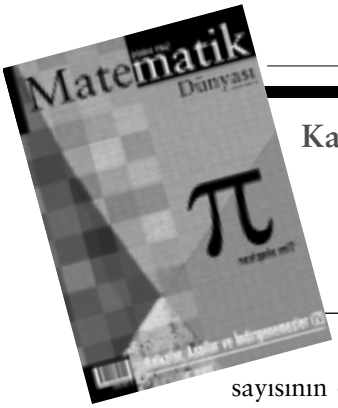

Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (2)

Halkalar, Sıfırbölenler, Asallar, İndirgenemezler vb.

Matematik Dünyası'nın her sayısının önceki sayılardan olabildiğince bağımsız olmasına dikkat etmeye çalışıyoruz. Bu sayının kapak konusu geçen sayının kapak konusuyla aynı olduğundan, bu yazıda, geçen sayıda tanımladığımız kavramlardan kısaca sözedeceğiz. Ama biraz daha ileri gidip yeni kavramlar ele alacağız. Ayrıca geçen sayıda sadece belli özelliklere sahip halkalar için tanımladığımız kavramları bu yazıda daha genel halkalar için tanımlayacağız.

"Halka" denilen ve birazdan tanımlayacağımız matematiksel yapı, toplama ve çarpma adı verilen ve alışık olduğumuz özellikleri sağlayan iki işlemin tanımlandığı bir kümedir.

I. Halka Örnekleri. Önce halka örnekleri verelim ki halkalarla çocukluğumuzdan beri içli dışlı olduğumuz anlaşılsın:

a) Tamsayılar kümesi $\mathbb{Z}$,
b) Kesirli sayılar kümesi $\mathbb{Q}$,
c) Gerçel sayılar kümesi $\mathbb{R}$,
d) "Modülo n" sayılar kümesi $\mathbb{Z}/n\mathbb{Z}$,
e) $\mathbb{Z}[X]$, $\mathbb{Q}[X, Y]$, $\mathbb{R}[X]$, $(\mathbb{Z}/n\mathbb{Z})[X]$ gibi bir ya da daha fazla değişkenli polinom kümeleri,
f) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$

ve

$$\mathbb{Q}[\sqrt{6}] = \{a + b\sqrt{6} : a, b \in \mathbb{Q}\}$$

gibi gerçel sayıların bazı altkümeleri,

g) Herhangi bir p asalı için,
$\mathbb{Q}_{<p>} = \{a/b : a, b \in \mathbb{Z}$ ve p, b'yi bölmez$\}$.

Bütün bu kümeler kümesi bildiğimiz toplama ve çarpma işlemleriyle birlikte birer halkadırlar. Daha binlerce halka örneği vardır.

II. Halkanın Tanımı. Bir **halka** her şeyden önce bir kümedir, ama bir halka sadece bir küme değildir elbet, yoksa yeni bir kavram elde etmezdik. Bir halkada, ayrıca, 0 (**sıfır**) ve 1 (**bir** ya da **birim öğe**) adı verilen iki özel öğe ve **toplama** ve **çarpma** adı verilen iki de işlem vardır. Bu işlemler + ve × olarak yazılırlar. Yani toplama ve çarpma, her ikisi de $R \times R$ kümesinden R kümesine giden birer fonksiyondurlar. Eğer $(x, y) \in R \times R$ ise, toplama ve çarpma işlemlerinin (fonksiyonlarının) sonucu sırasıyla $x + y$ ve $x \times y$ yazılırlar. Hemen hemen hep $x \times y$ yerine xy yazacağız.

Toplama ve çarpmanın sonucunun gene R kümesinde olması gerektiği gözardı edilmemelidir. Kolaylıkla gözden kaçabilecek bu ince nokta vahim hatalara yol açabilir.

Bu $(R, +, \times, 0, 1)$ beşlisinin (değişimli) halka adına hak kazanması için birtakım özelliklere sahip olması gerekmektedir. İşte o özellikler:

H1 [Birleşme Özelliği]. *Her* $x, y, z \in R$ *için*,
$x + (y + z) = (x + y) + z$ *ve* $x(yz) = (xy)z$.
H2 [Etkisiz ve Birim Öğe]. *Her* $x \in R$ *için*,
$0 + x = x + 0 = x$ *ve* $x1 = 1x = x$.
H3 [Değişme Özelliği]. *Her* x *ve* $y \in R$ *için*,
$x + y = y + x$ *ve* $xy = yx$.
H4 [Ters Öğenin Varlığı]. *Her* $x \in R$ *için*,
$x + y = y + x = 0$
eşitliklerini sağlayan bir $y \in R$ *vardır*.
H5. $1 \neq 0$.
H6 [Dağılma Özelliği]. *Her* $x, y, z \in R$ *için*,
$x(y + z) = xy + xz$.

Yukarda verdiğimiz örneklerin herbirinde bu özelliklerin sağlandığını okur sınayabilir. Dolayısıyla bu örneklerin herbiri gerçekten birer halkadır[1].

Bambaşka türden bir halka örneği verelim: A boş olmayan herhangi bir küme olsun. $\wp(A)$, A'nın altkümeleri kümesi olsun. Eğer $x, y \in \wp(A)$ ise, yani x ve y, A'nın birer altkümesiyse,

$$x + y := (x \cup y) \setminus (x \cap y),$$
$$xy := x \cap y$$

olarak tanımlayalım. Bu "toplama" ve "çarpma" işlemleriyle birlikte $\wp(A)$ bir halkadır. Bu halkada 0 görevini boşküme, 1 görevini de A kümesi üstlenir.

