subanéis

Definição. Uma parte A' de um anel (respetivamente, domínio de integridade, anel de divisão, corpo) A diz-se um *subanel (respetivamente, subdomínio de integridade, subanel de divisão, subcorpo) de* A se for um anel (respetivamente, domínio de integridade, anel de divisão, corpo) relativamente às restrições das operações de adição e produto do anel.

Exemplo 23. Quando consideradas as operações usuais de adição e multiplicação, o anel $\mathbb{Z}$ é subanel e subdomínio de integridade de $\mathbb{R}$, mas não é seu subanel de divisão, nem subcorpo.

Exemplo 24. Quando consideradas as operações usuais de adição e multiplicação, o anel $n\mathbb{Z}$ ($n \in \mathbb{N}\setminus\{1\}$) é subanel mas não é subdomínio de integridade de $\mathbb{Z}$.

Exemplo 25. Dado um anel A, $\{0_A\}$ e A são subanéis de A. No entanto, dado um anel de divisão ou corpo A, $\{0_A\}$ não é subanel de divisão nem subcorpo de A.

critérios de subanel

Proposição. Sejam A um anel e $A' \subseteq A$. Então, A' é subanel de A se e só se:

1. $A' \neq \emptyset$;
2. $x, y \in A' \Rightarrow x - y \in A'$;
3. $x, y \in A' \Rightarrow xy \in A'$ $\square$

Proposição. Sejam A um domínio de integridade e $A' \subseteq A$. Então, A' é subdomínio de integridade de A se e só se:

1. $1_A \in A'$;
2. $x, y \in A' \Rightarrow x - y \in A'$;
3. $x, y \in A' \Rightarrow xy \in A'$ $\square$

Proposição. Sejam A um anel de divisão (respetivamente, corpo) e $A' \subseteq A$. Então, A' é subanel de divisão (respetivamente, subcorpo) de A se e só se:

1. $A' \neq \emptyset$;
2. $x, y \in A' \Rightarrow x - y \in A'$;
3. $x, y \in A' \setminus \{0_A\} \Rightarrow xy^{-1} \in A' \setminus \{0_A\}$. $\square$

INTERSECÇÃO: Sejam A um anel e A_1 e A_2 subanéis de A. Então, $A_1 \cap A_2$ é subanel de A.

UNIÃO: Sejam A um anel e A_1 e A_2 subanéis de A. A união $A_1 \cup A_2$ não é necessariamente um subanel de A.

SOMA: Sejam A um anel e A_1 e A_2 subanéis de A. Como $(A_1, +)$ e $(A_2, +)$ são subgrupos do grupo comutativo $(A, +)$, sabemos que o subconjunto

$$A_1 + A_2 = \{a_1 + a_2 : a_1 \in A_1,\ a_2 \in A_2\}$$

de A é subgrupo de $(A, +)$ (Relembrar que se G é grupo e $H, K < G$ então $HK < G$ se e só se $HK = KH$; em linguagem aditiva, escrevemos $H + K < G$ se e só se $H + K = K + H$). No entanto, dados $a_1 + a_2, b_1 + b_2 \in A_1 + A_2$,

$$(a_1 + a_2)(b_1 + b_2) = a_1 b_1 + a_2 b_1 + a_1 b_2 + a_2 b_2$$

não é necessariamente um elemento de $A_1 + A_2$, pelo que $A_1 + A_2$ não é necessariamente um subanel de A.

ideais e relações de congruência num anel

Definição. Seja A um anel. Uma parte I de A diz-se um *ideal direito* (respetivamente, *ideal esquerdo*) de A se:

1. $(I, +) < (A, +)$;
2. $(\forall a \in A)\,(\forall x \in I) \quad xa \in I$ (respetivamente, $ax \in I$)

Se I for simultaneamente ideal esquerdo e ideal direito, então, I diz-se um *ideal de A*.

Exemplo 26. Consideremos o anel $(\mathbb{Z}, +, \times)$. O conjunto $2\mathbb{Z}$ é um seu ideal pois $(2\mathbb{Z}, +) < (\mathbb{Z}, +)$ e o produto de um inteiro qualquer por um inteiro par é um inteiro par.

Exemplo 27. Relativamente ao anel $(\mathbb{Z}_4,+,\cdot)$, o conjunto $\{\bar{0},\bar{2}\}$ é um ideal pois

$$(\{\bar{0},\bar{2}\},+) < (\mathbb{Z}_4,+)$$

e

$$\begin{array}{l} \bar{0}\cdot\bar{0}=\bar{0}\cdot\bar{1}=\bar{0}\cdot\bar{2}=\bar{0}\cdot\bar{3}=\bar{0}\in\{\bar{0},\bar{2}\} \\ \bar{2}\cdot\bar{0}=\bar{2}\cdot\bar{2}=\bar{0}\in\{\bar{0},\bar{2}\} \quad e \quad \bar{2}\cdot\bar{1}=\bar{2}\cdot\bar{3}=\bar{2}\in\{\bar{0},\bar{2}\}. \end{array}$$

Como o anel em questão é comutativo, concluímos que $\{\bar{0},\bar{2}\}$ é um ideal de $\mathbb{Z}_4$.

