6. előadás

Testelmélet

A továbbiakban is a számok alaptulajdonságaival foglalkozunk: elsősorban a komplex számtest elemeit vizsgáljuk, s az $\alpha \in \mathbb{C}$ számnak a racionális számokhoz való viszonyát elemezzük, de azért látni fogjuk az általános tárgyalásmód előnyeit is: ilyenkor olyan helyzeteket nézünk, amelyeknél egy szűkebb test résztestként benne van egy bővebb testben. Ezt nevezzük majd testbővítésnek.

Először tehát a $\mathbb{Q} \subseteq \mathbb{C}$ alaphelyzetet tekintjük át.

Algebrai és transzcendens számok

Def. $\alpha \in \mathbb{C}$ algebrai számnak nevezzük, ha $\exists f \in \mathbb{Q}[x]$ nem nulla polinom, melyre $f(\alpha)=0$, azaz α gyöke az f-nek. Az alg. számok halmaza: $\mathbb{A}$.

Megjegyzés: Ha α gyöke az $f \in \mathbb{Q}[x]$ polinomnak, akkor nyilván gyöke $\forall \frac{a}{b} \in \mathbb{Q}$ esetén az $\frac{a}{b} \cdot f(x)$ polinomnak is. Így nyugodtan fölhasználhatjuk az

f-beli együtthatók nevezőivel, s ily módon egy egész együtthatós nem 0 polinomot kapunk. Így minden algebrai szám gyöke egy $\mathbb{Z}[x]$-beli polinomnak is.

<u>Elnevezés:</u> Az algebrai számokat szokás úgy is megnevezni, hogy α <u>algebrai a $\mathbb{Q}$ test fölött.</u>

Ez a később bevezetendő kömyezetbe ad pontos megnevezést.

<u>Példák:</u> 1) $\forall \alpha \in \mathbb{Q}$ algebrai szám: α gyöke az $(x-\alpha) \in \mathbb{Q}[x]$ elsőfokú polinomnak.

2) $\sqrt{2}$ is algebrai: ez gyöke az x^2-2 polinomnak. Hasonlóképpen algebrai $\sqrt[5]{17}$ $(\rightsquigarrow x^5-17)$, vagy $\varepsilon = -\frac{1}{2} + \frac{\sqrt{3}}{2} \cdot i$ $(\rightsquigarrow x^3-1$, hiszen egy harmadik egységgyökről van szó$)$.

3) Általában nehéz megmutatni, hogy egy $\alpha \in \mathbb{C}$ nem algebrai. Ezeknek is van neve:

<u>Def.</u> $\alpha \in \mathbb{C}$ <u>transzcendens szám</u>, ha nem algebrai, azaz a nullapolinomon kívül egyetlen $f \in \mathbb{Q}[x]$ polinomnak sem gyöke.

Noha azt általában nehéz bebizonyítani egy számról, hogy algebrai-e vagy transzcendens (vannak máig eldöntetlen kérdések), azt könnyű belátni, hogy léteznek transzcendens számok, sőt, azok vannak „többségben":

<u>Tétel:</u> Létezik transzcendens szám, sőt, „majdnem minden" komplex szám transzcendens:

- az algebrai számok halmaza megszámlálható végtelen;
- a transzcendens számok halmazának számossága kontinuum

<u>Biz.</u> (vázlat, <u>azoknak, akik nem hallottak a különböző végtelen számosságokról</u>)

Megszámlálható végtelen: $\exists$ bijekció $\mathbb{N}$-nel

Kontinuum számosságú: $\exists$ bijekció $\mathbb{R}$-rel.

Megmutatható, hogy $\nexists$ $\mathbb{N} \to \mathbb{R}$ bijekció, így $\mathbb{N} \subseteq \mathbb{R}$ miatt azt mondjuk, hogy a megszámlálható végtelen kisebb, mint a kontinuum számosság.

