VII/11 $\quad K \leq L \ni \alpha \quad f(\alpha)=0 \quad gr(f)=n \quad f\in K[x]$

<u>Áll.</u> K feletti fok $\leq n$, ugyanis oszthatóság $gr_K(\alpha) \mid n$.

12. $f(\alpha)=0 \Rightarrow m_\alpha \mid f$

és $m_\alpha \leq gr(f)=n$ ✓

Példát nem lehetne $f(x) = m_\alpha(x)(x-1)$

$K = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ $\quad \varepsilon = \cos 120° + i\sin 120°$ pl. 3. egységgyök.

x^3-2 felbontási teste $\mathbb{Q}$ fölött

x^3-2 gyökei $\sqrt[3]{2}, \sqrt[3]{2}\varepsilon, \sqrt[3]{2}\varepsilon^2$

$K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\varepsilon, \sqrt[3]{2}\varepsilon^2) = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$

6 fokú $\mathbb{Q}$ fölött

$\varepsilon = \frac{\sqrt[3]{2}\varepsilon}{\sqrt[3]{2}}$

$|K:\mathbb{Q}| = 6$ $\quad$ 2 + 3.

$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[3]{2})(\varepsilon)$ with degrees 3 and 2

$\alpha = (\varepsilon\sqrt[3]{2})$ $\quad$ α foka $\mathbb{Q}(\sqrt[3]{2})$ fölött 2

α foka $\mathbb{Q}$ fölött 3 $\quad (x^3-2)$

x^3-2 irred $\mathbb{Q}$ fölött

valós!

x^2+x+1 irred $\mathbb{Q}(\sqrt[3]{2})$ fölött (2. fokú, nincs gyöke)

$\mathbb{Q}(\sqrt[3]{2})(\alpha) = \mathbb{Q}(\sqrt[3]{2})(\varepsilon)$

$\uparrow$ 3 fokú $\mathbb{Q}$ fölött.

$\alpha = \varepsilon\sqrt[3]{2}$

$\uparrow$ 6 fokú $\mathbb{Q}$ fölött

$\varepsilon\sqrt[3]{2}$ min. pol.-ja NEM x^3-2 lesz $\mathbb{Q}(\sqrt[3]{2})$ fölött, hanem

$x^3-2 = (x-\sqrt[3]{2})\,($ 2. fokú $)$

$\mathbb{Q}(\sqrt[3]{2})$ fölött

$\uparrow$ $\mathbb{Q}(\sqrt[3]{2})$ együtthatós

$\mathbb{Q}(\sqrt[3]{2})\varepsilon$ min. pol.

$(x-\varepsilon\sqrt[3]{2})(x-\varepsilon^2\sqrt[3]{2})$

---

20 $f \in \mathbb{Q}[x]$ n. fokú

felb. teste max hányadfokú?

n^n? (n gyök tbőv $\leq n$. fokú)

f gyöke $\alpha_1, \dots, \alpha_n$

$\mathbb{Q}(\alpha_1) \geq \mathbb{Q}$ ($\leq n$ fokú) $\quad \alpha_2$? $\mathbb{Q}(\alpha_1)$ fölött $\downarrow$ $\alpha_2, \dots, \alpha_n$ a gyökei $g \in \mathbb{Q}(\alpha_1)[x]$.

$f(x) = (x-\alpha_1)\,g(x)$ (g: $n-1$)

$\mathbb{Q}(\alpha_2,\alpha_1) \geq \mathbb{Q}(\alpha_1)$ ($\leq n-1$.)

α_3 foka $\mathbb{Q}(\alpha_1, \alpha_2) \leq n-2$

$f(x) = (x-\alpha_1)(x-\alpha_2)\, h(x)$ $\qquad h \in \mathbb{Q}(\alpha_1, \alpha_2)[x]$

↗ $n-2$ fokú

$\boxed{\leq n!}$ ← általában $\qquad x^3-2$ -re 6.

Mese. → S_n Aut $n!$, ha semmilyen rejtett öf. nincs a gyökök között!

19 $\quad x^3-2 \to \boxed{6}$

$x^4-2 \qquad \mathbb{Q}(\underset{\alpha_1}{\sqrt[4]{2}}, \underset{\alpha_2}{i\sqrt[4]{2}}, \underset{\alpha_3}{i^2\sqrt[4]{2}}, \underset{\alpha_4}{i^3\sqrt[4]{2}}) \geq \mathbb{Q}$

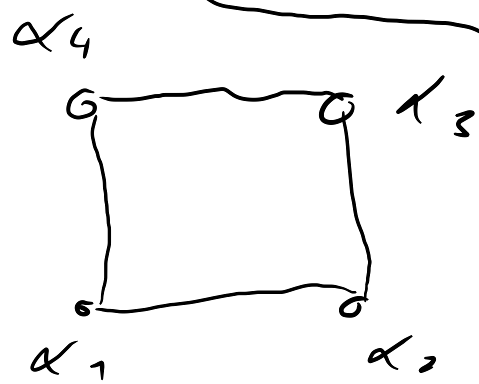
$\boxed{8}$ $\qquad = \mathbb{Q}(\sqrt[4]{2}, i) \underset{2}{\geq} \mathbb{Q}(\sqrt[4]{2}) \underset{4}{\geq} \mathbb{Q}$

nem $24 = 4!$ $\qquad$ x^2+1 $\mathbb{R}$ felett irred $\qquad$ x^4-2 Sch-E.

