Naj bo $f(x) \in F[x]$.

Razpadno polje je najmanjša razširitev E polja F, da $f(x)$ razpade nad E na linearne faktorje.

Naj bodo $\alpha_1, \ldots, \alpha_k$ vse ničle $f(x)$.

$\Rightarrow E = F(\alpha_1, \ldots, \alpha_k)$

Pojasni, zakaj je $\mathbb{Q}(\sqrt{2})$ razpadno polje vsakega izmed polinomov x^2-2, $3x^3-6x$, $x^4-3x^2+2 \in \mathbb{Q}[x]$.

- $f(x) = x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$

  Ničli: $\sqrt{2}, -\sqrt{2}$

  $E = \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$

- $g(x) = 3x^3-6x = 3x(x^2-2)$

  $E = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, 0) = \mathbb{Q}(\sqrt{2})$

- $h(x) = x^4-3x^2+2 = (x^2-2)(x^2-1) = (x-\sqrt{2})(x+\sqrt{2})(x-1)(x+1)$

  $E = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, 1, -1) = \mathbb{Q}(\sqrt{2})$

Pojasni, zakaj je $\mathbb{Q}(\sqrt{2},\sqrt{3})$ razpadno polje $x^4-5x^3+6 \in \mathbb{Q}[x]$.

$f(x) = x^4-5x^2+6 = (x^2-2)(x^2-3)$

$E = \mathbb{Q}(\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$

Označimo $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ primitivni 3. koren enote. Pokaži, da je $\mathbb{Q}(\sqrt[3]{2}, \omega)$ razpadno polje polinoma $x^3-2 \in \mathbb{Q}[x]$ in poišči njegovo stopnjo nad $\mathbb{Q}$.

$a^3-b^3 = (a-b)(a^2+ab+b^2)$

$x^3-2 = (x-\sqrt[3]{2})(x^2+\dots)$

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

($\subseteq$) Očitno.

($\supseteq$) $\sqrt[3]{2} \in F$

$\omega = \frac{\omega\sqrt[3]{2}}{\sqrt[3]{2}} \in F$

$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega) = 6$

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$: 3 $\quad$ $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$: ≤ 2

x^3-2 nerazcepen nad $\mathbb{Q}$
x^2+x+1 nek polinom

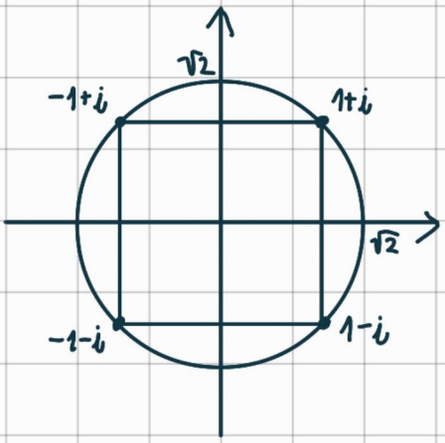
Pokaži:

a) $\mathbb{Q}(i)$ je razpadno polje polinoma $x^4+4 \in \mathbb{Q}[x]$

b) $\mathbb{Q}(\sqrt[4]{2}, i)$ je razpadno polje polinoma $x^4+2 \in \mathbb{Q}[x]$

c) $\mathbb{Q}(\sqrt{2}, i)$ je razpadno polje polinoma $x^4+1 \in \mathbb{Q}[x]$

a) $x^4 - i^2 \cdot 4 = (x^2 - i\cdot 2)(x^2 + i\cdot 2) = (x-1-i)(x-1+i)(x+1-i)(x+1+i)$



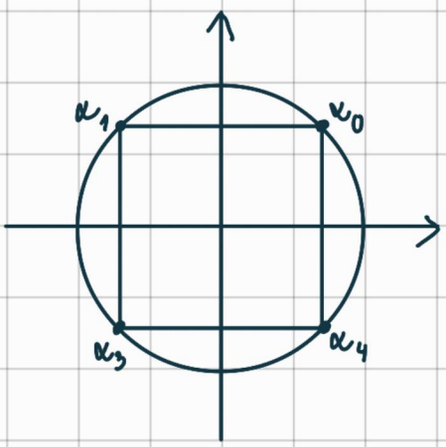
$\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = \sqrt{2}\, e^{i\frac{\pi}{4}} = \sqrt{2}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = 1+i$

$\mathbb{Q}(1+i, 1-i, -1+i, -1-i) = \mathbb{Q}(i)$

($\subseteq$) Očitno.

($\supseteq$) $i = \frac{(1+i)(-1+i)}{2} \in F$

b)



$\alpha_0 = \sqrt[4]{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = \sqrt[4]{2}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = \frac{\sqrt[4]{2^3}}{2} + i\frac{\sqrt[4]{2^3}}{2}$

$\alpha_1 = -\frac{\sqrt[4]{2^3}}{2} + i\frac{\sqrt[4]{2^3}}{2}$

$\alpha_2 = -\frac{\sqrt[4]{2^3}}{2} - i\frac{\sqrt[4]{2^3}}{2}$

$\alpha_3 = \frac{\sqrt[4]{2^3}}{2} - i\frac{\sqrt[4]{2^3}}{2}$

$\mathbb{Q}(\alpha_0, \alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\sqrt[4]{2}, i)$

($\subseteq$) Očitno.

