Capítulo 2

Anéis

2.1 Conceitos básicos

Definição 2.1.1. Um *anel* é um triplo $(A, +, \cdot)$ em que A é um conjunto e $+$ e $\cdot$ são operações binárias em A tais que

- $(A, +)$ é um grupo abeliano;
- $(A, \cdot)$ é um monóide;
- para quaisquer $a, b, c \in A$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ e $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (*distributividade* de $\cdot$ em relação a $+$).

A operação $+$ diz-se a *adição* do anel e a operação $\cdot$ diz-se a *multiplicação* do anel. Muitas vezes indica-se um anel pelo símbolo do conjunto subjacente, isto é, escreve-se simplesmente A em vez de $(A, +, \cdot)$. O elemento neutro do *grupo aditivo* $(A, +)$ de um anel $A = (A, +, \cdot)$ é denotado por 0. O elemento neutro do *monóide multiplicativo* $(A, \cdot)$ de A é chamado *identidade* de A e é denotado por 1. O *simétrico* de um elemento a de um anel A é o inverso de a no grupo aditivo de A e é denotado por $-a$. Se a é invertível no monóide multiplicativo de A, o *inverso* de a é o inverso de a em $(A, \cdot)$ e é denotado por a^{-1}. Um elemento invertível no monóide multiplicativo de A diz-se uma *unidade* de A. Omitiremos muitas vezes o símbolo da multipicação e escreveremos ab em vez de $a \cdot b$. Usaremos as convenções habituais de omissão de parênteses e escreveremos, por exemplo, $ab + c$ em vez de $(ab) + c$ e $-ab$ em vez de $-(ab)$. Um anel diz-se *comutativo* se a sua multiplicação é comutativa.

Nota 2.1.2. Alguns autores não exigem a existência de um elemento neutro para a multiplicação na definição de um anel. Num tal contexto, a nossa definição de anel corresponde à noção de *anel unitário* ou *anel com identidade*.

Exemplos 2.1.3. (i) $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são anéis comutativos relativamente à adição e à multiplicação habituais.

(ii) Para qualquer inteiro $n \geq 1$, o grupo abeliano $\mathbb{Z}_n$ é um anel comutativo relativamente à multiplicação dada por $(k + n\mathbb{Z}) \cdot (l + n\mathbb{Z}) = kl + n\mathbb{Z}$.

(iii) Para cada natural $n \geq 1$, o conjunto $\mathcal{M}_{n\times n}(\mathbb{R})$ das matrizes reais $n \times n$ é um anel relativamente à adição e à multiplicação de matrizes.

(iv) O *produto directo* $A_1 \times \cdots \times A_n$ dos anéis $A_1, \ldots, A_n$ é o anel cujo conjunto subjacente é o produto cartesiano $A_1 \times \cdots \times A_n$ e cujas operações $+$ e $\cdot$ são definidas componente por componente.

(v) O conjunto $\{0\}$ admite uma única estrutura de anel. Note-se que neste anel, $1 = 0$.

Proposição 2.1.4. *Sejam A um anel e $x, y \in A$. Então*

(i) $0x = x0 = 0$;

(ii) $(-x)y = x(-y) = -xy$;

(iii) $(-x)(-y) = xy$.

Demonstração: (i) Tem-se $0x = (0 + 0)x = 0x + 0x$ e portanto $0 = 0x - 0x = 0x$. Do mesmo modo, $x0 = 0$.

(ii) Tem-se $xy + (-x)y = (x + (-x))y = 0y = 0$ e portanto $-xy = (-x)y$. Do mesmo modo, $-xy = x(-y)$.

(iii) Tem-se $(-x)(-y) = -x(-y) = -(-xy) = xy$. □

Observação 2.1.5. Pela propriedade (ii) da proposição precedente, $(-1)x = x(-1) = -x$ para qualquer elemento x de um anel.

