# Feliz Aniversário, Monsieur Galois!

Este seminário de coisas legais é um oferecimento de ET

25 de outubro de 2011

# Qual a ave que mais sabe matemática?

O Galo B?

O Galo C?

É Galois, é claro!

- Nasceu em 25 de outubro de 1811 em Bourg-la-Reine (França)
- Aos 14 anos, leu "Éléments de Géométrie" de Legendre
- Aos 15 anos, já lia artigos de Lagrange, tais como "Réflexions sur la résolution algébrique des équations"

- Foi um menino levado: não passou no vestibular 2 vezes (para a École Polytechnique), foi preso por participar em movimentos republicanos.
- Morreu aos 20 anos, em 31 de maio de 1832, vítima de bala perdida (em um duelo do qual participava).

# Galois e seu trabalho

A maior contribuição de Galois para a Matemática foi a **Teoria de Galois**. Galois foi o primeiro a formular um critério necessário e suficiente para que uma equação polinomial seja solúvel por radicais. Descobriu também os chamados **corpos finitos**.
Seu trabalho foi reconhecido apenas postumamente, devido à influência de ilustres matemáticos tais como

- Cauchy, que recusou os 2 artigos que Galois submeteu aos 18 anos à Academia de Ciências da França;
- Fourier, que morreu logo após receber uma monografia do trabalho de Galois sobre a Teoria de Galois.

Na noite que antecedeu o duelo, Galois permeneceu acordado escrevendo uma carta-testamento a Auguste Chevalier contendo um esboço de suas ideias matemáticas, à qual anexou 3 manuscritos. Os resultados de Galois só foram publicados em 1843 após a revisão de Liouville.

# Soluções por radicais

**Problema:** dado um polinômio, escrever suas raízes utilizando somente as 4 operações básicas $+, -, \times, \div$ e $\sqrt{}$.

- Fórmula de Bhaskhara:

$$ax^2 + bx + c = 0 \iff x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

- Fórmula de Cardano:

$$ax^3 + bx^2 + cx + d = 0$$

$$\begin{aligned} x_1 = &-\frac{b}{3a} \\ &-\frac{1}{3a}\sqrt[3]{\frac{1}{2}\left[2b^3 - 9abc + 27a^2d + \sqrt{\left(2b^3 - 9abc + 27a^2d\right)^2 - 4\left(b^2 - 3ac\right)^3}\right]} \\ &-\frac{1}{3a}\sqrt[3]{\frac{1}{2}\left[2b^3 - 9abc + 27a^2d - \sqrt{\left(2b^3 - 9abc + 27a^2d\right)^2 - 4\left(b^2 - 3ac\right)^3}\right]} \end{aligned}$$

# Corpos

Para esta palestra, adotaremos

## Definição

*Um* **corpo** $K$ *é um subconjunto de* $\mathbb{C}$ *que é fechado pelas 4 operações básicas* $+, -, \times, \div$, *ou seja,*

$$\begin{cases} a \in K \\ b \in K \end{cases} \implies a+b,\ a-b,\ a\cdot b,\ a/b \in K \quad (b \neq 0 \text{ no último caso})$$

Exemplos: $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

## Definição

*Se* $K$ *é um corpo e* $\theta \in \mathbb{C}$, *denotamos por*

$$\begin{aligned} K(\theta) &= \text{menor corpo contendo } K \text{ e } \theta \\ &= \left\{ \begin{array}{l} \underline{\textbf{todas}} \text{ as expressões formadas a partir de elementos} \\ \text{de } K \text{ e } \theta \text{ utilizando as 4 operações } +,\ -,\ \times \text{ e } \div \end{array} \right\} \end{aligned}$$

# Exemplo: $\mathbb{Q}(\sqrt{2})$

Por exemplo, $\mathbb{Q}(\sqrt{2})$ é o conjunto de todas as expressões tais como

$$3-5\sqrt{2}, \qquad \frac{3-5\sqrt{2}}{1+(\sqrt{2})^{2001}}, \qquad \frac{1+3(\sqrt{2})^{21}}{1+\frac{3}{\sqrt{2}}} - \frac{5\sqrt{2}}{1-\sqrt{2}}, \ldots$$

