7. BÖLÜM
HALKA

HALKA KAVRAMI

7.1. Tanım: $A \neq \emptyset$ ve A kümesi üzerinde sırası ile ★ ve ☐ işlemleri tanımlansın. Eğer (A, ★, ☐) sistemi üzerinde,

H1) (A, ★) sistemi değişmeli grup,
H2) A kümesi ☐ işlemine göre yarı grup,
H3) A kümesinde ☐ işlemi ★ işlemi üzerine sağdan ve soldan dağılma özelliği var,

H1, H2 ve H3 aksiyomlarını sağlıyorsa (A, ★, ☐) sistemi bir halkadır. Burada özel olarak etkisiz elemanlar karıştırmamak için. ★ işleminin etkisiz elemanına sıfır eleman ☐ işleminin etkisiz elemanına birim eleman diyeceğiz.

Eğer;

H4) "☐" işlemine göre A kümesinin birim elemanı varsa (A, ★, ☐) sistemi birimli halka denir.

H5) "☐" işlemine göre A kümesinin değişme elemanı varsa (A, ★, ☐) sistemi değişmeli halka denir.

Buna göre değişmeli ve birimli bir halka

i) ★ işlemine göre kapalı
ii) ★ işlemine göre değişmeli
iii) ★ işlemine göre birleşmeli
iv) ★işlemine göre sıfır (etkisiz) elemanın varlığı
v) ★işlemine göre ters elemanın varlığı
vi) ☐ işlemine göre kapalı
vii) ☐ işlemine göre değişmeli
viii) ☐ işlemine göre birleşmeli
ix) ☐ işlemine göre birim (etkisiz) elemanın varlığı
x) ★işlemi ☐ işlemi üzerine sağdan ve soldan dağılmalı

aksiyomlarını sağlar.

Örnek: $S = \{a + 2b : a, b \in \mathbb{Z}\}$ kümesi toplama ve çarpma işlemleri üzerinde bir halkadır.

Çözüm: H1) $(S, +)$ sistemi değişmeli grup mudur?

G1) Her $s_1, s_2, s_3 \in S$, $s_1 = a + 2b$, $s_2 = c + 2d$, $s_3 = e + 2f$ olmak üzere,

$$\begin{aligned} s_1 + (s_2 + s_3) &= (a + 2b) + [(c + 2d) + (e + 2f)] \\ &= (a + 2b) + [c + e + 2(d + f)] \\ &= (a + (c + e)) + 2(b + (d + f)) \\ &= ((a + c) + e) + 2((b + d) + f) \\ &= [(a + c) + 2(b + d)] + (e + 2f) \\ &= [(a + 2b) + (c + 2d)] + (e + 2f) \\ &= (s_1 + s_2) + s_3 \end{aligned}$$

olup toplama işleminin birleşme özelliği vardır.

G2) Her $s \in S$ ve $s = a + 2b$, $e = e_1 + 2e_2$ birim (etkisiz) eleman olmak üzere,

$$\begin{aligned} &s + e = s \\ &(a + 2b) + (e_1 + 2e_2) = a + 2b \\ &a + e_1 + 2(b + e_2) = a + 2b \\ &e_1 = e_2 = 0 \end{aligned}$$

ise $e = e_1 + 2e_1 = 0 + 2 \cdot 0$ olup toplama işleminin birim eleman $e = 0$ dır.

G3) Her $s \in S$ ve $s = a + 2b$ sayısının $x^{-1} = x_1^{-1} + 2x_2^{-1}$ ters eleman olmak üzere,

$$\begin{aligned} &s + x^{-1} = 0 \\ &(a + 2b) + (x_1^{-1} + 2x_2^{-1}) = 0 + 2 \cdot 0 \\ &(a + x_1^{-1}) + 2(b + x_2^{-1}) = 0 + 2 \cdot 0 \\ &x_1^{-1} = -x, x_2^{-1} = -y \end{aligned}$$

olup toplama işleminin ters elemanı $x^{-1} = -x - 2y$ dir.

G4) Her $s_1, s_2 \in \mathbb{Z}$, $s_1 = a + 2b$, $s_2 = c + 2d$ olmak üzere,

$$\begin{aligned} s_1, + s_2 &= (a+2b)+(c+2d) \\ &= (a+c)+2(b+d) \\ &= (c+a)+2(d+b) \\ &= (c+2d)+(a+2b) \\ &= s_2+s_1 \end{aligned}$$

olup toplama işleminin değişme özelliği vardır. Buna göre $(S,+)$ sistemi değişmeli gruptur.

H2) Her $s_1, s_2, s_3 \in S$, $s_1 = a+2b$, $s_2 = c+2d$, $s_3 = e+2f$ olmak üzere,

$$\begin{aligned} s_1 \cdot (s_2 \cdot s_3) &= (a+2b)[(c+2d)(e+2f)] \\ &= (a+2b)[ce+2(cf+de)+4df] \\ &= ace+2(acf+ade+bce)+4(adf+bcf+bde)+8bdf \\ &= [(ac+2(ad+bc)+4bd](e+2f) \\ &= [(a+2b)(c+2d)](e+2f) \\ &= (s_1 \cdot s_2) \cdot s_3 \end{aligned}$$

olup çarpma işleminin birleşme özelliği vardır. Şu halde $(S, \cdot)$ sistemi yarı gruptur.

H3) Her $s_1, s_2, s_3 \in S$, $s_1 = a+2b$, $s_2 = c+2d$, $s_3 = e+2f$ olmak üzere,

$$\begin{aligned} s_1 \cdot (s_2 + s_3) &= (a+2b)[(c+2d)+(e+2f)] \\ &= (a+2b)(c+2d)+(a+2b)(e+2f) \\ &= s_1 \cdot s_2 + s_1 \cdot s_3 \end{aligned}$$

olup toplam işleminin çarpma işlemi üzerine soldan dağılma özellikleri vardır. Benzer şekilde sağdan dağılma özellikleri gösterilir.

H4) Her $s \in S$, $s = a+2b$ ve $e = e_1 + 2e_2$ birim (etkisiz) eleman olmak üzere,

$$s \cdot e = s$$
$$(a+2b) \cdot (e_1 + 2e_2) = a+2b$$
$$ae_1 + 2(ae_2 + be_1) + 4be_2 = a+2b$$
$$e_1 = 1, e_2 = 0$$

olup çarpma işleminin birim eleman $e = 1$ dır.

H5) Her $s_1, s_2 \in S, s_1 = a + 2b, s_2 = c + 2d$ olmak üzere,

$$
\begin{aligned}
s_1 \cdot s_2 &= (a + 2b)(c + 2d) \\
&= ac + 2(ad + bc) + 4bd \\
&= ca + 2(cb + da) + 4db \\
&= (c + 2d)(a + 2b) \\
&= s_2 \cdot s_1
\end{aligned}
$$

olup çarpma işleminin değişme özelliği vardır.

H1, H2, H3, H4 ve H5 aksiyomlarını sağlandığından $(S, +, \cdot)$ sistemi değişmeli ve birim elemanlı halkadır.

Örnek: $\mathbb{R}$ sayılar kümesi üzerinde tanımlanan bütün polinomların kümesini $R_{[x]}$ ile gösterelim. $(R_{[x]}, +, \cdot)$ sistemi değişmeli halka olduğunu gösterelim.

Çözüm: Her $n \in \mathbb{N}^+, a_n \neq 0$ olmak üzere $P : \mathbb{R} \to \mathbb{R}$,

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{k=0}^{n} a_k x^n$$

biçiminde polinom fonksiyonları olduğunu biliyoruz.

H1) $(R_{[x]}, +, \cdot)$ sistemi değişmeli grup mudur?

Her n. dereceden $P(x), Q(x), R(x) \in R_{[x]}$ polinomları

$$P(x) = \sum_{k=0}^{n} a_k x^k \ , \ Q(x) = \sum_{k=0}^{n} a_k x^k \ , \ R(x) = \sum_{k=0}^{n} a_k x^k$$

olsunlar. Bu takdirde,

G1)

$$
\begin{aligned}
P(x) + \big(Q(x) + R(x)\big) &= \sum_{k=0}^{n} a_k x^k + \left(\sum_{k=0}^{n} b_k x^k + \sum_{k=0}^{n} c_k x^k \right) \\
&= \sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{n} (b_k + c_k) x^k \\
&= \sum_{k=0}^{n} (a_k + (b_k + c_k)) x^k
\end{aligned}
$$

$$=\sum_{k=0}^{n}((a_k+b_k)+c_k)x^k$$
$$=\sum_{k=0}^{n}(a_k+b_k)x^k+\sum_{k=0}^{n}c_kx^k$$
$$=\left(\sum_{k=0}^{n}a_kx^k+\sum_{k=0}^{n}b_kx^k\right)+\sum_{k=0}^{n}c_kx^k$$
$$=(P(x)+Q(x))+R(x)$$

olduğundan toplama işleminin birleşme özelliği vardır.

G2) Her n. dereceden $P(x) \in R_{[x]}$ polinom olsun. Bu takdirde,

$$P(x)+e(x)=P(x)$$
$$\sum_{k=0}^{n}a_kx^k+\sum_{k=0}^{n}0\cdot x^k=\sum_{k=0}^{n}a_kx^k$$
$$\sum_{k=0}^{n}(a_k+0)x^k=\sum_{k=0}^{n}a_kx^k$$

olacak şekilde $e(x)=0$ (sıfır polinomu) vardır. Bu sıfır polinomu toplama işleminin birim elemanıdır.

G3) Her n. dereceden $P(x) \in R_{[x]}$ polinom olsun. Bu takdirde,

$$P(x)+P^{-1}(x)=e(x)$$
$$\sum_{k=0}^{n}a_kx^k+\sum_{k=0}^{n}(-a_k)x^k=\sum_{k=0}^{n}0\cdot x^k$$
$$\sum_{k=0}^{n}(a_k-a_k)x^k=\sum_{k=0}^{n}0\cdot x^k$$

olacağından $P^{-1}(x)=-a_nx^n-a_{n-1}x^{n-1}-\cdots-a_1x-a_0$ polinomu toplama işleminin ters elemanıdır.

G4) Her n. dereceden $P(x), Q(x) \in R_{[x]}$ polinomları

$$P(x)+Q(x)=\sum_{k=0}^{n}a_kx^k+\sum_{k=0}^{n}b_kx^k$$

$$=\sum_{k=0}^{n}(a_k+b_k)x^k$$
$$=\sum_{k=0}^{n}(b_k+a_k)x^k$$
$$=\sum_{k=0}^{n}b_kx^k+\sum_{k=0}^{n}a_kx^k$$
$$=Q(x)+P(x)$$

olduğundan toplama işleminin değişme özelliği vardır. Buna göre $(P_{[x]},+)$ sistemi değişmeli gruptur.

H2) Her n. dereceden $P(x), Q(x), R(x) \in R_{[x]}$ polinomları verilsin. "Toplam ve Çarpım Sembolü" konusundaki "iki polinomun çarpımı" teoremi gereği

$$P(x)\cdot\big(Q(x)\cdot R(x)\big)=\left(\sum_{k=0}^{n}a_kx^k\right)\cdot\left(\left(\sum_{k=0}^{n}b_kx^k\right)\cdot\left(\sum_{k=0}^{n}c_kx^k\right)\right)$$
$$=\left(\sum_{k=0}^{n}a_kx^k\right)\cdot\left(\sum_{k=0}^{n}s_{2k}x^{2k}\right) \qquad (1)$$

olacak şekilde $s_i, i = 0,1,2,\dots,n$ vardır. Burada

$$s_i = b_0c_i + b_1c_{i-1} + \cdots + b_ic_0$$

dir. (1) eşitliğinde yine iki polinom çarpımı yapılırsa

$$P(x)\cdot\big(Q(x)\cdot R(x)\big)=\sum_{k=0}^{n}t_{2k}x^{2k} \qquad (2)$$

olacak şekilde $t_i, i = 0,1,2,\dots,n$ vardır. Burada

$$t_i = a_0s_i + a_1s_{i-1} + \cdots + a_is_0$$

dir. Gerekli düzenlemeler yapılırsa

$$t_i = u_0c_i + u_1c_{i-1} + \cdots + u_ic_0$$

olacak şekilde

$$u_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0$$

vardır. Buna göre (2) eşitliği

$$P(x)\cdot\big(Q(x)\cdot R(x)\big)=\left(\sum_{k=0}^{n}u_{2k}x^{2k}\right)\cdot\left(\sum_{k=0}^{n}c_kx^k\right)$$
$$=\left(\left(\sum_{k=0}^{n}a_kx^k\right)\cdot\left(\sum_{k=0}^{n}b_kx^k\right)\right)\cdot\left(\sum_{k=0}^{n}c_kx^k\right)$$
$$=\big(P(x)\cdot Q(x)\big)\cdot R(x)$$

olduğundan çarpma işleminin birleşme özelliği vardır. Şu halde $(R_{[x]},\cdot)$ sistemi yarı gruptur.

