Conteúdo

Prefácio

A divisão tradicional da Matemática nas três áreas fundamentais, Álgebra, Análise e Geometria/Topologia, subsiste até aos dias de hoje. Embora a Matemática contemporânea cada vez menos possa ser caracterizada desta forma, quer pelas novas áreas que não encaixam nesta divisão tradicional, quer pela importância crescente de áreas multidisciplinares, é nossa opinião que a formação do aluno deve ter por base uma forte preparação em cada uma destas três áreas fundamentais. O programa de estudos de qualquer licenciatura em Matemática bem estruturada, seja ela virada para o ensino, para a investigação ou para a indústria, deve pois incluir, pelo menos, três semestres de preparação em cada uma destas áreas. O presente texto pretende ser um livro de apoio às disciplinas de formação de base em uma delas: a Álgebra.

Antes de mais, deve-se observar que, hoje em dia, é aceite por toda a comunidade matemática a formulação conceptual, axiomática, da Álgebra. Mais do que isso, a metodologia algébrica é uma das ferramentas essenciais da Matemática. Por outro lado, depois de na segunda metade do século XX se ter assistido a uma abstracção sem paralelo na Matemática, mais recentemente, verificou-se um retorno a uma tradição nunca perdida: os desafios criados por problemas concretos, por vezes de natureza elementar, mas cuja solução requer métodos de extrema complexidade. O ensino da Álgebra deve, quanto a nós, reflectir este binómio abstracto-concreto. Como perguntava o grande matemático contemporâneo Vladimir Arnol'd, de que serve a um estudante saber o que é um anel local e as suas propriedades, se desconhecer o exemplo do anel das séries de potências?

Este texto é, pois, uma iniciação ao estudo sistemático da Álgebra assente nestes princípios. Ao longo do texto, apresentam-se as estruturas algébricas elementares e estudam-se as suas propriedades. A introdução de uma nova estrutura algébrica é sempre precedida de exemplos e/ou problemas que a motivam, partindo-se daí para a sua definição axiomática. O nível de abstracção é progressivo em cada secção, em cada capítulo e em cada novo capítulo. Para além das preocupações pedagógicas, o leitor deve estar consciente de que assim sucede com a formação de qualquer matemático, e foi assim que aconteceu ao longo dos tempos com a própria Matemática: as funções foram introduzidas e estudadas, antes de qualquer definição axiomá-

tica em termos de pares ordenados; os grupos e os anéis foram introduzidos, estudados e investigados, muito antes de terem sido conceptualizados; as semelhanças de construções entre as várias estruturas algébricas foram notadas e utilizadas, muito antes de o conceito abstracto de categoria ter sido descoberto.

Este livro nasceu de notas compiladas pelos autores durante a leccionação das disciplinas de Álgebra I e II da Licenciatura em Matemática Aplicada e Computação, do Instituto Superior Técnico (IST). O material aqui exposto inclui todos os tópicos cobertos por essas disciplinas e ainda alguns tópicos adicionais que, principalmente por limitações de tempo, não eram normalmente cobertos. A escolha de tópicos pretende ser representativa, de forma a constituir o essencial de uma formação básica em Álgebra. Para além disso, dentro dos princípios acima enunciados, pretendemos estabelecer pontes com outras áreas da Matemática. É frequente um capítulo incluir uma secção de "aplicações", que pressupõe conhecimentos de outras áreas da Matemática por parte do leitor. Como já referimos acima, os autores não vêem o estudo da Álgebra de forma independente do estudo das outras áreas da Matemática, e estas secções, embora não prejudicando a dependência lógica entre os capítulos, devem ser entendidas como parte integrante do texto, em vez de meras curiosidades. Nunca é de mais referir que os exercícios propostos são igualmente parte integrante do texto. Na Matemática, como em tudo, aprende-se experimentando e enfrentando problemas. Por isso mesmo, as demonstrações de alguns dos resultados enunciados no texto são propostas como exercício.

Existem certamente outras possibilidades de ordenação da matéria para além da sugerida pela sequência dos vários capítulos. Um exemplo de programa alternativo possível para um curso de três semestres é o seguinte:

- *Semestre 1:* noções elementares (Capítulo 1), inteiros (Capítulo 2), aritmética mod p e anéis de polinómios (Capítulo 3, excepto duas últimas secções), quocientes e isomorfismo (primeiras 5 secções do Capítulo 4);

- *Semestre 2:* grupos finitos e sua estrutura (Capítulo 5) e Teoria de Galois (Capítulo 7);

- *Semestre 3:* módulos (Capítulo 6 e duas últimas secções do Capítulo 3 e do Capítulo 4) e Álgebra Comutativa (Capítulo 8);

Deve notar-se que o livro assume conhecimentos elementares de Álgebra Linear.

Os autores gostavam, em primeiro lugar, de agradecer a todos os alunos que ao longo de mais de dez anos utilizaram as notas que deram origem a este livro. A interacção com estes alunos, o que aprendemos com eles, foi o principal motor de aperfeiçoamento das notas que deram origem a este

texto. Foi com grande satisfação que pudemos testemunhar como alguns desses alunos vieram a singrar como matemáticos profissionais. Gostávamos também de agradecer a todos os colegas do Departamento de Matemática do Instituto Superior Técnico, o seu apoio e o excelente ambiente de trabalho, que possibilitou o desenvolvimento deste texto. Uma menção especial a Maria Vaz Pinto, colega que também leccionou Álgebra no IST com recurso a este texto, e aos dois *referees* anónimos, que nos transmitiram inúmeros comentários e sugestões que ajudaram a melhorar significativamente o texto.

Lisboa, Janeiro de 2003

Rui Loja Fernandes
Manuel Ricou

Departamento de Matemática
Instituto Superior Técnico
1096 Lisboa Codex
PORTUGAL

rfern@math.ist.utl.pt
mricou@math.ist.utl.pt

Capítulo 1

Noções Básicas da Álgebra

1.1 Introdução

A Álgebra é hoje, como sempre foi, o estudo das operações, regras de cálculo, e procedimentos para a solução de equações. A origem do próprio termo "Álgebra" é especialmente elucidativa. De acordo com B. L. van der Waerden, um distinto algebrista contemporâneo, este termo foi utilizado pela primeira vez por um autor árabe do século *IX*, no título[1] de um tratado apresentando conhecimentos matemáticos de utilidade "prática". A palavra árabe *al-jabr* é utilizada nesse tratado para designar dois procedimentos fundamentais para a resolução de equações:

1. a soma da mesma quantidade positiva a ambos os membros de uma equação, para eliminar quantidades negativas, e

2. o produto da mesma quantidade positiva por ambos os membros de uma equação, para eliminar fracções.

O tratado referido descreve conhecimentos de natureza diversa, incluindo não só a resolução de equações do 1º e 2º graus, como o estudo de problemas geométricos, astronómicos, comerciais, o cálculo de calendários, etc. Com o tempo, o termo *al-jabr*, ou *Álgebra*, passou a ser utilizado para representar em geral conhecimentos sobre operações e equações numéricas.

Hoje em dia, é comum distinguir a chamada *Álgebra Clássica* da *Álgebra Moderna*. Estas expressões não são particularmente felizes, e parafraseando o matemático italiano F. Severi, sem dúvida que a *Álgebra Moderna* de hoje se tornará na *Álgebra Clássica* de amanhã. Na realidade, se compararmos, por exemplo, a Álgebra do século *XX* com a Álgebra do século *XVI*, e eliminarmos diferenças que são visíveis em qualquer outro ramo científico (rigor, formalismo, notações, pura quantidade de conhecimentos), a principal

[1] A tradução para inglês do título completo é "The Compendious Book on Calculation by al-jabr and al-muqabala".

diferença que nos resta é a da generalidade com que os problemas algébricos são hoje enunciados e estudados.

Mesmo esta tendência para a generalização do âmbito da Álgebra sempre esteve presente no passado. Inicialmente, reflectiu-se apenas nas sucessivas generalizações do conceito de número (de natural, para racional positivo, para mais recentemente incluir números negativos, complexos e irracionais). No século XIX, reconheceu-se que muitas das ideias ditas "algébricas" se aplicavam igualmente a objectos que não são números, como por exemplo vectores, matrizes e transformações.

À lenta expansão do domínio da Álgebra sucedeu-se uma brusca explosão, quando se compreendeu que é possível estudar propriedades de qualquer operação algébrica sem especificar a natureza dos objectos sobre os quais essa operação actua, nem descrever como o resultado da operação deve ser calculado. Na realidade, este estudo faz-se simplesmente postulando (*i.e.*, tomando como hipótese) um determinado conjunto de propriedades algébricas básicas que a operação é suposta verificar, como por exemplo a comutatividade e a associatividade. A Álgebra tornou-se finalmente *axiomática* (se bem que com um atraso de mais de 2000 anos em relação à Geometria). Esta foi a inovação mais significativa introduzida no século passado, e justifica o uso do nome "Álgebra Geral", quando nos referimos à Álgebra dos nossos dias.

A axiomatização da Álgebra exigiu antes do mais a definição de *estruturas algébricas abstractas*. No caso mais simples, uma estrutura algébrica abstracta é formada por um conjunto não-vazio X, dito o *suporte* da estrutura, e uma *operação binária* em X, que não é mais do que uma função $\mu : X \times X \to X$. Diferentes conjuntos de suposições, ou axiomas, exigidos a esta operação, conduzem à definição de diferentes estruturas algébricas abstractas. Estas definições não incluem qualquer hipótese sobre a natureza dos elementos do conjunto X, nem sobre os procedimentos a seguir para calcular os valores da função μ.

Certas convenções simples são universalmente seguidas. Se $\mu : X \times X \to X$ for uma operação binária em X, é comum escolher um símbolo como por exemplo "$+$" ou "$*$" para a representar, escrevendo "$x + y$" ou "$x * y$" em vez de "$\mu(x, y)$". Frequentemente indicamos a operação por simples justaposição, *i.e.*, escrevemos "xy" em vez de "$\mu(x, y)$". A utilização de notações como "$x + y$" e "xy" não significa de modo algum que os símbolos designem as usuais operações sobre números. A este respeito, a única convenção geralmente aceite é que o símbolo "$+$" só é utilizado para designar operações *comutativas*, *i.e.*, operações tais que $\mu(x, y) = \mu(y, x)$. Para simplificar a nossa terminologia, sempre que lidarmos com uma operação comutativa representada pelo símbolo "$+$" diremos que usamos *notação aditiva*. Em todos os outros casos, a notação diz-se *multiplicativa*. Usamos sistematicamente

as convenções habituais sobre o uso de parênteses, ou seja,

$$x * (y * z) = \mu(x, \mu(y, z)),$$

em geral diferente de

$$(x * y) * z = \mu(\mu(x, y), z).$$

Quando impomos poucos axiomas à estrutura algébrica em estudo, obtemos resultados de grande generalidade, porque aplicáveis a muitas estruturas algébricas concretas. Naturalmente, os resultados muito gerais tendem a ser pouco interessantes, precisamente porque se baseiam num número reduzido de hipóteses. Se escolhermos à partida um conjunto de axiomas mais rico, podemos em princípio derivar resultados mais interessantes, mas naturalmente menos gerais, porque menos estruturas algébricas concretas verificam os axiomas de partida. Consequentemente, um dos problemas principais da Álgebra Geral é exactamente o de determinar conjuntos de axiomas (*i.e.*, definições de estruturas algébricas abstractas) que são suficientemente gerais para incluir muitos exemplos concretos úteis e, ao mesmo tempo, suficientemente ricos para permitir obter resultados interessantes.

Ilustramos estas observações com alguns exemplos muito simples. Sem qualquer hipótese adicional sobre a operação $*$, podemos introduzir a noção de *elemento neutro*, sugerida pelo comportamento dos inteiros 0 e 1, respectivamente em relação à soma e produto usuais.

Definição 1.1.1. Seja $*$ uma operação binária no conjunto X. O elemento $e \in X$ diz-se ELEMENTO NEUTRO para esta operação se e só se $x*e = e*x = x$ para qualquer $x \in X$.

Podemos provar imediatamente um resultado válido para *qualquer* operação binária.

Proposição 1.1.2. *Toda a operação binária tem no máximo um elemento neutro.*

Demonstração. Suponha-se que e e $\tilde{e}$ são ambos elementos neutros para a operação $*$. Temos então

$$\begin{aligned} e * \tilde{e} &= \tilde{e} \qquad \text{(porque } e \text{ é elemento neutro)}, \\ e * \tilde{e} &= e \qquad \text{(porque } \tilde{e} \text{ é elemento neutro)}. \end{aligned}$$

Concluímos portanto que $e = \tilde{e}$. □

É comum usar os termos "zero" e "um" (este último mais frequentemente chamado "identidade") para designar o elemento neutro da operação $*$, quando este elemento neutro existe. Convém evidentemente usar estes termos de forma consistente, *i.e.*, o termo "zero" (e mesmo o símbolo "0")

usa-se em notação aditiva, e o termo "identidade" (e possivelmente o símbolo "1", ou "I") usa-se em notação multiplicativa.

Quando a operação $*$ tem identidade e, é possível introduzir a noção de elementos *inversos*. A definição é a seguinte:

Definição 1.1.3. O elemento $x \in X$ diz-se INVERTÍVEL se e só se existe $y \in X$ tal que

$$x * y = y * x = e.$$

Neste caso, y diz-se INVERSO de x.

Mais uma vez, por uma questão de familiaridade, quando usamos notação aditiva, os inversos dizem-se *simétricos*. Note que y é inverso de x se e só se x é inverso de y, *i.e.*, a relação "é inverso de" é simétrica. Quando temos apenas $x * y = e$, dizemos que y é inverso de x *à direita*, e x é inverso de y *à esquerda*. É claro que y é inverso de x se e só se y é inverso à direita e à esquerda de x. No entanto, um inverso à direita não é necessariamente inverso à esquerda. Apesar disso, e se a operação $*$ é associativa, podemos ainda provar o seguinte resultado.

Proposição 1.1.4. *Seja $*$ uma operação associativa em X. Se $x \in X$ tem inverso à direita y, e inverso à esquerda z, então $y = z$ e x é invertível.*

Demonstração. Supomos que $y, z \in A$ são tais que $x * y = z * x = e$. Temos então

$$\begin{aligned}
x * y = e &\Rightarrow z * (x * y) = z && (\text{porque } z * e = z),\\
&\Rightarrow (z * x) * y = z && (\text{porque a operação é associativa}),\\
&\Rightarrow e * y = z && (\text{porque } z * x = e),\\
&\Rightarrow y = z && (\text{porque } e * y = y).
\end{aligned}$$

□

A utilidade de resultados como o anterior é o de serem aplicáveis a qualquer estrutura algébrica concreta que satisfaça as hipóteses que utilizámos (existência de identidade, e associatividade da operação). Essas hipóteses são precisamente as usadas na definição da estrutura algébrica que agora introduzimos:

Definição 1.1.5. A estrutura algébrica $(X, *)$ diz-se um MONÓIDE se satisfaz as seguintes propriedades:

(i) A operação $*$ tem identidade e em X.

(ii) A operação é associativa, *i.e.*, $(x * y) * z = x * (y * z)$, para quaisquer $x, y, z \in X$.

Se a operação é *comutativa*, *i.e.*, se $x * y = y * x$ para quaisquer $x, y \in X$, dizemos que o monóide é *abeliano*[2]. Se a operação é comutativa e usamos notação aditiva, dizemos que o monóide é *aditivo*.

A Proposição 1.1.4 permite concluir que:

Proposição 1.1.6. *Se $(X, *)$ é um monóide (com identidade e), e $x \in X$ é invertível, existe um* único *elemento $y \in X$ tal que $x * y = y * x = e$.*

Algumas das operações mais conhecidas fornecem exemplos de monóides.

Exemplos 1.1.7.

1. *O conjunto das matrizes $n \times n$ com entradas reais com o produto usual de matrizes é um monóide. Portanto, se A, B, C são matrizes $n \times n$, I é a matriz identidade, e $AB = CA = I$, então $B = C$ e a matriz A é invertível.*

2. *O conjunto $\mathbb{R}^{\mathbb{R}}$ das funções* [3] *$f : \mathbb{R} \to \mathbb{R}$ com o "produto de composição", definido por $(f \circ g)(x) = f(g(x))$ é um monóide. A identidade é a função $I : \mathbb{R} \to \mathbb{R}$ dada por $I(x) = x$. Portanto, se existem funções $g, h : \mathbb{R} \to \mathbb{R}$ tais que $f \circ g = h \circ f = I$, então $g = h$ e f é invertível (*i.e.*, é uma bijecção).*

3. *O conjunto dos reais com a soma habitual é um monóide (aditivo). Neste caso, qualquer elemento é invertível.*

4. *O conjunto dos reais positivos com o produto usual é um monóide. Mais uma vez a operação é comutativa, e todo o real não nulo é invertível.*

Se o elemento x do monóide $(X, *)$ é invertível, vimos que o *inverso* de x é único. Tal como fazemos para os números, usamos em notação multiplicativa a designação "x^{-1}" para representar este inverso, e em notação aditiva a designação "$-x$". Com estas convenções, certas regras algébricas básicas sobre simétricos e inversos aplicam-se na realidade em qualquer monóide. Deixamos a demonstração dos seguintes resultados como exercício:

Proposição 1.1.8. *Se $(X, *)$ é um monóide, e $x, y \in X$ são invertíveis, então x^{-1} e y^{-1} são invertíveis e temos*

$$(x^{-1})^{-1} = x, \ e \ (xy)^{-1} = y^{-1}x^{-1}.$$

Para um monóide aditivo, temos

$$-(-x) = x, \ e \ -(x + y) = (-x) + (-y).$$

Exercícios.

[2] Em honra de Niels Henrik Abel (1802-1829), matemático norueguês considerado um dos fundadores da Álgebra Moderna.

[3] Se X e Y são conjuntos, Y^X é o conjunto de todas as funções $f : X \to Y$ (Ver a definição A.2.4 no Apêndice).

1. Seja $X = \{x, y\}$ um conjunto com dois elementos. Quantas operações binárias existem em X? Quantas dessas operações são (i) comutativas, (ii) associativas, (iii) têm identidade?

2. Quantas operações binárias existem num conjunto com 10 elementos?

3. Em $(\mathbb{Z}, -)$ existe identidade? Existem inversos? A operação é associativa?

4. Seja $\mathbb{R}^{\mathbb{R}}$ o conjunto de funções referido no exemplo 1.1.7.2, e suponha que $f \in \mathbb{R}^{\mathbb{R}}$.

   (a) Mostre que existe $g \in \mathbb{R}^{\mathbb{R}}$ tal que $f \circ g = I$ se e só se f é sobrejectiva.

   (b) Mostre que existe $g \in \mathbb{R}^{\mathbb{R}}$ tal que $g \circ f = I$ se e só se f é injectiva.

   (c) Se $f \circ g = f \circ h = I$, é sempre verdade que $g = h$?

5. Prove a Proposição 1.1.8.

6. Seja $*$ uma operação binária em X, e $x, y \in X$. Se $n \in \mathbb{N}$ é um número natural, definimos a *potência* x^n por indução como se segue: $x^1 = x$ e, para $n \geq 1$, $x^{n+1} = x^n * x$. Suponha que $*$ é associativa, e prove:

   (a) $x^n * x^m = x^{n+m}$, e $(x^n)^m = x^{nm}$, para quaisquer $n, m \in \mathbb{N}$.

   (b) $x^n * y^n = (x * y)^n$, para qualquer $n \in N$ se $x * y = y * x$.

   Como se podem exprimir estes resultados em notação aditiva?

7. Suponha que $(X, *)$ é um monóide com identidade e, e $x \in X$ é invertível. Neste caso, definimos para $n \in \mathbb{N}$ qualquer, $x^{-n} = (x^{-1})^n$, $x^0 = e$. Prove que as identidades do problema anterior são válidas para quaisquer $n, m \in \mathbb{Z}$.

1.2 Grupos

Os exemplos discutidos na secção anterior mostram que num monóide arbitrário nem todos os elementos são necessariamente invertíveis. Os monóides em que *todos* os elementos são invertíveis correspondem à estrutura abstracta mais central da Álgebra.

Definição 1.2.1. O monóide $(G, *)$ diz-se um GRUPO se e só se todos os elementos de G são invertíveis. O grupo diz-se ABELIANO se a sua operação é comutativa.

Os seguintes exemplos dão uma ideia por pálida que seja da generalidade deste conceito.

Exemplos 1.2.2.

1. $(\mathbb{R}, +)$ *é um grupo abeliano.*

2. $(\mathbb{R}^+, \cdot)$ *é igualmente um grupo abeliano.*

3. $(\mathbb{R}^n, +)$*, onde a soma é a* soma vectorial*, é um grupo abeliano.*

4. *O conjunto das matrizes $n \times n$ invertíveis (não-singulares) de entradas reais é um grupo não-abeliano com o produto usual de matrizes (o chamado* Grupo Geral Linear*, por vezes designado por $GL(n, \mathbb{R})$).*

5. *Os complexos $\mathbb{C}$ com $|z| = 1$ (o* círculo unitário*, usualmente designado por $\mathbb{S}^1$) com o produto complexo formam um grupo abeliano.*

6. *Os complexos $\{1, -1, i, -i\}$ com o produto complexo formam um grupo finito abeliano.*

7. *As funções $f : \mathbb{R} \to \mathbb{R}$ formam um grupo abeliano com a soma usual de funções. Podemos também considerar classes especiais de funções, tais como as funções contínuas, as funções diferenciáveis ou, ainda, as funções integráveis, e todas elas formam grupos abelianos.*

8. *Se X é um conjunto qualquer e $(G, +)$ é um grupo abeliano, então as funções $f : X \to G$ formam um grupo abeliano, com a operação "$+$" definida por*

$$(f + g)(x) = f(x) + g(x), \quad \forall x \in X.$$

(Nesta última expressão o símbolo "$+$" tem dois significados distintos!)

9. *Mais geralmente, se X é um conjunto e $(G, *)$ é um grupo, então as funções $f : X \to G$ formam um grupo, com a operação "$*$" definida por*

$$(f * g)(x) = f(x) * g(x), \quad \forall x \in X.$$

(Mais uma vez, nesta expressão o símbolo "$*$" tem dois significados distintos.)

O quarto exemplo ilustra um facto absolutamente geral: os elementos invertíveis de qualquer monóide formam *sempre* um grupo.

Proposição 1.2.3. *Seja $(X, *)$ um monóide, e G o conjunto dos elementos invertíveis em X. Então G é fechado em relação a $*$, e $(G, *)$ é um grupo.*

Demonstração. A identidade e de X é invertível, e $e^{-1} = e$, porque $e * e = e$. Portanto, G não é vazio, e contém a identidade de X.

A Proposição 1.1.8 mostra que

$$x \in G \Longrightarrow x^{-1} \in G \qquad (\text{porque } (x^{-1})^{-1} = x),$$

e, ainda, que

$$x, y \in G \Longrightarrow x * y \in G \qquad (\text{porque } (x * y)^{-1} = y^{-1} * x^{-1}).$$

Como a operação $*$ é associativa (no monóide original), $(G, *)$ é um grupo. □

Não é objectivo desta secção discutir a teoria dos grupos em profundidade. Referimos aqui apenas alguns resultados elementares que nos serão úteis no estudo de muitas outras estruturas algébricas.

Proposição 1.2.4. *Se $(G,*)$ é um grupo (com elemento neutro e), temos*[4]*:*

*(i) Se $g,g',h \in G$ e $g*h = g'*h$ ou $h*g = h*g'$, então $g = g'$ (*LEIS DO CORTE*);*

(ii) Em particular, se $g*g = g$ então $g = e$;

(iii) A equação $g*x = h$ (respectivamente, $x*g = h$) tem como solução única $x = g^{-1}*h$ (respectivamente, $x = h*g^{-1}$).

Demonstração. Temos:

$$\begin{aligned} g*h = g'*h &\Longrightarrow (g*h)*h^{-1} = (g'*h)*h^{-1} && \text{(porque } h \text{ é invertível)},\\ &\Longrightarrow g*(h*h^{-1}) = g'*(h*h^{-1}) && \text{(por associatividade)},\\ &\Longrightarrow g*e = g'*e && \text{(porque } h*h^{-1} = e\text{)},\\ &\Longrightarrow g = g' && \text{(porque } e \text{ é identidade)}. \end{aligned}$$

A demonstração para $h*g = h*g'$ é análoga, logo (i) verifica-se. Por outro lado,

$$\begin{aligned} g*g = g &\Longrightarrow g*g = g*e && \text{(porque } g*e = g\text{)},\\ &\Longrightarrow g = e && \text{(pelo resultado anterior)}. \end{aligned}$$

e (ii) é verdadeira. A demonstração de (iii) fica como exercício. □

Se $(G,*)$ é um grupo e $H \subset G$ é um conjunto *não-vazio*, é possível que H seja fechado em relação à operação $*$, *i.e.*, é possível que $h*h' \in H$, sempre que $h,h' \in H$. Neste caso, a operação $*$ é uma operação binária em H, e podemos investigar em que condições é que $(H,*)$ é um grupo, caso em que $(H,*)$ se diz SUBGRUPO de $(G,*)$.

O resultado seguinte fornece um critério simples para decidir se um dado subconjunto H de um grupo G é um subgrupo.

Proposição 1.2.5. *Se $(G,*)$ é um grupo (com elemento neutro e), e $H \subset G$ é não-vazio, então $(H,*)$ é um subgrupo de $(G,*)$ se e só se $h*h'^{-1} \in H$, para quaisquer $h,h' \in H$.*

Demonstração. Supomos primeiro que $(H,*)$ é um grupo. Temos a provar que $h*h'^{-1} \in H$, para quaisquer $h,h' \in H$. Neste caso, H tem um elemento neutro $\tilde{e}$, que naturalmente satisfaz $\tilde{e}*\tilde{e} = \tilde{e}$. Concluímos da Proposição

[4]Note que os resultados neste teorema são em última análise variantes "sofisticadas" da operação de *al-jabr* mencionada na introdução.

1.2.4 (ii) que $\tilde{e} = e$, e portanto H contém a identidade de G. Sendo $h \in H$, considere-se a equação $h * x = e$. De acordo com a Proposição 1.2.4 (iii), esta equação tem solução única em H, que é igualmente solução da mesma equação em G, e portanto só pode ser $x = h^{-1}$ (o inverso de h no grupo original G). Portanto, se $h \in H$, temos $h^{-1} \in H$. Finalmente, se $h, h' \in H$, temos $h'^{-1} \in H$, como acabámos de ver, e como H é fechado em relação ao produto, temos $h * h'^{-1} \in H$, como queríamos demonstrar.

Supomos agora que $h * h'^{-1} \in H$, para qualquer $h, h' \in H$. Temos a provar que $(H, *)$ é um grupo. Como H é não-vazio, tomamos $h \in H$, e observamos que $h * h^{-1} = e \in H$, donde H contém a identidade de G. Analogamente, se $h \in H$, temos $e * h^{-1} = h^{-1} \in H$, e portanto H contém os inversos (em G) de todos os seus elementos. Finalmente, e para provar que H é fechado em relação à operação $*$, observamos que, se $h, h' \in H$, temos como já vimos que $h'^{-1} \in H$, donde $h * (h'^{-1})^{-1} = h * h' \in H$ (a operação $*$ é associativa em H porque já o era em G). □

Exemplos 1.2.6.

1. *Considere-se o grupo $(\mathbb{R}, +)$ e o conjunto dos inteiros $\mathbb{Z} \subset \mathbb{R}$. Como o conjunto dos inteiros é não-vazio e a diferença de dois inteiros é ainda um inteiro, concluímos que $(\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{R}, +)$. (Observe que em notação aditiva a condição "$h * h'^{-1} \in H$" escreve-se "$h + (-h') \in H$" ou ainda "$h - h' \in H$"[5]).*

2. *No mesmo grupo $(\mathbb{R}, +)$, consideramos o conjunto dos naturais $\mathbb{N} \subset \mathbb{R}$. Como a diferença de dois naturais não é necessariamente um natural, $(\mathbb{N}, +)$ não é um subgrupo de $(\mathbb{R}, +)$. Note que apesar disso a soma de dois naturais é um natural, e portanto a soma é uma operação binária no conjunto dos naturais.*

Sejam $(G, *)$ e $(H, \cdot)$ dois grupos, e considere o produto cartesiano

$$G \times H = \{(g, h) : h \in G, h \in H\}.$$

Definimos em $G \times H$ a operação binária

$$(g, h) \circ (g', h') = (g * g', h \cdot h'). \tag{1.2.1}$$

Deixamos como exercício verificar que esta estrutura algébrica é um grupo, dito PRODUTO DIRECTO dos grupos G e H. Note que G e H podem ser vistos como subgrupos de $G \times H$ se os identificarmos com

$$G \times \{e\} = \{(g, e) : g \in G\} \quad \text{e} \quad \{e\} \times H = \{(e, h) : h \in H\}.$$

Se G e H são grupos abelianos e usamos a notação aditiva, então vamos escrever $G \oplus H$ em vez de $G \times H$, e designamos este grupo por SOMA DIRECTA de G e H.

[5] A diferença $h - h'$ define-se em qualquer grupo aditivo por $h - h' = h + (-h')$.

Naturalmente que a noção de produto directo ou soma directa de grupos se aplica sem modificações significativas a um número arbitrário mas finito de grupos[6]. Por exemplo, se G, H, e K são grupos, o produto directo $G \times H \times K$ pode ser definido por $G \times H \times K = (G \times H) \times K$. Mais geralmente, dados grupos $G_1, G_2, \cdots, G_n$, temos:

$$\prod_{k=1}^{1} G_k = G_1, \text{ e } \prod_{k=1}^{n} G_k = \left(\prod_{k=1}^{n-1} G_k\right) \times G_n.$$

Exemplos 1.2.7.

1. *Considere-se o grupo* $(\mathbb{Z}, +)$. *Podemos fazer a soma directa deste grupo com ele próprio um número arbitrário mas finito de vezes, e o grupo resultante designa-se usualmente por*

$$\bigoplus_{k=1}^{n} \mathbb{Z}.$$

Este grupo, que como veremos no Capítulo 4 é o chamado grupo abeliano livre em n símbolos*, é bem entendido um subgrupo do grupo* $(\mathbb{R}^n, +)$.

Exercícios.

1. Prove que os conjuntos $G = \{0, 1\}$ e $H = \{1, -1\}$ com as operações dadas pelas tabuadas seguintes são grupos.[7]

+	0	1
0	0	1
1	1	0

×	1	-1
1	1	-1
-1	-1	1

2. Repita a questão anterior para os conjuntos $G = \{0, 1, 2\}$ e $H = \{1, x, x^2\}$, com as operações dadas pelas tabuadas. [8]

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	1	x	x^2
1	1	x	x^2
x	x	x^2	1
x^2	x^2	1	x

3. Conclua a demonstração da Proposição 1.2.4 (iii).

4. Verifique que a lei do corte não é em geral válida em monóides.

[6] Uma outra distinção entre soma e produto directo será explicitada mais tarde, quando considerarmos o caso da soma ou produto directos de uma família *infinita* de grupos.

[7] O grupo da esquerda designa-se usualmente por $(\mathbb{Z}_2, +)$, por razões que esclareceremos mais adiante. O grupo da direita é formado pelas *raízes quadradas da unidade*.

[8] O grupo da esquerda designa-se por $(\mathbb{Z}_3, +)$. O grupo da direita é formado pelas raízes *cúbicas* da unidade. Podemos por exemplo supor que x é o número complexo $e^{\frac{2\pi}{3}i}$.

5. Sendo $(G, *)$ um grupo, mostre que a função definida em G por $f(x) = x^{-1}$ é uma bijecção de G em G.

6. Exprima as Proposições 1.2.4 e 1.2.5 em notação aditiva.

7. Sendo $(G, *)$ um grupo, seja $C(G) = \{x \in G : g * x = x * g, \forall g \in G\}$. Mostre que $(C(G), *)$ é um subgrupo de G (dito o CENTRO de G). Determine o centro de $G = GL(n, \mathbb{R})$.

8. Sendo $(G, *)$ um grupo, e H_1, H_2 subgrupos de G, mostre que $H_1 \cap H_2$ é um subgrupo de G.

9. Prove que o grupo $(G, *)$ é abeliano se e só se $(g * g')^2 = g^2 * g'^2$, para quaisquer $g, g' \in G$.

10. Seja $*$ uma operação binária associativa no conjunto G, que satisfaz:

    (i) Existe $e \in G$ tal que, para qualquer $g \in G$, $g*e = g$ (*identidade à direita*).

    (ii) Para qualquer $g \in G$ existe $g' \in G$ tal que $g * g' = e$ (*inversos à direita*).

    Mostre que:

    (a) $(G, *)$ é um grupo.
    (SUGESTÃO: prove primeiro que $g * g = g \Rightarrow g = e$).

    (b) Seja G a classe das funções sobrejectivas $f : X \to X$, $*$ a operação de composição (com X um conjunto fixo arbitrário). Por que razão este exemplo não contradiz (a)?

11. Seja $*$ uma operação binária associativa no conjunto não-vazio G, que satisfaz:

    (i) A equação $g * x = h$ tem solução em G para quaisquer $g, h \in G$.

    (ii) A equação $x * g = h$ tem solução em G para quaisquer $g, h \in G$.

    Prove que $(G, *)$ é um grupo.

12. Sejam $(G, *)$ e $(H, \cdot)$ dois grupos. Mostre que a operação binária em $G \times H$ definida por (1.2.1) é uma estrutura de grupo. Verifique que o produto directo $(\mathbb{R}, +) \times (\mathbb{R}, +)$ é precisamente $(\mathbb{R}^2, +)$.

13. Determine o produto directo dos grupos descritos nos Exercícios 1 e 2.

14. Considere o grupo $(\mathbb{Z}_4, +)$, que é dado pela tabuada seguinte:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(a) Determine todos os seus subgrupos.

(b) Considere o grupo com suporte $H = \{1, -1, i, -i\} \subset \mathbb{C}$ e o produto complexo. Existe alguma bijecção $f : G \to H$ tal que $f(x+y) = f(x)f(y)$, para quaisquer $x, y \in G$? Se tal acontecer, quantas existem?

1.3 Permutações

As funções bijectivas $f : X \to X$ com a operação de composição formam um grupo S_X, dito o GRUPO SIMÉTRICO em X. As bijecções de X em X dizem-se PERMUTAÇÕES de X, especialmente quando X é um conjunto finito. Estudaremos aqui os grupos de permutações nos conjuntos $\{1, 2, 3, \ldots, n\}$, usualmente designados por S_n. Um argumento simples de contagem mostra que S_n é um grupo finito com $n!$ elementos ($n!$ designa o *factorial* de n, *i.e.*, o produto dos primeiros n inteiros).

Exemplos 1.3.1.

1. *O grupo S_2 tem apenas dois elementos, I e ϕ, onde I é a identidade no conjunto $\{1, 2\}$, e ϕ "troca" 1 com 2, (*i.e., *$\phi(1) = 2$ e $\phi(2) = 1$).*

2. *A função $\delta : \{1, 2, 3\} \to \{1, 2, 3\}$ definida por $\delta(1) = 2$, $\delta(2) = 3$, e $\delta(3) = 1$ é uma das seis permutações em S_3.*

3. *Mais geralmente, em S_n temos a permutação $\pi : S_n \to S_n$ que permuta ciclicamente todos os elementos: $\pi(i) = i + 1$ $(i = 1, \ldots, n-1)$ e $\pi(n) = 1$.*

É comum representar uma permutação π de S_n por uma matriz de duas linhas, indicando na primeira linha a variável x e na segunda linha os valores $\pi(x)$. No caso de S_3, os seus elementos podem ser representados por

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \delta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Não é difícil calcular todos os possíveis produtos destas permutações indicados na tabuada seguinte:

	I	α	β	γ	δ	ε
I	I	α	β	γ	δ	ε
α	α	I	δ	ε	β	γ
β	β	ε	I	δ	γ	α
γ	γ	δ	ε	I	α	β
δ	δ	γ	α	β	ε	I
ε	ε	β	γ	α	I	δ

Dada uma permutação π de X e um elemento $x \in X$, o conjunto dos elementos que se obtém de x por aplicação repetida de π designa-se por $\mathcal{O}_x$ e diz-se uma ÓRBITA da permutação π. Temos portanto $\mathcal{O}_x = \{x, \pi(x), \pi(\pi(x)), \dots\}$.

Exemplos 1.3.2.

1. *No caso de S_3, temos*
   - *I: as órbitas são $\mathcal{O}_1 = \{1\}$, $\mathcal{O}_2 = \{2\}$ e $\mathcal{O}_3 = \{3\}$;*
   - *α: as órbitas são $\mathcal{O}_1 = \{1\}$, $\mathcal{O}_2 = \mathcal{O}_3 = \{2, 3\}$;*
   - *ε: a única órbita é $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$.*

   A estrutura das órbitas de β e γ é semelhante à de α (é capaz de dizer precisamente como são?), enquanto que ε, tal como δ, possui uma só órbita (qual?).

2. *A permutação $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ de S_4 tem as órbitas $\mathcal{O}_1 = \mathcal{O}_2 = \{1, 2\}$ e $\mathcal{O}_3 = \mathcal{O}_4 = \{3, 4\}$.*

O COMPRIMENTO duma órbita é simplesmente o número de elementos que essa órbita contém. Note que as órbitas associadas a uma dada permutação π de X são subconjuntos *disjuntos* de X, cuja união é X. Dizemos por isso que as órbitas de π constituem uma PARTIÇÃO do conjunto X. Note também que a identidade é a única permutação com todas as órbitas de comprimento 1. As permutações com no máximo uma órbita de comprimento maior do que 1 dizem-se CICLOS. Deve ser evidente que todos as permutações de S_3 são ciclos, mas a permutação π de S_4 mencionada acima não é um ciclo, porque tem duas órbitas de comprimento 2. Observe igualmente que $\pi(x) \neq x$, precisamente quando x pertence a uma órbita de π de comprimento maior que 1. A um ciclo com uma órbita de comprimento 2 chama-se uma TRANSPOSIÇÃO.

Se a permutação π é um ciclo, é mais simples representá-la indicando os elementos da sua maior órbita O_x, escrevendo $(x, \pi(x), \pi^2(x), \dots, \pi^{k-1}(x))$, onde k é o comprimento de $\mathcal{O}_x$, ou seja, o menor natural tal que $\pi^k(x) = x$.

Exemplo 1.3.3.

No caso de S_3, escrevemos:

$$\alpha = (2,3) = (3,2), \qquad \beta = (1,3) = (3,1), \qquad \gamma = (1,2) = (2,1),$$

$$\delta = (1,2,3) = (2,3,1) = (3,1,2), \qquad \varepsilon = (1,3,2) = (3,2,1) = (2,1,3).$$

A identidade I pode ser representada, por exemplo, como $I = (1)$. Note-se que a permutação inversa dum ciclo se obtém invertendo a ordem pela qual os elementos aparecem na respectiva órbita. Em particular, a permutação

inversa de uma transposição é a mesma transposição. No exemplo acima, α, β, e γ são iguais às respectivas inversas, e ε e δ são inversas uma da outra.

Dois ciclos dizem-se *disjuntos* se as suas órbitas de comprimento maior do que 1 são disjuntas. Quaisquer ciclos disjuntos π e ρ *comutam*, *i.e.*, $\pi\rho = \rho\pi$, e qualquer permutação é um produto de ciclos disjuntos (um ciclo por cada uma das suas órbitas de comprimento maior do que 1). Mais precisamente, temos em S_n o seguinte resultado sobre factorização, que de certo modo é análogo ao Teorema Fundamental da Aritmética[9]:

Proposição 1.3.4. *Qualquer permutação π em S_n é um produto de ciclos disjuntos. Esta factorização é única a menos da ordem dos factores.*

Observe-se que, em geral, temos

$$(x_1, x_2, \ldots, x_m) = (x_1, x_m) \ldots (x_1, x_3)(x_1, x_2)$$

logo é possível factorizar permutações de S_n usando como factores apenas ciclos de comprimento 2 (naturalmente, desde que $n \geq 2$). Neste caso, no entanto, os factores não são únicos e a sua ordem é relevante, porque se torna indispensável usar transposições que não são disjuntas.

Exemplos 1.3.5.

1. *No caso da permutação π de S_4 acima, temos*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix},$$

   i.e.*, podemos escrever esta permutação na forma $\pi = (1,2)(3,4) = (3,4)(1,2)$.*

2. *Da mesma forma, o ciclo $(1,2,4,3)$ pode ser escrito como um produto de transposições:*

$$(1,2,4,3) = (1,3)(1,4)(1,2).$$

   Observe-se que este ciclo também admite, por exemplo, as factorizações

$$(1,2,4,3) = (2,1)(2,3)(2,4) = (1,3)(1,4)(1,2)(2,4)(1,3)(2,4)(1,3).$$

O exemplo anterior mostra que, na factorização de uma permutação como um produto de transposições, estas *não* são unicamente determinadas. Note-se também que o *número* de transposições utilizadas não é único. Apesar desta falta de unicidade, é possível provar que o número de factores necessários tem *paridade* fixa, *i.e.*, é sempre par ou sempre ímpar. Para este fim, sendo π uma permutação com órbitas $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_L$, com comprimentos $n_1, n_2, \ldots, n_l$, definimos $P(\pi) = \sum_{i=1}^{L}(n_i - 1)$, e provamos:

[9] "Qualquer natural $n \geq 2$ é um produto de números primos, que são únicos a menos da ordem dos factores" (ver Capítulo 2).

Proposição 1.3.6. *Se π é uma permutação e τ é uma transposição, então*

$$P(\pi\tau) = P(\pi) \pm 1.$$

Demonstração. Sendo $\tau = (a, b)$, temos dois casos distintos a considerar:

(a) os elementos a e b pertencem a órbitas distintas $\mathcal{O}_i$ e $\mathcal{O}_j$ de π, e

(b) os elementos a e b pertencem à mesma órbita $\mathcal{O}_i$.

Pode verificar-se as seguintes afirmações, para cada um dos casos indicados acima:

(a) $\pi\tau$ tem as mesmas órbitas que π, com excepção de $\mathcal{O}_i$ e $\mathcal{O}_j$, que passam a formar uma única órbita, com comprimento $n_i + n_j$. Portanto, $P(\pi\tau) = P(\pi) + 1$;

(b) $\pi\tau$ tem as mesmas órbitas que π, com excepção de $\mathcal{O}_i$, que é separada em duas órbitas. Neste caso, $P(\pi\tau) = P(\pi) - 1$.

□

Podemos agora provar:

Teorema 1.3.7. *Se $\tau_1, \tau_2, \ldots, \tau_m$ são transposições tais que $\pi = \tau_1\tau_2\cdots\tau_m$, então $P(\pi) - m$ é par, e portanto $P(\pi)$ e m têm a mesma paridade (são ambos pares, ou ambos ímpares).*

Demonstração. Argumentamos por indução em m.

Se $m = 1$, então π é uma transposição e $P(\pi) = 1$, donde $P(\pi) - m = 0$ é par.

Se $m > 1$, tomamos $\alpha = \tau_1\tau_2\cdots\tau_{m-1}$. Temos, pela hipótese de indução, que $P(\alpha) - (m-1)$ é par, e pelo resultado anterior temos $P(\pi) = P(\alpha) \pm 1$. Concluímos que

$$P(\pi) - m = (P(\alpha) \pm 1) - m - 1 + 1 = P(\alpha) - (m-1) - (1 \pm 1)$$

é par. □

A PARIDADE DUMA PERMUTAÇÃO π de S_n é a paridade do número de transposições numa sua factorização em transposições ou, como acabámos de ver, a paridade de $P(\pi)$. Se $P(\pi)$ é um número par (respectivamente, ímpar), dizemos que π é uma permutação par (respectivamente, ímpar). O SINAL de π é $+1$ (respectivamente, -1), se π é par (respectivamente, ímpar), e designa-se por $\operatorname{sgn}(\pi)$. Em particular, qualquer transposição é ímpar, assim como o ciclo $(1, 2, 4, 3)$, e a identidade é uma permutação par, já que $I = (1, 2)(1, 2)$.

As permutações pares de S_n formam um grupo, designado por A_n, dito GRUPO ALTERNADO (em n símbolos). Deixamos como exercício verificar que A_n contém $\frac{n!}{2}$ elementos.

Exercícios.

1. Factorize a permutação

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 7 & 5 \end{pmatrix}$$

num produto de ciclos disjuntos.

2. Qual é a paridade da permutação π do exercício anterior?

3. Quantas transposições existem em S_n?

4. Quantos ciclos distintos de comprimento k $(1 \leq k \leq n)$ existem em S_n?

5. Mostre que, se $\pi, \rho \in S_n$, então $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$.

6. Prove que A_n é um subgrupo de S_n.

7. Indique todos os elementos do grupo A_3.

8. Determine todos os subgrupos de S_3.

9. Mostre que em S_n o número de permutações pares é igual ao número de permutações ímpares, se $n > 1$.

1.4 Homomorfismos e Isomorfismos

A comparação de estruturas algébricas que satisfazem a mesma definição abstracta faz-se com recurso a uma das noções mais fundamentais da Álgebra, a de *isomorfismo*, ela própria um caso particular da noção de *homomorfismo*. A respectiva definição formal apresenta-se a seguir para monóides:

Definição 1.4.1. Se $(X, *)$ e $(Y, \cdot)$ são monóides, a função $\phi : X \to Y$ diz-se um HOMOMORFISMO se e só se

$$\phi(x_1 * x_2) = \phi(x_1) \cdot \phi(x_2), \qquad \forall x_1, x_2 \in X.$$

Se o homomorfismo ϕ é uma bijecção, então diz-se um ISOMORFISMO, e neste caso os monóides dizem-se ISOMORFOS[10].

[10] O uso dos seguintes termos também é frequente: um MONOMORFISMO é um homomorfismo injectivo; e um EPIMORFISMO é um homomorfismo sobrejectivo. Por outro lado, um ENDOMORFISMO é um homomorfismo de uma estrutura algébrica em si própria, enquanto que um AUTOMORFISMO é um isomorfismo de uma estrutura algébrica em si própria.

Uma forma particularmente sugestiva de descrever a noção de homomorfismo é através do seguinte diagrama:

$$\begin{array}{ccc} X \times X & \xrightarrow{\text{“}*\text{”}} & X \\ {\scriptstyle \phi\times\phi}\downarrow & & \downarrow{\scriptstyle \phi} \\ Y \times Y & \xrightarrow[\text{“}\cdot\text{”}]{} & Y \end{array}$$

Este tipo de diagrama diz-se *comutativo*, precisamente porque pode ser percorrido por dois caminhos distintos, sem alterar o resultado final de chegada.

Exemplos 1.4.2.

1. *A função* logaritmo $\phi : \mathbb{R}^+ \to \mathbb{R}$ *dada por* $\phi(x) = \log(x)$ *é uma bijecção. Como* $\log(xy) = \log(x) + \log(y)$*, os grupos* $(\mathbb{R}^+, \cdot)$ *e* $(\mathbb{R}, +)$ *são isomorfos. Note-se que a função inversa (*exponencial*)* $\psi(x) = \exp(x)$ *é igualmente um isomorfismo.*

2. *O conjunto das transformações lineares* $T : \mathbb{R}^n \to \mathbb{R}^n$ *com a operação de composição é um monóide. Fixada uma base de* $\mathbb{R}^n$*, é possível calcular para cada transformação* T *a sua representação matricial* $\mathcal{M}(T)$*, que é uma matriz* $n \times n$*. É fácil verificar que a função* $\mathcal{M}(T)$ *é um isomorfismo de monóides (a composição de transformações lineares corresponde ao produto das respectivas representações matriciais).*

Se $(G, *)$ e $(H, \cdot)$ são grupos *isomorfos*, indicamos este facto escrevendo "$(G, *) \simeq (H, \cdot)$", ou mesmo, quando as operações são evidentes do contexto da discussão, apenas "$G \simeq H$". Escrevemos por isso $(\mathbb{R}^+, \cdot) \simeq (\mathbb{R}, +)$, ou $\mathbb{R}^+ \simeq \mathbb{R}$. [11]

Suponha-se agora que $(G, *)$ e $(H, \cdot)$ são grupos, com identidades designadas respectivamente por e e $\tilde{e}$, e $\phi : G \to H$ é um homomorfismo (não necessariamente um isomorfismo). Temos neste caso:

Proposição 1.4.3. *Se* $(G, *)$ *e* $(H, \cdot)$ *são grupos, com identidades designadas respectivamente por* e *e* $\tilde{e}$*, e* $\phi : G \to H$ *é um homomorfismo, então*

(i) Invariância da identidade*:* $\phi(e) = \tilde{e}$.