Não é difícil se convencer de que

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

pois todas as expressões acima podem ser "simplificadas" para a forma acima. Por exemplo:

$$\frac{3-5\sqrt{2}}{1+(\sqrt{2})^3} = \frac{3-5\sqrt{2}}{1+2\sqrt{2}} \overset{\text{racionalize}}{=} \frac{3-5\sqrt{2}}{1+2\sqrt{2}} \cdot \frac{1-2\sqrt{2}}{1-2\sqrt{2}}$$

$$= \frac{23-11\sqrt{2}}{-7} = \underbrace{-\frac{23}{7}}_{a\in\mathbb{Q}} + \underbrace{\frac{11}{7}}_{b\in\mathbb{Q}} \cdot \sqrt{2}$$

# Ok, mas o que isto tem a ver com nosso problema?

Em linguagem corporal: existir uma "fórmula" para as raízes

$$\alpha_1, \alpha_2, \ldots, \alpha_n$$

de um polinômio $p(x) \in \mathbb{Q}[x]$ é o mesmo que existir uma "torre radical de corpos"

$$\begin{array}{rcll}
\alpha_1, \ldots, \alpha_n \in K_r & = & K_{r-1}(\sqrt[n_r]{a_{r-1}}) & \quad (a_{r-1} \in K_{r-1}) \\
\cup & & & \\
\vdots & & & \\
\cup & & & \\
K_2 & = & K_1(\sqrt[n_2]{a_1}) & \quad (a_1 \in K_1) \\
\cup & & & \\
K_1 & = & K_0(\sqrt[n_1]{a_0}) & \quad (a_0 \in K_0) \\
\cup & & & \\
K_0 & = & \mathbb{Q} &
\end{array}$$

# Exemplo: torre radical de corpos

Por exemplo, para a equação $x^3 + 6x - 20 = 0$, a raiz

$$\sqrt[3]{10+\sqrt{108}} + \sqrt[3]{-10+\sqrt{108}} \in K_3$$

onde

$$\begin{aligned} K_3 &= K_2\left(\sqrt[3]{-10+\sqrt{108}}\right) \\ &\cup \\ K_2 &= K_1\left(\sqrt[3]{10+\sqrt{108}}\right) \\ &\cup \\ K_1 &= K_0(\sqrt{108}) \\ &\cup \\ K_0 &= \mathbb{Q} \end{aligned}$$

# Simetrias de Corpos

Ideia genial de Galois: estudar **simetrias** ou **automorfismos** de extensões de corpos $L \supset K$.

## Definição

*Dada uma extensão de corpos $L \supset K$, um $K$-***automorfismo** *é uma função bijetora*

$$\sigma : L \to L$$

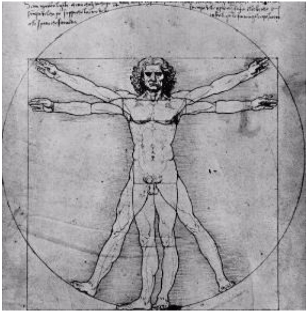
*que preserva as 4 operações*

$$\begin{array}{ll} \sigma(a+b) = \sigma(a) + \sigma(b) & \sigma(a \cdot b) = \sigma(a) \cdot \sigma(b) \\ \sigma(a-b) = \sigma(a) - \sigma(b) & \sigma(a/b) = \sigma(a)/\sigma(b) \end{array}$$

