Depois do passeio por algumas aplicações do conceito de grau de uma extensão e do Teorema da Torre, voltemos ao estudo das extensões de corpos, começando por observar mais uma consequência do Teorema da Aula 13.

Seja $K$ um corpo, $L$ uma extensão de $K$ e $\theta \in L$. Consideremos o homomorfismo de anéis

$$\begin{array}{rccc} \phi : & K[x] & \rightarrow & L \\ & \sum_{i=0}^{n} a_i x^i & \mapsto & \sum_{i=0}^{n} a_i \theta^i \end{array}$$

que a um polinómio $p(\boldsymbol{x}) = \sum_{i=0}^{n} a_i x^i$ faz corresponder o seu valor em $\theta$. O núcleo $Nuc(\phi)$ deste homomorfismo é um ideal de $K[x]$, logo necessariamente principal. Por outro lado, o contradomínio de $\phi$ é claramente o subanel

$$K[\theta] := \{a_0 + a_1\theta + \cdots + a_n\theta^n \mid n \in \mathbb{N}, a_i \in K\}$$

de $L$.

`[`$K[\theta]$` é um subdomínio de integridade de `$K(\theta)$`]`

Portanto $\phi : K[x] \rightarrow K[\theta]$ é um homomorfismo sobrejectivo de anéis, donde, pelo Teorema do Homomorfismo,

$$\frac{K[x]}{Nuc(\phi)} \cong K[\theta]. \tag{1}$$

Temos então dois casos:

(1) <u>$\theta$ é algébrico sobre $K$</u>: Então $Nuc(\phi) \neq \{0\}$, donde $Nuc(\phi) = (m(\boldsymbol{x}))$, onde $m(\boldsymbol{x})$ é um polinómio irredutível que tem $\theta$ por raiz, e é o de menor grau nessas condições, ou seja, $m(\boldsymbol{x})$ é o polinómio mínimo de $\theta$ sobre $K$. Pelo Teorema da Aula 13 sabemos que, neste caso, $K(\theta) = K[\theta]$. Logo, por (1), temos

$$K(\theta) = K[\theta] \cong \frac{K[x]}{(m(\boldsymbol{x}))}.$$

Poe exemplo, no caso $K = \mathbb{R}$ e $\theta = i$, obtemos $\mathbb{R}(i) \cong \mathbb{R}[x]/(\boldsymbol{x}^2 + 1)$. Já vimos que $\mathbb{R}(i) = \mathbb{C}$, logo

$$\mathbb{C} \cong \frac{\mathbb{R}[x]}{(\boldsymbol{x}^2 + 1)}.$$

(2) <u>$\theta$ é transcendente sobre $K$</u>: Neste caso, $Nuc(\phi) = \{0\}$, logo

$$K[\theta] \cong \frac{K[x]}{\{0\}} \cong K[x].$$

[Dado um domínio $K[x]$, seja $L := \left\{ \frac{p(\boldsymbol{x})}{q(\boldsymbol{x})} \mid p(\boldsymbol{x}), q(\boldsymbol{x}) \in K[x], q(\boldsymbol{x}) \neq 0 \right\}$, com as operações óbvias de adição e multiplicação de "fracções". Verifique que $L$ é um corpo, o chamado *corpo das fracções* do domínio $K[x]$. Se identificarmos $a \in K$ com o elemento $\frac{a}{1}$ de $L$ e $p(\boldsymbol{x}) \in K[x]$ com o elemento $\frac{p(\boldsymbol{x})}{1}$ de $L$, não é difícil mostrar que $L$ coincide com a extensão simples $K(\boldsymbol{x})$ de $K$. Uma vez que o polinómio $p(\boldsymbol{x}) = a_n x^n + \cdots + a_0$ satisfaz $p(\boldsymbol{x}) = 0 \in K[x]$ se e só se $a_n = \cdots = a_0 = 0$, então $\boldsymbol{x}$ não é raiz de nenhum polinómio $p(\boldsymbol{x}) \neq 0$ em $K[x]$, ou seja, $\boldsymbol{x}$ é transcendente sobre $K$. Portanto, o corpo das fracções $K(\boldsymbol{x})$ é uma extensão simples e transcendente de $K$.

Assim, no caso (2), quando $\theta$ é transcendente sobre $K$, como $K[\theta] \cong K[x]$, os respectivos corpos de fracções $K(\theta)$ e $K(\boldsymbol{x})$ são isomorfos]

Em conclusão:

| EXTENSÕES SIMPLES DE $K$ |
|---|
| (1) $\theta$ é algébrico sobre $K$: $K(\theta) \cong \frac{K[x]}{(m(\boldsymbol{x}))}$. |
| (2) $\theta$ é transcendente sobre $K$: $K(\theta) \cong K(\boldsymbol{x})$. |

Quando estamos em subcorpos do corpo $\mathbb{C}$ dos números complexos, não há qualquer problema em determinar extensões em que um dado polinómio possua raízes, devido a uma propriedade fundamental de $\mathbb{C}$:

**Teorema Fundamental da Álgebra**: qualquer polinómio (de grau $\geq 1$) com coeficientes em $\mathbb{C}$ tem pelo menos uma raiz.