($\supseteq$) $\sqrt[4]{2} = (\alpha_0 + \alpha_3)\cdot\frac{1}{\sqrt{2}}$

$(\sqrt[4]{2})^3 \in F \overset{\text{inv}\neq 2}{\Rightarrow} \frac{\sqrt[4]{2}}{2} \in F \Rightarrow \sqrt[4]{2} \in F$

$i = 2\cdot\frac{\alpha_0 + \alpha_1}{\sqrt[4]{2^3}} \in F$

Stopnja: $4\cdot 2 = 8$

$f(x) \in F[X]$, st $f(x) = n$
E razpadno polje $f(x)$

Pokaži:

a) $[E:F] \leq n!$

b) $f(x)$ nerazcepen $\Rightarrow n \mid [E:F]$

a) $E = F(a_1, \ldots, a_k)$, a_i ničle, $k \leq n$

$$F \subseteq F(a_1) \subseteq F(a_1, a_2) \subseteq \dots \subseteq F(a_1, \dots, a_k)$$

$\leq n$ ($m_1(x) \mid f(x)$) ; $\leq n-1$ ($m_2(x) \mid g(x)$) ; $\leq n-2$; $\dots$

$f(x) = (x - a_1) \cdot g(x)$, st $g(x) = n-1$

$\Rightarrow [E:F] \leq n!$

b) $f(x)$ nerazcepen $\Rightarrow$ stopnja je n

Naj bo F polje in $a_1, \dots, a_n \in F$. Pokaži, da obstaja $f(x) \in F[x]$, da velja $f(a_1) = \dots = f(a_n) = 1$. Sklepaj, da končno polje ne more biti algebraično zaprto.

$$f(x) = (x - a_1) \cdots (x - a_n) + 1$$

Naj bo F končno polje. Pokazati želimo, da obstaja polinom, ki nima vsaj ene ničle v F.

Vzemimo kar zgornji polinom. Ta nima vsaj ene ničle v F, saj je $f(a) = 1$ za vse $a \in F = \{a_1, \dots, a_n\}$.

Pokaži, da je polje F algebraično zaprto natanko tedaj, ko ne dostaja končna razširitev E/F.

($\Rightarrow$) Naj bo F algebraično zaprto. Denimo, da dostaja končna razširitev E/F, $E \neq F$.

$\exists a \in E \setminus F$

$k := [E:F]$

Izberimo $1, a, \dots, a^n$, ki so linearno odvisni, kjer so $1, a, \dots, a^{n-1}$ neodvisni.

$\Rightarrow a^n = \alpha_0 + \alpha_1 a + \dots + \alpha_{n-1} a^{n-1}$, $\alpha_i \in F$

$f(x) = -x^n + \alpha_0 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1}$

$= -x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0$

$f(a) = 0$, $a \notin F$

($\Leftarrow$) Recimo, da ne obstaja končna razširitev. Denimo, da polje ni algebraično zaprto.

$\exists f(x): \; f(a) = 0, \; a \in E \setminus F$

$F(a)/F$ je končna razširitev, saj je $[F(a) : F] \leq \text{st } p(x)$.

Naj bo $E \neq \mathbb{R}$ končna razširitev polja $\mathbb{R}$. Pokaži, da je $E \cong \mathbb{C}$.

Vsak element iz končne razširitve E je ničla nekega nerazcepnega polinoma iz $\mathbb{R}$.

$a \in E \setminus \mathbb{R}$

$\Rightarrow$ a je ničla nerazcepnega kvadratnega polinoma iz $\mathbb{R}$

$\Rightarrow a \in \mathbb{C}$

$\Rightarrow \underbrace{\mathbb{R} \subseteq E \subseteq \mathbb{C}}_{2}$ (nad $\mathbb{R}$: ≥ 2, $\Rightarrow 1$)

$\Rightarrow E = \mathbb{C}$

Naj bo $f(x) = x^2+x+1 \in \mathbb{Z}_2[x]$ nerazcepen nad $\mathbb{Z}_2$. (x^2+x+1) je max. ideal, ker je x^2+x+1 nerazcepen.

$F = \mathbb{Z}[x]/(x^2+x+1)$

Elementi polja F so odseki.

$p(x)+I = q(x)+I \iff p(x)-q(x) \in I$

$st(p(x)) \geq 2$

$p(x) = \alpha(x)\cdot\underbrace{(x^2+x+1)}_{\in I} + q(x), \quad st(q(x)) \leq 1$

$F = \{0+I, 1+I, x+I, x+1+I\} =$

$= \{0, 1, \overline{x}, \overline{x}+1\} \cong \mathbb{Z}_2$

$\overline{x}$ je ničla x^2+x+1 v F.

$\overline{x}^2+\overline{x}+1 = (x+I)^2+(x+I)+(1+I) = (x^2+x+1)+I = I$

$+$	0	1	$\overline{x}$	$\overline{x}+1$
0	0	1	$\overline{x}$	$\overline{x}+1$
1	1	0	$\overline{x}+1$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x}+1$	0	1
$\overline{x}+1$	$\overline{x}+1$	$\overline{x}$	1	0

$\cdot$	0	1	$\overline{x}$	$\overline{x}+1$
0	0	0	0	0
1	0	1	$\overline{x}$	$\overline{x}+1$
$\overline{x}$	0	$\overline{x}$	$\overline{x}+1$	1
$\overline{x}+1$	0	$\overline{x}+1$	1	$\overline{x}$

Velmo: $x^2+x+1=0$ v $F \Rightarrow x^2 = x+1$

$(\overline{x}+1)\cdot\overline{x} = (x+1+I)\cdot(x+I) = (x^2+x+I) = 1+I$

Pokaži, da je F razpadno polje $x^2+x+1 \in \mathbb{Z}_2[x]$.

