$F \subset \mathbb{C}$ $p \in \mathbb{Z}_+$ primo. $\xi = e^{2\pi i/p} \in F$

$a \in F$ não seja p-potência.

$f = X^p - a \in F[X]$.

$F \subset K$ - corpo de decomposição de f

$[K:F] \leq p$.

Proposição: $G = Gal(K/F)$ $[K:F] = p$,
$G \simeq C_p$ grupo cíclico de ordem p.

Pf: $\alpha \in K$ $f(\alpha) = 0$ $a \notin F$

$\exists\, g \in G$. $g\alpha \neq \alpha$

as raízes de f são

$\alpha, \xi\alpha, \xi^2\alpha, \ldots, \xi^{p-1}\alpha$

$g\alpha = \xi^i \alpha$ para algum i.

$g^2\alpha = g(\xi^i\alpha) = \xi^i(g\alpha) = \xi^i \cdot \xi^i\alpha = \xi^{2i}\alpha$

$g^k\alpha = \xi^{ki} \cdot \alpha$ $\xi^p = 1$.

$g^p\alpha = \xi^{pi}\alpha = \alpha$.

Não existe um $k < p$. Tq $g^k\alpha = \alpha$
ordem de g em G $\geq p$.

$|G| \geq p \Rightarrow [K:F] = p = |G|$

$\Rightarrow f$ é irred., extensão é Galois

$G = G_p$. $\square$.

Conversa $F \subset \mathbb{C}$ $\zeta \in F$ $\zeta = e^{2\pi i/p}$.

K/F Galois $[K:F] = p$.

$\Rightarrow K = F(\alpha)$ para $\alpha^p = a \in F$.

Def. Uma extensão assim é dita uma extensão de **Kummer**.

$p = 2$. $x^2 + ax + b$

$$\frac{1}{2}\left(-b \pm \sqrt{b^2 - 4a}\right)$$

$$F\left(\sqrt{b^2-4a}\right) = K.$$

$|G| = p \Rightarrow G = C_p$ $1 \neq g \in G$

$g \in \mathrm{End}_F(K)$

$\cap$

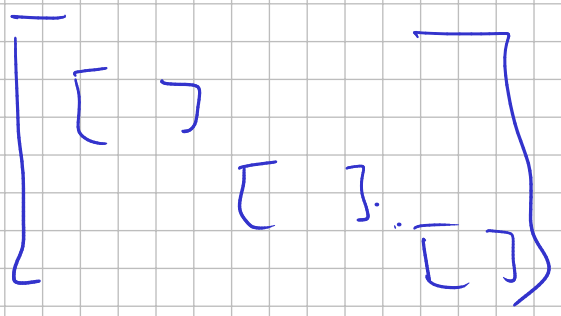
$GL_F(K)$. $g^p = \mathrm{id}_K$.

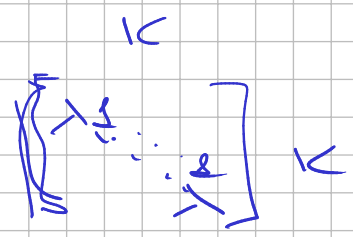
$\Rightarrow \exists\, 1 \neq \lambda \in F$ $0 \neq \alpha \in K$.

Tq $g \cdot \alpha = \lambda\alpha$. $\lambda^p = 1$. $\lambda \neq 1$.

g é diagonalizável em K.

Forma de Jordan de $g \in \mathrm{Mat}_{p\times p}(F)$





$g^p = id. \qquad \kappa = 1$

$\Rightarrow \lambda^p = 1. \qquad \lambda = \xi^i$ para algum i

Γ

$\Rightarrow g$ é diagonalizável em Γ.

$\Rightarrow (\alpha \notin F) \Leftarrow \exists\, g$ não fixa α

Claim $\alpha^p \in F$.

$\lambda^p = 1 \qquad \lambda = \xi^i$ para algum i

~~$g^k \cdot \alpha = \lambda^k \cdot \alpha = \xi^{ik} \alpha$~~

$g(\alpha^k) = g(\alpha)^k = (\lambda \cdot \alpha)^k = \lambda^k \alpha^k$

$g(\alpha^p) = 1 \cdot \alpha^p \Rightarrow \alpha^p$ é fixo por g

$\Rightarrow \alpha^p$ é fixo por todo G

$\Rightarrow \alpha^p \in \Gamma. \qquad x^p - \alpha^p \in F[x].$

$\Rightarrow F(\alpha) = K. \qquad \square.$

Extensões ciclotômicas.