Proposição 2.1.6. *Sejam A um anel, $n, m \geq 1$ inteiros e $x_1, \ldots, x_n, y_1, \ldots, y_m \in A$. Então*

$$\left(\sum_{i=1}^{n} x_i\right) \cdot \left(\sum_{j=1}^{m} y_j\right) = \sum_{1\leq i\leq n,\ 1\leq j\leq m} x_i y_j.$$

Demonstração: Exercício. □

Proposição 2.1.7. *Sejam A um anel, $n \in \mathbb{N}$ e $a, b \in A$ tais que $ab = ba$. Então*

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

Demonstração: Exercício. □

Definição 2.1.8. Um subconjunto B de um anel A diz-se um *subanel* de A se $1 \in B$ e para quaisquer $x, y \in B$, $x - y \in B$ e $xy \in B$.

Observação 2.1.9. Um subanel B de um anel A é um anel relativamente à adição e à multiplicação de A.

Exemplos 2.1.10. (i) Qualquer anel é sempre um subanel de si próprio.
(ii) O único subanel de $\mathbb{Z}$ é $\mathbb{Z}$.
(iii) O único subanel de $\mathbb{Z}_n$ é $\mathbb{Z}_n$.
(iv) $\mathbb{Q}$ é um subanel de $\mathbb{R}$.
(v) Os matrizes reais diagonais $n \times n$ formam um subanel de $\mathcal{M}_n(\mathbb{R})$.

Definição 2.1.11. Um aplicação entre dois anéis $f\colon A \to B$ diz-se um *homomorfismo de anéis* se $f(1) = 1$ e se para quaisquer dois elements $x, y \in A$, $f(x + y) = f(x) + f(y)$ e $f(xy) = f(x)f(y)$. Um homomorfismo de anéis diz-se um *monomorfismo* (*epimorfismo, isomorfismo*) se é injectivo (sobrejectivo, bijectivo). Um homomorfismo (isomorfismo) de anéis $f\colon A \to A$ diz-se um *endomorfismo* (*automorfismo*) de anéis. Dois anéis A e B dizem-se *isomorfos*, $A \cong B$, se existe um isomorfismo de anéis entre eles.

Observações 2.1.12. (i) Um homomorfismo de anéis é um homomorfismo dos grupos aditivos. Em particular $f(0) = 0$.
(ii) O núcleo Ker$f$ de um homomorfismo de anéis $f\colon A \to B$ é o seu núcleo enquanto homomorfismo de grupos aditivos, isto é, $Ker(f) = \{a \in A \mid f(a) = 0\}$.
(ii) Um homomorfismo de anéis $f\colon A \to B$ é um monomorfismo de anéis se e só se é um monomorfismo de grupos aditivos e isto é caso se e só se $\mathrm{Ker}(f) = \{0\}$.

Exemplos 2.1.13. (i) Se B é um subanel do anel A, então a inclusão $B \to A$, $x \mapsto x$ é um monomorfismo de anéis.
(ii) Para qualquer anel A, id_A é um automorfismo de anéis.
(iv) O epimorfismo canónico $\mathbb{Z} \to \mathbb{Z}_n$, $k \mapsto k + n\mathbb{Z}$ é um epimorfismo de anéis.

Proposição 2.1.14. *A composta de dois homomorfismos de anéis $f\colon A \to B$ e $g\colon B \to C$ é um homomorfismo de anéis.*

Demonstração: A composta $g \circ f\colon A \to C$ é um homorfismo de grupos. Como $g \circ f(1) = g(f(1)) = g(1) = 1$ e $g \circ f(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = g \circ f(x)g \circ f(y)$ para todos os $x, y \in A$, $g \circ f$ é um homomorfismo de anéis. □

Proposição 2.1.15. *A função inversa de um isomorfismo de anéis $f\colon A \to B$ é um isomorfismo de anéis.*

