~~Essa idéia pressupõe, de um lado, uma correspondência biunívoca entre todos os anéis da mesma classe. E, de outro, que essa correspondência preserve as operações envolvidas, no sentido da definição 12.~~

5. HOMOMORFISMOS DE ANÉIS

Definição 12: Dá-se o nome de *homomorfismo* de um anel $(A, +, \cdot)$ num anel $(B, +, \cdot)$ a toda aplicação $f: A \to B$ tal que, quaisquer que sejam $x, y \in A$:

$$f(x + y) = f(x) + f(y)$$

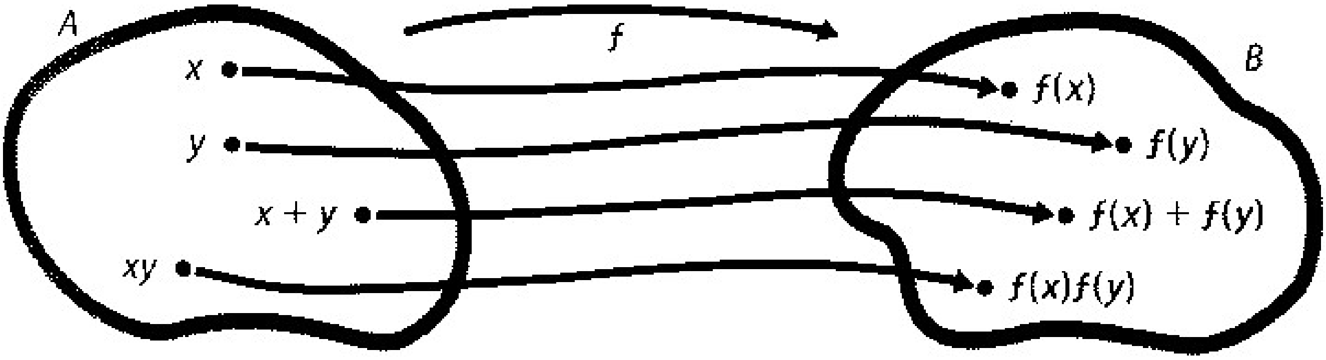
e

$$f(xy) = f(x)f(y).$$

Nessas condições, para simplificar a linguagem, nos referiremos a $f: A \to B$ como um *homomorfismo de anéis*. Quando se tratar do mesmo anel, o que pressupõe $A = B$, a mesma adição e a mesma multiplicação em A, tanto como domínio como contradomínio, então f será chamada de *homomorfismo* de A.

Se um homomorfismo é uma função injetora, então é chamado de *homomorfismo injetor*. E, se for uma função sobrejetora, de *homomorfismo sobrejetor*. O caso em que f é bijetora corresponde ao conceito de *isomorfismo* e será estudado separadamente.

~~Convém observar ainda que, se A e B são anéis, então $(A, +)$ e $(B, +)$ são grupos e, portanto, um homomorfismo de anéis $f: A \to B$ também é um homomorfismo do grupo aditivo A no grupo aditivo B.~~



Exemplo 23: Quaisquer que sejam os anéis A e B, a aplicação $f: A \to B$, $f(x) = 0_B$ $(x \in A)$ é um homomorfismo de anéis, já que:

- $f(a + b) = 0_B = 0_B + 0_B = f(a) + f(b)$;
- $f(ab) = 0_B = 0_B \cdot 0_B = f(a)f(b)$.

Exemplo 24: Consideremos os anéis $A = \mathbb{Z}$ e $B = \mathbb{Z} \times \mathbb{Z}$ (produto direto) e a aplicação $f: A \to B$ assim definida: $f(n) = (n, 0)$. A aplicação f é um homomorfismo, pois:

- $f(m + n) = (m + n, 0) = (m, 0) + (n, 0) = f(m) + f(n)$;
- $f(mn) = (mn, 0) = (m, 0)(n, 0) = f(m)f(n)$.

Exemplo 25: Para cada inteiro $m > 1$, há um homomorfismo natural do anel $\mathbb{Z}$ no anel $\mathbb{Z}_m$ das classes de resto módulo m: a aplicação $p_m: \mathbb{Z} \to \mathbb{Z}_m$ definida por $p_m(r) = \overline{r}$, para cada $r \in \mathbb{Z}$. De fato, para quaisquer $r, s \in \mathbb{Z}$:

- $p_m(r + s) = \overline{r + s} = \overline{r} + \overline{s} = p_m(r) + p_m(s)$;
- $p_m(rs) = \overline{rs} = \overline{r}\,\overline{s} = p_m(r)\,p_m(s)$

p_m é um homomorfismo sobrejetor, porque todo $y \in \mathbb{Z}_m$ é uma classe $y = \overline{r}$, que obviamente provém de $r \in \mathbb{Z}$ através de p_m.

