1/3. 2014. szeptember 11.

10:15 – 12:00, kb. 11:00 – 11:15 szünet

2 ZH, szóbeli vizsga lesz, a vizsgán szívün közbe fog kérdezni, az anyag mély ismerete szükséges.

3-710a szoba, pelikan@cs.elte.hu. Bármi van, kérjetek.
Jegyzetelő, de a tanár úr se rossz. „Mindenkinek szabad tőlem engem, ha van hozzá bátorsága."
„Mindenkit megnyugtatok, hogy itt nem annyira ismert dolog lesz, és matekozni fogunk. NEM fogunk matekozni."

— o —

$\mathbb{R}$ – valós számok („azt gondoljátok, hogy ismertek.")
$\hookrightarrow$ nincs $x \in \mathbb{R}$, hogy $x^2 = -1$

Kreáció: $i^2 = -1$ imaginárius egység

$\longrightarrow$ $a + bi$ is lehet: komplex számok $(a, b \in \mathbb{R})$

Permanencia elv, a $\mathbb{R}$-ban megszokott számolást szeretnénk fenntartani

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

$$(a + bi) \cdot (c + di) = a \cdot c + bd \cdot i^2 + adi + bci = (ac - bd) + (ad + bc)i$$

$$\mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \}$$ Komplex számok

Probléma: ellentmondásmentes?
Ez nem precíz bevezetés! Olyan dolgokkal kell munkálkodni, amik biztos, hogy léteznek.

— o —

$\{(a; b) \mid a, b \in \mathbb{R}\}$ halmaz $(\mathbb{R} \times \mathbb{R})$

Def. $(a; b) + (c, d) = (a + c, b + d)$ „összeg"

Def. $(a, b) + (c, d) = (ac - bd, ad - bc)$ „szorzat"

Def. Test: K halmaz, K-n def. $+$ és $\cdot$ műveletek $\rightarrow (K, +, \cdot)$, $|K| \geq 2$
$+ : K \times K \rightarrow K$
$\cdot : K \times K \rightarrow K$
(Körper, Corps, $\rightarrow K$
field, nore $\rightarrow F$)

összeadás axiómái → az Abel-csoport axiómarendszere (pl. $(\mathbb{Z}_m, +)$)

A1:	$(a + b) + c = a + (b + c)$	$\forall a, b, c \in K$	asszociativitás
A2:	$a + b = b + a$	$\forall a, b \in K$	kommutativitás
A3:	$\exists\, 0 \in K\ \forall a \in K$	$a + 0 = 0 + a = a$	null
A4:	$\forall a \in K\ \exists (-a) \in K$	$a + (-a) = (-a) + a = 0$	ellentett elem / inverz

Állítás: A3-ban a 0 egyértelmű. (A3-ból levezetve)
B: Tfh. nem $\rightarrow$ $0_1, 0_2$
$0_1 + 0_2 = 0_2$ per def.
$0_1 + 0_2 = 0_1$ per def.
$\Big\}\ 0_1 = 0_2$ Q.E.D.

Állítás: A4-ben az ellentett elem egyértelmű.
B. Tfh. nem $\rightarrow$ a', a''
$(a' + a) + a'' \overset{A1}{=} a' + (a + a'')$
$0 + a'' = a' + 0 \implies a'' = a'$ Q.E.D.

szorzás axiómái:

$$\begin{cases} M1: & (ab)c = a(bc) & \forall a,b,c \in K & \text{associativitás} \\ M2: & ab = ba & \forall a,b \in K & \text{kommutatívitás} \\ M3: & \exists 1 \in K \quad \forall a \in K & 1\cdot a = a\cdot 1 = a & \text{egység} \\ M4: & \forall a \in K \quad \exists a^{-1} \in K & a\cdot a^{-1} = a^{-1}\cdot a = 1 & \text{inverz} \\ & a \neq 0 & & \end{cases}$$

disztributivitás axiómái:

$$\begin{cases} D1: & (a+b)c = ac + bc & \forall a,b,c \in K \\ D2: & a(b+c) = ab + ac & \forall a,b,c \in K \end{cases}$$

<u>Állítás.</u> $a \cdot 0 = 0 \cdot a = 0 \quad \forall a \in K$

B: $0 + 0 = 0$

$a(0+0) = a\cdot 0$ $\quad$ D2

$a\cdot 0 + a\cdot 0 = a\cdot 0$

$$\underbrace{(a\cdot 0 + a\cdot 0) + (-(a\cdot 0))}_{a\cdot 0 + \underbrace{(a\cdot 0 + (-(a\cdot 0)))}_{0}} = \underbrace{a\cdot 0 + (-(a\cdot 0))}_{0}$$

$\Rightarrow \quad a \cdot 0 = 0$ $\qquad$ Q.E.D.

<u>Állítás.</u> Ha M4-ben $a = 0$ lehet, akkor $|K| = 1$.

B: $a\cdot 0 = 0, \quad a\cdot 0 = 1 \quad \Rightarrow \quad 0 = 1 \quad \Rightarrow \quad \forall b \in K: b\cdot 1 = b\cdot 0$

$b = 0$

Q.E.D.

<u>Állítás.</u> $a, b \in K \qquad a, b \neq 0 \quad \Rightarrow \quad a\cdot b \neq 0$ $\qquad$ testben a szorzás nulloszt.mentes

B: Tfh. $ab = 0, \quad a \neq 0$

$\exists a^{-1}$

$a^{-1}(ab) = a^{-1}\, 0$

$(a^{-1}a)b = 0$

$1 \cdot b = 0$

$b = 0$ $\quad$ ↯ $\qquad$ Q.E.D.

Például test: $(\mathbb{R}, +, \cdot)$

$(\mathbb{Q}, +, \cdot)$

<u>Állítás.</u> $(\mathbb{C}, +, \cdot)$ test.

B: A1: $((a,b) + (c,d)) + (e,f) = (a,b) + ((c,d) + (e,f))$

$(a+c,\ b+d) + (e,f) = (a,b) + (c+e,\ d+f)$

$((a+c)+e,\ (b+d)+f) = (a+(c+e),\ b+(d+f))$

Egyenlőek, mert + asszociatív a valósokon. ✓

A2: nincs

A3: $0 = (0,0)$

A4: $-(a,b) = (-a,-b)$

M1: nincs

M2: nincs

M3: $(1;0)\cdot(a,b) = (1\cdot a - 0\cdot b,\ 1\cdot b + 0\cdot a) = (a,b)$ ✓

M4: $(a,b) \neq (0,0) \qquad (a,b)^{-1} = (a',b')$

$(a,b)\cdot(a',b') = (aa' - bb',\ ab' + a'b) = (1,0)$

$$\left.\begin{aligned} aa' - bb' &= 1 \\ ab' + a'b &= 0 \end{aligned}\right\} \quad \cancel{aa'b' - bb'b' = b'} \quad \cancel{aa'b' + a'a'b = 0} \quad \cancel{a'a'b + bb'b' = -b'}$$

$$\left.\begin{aligned} a^2a' - abb' &= a \\ abb' + a'b^2 &= 0 \end{aligned}\right\} \quad a^2a' + a'b^2 = (a^2+b^2)\cdot a' = a \rightarrow a' = \frac{a}{a^2+b^2}$$

$$\left.\begin{aligned} aba' - b^2b' &= b \\ a^2b' + aba' &= 0 \end{aligned}\right\} \rightarrow a^2b' + b^2b' = -b \rightarrow b' = \frac{-b}{a^2+b^2}$$

$$(a,b)\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \frac{1}{a^2+b^2}\left(a^2+b^2, ab-ab\right) = (1,0) \quad ✓ \qquad \text{QED.}$$

D1: nincs

D2: nincs

— o —

$i = (0,1)$

$i^2 = (0,1)\cdot(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1,0) \longrightarrow \underline{\underline{i^2 = -1}}$

$\{(a,0) \mid a \in \mathbb{R}\} \longrightarrow$ a valósszinak megfelelő viselkedés

$(a,0) + (b,0) = (a+b, 0)$

$(a,0)\cdot(b,0) = (ab, 0)$

$(a,0) \longleftrightarrow a$

$(a,b) = (a,0) + (0,b) = a + bi$

$(0,b) = \underbrace{(b,0)}_{b}\underbrace{(0,1)}_{i}$

„Visszaszereztük a becsületet ennek a jelölésnek."

$z = a + bi$ (Zahl)

<u>Def.</u> $\mathrm{Re}\, z = a$ valós rész (reális)

$\mathrm{Im}\, z = b$ képzetes rész (imaginárius)

<u>Def.</u> $\overline{z} = a - bi$ konjugált

$\mathrm{Re}(\overline{z}) = \mathrm{Re}(z)$, $\mathrm{Im}(\overline{z}) = -\mathrm{Im}(z)$

$\overline{\overline{z}} = z$

a konjug. +-ra, ·-ra műveletartó

$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ $\qquad a + c - bi - di = a - bi + c - di$ ✓

$\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$ $\qquad ac - bd - adi - bci = (a-bi)(c-di) =$

$= ac + bc - bci - adi$ ✓

<u>Áll.</u> $z = \overline{z} \iff z \in \mathbb{R}$

<u>Áll.</u> $\forall a, b \in K \quad \exists!\, x \in K \quad b + x = a$ „Kivonás"

B: $x = a + (-b)$ megfelel

$b + x = b + (a + (-b)) = b + ((-b) + a) = (b + (-b)) + a =$

$= 0 + a = a$ ✓ $\longrightarrow a + (-b)$ jó

$b + x = a$

$(-b) + (b + x) = (-b) + a$

$(-b + b) + x = (-b) + a$

$0 + x = x = a + (-b) \longrightarrow$ csak ez lehet az x QED.

Rövid jelölés: $a + (-b) \overset{def}{=} \underline{\underline{a - b}}$

Állítás. $\forall a, b \in K,\ b \neq 0 \Rightarrow \exists!\, y \quad by = a$ „osztás"

B: $y = a b^{-1}$ jó $\qquad a b^{-1} \overset{def}{=} \frac{a}{b}$

$b \cdot (a \cdot b^{-1}) = b \cdot (b^{-1} \cdot a) = (b \cdot b^{-1}) \cdot a = 1 \cdot a = a$ ✓ jó

$$b \cdot y = a$$
$$b^{-1}(b \cdot y) = b^{-1} \cdot a$$
$$(b^{-1} \cdot b) y = b^{-1} \cdot a$$
$$1 \cdot y = a \cdot b^{-1}$$
$$y = a \cdot b^{-1} \longrightarrow \text{csak ez lehet}$$

QED.

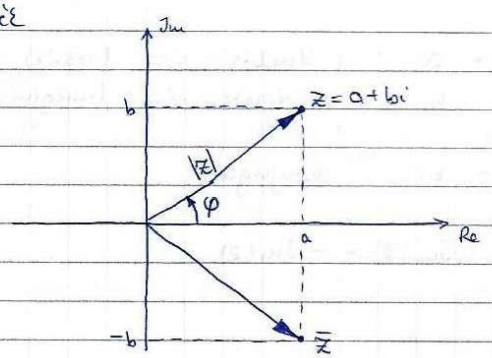
$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{-ad+bc}{c^2+d^2} i$$

$$\frac{1}{c+di} = \frac{c}{c^2+d^2} + \frac{-d}{c^2+d^2} \cdot i$$

$z + \bar{z} = 2 \operatorname{Re} z$

$z \cdot \bar{z} = (a+bi)(a-bi) = a^2 + b^2 \geqslant 0$

Def. $|z| = \sqrt{z \cdot \bar{z}} = \sqrt{a^2+b^2}$ abszolút érték



Gauss-féle számsík

$z = a + bi \longleftrightarrow (a; b)$ pont

sík $\longleftrightarrow \mathbb{C}$

A valósok továbbra is a számegyenesen.

Konjugálás: Re-re tükrözés.

2014. szeptember 18. írásbeli

Def. $\varphi = \arg(z)$ z argumentuma

$\arg z$ nem egyértelmű: $\pm 2k\pi$ hozzáadható (Szokás: $0 \leq \varphi < 2\pi$ vagy $-\pi < \varphi \leq \pi$)

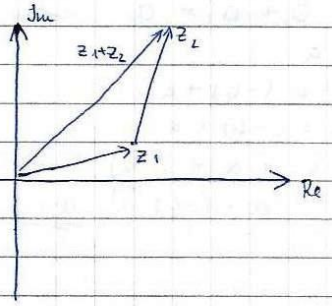
Állítás. $|z_1 z_2| = |z_1||z_2|$

B: Nemnegatívok: $\Leftrightarrow \quad |z_1 z_2|^2 = |z_1|^2 |z_2|^2$

$$z_1 z_2 \overline{z_1 z_2} = z_1 \overline{z_1}\, z_2 \overline{z_2}$$
$$z_1 z_2 \overline{z_1}\, \overline{z_2} = z_1 z_2 \overline{z_1}\, \overline{z_2}$$

QED.

Állítás. $|z_1 + z_2| \leqq |z_1| + |z_2|$



B: $z_1 + z_2 = (a+c) + (b+d) i$

$(a; b) + (c; d) = (a+c; b+d)$

Háromszög-egyenlőtlenség.

QED.

$(=) \Leftrightarrow z_1$ és z_2 vektora egy egyenesre esik és azonos irányú

$\Leftrightarrow z_2 = c \cdot z_1 \quad (c \in \mathbb{R},\ c \geqslant 0)$

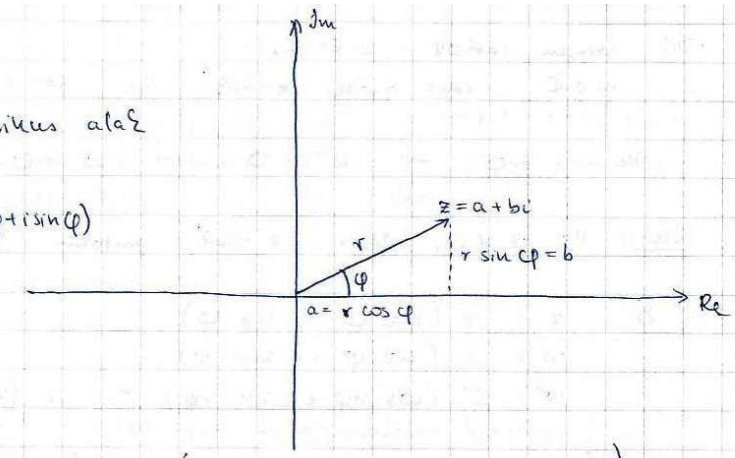
$z = a + bi \qquad |z| = r$

$z = r \cdot \underbrace{(\cos\varphi + i \sin\varphi)}_{\text{abs. érték } \cos^2\varphi + \sin^2\varphi = 1}$ trigonometrikus alak

$|z| = |r| \cdot 1 = r$ ✓

szöge φ ✓

$\Big\}\ a + bi = r(\cos\varphi + i\sin\varphi)$



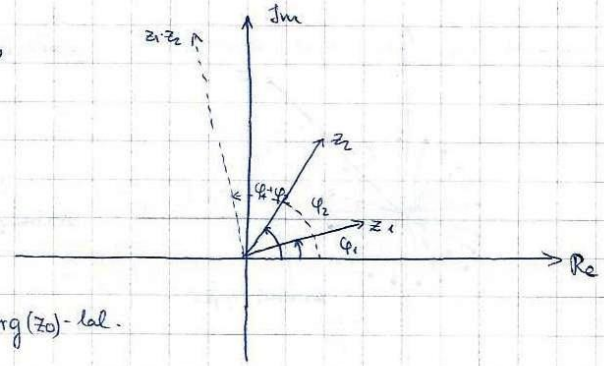
$z_1 = r_1(\cos\varphi_1 + i \sin\varphi_1)$

$z_2 = r_2(\cos\varphi_2 + i \sin\varphi_2)$

$\rightarrow z_1 \cdot z_2 = r_1 \cdot r_2 \cdot \big((\cos\varphi_1 \cos\varphi_2 - \sin\varphi_1 \sin\varphi_2) + i(\sin\varphi_1 \cos\varphi_2 + \cos\varphi_1 \sin\varphi_2)\big) =$

$= r_1 \cdot r_2 \cdot (\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2)) \rightarrow$ ez is trig. alak

Forgatva nyújtás: forgatás φ-vel, nyújtás az origóból r-vel.

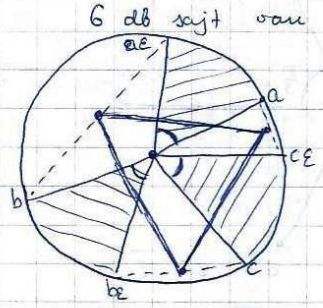


Geometriai transformációk ($z_0 \in \mathbb{C}$)

- $z \mapsto z + z_0$ eltolás $\vec{z_0}$-lal
- $z \mapsto z \cdot z_0$ forgatás $\arg z_0$-lal, nyújtás $|z_0|$-lal

Ha $|z_0| = 1 \rightarrow$ origó körüli forgatás $\arg(z_0)$-lal.

<u>Feladat.</u> Tegyük fel, hogy vásárolunk egy dobozt macskósajtot. 6 db sajt van a dobozban, de 3-at kiettünk belőle. Szalamfelezés → bbe. szab. Δ



Origó: a középpont, legyen a sajtok sugara 1.