$F \subset \mathbb{C}$ $\quad \zeta = e^{2\pi i/n} \in F \subset \mathbb{C}$

n não é necessariamente primo.

$f: X^n - 1$ $\quad \zeta$ é raiz de f.

$g = 1 + X + \dots + X^{n-1}$ $\quad \zeta$ é raiz.

g é irredutível / $\mathbb{Q}$.

$\mathbb{Q}(\zeta)/\mathbb{Q}$ é uma extensão de Galois.

$G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ $\quad |G| = n-1$

Lemma $n = p$ é primo.

$\varphi: G \cong \mathbb{F}_p^{\times}$ é um grupo cíclico de ordem $p-1$.

$h \in G$. $\quad h(\zeta)$ é uma outra raiz de g., ζ^i. $\quad i = 1, \dots, p-1$.

$h \xrightarrow{\varphi} i \pmod p \in \mathbb{F}_p^{\times}$

φ é um homomorfismo de Grupos.

$\varphi(h') = i' \in \mathbb{F}_p^*$ $\quad h'(\zeta) = \zeta^{i'}$

$\varphi(h \cdot h') = ?$ $\quad (h \cdot h')(\xi) = h(h'\xi)$

$= h(\xi^{i'}) = h(\xi)^{i'} = (\xi^i)^{i'} = \xi^{i i'}$

$\varphi(h \cdot h') = i \cdot i' = \varphi(h) \cdot \varphi(i') \pmod p$

$\mathbb{F}_p^\times$

o morfismo φ é um isomorfismo.

é injetivo porque $\xi \in K$ gera K

uma vez que sei $h(\xi)$ em conheço $h \in K$.

G_2

$\mathbb{F}_p^*$ é cíclico. $\varphi(G) \subset \mathbb{F}_p^*$

é cíclico. $\Rightarrow$ G é cíclico.

$|G| = p-1$ $\Rightarrow$ φ isomorfismo.

$\mathbb{D} \subset F \subset \mathbb{C}$. corpo de números.

$G\left(F(\xi)/F\right)$ é cíclico.

não sei se $g(x) = X^{p-1} + X^{p-2} + \dots + 1$

é irred. / F:

$\Rightarrow$ G é um grupo cíclico. $\subset \mathbb{F}_p^*$

$|G| \mid p-1$ □.

$F = \mathbb{Q}$. $|G| = p-1$ $\forall\ k \geq 0$.

$\mathbb{Q} \subset \mathbb{Q}(\zeta)$ G tem um subgrupo de ordem k $\iff$ $k \mid p-1$

$$\begin{array}{ccccc} \mathbb{Q} & \subset & F & \subset & \mathbb{Q}(\zeta) \\ \updownarrow & & & \nearrow \approx & \\ & & & \mathbb{F}_p^{\times} & \end{array} \qquad u \neq 1$$

F sobre $\mathbb{Q}$: grau k

$(p-1) = k \cdot r$ $\quad h = h'^{r}$ gera o

$(h')^k = h^{rk} = 1 \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

h' gera $\mathrm{Gal}(\mathbb{Q}(\zeta)/F)$.

$p > 2$. $p-1$ é divisível por 2.

Toda extensão ciclotômica. $\mathbb{Q}(\zeta)$ $\zeta = e^{2\pi i/p}$ tem uma subextensão $F \subset \mathbb{Q}(\zeta)$ que. $[\mathbb{Q}(\zeta) : F] = 2$.

(B) $\zeta + \zeta^{p-1}$ $\quad p > 2$.

$$\beta \cdot \xi = \xi^2 + \xi^p = \xi^2 + 1$$

ξ é uma raiz de $x^2 - \beta x + 1 \in F[x]$

$$\mathbb{Q}(\beta) = F \subset \mathbb{Q}(\xi)$$

irredutível.

$\xi \notin F$.

$$\mathbb{Q} \subset F = \mathbb{Q}(\beta) \subset \mathbb{Q}(\xi) \subset \mathbb{C}.$$

$\xi \in \mathbb{C} \setminus \mathbb{R}$.

$$\beta = \xi + \xi^{p-1} = \xi + \xi^{-1} = \xi + \overline{\xi} \in \mathbb{R}$$

$\mathbb{Q} \subset \mathbb{R} \Rightarrow F \subset \mathbb{R}$.

$\Rightarrow \mathbb{Q}(\xi) \neq F \Rightarrow [\mathbb{Q}(\xi) : F] = 2$.

□

Ex $p = 7$, $\beta_1 = \xi + \xi^6$.