Exemplo 26: Seja $A = \mathbb{Z}\left[\sqrt{2}\right] = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ e consideremos $f: A \to A$ assim definida: $f\left(m + n\sqrt{2}\right) = m - n\sqrt{2}$ · f é um homomorfismo de anéis, pois:

- $f\left(\left(m + n\sqrt{2}\right) + \left(r + s\sqrt{2}\right)\right) = f\left((m + r) + (n + s)\sqrt{2}\right) = (m + r) - (n + s)\sqrt{2}$

e também

$$f\left(m + n\sqrt{2}\right) + f\left(r + s\sqrt{2}\right) = \left(m - n\sqrt{2}\right) + \left(r - s\sqrt{2}\right) = (m + r) - (n + s)\sqrt{2}$$

- $f\left(\left(m + n\sqrt{2}\right)\left(r + s\sqrt{2}\right)\right) = f\left((mr + 2ns) + (ms + nr)\sqrt{2}\right) = (mr + 2ns) - (ms + nr)\sqrt{2}$

e também

$$f\left(m + n\sqrt{2}\right)f\left(r + s\sqrt{2}\right) = \left(m - n\sqrt{2}\right)\left(r - s\sqrt{2}\right) = (mr + 2ns) - (ms + nr)\sqrt{2}\,.$$

6. PROPOSIÇÕES SOBRE HOMOMORFISMOS DE ANÉIS

Demonstrar!! **Proposição 8:** Se $f: A \to B$ é um homomorfismo de anéis, então: (i) $f(0_A) = 0_B$; (ii) $f(-a) = -f(a)$; (iii) $f(a - b) = f(a) - f(b)$.

~~Essas propriedades decorrem do fato de que f é um homomorfismo do grupo aditivo A no grupo aditivo B. #~~

Proposição 9: Seja $f: A \to B$ um homomorfismo sobrejetor de anéis e suponhamos que A possua unidade. Então: (i) $f(1_A)$ é a unidade de B e, portanto, B também é um anel com unidade; (ii) se $a \in A$ é inversível, então $f(a)$ também o é e $[f(a)]^{-1} = f(a^{-1})$.

Demonstração:

(i) Seja b um elemento arbitrário de B. Como f é sobrejetora, então $b = f(a)$, para algum $a \in A$. Portanto:

$$b \cdot f(1_A) = f(a)f(1_A) = f(a \cdot 1_A) = f(a) = b$$

Analogamente se mostra que $f(1_A) \cdot b = b$. Logo, $f(1_A)$ é a unidade de B.

(ii) Observemos que:

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_B$$

De modo análogo:

$$f(a^{-1})f(a) = f(a^{-1}a) = f(1_A) = 1_B$$

Portanto:

$$f(a^{-1}) = [f(a)]^{-1} \;\#$$

Contra-exemplo 4: O homomorfismo $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ do exemplo 24 não é sobrejetor, pois $Im(f) = \{(n, 0) \mid n \in \mathbb{Z}\} \neq \mathbb{Z} \times \mathbb{Z}$. Neste caso, $f(1) = (1, 0) \neq (1, 1)$, ou seja, a imagem da unidade de $\mathbb{Z}$ (o número 1) não é a unidade de $\mathbb{Z} \times \mathbb{Z}$, que é o par $(1, 1)$.

Demonstrar!!! **Proposição 10:** (i) Se $f: A \to B$ é um homomorfismo de anéis e L é um subanel de A, então $f(L)$ é um subanel de B; ~~(ii) se $f: M \to N$ é um homomorfismo de corpos, $f(1_m) \neq 0_n$ e K é um subcorpo de M, então $f(K)$ é um subcorpo de N~~.

~~*Demonstração:*~~

~~Demonstraremos apenas (ii). A demonstração de (i) é análoga e fica proposta como exercício.~~

~~Sejam $c, d \in f(K)$. Então $c = f(a)$ e $d = f(b)$, para convenientes elementos a, $b \in K$. Logo:~~

$$\cancel{c - d = f(a) - f(b) = f(a - b)}$$

~~Como $a - b \in K$, pois K é um subgrupo do grupo aditivo M, então $c - d \in f(K)$. Além disso, se $d \neq 0$, então $b \neq 0$ e, portanto:~~

$$\cancel{cd^{-1} = f(a)[f(b)]^{-1} = f(a)f(b^{-1}) = f(ab^{-1})}$$

~~Como $ab^{-1} \in K$, porque K é subcorpo de M, então $cd^{-1} \in f(K)$. #~~

~~Em particular, com as condições da proposição, $Im(f)$ é um subanel (subcorpo) do contradomínio — naturalmente o próprio B (ou N) se f for sobrejetora.~~

Exemplo 27: Se $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ é o homomorfismo do exemplo 24, então $Im(f) = \{(n, 0) \mid n \in \mathbb{Z}\}$ é um subanel de $\mathbb{Z} \times \mathbb{Z}$.

