ALGEBRA ÉS SZÁMELMÉLET

7. előadás

Emlékeztető az előző órákról

- Algebrai és transzcendens számok
- algebrai számok minimálpolinomja; a minimálpolinom irreducibilitása
- algebrai szám foka: a minimálpolinom foka
- algebrai szám hatványainak függetlensége, ill. lineáris összefüggősége
- α algebrai, $\mathbb{Q}(\alpha)$ az α által generált résztest $\mathbb{C}$-ben
- $\mathbb{Q}(\alpha)$ elemei az α kis fokú polinomjai, ha α algebr.

Általánosabban:

- Testbővítések: $K \leq M$; testbővítés foka: $|M:K|$ – az az M dimenziója K fölött
- algebrai és transzcendens elemek K fölött; minimálpolinom K fölött; algebrai elem foka K fölött
- a K és α által generált résztest: $K(\alpha)$;
- $|K(\alpha):K| = \operatorname{gr} \alpha$, ha α algebrai; $K(\alpha)$ elemei az α kis fokú polinomjai.
- $|K(\alpha):K| = \infty$, ha α transzcendens K fölött
- Ha α algebrai, akkor $K(\alpha)$ minden eleme is algebrai K fölött; sőt: $|M:K|$ véges $\Rightarrow$ M minden eleme algebrai K fölött

$\boxed{\text{ASZ 4}}$ 7/2

$K(\alpha)$ szerkezete, ha α transzcendens K fölött

__Áll.:__ T. fel: $K \leq M$, $\alpha \in M$ transzcendens K fölött. Ekkor, ha $K(\alpha)$ az a legszűkebb résztest, mely tartalmazza K-t és α-t, ebben az esetben

$$K(\alpha) \cong K(x)$$

ahol $K(x)$ a $K[x]$ polinomgyűrű hányadosteste.

__Biz.__ Könnyen ellenőrizhető, hogy az

$$L = \left\{ \frac{f(\alpha)}{g(\alpha)} \in M \;\middle|\; f, g \in K[x],\ g \neq 0 \right\}$$

benne kell, hogy legyen $K(\alpha)$-ban, hisz K-val és α-val együtt minden test tartalmazza az $f(\alpha)$ és $g(\alpha)$ típusú számokat, sőt, az ilyenek hányadosait is. (Vegyük észre: $g \neq 0$ esetén $g(\alpha) \neq 0$, hisz α transzcendens K fölött.) Tehát $L \subseteq K(\alpha)$.

Másrészt az is ellenőrizhető, hogy L maga résztest M-ben: zárt a gyűrűműveletekre és a nem nulla elemekkel való osztásra. Így: $K(\alpha) \subseteq L$.

Ez azt jelenti, hogy $K(\alpha) = L$.

~~Másrészt~~ Ugyanakkor vegyük észre, hogy

$$\frac{f_1(\alpha)}{g_1(\alpha)} = \frac{f_2(\alpha)}{g_2(\alpha)}, \quad g_i(\alpha) \neq 0 \iff$$

$$f_1(\alpha) g_2(\alpha) = f_2(\alpha) g_1(\alpha) \iff$$

$$f_1(\alpha)g_2(\alpha) - f_2(\alpha)g_1(\alpha) = 0 \iff$$ (mivel α transzcendens)

$$f_1(x)g_2(x) - f_2(x)g_1(x) = 0 \iff$$

$$\frac{f_1(x)}{g_1(x)} = \frac{f_2(x)}{g_2(x)}$$

Vagyis létezik egy bijekció $K(\alpha) = L$ elemei és $K[x]$ hányadostestének elemei között, s ez a bijekció nyilván műveletttartó, tehát izomorfizmus a két test között. $\square$

Összefoglalva tehát:

Tétel: Legyen $K \leq M$, $\alpha \in M$.

1) Ha α algebrai K fölött, akkor

a) $K(\alpha) = \{ f(\alpha) \in M \mid f = 0 \text{ v. } gr f < gr_K \alpha,\ f \in K[x] \}$,

b) és $|K(\alpha) : K| = gr_K \alpha < \infty$,

c) továbbá $K(\alpha)$ minden eleme algebrai K fölött.

2) Ha α transzcendens K fölött, akkor

a) $K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \in M \mid f \in K[x], g \in K[x], g \neq 0 \right\}$

b) és $|K(\alpha) : K| = \infty$,

c) továbbá $K(\alpha)$ minden K-n kívüli eleme transzcendens K fölött.

