Do trabalho de Vandermonde (1735-96), Lagrange (1736-1813), Gauss (1777-1855), Ruffini (1765-1822), Abel (1802-29) e, principalmente, de Galois (1811-32), sobre a existência de "fórmulas resolventes" de grau ≤ 5, resultaram muitas das noções que temos vindo a estudar. Vamos agora fazer uma descrição muito concisa (por manifesta falta de tempo) do principal resultado de Galois, numa reformulação feita por Artin nos anos 30 do século passado, que resolve completamente o problema de saber quando um determinado polinómio é *resolúvel por radicais*, ou seja, quando as suas raízes são números que são combinações finitas de elementos do corpo dos seus coeficientes, usando as operações do corpo e raízes de índice arbitrário.

Como os corpos de decomposição de um polinómio, como vimos, são isomorfos é natural a seguinte definição:

GRUPO DE GALOIS de um polinómio
Seja $p(x) \in K[x]$. Chama-se *grupo de Galois de* $p(x)$ *sobre* K (ou *grupo de Galois da equação* $p(x) = 0$), que denotaremos por $Gal(p(x), K)$, ao grupo $Gal(L, K)$, onde L é uma qualquer extensão de decomposição de $p(x)$ sobre K.

Os automorfismos de Galois de uma extensão L de K permutam as raízes, nessa extensão, dos polinómios com coeficientes no corpo de base K. De facto, se $p(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$, $\theta \in L$ é uma raiz de $p(x)$ e $\Phi \in Gal(L, K)$, então $\Phi(\theta)$ é também uma raiz de $p(x)$:

$$p(\Phi(\theta)) = \sum_{i=0}^{n} a_i \Phi(\theta)^i = \sum_{i=0}^{n} \Phi(a_i)\Phi(\theta^i) = \sum_{i=0}^{n} \Phi(a_i\theta^i) = \Phi\Big(\sum_{i=0}^{n} a_i\theta^i\Big) = \Phi(0) = 0.$$

Portanto, é natural identificar o grupo de Galois de um polinómio $p(x)$ com um subgrupo de permutações[1] das raízes de $p(x)$. Se L é uma extensão de decomposição de $p(x)$, e $R = \{\theta_1, \ldots, \theta_n\}$ são as raízes distintas de $p(x)$, então $L = K(\theta_1, \ldots, \theta_n)$. Se soubermos como Φ transforma as raízes de $p(x)$, então sabemos como Φ transforma todo o elemento de $L = K(\theta_1, \ldots, \theta_n)$. Portanto, o automorfismo Φ é completamente descrito pelas imagens das raízes θ_i $(i = 1, 2, \ldots, n)$. Por outro lado, como acabámos de ver, se $\Phi \in Gal(p(x), K)$, então Φ transforma raízes de $p(x)$ em raízes de $p(x)$. Portanto

$$\Phi(\theta_i) = \theta_{\tilde{\Phi}(i)} \text{ para algum } \tilde{\Phi}(i) \in \{1, 2, \ldots, n\}.$$

[1]Era assim que Galois concebia o grupo que hoje tem o seu nome, ainda antes de se ter formalizado sequer o conceito de grupo!

É evidente que, como Φ é injectiva, $\tilde{\Phi} : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ é uma permutação.

Em conclusão, todo o $\Phi \in Gal(L, K)$ fica completamente descrito pela respectiva permutação $\tilde{\Phi} \in \mathcal{S}_n$ e a aplicação $\Phi \mapsto \tilde{\Phi}$ é claramente um homomorfismo injectivo $Gal(p(x), K) \to \mathcal{S}_n$:

$$\theta_{\widetilde{\Phi_1 \circ \Phi_2}(i)} = (\Phi_1 \circ \Phi_2)(\theta_i) = \Phi_1(\theta_{\widetilde{\Phi_2}(i)}) = \theta_{\widetilde{\Phi_1}\widetilde{\Phi_2}(i)} \Rightarrow \widetilde{\Phi_1 \circ \Phi_2} = \widetilde{\Phi_1} \circ \widetilde{\Phi_2}.$$

