Parte 2

Teoria de Galois

Nosso objetivo é apresentar a Teoria de Galois, que a extensões finitas de corpos $L|K$ associa o seu grupo de automorfismos $G(L|K)$, chamado de Grupo de Galois de $L|K$; assim como, a subgrupos H de $G(L|K)$ associa um corpo intermediário, chamado de corpo fixo de H, definido por

$$L_H = \{x \in L \,;\, \varphi(x) = x, \text{ para todo } \varphi \in H\},$$

com $K \subset L_H \subset L$.

Quando $L|K$ é uma extensão finita normal e separável, dizemos que $L|K$ é extensão galoisiana finita. Nesse caso, a correspondência de Galois estabelece uma bijeção entre os subgrupos de $G(L|K)$ e os corpos intermediários de $L|K$, que reverte a inclusão. Essa correspondência permite traduzir informações sobre o grupo de automorfismos de $L|K$ em propriedades de seus corpos intermediários e vice-versa.

A resolução de equações por meio de radicais será relacionada com o conceito de grupos solúveis. Mostraremos a impossibilidade de expressar as raízes da equação geral do quinto grau em termos de radicais de funções algébricas racionais dos seus coeficientes.

Finalizamos dando uma demonstração de que $\mathbb{C}$ é um corpo algebricamente fechado, usando os conceitos abordados.

A idéia da Teoria de Galois

A idéia da Teoria de Galois é associar a uma extensão de corpos $L|K$ o seu grupo de automorfismos $G(L|K)$. Quando a extensão de corpos é galoisiana, isto é, normal e separável, fica estabelecida uma correspondência biunívoca entre os corpos intermediários F de $L|K$ e os subgrupos $H = G(L|F)$ de $G(L|K)$, que reverte a inclusão.

Definição 1 (K-automorfismo)
Seja $L|K$ uma extensão de corpos. Um automorfismo $\varphi : L \longrightarrow L$ é um K-*automorfismo* se, e somente se, $\varphi(\alpha) = \alpha$, para todo $\alpha \in K$.

Equivalentemente, φ é um automorfismo de L tal que $\varphi|_K = I$.

Proposição 1
Seja $L|K$ uma extensão de corpos. Então,

$$G(L|K) = \{\varphi : L \longrightarrow L, \text{ automorfismo tal que } \varphi|_K = I\}$$

é um grupo com a operação de composição de funções.

Demonstração: Como a composição de bijeções é uma bijeção e a composição de homomorfismos é um homomorfismo, então a composição de automorfismos é um automorfismo. Se φ e ψ são K-automorfismos então, para todo $\alpha \in K$, temos $\varphi(\alpha) = \alpha$ e $\psi(\alpha) = \alpha$ e logo, $(\varphi \circ \psi)(\alpha) = \varphi(\psi(\alpha)) = \varphi(\alpha) = \alpha$, mostrando $\varphi \circ \psi \in G(L|K)$. Além disso, se $\varphi \in G(L|K)$, então φ^{-1} é um automorfismo de L tal que, para todo $\alpha \in K$,

$$\alpha = I(\alpha) = (\varphi^{-1}\varphi)(\alpha) = \varphi^{-1}(\varphi(\alpha)) = \varphi^{-1}(\alpha),$$

É claro que $I : L \longrightarrow L$ é um K–automorfismo de L.

mostrando que $\varphi^{-1} \in G(L|K)$. Portanto, $G(L|K)$ é um grupo. ■

Definição 2 (Grupo de Galois de L|K)
O *grupo de Galois de* $L|K$ é o grupo $G(L|K)$.

Exemplo 1
Consideremos a extensão $\mathbb{C}|\mathbb{R}$. Seja $\varphi : \mathbb{C} \longrightarrow \mathbb{C}$ um $\mathbb{R}$-automorfismo. Como $\{1, i\}$ é uma base de $\mathbb{C}|\mathbb{R}$, então cada $\alpha \in \mathbb{C}$ se escreve de uma única maneira como $\alpha = a + bi$ com $a, b \in \mathbb{R}$. Assim,

$$\varphi(\alpha) = \varphi(a + bi) = \varphi(a) + \varphi(b)\varphi(i) = a + b\varphi(i).$$

Portanto, φ está perfeitamente determinada por $\varphi(i)$. Como $-1 = i^2$ e $-1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2$, então $\varphi(i)$ também é raiz em $\mathbb{C}$ de $x^2 + 1 \in \mathbb{R}[x]$.

Portanto, $\varphi(i) = i$ ou $\varphi(i) = -i$. Temos dois $\mathbb{R}$-automorfismos, a saber, $I : \mathbb{C} \longrightarrow \mathbb{C}$, com $I(a+bi) = a+bi$, e $\varphi : \mathbb{C} \longrightarrow \mathbb{C}$, com $\varphi(a+bi) = a-bi$, a conjugação complexa. Nesse caso, $G(\mathbb{C}|\mathbb{R}) = \langle\varphi\rangle = \{I, \varphi;\ \varphi^2 = I\}$.

Verifique que a conjugação complexa é um $\mathbb{R}$-automorfismo de $\mathbb{C}$.

Exemplo 2

Seja $\alpha \in \mathbb{R}$ tal que $\alpha^3 = 2$. Consideremos a extensão $\mathbb{Q}(\alpha)|\mathbb{Q}$ e um $\mathbb{Q}$-automorfismo $\varphi : \mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\alpha)$. Como $\{1, \alpha, \alpha^2\}$ é uma base de $\mathbb{Q}(\alpha)|\mathbb{Q}$, todo elemento β de $\mathbb{Q}(\alpha)$ se escreve, de uma única maneira, como

$$\beta = a + b\alpha + c\alpha^2, \text{ com } a, b, c \in \mathbb{Q}.$$

Então,

$$\begin{aligned} \varphi(\beta) &= \varphi(a + b\alpha + c\alpha^2) \\ &= \varphi(a) + \varphi(b)\varphi(\alpha) + \varphi(c)\varphi(\alpha^2) \\ &= a + b\varphi(\alpha) + c\varphi(\alpha)^2. \end{aligned}$$

Assim, $\varphi(\beta)$ está perfeitamente determinada por $\varphi(\alpha)$.

Como $2 = \alpha^3$, então $2 = \varphi(2) = \varphi(\alpha)^3$, logo $\varphi(\alpha)$ também é uma raiz em $\mathbb{Q}(\alpha)$ de $x^3 - 2$. O único valor possível é $\varphi(\alpha) = \alpha$. Portanto, $\varphi = I$ e $G(\mathbb{Q}(\alpha)|\mathbb{Q}) = \{I\}$.

Lema 1

Seja $f(x) \in K[x]\backslash K$ e seja L um corpo de raízes de $f(x)$ sobre K. Se $\varphi : L \longrightarrow L$ é um K-automorfismo de L e α é uma raiz de $f(x)$, então $\varphi(\alpha)$ também é uma raiz de $f(x)$.

Demonstração: Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$.

Logo, $0 = a_0 + a_1\alpha + \cdots + a_n\alpha^n$. Aplicando φ, obtemos

$$\begin{aligned} 0 = \varphi(0) &= \varphi(a_0) + \varphi(a_1)\varphi(\alpha) + \cdots + \varphi(a_n)\varphi(\alpha)^n \\ &= a_0 + a_1\varphi(\alpha) + \cdots + a_n\varphi(\alpha)^n \\ &= f(\varphi(\alpha)) \ \blacksquare \end{aligned}$$

Definição 3 (Grupo de Galois de $f(x)$)

Seja $f(x) \in K[x]\backslash K$ e seja L um corpo de raízes de $f(x)$ sobre K. O *grupo de Galois de* $f(x)$ é $G(f(x)|K) = G(L|K)$.

Teorema 1

Se $f(x) \in K[x]\backslash K$ tem n raízes distintas em seu corpo de raízes L, então $G(L|K)$ é isomorfo a um subgrupo de S_n.

Demonstração: Seja $\mathcal{R} = \{\alpha_1, \ldots, \alpha_n\}$ o conjunto das n raízes de $f(x)$. Pelo Lema anterior, se $\varphi \in G(L|K)$, então $\varphi(\alpha_j)$ também é uma raiz de $f(x)$ e, como φ é injetora, $\varphi(\mathcal{R}) = \mathcal{R}$, isto é, φ permuta as raízes distintas de $f(x)$. Consideremos a função

$$\begin{array}{ccc} G(L|K) & \longrightarrow & S_{\mathcal{R}} \\ \varphi & \longmapsto & \varphi|_{\mathcal{R}} \end{array}$$

$S_{\mathcal{R}}$ é o grupo das bijeções de $\mathcal{R}$.

Facilmente, verificamos que essa função é um homomorfismo. Como

$$\begin{aligned} L = K(\alpha_1, \ldots, \alpha_n) &= K[\alpha_1, \ldots, \alpha_n] \\ &= \{h(\alpha_1, \ldots, \alpha_n),\ h(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]\}, \end{aligned}$$

Veja Exercício 10, item (c), da Secão 1, na Parte 1. Nesse caso, a adjunção é de um conjunto de elementos algébricos sobre K e $K[\mathcal{R}] = K(\mathcal{R})$.

então $\varphi \in G(L|K)$ está perfeitamente determinada por seus valores em $\mathcal{R}$. Logo, se $\varphi, \psi \in G(L|K)$ são tais que $\varphi|_{\mathcal{R}} = \psi|_{\mathcal{R}}$, então $\varphi = \psi$, mostrando que a função acima é injetora. Portanto, $G(L|K)$ é isomorfo a um subgrupo de $S_{\mathcal{R}} \simeq S_n$. ■

Teorema 2

Seja $f(x) \in K[x]\backslash K$ um polinômio separável. Seja L um corpo de raízes de $f(x)$ sobre K. Então, $|G(L|K)| = [L : K]$.

Demonstração: Mostraremos que $I : K \longrightarrow K$ tem $[L : K]$ extensões a L. A demonstração é por indução sobre $[L : K]$. Se $[L : K] = 1$, então $G(L|K) = \{I\}$ e o resultado é válido. Suponhamos que $[L : K] > 1$. Então, $f(x)$ tem algum fator irredutível $p(x) \in K[x]$ de grau $d > 1$. Fixemos $\alpha \in L$ uma raiz de $p(x)$. Como $f(x)$ é separável, então $p(x)$ tem d raízes distintas, todas em L. Assim, cada $\varphi \in G(L|K)$ é tal que $\beta = \varphi(\alpha) \in L$, também é uma raiz de $p(x)$. Há exatamente d K-isomorfismos $\varphi : K(\alpha) \longrightarrow K(\beta)$ extensões de $I : K \longrightarrow K$, um para cada β raiz de $p(x)$. Observamos que L é um corpo de raízes de $f(x)$ sobre $K(\alpha)$, assim como L é um corpo de raízes de $f(x)$ sobre $K(\beta)$. Pelo Teorema 4 da Seção 3, na Parte 1, cada $\varphi : K(\alpha) \longrightarrow K(\beta)$ admite extensão $\tilde{\varphi} : L \longrightarrow L$. Como $[L : K(\alpha)] = \frac{[L:K]}{[K(\alpha):K]} = \frac{[L:K]}{d} < [L : K]$, por hipótese de indução, há $[L : K(\alpha)] = \frac{[L:K]}{d}$ extensões de cada um dos d K-isomorfismo $\varphi : K(\alpha) \longrightarrow K(\beta)$. Portanto, há $[L : K]$ K-automorfismos de L. ■

Exemplo 3

Seja $f(x) = x^3 - 1 \in \mathbb{Q}[x]$. Já vimos que o corpo de decomposição de $f(x)$ sobre $\mathbb{Q}$ é $\mathbb{Q}(\omega)$, onde $\omega = \cos\frac{2\pi}{3} + i\,\mathrm{sen}\,\frac{2\pi}{3}$ e $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ e o polinômio mínimo de ω sobre $\mathbb{Q}$ é $x^2 + x + 1 = (x - \omega)(x - \omega^2)$.

Então, $G(\mathbb{Q}(\omega)|\mathbb{Q}) = \{I, \varphi\} = \langle\varphi\rangle$, onde $\varphi(\omega) = \omega^2$, é um grupo cíclico de ordem 2.

Exemplo 4
Seja $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. O seu corpo de raízes sobre $\mathbb{Q}$ é $\mathbb{Q}(\omega, \sqrt[3]{2})$ e $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6$. Pelo Teorema 1, como $f(x)$ tem 3 raízes distintas, $G(\mathbb{Q}(\omega, \sqrt[3]{2})|\mathbb{Q})$ é isomorfo a um subgrupo de S_3. Pelo Teorema anterior, $|G(\mathbb{Q}(\omega, \sqrt[3]{2})|\mathbb{Q})| = 6$. Portanto, $G(\mathbb{Q}(\omega, \sqrt[3]{2})|\mathbb{Q}) \simeq S_3$.

Exemplo 5
Seja $L = K(x)$, onde $K = \mathbb{Z}_p(x^p)$, p um natural primo. Então, L é corpo de decomposição sobre K de $f(y) = y^p - x^p \in K[y]$. O polinômio $f(y)$ é irredutível em $K[y]$ e não é separável. Observamos que $f(y) = (y - x)^p$ em $L[y]$. Nesse caso, $[L : K] = p$ e $G(L|K) = \{I\}$.

Definição 4 (Corpo intermediário)
Seja $L|K$ uma extensão de corpos. Chamamos um corpo F, tal que $K \subset F \subset L$ de um *corpo intermediário*.

Proposição 2
Sejam $L|K$ uma extensão de corpos e F um corpo intermediário. Então, $G(L|F)$ é um subgrupo de $G(L|K)$. Mais ainda, se F e F' são corpos intermediários e $F \subset F'$, então $G(L|F) \supset G(L|F')$.

Demonstração: Se $\varphi \in G(L|F)$, então φ é um automorfismo de L que fixa $F \supset K$, logo φ é K-automorfismo, mostrando que $G(L|F) \subset G(L|K)$. É claro que $G(L|F)$ é um subgrupo de $G(L|K)$. A afirmação $G(L|F) \supset G(L|F')$ é óbvia. ■

Um subconjunto não-vazio de um grupo é subgrupo se, e somente se, é um grupo com a mesma operação do grupo.

Lema 2
Seja $K \subset F \subset L$ uma cadeia de corpos, com $F|K$ corpo de decomposição sobre K de algum polinômio $f(x) \in K[x]\backslash K$. Se $\varphi \in G(L|K)$, então $\varphi|_F \in G(F|K)$.

