarak almaktır. Çarpma işleminin tanımını, $\mathbf{1}$, birim eleman olacak biçimde, yani her $\mathbf{x} \in K$ için

$$\mathbf{x1} = \mathbf{1x} = \mathbf{x}$$

olacak biçimde sürdürüyoruz. K nın herhangi iki elemanının çarpımını da yukarıdakilere ek olarak, birleşme özelliği ve dağılma özellikleri sağlanacak biçimde, şöyle tanımlıyoruz:

$$\begin{aligned}
&(x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k})(y_1 + y_2\mathbf{i} + y_3\mathbf{j} + y_4\mathbf{k}) \\
&\qquad = (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4) \\
&\qquad\quad +(x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)\mathbf{i} \\
&\qquad\quad +(x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2)\mathbf{j} \\
&\qquad\quad +(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)\mathbf{k}.
\end{aligned}$$

$< K, +, \cdot >$ nın birimli bir halka olduğunu göstermeyi okuyucuya alıştırma olarak bırakıyoruz. $\mathbf{ij} = \mathbf{k}$ ve $\mathbf{ji} = -\mathbf{k}$ olduğundan, bu halka değişmeli halka değildir. $\mathbf{0}_K = (0, 0, 0, 0)$, $\mathbf{1}_K = \mathbf{1}$ dir ve $\mathbf{1}_K \neq \mathbf{0}_K$ dır. K nın bir $\mathbf{x} = x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k}$ elemanının sıfırdan farklı olması için gerek ve yeter koşul, $x_1,\ x_2,\ x_3,\ x_4$ ten en az birinin sıfırdan farklı olmasıdır. K nın sıfırdan farklı her elemanının tersinir olduğunu gösterirken, her $x_1,\ x_2,\ x_3,\ x_4 \in \mathbb{R}$ için

$$(x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k})(x_1 - x_2\mathbf{i} - x_3\mathbf{j} - x_4\mathbf{k}) = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

olduğunu görmek önemlidir. Karmaşık sayılardakine benzer biçimde, her $\mathbf{x} = x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k}$ için

$$\overline{\mathbf{x}} = x_1 - x_2\mathbf{i} - x_3\mathbf{j} - x_4\mathbf{k} \quad , \quad |\mathbf{x}|^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

tanımlanırsa, sıfırdan farklı her $\mathbf{x}$ elemanının tersinin,

$$\mathbf{x}^{-1} = \tfrac{x_1}{|\mathbf{x}|^2} - \tfrac{x_2}{|\mathbf{x}|^2}\mathbf{i} - \tfrac{x_3}{|\mathbf{x}|^2}\mathbf{j} - \tfrac{x_4}{|\mathbf{x}|^2}\mathbf{k}$$

olduğu görülür. Sonuç olarak, K (değişmeli olmayan) bir aykırı cisimdir. *Kuaterniyonlar halkası* olarak bilinen K nın,

$$G = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$$

altkümesi, bir çarpımsal gruptur ve mertebesi 8 olan bu grubun Alıştırma 8.5'te verilen gruba izomorf olduğunu görmek zor değildir. Bu, söz konusu grubun neden kuaterniyonlar grubu olarak adlandırıldığını açık lar. $\square$

Tanım 5. Eğer H, değişmeli aykırı cisim ise, H ye bir *cisim* denir. $\square$

Yukarıdaki tanımdan da görüleceği üzere, $1_H \neq 0_H$ olan bir H halkasının cisim olması için gerek ve yeter koşul, $H\backslash\{0\}$ ın bir Abel grubu olmasıdır. Şimdiye kadar ele aldığımız halkalar arasında $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ve p asal olmak üzere $\mathbb{Z}_p$, cisim örnekleridir. Eğer n asal değilse, $\mathbb{Z}_n$ cisim değildir. Kuaterniyonlar halkası, K, değişmeli olmadığından, cisim değildir.

Cebirde önemli sonuçlardan biri, her sonlu aykırı cismin bir cisim olduğunu ifade eder. Wedderburn Teoremi olarak bilinen bu sonucun ispatı bu kitabın kapsamı dışındadır. İlgilenen okuyucu, ispat için daha ileri düzeyde cebir kitaplarına bakabilir. Bu bağlamda, aşağıdaki teoremi veriyoruz.

