2.3 Domínios de integridade e corpos

Vamos supor que A é um anel não nulo, isto é $A \neq \{0\}$. Sendo assim, $1 \neq 0$ e A tem pelo menos dois elementos.

Definição 2.3.1. Seja A um anel não nulo. Um elemento $a \neq 0$ de A diz-se um *divisor de zero* se existe um elemento $b \neq 0$ em A tal que $ab = 0$ ou $ba = 0$.

Definição 2.3.2. Um *domínio de integridade* é um anel A comutativo não nulo que não admite divisores de zero, isto é, para quaisquer $a, b \in A$, $ab = 0$ implica $a = 0$ ou $b = 0$.

Exemplos 2.3.3. (i) $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são domínios de integridade.
(ii) $\mathbb{Z}_4$ não é um domínio de integridade. $[2]$ é um divisor de zero em $\mathbb{Z}_4$ pois $[2]\cdot[2] = [0]$.
(iii) Qualquer subanel de um domínio de integridade é um domínio de integridade.

Proposição 2.3.4. *Sejam A um domínio de integridade, $a \in A \setminus \{0\}$ e $b, c \in A$. Então $ab = ac \Rightarrow b = c$ e $ba = ca \Rightarrow b = c$.*

Demonstração: Como A é comutativo, basta mostrar a primeira implicação. Se $ab = ac$, então $a(b - c) = ab - ac = 0$. Como $a \neq 0$, $b - c = 0$. Logo $b = c$. □

Definição 2.3.5. Um ideal I de um anel A diz-se *primo* se $I \neq A$ e se para quaisquer dois elementos $a, b \in A$, $ab \in I$ implica $a \in I$ ou $b \in I$.

Exemplos 2.3.6. (i) Um anel comutativo não nulo é um domínio de integridade se e só se $\{0\}$ é um ideal primo.
(ii) Para $n \geq 1$, $n\mathbb{Z}$ é um ideal primo de $\mathbb{Z}$ se e só se n é primo.

Proposição 2.3.7. *Sejam A um anel comutativo e $I \neq A$ um ideal de A. Então I é primo se e só se A/I é um domínio de integridade.*

Demonstração: Suponhamos primeiramente que I é primo. Como A é comutativo, A/I é comutativo também. Como $I \neq A$, o anel A/I é não nulo. Sejam $a, b \in I$ tais que $(a + I)(b + I) = ab + I = I$. Então $ab \in I$ e portanto $a \in I$ ou $b \in I$. Logo $a + I = I$ ou $b + I = I$. Segue-se que A/I é um domínio de integridade.

Suponhamos inversamente que A/I é um domínio de integridade. Sejam $a, b \in A$ tais que $ab \in I$. Então $(a + I)(b + I) = ab + I = I$, pelo que $a + I = I$ ou $b + I = I$. Segue-se que $a \in I$ ou $b \in I$ e então que I é primo. □

Corolário 2.3.8. *$\mathbb{Z}_n$ é um domínio de integridade se e só se n é primo.*

Definição 2.3.9. Um anel comutativo A não nulo é um *corpo* se todo o elemento $a \in A$ não nulo é invertível (relativamente à multiplicação).

Exemplos 2.3.10. (i) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ são corpos.
(ii) $\mathbb{Z}$ não é um corpo.

Proposição 2.3.11. *Qualquer corpo é um domínio de integridade.*

Demonstração: Sejam K um corpo e $a, b \in K$ tais que $ab = 0$ e $a \neq 0$. Então $b = a^{-1}ab = a^{-1}0 = 0$. Como K é comutativo e não nulo, podemos concluir que K é um domínio de integridade. □

Proposição 2.3.12. *$\mathbb{Z}_n$ é um corpo se e só se n é primo.*

Demonstração: Se n não é primo, $\mathbb{Z}_n$ não é um anel de integridade, pelo que não é um corpo. Se n é primo, $\mathbb{Z}_n$ é comutativo e não nulo e segue-se do Exercício que qualquer elemento não nulo de $\mathbb{Z}_n$ é invertível. Consequentemente, $\mathbb{Z}_n$ é um corpo. □

Observação 2.3.13. Num corpo K, os únicos ideais são os ideais principais $(0) = \{0\}$ e $(1) = K$. Com efeito, se $I \neq \{0\}$ é um ideal de K e $x \in I \setminus \{0\}$, então $1 = x^{-1}x \in I$, pelo que $I = K$.

Definição 2.3.14. Um ideal I de um anel A diz-se *maximal* se $I \neq A$ e se para qualquer ideal J de A, $I \subseteq J \neq A \Rightarrow J = I$.

