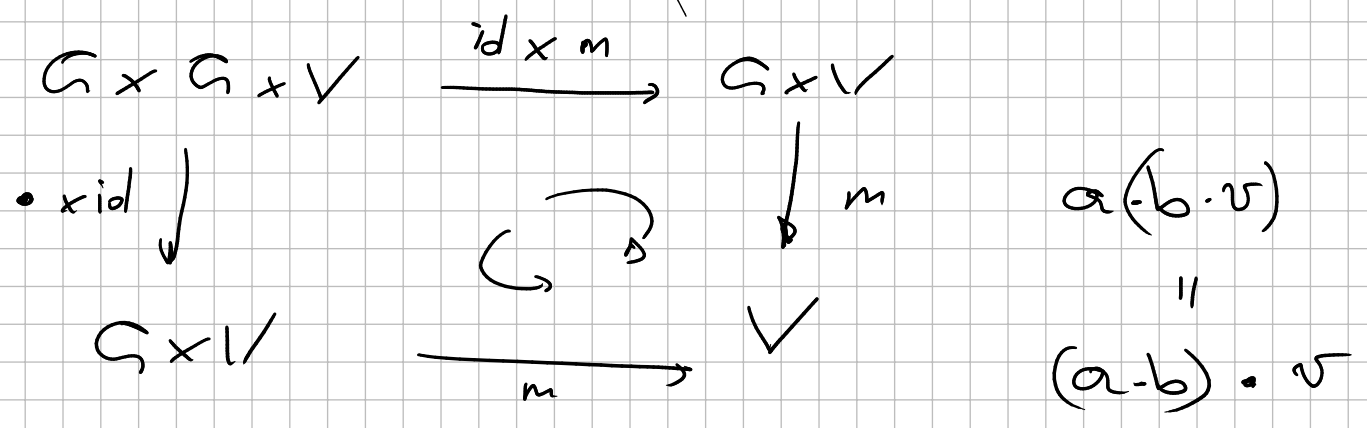


O grupo Simétrico.

G - grupo. uma representação ρ ou um G -módulo. $\rho: G \rightarrow \underline{GL(V)}$ $V \in k\text{-Vect}$

$$G \times V \xrightarrow{\rho} V$$

$$a, v \longmapsto \rho(a)(v) =: a \cdot v$$



$GL(V) = \text{Aut}_k(V) \subset \text{End}_k(V)$

$G = S_n = \text{Aut} \{1, \dots, n\}$ $|G| = n!$

$\rho: G \hookrightarrow GL_n(k)$ k -arbitrário

$V = k^{\oplus n}$ $\{e_i\}_{i=1}^n$

$\rho(\sigma) e_i = e_{\sigma(i)}$

Coro O grupo S_n age naturalmente em k^n . (Permutando a base).

G grupo. V, W duas representações $k\text{-Vect}$.

$V \oplus W \in G\text{-mod}$. $a \in G$ $v \in V$
 $w \in W$

$$a \cdot (v+w) = a \cdot v + a \cdot w$$

bases de V , e de $W \rightsquigarrow V \oplus W$

$$P_V: G \rightarrow GL(V) \quad P_W: G \rightarrow GL(W)$$

\downarrow $GL_{\dim V}(\mathbb{K})$

$$P_{V \oplus W}: G \rightarrow GL(V \oplus W)$$

$$P_{V \oplus W}(a) = \begin{bmatrix} P_V(a) & 0 \\ 0 & P_W(a) \end{bmatrix}$$

$V, W \in G\text{-mod}$. um homomorfismo de reps.

$$\varphi \in \text{Hom}_G(V, W) \quad T\varphi. \forall a \in G$$

$$v \in V. \quad \varphi(a \cdot v) = a \cdot \varphi(v)$$

$G\text{-mod}_G$ é uma categoria com esses morfismos.

$$\varphi \in \text{Hom}_G(V, W) = \left. \begin{array}{l} \varphi \in \text{Hom}_k(V, W) \\ \text{Ty } \varphi \text{ é morfismo} \\ \text{de } G\text{-mod} \end{array} \right\}$$

$$U := \text{Ker } \varphi \subset V \quad U \in G\text{-mod.}$$

$$\forall a \in G \quad u \in U.$$

$$a \cdot u \in V.$$

$$\downarrow$$

$$\text{ação em } V$$

$$\varphi(au) = \varphi(u) = 0$$

$$au \in U \subset V$$

$$K = \text{im } \varphi \subset W \quad K \in G\text{-mod.}$$

$$\vec{b} = \varphi(v)$$

$$a \cdot \vec{b} = a \varphi(v) = \varphi(\underbrace{a \cdot v}) \in K$$

$V \in G\text{-mod}$ Def um sub-módulo
é um $U \subset V$ estável pela ação
de G .

$$U \subset V \quad \rightsquigarrow \quad V/U \in G\text{-mod.}$$

$$a \cdot (v + U) = a \cdot v + U$$

⚠ categoria de grupos não
tem quocientes

$H \subset G \rightsquigarrow G/H$ não é um grupo



A categoria de G -módulos tem

$$\varphi \in \text{Hom}(V, W)$$

$$\text{coker } \varphi = W / \text{im}(\varphi) \in G\text{-mod}$$

$$0 \longrightarrow \text{Ker } \varphi \xrightarrow{i} V \longrightarrow \text{Coker } \varphi \longrightarrow 0$$

sequência exata curta.

$$V, W \in G\text{-mod} \rightsquigarrow \underline{V \otimes W} \in G\text{-mod}$$

$$a(v \otimes w) = av \otimes aw$$

$$\begin{aligned} (a \cdot b)(v \otimes w) &= (a \cdot b) \cdot v \otimes (a \cdot b) \cdot w \\ &= (a(b \cdot v)) \otimes (a \cdot (b \cdot w)) \\ &= a \cdot (b \cdot v \otimes b \cdot w) \\ &= a \cdot (b \cdot (v \otimes w)) \end{aligned}$$

$$V \in G\text{-mod} \text{ então } V^{\otimes n} := \underbrace{V \otimes V \otimes \dots \otimes V}_n$$

$\forall n$ n -vezes.

$$V^{\otimes 0} = \underset{\epsilon}{k} \in \bar{G}\text{-mod.}$$

$$a \cdot \alpha = \alpha$$

$$P: \bar{G} \rightarrow GL(V) \\ a \mapsto \text{id}_V.$$



$$\bar{G} = GL(V)$$

$$V \in \bar{G}\text{-mod.}$$

$$\text{id} = P: \bar{G} \rightarrow GL(V)$$

$$GL(V) \text{ acts on } V^{\otimes n} \quad \forall n.$$

$$\text{Sege } V \in k\text{-Vect} \quad \dim V < \infty.$$

$$\dim_k V^{\otimes n} = (\dim_k V)^n$$

$$V^{\otimes n} \in S_n\text{-modulo. natural}$$

$$\downarrow \quad v_1 \otimes \dots \otimes v_n \quad v_i \in V$$

$$\tau \in S_n \\ \tau =$$

$$\tau \cdot (v_1 \otimes \dots \otimes v_n) = v_{\tau(1)} \otimes \dots \otimes v_{\tau(n)}$$

$$(\tau \cdot \sigma) (v_1 \otimes \dots \otimes v_n) = \tau (\sigma(v_1 \otimes \dots \otimes v_n))$$

Observação. Seja $V \in k\text{-vect.}$

H, G dois grupos que agem em V . As ações comutam se

$$\forall v \in V \quad h \in H \quad g \in G.$$

$$h(g \cdot v) = g \cdot (h \cdot v)$$

Exemplo $V^{\otimes n}$ as ações de $a \in GL(V)$ e de S_n comutam.

$$\nabla (a \cdot v_1 \otimes \dots \otimes v_n) = (a v_{\tau(1)}) \otimes \dots \otimes (a v_{\tau(n)})$$

$$a (v_{\tau(1)} \otimes \dots \otimes v_{\tau(n)}) \neq$$



$V \in G\text{-mod.}$ $\left. \begin{array}{l} V^G \\ V_G \end{array} \right\} k\text{-Vect.}$

$$\underline{V^G} = \left\{ v \in V \mid a v = v \quad \forall a \in G \right\}$$

$$\underline{V_G} = V / \sim \quad \begin{array}{l} v \sim w \quad \exists a \in G \\ \text{t.q. } v = a \cdot w \end{array}$$

