Capítulo 1

Anéis (revisitados)

Pré-requisitos

- noções básicas de grupos, anéis, domínios de integridade e corpos.
- os anéis $(\mathbb{Z}, +, \times)$ e $(\mathbb{Z}_n, +_n, \times_n)$; anéis de polinómios.
- divisibilidade, mdc e mmc.
- ideais principais, ideais primos e ideais maximais. Domínios de ideais principais (DIP).

(`www.mat.uc.pt/~picado/corpos/apontamentos.html`: Capítulos 1 e 2)

Ao longo do curso, se nada for dito em contrário, assumiremos que A denota um **anel comutativo com identidade**. Denotaremos por A^* o conjunto das unidades de A.

1. Divisibilidade. Elementos primos e irredutíveis

Dois elementos $a, b \in A$ dizem-se *associados* se existir $u \in A^*$ tal que $a = ub$.
Diz-se que a *divide* b (e escreve-se $a \mid b$) se existir $c \in A$ tal que $ac = b$.

Propriedades básicas:

(1) A relação "ser associado" (que denotaremos por $\sim$) é uma relação de equivalência, em que a classe de cada elemento a é o conjunto $aA^* = \{au \mid u \in A^*\}$.

(2) A relação $\mid$ é reflexiva e transitiva mas nunca é simétrica ($1 \mid 0$ mas $0 \nmid 1$) e não é necessariamente anti-simétrica (pense por exemplo em $\mathbb{Z}$, no facto de $2 \mid -2$ e $-2 \mid 2$; mas em $\mathbb{Z}_2$ já é anti-simétrica).

(3) Se $a \mid b$ e $c \mid d$ então $ac \mid bd$.

(4) Num domínio de integridade, $\langle a \rangle \subseteq \langle b \rangle$ se e só se $b \mid a$. Como $p \mid q$ e $q \mid p$ se e só se p e q forem associados, então $\langle a \rangle = \langle b \rangle$ se e só se a e b são associados. Além disso, $a \in A^*$ se e só se $\langle a \rangle = A$.

(5) Se A é um domínio de integridade então $A[x]^* = A^*$.

Demonstração. Exercício. ∎

O Teorema da Factorização Única nos inteiros e nos anéis de polinómios (com coeficientes num domínio de integridade) são tão importantes que é natural averiguar se se podem generalizar a outros anéis. Por outro lado, os anéis de polinómios exibem tantas semelhanças com o anel $\mathbb{Z}$ dos inteiros que é bem possível que não sejam mera coincidência, e sejam sim casos particulares de resultados válidos num contexto muito mais geral.

Como sabemos, os inteiros primos podem ser caracterizados de várias maneiras. Por exemplo, um inteiro $p \neq 0$ não invertível é primo se e só se

$$p \mid ab \Rightarrow p \mid a \text{ ou } p \mid b.$$

Equivalentemente, p é primo se e só se

$$p = ab \Rightarrow a = \pm 1 \text{ ou } b = \pm 1.$$

É claro que podemos adaptar qualquer uma destas condições a um domínio de integridade qualquer. Como deixam de ser equivalentes teremos que arranjar um nome diferente para denominar os elementos que verificam a segunda:

Seja D um domínio de integridade.

- Um elemento $p \in D$ diz-se *primo* se $p \neq 0$, $p \notin D^*$, e $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.
- Um elemento $q \in D$ diz-se *irredutível* se $q \neq 0$, $q \notin D^*$, e $q = ab \Rightarrow a \in D^*$ ou $b \in D^*$.

Portanto, os elementos irredutíveis são os que apenas admitem factorizações triviais e um elemento $p \neq 0$ é primo se e só se o respectivo ideal principal $\langle p \rangle$ é primo. As tabelas seguintes comparam estas definições em 3 exemplos importantes: $\mathbb{Z}$, $C[x]$ (C: corpo) e $D[x]$ (D: domínio).

DOMÍNIO	$\mathbb{Z}$
unidades	$\mathbb{Z}^* = \{-1, 1\}$
primo	$p \neq 0, \pm 1$ $p\|ab \Rightarrow p\|a$ ou $p\|b$
irredutível	$p \neq 0, \pm 1$ $p = ab \Rightarrow a \in \mathbb{Z}^*$ ou $b \in \mathbb{Z}^*$ isto é $p = ab \Rightarrow a = 1$ ou $a = -1$ ou $b = 1$ ou $b = -1$

DOMÍNIO	$\boldsymbol{C[x]}$ (C: corpo)
unidades	$C[x]^* = \{p(\boldsymbol{x}) \in C[x] : gr(p(\boldsymbol{x})) = 0\}$
primo	$gr(p(\boldsymbol{x})) \geq 1$ $p(\boldsymbol{x})\|a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow p(\boldsymbol{x})\|a(\boldsymbol{x})$ ou $p(\boldsymbol{x})\|b(\boldsymbol{x})$
irredutível	$gr(p(\boldsymbol{x})) \geq 1$ $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow a(\boldsymbol{x}) \in C[x]^*$ ou $b(\boldsymbol{x}) \in C[x]^*$ isto é $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow gr(a(\boldsymbol{x})) = 0$ ou $gr(b(\boldsymbol{x})) = 0$

DOMÍNIO	$\boldsymbol{D[x]}$ (D: domínio de integridade)
unidades	$D[x]^* = \{p(\boldsymbol{x}) \in D[x] : gr(p(\boldsymbol{x})) = 0, p(\boldsymbol{x}) = c \in D^*\}$
primo	$p(\boldsymbol{x}) \neq 0$, $p(\boldsymbol{x}) \notin D[x]^*$ $p(\boldsymbol{x})\|a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow p(\boldsymbol{x})\|a(\boldsymbol{x})$ ou $p(\boldsymbol{x})\|b(\boldsymbol{x})$
irredutível	$p(\boldsymbol{x}) \neq 0$, $p(\boldsymbol{x}) \notin D[x]^*$ $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow a(\boldsymbol{x}) \in D[x]^*$ ou $b(\boldsymbol{x}) \in D[x]^*$ isto é $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow a(\boldsymbol{x}) = c \in D^*$ ou $b(\boldsymbol{x}) = d \in D^*$

Como sabemos, além de $\mathbb{Z}$, também em $C[x]$ os elementos primos coincidem com os elementos irredutíveis. Não é esse o caso em todos os domínios de inte-

gridade, mas é possível identificar extensas classes de domínios onde estas duas noções são equivalentes.

Proposição 1.1. *Seja D um domínio de integridade e $u \in D^*$.*

(1) *Se p é primo então up é primo. Se q é irredutível então uq é irredutível.*

(2) *Todo o elemento primo é irredutível.*

Demonstração. (1) Exercício.

(2) Se p é primo e $p = ab$ então $p \mid ab$ e, portanto, $p|a$ ou $p|b$. Se, por exemplo, $p|a$, então existe $x \in D$ tal que $a = px$. Concluímos então que $p = ab = pxb$, e como $p \neq 0$, $1 = xb$, ou seja, b é uma unidade. De igual forma, se $p|b$ concluímos que a é invertível. ∎

A implicação recíproca da de (2) é, em geral, falsa. Por exemplo, no domínio

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\},$$

3 é irredutível mas não é primo, uma vez que 3 divide $(2 + \sqrt{-5})(2 - \sqrt{-5})$ (pois $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 3 \cdot 3$) mas não divide $2 + \sqrt{-5}$ nem $2 - \sqrt{-5}$. Note que neste exemplo não há factorizações únicas:

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}),$$

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Proposição 1.2. *Seja D um domínio de integridade e $p \in D$, $p \neq 0$.*

(1) *p é primo se e só se o ideal principal $\langle p \rangle$ é primo.*

(2) *Se o ideal principal $\langle p \rangle$ é maximal então p é irredutível.*

Demonstração. São consequência imediata das definições e das propriedades básicas que já verificámos. ∎

A recíproca da afirmação (2) não é, em geral, verdadeira: 2 é um elemento irredutível de $\mathbb{Z}[x]$ mas $\langle 2 \rangle$ não é um ideal maximal de $\mathbb{Z}[x]$ pois $\langle 2 \rangle \subset \langle 2, x \rangle \subset \mathbb{Z}[x]$. O problema neste exemplo reside no facto de o ideal $\langle 2, x \rangle$ não ser principal (e, portanto, $\mathbb{Z}[x]$ não ser um DIP). Com efeito:

Proposição 1.3. *Seja D um domínio de ideais principais. Então $\langle p \rangle$ é maximal se e só se p é irredutível.*

Demonstração. Seja p irredutível e $\langle p\rangle \subseteq \langle a\rangle$. Então $a \mid p$, e portanto ou $a \in D^*$ (e logo $\langle a\rangle = D$), ou a é um associado de p (e logo $\langle a\rangle = \langle p\rangle$). Assim, $\langle p\rangle$ é maximal. ∎

(Onde usámos a hipótese de D ser um DIP?)

Corolário 1.4. *Num domínio de ideais principais, um elemento é irredutível se e só se é primo.*

Demonstração. Seja p um elemento irredutível e suponhamos que $p \mid ab$. Consideremos o ideal principal $I = \langle p\rangle$. Pela proposição anterior, I é maximal pelo que o anel quociente D/I é um corpo (logo não tem divisores de zero). Mas

$$(a + I) \cdot (b + I) = ab + I = I,$$

uma vez que, por hipótese, $ab \in I$. Então, necessariamente um dos factores é nulo, isto é, $a + I = I$ ou $b + I = I$. Isto significa precisamente que $a \in I$ ou $b \in I$, ou seja, $p \mid a$ ou $p \mid b$. ∎

Observação. É claro que se nos tivéssemos lembrado (Corpos e Equações Algébricas) que

todo o ideal maximal é primo,

ou que

I é primo sse D/I é um domínio de integridade,

a prova era ainda mais rápida: decorre imediatamente de 1.2 e 1.3.

2. Domínios de factorização única

Um domínio de integridade D diz-se um *domínio de factorização única* (abreviadamente, DFU) se as seguintes duas condições são satisfeitas para todo o elemento não nulo $a \in D \setminus D^*$:

(F) Existem elementos **irredutíveis** $p_1, p_2, \ldots, p_n$ tais que

$$a = p_1 p_2 \cdots p_n. \tag{2.1.1}$$

(U) Se $p_1, p_2, \ldots, p_n$ e $q_1, q_2, \ldots, q_m$ são irredutíveis e $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, então $m = n$ e existe uma permutação $\pi \in S_n$ tal que $p_i \sim q_{\pi(i)}$ para $i = 1, 2, \ldots, n$.

Por outras palavras, num domínio de factorização única, todo o elemento não nulo e não invertível possui uma factorização num produto de elementos irredutíveis, e esta decomposição é única a menos da ordem dos factores e de produto por unidades; após reordenação, para cada i existe uma unidade u_i tal que $p_i = q_i u_i$.

Por exemplo, em $\mathbb{Z}$,

$$1 \times 5 = 5 \times 1 = (-1) \times (-5) = (-5) \times (-1)$$

são as únicas factorizações do primo 5 e

$$1 \times (-5) = (-5) \times 1 = (-1) \times 5 = 5 \times (-1)$$

são as únicas factorizações do primo -5. Pelo Teorema Fundamental da Aritmética, $\mathbb{Z}$ é um domínio de factorização única. Pelo Teorema da Factorização Única em $C[x]$ (estudado no ano passado) $C[x]$ é também um DFU. Outro exemplo de domínio de factorização única é o anel dos *inteiros de Gauss*,

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

O exemplo $\mathbb{Z}[\sqrt{-5}]$ que vimos logo a seguir à Proposição 1.1 mostra que nem todo o domínio de integridade é um DFU.