Velmo: $f(\overline{x}) = 0$

$f(\overline{x}+1) = (\overline{x}+1)^2 + (\overline{x}+1) + 1 = \underset{\overset{\shortparallel}{x+1}}{x^2} + 1 + x = 0$

Nad F: $f(x) = (x-\overline{x}-1)(x-\overline{x}) = x^2+x+1$

$GF(p^n)$ je razpadno polje $x^{p^n}-x \in \mathbb{Z}_p[x]$.

$x^{p^n}-x = \prod_{a \in GF(p^n)} (x-a)$

Naj bo $q(x) \in \mathbb{Z}_p[x]$ nerazcepen stopnje n.

a) Pokaži, da je $GF(p^n) = \mathbb{Z}_p[x]/(q(x))$.

b) Pokaži, da $q(x) \mid x^{p^n}-x$.

a) $F := \mathbb{Z}_p[x]/(q(x))$
$I := (q(x))$

Elementi F so odseki $p(x)+I$, kjer je $\text{st}\, p(x) < n$.

$p_1(x)$, $p_2(x)$ stopnje manj kot n.

$p_1(x) + I = p_2(x) + I \iff p_1(x) = p_2(x)$

Elementi F: $a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + I$

$\Rightarrow |F| = p^n$

$\Rightarrow F \cong GF(p^n)$

b) $\overline{x}$ je ničla $g(x)$.

$g(\overline{x}) = g(x+I) = g(x) + I = I = 0$ (H3)

$x^{p^n} - x = \prod_{a \in F} (x-a)$

$\Rightarrow \overline{x}$ je ničla $g(x)$ in $x^{p^n} - x$ v F.

Če $g(x) \nmid x^{p^n} - x$, potem sta si tuja:

$\exists k(x), l(x) \in \mathbb{Z}_p[x]: \; g(x)k(x) + (x^{p^n} - x)l(x) = 1$

V razširitvi ustavimo $\overline{x}$: $0 = 1$

Pokaži:

a) $GF(8) = \mathbb{Z}_2[x]/(x^3+x+1)$

b) $GF(9) = \mathbb{Z}_3[x]/(x^2+1)$

c) $GF(16) = \mathbb{Z}_2[x]/(x^4+x+1)$

To sledi iz prejšnje naloge. Preveriti je treba le nerazcepnost.

a) Če je x^3+x+1 razcepen, ima ničlo, ampak ta je nima.

c) Vemo, da je x^4+x+1 nerazcepen.

Zapiši x^8-x kot produkt nerazcepnih polinomov iz $\mathbb{Z}_2[x]$.

$x^8-x = x(x^7-1) = x(x-1)(x^6+\ldots+1)$

Po prejšnji nalogi x^3+x+1 deli $x^6+\ldots+1$.

Ker ima x^8-x same različne ničle, to ni dvojni delitelj.

Še en delitelj je x^3+x^2+1.

$x^8-x = x(x-1)(x^3+x+1)(x^3+x^2+1)$

NORMALNE RAZŠIRITVE

$L \supseteq K$ je normalna:

- L je razpadno polje nekega polinoma $f(x) \in K[x]$ ali
- če ima nerazcepen $f(x) \in L[x]$ ničlo v L, razpade nad L

Naj bo $[L:K]=2$. Pokaži, da je $L \supseteq K$ normalna.

$\exists\, a \in L \setminus K$

$[L:K] = 2$

$\Rightarrow 1, a, a^2$ linearno odvisni

$\Rightarrow$ Obstaja nerazcepen polinom $f(x)$ stopnje 2 nad K

$f(a) = 0$

$\Rightarrow f(x) = m_a(x)$

$f(x) = (x-a) \cdot q(x)$ nad L

$\Rightarrow$ st $q(x) = 1$

$\Rightarrow$ Linearen polinom ima v polju ničlo

$\Rightarrow$ je normalen po definiciji

Določi, ali je naslednja razširitev $\mathbb{Q}$ normalna.

a) $\mathbb{Q}(\sqrt{2}, i)$

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

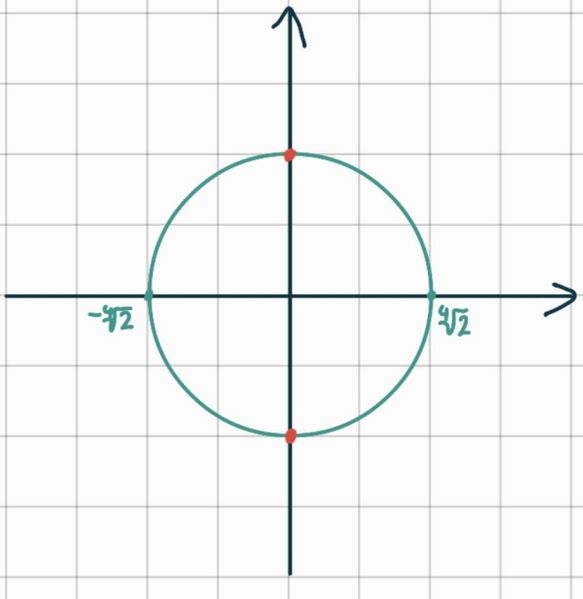
$\mathbb{Q}(\sqrt{2}, -\sqrt{2}, i, -i) = \mathbb{Q}(\sqrt{2}, i)$

$\Rightarrow$ Je normalna.

b) $\mathbb{Q}(\sqrt[4]{2}) = L$

$f(x) = x^4 - 2 = (x^2-\sqrt{2})(x^2+\sqrt{2}) = (x-\sqrt[4]{2})(x+\sqrt[4]{2})(x^2+\sqrt{2}) =$

$= (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$



$f(x)$ je nerazcepen nad $\mathbb{Q}$ in ima ničlo $\sqrt[4]{2}$ v L, nima pa vseh ničel v L.