Demonstrar!!! **Proposição 11:** Sejam $f: A \to B$ e $g: B \to C$ homomorfismos de anéis. Então $g \circ f: A \to C$ também é um homomorfismo de anéis.

Deixamos a *demonstração* como exercício. Sugerimos ao estudante que tiver dúvidas reler a demonstração da proposição 5, capítulo IV. A argumentação é a mesma da demonstração citada — só que, obviamente, deverá ser usada para a adição e a multiplicação. #

7. NÚCLEO DE UM HOMOMORFISMO DE ANÉIS

Definição 13: Seja $f: A \to B$ um homomorfismo de anéis. Damos o nome de *núcleo de* f, e denotamos por $N(f)$ (usa-se também a notação $Ker(f)$), ao seguinte subconjunto de A:

$$N(f) = \{x \in A \mid f(x) = 0_B\}$$

Vale observar que, como $f(0_A) = 0_B$ (proposição 8), então $0_A \in N(f)$. Logo, pelo menos o zero de A pertence ao núcleo de f.

Exemplo 28: O núcleo do homomorfismo do exemplo 23 é A, já que, devido à definição de f, todos os elementos de A têm imagem igual a 0_B.

Exemplo 29: Determinemos o núcleo do homomorfismo $p_m: \mathbb{Z} \to \mathbb{Z}_m$ do exemplo 25. Lembremos que p_m é definido assim: $p_m(r) = \overline{r}$ $(r \in \mathbb{Z})$.

Um inteiro $r \in N(p_m)$ se, e somente se, $\overline{r} = \overline{0}$;

se, e somente se, $r \equiv 0 \pmod{m}$;

se, e somente se, r é múltiplo de m.

Portanto, $N(p_m) = \{0\ , \pm m, \pm 2m, ...\}$.

Exemplo 30: Determinemos o núcleo do homomorfismo $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ do exemplo 24. Como o zero do anel $\mathbb{Z} \times \mathbb{Z}$ é o par $(0, 0)$, então um inteiro n pertence a $N(f)$ se, e somente se, $f(n) = (n, 0) = (0, 0)$. Ou seja, se, e somente se, $n = 0$. Logo, $N(f) = \{0\}$.

Exemplo 31: Vamos encontrar agora o núcleo do homomorfismo f do exemplo 26. Neste caso os anéis são $A = B = \mathbb{Z}\left[\sqrt{2}\right]$ e o zero de B é o número 0. Então um número $a + b\sqrt{2}$ pertence a $N(f)$ se, e somente se, $f(a + b\sqrt{2}) = a - b\sqrt{2} = 0$. Mas isso implica que $a = b = 0$ e, portanto, $a + b\sqrt{2} = 0$. Logo, $N(f) = \{0\}$.

Exemplo 32: Consideremos $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida por $f(a, b) = a$. É fácil provar que f é um homomorfismo de anéis (deixamos como exercício a verificação desse fato). Então um par $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ pertence a $N(f)$ se, e somente se, $f(a, b) = a = 0$. Portanto:

$$N(f) = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid f(a, b) = a = 0\} = \{(0, b) \mid b \in \mathbb{Z}\}$$

Note-se que, neste caso, $N(f)$ é um conjunto infinito.

Proposição 12: Seja $f: A \to B$ um homomorfismo de anéis. Então: (i) $N(f)$ é um subanel de A; (ii) f é injetor se, e somente se, $N(f) = \{0_A\}$.

Demonstração:

(i) Se $a, b \in N(f)$, então $f(a) = f(b) = 0_B$. Daí, $f(a - b) = f(a) - f(b) = 0_B$ e $f(ab) = f(a)f(b) = 0_B \cdot 0_B = 0_B$. Portanto, $a - b, ab \in N(f)$, o que prova que o núcleo de f é um subanel de A.

(ii) Considerando-se que A e B são grupos aditivos e que f é, em particular, um homomorfismo de grupos aditivos, então (devido à proposição 6, capítulo IV) f é injetor se, e somente se, $N(f) = \{0_A\}$. #

~~8. ISOMORFISMO DE ANÉIS~~

~~Consideremos os anéis $\mathbb{Z}_6$ e $\mathbb{Z}_2 \times \mathbb{Z}_3$ (produto direto), ambos constituídos de 6 elementos. À primeira vista, é difícil perceber algo em comum entre eles além da cardinalidade: afinal, os elementos e as operações de um e de outro têm natureza diferente. Na verdade, porém, pode-se mostrar que, enquanto anéis, eles "têm tudo" em comum.~~