Grupos e Corpos

Prof. Lucas Calixto

Aula 11 - Teoria de Galois

Problema: dado um poli $p(x)$, queremos achar uma formula para as raízes de $p(x)$ que envolva somente seus coeficientes (soma, multiplicação, divisão, extrair raízes). Quando isso é possível, dizemos que $p(x)$ é solúvel por radicais

Exemplo: Se $\text{gr}(p(x)) \leq 4 \Rightarrow p(x)$ é solúvel por radicais

- $p(x) = ax + b \Rightarrow b/a$

- $p(x) = ax^2 + bx + c \Rightarrow \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

- matemáticos italianos resolveram para $\text{gr}(p(x)) = 3, 4$

- Se $\text{gr}(p(x)) \geq 5$, Abel e Ruffini acharam exemplos que não são solúveis por radicais

E. Galoi foi quem determinou critérios para se responder essa pergunta. Para isso ele desenvolveu e conectou teoria de grupos com teoria de corpos

Corpo de automorfismos

Lembrem: o grupo de automorfismos de $\mathbb{F}$ é $\mathrm{Aut}(\mathbb{F}) = \{\sigma : \mathbb{F} \to \mathbb{F} \mid \sigma \text{ é iso}\}$

Proposição: $(\mathrm{Aut}(\mathbb{F}), \circ = \text{composição})$ é um grupo (exercício)

Proposição: Se $\mathbb{F} \subset \mathbb{E}$, então $\{\sigma \in \mathrm{Aut}(\mathbb{E}) \mid \sigma(\alpha) = \alpha \ \forall \alpha \in \mathbb{F}\}$ é subgrupo de $\mathrm{Aut}(\mathbb{E})$ (exercício)

O grupo de Galois de $\mathbb{E}$ sobre $\mathbb{F}$ é

$$G(\mathbb{E}/\mathbb{F}) = \{\sigma \in \mathrm{Aut}(\mathbb{E}) \mid \sigma(\alpha) = \alpha \ \forall \alpha \in \mathbb{F}\}$$

Se $f(x) \in \mathbb{F}[x]$ e $\mathbb{E}$ é o corpo de fatoração de $f(x)$ sobre $\mathbb{F}$, definimos o grupo de Galois de $f(x)$ como sendo $G(\mathbb{E}/\mathbb{F})$

Exemplo: $\sigma : \mathbb{C} \to \mathbb{C}$, $\sigma(a + bi) = a - bi$ é elemento de $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$

Exemplo: Considere $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Note que

$$\sigma : \mathbb{Q}(\sqrt{5}) \to \mathbb{Q}(\sqrt{5}), \quad \sigma(a + b\sqrt{5}) = a - b\sqrt{5}$$

é elemento de $\mathrm{Aut}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$

Similarmente,

$$\tau : \mathbb{Q}(\sqrt{3}, \sqrt{5}) \to \mathbb{Q}(\sqrt{3}, \sqrt{5}), \quad \tau(a + b\sqrt{3}) = a - b\sqrt{3}$$

é elemento de $\mathrm{Aut}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{5}))$

Note: $\mu = \sigma\tau$ mexe com ambos $\sqrt{3}$ e $\sqrt{5}$, mas ainda fixa elementos de $\mathbb{Q}$. Veremos que $\{\mathrm{id}, \sigma, \tau, \mu\} = G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$

$$\begin{array}{c|cccc} \cdot & \mathrm{id} & \sigma & \tau & \mu \\ \hline \mathrm{id} & \mathrm{id} & \sigma & \tau & \mu \\ \sigma & \sigma & \mathrm{id} & \mu & \tau \\ \tau & \tau & \mu & \mathrm{id} & \sigma \\ \mu & \mu & \tau & \sigma & \mathrm{id} \end{array} \quad \Rightarrow \quad G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Sabemos também que $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ é $\mathbb{Q}$-esp. vet. com base $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$, e portanto

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4 = |G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})| \quad \text{(não é coincidencia!)}$$

Proposição: Seja $\mathbb{F} \subset \mathbb{E}$, $f(x) \in \mathbb{F}[x]$, e $R \subset \mathbb{E}$ o conjunto das raízes de $f(x)$ que vivem em $\mathbb{E}$. Se $\sigma \in G(\mathbb{E}/\mathbb{F})$, então $\sigma \in S_R =$ grupo das permutações de R

Prova: Segue do simples fato que $\sigma(f(\alpha)) = f(\sigma(\alpha))$, $\forall \alpha \in \mathbb{E}$ ■

Seja $\mathbb{F} \subset \mathbb{E}$ extensão algébrica. Dizemos que $\alpha, \beta \in \mathbb{E}$ são conjugados sobre $\mathbb{F}$ se $m_\alpha(x) = m_\beta(x) \in \mathbb{F}[x]$.