H1, H2, H3 özellikleri toplamayla çarpma arasında pek bir ayrım yapmıyor. Toplama ve 0 için doğru olan, çarpma ve 1 için de doğru ve bunun ter-

1 Geçen sayıda verdiğimiz halka tanımı hafifçe değişikti, bu tanımın diğerine eşdeğer olduğunu kanıtlamak zor değildir.

si de geçerli: Çarpma ve 1 için doğru olan toplama ve 0 için de doğru. Toplamayla çarpma arasındaki ayrım ancak H4 ve H6'da belli oluyor.

H1, bir halkanın öğeleri toplanırken ya da çarpılırken paranteze gerek olmadığını söylüyor. Üç öğe için geçerli olan bu özellik dört öğe için de geçerlidir. Örneğin x, y, z, t öğelerini toplarken işlemlerin hangi sırayla yapıldıkları önemli değildir, sözgelimi,

$$(x + y) + (z + t) = (x + (y + z)) + t$$
$$= ((x + y) + z) + t = (x + y) + (z + t)$$
$$= x + ((y + z) + t) = x + (y + (z + t)).$$

Dolayısıyla x, y, z, t öğelerinin toplamını ya da çarpımını parantezsiz olarak $x + y + z + t$ ya da $xyzt$ biçiminde yazabiliriz; parantezlerin işlevi kalmamıştır.

Aslında halkanın tanımında H3'ün ikinci yarısı, yani $xy = yx$ eşitliği yoktur. Bu eşitliği sağlayan halkalara **değişimli halka** adı verilir. Biz bu sayıda sadece değişim özelliği olan halkalarla ilgileneceğiz ve halka terimini sadece ve sadece değişim özelliği olan halkalar için kullanacağız.

H3'ten toplama ve çarpma yaparken x, y, z ve t'nin yerlerinin de önemli olmadığını anlarız. Örneğin, $xyzt = zxty$.

Doğal sayılar kümesi $\mathbb{N}$ bir halka değildir, çünkü H4 özelliği $\mathbb{N}$'de doğru değildir. Tek tamsayılar kümesine 0 eklersek, bu kümede H1-H6 özelliklerinin hepsi geçerli olmasına karşın, bu küme halka değildir, çünkü bu kümede toplama yapılamaz: iki tek sayının toplamı her zaman bir tek sayı ya da 0 değildir. Bir halkada iki öğenin toplamı ve çarpımı gene o halkada olmalıdır.

III. Halkaların Başat Özellikleri. Aşağıdaki özellikler tanımlardan doğrudan çıkar ve geçen sayımızda kanıtlanmıştı. Kanıtları kolay olan bu özellikleri okur geçen sayıya bakmadan kanıtlamaya çalışmalıdır.

Önsav 1. i. *Eğer bir halkanın x, y ve z öğeleri $x + y = x + z$ eşitliğini sağlıyorsa o zaman $y = z$'dir.*

ii. *Bir halkada* H2 *özelliğini sağlayan* 0 *ve* 1 *öğelerinden tam birer tane vardır.*

iii. *Bir halkada, her x için* H3 *özelliğini sağlayan, yani $x + y = 0$ eşitliğini sağlayan tek bir y vardır.*

Kanıt: MD-2004-I, sayfa 30, Önsav 1 ve ardından yazılanlar. □

Madem ki, $x + y = 0$ eşitliğini sağlayan tek bir y var, (x'e bağımlı olan, yani x değiştikçe değişen) bu y öğesine bir ad verebiliriz. Bundan böyle $x + y = 0$ özelliğini sağlayan y'yi $-x$ olarak yazalım. Ayrıca bundan böyle

$x + (-y)$ yerine $x - y$,
$(-x) + y$ yerine $-x + y$,
$(-x) + (-y)$ yerine $-x - y$

yazalım.

Demek ki bir halkada, 1 diye bir öğe olduğundan, –1 diye de bir öğe vardır.

Önsav 2. *R bir halka ve $x, y \in R$ olsun.*
i. $-(x + y) = -x - y$.
ii. $-(x - y) = -x + y$.
iii. $-(-x) = x$.
Kanıt: MD-2004-I, sayfa 30, Önsav 3. □

Önsav 3. *R bir halka ve $x, y \in R$ olsun.*
i. $x0 = 0$.
ii. $(-x)y = -(xy) = x(-y)$.
iii. $(-1)y = -y$.
iv. $(-1)^2 = 1$.
Kanıt: MD-2004-I, sayfa 31, Önsav 5. □

IV. Tersinir Elemanlar. H4'e göre bir halkada toplama işlemi için her elemanın bir "tersi" var, ama aynı şey çarpma için geçerli değil, yani her $x \in R$ için $xy = 1$ eşitliğini sağlayan bir y olmayabilir, örneğin $x = 0$ için böyle bir y olamaz, olsa, Önsav 3.i'den dolayı, $1 = 0y = 0$ olurdu, ki bu da H5'le çelişir.

R bir halka olsun. $a \in R$ olsun. Eğer R halkasında $ab = 1$ eşitliğini sağlayan bir b öğesi varsa, a'ya **tersinir öğe** denir. Tersinir öğeler kümesi R^* olarak gösterilir:

$$R^* = \{x \in R : \text{belli bir } y \in R \text{ için } xy = 1\}.$$

Kolayca görüleceği üzere,

$\mathbb{Z}^* = \{1, -1\}$,
$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$,
$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$,
$\mathbb{R}[X]^* = \mathbb{R} \setminus \{0\}$ = sıfır olmayan sabit polinomlar,
$\mathbb{Z}[X]^* = \{1, -1\}$,
$\mathbb{Q}_{<p>}{}^* = \{\pm p^n : n \in \mathbb{Z}\}$,
$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{d} : d, n\text{'ye asal}\}$.

Sonuncu eşitlik MD-2004-I, Sonuç 4, sayfa 16'da kanıtlanmıştı.

Alıştırmalar.

1. $(\mathbb{Z}/4\mathbb{Z})[X]^* = \{1 + 2f(X) : f(X) \in (\mathbb{Z}/4\mathbb{Z})[X]\}$ eşitliğini kanıtlayın.