Chama-se também *anéis de Gauss* aos domínios de factorização única. O Corolário 1.4 pode ser estendido aos domínios de factorização única:

Teorema 2.1. *Seja D um domínio de integridade. Então D é um DFU se e só se as seguintes condições se verificam:*

(1) *Todo o elemento irredutível é primo.*

(2) *toda a cadeia ascendente de ideais principais estabiliza, isto é, se*

$$\langle d_1 \rangle \subseteq \langle d_2 \rangle \subseteq \cdots \subseteq \langle d_n \rangle \subseteq \cdots$$

é uma cadeia ascendente de ideais, então existe um natural k tal que

$$\langle d_n \rangle = \langle d_k \rangle \text{ para todo o } n \geq k.$$

(Equivalentemente, a condição (2) significa que, sempre que $\cdots d_n \mid d_{n-1} \mid \cdots \mid d_1$ em D, então existe um natural k tal que $d_n \sim d_k$ para todo o $n \geq k$.)

Demonstração. Seja D um DFU e $p \in D$ um elemento irredutível. Se $p \mid ab$ então $ab = px$ para algum $x \in D$, onde x, a e b possuem factorizações do tipo (2.1.1):

$$x = p_1 p_2 \cdots p_n,\ a = q_1 q_2 \cdots q_m,\ b = r_1 r_2 \cdots r_k$$

com p_i, q_i, r_i irredutíveis em D. Logo $pp_1p_2\cdots p_n = q_1q_2\cdots q_m r_1 r_2 \cdots r_k$, e pela unicidade da factorização, p é associado de algum q_i ou de algum r_j. No primeiro caso, $p \mid a$, e no segundo, $p \mid b$. Logo, p é primo.

Por outro lado, seja

$$\langle d_1\rangle \subseteq \langle d_2\rangle \subseteq \cdots \subseteq \langle d_n\rangle \subseteq \cdots$$

uma cadeia ascendente de ideais principais. Claro que podemos supor $d_1 \neq 0$ e $d_i \notin D^*$ para todo o i. Seja

$$p_{i,1}\, p_{i,2}\, \cdots\, p_{i,n_i}$$

a factorização de cada d_i em factores irredutíveis. Como $d_i \mid d_1$ para qualquer i, os factores irredutíveis de d_i são factores de d_1, pelo que $n_i \leq n_1$. É então evidente que não poderão existir na cadeia mais de n_1 ideais distintos entre si. Consequentemente, existe um natural k tal que $\langle d_n\rangle = \langle d_k\rangle$ para todo o $n \geq k$.

Reciprocamente, suponhamos que D é um domínio de integridade que verifica as condições (1) e (2). Seja $a \in D \setminus D^*$ um elemento não nulo. Suponhamos por absurdo que a não é factorizável num produto de irredutíveis. Definamos por indução uma sucessão $\{a_n\}_{n\in\mathbb{N}}$ tal que

$$a_1 = a, a_{n+1} \mid a_n \quad \text{e} \quad a_n \nsim a_{n+1},$$

do seguinte modo:

Como a não é irredutível, $a = bc$ onde b e c não são unidades. É claro que b e c não podem ser ambos factorizáveis num produto de irredutíveis. Suponhamos (sem perda de generalidade) que b não o é; definimos $a_2 = b$. Claro que $a_2 \mid a_1$ e $a_1 \nsim a_2$. Como a_2 não é irredutível, podemos repetir o raciocínio e definir a_3 nas condições requeridas, e assim sucessivamente.

Os ideais principais gerados pelos a_n's satisfazem

$$\langle a_1\rangle \subset \langle a_2\rangle \subset \cdots \subset \langle a_n\rangle \subset \cdots$$

contradizendo a condição (2) de toda a cadeia ascendente de ideias principais estabilizar. Concluímos assim que todos os elementos não nulos em $D \setminus D^*$ são factorizáveis em produtos de elementos irredutíveis.

Quanto à unicidade, suponhamos que

$$p_1p_2\cdots p_n = q_1q_2\cdots q_m$$

com, digamos, $n \leq m$. Como os p_i's e q_j's são irredutíveis, por (1) são primos. Mas

$$p_n \mid q_1q_2\cdots q_m$$

logo p_n é associado de algum q_j (que designamos por $q_{\pi(n)}$). Excluindo estes dois elementos, e repetindo o raciocínio, concluímos por exaustão que $n = m$ e $p_i \sim q_{\pi(i)}$ para alguma permutação $\pi \in S_n$. ∎

Este resultado justifica o uso indiferente nos DFU's da expressão "*factorização irredutível*" ou "*factorização prima*" para designar factorizações do tipo (2.1.1). É evidente que nas factorizações (2.1.1) podemos agrupar os elementos irredutíveis que sejam associados entre si e reescrever a factorização na forma

$$a = uq_1^{n_1} q_2^{n_2} \cdots q_k^{n_k} \tag{2.1.2}$$

onde $u \in D^*$, $q_1, q_2, \ldots, q_k$ são irredutíveis (=primos), não associados dois a dois, e $n_1, n_2, \ldots, n_k \in \mathbb{N}$.

Corolário 2.2. *Todo o domínio de ideais principais é um domínio de factorização única.*

Demonstração. Pelo teorema anterior bastará mostrar que qualquer DIP satisfaz as condições (1) e (2). A primeira é verdade pelo Corolário 1.4. Quanto à segunda, consideremos a cadeia

$$\langle d_1 \rangle \subseteq \langle d_2 \rangle \subseteq \cdots \subseteq \langle d_n \rangle \subseteq \cdots$$

É um exercício simples verificar que $\bigcup_{i=1}^{\infty} \langle d_i \rangle$ é um ideal, necessariamente principal, por hipótese, e portanto $\bigcup_{i=1}^{\infty} \langle d_i \rangle = \langle d \rangle$. Isto significa que existe k tal que $d \in \langle d_k \rangle$ e então, claramente, $\langle d_n \rangle = \langle d_k \rangle$ para qualquer $n \geq k$. ∎

O recíproco é falso, como o exemplo $\mathbb{Z}[x]$ mostra (não é um DIP pois o ideal $\langle 2, x \rangle$ não é principal, e é um DFU como veremos na secção seguinte).

Seja D um domínio de integridade e $a, b \in D$.

- Um elemento $d \in D$ diz-se um *máximo divisor comum* de a e b se $d \mid a$, $d \mid b$ e se, para qualquer divisor comum d' de a e b, $d' \mid d$.
- Um elemento $m \in D$ diz-se um *mínimo múltiplo comum* de a e b se $a \mid m$, $b \mid m$ e se, para qualquer múltiplo comum m' de a e b, $m \mid m'$.

Observe que se d é um máximo divisor comum de a e b então o conjunto dos máximos divisores comuns de a e b, que denotaremos por $\mathrm{mdc}(a, b)$, é o conjunto $dD^* = \{du \mid u \in D^*\}$. (Analogamente para os mínimos múltiplos comuns; neste caso, denotaremos o respectivo conjunto por $\mathrm{mmc}(a, b)$.)

Proposição 2.3. *Seja D um DFU e $a, b \in D$. Suponhamos que*

$$a = uq_1^{r_1} q_2^{r_2} \cdots q_k^{r_k} \quad e \quad b = vq_1^{s_1} q_2^{s_2} \cdots q_k^{s_k}$$

para certos primos $q_1, q_2, \ldots, q_k$, unidades u, v e $r_1, r_2, \ldots, r_k, s_1, s_2, \ldots, s_k \in \mathbb{N}_0$. Então:

(1) $d = q_1^{\min(r_1,s_1)} \cdots q_k^{\min(r_k,s_k)} \in \operatorname{mdc}(a,b)$ *e* $m = q_1^{\max(r_1,s_1)} \cdots q_k^{\max(r_k,s_k)} \in \operatorname{mmc}(a,b)$.

(2) *Se $d' \in \operatorname{mdc}(a,b)$ e $m' \in \operatorname{mmc}(a,b)$, então existe $w \in D^*$ tal que $d'm' = wab$.*

(Note que é possível que, para algum primo q_i, tenhamos $r_i = 0$ ou $s_i = 0$; isso quer dizer que esse primo aparece efectivamente na factorização de a mas não na de b, ou vice-versa.)

Demonstração. (1) É claro que d é um divisor comum de a e b. Seja d' um outro divisor comum. É claro que não pode existir nenhum primo p que divida d' sem dividir a e b, e assim, é possível escrever

$$d' = wq_1^{t_1} \cdots q_k^{t_k}$$

com $w \in D^*$. Como $d' \mid a$ e $d' \mid b$, necessariamente $t_i \leq r_i, s_i$, e portanto

$$p_i^{t_i} \mid p_i^{\min(r_i,s_i)} \quad \text{e} \quad d' \mid d.$$

A prova para o mmc é análoga.

(2) Já sabemos que $d' = u'd$ e $m' = v'm$ para alguns $u', v' \in D^*$. Assim, $d'm' = u'v'dm$ e

$$\begin{aligned} dm &= q_1^{\min(r_1,s_1)+\max(r_1,s_1)} \cdots q_k^{\min(r_k,s_k)+\max(r_k,s_k)} \\ &= q_1^{r_1+s_1} \cdots q_k^{r_k+s_k} = u^{-1}v^{-1}ab. \end{aligned}$$

Basta tomar $w = u'v'u^{-1}v^{-1}$. ∎

Este último resultado generaliza o resultado básico dos inteiros que afirma que o máximo divisor comum é o produto dos factores primos comuns elevados ao menor expoente (e o mínimo múltiplo comum é o producto dos factores primos comuns e não comuns elevados ao maior expoente). Há muitas outras propriedades dos inteiros que se estendem aos DFU's e muitas vezes as próprias demonstrações estendem-se imediatamente ao caso geral. É o caso da prova da infinitude dos números primos em $\mathbb{Z}$ (atribuída a Euclides):

Proposição 2.4. *Num DFU que não é um corpo, existe um número infinito de elementos primos não associados.*

Demonstração. Seja D um DFU e suponhamos por absurdo que $p_1, \ldots, p_n$ era uma família completa de primos não associados de D (claro que esta família não é vazia pois D não é um corpo). Mas o elemento $a = p_1 \ldots p_n + 1$ não é divisível por nenhum dos primos naquela família (pois $p_i \mid a \Rightarrow p_i \mid a - p_1 p_2 \ldots p_n = 1$ e, como é óbvio, $p_i \mid 1$ sse $p_i \in D^*$, um absurdo). Consequentemente, a não admitiria nenhuma factorização em primos, o que é absurdo. ∎

3. Domínios de factorização única e polinómios

Quando estudámos polinómios em CORPOS E EQUAÇÕES ALGÉBRICAS provámos que se A é um corpo então $A[x]$ é um DFU. Vamos agora demonstrar que, mais geralmente, se A é um DFU também $A[x]$ o é. Começamos por determinar os irredutíveis em $A[x]$ de grau zero:

Proposição 3.1. *Seja D um domínio de integridade e $p(x) = a \in D$ um polinómio de grau 0. Então $p(x)$ é irredutível em $D[x]$ se e só se a for irredutível em D.*

Demonstração. Suponhamos que $p(x) = a$ é irredutível em $D[x]$ e $a = bc$ em D. Então b ou c pertencem a $D[x]^* = D^*$ o que mostra que a é irredutível em D.

Reciprocamente, se a for irredutível em D e $p(x) = a = q(x)r(x)$ em $D[x]$ então $\mathrm{gr}(q(x)) = \mathrm{gr}(r(x)) = 0$. Assim $q(x) = b$ e $r(x) = c$ com $b, c \in D$, $b, c \neq 0$. Como $a = bc$, pelo menos um dos elementos b ou c é uma unidade de D, ou seja, um dos polinómios $q(x)$ ou $r(x)$ é uma unidade de $D[x]$. ∎

Seja D um domínio de integridade e $p(x) \in D[x]$.

- $p(x)$ é um *polinómio primitivo* se $\mathrm{gr}(p(x)) \geq 1$ e os únicos divisores de $p(x)$ de grau zero forem unidades.
- Uma *factorização própria* de $p(x)$ é uma decomposição do tipo $p(x) = a(x)b(x)$ com $\mathrm{gr}(a(x)), \mathrm{gr}(b(x)) < \mathrm{gr}(p(x))$.

