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 találhatók 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, …}

Z: az egész számok halmaza, {…,-2, -1, 0, 1, 2, …}

Q: a racionális számok halmaza,
{p/q, ahol p és q tetszőleges egész szám, q≠0}

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

C: a komplex számok halmaza, {a+bi, ahol a,b 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 maradékosztáy

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

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

m|g: m osztója g-nek

Bevezetés

Emlékeztető

Definíció.

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

Példa: (**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: (**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: $(\mathbf{Z},+,\cdot)$

Definíció.

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

Példa: $(\mathbf{Z},+,\cdot)$

Emlékeztető

Definíció.

Az R gyűrű *test*, ha

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

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

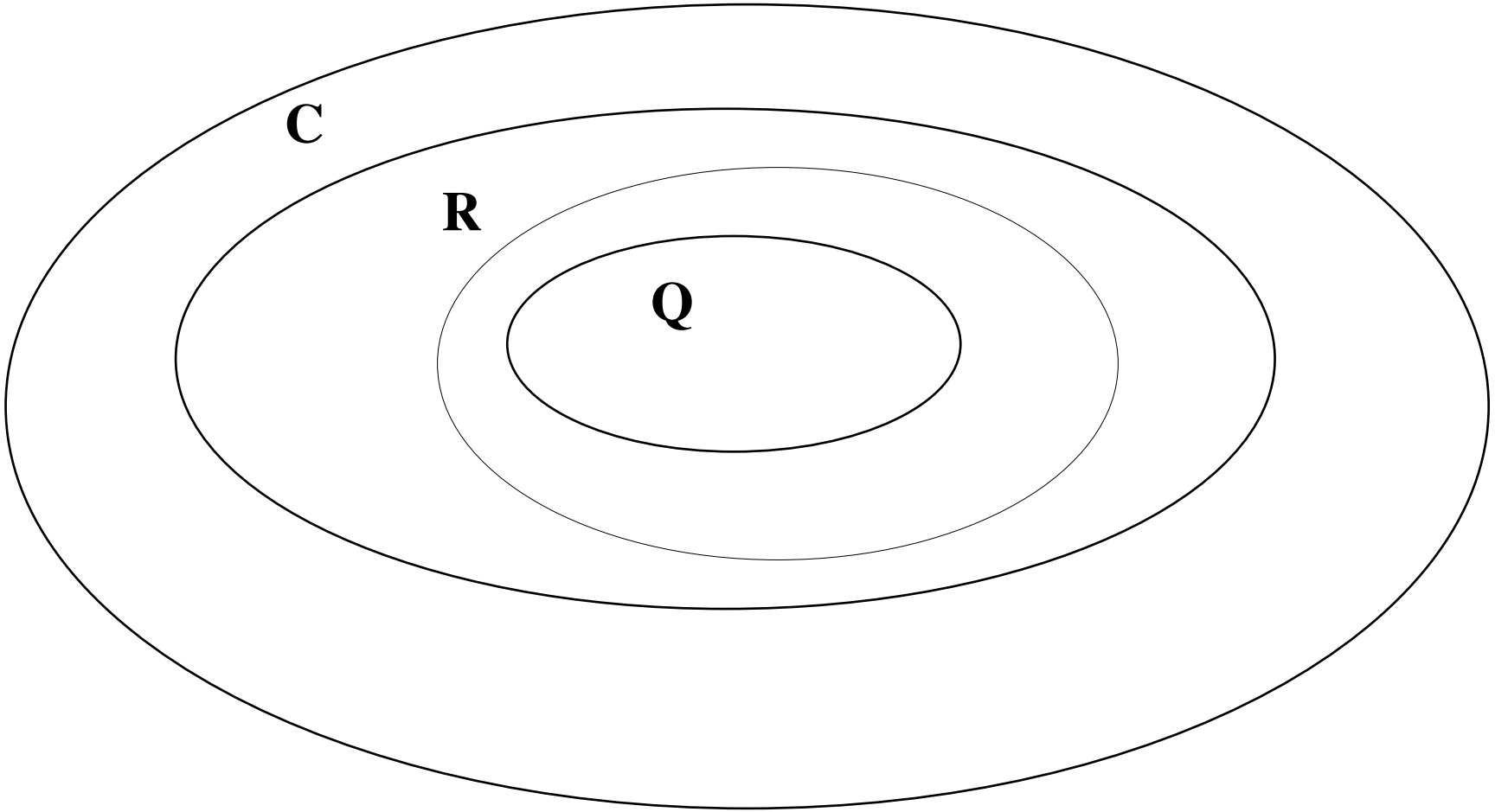
N-től **C**-ig

félgyűrű gyűrű test test test

integritási tartomány

euklideszi gyűrű

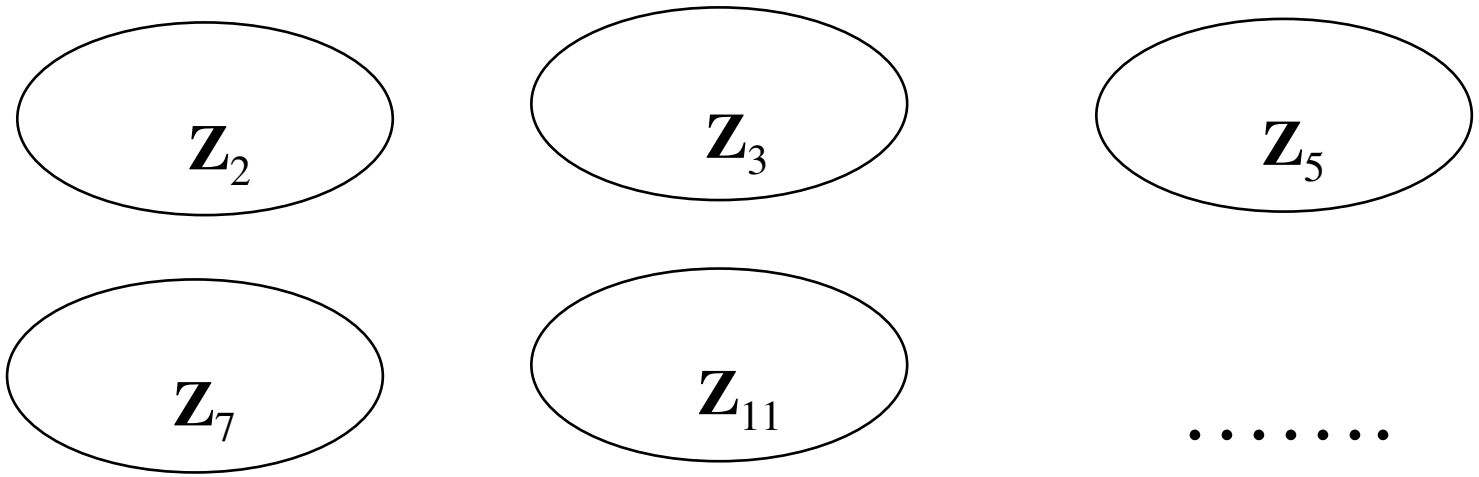
Számtestek



Eddig ismert véges testek

Tétel.

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



Testek bővítése

Feladatok

- 2. Testet alkotnak-e a szokásos műveletekre a következő halmazok?
  - a. $T_1 = \left\{ a + b\sqrt[4]{2} \,\middle|\, a,b \in \mathbf{Q} \right\}$
  - b. $T_2 = \left\{ a + bi\sqrt{5} \,\middle|\, a,b \in \mathbf{Q} \right\}$

Definíció.

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

Példa: R|Q, **C|Q**, **C|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.