$\deg \beta = 3 \quad / \mathbb{Q}$.

$$\deg [\mathbb{Q}(\xi) : \mathbb{Q}(\beta)] = 2.$$

$$\deg [\mathbb{Q}(\xi) : \mathbb{Q}] = 6$$

qual é o polynômio irredutível de β / $\mathbb{Q}$?

$\beta_2 = \zeta^2 + \zeta^5$ $\qquad$ $\beta_3 = \zeta^3 + \zeta^4$

$(x-\beta_1)(x-\beta_2)(x-\beta_3)$

$= x^3 - x^2(\beta_1+\beta_2+\beta_3) + x(\beta_1\beta_2+\beta_2\beta_3+\beta_3\beta_1) - \beta_1\beta_2\beta_3$

$-1 \qquad -2 \qquad 1$

$1+\beta_1+\beta_2+\beta_3 = 1+\zeta^1+\zeta^2+\cdots+\zeta^6 = 0$

$(\beta_1\cdot\beta_2) = (\zeta+\zeta^{-1})(\zeta^2+\zeta^{-2})$

$= \zeta^3 + \zeta^{-3} + \zeta^1 + \zeta^{-1}$

$= \beta_3 + \beta_1$

$\beta_2\beta_3 = (\zeta^2+\zeta^{-2})(\zeta^3+\zeta^{-3})$

$\zeta^2 + \zeta^{-2} + \zeta + \zeta^{-1} = \beta_2 + \beta_1$

$\beta_1\beta_3 = \beta_2 + \beta_3$

$\beta_1\cdot\beta_2\cdot\beta_3 = (\beta_3+\beta_1)\beta_3 = \beta_2+\beta_3+2+\beta_1$ $\qquad 1$

$(\zeta^3+\zeta^{-3})(\zeta^3+\zeta^{-3}) = \zeta^1+\zeta^{-1}+2$

x^3+x^2-2x-1 é irredutível.

Temos que $\mathbb{Q} \subseteq \mathbb{Q}(\beta) \subset \mathbb{Q}(e^{2\pi i/7})$ $\square$

Serre representations...

Etingof representation theory.

Polynômios de graus.

Lembrar construção de números reais com regra e compás.

↝ Torre de corpos cada um uma extensão de grau 2 da anterior

$F \subset \mathbb{C}$ um corpo.

Def. Um $\alpha \in \mathbb{C}$ é expressável por radicais sobre F se $\exists$ uma Torre

$$F = F_0 \subset F_1 \subset F_2 \dots \subset F_r \subset \mathbb{C}$$

1) $\alpha \in F_r$

2) $\forall\ 0 < i \leq r \quad \exists\ \beta_i,\ n_i \geq 2$

Tq $F_i = F_{i-1}(\beta_i)$

$\beta_i \in F_i \setminus F_{i-1} \qquad \beta_i^{n_i} \in F_{i-1}$

Prop: Seja $f \in F[x]$ deg ≤ 4

$f(\alpha) = 0$ então α é expressável por radicais.

deg $= 2$ $\quad \dfrac{b \pm \sqrt[2]{b^2 - 4ac}}{2}$ ←

deg $= 3$ ↝ cardano $\sqrt[3]{\ } \quad \sqrt[3]{\ }$

deg $= 4$, f tem uma raiz em F.

$f = (x-\beta)\,g$ $\quad \deg g = 3$.

$\beta \in F$

f é redutível $\Rightarrow$ $f = g \cdot h$ polyna de grau 2.

Basta analisar a situação com f irredutível.

Discriminante $D = \delta^2$

Ressolventes g $\deg g = 3$ def.

$\mathrm{Gal}(K/F(\delta)) \subset A_4$.

se g irred. $\mathrm{Gal}(K/F(\delta)) = V_4$ (Klein) $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$

α é expressável por.

$F = F_0 \subset F_1 \subset \dots \subset F_r$.

$\delta^2 \sqrt{}$, $\sqrt[3]{} \sim g \sim 2 \cdot \sqrt{}$ Por $\mathbb{Z}_2 \times \mathbb{Z}_2$

— o —

$F \subset F_0 \subset F_1 \subset F_2 \dots \subset F_r$

$\xi_n = e^{2\pi i/n}$ estão permutados nessas torres.

$$\sqrt[n]{a} = \sqrt[r]{\sqrt[s]{a}} \qquad n = r \cdot s$$

$F_0 \subset F_1$ (grau n)

$F_0 \overset{s}{\subset} F_1 \overset{r}{\subset} F_2$, $F_2 = F_1(\sqrt[n]{a})$

Posso então assumir que é um

$F = F_0 \subset F_1 \subset \dots \subset F_r$

$[F_i : F_{i-1}] = p$ Para algum primo p dependendo de i.

