O grupo Symmétrico.

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

$$\begin{array}{ccc} G \times V & \xrightarrow{m} & V \\ a, v & \longmapsto & \rho(a)(v) =: a \cdot v \end{array}$$

$$\begin{array}{ccc} G \times G \times V & \xrightarrow{id \times m} & G \times V \\ \cdot \times id \downarrow & \circlearrowright & \downarrow m \\ G \times V & \xrightarrow[m]{} & V \end{array} \qquad \begin{array}{c} a(b \cdot v) \\ \| \\ (a \cdot b) \cdot v \end{array}$$

$$GL(V) = Aut_k(V) \subset End_k(V)$$

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

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

$\downarrow \tau$

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

$$\rho(\tau)\, e_i := e_{\tau(i)}$$

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

G grupo. V, k-Vect c/ duas representações

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

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

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

$\rho_V : G \to GL(V)$ $\quad$ $\rho_W : G \to GL(W)$

$\downarrow \quad GL_{\dim V}(k)$

$\rho_{V \oplus W} : G \to GL(V \oplus W)$

$$\rho_{V \oplus W}(a) = \begin{bmatrix} \boxed{\rho_V(a)} & 0 \\ 0 & \boxed{\rho_W(a)} \end{bmatrix}$$

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

$\varphi \in \mathrm{Hom}_{k}(V, W)$ Tq. $\forall a \in G$

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

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

$\varphi \in \mathrm{Hom}_G(V, W) = \{ \varphi \in \mathrm{Hom}_k(V, W)$ tq φ é morfismo de G-mod $\}$

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

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

$a \cdot u \in V$. $\quad \varphi(au) = \varphi(0) = 0$

$\downarrow$ ação em V $\quad au \in U \subset V$

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

$"k = \varphi(v)$

$a \cdot k = a\,\varphi(v) = \varphi(\underline{a}\, v) \in K$

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

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

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

⚠ categoria de grupos não tem quocientes

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

$\downarrow$

A categoria de G-modules tem

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

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

$0 \longrightarrow \ker\varphi \xhookrightarrow{i} V \twoheadrightarrow \mathrm{coker}\,\varphi \to 0$

sequência exata curta.

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

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

$(a \cdot b)(v \otimes w) = (a \cdot b) \cdot v \otimes (a \cdot b) \cdot w$

$= (a(bv)) \otimes (a \cdot (b \cdot w))$

$= a \cdot (b \cdot v \otimes bw)$

$= a \cdot (b \cdot (v \otimes w))$

$V \in G\text{-mod}$ então $V^{\otimes n} := \underbrace{V \otimes V \otimes \cdots \otimes V}_{n\text{-vezes}}$

$\forall\, n$.

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

$a \cdot \alpha = \alpha$ $\qquad \rho : G \longrightarrow GL(V)$, $a \longmapsto id_V$.

$G = GL(V)$ $\qquad V \in G\text{-mod}$

$id = \rho : G \longrightarrow GL(V)$

$GL(V)$ actúa en $V^{\otimes n}$ $\forall n$.

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

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

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

$v_1 \otimes \dots \otimes v_n$ $\qquad v_i \in V$

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

τ

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

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

H, G dois grupos que agem em V. Os 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 $GL(V)$ e de S_n (σ) comutam.

$$\sigma(a \cdot v_1 \otimes \dots \otimes v_n) = (av)_{\sigma(1)} \otimes \dots \otimes (av)_{\sigma(n)}$$

$$a(v_{\sigma(1)} \otimes \dots \otimes v_{\sigma(n)}) \rightleftarrows$$

$V \in G\text{-mod}$. $\begin{cases} V^G \\ V_G \end{cases}$ $k\text{-Vect}$.

$$V^G = \{ v \in V \ \text{tq}\ av = v\ \forall a \in G \}$$

$$V_G = V/\sim \qquad v \sim w \iff \exists a \in G \ \text{tq}\ v = a \cdot w$$

$\sim$ é uma relação de equivalência:

$v \sim v$ $\quad a = id_G$.

$v \sim w \Rightarrow w \sim v$ $\quad v = a \cdot w \Rightarrow w = a^{-1} v$

$v \sim w \quad w \sim z \Rightarrow v \sim z \quad v = aw \quad w = bz$

$v = a(bz) = (a \cdot b) \cdot z$

1_G

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

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

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

φ, ψ $\quad \alpha, \beta \in k$.

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

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

$= \alpha\varphi(av) + \beta\psi(av)$.

2) $\mathrm{Hom}_k(k, V) \simeq V$ como conjunto.

3). $\mathrm{Hom}_G(\mathbb{1}, V) \ni \varphi$

$\varphi(1) \in V^G$. $\quad \varphi(a1) = a\varphi(1)$

$\varphi(1)$ $=$

$V_G = ?$ $\quad V /\!\!/ N \quad$ $N \trianglelefteq G$

$\mathrm{Hom}_G(V, \mathbb{1}) \ni \varphi$

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

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

$\mathrm{Hom}_k(V /\!\!/ N, k)$

$N \trianglelefteq G$

$\mathrm{Hom}_G(V, \mathbb{1}) = \mathrm{Hom}_k(V_G, k)$

$\| \qquad\qquad\qquad\quad \| \; V_G^*$

$V_G = \mathrm{Hom}_G(V, \mathbb{1})^*$

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

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

$GL(V)$

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

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

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

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

$\Downarrow$

$gv \in V^H \subset V$

$\Downarrow$

sub G-mod.

