

# 1. Egyszerű gyűrűk

## Testek ideáljai

### 5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak:  $\{0\}$  és önmaga.

### Bizonyítás

Legyen  $T$  test és  $I$  ideálja  $T$ -nek, amely nem csak a nullából áll.

Ha  $0 \neq s \in I$ , akkor  $1 = ss^{-1} \in I$ , hiszen  $I$  ideál. Tehát minden  $r \in T$ -re  $r = 1r \in I$ . Ezért  $I = T$ .  $\square$

HF: Ferdetestnek minden balideálja és jobbideálja triviális.

### 5.3.1. Definíció

Az  $R$  egyszerű gyűrű, ha pontosan két ideálja van:  $0$  és  $R$ .

Főpélda (5.3.3): (Ferde)test fölötti teljes mátrixgyűrű egyszerű.

8.7.10, 8.7.12: A teljes mátrixgyűrű balideáljainak leírása.

## Kommutatív egyszerű gyűrűk

### Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

### Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$  miatt az  $(s)$  ideál nem  $(0)$ , és így  $(s) = R$ .

Ezért  $1 \in (s)$ , vagyis van olyan  $r \in R$ , hogy  $sr = 1$ .

Tehát az  $s$  elem invertálható, és így  $R$  test.  $\square$

### Általánosítás (5.3.8. Tétel, NB)

Legyen  $R$  gyűrű, amelynek csak a két triviális balideálja van.

Ekkor  $R$  vagy ferdetest, vagy olyan prímelemű gyűrű, amelyben bármely két elem szorzata nulla.

## Ideálok és nullosztók

### Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ , akkor  $r$  baloldali,  $s$  jobboldali nullosztó.

### 5.3.7. Lemma

Legyen  $r \in R$  rögzített. Ekkor  $\{x \in R : xr = 0\}$  balideál,

pontatlanul: az „ $r$ -hez tartozó” bal nullosztók balideált alkotnak.

### Bizonyítás

Ha  $xr = 0$  és  $yr = 0$ , akkor nyilván  $(x \pm y)r = 0$ .

Ha  $xr = 0$  és  $s \in R$ , akkor pedig  $(sx)r = s(xr) = s0 = 0$ .  $\square$

Elnevezés: Ez az  $r$  elem bal oldali *annullátora*. Fontos szerepet játszik a balideálmentes gyűrűk leírásában.

## 2. Faktorgyűrű

### Faktorcsoporthat

#### Állítás

Minden ideál alkalmas gyűrűhomomorfizmus magja.

#### Ismétlés

Legyen  $G$  kommutatív csoport a  $+$  műveletre. Ha  $N$  részcsoporthat  $G$ -ben, akkor tehát normálosztó is. A  $G/N$  faktorcsoporthat elemei az  $N$  szerinti mellékosztályok (ezek a  $g + N$  halmazok, ahol  $g$  befutja  $G$ -t).

Az összeadás:  $(g_1 + N) + (g_2 + N) = (g_1 + g_2) + N$ . A  $G/N$  csoport *egységeleme* az  $N = 0 + N$  mellékosztály, a  $g + N$  *inverze*  $(-g) + N$ . A  $\psi : g \mapsto (g + N)$  leképezés a *természetes homomorfizmus*  $G$ -ből  $G/N$ -re. Ennek *képe* az egész  $G/N$ , *magja*  $N$ .

### Faktorgyűrű

#### Állítás

Ha  $I$  ideál  $R$ -ben, akkor az  $R^+ / I^+$  faktorcsoporthat értelmezhető gyűrű-szorzás úgy, hogy a természetes homomorfizmus gyűrűhomomorfizmus legyen. Így az  $R/I$  faktorgyűrűt kapjuk.

#### Bizonyítás (lásd az 5.2. szakasz elején)

Legyen  $(r_1 + I)(r_2 + I) = r_1 r_2 + I$ . Be kell látni, hogy *jóldefiniált*.