H3) Her n. dereceden $P(x), Q(x), R(x) \in R_{[x]}$ polinomları verilsin.

$$\begin{aligned} P(x)\cdot\big(Q(x)+R(x)\big) &= \left(\sum_{k=0}^{n} a_k x^k\right)\cdot\left(\left(\sum_{k=0}^{n} b_k x^k\right)+\left(\sum_{k=0}^{n} c_k x^k\right)\right) \\ &= \left(\sum_{k=0}^{n} a_k x^k\right)\cdot\left(\sum_{k=0}^{n} b_k x^k\right)+\left(\sum_{k=0}^{n} a_k x^k\right)\cdot\left(\sum_{k=0}^{n} c_k x^k\right) \\ &= P(x)Q(x)+P(x)R(x) \end{aligned}$$

olup sağdan çarpmanın toplama üzerine dağılma özelliği olduğunu gösterir. Benzer şekilde soldan çarpmanın toplama üzerine dağılma özelliği gösterilir.

H4) Her n. dereceden $P(x) \in R_{[x]}$ polinom olsun.

$$P(x)\cdot e(x) = P(x)$$

olması için $e(x) = 1$ olmalıdır. Bu polinoma çarpma işleminin birim elemanıdır.

H5) Her n. dereceden $P(x), Q(x) \in R_{[x]}$ polinomları verilsin. “Toplam ve Çarpım Sembolü” konusundaki “iki polinomun çarpımı” teoremi gereği

$$\begin{aligned} P(x)\cdot Q(x) &= \left(\sum_{k=0}^{n} a_k x^k\right)\cdot\left(\sum_{k=0}^{n} b_k x^k\right) \\ &= \sum_{k=0}^{n} s_{2k} x^{2k} \qquad (1) \end{aligned}$$

olacak şekilde $s_i, i = 0,1,2,\dots,n$ vardır. Burada

$s_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$

$s_i = b_0 a_i + b_1 a_{i-1} + \cdots + b_i a_0$

yazılabileceğinden (1) eşitliği

$$\begin{aligned} P(x)\cdot Q(x) &= \left(\sum_{k=0}^{n} b_k x^k\right)\cdot\left(\sum_{k=0}^{n} a_k x^k\right) \\ &= Q(x)\cdot P(x) \end{aligned}$$

olduğundan çarpma işleminin değişme özelliği vardır.

H1, H2, H3, H4 ve H5 aksiyomları sağlandığından $(R_{[x]}, +, \cdot)$ sistemi değişmeli ve birim elemanlı halkadır.

Örnek: i) $(\mathbb{Z}, +, \cdot)$ sistemi halkadır.
ii) $(\mathbb{R}, +, \cdot)$ sistemi halkadır.
iii) $(\mathbb{C}, +, \cdot)$ sistemi halkadır.

Bu örneğin çözümü okuyucuya bırakılmıştır.

Örnek: Her $\bar{a}, \bar{b} \in \mathbb{Z}_m$ ve $m \in \mathbb{Z}^+$ için

$$\bar{a} \oplus \bar{b} = \overline{a+b} \text{ ve } \bar{a} \otimes \bar{b} = \overline{a+b}$$

biçiminde işlemler tanımlansın. Bu takdirde $(\mathbb{Z}_m, +, \cdot)$ sistemi halkadır.

Bu örneğin çözümü okuyucuya bırakılmıştır.

Örnek: $L = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} = \{(a, b, c) : a, b, c \in \mathbb{Z}\}$ kümesinde toplama ve çarpma işlemleri

$$(a, b, c) + (d, e, f) = (a + d, b + e, c + f)$$
$$(a, b, c)(d, e, f) = (a\,d, b\,d + c\,e, cf)$$

biçiminde olsun. $(L, +, \cdot)$ cebirsel yapısının bir halkadır.

Çözüm:

H1) $(L, +)$ değişmeli gruptur. Çünkü kapalıdır, birleşimlidir, birim eleman $(0, 0, 0)$ dır, (a, b, c) nin tersi $-(a, b, c) = (-a, -b, -c)$ dir ve değişme özelliği vardır.

H2)
$$\begin{aligned}(a, b, c)[(d, e, f)(g, h, i)] &= (a, b, c)[(d\,g, e\,g + f\,h, f\,i)] \\ &= (a\,d\,g, b\,d\,g + c\,e\,g + c\,f\,h, c\,f\,i) \\ &= (a\,d, b\,d + c\,e, c\,f)(g, h, i) \\ &= [(a, b, c)(d, e, f)](g, h, i)\end{aligned}$$

H3)
$$(a, b, c)[(d, e, f) + (g, h, i)] = (a, b, c)[(d + g, e + h, f + i)]$$

$$= (ad + ag, bd + bg + ce + ch, cf + ci)$$
$$= (a, b, c)(d, e, f) + (a, b, c)(g, h, i)$$

olduğundan soldan dağılma özelliği vardır. Benzer şekilde sağdan dağılma özelliğini gösterilir. Şu halde $(L, +, \cdot)$ bir halkadır.

H4) Birim elemanı bulalım;

$$(a, b, c)(x, y, z) = (a, b, c)$$
$$(ax, bx + cy, cz) = (a, b, c)$$
$$ax = a, bx + cy = b, cz = c$$
$$x = 1, y = 0, z = 1$$

olur. Ayrıca $(1, 0, 1)(a, b, c) = (a, b, c)$ olup $(1, 0, 1)$ birim elemandır. Yani $(L, +, \cdot)$ birim elemanlı bir halkadır.

H5) $(1, 0, 0)(0, 1, 0) = (0, 0, 0)$ fakat $(0, 1, 0)(1, 0, 0) = (0, 1, 0)$ olup çarpmanın değişme özelliği yoktur. $(L, +, \cdot)$ değişmeli halka değildir.

7.1. Not: Bundan sonraki kısımlarda kolaylık olması amacıyla ★ ve ☐ semboller yerine toplama ve çarpma işlemi sembolleri tercih edilecektir. Klasik sembollerle işlemler yapılacaktır.

Bir a elemanının toplama işlemine göre tersi $-a$ ile gösterilir ve $a + (-b)$ yerine $a - b$ yazacağız.

7.2. Tanım: $(R, +, \cdot)$ halkasında toplama işlemine göre olan birim elemana halkanın sıfırı denir ve 0_R veya 0 ile gösterilir.

7.2. Not: Bir halkada çarpma işleminin toplama üzerine soldan dağılma özelliği varsa ve bu halka değişmeli ise çarpma işleminin toplama üzerine sağdan dağılma özelliği de vardır, gerçekten:

$$(a + b) \cdot c = c \cdot (a + b) = c \cdot a + c \cdot b = a \cdot c + b \cdot c$$

biçimindedir.

7.1. Teorem: R bir halka ve $a, b, c \in R$ olsun.

i. $a + c = b + c$ ise $a = b$ (Sağdan kısaltma)
ii. $c + a = c + b$ ise $a = b$ (Soldan kısaltma)
iii. Bir halkanın sıfırı tektir.
iv. Toplamaya göre ters eleman tektir.
v. $a + x = b$ denkleminin tek çözümü $x = b - a$ dir.
vi. R'nin birim elemanı varsa tektir.
vii. a'nın çarpmaya göre tersi varsa tektir.

Bu teoremin ispatı grup konusundaki ispatın benzeri olduğundan okuyucuya bırakılmıştır.

7.2. Teorem: R bir halka olsun. Her $a, b \in R$ için:

i. $a0 = 0a = 0$
ii. $(-a)b = a(-b) = -(ab)$
iii. $(-a)(-b) = ab$

İspat:

i. $a0 = a(0 + 0) = a0 + a0$ veya $0 + a0 = a0 + a0$ yazabiliriz. Sağdan kısaltma kuralını kullanırsak $a0 = 0$ elde edilir. Benzer şekilde $0a = 0$ olduğu gösterilebilir.

ii. $(-a)b + ab = (-a + a)b = 0b = 0$ olduğundan $-(ab) = (-a)b$ olur. Benzer şekilde $a(-b) = -(ab)$ gösterilebilir.

iii. Eğer $(-a)b = a(-b)$ eşitliğinde b yerine $(-b)$ yazarsak,
$$(-a)(-b) = a(-(-b)) = ab$$
dır.

7.3. Tanım: $R = \{0\}$ olması durumunda birim elemanlı bir halkanın sıfırı ile birim elemanı eşit olabilir. Yani $0_R = 1_R$ dir. Bu halkaya trivial halka veya sıfır halkası denir. Şöyle ki; bir R halkasında $0_R = 1_R$ ise her $a \in R$ için $0 = 0 \cdot a = 1 \cdot a = a$ olup $R = \{0\}$ olur.

Alt Halka

7.4. Tanım: R bir halka ve $\varnothing \neq S \subseteq R$ olsun. Eğer S, R'deki işlemlerle birlikte bir halka oluyorsa S'ye R'nin bir alt halkası denir.

Örnek: $\mathbb{Z}$ halkası $\mathbb{Q}$'nun; $\mathbb{Q}$ halkası da $\mathbb{R}$'nin alt halkasıdır. $2\mathbb{Z}$ halkası $\mathbb{Z}$'nin alt halkasıdır.

7.3. Teorem: R bir halka ve $\varnothing \neq S \subseteq R$ olsun. S'nin alt halka olması için gerek ve yeter şartlar:

i) Her $a, b \in S$ için $a - b \in S$

ii) Her $a, b \in S$ için $ab \in S$

İspat: $\Rightarrow$: S bir alt halka ve $a, b \in S$ olsun. $(S, +)$ grubu $(R, +)$ grubunun alt grubu olduğundan, alt grup olma teoreminden $a - b \in S$ ve yine aynı sebepten $ab \in S$ dir.

$\Leftarrow$ $S \neq \varnothing$ ve her $a, b \in S$ için $a - b \in S$ ve $ab \in S$ olsun. Alt grup teoreminden $(S, +)$ grubu $(R, +)$ grubunun alt grubudur. $S \subseteq R$ olduğundan + işlemi S'de de değişmelidir. Yine, $S \subseteq R$ olduğundan çarpma işlemi S'de de birleşmelidir ve $\cdot$ işleminin + üzerine soldan ve sağdan dağılma özelliği S'de de vardır. O halde S bir alt halkadır.

Örnek: H bir halka, $a \in H$ olsun. $I_a = \{x \in H : ax = 0\}$ kümesi H'nin bir alt halkası olduğunu gösteriniz.

Çözüm: $x, y \in I_a$ alalım. O zaman $ax = ay = 0$ dır.

i) $a(x - y) = a(x + (-y)) = ax + a(-y) = ax + (-(ay)) = ax - ay = 0$ olup $x - y \in I_a$ dır.

ii) $a(xy) = (ax)y = 0y = 0$ olup $xy \in I_a$ dır.

Buna göre I_a bir alt halkadır.

Örnek: $T = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$ kümesi $(\mathbb{R}, +, \cdot)$ halkasının bir alt halkası mıdır?

Çözüm: $a, b, c, d, e, f \in \mathbb{Q}$ ve $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, $y = d + e\sqrt[3]{2} + f\sqrt[3]{4}$ olsun. $a - d, b - e, c - f \in \mathbb{Q}$ olacağından

$$x-y=(a-d)+(b-e)\sqrt[3]{2}+(c-f)\sqrt[3]{4}\in T$$

olur. $(ad+2bf+2ce),(ae+bd+2cf),(af+be+cd)\in\mathbb{Q}$

$$xy=(ad+2bf+2ce)+(ae+bd+2cf)\sqrt[3]{2}+(af+be+cd)\sqrt[3]{4}+\in T$$

olur. Şu halde T bir alt halkadır.

