

Láng Csabáné

Testbővítés, véges testek

Készült a
programtervező matematikus szak esti tagozat III. év II. félév,
valamint az esti informatikus Bsc szak II. év II. félév számára

Lektorálta Burcsi Péter

A **feladatok** a

Testbővítés, véges testek; hibajavító kódok: Példák és megoldások
című példatárban található meg kidolgozva.

A példatár letölthető Láng Csabáné honlapjáról:

<http://compalg.inf.elte.hu/~zslang/>

valamint az IK Digitális könyvtárából.

Az **Emlékeztetők** olyan korábban tanult fogalmakat és tételeket jelölnek, amelyekre szükség van ennek az anyagnak a megértéséhez. Megtalálhatóak a következő jegyzetben.

Láng Csabáné: *Bevezető fejezetek a matematikába II.* ELTE, Bp. 1998.

Témavázlat

- Testbővítések, véges testek
 - Bevezetés
 - Testek bővítése
 - Algebrai bővítés
 - Prímtest
 - Minimálpolinom
 - Egyszerű algebrai bővítés
 - Felbontási test
 - Véges testek
 - Irodalomjegyzék

Jelölések:

N: a természetes számok halmaza, $\{1, 2, \dots\}$

Z: az egész számok halmaza, $\{\dots, -2, -1, 0, 1, 2, \dots\}$

Q: a racionális számok halmaza,
 $\{p/q, \text{ ahol } p \text{ és } q \text{ tetszőleges egész szám, } q \neq 0\}$

R: a valós számok halmaza,
a racionális számokon kívül pl. $\sqrt{2}$, π , e , ...

C: a komplex számok halmaza, $\{a+bi, \text{ ahol } a, b \text{ valósak}\}$

Z_m: a modulo m vett maradékosztályok gyűrűje a maradékosztály-
összeadással és a maradékosztály-szorzással

|K|: a K halmaz elemszáma, illetve számossága

[r]: maradékosztálygyűrűben az r elem által reprezentált
maradékosztály

K[x]: A K gyűrű fölötti polinomok gyűrűje, K -beli együtthatós
polinomok

L*: L test esetén az L halmaz a nullelem kivételével, $L^* = L \setminus \{0\}$

mlg: m osztója g -nek

Bevezetés

Emlékeztető

Definíció.

A (H, Ω) algebrai struktúra *félcsoport*, ha egyetlen kétváltozós műveletet tartalmaz, mely asszociatív.

Példa: $(\mathbb{N}, +)$

Definíció.

A (H, \cdot) félcsoport *csoport*, ha

1. létezik benne e egységelem, és
2. minden $a \in H$ elemnek létezik erre az egységelemre vonatkozó a^{-1} inverze : $a^{-1}a = aa^{-1} = e$.

Példa: $(\mathbb{Z}, +)$

Emlékeztető

Definíció.

Az $(R, +, \cdot)$ algebrai struktúra *gyűrű*, ha $+$ és \cdot R -en binér műveletek, valamint

I. $(R, +)$ Abel-csoport, (kommutatív csoport)

II. (R, \cdot) félcsoport, és

III. teljesül mindkét oldalról a disztributivitás, vagyis

$$a(b+c)=ab+ac,$$

$$(b+c)a=ba+ca$$

minden $a, b, c \in R$ esetén.

Példa: $(\mathbb{Z}, +, \cdot)$

Definíció.

R *integritási tartomány*, ha legalább két elemű nullosztómentes gyűrű

Példa: $(\mathbb{Z}, +, \cdot)$

Emlékeztető

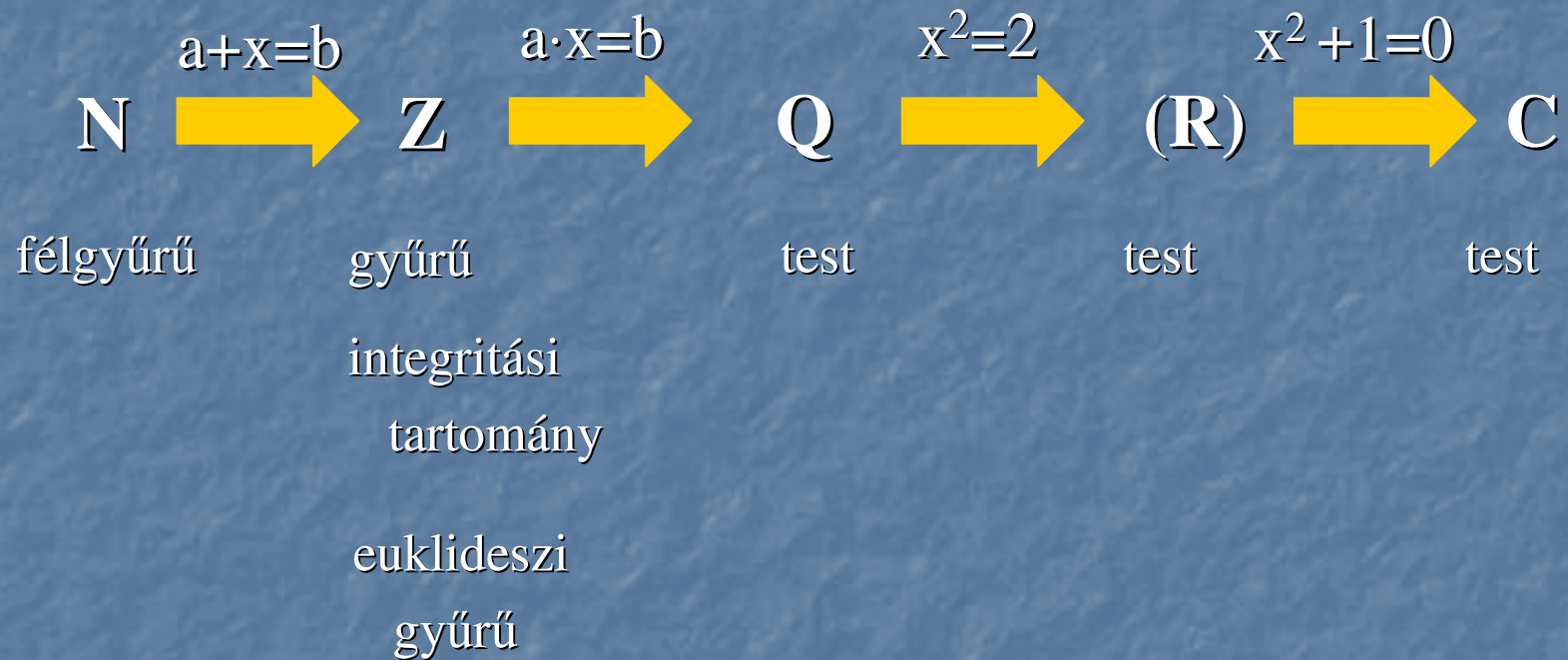
Definíció.

