A partir da proposição da aula anterior é possível provar, por indução sobre o grau $[L_1 : K_1]$, o seguinte resultado (não o faremos na aula):

Teorema. *Seja $\phi : K_1 \to K_2$ um isomorfismo de corpos, $p(x) \in K_1[x]$ e $p^\phi(x) \in K_2[x]$. Se L_1 é uma extensão de decomposição de $p(x)$ e L_2 é uma extensão de decomposição de $p^\phi(x)$, existe um isomorfismo $\Phi : L_1 \to L_2$ tal que $\Phi|_{K_1} = \phi$.*

$$\begin{array}{ccc} L_1 & \overset{\Phi}{\underset{\cong}{\rightarrowtail}} & L_2 \\ \uparrow & & \uparrow \\ K_1 & \underset{\cong}{\overset{\phi}{\rightarrowtail}} & K_2 \end{array}$$

O número de tais prolongamentos é $\leq [L_1 : K_1]$, e é precisamente $[L_1 : K_1]$ quando $p^\phi(x)$ tem raízes distintas em L_2.

[A demonstração é por indução sobre $[L_1 : K_1]$. Se $[L_1 : K_1] = 1$, então $p(x) = a_n \prod_{i=1}^{n}(x - \theta_i)$, onde $\theta_i \in L_1 = K_1$. Como as raízes de um polinómio geram o seu corpo de decomposição, concluímos que $L_2 = K_2$, logo existe apenas 1 $(= [L_1 : K_1])$ prolongamento. Suponhamos que $[L_1 : K_1] > 1$. Então $p(x)$ possui um factor irredutível $q(x)$ de grau ≥ 1. Seja θ uma raiz de $q(x)$ em L_1. Pela Proposição, o isomorfismo $\phi : K_1 \to K_2$ pode ser prolongado num homomorfismo injectivo $\overline{\phi} : K_1(\theta) \to L_2$ e existem tantos prolongamentos quantas as raízes distintas de $q^\phi(x)$ em L_2. Podemos considerar L_1 e L_2 como corpos de decomposição de $p(x)$ e $p^\phi(x)$ sobre $K_1(\theta)$ e $\overline{\phi}(K_1(\theta))$, respectivamente. Como $[L_1 : K_1(\theta)] = [L_1 : K_1]/[K_1(\theta) : K_1] = [L_1 : K_1]/gr(q(x)) < [L_1 : K_1]$, podemos utilizar a hipótese de indução para prolongar $\overline{\phi}$ num isomorfismo $\Phi : L_1 \to L_2$, e o número de prolongamentos é $\leq [L_1 : K_1(\theta)]$, sendo precisamente igual a $[L_1 : K_1(\theta)]$ se $p^\phi(x)$ tem raízes distintas em L_2. Combinando estes resultados, é fácil de ver que Φ é um prolongamento de ϕ, e o número de prolongamentos de ϕ deste tipo é precisamente $[L_1 : K_1(\theta)] \cdot gr(q(x)) = [L_1 : K_1(\theta)] \cdot [K_1(\theta) : K_1] = [L_1 : K_1]$ se $p^\phi(x)$ tem raízes distintas em L_2. Finalmente, observe-se que obtemos todos os prolongamentos de ϕ se prolongarmos primeiro a

$K_1(\theta)$ e depois a L_1. Com efeito, se Φ é um prolongamento de ϕ a L_1, então a sua restrição a $K_1(\theta)$ fornece um homomorfismo injectivo $K_1(\theta) \to L_2$, que é necessariamente um dos prolongamentos de ϕ fornecidos pela Proposição.■]

Se neste teorema tomarmos $K_1 = K_2 = K$ e $\phi = id$, obtemos imediatamente:

Corolário. *Dois quaisquer corpos de decomposição de $p(x) \in K[x]$ são isomorfos (por um isomorfismo que deixa fixos os elementos de K).* ■

Exemplo: O polinómio $x^3 - 2$ é irredutível sobre $\mathbb{Q}$. Formemos a extensão $L = \mathbb{Q}[x]/(x^3 - 2)$, e seja $\theta_1 = x + (x^3 - 2)$. Já sabemos (aula anterior) que L é uma extensão de $\mathbb{Q}$ da forma $\mathbb{Q}(r_1)$, e em L o polinómio $x^3 - 2$ admite uma factorização através do monómio $(x - \theta_1)$, nomeadamente $(x - \theta_1)(x^2 + \theta_1 x + \theta_1^2)$. O polinómio $x^2 + \theta_1 x + \theta_1^2$ é irredutível sobre $\mathbb{Q}(\theta_1)$.