2. $(\mathbb{Z}/6\mathbb{Z})[X]^*$ kümesini bulun.

3. Her $n > 1$ için, $(\mathbb{Z}/n\mathbb{Z})[X]^*$ kümesini bulun.

Bir halkada a verilmişse, $ab = 1$ eşitliğini sağlayan en fazla bir tek b vardır (hiç olmayabilir de.) Nitekim $ab = ac = 1$ ise, o zaman $c = c1 = c(ab) = b(ac) = b1 = b$. Dolayısıyla tersinir bir a öğesi için $ab = 1$ eşitliğini sağlayan bir ve bir tane b öğesi vardır. Bu öğe a^{-1} olarak gösterilir ve bu öğeye a'nın (çarpma için) **tersi** ya da **çarpımsal tersi** denir. Demek ki, eğer bir halkada, $ab = 1$ ise a tersinirdir ve $b = a^{-1}$ dir.

Önsav 4. *R bir halka olsun.*

i. *$x, y \in R^*$ ise, $xy \in R^*$ ve $(xy)^{-1} = x^{-1}y^{-1}$.*

ii. *$x \in R^*$ ise, $x^{-1} \in R^*$ ve $(x^{-1})^{-1} = x$.*

iii. *$x \in R^*$ ve $xy = 0$ ise, o zaman $y = 0$.*

iv. *$x \in R^*$ ve $xy = xz$ ise, o zaman $y = z$.*

v. *$xy \in R^*$ ise, $x, y \in R^*$.*

Kanıt: MD-2004-I, sayfa 31, Önsav 4. □

Bir R halkasında, eğer bir $u \in R^*$ için $x = yu$ eşitliği sağlanıyorsa, x ve y elemanlarına **denk** denir. Bu durumda $x \sim y$ yazılır. Örneğin $\mathbb{Z}$ halkasında n ve $-n$ elemanları denktir. R^* kümesinin tüm elemanları birbirine denktir. Kolayca görüleceği üzere,

$$x \sim y \Leftrightarrow x \in yR^* \Leftrightarrow y \in xR^* \Leftrightarrow xR^* = yR^*.$$

V. Bölmek. R bir halka ve $a, b \in R$ olsun. Eğer $ax = b$ eşitliğini sağlayan bir $x \in R$ varsa, o zaman a, b'yi **böler** denir ve bu $a|b$ olarak yazılır. Eğer halkada bu denklemi sağlayan bir tane x varsa, o zaman $x = b/a$ yazılır. Eğer bu denklemi sağlayan birden fazla x varsa, b/a diye bir elemandan sözedemeyiz. Örneğin, $\mathbb{Z}/12\mathbb{Z}$'de, $2 \times 3 = 6 = 2 \times 9$ ve $\mathbb{Z}/12\mathbb{Z}$'de 6/2 diye bir elemandan sözedemeyiz. Öte yandan, $\mathbb{Z}/11\mathbb{Z}$'de 6/2 diye bir elemandan sözedebiliriz, çünkü $\mathbb{Z}/11\mathbb{Z}$ halkasında sadece $x = 3$ elemanı $2x = 6$ eşitliğini sağlar.

Verdiğimiz tanıma göre 0, 0'ı böler (bazı kitaplar bunu kabul etmezler, ama bizim kitabımız kabul ediyor) ve 0, halkanın başka hiçbir elemanını bölmez. Bir halkada 0/0 diye bir eleman yoktur, çünkü $1 \times 0 = 0 \times 0 = 0$.

Aşağıdaki önsavın kanıtı kolaydır ve okura bırakılmıştır.

Önsav 5. *R bir halka olsun.*

i. *Her $r \in R$, 0'ı böler ve eğer $r \neq 0$ ise sonuç her zaman 0'dır.*

ii. *R^* kümesinin her elemanı her elemanı böler. 1 her elemanı böler ve her $r \in R$ için, $r/1 = r$.*

iii. *R^* kümesinin bir elemanı ancak R^* kümesinden bir elemana bölünebilir.*

iv. *Eğer $u \in R^*$ ise, her x için $xu|x$.*

v. *Her $x \in R$ için, $x|x$.*

vi. *Her $x, y, z \in R$ için, $x|y$ ve $y|z$ ise $x|z$.*

VI. Tamlık Bölgeleri ve Cisimler. Eğer bir halkada her x, y için, $xy = 0$ eşitliği ya x'in ya da y'nin 0 olmasını gerektiriyorsa, o zaman o halkaya **tamlık bölgesi** ya da kısaca **bölge** adı verilir. Örneğin $\mathbb{Z}/6\mathbb{Z}$ bir tamlık bölgesi değildir, çünkü $\overline{2} \times \overline{3} = \overline{6} = \overline{0}$'dır ama ne $\overline{2}$ ne de $\overline{3}$ elemanı $\mathbb{Z}/6\mathbb{Z}$'de $\overline{0}$ değildir. Bu örnekten de anlaşılacağı üzere $\mathbb{Z}/n\mathbb{Z}$ halkasının bir tamlık bölgesi olması için gerek ve yeter koşul n doğal sayısının asal olmasıdır.

$\mathbb{Z}$, $\mathbb{Q}$ ve $\mathbb{R}$ birer tamlık bölgesidir. Eğer R bir tamlık bölgesiyse, $R[X]$ ve $R[X, Y]$ gibi polinom halkaları da tamlık bölgeleridir. [MD-2004-I, Sonuç 3, sayfa 28].

Tamlık bölgelerinde sadeleştirme yapılabilir, yani bir tamlık bölgesinde $a \neq 0$ ise ve $ab = ac$ ise $b = c$'dir, çünkü $a(b - c) = 0$'dır ve bir tamlık bölgesinde olduğumuzdan $b - c = 0$, yani $b = c$'dir.