\sim é uma relação de equivalência:

$$\nu \sim \nu \quad \alpha = \text{id}_G$$

$$\nu \sim w \Rightarrow w \sim \nu \quad \nu = \alpha \cdot w \Rightarrow w = \alpha^{-1} \nu$$

$$\nu \sim w \quad w \sim z \Rightarrow \nu \sim z \quad \nu = \alpha w \quad w = \beta z$$
$$\nu = \alpha(\beta z) = (\alpha \cdot \beta) \cdot z$$

$$\mathbb{1} = \mathbb{k} \in G\text{-mod}$$

$$\text{Hom}_G(\mathbb{1}, V) = V^G$$

1). $\text{Hom}_G(V, W) \in \mathbb{k}\text{-Vect.}$

$$\varphi, \psi \in \text{Hom}_G(V, W) \quad \alpha, \beta \in \mathbb{k}$$

$$(\alpha \varphi + \beta \psi)(v) = \alpha \varphi(v) + \beta \psi(v)$$

$$\alpha \cdot (\alpha \varphi + \beta \psi)(v) = \alpha (\alpha \varphi(v)) + \alpha (\beta \psi(v))$$
$$= \alpha \varphi(\alpha v) + \beta \psi(\alpha v)$$

2) $\text{Hom}_{\mathbb{k}}(\mathbb{k}, V) \cong V$ como conj. mod.

3). $\text{Hom}_G(\mathbb{1}, V) \cong V^G$

$$\varphi(\mathbb{1}) \in V^G$$

$$\varphi(\alpha \mathbb{1}) = \alpha \varphi(\mathbb{1})$$
$$\varphi(\mathbb{1}) = \varphi(\mathbb{1})$$

$$V_S = ? \quad \cdot \quad V/\sim \quad \text{v.v.e.w}$$

* $\text{Hom}_S(V, \mathbb{1}) \cong \varphi$

$\varphi(v) \in k$ V^*

$\varphi(av) = a \cdot \varphi(v) = \varphi(v)$

$\text{Hom}_k(V/\sim, k)$ v.v.e.w

$$\text{Hom}_S(V, \mathbb{1}) = \text{Hom}_k(V_S, k)$$

\Downarrow

V_S^*

$$V_S = \text{Hom}_S(V, \mathbb{1})^*$$

$V \in k\text{-Vect} \quad \dim V < \infty.$

$$V^{\otimes n} \in S_n - G\text{-mod.}$$

$$GL(V)$$

—

$V \in \text{Vect } H, G \text{ commutes.}$

$$V^H, V_H \in G\text{-mod.}$$

$$g \in G, v \in V^H.$$

$$h(g \cdot v) = g h v = g v$$

\Downarrow

$$g v \in V^H \subset V$$

sub G -mod.

$$V \twoheadrightarrow V_H = V/\sim$$

$$0 \rightarrow U \rightarrow V \xrightarrow{\sim} V_H \rightarrow 0$$

$$v + U = [v].$$

$$g(v + U) = gv + U$$

$$V^H \hookrightarrow V \in \text{Hom}_G(V^H, V)$$

$$V \twoheadrightarrow V^H \in \text{Hom}_G(V, V^H)$$

$$V \in k\text{-vect} \quad V \otimes n \quad \hookrightarrow \quad S_n$$

$$\begin{array}{ccc} & & \\ & \searrow & \searrow \\ (V \otimes n)^{S_n} & & (V \otimes n)^{S_n} \end{array}$$

$$GL(V)\text{-mod}$$

$$V \in G\text{-mod.}$$

$$\left(H = \left. \begin{array}{l} a \in GL(V) \\ \neq \\ g \cdot a \cdot g^{-1} \\ = \\ a \cdot g \cdot g^{-1} \end{array} \right\} \right)$$

$$\text{Hom}_G(V, V) \stackrel{\text{invert.}}{\cong} \text{Aut}_G(V)$$

Let $\alpha \in V$. e counts α .

Theorem (Schur-Weyl) duality

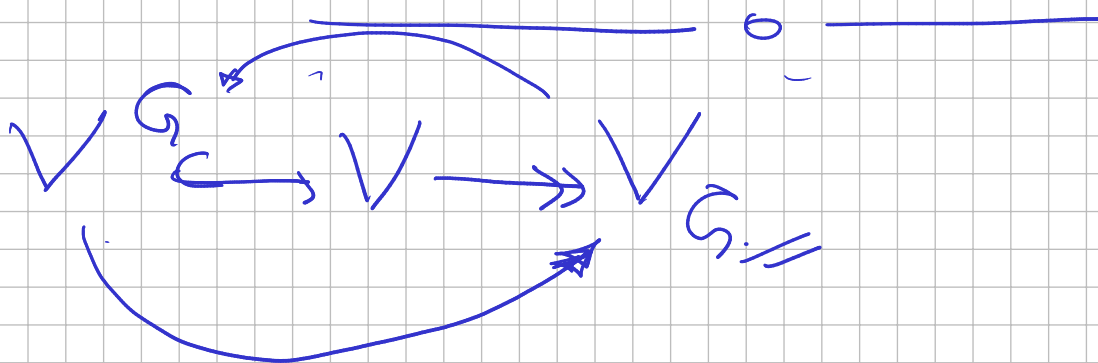
$$\text{As }_{GL(V)\text{-mod}} (V^{\otimes n}) \cong S_n$$



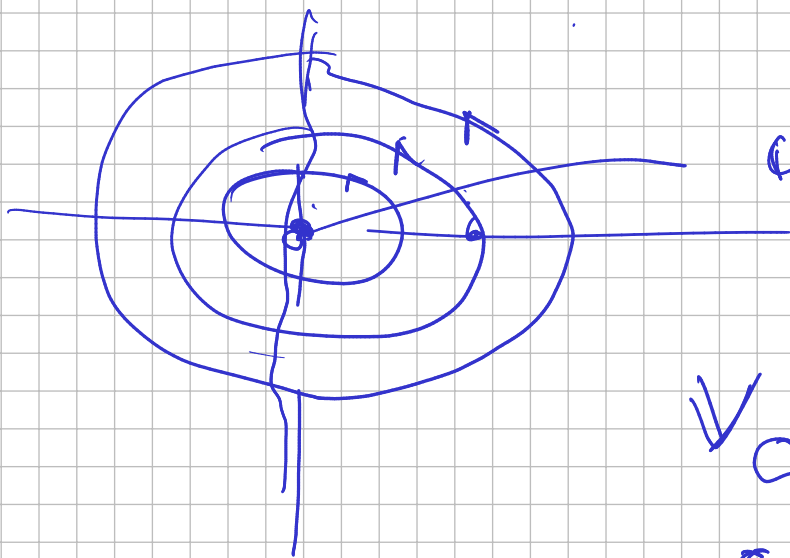
$$\text{As }_{S_n} (V^{\otimes n}) \cong GL(V)$$

$$\mathbb{C}^2 = \{ \uparrow, \downarrow \}$$

$$\underbrace{\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}_{n\text{-vectors}} \hookrightarrow GL(V)$$



$$G = \{ \sigma \in U(1) \subset \mathbb{C} \}$$



um = 2
quatro raios.

$$\begin{aligned} \mathbb{V}_G &\cong \mathbb{R}_{\neq 0} \\ \mathbb{V}_G &= * 0 \end{aligned}$$

Seja $\{v\} \in V_G$ G grupo

$v \in V$ uma preimagem de v .