A csúcsok: $a \quad b \quad c$

$a\varepsilon \quad b\varepsilon \quad c\varepsilon$

A felezőpontok: $\frac{a\varepsilon + b}{2}, \frac{b\varepsilon + c}{2}, \frac{c\varepsilon + a}{2}$

Belátjuk, hogy az oldalak 60°-kal egymásba forgathatók.

$\frac{c + b\varepsilon - b - a\varepsilon}{\cancel{2}} \cdot \varepsilon \overset{?}{=} \frac{a + c\varepsilon - b - a\varepsilon}{\cancel{2}}$

$a(-\varepsilon^2) + b(\varepsilon^2 - \varepsilon) + c \cdot \varepsilon = a(1 - \varepsilon) + b(-1) + c \cdot \varepsilon$ ✓

$\varepsilon = \cos\frac{\pi}{3} + i \sin\frac{\pi}{3} =$

$= \frac{1}{2} + i \cdot \frac{\sqrt{3}}{2}$

$\varepsilon^3 = -1$

$\varepsilon^3 + 1 = 0$

$(\varepsilon + 1)(\varepsilon^2 - \varepsilon + 1) = 0$

$\Rightarrow \varepsilon^2 - \varepsilon + 1 = 0$

$1 - \varepsilon = -\varepsilon^2$

$\varepsilon^2 - \varepsilon = -1$

<u>Moivre-formula.</u>

$$\boxed{\begin{aligned} z &= r(\cos\varphi + i \sin\varphi) \\ z^n &= r^n(\cos n\varphi + i \sin n\varphi) \qquad n \geq 1 \end{aligned}}$$

Def. Legyen adott $z \in \mathbb{C}$.
$w \in \mathbb{C}$ n-edik gyöke z-nek, ha $w^n = z$. $(n \in \mathbb{N}_{\geq 1})$

Ha $z = 0 \rightarrow w^n = 0 \rightarrow w = 0$.

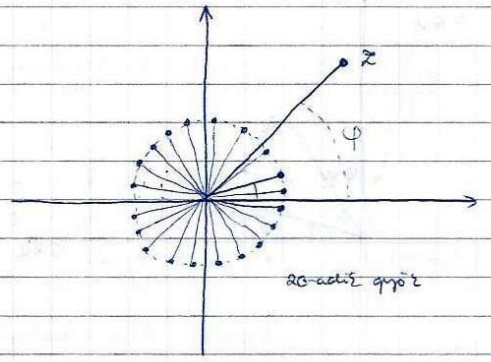
Tétel. Ha $z \neq 0$, akkor z-nek pontosan n darab n-edik gyöke van $(n \geq 1)$.

B: $z = r(\cos\varphi + i\sin\varphi)$
$w = s(\cos\psi + i\sin\psi)$
$w^n = s^n(\cos n\psi + i\sin n\psi) = r(\cos\varphi + i\sin\varphi)$

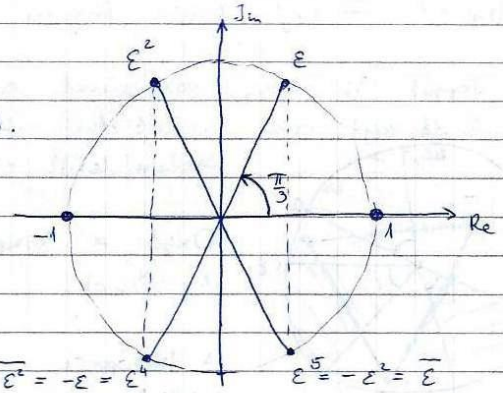
$$\begin{cases} s^n = r \\ n\psi = \varphi + 2k\pi \quad (k \in \mathbb{Z}) \end{cases} \longrightarrow \psi = \frac{\varphi}{n} + k \cdot \frac{2\pi}{n} \quad (k = 0, 1, \dots, n-1)$$

↪ különbözőek mod 2π

$s = \sqrt[n]{r}$ egyértelmű, mert poz. valós



szabályos n-szög csúcsai



Def. z n-edik egységgyök, ha $z^n = 1$.

Ilyenből n db van, az egyik az 1.
-1 párosadik egységgyök.

Def. z primitív n-edik egységgyök, ha $z^n = 1$, de $z^k \neq 1$, ha $1 \leq k < n$.
(n-re lesz először a hatványa 1.)

Minden n-re van: pl. $\varepsilon_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$
$\overline{\varepsilon_n}$ is.

Állítás. ε_n^l primitív n-edik egységgyök $\Leftrightarrow (n; l) = 1$.

B: $(\varepsilon_n^l)^k = \varepsilon_n^{lk} = 1 \Leftrightarrow n \mid lk$
Ha $(n; l) = 1 \Rightarrow n \mid k$. ✓
Ha $(n; l) \neq 1 \Rightarrow (n; l) = d \Rightarrow k = \frac{n}{d}$ -re már 1.

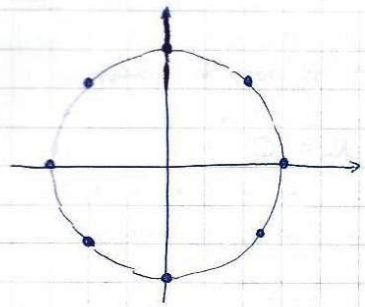
Tehát $\varphi(n)$ darab primitív n-edik egységgyök van.

Def. Euler-féle fi-függvény: $\varphi(n) = \left|\{l \mid 1 \leq l \leq n, (l; n) = 1\}\right|$.

n	$\varphi(n)$
1	1
2	1
3	2
4	2
5	4
6	2

Állítás. A komplex n-edik egységgyökök összege 0, ha $n \geq 2$. ($n=1$-re 1.)

Biz.:



Forgassuk el az ábrát $\frac{2\pi}{n}$-nel! ($n \geq 2$-re $\frac{2\pi}{n} \not\equiv 2\pi$)
A vektorok egymásba mennek át $\rightarrow$ az összeg invariáns.
Tehát az összegvektor csak $\underline{0}$ lehet.

QED.

Biz. II. $1 + \varepsilon + \varepsilon^2 + \ldots + \varepsilon^{n-1} = \dfrac{\varepsilon^n - 1}{\varepsilon - 1}$ (ez igaz, testaxiómából következhetik)

$\varepsilon^n = 1 \Rightarrow 0$ ✓ ($n \geq 2$-re értelmes csak)

QED.

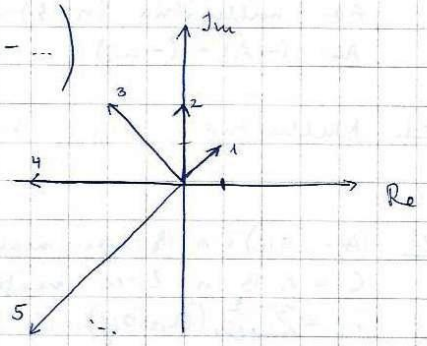
Feladat ⊛ Mi a primitív n-edik egységgyökök összege? (Válasz: $\mu(n)$, ahol μ a Möbius-fgv.)

Feladat. $\binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \ldots = ? \quad \sum_{k=0}^{[n/2]} \binom{n}{2k} (-1)^k$

$$(1+i)^n = \binom{n}{0} + \binom{n}{1} \cdot i + \binom{n}{2} i^2 + \binom{n}{3} i^3 + \ldots + \binom{n}{n-1} i^{n-1} + \binom{n}{n} i^n =$$

$$= \left(\binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \ldots\right) + i\left(\binom{n}{1} - \binom{n}{3} + \binom{n}{5} - \ldots\right)$$

$$1 + i = \sqrt{2}\left(\cos\frac{\pi}{4} + i \sin\frac{\pi}{4}\right)$$



$$\mathrm{Re}\,(1+i)^n = \binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \ldots =$$

$$= 2^{\frac{n}{2}} \cos\left(\frac{n\pi}{4}\right) = \begin{cases} 0 & n \equiv 2 \ (4) \\ \sqrt{2}^{n+1} & n \equiv 1 \ (8) \\ -2\sqrt{2}^{n+1} & n \equiv 3 \ (8) \\ -4\sqrt{2}^{n} & n \equiv 4 \ (8) \\ -4\sqrt{2}\sqrt{2}^{n} & n \equiv 5 \ (8) \\ -8\sqrt{2}\sqrt{2}^{n} & n \equiv 7 \ (8) \\ \sqrt{2}^{n} & n \equiv 0 \ (8) \end{cases}$$

$(1+i)^n = \sqrt{2}^n \left(\cos\frac{n\pi}{4} + i \sin\frac{4\pi}{4}\right)$

Tehát $\mathrm{Re}\,(1+i)^n = 2^{n/2} \cdot \cos\left(\frac{n\pi}{4}\right)$

— ∘ —

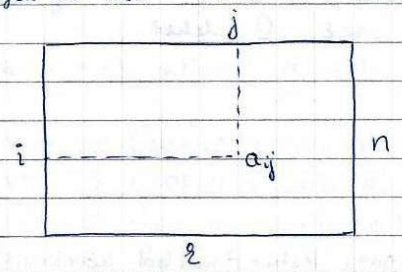
2014. szeptember 25.

szerda

2014. szeptember 25. szerda

Mátrixok

Def. Legyen K test. $n \times k$-as mátrix K felett $(n, k \geq 1)$ $\rightarrow$ n sor, k oszlop.



Ha más nem mondunk, $K = \mathbb{C}$.

Def. $A = (a_{ij})$, $B = (b_{ij})$ $n \times k$-as mátrixokra $C = A + B$ $n \times k$-as mátrix, $C = (a_{ij} + b_{ij}) = (c_{ij})$

$$\begin{pmatrix} 5 & -2 & 0 \\ 7 & 1 & -8 \end{pmatrix} + \begin{pmatrix} -3 & 4 & 72 \\ 8 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 72 \\ 15 & 1 & -9 \end{pmatrix}$$

A1 — A4 teljesülnek a mátrixösszeadásra

A1, mert az elemekre + asszociatív

A2, —"— + kommutatív

A3: nullmátrix $(n \times k)$-as

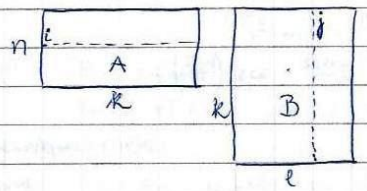
A4: $(-A) = (-a_{ij})$

Def. Nullmátrix: $\forall i,j : a_{ij} = 0$ $\quad A = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$

Def. $A = (a_{ij})$ $n \times k$-as mátrix, $B = (b_{ij})$ $k \times l$-es mátrix.

$C = A \cdot B$ $n \times l$-es mátrix, $C = (c_{ij})$

$c_{ij} = \sum_{t=1}^{k} (a_{it} b_{tj})$ $\rightarrow$ sor-oszlop szorzat.



M1 — M4 teljesülnek?

M1: asszociativitás teljesül: $(AB)C = A(BC)$ $\quad A: n \times k$, $B: k \times l$, $C: l \times m$

Biz.: $AB: n \times l$, $(AB)C: n \times m$ $\quad$ A szorzat létezik és azonos méretűek. ✓

$BC: k \times m$, $A(BC): n \times m$

$(AB)_{is} = \sum_{t=1}^{k} a_{it} b_{ts}$ $\qquad (BC)_{tj} = \sum_{s} b_{ts} c_{sj}$

$((AB)C)_{ij} = \sum_{s=1}^{l} \left(\sum_{t=1}^{k} a_{it} b_{ts} \right) c_{sj}$ $\qquad (A(BC))_{ij} = \sum_{t} a_{it} \left(\sum_{s} b_{ts} c_{sj} \right)$

$\rightarrow \sum_{\substack{1 \leq t \leq k \\ 1 \leq s \leq l}} a_{it} b_{ts} c_{sj} \leftarrow$

a ⊂ D.

M2 kommutativitás nem teljesül

Elvre csak így érdemes nézni, ha két $n \times n$-es mátrixot szorzunk

Ha véletlenül $AB = BA$ mégis, ettől A és B felcserélhetők.

$A = \begin{pmatrix} 3 & -8 \\ 8 & 11 \end{pmatrix}$ $\quad B = \begin{pmatrix} -2 & 5 \\ 0 & 32 \end{pmatrix}$ $\quad AB = \begin{pmatrix} -6 & -241 \\ -16 & 392 \end{pmatrix}$

$BA = \begin{pmatrix} 34 & 71 \\ 256 & 352 \end{pmatrix}$

M3: van egység megfelelő szorzás

<u>Def.</u> $M_n(K)$: a K feletti $n \times n$-es mátrixok halmaza.

Ezen belül az összeadás megvan, A1–A4 igaz, szorzás van, $\cdot$ assoc.

Egység.

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

főátlójában 1-ek, máshol 0

(1 a K-beli egységelem, 0 a nullelem)

$$I A = A I = A, \quad \forall A \in M_n(K)$$

M4: általában nincs inverz

<u>Def.</u> Négyzetes mátrix: $n \times n$-es mátrix $(n \in \mathbb{N})$

D1, D2 teljesül (nincs számolás)

<u>Def.</u> gyűrű: $(R, +, \cdot)$ $\quad + : R \times R \to R$, $\quad \cdot : R \times R \to R$ (der Ring, ring, anneau, кольцо)

A1 – A4 teljesül

M1 teljesül

D1 – D2 teljesül

$\Rightarrow$ $M_n(K)$ mindig gyűrű, de $n \geq 1$ -re nem test.

Minden test gyűrű.

Pl. $\mathbb{Z}$ gyűrű

<u>Tétel.</u> $M_n(K)$ nem nulloszt̀ómentes $n > 1$-re.

Van olyan elem, hogy $A \neq 0$, ~~de~~ $A^2 = 0$. (tehát A nilpotens), $A \in M_2(K)$

<u>Def.</u> $a \in R$ nilpotens elem, ~~ha $a \neq 0$, de~~ $\exists\, n \geq 1$, hogy $a^n = 0$.

$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $\quad A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$$\begin{array}{c|cc|cc} & & & 0 & 1 \\ & & & 0 & 0 \\ \hline A & 0 & 1 & 0 & 0 \\ & 0 & 0 & 0 & 0 \end{array} \quad B$$

Tehát nem csak nulloszt̀ó van, de nilpotens elem is.

n-re pl. $\begin{pmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 \end{pmatrix}$ nilpotens.

Példák gyűrűre: $\mathbb{Z}$, testek, $M_n(K)$ $\longrightarrow$ van bennük egység

Van mindig egység? nem, pl. páros számok gyűrűje.

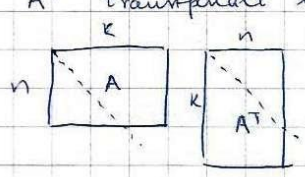
Van-e minden n-re n elemű test? nincs

Van-e minden n-re n elemű gyűrű? igen, pl. $\mathbb{Z}_n$ (ez véges, kommutatív, egységelemes)

$M_n(R)$ is gyűrű minden R gyűrűre

A $n \times k$-as mátrix $\to$ $k \times n$-es

<u>Def.</u> A^T transzponált $k \times n$-es mátrix, $A^T = (c_{ij})$, $\forall i, j$: $a_{ij} = c_{ji}$



Tétel. $(A+B)^T = A^T + B^T$, ha A, B $n \times k$-as mátrixok

B: triviális

Állítás. $(A \cdot B)^T = B^T A^T$ A $n \times k$, B $k \times l$-es mátrix

B: nincs

} a transzponálás művelettartó (majdnem)

Def. $A \in M_n(R)$ szimmetrikus, ha $A = A^T$.

$$A = \begin{pmatrix} 1 & 3 & 5 \\ 3 & 2 & 4 \\ 5 & 4 & 3 \end{pmatrix} = A^T \quad B = \begin{pmatrix} -2 & 8 & 5 \\ 8 & 1 & -1 \\ 5 & -1 & 4 \end{pmatrix} = B^T$$

$A \cdot B$		$B \cdot A$	
$-2\ 8\ 5$		$1\ 3\ 5$	
$8\ 1\ -1$		$3\ 2\ 4$	
$5\ -1\ 4$		$5\ 4\ 3$	
$1\ 3\ 5$		$-2\ 8\ 5$	
$3\ 2\ 4$	29	$8\ 1\ -1$	33
$5\ 4\ 3$		$5\ -1\ 4$	

Szimm. mátrixok szorzata nem mindig (általában nem) felcserélhető.

$(A\,B)^T = B^T A^T = B \cdot A \overset{?}{=} A \cdot B$ Két szimm. mátrix szorzata szimm. $\Leftrightarrow$ felcserélhető.

Megjegyzés. O, I szimmetrikus.

Def. $\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}$ diagonális mátrix (eleve négyzetes).

Megjegyzés. Diagonális mátrix szimmetrikus.

Def. Skalármátrix: $a_{11} = \dots = a_{nn} = a$, diagonális is. $\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix}$

Def. Skalárral való szorzás: $c \in R$

$A = (a_{ij})$

$c \cdot A = (c \cdot a_{ij})$

$\Rightarrow$ skalármátrix: $a \cdot I$ $(a \in R)$

— o —

Permutációk

Definíció. H halmaz önmagára való kölcsönösen egyértelmű leképezése (bijekció).