Exemplo 28. Seja A um anel. Então, $\{0_A\}$ é um ideal de A (ao qual se chama *ideal trivial de A*).

Exemplo 29. Um anel A é um ideal de si próprio (ao qual se chama *ideal impróprio de A*).

Proposição. Todo o ideal de um anel A é um subanel de A. $\square$

Proposição. A intersecção de uma família de ideais de um anel A é um ideal de A. $\square$

Proposição. Num anel com identidade todo o ideal que contém essa identidade é impróprio.

Demonstração. Sejam A um anel com identidade 1_A e I um ideal de A tal que $1_A \in I$. Então,

$$\forall a \in A, \qquad a = a \cdot 1_A \in I.$$

Logo, $A \subseteq I$. Como, por definição, $I \subseteq A$, temos o resultado pretendido, i.e., $I = A$. $\square$

Proposição. Num anel de divisão existem apenas dois ideais: o trivial e o impróprio.

Exemplo 30. Os únicos ideias do corpo $\mathbb{R}$ são $\{0\}$ e o próprio $\mathbb{R}$.

O facto de $2\mathbb{Z}$ ser ideal de $\mathbb{Z}$ permite-nos concluir que $\mathbb{Z}$ não é corpo.

Podemos ter ideais de um anel A que sejam gerados por um elemento de a.

Definição. Sejam A um anel e $a \in A$. Chama-se *ideal principal direito* (respetivamente, *ideal principal esquerdo, ideal principal*) *gerado por a*, e representa-se por $(a)_d$ (respetivamente $(a)_e$, (a)) ao menor ideal direito (respetivamente, ideal esquerdo, ideal) que contém a.

Exemplo 31. Consideremos o anel $\mathbb{Z}_4$ com as operações usuais de adição e multiplicação de classes. Como a multiplicação é comutativa, todos os ideais esquerdos são direitos e viceversa, pelo que podemos falar simplesmente em ideais. Os ideais de $\mathbb{Z}_4$ são $\{\bar{0}\}$, $\{\bar{0}, \bar{2}\}$ e $\mathbb{Z}_4$. Assim, temos que

$$(\bar{0}) = \{\bar{0}\}, \quad (\bar{2}) = \{\bar{0}, \bar{2}\}, \quad (\bar{1}) = (\bar{3}) = \mathbb{Z}_4.$$

Proposição. Sejam A um anel e $a \in A$. Então,

1. $(a)_d$ é a intersecção de todos os ideais direitos de A que contêm a.
2. $(a)_e$ é a intersecção de todos os ideais esquerdos de A que contêm a.
3. (a) é a intersecção de todos os ideais de A que contêm a.

$\square$

Exemplo 32. No corpo $\mathbb{R}$, $(0) = \{0\}$ e $(x) = \mathbb{R}$, para todo $x \neq 0$.

Exemplo 33. No domínio de integridade $\mathbb{Z}$, $(-n) = (n) = n\mathbb{Z}$, para todo $n \in \mathbb{N}_0$.

Proposição. Sejam A um anel com identidade e $a \in A$. Então, $(a)_d = aA$ e $(a)_e = Aa$.

Corolário. Sejam A um anel comutativo com identidade e $a \in A$. Então, $(a) = Aa = aA$. $\square$

Definição. Seja A um anel. Uma relação de equivalência ρ definida em A diz-se uma *relação de congruência* se, para todos $x, x', y, y' \in A$,

$$x \,\rho\, x' \quad \text{e} \quad y \,\rho\, y' \Rightarrow (x+y) \;\rho\; \left(x'+y'\right) \quad \text{e} \quad (xy) \;\rho\; \left(x'y'\right).$$

Exemplo 34. Considere-se em $\mathbb{Z}$ a relação

$$a \,\rho\, b \Leftrightarrow a - b \in 2\mathbb{Z}.$$

Esta relação é de equivalência e é tal que

$$\begin{aligned}
a \,\rho\, b \quad \text{e} \quad a' \,\rho\, b' \quad &\Leftrightarrow \quad a - b, a' - b' \in 2\mathbb{Z} \\
&\Rightarrow \quad a + a' - \left(b + b'\right) \in 2\mathbb{Z} \quad \text{e} \\
& \quad aa' - bb' = aa' - ba' + ba' - bb' = (a-b)\,a' + b\left(a' - b'\right) \in 2\mathbb{Z} \\
&\Leftrightarrow \quad \left(a + a'\right) \;\rho\; \left(b + b'\right) \quad \text{e} \quad aa' \,\rho\, bb',
\end{aligned}$$

pelo que ρ é uma relação de congruência em $\mathbb{Z}$.

Proposição. Sejam A um anel e I um ideal de A. Então, a relação definida em A por

$$a \,\rho\, b \Leftrightarrow a - b \in I$$

é uma relação de congruência.