Demonstração: Por 1.3.8, f^{-1} é um isomorfismo de grupos. Como $f(1) = 1$, $1 = f^{-1}(f(1)) = f^{-1}(1)$. Para quaisquer $x, y \in B$, $f(f^{-1}(xy)) = xy = f(f^{-1}(x))f(f^{-1}(y)) = f(f^{-1}(x)f^{-1}(y))$. Como f é um monomorfismo, isto implica que $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$. Segue-se que f^{-1} é um homomorfismo de anéis e então um isomorfismo de anéis. □

Proposição 2.1.16. *Sejam $f\colon A \to B$ um homomorfismo de anéis, X um subanel de A e Y um subanel de B. Então $f(X)$ é um subanel de B e $f^{-1}(Y)$ é um subanel de A.*

Demonstração: Como $1 \in X$, $1 = f(1) \in f(X)$. Sejam $x, y \in X$. Então $x - y, xy \in X$. Logo $f(x) - f(y) = f(x - y) \in f(X)$ e $f(x)f(y) = f(xy) \in f(X)$. Segue-se que $f(X)$ é um subanel de B. Como $f(1) = 1 \in Y$, $1 \in f^{-1}(Y)$. Sejam $x, y \in f^{-1}(Y)$. Então $f(x-y) = f(x)-f(y) \in Y$ e $f(xy) = f(x)f(y) \in Y$. Logo $x-y \in f^{-1}(Y)$ e $xy \in f^{-1}(Y)$. Segue-se que $f^{-1}(Y)$ é um subanel de A. □

2.2 Ideais e anéis quociente

Definição 2.2.1. Um *ideal* de um anel A é um subgrupo I do grupo aditivo de A tal que para quaisquer $a \in A$ e $x \in I$, $ax \in I$ e $xa \in I$.

Observações 2.2.2. (i) Como o grupo aditivo de um anel é abeliano, qualquer ideal de um anel é um subgrupo normal do anel.

(ii) Se um ideal I de um anel A contém o elemento 1, então $I = A$. Com efeito, para qualquer $a \in A$, $a = 1a \in I$.

Exemplos 2.2.3. (i) Em qualquer anel A, $\{0\}$ e A são ideais.

(ii) Para $n \in \mathbb{Z}$, $n\mathbb{Z}$ é um ideal em $\mathbb{Z}$.

(iii) Sejam A e B dois anéis, I um ideal de A e J um ideal de B. Então $I \times J$ é um ideal em $A \times B$.

Proposição 2.2.4. *Sejam $f\colon A \to B$ um homomorfismo de anéis, I um ideal de A e J um ideal de B. Então $f(I)$ é um ideal de* $\mathrm{Im}(f)$ *e $f^{-1}(J)$ é um ideal de A. Em particular,* $\mathrm{Ker}(f) = f^{-1}(\{0\})$ *é um ideal de A.*

Demonstração: Por 1.6.5, $f(I)$ é um subgrupo do grupo aditivo de $\mathrm{Im}(f)$ e $f^{-1}(J)$ é um subgrupo do grupo aditivo de A. Sejam $a \in A$ e $x \in I$. Então $f(a)f(x) = f(ax) \in f(I)$ e $f(x)f(a) = f(xa) \in f(I)$. Segue-se que $f(I)$ é um ideal de $\mathrm{Im}(f)$. Sejam $a \in A$ e $x \in f^{-1}(J)$. Então $f(ax) = f(a)f(x) \in J$ e $f(xa) = f(x)f(a) \in J$, pelo que $ax \in f^{-1}(J)$ e $xa \in f^{-1}(J)$. Segue-se que $f^{-1}(J)$ é um ideal de A. □

Proposição 2.2.5. *Sejam A um anel e $(I_k)_{k\in K}$ uma familia não vazia de ideais de A. Então $\bigcap_{k\in K} I_k$ é um ideal de A.*

