53. Prove que, num anel não nulo com identidade, uma unidade não é divisor de zero. (1)

Provemos a implicação usando a redução ao absurdo:
Suponhamos que existe $a \in A$ t.q. $\underline{a}$ é unidade e $\underline{a}$ é divisor de zero, i.e., suponhamos que existe $a^{-1} \in A$ e existe $b \in A \setminus \{0_A\}$ t.q. $ab = 0_A$ ou $ba = 0_A$.

Mas, $ab = 0_A$ ou $ba = 0_A$ $\Rightarrow a^{-1}(ab) = a^{-1}0_A$ ou $(ba)a^{-1} = 0_A a^{-1}$

$\Leftrightarrow (a^{-1}a)b = 0_A$ ou $b(aa^{-1}) = 0_A$

$\Rightarrow b = 0_A$,

o que é uma contradição com o facto de $b \in A \setminus \{0_A\}$.
Logo, $\underline{a}$ não pode ser simultaneamente unidade e divisor de zero.

Assim, se $\underline{a}$ é unidade então $\underline{a}$ não é divisor de zero.

54. Sejam A um anel de característica zero e $a \in A \setminus \{0_A\}$ um elemento de ordem finita. Prove que $\underline{a}$ é um divisor de zero.

Recordar:

De $c(A) = 0$, concluímos que
$$kx = 0_A, \ \forall x \in A \Rightarrow k = 0$$
De $o(a) = n$, concluímos que
$$ka = 0_A \Rightarrow n \mid k$$

Seja $n \in \mathbb{N}$ t.q. $o(a) = n$. Como $n \in \mathbb{N}$ e $c(A) = 0$, temos que
$$\exists b \in A \setminus \{0_A\} : nb \neq 0_A$$
Além disso, como $o(a) = n$, temos que
$$a(nb) = n(ab) = (na)b = 0_A b = 0_A.$$

Logo, $y = xb \neq 0_A$ é t.q. $ay = 0_A$.
Assim sendo, estamos em condição de concluir que $\underline{a}$ é divisor de zero.

[55.] Prove que, num anel com identidade, um elemento idempotente não nulo e diferente da identidade é um divisor de zero. Conclua que o único idempotente não nulo num domínio de integridade é a sua identidade.

Seja $e \neq 0_A$ e $e \neq 1_A$ t.q. $ee = e$. Queremos provar que $\underline{e}$ é divisor de zero.

Sabemos que
$$ee = e \Leftrightarrow ee = e1_A$$
$$\Leftrightarrow ee - e1_A = 0_A$$
$$\Leftrightarrow e(e - 1_A) = 0_A$$

Como $e \neq 1_A$, temos que $e - 1_A \neq 0_A$.
Logo, $\underline{e}$ é divisor de zero.

- Como, num D.I., o único divisor de zero é 0_A, concluímos que se existe um idempotente não nulo no anel, ele tem de ser 1_A. Caso contrário, pelo que acabámos de provar, esse idempotente seria um divisor de zero não nulo no D.I. A, que é um elemento que não existe num D.I..

[56] Prove que um domínio de integridade finito é um corpo.

Se D é D.I, então $(D\setminus\{0_D\}, \cdot)$ é um semigrupo comutativo com identidade. (3)

Mais ainda, para $x, y, z \in D\setminus\{0_D\}$, temos que

$$xy = xz \Leftrightarrow xy - xz = 0_D \Leftrightarrow x(y-z) = 0_D$$

Como $x \neq 0_D$ não é divisor de zero, temos que se $xy = xz$ então $y - z = 0_D$, ou seja, $y = z$.

Logo, x é simplificável (provámos que é simplificável à esquerda, mas o semigrupo é comutativo)

Logo, $(D\setminus\{0_D\}, \cdot)$ é um semigrupo finito comutativo onde é válida a lei do corte, pelo que é um grupo comutativo. Assim sendo, podemos concluir que $(D, +, \cdot)$ é corpo.

[57] Um elemento $\underline{a}$ de um anel A diz-se nilpotente se $a^n = 0_A$ para algum natural n. Mostre que 0_A é o único elemento nilpotente num domínio de integridade A.

