UMA INTRODUÇÃO A ANÉIS

TIAGO MACEDO

Resumo. Neste seminário vamos falar sobre conceitos básicos relacionados a anéis. Começaremos definindo o que é um anel e mostrando alguns exemplos. Em seguida, introduziremos a noção de morfismos de anéis e ideais. Por fim, vamos enunciar o famoso Teorema do Isomorfismo e mostrar uma de suas aplicações.

1. Definições e exemplos de anéis

Definição 1. Um anel é um conjunto R munido de duas funções

$$\begin{array}{rcl} \sigma : R \times R & \longrightarrow & R \\ (r,s) & \longmapsto & r+s \end{array} \qquad \begin{array}{rcl} \pi : R \times R & \longrightarrow & R \\ (r,s) & \longmapsto & r \cdot s \end{array}$$

satisfazendo as seguintes condições

1. (R, σ) é um grupo abeliano
2. $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ para quaisquer $r, s, t \in R$
3. $r \cdot (s+t) = r \cdot s + r \cdot t$ para quaisquer $r, s, t \in R$
4. $(s+t) \cdot r = s \cdot r + t \cdot r$ para quaisquer $r, s, t \in R$
5. Existe $e \in R$ tal que $e \cdot r = r = r \cdot e$ para qualquer $r \in R$.

Observação 2. (R, π) não é necessariamente um grupo. De fato, pode haver $r \in R$ para o qual não existe nenhum $s \in R$ tal que $r \cdot s = e$.

Exemplo 3. Considere $R = \mathbb{Z}$, $\sigma : R \times R \to R$ a soma usual e $\pi : R \times R \to R$ o produto usual de números inteiros. Nós já sabemos que $(\mathbb{Z}, \sigma)$ é um grupo abeliano. Do Ensino Fundamental, nós também sabemos que

2. $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ para quaisquer $r, s, t \in \mathbb{Z}$;
3. $r \cdot (s+t) = r \cdot s + r \cdot t$ para quaisquer $r, s, t \in \mathbb{Z}$;

Data: 8 de abril de 2014.

4. $(s+t)\cdot r = s\cdot r + t\cdot r$ para quaisquer $r,s,t\in\mathbb{Z}$;
5. $1\cdot r = r = r\cdot 1$ e $1\in\mathbb{Z}$.

Portanto $\mathbb{Z}$ é um anel. Observe ainda que $z_1\cdot z_2 = z_2\cdot z_1$ para quaisquer $z_1, z_2\in\mathbb{Z}$.

Exemplo 4. Considere $n>0$ e $\Bbbk=\mathbb{R}$ ou $\mathbb{C}$. Considere $\mathfrak{gl}_n(\Bbbk)$ o conjunto de matrizes de ordem $n\times n$ e entradas em $\Bbbk$

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}, \qquad a_{ij}\in\Bbbk.$$

Munindo $\mathfrak{gl}_n(\Bbbk)$ com a soma usual e multiplicação usual de matrizes, obtemos um anel.

Neste caso, observe que

$$0_{\mathfrak{gl}_n} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}, \quad e = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix},$$

$$-\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} -a_{11} & \cdots & -a_{1n} \\ \vdots & & \vdots \\ -a_{n1} & \cdots & -a_{nn} \end{pmatrix}.$$

Observe ainda que nem sempre $AB=BA$. De fato, tomando $n=2$, $A=\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ e $B=\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$, vemos que

$$AB = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \quad \text{e} \quad BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Definição 5. Um anel R munido das funções σ e π é dito:

(i) comutativo quando $r\cdot s = s\cdot r$ para quaisquer $r,s\in R$.
(ii) corpo quando $(R\setminus\{0\},\pi)$ é um grupo.

Exemplo 6. Como vimos no Exmeplo 3, $\mathbb{Z}$ é um anel comutativo. Mas $\mathbb{Z}$ não é um corpo. De fato, se $z\in\mathbb{Z}\setminus\{-1,1\}$, então não existe solução para a equação $xz=1$ em $\mathbb{Z}$.

Exemplo 7. Como vimos no Exemplo 4, $\mathfrak{gl}_n(\mathbb{k})$ é um anel que não é comutativo. Além disso, $\mathfrak{gl}_n(\mathbb{k})$ também não é um corpo. De fato, para que existisse uma matriz satisfazendo

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

teríamos que ter $0b + 0d = 1$, o que é impossível.

Exemplo 8. Tanto $\mathbb{Q}$, quanto $\mathbb{R}$, quanto $\mathbb{C}$ são corpos comutativos.

Exemplo 9. Considere $n > 0$ e o conjunto $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{(n-1)}\}$, munido da soma módulo n e do produto módulo n. Observe que:

- Para todo $d < n$ tal que $d > 1, d|n$, temos que $q \cdot d = n$ para algum $0 < q < n$. Logo $d \cdot x = 1$ se, e somente se, $\bar{0} \cdot \bar{x} = \overline{(q \cdot d)} \cdot \bar{x} = \bar{q} \cdot \overline{(d \cdot x)} = \bar{q} \cdot \bar{1} = \bar{q}$. Isso é uma contradição, logo $\bar{d}$ não tem inversos, se $d|n$. Consequentemente, $\mathbb{Z}_n$ não é um corpo, se n não for primo.
- Para todo $d < n$, tal que $(d, n) = 1$, existem $a, b \in \mathbb{Z}$ tais que $ad + bn = 1$. Logo $\overline{ad} = \bar{1}$, e $\bar{d}$ é inversível em $\mathbb{Z}_n$.

