Recordemos a questão que começámos a estudar na aula passada:

> *Seja K um corpo e $p(x) \in K[x]$ um polinómio de grau ≥ 1. Existirá uma extensão L de K onde $p(x)$ se decomponha em factores lineares?*

É claro que se K for o corpo $\mathbb{Q}$ ou o corpo $\mathbb{R}$ há uma resposta óbvia: o corpo $\mathbb{C}$. E se K for o corpo $\mathbb{Z}_2$? Por exemplo, o polinómio $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ é irredutível sobre $\mathbb{Z}_2$, uma vez que não tem raízes em $\mathbb{Z}_2$: $p(0) = 1$ e $p(1) = 1$. Existirá uma extensão de $\mathbb{Z}_2$ onde $p(x)$ já tenha raízes e possa ser então decomposto num produto de termos lineares?

A resposta a todas estas questões é afirmativa. Como K não é *a priori* um subcorpo de um corpo algebricamente fechado, tal extensão é, necessariamente, "abstracta". A construção desta extensão é dada no seguinte teorema, e é inspirada na construção de $\mathbb{C}$ a partir de $\mathbb{R}$, como o quociente $\mathbb{R}[x]/(x^2 + 1)$.

Teorema. [Teorema de Kronecker]
Seja K um corpo e $p(x) \in K[x]$ um polinómio de grau $n \geq 1$. Existe uma extensão L de K onde $p(x)$ se decompõe num produto de termos lineares. Tal extensão pode ser tomada da forma $L = K(\theta_1, \ldots, \theta_n)$, onde $\theta_1, \ldots, \theta_n$ são as raízes de $p(x)$ em L.

Demonstração. Como $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = a_n q(x)$, sendo $q(x) = x^n + \frac{a_{n-1}}{a_n}x^{n-1} + \cdots + \frac{a_1}{a_n}x + \frac{a_0}{a_n}$ mónico, é evidente que $p(x)$ se decompõe num produto de termos lineares se e só se $q(x)$ se decompõe num produto de termos lineares. Assim, sem perda de generalidade, podemos assumir que $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ é mónico. Podemos ainda supor que $p(x)$ é irredutível. Com efeito, se $p(x)$ for redutível, sendo $p(x) = p_1(x)p_2(x)\ldots p_t(x)$ a factorização (única) de $p(x)$ em polinómios mónicos irredutíveis, se o resultado for válido para polinómios irredutíveis, provamos imediatamente o caso geral:

$$\begin{array}{ll} p_1(x) = (x-\theta_1^1)\ldots(x-\theta_{m_1}^1) & \text{em } K(\theta_1^1, \ldots, \theta_{m_1}^1), \\ p_2(x) = (x-\theta_1^2)\ldots(x-\theta_{m_2}^2) & \text{em } K(\theta_1^2, \ldots, \theta_{m_2}^2), \\ \vdots & \vdots \\ p_t(x) = (x-\theta_1^t)\ldots(x-\theta_{m_t}^t) & \text{em } K(\theta_1^t, \ldots, \theta_{m_t}^t), \end{array}$$

pelo que

$$p(x) = (x-\theta_1^1)\ldots(x-\theta_{m_1}^1)\ldots(x-\theta_1^t)\ldots(x-\theta_{m_t}^t)$$

em $K(\theta_1^1, \ldots, \theta_{m_1}^1)\ldots(\theta_1^t, \ldots, \theta_{m_t}^t) = K(\theta_1^1, \ldots, \theta_{m_1}^1 \ldots \theta_1^t, \ldots, \theta_{m_t}^t)$.

Suponhamos então que $p(x)$ é um polinómio mónico irredutível. Então $I := (p(x))$ é maximal e, como vimos no final da aula anterior, $\psi : K \to K[x]/I$, definida por $\psi(a) = a + I$, é um homomorfismo injectivo,

[$\psi(a) = \psi(b) \Leftrightarrow a + I = b + I \Leftrightarrow a - b \in I \Rightarrow a = b$,
pois $gr(a-b) = 0$ e $gr(p(x) \geq 1$]

donde $K \cong \psi(K) \subseteq K[x]/I$. Portanto, $L := K[x]/I$ é uma extensão de K.