Sabendo que, para $a \in A$, existe $n \in \mathbb{N}$ t.q. $a^n = 0_A$, consideremos $n' = \min\{n \in \mathbb{N} : a^n = 0_A\}$ (o mínimo deste subconjunto de $\mathbb{N}$ existe pelo Princípio da Boa Ordenação de $\mathbb{N}$: todo o subconjunto não vazio de $\mathbb{N}$ admite elemento mínimo).

- Se $n' = 1$, então, obtemos de imediato que
$$a = a^1 = 0_A$$
- Se $n' > 1$, então, $n-1 \in \mathbb{N}$ e

$$0_A = a^{n'} = a \cdot a^{n'-1} \quad (*)$$

Como $n'-1 < n'$, temos que $a^{n'-1} \neq 0_A$ e, por $(*)$ $\underline{\underline{a}}$ é divisor de zero.

Como 0_A é o único divisor de zero num D.I., concluímos que $a = 0_A$

$\boxed{58}$ Justifique que $\mathbb{Z}_3$ não é subanel de $\mathbb{Z}_9$.

O anel $\mathbb{Z}_3$ não é subanel do anel $\mathbb{Z}_9$ porque $\mathbb{Z}_3 \not\subseteq \mathbb{Z}_9$

$\boxed{59}$ Prove que o centro $Z(A)$ de um anel A, definido por $Z(A) = \{x \in A : \forall y \in A,\ xy = yx\}$ é um subanel de A.

Recordar: Sejam A um anel e $B \subseteq A$. Então, B é subanel de A sse:

$\rightarrow B \neq \emptyset$

$\rightarrow x, y \in B \Rightarrow x - y \in B$

$\rightarrow x, y \in B \Rightarrow xy \in B$

$\rightarrow$ $0_A \in A$ e $\forall y \in A$, $0_A y = 0_A = y \cdot 0_A \Rightarrow 0_A \in Z(A)$

$\Rightarrow Z(A) \neq \emptyset$

$\rightarrow$ $a, b \in Z(A) \Leftrightarrow a, b \in A$ e $\forall y \in A$ $ay = ya$ e $by = yb$

$\Rightarrow a - b \in A$ e $\forall y \in A$ $(a-b)y = ay - by =$

$= ya - yb = y(a-b)$

$\Rightarrow a - b \in Z(A)$

$\rightarrow a,b \in Z(A) \Rightarrow a,b \in A$ e $\forall y \in A \; ay = ya$ e $by = yb$

$\Rightarrow ab \in A$ e $\forall y \in A$,

$(ab)y = a(by) = a(yb) = (ay)b = (ya)b$
$= y(ab)$

$\Rightarrow ab \in Z(A)$

Como as condições do critério de subanel são satisfeitas, concluímos que $Z(A)$ é subanel de A.

$\boxed{160}$ Sejam A um anel e $N = \{n \in \mathbb{Z} : na = 0_A, \forall a \in A\}$

(a) Mostre que N é um ideal do anel $\mathbb{Z}$

(b) Determine N, sabendo que

i. $A = \mathbb{Z}_5$

(ii) A é um anel c/ 1_A e $\theta(1_A) = \infty$

(c) Dê um exemplo de um anel A para o qual $\mathbb{Z}/N$ é corpo.

(a) $\rightarrow 0 \in \mathbb{Z}$ e $0a = 0_A, \forall a \in A \Rightarrow 0 \in N \Rightarrow N \neq \emptyset$

$\rightarrow n,m \in N \Rightarrow n,m \in \mathbb{Z}$ e $\forall a \in A \; na = 0_A$ e $ma = 0_A$

$\Rightarrow n - m \in \mathbb{Z}$ e $(n-m)a = na - ma = 0_A - 0_A$
$= 0_A$

$\Rightarrow n - m \in N$

$\rightarrow n \in N$ e $m \in \mathbb{Z} \Rightarrow n,m \in \mathbb{Z}$ e $\forall a \in A \; na = 0_A$

$\Rightarrow mn \in \mathbb{Z}$ e $\forall a \in A$,

$(mn)a = m(na) = m0_A = 0_A$

$\Rightarrow mn \in N$

Como $\mathbb{Z}$ é anel comutativo, tb concluímos que $nm \in N$

Logo, N é ideal de $\mathbb{Z}$

(b) Num anel A, associamos a condição "$na = 0_A$, $\forall a \in A$" ao conceito de característica do anel. Sabemos que:

1) Se $c(A)=0$ então $(na = 0_A, \forall a \in A) \Rightarrow n=0$
2) Se $c(A)=k \in \mathbb{N}$ então $(na = 0_A, \forall a \in A) \Rightarrow k \mid n$

Assim,

i) $A = \mathbb{Z}_5 \rightarrow c(A) = 5 \Rightarrow N = 5\mathbb{Z}$
ii) A é anel com 1_A e $o(1_A) = \infty \Rightarrow c(A) = 0$
$\Rightarrow N = \{0\}$

(c) $\mathbb{Z}/N$ é corpo sse N é um ideal maximal de $\mathbb{Z}$, ou seja, sse $N = p\mathbb{Z}$ com p primo. Pelo que vimos em (b), para $N = p\mathbb{Z}$ ser ideal de $\mathbb{Z}$, basta que A seja um anel de característica p. Assim, podemos considerar como exemplo $A = \mathbb{Z}_p$, com p primo.

16] Mostre que um subanel de um anel A não é necessariamente um ideal de A.

O anel dos inteiros $\mathbb{Z}$ é um subanel do anel dos reais $\mathbb{R}$. No entanto, $\mathbb{Z}$ não é ideal de $\mathbb{R}$ pois, por exemplo,

$2 \in \mathbb{Z}$, $\pi \in \mathbb{R}$ e $2 \times \pi \notin \mathbb{Z}$ e
$\pi \times 2 \notin \mathbb{Z}$.

62) Seja A um anel comutativo com identidade e $a \in A \setminus \{0_A\}$. Prove que $R_a = \{x \in A : xa = 0_A\}$ é um ideal próprio de A.

- $0_A \in A$ e $0_A a = 0_A \Rightarrow 0_A \in R_a$
- $x, y \in R_a \Rightarrow x, y \in A$ e $xa = 0_A$ e $ya = 0_A$

$\Rightarrow x - y \in A$ e $(x-y)a = xa - ya = 0_A - 0_A = 0_A$

$\Rightarrow x - y \in R_a$

- $x \in R_a, y \in A \Rightarrow x, y \in A$ e $xa = 0_A$

$\Rightarrow xy \in A$ e $(xy)a = (yx)a = y(xa)$

$= y\, 0_A = 0_A$

$\Rightarrow (yx)\, xy \in R_a$

Logo, R_a é ideal de A.

Para provar que R_a é próprio, i.e., que $R_a \subsetneq A$ basta provar que $1_A \notin R_a$. De facto,

$1_A \in R_a \Rightarrow 1_A \cdot a = 0_A \Leftrightarrow a = 0_A$

(o que contradiz o facto de $a \in A \setminus \{0_A\}$)

63) Sejam X e Y dois subconjuntos de um anel A. Defina soma de X com Y, $X+Y$, e produto de X por Y, XY, por

$$X+Y = \{x+y \in A : x \in X \text{ e } y \in Y\}$$

e $$XY = \left\{ \sum_{i=1}^{n} x_i y_i \in A : n \in \mathbb{N}, x_i \in X, y_i \in Y, i = 1, \dots, n \right\}$$

(a) Mostre que a soma de 2 subanéis de A não é necessariamente um subanel de A.

(b) Mostre que o produto de 2 subanéis B e C de A é subanel de A se $BC = CB$.

(a) Se considerarmos apenas a adição, que sabemos ser comutativa, temos que

$$(B,+),(C,+) < (A,+) \Rightarrow (B+C,+) < (A,+)$$

O problema coloca-se no produto de elementos:

Se $b_1+c_1, b_2+c_2 \in B+C$, temos que

$$(b_1+c_1)(b_2+c_2) = \underbrace{b_1b_2}_{\in B} + \underbrace{c_1b_2+b_1c_2}_{\downarrow} + \underbrace{c_1c_2}_{\in C}$$

não sabemos a que subconjunto de A pertence.