Demonstração: Por 1.4.11, $\bigcap_{k\in K} I_k$ é um subgrupo do grupo aditivo de A. Sejam $a \in A$ e $x \in \bigcap_{k\in K} I_k$. Então $x \in I_k$ para todo o $k \in K$. Logo $ax \in I_k$ e $xa \in I_k$ para todo o $k \in K$. Segue-se que ax, $xa \in \bigcap_{k\in K} I_k$ e que $\bigcap_{k\in K} I_k$ é um ideal de A. □

Definição 2.2.6. Sejam A um anel e $X \subseteq A$ um subconjunto. O *ideal gerado por* X, (X), é a intersecção dos ideais de A que contêm X. Se $X = \{x_1, \ldots, x_n\}$, escrevemos também $(x_1, \ldots, x_n)$ em vez de (X) e falamos do *ideal de A gerado pelos elementos* $x_1, \ldots, x_n$.

Proposição 2.2.7. *Sejam A um anel e $X \subseteq A$ um subconjunto. Então os elementos de (X) são o elemento 0 e as somas finitas formadas a partir dos elementos da forma axb, onde $a, b \in A$ e $x \in X$.*

Demonstração: Seja I o subconjunto de A cujos elementos são o elemento 0 e as somas finitas formadas a partir dos elementos de A da forma axb, onde $a, b \in A$ e $x \in X$. Então I é um ideal de A e $X \subseteq I$. Logo $(X) \subseteq I$. Por outro lado, qualquer elemento de I pertence necessariamente a qualquer ideal de A que contém X. Logo $I \subseteq (X)$. □

Exemplos 2.2.8. (i) Em qualquer anel A, $(\emptyset) = \{0\}$.

(ii) Num anel comutativo A, tem-se $(a) = aA = \{ax \mid x \in A\}$ para todo o $a \in A$. Em particular, em $\mathbb{Z}$, $(n) = n\mathbb{Z}$. Em $\mathbb{Z}_4$, $([2]) = [2]\mathbb{Z}_2 = \{[0], [2]\}$.

Nota 2.2.9. Sejam A um anel e I e J ideais de A. Então a soma $I + J = \{i + j \mid i \in I,\ j \in J\}$ também é um ideal de A e tem-se $(I \cup J) = I + J$.

Definição 2.2.10. Um ideal I de um anel A diz-se *principal* se existe um elemento $a \in A$ tal que $I = (a)$.

Exemplos 2.2.11. (i) Seja A um anel cujo grupo aditivo é cíclico. Então qualquer subgrupo de A é um ideal principal. Com efeito, seja $A = \langle a \rangle$ e consideremos um inteiro k e o subgrupo $I = \langle ka \rangle$. Então a^2 é um múltiplo de a e isto implica que I é um ideal de A. Como $(ka) \subseteq I = \langle ka \rangle \subseteq (ka)$, $I = (ka)$. Em particular, todos os subgrupos de $\mathbb{Z}$ e $\mathbb{Z}_n$ são ideais principais.

Lema 2.2.12. *Sejam A um anel, I um ideal de A e $a, a', b, b' \in A$ tais que $a - a', b - b' \in I$. Então $ab - a'b' \in I$.*

Demonstração: Tem-se $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I$. □

Definição 2.2.13. Sejam A um anel e I um ideal. O *anel quociente* A/I é o grupo quociente A/I com a multiplicação definida por $(a+I)\cdot(b+I) = ab+I$. Pelo lema precedente, esta multiplicação está bem definida. Verifica-se facilmente que A/I é um anel e que o epimorfismo canónico $A \to A/I$, $a \mapsto a+I$ é um homomorfismo de anéis.

Exemplo 2.2.14. O anel $\mathbb{Z}_n$ é o anel quociente $\mathbb{Z}/n\mathbb{Z}$.