$F \subset \mathbb{C}$ $\quad f \in F[x]$ — irredutível

se $f(\alpha) = 0$.

f é expressável por radicais então todas as raízes de f são

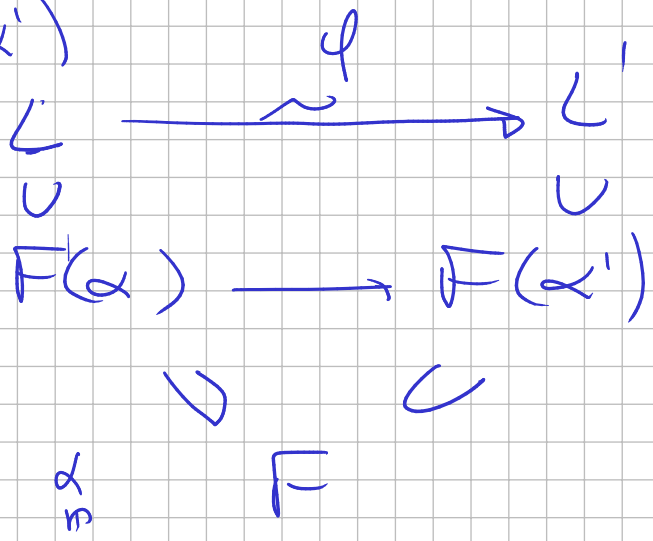
$F = F_0 \subset F_1 \subset \dots \subset F_r \subset \mathbb{C}$

α

escolhe $L \supset F_r$ corpo de decomposição de $f \cdot g$ / F. L corpo de decomp. de $f \cdot g$ / $F(\alpha)$.

$f(\alpha') = 0 \qquad \alpha' \in L'$

L' corpo de decomposição de f_g sobre $F(\alpha')$



$F = F_0 \subset \dots \subset F_r$

$\varphi \downarrow$

$F = \varphi(F_0) \subset \varphi(F_1) \subset \dots \subset \varphi(F_\alpha) \supset \alpha'$

Porque eu escolhi L corpo de decomposição de f_g e não $\mathbb{Q}$!

α é expressável por radicais.

$F = F_0 \subset F_1 \subset \dots \subset F_r \supset \alpha$

$\mathrm{Gal}(F_i / F_{i-1}) \simeq \mathbb{Z}_{p_i} \quad \forall i.$

p_i é primo.

$G_1 = \mathbb{Z}_{p_1}$

$\searrow$

$0 \to \mathbb{Z}_{p_2} \to G_2 \twoheadrightarrow G_1 \to 1$

$0 \to \mathbb{Z}_{p_3} \to G_3 \twoheadrightarrow G_2 \to 1.$

G_i ~ solúveis. em particular não são simples.

G_{i-1} é um quociente não trivial.

$T^n = S^1 \times S^1 \times \cdots \times S^1$

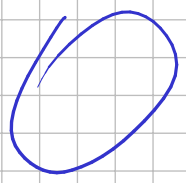
$T^{n_1} \hookrightarrow X$

$\downarrow$

T^{n_0}

Exemplo. $n_0 = 2$. $n_1 = 1$

$T^{n_0} =$ 

$T^{n_1} = S^1 =$ 

$$X = \mathrm{Heis}(\mathbb{R}) / \mathrm{Heis}(\mathbb{Z})$$

$$\mathrm{Mat}_{3\times 3} \supset \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix} \simeq \mathbb{R}^3 \qquad \alpha, \beta, \gamma \in \mathbb{R}$$

$$\cup$$

$$\begin{pmatrix} 1 & n & m \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix} \qquad n, m, k \in \mathbb{Z}$$

$\mathbb{Z}^3$

Quociente

$$X = \mathbb{R}^3 / \mathbb{Z}^3 \neq T^3 = S^1 \times S^1 \times S^1$$

$$X \longrightarrow T^2 = \mathbb{R}^2 / \mathbb{Z}^2 = S^1 \times S^1$$

$$\begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix} \longrightarrow (\alpha, \gamma) \bmod \mathbb{Z}$$

$$\begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n & m \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha+n & * \\ 0 & 1 & \gamma+k \\ 0 & 0 & 1 \end{pmatrix}$$

$$S^1 \hookrightarrow X \qquad T^{n_1} \hookrightarrow X_2$$

$$\downarrow \qquad\qquad \downarrow$$

$$T^2 \qquad\qquad X$$

$$T^{n_i} \hookrightarrow X_i \qquad \rightsquigarrow \text{variedades deste tipo são solvmanifolds.}$$

$$\downarrow$$

$$X_{i-1}$$

$f, g \in F[x]$ $\quad$ K' corpo decomp. de $f\,g$.