Exemplo:

Considere-se

$$A = \mathcal{M}_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R} \right\},$$

$$B = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a,b \in \mathbb{R} \right\} \text{ e } C = \left\{ \begin{bmatrix} a & 0 \\ b & a \end{bmatrix} : a,b \in \mathbb{R} \right\}$$

$\underline{\underline{A}}$ é anel para a adição e multiplicação de matrizes quadradas e B e C são subanéis de A. De facto, B é subanel de A porque:

$\rightarrow \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in B$ e por isso $B \neq \emptyset$

$\rightarrow \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} - \begin{bmatrix} x & y \\ 0 & x \end{bmatrix} = \begin{bmatrix} a-x & b-y \\ 0 & a-x \end{bmatrix} \in B$

$\rightarrow \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\begin{bmatrix} x & y \\ 0 & x \end{bmatrix} = \begin{bmatrix} ax & ay+bx \\ 0 & ax \end{bmatrix} \in B$

De igual modo, provamos que C é subanel de A.

Considerando agora B+C, obtemos

$$B+C = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} + \begin{bmatrix} a' & 0 \\ b' & a' \end{bmatrix} : a,b,a',b' \in \mathbb{R} \right\}$$

$$= \left\{ \begin{bmatrix} a+a' & b \\ b' & a+a' \end{bmatrix} : a,b,a',b' \in \mathbb{R} \right\}$$

$$= \left\{ \begin{bmatrix} x & y \\ z & x \end{bmatrix} : x,y,z \in \mathbb{R} \right\}$$

$B+C$ não é subanel de A pois, por exemplo,

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \in B+C \quad \text{e}$$

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 7 \\ 3 & 5 \end{bmatrix} \notin B+C$$

pois $4 \neq 5$.

(b)

Observemos primeiro que BC é o conjunto de somas finitas de produtos de eltos de B por eltos de C.

$\rightarrow$ Como $0_A \in B$, $0_A \in C$ e $0_A = 0_A \cdot 0_A$ podemos ver 0_A como a soma de uma única parcela que é o produto de 1 elemento de B (0_A) por um elemento de C (0_A). Logo, $0_A \in BC$ e por isso, $BC \neq \emptyset$

$\rightarrow$ $x, y \in BC \Rightarrow x = \sum_{i=1}^{n} b_i c_i$ e $y = \sum_{j=1}^{m} b'_j c'_j$

onde $b_i, b'_j \in B$, $c_i, c'_j \in C$, para todos $i = 1, \dots, n$ e $j = 1, \dots, m$ $(n, m \in \mathbb{N})$

$$\Rightarrow x - y = \sum_{i=1}^{n} b_i c_i - \sum_{j=1}^{m} b'_j c'_j$$

$$= \sum_{i=1}^{n} b_i c_i + \sum_{j=1}^{m} (-b'_j) c'_j$$

$$= \sum_{i=1}^{n} b_i c_i + \sum_{j=1+n}^{m+n} (-b'_{j-n})(c'_{j-n})$$

$$= \sum_{k=1}^{n+m} b''_k c'_k \quad \text{onde}$$

$$b''_k = \begin{cases} b_k & \text{se } 1 \leq k \leq n \\ -b'_{k-n} & \text{se } n+1 \leq k \leq n+m \end{cases} \quad \text{e}$$

e $c''_k = \begin{cases} c_k & \text{se } 1 \leq k \leq n \\ c'_{k-n} & \text{se } n+1 \leq k \leq m+n \end{cases}$

$\Rightarrow x - y \in BC$

$\longrightarrow x, y \in BC \Rightarrow x = \sum_{i=1}^{n} b_i c_i$ e $y = \sum_{j=1}^{m} b'_j c'_j$

em $n, m \in \mathbb{N}$, $b_i, b'_j \in B$, $c_i, c'_j \in C$

para todos $i = 1, \dots, n$ e $j = 1, \dots, m$

$$\Rightarrow xy = \left(\sum_{i=1}^{n} b_i c_i\right)\left(\sum_{j=1}^{m} b'_j c'_j\right)$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{m} b_i \underbrace{c_i b'_j} c'_j$$

$$\overset{\otimes}{=} \sum_{i=1}^{n} \sum_{j=1}^{m} b_i \left(\sum_{k=1}^{s_{ij}} b_k^{(ij)} c_k^{(ij)}\right) c'_j$$

$$= \underbrace{\sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{k=1}^{s_{ij}}}_{\text{soma finita}} \underbrace{b_i b_k^{(ij)}}_{\in B} \underbrace{c_k^{(ij)} c'_j}_{\in C}$$

$\Rightarrow xy \in BC$

$\otimes$

$c_i b'_j \in CB = BC$

$\Rightarrow c_i b'_j = \sum_{k=1}^{s_{ij}} b_k^{(ij)} c_k^{(ij)}$) o nº de parcelas depende de c_i, b'_j, assim como os elementos de B e C que vão definir as parcelas, ou seja, vão depender de i e de j.