Az R gyűrű *test*, ha

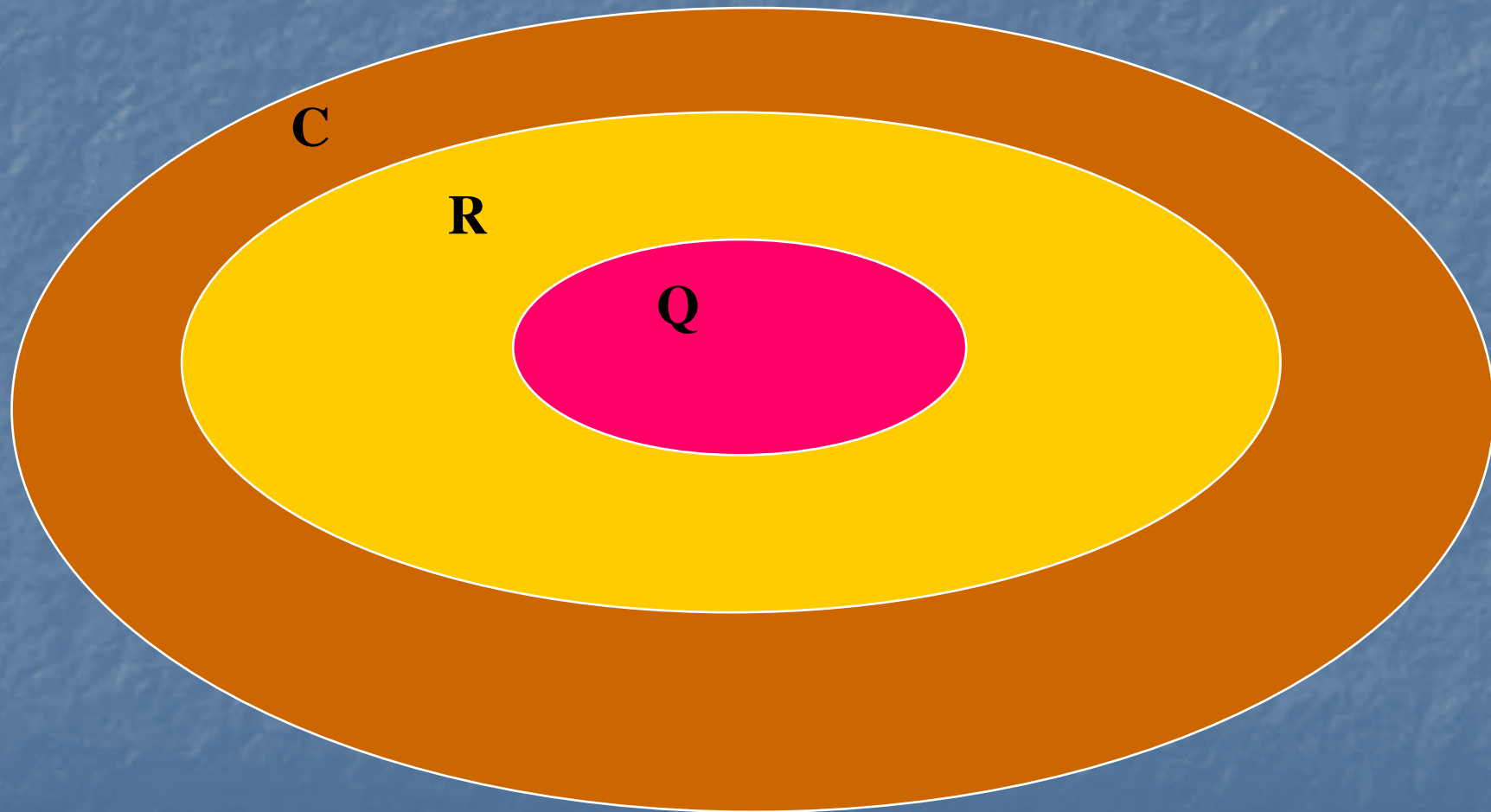
1. kommutatív, (a szorzás kommutatív)
2. (R^*, \cdot) csoport (R a nullelem kivételével).

Példa: $(\mathbf{Q}, +, \cdot)$, $(\mathbf{R}, +, \cdot)$, $(\mathbf{C}, +, \cdot)$

N-től C-ig



Számtestek



Eddig ismert véges testek

Tétel.

$m \in \mathbb{N}$ esetén \mathbb{Z}_m akkor és csak akkor test, ha m prím.



.....

Testek bővítése

Feladatok

- 2. Testet alkotnak-e a szokásos műveletekre a következő halmazok?

- a. $T_1 = \{a + b\sqrt[4]{2} \mid a, b \in \mathbf{Q}\}$

- b. $T_2 = \{a + bi\sqrt{5} \mid a, b \in \mathbf{Q}\}$

Definíció.

Ha a K test részteste az L testnek, akkor azt mondjuk, hogy L a K *bővítése*. $L|K$.

Példa: $\mathbb{R}|\mathbb{Q}$, $\mathbb{C}|\mathbb{Q}$, $\mathbb{C}|\mathbb{R}$.

Definíció.

Legyen $L|K$, és $H \subseteq L$. A K test H *halmazzal való bővítése* az L test legszűkebb olyan részteste, amely tartalmazza K -t és H -t. $K(H)$.

Ez a test létezik, és egyértelmű. Vegyük ugyanis L -nek az összes olyan résztestét, amely tartalmazza K -t és H -t. Ezeknek a résztesteknek a metszete test, és a feltételnek megfelel.

Definíció.

