Seja I um ideal de um anel $(A, +, \cdot)$. Como $(I, +)$ é um subgrupo normal do grupo abeliano $(A, +)$, sabemos da Álgebra I que o conjunto A/I das classes laterais $a + I := \{a + x \mid x \in A\}$, $a \in A$, forma um grupo abeliano (o chamado *grupo quociente*) para a operação

$$(a + I) + (b + I) := (a + b) + I.$$

Exercício. Dois elementos a e b de A dizem-se *congruentes* módulo I (e escreve-se $a \equiv b \mod I$) se pertencem à mesma classe lateral, ou seja, $a + I = b + I$. Mostre que $a \equiv b \mod I$ implica $a + x \equiv b + x \mod I$, $ax \equiv bx \mod I$, e $xa \equiv xb \mod I$ para qualquer $x \in A$ e $na \equiv nb \mod I$ para qualquer $n \in \mathbb{Z}$.

[Recorde: $a + I = b + I$ sse $a - b \in I$]

Mas agora, no contexto dos anéis, temos mais estrutura em A/I:

$$(a + I)(b + I) := ab + I \tag{1}$$

define outra operação em A/I. Com efeito, se $a + I = c + I$ e $b + I = d + I$ então

$$\left.\begin{array}{l} a + I = c + I \Leftrightarrow a - c \in I \overset{(*)}{\Rightarrow} (a - c)b \in I \Leftrightarrow ab - cb \in I \\ \\ b + I = d + I \Leftrightarrow b - d \in I \overset{(*)}{\Rightarrow} c(b - d) \in I \Leftrightarrow cb - cd \in I \end{array}\right\} \Rightarrow ab - cd \in I,$$

isto é, $ab + I = cd + I$.

[Observe: a condição 3 na definição de ideal é decisiva no passo (*): se I for somente um subanel, (1) pode não definir uma operação em A/I]

Proposição. *A/I forma um anel relativamente às operações*

$$(a + I) + (b + I) := (a + b) + I,$$

$$(a + I)(b + I) := ab + I.$$

Demonstração. $(A/I, +)$ é um grupo abeliano (Álgebra I) e decorre imediatamente da definição do anel A que a operação $\cdot$ de A/I é associativa e é distributiva relativamente à adição. ∎

O anel $(A/I, +, \cdot)$ chama-se *anel quociente* de A por I. É evidente que se A é comutativo então A/I também é comutativo e se A tem identidade 1 então A/I também tem identidade (o elemento $1 + I$).

Exemplo: $\mathbb{Z}/(5)$ tem 5 elementos:

$$0+(5), 1+(5), 2+(5), 3+(5), 4+(5), 5+(5) = 0+(5), 6+(5) = 1+(5), \ldots$$

$$-1+(5) = 4+(5), -2+(5) = 3+(5), \ldots$$

Identifiquemo-los simplesmente por $[0], [1], [2], [3]$ e $[4]$, respectivamente.
As tabelas das operações do anel $\mathbb{Z}/(5)$ são então:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

`[É um corpo]`

Mais geralmente, para cada $n \in \mathbb{N}$, os elementos de $\mathbb{Z}/(n)$ são

$$[0] := 0+(n), [1] := 1+(n), \ldots, [n-1] := n-1+(n).$$

Em geral, é um anel comutativo com identidade $[1]$. É um corpo se e só se n é primo.

`[Recorde:` $(\mathbb{Z}_n \setminus \{0\}, \otimes_n)$ `é um grupo sse` n `é primo]`

Por exemplo, para $n = 6$ existem divisores de zero: $[2] \cdot [3] = [0]$. Este exemplo mostra que as propriedades do anel A não são necessariamente herdadas pelo anel quociente: $\mathbb{Z}$ é um domínio de integridade mas $\mathbb{Z}/(6)$ não é.

Seja A um anel comutativo com identidade. Vejamos quais ideais dão origem a anéis quociente que são domínios de integridade ou corpos.

IDEAL PRIMO
Um ideal $P \neq A$ do anel A chama-se *primo* se, para quaisquer $a, b \in P$, $ab \in P$ implica $a \in P$ ou $b \in P$.

Exemplos: Seja $A = \mathbb{Z}$. (6) não é um ideal primo: $3 \cdot 2 = 6 \in (6)$ mas $(3) \notin (6)$ e $(2) \notin (6)$. (5) é um ideal primo:

$$ab \in (5) \Leftrightarrow 5|ab \Rightarrow 5|a \text{ ou } 5|b \Leftrightarrow a \in (5) \text{ ou } b \in (5).$$

`[Caso geral: para` $n \geq 1$, (n) `é primo sse` n `é primo]`

$(0) = \{0\}$ é evidentemente um ideal primo de $\mathbb{Z}$. Com efeito, é óbvio que num anel A comutativo com identidade, (0) é primo se e só se A não tem divisores de zero.