Ismert: $\mathbb{N}$ megszámlálható végtelen számosságú

$\mathbb{Z}$ szintén (felsorolhatók az elemek: $0, 1, -1, 2, -2, 3, -3, \dots$)

$\mathbb{Q}$ szintén (táblázatba rendezhetők:

ELTE

$$\begin{array}{cccccc}
\frac{0}{1} & \frac{1}{1} & \frac{-1}{1} & \frac{2}{1} & \frac{-2}{1} & \cdots \\
\frac{1}{2} & \frac{-1}{2} & \frac{3}{2} & \frac{-3}{2} & \frac{5}{2} & \cdots \\
\frac{1}{3} & \frac{-1}{3} & \frac{2}{3} & \frac{-2}{3} & \frac{4}{3} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

Minden $\frac{a}{b}$ szerepel, ahol $(a, b) = 1$

Sorban leolvassuk az elemeket $\frac{0}{1}$-től indulva a bejelölt vonalak mentén.

Hasonlóan megmutathatjuk, hogy megszámlálhatóan végtelen sok első-, másod-, harmad- stb. fokú polinom van $\mathbb{Z}[x]$-ben, majd még egyszer alkalmazva a fenti trükköt: $\mathbb{Z}[x]$-nek megszámlálható sok eleme van.

MESE

Sőt: pl. az n-edfokú $\mathbb{Z}[x]$-beli polinomok $\mathbb{C}$-beli gyökeit az n-edik sorba sorbarendezve ugyanígy sorbarendezhetjük a gyököket, mint $\mathbb{Q}$ elemeit (ugyanúgy a „kígyózó" leolvasással), csak vigyázni kell, hogy ha egy α szám már szerepelt, azt a sorban átugorjuk.

Ez azt jelenti, hogy $\mathbb{A}$ megszámlálható.

Ugyanakkor $\mathbb{C}$ számossága kontinuum, tehát kell lennie transzcendens számnak. (Megmutatható: $\mathbb{C} \setminus \mathbb{A}$ számossága is csak kontinuum lehet.) □

Megjegyzés: Az előző gondolatmenet nem ad egyetlen transzcendens számot sem konkrétan. De bizonyították transzcendensek az alábbiak:

- π (nehezebb, de azért „emészthető")
- e (a transzcendencia bizonyítása megtalálható a Freud–Gyarmati-könyvben)
- $\sin n$ ($0 \neq n \in \mathbb{N}$; nem fokokban, hanem radiánban)
- $\lg n$ ($n \in \mathbb{N}$, $n \neq 10^k$)

Ugyanakkor algebrai számból sem ismerünk sokat, de „gyárthatunk":

1) α algebrai $\Rightarrow$ $-\alpha$ is algebrai

$f(\alpha) = 0$, $f(x) = a_n x^n + \dots + a_0$ $\rightsquigarrow$

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

esetén $g(-\alpha) = f(\alpha) = 0$. $\Rightarrow$ $-\alpha$ algebrai

2) α algebrai $\Rightarrow$ $\sqrt{\alpha}$, sőt $\sqrt[k]{\alpha}$ is algebrai ($k \in \mathbb{N}$)

$f(\alpha) = 0$; $g(x) = f(x^k)$ esetén $g(\sqrt[k]{\alpha}) = 0$

$\Rightarrow$ $\sqrt[k]{\alpha}$ algebrai

Később meg fogjuk mutatni, hogy algebrai számok összege, szorzata, hányadosa is algebrai. De már nem olyan egyszerű megtalálni azt a polinomot, aminek gyöke, mint fönt.

Milyen polinomoknak lesz gyöke egy algebrai szám?

Nyilván, ha: 1) $f(\alpha) = 0 \Rightarrow (fg)(\alpha) = 0$ bármely $g \in \mathbb{Q}[x]$-re.

2) $f(\alpha), g(\alpha) = 0 \Rightarrow (f \pm g)(\alpha) = 0$

Tetszőleges algebrai szám így végtelen sok polinomnak gyöke.