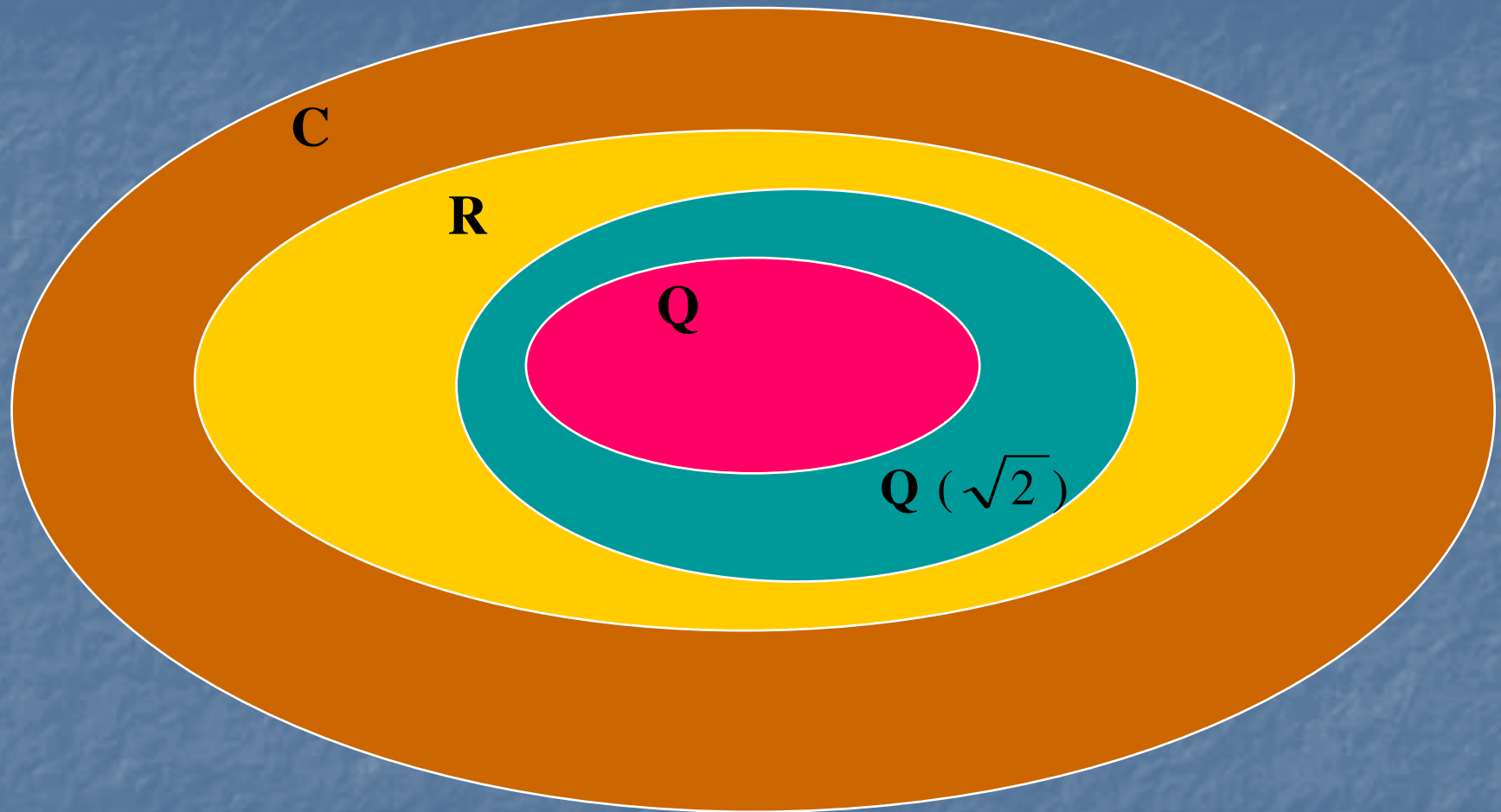
Egyszerű a bővítés, ha a bővítő halmaz egyetlen elemű.

Példa: $\mathbb{Q}(\sqrt{2})$, $\mathbb{R}(i)$ ($=\mathbb{C}$), ezek egyszerű bővítések.

- Ha $L|K$, $H1, H2 \subseteq L$, akkor

$$K(H1, H2) = K(H1)(H2) = K(H1 \cup H2)$$

Ha például $K(a, b, c, \dots)$ elkészítése a feladat, ezt elvégezhetjük lépésenként, a bővítő elemeket egyenként *adjungálva* az alaptesthez.



Feladatok

- 3. Mi a kapcsolat az alábbi testek között?

$$\mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(1+\sqrt{2}), \quad \mathbb{Q}(\sqrt{8}).$$

- 4. Mely a, b racionális számokra teljesül, hogy

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(a + b\sqrt{2})$$

- 5. Van-e olyan szám, amellyel bővítve a racionális számok testét, rögtön az alábbi testet kapjuk?

$$\mathbb{Q}(\sqrt{2} + \sqrt{3})$$

Definíció.

$V \neq \emptyset$ *vektortér a T test felett*, ha létezik V-n egy + binér művelet, melyre

- I. $(V, +)$ Abel-csoport
- II. T test és V halmaz között értelmezve van egy *skalárral* való szorzás: $\forall \lambda \in T, \underline{u} \in V \rightarrow \lambda \underline{u} \in V$
- IIa. $\forall \lambda, \mu \in T, \underline{v} \in V: (\lambda + \mu) \underline{v} = \lambda \underline{v} + \mu \underline{v}$
- IIb. $\forall \lambda \in T, \underline{u}, \underline{v} \in V: \lambda(\underline{u} + \underline{v}) = \lambda \underline{u} + \lambda \underline{v}$
- IIc. $\forall \lambda, \mu \in T, \underline{v} \in V: (\lambda \mu) \underline{v} = \lambda(\mu \underline{v})$
- IId. $\forall \underline{v} \in V: e \underline{v} = \underline{v}$ (e: T egységeleme)

V elemei *vektorok*, T elemei *skalárok*.

Tétel.

Legyen az L test a K test bővítése. Ekkor L vektortér K felett az L -beli műveletekkel.

Bizonyítás.

Legyen $u, u_1, u_2 \in L$ és $k, k_1, k_2 \in K$. ($k, k_1, k_2 \in L$ is fennáll.)

$(L, +)$ Abel-csoport, mert L test.

$k \cdot u \in L$, mert testben a szorzás művelet,

$(k_1 + k_2) \cdot u = k_1 \cdot u + k_2 \cdot u$, és

$k \cdot (u_1 + u_2) = k \cdot u_1 + k \cdot u_2$ a disztributivitás miatt

$(k_1 \cdot k_2) \cdot u = k_1 \cdot (k_2 \cdot u)$ a szorzás asszociativitása miatt,

$e \cdot u = u$, ahol e a K és L egységeleme.

$\Rightarrow L$ vektortér a K test fölött az L -beli műveletekkel.



Definíció.

V vektortér *dimenziója* egy bázisának az elemszáma.

Ha V -nek nincs véges generátorrendszere, akkor a dimenziója ∞ .

A 0 tér dimenziója 0 .

Jelölés: $\dim V$.

Definíció.

Legyen L és K test, $L|K$.

L -nek, mint K feletti vektortérnek a dimenziója a *bővítés foka*.

Jelölés: $[L:K]$.

Ha a bővítés foka véges, akkor a bővítés *véges bővítés*, különben *végtelen bővítés*.

Példa: $\mathbb{R}|\mathbb{Q}$ végtelen bővítés;

$\mathbb{C}|\mathbb{R}$ véges bővítés, mert $\{1, i\}$ bázist alkot \mathbb{C} -ben, mint \mathbb{R} feletti vektortérben.

Tétel.

Legyen az $L|K$, $[L:K]=n$, $|K|=q$. Ekkor $|L|=q^n$.

Bizonyítás.

Tudjuk, hogy L vektortér a K felett, s mivel a bővítés foka n , minden bázis n elemű.

Legyen $\{a_1, a_2, \dots, a_n\}$ egy bázis. Ekkor L minden u eleme előállítható a bázis elemeinek lineáris kombinációjaként, s az előállítás egyértelmű.

$$u = k_1 a_1 + k_2 a_2 + \dots + k_n a_n, \quad \text{ahol } k_i \in K$$

Mivel mindegyik k_i elem q különböző értéket vehet fel, s ezeket az értékeket egymástól függetlenül felvehetik, q^n különböző előállítás van, tehát q^n eleme van L -nek.



Tétel. (Testbővítések fokszám-tétele)

Legyen $M|L|K$, valamint $[M:L]$ és $[L:K]$ véges. Ekkor

$$[M:K] = [M:L] \cdot [L:K].$$

Megjegyzés.

