8. előadás

Számolás egyszerű algebrai bővítésekben (ismétlés, összefoglaló)

Emlékeztető: $K \leq L$ esetén (ahol K és L testek) L egyszerű bővítése K-nak, ha $\exists \alpha \in L$, melyre $L = K(\alpha)$. Ez azt jelenti, hogy a legszűkebb olyan részteste, ami a K elemei mellett α-t is tartalmazza, maga az egész L. (Ez belőle nem azt jelenti, hogy K mellé egyetlen új elem kerül, hiszen α mellé be kell kerülnie α^2-nek, α^3+1-nek, $\frac{3\alpha-1}{4\alpha^2+5}$-nek is stb.)

A $K(\alpha)$ egyszerű bővítést algebrainak nevezzük, ha α algebrai a K fölött. Vegyük észre, hogy a megnevezés nem alaptalan: ugyanis elképzelhető lenne, hogy $K(\alpha) = K(\beta)$, és α algebrai, β pedig nem az, s ebben az esetben nem lenne világos a megnevezés, szerencsére tudhatjuk, hogy ez az eset nem fordulhat elő, mert:

- ha α algebrai K fölött, és a minimálpolinomjának a foka n ($< \infty$), akkor a $|K(\alpha):K|$ bővítés foka n;
- ha az $|L:K|$ fok véges, akkor L minden eleme algebrai K fölött, és a fokuk legfeljebb $|L:K|$, sőt, a fokszámtételből az is következik, hogy ilyenkor $\beta \in L$-re $\underbrace{\operatorname{gr}_K \beta}_{\beta \text{ minimálpolinomjának a foka}} \mid |L:K|$.

Egyszerű algebrai bővítés elemei: Ha $\alpha \in L$ algebrai K felett:

$$K(\alpha) = \{ f(\alpha) \in L \mid f \in K[x],\ f = 0 \text{ v. } \operatorname{gr} f < \operatorname{gr}_K \alpha \}$$

Tehát $K(\alpha)$ elemei az α adeszy feletti polinomiális kifejezései, ahol az adeszy fok azt jelenti, hogy az α fokánál (azaz az α minimálpolinomjának fokánál) adeszerebb fokú.

Pl. $\mathbb{Q}(\sqrt[3]{2}) = \{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q} \}$

$$\updownarrow$$

$$f(x) = a + bx + cx^2;\quad \operatorname{gr}_{\mathbb{Q}}(\sqrt[3]{2}) = 3$$

Ami ne teljesen nyolctól elkülönülő:

- a) Miért lesz az a halmaz zárt a szorzásra?
- b) Miért lesz az a halmaz zárt a nem nulla elem inverzének a képzésére?

A fenti példánál az első, a) kérdésre több levezetés nélkül is a vektorok: a szorzásnál racionális számokat, $\sqrt[3]{2}$-t és $\sqrt[3]{4}$-et kell szorozni; de azok közül az összefüggések: $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$; $\sqrt[3]{2} \cdot \sqrt[3]{4} = 2 \in \mathbb{Q}$, $\sqrt[3]{4} \cdot \sqrt[3]{4} = 2 \cdot \sqrt[3]{2}$, tehát csupa megengedett alakú számot kapunk.

Másik példánál az már ne ennyire kézenfekvő esetleg: pl. a $\beta = \sqrt{2} + \sqrt{3}$ gyöke az $f = x^4 - 10x^2 + 1$ polinomnak: ha β^3-öt szorzik β^2-tel, miért lehet azt β-beli együtthatókkal felírni, méghozzá hogy kitevővel:

Szerencsére, tudjuk a választ erre is: β gyöke az $x^4 - 10x^2 + 1$ polinomnak, így:

$$\beta^4 = 10\beta^2 - 1$$

$$\beta^5 = 10\beta^3 - \beta$$

$$\beta^6 = 10\beta^4 - \beta^2 = 10(10\beta^2 - 1) - \beta^2$$

stb.

b) Az osztás (reciprok kiszámolása) is lehet gyors!