Def. Legyen $\alpha \in \mathbb{C}$ algebrai szám. Ekkor $0 \neq m_\alpha(x) \in \mathbb{Q}[x]$ az α minimálpolinomja, ha:

1) $m_\alpha(\alpha) = 0$ (azaz α gyöke m_α-nak)

2) $0 \neq f \in \mathbb{Q}[x]$-re: $f(\alpha) = 0 \Rightarrow \operatorname{gr} f \geq \operatorname{gr} m_\alpha$ (azaz m_α minimális fokú azon polinomok között, amelyeknek α gyöke)

3) $m_\alpha(x)$ normált (azaz a főegyütthatója 1).

Vegyük észre, hogy tetszőleges α algebrai számra $\exists m_\alpha$: azon polinomok között, melyeknek α gyöke, kiválasztható egy minimális fokút (1) és 2) teljesül), és ha nem normált, akkor leosztjuk a főegyütthatójával.

Igaz azonban az is, hogy a minimálpolinom egyértelmű:

Áll: m_α, n_α minimálpolinomja α-nak $\Rightarrow m_\alpha = n_\alpha$.

Biz: $\operatorname{gr}(m_\alpha - n_\alpha) < \operatorname{gr} m_\alpha$, de $(m_\alpha - n_\alpha)(\alpha) = 0$.

A 2)-es feltétel miatt $m_\alpha - n_\alpha = 0$.

Ennél egy kicsit erősebb állítást is mondhatunk:

Áll.: Legyen m_α az α minimálpolinomja, továbbá $f(x) \in \mathbb{Q}[x]$ olyan, hogy $\operatorname{gr} f = \operatorname{gr} m_\alpha$. Ekkor $\exists\, c \in \mathbb{Q}$, melyre: $f = c \cdot m_\alpha$.

Biz.: $f(x) = a_n \cdot x^n + \dots + a_0$ esetén $\frac{1}{a_n} \cdot f$ minimálpolinom, és az előbbiek szerint: $\frac{1}{a_n} f = m_\alpha$. □

Vagyis azon minimális fokú polinomok, ~~[illegible]~~ amelyeknek α gyöke, a minimálpolinom konstansszorosai.

Megjegyzés: Szokás a minimálpolinom definíciójából kihagyni a normáltságot. Ilyenkor a minimálpolinomok egymás konstansszorosai. (Néha esetleg mi is élünk ezzel a lehetőséggel.)

Valójában a minimálpolinom nemcsak a minimális fokúakat határozza meg az $f(\alpha) = 0$ feltételt ~~[illegible]~~ kielégítők közül, hanem az összeset

Áll.: Legyen $f \in \mathbb{Q}[x]$. Ekkor $f(\alpha) = 0 \iff m_\alpha \mid f$.

Biz.: $\Leftarrow$: Ez világos a korábbi megjegyzés alapján:

$$f(x) = m_\alpha(x) \cdot g(x) \implies f(\alpha) = m_\alpha(\alpha) \cdot g(\alpha) = 0 \cdot g(\alpha) = 0.$$

$\Rightarrow$: Osszuk el f-et maradékosan m_α-val:

$$f(x) = q(x)\cdot m_\alpha(x) + r(x),$$

ahol r foka $<$ gr m_α, vagy $r=0$.

De $f(\alpha)=0$, $m_\alpha(\alpha)=0 \implies r(\alpha)=0$.

Így a minimálpolinom def.-ja alapján $r=0$.

Tehát: $m_\alpha \mid f$. □

Megjegyzés: Az előző állítást α helyett egy A mátrixra és az A minimálpolinomjára is kimondhatjuk. Ugyanakkor a következő tulajdonsággal már nem rendelkezik egy mátrix minimálpolinomja.

Áll: Legyen $\alpha \in \mathbb{C}$ algebrai. Ekkor m_α irreducibilis ($\mathbb{Q}$ fölött).