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$$

$$a \cdot b = ab$$

Permutációk kompozíciója / szorzata is permutáció.

$$3 = 1a = (1)a = a(1) = 1^a$$

Def. $\alpha(a \cdot b) = (\alpha a) \cdot b$ α elem, a és b permutációk.

balról jobbra olvassuk ki ($b(a(\alpha))$ - b jobbról balra kell)

Def. G csoport $(G, \cdot)$ $\quad \cdot : G \times G \to G$

G1: $(ab)c = a(bc) \quad \forall a, b, c \in G$

G2: $\exists e \in G \quad ae = ea = a \quad \forall a \in G$

G3: $\forall a \in G \ \exists a^{-1} \in G : \quad aa^{-1} = a^{-1}a = e$

A testek, gyűrűk $+$-ra csoportot alkotnak.
0-tól különböző testben $\cdot$-ra csoport.

Def. n elem összes permutációja: S_n: n-edfokú szimmetrikus csoport
(Nem n-edrendű!)

Megjegyzés. $|S_n| = n!$

Állítás.
S_n valóban csoport: G1 ✓, G2: identitás, G3: $a^{-1} = \begin{pmatrix} 3 & 1 & 4 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$ DEF.
„feje tetejére állítás"

Ciklusok

2014. 10. 02.

Def. Egy permutáció ciklus, ha $a_1 \to a_2 \to \dots \to a_k \to a_1$ a megfeleltetés ($i, j \in \{1, \dots, k\}$-ra $a_i \neq a_j$)
másképp leírva $(a_1 a_2 \cdots a_k)$ vagy $\begin{pmatrix} a_1 & a_2 & \cdots & a_k & b_1 & \cdots & b_{n-k} \\ a_2 & a_3 & \cdots & a_1 & b_1 & \cdots & b_{n-k} \end{pmatrix}$

Def. (ij) 2 hosszúságú ciklus, más néven transzpozíció.

Állítás. Minden permutáció felírható diszjunkt ciklusok szorzataként lényegében egyértelműen.

B: Induljunk el valamelyik $\bullet$-ból.

Előbb-utóbb visszatérünk egy korábbi pontba. Ez csak az 1. lehet.
Így kiválasztottunk egy ciklust. Ha van még kimaradó pont, abból kiindulva is kiválasztható egy másik ciklus, ami nyilván diszjunkt az előzőtől. Ezt folytatva a ciklusok előállnak.
Az egyértelműségben csak a sorrendek számítanak (a ciklusoké és a ciklusokon belül). □

Pl: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} = (1\,2\,5\,4)(3)$

Mj: Az 1 elemű ciklust nem szokás kiírni. Identitás konvenció szerint: $(1)(2)\cdots(n) = (1)$.

Állítás. Minden permutáció előáll transzpozíciók szorzataként.

B: Elegendő ciklusokra igazolni.
$(1\,2\,3 \cdots k) = (1\,2)(1\,3)\cdots(1\,k)$ könnyen ellenőrizhető □
$= (k, k-1)(k-1, k-2)\cdots(2\,1)$ → nem egyértelmű.

Kérdés. Egyértelmű-e legalább a felíráshoz használt permutációk száma?
Nem: $(1\,2) = (1\,2)(1\,3)(3\,1)$;
$(i\,j)^2 = (1)$.

Állítás. $\pi = (a_1 b_1)(a_2 b_2)\cdots(a_k b_k) = (c_1 d_1)(c_2 d_2)\cdots(c_l d_l) \Rightarrow k \equiv l \pmod 2$.

B: $f(x_1, \dots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)$ polinom

alkalmazzuk ezekre a változókra π-t:
$x_1 \to x_1\pi$
$x_2 \to x_2\pi$
$\vdots \qquad \vdots$
$x_n \to x_n\pi$

Ezen a módon újabb polinomot kapunk. $f^\pi(x_1, \dots, x_n) = \pm f(x_1, \dots, x_n)$, mert
$\forall$ tényező ± 1-szeresére változik a szorzatban.

Tekintsük a $\pi = (st)$ spec. esetet, ahol $1 \le s < t \le n$.
Ekkor csak az s-et és t-t tartalmazó tényezők változnak.
Minden páratlan sok előjelváltozást jelent, tehát ha π transzpozíció, $f^{\pi}(\dots) = -f(x_1, \dots, x_n)$
A feltevés szerint $f^{\pi} = (-1)^k f = (-1)^l f \Rightarrow k = l \mod 2$. $\square$

<u>Def.</u> $\pi \in S_n$ páros, ha ps sok tr. pcs. szorzataként írható fel.,
páratlan, ha pt sok tr. pcs szorzataként írható fel.

<u>Állítás.</u> $n \geqslant 2$-re a permutációk fele páros, fele páratlan. (A páros permutációk csoportot alkotnak: A_n: az n-edfokú alternáló csoport.)
B: Vegyünk egy rögzített páratlan permutációt.
Ezzel a párosakat végigszorozva rendre páratlanokat kapunk, amik különböznek.
$\Rightarrow \# pt \geqslant \# ps$.
Ugyanez fordítva $\Rightarrow \# ps \geqslant \# pt$.
$\Rightarrow \# pt = \# ps$. $\square$

Példák csoportra.: $(K, +)$
$(K \setminus \{0\}, \cdot)$
mod n maradékosztály
} kommutatív csoportok (Abel-csoportok)
S_n $n \geqslant 3$-ra nem komm.
$(12)\cdot(13) = (123)$, $(13)(12) = (132)$

<u>Def.</u> Elem rendje csoportban: $a \in G$-re $o(a)$ a legkisebb pozitív egész, melyre $a^{o(a)} = 1$ ($o(a) = \infty$ is lehet).
Véges csoportban $o(a)$ mindig véges: $\exists i < j : a^i = a^j \to 1 = a^{i-j}$
Ellenőrizhető, hogy $1 = a^0, a^1, \dots, a^{o(a)-1}$ különböznek.

Determinánsok

<u>Def.</u> $A \in M_n(K)$ determinánsa $\det(A) \in K$
Veszünk n elemet, hogy bmely 2 eltérő sorban és oszlopban legyen, tehát az oszlopindexek a sorindexek egy permutációja.
Ezt végezzük el $\forall$ lehetséges módon és vegyük az n tényező szorzatát.
Ha az adott permutáció pt, negatív, ha ps, pozitív előjellel összegezzük:

$$\det A = \sum_{\pi \in S_n} \pm a_{1k_1} a_{2k_2} \cdots a_{nk_n} = \sum \pm a_{i_1 j_1} \cdots a_{i_n j_n}$$

Másképp: legyen egy permutációban az inverziók száma annyi, ahányszor egy elem megelőz egy kisebbet. Az inv.-k száma = a paritással.

$$\det A = \sum_{\pi \in S_n} (-1)^k a_{1k_1} \cdots a_{nk_n}$$, ahol k az inv.-k száma π-ben.

Mj: végig pozitív előjellel A permanense: $\mathrm{per}(A)$.

Tulajdonságok

① $\det A = \det A^T$

Természetes, csak az indexeket cseréljük. [1]

② A-ban van 0 sor $\Rightarrow \det A = 0$ [2]

③ A két sorát felcserélve $A' \Rightarrow \det A' = -\det A$ [3]

Ez épp egy tr. pozícióval való szorzás.

④ A két sora egyenlő $\Rightarrow \det A = 0$

B: 3. tul. következménye: felcseréljük 2 sorát $\Rightarrow \det A = -\det A$

Ez hibás bizonyítás!

$\Updownarrow$ $a = -a \Rightarrow a = 0$ nem $\forall K$ testben igaz! 2014. 10. 09. csütörtök

$2a = 0$ Ebből csak akkor következik, hogy $a = 0$, ha $2 \neq 0$.

Pl. a mod 2 test:

+	0	1
0	0	1
1	1	0

–

·	0	1
0	0	0
1	0	1

Van más ilyen test is.

Általánosan: $1 \in K$, mennyi $o(1)$ Kodlitív csoportjában: $(K; +)$?

$\underbrace{1 + 1 + 1 + \ldots + 1}_{n} = 0$

Def. Test karakterisztikája: $\mathrm{char}(K) = o(1)$.

Pl. $\mathrm{char}(\mathbb{R}) = \infty$

Áll. $\mathrm{char}(K)$ vagy ∞, vagy prím.

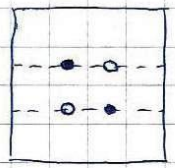
B. Tfh. $\mathrm{char}(K) \neq \infty$ $\quad o(1) = n = k \cdot l$, $k, l > 1$

$\underbrace{(1 + 1 + \ldots + 1)}_{k}\underbrace{(1 + 1 + \ldots + 1)}_{l}$ $\quad \lightning \Rightarrow n$ prím □

Pl. $\mathbb{F}_2(x) = \left\{ \frac{f(x)}{g(x)} \,\middle|\, f, g \in \mathbb{F}_2[x] \right\} \rightarrow 1 + 1 = 0$ továbbra is $\rightarrow \mathrm{char}(\mathbb{F}_2(x)) = 2$, ∞ test.

Tehát 4.-re adott bizonyítás csak $\mathrm{char}\, K \neq 2$ esetén jó.

B_2: (Ez már jó lesz.)



Ugyanaszon tagok, de ellentétes előjellel $\rightarrow$ kiesik. [4]

⑤ Determináns egy sorát szorozva $c \in K$-val $\rightarrow$ a det értéke szorozódik c-vel. [5]

⑤' $\Rightarrow \det(cA) = c^n \cdot \det(A)$ [5']

⑥ (lemma) Ha egy mátrix i-edik sorában $\forall$ elem egy 2 tagú összeg, akkor a det. felírható 2 det összegeként, ahol az egyikben az összegek 1., a másikban a 2. tagjai szerepelnek.

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a'_{i1} + a''_{i1} & \cdots & a'_{in} + a''_{in} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a'_{i1} & & a'_{in} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a''_{i1} & \cdots & a''_{in} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}$$

B: disztributivitás a definícióban. $\boxed{E}$

(7.) Egy det. értéke nem változik, ha valamelyik sorokat hozzáadjuk egy másik sor c-szeresit. $(c \in K)$

B: i-edik sor: $a_{i1} + c a_{j1}$; $a_{i2} + c a_{j2}$; $\dots$; $a_{in} + c a_{jn}$

(6) szerint ez 2 det. összege.

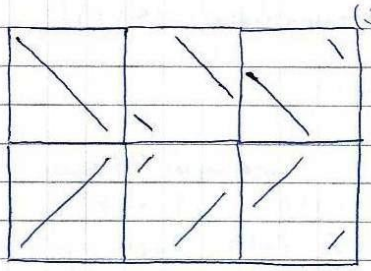
(5) szerint c kiemelhető

(4): 2 sor egyenlő: a második det 0. $\boxed{7}$

Kiszámolás

$\underline{2 \times 2}$: $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$

$\underline{3 \times 3}$: $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \underbrace{a_{11} a_{22} a_{33}}_{(0)} + \underbrace{a_{12} a_{23} a_{31}}_{(2)} + \underbrace{a_{13} a_{21} a_{32}}_{(2)} - \underbrace{a_{13} a_{22} a_{31}}_{(3)} - \underbrace{a_{11} a_{23} a_{32}}_{(1)} - \underbrace{a_{12} a_{21} a_{33}}_{(1)}$



(+) → Sarrus-„szabály"

(−)

Tétel. (Kifejtési tétel) $A = (a_{ij})_{i,j=1}^{n} \in M_n(K)$

$\det(A) = a_{i1} \cdot A_{i1} + a_{i2} \cdot A_{i2} + \dots + a_{in} A_{in}$ i-edik sor szerinti kifejtés

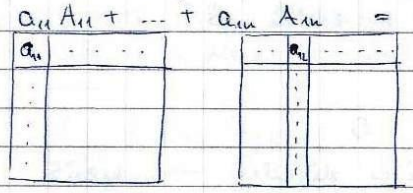
D_{ij} = az a ~~mátrix~~ det., amiből elhagyjuk az i. és j. sort → $(n-1) \times (n-1)$-es mátrix

$A_{ij} = (-1)^{i+j} D_{ij}$ → előjeles aldeterminánsok

$$\begin{vmatrix} + & - & + & - & \dots \\ - & + & - & + & \dots \\ + & - & + & \dots & \\ - & + & \dots & & \end{vmatrix}$$

B: Először bizonyítjuk $i = 1$-re.

$a_{11} A_{11} + \dots + a_{1n} A_{1n} = \det A$



a_{11} semmivel nem áll inv-ban (+)

az 1. oszloppal inverzió (−)

... → $i = 1$-re ✓

Általános i-re: csere $(i-1; i)$, $(i-2; i-1)$; $\dots$; $(1; 2)$ → $i-1$ sorcsere, ekkor az i-edik sor az 1. → elhagyható $\square$

Tétel. (ferde kifejtés)

$$a_{i1} A_{j1} + a_{i2} A_{j2} + \dots + a_{in} A_{jn} = 0 \qquad (i \neq j)$$

B:

$$\begin{array}{c} \\ i \\ j \\ \\ \end{array} \begin{vmatrix} & & \\ a_{i1} & \dots & a_{in} \\ a_{i1} & \dots & a_{in} \\ & & \end{vmatrix}$$

Írjunk a j-edik sor helyére az i-edik sort! Ekkor az új determináns kifejtése a fenti. De ebben a det-ban 2 sor azonos → 0. $\square$

Def. alsó mátrix: $a_{ij} = 0$, ha $i < j$.

Ha A alsó Δmátrix $\rightarrow$ $\det A = \prod_{i=1}^{n} a_{ii}$, mert $\forall$ más ~~elem~~ tag 0.

Def. felső Δmátrix $a_{ij} = 0$, ha $i > j$

Ha A felső Δmátrix $\rightarrow$ $\det A = \prod_{i=1}^{n} a_{ii}$

Ha A diag. mátrix $\rightarrow$ alsó és felső is $\rightarrow$ $\det A = \prod_{i=1}^{n} a_{ii}$

Ha $A = aI$ skalármátrix $\rightarrow$ $\det A = a^n$

$\det I = 1$

Feladat.

$$\begin{vmatrix} 1^2 & 2^2 & 3^2 & \cdots & n^2 \\ 2^2 & 3^2 & 4^2 & \cdots & (n+1)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n^2 & (n+1)^2 & (n+2)^2 & \cdots & (2n+1)^2 \end{vmatrix} = ?$$

$a_{ij} = (i+j-1)^2$

$n = 2$: $\begin{vmatrix} 1 & 4 \\ 4 & 9 \end{vmatrix} = -7$

$n = 1$: $|1| = 1$

Sarrus

$$n = 3: \begin{vmatrix} 1 & 4 & 9 \\ 4 & 9 & 16 \\ 9 & 16 & 25 \end{vmatrix} = \underbrace{1\cdot 9\cdot 25 + \underbrace{4\cdot 16\cdot 9 + 4\cdot 16\cdot 9}_{72\cdot 16 = 1152}}_{1377} - \underbrace{\underbrace{9\cdot 9\cdot 9}_{729} - \underbrace{25\cdot 4\cdot 4}_{400} - \underbrace{16\cdot 16\cdot 1}_{256}}_{-1385} = \underline{\underline{-8}}$$

Másképp:

$$\begin{vmatrix} 1 & 4 & 9 \\ 4 & 9 & 16 \\ 9 & 16 & 25 \end{vmatrix} = \begin{vmatrix} 1 & 4 & 9 \\ 0 & -7 & -20 \\ 0 & -20 & -56 \end{vmatrix} = 1 \cdot \begin{vmatrix} -7 & -20 \\ -20 & -56 \end{vmatrix} = 392 - 400 = \underline{\underline{-8}}$$

„4-re már mindenki látja, hogy így fogjuk csinálni. Nem, nem, így fogjuk csinálni."

$$n = 4 \quad \begin{vmatrix} 1^2 & 2^2 & 3^2 & 4^2 \\ 2^2 & 3^2 & 4^2 & 5^2 \\ 3^2 & 4^2 & 5^2 & 6^2 \\ 4^2 & 5^2 & 6^2 & 7^2 \end{vmatrix} = \begin{vmatrix} 1^2 & 2^2 & 3^2 & 4^2 \\ 3 & 5 & 7 & 9 \\ 7 & 7 & 9 & 11 \\ 7 & 9 & 11 & 13 \end{vmatrix} = \begin{vmatrix} 1^2 & 2^2 & 3^2 & 4^2 \\ 3 & 5 & 7 & 9 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{vmatrix} = 0$$

$(k+1)^2 - k^2 = 2k+1$

$n \geq 4$-re ezt meg lehet csinálni $\rightarrow$ $\det = 0$

Feladat.

$$\underset{n \times n}{\begin{vmatrix} a & b & b & \cdots & b \\ b & a & b & \cdots & b \\ b & b & a & \cdots & b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdots & a \end{vmatrix}} = \begin{vmatrix} a & b & b & \cdots & b & b \\ b-a & a-b & 0 & \cdots & 0 & 0 \\ 0 & b-a & a-b & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a-b & 0 \\ 0 & 0 & 0 & \cdots & b-a & a-b \end{vmatrix} = \begin{vmatrix} a+(n-1)\cdot b & (n-1)b & (n-2)b & \cdots & 3b & 2b & b \\ 0 & a-b & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & a-b & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & a-b & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & a-b \end{vmatrix} = (a-b)^{n-1} \cdot [a + (n-1)b]$$

Itt kellett a számolás, mert az eredmény nem annyira plausibilis.

