

Diszkrét Matematika III

ALGEBRA Véges Testek

Gabor Farkas

farkasg@inf.elte.hu

gaborfarkasphd.wixsite.com/gaborfarkasphd

2017 Tavasz
ELTE

Def

Legyen F tetszőleges test. K az F **részteste**, ha $K \subseteq F$ és K maga is testet alkot az F műveleteivel. Jel.: $F : K$.

Ekkor F a K **test bővítése**. Ha $K \neq F$, akkor K **valódi részteste** F -nek, illetve F **valódi bővítése** K -nak.

Egy test **prímtest**, ha nincs valódi részteste.

Ész

Legyen F test és K részteste F -nek, ekkor F és K karakterisztikája megegyezik. Véges test karakterisztikája prímszám.

Résztestek metszete résztest $\Rightarrow$

F test összes résztestének metszete résztest F -ben

$\Rightarrow$ a legszűkebb résztest F -ben

$\Rightarrow$ nincs valódi részteste

$\Rightarrow$ prímtest

Def

Ha K az F –nek a legszűkebb részteste, akkor K az F **prím részteste (prímteste)**. (jelölés $K = Fp$)

Ész

Test prím részteste prímtest.

Ha F a K test bővítése, akkor prím résztesteik megegyeznek.

Tétel (Prím résztestek)

Tetszőleges F test prím részteste izomorf

$\mathbb{Z}_p$ –vel, ha $\text{char}(F) = p$,

$\mathbb{Q}$ –val, ha $\text{char}(F) = 0$.

Köv

minden p karakterisztikájú test $\mathbb{Z}_p$ bővítése, és minden nullkarakterisztikájú test $\mathbb{Q}$ bővítése.

Def

Legyen egy K részteste, M egy részhalmaza F -nek.

$K(M)$ a K test M halmazzal való bővítése,

ha F -nek a legszűkebb részteste, mely tartalmazza K -t és M -et is.

Ha $M = \{ \alpha \}$ alakú, valamely $\alpha \in F$ -re, akkor

$K(\alpha)$ egyszerű bővítés az α bővítő elemmel.

Legyen egy K részteste F -nek, és $\alpha \in F$,

ha α gyöke egy nem nulla K feletti polinomnak, akkor
 α algebrai elem K felett.

F algebrai bővítése K -nak, ha F minden eleme algebrai K felett.

Def

$F : K$ esetén, ha F mint K feletti vektortér nem véges dimenziós akkor a **bővítés végtelen**, egyébként **véges bővítésről** beszélünk.

Def

Az $F : K$ **testbővítés foka** az F K feletti vektortér dimenziója, jelben $[F : K]$.

Tétel (Testbővítések foka)

Ha $M : L$ és $L : K$ véges testbővítés, akkor $M : K$ véges bővítés és

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

Tétel (Véges bővítés algebrai)

Tetszőleges K test véges bővítése algebrai K felett.

Tétel (Egyszerű bővítés létezése)

Legyen $f \in K[x]$ irreducibilis polinom K test felett. Ekkor létezik K -nak olyan egyszerű algebrai bővítése, ahol a bővítő elem f -nek gyöke.

Példa

$$f(x) = x^2 + x + 2 \in \mathbb{Z}_3$$

$$f(0) = -1 \quad \& \quad f(1) = 1 \quad \& \quad f(-1) = -1$$

$f(x)$ irreducibilis $\mathbb{Z}_3$ felett.

Legyen $u^2 + u + 2 = 0$ azaz

u gyöke f -nek $\Rightarrow$

u egy maradékosztály $\mathbb{Z}_3 / \langle f \rangle$ -ben

legyen a tétel szerint $u = [x] = x + \langle f \rangle$.

$$\text{Mivel } \mathbb{Z}_3 / \langle f \rangle = \mathbb{Z}_3(u)$$

$$\text{tétel} \Rightarrow \mathbb{Z}_3 / \langle f \rangle \text{ bázisa: } \{ 1, u \}$$

$$\mathbb{Z}_3 / \langle f \rangle \text{ elemei: } 0, 1, 2, u, u+1, u+2, 2u, 2u+1, 2u+2$$

Vegyük észre:

f -nek $2u+2$ is gyöke !

$$f(2u+2) = (2u+2)^2 + (2u+2) + 2 =$$

$$4u^2 + 8u + 4 + 2u + 2 + 2 =$$

$$4(\underbrace{u^2 + u + 2}_0) + 4u - 4 + 2u + 2 + 2 =$$

$$6u = 0$$

Ha $2u+2$ -vel végezzük a bővítést, algebrai szempontból ugyanazt a testet kapjuk!



Tétel (Egyszerű bővítések izomorfizma)

Legyen α és β gyöke a K test felett irreducibilis $f \in K[x]$ polinomnak. Ekkor $K(\alpha)$ és $K(\beta)$ izomorf. Az izomorfizmus α -t β -ba viszi át, K elemeit pedig fixen hagyja.

Kérdés: van olyan bővítés, ami f minden gyökét tartalmazza ?

Def

Legyen K test és $f \in K[x]$, úgy, hogy $\deg(f) = n > 0$. Ekkor K -nak az a legszűkebb bővítése, amelyben f -nek multiplicitással számolva pontosan n gyöke van, f polinom K feletti felbontási teste.

Tétel (Felbontási test egzisztenciája és unicitása)

Legyen K test és $f \in K[x]$, úgy, hogy $\deg(f) = n > 0$. Ekkor létezik f polinom K feletti felbontási teste és bármely két ilyen izomorf, azon a leképezés mellett, amely K elemeit önmagukba, f gyökeit egymásba képezi le.

Tétel (Véges testek egzisztenciája)

Tetszőleges véges test elemszáma p^n , ahol p prím és n pozitív egész, továbbá tetszőleges p prím és n pozitív egész számhoz található p^n elemszámú véges test.

Tétel (Véges testek unicitása)

Tetszőleges $q = p^n$ elemszámú véges test izomorf az $f = x^q - x$ polinom F_p feletti felbontási testével.

Tétel (Véges testek résztest kritériuma)

Legyen F_q tetszőleges $q = p^n$ elemszámú véges test.

F_q minden részteste p^m –edrendű, ahol $m \mid n$, és

minden $m \mid n$ -hez egyértelműen létezik F_q -nak p^m –edrendű részteste.

Példa