Na outra direção da proposição anterior, temos

Proposição: Seja $\mathbb{F} \subset \mathbb{E}$. Se $\alpha, \beta \in \mathbb{E}$ são conjugados, então existe único isomorfismo $\sigma : \mathbb{F}(\alpha) \to \mathbb{F}(\beta)$ tal que $\sigma|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$

Prova: Segue da aula passada (ou lema 21.32 do livro tomando $\phi = \mathrm{id}_{\mathbb{F}}$) ■

Exemplo: $\sqrt{2}, -\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ são conjugados sobre $\mathbb{Q}$

O exemplo do slide anterior não era coincidência

Proposição: Seja $f(x) \in \mathbb{F}[x]$ e $\mathbb{E} \supset \mathbb{F}$ o corpo de fatoração de $f(x)$. Se $f(x)$ é separável, então

$$|G(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]$$

Prova: Indução sobre $[\mathbb{E} : \mathbb{F}]$

$[\mathbb{E} : \mathbb{F}] = 1 \Rightarrow \mathbb{E} = \mathbb{F} \Rightarrow G(\mathbb{E}/\mathbb{F}) = \{\mathrm{id}\}$

Suponha $[\mathbb{E} : \mathbb{F}] > 1$. Escreva $f(x) = p(x)q(x)$ em $\mathbb{F}[x]$, com $p(x)$ irredutível (monico) e $\mathrm{gr}(p(x)) = d > 1$ (se todo irredutível tivesse grau 1, f seria fatorável em $\mathbb{F}[x]$)

Fixe $\alpha \in \mathbb{E}$ raiz de $p(x)$

$p(x)$ separável $\Rightarrow p(x)$ tem d raízes distintas $R = \{\beta_1, \ldots, \beta_d\}$

ultimo slide $\Rightarrow$ cada $\phi \in G(\mathbb{E}/\mathbb{F})$ nos dá um homomorfismo injetor $\phi : \mathbb{F}(\alpha) \to \mathbb{E}$ que fixa $\mathbb{F}$, e este deve nos dar um isomorfismo $\phi : \mathbb{F}(\alpha) \to \mathbb{F}(\beta)$, onde $\beta = \phi(\alpha)$

ultimo slide $\Rightarrow$ para cada β_i, temos um isomorfismo $\phi : \mathbb{F}(\alpha) \to \mathbb{F}(\beta_i)$ que fixa $\mathbb{F}$

Logo, temos exatamente d homomorfismos injetores $\phi : \mathbb{F}(\alpha) \to \mathbb{E}$ que fixam $\mathbb{F}$

$p(x)$ irredutível $\Rightarrow p(x) = m_\alpha(x)$. Daí

$$[\mathbb{F}(\alpha):\mathbb{F}] = d \text{ e } [\mathbb{E}:\mathbb{F}] = [\mathbb{E}:\mathbb{F}(\alpha)][\mathbb{F}(\alpha):\mathbb{F}] \Rightarrow [\mathbb{E}:\mathbb{F}(\alpha)] = [\mathbb{E}:\mathbb{F}]/d$$

Indução $\Rightarrow [\mathbb{E}:\mathbb{F}(\alpha)] = |G(\mathbb{E}/\mathbb{F}(\alpha))| = [\mathbb{E}:\mathbb{F}]/d$. Ou seja, temos $[\mathbb{E}:\mathbb{F}]/d$ automorfismos $\psi : \mathbb{E} \to \mathbb{E}$ que estendem $\mathrm{id}_{\mathbb{F}(\alpha)}$

$\Rightarrow$ para cada um dos d isomorfismos $\phi : \mathbb{F}(\alpha) \to \mathbb{F}(\beta_i)$ acima, temos $[\mathbb{E}:\mathbb{F}]/d$ automorfismos $\psi : \mathbb{E} \to \mathbb{E}$ que estendem ϕ (todos fixando elementos de $\mathbb{F}$)

Logo, temos $[\mathbb{E}:\mathbb{F}]$ elementos de $G(\mathbb{E}/\mathbb{F})$ construidos como sendo a extensões dos ϕ

Por outro lado, cada $\psi \in G(\mathbb{E}/\mathbb{F})$ quando restrito a $\mathbb{F}(\alpha)$ coincide com algum dos ϕ, e portanto é construido como acima $\Rightarrow [\mathbb{E}:\mathbb{F}] = |G(\mathbb{E}/\mathbb{F})|$ $\blacksquare$