(ii) Invariância dos inversos*:* $\phi(g^{-1}) = (\phi(g))^{-1},\ \forall g \in G$.

Demonstração. (i) Como

$$\phi(e) \cdot \phi(e) = \phi(e * e) = \phi(e),$$

segue-se, da lei do corte, que $\phi(e) = \tilde{e}$.

[11] Usamos o símbolo $\simeq$ para indicar que dois objectos do mesmo tipo (monóides, grupos, etc.) são isomorfos.

(ii) Como

$$\phi(g) \cdot \phi(g^{-1}) = \phi(g * g^{-1}) = \phi(e) = \tilde{e},$$

concluímos que $\phi(g^{-1}) = (\phi(g))^{-1}$. □

Exemplos 1.4.4.

1. *Considerem-se os grupos* $(\mathbb{R}, +)$ *e* $(\mathbb{C}^*, \cdot)$*, onde* $\mathbb{C}^*$ *designa o conjunto dos complexos não-nulos. Definimos* $\phi : \mathbb{R} \to \mathbb{C}^*$ *por* $\phi(x) = e^{2\pi x i} = \cos(2\pi x) + i\,\mathrm{sen}(2\pi x)$*. A função* ϕ *é um homomorfismo* ($e^z \cdot e^w = e^{z+w}$*, mesmo quando* z *e* w *são complexos*[12]*). É claro que* ϕ *não é sobrejectiva (porque* $\phi(x)$ *é um complexo de módulo 1), e não é injectiva (porque, se* $x = n$ *é um inteiro, temos* $\phi(n) = 1$*. Note que a função* ϕ *corresponde a "enrolar" a recta real sobre o círculo unitário. De acordo com a Proposição, o elemento neutro do grupo de partida (o real* 0*), é transformado no elemento neutro do grupo de chegada (o complexo* 1*), e a imagem do* simétrico *do real* x *é o* inverso *do complexo* $\phi(x)$*.*

2. *Considerem-se os grupos* $(\mathbb{Z}, +)$ *e* $(\mathbb{C}^*, \cdot)$*. Definimos* $\phi : \mathbb{Z} \to \mathbb{C}^*$ *por* $\phi(n) = i^n$*. A função* ϕ *é mais uma vez um homomorfismo que não é sobrejectivo nem injectivo. O elemento neutro do grupo de partida, que é o inteiro* 0*, é transformado no elemento neutro do grupo de chegada, que é o complexo* 1*, e a imagem do* simétrico *do inteiro* n *é o* inverso *do complexo* $\phi(n)$*.*

3. *O exemplo anterior pode ser generalizado: se* $(G, *)$ *é um grupo arbitrário e* $g \in G$*, podemos sempre definir* $\phi : \mathbb{Z} \to G$ *por* $\phi(n) = g^n$ *(notação multiplicativa). A função* ϕ *é um homomorfismo de* $(\mathbb{Z}, +)$ *para* $(G, *)$*.*

Dado um homomorfismo de grupos $\phi : G \to H$, consideramos agora a equação $\phi(x) = y$, onde supomos $y \in H$ fixo, e x a incógnita a determinar. Por analogia com a Álgebra Linear, a equação diz-se *homogénea* quando $y = \tilde{e}$ é a identidade do grupo de chegada, e *não-homogénea* quando $y \neq \tilde{e}$. O conjunto das soluções da equação homogénea diz-se NÚCLEO DO HOMOMORFISMO, designado por $N(\phi)$, e o conjunto dos $y \in H$ para os quais a equação $\phi(x) = y$ tem solução $x \in G$, designado por $\phi(G)$ (ou ainda por $\mathrm{Im}(\phi)$) diz-se IMAGEM DO HOMOMORFISMO.

Exemplos 1.4.5.

1. *Continuando os Exemplos 1.4.4, o núcleo de* $\phi : \mathbb{R} \to \mathbb{C}^*$ *é precisamente o conjunto dos inteiros, e* $\phi(\mathbb{R})$ *é o conjunto* $\mathbb{S}^1$ *dos complexos de módulo* 1 *(o círculo unitário).*

2. *De igual modo, o núcleo de* $\phi : \mathbb{Z} \to \mathbb{C}^*$ *é precisamente o conjunto dos inteiros que são múltiplos de 4, e* $\phi(Z)$ *é o conjunto* $\{1, -1, i, -i\}$*.*

A figura seguinte ilustra os conceitos de núcleo e imagem de um homomorfismo.

[12] Recorde que se $z = x + iy$ é um complexo, com $x, y \in \mathbb{R}$, definimos $e^z = e^x(\cos(y) + i\,\mathrm{sen}(y))$.

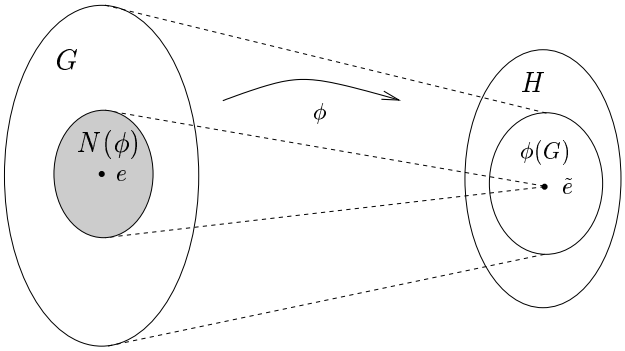


Figura 1.4.1: Núcleo e imagem dum homomorfismo.

Nos exemplos acima, tanto o núcleo do homomorfismo como a imagem do conjunto de partida são subgrupos dos grupos originais. O próximo resultado mostra que este facto não é uma coincidência.

Proposição 1.4.6. *Se $(G,*)$ e $(H,\cdot)$ são grupos, e $\phi : G \to H$ é um homomorfismo, então:*

(i) O núcleo de ϕ é um subgrupo de G;

(ii) $\phi(G)$ é um subgrupo de H.

Demonstração. (i) O núcleo de ϕ não é vazio, pois contém pelo menos a identidade de G (Proposição 1.4.3 (i)). Além disso, se $g_1, g_2 \in N(\phi)$ temos

$$\begin{aligned}
\phi(g_1 * g_2^{-1}) &= \phi(g_1) \cdot \phi(g_2^{-1}) && \text{(porque } \phi \text{ é um homomorfismo)},\\
&= \tilde{e} \cdot (\phi(g_2))^{-1} && \text{(pela Proposição 1.4.3 e porque } g_1 \in N(\phi)),\\
&= \tilde{e} \cdot \tilde{e}^{-1} && \text{(porque } g_2 \in N(\phi)),\\
&= \tilde{e}.
\end{aligned}$$

(ii) $\phi(G)$ não é vazio, porque G não é vazio. Se $h_1, h_2 \in \phi(G)$, existem $g_1, g_2 \in G$ tais que $h_1 = \phi(g_1)$ e $h_2 = \phi(g_2)$, e portanto $h_1 \cdot h_2^{-1} = \phi(g_1) \cdot (\phi(g_2))^{-1} = \phi(g_1 * g_2^{-1}) \in \phi(G)$. □

De ora em diante deixamos de explicitar as operações nos grupos, excepto se isso puder dar azo a alguma confusão. Assim, se G e H são grupos, $g_1, g_2 \in G$ e $h_1, h_2 \in H$, escrevemos $g_1 g_2$ e $h_1 h_2$ para os produtos dos elementos em G e H, embora estes possam não estar de alguma forma relacionados. Do contexto deverá ser claro a que operação nos referimos. Da mesma forma designamos por e indistintamente a unidade em G e em H.

É interessante observar que o núcleo de um homomorfismo não é um subgrupo arbitrário, mas sim um subgrupo com a seguinte característica:

Definição 1.4.7. Se $H \subset G$ é subgrupo, dizemos que H é um subgrupo NORMAL de G se e só se, para qualquer $h \in H$ e $g \in G$, temos $ghg^{-1} \in H$.

Exemplos 1.4.8.

1. *Se G é um grupo abeliano, é claro que $ghg^{-1} = hgg^{-1} = h \in H$, ou seja, todos os subgrupos de um grupo abeliano são normais.*

2. *Se $G = S_3$ e $H=\{I, \alpha\}$, então H é subgrupo de G. H não é normal, pois $\varepsilon\alpha\varepsilon^{-1} = \gamma \notin H$.*

3. *Supondo ainda $G = S_3$, tomamos $H = A_3 = \{I, \delta, \varepsilon\}$, e recordamos que o grupo alternado A_3 é formado pelas permutações* pares *de S_3. Se $\pi \in A_3$ e $\sigma \in S_3$, é claro que $\sigma\pi\sigma^{-1}$ é uma permutação par (porquê?), e portanto $\sigma\pi\sigma^{-1} \in A_3$, logo, A_3 é um subgrupo normal de S_3.*

4. *Se G e H são grupos e formarmos o produto directo $G \times H$, então G e H (identificados com, respectivamente, $G\times\{e\}$ e $\{e\}\times H$) são subgrupos normais de $G \times H$.*

Podemos agora demonstrar:

Teorema 1.4.9. *Se $\phi : G \to H$ é um homomorfismo e $N(\phi)$ é o respectivo núcleo, então $N(\phi)$ é um subgrupo normal de G.*

Demonstração. Sendo $n \in N(\phi)$ e $g \in G$, temos a provar que $gng^{-1} \in N(\phi)$, ou seja, $\phi(gng^{-1}) = e$, onde e é a identidade do grupo H. Notamos apenas que:

$$\begin{aligned} \phi(gng^{-1}) &= \phi(g)\phi(n)\phi(g^{-1}) && \text{(definição de homomorfismo)}, \\ &= \phi(g)\phi(g^{-1}) && \text{(porque } \phi(n) = e, \text{ já que } n \in N(\phi)), \\ &= e. \end{aligned}$$

□

Tal como na Álgebra Linear, o número de soluções da equação não-homogénea $\phi(x) = y$, *i.e.*, a questão da possível injectividade de ϕ, depende apenas do núcleo $N(\phi)$. A este respeito, é fácil provar o seguinte:

Teorema 1.4.10. *Seja $\phi : G \to H$ um homomorfismo. Temos então:*

(i) $\phi(g_1) = \phi(g_2)$ *se e só se* $g_1 g_2^{-1} \in N(\phi)$;

(ii) ϕ *é injectivo se e só se* $N(\phi) = \{e\}$;

(iii) se x_0 é uma solução particular de $\phi(x) = y_0$, a solução geral é $x = x_0 n$, com $n \in N(\phi)$.

Demonstração. (i) Observemos que:

$$\begin{aligned}\phi(g_1)=\phi(g_2) &\Leftrightarrow \phi(g_1)(\phi(g_2))^{-1}=e && \text{(multiplicação em } H \text{ por } (\phi(g_2))^{-1}),\\ &\Leftrightarrow \phi(g_1g_2^{-1})=e && \text{(porque } \phi \text{ é um homomorfismo)},\\ &\Leftrightarrow g_1g_2^{-1}\in N(\phi) && \text{(por definição de } \phi).\end{aligned}$$

(ii) ϕ é injectiva se e só se $\phi(g_1)=\phi(g_2)\Leftrightarrow g_1=g_2\Leftrightarrow g_1g_2^{-1}=e$. Por (i), concluímos que $N(\phi)=\{e\}$.

(iii) Se $\phi(x_0)=y_0$, $n\in N(\phi)$, e $x=x_0n$, é claro que

$$\phi(x)=\phi(x_0n)=\phi(x_0)\phi(n)=\phi(x_0)e=\phi(x_0)=y_0,$$

e portanto x é igualmente solução da equação não-homogénea. Por outro lado, se x é solução da equação não-homogénea, temos $\phi(x)=\phi(x_0)$, donde $xx_0^{-1}\in N(\phi)$. Sendo $xx_0^{-1}=n$, obtemos $x=x_0n$. □

Exemplos 1.4.11.

1. *Continuando os Exemplos 1.4.4, vimos que o núcleo de* $\phi:\mathbb{R}^+\to\mathbb{C}^*$ *é o conjunto dos inteiros,* i.e.*,*

$$\phi(x)=1\Leftrightarrow \cos(2\pi x)=1,\operatorname{sen}(2\pi x)=0\Leftrightarrow x\in\mathbb{Z},$$

Considere-se a equação $\phi(x)=i$, i.e., $[\cos(2\pi x)=0,\operatorname{sen}(2\pi x)=1]$. *Uma solução óbvia desta equação é* $x=\frac{1}{4}$. *A solução geral é portanto* $x=\frac{1}{4}+n$, *com* $n\in\mathbb{Z}$.

2. *O núcleo de* $\phi:\mathbb{Z}\to\mathbb{C}^*$ *é o conjunto dos múltiplos de 4,* i.e.*,*

$$\phi(n)=1\Leftrightarrow i^n=1\Leftrightarrow n=4k,\ \text{com } k\in\mathbb{Z}.$$

Considere-se a equação $\phi(n)=i$, i.e., $i^n=i$. *Uma solução óbvia desta equação é* $n=1$. *A solução geral é portanto* $n=1+4k$, *com* $k\in\mathbb{Z}$.

3. *As estruturas algébricas* $(\mathbb{R}^n,+)$ *e* $(\mathbb{R}^m,+)$, *onde a adição é a usual* soma vectorial*, são claramente grupos abelianos. Se* $T:\mathbb{R}^n\to\mathbb{R}^m$ *é uma transformação linear, é fácil verificar que* T *é igualmente um homomorfismo de grupos, e que o teorema estudado na Álgebra Linear sobre a equação* $T(x)=y$ *não passa de um caso muito particular do teorema anterior.*

A noção de isomorfismo entre estruturas algébricas que satisfazem a mesma definição abstracta está na origem de outro dos problemas fundamentais da Álgebra contemporânea, dito o problema da *classificação* de estruturas algébricas. De uma forma um pouco imprecisa, este problema é o seguinte:

Dada uma definição (abstracta, axiomática) de estrutura algébrica, determinar uma classe $\mathcal{C}$ de estruturas algébricas concretas que satisfazem essa definição, e tais que qualquer outra estrutura algébrica que satisfaça a mesma definição seja isomorfa exactamente a uma estrutura algébrica da classe $\mathcal{C}$.

A título de exemplo, o problema da classificação para os *grupos finitos simples* (uma classe muito importante de grupos que estudaremos mais adiante no Capítulo 5) foi resolvido muito recentemente, no que foi seguramente um dos resultados mais importantes da Matemática do século XX. Apresentaremos neste texto a resolução de alguns problemas de classificação, de complexidade crescente. Começamos por discutir um exemplo trivial, apenas para substanciar as ideias expostas: a classificação dos monóides com exactamente *dois* elementos.

Se $(X, *)$ é um monóide com dois elementos, temos $X = \{I, a\}$, onde I designa a identidade, e $I \neq a$. Note-se que os produtos $I*I$, $I*a$ e $a*I$ estão determinados pelo facto de I ser a identidade ($I * I = I$, $I * a = a * I = a$). Resta-nos calcular o produto $a*a$, que só pode verificar $a*a = a$ ou $a*a = I$ (no segundo caso, a seria invertível, e portanto o monóide seria um grupo). As tabuadas seguintes descrevem estas duas possibilidades:

	I	a
I	I	a
a	a	I

	I	a
I	I	a
a	a	a

Para verificar que ambos os casos são possíveis, considerem-se os conjuntos $M = \{0, 1\}$, e $G = \{1, -1\}$, sendo a operação correspondente em ambos os casos o produto usual. É evidente que o produto é uma operação binária, associativa, e com identidade, em qualquer um destes conjuntos. Portanto, cada um destes conjuntos, com o produto usual, é um monóide com dois elementos. Note-se também, inspeccionando as diagonais principais das respectivas tabuadas, que estes monóides não são isomorfos.

	1	-1
1	1	-1
-1	-1	1

	1	0
1	1	0
0	0	0

É claro que qualquer uma das duas primeiras tabuadas representa um monóide isomorfo a um destes monóides. Na realidade, se $a * a = I$, o isomorfismo é a função $\phi : X \to G$ dado por $\phi(I) = 1$ e $\phi(a) = -1$, e se $a*a = a$, o isomorfismo é a função $\phi : X \to M$ dada por $\phi(I) = 1$ e $\phi(a) = 0$. Resumimos estas observações como se segue:

- G e M *são* monóides com dois elementos,
- G e M *não* são isomorfos entre si, e
- Se X é um *qualquer* monóide com dois elementos, temos $X \simeq G$ ou $X \simeq M$.

Dizemos por isso que, "a menos de isomorfismo", existem exactamente *dois* monóides com dois elementos, e a *classificação* dos monóides com dois

elementos é a *família* $\{G, M\}$. Note-se que, como qualquer grupo é um monóide, e apenas G é um grupo, podemos também concluir que, "a menos de isomorfismo", existe um *único* grupo com dois elementos, que é G.[13]

Exercícios.

1. Mostre que a identidade $e^{z+w} = e^z e^w$ com z e w complexos resulta das identidades usuais para e^{x+y}, $\cos(x+y)$ e $\text{sen}(x+y)$ com x e y reais.

2. As soluções complexas da equação $x^n = 1$ são os complexos $e^{2\pi ki/n}$, onde $1 \leq k \leq n$. Estas *raízes-n da unidade*, formam os vértices de um polígono regular de n lados, inscrito no círculo unitário, com um dos vértices sobre o ponto 1.

   (a) Verifique que $\phi : \mathbb{Z} \to \mathbb{C}^*$ dada por $\phi(k) = e^{2\pi ki/n}$ é um homomorfismo.

   (b) Conclua que as raízes-n da unidade formam um subgrupo de $\mathbb{C}^*$.

   (c) Determine o núcleo do homomorfismo ϕ.

3. Suponha que G, H e K são grupos.

   (a) Prove que $G \times H \simeq H \times G$, e $G \times (H \times K) \simeq (G \times H) \times K$.

   (b) Mostre que $\phi : G \to H \times K$ é um homomorfismo se e só se $\phi(x) = (\phi_1(x), \phi_2(x))$, onde $\phi_1 : G \to H$ e $\phi_2 : G \to K$ são homomorfismos.

4. Considere a estrutura algébrica $(\mathbb{R}^2, +)$ com a soma vectorial usual.

   (a) Mostre que $(\mathbb{R}^2, +)$ é um grupo abeliano.

   (b) Prove que qualquer transformação linear $T : \mathbb{R}^2 \to \mathbb{R}$ é um homomorfismo do grupo $(\mathbb{R}^2, +)$ para o grupo $(\mathbb{R}, +)$.

   (c) Mostre que qualquer homomorfismo do grupo $(\mathbb{R}^2, +)$ para o grupo $(\mathbb{R}, +)$ que seja uma função *contínua* é igualmente uma transformação linear[14].

   (d) Sendo $a \in \mathbb{R}^2$ fixo, definimos $T : \mathbb{R}^2 \to \mathbb{R}$ por $T(\boldsymbol{x}) = a \cdot \boldsymbol{x}$, onde "$\cdot$" designa o produto interno usual. Calcule o núcleo de T, e verifique directamente que esse núcleo é um subgrupo e um subespaço.

   (e) Dê um exemplo de um subgrupo de $(\mathbb{R}^2, +)$ que não seja um subespaço vectorial.

5. Suponha que $(A, *)$ e $(B, \cdot)$ são monóides com identidades designadas respectivamente por e e $\tilde{e}$, e $\phi : A \to B$ é um isomorfismo. Prove que:

   (a) $\phi(e) = \tilde{e}$.

   (b) $\phi(a^{-1}) = (\phi(a))^{-1}$ se $a \in A$ é invertível.

   (c) $\phi^{-1} : B \to A$ é igualmente um isomorfismo.

[13] Este grupo é evidentemente isomorfo ao grupo $(\mathbb{Z}_2, +)$, que também já mencionámos.

[14] Existem efectivamente homomorfismos que não são contínuos e não são transformações lineares. A sua existência só pode ser demonstrada com recurso ao Axioma da Escolha, discutido no Apêndice.

(d) $(A, *)$ é um grupo se e só se $(B, \cdot)$ é um grupo.

6. Continuando o exercício anterior, suponha agora apenas que ϕ é um homomorfismo injectivo (respectivamente, sobrejectivo). Quais das afirmações anteriores são ainda válidas em cada um destes casos?

7. Seja G um grupo, e $\mathrm{Aut}(G)$ o conjunto dos automorfismos $\phi : G \to G$.

   (a) Prove que $\mathrm{Aut}(G)$ com a operação de composição é um grupo.

   (b) Determine $\mathrm{Aut}(G)$ quando G é o grupo formado pelas soluções complexas de $x^4 = 1$.

8. Seja G um grupo qualquer.

   (a) Sendo $g \in G$ fixo, mostre que $\phi_g : G \to G$ dada por $\phi_g(x) = gxg^{-1}$ é um automorfismo.

   (b) Prove que a função $T : G \to \mathrm{Aut}(G)$ dada por $T(g) = \phi_g$ é um homomorfismo.

   (c) Prove que o núcleo de T é o centro do grupo G (ver Exercício 7, na secção anterior).

9. Classifique os grupos com três e quatro elementos.

10. Mostre que A_n é o núcleo do homomorfismo $\phi : S_n \to \mathbb{Z}_2$ que a uma permutação π associa o seu sinal $\mathrm{sgn}(\pi)$.

11. Determine todos os subgrupos normais de S_3.

12. Seja G um grupo qualquer e $\phi : S_3 \to G$ um homomorfismo. Classifique o grupo $\phi(S_3)$ (*i.e.*, diga quais são as possibilidades para $\phi(S_3)$ a menos de isomorfismo).

13. Seja G um grupo qualquer, e $g \in G$. Considere a função $T_g : G \to G$ dada por $T_g(x) = gx$.

   (a) Mostre que T_g é uma permutação no conjunto G.

   (b) Considere a função $\phi(g) : G \to S_G$ dada por $\phi(g) = T_g$. Prove que ϕ um homomorfismo injectivo, e conclua que G é isomorfo a um subgrupo de um grupo de permutações.

   (c) Conclua que, se G é um grupo finito com n elementos, então existe um subgrupo $H \subseteq S_n$ tal que $G \simeq H$.

1.5 Anéis, Domínios Integrais e Corpos

Os números inteiros, racionais, reais e complexos podem ser somados e multiplicados por números do mesmo tipo, e o resultado de cada operação é

ainda um número do mesmo tipo. Analogamente, podemos somar e multiplicar matrizes quadradas da mesma dimensão, transformações lineares de um espaço vectorial sobre si próprio, e muitos outros tipos de objectos que são hoje de utilização corrente na Matemática e nas suas aplicações a outras ciências. Estes exemplos são estruturas algébricas mais complexas do que os grupos ou monóides, precisamente porque envolvem duas operações. Partilham um conjunto de propriedades básicas comuns, que são a base da definição da estrutura algébrica chamada de *anel*, introduzida nesta secção. Ainda nesta secção, distinguimos certos casos especiais de anéis, o dos *corpos* (anéis onde o produto é comutativo e a divisão por elementos não-nulos é sempre possível, de que são exemplos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$), e o dos *domínios integrais* (anéis com propriedades análogas às dos inteiros).

Seja A um conjunto não-vazio, e $\sigma, \pi : A \times A \to A$ duas operações binárias em A. Para simplificar a notação, escrevemos "$a + b$" em vez de "$\sigma(a, b)$", e "$a \cdot b$" (ou ainda ab) em vez de "$\pi(a, b)$". Dizemos que $a + b$ e $a \cdot b$ são respectivamente a *soma* e o *produto* dos elementos a e b de A.

Definição 1.5.1. O terno ordenado $(A, +, \cdot)$ diz-se um ANEL se:

(i) *Propriedades da soma*: $(A, +)$ é um grupo abeliano.

(ii) *Propriedades do produto*: O produto é associativo, *i.e.*,

$$\forall a, b, c \in A,\ (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(iii) *Propriedades mistas*: A soma e o produto são distributivos, *i.e.*,

$$\forall a, b, c \in A,\ a \cdot (b + c) = a \cdot b + a \cdot c,\ \text{e}\ (b + c) \cdot a = b \cdot a + c \cdot a.$$

O significado preciso das propriedades (i) a (iii) desta definição é:

- *Associatividade da soma*: $\forall a, b, c \in A,\ (a + b) + c = a + (b + c)$.
- *Comutatividade da soma*: $\forall a, b \in A,\ a + b = b + a$.
- *Identidade para a soma*: $\exists 0 \in A\ \forall a \in A,\ a + 0 = a$.
- *Simétricos em relação à soma*: $\forall a \in A\ \exists b \in A :\ a + b = 0$.
- *Associatividade do produto*: $\forall a, b, c \in A,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- *Distributividade*: $\forall a, b, c \in A,\ a \cdot (b+c) = a \cdot b + a \cdot c$, e $(b+c) \cdot a = b \cdot a + c \cdot a$.

Como dissemos acima, a Definição 1.5.1 é pelo menos parcialmente inspirada pelo caso em que $A = \mathbb{Z}$ é o conjunto dos inteiros, quando a "soma" e o "produto" nela mencionados são as habituais operações sobre números inteiros, e 0 é o inteiro zero. Em particular, todas as propriedades indicadas são nesse caso bem conhecidas. No entanto, a comparação dum qualquer

anel A com o anel dos inteiros deve ser sempre feita com prudência. Note-se que em geral o "produto" *não* é comutativo, nem se faz na Definição 1.5.1 qualquer referência à existência duma identidade para esta operação (semelhante ao inteiro 1). Os exemplos que estudaremos mais à frente mostrarão que, por vezes, um anel goza de propriedades radicalmente diferentes das do anel dos inteiros.

Se o anel A tem identidade (para o produto) então $(A, \cdot)$ é um monóide. Nesse caso dizemos que A é um ANEL UNITÁRIO. Referimo-nos sempre à (única) identidade para a soma como o ZERO do anel, reservando o termo IDENTIDADE sem mais qualificativos para a (única) identidade para o produto, quando esta existir no anel em causa (*i.e.*, quando o anel for unitário). Mais uma vez, um ANEL COMUTATIVO, ou ABELIANO, é um anel em que $a \cdot b = b \cdot a$, para quaisquer $a, b \in A$.

Exemplos 1.5.2.

1. *O conjunto dos inteiros com as operações habituais de soma e produto é um anel abeliano unitário. Por outro lado, o conjunto dos inteiros* pares *com as operações habituais de soma e produto é um anel abeliano sem identidade.*

2. *Os conjuntos de números* racionais, reais *e* complexos *(designados respectivamente por $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$) também com a soma e o produto habituais são anéis abelianos unitários.*

3. *O conjunto das* matrizes quadradas *$(n \times n)$ com entradas em $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, que designaremos respectivamente por $M_n(A)$, onde $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, ainda com as operações de soma e produto usuais para matrizes, são anéis (não-abelianos se $n > 1$) unitários (a identidade é a* matriz identidade *I). Mais geralmente, podemos considerar o anel das matrizes $M_n(A)$ com entradas num anel arbitrário A.*

4. *O conjunto de todas as* funções *$f : \mathbb{R} \to \mathbb{R}$, com a soma e o produto definidos por*

$$(f + g)(x) = f(x) + g(x),$$
$$(fg)(x) = f(x)g(x),$$

é um anel abeliano unitário (a identidade é a função constante igual a 1). De forma semelhante, podemos considerar o anel das funções contínuas, o anel das funções diferenciáveis, etc.

5. *O conjunto $\mathbb{Z}_2 = \{0, 1\}$, com a soma e produto definidos por*

$$0 + 0 = 1 + 1 = 0, \qquad 0 + 1 = 1 + 0 = 1,$$
$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \qquad 1 \cdot 1 = 1,$$

é um anel abeliano unitário. Note-se que as operações deste anel correspondem às operações lógicas de "disjunção (ou exclusivo)" e "conjunção (e)", se associarmos

$$0 \to \textit{Falso}, \quad 1 \to \textit{Verdadeiro}.$$

As operações deste anel correspondem igualmente à usual aritmética "binária", i.e., *na* base 2, *sendo a soma sem transporte.*

6. *O conjunto dos complexos da forma $z = n + mi$, com $n, m \in \mathbb{Z}$, é um anel abeliano unitário. Este anel designa-se habitualmente por $\mathbb{Z}[i]$, e os seus elementos dizem-se* OS INTEIROS DE GAUSS[15]

Passamos agora a enunciar propriedades básicas de qualquer anel, começando por algumas consequências directas de resultados que já provámos num contexto mais geral:

Proposição 1.5.3. *Seja A um anel.*

(i) Lei do corte para a adição*: $a + c = b + c \Rightarrow a = b$, e em particular $d + d = d \Rightarrow d = 0$.*

(ii) Unicidade dos simétricos*: A equação $a + x = 0$ tem uma só solução em A, dada por $x = -a$.*

(iii) Regras dos sinais*: $-(-a) = a$, $-(a + b) = (-a) + (-b)$, e $-(a - b) = (-a) + b$.*

Mencionámos acima que A é um anel unitário se e só se $(A, \cdot)$ é um monóide. Neste caso, designamos por A^* o conjunto dos elementos invertíveis do monóide $(A, \cdot)$, ditos igualmente elementos *invertíveis do anel* A, e recordamos resultados provados num contexto mais geral:

Proposição 1.5.4. *Seja A um anel unitário. Então $(A^*, \cdot)$ é um grupo, donde:*

(i) A^* é fechado em relação ao produto.

(ii) Se $a \in A^*$, $ax = 1$ tem como única solução $x = a^{-1}$, onde $a^{-1} \in A^*$.

(iii) Se $a, b \in A^*$, $(ab)^{-1} = b^{-1}a^{-1}$, e $(a^{-1})^{-1} = a$.

Exemplos 1.5.5.

1. *Os únicos inteiros invertíveis são* 1 *e* -1, i.e., $\mathbb{Z}^* = \{-1, 1\}$.

2. *Todos os racionais, reais e complexos diferentes de zero são invertíveis. Assim, temos por exemplo $\mathbb{Q}^* = \mathbb{Q} - \{0\}$* [16].

[15] Carl Friedrich Gauss (1777-1855) foi um dos grandes matemáticos de Göttingen. Foi uma criança prodígio, e com apenas 19 anos descobriu um método de construção dum polígono regular de 17 lados usando exclusivamente régua e compasso (ver Capítulo 7). Durante mais de 2000 anos, desde os geómetras gregos, os únicos polígonos regulares com um número primo de lados que se sabia construir com régua e compasso eram o triângulo equilátero e o pentágono regular. Alguns dos resultados mais relevantes que discutiremos são de facto descobertas de Gauss, como por exemplo a teoria das congruências.

[16] Se A e B são conjuntos, $A - B = \{x \in A : x \notin B\}$.

3. *No anel $M_n(\mathbb{R})$, os elementos invertíveis são as matrizes* não-singulares*, que sabemos serem as matrizes com determinante $\neq 0$.*

Em geral, num anel arbitrário A com identidade $1 \neq 0$, podemos apenas dizer que 1 e -1 são invertíveis, porque $1 \cdot 1 = (-1) \cdot (-1) = 1$, o que é precisamente o caso do anel $\mathbb{Z}$. No outro extremo, existem anéis como $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, onde *todos* os elementos não-nulos são invertíveis. Existem igualmente casos intermédios como o do anel $M_n(A)$ (A um anel), onde a determinação dos elementos invertíveis pode ser bastante complicada.

Enunciamos em seguida algumas propriedades elementares de anéis que envolvem as duas operações do anel, e que por isso não são consequências directas de resultados provados anteriormente. A primeira propriedade, por exemplo, mostra que o zero de qualquer anel não é invertível (a divisão por zero é sempre impossível), excepto no caso trivial do anel $A = \{0\}$.

Proposição 1.5.6. *Para quaisquer $a, b \in A$, temos:*

(i) Produto por zero: $a0 = 0a = 0$.

(ii) Regras dos sinais: $-(ab) = (-a)b = a(-b)$, e $(-a)(-b) = ab$.

Demonstração. As demonstrações destes resultados não oferecem dificuldades especiais. Provamos a título de exemplo apenas a regra do produto por zero, deixando a demonstração das restantes afirmações como exercício.

Para mostrar que $a0 = 0$ notamos que

$$\begin{aligned} a0 + a0 &= a(0+0) && \text{(propriedade distributiva)},\\ &= a0 && \text{(porque 0 é elemento neutro)},\\ &\Rightarrow a0 = 0 && \text{(pela lei do corte)}. \end{aligned}$$

□

Uma parte das diferenças mais óbvias entre os diversos anéis que já referimos prendem-se claramente com propriedades do produto, e têm a ver não só com a invertibilidade dos respectivos elementos como igualmente com a possível aplicação da "lei do corte" ao produto, formalmente definida como se segue:

Definição 1.5.7. O anel A verifica a LEI DO CORTE PARA O PRODUTO se

$$\forall a, b, c \in A,\ [c \neq 0 \text{ e } (ac = bc \text{ ou } ca = cb)] \Rightarrow a = b.$$

A restrição $c \neq 0$ (que não tem correspondente na lei do corte para a soma) é evidentemente inevitável devido à regra do produto por zero. Para mostrar que a lei do corte para o produto não é válida em todos os anéis, e

portanto não é uma consequência lógica da Definição 1.5.1, basta considerar por exemplo em $M_2(\mathbb{R})$ o produto

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

onde temos $ca = cb$, com $c \neq 0$ e $a \neq b$.

Este exemplo mostra também que existem anéis onde podemos ter $cd = 0$ com $c \neq 0$ e $d \neq 0$, caso em que c e d se dizem DIVISORES DE ZERO. Esta noção não deve ser confundida com a de elemento não-invertível. Se $ca = cb$ (ou $ac = bc$) e c *é invertível*, é claro que qualquer das igualdades pode ser multiplicada pelo inverso de c, para concluir que $a = b$. Assim, é óbvio que um divisor de zero é sempre não-invertível, mas observe que podem existir elementos não-invertíveis que *não são* divisores de zero (em $\mathbb{Z}$, por exemplo, onde não há divisores de zero).

Deixamos como exercício verificar que:

Proposição 1.5.8. *A lei do corte para o produto é válida num anel A se e só se em A não existem divisores de zero.*

Pelas observações acima, concluímos ainda que num anel em que todos os elementos não-nulos são invertíveis ($A^* = A - \{0\}$), a lei do corte é válida. Estes anéis são distinguidos com um nome especial.

Definição 1.5.9. Um ANEL DE DIVISÃO é um anel unitário A tal que $A^* = A - \{0\}$. Um CORPO é um anel de divisão abeliano.

Os anéis $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são evidentemente corpos (no entanto, já mencionámos mais um corpo; qual?). Descreveremos adiante um anel de divisão que *não* é um corpo.

Existem igualmente anéis que não são anéis de divisão, porque nem todos os seus elementos não-nulos são invertíveis, mas nos quais a lei do corte para o produto é mesmo assim válida. Exemplos típicos são os inteiros $\mathbb{Z}$, os anéis de polinómios com coeficientes em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, e os inteiros de Gauss. Veremos ainda outros exemplos mais adiante. Esta classe de anéis também toma um nome especial:

Definição 1.5.10. Um DOMÍNIO INTEGRAL [17] é um anel unitário abeliano $A \neq \{0\}$ no qual a lei do corte para o produto é válida.

Pela proposição (1.5.8), um anel unitário abeliano $A \neq \{0\}$ é um domínio integral se e só se não possui divisores de zero. Note-se também que se A é um anel unitário com identidade 1 então $A \neq \{0\}$ se e só se $1 \neq 0$.

A figura seguinte mostra a relação entre os diversos tipos de anéis que mencionámos até ao momento (veja também os exercícios no final desta secção).

[17] Preferimos esta designação à outra designação também usual de DOMÍNIO DE INTEGRIDADE.

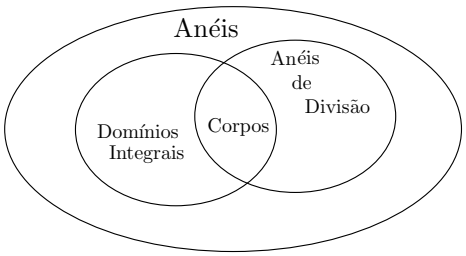


Figura 1.5.1: Domínios integrais, anéis de divisão e corpos.

Se $(A, +, \cdot)$ é um anel, e $B \subset A$, é possível que B seja *fechado* em relação às operações de soma e produto de A, *i.e.*, é possível que

$$a, b \in B \Rightarrow a + b \in B \text{ e } a \cdot b \in B.$$

Neste caso, é possível que $(B, +, \cdot)$ seja por sua vez um anel.

Definição 1.5.11. Seja $B \subset A$ um subconjunto fechado em relação à soma e ao produto do anel $(A, +, \cdot)$. B diz-se um SUBANEL de A se $(B, +, \cdot)$ é um anel. Dizemos também que o anel A é uma EXTENSÃO do anel B.

Exemplos 1.5.12.

1. *$\mathbb{Z}$ é um subanel de $\mathbb{Q}$, e o anel dos inteiros pares é um subanel de $\mathbb{Z}$.*
2. *O conjunto $\mathbb{N}$ dos números naturais (inteiros positivos) é fechado em relação à soma e produto de $\mathbb{Z}$, mas não é um subanel de $\mathbb{Z}$.*
3. *$\mathbb{C}$ é uma extensão de $\mathbb{R}$.*
4. *O anel $M_n(\mathbb{C})$ é uma extensão de $M_n(\mathbb{Z})$.*

De acordo com o resultado provado para grupos na secção anterior, se $B \subset A$ e B não é vazio, então $(B, +)$ é subgrupo de $(A, +)$ (*i.e.*, verifica (i) na Definição 1.5.1) se e só se é fechado em relação à *diferença*. Se B é fechado em relação à soma e produto de A, é evidente que verifica as propriedades (ii) e (iii) da Definição 1.5.1, simplesmente porque as suas operações são as do anel A. Concluímos imediatamente que:

Proposição 1.5.13. *Seja A um anel. Um subconjunto B é um subanel de A se e só se não é vazio, e é fechado em relação à diferença e ao produto.*

Se A e B são anéis, é claro que podemos formar a *soma directa* dos respectivos grupos aditivos. Mas é evidente que podemos definir de forma

análoga tanto a *soma* como o *produto*:

$$(a,b)+(a',b')=(a+a',b+b'),(a,b)(a',b')=(aa',bb'). \tag{1.5.1}$$

Deixamos como exercício verificar que o produto cartesiano $A \times B$ com as operações de soma e produto aqui referidas forma um anel, que dizemos ser a SOMA DIRECTA dos anéis A e B, e designamos por $A \oplus B$. Mais uma vez é claro que podemos formar somas directas de um número arbitrário mas finito de anéis, e deixamos para mais tarde a discussão do caso de um número *infinito* de anéis.

Exercícios.

1. Verifique se cada uma das seguintes estruturas algébricas é um anel. Em caso afirmativo, indique se se trata de um anel comutativo, se tem identidade, e se verifica a lei do corte para o produto. Em caso negativo, especifique as condições da Definição 1.5.1 que são violadas.
   (a) o conjunto dos inteiros múltiplos dum inteiro fixo m, com a soma e o produto usuais;
   (b) o conjunto das transformações lineares $T : \mathbb{R}^n \to \mathbb{R}^n$, com a soma usual e o produto de composição;
   (c) o conjunto das funções $f : \mathbb{R} \to \mathbb{R}$ com a soma usual e o produto de composição;
   (d) o conjunto dos inteiros não-negativos, com a soma e o produto usuais;
   (e) o conjunto dos reais irracionais, com a soma e o produto usuais;
   (f) o conjunto dos inteiros de Gauss $\mathbb{Z}[i]$, com a soma e o produto usuais;
   (g) o conjunto $\mathbb{R}[x]$[18] dos polinómios na variável x com coeficientes reais, ainda com a soma e o produto usuais.

2. Prove que $0 = -0$ num anel qualquer.

3. Complete a demonstração do teorema 1.5.6.

4. Seja A um conjunto com três elementos distintos, que designaremos por $0, 1$, e 2. De quantas maneiras pode definir operações de "adição" e "produto" em A de modo a obter um anel unitário, sendo 0 o zero do anel, e 1 a sua identidade?

5. Mostre que em geral a operação de diferença num qualquer anel não é nem comutativa nem associativa, mas verifique que existem anéis onde esta operação tem as duas propriedades referidas.

6. A equação $a + x = b$ tem exactamente uma solução em A. O que é que pode dizer sobre a equação $ax = b$? E sobre a equação $x = -x$?

[18] Veremos adiante que, se A é um anel, é possível definir o anel dos polinómios "na variável x" com coeficientes em A, o qual é normalmente designado por $A[x]$. Note-se que o símbolo $\mathbb{Z}[i]$ para o anel dos inteiros de Gauss usa a mesma ideia, já que um polinómio na unidade imaginária i se pode sempre reduzir ao 1º grau.

7. Suponha que A, B e C são anéis. Prove as seguintes afirmações:
   (a) O conjunto $A \times B$ com as operações definidas em 1.5.1 é um anel.
   (b) Se A e B têem mais de um elemento, então $A \oplus B$ tem divisores de zero.
   (c) Se A e B são unitários então $A \oplus B$ é unitário, e $(A \oplus B)^* = A^* \times B^*$.
   (d) $A \oplus B$ é isomorfo a $B \oplus A$, e $A \oplus (B \oplus C)$ é isomorfo a $(A \oplus B) \oplus C$.
   (e) $\phi : A \to B \oplus C$ é um homomorfismo de anéis se e só se $\phi(x) = (\phi_1(x), \phi_2(x))$, onde $\phi_1 : A \to B$ e $\phi_2 : A \to C$ são homomorfismos de anéis.

8. Sendo X um conjunto e A um anel, mostre que a classe de funções $f : X \to A$ é um anel com as operações "usuais" de soma e produto de funções.

9. Use o exercício anterior com $X = \{0, 1\}$ e $A = \mathbb{Z}_2$ para obter um exemplo de um anel com 4 elementos. Mostre que esse anel é isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

10. Seja $A = \{0, 1, 2, 3\}$ um conjunto com quatro elementos. Mostre que existe um corpo com suporte em A, sendo 0 o zero de A, e 1 a sua identidade.

11. Seja A um anel. Mostre que o conjunto das matrizes $n \times n$ com entradas em A, que se designa por $M_n(A)$, é um anel. Mostre ainda que, se A tem identidade, então $M_n(A)$ tem identidade.

12. Seja B um subanel de A. Mostre que os seguintes casos são todos possíveis:
   (a) A tem identidade e B não tem identidade.
   (b) A não tem identidade e B tem identidade.
   (c) A e B têm identidades distintas.
   (SUGESTÃO: recorra a subanéis apropriados de anéis de matrizes 2×2).

13. Dê um exemplo dum anel finito não-abeliano.

14. Mostre que qualquer subanel dum anel de divisão verifica a lei do corte para o produto, e em particular que qualquer subanel dum corpo contendo a identidade desse corpo é um domínio integral, mas não necessariamente um corpo.

15. Prove que a lei do corte para o produto é válida no anel A se e só se não existem em A divisores de zero.

16. Seja A um domínio integral. Diga se se tem necessariamente:
   (a) $x^2 = 1$ implica $x = 1$ ou $x = -1$;
   (b) $-1 \neq 1$.

17. Suponha que o anel A é uma extensão do corpo K, e que K contém a identidade de A. Prove que A é um espaço vectorial sobre K.

18. Determine os elementos invertíveis no anel $\mathbb{Z}[i]$ dos inteiros de Gauss.

19. Prove que qualquer domínio integral finito $\neq \{0\}$ é um corpo.

20. Mostre que $M_2(\mathbb{Z})^*$ é infinito.
(SUGESTÃO: mostre que $M_2(\mathbb{Z})^* = \{A \in M_2(\mathbb{Z}) : \det(A) = \pm 1\}$).

21. Suponha que B é um subanel de A. Verifique que:
   (a) o zero de B é o zero de A;
   (b) o simétrico de um elemento de B é o mesmo em B e em A.

   Suponha agora que A e B têm identidade.
   (c) É verdade que $B^* \subset A^*$?
   (d) É verdade que o inverso dum elemento em B^* é necessariamente o mesmo que o seu inverso em A^*? E se as identidades de A e B forem iguais?

1.6 Homomorfismos e Isomorfismos de Anéis

Na secção anterior introduzimos a definição de anel. Estudamos agora os homomorfismos e isomorfismos associados a esta definição. Naturalmente, estes são *funções* que têm como domínio e contradomínio conjuntos que são suportes de anéis, e que além disso *preservam* as operações algébricas dos anéis envolvidos. Observe que na definição seguinte usamos os mesmos símbolos para representar as operações algébricas de anéis distintos, apesar de estas operações serem em geral diferentes. Note também que um homomorfismo de anéis é um caso especial de homomorfismo de grupos.

Definição 1.6.1. Sejam A e B anéis, e $\phi : A \to B$ uma função. ϕ é um HOMOMORFISMO DE ANÉIS se:

(i) $\phi(a_1 + a_2) = \phi(a_1) + \phi(a_2), \forall a_1, a_2 \in A$;

(ii) $\phi(a_1 a_2) = \phi(a_1)\phi(a_2), \forall a_1, a_2 \in A$.

Um ISOMORFISMO DE ANÉIS é um homomorfismo bijectivo[19]. Dizemos que os anéis A e B são *isomorfos* se existe algum isomorfismo $\phi : A \to B$.

Exemplos 1.6.2.

1. *Designamos o* complexo conjugado *de $z = x + iy$ por $\overline{z} = x - iy$. Temos*

$$\overline{z + w} = \overline{z} + \overline{w}, \qquad \overline{zw} = \overline{z}\,\overline{w}.$$

De acordo com a definição anterior, a função $\phi : \mathbb{C} \to \mathbb{C}$ dada por $\phi(z) = \overline{z}$ é um automorfismo do anel $\mathbb{C}$.

[19] Tal como no caso dos monóides e dos grupos, também usaremos os termos *epimorfismo* e *monomorfismo* de anéis, bem como *endomorfismo* e *automorfismo* de anéis, cujas definições são óbvias.