$n = 2$: $\begin{vmatrix} a & b \\ b & a \end{vmatrix} = a^2 - b^2 = (a-b)\cdot(a+b)$

$n = 3$ $\quad (a-b)^2 \cdot (a+2b)$ $\quad \begin{vmatrix} a & b & b \\ b & a & b \\ b & b & a \end{vmatrix} = a^3 + 2b^3 - 3ab^2 = (a-b)^2 (a+2b)$

Mellékfeltétel.

Def. Vandermonde-determináns. (felga)

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} = V(a_1; \dots; a_n)$$

Állítás. $V(a_1; \dots; a_n) = \prod_{1 \le i < j \le n} (a_j - a_i)$

Megjegyzés $V(\dots) \neq 0$, ha $a_1; \dots; a_n$ páronként különbözőek.

B: n szerinti teljes indukció

$$\begin{vmatrix} 1 & a_1 \\ 1 & a_2 \end{vmatrix} = a_2 - a_1 \checkmark$$

$n-1 \Rightarrow n$

$$\begin{vmatrix} 1 & a_1 & \cdots & a_1^{n-2} & a_1^{n-1} \\ 1 & a_2 & \cdots & a_2^{n-2} & a_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & a_n & \cdots & a_n^{n-2} & a_n^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & 0 & \cdots & 0 & 0 \\ 1 & a_2-a_1 & \cdots & a_2^{n-3}(a_2-a_1) & a_2^{n-2}\cdot(a_2-a_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & a_n-a_1 & \cdots & a_n^{n-3}(a_2-a_1) & a_n^{n-2}(a_n-a_1) \end{vmatrix} =$$

$\cdot a_1$

$$= + \begin{vmatrix} a_2-a_1 & \cdots & a_2^{n-2}(a_2-a_1) \\ a_3-a_1 & \cdots & a_3^{n-2}(a_3-a_1) \\ \vdots & \ddots & \vdots \\ a_n-a_1 & \cdots & a_n^{n-2}(a_n-a_1) \end{vmatrix} = (a_2-a_1)\cdot\ldots\cdot(a_n-a_1)\cdot \overbrace{V(a_2; \dots; a_n)}^{\prod_{2 \le i < j \le n}(a_j-a_i)} = \prod_{1 \le i < j \le n} (a_j - a_i) \quad \square$$

Tétel. (Determinánsok szorzástétele) $A, B \in M_n(K)$

$$\det(AB) = \det(A)\cdot\det(B)$$

B:

$$\underbrace{\left(\begin{array}{c|c} A & 0 \\ \hline -I & B \end{array}\right)}_{\substack{\text{blokkmátrix} \\ 2n \times 2n}} = \left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1n} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} & 0 & \cdots & 0 \\ \hline -1 & \cdots & 0 & b_{11} & & \\ \vdots & \ddots & \vdots & & \ddots & \\ 0 & \cdots & -1 & & & b_{nn} \end{array}\right) = D$$

$\det D = \det A \cdot \det B$, mert det C-ben $\frac{1}{\det}$ inverzió nem lép fel, és csak $\det A$-beli és $\det B$-beli elemek vannak.

2014. 10. 16.

$$\det D = \left|\begin{array}{cccc|ccc} a_{11} & a_{12} & \cdots & a_{1n} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} & 0 & & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} & 0 & \cdots & 0 \\ \hline & & & & b_{11} & & \\ & -I & & & & \ddots & \\ & & & & & & b_{nn} \end{array}\right|$$

A b_{ij}-ket kell eltüntetni.

$C = AB \qquad c_{ij} = \sum_{t=1}^{n} a_{it} b_{tj}$

$$\det D = \left|\begin{array}{c|c} A & \begin{matrix} a_{11}b_{11}+a_{12}b_{21}+\cdots \\ a_{21}b_{11}+a_{22}b_{21}+\cdots \\ \vdots \\ a_{n1}b_{11}+a_{n2}b_{21}\cdots \end{matrix} \\ \hline -I & \begin{matrix} 0 \\ 0 \\ \vdots \end{matrix} \end{array}\right| = \left|\begin{array}{c|c} A & \begin{matrix} c_{11} & 0 \\ c_{21} & 0 \\ \vdots & \\ c_{n1} & 0 \end{matrix} \\ \hline -I & \begin{matrix} 0 & b_{12} \\ 0 & b_{22} \\ \vdots & \\ 0 & b_{n2} \end{matrix} \end{array}\right| = \left|\begin{array}{c|c} A & C \\ \hline -I & 0 \end{array}\right| =$$

Kifejtés utolsó sor szerint sokszor

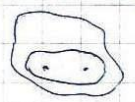
$$= \underbrace{(-1)^{2n+n}\,(-1)^{(2n-1)+(n-1)}\cdot\ldots\cdot(-1)^{(n+1)+1}\cdot(-1)\cdot(-1)\cdot\ldots\cdot(-1)}_{(-1)^{2n^2+2n}} \cdot \det C$$

$\square$

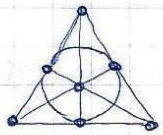
Def. Blokkrendszer: v elemű véges halmaz

k elemű részhalmazok: blokkok

Ez akkor blokkrendszer, ha bármely 2 különböző pont pontosan λ közös blokkban van benne. (Poz. egész.)



Pl. $v = 7$, $k = 3$, $\lambda = 1$ $\longrightarrow$



$b = 7$
$r = 3$

Blokkok száma összesen b.

Állítás. Blokkrendszerben $\forall$ pont ugyanannyi (r) db blokkban van benne.

B: r_P: a P pont hány bl.-ben van benne.

Számoljuk a (B, Q) párokat, ahol $P \neq Q$ pont, B blokk, $P, Q \in B$.

$\longrightarrow$ ez $r_P \cdot (k-1)$, mert a Q $k-1$ módon választható.

$\longrightarrow$ másrészt Q $(v-1)$ módon választható, λ közös blokk: $\lambda(v-1)$

$\Longrightarrow$ $r_P(k-1) = \lambda(v-1)$ = állandó $\Rightarrow$ r állandó. $\square$

Melléktermék: $r(k-1) = \lambda(v-1)$. $\longrightarrow$ $r = \dfrac{\lambda(v-1)}{k-1} \in \mathbb{Z}$

$\{(B, P) \mid P \in B\}$ $\longrightarrow$ $\underbrace{bk}_{\text{blokkok szerint}} = \underbrace{vr}_{\text{pontok szerint}}$ $\longrightarrow$ $b = \dfrac{vr}{k} = \dfrac{\lambda v(v-1)}{k(k-1)} \in \mathbb{Z}$

Blokkr. paraméterei (b, v, k, r, λ)

$k = v$:

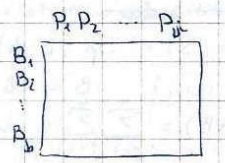
$b = 1$

A továbbiakban legyen $k < v$. $\Rightarrow$ $r > \lambda$

Tétel. (Fisher-egyenlőtlenség) $\forall$ blokkrendszerben $b \geq v$.

B: **Def.** Blokkrendszer incidenciamátrixa A, $b \times v$

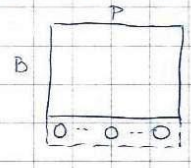
$$a_{ij} = \begin{cases} 1, & \text{ha } P_j \in B_i \\ 0, & \text{ha } P_j \notin B_i \end{cases}$$



$\forall$ sorban k db 1-es van,
$\forall$ oszlopban r db 1-es van. (Illeszkedési mátrix)

$A^T \cdot A$ $v \times v$-es mátrix $\quad A^T \cdot A = \begin{pmatrix} r & & \lambda \\ & r & \\ \lambda & & \ddots \\ & & & r \end{pmatrix}$ $\quad \det(A^T \cdot A) = \underbrace{(r-\lambda)^{v-1}}_{\neq 0} \cdot (r + (v-1)\lambda)$ $\quad r > \lambda$

Tfh. $b < v$. $\longrightarrow$ négyzetes-ítsük.



$(A')^T \cdot A'$ determinánsa ugyanaz, mert csak ~~sor~~ oszlopokat szorzunk önmagukkal.

$\det((A')^T \cdot A') = (r-\lambda)^{v-1} \cdot (r + (v-1)\lambda) \neq 0$ $\quad \lightning$

$\det((A')^T) \cdot \det(A') = 0 \cdot 0 = 0$ $\square$

$b = v \rightarrow$ szimmetrikus blokkrendszer

<u>Feladat</u>⊛. Szimm. blokkr.-ben $|B_i \cap B_j| = \lambda$. $\forall i,j,\ i \neq j$.
(Algebrai megoldás!)

Ha szimmetrikus és $\lambda = 1 \rightarrow$ véges projektív sík.

Belátható: $\exists\, n \geq 2$:
$$\left.\begin{aligned} v = b &= n^2+n+1 \\ k = r &= n+1 \\ \lambda &= 1 \end{aligned}\right\} \text{ n-edrendű véges proj. sík}$$

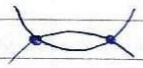
$n = p^a \Rightarrow \exists$ n-edrendű v.p.s. Elég nagy a-ra már több különböző van.

Megoldatlan: van-e nem prímhatvány rendű v.p.s.?

Bizonyított: $n = 6$-ra, $n = 10$-re nincs. De $n = 12$-re már van tudjuk.

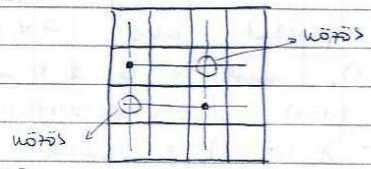
Megoldatlan: $a = 1$-re mindig csak 1 van-e?

Ha $b = v$ és $\lambda = 2 \rightarrow$ <u>biplane</u>, duplasík.



Pl. Fano komplementer halmazokkal.

Pl. $b = v = 16$, $k = r = 6$, $\lambda = 2$



Megoldatlan: van-e ∞ sok duplasík?

— o —

Van-e a determinánsoknak valami féle összeadási tétele? Nincs, és nem is lehet.

<u>Állítás</u>. $\forall\, a, b, c \in K$ $\exists\, A, B \in M_2(K)$, $\det(A) = a$, $\det(B) = b$, $\det(A+B) = c$.

B:
$$A = \begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 \\ y & b \end{pmatrix} \quad A+B = \begin{pmatrix} a+1 & x \\ y & b+1 \end{pmatrix}$$
$\det A = a$ $\quad \det B = b$ $\quad \det(A+B) = (a+1)(b+1) - xy = c$ lehet. □

<u>Def</u>. Legyen $A \in M_n(K)$, $A = (a_{ij})$ $\quad tr(A) = \sum_{i=1}^{n} a_{ii}$ A főátló elemeinek összege: nyom. (trace)

Más jelölés: $Sp(A)$: Spur

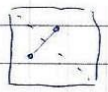
<u>Állítás</u>. $Sp(A) + Sp(B) = Sp(A+B)$.

De nincs ~~összeadási~~ szorzástételük. Igaz viszont, hogy:

<u>Állítás</u>. $Sp(A \cdot B) = Sp(B \cdot A)$

B: $A = (a_{ij})$, $B = (b_{ij})$

$$Sp(AB) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} b_{ji}$$



tükörkép

$$= Sp(BA)$$ □

<u>Kérdés</u>⊛. $A, B \in M_2(K)$ adott. Keressük $X, Y \in M_2(K) - t$, hogy $A = XY$, $B = YX$.

Szükséges: $\det A = \det B$, $Sp\, A = Sp\, B$.

De ez nem elég: pl. $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Most nézzünk általában grűpöket!

Def. R gyűrű, $e \in R$ baloegységelem: $er = r \quad \forall r \in R$.
$f \in R$ jobboegységelem: $rf = r \quad \forall r \in R$.

Példa olyan R-re, amiben $\exists$ bee., $\nexists$ jee.

$M_2(K) > \left\{ \begin{pmatrix} a & b \\ a & b \end{pmatrix} \middle| \; a, b \in K \right\} \rightarrow$ gyűrű $+$-ra zárt, $\cdot$-ra: $\begin{pmatrix} (a+b)c & (a+b)d \\ (a+b)c & (a+b)d \end{pmatrix}$

Def. $K_1 \leq K_2$ résztest $<$: valódi ...
$R_1 \leq R_2$ részgyűrű (hasonlóan: $\subset$ valódi résztest., $\subseteq$ résztest.)
$G_1 \leq G_2$ részcsoport, $H \leq G$ (ált. H a részcsoport jele)

$\begin{pmatrix} a & b \\ a & b \end{pmatrix}$ bee $\Leftrightarrow (a+b) = 1$ Ha K ∞: ∞ sok bee van.

De $\emptyset$ jee. (A következő állítás következménye.)

Állítás. $\exists e \in R$ bee, $\exists f \in R$ jee $\Rightarrow e = f$. (Ebből következően csak 1 van mindkettőből.)

B: $\left.\begin{array}{l} ef = e \\ ef = f \end{array}\right\} e = f$ ✓ $\square$

Ha $e = f \rightarrow 1 \in R$ egységelemes gyűrű.

Def. $1 \in R$. $a \in R$ a' balinverze a-nak: $a'a = 1$
a'' jobbinverze a-nak: $aa'' = 1$.

Állítás. a-nak van a' binv., a'' jinv. $\Rightarrow a' = a''$.

B: $\left.\begin{array}{l} a'aa'' = a'(aa'') = a' \cdot 1 = a' \\ \quad\;\; = (a'a)a'' = 1 \cdot a'' = a''. \end{array}\right\} a' = a''$ $\square$

Feladat. Ha egy gyűrűben csak 1 bee van, akkor az jobboegységelem is.

Feladat. (Nehezebb) $1 \in R$. a-nak van legalább 2 balinverze $\rightarrow \infty$ sok binv.-e van.

„Mindenkire magára bízom, hogy ezek ugyanúgy találjon ki egy 3. feladatot magának és oldja meg."

Térjünk vissza a mátrixokhoz!
$A \in M_n(K)$ $\exists ?\; A' : \; A' \cdot A = I$
$\nexists A'$, ha $\det(A) = 0$ a det. szorzástétele miatt, ugyanígy jobbinverze se lesz.

Állítás. Ha $A \in M_n(K)$, $\det(A) = D \neq 0$. Ekkor $\exists A^{-1}$: $A^{-1}A = AA^{-1} = I$.
$A^{-1} = (b_{ij})$ A inverze
$$b_{ij} = \frac{A_{ji}}{D}$$

B: $A^{-1} \cdot A$ i-edik sor k-adik eleme: $\displaystyle\sum_{t=1}^{n} \frac{A_{ti}}{D} \cdot a_{tk} = \frac{\sum_{t=1}^{n} a_{tk} \cdot A_{ti}}{D}$

$\left.\begin{array}{ll} \text{Ha } i = k: & \sum a_{tk} \cdot A_{ti} \text{ egy kifejtés} \rightarrow D/D = 1 \\ \text{Ha } i \neq k: & \text{— " — ferde kifejtés} \rightarrow 0 \end{array}\right\} I$ $\square$

„Az előbb mutattam egy jófofa példát $M_2(K)$-ben részgyűrűre."

Def. Izomorfizmus: $R_1 \simeq R_2$, ha $\exists$ kölcs. eé. műveletartó leképezés R_1 és R_2 között.

$K_1 \simeq K_2$, ...

$G_1 \simeq G_2$, ...

Pl. $G_1 = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ mod n
$G_2 = \varepsilon \in \mathbb{C}$, $\{1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}\}$ } izomorf ✓

Pl. $(\mathbb{R}, +)$ és csoport
$(\mathbb{R}^{>0}, \cdot)$ csoport } megegyező módon izomorfak!

$(\mathbb{R}, +) \simeq (\mathbb{R}^{>0}, \cdot)$

$\xleftarrow{\log}$ $\log(ab) = \log a + \log b$

$\xrightarrow{a^x}$ $a \neq 1, a > 0$ $a^{b+c} = a^b \cdot a^c$ ✓

$$R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a, b \in \mathbb{R} \right\} \leq M_2(\mathbb{R}) \qquad R \simeq \mathbb{C}$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longrightarrow a + bi \qquad \text{Pl. } i: \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rightarrow i^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

2014.11.06.

$$\left.\begin{matrix} a_{11}x_1 + \dots + a_{1k}x_k = b_1 \\ \vdots \qquad \ddots \qquad \vdots \\ a_{n1}x_1 + \dots + a_{nk}x_k = b_{kn} \end{matrix}\right\} \qquad \begin{matrix} a_{ij}, b_j \in K \\ x_j \in K \end{matrix} \rightarrow n = k$$

Tétel. (Cramer-szabály)

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nk} \end{pmatrix}$$ az egyenletrendszer mátrixa.

$n = k$-ra: vehető $D = \det A$.