Pl.: $\mathbb{Q}(\sqrt[3]{2})$-ben: $\frac{1}{1+\sqrt[3]{2}}$ „gyöktelenítéssel" végezhető:

$$\frac{1}{1+\sqrt[3]{2}} = \frac{1}{1+\sqrt[3]{2}} \cdot \frac{1-\sqrt[3]{2}+\sqrt[3]{4}}{1-\sqrt[3]{2}+\sqrt[3]{4}} = \frac{1-\sqrt[3]{2}+\sqrt[3]{4}}{3} = \frac{1}{3} - \frac{1}{3}\sqrt[3]{2} + \frac{1}{3}\sqrt[3]{4}$$

De a képlet már itt sem látszik könnyen. Mi lesz pl.

$$\frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} + 4}\ ?$$

A nevezőben található $f(x) = x^2 - 2x + 4$-re $f(\sqrt[3]{2})$ áll.

Itt már nem látszik olyan jól, hogy hogyan kell gyöktelenítsünk.

Persze, valahogy az általános módszert, amivel igazoltuk az osztás elvégezhetőségét: Keressük olyan $u(x), v(x) \in \mathbb{Q}[x]$ polinomokat, melyekre:

$$u(x)\cdot(x^3 - 2) + v(x)\cdot f(x) = 1,$$

mert akkor: $u(\sqrt[3]{2})\cdot(\underbrace{(\sqrt[3]{2})^3 - 2}_{=0}) + v(\sqrt[3]{2})\cdot f(\sqrt[3]{2}) = 1.$

De ez elég hosszadalmas az euklidészi algoritmussal. Pusztán, ha elkerüljük a maradékos osztást, akkor az alábbit kapjuk:

$$(x^3-2) : (x^2-2x+4) = x+2$$
$$-(x^3-2x^2+4x)$$
$$2x^2-4x-2$$
$$-(2x^2-4x+8)$$
$$-10$$

Tehát: $x^3-2 = (x+2)(x^2-2x+4)-10$, vagyis:

$\sqrt[3]{2}$-t helyettesítve írható előállításba:

$$0 = (\sqrt[3]{2}+2)(\sqrt[3]{4}-2\sqrt[3]{2}+4)-10, \text{ azaz:}$$

$$(\sqrt[3]{2}+2)(\sqrt[3]{4}-2\sqrt[3]{2}+4) = 10, \text{ és innen:}$$

$$\frac{1}{\sqrt[3]{4}-2\sqrt[3]{2}+4} = \frac{\sqrt[3]{2}+2}{10}$$

Vagyis itt most szerencsénk volt, mert az euklidészi algoritmus egy lépésben véget ért.

De nehezebb helyzetben lennénk pl. az előbb vizsgált $\beta = \sqrt{2}+\sqrt{3}$-mal, ill. annak egy hatványával.

Az előző példánkra visszatérve: érdekes kiszámítani,

Hogy kapjuk: $\frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} + 4} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ valamilyen

$a, b, c \in \mathbb{Q}$ számokra (mégpedig egyértelműen).

Ebben segít a reciprok keresését visszavezetni egy lineáris egyenletrendszerre:

$$(4 - 2\sqrt[3]{2} + \sqrt[3]{4})(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = 1$$

$$\Leftrightarrow 4a + 4b\sqrt[3]{2} + 4c\sqrt[3]{4} -$$
$$- 2a\sqrt[3]{2} - 2b\sqrt[3]{4} - 2c\sqrt[3]{2}\cdot\sqrt[3]{4} +$$
$$+ a\sqrt[3]{4} + b\sqrt[3]{2}\cdot\sqrt[3]{4} + c\cdot\sqrt[3]{4}\cdot\sqrt[3]{4} = 1$$

($\sqrt[3]{2}\cdot\sqrt[3]{4} = \alpha^3 = 2$, $\sqrt[3]{4}\cdot\sqrt[3]{4} = \alpha^4 = 2\cdot\sqrt[3]{2}$)

$$\Leftrightarrow 4a + 4b\sqrt[3]{2} + 4c\sqrt[3]{4} -$$
$$- 4c - 2a\sqrt[3]{2} - 2b\sqrt[3]{4} +$$
$$+ 2b + 2c\sqrt[3]{2} + a\sqrt[3]{4} = 1$$

$$\Leftrightarrow (4a + 2b - 4c) + (-2a + 4b + 2c)\sqrt[3]{2} + (a - 2b + 4c)\sqrt[3]{4} = 1$$

$$\Leftrightarrow \begin{aligned} 4a + 2b - 4c &= 1 \\ -2a + 4b + 2c &= 0 \\ a - 2b + 4c &= 0 \end{aligned}$$

← (Ez a rész akkor érdekes, ha $1, \sqrt[3]{2}$ és $\sqrt[3]{4}$ lineárisan függetlenek.)