$V \twoheadrightarrow V_H = V/\!/_H$

$v \curvearrowright [v]$

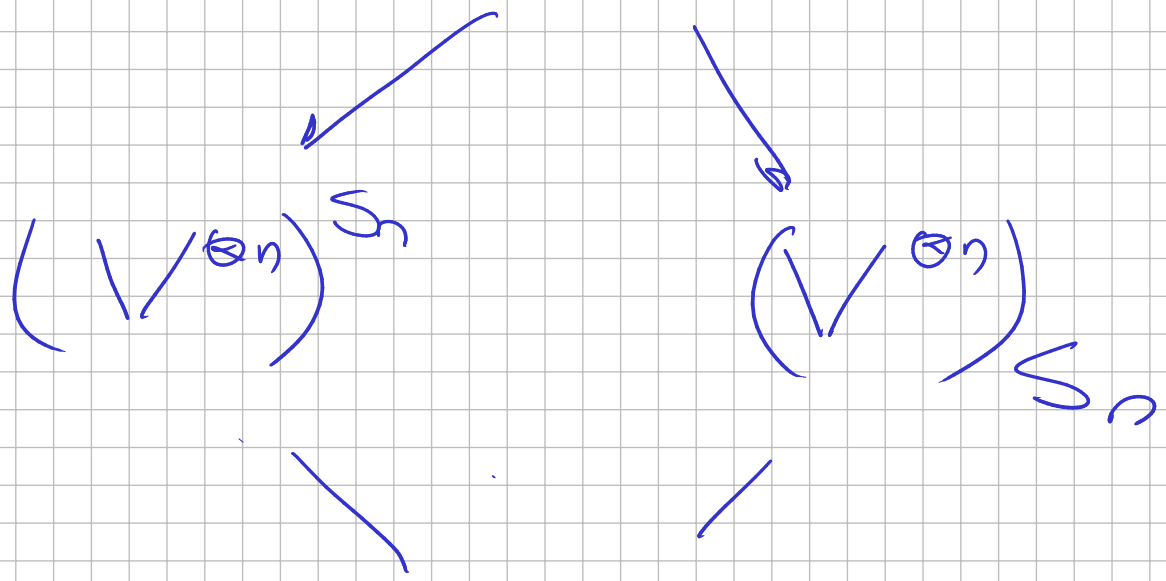
$0 \to U \to V \to V_H \to 0$

$v + U = [v]$. $g(v+U) = gv + U$

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

$V \twoheadrightarrow V_H \quad \in \mathrm{Hom}_G(V, V_H)$

$V \in k\text{-Vect} \qquad V^{\otimes n} \circlearrowright S_n$



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

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

$H = \{ a \in GL(V) \mid g \cdot av = a \cdot gv \}$

$\mathrm{Hom}_G(V,V) \overset{\text{invert.}}{\simeq} \mathrm{Aut}_G(V)$

H agit en V. $\quad$ e commute avec G.

Theorem (Schur–Weyl) duality

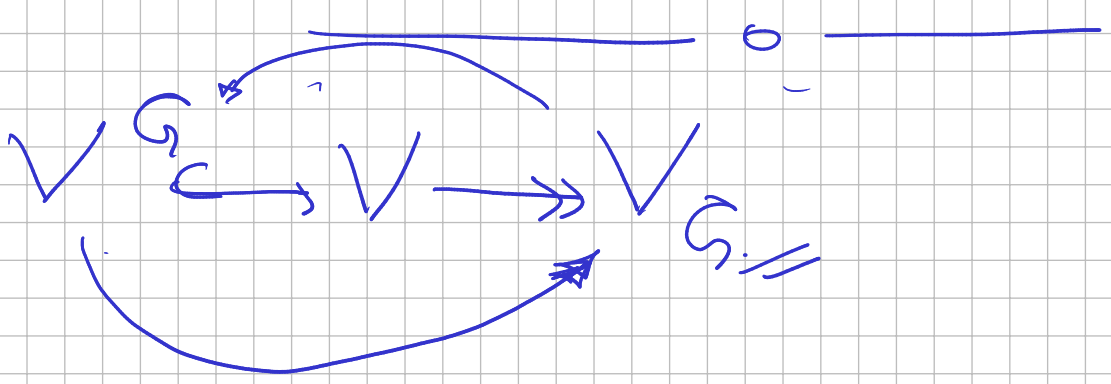
$$\mathrm{Aut}_{GL(V)\text{-mod}}\left(V^{\otimes n}\right) \simeq S_n$$

$$\updownarrow$$

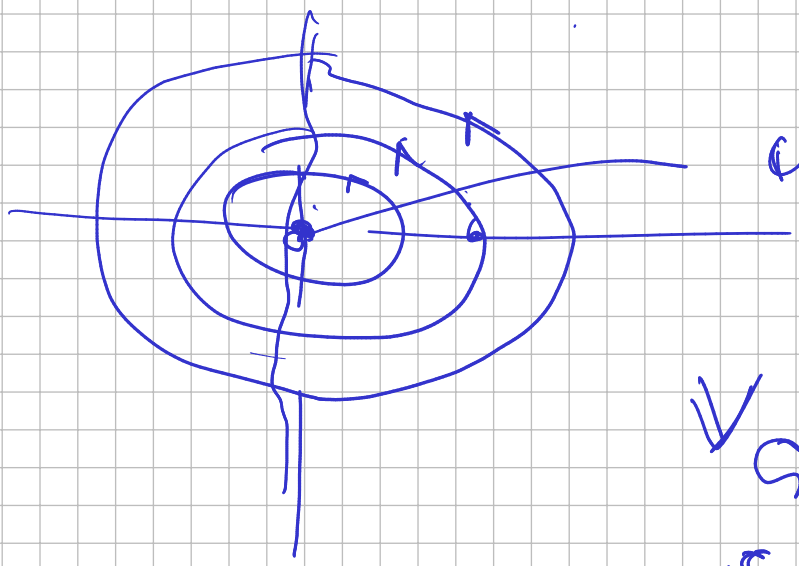
$$\mathrm{Aut}_{S_n}\left(V^{\otimes n}\right) = GL(V)$$

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

$$\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n\text{-times}} \curvearrowleft GL(2)$$



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



um ponto fixo.

$V_G \simeq \mathbb{R}_{\geq 0}$

$V^G = * \ 0$

Seja $[v] \in V_G$. G finito

$v \in V$ uma preimagem de v.

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

$\boxed{w \sim v}$

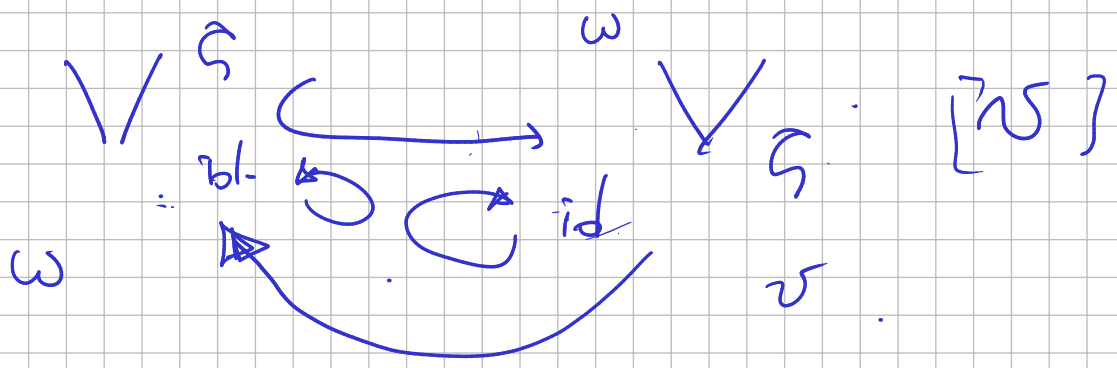
$a = id_G \cdot v + \sum$

$|G|$-elementos todos equivalentes a v.

