Egyszerű algebrai testbővítések

3.37. Tétel.

Ha R főideálgyűrű és $m \in R \setminus \{0\}$, akkor

$$R/\langle m \rangle \text{ test} \iff m \text{ irreducibilis.}$$

Bizonyítás.

Ha $m \sim 1$, akkor $R/\langle m \rangle$ egyelemű gyűrű, így nem lehet test.

Ha $m \nsim 1$, akkor $R/\langle m \rangle$ legalább kételemű kommutatív egységelemes gyűrű, tehát azt kell megvizsgálnunk, hogy van-e minden nemnulla elemének multiplikatív inverze.

- Ha m nem irreducibilis, akkor van nemtriviális faktorizációja: $m = ab$, ahol $a \nsim m$ és $b \nsim m$. Ekkor $\overline{a} \neq \overline{0}$ és $\overline{b} \neq \overline{0}$, de $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{m} = \overline{0}$, tehát $\overline{a}$ és $\overline{b}$ zérusosztók az $R/\langle m \rangle$ gyűrűben, így az nem test.

- Tfh. m irreducibilis, és legyen $\overline{a} \in R/\langle m \rangle$. Ha $\overline{a} \neq \overline{0}$, akkor $m \nmid a$, és így $\operatorname{lnko}(a, m) \sim 1$. A 3.28. Állítás szerint vannak olyan $u, v \in R$ elemek, amelyekre $au + mv = 1$. Ebből következik, hogy $\overline{a} \cdot \overline{u} = \overline{1}$, azaz $\overline{a}^{-1} = \overline{u}$. □

Megjegyzés.

Ha $m = 0$, akkor $R/\langle m \rangle \cong R$, tehát ebben az esetben $R/\langle m \rangle$ akkor és csak akkor test, ha R test.

Következmény.

Tetszőleges K test és $m \in K[x]$ polinom esetén $K[x]/\langle m \rangle$ akkor és csak akkor test, ha m irreducibilis K felett.

Bizonyítás.

Tudjuk, hogy $K[x]$ főideálgyűrű (3.33. Következmény), ezért $m \neq 0$ esetén alkalmazható az előző tétel.
Az $m = 0$ esetben $K[x]/\langle m \rangle \cong K[x]$, ami nem test. □

Példa.

Melyek testek az alábbi faktorgyűrűk közül?

- $\mathbb{Z}_2[x]/\langle x^2+1 \rangle$: nem, mert $x^2+1 = (x+1)^2$.
- $\mathbb{Z}_3[x]/\langle x^2+1 \rangle$: igen, mert x^2+1 másodfokú, és nincs gyöke $\mathbb{Z}_3$-ban.
- $\mathbb{Z}_2[x]/\langle x^2+x+1 \rangle$: igen, mert x^2+x+1 másodfokú, és nincs gyöke $\mathbb{Z}_2$-ben.
- $\mathbb{Z}_2[x]/\langle x^4+x^2+1 \rangle$: nem, mert $x^4+x^2+1 = (x^2+x+1)^2$.
- $\mathbb{Q}[x]/\langle x^4+4x^3+6x^2+8x+10 \rangle$: igen, mert $x^4+4x^3+6x^2+8x+10$ irreducibilis $\mathbb{Q}$ felett.

Példa.

Számoljunk a $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ testben.

$$\mathbb{Z}_2[x]/\langle x^2+x+1\rangle = \{\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1}\}$$

$$\overline{x+1}+\overline{1} = \overline{x}$$

$$-\overline{x+1} = \overline{x+1}$$

$$\overline{x+1}\cdot\overline{x+1} = \overline{x^2+1} = \overline{x}$$

$$\begin{aligned}
\overline{x+1}^{-1} = \overline{u} &\iff \overline{x+1}\cdot\overline{u} = \overline{1} \\
&\iff (x+1)\,u \equiv 1 \pmod{x^2+x+1} \\
&\iff \exists v \in \mathbb{Z}_2[x] : (x+1)\,u = 1 + (x^2+x+1)\,v \\
&\iff u \equiv x \pmod{x^2+x+1} \\
&\iff \overline{u} = \overline{x}
\end{aligned}$$

A négyelemű $L := \mathbb{Z}_2[x] / \langle x^2 + x + 1 \rangle$ test művelettáblázatai:

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

Ugyanez tömörebben, a $0 := \overline{0}$, $1 := \overline{1}$, $\alpha := \overline{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Figyeljük meg, hogy

- $\{0, 1\} = \{\overline{0}, \overline{1}\}$ egy $\mathbb{Z}_2$-vel izomorf résztestet alkot L-ben;
- $\alpha = \overline{x}$ gyöke az $x^2 + x + 1 \in L[x]$ polinomnak:
  $\alpha^2 + \alpha + 1 = \overline{x}^2 + \overline{x} + \overline{1} = \overline{x^2 + x + 1} = \overline{0} = 0.$

Példa.