[Cometemos aqui um abuso de linguagem;
em rigor, L é uma extensão de uma cópia isomorfa de K:
$\psi(K) = \{a + I : a \in K\}$ é um subcorpo de L isomorfo a K]

Pelo isomorfismo $K \cong \psi(K)$, podemos identificar dentro do novo corpo L os elementos do corpo inicial K, como os elementos $a+I$ ($a \in K$). Por essa identificação, o polinómio $p(x) \in K[x]$ pode ser visto como um polinómio em $L[x]$:

$$p(x) = x^n + (a_{n-1} + I)x^{n-1} + \cdots + (a_1 + I)x + (a_0 + I).$$

Seja $\theta := x + I \in K[x]/I$. Trata-se de uma raiz de $p(x)$ em L:

$$\begin{aligned}
p(\theta) &= \theta^n + (a_{n-1} + I)\theta^{n-1} + \cdots + (a_1 + I)\theta + (a_0 + I) \\
&= (x + I)^n + (a_{n-1} + I)(x + I)^{n-1} + \cdots + (a_1 + I)(x + I) + (a_0 + I) \\
&= (x^n + I) + (a_{n-1} + I)(x^{n-1} + I) + \cdots + (a_1 + I)(x + I) + (a_0 + I) \\
&= x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 + I \\
&= p(x) + I = 0.
\end{aligned}$$

Portanto, em L já $p(x)$ se factoriza na forma $(x - \theta)p_1(x)$. Além disso, $p(x)$ é o polinómio mínimo de θ sobre K. Consequentemente, pelo que vimos na aula anterior,

$$L = \frac{K[x]}{(p(x))} \cong K(\theta).$$

Repetindo o raciocínio para $p_1(x)$, que é também irredutível sobre K, chegaremos por indução (sobre o grau do polinómio) à solução que procuramos. ∎

Tal extensão chama-se *extensão* (ou *corpo*) *de decomposição* de $p(x)$.

Exemplo: Apliquemos a construção geral dada pelo Teorema ao polinómio $p(x) = x^2 + x + 1$ de $\mathbb{Z}_2[x]$, que é irredutível sobre $\mathbb{Z}_2$, como observámos no início.

Seja L a extensão

$$\begin{aligned}\frac{\mathbb{Z}_2[x]}{(p(x))} &= \{a_0 + a_1x + (p(x)) \mid a_0, a_1 \in \mathbb{Z}_2\} \\ &= \{0 + (p(x)), 1 + (p(x)), x + (p(x)), 1 + x + (p(x))\}\end{aligned}$$

constituída pelas classes definidas pelos restos da divisão dos polinómios de coeficientes em $\mathbb{Z}_2[x]$ por $p(x)$. Denotando $0+(p(x))$ por 0, $1+(p(x))$ por 1, $x+(p(x))$ por α e $1+x+(p(x))$ por β, as tabelas das operações de L são as seguintes:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

[Por exemplo, $\alpha+\beta = (x+(p(x))) + (1+x+(p(x))) = 1+(p(x)) = 1$ e $\alpha\beta = x(1+x)+(p(x)) = x+x^2+(p(x)) = 1+(p(x)) = 1$. Observe que $L = \mathbb{Z}_2(\alpha) = \mathbb{Z}_2(\beta)$.]

O Teorema garante-nos que α é uma raiz de $p(x)$. Portanto, em L já o polinómio $p(x)$ é redutível. De facto,

$$x^2 + x + 1 = (x-\alpha)(x-\beta).$$

Consideremos agora o polinómio $q(x) = x^2 + \beta x + \beta \in L[x]$. Como $q(0) = \beta$, $q(1) = 1$, $q(\alpha) = \alpha$ e $q(\beta) = \beta$, $q(x)$ é irredutível sobre L. O Teorema diz-nos agora que a extensão de decomposição de $q(x)$ é dada pelo corpo

$$M := \frac{L[x]}{(q(x))} = \{a_0 + a_1x + (q(x)) \mid a_0, a_1 \in L\},$$

que tem 16 elementos:

$$[0],\ [1],\ [\alpha],\ [\beta],\ [x],\ [1+x],\ [\alpha+x],\ [\beta+x],\ [\alpha x],\ [1+\alpha x],$$

$$[\alpha+\alpha x],\ [\beta+\alpha x],\ [\beta x],\ [1+\beta x],\ [\alpha+\beta x],\ [\beta+\beta x]$$