Sıfır dışında her elemanı tersinir olan halkalara **cisim** denir. Yani bir cisimde $R^* = R \setminus \{0\}$ dir. $\mathbb{Q}$ ve $\mathbb{R}$ birer cisimdir, ama $\mathbb{Z}$ ve polinom halkalarının hiçbiri bir cisim değildir. Önsav 4.iii'e göre her cisim bir tamlık bölgesidir.

Alıştırmalar

1. $\mathbb{Z}/n\mathbb{Z}$ halkasının bir cisim olması için yeterli ve gerekli koşulun n'nin asal olmasıdır.

2. Bir tamlık bölgesinde eğer $x|y$ ve $y|x$ ise $x \sim y$.

3. $d \in \mathbb{N}$ bir tamkareye bölünmesin, örneğin $d = 2$ olabilir. $\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\}$ olsun. Bildiğimiz toplama ve çarpma altında $\mathbb{Q}[\sqrt{d}]$ bir halkadır. Bunun kanıtlaması oldukça kolaydır. $\mathbb{Q}[\sqrt{d}]$ halkasının ayrıca bir cisim olduğunu kanıtlayın.

4. Sonlu her tamlık bölgesinin bir cisim olduğunu kanıtlayın.

VII. Kartezyen Çarpım. R ve S birer halka olsun. $R \times S$ kartezyen çarpımını ele alalım:

$$R \times S = \{(r, s) : r \in R, s \in S\}.$$

Bu küme üstünde şu işlemleri tanımlayalım:

$$(r, s) + (r', s') = (r + r', s + s')$$
$$(r, s)(r', s') = (rr', ss').$$

Bu iki işlem altında $R \times S$ bir halkadır. $R \times S$ kümesinin sıfır ve birim elemanları sırasıyla $(0, 0)$ ve $(1, 1)$ elemanlarıdır.

Alıştırmalar

1. $(R \times S)^* = R^* \times S^*$ eşitliğini kanıtlayın.

2. $\mathbb{Z} \times \mathbb{Z}$ halkasında ne zaman bir (a, b) elemanı bir (c, d) elemanını böler?

3. R ve S birer halka olsun. $(R \times S)[X]$ polinom halkasının elemanları

$$\sum_i (r_i, s_i)X^i$$

biçiminde yazılırlar. $R[X] \times S[X]$ halkasının elemanları da

$$(\sum_i r_iX^i, \sum_i s_iX^i)$$

biçiminde yazılır. $\varphi : (R \times S)[X] \to R[X] \times S[X]$ fonksiyonu,

$$\varphi(\sum_i (r_i, s_i)X^i) = (\sum_i r_iX^i, \sum_i s_iX^i)$$

kuralıyla tanımlanmış fonksiyon olsun. φ'nin birebir ve örten olduğunu, birim elemanı birim elemana götürdüğünü ve toplama ve çarpmaya saygı duyduğunu, yani her $p, q \in (R \times S)[X]$ için,

$$\varphi(p + q) = \varphi(p) + \varphi(q)$$
$$\varphi(pq) = \varphi(p)\varphi(q)$$

eşitliklerini kanıtlayın.

4. R bir halka olsun. $e \in R$, $e^2 = e$ eşitliğini sağlasın. $Re = \{re : r \in R\}$ kümesinin toplama, çıkarma ve çarpma altında kapalı olduğunu kanıtlayın. Re'nin bir halka olduğunu kanıtlayın (e, bu halkanın birim elemanıdır.) $f = 1 - e$ olsun. $f^2 = f$ eşitliğini kanıtlayın. Dolayısıyla Rf de Re gibi bir halkadır. $R = Re + Rf$ ve $Re \cap Rf = \{0\}$ eşitliklerini kanıtlayın. Şimdi $\varphi : R \to Re \times Rf$ fonksiyonu $\varphi(r) = (re, rf)$ olarak tanımlansın. φ'nin birebir ve örten olduğunu, birim elemanı birim elemana götürdüğünü ve toplama ve çarpmaya saygı duyduğunu kanıtlayın.

VIII. Althalka. R ve S birer halka olsunlar. R'nin S'nin altkümesi olduğunu varsayalım. Ayrıca her $r_1, r_2 \in R$ için, $r_1 + r_2$ ve r_1r_2 işlemlerinin sonucunun R'de ve S'de aynı sonuçları verdiğini varsayalım. Yani R'nin elemanları R'de de toplansa, S'de de toplansa aynı sonucu bulduğumuzu varsayalım. Daha matematiksel deyişle $+_R$ ve $\times_R$, R'deki toplama ve çarpma işlemlerini, $+_S$ ve $\times_S$, S'deki toplama ve çarpma işlemlerini simgeliyorsa, her $r_1, r_2 \in R$ için

$$r_1 +_R r_2 = r_1 +_S r_2 \text{ ve } r_1 \times_R r_2 = r_1 \times_S r_2$$

olsun. Ayrıca $1_R = 1_S$ olsun. O zaman R'ye S'nin **althalkası** adı verilir. Bu durumda $R \leq S$ yazarız.

Örneğin $\mathbb{Z}$, $\mathbb{Z}[\sqrt{5}]$'in bir althalkasıdır, yani $\mathbb{Z} \leq \mathbb{Z}[\sqrt{5}]$. Ama $\mathbb{Z} \times \{0\}$ halkası $\mathbb{Z} \times \mathbb{Z}$ halkasının bir althalkası değildir. İşlemlerle ilgili koşullar sağlanmasına karşın, iki halkanın birim elemanları aynı değildir. Kolayca kanıtlanacağı üzere, eğer $R \leq S$ ise, $0_R = 0_S$'tir. Elbette $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$ ve her R halkası için $R \leq R[X] \leq R[X, Y]$. Ama $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}$'nin bir althalkası değildir. Eğer $n \neq m$ ise $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$'nin hiçbir zaman bir althalkası değildir.