Isto implica que, em $\mathbb{C}$, todo o polinómio se decomponha em factores lineares do tipo $x - \theta$.

Mas existem muitos exemplos interessantes de corpos que não são subcorpos de $\mathbb{C}$ (por exemplo, os corpos de Galois $\mathbb{F}_p$, importantes na Teoria dos Números). Para estes corpos não é claro que dado um polinómio com coeficientes nesse corpo, exista uma extensão onde o polinómio possua raízes (e, consequentemente, se possa decompor em factores lineares). Iremos agora abordar esta questão.

---

**CORPO ALGEBRICAMENTE FECHADO**

Um corpo $K$ diz-se *algebricamente fechado* se qualquer polinómio $p(\boldsymbol{x}) \in K[x]$, de grau $\geq 1$, possui uma raiz em $K$.

---

Portanto, $\mathbb{C}$ é um corpo algebricamente fechado.

**Proposição.** *As seguintes afirmações são equivalentes:*

(i) *$K$ é um corpo algebricamente fechado.*

(ii) *Todo o polinómio $p(\boldsymbol{x}) = a_x\boldsymbol{x}^n + \cdots + a_1\boldsymbol{x} + a_0 \in K[x]$ se decompõe num produto de factores lineares $a_n\prod_{i=1}^n(\boldsymbol{x} - \theta_i)$.*

(iii) *Todo o polinómio irredutível de $K[x]$ tem grau 1.*

(iv) *Não existem extensões algébricas próprias de $K$.*

*Demonstração.*
"(i)⇔(ii)" Por hipótese, $p(\boldsymbol{x})$ tem uma raiz $\theta_1$ em $K$, pelo que $p(\boldsymbol{x}) = a_n(\boldsymbol{x} - \theta_1)q_1(\boldsymbol{x})$. Por sua vez, $q_1(\boldsymbol{x})$ também tem uma raiz $\theta_2$ em $K$, donde $p(\boldsymbol{x}) = a_n(\boldsymbol{x} - \theta_1)(\boldsymbol{x} - \theta_2)q_2(\boldsymbol{x})$. Repetindo este raciocínio indutivamente chegaremos à conclusão que

$$p(\boldsymbol{x}) = a_n\prod_{i=1}^n(\boldsymbol{x} - \theta_i).$$

A implicação recíproca é trivial.

"(ii)⇔(iii)" Óbvio.

"(iii)⇒(iv)" Seja $L$ uma extensão algébrica de $K$ e seja $\theta \in L$. Como $[K(\theta) : K]$ é dada pelo grau de um polinómio irredutível, então $[K(\theta) : K] = 1$. Logo $K(\theta) = K$, ou seja, $\theta \in K$, o que mostra que $L = K$.

"(iv)⇒(iii)" Seja $p(\boldsymbol{x}) \in K[x]$ um polinómio irredutível de grau $\geq 1$. Então o ideal $I = (p(\boldsymbol{x}))$ é maximal e $K[x]/I$ é um corpo. Consideremos o homomorfismo de corpos

$$\begin{array}{rccc} \psi : & K & \to & K[x]/I \\ & a & \mapsto & a + I. \end{array}$$

Como $Nuc(\psi)$ é um ideal de $K$ e $K$ é um corpo, só há duas possibilidades: $Nuc(\psi) = \{0\}$ ou $Nuc(\psi) = K$. Esta última possibilidade é claramente impossível, pelo que $Nuc(\psi) = \{0\}$ e $\psi$ é injectivo. Então $K \cong \psi(K) \subseteq K[x]/I$. Como, por hipótese, não existem extensões algébricas próprias de $K$, necessariamente $K[x]/I = \psi(K) = \{a + (p(\boldsymbol{x})) \mid a \in K\}$. Daqui decorre imediatamente que $gr(p(\boldsymbol{x})) = 1$. ∎

`[O Teorema Fundamental da Álgebra assegura que` $\mathbb{C}$ `é` algebricamente fechado. Outro facto importante é que qualquer corpo $K$ pode ser imerso num corpo algebricamente fechado. Mais do que isso, existe uma extensão algebricamente fechada $L$ de $K$, que é menor que todas as outras, no sentido de que, se $L'$ é uma extensão algebricamente fechada de $K$, $L'$ contém uma cópia isomorfa de $L$. Uma tal extensão chama-se o *fecho algébrico* de $K$. Portanto, *todo o corpo tem um fecho algébrico, que é único,* a menos de isomorfismo. As demonstrações deste facto e do Teorema Fundamental da Álgebra podem encontrar-se na bibliografia]