2. *Considere-se a função* $\phi : \mathbb{C} \to M_2(\mathbb{R})$ *definida por*

$$\phi(x+iy) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

Verificamos que

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} + \begin{pmatrix} x' & -y' \\ y' & x' \end{pmatrix} = \begin{pmatrix} x+x' & -y-y' \\ y+y' & x+x' \end{pmatrix},$$

ou seja,

$$\phi(x+iy) + \phi(x'+iy') = \phi((x+iy)+(x'+iy')),$$

e, analogamente,

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} \begin{pmatrix} x' & -y' \\ y' & x' \end{pmatrix} = \begin{pmatrix} xx'-yy' & -(xy'+x'y) \\ xy'+x'y & xx'-yy' \end{pmatrix},$$

ou seja,

$$\phi(x+iy)\phi(x'+iy') = \phi((x+iy)(x'+iy')).$$

Temos portanto que ϕ *é um homomorfismo de anéis. Neste caso,* ϕ *é injectivo (*i.e.*, é um* monomorfismo*) mas não é sobrejectivo.*

3. *Seja* $\phi : \mathbb{Z} \to \mathbb{Z}_2$ *dado por* $\phi(n) = 0$*, se* n *é par, e* $\phi(n) = 1$*, se* n *é ímpar. É fácil verificar que* ϕ *é ainda um homomorfismo de anéis sobrejectivo (*i.e.*, é um* epimorfismo*), mas não é injectivo.*

4. *Seja* $\phi : \mathbb{R} \to M_2(\mathbb{R})$ *dado por*

$$\phi(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}.$$

Deve ser evidente que ϕ *é um monomorfismo (mas não-sobrejectivo)*[20]*.*

5. *Sejam* $S, T : \mathbb{R}^n \to \mathbb{R}^n$ *duas transformações lineares. Definimos a soma* $S+T$ *e composição* ST *por*

$$(S+T)(x) = S(x) + T(x), \qquad (ST)(x) = S(T(x)).$$

Já observámos que com estas operações o conjunto das transformações lineares de $\mathbb{R}^n$ *em* $\mathbb{R}^n$ *é um anel, que designamos aqui por* $L(\mathbb{R}^n, \mathbb{R}^n)$*. Fixada uma base para* $\mathbb{R}^n$*, seja* $\mathcal{M}(S)$ *a matriz da transformação linear* S *relativa a esta base. É claro que* $\mathcal{M}(S)$ *é uma matriz* $n \times n$ *com entradas reais, e sabemos da Álgebra Linear que a função* $\mathcal{M} : L(\mathbb{R}^n, \mathbb{R}^n) \to M_n(\mathbb{R})$ *verifica as identidades*

$$\mathcal{M}(S+T) = \mathcal{M}(S) + \mathcal{M}(T), \qquad \mathcal{M}(ST) = \mathcal{M}(S)\mathcal{M}(T).$$

Temos portanto que $\mathcal{M}$ *é um isomorfismo de anéis.*

---

[20] Note-se que as matrizes da forma $\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$ constituem um subanel de $M_2(\mathbb{R})$ com identidade distinta da identidade do anel $M_2(\mathbb{R})$.

Em certos casos, quando existe um homomorfismo injectivo $\phi : A \to B$ "óbvio", usamos o mesmo símbolo para designar a e $\phi(a)$. Apesar de esta prática não ser recomendável de um ponto de vista estritamente lógico, é frequentemente inevitável para não sobrecarregar excessivamente a notação utilizada. Casos típicos desta prática são a representação do *real* a, do *complexo* $(a, 0)$, e do polinómio constante $p(x) = a$ pelo mesmo símbolo.

Como qualquer homomorfismo de anéis $\phi : A \to B$ é igualmente um homomorfismo entre os grupos aditivos $(A, +)$ e $(B, +)$, podemos reescrever a Proposição 1.4.3 na forma:

Proposição 1.6.3. *Seja $\phi : A \to B$ um homomorfismo de anéis. Então:*

(i) $\phi(0) = 0$*;*

(ii) $\phi(-a) = -\phi(a)$*.*

De acordo com a definição de homomorfismo e o resultado anterior, podemos dizer que qualquer homomorfismo $\phi : A \to B$ "preserva" somas, produtos, o zero, e os simétricos. Deve no entanto observar-se que certas noções associadas ao produto não são mantidas da forma mais simples. Em particular, um dos exemplos acima mostra que, quando A tem identidade 1 para o produto, não se segue que $\phi(1)$ seja a identidade de B. Veremos nos exercícios como enunciar um resultado correcto desta natureza.

O estudo da equação $\phi(x) = y$ não sofre alterações significativas, quando comparado com o estudo feito atrás para grupos. O *núcleo* de ϕ é naturalmente o conjunto das soluções da equação homogénea $\phi(x) = 0$, *i.e.*,

$$N(\phi) = \{x \in A : \phi(x) = 0\},$$

e o conjunto $\phi(A)$ é o conjunto dos $y \in B$ para os quais a equação $\phi(x) = y$ tem soluções $x \in A$. Claro que ϕ é sobrejectivo se e só se $\phi(A) = B$, e ϕ é injectivo, como já vimos, se e só se $N(\phi) = \{0\}$.

Basta-nos reescrever o Teorema 1.4.10 em notação aditiva para obter:

Teorema 1.6.4. *Se $\phi : A \to B$ um homomorfismo de anéis, temos:*

(i) $\phi(x) = \phi(x')$ *se e só se* $x - x' \in N(\phi)$*;*

(ii) ϕ *é injectivo se e só se* $N(\phi) = \{0\}$*;*

(iii) se x_0 é uma solução particular de $\phi(x) = y_0$, a solução geral é $x = x_0 + n$, com $n \in N(\phi)$.

O exemplo seguinte é uma ilustração muito simples deste resultado.

Exemplo 1.6.5.

No caso do homomorfismo $\phi : \mathbb{Z} \to \mathbb{Z}_2$ dado por $\phi(n) = 0$, se n é par, e $\phi(n) = 1$, se n é ímpar, o respectivo núcleo é o conjunto dos inteiros pares. Como $\phi(0) = 0$ e $\phi(1) = 1$, temos

$$\begin{aligned} \phi(x) = 0 &\Leftrightarrow x = 2n, \text{ com } n \in \mathbb{Z}, \\ \phi(x) = 1 &\Leftrightarrow x = 1 + 2n, \text{ com } n \in \mathbb{Z}. \end{aligned}$$

Dado um homomorfismo $\phi : A \to B$, sabemos que $N(\phi)$ e $\phi(A)$ são subgrupos dos grupos aditivos $(A, +)$ e $(B, +)$. Podemos verificar facilmente que neste caso esses subgrupos são na realidade subanéis.

Proposição 1.6.6. *Se $\phi : A \to B$ é um homomorfismo, então $N(\phi)$ é um subanel de A, e $\phi(A)$ é um subanel de B. Em particular, se ϕ é injectivo, então A é isomorfo a $\phi(A)$.*

Demonstração. Temos apenas a provar que $N(\phi)$ e $\phi(A)$ são fechados em relação aos respectivos produtos.

Se $b_1, b_2 \in \phi(A)$, existem $a_1, a_2 \in A$ tais que $b_1 = \phi(a_1)$ e $b_2 = \phi(a_2)$. É portanto óbvio que

$$b_1 b_2 = \phi(a_1)\phi(a_2) = \phi(a_1 a_2) \in \phi(A),$$

e $\phi(A)$ é fechado em relação ao produto de B, logo é um subanel de B.

Se $a_1, a_2 \in N(\phi)$, temos $\phi(a_1) = \phi(a_2) = 0$. Concluímos que

$$\phi(a_1 a_2) = \phi(a_1)\phi(a_2) = 0 \cdot 0 = 0,$$

donde $a_1 a_2 \in N(\phi)$, e $N(\phi)$ é fechado em relação ao produto de A, logo é um subanel de A.

Finalmente, é evidente que, se ϕ é injectivo, então ϕ é um isomorfismo entre A e $\phi(A)$. □

Exemplos 1.6.7.

1. *Considere-se mais uma vez o homomorfismo $\phi : \mathbb{C} \to M_2$ definido por*

$$\phi(x + iy) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

Do teorema, concluímos que o conjunto das matrizes da forma

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

é um subanel de $M_2(\mathbb{R})$, isomorfo ao corpo dos complexos.

2. *No caso do homomorfismo $\phi : \mathbb{R} \to M_2$ dado por*

$$\phi(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix},$$

observamos que M_2 contém igualmente um subanel isomorfo ao corpo dos reais. Note-se no entanto que M_2 contém vários subanéis distintos, todos eles isomorfos ao corpo dos reais. Na realidade, o exemplo anterior, quando restrito aos reais, conduz ao homomorfismo injectivo $\phi : \mathbb{R} \to M_2$ dado por $\phi(x) = xI$, onde I é a matriz identidade.

Vimos que o núcleo de qualquer homomorfismo de grupos é um subgrupo de tipo especial, dito um subgrupo normal, ou invariante. Analogamente, o núcleo $N(\phi)$ de um homomorfismo de anéis $\phi : A \to B$ é um subanel de A de tipo especial. A sua especificidade prende-se com o seu comportamento face ao produto. Não só $N(\phi)$ é fechado em relação ao produto, como qualquer subanel, mas também para que o produto ab pertença a $N(\phi)$ basta que *apenas um* dos factores a ou b pertença a $N(\phi)$. Para verificar esta afirmação, observe que

$$a_1a_2 \in N(\phi) \Leftrightarrow \phi(a_1a_2) = 0 \Leftrightarrow \phi(a_1)\phi(a_2) = 0,$$

e que o produto $\phi(a_1)\phi(a_2)$ é nulo sempre que um dos factores $\phi(a_1)$ ou $\phi(a_2)$ é nulo, *i.e.*, desde que pelo menos um dos elementos a_1 ou a_2 pertença ao núcleo $N(\phi)$. É este o conteúdo da

Proposição 1.6.8. *Se $a \in N(\phi)$ e a' é um qualquer elemento de A, então tanto aa' como $a'a$ pertencem a $N(\phi)$.*

Os subanéis com esta propriedade são distinguidos como se segue.

Definição 1.6.9. Seja A um anel e I um subanel de A. Dizemos que I é um IDEAL de A se para qualquer $a \in A$ e $b \in I$ se tem $ab, ba \in I$.

Nem todos os subanéis de um anel fixo são ideais desse anel. Os exemplos abaixo ilustram ambas as possibilidades.

Exemplos 1.6.10.

1. *É claro que $\mathbb{Z}$ é um subanel de $\mathbb{R}$ (a diferença e o produto de inteiros é sempre um inteiro). No entanto, $\mathbb{Z}$ não é um ideal de $\mathbb{R}$ (o produto dum inteiro por um real arbitrário não é necessariamente um inteiro).*

2. *Seja $A = \mathbb{Z}$ e I o conjunto dos inteiros pares. É claro que I é um subanel de $\mathbb{Z}$ (a diferença e o produto de inteiros pares é um inteiro par) mas I é além disso um ideal de $\mathbb{Z}$ (o produto de qualquer inteiro por um inteiro par é sempre um inteiro par). Veremos mais adiante que* todos *os subanéis de $\mathbb{Z}$ são automaticamente seus ideais. Note-se também que I é igualmente um subanel de $\mathbb{R}$, mas é evidente que* não *é um ideal de $\mathbb{R}$.*

3. *Qualquer anel A tem pelo menos os ideais $\{0\}$ e A.*

4. *Em certos casos, um anel tem apenas os ideais mencionados acima. Na verdade, é isso que ocorre com qualquer corpo. Para o verificar, suponha-se que K é um corpo, e $I \subset K$ é um ideal. Se I contém um elemento $x \neq 0$ (*i.e.*, se $I \neq \{0\}$), então $xx^{-1} = 1 \in I$ (porque $x \in I$ e $x^{-1} \in K$). Mas neste caso qualquer elemento $y \in K$ pertence a I, porque $y = 1y$, onde $1 \in I$ e $y \in K$.*

Num anel não-abeliano A podemos considerar subanéis para as quais a condição de ideal se verifica apenas num dos lados. Assim, um IDEAL ESQUERDO de A é um subanel $B \subset A$ tal que para qualquer $a \in A$ e $b \in B$ se tem $ab \in B$. Da mesma forma, um IDEAL DIREITO de A é um subanel $B \subset A$ tal que para qualquer $a \in A$ e $b \in B$ se tem $ba \in B$. É claro que $I \subset A$ é um ideal num sentido da Definição 1.6.9 se e só se é, simultaneamente, um ideal esquerdo e um ideal direito. Para um anel abeliano, todas estas noções coincidem. Os ideais laterais desempenham um papel bem menos importante que os ideais bilaterais, por causa da Proposição 1.6.8.

Exercícios.

1. Seja A um anel e $\phi, \psi : A \to A$ endomorfismos. Mostre que a composição $\phi \circ \psi$ é um endomorfismo, mas que $\phi + \psi$ pode não o ser. Em particular, mostre que o conjunto dos endomorfismos de A, designado por $\mathrm{End}(A)$, com a operação de composição, forma um *monóide*.

2. Seja A um anel e $\phi, \psi : A \to A$ automorfismos. Mostre que a composição $\phi \circ \psi$ e a inversa ϕ^{-1} são automorfismos. Em particular, mostre que o conjunto de todos os automorfismos de A, designado por $\mathrm{Aut}(A)$, com a operação de composição, forma um *grupo*.

3. Qualquer inteiro m é da forma $m = 3n+r$, onde n é o quociente da divisão de m por 3 e r o respectivo resto. Note que n e r são únicos desde que $0 \leq r < 3$. Prove que a função $\phi : \mathbb{Z} \to \mathbb{Z}_3$ dada por $\phi(m) = r$ é um homomorfismo de anéis. Qual é o núcleo deste homomorfismo?

4. Prove que, se A e B são anéis, A tem identidade 1, e $\phi : A \to B$ é um homomorfismo então $\phi(1)$ é a identidade de $\phi(A)$, não necessariamente a identidade de B. Mostre também que, se $a \in A^*$, então $\phi(a)^{-1}$ é o inverso de $\phi(a)$ em $\phi(A)$, não necessariamente o inverso de $\phi(a)$ em B. Em particular, $\phi(a)$ pode não ser invertível em B.

5. Prove que, se A e B são anéis, A tem identidade 1, e $\phi : A \to B$ é um isomorfismo então $\phi(1)$ é a identidade de B. Mostre também que, se $a \in A^*$, então $\phi(a)^{-1}$ é o inverso de $\phi(a)$ em B e $\phi(A^*) = B^*$.

6. Prove que, se A e B são anéis, A tem identidade 1, e $\phi : A \to B$ é um isomorfismo, então B é um corpo (respectivamente, anel de divisão, domínio integral) se e só se A é um corpo (respectivamente, anel de divisão, domínio integral).

7. Mostre que, se K é um corpo, A é um anel, e $\phi : K \to A$ é um homomorfismo, então A contém um subanel isomorfo a K, ou ϕ é identicamente 0.

8. Existem subanéis de $\mathbb{Z} \oplus \mathbb{Z}$ que não são ideais de $\mathbb{Z} \oplus \mathbb{Z}$?

9. Determine $\mathrm{End}(A)$ quando $A = \mathbb{Z}$ e $A = \mathbb{Q}$.
(SUGESTÃO: Calcule $\phi(1)$ e proceda por indução.)

10. Determine End($\mathbb{R}$).
(SUGESTÃO: Mostre que $\phi(x) \geq 0$ quando $x \geq 0$, donde ϕ é crescente.)

11. Determine todos os homomorfismos $\phi : \mathbb{C} \to \mathbb{C}$ que satisfazem $\phi(x) \in \mathbb{R}$ quando $x \in \mathbb{R}$.
(SUGESTÃO: Mostre que se $\phi(1) \neq 0$ e $x = \phi(i)$ então $x^2 = -1$.)

12. Suponha que I é um ideal de $M_2(\mathbb{R})$ e $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I$. Prove que $I = M_2(\mathbb{R})$.

13. Determine todos os ideais de $M_2(\mathbb{R})$.

14. Seja A um anel comutativo com identidade e considere o anel $M_n(A)$. Mostre que a aplicação $\det : M_n(A) \to A$ definida por

$$\det(B) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)},$$

onde $B = (a_{ij})$, preserva produtos (mas não é um homomorfismo de anéis). Conclua que a matriz $B \in M_n(A)^*$ se e só se $det(B) \in A^*$.

15. Suponha que $C \subset B \subset A$ onde B é um subanel de A.

(a) Se C é um subanel de B, pode concluir que C é um subanel de A?

(b) Se C é um ideal de B, pode concluir que C é um ideal de A?

(c) Se C é um ideal de A, pode concluir que C é um ideal de B?

16. Prove que, se A é um anel abeliano unitário e os seus únicos ideais são $\{0\}$ e A, então A é necessariamente um corpo. Se A for não abeliano, será que A é necessariamente um anel de divisão?

17. Sejam A e B anéis unitários.

(a) Suponha que J é um ideal de $A \oplus B$, e prove que $(a, b'), (a', b) \in J \Rightarrow (a, b) \in J$.

(b) Prove que $K \subset A \times B$ é um ideal de $A \oplus B$ se e só se $K = K_1 \times K_2$, onde K_1 é um ideal de A, e K_2 é um ideal de B.

18. Este exercício refere-se à decomposição de anéis em somas directas.

(a) Suponha, primeiro, que A é isomorfo a $B \oplus C$, e prove que existem ideais I e J de A tais que $I \cap J = \{0\}$, e $I + J = \{i + j : i \in I, j \in J\} = A$.

(b) Suponha agora que existem ideais I e J de A tais que $I \cap J = \{0\}$, e $I + J = A$. Prove que A é isomorfo a $I \oplus J$. Para este fim, proceda como se indica a seguir:

(i) Mostre que, se $i \in I$, $j \in J$ e $i + j = 0$, então $i = j = 0$.

(ii) Mostre que, se $i \in I$ e $j \in J$, então $ij = 0$.

(iii) Mostre que a função $\phi : I \oplus J \to A$, dada por $\phi(i, j) = i + j$, é um isomomorfismo de anéis.

1.7 Os Quaterniões

O corpo dos complexos é uma extensão do corpo dos reais. Este último é uma extensão do corpo dos racionais, que são por sua vez uma extensão do anel dos inteiros. É curioso investigar se é possível criar uma extensão do corpo dos complexos, e de procurar determinar até que ponto é que este processo de extensões sucessivas tem um fim "natural". No século passado, W. R. Hamilton [21] colocou a si próprio esta questão.

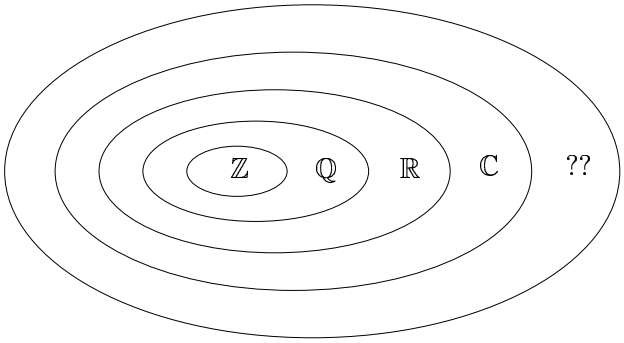


Figura 1.7.1: O problema de Hamilton.

Numa primeira tentativa (que durou 20 anos!), Hamilton procurou utilizar "números" da forma $a+ib+cj$, onde $a, b, c \in \mathbb{R}$ e i é a unidade imaginária, *i.e.*, em linguagem moderna, procurou criar um corpo com suporte em $\mathbb{R}^3$ e contendo um subcorpo isomorfo ao corpo dos complexos. Depois de muitas tentativas para atribuir um valor "razoável" ao produto ij (na forma $ij = a + bi + cj$), viu-se na necessidade de introduzir um "número" adicional k, de forma a ter $ij = k$. No seguimento das suas investigações, descobriu a existência não de um corpo mas de um anel de divisão, com suporte em $\mathbb{R}^4$, e cujos elementos se dizem QUATERNIÕES, ou NÚMEROS DE HAMILTON.

Designamos os elementos da base canónica do espaço vectorial $\mathbb{R}^4$ por

$$\mathbf{1} = (1,0,0,0), \qquad \boldsymbol{i} = (0,1,0,0), \qquad \boldsymbol{j} = (0,0,1,0), \qquad \boldsymbol{k} = (0,0,0,1).$$

O quaternião $\boldsymbol{q} = (a,b,c,d)$ escreve-se portanto $\boldsymbol{q} = a\mathbf{1} + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$, onde a, b, c, d são números reais. Desejamos naturalmente que as funções injectivas $\phi : \mathbb{R} \to \mathbb{R}^4$ e $\psi : \mathbb{C} \to \mathbb{R}^4$ definidas por $\phi(x) = x\mathbf{1}$ e $\psi(x+iy) = x\mathbf{1}+y\boldsymbol{i}$, sejam homomorfismos, de modo a poder identificar o conjunto $\mathbb{R}$ com o conjunto $\{(x,0,0,0) : x \in \mathbb{R}\}$, e o conjunto $\mathbb{C}$ com o conjunto $\{(x,y,0,0) : x, y \in \mathbb{R}\}$.

Dado um quaternião $\boldsymbol{q} = a\mathbf{1} + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$, $a\mathbf{1}$ diz-se a parte *real* de $\boldsymbol{q}$, e $b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k}$ a parte *vectorial*. Tal como no caso dos complexos, escreveremos

[21] William Rowan Hamilton (1805-1865), grande astrónomo e matemático irlandês. Hamilton foi também muito precoce: aos 5 anos sabia ler grego, hebraico e latim, e aos 10 anos estava familiarizado com meia dúzia de línguas orientais!

normalmente $\boldsymbol{q} = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$, deixando o quaternião $\mathbf{1}$ subentendido. A SOMA DE QUATERNIÕES é a soma vectorial usual em $\mathbb{R}^4$. É portanto evidente que, se x e y são reais e z e w complexos, se tem

$$\phi(x+y) = \phi(x) + \phi(y), \qquad \psi(z+w) = \psi(z) + \psi(w).$$

O PRODUTO DE QUATERNIÕES é mais difícil de descobrir. Observamos primeiro que, se entendermos o produto dum real a pelo quaternião $\boldsymbol{q}$ como o produto $(a\mathbf{1})\boldsymbol{q}$, então esse produto reduz-se ao produto habitual dum escalar por um vector, e em particular os quaterniões formam um espaço vectorial de dimensão 4 sobre os reais. Por outro lado, devemos também ter

$$\boldsymbol{i}^2 = -\mathbf{1}, \tag{1.7.1}$$

pois

$$\boldsymbol{i}^2 = \psi(i)\psi(i) = \psi(i^2) = \psi(-1) = \phi(-1) = -\phi(1) = -\mathbf{1}.$$

Hamilton descobriu as identidades:

$$\boldsymbol{ij} = \boldsymbol{k}, \qquad \boldsymbol{jk} = \boldsymbol{i}, \qquad \boldsymbol{ki} = \boldsymbol{j}. \tag{1.7.2}$$

Com base nestas identidades, é possível calcular os produtos $\boldsymbol{ji}$, $\boldsymbol{kj}$, $\boldsymbol{ik}$, $\boldsymbol{j}^2$ e $\boldsymbol{k}^2$ usando apenas a propriedade associativa do produto e a relação $\boldsymbol{i}^2 = -\mathbf{1}$. A título de exemplo, note-se que

$$\boldsymbol{ij} = \boldsymbol{k} \Rightarrow \boldsymbol{i}(\boldsymbol{ij}) = \boldsymbol{ik} \Rightarrow (\boldsymbol{ii})\boldsymbol{j} = \boldsymbol{ik} \Rightarrow (-1)\boldsymbol{j} = \boldsymbol{ik} \Rightarrow -\boldsymbol{j} = \boldsymbol{ik}.$$

Deixamos os detalhes destes cálculos como exercício, mas indicamos aqui os resultados:

$$\boldsymbol{j}^2 = \boldsymbol{k}^2 = -\mathbf{1}, \qquad \boldsymbol{ji} = -\boldsymbol{k}, \qquad \boldsymbol{kj} = -\boldsymbol{i}, \qquad \boldsymbol{ik} = -\boldsymbol{j}. \tag{1.7.3}$$

Observe que o produto de quaterniões *não* é comutativo, e portanto os quaterniões não formam um corpo. A partir das identidades (1.7.1), (1.7.2), e (1.7.3) é possível calcular o produto de dois quaterniões arbitrários usando as propriedades associativa e distributiva. Em vez de fazer isso, preferimos inverter todo o processo e definir formalmente o anel dos quaterniões.

Teorema 1.7.1. *O conjunto $\mathbb{R}^4$ com a adição vectorial usual e o produto de $\boldsymbol{q} = a + \boldsymbol{v}$ e $\boldsymbol{r} = b + \boldsymbol{w}$ definido por*[22]

$$(a + \boldsymbol{v})(b + \boldsymbol{w}) = ab - (\boldsymbol{v} \cdot \boldsymbol{w}) + a\boldsymbol{w} + b\boldsymbol{v} + \boldsymbol{v} \times \boldsymbol{w}, \tag{1.7.4}$$

é um anel de divisão (que não é um corpo) e que se designa por $\mathbb{H}$.

[22] Nesta fórmula, $(\boldsymbol{v} \cdot \boldsymbol{w})$ e $\boldsymbol{v} \times \boldsymbol{w}$ designam os habituais produtos *interno* e *externo* da álgebra vectorial moderna. Na realidade, estas operações e a notação $\boldsymbol{i}$, $\boldsymbol{j}$ e $\boldsymbol{k}$ para a base canónica de $\mathbb{R}^3$ são vestígios do trabalho de Hamilton.

Demonstração. Antes de mais observamos que o produto $(\boldsymbol{q}, \boldsymbol{r}) \to \boldsymbol{qr}$ definido por (1.7.4) coincide com o produto por escalares se $\boldsymbol{q} \in \mathbb{R}$, e ainda que é uma aplicação $\mathbb{R}$-bilinear: dados $a_1, a_2 \in \mathbb{R}$, $\boldsymbol{q}, \boldsymbol{q}_1, \boldsymbol{q}_2 \in \mathbb{R}^4$ e $\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r} \in \mathbb{R}^4$ temos

$$(a_1\boldsymbol{q}_1 + a_2\boldsymbol{q}_2)\boldsymbol{r} = a_1(\boldsymbol{q}_1\boldsymbol{r}) + a_2(\boldsymbol{q}_2\boldsymbol{r}), \quad \boldsymbol{q}(a_1\boldsymbol{r}_1 + a_2\boldsymbol{r}_2) = a_1(\boldsymbol{q}\boldsymbol{r}_1) + a_2(\boldsymbol{q}\boldsymbol{r}_2).$$

Verificamos também que, com a notação $\boldsymbol{i}$, $\boldsymbol{j}$ e $\boldsymbol{k}$ para a base canónica de $\mathbb{R}^3$, são válidas as identidades (1.7.1), (1.7.2), e (1.7.3).

Para obter a associatividade da operação usamos agora a bilinearidade e as identidades (1.7.1), (1.7.2), e (1.7.3), para calcular os produtos

$$(a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{k})\left((b_0 + b_1\boldsymbol{i} + b_2\boldsymbol{j} + b_3\boldsymbol{k})(c_0 + c_1\boldsymbol{i} + c_2\boldsymbol{j} + c_3\boldsymbol{k})\right),$$

e

$$\left((a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{k})(b_0 + b_1\boldsymbol{i} + b_2\boldsymbol{j} + b_3\boldsymbol{k})\right)(c_0 + c_1\boldsymbol{i} + c_2\boldsymbol{j} + c_3\boldsymbol{k}),$$

e verificar assim que coincidem.

Finalmente, é claro que

$$\boldsymbol{q}\mathbf{1} = \mathbf{1}\boldsymbol{q} = \boldsymbol{q},$$

e deixamos como exercício verificar que para todo o quaternião $\boldsymbol{q} = (a, b, c, d)$ não-nulo são válidas as identidades:

$$\boldsymbol{q}\boldsymbol{q}' = \boldsymbol{q}'\boldsymbol{q} = \mathbf{1}, \text{ onde } \boldsymbol{q}' = \frac{a - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k}}{a^2 + b^2 + c^2 + d^2}. \tag{1.7.5}$$

□

É ainda interessante constatar que os quaterniões formam um anel isomorfo a um subanel do anel $M_4(\mathbb{R})$ das matrizes 4×4 com entradas reais, o que fornece uma *realização concreta* deste anel de divisão, e outra demonstração do Teorema 1.7.1. Para isso considerem-se as matrizes 2×2:

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad N = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

que permitem definir a transformação linear $\rho : \mathbb{R}^4 \to M_4(\mathbb{R})$ através de

$$\begin{aligned} \rho(\mathbf{1}) &= \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}, \\ \rho(\boldsymbol{i}) &= \begin{pmatrix} N & 0 \\ 0 & -N \end{pmatrix}, \\ \rho(\boldsymbol{j}) &= \begin{pmatrix} 0 & M \\ -M & 0 \end{pmatrix}, \\ \rho(\boldsymbol{k}) &= \begin{pmatrix} 0 & N \\ N & 0 \end{pmatrix} \end{aligned}$$

(como $\{\mathbf{1}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ é uma base de $\mathbb{R}^4$ esta aplicação linear fica bem definida). Temos então:

Proposição 1.7.2. *A aplicação $\rho : \mathbb{H} \to M_4(\mathbb{R})$ é um homomorfismo injectivo, logo o anel das matrizes 4×4 com entradas reais possui um subanel isomorfo ao anel de divisão $\mathbb{H}$.*

A demonstração deste resultado é um simples exercício de cálculo. Veremos mais adiante que do Teorema Fundamental da Álgebra ("*Qualquer polinómio com coeficientes complexos de grau maior que zero tem pelo menos uma raiz complexa*") se segue que não existe nenhum corpo que seja uma extensão de $\mathbb{C}$ e simultaneamente um espaço vectorial de dimensão finita sobre $\mathbb{R}$ ou $\mathbb{C}$. Por outras palavras, sabemos hoje que o problema original de Hamilton *não* tem solução.

Exercícios.

1. Demonstre, a partir da fórmula (1.7.4) para o produto de dois quaterniões, que são válidas as relações (1.7.1), (1.7.2) e (1.7.3).

2. Verifique, a partir de (1.7.4), da bilinearidade e das identidades (1.7.1), (1.7.2), e (1.7.3), a fórmula (1.7.5) para o inverso de um quaternião $\boldsymbol{q} \neq 0$.

3. Para um quaternião $\boldsymbol{q} = a\mathbf{1}+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k}$ definimos o seu complexo conjugado por $\overline{\boldsymbol{q}} = a\mathbf{1} - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k}$. Mostre que:
   (a) A aplicação $\phi : \mathbb{H} \to \mathbb{H}$ definida por $\phi(\boldsymbol{q}) = \overline{\boldsymbol{q}}$ é um automorfismo de $(\mathbb{H}, +)$. O que é que pode dizer sobre $\phi(\boldsymbol{q}_1\boldsymbol{q}_2)$?
   (b) $\boldsymbol{q}\overline{\boldsymbol{q}} = ||\boldsymbol{q}||^2$ onde $||\boldsymbol{q}|| = \sqrt{a^2+b^2+c^2+d^2}$ designa a norma do quaternião $\boldsymbol{q} = a\mathbf{1} + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$;
   (c) O inverso de um quaternião $\boldsymbol{q}$ é o quaternião $\boldsymbol{q}^{-1} = \frac{\overline{\boldsymbol{q}}}{||\boldsymbol{q}||^2}$.

4. Mostre directamente que o conjunto formado por todas as combinações lineares das matrizes 4×4:
$$\begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}, \quad \begin{pmatrix} N & 0 \\ 0 & -N \end{pmatrix}, \quad \begin{pmatrix} 0 & M \\ -M & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & N \\ N & 0 \end{pmatrix},$$
é um subanel de $M_4(\mathbb{R})$.

5. Demonstre a Proposição 1.7.2, *i.e.*, mostre que a aplicação $\rho : \mathbb{H} \to M_4(\mathbb{R})$ é um homomorfismo injectivo.

6. Descreva todas as soluções da equação $x^2 = -1$ no anel $\mathbb{H}$ dos quaterniões.

7. Suponha que $\{1\} \subset K \subset L \subset M$ são corpos, com M uma extensão de L, e L uma extensão de K. Sabemos que M é um espaço vectorial sobre K e sobre L, e que L é por sua vez um espaço vectorial sobre K. Suponha que a dimensão de M sobre L é m, e a dimensão de L sobre K é n. Prove que a dimensão de M sobre K é mn. Conclua que uma extensão não-trivial de $\mathbb{C}$ tem pelo menos dimensão 4 sobre $\mathbb{R}$.

8. Considere os quaterniões da forma $a+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k}$, com $a, b, c, d \in \mathbb{Z}$. Verifique que estes quaterniões formam um anel não-abeliano, que não é de divisão, mas onde a lei do corte é válida.

9. Verifique que o conjunto formado pelos elementos invertíveis do anel referido no exercício anterior formam um grupo não-abeliano com oito elementos, designado por $\mathbb{H}_8$. Determine todos os subgrupos de $\mathbb{H}_8$, e identifique todos os subgrupos normais.

1.8 Simetrias

Ilustramos nesta secção a forma como a teoria dos grupos pode ser utilizada para formalizar a noção de simetria, considerando sobretudo o caso das simetrias de figuras geométricas planas. Para isso, começamos por notar que uma "figura plana" é formalmente um conjunto $\Omega \subset \mathbb{R}^2$, e vamos chamar SIMETRIA de Ω a uma função $\boldsymbol{f} : \mathbb{R}^2 \to \mathbb{R}^2$ que *preserva as distâncias* entre pontos de $\mathbb{R}^2$, *i.e.*, tal que

$$||\boldsymbol{f}(\boldsymbol{x}) - \boldsymbol{f}(\boldsymbol{y})|| = ||\boldsymbol{x} - \boldsymbol{y}||, \qquad \forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^2,$$

e que transforma o conjunto Ω nele próprio, *i.e.*, tal que

$$\boldsymbol{f}(\Omega) = \Omega.$$

Exemplo 1.8.1.

Se Ω é o círculo unitário de raio 1 e centro na origem, é fácil ver que qualquer rotação do plano em torno da origem é uma simetria de Ω. Analogamente, qualquer reflexão do plano numa recta que passe pela origem é também uma simetria de Ω.

As simetrias do plano, ou mais geralmente as simetrias de $\mathbb{R}^n$, são as funções $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$ que preservam distâncias, e que por isso se dizem *isometrias*.

Exemplos 1.8.2.

1. *Qualquer translação é uma isometria do plano.*
2. *Qualquer rotação é uma isometria do plano.*
3. *Qualquer reflexão (numa linha ou num ponto) é uma isometria do plano.*

O nosso próximo objectivo é classificar todas as isometrias de $\mathbb{R}^n$. Para isso, começamos por estudar as isometrias $\boldsymbol{f}$ que mantêm fixa a origem, *i.e.*, tais que $\boldsymbol{f}(\boldsymbol{0}) = \boldsymbol{0}$.

Proposição 1.8.3. *Se $\boldsymbol{f}(\mathbf{0}) = \mathbf{0}$, então as seguintes afirmações são equivalentes:*

(i) $\boldsymbol{f}$ *é uma isometria,* i.e.*,*

$$||\boldsymbol{f}(\boldsymbol{x}) - \boldsymbol{f}(\boldsymbol{y})|| = ||\boldsymbol{x} - \boldsymbol{y}||, \ \forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n;$$

(ii) $\boldsymbol{f}$ *preserva produtos internos,* i.e.*,*[23]

$$\boldsymbol{f}(\boldsymbol{x}) \cdot \boldsymbol{f}(\boldsymbol{y}) = \boldsymbol{x} \cdot \boldsymbol{y}, \forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n.$$

Demonstração. Supomos primeiro que $\boldsymbol{f}$ é uma isometria, e notamos que

$$||\boldsymbol{x}|| = ||\boldsymbol{x} - \mathbf{0}|| = ||\boldsymbol{f}(\boldsymbol{x}) - \boldsymbol{f}(\mathbf{0})|| = ||\boldsymbol{f}(\boldsymbol{x})||.$$

Além disso, temos

$$\begin{aligned} ||\boldsymbol{f}(\boldsymbol{x}) - \boldsymbol{f}(\boldsymbol{y})||^2 &= ||\boldsymbol{f}(\boldsymbol{x})||^2 + ||\boldsymbol{f}(\boldsymbol{y})||^2 - 2\boldsymbol{f}(\boldsymbol{x}) \cdot \boldsymbol{f}(\boldsymbol{y}), \\ ||\boldsymbol{x} - \boldsymbol{y}||^2 &= ||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2 - 2\boldsymbol{x} \cdot \boldsymbol{y}. \end{aligned}$$

Como por hipótese $||\boldsymbol{f}(\boldsymbol{x}) - \boldsymbol{f}(\boldsymbol{y})|| = ||\boldsymbol{x} - \boldsymbol{y}||$, e já provámos acima que $||\boldsymbol{x}|| = ||\boldsymbol{f}(\boldsymbol{x})||$, é imediato que $\boldsymbol{f}(\boldsymbol{x}) \cdot \boldsymbol{f}(\boldsymbol{y}) = \boldsymbol{x} \cdot \boldsymbol{y}$, para quaisquer $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$. Concluímos portanto que (i) implica (ii).

Deixamos como exercício a demonstração de que (ii) implica (i). □

Continuando a considerar apenas isometrias que mantêm fixa a origem, mostramos em seguida que estas isometrias são necessariamente transformações lineares.

Proposição 1.8.4. *Se $\boldsymbol{f}$ é uma isometria, e $\boldsymbol{f}(\mathbf{0}) = \mathbf{0}$, então $\boldsymbol{f}$ é uma transformação linear.*

Demonstração. Seja $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ a base canónica de $\mathbb{R}^n$. e $\boldsymbol{v}_k = \boldsymbol{f}(\boldsymbol{e}_k)$. Os vectores $\boldsymbol{v}_k$ são *unitários* (porque $||\boldsymbol{v}_k|| = ||\boldsymbol{f}(\boldsymbol{e}_k)|| = ||\boldsymbol{e}_k|| = 1$) e *ortogonais* (porque $\boldsymbol{v}_i \cdot \boldsymbol{v}_j = \boldsymbol{f}(\boldsymbol{e}_i) \cdot \boldsymbol{f}(\boldsymbol{e}_j) = \boldsymbol{e}_i \cdot \boldsymbol{e}_j$). Portanto, os vectores $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ formam igualmente uma base de $\mathbb{R}^n$ (porquê?).

Seja agora $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$, onde $\boldsymbol{y} = \boldsymbol{f}(\boldsymbol{x})$. Sendo $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ e $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ bases de $\mathbb{R}^n$, existem escalares $x_1, \ldots, x_n$ e $y_1, \ldots, y_n$ tais que

$$\boldsymbol{x} = \sum_{k=1}^{n} x_k \boldsymbol{e}_k, \qquad \boldsymbol{y} = \sum_{k=1}^{n} y_k \boldsymbol{v}_k.$$

Deve ser claro que $x_k = \boldsymbol{x} \cdot \boldsymbol{e}_k$ e $y_k = \boldsymbol{y} \cdot \boldsymbol{v}_k$, e como

$$\boldsymbol{y} \cdot \boldsymbol{v}_k = \boldsymbol{f}(\boldsymbol{x}) \cdot \boldsymbol{f}(\boldsymbol{e}_k) = \boldsymbol{x} \cdot \boldsymbol{e}_k,$$

[23] Designamos nesta secção, por "$\cdot$" o produto interno usual de $\mathbb{R}^n$.

temos $x_k = y_k$, donde

$$\boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{f}(\sum_{k=1}^{n} x_k \boldsymbol{e}_k) = \sum_{k=1}^{n} y_k \boldsymbol{v}_k = \sum_{k=1}^{n} x_k \boldsymbol{f}(\boldsymbol{e}_k),$$

logo $\boldsymbol{f}$ é uma transformação linear. □

As isometrias tais que $\boldsymbol{f}(\mathbf{0}) = \mathbf{0}$ são, como acabámos de ver, transformações lineares. É pois natural caracterizar estas funções em termos da sua representação matricial. Para isso, recordamos que a matriz $n \times n$ se diz *ortogonal* se $A^T A = I$, ou seja, se $A^{-1} = A^T$. (Recorde-se igualmente que como $\det(A^T) = \det(A)$, temos ainda $[\det A]^2 = \det A^T \det A = \det(A^T A) = \det I = 1$, donde $\det A = \pm 1$).

Proposição 1.8.5. *Se $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$, as seguintes afirmações são equivalentes:*

(i) $\boldsymbol{f}$ é uma isometria e $\boldsymbol{f}(\mathbf{0}) = \mathbf{0}$;

(ii) $\boldsymbol{f}$ é uma transformação linear, e a matriz de $\boldsymbol{f}$ na base canónica é ortogonal.

Demonstração. (i) ⇒ (ii). Sendo A a matriz de $\boldsymbol{f}$ na base canónica, temos $A = (a_{ij})$, onde $\boldsymbol{v}_j = \sum_{i=1}^{n} a_{ij} \boldsymbol{e}_i$. Por palavras, a coluna j da matriz A é formada pelas componentes do vector $\boldsymbol{v}_j$ na base canónica. Como os vectores $\boldsymbol{v}_j$ são unitários e ortogonais, temos

$$\boldsymbol{v}_j \cdot \boldsymbol{v}_k = \sum_{i=1}^{n} a_{ij} a_{ik} = \begin{cases} 1 & \text{se} \quad j = k, \\ \\ 0 & \text{se} \quad j \neq k, \end{cases}$$

ou seja, $A^T A = I$, e a matriz A é ortogonal.

(ii) ⇒ (i). Exercício. □

As transformações lineares que são isometrias dizem-se simplesmente transformações *ortogonais*. Podemos agora caracterizar completamente as isometrias de $\mathbb{R}^n$.

Teorema 1.8.6. *Se $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$, as seguintes afirmações são equivalentes:*

(i) $\boldsymbol{f}$ é uma isometria,

(ii) existe uma transformação ortogonal $\boldsymbol{g} : \mathbb{R}^n \to \mathbb{R}^n$ e $\boldsymbol{a} \in \mathbb{R}^n$ tal que $\boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{a} + \boldsymbol{g}(\boldsymbol{x})$.

Demonstração. (i) $\Rightarrow$ (ii). Seja $\boldsymbol{f}$ uma isometria, e $\boldsymbol{a} = \boldsymbol{f}(0)$. A função $\boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{f}(\boldsymbol{x}) - \boldsymbol{a}$ satisfaz $\boldsymbol{g}(\mathbf{0}) = \mathbf{0}$ e é uma isometria:

$$||\boldsymbol{g}(\boldsymbol{x}) - \boldsymbol{g}(\boldsymbol{y})|| = ||\boldsymbol{f}(\boldsymbol{x}) - \boldsymbol{f}(\boldsymbol{y})|| = ||\boldsymbol{x} - \boldsymbol{y}||.$$

De acordo com a Proposição 1.8.5, $\boldsymbol{g}$ é uma transformação ortogonal.

(ii) $\Rightarrow$ (i). Se $\boldsymbol{g}$ é uma transformação ortogonal, sabemos que $\boldsymbol{g}$ é uma isometria. É imediato que, se $\boldsymbol{a} \in \mathbb{R}^n$, então $\boldsymbol{a} + \boldsymbol{g}(\boldsymbol{x})$ é uma isometria. □

As transformações ortogonais $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$ formam um grupo $O(n, \mathbb{R})$, a que se chama GRUPO ORTOGONAL. O determinante de uma transformação ortogonal $\boldsymbol{f}$ só pode ser 1 ou -1, como foi observado acima, e as transformações ortogonais $\boldsymbol{f}$ com determinante 1 formam um subgrupo do grupo ortogonal, designado por $SO(n, \mathbb{R})$ e dito GRUPO ORTOGONAL ESPECIAL. Aos elementos de $SO(n, \mathbb{R})$ chamamos ROTAÇÕES PRÓPRIAS ou simplesmente ROTAÇÕES.

As isometrias $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$ formam igualmente um grupo $E(n, \mathbb{R})$, dito o GRUPO DE SIMETRIA DE $\mathbb{R}^n$ ou GRUPO EUCLIDIANO, do qual os grupos ortogonal e ortogonal especial são subgrupos:

$$SO(n, \mathbb{R}) \subset O(n, \mathbb{R}) \subset E(n, \mathbb{R}).$$

Mais geralmente, se $\Omega \subset \mathbb{R}^n$, então as isometrias de $\mathbb{R}^n$ que são simetrias de Ω formam um grupo, que se diz GRUPO DE SIMETRIA de Ω. Podemos então falar das simetrias de Ω que são translações, transformações ortogonais, rotações, reflexões, etc.

Exemplos 1.8.7.

1. *Se $\Omega \subset \mathbb{R}^2$ é um rectângulo centrado na origem, com lados (de comprimentos distintos) paralelos aos eixos coordenados, então o respectivo grupo de simetria tem 4 elementos: a identidade, as reflexões nos eixos Ox e Oy, e a rotação de 180^o em torno da origem (que é igualmente a reflexão na origem). O grupo de simetria do rectângulo, dito frequentemente* GRUPO DE KLEIN*, é isomorfo ao produto directo $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

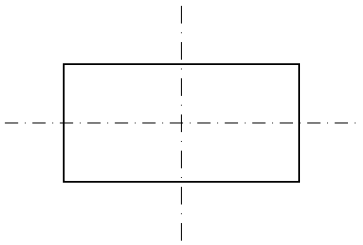


Figura 1.8.1: Simetrias dum rectângulo.

2. Se $\Omega \subset \mathbb{R}^2$ é um polígono regular com n lados centrado na origem, então o respectivo grupo de simetria, dito GRUPO DIEDRAL, *tem $2n$ elementos: as rotações de $2k\pi/n$ em torno da origem, as reflexões em relação às rectas que passam na origem e pelos vértices, e as reflexões em relação às rectas que passam pela origem e bissectam os lados do polígono. Costuma-se designar este grupo pelo símbolo D_n.*

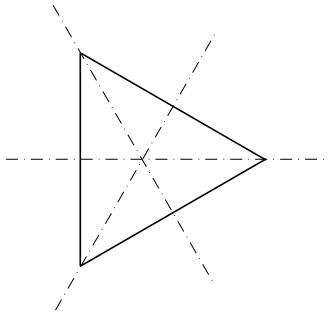


Figura 1.8.2: Simetrias dum triângulo equilátero.

Por exemplo, para um triângulo equilátero ($n = 3$), temos três simetrias rotacionais $\{R, R^2, R^3 = I\}$ geradas por uma rotação R de $2\pi/3$ em torno da origem. A representação matricial de R em relação à base canónica de $\mathbb{R}^2$ é

$$R = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

Temos ainda três eixos de simetria que dão origem a outras tantas reflexões $\{\sigma_1, \sigma_2, \sigma_3\}$. Escolhendo o triângulo com vértices em 1, $e^{\frac{2\pi i}{3}}$, e $e^{\frac{4\pi i}{3}}$, as representações matriciais destas reflexões em relação à base canónica são:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}, \quad \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{pmatrix}.$$

Deixamos como exercício verificar que o grupo de simetrias D_3 que se obtém desta forma é isomorfo ao grupo simétrico S_3.

Nos exemplos anteriores, as figuras eram limitadas. Também é muito interessante estudar grupos de simetria de figuras ilimitadas. Considere-se a título de exemplo um subconjunto do plano da forma:

$$\Omega = \{n\boldsymbol{a} + m\boldsymbol{b} : n, m \in \mathbb{Z}\},$$

onde $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^2$ são vectores fixos do plano linearmente independentes. Ω é um conjunto discreto de pontos, e podemos considerá-lo como um modelo simplificado de uma rede bidimensional de átomos, estendendo-se indefinidamente sobre todo o plano.

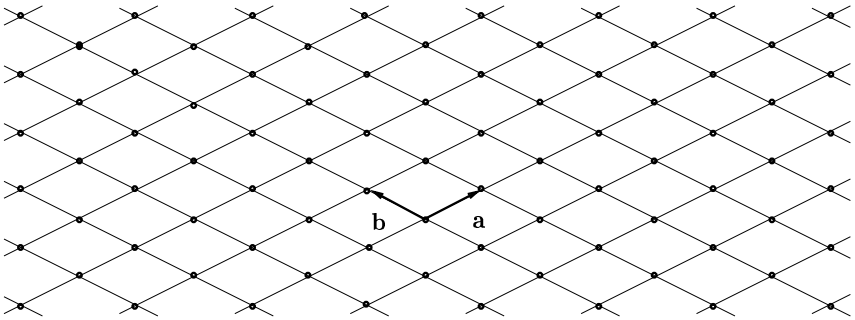


Figura 1.8.3: Uma rede bidimensional Ω.

Não determinaremos aqui os possíveis grupos de simetria de Ω, detendo-nos apenas no estudo de um problema mais simples, o de calcular as rotações que podem ser simetrias de Ω.

As simetrias de conjuntos ilimitados no plano são extensivamente utilizadas na decoração de superfícies planas: a contemplação de exemplos reais sugere que se baseiam na repetição de motivos enquadrados por uma das seguintes figuras: triângulo equilátero, quadrado, rectângulo ou hexágono[24].