Ha $[M:L]$ és $[L:K]$ közül valamelyik végtelen, akkor $[M:K]$ is az.

Bizonyítás.

Tegyük fel, hogy $[L:K]=n$, $[M:L]=k$, valamint az $L|K$ vektortér egyik bázisa $\{b_1, b_2, \dots, b_n\}$, az $M|L$ vektortér egyik bázisa $\{c_1, c_2, \dots, c_k\}$.

Belátjuk, hogy ekkor a két bázis szorzataként előálló

$$\{b_r c_s \mid 1 \leq r \leq n, 1 \leq s \leq k\}$$

halmaz bázis az $M|K$ vektortérben, ami igazolja állításunkat.

- Először belátjuk, hogy a $b_r c_s$ elemek lineárisan függetlenek.
Legyen

$$\alpha_{11} (b_1 c_1) + \dots + \alpha_{rs} (b_r c_s) + \dots + \alpha_{nk} (b_n c_k) = 0 \quad \alpha_{rs} \in K$$

Rendezzük az egyenlőséget c_s -ek szerint.

$$(\alpha_{11} b_1 + \dots + \alpha_{n1} b_n) c_1 + \dots + (\alpha_{1k} b_1 + \dots + \alpha_{nk} b_n) c_k = 0$$

A c_s elemek lineárisan függetlenek, így mindegyikük együtthatója 0.

$$\alpha_{1s} b_1 + \dots + \alpha_{ns} b_n = 0 \quad (s=1, \dots, k)$$

A b_r elemek L/K bázisát képezik, szintén lineárisan függetlenek, így mindegyik $\alpha_{rs} = 0$, tehát a $b_r c_s$ elemek lineárisan függetlenek.

- Most megmutatjuk, hogy a $b_r c_s$ elemek K fölött generálják az M testet. Legyen $u \in M$ tetszőleges. Ekkor M -ben

$$u = v_1 c_1 + \dots + v_k c_k \quad v_s \in L. \quad *$$

Az $L|K$ bővítésben minden v_s előállítható a b_1, b_2, \dots, b_n bázis segítségével.

$$v_s = \alpha_{1s} b_1 + \dots + \alpha_{rs} b_r + \dots + \alpha_{ns} b_n \quad \alpha_{rs} \in K$$

Ezeket az $*$ -ba helyettesítve:

$$u = \sum_s v_s c_s = \sum_s \left(\sum_r \alpha_{rs} b_r \right) c_s = \sum_{r,s} \alpha_{rs} (b_r c_s)$$



Feladatok

- 22. Bizonyítsuk be, hogy ha $\alpha \in \mathbb{C}$ megoldása a $10x^3 - 105x^2 + 84x + 210 = 0$ racionális együtthatós egyenletnek, és valamely K testre fennáll, hogy $\mathbb{Q}(\alpha) \mid K$ és $K \mid \mathbb{Q}$, akkor $K = \mathbb{Q}(\alpha)$ vagy $K = \mathbb{Q}$.

Algebrai bővítés

Emlékeztető

Definíció.

Az $\alpha \in \mathbb{C}$ számot *algebrai számnak* nevezzük, ha létezik olyan racionális együtthetős

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ nem azonosan zérus polinom, amelyiknek α gyöke.

Ha valamely α számhoz ilyen polinom nem található, akkor α *transzcendens szám*.

Példa:

Algebrai számok: a racionális számok, $\sqrt{2}$, i , ... (megszámlálható számosságúak)

Transzcendens számok: π , e , $2^{\sqrt{3}}$, ... (kontinuum számosságúak)

Definíció.

Legyen $L|K$. Az $\alpha \in L$ elemet *K felett algebrai elemnek* nevezzük, ha létezik olyan K -beli együtthatós $f(x)$ nem azonosan zérus polinom, amelyiknek α gyöke.

Ha valamely α elemhez ilyen polinom nem található, akkor α *K felett transzcendens*.

Példa: Az algebrai számok \mathbb{Q} felett algebraiak.

2 \mathbb{Q} fölött algebrai $x-2$

\mathbb{R} fölött algebrai $x-2$

\mathbb{C} fölött algebrai $x-2$

$\sqrt{2}$ \mathbb{Q} fölött algebrai x^2-2 ,

\mathbb{R} fölött algebrai x^2-2 ,

\mathbb{C} fölött algebrai x^2-2 ,

i \mathbb{Q} fölött algebrai x^2+1

\mathbb{R} fölött algebrai x^2+1

\mathbb{C} fölött algebrai x^2+1

- Valamely K test minden eleme algebrai K felett.
- Ha $L|K$, és L valamely eleme algebrai K fölött, akkor algebrai L fölött is.

Definíció.

Az $L|K$ bővítés *algebrai*, ha L minden eleme algebrai K fölött.
Egyébként a bővítés *transzcendens*.

Példa: $\mathbb{C}|\mathbb{R}$ algebrai bővítés, $\mathbb{R}|\mathbb{Q}$ transzcendens bővítés.

Tétel.

Véges bővítés algebrai.

Bizonyítás.

Legyen $L|K$, és $[L:K]=n$. Vegyük L -nek egy tetszőleges u elemét.

Az L -ben, mint K feletti vektortérben az u^0, u, u^2, \dots, u^n elemek lineárisan összefüggőek, mert legfeljebb n elem lehet lineárisan független. Van tehát olyan

$$\alpha_0 u^0 + \alpha_1 u + \alpha_2 u^2 + \dots + \alpha_n u^n = 0 \quad \alpha_s \in K$$

lineáris kombinációs előállítás, amelyikben nem mindegyik α_s együttható 0.

Tekintsük a

$$g = \alpha_0 x^0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_n x^n$$

polinomot. Ez K feletti nem zérus polinom, ugyanakkor u gyöke.

Tehát u algebrai K felett. Mivel ez L minden u elemére igaz, a bővítés algebrai.



Feladatok

- 25. A következő bővítések közül melyik véges és melyik algebrai? (A az algebrai számok halmazát jelöli.)
 - a. $\mathbb{C}|\mathbb{R}$
 - b. $\mathbb{Q}(\sqrt{5})|\mathbb{Q}$
 - c. $\mathbb{A}|\mathbb{Q}$
 - d. $\mathbb{A}|\mathbb{Q}(\sqrt{5})$
 - e. $\mathbb{R}|\mathbb{Q}(\pi)$

Prímtest

Emlékeztető

Tétel.

Ha az R gyűrű legalább két elemű, nullosztómentes, akkor $(R, +)$ -ban a 0-tól különböző elemek rendje megegyezik. Ez a közös rend vagy végtelen, vagy egy p prímszám.

Előző esetben a gyűrűt *nulla-karakterisztikájúnak* ($\text{char } R = 0$), az utóbbiban *p -karakterisztikájúnak* ($\text{char } R = p$) nevezzük.

Másként megfogalmazva p -karakterisztikájú gyűrűben $pr=0$ minden r elemre, míg nulla karakterisztikájú gyűrű esetén nincs olyan n természetes szám, amelyre $nr=0$ lenne, ha maga az r nem nulla.

