HOMOMORFISMOS DE ANÉIS
um resumo

Guilherme Philippi

16 de março de 2021

Esse texto pretende ser uma introdução aos conceitos fundamentais entorno de homomorfismos de anéis. Tudo que aqui se apresenta fora extraído de [1, 2, 3], principalmente de [3].

1 Grupos

Definição 1.1 (Grupo)**.** Um *grupo* $(G, *)$ é um conjunto G onde uma lei de composição $*$ é dada sobre G tal que os seguintes axiomas são satisfeitos:

1. *(Associatividade).* Para todo $a, b, c \in G$, tem-se
$$(a * b) * c = a * (b * c);$$
2. *(Existência da identidade).* Existe um elemento $\vec{1} \in G$ tal que, para todo $a \in G$,
$$\vec{1} * a = a * \vec{1} = a;$$
3. *(Existência do inverso).* Para todo $a \in G$ existe um elemento $a' \in G$ tal que
$$a * a' = a' * a = \vec{1}.$$

Observação 1.1 (Notação)**.** É comum abusar da notação e chamar um grupo $(G, *)$ e o conjunto de seus elementos G pelo mesmo simbolo, omitindo a lei de composição, na falta de ambiguidade. Também, quando não houver ambiguidade, suprimiremos o simbolo da lei, fazendo $a * b = ab$.

Definição 1.2 (Grupo abeliano)**.** Um *grupo abeliano* é um grupo G com uma *lei de composição comutativa*, isto é, $ab = ba$, para todo $a, b \in G$.

Proposição 1.1 (Lei do cancelamento)**.** *Seja a, b, c elementos de um grupo G. Se $ab = ac$, então $b = c$.*

2 Anéis

Definição 2.1 (Anel)**.** Um *anel* $(R, +, \cdot)$ é um conjunto R acompanhado de duas operações binárias $+$ e $\cdot$ definidas sobre R tais que os seguintes axiomas são satisfeitos:

1. $(R, +)$ é um grupo abeliano.
2. A operação $\cdot$ é associativa.
3. Para todo $a, b, c \in R$ vale a *lei da distributividade à esquerda* e a *lei de distributividade à direita*, respectivamente,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{e} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Exemplo 2.1. Todo subconjunto dos números complexos que é fechado para a adição e multiplicação usual dos complexos é um anel. Por exemplo, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são todos anéis.

Observação 2.1 (Notação)**.** Da mesma forma que com os grupos, costuma-se denotar o anel $(R, +, \cdot)$ apenas por seu conjunto R. Também, para um anel $(R, +, \cdot)$, chama-se sua primeira operação $+$ de *adição do anel* e sua segunda operação $\cdot$ de *multiplicação do anel.*

Proposição 2.1. *Se R é um anel com identidade aditiva $\vec{0}$, então, $\forall a \in R$,*

$$\vec{0} \cdot a = a \cdot \vec{0} = \vec{0}.$$

Demonstração. Pelas propriedades do grupo $(R, +)$,

$$a\vec{0} + a\vec{0} = a(\vec{0} + \vec{0}) = a\vec{0} = \vec{0} + a\vec{0}.$$

E, pela lei de cancelamento do grupo,

$$a\vec{0} + a\vec{0} = \vec{0} + a\vec{0} \implies a\vec{0} = \vec{0}.$$

De forma semelhante,

$$\vec{0}a + \vec{0}a = (\vec{0} + \vec{0})a = \vec{0}a = \vec{0} + \vec{0}a \implies \vec{0}a = \vec{0}.$$

Daí, segue que $a\vec{0} = \vec{0}a = \vec{0}$. □

Proposição 2.2. *Se R é um anel, então, para todo $a, b \in R$ vale*

1. $a(-b) = (-a)b = -(ab)$ *e*
2. $(-a)(-b) = ab$.