Por exemplo, $p(x) = 2x^2 + 2$ não é primitivo em $\mathbb{Z}[x]$ pois 2 divide $p(x)$ (mas em $\mathbb{Q}[x]$ já $p(x)$ é primitivo). Também não admite factorizações próprias em $\mathbb{Z}[x]$ (apesar de admitir a factorização $2(x^2 + 1)$).

Quanto aos irredutíveis não constantes:

Proposição 3.2. *Seja D um domínio de integridade. Se o grau de $p(x) \in D[x]$ for maior ou igual a 1, então $p(x)$ é irredutível em $D[x]$ se e só se for um polinómio primitivo que não admite factorizações próprias.*

Demonstração. Suponhamos que $p(x)$ é irredutível com $\mathrm{gr}(p(x)) \geq 1$. Por absurdo, se não fosse primitivo, podíamos factorizá-lo pondo em evidência um mdc dos seus coeficientes, e nessa factorização nenhum dos factores era uma unidade, uma contradição. Por outro lado, se admitisse uma factorização própria, é claro que também não poderia ser irredutível.

Reciprocamente, se $p(x)$ é primitivo sem factorizações próprias, claramente não é o polinómio nulo nem uma unidade. Se $p(x) = q(x)r(x)$ então, por hipótese, ou $q(x)$ ou $r(x)$ tem de ter grau zero. Suponhamos, sem perda de generalidade, que é $q(x)$. Portanto, $q(x) = a \in D$. Como $q(x) \mid p(x)$ e $p(x)$ é primitivo, necessariamente $q(x)$ é uma unidade. Logo $p(x)$ é irredutível. ∎

Teorema 3.3. *Seja D um DFU. Todo o elemento não nulo de $D[x] \setminus D[x]^*$ é um produto de elementos irredutíveis em $D[x]$. Estes são*

- *de grau zero, irredutíveis (=primos) em D, ou*
- *polinómios primitivos que não admitem factorizações próprias.*

Demonstração. Faremos a demonstração por indução sobre o grau n de $p(x)$:

Se $n = 0$, $p(x) = a \in D$ e portanto é claramente um produto de irredutíveis de D (por D ser um DFU).

Tomemos $p(x)$ de grau n e suponhamos, como hipótese de indução, que o resultado é válido para todos os polinómios de grau $< n$.

Se $p(x)$ admitir uma factorização própria então $p(x) = q(x)r(x)$ com $\mathrm{gr}(q(x)), \mathrm{gr}(r(x)) < n$ e, pela hipótese de indução, ambos são factorizáveis em polinómios dos dois tipos descritos. No caso em que $p(x)$ não admite factorizações próprias, se $p(x)$ for primitivo então é irredutível e está provado; se não for primitivo, podemos escrever $p(x) = aq(x)$ onde a é um mdc dos coeficientes de $p(x)$, não é unidade, e $q(x)$ é primitivo e também não tem factorizações próprias. Factorizando agora a em factores primos (usando o facto de D ser um DFU), e tendo em conta que $q(x)$ é irredutível por ser primitivo e não admitir factorizações próprias, chegamos à conclusão pretendida. ∎

Falta somente garantir a unicidade das factorizações para concluirmos que $D[x]$ é um DFU. Para isso vamos fazer o mesmo que se faz em $\mathbb{Z}$, em $C[x]$ ou na demonstração de que todo o DIP é DFU (Corolário 2.2): garantir que todos os irredutíveis mencionados no teorema anterior são primos em $D[x]$.

Proposição 3.4. *Seja D um DFU e p um elemento primo de D. Então $p(x) = p$ é primo em $D[x]$.*

Demonstração. Suponhamos que $p(x) \mid q(x)r(x)$ em $D[x]$ com

$$q(x) = a_n x^n + \cdots + a_1 x + a_0 \quad \text{e} \quad r(x) = b_m x^m \cdots + b_1 x + b_0.$$

Queremos provar que $p(x) \mid q(x)$ ou $p(x) \mid r(x)$, isto é, p divide todos os coeficientes de $q(x)$ ou todos os coeficientes de $r(x)$. Suponhamos, por absurdo, que isso não acontece (ou seja, que p não divide um dos factores de $q(x)$ e um dos factores de $r(x)$). Seja s o maior índice tal que $p \nmid a_s$ e t o maior índice tal que $p \nmid b_t$. Então $p \mid a_i$ e $p \mid b_j$ para quaisquer $i > s$ e $j > t$. Como o coeficiente c_{s+t} de x^{s+t} no produto $q(x)r(x)$ é igual a

$$a_{s+t}b_0 \cdots + a_{s+1}b_{t-1} + a_s b_t + a_{s-1}b_{t+1} + \cdots + a_0 b_{s+t}$$

e $p \nmid a_s b_t$, então $p \nmid c_{s+t}$ (pois por definição de s e t, p divide todas as outras parcelas em c_{s+t}). Isto contradiz o facto de p, por hipótese, dividir todos os coeficientes do produto $q(x)r(x)$. ∎

Lema 3.5. *Seja D um DFU, K o seu corpo de fracções, $p(x), q(x) \in D[x]$ e suponhamos que $p(x)$ é primitivo. Se $p(x) \mid q(x)$ em $K[x]$ então $p(x) \mid q(x)$ em $D[x]$.*

Demonstração. Por hipótese, $q(x) = r(x)p(x)$ para algum

$$r(x) = \frac{a_n}{b_n}x^n + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0} \in K[x] \quad (a_i, b_i \in D,\ b_i \neq 0).$$

Seja c um elemento de $\text{mmc}(b_0, b_1, \ldots, b_n)$ e $f(x) = cr(x) \in D[x]$. Então $cq(x) = cr(x)p(x) = f(x)p(x)$. Se c é uma unidade então $r(x) \in D[x]$ e imediatamente $p(x) \mid q(x)$ em $D[x]$. Caso contrário, seja $d \in D$ um dos factores primos de c.

> (Cuidado: apesar de d dividir c em D, não é óbvio que $d|f(x)$ em $D[x]$;
> nem sequer sabemos se $c|f(x)$ em $D[x]$ pois $r(x) \in K[x]$.)

Como $d \mid f(x)p(x)$ então, pela proposição anterior, $d \mid f(x)$ ou $d \mid p(x)$. Mas $p(x)$ é primitivo, logo $d \nmid p(x)$ e necessariamente $d \mid f(x)$. Então $(1/d)f(x) \in D[x]$ e,

como $(1/d)f(x) = (c/d)r(x)$, c/d é múltiplo de todos os b_i $(i = 0, 1, \ldots, n)$, o que é impossível pois c/d divide estritamente c e $c \in \text{mmc}(b_0, b_1, \ldots, b_n)$. Portanto, c é mesmo uma unidade e $r(x) \in D[x]$. ∎

Lema 3.6. [Lema de Gauss] *Seja D um DFU e K o seu corpo de fracções. Se $p(x) \in D[x]$, $p(x) \neq 0$, com $p(x) = q(x)r(x)$, $q(x), r(x) \in K[x]$, então existe $a \in K$, $a \neq 0$, tal que*

$$q'(x) := aq(x) \in D[x], \quad r'(x) := (1/a)r(x) \in D[x] \quad e \quad p(x) = q'(x)r'(x).$$

(Isto implica que $p(x) \in D[x]$ não admite factorizações próprias em $D[x]$ sse é irredutível em $K[x]$.)

Demonstração. Seja c um múltiplo dos denominadores dos coeficientes de $q(x)$. É claro que $cq(x) \in D[x]$. Seja agora d um mdc dos coeficientes de $cq(x)$. Pondo-o em evidência obtemos $cq(x) = dq'(x)$, sendo $q'(x) \in D[x]$ primitivo. Então

$$p(x) = \frac{c}{d}\, q(x) \cdot \frac{d}{c}\, r(x) = q'(x)\frac{d}{c}\, r(x).$$

Bastará então tomar $a := c/d$. De facto: $aq(x) \in D[x]$; como $q'(x) \in D[x]$ é primitivo e divide $p(x)$ em $K[x]$, pelo lema anterior divide $p(x)$ em $D[x]$; assim, $(1/a)r(x) = p(x)/q'(x) \in D[x]$. ∎

Proposição 3.7. *Seja D um DFU e $p(x) \in D[x]$ um polinómio primitivo que não admite factorizações próprias. Então $p(x)$ é primo em $D[x]$.*

Demonstração. Suponhamos então que $p(x) \mid q(x)r(x)$, com $q(x), r(x) \in D[x]$, e seja K o corpo das fracções de D. Comecemos por verificar que $p(x)$ é irredutível em $K[x]$. Se não fosse, teríamos $p(x) = p_1(x)p_2(x)$, $p_1(x), p_2(x) \in K[x]$, ambos com grau ≥ 1. Então, pelo Lema de Gauss, teríamos $p(x) = p_1'(x)p_2'(x)$, com $p_1'(x), p_2'(x) \in D[x]$ de grau ≥ 1 ($\text{gr}(p_1'(x)) = \text{gr}(p_1(x))$ e $\text{gr}(p_2'(x)) = \text{gr}(p_2(x))$), o que é contraditório com a hipótese.

Portanto, $p(x)$ é irredutível em $K[x]$, e como $K[x]$ é um DFU, $p(x)$ é primo em $K[x]$ e portanto $p(x) \mid q(x)$ ou $p(x) \mid r(x)$ em $K[x]$. Como $p(x)$ é primitivo, o Lema 3.5 assegura-nos que $p(x) \mid q(x)$ ou $p(x) \mid r(x)$ em $D[x]$, e portanto, que $p(x)$ é primo em $D[x]$. ∎

Demonstrámos assim que todos os irredutíveis de $D[x]$ são primos e podemos assim obter finalmente o tão desejado teorema:

Teorema 3.8. *Seja D um DFU. Então $D[x]$ é um DFU.*

Demonstração. A factorização em irredutíveis existe pelo Teorema 3.3. Provámos em 3.4 e 3.7 que todos os irredutíveis nestas factorizações são primos. Isto é suficiente para garantirmos a unicidade das factorizações:

Sejam

$$p_1(x)\cdots p_n(x) = q_1(x)\cdots q_m(x)$$

duas factorizações em irredutíveis (que já sabemos serem primos) do mesmo elemento de $D[x]$. Vamos usar indução sobre n. Para $n = 1$ temos $p_1(x) = q_1(x)\cdots q_m(x)$. Como $p_1(x)$ é irredutível, não admite factorizações próprias, logo $m = 1 = n$ e $q_1(x) = p_1(x)$.

Supondo agora que o resultado vale para $n-1$, consideremos

$$p_1(x)\cdots p_n(x) = q_1(x)\cdots q_m(x)$$

duas factorizações do mesmo elemento em irredutíveis de $D[x]$. Como

$$p_1(x) \mid q_1(x)\cdots q_m(x)$$

e $p_1(x)$ é primo, existe i tal que $p_1(x) \mid q_i(x)$; reordenando os q_i's podemos supor $i = 1$. Como $q_1(x)$ é irredutível, $q_1(x) = u_1(x)p_1(x)$ onde $u_1(x)$ é uma unidade. Aplicando a lei do corte obtemos

$$p_2(x)\cdots p_n(x) = (u_1(x)q_2(x))\cdots q_m(x).$$

A decomposição da direita ainda é uma decomposição em irredutíveis e a da esquerda tem $n-1$ factores. Pela hipótese de indução, $m-1 = n-1$ (ou seja, $m = n$) e, após reordenação, $p_i(x) \sim q_i(x)$ $(i = 1, 2, \ldots, n)$. ∎

Em particular, $\mathbb{Z}[x]$ é um DFU, assim como $D[x, y] := D[x][y]$.