Test nullosztómentes gyűrű, így minden testnek van karakterisztikája, ami 0, vagy p prímszám.

Példa: $\text{char}(\mathbb{Q})=0$, $\text{char}(\mathbb{Z}_5)=5$.

- Ha $L|K$, akkor L és K karakterisztikája nyilvánvalóan megegyezik.

Példa: $\text{char}(\mathbf{Q})=0$, $\text{char}(\mathbf{R})=0$, $\text{char}(\mathbf{C})=0$.

Definíció.

Valamely K test legszűkebb T résztestét a K *prímtestének* nevezzük. Ha valamely K testnek nincs valódi részteste, akkor K *prímtest*.

Valamely K test legszűkebb T részteste egyértelműen létezik, hiszen K összes résztestének a metszete.

Példa: \mathbb{R} prímteste \mathbb{Q} ; \mathbb{Q} prímteste önmaga; \mathbb{Z}_p prímteste önmaga (p tetszőleges prím); \mathbb{Q} és \mathbb{Z}_p prímtestek

Tétel.

0 karakterisztikájú prímtest izomorf \mathbb{Q} -val,
 p -karakterisztikájú prímtest izomorf \mathbb{Z}_p -vel.

Következmény.

Minden 0 karakterisztikájú test lényegében \mathbb{Q} bővítése,
minden p karakterisztikájú test lényegében \mathbb{Z}_p bővítése.

Feladatok

- 1. Van-e a valós számoknak olyan részteste, amelyet a valós számok minden részteste tartalmaz?

Minimálpolinom

Feladatok

- 6. Felbonthatatlan-e az x^5+5 polinom \mathbf{Z} , \mathbf{Q} , \mathbf{C} , \mathbf{Z}_2 , \mathbf{Z}_3 , illetve \mathbf{Z}_5 felett?
- 7. Keressük meg \mathbf{Z}_2 fölött az összes másod-, harmad-, és negyedfokú felbonthatatlan (irreducibilis) polinomot.
- 8. Igazoljuk, hogy az alábbi polinomok felbonthatatlanok (irreducibilisek) \mathbf{F}_2 (\mathbf{Z}_2) felett. ($[1]$ az 1 által reprezentált maradékosztályt jelöli.)
 - a. $x^5+x^2+[1]$
 - b. $x^6+x+[1]$
 - c. $x^7+x^3+[1]$
- 9. Hány másodfokú normált (1 főegyütthatójú) irreducibilis polinom van egy q elemű testben?

Definíció.

Legyen $L|K$ és $\alpha \in L$ algebrai K felett. Az m K fölötti polinom az α K fölötti *minimálpolinomja*, ha

1. m főpolinom,
2. $m(\alpha)=0$
3. m a legkisebb fokszámú polinom az 1. és 2. tulajdonságúak közül.

Tétel.

α K fölötti m minimálpolinomja

1. létezik és egyértelmű,
2. irreducibilis,
3. ha $g \in K[x]$ és $g(\alpha)=0$, akkor $m|g$.

Példa:

2 minimálpolinomja \mathbf{Q} fölött $x-2$

\mathbf{R} fölött $x-2$

\mathbf{C} fölött $x-2$

$\sqrt{2}$ minimálpolinomja \mathbf{Q} fölött x^2-2 ,

\mathbf{R} fölött $x-\sqrt{2}$,

\mathbf{C} fölött $x-\sqrt{2}$,

i minimálpolinomja \mathbf{Q} fölött x^2+1

\mathbf{R} fölött x^2+1

\mathbf{C} fölött $x-i$

Példa:

π minimálpolinomja \mathbb{Q} fölött **nem létezik**

\mathbb{R} fölött $x - \pi$

\mathbb{C} fölött $x - \pi$

Feladatok

- 17. Határozzuk meg $\sqrt{2-\sqrt[3]{2}}$ minimálpolinomját \mathbb{Q} felett.

- 27. Az alábbi bővítésekben határozzuk meg a bővítő elem minimálpolinomját \mathbb{Q} fölött.
 - a. $\mathbb{Q}(\sqrt{7})|\mathbb{Q}$

 - b. $\mathbb{Q}(i\sqrt{5})|\mathbb{Q}$

 - c. $\mathbb{Q}(1+i\sqrt{3})|\mathbb{Q}$

Egyszerű algebrai bővítés

Emlékeztető

Definíció.

Az R integritási tartomány *euklidészi gyűrű*, ha létezik olyan φ függvény, amelyre $\varphi : R^* \rightarrow \mathbf{N}_0$, és I. $a, b \in R, b \neq 0$ esetén létezik olyan $c, d \in R$, hogy

$$a = bc + d, \text{ ahol}$$

i. $d = 0$ vagy

ii. $d \neq 0$ és $\varphi(d) < \varphi(b)$,

II. $\varphi(ab) \geq \max(\varphi(a), \varphi(b))$, ha $a, b \in R^*$.

Tétel.

Euklidészi gyűrűben elvégezhető az euklidészi algoritmus.

Ezzel az algoritmussal megkapjuk (a, b) -t, a és b legnagyobb közös osztóját. Léteznek olyan $x, y \in R$ elemek, hogy $(a, b) = ax + by$. (*Lineáris kombinációs előállítás.*)

Emlékeztető

Tétel.

Legyen R test, és $f \in R[x]^*$ esetén $\varphi: R[x]^* \rightarrow \mathbf{N}_0$, $\varphi(f) = \deg f$.

Ekkor $R[x]$ φ -vel euklidészi gyűrűt alkot.

(A test fölötti polinomgyűrűk euklidészi gyűrűt alkotnak a polinom fokszám függvényével.)

Tétel.

Legyen R egységelemes integritási tartomány,

$f \in R[x]^*$, és $\deg f = n \geq 0$.

Ekkor f -nek legfeljebb n különböző gyöke van R -ben.

Megjegyzés.

Az előbbi állítás **nem igaz** ha nullosztókat is tartalmaz a polinomgyűrű, vagy pedig nem kommutatív.

Emlékeztető

Definíció.

Legyen R gyűrű, $I \subseteq R$, $I \neq \emptyset$. I az R *balideálja*, ha

1. $I-I \subseteq I$, és
2. $R \cdot I \subseteq I$.

A *jobbideál* definíciója hasonló. I *ideál*, ha jobb és bal oldali ideál egyszerre.

Triviális ideál: $\{0\}$, R .

Valódi ideál: R -től különböző ideál.

Tétel

Ha R kommutatív gyűrű, akkor az

$I = (a) = \{x \cdot a \mid x \in R\}$ halmaz R -nek ideálja.

Emlékeztető

Definíció.