64. Sejam A um anel, B um subanel e I e J ideais de A. Prove que: (11)

(a) $B+I$ é um subanel de A

(b) $I+J$ é um ideal de A

(c) IJ é um ideal de A t.q. $IJ \subseteq I+J$

(a) $B+I$ subanel de A pois:

→ Como $+$ é comutativa e $(B,+)$ e $(I,+)$ são subgrupos de $(A,+)$, temos que

$$(B+I, +) < (A,+),$$

o que prova as duas primeiras condições do critério de subanel. Falta provar que

$$x, y \in B+I \Longrightarrow xy \in B+I.$$

Temos:

$x, y \in B+I \Rightarrow x = b_1 + i_1$ e $y = b_2 + i_2$ com $b_1, b_2 \in B$ e $i_1, i_2 \in I$

$$\Rightarrow xy = (b_1+i_1)(b_2+i_2) = \underbrace{b_1 b_2}_{\in B} + \underbrace{\underbrace{i_1}_{\in I} b_2}_{\in I} + \underbrace{b_1 \underbrace{i_2}_{\in I}}_{\in I} + \underbrace{i_1 i_2}_{\in I}$$

porque I é ideal de A

$$\Rightarrow xy \in B+I$$

(b) $I+J$ é ideal de A pois

→ $(I,+)$ e $(J,+)$ são subgrupos de $(A,+)$ e $+$ é comutativa, temos que

$$(I+J, +) < (A,+)$$

→ Falta provar que

$$x \in I+J \text{ e } a \in A \Rightarrow xa,\ ax \in I+J$$

$$x \in I+J \text{ e } a \in A \Rightarrow x = i+j,\ i \in I,\ j \in J \text{ e } a \in A$$

$$\Rightarrow ax = a(i+j) = \underbrace{ai}_{\in I} + \underbrace{aj}_{\in J} \in I+J$$

e

$$xa = (i+j)a = ia + ja \in I+J$$

$$\Rightarrow xa,\ ax \in I+J$$

$\boxed{\text{Obs}}$ $I+J$ é, na realidade, o <u>menor</u> <u>ideal</u> de A que <u>contém</u> simultaneamente I e J:

→ $i \in I \Rightarrow i = i + 0_A \in I+J$

$j \in J \Rightarrow j = 0_A + j \in I+J$

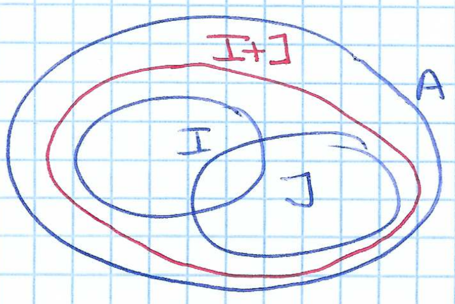
Logo $I \subseteq I+J$ e $J \subseteq I+J$

→ Seja K um ideal t.q. $I \subseteq K$ e $J \subseteq K$

Então

$$x = i+j \in I+J \Rightarrow x = \underbrace{i}_{\in K} + \underbrace{j}_{\in K} \in K$$

Logo, $I+J \subseteq K$



(c) • IJ é um ideal de A pois

→ $(IJ,+) < (A,+)$ pois, sendo ideais de A, I e J são também subanéis de A e, assim, podemos fazer o mesmo raciocínio que fizemos na primeira parte de 63b)

→ Falta provar que se $x \in IJ$ e $a \in A$, temos que $xa, ax \in IJ$.

$$x \in IJ \text{ e } a \in A \Rightarrow x = \sum_{k=1}^{n} i_k j_k \text{ e } a \in A,$$

com $i_k \in I$, $j_k \in J$, $\forall k = 1, \dots, n$

$$\Rightarrow ax = a \sum_{k=1}^{n} i_k j_k = \sum_{k=1}^{n} \underbrace{\underbrace{(a i_k)}_{\in I} j_k}_{\in I} \in IJ$$

e

$$xa = \left(\sum_{k=1}^{n} i_k j_k \right) a = \sum_{k=1}^{n} i_k \underbrace{\underbrace{(j_k a)}_{\in J}}_{\in J} \in IJ$$