Proposição: Seja $\mathbb{F}$ corpo finito e $\mathbb{E} \supset \mathbb{F}$ extensão finita. Se $[\mathbb{E} : \mathbb{F}] = k$, então $G(\mathbb{E}/\mathbb{F})$ é cíclico de ordem k

Prova: Sobre essas condições, temos $\operatorname{car} \mathbb{E} = \operatorname{car} \mathbb{F} = p$ para algum p (pois $1_{\mathbb{E}} = 1_{\mathbb{F}}$). Além disso, $|\mathbb{E}| = p^m$ e $|\mathbb{F}| = p^n$ com $m = kn$ pois

$$m = [\mathbb{E} : \mathbb{Z}_p] = [\mathbb{E} : \mathbb{F}][\mathbb{F} : \mathbb{Z}_p] = kn$$

ultima aula $\Rightarrow$ $\mathbb{E}$ é o corpo de fatoração de $x^{p^m} - x$ sobre $\mathbb{Z}_p$ (e sobre $\mathbb{F}$)

Teorema anterior $\Rightarrow |G(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}] = k$

Afirmamos que $\sigma : \mathbb{E} \to \mathbb{E}$ tal que $\sigma(\alpha) = \alpha^{p^n}$ é gerador de $G(\mathbb{E}/\mathbb{F})$

Use formula binomial + $\mathbb{F}$ ser corpo de fatoração de $x^{p^n} - x$ sobre $\mathbb{Z}_p$ para ver que $\sigma \in G(\mathbb{E}/\mathbb{F})$ (lembrem $\mathbb{F}$ = conjunto das raízes desse poli)

Para ver que $|\sigma| = k$. Note que, para todo $\alpha \in \mathbb{E}$, temos $\sigma^k(\alpha) = (\alpha^{p^n})^k = \alpha^{p^m} = \alpha$, pois $\mathbb{E}$ = conjunto das raízes de $x^{p^m} - x \Rightarrow \sigma^k = \mathrm{id}_{\mathbb{E}}$

Se $\sigma^r = \mathrm{id}_{\mathbb{E}}$ para $r < k$, então para todo $\alpha \in \mathbb{E}$, teríamos

$$\sigma^r(\alpha) = \alpha \Rightarrow \alpha^{p^{nr}} = \alpha$$

$\Rightarrow x^{p^{rn}} - x$ teria p^m raízes, o que é uma contradição $(p^{rn} < p^m)$ ■

Exemplo: Considere a extensão $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Já sabemos que $H = \{\mathrm{id}, \sigma, \tau, \mu\} \leq G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$. A igualdade segue do fato que

$$|G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4 = |H|$$

Exemplo: Vamos calcular o grupo de Galois do poli ciclotômico

$$f(x) = x^4 + x^3 + x^2 + x + 1$$

sobre $\mathbb{Q}$. Para achar o corpo de fatoração de $f(x)$, note que $(x-1)f(x) = x^5 - 1 \Rightarrow$ as raízes de $f(x)$ são $e^{\frac{ik2\pi}{5}}$ para $k = 1, 2, 3, 4$, ou seja, ω^k onde

$$\omega = e^{\frac{i2\pi}{5}} = \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5})$$

Logo, o corpo de fatoração de $f(x)$ é $\mathbb{Q}(\omega)$. Sabemos que para cada $k = 1, 2, 3, 4$, podemos definir $\sigma : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$, que fixa $\mathbb{Q}$ e tal que $\sigma(\omega) = \omega^k$. Como temos 4 desses, e

$$|G(\mathbb{Q}(\omega)/\mathbb{Q})| = [\mathbb{Q}(\omega) : \mathbb{Q}] = 4 \qquad \text{(pois } f(x) \text{ é irredutível)}$$

conluímos que $G(\mathbb{Q}(\omega)/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{Z}_4$

Extensões separáveis

Lembrem: $\mathbb{F} \subset \mathbb{E}$ é dita separável se todo elemento de $\mathbb{E}$ é raíz de poli separável em $\mathbb{F}[x]$

Proposição: Seja $f(x) \in \mathbb{F}[x]$ irredutível. Se $\operatorname{car} \mathbb{F} = 0$, então $f(x)$ é separável. Se $\operatorname{car} \mathbb{F} = p$ e $f(x) \neq g(x^p)$ para qualquer $g(x) \in \mathbb{F}[x]$, então $f(x)$ também é separável

