$\sqrt{3+4i}$ ① felett

4 felbővítése's $\sqrt{3+4i} = \pm(2+i)$ 12

$\mathbb{Q} \leq \mathbb{Q}(i) \leq \mathbb{Q}(\sqrt{3+4i})$

2 $\quad \leq 2$

x^2+1 $\quad x^2-(3+4i) \overset{\text{NEM}}{=} (x-(2+i))$ onfoja

irred $\quad$ irred-e $\mathbb{Q}(i)$ felett

$\sqrt[6]{5}$ foka $\mathbb{Q}(\sqrt{5})$ felett

$\mathbb{Q} \leq \mathbb{Q}(\sqrt{5}) \leq \mathbb{Q}(\sqrt[6]{5}, \sqrt{5}) = \mathbb{Q}(\sqrt[6]{5})$

x^2-5 $\quad x^6-5$ $\quad$ ↑

irred $\quad \leq 6$

12 $\quad x^3-\sqrt{5}$ $\quad (\sqrt[6]{5})^3 = \sqrt{5}$ 3

$x \leq 3$

Part 3: $\mathbb{Q} \leq \mathbb{Q}(\sqrt[6]{5})$ foka 6

x^6-5 Sch-E

$2 \cdot x = 6$ $\quad \Rightarrow x = 3$

$x \leq 3$

$x^{200} - 1$ összetett test

$\mathbb{Q} \leq \mathbb{Q}(\varepsilon)$ ε pr. 200. egységgyök

$\exists$ ct. $\forall$ j-re.

$\varphi(200) = \varphi(8)\varphi(25) = 4 \cdot 20 = \boxed{80}$

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

$\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \varepsilon)$ ε pr. 3 e.gy. $\boxed{12}$

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

$\leq \mathbb{Q}(\sqrt[6]{3})$ ε nem valós $x^2 + x + 1$-nek gyöke

$[6, 3] = 1$

$a + bi + cj + dk = \alpha$ $\alpha^{-1} = ?$

$\bar{\alpha} = a - bi - cj - dk$

$\alpha\bar{\alpha} = N(\alpha) = a^2 + b^2 + c^2 + d^2$

$N(\alpha\beta) = N(\alpha) N(\beta)$ $\overline{\alpha\beta} = \bar{\beta}\,\bar{\alpha}$.

$\alpha^{-1} = ?$ $\qquad \alpha\bar{\alpha} = N(\alpha)$

$\alpha \cdot \left(\frac{\bar{\alpha}}{N(\alpha)} \right) = 1$

$\Rightarrow$ valós!

$$\boxed{\alpha^{-1} = \frac{\bar{\alpha}}{N(\alpha)}}$$ mint $\mathbb{C}$-ben.

$\alpha^2 = ?$ $\qquad$ mi. pl. $= ?$

$x^2 + 1$ megoldásai? $\qquad x^2 + r$ megoldásai:

$r > 0$ valós.

z megoldás $\qquad z^2 = -r$

$N(z^2) = N(-r) = r^2 \qquad N(z) = r, \; r > 0$ valós

$N(z)^2 \qquad \Rightarrow \boxed{N(z) = r}$

$z^2 = -r = -N(z) = -z\bar{z} \qquad z \neq 0$

$\Rightarrow z = -\bar{z}$ azaz (z tiszta), vagy zérus 0.

$a + bi + cj + dk = -(a - bi - cj - dk) \Leftrightarrow a = 0.$

Megfordítva: Tfh $N(z) = r$, z tiszta (azaz $\mathrm{Re}(z) = 0$)

$\Rightarrow z = -\bar{z} \Rightarrow z^2 = -z\bar{z} = -N(z) = r$.

$x^2 + r = 0$ megoldása.

Ha m.p.h. z valós $\Rightarrow x - z$ a min.pol.

z nem valós: $w = z - \mathrm{Re}(z)$ tiszta

$w^2 = -N(w)$

$(z - \mathrm{Re}(z))^2 = -N(w)$

z gyöke $(x - \mathrm{Re}(z))^2 + N(z - \mathrm{Re}(z)) \in \mathbb{R}[x]$

Ez a min.pol, mert $z \notin \mathbb{R} \Rightarrow$ min.pol ≥ 2. fokú

$\mathbb{Z}_{17}$ főideál x^2+1, x^2-3 → $\mathbb{Z}_{17}$ mező

fels. lesz?