$w \in V^G$.

$b \cdot w = \frac{1}{|G|} \sum b \cdot g v$

$= \frac{1}{|G|} \sum_{g \in G} g v = w.$



$\omega \in V^G \longrightarrow \overline{\{\omega\}} \in V_G$

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

$V^G \xrightarrow{\sim} V_G$ são espaços isomorfos.

$U \to V \twoheadrightarrow V_G \to 0$

$\boxed{v+U}$ $\quad \frac{1}{|G|}\sum g\cdot v$

$[v] \longrightarrow \omega = \frac{1}{|G|}\sum g\cdot v$

$v+u \quad u\in U$

$\omega' = \frac{1}{|G|}\sum g\cdot v + g\cdot u$

$= \omega + \left(\frac{1}{|G|}\sum g\cdot u\right) = 0$?

O que é $U \subset V$?

$$v - \sigma v \in U$$

$$V^G \hookrightarrow V \twoheadrightarrow V_G$$

π é injetiva?

$v \in V^G \quad \sigma \cdot v = v \quad \forall \sigma \in G.$

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

$\pi(0) = 0$ $\quad \sigma \cdot v = 0$

$$V^G \rightleftarrows V_G$$

$$\omega \longmapsto [\omega]$$

$$\frac{1}{|G|} \sum \sigma \cdot v \longleftarrow [v]$$

$\operatorname{char} k = 0$ ou se $|G|$ é invertível ($\neq 0$). então $V^G \cong V_G$.

Existen grupos abelianos.

$H^*(G, V)$ $\qquad$ $H_*(G, V)$

$$H^0(G, V) = V^G$$

$$H_0(G, V) = V_G$$

en char 0 son isomorfos.

char p son diferentes.

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

(2 char 0 $\Rightarrow$ $\mathbb{1}$ es proyectivo)

$$V_G = \mathrm{Hom}_G(V, \mathbb{1})^* \simeq (V^*)^*$$

$$\mathrm{Hom}(V, k) \simeq V^* \otimes k$$

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

$$\mathrm{Hom}(k, V) \simeq V \otimes k^*$$

$$\mathrm{Hom}(V, k) \xrightarrow{\sim} V^* \otimes k$$

$$\downarrow 2^* \qquad\qquad \downarrow$$

$$\mathrm{Hom}(k^*, V^*) \xrightarrow{\sim} k \otimes V^*$$

$$\| \qquad\qquad \mathrm{Sym}^n V \subset V^{\otimes n}$$

$$\| \qquad\qquad \| \qquad\qquad \nearrow$$

$$\Lambda^\bullet T^* \qquad (V^{\otimes n})^{S_n}$$

$$V^{\otimes n} \twoheadrightarrow (V^{\otimes n})^{S_n} \qquad \text{char.} = 0.$$

$$V = k^{\oplus n} \rightsquigarrow k\langle V \rangle = \bigoplus_{k \geq 0} V^{\otimes k} \circlearrowright S_n$$

$$k\langle V \rangle^{\mathrm{Sym}} = \bigoplus_{k \geq 0} \mathrm{Sym}^k(V^*) = \bigoplus_{k \geq 0} (V^{*\otimes k})^{S_k} \circlearrowright S^k \circlearrowright S_n$$

$$k\langle V \rangle^{\mathrm{Sym}} = \text{fonctions polynomiales en } V.$$

em $k/^{Sym}$ tenho uma ação de

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

R anel $R[u_1, \dots, u_n]$

o grupo S_n age em $R[u_1, \dots, u_n]$

$\sigma \in S_n$ $\quad f \in R[u_1, \dots, u_n]$.

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

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

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

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

$$= ((\tau \cdot \sigma) \cdot f)(u_1, \dots, u_n)$$

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

Def. um polinómio $f \in R[u_1, \dots, u_n]$ é simétrico se é invariante por S_n.

$$\mathbb{R}[x_1,\dots,x_n] = \bigoplus \text{Espaços dim. finita}$$

$$\bigoplus_{k\geq 0} \text{polynomios homog. de grau } k$$

$$\bigoplus \operatorname{Sym}^k(\mathbb{R}^n)$$

Seja $f \in \mathbb{R}[x_1,\dots,x_n]$.

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

Exemplo. $f = x_1 x_2^2 \in \mathbb{R}[x_1,x_2,x_3]$

$$x_1x_2^2 + x_2x_3^2 + x_3x_1^2$$
$$x_2x_1^2 + x_3x_2^2 + x_1x_3^2$$

é simétrico.

$$(X-x_1)(X-x_2)\cdots(X-x_n) \in \underbrace{\mathbb{R}[x_1,\dots,x_n]^{Sym}[X]}$$

os coeficientes de X^k são simétricos

$$X^n - \underbrace{\left(\sum x_i\right)}_{S_1} X^{n-1} + \underbrace{\sum_{1\leq i<j\leq n} x_ix_j}_{S_2} \cdot X^{n-2}$$

$$+ \dots + (-1)^n \underbrace{\prod u_i}_{s_n} \cdot X^0$$

$$\sum_{k=0}^{n} (-1)^k X^{n-k} \cdot s_k$$

$$s_k \in R[u_1, \dots, u_n]^{S_n}$$

$$\deg s_k = k.$$

$$s_0 = 1 \qquad s_1 = \sum u_i \qquad s_2 = \sum_{1 \le i < j \le n} u_i u_j$$

$$s_n = \prod_{i=1}^{n} u_i$$

Teorema Todo polynomio simétrico em n-variaveis se escreve de forma unica como polynomio nos s_i, $i = 0, \dots, n$.

$$R[z_1, \dots, z_n] \longrightarrow R[u_1, \dots, u_n]$$

$$z_i \longmapsto s_i$$

1). Todo polynomio simétrico está na imagem

2). O núcleo do morfismo é nulo.

Corolário: Não existem relações polinomiais entre os s_i

$\Leftrightarrow$ o subanel de polinomios simétricos em n-variáveis é isomorfo ao anel de polinomios em n-variáveis.

$$(X-u_1)\cdots(X-u_n).$$

$$\Delta(u_1,\dots,u_n)=\prod_{1\le i<j\le n}(u_i-u_j)^2$$

$$\Delta \in \mathbb{R}[u_1,\dots,u_n]^{S_n}$$

Pelo teorema Δ se escreve de forma única como combinação dos s_i!