3 Homomorfismos de anéis

Definição 3.1 (Homomorfismo de anéis)**.** Sejam dois anéis $(R, +, \cdot)$ e $(R', +', \cdot')$. Um mapa $\phi : R \longrightarrow R'$ é um *homomorfismo* se a *propriedade de homomorfismo* vale para ambas as operações, isso é, se, para todo $a, b \in R$,

$$\phi(a + b) = \phi(a) +' \phi(b) \quad \text{e} \quad \phi(a \cdot b) = \phi(a) \cdot' \phi(b).$$

Exemplo 3.1 (Homomorfismo trivial)**.** Sejam os anéis R, R' e o elemento neutro $\vec{0}$ da adição do anel R'. A aplicação $\phi : R \longrightarrow R'$ definida por $\phi(a) = \vec{0}$, para todo $a \in R$, é um homomorfismo de anéis porque

$$\phi(a + b) = \vec{0} = \vec{0} \ +' \vec{0} = f(a) +' f(b) \quad \text{e} \quad f(a \cdot b) = \vec{0} = \vec{0} \ \cdot' \vec{0} = f(a) \ \cdot' f(b).$$

A essa aplicação dá-se o nome *homomorfismo trivial de anéis.*

Definição 3.2 (Homomorfismo injetivo e sobrejetivo)**.** Chama-se de *homomorfismo injetivo* e *homomorfismo sobrejetivo* um homomorfismo de anéis definido, respectivamente, por uma função injetiva ou uma função sobrejetiva.

Exemplo 3.2. Seja o homomorfismo de anéis $\phi : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ tal que $\phi(n) = (n, 0)$, para todo $n \in \mathbb{Z}$. Perceba que, para cada $(n, 0) \in \mathbb{Z} \times \mathbb{Z}$ tem-se um único $n \in \mathbb{Z}$ tal que $\phi(n) = (n, 0)$, daí, ϕ é injetiva e esse é um homomorfismo injetivo. Também, seja $\mu : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ o homomorfismo tal que $\mu(n, m) = n$ para todo $(n, m) \in \mathbb{Z} \times \mathbb{Z}$. É fácil perceber que para todo $z \in \mathbb{Z}$, existirá $(z, 0) \in \mathbb{Z} \times \mathbb{Z}$, donde μ é um homomorfismo sobrejetivo.

Proposição 3.1. *Se $\phi : R \longrightarrow R'$ é um homomorfismo de anéis, então, para todo $a, b \in A$,*

- $\phi(0_R) = 0_{R'}$,
- $\phi(-a) = -\phi(a)$ *e*
- $\phi(a - b) = \phi(a) - \phi(b)$.

Demonstração. Como $\phi(a) = \phi(a + 0_R) = \phi(a) + \phi(0_R)$, pela propriedade de homomorfismo, então,

$$\phi(a) = \phi(a) + \phi(0_R) \implies -\phi(a) + \phi(a) = -\phi(a) + \phi(a) + \phi(0_R),$$

isto é, $0_{R'} = \phi(0_R)$.

Daí segue que,

$$0_{R'} = \phi(0_R) = \phi(a - a) = \phi(a) + \phi(-a),$$

e como $0_{R'} = \phi(a) + \phi(-a)$,

$$\phi(-a) = -\phi(a).$$

Fica evidente que

$$\phi(a - b) = \phi(a) + \phi(-b) = \phi(a) - \phi(b).$$

□

Proposição 3.2. *Seja* $\phi : R \longleftarrow R'$ *um homomorfismo de anéis onde* $1_R \in R$ *é identidade do produto de* R*. Então*

- R' *possui identidade multiplicativa* $1_{R'}$ *e* $\phi(1_R) = 1_{R'}$*;*
- *se* $a \in R$ *possui inversa multiplicativa* a^{-1}*, então* $\phi(a)^{-1} = \phi(a^{-1})$*.*

Definição 3.3 (Imagem de homomorfismo de anéis)**.** A *imagem* de um homomorfismo de anéis $\phi : R \longrightarrow R'$ é o subconjunto de R'

$$\text{im } \phi = \{x \in R' \mid x = \phi(a), \text{ para algum } a \in R\} = \phi(R).$$

Definição 3.4 (subanel)**.** Um subconjunto S de um anel R é um subanel de R (escreve-se $S \leq R$) se, e somente se, valem os seguintes axiomas:

1. *(Existência do elemento nulo).* $0 \in S$;
2. *(Subtração fechada).* $a - b \in S$, para todo $a, b \in S$;
3. *(Produto fechado).* $ab \in S$, para todo $a, b \in S$.