Terminamos com alguns critérios de irredutibilidade que permitem identificar alguns polinómios irredutíveis de $D[x]$ quando D é um DFU, e que generalizam resultados estudados em CORPOS E EQUAÇÕES ALGÉBRICAS.

Proposição 3.9. [Critério de Eisenstein] *Seja D um DFU e K o seu corpo de fracções. Se*

$$p(x) = a_n x^n + \cdots a_1 x + a_0 \in D[x]$$

e existe um primo $p \in D$ tal que

$$p \mid a_i \quad (i = 0, 1, \ldots, n-1), \quad p \nmid a_n \quad \text{e } p^2 \nmid a_0$$

então $p(x)$ é irredutível em $K[x]$.

(Equivalentemente, pelo Lema de Gauss, $p(x)$ não tem factorizações próprias em $D[x]$; portanto, será irredutível em $D[x]$ se for primitivo.)

Demonstração. Se, por absurdo, $p(x)$ não for irredutível em $K[x]$ então, pelo Lema de Gauss, admite uma factorização própria em $D[x]$

$$q(x)r(x) = (b_s x^s + \cdots b_1 x + b_0)(c_t x^t + \cdots c_1 x + c_0) \quad (s, t \geq 0).$$

Como $b_0 c_0 = a_0$ é divisível por p e não por p^2, um dos factores não é divisível por p (digamos b_0) e necessariamente $p \mid c_0$. Como $b_s c_t = a_n$ e $p \nmid a_n$, então $p \nmid c_t$. Seja k o menor índice tal que $p \nmid c_k$ (já vimos que $0 < k \leq t = n - s < n$). Como

$$a_k = b_0 c_k + b_1 c_{k-1} + \cdots$$

e $p \nmid b_0 c_k$ (mas divide todas as outras parcelas), então $p \nmid a_k$, uma contradição. ∎

O próximo resultado ajuda a encontrar as raízes em K de um polinómio com coeficientes em D.

Proposição 3.10. [das raízes fraccionárias] *Seja D um DFU, K o seu corpo de fracções e*

$$p(x) = a_n x^n + \cdots a_1 x + a_0 \in D[x].$$

Se $c/d \in K$ é uma raiz de $p(x)$ com $c, d \in D$ tais que $1 \in \mathrm{mdc}(c, d)$, então $c \mid a_0$ e $d \mid a_n$ em D. Em particular, se $c \in D$ é uma raiz de $p(x)$ então $c \mid a_0$.

Demonstração. Por hipótese

$$0 = p\left(\frac{c}{d}\right) = \frac{a_n c^n + a_{n-1} c^{n-1} d + \cdots + a_1 c d^{n-1} + a_0 d^n}{d^n}.$$

Portanto, $a_n c^n + a_{n-1} c^{n-1} d + \cdots + a_1 c d^{n-1} + a_0 d^n = 0$. Daqui podemos concluir que

$$a_n c^n + a_{n-1} c^{n-1} d + \cdots + a_1 c d^{n-1} = -a_0 d^n$$

e

$$-a_n c^n = a_{n-1} c^{n-1} d + \cdots + a_1 c d^{n-1} + a_0 d^n.$$

Da primeira identidade segue que $c \mid a_0 d^n$ e da segunda que $d \mid a_n c^n$. Como $1 \in \mathrm{mdc}(c, d)$, então $c \mid a_0$ e $d \mid a_n$ (Exercício 1.16). ∎

4. Domínios Euclidianos

As demonstrações de que $\mathbb{Z}$ e $C[x]$ (para qualquer corpo C) são DIP's (estudadas no ano passado) são formalmente muito parecidas e assentam no algoritmo da divisão. Isto sugere que possa haver uma classe genérica de anéis contida na classe dos DIP's onde aquelas demonstrações podem ser reformuladas, baseadas numa generalização do algoritmo da divisão. Essa classe é a classe dos domínios euclidianos.

Um domínio de integridade D diz-se um *domínio euclidiano* se for possível definir em D uma função $\delta\colon D \setminus \{0\} \to \mathbb{N}$ tal que

- para quaisquer $a, b \in D$ $(b \neq 0)$ existem $q, r \in D$ tais que $a = qb + r$ onde ou $r = 0$ ou $\delta(r) < \delta(b)$.

δ diz-se uma *função euclidiana* em D.

Os anéis $\mathbb{Z}$ com a função módulo e $C[x]$ (C corpo) com a função grau (em rigor, para que a função tenha valores positivos teremos que adicionar uma unidade ao grau) são domínios euclidianos. Observe que $\delta(a) = |a|$ não é uma função euclidiana em $\mathbb{Q}$. Qualquer corpo C é um domínio euclidiano, com função euclidiana δ definida por $\delta(x) = 1$ para todo o $x \in C \setminus \{0\}$.

Alguns autores acrescentam à definição de função euclidiana a condição

$$\delta(a) \leq \delta(ab) \text{ para quaisquer } a, b \in D \setminus \{0\} \tag{4.1.1}$$

mas isso é desnecessário pois as duas definições descrevem as mesmas classes de domínios. De facto:

Proposição 4.1. *Se D é um domínio euclidiano com função euclidiana δ então*

$$\widetilde{\delta}(a) = \min_{b \neq 0} \delta(ab)$$

define uma função euclidiana em D com as seguintes propriedades:

(1) $\widetilde{\delta}(a) \leq \widetilde{\delta}(ab)$ *para quaisquer a, b em $D \setminus \{0\}$.*

(2) $\widetilde{\delta}(1)$ *é o valor mínimo de δ em $D \setminus \{0\}$.*

(3) $\widetilde{\delta}(a) \leq \delta(a)$ *para qualquer a em $D \setminus \{0\}$.*

Demonstração. Começamos por demonstrar as propriedades (1)-(3) e deixamos para o fim a prova de que $\widetilde{\delta}$ é de facto uma função euclidiana em D.

(1) Sejam a, b em $D \setminus \{0\}$. Pela definição de $\widetilde{\delta}$, $\widetilde{\delta}(ab) = \delta(abc_0)$ para algum $c_0 \in D \setminus \{0\}$. Mas abc_0 é um múltiplo de a logo $\widetilde{\delta}(a) \leq \delta(abc_0) = \widetilde{\delta}(ab)$.

(2) Óbvio (da definição de $\widetilde{\delta}$).

(3) $\widetilde{\delta}(a) = \min_{b \neq 0} \delta(ab) \leq \delta(a \cdot 1) = \delta(a)$.

Mostremos agora que D admite um algoritmo da divisão relativamenta a $\widetilde{\delta}$. Sejam $a, b \in D$ com $b \neq 0$. Claro que $\widetilde{\delta}(b) = \delta(bc_0)$ para algum $c_0 \in D \setminus \{0\}$. Pelo algoritmo da divisão em (D, δ) para o par a, bc_0 existem $q, r \in D$ tais que $a = (bc_0)q_0 + r_0$ com $r_0 = 0$ ou $\delta(r_0) < \delta(bc_0)$. Basta agora tomar $q = c_0 q_0$ e $r = r_0$. De facto, $a = bq + r$, e $r = 0$ ou (usando a propriedade (3)) $\widetilde{\delta}(r) \leq \delta(r) < \delta(bc_0) = \widetilde{\delta}(b)$. ∎

Proposição 4.2. *Todo o domínio euclidiano é um DIP.*

Demonstração. Seja I um ideal arbitrário de um domínio euclidiano D. Se $I = \{0\}$, então $I = \langle 0 \rangle$ é um ideal principal. Podemos pois admitir que $I \neq \{0\}$. Nesse caso seja $N = \{\delta(a) \mid a \in I, a \neq 0\} \subseteq \mathbb{N}$. É claro que N é não vazio (pois $I \neq \{0\}$), pelo que tem um mínimo. Seja b um elemento de $I \setminus \{0\}$ onde esse mínimo é atingido. Provemos que $I = \langle b \rangle$. Como $b \in I$, é óbvio que $\langle b \rangle \subseteq I$. Por outro lado, se $a \in I$, usando a definição de domínio euclidiano, existem $q, r \in D$ tais que $a = qb + r$ com $r = 0$ ou $\delta(r) < \delta(b)$. Dado que I é um ideal, podemos concluir que $r = a - qb \in I$. Mas então $r = 0$ (se r fosse não nulo, teríamos $r \in I \setminus \{0\}$ com $\delta(r) < \delta(b)$, um absurdo). Assim, a é um múltiplo de b pelo que pertence ao ideal $\langle b \rangle$. ∎

Por outro lado, nem todo o DIP é um domínio euclidiano. O anel

$$\mathbb{Z}\Big[\frac{1 + i\sqrt{19}}{2}\Big]$$

é um exemplo.

Uma vez que o algoritmo de Euclides para a determinação do mdc em $\mathbb{Z}$ (ou em $C[x]$) depende apenas do algoritmo da divisão, é previsível que se possa generalizar a qualquer domínio euclidiano.

Proposição 4.3. [Algoritmo de Euclides] *Em qualquer domínio euclidiano D,* $\mathrm{mdc}(a, b) \neq \emptyset$ *para quaisquer $a, b \in D \setminus \{0\}$. Um elemento deste conjunto pode ser obtido dividindo a por b e, iterando, dividindo sucessivamente os sucessivos divisores pelos sucessivos restos, até que o resto seja zero. O último resto não nulo r_t será esse elemento (e, consequentemente,* $\mathrm{mdc}(a, b) = \{u\, r_t \mid u \in D^*\}$*).*

Demonstração. Como D é um DFU, $\text{mdc}(a,b) \neq \emptyset$ pela Proposição 2.3. Quanto ao algoritmo de cálculo de um elemento desse conjunto, ele termina pois cada divisão sucessiva origina um novo resto r_{t+1} com $\delta(r_{t+1}) < \delta(r_t)$ e estes valores são sempre não negativos. Resta-nos mostrar que o elemento encontrado pelo algoritmo é de facto um mdc de a e b. Faremos a demonstração por indução sobre $\delta(b)$.

Se $\delta(b) = 1$ então $b \mid a$ (pois $a = q_1 b + r_1$ com $r_1 = 0$ ou $\delta(r_1) < \delta(b) = 1$; como a última condição é impossível, então $r_1 = 0$). Portanto $a = q_1 b$ e é óbvio que $b \in \text{mdc}(a,b)$.

Suponhamos que o algoritmo funciona para qualquer b tal que $\delta(b) < n$. Consideremos então b com $\delta(b) = n$. Então existem $q_1, r_1 \in D$ tais que

$$a = q_1 b + r_1 \qquad (*)$$

com $r_1 = 0$ ou $\delta(r_1) < \delta(b) = n$. Se $r_1 = 0$ então $a = q_1 b$ e é óbvio que $b \in \text{mdc}(a,b)$. Caso contrário, podemos usar a hipótese de indução e ter a garantia de que usando o algoritmo para b e r_1 encontramos no final um elemento d em $\text{mdc}(b, r_1)$. Só precisamos de garantir que $d \in \text{mdc}(a,b)$. Em primeiro lugar, como $d \mid r_1$ e $d \mid b$ então, usando $(*)$, $d \mid a$. Por outro lado, se $c \mid a$ e $c \mid b$ então, novamente por $(*)$, $c \mid r_1$ e portanto $c \mid d$. ∎

Resumindo:

ALGORITMO DE EUCLIDES

Sejam $a, b \in D$, com $b \neq 0$.

- Se $b \mid a$, então $b \in \text{mdc}\,(a,b)$.
- Se $b \nmid a$, usamos a definição de domínio euclidiano repetidamente, do seguinte modo:

$$\begin{array}{ll} a = q_1 b + r_1 & 0 < \delta(r_1) < \delta(b) \\ b = q_2 r_1 + r_2 & 0 < \delta(r_2) < \delta(r_1) \\ r_1 = q_3 r_2 + r_3 & 0 < \delta(r_3) < \delta(r_2) \\ \quad\vdots & \quad\vdots \\ r_{t-2} = q_t r_{t-1} + r_t & 0 < \delta(r_t) < \delta(r_{t-1}) \\ r_{t-1} = q_{t+1} r_t. & \end{array}$$

  Como $\delta(b)$ é finito, o processo terá que parar ao cabo de um número finito de passos. Então $r_t \in \text{mdc}\,(a,b)$.