Biz: Tegyük fel, hogy $m_\alpha(x) = f(x)\cdot g(x)$ nem triviális felbontás. Mivel $0 = m_\alpha(\alpha) = f(\alpha)\cdot g(\alpha)$, ezért vagy $f(\alpha)=0$, vagy $g(\alpha)=0$. Mivel azonban gr f, gr $g <$ gr m_α, ez ellentmondás.

Megj: A fenti érvelésnél kihasználtuk, hogy $\mathbb{C}$ nullosztómentes. Ez az, ami nem menne volna a négyzetes mátrixokra.

Jelen esetben viszont az irreducibilitás „perdöntő":

Áll.: Tegyük föl, hogy $f \in \mathbb{Q}[x]$-re és $\alpha \in \mathbb{C}$-re: $f(\alpha) = 0$. Ha f irreducibilis (és normált), akkor $f = m_\alpha$, azaz f a minimálpolinom.

Biz. Láttuk korábban: $m_\alpha \mid f$; ha f irreducibilis, akkor m_α nem lehet alacsonyabb fokú, és ekkor $\operatorname{gr} m_\alpha = \operatorname{gr} f$. Mivel mindkettő normált $\Rightarrow$ $m_\alpha = f$ a korábbi állítás szerint. $\square$

Def. α algebrai $\mathbb{C}$-ben $\mathbb{Q}$ fölött. Ekkor a minimálpolinom, azaz m_α fokát nevezzük az α algebrai száma fokának: $\operatorname{gr} \alpha = \operatorname{gr} m_\alpha$ (vagy $\deg \alpha = \deg m_\alpha$).

Példák: 1) $\alpha \in \mathbb{C}$-re: $\operatorname{gr} \alpha = 1 \iff \alpha \in \mathbb{Q}$, hiszen mindkét eset azt jelenti, hogy $m_\alpha(x) = x - \alpha$.

2) $\sqrt{2}$ foka 2: minimálpolinomja nem lehet elsőfokú, mert $\sqrt{2}$ nem racionális; de gyöke az $x^2 - 2$ polinomnak. Így spec. megkaptuk azt is, hogy $x^2 - 2$ irreducibilis $\mathbb{Q}[x]$-ben (ami kijönne a Sch.-Eis. kritériummal is). Ugyanakkor $\sqrt{72}$ minimálpolinomja $x^2 - 72$, és így az is irreduc., de nem alkalmazható a Sch.-Eis.

3) Legyen ε primitív n-edik egységgyök. Ekkor def. szerint ε gyöke a $\Phi_n(x)$-nek, az n-edik körosztási polinomnak.

Mivel tétel mondja ki, hogy $\Phi_n(x)$ irred. $\mathbb{Q}[x]$-ben (csak $n=p$-re bizonyítottuk), ezért $\Phi_n(x)$ az ε minimálpolinomja, és így $gr(\varepsilon) = \varphi(n)$.

<u>Megjegyzés:</u> A minimálpolinom irreducibilitása egy új irreducibilitási kritériumot szolgáltat általában: pl. x^2-72-re ez bizonyította a polinom felbonthatatlanságát.

<u>Emlékeztető:</u> A korábbiakban már foglalkoztunk az $a+b\sqrt{2}$ típusú számokkal, és időnként szükség volt arra, hogy:

$a, b, c, d \in \mathbb{Q}$ esetén:

$$a+b\sqrt{2} = c+d\sqrt{2} \iff a=c,\ b=d.$$

Ezt az állítást (vagy ehhez hasonlókat) általában könnyen bizonyítottuk. Most megmutatjuk általánosan, hogy ez miért igaz:

Tétel: Legyen $\alpha \in \mathbb{C}$ algebrai szám, $d = \mathrm{gr}\, \alpha$.

Ekkor: a) $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$ lineárisan függetlenek $\mathbb{Q}$ fölött,

b) $1, \alpha, \alpha^2, \dots, \alpha^{d-1}, \alpha^d$ lin. összefüggők $\mathbb{Q}$ fölött.