(denotando cada elemento $a_0 + a_1x + (q(x))$ por $[a_0 + a_1x]$). Simplifiquemos a escrita um pouco mais, denotando os 16 elementos de M por, respectivamente,

$$0, 1, \alpha, \beta, c, d, e, f, g, h, i, j, k, l, m, n.$$

As tabelas das operações de M são:

$+$	0	1	α	β	c	d	e	f	g	h	i	j	k	l	m	n
0	0	1	α	β	c	d	e	f	g	h	i	j	k	l	m	n
1	1	0	β	α	d	c	f	e	h	g	j	i	l	k	n	m
α	α	β	0	1	e	f	c	d	i	j	g	h	m	n	k	l
β	β	α	1	0	f	e	d	c	j	i	h	g	n	m	l	k
c	c	d	e	f	0	1	α	β	k	l	m	n	g	h	i	j
d	d	c	f	e	1	0	β	α	l	k	n	m	h	g	j	i
e	e	f	c	d	α	β	0	1	m	n	k	l	i	j	g	h
f	f	e	d	c	β	α	1	0	n	m	l	k	j	i	h	g
g	g	h	i	j	k	l	m	n	0	1	α	β	c	d	e	f
h	h	g	j	i	l	k	n	m	1	0	β	α	d	c	f	e
i	i	j	g	h	m	n	k	l	α	β	0	1	e	f	c	d
j	j	i	h	c	n	m	l	k	β	α	1	0	f	e	d	c
k	k	l	m	n	g	h	i	j	c	d	e	f	0	1	α	β
l	l	k	n	m	h	g	j	i	d	c	f	e	1	0	β	α
m	m	n	k	l	i	j	g	h	e	f	c	d	α	β	0	1
n	n	m	l	k	j	i	h	g	f	e	d	c	β	α	1	0

$\cdot$	0	1	α	β	c	d	e	f	g	h	i	j	k	l	m	n
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	α	β	c	d	e	f	g	h	i	j	k	l	m	n
α	0	α	β	1	g	i	j	h	k	m	n	l	c	e	f	d
β	0	β	1	α	k	n	l	m	c	f	d	e	g	j	h	i
c	0	c	g	k	n	j	f	β	d	1	l	h	i	m	α	e
d	0	d	i	n	j	m	1	c	l	g	f	α	e	β	k	h
e	0	e	j	l	f	1	k	i	h	n	α	c	m	g	1	β
f	0	f	h	m	β	c	i	l	1	e	g	n	α	d	j	k
g	0	g	k	c	d	l	h	1	i	α	e	m	n	f	β	j
h	0	h	m	f	1	g	n	e	α	j	k	d	β	i	l	c
i	0	i	n	d	l	f	α	g	e	k	h	β	j	1	c	m
j	0	j	l	e	h	α	c	n	m	d	β	g	f	k	i	1
k	0	k	c	g	i	e	m	α	n	β	j	f	d	h	1	l
l	0	l	e	j	m	β	g	d	f	i	1	k	h	c	n	α
m	0	m	f	h	α	k	d	j	β	l	c	i	1	n	e	g
n	0	n	d	i	e	h	β	k	j	c	m	1	l	α	g	f

[Verifique]

O Teorema garante-nos que c é uma raiz de $q(x)$ em M. Assim, o corpo M (que coincide com a extensão simples $L(c)$ de L) é, de facto, a extensão de decomposição de $q(x)$:

$$q(x) = x^2 + \beta x + \beta = (x - c)(x - f).$$

`[Verifique]`

O Teorema motiva a seguinte definição:

EXTENSÃO DE DECOMPOSIÇÃO
Seja $p(x)$ um polinómio com coeficientes num corpo K. Uma *extensão de decomposição* de $p(x)$ é uma extensão L de K em que:

(1) $p(x)$ decompõe-se em L num produto de termos de grau 1.

(2) $L = K(\theta_1, \ldots, \theta_n)$ onde $\theta_1, \ldots, \theta_n$ são as raízes de $p(x)$ em L.

Analogamente, dizemos que uma extensão L de K é uma *extensão de decomposição de uma família de polinómios* $\{p_i(x)\}_{i \in I} \subseteq K[x]$ se

(1) cada $p_i(x)$ decompõe-se em L num produto de termos de grau 1.

(2) L é gerada pelas raízes destes polinómios.