Halka Homomofizması ve İzomorfizması

7.5. Tanım: $(R,\oplus,\ \odot)$ ve $(S,\boxplus,\otimes)$ iki halka ve $f\colon R\to S$ bir fonksiyon olsun. Eğer f toplama ve çarpma işlemlerini koruyorsa; yani

i) Her $a,b\in R$ için $f(a\oplus b)=f(a)\boxplus f(b)$

ii) Her $a,b\in R$ için $f(a\odot b)=f(a)\otimes f(b)$

ise f 'ye bir halka homomorfizması denir. Bu durumda $f\colon(R,\oplus)\to(S,\boxplus)$ bir grup homomorfizması olduğu açıktır. O halde grup homomorfizmalarındaki sonuçlar geçerlidir.

Mesela;

i) $f(0_R)=0_S$

ii) $f(-a)=-f(a)$

iii) $f(a-b)=f\big(a+(-b)\big)=f(a)\oplus f(-b)=f(a)\oplus\big(-f(b)\big)=f(a)-f(b)$

dir.

Örnek: $f:\mathbb{Z}_{20}\to\mathbb{Z}_{30}$, $f(\bar{x})=6\bar{x}$ şeklinde tanımlansın. $\bar{x},\bar{y}\in\mathbb{Z}_{20}$ için $\bar{x}\oplus\bar{y}=\bar{r}$ ve $\bar{x}\ \odot\ \bar{y}=\bar{s}$ ise $\mathbb{Z}$ 'de $x+y=20q+r$ ve $xy=20t+s$ dir ($q,t\in\mathbb{Z}$ ve $0\le r,s<20$). Bu durumda Z'de

$$6x+6y=6(x+y)=120q+6r\ \text{ ve } 6(xy)=120t+6s$$

olur. $\mathbb{Z}_{30}$'da ise

$f(\bar{x}\oplus\bar{y})=6(\bar{x}\oplus\bar{y})=6\bar{r}\ =\ 6\bar{x}\oplus 6\bar{y}\ =f(\bar{x})\oplus f(\bar{y})$

$f(\bar{x}\odot\bar{y})=6(\bar{x}\odot\bar{y})=6\bar{s}\ =(6\cdot 6)\bar{s}=(6\cdot 6)(\bar{x}\odot\bar{y})=(6\bar{x})\odot(6\bar{y})=f(\bar{x})\ \odot f(\bar{y})$

olur ve böylece f bir halka homomorfizmasıdır.

Örnek: $f:\mathbb{Z}_5 \to \mathbb{Z}_{10}$, $f(\bar{x}) = 5\bar{x}$ şeklinde tanımlansın. f bir halka homomorfizması değildir, gerçekten

$$f(\bar{3}\odot\bar{3}) = f(\bar{4}) = \bar{0} \text{ fakat } f(\bar{3})\odot f(\bar{3}) = \bar{5}\odot\bar{5} = \bar{5}$$

dir. Ayrıca, $f:(\mathbb{Z}_5,\oplus)\to(\mathbb{Z}_{10},\oplus)$ grup homomorfizması da değildir, gerçekten

$$f(\bar{4}\oplus\bar{4}) = f(\bar{3}) = \bar{5} \text{ fakat } f(\bar{4})\oplus f(\bar{4}) = \bar{0}\odot\bar{0} = \bar{0}$$

dir.

Örnek: $R = (\mathbb{Z},+,\cdot)$, $S = (2\mathbb{Z},+,\cdot)$ olsun. $f:R\to S$, $f(x) = 2x$ olarak tanımlansın.

$$f(x\oplus y) = 2f(x+y) = 2x+2y = f(x)+f(y)$$

olup f bir grup homomorfizmasıdır. Fakat genelde $f(xy) = 2xy \neq 2x2y = f(x)f(y)$ olup f bir halka homomorfizması değildir.

7.6. Tanım: $f:R\to S$ bir halka homomorfizması olsun. f birebir ve örten ise f 'ye bir halka izomorfizması denir. Eğer R'den S'ye bir halka izomorfizması var ise R ve S halkalarına izomorfiktir denir. $f:R\to R$ izomorfizma ise f 'ye bir halka otomorfizması denir.

Örnek: $H = \left\{\begin{bmatrix} a & b \\ -b & a\end{bmatrix} : a,b\in\mathbb{R}\right\}$ bilinen matris toplamı ve çarpımı ile bir halkadır.

a) $f:\mathbb{C}\to H$, $f(a+bi) = \begin{bmatrix} a & b \\ -b & a\end{bmatrix}$ bir halka homomorfizması mıdır?
b) f dönüşümü $\mathbb{C}$ ile H'yi izomorfik yapar mı?

Çözüm: $a,b,c,d\in\mathbb{R}$ olmak üzere $z = a+bi\in\mathbb{C}$ ve $w = c+di\in\mathbb{C}$ alalım.

$$\begin{aligned} f(z+w) &= f((a+c)+(b+d)i) \\ &= \begin{bmatrix} a+c & b+d \\ -b-d & a+c\end{bmatrix} \\ &= \begin{bmatrix} a & b \\ -b & a\end{bmatrix} + \begin{bmatrix} c & d \\ -d & c\end{bmatrix} \\ &= f(z)+f(w) \end{aligned}$$

$$\begin{aligned} f(zw) &= f((ac-bd)+(ab+bc)i) \\ &= \begin{bmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= f(z)\, f(w) \end{aligned}$$

şu halde f bir halka homomorfizmasıdır.

$$\begin{aligned} f(z) = f(w) &\Leftrightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &\Leftrightarrow a = c, b = d \\ &\Leftrightarrow a + bi, c + di \\ &\Leftrightarrow z = w \end{aligned}$$

olup f birebirdir. Şimdi verilen her $Y = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in H$ matrisi için $X = a + bi \in \mathbb{C}$ seçilirse $f(X) = Y$ olup f'nin örten olduğu görülür. Yani $\mathbb{C}$ ile H izomorfiktir.

Çarpık Halka

7.7. Tanım: R birim elemanlı bir halka olsun. Bir $u \in R$ elemanının çarpmaya göre tersi varsa u'ya bir birim denir. Bir halkadaki bütün birimlerin kümesi $U(R)$ ile gösterilir. $(U(R), \cdot)$ cebirsel yapısı bir gruptur.

7.3. Not: f birim elemanı ile f birimi faklı farklı kavramlardır.

Örnek: $U(\mathbb{Z}) = \{1, -1\}, U(\mathbb{Q}) = \mathbb{Q}\backslash\{0\}, U(\mathbb{C}) = \mathbb{C}\backslash\{0\}, U(\mathbb{Z}_6) = \{\overline{1}, \overline{5}\}$

7.8. Tanım: R bir halka olsun. Bir $a \in R$ için $a^n = 0$ olacak şekilde bir $n \in \mathbb{Z}^+$ varsa a'ya nilpotent denir. Mesela;

$\mathbb{Z}$ halkasındaki nilpotent elemanlar: $\{0\}$
$\mathbb{Q}$ halkasındaki nilpotent elemanlar: $\{0\}$
$\mathbb{Z}_8$ halkasındaki nilpotent elemanlar: $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$
$\mathbb{Z}_9$ halkasındaki nilpotent elemanlar: $\{\overline{0}, \overline{3}, \overline{6}\}$

Örnek: H birim elemanlı bir halka olsun. $x \in H$ nilpotent ise $(1-x)$ in ve $(1+x)$ in bir birim olduğunu gösteriniz.

Çözüm: $x \in H$ nilpotent olsun. O halde $\exists\, n \in \mathbb{Z}^{+}$ için $x^n = 0$ dır.

$$(1-x)(1+x+\cdots+x^{n-1}) = 1-x^n = 1$$

olup $(1-x)$ in tersi vardır. Yani $1-x$ birimdir. Ayrıca

$$(1-x)(1+x+\cdots+x^{n-1}) = \begin{cases} 1+x^n, & n \text{ tek sayı} \\ 1-x^n, & n \text{ çift sayı} \end{cases}$$

Her iki durumda da $1 \pm x^n = 1$ olup $1+x$ in birim olduğu görülür.

7.9. Tanım: Birim elemanlı bir halkanın, 0 hariç bütün elemanları birim ise bu halkaya çarpık halka denir. (Bazı kitaplarda bu kavrama çarpık cisim veya bölüm halkası adı verilmektedir.)

Örnek: $(\mathbb{Z}, +, \cdot)$ halkasının her elemanının çarpmaya göre tersi olmadığından çarpık halka değildir. $(\mathbb{Q}, +, \cdot)$ halkasının 0 hariç her elemanının çarpmaya göre tersi olduğundan bu halka bir çarpık halkadır. $\mathbb{Z}_6$ bir çarpık halkasıdır, gerçekten

$$1^{-1} = 1, 2^{-1} = 4, 3^{-1} = 5, 4^{-1} = 2, 5^{-1} = 3, 6^{-1} = 6$$

dır.

William Rowan Hamilton
04 Ağustos 1805, Dublin, İrlanda-02 Eylül 1865, Dublin, İrlanda

Örnek: $H = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}$ kümesi olarak tanımlanan Hamilton sayılarının oluşturduğu $(H, +, \cdot)$ sistemi çarpık halkadır. Gerçekten;

$$z_1 = a_1 + b_1 i + c_1 j + d_1 k \text{ ve } z_2 = a_2 + b_2 i + c_2 j + d_2 k$$

sayıları için toplama ve çarpma işlemi şöyle tanımlanır:

$$z_1 + z_1 = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$$

$$z_1 \cdot z_1 = (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i + \\ +(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k$$

Bu işlemlerle $(H, +, \cdot)$ birim elemanı 1 olan bir halkadır. $z = a + bi + cj + dk$ ise z'nin uzunluğu ve eşleniği

$$|z| = \sqrt{a^2 + b^2 + c^2 + d^2} \text{ ve } \bar{z} = a - bi - cj - dk$$

şeklinde tanımlanır. O zaman $z \neq 0$ ise

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$$

olup çarpma işlemine göre 0 hariç her elemanın tersi vardır.

Tamlık Bölgesi

7.10. Tanım: R bir halka, $a, b \in R$ ve $a \neq 0, b \neq 0$ olsun. Eğer $a \cdot b = 0$ ise a ve b'ye R'nin sıfır bölenleri denir. a'ya sol sıfır bölen, b'ye sağ sıfır bölen denir. R halkası değişmeli ise sol (sağ) sıfır bölen aynı zamanda sağ (sol) sıfır bölendir.

Örnek: $(\mathbb{Z}_{12}, \oplus, \odot)$ halkasının sıfır bölenlerini bulalım:

$$\bar{2}\odot\bar{6} = \bar{0}, \quad \bar{3}\odot\bar{4} = \bar{0}, \quad \bar{8}\odot\bar{9} = \bar{0}, \quad \bar{6}\odot\overline{10} = \bar{0}$$

olduğundan sıfır bölenlerin kümesi $\{\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \overline{10}\}$ dir.

7.4. Teorem: $\mathbb{Z}_n$ halkasının sıfır bölenleri, m ile n ile aralarında asal olmamak üzere m şeklindedir.

İspat: $m \in \mathbb{Z}_n$, m ile n aralarında asal olmasın. $\text{OBEB}(m;\ n) = d > 2$ olsun. Bu durumda

$$m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right)n \equiv 0 (\text{mod}\ n)$$

olur. Burada $\overline{m} \neq 0$ ve $\left(\frac{\overline{n}}{d}\right) \neq 0$ olduğundan $\overline{m}$ bir sıfır bölendir.

7.1. Sonuç: p asal ise $\mathbb{Z}_p$ nin sıfır bölenleri yoktur.

7.11. Tanım: Sıfır böleni olmayan, birim elemanlı, değişmeli ve en az 2 elemanlı bir halkaya tamlık bölgesi denir.

Örnek: p asal ise $\mathbb{Z}_p$ bir tamlık bölgesidir. Ayrıca $(\mathbb{Z}, +,\ \cdot)$, $(\mathbb{Q}, +,\ \cdot)$ ve $(\mathbb{R}, +,\ \cdot)$ birer tamlık bölgesidir. $(H, +,\ \cdot)$ halkası sıfır bölensizdir fakat değişmeli olmadığından bir tamlık bölgesi değildir.

