Gyűrűk

2014. április 11.

1. Hányadostest

2. Karakterisztika, prímtest

3. Egyszerű gyűrűk

Tétel

Minden integritástartomány beágyazható testbe.

Biz.

Legyen R integritástartomány, és értelmezzünk az $R \times (R \setminus \{0\})$ halmazon két műveletet a következőképpen:

$$(a,b) + (c,d) = (ad + bc, bd)\,,$$
$$(a,b) \cdot (c,d) = (ac, bd)\,.$$

Mindkét művelet asszociatív és kommutatív (HF), viszont a szorzás sajnos nem disztributív az összeadásra:

$$\big((a,b) + (c,d)\big) \cdot (e,f) = (ade + bce, bdf)\,,$$
$$(a,b) \cdot (e,f) + (c,d) \cdot (e,f) = \big(adef + bcef, bdf^2\big)\,.$$

Vezessünk be egy $\sim$ relációt az $R \times (R \setminus \{0\})$ halmazon:

$$(a,b) \sim (c,d) \overset{\text{def}}{\iff} ad = bc.$$

Ez egy ekvivalenciareláció, ami kompatibilis a fenti műveletekkel, vagyis kongruenciája az $(R \times (R \setminus \{0\})\,; +, \cdot)$ algebrának (HF).

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el). Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem $\sim$ szerinti osztályát $\overline{(a, b)}$.

- additív egységelem: $\overline{(0, 1)}$
- $\overline{(a, b)}$ additív inverze: $\overline{(-a, b)}$

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(0, b^2)} = \overline{(0, 1)}$$

- multiplikatív egységelem: $\overline{(1, 1)}$
- $\overline{(a, b)} \neq \overline{(0, 1)}$ multiplikatív inverze: $\overline{(b, a)}$

$$\overline{(a, b)} \cdot \overline{(b, a)} = \overline{(ab, ba)} = \overline{(1, 1)}$$

Tehát T test.

Az $\overline{(a, 1)}$ alakú elemek egy R-rel izomorf részgyűrűt alkotnak T-ben, hiszen könnyű ellenőrizni (HF), hogy

$$\varphi \colon R \to T,\ a \mapsto \overline{(a, 1)}$$

injektív homomorfizmus (vagyis beágyazás). □

Megjegyzés

Mivel T tartalmaz R-rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T-nek (az $\overline{(a,1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R-beli elem hányadosaként:

$$\overline{(a,b)} = \overline{(a,1)} \cdot \overline{(1,b)} = \overline{(a,1)} \cdot \overline{(b,1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a legszűkebb test, ami tartalmazza R-et.

Példa

- $Q_{\mathbb{Z}} \cong \mathbb{Q}$, $Q_{\mathbb{Z}[i]} \cong \mathbb{Q}(i)$, $Q_{\mathbb{Z}[\sqrt{2}]} \cong \mathbb{Q}(\sqrt{2})$
- Ha K test, akkor $Q_K \cong K$, hiszen $\overline{(a,b)} = \overline{(ab^{-1},1)}$.
- Ha K test, akkor $Q_{K[x]} = K(x) = \left\{ \frac{f}{g} : f, g \in K[x], g \neq 0 \right\}$; ez a K feletti **racionális törtek** teste.
  (Nem keverendő a racionális törtfüggvényekkel, ahogy a polinomok se keverendők a polinomfüggvényekkel!)

Tétel

Izomorf integritástartományok hányadostestei is izomorfak.

Biz.

Legyen $\varphi\colon R \to S$ izomorfizmus; ekkor

$$\widehat{\varphi}\colon Q_R \to Q_S,\ \overline{(a,b)} \mapsto \overline{(a\varphi, b\varphi)}$$

izomorfizmus, amely kiterjesztése φ-nek (azaz $\widehat{\varphi}$ megszorítása az $R \leq Q_R$ részgyűrűre éppen φ). □

Tétel

Ha K olyan test, ami részgyűrűként tartalmazza az R integritástartományt, akkor K résztestként tartalmazza Q_R egy izomorf példányát.