Demonstração: É suficiente demonstrar que $\varphi(F) = F$. Sejam $\alpha_1, \ldots, \alpha_n$ as raízes distintas de $f(x)$ e $\varphi \in G(L|K)$. Então, $\varphi(f)(x) = f(x)$ e $\varphi(\alpha_i) = \alpha_j$ está em F, pois $F = K(\alpha_1, \ldots, \alpha_n)$, então $\varphi(F) = K(\varphi(\alpha_1), \ldots, \varphi(\alpha_n)) \subset F$. Como φ é $K-$linear e injetora, $[\varphi(F) : K] = [F : K]$, logo $\varphi(F) = F$. ■

Teorema 3
Seja $K \subset F \subset L$ uma cadeia de corpos, com $F|K$ corpo de decomposição sobre K de algum polinômio $f(x) \in K[x]\backslash K$, e seja $L|K$ corpo de decomposição sobre K de algum polinômio $g(x) \in K[x]\backslash K$. Então, $G(L|F)$ é um subgrupo normal de $G(L|K)$ e

$$G(L|K)/G(L|F) \simeq G(F|K).$$

Demonstração: Definimos $\psi : G(L|K) \longrightarrow G(F|K)$ por $\psi(\varphi) = \varphi|_F$. Pelo Lema anterior, ψ está bem definida. Verificamos facilmente que ψ é um homomorfismo de grupos, pois para quaisquer $\varphi, \sigma \in G(L|K)$, temos que $(\varphi \circ \sigma)|_F = \varphi|_F \circ \sigma|_F$. Núcleo$(\psi) = \{\varphi \in G(L|K) \ ; \ \varphi|_F = I\} = G(L|F)$. Portanto, $G(L|F)$ é um subgrupo normal de $G(L|K)$. Se $\tau \in G(F|K)$, pelo Teorema 4 da Seção 3, na Parte 1, τ se estende a um K-automorfismo de L, isto é, existe $\varphi \in G(L|K)$ tal que $\varphi|_F = \tau$, mostrando que ψ é sobrejetor. Pelo Teorema Fundamental dos homomorfismos de grupos, obtemos o isomorfismo de grupos $G(L|K)/G(L|F) \simeq G(F|K)$. ■

Proposição 3
Sejam $L|K$ uma extensão de corpos e $G = G(L|K)$. Para cada subgrupo H de G, definimos

$$L_H = \{x \in L \ ; \ \varphi(x) = x, \text{ para todo } \varphi \in H\}.$$

Então, L_H é um corpo intermediário de $L|K$. Mais ainda, se H e H' são subgrupos de G com $H \subset H'$, então $L_H \supset L_{H'}$.

Demonstração: Sejam $\alpha, \beta \in L_H$ e $\varphi \in H$. Então,

$\varphi(\alpha - \beta) = \varphi(\alpha) - \varphi(\beta) = \alpha - \beta$,

$\varphi(\alpha \cdot \beta) = \varphi(\alpha) \cdot \varphi(\beta) = \alpha \cdot \beta$,

$\varphi(\beta^{-1}) = \varphi(\beta)^{-1} = \beta^{-1}$, se $\beta \neq 0$,

para todo $\varphi \in H$, mostrando que L_H é um subcorpo de L. Como $H \subset G$, então $\varphi \in G$ e para todo $a \in K$, temos $\varphi(a) = a$, logo $K \subset L_H$. Portanto, L_H é um corpo intermediário de $L|K$.

Se $\alpha \in L$ é fixado por todos os elementos de H', então α é fixado por todos os elementos de qualquer subconjunto de H', em particular, α é fixado por todos os elementos de $H \subset H'$, logo $L_H \supset L_{H'}$. ■

O diagrama da esquerda ilustra a função φ que faz a correspondência entre os corpos intermediários F de $L|K$ e os subgrupos de $G(L|K)$. O diagrama da direita mostra a função ψ que faz a correspondência entre os subgrupos H de $G(L|K)$ e os corpos intermediários de $L|K$.

$$\begin{array}{ccc} L & & I \\ | & & | \\ F & \overset{\varphi}{\longmapsto} & H = G(L|F) \\ | & & | \\ K & & G = G(L|K) \end{array} \qquad\qquad \begin{array}{ccc} I & & L \\ | & & | \\ H & \overset{\psi}{\longmapsto} & L_H \\ | & & | \\ G = G(L|K) & & K \end{array}$$

Observações:

(1) Se $K \subset F \subset L$ e $H = G(L|F) = \varphi(F)$, então $F \subset L_{G(L|F)} = \psi(\varphi(F))$, pois cada elemento de F é fixado por cada automorfismo que fixa todo F.

(2) Se H é um subgrupo de $G(L|K)$, então $H \subset G(L|L_H) = \varphi(\psi(H))$, pois cada elemento de H fixa os elementos que são fixados por todos os elementos de H.

(3) As inclusões acima nem sempre são igualdades. No Exemplo 2, $G = G(\mathbb{Q}(\alpha)|\mathbb{Q}) = \{I\}$ e $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha) = L_G = \psi(\varphi(\mathbb{Q}))$.

(4) Seja $\mathcal{F}$ o conjunto dos corpos intermediários de $L|K$ e seja $\mathcal{H}$ o conjunto dos subgrupos de $G(L|K)$. As funções descritas acima são

$$\begin{array}{rcl} \varphi : \mathcal{F} & \longrightarrow & \mathcal{H} \\ F & \longmapsto & \varphi(F) = G(L|F) \end{array} \qquad \begin{array}{rcl} \psi : \mathcal{H} & \longrightarrow & \mathcal{F} \\ H & \longmapsto & \psi(H) = L_H \end{array}$$

e ambas revertem a inclusão.

Galois deu condições sobre $L|K$ para que essas funções sejam bijeções, inversas uma da outra, a saber, a separabilidade e a normalidade da extensão $L|K$, conforme veremos na próxima seção.

Exercícios

1. Determine $G(L|K)$:
   (a) $L = \mathbb{Q}(\sqrt[4]{2})$ e $K = \mathbb{Q}$;
   (b) $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ e $K = \mathbb{Q}$, onde $\omega = \cos\frac{2\pi}{3} + i\,\mathrm{sen}\,\frac{2\pi}{3}$;
   (c) $L = \mathbb{Q}(\omega)$ e $K = \mathbb{Q}$, onde $\omega = \cos\frac{2\pi}{5} + i\,\mathrm{sen}\,\frac{2\pi}{5}$.
   (d) $L = \mathbb{Q}(i)$ e $K = \mathbb{Q}$.
   (e) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ e $K = \mathbb{Q}$

2. Seja α algébrico sobre K e seja $\tau \in G(K(\alpha)|K)$. Mostre que $\tau(\alpha)$ tem o mesmo polinômio mínimo de α sobre K.

3. Diga quais das afirmações são falsas ou verdadeiras, justificando a sua resposta:
   (a) Todo K-automorfismo de L é um automorfismo de L.
   (b) Todo L-automorfismo é a identidade em L.
   (c) Se $G(L|K) = \{I\}$, então $L = K$.
   (d) Se $L = K$, então $G(L|K) = \{I\}$.

(e) $G(\mathbb{C}|\mathbb{R})$ é abeliano.

4. Seja $\sigma : \mathbb{R} \longrightarrow \mathbb{R}$ um automorfismo de corpos.

   (a) Mostre que $\sigma(1) = 1$.

   (b) Mostre que $\sigma(a) = a$, para todo $a \in \mathbb{Q}$.

   (c) Seja $a \in \mathbb{R}$ tal que $a > 0$. Mostre que $\sigma(a) > 0$.

   (d) Sejam $a, b \in \mathbb{R}$, tais que $a < b$. Mostre que $\sigma(a) < \sigma(b)$.

   (e) Mostre que $\sigma = I$.

EXTENSÃO
DE CORPOS

A conexão de Galois

Estamos próximos de obter o Teorema de Galois, que estabelece que as funções φ e ψ da Seção 1 são inversas uma da outra quando $L|K$ é uma extensão finita normal e separável. Para isto, precisamos mostrar que se H é um subgrupo de $G(L|K)$, então $\varphi(\psi(H)) = H$. Já sabemos que $H \subset G(L|L_H) = \varphi(\psi(H))$. Vamos mostrar H e $\varphi(\psi(H))$ são grupos finitos de mesma ordem, seguindo assim, a igualdade dos grupos.

Conjuntos infinitos de mesma cardinalidade, um contido no outro, podem ser diferentes, por exemplo $2\mathbb{Z} \subset \mathbb{Z}$ são ambos enumeráveis e $2\mathbb{Z} \subsetneq \mathbb{Z}$.

Vamos, primeiramente, determinar $[L_H : K]$ em termos de $|H|$ e depois $|G(L|L_H)|$ em termos de $[L_H : K]$.

Proposição 4 (Dedekind)
Sejam L um corpo e $\lambda_1, \ldots, \lambda_n$ automorfismos distintos de L. Então, o conjunto $\{\lambda_1, \ldots, \lambda_n\}$ é linearmente independente sobre L.

Demonstração: Suponhamos, por absurdo, que o conjunto acima seja linearmente dependente sobre L. Então, existem $a_1, \ldots, a_n \in L$, nem todos nulos, tais que

$$a_1\lambda_1(x) + a_2\lambda_2(x) + \cdots + a_n\lambda_n(x) = 0, \text{ para todo } x \in L.$$

Nesse caso, podemos encontrar uma relação que tem o menor número de coeficientes não-nulos e, reenumerando os automorfismos, podemos supor que

$$a_1\lambda_1(x) + a_2\lambda_2(x) + \cdots + a_m\lambda_m(x) = 0, \text{ para todo } x \in L, \qquad (\star)$$

com $a_1, \ldots, a_m$ não-nulos, seja a relação minimal.

Como
$\lambda_1(1_L) = \lambda_1(1_L \cdot 1_L) = \lambda_1(1_L) \cdot \lambda_1(1_L)$
e $\lambda_1(1_L) \neq \lambda_1(0_L) = 0_L$, cancelando $\lambda_1(1_L)$ obtemos $\lambda_1(1_L) = 1_L$.

Afirmamos que $m \geq 2$. De fato, se $m = 1$, então $\{\lambda_1\}$ é linearmente independente sobre L, pois se $0 = a_1\lambda_1(x)$, com $a_1 \in L$, para todo $x \in L$, como $\lambda_1(1_L) = 1_L$, então $0 = a_1\lambda(1_L) = a_1 \cdot 1_L = a_1$.

Podemos assumir que $m \geq 2$ e não haja equação do tipo $(\star)$ com menos de m coeficientes não-nulos.

Como $\lambda_1 \neq \lambda_m$, existe $y \in L$ tal que $\lambda_1(y) \neq \lambda_m(y)$. Substituindo x por yx em $(\star)$, obtemos:

$$a_1\lambda_1(y)\lambda_1(x) + a_2\lambda_2(y)\lambda_2(x) + \cdots + a_m\lambda_m(y)\lambda_m(x) = 0, \qquad (1)$$

para todo $x \in L$. Multiplicando a equação $(\star)$ por $\lambda_1(y)$, obtemos:

$$a_1\lambda_1(y)\lambda_1(x) + a_2\lambda_1(y)\lambda_2(x) + \cdots + a_m\lambda_1(y)\lambda_m(x) = 0, \qquad (2)$$

para todo $x \in L$. Subtraindo (2) de (1), temos:

$$a_2(\lambda_2(y) - \lambda_1(y))\lambda_2(x) + \cdots + a_m(\lambda_m(y) - \lambda_1(y))\lambda_m(x) = 0, \qquad (3)$$

para todo $x \in L$. O coeficiente de $\lambda_m(x)$ é $a_m(\lambda_m(y) - \lambda_1(y)) \neq 0$, então (3) é uma equação do tipo $(\star)$ com no máximo $m - 1 < m$ escalares não-nulos, contradizendo a hipótese acima.

Conseqüentemente, não há equação da forma $(\star)$ e o conjunto é linearmente independente sobre L. ■

Teorema 4

Seja G um subgrupo finito de um grupo de automorfismos de um corpo L e seja L_G o corpo fixo de G, isto é, $L_G = \{x \in L; \sigma(x) = x, \text{ para todo } \sigma \in G\}$. Então, $[L : L_G] = |G|$.

Demonstração: Seja $n = |G|$ e $G = \{I = \sigma_1, \ldots, \sigma_n\}$.

Suponhamos, primeiramente, que $[L : L_G] = m < n$. Seja $\{\alpha_1, \ldots, \alpha_m\}$ uma base de $L|L_G$. Seja A a matriz $m \times n$ com coeficientes em L definida por $A_{ij} = \sigma_j(\alpha_i)$. O sistema $AX = 0$ tem uma solução não-nula $(x_1, \ldots, x_n)$ em L^n, tal que

$$\sigma_1(\alpha_i)x_1 + \cdots + \sigma_n(\alpha_i)x_n = 0, \text{ para todo } i = 1, \ldots, m. \qquad (1)$$

Seja $\alpha \in L$.

Então, existem $a_1, \ldots, a_m \in L_G$, tais que $\alpha = a_1\alpha_1 + \cdots + a_m\alpha_m$. Assim,

$$\begin{aligned}
\sigma_1(\alpha)x_1 + \cdots + \sigma_n(\alpha)x_n &= \sigma_1\big(\textstyle\sum a_i\alpha_i\big)x_1 + \cdots + \sigma_n\big(\sum a_i\alpha_i\big)x_n \\
&= \big(\textstyle\sum a_i\sigma_1(\alpha_i)\big)x_1 + \cdots + \big(\sum a_i\sigma_n(\alpha_i)\big)x_n \\
&= \textstyle\sum \big(a_i\sigma_1(\alpha_i)x_1\big) + \cdots + \sum \big(a_i\sigma_n(\alpha_i)x_n\big) \\
&= \textstyle\sum a_i\big(\sigma_1(\alpha_i)x_1 + \cdots + \sigma_n(\alpha_i)x_n\big) \\
&= \textstyle\sum a_i \cdot 0 \\
&= 0,
\end{aligned}$$

A penúltima igualdade segue da equação (1).

para todo $\alpha \in L$, com $x_1, \ldots, x_n$ nem todos nulos.