Halkanın Karakteristiği

7.12. Tanım: R bir halka olsun. Her $a \in R$ için $na = 0$ olacak şekildeki en küçük n pozitif tamsayısına R halkasının karakteristiği denir ve kar R ile gösterilir. Eğer böyle bir n sayısı yoksa "halkanın karakteristiği sıfırdır" denir.

Örnek: $\text{kar}\ \mathbb{Z} = \text{kar}\ \mathbb{Q} = 0$ dır. $\text{kar}\ \mathbb{Z}_8 = 8$ dir. Ayrıca $\text{kar}\ 2\mathbb{Z} = 0$ dir. Karakteristiği 1 olan tek halka $R = \{0\}$ halkasıdır.

7.5. Teorem: R birim elemanı e ve karakteristiği n olan bir halka olması için gerek ve yeter şart n sayısı $ne = 0$ olacak şekildeki en küçük pozitif tamsayıdır.

İspat: $\Rightarrow$: Her $a \in R$ için $na = 0$ olup $e \in R$ için de $ne = 0$ dır.

$\Leftarrow$: n sayısı $ne = 0$ olacak şekildeki en küçük pozitif tamsayı olsun. Her $a \in R$ için;

$$\begin{aligned} na &= \underbrace{a + a + \cdots + a}_{\text{n tane}} \\ &= \underbrace{ae + ae + \cdots + ae}_{\text{n tane}} \end{aligned}$$

$$
\begin{aligned}
&= a(\underbrace{e + e + \cdots + e}_{\text{n tane}}) \\
&= a(ne) \\
&= a \cdot 0 \\
&= 0
\end{aligned}
$$

olur.

7.6. Teorem: Bir tamlık bölgesinin karakteristiği 0 veya asal bir sayıdır.

İspat: D bir tamlık bölgesi olsun. $\text{kar}\, D = 0$ ise ispat biter. $\text{kar}\, D = 1$ olamaz, gerçekten o zaman $D = \{0\}$ olurdu ve $\{0\}$ bir tamlık bölgesi değildir. $\text{kar}\, D = n > 2$ olsun. n'nin asal olduğunu göstermeliyiz. Aksine n asal olmasın. O halde $1 < n_1, n_2 < n$ olmak üzere $n = n_1 n_2$ şeklinde yazılabilir. $e \in D$ için $ne = 0$ dır. Şimdi:

$$
\begin{aligned}
&ne = 0 \\
&\underbrace{e + e + \cdots + e}_{\text{n tane}} = 0 \\
&(\underbrace{e + e + \cdots + e}_{n_1 \text{ tane}})(\underbrace{e + e + \cdots + e}_{n_2 \text{ tane}}) = 0 \\
&(n_1 e)(n_2 e) = 0
\end{aligned}
$$

olup D tamlık bölgesi olduğundan $n_1 e = 0$ veya $n_2 e = 0$ olmalıdır. Ancak bu durum n'nin $ne = 0$ olacak şekildeki en küçük pozitif tamsayı olması ile çelişir. O halde n asaldır.

Örnek: Birim elemanlı bir R halkasının birim elemanı ile onun en az 2 elemanlı bir S alt halkasının birim elemanı farklı olabildiğini gösteriniz.

Çözüm: $R = \mathbb{Z}_6$ ve $S = \{\bar{0}, \bar{3}\}$ alalım. Bu durumda R'nin birim elemanı $\bar{1}$ dir, fakat S'nin birim elemanı $\bar{3}$ dür. Ayrıca $S = \{\bar{0}, \bar{2}, \bar{4}\}$ alt halkasının birim elemanı $\bar{4}$ dür.

Örnek: R en az iki elemanlı bir halka olsun. Her $a \in R$ için $a^2 = a$ ise R'nin karakteristiğinin 2 olduğunu gösteriniz.

Çözüm: $(a + a)^2 = a + a$ olmalıdır. Tam kare açılımı yapılırsa

$$
\begin{aligned}
&a^2 + a^2 + a^2 + a^2 = a + a \\
&2a = 0
\end{aligned}
$$

elde edilir. R en az 2 elemanlı olduğundan $\text{kar}\, R \neq 1$ dir. O halde $\text{kar}\, R = 2$ dir.

7.7. Teorem: D birim elemanı e olan bir tamlık bölgesi, R'de D'nin en az iki elemanlı bir alt halkası olsun. R birim elemanlı ise $e \in R$ dir ve e, R'nin de birim elemanıdır.

İspat: $f \in R$ birim eleman olsun. Şimdi $f(fe - e) = f^2e - fe = fe - fe = 0$ elde edilir. D bir tamlık bölgesi olduğundan $f = 0$ veya $fe - e = 0$ olur. Ancak R en az 2 elemanlı olduğundan $f \neq 0$ dır. O halde $fe - e = 0$; yani $fe = e$ bulunur. Ayrıca e, D'nin birim elemanı olduğundan $fe = f$ olup $e = f$ elde edilir.

Örnek: Elemanları bir R halkasından seçilen $n \times n$ tipindeki matrislerin kümesi, matrislerdeki bilinen toplama ve çarpma işlemi ile bir halkadır. Bu halka $M_n(R)$ ile gösterilir.

$M_n(\mathbb{Z}) = \{n \times n \text{ tamsayı haneli matrisler}\}$
$M_n(\mathbb{R}) = \{n \times n \text{ reel haneli matrisler}\}$
$M_n(\mathbb{C}) = \{n \times n \text{ kompleks haneli matrisler}\}$

gibi. Benzer şekilde $M_n(\mathbb{Z}_7)$ ve $M_n(3\mathbb{Z})$ de tanımlıdır. $n \geq 2$ için bu halkalar değişmeli değildir. Eğer R birim elemanlı ise $M_n(R)$ de birim elemanlıdır ve birim elemanı, köşegeni 1_R olan skaler matristir. Ayrıca bu halkalar sıfır bölenlidir. Mesela $M_2(\mathbb{R})$ halkasında:

$$\begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix}\begin{bmatrix} 8 & -2 \\ -4 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

olur.

İDEALLER

Şimdi burada gruplardaki normal altgrup kavramına benzer bir kavram olan "ideal" kavramını vereceğiz.

7.13. Tanım: R bir halka, I'da R'nin bir alt halkası olsun. Eğer her $r \in R$ için $rI \subseteq I$ ise I'ya bir sol ideal, $Ir \subseteq I$ ise I'ya bir sağ ideal denir. Başka bir ifadeyle;

$\forall r \in R, \forall x \in I$ için $rx \in I$ oluyorsa I'ya sol idealdir
$\forall r \in R, \forall x \in I$ için $xr \in I$ oluyorsa I'ya sağ idealdir

Eğer I hem sağ hem de sol ideal ise I ya kısaca bir ideal denir.

Örnek: $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ ve $(\mathbb{R},+,\cdot)$ halkasında her $n\in\mathbb{Z}$ için $I=n\mathbb{Z}$ alt halkası bir idealdir. Gerçekten, $r\in\mathbb{Z}$ ve $x\in I$ seçelim. O zaman $\exists\, k\in\mathbb{Z}$ için $x=nk$ dır. Bu durumda

$$rx=r(nk)=n(rk)\in I \text{ ve } xr=(nk)r=n(kr)\in I$$

olup I'nın bir ideal olduğu görülür.

Örnek: $(\mathbb{Z},+,\cdot)$ halkası $(\mathbb{Q},+,\cdot)$ halkasının bir ideali değildir. Gerçekten $x=2\in\mathbb{Z}$ ve $r=\frac{1}{5}\in\mathbb{Q}$ seçilirse $xr=\frac{2}{5}\notin\mathbb{Z}$ olur.

Örnek: $W=\left\{\begin{bmatrix} a & b\\ c & d\end{bmatrix}: a,b,c,d\in\mathbb{Z}\right\}$ halkası ve $I=\left\{\begin{bmatrix} a & b\\ 0 & 0\end{bmatrix}: a,b\in\mathbb{Z}\right\}$ kümesi verilsin. I kümesi W'nun alt halkasıdır. $A=\begin{bmatrix} a & b\\ c & d\end{bmatrix}\in W$ ve $X=\begin{bmatrix} x & y\\ 0 & 0\end{bmatrix}\in I$ seçelim.

$$AX=\begin{bmatrix} ax & ay\\ cx & cy\end{bmatrix} \text{ ve } XA=\begin{bmatrix} ax+yc & xb+yd\\ 0 & 0\end{bmatrix}$$

olup genelde $AX\notin I$ ve $XA\in I$ olduğu görülür. Yani I bir sağ idealdir ama sol ideal değildir.

Örnek: A ve B bir R halkasının iki ideali olsun. $A+B=\{a+b: a\in A, b\in B\}$ kümesine A ile B'nin toplamı denir. $A+B$ nin R'nin bir ideali olduğunu gösterelim. $A+B$ nin alt halka olduğu kolayca gösterilebilir. Şimdi $r\in R$ ve $a+b\in A+B$ alalım. A ve B ideal olduğundan $ra, ar\in A$ ve $rb, br\in B$ olur. O zaman

$$r(a+b)=ra+rb\in A+B \text{ ve } (a+b)r=ar+br\in A+B$$

olup $A+B$ nin ideal olduğu görülür.

Örnek: Bir R halkasında $\{0\}$ ve R her zaman birer idealdir. Bunlara sırasıyla sıfır ideali (veya trivial ideal) ve öz olmayan ideal denir. Eğer $I\neq R$ ideal ise I'ya bir özideal denir.

7.8. Teorem: R bir halka $U\subseteq R$ olsun. U'nun bir ideal olması için gerek ve yeter şartlar:

i) $0\in U$

ii) Her $u,v\in U$ için $u-v\in U$

iii) Her $u,v\in U$ ve $r\in R$ için $ur\in U$ ve $ru\in U$

dır.

İspat: $\Rightarrow$: U bir ideal olsun. U bir alt halka olduğundan $0 \in U$ dur. Ayrıca $(U,+)$ grubu $(R,+)$ grubunun altgrubu olduğundan $u,v \in U$ ise $u-v \in U$ olduğu açıktır. U bir ideal olduğundan, tanımdan dolayı (iii) sağlanır.

$\Leftarrow$: (i), (ii) ve (iii) doğru olsun. $0 \in U$ olduğundan $U \neq 0$ U dir. $u,v \in U$ olsun. (ii) den dolayı $u-v \in U$ olduğu açıktır. $u \in R$ ve $v \in U$ olup (iii) den dolayı $uv \in U$ olur. Böylece U'nun bir alt halka olduğu görülür. Ayrıca, (iii) den dolayı da U bir idealdir.

Örnek: $I = \{m + rx : \ m \in M, r \in R\}$ kümesinin bir ideal olduğunu gösteriniz.

Çözüm: i) M ideal olduğundan $0 \in M$ olup $m = r = 0$ alınırsa $0 + 0x = 0 \in I$ dir.

ii) $m_1, m_2 \in M$ ve $r_1, r_2 \in R$ olmak üzere $a = m_1 + r_1 x \in I$ ve $b = m_2 + r_2 x \in I$ alalım. M ideal olduğundan $m_1 - m_2$ dir ve R halka olduğundan $r_1 - r_2 \in R$ dir. O halde

$$a - b = (\underbrace{m_1 - m_2}_{\in M}) + (\underbrace{r_1 - r_2}_{\in R})x \in I$$

olur.

iii) $m \in M$ ve $r \in R$ olmak üzere $a = m + rx \in I$ ve $y \in R$ alalım. M ideal olduğundan $ym \in M$ dir. O halde

$$ya = y(m + rx) = ym + y(rx) = \underset{\in M}{ym} + \underset{\in R}{(yr)}x \in I$$

elde edilir. Ayrıca, R değişmeli olduğundan $ay \in I$ dır.

Buna göre I bir idealdir.