$\Rightarrow$ Ni normalna.

c) $\mathbb{Q}(\sqrt[3]{2}, i) = E$

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

$f(x)$ je nerazcepen nad $\mathbb{Q}$.

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

Če je M normalna, je $w \in E$.

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

Če je $w \in E$, je $\sqrt{3} \in E$, torej $\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2})$.

Pokazali bomo, da to ni res.

Baza: $\{1, \sqrt[3]{2}, \sqrt[3]{4}, i, i\sqrt[3]{2}, i\sqrt[3]{4}\}$

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

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[3]{2})$$
$$\qquad\quad 2 \qquad\qquad 3$$

$2 \nmid 3$

Ali je razširitev $\mathbb{Z}_3(x^3) \leq \mathbb{Z}_3(x)$ normalna?

$\mathbb{Z}_3(x)$ = polje racionalnih funkcij nad $\mathbb{Z}_3$ v spremenljivki x
$\mathbb{Z}_3(x^3)$ = polje racionalnih funkcij nad $\mathbb{Z}_3$ v spremenljivki x^3

$f(t) \in \mathbb{Z}_3(x^3)[t]$

(Primer: $t^2 + \frac{x^3+1}{2x^6} \cdot t + \frac{x^3+1}{x^6+x^3}$)

$\mathbb{Z}_3(x) = \mathbb{Z}_3(x^3)(x)$

$f(t) = t^3 - x^3 = (t-x)^3 \in \mathbb{Z}_3(x^3)[t]$

$[\mathbb{Z}_3(x) : \mathbb{Z}_3(x^3)] \leq 3$

Stopnja razširitve deli 3 in ni 1, torej je 3.

$f(t)$ je nerazcepen nad $\mathbb{Z}_3(x^3)$, ker nima ničle v $\mathbb{Z}_3(x^3)$.

$\mathbb{Z}_3(x)$ je razpadno polje za $f(t)$.

Torej je razširitev normalna.

Izrek o primitivnem elementu:

$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\beta + c \cdot \alpha)$

$c \in \mathbb{Q}, \quad c \neq c_{ij} = \frac{\beta_i - \beta_1}{\alpha_j - \alpha_1}, \quad j \neq 1$

$\beta = \beta_1, \beta_2, \ldots, \beta_n$ ničle min. polinoma za β
$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ ničle min. polinoma za α

Z uporabo izreka o primitivnem elementu poišči primitivni element razširitve.

a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \geq \mathbb{Q}$

$x^2 + 2 \Rightarrow \pm\sqrt{2}$
$x^2 + 3 \Rightarrow \pm\sqrt{3}$

Prepovedani elementi: $0, \frac{\sqrt{3} - (-\sqrt{3})}{\sqrt{2} - (-\sqrt{2})}$

$\Rightarrow a = \sqrt{3} + c \cdot \sqrt{2}, \quad c \in \mathbb{Q} \setminus \{0\}$ primitivni element

b) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \geq \mathbb{Q}$

Vemo: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

$\Rightarrow F = \mathbb{Q}(\sqrt{2} + \sqrt{3}, \sqrt{5})$

$\alpha = \sqrt{2}+\sqrt{3}$

$\beta = \sqrt{5} \quad \Rightarrow \quad x^2-5 \quad \Rightarrow \quad \beta_1 = \sqrt{5}, \beta_2 = -\sqrt{5}$

$\underset{4}{\mathbb{Q}(\sqrt{2},\sqrt{3})} \geq \mathbb{Q}$ je Galoisova razširitev.

$\sigma \in Aut(\underset{E}{\mathbb{Q}(\sqrt{2},\sqrt{3})}) = Gal(E|\mathbb{Q})$

$\sigma(\sqrt{2}) = \pm\sqrt{2}$

$\sigma(\sqrt{3}) = \pm\sqrt{3}$

$x^2-2=0$

$\sigma(x)^2-2=0$

Ker je stopnja 4, imamo 4 avtomorfizme.

Naj bo $f(x)$ minimalni polinom za $\alpha = \sqrt{2}+\sqrt{3}$.

$f(\alpha)=0$

$\sigma(f(\alpha)) = f(\sigma(\alpha)) = 0$

Ničle $f(x)$: $\pm\sqrt{2} \pm \sqrt{3}$ (4 ničle)

$a = \alpha + c\cdot\beta$

$c \neq \frac{\alpha_i - \alpha}{\beta_j - \beta} = \frac{\alpha_i - \alpha}{-2\sqrt{5}}$

$i=1: \ 0$

$i=2: \ \frac{\sqrt{2}-\sqrt{3}-\sqrt{2}-\sqrt{3}}{-2\sqrt{5}} = \frac{\sqrt{3}}{\sqrt{5}}$

$i=3: \ \frac{\sqrt{2}}{\sqrt{5}}$

$i=4: \ \frac{\sqrt{2}+\sqrt{3}}{\sqrt{5}}$

$\Rightarrow a = \sqrt{2}+\sqrt{3}+\sqrt{5}$

Poišči primer algebraičnih a, b nad $\mathbb{Q}$, da $\mathbb{Q}(a,b) \neq \mathbb{Q}(a+b)$.
Navedi $\alpha \in \mathbb{Q}$, da $\mathbb{Q}(a,b) = \mathbb{Q}(a + \alpha \cdot b)$.