Exemplo. Calculemos $\mathrm{mdc}(114, 87)$ (em $\mathbb{Z}$) pelo método de Euclides das divisões sucessivas e apresentemos uma expressão desse mdc como combinação linear inteira $p \times 114 + q \times 87$ de 114 e 87 (ver Exercício 1.21):

$$114 = 1 \times 87 + 27, \quad 87 = 3 \times 27 + 6, \quad 27 = 4 \times 6 + \boxed{3}, \quad 6 = 2 \times \boxed{3}.$$

Portanto, $\mathrm{mdc}(114, 87) = \{3, -3\}$.

A partir da penúltima divisão, substituindo sucessivamente, obtemos:

$$\begin{aligned} 3 &= 27 - 4 \times 6 \\ &= 27 - 4 \times (87 - 3 \times 27) \\ &= 13 \times 27 - 4 \times 87 \\ &= 13 \times (114 - 1 \times 87) - 4 \times 87 \\ &= 13 \times 114 - 17 \times 87. \end{aligned}$$

Portanto, $p = 13$ e $q = -17$.

Alternativamente, podemos calcular p e q sem fazer as substituições sucessivas, observando que podemos representar uma divisão $a = qb + r$ na forma matricial

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r \end{pmatrix}.$$

Assim, as sucessivas divisões no método de Euclides dão-nos

$$\begin{aligned} \begin{pmatrix} 114 \\ 87 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 87 \\ 27 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 27 \\ 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 6 \\ 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 \\ 0 \end{pmatrix}. \end{aligned}$$

Mas

$$\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix},$$

como é fácil de verificar. Logo, fazendo o produto dos inversos pela ordem inversa, obtemos

$$\begin{aligned} \begin{pmatrix} 3 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 114 \\ 87 \end{pmatrix} \\ &= \begin{pmatrix} 13 & -17 \\ -29 & 38 \end{pmatrix} \begin{pmatrix} 114 \\ 87 \end{pmatrix}, \end{aligned}$$

o que mostra que $3 = 13 \times 114 - 17 \times 87$.

Proposição 4.4. *O anel dos inteiros de Gauss, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, é um domínio euclidiano, com*

$$\delta(a + bi) := |a + bi|^2 = a^2 + b^2.$$

Demonstração. Teremos que mostrar que para quaisquer $a+bi, c+di \in \mathbb{Z}[i]$ com $c + di \neq 0$, existem $q_1 + q_2 i$ e $r_1 + r_2 i$ em $\mathbb{Z}[i]$ tais que

$$a+bi = (c+di)(q_1+q_2i)+(r_1+r_2i) \quad \text{onde } r_1 = r_2 = 0 \text{ ou } r_1^2+r_2^2 < c^2+d^2. \quad (4.4.1)$$

Se tal for possível, teremos necessariamente (em $\mathbb{C}$) o seguinte:

$$\begin{aligned} r_1 + r_2 i &= (a + bi) - (c + di)(q_1 + q_2 i) \\ &= (c + di)\Big[\frac{a + bi}{c + di} - (q_1 + q_2 i)\Big]. \end{aligned}$$

Denotando $\frac{a+bi}{c+di} \in \mathbb{C}$ por $u + vi$ (note que $u, v \in \mathbb{Q}$) é claro que no caso em que $u, v \in \mathbb{Z}$ basta fazer $q_1 = u, q_2 = v$ e $r_1 + r_2 i = 0$. Caso contrário, como

$$\begin{aligned} r_1 + r_2 i &= (c + di)\Big[(u + vi) - (q_1 + q_2 i)\Big] \\ &= (c + di)\Big[(u - q_1) + (v - q_2)i\Big] \\ &= [c(u - q_1) - d(v - q_2)] + [c(v - q_2) + d(u - q_1)]i, \end{aligned}$$

então

$$\begin{aligned} r_1^2 + r_2^2 &= [c(u - q_1) - d(v - q_2)]^2 + [c(v - q_2) + d(u - q_1)]^2 \\ &= (c^2 + d^2)[(u - q_1)^2 + (v - q_2)^2], \end{aligned}$$

donde

$$r_1^2 + r_2^2 < c^2 + d^2 \Leftrightarrow \boxed{(u - q_1)^2 + (v - q_2)^2 < 1}$$

o que mostra que neste caso para satisfazer (4.4.1) basta encontrar inteiros q_1 e q_2 tais que $(u - q_1)^2 + (v - q_2)^2 < 1$. Será isto possível? Claro que sim: basta tomar para q_1 o inteiro mais próximo de u e para q_2 o inteiro mais próximo de v (de facto, nesse caso $(u - q_1)^2 + (v - q_2)^2 \leq \frac{1}{4} + \frac{1}{4} < 1$).

(Repare que esta não é a única solução, o que mostra que esta divisão euclidiana em $\mathbb{Z}[i]$ não tem necessariamente quociente e resto únicos.)

Depois de calculados q_1 e q_2 basta tomar $r_1 + r_2 i = (a + bi) - (c + di)(q_1 + q_2 i)$.

■

Resumindo:

ALGORITMO DA DIVISÃO em $\mathbb{Z}[i]$

Sejam $a+bi, c+di \in \mathbb{Z}[i]$, com $c+di \neq 0$.

- Calcule-se $u+vi = \dfrac{a+bi}{c+di}$ em $\mathbb{C}$.
- Se $u, v \in \mathbb{Z}$, faça-se $q_1 = u, q_2 = v$ e $r_1 = r_2 = 0$.
- Caso contrário, tome-se para q_1 um inteiro tal que

$$(u-q_1)^2 \leq \frac{1}{4}$$

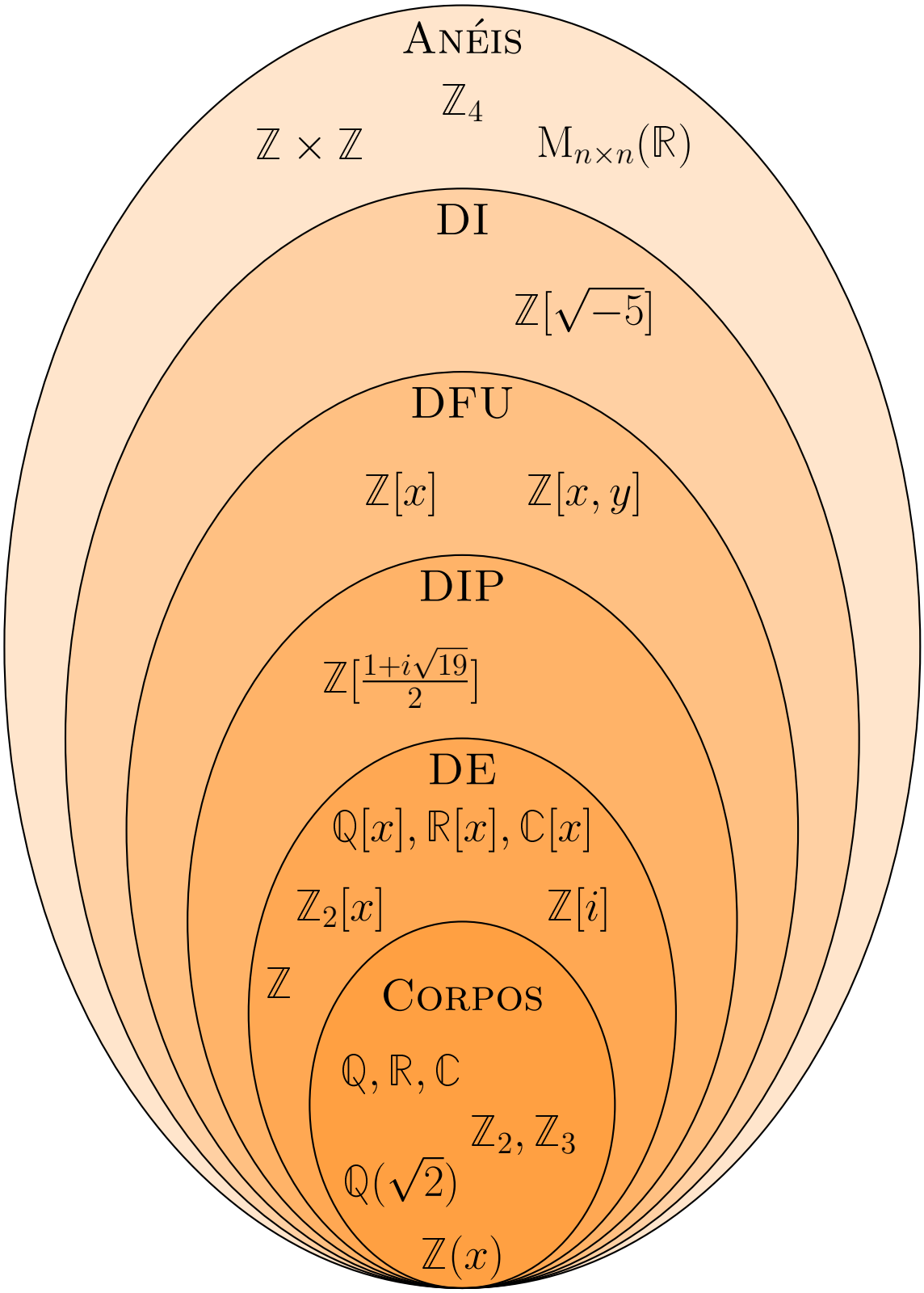
e para q_2 um inteiro tal que

$$(v-q_2)^2 \leq \frac{1}{4}.$$

O resto $r_1 + r_2 i$ é calculado pela fórmula

$$r_1 + r_2 i = (a+bi) - (c+di)(q_1 + q_2 i).$$

A figura seguinte resume as relações de inclusão entre as diversas classes de domínios de integridade estudadas neste capítulo.


ANÉIS
$\mathbb{Z}_4$
$\mathbb{Z} \times \mathbb{Z}$
$\mathrm{M}_{n\times n}(\mathbb{R})$
DI
$\mathbb{Z}[\sqrt{-5}]$
DFU
$\mathbb{Z}[x]$
$\mathbb{Z}[x, y]$
DIP
$\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$
DE
$\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$
$\mathbb{Z}_2[x]$
$\mathbb{Z}[i]$
$\mathbb{Z}$
CORPOS
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$
$\mathbb{Z}_2, \mathbb{Z}_3$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Z}(x)$

5. Teoremas do isomorfismo para anéis

Terminamos este primeiro capítulo com um tema diferente: vamos generalizar os teoremas de isomorfismos, estudados em Grupos, aos anéis, resultados de que necessitaremos ao longo do curso. É claro que tendo as demonstrações para os grupos na mão, estas são facilmente adaptáveis aos anéis (bastando verificar as propriedades relativamente à segunda operação dos anéis em causa); aqui (com o propósito de que o texto seja auto-contido) apresentaremos as demonstrações completas. Dado um homomorfismo de anéis $\phi\colon A \to B$, denotaremos o seu *núcleo* $\{a \in A \mid \phi(a) = 0\}$, que é um ideal de A, por $N(\phi)$.