*e cuja restrição a $K$ é a identidade:*

$$a \in K \implies \sigma(a) = a$$

# Exemplo: simetria de corpos





Responda rápido: se

$$\frac{(1+5i)(2+i)^2}{5(1-3i)} = -\frac{37}{25} - \frac{16}{25}i$$

quanto vale

$$\frac{(1-5i)(2-i)^2}{5(1+3i)} = ?$$

Você acaba de aplicar o $\mathbb{R}$-automorfismo $\sigma(z) = \overline{z}$:

$$\sigma\left(\frac{(1+5i)(2+i)^2}{5(1-3i)}\right) = \sigma\left(-\frac{37}{25} - \frac{16}{25}i\right) \implies$$

$$\frac{\sigma(1+5i)\cdot\sigma(2+i)^2}{\sigma(5)\cdot\sigma(1-3i)} = -\frac{37}{25}+\frac{16}{25}i \iff \frac{(1-5i)(2-i)^2}{5(1+3i)} = -\frac{37}{25}+\frac{16}{25}i$$

# Grupo de Galois

## Definição

*Dada uma extensão de corpos $L \supset K$, o conjunto $\mathsf{Gal}(L/K)$ de* **todos** *os $K$-automorfimos $\sigma\colon L \to L$ é chamado de* **grupo de Galois** *de $L$ sobre $K$. Note que*

$$\sigma, \tau \in \mathsf{Gal}(L/K) \implies \sigma \circ \tau \in \mathsf{Gal}(L/K)$$

Por exemplo, $\mathsf{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$, onde $\sigma$ é a conjugação complexa. Temos a relação $\sigma \circ \sigma = \mathrm{id}$.
Um caso muito importante para nós é o grupo de Galois de extensões radicais $K(\sqrt[n]{a}) \supset K$.

# Exemplo: $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{3})/\mathbb{Q}(i))$

Dado $\sigma \in \mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{3})/\mathbb{Q}(i))$, temos

$$\sigma|_{\mathbb{Q}(i)} = \mathrm{id}$$

então $\sigma$ é determinado por sua ação sobre o gerador $\sqrt[4]{3}$ da extensão.

**Pergunta**: Quais valores $\sigma(\sqrt[4]{3})$ pode assumir?

Note: $\sqrt[4]{3}$ é raiz de $f(x) = x^4 - 3$, ou seja,

$$(\sqrt[4]{3})^4 - 3 = 0 \implies \sigma\Big((\sqrt[4]{3})^4 - 3\Big) = \sigma(0)$$

$$\implies \Big(\sigma(\sqrt[4]{3})\Big)^4 - 3 = 0 \iff \Big(\sigma(\sqrt[4]{3})\Big)^4 = 3$$

**Resumindo:**

$$\sigma(\sqrt[4]{3}) \in \{\sqrt[4]{3}, -\sqrt[4]{3}, i\sqrt[4]{3}, -i\sqrt[4]{3}\}$$

é uma das 4 raízes complexas de $f(x) = x^4 - 3$.

**Teorema (Princípio da Conservação de Raízes)**

*Seja $K$ um corpo, $f(x) \in K[x]$ um polinômio e $\theta \in \mathbb{C}$ uma raiz de $f(x)$. Se $\sigma \in \mathrm{Gal}(K(\theta)/K)$, então $\sigma(\theta)$ é outra raiz de $f(x)$.*
*Em suma,*

$\sigma\Big($ 

$\Big) =$ 

Note que isto implica que se $L \supset K$ é gerado por um número finito de elementos, então há um número finito de simetrias!

$$|\,\mathrm{Gal}(L/K)| < \infty$$

# Exemplo: $\mathrm{Gal}(\mathbb{Q}(i,\sqrt[4]{3})/\mathbb{Q}(i))$ (continuação)

Voltando: temos

$$\mathrm{Gal}(\mathbb{Q}(i,\sqrt[4]{3})/\mathbb{Q}(i)) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$$

onde

$$\begin{aligned} \mathrm{id}\colon \sqrt[4]{3} &\mapsto \sqrt[4]{3} \\ \sigma_1\colon \sqrt[4]{3} &\mapsto i\sqrt[4]{3} \\ \sigma_2\colon \sqrt[4]{3} &\mapsto -\sqrt[4]{3} \\ \sigma_3\colon \sqrt[4]{3} &\mapsto -i\sqrt[4]{3} \end{aligned}$$