$$\omega = \frac{1}{|G|} \sum_{g \in G} g \cdot v$$

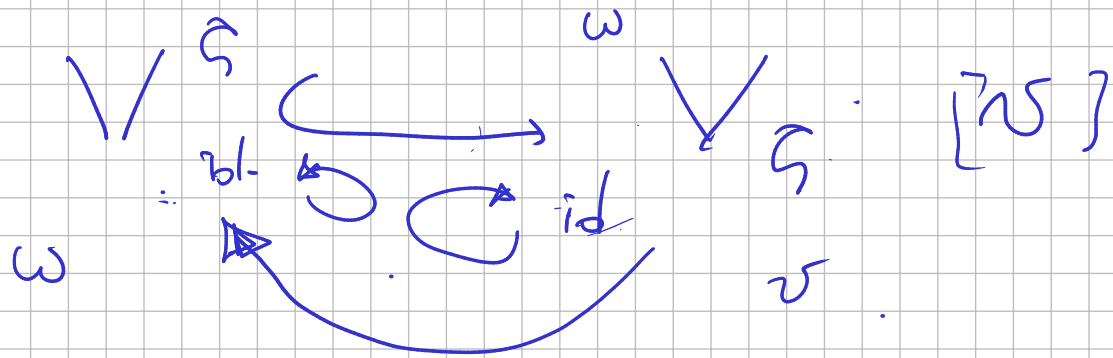
$$\boxed{\omega \sim v}$$

$$a = \text{id}_G \cdot v + \sum_{g \in G, g \neq 1} g \cdot v$$

$|G|$ elementos
todos equivalentes a v .

$$\omega \in V^G$$

$$\begin{aligned} b \cdot \omega &= \frac{1}{|G|} \sum b \cdot g \cdot v \\ &= \frac{1}{|G|} \sum_{g \in G} g \cdot v = \omega \end{aligned}$$



$$\omega \in V^S \longrightarrow [\omega]_S \in V/S$$

$$\frac{1}{|S|} \sum_{\alpha \in S} \alpha \cdot \omega = \frac{1}{|S|} \sum \omega = \omega$$

$$V^S \xrightarrow{\cong} V/S \quad \text{são espaços isomorfos.}$$

$$0 \rightarrow V \rightarrow V/S \rightarrow 0$$

$$\boxed{S+0} \quad \frac{1}{|S|} \sum \alpha \cdot v$$

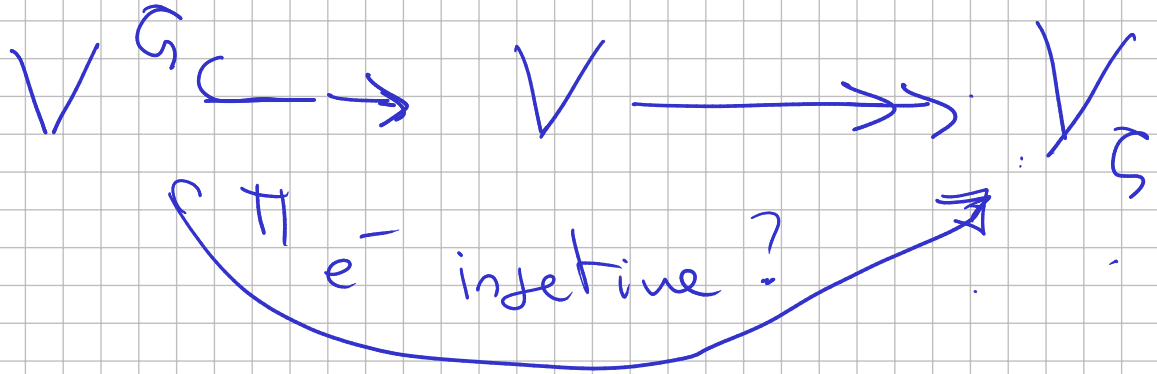
$$[v]_S \xrightarrow{\cong} \omega = \frac{1}{|S|} \sum \alpha \cdot v$$

$$\begin{aligned} \omega' &= \frac{1}{|S|} \sum \alpha v + \alpha u \\ &= \omega + \left(\frac{1}{|S|} \sum \alpha u \right) \end{aligned}$$

$$= \omega + \left(\frac{1}{|S|} \sum \alpha u \right) = \omega + 0 = \omega$$

0 que $e^{-1} U \subset V$?

$$\alpha \cdot v = v \quad \forall v \in U$$



$$v \in V^S$$

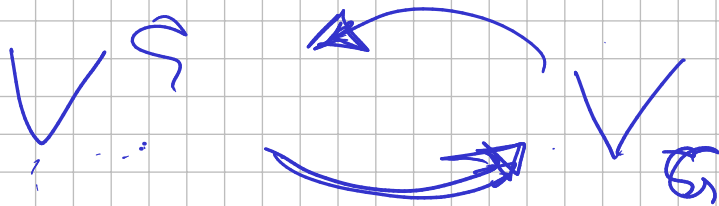
$$\alpha \cdot v = v \quad \forall \alpha \in G$$

$$\boxed{\pi(v) = 0}$$

$$0 \sim v$$

$$\pi(0) = 0$$

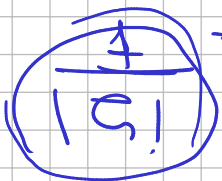
$$\alpha \cdot v = 0$$



$$w$$



$$[w]$$



$$\sum \alpha \cdot v$$



$$[v]$$

char $k = 0$ ou se $|G|$
 e^{-1} invertível ($\neq 0$). então.

$$V^S \xrightarrow{\cong} V^S$$

Existen grupos abelianos.

$$H^i(\mathfrak{g}, V)$$

$$H_0(\mathfrak{g}, V)$$

$$H^0(\mathfrak{g}, V) = V^{\mathfrak{g}}$$

$$H_0(\mathfrak{g}, \underline{V}) = V_{\mathfrak{g}}$$

em char 0 S_0 isomorphic.

char p S_0 diferentes.

$$V^{\mathfrak{g}} = \text{Hom}(\mathbb{1}, V) = V$$

(char 0 $\mathbb{1} = \mathbb{1}$)

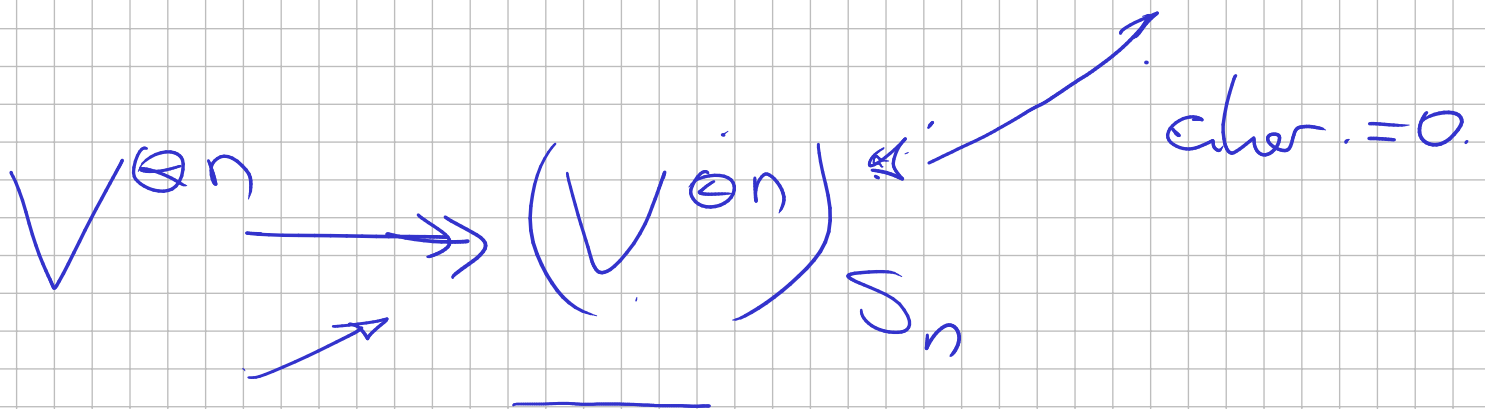
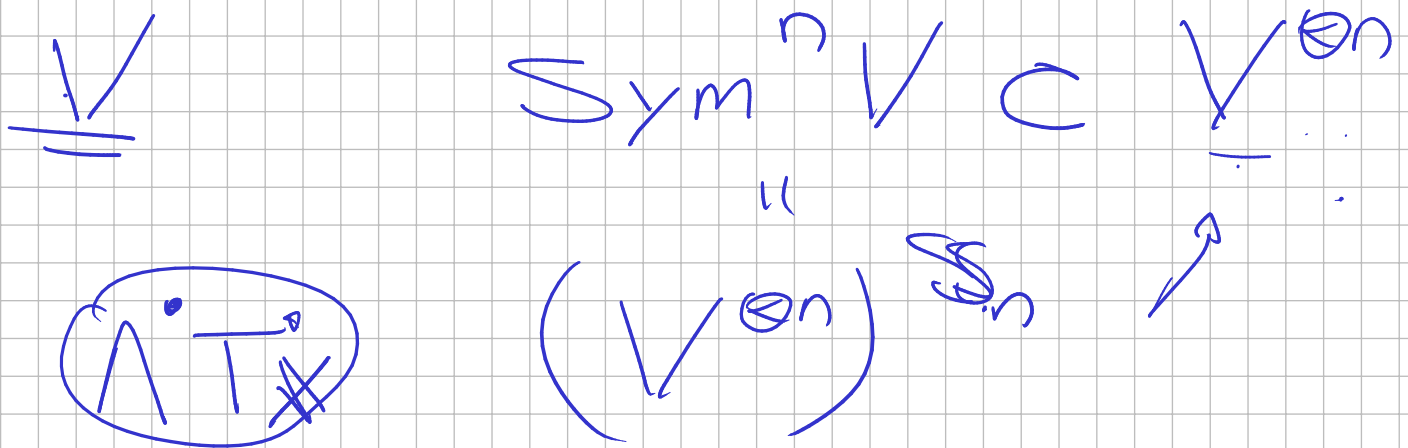
$$V_{\mathfrak{g}} = \text{Hom}_{\mathfrak{g}}(V, \mathbb{1})^* = (V^*)^*$$

