K corpo de decomposição de $f \in F[x]$
$\deg f = 4$.

if (se f tem 1 raiz em F.)

$$(x-\alpha)\cdot g(x) \qquad \deg g = 3$$

?

Corpo de decomposição de g.

else if { f é redutível

$$f = g\,h \qquad \deg g = \deg h = 2$$

Estudamos na última aula os possíveis grupos de Galois.

?

$$\sqrt{a+b\sqrt{c}} = \alpha\sqrt{\beta} + \gamma\sqrt{\delta} \quad \}$$

Se f é irredutível ?

Topologia algébrica.) é o caso geral. no sentido que é um aberto denso no conjunto de polynomios.

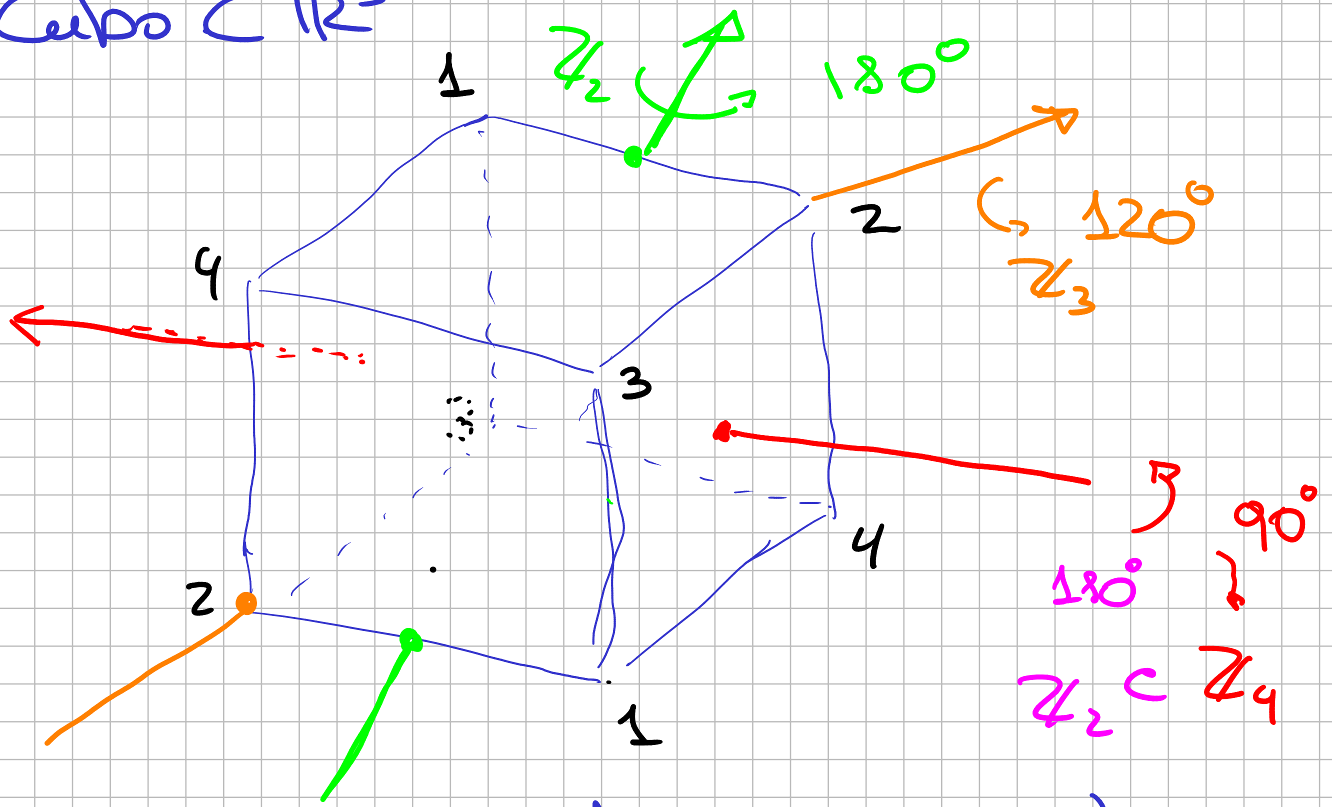
$$\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in K \setminus F$$

$$G = \mathrm{Gal}(K/F) \hookrightarrow S_4 \quad \text{permuta elas}$$

$\{\alpha_1, \dots, \alpha_4\}$ é uma órbita de G.

Não todo grupo de S_4 é transitivo.

