Seja $L \supseteq K$ uma extensão de $L$ e seja $\theta \in L$ um elemento algébrico sobre $K$. Consideremos o conjunto

$$I = \{p(\boldsymbol{x}) \in K[x] : p(\theta) = 0\}.$$

[Exercício: $I$ é um ideal de $K[x]$]

Como $I$ é um ideal de $K[x]$, pela demonstração do teorema da Aula 8, podemos concluir que existe um polinómio mónico $m_\theta(\boldsymbol{x}) \in K[x]$, único, tal que $I = (m_\theta(\boldsymbol{x}))$.

Este polinómio satisfaz as seguintes propriedades:

**Proposição.** *Seja $\theta \in L$ um elemento algébrico sobre $K$. Então:*

(1) *$m_\theta(\boldsymbol{x})$ é irredutível sobre $K$.*

(2) *Para cada $p(\boldsymbol{x}) \in K[x]$, $p(\theta) = 0$ se e só se $m_\theta(\boldsymbol{x}) \mid p(\boldsymbol{x})$.*

(3) *$m_\theta(\boldsymbol{x})$ é o polinómio mónico não-nulo em $K[x]$ de menor grau que tem $\theta$ por raiz.*

*Demonstração.* (1) Como $m_\theta(\boldsymbol{x})$ tem uma raiz, tem de ser de grau $\geq 1$ necessariamente. Suponhamos que $m_\theta(\boldsymbol{x})$ era redutível, isto é, que $m_\theta(\boldsymbol{x}) = p_1(\boldsymbol{x})p_2(\boldsymbol{x})$, com

$$1 \leq gr(p_1(\boldsymbol{x})), gr(p_2(\boldsymbol{x})) < gr(m_\theta(\boldsymbol{x})). \tag{A}$$

Então $0 = m_\theta(\theta) = p_1(\theta)p_2(\theta)$, donde $p_1(\theta) = 0$ ou $p_2(\theta) = 0$. Qualquer uma destas possibilidades contradiz (A): se $p_i(\theta) = 0$ ($i = 1$ ou $i = 2$), então $p_i(\boldsymbol{x}) \in I$, ou seja, $m_\theta(\boldsymbol{x}) \mid p_i(\boldsymbol{x})$, donde $gr(p_i(\boldsymbol{x})) \geq gr(m_\theta(\boldsymbol{x})$.

(2) É evidente: $m_\theta(\boldsymbol{x}) \mid p(\boldsymbol{x}) \Leftrightarrow p(\boldsymbol{x}) \in (m_\theta(\boldsymbol{x})) = I \Leftrightarrow p(\theta) = 0$.

(3) É consequência imediata de (2): seja $p(\boldsymbol{x})$ mónico; se $p(\theta) = 0$ então $m_\theta(\boldsymbol{x}) \mid p(\boldsymbol{x})$, logo $p(\boldsymbol{x}) = m_\theta(\boldsymbol{x})$ ou $gr(p(\boldsymbol{x})) > gr(m_\theta(\boldsymbol{x}))$. ∎

---

**POLINÓMIO MÍNIMO**

O polinómio $m_\theta(\boldsymbol{x})$ chama-se o *polinómio mínimo* de $\theta$ sobre $K$.

---

Exemplos: $\boldsymbol{x}^2+1$ é o polinómio mínimo de $i$ sobre $\mathbb{R}$, $\boldsymbol{x}^2-2$ é o polinómio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$ e $\boldsymbol{x}-\sqrt{2}$ é o polinómio mínimo de $\sqrt{2}$ sobre $\mathbb{R}$.

**Teorema.** *Seja $\theta$ algébrico sobre $K$, com polinómio mínimo $m_\theta(\boldsymbol{x})$ sobre $K$. Então cada elemento $\lambda \in K(\theta)$ tem uma expressão única na forma $\lambda = p(\theta)$ onde $p(\boldsymbol{x}) \in K[x]$ é tal que $gr(p(\boldsymbol{x})) < gr(m_\theta(\boldsymbol{x}))$.*

[Por outras palavras: se $gr(m_\theta(\boldsymbol{x})) = n$ então existem únicos $a_0, a_1, \ldots, a_{n-1} \in K$ tais que $\lambda = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$]

*Demonstração.* Comecemos por provar que todo o elemento $\lambda$ de $K(\theta)$ se pode escrever na forma $p(\theta)$ para algum $p(\boldsymbol{x}) \in K[x]$ tal que $gr(p(\boldsymbol{x})) < n$. É evidente que

$$K \cup \{\theta\} \subseteq \{p(\theta) : p(\boldsymbol{x}) \in K[x]\} \subseteq K(\theta).$$

Mas $\mathcal{S} := \{p(\theta) : p(\boldsymbol{x}) \in K[x]\}$ é um subcorpo de $K(\theta)$:

- Se $p(\theta), q(\theta) \in \mathcal{S}$, é evidente que $p(\theta) - q(\theta) \in \mathcal{S}$, pois $p(\boldsymbol{x}) - q(\boldsymbol{x}) \in K[x]$.
- Se $p(\theta), q(\theta) \in \mathcal{S}$, com $q(\theta \neq 0$ então, como $\theta$ não é raiz de $q(\boldsymbol{x})$, pela propriedade (2) na Proposição, $m_\theta(\boldsymbol{x}) \nmid q(\boldsymbol{x})$, donde $\mathrm{mdc}(m_\theta(\boldsymbol{x}), q(\boldsymbol{x})) = 1$, uma vez que $m_\theta(\boldsymbol{x})$ é irredutível sobre $K$. Isto significa que existem polinómios $a(\boldsymbol{x}), b(\boldsymbol{x}) \in K[x]$ tais que $1 = a(\boldsymbol{x})m_\theta(\boldsymbol{x}) + b(\boldsymbol{x})q(\boldsymbol{x})$. Mas então $1 = a(\theta)m_\theta(\theta) + b(\theta)q(\theta) = b(\theta)q(\theta)$, o que mostra que $b(\theta)$ é o inverso de $q(\theta)$ em $K(\theta)$. Portanto, $p(\theta)q(\theta)^{-1} = p(\theta)b(\theta)$, que ainda pertence a $\mathcal{S}$, porque $p(\boldsymbol{x})q(\boldsymbol{x}) \in K[x]$.

Logo, $\{p(\theta) : p(\boldsymbol{x}) \in K[x]\} = K(\theta)$.

Observemos agora que

$$\{p(\theta) : p(\boldsymbol{x}) \in K[x]\} = \{p(\theta) : p(\boldsymbol{x}) \in K[x],\ gr(p(\boldsymbol{x})) < n\},$$

uma vez que, para cada $p(\boldsymbol{x}) \in K[x]$, $p(\boldsymbol{x}) = q(\boldsymbol{x})m_\theta(\boldsymbol{x}) + r(\boldsymbol{x})$, com $gr(r(\boldsymbol{x})) < gr(m_\theta(\boldsymbol{x}))$, donde $p(\theta) = q(\theta)m_\theta(\theta) + r(\theta) = r(\theta)$.

Em conclusão, $K(\theta) = \{p(\theta) : p(\boldsymbol{x}) \in K[x],\ gr(p(\boldsymbol{x})) < n\}$, o que mostra que todo o elemento se pode escrever na forma desejada. Finalmente, provemos a unicidade: se $\lambda = p(\theta) = q(\theta)$, com $p(\boldsymbol{x}), q(\boldsymbol{x}) \in K[x]$ ambos de grau $< n$, então $gr(p(\boldsymbol{x}) - q(\boldsymbol{x})) < n$. Mas $p(\theta) - q(\theta) = 0$. Se $p(\boldsymbol{x}) \neq q(\boldsymbol{x})$, o polinómio $p(\boldsymbol{x}) - q(\boldsymbol{x})$ seria um polinómio não-nulo de grau $< n$ com a raiz $\theta$, o que contradiz a propriedade (3) da Proposição. ∎

Daqui decorre imediatamente que toda a extensão algébrica simples é finita:

**Corolário.** *Se $\theta$ é algébrico sobre $K$ e $gr(m_\theta(\boldsymbol{x})) = n$, então $[K(\theta) : K] = n$ e $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ é uma base do espaço vectorial $K(\theta)$ sobre $K$.* ∎

[Agora entende-se porque se chama ***grau*** da extensão à dimensão $[K(\theta) : K]$: este número coincide com o grau do polinómio mínimo $m_\theta(\boldsymbol{x})$]

Exemplos: (1) O que fizemos nos exemplos da aula anterior pode agora ser feito de modo muito mais rápido: por este corolário, segue imediatamente que, para qualquer inteiro primo $p$, $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$ e $\{1, \sqrt{p}\}$ é uma base de $\mathbb{Q}(\sqrt{p})$ sobre $\mathbb{Q}$; basta para isso observar que $x^2 - p$ é o polinómio mínimo de $\sqrt{p}$ sobre $\mathbb{Q}$.

(2) Consideremos a extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $\mathbb{Q}$. Podemos olhar para $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ como a extensão simples $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ de $\mathbb{Q}(\sqrt{2})$. Pelo Teorema da Torre,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})].$$

Qual é o polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$? $\sqrt{3}$ é raiz de $x^2 - 3 \in \mathbb{Q}[x] \subset \mathbb{Q}(\sqrt{2})[x]$. Será que este polinómio é irredutível sobre $\mathbb{Q}(\sqrt{2})$? Sim, pois as suas duas raízes $\pm\sqrt{3}$ não pertencem a $\mathbb{Q}(\sqrt{2})$:

Com efeito, $\pm\sqrt{3} = a + b\sqrt{2}$ para algum par $a, b$ de racionais implicaria $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, ou seja,

$$\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q} \quad \text{(no caso } a, b \neq 0)$$

ou $3 = 2b^2$ (no caso $a = 0$) ou $3 = a^2$ (no caso $b = 0$), uma contradição, em qualquer um dos três casos.

Portanto, $x^2 - 3$ é o polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2})$, pelo que

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2,$$

sendo $\{1, \sqrt{3}\}$ uma base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$.

Em conclusão, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ e, pela demonstração do Teorema da Torre, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ constitui uma base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$. Assim,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.$$

[Por vezes, uma extensão está escrita de tal maneira que ‘‘esconde" a sua simplicidade. Por exemplo, a extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é simples porque coincide com $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, como facilmente se pode verificar]