Biz.

Definiáljuk az alábbi φ leképezést:

$$\varphi\colon Q_R \to K,\ \overline{(a,b)} \mapsto ab^{-1}.$$

Egyszerű számolás mutatja (HF), hogy ez a leképezés egy jóldefiniált injekció, ami felcserélhető az összeadással és a szorzással is, tehát beágyazás. □

Következmény

Legyen K minimális olyan test, ami részgyűrűként tartalmazza az R integritástartományt (azaz K-nak nincs olyan valódi részteste, ami tartalmazza R-et). Ekkor $K \cong Q_R$.

Biz.

Az előző tételt alkalmazva kapjuk, hogy K tartalmaz Q_R-rel izomorf résztestet. A minimalitás miatt ez a résztest csak maga K lehet. □

1. Hányadostest

2. Karakterisztika, prímtest

3. Egyszerű gyűrűk

[F] III/9

Definíció

Az R gyűrű **karakterisztikáján** a legkisebb olyan n pozitív egész számot értjük, amelyre

$$\forall a \in R: \quad na = \underbrace{a + \cdots + a}_{n} = 0.$$

Ha nincs ilyen n, akkor azt mondjuk, hogy R karakterisztikája ~~végtelen~~ nulla. Jelölés: $\operatorname{char} R$.

Megjegyzés

A karakterisztika (ha véges), nem más, mint a gyűrűelemek additív rendjeinek legkisebb közös felső korlátja.

Példa

- $\operatorname{char} \mathbb{C} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{Z} = 0$
- $\operatorname{char} \mathbb{Z}_n = n$
- $\operatorname{char} R[x] = \operatorname{char} R$
- $\operatorname{char} R^{n \times n} = \operatorname{char} R$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ $(1 < k, m < n)$.

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_{k} \cdot \underbrace{(e + \cdots + e)}_{m} = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

ami ellentmond a zérusosztómentességnek.

Tetszőleges $0 \neq a \in R$ és $\ell \in \mathbb{N}$ esetén

$$\begin{aligned} \ell a &= a + \cdots + a = e \cdot a + \cdots + e \cdot a = (e + \cdots + e) \cdot a \\ &= \ell e \cdot a = 0 \iff \ell e = 0, \end{aligned}$$

tehát $o_{(R;+)}(a) = n$. Ebből rögtön következik, hogy $\operatorname{char} R = n$. □

Definíció

Az olyan testet, amelynek nincs valódi részteste **prímtestnek** nevezzük.

Állítás

Bármely T testben a multiplikatív egységelem által generált résztest prímtest, amelyet T prímtestének nevezünk. Ez a T test legszűkebb részteste.

Biz.

Trivi. (HF) □

Tétel

Ha a T test karakterisztikája p, akkor prímteste izomorf $\mathbb{Z}_p$-vel.
Ha a T test karakterisztikája 0, akkor prímteste izomorf $\mathbb{Q}$-val.

Biz.

A $\varphi\colon \mathbb{Z} \to T$, $k \mapsto ke$ leképezés gyűrűhomomorfizmus
(itt $e \in T$ a multiplikatív egységelem):

$$k\varphi + \ell\varphi = ke + \ell e = (k+\ell)\,e = (k+\ell)\,\varphi;$$

$$k\varphi \cdot \ell\varphi = ke \cdot \ell e = (k\cdot\ell)\,e = (k\cdot\ell)\,\varphi.$$

Biz. (folyt.)

Alkalmazzuk a homomorfiatételt a $\varphi\colon \mathbb{Z} \to T$, $k \mapsto ke$ gyűrű-homomorfizmusra.

$$\begin{aligned} \ker\varphi &= \{k \in \mathbb{Z}\colon ke = 0\} = (\operatorname{char} T) \\ \mathbb{Z}\varphi &= \{\ldots, -2e, -e, 0, e, 2e, 3e, \ldots\} \leq_{\text{gy}} T \end{aligned}$$

- Ha $\operatorname{char} T = p$, akkor $\mathbb{Z}/\ker\varphi = \mathbb{Z}/(p) \cong \mathbb{Z}\varphi \leq_{\text{t}} T$.