$$\begin{array}{ccc} \text{Hom}(V, W) & \cong & V^* \otimes W \\ \downarrow * & & \downarrow * \\ \text{Hom}(W, V) & \cong & V \otimes W^* \end{array}$$

$$\text{Hom}(V, W) \xrightarrow{\cong} V^* \otimes W$$

$|2^*$

$$\text{Hom}(W^*, V^*) \xrightarrow{\cong} W \otimes V^*$$



$$V = k^{\oplus n} \mapsto W = \bigoplus_{k \geq 0} V^{\otimes k} \hookrightarrow S_n$$

$$W^{\text{Sym}} = \bigoplus_{k \geq 0} \text{Sym}^k(V^*) = \bigoplus_{k \geq 0} (V^{\otimes k})^{S_k} \hookrightarrow S_n^k$$

$W^{\text{Sym}} \subset W$ = polinômios polinômiais em

em k/Sym temos uma ação de

$$GL(V^*) \curvearrowright S_n$$

$$R \text{ anal. } \mathbb{R}[\mu_1, \dots, \mu_n]$$

o grupo S_n age em $\mathbb{R}[\mu_1, \dots, \mu_n]$

$$\sigma \in S_n \quad f \in \mathbb{R}[\mu_1, \dots, \mu_n]$$

$$(\sigma \cdot f) = f(\mu_{\sigma^{-1}(1)}, \dots, \mu_{\sigma^{-1}(n)})$$

$$\tau \in S_n \quad \tau \cdot (\sigma \cdot f) = (\sigma \cdot f)(\mu_{\tau^{-1}(1)}, \dots, \mu_{\tau^{-1}(n)})$$

$$= f(\mu_{\sigma^{-1}(\tau^{-1}(1))}, \dots, \mu_{\sigma^{-1}(\tau^{-1}(n))})$$

$$= f(\mu_{(\tau \cdot \sigma)^{-1}(1)}, \dots, \mu_{(\tau \cdot \sigma)^{-1}(n)})$$

$$= ((\tau \cdot \sigma) \cdot f)(\mu_1, \dots, \mu_n)$$

$$\tau \cdot (\sigma \cdot f) = (\tau \cdot \sigma) \cdot f$$

Def. um polinômio $f \in \mathbb{R}[\mu_1, \dots, \mu_n]$ é simétrico se é invariante por S_n .

$$\mathbb{R}[\mu_1, \dots, \mu_n] = \bigoplus \text{Especos de m. finte.} \\ \bigoplus_{k \geq 0} \text{polynomial homog.} \\ \text{de grau } k \\ \bigoplus \text{Sym}^k(\mathbb{R}^n)$$

seja $f \in \mathbb{R}[\mu_1, \dots, \mu_n]$.

$\frac{1}{|S_n|} \sum_{\sigma \in S_n} (f \circ \sigma)$ é simétrica.

Exemplo. $f = \underline{\mu_1} \cdot \mu_2^2 \in \mathbb{R}[\mu_1, \mu_2, \mu_3]$

$$\begin{aligned} &\mu_1 \mu_2^2 + \mu_2 \mu_3^2 + \mu_3 \mu_1^2 \\ &\mu_2 \mu_1^2 + \mu_3 \mu_2^2 + \mu_1 \mu_3^2 \end{aligned}$$

é simétrico.

$$(x - \mu_1) \cdot (x - \mu_2) \cdots (x - \mu_n) \in \mathbb{R}[\mu_1, \dots, \mu_n] \text{ Sym}$$

os coeficientes de x^k são simétricos

$$x^n - \overbrace{\left(\sum \mu_i\right)}^{S_1} x^{n-1} + \overbrace{\sum_{1 \leq i < j \leq n} \mu_i \mu_j}^{S_2} x^{n-2} - \dots$$

$$+ \dots + (-1)^n \underbrace{\prod \mu_i}_{S_n} \cdot x^0$$

$$\sum_{k=0}^n (-1)^k x^{n-k} \cdot S_k$$

$$S_k \in \mathbb{R}[\mu_1, \dots, \mu_n]^{S_n}$$

$$\deg S_k = k.$$

$$S_0 = 1 \quad S_1 = \sum \mu_i \quad S_2 = \sum_{1 \leq i < j \leq n} \mu_i \mu_j$$

$$S_n = \prod_{i=1}^n \mu_i$$

Teorema Todo polynômio simétrico em n -variáveis se escreve de fato como polynômio nas S_i , $i=0, \dots, n$.

$$\begin{array}{ccc} \mathbb{R}[z_1, \dots, z_n] & \longrightarrow & \mathbb{R}[\mu_1, \dots, \mu_n] \\ \underbrace{z_i} & \longmapsto & \underbrace{S_i} \end{array}$$

- 1) Todo polynômio simétrico está na imagem
- 2) O núcleo do morfismo é nulo.

Corollário... Não existem relações polinômiais entre os s_i

\Leftrightarrow O subanel de polinômios simétricos em n -variáveis é isomorfo ao anel de polinômios em n -variáveis.

$$(x - \mu_1) \cdots (x - \mu_n)$$

$$\Delta(\mu_1, \dots, \mu_n) = \prod_{1 \leq i < j \leq n} (\mu_i - \mu_j)^2$$

$$\mathbb{R}[\mu_1, \dots, \mu_n]^{S_n}$$

Pelo teorema Δ se escreve de fato único como combinação das s_i !