Legyen R gyűrű, I kétoldali ideál R -ben. R -nek I szerinti

maradékosztály gyűrűje (faktorgyűrűje)

$R/I = \{r + I \mid r \in R\}$ a következő műveletekkel:

1. $(r+I)+(s+I)=(r+s)+I$

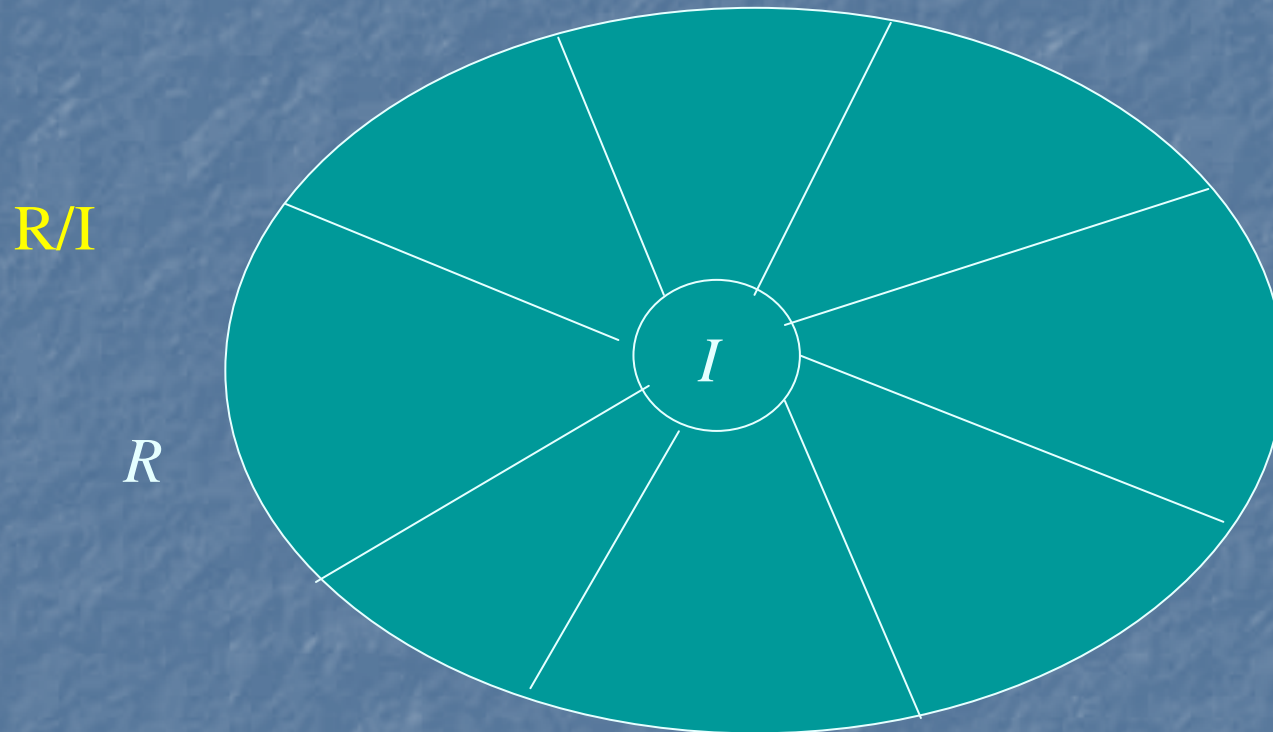
2. $(r+I)\cdot(s+I)=(r \cdot s)+I$

R/I gyűrűt alkot a definícióban szereplő műveletekre nézve.

I a nullelem. Ha R egységelemes, akkor $I+e$ az R/I -ben az egységelem.

Egy maradékosztály bármely elemével reprezentálható. Az r elem által reprezentált maradékosztályt, tehát $(r+I)$ -t $[r]$ fogja jelölni.

Faktorgyűrű



Tétel.

Legyen $f \in K[x]$ irreducibilis polinom, (f) az $f \in K[x]$ -beli többszöröseiből álló ideál. Ekkor a $K[x]/(f)$ maradékosztálygyűrű test.

Bizonyítás.

Tudjuk, hogy $K[x]/(f)$ gyűrű, van egységeleme, kommutatív.

Csupán azt kell belátnunk, hogy minden nem 0 elemének van inverze.

Legyen $g \in K[x]$ tetszőleges olyan polinom, amelyik nincs az ideálban.

$(f, g) = 1$, egyrészt mert f irreducibilis, másrészt mert g nem többszöröse f -nek. Állítsuk elő 1-et f és g lineáris kombinációjaként:

$$1 = f \cdot u + g \cdot v, \quad u, v \in K[x]$$

Vegyük a faktorgyűrűben azokat az osztályokat, melyeknek a fenti polinomok reprezentánsai.

$$[1] = [f \cdot u + g \cdot v] = [f \cdot u] + [g \cdot v] = [f] \cdot [u] + [g] \cdot [v]$$

Mivel a faktorgyűrűben $[f] = 0$, ezért

$$[1] = [g] \cdot [v]$$

Ebből láthatjuk, hogy a $[g]$ osztálynak van inverze, mégpedig $[v]$.

Ebből pedig következik, hogy $K[x]/(f)$ testet alkot.



Tétel.

Legyen $f \in K[x]$ irreducibilis polinom. Ekkor létezik K -nak olyan bővítése, amelyikben f -nek van gyöke.

Bizonyítás.

Ha f elsőfokú, akkor ez a bővítés maga a K . Egyébként tekintsük a $K[x] / (f)$ testet.

- Ez a test egyrészt K bővítésének tekinthető, mert K izomorf $K[x] / (f)$ egy részstruktúrájával, nevezetesen a 0-adfokú polinomokból álló résztesttel.
- Másrészt $K[x] / (f)$ -ben van gyöke f -nek.

$$\text{Legyen } f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Tekintsük azt az osztályt, amelyet az x polinom reprezentál: $[x]$. Helyettesítsük be f -be.

$$\begin{aligned} f([x]) &= a_n [x]^n + a_{n-1} [x]^{n-1} + \dots + a_1 [x] + a_0 = \\ &= [a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0] = (f) = 0 \end{aligned}$$

f -nek van tehát gyöke $K[x] / (f)$ -ben, mégpedig $[x]$, az x polinom által reprezentált maradékosztály.



Következmény.

A legfeljebb $(n-1)$ -edfokú polinomok reprezentáns rendszert alkotnak $K[x] / (f)$ -ben

Tétel.

Legyen $f \in K[x]$ n -edfokú irreducibilis polinom, α gyöke. Ekkor
 $K[x] / (f) \cong K(\alpha)$ és
 $\{\alpha^0, \alpha, \dots, \alpha^{n-1}\}$ bázis $K(\alpha)$ -ban.

Feladatok

- 10. Készítsünk 9 elemű testet.
 - a. Adjuk meg a műveletábrákat.
 - b. Határozzuk meg az egyes elemek multiplikatív rendjét, keressünk primitív elemeket.
 - c. Határozzuk meg az egyes elemek additív rendjét.

- 12.
 - a. Bizonyítsuk be, hogy az $f(x)=x^3+x+[1] \in \mathbf{Z}_5[x]$ polinom irreducibilis \mathbf{Z}_5 felett. ($[1]$ az 1 által reprezentált maradékosztályt jelöli.)
 - b. Hány eleme van a $\mathbf{Z}_5[x]/(f)$ maradékosztálygyűrűnek (testnek), ahol (f) az f többszöröseiből álló ideál? Adjunk meg egy reprezentánsrendszert.