α, β gyök $\Rightarrow$ additív főideál

$\Rightarrow \alpha+\beta \in$ alaptest. (U. igaz!)

(2 főideál összege maradék!)

Ha van gyök $\mathbb{Z}_{17}$-ben $\rightarrow \mathbb{Z}_{17}$

nincs → 2 főideál összes (mar. mod)

x^2+x+1 $\overline{F}_{11}$, $\overline{F}_{125}$ főideál? $\overline{F}_{17^2}$

$x^2 \equiv -1 \ (17)$ $x^2 = 16 \ (17) \Rightarrow x \equiv \pm 4 \ (17)$

16 KVADRATIKUS MARADÉK mod 17.

$x^2 \equiv 3 \ (17)$ megoldható-e?

I. mo. 3 ∀ Fermat-prímre primitív gyök.

⇒ rendje 16

Kv. maradék az, ami a primitív gyök páros hatványa.

$\varphi(17) = 16$

$O_{17}(3) \mid 16$

Ha nem 16, akkor 8 osztója, de $3^{8} \equiv 1 \ (17)$ NEM!

II. mo. Kv. reciprocitás

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right)(-1)^{\left(\frac{17-1}{2}\right)}(-1)^{\left(\frac{3-1}{2}\right)}$$

$$= \left(\frac{2}{3}\right) = -1$$

x^2+x+1

$\|$

$\frac{x^3-1}{x-1}$

$\mathbb{F}_{121}$

$\mathbb{F}_{125}$

fels. test $\overline{\mathbb{F}_{121}}$

$\mathbb{F}_{121} = \mathbb{F}_{5^2} = \mathbb{F}_{5^6}$.

Ha van α gyöke

$\Rightarrow \alpha^3 = 1 \Rightarrow o(\alpha) = 3$ vagy 1

Ha $o(\alpha) = 1 \Rightarrow \alpha = 1$

1 gyöke-e x^2+x+1-nek?

VIGYÁZAT $1+1+1=0$ lehetséges

$\Leftrightarrow$ karakterisztika $= 3$!

[$\mathbb{Z}_3$ fölött $x^2+x+1 = (x-1)^2$]

$3 \nmid 121, 125 \Rightarrow \alpha$ rendje 3. $\Rightarrow 3 \mid |K| - 1$

Legalább.

$\mathbb{F}_{121}$-ben 7-e 3 rendű?

$3 \mid 121-1 = 120$ ✓ ciklikus $\Rightarrow \exists$ 3 rendű.

$3 \nmid 125-1 \Rightarrow x^2+x+1$ irred $\Rightarrow$? főid.

$\varphi(3) = 2$.

$x^{11}-1$ felb. teste $\mathbb{Z}_2$ fölött

$\mathbb{Z}_{11}$ fölött $\mathbb{Z}_{11}$

$\mathbb{Z}_{11}$ fölött $x^{11}-1=(x-1)^{11}$

$\Rightarrow$ egyetlen gyöke az 1, $\mathbb{Z}_{11}$-ben gyöktényezős bontás.

$\alpha \in K \geq \mathbb{Z}_2$ $\quad o(\alpha) \mid 11 \Rightarrow 1$ vagy 11

$\alpha^{11}=1$ $\qquad \alpha=1$

De $x^{11}-1 \neq (x-1)^{11}$ $\mathbb{Z}_2$ fölött (miért?)

$\Rightarrow$ van még olyan gyök is, aminek 11 a rendje.

[$x^{11}-1$-nek nincs többszörös gyöke $\mathbb{Z}_{11}$ fölött, mert deriváltja $11x^{10}$: csak a 0 gyöke, de az nem gyöke $x^{11}-1$-nek].

[Van: $x^{11}-1=(x-1)(1+x+\dots+x^{10})$ — 1 nem gyöke]

$\mathbb{Z}_2 \subseteq K = ?$ $\quad \exists\, \alpha \in K$
$o(\alpha) = 11.$

$\mathbb{F}_{2^{10}}$

$11 \mid |K| - 1 \qquad |K| = 2^x$

$2^x \equiv 1 \ (11)$ $\quad x$ jó kitevő 2-nek mod 11.

