

1. 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” (együtthatója) r -nek, és így $m = o(r) \mid n$. Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$. 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.

ψ 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 ψ^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 $P = \{(me)/(ne) : m, 0 \neq n \in \mathbb{Z}\}$ \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

2. Véges testek

Véges test elemszáma.

6.7.2. Következmény

Minden véges test elemszáma *prímhatvány*.

Bizonyítás

Legyen T karakterisztikája p , prímteste P , és $|T : P| = n$. Ekkor T elemei egyértelműen írhatók $\lambda_1 b_1 + \dots + \lambda_n b_n$ alakban, ahol b_1, \dots, b_n bázis T -ben P fölött, és $\lambda_1, \dots, \lambda_n \in P$. Mindegyik λ_i skalár $|P| = p$ -féle lehet, így $|T| = p^n$. \square

Megjegyzés

A $\lambda_1 b_1 + \dots + \lambda_n b_n \mapsto (\lambda_1, \dots, \lambda_n)$ megfeleltetés nyilván *összegtartó*. Ezért T additív csoportja izomorf a $\mathbb{Z}_p^+ \times \dots \times \mathbb{Z}_p^+$ n -tényezős direkt szorzattal.

Véges test multiplikatív csoportja.

4.3.22. Tétel

Minden véges test multiplikatív csoportja *ciklikus*.

Bizonyításvázlat

Legyen T elemszáma $k + 1$, azaz $|T^\times| = |T - \{0\}| = k$. Az $x^d - 1$ polinomnak legfeljebb d gyöke van T -ben. Így ha $g \in T^\times$ rendje d , akkor e gyökök éppen g hatványai. Speciálisan minden d rendű elem g -nek hatványa! A $\langle g \rangle$ ciklikus részcsoporthoz $\varphi(d)$ darab d rendű elem van. Vagyis a d rendű elemek száma T^\times -ben $\varphi(d)$ vagy 0 . Ha $d \nmid k$, akkor nincs d rendű elem Lagrange tétele miatt. Az $x^k - 1 = \prod_{d|k} \Phi_d(x)$ -ben a fokokat véve $\sum_{d|k} \varphi(d) = k$. Ez csak úgy lehet, ha minden $d \mid k$ -ra van d rendű elem! Speciálisan van k rendű elem, azaz T^\times ciklikus. \square

Véges test konstrukciója.

6.7.5. Tétel

Minden $q = p^k$ prímszámra izomorfa erejéig pontosan egy darab q elemű test létezik. Jele \mathbb{F}_q . **Egyértelműség: NB.**

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste \mathbb{Z}_p fölött (létezik!). Jelölje L az $x^q - x$ gyökeinek halmazát K -ban. Ez résztest, mert $(a + b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K -ban, (hiszen K karakterisztikája p és $q = p^k$; **HF**). Az L elemszáma q , mert $x^q - x$ -nek nincs többszörös gyöke. Ha ugyanis lenne, akkor az gyöke lenne a deriváltjának is. De $x^q - x \in \mathbb{Z}_p[x]$ deriváltja $qx^{q-1} - 1 = -1$, hiszen $p \mid q$. A -1 konstans polinomnak pedig nincs gyöke K -ban. \square

Véges test résztestei.

6.7.8. Tétel

A $q = p^n$ elemű \mathbb{F}_q testnek minden $k \mid n$ esetén egyetlen \mathbb{F}_{p^k} -vel izomorf részteste van, más részteste pedig nincs. Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$, hiszen L karakterisztikája is p . A szorzástétel miatt $k = |L : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$ -nek. Lagrange tételét alkalmazzuk az L^\times csoportra. Azt kapjuk, hogy L nem nulla elemei gyökei $x^{p^k-1} - 1$ -nek. Így L elemei gyökei $x^{p^k} - x$ -nek; $|L| = p^k$ miatt több gyök nincs.

Megfordítva, $k \mid n$ esetén $p^k - 1 \mid p^n - 1 = |\mathbb{F}_q^\times|$. Mivel L^\times ciklikus, $x^{p^k-1} - 1$ -nek $p^k - 1$ gyöke van L -ben. Ezek a nullával együtt p^k elemű résztestet alkotnak. \square

Véges test, mint egyszerű bővítés.

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik \mathbb{Z}_p fölött irreducibilis n -edfokú f polinom. Minden ilyen f polinomnak \mathbb{F}_{p^n} a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^\times$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.

Ezért az irreducibilis m_α foka $|\mathbb{F}_{p^n} : \mathbb{Z}_p| = n$.

Legyen L az n -edfokú, irreducibilis $f \in \mathbb{Z}_p[x]$ felbontási teste. Ha $\beta \in L$ gyöke f -nek, akkor $|\mathbb{Z}_p(\beta) : \mathbb{Z}_p| = n$, így $|\mathbb{Z}_p(\beta)| = p^n$. Mivel csak egy p^n elemű résztest van, ez f felbontási teste. Az α közös gyöke f -nek és $x^{p^n} - x$ -nek, így $f(x) \mid x^{p^n} - x$. \square

A nyolcelemű test példája.

\mathbb{Z}_2 fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$. Ezek irreducibilisek \mathbb{Z}_2 fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az \mathbb{F}_8 elemei az $x^8 - x$ polinom összes gyökei. Az egyetlen valódi résztest a prímtest: $\{0, 1\}$. A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$. A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$. Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3 + x + 1)$, $O = 0 + (x^3 + x + 1)$ és $E = 1 + (x^3 + x + 1)$; ekkor $\{O, E\}$ a prímtest. $A = x + (x^3 + x + 1)$ gyöke $Ex^3 + Ex + E$ -nek. A másik két gyök $A^2 = x^2 + (x^3 + x + 1)$ és $A^4 = x^2 + x + (x^3 + x + 1)$. A maradék három elem $Ex^3 + Ex^2 + E$ -nek lesz gyöke, ezek $A + E, A^2 + E, A^2 + A + E$.