$n=0 \quad \Delta = 1$

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

$n=2 \rightarrow \quad \Delta = (u_1-u_2)^2$

$=$

$s_0=1 \qquad s_1 = u_1+u_2 \qquad s_2 = u_1\cdot u_2$

$$(u_1-u_2)^2 = u_1^2+u_2^2-2u_1u_2$$

$$s_1^2 = u_1^2+u_2^2+2u_1u_2.$$

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

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

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

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

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

$n=3$ $\quad \Delta = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2$

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

$$S_3^2 \quad S_3 S_2 S_1 \quad S_3 S_1^3$$
$$S_2^3 \quad S_2^2 S_1^2 \quad S_2 S_1^4$$
$$S_1^6$$

α

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

$$\Delta = -27 S_3^2 + 18 \cdot S_3 S_2 S_1 - 4 S_3 S_1^3 - 4 S_2^3 + S_2^2 S_1^2 + 0 \cdot S_2 S_1^4 + 0 S_1^6$$

$X^2(X-1) \rightarrow D = 0$

$X^3 - X^2 \Rightarrow S_1 = 1 \quad S_2 = S_3 = 0.$

$= \text{Coef}(S_1^6) = 0$

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

$S_1 = S_3 = 0 \quad S_2 = -1$

$\text{Coef}(S_2^3) = -4$

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

$S_1 S_2 = 0 \quad S_3 = 1 \qquad \left(X - \frac{-1-\sqrt{-3}}{2}\right)$

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

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

$\text{Coef}(S_3^2) = +27$

$X^3 - 2X^2 + 1 \qquad S_2 = 0 \quad S_1 = 2 \quad S_3 = -1$

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

$\left(X - \frac{1-\sqrt{5}}{2}\right)$

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

$$= \left(\frac{-4}{4}\right)^2 \cdot 5 = 5 = D.$$

$$(-27)\,4 - \alpha\, 8 = 5$$

$$\alpha = -\frac{5 - 27}{8} = -4$$

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

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

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

$$S_3 = 0$$

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

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

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

} Achar o erro.

$$X(X+1)(X-3) \ldots \longrightarrow$$

$D \neq 0$. As raízes são distintas 2 e -2. No corpo de decomposi

cão. $\Rightarrow$ Galois $= S_n$?

Prova do teorema.

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

$$f \in R[u_1, \ldots, u_n]^{S_n}$$

$$\overline{f} = f(u_1, \ldots, u_{n-1}, 0)$$

$$\in R[u_1, \ldots, u_{n-1}]^{S_{n-1}}$$

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

tq $\overline{f} = \psi\left[S_1^{(n-1)}, \ldots, S_{n-1}^{(n-1)}\right]$

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

g é simétrico em n-variáveis.

$$g(u_1, \ldots, u_{n-1}, 0) = \overline{f} - \psi\left(S_1^{(n)}(u_1, \ldots, u_{n-1}, 0), \ldots, S_{n-1}^{(n)}(u_1, \ldots, u_{n-1}, 0)\right)$$

observação. $S_i^{(n)}(u_1, \ldots, u_{n-1}, 0) = S_i^{(n-1)}$

$\Rightarrow g(u_1, \ldots, u_{n-1}, 0) = 0$

$u_n \mid g$. como g é simétrico

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

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

u

$S_n^{(n)}$

$f - \psi(S_1^{(n)}, \ldots, S_{n-1}^{(n)}) = S_n^{(n)} \cdot h$

$\deg h < \deg f$.

h é simétrico em n-variáveis.

Por indução. $\exists! \varphi \in R[Z_1, \ldots, Z_n]$

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

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

□.

$$R[z_1, \ldots, z_n] \hookrightarrow R[u_1, \ldots, u_s]$$

$$\downarrow$$

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

π: $\mathbb{A}^n \ni x$ ideal maximal $(u_1 - x_1, \ldots, u_n - x_n)$

$R = \mathbb{C}$.

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

$\mathbb{A}^n$ $\qquad$ $\pi(x)$ = polin simétricos que são 0 em x.

$\pi(y) = \pi(x)$ $\qquad \exists\, \sigma \in S_n$ t.q. $\sigma(x) = y$. !

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

Elementos primitivos.

Teorema: Seja $F \subset K$ uma extensão finita com $\mathrm{char}\, F = 0 \Rightarrow \exists\, \gamma \in K$ s.t. $F(\gamma) = K$.

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

Pf. $F \subset K$ é finito. $K = F(\alpha_1, \dots, \alpha_n)$ finitos elementos. Retemos indução em n.

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

Assumindo o teorema para n.

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

$\cup$, indução.

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

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

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.

Char 0 $\quad \exists K'$ Tq. f, g se fatoram como produto de lineares com fatores diferentes.

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

$f(x) \qquad\qquad g(x)$

$\alpha_i \neq \alpha_j \quad i \neq j \qquad \beta_i \neq \beta_j \quad i \neq j.$

$\gamma = \beta + c\alpha \qquad c \in F$

$K \quad n \quad K$

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

Basta provar $\alpha \in F(\gamma)$ ⟵

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

f é o polynómio irred. de α

g " " β } $F[x]$

$h(x) = g(\gamma - cx) \in F(\gamma)[x]$

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

Quais são os factores comuns entre h e f em $F(\gamma)[x] \subset K'[x]$

Tem uma raiz comum α.

gcd em $K'[x]$.

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

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

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

$\Rightarrow \gcd(h, f) = (X-\alpha)$

$K'[x]$ ou $F(\gamma)[x]$

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

$\beta_1, \ldots, \beta_m$ são os raízes de g.

$h(x) = g(\underbrace{\gamma - cx}_{\beta_i})$.

$\gamma - cx = \beta_i$ para algum i.

$x = \dfrac{\gamma - \beta_i}{c}$ $\qquad \gamma = \beta + c\alpha$

$x = \dfrac{\beta - \beta_i}{c} + \alpha$ para $i = 1, \ldots, m$

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

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

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

(*) é um conjunto finito de elementos.

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

$c \in F \qquad |F| = \infty. \qquad \text{char } F = 0.$

$\cup$

$\mathbb{Q} \subset F.$

$\exists\, c_i \in F$ tque $\alpha = \alpha_1$ é o único divisor comum de h e f. $\square$.