Portanto, os automorfismos distintos $\sigma_1, \ldots, \sigma_n$ são linearmente dependentes sobre L, contradizendo a Proposição 4. Conseqüentemente, $m \geq n$.

Suponhamos que $[L : L_G] > n$. Então, existem $\alpha_1, \ldots, \alpha_{n+1}$ em L linearmente independentes sobre L_G. Consideremos a matriz $n \times (n+1)$ com coeficientes em L definida por $A_{ij} = \sigma_i(\alpha_j)$. Então, o sistema $AX = 0$ tem uma solução não-nula $(x_1, \ldots, x_{n+1}) \in L^{n+1}$ e

$$\sigma_i(\alpha_1)x_1 + \cdots + \sigma_i(\alpha_{n+1})x_{n+1} = 0, \text{ para todo } i = 1, \ldots, n. \qquad (2)$$

Entre todas as soluções não-nulas, escolhemos a relação com o menor número de coeficientes não-nulos, digamos $x_1, \ldots, x_r$ são não-nulos e $x_{r+1} = \cdots = x_{n+1} = 0$. Assim, a equação (2) se reescreve como

Caso necessário, reenumeramos os elementos da base de $L|L_G$.

$$\sigma_i(\alpha_1)x_1 + \cdots + \sigma_i(\alpha_r)x_r = 0, \text{ para todo } i = 1, \ldots, n. \qquad (3)$$

Seja $\sigma \in G$. Então, $\{\sigma \circ \sigma_1, \ldots, \sigma \circ \sigma_n\} = G$. Aplicando σ em (3), obtemos

A função
$G \longrightarrow G$
$\sigma_j \longmapsto \sigma \circ \sigma_j$
é um automorfismo do grupo G.

$$\sigma(\sigma_i(\alpha_1))\sigma(x_1) + \cdots + \sigma(\sigma_i(\alpha_r))\sigma(x_r) = 0, \text{ para todo } i = 1, \ldots, n. \qquad (4)$$

O sistema de equações lineares em (4) é equivalente ao sistema

$$\sigma_i(\alpha_1)\sigma(x_1) + \cdots + \sigma_i(\alpha_r)\sigma(x_r) = 0, \text{ para todo } i = 1, \ldots, n. \qquad (5)$$

Multiplicando a equação (3) por $\sigma(x_1)$ e multiplicando a equação (5) por x_1 temos, respectivamente,

$$\begin{cases} \sigma_i(\alpha_1)x_1\sigma(x_1) + \sigma_i(\alpha_2)x_2\sigma(x_1) + \cdots + \sigma_i(\alpha_r)x_r\sigma(x_1) = 0 \\ \sigma_i(\alpha_1)\sigma(x_1)x_1 + \sigma_i(\alpha_2)\sigma(x_2)x_1 + \cdots + \sigma_i(\alpha_r)\sigma(x_r)x_1 = 0, \end{cases}$$

para todo $i = 1, \ldots, n$.

Subtraindo, obtemos:

$$\sigma_i(\alpha_2)\big(x_2\sigma(x_1) - \sigma(x_2)x_1\big) + \cdots + \sigma_i(\alpha_r)\big(x_r\sigma(x_1) - \sigma(x_r)x_1\big) = 0,$$

para todo $i = 1, \ldots, n$.

Esse sistema de equações é do tipo (3) com menos termos não-nulos, o que é uma contradição, a não ser que os coeficientes

$$x_j\sigma(x_1) - \sigma(x_j)x_1 = 0, \text{ para todo } j = 1, \ldots, r.$$

Se isso ocorre, então $x_j\sigma(x_1) = \sigma(x_j)x_1$, logo $x_j{x_1}^{-1} = \sigma(x_j)\big(\sigma(x_1)\big)^{-1} = \sigma(x_j)\sigma({x_1}^{-1})$. Portanto,

$$x_j x_1^{-1} = \sigma(x_j x_1^{-1}), \text{ para todo } \sigma \in G \text{ e para todo } j = 1, \ldots, r.$$

Logo, $x_j x_1^{-1} \in L_G$. Assim, existem $\beta_1, \ldots, \beta_r \in L_G$ não-nulos e um elemento $x_1 \in L$ tais que $x_j = x_1\beta_j$, para todo $j = 1, \ldots, r$.

A equação (3), com $i = 1$, isto é, $\sigma_1 = I$ se torna:

$$\alpha_1 x_1 \beta_1 + \cdots + \alpha_r x_1 \beta_r = 0.$$

Como $x_1 \neq 0$, cancelando x_1, obtemos que $\{\alpha_1, \ldots, \alpha_r\}$ é linearmente dependente sobre L_G, uma contradição. Portanto, $[L : L_G] \leq n$.

Pela primeira etapa da demonstração, $[L : L_G] = n = |G|$. ■

Proposição 5
Sejam $L|K$ uma extensão finita e $G = G(L|K)$. Se H é um subgrupo de G, então

$$[L_H : K] = \frac{[L : K]}{|H|}.$$

Demonstração: Basta mostrarmos que $G = G(L|K)$ é finito. Assim, H também é finito e, pelo Teorema anterior, $[L : L_H] = |H|$. Logo,

$$[L_H : K] = \frac{[L : K]}{[L : L_H]} = \frac{[L : K]}{|H|}.$$

L
|
L_H
|
K

Vamos mostrar que $|G(L|K)| \leq [L : K]$. Seja $\{\alpha_1, \ldots, \alpha_m\}$ uma base de $L|K$. Suponhamos, por absurdo, que existam $\sigma_1, \ldots, \sigma_{m+1}$ K-automorfismos distintos de L. Seja A a matriz $m \times (m+1)$ com coeficientes em L definida por $A_{ij} = \sigma_j(\alpha_i)$. O sistema linear $AX = 0$ tem uma solução não-nula $(x_1, \ldots, x_{m+1}) \in L^{m+1}$, tal que

$$\sigma_1(\alpha_i)x_1 + \cdots + \sigma_{m+1}(\alpha_i)x_{m+1} = 0, \text{ para todo } i = 1, \ldots, m \qquad (1)$$

Seja $\alpha \in L$.

Então, existem $a_1, \ldots, a_m \in K$, tais que $\alpha = a_1\alpha_1 + \cdots + a_m\alpha_m$. Assim,

$$\begin{aligned}
\sigma_1(\alpha)x_1 + \cdots + \sigma_{m+1}(\alpha)x_{m+1} &= \sigma_1\big(\textstyle\sum a_i\alpha_i\big)x_1 + \cdots + \sigma_{m+1}\big(\sum a_i\alpha_i\big)x_{m+1} \\
&= \big(\textstyle\sum a_i\sigma_1(\alpha_i)\big)x_1 + \cdots + \big(\sum a_i\sigma_{m+1}(\alpha_i)\big)x_{m+1} \\
&= \big(\textstyle\sum a_i\sigma_1(\alpha_i)x_1\big) + \cdots + \big(\sum a_i\sigma_{m+1}(\alpha_i)x_{m+1}\big) \\
&= \textstyle\sum a_i\big(\sigma_1(\alpha_i)x_1 + \cdots + \sigma_{m+1}(\alpha_i)x_{m+1}\big) \\
&= \textstyle\sum a_i \cdot 0 \\
&= 0,
\end{aligned}$$

A penúltima igualdade segue da equação (1).

para todo $\alpha \in L$, com $x_1, \ldots, x_{m+1}$ nem todos nulos, contradizendo a Proposição 4.

Conseqüentemente, $|G(L|K)| \leq [L : K]$. ■

A discussão do Grupo de Galois de $f(x) \in K[x]$ começa com um corpo de decomposição L de $f(x)$ sobre K. Temos a cadeia de corpos

$$K \subset L_G \subset L.$$

A questão natural é: quando $L_G = K$?

Teorema 5
Seja $L|K$ uma extensão finita com $G = G(L|K)$. As seguintes condições são equivalentes:

(i) $L_G = K$;

(ii) cada polinômio irredutível $p(x) \in K[x]$ com uma raiz em L é separável e tem todas as raízes em L;

(iii) L é corpo de decomposição sobre K de algum polinômio separável $f(x) \in K[x]$.

Demonstração:

(i) $\Longrightarrow$ (ii): Seja $p(x) \in K[x]$ um polinômio mônico irredutível tendo uma raiz $\alpha \in L$. Como $K = L_G$, pelo Teorema anterior $|G| = [L : L_G] = [L : K]$. Consideremos os elementos distintos do conjunto finito $\{\sigma(\alpha)\ ;\ \sigma \in G\} \subset L$ sendo $\alpha = \alpha_1, \ldots, \alpha_n$. Definimos $g(x) \in L[x]$ por

$$g(x) = \prod_{j=1}^{n}(x - \alpha_j) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n, \text{ com}$$

$$\begin{aligned}
s_1 &= \alpha_1 + \cdots + \alpha_n \\
s_2 &= \sum_{1 \leq i < j \leq n} \alpha_i\alpha_j \\
&\vdots \\
s_j &= \sum_{1 \leq i_1 < \cdots < i_j \leq n} \alpha_{i_1} \cdots \alpha_{i_j} \\
&\vdots \\
s_n &= \alpha_1\alpha_2 \cdots \alpha_n
\end{aligned}$$

Cada $\sigma \in G$ permuta $\{\alpha_1, \ldots, \alpha_n\}$, logo fixa as suas funções simétricas elementares, isto é, $\sigma(s_j) = s_j$, para todo $j = 1, \ldots, n$. Como $L_G = K$,

então $g(x) \in K[x]$ e tem todas as raízes distintas. Os polinômios $p(x)$ e $g(x)$ têm α como raiz comum em L, temos que $\mathrm{mdc}_{L[x]}(p(x), g(x)) \neq 1$, então $\mathrm{mdc}_{K[x]}(p(x), g(x)) \neq 1$. Como $p(x)$ é irredutível em $K[x]$ segue que $\mathrm{mdc}_{K[x]}(p(x), g(x)) = p(x)$, logo $p(x)$ divide $g(x)$. Portanto, todas as raízes de $p(x)$ são distintas.

(ii) $\Longrightarrow$ (iii): Primeiramente, observamos que cada $\alpha \in L$ é algébrico sobre K, porque $L|K$ é uma extensão finita. Escolha $\alpha_1 \in L$ e seja $p_1(x) \in K[x]$ o polinômio mínimo de α_1 sobre K. Por hipótese, $p_1(x)$ tem todas as suas raízes em L e é separável. Seja $K_1 \subset L$ um corpo de decomposição de $p_1(x)$ sobre K. Se $K_1 = L$, estamos prontos. Caso contrário, escolha $\alpha_2 \in L$ tal que $\alpha_2 \notin K_1$. Seja $p_2(x) \in K[x]$ o polinômio mínimo de α_2 sobre K. Por hipótese, $p_2(x)$ é separável e tem todas as suas raízes em L. Consideremos $K_2 \subset L$ o corpo de decomposição do polinômio separável $p_1(x)p_2(x) \in K[x]$. Se $K_2 = L$, estamos prontos. Caso contrário, continuamos o processo, que tem que parar, em virtude de $[L : K]$ se finito.

(iii) $\Longrightarrow$ (i): Pelo Teorema 2, $|G(L|K)| = [L : K]$ e, pelo Teorema 4, temos que $|G(L|K)| = [L : L_G]$. Portanto, $[L : L_G] = [L : K]$. Como $K \subset L_G \subset L$, segue da multiplicatividade dos graus que $K = L_G$. ■

Definição 5 (Extensão galoisiana)
Uma extensão finita de corpos é dita *galoisiana* se, e somente se, tem uma das condições equivalentes do Teorema anterior.

Lema 3
Sejam $L|K$ uma extensão finita, F um corpo intermediário e $\sigma \in G(L|K)$. Então,

$$G(L|\sigma(F)) = \sigma G(L|F)\sigma^{-1}.$$

Demonstração: De fato, tome $\gamma \in G(L|F)$ e $\beta \in \sigma(F)$. Então, $\beta = \sigma(\alpha)$, para algum $\alpha \in F$ e

$$(\sigma\gamma\sigma^{-1})(\beta) = \sigma(\gamma(\sigma^{-1}(\beta))) = \sigma(\gamma(\alpha)) = \sigma(\alpha) = \beta.$$

É claro que $\sigma\gamma\sigma^{-1}$ é um automorfismo de L.

Logo, $\sigma\gamma\sigma^{-1} \in G(L|\sigma(F))$ e

$$\sigma G(L|F)\sigma^{-1} \subset G(L|\sigma(F)).$$

Analogamente, tomando $\tau \in G(L|\sigma(F))$ e $\alpha \in F$, então

$$(\sigma^{-1}\tau\sigma)(\alpha) = \sigma^{-1}(\tau(\sigma(\alpha))) = \sigma^{-1}(\sigma(\alpha)) = \alpha.$$

Logo, $\sigma^{-1}\gamma\sigma \in G(L|F)$ e

É claro que $\sigma^{-1}\gamma\sigma$ é um automorfismo de L.

$$\sigma^{-1}G(L|\sigma(F))\sigma \subset G(L|F),$$

portanto

$$\sigma G(L|F)\sigma^{-1} \supset G(L|\sigma(F)),$$

e o Lema está demonstrado. ■

Agora, finalmente, estamos prontos para o Teorema de Galois.

Teorema 6 (Teorema Fundamental da Teoria de Galois)
Sejam $L|K$ uma extensão finita normal e separável, com $[L : K] = n$, $G = G(L|K)$, $\mathcal{F} = \{F\ ;\ K \subset F \subset L \text{ e } F \text{ é corpo}\}$, $\mathcal{H} = \{H\ ;\ H \text{ é subgrupo de } G\}$. Consideremos

$$\begin{array}{rcl} \varphi : \mathcal{F} & \longrightarrow & \mathcal{H} \\ F & \longmapsto & \varphi(F) = G(L|F) \end{array} \quad \text{e} \quad \begin{array}{rcl} \psi : \mathcal{H} & \longrightarrow & \mathcal{F} \\ H & \longmapsto & \psi(H) = L_H \end{array}$$

Então,

L	{I}
|	|
$F = L_H$	$H = G(L\|F)$
|	|
K	$G = G(L\|K)$

(i) $|G| = n$.

(ii) φ e ψ revertem as inclusões, $\varphi \circ \psi = I_{\mathcal{H}}$ e $\psi \circ \varphi = I_{\mathcal{F}}$.

