Estamos finalmente em condições de explicar como é que a teoria de Galois permite substituir problemas sobre polinómios por um problema em princípio mais simples de teoria dos grupos. Galois descobriu que existe uma correspondência entre extensões intermédias e subgrupos do grupo de Galois, que passamos a descrever.

CORRESPONDÊNCIA DE GALOIS

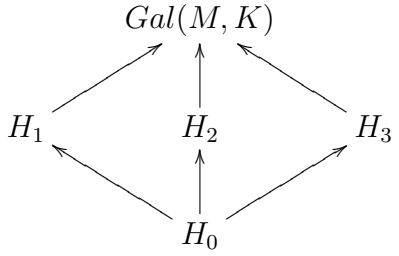
Seja M uma extensão de K. Se L é uma extensão intermédia (isto é, $K \subseteq L \subseteq M$), todo o L-automorfismo de M é obviamente um K-automorfismo de M e, portanto, $Gal(M, L)$ é um subgrupo do grupo $Gal(M, K)$. Por outro lado, se H é um subgrupo de $Gal(M, K)$, o conjunto $Fix(H) := \{a \in M \mid \Phi(a) = a \ \forall \Phi \in H\}$ dos pontos fixos por H é uma extensão intermédia $K \subseteq Fix(H) \subseteq M$. A esta correspondência entre extensões intermédias de $K \subseteq M$ e subgrupos de $Gal(M, K)$ chama-se *correspondência de Galois*.

[Esta correspondência não é, em geral, uma bijecção,
mas tem boas propriedades:
(1) Se $L_1 \subseteq L_2$ então $Gal(M, L_1) \supseteq Gal(M, L_2)$.
(2) Se $H_1 \subseteq H_2$ então $Fix(H_1) \supseteq Fix(H_2)$.
(3) $Fix(Gal(M, L)) \supseteq L$.
(4) $Gal(M, Fix(H)) \supseteq H$]

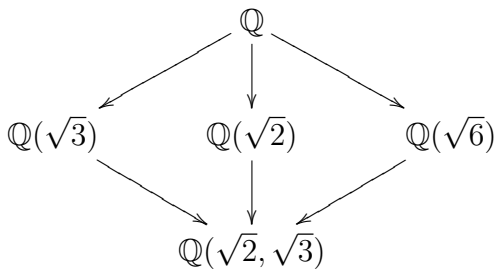
Exemplo: Consideremos a extensão $M = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $K = \mathbb{Q}$. Vimos no final da Aula 19 que o grupo de Galois desta extensão contém 4 elementos e é isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$:

$$Gal(M, K) := \{\Phi_0, \Phi_1, \Phi_2, \Phi_3\}.$$

Este grupo possui, para além do subgrupo trivial $H_0 = \{\Phi_0\}$, os subgrupos $H_1 = \{\Phi_0, \Phi_1\}$, $H_2 = \{\Phi_0, \Phi_2\}$ e $H_3 = \{\Phi_0, \Phi_3\}$. Assim, o conjunto parcialmente ordenado dos subgrupos de $Gal(M, K)$ pode ser representado pelo diagrama



O corpo fixo pelo grupo de Galois $Gal(M,K)$ é o corpo de base $\mathbb{Q}$, enquanto que $Fix(H_0) = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Por outro lado, é facil de ver que $Fix(H_1) = \mathbb{Q}(\sqrt{3})$, $Fix(H_2) = \mathbb{Q}(\sqrt{2})$, $Fix(H_3) = \mathbb{Q}(\sqrt{6})$. Assim, o conjunto parcialmente ordenado das extensões intermédias de $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ é dado pelo diagrama



Teorema. [Teorema Fundamental de Galois]
Seja $K \subseteq L \subseteq M$ uma torre de corpos, onde M é uma extensão de Galois de K. Então $Gal(M,L)$ é um subgrupo normal de $Gal(M,K)$ se e só se L é também uma extensão de Galois de K. Neste caso, $Gal(L,K) \cong Gal(M,K)/Gal(M,L)$:

$$G \left\{ \begin{array}{l} \\ H \left\{ \begin{array}{l} M \\ \uparrow \\ L \end{array} \right. \\ \\ \end{array} \right. \begin{array}{l} \\ \\ \uparrow \\ K \end{array} \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} G/H$$

Demonstração. Faremos somente a prova da implicação "$\Leftarrow$".