  Ekkor T prímteste $\{0, e, 2e, \ldots, (p-1)e\} \cong \mathbb{Z}_p$.

- Ha $\operatorname{char} T = 0$, akkor $\mathbb{Z}/\ker\varphi = \mathbb{Z}/(0) \cong \mathbb{Z}\varphi \leq_{\text{gy}} T$.

  Nyilván $\mathbb{Z}/(0) \cong \mathbb{Z}$, tehát T tartalmazza részgyűrűként $\mathbb{Z}$ egy izomorf példányát, és így $\mathbb{Z}$ hányadosteste, vagyis $\mathbb{Q}$ egy izomorf példányát is.

  Ekkor T prímteste $\left\{\frac{ke}{me} : k, m \in \mathbb{Z}, m \neq 0\right\} \cong \mathbb{Q}$.

Tétel

Ha T véges test, akkor T elemszáma prímhatvány.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \operatorname{char} T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$,
akkor T izomorf a $\mathbb{Z}_p$ feletti elem n-esek vektorterével
(az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Következésképp $|T| = p^n$. □

Megjegyzés

Minden q prímhatványra létezik q elemszámú test, és ez a test izomorfia erejéig egyértelműen meghatározott. Jelölés: $\mathrm{GF}(q)$.

Például

- $\mathbb{Z}_p \cong \mathrm{GF}(p)$,
- $\mathbb{Z}_2[x] / \left(x^2 + x + 1\right) \cong \mathrm{GF}(4)$,
- $\mathbb{Z}_2[x] / \left(x^3 + x + 1\right) \cong \mathrm{GF}(8)$,
- $\mathbb{Z}_3[x] / \left(x^2 + 1\right) \cong \mathrm{GF}(9)$, stb.

1. Hányadostest

2. Karakterisztika, prímtest

3. Egyszerű gyűrűk

1. Hányadostest

2. Karakterisztika, prímtest

3. Egyszerű gyűrűk

[F] III/5,14

Állítás

(1) *Ha R kommutatív egységelemes gyűrű, akkor az $a \in R$ elem által generált főideál (azaz a legszűkebb ideál, ami tartalmazza a-t):*

$$(a) = aR = \{ar \colon r \in R\}.$$

(2) *Ha R nem egységelemes, akkor az aR halmaz nem biztos, hogy tartalmazza az a elemet (de $aR \lhd R$ továbbra is fennáll). Ilyenkor az a elem által generált főideál így fest:*

$$(a) = \{ka + ra \colon k \in \mathbb{Z}, r \in R\}.$$

Biz.

A táblán. □

Mostantól R kommutatív (de nem feltétlenül egységelemes) gyűrűt jelöl.

Definíció

Az $a \in R$ elem **annullátorán** az alábbi halmazt értjük:

$$\operatorname{Ann}(a) = \{r \in R : ra = 0\}.$$

Állítás

Minden $a \in R$ esetén $\operatorname{Ann}(a)$ *ideál R-ben.*

Biz.

HF □

Megjegyzés

Az $a \in R$ elem akkor és csak akkor zérusosztó, ha $\operatorname{Ann}(a) \neq \{0\}$.

Definíció

Az R gyűrűt **zérógyűrűnek** nevezzük, ha $\forall a, b \in R : ab = 0$.

Megjegyzés

Tetszőleges $(R; +)$ Abel-csoport zérőgyűrűvé tehető, ha a szorzást a fenti módon definiáljuk.
Ebben a gyűrűben minden additív részcsoport részgyűrű (sőt ideál) lesz.

Tétel

Bármely legalább kételemű kommutatív R gyűrű esetén az alábbiak ekvivalensek:

(1) *R egyszerű gyűrű.*

(2) *R test vagy prímrendű zérógyűrű.*

Biz.