Rejtett öf

$\alpha_1 + \alpha_3 = 0$

$\alpha_2 + \alpha_4 = 0$



(D_4 Galois-csop.)

mese!

$x^6 - 2$ ε 6. primitív egységgyök

$\mathbb{Q}(\sqrt[6]{2}, \varepsilon\sqrt[6]{2}, \dots, \varepsilon^5(\sqrt[6]{2})) = \mathbb{Q}(\sqrt[6]{2}, \varepsilon)$

$\varepsilon = \cos 60^\circ + i \sin 60^\circ = 1/2 + \frac{\sqrt{3}}{2} i \notin \mathbb{R}$

$\Rightarrow$ $6 \cdot 2 = \boxed{12}$ min pol $x^2 - x + 1 = \Phi_6(x)$

$x^n - 1$ ε primitív n. egységgyök

$\mathbb{Q}(\varepsilon, \varepsilon^2, \dots, \varepsilon^n) = \mathbb{Q}(\varepsilon)$

ε min. pol $\Phi_n(x)$ fokszám $\boxed{\varphi(n)}$

IRREDUCIBILITÁS, TESI

$(x^2 - 2)(x^2 - 3)$

$\mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ fok $\boxed{4}$

(volt feladat)

$(x^2 - 2)(x^3 - 2)$ HF: $x^6 - 2$ cs $(x^2 - 2)(x^3 - 2)$ felsbb test ugyanaz-e?

$\mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt[3]{2}, \varepsilon\sqrt[3]{2}, \varepsilon^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{2}, \varepsilon)$ $\boxed{12}$

$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}, \sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \varepsilon)$

$\uparrow$ 6, mert $(2,3) = 1$ 2 mert ε nem valós, de gyöke $x^2 + x + 1$-nek

13. $a+bi$ alg $\Leftrightarrow$ a, b algebrai $\quad a,b \in \mathbb{R}$.

$\Leftarrow$ i algebrai x^2+1-nek gyöke

Alg. vagy test $\Rightarrow$ a, b, i benne van

$\Rightarrow a+bi$ is benne van.

$\Rightarrow \alpha = a+bi$ $f(x)$-nek gyöke, $f \in \mathbb{Q}[x]$, $f \neq 0$.

α gyöke $f(x)$-nek $\Rightarrow$ $\bar{\alpha}$ is $\Rightarrow$ $\bar{\alpha}$ is algebrai

$\alpha + \bar{\alpha} = 2a$ is, $\Rightarrow$ a alg $\Rightarrow bi$ alg

i alg $\Rightarrow b$ is alg.

---

15. alg + transzcendens = transzcendens, mert

$\alpha + \beta$ Ha $\nearrow$ alg. lenne

$\beta = (\alpha+\beta) - \alpha$ is alg. lenne $\lightning$. stb.

---

16. $\mathbb{Q} \subseteq K$ K alg. zárt? $X^{n+1}-2$ $\sqrt[n+1]{2} \notin K$

vége fogva n

$\nearrow$ minden K-ban a gyöke.

$n+1$ a fok

K alg. zárt $\Leftrightarrow$ $\forall$ alg. bővítése elsőfokú.

K alg. zárt $K \leq L$ alg. bővítés
$\alpha \in L$, $\alpha \notin K$
ua. izomf K felett
≥ 2-fokú ξ.
$\Rightarrow L \geq K$ elsőfokú.

Rögzítsünk: $f \in K[x]$ irred
$K \leq K(\alpha)$ α jobb f-nek.
$\nearrow$ alg. $=$, elsőfokú $=$ $\alpha \in K$ $\Rightarrow$ $\deg f = 1$.

K véges test, nem alg. zárt.
$K = \{a_1 - a_n\}$
$f(x) = (x-a_1) \dots (x-a_n) + 1$
nincs gyöke K-ban ξ.
ei, főleg nem 1

U11/16

HF VII/17,18.

9 elemű test $9 = 3^2$ $|K|$

Részteste $L \leq K$ $3^k = |L|$ $k|2$.

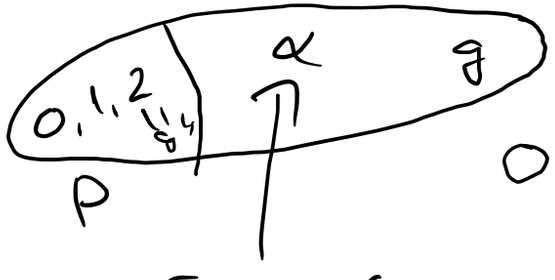
↳ $\mathbb{Z}_3 = \{0,1,2\} = P$ $k = 2, 1$

egész.