Suponhamos então que L é uma extensão de Galois de K, ou seja, $L = K(\theta_1,\ldots,\theta_n) \subseteq M$, onde $\theta_1,\ldots,\theta_n$ são as raízes de algum polinómio $p(x) \in K[x]$. Como cada $\Phi \in Gal(M,K)$ permuta as raízes de p(x) e mantém fixos os elementos de K, então $\Phi(L) \subseteq L$. Podemos assim considerar a aplicação

$$\begin{array}{rccc} h: & Gal(M,K) & \to & Gal(L,K) \\ & \Phi & \mapsto & \Phi|_L \end{array}$$

É evidente que se trata de um homomorfismo de grupos, sendo o seu núcleo precisamente o subgrupo $Gal(M,L)$. Assim, $Gal(M,L)$ é um subgrupo normal de $Gal(M,K)$. O Teorema da Aula 19 garante que, dado $\Psi \in Gal(L,K)$, existe $\Phi \in Gal(M,K)$ que prolonga Ψ. Portanto, h é sobrejectivo e, pelo Teorema do Homomorfismo estudado em Álgebra I, tem-se $Gal(L,K) \cong Gal(M,K)/Gal(M,L)$.

■

Vamos agora discutir o critério descoberto por Galois que permite decidir se uma equação algébrica é ou não resolúvel por radicais. Até ao final, para simplificar, assumiremos que todos os corpos têm característica 0.

EXTENSÃO PURA

Uma extensão L de K diz-se *pura* se $L = K(\theta)$, onde $\theta \in L$ é tal que $\theta^m \in K$ para algum $m \in \mathbb{N}$ (isto é, θ é um *radical* de K).

POLINÓMIO RESOLÚVEL POR RADICAIS

Uma extensão L de K diz-se uma *extensão por radicais* se existir uma torre de corpos

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_t = L$$

tal que cada L_{i+1} é uma extensão pura de L_i, para $i = 0, 1, \ldots, t-1$.

Um polinómio $p(x) \in K[x]$ diz-se *resolúvel por radicais* sobre K se existir uma extensão por radicais L de K onde $p(x)$ se decompõe em factores lineares (isto é, que contém um corpo de decomposição de $p(x)$).

Exemplos: (1) Suponhamos que uma raiz θ de um polinómio $p(x) \in \mathbb{Q}[x]$ se exprime por meio dos seguintes radicais:

$$\theta = \frac{\sqrt[5]{2 - \sqrt[3]{2}} + \sqrt{3}}{\sqrt[7]{1 - \sqrt[4]{5}}}.$$

Considerando $a_1 = \sqrt[4]{5}$, $a_2 = \sqrt[7]{1 - a_1}$, $a_3 = \sqrt[3]{2}$, $a_4 = \sqrt[5]{2 - a_3}$, $a_5 = \sqrt{3}$, temos

$$\mathbb{Q} \subseteq \underbrace{\mathbb{Q}(a_1)}_{L_1} \subseteq \underbrace{\mathbb{Q}(a_1, a_2)}_{L_2 = L_1(a_2)} \subseteq \underbrace{\mathbb{Q}(a_1, a_2, a_3)}_{L_3 = L_2(a_3)} \subseteq \underbrace{\mathbb{Q}(a_1, a_2, a_3, a_4)}_{L_4 = L_3(a_4)} \subseteq \underbrace{\mathbb{Q}(a_1, a_2, a_3, a_4, a_5)}_{L_5 = L_4(a_5)}.$$

Como

$$a_1^4 \in \mathbb{Q}, a_2^7 \in L_1, a_3^3 \in L_2, a_4^5 \in L_3, a_5^2 \in L_4,$$

então L_5 é uma extensão por radicais de $\mathbb{Q}$ que contém $\frac{a_4 + a_5}{a_2} = \theta$.

Este exemplo ilustra como, a partir de um dado elemento θ, expresso por radicais em termos dos elementos de um determinado corpo de base, se pode construir uma extensão por radicais desse corpo contendo o elemento θ.