Proposição 2.3.15. *Sejam A um anel comutativo e $I \neq A$ um ideal. Então I é maximal se e só se A/I é um corpo.*

Demonstração: Suponhamos primeiramente que I é maximal. Seja $a \in A \setminus I$. Então $(a) + I$ é um ideal de A que contém I como subconjunto próprio. Como I é maximal, $(a) + I = A$. Logo existem $b \in A$ e $x \in I$ tais que $1 = ab + x$. Tem-se $(a + I)(b + I) = ab + I = ab + x + I = 1 + I$, pelo que $a + I$ é uma unidade de A/I. Para qualquer $x \in A$, $(x + I)I = I \neq 1 + I$, pelo que I não é invertível em A/I. Segue-se que A/I é um corpo.

Suponhamos agora que A/I é um corpo. Seja J um ideal de A tal que $I \subseteq J \neq A$. Seja $a \in J$. Suponhamos, por absurdo, que $a \notin I$. Então $a + I$ é uma unidade de A/I e existe $b \in A$ tal que $ab + I = (a + I)(b + I) = 1 + I$. Logo $ab - 1 \in I \subseteq J$. Como $ab \in J$, obtém-se $1 \in J$ e então $J = A$. Contradição! Portanto $a \in I$ e I é maximal. □

Corolário 2.3.16. *Qualquer ideal maximal de um anel é primo.*

Proposição 2.3.17. *Seja A um domínio de integridade. Uma relação de equivalência em $A \times (A \setminus \{0\})$ é dada por $(a, b) \sim (x, y) \Leftrightarrow ay = xb$. Se $(a, b) \sim (x, y)$ e $(c, d) \sim (u, v)$, então $(ad + cb, bd) \sim (xv + uy, yv)$ e $(ac, bd) \sim (xu, yv)$.*

Demonstração: É óbvio que a relação $\sim$ é reflexiva e simétrica. Sejam $(a,b),(x,y),(u,v) \in A \times (A \setminus \{0\})$ tais que $(a,b) \sim (x,y)$ e $(x,y) \sim (u,v)$. Então $ay = xb$ e $xv = uy$. Logo $avy = ayv = xbv = bxv = buy$. Como $y \neq 0$, obtém-se $av = bu = ub$, ou seja, $(a,b) \sim (u,v)$. Logo $\sim$ é transitiva e então uma relação de equivalência.

Suponhamos agora que $(a,b) \sim (x,y)$ e $(c,d) \sim (u,v)$. Então $(ad+cb)yv = adyv + cbyv = aydv + cvby = xbdv + udby = xvbd + uybd = (xv+uy)bd$. Logo $(ad+cb,bd) \sim (xv+uy,yv)$. Tem-se $acyv = aycv = xbud = xubd$ e então $(ac,bd) \sim (xu,yv)$. □

Definição 2.3.18. Seja A um domínio de integridade e $\sim$ a relação de equivalência em $A \times (A \setminus \{0\})$ dada por $(a,b) \sim (x,y) \Leftrightarrow ay = xb$. A classe de equivalência de um par $(a,b) \in A \times (A \setminus \{0\})$ é a *fracção* $\dfrac{a}{b}$. Pela proposição precedente podemos definir a adição e a multiplicação de fracções por

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} \qquad \text{e} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

O *corpo de fracções* de A, $Frac(A)$, é o conjunto das fracções $\dfrac{a}{b}$ $(a,b \in A,\ b \neq 0)$ munido da adição e da multiplicação de fracções.

Exemplo 2.3.19. $Frac(\mathbb{Z}) = \mathbb{Q}$.

Definição 2.3.20. Seja A um anel. A *característica* de A é definida por

$$\operatorname{car}(A) = \begin{cases} 0, & \text{se } |1| = \infty, \\ |1|, & \text{caso contrário.} \end{cases}$$

Exemplos 2.3.21. Tem-se $\operatorname{car}(\mathbb{Z}) = \operatorname{car}(\mathbb{Q}) = \operatorname{car}(\mathbb{R}) = 0$ e $\operatorname{car}(\mathbb{Z}_n) = n$.

Notas 2.3.22. (i) Num anel A de característica n tem-se $na = 0$ para todo o $a \in A$. Com efeito, para qualquer $a \in A$, $na = n(1a) = (n1)a = 0a = 0$.