Azaz ha  $r_1 + I = r'_1 + I$  és  $r_2 + I = r'_2 + I$ , akkor  $r_1 r_2 + I = r'_1 r'_2 + I$ .

$r_1 + I = r'_1 + I \implies r_1 - r'_1 \in I$  és  $r_2 + I = r'_2 + I \implies r_2 - r'_2 \in I$ .

De akkor  $r_1 r_2 - r'_1 r'_2 = r_1(r_2 - r'_2) + (r_1 - r'_1)r'_2 \in I$ , hiszen  $r_2 - r'_2 \in I$  és  $r_1 \in R$  miatt  $r_1(r_2 - r'_2) \in I$ , ugyanígy  $(r_1 - r'_1)r'_2 \in I$ .

HF: Igazak erre a szorzásra a gyűrűaxiómák (szorzás asszociativitása, mindkét oldali disztributivitás);

az  $r \mapsto r + I$  természetes homomorfizmus szorzattartó is. □

## Számolás a faktorgyűrűben

### Állítás

$\mathbb{Z}/(n) \cong \mathbb{Z}_n$ .

$$a + (n) = b + (n) \iff a - b \in (n) \iff n \mid a - b \iff a \equiv b \pmod{n}.$$

Vagyis két szám akkor van ugyanabban a mellékosztályban, ha  $n$ -nel osztva ugyanazt a maradékot adják.

Ezért az összes különböző mellékosztály:  $0 + (n), 1 + (n), \dots, n - 1 + (n)$ .

Állítás: A  $\psi : k \mapsto k + (n)$  bijekció izomorfizmus  $\mathbb{Z}_n \rightarrow \mathbb{Z}/(n)$ .

Szorzáttartás:  $k_1 *_n k_2$  a  $k_1 k_2$  maradéka modulo  $n$ .

Vagyis  $\psi(k_1 *_n k_2) = k_1 *_n k_2 + (n) = k_1 k_2 + (n)$ .

Másrészt  $\psi(k_1)\psi(k_2) = (k_1 + (n))(k_2 + (n)) = k_1 k_2 + (n)$ .

Azaz  $\psi(k_1 *_n k_2) = \psi(k_1)\psi(k_2)$ . Összegtartás hasonló, HF. □

$0, 1, \dots, n - 1$  egy reprezentánsrendszer az  $(n)$  ideál szerint.

## Példa polinomgyűrű faktorára

### 5.2.6. Állítás

„Számítsuk ki” az  $\mathbb{R}[x]/(x^2 + 1)$  faktorgyűrűt.  $I := (x^2 + 1)$ .

$$f + I = g + I \iff f - g \in I \iff x^2 + 1 \mid f - g.$$

Vagyis két polinom akkor van ugyanabban a mellékosztályban, ha  $x^2 + 1$ -gyel osztva ugyanazt a maradékot adják.

A lehetséges maradékok a legfeljebb elsőfokú polinomok. Így az összes különböző mellékosztály:  $(a + bx) + I$  ( $a, b \in \mathbb{R}$ ).

Példa: Mi lesz  $x + I$  négyzete?

$$(x + I)(x + I) = x^2 + I = -1 + ((x^2 + 1) + I) = -1 + I.$$

$$\text{HF: } ((a + bx) + I) + ((c + dx) + I) = ((a + c) + (b + d)x) + I.$$

$$\text{HF: } ((a + bx) + I)((c + dx) + I) = ((ac - bd) + (ad + bc)x) + I.$$

Azaz  $a + bi \mapsto (a + bx) + I$  izomorfizmus  $\mathbb{C} \rightarrow \mathbb{R}[x]/(x^2 + 1)$ .

## A homomorfizmustétel

### 5.2.5 Homomorfizmustétel

Ha  $\varphi : R \rightarrow S$  gyűrűhomomorfizmus, akkor  $\text{Im}(\varphi) \cong R/\text{Ker}(\varphi)$ .