$R \leq S$ ve $r, r' \in R$ olsun. r elemanı r' elemanını R'de bölmeyebilir, ama S'de bölebilir. Ya da R'de tersinir olmayan bir eleman S'de tersinir olabilir. Bir başka deyişle tersinir olmak, bölmek gibi kavramlar ve tanımlayacağımız daha birçok kavram mutlak kavramlar değildir, içinde bulunduğumuz halkaya göre değişirler. Bu yüzden hangi halkada düşündüğümüzü belirtmek için, kimileyin, "R'de böler", "R'de tersinirdir" diyeceğiz.

IX. Sıfırbölenler. Bir halkada, bir $y \neq 0$ için $xy = 0$ eşitliği sağlanabiliyorsa, o zaman x'e **sıfırbölen** adı verilir. 0 her zaman sıfırbölendir. Tersinir bir eleman sıfırbölen olamaz. Sıfır dışında sıfırböleni olmayan halkalara **tamlık bölgesi** adı vermiştik.

$\mathbb{Z}/12\mathbb{Z}$ halkasının sıfırbölenleri 2, 3, 4, 6, 8, 9, 10 elemanlarıdır. Genel olarak, $\mathbb{Z}/n\mathbb{Z}$ halkasının sıfırbölenleri n'yle ortak böleni olan elemanlardır (diğerleri de tersinir elemanlardır.)

Sıfırbölenlerin toplamı sıfırbölen olmak zorunda değildir. Örneğin 2 ve 3 elemanları $\mathbb{Z}/12\mathbb{Z}$'de sıfır bölendir, ama toplamı olan 2 + 3, yani 5 bu halkada bir sıfırbölen değildir.

Sıfırbölen olmayan bir eleman sadeleştirmeye izin verir: Eğer a sıfırbölen değilse (yani $ax = 0$ olduğunda $x = 0$ oluyorsa) ve $ab = ac$ ise, o zaman $b = c$'dir. Nitekim, $a(b - c) = ab - ac = 0$ eşitliğinden, $b - c = 0$ ve $b = c$ elde edilir.

Alıştırmalar

1. $\mathbb{Z}/6\mathbb{Z}[X]$ ve $\mathbb{Z}/8\mathbb{Z}[X]$ halkalarının sıfırbölenlerini bulun.

2. $\mathbb{Z}/n\mathbb{Z}$ halkasının sıfırbölenlerinin n'yle ortak böleni olan elemanların sınıfları olduğunu kanıtlayın. Bunlardan $n - \varphi(n)$ tane vardır (bknz. MD-2004-I, sayfa 39-41).

3. Bir R halkasında, belli bir n doğal sayısı için, $x^n = 0$ eşitliğini sağlayan elemanlara **sıfırgüç-**

lü denir. Sıfırgüçlü elemanlar sıfırbölendir elbet. Sıfırgüçlü elemanların toplamlarının da sıfırgüçlü olduğunu kanıtlayın. $\mathbb{Z}/n\mathbb{Z}$ halkasının sıfırgüçlü elemanlarını bulun.

4. R ve S birer halka olsun. $R \times S$ halkasının sıfırbölen ve sıfırgüçlülerini bulun.

X. Öznitelikseł Sayı ya da Karakteristik. $\mathbb{Z}/n\mathbb{Z}$ halkasında, bir elemanı kendisiyle n kez toplayınca halkanın sıfır elemanını elde ederiz, yani $\mathbb{Z}/n\mathbb{Z}$ halkasında, her $x \in \mathbb{Z}/n\mathbb{Z}$ için $nx = \bar{0}$'dır. Ayrıca n, $\mathbb{Z}/n\mathbb{Z}$ halkası için bu özelliği sağlayan en küçük pozitif doğal sayıdır. Bu kavramı $\mathbb{Z}/n\mathbb{Z}$ halkasından herhangi bir halkaya genelleştireceğiz.

R bir halka olsun. $n > 0$ bir doğal sayı olsun. Her $x \in R$ için $nx = 0$ ise ve n bu özelliği sağlayan en küçük pozitif doğal sayıysa, o zaman n'ye R'nin **öznitelikseł sayısı** ya da **karakteristiği** denir ve $\mathrm{char}(R) = n$ yazılır. Örneğin, $\mathrm{char}(\mathbb{Z}/n\mathbb{Z}) = n$, $\mathrm{char}((\mathbb{Z}/n\mathbb{Z})[X])) = n$ ve sayfa 21'deki $\wp(A)$ örneğinde, $\mathrm{char}(\wp(A)) = 2$.

Eğer böyle bir n yoksa, o zaman $\mathrm{char}(R) = 0$ yazılır.

Alıştırmalar

1. $\mathrm{char}(R) = n$ ve $\mathrm{char}(S) = m$ olsun. $\mathrm{char}(R \times S) = \mathrm{ekok}(n, m)$ eşitliğini kanıtlayın.

2. $R \leq S$ ise $\mathrm{char}(R) = \mathrm{char}(S)$.

XI. Asallar. R bir halka olsun. p, halkanın ne tersinir ne de sıfırbölen olan bir elemanı olsun. Her x, y için, p, xy çarpımını böldüğünde x ya da y'den en az birini bölmek zorundaysa o zaman p'ye **asal** denir.

$\mathbb{Z}$ halkasının asalları bildiğimiz 2, 3, 5, 7, 11, ... sayılarıdır. Ama bunların dışında –2, –3, –5, –7, –11 sayıları da asaldır. Bir halkada p asalsa ve $q \sim p$ ise q de asaldır. Birbirine denk olan asallar arasında ayrım gözetmemek gerekir, aynı rolleri üstlenirler.