Podemos assim identificar $Gal(p(x), K)$ com um subgrupo do grupo das permutações de R, e concluir o seguinte:

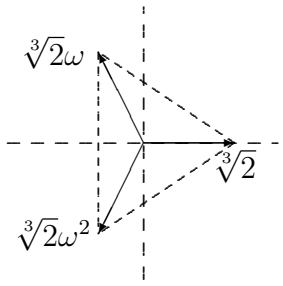
Proposição. *Se $p(x) \in K[x]$ tem n raízes distintas no seu corpo de decomposição então $Gal(p(x), K)$ é isomorfo a um subgrupo do grupo simétrico $\mathcal{S}_n$.* ∎

Note que, mesmo quando $p(x)$ é irredutível, $Gal(p(x), K)$ pode ser isomorfo a um subgrupo próprio de $\mathcal{S}_n$, como os exemplos (2) e (3) abaixo mostram.

Exemplos: (1) Vejamos que $Gal(x^3 - 2, \mathbb{Q}) \cong \mathcal{S}_3$. Da Proposição sabemos que o grupo de Galois $Gal(x^3 - 2, \mathbb{Q})$ é isomorfo a um subgrupo de $\mathcal{S}_3$, pelo que bastará assegurar que $|Gal(x^3 - 2, \mathbb{Q})| = 6$. Em primeiro lugar, como em $\mathbb{C}$ temos

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2),$$

onde ω é uma raiz cúbica *primitiva* da unidade (isto é, $\omega^3 = 1$ e $\omega^t \neq 1 \; \forall \; 0 < t < 3$),



então $\mathbb{Q}(\omega, \sqrt[3]{2})$ é o corpo de decomposição de $x^3 - 2$ em $\mathbb{C}$. Como $x^3 - 2$ é o polinómio mínimo de $\sqrt[3]{2}\omega^t$ $(t = 0, 1, 2)$ sobre $\mathbb{Q}$ e $x^2 + x + 1$ é o polinómio mínimo de ω sobre $\mathbb{Q}$, então

$$[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}(\omega)]}_{\leq 3} \underbrace{[\mathbb{Q}(\omega) : \mathbb{Q}]}_{=2} \leq 6.$$

Por outro lado, $\mathbb{Q}(\omega, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}\omega, \omega)$ e

$$[\mathbb{Q}(\sqrt[3]{2}\omega, \omega) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[3]{2}\omega, \omega) : \mathbb{Q}(\sqrt[3]{2}\omega)]}_{\leq 2} \underbrace{[\mathbb{Q}(\sqrt[3]{2}\omega) : \mathbb{Q}]}_{=3} \leq 6.$$

Portanto, $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] \leq 6$ e é divisível por 2 e 3, logo $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6$. Isto significa que $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega\}$ constitui uma base da extensão $\mathbb{Q}(\omega, \sqrt[3]{2})$. É facil de ver (de modo análogo aos exemplos da aula anterior) que existem precisamente seis $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\omega, \sqrt[3]{2})$.

`[Descreva esses seis automorfismos explicitamente]`

Como $|\mathcal{S}_3| = 3! = 6$, teremos necessariamente $Gal(x^3 - 2, \mathbb{Q}) \cong \mathcal{S}_3$.