Az $m = x^3 + x + 1 \in \mathbb{Z}_2[x]$ polinom irreducibilis (mert nincs gyöke, és csak harmadfokú), ezért az $L := \mathbb{Z}_2[x] / \langle x^3 + x + 1 \rangle$ maradékosztály-gyűrű test. Ennek a testnek 8 eleme van:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1}.$$

Vezessük be az $\alpha = \overline{x}$ jelölést, és hagyjuk el a vonásokat a konstansokról. Ezzel a jelöléssel az L test 8 eleme:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

Figyeljük meg, hogy $\{0, 1\}$ egy $\mathbb{Z}_2$-vel izomorf résztestet alkot K-ban, tehát kis jóindulattal mondhatjuk, hogy $\mathbb{Z}_2 \subseteq L$, vagyis L kibővítése $\mathbb{Z}_2$-nek.

Számítsuk ki $m(\alpha)$ értékét:

$$m(\alpha) = \alpha^3 + \alpha + 1 = \overline{x}^3 + \overline{x} + \overline{1} = \overline{x^3 + x + 1} = \overline{m} = \overline{0}.$$

Ez azt jelenti, hogy az L testben már van gyöke az m polinomnak!

Számoljunk a $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ testben. A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo x^3+x+1 kell számolni.

$$\overline{x+1}+\overline{x^2+x}=\ \overline{x^2+2x+1}\ =\quad \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1}\cdot\overline{x^2+x}\ =\overline{x^3+2x^2+x}=\overline{x^3+x}=\overline{1} \quad \text{(redukció mod } x^3+x+1)$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3+\alpha+1=0, \quad \text{azaz}\ \ \alpha^3=\alpha+1.$$

$$(\alpha+1)+\left(\alpha^2+\alpha\right)=\ \alpha^2+2\alpha+1\ =\alpha^2+1 \qquad \text{(s.v.)}$$

$$(\alpha+1)\cdot\left(\alpha^2+\alpha\right)\ =\alpha^3+2\alpha^2+\alpha=\alpha^3+\alpha=(\alpha+1)+\alpha=1 \quad \text{(sz.sz.)}$$

A nyolcelemű test művelettáblázatai

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

4.9. Tétel.

Legyen $m \in K[x]$ irreducibilis n-edfokú polinom, és legyen $L = K[x]/\langle m \rangle$.

(1) L test.

(2) L-ben a konstans polinomok modulo m maradékosztályai egy K-val izomorf résztestet alkotnak ($K \longrightarrow L$, $a \mapsto \overline{a}$ beágyazás).

(3) Az $\alpha = \overline{x}$ jelöléssel L minden eleme egyértelműen előáll a következő alakban:

$$a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \quad (a_{n-1}, \ldots, a_1, a_0 \in K).$$

(4) $L = K[\alpha] = K(\alpha)$.

(5) L egy n-dimenziós vektorteret alkot K felett.

(6) $m(\alpha) = 0$.

Bizonyítás.

(1) Láttuk már, hogy a 3.37. Tétel szerint $K[x]/\langle m \rangle$ valóban test, hiszen $K[x]$ főideálgyűrű és $m \in K[x]$ irreducibilis.

Biz. (folyt.)

(2) Tetszőleges $a, b \in K$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy $K_1 := \{\overline{a} \colon a \in K\}$ egy K-val izomorf résztest L-ben (a megfelelő izomorfizmus: $K \to K_1$, $a \mapsto \overline{a}$).

Ha K_1-et azonosítjuk magával K-val (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in K$-ra), akkor K részteste lesz L-nek (azaz L egy bővítése K-nak).

(3) A $K[x]/\langle m \rangle$ test elemei a K feletti polinomok modulo m maradékosztályai. A maradékos osztás tétele alapján minden maradékosztály egyértelműen reprezentálható egy $\deg m = n$-nél kisebb fokú polinommal, tehát L minden eleme egyértelműen felírható a következő alakban (alkalmas $a_0, a_1, \ldots, a_{n-1} \in K$ együtthatókkal):

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} = \overline{a_{n-1}} \cdot \overline{x}^{n-1} + \cdots + \overline{a_1} \cdot \overline{x} + \overline{a_0} =$$
$$= a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0.$$

Biz. (folyt.)

$$\forall \beta \in L \; \exists! a_0, a_1, \ldots, a_{n-1} \in K: \;\; \beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}. \qquad (\Diamond)$$

(4) Kiolvasható $(\Diamond)$-ból, hogy L minden elme előáll α-ból és K elemeiből az első három alapművelet segítségével, azaz $L \subseteq K[\alpha]$.
Mivel $K[\alpha] \subseteq K(\alpha) \subseteq L$, rögtön következik, hogy $L = K[\alpha] = K(\alpha)$.

(5) Az is látható $(\Diamond)$-ból, hogy L minden eleme felírható, mégpedig egyértelműen, az $1, \alpha, \ldots, \alpha^{n-1}$ elemek K-beli együtthatós lineáris kombinációjaként. Tehát $1, \alpha, \ldots, \alpha^{n-1}$ bázisa L-nek, mint K feletti vektortérnek, és így $\dim_K L = n$.