(iii) Seja F um corpo intermediário. Então,

$$[L : F] = |G(L|F)| \text{ e } [F : K] = \frac{|G|}{|G(L|F)|} = (G : G(L|F)).$$

(iv) Seja F um corpo intermediário. $F|K$ é normal se, e somente se, $G(L|F)$ é subgrupo normal de G. Nesse caso, $G(F|K)$ é isomorfo a $G/G(L|F)$.

Demonstração:

(i): Pelo Teorema 5, temos $K = L_G$. Pelo Teorema 4, obtemos $|G| = [L : L_G]$. Portanto, $|G| = [L : K] = n$.

(ii): Já sabemos que φ e ψ revertem as inclusões, $F \subset L_{G(L|F)} = \psi(\varphi(F))$, assim como $H \subset G(L|L_H) = \varphi(\psi(H))$.

Como $L|K$ é normal e separável, então $L|F$ é normal e separável e, pelo Teorema 5,

Fez o Exercício 3 da Seção 4, na Parte 1?

$$L_{G(L|F)} = F, \quad (1)$$

isto é, $\psi \circ \varphi = I_{\mathcal{F}}$.

Seja agora H um subgrupo de $G = G(L|K)$. Então, pela equação (1) $L_{G(L|L_H)} = L_H$. Pelo Teorema 4, temos que

$$|H| = [L : L_H].$$

Portanto,

$$|H| = [L : L_H] = [L : L_{G(L|L_H)}].$$

Pelo Teorema 4,

$$[L : L_{G(L|L_H)}] = |G(L|L_H)|.$$

Logo,

$$|H| = |G(L|L_H)|.$$

Como $H \subset G(L|L_H)$ e esses grupos são finitos, obtemos que $H = G(L|L_H) = \varphi(\psi(H))$, que é equivalente a, $\varphi \circ \psi = I_{\mathcal{H}}$.

(iii) Seja F um corpo intermediário. Então, $L|F$ é normal e separável e $F = L_{G(L|F)}$. Então, $[L : F] = |G(L|F)|$ seguindo, imediatamente, a igualdade $[F : K] = \dfrac{[L : K]}{[L : F]} = \dfrac{|G(L|K)|}{|G(L|F)|}$.

(iv)

($\Longrightarrow$:) Segue do Teorema 3.

($\Longleftarrow$:) Reciprocamente, suponhamos que $H = G(L|F) \lhd G(L|K)$. Então, $\sigma G(L|F)\sigma^{-1} = G(L|F)$, para cada $\sigma \in G(L|K)$. Pelo Lema anterior, para cada $\sigma \in G(L|K)$, $\sigma G(L|F)\sigma^{-1} = G(L|\sigma(F))$. Logo, $G(L|\sigma(F)) = G(L|F)$, para cada $\sigma \in G(L|K)$. Pelo item (ii), $\sigma(F) = L_{G(L|\sigma(F))} = L_{G(L|F)} = F$, para cada $\sigma \in G(L|K)$. Portanto $\sigma|_F$ é um K-automorfismo de F, para cada $\sigma \in G(L|K)$.

Seja agora $\alpha \in F$ e $p(x) \in K[x]$ o polinômio mínimo de α sobre K. Então, $p(x)$ é separável e tem todas as suas raízes em L. Se $\beta \in L$ é outra raiz de $p(x)$, então existe $\sigma \in G(L|K)$ tal que $\sigma(\alpha) = \beta$. Logo, $\beta \in F$. Pelo Teorema 5, isto é equivalente a $F|K$ ser corpo de decomposição de um polinômio separável sobre K. Portanto, $F|K$ é normal.

Pelo Proposição 10 e seu Corolário, na Seção 3 da Parte 1, $K(\alpha)$ e $K(\beta)$ são K-isomorfos, com um isomorfismo σ tal que $\sigma(\alpha) = \beta$, e σ admite extensão a L.

Os seguintes diagramas ilustram a correspondência de Galois.

$$\begin{array}{ccc} L & & I \\ | & & | \\ F & \overset{\varphi}{\longmapsto} & H = G(L|F) \\ | & & | \\ K & & G = G(L|K) \end{array} \qquad \begin{array}{ccc} I & & L \\ | & & | \\ H & \overset{\psi}{\longmapsto} & F = L_H \\ | & & | \\ G = G(L|K) & & K \end{array}$$

Exemplo 6

Seja $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. L é corpo de decomposição sobre $\mathbb{Q}$ do polinômio $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$, portanto $L|\mathbb{Q}$ é galoisiana.

As extensões algébricas dos racionais são separáveis.

Como $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, então $|G(L|\mathbb{Q})| = 4$. Cada $\sigma \in G(L|Q)$ é tal que $\sigma|_{\mathbb{Q}(\sqrt{2})} \in G(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$, pois $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ é normal sobre $\mathbb{Q}$. Logo, $\sigma(\sqrt{2}) = \sqrt{2}$ ou $\sigma(\sqrt{2}) = -\sqrt{2}$. Também, $\sigma|_{\mathbb{Q}(\sqrt{3})} \in G(\mathbb{Q}(\sqrt{3})|\mathbb{Q})$, pois $\mathbb{Q}(\sqrt{3})|\mathbb{Q}$ é normal sobre $\mathbb{Q}$. Logo, $\sigma(\sqrt{3}) = \sqrt{3}$ ou $\sigma(\sqrt{3}) = -\sqrt{3}$.

Os $\mathbb{Q}$-automorfismos de L são:

$$I: \begin{array}{l} \sqrt{2} \longmapsto \sqrt{2} \\ \sqrt{3} \longmapsto \sqrt{3} \end{array} \qquad \varphi: \begin{array}{l} \sqrt{2} \longmapsto -\sqrt{2} \\ \sqrt{3} \longmapsto \sqrt{3} \end{array}$$

$$\psi: \begin{array}{l} \sqrt{2} \longmapsto \sqrt{2} \\ \sqrt{3} \longmapsto -\sqrt{3} \end{array} \qquad \varphi \circ \psi: \begin{array}{l} \sqrt{2} \longmapsto -\sqrt{2} \\ \sqrt{3} \longmapsto -\sqrt{3} \end{array}$$

Observamos que $\varphi^2 = I$, $\psi^2 = I$ e $\psi \circ \varphi = \varphi \circ \psi$. Logo, $G(L|\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Os corpos intermediários não-triviais de $L|\mathbb{Q}$ são $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{6})$, corpos fixos dos subgrupos não-triviais de $G(L|K)$, respectivamente, $H_1 = \langle\varphi\rangle$, $H_2 = \langle\psi\rangle$, $H_3 = \langle\varphi \circ \psi\rangle$.

Verifique!

Exemplo 7

Seja $L = \mathbb{Q}(\omega, \sqrt[3]{2})$, onde $\omega = \cos\frac{2\pi}{3} + i\,\mathrm{sen}\,\frac{2\pi}{3}$. L é normal sobre $\mathbb{Q}$, pois é corpo de decomposição sobre $\mathbb{Q}$ de $f(x) = x^3 - 2$. Logo, $L|\mathbb{Q}$ é galoisiana. Já observamos que $G(L|\mathbb{Q}) \simeq S_3$. O polinômio mínimo de ω sobre $\mathbb{Q}$ é x^2+x+1 e suas raízes são ω e ω^2. Logo, se $\sigma \in G(L|K)$, então $\sigma(\omega) \in \{\omega, \omega^2\}$ e $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$. Observamos que $\mathbb{Q}(\omega)|\mathbb{Q}$ é galoisiana e, para todo $\sigma \in G(L|\mathbb{Q})$, $\sigma|_{\mathbb{Q}(\omega)} \in G(\mathbb{Q}(\omega)|\mathbb{Q})$.

Os $\mathbb{Q}$-automorfismos de L são:

$$I: \begin{array}{l} \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \omega \longmapsto \omega \end{array} \qquad \tau: \begin{array}{l} \sqrt[3]{2} \longmapsto \omega\sqrt[3]{2} \\ \omega \longmapsto \omega \end{array}$$

Verifique que $\tau^3 = I$, $\sigma^2 = I$, $\tau \circ \sigma = \sigma \circ \tau^2$, $(\sigma \circ \tau)^2 = I$ e $(\sigma \circ \tau^2)^2 = I$.

$$\tau^2: \begin{array}{l} \sqrt[3]{2} \longmapsto \omega^2\sqrt[3]{2} \\ \omega \longmapsto \omega \end{array} \qquad \sigma: \begin{array}{l} \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \omega \longmapsto \omega^2 \end{array}$$

$$\sigma\circ\tau^2:\ \sqrt[3]{2}\ \longmapsto\ \omega\sqrt[3]{2} \qquad \sigma\circ\tau:\ \sqrt[3]{2}\ \longmapsto\ \omega^2\sqrt[3]{2}$$
$$\omega\ \longmapsto\ \omega^2 \qquad\qquad \omega\ \longmapsto\ \omega^2$$

Os subgrupos não-triviais de S_3 são $H_1=\langle\tau\rangle$, $H_2=\langle\sigma\rangle$, $H_3=\langle\sigma\circ\tau\rangle$ e $H_4=\langle\sigma\circ\tau^2\rangle$.

Use a correspondência de Galois para verificar a afirmação ao lado.

Os corpos intermediários não-triviais de $\mathbb{Q}(\omega,\sqrt[3]{2})|\mathbb{Q}$ são $\mathbb{Q}(\omega)$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\omega\sqrt[3]{2})$ e $\mathbb{Q}(\omega^2\sqrt[3]{2})$, respectivamente, os corpos fixos de H_1, H_2, H_3 e H_4.

Finalizamos essa Seção com a determinação do grau e do grupo de Galois de uma extensão galoisiana $L|\mathbb{Q}$ muito importante.

Seja $n\geq 1$ um natural. O polinômio $x^n-1\in\mathbb{Q}[x]$ se decompõe em $\mathbb{C}[x]$ como

$$x^n-1=(x-1)(x-\omega)\cdots(x-\omega^{n-1}),$$

onde $\omega=\cos\frac{2\pi}{n}+i\,\mathrm{sen}\,\frac{2\pi}{n}$.

$\mathbb{Q}(\omega)$ é corpo de decomposição sobre $\mathbb{Q}$ de $x^n-1\in\mathbb{Q}[x]$.

Nosso objetivo é responder às questões:

(1) Qual o grau $[\mathbb{Q}(\omega):\mathbb{Q}]$?

(2) Quem é o grupo de Galois $G(\mathbb{Q}(\omega)|\mathbb{Q})$?

A resposta para a primeira questão é $\phi(n)$, onde ϕ é a função de Euler e para respondê-la vamos determinar o polinômio mínimo de ω sobre $\mathbb{Q}$.

A resposta para a segunda questão é ${\mathbb{Z}_n}^\star$. Precisamos construir o grupo de $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\omega)|\mathbb{Q}$.

Vamos denotar por $U_n(\mathbb{C})$ o conjunto das raízes complexas n-ésimas da unidade.

$U_n(\mathbb{C})=\{1,\omega,\ldots,\omega^{n-1}\}$ é um grupo cíclico de ordem n gerado por ω.

Qualquer gerador do grupo $U_n(\mathbb{C})$ é chamado de *raiz primitiva* n-*ésima da unidade*. Pelo Teorema de estrutura dos grupos cíclicos finitos, as raízes primitivas n-ésimas da unidade são ω^j, onde $1\leq j<n$ e $\mathrm{mdc}(n,j)=1$.

Definição 6 (n-ésimo polinômio ciclotômico)
Definimos o n-*ésimo polinômio ciclotômico* por

$$\phi_n(x)=\prod_{\substack{1\leq j<n\\ \mathrm{mdc}(n,j)=1}}(x-\omega^j),\quad \text{onde } \omega=\cos\tfrac{2\pi}{n}+i\,\mathrm{sen}\,\tfrac{2\pi}{n}.$$

Observamos que

$$\begin{aligned}\text{grau}(\phi_n(x)) &= \sharp\{\, j \,;\, 1 \le j < n,\ \text{mdc}(j,n) = 1\,\} \\ &= \phi(n),\ \text{onde } \phi \text{ é a função de Euler.}\end{aligned}$$

Também é claro que $\phi_n(x)$ é polinômio mônico.

Exemplo 8

Sabemos que se p é primo, então $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$, $x^{p-1}+\cdots+x+1$ é irredutível em $\mathbb{Q}[x]$ e é o polinômio mínimo de $\omega, \ldots, \omega^{p-1}$, as $p-1$ raízes primitivas p-ésimas da unidade. Nesse caso,

$$\begin{aligned}&[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1 \text{ e} \\ &\phi_p(x) = (x-\omega)\cdots(x-\omega^{p-1}) = x^{p-1} + \cdots + x + 1.\end{aligned}$$

Além disso, $\phi_1(x)\phi_p(x) = x^p - 1$.

O Lema a seguir generaliza a fórmula obtida no Exemplo acima.

Lema 4

$$x^n - 1 = \prod_{\substack{d|n \\ d \ge 1}} \phi_d(x).$$

Demonstração: Seja $d \ge 1$ um natural. Vamos denotar por E_d os elementos de ordem d do grupo $U_n(\mathbb{C})$, a saber,

$$E_d = \{\xi \in U_n(\mathbb{C}) \,;\, \circ(\xi) = d\}.$$

$E_d \neq \emptyset$ se, e somente se, d divide n. Nesse caso, $\omega^{\frac{n}{d}} \in E_d$.

Mais ainda, se $\xi \in E_d$, então $\xi^d = 1$, isto é, ξ é raiz de $x^d - 1$. Há $\phi(d)$ elementos em E_d, isto é, $\sharp E_d = \phi(d)$.

De $U_n(\mathbb{C}) = \bigcup_{\substack{d|n \\ 1 \le d \le n}} E_d$, onde a união é disjunta, obtemos:

$$\begin{aligned}x^n - 1 = \prod_{\xi \in U_n(\mathbb{C})} (x - \xi) &= \prod_{\substack{d|n \\ 1 \le d \le n}} \left(\prod_{\xi \in E_d} (x - \xi) \right) \\ &= \prod_{\substack{d|n \\ 1 \le d \le n}} \phi_d(x). \quad \blacksquare\end{aligned}$$

Corolário 1

$$n = \sum_{\substack{d|n \\ d \ge 1}} \phi(d), \text{ onde } \phi \text{ é a função de Euler.}$$

Demonstração: É imediata, a partir da igualdade dos polinômios no Lema anterior.