A reciprok kiszámolásához tehát ezt a lineáris egyenletrendszert kell megoldanunk. Ezt β polinomjával is meg tudnánk csinálni, hiszen β hatványait már kiszámoltuk meg felhasználtuk is.

Ez azt jelenti, hogy $f \neq 0$, $\deg f < \deg_K \alpha$ esetén $\frac{1}{f(\alpha)}$ kiszámolható, ha:

1) tudjuk az α negyedik hatványait felírni legfeljebb harmadfokú kifejezéssel

2) megoldunk egy lineáris egyenletrendszert.

Minimálpolinom kiszámolása:

Hogyan számoljuk ki egy algebrai elem minimálpolinomját? A korábban már említett $\beta = \sqrt{2} + \sqrt{3}$-nak pl. mi lesz a minimálpolinomja? Pl. „ügyeskedéssel" az alábbiakat tesszük:

$$\beta = \sqrt{2} + \sqrt{3}$$

$$\beta - \sqrt{2} = \sqrt{3} \quad / ()^2$$

$$\beta^2 - 2\sqrt{2}\beta + 2 = 3$$

$$\beta^2 - 1 = 2\sqrt{2}\beta \quad / ()^2$$

$$\beta^4 - 2\beta^2 + 1 = 8\beta^2$$

$$\beta^4 - 10\beta^2 + 1 = 0$$

Vagyis β valóban gyöke az $x^4 - 10x^2 + 1$ polinomnak, mint azt állítottuk.

Vajon ez lesz-e a minimálpolinom?

Mivel a fent megtalált polinom x^2-ben másodfokú, kiszámolhatjuk a gyökeit: x^2 értéke $5 \pm 4\sqrt{6}$ lehet, így az $x_{1,2,3,4}$ gyökök: $\pm\sqrt{2} \pm \sqrt{3}$. Vagyis $\mathbb{R}$ felett:

$$x^4 - 10x^2 + 1 = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}).$$

Könnyen látható, hogy egyik gyök sem racionális (bizonyítandó!), így ha ez $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ felbomlik, akkor csakis két másodfokú szorzatra bomolhatna, az ilyen tényezők pedig 2-2 gyöktényező összeszorzásából adódnának. De egyik ilyen párosítás sem ad $\mathbb{Q}[x]$-beli szorzatot $\Rightarrow$ $x^4 - 10x^2 + 1$ irreducibilis $\mathbb{Q}[x]$-ben, így az valóban minimálpolinomja $\beta = \sqrt{2} + \sqrt{3}$-nak.

Persze, az egy hosszú számolással kijön, hogy ilyen könnyen meghatározni a polinom gyökeit (ne feledjük az!)

Vissza alkalmazhatjuk a szorzástételt is!

Az előbbi levezetésből látszik, hogy:

$$\beta^2 - 1 = 2\sqrt{2}\beta, \quad \text{azaz}$$

$$\frac{\beta^2 - 1}{2\beta} = \sqrt{2}$$

Ez azt jelenti, hogy $\sqrt{2} \in \mathbb{Q}(\beta)$.

(Mellesleg: az nem automatikus!) Tehát:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\beta).$$

Ebből, mivel $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$, már következik, hogy β foka csak 2 v. 4 lehet, hiszen:

$$2 = |\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| \;\Big|\; |\mathbb{Q}(\beta) : \mathbb{Q}| = \deg \beta. \quad (\leq 4).$$

Ahhoz, hogy megtaláljuk, a fok 4, ezt kell igazolnunk, hogy $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\beta)$, azaz $\exists \gamma \in \mathbb{Q}(\beta) \setminus \mathbb{Q}(\sqrt{2})$.

De ezt megelőzi egy jelölés: $\sqrt{3}$. Ugyanis:

$$\left.\begin{array}{l} \sqrt{2}+\sqrt{3} = \beta \in \mathbb{Q}(\beta) \\ \sqrt{2} \in \mathbb{Q}(\beta) \end{array}\right\} \Rightarrow \quad \beta - \sqrt{2} = \sqrt{3} \in \mathbb{Q}(\beta)$$

Vissza $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, hiszen

$\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \} \Rightarrow \sqrt{3}$ esetén:

$\exists a, b \in \mathbb{Q}$: $\quad a + b\sqrt{2} = \sqrt{3}$.