$o_{11}(2) \mid x$ $\qquad o_{11}(2) \mid \varphi(11) = 10$

lehet $1, 2, 5, 10$

11 osztója-e $2^1-1,\ 2^2-1,\ 2^5-1 = 31$ — nem.

$\Rightarrow o_{11}(2) = 10 \Rightarrow \boxed{10 \mid x}$

$x = 10$? $\quad K = \mathbb{F}_{2^{10}}$ jó-e? $\qquad x \geq 10.$

$\mathbb{F}_{2^{10}}^{\times} \cong \mathbb{Z}_{2^{10}-1}$ rendje 11-gyel osztható

$\Rightarrow \varphi(11) = 10$ db 11 rendű elem.

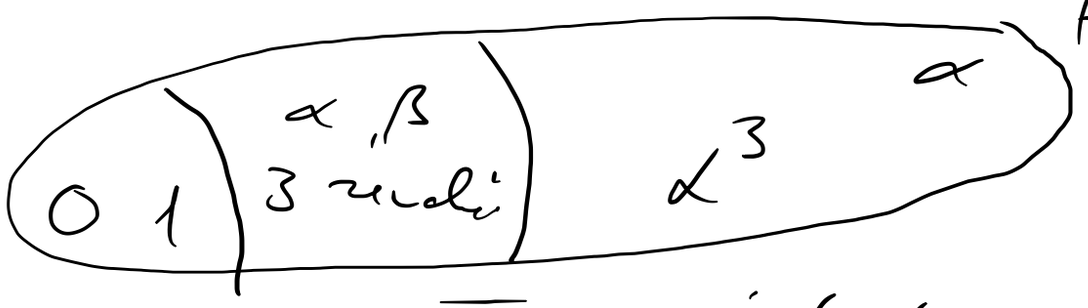
Ekkor $x^{11}-1$ tehát gyöktényezőkre bomlik,

generálják is a bővítést, mert $\mathbb{Z}_2 \subseteq L \subsetneq K = \mathbb{F}_{2^{10}}$
(benne 11 rendű ε)

$\mathbb{F}_{16}$ a speciál $\mathbb{F}_{16}^\times$ - ot.

$O(\alpha) = 15$.

α^3 řeší a primitivní?



$\mathbb{F}_{16}$ $\quad 16 = 2^4$

$1, 2, 4 \mid 4$

$\mathbb{F}_2$ $\quad \mathbb{F}_4$ primitivní

$|\mathbb{F}_4^\times| = 3$

$O(\alpha^3) = \frac{O(\alpha)}{(O(\alpha), 3)} =$

$= \frac{15}{(15, 3)} = \boxed{5}$

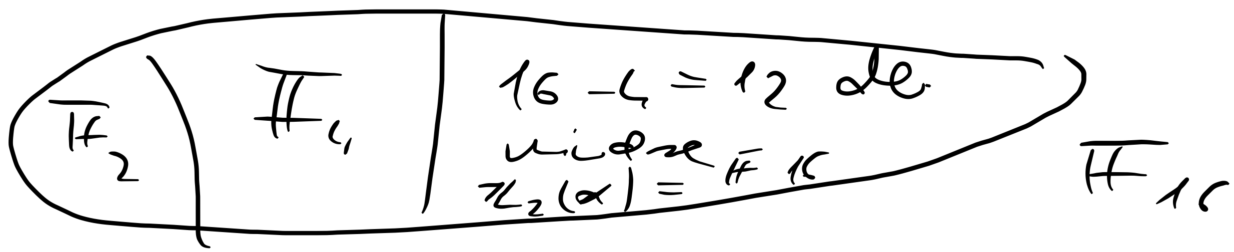
$\alpha^3 \in \mathbb{F}_4^\times$

$\mathbb{Z}_2(\alpha^3) =$ ejóva $= 3$ a řeší $= |\mathbb{F}_{2^4} : \mathbb{F}_2| = 4$

(nelze volit a min. pol-ic).

$\mathbb{Z}_2$ fölött 8 fokú ?
irred 12 fokú

4 fokú 3 db
van-e?