Proposição 6

O n-ésimo polinômio ciclotômico $\phi_n(x)$ tem as seguintes propriedades:

(i) $\phi_n(x) \in \mathbb{Z}[x]$.

(ii) $\phi_n(x)$ é irredutível em $\mathbb{Q}[x]$.

Demonstração:

(i) Indução sobre n. Se $n = 1$, então $\phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Seja $n > 1$ e suponhamos que o resultado seja válido para k com $1 \leq k < n$. Então,

$$x^n - 1 = \prod_{\substack{d|n \\ 1 \leq d \leq n}} \phi_d(x) = \left(\prod_{\substack{d|n \\ d < n}} \phi_d(x) \right) \phi_n(x) = f(x)\phi_n(x).$$

Por hipótese de indução, $f(x) = \prod_{\substack{d|n \\ 1 \leq d < n}} \phi_d(x) \in \mathbb{Z}[x]$.

Como $f(x)$ é mônico, a divisão euclidiana de $x^n - 1$ por $f(x)$ vale em $\mathbb{Z}[x]$. Assim, $x^n - 1 = f(x)q(x) + r(x)$, onde $r(x), q(x) \in \mathbb{Z}[x]$ com $r(x) = 0$ ou $0 \leq \text{grau}(r(x)) < \text{grau}(f(x))$.

Pela unicidade do quociente e do resto em $\mathbb{Q}[x]$, temos $q(x) = \phi_n(x)$ e $r(x) = 0$. Portanto, $\phi_n(x) \in \mathbb{Z}[x]$.

(ii) Seja $\xi \in \mathbb{C}$ uma raiz primitiva n-ésima da unidade e $p(x) \in \mathbb{Q}[x]$ o seu polinômio mínimo. Vamos mostrar que $p(x) = \phi_n(x)$.

Primeiramente, $p(x)$ é mônico e $p(x)$ divide $\phi_n(x)$ em $\mathbb{Q}[x]$. Como $\phi_n(x) \in \mathbb{Z}[x]$ e $p(x)$ é mônico, pelo Lema de Gauss, $p(x)$ divide $\phi_n(x)$ em $\mathbb{Z}[x]$. Logo,

$\phi_n(x) = p(x)f(x)$, com $p(x), f(x) \in \mathbb{Z}[x]$.

Seja agora p um natural primo tal que p não divide n.

Então, $\text{mdc}(p, n) = 1$ e ξ^p também é uma raiz primitiva n-ésima da unidade. Tomamos $q(x)$, o polinômio mínimo de ξ^p sobre $\mathbb{Q}$. Temos que:

$q(x)$ divide $\phi_n(x)$ em $\mathbb{Z}[x]$ e

$q(x^p)$ tem ξ como raiz.

Assim, $q(x^p) = p(x)h(x)$, para algum polinômio $h(x) \in \mathbb{Z}[x]$. Passando módulo p, temos:

$$q(x^p) \equiv p(x)h(x) \mod p. \qquad (\star)$$

Escrevendo $q(x) = \sum a_j x^j, a_j \in \mathbb{Z}$, como $a^p \equiv a \mod p$, para todo $a \in \mathbb{Z}$, vemos que

$$\begin{aligned} g(x^p) &= \sum a_j (x^p)^j \\ &= \sum a_j (x^j)^p \\ &\equiv \sum {a_j}^p x^{jp} \mod p \\ &\equiv \sum (a_j x^j)^p \mod p \\ &\equiv \left(\sum a_j x^j\right)^p \mod p \\ &= (q(x))^p \mod p \end{aligned}$$

$a^p \equiv a \mod p$, para todo $a \in \mathbb{Z}$ e
$(a+b)^p \equiv a^p + b^p \mod p$, para todo $a, b \in \mathbb{Z}[x]$.

Portanto, a relação $(\star)$ é equivalente a $(\overline{q}(x))^p = \overline{p}(x)\overline{h}(x)$ em $\mathbb{Z}_p[x]$.

Logo, $\overline{p}(x)$ divide $\overline{q}(x)^p$ e $\overline{p}(x)$ e $\overline{q}(x)$ têm raiz comum em algum corpo de decomposição sobre $\mathbb{Z}_p$ de $\overline{p}(x)\overline{h}(x)$.

Também, $p(x)$ divide $x^n - 1$ em $\mathbb{Q}[x]$ e pelo Lema de Gauss existe $g(x)$ em $\mathbb{Z}[x]$ tal que $x^n - 1 = p(x)g(x)$, com $g(x) \in \mathbb{Z}[x]$. Como $x^n - \overline{1} = \overline{p}(x)\overline{g}(x)$ e $p \nmid n$, então $(x^n - \overline{1})' = \overline{n}x^{n-1}$ só tem $\overline{0}$ como raiz, que não é raiz de $x^n - \overline{1}$, logo todas as raízes de $x^n - \overline{1}$ são simples. Portanto, $\overline{q}(x)$ não divide $\overline{g}(x)$. Também, $\overline{q}(x)$ não divide $\overline{f}(x)$.

$\phi_n(x) = p(x)f(x)$ e $q(x)$ divide $\phi_n(x)$.

Logo, $q(x)$ não divide $f(x)$. Entretanto, $q(x)$ divide $\phi_n(x) = p(x)f(x)$ e $q(x)$ é irredutível em $\mathbb{Q}[x]$. Portanto, $q(x)$ divide $p(x)$. Como $p(x)$ também é mônico e irredutível em $\mathbb{Q}[x]$, obtemos que $q(x) = p(x)$ e $p(\xi^p) = q(\xi^p) = 0$.

Moral da história: para todo q primo tal que $q \nmid n$, temos que $(\xi^p)^q$ é uma raiz primitiva n-ésima da unidade e, pelo mesmo argumento, $p(\xi^{pq}) = 0$. Por indução, se $\mathrm{mdc}(m, n) = 1$ e $1 \leq m < n$, então $p(\xi^m) = 0$ e $p(x)$ tem $\phi(n)$ raízes, com $\mathrm{grau}(p(x)) \leq \phi(n)$, pois $p(x)$ divide $\phi_n(x)$. Portanto, $\mathrm{grau}(p(x)) = \phi(n)$ e $p(x) = \phi_n(x)$. Concluímos então que $\phi_n(x)$ é irredutível em $\mathbb{Q}[x]$. ■

m se escreve como um produto de potências de primos que não dividem n.

Corolário 2

Se ξ é uma raiz complexa primitiva n-ésima da unidade, então temos que $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n)$ e $G(\mathbb{Q}(\xi)|\mathbb{Q}) \simeq {\mathbb{Z}_n}^*$.

Demonstração: A primeira afirmação segue do fato de $\phi_n(x)$ ser o polinômio mínimo de ξ sobre $\mathbb{Q}$ e $\mathrm{grau}(\phi_n(x)) = \phi(n)$. Para a segunda afirmação, seja $\sigma \in G(\mathbb{Q}(\xi)|\mathbb{Q})$. Então, $\sigma(\xi) = \xi^j$, para algum $j \in \mathbb{Z}$ tal que $\mathrm{mdc}(j, n) = 1$.

Como $\xi^n = 1$, escrevendo $j = qn + r$ onde $1 \leq r < n$, temos que $\xi^j = \xi^{qn+r} = (\xi^n)^q \xi^r = \xi^r$ e a potência ξ^j só depende do resto que j deixa na divisão por n. Portanto, existe um único j tal que $1 \leq j < n$ com $\mathrm{mdc}(j, n) = 1$ tal que $\sigma(\xi) = \xi^j$. Definimos

$\mathrm{mdc}(j, n) = \mathrm{mdc}(j - qn, n)$
$= \mathrm{mdc}(r, n)$.

$\psi : G(\mathbb{Q}(\xi)|\mathbb{Q}) \longrightarrow \mathbb{Z}_n{}^*$ por $\psi(\sigma) = j \mod n$, onde $\sigma(\xi) = \xi^j$.

É fácil verificar que ψ é um homomorfismo de grupos injetor. Logo, $G(\mathbb{Q}(\xi)|\mathbb{Q})$ é isomorfo a um subgrupo de $\mathbb{Z}_n{}^*$. Como

A extensão $\mathbb{Q}(\xi)|\mathbb{Q}$ é galoisiana.

$$|G(\mathbb{Q}(\xi)|\mathbb{Q})| = [\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n) = |\mathbb{Z}_n{}^*|,$$

então $G(\mathbb{Q}(\xi)|\mathbb{Q}) \simeq \mathbb{Z}_n{}^*$. ■

A fórmula do Lema anterior, permite calcular $\phi_n(x)$ indutivamente.

$\phi_1(x) = x - 1$, $\phi_2(x) = x + 1$.

$x^3 - 1 = \phi_1(x)\phi_3(x) \Longrightarrow \phi_3(x) = \dfrac{x^3 - 1}{x - 1} = x^2 + x + 1.$

As raízes complexas primitivas quartas da unidade são i e $-i$.

$x^4 - 1 = \phi_1(x)\phi_2(x)\phi_4(x) = (x^2 - 1)\phi_4(x) \Longrightarrow \phi_4(x) = \dfrac{x^4 - 1}{x^2 - 1} = x^2 + 1$

$$\begin{aligned} x^6 - 1 &= \phi_1(x)\phi_2(x)\phi_3(x)\phi_6(x) \\ &= (\phi_1(x)\phi_3(x))\phi_2(x)\phi_6(x) \\ &= (x^3 - 1)(x + 1)\phi_6(x) \end{aligned}$$

Então, $\phi_6(x) = \dfrac{x^6 - 1}{(x^3 - 1)(x + 1)} = \dfrac{x^3 + 1}{x + 1} = x^2 - x + 1.$

$$\begin{aligned} x^8 - 1 &= \phi_1(x)\phi_2(x)\phi_4(x)\phi_8(x) \\ &= (x^4 - 1)\phi_8(x) \end{aligned}$$

Então, $\phi_8(x) = \dfrac{x^8 - 1}{(x^4 - 1)} = x^4 + 1.$

Exercícios

1. Sejam $f(x) \in \mathbb{Q}[x]$ e L o corpo de raízes de $f(x)$ sobre $\mathbb{Q}$.

   Determine L e $[L : \mathbb{Q}]$.

   (a) $f(x) = x^7 - 1$ (b) $f(x) = x^3 - 3$ (c) $f(x) = x^4 + 1$
   (d) $f(x) = x^6 + 1$ (e) $f(x) = x^4 - 3$ (f) $f(x) = (x^2 + 1)(x^2 - 5)$

2. Para cada L do exercício anterior, determine $G = G(L|\mathbb{Q})$, a rede de subgrupos de G e todos os corpos intermediários de $L|\mathbb{Q}$.

3. Sejam p e q primos e $f(x) = x^p - q$.

   Determine L, o corpo de raízes de $f(x)$ sobre $\mathbb{Q}$, e $[L : \mathbb{Q}]$.

4. Mostre que $G(L|\mathbb{Q})$ é isomorfo a $\mathbb{Z}_4$, onde $L = \mathbb{Q}\left(\sqrt{2 + \sqrt{2}}\right)$.

5. Determine $G(f(x)|K)$:

   (a) $f(x) = x^4 + 2$ e $K = \mathbb{Q}$.

   (b) $f(x) = x^4 + 2$ e $K = \mathbb{Q}(i)$.

   (c) $f(x) = x^4 + 4x^2 + 2$ e $K = \mathbb{Q}$.

   (d) $f(x) = x^4 - 2$ e $K = \mathbb{Q}(\sqrt{2})$.

6. Sejam F e K subcorpos de $\mathbb{C}$. O compósito de F e K, denotado por $F \cdot K$ é o menor subcorpo de $\mathbb{C}$ que contém F e K.

   Determine o compósito de F e K e $[F \cdot K : \mathbb{Q}]$:

   (a) $F = \mathbb{Q}(\sqrt{2})$ e $K = \mathbb{Q}(\sqrt{3})$

   (b) $F = \mathbb{Q}(i)$ e $K = \mathbb{Q}(\sqrt[4]{2})$

   (c) $F = \mathbb{Q}(\sqrt{2}, i)$ e $K = \mathbb{Q}(\sqrt[4]{2})$

7. Sejam F e K subcorpos de $\mathbb{C}$, tais que $[F : \mathbb{Q}] = 7$ e $[K : \mathbb{Q}] = 11$. Considere $F \cdot K$, o compósito de F e K.

   (a) Determine $[F \cdot K : \mathbb{Q}]$.

   (b) Mostre que $F \cdot K|\mathbb{Q}$ é normal se, e somente se, $F|\mathbb{Q}$ e $K|\mathbb{Q}$ são normais.

   (c) No caso em que $F \cdot K|\mathbb{Q}$ é normal, determine os corpos intermediários dessa extensão.

8. Seja L o corpo de raízes de $x^5 - 2$ sobre $\mathbb{Q}$.

   (a) Mostre que $|G(L|\mathbb{Q})| = 20$.

   (b) Mostre que existe um único subcorpo F de $L|\mathbb{Q}$ tal que $[F : \mathbb{Q}] = 4$. Conclua que $F|\mathbb{Q}$ é normal.

   (c) Quantos subgrupos de ordem 4 tem $G(L|\mathbb{Q})$?

   (d) Verifique que $L|\mathbb{Q}$ admite subextensões quadráticas.

9. Seja $\omega \in \mathbb{C}$ tal que $\omega^7 = 1$ e $\omega \neq 1$.

   (a) Mostre que $\mathbb{Q}(\omega)$ admite um único subcorpo de grau 2 sobre $\mathbb{Q}$ e que este corpo é $\mathbb{Q}(i\sqrt{7})$.

   (b) Mostre que $\mathbb{Q}(\omega)$ admite um único subcorpo F com $[F : \mathbb{Q}] = 3$ e que F é corpo de raízes de $x^3 + x^2 - 2x - 1$ sobre $\mathbb{Q}$.

(c) Explicite na forma $a_0 + a_1\omega + \cdots + a_5\omega^5$, com $a_j \in \mathbb{Q}$, para $j = 0, \ldots, 5$, as raízes de $x^3 + x^2 - 2x - 1$.

10. Determine a estrutura de $G(f(x)|\mathbb{Q})$ (isto é, se é cíclico ou não, se é abeliano ou não) e descreva tais grupos por meio de geradores e relações, exibindo a ação dos geradores nas raízes do polinômio $f(x)$:

    (a) $f(x) = x^9 - 1$ (b) $f(x) = x^{36} - 1$ (c) $f(x) = x^7 - 2$

11. Seja L o corpo de raízes do 9-ésimo polinômio ciclotômico.

    Determine:

    (a) $[L : \mathbb{Q}]$.