Feladatok

- 13.
 - a. Bizonyítsuk be, hogy az $f(x)=x^2+x+[1] \in \mathbf{Z}_5[x]$ polinom irreducibilis \mathbf{Z}_5 felett. ([1] az 1 által reprezentált maradékosztályt jelöli.)
 - b. Hány eleme van a $\mathbf{Z}_5[x]/(f)$ maradékosztálygyűrűnek (testnek), ahol (f) az f többszöröseiből álló ideál? Adjunk meg egy reprezentánsrendszert.
- 14.
 - a. Bizonyítsuk be, hogy az $f(x)=x^3+x+[2]$ reducibilis \mathbf{Z}_7 felett. ([2] a 2 által reprezentált maradékosztályt jelöli.)
 - b. Hány eleme van a $\mathbf{Z}_7[x]/(f)$ maradékosztálygyűrűnek, ahol (f) az f többszöröseiből álló ideál? Adjunk meg egy reprezentánsrendszert.
 - c. Mutassuk meg, hogy a $\mathbf{Z}_7[x]/(f)$ maradékosztálygyűrű tartalmaz nullosztót.

Feladatok

- 15. Legyen $u \in \mathbb{C}$ a \mathbb{Q} feletti $x^3 - 2x + 2$ polinom egyik gyöke. Lássuk be, hogy a polinom \mathbb{Q} felett irreducibilis. Írjuk fel $\mathbb{Q}(u) | \mathbb{Q}$ $\{1, u, u^2\}$ bázisában a következő elemeket:
 - a. u^7
 - b. u^{-1}
 - c. $u^4 + u^{-2}$

- 16. Legyen $u \in \mathbb{C}$ az $x^3 - 6x^2 + 9x + 3$ \mathbb{Q} felett irreducibilis polinom gyöke. Fejezzük ki $\mathbb{Q}(u) | \mathbb{Q}$ $\{1, u, u^2\}$ bázisában a következő elemeket:
 - a. $3u^5 - 2u$
 - b. $\frac{1}{1+u}$

Feladatok

- 27. Határozzuk meg a $T|Q$ testbővítés fokát, ahol T az alábbi. Mi a bővítő elem minimálpolinomja Q fölött? Adjunk meg egy bázist.
 - a. $Q(\sqrt{7})$
 - b. $Q(i\sqrt{5})$
 - c. $Q(1+i\sqrt{3})$

Felbontási test

Definíció.

Legyen $f \in K[x]$ n -edfokú polinom. f *K feletti felbontási teste* a K test legszűkebb olyan bővítése, amelyben f elsőfokú tényezők szorzatára bomlik.

Tétel.

Legyen $f \in K[x]$ n -edfokú polinom. Ekkor létezik f K feletti felbontási teste.

Bizonyítás.

f -et bontsuk irreducibilis polinomok szorzatára. Ha ezek között van legalább másodfokú, akkor bővítenünk kell.

Tudjuk, hogy irreducibilis polinom esetén van K -nak olyan bővítése, amelyben a polinomnak van gyöke.

Ennek a tételnek az alkalmazásával teljes indukcióval bizonyíthatunk.



Példa.

Az $x - 2$ polinom felbontási teste \mathbf{Q} fölött \mathbf{Q} .

Az $x - 2$ polinom felbontási teste \mathbf{R} fölött \mathbf{R} .

Az $x - \pi$ polinom felbontási teste \mathbf{R} fölött \mathbf{R} .

Az $x^2 + 1$ polinom felbontási teste \mathbf{Q} fölött $\mathbf{Q}(i)$.

Az $x^2 + 1$ polinom felbontási teste \mathbf{R} fölött \mathbf{C} .

Feladatok

- 19. Határozzuk meg az $(x^2+1)(x^2-2x+1)$ polinom felbontási testét \mathbb{Q} felett.
- 20. $\mathbb{Q}(\sqrt[3]{2})$ megegyezik-e $\sqrt[3]{2}$ minimálpolinomjának a felbontási testével?
- 21. Van-e racionális gyöke az $f(x)=x^3-x^2-x-2$ polinomnak? Mi az $f(x)$ felbontási teste \mathbb{Q} felett?

Véges testek

Tétel.

Tetszőleges p prím és n természetes szám esetén létezik p^n elemű véges test.

Bizonyítás.

Legyen $K = \mathbb{Z}_p$, és vegyünk az $f = x^{p^n} - x$ felbontási testét K felett.

Ebben a testben benne van a polinom mindegyik gyöke.

Vizsgáljuk meg, hogy van-e az f polinomnak többszörös gyöke.

$$f' = p^n x^{p^n - 1} - 1$$

Mivel a test karakterisztikája p (vagyis $pr = 0$ minden r elem esetén), így $p^n r = 0$ is teljesül, tehát $f' = -1$. Mivel f' -nek nincs gyöke, f -nek nincs többszörös gyöke. f gyökeinek a száma p^n .

Megmutatjuk, hogy a gyökök L halmaza testet alkot.

Ehhez csak azt kell belátnunk, hogy az M felbontási testben L résztest, vagyis

$$1. L-L \subseteq L \quad 2. L \cdot (L^*)^{-1} \subseteq L$$

1. Legyen $u, v \in L$, tehát $u^{p^n} - u = 0$ és $v^{p^n} - v = 0$

Amiből $u^{p^n} = u$ és $v^{p^n} = v$ *

Vegyük $u-v$ -t. $(u-v)^{p^n} = u^{p^n} - v^{p^n}$

mert a hatvány kifejtésénél a p karakterisztika miatt a többi együttható 0. Ez utóbbi azonban * miatt éppen

$u-v$, ami azt jelenti, hogy $(u-v)^{p^n} - (u-v) = 0$

tehát $u-v$ is gyöke L -nek. Beláttuk, hogy $L-L \subseteq L$.

Hasonlóan látható be, hogy $L \cdot (L^*)^{-1} \subseteq L$, s így L testet alkot. Ezek szerint az M felbontási test maga az L .

Megkaptuk az ígért p^n elemű testet.



Megjegyzés.

Belátható, hogy minden p^n elemű test izomorf egymással.

Láttuk korábban, hogy minden véges test \mathbb{Z}_p bővítésének tekinthető valamilyen p prím esetén, így p^n elemű, ahol n alkalmas természetes szám. Most láttuk, hogy tetszőleges p prím és n természetes szám esetén létezik p^n elemű véges test.

Ezzel teljesen felderítettük a véges testeket.

Tétel.

Véges test multiplikatív csoportja ciklikus.

A generáló elemet a test *primitív elemének* nevezzük. A multiplikatív csoportnak több generáló eleme is van általában.

Feladatok

Véges test elemeinek összege, szorzata

29. Bizonyítsuk be a Wilson-tételt: $(p-1)! \equiv -1 \pmod{p}$, ha p prím.

Megoldás.