K - corpo de decomp. de f $\subset K'$

F' - cor. decom. de g. $\subset K'$

$$\begin{array}{ccc} K & \subset & K' \\ \cup & & \cup \\ f & & F' \\ \cup & & \cup \\ F & & g \end{array}$$

Seja $G = Gal(K/F)$ $\quad H = Gal(F'/F)$

$Gal(K'/F) \hookrightarrow G \times H$ subgrup.

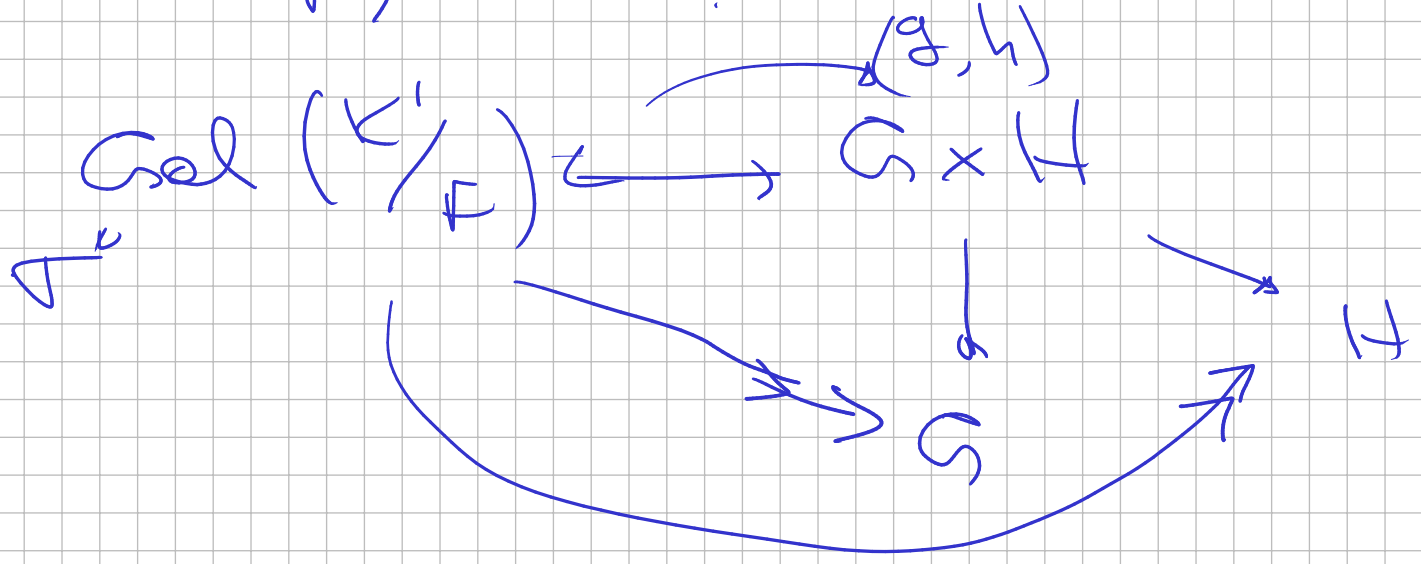
Teorema principal de Galois.

$$F \subset K \subset K'$$

$\longleftrightarrow$ Galois. $Gal(K'/F) \twoheadrightarrow G$

$$G = Gal(K'/F) \Big/ Gal(K'/K)$$

$Gal(K'/F) \twoheadrightarrow H$.



g, h age nas raízes de f.g.

se imagem de $\sigma = (id, id)$.

σ fixa raízes de $fg \Rightarrow \sigma = id$.

Teorema principal $f \in F[x]$.