De fato, é possível mostrar que $\mathbb{Z}_p$ é um corpo se, e somente se, p for primo.

2. Morfismos de anéis

Definição 10. Considere dois anéis R e S. Um homomorfismo de anéis $\varphi : R \to S$ é uma função satisfazendo

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$,
2. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,
3. $\varphi(e_R) = e_S$,

para quaisquer $a, b \in R$. Um homomorfismo φ é dito isomorfismo, quando φ também for uma bijeção.

Exemplo 11. Dado um anel R, considere a função $id_R : R \to R$ dada por $id_R(r) = r$ para todo $r \in R$. Essa função, que é chamada de identidade, é um homomorfismo de anéis. De fato,

1. $id_R(a+b) = a+b = id_R(a) + id_R(b)$,
2. $id_R(a \cdot b) = a \cdot b = id_R(a) \cdot id_R(b)$,
3. $id_R(e_R) = e_r$,

para quaisquer $a, b \in R$.

Além disso, observe que para qualquer anel S e quaisquer homomorfismos $\varphi : R \to S$ e $\psi : S \to R$, temos que

$$\varphi \circ id_R(r) = \varphi(id_R(r)) = \varphi(r) \quad \text{para qualquer } r \in R,$$
$$id_R \circ \psi(s) = id_R(\psi(s)) = \psi(s) \quad \text{para qualquer } s \in S.$$

Exemplo 12. Considere três anéis R, S, T e dois homomorfismos de anéis $\varphi : R \to S$ e $\psi : S \to T$. A função $\psi \circ \varphi : R \to T$ é um homomorfismo de anéis. De fato,

1. $\psi \circ \varphi(a+b) = \psi(\varphi(a+b)) = \psi(\varphi(a) + \varphi(b))$
$= \psi(\varphi(a)) + \psi(\varphi(b)) = \psi \circ \varphi(a) + \psi \circ \varphi(b)$.
2. $\psi \circ \varphi(a \cdot b) = \psi(\varphi(a \cdot b)) = \psi(\varphi(a) \cdot \varphi(b))$
$= \psi(\varphi(a)) \cdot \psi(\varphi(b)) = (\psi \circ \varphi(a)) \cdot (\psi \circ \varphi(b))$.
3. $\psi \circ \varphi(e_R) = \psi(\varphi(e_R)) = \psi(e_S) = e_T$.

3. Teorema do isomorfismo para anéis

Nesta seção assuma que todo anel é comutativo com unidade.

Definição 13. Dado um homomorfismo de anéis $\varphi : R \to S$, definimos:

(a) O núcleo de φ como o conjunto $\ker \varphi = \{r \in R : \varphi(r) = 0_S\} \subseteq R$.
(b) A imagem de φ como o subconjunto

$$im(\varphi) = \{s \in S : s = \varphi(r) \text{ para algum } r \in R\} \subset S.$$

Dado um anel (A, σ, π), um subconjunto $I \subseteq A$ é dito um ideal quando:

(i) (I, σ) é um subgrupo de (A, σ),
(ii) $i \cdot a \in I$ para quaisquer $i \in I, a \in A$.

Dados um anel A e um ideal $I \subseteq A$, o anel quociente A/I é definido da seguinte forma:

(a) Como conjunto, ele é formado pelos elementos da forma $a+I$ com $a \in A$, satisfazendo $a+I = b+I$ quando $(a-b) \in I$;
(b) A função $\sigma : A/I \times A/I \to A/I$ dada por $\sigma(a+I, b+I) = (a+b)+I$ para todo $a, b \in A$;
(c) A função $\pi : A/I \times A/I \to A/I$ dada por $\pi(a+I, b+I) = (a \cdot b)+I$ para todo $a, b \in A$.

Teorema 14 (do Isomorfismo)**.** Se $\varphi : R \to S$ é um homomorfismo sobrejetivo de anéis, então

(i) $\ker \varphi \subseteq A$ é um ideal,
(ii) $R/\ker \varphi$ é isomorfo a S.

Exemplo 15. Todo subgrupo de $\mathbb{Z}$ é da forma

$$n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$$

para algum $n > 0$. Pelo Teorema do Isomorfismo, se $A = im\varphi$ para algum homomorfismo de anéis $\varphi : \mathbb{Z} \to A$, então $A \cong \mathbb{Z}/n\mathbb{Z}$ para algum $n > 0$. Vamos descrever o anel $\mathbb{Z}/n\mathbb{Z}$.

Por construção, $\mathbb{Z}/n\mathbb{Z}$ é o conjunto formado por $z + n\mathbb{Z}$, onde $z_1 + n\mathbb{Z} = z_2 + n\mathbb{Z}$ quando $n|(z_1 - z_2)$. Logo

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

Além disso, a soma é dada por

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z},$$

ou seja, a soma módulo n e o produto é dado por

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (a \cdot b) + n\mathbb{Z},$$

ou seja, o produto módulo n. A conclusão é que: toda imagem por homomorfismo do anel $\mathbb{Z}$ é isomorfa a $\mathbb{Z}_n$ para algum $n > 0$.