Teorem 1. *Her cisim bir tamlık bölgesidir ve her sonlu tamlık bölgesi bir cisimdir.*

Kanıt. F bir cisim olsun. Cisim tanımından, F, birimli değişmelidir ve $1_F \neq 0_F$ dır. Önerme 1 e göre, F nin hiç sıfır-böleni yoktur. Böylece, her cisim bir tamlık bölgesidir. Şimdi, H, bir sonlu tamlık bölgesi olsun. Tamlık bölgesi tanımından, $1_H \neq 0_H$ dir. $a \in H \backslash \{0\}$ alalım. Eğer $a = 1_H$ ise, a tersinir ve $a^{-1} = 1_H$ dir. $a \neq 1_H$ ise, H içinde

$$1_H = a^0, a, a^2, \ldots, a^i, \ldots$$

dizisini düşünelim. H sonlu olduğundan, öyle $i \geq 0$ ve $j > i$ tamsayıları vardır ki $a^i = a^j$ dir. Böylece,

$$a^i = a^j = a^i(a^{j-i})$$

olup Önerme 3 ten $1_H = a^{j-i}$ olduğu; dolayısıyla,

$$1_H = a^{j-i} = a(a^{j-i-1}),$$

buradan da a nın tersinir ve

$$a^{-1} = a^{j-i-1}$$

olduğu görülür. ∎

Şimdi, halkaları birbirinden ayırt edici bir kavramı ele alacağız.

Tanım 6. Bir H halkası verilmiş olsun. Eğer her $x \in H$ için $nx = 0$ olacak biçimde x den bağımsız n pozitif tamsayıları varsa, bu özelliğe sahip en küçük pozitif tamsayıya H halkasının *karakteristiği* denir. Böyle bir pozitif tamsayı yoksa, H nin karakteristiği, *sıfır* olarak tanımlanır. □

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ve $\mathbb{C}$ nin her birinin karakteristiği sıfırdır. Her $n > 1$ için $\mathbb{Z}_n$ nin karakteristiği n dir. Katsayıları $\mathbb{Z}_n$ içinde olan polinomların oluşturduğu $\mathbb{Z}_n[x]$ halkasının karakteristiği de n dir.

Birimli halkalarda karakteristiği belirlemek daha kolaydır:

Teorem 2. *H, birim elemanı 1 olan bir birimli halka olsun. Bu takdirde,*

(i) 1 in $< H, + >$'da mertebesi sonsuz ise, H nin karakteristiği sıfırdır.

(ii) 1 in $< H, + >$'da mertebesi n ise, H nin karakteristiği n dir.

Kanıt. (i) Eğer 1 in $< H, + >$'da mertebesi sonsuz ise, $n \cdot 1 = 0$ olacak biçimde hiç pozitif tamsayı yoktur. Dolayısıyla, H nin karakteristiği sıfırdır.

(ii) Eğer 1 in mertebesi n ise, $n \cdot 1 = 0$ özelliğine sahip olan en küçük pozitif tamsayı n dir. Ayrıca, her $x \in H$ için $nx = (n \cdot 1)x = 0x = 0$ olduğu açıktır. Demek ki her $x \in H$ için $nx = 0$ dır ve bu özelliğe sahip en küçük pozitif tamsayı n dir. ∎

Teorem 3. *Bir tamlık bölgesinin karakteristiği ya sıfır ya da bir asal sayıdır.*

Kanıt. H bir tamlık bölgesi, H nin karakteristiği, $n \neq 0$ olsun. Eğer n asal değilse, $n = rs$ olacak biçimde $1 < r, s < n$ tamsayıları vardır ve bu durumda $0 = n \cdot 1 = (rs) \cdot 1 = (r \cdot 1)(s \cdot 1)$ olur. H, tamlık bölgesi olduğundan, $r \cdot 1 = 0$ veya $s \cdot 1 = 0$ olması gerekir ki bu, n nin $n \cdot 1 = 0$ özelliğine sahip en küçük pozitif tamsayı olma özelliği ile çelişir. O halde, n, asal olmalıdır. ∎

Bölüm 13'te kanıtladığımız Binom Teoremi, karakteristiği sıfır olmayan halkalarda çok basit bir görünüm alır. Aşağıdakiler, Binom Teoremi'nin sonuçlarıdır.

Önerme 4. *H, karakteristiği bir asal sayı, p, olan bir halka; $x\ , y\ \in H$ ve $xy = yx$ olsun. Bu takdirde,*

$$(x + y)^p = x^p + y^p$$

olur.

Kanıt. Binom Teoremi'ne göre

$$(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

ve Önerme 13.1(iv) e göre her $k = 1, 2, \cdots, p-1$ için $p \mid \binom{p}{k}$. Böylece, her $k = 1, 2, \cdots, p-1$ ve her $a \in H$ için $\begin{pmatrix} p \\ k \end{pmatrix} \cdot a = 0$ olur ve

$$(x+y)^p = x^p + y^p$$

olduğu görülür. ■

Önerme 4 ten tümevarımla aşağıdaki sonuç elde edilir:

Önerme 5. *H, karakteristiği bir asal sayı, p, olan bir halka; x , y $\in H$ ve $xy = yx$ olsun. Bu takdirde,*

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}$$

olur. ■