Ideais e Quocientes de Anéis - 162

<u>Exemplo</u>: No anel $\mathbb{Z}$, $a \equiv b \pmod 3$ significa que $(a-b)$ é um múltiplo de 3. Temos I sendo o conjunto de todos os múltiplos de 3, que:

$$I = \{0, \pm 3, \pm 6, \dots\}$$

A congruência módulo 3, pode ser caracterizada como:

$$a \equiv b \pmod 3 \longrightarrow (a-b) \in I$$

Observe que o subconjunto I é um subanel de $\mathbb{Z}$ (somas e produtos de múltiplos de 3 são também múltiplos de 3).

Assim um subanel I tem a propriedade:

Qualquer $k \in \mathbb{Z}$ e $i \in I$, então $ki \in I$.

O mesmo vale para polinômios:

Qualquer $k(x) \in \mathbb{Q}[x]$ e $i(x) \in I$, então $k(x) \cdot i(x) \in I$

$$f(x) \equiv g(x) \pmod{x^2-2} \longrightarrow f(x) - g(x) \in I$$

<u>① Definição</u>: Um subanel (I) de um anel (R) é um ideal fornecido:

Qualquer $r \in R$ e $a \in I$, então $ra \in I$ e $ar \in I$.

Teorema: Um subconjunto não vazio I de um anel R é um ideal se e somente se ele tem estas propriedades:

i) Se $a, b \in I$, então $(a-b) \in I$
ii) Se $r \in R$ e $a \in I$, então $ra \in I$ e $ar \in I$

Ideais finitamente gerados:

Teorema: Temos R sendo um anel comutativo com identidade, $c \in R$, e I o conjunto de todos os multiplos de c em R, que é, $I = \{rc \mid r \in R\}$. Então I é um ideal.

Em um anel comutativo com identidade, um principal ideal consiste de todos os multiplos de um elemento fixado. Aqui é uma generalização da ideia.

Teorema: Temos R sendo um anel comutativo com identidade e $c_1, c_2, \dots, c_N \in R$. Então o conjunto $I = \{r_1 c_1 + r_2 c_2 + \dots + r_N c_N \mid r_1, r_2, \dots, r_N \in R\}$ é um ideal em R.

Conguencia:

Definição: Temos I sendo um ideal em um anel R e temos $a, b \in R$. Então a é conguente para b modulo I ($a \equiv b \pmod I$) fornecido por $(a-b) \in I$.

Teorema: Temos I sendo um ideal em um anel R. Então na relação de congruência módulo I é:

i) reflexiva: $a \equiv a \pmod I$ $\forall a \in R$
ii) simétrica: se $a \equiv b \pmod I$, então $b \equiv a \pmod I$.;
iii) transitiva: se $a \equiv b \pmod I$ e $b \equiv c \pmod I$, então $a \equiv c \pmod I$

Teorema: Temos I sendo um ideal em um anel R. Se $a \equiv b \pmod I$ e $c \equiv d \pmod I$, então:

i) $a+c \equiv b+d \pmod I$.;
ii) $ac \equiv bd \pmod I$.;

Teorema: Temos I sendo um ideal em um anel R e temos $a, c \in R$. Então $a \equiv c \pmod I$ se e somente se: $a+I = c+I$.

Corolário: Temos I sendo um ideal em um anel R. Então 2 conjuntos de I são disjuntos ou idênticos.

Exemplos de Subanéis:

1) $\mathbb{Z}$ é um subanel de $\mathbb{Q}$.;
2) $\mathbb{Q}$ " " " " $\mathbb{R}$.;
3) Seja $B = \{\bar{0}, \bar{2}\} \subset \mathbb{Z}_4$., B é um subanel de $\mathbb{Z}_4$.;
4) $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$.;
5) $B = \{2k+1, k \in \mathbb{Z}\}$, não é um subanel de $\mathbb{Z}$., Tomamos: $1, 3 \in B \longrightarrow 3-1 = 2 \notin B$.

Restringindo ao estudo de anéis abelianos:

Sejam A um anel e I um subanel não vazio de A, dizemos que I é um ideal de A se:

i) $\forall a, b \in I$, $(a-b) \in I$
ii) $\forall a \in A$, temos $a.I \subseteq I$

Onde $a.I = \{a.x \mid x \in I\}$

Exemplo:

1) Seja A um anel, $I = \{0\}$ e $J = A$, são ideais de A, são chamados triviais.