Exemplo: $K = \mathbb{Q}[i, \sqrt[3]{2}] \supset \mathbb{Q}$

α, β

$\deg = 6.$

x^2+1 $\qquad$ x^3-2

$\alpha, -\alpha$ $\qquad$ $\beta = \sqrt[3]{2}$ $\qquad$ $\xi\sqrt[3]{2}$ $\qquad$ $\xi^2\sqrt[3]{2}$

α_1, α_2 $\qquad$ β_1 $\qquad$ β_2 $\qquad$ β_3

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

K é gerado por combinações da forma.

$\beta + c\alpha$

$c \neq \dfrac{\beta - \beta_i}{\alpha_i - \alpha}$ $\quad j = 2$

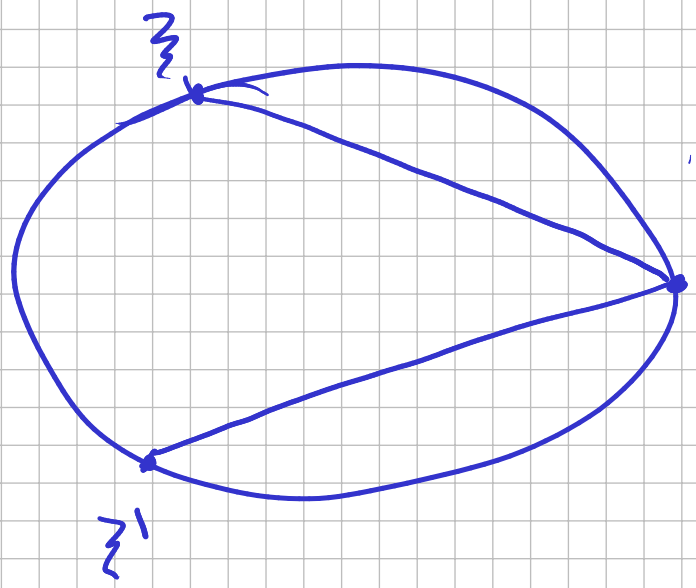
$i = 2, 3$

$i = 1, 2$

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

α

$\mathbb{Q}$.



$\forall \; c \in \mathbb{Q}. \quad (\sqrt[3]{2} + c \cdot i)$ gera

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

irred. desse γ tem grau 6.

Prop. Seja $G \subset \mathrm{Aut}\, K$. seja $F = K^G$. seja $\beta \in K$.

$\beta = \beta_1, \beta_2, \ldots, \beta_n$ órbita de β

Pela ação de G $\Rightarrow$

1) β é algébrico / F

2) $\deg \beta = n$

3) irred de $\beta = (X-\beta_1) \cdots (X-\beta_n)$.

Seja $f \in F[x]$ o polynômio mônico irred. de β.

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

$\Rightarrow$ Todo β_i é uma raiz de f

$g = (X-\beta_1) \cdots (X-\beta_n) \mid f$.

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

$\Rightarrow$ $g = f$. □

Ex $\mathbb{Q} \subset K = \mathbb{Q}(i, \sqrt{2})$

grau 4. $Gal(K/\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2$

$i \longmapsto -i$ $\quad \sqrt{2} \longmapsto -\sqrt{2}$

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

$\beta_2 = -i + \sqrt{2}$ $\quad \beta_3 = i - \sqrt{2}$ $\quad \beta_4 = -i - \sqrt{2}$

irred. de p. tem grau 4

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

$$\{ \text{grau } 4.$$

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

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

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

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

é irred. sobre $\mathbb{Q}$, grau 4.

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

Não é surpreendente que polynómio é de forma $g(h(x))$ com $\deg g = \deg h = 2$

□

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

$F = K^{Gal(K/F)}$ $\alpha = \alpha_1$ raiz de f.

$\forall\ g \in G = Gal.$ $g(\alpha)$ é raiz de f.

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

$g(x) = (x-\alpha_1)\ldots(x-\alpha_n)$. □

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

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

$f_1, \ldots, f_n \in F[x]$ irred para α_1, α_n

$f = \prod f_i$ K é corpo de decomposição de f.

Teorema: $G \subset Aut(K)$ $|G| = n$

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

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

$\Rightarrow \beta$ é algébrico / F

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

$\Rightarrow m \mid n$.

$\exists\ \beta \in K$ primitivo. $[K:F] = \deg \beta = m \mid n$

$[K:F] \geq n$. ———

Seja $\beta \in K$ primitivo.

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

é orbita. $m \leq n$

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

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

$g \cdot G_\beta \longrightarrow g \cdot \beta$

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

m

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

$id \neq g \in G_\beta$ $g(\beta) = \beta$.

g fixa $F(\beta) = K$.

$\Rightarrow g = id$. absurdo

$|\mathcal{O}_\beta| = n$. □

———

K/F finita. $\Rightarrow |Gal(K/F)|$ divide $[K:F]$

$K \supset K^{Gal} \supset F$

deg.

$F \subset K$ extensão finita $|Gal(K/F)| \mid [K:F]$

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

e temos $F \subset K^G \subset K$

$[K:K^G] \mid [K:F]$. □

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

Usei isso no teorema da última aula.

Controlar que não tem raciocínio circular.

Corollario. - G grupo finito automor. de K seja $F = K^G$. $\Rightarrow$

$K \supset F$ é Galois e

$G = Gal(K/F)$.

Pf. $\forall g \in G$. seja F-automorfismos de K. $\Rightarrow$ $G \subset Gal(K/F)$

$|Gal(K/F)| \leq [K:F]$

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

$\Rightarrow$ $K \supset F$ é Galois $\quad G(K/F) = G$.

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

$\mathbb{Z}_2 \times \mathbb{Z}_2$ age por $\quad y \to -y$

$y \to i y^{-1}$

$K^G = F$

Lemma. $F \simeq \mathbb{C}(\omega) \quad \omega = y^2 - y^{-2}$

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

$$Y \longleftarrow X$$

Pf. G fixe $\omega = y^2 - y^{-2}$

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

$\omega \in F = K^G$ Seja $p \in F[x]$

o Polynômio irredutível de y

$y \to -y \to i y^{-1} \to -i y^{-1}$

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

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

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

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

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

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

$\square$.

Thm (Lüroth).

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

$\mathbb{C} \subsetneq F$ é o corpo de funções racionais em uma variável w

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

Teorema principal de Galois.

$f(x)$ polynômio mônico $\deg f = n$

$\uparrow$

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

α_i são as raízes de f.

Quaisquer dois corpos de decomp. de f. são isomorfos.

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

$\hookrightarrow$ α é determinado de

feito único pelo polynomio irred. de α.

Todo isomorfismo. $\varphi: F \longrightarrow \tilde{F}$ extende para um isomorfismo.

