# 1. Az algebrai számok teste

**Véges és algebrai bővítés.**

**Ismétlés (6.1.20, 6.2.4, 6.1.11)**
Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor *véges*, ha $\alpha$ *algebrai* $K$ fölött. A $K \leq L$ véges bővítés, ha $|L : K|$ véges. Ekkor $L$ minden eleme algebrai $K$ fölött. A $K \leq L$ *algebrai bővítés*, ha $L$ minden eleme algebrai $K$ fölött. Tehát minden véges bővítés algebrai.

**6.2.12. Tétel**
Az $L$-nek a $K$ fölött algebrai elemei résztestet alkotnak.

Speciálisan az algebrai számok $\mathbb{A}$ halmaza résztest $\mathbb{C}$-ben. Ez tehát az *algebrai számok teste*. A $\mathbb{Q} \leq \mathbb{A}$ bővítés algebrai (nyilván), de nem véges (HF).

**Fok bővebb test fölött.**

**6.2.5. Állítás**
Algebrai elem $k$-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$. Ekkor $\sqrt[k]{\alpha}$ gyöke az $s(x^k) \in K[x]$ nem nulla polinomnak. □

**6.2.8. Lemma**
Elem foka nagyobb test fölött nem nőhet. Vagyis $K \leq L \leq M$, $\alpha \in M$ esetén $\mathrm{gr}_L(\alpha) \leq \mathrm{gr}_K(\alpha)$.

Ha $s(x)$, illetve $t(x)$ az $\alpha$ minimálpolinomja $K$, illetve $L$ fölött, akkor $s \in L[x]$ és $s(\alpha) = 0$ miatt $t \mid s$. Így $\mathrm{gr}_L(\alpha) = \mathrm{gr}(t) \leq \mathrm{gr}(s) = \mathrm{gr}_K(\alpha)$. □

**Összeg és szorzat foka.**

**6.2.10. Következmény**
Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai $K$ fölött. Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén $\alpha/\beta$ is *algebrai* $K$ fölött, és fokuk legfeljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

**Bizonyítás**
$K \leq K(\alpha) \leq K(\alpha)(\beta)$ testlánc. A szorzástétel miatt
$|K(\alpha)(\beta) : K| = \mathrm{gr}_K(\alpha)\mathrm{gr}_{K(\alpha)}(\beta)$.
Láttuk, hogy $K \leq K(\alpha)$ miatt $\mathrm{gr}_{K(\alpha)}(\beta) \leq \mathrm{gr}_K(\beta)$.
Ezért $|K(\alpha)(\beta) : K| \leq \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.
De $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha)(\beta)$, így fokuk $\leq \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$. □

Így például $\sqrt[7]{3 - \sqrt[5]{23}} - \sqrt[4]{5 + i\sqrt{7 + \sqrt[6]{3}}}$ is algebrai szám.

**$\mathbb{A}$ algebrailag zárt.**

**6.2.13. Tétel**
Az algebrai számok $\mathbb{A}$ teste *algebrailag zárt*.

**Bizonyítás**
Legyen $0 \neq f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke $f$-nek. Belátjuk, hogy $\alpha$ algebrai szám. Mivel $a_j$ algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is. Ezért az $a_j$ elemekkel sorban bővítve mindegyik lépésben *véges* bővítést kapunk. Így $|\,\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}\,|$ véges. De $f(x) \in \mathbb{Q}(a_0, \ldots, a_k)[x]$, ezért $\alpha$ algebrai $\mathbb{Q}(a_0, \ldots, a_k)$ fölött. Tehát $|\,\mathbb{Q}(a_0, \ldots, a_k)(\alpha) : \mathbb{Q}\,|$ is véges. Beláttuk, hogy $\alpha$ eleme $\mathbb{Q}$ egy véges bővítésének. Ezért $\alpha$ algebrai szám.

**Algebrailag zárt testek.**

**Emlékeztető (2.5.3. Definíció)**
Egy $T$ test *algebrailag zárt,* ha minden nem konstans polinom gyöktényezőkre bomlik $T$ fölött.

Azt láttuk be, hogy minden $f \in \mathbb{A}[x]$ gyökei algebrai számok. Tudjuk analízisből, hogy $\mathbb{C}$ algebrailag zárt. Ezért $f$ gyöktényezőkre bomlik $\mathbb{C}$ fölött, és így $\mathbb{A}$ fölött is. □

Tehát a bizonyításban *kihasználtuk, hogy $\mathbb{C}$ algebrailag zárt!*

**2.5.18, 6.2.20, 6.4.6, NB**
Sem a $\mathbb{Q}$ véges bővítései, sem a véges testek nem algebrailag zártak, de minden testnek van algebrailag zárt bővítése. Ezért minden polinomnak számolhatunk formálisan a gyökeivel!