Proposição. Seja ρ uma relação de congruência definida num anel A. Então:

1. a classe $[0_A]_\rho$ é um ideal de A;
2. $a \,\rho\, b \Leftrightarrow a - b \in [0_A]_\rho$;
3. $(\forall a \in A) \quad [a]_\rho = a + [0_A]_\rho \,(= \{a + x \in A \mid x \,\rho\, 0_A\})$.

anéis quociente

Se ρ é uma relação de congruência num anel A (e, portanto, de equivalência), podemos então falar no conjunto quociente

$$A/\rho = \left\{ [a]_\rho \mid a \in A \right\}.$$

Neste conjunto, definem-se duas operações binárias:

1. uma adição de classes: para $a, b \in A$,

$$[a]_\rho + [b]_\rho = [a+b]_\rho\,;$$

2. uma multiplicação de classes: para $a, b \in A$,

$$[a]_\rho \cdot [b]_\rho = [a \cdot b]_\rho\,.$$

Sendo ρ uma relação de congruência, prova-se que as operações estão bem definidas, i.e., não dependem da escolha do representante da classe:

Se $[a]_\rho = [a']_\rho$ e $[b]_\rho = [b']_\rho$, temos que

$$a \,\rho\, a' \text{ e } b \,\rho\, b',$$

pelo que

$$(a+b)\,\rho\,\left(a'+b'\right) \quad \text{e} \quad (ab)\,\rho\,\left(a'b'\right)$$

e, portanto,

$$[a+b]_\rho = \left[a'+b'\right]_\rho \quad \text{e} \quad [ab]_\rho = \left[a'b'\right]_\rho .$$

Teorema. Sejam A um anel e ρ uma relação de congruência definida em A. Então, considerando a adição e a multiplicação acima definidas, $(A/\rho, +, \cdot)$ é um anel. $\square$

Observação. Sabemos que existe uma relação biunívoca entre o conjunto das relações de congruência em A e o conjunto dos ideais de A. Assim, se I é ideal de A, podemos também falar num anel quociente:

Definição. Sejam A um anel e I é ideal de A. Chama-se *anel quociente módulo* I ao anel $(A/I, +, \cdot)$, onde

- $A/I = \{x + I : x \in A\}$ e
$$y \in x + I \Leftrightarrow y - x \in I.$$
- para todos $x, y \in A$,
$$(x + I) + (y + I) = (x + y) + I$$
e
$$(x + I)(y + I) = xy + I.$$

Proposição. Sejam A um anel e I um ideal de A.

1. Se A é uma anel comutativo, então A/I é um anel comutativo;
2. Se A é um anel com identidade 1_A, então A/I é um anel com identidade $1_A + I$. $\square$

Exemplo 32. Considerando o anel dos inteiros relativos, sabemos que, para cada $n \in \mathbb{N}$, $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$. Podemos então considerar o anel quociente $\mathbb{Z}/n\mathbb{Z}$. Mais ainda, para cada $x \in \mathbb{Z}$,

$$[x]_{n\mathbb{Z}} = x + n\mathbb{Z} = r + n\mathbb{Z} = [r]_n,$$

onde r é o resto da divisão inteira de x por n e, por isso, é tal que $0 \leq r \leq n - 1$.

Logo,

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

Definição. Seja A um anel comutativo com identidade. Um ideal I de A diz-se *maximal* se não existir um ideal K de A tal que

$$I \underset{\neq}{\subseteq} K \underset{\neq}{\subseteq} A.$$

Exemplo 33. O ideal $2\mathbb{Z}$ do anel $\mathbb{Z}$ é maximal. O ideal $4\mathbb{Z}$ não é maximal pois

$$4\mathbb{Z} \underset{\neq}{\subseteq} 2\mathbb{Z} \underset{\neq}{\subseteq} \mathbb{Z}.$$

Definição. Seja A um anel comutativo com identidade. Um ideal I de A diz-se *primo* se $A \backslash I \neq \emptyset$ e $A \backslash I$ é fechado para o produto.

Exemplo 34. O ideal $2\mathbb{Z}$ do anel $\mathbb{Z}$ é primo. De facto, $\mathbb{Z} \backslash 2\mathbb{Z} = 2\mathbb{Z} + 1$ é fechado para o produto, já que, para todos $n, m \in \mathbb{Z}$,

$$(2n+1)(2m+1) = 2(n+m+2nm)+1.$$

Teorema. Sejam A um anel comutativo com identidade e I um ideal de A. Então, são equivalentes as seguintes afirmações:

1. I é maximal;
2. A/I é corpo.

Exemplo 35. Se considerarmos o anel $\mathbb{Z}$, um ideal é maximal se e só se é do tipo $p\mathbb{Z}$, com p primo, pois $\mathbb{Z}_p$ só é corpo se p for primo.

Teorema. Sejam A um anel comutativo com identidade e I um ideal de A. Então, são equivalentes as seguintes afirmações:

1. I é ideal primo;
2. A/I é um domínio de integridade.

Como consequência dos dois últimos teoremas, temos que

Corolário. Qualquer anel maximal de um anel comutativo com identidade é ideal primo.