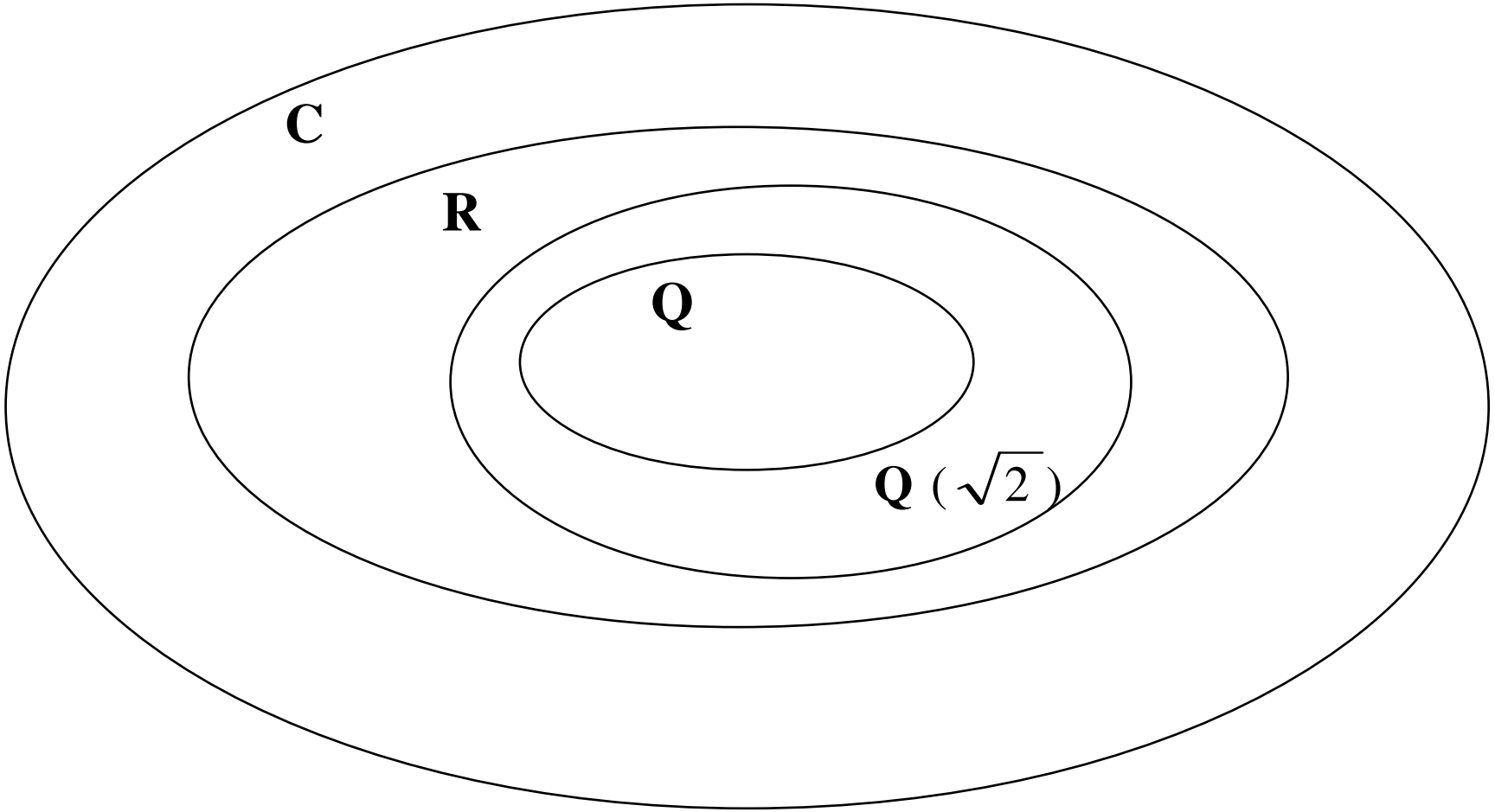
Egyszerű a bővítés, ha a bővítő halmaz egyetlen elemű.

Példa: $\mathbf{Q}(\sqrt{2})$ **,** $\mathbf{R}(i)$ (=**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, …) elkészítése a feladat, ezt elvégezhetjük lépésenként, a bővítő elemeket egyenként *adjungálva* az alaptesthez.