Ha $\det A \neq 0 \rightarrow$ az egyenletrendszernek pontosan 1 megoldása van és

$$x_j = \frac{D_j}{D}, \text{ ahol } D_j = \begin{vmatrix} a_{11} & \cdots & a_{1,j-1} & b_1 & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & \cdots & \vdots & \vdots & \vdots & & \\ a_{n1} & \cdots & a_{n,j-1} & b_n & a_{n,j+1} & \cdots & a_{nn} \end{vmatrix}$$

B:

$$\underline{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}, \quad \underline{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} \longrightarrow \underset{n \times n}{A} \, \underset{n \times 1}{\underline{x}} = \underset{n \times 1}{\underline{b}}$$ az egyenletrendszer

A^{-1} létezik, mert $\det A \neq 0 \Rightarrow A^{-1} \cdot A \cdot \underline{x} = A^{-1} \cdot \underline{b}$

$\underbrace{A^{-1} \cdot A}_{I} \cdot \underline{x} = A^{-1} \cdot \underline{b}$

$\Leftrightarrow \underline{x} = A^{-1} \cdot \underline{b}$

$$A^{-1}\underline{b} = \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix} \cdot \frac{1}{D} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} =$$

$$= \rightarrow x_j = \frac{A_{1j} b_1 + A_{2j} b_2 + \dots + A_{nj} b_n}{D} = \frac{D_j}{D}$$

$\square$

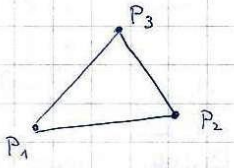
Ha $\underline{b} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ → homogén lineáris egyenletrendszer

⇒ Cramer szerint $(x_1, \dots, x_n) = (0, 0, \dots, 0)$, mert $\forall D_j = 0$. (ha $\det A \neq 0$)

<u>Megjegyzés.</u> Hom. lin. ex.-nek $\det A = 0$ esetén megoldása $(0, 0, \dots, 0)$ (triviális megoldás) és van nemtriviális megoldása is. (Később bizonyítjuk)

— o —

$P_1(x_1, y_1)$
$P_2(x_2, y_2)$
$P_3(x_3, y_3)$



$$T = \frac{1}{2} \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix}$$ előjeles terület

$T > 0$, ha P_1, P_2, P_3 ⊕ körüljárású
$T < 0$, ha —"— ⊖ —"—

3 pont egy egyenesen, ha $T = 0$.

— o —

Polinomok

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ $\quad a_i \in K, \quad a_n \neq 0$

$K[x] = \{ f(x) \mid a_i \in K \}$ $\quad$ f foka n: $n = \deg f$

$\deg(1) = 0$

$\deg(0) = ?$

$g(x) = b_k x^k + \dots + b_0$

Def. (intuitív) $f(x) + g(x) = \sum_i (a_i + b_i) x^i$

Formálisan:

$$f(x) \longleftrightarrow (a_0, a_1, \dots, a_n) \longleftrightarrow (a_0, a_1, \dots, a_n, 0, 0, \dots)$$
$$g(x) \longleftrightarrow (b_0, b_1, \dots, b_k) \longleftrightarrow (b_0, b_1, \dots, b_k, 0, 0, \dots)$$

Def. Polinom: K elemeiből kitöltött ∞ sorozatok, amiknek csak véges sok tagja $\neq 0$.

Def. (intuitív) $f(x) \cdot g(x) = \sum c_i x^i$, ahol $c_i = a_0 b_i + a_1 b_{i-1} + \dots + a_i b_0$

$$\underset{a_2}{(x^2} + \underset{a_1}{x} + \underset{a_0}{1)}\,(\underset{b_3}{2x^3} + \underset{b_2}{3x^2} + \underset{b_1}{4x} + \underset{b_0}{5}) \Rightarrow c_4 = \underbrace{a_0 b_4}_{0} + \underbrace{a_1 b_3}_{1 \cdot 2} + \underbrace{a_2 b_2}_{1 \cdot 3} + \underbrace{a_3 b_1}_{0} + \underbrace{a_4 b_0}_{0} = 5$$

Állítás. $(K[x], +, \cdot)$ gyűrű, egységelemes, kommutatív, nulloszt\ó mentes.

$\hookrightarrow$ K feletti polinomgyűrű

Állítás. $\deg(fg) = \deg(f) + \deg(g)$ $\quad f, g \in K[x]$

$\deg 0$ nem értelmezett (vagy $\deg 0 = -\infty$, ha nagyon muszáj)

Legyen R gyűrű $\rightarrow$ $R[x]$ ugyanúgy def. ható: R feletti polinomgyűrű

Gyűrűben nem igaz a deg-ére vonatkozó összefüggés!

$$R = \mathbb{Z}_4 \quad \underbrace{(2x+1)}_{\neq 0}\underbrace{(2x+3)}_{\neq 0} = \underbrace{4x^2}_{0} + 5x + 3 = 5x + 3$$

Nem egységelemes R-ben x sem polinom.

$f(x) = a_n x^n + \dots + a_0$ $\quad f \in R[x]$

$c \in R \rightarrow f(c) = a_n c^n + \dots + a_0$ $\quad R \rightarrow R$ függvény ($\neq$ polinom!)

Különböző polinomok adhatják ugyanazt a függvényt.

Pl. $\left.\begin{array}{l} x^p \in \mathbb{F}_p[x] \quad c^p = c \quad \text{(Kis Fermat)} \\ x \in \mathbb{F}_2[x] \end{array}\right\}$ a 2 függvény ugyanaz

$fg(c) = f(c)\,g(c) \rightarrow$ csak komm. gyűrűben!

$$(\dots + a_i c^i + \dots) \cdot (\dots + b_j c^j + \dots) = \dots + a_i c^i b_j c^j + \dots \neq \dots + a_i b_j c^{i+j} + \dots$$

$\Rightarrow$ Óvatosnak kell lenni gyűrű felett!

Def. $c \in R$ gyöke f-nek ($f \in R[x]$), ha $f(c) = 0$.

Maradékos osztás

Tétel. $K[x]$-ben $\exists$ m. osztás: $f, g \in K[x]$ $(g \neq 0)$ $\exists! q, r \in K[x]$
$\rightarrow f(x) = g(x)\, q(x) + r(x)$, ahol $\deg r < \deg g$ vagy $r = 0$.

B: Ha $f = 0 \rightarrow$ igaz ✓

Tfh. $f = a_n x^n + \dots + a_0$

$g = b_k x^k + \dots + b_0$

Ha $k > n \rightarrow q = 0,\ r = f$ ✓

Ha $k \leqslant n$

$$f(x) - \underbrace{a_n b_k^{-1} x^{n-k}}_{q(x)} \cdot g(x) \quad \text{lépések}$$

Egyértelműség: ha $f = g\, q_1 + r_1 = g\, q_2 + r_2$

$$\Rightarrow \underbrace{g\, \underbrace{(q_1 - q_2)}_{\neq 0}}_{\deg \geqslant \deg g} = \underbrace{r_2 - r_1}_{\deg < \deg g}$$

↯ □

Tétel. $K[x] \ni f$, $K \ni c$. $f(c) = 0 \iff \underbrace{(x-c)}_{\text{gyöktényező}} \mid f$, azaz $\exists\, g(x) \in K[x]$: $f(x) = (x-c)\, g(x)$.

B: $\Leftarrow$ triviálisan igaz.

$\Rightarrow$: maradékos osztás: f-et $(x-c)$-vel

$f(x) = (x-c) \cdot q(x) + r(x)$ $\quad \deg(r) < 1$ vagy $r = 0$.

$\rightarrow f(c) = r(c)$ $\quad$ ~~deg~~

$f(c) = 0$, azaz gyök, ha $r = 0$. □

B₂: $\left.\begin{array}{l} f(x) = a_n x^n + \dots + a_0 \\ f(c) = 0 \end{array}\right\} \Rightarrow f(x) = f(x) - f(c) = a_n \underbrace{(x^n - c^n)}_{(x-c)\mid} + \dots + a_1 \underbrace{(x-c)}_{(x-c)\mid}$ ✓ □

$\Rightarrow$ $\deg f = n$, $f(c_1) = 0 \Rightarrow f(x) = (x - c_1) \cdot f_1(x)$

$c_1 \neq c_2$ $\quad f(c_2) = 0 \Rightarrow f_1(x_2) = (x - c_2) \cdot f_2(x)$

$\dots$

$f(x) = (x - c_1)(x - c_2) \cdot \dots \cdot (x - c_n) \cdot a_n$

Következmény. $K[x]$-ben egy n-edfokú polinomnak legfeljebb n gyöke lehet.

$R = \mathbb{Z}_8$ $\quad x^2 - 1 \in \mathbb{Z}_8[x] \rightarrow 1, 3, 5, 7$ gyökök

Def. Ferdetest: test, ahol minus kihötve MT.

Igaz, hogy minden véges ferdetest test (nemtriviális tétel, bizonyítani fogjuk).

Def. Kvaterniók. i, j, k $\quad \mathbb{H} = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \}$

Def. Egyenlő, ha $(a, b, c, d) = (a', b', c', d')$

Def. Összeadás $(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) = (a_1 + a_2) + (b_1 + b_2) i + (c_1 + c_2) j + (d_1 + d_2) k$

$\rightarrow$ Abel-csoport lesz

$i^2 = j^2 = k^2 = -1$, $\quad ij = k$, $jk = i$, $ki = j$ $\quad$ „Az abc ismerőinek környű megjegyezni."

$ji = -k$, $kj = -i$, $ik = -j$

$x i = i x$, $x j = j x$, $x k = k x$ $\quad (x \in \mathbb{R})$

$c j \cdot b i = b c (-k)$

Szorzás ez alapján def. hatő.

A legtöbb tulajdonság látszik, de az osztás nem (és persze a kommutativitás se, de ezt épp ez a pont).

<u>Def.</u> $\alpha = a + bi + cj + dk \longrightarrow \bar{\alpha} = a - bi - cj - dk$ konjugált

$\alpha\bar{\alpha} = \bar{\alpha}\alpha = a^2 + b^2 + c^2 + d^2$ pozitív, ha $\alpha \neq 0$

$N(\alpha) = a^2 + b^2 + c^2 + d^2$ norma

$\Rightarrow \alpha^{-1} = \dfrac{\bar{\alpha}}{N(\alpha)}$ jó inverznek

$x^2 + 1 \in \mathbb{H}[x] \longrightarrow$ gyökei $i, -i, j, -j, k, -k$

<u>Feladat:</u> x^2+1-nek ∞ sok gyöke van (igényesebbek keresési mag ötlet).

11.13.

$\mathbb{R}$	a	test	lehet-e 8 dimenziós? Lemondunk a szorzás asszociativitásáról is $\longrightarrow$ „nagyon ferde test", de a disztributivitásról nem.
$\mathbb{C}$	$a+bi$	test	
$\mathbb{H}$	$a+bi+cj+dk$	ferdetest	

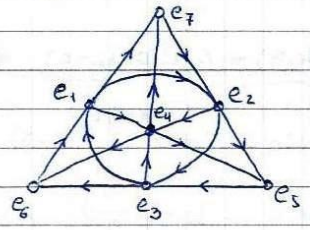
A válasz NEM. 8 dimenziós Cayley-számok vannak, de itt vége: 16, 32 nincs.

<u>Def.</u> Cayley-számok $e_0, \dots, e_7$ bázis

$x_0 e_0 + \dots + x_7 e_7$ $(x_i \in \mathbb{R})$

$e_0 e_i = e_i e_0 = e_0 \longrightarrow e_0$ egységelem a disztrib. miatt

$e_i^2 = -e_0$ $1 \le i \le 7$



$e_i e_j = \pm e_k$ e_k a 3. pont az egyenesen

+, ha az irányításnak megfelelően

$e_1 e_2 = e_3$, $e_2 e_1 = -e_3$

$e_5 e_3 = e_6$, $e_3 e_5 = -e_6$

$e_7 e_3 = e_4$, $e_3 e_7 = -e_4$

$e_4 e_6 = e_2$ $e_6 e_4 = -e_2$

A szorzás nem asszociatív.

Gyenge verziója igaz: $\begin{cases} (aa)b = a(ab) \\ (ab)a = a(ba) \\ (ba)a = b(aa) \end{cases}$ Megmutatható, hogy 2-ből következik a 3.

alternatív tulajdonság $\Rightarrow$ alternatív gyűrű

Konjugált: $\bar{\alpha} = x_0 e_0 - x_1 e_1 - \dots - x_7 e_7$

$N(\alpha) = \alpha\bar{\alpha} = x_0^2 + x_1^2 + \dots + x_7^2$ norma (≥ 0) $\longrightarrow \alpha^{-1} = \dfrac{\bar{\alpha}}{N(\alpha)}$

Cayley-számok: $\mathbb{O}$ (októniók).

Miért ez a definíció? Van standard eljárás:

Megköveteljük: $\exists$ konjugálás: $\bar{\bar{\alpha}} = \alpha$

$\overline{ab} = \bar{b}\bar{a}$ (Hf. $\mathbb{H}$-ban bizonyítani)

$\overline{a+b} = \bar{a} + \bar{b}$

Bővebb gyűrű:

$R \to R^*$ $R^* = \{(a,b) \mid a, b \in R\}$, $\overline{(a,b)} = (\bar{a}, -\bar{b})$

$(a,b)\cdot(c,d) = (ac - \bar{d}b\,;\ da + b\bar{c})$

Ezt $\mathbb{O}$-ra kiterjesztve nem lesz jó: lesznek nulloszlók.

$1 \in R$, kommutatív, nullosztómentes,
integritási tartomány

Def: a osztója b-nek: $a|b \iff \exists c \in R \quad ac = b$

Triviálisan: $1|a \quad \forall a \in R$. Tranzitív reláció: $a|b,\ b|c \Rightarrow a|c$. Reflexív: $a|a$.
$b=ad \quad c=bf \qquad c=adf$

Def. $e \in R$ egység, ha $\forall a \in R$: $e|a$.

Ekvivalens: $e|1$. Tehát az egységek pont az invertálható elemek: $ee' = 1$.

$\mathcal{U}(R) = \{ e \in R \mid e \text{ egység} \} = R^*$ (Angolul egység: unit
egységelem: identity)

Állítás. $\mathcal{U}(R)$ csoport a szorzásra.

Ismeretlel. R test $\iff \mathcal{U}(R) = R \setminus \{0\}$

Def. a asszociáltja b-nek, ha $\exists e \in \mathcal{U}(R)$: $b = ae$: $a \sim b$.

Állítás. $\sim$ ekvivalenciareláció

B: $a \sim a$: $a = a \cdot 1$
$a \sim b \iff b \sim a$: $b = ae$, $be' = aee' = a$ $\quad e' \in \mathcal{U}(R)$
$a \sim b,\ b \sim c \Rightarrow a \sim c$: $b = ae$, $c = bf$, $c = aef = ag$, $g = ef \in \mathcal{U}(R)$. □

Állítás. $a \sim b \iff a|b \wedge b|a$.

B: $b = ad$
$a = b \cdot c = a(dc)$ $\quad a \neq 0 \Rightarrow dc = 1 \Rightarrow d, c \in \mathcal{U}(R)$
Ha $a = 0 \to b = a \cdot e = 0 \cdot e = 0$. □

Ekvivalenciareláció $\iff$ osztályokra bontás.

$\mathbb{Z}$-ben: $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$
$\mathcal{U}(K[x]) = K^*$ $\Rightarrow$ pl. $\mathbb{Q}$ felett $(x^2+3) \sim (-7x^2-21)$

Def. Legyen R egységelemes integritási tartomány. $p \in R$ irreducibilis, ha $p \neq 0, p \neq 1$,
$p = ab \Rightarrow (a \sim p \wedge b \sim 1) \vee (a \sim 1 \wedge b \sim p)$.

Def. $p \in R$ prím, ha $p \neq 0$, $p \neq 1$, $p|ab \Rightarrow p|a \vee p|b$.

Állítás: p prím $\Rightarrow p$ irreducibilis

B: $p = ab \Rightarrow p|a$, $a|p$ $\Big\}$ $p \sim a \Rightarrow a = pe \Rightarrow p = peb \Rightarrow 1 = eb \Rightarrow b \in \mathcal{U}(R)$.

□

A fordított irány nem igaz mindig!
Pl. Legyen $d \in \mathbb{Z}$, d nem négyzetszám. $\mathbb{Z}[\sqrt{d}] = \{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \}$
$a_1 + b_1\sqrt{d} = a_2 + b_2\sqrt{d}$
$\Rightarrow a_1 = a_2 \wedge b_1 = b_2$, mert $(b_1 - b_2)\sqrt{d} = a_2 - a_1$.
Részgyűrűje $\mathbb{C}$-nek.
($\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ Gauss-egészek)

d-től nagyon függ, hogy $\mathbb{Z}[\sqrt{d}]$-ben milyen a számelmélet.

Legyen $d = -5$.