**Transzcendens számok.**

Konkrét számokról nehéz bizonyítani, hogy transzcendensek.

$\sum_{k=0}^{\infty} 10^{-k!}$ transzcendens (Liouville, 1851).
$e$ transzcendens (Hermite, 1873).
$\pi$ transzcendens (Lindemann, 1882).
$2^{\sqrt{3}}$ transzcendens. Általában: $\alpha^{\beta}$ transzcendens, ha
$\alpha$, $\beta$ algebrai, $\beta$ irracionális, $\alpha \neq 0, 1$ (Gelfond-Schneider, 1935).
$e + \pi$ transzcendens-e, racionális-e: *megoldatlan*.

Cantor (1874): *a valós számok döntő többsége transzcendens.* Ugyanis az algebrai számok *megszámlálható* halmazt alkotnak (fel lehet őket sorolni: $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$). A megszámlálható a „legkisebb lehetséges végtelen halmaz”, de a transzcendens számok halmaza nem megszámlálható.

# 2. Testbővítések konstrukciója

**Polinomok „nemlétező” gyökei.**

**Példa**
A $z^2+1$-nek nincs gyöke $\mathbb{R}$-ben, de $i$-vel kényelmes számolni. Ezért bevezettük $\mathbb{C}$-t, az $\mathbb{R}$ egy *testbővítését*. A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel, és $a+bi$-nek az $a+bx+(x^2+1)$ mellékosztály felel meg. Így az $a+(x^2+1)$ alakú mellékosztályok $\mathbb{R}$-rel izomorf résztestet alkotnak, az $i$-nek megfelelő elem $x+(x^2+1)$.

(2) *Definiáljuk* $\mathbb{C}$-t $\mathbb{R}[x]/(x^2+1)$-nek, és igazoljuk, hogy test.

(3) *Azonosítsuk* $a \in \mathbb{R}$-et $a+(x^2+1)$-gyel, és mutassuk meg, hogy ezek az elemek $\mathbb{R}$-rel izomorf résztestet alkotnak.

(4) *Definiáljuk* $i$-t $x+(x^2+1)$-nek, és lássuk be, hogy ez gyöke a $z^2+1$ polinomnak.

**Egyszerű testbővítés, mint faktorgyűrű.**

**6.4.1. Tétel**
Legyen $K \leq L$ testbővítés és $\alpha \in L$ egy $K$ fölött algebrai elem, melynek $K$ fölötti minimálpolinomja $s$. Ekkor $K(\alpha) \cong K[x]/(s)$. Az izomorfizmusnál $\alpha \leftrightarrow x+(s)$ és $k \in K$ esetén $k \leftrightarrow k+(s)$.

**Bizonyítás**
Legyen $\varphi : K[x] \to L$, $\varphi(f) = f(\alpha)$ az „$\alpha$ behelyettesítése”. A gyűrűk homomorfizmustétele miatt $\mathrm{Im}(\varphi) \cong K[x]/\mathrm{Ker}(\varphi)$.
Ekkor $f \in \mathrm{Ker}(\varphi) \iff f(\alpha)=0 \iff s \mid f$, így $\mathrm{Ker}(\varphi)=(s)$. Az $\mathrm{Im}(\varphi)$ az $f(\alpha)$ alakú elemek halmaza, ahol $f \in K[x]$. Ez tehát $\alpha$ „polinomjainak” halmaza, vagyis $K(\alpha)$. A homomorfizmustétel bizonyítása miatt az $\mathrm{Im}(\varphi) \cong K[x]/\mathrm{Ker}(\varphi)$ izomorfizmusnál $\varphi(f) \leftrightarrow f+(s)$. De $\varphi(x)=\alpha$, és $k \in K$ esetén $\varphi(k)=k$. □

**A faktorgyűrű mikor test.**

**5.2.9. Állítás**
Ha $T$ test és $f \in T[x]$, akkor a $T[x]/(f)$ faktorgyűrű akkor és csak akkor *test*, ha $f$ *irreducibilis* $T$ fölött.