Este facto sugere, ainda, que, se existe alguma rotação que seja simetria de Ω, então essa rotação só pode ser de 60^o, 90^o, 120^o ou 180^o (além naturalmente da identidade, que é igualmente uma rotação). Para vermos que de facto assim é, seja $\boldsymbol{f}$ uma rotação que é simetria de Ω, e A a sua representação matricial na base canónica, donde

$$A = \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix}.$$

Seja ainda B a representação matricial de $\boldsymbol{f}$ na base $\{\boldsymbol{a}, \boldsymbol{b}\}$. Nesta base todos os elementos de Ω têm coordenadas *inteiras* (na realidade, os pontos de Ω são precisamente os vectores de $\mathbb{R}^2$ cujas componentes na base $\{\boldsymbol{a}, \boldsymbol{b}\}$ são inteiros). Portanto, a própria matriz B tem entradas inteiras, já que estas entradas representam os vectores $\boldsymbol{f}(\boldsymbol{a})$ e $\boldsymbol{f}(\boldsymbol{b})$, que são necessariamente pontos de Ω. Escrevemos

$$B = \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix},$$

onde os n_{ij} são inteiros.

As matrizes A e B são *semelhantes*, *i.e.*, existe uma matriz não-singular S tal que $S^{-1}AS = B$. As matrizes $A - xI$ e $B - xI$ são igualmente

[24]Para uma discussão pormenorizada da noção de simetria e a sua relação com a arte, recomendamos a leitura da monografia de H. Weyl, *Symmetry*, Princeton University Press, Princeton N. J. (1952).

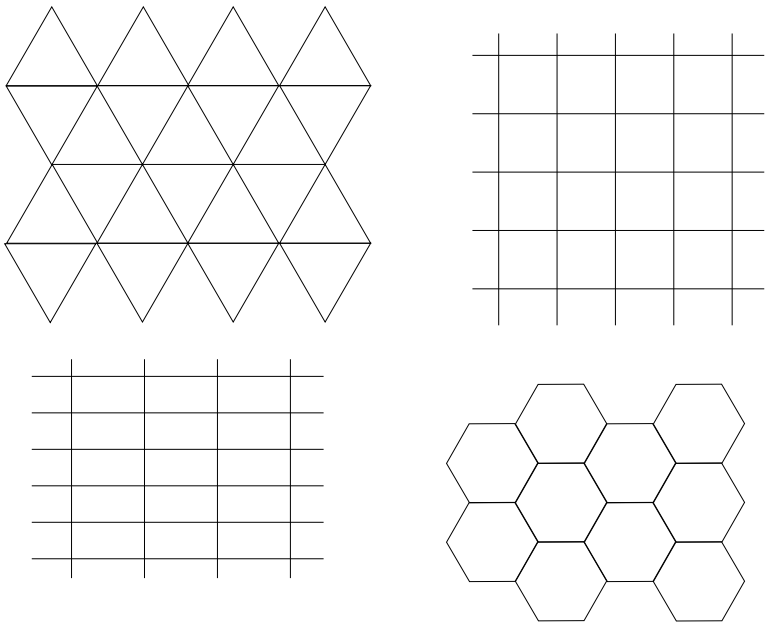


Figura 1.8.4: Simetrias de figuras planas ilimitadas.

semelhantes, e portanto têm o mesmo determinante, ou seja, os polinómios característicos de A e B são iguais. O polinómio característico de qualquer matriz C, de tamanho 2×2, é dado por

$$p(x) = \det(C - xI) = x^2 - \mathrm{tr}(C)x + \det(C)$$

(o termo independente do polinómio é o *determinante* de C, e o coeficiente de x é o simétrico da soma dos elementos da diagonal principal, ou seja, o simétrico do *traço* de C). Como as matrizes A e B têm o mesmo polinómio característico, podemos concluir que os respectivos traços são iguais, ou seja,

$$2\cos\theta = n_{11} + n_{22},$$

e, portanto, $2\cos\theta$ é um inteiro. É claro que $-1 \leq \cos\theta \leq 1$, donde concluímos que $\cos\theta$ só pode ser -1, $-1/2$, 0, $1/2$ ou 1, *i.e.*, que $\theta = 180^o,\ 120^o,\ 90^o,\ 60^o$ ou 0^o.

Existem muitos outros exemplos de importância prática onde a teoria dos grupos é fundamental para a compreensão de problemas relacionados com a ideia de simetria:

Exemplos 1.8.8.

1. *A exploração das simetrias de determinadas regiões ilimitadas do espaço conduz ao cálculo dos chamados* grupos cristalográficos*, utilizados na classificação dos cristais que ocorrem na natureza.*

2. Veremos no Capítulo 7 que é possível associar a cada polinómio um grupo de simetrias formado por permutações das suas raízes, dito grupo de Galois *do polinómio. A natureza do grupo de Galois de cada polinómio distingue os polinómios cujas raízes podem ser calculadas usando expressões envolvendo radicais e os coeficientes do polinómio, e permite explicar a razão pela qual não existem "fórmulas resolventes" para polinómios de grau superior a 4.*

*3. Uma das ideias mais básicas e mais frutuosas da Física é o "*princípio de objectividade*". De uma forma necessariamente vaga, este princípio exprime a ideia de que observadores diferentes, usando sistemas diferentes de coordenadas espaciais e temporais, descrevem os mesmos fenómenos físicos usando as mesmas leis físicas. De um ponto de vista matemático, este facto força as leis da natureza a ter como grupos de simetrias os grupos das transformações que relacionam as coordenadas usadas por diferentes observadores. De acordo com este princípio, e a título de exemplo, as leis da Mecânica e as leis do Electromagnetismo devem ter o mesmo grupo de simetria: foi a exploração cuidada desta ideia por Albert Einstein que o levou à descoberta da Teoria da Relatividade, seguramente uma das conquistas mais importantes da Ciência.*

Exercícios.

1. Suponha que $\boldsymbol{f} : \mathbb{R}^2 \to \mathbb{R}^2$ é uma isometria do plano. Mostre que:
   (a) Se $\boldsymbol{f}$ mantém fixos dois pontos $\boldsymbol{a}$ e $\boldsymbol{b}$ do plano, então $\boldsymbol{f}$ é uma reflexão na recta determinada por $\boldsymbol{a}$ e $\boldsymbol{b}$;
   (b) Se $\boldsymbol{f}$ mantém fixo um único ponto $\boldsymbol{a}$, então $\boldsymbol{f}$ é uma rotação em torno de $\boldsymbol{a}$;
   (c) Se $\boldsymbol{f}$ não mantém nenhum ponto fixo, então $\boldsymbol{f}$ é uma translação, seguida possivelmente de uma rotação ou de uma reflexão.

2. Conclua a demonstração da Proposição 1.8.3.

3. Conclua a demonstração da Proposição 1.8.5.

4. Mostre que o grupo de Klein é isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

5. Prove que os seguintes conjuntos de transformações são grupos:
   (a) As transformações ortogonais e rotações próprias $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$.
   (b) As isometrias $\boldsymbol{f} : \mathbb{R}^n \to \mathbb{R}^n$.
   (c) As simetrias de uma figura $\Omega \subset \mathbb{R}^n$.

6. Mostre que o grupo ortogonal especial $SO(n, \mathbb{R})$ é um subgrupo normal de $O(n, \mathbb{R})$, mas não é um subgrupo normal de $E(n, \mathbb{R})$.

7. Mostre que D_3 (o grupo de simetria do triângulo equilátero) é isomorfo a S_3.

8. Determine o grupo D_4 (grupo de simetria do quadrado).

9. A colmeia da Figura 1.8.4 admite como simetrias rotacionais as rotações de 60^o em torno dos centros das faces, bem como as rotações de 120^o em torno dos vértices. Como pode alterar esta figura de forma que as simetrias rotacionais sejam apenas as rotações de 120^o?

10. Seja $\boldsymbol{f} : \mathbb{R}^3 \to \mathbb{R}^3$ uma rotação. Mostre que existe uma base $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3\}$ de $\mathbb{R}^3$ em relação à qual a representação matricial de $\boldsymbol{f}$ é

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\operatorname{sen}\theta \\ 0 & \operatorname{sen}\theta & \cos\theta \end{pmatrix}.$$

A $\boldsymbol{v}_1$ chama-se *eixo de rotação* e a θ chama-se *ângulo de rotação* de $\boldsymbol{f}$. Consegue generalizar este resultado a dimensões $n > 3$?

Capítulo 2

Os Números Inteiros

2.1 Axiomática dos Inteiros

Já referimos várias vezes (sempre informalmente) o anel dos inteiros e algumas das propriedades destes números. Temos suposto que essas propriedades são conhecidas e "óbvias". Não é no entanto possível desenvolver teorias matemáticas precisas sem um cuidadoso exame dos seus fundamentos, e em particular sem distinguir entre os seus resultados aqueles que não são postos em causa pela teoria em questão, *i.e.*, os seus *axiomas*, e os que devem ser exibidos como consequência lógica dos primeiros, ou seja, os seus *teoremas*.

Desejamos agora indicar as propriedades dos números inteiros que consideraremos como axiomas. Note-se no entanto que a nossa exposição nunca será completamente formal. Em particular, continuaremos a usar noções e resultados da teoria dos conjuntos sem nos preocuparmos com a sua formulação rigorosa, já que esse é um assunto que sai claramente do âmbito da Álgebra. A escolha dos axiomas que servem de base a uma teoria dada é, até certo ponto, arbitrária, porque é sempre possível escolher axiomas *distintos*, mas logicamente *equivalentes*. Portanto, a escolha final é necessariamente ditada por critérios subjectivos de elegância, brevidade e economia de pensamento. Preferimos começar por um axioma que se encadeia facilmente com a nossa discussão anterior.

Axioma I. *Existe um domínio integral $\mathbb{Z}$, cujos elementos se designam por* INTEIROS.

O zero e a identidade de $\mathbb{Z}$ designam-se respectivamente por 0 e 1. Segue-se do capítulo anterior que um grande número de propriedades elementares dos inteiros é consequência directa do Axioma I. Em particular, as leis do corte para a soma e o produto e as regras dos sinais provadas anteriormente são válidas em $\mathbb{Z}$, assim como a afirmação $0 = -0$ que consta dos exercícios. Por outro lado, deve ser claro que o axioma acima não caracteriza completamente os inteiros; por exemplo, é impossível decidir com base neste

axioma se a afirmação $1 \neq -1$ é verdadeira ou falsa, ou decidir se os inteiros formam um conjunto finito ou infinito (porquê?). Para o completar, vamos agora examinar com algum cuidado certas propriedades dos *números naturais*.

De um ponto de vista intuitivo, os naturais são os inteiros que se obtêm de 1 por "adição sucessiva" de 1, ou seja, são os números da forma

$$1,\ 2 = 1 + 1,\ 3 = 2 + 1,\ 4 = 3 + 1, \ldots$$

Designando o conjunto dos naturais por $\mathbb{N}$, devemos portanto ter

$$1 \in \mathbb{N},\ \text{e } n \in \mathbb{N} \Rightarrow n + 1 \in \mathbb{N}.$$

Em geral, introduzimos a seguinte definição.

Definição 2.1.1. Se A é um anel unitário com identidade 1, um subconjunto $B \subset A$ diz-se INDUTIVO se:

(i) $1 \in B$;

(ii) $n \in B \Rightarrow n + 1 \in B$.

O próprio anel A é evidentemente um subconjunto indutivo de A. Portanto, $\mathbb{Z}$ é subconjunto indutivo de si próprio, e $\mathbb{N}$ não pode ser o único subconjunto indutivo de $\mathbb{Z}$. Mas na realidade a descrição heurística de $\mathbb{N}$ que demos acima sugere uma outra propriedade deste conjunto: a de que *qualquer* subconjunto indutivo de $\mathbb{Z}$ contém necessariamente *todos* os números naturais. Dito doutra forma, $\mathbb{N}$ é o *menor* subconjunto indutivo de $\mathbb{Z}$.

Regressemos ao contexto dum anel arbitrário A com identidade 1, para formalizar estas ideias. Já notámos que o próprio anel A é sempre indutivo. Por este motivo, a família de subconjuntos indutivos de A é necessariamente não-vazia. Seja agora $N(A)$ a *intersecção* de todos os subconjuntos indutivos de A. É imediato da sua própria definição que $N(A)$ está contido em qualquer subconjunto indutivo de A, observação a que damos o seguinte nome:

Teorema 2.1.2 (Princípio de Indução Finita). *Seja A um anel unitário. Então:*

(i) se $B \subset A$ é indutivo, então $N(A) \subset B$, e

(ii) se $B \subset N(A)$ é indutivo, então $B = N(A)$.

A afirmação anterior torna-se mais interessante tendo em conta o seguinte:

Proposição 2.1.3. *Se A é um anel unitário, então $N(A)$ é um subconjunto indutivo de A.*

Demonstração. Como 1 pertence a todos os subconjuntos indutivos de A, vemos que $1 \in N(A)$.

Suponha-se que $a \in N(A)$ e B é um qualquer subconjunto indutivo de A. Então $a \in B$ (porque $N(A) \subset B$) e $a+1 \in B$ (porque B é indutivo). Como B é arbitrário, segue-se que $a+1$ pertence a todos os subconjuntos indutivos de A, *i.e.*, $a+1 \in N(A)$. Concluímos, pois, que $N(A)$ é indutivo. □

De acordo com os dois resultados anteriores, $N(A)$ é indutivo e está contido em qualquer subconjunto indutivo de A. Por este motivo, introduzimos:

Definição 2.1.4. Chama-se a $N(A)$ o MENOR SUBCONJUNTO INDUTIVO de A. Se $A = \mathbb{Z}$, escrevemos $\mathbb{N}$ em lugar de $N(\mathbb{Z})$, e chamamos a $\mathbb{N}$ CONJUNTO DOS NÚMEROS NATURAIS.

Veremos adiante que a forma usual do princípio de indução finita é exactamente o Teorema 2.1.2 aplicado ao anel dos inteiros, e identificaremos todos os possíveis conjuntos $N(A)$ (a menos de um isomorfismo). Note-se também que a descrição (heurística) de $\mathbb{N}$ que demos no início desta secção se aplica igualmente ao conjunto $N(A)$, *i.e.*, este é sempre formado pelos elementos de A que se obtêm da identidade 1 por "adição sucessiva" da mesma identidade, observação a que eventualmente daremos uma forma mais precisa.

Exemplos 2.1.5.

1. *Se* $A = \mathbb{C}$, *então* $N(A) = \mathbb{N}$.
2. *Se* $A = M_n(\mathbb{C})$, *então* $N(A) = \{mI : m \in \mathbb{N}\}$.
3. *Se* $A = \mathbb{Z}_2$, *então* $N(A) = \mathbb{Z}_2$.

Sabemos que a soma e o produto de números naturais são ainda números naturais. Podemos agora *provar* esta afirmação, e simultaneamente generalizá-la a qualquer anel com identidade.

Proposição 2.1.6. $N(A)$ *é fechado em relação à soma e ao produto,* i.e.*,*

$$\forall a, b \in N(A), a + b \in A \text{ e } ab \in N(A).$$

Demonstração. Provamos apenas que a soma de dois elementos de $N(A)$ é um elemento de $N(A)$. Para isso, fixamos $a \in N(A)$ e definimos $B_a \subset N(A)$ como o conjunto dos elementos $b \in N(A)$ tais que $a + b \in N(A)$. Temos a provar que $B_a = N(A)$, o que faremos mostrando que B_a é indutivo, e aplicando o Teorema 2.1.2 (ii):

1. Como $N(A)$ é indutivo, é claro que $a + 1 \in N(A)$, e portanto $1 \in B_a$.
2. Se $b \in B_a$, então $a + b \in N(A)$ e temos $(a + b) + 1 \in N(A)$, pois $N(A)$ é indutivo. Como $(a + b) + 1 = a + (b + 1)$, segue-se que $b + 1 \in B_a$.

Concluímos que B_a é indutivo. Logo, pelo Teorema 2.1.2 (ii), $B_a = N(A)$. □

Regressando ao problema de caracterizar axiomaticamente o anel dos inteiros, recordamos que o conjunto dos inteiros é usual e informalmente descrito como formado pelos naturais, os simétricos dos naturais, e o zero, ou seja,

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\},$$

sendo subentendido que a lista acima não inclui repetições. O nosso próximo axioma precisa e refina esta propriedade dos inteiros.

Axioma II. *Se $m \in \mathbb{Z}$, verifica-se* exactamente um *dos seguintes três casos:*

$$m = 0 \text{ } ou \text{ } m \in \mathbb{N} \text{ } ou \text{ } -m \in \mathbb{N}.$$

Observe-se que, se neste axioma substituirmos o anel $\mathbb{Z}$ por outro anel A e o conjunto $\mathbb{N}$ pelo correspondente conjunto $N(A)$, obtemos uma afirmação claramente falsa para *todos* os outros exemplos de anéis que já mencionámos. Designaremos o conjunto $\mathbb{N} \cup \{0\}$ por $\mathbb{N}_0$.

Os Axiomas I e II que indicámos acima serão a base do nosso estudo dos inteiros. Mostraremos também que os axiomas usuais sobre números racionais e reais são consequência lógica destes axiomas para os inteiros. A questão de saber se estes axiomas são *completos*, ou seja, se permitem decidir a respeito de qualquer afirmação "razoável" sobre os inteiros se essa afirmação é *falsa ou verdadeira*, e *não-contraditórios*, no sentido de nunca levarem à conclusão de que determinada afirmação é simultaneamente *falsa e verdadeira*, é um problema profundo e delicado da alçada da Lógica Matemática, sobre o qual não poderemos debruçar-nos. Acrescente-se que uma pergunta equivalente a esta constituía o 2º problema de Hilbert[1]. A resolução que lhe foi dada por Kurt Gödel [2] em 1930 é um dos resultados mais surpreendentes e significativos da Matemática contemporânea. Gödel mostrou que estes dois atributos duma axiomática para os inteiros (completa e não-contraditória) são eles próprios contraditórios: qualquer sistema de axiomas para $\mathbb{Z}$ que seja não-contraditório admite afirmações cujo valor lógico não pode ser decidido com base nesses mesmos axiomas.

Por estranho que pareça alguém sequer colocar estas questões, o que é verdadeiramente surpreendente é o reflexo que o seu estudo veio a ter no mundo actual. Registe-se que os trabalhos de Gödel foram estudados pelo

[1] David Hilbert (1862-1943), matemático alemão, professor em Göttingen. A comunicação de Hilbert ao Congresso Internacional de Matemáticos em Paris (1900) incluía uma lista de 23 problemas que ele achava que deveriam ser considerados pelos matemáticos do século *XX* (ver *Bull. Am. Math. Soc.*, 2nd ser., vol. 8 (1901-02), pp. 437-79).

[2] Kurt Gödel (1906-1978) nasceu na Áustria e emigrou jovem para os EUA, onde se tornou membro do Institute for Advanced Study em Princeton. A sua resolução do 2º problema de Hilbert foi feita com 24 anos apenas.

matemático inglês Alan Turing, que os transformou em 1936 na sua teoria de um Autómato Universal (hoje dito Máquina de Turing). As ideias puramente teóricas de Turing, por sua vez, inspiraram o matemático húngaro John von Neumann [3], já então nos EUA, a colaborar no aperfeiçoamento dum Autómato Universal Electrónico, o ENIAC. Esta máquina e outras semelhantes, construídas na década que se seguiu à publicação do trabalho de Turing, foram, naturalmente, os precursores dos modernos computadores. Na realidade, os esforços destes dois homens não ficaram por aqui. A Segunda Guerra Mundial tinha entretanto começado em 1939, e Turing teve um papel central para os esforços militares ingleses, decifrando os códigos alemães baseados na utilização da máquina ENIGMA. Von Neumann e o ENIAC foram mobilizados para complexos problemas de cálculo de interesse militar, e em particular para o gigantesco projecto Manhattan. Este culminou na construção da bomba atómica, que com a destruição de Hiroxima e Nagasáqui pôs fim à guerra.

Exercícios.

1. Complete a demonstração do Teorema 2.1.2 e da Proposição 2.1.6.

2. Indique o menor subconjunto indutivo de cada um dos anéis com identidade mencionados no Exercício 1 da Secção 1.5.

3. Quais dos anéis referidos no problema anterior verificam um axioma análogo ao Axioma II se a expressão "exactamente um" for substituída por "um"?

4. Investigue a possibilidade de substituir a expressão "exactamente um" no Axioma II por "um", acrescentando-lhe:
   (a) $0 \notin \mathbb{N}$, ou
   (b) $n \in \mathbb{N} \Rightarrow -n \notin \mathbb{N}$, ou
   (c) $n \notin \mathbb{N} \Rightarrow -n \in \mathbb{N}$.

5. Um conjunto X diz-se INFINITO [4] se existe uma função $\Psi : X \to X$ injectiva mas não-sobrejectiva. Prove que $\mathbb{N}$ é infinito.

6. Prove que, se existe uma função bijectiva $\Psi : X \to Y$, então X é infinito se e só se Y é infinito.

7. Prove que, se $Y \subset X$ e Y é infinito, então X é também infinito. Em particular, prove que $\mathbb{Z}$ é infinito.

[3] John von Neumann (1903-1957), nasceu na Hungria, tendo ensinado em Berlim e Hamburgo antes de emigrar para os EUA. Foi conjuntamente com Einstein um dos primeiros membros do Institute for Advanced Study em Princeton. A ele devemos também a primeira axiomatização da noção de espaço de Hilbert, uma noção da Análise Funcional fundamental para a Mecânica Quântica.

[4] A noção de número de elementos (ou cardinal) dum conjunto é discutida no Apêndice.

2.2 Desigualdades

Parte das propriedades elementares dos números inteiros, racionais e reais dizem respeito à manipulação de *desigualdades*, ou seja, dizem respeito à *relação de ordem* existente nestes anéis. Nesta secção vamos estudar a ordenação dum anel de uma forma abstracta, exibindo propriedades que são comuns a todos os anéis ordenados. Procuraremos compreender os motivos pelos quais certos anéis podem ser ordenados, enquanto outros não o podem ser, e se a ordenação é única. Faremos ainda referência a propriedades de ordem que são características dos inteiros, e mostraremos que as propriedades de ordem deste anel são consequência dos axiomas mencionados na secção anterior. Parte das noções que utilizaremos podem ser definidas no contexto dum qualquer conjunto, sem referência a operações algébricas, e é isso que passamos a fazer.

Definição 2.2.1. Uma relação binária "$>$" num conjunto X diz-se uma RELAÇÃO DE ORDEM ESTRITA E TOTAL[5] se:

(i) *Transitividade*: $\forall x, y, z \in X$, $x > y$ e $y > z \Rightarrow x > z$.

(ii) *Tricotomia:* $\forall x, y \in X$, verifica-se exactamente um dos três casos $x > y$ ou $y > x$ ou $x = y$.

Note que a condição (ii) afirma que quaisquer dois elementos podem sempre ser comparados.

Dado um conjunto X com uma relação de ordem "$>$", que lemos "*maior que*", podem definir-se (tal como no caso dos números) as relações "$<$", "$\geq$" e "$\leq$", que se lêem da forma usual, por

- $a < b$ se e só se $b > a$;
- $a \geq b$ se e só se $a > b$ ou $a = b$;
- $a \leq b$ se e só se $a < b$ ou $a = b$.

Relembramos a seguir alguns conceitos elementares aplicáveis em qualquer conjunto ordenado X.

Definição 2.2.2. Se $Y \subset X$ e $x \in X$,

(i) x diz-se MAJORANTE (respectivamente MINORANTE) de Y se $x \geq y$ (respectivamente $x \leq y$), $\forall y \in Y$;

(ii) Y diz-se MAJORADO (respectivamente MINORADO) em X se Y tem pelo menos um majorante (respectivamente minorante) em X;

(iii) Y diz-se LIMITADO em X se é majorado e minorado em X.

[5] Para a definição e propriedades das relações de ordem em geral, ver o Apêndice.

Com estas noções temos ainda as noções usuais de máximo, mínimo, supremo e ínfimo, que passamos a enunciar para referência futura.

Definição 2.2.3. Se $Y \subset X$ e $x \in X$, então

(i) se x é majorante (respectivamente minorante) de Y e x pertence a Y, x diz-se MÁXIMO (respectivamente MÍNIMO) de Y, e designamos x por $\max Y$ (respectivamente $\min Y$);

(ii) o mínimo (respectivamente máximo) do conjunto dos majorantes de Y, se existir, chama-se SUPREMO (respectivamente ÍNFIMO) de Y, designado por $\sup Y$ (respectivamente $\inf Y$).

Os diferentes tipos de *intervalos* que nos são familiares podem ser generalizados a qualquer conjunto ordenado. Por exemplo, se $a, b \in X$, então

$$\begin{aligned}]a, +\infty[&= \{y \in X : y > a\}, \\ ]a, b] &= \{y \in X : a < y \leq b\}, \\ &\vdots \end{aligned}$$

Exemplo 2.2.4.

Seja $X = \mathbb{R}$ com a relação usual "$>$", e $Y =]-\infty, 0[$. Neste caso, Y não tem minorantes em $\mathbb{R}$, e portanto não pode ter ínfimo ou mínimo. O conjunto dos seus majorantes é o intervalo $[0, +\infty[$, com mínimo 0 que não pertence a Y. Claramente $0 = \sup Y$, e Y não tem máximo.

Se o conjunto X é o suporte dum anel, é natural considerar apenas relações de ordem que de algum modo respeitam as operações algébricas desse anel. Exigiremos no caso dum anel que

$$a > b \Longleftrightarrow a - b > 0,$$

i.e, que $a > b$ se e só se $a - b$ é *positivo*, e que a soma e o produto de elementos *positivos* seja um elemento *positivo*. É por isso mais conveniente descrever uma relação de ordem num anel em termos do conjunto dos seus elementos positivos.

Definição 2.2.5. O anel A diz-se um ANEL ORDENADO se existe um subconjunto A^+ em A que verifique:

(i) *Fecho em relação à soma e ao produto*: $a + b, ab \in A^+$, $\forall a, b \in A^+$.

(ii) *Tricotomia*: Para todo o $a \in A$ não-nulo verifica-se exactamente um dos casos $a \in A^+$ ou $-a \in A^+$.

Se A é um anel ordenado, definimos em A a relação "$>$" por

$$a > b \Longleftrightarrow a - b \in A^+$$

Em particular, temos $a > 0$ se e só se $a \in A^+$, e consequentemente dizemos que A^+ é o conjunto dos elementos *positivos* do anel A. Temos naturalmente $a < 0$ se e só se $-a \in A^+$, e por isso os elementos do conjunto $A^- = \{a \in A : -a \in A^+\}$ dizem-se *negativos*. Note-se que esta relação é efectivamente uma relação de ordem em A. A transitividade da relação "$>$" segue-se do fecho de A^+ em relação à soma, e a tricotomia de "$>$" é consequência imediata de (ii) na Definição 2.2.5.

Indicamos a seguir regras básicas para manipular desigualdades que são válidas em qualquer anel ordenado.

Proposição 2.2.6. *Seja A um anel ordenado. Para quaisquer $a, b, c \in A$, temos as seguintes propriedades:*

(i) $a > b \Longleftrightarrow a + c > b + c$;

(ii) $a > b \Longleftrightarrow -a < -b$;

(iii) $ab > 0 \Longleftrightarrow (a > 0 \text{ e } b > 0) \text{ ou } (a < 0 \text{ e } b < 0)$;

(iv) $ab < 0 \Longleftrightarrow (a > 0 \text{ e } b < 0) \text{ ou } (a < 0 \text{ e } b > 0)$;

(v) $ac > bc \Longleftrightarrow (a > b \text{ e } c > 0) \text{ ou } (a < b \text{ e } c < 0)$;

(vi) $a \neq 0 \Longleftrightarrow a^2 = aa > 0$.

Assim, uma boa parte das propriedades de ordem dos inteiros, racionais e reais são idênticas, porque são comuns a todos os anéis ordenados.

A demonstração destas propriedades é muito simples, e remetemo-la para os exercícios, exemplificando aqui apenas a demonstração da propriedade (i):

Demonstração. Pela Definição 2.2.5,

$$\begin{aligned} a + c > b + c &\Leftrightarrow (a + c) - (b + c) \in A^+ \\ &\Leftrightarrow a - b \in A^+ \Leftrightarrow a > b. \end{aligned}$$

□

É evidente das considerações acima que o anel dos inteiros pode ser ordenado fazendo $\mathbb{Z}^+ = \mathbb{N}$, o que corresponde à *ordenação usual* dos inteiros. A propriedade de tricotomia de $\mathbb{N}$ é exactamente o Axioma II sobre os inteiros, e já provámos que em qualquer anel com identidade o conjunto $N(A)$ é fechado em relação à soma e ao produto. Talvez mais interessante é verificar que a ordenação usual dos inteiros é a única possível neste anel. Para isso necessitamos de mais um resultado aplicável a qualquer anel ordenado A com identidade $1 \neq 0$ (*i.e.*, com mais de um elemento).

Teorema 2.2.7. *Se A é ordenado com identidade $1 \neq 0$, então $N(A) \subset A^+$.*

Demonstração. Temos apenas de provar que A^+ é indutivo e usar a definição de $N(A)$:

(a) Como $1 \neq 0$ e $1 = (1)(1) = 1^2$, segue-se da propriedade (vi) da Proposição 2.2.6 que $1 > 0$, *i.e.*, que $1 \in A^+$;

(b) Como A^+ é fechado em relação à adição,

$$a \in A^+ \Rightarrow a + 1 \in A.$$

Assim, A^+ é indutivo e concluímos que $N(A) \subset A^+$. □

É claro que existem anéis A para os quais $A^+ \neq N(A)$, ou seja, para os quais $N(A) \subsetneq A^+$. Exemplos óbvios são os anéis dos racionais e dos reais. No entanto, e como sugerimos acima, se A é o anel dos inteiros, então $N(A) = A^+$.

Teorema 2.2.8. *O anel dos inteiros só pode ser ordenado fazendo $\mathbb{Z}^+ = \mathbb{N}$.*

Demonstração. Suponha-se $\mathbb{Z}$ ordenado duma forma possivelmente diferente da usual, e seja $\mathbb{Z}^+$ o correspondente conjunto de inteiros "positivos". Sabemos do resultado anterior que $\mathbb{N} \subset \mathbb{Z}^+$. Resta-nos portanto provar que $\mathbb{Z}^+ \subset \mathbb{N}$.

Se $m \in \mathbb{Z}^+$, então $m \neq 0$ e $-m \notin \mathbb{Z}^+$, de acordo com a propriedade de tricotomia na Definição 2.2.5. Como $\mathbb{N} \subset \mathbb{Z}^+$, segue-se também que $-m \notin \mathbb{N}$. Finalmente, segue-se do Axioma II que, neste caso, $m \in \mathbb{N}$. □

Não se deve concluir do resultado anterior que a ordenação de um anel arbitrário é sempre única! Indicaremos nos exercícios desta secção um subanel de $\mathbb{R}$ que pode ser ordenado de maneiras distintas.

Como dissemos acima, os primeiros resultados desta secção mostram que uma boa parte das propriedades de ordem dos inteiros é comum aos anéis dos racionais e dos reais. O resultado anterior sugere por sua vez que as propriedades de ordem específicas dos inteiros resultam de, no caso $A = \mathbb{Z}$, termos $A^+ = N(A)$, *i.e.*, $\mathbb{Z}^+ = \mathbb{N}$. A título de exemplo, provamos que os inteiros positivos são os inteiros maiores ou iguais a 1, afirmação que se torna obviamente falsa se substituirmos a palavra "inteiros" por "racionais" ou "reais".

Proposição 2.2.9. $\mathbb{Z}^+ = \{m \in \mathbb{Z} : m \geq 1\}$.

Demonstração. Seja $S = \{m \in \mathbb{Z} : m \geq 1\}$. Se $m \in S$, então $m \geq 1$, e como $1 > 0$, temos que $m \geq 0$. Logo, $S \subset \mathbb{N}$.

É evidente que $1 \in S$ e que

$$1 > 0 \Rightarrow 1 + 1 > 1 + 0 = 1.$$

Portanto, se $m \in S$, então $m + 1 \geq 1 + 1 > 1$, donde $m + 1 \in S$, e S é indutivo. Pelo Princípio de Indução e pelo Teorema 2.2.8, $S = \mathbb{N} = \mathbb{Z}^+$. □

A proposição anterior é ainda equivalente a dizer que no anel dos inteiros $]0, +\infty[= [1, +\infty[$, ou que $]0, 1[= \emptyset$. Note-se que em $\mathbb{Q}$ e $\mathbb{R}$ o intervalo $]0, 1[$ é um conjunto infinito. Discutiremos outras propriedades de ordem específicas dos inteiros nos exercícios que se seguem e na secção seguinte.

A noção de valor absoluto (ou módulo) pode ser introduzida sem dificuldades num qualquer anel ordenado A.

Definição 2.2.10. Seja A um anel ordenado e $a \in A$. O VALOR ABSOLUTO ou MÓDULO de a designa-se por $|a|$ e define-se por $|a| = \max\{-a, a\}$.

Indicamos a seguir algumas das propriedades do valor absoluto que podem ser provadas directamente desta definição. A respectiva demonstração faz parte dos exercícios.

Proposição 2.2.11. *Para quaisquer $a, b \in A$, temos:*

(i) $-|a| \leq a \leq |a|$;

(ii) $|a + b| \leq |a| + |b|$;

(iii) $|ab| = |a||b|$.

Exercícios.

1. Complete a demonstração da Proposição 2.2.6.

2. Mostre que, se A é um anel com identidade $1 \neq 0$ e existe em A um elemento i tal que $i^2 = -1$, então A não pode ser ordenado.

3. Prove que, se $m \in \mathbb{Z}$, então $]m, m + 1[= \emptyset$ em $\mathbb{Z}$.

4. Prove que em $\mathbb{Z}$:

   (a) $m > n \Leftrightarrow m \geq n + 1$;

   (b) $mn = 1 \Leftrightarrow (m = n = 1)$ ou $(m = n = -1)$;

   (c) $m = \sup S$ se e só se $m = \max S$;

   (d) $m = \inf S$ se e só se $m = \min S$.

5. Prove a Proposição 2.2.11.

6. Mostre que em qualquer anel ordenado:

   (a) $|a| \leq |b| \Leftrightarrow -|b| \leq a \leq |b| \Leftrightarrow a^2 \leq b^2$;

   (b) $||a| - |b|| \leq |a - b|$;

7. Seja B um anel ordenado e $\phi : A \to B$ um isomorfismo de anéis. Mostre que A pode ser ordenado com $A^+ = \{a \in A : \phi(a) \in B^+\}$.

8. Seja $A = \{m + n\sqrt{2} : m, n \in \mathbb{Z}\}$. Mostre que A pode ser ordenado com uma ordenação distinta da usual (induzida de $\mathbb{R}$). De quantas maneiras distintas pode ordenar A? (SUGESTÃO: Note que $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$ é um automorfismo de A e utilize o exercício anterior.)

9. Mostre que, se o anel ordenado A é majorado ou minorado, então $A = \{0\}$.

10. Mostre que qualquer anel ordenado $A \neq \{0\}$ é infinito.

11. Mostre que a lei do corte para o produto é válida em qualquer anel ordenado.

12. O anel ordenado A diz-se ARQUIMEDIANO se e só se para quaisquer $a, b \in A$ com $a \neq 0$ existe $x \in A$ tal que $ax > b$. Prove que o anel dos inteiros é arquimediano.

2.3 Princípio de Indução

De acordo com a definição de $\mathbb{N}$ discutida na secção anterior, o conjunto dos naturais verifica o *princípio de indução*:

Teorema 2.3.1 (Princípio de Indução). *Se $S \subset \mathbb{Z}$ é um conjunto indutivo em $\mathbb{Z}$, então $\mathbb{N} \subset S$. Em particular, se $S \subset \mathbb{N}$, então $S = \mathbb{N}$.*

Tradicionalmente, uma demonstração "por indução" obedece ao seguinte esquema: dada uma proposição $\mathcal{P}(n)$, há que provar que $\mathcal{P}(1)$ é verdadeira, e demonstrar que, se $\mathcal{P}(n)$ é verdadeira, então $\mathcal{P}(n+1)$ é também verdadeira. A relação entre este procedimento e o Princípio de Indução é facilmente esclarecida introduzindo o conjunto

$$S = \{n \in \mathbb{N} : \mathcal{P}(n) \text{ é verdadeira}\}.$$

Temos então

- $(\mathcal{P}(1)$ é verdadeira$) \iff (1 \in S)$;
- $(\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)) \iff (n \in S \Rightarrow n + 1 \in S)$.

O argumento por indução habitual resume-se portanto a provar que o conjunto dos naturais para os quais determinada afirmação é verdadeira é um subconjunto indutivo de $\mathbb{N}$. Frequentemente não chegamos a mencionar explicitamente o conjunto S, mas isso não deve causar qualquer confusão.

Exemplo 2.3.2.

Dizemos que $n \in \mathbb{N}$ é par *(respectivamente,* ímpar*) se existe $k \in \mathbb{Z}$ tal que $n = 2k$ (respectivamente, $n = 2k + 1$). Para provar a afirmação "qualquer natural é par ou ímpar", consideramos $\mathcal{P}(n) =$"n par ou ímpar". Agora:*

(i) Se $n = 1$, temos $1 = 2 \cdot 0 + 1$, donde 1 é ímpar, e $\mathcal{P}(1)$ é verdadeira.

(ii) Se n é um natural tal que $\mathcal{P}(n)$ é verdadeira, temos $n = 2k$ ou $n = 2k+1$. Segue-se que $n+1 = 2k+1$ ou $n+1 = (2k+1)+1 = 2(k+1)$, e portanto $\mathcal{P}(n+1)$ é verdadeira.

Concluímos que $\mathcal{P}(n)$ é verdadeira para qualquer natural.

Aproveitaremos esta técnica de demonstração para provar mais algumas propriedades de ordem dos naturais e dos inteiros. Começamos pelo *princípio de boa ordenação.*

Teorema 2.3.3 (Princípio de Boa Ordenação). *Qualquer conjunto não vazio de naturais tem mínimo.*

Demonstração. Seja S um qualquer conjunto não vazio de naturais e considere a proposição

$$\mathcal{P}(n) =\text{"Se } S \text{ contém um natural } k \leq n, \text{ então } S \text{ tem mínimo"}.$$

Observe que o teorema a demonstrar é equivalente à afirmação (porquê?)

"$\mathcal{P}(n)$ é verdadeira para qualquer natural n".

Podemos pois utilizar o Princípio de Indução:

(i) $\mathcal{P}(1)$ é verdadeira, porque, se S contém um natural $k \leq 1$, então de acordo com a Proposição (2.2.9) temos $k = 1$, e 1 é obviamente o mínimo de S, porque é o mínimo de $\mathbb{N}$.

(ii) Suponha-se que $\mathcal{P}(n)$ é verdadeira para o natural n, e suponha-se que S contém um natural $k \leq n + 1$. Temos de provar que S tem mínimo. Se S contém algum natural $k \leq n$, segue-se de $\mathcal{P}(n)$ que S tem mínimo. Caso contrário, S contém um natural no intervalo $[1, n + 1]$, mas nenhum natural no intervalo $[1, n]$. Como sabemos que o intervalo $]n, n + 1[$ é vazio, concluímos que $n + 1$ é o mínimo de S.

□

Quando S é um conjunto de inteiros, temos

Teorema 2.3.4. *Qualquer conjunto não-vazio de inteiros tem mínimo (respectivamente, máximo) desde que seja minorado (respectivamente, majorado).*

Deixamos a demonstração deste teorema como exercício, mas provamos o resultado seguinte, que pode ser utilizado para fazer demonstrações por indução que "começam" num qualquer inteiro $k \neq 1$. Note-se, do argumento seguinte, que os Teoremas 2.3.3 e 2.3.4 são ocasionalmente de utilização mais prática do que o princípio de indução finita, e podem substituí-lo.

Proposição 2.3.5. *Se a afirmação $\mathcal{P}(n)$ é verdadeira para $n = k$ e se $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ para qualquer $n \geq k$, então $\mathcal{P}(n)$ é verdadeira para qualquer inteiro $n \geq k$.*

Demonstração. Seja

$$S = \{n \in \mathbb{Z} : n \geq k \text{ e } \mathcal{P}(n) \text{ é } \textit{falsa}\}.$$

Pretendemos provar que S é vazio, *i.e.*, que $\mathcal{P}(n)$ é verdadeira para qualquer $n \geq k$. Note-se que S é por definição minorado por k. Portanto, de acordo com o Teorema 2.3.4, se S é não-vazio tem necessariamente um elemento mínimo m. Além disso, como $m \in S$, segue-se que $m \geq k$.

Por hipótese $\mathcal{P}(k)$ é verdadeira, e portanto $k \notin S$, donde $m > k$. Considere-se agora o inteiro $m-1$. Como $m > k$, temos $m - 1 \geq k$. Como $m-1$ é menor que o mínimo de S, $m-1 \notin S$, ou seja, $\mathcal{P}(m-1)$ é verdadeira. Mas também por hipótese $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ para qualquer $n \geq k$ e portanto $\mathcal{P}(m)$ é verdadeira. Esta conclusão é absurda, porque m é elemento de S. Ou seja, S não pode ter mínimo, e por isso é necessariamente vazio. □

Em certas circunstâncias é mais conveniente utilizar ainda uma outra forma do princípio de indução. A título de exemplo, considere-se a sucessão a_n dos *números de Fibonacci*, constituída pelos naturais

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

Esta sucessão costuma ser introduzida como *a sucessão* a_n que satisfaz[6]:

$$a_0 = a_1 = 1, \text{ e } a_{n+1} = a_n + a_{n-1} \text{ para } n \geq 1. \tag{2.3.1}$$

É possível determinar uma expressão explícita para a sucessão de Fibonacci. Não nos detemos para examinar o processo do seu cálculo, mas a expressão é a seguinte:

$$a_n = \frac{5+\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{5-\sqrt{5}}{10}\left(\frac{1-\sqrt{5}}{2}\right)^n. \tag{2.3.2}$$

[6]Fibonacci, também conhecido por Leonardo de Pisa (1180-1250), chegou a esta sucessão, considerando o seguinte problema: Quantos casais de lebres existem ao fim de um ano se cada casal origina um novo casal ao fim de um mês que, por sua vez, passa a reproduzir-se ao fim de 2 meses.

Parece óbvio que a sucessão a_n acima definida deve ser a *única* que satisfaz (2.3.1). No entanto, a demonstração desta última afirmação não é tão simples como à primeira vista pode parecer. Convém antes do mais formalizar a noção de *sucessão* num qualquer conjunto X.

Definição 2.3.6. Uma SUCESSÃO de elementos do conjunto X é uma função $f : \mathbb{N} \to X$.

Quando discutimos sucessões, é tradicional escrever f_n em vez de $f(n)$, e falar da "sucessão $\{f_1, f_2, \dots\}$", "$\{f_n\}$", ou mesmo "f_n", em vez de mencionar "a sucessão f". Cometeremos frequentemente o mesmo abuso de linguagem (porque é que este hábito é um abuso de linguagem?).

Note-se também que, se k é um inteiro, então à função $g : [k, \infty[\cap\mathbb{Z} \to X$ corresponde a sucessão $f : \mathbb{N} \to X$ dada por $f(n) = g(n + k - 1)$. Por este motivo, dizemos que g é uma sucessão *definida em* $[k, \infty[$. A "sucessão de Fibonacci" mencionada acima é portanto uma sucessão definida em $[0, \infty[$.

O resultado que pretendemos demonstrar é o seguinte:

Proposição 2.3.7. *Se f é uma sucessão de naturais definida em $\mathbb{N}_0$, tal que $f_0 = f_1 = 1$ e $f_{n+1} = f_n + f_{n-1}$ para $n \geq 1$, então $f(n) = a(n)$, onde $a(n) = a_n$ é a sucessão definida por (2.3.2).*

Sendo $\mathcal{P}(n)$ a afirmação "$f(n) = a(n)$", temos de provar $\mathcal{P}(n)$ para qualquer inteiro $n \geq 0$. A dificuldade em empregar o habitual método de indução está em que, por razões evidentes, não conseguimos demonstrar que $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$, mas apenas que $(\mathcal{P}(n)$ e $\mathcal{P}(n-1)) \Rightarrow \mathcal{P}(n+1)$. Para tornar mais fácil a resolução deste problema e doutros semelhantes, introduzimos a seguinte forma do princípio de indução:

Teorema 2.3.8. *Seja S um conjunto de inteiros tal que*

(i) $k \in S$, e

(ii) para qualquer $n \geq k$, $[k, n] \subset S \Rightarrow [k, n + 1] \subset S$.

Então $[k, +\infty[\subset S$.

Em termos da proposição $\mathcal{P}(n) =$"$n \in S$", o resultado anterior diz que, se $\mathcal{P}(k)$ é verdadeira e se $\mathcal{P}(n)$ é verdadeira sempre que $\mathcal{P}(m)$ é verdadeira para (qualquer) m, $k \leq m < n$, (e não apenas para $m = n - 1$), então $\mathcal{P}(n)$ é verdadeira para qualquer $n \geq k$. A demonstração desta afirmação faz-se sem dificuldades de maior, a partir do princípio de boa ordenação, de forma semelhante à demonstração da Proposição 2.3.5.

Demonstração do Teorema 2.3.8. Seja $F = \{n \geq k : n \notin S\}$. Pretendemos provar que F é vazio. Se $F \neq \emptyset$, como F é por definição minorado, concluímos que F tem mínimo $m \geq k$.

Como $k \in S$, é claro que $m > k$. Portanto $m - 1 > k$, e o intervalo $[k, m-1]$ não contém nenhum elemento de F, porque todos os seus elementos são menores do que o mínimo de F. Por outras palavras, $[k, m-1] \subset S$. Segue-se da hipótese (ii) que $[k, m] \subset S$, e portanto $m \in S$, *i.e.*, $m \notin F$, o que é absurdo.

Concluímos que F não pode ter mínimo, donde F é vazio, ou seja, $[k, +\infty[\subset S$. □

O teorema anterior permite uma demonstração imediata da Proposição 2.3.7 que deixamos como exercício.

Este resultado, no entanto, não elimina totalmente as dificuldades lógicas com definições como (2.3.1). Esta é, na realidade, um exemplo duma definição *recursiva*, ou seja, duma definição que refere o objecto a definir na descrição que dá desse mesmo objecto. Como sabemos pelo menos desde que Epiménides de Creta se tornou famoso pela sua frase "Todos os homens de Creta são mentirosos", é possível criar paradoxos lógicos, ou afirmações cujo valor lógico não pode ser decidido, utilizando proposições que de algum modo se referem a elas próprias. Um exemplo já clássico é o *paradoxo de Bertrand Russell*[7], sugerido pela tentativa de definir o "*conjunto de todos os conjuntos*".

Observe-se que a definição "U é o conjunto de todos os conjuntos" é recursiva, porque U, sendo um conjunto, é um dos elementos que entram na sua própria composição, ou seja, U tem a estranha propriedade de ser elemento dele próprio, o que não é usual nos conjuntos que conhecemos! Se nos desagrada esta propriedade de U, podemos considerar em seu lugar o conjunto N dos conjuntos "normais", *i.e.*, dos que não são elementos deles próprios. Em símbolos,

$$N = \{C \in U : C \notin C\}.$$

A pergunta a pôr agora é simples: N é ou não um conjunto "normal"? Infelizmente, se supusermos que N é "normal" (*i.e.*, $N \notin N$) então N pertence ao conjunto dos conjuntos normais (*i.e.*, $N \in N$!). Se supusermos que N não é "normal", temos $N \in N$. Mas então N é um elemento do conjunto dos conjuntos normais, e portanto N é ele próprio normal ($N \notin N$!). Por outras palavras, não conseguimos atribuir um valor lógico à afirmação "$N \in N$".