Bizonyítás: Nyilván  $\text{Im}(\varphi)^+$  és  $R^+/\text{Ker}(\varphi)^+$  izomorf csoportok. Ellenőrizni kell, hogy ez a megfeleltetés szorzattartó is (HF).

### Két alkalmazás

- (1)  $R = \mathbb{Z}$ ,  $S = \mathbb{Z}_n$ ,  $\varphi(k) = k$  maradéka mod  $n$ .  
Itt  $\text{Im}(\varphi) = \mathbb{Z}_n$  és  $\text{Ker}(\varphi) = (n)$ , ezért  $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ .
- (2)  $R = \mathbb{R}[x]$ ,  $S = \mathbb{C}$ ,  $\varphi(f) = f(i)$  ( $\varphi$  az  $i$  behelyettesítése).  
Itt  $\text{Im}(\varphi) = \mathbb{C}$  és  $\text{Ker}(\varphi) = (x^2 + 1)$ , ezért  $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ .

Megjegyzés: Ez csak akkor működik, ha  $\mathbb{C}$  már ismert! Ha meg akarjuk konstruálni  $\mathbb{C}$ -t (vagy más testeket), akkor érdemes a faktorgyűrűt használni.

### 3. Test, mint faktorgyűrű

#### Négyelemű test

##### 5.2.10 Gyakorlat

A  $\mathbb{Z}_2[x]/(x^2 + x + 1)$  faktorgyűrű négyelemű test.

Az  $x^2 + x + 1$ -gyel való osztási maradék legfeljebb elsőfokú.

$I = (x^2 + x + 1)$ ,  $O = 0 + I$ ,  $E = 1 + I$ ,  $A = x + I$ ,  $B = (x + 1) + I$ .

+	O	E	A	B
O	O	E	A	B
E	E	O	B	A
A	A	B	O	E
B	B	A	E	O

*	O	E	A	B
O	O	O	O	O
E	O	E	A	B
A	O	A	B	E
B	O	B	E	A

Példa:  $AB = (x + I)(x + 1 + I) = (x^2 + x) + I = 1 + I = E$ ,

mert  $x^2 + x = 1 + (x^2 + x + 1)$  és  $x^2 + x + 1 \in I$

(azaz  $x^2 + x$ -nek az  $x^2 + x + 1$ -gyel való *osztási maradéka* 1).

*Test*, mert a táblázat szerint  $A^{-1} = B$ ,  $B^{-1} = A$ ,  $E^{-1} = E$ .

#### A faktorgyűrű mikor test

##### 5.2.9. Állítás

Ha  $T$  test és  $f \in T[x]$ , akkor a  $T[x]/(f)$  faktorgyűrű akkor és csak akkor *test*, ha  $f$  *irreducibilis*  $T$  fölött.

#### Elemi bizonyítás

Ha  $f = gh$  nemtriviális felbontás, akkor  $(g + (f))(h + (f))$  nulla, vagyis  $T[x]/(f)$  nem nullosztómentes, és így nem is test.

Ha  $f$  *irreducibilis*, akkor legyen  $g \in T[x]$ , ahol  $g + (f)$  nem nulla. Azaz  $f$  nem osztója  $g$ -nek, és mivel  $f$  irreducibilis,  $(f, g) = 1$ . Ezért  $fp + gq = 1$  alkalmas  $p, q \in T[x]$  polinomokra. Innen  $(g + (f))(q + (f)) = 1 - fp + (f) = 1 + (f)$ , hiszen  $f \mid fp$  miatt  $-fp + (f)$  nulla. Beláttuk tehát, hogy  $q + (f)$  inverze  $g + (f)$ -nek, hiszen  $1 + (f)$  a  $T[x]/(f)$  faktorgyűrű egységeleme.  $\square$