(2) Consideremos uma equação quadrática $ax^2+bx+c=0$ ($a\neq 0$) em $\mathbb{Q}$, arbitrária. A fórmula resolvente dá-nos as suas duas raízes expressas por radicais, em termos dos seus coeficientes a, b, c:

$$r_1 = \frac{-b+\sqrt{b^2-4ac}}{2a} = \underbrace{-\frac{b}{2a}}_{\in\mathbb{Q}} \underbrace{+\sqrt{\frac{b^2-4ac}{4a^2}}}_{\theta},$$

$$r_2 = \frac{-b-\sqrt{b^2-4ac}}{2a} = \underbrace{-\frac{b}{2a}}_{\in\mathbb{Q}} \underbrace{-\sqrt{\frac{b^2-4ac}{4a^2}}}_{-\theta}.$$

É evidente que $\mathbb{Q}(\theta)$ é o corpo de decomposição do polinómio ax^2+bx+c, e é uma extensão pura de $\mathbb{Q}$ (pois $\theta^2\in\mathbb{Q}$), pelo que se trata de uma extensão por radicais de $\mathbb{Q}$. Isto mostra que qualquer polinómio de grau 2 é resolúvel por radicais.

[Do mesmo modo, não é difícil, usando as "fórmulas resolventes", provar que todos os polinómios de grau 3 e 4, com coeficientes em corpos de característica 0, também são resolúveis por radicais]

Observe-se bem o significado desta definição: qualquer raiz de $p(x)$ pertence a L e pode ser expressa a partir de elementos de K por uma sequência de operações em K e de extracção de raízes. De facto: numa extensão por radicais L de K, os elementos de L são "combinações polinomiais" de radicais de radicais de ... etc. (em número finito) ... de elementos de K, com coeficientes em K. Por outras palavras, todos os elementos de L são construídos a partir de um número finito de elementos do corpo de base K, e usando as operações $+$, $\cdot$ e $\sqrt[*]{\ }$. A definição de polinómio resolúvel por radicais é pois equivalente a dizer que as suas raízes, num corpo de decomposição, são "combinações" de radicais de radicais de ... etc. (em número finito) ... de elementos do seu corpo dos coeficientes.

GRUPO RESOLÚVEL

Um grupo G diz-se *resolúvel* se existir uma torre de subgrupos

$$\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$$

tal que, para cada $i\in\{1,2,\ldots,n\}$, G_{i-1} é um subgrupo normal de G_i e G_i/G_{i-1} é abeliano.

[Tem-se que: (1) Subgrupos de grupos resolúveis são resolúveis.
(2) Quocientes de grupos resolúveis são resolúveis.
(3) Dado um subgrupo normal de um grupo G,
G é resolúvel se e só se H e G/H são resolúveis]

Exemplos: (1) Todo o grupo abeliano G é resolúvel pois $\{e\} \subseteq G$ satisfaz a definição. Em particular, $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{A}_1$, $\mathcal{A}_2$ e $\mathcal{A}_3$ são resolúveis.

(2) $\mathcal{S}_3$ é resolúvel pois $\{id\} \subseteq \{id, (1\,2\,3), (1\,3\,2)\} \subseteq \mathcal{S}_3$ satisfaz a definição.

(3) $\mathcal{S}_4$ e $\mathcal{A}_4$ são resolúveis pois

$$\{id\} \subseteq \{id, (1\,2)(3\,4)\} \subseteq \{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \subseteq \mathcal{A}_4 \subseteq \mathcal{S}_4$$

satisfaz a definição.

(4) $\mathcal{S}_n$ $(n \geq 5)$ não é resolúvel.

[Demonstração na bibliografia]

(5) Seja $\mathbb{Z}_m^*$ o grupo das unidades de Z_m. O conjunto $\mathbb{Z}_m \times \mathbb{Z}_m^*$, munido da operação

$$(a, b) \cdot (c, d) := (a + bc, bd),$$

é um grupo

[Verifique]

a que se chama *produto semi-directo* de $\mathbb{Z}_m$ e $\mathbb{Z}_m^*$, e que se denota por $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$.

[Observe: (1) $\mathbb{Z}_3 \rtimes \mathbb{Z}_3^* \cong \mathcal{S}_3$.
(2) $\mathbb{Z}_m$ pode ser visto como um subgrupo normal de $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$
através da imersão natural $i : x \mapsto (x, 1)$ $(x \in \mathbb{Z}_m)$]

$\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$ é resolúvel pois $\{(1, 1)\} \subseteq i(\mathbb{Z}_m) \subseteq \mathbb{Z}_m \rtimes \mathbb{Z}_m^*$ satisfaz a definição de grupo resolúvel.