Prova: Sabemos que $f(x)$ é separável se e só se $mdc(f(x), f'(x)) = 1$

Note que $\operatorname{gr}(f'(x)) < \operatorname{gr}(f(x))$. Logo, $mdc(f(x), f'(x)) \neq 1 \Leftrightarrow f'(x) = 0$

Se $\operatorname{car} \mathbb{F} = 0$, então $f'(x) = 0$ não é possível

Se $\operatorname{car} \mathbb{F} = p$, então $f'(x) = 0 \Leftrightarrow f(x) = g(x^p)$ para algum $g(x) \in \mathbb{F}[x]$ (cheque) ■

Lembrem que uma extensão $\mathbb{F} \subset \mathbb{E}$ é simples se $\mathbb{E} = \mathbb{F}(\alpha)$ para algum $\alpha \in \mathbb{E}$. Nesse caso, chamamos α de primitivo

Vimos que podemos ter casos em que $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5}), \qquad \mathbb{Q}(\sqrt[3]{5}, i\sqrt{5}) = \mathbb{Q}(i\sqrt[6]{5})$$

Já sabemos também que qualquer extensão finita $\mathbb{F} \subset \mathbb{E}$ de um corpo finito $\mathbb{F}$ deve ser simples, ou seja, deve existir elemento primitivo em $\mathbb{E}$ (lembrem, nesse caso tal extensão é separável: precisamente, $\mathbb{E}$ é corpo de fatoração do poli separável $x^{p^n} - x$)

Em geral, temos

Proposição: Se $\mathbb{F} \subset \mathbb{E}$ é finita e separável, então $\mathbb{E} = \mathbb{F}(\alpha)$ para algum $\alpha \in \mathbb{E}$

Prova: Podemos assumir que $\mathbb{F} = \infty$

Sabemos que $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ para alguns elementos $\alpha_i \in \mathbb{E}$

Assim, se provarmos que $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$ para algum $\gamma \in \mathbb{F}(\alpha, \beta)$, então o resultado segue por indução

Tome $f(x), g(x) \in \mathbb{F}[x]$ os polis minimais de α e β, respetivamente. Seja $\mathbb{K}$ um corpo que contem todas as raízes de $f(x)$ e $g(x)$ (sejam elas $\{\alpha_1 = \alpha, \ldots, \alpha_n\}$ e $\{\beta_1 = \beta, \ldots, \beta_m\}$)

Como F é infinito, existe $a \in \mathbb{F}$ tal que

$$a \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}, \quad \forall j \neq 1 \Rightarrow a(\beta - \beta_j) \neq \alpha_i - \alpha$$

Tome $\gamma = \alpha + a\beta$. Afirmamos que $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$. Por construção de γ, temos

$$\gamma \neq \alpha_i + a\beta_j, \quad \forall j \neq 1 \Rightarrow \gamma - a\beta_j \neq \alpha_i \quad \forall j \neq 1$$

Defina $h(x) \in \mathbb{F}(\gamma)[x]$ por $h(x) = f(\gamma - ax)$

Note: $h(\beta) = f(\alpha) = 0$, mas $h(\beta_j) = f(\gamma - a\beta_j) \neq 0$ pois $\gamma - a\beta_j \neq \alpha_i \Rightarrow x - \beta$ é o único fator comum de $h(x)$ e $g(x)$ em $\mathbb{K}[x] \Rightarrow mdc(h(x), g(x)) = x - \beta$ em $\mathbb{K}[x]$

Como o poli minimal de β sobre $\mathbb{F}(\gamma)$ divide ambos $h(x)$ e $g(x)$ e é obviamente um elemento de $\mathbb{K}[x]$, este deve ser igual a $x - \beta$

$\Rightarrow x - \beta \in \mathbb{F}(\gamma)[x] \Rightarrow \beta \in \mathbb{F}(\gamma) \Rightarrow \alpha = \gamma - a\beta \in \mathbb{F}(\gamma) \Rightarrow \mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$ ■

Corpos intermediários

Para cada extensão $\mathbb{F} \subset \mathbb{E}$, associamos um subgrupo de $\mathrm{Aut}(\mathbb{E})$ (o grupo de Galois $G(\mathbb{E}/\mathbb{F})$)

Na outra direção, dado um subgrupo de $\mathrm{Aut}(\mathbb{E})$ vamos associar um subcorpo de $\mathbb{E}$

Proposição: Seja $A \subset \mathrm{Aut}(\mathbb{F})$. Então

$$\mathbb{F}_A = \{a \in \mathbb{F} \mid \sigma(a) = a,\ \forall \sigma \in A\}$$