(2) Consideremos o polinómio $p(x) = x^4 - 2$, que é irredutível sobre $\mathbb{Q}$. As suas quatro raízes em $\mathbb{C}$ são

$$\theta_1 = \sqrt[4]{2},\ \theta_2 = \sqrt[4]{2}i,\ \theta_3 = -\sqrt[4]{2},\ \theta_4 = -\sqrt[4]{2}i,$$

e $\mathbb{Q}(i, \sqrt[4]{2})$ é o seu corpo de decomposição. Para definir um $\mathbb{Q}$-automorfismo de $\mathbb{Q}(i, \sqrt[4]{2})$, basta fixarmos as imagens das raízes θ_1 e θ_2 (pois as imagens de θ_3 e θ_4 ficam automaticamente definidas). Por exemplo,

$$\begin{array}{rcl} \theta_1 & \mapsto & \theta_2 \\ \theta_2 & \mapsto & \theta_3 \end{array}$$

define um $\mathbb{Q}$-automorfismo $\alpha : \mathbb{Q}(i, \sqrt[4]{2}) \to \mathbb{Q}(i, \sqrt[4]{2})$. É óbvio que $\alpha(\theta_3) = \theta_4$ e $\alpha(\theta_4) = \theta_1$ (e $\alpha(i) = i$). Pelo isomorfismo da Proposição, a este automorfismo corresponde a permutação $(1\,2\,3\,4)$ de $\mathcal{S}_4$.

Outro exemplo: a $\beta : \mathbb{Q}(i, \sqrt[4]{2}) \to \mathbb{Q}(i, \sqrt[4]{2})$, definido por $\beta(\theta_1) = \theta_1$ e $\beta(\theta_2) = \theta_4$, corresponde a permutação $(2\,4)$.

No entanto, nem todas as 24 permutações de $\mathcal{S}_4$ correspondem a elementos de $Gal(p(x), \mathbb{Q})$, uma vez que este grupo tem, no máximo, 8 elementos:

É evidente que $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(i)] = 4$ e $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, logo $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$. Então, pelo Teorema da aula anterior, existem, no máximo, oito $\mathbb{Q}$-automorfismos de $\mathbb{Q}(i, \sqrt[4]{2})$, isto é, $|Gal(p(x), \mathbb{Q})| \leq 8$ Portanto, neste caso, $Gal(p(x), \mathbb{Q})$ é isomorfo a um subgrupo próprio de $\mathcal{S}_4$.

Por exemplo, o ciclo $(1\,2)$ não corresponde a nenhum $\mathbb{Q}$-automorfismo $\Phi : \mathbb{Q}(i, \sqrt[4]{2}) \to \mathbb{Q}(i, \sqrt[4]{2})$, uma vez que Φ, para originar tal ciclo, teria que satisfazer $\Phi(\theta_1) = \theta_2$, $\Phi(\theta_2) = \theta_1$, $\Phi(\theta_3) = \theta_3$ e $\Phi(\theta_4) = \theta_4$, mas tal Φ não é, claramente, um homomorfismo de corpos (com efeito, $\theta_1 + \theta_3 = 0$ mas $\Phi(\theta_1) + \Phi(\theta_3) = \theta_2 + \theta_3 \neq 0$).

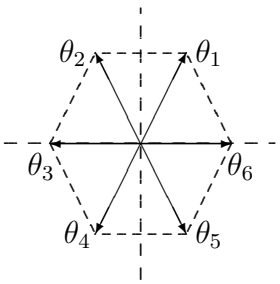
`[Conclua que` $|Gal(p(x)), \mathbb{Q})| = 8$`, observando que, respectivamente,`
$\theta_1 \mapsto \theta_1$ `e` $\theta_2 \mapsto \theta_2$`,` $\theta_1 \mapsto \theta_1$ `e` $\theta_2 \mapsto \theta_4$`,` $\theta_1 \mapsto \theta_2$ `e` $\theta_2 \mapsto \theta_1$`,`
$\theta_1 \mapsto \theta_2$ `e` $\theta_2 \mapsto \theta_3$`,` $\theta_1 \mapsto \theta_3$ `e` $\theta_2 \mapsto \theta_2$`,` $\theta_1 \mapsto \theta_3$ `e` $\theta_2 \mapsto \theta_4$`,`