Örnek: A ve B bir R halkasının iki ideali olsun.

$$A \cdot B = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in A, b_i \in B, n \in \mathbb{Z} \right\}$$

kümesine A ile B'nin çarpımı denir. $A \cdot B$ nin R'nin bir ideali olduğunu gösteriniz.

Çözüm: $A \cdot B$ kümesi A'daki elemanlar ile B'deki elemanların ikili çarpımlarının sonlu toplamından oluşmaktadır. Buna göre:

i) $0 \in A$, $0 \in B$ olup $0 = 0 \cdot 0 \in A \cdot B$ olur. ($a_1 = b_1 = 0$ ve $n = 1$ alınır.)

ii) $x = a_1b_1 + a_2b_2 + \cdots + a_nb_n \in AB$ ve $y = c_1d_1 + c_2d_2 + \cdots + c_md_m \in AB$ olsun. ($m, n \in \mathbb{Z}^+, a_ic_i \in A, b_id_i \in B$)

$$\begin{aligned} x - y &= (a_1b_1 + a_2b_2 + \cdots + a_nb_n) - (c_1d_1 + c_2d_2 + \cdots + c_md_m) \\ &= a_1b_1 + a_2b_2 + \cdots + a_nb_n + (-c_1)d_1 + (-c_2)d_2 + \cdots + (-c_m)d_m \end{aligned}$$

olup A ideal olduğundan $(-c_i) \in A$ dır ve $m + n \in \mathbb{Z}^+$ olduğundan $x - y \in AB$ olur.

iii) $x = a_1b_1 + a_2b_2 + \cdots + a_nb_n \in AB$ ve $r \in R$ alalım. A ideal olduğundan $i = 1,2,\cdots,n$ için $ra_i \in A$ olup

$$rx = r(a_1b_1 + a_2b_2 + \cdots + a_nb_n) = (ra_1)b_1 + (ra_2)b_2 + \cdots + (ra_n)b_n \in AB$$

olur. Benzer şekilde B ideal olduğundan $i = 1,2,\cdots,n$ için $b_ir \in B$ olup

$$xr = (a_1b_1 + a_2b_2 + \cdots + a_nb_n)r = a_1(rb_1) + a_2(rb_2) \ldots + a_n(rb_n) \in AB$$

olur. O halde dolayı AB bir ideal olur.

Örnek: R değişimli bir halka, $a \in R$ olsun. $I_a = \{x \in R : ax = 0\}$ kümesi R'nin bir idealidir, gösteriniz.

Çözüm: i) $a \cdot 0 = 0$ olduğundan $a \in I_a$ dır.

ii) $x, y \in I_a$ olsun. $a(x - y) = ax - ay = 0 - 0 = 0$ olup $x - y \in I_a$ dir.

iii) $x \in I_a$, $r \in R$ olsun. $a(xr) = (ax)r = 0r = 0$ olup $xr \in I_a$ dır. Ayrıca R değişmeli olduğundan $a(rx) = a(xr)$ (çünkü) $= (ax)r = 0r = 0$ dir.

Buna göre I_a bir ideal olur.

7.9. Teorem: R birim elemanlı bir halka, N de onun bir ideali olsun. Eğer N bir birim (. işlemine göre tersi olan bir eleman) içeriyor ise $N = R$ dir.

İspat: $u \in N$ bir birim olsun. $u^{-1} \in R$ olup N ideal olduğundan $uu^{-1} = 1_R \in R$ olur. Yine N ideal olduğundan her $r \in R$ için $u \cdot 1_R \in N$ olmalıdır. Yani her $r \in R$ için $r \in N$ olup $N = R$ elde edilir.

Örnek: $(H,+,\cdot)$, R'den R'ye bütün fonksiyonların halkası olsun. $I=\left\{f\in H : f\left(\frac{1}{2}\right)=0\right\}$ kümesi H'nin bir ideali midir?

Çözüm: (i) Bu halkanın sıfırı O ile gösterilen "sıfır" fonksiyonudur. $O\left(\frac{1}{2}\right)=0$ olduğundan $O\in I$ dır.

(ii) $f,g\in I$ ise $f\left(\frac{1}{2}\right)=g\left(\frac{1}{2}\right)=0$ olup

$$(f-g)\left(\frac{1}{2}\right)=f\left(\frac{1}{2}\right)-g\left(\frac{1}{2}\right)=0-0=0$$

olup $f-g\in$ dır.

(iii) $h\in H$ ve $f\in I$ alalım. O halde $f\left(\frac{1}{2}\right)=0$ dır.

$$(h\cdot f)\left(\frac{1}{2}\right)=h\left(\frac{1}{2}\right)f\left(\frac{1}{2}\right)=h\left(\frac{1}{2}\right)\cdot 0=0 \text{ ve}$$

$$(f\cdot h)\left(\frac{1}{2}\right)=f\left(\frac{1}{2}\right)g\left(\frac{1}{2}\right)=0\cdot h\left(\frac{1}{2}\right)=0$$

olup $h\cdot f, f\cdot h\in I$ olur ve şu halde I bir idealdir.

Örnek: $\phi : H\to K$ bir halka homomorfizması olsun.

a) Çek(ϕ), H'nin bir idealidir.

b) A, H'nin bir ideali ise $\phi(A)$ da $\phi(H)$ nin bir idealidir.

c) B, K'nın bir ideali ise $\phi^{-1}(B)$ de H'nin bir idealidir.
Gösteriniz.

Çözüm a) Çek(ϕ) nin bir alt halka olduğu gösterilmişti. Şimdi $x\in$ Çek(ϕ), $h\in H$ alalım.

$$\phi(xh)=\phi(x)\phi(h)=0_K\phi(h)=0_K$$

ve

$$\phi(hx)=\phi(h)\phi(x)=\phi(h)0_K=0_K$$

olup $xh, hx\in$ Çek(ϕ) olur. Yani Çek(ϕ) bir idealdir.

b) A bir alt halka olup ilgili teoremden dolayı $\phi(A)$ da bir alt halkadır. Burada $x \in \phi(A)$ ve $k \in \phi(H)$ alalım. Bu durumda $\exists\, a \in A$ için $\phi(a) = x$ ve $\exists\, h \in H$ için $\phi(h) = k$ dır. A bir ideal olduğundan $ah, ha \in A$ dır. O zaman

$$\phi(ah) = \phi(a)\phi(h) = xk, \phi(ha) = \phi(h)\phi(a) = kx \text{ ise } xk, kx \in \phi(A)$$

olup $\phi(A)$ bir idealdir.

c) B, K'nın bir ideali olsun. $\phi^{-1}(B) = \{x \in H :\ \phi(x) \in \phi(B)\}$ kümesidir.

i) $\phi : (H, +) \to (K, +)$ grup homomorfizması olduğundan $\phi(0_H) = 0_K$ dır ve B ideal olduğundan $0_K \in B$ dır. O halde $0_H \in \phi^{-1}(B)$ dir.

ii) $x, y \in \phi^{-1}(B)$ ise $\phi(x)\phi(y) \in B$ olup B bir ideal olduğundan

$$\phi(x) - \phi(h) \in B$$
$$\phi(x - y) \in B$$
$$x - y \in \phi^{-1}(B)$$

bulunur.

iii) $x \in \phi^{-1}(B)$ $h \in H$ alalım. $\phi(x) \in B$ ve $\phi(h) \in K$ olup B ideal olduğundan

$$\phi(xh) = \phi(x)\phi(h) \in B \ \text{ ve } \phi(hx) = \phi(h)\phi(x) \in B$$

olur. Yani $xh, hx \in \phi^{-1}(B)$ dir.

Buna göre $\phi^{-1}(B)$ bir ideal olur.

Örnek: Değişmeli bir R halkasında nilpotent elemanların oluşturduğu küme bir ideal olduğunu gösteriniz.

Çözüm: $N = \{x \in R : \exists\, n \in \mathbb{Z}^+, x^n = 0\}$ kümesi nilpotent elemanların kümesi olsun. $0^1 = 0$ olacağından $0 \in N$ dir.

$x \in N, r \in R$ alalım. O zaman $x^n = 0$ olacak şekilde $n \in \mathbb{Z}^+$ vardır. R değişmeli olduğundan

$$(rx)^n = (xr)^n = x^n r^n = 0 \cdot r^n = 0$$

olup $xr, rx \in N$ dir. Şimdi $x, y \in N$ olsun. O halde $x^m = 0$ ve $y^n = 0$ dır $(m, n \in \mathbb{Z}^+)$ dir. R değişmeli olduğundan

$$(x-y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^{n+m-i} (-1)^1 y^i$$

dir. Bu toplamdaki her bir terimde ya $n + m - i \geq m$ ya da $i > n$ dir. Yani toplamdaki her bir terim 0'dır.

O halde $(x - y)^{n+m} = 0$ olup $x - y \in N$ dir. O halde N bir idealdir.

7.14. Tanım: R değişmeli bir halka ve $I \neq R$ bir ideal olsun. Eğer her $a, b \in R$ için "$ab \in I$ ise $a \in I$ veya $b \in I$" önermesi doğru ise I'ya asal ideal denir.

Örnek: Bir R tamlık bölgesinde,

$$ab = 0 \text{ ise } a = 0 \text{ veya } b = 0$$

olduğundan $\{0_R\}$ bir asal idealdir

7.1. Lemma: $\mathbb{Z}$ halkasında $1 < n \in \mathbb{Z}$ verilsin. $P = n\mathbb{Z}$ ideali asal ideal olması için gerek ve yeter şart n asal olmasıdır.

İspat: $\Leftarrow$: n asal olsun. $a, b \in \mathbb{Z}$ ve $ab \in P = n\mathbb{Z}$ olsun. O zaman $n|(ab)$ demektir. n asal olduğundan $n|a$ veya $n|b$ dir. O zaman $a \in n\mathbb{Z} = P$ veya $b \in n\mathbb{Z} = P$ olur. O halde P asal idealdir.

$\Rightarrow$: Tersine, $P = n\mathbb{Z}$ bir asal ideal olsun. n'nin asal olduğunu gösterelim. Kabul edelim ki n asal olmasın. O halde $n = ab$ ve $a, b > 1$ dir. $ab \in P = n\mathbb{Z}$ olup P asal ideal olduğundan $a \in n\mathbb{Z}$ veya $b \in n\mathbb{Z}$ dir. Buna göre $n|a$ veya $n|b$ dir. $1 < a, b < n$ olduğundan çelişkidir. O halde n asaldır.

7.15. Tanım: R bir halka, $M \neq R$ de onun bir ideali olsun. Eğer R'nin $M \subsetneq R$ olacak şekilde başka bir I özideali yoksa M'ye maksimal ideal denir.

Örnek: $(\mathbb{Z}, +, \cdot)$ halkasında $6\mathbb{Z} \subsetneq 3\mathbb{Z} \subsetneq \mathbb{Z}$ olup $6\mathbb{Z}, 3\mathbb{Z}$ de bir ideal olduğundan $6\mathbb{Z}$ ideali maksimal ideal değildir.

Örnek: $(\mathbb{Z}, +, \cdot)$ da $M = 3\mathbb{Z}$ idealinin maksimal olduğunu gösterelim. $M \subsetneq R$ olacak şekilde bir I ideali olduğunu kabul edelim. Bu durumda I'da olup $3\mathbb{Z}$ de bulunmayan bir t elemanı vardır. O halde t, 3'ün katı olmadığından $t = 3k + \alpha$ şeklindedir $(k \in \mathbb{Z}, 1 \leq \alpha \leq 2)$. $t - \alpha = 3k$ olup $t - \alpha \in M$ yani $t - \alpha \in I$ dır. I ideal olduğundan $t - (t - \alpha) = \alpha \in I$ dır. Burada

$\alpha = 1$ ise $1 \in I$ olup $I = \mathbb{Z}$
$\alpha = 2$ ise $3 \in I, 2 \in I$ olup $3 - 2 = 1 \in I$ yani $I = \mathbb{Z}$

Her iki halde de $I = \mathbb{Z}$ olup M'nin maksimal ideal olduğu görülür.