Sejam A e B anéis e I um ideal de A. Investiguemos a relação entre os homomorfismos $\widetilde{\phi}\colon A/I \to B$ e os homomorfismos $\phi\colon A \to B$. Uma vez que a aplicação quociente usual

$$\begin{array}{rccc} \pi\colon & A & \to & A/I \\ & a & \mapsto & a+I \end{array}$$

é um homomorfismo de anéis, não é difícil provar o seguinte:

Lema 5.1. (1) *Seja $\widetilde{\phi}\colon A/I \to B$ um homomorfismo de anéis. Então a composição $\phi = \widetilde{\phi} \circ \pi\colon A \to B$ é um homomorfismo de anéis tal que $N(\phi) \supseteq I$.*

(2) *Reciprocamente, seja $\phi\colon A \to B$ um homomorfismo de anéis tal que $N(\phi) \supseteq I$. Então existe um (único) homomorfismo $\widetilde{\phi}\colon A/I \to B$ tal que $\widetilde{\phi} \circ \pi = \phi$.*

Demonstração. (1) É claro que ϕ é um homomorfismo de anéis pois é a composição de dois homomorfismos de anéis. Além disso, $N(\phi) \supseteq I$: se $a \in I$ então $a + I = I$ é o zero de A/I, e portanto $\phi(a) = \widetilde{\phi}(\pi(a)) = \widetilde{\phi}(a + I)$ é o zero de B.

(2) Se $\phi\colon A \to B$ é um homomorfismo de anéis tal que $N(\phi) \supseteq I$, então

$$b + I = a + I \Leftrightarrow b - a \in I \Rightarrow b - a \in N(\phi) \Leftrightarrow \phi(b) = \phi(a).$$

Isto garante que a correspondência $a + I \mapsto \phi(a)$ é independente da escolha do representante de $a + I$, ou seja, define uma aplicação $\widetilde{\phi}\colon A/I \to B$. É evidente que $\widetilde{\phi}$ é um homomorfismo, pois

$$\widetilde{\phi}(a+I) + \widetilde{\phi}(b+I) = \phi(a) + \phi(b) = \phi(a+b) = \widetilde{\phi}(a+b+I) = \widetilde{\phi}((a+I) + (b+I))$$

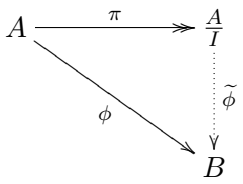
e

$$\widetilde{\phi}(a+I) \cdot \widetilde{\phi}(b+I) = \phi(a) \cdot \phi(b) = \phi(a \cdot b) = \widetilde{\phi}(ab+I) = \widetilde{\phi}((a+I) \cdot (b+I)).$$

■

Portanto, qualquer homomorfismo $\widetilde{\phi}\colon A/I \to B$ é da forma $\widetilde{\phi}(a+I) = \phi(a)$ para algum homomorfismo $\phi\colon A \to B$ definido no anel original A.

É habitual descrever a conclusão em (2), de modo mais abreviado, por um diagrama comutativo (onde a seta a ponteado serve para indicar que desejamos afirmar a existência do homomorfismo correspondente):



Observe ainda que o Lema nos diz com exactidão quais os homomorfismos $\phi\colon A \to B$ para os quais existe algum homomorfismo $\widetilde{\phi}\colon A/I \to B$ dado por $\widetilde{\phi}(a+I) = \phi(a)$ (ou seja, tal que $\widetilde{\phi} \circ \pi = \phi$):

Proposição 5.2. *Sejam A e B anéis, I um ideal de A e $\pi\colon A \to A/I$ o homomorfismo quociente usual.*

(1) *Os homomorfismos de anéis $\widetilde{\phi}\colon A/I \to B$ são as funções dadas por $\widetilde{\phi}(\pi(a)) = \phi(a)$, onde $\phi\colon A \to B$ é um qualquer homomorfismo de anéis com núcleo $N(\phi) \supseteq I$.*

(2) *Sendo $\phi\colon A \to B$ um homomorfismo de anéis com núcleo $N(\phi) \supseteq I$ e $\widetilde{\phi}\colon A/I \to B$ o correspondente homomorfismo de anéis dado por $\widetilde{\phi}(\pi(x)) = \phi(x)$, então*

$$N(\widetilde{\phi}) = \frac{N(\phi)}{I} = \pi(N(\phi))$$

e, em particular, $\widetilde{\phi}$ é injectiva se e só se $N(\phi) = I$.

Demonstração. (1) Imediato pelo Lema.

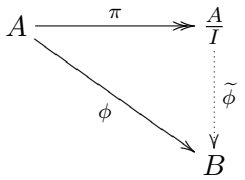
(2) Determinemos o núcleo de $\widetilde{\phi}$:

$$\begin{aligned} N(\widetilde{\phi}) &= \{a+I \mid \widetilde{\phi}(a+I) = 0\} = \{a+I \mid \phi(a) = 0\} \\ &= \{a+I \mid a \in N(\phi)\} = \pi(N(\phi)) = N(\phi)/I. \end{aligned}$$

É então evidente que $\widetilde{\phi}$ é injectiva se e só se $N(\widetilde{\phi}) = \{I\}$, o que ocorre se e só se $N(\phi) = I$. ∎

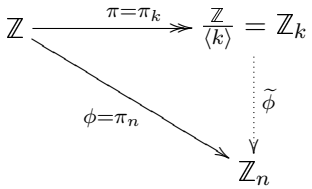
Portanto, para cada homomorfismo $\phi\colon A \to B$ tal que $N(\phi) \supseteq I$, existe um homomorfismo $\widetilde{\phi}$ (com núcleo igual a $N(\phi)/I$) que torna o seguinte diagrama

comutativo:



(5.2.1)

Exemplos. (1) Tomemos $A = \mathbb{Z}$, $B = \mathbb{Z}_n$ e $I = \langle k \rangle$. A aplicação $\phi = \pi_n \colon \mathbb{Z} \to \mathbb{Z}_n$ dada por $\phi(a) = a \,(\mathrm{mod}\, n)$ é um homomorfismo de anéis. Então, se $n \mid k$, é evidente que $N(\phi) \supseteq I$, pelo que a proposição anterior produz o diagrama comutativo

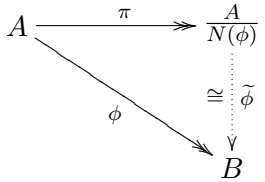


(2) Tomemos $A = \mathbb{Q}[x]$, $B = \mathbb{Q}$ e $\phi \colon \mathbb{Q}[x] \to \mathbb{Q}$ definido por $\phi(p(x)) = p(1)$. O núcleo de ϕ é (de acordo com o Teorema do Resto), $\langle x - 1 \rangle$. Sendo $I = \langle m(x) \rangle$ o ideal de $\mathbb{Q}[x]$ gerado pelo polinómio $m(x)$, a proposição anterior garante a existência de um homomorfismo de anéis $\widetilde{\phi} \colon \mathbb{Q}[x]/I \to \mathbb{Q}$, dado por $\widetilde{\phi}(p(x) + I) = p(1)$, desde que $(x - 1) \mid m(x)$ (isto é, $p(1) = 0$).

Quando o homomorfismo ϕ é sobrejectivo e I é o núcleo de ϕ, a proposição anterior reduz-se ao chamado Primeiro Teorema do Isomorfismo, um resultado central da Teoria dos Anéis (tal como a sua versão para grupos é um resultado central da Teoria dos Grupos), que usaremos repetidamente ao longo do curso:

Teorema 5.3. [Primeiro Teorema do Isomorfismo] *Seja $\phi \colon A \to B$ um homomorfismo sobrejectivo de anéis. Os anéis $A/N(\phi)$ e B são isomorfos. Em particular, existe um isomorfismo de anéis $\widetilde{\phi}$ tal que $\widetilde{\phi} \circ \pi = \phi$.* ∎

Este teorema exprime, em particular, a comutatividade do seguinte diagrama (onde a seta a ponteado significa a existência do homomorfismo correspondente, que é neste caso um *isomorfismo*):



(5.3.1)

Note que, mesmo quando ϕ não é sobrejectivo, o teorema se aplica automaticamente à imagem $B' = \phi(A)$.

Exemplos. (1) Supondo n e m naturais primos entre si, podemos mostrar que os anéis $\mathbb{Z}_{nm}$ e $\mathbb{Z}_n \oplus \mathbb{Z}_m$ são isomorfos. Para isso, definimos $\phi\colon \mathbb{Z} \to \mathbb{Z}_n \oplus \mathbb{Z}_m$ da forma "óbvia", tomando $\phi(a) = (\pi_n(a), \pi_m(a))$. O cálculo do núcleo de ϕ é simples:

$$a \in N(\phi) \Leftrightarrow \pi_n(a) = 0 \text{ e } \pi_m(a) = 0 \Leftrightarrow n \mid a \text{ e } m \mid a \Leftrightarrow nm \mid a.$$

Portanto, $N(\phi) = \langle nm \rangle$. Observe ainda que, como $\text{mdc}(n, m) = 1$, ϕ é sobrejectiva. Imediatamente, pelo Primeiro Teorema do Isomorfismo, obtemos um isomorfismo $\widetilde{\phi}\colon \mathbb{Z}/\langle nm \rangle = \mathbb{Z}_{nm} \to \mathbb{Z}_n \oplus \mathbb{Z}_m$, dado por $\widetilde{\phi}(\pi_{nm}(x)) = (\pi_n(x), \pi_m(x))$. Em conclusão, $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ sempre que $\text{mdc}(n, m) = 1$.

(2) Seja $\alpha \in \mathbb{C}$ um elemento algébrico sobre $\mathbb{Q}$, $\alpha \notin \mathbb{Q}$, e $m(x)$ o seu polinómio mínimo. Recorde que a aplicação $\phi\colon \mathbb{Q}[x] \to \mathbb{C}$ definida por $\phi(p(x)) = p(\alpha)$ é um homomorfismo de anéis com núcleo $N(\phi) = \langle m(x) \rangle$. Além disso, $\phi(\mathbb{Q}[x]) = \mathbb{Q}[\alpha]$. Logo, o Primeiro Teorema do Isomorfismo diz-nos que

$$\frac{\mathbb{Q}[x]}{\langle m(x) \rangle} \cong \mathbb{Q}[\alpha].$$

Por outro lado, $m(x)$ é irredutível, pelo que $\mathbb{Q}[x]/\langle m(x) \rangle$ é um corpo, e portanto

$$\frac{\mathbb{Q}[x]}{\langle m(x) \rangle} \cong \mathbb{Q}[\alpha] = \mathbb{Q}(\alpha).$$

O Primeiro Teorema do Isomorfismo pode ser aplicado para esclarecer a natureza do anel $B + I/I$ quando I e B são subanéis de A, sendo I um ideal.

Teorema 5.4. [Segundo Teorema do Isomorfismo] *Seja A um anel, I um ideal de A e B um subanel de A. Então $B + I$ é um subanel de A, I é um ideal de $B + I$, $B \cap I$ é um ideal de B e existe um isomorfismo de anéis*

$$\frac{B + I}{I} \cong \frac{B}{B \cap I}.$$

Demonstração. É fácil de verificar que se I é um ideal de A e B um subanel de A, então $B + I$ é igualmente um subanel de A, I é um ideal de $B + I$ e $B \cap I$ é um ideal de B (verifique!).