A um nível superficial, a lição a tirar deste exemplo é simplesmente que é necessário algum cuidado com definições recursivas, afirmação que,

[7]Bertrand Russell (1872-1970) foi juntamente com Alfred N. Whitehead (1861-1947) autor do famoso tratado *Principia Mathematica* (3 vols., 1910-13), onde se tentavam formalizar de forma axiomática as noções fundamentais da aritmética. Este trabalho monumental foi sem dúvida o auge de um programa de formalizar a Matemática, a que se poderá chamar "logística", e que consistia em construir toda a Matemática através da dedução lógica a partir de um pequeno número de conceitos e princípios. Embora essa abordagem tenha falhado, devido aos trabalhos posteriores de Gödel, ela deu uma contribuição notável para a Lógica Matemática.

como dissemos acima, já era compreendida por alguns filósofos da Grécia Antiga. Mais prosaicamente, a mesma dificuldade surge quando se utilizam folhas de cálculo automático (*spreadsheets*), e se cria um circuito fechado de referências entre células da folha, ou quando se enuncia um "teorema" como o que se segue:

Teorema 2.3.9. *Esta afirmação é falsa...*

É intuitivamente claro que dificuldades deste tipo não podem surgir com definições semelhantes à utilizada para a sucessão de Fibonacci, e na realidade empregaremos frequentemente definições recursivas para introduzir noções fundamentais. Discutiremos vários exemplos na secção seguinte, e esboçaremos o processo formal que as sustenta no Apêndice a este texto. A um nível mais profundo, no entanto, as dificuldades lógicas com definições recursivas, ou mais geralmente com proposições que se referem a elas próprias, parecem inevitáveis e estão relacionadas com alguns dos problemas mais difíceis contemplados por matemáticos e filósofos. É possível dar uma definição (rigorosa!) de "definição rigorosa"? Podemos compreender o funcionamento da nossa própria inteligência? Como podemos conciliar o aspecto mecânico das deduções lógicas, espelhado no funcionamento dum programa de computador, com a infinita adaptabilidade que chamamos comportamento "inteligente"? Afinal de contas, e regressando à vida "prática", este é o problema central do desenvolvimento da Inteligência Artificial.

Exercícios.

1. Determine todos os subconjuntos indutivos de $\mathbb{Z}$.

2. Prove o Teorema 2.3.4.

3. Prove a Proposição 2.3.7.

4. Considere-se a afirmação (obviamente falsa!) "Todas as mulheres loiras têm olhos azuis". Qual é o erro da seguinte "demonstração" por indução? Designamos por $\mathcal{P}(n)$ a afirmação "Se num conjunto de n mulheres loiras existe uma com olhos azuis, então todas têm olhos azuis". Então:

   (a) $\mathcal{P}(1)$ é evidentemente verdadeira.

   (b) Suponha-se que $\mathcal{P}(n)$ é verdadeira, e considere-se um conjunto com $n+1$ mulheres loiras $L = \{M_1, \ldots, M_{n+1}\}$. Supomos que M_1 tem olhos azuis. Definimos $L_{n+1} = \{M_k : k \neq n+1\}$, e $L_n = \{M_k : k \neq n\}$. Como $\mathcal{P}(n)$ é verdadeira, todas as mulheres em L_n e L_{n+1} têm olhos azuis. Como $L = L_n \cup L_{n+1}$, todas as mulheres em L têm olhos azuis.

   (c) Como existe pelo menos uma mulher loira com olhos azuis, todas as mulheres loiras têm olhos azuis.

5. Uma outra variante do problema das mulheres loiras de olhos azuis é a seguinte. Considere-se a afirmação (obviamente falsa!) "Todas os grupos finitos

são abelianos". Temos a seguinte "demonstração" por indução: Seja G um grupo e designemos por $\mathcal{P}(n)$ a afirmação "Num subconjunto de G com n elementos, todos os elementos comutam".

(a) $\mathcal{P}(1)$ é evidentemente verdadeira.

(b) Suponha-se que $\mathcal{P}(n)$ é verdadeira, e considere-se um subconjunto de G com $n+1$ elementos $L = \{g_1, \ldots, g_{n+1}\}$. Designe-se ainda por $L_i = \{g_k : k \neq i\}$ o conjunto formado pelos elementos de L, à excepção do elemento i. Como $\mathcal{P}(n)$ é verdadeira, cada L_i é comutativo. Como os L_i esgotam os elementos de L, vemos que L é comutativo.

(c) Como G é finito, concluímos que G é comutativo.

6. A fórmula (2.3.2) para a sucessão de Fibonacci pode ser obtida determinando as sucessões da forma β^n que satisfazem a equação (2.3.1). Quais são as sucessões de inteiros que satisfazem

$$b_{n+1} = b_n + 6b_{n-1} \qquad \text{e} \qquad b_0 = b_1 = 1?$$

2.4 Somatórios e Produtos

Só raramente utilizamos somas e produtos de apenas dois elementos. Por este motivo, convém-nos generalizar estas operações algébricas para um número arbitrário, mas finito, de parcelas ou factores. Começamos por analisar a definição de produtos de mais de dois factores, dado que os resultados referentes a somatórios se obtêm por uma simples mudança de notação.

Nesta secção, S designa um conjunto com uma operação binária associativa. Dada uma sucessão $a_1, a_2, \ldots, a_n, \ldots$ de elementos de S, a sucessão dos respectivos *produtos parciais*, *i.e.*, a sucessão $\pi_1 = a_1$, $\pi_2 = a_1a_2$, $\pi_3 = (a_1a_2)a_3$, ... é definida formalmente como se segue.

Definição 2.4.1. A sucessão $\pi : \mathbb{N} \to S$ é dada por:

(i) para $n = 1$, $\pi_1 = a_1$;

(ii) para $n > 1$, $\pi_n = \pi_{n-1}a_n$.

π_n diz-se o PRODUTO dos a_k's, com k de 1 até n, e escrevemos $\prod_{k=1}^{n} a_k = \pi_n$.

A propriedade associativa do produto exprime-se em termos das sucessões agora introduzidas, como se indica na seguinte proposição.

Proposição 2.4.2. *Se $a, b : \mathbb{N} \to S$ são sucessões em S, temos:*

(i) sempre que $n > m$

$$\left(\prod_{k=1}^{m} a_k\right)\left(\prod_{k=m+1}^{n} a_k\right) = \prod_{k=1}^{n} a_k;$$

(ii) se a operação é comutativa,

$$\left(\prod_{k=1}^{n} a_k\right)\left(\prod_{k=1}^{n} b_k\right) = \prod_{k=1}^{n} (a_k b_k)\,.$$

A demonstração, por indução, fica para exercício (note que a definição acima pode ser alterada sem dificuldade para produtos que começam com $k > 1$).

Um caso particular interessante da Definição 2.4.1 é o duma sucessão $a : \mathbb{N} \to S$ *constante* (*i.e.*, com $a_n = c$, para qualquer $n \in \mathbb{N}$). O produto dos n primeiros termos da sucessão a corresponde então claramente à noção de *potência* de *base* c e *expoente* n.

Definição 2.4.3. A POTÊNCIA de base c e expoente $n \in \mathbb{N}$ é dada por $c^n = \prod_{k=1}^{n} c$.

Note-se que a potência é formalmente uma função $\Phi : \mathbb{N} \times S \to S$, dada por $\Phi(n, c) = c^n$. Se fixarmos c, obtemos uma função *exponencial* $\phi : \mathbb{N} \to S$, mas podemos igualmente fixar n, para obter uma função $\psi : S \to S$. De acordo com as Definições 2.4.1 e 2.4.3, temos:

$$c^n = (c^{n-1})c \ (n > 1), \text{ e } c^1 = c. \tag{2.4.1}$$

Se S é um monóide com identidade I e o elemento c é invertível, usaremos também as definições

$$c^{-n} = (c^{-1})^n \ (n > 1), \text{ e } c^0 = I. \tag{2.4.2}$$

Se c é invertível, a potência c^m fica assim definida para qualquer inteiro m. Portanto, se S é um grupo, então a função $\Phi : \mathbb{N} \times S \to S$ pode ser substituída por uma função $\tilde{\Phi} : \mathbb{Z} \times S \to S$. As seguintes regras elementares sobre potências são em qualquer caso válidas neste contexto mais geral.

Proposição 2.4.4. *Se a operação no conjunto S é associativa, e $a, b \in S$. Então:*

(i) $a^n a^m = a^{n+m}$ *e* $(a^n)^m = a^{nm}$, *para* $n, m \in \mathbb{N}$;

(ii) Se $ab = ba$, *então* $(ab)^n = a^n b^n$, *para* $n \in \mathbb{N}$;

Se S é um monóide, e a e b são invertíveis, então:

(iii) $a^n a^m = a^{n+m}$ *e* $(a^n)^m = a^{nm}$, *para* $n, m \in \mathbb{Z}$;

(iv) Se $ab = ba$, *então* $(ab)^n = a^n b^n$, *para* $n \in \mathbb{Z}$;

Mais uma vez a demonstração destes resultados requer o Princípio de Indução. Ilustramos a demonstração de (i), como exemplo de um argumento que envolve *dois* naturais.

Demonstração. Provamos $a^n a^m = a^{n+m}$ por indução no natural m. Seja $\mathcal{P}(m)$ a afirmação:

> $\mathcal{P}(m)$ = "$a^n a^m = a^{n+m}$ para qualquer $a \in S$ e qualquer natural n".

$\mathcal{P}(1)$ segue-se da Definição 2.4.1, e para provar $\mathcal{P}(m+1)$, note-se que

$$\begin{aligned} a^n a^{m+1} &= (a^n)(a^m a) && \text{(por (2.4.1))}, \\ &= ((a^n)(a^m))a && \text{(por associatividade)}, \\ &= (a^{n+m})a && \text{(por hipótese de indução)}, \\ &= a^{n+m+1} && \text{(por (2.4.1))}. \end{aligned}$$

□

Repare-se, ainda, que de acordo com (iii), e supondo que S é um grupo, a função $f : \mathbb{Z} \to S$ dada por $f(n) = a^n$ (com $a \in S$ fixo) é um homomorfismo de grupos. Se S é apenas um monóide, a restrição da mesma função a $\mathbb{N}_0$ é ainda um homomorfismo de monóides.

A passagem dos resultados anteriores à notação aditiva não oferece dificuldades de maior. Se "+" designa uma operação binária comutativa no conjunto S, a Definição 2.4.1 deve ser reescrita como se segue:

Definição 2.4.5. A sucessão $\sigma : \mathbb{N} \to S$ é dada por

(i) para $n = 1$, $\sigma_1 = a_1$;

(ii) para $n > 1$, $\sigma_n = \sigma_{n-1} + a_n$.

σ_n diz-se o SOMATÓRIO dos a_k's, com k de 1 até n, e escrevemos $\sum_{k=1}^{n} a_k = \sigma_n$.

Da mesma forma, se $a : \mathbb{N} \to S$ é constante com $a_n = c$, então escrevemos $nc = \sum_{k=1}^{n} c$. Além disso, se S tem identidade 0 e o elemento c tem simétrico, definimos

$$0c = 0, \qquad (-n)c = n(-c).$$

Referimo-nos à operação $\Phi : \mathbb{N} \times S \to S$ dada por $\Phi(n, c) = nc$ como o "*produto de um natural n por um elemento c de S*", e à correspondente operação $\Psi : \mathbb{Z} \times S \to S$ como o "*produto de um inteiro n por um elemento c de S*". Esta terminologia causa no entanto uma pequena ambiguidade quando S é ele próprio o conjunto dos inteiros. Neste caso, passamos a dispor aparentemente de duas operações de produto: a operação mencionada no Axioma 1 deste Capítulo, e a operação introduzida na Definição 2.4.5. Deixamos como exercício verificar que estas duas operações são efectivamente a mesma. Na realidade, o que esta duplicação sugere é que as

referências ao produto na axiomática dos inteiros são supérfluas e desnecessárias, o que é efectivamente o caso: é possível apresentar conjuntos de axiomas para os inteiros sem mencionar a operação do produto, e provar todas as propriedades usuais do produto como teoremas, se bem que não tenhamos explorado aqui essa via.

Se $(G,+)$ é um grupo abeliano, as propriedades algébricas básicas do produto de inteiros por elementos de G podem ser resumidas como se segue:

Proposição 2.4.6. *Se $g,h \in G$, e m e n são inteiros temos:*

(i) Identidade: $1g = g$.

(ii) Distributividade: $(n+m)g = ng + mg$ *e* $n(g+h) = ng + nh$.

(iii) Associatividade: $n(mg) = (nm)g$.

Note-se a título de curiosidade que estas propriedades são formalmente semelhantes às da definição de espaço vectorial. Mais exactamente, se substituirmos os elementos do grupo G por vectores de um qualquer espaço vectorial e os inteiros por escalares do correspondente corpo, então as propriedades expressas na Proposição 2.4.6 são exactamente as exigidas à operação "*produto dum escalar por um vector*" na definição de espaço vectorial. De facto, existe uma noção básica da Álgebra que permite tratar ao mesmo nível os conceitos de grupo abeliano e de espaço vectorial: a noção de *módulo sobre um anel*. Esta noção será formalizada num capítulo mais adiante.

Se $(A,+,\cdot)$ é um anel, podemos ainda verificar algumas propriedades adicionais "mistas", ou seja, combinando a soma e o produto. Temos então:

Proposição 2.4.7. *Se $a, a_1, \ldots, a_n, b, c \in A$ e $n \in \mathbb{N}$, então temos:*

(i) $c\left(\sum_{k=1}^{n} a_k\right) = \sum_{k=1}^{n}(ca_k)$;

(ii) $\left(\sum_{k=1}^{n} a_k\right) c = \sum_{k=1}^{n}(a_k c)$;

(iii) $n(ab) = (na)b = a(nb)$.

Mencionámos acima que, quando G é um grupo e $g \in G$, então a função $\psi : \mathbb{Z} \to G$ dada por $\psi(n) = g^n$ é um homomorfismo de grupos. Naturalmente, se G é um grupo abeliano e $\psi(n) = ng$, então ψ é igualmente um homomorfismo de grupos. Deve notar-se finalmente que se $(A,+,\cdot)$ é um anel e $a \in A$, então $\psi(n) = na$ é sempre um homomorfismo de grupos entre $(\mathbb{Z},+)$ e $(A,+)$, mas só é um homomorfismo de anéis se, por acaso, $a^2 = a$ (porquê?).

Exercícios.

1. Qual é a sucessão definida em $\mathbb{Z}$ por $a_1 = 1$, $a_{n+1} = \sum_{k=1}^{n} a_k$?

2. Complete as demonstrações dos resultados enunciados nesta secção.

3. Mostre que, se S é um monóide onde a lei do corte é válida, então a igualdade

$$\left(\prod_{k=1}^{n} a_k\right)\left(\prod_{k=1}^{n} b_k\right) = \prod_{k=1}^{n}(a_k b_k)$$

verifica-se se e só se S é abeliano.

4. Suponha que $n \in \mathbb{Z}$, e $g_1, g_2 \in G$, onde G é um grupo aditivo. Diga se é sempre verdade que

$$n \neq 0 \text{ e } ng_1 = ng_2 \Rightarrow g_1 = g_2.$$

(SUGESTÃO: Considere o grupo $\mathbb{Z}_2$ referido no Capítulo 1.)

5. Prove que, se B é um subconjunto do anel A fechado em relação à diferença em A, então B é também fechado em relação ao produto por inteiros, ou seja,

Se $[a, b \in B \Rightarrow a - b \in B]$ então $[(n \in \mathbb{Z} \text{ e } b \in B) \Rightarrow nb \in B]$.

6. Use o resultado anterior para provar que no anel dos inteiros, as seguintes afirmações são equivalentes para um subconjunto $B \subset \mathbb{Z}$ não vazio:

   (a) B é fechado em relação à diferença;

   (b) B é um subanel de $\mathbb{Z}$;

   (c) B é um ideal de $\mathbb{Z}$.

7. Mostre que:

   (a) se $\phi : G \to H$ é um homomorfismo de grupos aditivos, então $\phi(ng) = n\phi(g), n \in \mathbb{Z}, g \in G$;

   (b) se $\phi : \mathbb{Z} \to G$ é um homomorfismo de grupos aditivos, então $\phi(n) = ng$, para algum $g \in G$.

   Como é que pode generalizar estes resultados a grupos que não são aditivos?

8. Mostre que, se G é um grupo e $g \in G$, então $H = \{a^n : n \in \mathbb{N}\}$ é o menor subgrupo de G que contém g.

9. Seja A um anel com identidade I, e $\phi : \mathbb{Z} \to A$ dada por $\phi(n) = nI$. Mostre que:

   (a) ϕ é um homomorfismo, e $\phi(\mathbb{Z}) = \{nI : n \in \mathbb{N}\}$ é o menor subanel de A que contém I;

   (b) $\{n \in \mathbb{Z} : na = 0\}$ é um ideal de A que contém o núcleo $N(\phi)$;

   (c) $\phi(\mathbb{N}) = \{nI : n \in \mathbb{N}\} = \{\sum_{k=1}^{n} I : n \in \mathbb{N}\}$ é o conjunto $N(A)$[8].

[8]Esta é a forma mais rigorosa que podemos dar à ideia de que os elementos de $N(A)$ se obtêm somando a identidade I a si própria, um número arbitrário, mas finito, de vezes.

10. Seja $A \neq \{0\}$ um anel com identidade I, e $\phi : \mathbb{Z} \to A$ dada por $\phi(n) = nI$. Prove que, se A é bem-ordenado (*i.e.*, se A é ordenado e qualquer subconjunto não-vazio de A^+ tem mínimo), então A é isomorfo a $\mathbb{Z}$.
SUGESTÃO: Mostre, pela seguinte ordem, que:
    (a) O conjunto $\{a \in A : 0 < a < I\}$ é vazio;
    (b) $A^+ = \phi(\mathbb{N})$:
    (c) $A = \phi(\mathbb{Z})$;
    (d) ϕ é injectiva.

2.5 Factores, Múltiplos e Divisão

Num anel arbitrário A a equação $ax = b$ não tem necessariamente solução para quaisquer a e b, mesmo que $a \neq 0$ (se $a = 0$ a equação só pode em qualquer caso ter solução para $b = 0$). Para evitar a necessidade de distinguir a equação $ax = b$ da equação $xa = b$, suporemos sempre nesta secção que A designa um anel comutativo.

Definição 2.5.1. Se $a, b \in A$, dizemos que a é FACTOR (ou DIVISOR[9]) de b, ou que b é MÚLTIPLO de a, e escrevemos "$a|b$", se a equação $ax = b$ tem alguma solução $x \in A$.

Exemplos 2.5.2.

1. *Num anel com identidade* 1*, qualquer elemento* b *tem pelo menos os factores* $1, -1, b, -b$*, porque* $b = 1b = (-1)(-b)$ *(se bem que possa acontecer que* $1 = -1 = b = -b$*!).*
2. *Se* K *é um corpo, e* $k \neq 0$*, qualquer* $r \in K$ *é múltiplo de* k*.*
3. *Se* $A = \mathbb{Z}$*, e* $a^2 \neq 1$*, o conjunto dos múltiplos de* a *é distinto de* $\mathbb{Z}$*.*
4. *Os múltiplos de* $(x - 1)$ *no anel* $\mathbb{R}[x]$ *dos polinómios reais na variável* x *são precisamente* $\{p(x) \in \mathbb{R}[x] : p(1) = 0\}$*.*

É evidente que a relação "*é factor de*" é transitiva (se $a|b$ e $b|c$, então $a|c$), e se $c \neq 0$ não é divisor de zero, temos que $ac|bc$ se e só se $a|b$. Por outro lado, se A é um anel ordenado, é também claro que $a|b$ se e só se $|a| \mid |b|$.

Neste capítulo estamos interessados no caso $A = \mathbb{Z}$. O estudo da factorização e divisibilidade em anéis mais gerais será efectuado no próximo capítulo. No caso dos inteiros, a implicação $n > 0 \Rightarrow n \geq 1$ permite-nos obter ainda:

[9]Note-se que o termo *divisor* é utilizado aqui numa acepção ligeiramente diferente da que usámos quando definimos *divisor de zero*. Recorde-se que $a \neq 0$ se diz divisor de zero se a equação $ax = 0$ tem solução $x \neq 0$.

Lema 2.5.3. *Se $m, n \in \mathbb{Z}$, então:*

(i) $m|n \Longrightarrow (|m| \leq |n|$ *ou* $n = 0)$*;*

(ii) $(m|n$ *e* $n|m) \Longleftrightarrow |m| = |n|$*.*

De acordo com o lema anterior, se n e k são naturais e $k|n$, então $k < n$. Como já observámos, 1 é factor de qualquer natural n. Portanto, se n e m são naturais, o conjunto dos *factores (ou divisores) comuns* a n e m é não-vazio e majorado, e consequentemente tem máximo.

Analogamente, o conjunto dos múltiplos naturais de n e m, *i.e.*, o conjunto $\{k \in \mathbb{N} : n|k \text{ e } m|k\}$, é não-vazio, já que $nm > 0$ é múltiplo comum de n e m. Tem portanto um elemento mínimo, de acordo com o Princípio de Boa Ordenação.

Definição 2.5.4. Se $n, m \in \mathbb{N}$, então:

(i) $\text{mdc}(n, m) = \max\{k \in \mathbb{N} : k|n \text{ e } k|m\}$ diz-se MÁXIMO DIVISOR COMUM de n e m;

(ii) $\text{mmc}(n, m) = \min\{k \in \mathbb{N} : n|k \text{ e } m|k\}$ diz-se MÍNIMO MÚLTIPLO COMUM de n e m.

Exemplo 2.5.5.

Se $n = 12$ *e* $m = 16$*, os divisores naturais de* n *e* m *formam os conjuntos*

$$\{k \in \mathbb{N} : k|12\} = \{1, 2, 3, 4, 6, 12\},$$
$$\{k \in \mathbb{N} : k|16\} = \{1, 2, 4, 8, 16\}.$$

Consequentemente, os divisores naturais comuns a 12 *e* 16 *formam o conjunto*

$$\{k \in \mathbb{N} : k|12 \text{ e } k|16\} = \{1, 2, 4\},$$

e o respectivo máximo divisor comum é $\text{mdc}(12, 16) = 4$*.*

Os múltiplos naturais de 12 *e* 16 *são*

$$\{k \in \mathbb{N} : 12|k\} = \{12, 24, 36, 48, \dots\},$$
$$\{k \in \mathbb{N} : 16|k\} = \{16, 32, 48, \dots\},$$

donde concluímos que os múltiplos naturais comuns a 12 *e* 16 *formam o conjunto*

$$\{k \in \mathbb{N} : 12|k \text{ e } 16|k\} = \{48, 96, \dots\}$$

e que o respectivo mínimo múltiplo comum é $\text{mmc}(12, 16) = 48$*.*

Observe-se que, pelo menos neste exemplo, $\text{mdc}(m, n)$ é *múltiplo* de todos os divisores comuns a n e m, e $\text{mmc}(n, m)$ é *factor* de todos os múltiplos comuns a n e m, sugerindo que:

Proposição 2.5.6. *Sejam $n, m, d, l \in \mathbb{N}$. Então:*

(i) $d = \text{mdc}(n, m)$ *se e só se:*

(a) $d|n$ *e* $d|m$*;*

(b) para qualquer $k \in \mathbb{N}$, $(k|n \text{ e } k|m) \Rightarrow k|d$.

(ii) $d = \text{mmc}(n, m)$ *se e só se:*

(a) $n|d$ *e* $m|d$*;*

(b) para qualquer $k \in \mathbb{N}$, $(n|k \text{ e } m|k) \Rightarrow d|k$.

Provaremos estas afirmações na secção seguinte.

Indicamos aqui para referência futura mais duas definições elementares. Note-se que convencionamos dizer que o natural 1 *não* é primo.

Definição 2.5.7. Sejam $p, m, n \in \mathbb{N}$.

(i) Dizemos que p é PRIMO se $p > 1$ e se, para todo o $k \in \mathbb{N}$ tal que $k|p$, temos que $k = 1$ ou $k = p$.

(ii) Dizemos que n e m são PRIMOS ENTRE SI se $\text{mdc}(n, m) = 1$.

Exemplo 2.5.8.

É fácil verificar enumerando todas as possibilidades que 4 *e* 9 *são primos entre si,* i.e., $\text{mdc}(4, 9) = 1$*, e que* 13 *é um número primo. Para provar que* p *é primo não é necessário testar todos os números* k *com* $1 < k < p$*, podendo o teste terminar com o maior natural* k *tal que* $k^2 < p$*. No caso de* $p = 13$*, basta portanto constatar que 13 não é múltiplo de* 2 *nem de* 3*.*

Na secção anterior provámos por indução que qualquer natural n é par ou ímpar, ou seja, dado n, existem inteiros q e r tais que $n = 2q + r$, com $0 \leq r < 2$. Este resultado não é específico do natural 2. Por outras palavras, podemos escrever sempre $n = 3q' + r'$, com $0 \leq r' < 3$, ou $n = 4q'' + r''$, com $0 \leq r'' < 4$, etc. Um momento de reflexão mostra que estas afirmações estão relacionadas com o Algoritmo de Divisão que todos aprendemos na escola primária.

Teorema 2.5.9 (Algoritmo de Divisão). *Se* $n, m \in \mathbb{Z}$ *e* $n \neq 0$*, existem inteiros únicos* q, r*, tais que* $m = nq + r$*, e* $0 \leq r < |n|$.

Demonstração. Provamos apenas o caso $n, m \in \mathbb{N}$, deixando o caso geral como exercício. Note-se que o argumento para provar a existência corresponde ao processo usual para efectuar uma divisão.

(i) *Existência:* Considere-se o conjunto $Q = \{x \in \mathbb{N}_0 : nx \leq m\}$. Note-se que Q é não-vazio (porque $0 \in Q$) e majorado (porque $x \leq nx \leq m$). Tem consequentemente um máximo $x = q$. É claro que $nq \leq m < n(q + 1)$,

porque $q \in Q$ e $(q+1) \notin Q$. Subtraindo nq destas desigualdades, obtemos $0 \leq r \leq n$, já que $r = m - nq$.

(ii) *Unicidade:* Se $m = nq + r = nq' + r'$, segue-se que $n(|q - q'|) = |r - r'|$. Agora, se $q \neq q'$, é óbvio que $|q - q'| \geq 1$ e $|r - r'| > n$. Por outro lado, r e r' verificam $0 \leq r, r' < n$, donde temos $-n < r - r' < n$, ou seja, $|r - r'| < |n|$. Assim, só pode ser $q = q'$, mas como $n(|q - q'|) = |r - r'|$, também $r = r'$. □

Definição 2.5.10. Se $n, m \in \mathbb{Z}$, $n \neq 0$, e $m = nq + r$ com $0 \leq r < |n|$, dizemos que q e r são respectivamente o QUOCIENTE e o RESTO da divisão de m por n.

O quociente e o resto dependem dos sinais algébricos de m e n duma forma que não é imediatamente óbvia. Para o verificar, considerem-se os exemplos abaixo:

m	n	q	r
5	3	1	2
5	−3	−1	2
−5	3	−2	1
−5	−3	2	1

Supondo $n \neq 0$ fixo, considere a função $\rho : \mathbb{Z} \to \{0, 1, \ldots, n-1\}$, onde $\rho(m)$ é o resto da divisão de m por n. Deixamos como exercício a verificação do seguinte resultado:

Proposição 2.5.11. *Se x, y são inteiros arbitrários, temos*

(i) $\rho(x) = \rho(y)$ *se e só se* $n|(x - y)$;

(ii) $\rho(x \pm y) = \rho(\rho(x) \pm \rho(y))$;

(iii) $\rho(xy) = \rho(\rho(x)\rho(y))$.

Vamos usar o Teorema 2.5.9 já na próxima secção para descrever completamente os ideais do anel dos inteiros, e tornaremos a encontrá-lo repetidas vezes. No próximo capítulo apresentaremos uma sua generalização a certos anéis de polinómios e outros anéis mais gerais. De facto, todas as noções introduzidas nesta secção (primo, mdc, mmc, etc.) serão eventualmente generalizadas a uma classe muito extensa de anéis.

Exercícios.

1. Seja A um anel comutativo, e $a, b, c \in A$. Prove que, se $a|b$ e $b|c$, então $a|c$, e que, se $c \neq 0$ não é divisor de zero, temos $ac|bc$ se e só se $a|b$.

2. Prove o Lema 2.5.3.

3. Conclua a demonstração do Teorema 2.5.9.

4. Mostre que, para $m, n, k \in \mathbb{N}$, se $mn = k$ e $m^2 > k$, então $n^2 < k$.

5. Faça uma lista com os naturais entre 100 e 200. Observe que $17^2 = 289$, e corte da sua lista todos os múltiplos de 2, 3, 5, 7, 11 e 13. Quais são os números que restam[10]?

6. Determine os números primos entre 1950 e 2000.
(SUGESTÃO: Determine primeiro os primos $p \leq \sqrt{2000}$).

7. Se $m, n \in \mathbb{Z}$, $n \neq 0$ e $\rho : \mathbb{Z} \to \{0, 1, \ldots, n-1\}$ é o resto da divisão por n, quando é que $\rho(m) = \rho(-m)$?

8. Prove a Proposição 2.5.11. Qual é a relação entre este teorema e a "prova dos nove" da Aritmética elementar?

9. Diga se o Teorema 2.5.9 é válido se substituirmos o anel dos inteiros pelo anel formado pelos múltiplos de 2. E se substituirmos o anel dos inteiros pelo anel dos reais?

10. Enuncie e demonstre um resultado análogo ao Teorema 2.5.9 para o anel dos inteiros de Gauss.

2.6 Ideais e o Algoritmo de Euclides

Se dispusermos de dois relógios de areia (ampulhetas), um marcando um intervalo de tempo de 21 minutos e o outro marcando um intervalo de tempo de 30 minutos, que intervalos podemos medir utilizando as duas ampulhetas? Certos intervalos são obviamente possíveis, se utilizarmos sucessivamente uma ou outra ampulheta. Por exemplo, 30, 60, 90,..., 21, 42, 63,..., ou somas destes números, como 51, 81, 111,..., 102, 123,..., 132, 153,..., etc. Se usarmos simultaneamente as duas ampulhetas, podemos obter diferenças destes números. Exemplos são $9 = 30 - 21$, $3 = 63 - 60$, etc.

Um exame mais cuidadoso dos números que se podem obter sugere as seguintes observações:

- Podemos obter qualquer natural da forma $x21 + y30$ com $x, y \in \mathbb{Z}$.
- Todos os números da forma $x21 + y30$ são múltiplos de 3 (pois 3 é o máximo divisor comum de 21 e 30).

Por outro lado, existem inteiros x' e y' (*e.g.*, $x' = 3, y' = -2$) tais que $3 = x'21 + y'30$. Em particular, se $m = k3$ é um qualquer múltiplo de

[10]Chama-se a este procedimento o FILTRO DE ERATÓSTENES. Eratóstenes (276 a.C.-194 a.C.) nascido na actual Líbia, foi o terceiro bibliotecário da famosa Biblioteca de Alexandria. Entre outras coisas estabeleceu a esfericidade da Terra, e calculou com grande exactidão o seu diâmetro.

3, então $m = k(x'21 + y'30) = k(x'21 + y'30) = x''21 + y''30$. Por outras palavras,

- Os números da forma $x21 + y30$ são precisamente os múltiplos de 3;
- $3 = \text{mdc}(21, 30)$ é o menor natural da forma $x21 + y30$.

O objectivo desta secção é explorar estas observações, generalizando a um anel arbitrário as ideias que se têm revelado úteis noutros contextos. Como subprodutos do nosso trabalho determinaremos todos os ideais de $\mathbb{Z}$ e encontraremos um processo de cálculo de $\text{mdc}(n, m)$, o chamado *Algoritmo de Euclides*, que não envolve o conhecimento dos factores primos de n e m, é facilmente generalizável a polinómios, e é especialmente apropriado ao cálculo automático.

Sendo n e m inteiros arbitrários fixos, considere-se o conjunto $I = \{xn + ym : x, y \in \mathbb{Z}\}$. É evidente que I não é vazio, e é fechado em relação à diferença e ao produto por inteiros arbitrários, *i.e.*, se $x, y, x', y', z \in \mathbb{Z}$, então

$$(xn + ym) \pm (x'n + y'm) = (x \pm x')n + (y \pm y')m \in I,$$
$$z(xn + ym) = (xn + ym)z = (zx)n + (zy)m \in I.$$

Por outras palavras, I é um *ideal* de $\mathbb{Z}$. Por outro lado, se J é um ideal tal que $n, m \in J$, é claro que $xn, ym \in J$ para quaisquer $x, y \in \mathbb{Z}$, donde $xn + ym \in J$, ou seja, $I \subset J$. Dizemos por isso que I é o *menor* ideal de $\mathbb{Z}$ que contém n e m, ou ainda que I é o ideal *gerado* por n e m.

Mais geralmente, considere-se um qualquer anel A em lugar do anel dos inteiros, e substitua-se o conjunto $\{n, m\}$ por um subconjunto arbitrário (não-vazio) S em A. Notamos que o próprio anel A é um ideal de A que contém S. Portanto, a família dos ideais de A que contêm S não é vazia. Designamos por $\langle S\rangle$ a *intersecção* de todos os ideais pertencentes a esta família, sendo claro que $S \subset \langle S\rangle$. É fácil verificar da definição de ideal que a intersecção duma família de ideais de A é ainda um ideal de A, e portanto $\langle S\rangle$ é um ideal de A que contém S. É também evidente que, se $S \subset I \subset A$ e I é um ideal, então $\langle S\rangle \subset I$. A verificação de todas estas afirmações é deixada como exercício.

Definição 2.6.1. Se A é um anel, e $S \subset A$, chama-se a $\langle S\rangle$ o IDEAL GERADO por S, ou o MENOR IDEAL de A que contém S. Os elementos de S dizem-se GERADORES do ideal $\langle S\rangle$, e S diz-se CONJUNTO GERADOR de $\langle S\rangle$.

Se $S = \{a_1, a_2, \ldots, a_n\}$ é um subconjunto finito dum anel A, escrevemos por vezes $\langle a_1, a_2, \ldots, a_n\rangle$ em lugar de $\langle S\rangle$. Vimos no caso dos inteiros que $\langle n, m\rangle = \{xn + ym : x, y \in \mathbb{Z}\}$, e é imediato provar que $\langle n\rangle = \{xn : x \in \mathbb{Z}\}$. Existem no entanto anéis onde não é tão fácil determinar o ideal gerado por um dado conjunto de elementos.

Exemplos 2.6.2.

1. *Seja A um anel abeliano e $a \in A$. Então $\{xa : x \in A\}$ é um subanel de A, pois, se $x, y \in A$, temos*

$$xa - ya = (x - y)a,\ (xa)(ya) = (xay)a,$$

logo $\{xa : x \in A\}$ é fechado para a diferença e o produto. Por outro lado, se $x, b \in A$, como A é abeliano, temos

$$b(xa) = (xa)b = (bx)a,$$

logo $\{xa : x \in A\}$ é um ideal. Finalmente $\langle a \rangle$ contém necessariamente os "múltiplos" de a, e concluímos que $\langle a \rangle = \{xa : x \in A\}$.

2. *Seja $A = M_2(\mathbb{Z})$ o anel das matrizes 2×2 com entradas em $\mathbb{Z}$, e*

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

O conjunto dos "múltiplos" de a é

$$\{ax : x \in M_2(\mathbb{Z})\} = \{\begin{pmatrix} n & m \\ 0 & 0 \end{pmatrix} : n, m \in \mathbb{Z}\},$$

mas $\langle a \rangle = M_2(\mathbb{Z})$ por razões que exploraremos nos exercícios.

O ideal de $\mathbb{Z}$ gerado por 21 e 30 é também gerado por 3. De facto acontece que qualquer ideal dos inteiros é gerado por um dos seus elementos, propriedade que não é de modo nenhum generalizável a todos os anéis.

Teorema 2.6.3. *I é um ideal de $\mathbb{Z}$ se e só se existe $d \in \mathbb{Z}$ tal que $I = \langle d \rangle$.*

Demonstração. Vejamos que ambas as implicações se verificam.

(a) Se $I = \langle d \rangle$, então I é obviamente um ideal de $\mathbb{Z}$.

(b) Seja I um ideal de $\mathbb{Z}$. Se I se reduz ao conjunto $\{0\}$, é claro que $I = \langle 0 \rangle$. Podemos portanto supor $I \neq \langle 0 \rangle$, e notamos que neste caso o ideal I contém inteiros positivos (note que, se $n \in I$, então $-n \in I$). Sendo $I^+ = \{n \in I : n > 0\}$, tomamos d igual ao mínimo de I^+ (mínimo esse que existe pelo Princípio de Boa Ordenação).

Como $d \in I$ segue-se (porquê?) que $\langle d \rangle \subseteq I$, restando-nos portanto provar a inclusão oposta $I \subseteq \langle d \rangle$, ou seja, que, se $m \in I$, então m é múltiplo de d. Seja $m \in I$, e q e r o quociente e resto da divisão de m por d (recorde-se que $d > 0$, donde $d \neq 0$). Temos então $m = qd + r$, ou $r = m - qd$. Observe-se que $qd \in \langle d \rangle$, e portanto $qd \in I$ (já vimos que $\langle d \rangle \subseteq I$). Como $r = m - qd$ é a diferença de dois elementos do ideal I, temos $r \in I$. Finalmente, como $0 \leq r < d$ e d é por definição o menor elemento positivo do ideal I, temos necessariamente $r = 0$, donde m é múltiplo de d, *i.e.*, $m \in \langle d \rangle$. Portanto, $I \subseteq \langle d \rangle$. □

O exemplo do ideal $\langle 21, 30\rangle$ sugere que, se $I = \langle d\rangle = \langle n, m\rangle$, então $|d|$ é o máximo divisor comum de n e m. O resultado anterior permite estabelecer este resultado e ainda a parte (i) da Proposição 2.5.6.

Corolário 2.6.4. *Se $n, m \in \mathbb{N}$, então $\langle n, m\rangle = \langle d\rangle$ onde $d = \text{mdc}(n, m)$. Em particular, temos que:*

(i) a equação $xn + ym = d$ tem soluções $x, y \in \mathbb{Z}$;

(ii) se k é um divisor comum de n e m, então k é também divisor de d.

Demonstração. (i) Sabemos, do teorema anterior, que existe um natural d tal que $\langle n, m\rangle = \langle d\rangle$. É óbvio que $d \in \langle d\rangle = \langle n, m\rangle$. Como $\langle n, m\rangle$ é o conjunto dos inteiros da forma $xn + ym$, existem inteiros x', y' tais que $d = x'n + y'm$.

(ii) É igualmente óbvio que $n, m \in \langle n, m\rangle = \langle d\rangle$. Portanto, n e m são múltiplos de d, que é um divisor comum a n e m. Por outro lado, se $k \in \mathbb{N}$ é um qualquer divisor comum a n e m, temos $n = kn'$ e $m = km'$, donde $d = x'n + y'm = k(x'n' + y'm')$, ou seja, $k|d$. Em especial, $k \leq d$ e d é o máximo divisor comum de n e m. □

Este corolário sugere que o cálculo de $\text{mdc}(n, m)$ pode ser feito por busca do menor natural no ideal $\langle n, m\rangle$. O Algoritmo de Divisão torna essa busca possível recorrendo ao seguinte lema.

Lema 2.6.5. *Se $n, m \in \mathbb{N}$ e $m = qn + r$, então $\langle n, m\rangle = \langle n, r\rangle$.*

Demonstração. Por um lado,

$$\begin{aligned} k \in \langle n, m\rangle &\Longrightarrow k = xm + yn \\ &\Longrightarrow k = x(qn + r) + yn \\ &\Longrightarrow k = (xq + y)n + xr \\ &\Longrightarrow k \in \langle n, r\rangle, \end{aligned}$$

logo $\langle n, m\rangle \subset \langle n, r\rangle$. Por outro lado,

$$\begin{aligned} k \in \langle n, r\rangle &\Longrightarrow k = xn + yr \\ &\Longrightarrow k = xn + y(m - qn) \\ &\Longrightarrow k = (x - yq)n + ym \\ &\Longrightarrow k \in \langle n, m\rangle, \end{aligned}$$

ou seja, $\langle n, r\rangle \subset \langle n, m\rangle$. □

O Algoritmo de Euclides é a aplicação repetida do lema anterior até obter uma divisão exacta ($r = 0$). Este é um procedimento muito simples, fácil de programar, e que passamos a ilustrar no caso com que iniciámos esta secção:

Exemplo 2.6.6.

Se $n = 21$ *e* $m = 30$*, então*

$$30 = 1 \cdot 21 + 9 \Longrightarrow \langle 30, 21\rangle = \langle 21, 9\rangle,$$
$$21 = 2 \cdot 9 + 3 \Longrightarrow \langle 21, 9\rangle = \langle 9, 3\rangle,$$
$$9 = 3 \cdot 3 + 0 \Longrightarrow \langle 9, 3\rangle = \langle 3\rangle.$$

Logo

$$\langle 30, 21\rangle = \langle 3\rangle,$$

e pelo corolário anterior temos que $3 = \text{mdc}(21, 30)$*. Em termos gerais,* i.e.*, começando com dois naturais quaisquer* n *e* m*, e supondo* $n < m$*, o procedimento a seguir deve ser claro, e corresponde a um processo iterativo muito fácil de programar (experimente-o!). Observe-se também que é simultaneamente possível determinar inteiros* x *e* y *tais que* $\text{mdc}(n, m) = xn + ym$*. Das equações acima temos imediatamente*

$$3 = 21 + (-2)9 \text{ e } 9 = 30 + (-1)21,$$

donde

$$3 = 21 + (-2)[30 + (-1)21] = (3)21 + (-2)30.$$

Apresentamos a seguir um argumento que explora o facto de $\text{mdc}(n, m)$ ser uma combinação linear de n e m.

Proposição 2.6.7. *Sejam* $m, n, p, k \in \mathbb{N}$ *e suponha-se que* $mn|kp$*. Se* m *e* p *são primos entre si, então* m *é factor de* k*.*

Demonstração. Como por hipótese $\text{mdc}(m, p) = 1$, existem inteiros x', y' tais que $1 = x'm + y'p$, donde $k = k(x'm + y'p)$. Além disso, como $mn|kp$, existe um inteiro z' tal que $kp = z'mn$. Portanto,

$$\begin{aligned} k &= k(x'm + y'p) \\ &= kx'm + y'kp \\ &= kx'm + y'z'mn = (kx' + y'z'n)m, \end{aligned}$$

donde $m|k$. □

O mínimo múltiplo comum de dois naturais pode também ser estudado a partir do Teorema 2.6.3. Dados os naturais n e m, observamos que $\langle n\rangle \cap \langle m\rangle$ é o conjunto dos múltiplos comuns a n e m. Como a intersecção de dois ideais é um ideal, concluímos, do Teorema 2.6.3, que $\langle n\rangle \cap \langle m\rangle = \langle l\rangle$, onde l é um natural. É claro que l é um múltiplo comum de n e m, e que qualquer múltiplo comum k de n e m é múltiplo de l, e portanto $l \leq |k|$. Assim, podemos verificar, analogamente ao caso do do máximo divisor comum, a parte (ii) da Proposição 2.5.6.

Estas observações sugerem a definição de máximo divisor comum e mínimo múltiplo comum de dois *inteiros* como se segue.

Definição 2.6.8. Se m, n, d, l são inteiros, e $d, l \geq 0$, então:

(i) $d = \text{mdc}(n, m)$ se $\langle d \rangle = \langle n, m \rangle$;

(ii) $l = \text{mmc}(n, m)$ se $\langle l \rangle = \langle n \rangle \cap \langle m \rangle$.

A definição acima é compatível com o Teorema 2.6.3 e conduz ao resultado "natural" $\text{mdc}(n, m) = \text{mdc}(|n|, |m|)$ e $\text{mmc}(n, m) = \text{mmc}(|n|, |m|)$. Note-se de passagem que $\text{mdc}(n, 0) = n$ e $\text{mmc}(n, 0) = 0$. Veremos mais adiante que é possível explorar estes resultados para estender as noções de máximo divisor comum e mínimo múltiplo comum a certas classes de anéis.

Num anel arbitrário, distinguimos com um nome especial os ideais que, tal como os ideais do anel $\mathbb{Z}$, são gerados por um dos seus elementos.

Definição 2.6.9. O ideal I num anel A diz-se um IDEAL PRINCIPAL se existe $a \in A$ tal que $I = \langle a \rangle$.

De acordo com o Teorema 2.6.3, *todos* os ideais do anel dos inteiros são ideais *principais*, mas veremos adiante anéis com ideais que não são principais. No entanto, os anéis onde todos os ideais são principais constituem uma classe importante de anéis.

Sabemos que, se A é um anel com identidade I, então a função $\phi : \mathbb{Z} \to A$ dada por $\phi(n) = nI$ é um homomorfismo. Segue-se naturalmente que o conjunto das soluções da equação homogénea $nI = 0$ ($n \in \mathbb{Z}$), que é o núcleo de ϕ, é um ideal de $\mathbb{Z}$. Portanto, e dado que todos os ideais de $\mathbb{Z}$ são principais, existe um inteiro $m \geq 0$ tal que

$$\{n \in \mathbb{Z} : nI = 0\} = \langle m \rangle.$$

Na realidade, e de acordo com a demonstração do Teorema 2.6.3, se $m > 0$, então m é simplesmente a menor solução positiva da equação $nI = 0$. Em qualquer caso, o inteiro m merece um nome especial.

Definição 2.6.10. Dizemos que um inteiro $m \geq 0$ é a CARACTERÍSTICA do anel A se

$$\{n \in \mathbb{Z} : nI = 0\} = \langle m \rangle.$$

Exemplos 2.6.11.

1. *Os anéis mais "comuns" ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, etc.) têm característica 0.*
2. *O anel $\mathbb{Z}_2$ tem característica* 2.

Se $\langle m \rangle$ e $\langle n \rangle$ são ideais de $\mathbb{Z}$, é claro que $\langle n \rangle \subset \langle m \rangle$ se e só se $m|n$. Por outras palavras, determinar todos os ideais que contêm $\langle n \rangle$ é equivalente a determinar todos os divisores de n.

Isto mesmo é ilustrado na próxima figura, quando $n = 12$, onde cada rectângulo representa um ideal de $\mathbb{Z}$ que contém $\langle 12 \rangle$. Note-se que, se um

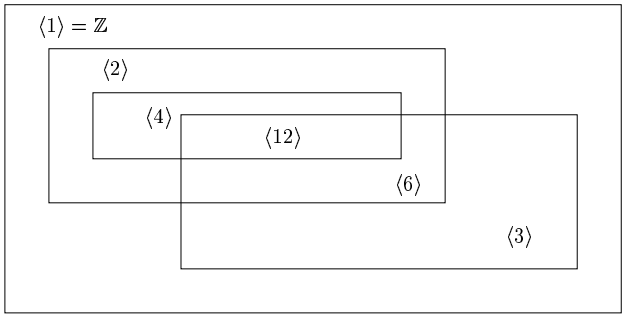


Figura 2.6.1: Ideais de $\mathbb{Z}$ que contêm $\langle 12\rangle$.

rectângulo está contido noutro, então os ideais correspondentes também o estão, e que o ideal gerado por 1 é obviamente o anel $\mathbb{Z}$.

Em alternativa, podemos representar os ideais que contêm $\langle 12\rangle$ como no seguinte diagrama (note o subdiagrama à direita).

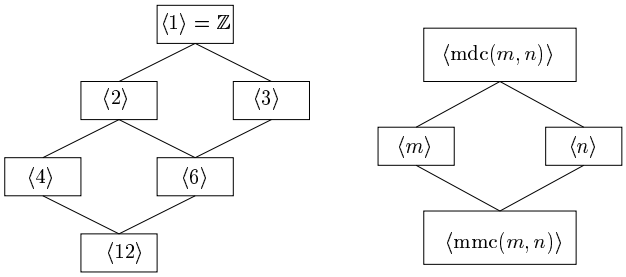


Figura 2.6.2: Os divisores de 12.