Biz. Ebből már csak 2) c)-t nem bizonyítottuk, viszont ezt ellenőrizzük a fokszámtétel után.

Megjegyzés A fenti tétel elég jól leírja a $K(\alpha)$ típusú bővítések szerkezetét.

Def. 1) Az $M \geq K$ bővítést a K egyszerű bővítésének nevezzük, ha $\exists\, \alpha \in M$: $M = K(\alpha)$, azaz egyetlen elem hozzávételével generálható.

2) Ha $K \leq M$, és $H \subseteq M$, akkor $K(H)$ az a legszűkebb résztest, ami tartalmazza K-t is és H-t is.

Jel.: $H = \{\alpha_1, \alpha_2, \dots \alpha_n\} \Rightarrow K(H) = K(\alpha_1, \alpha_2, \dots \alpha_n)$.

($|H| = 1$ esetén a bővítés egyszerű.)

Megjegyzés: $K(\alpha_1, \dots \alpha_n) = K(\alpha_1)(\alpha_2) \dots (\alpha_n)$ könnyen igazolható.

Visszatérve a múlt előadásra, kimondtuk a fokszámtételt (vagy szorzástételt).

Tétel (Fokszámtétel): Legyen $K \leq L \leq M$. Ekkor:

$$|M:K| = |M:L| \cdot |L:K|$$

Biz. (A múltkor ez elmaradt).

a) Ha $|L:K| = \infty$, akkor $\exists\, l_1, l_2, \dots, l_n, \dots \in L$ végtelen sok elem, amelyek lineárisan függetlenek K fölött, s akkor mivel $l_i \in M$, így $\dim_K M = \infty$.

b) Ha $|M:L| = \infty$, akkor $\exists\, m_1, \dots, m_n, \dots \in M$

végtelen sok elem, amelyek lineárisan függetlenek L fölött. De $K \leq L$ miatt így nyilván K fölött is függetlenek $\Rightarrow |M:K| = \infty$.

c) Az érdekes eset tehát az, amikor

$|M:L| = m$, $|L:K| = l$ végesek.

Megmutatjuk, hogy $|M:K| = m \cdot l$.

Vegyünk ehhez egy $\alpha_1, \dots \alpha_m$ bázisát M-nek L fölött, és egy $\beta_1, \dots \beta_l$ bázisát L-nek K fölött.

Belátjuk, hogy $\{\alpha_i \beta_j \mid 1 \leq i \leq m, 1 \leq j \leq l\}$ bázisa M-nek K fölött. Ezzel $\dim_K M = m \cdot l$.

c1) $\{\alpha_i \beta_j \mid i, j\}$ generátorrendszer M-ben.

Ha ugyanis $\gamma \in M$, akkor mivel $\{\alpha_i\}$ bázis M-ben

$\exists \lambda_1, \dots \lambda_m \in L$: $\gamma = \lambda_1 \alpha_1 + \lambda_2 \alpha_2 + \dots + \lambda_m \cdot \alpha_m$.

Ugyanakkor $\lambda_i \in M$ miatt, mivel $\{\beta_j\}$ bázis L-ben:

$\exists \kappa_{i1}, \dots \kappa_{il} \in K$: $\lambda_i = \kappa_{i1} \cdot \beta_1 + \dots + \kappa_{il} \cdot \beta_l$.

Ez azt jelenti, hogy:

$$\gamma = (\kappa_{11} \beta_1 + \kappa_{12} \beta_2 + \dots + \kappa_{1l} \beta_l) \alpha_1 +$$
$$(\kappa_{21} \beta_1 + \kappa_{22} \beta_2 + \dots + \kappa_{2l} \beta_l) \alpha_2 + \dots$$
$$\vdots$$
$$\dots + (\kappa_{m1} \beta_1 + \kappa_{m2} \beta_2 + \dots + \kappa_{ml} \beta_l) \alpha_m$$

A szorzatokat felbontva azt kapjuk, hogy γ felírható az $\alpha_i \beta_j$ elemek K-együtthatós lineáris kombinációjaként.

Ezzel beláttuk, hogy generátorrendszert alkotnak K fölött.

c2) Most megmutatjuk, hogy az $\{\alpha_i \beta_j \mid i, j\}$ halmaz lineárisan független K fölött.