$\mathbb{Z}/n\mathbb{Z}$ halkalarının her elemanı ya tersinir ya da sıfırbölen olduğundan bu halkalarda asal eleman yoktur.

5, $\mathbb{Z}$ halkasında asaldır, ancak aynı 5, $\mathbb{Z}[\sqrt{5}]$ halkasında asal değildir. Nitekim $\mathbb{Z}[\sqrt{5}]$ halkasında $5 = \sqrt{5} \times \sqrt{5}$, yani 5, $\sqrt{5} \times \sqrt{5}$ çarpımını $\mathbb{Z}[\sqrt{5}]$ halkasında böler ama $\sqrt{5}$'i bölmez.

Gene $\mathbb{Z}[\sqrt{5}]$ sayı halkasında, 2, $(\sqrt{5} + 1)(\sqrt{5} - 1)$ sayısını (yani 4'ü) böler ama 2 ne $\sqrt{5} + 1$'i ne de $\sqrt{5} - 1$'i böler. Demek ki $\mathbb{Z}$'de asal olan 2 sayısı, $\mathbb{Z}[\sqrt{5}]$ sayı halkasında asal değildir.

Asalların en önemli kullanım alanı aşağıdaki önsavda saklıdır.

Teorem 6. *Eğer bir halkada bir eleman sonlu sayıda asalın çarpımı olarak yazılıyorsa, o zaman böyle bir yazılım büyük ölçüde tek bir biçimde yapılır:* $p_1, ..., p_n$ *ve* $q_1, ..., q_m$ *asallarsa ve*

$$p_1 \cdots p_n = q_1 \cdots q_m$$

ise, o zaman $n = m$*'dir ve öyle bir*

$$\sigma: \{1, ..., n\} \to \{1, 2, ..., n\}$$

eşleşmesi vardır ki, her i *için* $p_i \sim q_{\sigma(i)}$ *denkliği sağlanır*[2].

Kanıt: Oldukça kolaydır. n üzerine tümevarımla yapılır. Bir tamlık bölgesi için kanıt MD-2004-I, Teorem 2, sayfa 36'da verilmiştir. Herhangi bir halka için de aynı kanıt geçerlidir (çünkü bir asal sıfırbölen değildir.) □

$\mathbb{Z}[\sqrt{5}]$ sayı halkasında,

$$(\sqrt{5} + 1)(\sqrt{5} - 1) = 2 \times 2$$

eşitliği geçerli olduğundan, Teorem 6'ya göre, 2, $\sqrt{5} - 1$ ve $\sqrt{5} + 1$ sayılarının $\mathbb{Z}[\sqrt{5}]$'te asal olamayacakları bir kez daha anlaşılır. (Ayrıntılar için, bknz. MD-2004-I, sayfa 23-24.)

Tersinir ve sıfırbölen olmayan her elemanın sonlu sayıda asalın çarpımı olarak yazıldığı halkalara **tek çarpanlama halkası** (TÇH) denir. Eğer halka ayrıca bir tamlık bölgesiyse, o zaman **tek çarpanlama bölgesi**nden ya da kısaca TÇB'den sözedilir. Örneğin $\mathbb{Z}$ bir TÇB'dir. $\mathbb{Z}/n\mathbb{Z}$ halkalarında her eleman ya tersinir ya da sıfırbölen olduğundan (yani hiç asal olmadığından), bu halkalar TÇH'dirler. Aynı nedenden bir cisim TÇB'dir. Bu sayımızda daha birçok TÇB örneği vereceğiz.

Şimdi Gauss'un çok yararlı bir sonucunu kanıtlayalım.

Önsav 7 [Gauss]. *R herhangi bir halka olsun. R'nin bir p elemanı R'de asalsa, $R[X]$ polinom halkasında da asaldır.*

Kanıt: Her şeyden önce R'de tersinir ya da sıfırbölen olmayan bir eleman, $R[X]$'te de tersinir ya da sıfırbölen değildir. Bu kolay. Şimdi R'nin p asalı

2 Bu teorem geçen sayıda böyle ifade edilmemişti. Doğru ifade yukardaki gibi olmalıdır. Bir önceki sayıdaki ifade şekli yanlış değildir ama eksiktir. Bir önceki sayıdaki kanıt bu teoremi de kanıtlar.

$a(X)b(X)$ polinom çarpımını $R[X]$'te bölsün. Bu, $a(X)b(X)$ polinomunun tüm katsayıları R'de p'ye bölünüyor demektir. p'nin ya $a(X)$'i ya da $b(X)$'i $R[X]$'te böldüğünü, yani p'nin ya $a(X)$'in ya da $b(X)$'in tüm katsayılarını böldüğünü kanıtlayacağız.

$$a(X) = a_0 + a_1X + ... + a_nX^n,$$
$$b(X) = b_0 + b_1X + ... + b_mX^m$$

olsun. p'nin ne $a(X)$'in ne de $b(X)$'in katsayılarının hepsini böldüğünü varsayalım. Demek ki belli $i \in \{0, 1, ..., n\}$ ve $j \in \{0, 1, ..., m\}$ için, p asalı $a_0, ..., a_{i-1}$ ve $b_0, ..., b_{j-1}$ katsayılarını R'de böler ama ne a_i'yi ne de b_j'yi R'de böler. (i ya da $j = 0$ olabilirler; örneğin $i = 0$ ise, bu, p, a_0'ı bölmez demektir.) Bundan bir çelişki elde edeceğiz. $a(X)b(X)$ çarpımının $(i + j)$-inci katsayısına bakalım:

$$\sum_{r+s = i+j} a_rb_s = a_0b_{i+j} + ... + a_ib_j + ... + a_{i+j}b_0.$$

p asalı bu toplamı bölüyor. Öte yandan, p, sağdaki terimlerin, belki a_ib_j dışında herbirini bölüyor, çünkü p asalı $a_0, ..., a_{i-1}$ ve $b_0, ..., b_{j-1}$ elemanlarının herbirini bölüyor. Demek ki p, a_ib_j elemanını da bölüyor. Ama asal olduğundan, bundan p'nin a_i ve b_j elemanlarından birini böldüğü çıkar. Bu bir çelişkidir. Demek ki p ya tüm a_i'leri ya da tüm b_j'leri bölüyor. □