$U(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}$

$\alpha = a + b\sqrt{-5}$

$\bar{\alpha} = a - b\sqrt{-5}$

$\alpha\bar{\alpha} = a^2 + 5b^2 = N(\alpha) \geq 0$ A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$

$\alpha\beta\overline{\alpha\beta} = \alpha\bar{\alpha}\,\beta\bar{\beta}$

$\alpha(\beta\bar{\beta})\bar{\alpha} = \alpha\bar{\alpha}\,\beta\bar{\beta}$

$\alpha\bar{\alpha}\,\beta\bar{\beta} = \alpha\bar{\alpha}\,\beta\bar{\beta}$ (IH-ban is)

$\alpha \mid \beta \Rightarrow N(\alpha) \mid N(\beta)$

$\alpha \mid 1 \Leftrightarrow N(\alpha) \mid N(1) = 1 \Leftrightarrow N(\alpha) = 1 \Leftrightarrow \alpha\bar{\alpha} = 1$

$\Rightarrow a^2 = 1,\ b = 0 \Rightarrow U(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}$. ✓

$6 = 2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$

Áll.: $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ irreducibilisek.

$4 = N(2) = N(\alpha)N(\beta)$ $\quad 4 = 1 \cdot 4 = 4 \cdot 1 = 2 \cdot 2$

A 2 nem lehet norma → a 2-t csak $1 \cdot 4 = 4 \cdot 1$-ként lehet felbontani.

Ugyanez a 3-ra, stb.

De $2 \nmid (1+\sqrt{-5})$ stb. ↯ → az irreduc. nem feltétlenül prím.

Példa. $\mathbb{Z}[\sqrt{5}]$-ben

$3 - 7\sqrt{5} \sim -113 - 51\sqrt{5}$ igaz → vannak nemtrivi egységek.

Def. R egységelemes integritási tartomány. $a, b \in R$

d a, b-nek legnagyobb közös osztója: $d = (a, b)$, ha $d \sim (a, b)$

1) $d \mid a$, $d \mid b$,

2) $d' \mid a$, $d' \mid b \Rightarrow d' \mid d$.

Állítás. Ha d_1, d_2 lnko.-k, akkor associáltak.

B: $d_1 \mid d_2 \wedge d_2 \mid d_1 \Rightarrow d_1 \sim d_2$. □

Tétel. $R = K[x]$ $\quad f, g \in K[x] \Rightarrow \exists (f, g)$ és előáll lin. kombinációként: $(f, g) = fh_1 + gh_2$.

B:

$f = g \cdot q_1 + r_1$ $\quad \deg r_1 < \deg g$

$g = r_1 q_2 + r_2$ $\quad \deg r_2 < \deg r_1$ $\quad$ A 2. lépéstől kezdve az osztó kisebb

$r_1 = r_2 q_3 + r_3$ $\quad \deg r_3 < \deg r_2$ $\quad$ fokú, mint az osztandó

$\vdots$ $\quad \vdots$ $\quad$ A deg monovariáns.

$r_{k-2} = r_{k-1} q_k + r_k$ $\quad \deg r_k < \deg r_{k-1}$

$r_{k-1} = r_k q_{k+1}$ $\quad$ → euklidesi algoritmus

$r_k = (f, g)$.

1) $r_k \mid r_k$, $r_k \mid r_{k-1} \Rightarrow r_k \mid r_{k-2} \Rightarrow \ldots \Rightarrow r_k \mid g$, $r_k \mid f$. ✓

2) $d \mid f$, $d \mid g \Rightarrow d \mid r_1 \Rightarrow \ldots \Rightarrow d \mid r_k$. ✓

És tényleg előáll lin. komb.-ként. □

$K[x]$-ben szokás f-nek azt az associáltját venni, aminek a főeh.-ja 1.

Ha R-ben teljesül a számelmélet alaptétele: $a = p_1 \cdots p_n$, ahol p_i irreducibilisek, ahol a felb. lény. egyértelmű: $a = p_1 \cdots p_n = q_1 \cdots q_k \Rightarrow k = n$ és valahány sorendre $p_i \sim q_i$. ($\Rightarrow$ az a gyűrű a kívánatos)

Tétel. $K[x]$-ben igaz a SzAT.

Amiben igaz a SzAT: UFD (unique factorization domain), esetleg egy alaptételes gyűrű.

Lemma. Egységelemes integritási tartomány UFD $\Leftrightarrow$ 2014.11.20.

1) $\forall a \in R$ irreducibilisek szorzata $(a \neq 0)$

2) $\forall$ irreducibilis prím.

B: $\Rightarrow$ 1) triviálisan

2): legyen a irreducibilis, $a \mid bc$.

$\exists d: \quad ad = bc$

$$\begin{aligned} b &= p_1 \cdots p_k \quad (p_i \text{ irred.}) \\ \text{UFD} \Rightarrow c &= q_1 \cdots q_\ell \quad (q_j \text{ irred.}) \\ d &= r_1 \cdots r_t \quad (r_i \text{ irred.}) \end{aligned}$$

$\Rightarrow a \sim p_1 \vee a \sim q_1 \Rightarrow a \mid p \vee a \mid q.$ $\boxtimes$

$\Leftarrow$ Tfh. $a = p_1 \cdots p_k = q_1 \cdots q_\ell \quad (p_i, q_j \text{ irred.})$

Belátjuk: $k = \ell$ és alkalmas számozásra $p_i \sim q_i$.

$p_1 \mid q_1 \cdots q_\ell \xRightarrow{2) \text{ miatt}}$ (ha 2 tényezőnek osztója $\Rightarrow$ ℓ tényezőnek is)

$p_1 \mid q_1 \Rightarrow d\, p_1 = q_1 d$. p_1, q_1 irreducibilisek

$\Rightarrow d = e_1: \quad e p_1 = q_1$

$\Rightarrow p_2 \cdots p_k = e_1' \cdot q_2 \cdots q_\ell$

$\Rightarrow p_3 \cdots p_k = e_1' \cdot e_2' \cdot q_3 \cdots q_\ell$

Ha $k \neq \ell \rightarrow$ valamelyik p vagy q egység

$\Rightarrow k = \ell$ és páronként = tényező. $\boxtimes$

Tétel. $K[x]$ UFD.

B: $K[x]$-ben vem formám. Fokszámra vonatkozó indukció $\Rightarrow$ 1).

2): Legyen f irreducibilis. $f \mid gh$. Megmutatjuk: $f \nmid g \Rightarrow f \mid h$.

$(f, g) = 1 \quad \exists u, v \in K[x]: \quad 1 = fu + gv$

$\Rightarrow h = fuh + ghv = \underbrace{f(uh)}_{f \mid} + \underbrace{(gh)v}_{f \mid} \Rightarrow f \mid h$. f prím. $\square$

Az, ha egy i.t. UFD, az egy ünnep. Kérdés: mik az irreducibilisek?

Állítás. $f \in K[x]$, $\deg f = 1 \Rightarrow f$ irreducibilis.

B: Triviális. $\square$

$\mathbb{C}$-ben csak az elsőfokúak irred.

Algebra alaptételét használjuk majd (megelőlegezve): $\forall f \in \mathbb{C}[x]$ $\deg f \geq 1 \Rightarrow$ $\exists \alpha \in \mathbb{C}$ $f(\alpha) = 0$.

~~Ha $\forall f \in$~~

Definíció. $\forall f \in K[x]$ $\deg f \geq 1 \Rightarrow \exists \alpha \in K: f(\alpha) = 0$, akkor K algebrailag zárt.

Állítás. $\mathbb{C}[x]$-ben csak az elsőfokúak irreducibilisek.

B: $\deg f \geq 2 \Rightarrow f = (x - \alpha) \cdot f_1 \rightarrow$ nem irred. $\square$

$\mathbb{R}[x]$-ben $ax^2 + bx + c$ irred. ocsa., ha $b^2 - 4ac < 0$.

Állítás. 2-nél magasabb fokúak $\mathbb{R}[x]$-ben nem irred.

B: $f(x) = a_n (x - \alpha_1) \cdots (x - \alpha_n) \quad (\alpha_i \in \mathbb{C}) \qquad f(\alpha) = 0 \Rightarrow f(\bar{\alpha}) = 0$

Alg. alaptételéből $\nearrow$ $\qquad (x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} \in \mathbb{R}[x]$

$\rightarrow f$ felbomlik első- és másodfokúak szorzatára. $\square$

Gyökök és eh.-k közti összefüggések:

$$f(x) = a_n (x-\alpha_1) \cdots (x-\alpha_n) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$\Rightarrow \quad \alpha_1 + \dots + \alpha_n = \frac{-a_{n-1}}{a_n}, \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_1\alpha_n + \dots + \alpha_{n-1}\alpha_n = \frac{a_{n-2}}{a_n},$$

$$\dots, \quad \alpha_1 \cdots \alpha_n = (-1)^n \frac{a_0}{a_n}$$

Például: $x^n - 1 \in \mathbb{C}[x]$ $\quad x^n - 1 = \prod_{i=1}^{n} (x - \varepsilon_i)$

$$\Rightarrow \sum_{i=1}^{n} \varepsilon_i = 0, \text{ ha } n > 1; \quad \prod_{i=1}^{n} \varepsilon_i = (-1)^{n+1}$$

$f \in \mathbb{Z}[x]$ → irred. $\mathbb{Q}[x]$-ben? ⇓⇑
→ irred. $\mathbb{Z}[x]$-ben? (most ez alatt azt értjük, hogy 2 alacsonyabb fokú szorzatára bomlik) (Ez azért kell, mert $2x-4$ irred. lenne, mert 2 nem egység $\mathbb{Z}[x]$-ben.)

Tétel. $f \in \mathbb{Z}[x]$, $f = gh$, $g, h \in \mathbb{Q}[x]$, $\deg g, \deg h < \deg f$.
$\Rightarrow \exists\, s, t \in \mathbb{Q}$, $st = 1$, $sg, th \in \mathbb{Z}[x]$.
(Ha felbomlik rac.-ok szorzatára, akkor egész eh.-sokra is.)

Def. $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ primitív, ha $(a_n, a_{n-1}, \dots, a_1, a_0) = 1$.

Lemma (Gauss-lemma): $f, g \in \mathbb{Z}[x]$ primitív $\Rightarrow$ $fg \in \mathbb{Z}[x]$ primitív

B. ↯ p prím osztja fg $\forall$ eh-ját
$p \mid a_0, \dots, a_{i-1}$, de $p \nmid a_i$ → ilyen i van, mert f primitív (lehet $i=0$ is)
$p \mid b_0, \dots, b_{j-1}$, de $p \nmid b_j$
fg-ben x^{i+j} eh-ja: $p \nmid a_i b_j + (a_{i-1} b_{j+1} + \dots + a_0 \cdot b_{i+j}) + (a_{i+1} b_{j-1} + \dots + a_{i+j} b_0)$ (itt lehetnek 0 tagok) ↯ □

A tétel bizonyítása: $f = k f_1$, f_1 primitív, $k \in \mathbb{Z}$,
$g = \frac{a}{b} g_1$ $\quad g_1$ primitív, $(a,b) = 1$
$h = \frac{c}{d} h_1$ $\quad h_1$ primitív $(c,d) = 1$

$$k f_1 = \frac{a}{b} g_1 \cdot \frac{c}{d} h_1$$

$$k b d \underline{f_1} = a c \underline{(g_1 h_1)}$$

$g_1 h_1$ primitív (Gauss)
A bal oldal lukó-ja kbd, a jobb oldalé ac
$\Rightarrow kbd = ac$
⇓

$$\underbrace{\frac{b}{a}}_{s} g = g_1, \quad \underbrace{\frac{d}{c} \cdot k h_1}_{t} = k h_1$$

$\rightarrow st = 1$, $sg \in \mathbb{Z}[x]$; $kh_1 = th \in \mathbb{Z}[x]$. ✓ □

Schönemann–Eisenstein-kritérium.
$f \in \mathbb{Z}[x]$ $\quad f(x) = a_n x^n + \dots + a_1 x + a_0$
Tfh. $\exists\, p$ prím, amire
1) $p \nmid a_n$
2) $p \mid a_{n-1}, \dots, a_0$
3) $p^2 \nmid a_0$ $\quad (p \| a_0)$

$\Rightarrow f$ irreducibilis $\mathbb{Z}[x]$-ben. (és így $\mathbb{Q}[x]$-ben is)

B: $\nexists$ g eh-i b_i, h eh-i c_j. $f = gh$

$a_0 = b_0 c_0 \rightarrow p \mid b_0,\ p \nmid c_0$

Innen fellelt lépheduünk:

$$p \mid b_1,\ p \mid b_2, \dots, p \mid b_{t-1}, \text{ de } p \nmid b_t.$$

Ilyen t van, mert különben $\forall b_i$ osztható lenne $\Rightarrow a_n$ is osztható lenne.

x^t eh-ja f-ben:

$$a_t = \underbrace{b_0 c_t}_{p \mid} + \underbrace{b_1 c_{t-1}}_{p \mid} + \dots + \underbrace{b_{t-1} c_1}_{p \mid} + \underbrace{b_t c_0}_{p \nmid} \quad \text{(lehetnek 0 vagy } \nexists \text{ egyáltalán)}$$

$\Rightarrow t = n$, mert $p \nmid a_t$. De ez ror $\deg g = \deg f$. $\nexists$ $\square$

<u>Következmény.</u> $x^n + 2 \in \mathbb{Z}[x]$ irreducibilis.

B: $p = 2$-vel Sch-E.: $2 \| 2,\ 2 \mid 0, \dots, 2 \mid 0,\ 2 \nmid 1$ $\square$

Ez $x^n \pm p$-re is működik analóg. Tehát van tetsz. fokú irred. $\mathbb{Z}[x]$-ben.

A Sch-E csak elégséges: ~~x^4+4~~

$(x^4 + 4 = x^4 + 4x^2 + 4 - 4x^2 = (x^2+2)^2 - (2x)^2 = (x^2+2x+2)(x^2-2x+2))$

$x^4 + 8$ viszont tényleg irred., pedig nem alkalmazható a Sch-E.

$$x^n - 1 = \prod_{j=1}^{n} (x - \varepsilon_j) \longrightarrow \text{mi a helyzet primitívekre?}$$

Legyenek $\varepsilon_1, \dots, \varepsilon_{\varphi(n)}$ pr. egys.-ek: $\Phi_n = \prod_{j=1}^{\varphi(n)} (x - \varepsilon_j)$ az n-edik körosztási polinom.

$\Phi_n \in \mathbb{C}[x]$, $\deg \Phi_n = \varphi(n)$.

<u>Tétel.</u> $\Phi_n(x) \in \mathbb{Z}[x]$.

B: $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$, mert $\forall$ n-edik egységgyök valamely d-re (és csak 1-re) primitív egységgyök.

$$\Rightarrow \boxed{\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x)}}$$

$\Phi_1 = x - 1$

$\Phi_2 = x + 1$

$\Phi_3 = (x - \omega)(x - \bar{\omega}) = x^2 + x + 1$

Φ_n főeh.-ja def. miatt 1 főeh.-jű.

A nevező 1 főeh.-jűek szorzata $\Rightarrow$ 1 főeh.-jű. $F(x) = \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x)$

$x^n - 1 = F(x)\, G(x) + R(x)$

A maradékos osztás algoritmusa miatt $G(x) \in \mathbb{Z}[x]$ lesz, mert a főeh.-k 1-ek.

$\Rightarrow R(x) \in \mathbb{Z}[x]$.

Mindegyik $\Phi_d \mid (x^n - 1)$. $\Rightarrow \Phi_n \in \mathbb{Z}[x]$ $\square$

$\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1.$

„Aki ezt az $x+1$-et behelyettesíti és kifejti binomiális tétellel, az meg is érdemli."

<u>Állítás.</u> $\Phi_p(x)$ irreducibilis. ($\mathbb{Q}[x]$, $\mathbb{Z}[x]$ felett)

B: $f(x)$ irreducibilis $\Leftrightarrow g(x) = f(x+1)$ irreducibilis

(B: $f = a \cdot b \Rightarrow f(x+1) = a(x+1)\, b(x+1)$ és viszont.)

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + \binom{p}{1} x^{p-1} + \dots + \binom{p}{p-1} x + 1 - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-2} + \dots + \binom{p}{p-1}$$

$\Phi_p(x+1)$-re Sch-E. p-vel $\Rightarrow$ irred. $\Rightarrow \Phi_p(x)$ is irred. $\square$

Megmutatnád, hogy $\Phi_n(x)$ is irreducibilis.

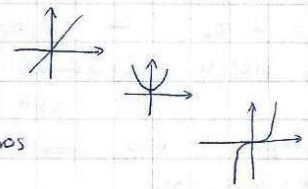
2014. 11. 27.

Legyen $K = \mathbb{R}$. (a példa erejéig)

$f(x) = x \quad \to \quad x = 0$ gyöke

$f(x) = x^2 \quad \to \quad x = 0$ gyöke, de másként: kétszeres

$f(x) = x^3 \quad \to \quad x = 0$ gyöke, „nagyon belesimul": háromszoros



Vegyük $K[x] \ni f(x)$-et, $\alpha \in K$, $f(\alpha) = 0 \iff x - \alpha \mid f(x)$, $f(x) = (x-\alpha)\, g(x)$.

Def. $f(x) \in K[x]$ $\alpha \in K$ legalább k-szoros gyöke, ha $\exists\, h(x) \in K[x]$: $f(x) = (x-\alpha)^k\, h(x)$
$(k \geq 1)$

Def. α pontosan k-szoros gyök, ha legalább k-szoros, de nem legalább $k+1$-szeres gyök.