$$\Rightarrow \quad a^2 + 2ab\sqrt{2} + b^2 = 3$$

$$\Rightarrow \quad 2ab\sqrt{2} = 3 - a^2 - b^2$$

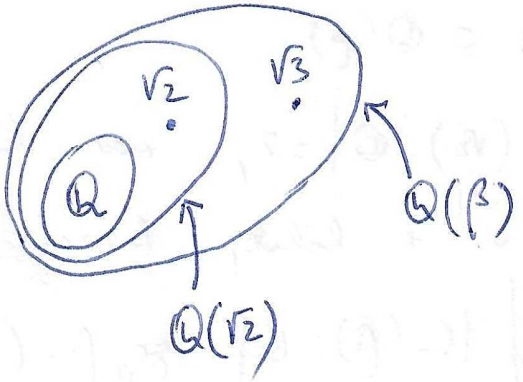
$a, b \neq 0$ esetén: $\sqrt{2} = \dfrac{3-a^2-b^2}{2ab} \in \mathbb{Q}$ ↯.

Tehát vagy a, vagy $b = 0$, és valamelyik sem 0.

$a = 0$ esetén: $b\sqrt{2} = \sqrt{3} \Rightarrow b = \dfrac{\sqrt{3}}{\sqrt{2}} \in \mathbb{Q}$ ↯.

$b = 0$ esetén: $a = \sqrt{2} \in \mathbb{Q}$ ↯.

Ez azt jelenti, hogy:



, és így $|\mathbb{Q}(\beta) : \mathbb{Q}| = 4$.

Ezzel bebizonyítottuk az $x^4 - 10x^2 + 1$ polinom irreducibilitását $\mathbb{Q}$ felett.

AS2 4

Hogyan adható minimálpolinomot $\mathbb{Q}(\alpha)$-ban?

Mi lesz $\gamma = 1 + \sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$ minimálpolinomja?

Tudjuk: $\gamma \notin \mathbb{Q}$, de $\gamma \in \mathbb{Q}(\sqrt[3]{2}) \Rightarrow$

γ felett $\mathbb{Q}$ fölött > 1, és osztója 3-nak $\left(= |\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}|\right)$

$\Rightarrow \gamma$ minimálpolinomja 3-adfokú.

Ez azt jelenti, hogy $\exists\, a, b, c \in \mathbb{Q}$:

$$a + b\gamma + c\gamma^2 + \gamma^3 = 0 \quad \left(= 0 + 0\cdot\sqrt[3]{2} + 0\cdot\sqrt[3]{4}\right)$$

Itt γ^3 együtthatója 1, mivel tudjuk, a minimálpolinom 3-adfokú.

Fejtsük ki a bal oldalt:

$$a + b\gamma + c\gamma^2 + \gamma^3 = a + b + b\sqrt[3]{2} + c + 2c\sqrt[3]{2} + c\sqrt[3]{4} + 1 + 3\sqrt[3]{2} + 3\sqrt[3]{4} + 2 =$$

$$= (a + b + c + 3) + (b + 2c + 3)\sqrt[3]{2} + (c + 3)\sqrt[3]{4} = 0$$

Mivel a $\mathbb{Q}(\sqrt[3]{2})$ elemeinek a felírása egyértelmű $1, \sqrt[3]{2}$ és $\sqrt[3]{4}$ lineáris kombinációjaként, azért:

$$\begin{aligned} a + b + c &= -3 \\ b + 2c &= -3 \\ c &= -3 \end{aligned} \quad \Bigg| \quad \Rightarrow \begin{aligned} a &= -3 \\ b &= 3 \\ c &= -3 \end{aligned}$$

A minimálpolinom tehát: $f(x) = x^3 - 3x^2 + 3x - 3$

(Megjegyzés, azt tudhattuk is volna: $g(x) = x^3 - 2$-vel $f(x) = g(x-1)$.)

ASZ 4

Véges testek konstrukciója, szórás véges testekbe

Emlékeztető: K test: 1) $\operatorname{char} K = 0 \iff \forall a \in K^+$-re $o(a) = \infty$ v. $(a = 0)$

Vagy:

2) $\operatorname{char} K = p$ prím $\iff \forall a \in K^+$-re $o(a) = p$ v. $a = 0$

Más eset nincs.

Világos továbbá: $|K| < \infty \Rightarrow \operatorname{char} K = p$ valamely p prím.

Azt is tudtuk: $\operatorname{char} K = p \Rightarrow \mathbb{Z}_p \leq K$, hiszen az 1 által generált részteste $\cong \mathbb{Z}_p$.

Köv: K test, $|K| < \infty \Rightarrow \operatorname{char} K = p$ esetén $|K| = p^n$ valamilyen n-re.