$$n=0 \quad \Delta = 1$$

$$n=1 \quad \Delta = 1$$

$$n=2 \quad \Delta = (\mu_1 - \mu_2)^2$$

$$s_0 = 1 \quad s_1 = \mu_1 + \mu_2 \quad s_2 = \underbrace{\mu_1 \cdot \mu_2}$$

$$(\mu_1 - \mu_2)^2 = \mu_1^2 + \mu_2^2 - 2\mu_1 \mu_2$$

$$s_1^2 = \mu_1^2 + \mu_2^2 + 2\mu_1 \mu_2$$

$$\Delta = S_1^2 - 4S_2 \quad \Leftarrow n=2$$

Def. Seja $f = X^n - a_1 X^{n-1} + a_2 X^{n-2} + \dots + (-1)^n a_n X^0$

$$a_i \in \mathbb{R} \quad f \in \mathbb{R}[X]$$

$$D(f) := \Delta(a_1, \dots, a_n) \in \underline{\mathbb{R}}$$

Ex.: $D(X^2 - bx + a) = b^2 - 4a$

n=3 $\Delta = (\mu_1 - \mu_2)(\mu_1 - \mu_3)(\mu_2 - \mu_3)^2$

Pode ser escrito de jeito único em termos de S_1, S_2, S_3

$$\Delta = \underbrace{-27}_{.27} S_3^2 + 18 S_3 S_2 S_1 + \underbrace{-4}_{-4} S_3^3 S_1^3 - 4 S_2^3 + S_2^2 S_1^2 + 0 S_2 S_1^4 + 0 S_1^6$$

$3\alpha + 4\alpha - 2\beta = 4$

$$x^2(x-1) \Rightarrow D=0$$

$$x^3 - x^2 \Rightarrow s_1 = 1 \quad s_2 = s_3 = 0$$
$$= \text{coef.}(s_1^6) = 0$$

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

$$s_1 = s_2 = 0 \quad s_3 = -1$$
$$\text{coef}(s_2^3) = -4$$

$$x^3 - 1 = (x-1)(x^2+x+1) = (x-1)\left(x - \frac{-1+\sqrt{-3}}{2}\right)$$
$$s_1 s_2 = 0 \quad s_3 = 1 \quad \left(x - \frac{-1-\sqrt{-3}}{2}\right)$$

$$D = \left(\frac{3-\sqrt{-3}}{2}\right)^2 \left(\frac{3+\sqrt{-3}}{2}\right)^2 (\sqrt{-3})^2$$

$$\left(\frac{9+3}{4}\right)^2 \cdot (-3) = -27$$

$$\text{coef}(s_3^2) = +27$$

$$x^3 - 2x^2 + 1 \quad s_2 = 0 \quad s_1 = 2 \quad s_3 = -1$$

$$(x-1) \cdot (x^2 - x - 1) = (x-1)\left(x - \frac{1+\sqrt{5}}{2}\right)$$
$$\left(x - \frac{1-\sqrt{5}}{2}\right)$$

$$D = \left(\frac{1 - \sqrt{3}}{2} \right)^2 \left(\frac{1 + \sqrt{3}}{2} \right)^2 (\sqrt{3})^2$$

$$= \left(\frac{-4}{4} \right)^2 S = S = D.$$

$$(-2\alpha) \cdot 4 - \alpha \cdot 8 = S$$

$$\alpha = \frac{-S - 2\alpha \cdot 8}{8} = -4$$

$$\underline{\text{coef}} (S_1^3 \cdot S_3) = -4.$$

$$P = X(X+1)(X-2) = X(X^2 - X - 2)$$

$$X^3 - X^2 - 2X \quad S_1 = 1 \quad S_2 = -2$$

$$S_3 = 0$$

$$D = 4 \cdot 9 = 36$$

$$32 + 4\alpha \cdot -2\beta = 36 =$$

$$\beta = -2 + 2\alpha$$

achar o erro.

$$X(X+1)(X-3) \rightarrow$$

$D \neq 0$. os raízes são diferentes
2 e -2. no corpo de decomposição

é o ~~an~~ Galois = S_n ?

Prove o teorema.

$\{S_i^{(n)}\}_{i=1}^n$ os polinômios são simétricos em n -variáveis.

$$P \in \mathbb{R}[x_1, \dots, x_n]^{S_n}$$

$$\bar{P} = P(x_1, \dots, x_{n-1}, 0)$$

$$\in \mathbb{R}[x_1, \dots, x_{n-1}]^{S_{n-1}}$$

indução. $\exists! \psi \in \mathbb{R}[z_1, \dots, z_{n-1}]$

$$\forall \bar{P} = \psi \left(\overline{S_1^{(n-1)}}, \dots, \overline{S_{n-1}^{(n-1)}} \right)$$

$$P = \psi \left(S_1^{(n)}, \dots, S_{n-1}^{(n)} \right) = g$$

g é simétrico em n -variáveis.

$$g(x_1, \dots, x_{n-1}, 0) = \bar{P} = \psi \left(\overbrace{S_1^{(n)}(x_1, \dots, x_{n-1}, 0)}^{S_1^{(n-1)}(x_1, \dots, x_{n-1})}, \dots, \overbrace{S_{n-1}^{(n)}(x_1, \dots, x_{n-1}, 0)}^{S_{n-1}^{(n-1)}(x_1, \dots, x_{n-1})} \right)$$

observação. $S_i^{(n)}(x_1, \dots, x_{n-1}, 0) = S_i^{(n-1)}$

$$g(\mu_1, \dots, \mu_{n-1}, 0) = 0$$

$\mu_n \mid g$ como g é simétrico

$\mu_{\tau^{-1}(n)} \mid g \quad \forall \tau \in S_n.$

$$\prod_{i=1}^n \mu_i \mid g$$

$S_n^{(n)}$

$$R - \psi(S_1^{(n)}, \dots, S_{n-1}^{(n)}) = S_n^{(n)} \cdot \underline{h}$$

$$\deg h < \deg R.$$

h é simétrico em n -variáveis.

por indução. $\exists! \varphi \in \mathbb{R}[z_1, \dots, z_n]$

$$h = \varphi[S_1^{(n)}, \dots, S_n^{(n)}]$$

$$R = \psi(S_1^{(n)}, \dots, S_{n-1}^{(n)}) + S_n^{(n)} \cdot \varphi(S_1^{(n)}, \dots, S_n^{(n)})$$

□.

$$\mathbb{R}[z_1, \dots, z_n] \hookrightarrow \mathbb{R}[u_1, \dots, u_n]$$

$$\text{funções } (\mathbb{A}^n) \longrightarrow \text{funções } (\mathbb{A}^n)$$

$\pi: \mathbb{A}^n \rightarrow \mathbb{A}^n$ ideal maxi $(u_1 - x_1, \dots, u_n - x_n)$
 $\pi(x) = \underline{\underline{\pi(x)}}$ = polim simétricos que são 0 em x .
 $\mathbb{R} = \mathbb{C}$

$$\pi(y) = \pi(x) \quad \exists \sigma \in S_n \text{ t.q. } \sigma(x) = y \quad !$$

$$\mathbb{A}^n \longrightarrow (\mathbb{A}^n) / S_n$$

Elementos primitivos.

Teorema: seja $F \subset K$ uma extensão finita com $\text{char } F = 0 \Rightarrow \exists \gamma \in K$ st $F(\gamma) = K$.

Def Um elemento $\gamma \in K$ como no Teorema é chamado primitivo

Pt $F \subset K$ é finita. $K = F(\alpha_1, \dots, \alpha_n)$
finitos elementos. Podemos
indução em n .

$$n=1 \quad \checkmark \quad K = F(\alpha_1) \Rightarrow \gamma = \alpha_1$$

Assumindo o teorema para n .

$$K = F(\alpha_1, \dots, \alpha_n, \alpha_{n+1})$$

U

, indução.

$$F(\alpha_1, \dots, \alpha_n) = F(\gamma')$$

$$K = F(\underline{\gamma'}, \alpha_{n+1}) \supset F$$

Reduzimos o problema para
o caso $K = F(\alpha, \beta) \supset F$.

Sejam $f(x), g(x) \in F[x]$ irred.
Para α e β respectivamente.