[Verifique]

Podemos então formar uma nova extensão $M = \mathbb{Q}(\theta_1)[x]/(x^2 + \theta_1 x + \theta_1^2)$. Designando por θ_2 o elemento $x+(x^2+\theta_1 x+\theta_1^2)$ desta extensão, vemos que $M = \mathbb{Q}(\theta_1, \theta_2)$. Em $\mathbb{Q}(\theta_1, \theta_2)[x]$ temos finalmente a factorização $x^3 - 2 = (x - \theta_1)(x - \theta_2)(x - \theta_3)$ de $x^3 - 2$ em factores lineares. Portanto, $M = \mathbb{Q}(\theta_1, \theta_2) = \mathbb{Q}(\theta_1, \theta_2, \theta_3)$ é uma extensão de decomposição (abstracta) de $x^3 - 2$, que tem grau $[\mathbb{Q}(\theta_1, \theta_2, \theta_3) : \mathbb{Q}] = 3 \cdot 2 = 6$.

Podemos construir uma outra extensão de decomposição M_2 considerando o subcorpo de $\mathbb{C}$ gerado por $\mathbb{Q}$ e as três raízes complexas de $x^3 - 2$ (que são $\sqrt[3]{2}$, $\sqrt[3]{2}(-1+i\sqrt{3})/2$ e $\sqrt[3]{2}(-1-i\sqrt{3})/2$). Pelos resultados que acabámos de ver, existem isomorfismos $M \to M_2$ que deixam fixos os números racionais e transformam $\theta_1, \theta_2, \theta_3$ em qualquer uma das raízes $\sqrt[3]{2}$, $\sqrt[3]{2}(-1 + i\sqrt{3})/2$, $\sqrt[3]{2}(-1 - i\sqrt{3})/2$.

A ideia fulcral da Teoria de Galois consiste em substituir um problema de extensões de corpos por um problema de teoria dos grupos. Os grupos em questão são os que agora introduzimos.

AUTOMORFISMOS DE GALOIS

Seja L uma extensão de K. Um automorfismo Φ de L diz-se um *K-automorfismo* (ou *automorfismo de Galois*) se deixa fixos os elementos de K, isto é, $\Phi|_K = id$.

Se Φ_1 e Φ_2 são K-automorfismos de L, então $\Phi_1 \circ \Phi_2$ ainda é um K-automorfismo. É evidente então que o conjunto dos K-automorfismos de L, munido da operação usual de composição de funções, forma um grupo.

GRUPO DE GALOIS de uma extensão

Chama-se *grupo de Galois* de uma extensão L de K, que se denota por $Gal(L, K)$, ao grupo dos K-automorfismos de L.

Como observámos na aula anterior, os automorfismos de Galois $\Phi : L \to L$ de uma extensão L de K permutam as raízes em L dos polinómios com coeficientes no corpo de base K. De facto, sendo $p(x) \in K[x]$ e θ uma raiz de $p(x)$ em L, então $\Phi(\theta)$ é também uma raiz de $p(x)$:

$$p(\Phi(\theta)) = \Phi(p(\theta)) = \Phi(0) = 0.$$

Exemplos: (1) Seja $L = \mathbb{Q}(\sqrt{2})$. O elemento $\sqrt{2}$ tem polinómio mínimo $x^2 - 2$. Como vimos na aula anterior, qualquer $\mathbb{Q}$-automorfismo $\Phi : L \to L$ transforma raízes deste polinómio em raízes. Existem, pois, precisamente dois $\mathbb{Q}$-automorfismos:

$$\begin{array}{rccc} \Phi_{\sqrt{2}}: & \mathbb{Q}(\sqrt{2}) & \to & \mathbb{Q}(\sqrt{2}) \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{2} & \mapsto & \sqrt{2} \end{array} \quad \text{e} \quad \begin{array}{rccc} \Phi_{-\sqrt{2}}: & \mathbb{Q}(\sqrt{2}) & \to & \mathbb{Q}(\sqrt{2}) \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{2} & \mapsto & -\sqrt{2}. \end{array}$$

O primeiro é a identidade e o segundo aplica cada elemento $a + b\sqrt{2}$ de $\mathbb{Q}(\sqrt{2})$ em $a - b\sqrt{2}$. Portanto, $Gal(L, \mathbb{Q}) = \{id, \Phi_{-\sqrt{2}}\}$, que é um grupo isomorfo a $\mathbb{Z}_2$.