Biz. Legyen $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0 \in \mathbb{Q}[x]$ az α minimálpolinomja. Ekkor:

$$\alpha^d + a_{d-1}\alpha^{d-1} + \dots + a_1 \cdot \alpha + a_0 \cdot 1 = 0$$

mutatja b)-t.

Ugyanakkor, ha $1, \alpha, \dots, \alpha^{d-1}$ lineárisan öf. lenne, akkor $\exists\ \lambda_0, \dots, \lambda_{d-1} \in \mathbb{Q}$ (nem mind 0), hogy:

$$\lambda_0 + \lambda_1\alpha + \dots + \lambda_{d-1}\alpha^{d-1} = 0.$$

Ez viszont azt jelenti, hogy α gyöke az

$$0 \neq f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_{d-1}x^{d-1} \in \mathbb{Q}[x]$$

polinomnak, és $\mathrm{gr}\, f \leq d-1 < \mathrm{gr}\, m_\alpha$ ellentmondás.

Tehát az a)-t is igazoltuk. $\square$

Az előző esetre vonatkoztatva: $1, \sqrt{2}$ lin. ftlenek $\mathbb{Q}$ fölött, így bármely lin. kombinációknál az együtthatók egyértelműek.

Az előző analógiával tovább is mehetünk.
Bebizonyítottuk, hogy $\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}\le\mathbb{C}$ résztest $\mathbb{C}$-ben (valójában $\mathbb{R}$-ben is).
A bizonyításnál valószínűleg használtuk az osztálos, hogy tudtuk a nevezőt gyöktelenítani.
Most ezt is megcsináljuk általánosan.

<u>Tétel:</u> Legyen $\alpha\in\mathbb{C}$ algebrai szám. Ekkor, ha $\mathrm{gr}\,\alpha=d$:

$$R=\{a_0+a_1\alpha+\dots+a_{d-1}\alpha^{d-1}\in\mathbb{C} \mid a_i\in\mathbb{Q}\}$$

résztestet alkot $\mathbb{C}$-ben. Ez a legszűkebb olyan résztest, amely tartalmazza $\mathbb{Q}$-t is és α-t is, így a jele: $\mathbb{Q}(\alpha)$. („<u>α által generált bővítése $\mathbb{Q}$-nak</u>")
($\mathbb{Q}$-t egyébként minden résztest tartalmazza.)

<u>Biz.</u> 1) Vegyük először észre, hogy R az $1,\alpha,\dots\alpha^{d-1}$ által generált (d-dimenziós) altér $\mathbb{C}$-ben, tehát zárt az összeadásra.

2) Most megmutatjuk, hogy R zárt a szorzásra.
Ehhez világos módon elegendő megmutatnunk, hogy $\alpha^d,\alpha^{d+1},\dots\alpha^n,\dots\in R$ $\forall n$-re.
Ha $m_\alpha(x)=x^d+a_{d-1}\cdot x^{d-1}+\dots+a_0$ az α minimál-polinomja, akkor: $\alpha^d=-(a_{d-1}\alpha^{d-1}+\dots+a_0)\in R$.

Innen most már indukcióval léphetünk tovább:

ha $\alpha^n = \lambda_0\cdot 1 + \lambda_1\cdot\alpha + \dots + \lambda_{d-1}\alpha^{d-1}$, akkor

$$\alpha^{n+1} = \alpha\cdot\alpha^n = \alpha\cdot(\lambda_0\cdot 1+\dots+\lambda_{d-1}\alpha^{d-1}) =$$
$$= \lambda_0\cdot\alpha + \lambda_1\cdot\alpha^2+\dots+\lambda_{d-2}\cdot\alpha^{d-1} + \underbrace{\lambda_{d-1}\cdot\alpha^d}$$

Itt viszont az utolsó tagot ki tudjuk fejezni kis foki α-hatványok lineáris kombinációjaként, ezért $\lambda_{d-1}\cdot\alpha^d$ is R-ben van, s így az összeg is R-ben van.