(ii) Sejam A um anel e $f\colon \mathbb{Z} \to A$ o homomorfismo de anéis dado por $f(n) = n \cdot 1$. Note-se que f é o único homomorfismo de anéis de $\mathbb{Z}$ para A. Tem-se $\operatorname{car}(A) = n$ se e só se $\operatorname{Ker}(f) = n\mathbb{Z}$. Segue-se que a característica de A é o único número natural n tal que A contém um subanel isomorfo a $\mathbb{Z}/n\mathbb{Z}$.

Proposição 2.3.23. *A característica de um domínio de integridade é ou* 0 *ou um número primo.*

Demonstração: Seja A um domínio de integridade com $\operatorname{car}(A) \neq 0$. Então o elemento 1 de A tem ordem finita e $\operatorname{car}(A) = |1|$. Sejam $1 \leq k \leq l \leq |1|$ inteiros tais que $kl = |1|$. Então $k1 \cdot l1 = kl1 = |1|1 = 0$, pelo que $k1 = 0$ ou $l1 = 0$. Segue-se que $l = |1|$ e $k = 1$. Logo $\operatorname{car}(A) = |1|$ é um número primo. □

Nota 2.3.24. Existe uma múltiplicação com a qual o grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ é um corpo. Este corpo tem característica 2 e 4 elementos. Note-se que para qualquer número primo p e qualquer número natural $n \geq 1$, existe um corpo $\mathbb{F}_{p^n}$ de característica p com p^n elementos e este corpo é único a menos de isomorfismo. Além disso, qualquer corpo finito é isomorfo a um dos corpos $\mathbb{F}_{p^n}$.

2.4 Divisibilidade num domínio de integridade

Definição 2.4.1. Seja A um domínio de integridade e sejam $a, b \in A$. Diz-se que a *divide* b (escreve-se $a|b$) se existir $q \in A$ tal que $a = bq$. Diz-se que a e b são *associados* se $a|b$ e $b|a$.

Notas 2.4.2. (i) Tem-se: $a|b \Leftrightarrow b \in (a) \Leftrightarrow (a) \subset (a)$.

(ii) Os elementos a e b são associados se e só se $(a) = (b)$. Mostra-se também que a e b são associados se e só se existir $u \in A$ invertível tal que $b = au$.

(iii) Qualquer elemento $a \in A$ divide 0 pois $0 = 0 \cdot a$ mas não é um divisor de zero no sentido da definição 2.3.1 pois, sendo A um domínio de integridade, não existe $q \neq 0$ tal que $0 = aq$.

Definição 2.4.3. Seja A um domínio de integridade e seja $p \in A$ um elemento não nulo, não invertível.

- p é dito *primo* se, para todos os $a, b \in A$, $p|ab \Rightarrow p|a$ ou $p|b$.
- p é dito *irredutível* se, para todos os $a, b \in A$, $p = ab \Rightarrow a$ é invertível ou b é invertível .

Nota 2.4.4. São duas noções que estendem a noção usual de primo nos inteiros. Em particular, $p \in \mathbb{Z}$ é primo/irredutível se e só se $|p|$ é um natural primo no sentido usual.

Proposição 2.4.5. Seja A um domínio de integridade e seja $p \in A$ um elemento não nulo, não invertível. Se p é primo então p é irredutível.

Demonstração: Sejam $a, b \in A$ tais que $p = ab$. Como $p \neq 0$, temos $a \neq 0$ e $b \neq 0$. Como $p = ab$, podemos dizer que $p|ab$ (pois $ab = 1 \cdot p$) e, como p é primo, temos $p|a$ ou $p|b$. Se $p|a$, então existe $q \in A$ tal que $a = pq$. Como $p = ab$, obtemos $a = abq$ e $a(1 - bq) = 0$. Como $a \neq 0$ e A é um domínio de integridade, obtemos $1 - bq = 0$. Logo $bq = 1$ e, sendo A comutativo, podemos concluir que b é invertível. Da mesma forma, se $b \neq 0$, obtemos que a é invertível. Em todos os casos, obtemos a invertível ou b invertível e podemos concluir que p é irredutível. □

Proposição 2.4.6. Seja A um domínio de integridade e seja $p \in A$ um elemento não nulo, não invertível. Considere o ideal (p) de A gerado por p. Tem-se

(i) p é primo se e só se (p) é primo.

(ii) Se (p) é maximal então p é irredutível.

Demonstração: Como p é não invertível tem-se $(p) \neq A$. A alínea (i) segue imediatamente das definições de elemento e ideal primo. Como um ideal maximal e sempre primo, a alínea (ii) segue da alínea (i) e da proposição anterior. □

Não é verdade em geral que um elemento irredutível seja um elemento primo (ver Folha 6 - Ex 9). No entanto, existem classes de anéis em que isto é verdade.