Cher o $\exists K'$ Tq. f, g se
fatoram como produto de lineares
com fatores diferentes.

$$\alpha = \alpha_1, \dots, \alpha_n \quad \beta = \beta_1, \dots, \beta_m$$

$f(x)$ $g(x)$

$$\alpha_i \neq \alpha_j \quad i \neq j$$

$$\beta_i \neq \beta_j \quad i \neq j.$$

$$\begin{array}{c} K \\ \Rightarrow \\ K \end{array} = \beta + c\alpha \quad c \in F$$

$F \subset F(\alpha) \subset F(\alpha, \beta) = K$

basta provar $\alpha \in F(\beta)$ \Leftarrow

$$\Rightarrow \beta = \gamma - c \cdot \alpha \in F(\alpha)$$

f é o polinômio irred. de α } $F(\alpha)$
 g " " " " β }

$$h(x) = g(\gamma - c\alpha) \in \underline{\underline{F(\alpha)[x]}}$$

$$h(\alpha) = g(\gamma - c\alpha) = g(\beta) = 0$$

Quais são os fatores comuns. entre

$$h \text{ e } f. \text{ em } \underline{\underline{F(\alpha)[x]}} \subset K'[\alpha]$$

Tem uma raiz comum α .

$g \text{ col. em } K'[\alpha]$.

$$f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_n).$$

$$\underline{(x - \alpha)} \mid f \text{ e } h. \text{ em } K'[\alpha]$$

Suponha nenhum outro fator $(x - \alpha_i)$ $i \neq 1$ divide h .

$$\Rightarrow \gcd(h, p) = (x - \alpha)$$

$$K[x] \text{ ou } F(\alpha)[x]$$

$$\Rightarrow \alpha \in F(\alpha) \Rightarrow F(\alpha) = K.$$

β_1, \dots, β_m são os raízes de g .

$$h(x) = g(\underbrace{x - c \cdot x}_{\beta_i}).$$

$$x - cx = \beta_i \text{ para algum } i.$$

$$x = \frac{x - \beta_i}{c} \quad x = \beta + c \cdot \alpha$$

$$x = \frac{\beta - \beta_i}{c} + \alpha \quad \text{para } i=1, \dots, m$$

outra. $x \neq \alpha_j$ quando x seja raiz de h $j \neq 1$.

$$\alpha_j = \frac{\beta - \beta_i}{c} + \alpha$$

$$\Rightarrow c = \frac{\beta - \beta_i}{\alpha_j - \alpha} \quad j \neq 1 \quad (*)$$

(*) \bar{K} é um corpo finito de elementos.

$$i = 2, \dots, m \quad j = 2, \dots, n.$$

$$C \in \mathcal{A} \quad |F| = \infty. \quad \text{char } F = 0.$$

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

$\exists c \in F$ tal que $\alpha = \alpha_c$ e

o único divisor comum de

h e f . □.

Exemplo: $K = \mathbb{Q}[\alpha, \beta] \supset \mathbb{Q}$
 $\alpha = \sqrt{-1}$ $\beta = \sqrt[3]{2}$
 $\deg = 6.$

$$x^2 + 1$$

$$x^3 - 2$$

$$\alpha, -\alpha$$

$$\beta = \sqrt[3]{2}$$

$$\zeta \sqrt[3]{2}$$

$$\zeta^2 \sqrt[3]{2}$$

$$\alpha_1, \alpha_2$$

$$\beta_1$$

$$\beta_2$$

$$\beta_3$$

$$\zeta = e^{2\pi i/3}$$

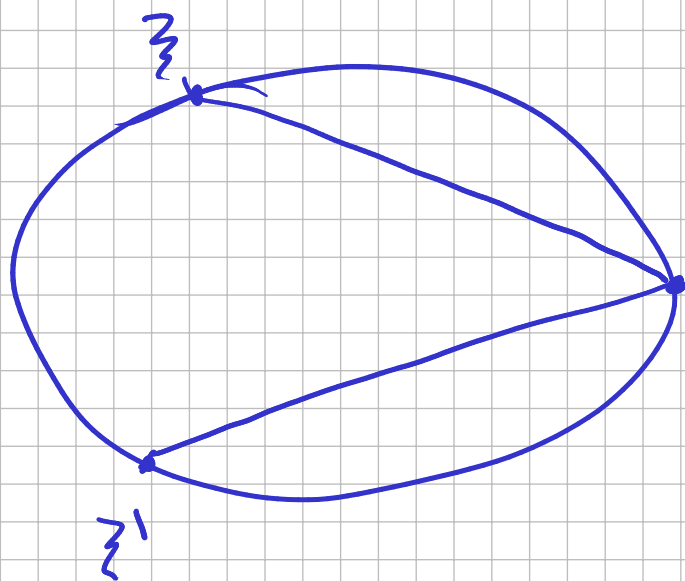
K é gerado por combine com de forma.

$$c \neq \frac{\beta + c\alpha}{\alpha_j - \alpha}$$

$$j = 2 \\ i = 2, 3$$

$$c \neq - \frac{\beta - \beta_i}{2\alpha} = i \frac{\sqrt[3]{2}}{2} \left(1 - \zeta^i \right)$$

\mathbb{P}
 \mathbb{Q} .



$$\forall c \in \mathbb{Q}. \quad \left(\sqrt[3]{2} + c \cdot i \right) \text{ gera} \\ K = \mathbb{Q}(\sqrt[3]{2}, i).$$

irred. desse \mathcal{P} tem grau G .

Prop. Seja $G \subset \text{Aut } K$. seja $F = K^G$. seja $\beta \in K$.
 $\beta = \beta_1, \beta_2, \dots, \beta_n$ órbita de β

Pela ação de G . \Rightarrow

1) β é algébrico / F

2) $\deg \beta = n$

3) irred de $\beta = (x - \beta_1) \dots (x - \beta_n)$.

seja $f \in F[x]$ o polinômio monico irred. de β .

G age em K e fixa $f \in F[x]$

\Rightarrow Todo β_i é uma raiz de f

$g = (x - \beta_1) \dots (x - \beta_n) \mid f$.

g é fixo por todos os elms de G . $\Rightarrow g \in F[x]$

$\Rightarrow g = f$. \square

\overline{E}_x $\mathbb{Q} \subset K = \mathbb{Q}(i, \sqrt{2})$
↑ grau 4. $\text{Gal}(K/\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2$

$i \longleftrightarrow -i$

$\sqrt{2} \longleftrightarrow -\sqrt{2}$

$\beta = \beta_1 = i + \sqrt{2}$

$\beta_2 = -i + \sqrt{2}$

$\beta_3 = i - \sqrt{2}$

$\beta_4 = -i - \sqrt{2}$

irred. de p. tem grau 4

$$K = \mathbb{Q}(i + \sqrt{2}) \supset \mathbb{Q}$$

↑
grau 4.

$$(x - i - \sqrt{2})(x + i - \sqrt{2})(x - i + \sqrt{2})(x + i + \sqrt{2})$$

$$(x^2 - 2\sqrt{2}x + 3)(x^2 + 2\sqrt{2}x + 3)$$

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

$$= x^4 - 2x^2 + 9$$

é irred. sobre \mathbb{Q} , grau 4.
sobre $\mathbb{Q}(i, \sqrt{2})$.

Não é surpreendente que

polinômio é de forma:

$$g(h(x)) \quad \text{com} \quad \deg g = \deg h = 2$$

⇔

Cor: se K/F é Galois $g \in F[x]$
é irreduzível. se g tem uma raiz
em $K \Rightarrow g = (x - \alpha_1) \dots (x - \alpha_n)$
em $K[x]$.

$$F = K^{\text{Gal}(K/F)}$$

$$\alpha = \alpha_1 \text{ raíz de } g.$$

$$\forall g \in G = \text{Gal.}$$

$$g(\alpha) \text{ é raíz de } g.$$

$\alpha_1, \dots, \alpha_n$ órbita de α .

$$g(x) = (x - \alpha_1) \dots (x - \alpha_n). \quad \square$$

Cor. K/F é Galois então é o corpo de decomposição de algum $f \in F[x]$.

$$K = F(\alpha_1, \dots, \alpha_n)$$

$f_1, \dots, f_n \in F[x]$ irred para $\alpha_1, \dots, \alpha_n$

$$K = \underline{\underline{\prod f_i}}$$

K é corpo de decomposição de f .

Teorema: $G \subset \text{Aut}(K) \quad |G| = n$

$$F = K^G \Rightarrow [K:F] = n$$

Pf. $\forall \beta \in K$ G -órbita é finita

$\Rightarrow \beta$ é algébrico. / F

Seja $\{\beta_1, \dots, \beta_m\}$ a G -órbita de β .