• Para concluir que $IJ \subseteq I+J$, basta observar que

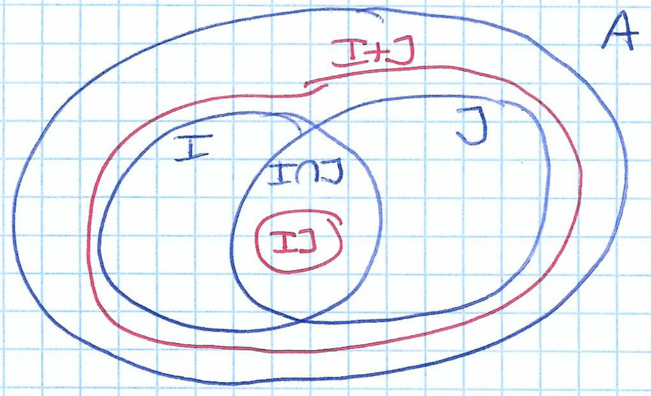
$$x \in IJ \Rightarrow x = \sum_{k=1}^{n} \underbrace{\underbrace{i_k}_{\in I} j_k}_{\in I} \qquad i_k \in I, j_k \in J \quad k = 1, \dots, n$$

$$\Rightarrow x \in I$$

(e, de modo análogo, temos que $x \in IJ \Rightarrow x \in J$)

Como $I \subseteq I+J$, concluímos que $IJ \subseteq I+J$

<u>Obs</u>: Acabámos de provar que $IJ \subseteq I$ e $IJ \subseteq J$, pelo que podemos concluir que $IJ \subseteq I \cap J$, que tb é um ideal de A. Podemos então completar o diagrama da página 12:



Obs: O ideal $I+J$ pode ser ou não o anel A. No exercício seguinte prova-se que quando isto acontece num anel comutativo com 1_A, os ideais IJ e $I\cap J$ tb coincidem

$\boxed{65}$ Seja A um anel comutativo com 1_A. Mostre que se I e I' são ideais de A t.q. $A=I+I'$ então $II'=I\cap I'$

Sabemos já que $II'\subseteq I\cap I'$. Falta provar que $I\cap I'\subseteq II'$. Temos:

$$x\in I\cap I' \Rightarrow x\in I \text{ e } x\in I'$$

$$\Rightarrow x = x1_A = x(i+i')$$

$1_A\in A=I+I'$

com $x,i\in I$ e $x,i'\in I'$

$$\Rightarrow x = xi + xi'$$

$$= \underbrace{\underbrace{i}_{\in I}\underbrace{x}_{\in I'} + \underbrace{x}_{\in I}\underbrace{i'}_{\in I'}}$$

soma de 2 parcelas de produtos de el.tos de I por elementos de I'

$$\Rightarrow x\in II'$$

66 Sejam A um anel e I um ideal de A.
Prove que:

(a) os subanéis do anel quociente A/I são todos os anéis quociente B/I, em que B é um subanel de A que contém I

(b) Os ideais do anel quociente A/I são todos os anéis quociente J/I, em que J é um ideal de A que contém I.

a) Se B é subanel de A e $I \subseteq B$, então B é um anel e I é ideal de B. Logo, B/I é um anel. Claramente, de $B \subseteq A$ temos que $B/I \subseteq A/I$.
Logo, B/I é subanel de A/I.

Reciprocamente, suponhamos que X é um subanel de A/I. Então,

$$X = B/I \quad \text{onde} \quad B = \bigcup_{x+I \in X} (x+I)$$

Porque $I \in X$, temos que $I \subseteq B$.
Além disso, B é subanel de A pois:

i) $0_A \in I \subseteq B \Rightarrow 0_A \in B$

ii) $x, y \in B \Rightarrow x+I,\ y+I \in X$
$\Rightarrow (x-y)+I \in X$ (X subanel de A)
$\Rightarrow x-y \in B$

iii) $x, y \in B \Rightarrow x+I,\ y+I \in X$
$\Rightarrow xy+I = (x+I)(y-I) \in X$
$\Rightarrow xy \in B$

b) Se J é ideal de A e $I \subseteq J$ então J é subanel de A (e, por isso, é um anel) e I é ideal de J. Logo J/I é um anel (e, por isso, subanel de A/I). Para concluirmos que J/I é ideal de A/I falta provar então que

$$\forall_{j+I \in J/I} \; \forall_{a+I \in A/I} \quad (j+I)(a+I), (a+I)(j+I) \in J/I$$