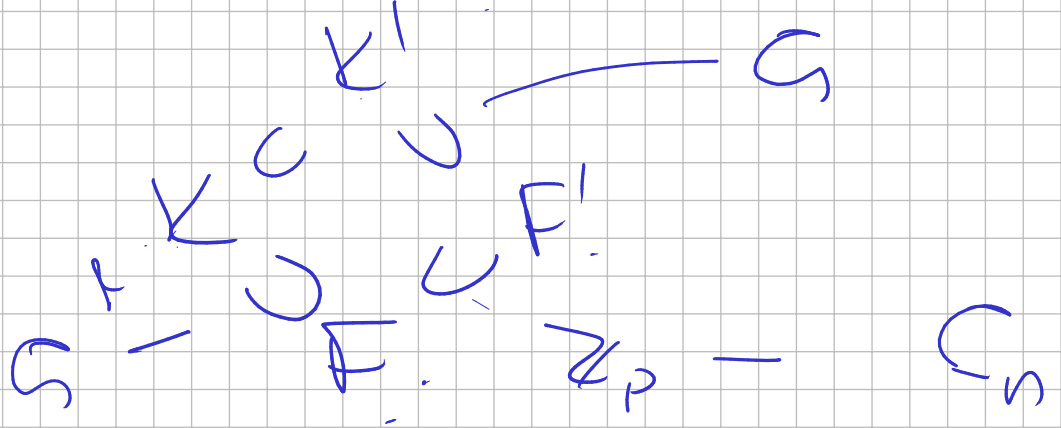
K = corpo decomp. de f. $G = Gal(K/F)$.

Suponha G simples não comutativo.

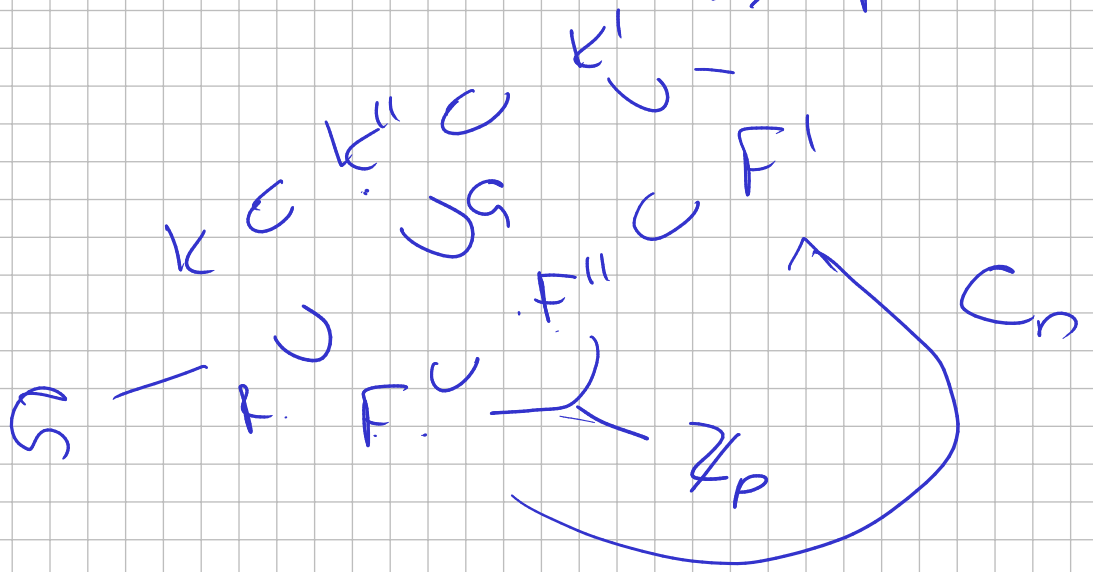
Seja $F' \supset F$ extensão cíclica.

K' corpo decomposição de f / F'

$\Rightarrow Gal(K'/F') \simeq G$.



Pf. escolhe $C_n \twoheadrightarrow Z_p$.



indução em $n \Rightarrow Gal(K/F) = G$.