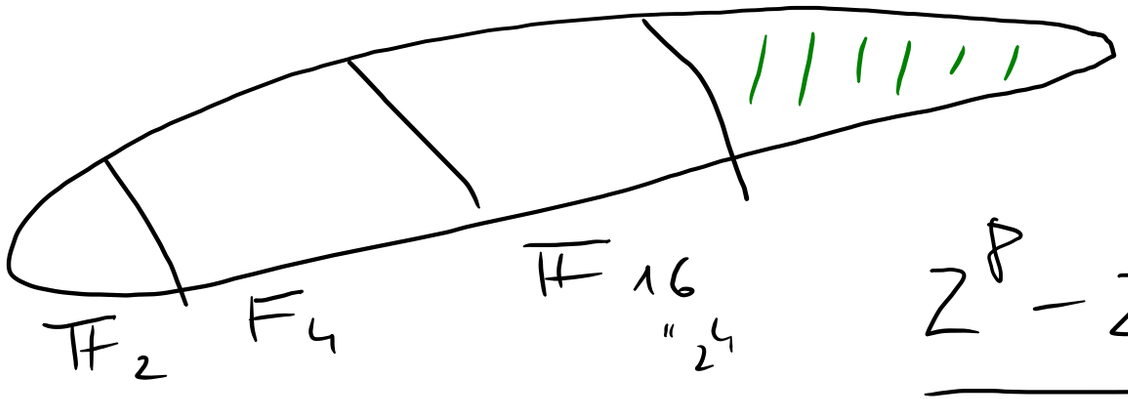


f 4. fokú irred
nincs többszörös gyöke
(véges test fölött
irred pol-nak
nincs többszörös
gyöke)

$\mathbb{F}_2$ feletti felb. teste 4 fokú
ha 1 gyökkel bővítés.
De ebben már lineáris
tényezőkre bomlik mert véges
testből ∀ bővítés normális

$$\frac{16-4}{4} = \boxed{3}.$$

→ ennyi van ∀ irred-ből

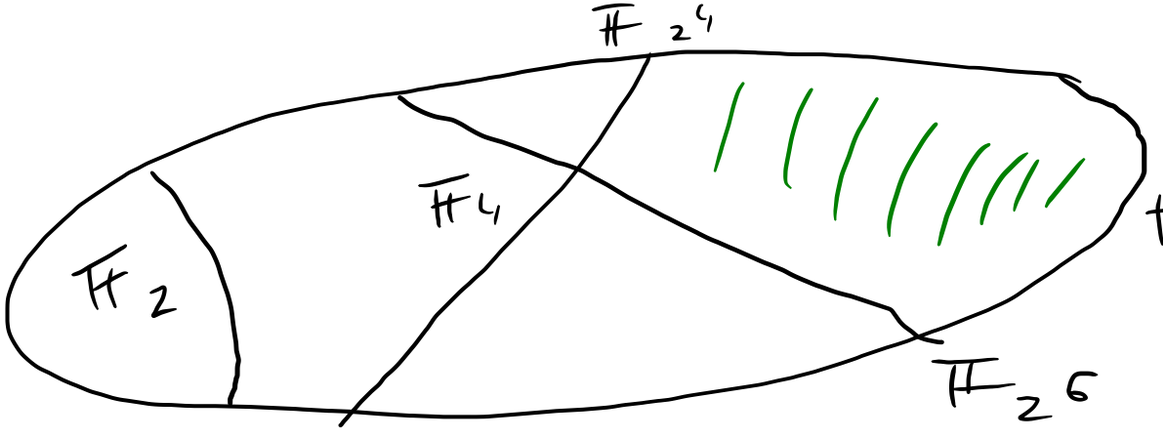


$\mathbb{F}_{2^8}$

1, 2, 4, 8 | 8

$$\frac{2^8 - 2^4}{8} = 2^5 - 2 = \boxed{30}$$

$\mathbb{F}_{2^{12}}$ 1, 2, 3, 4, 6, 12 | 12 $(6,4) = 2$



$\mathbb{F}_{2^6} \cap \mathbb{F}_{2^4} = \mathbb{F}_{2^2}$

$$\frac{2^{12} - 2^4 - 2^6 + 2^2}{12} = \boxed{335}$$