Deve observar-se que um diagrama deste tipo pode ser prolongado para baixo indefinidamente, mas não o pode ser para cima. Em particular, dado um ideal $\langle m\rangle$ dos inteiros é possível que o único ideal que o contenha estritamente seja o próprio $\mathbb{Z}$, o que acontece precisamente quando n é um número primo ou 1. O mesmo pode acontecer a um ideal arbitrário de um qualquer anel, pelo que introduzimos:

Definição 2.6.12. O ideal I em A diz-se MÁXIMO ou MAXIMAL se para qualquer ideal J em A,

$$I \subset J \Longrightarrow J = I \text{ ou } J = A.$$

Os ideais máximos de um domínio integral D podem ser utilizados, como veremos adiante, para associarmos a D certos corpos. Como dissemos acima, é fácil identificar os ideais máximos de $\mathbb{Z}$, que usaremos adiante para definir uma classe importante de corpos finitos.

Teorema 2.6.13. *O ideal $\langle p\rangle$ em $\mathbb{Z}$ é máximo se e só se $p = 1$ ou $|p|$ é um número primo.*

Demonstração. Suponha-se $p, q \in \mathbb{N}$ e $\langle p\rangle \subset \langle q\rangle$, *i.e.*, $q|p$. Se $p = 1$ ou p é primo, temos $q = 1$ ou $q = p$, donde $\langle q\rangle = \mathbb{Z}$ ou $\langle q\rangle = \langle p\rangle$, e $\langle p\rangle$ é máximo.

Se, por outro lado, $p > 1$ não é primo, então existe $q \in \mathbb{N}$ tal que $1 < q < p$ e $q|p$. Segue-se que $\mathbb{Z} \neq \langle q\rangle \neq \langle p\rangle$, e $\langle p\rangle \subsetneq \langle q\rangle$, donde $\langle p\rangle$ não é máximo. □

Na próxima secção examinaremos mais pormenorizadamente outras propriedades dos números primos.

Exemplos 2.6.14.

1. *O ideal $\langle 0\rangle$ é máximo no anel $\mathbb{R}$, mas não no anel $\mathbb{Z}$.*
2. *O ideal $\langle x^2 - 2\rangle$ não é máximo em $\mathbb{R}[x]$, porque $\langle x^2 - 2\rangle \subsetneq \langle x + \sqrt{2}\rangle$, e $\langle x + \sqrt{2}\rangle \neq \mathbb{R}[x]$. Por outro lado, $\langle x^2 - 2\rangle$ é maximal em $\mathbb{Z}[x]$ (porquê?).*
3. *No apêndice mostra-se, recorrendo ao lema de Zorn, que num anel arbitrário A qualquer ideal próprio $I \subsetneq A$ está contido num ideal maximal.*

Exercícios.

1. Dê exemplos de naturais a, b, n tais que ab não é factor de n, mas $a|n$ e $b|n$.
2. Determine inteiros x e y tais que $\text{mdc}(135, 1987) = x135 + y1987$.
3. Como pode medir 1 litro de água, se tiver à sua disposição apenas dois recipientes com capacidades respectivamente de 15 e 23 litros?
4. Sejam $a, b, d, m, x, y, s, t \in \mathbb{Z}$. Mostre que:
   (a) $d = MDC(a, b), a = dx, b = dy \Rightarrow \text{mdc}(x, y) = 1$;
   (b) $as + bt = 1 \Rightarrow \text{mdc}(a, b) = \text{mdc}(a, t) = \text{mdc}(s, b) = \text{mdc}(s, t) = 1$;
   (c) $\text{mdc}(ma, mb) = |m|\ \text{mdc}(a, b)$;
   (d) $\text{mdc}(a, m) = \text{mdc}(b, m) = 1 \Leftrightarrow \text{mdc}(ab, m) = 1$;
   (e) $a|m$ e $b|m \Rightarrow ab|m\ \text{mdc}(a, b)$;
   (f) $|ab| = \text{mdc}(a, b)\,\text{mmc}(a, b)$.
5. Seja $\mathcal{I} = \{I_\beta\}_{\beta\in B}$ uma família de ideais de um anel A indexada por um conjunto B qualquer. Considere o conjunto intersecção desta família:

$$I = \bigcap_{\beta\in B} I_\beta = \{a \in A : a \in I_\beta, \text{ para qualquer } \beta \in B\}.$$

   (a) Prove que I é um ideal de A.

(b) Seja $S \subset A$, e $\mathcal{I}$ a família de todos os ideais de A que contêm S. Prove que neste caso I é o menor ideal de A que contém S.

6. Prove que, se $S_1 \subset S_2 \subset A$, então $\langle S_1 \rangle \subset \langle S_2 \rangle$.

7. Suponha que $m, n \in \mathbb{Z}$, e prove que:
   (a) $\langle n \rangle \subset \langle m \rangle \iff m|n$;
   (b) $\langle n \rangle = \langle m \rangle \iff m = \pm n$.

8. Prove que, se A é um anel abeliano com identidade e $a_1, a_2, \ldots, a_n \in A$, então
$$\langle a_1, a_2, \ldots, a_n \rangle = \left\{ \sum_{k=1}^{n} x_k a_k : x_k \in A, 1 \leq k \leq n \right\}.$$
Como é que descreveria $\langle a_1, a_2, \ldots, a_n \rangle$ se A fosse abeliano, mas não contivesse identidade?

9. Seja $\{a_n\}_{n \in \mathbb{N}}$ uma sucessão de inteiros.
   (a) Defina $d_n = \text{mdc}(a_1, a_2, \ldots, a_n)$ e $l_n = \text{mmc}(a_1, a_2, \ldots, a_n)$, e prove que a equação $d_n = \sum_{k=1}^{n} x_k a_k$ tem soluções $x_k \in \mathbb{Z}$.
   (b) Prove que $d_{n+1} = \text{mdc}(d_n, a_{n+1})$ e $l_{n+1} = \text{mmc}(l_n, a_{n+1})$.
   (c) Quais são os valores de n para os quais $30x + 105y + 42z = n$ tem soluções inteiras?

10. Faça um diagrama semelhante ao dos divisores de 12 para $n = 18$.

11. Suponha que A e B são anéis unitários, de característica respectivamente n e m. Prove que a característica de $A \oplus B$ é $\text{mmc}(n, m)$.

12. Seja A um anel abeliano com identidade 1, e J um ideal de A. Prove que J é maximal se e só se, para qualquer $a \notin J$, a equação $xa + y = 1$ tem soluções $x \in A$ e $y \in J$.
(Sugestão: Verifique primeiro que $\{xa + y : x \in A \text{ e } y \in J\}$ é o ideal gerado por $J \cup \{a\}$.)

13. Suponha que A é um anel com identidade I e característica $m > 0$, e prove que
$$\{nI : n \in \mathbb{Z}\} = \{nI : n \in \mathbb{N}\} = \{\phi(1), \phi(2), \ldots, \phi(m)\}$$
é um anel com m elementos. Prove também que, se $a \in A$, então a menor solução positiva de $na = 0$ é um factor de m.
(Sugestão: se $n = mq + r$ então $\phi(n) = \phi(r)$.)

14. Suponha que A é um anel com característica 4, e determine as tabuadas da soma e do produto do anel $\phi(\mathbb{Z})$. Verifique se este anel é ou não isomorfo ao corpo de 4 elementos referido no Capítulo 1.

15. Determine os ideais de cada um dos seguintes anéis.

(a) O anel dos inteiros pares.

(b) O anel $\mathbb{Z}[i]$ dos inteiros de Gauss.

(c) O anel $\mathbb{Z} \oplus \mathbb{Z}$.

(d) O anel $M_n(\mathbb{Z})$.

16. Determine no caso de cada um dos anéis do exercício 15 se os respectivos ideais são *todos* principais.

2.7 O Teorema Fundamental da Aritmética

Uma das propriedades mais importantes dos números primos é a de gerarem por multiplicações todos os naturais $n \geq 2$. O objectivo deste secção é precisar e demonstrar esta observação que, formulada convenientemente, se diz o *Teorema Fundamental da Aritmética*.

Proposição 2.7.1. *Qualquer natural $n \geq 2$ tem pelo menos um divisor primo p.*

Demonstração. O conjunto

$$D = \{m \in \mathbb{N} : m > 1 \text{ e } m|n\}$$

é não-vazio, já que contém n. Seja p o mínimo de D. Se p não é primo, então $p = mk$, onde $1 < m < p$. Como m é obviamente factor de n ,p não pode ser o mínimo de D. Concluímos que p é primo. □

Uma consequência desta proposição é a *existência* de factorizações em números primos para qualquer natural $n \geq 2$.

Corolário 2.7.2. *Se $n \geq 2$, existem números primos $p_1 \leq p_2 \leq \cdots \leq p_k$ tais que $n = \prod_{i=1}^{k} p_i$.*

Demonstração. Demonstramos este resultado por indução.

Se $n = 2$, é evidente que n tem uma factorização do tipo indicado ($k = 1$ e $p_1 = 2$). Supomos agora que qualquer natural m com $2 \leq m < n$ tem uma factorização do tipo indicado. Pretendemos provar que n tem também uma factorização deste tipo.

Seja $P = \{p \in \mathbb{N} : p|n,\ p \text{ primo}\}$ o conjunto dos factores primos de n. Sabemos que P é majorado (n é um majorante) e não-vazio (de acordo com a Proposição 2.7.1). P tem portanto um elemento máximo q. Se $q = n$, então n é primo, e tomamos $k = 1$ e $p_1 = q = n$. Caso contrário, $q < n$ e, portanto, $n = mq$, onde $2 \leq m < n$. Pela hipótese de indução, existem números primos $p_1 \leq p_2 \leq \cdots \leq p_{k'}$ tais que $m = \prod_{i=1}^{k'} p_i$, todos eles majorados por q. Tomamos neste caso $k = k' + 1$, e $p_k = q$. □

Verificámos acima a *existência* de factorizações em primos para qualquer natural $n > 2$. A questão da *unicidade* dessas factorizações (a menos da ordem dos factores) será esclarecida em seguida, mas convém desde já notar que corresponde a um problema conceptualmente distinto do anterior, como se ilustra no exemplo seguinte.

Exemplo 2.7.3.

Se classificarmos como "primos" no anel dos números pares *os inteiros pares que não podem ser expressos como produtos de outros inteiros* pares*, é fácil constatar que* 2*,* 6 *e* 18 *são "primos". Deixaremos para os exercícios a demonstração dos análogos dos resultados anteriores para este anel que, tal como o dos inteiros, é bem ordenado. Por outro lado, como* $36 = 2 \cdot 18 = 6 \cdot 6$*, é óbvio que as decomposições em "primos" não são únicas no anel dos inteiros pares.*

O resultado fundamental para provar a unicidade das factorizações em primos no anel dos inteiros é o seguinte lema.

Lema 2.7.4 (Euclides). *Sejam* $m, n, p \in \mathbb{Z}$ *e suponha-se que* p *é um número primo. Se* p *é factor do produto* mn*, então* p *é factor de* m *ou factor de* n*.*

Demonstração. Seja $d = \text{mdc}(m, p)$. Como d é factor de p e p é primo, temos d=1 ou $d = p$.

É evidente que, se $d = p$, então p é factor de m. Se $d = 1$, existem inteiros x e y tais que $1 = xm + yp$, donde $n = nxm + nyp$. Como p é factor de mn, existe também um inteiro z tal que $mn = zp$. Concluímos que $n = xzp + nyp = (zx + ny)p$, e portanto p é factor de n. □

Note-se de passagem que o exemplo apresentado antes do Lema de Euclides mostra que este lema não é aplicável no anel dos inteiros pares, se interpretarmos o qualificativo "primo" como indicámos.

Exemplo 2.7.5.

Uma das descobertas dos matemáticos gregos da Antiguidade que mais os surpreendeu e intrigou foi, em linguagem moderna, a da existência de números irracionais*. Podemos verificar agora sem dificuldade que* $\sqrt{2}$ *é irracional,* i.e.*, que não existem inteiros* n *e* m *tais que* $\left(\frac{n}{m}\right)^2 = 2$*, ou seja,* $n^2 = 2m^2$*. Argumentamos por absurdo.*

Podemos supor sem perda de generalidade que m *e* n *são primos entre si (porquê?). Notamos agora que*

$$n^2 = 2m^2 \Rightarrow 2|n^2 \Rightarrow 2|n,$$

pelo Lema de Euclides. Concluímos que $n = 2k$*, para algum inteiro* k*. Assim,* $n^2 = 4k^2$*, donde* $4k^2 = 2m^2$*, ou ainda* $2k^2 = m^2$*. Como* $2|m^2$*, segue-se novamente do Lema de Euclides que* $2|m$*, contradizendo a hipótese de* m *e* n *serem primos entre si. Concluímos que a equação* $n^2 = 2m^2$ *não tem soluções nos inteiros, e* $\sqrt{2}$ *não é racional.*

Deixamos para os exercícios a generalização deste exemplo para o caso $\sqrt{n}$, quando $n \in \mathbb{N}$ não é um quadrado perfeito. Por palavras, quando n é um natural, a sua raiz quadrada é ou outro natural (caso em que n é um quadrado perfeito) ou é um número irracional.

Podemos generalizar o Lema de Euclides para um qualquer produto finito de inteiros. A demonstração (que fica como exercício) deve ser feita por indução no número de factores.

Corolário 2.7.6. *Se p é primo e $p \mid \prod_{i=1}^{k} m_i$, então:*

(i) $p|m_j$ para algum j, com $1 \leq j \leq k$.

(ii) Se os inteiros m_i são primos, então $p = m_j$, para algum j, com $1 \leq j \leq k$.

Podemos agora enunciar e provar o

Teorema 2.7.7 (Teorema Fundamental da Aritmética). *Qualquer natural $n > 2$ tem uma factorização em primos, que é única a menos da ordem dos factores.*

Demonstração. A *existência* de factorizações em primos decorre do Corolário 2.7.2. Resta-nos por isso provar a sua *unicidade*.

Procedemos como se segue. Supondo que k e m são naturais, $p_1 \leq p_2 \leq \cdots \leq p_k$ e $q_1 \leq q_2 \cdots \leq q_m$ são primos, e

$$\prod_{i=1}^{k} p_i = \prod_{j=1}^{m} q_j,$$

provamos que $k = m$ e $p_i = q_i$. Para isso, argumentamos por indução em k:

Para k =1, o resultado é óbvio da definição de número primo;

Supomos o resultado válido para o natural $k-1$, e

$$\prod_{i=1}^{k} p_i = \prod_{j=1}^{m} q_j.$$

Seja $P = \{p_i : 1 \leq i \leq k\}$ e $Q = \{q_j : 1 \leq j \leq m\}$. Note-se mais uma vez que de acordo com a definição de primo temos necessariamente $m > 1$, porque $k > 1$. Pelo Corolário 2.7.6 é evidente que $p_k \in Q$, donde $p_k \leq q_m$, e analogamente $q_m \in P$, donde $q_m \leq p_k$. Concluímos que $p_k = q_m$, e segue-se da lei do corte que

$$\prod_{i=1}^{k-1} p_i = \prod_{j=1}^{m-1} q_j.$$

Pela hipótese de indução, $k-1 = m-1$ e $p_i = q_i$, para $i < k$, donde $k = m$ e $p_i = q_i$, para $i \leq k$. □

A factorização de n em primos pode evidentemente conter factores repetidos, e é por isso comum escrevê-la na forma

$$n = \prod_{i=1}^{m} {p_i}^{e_i} \qquad (e_i \geq 1),$$

que se diz a *factorização de n em potências primas*. Esta expressão é única, a menos da ordem dos factores.

O Teorema Fundamental da Aritmética não implica directamente a existência dum número infinito de primos. Este último facto foi também descoberto por Euclides.

Teorema 2.7.8 (Euclides). *O conjunto dos primos é ilimitado.*

Demonstração. Pretendemos provar que para qualquer natural n existe um primo $p > n$. Dado um natural n, considere-se o natural $m = n! + 1$, onde $n!$ é o factorial de n. É evidente do Algoritmo de Divisão que o resto da divisão de m por qualquer natural entre 2 e n é 1. Em particular, todos os factores de m, incluindo os seus factores primos (que existem de acordo com a Proposição 2.7.1), são maiores do que n. Concluímos que existem números primos maiores do que n. □

Como acabámos de ver, os números primos formam uma sucessão ilimitada

$$2, 3, 5, 7, 11, 13, \ldots, p_n, \ldots$$

sobre a qual a mais elementar curiosidade sugere algumas perguntas simples. Por exemplo, é possível determinar uma fórmula explícita, envolvendo o natural n, que permita calcular o primo p_n? Quantos números primos existem no intervalo de 1 a n? Até que ponto é difícil determinar os factores primos dum dado natural n?

Sobre a primeira questão mencionada acima, a resposta parece ser negativa. Em particular, não se conhece nenhuma fórmula explícita que produza *apenas* números primos. A título de exemplo, descrevemos aqui uma das mais famosas tentativas nesta direcção, devida a Fermat[11], e que envolveu os números da forma

$$F_n = 2^{2^n} + 1,$$

hoje conhecidos por *números de Fermat*. É fácil calcular os números de Fermat correspondentes a $n = 0$, 1, 2 e 3, obtendo-se respectivamente 3, 5, 17, e 257, todos eles primos. A escolha $n = 4$ corresponde a 65537, que é

[11] Pierre de Fermat (1601-1665), matemático francês. Fermat, advogado de profissão, é um dos personagens mais interessantes da história da Matemática. Foi um dos fundadores do Cálculo Infinitesimal, e descobriu independentemente de Descartes (de quem aliás foi amigo) os princípios da Geometria Analítica. O seu trabalho mais importante foi sem dúvida a criação da moderna Teoria dos Números.

ainda um número primo. Há no entanto números de Fermat que não são primos, como Euler[12] descobriu em 1732 para $n = 5$. Se esta lhe parece uma observação simples de demonstrar, note que $n = 5$ corresponde a

$$2^{2^5} + 1 = 4\ 294\ 967\ 297,$$

e Euler descobriu que a factorização deste número em primos é

$$2^{2^5} + 1 = 641 \cdot (6\ 700\ 417).$$

A escolha do expoente $e = 2^n$ é fácil de explicar. Suponha-se que $F = 2^e + 1$, e $e = ks$, onde $k, s > 1$, com s ímpar. O polinómio $p(x) = x^s + 1$ tem a raiz $x = -1$, logo factoriza-se

$$p(x) = (x + 1)q(x),$$

onde $q(x)$ é um polinómio com coeficientes inteiros. Substituindo x por 2^k, concluímos que

$$F = 2^e + 1 = (2^k)^s + 1 = (2^k + 1)q(2^k),$$

seguindo-se imediatamente que o número F não é primo. Por outras palavras, se $F = 2^e + 1$ é primo então e não tem factores ímpares maiores do que 1, logo o seu único factor primo é 2, donde $e = 2^n$, e F é o número de Fermat F_n.

Apesar do começo "auspicioso" da sucessão de Fermat, não conhecemos números de Fermat com $n > 4$ que sejam primos, e sabemos que alguns desses números são compostos. Sabemos por exemplo que o menor factor primo do número de Fermat correspondente a $n = 1945$ (número esse com mais de 10^{582} dígitos na sua expansão decimal!) é um número primo p de 587 dígitos: $p = 5 \cdot 2^{1947} + 1$, e julga-se que nenhum dos números de Fermat com $n > 4$ é primo. Apesar disso, veremos nos exercícios que estes números podem ser usados para provar a existência de um número infinito de primos.

As questões sobre o número de primos no intervalo de 1 a n, ou sobre a *distribuição dos primos*, referem-se evidentemente à probabilidade de um número natural escolhido ao acaso no intervalo $[1, n]$ ser primo. Estão também directamente relacionadas com o problema mencionado inicialmente, sobre a determinação duma expressão explícita para o enésimo primo. Legendre[13] e Gauss foram os primeiros matemáticos a sugerir uma

[12] Leonhard Euler (1707-1783), matemático suíço. Euler foi um dos mais prodigiosos matemáticos de sempre, tendo trabalhado nas mais diversas áreas da Matemática Pura e Aplicada (análise, geometria, geometria diferencial, teoria dos números, física, mecânica dos fluidos, e outras).

[13] Adrien Marie Legendre (1752-1833), matemático francês. Legendre distinguiu-se na teoria dos números e no estudo das funções elípticas.

expressão *aproximada* para o número de primos $< x$, que designamos por $\pi(x)$. Nos finais do século *XIX*, Hadamard [14] provou que

$$\frac{\pi(x)}{\frac{x}{\log x}} \to 1 \text{ quando } x \to \infty.$$

Não provaremos aqui resultados desta natureza, que tipicamente requerem técnicas analíticas para a sua demonstração.

Problemas como os referidos são talvez dos mais teóricos e difíceis que podemos conceber, e ilustram bem as capacidades e limitações do espírito humano. Apesar da sua origem, têm também reflexos interessantes na vida actual. Referiremos adiante técnicas de Criptografia que exploram a relativa facilidade de cálculo de grandes números primos, comparada com a dificuldade de determinar os factores primos dos naturais que podemos obter pela multiplicação desses primos. Neste contexto, os números "grandes" podem ter mais duma centena de dígitos; a sua factorização por verificação sequencial de todos os possíveis factores envolveria um número de divisões da ordem de 10^{50}! Não sabemos até que ponto é possível estabelecer um algoritmo prático para a factorização de números desta ordem de grandeza, mas enquanto essa ignorância se mantiver, as mais secretas comunicações políticas e militares poderão continuar a fazer-se com segurança recorrendo aos números primos. É difícil neste momento indicarmos outros problemas "práticos" onde as propriedades dos números primos têm reflexos importantes, porque todos tendem a ser tecnicamente sofisticados. Refira-se no entanto que o problema do reconhecimento da fala por computadores exige o desenvolvimento de algoritmos tão rápidos quanto possível para a decomposição de sons nas suas frequências fundamentais, uma técnica conhecida como Análise de Fourier. A velocidade teórica máxima desses algoritmos está directamente relacionada com a função $\pi(x)$.

Exercícios.

1. Se $n = \prod_{i=1}^{k} {p_i}^{e_i}$ e $m = \prod_{i=1}^{k} {p_i}^{f_i}$ com $e_i, f_i \geq 0$ inteiros, obtenha expressões para o $\text{mdc}(n, m)$ e $\text{mmc}(n, m)$.

2. Sejam p e q primos distintos, e $n = p^2q^3$. Conte os factores naturais de n, e mostre que a sua soma é $(1 + p + p^2)(1 + q + q^2 + q^3)$.

3. Generalize o resultado anterior para o caso em que $n = \prod_{i=1}^{k} {p_i}^{e_i}$.

4. Prove uma versão do Corolário 2.7.2 para o anel dos inteiros pares.

5. Demonstre o Corolário 2.7.6.

[14] Jacques Hadamard (1865-1963), um dos matemáticos franceses mais influentes do virar dos séculos *XIX* e *XX*, e que trabalhou em domínios muito diferentes da Matemática (*e.g.*, na teoria do números e no cálculo de variações).

6. Prove que, para qualquer natural n, o intervalo $[n+1, n!+1]$ contém pelo menos um primo.

7. Os primos da forma $2^n - 1$ dizem-se PRIMOS DE MERSENNE. Prove que, se $a^n - 1$ é primo e $n > 1$, então $a = 2$ e n é primo.

8. Prove que a sucessão $a_n = n^2 - n + 41$ não é só constituída por primos.

9. Mostre que, se $p(x)$ é um polinómio não-constante com coeficientes inteiros, então o conjunto dos inteiros n para os quais $a_n = p(n)$ não é primo é infinito.

10. Seja $F_n = 2^{2^n} + 1$ o enésimo número de Fermat ($n \geq 0$).
    (a) Prove que $F_{n+1} = 2 + \prod_{i=0}^{n} F_i$;
    (b) Prove que se $n \neq m$ então $\text{mdc}(F_n, F_m) = 1$;
    (c) Porque é que o resultado anterior estabelece a existência de um número infinito de primos?

11. Prove que, se n não é um quadrado perfeito, então $\sqrt{n}$ é irracional (*i.e.*, a equação $x^2 = ny^2$ não tem soluções $x, y \in \mathbb{Z}$).

2.8 Congruências

Estudaremos nesta secção novas relações binárias em $\mathbb{Z}$, as de "*congruência módulo m*", associadas à relação de divisibilidade. Usaremos a teoria aqui desenvolvida para resolver equações do tipo $ax + by = n$, onde todas as variáveis são *inteiros*. No próximo capítulo, as mesmas ideias serão usadas para exibir uma classe muito importante de anéis finitos.

Definição 2.8.1. Se $x, y \in \mathbb{Z}$, dizemos que x é CONGRUENTE MÓDULO m com y se e só se $x - y$ é múltiplo de m. O inteiro m diz-se o MÓDULO DE CONGRUÊNCIA.

Se x é congruente com y módulo m, escrevemos $x \equiv y \pmod{m}$. Temos portanto

$$x \equiv y \pmod{m} \iff m|(x-y) \iff (x-y) \in \langle m \rangle.$$

Recorde-se que uma relação binária se diz uma RELAÇÃO DE EQUIVALÊNCIA quando é *reflexiva*, *simétrica* e *transitiva*.

Proposição 2.8.2. *A relação de congruência módulo m é de equivalência.*

Demonstração. Vejamos que a relação de congruência módulo m satisfaz as três propriedades:

(i) $\equiv$ é reflexiva: Como 0 é múltiplo de m, temos

$$x \equiv x \pmod{m}.$$

(ii) $\equiv$ é simétrica: É claro que $x - y = km$ se, e só se, $y - x = (-k)m$, logo

$$x \equiv y \pmod{m} \iff y \equiv x \pmod{m}.$$

(iii) $\equiv$ é transitiva: Se $x \equiv y \pmod{m}$ e $y \equiv z \pmod{m}$, então existem inteiros k e n tais que $x - y = km$ e $y - z = nm$. Mas então,

$$x - z = (x - y) + (y - z) = km + nm = (k + n)m,$$

logo $x \equiv z \pmod{m}$. □

Exemplos 2.8.3.

1. *Ignorando a incógnita y, a equação $3 = 21x + 30y$ (x, y inteiros) escreve-se*

$$3 \equiv 21x \pmod{30}, \text{ ou } 21x \equiv 3 \pmod{30}.$$

2. *Se $m = 0$, então como 0 é o único múltiplo de 0,*

$$x \equiv y \pmod{0} \iff x = y,$$

ou seja, a relação de congruência módulo 0 é a habitual relação de igualdade. Num outro extremo, se $m = 1$, então $x \equiv y \pmod{1}$, para qualquer $x, y \in \mathbb{Z}$ (o inteiro $x - y$ é sempre múltiplo de 1).

3. *Qualquer inteiro n é par ou ímpar,* i.e., *$n = 0 + 2k$ ou $n = 1 + 2k$. Portanto*

$$n \equiv 0 \pmod{2}, \text{ ou } n \equiv 1 \pmod{2}.$$

De acordo com o Algoritmo de Divisão, se $m > 0$ e x é fixo, então $x = mq + r$, onde $q, r \in \mathbb{Z}$ (*i.e.*, $x \equiv r \pmod{m}$), e estes inteiros são únicos se $0 \leq r < m$. Portanto, $x \equiv r \pmod{m}$, com $0 \leq r < m$, se e só se r é o resto da divisão de x por m. É consequentemente fácil generalizar a observação acima, a propósito de $m = 2$, a qualquer $m > 0$.

Proposição 2.8.4. *Se $m > 0$, qualquer inteiro x é congruente com exactamente um inteiro r do conjunto $\{0, 1, 2, \ldots, m - 1\}$, onde r é o resto da divisão de x por m.*

Com $m \neq 0$ fixo, o conjunto $\{x \in \mathbb{Z} : x \equiv r \pmod{m}\}$ diz-se por esta razão uma CLASSE DE RESTOS. Veremos no próximo capítulo que a família das classes de restos $\pmod{m}$ é na realidade o *suporte* do anel $\mathbb{Z}_m$, de que já mencionámos, informalmente, alguns exemplos, como $\mathbb{Z}_2$ e $\mathbb{Z}_3$.

Exemplo 2.8.5.

Qualquer inteiro x verifica exactamente uma das equações

$$x \equiv 0 \pmod 4,\ x \equiv 1 \pmod 4,\ x \equiv 2 \pmod 4 \text{ ou } x \equiv 3 \pmod 4.$$

As equações que envolvem relações de congruência podem ser manipuladas como equações algébricas vulgares, excepto no que diz respeito à "lei do corte" para o produto.

Proposição 2.8.6. *Se $x \equiv x' \pmod m$ e $y \equiv y' \pmod m$, então verificam-se as propriedades:*

(i) $x \pm y \equiv x' \pm y' \pmod m$;

(ii) $xy \equiv x'y' \pmod m$.

Em particular, temos que:

(iii) $x \equiv x' \pmod m \Leftrightarrow x + a \equiv x' + a \pmod m$;

(iv) $x \equiv x' \pmod m \Rightarrow ax \equiv ax' \pmod m$.

Demonstração. Por hipótese, tanto $x - x'$ como $y - y'$ são múltiplos de m. É portanto evidente que $(x - x') \pm (y - y') = (x \pm y) - (x' \pm y')$ são múltiplos de m, *i.e.*, $x \pm y \equiv x' \pm y' \pmod m$.

Por outro lado, $(x - x')y$ e $x'(y' - y)$ são ainda múltiplos de m. Por isso, $(x - x')y - x'(y' - y) = xy - x'y'$ é múltiplo de m, ou seja, $xy \equiv x'y' \pmod m$.

Deixamos as restantes afirmações para os exercícios. □

Exemplo 2.8.7.

É claro que $10 \equiv 3 \pmod 7$ *e* $11 \equiv -3 \pmod 7$. *De acordo com a Proposição 2.8.6, temos que*

$$\begin{aligned} 10 + 11 \equiv 3 + (-3) \pmod 7 &\iff 21 \equiv 0 \pmod 7, \\ 10 - 11 \equiv 3 - (-3) \pmod 7 &\iff -1 \equiv 6 \pmod 7, \\ 10 \cdot 11 \equiv 3 \cdot (-3) \pmod 7 &\iff 110 \equiv -9 \pmod 7. \end{aligned}$$

Por outro lado, observe que

$$4 \cdot 5 \equiv 4 \cdot 8 \pmod 6,$$

mas $5 \not\equiv 8 \pmod 6$. *Assim, em geral,* $ax \equiv ax' \pmod m$ *não implica* $x \equiv x' \pmod m$.

É importante compreender que a Proposição 2.8.6 usa precisamente as propriedades de $\langle m \rangle$ que tornam este conjunto um ideal. A demonstração do seguinte corolário desta proposição fica como exercício.

Corolário 2.8.8. *Se* $x \equiv y \pmod{m}$*, então* $x^n \equiv y^n \pmod{m}$ *para todo o natural* n*.*

Uma das aplicações mais simples da Proposição 2.8.6 e do seu Corolário é o estabelecimento de *critérios de divisibilidade* de n por m em termos dos algarismos da representação decimal de x.

Exemplo 2.8.9.

Tomando $m = 3$*, observamos que*

$$10 \equiv 1 \pmod{3} \Longrightarrow 10^k \equiv 1 \pmod{3} \text{ para qualquer natural } k.$$

Para $n = 1998$*, notamos que*

$$1998 = 1 \cdot 1000 + 9 \cdot 100 + 9 \cdot 10 + 8,$$

logo:

$$1998 \equiv 1 + 9 + 9 + 8 \equiv 27 \equiv 0 \pmod{3}.$$

Concluímos, assim, que o número 1998 *é divisível por* 3*, sem que para tal seja necessário usar o Algoritmo de Divisão.*

Este exemplo ilustra o seguinte critério de divisibilidade:

Proposição 2.8.10. *O natural* n *é divisível por* 3 *se e só se a soma dos dígitos da sua representação decimal é divisível por* 3*.*

Deixamos para os exercícios os critérios de divisibilidade por 2, 5, 9 e 11.

Passamos agora a estudar em pormenor as equações (lineares) do tipo $ax \equiv b \pmod{m}$. Como sabemos, a equação $ax = b$ só tem soluções inteiras quando b é múltiplo de a, sendo a sua solução nestes casos única (excepto se $a = 0$). Pretendemos determinar os valores de b (em termos de a e m) para os quais a equação $ax \equiv b \pmod{m}$ tem soluções, e estabelecer algoritmos de cálculo de *todas* as suas soluções.

É interessante reconhecer que a questão da existência de soluções para $ax \equiv b \pmod{m}$ se reduz às ideias que introduzimos a propósito do máximo divisor comum de dois inteiros.

Teorema 2.8.11. *A equação* $ax \equiv b \pmod{m}$ *tem soluções, se e só se* b *é múltiplo de* $d = \text{mdc}(a, m)$*.*

Demonstração. Na realidade, $ax \equiv b \pmod{m}$ tem soluções se e só existem inteiros x e y tais que $b - ax = my$, *i.e.*, $b = ax + my$. Dito doutra forma, $ax \equiv b \pmod{m}$ tem soluções precisamente quando b é uma combinação linear de a e m com coeficientes inteiros. Como vimos na Secção 2.6 (ver Definição 2.6.8), as combinações lineares de a e m com coeficientes inteiros são exactamente os múltiplos de $\text{mdc}(a, m)$. □

De um ponto de vista prático, o resultado anterior mostra que a existência de soluções da equação $ax \equiv b \pmod{m}$ pode ser decidida com o auxílio do Algoritmo de Euclides. Na realidade, como este permite obter $d = \text{mdc}(a, m)$ como combinação linear de a e m, obtemos também uma solução de $ax \equiv d \pmod{m}$, e desta obtemos facilmente soluções da equação original. Ilustramos este procedimento no próximo exemplo.

Exemplo 2.8.12.

Considere-se a equação

$$15x \equiv b \pmod{40}.$$

Usando o Algoritmo de Euclides, temos

$$\begin{aligned}
&40 = 15 \cdot 2 + 10, \text{ ou } 10 = 40 + 15 \cdot (-2),\\
&15 = 10 \cdot 1 + 5, \text{ ou } 5 = 15 + 10 \cdot (-1) = 15 \cdot 3 + 40 \cdot (-1),\\
&10 = 5 \cdot 2 + 0, \text{ logo } 5 = \text{mdc}(15, 40) = 15 \cdot 3 + 40 \cdot (-1).
\end{aligned}$$

Concluímos do Teorema 2.8.11 que a equação tem soluções precisamente quando b é múltiplo de 5.

Ainda de acordo com os mesmos cálculos, temos

$$5 = 15 \cdot 3 + 40 \cdot (-1),$$

donde x=3 é solução de $15x \equiv 5 \pmod{40}$, ou mais geralmente $x = 3k$ é solução de $15x \equiv 5k \pmod{40}$. Tomando como exemplo a equação $15x \equiv 10 \pmod{40}$, observamos que $x = 6$ é uma sua solução óbvia, porque

$$15 \cdot 3 \equiv 5 \pmod{40} \Longrightarrow 15 \cdot 3 \cdot 2 \equiv 5 \cdot 2 \pmod{40},$$

de acordo com a Proposição 2.8.6. É evidente que qualquer inteiro x que verifique $x \equiv 6 \pmod{40}$ é também solução de $15x \equiv 10 \pmod{40}$, e portanto esta última equação tem um número infinito de soluções.

No entanto, os inteiros que satisfazem $x \equiv 6 \pmod{40}$ não *incluem todas as soluções de $15x \equiv 10 \pmod{40}$, e. g., $x = -2$ é solução de $15x \equiv 10 \pmod{40}$, mas $-2 \not\equiv 6 \pmod{40}$. É claro que este facto é um outro reflexo da ausência de uma "lei do corte" geral para o produto, porque*

$$3 \cdot 5 \cdot (-2) \equiv 5 \cdot 2 \pmod{40} \not\Rightarrow 6 \equiv -2 \pmod{40}.$$

Analisamos agora as circunstâncias em que esta multiplicidade de soluções que existia neste exemplo não é possível. Segue-se também do Teorema 2.8.11 que a equação $ax \equiv b \pmod{m}$ tem soluções para *qualquer* b precisamente quando $\text{mdc}(a, m) = 1$, ou seja, quando a e m são primos entre si. Este caso ocorre evidentemente quando a equação $ax \equiv 1 \pmod{m}$ tem soluções.

Definição 2.8.13. Diz-se que $a \in \mathbb{Z}$ é INVERTÍVEL $\pmod{m}$ se e só se $ax \equiv 1 \pmod{m}$ tem solução, *i.e.*, se e só se a e m são primos entre si. Se a' é solução da equação $ax \equiv 1 \pmod{m}$, dizemos que a' é INVERSO $\pmod{m}$ de a.

Exemplos 2.8.14.

1. *A equação* $4x \equiv b \pmod 9$ *tem soluções para qualquer* b*, pois vemos que* $\text{mdc}(4,9) = 1$*. Em particular,* $4x \equiv 1 \pmod 9$ *tem a solução* $x = -2$ *porque* $4(-2) + 9 = 1$*. Portanto,*
   (a) -2 *é inverso de* $4 \pmod 9$*, e*
   (b) $x = -2b$ *é solução de* $4x \equiv b \pmod 9$*, qualquer que seja o inteiro* b*.*
2. *Como* $\text{mdc}(21, 30) = 3$*,* 21 *não é invertível* $\pmod{30}$*.*

Suponha-se que $x = c$ é uma solução particular de $ax \equiv b \pmod m$. Já observámos que qualquer inteiro x' congruente com c é também solução da mesma equação, ou seja,

$$x' \equiv c \pmod m \Longrightarrow ax' \equiv ac \equiv b \pmod m,$$

mas que podem existir soluções x'' que não são congruentes com c, *i.e.*, podemos ter

$$ax'' \equiv b \pmod m \text{ com } x'' \not\equiv c \pmod m.$$

No entanto, se a e m são primos entre si, é agora fácil constatar que este último caso é impossível, em virtude da seguinte "lei do corte".

Teorema 2.8.15. *Se* a *e* m *são primos entre si,*

$$ax \equiv ay \pmod m \iff x \equiv y \pmod m.$$

Demonstração. Já sabemos que

$$x \equiv y \pmod m \Longrightarrow ax \equiv ay.$$

Por outro lado, seja a' um inverso $\pmod m$ de a, donde $aa' \equiv a'a \equiv 1 \pmod m$. Então

$$\begin{aligned} ax \equiv ay \pmod m &\Longrightarrow a'(ax) \equiv a'(ay) \pmod m \quad \text{(Proposição 2.8.6)}, \\ &\Longrightarrow (a'a)x \equiv (a'a)y \pmod m \quad \text{(associatividade)}, \\ &\Longrightarrow x \equiv y \pmod m \quad (a'a \equiv 1 \pmod m). \end{aligned}$$

□

Concluímos dos Teoremas 2.8.11 e 2.8.15 que

Teorema 2.8.16. *Se* a *e* m *são primos entre si e* $b \in \mathbb{Z}$*, então:*

(i) A equação $ax \equiv b \pmod m$ *tem pelo menos uma solução* $c \in \mathbb{Z}$*;*

(ii) $ax \equiv b \pmod m \Rightarrow x \equiv c \pmod m$.

Temos pois um método simples para resolver a equação linear $ax \equiv b \pmod{m}$ no caso em que a e m são primos entre si. Isto mesmo é ilustrado no próximo exemplo.

Exemplo 2.8.17.

Como $\mathrm{mdc}(4,7) = 1$*, e* $4 \cdot 2 \equiv 1 \pmod{7}$*, concluímos que as soluções de* $4x \equiv 1 \pmod{7}$ *(os inversos de* $4 \pmod{7}$*) são precisamente os inteiros que satisfazem* $x \equiv 2 \pmod{7}$*, ou seja, são os números da forma* $x = 2 + 7k$*. Tomando como exemplo b=3, temos*

$$4x \equiv 3 \pmod{7} \iff x \equiv 6 \pmod{7}.$$

Quando a e m não são primos entre si, é mesmo assim fácil determinar todas as soluções da equação

$$ax \equiv b \pmod{m}.$$

Convém para isso recordar que, se $a = a'd$ e $m = m'd$ com $d = \mathrm{mdc}(a,m) \neq 0$, então a' e m' são primos entre si.

Exemplo 2.8.18.

Para calcular todas *as soluções de* $15x \equiv 10 \pmod{40}$*, notamos que esta equação é equivalente a* $15x = 10 + 40y$*, que dividimos por* $\mathrm{mdc}(15,40) = 5$ *para obter* $3x = 2 + 8y$*, ou* $3x \equiv 2 \pmod{8}$*. Temos portanto*

$$15x \equiv 10 \pmod{40} \iff 3x \equiv 2 \pmod{8},$$

onde naturalmente na última equação $\mathrm{mdc}(3,8) = 1$*. Já vimos que* $x = 6$ *é solução da equação original, e consequentemente de* $3x \equiv 2 \pmod{8}$*. Segue-se, do Teorema 2.8.16, que as soluções da segunda equação são os inteiros que satisfazem* $x \equiv 6 \pmod{8}$*.*

Concluímos que as soluções de $15x \equiv 10 \pmod{40}$ *são os números da forma* $x = 6 + 8k$*. Em particular, é claro que a primeira equação tem 5 soluções que não são congruentes* $\pmod{40}$*, nomeadamente,* $x = 6, 14, 22, 30, 38$ *(a solução que referimos anteriormente,* i.e.*,* $x = -2$*, corresponde a* $x = 38$*).*

Veremos nos exercícios como calcular o número de soluções da equação $ax \equiv b \pmod{m}$ que não são congruentes entre si para o módulo m.

Teremos ocasionalmente necessidade de resolver sistemas do tipo

$$\left\{ \begin{array}{ll} x \equiv a & \pmod{m}, \\ x \equiv b & \pmod{n}. \end{array} \right. \tag{2.8.1}$$

O resultado seguinte foi descoberto pelo matemático chinês Sun-Tsu (no século *I*!) e por isso é muitas vezes referido pela designação de *Teorema Chinês do Resto*.

Teorema 2.8.19 (Teorema Chinês do Resto). *O sistema (2.8.1) tem soluções para quaisquer a e b se e só se m e n são primos entre si. Neste caso, se c é uma solução, então (2.8.1) é equivalente a $x \equiv c \pmod{mn}$.*

Demonstração. É evidente que os inteiros da forma $x = a + ym$ são as soluções da equação $x \equiv a \pmod{m}$. Portanto $x = a + ym$ é solução de (2.8.1) se e só se

$$x \equiv b \pmod{n} \Rightarrow a + ym \equiv b \pmod{n} \Rightarrow my \equiv b - a \pmod{n}.$$

Pelo que vimos acima, esta última equação tem solução para quaisquer a e b se e só se m e n são primos entre si. Nesse caso, segue-se, do Teorema 2.8.16, que as soluções são os inteiros da forma $y = y' + zn$, onde y' é uma qualquer solução fixa, e z é arbitrário. Concluímos que as soluções do sistema (2.8.1) são os inteiros da forma $x = a + (y' + zn)m = c + z(nm)$, onde $c = a + y'm$, *i.e.*, são as soluções de $x \equiv c \pmod{mn}$. □

O caso em que m e n não são primos entre si será tratado num exercício da próxima secção.

Exemplo 2.8.20.

Considere-se o sistema

$$\begin{cases} x \equiv 1 & \pmod 4, \\ x \equiv 2 & \pmod 9. \end{cases}$$

As soluções da primeira equação são os inteiros da forma $x = 1 + 4y$, que de acordo com a segunda equação devem também satisfazer

$$1 + 4y \equiv 2 \pmod 9 \iff 4y \equiv 1 \pmod 9 \text{ com solução } y = -2$$

(vimos acima que -2 é inverso de $4 \pmod 9$). Concluímos que $c = 1+4(-2) = -7$ é uma solução particular do sistema, sistema esse que é portanto equivalente à equação $x \equiv -7 \pmod{36}$. As suas soluções são consequentemente os inteiros da forma $x = -7 + 36z$, com $z \in \mathbb{Z}$.

Nas equações que temos vindo a estudar as incógnitas são *inteiros*. Por este motivo, estas equações dizem-se *diofantinas*[15]. Apesar da relativa simplicidade da teoria que expusemos (que diz respeito basicamente a equações lineares do tipo $ax + by = n$), deve notar-se que alguns dos problemas mais difíceis (e mais famosos) da Matemática se referem a equações diofantinas não-lineares. Um dos exemplos mais célebres é o chamado "*Último Teorema de Fermat*", que envolve a equação $x^n + y^n = z^n$. Apesar de esta equação ter

[15] De Diofanto de Alexandria, matemático grego do século *III*, autor do tratado *Arithmetica*, onde se expunham entre outros assuntos soluções (por vezes extremamente engenhosas!) de equações algébricas. Diofanto apenas se interessava pelas soluções racionais, e designava as irracionais por "impossíveis".

um número infinito de soluções para n=2 (*e.g.*, $x = 3$, $y = 4$ e $z = 5$), nunca se encontraram soluções naturais para $n > 2$. Fermat escreveu na margem duma cópia da *Arithmetica* de Diofanto, junto à discussão sobre o teorema de Pitágoras, que sabia demonstrar a não-existência de soluções para $n > 2$, mas que a margem do livro era demasiado pequena para descrever o seu argumento. Não nos chegou até hoje a demonstração de Fermat. De facto, foi preciso esperar 300 anos, e pelos esforços de gerações de matemáticos famosos, para que se obtivesse uma demonstração completa do Último Teorema de Fermat . Esta demonstração, devida ao matemático americano Andrew Wiles[16], é sem dúvida uma das grandes descobertas da Matemática contemporânea. O grau de sofisticação da demonstração, que culmina os trabalhos de matemáticos célebres ao longo de mais de 200 anos, é tal que a transforma numa das mais elaboradas construções intelectuais alcançadas pela humanidade.

Exercícios.

1. Calcule todas as soluções (inteiras) de $21x + 30y = 9$.

2. Para que inteiros b é que a equação $533x \equiv b \pmod{4141}$ tem soluções?

3. Enuncie e demonstre critérios de divisibilidade por $2, 5, 9$ e 11, em termos da representação decimal de um natural n.

4. Calcule para qualquer natural k o resto da divisão de 3^k por 7.

5. Determine todas as soluções de $xy \equiv 0 \pmod{12}$.

6. Prove que exactamente uma das seguintes alternativas é válida para qualquer $a, m \in \mathbb{Z}$, $m \neq 0$:
   (a) a equação $ax \equiv 1 \pmod{m}$ tem soluções (caso $\text{mdc}(a, m) = 1$), ou
   (b) a equação $ax \equiv 0 \pmod{m}$ tem soluções $x \not\equiv 0 \pmod{m}$ (caso em que $\text{mdc}(a, m) \neq 1$).

7. Suponha que $\text{mdc}(a, m) = d$, e $m = dn$. Prove que:
   (a) a equação $ax \equiv 0 \pmod{m}$ tem d soluções x, com $0 < x \leq m$, que são $n, 2n, \ldots, dn$;

[16] Andrew Wiles anunciou no Verão de 1993 que possuía uma demonstração do Último Teorema de Fermat. Veio posteriormente a verificar-se que de facto nessa demonstração faltava justificar um passo crucial. Finalmente, em Setembro de 1994 o próprio Wiles em conjunto com Richard Taylor descobriram um argumento que permite evitar esse passo. A demonstração correcta foi entretanto publicada sob o título "Modular elliptic curves and Fermat's last theorem", *Ann. of Math.* **141** (1995), no. 3, 443–551, e recorre ao artigo seguinte dos *Annals* que é precisamente o artigo conjunto de Wiles e Taylor, "Ring-theoretic properties of certain Hecke algebras", *Ann. of Math.* **141** (1995), no. 3, 553–572.

(b) a equação $ax \equiv b \pmod{m}$ tem 0 ou d soluções x, com $0 < x \leq m$.