Definição 2.4.7. Seja A um domínio de integridade. Diz-se que A é um *domínio de fatorização única* se

(E) Para todo o $a \in A$ não nulo e não invertível, existem $p_1, \ldots, p_n$ elementos irredutíveis de A tais que $a = p_1 \cdots p_n$.

(U) Esta decomposição é única a menos da ordem e de fatores invertíveis. Isto é, se $p_1 \cdots p_n = q_1 \cdots q_m$ onde os p_i e q_j $(1 \leq i \leq n,\ 1 \leq j \leq m)$ são irredutíveis, então $n = m$ e existe uma permutação $\sigma \in S_n$ tal que, para todo o $i \in \{1, \cdots, n\}$, p_i e $q_{\sigma(i)}$ são associados.

Exemplos de domínios de fatorização única são $\mathbb{Z}$ (através da decomposição de um natural em naturais primos) e anéis de polinómios.

Proposição 2.4.8. Seja A um domínio de fatorização única e seja $p \in A$ um elemento não nulo não invertível. Se p é irredutível então p é primo.

Demonstração: Sejam $a, b \in A$ tais que $p|ab$. Queremos ver que $p|a$ ou $p|b$. Como $p|ab$ existe $q \in A$ tal que $ab = pq$. Em primeiro lugar, analisemos alguns casos particulares. Se $a = 0$ temos $a = 0 \cdot p$ pelo que $p|a$. Se a é invertível, temos $b = a^{-1}pq$ pelo que $p|b$. Da mesma forma, se $b = 0$, tem-se $p|b$ e, se b é invertível, tem-se $p|a$. Se $q = 0$ tem-se $a = 0$ ou $b = 0$ pelo que $p|a$ ou $p|b$. Se q é invertível, temos $p = abq^{-1}$. Como p é irredutível, temos a invertível ou bq^1 invertível. No primeiro caso, obtemos $b = pqa^{-1}$ pelo que $p|b$. No segundo caso, $a = pqb^{-1}$ pelo que $p|a$. Em todos os casos analisados, chegamos à conclusão que $p|a$ ou $p|b$. Podemos agora supor que a, b e q são não nulos, não invertíveis. Como A é um domínio de fatorização única, existem $p_1, \ldots, p_n, p'_1, \ldots, p'_m, p''_1, \ldots, p''_l$ elementos irredutíveis de A tais que $a = p_1 \cdots p_n$, $b = p'_1 \cdots p'_m$ e $q = p''_1 \cdots p''_l$. Como $ab = pq$ obtemos

$$p_1 \cdots p_n \cdot p'_1 \cdots p'_m = p \cdot p''_1 \cdots p''_l.$$

Pela unicidade da decomposição em irredutíveis, p é associado a um dos p_i (neste caso $p|a$) ou a um dos p'_j (neste caso $p|b$). Em todos os casos $p|a$ ou $p|b$ e podemos concluir que p é primo.

Definição 2.4.9. Um domínio de integridade A diz-se um *domínio de ideais principais* se todos os ideais de A são principais.

Exemplos 2.4.10. (i) Qualquer corpo é um domínio de ideais principais.
(ii) $\mathbb{Z}$ é um domínio de ideais principais.

Proposição 2.4.11. Seja A um domínio de ideais principais e seja $p \in A$ um elemento não nulo, não invertível. Se p é irredutível então (p) é maximal.

Demonstração: Como p não é invertível, $(p) \neq A$. Seja J um ideal de A tal que $(p) \subset J$. Queremos mostrar que $J = (p)$ ou $J = A$. Como A é um domínio de ideais principais, existe $a \in A$ tal que $J = (a)$. De $(p) \subset (a)$ deduzimos que $p \in (a)$ e que existe $b \in A$ tal que $p = ab$. Como p é irredutível, a é invertível ou b é invertível. Se a é invertível temos $J = (a) = A$. Se b é invertível, p e a são associados e consequentemente $J = (a) = (p)$. Podemos concluir que (p) é maximal. □

Corolário 2.4.12. Sejam A um domínio de ideais principais e seja $p \in A$ um elemento não nulo, não invertível. São equivalentes:

(i) p é primo;

(ii) p é irredutível;

(iii) (p) é maximal;

(iv) (p) é primo.

Por fim, pode se estabelecer o seguinte resultado:

Teorema 2.4.13. Seja A um anel. Se A é um domínio de ideais principais então A é um domínio de fatorização única.