De facto,

- $(j+I)(a+I) = \underbrace{ja}_{\in J \text{ porque } J \text{ é ideal de } A} + I \in J/I$
- $(a+I)(j+I) = \widetilde{aj} + I \in J/I$

Reciprocamente, seja Y um ideal de A/I. Então, $Y = J/I$ onde $J = \bigcup_{j+I \in Y} j+I$

Provemos que J é um ideal de A e que $I \subseteq J$:

- Como Y é ideal de A/I, $I \, (= 0_{A/I}) \in Y$ pelo que $\forall_{x \in I} \; x \in J$

  Assim, $0_A \in I \subseteq J$.

  Logo, $J \neq \emptyset$ e $I \subseteq J$.

- Dados $i, j \in J$, temos que $i+I, j+I \in Y$. Como Y é ideal de A/I, temos que

$$x+I - (y+I) \in Y$$
$$(=) \quad (x-y) + I \in Y$$
$$\Rightarrow \quad x-y \in J.$$

- Dado $x \in J$ e $a \in A$, temos que

$$x+I \in Y \quad e \quad a+I \in A/I.$$

Como Y é ideal de A/I, temos que

$$(x+I)(a+I) \in Y \quad e \quad (a+I)(x+I) \in Y$$

ou seja

$$xa + I \in Y \quad e \quad ax + I \in Y$$

Logo,

$$xa \in J \quad e \quad ax \in J.$$

Logo, J é um ideal de A t.q. $I \subseteq J$.

$\boxed{67}$ Sejam A e B anéis com identidade. Prove que o conjunto dos ideais do anel com identidade $A \times B$ é

$$\mathcal{I}(A\times B) = \{I \times J : I \text{ ideal de } A \text{ e } J \text{ ideal de } B\}$$

→ Se I é ideal de A e J é ideal de B então $I \times J$ é ideal de $A \times B$. De facto,

i) $(0_A, 0_B) \in I \times J$ pelo que $I \times J \neq \emptyset$

ii) Se $(i_1, j_1), (i_2, j_2) \in I \times J$, então, $i_1, i_2 \in I$ e $j_1, j_2 \in J$. Como I é ideal de A e J é ideal de B, temos que

$$i_1 - i_2 \in I \quad e \quad j_1 - j_2 \in J$$

Logo,

$$(i_1 - i_2, j_1 - j_2) \in I \times J$$

ou seja

$$(i_1, j_1) - (i_2, j_2) \in I \times J.$$

iii) Se $(i, j) \in I \times J$ e $(a, b) \in A \times B$, então, $i \in I$, $a \in A$ e $j \in J$ e $b \in B$

Porque I é ideal de A, temos que

$$ia,\ ai \in I$$

e como J é ideal de B, temos que

$$jb,\ bj \in J$$

Logo, $(ia, jb) \in I \times J$ e $(ai, bj) \in I \times J$

ou seja

$$(i,j)(a,b) \in I \times J \quad \text{e} \quad (a,b)(i,j) \in I \times J.$$

→ Reciprocamente, suponhamos que X é ideal de $A \times B$. Então,

$$X \subseteq A_1 \times B_1$$

onde

$$A_1 = \{ x \in A : (\exists y \in B)\ (x,y) \in X \}$$

e

$$B_1 = \{ y \in B : (\exists x \in A)\ (x,y) \in X \}$$

Temos de provar 3 coisas:

1) $X = A_1 \times B_1$

2) A_1 ideal de A

3) B_1 ideal de B

1) Falta apenas provar que $A_1 \times B_1 \subseteq X$.