\mathbb{Z}_p elemeivel dolgozunk. Minden $[a]$ maradékosztályhoz párosítjuk azt a $[b]$ maradékosztályt, amellyel szorozva $[1]$ -et ad. Mivel \mathbb{Z}_p test, minden $[a] \neq [0]$ -hoz van ilyen $[b]$. Ha $[a]$ párja $[b]$, akkor nyilván $[b]$ párja $[a]$.

E párosítás során csak az $[1]$ és $[-1]$ osztály lesz önmaga párja. Ha ugyanis $[u]$ párja önmaga, akkor

$$u^2 \equiv 1 \pmod{p} \rightarrow 0 \equiv u^2 - 1 \equiv (u-1)(u+1) \pmod{p}$$

$$p \text{ prím} \rightarrow pu-1 \text{ vagy } pu+1 \rightarrow u \equiv 1 \pmod{p} \text{ vagy } u \equiv -1 \pmod{p}$$

Szorozzuk össze tehát mindegyik osztályt a párjával, ha az különbözik tőle. Ezeket az értékeket egymással is összeszorozva $[1]$ -et kapunk, amit még meg kell szoroznunk a kimaradt osztályokkal, az $[1]$ -gyel, és – ha ettől különbözik – akkor a $[-1]$ -gyel is.

Ha $[1] \neq [-1]$ akkor $(p-1)! \equiv 1(-1) = -1 \pmod{p}$

$p=2$ esetén $[1] = [-1]$, s így $(p-1)! \equiv 1 \equiv -1 \pmod{p}$ szintén teljesül.



30. Mennyi valamely véges test nem nulla elemeinek a szorzata?

Megoldás. Tetszőleges véges testben is megtehetjük, hogy mindegyik elemet megszorozzuk az inverzével, s a szorzatok értéke 1-et ad (most 1 az adott véges test egységeleme).

Meg kell vizsgálnunk, hogy van-e olyan elem, amelyik önmaga inverze.

Ha u inverze önmaga, akkor $u = \frac{1}{u}$

vagyis $0 = u^2 - 1 = (u-1)(u+1)$

Mivel testben nincs nullosztó, ebből $u-1=0$, vagy $u+1=0$,
amiből $u=1$, vagy $u=-1$.

Szorozzuk össze mindegyik elemet az inverzével, ha az különbözik tőle. Ha ezeket az értékeket egymással is összeszorozzuk, 1-et kapunk, amit még meg kell szoroznunk a kimaradt -1 -gyel, s így az eredmény -1 lesz.

Ha a véges testben $1 \neq -1$, akkor az eddigi eredményt még 1 -gyel is szoroznunk kell – ami természetesen nem változtat a szorzat értékén.

Így tetszőleges véges test nem nulla elemeinek a szorzata -1 -et ad.



31. Véges testben mi az elemek számának paritása?

Megoldás.

Az előző példa magyarázatából kiderül, hogy

- ha $1 = -1$, akkor az elemszám páros, mert a párosításból csak az 1 és a 0 marad ki,
- ha $1 \neq -1$, akkor páratlan az elemszám, mert a párosításból az 1, -1 és a 0 marad ki.



Vieta formulák, gyökök és együtthatók közötti összefüggések

Legyen R egységelemes integritási tartomány, és tegyük fel, hogy az $f(x)$ n -edfokú polinom – multiplicitással együtt vett – n gyöke mind R -ben van. Legyenek ezek a gyökök:

$$c_1, c_2, \dots, c_n$$

$$\begin{aligned}
f(x) &= a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = \\
&= a_n (x - c_1) \cdot (x - c_2) \cdot \dots \cdot (x - c_n) = \\
&= a_n (x^n - (c_1 + c_2 + \dots + c_n) x^{n-1} + \\
&\quad + (c_1 \cdot c_2 + c_1 \cdot c_3 + \dots + c_{n-1} \cdot c_n) x^{n-2} + \\
&\quad \dots + (-1)^n (c_1 \cdot c_2 \cdot \dots \cdot c_n))
\end{aligned}$$

Ebből

$$\begin{aligned}
\frac{a_{n-1}}{a_n} &= -(c_1 + c_2 + \dots + c_n) \\
\frac{a_{n-2}}{a_n} &= (c_1 \cdot c_2 + c_1 \cdot c_3 + \dots + c_{n-1} \cdot c_n) \\
&\dots \\
\frac{a_0}{a_n} &= (-1)^n (c_1 \cdot c_2 \cdot \dots \cdot c_n)
\end{aligned}$$

32. Legyen L egy véges test, $|L|=q^k$. Számítsuk ki a következő összeget: $\sum_{l \in L} l$.

Megoldás. Legyen

$$g(x) = x^{q^k} - x$$

Ennek a polinomnak a gyökei éppen az L test elemei.
A Vieta-formulát alkalmazzuk.

$$\frac{a_{n-1}}{a_n} = -(c_1 + c_2 + \dots + c_n)$$

Ha $n = q^k \geq 3$, akkor $a_{n-1} = 0$, a fenti érték is nulla, s így a test elemeinek összege nulla.

Ha $n = q^k = 2$, akkor a test elemeinek összege 1, mert a testnek egyik eleme a 0, másik eleme az 1.



33. Legyen L véges test, $|L|=q^k$. Jelölje L^* az L multiplikatív csoportját. Számítsuk ki a következő szorzatot: $\prod_{l \in L^*} l$.

Megoldás.

Az alábbi $k(x)$ polinom gyökei az L test nemnulla elemei.

$$k(x) = x^{q^k - 1} - 1$$

A Vieta formulát alkalmazzuk

$$\frac{a_0}{a_n} = (-1)^n (c_1 \cdot c_2 \cdot \dots \cdot c_n)$$

Most $a_0 = -1$, $a_1 = 1$.

- Ha $n = q^k - 1$ páros, akkor a nem nulla elemek szorzata -1 .
- Ha $n = q^k - 1$ páratlan, akkor a nem nulla elemek szorzata 1 . Ekkor azonban a test karakterisztikája 2 , így $1+1=0$, vagyis $1=-1$. Ekkor is mondhatjuk, hogy a nem nulla elemek szorzata -1 .



Irodalomjegyzék

- G. Birkhoff-T. C. Barte: *A modern algebra a számítógéptudományban* Műszaki Könyvkiadó, 1974
- Freud Róbert: *Lineáris algebra* ELTE Eötvös Kiadó, Budapest, 1996
- Fuchs László: *Algebra* Tankönyvkiadó, Bp, 1991
- Gonda János: *Bevezető fejezetek a matematikába III.* ELTE TTK, Bp. 1998
- Járai Antal: *Bevezetés a matematikába* Eötvös Kiadó, Budapest, 2005
- Láng Csabáné: *Bevezető fejezetek a matematikába II.* ELTE, Bp. 1998
- Környei Imre: *Algebra* Tankönyvkiadó, Bp, 1965
- F. Reinhardt-H. Soeder: *SH atlasz Matematika* Springer, 1993
- Schmidt Tamás: *Algebra* Tankönyvkiadó, Bp, 1980
- Surányi László: *Algebra, testek, gyűrűk, polinomok* Typotex Bp. 1997