$$\mathrm{Gal}(K''/F) \hookrightarrow G \times \mathbb{Z}_p$$

$$|G| \cdot p = [K:F] \cdot p$$

$$G$$

$$|\mathrm{Gal}(K''/F)| \;\Big|\; |G| \cdot p$$

$$\Downarrow$$

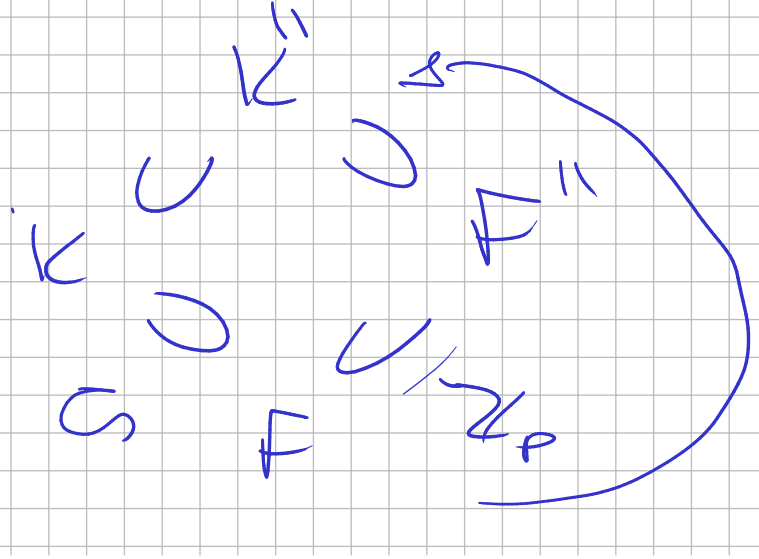
$$|G|$$

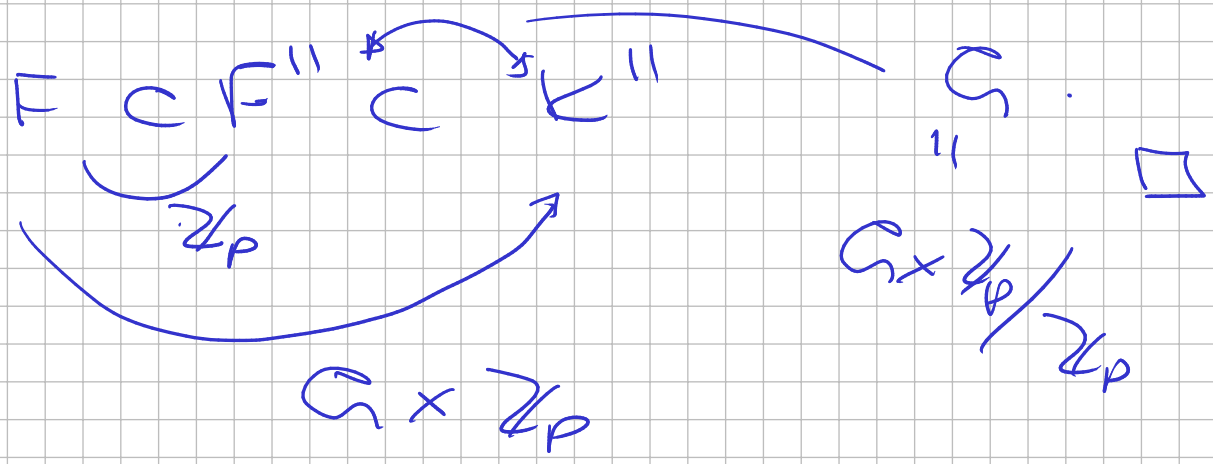
se $\mathrm{Gal}(K''/F) = G \Rightarrow K'' = K$.

mas K'' tem $\mathbb{Z}_p$ como quociente.

Absurdo.

$$\mathrm{Gal}(K''/F) \simeq G \times \mathbb{Z}_p.$$





□

Corollario: As raízes de $f \in F[x]$

$\deg f = 5$ $\quad Gal(K/F) = S_5$ ou A_5

K = corpo decomposição de f.

não são expressáveis por radicais

PR $\delta^2 = D$ $\quad \delta \in F$ $\quad F \subset F(\delta)$

$\sqrt{\ }$

posso assumir grupo de Galois é A_5

$f(\alpha) = 0$ α expressável por radicais.

$$F = F_0 \subset F_1 \subset \dots \subset F_r$$

$$A_5 \cap \quad A_5 \cap \quad \cap A_5$$

$$K \subset K_1 \subset K_r$$

$\alpha \in F_r$ agora. $f \in F_r[x]$ não é irredutível. $f = (x-\alpha)\, g$ $\deg g = 4$.

$\tau \in Gal\left(K_\tau / F_\tau\right)$ $\quad \tau \cdot \alpha = \alpha$.

$A_5 \curvearrowright \{\text{Raízes de } f\}$

não transitivamente.

Absurdo. $\lightning$

Observação: A_5 é o menor grupo simples não abeliano.

Por isso precisamos grau 5.

$f \sim Gal = S_5$

$G = \dfrac{Gal}{\text{Estab.}(\alpha_1)} \simeq \{\alpha_1, \ldots, \alpha_5\}$

$5 \mid |G|$ $\quad \tau = (12345) \in G$

O grupo S_5 é gerado por τ e qualquer transposição $\tilde{\tau}$.