S_4 é o grupo de simetrias rotacionais do cubo $C \subset \mathbb{R}^3$



$$S_4 = \{ g \in SO(3) \mid g \cdot C = C \}$$

$\mathbb{Z}_4$ permuta ciclicamente 4-faces e fixa duas.

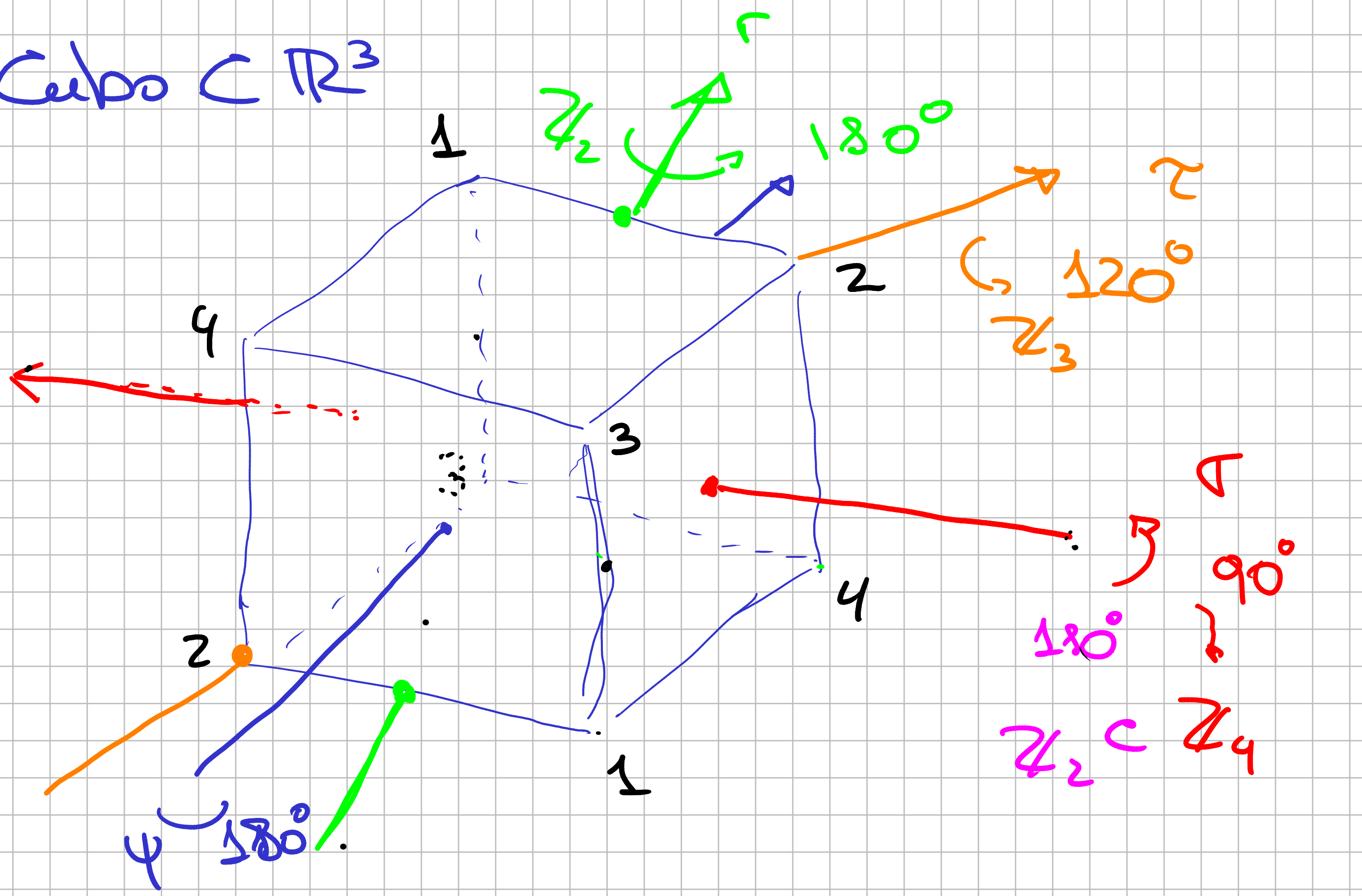
$\mathbb{Z}_2$ permuta as 12 arestas do cubo e fixa 2.

$\mathbb{Z}_3$ fixa dois vértices opostos do cubo.

$g \in Aut(C) \to$ ação de g nas 4 diagonais principais do cubo é uma permutação.

?

Cubo $\subset \mathbb{R}^3$



$\mathbb{Z}_4$ $\sigma = (1423)$ Não fixa diagonais.