$\theta_1 \mapsto \theta_4$ e $\theta_2 \mapsto \theta_1$, $\theta_1 \mapsto \theta_4$ e $\theta_2 \mapsto \theta_3$,
definem oito $\mathbb{Q}$-automorfismos de $\mathbb{Q}(i, \sqrt[4]{2})$.
Portanto, $Gal(p(x)), \mathbb{Q})$é isomorfo a
$\{id, (2\,4), (1\,2)(3\,4), (1\,2\,3\,4), (1\,3), (1\,3)(2\,4), (1\,4\,3\,2), (1\,4)(2\,3)\}$.
Este grupo G é isomorfo ao grupo diedral D_4 das simetrias de um quadrado, pois é gerado pelos elementos $\sigma = (2\,4)$ e $\tau = (1\,2\,3\,4)$, de ordens 2 e 4, que satisfazem a relação $(\tau\sigma)^2 = id$:
$G = \{id, \sigma, \sigma\tau, \tau, \sigma\tau^2, \tau^2, \tau^3, \sigma\tau^3\}$]

(3) Seja $L \subseteq \mathbb{C}$ a extensão de decomposição sobre $\mathbb{Q}$ do polinómio irredutível $p(x) = x^6 - 2$. As raízes de $p(x)$ são

$$\theta_k = \sqrt[6]{2}e^{\frac{2k\pi i}{6}}, \quad k = 1, \ldots, 6.$$

Neste caso, $|\mathcal{S}_6| = 6! = 720$ mas $|Gal(p(x), \mathbb{Q})| < 720$; por exemplo, não existe um automorfismo do grupo de Galois que corresponda à transposição $(1\,6)$, pois $\theta_3 + \theta_6 = 0$ mas $\theta_3 + \theta_1 \neq 0$, como se observa imediatamente na representação, no plano complexo, das raízes de $p(x)$:



Outro exemplo: como $(\theta_1 + \theta_5)^6 = \theta_6^6 = 2$, não existem automorfismos do grupo de Galois que correspondam às permutações $(1\,3)(5\,6)$ e $(1\,6)(3\,5)$. Muitos outros elementos de $\mathcal{S}_6$ podem ser excluídos; de facto, como veremos mais adiante,

$$|Gal(x^6 - 2, \mathbb{Q})| = 12.$$

EXTENSÃO DE GALOIS

Diz-se que uma extensão finita L de K é uma *extensão de Galois* se L for um corpo de decomposição de algum polinómio de $K[x]$.

Trabalhando a demonstração (que não estudámos) do teorema da aula anterior sobre extensões de isomorfismos a corpos de decomposição, não é difícil provar o seguinte resultado:

Teorema. *Seja L uma extensão finita de K. Então:*

(1) $|Gal(L,K)| \leq [L:K]$.

(2) *Se L é uma extensão de Galois de K então* $|Gal(L,K)| = [L:K]$.

[A demonstração pode ser consultada em *Introdução à Álgebra*, R. Loja Fernandes e M. Ricou, IST Press, 2004]

Exemplos: (1) A observação, no exemplo (2) acima, que $|Gal(p(x),\mathbb{Q})| = 8$, é uma consequência imediata do Teorema, uma vez que $\mathbb{Q}(i,\sqrt[4]{2})$ é uma extensão de Galois de $\mathbb{Q}$ e $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}] = 8$.

(2) No exemplo (3), $\mathbb{Q}(\sqrt[6]{2}, e^{\frac{2\pi}{3}i})$ é uma extensão de decomposição de $p(x) = x^6 - 2$. Como

$$[\mathbb{Q}(\sqrt[6]{2}, e^{\frac{2\pi}{3}i}):\mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{2}, e^{\frac{2\pi}{3}i}):\mathbb{Q}(\sqrt[6]{2})] \cdot [\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}] = 2 \cdot 6 = 12,$$

então $|Gal(x^6-2,\mathbb{Q})| = 12$, como tínhamos anunciado.