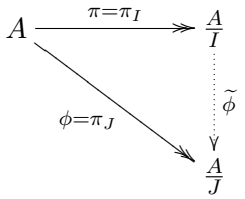
Consideremos a aplicação canónica $\pi\colon A \to A/I$ restrita a B, ou seja, a função $\phi\colon B \to A/I$ definida por $\phi(b) = \pi(b) = b + I$ para qualquer $b \in B$. É um exercício simples verificar que ϕ é um homomorfismo de anéis com núcleo $N(\phi) = \{b \in B \mid b \in I\} = B \cap I$. Por outro lado, $\phi(B)$ é um subanel de A/I, ou seja, $\phi(B) = K/I$ onde K é um subanel de A que contém necessariamente B e I, donde $B + I \subseteq K$. Mas para qualquer $k \in K$ existe $b \in B$ tal que $\phi(b) = k + I$, isto é, $b + I = k + I$;

portanto, existe $x := k-b \in I$ tal que $k = b+x$. Logo $K = B+I$. Então, aplicando o Teorema do Isomorfismo ao homomorfismo sobrejectivo $\phi\colon B \to \phi(B) = K/I$, obtemos um isomorfismo

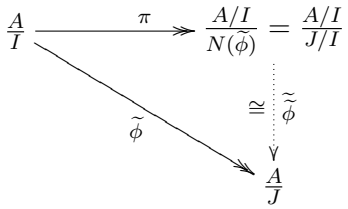
$$\frac{B}{N(\phi)} = \frac{B}{B \cap I} \xrightarrow{\ \widetilde{\phi}\ } \frac{K}{I} = \frac{B+I}{I}$$

■

Finalmente, podemos usar ainda o Primeiro Teorema do Isomorfismo para estudar os anéis quociente formados a partir de anéis quociente de A ("quocientes de quocientes de anéis"). Com efeito, seja A um anel e I e J ideais de A com $I \subseteq J$. Sejam $\pi_J\colon A \to A/J$ e $\pi_I\colon A \to A/I$ os respectivos homomorfismos quociente. Note que $N(\pi_J) = J \supseteq I = N(\pi_I)$. Pelo Lema 5.1(2), dados $\phi = \pi_J$ (que é sobrejectivo) e $\pi = \pi_I$, existe um homomorfismo $\widetilde{\phi}\colon A/I \to A/J$ tal que o seguinte diagrama é comutativo:



O homomorfismo $\widetilde{\phi}$ é claramente sobrejectivo (porque π_J o é). Além disso, pela Proposição 5.2, sabemos que $N(\widetilde{\phi}) = J/I$. Aplicando o Primeiro Teorema do Isomorfismo ao homomorfismo $\widetilde{\phi}$, obtemos imediatamente um isomomorfismo $\widetilde{\widetilde{\phi}}$ tal que o diagrama



comuta. Portanto:

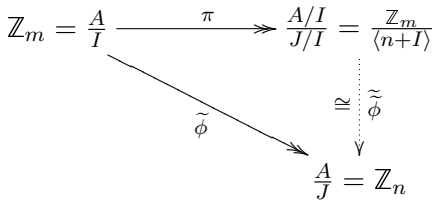
Teorema 5.5. [Terceiro Teorema do Isomorfismo] *Seja A um anel, I e J ideais de A com $I \subseteq J$. Então I é um ideal de J, J/I é um ideal de A/I e temos o isomorfismo de anéis*

$$\frac{A/I}{J/I} \cong \frac{A}{J}.$$

■

(Isto mostra que os quocientes de quocientes de A são isomorfos a quocientes de A.)

Exemplo. Com $A = \mathbb{Z}$, suponhamos que $n \mid m$. Consideremos $I = \langle m \rangle$ e $J = \langle n \rangle$. Neste caso $A/I = \mathbb{Z}_m$, $A/J = \mathbb{Z}_n$ e $J/I = \langle n + I \rangle \subseteq \mathbb{Z}_m$. Então, pelo Terceiro Teorema do Isomorfismo, $\mathbb{Z}_m / \langle n + I \rangle \cong \mathbb{Z}_n$:



Em particular, os anéis quociente formados a partir dos anéis $\mathbb{Z}_m$ são anéis $\mathbb{Z}_n$.

Exercícios

1.1. Mostre que num domínio de integridade D:

(a) $\langle a\rangle \subseteq \langle b\rangle$ sse $b \mid a$.

(b) $\langle a\rangle = \langle b\rangle$ sse $a \sim b$.

(c) $\langle a\rangle = D$ sse $a \in D^*$.

(d) $D[x]^* = D^*$.

1.2. Mostre que num domínio de integridade D:

(a) $u \in D^*$ sse $u \mid d$ para todo o $d \in D$.

(b) Qualquer associado de uma unidade é uma unidade.

(c) Qualquer associado de um elemento irredutível é irredutível.

1.3. Demonstre a Proposição 1.2.

1.4. Verifique que um anel (comutativo com identidade) A é um domínio de integridade se e só $ab \in \langle 0\rangle \Rightarrow a \in \langle 0\rangle$ ou $b \in \langle 0\rangle$.

1.5. (a) Determine as unidades do *anel dos inteiros de Gauss* $\mathbb{Z}[i]$.

(b) Verifique que $1 \pm i$ são elementos irredutíveis de $\mathbb{Z}[i]$. Observe que $2 \in \mathbb{Z}[i]$ não é irredutível em $\mathbb{Z}[i]$ apesar de o ser em $\mathbb{Z}$.

1.6. Seja D um domínio de integridade onde é possível definir uma função $N\colon D \to \mathbb{N}_0$ (chamada *norma*) com as seguintes propriedades:

(1) $N(a) = 0$ sse $a = 0$.

(2) $N(a) = 1$ sse $a \in D^*$.

(3) $N(ab) = N(a)N(b)$ para quaisquer $a, b \in D \setminus \{0\}$.

Mostre que todo o elemento de $D \setminus D^*$ não nulo admite uma factorização como produto de elementos irredutíveis.

1.7. Considere o anel $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ onde $d \neq 0, 1$ é *livre de quadrados*, isto é, para qualquer primo $p \in \mathbb{Z}$, $p^2 \nmid d$.

(a) Mostre que $a + b\sqrt{d} = a' + b'\sqrt{d}$ se e só se $a = a'$ e $b = b'$.

(b) Prove que a aplicação $N\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{N}_0$ definida por $N(a + b\sqrt{d}) = |a^2 - db^2|$ é uma norma (recorde o exercício anterior).

(c) Conclua que em $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[i\sqrt{5}]$ os elementos 3 e $2 \pm \sqrt{-5}$ são irredutíveis.

(d) Mostre que em $\mathbb{Z}[\sqrt{-5}]$ todos os elementos admitem factorizações em irredutíveis, mas a decomposição não é, em geral, única.

1.8. Seja C um corpo. Verdadeiro ou falso?

(a) Se $a, b, c \in C^*$ então $a \in \text{mdc}(b, c)$.

(b) C é um DFU.

1.9. Seja D um DIP e $a, b \in D$. Prove que:

(a) $d \in \text{mdc}(a, b)$ se e só se $\langle d\rangle = \langle a, b\rangle = \langle a\rangle + \langle b\rangle$.

(b) $m \in \text{mmc}(a, b)$ se e só se $\langle m\rangle = \langle a\rangle \cap \langle b\rangle$.

(c) Se $d \in \text{mdc}(a, b)$ então existem $p, q \in D$ tais que $d = pa + qb$ (*Relação de Bézout*).

1.10. Seja D um domínio de integridade e $a_1, \ldots, a_n \in D$.

(a) Defina $\text{mdc}(a_1, \ldots, a_n)$ e $\text{mmc}(a_1, \ldots, a_n)$.

(b) Mostre que se $d' \in \text{mdc}(a_1, \ldots, a_{n-1})$ e $d \in \text{mdc}(d', a_n)$ então $d \in \text{mdc}(a_1, \ldots, a_n)$.

(c) Enuncie e demonstre o resultado análogo para mmc's.

1.11. Seja A um anel comutativo com identidade e seja $\mathcal{S}$ o conjunto das sequências infinitas $(a_n)_{n\in\mathbb{N}_0}$ de elementos de A. Defina $+$ e $\cdot$ em $\mathcal{S}$ por

$$(a_n)_{n\in\mathbb{N}_0} + (b_n)_{n\in\mathbb{N}_0} = (a_n + b_n)_{n\in\mathbb{N}_0} \quad \text{e} \quad (a_n)_{n\in\mathbb{N}_0} \cdot (b_n)_{n\in\mathbb{N}_0} = (c_n)_{n\in\mathbb{N}_0}$$

onde $c_n = a_0b_n + a_1b_{n-1} + \cdots + a_nb_0$ para $n = 0, 1, 2, \ldots$. Mostre que:

(a) $(\mathcal{S}, +, \cdot)$ é um anel comutativo com identidade.

(b) $(a_n)_{n\in\mathbb{N}_0} \in \mathcal{S}^*$ se e só se $a_0 \in A^*$.

(c) Se A é um corpo então $\mathcal{S}$ é um domínio de ideais principais.

1.12. Seja D um DFU e C o seu corpo de fracções. Mostre que é possível escrever qualquer elemento de C como a/b com $a, b \in D$ elementos *coprimos* (ou *primos entre si*, isto é, tais que $\text{mdc}(a, b) = D^*$).

1.13. Seja $A = \{p(x) \in \mathbb{R}[x] \colon p(x) \text{ não tem monómio de grau } 1\}$.

(a) Verifique que A é um anel (subanel de $\mathbb{R}[x]$).

(b) Verifique que todos os polinómios de grau 2 ou 3 são irredutíveis em A.

(c) Verifique que os polinómios $x^2(x^2 + x)^2$ e $x^3(x^2 + x)$ não têm mdc em A. Que pode dizer do mmc?

(d) Prove que todo o elemento de A se factoriza como produto de irredutíveis, mas esta factorização nem sempre é única.

(**Observação:** este exercício mostra que um subanel de um DFU não é necessariamente um DFU.)

1.14. Seja D um domínio de integridade.

(a) Verifique que se $p(x) \in D[x]$ é primitivo e $q(x) \mid p(x)$, com $\mathrm{gr}(q(x)) \geq 1$, então $q(x)$ é primitivo.

(b) Mostre que todo o polinómio primitivo de $D[x]$ admite factorizações em irredutíveis em $D[x]$.

1.15. Seja D um DFU, $a \in D$, com $a \neq 0$, e $p(x), q(x) \in D[x]$ tais que $q(x) \mid ap(x)$ e $q(x)$ é primitivo. Prove que $q(x) \mid p(x)$.

1.16. Seja D um DFU. Mostre que, para quaisquer $a, b, c \in D$, se $1 \in \mathrm{mdc}(a, b)$ e $a \mid bc$ então $a \mid c$.

1.17. Seja D um domínio euclidiano com função euclidiana δ.

(a) Prove que $a \in D$ é uma unidade se $\delta(a)$ for um mínimo do conjunto $\{\delta(x) \mid x \in D, x \neq 0\}$. Mostre que se $\delta(a) \leq \delta(ab)$ para quaisquer $a, b \in D \setminus \{0\}$, então a implicação recíproca também é verdadeira.

(b) Revisite o Exercício 1.5, resolvendo-o agora usando o facto de $\mathbb{Z}[i]$ ser um domínio euclidiano.

1.18. Calcule em $\mathbb{Z}[i]$:

(a) $\mathrm{mdc}(2, 3 + i)$.

(b) $\langle 2 \rangle + \langle 3 + i \rangle$.

(c) $\langle 2 \rangle \cap \langle 3 + i \rangle$.

(d) $\mathrm{mdc}(9 - 5i, -9 + 13i)$.

1.19. Seja D um domínio euclidiano com função euclidiana δ (satisfazendo $\delta(a) \leq \delta(ab)$ para quaisquer $a, b \in D \setminus \{0\}$). Seja $I \neq \{0\}$ um ideal de D. Prove que se existir $a \in I$ tal que $\delta(a) = \delta(1)$, então $I = D$.

1.20. Seja D um domínio euclidiano com função euclidiana δ (satisfazendo $\delta(a) \leq \delta(ab)$ para quaisquer $a, b \in D \setminus \{0\}$). Mostre que se n é um inteiro tal que $\delta(1) + n > 0$, então a função $\delta' \colon D \setminus \{0\} \to \mathbb{N}$ definida por $\delta'(a) = \delta(a) + n$ é também uma função euclidiana em D.

1.21. Seja D um domínio euclidiano. Mostre, usando o método das divisões sucessivas (Euclides), que dados $a, b \in D$ (não simultaneamente nulos), existem $p, q \in D$ tais que $pa + qb \in \text{mdc}(a, b)$.

1.22. Seja A um anel comutativo com 1. Mostre que as seguintes condições são equivalentes:

(i) A é um corpo.

(ii) $A[x]$ é um domínio euclidiano.

(iii) $A[x]$ é um DIP.