é subcorpo de $\mathbb{F}$

Prova: Exercício

Corolário: Se $G \leq \mathrm{Aut}(\mathbb{F})$, então

$$\mathbb{F}_G = \{a \in \mathbb{F} \mid \sigma(a) = a,\ \forall \sigma \in G\}$$

é subcorpo de $\mathbb{F}$

Chamamos $\mathbb{F}_G$ de subcorpo dos pontos fixos por G

Exemplo: Seja $\sigma : \mathbb{Q}(\sqrt{3}, \sqrt{5}) \to \mathbb{Q}(\sqrt{3}, \sqrt{5})$ tal que $\sigma(\sqrt{3}) = -\sqrt{3}$. Então $\mathbb{Q}(\sqrt{3}, \sqrt{5})_\sigma = \mathbb{Q}(\sqrt{5})$

Proposição: Seja $\mathbb{E}$ o corpo de fatoração de um poli separável sobre $\mathbb{F}$. Então $\mathbb{E}_{G(\mathbb{E}/\mathbb{F})} = \mathbb{F}$

Prova: Seja $G = G(\mathbb{E}/\mathbb{F})$. Sabemos que $\mathbb{F} \subset \mathbb{E}_G \subset \mathbb{E}$

Pela definição de $\mathbb{E}_G$, segue que $G(\mathbb{E}/\mathbb{F}) = G(\mathbb{E}/\mathbb{E}_G)$. Logo,

$$|G| = [\mathbb{E} : \mathbb{E}_G] = [\mathbb{E} : \mathbb{F}] \text{ e } [\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{E}_G][\mathbb{E}_G : \mathbb{F}] \Rightarrow [\mathbb{E}_G : \mathbb{F}] = 1 \Rightarrow \mathbb{E}_G = \mathbb{F}$$

Proposição: Seja $G \leq \mathrm{Aut}(\mathbb{E})$ um grupo finito e $\mathbb{F} = \mathbb{E}_G$. Então, $[\mathbb{E} : \mathbb{F}] \leq |G|$

Prova: Seja $G = \{\sigma_1 = \mathrm{id}, \sigma_2, \dots, \sigma_n\}$. Tome $e_1, \dots, e_{n+1} \in \mathbb{E}$ quaisquer

Considere o sistema linear homogêneo

$$\begin{cases} \sigma_1(e_1)x_1 + \cdots + \sigma_1(e_{n+1})x_{n+1} = 0 \\ \qquad\qquad \vdots \\ \sigma_m(e_1)x_1 + \cdots + \sigma_m(e_{m+1})x_{n+1} = 0 \end{cases}$$

que tem mais variáveis do que equações e portanto admite solução não trivial
$a_1, \ldots, a_{n+1} \Rightarrow a_1 e_1 + \cdots + a_{n+1} e_{n+1} = 0$ (1º equação)

Afirmamos que todos os a_i são elementos de $\mathbb{F}$. Suponha o contrário

Dentre todas as soluções com algum $a_i \in \mathbb{E} \setminus \mathbb{F}$, escolha uma que possui mais a_i's iguais a zero

Podemos assumir $a_1 \neq 0$ e portanto $a_1 = 1$, e também que $a_2 \in \mathbb{E} \setminus \mathbb{F}$ (basta multiplicar tal solução por a_1^{-1} e reordenar os e_i's)

Tome $\sigma_i \in G$ tal que $\sigma_i(a_2) \neq a_2$ (tal σ_i existe pois $\mathbb{F} = \mathbb{E}_G$)

Aplicando σ_i no sistema de equações (com a_i no lugar de x_i) nos dá o mesmo sistema de equações, pois G é grupo

Portanto $b_1 = \sigma_i(a_1) = 1$, $b_2 = \sigma(a_2) \neq a_2, \ldots, b_{n+1} = \sigma_i(a_{n+1})$ também é uma solução

Note que

$$(a_1, \ldots, a_{n+1}) - (b_1, \ldots, b_{n+1}) = (0, a_2 - b_2 \neq 0, \ldots, a_{n+1} - b_{n+1}) \neq (0, \ldots, 0)$$

é solução não trivial do sistema, e tem mais zeros do que $(a_1, \ldots, a_{n+1})$ $(a_i = 0 \Rightarrow b_i = 0$, mas $a_1 \neq 0$ e $b_1 = 0)$, contradizendo nossa hipótese

Logo, $a_i \in \mathbb{F}$ para todo i e portanto $\{e_1, \ldots, e_{n+1}\}$ é LD $\Rightarrow [\mathbb{E} : \mathbb{F}] \leq |G|$ ■