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

$f(x) \longrightarrow \tilde{f}(x)$

$\tilde{f}$ é irredutível $\Leftrightarrow$ f irredu

Lemma: Seja $f \in F[x]$ irredutível.

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

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

$\psi : F(\alpha) \longrightarrow \tilde{F}(\tilde{\alpha})$

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

Pf. $F[x]/(f) \simeq F(\alpha)$

$\tilde{F}[x]/(\tilde{f}) \simeq \tilde{F}(\tilde{\alpha})$

Proposição: Seja $\varphi: F \simeq \tilde{F}$ iso. $f \in F[x]$ polinômio. $\tilde{f} \in \tilde{F}[x]$

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

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

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

$F = \tilde{F}$ $\quad \varphi = id_F$.

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

$$\begin{array}{ccc} K & \xrightarrow{\sim} & \tilde{K} \\ \cup & & \cup \\ F & = & \tilde{F} \end{array} \qquad \begin{array}{ccc} K & \xrightarrow{\psi}_{\sim} & \tilde{K} \\ \cup & & \cup \\ F & \xrightarrow[\varphi]{\sim} & \tilde{F} \end{array}$$

Prova da existência de ψ:

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

$\tilde{f}$ se fatora como produto de lineares

se obv nesta situação $\Rightarrow$

$K = F \qquad \tilde{K} = \tilde{F} = F \qquad \varphi = \psi$

Suponha que a fatoração ocorre em $K \neq F$.

Seja $g \mid f$ um fator irredutível de f. $\deg g > 1$.

$\tilde{g} \mid \tilde{f}$ $\tilde{g}$ é um fator irred. de $\tilde{f}$.

$f(\alpha) = 0$ em K. estendemos φ para um iso. $\tilde{\varphi}$. $\tilde{\alpha} = \varphi(\alpha)$.

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\tilde{\varphi}} & \tilde{F}(\tilde{\alpha}) \\ \cup & & \cup \\ F & \xrightarrow{\varphi} & \tilde{F} \end{array}$$

K é o corpo de decomposição de f, e tomem o corpo de decom. de $\tilde{f} \in F(\alpha)[x]$.

$$\begin{array}{ccc} K & \xrightarrow{\sim} & \tilde{K} \\ \cup & & \cup \\ F(\alpha) & \xrightarrow{\sim} & \tilde{F}(\tilde{\alpha}) \\ \cup & & \cup \\ F & \xrightarrow{\sim} & \tilde{F} \end{array}$$

— indução em $\hat{f}$ no grau.

□

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

$K \supset F$ é Galois

Lemma. O número de isomorfismos

$$\begin{array}{ccc} \varphi : K & \to & \tilde{K} \\ \cup & & \cup \\ \varphi : F & \to & \tilde{F} \end{array}$$

é igual ao $[K:F]$.

Pf. do Teorema: $F = \tilde{F}$ $\varphi = id$.

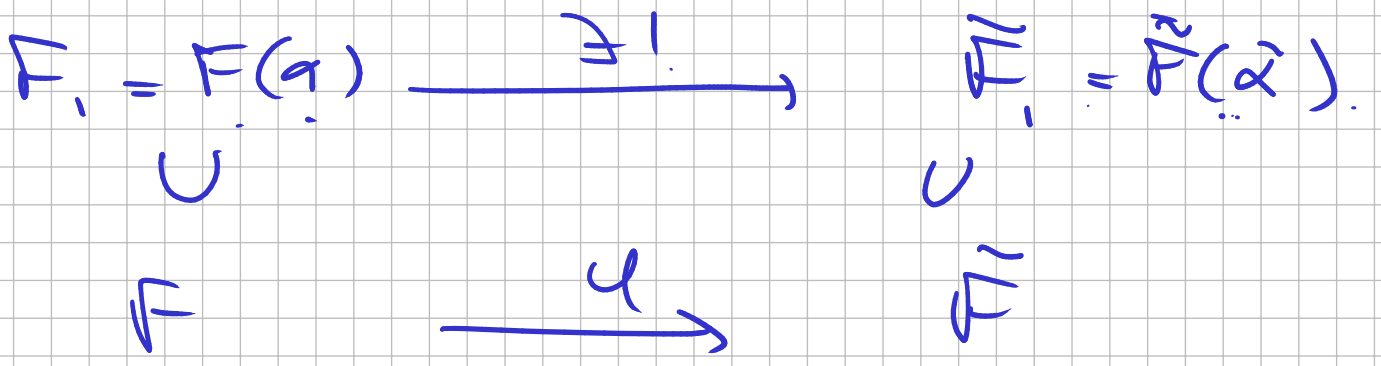
$$|\mathrm{Gal}(K/F)| = [K:F]$$

$\Rightarrow K$ é Galois.

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

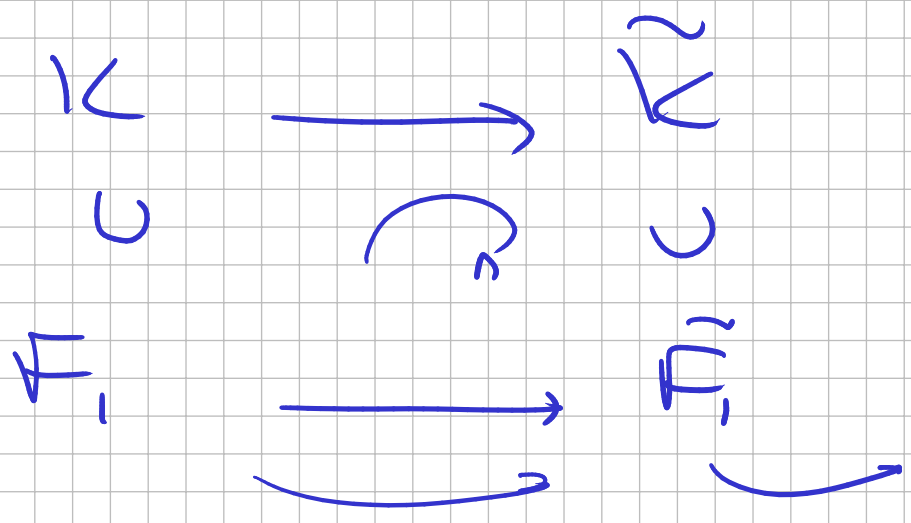
$$\begin{array}{ccc} F_1 = F(\alpha) & & \\ \cup K & \longrightarrow & \tilde{K} \\ F_1 = F(\alpha) & \to & \tilde{F}(\alpha) = \tilde{F}_1 \\ \cup & & \cup \\ F & \xrightarrow[\varphi]{} & \tilde{F} \end{array}$$

Conversamente para extender φ podemos começar com uma raiz arbitrária $\tilde{\alpha}$ de $\tilde{g}$. $\tilde{\alpha} \in \tilde{K}$.