#### A faktorgyűrű mikor egyszerű

##### Második, elegáns (számlásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ . Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű, hiszen tudjuk, hogy minden ilyen kommutatív gyűrű test. Nyilván  $1 + (f)$  egységelem. Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ . Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím. Ezért vagy  $f \mid g$  vagy  $f \mid h$ . Az első esetben  $g + (f)$ , a másodikban  $h + (f)$  lesz a nullelem  $R$ -ben. Ha  $I \triangleleft R$ , akkor álljon  $J$  azokból a  $g \in T[x]$  polinomokból, melyekre  $g + (f) \in I$ . Ez ideál  $T[x]$ -ben, ezért főideál:  $J = (h)$ . Nyilván  $(f) \subseteq J$ , ezért  $h \mid f$ . Mivel  $(f)$  irreducibilis, vagy  $h$  egység, így  $I = R$ , vagy az  $f$ -nek egységszerese, és  $I$  az  $R$  nulla ideálja.  $\square$

( $J$  az  $I$  teljes inverz képe a természetes homomorfizmusnál.)

## Polinomok „nemlétező” gyökei

### Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy *testbővítését*. A bevezetés egy lehetséges módja a következő.

- (1) Tudjuk, hogy  $\mathbb{R}[x]/(x^2 + 1)$  izomorf  $\mathbb{C}$ -vel, és  $a + bi$ -nek az  $a + bx + (x^2 + 1)$  mellékosztály felel meg. Így az  $a + (x^2 + 1)$  alakú mellékosztályok  $\mathbb{R}$ -rel izomorf résztestet alkotnak, az  $i$ -nek megfelelő elem  $x + (x^2 + 1)$ .
- (2) *Definiáljuk*  $\mathbb{C}$ -t  $\mathbb{R}[x]/(x^2 + 1)$ -nek, és igazoljuk, hogy test.
- (3) *Azonosítsuk*  $a \in \mathbb{R}$ -et  $a + (x^2 + 1)$ -gyel, és mutassuk meg, hogy ezek az elemek  $\mathbb{R}$ -rel izomorf résztestet alkotnak.
- (4) *Definiáljuk*  $i$ -t  $x + (x^2 + 1)$ -nek, és lássuk be, hogy ez gyöke a  $z^2 + 1$  polinomnak.

## Testbővítés konstrukciója

### 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor *létezik* olyan  $L$  test, amelyben  $K$  résztest, és amelyben az  $s$  polinomnak már *van gyöke*.

### Bizonyítás

Legyen  $L = K[x]/(s)$ , ez test, mert  $s$  irreducibilis. A  $k \mapsto k + (s)$  megfeleltetés nyilván művelettartó és injektív. Ezért a  $k + (s)$  elemek ( $k \in K$ ) a  $K$ -val izomorf résztestet alkotnak  $L$ -ben. Végezzük el a  $k = k + (s)$  azonosítást (az azonosítás precíz részleteit lásd Kiss-jegyzet, 361. oldal). Legyen  $\alpha = x + (s) \in L$ . Be kell látni, hogy  $\alpha$  gyöke  $s$ -nek. Ezzel a bizonyítást be is fejezzük majd.

## Gyök a bővítésben

### Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek. Így  $\alpha = x + (s)$  miatt  $s(\alpha) = (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s)$ , vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme. Ezért  $\alpha$  tényleg gyöke az  $s$  polinomnak.  $\square$

A  $\mathbb{Z}_2[x]/(x^2 + x + 1)$  négyelemű testben  $E = 1 + (x^2 + x + 1)$ ,  $0 = (x^2 + x + 1)$ ,  $A = x + (x^2 + x + 1)$ ,  $B = x + 1 + (x^2 + x + 1)$ .

*Azonosítás:*  $O \leftrightarrow 0$ ,  $E \leftrightarrow 1$ ,  $z^2 + z + 1 \leftrightarrow Ez^2 + Ez + E$ . Az  $\alpha = A$  elem tényleg gyöke  $Ez^2 + Ez + E$ -nek.

## 4. Karakterisztika, prímtest

### Karakterisztika

#### Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

Ha  $n < 0$ , akkor  $nr$  a  $(-n)r$  ellentettje (ami  $(-n)(-r)$  is).

Ez  $R$  additív csoportjában a „hatványozás” (többszörös).