Ezzel igazoltuk, hogy R részgyűrű.

3) Megmutatjuk végezetül, hogy tetszőleges R-beli, nullától különböző elemnek van reciproka R-ben.

Vegyük észre, hogy $\beta = a_0+\dots+a_{d-1}\alpha^{d-1}\in R$ pontosan akkor nem 0, ha az $f(x)=a_0+\dots+a_{d-1}x^{d-1}$ polinom nem 0, azaz valamelyik együttható $\neq 0$.

Mivel $m_\alpha(x)$ irreducibilis, és $\text{gr}\, m_\alpha > \text{gr}\, f$, ezért m_α és f relatív prímek.

A test fölötti polinomokra tanult euklideszi algoritmus alapján tudjuk, hogy ilyenkor $\exists\, p, q \in \mathbb{Q}[x]$ polinomok, melyekre:

$$p(x)\cdot m_\alpha(x) + q(x)\cdot f(x) = 1.$$

Ha most ide α-t helyettesítünk, akkor $m_\alpha(\alpha)=0$ miatt: $q(\alpha)\cdot f(\alpha)=1$, azaz $1=q(\alpha)$.
Itt viszont $q(\alpha)=b_0+b_1\alpha+\dots+b_k\cdot\alpha^k$ valamilyen k-ra, és a 2. rész miatt $q(\alpha)\in R$.
Ezzel beláttuk, hogy R-ben lehet osztani. $\square$

<u>Megjegyzés:</u> Az előző tétel tehát azt mondja ki, hogy ha $\mathbb{Q}(\alpha)$ az α által generált résztest, akkor minden elemet föl tudunk írni α-nak egy „kis" fokú polinomjaként („kis" fok = kisebb mint az α foka). Ebben bázist alkotnak: $1, \alpha, \dots \alpha^{d-1}$!

<u>Példa:</u> $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$ – ezt láttuk korábban

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

ennek az igazolása már nehezebb lenne (a bonyolultabb „gyöktelenítés" miatt), viszont most általánosan megkaptuk.

<u>Testbővítések</u>

Az eddig elmondottak alkalmazhatók általánosabb helyzetben is.

<u>Def.:</u> Egy M test a K test <u>bővítése</u>, ha K résztestre M-nek, azaz $K\subseteq M$, és a K-beli

műveletek az M-beli műveletek megszorításai.

A bővítés foka az M-nek mint K fölötti vektortérnek a dimenziója, jele: $|M:K|$.

Tehát: $|M:K| = \dim_K M$.

A korábbiakat most általánosan is végigcsinálhatjuk!

Def.: ∃ $K \leq M$ esetén:

a) $\alpha \in M$ algebrai a K fölött, ha $\exists\, 0 \neq f(x) \in K[x]$: $f(\alpha)=0$

b) $\alpha \in M$ transzcendens a K fölött, ha $\nexists\, 0 \neq f(x) \in K[x]$: $f(\alpha)=0$

c) $m_\alpha \in K[x]$ minimálpolinomja $\alpha \in M$-nek K fölött, ha: ~~[illegible]~~, $m_\alpha(\alpha)=0$, minimális fokú, normált.

d) $\alpha \in M$ foka a K fölött: $gr_K\,\alpha = gr\, m_\alpha$.

Áll: A minimálpolinom egyértelmű, irreducibilis K fölött, $f(\alpha)=0 \Leftrightarrow m_\alpha \mid f$ stb.

Áll: $gr_K\,\alpha = n \Rightarrow 1, \alpha, \dots, \alpha^{n-1}$ lin. függetlenek K fölött

Áll: Jelölje $K \leq M$, $\alpha \in M$ esetén $K(\alpha)$ a legszűkebb olyan résztestet, mely tartalmazza K-t, α-t. Ha α algebrai K fölött, akkor: $K(\alpha)=\{a_0+\dots+a_{d-1}\alpha^{d-1} \mid a_i \in K,\ d=gr_K\alpha\}$.