2) $2\mathbb{Z}$ é um ideal de $\mathbb{Z}$.

3) $I = \mathbb{Z}$ não é um ideal de $\mathbb{Q}$, pois:

$1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$ e $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$

Assim $\mathbb{Z}$ é apenas subanel dos $\mathbb{Q}$.

Proposição: Todo ideal de um anel A é um subanel.

A volta é falsa: $\mathbb{Z}$ é um subanel de $\mathbb{Q}$, mas não é um ideal de $\mathbb{Q}$.

Proposição: Um subanel B de A é um ideal para todo $a \in A$, $a.B \subseteq B$.

Ideais: Seja A um anel unitário, $a \in A$ é chamado inversível se existir $b \in A$ tal que $a.b = b.a = 1$, neste caso $b = a^{-1}$.

Proposição: Seja I um ideal de A. Se I contém algum elemento inversível de A, então $I = A$.

Dem: $I \subseteq A$, pois é um ideal de A.

Vamos mostrar que $A \subset I$.

Seja $x \in I$ um inversível de A. Dado qualquer $a \in A$, $a \cdot x^{-1} \in A$, como I é um ideal, $(a \cdot x^{-1}) \cdot x \in I = a \cdot (x \cdot x^{-1}) \in I \rightarrow a \in I$.

Definição: Sejam A um anel e $x \in A$. Temos que $I = A \cdot x$ é um ideal de A, chamado ideal gerado por x.

Sejam A um anel, $x_1, x_2, \dots, x_n \in A$, podemos mostrar que o conjunto $I = A \cdot x_1 + A x_2 + \dots + A \cdot x_n$ é um ideal de A, que será chamado ideal gerado por $x_1, x_2, \dots, x_n$.

Assim, sejam A um anel e I um ideal de A. O ideal será chamado um ideal principal de A se existir $x \in A$, tal que: $I = A \cdot x$.

Definição: Um anel comutativo A é chamado principal quando todo ideal de A for um ideal principal.

Exemplo:

1) $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ é um anel principal.

Quais são os subaneis de $\mathbb{Z}_4$?

i) $\{\bar{0}\} = \bar{0}.\mathbb{Z}_4$, logo é um ideal principal.

Quando todo ideal de A for um ideal principal.

Ideal principal: se existir $x \in A$ tal que:

$$I = A.x$$

$\bar{0}.\mathbb{Z}_4 = \bar{0}$ é um ideal principal, gerado por $\bar{0}$

ii) $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \bar{1}.\mathbb{Z}_4$, também é um ideal principal

iii) $\{\bar{0}, \bar{2}\} = \bar{2}.\mathbb{Z}_4$, logo é um ideal principal.

Exemplo: $\mathbb{Z}$ e $n\mathbb{Z}$ são aneis principais

Definição: Seja A um anel:

a) Um ideal P será chamado ideal primo de A se:

i) $P \neq A$
ii) Se $a, b \in A$, e $a.b \in P$, então $a \in P$ ou $b \in P$.

b) Um ideal M será chamado ideal maximal de A se:

i) $M \neq A$
ii) Se I é um ideal de A e $M \subset I$, então $I = A$.

Exemplos:

1) Em $\mathbb{Z}$ o ideal $P = \{0\}$ é primo, mas não é maximal.

De fato, sejam $a, b \in \mathbb{Z}$, se $a.b \in P \Rightarrow a.b = 0$, logo $a = 0 \Rightarrow a \in P$ ou $b = 0 \Rightarrow b \in P$.

Então P é primo.

$2\mathbb{Z}$ é um ideal de $\mathbb{Z}$ e $P \subset 2\mathbb{Z}$, como $2\mathbb{Z} \neq \mathbb{Z}$, temos que P não é maximal.

2) Em $\mathbb{Z}_4$ o ideal $I = \{\bar{0}\}$ não é maximal e nem primo.

De fato. $I \subset \{\bar{0}, \bar{2}\} \subset \mathbb{Z}_4$

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ $I \subset \mathbb{Z}_4$, e $I \subset \{\bar{0}, \bar{2}\} \subset \mathbb{Z}_4$

Vamos mostrar que ele não é primo. Temos que $\bar{2} \in \mathbb{Z}_4$ e $\bar{2}.\bar{2} = \bar{0} \in I$, mas $\bar{2} \notin I$.

<u>Proposição</u>: Se A é um anel comutativo com unidade, então todo ideal maximal é primo.