$$\mathbb{Q}(-\sqrt{2}, \sqrt{2}) \neq \mathbb{Q}(-\sqrt{2}+\sqrt{2}) = \mathbb{Q}(0)$$

Recimo, da hočemo še $\mathbb{Q}(a) \neq \mathbb{Q}(b)$.

$$\mathbb{Q}(\sqrt{2}-\sqrt{3}, \sqrt{3}) \neq \mathbb{Q}(\sqrt{2}-\sqrt{3}+\sqrt{3}) = \mathbb{Q}(\sqrt{2})$$

Določi razpadno polje $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ nad $\mathbb{Q}$.

$$\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$$

$$\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})}_{4} \overbrace{\subseteq \mathbb{Q}(\sqrt[4]{2}, i)}^{2}$$

$$\Rightarrow [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$$

Ali je ta razširitev Galoisova? Da.

$$\mathrm{Gal}(F|K) = \{\sigma \in \mathrm{Aut}(F) ; \ \sigma(k) = k \ \forall k \in K\}$$

Velja: $\mathrm{Gal}(F|\mathbb{Q}) = \mathrm{Aut}(F)$

Določi:

a) $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}))$

b) $Gal(\mathbb{Q}(\sqrt[4]{2}, i)|\mathbb{Q}) = Aut(\mathbb{Q}(\sqrt[4]{2}, i))$

a) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$

$x^4 - 2 = 0$

Baza: $1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}$

id: $\sqrt[4]{2} \mapsto \sqrt[4]{2}$
σ: $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$

Preveriti moramo, ali je σ res avtomorfizem:

$\sigma(\sqrt[4]{2^2}) = \sigma(\sqrt[4]{2})^2 = \sqrt[4]{2^2}$
$\sigma(\sqrt[4]{2^3}) = \sigma(\sqrt[4]{2})^3 = -\sqrt[4]{2^3}$

σ: $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$
$\sqrt{2} \mapsto \sqrt{2}$
$2\sqrt[4]{2} \mapsto -2\sqrt[4]{2}$

Veljati mora:

$\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$, $a, b \in \mathbb{S}$

$a^m \cdot a^n = a^{n+m}$ $\qquad$ $(-a)^n \cdot (-a)^m$

$\Rightarrow$ To je res avtomorfizem.

$\Rightarrow Gal(\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}) \cong \mathbb{Z}_2$

Ker je moč Galoisove grupe 2, stopnja razširitve pa 4, razširitev ni Galoisova.

b) $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$

$x^4 - 2 = 0$

Ker je razširitev normalna, je $|Gal((\mathbb{Q}(\sqrt[4]{2}, i)|\mathbb{Q})| = 8$.

Ničle: r_1, r_2, r_3, r_4

Opazimo:

- $Gal(\dots) \leq S_4$
  $\Rightarrow |Gal| \leq 24$

- G deluje tranzitivno na $\{r_1, r_2, r_3, r_4\}$:

  $\exists \sigma_1 \in G : \sigma(r_1) = r_2$
  $\exists \sigma_2 \in G : \sigma(r_1) = r_3$
  $\exists \sigma_3 \in G : \sigma(r_1) = r_4$

  $\Rightarrow |Gal| \geq 4$

$Gal \leq S_4$, $|Gal| = 8$, $D_8 \leq S_4$, $|D_8| = 8$

$\Rightarrow G \cong D_8$

$r_1 = \sqrt[4]{2}$
$r_2 = i\sqrt[4]{2}$
$r_3 = -\sqrt[4]{2}$
$r_4 = -i\sqrt[4]{2}$

$\{r_1, r_3\} \rightarrow \{r_1, r_3\}$
$\{r_1, r_3\} \rightarrow \{r_2, r_4\}$

i) $\{r_1, r_3\} \to \{r_1, r_3\}$
$\{r_2, r_4\} \to \{r_2, r_4\}$

ii) $\{r_1, r_3\} \to \{r_2, r_4\}$
$\{r_2, r_4\} \to \{r_1, r_3\}$

Vsi avtomorfizmi so oblike:

$r_i \mapsto r_{\sigma(i)}$, $\sigma \in D_8$

$L_1 = \mathbb{Q}(i)$
$L_2 = \mathbb{Q}(\sqrt{2})$
$L_3 = \mathbb{Q}(i\sqrt{2})$

$E = \mathbb{Q}(\sqrt[4]{2}, i)$

Pokaži: $[E : L_1] = [E : L_2] = [E : L_3] = 4$

Določi: $Gal(E|L_1)$, $Gal(E|L_2)$, $Gal(E|L_3)$

$f(x) = x^4 + bx^2 + c \in \mathbb{Q}[x]$

Ničle:

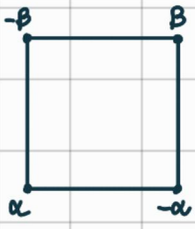
$y = x^2$
$y^2 + by + c$
$\vdots$

$\Rightarrow \alpha, -\alpha, \beta, -\beta$

$\sigma(\{\pm\alpha\}) = \{\pm\alpha\}$ ali $\{\pm\beta\}$
$\sigma(\{\pm\beta\}) = \{\pm\alpha\}$ ali $\{\pm\beta\}$

$\Rightarrow |G| \leq 8$

$\Rightarrow G \leq D_8$



Če so vse ničle racionalne, je $E = \mathbb{Q}$, torej $G = \{id\}$.

$\gamma = \alpha \cdot \beta$

$\gamma^2 = \alpha^2 \cdot \beta^2 \in \mathbb{Q}$ po Vietovih formulah

$f(x) = (x^2 - \alpha^2)(x^2 - \beta^2) = \ldots + \alpha^2\beta^2$

γ je ničla polinoma $x^2 - \gamma^2 = 0$.