Örnek: $(\mathbb{Z}, +, \cdot)$ da p asal olmak üzere $p\mathbb{Z}$ ideali maksimaldir. Çünkü $p\mathbb{Z} \subsetneq R$ olacak şekilde bir I ideali varsa $I = n\mathbb{Z}$ olacak şekilde pozitif bir n tamsayısı vardır. $p\mathbb{Z} \subsetneq n\mathbb{Z}$ olduğundan $n|p$ olmalıdır. $n \neq p$ ve p asal olduğundan $n = 1$ olmalıdır. O halde $I = 1 \cdot \mathbb{Z} = \mathbb{Z}$ dir.

BÖLÜM HALKALARI

Gruplar teorisindeki faktör grubu kavramına benzer bir kavramı halkalar için vereceğiz.

7.16. Tanım: $(\mathbb{R}, +, \cdot)$ bir halka ve I'da onun bir ideali olsun.

$$R/I = \{I + x : x \in R\}$$

kümesi üzerinde

$$(I + x) \oplus (I + y) = I + (x + y)$$
$$(I + x) \odot (I + y) = I + (xy)$$

biçiminde tanımlanan $(R/I, \oplus, \odot)$ halkasına R ile I'nın bölüm halkası denir. (Bundan sonraki kısımlarda kolaylık olması için $\oplus$ ve $\odot$ yerine + ve $\cdot$ kullanılacaktır)

7.4. Not: R/I kümesinin bu işlemlerle bir halka olduğunu göstermeden önce bu işlemlerin iyi tanımlandığını göstermeliyiz. $(I, +)$ grubu $(R, +)$ abelyen grubunun altgrubu olduğundan $I \lhd R$ dir. O halde toplama işlemi iyi tanımlanmıştır. Şimdi çarpma işleminin iyi tanımlandığını gösterelim.

$I + x = I + a$ ve $I + y = I + b$ ise $I + xy = I + ab$

olduğunu göstermeliyiz. $I + a = I + b \Leftrightarrow a - b \in I$ veya $b - a \in I)$ olduğunu hatırlayalım. Buradan

$I + x = I + a$ ise $x - a \in I$ ve $I + y = I + b$ ise $y - b \in I$

yazabiliriz. I bir ideal olduğundan $(x - a)y \in I$ ve $a(y - b) \in I$ dır. O halde

$$(x - a)y + a(y - b) = xy - ab \in I$$

elde edilir. Yani $I + xy = I + ab$ bulunur. O halde çarpma işlemi de iyi tanımlıdır.

7.5. Not: Eğer I, R'nin bir alt halkası olsaydı fakat bir ideali olmasaydı, çarpma işlemi iyi tanımlı olmayabilirdi. Bunu bir misal ile açıklayalım. $\mathbb{Z}$ halkası $\mathbb{Q}$ 'nun bir alt halkasıdır, fakat ideali değildir.

$\mathbb{Z} + (1/2) = \mathbb{Z} + (3/2)$ ve $\mathbb{Z} + (1/3) = \mathbb{Z} + (4/3)$

olup

$$(\mathbb{Z} + (1/2)) \cdot (\mathbb{Z} + (1/3)) = \mathbb{Z} + (1/6)$$

fakat

$$(\mathbb{Z} + (3/2)) \cdot (\mathbb{Z} + (4/3)) = \mathbb{Z} + (4/2) = \mathbb{Z} + 0$$

dır.

7.10. Teorem: R bir halka ve I'da onun bir ideali olsun.

a) R/I yukarıda tanımlanan işlemlerle bir halkadır.

b) R değişmeli halka ise R/I da değişmeli halkadır.

c) R birim elemanlı halka ise R/I da birim elemanlıdır ve birim elemanı $I + 1_R$ dir.

İspat: a) $I + a, I + b, I + c \in R/I$ verilsin.

i) $(I + a) + (I + b) = I + (a + b) \in R/I$, çünkü $a + b \in R$

ii) $[(I + a) + (I + b)] + (I + c) = I + (a + b + c)$
$= (I + a) + [(I + b) + (I + c)]$

iii) $(I + a) + (I + b) = I + (a + b) = I + (b + a) = (I + b) + (I + a)$

iv) $I + 0 = I$ birim eleman, çünkü $(I + a) + (I + 0) = I + (a + 0) = I + a$

v) $(I + a) + (I + (-a)) = I + 0$ olup $-(I + a) = I + (-a)$ dır.

vi) $(I + a)(I + b) = I + (ab) \in R/I$, çünkü $ab \in R$

vii) $[(I + a)(I + b)](I + c) = I + ((ab)c)$
$= I + (a(bc))$
$= (I + a)[(I + b)(I + c)]$

(viii) $(I + a)[(I + b) + (I + c)] = (I + a)(I + (b + c))$
$= I + (ab + ac)$
$= (I + a)(I + b) + (I + a)(I + c)$

olup çarpma işleminin toplama üzerine soldan dağılma özelliği vardır. Benzer şekilde sağdan dağılma özelliği de gösterilebilir.

b) R halkası değişmeli ve $ab \in R$ olsun.

$(I + a)(I + b) = I + ab = I + ba = (I + b)(I + a)$

olduğundan R/I da değişmelidir

c) $I + a \in R/I$ olsun.

$(I + a)(I + 1_R) = I + (a \cdot 1_R) = I + a$

ve

$(I + 1_R)(I + a) = I + (1_R \cdot a) = I + a$
olup $I + 1_R$ birim elemandır.

Örnek: $R = \mathbb{Z}$ halkasında $I = 4\mathbb{Z}$ idealini ele alalım.

$$R/I = \{I + 0, I + 1, I + 2, I + 3\}$$

bölüm halkasını elde ederiz. Bu halkanın işlem tabloları;

$+$	$I+0$	$I+1$	$I+2$	$I+3$
$I+0$	$I+0$	$I+1$	$I+2$	$I+3$
$I+1$	$I+1$	$I+2$	$I+3$	$I+0$
$I+2$	$I+2$	$I+3$	$I+0$	$I+1$
$I+3$	$I+3$	$I+0$	$I+1$	$I+2$

$\cdot$	$I+0$	$I+1$	$I+2$	$I+3$
$I+0$	$I+0$	$I+0$	$I+0$	$I+0$
$I+1$	$I+0$	$I+1$	$I+2$	$I+3$
$I+2$	$I+0$	$I+2$	$I+0$	$I+2$
$I+3$	$I+0$	$I+3$	$I+2$	$I+3$

Bu tablo $\mathbb{Z}/4\mathbb{Z}$ halkası ile $\mathbb{Z}_4$ halkası izomorfiktir. (Genel olarak $\mathbb{Z}/n\mathbb{Z}$ halkası ile $\mathbb{Z}_n$ halkası izomorfiktir.)

7.11. Teorem: R bir halka, I'da R'nin bir ideali olsun.

$$\phi : R \to R/I,\ \ \phi(x) = I + x$$

şeklinde tanımlanan dönüşüm, çekirdeği I olan, örten bir homomorfizmadır. Bu homomorfizmaya R'den R/I ya doğal homomorfizma denir.

İspat: $I + x \in R/I$ verilsin. $\phi(x) = I + x$ olup ϕ örtendir. Ayrıca $x, y \in R$ için

$$\phi(x + y) = I + (x + y) = (I + x) + (I + y) = \phi(x) + \phi(y)$$
$$\phi(xy) = I + (xy) = (I + x)(I + y) = \phi(x)\phi(y)$$

olup ϕ bir homomorfizmadır. Burada

$$k \in \text{Çek}(\phi) \Leftrightarrow \phi(k) = I + 0 = I \Leftrightarrow I + k = I \Leftrightarrow k \in I$$

olup $\text{Çek}(\phi) = I$ olduğu görülür.

Örnek: R bir halka I'da onun bir ideali olsun. R/I nın değişmeli olması için gerek ve yeter şart her $x, y \in R$ için $xy - yx \in I$ olmasıdır. Gösteriniz.

Çözüm:

$$\begin{aligned} R/I \text{ değişmeli} &\Leftrightarrow \forall\, x, y \in R \text{ için } (I + x)(I + y) = (I + y)(I + x) \\ &\Leftrightarrow \forall\, x, y \in R \text{ için } I + xy = I + xy \\ &\Leftrightarrow \forall\, x, y \in R \text{ için } I + (xy - yx) = I \\ &\Leftrightarrow \forall\, x, y \in R \text{ için } xy - yx \in I \end{aligned}$$

7.12. Teorem: R değişmeli ve birim elemanlı bir halka ve $I \subseteq R$ bir ideal olsun. I asal ideal olması için gerek ve yeter şart R/I tamlık bölgesidir.

İspat: $\Rightarrow$: I asal ideal olsun. $I \neq R$ olup R/I en az 2 elemanlıdır. $I + x, I + y \in R/I$ alalım ve R/I nın sıfırının I olduğunu hatırlayalım.

$$\begin{aligned}(I+x)(I+y) = I &\Rightarrow I + xy = I\\ &\Rightarrow xy \in I\\ &\Rightarrow x \in I \text{ veya } y \in I \text{ (I asal ideal)}\\ &\Rightarrow I + x = I \text{ veya } I + y = I\end{aligned}$$

olup R/I sıfır bölensizdir. R birim elemanlı ve değişmeli olup R/I da birim elemanlı ve değişmelidir, şu halde tamlık bölgesidir.

$\Leftarrow$: R/I bir tamlık bölgesi olsun. R/I en az 2 elemanlı olup $I \neq R$ dir. $x, y \in R$ olsun.

$$\begin{aligned}xy \in I &\Rightarrow I + xy = I\\ &\Rightarrow (I+x)(I+y) = I\\ &\Rightarrow I + x = I \text{ veya} I + y = I \text{ (R/I tamlık bölgesi)}\\ &\Rightarrow x \in I \text{ veya } y \in I\end{aligned}$$

olup I'nın asal ideal olduğu gösterilmiş olur.

ÇÖZÜMLÜ ALIŞTIRMALAR

1. R'de toplama ve çarpma,

$A + B = (A \cup B)\backslash(A \cap B)$ ve $A \cdot B = A \cap B$

olarak tanımlansın. Toplama işlemi birleşmeli olmak üzere $(R, +, \cdot)$ sistemi değişmeli ve birimli halka mıdır?

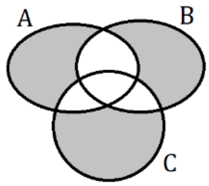
Çözüm:

i) $A, B \in R$ için $A + B = (A \cup B)\backslash(A \cap B) = A \,\Delta\, B \in R$

ii) $A + B = A \,\Delta\, B = B \,\Delta\, A = B + A$

iii) $A + (B + C) = A \,\Delta\, (B \,\Delta\, C) = (A \,\Delta\, B) \Delta\, C = (A + B) + C$

olduğunu en rahat Venn şaması çizerek gösterilir.



iv) $A + I = A$

$A \Delta I = A$

$(A \cup I) \setminus (A \cap I) = A$

olması için $I = \varnothing$ olmalıdır. Şu halde halkanın sıfırı boş kümedir.

v) $A + A^{-1} = \varnothing$

$A \Delta A^{-1} = \varnothing$

$(A \cup A^{-1}) \setminus (A \cap A^{-1}) = \varnothing$

olması için $A^{-1} = A$ olmalıdır.

vi) $A, B \in R$ için $A \cdot B = A \cap B \in R$

vii) $A \cdot B = A \cap B = B \cap A = B \cdot A$

viii) $A \cdot (B \cdot C) = A \cap (B \cap C) = (A \cap B) \cap C = (A \cdot B) \cdot C$

ix) Her $A \in R$ için

$A \cdot I = A$

$A \cap I = A$

olması için $I = A$ olmalıdır. Şu halde halkanın birimi kendisidir.

x) $A \cdot (B + C) = A \cdot (B \Delta C)$

$= A \cap (B \Delta C)$

$= (A \cap B) \Delta (A \cap C)$

$= (A \cdot B) \Delta (A \cdot C)$

çarpma işlemi değişmeli olduğundan sağdan ve soldan dağılma özelliği vardır.

Sonuç olarak R birim elemanlı ve değişmeli bir halkadır.

