[Conclusão da aula anterior: corpos de decomposição]

HOMOMORFISMO DE EXTENSÕES

Seja L_1 uma extensão de K_1 e L_2 uma extensão de K_2. Um homomorfismo de corpos $\Phi : L_1 \to L_2$ diz-se um *homomorfismo de extensões* se $\Phi(K_1) \subseteq K_2$.

Vamos analisar a seguinte questão:

> *Dado um isomorfismo de corpos $\phi : K_1 \to K_2$, é possível prolongar ϕ a um isomorfismo de extensões $\Phi : L_1 \to L_2$?*

$$\begin{tikzcd} L_1 \arrow[r, dashed, "\Phi?", "\cong"'] & L_2 \\ K_1 \arrow[u, tail] \arrow[r, "\phi", "\cong"'] & K_2 \arrow[u, tail] \end{tikzcd}$$

[$K_i \rightarrowtail L_i$ `denota a inclusão de` K_i `em` L_i $(i = 1, 2)$]

O estudo desta questão servirá, em particular, para provarmos a unicidade (a menos de um isomorfismo) das extensões de decomposição.

Dados um homomorfismo de corpos $\phi : K_1 \to K_2$ e um polinómio

$$p(x) = a_n x^n + \cdots + a_1 x + a_0 \in K_1[x],$$

designaremos por $p^\phi(x)$ o polinómio

$$\phi(a_n)x^n + \cdots + \phi(a_1)x + \phi(a_0)$$

de $K_2[x]$.

Proposição. *Seja $\phi : K_1 \to K_2$ um isomorfismo de corpos, L_1 e L_2 extensões de K_1 e K_2, e $\theta \in L_1$ um elemento algébrico sobre K_1 com polinómio mínimo $m(x)$. O isomorfismo ϕ pode ser prolongado a um homomorfismo injectivo de extensões $\Phi : K_1(\theta) \to L_2$ se e só se o polinómio $m^\phi(x)$ tem uma raiz em L_2. O número de prolongamentos é igual ao número de raízes distintas de $m^\phi(x)$ em L_2.*

Demonstração. Suponhamos que $m(x) = a_n x^n + \cdots + a_1 x + a_0$. Se $\Phi : K_1(\theta) \to L_2$ é um prolongamento de ϕ, então $\Phi(\theta) \in L_2$ é uma raiz de $m^\phi(x)$:

$$\begin{aligned} m^\phi(\Phi(\theta)) &= \phi(a_n)\Phi(\theta)^n + \cdots + \phi(a_1)\Phi(\theta) + \phi(a_0) \\ &= \Phi(a_n)\Phi(\theta)^n + \cdots + \Phi(a_1)\Phi(\theta) + \Phi(a_0) \\ &= \Phi(a_n\theta^n + \cdots + a_1\theta + a_0) \\ &= \Phi(m(\theta)) = \Phi(0) = 0. \end{aligned}$$

Reciprocamente, seja λ uma raiz de $m^\phi(x)$ em L_2. É fácil verificar que

$$\begin{array}{rccc} \Phi_\lambda : & K_1(\theta) & \to & L_2 \\ & a \in K_1 & \mapsto & \phi(a) \\ & \theta & \mapsto & \lambda \end{array}$$

define um homomorfismo injectivo de corpos que prolonga ϕ. Trata-se do único homomorfismo de corpos tal que $\Phi|_{K_1} = \phi$ e $\Phi(\theta) = \lambda$.

É evidente que o número destes prolongamentos é assim igual ao número de raízes distintas de $m^\phi(x)$ em L_2. ∎