    (b) $G(L|\mathbb{Q})$ e todos os seus subgrupos.

    (c) Todos os corpos intermediários de $L|\mathbb{Q}$.

12. Seja L o corpo de raízes do 10-ésimo polinômio ciclotômico.

    Determine:

    (a) $[L : \mathbb{Q}]$.

    (b) $G(L|\mathbb{Q})$ e todos os seus subgrupos.

    (c) Todos os corpos intermediários de $L|\mathbb{Q}$.

13. Seja L o corpo de raízes do 12-ésimo polinômio ciclotômico.

    Determine:

    (a) $[L : \mathbb{Q}]$.

    (b) $G(L|\mathbb{Q})$ e todos os seus subgrupos.

    (c) Todos os corpos intermediários de $L|\mathbb{Q}$.

    (d) Interprete $G(L|\mathbb{Q})$ como um subgrupo de S_4.

A equação geral de grau n

Resolvemos equações do 2º, 3º e 4º graus escrevendo as raízes da equação como radicais de funções algébricas racionais dos coeficientes da equação. Para a equação geral de grau $n \geq 5$ não há fórmulas explícitas. Por quê?

Vamos relacionar a solubilidade da equação por radicais com propriedade do grupo de automorfismos do seu corpo de raízes.

Dado $f(x) \in K[x] \backslash K$ associamos $G(f(x)|K)$, o grupo de automorfismos de um corpo de raízes L de $f(x)$ sobre K, chamado de grupo de Galois de $f(x)$ sobre K.

Veremos que se $G(f(x)|K)$ é solúvel, então a equação é solúvel por radicais.

Sejam K um corpo, com $\text{car}(K) = 0$, e $x_1, \ldots, x_n$ indeterminadas sobre K.

Indeterminadas sobre K são elementos transcendentes sobre K, sem relações algébricas entre eles, chamados de algebricamente independentes.

Consideremos $L = K(x_1, \ldots, x_n)$ e o polinômio

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_n) \in L[x].$$

Consideremos as funções simétricas elementares

$$\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n \\
s_2 &= \sum_{1 \leq i < j \leq n} x_i x_j \\
s_3 &= \sum_{1 \leq i < j < k \leq n} x_i x_j x_k \\
&\vdots \\
s_j &= \sum_{1 \leq i_1 < \cdots < i_j \leq n} x_{i_1} \cdots x_{i_j} \\
&\vdots \\
s_n &= x_1 \cdots x_n
\end{aligned}$$

Para cada $j = 1, \ldots, n$, a função simétrica elementar s_j é obtida pela adição dos $\binom{n}{j}$ produtos possíveis de j indeterminadas distintas.

Exemplo 9

Para $n = 2$, temos $s_1 = x_1 + x_2$ e $s_2 = x_1 x_2$.

Exemplo 10

Para $n = 3$, temos $s_1 = x_1 + x_2 + x_3$ e $s_2 = x_1 x_2 + x_1 x_3 + x_2 x_3$ e $s_3 = x_1 x_2 x_3$.

Seja $F = K(s_1, \ldots, s_n)$. Então, $F \subset L$ e podemos reescrever $f(x)$ como:

$$f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n \in F[x].$$

Portanto, $f(x) \in F[x]$ se decompõe em produto de fatores lineares em $L[x]$, $f(x)$ tem todas as suas raízes em L e o menor corpo contendo $F \cup \{x_1, \ldots, x_n\}$ é $F(x_1, \ldots, x_n) = K(x_1, \ldots, x_n) = L$. Logo, L é corpo de raízes de $f(x)$ sobre F.

$F = K(s_1, \ldots, s_n)$, com $s_j \in K(x_1, \ldots, x_n)$.

Cada $\sigma \in S_n$ define, de maneira natural, um automorfismo de L do seguinte modo.

Para cada $r(x_1, \ldots, x_n) \in L = K(x_1, \ldots, x_n)$, existem polinômios com coeficientes em K, $g(x_1, \ldots, x_n), h(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ tais que

$$r(x_1, \ldots, x_n) = \frac{g(x_1, \ldots, x_n)}{h(x_1, \ldots, x_n)}.$$

Definimos $\sigma : L \longrightarrow L$ por

O grupo S_n age nas funções racionais.

$$\sigma(r(x_1, \ldots, x_n)) = r(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \frac{g(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}{h(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}.$$

Exemplo 11

Sejam $\sigma = (1, 2, 3) \in S_3$ e $r(x_1, x_2, x_3) = \dfrac{x_1 + x_2}{x_1 + x_2 - x_3}$. Então,

$$\sigma(r(x_1, x_2, x_3)) = \frac{x_{\sigma(1)} + x_{\sigma(2)}}{x_{\sigma(1)} + x_{\sigma(2)} - x_{\sigma(3)}} = \frac{x_2 + x_3}{x_2 + x_3 - x_1}.$$

Exemplo 12

Para todo $\sigma \in S_n$, temos que $\sigma(s_j) = s_j$, para $j = 1, \ldots, n$.

Para isto, observamos que s_j é a soma de todas as parcelas possíveis da forma $x_{i_1} x_{i_2} \cdots x_{i_j}$, com $1 \leq i_1 < i_2 < \cdots < i_j \leq n$.

S_n é um grupo de automorfismos de L.

O corpo fixo desse grupo é

$$L_{S_n} = \{r(x_1, \ldots, x_n) \in L \,;\, \sigma(r) = r\},$$

é chamado de *corpo das funções simétricas*.

Observamos que $K \subset L_{S_n}$ e, pelo Exemplo 12, $s_1, \ldots, s_n \in L_{S_n}$. Portanto, $F = K(s_1, \ldots, s_n) \subset L_{S_n} \subset L$.

Por outro lado, pelo Teorema 4,

A última desigualdade segue do Teorema 3 da Seção 2, na Parte 1, pois $f(x) \in F[x]$ e $\text{grau}(f(x)) = n$.
Fez o Exercício 17 da Seção 1, na Parte 1?

$$n! = |S_n| = [L : L_{S_n}] \leq [L : F] \leq n!.$$

Portanto, $[L : L_{S_n}] = [L : F] = n!$, $L_{S_n} = F = K(s_1, \ldots, s_n)$ e $S_n = G(L|K(s_1, \ldots, s_n))$.

Acabamos de demonstrar o seguinte Teorema.

Teorema 7
Sejam K um corpo, com $car(K) = 0$, e $x_1, \ldots, x_n$ indeterminadas sobre K, $F = K(s_1, \ldots, s_n)$, onde $s_1, \ldots, s_n$ são as funções simétricas elementares, e $f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n \in F[x]$. Então, $L = K(x_1, \ldots, x_n)$ é corpo de raízes de $f(x)$ sobre F e $S_n = G(L|F)$ é o grupo de automorfismos de $L|F$.

Agora vamos introduzir o conceito de grupo solúvel.

Definição 7 (Grupo solúvel)
Um grupo finito G é *solúvel*, se e somente se, existe uma cadeia de subgrupos

$$G = N_0 \supset N_1 \supset \cdots \supset N_s = \{e\},$$

tal que $N_{j+1} \lhd N_j$ e N_j/N_{j+1} é abeliano, para $j = 0, \ldots, s-1$.

Exemplo 13
Todo grupo abeliano é solúvel. Tomamos $G = N_0 \supset N_1 = \{e\}$.

Exemplo 14
S_3 é um grupo solúvel, pois $S_3 = N_0 \supset N_1 = \{I, \tau, \tau^2\} \supset N_2 = \{I\}$.

Exemplo 15
S_4 é um grupo solúvel, pois

$$S_4 = N_0 \supset N_1 = A_4 \supset N_2 = \{I, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \supset N_3 = \{I\}.$$

Exemplo 16
Todo p-grupo finito é solúvel.

De fato, é possível construir uma cadeia de subgrupos de G tal que

$$G = N_0 \supset N_1 \supset \cdots \supset N_s = \{e\}, \text{ onde}$$

$N_{j+1} \lhd N_j$ e N_j/N_{j+1} é cíclico de ordem p, portanto abeliano.

Faça indução sobre $n \geq 1$, onde $|G| = p^n$. Lembre que $Z(G) \neq \{e\}$ e, pelo Teorema de Cauchy, existe $x \in Z(G)$ tal que $o(x) = p$. Para $n > 1$, considere $G/\langle x \rangle$, use a hipótese de indução e a relação entre os subgrupos do grupo quociente e os subgrupos de G que contêm $\langle x \rangle$.

Há uma descrição alternativa para grupos solúveis, usando o comutador de um grupo.

Definição 8 (Comutador G' de G)
Sejam $(G, \cdot)$ um grupo e $a, b \in G$. Definimos o *comutador* de a, b por

$$[a, b] = aba^{-1}b^{-1}.$$

Note que $[a, b]^{-1} = [b, a]$.

O *comutador de* G é o subgrupo G' gerado pelos comutadores $[a, b]$, para quaisquer $a, b \in G$, isto é,

$$\begin{aligned} G' &= \langle aba^{-1}b^{-1} \,;\, a, b \in G \rangle \\ &= \{x_1 \cdots x_n \,;\, n \geq 1, x_j = a_j b_j a_j^{-1} b_j^{-1}, a_j, b_j \in G\}. \end{aligned}$$

Exemplo 17
Se $(G, \cdot)$ é abeliano, então $G' = \{e\}$.

Exemplo 18
O comutador de S_3 é $\{I, \tau, \tau^2\}$.

Proposição 7 (Propriedades do comutador)
Sejam $(G, \cdot)$ um grupo e G' seu comutador. Então:
(i) G' é normal em G.
(ii) G/G' é abeliano.
(iii) Se N é um subgrupo normal de G, tal que G/N é abeliano, então $G' \subset N$.
(Isto significa que G' é o menor subgrupo normal de G com a propriedade do grupo quociente ser abeliano.)

Demonstração:
(i) Para cada $c \in G$ e $[a, b]$, com $a, b \in G$, temos

$$\begin{aligned} c[a, b]c^{-1} &= c(aba^{-1}b^{-1})c^{-1} \\ &= (ca)(c^{-1}a^{-1}ac)(ba^{-1})(b^{-1}c^{-1}) \\ &= (cac^{-1}a^{-1})(acb)(a^{-1}b^{-1}c^{-1}) \\ &= (cac^{-1}a^{-1})(a(cb)a^{-1}(cb)^{-1}) \in G'. \end{aligned}$$

Para todo $c \in G$, $x_j = [a_j, b_j]$, $j = 1, \ldots, n$, se $x = x_1 x_2 \cdots x_n$, então

$$cxc^{-1} = c(x_1 x_2 \cdots x_n)c^{-1} = (cx_1c^{-1})(cx_2c^{-1}) \cdots (cx_nc^{-1}) \in G'.$$

(ii) Sejam $a, b \in G$. Então,

$$\begin{aligned} G'aG'b &= G'ab \\ &= G'(ab)(a^{-1}b^{-1}ba) \\ &= G'(aba^{-1}b^{-1})ba \\ &\overset{(1)}{=} G'ba \\ &= G'bG'a \end{aligned}$$

Em (1) usamos que $aba^{-1}b^{-1} \in G'$.

(iii) Seja $N \lhd G$ com G/N abeliano. Então,

$$\begin{aligned} NaNb = NbNa &\iff Nab = Nba \\ &\iff ab(ba)^{-1} \in N \\ &\iff aba^{-1}b^{-1} \in N \end{aligned}$$

Logo, $G' = \langle aba^{-1}b^{-1}, \text{ para quaisquer } a, b \in G\rangle \subset N$ ■

Procedemos agora indutivamente.

G' é um grupo. Definimos $G^{(2)} = (G')'$ o subgrupo de G' gerado por $a'b'a'^{-1}b'^{-1}$ com $a', b' \in G'$.

Continuamos desse modo definindo $G^{(m+1)} = (G^{(m)})'$.

Tomamos $G^{(1)} = G'$. Pela Proposição anterior, $G^{(m+1)} \lhd G^{(m)}$ e $G^{(m)}/G^{(m+1)}$ é grupo abeliano.

Proposição 8

$(G, \cdot)$ é um grupo solúvel se, e somente se, $G^{(r)} = \{e\}$, para algum $r \geq 1$.

Demonstração:

($\Longleftarrow$:) Seja $r \geq 1$ tal que $G^{(r)} = \{e\}$. Consideremos $N_0 = G$, $N_1 = G^{(1)}$, ..., $N_r = G^{(r)} = \{e\}$. Então,

$$G = N_0 \supset N_1 \supset \cdots \supset N_r = \{e\}$$

é uma cadeia de subgrupos de G. Pela Proposição anterior, obtemos que $N_{j+1} = G^{(j+1)} \lhd G^{(j)} = N_j$ e $N_j/N_{j+1} = G^{(j)}/G^{(j+1)}$ é abeliano. Portanto, G é solúvel.

($\Longrightarrow$:) Suponhamos que G seja solúvel. Então, existe uma cadeia de subgrupos

$$G = N_0 \supset N_1 \supset \cdots \supset N_r = \{e\},$$

tal que $N_{j+1} \lhd N_j$ e N_j/N_{j+1} é abeliano. Pelo item (iii) da Proposição 7, temos que ${N_j}' \subset N_{j+1}$. Logo,

$$\begin{aligned} N_1 \supset {N_0}' = G' &\implies N_1 \supset G^{(1)} \\ N_2 \supset {N_1}' \supset (G')' = G^{(2)} &\implies N_2 \supset G^{(2)} \\ N_3 \supset {N_2}' \supset (G^{(2)})' = G^{(3)} &\implies N_3 \supset G^{(3)} \end{aligned}$$

Indutivamente, temos $N_j \supset G^{(j)}$ e $\{e\} = N_r \supset G^{(r)} \supset \{e\}$. Portanto, $G^{(r)} = \{e\}$. ■

Algumas propriedades sobre solubilidade.

Proposição 9 (Propriedades adicionais)
Valem as seguintes propriedades:

(i) Se H é um subgrupo de G e G é solúvel, então H é solúvel.

(ii) Se G é solúvel e $\varphi : G \longrightarrow \overline{G}$ é homomorfismo sobrejetor, então $\overline{G}$ é solúvel. Em particular, se $N \lhd G$ e G é solúvel, então G/N é solúvel.