[O grupo $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$ é importante neste contexto por causa da proposição seguinte:

Proposição. Seja $K \subseteq \mathbb{C}$ e $x^m - a \in K[x]$ $(m \in \mathbb{N})$. O grupo de Galois deste polinómio é isomorfo a um subgrupo de $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$.

Demonstração. Se $\theta \in \mathbb{C}$ é uma raiz de índice m de a e ω é uma raiz *primitiva* de índice m da unidade (isto é, $\omega^m = 1$ e $\omega^t \neq 1$, $\forall\, 0 < t < m$; por exemplo, $\omega = \cos\frac{2\pi}{m} + i \sin\frac{2\pi}{m}$), então

$$x^m - a = \prod_{i=0}^{m-1} (x - \theta\omega^i).$$

Resulta daqui que o corpo de decomposição, em $\mathbb{C}$, de $x^m - a$ é $K(\theta, \omega)$. Assim, um elemento Φ de $Gal(x^m - a, K)$ é completamente determinado por $\Phi(\theta)$ e $\Phi(\omega)$. Como os K-automorfismos permutam as raízes de polinómios com coeficientes em K, tem-se $\Phi(\theta) = \theta\omega^{i_\Phi}$ e $\Phi(\omega) = \omega^{j_\Phi}$ para alguns $i_\Phi, j_\Phi \in \{0, 1, \ldots, m-1\}$. Vejamos que $mdc(j_\Phi, m) = 1$ para qualquer $\Phi \in Gal(x^m - a, K)$. Denotando $mdc(j_\Phi, m)$ por d temos $\Phi(\omega^{\frac{m}{d}} = \Phi(\omega)^{\frac{m}{d}} = \omega^{j_\Phi \cdot \frac{m}{d}} = \omega^{m \cdot \frac{j_\Phi}{d}} = 1$. Como Φ é injectiva, resulta que $\omega^{\frac{m}{d}} = 1$ e, consequentemente, como ω é uma raiz primitiva índice m da unidade, só pode ser $d = 1$. Assim, a correspondência

$$\begin{array}{rcl} Gal(x^m - a, K) & \to & \mathbb{Z}_m \rtimes \mathbb{Z}_m^* \\ \Phi & \mapsto & (i_\Phi \, mod \, m, j_\Phi \, mod \, m) \end{array}$$

define uma aplicação, que é um homomorfismo injectivo de grupos, como se pode verificar facilmente]

[Este resultado ainda é válido para qualquer subcorpo de um corpo de característica 0]

Corolário. *$Gal(x^m - a, K)$ é um grupo resolúvel para todo o subcorpo K de um corpo de característica zero, $a \in K$ e $m \in \mathbb{N}$.*

Demonstração. Resulta imediatamente da proposição anterior e do facto de subgrupos de grupos resolúveis serem ainda resolúveis. ∎

Teorema. [Critério de Galois]
Seja K um subcorpo de um corpo de característica zero e $p(x) \in K[x]$. Então $p(x)$ é resolúvel por radicais se e só se $Gal(p(x), K)$ for um grupo resolúvel.

[*Demonstração.* Esboçaremos somente a prova da implicação ‘‘⇒". Seja então $p(x) \in K[x]$ um polinómio resolúvel por radicais, sendo

$$K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_t = L$$

a correspondente torre de extensões puras tal que $L = L_t$ contém

um corpo de decomposição de $p(x)$. Então, para cada $i \in \{1, \ldots, t\}$, $L_i = L_{i-1}(\theta_i)$, onde cada θ_i é um radical de L_{i-1}, ou seja, $\theta_i^{m_i} \in L_{i-1}$ para algum $m_i \in \mathbb{N}$ (portanto, θ_i é raiz de $x^{m_i} - \theta_i^{m_i} \in L_{i-1}[x]$). Seja ω_i uma raiz primitiva de índice m_i da unidade. Na torre de extensões

$$\underbrace{K = L_0}_{\tilde{L}_0} \subseteq \underbrace{L_0(\theta_1, \omega_1)}_{\tilde{L}_1} \subseteq \underbrace{L_1(\theta_2, \omega_2)}_{\tilde{L}_2} \subseteq \cdots \subseteq \underbrace{L_{t-1}(\theta_t, \omega_t)}_{\tilde{L}_t}$$