Alıştırmalar

1. R ve S birer halka olsun. $R \times S$ halkasının asallarını bulun.

XII. İndirgenemezler. R bir halka olsun. p, halkanın ne tersinir ne de sıfırbölen olan bir elemanı olsun. Her x, y için, $p = xy$ eşitliği x ya da y'nin tersinir olmasını gerektiriyorsa, o zaman p'ye **indirgenemez** denir. Bu, bir anlamda, p elemanı "gerçekten" başka elemanların çarpımı olarak yazılamıyor demektir. Örneğin $\mathbb{Z}$'nin 11 elemanı 1×11, 11×1, $(-11) \times (-1)$ ve $(-1) \times (-11)$ biçiminde yazılır ama başka türlü iki sayının çarpımı olarak yazılamaz.

$\mathbb{Z}$ halkasının indirgenemezleri bildiğimiz 2, 3, 5, 7, 11, ... sayılarıdır. Ama bunların dışında –2, –3, –5, –7, –11 sayıları da indirgenemezdir. Genel olarak, bir halkada, p indirgenemezse ve $q \sim p$ ise q de indirgenemezdir. Birbirine denk olan indirgenemezler arasında ayrım gözetmemek gerekir, aynı rolleri üstlenirler.

$\mathbb{Z}/n\mathbb{Z}$ halkalarının her elemanı ya tersinir ya da sıfırbölen olduğundan bu halkalarda indirgenemez eleman yoktur.

5, $\mathbb{Z}$ halkasında indirgenemezdir, ancak aynı 5, $\mathbb{Z}[\sqrt{5}]$ halkasında indirgenir. Nitekim $\mathbb{Z}[\sqrt{5}]$ halkasında $5 = \sqrt{5} \times \sqrt{5}$ ve $\sqrt{5} \notin \mathbb{Z}[\sqrt{5}]^*$.

TÇB'lerde asalla indirgenemez arasında bir ayrım yoktur [MD-2004, sayfa 38, Teorem 7].

$\mathbb{Z}$ halkasında asallarla indirgenemezler arasında bir ayrım yoktur. [MD-2004-I, sayfa 17, Teorem 2] Birazdan göreceğimiz üzere her halkada her asal bir indirgenemezdir. Ama bunun tersi her zaman doğru olmayabilir, yani indirgenemezlerin asal olmadığı tamlık bölgeleri vardır.

Önsav 8. *Her asal bir indirgenemezdir.*

Kanıt: MD-2004-I, sayfa 36, Teorem 1'de bu önsav tamlık bölgeleri için kanıtlanmıştı. Ama aynı kanıt herhangi bir halka için de geçerlidir. □

Önsav 6 ve $(\sqrt{5} + 1)(\sqrt{5} - 1) = 2 \times 2$ eşitliği, 2, $\sqrt{5} - 1$ ve $\sqrt{5} + 1$ sayılarının $\mathbb{Z}[\sqrt{5}]$'te asal olmadığını söylüyor. Öte yandan bu elemanlar $\mathbb{Z}[\sqrt{5}]$ halkasında indirgenemezdirler (bknz. MD-2004-I, sayfa 24). Demek ki asal olmayan indirgenemezler de var.

Önsav 9. *R'nin bir indirgenemezi $R[X]$'te de indirgenemezdir.*

Kanıt: $p \in R$ indirgenemez olsun. Önce, p, R'de sıfırbölen ya da tersinir olmadığından, $R[X]$'te de sıfırbölen ya da tersinir değildir. Bunun kanıtı kolaydır ve okura bırakılmıştır. Şimdi $f, g \in R[X]$ için, $p = fg$ yazalım. Demek ki $p = f_0g_0$. Buradaki f_0 ve g_0, f ve g polinomlarının sabit terimleri elbet. Öte yandan, p, R'de indirgenemez olduğundan, ya f_0 ya da g_0 elemanı R'de tersinir. Diyelim $g_0 \in R^*$ ve $f_0 = pg_0^{-1}$. Şimdi Önsav 7'deki gibi düşünerek, tümevarımla, p'nin f'nin her katsayısını R'de böldüğü kolaylıkla kanıtlanabilir: p indirgenemezi $f_0, ..., f_{i-1}$ katsayılarını bölsün. fg'de X^i'nin katsayısı sıfır olduğundan,

$$f_0g_i + ... + f_{i-1}g_1 + f_ig_0 = 0$$

ve p indirgenemezi $f_0, ..., f_{i-1}$'i böldüğünden, en soldaki $f_0g_i + ... + f_{i-1}g_1$ terimini de böler, dolayısıyla f_ig_0'ı da böler. g_0 tersinir olduğundan, bundan, p'nin f_i'yi de böldüğü çıkar. Demek ki p, f'nin her katsayısını R'de bölüyor, yani p, f'yi $R[X]$'te bölüyor. Diyelim $h \in R[X]$ için, $f = ph$. Demek ki $p = fg = phg$, $hg = 1$ ve $g \in R[X]^*$. □

İndirgenemezlerin şu yararı vardır: Bir halkanın elemanlarının asalların çarpımı olarak yazılması Önsav 6'dan dolayı çok yararlıdır, büyük kolaylık sağlar, en azından halkanın çarpım tablosu kolaylıkla anlaşılır. Ama ne yazık ki bir halkanın

elemanları her zaman asallarının çarpımı olarak yazılamayabilir. O zaman, halkanın elemanlarını hiç olmazsa indirgenemezlerin çarpımı olarak yazmak isteriz. Bu da çoğunlukla tümevarımla kanıtlanır. En büyük sorun tümevarımın yapılacağı doğal sayının tanımlanmasıdır. Bu konudan MD-2004-I, sayfa 36-38'de sözetmiş ve 38inci sayfada aşağıdaki olguyu kanıtlamıştık:

Teorem 10. *K bir cisim ve d* = 0, 1, –1 *bir tamkareye bölünmeyen bir tamsayı olsun. O zaman,*
$K[X_1, ..., X_n]$, $\mathbb{Z}[X_1, ..., X_n]$, $\mathbb{Z}[\sqrt{d}][X_1, ..., X_n]$
halkalarının herbirinde tersinir ya da sıfır olmayan her eleman sonlu sayıda indirgenemezin çarpımıdır.