Multiplikatív csoport 8 elemű ciklikus

$g, g^2, g^3, g^4, g^5, g^6, g^7, g^8 = 1$

rendek 8, 4, 8, 2, 8, 4, 8, 1



$g - 3 = 6$ elem rendjei 4 vagy 8.

K $g^2 = 2$ ← kézdőelem

$o(2) = 2$

$2^2 \equiv 1 \ (3)$

$2 \not\equiv 1 \ (3)$

$\boxed{2 = g^4}$

$P(\alpha) = K$

$\alpha \notin P$

$\Rightarrow \alpha$ 2-féle.

$\varphi(8) = 4$ db 8 rendű

$\varphi(4) = 2$ db 4 rendű.

$X^9 - X = X(X-1)(X-2)(\quad)(\quad)(\quad)$

$\mathbb{Z}_3$ felett

↗ ↘ 2. fokú irred $\mathbb{Z}_3$ felett.

Hány 2. fokú irred elem?

3 db elsőfokú a mi. pol $0, 1, 2$

$9 - 3 = 6$ másodfokú — " — $x, x-1, x-2$

Ø 2. fokúból 2 jó van IC-ben

$6/2 = \boxed{3 \text{ db}}$

---

2. fokú irred $\mathbb{Z}_3$ fölött $x^2 + ax + b$

$b \neq 0$

$0, 1, 2$ nem jó

$=$

-1

$1 + a + b \neq 0$ nem jó !

$1 - a + b = 0$ — " — -1

$b = 1 \Rightarrow a = ?$

$b = 2$

$\boxed{x^2 + 1 \quad \text{jó}}$

x^2+1 : ennek kell $\mathbb{C}$ lenni.

„i" a régi ($i^2=-1$)

$K = \{ a+bi \mid a, b \in \mathbb{Z}_3 \}$ 9 db.

$i = x + (x^2+1)$

$x^2+1 = (x+i)(x-i)$

$i, \quad -i \quad (-i)$

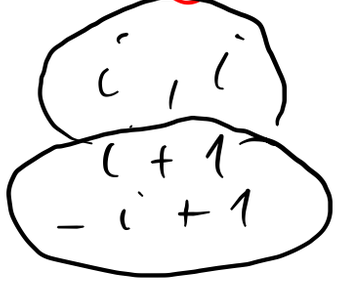
Frobenius : $\alpha \mapsto \alpha^3$ automorfizmus

permutálja a $\mathbb{Z}_3(x)$ feletti
2 db gyökét

$i^3 = -i$

= KOMPLEX KONJUGÁLÁS

Jelen test = Gauss-egészek mod 3.



Min. pol — „ — x^2+1, $(x-1)^2+1$ stb.

$= x^2 - 2x + 2 = x^2 + x - 1$.

3\. Hány négyzet- és köbelem van a 27 elemű testben?

Unelem köbelem

$|K| = 27 = 3^3$

Ez csoportelmélet!

$K - \{0\} = G \cong \mathbb{Z}_{26}^{+}$

$$\left[\begin{array}{ll} 2x \equiv y & (26) \\ 3x \equiv y & (26) \end{array}\right]$$

$\varphi(x) = x^2$

$\psi(x) = x^3$

$|G| = 26$

$\Rightarrow \operatorname{Im}\psi = G$

$0 = 0^2 = 0^3$

$\{2x \mid x \in G\}$

$\{3x \mid x \in G\}$

$\mathbb{Z}_p$-ben négyzetelem
KVADRATIKUS MARADÉK

$x^2 = 1 \iff$
$x = \pm 1$
$-1 \neq 1$
$\mathbb{Z}_3$-ban

négyzetelem

$\frac{26}{2} + 1$ ↗ nulla

$G \to G$ csoporthomomorfizmus

$|\operatorname{Im}\varphi| = ?$ $\quad \operatorname{Im}\varphi \cong G/\operatorname{Ker}\varphi$

$|\operatorname{Im}\psi| = ?$ $\quad \operatorname{Im}\psi \cong G/\operatorname{Ker}\psi \leftarrow 1$

$\operatorname{Ker}\varphi = ?$ $\quad x^2 = 1$

$\operatorname{Ker}\psi = ?$ $\quad x^3 = 1$

26 elemű ciklikus

$\Rightarrow o(x) \mid (3, 26) = 1$

$\Rightarrow x = 1$

$|K| = 27$

$x^4 + x^3 + x^2 + x + 1$ ← NINCS GYÖKE.

$x^2 - x + 1$ Lucy Lol?

$$\frac{x^5 - 1}{x - 1} = \Phi_5(x)$$

$$x^2 - x + 1 = \Phi_6(x) \mid x^6 - 1$$

α gyöke $x^4 + x^3 + x^2 + x + 1$ -nek

$\Rightarrow \alpha^5 = 1$ de $\alpha \neq 1$ mert

$1 + 1 + 1 + 1 + 1 = 5 \not\equiv 0 \pmod 3$.

$\Rightarrow o(\alpha) = 5$
a rendje

$K^\times \cong \mathbb{Z}_{26}^+$

$5 \nmid 26$ mivel 5 prím.

$x^2 - x + 1$ IF

IF VIII / 4, 5, 6, 10