1.23. Seja $\phi\colon A \to B$ um homomorfismo de anéis. Mostre que:

(a) $\phi(0) = 0$ e $\phi(-a) = -\phi(a)$.

(b) $N(\phi)$ é um ideal de A.

(c) ϕ é injectiva sse $N(\phi) = \{0\}$.

(d) $\phi(A)$ é um subanel de B.

1.24. Seja A um anel. Sendo I um ideal de A e B um subanel de A, mostre que:

(a) $B + I$ é um subanel de A e I é um ideal de $B + I$.

(b) A correspondência $a \mapsto a + I$ define um homomorfismo sobrejectivo $\pi\colon A \to A/I$ com núcleo I.

(c) A correspondência $b \mapsto b + I$ define um homomorfismo $B \to A/I$ com núcleo $B \cap I$ e imagem $(B + I)/I$.

1.25. (a) Sejam A um DIP, B um domínio de integridade e $\phi\colon A \to B$ um homomorfismo sobrejectivo de anéis com $N(\phi) \neq \{0\}$.

(i) Prove que $N(\phi)$ é um ideal maximal de A.

(ii) Conclua que B é um corpo.

(b) Sendo D um domínio de integridade, mostre que $D[x]$ é um DIP se e só se D é um corpo.

1.26. Prove que os anéis $\mathbb{Z}_n \oplus \mathbb{Z}_m$ e $\mathbb{Z}_{nm}$ são isomorfos se $\text{mdc}(n, m) = 1$. Mais geralmente, mostre que $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_d \oplus \mathbb{Z}_k$ para $d = \text{mdc}(n, m)$ e $k = \text{mmc}(n, m)$.

Soluções de exercícios seleccionados

1.11. (a) É fácil verificar que $\mathcal{S}$ é um anel comutativo com 1. A sequência $(1, 0, 0, \dots)$ é a identidade de $\mathcal{S}$.

(b) Consideremos $(a_n)_{n\in\mathbb{N}_0} \in \mathcal{S}$. Suponhamos que (a_n) é uma unidade. Então existe uma sequência $(b_n)_{n\in\mathbb{N}_0}$ tal que $(a_n)\cdot(b_n) = 1$. Logo, $a_0b_0 = 1$ e portanto a_0 é uma unidade de A.

Reciprocamente, suponhamos que $a_0 \in A^*$ e consideremos a sequência (b_n) definida por

$$b_0 = a_0^{-1}, \quad b_1 = -a_0^{-1}(a_1a_0^{-1}), \quad \dots, \quad b_k = -a_0^{-1}(a_1b_{k-1}+\cdots+a_kb_0), \quad k \geq 2.$$

É claro que $a_0b_0 = 1$, $a_0b_1 + a_1b_0 = a_0(-a_0^{-1}(a_1a_0^{-1})) + a_1a_0^{-1} = 0, \dots,$ $a_kb_0+a_{k-1}b_1+\cdots+a_0b_k = a_kb_0+a_{k-1}b_1+\cdots+a_0(-a_0^{-1}(a_1b_{k-1}+\cdots+a_kb_0)) =$ 0. Então $(a_n)\cdot(b_n) = 1$, o que prova que (a_n) é uma unidade de $\mathcal{S}$.

(c) Suponhamos que A é um corpo. Seja I um ideal de $\mathcal{S}$. Se $I = \{0\}$, então I é um ideal principal. Suponhamos então que $I \neq \{0\}$. Seja (a_n) um elemento não nulo de I. Definimos a *ordem* $\mathrm{o}(a_n)$ de uma sequência não nula (a_n) de $\mathcal{S}$ como sendo o primeiro inteiro não negativo tal que $a_n \neq 0$ e $a_i = 0$ para $i < n$. Existe uma sequência (a_n) tal que $\mathrm{o}(a_n) = \kappa \leq \mathrm{o}(b_n)$ para qualquer $(b_n) \in I$. Seja (c_n) a sequência tal que $c_i = a_{\kappa+i}$ para todo o $i \geq 0$. Então $(c_n)^{-1}$ existe e $(c_n)^{-1}\cdot(a_n) = (d_n) \in I$. Além disso, $d_\kappa = 1$ e $d_i = 0$ para todo o $i \neq \kappa$. Provemos que $I = \langle(d_n)\rangle$. Claramente $\langle(d_n)\rangle \subseteq I$. Seja $(u_n) \in I$ com ordem m. Então $m \geq \kappa$. Seja $(r_n) \in \mathcal{S}$ tal que $r_{m-\kappa+i} = u_{m+i}$ para qualquer $i \geq 0$ e $r_i = 0$ para qualquer $i \leq m - \kappa$. É fácil verificar que $(u_n) = (r_n)\cdot(d_n) \in \langle(d_n)\rangle$. Logo, $I = \langle(d_n)\rangle$.

1.14. (a) Seja $d \in D$ um divisor de $q(x)$ de grau zero. Como $d \mid p(x)$ então d é uma unidade.

(b) Seja $p(x)$ um polinómio primitivo de $D[x]$. Faremos a demonstração por indução sobre o grau $n \geq 1$ de $p(x)$:

Se $n = 1$ então $p(x)$ não admite factorizações próprias e, sendo primitivo, é irredutível e está provado.

Tomemos $p(x)$ de grau n e suponhamos, como hipótese de indução, que o resultado é válido para todos os polinómios de grau $< n$. Se $p(x)$ admitir uma factorização própria então $p(x) = q(x)r(x)$ com $\mathrm{gr}(q(x)), \mathrm{gr}(r(x)) < n$ e, pela hipótese de indução, ambos são factorizáveis em polinómios irredutíveis, o que nos dá uma factorização de $p(x)$ em irredutíveis. No caso em que $p(x)$

não admite factorizações próprias, como é primitivo, então é irredutível e está provado.

1.16. Seja $p_1p_2\cdots p_n$ a factorização de a em primos. Para cada $i = 1, 2, \ldots, n$, $p_i \mid bc$ logo $p_i \mid b$ ou $p_i \mid c$. Mas como a e b são primos entre si e $p_i \mid a$ (para qualquer i), se p_i dividisse b para algum i teríamos $p_i \mid 1$, isto é, $p_i \in D^*$, um absurdo. Logo nenhum p_i divide b pelo que $p_i \mid c$ para $i = 1, 2, \ldots, n$ e portanto $a \mid c$.

1.17. (b) $\mathbb{Z}[i]$ é um domínio euclidiano com função euclidiana

$$\delta(a + ib) = |a + ib|^2 = a^2 + b^2$$

que satisfaz a propriedade $\delta(xy) = \delta(x)\delta(y)$. As unidades de $\mathbb{Z}[i]$ são ± 1 e $\pm i$, pois $\delta(a + ib) = 1$ se e só se $a + ib \in \{\pm 1, \pm i\}$.

Se $1 \pm i = (a + ib)(c + id)$ então $\delta(1 \pm i) = \delta(a + ib)\delta(c + id)$, isto é, $2 = \delta(a + ib)\delta(c + id)$. Como 2 é primo em $\mathbb{Z}$, então $\delta(a + ib) = 1$ (ou seja, $a + ib$ é uma unidade) ou $\delta(c + id) = 1$ (ou seja, $c + id$ é uma unidade).

Claro que 2 é irredutível em $\mathbb{Z}$ porque é primo. Mas em $\mathbb{Z}[i]$, $2 = (1+i)(1-i)$, logo é redutível em $\mathbb{Z}[i]$.

1.18. (a) Pelo exercício anterior, $2 = (1 + i)(1 - i)$ é a factorização (única) de 2 em irredutíveis (primos). Como $3 + i = (1 + i)(2 - i)$ é a factorização de $3 + i$ em primos (de facto, $2 - i$ também é irredutível pois $\delta(2 + i) = 5$ é um inteiro primo), então $1 + i \in \text{mdc}(2, 3 + i)$. Logo,

$$\text{mdc}(2, 3 + i) = \{1 + i, -1 - i, -1 + i, 1 - i\}.$$

(b) Como em qualquer DIP, $\langle a\rangle + \langle b\rangle = \langle \text{mdc}(a, b)\rangle$, então $\langle 2\rangle + \langle 3 + i\rangle = \langle \text{mdc}(2, 3 + i)\rangle = \langle 1 + i\rangle = \{(a + ib)(1 + i) \mid a, b \in \mathbb{Z}\} = \{(a - b) + i(a + b) \mid a, b \in \mathbb{Z}\}$.

(c) Como em qualquer DIP, $\langle a\rangle \cap \langle b\rangle = \langle \text{mmc}(a, b)\rangle$, então $\langle 2\rangle \cap \langle 3 + i\rangle = \langle \text{mmc}(2, 3+i)\rangle = \langle (1+i)(1-i)(2-i)\rangle = \langle 4-2i\rangle = \{(4a+2b)+i(-2a+4b) \mid a, b \in \mathbb{Z}\}$.

1.22. (i)⇒(ii): Sendo A um corpo, dados $a(x), b(x) \in A[x]$ com $b(x) \neq 0$ sabemos que existem $q(x), r(x) \in A[x]$ tais que $a(x) = q(x)b(x) + r(x)$ com $r(x) = 0$ ou $gr(r(x)) < gr(b(x))$ (equivalentemente, $gr(r(x)) + 1 < gr(b(x)) + 1$). Portanto, fazendo $\delta(p(x)) = gr(p(x)) + 1$, temos claramente uma função euclidiana em $A[x]$.

(ii)⇒(iii): Basta aplicar a Proposição 4.2 que assegura que todo o domínio euclidiano é um DIP.

(iii)⇒(i): Seja $a \neq 0$ em A. Teremos que mostrar que a é invertível. Para isso consideremos o ideal $I = \langle a, x\rangle$ de $A[x]$, que é principal. Portanto, existe $p(x) \in A[x]$ tal que $I = \langle p(x)\rangle$. Como $a, x \in I$ então existem $a(x)$ e $b(x)$ em $A[x]$ tais que $a = a(x)p(x)$ e $x = b(x)p(x)$. Consequentemente, $gr(p(x)) = 0$ (observe que $A[x]$ sendo um domínio de integridade, implica necessariamente que A o seja), isto é, $p(x) = d \in A$. Então $x = b(x)d$, o que implica que $cd = 1$ para algum $c \in A$. Portanto d é uma unidade e $I = \langle d\rangle = A[x]$. Daqui podemos concluir que $1 \in I$, isto é, $1 = ap_1(x) + xp_2(x)$ para algum par $p_1(x), p_2(x)$ em $A[x]$. Isto implica $1 = ab$ para algum $b \in A$ e a é assim invertível.

1.26. A primeira parte do exercício foi provada no exemplo da página 26. Quanto à segunda parte:

Sejam

$$n = p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t} \quad \text{e} \quad m = p_1^{m_1}p_2^{m_2}\cdots p_t^{m_t}$$

as decomposições primas de n e m ($n_i, m_i \in \mathbb{N}_0$). Então

$$d = p_1^{\min(n_1,m_1)}p_2^{\min(n_2,m_2)}\cdots p_t^{\min(n_t,m_t)}$$

e

$$k = p_1^{\max(n_1,m_1)}p_2^{\max(n_2,m_2)}\cdots p_t^{\max(n_t,m_t)}.$$

Pelo resultado da primeira parte podemos concluir que

$$\mathbb{Z}_d \cong \mathbb{Z}_{p_1^{\min(n_1,m_1)}} \oplus \mathbb{Z}_{p_2^{\min(n_2,m_2)}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\min(n_t,m_t)}}$$

e

$$\mathbb{Z}_k \cong \mathbb{Z}_{p_1^{\max(n_1,m_1)}} \oplus \mathbb{Z}_{p_2^{\max(n_2,m_2)}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\max(n_t,m_t)}}.$$

Logo $\mathbb{Z}_d \oplus \mathbb{Z}_k \cong \mathbb{Z}_n \oplus \mathbb{Z}_m$ pois $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$ e $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{m_t}}$.