Az is igaz, hogy a $K(\alpha)$ bővítés foka K fölött: $|K(\alpha):K| = gr_K \alpha$.

<u>Megjegyzés:</u> Kényelmes a transzcendens elemek fokát K fölött végtelennek definiálni. Ekkor igaz az előbbi állítás:

<u>Állítás:</u> Legyen $K \leq M$, $\alpha \in M$, $K(\alpha)$ a legszűkebb résztest, ami tartalmazza K-t és α-t. Ekkor:

$$|K(\alpha):K| = gr_K \alpha.$$

<u>Biz.:</u> Most már csak azt kell bizonyítani, hogy

$$\alpha \text{ transzcendens} \implies |K(\alpha):K| = \infty,$$

hiszen az algebrai α esetét beláttuk.

De ha α transzcendens, akkor

$$1, \alpha, \alpha^2, \dots, \alpha^n, \dots \in K(\alpha)$$

és ezek lineárisan függetlenek (ellenkező esetben α gyöke lenne egy $f(x) \in K[x]$ polinomnak).

Így $\dim_K K(\alpha) = \infty$.

<u>Következmény:</u> $K \leq M$, $|M:K| = n < \infty$ véges. Ekkor M minden eleme algebrai K fölött. Speciálisan, ha α algebrai K fölött, akkor $\forall f, g \in K[x]$, $g(\alpha) \neq 0$-ra $f(\alpha)/g(\alpha)$ is algebrai K fölött.

Biz.: Ha $|M:K| < \infty$, akkor tetszőleges $\alpha \in M$-re

$K \leq K(\alpha) \leq M$, és így $\dim_K K(\alpha) \leq \dim_K M < \infty$.

Így α algebrai K fölött.

A speciális eset abból adódik, hogy $f(\alpha)/g(\alpha)$

benne van $K(\alpha)$-ba, ami a feltétel szerint

véges fokú. $\square$

Pl.: α algebrai K fölött $\Rightarrow \alpha^2, \frac{1}{\alpha}$ is algebrai K fölött

„Egymás utáni" bővítések esete

Mit mondhatunk a bővítések fokáról, ha több is van:

$K \leq L \leq M$

Tétel (Fokszámtétel, szorzástétel) Ha $K \leq L \leq M$, akkor

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

Ez vonatkozik arra az esetre is, ha valamelyik

bővítés foka ∞ (ilyenkor: $k \cdot \infty = \infty \cdot \infty = \infty$).

Biz. Legközelebb. Helyette

Következmény: α, β algebrai K fölött $\Rightarrow \alpha+\beta, \alpha \cdot \beta$,

α/β ($\beta \neq 0$ esetén) is algebrai K fölött.

Biz. T. fel: α, β algebrai K fölött, $\alpha \beta \in M$.

Ekkor: $|K(\alpha):K|$ véges, és $= \mathrm{gr}_K \alpha$.

Vegyük észre, hogy β algebrai K fölött $\Rightarrow$ alg. $K(\alpha)$

fölött is, és $\mathrm{gr}_K \beta \geq \mathrm{gr}_{K(\alpha)} \beta$.

Ezért: $|K(\alpha)(\beta):K(\alpha)|$ véges és $= gr_{K(\alpha)}\beta \le gr_K \beta$.

Így $|K(\alpha)(\beta):K|$ is véges a fokszámtétel miatt.

Ugyanakkor: $\alpha, \beta \in K(\alpha)(\beta) \Rightarrow \alpha+\beta, \alpha\cdot\beta, \alpha/\beta \in K(\alpha)(\beta)$

és az előbbiek miatt ezek is algebraiak. $\square$

<u>Következmény</u>: A K fölött algebrai elemek M-ben egy résztestet alkotnak. Spec. az algebrai számok halmaza, $\mathbb{A}$ résztestje $\mathbb{C}$-nek.

<u>Biz</u> Az előbb beláttuk, hogy algebrai elemek összege, szorzata, hányadosa szintén algebrai lesz. $\square$