(iii) Seja $N \lhd G$. Se N é solúvel e G/N é solúvel, então G é solúvel.

Demonstração:

(i) Primeiramente, observamos que:

$H < G \Longrightarrow H' < G' \Longrightarrow H^{(2)} < G^{(2)}$. Por indução, $H^{(j)} < G^{(j)}$, para todo $j \geq 1$.

Se G é solúvel, então existe $r \geq 1$ tal que $G^{(r)} = \{e\}$. Pela observação acima, $H^{(r)} \subset G^{(r)}$. Logo, $H^{(r)} = \{e\}$ e H é solúvel.

(ii) $\overline{G}' = \{\overline{x_1} \cdot \ldots \cdot \overline{x_n}\ ;\ \overline{x_j} = \overline{a_j}\overline{b_j}\overline{a_j}^{-1}\overline{b_j}^{-1}\ ;\ \overline{a_j}, \overline{b_j} \in \overline{G}\}$

Como φ é um homomorfismo sobrejetor, para cada $\overline{a} \in \overline{G}$, existe $a \in G$ tal que $\overline{a} = \varphi(a)$ e $\overline{a}^{-1} = \varphi(a^{-1})$. Logo,

$$\overline{x_j} = \overline{a_j}\overline{b_j}\overline{a_j}^{-1}\overline{b_j}^{-1} = \varphi(a_j)\varphi(b_j)\varphi(a_j{}^{-1})\varphi(b_j{}^{-1}) = \varphi(a_j b_j a_j{}^{-1} b_j{}^{-1})$$

Assim,

$$\overline{G}' = \{\overline{x_1} \cdot \ldots \cdot \overline{x_n}\ ;\ \overline{x_j} = \varphi(a_j b_j a_j{}^{-1} b_j{}^{-1})\ ;\ a_j, b_j \in G\} = \varphi(G').$$

Indutivamente, $\overline{G}^{(n)} = \varphi(G^{(n)})$, para todo $n \geq 1$. Tomando $r \geq 1$ tal que $G^{(r)} = \{e\}$, temos que $\overline{G}^{(r)} = \varphi(G^{(r)}) = \varphi(e) = \overline{e}$, mostrando que $\overline{G}$ é solúvel.

Para a última afirmação, tomamos o homomorfismo de grupos sobrejetor $\pi : G \longrightarrow G/N$.

(iii) Seja $N \lhd G$. Suponhamos que N e G/N são solúveis.

Seja

$$\overline{G_0} = G/N \supset \overline{G_1} \supset \cdots \supset \overline{G_s} = \{\overline{e}\} \qquad (1)$$

a cadeia de subgrupos de G/N, tal que $\overline{G_{j+1}} \lhd \overline{G_j}$ e $\overline{G_j}/\overline{G_{j+1}}$ é abeliano.

Seja

$$N = N_0 \supset N_1 \supset \cdots \supset N_r = \{e\} \qquad (2)$$

a cadeia de subgrupos de N, tal que $N_{j+1} \lhd N_j$ e N_j/N_{j+1} é abeliano.

Na cadeia (1) temos $\overline{G_j} = G_j/N$, onde $N < G_j < G$ e $G_{j+1} \lhd G_j$.

Assim, (1) induz a cadeia

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = N. \qquad (3)$$

Além disso, o homomorfismo sobrejetor

$$\begin{aligned} \psi : \overline{G_j} = G_j/N &\longrightarrow G_j/G_{j+1} \\ Nx &\longmapsto G_{j+1}x \end{aligned}$$

com Núcleo$(\psi) = G_{j+1}/N = \overline{G_{j+1}}$, pelo Teorema fundamental dos homomorfismos, induz um isomorfismo de $\overline{G_j}/\overline{G_{j+1}}$ com G_j/G_{j+1}. Como $\overline{G_j}/\overline{G_{j+1}}$ é abeliano, então G_j/G_{j+1} é abeliano.

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = N. \qquad (3)$$

Completando a cadeia (3) com a cadeia (2), obtemos

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = N = N_0 \supset N_1 \supset \cdots \supset N_r = \{e\},$$

que é a cadeia procurada para G. ■

Lema 5

Seja $G = S_n$, com $n \geq 5$. Então, $G^{(r)}$, para $r = 1, 2, \ldots$, contém cada 3-ciclo de S_n. Em particular, S_n não é solúvel, para $n \geq 5$.

Demonstração: Primeiramente, observamos que se G é um grupo e $N \lhd G$, então $N' \lhd G$.

De fato, sejam $c, d \in N$ e $a \in G$. Então, $cdc^{-1}d^{-1} \in N'$ e

$$a(cdc^{-1}d^{-1})a^{-1} = \underbrace{(aca^{-1})}_{c_1}\underbrace{(ada^{-1})}_{d_1}\underbrace{(ac^{-1}a^{-1})}_{c_1^{-1}}\underbrace{(ad^{-1}a^{-1})}_{d_1^{-1}} \in N',$$

pois $c_1, d_1, c_1^{-1}, d_1^{-1} \in N$.

Afirmamos agora que se $n \geq 5$ e N é um subgrupo normal de S_n que contém cada 3-ciclo de S_n, então seu comutador N' também contém cada 3-ciclo de S_n.

Com efeito, suponhamos que $\sigma = (1,2,3)$ e $\tau = (1,4,5)$ estejam em N. Então, $\sigma^{-1} = (2,1,3)$, $\tau^{-1} = (4,1,5)$ e

$$\sigma\tau\sigma^{-1}\tau^{-1} = (1,2,3)(1,4,5)(2,1,3)(4,1,5)$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} = (1,2,4) \in N'$$

Como $N' \lhd G$, para todo $\xi \in S_n$ temos que $\xi(1,2,4)\xi^{-1} \in N'$. Escolhemos $\xi \in S_n$ tal que $\xi(1) = i_1$, $\xi(2) = i_2$ e $\xi(4) = i_3$, com i_1, i_2, i_3 distintos, $1 \leq i_1, i_2, i_3 \leq n$ e $\xi(j) = j$, para todo $j \neq 1, 2, 4$. Então,

$$\xi(1,2,4)\xi^{-1} = (i_1, i_2, i_3) \in N'.$$

Logo, N' contém todo 3-ciclo de S_n.

Tomando $N = G = S_n$, temos que $N \lhd G$ e N contém todos os 3-ciclos de S_n. Como $G' \lhd G$, então $G^{(2)}$ contém todos os 3-ciclos de S_n. Como $G^{(2)} \lhd G$, então $G^{(3)}$ contém todos os 3-ciclos de S_n. Continuando dessa maneira, $G^{(r)}$, para todo $r \geq 1$, contém todos os 3-ciclos de S_n e, em particular, $G^{(r)} \neq \{I\}$, mostrando que S_n não é solúvel para $n \geq 5$. ■

Daqui por diante consideramos corpos de característica zero.

Definição 9

Uma extensão $M|K$ é dita radical se existe uma torre, chamada *torre radical simples*,

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = M,$$

tal que, para cada $j = 1, \ldots, s$, existem $\alpha_j \in K_j$, $n_j \geq 1$, com $\alpha_j^{n_j} \in K_{j-1}$ e $K_j = K_{j-1}(\alpha_j)$.

Exemplo 19

São extensões radicais:

$\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$ com $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$, como torre radical simples.

$\mathbb{Q}(i, \sqrt[4]{2})|\mathbb{Q}$ com $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2})(i)$, como uma torre radical simples.

$\mathbb{Q}(\sqrt{2}, \sqrt{3})|Q$ com $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(\sqrt{3})$, como uma torre radical simples.

$\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)|\mathbb{Q}$ com $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})\left(\sqrt{1+\sqrt{2}}\right)$, como uma torre radical simples.

Definição 10 (Polinômio solúvel por radicais)

Sejam $f(x) \in K[x]\backslash K$ e L um corpo de raízes de $f(x)$ sobre K. O polinômio $f(x)$ é *solúvel por radicais* se, e somente se, existe uma extensão radical $M|K$, tal que $L \subset M$.

Proposição 10
Seja $M|K$ uma extensão radical. Então, existe uma extensão radical normal $N|K$, tal que $M \subset N$.

Demonstração: Consideremos a torre radical simples

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = M,$$

onde para cada $j = 1, \ldots, s$ existem $\alpha_j \in K_j$, $n_j \geq 1$, com ${\alpha_j}^{n_j} \in K_{j-1}$ e $K_j = K_{j-1}(\alpha_j)$.

Seja N o corpo de raízes sobre K de $p_1(x) \cdots p_s(x)$, onde $p_j(x)$ é o polinômio mínimo de α_j sobre K. Para mostrar que $N|K$ é uma extensão radical precisamos construir uma torre radical simples. Faremos a construção no caso $s = 2$ e a demonstração é por indução sobre s.

Seja $M|K$ extensão radical com $M = K(\beta, \gamma)$, $\beta^n \in K$ e $\gamma^m \in K(\beta)$. Assim,

$$K \subset K(\beta) \subset K(\beta)(\gamma) = M.$$

é uma torre radical simples.

Sejam $p(x), q(x)$ os polinômios mínimos de β e γ sobre K. Sejam $\beta = \beta_1, \ldots, \beta_r$ e $\gamma = \gamma_1, \ldots, \gamma_s$ as raízes de $p(x)$ e $q(x)$, respectivamente. Vamos mostrar que $N|K$ é radical, onde $N = K(\beta_1, \ldots, \beta_r, \gamma_1, \ldots, \gamma_s)$ é o corpo de decomposição de $p(x)q(x)$ sobre K. A torre radical simples é

$$K \subset K(\beta_1) \subset K(\beta_1)(\beta_2) \subset \cdots \subset K(\beta_1, \ldots, \beta_{r-1})(\beta_r) = L$$

completada com

$$L \subset L(\gamma_1) \subset L(\gamma_1)(\gamma_2) \subset \cdots \subset L(\gamma_1, \ldots, \gamma_{s-1})(\gamma_s) = N$$

É claro que $M \subset N$, L é corpo de decomposição de $p(x)$ sobre K e $L(\gamma_1, \ldots, \gamma_s)$ é corpo de decomposição de $q(x)$ sobre L.

Para cada $j = 1, \ldots, r$, existe K-automorfismo $\tau : N \longrightarrow N$ tal que $\tau(\beta) = \beta_j$. Como $\beta^n = a \in K$, então

$$\beta_j^n = \tau(\beta)^n = \tau(\beta^n) = \tau(a) = a \in K \subset K(\beta_1, \ldots, \beta_{j-1}),$$

para cada $j \geq 2$.

Para cada $j = 1, \ldots, s$, existe K-automorfismo $\sigma : N \longrightarrow N$ tal que $\sigma(\gamma) = \gamma_j$ e $\sigma|_L$ é um K-automorfismo de L, pois $L|K$ é normal. Como $\gamma^m = f(\beta) \in K(\beta) \subset L$, para algum polinômio $f(x) \in K[x]$, então $\sigma(\beta) \in L$ e

$$\gamma_j^m = \sigma(\gamma)^m = \sigma(\gamma^m) = \sigma(f(\beta)) = f(\sigma(\beta)) \in L \subset L(\gamma_1, \ldots, \gamma_{j-1}),$$

para cada $j \geq 2$. ■

Teorema 8

Seja K um corpo, com $car(K) = 0$, que contém uma raiz primitiva n-ésima da unidade. Sejam $a \in K$, $a \neq 0$, $f(x) = x^n - a \in K[x]$ e L o corpo de raízes de $f(x)$ sobre K. Então,

(i) $L = K(b)$, onde b é qualquer raiz de $f(x)$.

(ii) $G(L|K)$ é abeliano.

Demonstração:

(i) Seja ω uma raiz primitiva n-ésima da unidade. Então, $1, \omega, \ldots, \omega^{n-1}$ são as n raízes da unidade e, tomando b tal que $b^n = a$, temos que $b\omega^j$, com $j = 0, \ldots, n-1$ são as n raízes de $x^n - a$ e

$$x^n - a = (x - b)(x - b\omega) \cdots (x - b\omega^{n-1}).$$

Como $\{1, \omega, \ldots, \omega^{n-1}\} \subset K$, temos que $L = K(b)$ é um corpo de raízes de $f(x)$ sobre K.

(ii) Sejam $\sigma, \tau \in G(L|K)$. Como $\sigma(b)$ e $\tau(b)$ são raízes de $x^n - a$, então $\sigma(b) = b\omega^i$ e $\tau(b) = b\omega^j$, para algum i, j com $0 \leq i, j \leq n-1$. Portanto,

Como $\omega^i, \omega^j \in K$, então $\sigma(\omega^j) = \omega^j$ e $\tau(\omega^i) = \omega^i$.

$$(\sigma \circ \tau)(b) = \sigma(\tau(b)) = \sigma(b\omega^j) = \omega^j\sigma(b) = \omega^j(\omega^i b) = \omega^{j+i}b \text{ e}$$

$$(\tau \circ \sigma)(b) = \tau(\sigma(b)) = \tau(b\omega^i) = \omega^i\tau(b) = \omega^i(\omega^j b) = \omega^{i+j}b.$$

Logo, $(\sigma \circ \tau)(b) = (\tau \circ \sigma)(b)$. Como $L = K(b)$, então $\sigma \circ \tau = \tau \circ \sigma$ em L, mostrando que $G(L|K)$ é abeliano. ■

Vale a recíproca, mas a demonstração não será feita aqui.

Teorema 9

Se $f(x) \in K[x] \backslash K$ é solúvel por radicais, então $G(L|K)$ é solúvel, onde L é um corpo de raízes de $f(x)$ sobre K.

Demonstração: Suponhamos que $f(x) \in K[x]$ seja solúvel por radicais. Então, existe uma torre radical $N|K$ tal que

$$K_1 = K \subset K_2 \subset \cdots \subset K_s = N,$$

existem $\alpha_j \in K_j$, $n_j \geq 1$, tais que $\alpha_j^{n_j} \in K_{j-1}$, $K_j = K_{j-1}(\alpha_j)$, para cada $j = 2, \ldots, s$, e $L \subset N$.