Bu teorem güzel olmasına güzel de, eksik. Nitekim,

$$K[X_1, ..., X_n] \text{ ve } \mathbb{Z}[X_1, ..., X_n]$$

halkaları için daha genel bir teorem doğrudur: Bu halkalarda tersinir ya da 0 olmayan her eleman sadece indirgenemezlerin değil, asalların çarpımı olarak yazılır, yani bu halkalar birer tek çarpanlama bölgesidir. Sayfa 47-50'de bu olguyu kanıtlayacağız. ♥

POLİNOMLARDA İNDİRGENEMEZLER

K bir cisim, R bir halka olsun.

$K[X]$'in sabit polinomları, ya sıfır ya da tersinir olduklarından, indigenemez olamazlar. Öte yandan 2, $\mathbb{Z}[X]$'te asaldır.

$K[X]$'in birinci dereceden polinomlarının hepsi elbette indirgenemezdir.

Sayfa 28'de kanıtlayacağımız Teorem 2'ye göre, $g \in R[X]$ ise ve bir $a \in R$ için, $g(a) = 0$ ise, o zaman $X - a$, g'yi $R[X]$'te böler, dolayısıyla böyle bir g, eğer derecesi 1'den büyükse indirgenir. Demek ki $R[X]$ halkasının derecesi 1'den büyük ve indirgenemez bir polinomunun R'de kökü olamaz. Ama bunun tersi doğru değildir, yani kökü olmamak indirgenemez olmak için yeterli neden değildir: Örneğin $(X^2 + 1)^2$ polinomunun $\mathbb{R}$'de kökü yoktur ama bu polinom $\mathbb{R}[X]$'te indirgenir. Hatta $2X - 4$ polinomunun $\mathbb{Z}$'de kökü yoktur ama bu polinom $\mathbb{Z}[X]$'te indirgenir.

$K[X]$'in ikinci ve üçüncü dereceden polinomları eğer indirgenebilirse, o zaman bu polinomları bölen indirgenemezlerden biri illa ki birinci dereceden olmak zorundadır, dolayısıyla ikinci ve üçüncü dereceden indirgenir polinomların kökleri vardır. Demek ki ikinci ve üçüncü dereceden polinomların $K[X]$'te indirgenemez olmaları için K'de köklerinin olmaması yeter ve gerekli koşuldur.

Bir polinomun indirgenirliği ya da indirgenemezliği içinde bulunduğu halkaya göre değişir. Örneğin, $X^2 + 1$ polinomu $\mathbb{R}[X]$ ve $\mathbb{Z}/3\mathbb{Z}[X]$ polinom halkalarında indirgenemezdir, ama aynı polinom $\mathbb{Z}/5\mathbb{Z}[X]$ ve $\mathbb{C}[X]$ halkalarında indirgenir, nitekim, $\mathbb{Z}/5\mathbb{Z}[X]$ halkasında $X^2 + 1 = (X - 2)(X - 3)$ ve $\mathbb{C}[X]$ halkasında $X^2 + 1 = (X + i)(X - i)$.

Eğer R, $2 = 0$ eşitliğinin sağlandığı bir halkaysa $X^2 + 1$ polinomu $R[X]$'te indirgenir, nitekim, böyle bir halkada $(X + 1)^2 = X^2 + 2X + 1 = X^2 + 1$ eşitliği geçerlidir.

Eğer K, $2 \neq 0$ eşitsizliğinin sağlandığı bir cisimse, o zaman $a \neq 0$ için $K[X]$'teki bir $aX^2 + bX + c$ polinomunun indirgenir olması için gerek ve yeter koşul $b^2 - 4ac$'nin K'de bir kare olmasıdır. Bunun kanıtını okura bırakıyoruz.

Gerçel sayılarda durum çok daha basittir, çünkü daha Matematik Dünyası'nda kanıtlamadığımız ve kanıtı pek de kolay olmayan Cebirin Temel Teoremi'ne göre, $\mathbb{R}[X]$'in ancak birinci ve ikinci dereceden polinomları asal olabilir.

$\mathbb{R}[X]$'in tek dereceli bir polinomunun kökü olduğunu, dolayısıyla derecesi 1'den büyükse indirgenir olduğunu kanıtlamak pek de zor değildir. Nitekim, eğer f'nin derecesi tekse, x, $\pm\infty$'a gittiğinde, $f(x)$ de başkatsayısının pozitif ya da negatifliğine göre, $\pm\infty$'a ya da $\mp\infty$'a gider, yani birbirine ters sonsuzlara gider, dolayısıyla f belli bir noktada sıfır olmak zorundadır; eğer $f(a) = 0$ ise, $X - a$, f'yi böler ve f indirgenirdir.

Genel olarak $K[X]$ halkasının indirgenemezlerini bulmak kolay olmayabilir, K oldukça basit bir cisim olsa bile. İndirgenemezlerini bulmak kolay olmasa da, $K[X]$'in her indirgenemezinin bir asal olduğunu kanıtlayabiliriz, sayfa 31'de kanıtlayacağız da. ♥