**Bizonyítás**
Ha $f=gh$ nemtriviális felbontás, akkor $\big(g+(f)\big)\big(h+(f)\big)$ nulla, vagyis $T[x]/(f)$ nem nullosztómentes, és így nem is test.
Ha $f$ irreducibilis, akkor legyen $g \in T[x]$, ahol $g+(f)$ nem nulla. Azaz $f$ nem osztója $g$-nek, és mivel $f$ irreducibilis, $(f,g)=1$. Ezért $fp+gq=1$ alkalmas $p,q \in T[x]$ polinomokra. Innen $\big(g+(f)\big)\big(q+(f)\big)=1-fp+(f)=1+(f)$, hiszen $f \mid fp$ miatt $-fp+(f)$ nulla. Beláttuk tehát, hogy $q+(f)$ inverze $g+(f)$-nek, hiszen $1+(f)$ a $T[x]/(f)$ faktorgyűrű egységeleme. □

**Egyszerű testbővítés konstrukciója.**

**6.4.3. Tétel**
Ha $K$ test, és $s$ egy $K$ fölött irreducibilis polinom, akkor *létezik* olyan $L$ test, amelyben $K$ résztest, és amelyben az $s$ polinomnak már *van gyöke*.

**Bizonyítás**
Legyen $L = K[x]/(s)$, ez test, mert $s$ irreducibilis. A $k \mapsto k + (s)$ megfeleltetés nyilván művelettartó és injektív. Ezért a $k + (s)$ elemek ($k \in K$) a $K$-val izomorf résztestet alkotnak $L$-ben. Végezzük el a $k = k + (s)$ azonosítást (az azonosítás precíz részleteit lásd Kiss-jegyzet, 361. oldal). Legyen $\alpha = x + (s) \in L$. Be kell látni, hogy $\alpha$ gyöke $s$-nek. Ezzel a bizonyítást be is fejezzük majd.

**Gyök a bővítésben.**

**Bizonyítás (folytatás)**
Legyen $s(z) = k_0 + k_1 z + \ldots + k_n z^n \in K[z]$. Az $s$-et $L[z]$-beli polinomnak képzeljük, hogy $\alpha$-t helyettesíthessünk. Ezért $s$ együtthatói a ($k_j$-vel azonosított) $k_j + (s)$ elemek. Így $\alpha = x + (s)$ miatt $s(\alpha) =$
$= \big(k_0 + (s)\big) + \big(k_1 + (s)\big)\big(x + (s)\big) + \ldots + \big(k_n + (s)\big)\big(x + (s)\big)^n =$
$= k_0 + k_1 x + \ldots + k_n x^n + (s) = s + (s) = (s)$, vagyis a $K[x]/(s)$ faktorgyűrű nulleleme. Ezért $\alpha$ tényleg gyöke az $s$ polinomnak. □

A $\mathbb{Z}_2[x]/(x^2 + x + 1)$ négyelemű testben $E = 1 + (x^2 + x + 1)$, $0 = (x^2 + x + 1)$, $A = x + (x^2 + x + 1)$, $B = x + 1 + (x^2 + x + 1)$.
*Azonosítás:* $O \leftrightarrow 0$, $E \leftrightarrow 1$, $z^2 + z + 1 \leftrightarrow Ez^2 + Ez + E$. Az $\alpha = A$ elem tényleg gyöke $Ez^2 + Ez + E$-nek.

**Felbontási test.**

**6.3.2. Definíció**
$K \leq L$ testbővítés, ahol $L$ tartalmazza $0 \neq f \in K[x]$ *összes* gyökét:
$f(x) = c(x - \alpha_1)\ldots(x - \alpha_n)$, ahol $\alpha_i \in L$ és $c \in K$.
Ekkor $K(\alpha_1, \ldots, \alpha_n)$ az $f$ polinom *felbontási teste* $K$ fölött.

Az $f$ *összes* gyökéről beszélni *értelmetlen*: például $x^2 + 1$ gyökei nemcsak $\pm i$, hanem sok mátrix is. Ezt javítja ki a fenti gyöktényezős alakkal való megfogalmazás.

**6.4.5. Következmény**
Minden nem nulla polinomnak van felbontási teste.

Vázlat: a faktorgyűrűs konstrukcióval készíthetünk gyököket, mindig bővítve az alaptestet. Legfeljebb $\mathrm{gr}(f)$ lépésben vége.
*Algebrailag zárt bővítés:* ugyanez az összes polinomra (transzfinit eszközökkel).