8. Prove que a equação $x^2 + 1 \equiv 0 \pmod{11}$ não tem soluções.

9. Determine quais são os números entre 1 e 8 que possuem inverso (mod 9).

10. Calcule todas as soluções da equação $x^2 + 1 \equiv 0 \pmod{13}$.

11. Prove que $x^5 - x \equiv 0 \pmod{30}$ para qualquer inteiro x.

12. Prove que, se $a \equiv a' \pmod{m}$, então $\text{mdc}(a, m) = \text{mdc}(a', m)$.

13. Para que valores de $c \in \mathbb{Z}$ é que o sistema

$$\begin{cases} x \equiv c & (\text{mod } 14) \\ 2x \equiv 10 & (\text{mod } 42) \end{cases}$$

tem soluções?

14. Resolva o sistema de equações

$$\begin{cases} 2x + 3y \equiv 3 & (\text{mod } 5) \\ 3x + y \equiv 4 & (\text{mod } 5). \end{cases}$$

15. Que dia da semana foi 15 de Março de 1800?
(SUGESTÃO: No calendário actual (chamado Calendário Gregoriano) um ano é bissexto se for divisível por 4 mas não por 100 ou se for divisível por 400.).

16. Cinco náufragos chegam a uma ilha onde encontram um chimpanzé. Depois de passarem o dia a apanhar cocos, decidem deixar a divisão dos cocos para o dia seguinte. Durante a noite, os náufragos acordam sucessivamente e vão buscar o que julgam ser a sua parte dos cocos. Todos eles descobrem que não podem dividir os cocos exactamente por 5, sobrando-lhes sempre 1 coco que deixam para o chimpanzé. No dia seguinte, dividem os cocos que sobraram das suas sucessivas incursões nocturnas por 5, e desta vez a divisão é exacta. Quantos cocos tinham apanhado no dia anterior, sabendo que apanharam menos de 10 000?

2.9 Factorização Prima e Criptografia

A título de exemplo, vamos descrever em detalhe uma aplicação das ideias anteriores à Criptografia. Precisamos para isso de alguns resultados preliminares. Supomos conhecida a expressão para C_k^n, o "número de combinações de n elementos em grupos de k", e em particular a equação

$$k!(n-k)!C_k^n = n!.$$

Como $n|n!$, é evidente, da equação anterior e do Lema de Euclides, que, se $n = p$ é primo e k verifica $0 < k < p$, então $p|C_k^p$. Enunciamos este resultado na seguinte forma:

Lema 2.9.1. *Se p é primo e $0 < k < p$, então $C_k^p \equiv 0 \pmod{p}$.*

Supomos também conhecida a fórmula do binómio de Newton, que pode em qualquer caso ser demonstrada por indução em qualquer anel comutativo. Esta fórmula é

$$(a+b)^n = \sum_{k=0}^{n} C_k^n a^k b^{n-k}. \tag{2.9.1}$$

No caso em que $n = p$ é primo, concluímos sem dificuldade que

Proposição 2.9.2 ("A fórmula do caloiro"). *Se p é primo, $(a+b)^p \equiv a^p + b^p \pmod{p}$.*

Demonstração. Pelo Lema 2.9.1, os únicos termos da expansão do binómio que podem não ser congruentes com zero (mod p) correspondem a $k = 0$ e $k = n$. □

Teorema 2.9.3 (Fermat). *Se p é primo, $a^p \equiv a \pmod{p}$.*

Demonstração. Provaremos este resultado por indução em a. O resultado é óbvio para $a = 0$. Se for verdadeiro para um inteiro $a \geq 0$, temos $(a+1)^p \equiv a^p + 1 \pmod{p}$, pela fórmula do caloiro, e $a^p \equiv a \pmod{p}$, pela hipótese de indução. Concluímos que $(a+1)^p \equiv a+1 \pmod{p}$, e o resultado é verdadeiro para qualquer inteiro $a \geq 0$. Como $(-1)^p \equiv (-1) \pmod{p}$ para qualquer primo p (porquê?), o resultado é válido para qualquer inteiro. □

Um corolário interessante deste teorema é o seguinte, que descreve explicitamente como calcular inversos (mod p).

Corolário 2.9.4. *Se p é primo e $a \not\equiv 0 \pmod{p}$, então $a^{p-1} \equiv 1 \pmod{p}$.*

Demonstração. É evidente que $\mathrm{mdc}(a,p) = p$ (donde $a \equiv 0 \pmod{p}$) ou então $\mathrm{mdc}(a,p) = 1$. Temos portanto e por hipótese que $\mathrm{mdc}(a,p) = 1$. De acordo com a lei do corte, obtemos, do teorema, que

$$a^p = a^{p-1}a \equiv a \pmod{p} \Longrightarrow a^{p-1} \equiv 1 \pmod{p}.$$

□

Podemos agora expor um mecanismo de codificação particularmente astucioso, do tipo a que se chama de *chave pública*. Esta expressão é utilizada porque o processo de codificação pode ser conhecido por todos, sendo apenas o processo de descodificação mantido secreto. Este tipo de codificação é por exemplo utilizado na Internet em transacções financeiras[17].

[17] O sistema mais utilizado na Internet é o chamado sistema de codificação RSA (descoberto por Rivest, Shamir e Adleman) ou suas variantes. Este é um sistema de chave pública, como o que descrevemos, que inclui ainda um esquema simples (mas engenhoso) de verificação de assinatura, crucial nas comunicações privadas via canais públicos.

Os ingredientes fundamentais são um natural N, da forma $N = pq$, onde p e q são primos distintos, e um outro natural r, que deve ser primo relativamente a $p-1$ e a $q-1$. Os números N e r são do domínio público, mas a factorização de N deve ser mantida secreta. Este sistema explora portanto a possibilidade de determinar números primos grandes, juntamente com a dificuldade de cálculo dos factores primos de naturais grandes.

O procedimento a seguir é o seguinte: os símbolos a transmitir são números a verificando $0 \leq a \leq N$. Em lugar de transmitir a, transmite-se o resto da divisão de a^r por N, que designamos por $b = \rho(a^r, N)$. A descodificação corresponde ao cálculo de a, conhecido $b = \rho(a^r, N)$. Este cálculo, por sua vez, só é prático se conhecidos os factores primos de N, e neste caso é uma aplicação de alguns dos resultados acima.

Por um lado, tomando $c = \rho(b, p)$ e $d = \rho(b, q)$, é evidente que

$$c \equiv a^r \pmod{p} \text{ e } d \equiv a^r \pmod{q}.$$

Por outro lado, como r é suposto primo relativamente a $p-1$ e $q-1$, existem inteiros x, y, x', y' tais que

$$1 = rx + (p-1)y = rx' + (q-1)y',$$

donde

$$\begin{aligned} a = a^{rx+(p-1)y} \equiv (a^r)^x \equiv c^x \pmod{p}, e \\ a = a^{rx'+(q-1)y'} \equiv (a^r)^{x'} \equiv d^{x'} \pmod{q}, \end{aligned}$$

de acordo com o corolário acima. Note-se que o cálculo de x e x' pode ser feito directamente com o Algoritmo de Euclides. As potências negativas de a devem ser interpretadas como potências positivas dum inverso de a, mas é claro que x e x' podem ser sempre escolhidos ambos positivos.

Concluímos que a mensagem original a satisfaz o sistema

$$\begin{cases} a \equiv (\rho(b,p))^x \pmod{p} \\ a \equiv (\rho(b,q))^{x'} \pmod{q} \end{cases}.$$

De acordo com o Teorema Chinês do Resto, estas equações determinam unicamente $a \pmod{pq}$, *i.e.*, $\pmod{N}$. A sua resolução envolve apenas conhecer um inverso de $p \pmod{q}$, o que representa mais uma vez uma aplicação do Algoritmo de Euclides. Isto tudo é ilustrado no exemplo seguinte.

Exemplo 2.9.5.

Seja $N = 21 = 3 \cdot 7 = p \cdot q$, e $r = 5$ que é primo relativamente a $p - 1 = 2$ e $q - 1 = 6$. Suponhamos que se quer transmitir a mensagem $a = 4$. De acordo com o procedimento descrito acima, em vez de transmitir a, transmite-se o resto da divisão de $a^r = 1024$ por $N = 21$, que é $b = \rho(1024, 21) = 16$ (pois $1024 = 48 \cdot 21 + 16$).

Suponhamos que recebíamos a mensagem codificada $b = 16$ *e que queríamos descodificar, de forma a recuperar a mensagem* a *(que desconhecíamos). Como*

$$1 = 5 \cdot (-1) + 2 \cdot 3 = 5 \cdot (-1) + 6' \cdot 1,$$

concluímos que $x = -1$ *e* $x' = -1$*. Por sua vez, os números* c *e* d *são dados por*

$$c = \rho(b, p) = 1, \ \textit{(pois } 16 = 3 \cdot 5 + 1)$$
$$d = \rho(b, q) = 2, \ \textit{(pois } 16 = 7 \cdot 2 + 2).$$

Assim, o número a *procurado satisfaz o sistema*

$$\begin{cases} a \equiv (1)^{-1} \pmod 3 \\ a \equiv (2)^{-1} \pmod 7 \end{cases}.$$

Como o inverso de $2 \pmod 7$ *é* 4 *(pois* $2 \cdot 4 = 8 \equiv 1 \pmod 7$*), concluímos que* a *satisfaz o sistema*

$$\begin{cases} a \equiv 1 \pmod 3 \\ a \equiv 4 \pmod 7 \end{cases}.$$

A primeira equação tem como soluções $a = 1 + 3n$ *onde* $n \in \mathbb{Z}$*, o que, substituindo na segunda equação, fornece*

$$1 + 3n \equiv 4 \pmod 7,$$

ou ainda

$$3n \equiv 3 \pmod 7.$$

Para resolver esta ultima equação notamos que o inverso de $3 \pmod 7$ *é* 5 *(pois* $3 \cdot 5 = 15 \equiv 1 \pmod 7$*), logo:*

$$n \equiv 3 \cdot 5 = 15 \pmod 7.$$

Assim, pelo Teorema Chinês do Resto, concluímos que $a \equiv 1 + 3 \cdot 15 = 46 \pmod{21}$*. Como* $0 \leq a < 21$*, obtemos finalmente a resposta correcta:* $a = 4$*.*

Exercícios.

1. Uma palavra é codificada fazendo corresponder a cada letra do alfabeto português (23 letras) um número inteiro, de forma que $a \mapsto 1$, $b \mapsto 2$, $c \mapsto 3$,.... De seguida é transmitida num sistema de chave pública com $N = 35$ e $r = 5$. Sabendo que a mensagem transmitida é "$33, 10, 12, 24, 14$" determine a palavra original.

2. Demonstre a seguinte generalização do Teorema Chinês do Resto: Seja $d = \text{mdc}(m, n)$. O sistema
$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$
tem soluções se e só se $d|(a-b)$. Neste caso, se c é uma solução, então o sistema é equivalente a $x \equiv c \pmod{\text{mmc}(n, m)}$.

Capítulo 3

Outros Exemplos de Anéis

3.1 Os Anéis $\mathbb{Z}_m$

No Capítulo 2 vimos em pormenor o anel dos inteiros. O leitor também conhece certamente muitas das propriedades algébricas de corpos como $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Existem no entanto outros exemplos de anéis muito importantes que vamos estudar neste capítulo.

Começamos pelo estudo dos anéis associados à congruência $(\text{mod } m)$, os anéis Z_m. No Capítulo 1 já vimos brevemente os casos $\mathbb{Z}_2$ e $\mathbb{Z}_3$, sem qualquer referência à congruência $(\text{mod } m)$. Um estudo sistemático destes anéis exige no entanto a utilização desta congruência. Observamos que a congruência $(\text{mod } m)$ pode ser substituída por uma *igualdade* se "identificarmos" (*i.e.*, tratarmos como um único objecto) todos os inteiros congruentes entre si. O procedimento que seguimos é aplicável a qualquer relação de equivalência, e consiste em utilizar em lugar de um determinado objecto a *classe* de todos os objectos que lhe são equivalentes. Para isso, supomos fixado o módulo de congruência $m \in \mathbb{Z}$, e sendo x um inteiro arbitrário, introduzimos:

Definição 3.1.1. A CLASSE DE EQUIVALÊNCIA $(\text{mod } m)$ de x é o conjunto $\underline{x}$ dos inteiros congruentes com x $(\text{mod } m)$, ou seja,

$$\underline{x} = \{y \in \mathbb{Z} : x \equiv y \pmod{m}\}.$$

Exemplo 3.1.2.

Com o módulo de congruência $m = 3$, temos

$$\begin{aligned}
\underline{0} &= \{0, \pm 3, \pm 6, \dots\}, \\
\underline{1} &= \{1, 1 \pm 3, 1 \pm 6, \dots\}, \\
\underline{2} &= \{2, 2 \pm 3, 2 \pm 6, \dots\}.
\end{aligned}$$

É claro que o símbolo $\underline{x}$ é ambíguo porque não contém qualquer informação sobre o módulo de congruência m em causa. No entanto, é evidente

que

$$\underline{x} = \{x + ym : y \in \mathbb{Z}\},$$

ou ainda

$$\underline{x} = \{x + z : z \in \langle m \rangle\}.$$

Por este motivo, sempre que necessário escrevemos $x + \langle m \rangle$ em lugar de $\underline{x}$.

Exemplo 3.1.3.

Para $m = 4$ e $m = 5$ temos respectivamente

$$\begin{aligned} m = 4: &\quad \underline{3} = 3 + \langle 4 \rangle = \{\ldots, -5, -1, 3, 7, 11, \ldots\}, \\ m = 5: &\quad \underline{3} = 3 + \langle 5 \rangle = \{\ldots, -7, -2, 3, 8, 13, \ldots\}. \end{aligned}$$

Para substituir a congruência $x \equiv y \pmod{m}$ por uma igualdade, usamos o seguinte lema, que como consequência directa da Proposição 2.8.2 é na realidade aplicável a qualquer relação de equivalência.

Lema 3.1.4. *Para todo os inteiros x, y temos:*

$$x \equiv y \pmod{m} \iff \underline{x} = \underline{y} \iff \underline{x} \cap \underline{y} \neq \emptyset.$$

Demonstração. É evidente da transitividade da relação de congruência que, se $x \equiv y \pmod{m}$, então $\underline{x} \supseteq \underline{y}$. Por simetria, $x \equiv y \pmod{m} \Leftrightarrow y \equiv x \pmod{m}$, logo também $\underline{x} \subseteq \underline{y}$. Concluímos que, se $x \equiv y \pmod{m}$, então $\underline{x} = \underline{y}$.

Por reflexividade, sabemos também que $y \in \underline{y}$. Portanto, se $\underline{x} = \underline{y}$, então $\underline{x} \cap \underline{y} \neq \emptyset$.

Finalmente, se $\underline{x} \cap \underline{y} \neq \emptyset$, seja z um elemento de $\underline{x} \cap \underline{y}$, e note-se que, por definição de classe de equivalência, se tem $x \equiv z \pmod{m}$ e $y \equiv z \pmod{m}$, donde se segue por simetria e transitividade que $x \equiv y \pmod{m}$. □

De acordo com a propriedade reflexiva, qualquer inteiro x pertence à classe $\underline{x}$, e portanto a união de todas as classes de equivalência é o conjunto $\mathbb{Z}$. Por este motivo, dizemos que o conjunto de todas as classes de equivalência para um dado módulo m, que é o conjunto $\{\underline{x} : x \in \mathbb{Z}\}$, é uma *cobertura* de $\mathbb{Z}$. Além disso, de acordo com o lema anterior, as classes de equivalências distintas são necessariamente disjuntas. Dizemos por isso que o conjunto $\{\underline{x} : x \in \mathbb{Z}\}$ é uma *partição* de $\mathbb{Z}$. Recorde-se ainda que, como indicámos no Capítulo anterior, e quando $m \neq 0$, dizemos que $\underline{x}$ é uma textscclasse de restos.

Exemplos 3.1.5.

1. *Se $m = 2$, a partição referida é a habitual classificação dos inteiros em pares e ímpares.*

2. Se $m = 3$, a partição corresponde à classificação dos inteiros em termos do resto da sua divisão por 3:

$$\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\} \cup \{1, 1 \pm 3, 1 \pm 6, \dots\} \cup \{2 \pm 3, 2 \pm 6, \dots\}.$$

Note-se de passagem que a classe de equivalência $\underline{x}$ fica unicamente determinada por qualquer um dos inteiros que a constituem. Por este motivo, qualquer inteiro y em $\underline{x}$ diz-se um *representante* da classe $\underline{x}$, já que $\underline{y} = \underline{x}$.

Exemplo 3.1.6.

Se $m = 3$, os inteiros $1, 4, 7, -2$ e -5 são todos representantes de $\underline{1}$, e temos

$$\underline{1} = \underline{4} = \underline{7} = \underline{-2} = \underline{-5}.$$

Dada uma relação de equivalência "$\sim$" num conjunto X, o conjunto das respectivas classes de equivalência diz-se o QUOCIENTE de X por $\sim$ e designa-se em geral por $X/\sim$. A função $\pi : X \to X/\sim$ dada por $\pi(x) = \underline{x}$, que transforma cada elemento de X na sua classe de equivalência, é a APLICAÇÃO QUOCIENTE. No caso de $X = \mathbb{Z}$, e quando $\sim$ é a relação de equivalência módulo m, designamos o conjunto quociente $\mathbb{Z}/\sim$ por $\mathbb{Z}_m$, e a aplicação quociente por π_m, ou apenas π. Temos por isso $\pi_m(x) = x + \langle m \rangle = \underline{x}$. Mais formalmente,

Definição 3.1.7. Sendo $\underline{x} = \{y \in \mathbb{Z} : y \equiv x \pmod{m}\}$, então $\mathbb{Z}_m = \{\underline{x} : x \in \mathbb{Z}\}$, e $\pi_m : \mathbb{Z} \to \mathbb{Z}_m$ é dada por $\pi_m(x) = \underline{x}$.

Com esta nova notação, a Proposição 2.8.4 resume-se agora em contar o número de elementos de $\mathbb{Z}_m$:

Proposição 3.1.8. *Se $m > 0$, $\mathbb{Z}_m = \{\underline{0}, \underline{1}, \dots, \underline{m-1}\}$ tem m elementos.*

Observe-se ainda que, se $m = 0$, então $\underline{x} = \{x\}$, e portanto $\mathbb{Z}_0$ é um conjunto infinito. Na realidade, e com as operações algébricas que definiremos a seguir, $\mathbb{Z}_0$ e $\mathbb{Z}$ são *anéis isomorfos*.

Exemplo 3.1.9.

O conjunto $\mathbb{Z}_6$ tem precisamente 6 elementos, e podemos escrever

$$\mathbb{Z}_6 = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}\} = \{\underline{6}, \underline{7}, \underline{8}, \underline{9}, \underline{10}, \underline{11}\} = \{\underline{36}, \underline{-5}, \underline{2}, \underline{63}, \underline{610}, \underline{-19}\}, \text{ etc.}$$

Note-se mais uma vez a ambiguidade da notação que utilizamos: quando escrevemos $\mathbb{Z}_4 = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}\}$, os símbolos nesta lista designam objectos que não *são elementos de $\mathbb{Z}_6$. Por exemplo,*

$$2 + \langle 4 \rangle \neq 2 + \langle 6 \rangle \text{ i.e., } \pi_4(2) \neq \pi_6(2).$$

De acordo com a Proposição 2.8.6, sabemos que, quando $x \equiv x' \pmod{m}$ e $y \equiv y' \pmod{m}$, então $x + y \equiv x' + y' \pmod{m}$ e $xy \equiv x'y' \pmod{m}$. Em termos de classes de equivalência, temos

$$\underline{x} = \underline{x'} \text{ e } \underline{y} = \underline{y'} \Longrightarrow \underline{x+y} = \underline{x'+y'} \text{ e } \underline{xy} = \underline{x'y'}.$$

Por outras palavras, as classes $\underline{x+y}$ e $\underline{xy}$ não dependem dos representantes x e y, mas apenas das classes $\underline{x}$ e $\underline{y}$. Aproveitamos este facto para introduzir operações de soma e produto em $\mathbb{Z}_m$.

Definição 3.1.10. A SOMA e PRODUTO em $\mathbb{Z}_m$ são dados por

$$\underline{x} + \underline{y} = \underline{x+y}, \qquad \text{e} \qquad \underline{x} \cdot \underline{y} = \underline{xy}.$$

Como seria de esperar, uma parte das propriedades das operações algébricas em $\mathbb{Z}$ transferem-se automaticamente para as operações agora definidas. Por exemplo, observe-se que

$$\begin{aligned} \underline{x} + (\underline{y} + \underline{z}) &= \underline{x} + \underline{y+z}, \\ &= \underline{x + (y+z)}, \\ &= \underline{(x+y) + z}, \\ &= \underline{x+y} + \underline{z}, \\ &= (\underline{x} + \underline{y}) + \underline{z}, \end{aligned}$$

donde concluímos que a adição em $\mathbb{Z}_m$ é associativa. Deixamos como exercício a verificação do seguinte

Teorema 3.1.11. *$(\mathbb{Z}_m, +, \cdot)$ é um anel abeliano com identidade.*

Exemplo 3.1.12.

As "tabuadas" da soma e do produto em $\mathbb{Z}_4$ são:

$+$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{0}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{1}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{0}$
$\underline{2}$	$\underline{2}$	$\underline{3}$	$\underline{0}$	$\underline{1}$
$\underline{3}$	$\underline{3}$	$\underline{0}$	$\underline{1}$	$\underline{2}$

$\cdot$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{2}$	$\underline{0}$	$\underline{2}$	$\underline{0}$	$\underline{2}$
$\underline{3}$	$\underline{0}$	$\underline{3}$	$\underline{2}$	$\underline{1}$

É curioso observar algumas diferenças e semelhanças entre este anel e $\mathbb{Z}$:

- *A equação $x = -x$ tem* duas *soluções em $\mathbb{Z}_4$;*
- *Como $\underline{2} \cdot \underline{2} = \underline{0}$ é claro que $\underline{2}$ é um divisor de zero, e portanto $\mathbb{Z}_4$* não *é um domínio integral;*
- *Os múltiplos naturais da identidade $\underline{1}$ são trivialmente*

  $$1 \cdot \underline{1} = \underline{1},\ 2 \cdot \underline{1} = \underline{2},\ 3 \cdot \underline{1} = \underline{3},\ 4 \cdot \underline{1} = \underline{4} = \underline{0},\ \textit{etc.}$$

  e consequentemente este anel tem característica 4;

- *Os subanéis de $\mathbb{Z}_4$ são todos ideais principais (tal como ocorre no anel dos inteiros), e reduzem-se a*

$$\langle \underline{1} \rangle = \langle \underline{3} \rangle = \mathbb{Z}_4, \qquad \langle \underline{2} \rangle = \{\underline{0}, \underline{2}\}, \qquad e \qquad \langle \underline{0} \rangle = \langle \underline{4} \rangle = \{\underline{0}\}.$$

Note-se que estes ideais correspondem exactamente aos divisores de 4.

Regressamos agora ao caso geral do anel $\mathbb{Z}_m$, com $m > 0$, e começamos por identificar os elementos invertíveis de $\mathbb{Z}_m$, que formam o conjunto $\mathbb{Z}_m^*$, (na notação introduzida no Capítulo 1). Dado $a \in \mathbb{Z}$, é claro que $\underline{a}$ é invertível em $\mathbb{Z}_m$ se e só se a equação $\underline{a} \cdot \underline{x} = \underline{1}$ tem soluções em $\mathbb{Z}_m$. De acordo com os resultados da Secção 2.8, temos, ainda, que:

$$\begin{aligned} \underline{a} \in \mathbb{Z}_m^* &\iff \underline{a} \cdot \underline{x} = \underline{1} \text{ tem solução em } \mathbb{Z}_m, \\ &\iff ax \equiv 1 \pmod{m} \text{ tem solução em } \mathbb{Z}, \\ &\iff \mathrm{mdc}(a, m) = 1. \end{aligned}$$

Por palavras, os elementos invertíveis de $\mathbb{Z}_m$ correspondem aos naturais k, $1 \leq k \leq m$, que são primos relativamente a m. O número de elementos de $\mathbb{Z}_m^*$, designa-se por $\varphi(m)$, e à função $\varphi : \mathbb{N} \to \mathbb{N}$ assim definida chamamos FUNÇÃO DE EULER.

Exemplo 3.1.13.

Os elementos invertíveis no anel $\mathbb{Z}_9$ formam o conjunto

$$\mathbb{Z}_9^* = \{\underline{1}, \underline{2}, \underline{4}, \underline{5}, \underline{7}, \underline{8}\},$$

portanto, $\varphi(9) = 6$.

Veremos adiante como calcular a função de Euler, conhecidos os factores primos do seu argumento. Para já, observamos que, se p é um número primo, então $\varphi(p) = p - 1$, e todos os elementos não-nulos de $\mathbb{Z}_p$ são invertíveis. Dito doutra forma:

Teorema 3.1.14. *Se p é primo, então $\mathbb{Z}_p$ é um corpo finito com p elementos.*

A característica dos anéis $\mathbb{Z}_m$ é muito fácil de calcular. Já observámos que $\mathbb{Z}_4$ tem característica 4. Na realidade, é fácil mostrar que

Teorema 3.1.15. *O anel $\mathbb{Z}_m$ tem característica m.*

Demonstração. De facto, por indução, vemos que

$$\forall n \in \mathbb{N}, a \in \mathbb{Z} \ : \ n\underline{a} = \underline{n} \cdot \underline{a} = \underline{na}. \tag{3.1.1}$$

No caso específico de $\underline{a} = \underline{1}$, temos

$$n\underline{1} = \underline{0} \quad \iff \quad \underline{n} = \underline{0} \quad \iff \quad n \in \langle m \rangle,$$

donde o resultado se segue. □

Identificámos acima todos os subanéis e ideais de $\mathbb{Z}_4$, e notámos que neste anel (tal como no anel dos inteiros) os respectivos subanéis são na realidade ideais principais. Antes de provar esta afirmação para qualquer valor de m, examinemos em pormenor os ideais gerados por cada um dos elementos de $\mathbb{Z}_m$. A proposição seguinte é óbvia da comutatividade da multiplicação de $\mathbb{Z}_m$, e de (3.1.1).

Proposição 3.1.16. *Se $a \in \mathbb{Z}$, então $\langle \underline{a} \rangle = \{\underline{a} \cdot \underline{n} : \underline{n} \in \mathbb{Z}_m\} = \{n\underline{a} : n \in \mathbb{Z}\}$.*

Assim, é fácil listar os elementos de um ideal de $\mathbb{Z}_m$, uma vez dado um gerador.

Exemplos 3.1.17.

1. *Em $\mathbb{Z}_{40}$ temos:*

$$\langle \underline{15} \rangle = \{\underline{15}, \underline{30}, \underline{45} = \underline{5}, \underline{20}, \underline{35}, \underline{50} = \underline{10}, \underline{25}, \underline{40} = \underline{0}\}.$$

2. *Em $\mathbb{Z}_{21}$ temos:*

$$\langle \underline{15} \rangle = \{\underline{15}, \underline{30} = \underline{9}, \underline{24} = \underline{3}, \underline{18}, \underline{33} = \underline{12}, \underline{27} = \underline{6}, \underline{21} = \underline{0}\}.$$

Um momento de reflexão mostra que os elementos do ideal $\langle \underline{a} \rangle$ correspondem aos inteiros b para os quais a equação $ax \equiv b \pmod{m}$ tem soluções. Estes inteiros são, como sabemos, os múltiplos de $d = \text{mdc}(a, m)$. É agora possível exprimir este resultado na seguinte forma:

Proposição 3.1.18. *Se $d = \text{mdc}(a, m)$, então temos que $\langle \underline{a} \rangle = \langle \underline{d} \rangle$ em $\mathbb{Z}_m$.*

Demonstração. Como $d = ax + my$, temos $\underline{d} = \underline{ax}$, donde $\underline{d} \in \langle \underline{a} \rangle$ e $\langle \underline{a} \rangle \supset \langle \underline{d} \rangle$. Como $a = dz$, temos $\underline{a} = \underline{dz}$, donde $\underline{a} \in \langle \underline{d} \rangle$, e $\langle \underline{d} \rangle \supset \langle \underline{a} \rangle$. □

Observe-se que o resultado anterior torna simples a contagem dos elementos de $\langle \underline{a} \rangle$. Na verdade, se $d = \text{mdc}(a, m)$, então $m = dk$, e $\langle \underline{a} \rangle = \langle \underline{d} \rangle$ tem k elementos[1].

Exemplos 3.1.19.

1. *Em $\mathbb{Z}_{40}$ temos:*

$$\langle \underline{15} \rangle = \langle \underline{5} \rangle = \{\underline{5}, \underline{10}, \underline{15}, \underline{20}, \underline{25}, \underline{30}, \underline{35}, \underline{0}\},$$

com $\frac{40}{5} = 8$ elementos.

2. *Em $\mathbb{Z}_{21}$ temos*

$$\langle \underline{15} \rangle = \langle \underline{3} \rangle = \{\underline{3}, \underline{6}, \underline{9}, \underline{12}, \underline{15}, \underline{18}, \underline{0}\},$$

com $\frac{21}{3} = 7$ elementos.

[1] Vemos aqui directamente que o número de elementos do ideal $\langle \underline{a} \rangle$ é um factor do número de elementos do anel Z_m. Veremos no próximo capítulo que este facto não passa de um caso particular do chamado Teorema de Lagrange.

Todos os subanéis do anel $\mathbb{Z}_4$ são ideais principais, tal como todos os subanéis do anel dos inteiros. Verificamos agora que esta é uma propriedade comum a todos os anéis $\mathbb{Z}_m$. Com este objectivo, começamos por estabelecer uma relação directa entre os subanéis de $\mathbb{Z}_m$ e os subanéis do anel dos inteiros. Esta relação envolve a aplicação quociente $\pi : \mathbb{Z} \to \mathbb{Z}_m$, dada como sabemos por $\pi(x) = \underline{x}$, e é ilustrada na figura seguinte.

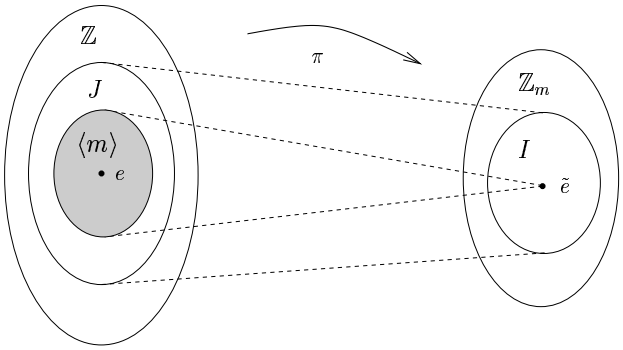


Figura 3.1.1: Subanéis de $\mathbb{Z}$ e de $\mathbb{Z}_m$.

Proposição 3.1.20. *Se I é um subconjunto de $\mathbb{Z}_m$, e $J = \{a \in \mathbb{Z} : \underline{a} \in I\} = \pi^{-1}(I)$, então I é um subanel de $\mathbb{Z}_m$ se e só se J é um subanel de $\mathbb{Z}$ que contém $\langle m \rangle$.*

Demonstração. Provamos apenas que, se I é um subanel, então J é também um subanel.

Obviamente, se $a, b \in J$, então $\underline{a}, \underline{b} \in I$. Logo, vemos que

$$\underline{a} - \underline{b} = \underline{a - b} \in I \Longrightarrow a - b \in J,$$
$$\underline{a} \cdot \underline{b} = \underline{ab} \in I \Longrightarrow ab \in J.$$

□

O seguinte corolário é imediato.

Corolário 3.1.21. *Se I é um subconjunto de $\mathbb{Z}_m$, as seguintes afirmações são equivalentes:*

(i) I é um subanel de $\mathbb{Z}_m$;

(ii) I é um ideal de $\mathbb{Z}_m$;

(iii) existe $d \in \mathbb{Z}$ tal que $d|m$ e $I = \langle \underline{d} \rangle$.

Demonstração. Deve ser óbvio que (iii)⇒(ii)⇒(i). O corolário fica portanto provado se estabelecermos que (i)⇒(iii), o que deixamos para os exercícios. □

Segue-se deste corolário que $\mathbb{Z}_m$ tem precisamente um subanel (que é necessariamente um ideal principal) por cada um dos divisores de m. Isto mesmo se ilustra na figura seguinte, para $m = 40$. Aproveitamos ainda este exemplo para ilustrar a utilização da Proposição 3.1.18 no cálculo de todos os geradores de cada um destes ideais.

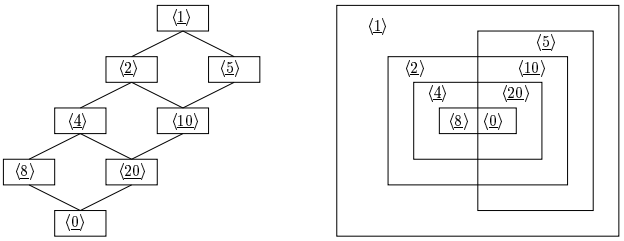


Figura 3.1.2: Os ideais de $\mathbb{Z}_{40}$.

Exemplo 3.1.22.

Os geradores de $\langle \underline{1} \rangle = \mathbb{Z}_{40}$ *correspondem às soluções de* $\mathrm{mdc}(x, 40) = 1$*:*

$$\langle \underline{1} \rangle = \langle \underline{3} \rangle = \langle \underline{7} \rangle = \langle \underline{9} \rangle = \langle \underline{11} \rangle = \langle \underline{13} \rangle = \langle \underline{17} \rangle = \langle \underline{19} \rangle = \\ \langle \underline{21} \rangle = \langle \underline{23} \rangle = \langle \underline{27} \rangle = \langle \underline{29} \rangle = \langle \underline{31} \rangle = \langle \underline{33} \rangle = \langle \underline{37} \rangle = \langle \underline{39} \rangle.$$

Os geradores de $\langle \underline{2} \rangle$ *correspondem às soluções de* $\mathrm{mdc}(x, 40) = 2$*:*

$$\langle \underline{2} \rangle = \langle \underline{6} \rangle = \langle \underline{14} \rangle = \langle \underline{18} \rangle = \langle \underline{22} \rangle = \langle \underline{26} \rangle = \langle \underline{34} \rangle = \langle \underline{38} \rangle.$$

Os geradores de $\langle \underline{4} \rangle$ *correspondem às soluções de* $\mathrm{mdc}(x, 40) = 4$*:*

$$\langle \underline{4} \rangle = \langle \underline{12} \rangle = \langle \underline{28} \rangle = \langle \underline{36} \rangle.$$

Os geradores de $\langle \underline{8} \rangle$ *correspondem às soluções de* $\mathrm{mdc}(x, 40) = 8$*:*

$$\langle \underline{8} \rangle = \langle \underline{16} \rangle = \langle \underline{24} \rangle = \langle \underline{32} \rangle.$$

Os geradores de $\langle \underline{5} \rangle$ *correspondem às soluções de* $\mathrm{mdc}(x, 40) = 5$*:*

$$\langle \underline{5} \rangle = \langle \underline{15} \rangle = \langle \underline{25} \rangle = \langle \underline{35} \rangle.$$

Os geradores de $\langle \underline{10} \rangle$ *correspondem às soluções de* $\mathrm{mdc}(x, 40) = 10$*:*

$$\langle \underline{10} \rangle = \langle \underline{30} \rangle.$$

Os ideais $\langle \underline{20} \rangle$ *e* $\langle \underline{0} \rangle$ *têm naturalmente um único gerador.*

Suponha-se que $n|m$, e B é o subanel de $\mathbb{Z}_m$ com n elementos. É muito interessante estudar desde já as seguintes questões:

- O *grupo aditivo* B é sempre isomorfo ao *grupo* $\mathbb{Z}_n$?

- O *anel* B é sempre isomorfo ao *anel* $\mathbb{Z}_n$?

A primeira destas questões é muito fácil de esclarecer:

Proposição 3.1.23. *Se $n|m$ e B é o subanel de $\mathbb{Z}_m$ com n elementos, então os* grupos aditivos *B e $\mathbb{Z}_n$ são isomorfos.*

Demonstração. Seja $m = dn$, donde $B = \langle \underline{d} \rangle$. Definimos $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ por $\phi(\underline{x}) = \underline{dx}$, onde bem entendido $\underline{x} \in \mathbb{Z}_n$, e $\underline{dx} \in \mathbb{Z}_m$.[2]

É fundamental mostrar aqui que a função ϕ está *bem definida*, *i.e.*, provar que o lado direito da igualdade $\phi(\underline{x}) = \underline{dx}$ *não depende* da escolha do inteiro x que representa a classe $\underline{x}$ no lado esquerdo. Para isso, basta verificar que

$$\underline{x} = \underline{x'} \text{ em } \mathbb{Z}_n \iff n|(x - x') \implies m = dn|(dx - dx') \implies \underline{dx} = \underline{dx'} \text{ em } \mathbb{Z}_m.$$

É imediato que ϕ é um homomorfismo *de grupos*, e também que

$$\phi(\mathbb{Z}_n) = \{\underline{dx} : x \in \mathbb{Z}\} = \langle \underline{d} \rangle = B.$$

Resta-nos provar que ϕ é um *isomorfismo* entre $\mathbb{Z}_n$ e B, ou seja, que ϕ é injectivo, o que se reduz a calcular o respectivo núcleo:

$$\phi(\underline{x}) = \underline{0} \iff \underline{dx} = \underline{0} \text{ (em } \mathbb{Z}_m) \iff dn = m|dx \iff n|x \iff \underline{x} = \underline{0} \text{ (em } \mathbb{Z}_n).$$

Como o núcleo de ϕ é trivial, ϕ é um isomorfismo entre B e $\mathbb{Z}_n$. □

Veremos mais adiante que este resultado não passa de uma propriedade geral dos chamados *grupos cíclicos*. A questão relativa aos isomorfismos de anel não é tão simples, e podemos ilustrar a complexidade adicional com alguns exemplos.

Exemplos 3.1.24.

1. *Considere-se, em $\mathbb{Z}_4$, o subanel $B = \langle \underline{2} \rangle = \{\underline{2}, \underline{0}\}$. Como acabámos de ver, $(B, +) \simeq (\mathbb{Z}_2, +)$. No entanto, os* anéis *B e $\mathbb{Z}_2$ não são certamente isomorfos, porque o produto em B é* sempre *nulo, ou seja, $x, y \in B \Rightarrow xy = 0$.*

2. *Considere-se, em $\mathbb{Z}_6$, os subanéis $B = \langle \underline{2} \rangle = \{\underline{2}, \underline{4}, \underline{0}\}$, e $C = \langle \underline{3} \rangle = \{\underline{3}, \underline{0}\}$. Mais uma vez, temos $(B, +) \simeq (\mathbb{Z}_3, +)$ e $(C, +) \simeq (\mathbb{Z}_2, +)$, mas neste caso os anéis em causa são igualmente isomorfos, apesar de este facto não ser óbvio.*

As observações feitas nos exemplos acima podem ser esclarecidas pelo resultado seguinte, cuja demonstração fica como exercício.

Proposição 3.1.25. *Se $n|m$ e B é o subanel de $\mathbb{Z}_m$ com n elementos, então as seguintes afirmações são equivalentes:*

[2] Podíamos igualmente escrever, para mais clareza, $\phi(\pi_n(x)) = \pi_m(dx)$.

(i) Os anéis B e $\mathbb{Z}_n$ são isomorfos,

(ii) O anel B é unitário,

(iii) $m = nd$, onde $\mathrm{mdc}(n, d) = 1$.

Neste caso, a identidade de B é o único $\underline{x} \in \mathbb{Z}_m$ tal que

$$x \equiv 0 \pmod{d}, \text{ e } x \equiv 1 \pmod{n}.$$

Exemplos 3.1.26.

1. *O anel $\mathbb{Z}_{36}$ tem 9 subanéis, porque 36 tem 9 divisores naturais. Exceptuando os subanéis* triviais $\langle \underline{0} \rangle = \{\underline{0}\}$ *e* $\langle \underline{1} \rangle = \mathbb{Z}_{36}$*, apenas os subanéis $B = \langle \underline{4} \rangle$, com 9 elementos, e $C = \langle \underline{9} \rangle$, com 4 elementos, têm identidade.*

2. *Continuando o exemplo anterior, a solução do sistema $x \equiv 0 \pmod 4$ e $x \equiv 1 \pmod 9$ é $x \equiv 28 \pmod{36}$, e portanto a identidade de B é $\underline{x} = \underline{28}$. Analogamente, a solução de $x \equiv 0 \pmod 9$ e $x \equiv 1 \pmod 4$ é $x \equiv 9 \pmod{36}$, e portanto a identidade de C é $\underline{x} = \underline{9}$.*

Exercícios.

1. Prove o Teorema 3.1.11.

2. Verifique directamente que os únicos subanéis de $\mathbb{Z}_4$ são $\langle \underline{1} \rangle$, $\langle \underline{2} \rangle$ e $\langle \underline{0} \rangle$.

3. Prove que, se $m > 1$, então $\mathbb{Z}_m$ ou é um corpo ou tem divisores de zero.

4. Prove que $n\underline{a} = \underline{na}$ (em particular, $\underline{n} = n\underline{1}$).

5. Mostre que, se $n > 1$, então $M_n(\mathbb{Z}_m)$ é um anel não-abeliano, com característica m, e m^{n^2} elementos.

6. Considere o anel das funções $f : \mathbb{Z} \to \mathbb{Z}_m$ e mostre que para qualquer $m > 1$ existem anéis infinitos com característica m.

7. Prove que $A \in M_n(\mathbb{Z}_m)$ é invertível se e só se $\det(A) \in \mathbb{Z}_m^*$ [3].

8. Dê um exemplo de um espaço vectorial finito sobre um corpo finito (compare $\mathbb{R}^n$ com $\mathbb{Z}_p^n$).

9. Determine todas as matrizes em $GL(2, \mathbb{Z}_2)$ (matrizes 2×2 com entradas em $\mathbb{Z}_2$, invertíveis).

[3] O determinante de uma matriz $A = (a_{ij})$ de dimensão $n \times n$ com entradas num anel comutativo define-se da forma usual:

$$\det A = \sum_{\pi \in S_n} \mathrm{sgn}(\pi) a_{1\pi(1)} \cdots a_{n\pi(n)}.$$

10. Qual é o cardinal de $GL(n, \mathbb{Z}_p)$, se p é primo? (SUGESTÃO: Note que as linhas da matriz $M \in GL(n, \mathbb{Z}_p)$, que são vectores de $\mathbb{Z}_p^n$, devem ser *linearmente independentes*.)

11. Calcule a inversa da matriz

$$\begin{pmatrix} \underline{1} & \underline{0} & \underline{0} \\ \underline{2} & \underline{3} & \underline{4} \\ \underline{3} & \underline{2} & \underline{4} \end{pmatrix} \in GL(3, \mathbb{Z}_5).$$

12. Resolva o sistema

$$\begin{cases} x + 2y &= \underline{a} \\ -3x + 3y &= \underline{b} \end{cases}$$

em $\mathbb{Z}_5$.

13. Prove que $\langle \underline{a} \rangle = \mathbb{Z}_m$ se e só se $\underline{a} \in \mathbb{Z}_m^*$.

14. Conclua as demonstrações da Proposição 3.1.20 e do Corolário 3.1.21.

15. Quais são os elementos e os geradores de $\langle \underline{85} \rangle$ em $\mathbb{Z}_{204}$?

16. Quantos elementos tem o ideal $\langle \underline{28}, \underline{52} \rangle$ em $\mathbb{Z}_{204}$?

17. Determine todos os ideais de $\mathbb{Z}_{30}$. Quais destes ideais são anéis unitários, e quais são as respectivas identidades?

18. Sendo p um número primo, e $n \in \mathbb{N}$, mostre que $\varphi(p^n) = p^n - p^{n-1}$. SUGESTÃO: Mostre que $\underline{x} \in \mathbb{Z}_{p^n}^* \iff \underline{x} \notin \langle \underline{p} \rangle$.

19. Calcule $\varphi(3000)$. SUGESTÃO: Mostre que

$$\underline{x} \in \mathbb{Z}_{3000}^* \iff \underline{x} \notin (\langle \underline{2} \rangle \cup \langle \underline{3} \rangle \cup \langle \underline{5} \rangle).$$

20. Suponha que $d = \text{mdc}(a, m)$, $m = dn$, e $\phi : \mathbb{Z}_m \to \mathbb{Z}_m$ é dada por $\phi(\underline{x}) = \underline{ax}$.

    (a) Mostre que ϕ é um homomorfismo de grupos.

    (b) Prove que o núcleo de ϕ é $\langle \underline{n} \rangle$, e $\phi(\mathbb{Z}_m)$ tem n elementos.

    (c) Supondo $m = 12$, quais são os valores de $\underline{a}$ para os quais ϕ é um automorfismo de grupos?

    (d) Supondo $m = 12$, quais são os valores de $\underline{a}$ para os quais ϕ é um homomorfismo de anéis?

21. Supondo $n|m$, prove que a função $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$ dada por $\phi(\underline{x}) = \underline{x}$, *i.e.*, $\phi(\pi_m(x)) = \pi_n(x)$, com $x \in \mathbb{Z}$, está bem definida, e é um homomorfismo de anéis. Qual é o respectivo núcleo?

22. Para provar a proposição 3.1.25, proceda como se segue:

    (a) Demonstre a implicação "(i) $\implies$ (ii)".

(b) Para provar que "(ii) $\Longrightarrow$ (iii)", mostre primeiro que se $\underline{a}$ é a identidade de B então $\langle \underline{a} \rangle = \langle \underline{d} \rangle$, e $\underline{a}^2 = \underline{a}$. Conclua que $a \equiv 0 \pmod{d}$, e $a \equiv 1 \pmod{n}$.

(c) Resolva o sistema $a \equiv 0 \pmod{d}$, e $a \equiv 1 \pmod{n}$, e considere a função $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ dada por $\phi(\underline{x}) = \underline{ax}$. Prove que ϕ está bem definida, é um homomorfismo injectivo de anéis, e $\phi(\mathbb{Z}_n) = B$, o que termina a demonstração.

23. Esta questão refere-se a homomorfismos $\phi : \mathbb{Z}_4 \to \mathbb{Z}_{36}$.

(a) Quais são os homomorfismos *de grupo* ϕ? Quais destes são injectivos?

(b) Quais são os homomorfismos *de anel* ϕ? Quais destes são injectivos?

24. Suponha que $\underline{a} \in \mathbb{Z}_m^*$, e considere $\Psi : \mathbb{Z}_m^* \to \mathbb{Z}_m$ dada por $\Psi(\underline{x}) = \underline{a} \cdot \underline{x}$.

(a) Prove que Ψ é injectiva, e que de facto $\Psi(\underline{x}) \in \mathbb{Z}_m^*$, para qualquer $\underline{x} \in \mathbb{Z}_m^*$.

(b) Sendo $\mathbb{Z}_m^* = \{x_1, x_2, x_3, \ldots, x_k\}$, onde $k = \phi(m)$ e ϕ é a função de Euler, mostre que $\prod_{i=1}^{k} \Psi(x_i) = \prod_{i=1}^{k} x_i$, e utilize este facto para provar o Teorema de Euler : $\underline{a}^k = \underline{1}$.

(c) Prove ainda o Teorema de Fermat : Se $m = p$ é primo, então $\underline{a}^p = \underline{a}$.

3.2 Fracções e Números Racionais

Esta secção tem como principais objectivos definir o corpo dos números racionais e mostrar que as suas propriedades (normalmente introduzidas por via axiomática) são consequência lógica dos axiomas para os inteiros que indicámos no Capítulo 2. Veremos simultaneamente que o processo de definição dos números racionais a partir dos números inteiros é efectivamente aplicável a qualquer anel abeliano onde a lei do corte seja válida, o que nos permitirá mais adiante introduzir outros corpos de importância prática.