O que é o que é? $\sigma_1 \circ \sigma_1$? Note que

$$\sqrt[4]{3} \xmapsto{\sigma_1} i \cdot \sqrt[4]{3} \xmapsto{\sigma_1} i \cdot i\sqrt[4]{3} = -\sqrt[4]{3}$$

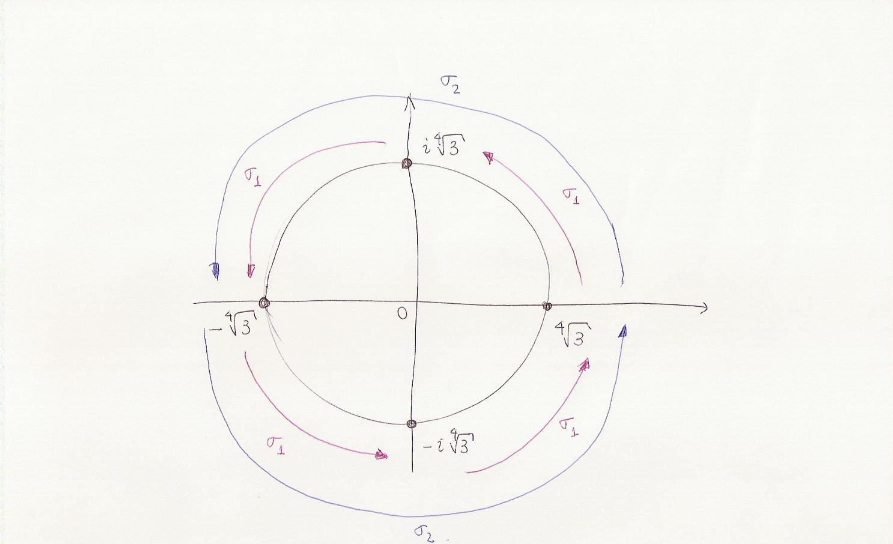
Ou seja,

$$\sigma_1 \circ \sigma_1 = \sigma_2$$

# Exemplo: Gal($\mathbb{Q}(i, \sqrt[4]{3})/\mathbb{Q}(i)$) (continuação)

Da mesma forma,

$$\sigma_1 \circ \sigma_1 \circ \sigma_1 = \sigma_3 \qquad \text{e} \qquad \sigma_1 \circ \sigma_1 \circ \sigma_1 \circ \sigma_1 = \mathrm{id}$$



# Extensões radicais e simetrias cíclicas

**Teorema**

*Suponha que $K$ contenha todas as raízes n-ésimas de 1. Então* $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ *é um grupo cíclico. Em outras palavras:*

$$\boxed{\boxed{\textit{extensões radicais possuem simetrias cíclicas}}}$$

**Teorema**

*Na presença de raízes de 1, suponha que*

$$K_0 \subset K_1 = K_0(\sqrt[n]{a_0}) \subset \cdots \subset K_r = K_{r-1}(\sqrt[n]{a_{r-1}})$$

*é uma torre de extensões radicais. Então* $G = \mathrm{Gal}(K_r/K_0)$ *admite uma sequência de subgrupos*

$$G = G_r \supset G_{r-1} \supset G_{r-2} \supset \cdots \supset G_0 = 1$$

*tal que* $G_{i-1} \lhd G_i$ *e* $\boxed{G_i/G_{i-1} \textbf{ é cíclico}}$.

# Um exemplo concreto de equação

**Resumindo:**
raízes de um polinômio solúvel por radicais $\longrightarrow$ torre radical de corpos $\longrightarrow$ grupo de simetria com fatores cíclicos

Poucos grupos possuem a decomposição acima. Por exemplo, seja

$$x^5 - x + 1 = 0$$

e sejam $\alpha, \beta, \gamma, \delta, \epsilon$ suas raízes. Se $L = \mathbb{Q}(\alpha, \beta, \gamma, \delta, \epsilon)$ então

$$\mathrm{Gal}(L/\mathbb{Q}) \cong S_5$$

não admite tal decomposição. Logo a equação acima não é solúvel por radicais.

# Créditos. . .

# Dilbert's Nullstellensatz