C
R
Q
Q (√2)

Feladatok

- 3. Mi a kapcsolat az alábbi testek között?

$$\mathbf{Q}\left(\sqrt{2}\right),\quad \mathbf{Q}\left(1+\sqrt{2}\right),\quad \mathbf{Q}\left(\sqrt{8}\right).$$

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

$$\mathbf{Q}\left(\sqrt{2}\right)=\mathbf{Q}\left(a+b\sqrt{2}\right)$$

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

$$\mathbf{Q}\left(\sqrt{2}+\sqrt{3}\right)$$

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 $u, u1, u2 \in L$ és $k, k1, k2 \in K$. ($k, k1, k2 \in L$ is fennáll.)

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

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

$(k1+k2) \cdot u = k1 \cdot u + k2 \cdot u$, és

$k \cdot (u1+u2) = k \cdot u1 + k \cdot u2$ a disztributivitás miatt

$(k1 \cdot k2) \cdot u = k1 \cdot (k2 \cdot u)$ 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 $\underline{0}$ tér dimenziója 0.

Jelölés: dimV.

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: R|Q végtelen bővítés;

C|R véges bővítés, mert {1, i} bázist alkot **C**-ben, mint **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 $\{a_1, a_2, \ldots, a_n\}$ egy bázis. Ekkor L minden u eleme előálllítható a bázis elemeinek lineáris kombinációjaként, s az előállítás egyértelmű.

$u= k_1a_1+ k_2a_2 + \ldots + k_na_n$, 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 fokszámtétele)

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 $\{b_1, b_2, ..., b_n\}$, az $M|L$ vektortér egyik bázisa $\{c_1, c_2, ..., c_k\}$.

Belátjuk, hogy ekkor a két bázis szorzataként előálló

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

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

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

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

Rendezzük az egyenlőséget c_s-ek szerint.

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

A c_s elemek lineárisan függetlenek, így mindegyikük együtthatója 0.

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

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|L-ben

  $u = v_1 c_1 + \ldots + v_k c_k \qquad v_s \in L.$ *

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

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

  Ezeket az * -ba helyettesítve:

Feladatok

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

Algebrai bővítés

Emlékeztető

Definíció.

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

$f(x)=a_n x^n+a_{n-1}x^{n-1}+...+a_1 x+a_0$ 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 **Q** felett algebraiak.

2 **Q** fölött algebrai x-2
R fölött algebrai x-2
C fölött algebrai x-2

$\sqrt{2}$ **Q** fölött algebrai x^2-2,
R fölött algebrai x^2-2,
C fölött algebrai x^2-2,

i **Q** fölött algebrai x^2+1
R fölött algebrai x^2+1
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: C|R algebrai bővítés, **R|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, …, u^n elemek lineárisan összefüggőek, mert legfeljebb n elem lehet lineárisan független. Van tehát olyan

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

lineáris kombinációs előállítás, amelyikben nem mindegyik α_s együttható 0.

Tekintsük a

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

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. $\mathbf{C}|\mathbf{R}$
  - b. $\mathbf{Q}(\sqrt{5})|\mathbf{Q}$
  - c. $A|\mathbf{Q}$
  - d. $A|\mathbf{Q}(\sqrt{5})$
  - e. $\mathbf{R}|\mathbf{Q}(\pi)$

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* (char R = 0), az utóbbiban *p-karakterisztikájúnak* (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: char($\mathbf{Q}$)=0, char($\mathbf{Z}_5$)=5.

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

Példa: char(**Q**)=0, char(**R**)=0, char(**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: R prímteste **Q**; **Q** prímteste önmaga; $\mathbf{Z}_p$ prímteste önmaga (p tetszőleges prím); **Q** és $\mathbf{Z}_p$ prímtestek

Tétel.

0 karakterisztikájú prímtest izomorf **Q**-val,

p-karakterisztikájú prímtest izomorf $\mathbf{Z}_p$-vel.

Következmény.