T. fel: $\sum_{i,j} \kappa_{ij} \alpha_i \beta_j = 0$ valamilyen $\kappa_{ij} \in K$ együtthatókkal. Csoportosítva a tagokat:

$$(\kappa_{11}\beta_1 + \kappa_{12}\beta_2 + \dots + \kappa_{1l}\beta_l)\alpha_1 +$$

$$(\kappa_{21}\beta_1 + \kappa_{22}\beta_2 + \dots + \kappa_{2l}\beta_l)\alpha_2 + \dots \quad = 0$$

Itt az α_i együtthatói L-beli elemek, tehát α_i-knek egy L-együtthatós lineáris kombinációját kapjuk. Mivel α_i-k lineárisan függetlenek az L fölött, ezért $\forall\, \alpha_i$ együtthatója 0, azaz:

$$\kappa_{11}\beta_1 + \kappa_{12}\beta_2 + \dots + \kappa_{1l}\beta_l = 0$$

$$\kappa_{21}\beta_1 + \kappa_{22}\beta_2 + \dots + \kappa_{2l}\beta_l = 0$$

$$\vdots$$

Itt viszont a β_j-knek K-együtthatós kombinációi szerepelnek, s mivel β_j-k lineárisan függetlenek K fölött, ezért $\forall\, i, j$: $\kappa_{ij} = 0$.

Ezzel a szorzattételt igazoltuk. $\square$

Emlékeztető: A szorzástétel következménye volt, hogy a K fölött algebrai elemek testet alkotnak L-ben. Spec. az algebrai számok $\mathbb{A}$-val jelölt halmaza szintén test.

Most megoldjuk a második adódó feladatot (csak a teljesség kedvéért).

Áll: Ha $K \leq M$, és $\alpha \in M$ transzcendens K fölött, akkor minden $\beta \in K(\alpha) \setminus K$ is transzcendens.

Biz. Tegyük föl: $\beta = \frac{f(\alpha)}{g(\alpha)}$, $g(\alpha) \neq 0$, $f, g \in K[x]$.

Ekkor $\beta \cdot g(\alpha) - f(\alpha) = 0$.

Ez azt jelenti, hogy α gyöke a $\beta \cdot g(x) - f(x)$ polinomnak; itt nyilván

$$h(x) = \beta \cdot g(x) - f(x) \in K(\beta)[x]$$

tehát h együtthatói $K(\beta)$-ból valók.

Megmutatjuk, hogy ha $\beta \notin K$, akkor $h(x) \neq 0$, így ilyenkor α algebrai $K(\beta)$ fölött.

Tudjuk ugyanis, hogy $g \neq 0$, így g-nek valamelyik együtthatója (pl. a k-adik: g_k) szintén nem 0. Jelölje f_k az $f(x)$ polinom k-adik együtthatóját.

Ekkor h-ban a k-adik együttható:

$h = \beta \cdot g(x) - f(x)$ miatt

$$h_k = \beta \cdot g_k - f_k$$

Ha $h_k = 0$ lenne, akkor $\beta = \frac{f_k}{g_k} \in K$ teljesülne ↯

Így beláttuk részletekben a következő bővítéssorozatot:

$$K \le K(\beta) \le K(\alpha)$$

Mivel $\beta \notin K$ esetén $K(\alpha)$ algebrai $K(\beta)$ fölött, ezért $|K(\alpha):K(\beta)| < \infty$.

MESE

Ha most $|K(\beta):K| < \infty$ is teljesülne, akkor

$$|K(\alpha):K| = |K(\alpha):K(\beta)| \cdot |K(\beta):K| < \infty \text{ lenne,}$$

ami azt jelentené, hogy α algebrai K fölött ↯.

Ezzel a $\beta \in K(\alpha) \setminus K$ transzcendenciáját beláttuk. □

A fokszámtétel néhány alkalmazása

Példa: 1a) $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$, mert $\sqrt[3]{2}$ foka 3, így

$\dim_K \mathbb{Q}(\sqrt[3]{2}) = 3$, viszont $\dim_K \mathbb{Q}(\sqrt{2}) = 2$, tehát

$$\mathbb{Q}(\sqrt[3]{2}) \not\subseteq \mathbb{Q}(\sqrt{2}).$$

Ekkor így nem teljesülne a fokszámtétel.

Viszont:

1b) $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$. Ha ez nem így lenne, akkor

$$? \quad \mathbb{Q} \le \mathbb{Q}(\sqrt{2}) \le \mathbb{Q}(\sqrt[3]{2}) \quad ? \text{ teljesülne.}$$

A két szélső test által nyert bővítés foka 3:

$$|\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}| = 3 = \underbrace{|\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}(\sqrt{2})|}_{?!?\ = 1{,}5\ ?!?} \cdot \underbrace{|\mathbb{Q}(\sqrt{2}):\mathbb{Q}|}_{=2} \quad ↯$$

2) Mennyi lesz $|\mathbb{Q}(\sqrt{2})(\sqrt[3]{2}) : \mathbb{Q}|$?