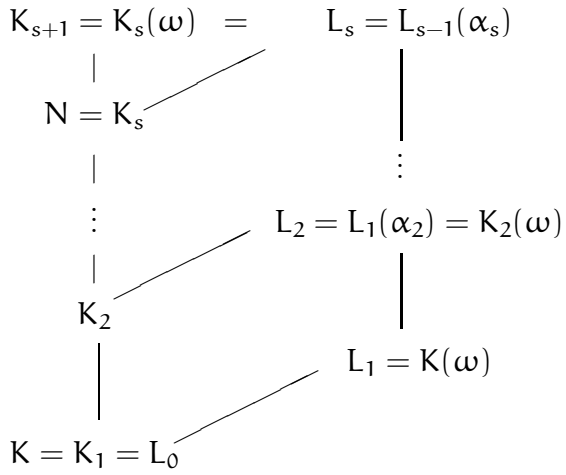
Pela Proposição 10 podemos supor que $N|K$ é normal. Sejam $n = mmc(n_2, \ldots, n_s)$ e ω uma raiz primitiva n-ésima da unidade. Consideramos $K_{s+1} = K_s(\omega)$.

Vamos construir uma nova torre para ter controle sobre o grupo de automorfismos e usar a correspondência de Galois.

Tomamos $L_0 = K_1 = K$, $L_1 = K(\omega)$ e $L_j = L_{j-1}(\alpha_j)$, para cada $j \geq 2$.

Observamos que $\omega^{\frac{n}{n_j}} \in L_{j-1}$ é uma raiz primitiva n_j-ésima da unidade.

Por indução, temos que $L_j = K_j(\omega)$. De modo que $L_s = K_s(\omega) = K_{s+1} = N(\omega)$. Veja o diagrama a seguir.



Para $j = 2, \ldots, s$ temos que $L_j = L_{j-1}(\alpha_j)$ e L_j é corpo de decomposição de $x^{n_j} - {\alpha_j}^{n_j}$ sobre L_{j-1}, pois L_{j-1} tem raiz primitiva n_j-ésima da unidade. Logo, $L_j|L_{j-1}$ é extensão normal e separável. Pelo Teorema anterior, $G(L_j|L_{j-1})$ é abeliano, para $j = 2, \ldots, s$.

$L_1|L_0$ é normal e separável, pois $G(L_1|L_0) = G(K(\omega)|K)$ é abeliano. De fato, cada $\sigma \in G(K(\omega)|K)$ está perfeitamente determinada por $\sigma(\omega)$ e $\sigma(\omega)$ deve ser uma raiz primitiva n-ésima da unidade. Portanto, existe um único i, com $1 \leq i < n$, $\text{mdc}(i, n) = 1$, tal que $\sigma(\omega) = \omega^i$. Assim, $G(K(\omega)|K) \simeq$ subgrupo de ${\mathbb{Z}_n}^*$ com o homomorfismo injetor

$$\begin{aligned} \varphi : G(K(\omega)|K) &\longrightarrow {\mathbb{Z}_n}^* \\ \sigma &\longmapsto \overline{i} = i \mod n, \end{aligned}$$

Se $\sigma, \tau \in G(K(\omega)|K)$, então existem $1 \leq i, j < n$ tais que $\sigma(\omega) = \omega^i$ e $\tau(\omega) = \omega^j$, com $\text{mdc}(i, n) = 1$ e $\text{mdc}(j, n) = n$. Logo, $(\tau \circ \sigma)(\omega) = \tau(\omega^i) = \tau(\omega)^i = (\omega^j)^i = \omega^{ij} = (\sigma \circ \tau)(\omega)$. Existe um único $s \equiv ij \mod n$, com $\text{mdc}(ij, n) = 1$, mostrando que φ é homomorfismo. Além disso, se $\varphi(\sigma) = \overline{1}$, então $\sigma(\omega) = \omega$ e $\sigma = I$.

Consideremos a cadeia de corpos

$$L_0 = K \subset L_1 \subset L_2 \subset \cdots \subset L_{s-1} \subset L_s$$

com $L_s|K$ normal e separável.

Tomando $G = G(L_s|K)$ e $G_j = G(L_s|L_j)$, pela correspondência de Galois, temos a cadeia de grupos

$$G \supset G_1 \supset G_2 \supset \cdots \supset G_{s-1} \supset G_s = \{I\}. \qquad (\star)$$

Como $L_j|L_{j-1}$ é normal, então $G_j \lhd G_{j-1}$ e $G_{j-1}/G_j \simeq G(L_j|L_{j-1})$ é abeliano.

Logo, a cadeia $(\star)$ de subgrupos de $G(L_s|K)$, mostra que $G(L_s|K)$ é solúvel.

Por hipótese, L, o corpo de decomposição de $f(x)$ sobre K, satisfaz

$$K \subset L \subset N \subset L_s.$$

Pelo Teorema de Galois, $G(L|K) \simeq G(L_s|K)/G(L_s|L)$. Como $G(L_s|K)$ é solúvel, então seu subgrupo $G(L_s|L)$ também é solúvel. Como $L_s|L$ é normal, então $G(L_s|L) \lhd G(L_s|K)$ e o grupo quociente é solúvel. ■

Corolário 3
O polinômio geral de grau $n \geq 5$ não é solúvel por radicais.

Agora vamos aprender a construir polinômios com coeficientes racionais que não são solúveis por radicais, isto é, o seu grupo de automorfismos sobre $\mathbb{Q}$ não é solúvel.

Proposição 11
Seja p um natural primo e $f(x) \in \mathbb{Q}[x]$ um polinômio mônico irredutível de grau p. Suponhamos que $f(x)$ tem exatamente duas raízes complexas não-reais. Então, $G(f(x)|\mathbb{Q})$ é o grupo simétrico S_p.

Demonstração: Pelo Teorema Fundamental da Álgebra, $\mathbb{C}$ contém um corpo de decomposição de $f(x)$ sobre $\mathbb{Q}$, digamos L. Como a $\mathrm{car}(\mathbb{Q}) = 0$, $f(x)$ tem p raízes distintas e $G(L|\mathbb{Q})$ é isomorfo a um subgrupo de S_p. Seja $\alpha \in \mathbb{C}$ uma raiz qualquer de $f(x)$. Então, $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha) \subset L$. Logo, $p = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ divide $[L : \mathbb{Q}] = |G(L|\mathbb{Q})|$. Pelo Teorema de Cauchy, $G(L|K)$ tem um elemento de ordem p. Os elementos de ordem p de S_p são p-ciclos. A conjugação complexa é um $\mathbb{Q}$-automorfismo de $\mathbb{C}$ e restrita a L induz um $\mathbb{Q}$-automorfismo de L, digamos σ. σ fixa as $p-2$ raízes reais de $f(x)$ e permuta as duas raízes complexas não-reais de $f(x)$. Portanto, $G(L|\mathbb{Q})$ tem um 2-ciclo. Podemos supor, após tomar uma potência do p-ciclo se necessário, que $(1,2)$, $(1,2,\ldots,p) \in G(L|\mathbb{Q})$. Logo, $G(L|\mathbb{Q}) \supset \langle (1,2), (1,2,\ldots,p) \rangle = S_p$. Portanto, $G(L|\mathbb{Q}) = S_p$. ■

Exemplo 20
O polinômio $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ não é solúvel por radicais.

De fato, pelo critério de Eisenstein com o primo 3, $f(x)$ é irredutível em $\mathbb{Q}[x]$. Vamos mostrar que $f(x)$ tem exatamente três raízes reais e duas raízes complexas não-reais. Temos $f'(x) = 5x^4 - 6$ e $f''(x) = 20x$, então f cresce de $\left(-\infty, -\sqrt[4]{\frac{6}{5}}\right) \cup \left(\sqrt[4]{\frac{6}{5}}, +\infty\right)$ e decresce em $\left(-\sqrt[4]{\frac{6}{5}}, \sqrt[4]{\frac{6}{5}}\right)$, o gráfico de f é côncavo para baixo em $(-\infty, 0)$ e côncavo para cima em $(0, +\infty)$. Como $f(-2) = -17$, $f(-1) = 8$, $f(1) = -2$ e $f(2) = 23$, então $f(x)$ tem uma raiz real em $(-2, -1)$, uma em $(-1, 1)$ e uma em $(1, 2)$. Fazendo um esboço do gráfico de f vemos que $f(x)$ tem exatamente três raízes reais. As raízes são simples, pois $\text{mdc}(f(x), f'(x)) = 1$.

Polinômio irredutível sobre corpo de cararacterística 0 tem raízes simples.

Exercícios

1. Determine extensões radicais $L|\mathbb{Q}$ contendo os seguintes elementos:

   (a) $\dfrac{\sqrt{11} - \sqrt[7]{23}}{\sqrt[4]{5}}$

   (b) $(\sqrt{6} + 2\sqrt[3]{5})^4$

   (c) $\dfrac{2\sqrt[5]{5} - 4}{1 + \sqrt{99}}$

2. Mostre que os seguintes polinômios em $\mathbb{Q}[x]$ não são solúveis por radicais:

   (a) $f(x) = x^5 - 4x + 2$

   (b) $f(x) = x^5 - 4x^2 + 2$

   (c) $f(x) = x^5 - 6x^2 + 3$

   (d) $f(x) = x^7 - 10x^5 + 15x + 5$

3. Mostre que um grupo com 44 elementos é solúvel.

4. Sejam a, b, c, d inteiros positivos distintos.

   (a) Mostre que se os 2-ciclos (a, b) e (a, c) são não-disjuntos, então $(a, b)(a, c) = (a, c, b)$.

   (b) Mostre que se os 2-ciclos (a, b) e (c, d) são disjuntos, então $(a, b)(c, d) = (a, b)(b, c)(b, c)(c, d) = (b, c, a)(c, d, b)$.

   (c) Mostre que o grupo alternado A_n é gerado pelos 3-ciclos.

5. Seja $\psi : S_n \longrightarrow \{1, -1\}$ a função definida por

$$\psi(\sigma) = \begin{cases} 1 & , \text{ se } \sigma \text{ é permutação par} \\ -1 & , \text{ se } \sigma \text{ é permutação ímpar} \end{cases}$$

(a) Mostre que ψ é um homomorfismo sobrejetor de grupos com Núcleo$(\psi) = A_n$.

(b) Conclua que S_n/A_n é um grupo abeliano.

Veja a Proposição 7.

(c) Mostre que o comutador de S_n é A_n.

(d) Mostre que se H é um subgrupo de S_n tal que $(S_n : H) = 2$, então $H = A_n$, isto é, A_n é o único subgrupo de S_n de índice 2.

$\mathbb{C}$ é um corpo algebricamente fechado

Definição 11 (Corpo algebricamente fechado)
O corpo K é chamado de *algebricamente fechado* se, e somente se, todo polinômio $f(x) \in K[x] \backslash K$ tem uma raiz em K.

Proposição 12 (Propriedade dos corpos algebricamente fechados)
Seja K um corpo algebricamente fechado. Se $f(x) \in K[x]$ é um polinômio de grau $n \geq 1$, então existem $a, \alpha_1, \ldots, \alpha_n \in K$ tais que

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

Demonstração: Indução sobre $n = \text{grau}(f(x))$. Se $n = 1$, então $f(x) = ax + b$, com $a, b \in K$ e $a \neq 0$. Logo, $f(x) = a(x + b \cdot a^{-1})$ com $\alpha = -b \cdot a^{-1} \in K$.

Suponhamos o resultado válido para polinômios em $K[x]$ de grau m, tais que $1 \leq m < n = \text{grau}(f(x))$. Vamos mostrar que vale para $f(x)$. Como K é algebricamente fechado, $f(x)$ tem uma raiz $\alpha_1 \in K$. Então,

$$f(x) = (x - \alpha_1)g(x), \text{ com } g(x) \in K[x] \text{ e } \text{grau}(g(x)) = n - 1.$$

Por hipótese de indução, existem $\alpha_2, \ldots, \alpha_n, a \in K$, tais que

$$g(x) = a(x - \alpha_2) \cdots (x - \alpha_n).$$

Portanto, $f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$. ■

Corolário 4
Se K é um corpo algebricamente fechado, então os polinômios mônicos irredutíveis são $x - \alpha$, com $\alpha \in K$.

Como uma aplicação dos Teoremas estudados vamos mostrar que o corpo dos números complexos é algebricamente fechado. Para isto, usaremos as seguintes propriedades:

Observação:

(i) O corpo dos números reais é um corpo ordenado.

(ii) Todo número real positivo é um quadrado em $\mathbb{R}$.

(iii) Todo polinômio de grau ímpar com coeficientes reais tem uma raiz real.

(iv) Cada elemento $a + bi \in \mathbb{C}$ tem uma raiz quadrada $c + di \in \mathbb{C}$, sendo

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2} \quad \text{e} \quad d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2},$$

$(c + di)^2 = c^2 - d^2 + 2cdi = a + bi$

onde $c, d \in \mathbb{R}$ são escolhidos de modo que o sinal de $c \cdot d$ seja o mesmo sinal de b.

Teorema 10

$\mathbb{C}$ é um corpo algebricamente fechado.

Demonstração: Queremos mostrar que se $L|\mathbb{C}$ é extensão finita, então $L = \mathbb{C}$. Seja $L|\mathbb{C}$ uma extensão finita. Sabemos que existe N tal que $L \subset N$ e $N|\mathbb{R}$ é extensão normal, forçosamente, separável. Vamos mostrar que $N = \mathbb{C}$.

Seja $G = G(N|\mathbb{R})$. Como $2 = [\mathbb{C} : \mathbb{R}]$ divide $[N : \mathbb{R}]$, então 2 divide $|G|$. Seja H um 2-Sylow subgrupo de G e F o corpo fixo de H. Temos que $[F : \mathbb{R}] = (G : H) = \frac{|G|}{|H|}$ é ímpar. Pelo Teorema do elemento primitivo, existe $\alpha \in F$ tal que $F = \mathbb{R}(\alpha)$. Então, α é raiz de um polinômio irredutível em $\mathbb{R}[x]$ de grau ímpar. Pela Observação (iii), o polinômio mínimo de α sobre $\mathbb{R}$ tem grau 1, isto é, $F = \mathbb{R}$ e logo, $G = H$ é um 2-grupo. Seja $H_1 = G(N|\mathbb{C})$. Se $H_1 \neq \{I\}$, então H_1 tem um subgrupo H_2 de índice 2 e tomando K, o corpo fixo de H_2, temos $[K : \mathbb{C}] = 2$, contradizendo (iv). Portanto, $H_1 = \{I\}$ e $[N : \mathbb{C}] = |H_1| = 1$, isto é, $N = \mathbb{C}$. ■