2. $H = \{f \mid f : \mathbb{R} \to \mathbb{R}$, bir fonksiyon$\}$ kümesi üzerinde $f, g \in H$ için

$(f + g)(x) = f(x) + g(x)$

$(f \cdot g)(x) = f(x) \cdot g(x)$

işlemleri tanımlansın.

a) $(H, +, \cdot)$ sisteminin bir halka mıdır?

b) $(H, +, \cdot)$ bir tamlık bölgesi midir?

Çözüm: a) $f, g, h \in H$ olsun.

i) $(f+g)(x) = f(x) + g(x) \in \mathbb{R}$ olup $f + g \in H$

ii) $f(x) + g(x) = g(x) + f(x)$ olup $f + g = g + f$

iii) $[f(x) + g(x)] + h(x) = f(x) + [g(x) + h(x)]$ olup $(f + g) + h = f + (g + h)$

iv) Her $x \in \mathbb{R}$ için $O(x) = 0$ şeklinde tanımlanan sıfır fonksiyonu bu halkanın sıfırıdır.

v) f 'nin toplama işlemine göre tersi $(-f)(x) = -f(x)$ şeklinde tanımlanan fonksiyondur. Gerçekten
$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0 = O(x)$$
dir.

vi) $f(x) \cdot g(x) \in \mathbb{R}$ olup $f \cdot g \in H$

vii) $[f(x) \cdot g(x)] \cdot h(x) = f(x) \cdot [g(x) \cdot h(x)]$ olup $(f \cdot g) \cdot h = f \cdot (g \cdot h)$

viii) $f(x)(g(x) + h(x)) = f(x) \cdot g(x) + f(x) \cdot h(x)]$ olup $f \cdot (g + h) = f \cdot g + f \cdot h$ dir. Benzer şekilde $(f + g) \cdot h = f \cdot h + g \cdot h$ bulunur.

Sonuç olarak, H bir halkadır.

b) $f(x) = \begin{cases} 0, & x \geq 1 \\ x^2, & x < 1 \end{cases}$ ve $g(x) = \begin{cases} \sin x\,, & x \geq 1 \\ 0, & x < 1 \end{cases}$
şeklinde alınırsa $f \neq 0$ ve $g \neq 0$ fakat $f\,g = 0$ olduğundan H bir tamlık bölgesi değildir.

3. $\mathbb{Z}$ üzerinde $a \oplus b = a + b - 1$ ve $a \odot b = a + b - ab$ işlemleri tanımlanıyor. $(\mathbb{Z}, \oplus, \odot)$ sistemi;
a) Değişmeli ve birim elemanlı bir halka mıdır?
b) Bir tamlık bölgesi midir?

Çözüm: a) $a, b, c \in \mathbb{Z}$ olsun.

i) $a \oplus b = a + b - 1 \in \mathbb{Z}$

ii) $a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$

iii) $a \oplus (b \oplus c) = a \oplus (b + c - 1)$
$$= a + (b + c - 1) - 1$$
$$= a + b + c - 2$$
$$= (a + b - 1) + c - 1$$
$$= (a \oplus b) + c - 1$$
$$= (a \oplus b) \oplus c$$

iv) $a \oplus e = a$
$$a + e - 1 = a$$
$$e = 1$$
halkanın sıfır elemanı 1'dir.

v) $a \oplus a^{-1} = e$
$$a + a^{-1} - 1 = 1$$
$$a^{-1} = 2 - a$$

vi) $a \odot b = a + b - ab \in \mathbb{Z}$

vi) $a \odot b = a + b - ab = b + a - ba = b \odot a$

viii) $a \odot (b \odot c) = a \odot (b + c - bc)$
$$= a + (b + c - bc) - a(b + c - bc)$$
$$= a + b + c - bc - ab - ac + abc$$
$$= (a + b - ab) + c - (a + b - ab)c$$
$$= (a \odot b) \odot c$$
olup çarpma işlemi birleşmelidir.

ix) $a \odot (b \oplus c) = a \odot (b + c - 1)$
$$= a + (b + c - 1) - a(b + c - 1)$$
$$= 2a + b + c - ab - ac - 1$$
$$= (a + b - ab) + (a + c - ac) - 1$$
$$= (a \odot b) \odot (a \odot b)$$
olup ı işlemi ı üzerine soldan dağılma özelliğine sahiptir. ı işlemi değişme özelliğine sahip olduğundan sağdan dağılma özelliği de vardır.

x) $a \odot e = a$
$$a + e - ae = a$$
$$e = 0$$
halkanın birim elemanı 0'dır.

$(\mathbb{Z}, \oplus, \odot)$ birim elemanlı ve değişmeli bir halkadır.

b) Sıfır bölen olmadığını gösterelim. Halkanın sıfırı 1, birim elemanı da 0’dır. $a\odot b = 1$ ve $a \neq 1$ olsun. Bu takdirde $b = 1$ olduğunu göstereceğiz.

$$a\odot b = 1$$
$$a + b - ab = 1$$
$$a + b - ab - 1 = 0$$
$$(a-1)(b-1) = 0$$

olup $a \neq 1$ olduğundan $b = 1$ dir.

Şu halde, $(\mathbb{Z}, \oplus, \odot)$ bir tamlık bölgesidir.

4. R birim elemanı 1 olan bir halka ve bir $a \in R$ için $a^2 = 1$ olsun. $H = \{axa : x \in R\}$ kümesinin R’nin bir alt halkası olduğunu gösteriniz.

Çözüm: $axa, aya \in H$ alalım.

i) $x - y \in R$ olduğundan $axa - aya = a(xa - ya) = a(x-y)a \in H$ dir.

ii) $xy \in R$ olduğundan $(axae)(aya) = axa^2ya = a(xy)a \in H$

Buna göre H bir alt halkadır.

5. $\mathbb{Z}[\sqrt{2}] = \{x + y\sqrt{2} : x, y \in \mathbb{Z}\}$ halkası verilsin. $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ fonksiyonu $f(x + y\sqrt{2}) = x - y\sqrt{2}$ ile tanımlansın. f'nin $\mathbb{Z}[\sqrt{2}]$ alt halka ve otomorfizması olduğunu gösteriniz.

Çözüm: a)

$$\begin{aligned} \text{i)} f[(a + b\sqrt{2}) + (c + b\sqrt{2})] &= f[(a + c) + (b + d)\sqrt{2})] \\ &= (a + c) - (b + d)\sqrt{2}) \\ &= (a - b\sqrt{2}) + (c - d\sqrt{2}) \\ &= f(a + b\sqrt{2}) + f(c + d\sqrt{2}) \end{aligned}$$

$$\begin{aligned} \text{ii)} f[(a + b\sqrt{2})(c + b\sqrt{2})] &= f[(ac + 2bd) + (ad + bc)\sqrt{2})] \\ &= (ac + 2bd) - (ad + bc)\sqrt{2}) \\ &= (a - b\sqrt{2})(c - d\sqrt{2}) \\ &= f(a + b\sqrt{2})f(c + d\sqrt{2}) \end{aligned}$$

olup f bir halka homomorfizmadır.

b) $f(a+b\sqrt{2}) = f(c+b\sqrt{2}) \Leftrightarrow a - b\sqrt{2} = c - d\sqrt{2}$
$\Leftrightarrow a = c \text{ ve } b = d$
$\Leftrightarrow a + b\sqrt{2} = c + d\sqrt{2}$
olduğundan f birebirdir.

Şimdi f 'nin örten olduğunu gösterelim. $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ verilsin. $f(x+y\sqrt{2}) = x - (-y)\sqrt{2}$ olup f'nin örten olduğu görülür.

O halde f bir otomorfizmadır.

6. Bir H halkasında $\forall\, x \in H$ için $x^2 = x$ biçimindedir.

a) $\forall\, x \in H$ için $x = -x$ olduğunu gösteriniz.
b) H'nin değişmeli olduğunu gösteriniz.

Çözüm: a) Her $x \in H$ için $(x+x)^2 = x + x$ olmalıdır. Tam kare açılımı yapılırsa
$x^2 + x^2 + x^2 + x^2 = x + x$
$x + x + x + x = x + x$
$x + x = 0$
$x = -x$
bulunur.

b) Her $a, b \in H$ için $(a+a)^2 = a + b$ olmalıdır. O halde
$a^2 + ab + ba + b^2 = a + b$
dir. $a^2 = a$ ve $b^2 = b$ olduğundan $ab + ba = 0$ olur. Şu halde
$ab = -(ba)$
$ab = (-b)(-a)$
$ab = ba$
bulunur. Şu halde halka değişmelidir.

7. Bir tamlık bölgesinde karesi kendisine eşit olan elemanların sadece 0 ve 1 olduğunu gösteriniz.

Çözüm: D bir tamlık bölgesi ve $x \in D$ olsun.

$x^2 = x \Leftrightarrow x^2 - x = 0 \Leftrightarrow x(x-1) = 0$

D bir tamlık bölgesi olduğundan $x = 0$ veya $x = 1$ olur.

8. $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ kümesinin bilinen kompleks sayı toplaması ve çarpması ile bir tamlık bölgesi olduğunu gösteriniz. (Bu halkaya Gauss tamsayılar halkası denir.)

Çözüm: Gauss tamsayılar halkasının birimli ve değişmeli halka olduğunu göstermek okuyucuya bırakılmıştır. Şimdi, $\mathbb{Z}[i]$ nin sıfır bölenleri olmadığını gösterelim.

$z_1, z_2 \in \mathbb{Z}[i], z_1 = a + ib, z_2 = c + id, z_1 z_1 = 0$ ve $z_1 \neq 0$ olsun. Bu durumda $a \neq 0$ veya $b \neq 0$ dır. $z_2 = 0$ olduğunu, yani $c = d = 0$ olduğunu göstereceğiz.

$$z_1 z_1 = 0$$
$$(a + ib)(c + id) = 0$$
$$(ac - bd) + i(ad + bc) = 0$$
$$ac - bd = 0, ad + bc = 0$$

denklemlerini çözeceğiz.

1. durum: $a \neq 0$ olmak üzere 1. denklemi c, 2. denklemi d ile çarpıp toplarsak

$$ac^2 - cbd = 0, ad^2 + bcd = 0$$
$$ac^2 + ad^2 = 0$$
$$a(c^2 + d^2) = 0$$
$$c^2 + d^2 = 0$$
$$c = d = 0$$

olur.

2. durum: $b \neq 0$ olmak üzere 1. denklemi $-d$, 2. denklemi c ile çarpıp toplarsak

$$-acd + bd^2 = 0, acd + bc^2 = 0$$
$$bd^2 + bc^2 = 0$$
$$b(d^2 + c^2) = 0$$
$$c^2 + d^2 = 0$$
$$c = d = 0$$

olur.

Buna göre $\mathbb{Z}[i]$ bir tamlık bölgesidir.

9. $A = \{a + b\sqrt[4]{5} : a, b \in \mathbb{Q}\}$ kümesi $(\mathbb{R}, +, \cdot)$ halkasının bir alt halkası mıdır?

Çözüm: $x = \sqrt[4]{5} \in A$ ve $y = \sqrt[4]{5} \in A$ alalım. $xy = \sqrt[4]{25} \notin A$ olur. Buna göre A bir alt halka değildir.

10. R ve H iki halka olsun. $f : R \to H$ dönüşümü her $x \in R$ için $f(x) = 0_H$ olarak tanımlansın. f 'nin bir halka homomorfizması olduğunu gösteriniz. (Bu homomorfizmaya sıfır homomorfizması denir.)

Çözüm: Her $x, y \in R$ için

$$f(x + y) = 0_H = 0_H + 0_H = f(x) + f(y)$$
$$f(x \cdot y) = 0_H = 0_H \cdot 0_H = f(x) \cdot f(y)$$

olup f bir halka homomorfizmasıdır.

11. R ve H iki halka $f : R \to H$ bir halka homomorfizması olsun.

a) I, R'nin bir alt halkası ise f(I) da H'nin bir alt halkasıdır.
b) $Çek(f) = \{x \in R : f(x) = 0_H\}$ kümesi R'nin bir alt halkasıdır.
c) R birim elemanlı halka, $H \neq \{0\}$ ve f örten ise H'da birim elemanlıdır ve $f(1_R) = 1_H$ dır.