Tudjuk, hogy $\sqrt{2}, \sqrt[3]{2} \in \mathbb{Q}(\sqrt{2})(\sqrt[3]{2})$, így

$gr_{\mathbb{Q}}\sqrt{2},\ gr_{\mathbb{Q}}\sqrt[3]{2} \ \Big|\ |\mathbb{Q}(\sqrt{2})(\sqrt[3]{2}) : \mathbb{Q}|$, hiszen

$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt[3]{2})$, és

$\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt[3]{2})$.

Vagyis a keresett fokszám osztható 2-vel is, és 3-mal is. $\Rightarrow$ $|\mathbb{Q}(\sqrt{2})(\sqrt[3]{2}) : \mathbb{Q}|$ osztható 6-tal.

Ugyanakkor:

$$\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt[3]{2})}_{\text{a bővítés foka } \leq 6.}$$

a bővítés foka 2 — a bővítés foka ≤ 3] $\sqrt[3]{2}$ gyöke az $x^3 - 2$ polinomnak $\Rightarrow$ $gr_{\mathbb{Q}(\sqrt{2})}\sqrt[3]{2} \leq gr_{\mathbb{Q}}\sqrt[3]{2} = 3$.

a bővítés foka ≤ 6.

Vagyis a keresett fok 6.

Ebből mellesleg az is kijön, hogy $\sqrt[3]{2}$ nem írható $a + b\sqrt{2}$ alakban (de ezt már az előbb is láttuk).

<u>Megjegyzés:</u> Kicsit kellemetlen kezelni a $\mathbb{Q}(\alpha)(\beta)\ldots$ típusú bővítéseket. Meg lehet mutatni, hogy (nem biz.):

<u>Tétel:</u> $\alpha_1, \ldots \alpha_n \in \mathbb{C}$ algebrai $\mathbb{Q}$ fölött $\Rightarrow \exists \gamma \in \mathbb{C}$: $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\gamma)$, azaz $\mathbb{Q}$ $\forall$ véges alg. bővítése egyszerű!

$\boxed{\text{ASZ \# 4}}$ 7/10

3) Hányadfokú lesz $\sqrt[5]{4}$? Minimálpolinomja = ?

Könnyen látható, hogy $\sqrt[5]{4}$ nem racionális (hiszen a 4 nem ötödik hatvány, és a SZAT alkalmazható a szokásos módon).

Ugyanakkor $\sqrt[5]{4}$ gyöke az x^5-4 polinomnak $\Rightarrow$ foka ≤ 5. De az miért irreducibilis?

A Sch.-Eis.-kritérium nem alkalmazható (bár ezek $x-1$ helyettesítéssel alkalmazható lenne).

De ehelyett tekintsük az $\sqrt[5]{2}$ számot: ennek már biztosan minimálpolinomja az x^5-2 (irr. a S-E-krit. miatt).

Viszont: $\sqrt[5]{4} = \sqrt[5]{2}\cdot\sqrt[5]{2} \in \mathbb{Q}(\sqrt[5]{2})$, tehát

$$\mathrm{gr}_{\mathbb{Q}}(\sqrt[5]{4}) \mid \mathrm{gr}_{\mathbb{Q}}\sqrt[5]{2} = 5$$

Mivel $\sqrt[5]{4}$ nem racionális, ezért a foka $\neq 1 \Rightarrow$ csak 5 lehet.

Vegyük észre, hogy ezzel azt is bizonyítottuk, hogy x^5-4 irreducibilis $\mathbb{Q}[x]$-ben.

<u>Néhány további észrevétel az algebrai számokról</u>

<u>Áll.</u>: $z \in \mathbb{C}$ algebrai $\Longleftrightarrow$ $\mathrm{Re}\, z$, $\mathrm{Im}\, z$ algebrai.

<u>Biz.</u> $\Leftarrow$: Legyen $z = a + bi$. Tudjuk: i algebrai.

Ha a, b algebrai $\Rightarrow$ z is algebrai, hiszen algebrai számok összege, szorzata szintén algebrai.