$\sigma(\gamma) = \pm\gamma$

Orbita γ:

$|G \cdot \gamma| = [G : G_\gamma]$

Kaj je $st(\gamma)$?

Naš polinom je separabilen.

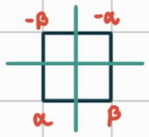
id

$\sigma_1 : \alpha \mapsto \beta, \quad \beta \mapsto \alpha$

$\sigma_2 : \alpha \mapsto -\alpha, \quad \beta \mapsto -\alpha$

$\sigma_1 \cdot \sigma_2$

$G_\gamma = K_4 \cap G$



$\gamma \in \mathbb{Q} \Rightarrow \sigma(\gamma) = \gamma \Rightarrow |G \cdot \gamma| = 1 \Rightarrow |G| = |G \cap K_4| \Rightarrow \underline{G \leq K_4}$

$\sigma' \in G_{\alpha^2}$

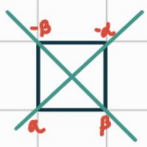
$\Rightarrow \sigma'(\alpha) = \pm\alpha$
$\sigma'(\beta) = \pm\beta$

$G_{\alpha^2} \leq K_4$

$|G \cdot \alpha^2| = [G : G_{\alpha^2}]$

$|G \cdot \alpha^2| = 1 \Leftrightarrow \alpha^2 \in \mathbb{Q}$

$\Rightarrow \underline{G \leq K_4}$



Kdaj je $G \leq C_4$?

$S = \alpha^3\beta - \beta^3\alpha$

C_4 stabilizira S
$G_S \leq C_4$

$|G \cdot S| = 1 \Leftrightarrow S \in \mathbb{Q} \Leftrightarrow G \leq C_4$

c $\quad D = b^2 - 4c$

$S^2 = \alpha^2\beta^2(\alpha^2 - \beta^2)^2 = c(b^2 - 4c)$

$S = \sqrt{c(b^2 - 4c)} \in \mathbb{Q} \Leftrightarrow \underline{G \leq C_4}$

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

$Gal(p(x)) = ?$

$p(x)$ je nerazcepen $\Rightarrow$ G deluje tranzitivno na ničlah $\Rightarrow |G| \geq 4$

$D = (-4)^2 - 4 \cdot 2 = 8$

$\Rightarrow D \cdot c = 16$ je kvadrat racionalnega $\Rightarrow G \leq C_4$

$\Rightarrow G = C_4$

Naj bo $f(x) \in \mathbb{Q}[x]$ nerazcepen polinom stopnje 3, ki ima eno realno ničlo. Pokaži, da je $Gal(f) \cong S_3$.

$a \in \mathbb{R}$ ničla

$|G| \geq 3$ (tranzitivno delovanje)
$G \leq S_3$, $|S_3| = 6$

$\Rightarrow G$ je C_3 ali S_3

$[\mathbb{Q}(a) : \mathbb{Q}] = 3$

$|G| = [E : \mathbb{Q}]$

$E \geq \underset{2}{\mathbb{Q}(a)} \geq \overset{3}{\mathbb{Q}}$

$\Rightarrow |G| = 6$

$\rightarrow G \cong S_3$

Osnovni izrek o simetričnih polinomih:

Vsak simetrični polinom se da izraziti preko osnovnih simetričnih polinomov:

$x_1 + x_2 + x_3$
$x_1x_2 + x_1x_3 + x_2x_3$
$x_1x_2x_3$

$f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ nerazcepen

$Gal(f) = ?$

$D = ((x_1 - x_2)(x_1 - x_3)(x_2 - x_3))^2$ ... diskriminanta
x_1, x_2, x_3 ... ničle

D je simetrični polinom v x_1, x_2, x_3.

$(g(x_1, x_2, x_3) = g(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}))$

$x_1 + x_2 + x_3 = -a$
$x_1x_2 + x_1x_3 + x_2x_3 = b$
$x_1x_2x_3 = -c$

$D = 18abc + a^2b^2 - 4b^3 - 4a^3c - 27c^2 \in \mathbb{Q}$

$\sigma: \{x_1, x_2, x_3\} \rightarrow \{x_1, x_2, x_3\}$

σ: $x_1 \leftrightarrow x_2$
$x_3 \to x_3$

$\Rightarrow \sqrt{D} = (x_1-x_2)(x_1-x_3)(x_2-x_3) \to -\sqrt{D}$

$\sigma \in G \Rightarrow \sqrt{D} \mapsto -\sqrt{D}$

$\sqrt{D} \in \mathbb{Q} \Rightarrow \sqrt{D} \mapsto \sqrt{D}$

$\Rightarrow \sqrt{D} \in \mathbb{Q} \Rightarrow G \cong C_3$
$\sqrt{D} \notin \mathbb{Q} \Rightarrow G \cong S_3$

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

$D = -108 \Rightarrow \sqrt{D} \notin \mathbb{Q} \Rightarrow G \cong S_3$

$D < 0 \Rightarrow$ 1 realna ničla
$D > 0 \Rightarrow$ 3 realne ničle

$f(x) = x^3 - 4x + 2$
$D = 202$

$\Rightarrow G \cong S_3$

$f(x) = x^3 - 3x + 1$
$D = 81$

$\Rightarrow G \cong C_3$

$f(x) = x^4 + x + 1$

$G \cong S_4$

Naj bo $f(x) \in \mathbb{Q}[x]$ nerazcepen polinom stopnje 5 z natanko 3 realnimi ničlami. Potem je $Gal(f) \cong S_5$.