A következő oldalon. □

Következmény

Bármely legalább kételemű egységelemes kommutatív R gyűrű esetén az alábbiak ekvivalensek:

(1) *R egyszerű gyűrű.*

(2) *R test.*

Tétel

Bármely legalább kételemű kommutatív R gyűrű esetén az alábbiak ekvivalensek:

(1) *R egyszerű gyűrű.*

(2) *R test vagy prímrendű zérógyűrű.*

Biz.

(2) $\Longrightarrow$ (1): Korábban láttuk, hogy a testek egyszerű gyűrűk.
Egy prímrendű zérógyűrűnek pedig a Lagrange-tétel szerint nincs nemtriviális additív részcsoportja.

(1) $\Longrightarrow$ (2): Ha R egyszerű, akkor

$$\forall a \in R \setminus \{0\}: \quad \operatorname{Ann}(a) = \{0\} \text{ vagy } \operatorname{Ann}(a) = R,$$

ezért (!)

$$\forall a \in R \setminus \{0\}: \ \operatorname{Ann}(a) = \{0\} \qquad \text{vagy} \qquad \forall a \in R \setminus \{0\}: \ \operatorname{Ann}(a) = R.$$

Biz. (folyt.)

Ha $\forall a \in R \setminus \{0\}: \ \operatorname{Ann}(a) = R$, akkor R zérógyűrű. Ekkor

$(R; +, \cdot)$ egyszerű gyűrű $\iff$ $(R; +)$ egyszerű csoport $\iff$ $|R|$ prímszám.

Ha $\forall a \in R \setminus \{0\}: \ \operatorname{Ann}(a) = \{0\}$, akkor R zérusosztómentes, tehát $R \setminus \{0\}$ zárt a szorzásra. Mivel R egyszerű, minden $a \in R$ esetén $aR = R$ (miért nem lehet $aR = \{0\}$?), azaz

$$\forall a \in R \setminus \{0\} \ \ \forall b \in R \ \exists x \in R: \ \ ax = b.$$

Ez azt jelenti, hogy az $(R \setminus \{0\}; \cdot)$ félcsoport művelete invertálható, tehát csoport. Következésképp R test. $\square$

Tétel

Ha T test, akkor a $T^{n\times n}$ mátrixgyűrű egyszerű.

Biz.

Jelölje $E_{pq} \in T^{n\times n}$ azt a mátrixot, amelyben a p-edik sor q-adik helyén 1 áll, az összes többi helyen pedig 0. Egyszerű számolással ellenőrizhetők az alábbiak tetszőleges $A = (a_{ij}) \in T^{n\times n}$ mátrixra:

- $E_{pq} \cdot A$ az a mátrix, amelynek p-edik sora megegyezik az A mátrix q-adik sorával, az összes többi eleme pedig 0;
- $A \cdot E_{st}$ az a mátrix, amelynek t-edik oszlopa megegyezik az A mátrix s-edik oszlopával, az összes többi eleme pedig 0;
- következésképpen $E_{pq} \cdot A \cdot E_{st} = a_{qs} \cdot E_{pt}$.

Biz. (folyt.)

Legyen most $\{0\} \neq I \triangleleft T^{n\times n}$, és legyen $0 \neq A \in I$. Az A mátrixnak van legalább egy nemnulla eleme, mondjuk $a_{qs} \neq 0$.
Ekkor minden $p, t \in \{1, \ldots, n\}$ esetén

$$a_{qs}^{-1} \cdot E_{pq} \cdot A \cdot E_{st} = a_{qs}^{-1} \cdot a_{qs} \cdot E_{pt} = E_{pt} \in I,$$

a szívó tulajdonság miatt. Tehát az E_{pt} mátrixok mind benne vannak I-ben. Ebből következik, hogy I minden mátrixot tartalmaz, hiszen bármely $B \in T^{n\times n}$ mátrixra

$$B = \sum_{p,t=1}^{n} b_{pt} \cdot E_{pt} \in I.$$

□