$\Rightarrow m | n$.

$\exists \beta \in K$ primitivo. $[K:F] = \text{deg } \beta = m | n$

$$[K:F] \geq n.$$

Seja $\beta \in K$ primitivo.

$$G \curvearrowright K. \quad \{\beta = \beta_1, \dots, \beta_m\} = \mathcal{O}_\beta$$

e_i e órbita. $m < n$.

$$G \supset G_\beta = \{g \in G \mid g \cdot \beta = \beta\} \neq \text{id}$$

$$\mathcal{O}_\beta \cong G/G_\beta$$

$$g \cdot G_\beta \xrightarrow{\sim} g \cdot \beta$$

$$|\mathcal{O}_\beta| \cdot |G_\beta| = |G| = n$$

m

os fixos por G são F . $\beta \notin F$

$$\text{id} \neq g \in G_\beta \quad g(\beta) = \beta.$$

$$g \text{ fixa } F(\beta) = K.$$

$$\Rightarrow g = \text{id}. \quad \text{absurdo.}$$

$$|\mathcal{O}_\beta| = n. \quad \square$$

$$K/F \text{ finita.} \Rightarrow |G(K/F)| \text{ divide } [K:F]$$

$$K \supset K^G \supset F$$

↖
deg.

$F \subset K$ extensão finita $|G| = |\text{Gal}(K/F)| \mid [K:F]$

$$G = \text{Gal}(K/F) \subset K. \quad |G| = [K:K^G]$$

$$\text{e temos } F \subset K^G \subset K$$

$$[K:K^G] \mid [K:F]. \quad \square$$

↙
Corollario $F = K^{\text{Gal}(K/F)}$

Usei isso no teorema da última aula.

Controlar que não tem rotaciones circulares.

Corollario. - G grupo de sim. sobre K .
seja $F = K^G \Rightarrow$

$K \supset F$ é Galois e

$$G = \text{Gal}(K/F).$$

Pr. $\forall g \in G$. see F -automorfismos de K .
 $\Rightarrow G \subset \text{Gal}(K/F)$
 $|\text{Gal}(K/F)| \leq [K:F]$

$$[K:F] = |G| \Rightarrow |G(K/F)| = [K:F]$$

$$\Rightarrow K/F \text{ é Galois} \quad G(K/F) = G.$$

$\mathbb{C}(y) = K$ funções racionais \mathbb{P}^1 .

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \quad \text{age por} \quad \begin{array}{l} y \rightarrow -y \\ y \rightarrow iy^{-1} \end{array}$$

$$K^G = F$$

lemme. $F \cong \mathbb{C}(w) \quad w = y^2 - y^{-2}$

$$\mathbb{C}(y^2 - y^{-2}) \subset \mathbb{C}(y)$$

$$Y \longleftarrow X$$

Pf. G fixa $w = y^2 - y^{-2}$

$$(-y)^2 = y^2$$

$$(-y)^{-2} = y^{-2}$$

$$w \in F = K^G$$

$$\text{seja } p \in F[X]$$

o polinômio irreduzível de y

$$y \rightarrow -y \rightarrow iy^{-1} \rightarrow -iy^{-1}$$

$$(x - y)(x + y)(x - iy^{-1})(x + iy^{-1})$$

$$= (x^2 - y^2)(x^2 + y^{-2}) = x^4 - (y^2 - y^{-2})x^2 - 1$$

$$x^4 - \omega x^2 - 1 \in \mathbb{C}(\omega)[x].$$

$\Rightarrow y$ tem grau 4 sobre $\mathbb{C}(\omega)$.

$$[K : \mathbb{C}(\omega)] = 4 \quad \mathbb{C}(\omega) \subset F \subset K.$$

$$|G| = 4 \Rightarrow [K : F] = 4 \Rightarrow F = \mathbb{C}(\omega)$$

□.

Thm (Lüroth).

Todo subcorpo $F \subset \mathbb{C}(y)$

$\mathbb{C} \not\subset F$ é o corpo de funções

racionais em uma variável w

$$w = w(y) \in \mathbb{C}(y).$$

Teorema principal de Galois.

$f(x)$ polinômio mônico $\deg f = n$

$$F[x]. \quad K \supset F \quad K = F(\alpha_1, \dots, \alpha_n)$$

α_i são as raízes de f .

Quaisquer outros corpos de decomposição de f são isomorfos.

$$F \subset F(\alpha) \subset K$$

\hookrightarrow este é determinado de

feito unico pelo polinomio irred.
de α .

Toda isomorfismo: $\varphi: F \rightarrow \tilde{F}$
extende para um isomorfismo.

$$F[x] \cong \tilde{F}[x]$$

$$\begin{array}{c} \varphi \\ \downarrow \\ F[x] \longrightarrow \tilde{F}[x] \end{array}$$

\tilde{f} é irredutível $\Leftrightarrow f$ irred.

Lemma: Seja $f \in F[x]$ irredutível.

$$f(\alpha) = 0 \quad \alpha \in K \quad \tilde{f}(\tilde{\alpha}) = 0$$

$\tilde{\alpha} \in \tilde{K} \Rightarrow \exists!$ isomorfismo.

$$\varphi: F(\alpha) \rightarrow \tilde{F}(\tilde{\alpha})$$

$$\varphi|_F = \varphi \quad \varphi(\alpha) = \tilde{\alpha}$$

$$\begin{array}{ccc} \mathbb{R} & F[x] & \cong & F(\alpha) \\ & \downarrow & & \downarrow \\ & (f) & & \\ \mathbb{R} & \tilde{F}[x] & \cong & \tilde{F}(\tilde{\alpha}) \\ & \downarrow & & \downarrow \\ & (\tilde{f}) & & \end{array}$$

Proposição: seja $\varphi: F \xrightarrow{\cong} \tilde{F}$ isom.
 $f \in F[x]$ Polinômio. $\tilde{f} \in \tilde{F}[x]$

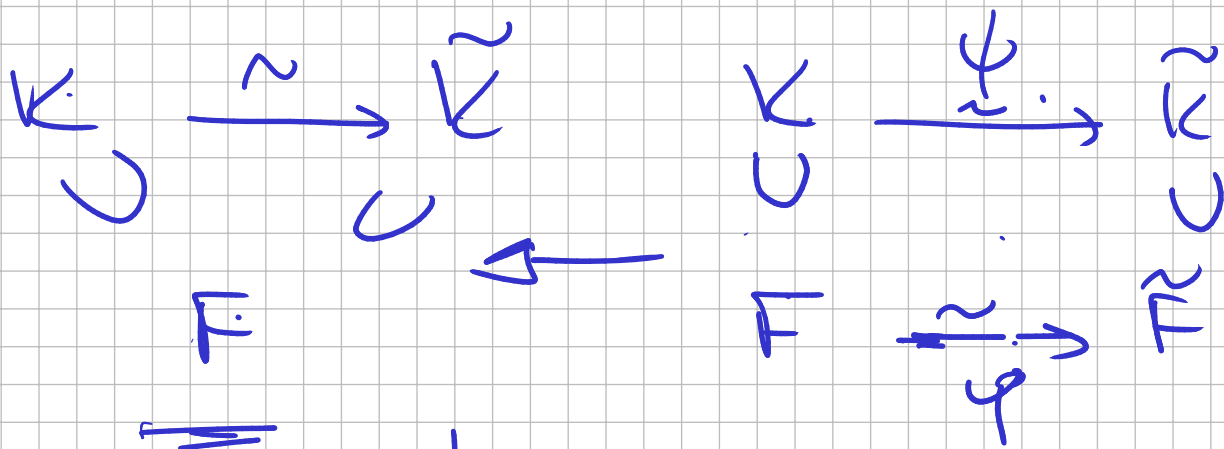
Sejam K e \tilde{K} os corpos de decomposição de f e $\tilde{f} \Rightarrow$

\exists isomorfismo. $\varphi: K \xrightarrow{\sim} \tilde{K}$

$$\varphi|_F: F \xrightarrow{\sim} \tilde{F} = \varphi$$

$$F = \tilde{F} \quad \varphi = \text{id}_F.$$

Corolário. Todos os corpos de decomposição de $f \in F[x]$ são isomorfos.