Realne: x_1, x_2, x_3
Kompleksni: x_4, x_5

Konjugiranje $\rightsquigarrow (x_4, x_5)$

G vsebuje 5-cikel:

$|G \cdot x_1| = 5 = [G : G_{x_1}]$

$\Rightarrow 5 \mid |G|$

$\Rightarrow$ Obstaja element reda 5

$G \leq S_5$

$\Rightarrow$ Imamo 5-cikel v S_5

$\Rightarrow G \cong S_5$

$f(x) = x^5 + 10x^4 - 2$

$G \cong S_5$

KUBIČNE ENAČBE NAD $\mathbb{Q}$

$f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ nerazcepen

$\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ ničle f

$$Gal(f) = \begin{cases} S_3 & ; \ \sqrt{D} \notin \mathbb{Q} \\ A_3 \cong C_3 & ; \ \sqrt{D} \in \mathbb{Q} \end{cases}$$

$$D = ((\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3))^2$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{D}) \subseteq E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$$

Iščemo formule za $\alpha_1, \alpha_2, \alpha_3$ ...

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

Naredimo zamenjavo:

$$x = t - \frac{a}{3}$$

$$\Rightarrow g(t) = t^3 + pt + q$$

f in g imata isto diskriminanto.

$$\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(t_1, t_2, t_3)$$

$t_1, t_2, t_3 \in \mathbb{C}$ ničle g

Vemo:

$D_f = 18abc + a^2b^2 - 4b^3 - 4a^3c - 27c^2$
$D_g = -4p^3 - 27q^2$

$D_f = D_g$

Označimo:

$z_1 = t_1 + t_2 + t_3$
$z_2 = t_1 + \omega t_2 + \omega^2 t_3$
$z_3 = t_1 + \omega^2 t_2 + \omega t_3$

Oglejmo si:

$\sigma: t_1 \to t_2 \to t_3$

$\sigma(z_1) = z_1$
$\sigma(z_2) = t_2 + \omega t_3 + \omega^2 t_1 = \omega^2 z_2$
$\sigma(z_3) = t_2 + \omega^2 t_3 + \omega t_1 = \omega z_3$

$\Rightarrow \sigma(z_1^3) = z_1^3$
$\sigma(z_2^3) = z_2^3$
$\sigma(z_3^3) = z_3^3$

$t^3 + pt + q = (t - t_1)(t - t_2)(t - t_3) = t^3 + t^2(\overbrace{-t_1 - t_2 - t_3}^{0}) + \dots$

$\Rightarrow z_1 = 0$

$$\begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{bmatrix}}_{M} \begin{bmatrix} t_1 \\ t_2 \\ t_3 \end{bmatrix}$$

$$\begin{bmatrix} t_1 \\ t_2 \\ t_3 \end{bmatrix} = M^{-1} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 1 & w^2 & w \\ 1 & w & w^2 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}$$

$$t_1 = \frac{1}{3}(z_1 + z_2 + z_3)$$
$$t_2 = \frac{1}{3}(z_1 + w^2 z_2 + w z_3)$$
$$t_3 = \frac{1}{3}(z_1 + w z_2 + w^2 z_3)$$

$$\Rightarrow t_1 = \underbrace{\tfrac{1}{3}z_2}_{u} + \underbrace{\tfrac{1}{3}z_3}_{v} = u + v$$
$$t_2 = \tfrac{1}{3}w^2 z_2 + \tfrac{1}{3}w z_3 = w^2 u + w v$$
$$t_3 = \tfrac{1}{3}w z_2 + \tfrac{1}{3}w^2 z_3 = w u + w^2 v$$

$$t^3 + pt + q = (t - t_1)(t - t_2)(t - t_3) \overset{\text{razun}}{=} t^3 - 3uvt - (u^3 + v^3)$$

$$\Rightarrow p = -3uv$$
$$q = -(u^3 + v^3)$$

$$\frac{p^3}{-27} = u^3 v^3$$
$$-q = u^3 + v^3$$

$$y^2 + qy - \frac{p^3}{27} = 0$$

$$y_{1,2} = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

Označimo:

$$d = \frac{q^2}{4} + \frac{p^3}{27} = \frac{-D_q}{108}$$

$$\Rightarrow u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$
$$v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

$$\Rightarrow u_1, u_1 w, u_1 w^2$$
$$v_1, v_1 w, v_1 w^2$$

Izbrati moramo taka u, v, da je $uv = -\frac{p}{3}$.

$u_i v_j = u_i v_1 w^j$

Izberemo ju in dobimo rešitve:

$t_1 = u + v$
$t_2 = w^2 u + wv$
$t_3 = wu + w^2 v$

$\alpha_1 = t_1 + \frac{a}{3}$
$\alpha_2 = t_2 + \frac{a}{3}$
$\alpha_3 = t_3 + \frac{a}{3}$

$x^3 - 3x + 1 = 0$

$g(x) = x^3 - 3x + 1$

$D_g = -4 \cdot (-3)^3 - 27 = 81 = 9^2$

$Gal(g) = A_3$

$-3 = -3uv \Rightarrow uv = 1 \Rightarrow u^3 v^3 = 1$
$1 = -(u^3 + v^3) \Rightarrow u^3 + v^3 = -1 \Rightarrow u^3 + v^3 = -1$