$\Rightarrow$ T. fel: $z = a + bi$ algebrai. Ekkor

$\exists f(x) \in \mathbb{Q}[x]$, melyre $f(z) = 0$.

De ekkor $\overline{f(z)} = \overline{0}$, és $\overline{f(z)} = \bar{f}(\bar{z}) = f(\bar{z})$, hiszen

f együtthatói valósak. Így – ezt már régről

tudhattuk – ha z gyöke $f \in \mathbb{Q}[x]$-nek, akkor

$\bar{z}$ is gyöke. Így $\bar{z}$ is algebrai.

De akkor: $z + \bar{z} = 2a = 2 \cdot \mathrm{Re}\, z$ is algebrai,

$\Rightarrow$ $\mathrm{Re}\, z$ is algebrai.

Hasonlóképpen: $z - \bar{z} = 2bi = 2 \cdot (\mathrm{Im}\, z) \cdot i$ is algebrai,

és mivel $2i$ algebrai $\Rightarrow$ $\mathrm{Im}\, z$ is algebrai.

<u>Másodfokú bővítések</u>

Ha $f(x) = ax^2 + bx + c$, akkor f gyökei a megoldóképlet

alapján: $\alpha_{1,2} = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ (Feltehető: $f \in \mathbb{Z}[x]$.)

A másodfokú bővítései $\mathbb{Q}$-nak így $\mathbb{Q}(\alpha)$ alakúak, ahol

α a fenti alakban írható. Megmutatjuk, hogy

$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$ valamilyen d négyzetmentes egész számra.

Először tegyük meg az alábbi hasznos észrevételt:

<u>Áll.</u>: $\mathbb{Q}(\alpha_1, \alpha_2, \ldots \alpha_k, \ldots) = \mathbb{Q}(\beta_1, \beta_2, \ldots \beta_l, \ldots)$ $\Leftrightarrow$

$\alpha_i \in \mathbb{Q}(\beta_1, \ldots \beta_l, \ldots)$ és $\beta_j \in \mathbb{Q}(\alpha_1, \ldots \alpha_k, \ldots)$ $\forall i, j$.

<u>Biz.</u> $\Rightarrow$ nyilvánvaló.

$\Leftarrow$ $\alpha_i \in \mathbb{Q}(\beta_1, \ldots \beta_l, \ldots)$ $\forall i$-re $\Rightarrow \mathbb{Q}(\alpha_1, \ldots \alpha_k, \ldots) \subseteq$

$\subseteq \mathbb{Q}(\beta_1, \ldots, \beta_l, \ldots)$ hiszen az előbbi test a legszűkebb olyan test, ami tartalmazza α_i-ket, tehát benne van $\mathbb{Q}(\beta_1, \dots, \beta_k, \dots)$-ban.

A feltétel másik része biztosítja a másik irányú tartalmazást. □

Áll: $\mathbb{Q}\left(\frac{a+\sqrt{b}}{c}\right) = \mathbb{Q}(\sqrt{b})$, ha $a, b, c \in \mathbb{Z}$.

Biz. $\sqrt{b} \in \mathbb{Q}\left(\frac{a+\sqrt{b}}{c}\right)$, hiszen:

$$\alpha := \frac{a+\sqrt{b}}{c} \in \mathbb{Q}(\alpha), \quad c, a \in \mathbb{Q} \Rightarrow$$

$$c \cdot \alpha - a = \sqrt{b} \in \mathbb{Q}(\alpha).$$

Hasonlóképpen: $\frac{a+\sqrt{b}}{c} \in \mathbb{Q}(\sqrt{b})$ nyilvánvaló.

Így a test bővítés megegyezik. □

Végeredmény:

Áll: Legyen $b = c^2 d$, ahol d négyzetmentes, azaz különböző prímek szorzata. Ekkor:

$$\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{d})$$

Biz. $\sqrt{b} = c \cdot \sqrt{d}$, és ebből: $c \cdot \sqrt{d} \in \mathbb{Q}(\sqrt{b}) \Rightarrow$
$\sqrt{d} \in \mathbb{Q}(\sqrt{b})$.

Hasonlóan: $\sqrt{b} = c \cdot \sqrt{d} \in \mathbb{Q}(\sqrt{d})$

Így: $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{d})$. □

Ezzel beláttuk, hogy $\forall$ másodfokú bővítése $\mathbb{Q}$-nak $\mathbb{Q}(\sqrt{d})$ alakú, ahol $d \neq 1$ négyzetmentes egész szám. (Igazolható: ezek mind különbözőek).