cada $\tilde{L}_i$ é uma extensão de Galois de $\tilde{L}_{i-1}$ (porque é o corpo de decomposição do polinómio $x^{m_i} - \theta_i^{m_i} \in L_{i-1}[x]$) e $\tilde{L}_t$ contém um corpo de decomposição de $p(x)$. Com um pouco mais de trabalho pode construir-se uma torre de extensões

$$K = \hat{L}_0 \subseteq \hat{L}_1 \subseteq \cdots \subseteq \hat{L}_s$$

tal que cada $\hat{L}_i$ é uma extensão de Galois de K e $\hat{L}_s$ contém um corpo de decomposição de $p(x)$, que designaremos por L. Seja $G_i := Gal(\hat{L}_s, \hat{L}_{s-i})$. Pelo Teorema Fundamental de Galois podemos concluir que na torre de subgrupos

$$\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_{s-1} \subseteq G_s = Gal(\hat{L}_s, K)$$

cada subgrupo é normal e, para cada $i \in \{1, \ldots, s\}$, G_i/G_{i-1} é isomorfo a $Gal(\hat{L}_{s-i+1}, \hat{L}_{s-i}) = Gal(x^{m_{s-i+1}} - \theta_{s-i+1}^{m_{s-i+1}}, \hat{L}_{s-i})$, que é, pelo Corolário, um grupo resolúvel. Como G_0 e G_1/G_0 são resolúveis, G_1 também é; então, como G_2/G_1 é resolúvel, G_2 também é; indutivamente, podemos concluir que G_s é resolúvel. Mas $Gal(p(x), K) = Gal(L, K)$ é isomorfo a $G_s/Gal(\hat{L}_s, L)$, pelo Teorema Fundamental. Uma vez que quocientes de grupos resolúveis são resolúveis, podemos finalmente concluir que $Gal(p(x), K)$ é resolúvel]

Corolário. [Teorema de Abel-Ruffini] *Existem polinómios de grau 5 que não são resolúveis por radicais.*

Demonstração. Seja $p(x) = x^5 - 4x + 2$ e seja G o seu grupo de Galois que, pela proposição da aula anterior, pode ser considerado como sendo um subgrupo de $\mathcal{S}_5$. É fácil de ver que $p(x)$ tem precisamente 3 raízes reais $\theta_1, \theta_2, \theta_3$ e 2 raízes complexas conjugadas θ_4, θ_5. Então $L = \mathbb{Q}(\theta_1, \theta_2, \theta_3, \theta_4, \theta_5)$ é a extensão de decomposição de

$p(x)$. Pelo critério de Eisenstein, $p(x)$ é irredutível sobre $\mathbb{Q}$, logo, para qualquer raiz θ de $p(x)$, $[\mathbb{Q}(\theta) : \mathbb{Q}] = 5$. Consequentemente, $[L : \mathbb{Q}]$ é um múltiplo de 5. Isto significa, pelo Teorema da aula anterior que $|G|$ é um múltiplo de 5. Portanto, pelos Teoremas de Sylow estudados em Álgebra I, $G \subseteq \mathcal{S}_5$ contém um elemento de ordem 5, ou seja, um ciclo de comprimento 5. Por outro lado, a aplicação $z \mapsto \bar{z}$ de $\mathbb{C}$ induz um $\mathbb{Q}$-automorfismo de L que mantém fixas as três raízes reais e permuta as duas raízes complexas, a que corresponde a transposição $(4\,5)$. Em conclusão, G contém um ciclo de ordem 5 e uma transposição. Mas pode provar-se que um quaquer ciclo de ordem 5 e uma transposição geram $\mathcal{S}_5$, pelo que $G = \mathcal{S}_5$. Como $\mathcal{S}_5$ não é resolúvel, o critério de Galois assegura que $p(x)$ não é resolúvel por radicais.

■

[Observe que a mesma argumentação vale para qualquer outro polinómio de grau 5 com coeficientes em $\mathbb{Q}$ que seja irredutível e que em $\mathbb{C}$ tenha exactamente 3 raízes reais]

[Pode ver a teoria de Galois na sua forma original em H.M. Edwards, *Galois Theory*, Springer, 1984, e no apêndice 4 de J. Rotman,*Galois Theory*, Springer, 1990. A prova de Abel da inexistência de uma "fórmula resolvente" do quinto grau encontra-se no seu artigo *Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré*, J. reine angew. Math. 1 (1826) 65-84]