Çözüm: a) $x, y \in f(I)$ ise $\exists\ a, b \in I$ için
$f(a) = x, f(b) = y$
$f(a - b) = f(a) - f(b) = x - y$, $(a - b \in I$, f grup homomorfizması)
$x - y \in f(I)$
olur. Ayrıca
$f(a \cdot b) = f(a) \cdot f(b) = x \cdot y$
olup $x \cdot y \in f(I)$ dır. f(I), H'nin alt halkasıdır.

b) $x, y \in Çek(f)$ ise
$f(a) = 0_H, f(b) = 0_H$
$f(a - b) = f(a) - f(b) = 0_H - 0_H = 0_H$, (f grup homomorfizması)
$x - y \in Çek(f)$
olur. Ayrıca
$f(a \cdot b) = f(a) \cdot f(b) = 0_H \cdot 0_H = 0_H$
olup $x \cdot y \in Çek(f)$ dır. Şu halde Çek(f), R'nin alt halkasıdır.

c) f örten olduğundan her $h \in H$ için $\exists\ r \in R$ vardır öyle ki $f(r) = h$ dir. Şimdi her $h \in H$ için
$$h = f(r) = f(1_R \cdot r) = f(1_R) \cdot f(r) = f(1_R) \cdot h$$
$$h = f(r) = f(r \cdot 1_R) = f(r) \cdot f(1_R) = h \cdot f(1_R)$$

olup H'nin birim elemanlı olduğu ve $f(1_R) = 1_H$ olduğu görülür.

15. D bir tamlık bölgesi olsun. $x \in D$ için "$x^2 = 1$ için $x = 1$ veya $x = -1$" olduğunu gösteriniz. Bunun sonucu olarak, eğer D sonlu sayıda birime sahipse bu birimlerin çarpımının -1 olduğunu gösteriniz.

Çözüm: $x^2 = 1 \Leftrightarrow x^2 - 1 = 0 \Leftrightarrow (x-1)(x+1) = 0 \Leftrightarrow$ D bir tamlık bölgesi olduğundan $x - 1 = 0$ veya $x + 1 = 0$ dır.

D deki bütün birimler $U = \{1, -1, u_1, u_2, \dots, u_n\}$ olsun. $x \in U$ için $x^{-1} = x \Leftrightarrow x^2 = 1$ olup tersi kendine eşit olan elemanların sadece 1 ve -1 olduğu görülür. $u = (-1)u_1u_2 \dots u_n$ dersek u_i lerin tersi kendisi olmadığından bu çarpımın sonucu -1 dir.

İdealler ve Bölüm Halkaları

16. $R = \mathbb{Z}_{12}$ halkasının bütün ideallerini, bölüm halkalarını, asal ve maksimal ideallerini belirleyiniz.

Çözüm: $\mathbb{Z}_{12}$ nin 6 tane ideali vardır.

$I = \{\bar{0}\}$	$R/I = \{I, I\oplus\bar{1}, I\oplus\bar{2}, \dots, I\oplus\overline{11}\}$
$J = \{\bar{0}, \bar{6}\}$	$R/J = \{J, J\oplus\bar{1}, J\oplus\bar{2}, J\oplus\bar{3}, J\oplus\bar{4}, J\oplus\bar{5}\}$
$K = \{\bar{0}, \bar{4}, \bar{8}\}$	$R/K = \{K, K\oplus\bar{1}, K\oplus\bar{2}, K\oplus\bar{3}\}$
$L = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$	$R/L = \{L, L\oplus\bar{1}, L\oplus\bar{2}\}$
$M = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$	$R/M = \{M, M\oplus\bar{1}\}$
$N = \mathbb{Z}_{12}$	$R/N = \{N\}$
Asal idealler:	K,L
Maksimal idealler:	K,L

17. İki idealin kesişiminin de bir ideal olduğunu gösteriniz.

Çözüm: I ve J bir R halkasının iki ideali olsun.

i) I ve J ideal olduklarından $0 \in I$ ve $0 \in J$ olup $0 \in I \cap J$ dir.

ii) $x, y \in I \cap J \Rightarrow x, y \in I$ ve $x, y \in J$
$\Rightarrow x - y \in I$ ve $x - y \in J$ (I ve J ideal)
$\Rightarrow x - y \in I \cap J$

iii) $x \in I \cap J$ ve $r \in R \Rightarrow x \in I, x \in J$ ve $r \in R$

$\Rightarrow xr, rx \in I$ ve $xr, rx \in J$ (I ve J ideal)

$\Rightarrow xr, rx \in I \cap J$

Şu halde $I \cap J$ bir idealdir.

18. A ve B bir R halkasının iki ideali ise $A \cdot B \subset A \cap B$ olduğunu gösteriniz.

Çözüm: $a_i \in A$ ve $b_i \in B$ olmak üzere $x = a_1b_1 + a_2b_2 + \cdots + a_nb_n \in AB$ alalım. Şimdi A bir ideal ve $i = 1,2,\cdots,n$ için $b_i \in R$ olduğundan $a_1b_1 + a_2b_2 + \cdots + a_nb_n \in A$ dir. O halde $x \in A$ dır. Benzer şekilde, B bir ideal ve $i = 1,2,\cdots,n$ için $a_i \in R$ olduğundan $a_1b_1 + a_2b_2 + \cdots + a_nb_n \in B$ dir. O halde $x \in B$ dır. Yani $x \in A \cap B$ dir. Buna göre $A \cdot B \subset A \cap B$ elde edilmiş olur.

19. R değişmeli bir halka ve N'de onun bir ideali olsun.

$$R_N = \{a^n \in N : n \in \mathbb{Z}^+, a \in R\}$$

kümesine N'nin radikali denir. R_N kümesi R'nin bir ideali olduğunu gösteriniz.

Çözüm: i) N ideal olduğundan $0 \in N$ dir. $0^1 = 0 \in N$ olup $1 \in \mathbb{Z}^+$ olduğundan $0 \in R_N$ dir.

ii) $x, y \in R_N$ yani $x^m, y^n \in N, m, n \in \mathbb{Z}^+$ olsun. R değişmeli olduğundan

$$(x-y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^{n+m-i} (-1)^i y^i$$

dir. N bir ideal olduğundan her bir terim N'nin bir elemanıdır. O halde $(x-y)^{m+n} \in N$ olup $m + n \in \mathbb{Z}^+$ olacağından $x - y \in R_N$ dir.

iii) $r \in R$ ve $x \in R_N$ olsun. En az bir $n \in \mathbb{Z}^+$ için $x^m \in N$ olsun. R değişmeli olduğundan ve N ideal olduğundan

$$(rx)^n = (xr)^n = \underbrace{x^n}_{\in N} \underbrace{r^n}_{\in R} \in N$$

olup $rx, xr \in R_N$ dir.

Buna göre R_N bir ideal olur.

20. R değişmeli bir halka, $K \subseteq R$ olsun.

$$S_K = \{ax = 0 : a \in R, \forall x \in K\}$$

kümesine K'nın sıfırlayıcısı denir. S_K kümesi R'nin bir ideali olduğunu gösteriniz.

Çözüm: i) Her $x \in K$ için $0 \cdot x = 0$ olup $0 \in S_K$ dır.

ii) $a, b \in S_K$ ise her $x \in K$ için $ax = bx = 0$ olup $(a - b)x = ax - bx = 0$ olduğundan $a - b \in S_K$ dır.

iii) $r \in R$, $a \in S_K$ olsun. O halde her $x \in K$ için $ax = 0$ dır. R değişmeli olduğundan, her $x \in K$ için

$$(ra)x = r(ax) = r \cdot 0 = 0 \text{ ve } (ar)x = (ra)x = r(ax) = 0$$

olup $ra, ar \in S_K$ dır.

Bundan dolayı S_K bir ideal olur.

21. $\mathbb{Z}_{12}$ de $S_K(\{\bar{3}\})$, $S_K(\{\bar{4}\})$ ve $S_K(\{\bar{3}, \bar{4}\})$ ideallerini bulunuz.

Çözüm:

$$S_K(\{\bar{3}\}) = \{a \in \mathbb{Z}_{12} : \bar{3} \odot a = \bar{0}\} = \{\bar{0}, \bar{4}, \bar{8}\}$$
$$S_K(\{\bar{4}\}) = \{a \in \mathbb{Z}_{12} : \bar{4} \odot a = \bar{0}\} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$$
$$S_K(\{\bar{3}, \bar{4}\}) = \{a \in \mathbb{Z}_{12} : \bar{3} \odot a = \bar{0} \text{ ve } \bar{4} \odot a = \bar{0}\} = \{\bar{0}\}$$

22. A ve B değişmeli bir R halkasının iki ideali olsun.

$$A : B = \{xb \in A : x \in R, \forall b \in B\}$$

kümesinin R nin bir ideali olduğunu gösteriniz.

Çözüm: i) Her $b \in B$ için $0 \cdot b = 0 \in A$ olup $0 \in A : B$ dir.

ii) $x, y \in A : B$ ise her $b \in B$ için $xb, yb \in A$ dır. $(x - y)b = xb - yb \in A$ olup $x - y \in A : B$ dir.

iii) $x \in A : B$ ve $r \in R$ alalım. Her $b \in B$ için $xb \in A$, R değişmeli ve A ideal olduğundan

$$(xr)b = (rx)b = r(\underbrace{xb}_{\in A}) \in A$$

olur. O halde $rx, xr \in A : B$ dir.

Buna göre A:B bir idealdir.

23. A ve B bir R halkasının iki ideali ve $A \cap B = \{0\}$ olsun. Her $a \in A$ ve her $b \in B$ için $ab = 0$ olduğunu gösteriniz.

Çözüm:

$a \in A, b \in B$ ise $a \in A, b \in R$ ve A ideal olup $ab \in A$

$a \in A, b \in B$ ise $a \in R, b \in B$ ve A ideal olup $ab \in B$

olduğundan $ab \in A \cap B = \{0\}$ olur. O halde $ab = 0$ dır.

24. A ve B bir R halkasının iki ideali ise $A + B$ nin bir alt halka olduğunu gösteriniz.

Çözüm: $x = a_1 + b_1 \in A + B$ ve $y = a_2 + b_2 \in A + B$ alalım.

i) A alt halka ise $(a_1 - a_2) \in A$ ve B alt halka ise $(b_1 - b_2) \in B$ olduğundan $x - y = (a_1 - a_2) + (b_1 - b_2) \in A + B$ dir.

ii) $xy = a_1a_2 + a_1b_2 + b_1a_2 + b_1b_2 \in A + B$ elde edilir. Şimdi bu toplamdaki terimlere teker teker bakalım:

$a_1a_2 \in A$, çünkü A alt halka

$a_1b_2 \in A$, çünkü A ideal ve $b_2 \in R$

$b_1a_2 \in B$, çünkü B ideal ve $a_2 \in R$

$b_1b_2 \in B$, çünkü B alt halka

O halde, A ve B alt halka olduklarından $(a_1a_2 + a_1b_2) \in A$ ve $(b_1a_2 + b_1b_2) \in A$ olup $xy \in A + B$ elde edilir.

Buna göre $A + B$ bir alt halkadır.

KAYNAKÇA

1. Prof. Dr. Fethi ÇALLIALP, Soyut Cebir, 2011, İstanbul.
2. Yrd. Doç. Dr. Hüseyin BİLGİÇ, Soyut Cebir Ders Notları, Kahramanmaraş Sütçü İmam Üniversitesi, 2012, Kahramanmaraş.
3. Prof. Dr. Şenol Eren, Soyut Cebir, Ondokuz Mayıs Üniversitesi Dijital Ders Platformu, 2021, Samsun.
4. Prof. Dr. Sait Halıcıoğlu, Doç. Dr. Burcu Üngör, Cebir, Açık ders, Ankara Üniversitesi, 2021, Ankara.
5. Doç. Dr. Sebahattin BALCI, Modern Cebire Giriş, Ankara Üniversitesi, Fen Fakültesi Döner Sermaye İşletmeleri Yayınları: 15, 1993, ANKARA.
6. Doç. Dr. Mustafa Bayraktar, Soyut Cebir ve Sayılar Teorisi, Atatürk Üniversitesi Basımevi, 1988, Erzurum.
7. Prof. Dr. H. İbrahim Karataş, Soyut Cebir, TÜBA, 2010, Ankara.