Teorema 2.2.15. *Sejam $f\colon A \to A'$ um homomorfismo de anéis, $I \subseteq A$ um ideal tal que $I \subseteq \mathrm{Ker}(f)$ e $\pi\colon A \to A/I$ o epimorfismo canónico. Então existe um único homomorfismo de anéis $\bar{f}\colon A/I \to A'$ tal que $\bar{f}\circ\pi = f$. O homomorfismo $\bar{f}$ é dado por $\bar{f}(a+I) = f(a)$ e é injetivo se e só se $I = \mathrm{Ker}(f)$.*

Demonstração: Por 1.6.13, existe um único homomorfismo de grupos $\bar{f}\colon A/I \to A'$ tal que $\bar{f}\circ\pi = f$. Como $\bar{f}(1+I) = \bar{f}\circ\pi(1) = f(1) = 1$ e $\bar{f}((a+I)(b+I)) = \bar{f}(ab+I) = \bar{f}\circ\pi(ab) = f(ab) = f(a)f(b) = \bar{f}\circ\pi(a)\bar{f}\circ\pi(b) = \bar{f}(a+I)\bar{f}(b+I)$ para todos os $a, b \in A$, $\bar{f}$ é de facto um homomorfismo de anéis. Por 1.6.13, $\bar{f}$ é injetivo se e só se $I = \mathrm{Ker}(f)$. □

Corolário 2.2.16. *(Teorema do homomorfismo) Seja $f\colon A \to A'$ um homomorfismo de anéis. Então um isomorfismo de anéis $A/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ é dado por $x+\mathrm{Ker}(f) \mapsto f(x)$.*

Teorema 2.2.17. *Sejam A um anel, $B \subseteq A$ um subanel e $I \subseteq A$ um ideal. Então $B+I$ é um subanel de A, I é um ideal de $B+I$, $B \cap I$ é um ideal de B e um isomorfismo de anéis $B/(B\cap I) \to (B+I)/I$ é dado por $x + B\cap I \mapsto x+I$.*

Demonstração: $B+I$ é um subgrupo do grupo aditivo de A que contém o elemento 1. Sejam $b, b' \in B$ e $x, x' \in I$. Então $(b+x)(b'+x') = bb' + bx' + xb' + xx' \in B+I$. Logo $B+I$ é um subanel de A. Como I é um ideal de A e $I \subseteq B+I$, I é um ideal de $B+I$. $B\cap I$ é um subgrupo de B e para $b \in B$ e $x \in B\cap I$, $bx \in B\cap I$ e $xb \in B\cap I$. Logo $B\cap I$ é um ideal de B. Por 1.6.17, um isomorfismo de grupos $f\colon B/(B\cap I) \to (B+I)/I$ é dado por $f(x+B\cap I) = x+I$. Como $f(1+B\cap I) = 1+I$ e $f((x+B\cap I)(y+B\cap I)) = f(xy+B\cap I) = xy+I = (x+I)(y+I) = f(x+B\cap I)f(y+B\cap I)$ para todos os $x, y \in B$, f é de facto um isomorfismo de anéis. □

Teorema 2.2.18. *Sejam A um anel e I e J ideais de A tais que $J \subseteq I$. Então I/J é um ideal de A/J e um isomorfismo de anéis $(A/J)/(I/J) \to A/I$ é dado por $x+J+I/J \mapsto x+I$.*

Demonstração: Por 1.6.18, I/J é um subgrupo do grupo aditivo de A/J. Para $a \in A$ e $x \in I$, $(a+J)(x+J) = ax+J \in I/J$ e $(x+J)(a+J) = xa+J \in I/J$. Logo I/J é um ideal de A/J. Por 1.6.18, um isomorfismo de grupos $f\colon (A/J)/(I/J) \to A/I$ é dado por $f(x+J+I/J) = x+I$. Como $f(1+J+I/J) = 1+I$ e $f((x+J+I/J)(y+J+I/J)) = f((x+J)(y+J)+I/J) = f(xy+J+I/J) = xy+I = (x+I)(y+I) = f(x+J+I/J)f(y+J+I/J)$ para todos os $x, y \in A$, f é de facto um isomorfismo de anéis. □