$\mathbb{Z}_2$ $\sigma^2 = (12)(34)$ Não fixa diag. $\}$ A_1

$\mathbb{Z}_3$ $\tau = (134)$ fixa 1 diagonal.

$\mathbb{Z}_2$ $r = (12)$ fixa 2 diagonais.

O subgrupo gerado por todos os $\mathbb{Z}_2$ verdes é S_4.

Os subgrupos transitivos de S_4 são

S_4, A_4, D_4 – dihedral $\supset$ C_4 $\supset$ Klein. – transitivo.

σ, ψ $\qquad$ σ

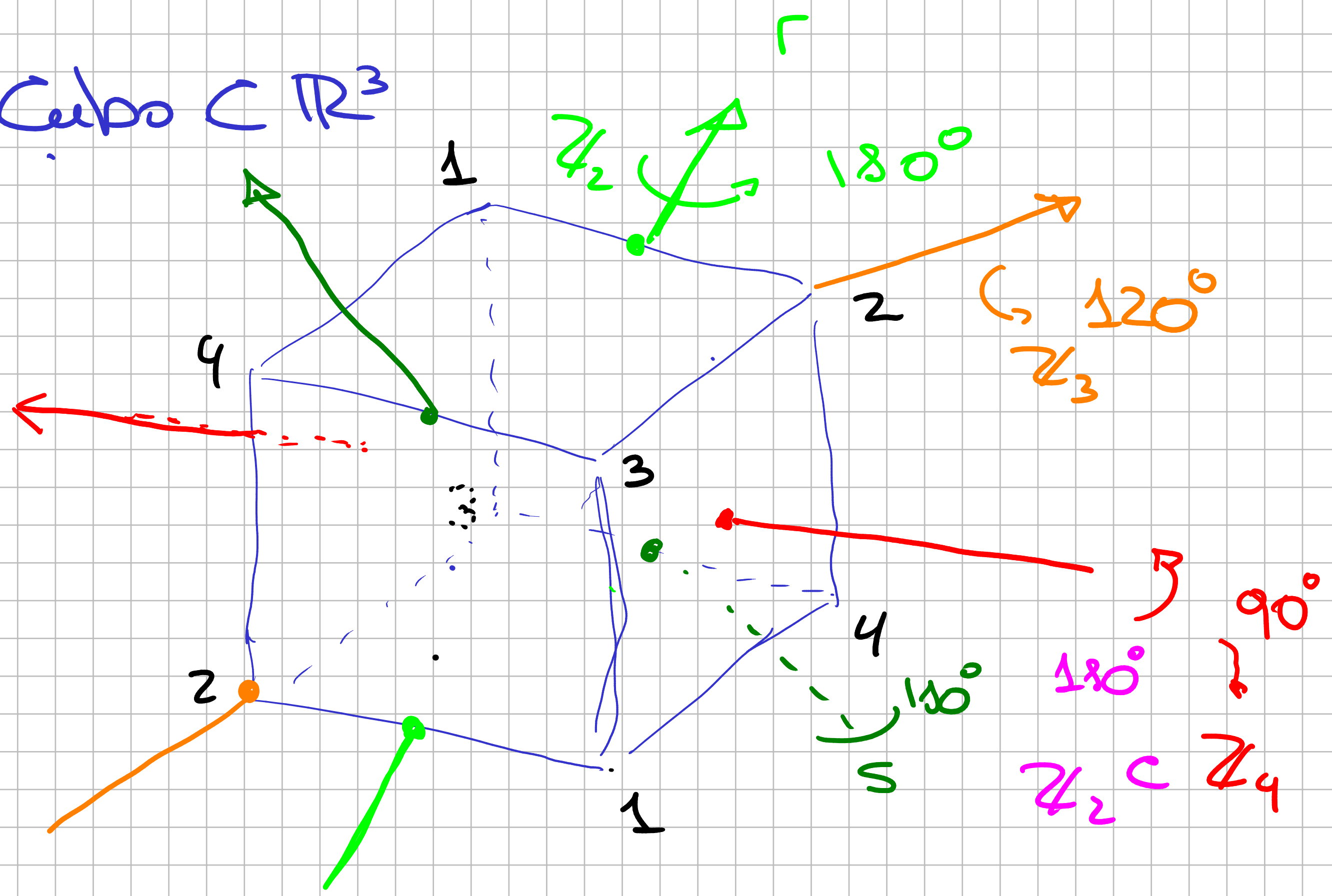
$\psi = (13)(24)$ $\quad$ $\sigma^2 = (12)(34)$

$\psi \cdot (\sigma^2) = (14)(23)$

$\{1, \psi, \sigma^2, \psi \cdot (\sigma^2)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

<u>Pergunta</u>: Achar um subgrupo de S_4 $\cong$ Klein $= \mathbb{Z}_2 \times \mathbb{Z}_2$. não seja Transitivo:

Cubo $\subset \mathbb{R}^3$



$s = (34)$ $\quad$ $r = (12)$

$\{1, r, s, \sigma^2\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Não é transitivo.

