ANEL QUOCIENTE

Queremos "imitar" a construção de $\mathbb{Z}_m$, inteiros módulo m.

Quando definimos em $\mathbb{Z}$ a relação

$a \equiv b \pmod m$ se e só se $m \mid b-a$,

essa é uma relação de equivalência em $\mathbb{Z}$.

Note que $m\mathbb{Z}$ é um ideal de $\mathbb{Z}$.

Podemos definir $a \equiv b \pmod m \iff b-a \in m\mathbb{Z}$.

Denotamos por $\mathbb{Z}_m = \{\overline{x} \mid x \in \mathbb{Z}\}$ o conjunto das classes de equivalência determinada pela relação de equivalência $\equiv \pmod m$.

E podemos dar a $\mathbb{Z}_m$ uma estrutura de anel definindo

$$\begin{aligned} \mathbb{Z}_m \times \mathbb{Z}_m &\xrightarrow{+} \mathbb{Z}_m \\ (\overline{a}, \overline{b}) &\longmapsto \overline{a}+\overline{b} \underset{\text{def}}{=} \overline{a+b} \\ \mathbb{Z}_m \times \mathbb{Z}_m &\xrightarrow{\cdot} \mathbb{Z}_m \\ (a,b) &\longmapsto \overline{a}\,\overline{b} \underset{\text{def}}{=} \overline{ab} \end{aligned}$$

} Essas operações estão bem definidas

$(\mathbb{Z}_m, +, \cdot)$ é um anel comutativo com unidade.

Além disso $q : \mathbb{Z} \longrightarrow \mathbb{Z}_m$

$q(x) = \overline{x}$ é um homomorfismo de anéis.

(Pois $q(x+y) = \overline{x+y} = \overline{x} + \overline{y} = q(x) + q(y)$

e $q(xy) = \overline{xy} = \overline{x}\,\overline{y} = q(x)\,q(y)$.)

Seja agora R um anel e $A \subset R$, $A \neq \emptyset$

(1) Que condições o conjunto A tem que satisfazer para que

$x, y \in R$, $x \equiv y \pmod{A} \Leftrightarrow x - y \in A$

seja uma relação de equivalência em R?

Queremos que:

E1 (Propriedade Reflexiva)

$\forall x \in R$, $x \equiv x \pmod{A}$

$x \equiv x \pmod{A} \Leftrightarrow x - x \in A \Leftrightarrow 0 \in A$

A primeira condição é então $0 \in A$.

E2 (Propriedade Simétrica)

$\forall x, y \in R$, se $x \equiv y \pmod{A}$ então $y \equiv x \pmod{A}$.

Pense então nesse caso particular:

Se $x \in A$ então $x - 0 \in A \Rightarrow$

$x \equiv 0 \pmod{A}$. Se vale a propriedade Simétrica, então $0 \equiv x \pmod{A} \Rightarrow$

$0 - x \in A \Rightarrow -x \in A$.

Assim, se valer a propriedade simética, isso implica que $\forall x \in A$, $-x \in A$.

Por outro lado, se A é tal que $\forall x \in A \Rightarrow -x \in A$, temos que vale a E2 (Propriedade Simétrica).

Se $x \equiv y \pmod{A} \Rightarrow x - y \in A$.

Mas $-(x - y) = y - x \in A \Rightarrow y \equiv x \pmod{A}$

A segunda condição é então: Se $x \in A$ então $-x \in A$.

E3 : Propriedade Transitiva

$\forall\, x, y, z \in R$, se $x \equiv y \pmod{A}$ e $y \equiv z \pmod{A}$ então $x \equiv z \pmod{A}$.

Suponha que vale a propriedade transitiva e que $x, y \in A$

$x \equiv 0 \pmod{A}$ e $0 \equiv -y \pmod{A}$

(pois $y \in A$, já temos $-y \in A$)

$\Rightarrow x \equiv -y \pmod{A} \Rightarrow x - (-y) \in A$

$\Rightarrow x + y \in A$.

Assim uma condição necessária para que $\equiv \pmod{A}$ seja uma relação de equivalência em R é que $(A, +)$ seja um subgrupo de $(R, +)$, isto é:

(1) $0 \in A$;
(2) Se $x \in A$ então $-x \in A$;
(3) Se $x, y \in A$ então $x + y \in A$.

Essa condição também é suficiente para que $\equiv \pmod{A}$ seja uma relação de equivalência em R.

Defato: $\forall\, x \in R$, $x \equiv x \pmod{A}$

(pois $x - x = 0$ e $0 \in A$)

Se $x \equiv y \pmod{A}$ então $y \equiv x \pmod{A}$

De fato: Se $x \equiv y \pmod{A} \Rightarrow x - y \in A$

$\Rightarrow -(x - y) \in A \Rightarrow y - x \in A \Rightarrow$

$y \equiv x \pmod{A}$

Se $x \equiv y \pmod{A}$ e $y \equiv z \pmod{A}$ então

$x - y \in A$ e $y - z \in A$.

Então $(x-y)+(y-z) \in A \Rightarrow$

$x-z \in A \Rightarrow x \equiv z \pmod{A}$.

Resumindo:

> Se $A \subset R$ é um subgrupo de $(R,+)$ $((A,+))$ se, e somente se, $\equiv \pmod{A}$ é uma relação de equivalência em R.