Corolário. $f \in F[x]$ irredutível grau 5 mónico $\{\alpha_1, \ldots, \alpha_5\} \subset K$ corpo decompõe $F(\alpha_1, \alpha_2, \alpha_3) < K$

$\mathrm{Gal}(K/F) = S_5$ $\quad F'$

$\exists\ T \in \mathrm{Gal}(K/F)$ fixa $\alpha_1, \alpha_2, \alpha_3$ e não é id. $\alpha_4 \longleftrightarrow \alpha_5$

$f \in \mathbb{Q}[x]$ irred. mónico. 3 raízes reais. $\Rightarrow \mathrm{Gal}(f) = S_5$.

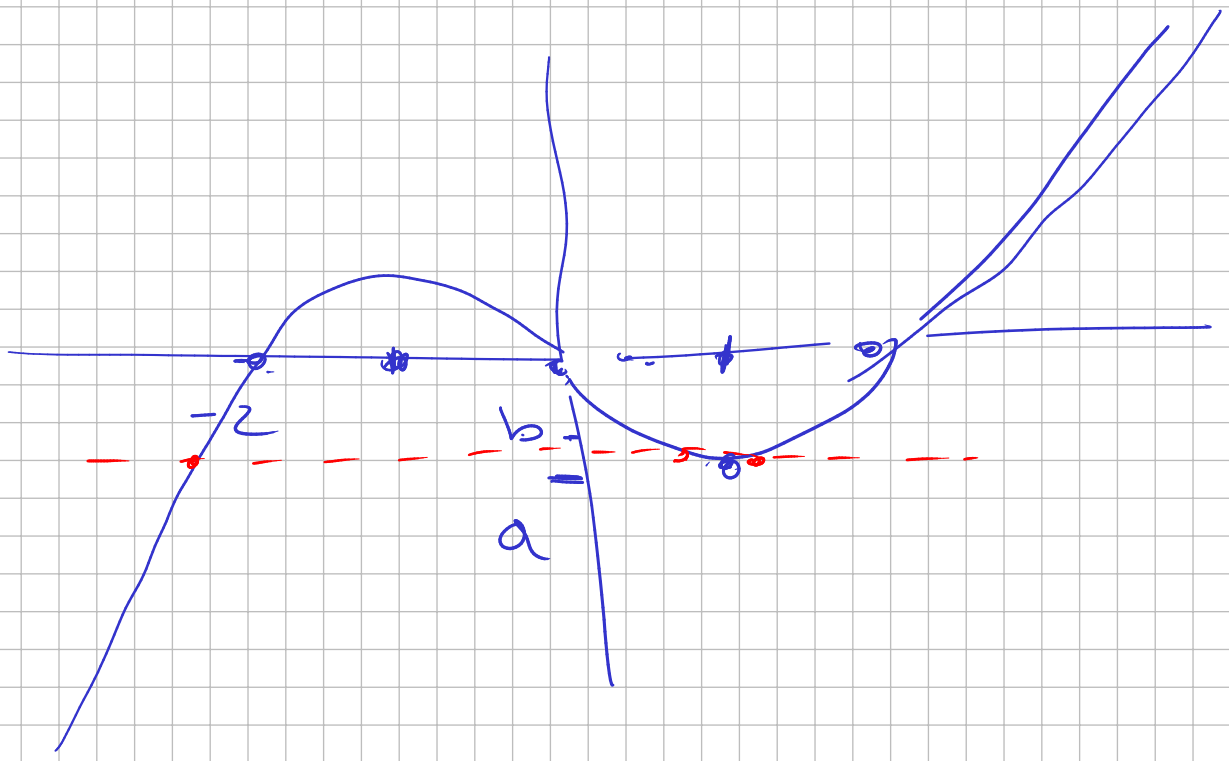
$\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subset \mathbb{R}$

$K \subset \mathbb{C}$

Encontrar polynomio com 3 raízes reais.

$$x^5 - 16x = x(x^4 - 16)$$
$$= x(x^2 - 4)(x^2 + 4)$$

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



$$x^5 - 16x + b \qquad b < a$$

$$\downarrow$$

$$x^5 - 16x + 2 \qquad \text{irred. pois} \quad 2 < a$$

$$f' = 5x^4 - 16 \Rightarrow x^4 = \frac{16}{5}$$

$$x = \sqrt[4]{\frac{16}{5}}$$

$$\left(\frac{16}{5}\right)^{5/4} - 16\left(\frac{16}{5}\right)^{1/4} < -2 \qquad \square$$