Informális kijelentés:

Állítás. $f(x) \in K(x)$. $\exists\, K_1 > K$ bővebb test (akár maga a K), hogy $\beta \in K_1$, $f(\beta) = 0$.

B: kellő időben.

Def. $f \in K[x]$. Az f polinom deriváltja: $f'(x) = \sum_{j=1}^{n} j a_j x^{j-1}$, ha $f(x) = \sum_{j=0}^{n} a_j x^j$.

Állítás. $f, g \in K[x]$-ra:

1) $(f+g)' = f' + g'$

2) $(c f)' = c \cdot f' \qquad (c \in K)$

3) $(fg)' = f' g + f g'$.

B: $f = \sum a_j x^j$, $g = \sum b_\ell x^\ell$

$fg = \sum c_\ell x^\ell$, $c_k = \sum a_j b_{k-j} \longrightarrow (fg)'$-ben x^{k-1} eh.-ja $\ell c_k = \ell \sum a_j b_{k-j}$

$\sum j a_j b_{\ell-j}$ $x^{\ell-1}$ eh.-ja $f'g$-ben,

$\sum a_j \cdot (k-j) \cdot b_{k-j}$ x^{k-1} eh.-ja fg'-ben

$\xrightarrow{\oplus}$ ✓

□

4) $f(g(x))' = f'(g(x)) \cdot g'(x)$

B: hosszadalmas számolás. („aki kíváncsi, csinálja meg maga - aki nem kíváncsi, valószínűleg nemberiki fog vele gyakorlatban.")

Tétel. $f(x) \in K[x]$-nek $\exists$ többszörös gyöke $\iff (f, f') \neq 1$.

(A bővebb testben, ahol vannak gyökök: $\iff$)

B: $\Rightarrow$: Tfh. $f(x) = (x-\alpha)^2\, g(x)$.

$f'(x) = 2(x-\alpha) \cdot g(x) + (x-\alpha)^2 \cdot g'(x) = (x-\alpha) \cdot \left[2g(x) + (x-\alpha)\, g'(x)\right]$

$x - \alpha \mid f, f' \Rightarrow x - \alpha \mid (f, f') \Rightarrow (f, f') \neq 1$. ✓

$\Leftarrow$: Tfh. $(f, f') \neq 1$. $\longrightarrow \exists\, \alpha \in K$: $x - \alpha \mid f, f'$, mert (f, f')-nek $K_1 > K$-ban van gyöke.

$f(x) = 0 \quad \to \quad (x-\alpha)\, g(x) = f(x) \qquad (K_1$-ben$)$.

Állítás: $g(\alpha) = 0$.

$f'(x) = 1 \cdot g(x) + (x-\alpha) \cdot g'(x)$

$f'(\alpha) = 0 = g(\alpha) + 0 \cdot g'(\alpha) \Rightarrow g(\alpha) = 0 \to \alpha$ legalább 2-szeres gyök. □

Példa: $f = (x^2+1)^2 \in \mathbb{R}[x] \longrightarrow \emptyset$ valós gyök.

$f' = ((x^2+1)^2)' = 2(x^2+1) \cdot 2x = 4x \cdot (x^2+1)$. $\quad (f, f') = x^2 + 1 \neq 1. \longrightarrow$ van többszörös gyök.

Most hátulról számozunk:

$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = a_0 (x - \alpha_1) \cdots (x - \alpha_n)$

$\alpha_1 + \dots + \alpha_n = -\frac{a_1}{a_0}$

$\vdots \qquad \vdots$

$\alpha_1 \cdots \alpha_n = (-1)^n \frac{a_n}{a_0}$

Vegyük $\prod_{1\le i<j\le n} (\alpha_i - \alpha_j)$ -t! Ha ez $0 \iff$ van többszörös gyök. Ezt már láttuk a permutációknál: ha a permutáció páros, önmagába megy át, ha nem, az ellentétjébe.

Nézzük a négyzetét: $\prod (\alpha_i - \alpha_j)^2$. $\rightarrow$ invariáns a permutációra

Def.

$$D(f) = a_0^{2n-2} \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2 \quad : \quad \text{az } f \text{ diszkriminánsa.} \qquad D(f) \in K.$$

$n=2 \rightarrow \quad f(x) = ax^2 + bx + c = a(x-\alpha_1)(x-\alpha_2) \qquad D(f) = a^2 \cdot (\alpha_1 - \alpha_2)^2 = a^2 \cdot \left((\alpha_1+\alpha_2)^2 - 4\alpha_1\alpha_2\right) =$

$$= a^2 \cdot \left(\left(-\frac{b}{a}\right)^2 - 4 \cdot \frac{c}{a}\right) = b^2 - 4ac.$$

Szép feladat: $x^{10} + 3x^9 + (+5)x^8 + a_7 x^7 + \dots + a_1 x + a_0 \in \mathbb{R}[x]$.

Hogy válasszunk $a_7, \dots, a_0$-t, hogy 10 valós gyök legyen (multiplicitással?)

Megoldás: nincsenek ilyenek. ↯ tfh. van.

$\alpha_1 + \dots + \alpha_{10} = -3$

$\alpha_1\alpha_2 + \dots + \alpha_9\alpha_{10} = +5 \qquad \alpha_1^2 + \dots + \alpha_{10}^2 = (\alpha_1 + \dots + \alpha_{10})^2 - 2(\alpha_1\alpha_2 + \dots + \alpha_9\alpha_{10}) =$

$= (-3)^2 - 2(+5) = 9 - 10 = -1 < 0$ ↯

$D(ax^3 + bx^2 + cx + d) = a^4 \cdot (\alpha_1 - \alpha_2)^2 (\alpha_2 - \alpha_3)^2 (\alpha_3 - \alpha_1)^2 =$ $\alpha_1, \alpha_2, \alpha_3$-nak szimmetrikus polinomja

$= \dots$ $\rightarrow$ jó lenne kifejezni az elemi-ekkel.

Def. $K[x_1, \dots, x_n]$ n-változós polinom. $f(x_1, \dots, x_n) = \sum a_{k_1, \dots, k_n} x_1^{k_1} \cdots x_n^{k_n}$ $\quad (k_i \ge 0)$ $\quad (a_{\dots} \in R)$

Pl. $-7x^5y^2z^{44} + 6x + 3y^7z^3 \in \mathbb{R}[x,y,z]$. Tfh. ha a gyűrű kommu, egységelemes, nullosztómentes, de nem kell.

Ezek sokkal izgalmasabbak, mint az egyváltozósok. Most csak a szimmetrikus polinomokról lesz szó.

Def. Legyen $f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$. f szimmetrikus polinom, ha $\forall \pi \in S_n$:
$f(x_{1\pi}, \dots, x_{n\pi}) = f(x_1, \dots, x_n)$.

Pl. $f = x_1^2x_2 + x_2^2x_3 + x_3^2x_1 \qquad \pi = (1\,2\,3) \longrightarrow x_2^2x_3 + x_3^2x_1 + x_1^2x_2$ ✓

de $\pi = (1\,2) \longrightarrow x_2^2x_1 + x_1^2x_3 + x_3^2x_2 \neq f \rightarrow$ nem szimmetrikus.

$g = x_1^2x_2 + x_2^2x_3 + x_3^2x_1 + x_1x_2^2 + x_2x_3^2 + x_3x_1^2 \longrightarrow$ ez szimmetrikus.

Elemi szimmetrikus polinomok:

$$\left.\begin{aligned} \sigma_1 &= x_1 + \dots + x_n \\ \sigma_2 &= x_1x_2 + \dots + x_{n-1}x_n \\ &\vdots \\ \sigma_n &= x_1 \cdots x_n \end{aligned}\right\} \in R[x_1, \dots, x_n] \quad (1 \in R) \qquad \text{Pl. } x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$$

Legyen $F \in K[x_1, \dots, x_n]$. $\longrightarrow F(\sigma_1, \dots, \sigma_n) \in K[x_1, \dots, x_n]$ szimmetrikus, mert a σ-k szimmetrikusak.
(Elemi szimmetrikus polinomok polinomja szimmetrikus.)

Tétel. (Szimmetrikus polinomok alaptétele) Legyen $1 \in R$, $f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ szimm. polinom.
$\Rightarrow \exists! F(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$, hogy $f(x_1, \dots, x_n) = F(\sigma_1, \dots, \sigma_n)$.

2014. 12. 04.

Def. $f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$. Monomokból áll: $c\,x_1^{a_1} \cdots x_n^{a_n}$. Monom foka: $a_1 + \dots + a_n$.
Polinom foka a monomok fokszámának maximuma.

Def. f homogén, ha minden monom foka egyenszámú.

Nyilván $\forall$ polinom előáll homogén polinomok összegeként: $f = f_0 + f_1 + \dots + f_d$ $\quad (\deg f_j = j)$.
f_j: homogén j fokú.

A szimmetrikus polinomok alaptételének bizonyítása:

<u>Konvenció</u> az n-változós polinomok felírására:

$x_1^{a_1} \dots x_n^{a_n} \succ x_1^{b_1} \dots x_n^{b_n}$ ($\succ$: megelőzi), ha a lexikogr. sorrendben előbb jön.

lexikogr. rendezés: $(a_1 > b_1)$

$\vee\ (a_1 = b_1 \wedge a_2 > b_2) \vee \dots \vee (a_1 = b_1 \wedge \dots \wedge a_{n-1} = b_{n-1} \wedge a_n > b_n)$.

Ez jól fog jönni a bizonyításban.

<u>Lemma.</u> f lex. első tagja $x_1^{a_1} \dots x_n^{a_n}$

g lgr. első tagja $x_1^{b_1} \dots x_n^{b_n}$

$\Rightarrow$ fg lgr. első tagja $x_1^{a_1+b_1} \dots x_n^{a_n+b_n}$

B: A szorzatban nincs olyan tag, amiben x_i kitevője $a_i + b_i$.

$\sigma_1^{t_1} \dots \sigma_n^{t_n}$ lgr. első tagja $x_1^{t_1+t_2+\dots+t_n} x_2^{t_2+\dots+t_n} \dots x_n^{t_n}$ a lemma szerint.

$f(x_1, \dots, x_n) = c\, x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} + \dots$

f szimmetrikus, ezért a vezető tagban $a_1 \geq a_2 \geq \dots \geq a_n$

Vessük össze ezt a két összevetett!

$c \cdot \sigma_1^{a_1-a_2} \cdot \sigma_2^{a_2-a_3} \dots \sigma_{n-1}^{a_{n-1}-a_n} \sigma_n^{a_n}$ vezető tagja megegyezik f vezető tagjával.

$f_1 := f - c \cdot \sigma_1^{a_1-a_2} \dots \sigma_n^{a_n}$ f_1-gyel ugyanezt csináljuk s.i.t.

Az eljárás véges sok lépés után véget ér, mert adott monomsorrat, ami csökken, csak véges lehet. Ez a halmaz jólrendezett ($\nexists \infty$ csökkenő sorozat).

Tehát f kifejleg előáll.

Egyértelműség: $F_1(\sigma_1, \dots, \sigma_n) = F_2(\sigma_1, \dots, \sigma_n) \rightarrow F_1 = F_2$, mert

ha nem: $F := F_1 - F_2 \neq 0$. De $F(\sigma_1, \dots, \sigma_n)$-ben vagyis $\sigma_1^{t_1} \dots \sigma_n^{t_n}$-ben $x_1^{t_1+\dots+t_n} \dots x_n^{t_n}$ vezető tagját $\rightarrow$ nem tud kiesni $\rightarrow$ nem lehet az x-ek 0 polinomja.

<u>Def.</u>

Legyen $s_k = x_1^k + \dots + x_n^k$. $\quad s_1 = \sigma_1 \quad k \geq 1$

$s_2 = \sigma_1^2 - 2\sigma_2 \quad (\longrightarrow n \geq 2)$

<u>Tétel.</u> (Newton–Girard-formulák) „Elég ezt rögzíteni fo[illegible] hogy mi minden van [illegible]

$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - + \dots + (-1)^{k-1} s_1 \sigma_{k-1} + (-1)^k k \cdot \sigma_k = 0$,

(Girard 1627, Newton 1666) ha $k \leq n$.

(legyen $\sigma_k = 0$, ha $k > n$.)

(legyen $\sigma_0 = 1$, $s_0 = n$.)

$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \dots + (-1)^{n-1} s_{k-n+1}\sigma_{n-1} + (-1)^n s_{k-n}\sigma_n$, ha $k > n$.

(Elég csak a $k \leq n$ alak valójából, és ha $k > n$, felhasználni, hogy $\sigma_k = 0$).

Példa: $s_3 - s_2\sigma_1 + s_1\sigma_2 - 3\sigma_3 = 0$

$s_3 = (\sigma_1^2 - 2\sigma_2)\sigma_1 - \sigma_1\sigma_2 + 3\sigma_3 = \sigma_1^3 - 3\sigma_1\sigma_2 - 3\sigma_3$

B: <u>$k \geq n$</u> $\quad R[x_1, \dots, x_n]$-ben:

$(x - x_1) \cdot \dots (x - x_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \dots + (-1)^n \sigma_n$

Behelyettesítünk x_j-t:

$0 = x_j^n - \sigma_1 x_j^{n-1} + \dots + (-1)^n \sigma_n \quad / \cdot x_j^{k-n}$

$0 = x_j^k - \sigma_1 x_j^{k-1} + \dots + (-1)^n x_j^{k-n} \sigma_n \quad j = 1, 2, \dots, n$ -re $\sum$

$\sum \Rightarrow 0 = s_k - \sigma_1 s_{k-1} + \dots + (-1)^n s_{k-n} \sigma_n$ ✓

Legyen most $k \le n$. $k = n$-re már kijött.
Indukció: $n-1$-re már megvan.

<u>Lemma.</u> Adott egy többváltozós polinom, amiben nincs olyan monomja, amiben $\forall$ változó szerepel. Ha ebben a polinomban bármely valamelyik változót 0-t téve 0-t kapunk, akkor az ~~eredeti~~ eredeti polinom a 0 volt.

B: ha van tag, van olyan tag, amiben vincs x_j $\rightarrow$ megmarad. $\square$

A polinomban nincs olyan tag, amiben $\forall$ változó szerepelne, mert $k \le n$.
$\rightarrow$ teljesül a lemma feltétele.
$x_n = 0$-t innen $\rightarrow$ az indukciós feltevés szerint 0-t kapjuk.
De szimmetrikus $\rightarrow$ bármely x_j-re igaz. $\square$

<u>Tétel.</u> Explicit képlet $s_k(x_1, \dots, x_n)$-re.

$$\begin{vmatrix} \sigma_1 & 1 & & & & \\ 2\sigma_2 & \sigma_1 & 1 & & 0 & \\ 3\sigma_3 & \sigma_2 & \sigma_1 & 1 & & \\ 4\sigma_4 & \sigma_3 & \sigma_2 & \sigma_1 & & \\ \vdots & \vdots & \vdots & \vdots & \ddots & \\ & & & & \sigma_1 & 1 \\ n\sigma_n & \sigma_{n-1} & \sigma_{n-2} & \sigma_{n-3} & \cdots & \sigma_2 \quad \sigma_1 \end{vmatrix} = s_n(x_1, \dots, x_n)$$

($n \times n$-es determináns)

Pl. $s_1 = |\sigma_1| = \sigma_1$

$$s_2 = \begin{vmatrix} \sigma_1 & 1 \\ 2\sigma_2 & \sigma_1 \end{vmatrix} = \sigma_1^2 - 2\sigma_2$$

$$s_3 = \begin{vmatrix} \sigma_1 & 1 & 0 \\ 2\sigma_2 & \sigma_1 & 1 \\ 3\sigma_3 & \sigma_2 & \sigma_1 \end{vmatrix} = \sigma_1^3 + 3\sigma_3 - 3\sigma_1\sigma_2$$

B. Vezessünk egy lineáris egyenletrendszert Newton – Girard alapján!

$$\left.\begin{aligned} \sigma_1 &= 1 \cdot s_1 \\ 2\sigma_2 &= \sigma_1 s_1 - 1 \cdot s_2 \\ 3\sigma_3 &= \sigma_2 s_1 - \sigma_1 s_2 + 1 \cdot s_3 \\ &\vdots \\ n\sigma_n &= \sigma_{n-1} s_1 - \dots + (-1)^n \sigma_1 s_{n-1} + (-1)^{n-1} s_n \end{aligned}\right\}$$

$s_1, -s_2, s_3, \dots, (-1)^n s_{n-1}, s_n$-re mint n ismeretlenre van egy egyenletrendszer

$$\begin{vmatrix} 1 & & & \\ \sigma_1 & 1 & & 0 \\ \sigma_2 & \sigma_1 & 1 & \\ \vdots & & & \ddots \\ \sigma_{n-1} & \sigma_{n-2} & \cdots & \sigma_1 \quad (-1)^{n-1} \end{vmatrix} = (-1)^{n-1}$$ az egyenletrendszer determinánsa

Cramer-szabály: $$s_n = \frac{\begin{vmatrix} 1 & 0 & \cdots & 0 & \sigma_1 \\ \sigma_1 & 1 & \cdots & 0 & 2\sigma_2 \\ \vdots & \sigma_1 & \cdots & 0 & 3\sigma_3 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_{n-1} & \sigma_{n-2} & \cdots & & n\sigma_n \end{vmatrix}}{(-1)^{n-1}}$$ $n-1$ db oszlopcsere $\rightarrow$ a nevező kiesik. $\square$

Legyen $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \quad (a_0 \neq 0)$,
$g(x) = b_0 x^k + b_1 x^{k-1} + \dots + b_{k-1} x + b_k \quad (b_0 \neq 0)$.