Proposição 3.3. *Seja* $(S, +, \cdot)$ *um subanel de* $(R, +, \cdot)$*. Então* $(S, +, \cdot)$ *é um anel.*

Proposição 3.4. *Seja um homomorfismo de anéis* $\phi : R \longrightarrow R'$*, então a imagem* $\phi(R) \leq R'$ *e, além disso, se* $S \leq R$ *então* $\phi(S) \leq R'$*.*

Demonstração. Como S é um subanel de R, então $0_R \in S$ e $\phi(0_R) = 0_{R'}$ implica que $0_{R'} \in \phi(S)$. Além disso, sejam $a, b \in \phi(S)$, então existem $s_1, s_2 \in S$ tais que $\phi(s_1) = a$, $\phi(s_2) = b$ e, como S é anel, $s_1 - s_2 \in S$ e segue que $\phi(s_1 - s_2) \in \phi(S)$. Como $\phi(s_1 - s_2) = \phi(s_1) - \phi(s_2) = a - b$, $a - b \in \phi(S)$. De forma semelhante para o produto, $a, b \in \phi(S) \implies s_1 s_2 \in S \implies ab \in \phi(S)$. □

Proposição 3.5. *Sejam* $\phi : R \longrightarrow T$ *e* $\mu : T \longrightarrow R'$ *homomorfismos de anéis. Então,* $\mu \circ \phi : R \longrightarrow R'$ *também é um homomorfismo de anéis.*

Demonstração. Sejam $a, b \in R$. Como ϕ é homomorfismo, segue que

$$\phi(a + b) = \phi(a) + \phi(b) \text{ e } \phi(ab) = \phi(a)\phi(b).$$

Portanto, aplicando μ,

$$\mu \circ \phi(a + b) = \mu(\phi(a) + \phi(b)) \text{ e } \mu \circ \phi(ab) = \mu(\phi(a)\phi(b)),$$

Mas como μ também respeita a propriedade de homomorfismo, segue que

$$\mu(\phi(a) + \phi(b)) = \mu(\phi(a)) + \mu(\phi(b)) = \mu \circ \phi(a) + \mu \circ \phi(b) \text{ e}$$

$$\mu(\phi(a)\phi(b)) = \mu(\phi(a))\mu(\phi(b)) = \mu \circ \phi(a)\mu \circ \phi(b).$$

□

Definição 3.5 (Núcleo)**.** O *núcleo* do homomorfismo de anéis $\phi : R \longrightarrow R'$ é o subconjunto de R formado pelos elementos que são mapeados pelo elemento nulo em R':

$$\text{nu } \phi = \{a \in R \mid \phi(a) = 0\}.$$

Exemplo 3.3. Seja $\phi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ definida por $\phi(a, b) = a$. Então ϕ é um homomorfismo de anéis e

$$\text{nu } \phi = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a = 0\}.$$

Proposição 3.6. *Seja um homomorfismo* $\phi : R \longrightarrow R'$ *com núcleo* nu ϕ *e seja* 0_R *o elemento nulo de* R*. Então* $0_R \in \text{nu } \phi$.

Proposição 3.7. *Seja* $\phi : R \longrightarrow R'$ *um homomorfismo de anéis. Então*

- *nu* $\phi \leq R$;
- ϕ *é injetor se, e somente se, nu* $\phi = \{0_R\}$.

Referências

[1] John B Fraleigh. *A First Course in Abstract Algebra.* Pearson, 2014.

[2] Michael Artin. *Algebra.* A Simon and Schuster Company, 1991.

[3] GELSON IEZZI and Hygino H DOMINGUES. Álgebra moderna. *São Paulo: Atual Editora*, 2003.