Minden 0 karakterisztikájú test lényegében **Q** bővítése,

minden p karakterisztikájú test lényegében $\mathbf{Z}_p$ 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 **Q** fölött x-2

R fölött x-2

C fölött x-2

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

R fölött $x-\sqrt{2}$,

C fölött $x-\sqrt{2}$,

i minimálpolinomja **Q** fölött x^2+1

R fölött x^2+1

C fölött x-i

Példa:

π minimálpolinomja **Q** fölött nem létezik

R fölött $x-\pi$

C fölött $x-\pi$

Feladatok

- 17. Határozzuk meg minimálpolinomját **Q** felett.
- 27. Az alábbi bővítésekben határozzuk meg a bővítő elem minimálpolinomját **Q** fölött.
  - a. $\mathbf{Q}\left(\sqrt{7}\right)|\mathbf{Q}$
  - b. $\mathbf{Q}\left(i\sqrt{5}\right)|\mathbf{Q}$
  - c. $\mathbf{Q}\left(1+i\sqrt{3}\right)|\mathbf{Q}$

Egyszerű algebrai bővítés

Emlékeztető

Definíció.

Az R integritási tartomány *euklidészi gyűrű,*

ha létezik olyan φ függvény, amelyre $\varphi : R^* \to \mathbf{N}_0$, és

I. $a, b \in R$, $b \neq 0$ esetén létezik olyan $c, d \in R$,hogy

$a=bc+d$, 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 $\varphi: R[x]^* \to \mathbf{N}_0$, $\varphi(f)=\deg f$.

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

(A test fölötti polinomgyűrűk euklideszi 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)·(s+I)=(r · s)+I

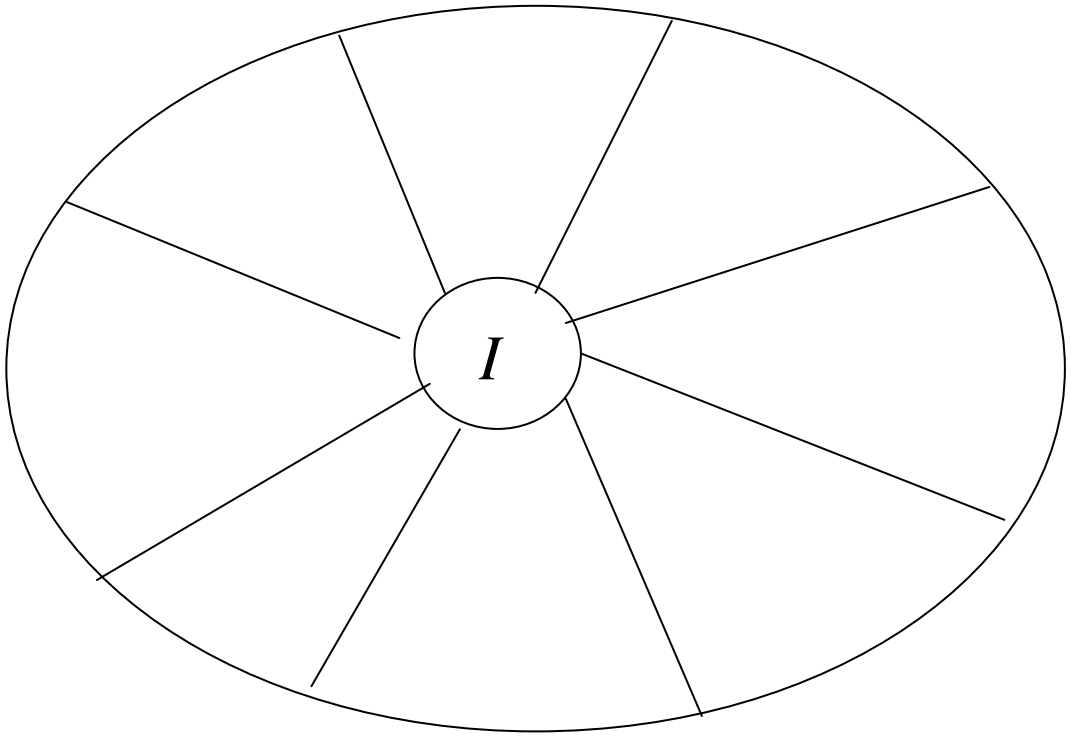
R/I gyűrűt alkot a definícióban szereplő műveletekre nézve.