Van-e közös gyöke f-nek és g-nek?

$$\left.\begin{aligned} f(x) &= a_0(x-\alpha_1)\cdots(x-\alpha_n) \\ g(x) &= b_0(x-\beta_1)\cdots(x-\beta_k) \end{aligned}\right\}$$ feltéve, hogy az elég nagy testben vagyunk

<u>Def.</u> f és g rezultánsa: $R(f,g) = a_0^k\, g(\alpha_1)\cdot\ldots\cdot g(\alpha_n)$.

A rezultáns pontosan akkor 0, ha van közös gyök.

$$\begin{aligned} R(f,g) &= a_0^k\, g(\alpha_1)\cdots g(\alpha_n) = \\ &= a_0^k\, b_0(\alpha_1-\beta_1)(\alpha_1-\beta_2)\cdots(\alpha_1-\beta_k) \\ &\quad\; b_0(\alpha_2-\beta_1)(\alpha_2-\beta_2)\cdots(\alpha_2-\beta_k) \\ &\quad\; \vdots \\ &\quad\; b_0(\alpha_n-\beta_1)(\alpha_n-\beta_2)\cdots(\alpha_n-\beta_k) = a_0^k b_0^n \prod_{i=1}^{n}\prod_{j=1}^{k}(\alpha_i-\beta_j) \end{aligned}$$

$\Rightarrow \quad R(g,f) = (-1)^{n\cdot k} R(f,g)$: majdnem szimmetrikus.

<u>Tétel.</u> $R(f,f') = (-1)^{\frac{n(n-1)}{2}} \cdot a_0 \cdot D(f)$.

B:
$$\begin{aligned} f'(x) &= a_0\cdot(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n) + \\ &\quad a_0\cdot(x-\alpha_1)(x-\alpha_3)\cdots(x-\alpha_n) + \\ &\quad \vdots \qquad\qquad\qquad\qquad\qquad + \\ &\quad a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{n-1}) \end{aligned}$$

$$\begin{aligned} f'(\alpha_1) &= a_0(\alpha_1-\alpha_2)\cdots(\alpha_1-\alpha_n) \\ f'(\alpha_2) &= a_0(\alpha_2-\alpha_1)\cdots(\alpha_2-\alpha_n) \\ &\vdots \\ f'(\alpha_n) &= a_0(\alpha_n-\alpha_1)\cdots(\alpha_n-\alpha_{n-1}) \end{aligned}$$

$$\begin{aligned} R(f,f') &= a_0^{n-1}\cdot f'(\alpha_1)\cdots f'(\alpha_n) = \\ &= a_0^{n-1}\cdot a_0^n\cdot(-1)^{\binom{n}{2}}\cdot\prod(\alpha_i-\alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}}\cdot a_0\cdot D(f). \checkmark \end{aligned}$$

<u>Tétel.</u> (Sylvester)

$$R(f,g) = \begin{vmatrix} \overbrace{a_0 \quad a_1 \quad \cdots \quad a_n}^{n+1\text{ db}} & \overbrace{0 \quad \cdots \quad 0}^{k-1\text{ db}} \\ 0 \quad a_0 \quad a_1 \quad \cdots \quad a_n & 0 \cdots 0 \\ \vdots & \vdots \\ 0 \quad \cdots \quad 0 \quad a_0 & \cdots \quad a_n \\ b_0 \quad b_1 \quad \cdots \quad b_k & 0 \quad \cdots \quad 0 \\ 0 \quad b_0 \quad \cdots \quad b_k & 0 \cdots 0 \\ \vdots & \vdots \\ 0 \quad \cdots \quad 0 & b_0 \quad b_1 \quad \cdots \quad b_k \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\0\\\vdots\\0\end{matrix}}\right\} k \text{ sor} \\ \left.\vphantom{\begin{matrix}a\\0\\\vdots\\0\end{matrix}}\right\} n \text{ sor} \end{matrix}$$

$$\underbrace{\qquad\qquad}_{n-1} \qquad \underbrace{\qquad\qquad}_{k+1}$$

Példa:

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \frac{1}{a_0} R(f,f') = (-1)^{\frac{n(n-1)}{2}} = \begin{vmatrix} 1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & & & & \vdots \\ 0 & \cdots & 0 & a_0 & \cdots & a_n \\ n & (n-1)a_1 & \cdots & a_{n-1} & 0 & \cdots 0 \\ 0 & na_0 & \cdots & a_{n-1} & 0 & \cdots 0 \\ \vdots & & & & & \vdots \\ 0 & \cdots & 0 & na_0 & \cdots & a_1 \end{vmatrix}$$

↓ 1. sorból a_0-t kiemelve

$$D(ax^2+bx+c) = -\begin{vmatrix} 1 & b & c \\ 2 & b & 0 \\ 0 & 2a & b \end{vmatrix} = (b^2+4ac-2b^2)(-1) = b^2-4ac$$

$$D(ax^3+bx^2+cx+d) = -\begin{vmatrix} 1 & b & c & d & 0 \\ 0 & a & b & c & d \\ 3 & 2b & c & 0 & 0 \\ 0 & 3a & 2b & c & 0 \\ 0 & 0 & 3a & 2b & c \end{vmatrix} = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$

$3ax^2+2bx+c$

B. Indukció n szerint. 2014. 12. 11.

$n = 0$:
$$\begin{vmatrix} a_0 & & & 0 \\ & a_0 & & \\ & & \ddots & \\ 0 & & & a_0 \end{vmatrix} = a_0^k = R(a_0, g) \quad ✓$$

Tfh. n-ig igaz!

$n-1$ fokú polinom: $f^* = a_0 (x-\alpha_1) \cdots (x-\alpha_{n-1}) =$
$$= \underset{\overset{\shortparallel}{a_0}}{a_0^*} x^{n-1} + a_1^* x^{n-2} + \dots + a_{n-2}^* x + a_{n-1}^*$$

$$\begin{array}{c} k \left\{ \begin{array}{c} \\ \\ \\ \\ \end{array} \right. \\ n-1 \left\{ \begin{array}{c} \\ \\ \\ \end{array} \right. \end{array} \begin{vmatrix} a_0 & a_1^* & \cdots & a_{n-1}^* & 0 & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_{n-1}^* & 0 & \cdots & & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & a_0 & \cdots & \cdots & a_{n-1}^* \\ b_0 & b_1 & \cdots & b_k & 0 & \cdots & & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & b_1 & \cdots & & b_k \end{vmatrix} \overset{\text{indukció}}{=} R(f^*, g) = a_0\, g(\alpha_1) \cdots g(\alpha_{n-1})$$

$$f(x) = f^*(x) \cdot (x - \alpha_n) \implies \begin{aligned} a_1 &= a_1^* - a_0 \alpha_n \\ a_2 &= a_2^* - a_1^* \alpha_n \\ &\vdots \\ a_{n-1} &= a_{n-1}^* - a_{n-2}^* \alpha_n \\ a_n &= -a_{n-1}^* \alpha_n \end{aligned}$$

$\cdot\alpha_n +$ $\quad$ $\cdot\alpha_n +$ $\quad$ $\cdots$

$$\begin{vmatrix} a_0 & a_1^* - a_0\alpha_n & a_2^* - a_1^*\alpha_n & \cdots & -a_{n-1}^* \cdot \alpha_n & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1^* - a_0\alpha_n & \cdots & \cdots & -\alpha_{n-1}^*\alpha_n & 0 & \cdots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \cdots & 0 & a_0 & \cdots & \cdots & \cdots & \cdots & -a_{n-1}^*\alpha_n \\ b_0 & b_1 & \cdots & b_k & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & b_0 & \cdots\ b_k \end{vmatrix} = R(f, g) =$$

$$= \begin{vmatrix} a_0 & a_1^* & a_2^* & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1^* & \cdots & a_{n-1}^* & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & \cdots & a_0 & a_1^* & a_2^* & \cdots & a_{n-1}^* \\ b_0 & b_0\alpha_n + b_1 & b_0\alpha_n^2 + b_1\alpha_n + b_2 & \cdots & g(\alpha_n) & g(\alpha_n)\cdot\alpha_n & \cdots & \alpha_n^{n-1} g(\alpha_n) \\ 0 & b_0 & b_0\alpha_n + b_1 & \cdots & \cdots\ g(\alpha_n) & \cdots & & \alpha_n^{n-2} g(\alpha_n) \\ \vdots & & & & & & & \vdots \\ 0 & 0 & \cdots & \cdots & b_0 & b_0\alpha_n + b_1 & \cdots & g(\alpha_n) \end{vmatrix} \cdot\alpha_n - \quad =$$

$$= \begin{vmatrix} a_0 & a_1^* & a_2^* & \cdots & a_{n-1}^* & 0 & \cdots & 0 \\ 0 & a_0 & a_1^* & \cdots & \cdots & a_{n-1}^* & 0 & \cdots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \cdots & 0 & \cdots & a_0^* & \cdots & \cdots & a_{n-1}^* & 0 \\ b_0 & b_1 & b_2 & \cdots & b_k & & & & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & 0 & \cdots & b_0 & b_0\alpha_n + b_1 & \cdots & & & g(\alpha_n) \end{vmatrix} =$$

$$= g(\alpha_n) \cdot R(f^*, g) = R(f, g) \qquad \square$$

Gyakorlat. $R(fg, h) = R(f, h) \cdot R(g, h)$

$R(\Phi_n, \Phi_k) = ?$ (0, 1, −2 vagy primitívvé lesz)

A harmadfokú egyenlet

$ax^3 + bx^2 + cx + d = 0$ $\quad a, b, c, d \in K$ (char $K \neq 2, 3$)

(és K algebrailag zárt)

$\downarrow$

$x^3 + ax^2 + bx + c = 0$ elegendő megoldani

$\rightsquigarrow y = x + \frac{a}{3} \quad \rightarrow \quad y^3 = x^3 + ax^2 + \frac{a^2}{3}x + \frac{a^3}{27}$

$$y^3 + \left(b - \frac{a^2}{3}\right)x + \left(c - \frac{a^3}{27}\right) = 0$$

$$y^3 + \left(b - \frac{a^2}{3}\right)\left(y - \frac{a}{3}\right) + \left(c - \frac{a^3}{27}\right) = 0$$

$$y^3 + \left(b - \frac{a^2}{3}\right)y + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right) = 0$$

$$y^3 + py + q = 0$$

$\downarrow$

$x^3 + px + q = 0$ típusút elegendő megoldani

$\rightsquigarrow x = u + v \qquad (u+v)^3 = u^3 + v^3 + 3uv(u+v)$

$\rightarrow (u+v)^3 - 3uv(u+v) - (u^3+v^3) = 0$

Ha van p, q; hogy $\left.\begin{array}{l} -3(u+v) = p \\ -(u^3+v^3) = q \end{array}\right\}$ $\qquad u^3 + v^3 = -q$, $\quad uv = -\frac{p}{3} \quad \rightarrow \quad u^3v^3 = -\left(\frac{p}{3}\right)^3$

$\rightarrow$ másodfokú u^3, v^3-re: $z^2 + qz - \left(\frac{p}{3}\right)^3 = 0$

$$u^3, v^3 = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

$$\boxed{x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}}$$ CARDANO-képlet

A $\sqrt{\ }$ nem egyértelmű, de nem baj, mert egymás ellentettjei, és szimmetrikusan szerepelnek.

A $\sqrt[3]{\ }$-nél ha az elsőnél azt egyszer választom, az meghatározza a másikat. Az kell nagyon, hogy $uv = -\frac{p}{3}$ teljesüljön.

$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

első harmadik egységgyök

$$\boxed{\begin{aligned} \alpha_1 &= u + v \\ \alpha_2 &= \omega u + \omega^2 v = -\tfrac{1}{2}(u+v) + \tfrac{\sqrt{3}}{2}i\,(u-v) \\ \alpha_3 &= \omega^2 u + \omega v = -\tfrac{1}{2}(u+v) - \tfrac{\sqrt{3}}{2}i\,(u-v) \end{aligned}}$$ $\mathbb{C}$-ben

Példa. $x^3 + 6x^2 + 21x + 52 = 0$

$y = x + 2$

$y^3 + 9y + 26 = 0 \qquad p = 9, \quad q = 26$

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} = \sqrt[3]{-13 + \sqrt{13^2 + 3^3}} = \sqrt[3]{-13 + 14} = 1$$

$v = -3 \qquad \rightarrow \quad \alpha_1 = -2 \quad \rightarrow \quad x_1 = -4$

$\alpha_2 = 1 + 2\sqrt{3}\,i \quad \rightarrow \quad x_2 = -1 + 2\sqrt{3}\,i$

$\alpha_3 = 1 - 2\sqrt{3}\,i \quad \rightarrow \quad x_3 = -1 - 2\sqrt{3}\,i$

$$D(x^3+px+q) = -\begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix} = -\begin{vmatrix} 1 & 0 & p & q \\ 0 & -2p & -3q & 0 \\ 3 & 0 & p & 0 \\ 0 & 3 & 0 & p \end{vmatrix} = -\begin{vmatrix} -2p & -3q & 0 \\ 0 & -2p & -3q \\ 3 & 0 & p \end{vmatrix} =$$

$$= -(27q^2 + 4p^3) = -4p^3 - 27q^2$$

$$\Rightarrow \quad x = \sqrt[3]{-\frac{q}{2} + \sqrt{D/(-108)}} + \sqrt[3]{-\frac{q}{2} - \sqrt{D/(-108)}}$$

Példa. $x^3 - 3x - 18 = 0$

$$u + v = \sqrt[3]{9 + \sqrt{80}} + \sqrt[3]{9 - \sqrt{80}} = 3$$ $\longrightarrow$ néha a megoldás alakja bonyolultabb, mint ami valójában

Legyen $x^3 + px + q \in \mathbb{R}[x]$.

1. $\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 > 0 \quad (D<0) \longrightarrow$ 1 valós és 2 különböző komplex konjugált gyök.
2. $\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 = 0 \quad (D=0) \longrightarrow u = v = \sqrt[3]{-\frac{q}{2}} \in \mathbb{R}$ $\quad \alpha_1 = 2u$, $\alpha_2 = \alpha_3 = -u$

   Kétszeres, sőt $u=0$, azaz $q=0$ esetén háromszoros gyök.
3. $\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 < 0 \quad (D>0) \longrightarrow$ negatív a $\sqrt{\ }$ alatt, de 3 valós gyök

   CASUS IRREDUCIBILIS

   $\rightarrow p<0$ $\qquad u^3 = -\frac{q}{2} + i\sqrt{-\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}$ $\qquad |u^3| = \sqrt{\left(-\frac{q}{2}\right)^2 + -\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3} = \sqrt{-\left(\frac{p}{3}\right)^3}$

   $\rightarrow |u| = \sqrt{\frac{p}{3}} \longrightarrow u\bar{u} = -\frac{p}{3}$

   $u = a + bi \longrightarrow v = \bar{u} = a - bi$ $\qquad \left.\begin{array}{l} \alpha_1 = 2a \\ \alpha_{2,3} = -a \pm b\sqrt{3} \end{array}\right\} \in \mathbb{R}$

   $u = r(\cos\varphi + i\sin\varphi)$ $\qquad x_1 = 2r\cos\varphi$, $x_{2,3} = 2r\cos(\varphi \pm 120°)$

Példa. $x^3 - 24x - 32 = 0 \longrightarrow \frac{p}{3} = -8, \ \frac{q}{2} = -16$

$$u = \sqrt[3]{16 + \sqrt{-256}} = \sqrt[3]{2+2i}$$
$$v = \sqrt[3]{16 - \sqrt{-256}} = \sqrt[3]{2-2i}$$

$\longrightarrow$
$$\alpha_1 = 2\left(\sqrt[3]{2+2i} + \sqrt[3]{2-2i}\right) = 2w$$
$$\alpha_2 = -w + \sqrt{3}i\bar{w} = 4\sqrt{2}\cos 150°$$
$$\alpha_3 = -w - \sqrt{3}i\bar{w} = 4\sqrt{2}\cos 135° = -4$$
$$= 4\sqrt{2}\cos 255° =$$
$$= 4\sqrt{2}\cos 75°$$

$$(x+4)(x^2 - 4x - 8)$$

$\cos 15° = \frac{\sqrt{6}+\sqrt{2}}{4}$ is kijön ebből

Tartaglia ($\approx$1530)

Cardano 1545 Ars magna

del Ferro ($\approx$1510) $x^3 + mx = n$ alakúakat megoldotta $(m, n > 0)$

Ferrari C. tanítványa $\longrightarrow$ negyedfokú : harmadfokúra eltüntethető : $x^4 + ax^2 + bx + c = 0$

$x = u + v + w$ alakban $\longrightarrow$ visszavezetés harmadfokúra :

harmadfokú resolvens