K/F corpo de decomposição de uma quártica irredutível tem Grupo de Galois $\hookrightarrow S_4$

K, C_4, D_4, A_4, S_4

$$\delta = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)(\alpha_2-\alpha_4) \times (\alpha_3-\alpha_4)$$

$\delta \in F \iff G \subset A_4$.

$\Updownarrow$

$G = A_4 \vee G = K$

$\delta \notin F \iff \underbrace{G = S_4 \quad G = D_4 \quad G = C_4}$

— . —

$\beta_1 = \alpha_1\alpha_3 + \alpha_2\alpha_4 \in K$

$\beta_2 = \alpha_1\alpha_2 + \alpha_3\alpha_4 \in K$

$\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3 \in K$

$g = (X-\beta_1)(X-\beta_2)(X-\beta_4) \in K[x]$

Claim $g \in F[x]$.

g é symmétrico.

1) $S_4 \curvearrowright \{\beta_1, \beta_2, \beta_3\}$

2) ação é transitiva.

3) $(S_4)_{\beta_1} = \text{Stab.}$ $\quad |(S_4)_{\beta_1}| = 8$

$\{\beta_1, \beta_2, \beta_3\} \simeq S_4 / \text{Stab}$

$|S_4| = 24 = 4!$

Stab. $\subset S_4$ subgrupo de ordem 8.

$D_4 \simeq$ Stab. de β_1.

$\exists\, 3$ subgrupos de $S_4 \simeq D_4$.

$\Updownarrow$

Sylow. – conjugados.

$\Updownarrow$

tres estabilizadores de cada 1 dos β_i

4. Segue que

$$g = (X-\beta_1)(X-\beta_2)(X-\beta_3) \in K[X]^{S_4}$$

$\Rightarrow$ s. $g \in F[X]$ (invariante por Galois).

⚠ Todo o que eu falei é correto se os β são variáveis formais.

Para corrigir falta ver que os β são differentes.

$$\beta_1 - \beta_2 = \cancel{\alpha_1}\alpha_3 + \alpha_2\alpha_4 - \cancel{\alpha_1}\alpha_2 - \alpha_3\alpha_4$$
$$= \alpha_1(\alpha_3 - \alpha_2) - \alpha_4(\alpha_3 - \alpha_2)$$
$$= (\alpha_1 - \alpha_4)\cdot(\alpha_3 - \alpha_2) \neq 0.$$

f irred char 0. $\Rightarrow \alpha_i \neq \alpha_j$

$$g = (X-\beta_1)(X-\beta_2)(X-\beta_3) \in F[X].$$

cúbica resolvente de f.

Quando as raízes de g estão em F. ?

$\beta_1 \in F$ $\qquad G = G(K/F)$

preserva β_1

$$G \subset (\text{Stab. de } \beta_1) \subset S_4$$

$\cong$

$\overset{12}{D_4}$

converse se g é irredutível

$\Rightarrow$ $\underline{\underline{G}} \not\subseteq D_4 \subset S_4$.

$\cdot\ g = (X-\beta_1)(X-\beta_2)(X-\beta_3)$

$h = (X^2 - \delta^2)$ $\to D \in F$

$\underline{\underline{D_4}}$ $\underline{\underline{A_4}}$ $\cup$ K

g \ h	redutível.	irred.
reduti.	$\mathbb{Z}_2 \times \mathbb{Z}_2$	D_4 v C_4
irred.	A_4	S_4

Quase completa a análise

exceto se $\delta \notin F$ $\beta_i \in F$

$[K : F] = 4 \vee 8$.

$D_4 \supset C_4 \supset \mathbb{Z}_2$.

encontrar subextensões.

No livro $\boxed{x^4 + p\cdot x + q}$.

o S_4 ou A_4.

Calcule explicitamente $\underline{D}$.

$$S_1 \quad S_2 \quad \underbrace{S_3 \quad S_4}_{\cancel{0} \qquad \cancel{p}}$$

$$1 \quad 2 \quad 3 \quad 4$$

$$x^4 + S_1 \cdot x^3 + S_2 x^2 + S_3 x + S_4$$

$$D = a\, S_3^4 + b\, S_4^3$$

a: $\pm 27 p$

b: 2^8.

?