(6) Legyen $m = c_n x^n + \cdots + c_1 x + c_0 \in K[x]$. Számítsuk ki $m(\alpha)$ értékét:

$$m(\alpha) = c_n\alpha^n + \cdots + c_1\alpha + c_0 = \overline{c_n} \cdot \overline{x}^n + \cdots + \overline{c_1} \cdot \overline{x} + \overline{c_0} = \\ = \overline{c_n x^n + \cdots + c_1 x + c_0} = \overline{m}.$$

Az világos, hogy $\overline{m} = \overline{0}$, tehát $m(\alpha) = \overline{0} = 0$.

□

ÖRÖMHÍR!

Minden polinomnak van gyöke! Ha nem az eredeti testben, akkor annak egy alkalmas kibővítésében.

Ha az $m = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in K[x]$ irreducibilis főpolinomnak akarunk „gyököt csinálni”, akkor az $L = K[x]/\langle m \rangle$ testet kell elkészítenünk.

Az L test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, a_1, \ldots, a_{n-1} \in K).$$

Az α szimbólumról csak annyit kell tudni, hogy $m(\alpha) = 0$, azaz $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$. Tehát a számolási szabály:

$$\alpha^n = -c_{n-1}\alpha^{n-1} - \cdots - c_1\alpha - c_0.$$

(És ha m nem irreducibilis?)

Példa.

Ha az L testet a $K = \mathbb{R}$ és $m = x^2 + 1$ esetre felírjuk, éppen a komplex számok testét kapjuk.

Most $n = 2$, tehát

$$L = \left\{ \overline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{R} \right\}.$$

Menjünk le alfába...

Az L test elemeinek kanonikus alakja:

$$a_0 + a_1 \alpha \quad (a_0, a_1 \in \mathbb{R}).$$

Az α szimbólumra vonatkozó számolási szabály: $m(\alpha) = \alpha^2 + 1 = 0$, vagyis

$$\alpha^2 = -1.$$

Ezzel éppen a komplex számok testét kaptuk (csak α helyett i a szokásos jelölés).

Tehát $\mathbb{C} \cong \mathbb{R}[x] / \langle x^2 + 1 \rangle$, és ezt tekinthetnénk akár a komplex számok definíciójának is.

Példa.

Határozzuk meg az $L = \mathbb{Q}[x] / \langle x^3 - 7 \rangle$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

L elemei $\overline{ax^2+bx+c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2-x}^{-1}$ elemet is megkapni.

$$\begin{aligned}
\overline{2-x}^{-1} = \overline{u} &\iff \overline{2-x} \cdot \overline{u} = \overline{1} \\
&\iff (2-x)\,u \equiv 1 \pmod{x^3-7} \\
&\iff \exists v \in \mathbb{Q}[x] : (2-x)\,u = 1 + (x^3-7)\,v \\
&\iff u \equiv x^2+2x+4 \pmod{x^3-7} \\
&\iff \overline{u} = \overline{x^2+2x+4}
\end{aligned}$$

Tehát $\overline{2-x}^{-1} = \overline{x^2+2x+4}$.

Gyöktelenítés

Menjünk le alfába:

$$L = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki: $\alpha = \sqrt[3]{7}$! (Vagy $\alpha = \sqrt[3]{7}\,\mathrm{cis}\,\frac{\pm 2\pi}{3}$.) Tehát L tekinthető számtestnek is:

$$L = \left\{ a\sqrt[3]{49} + b\sqrt[3]{7} + c \colon a, b, c \in \mathbb{Q} \right\}.$$

Az előbb kiszámoltuk, hogy $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$, ami azt jelenti, hogy $(2 - \alpha)^{-1} = \alpha^2 + 2\alpha + 4$, azaz

$$\frac{1}{2 - \sqrt[3]{7}} = \sqrt[3]{49} + 2\sqrt[3]{7} + 4.$$

Ezzel a módszerrel (lényegében az euklideszi algoritmussal) lehet bonyolult nevezőket gyöktelenníteni.

Megjegyzés.

- Az előbbi konstrukcióval bármely $f \in K[x]$ polinomnak lehet „gyököt csinálni” az alaptest egy megfelelő L kibővítésében.
  (Ha f nem irreducibilis, akkor dolgozzunk egy irreducibilis osztójával.)
- Az eljárást ismételve olyan test is konstruálható, amelyben már f-nek annyi gyöke van, amennyi a fokszáma, azaz f elsőfokú polinomok (gyöktényezők) szorzatára bomlik (f felbontási teste).
- Transzfinit indukcióval igazolható olyan $\overline{K}$ test létezése is, amelyben már nem csak egy kiválasztott $f \in K[x]$ polinom bomlik lineáris tényezők szorzatára, hanem minden K feletti polinom (a $\overline{K}$ testet a K test algebrai lezártjának nevezzük).
- Az algebra alaptétele szerint a komplex számok teste algebrailag zárt ($\overline{\mathbb{C}} = \mathbb{C}$), ez a valós számtest algebrai lezártja is ($\overline{\mathbb{R}} = \mathbb{C}$).
- A racionális számtest algebrai lezártja az algebrai számok teste.