(2) Quanto ao grupo de Galois da extensão $\mathbb{C}$ sobre $\mathbb{R}$, como $\mathbb{C} = \mathbb{R}(i)$, cada $\Phi \in Gal(\mathbb{C}, \mathbb{R})$ é completamente determinado por $\Phi(i)$. Mas, como $x^2 + 1$ é o polinómio mínimo de i sobre $\mathbb{R}$, tem-se pela proposição da aula anterior que $\Phi(i) = \pm i$. Assim, $Gal(\mathbb{C}, \mathbb{R}) = \{id, z \mapsto \overline{z}\}$ é também isomorfo a $\mathbb{Z}_2$.

(3) Seja $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Cada $\Phi \in Gal(L, \mathbb{Q})$ é completamente determinado pela sua acção no conjunto $\{\sqrt{2}, \sqrt{3}\}$. A restrição $\Phi|_{\mathbb{Q}(\sqrt{2})} : \mathbb{Q}(\sqrt{2}) \to L$ é um homomorfismo injectivo que mantém fixos os elementos de $\mathbb{Q}$. Então, pela proposição da aula anterior, só há duas possibilidades para esta restrição, como vimos no Exemplo

(1): é a identidade ou aplica cada elemento $a+b\sqrt{2}$ de $\mathbb{Q}(\sqrt{2})$ em $a-b\sqrt{2}$. Portanto, Φ prolonga o isomorfismo identidade de $\mathbb{Q}(\sqrt{2})$ ou prolonga o isomorfismo $\Phi_{-\sqrt{2}}$ de $\mathbb{Q}(\sqrt{2})$. Usando novamente a proposição da aula anterior, como x^2-3 é o polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2})$, estes dois isomorfismos de $\mathbb{Q}(\sqrt{2})$ só podem ser prolongados a $\mathbb{Q}(\sqrt{2},\sqrt{3})$ aplicando $\sqrt{3}$ em $\sqrt{3}$ ou $-\sqrt{3}$. Portanto, só existem 4 possibilidades para Φ: a identidade e

$$\Phi(\sqrt{2}) = -\sqrt{2},\ \Phi(\sqrt{3}) = \sqrt{3};$$

$$\Phi(\sqrt{2}) = \sqrt{2},\ \Phi(\sqrt{3}) = -\sqrt{3};$$

$$\Phi(\sqrt{2}) = -\sqrt{2},\ \Phi(\sqrt{3}) = -\sqrt{3}.$$

O grupo de Galois tem, pois, neste caso, 4 elementos, que designamos respectivamente por $\Phi_0, \Phi_1, \Phi_2, \Phi_3$:

$$\Phi_0(a+b\sqrt{2}+c\sqrt{3}) = a+b\sqrt{2}+c\sqrt{3},$$
$$\Phi_1(a+b\sqrt{2}+c\sqrt{3}) = a-b\sqrt{2}+c\sqrt{3},$$
$$\Phi_2(a+b\sqrt{2}+c\sqrt{3}) = a+b\sqrt{2}-c\sqrt{3},$$
$$\Phi_3(a+b\sqrt{2}+c\sqrt{3}) = a-b\sqrt{2}-c\sqrt{3}.$$

A tabela deste grupo é a seguinte:

$\circ$	Φ_0	Φ_1	Φ_2	Φ_3
Φ_0	Φ_0	Φ_1	Φ_2	Φ_3
Φ_1	Φ_1	Φ_0	Φ_3	Φ_2
Φ_2	Φ_2	Φ_3	Φ_0	Φ_1
Φ_3	Φ_3	Φ_2	Φ_1	Φ_0

Em conclusão, $Gal(L,\mathbb{Q})$ é isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

(4) Seja K um corpo de característica p tal que $K \neq K^p$. Se $a \notin K^p$, o polinómio $q(x) = x^p - a$ é irredutível sobre K. Seja L uma extensão de decomposição de $q(x)$. Em L temos $q(x) = (x-\theta)^p$, logo $L = K(\theta)$. Se $\Phi : L \to L$ é um K-automorfismo, então $\Phi(\theta) = \theta$ e concluímos que $\Phi = id$. Isto mostra que, neste exemplo, o grupo de Galois $Gal(L,K)$ é trivial.