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

Por indução posso assumir que temos exatamente $[K:F_1]$ isomorfismos.



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

$[K:F_1][F_1:F] = [K:F]$ □

Como corolário 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 $\subset Aut(K)$.

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

$H \subset G = Gal(K/F)$. $\qquad Gal(K/L) \subset G$.

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

$K^H \subset K \qquad\qquad F \subset L \subset K$

$Gal(K/L)$ fixa L $\quad L \subset K^{Gal(K/L)}$.

Mas K é uma extensão de Galois de L $\quad [K:L] = |Gal(K/L)|$

$[K : K^{Gal(K/L)}]$

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

Começamos com um subgrupo.

$H \subset Gal(K/F)$

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

$|H| = [K : K^H] = [K : L] = |Gal(K/L)|$

$\Rightarrow H = Gal(K/L)$. □

Observação: o corresp. do teorema principal reverte a ordem:

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

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

Teorema $F \subset L \subset K$ $L \supset F$ é Galois $\Leftrightarrow$ $Gal(K/L) \subset Gal(K/F)$ é um subgrupo normal.

Teorema. K/F Galois $F \subset L \subset K$

$H = Gal(K/L) \subset G = Gal(K/F)$

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 $G(L/K) \simeq G/H$.

PR. $g.L = L'$ $h \in H$

$\Rightarrow$ $ghg^{-1} \in Gal(K/L')$

H'

Aut. K/L' $\forall h \in H$

$H' \supset gHg^{-1}$

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

Suponha que $H \trianglelefteq G$ é normal.

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

$Gal(K/L) = Gal(K/gL)$

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

$G \longrightarrow Gal(L/F)$

$\ker = \{ g \in G \text{ t.q. } g|_L = Id_L \}$

$=$

$Gal(K/L).$

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

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

$\Rightarrow L$ é Galois e

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

Converse se L é Galois,

$\Rightarrow L$ é um corpo de decomposição de $f \in F[x]$

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

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

Todo automorfismo de K permute as raízes de f.

$\Downarrow$

Todo automorfismo de K leva L em L.

$$G \to Gal(L/F).$$

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

$\forall\ g \in G \Rightarrow Gal(K/L) \lhd G$

é normal $\square$.

$F \subset L \subset K$ Galois

Galois

Galois $G(K/L) \subset G(K/F)$ é normal.

Equações de grau 4.

Seja $K > F$ Galois. $\beta \in K$ $f(x)$ mónico irredutível / F. $f = \prod (x - \beta_i)$ em K

$\beta = \beta_1, \beta_2, \ldots, \beta_n$

$\beta_i \neq \beta_j$ (char $F = 0$). $G(K/F)$ age em K permutando os β_i.

$$\pi : G(K/F) \hookrightarrow S_n \qquad n = \deg f.$$

$$S_n = \mathrm{Aut}\{\beta_1, \ldots, \beta_n\}$$

G = imagem de $G(K/F) \subset S_n$ é sub-grupo transitivo.

$\pi(G)$ age transitivamente no conjunto $\beta_1, \ldots, \beta_n$

$\forall\ i, j \quad \exists\ g \in G.$ tq.

$$g(\beta_i) = \beta_j$$

K/F é o corpo de decomposição de um polynomio $f(x) \in F[x]$ então o grupo de Galois $G(K/F)$ age fielmente nas raízes de f.

π é injetivo.

Se f é irredutível. as raízes formam uma única orbita.

K/F o corpo decomposição de $f(x)$, $\alpha_1, \dots, \alpha_n$ $n = \deg f$.

1) Dado subgrupo $H \subset S_n$ será que $G(K/F) = G \subset H$?

2). Qual é $G \subset S_n$

Se eu conheço 1) $\forall H \Rightarrow$ eu conheço 2).

$(u_1 - u_2)(u_1 - u_3)(u_2 - u_3) = \delta$

é um polynomio $\in F[u_1, u_2, u_3]$ não é invariante por S_3.

$\tau_{12} \cdot \delta = -\delta$

mas é invariante por $\mathbb{Z}_3 \subset S_3$

Mais geralmente a raiz do discriminante

$$\underline{\delta} = \prod_{1 \le i < j \le n} (u_i - u_j) \in F[u_1, \dots, u_n]^{A_n}$$

Prop Seja K/F corpo decomp de um poly. n irred. $f \in F[x]$ $\deg f = n$.

$\alpha_1, \dots, \alpha_n$ raízes de f em K.

$\delta = \delta(\alpha_1, \dots, \alpha_n)$

1) $\delta \neq 0$

2) $\delta \in F \iff G \subset A_n \subset S_n$

3) Sempre $G(K/F(\delta)) \subset G = G(K/F)$

$\cap$ A_n

Pf $\delta = 0$ so $\alpha_i = \alpha_j$ com $i \neq j$

$\operatorname{char} F = 0$ ↯ absurdo. ∗

Ex: $\delta = -\delta$ $\delta \neq 0 \Rightarrow \delta$ não é invariante pela transposição T_{ij}.

□

$\sqrt{3+2\sqrt{2}}$ $\sqrt{5+\sqrt{21}}$ $\sqrt{7+2\sqrt{5}}$

$\sqrt{5+2\sqrt{5}}$

pergunte se é

$\exists a, b \in F$ tq são da forma

$a\sqrt{a} + a\sqrt{b}$

$\alpha = \sqrt{a+b\sqrt{c}}$ $a, b, c \in F$

$\alpha^2 = a + b\sqrt{c}$ $\alpha' = \sqrt{a-b\sqrt{c}}$

$(\alpha')^2 = a - b\sqrt{c}$

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

$$= x^4 - 2a x^2 + (a+b\sqrt{c})(a-b\sqrt{c})$$

$$= x^4 - 2a x^2 + (a^2 - b^2 c) = f(x)$$

F

$f(x) \in F[x]$ $\quad f(\alpha) = 0$

As raízes de f são $\alpha, \alpha', -\alpha, -\alpha'$

Como é o corpo de decomposição de $f(x)$?. $\quad K = F(\alpha, \alpha')$

$\sqrt{c}, \alpha, \alpha' \quad [K:F] \mid 8$

Porque cada um desses é de ordem 2.

$\alpha = \sqrt{a+b\sqrt{c}}$ se o grau for menor que 8 uma das raízes não é necessária.