$y^2 + y + 1 = 0$

$\Rightarrow u^3 = w$
$v^3 = w^2$

$w = -\frac{1}{2} + \frac{\sqrt{2}}{2} i = e^{i\frac{2\pi}{3}}$

$u = e^{i\varphi}$

$u^3 = w$

$e^{i3\varphi} = e^{i\frac{2\pi}{5}}$

$3\varphi = \frac{2\pi}{3} + 2\pi k$

$\varphi = \frac{2\pi}{9} + \frac{2}{3}\pi k$

$e^{i\frac{2\pi}{9}} \cdot v = 1$

$\Rightarrow u = e^{i\frac{2\pi}{9}}$

$v = e^{-i\frac{2\pi}{9}}$

$t_1 = e^{i\frac{2\pi}{9}} + e^{-i\frac{2\pi}{9}} = 2\cos\frac{2\pi}{9}$

$t_2 = e^{i\frac{4\pi}{5}} \cdot e^{i\frac{2\pi}{5}} + e^{i\frac{2\pi}{5}} \cdot e^{-i\frac{2\pi}{9}} = 2\cos\frac{4\pi}{9}$

$t_3 = e^{i\frac{2\pi}{5}} \cdot e^{i\frac{2\pi}{9}} + e^{i\frac{4\pi}{5}} \cdot e^{-\frac{2\pi}{9}} = 2\cos\frac{8\pi}{9}$

$\Rightarrow g(x) = x^3 - 3x + 1 = (x - 2\cos\frac{2\pi}{9})(x - 2\cos\frac{4\pi}{9})(x - 2\cos\frac{8\pi}{9})$

ENAČBE 4. STOPNJE NAD $\mathbb{Q}$

$f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Q}[x]$ nerazcepen

$t = x + \frac{a_3}{4}$

$\Rightarrow x = t - \frac{a_3}{4}$

$\Rightarrow g(t) = t^4 + pt^2 + qt + r \in \mathbb{Q}[x]$

$D = \prod_{\substack{i<j \\ i,j \in [4]}} (\alpha_j - \alpha_i)^2$

$\alpha_1, \alpha_2, \alpha_3, \alpha_4$ ničle $g(x)$

Polinom 3. stopnje ... kubična rezendenta

Označimo:

$\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$
$\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$
$\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$

$Gal(g) \leq S_4$

$\sigma = (\alpha_1\ \alpha_2)$

$\sigma(\theta_1) = \theta_1$
$\sigma(\theta_2) = \theta_3$
$\sigma(\theta_3) = \theta_2$

$R(x) = (x-\theta_1)(x-\theta_2)(x-\theta_3)$ ... kubična rezindenta

Predpostavimo, da je $R(x)$ nerazcepna.

Ali je $R(x) \in \mathbb{Q}[x]$?

Koeficienti $R(x)$ so simetrični polinomi v $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ polinomi v p, q, r, torej so v $\mathbb{Q}$.

Velja: $D_R = D_g$

$\mathbb{Q} \subseteq \mathbb{Q}(\theta_1, \theta_2, \theta_3) \subseteq \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$

$\sqrt{D} \in \mathbb{Q} \Rightarrow [\mathbb{Q}(\theta_1, \theta_2, \theta_3) : \mathbb{Q}] = 3$
$\sqrt{D} \notin \mathbb{Q} \Rightarrow [\mathbb{Q}(\theta_1, \theta_2, \theta_3) : \mathbb{Q}] = 6$

$S_3 \leq Gal(g)$

G deluje tranzitivno na $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.

G je ali S_4 ali A_4.

Ali je $(\alpha_1 \alpha_2)$ v G?

$\sqrt{D} \mapsto -\sqrt{D}$

Ampak $\mathbb{Q}$ mora postati pri miru.

$\Rightarrow (\alpha_1 \alpha_2) \notin D$

$\Rightarrow G \neq S_4$

- $R(x)$ nerazcepen, $\sqrt{D} \in \mathbb{Q}$:

  $\Rightarrow Gal(g) \cong A_4$

- $R(x)$ nerazcepen, $\sqrt{D} \notin \mathbb{Q}$:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\theta_1, \theta_2, \theta_3) \subseteq \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

$$\begin{matrix} \downarrow & \downarrow & \downarrow & \downarrow \\ G & G \cap A_4 & G \cap K_4 & \mathbb{Q} \end{matrix}$$

$$2 \quad 2 \quad 3$$

  $\Rightarrow Gal(g) \cong S_4$

$f(x) = x^4 - x - 1$

$\Rightarrow R(x) = x^3 + 4x + 1$

$D = -283$

$\Rightarrow Gal(g) \cong S_4$

$f(x) = x^4 + 8x + 12$

$\Rightarrow R(x) = x^3 - 16x + 16$

$D = 576^2$

$\Rightarrow Gal(g) \cong A_4$

---

p praštevilo, $p > 2$
E razpadno polje $x^p - 1 \in \mathbb{Q}[x]$

Pokaži, da je $G = Gal(E/\mathbb{Q}) \cong C_{p-1}$.

$[E : \mathbb{Q}] = ?$

$1 \in \mathbb{Q}$
druge ničle $\notin \mathbb{Q}$

$f(x) = (x-1)(\underbrace{x^{p-1} + \dots + x + 1}_{\text{nerazcepen}})$

$\Rightarrow [E : \mathbb{Q}] = p-1$

$\Rightarrow |G| = p-1$

$\sigma \in Aut(E|\mathbb{Q})$

$\sigma(w) = w^i, \quad i = 1, \dots, p-1$

$\sigma(w^2)$ poznamo
$\sigma(w^3)$ poznamo
$\vdots$

$\Rightarrow |Aut(E|\mathbb{Q})| \leq p-1$

$\Rightarrow$ Vsi so ciklični.