#### 5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy  $R$  nullosztómentes gyűrű. Ekkor vagy

- (1) van olyan  $p \in \mathbb{Z}$  prímszám, hogy  $pr = 0$  minden  $r \in R$ -re, ekkor  $R$  karakterisztikája  $p$ , vagy
- (2) tetszőleges  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$  esetén  $nr \neq 0$ , ekkor  $R$  karakterisztikája  $0$ .

Valójában  $R^+$  elemeinek *rendjeit* írjuk le.

### Karakterisztika: bizonyítás

#### Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ . Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ . Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ . Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ . Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik. Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek. Az  $r$  és  $s$  szerepét kicserélve  $s \neq 0$  esetén  $o(s) = o(r) = m$ .

Az (1)-hez már csak azt kell megmutatni, hogy  $m$  prímszám. Tegyük föl, hogy  $m = ab$ , ahol  $a, b$  pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel  $R$  nullosztómentes,  $ar = 0$  vagy  $br = 0$ . Az első esetben  $m = o(r) \mid a$ , vagyis  $a \mid m$  miatt  $a = m$ . A második esetben ugyanígy kapjuk, hogy  $b = m$ . Ezért  $m$  tényleg prímszám.  $\square$

### A Frobenius-endomorfizmus

#### 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím. Ekkor  $R$ -ben tagonként lehet  $p$ -edik hatványra emelni:

$$(r + s)^p = r^p + s^p \quad (r, s \in R).$$

Ezért a  $\psi(r) = r^p$  leképezés gyűrűhomomorfizmus  $R$ -ből  $R$ -be.

Neve: *Frobenius-endomorfizmus*. Ugyanez az állítás érvényes  $p$  hatványaira is.

*Endomorfizmus*: önmagába képző homomorfizmus.

$\psi$  szorzattartása nyilvánvaló, mert  $R$  kommutatív. Az összegtartás a *binomiális tételből* következik. Elemi számelmélet:  $\binom{p}{j}$  osztható  $p$ -vel, ha  $0 < j < p$ .

A  $p^k$ -ra emelés  $\psi^k$  ( $k$  tényezőös kompozíció).  $\square$

## Prímtest $p$ karakterisztikában

### 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem.

Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest, amely  $T$  minden résztestének része (*legsűkebb résztest*).

A legsűkebb résztest neve:  $P$  a  $T$  *prímteste*.

### Bizonyítás

Mivel  $e \neq 0$  de  $pe = 0$ , az  $e$  elem rendje  $p$ . Ezért  $P$  részcsoport és  $m \mapsto me$  izomorfizmus  $\mathbb{Z}_p^+$  és  $P^+$  között.

Ez tartja a szorzást is:  $(me)(ne) = (mn)e^2 = (mn)e$ .

Legsűkebb: Legyen  $K \leq T$  résztest. Ekkor  $K \neq \{0\}$ , és így  $K^\times$  részcsoportja  $T^\times$ -nek. Ezért  $T$  egységeleme,  $e \in K$ . Így  $P \subseteq K$ .  $\square$

## Prímtest $0$ karakterisztikában

### 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.

Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf résztest, amely  $T$  minden résztestének része (*prímtest*).

### Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen. Ellenőrizni kell, hogy  $\psi : m/n \mapsto (me)/(ne)$  jóldefiniált, és izomorfizmus  $\mathbb{Q}$  és  $P$  között.

Művelettartó: nyilván. Jóldefiniált:  $m/n = u/v \implies (me)/(ne) = (ue)(ve)$  **HF**.

Továbbá  $ne \neq 0$  ha  $n \neq 0$ , mert  $e$  rendje végtelen.

Szürjektív: nyilván. Injektív: elég, hogy  $\text{Ker}(\psi) = \{0\}$ . Ha  $(me)/(ne) = 0$  akkor  $me = 0$ , ezért  $m = 0$  mert  $o(e) = \infty$ .

Legsűkebb: mint a  $p$  karakterisztikájú esetben.  $\square$