IDEAL MAXIMAL

Um ideal $M \neq A$ do anel A chama-se *maximal* se, para qualquer ideal I de A, a propriedade $M \subseteq I$ implica $I = M$ ou $I = A$.

Exemplos: No anel dos inteiros $\mathbb{Z}$, (0) e (10) não são maximais:

$$(0) \subset (10) \subset (5) \subset \mathbb{Z}.$$

[Observe: O exemplo (0) mostra que, em geral, primo $\not\Rightarrow$ maximal]

Por outro lado, (5) é maximal:

$$(5) \subseteq (m) \subseteq \mathbb{Z} \Leftrightarrow m|5 \Rightarrow m = 1 \text{ ou } m = 5 \Leftrightarrow (m) = \mathbb{Z} \text{ ou } (m) = (5).$$

[Caso geral: para $n \geq 1$, (n) é maximal sse n é primo]

Finalmente, temos:

Teorema. *Seja A um anel comutativo com identidade e I um ideal de A. Então:*

(a) *A/I é um domínio de integridade se e só se I é primo.*

(b) *A/I é um corpo se e só se I é maximal.*

(c) *Todo o ideal maximal de A é primo.*

Demonstração. Já sabemos que A/I é um anel comutativo com identidade $1 + I$.
(a) Portanto, A/I será um domínio de integridade sse

$$\begin{cases} 1 + I \neq 0 + I & (*) \\ \\ (a + I)(b + I) = I \text{ implica } a \in I \text{ ou } b \in I. & (**) \end{cases}$$

Mas
$(*) \Leftrightarrow 1 \notin I \Leftrightarrow I \neq A$

[Verifique: para qualquer ideal I, $1 \in I \Leftrightarrow I = A$]

$(**) \Leftrightarrow ab + I = I$ implica $a \in I$ ou $b \in I \Leftrightarrow ab \in I$ implica $a \in I$ ou $b \in I$,

pelo que $(*)$ e $(**)$ significam precisamente que I é primo.

(b) Agora, A/I será um corpo sse

$$\begin{cases} 1+I \neq 0+I & (*) \\ \\ \text{qualquer } a+I \neq I \text{ é invertível.} & (**) \end{cases}$$

Mas
$(**) \Leftrightarrow$ para cada $(a+I) \neq I$ existe $(b+I) \neq I$ tal que $(a+I)(b+I) = 1+I \Leftrightarrow$ para cada $a \in A \setminus I$ existe $b \in A \setminus I$ tal que $ab + I = 1 + I \Leftrightarrow$ para cada $a \in A \setminus I$ existe $b \in A \setminus I$ tal que $ab - 1 \in I$.

Bastará agora observarmos que esta última condição é equivalente a

$$J \text{ ideal de } A,\ I \subset J \subseteq A \Rightarrow J = A,$$

para concluirmos que $(*)$ e $(**)$ significam que I é maximal:

("$\Rightarrow$") Seja então $a \in J \setminus I$. Por hipótese, existe $b \in A \setminus I$ tal que $ab - 1 \in I \subset J$. Como $ab \in J$, então $1 \in J$, logo $J = A$.

("$\Leftarrow$") Reciprocamente, para cada $a \in A \setminus I$ consideremos o menor ideal que contém $I \cup \{a\}$ (o chamado *ideal gerado* por $I \cup \{a\}$), ou seja, o ideal

$$J_a := \{xa + y \mid x \in A, y \in I\}.$$

[Verifique: $\{xa + y \mid x \in A, y \in I\}$ é um ideal de A]

É evidente que $I \subset J_a \subseteq A$ logo, por hipótese, $J_a = A$. Em particular, $1 \in J_a$, ou seja, 1 é um dos elementos $xa + y$ de J_a. Mas $1 = xa + y \Leftrightarrow xa - 1 = -y \in I$. Provámos assim que, para cada $a \in A \setminus I$, existe $b \in A \setminus I$ tal que $ab - 1 \in I$.
(c) É consequência imediata de (b) e (a): Se I é maximal, A/I é um corpo e, em particular, um domínio de integridade, logo I é primo. ∎

Exemplo de aplicação do Teorema: No caso $A = \mathbb{Z}$, $I = (5)$ é, como vimos maximal; daí o facto de $\mathbb{Z}/(5)$ ser um corpo, como tínhamos observado no início da aula.

Outras aplicações: No próximo capítulo, aos anéis de polinómios.