Será que f é irredutível?

$f = x^4 + px^2 + q \quad p = -2a$

$p, q \in F \quad q = a^2 - b^2 c$

$r(y) = y^2 + py + q$ raízes são

α^2, $(\alpha')^2$ –

é o r irredutível se for.

então o polinomio f não pode ter raiz em $\mathbb{Z}$.

f não for irredutível $\Rightarrow$ f é produto de dois quadráticos.

$$X^4 + pX^2 + q = (X^2 + \lambda X + \delta)(X^2 + \mu X + \varepsilon)$$

$$= X^4 + (\lambda + \mu)X^3 + (\varepsilon + \delta + \lambda\mu)X^2 + (\lambda\varepsilon + \delta\mu)X + \delta\varepsilon$$

$$\begin{cases} \lambda + \mu = 0 \Rightarrow \mu = -\lambda \\ \lambda(\varepsilon - \delta) = 0 \Rightarrow \lambda = 0 \ \vee \ \varepsilon = \delta \end{cases}$$

$\lambda = 0 \Rightarrow \mu = 0$

$$X^4 + (\varepsilon + \delta)X^2 + \delta\varepsilon$$

$$\varepsilon + \delta = p \qquad \varepsilon \cdot \delta = q$$

$$\begin{cases} \lambda = -\mu = 0 \\ \varepsilon + \delta = p \\ \varepsilon \cdot \delta = q \end{cases}$$

outra solução. $\varepsilon = \delta$

$$\begin{cases} 2\varepsilon - \lambda^2 = p & \lambda \\ \varepsilon^2 = q & \varepsilon \end{cases}$$

$$(x^2 + \delta)(x^2 + (p-\delta)) =$$

$$x^4 + px^2 + q \overset{?}{=} (x^2 + \lambda x + \varepsilon)(x^2 - \lambda x + \varepsilon)$$

$\exists \lambda$ e $\varepsilon \in F$ tq

Queremos ver se f se fatora como produto de quadráticas.

$r(y) = y^2 + py + q$ irredutível $\in (*)$

Se f é redutível $f(\alpha) = 0$.

α é raiz de algum dos fatores de f.

$$\sqrt{3+2\sqrt{2}} = 1+\sqrt{2}$$

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

os polynomios f para os outros números. São irred.

f de $\sqrt{5+2\sqrt{5}}$ $\quad a=5=c$, $b=2$

$f = X^4 - 10X^2 + 5$ é irred. sobre $\mathbb{Q}$.

f - irredutível. α = combinação de duas raízes bi-quadráticas.

$F(\sqrt{\lambda}, \sqrt{\mu'}) = K \Rightarrow \alpha$?

$G(K/F) = \mathbb{Z}_2 \times \mathbb{Z}_2$

K - Galois. $f(x)$ se fatora como produto de lineares em K

$K \supset L$ = corpo de decomposição de f.

f irred $\deg f = 4 \Rightarrow K = L$.

Converse. se K/F com grupo de Galois $\mathbb{Z}_2 \times \mathbb{Z}_2$.

$F \subset L \subset K$ extensões de grau 2

$\sqrt{p}$ $\sqrt{q}$

Qual é o discriminante de f?

$\alpha, \alpha', -\alpha, -\alpha'$

$D = \delta^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2$

$\alpha = \sqrt{a+b\sqrt{c}}$ $\quad \alpha' = \sqrt{a-b\sqrt{c}}$

$(\alpha-\alpha')^4 (2\alpha)^2 (\alpha+\alpha')^4 (\alpha'+\alpha)^2$

$(2\alpha')^2 (\alpha'-\alpha)^2$

$16\ \alpha^2 \alpha'^2 (\alpha-\alpha')^4 (\alpha+\alpha')^4$

$16 (a+b\sqrt{c})(a-b\sqrt{c}) (\alpha^2-(\alpha')^2)^4$

$16^{11} (a^2-b^2c)(2b\sqrt{c})^4$

$D = \underbrace{2^8 (a^2-b^2c) b^4 c^2}_{\delta^2} \in F$

$\delta \in F$?

Se a^2-b^2c é um quadrado em F.

$\Leftrightarrow \delta$ está em $F \Leftrightarrow G \subset A_4$.

$|G| \mid 8$. porque a extensão é de ordem 8.

$\mathbb{Z}_2 \times \mathbb{Z}_2 \subset A_4$ é único subgrupo de A_4 com ordem dividindo 8

Transitivo.

Proposição $\alpha = \sqrt{a + b\sqrt{c}}$ $\quad a, b, c \in F$

$$f(x) = x^4 + px^2 + q$$
$$p = -2a \qquad q = a^2 - b^2c$$
} irredutível / F.

$\Rightarrow \alpha$ se escreve como combinação de duas raízes $\Leftrightarrow$ q é um quadrado em F.

$\alpha = \sqrt{5 + \sqrt{21}}$ $\quad a^2 - b^2c = 25 - 21 = 4 = 2^2$

se escreve como combinação das raízes.

$\sqrt{5 + 2\sqrt{5}}$ $\quad 2^2 - 4 \cdot 5 = 5 \neq$ quadrado.

$\sqrt{21}, \alpha, \alpha'$ $\quad \mathbb{Q} \subset \mathbb{Q}(\sqrt{21}) \subset K$

$\mathbb{Z}_2, \quad \mathbb{Z}_2$

! $\alpha, \alpha', -\alpha, -\alpha'$

$$\boxed{(X-\alpha)(X-\alpha')} = X^2 - (\alpha+\alpha')X + \alpha\alpha'$$

(H) $\subset G = \mathbb{Z}_2 \times \mathbb{Z}_2$. tem ordem 2.

$\mathbb{Z}_2$

$L = F(\alpha + \alpha', \alpha \cdot \alpha') \subset K$

$: 2$

$L = K^H$ $\qquad \alpha \cdot \alpha' =$

$\alpha = \sqrt{5+\sqrt{21}} \qquad \alpha' = \sqrt{5-\sqrt{21}}$

$\alpha\alpha' = \sqrt{25-21} = 2.$

$(\alpha+\alpha')^2 = (\sqrt{14})^2$

$5+\sqrt{21}+5-\sqrt{21}+4 = 14$

$L = F(\sqrt{14})$

$(\alpha-\alpha') = \sqrt{6}$

$\alpha = \frac{1}{2}(\sqrt{6}+\sqrt{14})$ □.

(x^3+x+1) $\qquad \sqrt{-3}$ $\qquad \sqrt{3}i$