(Tehát pl. $\nexists$ 6 elemű test)

Biz. Ha $\mathbb{Z}_p \leq K \Rightarrow K$ vektortér $\mathbb{Z}_p$ fölött; ha $\dim_{\mathbb{Z}_p} K = n \Rightarrow K \cong (\mathbb{Z}_p)^n$, és így $|K| = |\mathbb{Z}_p|^n = p^n$.

Tehát $\forall$ véges test elemszáma prímhatvány!

VIGYÁZAT! $\mathbb{Z}_p$ test, $\mathbb{Z}_{p^n}$ nem test, ha $n > 1$.

Hogy nézhet ki pl. a 4-elemű test? Létezik-e, hogy ilyen van?

Tétel: $\forall p$ prím, $\forall n \in \mathbb{N}$-re létezik $q = p^n$ elemű test, és ez izomorfia erejéig egyértelmű.

(A tételt nem bizonyítjuk, bár abból, ami most csinálunk, tkp. nem lenne nagyon nehéz.)

Jelölés: $\mathbb{F}_q$ a $q = p^n$ elemű test (ez egyértelmű). Tehát:

$\mathbb{F}_p \cong \mathbb{Z}_p$, ha p prím; de $\mathbb{F}_q \not\cong \mathbb{Z}_q$, ha q nem prím.

$\mathbb{F}_4$ szerkezete: $\mathbb{F}_2 \leq \mathbb{F}_4$, $\mathbb{F}_2$-nek egy bázisa $\mathbb{F}_2$ felett: 1.

Vegyük egy $\alpha \notin \mathbb{F}_2$ elemet $\mathbb{F}_4$-ből.

Ekkor mivel $\langle 1, \alpha \rangle = \mathbb{F}_4$, (↑ vektortér-generált) tehát $\{1, \alpha\}$ bázis $\mathbb{F}_4$-ben.

Ezzel: $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$

A vektortérbeli tétel megadja az összeadást $\mathbb{F}_4$-ben.

De tudjuk: $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ és $|\mathbb{F}_4 : \mathbb{F}_2| = \dim_{\mathbb{F}_2} \mathbb{F}_4 = 2$

$\Rightarrow$ $\deg_{\mathbb{F}_2} \alpha = 2$.

α minimálpolinomja tehát másodfokú irreducibilis.

Egyet ilyen $\mathbb{F}_2[x]$-beli polinom van: $f(x) = x^2 + x + 1$.

Ez tehát azt jelenti, hogy $\alpha^2 + \alpha + 1 = 0$, azaz $\alpha^2 = \alpha + 1$.

AS2 4

(Ne feledjük: akar $\mathbb{F}_4 = 2$, tehát $-(\alpha+1) = +(\alpha+1)$.)

Ez azt jelenti, hogy: 1) $\mathbb{F}_4$ elemit tudjuk $\mathbb{F}_2$-beliek szerint, mint vektorokat

2) α-hat is tudjuk gyakorlatilag szorzani.

$\Rightarrow$ kiszámolható a szorzótábla:

$(\mathbb{F}_4, \cdot)$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Itt:

$\alpha(\alpha+1) = \alpha^2 + \alpha =$

$= (\alpha+1) + \alpha =$

$= 1$

$(\alpha+1)(\alpha+1) = \alpha^2 + 1$

$= (\alpha+1) + 1$

$= \alpha.$

(Ebből kiderült: ha $\exists$, akkor $\mathbb{F}_4$ egyértelmű $\exists$.)

Másik példa: $\mathbb{F}_8$: $\mathbb{F}_2 \leq \mathbb{F}_8$, $\alpha \in \mathbb{F}_8 \setminus \mathbb{F}_2 \Rightarrow$

α 3-adfokú $\mathbb{F}_2$ fölött $\Rightarrow$ minimálpolinomja

$x^3 + x^2 + 1$ v. $x^3 + x + 1$

$\mathbb{F}_8 = \{ a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{F}_2 \}$ és

a szorzási szabály:

$\alpha^3 + \alpha^2 + 1 = 0$ vagy $\alpha^3 + \alpha + 1 = 0$

$\mathbb{F}_8 \setminus \mathbb{F}_2$-ben 3 elem minimálpolinomja $x^3 + x^2 + 1$,

másik 3 elemé pedig $x^3 + x + 1$ ($\Rightarrow \mathbb{F}_8$ is egyértelmű)