Prova da existência de φ :

$f = f(x)$ se letora como produto de lineares. (char $F = 0$).

\tilde{f} se letora como produto de lineares.

se obu neste situação \Rightarrow

$$K = F \quad \tilde{K} = \tilde{F} = F \quad \varphi = \varphi$$

Suponha que a fatoração ocorre

em $K \not\equiv F$.
 Seja $g \in F[x]$ um fator irredutível
 de f . $\deg. g > 1$.

$g \in \tilde{F}$ é um fator irred.

$f(\alpha) = 0$ em K . extensões. φ .

para um iso. $F(\alpha) \xrightarrow{\sim \varphi} \tilde{F}(\tilde{\alpha})$

$$\tilde{\alpha} = \varphi(\alpha).$$

$$F \subset \tilde{F} \xrightarrow{\sim \varphi} \tilde{F} \subset \tilde{F}$$

K é o corpo de decomposição
 de f , e temos o corpo de decomp.

de $f \in F(\alpha)[x]$.

$$\begin{array}{ccc} K & \xrightarrow{\sim} & \tilde{K} \\ \uparrow \cup & & \uparrow \cup \\ F(\alpha) & \xrightarrow{\sim} & \tilde{F}(\tilde{\alpha}) \\ \uparrow \cup & & \uparrow \cup \\ F & \xrightarrow{\sim} & \tilde{F} \end{array} \quad \left. \begin{array}{l} \text{indução} \\ \text{no grau.} \end{array} \right\}$$

□

Teorema. Seja $K > F$ o corpo de
 decomposição de $f \in F[x]$. \Rightarrow

$K \supset F$ e Galois

Lema. O número de isomorfismos

$$\varphi: K \rightarrow \bar{K}$$

$$\varphi: F \rightarrow \bar{F}$$

é igual ao $[K:F]$.

Pr. do Teorema: $F = \bar{F}$ $\varphi = \text{id}$.

$$|\text{Gal}(K/F)| = [K:F]$$

$\Rightarrow K$ é Galois.

Pr. do lema. $g \mid h$ fator irred.
de h . $g(\alpha) = 0$ em K .

$$\begin{array}{ccc} F_1 = F(\alpha) & \xrightarrow{\quad} & \bar{K} \\ \uparrow \subset & & \uparrow \subset \\ F_1 = F(\alpha) & \xrightarrow{\quad} & \bar{F}_1(\alpha) = \bar{F}_1 \\ \uparrow \subset & & \uparrow \subset \\ \bar{F} & \xrightarrow{\varphi} & \bar{F} \end{array}$$

Conversamente para estender φ
podemos começar com uma raíz
arbitraria α de g . $\alpha \in \bar{K}$.

$$\begin{array}{ccc}
 F_1 = F(\alpha) & \xrightarrow{f_1} & \tilde{F}_1 = \tilde{F}(\tilde{\alpha}) \\
 \cup & & \cup \\
 F & \xrightarrow{f} & \tilde{F}
 \end{array}$$

Usamos indução no grau de extensão $[K:F] > [K:F_1]$

Por indução. posso afirmar que temos exatamente

$[K:F_1]$ isomorfismos.

$$\begin{array}{ccc}
 K & \xrightarrow{\quad} & \tilde{K} \\
 \cup & \curvearrowright & \cup \\
 F_1 & \xrightarrow{\quad} & \tilde{F}_1 \quad \tilde{\alpha} \in \tilde{K}
 \end{array}$$

g pode ter diferentes raízes $\tilde{\alpha}$ mas o número de escolhas é $\deg g = [\tilde{F}_1 : \tilde{F}] = [F : F] = \deg g$.

$$[K:F_1][F_1:F] = [K:F] \quad \square$$

Como caracterizar o Grupo de Galois de $K \supset F$ $K =$ corpo de decomposição de f só depende de f e não de K .

Corolário. $K \supset F$ é uma extensão finita. são equivalentes.

- 1) $K \supset F$ é Galois.
- 2) K é um corpo de decomp.
- 3) K " " " " de um irred.
- 4) F é o corpo fixo pela ação do grupo de Galois (K/F)
- 5) F é o corpo fixo pela ação de um corpo finito $\subset \text{Aut}(K)$.

Teorema principal de Galois:
 Seja $K \supset F$ uma extensão de Galois.

$$\begin{array}{ccc}
 H \subset G = \text{Gal}(K/F) & & \text{Gal}(K/L) \subset G \\
 \downarrow & & \uparrow \\
 K^H \subset K & & F \subset L \subset K \\
 & & \rightarrow
 \end{array}$$

$\text{Gal}(K/\mathbb{Q})$ fixa L . $L \subset K \subset \overline{\text{Gal}(K/\mathbb{Q})}$.

Mas o K é uma extensão de Galois de L . $[K:L] = |\text{Gal}(K/L)|$

$$[K:L] = |\text{Gal}(K/L)|$$

$$\Rightarrow L = K^{\text{Gal}(K/L)}$$

Começamos com um subgrupo.

$$H \subset \text{Gal}(K/\mathbb{Q})$$

$$L := K^H. \quad H \subset \text{Gal}(K/L).$$

$$|H| = [K:K^H] = [K:L] = |\text{Gal}(K/L)|$$

$$\Rightarrow H = \text{Gal}(K/L). \quad \square$$

Observação: a corresp. do teorema principal revolve a ordem:

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

$$K^H \subset K^{H'}$$

$$H' \subset H$$

Teorema $F \subset L \subset K$ L/F é Galois $\Leftrightarrow \underbrace{\text{Gal}(K/L)} \subset \text{Gal}(K/F)$ é um subgrupo normal.

Teorema. K/F Galois $F \subset L \subset K$
 $H = \text{Gal}(K/L) \subset G = \text{Gal}(K/F)$.

Seja $g \in G$

a) o subgrupo de G que corresp. a $F \subset g.L \subset K$ é o subgrupo conjugado gHg^{-1}

b) L é Galois. $\Leftrightarrow H$ é normal
 $G(L/F) \cong G/H$.

PR. $g.L = L'$ $h \in H$
 $\Rightarrow ghg^{-1} \in \text{Gal}(K/L')$
 $\text{Aut. } K/L' \xrightarrow{H'} H'$
 $H' \supset gHg^{-1}$

Agora é só contar número de elementos. Para ver que $H' = gHg^{-1}$

Suponha. $\sigma \in \text{HAC}$ é normal.

$$gHg^{-1} = H \quad \forall g \in G.$$

$$\text{Gal}(K/L) = \text{Gal}(K/gL)$$

$$L = gL \quad \forall g \in G.$$

$$G \longrightarrow \text{Gal}(L/F)$$

$$\text{Ker} = \{ g \in G \mid g|_L = \text{id}_L \}$$

$$= \text{Gal}(K/L).$$

$$\Rightarrow G/\text{Gal}(K/L) \subset \text{Gal}(L/F)$$

$$[L:F] = |G/\text{Gal}(K/L)| \leq |\text{Gal}(L/F)|$$

$$\Rightarrow L \text{ é Galois: } \Leftrightarrow$$

$$G/\text{Gal}(K/L) \cong \text{Gal}(L/F).$$

Converse se L é Galois,

$\Rightarrow L$ é um corpo de decomposição de $K \in F[X]$.

$$L = F(\alpha_1, \dots, \alpha_n).$$

$\alpha_1, \dots, \alpha_n$ são raízes de f .

Todos automorfismos de K permutam as raízes de f .

\Leftrightarrow

Todos automorfismos de K levam L em L .

$$G \rightarrow \text{Gal}(L/F).$$

$$\text{Gal}(K/L) = g \text{Gal}(K/L) g^{-1}$$

$$\forall g \in G \Rightarrow \text{Gal}(K/L) \triangleleft G$$

e' normal □.