Denotamos por $R/A = \{\bar{x} \mid x \in R\}$

$$\bar{x} = \{y \in R \mid x \equiv y \pmod{A}\}$$
$$= \{y \in R \mid y \equiv x \pmod{A}$$
$$= \{y \in R \mid y - x \in A\} =$$
$$= \{y \in R \mid \exists\, a \in A \text{ tal que } y = x+a\}$$

Note que $\bar{x} = \underset{\text{Notação}}{x+A} = \{x+a \mid a \in A\}$

Note que se definirmos

$$+ : R/A \times R/A \longrightarrow R/A$$
$$(\bar{x}, \bar{y}) \overset{+}{\longmapsto} \bar{x}+\bar{y}$$

e por definição $\bar{x}+\bar{y} = \overline{x+y}$, então essa operação de adição em R/A está bem definida:

Se $(\bar{x},\bar{y}) = (\bar{x}_1, \bar{y}_1)$, mostrar que

$$x+y \equiv x_1+y_1 \pmod{A}$$

De fato
$\overline{x} = \overline{x_1} \Rightarrow x - x_1 \in A$
$\overline{y} = \overline{y_1} \Rightarrow y - y_1 \in A$

Então $x + y - (x_1 + y_1) = (x - x_1) + (y - y_1) \in A$
($x - x_1 \in A$, $y - y_1 \in A$)

Em R/A vale, $\forall\, x, y, z \in R$

A1 $(\overline{x} + \overline{y}) + \overline{z} \overset{\text{def}}{=} (\overline{x+y}) + \overline{z}$

$\overset{\text{def}}{=} \overline{(x+y)+z} = \overline{x+(y+z)} =$

A1 (associativa em R)

$= \overline{x} + \overline{(y+z)} = \overline{x} + (\overline{y} + \overline{z})$.

A2 $\overline{x} + \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} + \overline{x}$

A3 $\overline{x} + \overline{0} = \overline{x+0} = \overline{x} = \overline{(0+x)} = \overline{0} + \overline{x}$

$\overline{0}$ é o elemento neutro da adição em R/A.

A4 $\forall\, \overline{x} \in R/A$, vale que $-\overline{x} = \overline{(-x)}$

pois $\overline{x} + \overline{(-x)} = \overline{x + (-x)} = \overline{0} = \overline{(-x)} + \overline{x}$

(2) Que condições A tenque satisfazer para que $\overline{x} \cdot \overline{y} = \overline{xy}$ esteja bem definido
Mas queremos que R/A seja um anel

definindo $\overline{x} \cdot \overline{y} = \overline{xy}$.

Se R/A for um anel, $\overline{0} \cdot \overline{x} = \overline{0}$ $\forall\, x \in R$
$\overline{x} \cdot \overline{0} = \overline{0}$ $\forall\, x \in R$

$\overline{0} = \overline{a}$, para todo $a \in A$

$\overline{x}\,\overline{a} = \overline{0} \Rightarrow \overline{xa} = \overline{0} \Rightarrow xa$
$xa - 0 \in A$

Logo, para todo $x \in R$ e $a \in A$, $xa \in A$

Analogamente, para todo $a \in A$ e $x \in R$, $ax \in A$.

Então, se R/A for anel, A é um ideal de R.

Por outro lado, se A for um ideal de R, a multiplicação em R/A definida por

$$\begin{aligned} R/A \times R/A &\longrightarrow R/A \\ (\bar{x}, \bar{y}) &\longmapsto \bar{x}\bar{y} \underset{\text{def}}{=} \overline{xy} \end{aligned}$$

está bem definida.

De fato:

Suponha que $(\bar{x}, \bar{y}) = (\bar{x_1}, \bar{y_1})$

$\Rightarrow \bar{x} = \bar{x_1}$ e $\bar{y} = \bar{y_1}$

$\Rightarrow x - x_1 \in A$ e $y - y_1 \in A$.

Mostrar que $xy - x_1y_1 \in A$

$$xy - x_1y_1 = xy - xy_1 + xy_1 - x_1y_1$$

$$= x\underbrace{(y - y_1)}_{\in A} + \underbrace{(x - x_1)}_{\in A} y_1 \in A.$$

$\in A$, $\in A$, $\in A$

Logo $\overline{xy} = \overline{x_1y}$ e $\bar{x} \cdot \bar{y}$ definida por $\bar{x} \cdot \bar{y} = \overline{xy}$ está bem definida.

Daí é claro que $\forall x, y, z \in R$ vale

M1. $\overline{x}(\overline{y}\overline{z}) = \overline{x}\cdot(\overline{yz}) = \overline{x(yz)}$

$= \overline{(xy)z} = \overline{(xy)}\cdot\overline{z} = (\overline{x}\,\overline{y})\overline{z}$

e vale D:

$\overline{x}(\overline{y}+\overline{z}) = \overline{x}\overline{y} + \overline{x}\overline{z}$

$(\overline{y}+\overline{z})\overline{x} = \overline{y}\overline{x} + \overline{z}\overline{x}$

} Prove isso:

Assim $(R/A, +, \cdot)$ é um anel $\Leftrightarrow$ A é um ideal de R.

R/A é o anel quociente de R pelo ideal A

A função $q: R \longrightarrow R/A$

$q(x) = \overline{x}$

é um homomorfismo de anéis.

É claro que R comutativo $\Rightarrow R/A$ comutativo

Se R tem unidade $\underline{1} \Rightarrow \overline{1}$ é unidade em R/A.