Seja $(a,b) \in A_1 \times B_1$. Então $a \in A_1$ e $b \in B_1$

Então

a) $(\exists y \in B)\ (a,y) \in A_1$

b) $(\exists x \in A)\ (x,b) \in B_1$

Assim, e como $(1_A, 0_B), (0_A, 1_B) \in A \times B$,

$(1_A, 0_B)(a, y) \in X$

e $(0_A, 1_B)(x, b) \in X$ (não esquecer que X é ideal de $A \times B$)

ou seja,

$(a, 0_B) \in X$ e $(0_A, b) \in X$

Novamente aplicando o facto de X ser ideal, temos que

$$(a, b) = (a, 0_B) + (0_A, b) \in X$$

2) i) Porque X é ideal de $A \times B$, $(0_A, 0_B) \in X$ e, por isso, $0_A \in A_1$. Logo, $A_1 \neq \emptyset$

ii) Dados $a_1, a_2 \in A_1$, temos que existe $y_1, y_2 \in B_1$ t.q.

$(a_1, y_1), (a_2, y_2) \in X$

Logo,

$$(a_1 - a_2, y_1 - y_2) = (a_1, y_1) - (a_2, y_2) \in X$$

pelo que $a_1 - a_2 \in A_1$

iii) Dados $a_1 \in A_1$ e $x \in A$ temos que existe $y \in B_1$ t.q.

$(a_1, y) \in X$ e $(x, y) \in A \times B$

Logo,

$$(a_1 x, y^2) = (a_1, y)(x, y) \in X$$ e
$$(x a_1, y^2) = (x, y)(a_1, y) \in X$$

pelo que $a_1 x, x a_1 \in A_1$

Logo, por i), ii) e iii), A_1 é ideal de A

3) Igual a 2)

68. Considere o anel $\mathbb{Z}\times\mathbb{Z}$. Indique:

(a) um ideal maximal

(b) um ideal primo que não seja maximal

(c) um ideal próprio não nulo que não seja primo

Observações: • Pelo exercício anterior, sabemos que os ideais de $\mathbb{Z}\times\mathbb{Z}$ são os conjuntos

$$n\mathbb{Z}\times m\mathbb{Z} \quad \text{com} \quad n,m\in\mathbb{Z}$$

(uma vez que I é ideal de $\mathbb{Z}$ sse $I=n\mathbb{Z}$ para algum $n\in\mathbb{Z}$)

• I é um ideal maximal de $\mathbb{Z}\times\mathbb{Z}$ sse não existe K ideal de $\mathbb{Z}\times\mathbb{Z}$ t.q. $I\subsetneq K\subsetneq \mathbb{Z}\times\mathbb{Z}$

• I é um ideal primo de $\mathbb{Z}\times\mathbb{Z}$ sse $(\mathbb{Z}\times\mathbb{Z})\setminus I\neq\emptyset$ e $(\mathbb{Z}\times\mathbb{Z})\setminus I$ é fechado para o produto.

Sabemos que os ideais maximais de $\mathbb{Z}$ são

$$p\mathbb{Z} \quad \text{com } p \text{ primo}$$

e os ideais primos de $\mathbb{Z}$ são

$$\{0\} \quad \text{ou} \quad p\mathbb{Z} \text{ com } p \text{ primo.}$$

a) $I=p\mathbb{Z}\times\mathbb{Z}$ ou $I=\mathbb{Z}\times p\mathbb{Z}$ com p primo

↳ só nestas condições é que

$$\nexists\, n\mathbb{Z}\times k\mathbb{Z} \;:\; I\subsetneq n\mathbb{Z}\times k\mathbb{Z}\subsetneq\mathbb{Z}\times\mathbb{Z}$$

b) $I = \mathbb{Z} \times \{0\}$ ou $I = \{0\} \times \mathbb{Z}$

↳ justificação análoga

$\downarrow$

$\therefore$ O ideal é primo pois, dados

$(a,b), (c,d) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\} \neq \emptyset$

$(ac, bd) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$

c) $I = n\mathbb{Z} \times m\mathbb{Z}$ com $n, m \in \mathbb{N} \setminus \{1\}$

Caso contrário, ou I é impróprio ou I é maximal e por isso é primo

$n\mathbb{Z} \times m\mathbb{Z}$ não é primo porque

$(n, 1), (1, m) \notin n\mathbb{Z} \times m\mathbb{Z}$

mas $(n,m) \left(= (n,1) \times (1,m)\right) \in n\mathbb{Z} \times m\mathbb{Z}$.