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

R/I



Tétel.

Legyen $f \in K[x]$ irreducibilis polinom, (f) az f 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∈ 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.

  Legyen $f(x)=a_n x^n+a_{n-1}x^{n-1}+...+a_1x+a_0$

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

$$f([x])= a_n[x]^n+a_{n-1}[x]^{n-1}+...+a_1[x]+a_0 =$$
$$=[a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0]=(f)=0$$

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

$\{\alpha^0, \alpha, \ldots, \alpha^{n-1}\}$ bázis $K(\alpha)$-ban.

Feladatok

- 10. Készítsünk 9 elemű testet.
  - a. Adjuk meg a művelettáblákat.
  - 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 $u \in \mathbf{C}$ a $\mathbf{Q}$ feletti x^3-2x+2 polinom egyik gyöke. Lássuk be, hogy a polinom $\mathbf{Q}$ felett irreducibilis. Írjuk fel $\mathbf{Q}(u)|\mathbf{Q}$ $\{1, u, u^2\}$ bázisában a következő elemeket:
  - a. u^7
  - b. u^{-1}
  - c. u^4+u^{-2}

- 16. Legyen $u \in \mathbf{C}$ az x^3-6x^2+9x+3 $\mathbf{Q}$ felett irreducibilis polinom gyöke. Fejezzük ki $\mathbf{Q}(u)|\mathbf{Q}$ $\{1, u, u^2\}$ 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. $\mathbf{Q}\left(\sqrt{7}\right)$
  - b. $\mathbf{Q}\left(i\sqrt{5}\right)$
  - c. $\mathbf{Q}\left(1+i\sqrt{3}\right)$

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 **Q** fölött **Q**.

Az $x-2$ polinom felbontási teste **R** fölött **R**.

Az $x-\pi$ polinom felbontási teste **R** fölött **R**.

Az x^2+1 polinom felbontási teste **Q** fölött **Q**(i).

Az x^2+1 polinom felbontási teste **R** fölött **C**.

Feladatok

- 19. Határozzuk meg az $(x^2+1)(x^2-2x+1)$ polinom felbontási testét **Q** felett.
- 20. $\mathbf{Q}(\sqrt[3]{2})$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 **Q** felett?

Véges testek

Tétel.

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

Bizonyítás.

Legyen K=$\mathbf{Z}_p$, és vegyük 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'-nak 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. $L-L \subseteq L$ 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 $\mathbf{Z}_p$ 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.

$\mathbf{Z}_p$ elemeivel dolgozunk. Minden [a] maradékosztályhoz párosítjuk azt a [b] maradékosztályt, amellyel szorozva [1]-et ad. Mivel $\mathbf{Z}_p$ 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

$$u^2 \equiv 1 \ (p) \quad \rightarrow \quad 0 \equiv u^2-1 \equiv (u-1)(u+1) \quad (p)$$

$$p \text{ prím} \ \rightarrow \ p \mid u-1 \quad \text{vagy} \quad p \mid u+1 \rightarrow u \equiv 1 \quad (p) \quad \text{vagy} \quad u \equiv -1 \quad (p)$$

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:

$$c_1, c_2, \ldots, c_n$$

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

$$= a_n (x - c_1) \cdot (x - c_2) \cdot \ldots \cdot (x - c_n) =$$

$$= a_n (x^n - (c_1 + c_2 + \ldots + c_n) x^{n-1} +$$

$$+ (c_1 \cdot c_2 + c_1 \cdot c_3 + \ldots + c_{n-1} \cdot c_n) x^{n-2} +$$

$$\ldots + (-1)^n (c_1 \cdot c_2 \cdot \ldots \cdot c_n))$$

Ebből

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

$$\frac{a_{n-2}}{a_n} = (c_1 \cdot c_2 + c_1 \cdot c_3 + \ldots + c_{n-1} \cdot c_n)$$

$\ldots$

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

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.

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

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

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

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. Bartee: *A modern algebra a számítógép-tudományban* 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