Os números racionais (fracções, razões, etc.) são normalmente e informalmente introduzidos como as "*expressões do tipo* $\frac{m}{n}$", em que m e n são inteiros, e $n \neq 0$. De um ponto de vista mais formal, observamos que o par ordenado de inteiros (m, n) determina um número racional, desde que $n \neq 0$. Por outro lado, todos sabemos que pares ordenados distintos podem corresponder ao mesmo número racional, ou seja, podemos ter $(m, n) \neq (m', n')$ e $\frac{m}{n} = \frac{m'}{n'}$, o que ocorre exactamente quando $mn' = m'n$. Estas observações sugerem a definição dos números racionais não como *pares ordenados de inteiros* mas sim como *classes de equivalência de pares ordenados de inteiros*. Como veremos, o êxito desta ideia não assenta em propriedades específicas dos inteiros, mas apenas no facto de $\mathbb{Z}$ ser um anel abeliano com mais de um elemento, onde a lei do corte para o produto é válida. Por este motivo, formularemos alguns dos nossos resultados num contexto mais abstracto.

No que se segue, $A \neq \{0\}$ designa um qualquer anel abeliano onde a lei do corte para o produto é válida (*i.e.*, sem divisores de zero).

Definição 3.2.1. Seja $B = \{(a, b) : a, b \in A, \text{ e } b \neq 0\}$. Designa-se por "$\simeq$" a relação binária em B definida por

$$(a, b) \simeq (a', b') \iff ab' = a'b.$$

A relação definida acima é sugerida pela igualdade de fracções que referimos. Naturalmente, só pode ser útil se corresponder a uma relação de equivalência, o que verificamos a seguir.

Lema 3.2.2. *A relação $\simeq$ é uma relação de equivalência.*

Demonstração. É evidente que a relação "$\simeq$" é reflexiva e simétrica. Para verificar a sua transitividade, suponha-se que $(a, b) \simeq (a', b')$, e $(a', b') \simeq (a'', b'')$. Usando a comutatividade e associatividade do produto, temos:

$$\begin{aligned} (a', b') \simeq (a'', b'') &\iff a'b'' = a''b' \implies a'bb'' = a''bb', \\ (a, b) \simeq (a', b') &\iff ab' = a'b \implies a'bb'' = ab''b'. \end{aligned}$$

Concluímos que $a''bb' = ab''b'$, donde $a''b = ab''$, e $(a, b) \simeq (a'', b'')$, usando naturalmente o facto de $b' \neq 0$, e A não ter divisores de 0. □

Como sabemos, uma relação de equivalência "$\simeq$" em B determina sempre uma partição de B em classes de equivalência. Se $(a, b) \in B$, diremos que a respectiva classe de equivalência $\underline{(a, b)}$ é uma FRACÇÃO DE A, que designaremos por "a/b", ou por "$\frac{a}{b}$". Por outras palavras, temos a seguinte definição:

Definição 3.2.3. Seja $A \neq \{0\}$ um anel abeliano onde a lei do corte é válida.

(i) Se $a, b \in A$ e $b \neq 0$, a FRACÇÃO $\frac{a}{b}$ é dada por

$$\frac{a}{b} = \{(a', b') \in A \times A : b' \neq 0 \text{ e } ab' = a'b\};$$

(ii) Designamos o conjunto de todas as fracções $\frac{a}{b}$ por $\mathrm{Frac}(A)$;

(iii) No caso em que $A = \mathbb{Z}$, a fracção $\frac{a}{b}$ diz-se um número *racional*, e o conjunto $\mathrm{Frac}(\mathbb{Z})$ designa-se por $\mathbb{Q}$.

No caso $A = \mathbb{Z}$, o conjunto dos números racionais $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ é de facto um anel. No caso geral, dotamos o conjunto das fracções de A com operações algébricas de soma e produto por simples cópia das operações usuais com números racionais, que são dadas, como sabemos, por

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \tag{3.2.1}$$

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}. \tag{3.2.2}$$

Para formalizar esta definição, que representa operações sobre classes de equivalência, resta-nos provar que o resultado de cada operação é independente do representante escolhido para cada classe. Deixamos a verificação deste facto, que enunciamos no próximo lema, como exercício.

Lema 3.2.4. *Se* $(a,b) \simeq (a',b')$*, e* $(c,d) \simeq (c',d')$*, então*

$$(ad+bc, bd) \simeq (a'd' + b'c', b'd'),$$
$$(ac, bd) \simeq (a'c', b'd').$$

De acordo com este lema, as Definições (3.2.1) e (3.2.2) não acarretam qualquer ambiguidade.

É óbvio que a soma e produto definidos acima são comutativos, e que o produto é associativo. Com um pouco mais de trabalho podemos também verificar que a soma é associativa e que o produto é distributivo em relação à soma. A existência de identidades para as duas operações não oferece igualmente quaisquer dificuldades. Na realidade, e exactamente como sabemos acontecer nos racionais, temos:

Teorema 3.2.5. *O conjunto* $\mathrm{Frac}(A)$ *com as operações algébricas definidas por (3.2.1) e (3.2.2) é um corpo, dito* CORPO DAS FRACÇÕES *de* A*.*

Demonstração. Seja $b \neq 0$ um *qualquer* elemento não-nulo de A, e defina-se $0' = \frac{0}{b}$, e $1' = \frac{b}{b}$. Então deixamos como exercício verificar que

$$0' = \{(0,c) : c \neq 0\} \text{ e}$$
$$1' = \{(c,c) : c \neq 0\}$$

são respectivamente identidades para a soma e produto em $\mathrm{Frac}(A)$. Note-se que os elementos $0'$ e $1'$ são efectivamente independentes da escolha de $b \neq 0$ em A. Em particular, e supondo $y \neq 0$, temos:

$$\frac{x}{y} = 0' \iff x = 0, \text{ e}$$
$$\frac{x}{y} = 1' \iff x = y.$$

Note-se, ainda, que a existência de uma identidade para o produto de fracções não depende da existência de uma identidade para o produto no anel original A, e observe-se finalmente que

$$\frac{a}{b} + \frac{(-a)}{b} = 0',$$

e que, se $\frac{a}{b} \neq 0'$, então $a \neq 0$ (donde $\frac{b}{a}$ é uma fracção) e

$$\frac{a}{b}\frac{b}{a} = 1'.$$

□

Quando $A = \mathbb{Z}$ é o anel dos inteiros, e $\mathrm{Frac}(A) = \mathbb{Q}$, estamos habituados a considerar $\mathbb{Z}$ como um subconjunto de $\mathbb{Q}$. É interessante observar que esta "identificação" é sempre possível para um anel arbitrário, ou seja, o corpo das fracções do anel A contém sempre um subanel isomorfo ao anel A.

Proposição 3.2.6. *Seja $a \neq 0$ um elemento fixo do anel A. Então:*

(i) a função $\iota : A \to \mathrm{Frac}(A)$ dada por $\iota(x) = \frac{ax}{a}$ é um isomorfismo entre os anéis A e $\iota(A)$;

(ii) o isomorfismo ι é independente da escolha de $a \in A - \{0\}$.

Demonstração. As identidades $\iota(x+y) = \iota(x) + \iota(y)$ e $\iota(xy) = \iota(x)\iota(y)$ são de verificação imediata. Portanto ι é um homomorfismo de anéis, e $\iota(A)$ é um subanel de $\mathrm{Frac}(A)$. Além disso,

$$\begin{aligned} \iota(x) = 0' &\iff \frac{ax}{a} = 0' \\ &\iff ax = 0 \\ &\iff x = 0, \end{aligned}$$

e consequentemente ι é um isomorfismo entre os anéis A e $\iota(A)$.

Por outro lado, se $a, a' \neq 0$ e $x \in A$, então $\frac{ax}{a} = \frac{a'x}{a'}$, (porque $(ax)a' = (a'x)a$, donde a função ι é independente da escolha de $a \in A - \{0\}$. □

De acordo com este resultado, os elementos de $\mathrm{Frac}(A)$ da forma $\frac{ax}{a}$, com $a, x \in A$ e $a \neq 0$ fixo, são "cópias" dos elementos $x \in A$. Por esse motivo, quando trabalhamos com elementos do corpo $\mathrm{Frac}(A)$, designamos a fracção $\frac{ax}{a}$ por "x", e dizemos que se trata de um elemento do anel A. Escrevemos também $\mathrm{Frac}(A) \supset A$, ou seja, consideramos $\mathrm{Frac}(A)$ como uma extensão do anel A. Cometemos evidentemente um abuso de linguagem, mas fazemo-lo para evitar sobrecarregar a notação que utilizamos. Usamos naturalmente o mesmo símbolo para designar os zeros de A e $\mathrm{Frac}(A)$, e procedemos analogamente com as suas identidades para o produto, sempre que essa identidade exista em A.

O mesmo tipo de dificuldade surge quando consideramos "fracções de fracções". Sabemos perfeitamente, do nosso estudo dos racionais, que a fracção $\frac{\frac{a}{b}}{\frac{c}{d}}$ *é a fracção* $\frac{ad}{bc}$, mas é evidente que de acordo com a definição formal de fracção que indicámos acima tal igualdade não pode ser literalmente verdadeira (note-se que $\frac{ad}{bc}$ é um elemento de $\mathbb{Q}$, enquanto que a fracção composta original é uma fracção de $\mathbb{Q}$, ou seja, um elemento de $\mathrm{Frac}(\mathbb{Q})$). O sentido em que a igualdade deve ser entendida é o seguinte:

Proposição 3.2.7. *Se K é um corpo, a função $\iota : K \to \mathrm{Frac}(K)$ definida na Proposição 3.2.6 é sobrejectiva, e é portanto um isomorfismo de anéis.*

Demonstração. A demonstração resume-se a observar que $\frac{x}{y} = \iota(xy^{-1})$, o que de acordo com as convenções mencionadas acima se escreve normalmente na forma "$\frac{x}{y} = xy^{-1}$". □

No caso da fracção composta acima ($x = \frac{a}{b}$ e $y = \frac{c}{d}$), temos, estritamente falando, que

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \iota\left(\frac{a}{b}\left(\frac{c}{d}\right)^{-1}\right) = \iota\left(\frac{a}{b}\frac{d}{c}\right) = \iota\left(\frac{ad}{bc}\right).$$

Usando a identificação de x com $\iota(x)$, temos, então, que $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}$.

Vimos na secção anterior que a existência dos corpos finitos $\mathbb{Z}_p$ se segue dos axiomas para os inteiros que indicámos, e acabámos de ver que a existência do corpo $\mathbb{Q}$ é outra das consequências desses axiomas. Mais adiante mostraremos que estes corpos são em certo sentido os *menores* corpos que existem. Por outras palavras, provaremos que qualquer corpo contém necessariamente um subcorpo isomorfo a um $\mathbb{Z}_p$ ou isomorfo a $\mathbb{Q}$.

Exercícios.

1. Demonstre o Lema 3.2.4.

2. Complete a demonstração do Teorema 3.2.5

3. Qual é o corpo das fracções do anel dos inteiros de Gauss?

4. Se Frac(A) é isomorfo a Frac(B), é sempre verdade que A é isomorfo a B? E se A é isomorfo a B, Frac(A) é sempre isomorfo a Frac(B)?

5. Mostre que, se o corpo K é uma extensão do anel A, então K contém um subcorpo isomorfo a Frac(A) (este resultado, que é uma generalização da Proposição 3.2.6, mostra que Frac(A) é o menor corpo que contém A). (SUGESTÃO: Se K é um corpo, a intersecção de todos os subcorpos de K é o menor subcorpo de K.)

6. Prove que, se A é numerável, então Frac(A) é numerável.

7. Suponha que A é um domínio integral, e mostre que as características de Frac(A) e A são iguais.

8. Prove que $\mathbb{Q}$ só pode ser ordenado da forma usual: $\frac{m}{n} > 0 \Leftrightarrow mn > 0$. (SUGESTÃO: Em qualquer corpo ordenado tem-se sempre $x > 0 \Leftrightarrow x^{-1} > 0$.)

9. Prove que, se A é um anel ordenado, então Frac(A) é ordenado.

3.3 Polinómios e Séries de Potências

Os polinómios com coeficientes reais são muitas vezes definidos como as *funções* $p : \mathbb{R} \to \mathbb{R}$ da forma

$$p(x) = \sum_{n=1}^{N} p_n x^n,$$

onde os números reais p_n são os coeficientes do polinómio p. Não podemos definir de modo análogo os polinómios com coeficientes num anel arbitrário A, se desejarmos que polinómios com coeficientes distintos sejam necessariamente polinómios distintos. Na realidade, desde que A tenha mais de um elemento, existe uma infinidade de possibilidades distintas para os coeficientes de um possível polinómio. No entanto, se A é finito, existe apenas um número *finito* de funções $f : A \to A$, que seguramente não podem ser usadas para definir *todos* os polinómios com coeficientes em A.

Exemplo 3.3.1.

O suporte do anel $\mathbb{Z}_2$ é o conjunto $\{\underline{0}, \underline{1}\}$, com dois elementos. O conjunto das funções $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ tem portanto 4 elementos. Por outro lado, se polinómios com coeficientes distintos são polinómios distintos, existe um número infinito de polinómios com coeficientes em $\mathbb{Z}_2$.

Resolvemos este problema identificando um polinómio com a sucessão dos seus próprios coeficientes, deixando a sua relação com funções de tipo especial para consideração posterior. Note-se que consideramos os polinómios (que têm um número *finito* de coeficientes não-nulos) como um caso particular de "séries de potências". Estas últimas são definidas sem qualquer referência a questões de convergência ou divergência.

No que se segue, A designa um anel abeliano com identidade 1.

Definição 3.3.2. Uma SÉRIE (FORMAL) DE POTÊNCIAS em A é uma função $\boldsymbol{s} : \mathbb{N}_0 \to A$. A série diz-se um POLINÓMIO se e só se existe $N \in \mathbb{N}_0$ tal que $\boldsymbol{s}(n) = 0$ para todo o $n > N$.

Exemplos 3.3.3.

1. *Os seguintes polinómios com coeficientes em A têm um papel importante:*
   - $\mathbf{0} = (0, 0, 0, \dots)$, *dito o* POLINÓMIO ZERO, *ou* nulo*;*
   - $\mathbf{1} = (1, 0, 0, \dots)$, *o* POLINÓMIO UM, *ou* identidade*;*
   - $\boldsymbol{x} = (0, 1, 0, \dots)$, *a que chamaremos a* INDETERMINADA $\boldsymbol{x}$.
2. *O polinómio $\boldsymbol{a} = (a, 0, 0, \dots)$, onde $a \in A$, diz-se um* POLINÓMIO CONSTANTE. *Em particular, os polinómios zero e um são polinómios constantes.*

3. O conjunto das séries de potências em $\mathbb{Z}_2$ é infinito não-numerável (trata-se de um conjunto obviamente isomorfo a $\mathcal{P}(\mathbb{N})$), e o conjunto dos polinómios em $\mathbb{Z}_2$ é infinito numerável.

Os termos $\boldsymbol{s}(0), \boldsymbol{s}(1), \boldsymbol{s}(2), \dots$ da sucessão (série formal) $\boldsymbol{s} : \mathbb{N}_0 \to A$ dizem-se naturalmente os COEFICIENTES DA SÉRIE. Para evitar confusões com os valores da função possivelmente associada à série pelos processos usuais, designaremos sempre estes coeficientes por s_0, s_1, s_2, etc. Designaremos os conjuntos das séries e polinómios com coeficientes em A respectivamente pelos símbolos $A[[\boldsymbol{x}]]$ e $A[\boldsymbol{x}]$, sendo óbvio que $A[\boldsymbol{x}] \subset A[[\boldsymbol{x}]]$[4].

A soma e produto de polinómios com coeficientes reais é-nos seguramente familiar. A título de exemplo, e considerando polinómios de grau 2, temos:

$$\begin{aligned}(a_0 + a_1x + a_2x^2) + (b_0 + b_1x + b_2x^2) &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2\\ (a_0 + a_1x + a_2x^2)(b_0 + b_1x + b_2x^2), &= (a_0b_0) + (a_0b_1 + a_1b_0)x\\ &\quad +(a_0b_2 + a_1b_1 + a_2b_0)x^2 + (a_1b_2 + a_2b_1)x^3 + (a_2b_2)x^4.\end{aligned}$$

A definição seguinte limita-se a reconhecer que as operações sobre os coeficientes dos polinómios que aparecem à direita das igualdades precedentes são possíveis em qualquer anel. Note que a soma introduzida não passa da soma usual de sucessões, mas o produto não é o habitual. Quando há risco de ambiguidade, referimo-nos ao produto definido abaixo como o PRODUTO DE CONVOLUÇÃO, e representamo-lo por $\boldsymbol{s} \star \boldsymbol{t}$ em lugar de $\boldsymbol{st}$.

Definição 3.3.4. Sendo $\boldsymbol{s}, \boldsymbol{t} : \mathbb{N}_0 \to A$ séries de potências, a SOMA $\boldsymbol{s} + \boldsymbol{t}$ e o PRODUTO (DE CONVOLUÇÃO) $\boldsymbol{s} \star \boldsymbol{t}$ são as sucessões dadas por:

$$(s + t)_n = s_n + t_n, \text{ e,} \tag{3.3.1}$$

$$(s \star t)_n = \sum_{k=0}^{n} s_k t_{n-k}. \tag{3.3.2}$$

Exemplos 3.3.5.

1. Se $\boldsymbol{a} = (a, 0, 0, \dots)$ e $\boldsymbol{b} = (b, 0, 0, \dots)$ são polinómios constantes, a sua soma e o seu produto são dados por $\boldsymbol{a} + \boldsymbol{b} = (a + b, 0, 0, \dots)$ e $\boldsymbol{a} \star \boldsymbol{b} = \boldsymbol{ab} = (ab, 0, 0, \dots)$. Portanto, o conjunto dos polinómios constantes com as operações acima indicadas é um anel isomorfo ao anel A.

2. Se $\boldsymbol{a} = (a, 0, 0, \dots)$ é constante e $\boldsymbol{s} = (s_0, s_1, s_2, \dots)$ é uma qualquer série, o produto $\boldsymbol{a} \star \boldsymbol{s}$ é a série $(as_0, as_1, as_2, \dots) = \boldsymbol{as}$, porque a soma $\sum_{k=0}^{n} a_k s_{n-k}$ se reduz sempre ao termo com $k = 0$.

[4] O uso da letra "$\boldsymbol{x}$" na notação $A[\boldsymbol{x}]$ ou $A[[\boldsymbol{x}]]$ é condicionado pela escolha desta letra para designar a indeterminada $(0, 1, 0, \dots)$. Poderemos por vezes designar esta indeterminada por uma outra letra, *e.g.* $\boldsymbol{y}$, caso em que usamos a notação $A[\boldsymbol{y}]$ ou $A[[\boldsymbol{y}]]$.

3. Considere-se a série $\boldsymbol{s} = (\underline{1}, \underline{1}, \underline{1}, \dots)$ *com coeficientes em* $\mathbb{Z}_2$*. Para calcular o seu quadrado, observamos que* $(\boldsymbol{ss})_n = \sum_{k=0}^{n} s_k s_{n-k} = \sum_{k=0}^{n} \underline{1} = \underline{n+1}$*. Concluímos que*

$$(\underline{1}, \underline{1}, \underline{1}, \dots)(\underline{1}, \underline{1}, \underline{1}, \dots) = (\underline{1}, \underline{0}, \underline{1}, \underline{0}, \dots).$$

4. Se $\boldsymbol{s} = (s_0, s_1, s_2, \dots)$ *é uma qualquer série, o produto* $\boldsymbol{xs}$ *é a série que se obtém de* $\boldsymbol{s}$ *por translação de todos os seus coeficientes para a direita, porque*

$$(\boldsymbol{xs})_0 = x_0 s_0 = 0,$$
$$(\boldsymbol{xs})_{n+1} = \sum_{k=0}^{n+1} x_k s_{n+1-k} = s_n.$$

No caso $\boldsymbol{s} = \boldsymbol{x}$*, concluímos que* $\boldsymbol{x}^2 = (0, 0, 1, 0, \dots)$*,* $\boldsymbol{x}^3 = (0, 0, 0, 1, 0, \dots)$*, etc. Alargamos esta observação ao caso* $n = 0$*, escrevendo por convenção*

$$\boldsymbol{x}^0 = (1, 0, 0, \dots) = \mathbf{1}.$$

O próximo teorema não apresenta dificuldades técnicas, e a sua demonstração fica como exercício.

Teorema 3.3.6. *Se* A *é um anel abeliano com identidade, tanto* $A[[\boldsymbol{x}]]$ *como* $A[\boldsymbol{x}]$[5] *são anéis abelianos com identidade (com a soma e o produto definidos por (3.3.1) e (3.3.2)), e* $A[\boldsymbol{x}]$ *é um subanel de* $A[[\boldsymbol{x}]]$*.*

Observámos acima que o conjunto dos polinómios constantes é um anel isomorfo a A. Como fizemos em casos análogos, passamos a usar o mesmo símbolo a para designar um dado elemento do anel A, e o correspondente polinómio constante $(a, 0, 0, \dots)$. Dizemos também que $A[\boldsymbol{x}]$ e (por maioria de razão) $A[[\boldsymbol{x}]]$ são extensões de A. Note-se que a expressão $a\boldsymbol{x}^n$ passa a representar assim o produto do polinómio constante $(a, 0, 0, \dots)$ pela potência n da indeterminada $\boldsymbol{x}$, *i.e.*, $\boldsymbol{x}^n$, que de acordo com o que dissemos acima tem como único coeficiente diferente de zero o coeficiente $(a\boldsymbol{x}^n)_n = a$ (nesta última igualdade, a tem dois significados diferentes!). Concluímos que, se $\boldsymbol{p} = (p_0, p_1, p_2, \dots, p_N, 0, \dots)$, então

$$\boldsymbol{p} = p_0 + p_1\boldsymbol{x} + \cdots + p_N\boldsymbol{x}^N = \sum_{n=0}^{N} p_n \boldsymbol{x}^n.$$

Dizemos que a soma à direita é a FORMA CANÓNICA do polinómio $\boldsymbol{p}$. Como é habitual, um coeficiente é omitido se for igual a 1.

[5] O anel $A[[\boldsymbol{x}]]$ das séries formais de potências em A e o anel S das sucessões em A têm evidentemente o mesmo suporte e a mesma operação de soma, sendo diferentes apenas na operação de multiplicação. Quando é necessário distinguir a série de potências $\boldsymbol{s}$ em $A[[\boldsymbol{x}]]$ da correspondente sucessão $\boldsymbol{a}$ em S, é frequente dizer que $\boldsymbol{s}$ é a TRANSFORMADA z de $\boldsymbol{a}$.

Exemplo 3.3.7.

Suponha-se que $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}_4[\boldsymbol{x}]$ *são dados por* $\boldsymbol{p} = \underline{1} + \boldsymbol{x} + \underline{2}\boldsymbol{x}^2$ *e* $\boldsymbol{q} = \underline{1} + \underline{2}\boldsymbol{x}^2$. *Para somar e multiplicar estes polinómios, procedemos exactamente como com polinómios com coeficientes reais, reconhecendo que os procedimentos usuais envolvem apenas propriedades algébricas comuns a qualquer anel. Deve ser fácil reconhecer essas propriedades nos cálculos pormenorizados que se seguem, complementados com detalhes específicos do anel a que pertencem os coeficientes:*

$$\begin{aligned}(\underline{1} + \boldsymbol{x} + \underline{2}\boldsymbol{x}^2) + (\underline{1} + \underline{2}\boldsymbol{x}^2) &= (\underline{1} + \underline{1}) + (\underline{1} + \underline{0})\boldsymbol{x} + (\underline{2} + \underline{2})\boldsymbol{x}^2 \\ &= \underline{2} + \boldsymbol{x}, \\ (\underline{1} + \boldsymbol{x} + \underline{2}\boldsymbol{x}^2)(\underline{1} + \underline{2}\boldsymbol{x}^2) &= (\underline{1} + \boldsymbol{x} + \underline{2}\boldsymbol{x}^2)\underline{1} + (\underline{1} + \boldsymbol{x} + \underline{2}\boldsymbol{x}^2)\underline{2}\boldsymbol{x}^2 \\ &= (\underline{1} + \boldsymbol{x} + \underline{2}\boldsymbol{x}^2) + (\underline{2}\boldsymbol{x}^2 + \underline{2}\boldsymbol{x}^3) \\ &= \underline{1} + \boldsymbol{x} + \underline{2}\boldsymbol{x}^3.\end{aligned}$$

Em certos casos, é possível atribuir significado a "somas" do tipo $\sum_{n=0}^{\infty} \boldsymbol{s}_n$, em que cada $\boldsymbol{s}_n$ é uma série de potências. Se s_{nk} designa o coeficiente k da série $\boldsymbol{s}_n$, o significado mais simples a atribuir à igualdade $\boldsymbol{t} = \sum_{n=0}^{\infty} \boldsymbol{s}_n$ é

$$\boldsymbol{t} = \sum_{n=0}^{\infty} \boldsymbol{s}_n \iff t_k = \sum_{n=0}^{\infty} s_{nk}, \text{ para todo o } k \in \mathbb{N}_0.$$

Utilizaremos esta definição sempre que a sucessão s_{nk} for eventualmente zero para qualquer $k \geq 0$, interpretando a "soma" infinita à direita como a soma (finita) dos seus termos diferentes de zero. Escreveremos em particular

$$\boldsymbol{s} = \sum_{n=0}^{\infty} s_n \boldsymbol{x}^n,$$

para qualquer série de potências $\boldsymbol{s}$.

Definição 3.3.8. Se $\boldsymbol{p} \neq 0$ é um polinómio, o GRAU de p é o inteiro $\deg \boldsymbol{p}$ definido por

$$\deg \boldsymbol{p} = \max\{n \in \mathbb{N}_0 : p_n \neq 0\}.$$

Se $\boldsymbol{p} = 0$, então convencionamos que $\deg \boldsymbol{p} = -\infty$.

Exemplo 3.3.9.

Claramente, $\deg \boldsymbol{x}^n = n$, *para qualquer* $n \geq 0$.

O exemplo de produto de polinómios em $\mathbb{Z}_4[\boldsymbol{x}]$ que vimos acima mostra que nem sempre o grau do produto de dois polinómios é a soma dos graus dos polinómios factores. O próximo teorema esclarece completamente as

propriedades do grau, face à soma e ao produto de polinómios. Para evitar frequentes excepções envolvendo o polinómio nulo, convencionamos que $\deg \boldsymbol{p} + \deg \boldsymbol{q} = -\infty$, sempre que $\boldsymbol{p} = 0$ ou $\boldsymbol{q} = 0$.

Proposição 3.3.10. *Sejam $\boldsymbol{p}, \boldsymbol{q} \in A[\boldsymbol{x}]$. temos então:*

(i) $\deg(\boldsymbol{p} + \boldsymbol{q}) \leq \max\{\deg \boldsymbol{p}, \deg \boldsymbol{q}\}$, *e* $\deg(\boldsymbol{pq}) \leq \deg \boldsymbol{p} + \deg \boldsymbol{q}$;

(ii) se A é um domínio integral, $\deg(\boldsymbol{pq}) = \deg \boldsymbol{p} + \deg \boldsymbol{q}$, *e $A[\boldsymbol{x}]$ é um domínio integral.*

A demonstração deste teorema fica como exercício. Note-se que, de acordo com (ii), quando A é um domínio integral, podemos formar o corpo das fracções de $A[\boldsymbol{x}]$ (*i.e.*, $\mathrm{Frac}(A[\boldsymbol{x}])$ na notação da secção anterior). Um momento de reflexão mostra que este corpo é o análogo formal e abstracto do corpo das FUNÇÕES RACIONAIS da Álgebra elementar.

Definição 3.3.11. Se A é um domínio integral, $A(\boldsymbol{x})$ designa o CORPO DE FRACÇÕES de $A[\boldsymbol{x}]$.

Exemplo 3.3.12.

Se $A = \mathbb{Z}$, então $\mathbb{Z}(\boldsymbol{x})$ é o corpo das fracções cujos numeradores e denominadores são polinómios com coeficientes inteiros. Neste corpo, temos

$$\frac{\boldsymbol{x}^2 - 1}{\boldsymbol{x} + 1} = \boldsymbol{x} - 1.$$

No entanto, as funções $f(x) = \frac{\boldsymbol{x}^2-1}{\boldsymbol{x}+1}$ *e* $g(x) = \boldsymbol{x} - 1$ *não são iguais, porque têm domínios distintos.*

Sendo $\phi : A \to B$ um homomorfismo de anéis, é fácil verificar que a função $\Phi : A[\boldsymbol{x}] \to B[\boldsymbol{x}]$ dada por

$$\Phi\left(\sum_{n=0}^{N} p_n \boldsymbol{x}^n\right) = \sum_{n=0}^{N} \phi(p_n)\boldsymbol{x}^n$$

é igualmente um homomorfismo de anéis. Frequentemente, se $\boldsymbol{p} \in A[\boldsymbol{x}]$, então designamos o polinómio $\boldsymbol{q} = \Phi(\boldsymbol{p})$ por $\boldsymbol{p}^{\phi}(\boldsymbol{x})$. Em certos casos (por exemplo, se $A \subset B$ é um subanel e $\phi : A \to B$ é a inclusão), utilizamos a mesma letra para designar estes dois polinómios, sendo claro do contexto a que anel pertencem os coeficientes do polinómio. O exemplo seguinte mostra que este é um "abuso" razoável (mesmo natural) de notação ao qual já estamos habituados!

Exemplo 3.3.13.

Seja $\boldsymbol{p} = 1 + 2\boldsymbol{x} + 3\boldsymbol{x}^2 \in \mathbb{Z}[\boldsymbol{x}]$ um polinómio com coeficientes inteiros. Claro que $\mathbb{Z} \subset \mathbb{Q}$, e podemos considerar a inclusão canónica $\iota : \mathbb{Z} \to \mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$. Temos obviamente $\boldsymbol{p}^\iota(\boldsymbol{x}) = 1+2\boldsymbol{x}+3\boldsymbol{x}^2 \in \mathbb{Q}[\boldsymbol{x}]$. Na realidade, os símbolos "1", "2" e "3" nesta segunda expressão designam números racionais e não números inteiros, mas esse é um abuso de notação aceitável, tal como discutimos a propósito dos corpos de fracções: a fracção $\frac{ax}{a}$ designa-se por x. É pois natural representar este novo polinómio pela mesma letra do original.

Finalmente, observe-se que, se $\phi : A \to B$ é um monomorfismo de anéis e $\boldsymbol{p} \in A[\boldsymbol{x}]$, então $\boldsymbol{p}$ e $\boldsymbol{p}^\phi(\boldsymbol{x})$ possuem o mesmo grau.

Exercícios.

1. Para $m = 2$, 3 e 6, calcule em $\mathbb{Z}_m[\boldsymbol{x}]$ o produto
$$(\underline{1} + \boldsymbol{x} + \underline{2}\boldsymbol{x}^2)(\underline{2} + \underline{3}\boldsymbol{x} + \underline{2}\boldsymbol{x}^2).$$

2. Demonstre o Teorema 3.3.6.

3. Mostre que o ideal $\langle 2, \boldsymbol{x}\rangle$ em $\mathbb{Z}[\boldsymbol{x}]$ não é principal.

4. Demonstre a Proposição 3.3.10.

5. Quais são os elementos de $A[\boldsymbol{x}]^*$, quando A é um domínio integral?

6. Suponha que A é um domínio integral, e mostre que as características de $A[\boldsymbol{x}]$ e A são iguais.

7. Os polinómios em mais de uma variável podem ser definidos de diversas maneiras. Para o caso de 2 variáveis, podemos considerar:

   (i) O anel $A[\boldsymbol{x}]$, e os polinómios com coeficientes em $A[\boldsymbol{x}]$ que denotamos por $A[\boldsymbol{x}][\boldsymbol{y}]$ (designamos neste caso a nova indeterminada por $\boldsymbol{y}$);

   (ii) As funções $s : \mathbb{N}_0 \times \mathbb{N}_0 \to A$, definindo de forma apropriada as operações de soma e produto de convolução, e as indeterminadas $\boldsymbol{x}$ e $\boldsymbol{y}$, de modo a obter um anel que denotamos por $A[\boldsymbol{x}, \boldsymbol{y}]$.

   Estas duas formas de encarar polinómios a várias variáveis são ambas úteis. Os exercícios seguintes mostram que são equivalentes.

   (a) Descreva completamente a definição sugerida em (ii).

   (b) Prove que as duas definições indicadas são equivalentes, *i.e.*, conduzem a anéis isomorfos.

   (c) Como se devem generalizar estas definições para polinómios nas variáveis $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$?

   (d) Como se devem generalizar estas definições para polinómios nas variáveis $\boldsymbol{x}_\alpha$, com $\alpha \in I$, onde I pode ser um conjunto infinito?

8. Mostre que as seguintes afirmações são equivalentes:

   (a) A é um domínio integral;

   (b) $A[\boldsymbol{x}]$ é um domínio integral;

   (c) $A[[\boldsymbol{x}]]$ é um domínio integral;

   (d) para quaisquer $\boldsymbol{p}, \boldsymbol{q} \in A[\boldsymbol{x}]$, $\deg(\boldsymbol{pq}) = \deg \boldsymbol{p} + \deg \boldsymbol{q}$.

9. Mostre que existem anéis com característica p (primo) que não são corpos, e corpos com característica p que são infinitos (tanto numeráveis como não-numeráveis).

10. Se $\boldsymbol{p} \in A[\boldsymbol{x}]$ é o polinómio $\boldsymbol{p} = \sum_{n=0}^{N} p_n \boldsymbol{x}^n$, a sua DERIVADA (FORMAL) $\boldsymbol{p}'$ é o polinómio
$$\boldsymbol{p}' = \sum_{n=1} n p_n \boldsymbol{x}^{n-1}.$$
É sempre verdade que $\boldsymbol{p}' = 0$ implica que $\boldsymbol{p}$ é constante?

11. Use o exercício anterior e o homomorfismo $\phi : \mathbb{Z} \to \mathbb{Z}_p$ dado por $\phi(n) = \underline{n}$ para provar a seguinte generalização do Lema de Euclides: se $p \in \mathbb{N}$ é primo, $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}[\boldsymbol{x}]$ e $p | \boldsymbol{ab}$, então $p | \boldsymbol{a}$ ou $p | \boldsymbol{b}$.

12. Seja D um domínio integral, e $K = \mathrm{Frac}(D)$. Prove que $D(\boldsymbol{x})$ é isomorfo a $K(\boldsymbol{x})$.

13. Defina um anel com suporte nas séries de potências da forma $\sum_{n=k}^{\infty} s_n \boldsymbol{x}^n$, onde $k \in \mathbb{Z}$ é arbitrário[6]. Mostre que, se os coeficientes pertencem a um corpo K, então o anel assim definido é um corpo isomorfo a $\mathrm{Frac}(K[[x]])$.

14. Prove que em $K[[\boldsymbol{x}]]$ temos
$$\frac{1}{1-\boldsymbol{x}} = \sum_{n=0}^{\infty} \boldsymbol{x}^n.$$
(Note o abuso de notação que o exercício anterior possibilita!)

15. Determine as séries de potências inversas de $(a - \boldsymbol{x})$ e de $(a - \boldsymbol{x})(b - \boldsymbol{x})$ em $K[\boldsymbol{x}]$.

16. Mostre que em $\mathbb{Z}_2[[\boldsymbol{x}]]$, temos
$$\frac{1}{(1-\boldsymbol{x})^2} = \sum_{n=0}^{\infty} \boldsymbol{x}^{2n}.$$

[6] Estas séries são conhecidas pelo nome de SÉRIES DE LAURENT, sendo pois este anel designado por anel das séries de Laurent com coeficientes em A. O caso em que $A = \mathbb{C}$ desempenha um papel crucial na Análise Complexa e na Geometria Algébrica.

17. É possível resolver problemas como o da sucessão de Fibonacci da Secção 2.3 através de cálculos com séries formais de potências. Recordando que esta é definida recursivamente pela equação

$$a_{n+2} = a_{n+1} + a_n, \qquad (n \geq 0),$$

começamos por observar a sua equivalência com

$$\sum_{n=0}^{\infty} a_{n+2}\boldsymbol{x}^n = \sum_{n=0}^{\infty} a_{n+1}\boldsymbol{x}^n + \sum_{n=0}^{\infty} a_n\boldsymbol{x}^n,$$

e com

$$\sum_{n=0}^{\infty} a_{n+2}\boldsymbol{x}^{n+2} = \boldsymbol{x}\sum_{n=0}^{\infty} a_{n+1}\boldsymbol{x}^{n+1} + \boldsymbol{x}^2\sum_{n=0}^{\infty} a_n\boldsymbol{x}^n.$$

Como, se $\boldsymbol{s} = \sum_{n=0}^{\infty} a_n\boldsymbol{x}^n$, então

$$\sum_{n=0}^{\infty} a_{n+2}\boldsymbol{x}^{n+2} = \boldsymbol{s} - a_0 - a_1\boldsymbol{x},$$
$$\sum_{n=0}^{\infty} a_{n+1}\boldsymbol{x}^{n+1} = \boldsymbol{s} - a_0,$$

concluímos que a relação de recorrência é equivalente a

$$\boldsymbol{s} - a_0 - a_1\boldsymbol{x} = \boldsymbol{x}(\boldsymbol{s} - a_0) + \boldsymbol{x}^2\boldsymbol{s}.$$

Resolvendo em ordem a $\boldsymbol{s}$, obtemos:

$$\boldsymbol{s} = \frac{-a_0 + (a_0 - a_1)\boldsymbol{x}}{\boldsymbol{x}^2 + \boldsymbol{x} - 1}.$$

Sendo α e β as raízes de $\boldsymbol{x}^2 + \boldsymbol{x} - 1$, podemos decompor a fracção racional anterior na forma

$$\frac{-a_0 + (a_0 - a_1)\boldsymbol{x}}{\boldsymbol{x}^2 + \boldsymbol{x} - 1} = \frac{A}{\alpha - \boldsymbol{x}} + \frac{B}{\beta - \boldsymbol{x}},$$

e usar o resultado do exercício acima para calcular explicitamente os coeficientes de $\boldsymbol{s}$, que são os termos da sucessão de Fibonacci.

Verifique todas estas afirmações, e calcule os coeficientes da sucessão de Fibonacci.

3.4 Funções Polinomiais

Observámos na secção anterior que não é de todo conveniente definir os *polinómios* com coeficientes em A como *funções* de determinado tipo, com domínio e valores em A. Apesar disso, nada nos impede de definir funções de A em A a partir de polinómios em $A[\boldsymbol{x}]$.

Definição 3.4.1. Se $\boldsymbol{p} = \sum_{n=0}^{N} p_n \boldsymbol{x}^n$ é um polinómio em $A[\boldsymbol{x}]$, a função $\boldsymbol{p}^* : A \to A$ definida por $\boldsymbol{p}^*(a) = \sum_{n=0}^{N} p_n a^n$ diz-se FUNÇÃO POLINOMIAL ASSOCIADA a $\boldsymbol{p}$.

Exemplo 3.4.2.

Seja $A = \mathbb{Z}_2$, e $\boldsymbol{p} = 1+\boldsymbol{x}+\boldsymbol{x}^2$ ([7]). A função polinomial associada ao polinómio $\boldsymbol{p}$ é $\boldsymbol{p}^* : \mathbb{Z}_2 \to \mathbb{Z}_2$ dada por $\boldsymbol{p}^*(a) = 1 + a + a^2$, para qualquer $a \in \mathbb{Z}_2$. Neste caso, temos $\boldsymbol{p}^*(0) = \boldsymbol{p}^*(1) = 1$, e portanto $\boldsymbol{p}^*$ é uma função constante, apesar de $\boldsymbol{p}$ não ser um polinómio constante. Em particular, se $\boldsymbol{q} = 1$, temos $\boldsymbol{p} \neq \boldsymbol{q}$ e $\boldsymbol{p}^* = \boldsymbol{q}^*$.

Sendo A um anel e designando por A^A o conjunto das funções $f : A \to A$, observámos no Capítulo 1 que A^A é um anel, com as operações usuais de soma e produto de funções. A função que associa a cada polinómio $\boldsymbol{p} \in A[\boldsymbol{x}]$ a respectiva função $\boldsymbol{p}^* : A \to A$ é uma função $\Psi : A[\boldsymbol{x}] \to A^A$, e temos

Proposição 3.4.3. *$\Psi : A[\boldsymbol{x}] \to A^A$ é um homomorfismo.*

Demonstração. Sejam $\boldsymbol{p}, \boldsymbol{q} \in A[\boldsymbol{x}]$, onde podemos sempre escrever (tomando se necessário coeficientes nulos adicionais) $\boldsymbol{p} = \sum_{n=0}^{N} p_n \boldsymbol{x}^n$ e $\boldsymbol{q} = \sum_{n=0}^{N} q_n \boldsymbol{x}^n$.

Supondo que $a \in A$, temos a provar as seguintes igualdades:

$$(\boldsymbol{p} + \boldsymbol{q})^*(a) = \boldsymbol{p}^*(a) + \boldsymbol{q}^*(a), \text{ e}$$
$$(\boldsymbol{pq})^*(a) = \boldsymbol{p}^*(a)\boldsymbol{q}^*(a).$$

A primeira destas igualdades foi provada no Capítulo 2 em termos um pouco mais gerais. A segunda pode ser demonstrada sem grandes dificuldades por indução em N. □

Exemplos 3.4.4.

1. *Dado um polinómio $\boldsymbol{p} \in A[\boldsymbol{x}]$, a função $\boldsymbol{p}^*$ associada está definida não só no anel A como em qualquer extensão de A. Por exemplo, sendo $\boldsymbol{p} = 1 + 2\boldsymbol{x} + 3\boldsymbol{x}^2 \in \mathbb{Z}[\boldsymbol{x}]$, a função polinomial associada é em princípio $\boldsymbol{p}^* : \mathbb{Z} \to \mathbb{Z}$, dada naturalmente por $\boldsymbol{p}^*(n) = 1 + 2n + 3n^2$, para qualquer $n \in \mathbb{Z}$. No entanto, como $\mathbb{Z} \subset \mathbb{Q}$ podemos também considerar $\boldsymbol{q}^* : \mathbb{Q} \to \mathbb{Q}$, dada igualmente por $\boldsymbol{q}^*(r) = 1 + 2r + 3r^2$, para qualquer $r \in \mathbb{Q}$.*

   De um modo geral, se o anel B é uma extensão do anel A (no sentido em que existe um homomorfismo injectivo $\phi : A \to B$, donde $\phi(A)$ é um subanel de B isomorfo a A), e $\boldsymbol{p} = \sum_{n=0}^{N} p_n \boldsymbol{x}^n$ é um polinómio em $A[\boldsymbol{x}]$, então $\boldsymbol{p}$ determina uma função polinomial $\boldsymbol{q}^* : B \to B$, nomeadamente $\boldsymbol{q}^*(b) = \sum_{n=0}^{N} \phi(p_n) b^n$. É claro que, na notação da secção anterior, temos $\boldsymbol{q}^* = (\boldsymbol{p}^\phi)^*$. Tal como observámos em relação à forma canónica de $\boldsymbol{p}^*$, é uma mera questão de bom

[7] Daqui em diante, não distinguimos entre o inteiro n e a classe $\underline{n}$, sendo claro do contexto se nos referimos a um inteiro (elemento de $\mathbb{Z}$) ou a uma classe de equivalência nalgum $\mathbb{Z}_m$.

senso saber se utilizamos uma letra diferente para $\boldsymbol{q}^*$ e se é necessário escrever explicitamente os coeficientes na forma $\phi(p_n)$, ou se é mais razoável usar o mesmo símbolo para p_n e $\phi(p_n)$.

2. *Continuando o exemplo anterior, recordamos que $M_2(\mathbb{Z})$ é o anel das matrizes 2×2 com entradas inteiras, e que o conjunto das matrizes da forma nI (onde I é a matriz identidade e $n \in \mathbb{Z}$) é isomorfo a $\mathbb{Z}$. O monomorfismo $\phi : \mathbb{Z} \to M_2(\mathbb{Z})$ é dado por $\phi(n) = nI$, e portanto $(\boldsymbol{p}^\phi)^* : M_2(\mathbb{Z}) \to M_2(\mathbb{Z})$ é dada por $(\boldsymbol{p}^\phi)^*(C) = \phi(1) + \phi(2)C + \phi(3)C^2$, onde C designa agora uma qualquer matriz em $M_2(\mathbb{Z})$. É claro que a expressão $\phi(1) + \phi(2)C + \phi(3)C^2$ se pode simplificar neste caso para $I + 2C + 3C^2$, expressão em tudo igual à usada no exemplo 1, com excepção da pequena "subtileza" de substituir o símbolo "1" pelo símbolo "I", este último representando evidentemente a matriz identidade.*

No primeiro exemplo, a identificação do anel $\mathbb{Z}$ com a sua imagem em $\mathbb{Q}$ é aceitável e recomendável. No segundo exemplo não é necessário substituir os coeficientes de grau > 0 (porque o produto de uma matriz pelo inteiro n é igual ao produto da mesma matriz por nI), mas é indispensável substituir o coeficiente com grau zero, porque a soma de uma matriz com um inteiro n não está definida, e portanto não deve ser usada para representar a soma da mesma matriz com a matriz nI.

Por outro lado, podemos utilizar estas ideias para formalizar a noção de raiz de um polinómio:

Definição 3.4.5. Seja $\boldsymbol{p} \in A[\boldsymbol{x}]$ e B uma extensão de A. Dizemos que $b \in B$ é uma RAIZ de $\boldsymbol{p}$ se $\boldsymbol{p}^*(b) = 0$.

Quando escrevemos a expressão $\boldsymbol{p}^*(a)$, estamos habituados a considerar $\boldsymbol{p}^*$ como fixo e a como variável (a "variável independente" da função $\boldsymbol{p}^*$). No entanto, é possível considerar ao mesmo tempo $\boldsymbol{p}^*$ e a como variáveis independentes. Supondo que A é mais uma vez um qualquer anel abeliano com identidade e B uma sua extensão, introduzimos a seguinte definição (sem esquecer as observações acima a propósito da identificação entre um anel e uma sua imagem isomorfa):

Definição 3.4.6. A função $\mathrm{Val} : A[\boldsymbol{x}] \times B \to B$ é dada por $\mathrm{Val}(\boldsymbol{p}, b) = \boldsymbol{p}^*(b)$. $\mathrm{Val}(\boldsymbol{p}, b)$ diz-se o VALOR do polinómio $\boldsymbol{p}$ no ponto b.

A função Val tem duas variáveis independentes (o polinómio $\boldsymbol{p}$ e o ponto b). Se fixarmos o polinómio $\boldsymbol{p}$, Val reduz-se à função $\boldsymbol{p}^* : B \to B$, associada ao polinómio $\boldsymbol{p}$, de que já vimos vários exemplos. É também possível fixar o valor de b, para obter uma função $\psi : A[\boldsymbol{x}] \to B$.

Exemplos 3.4.7.

1. *Seja $A = \mathbb{Z}$, $B = \mathbb{C}$ e $b = i$. Temos portanto $\psi : \mathbb{Z}[\boldsymbol{x}] \to \mathbb{C}$ dada por $\psi(\boldsymbol{p}) = \boldsymbol{p}^*(i)$, e para determinar a imagem de $\psi(\mathbb{Z}[\boldsymbol{x}])$ recordamos que qualquer polinómio $\boldsymbol{p} \in \mathbb{Z}[\boldsymbol{x}]$ pode ser dividido por $1 + \boldsymbol{x}^2$, com um resto de grau inferior*

a 2. *Por outras palavras,* $\boldsymbol{p} = (1+\boldsymbol{x}^2)\boldsymbol{q}+(a_0+a_1\boldsymbol{x})$*, onde* $\boldsymbol{q} \in \mathbb{Z}[\boldsymbol{x}]$ *e* $a_0, a_1 \in \mathbb{Z}$*. Logo* $\boldsymbol{p}^*(i) = a_0 + a_1 i$ *é um inteiro de Gauss.*

2. *Seja* $A = \mathbb{Q}$*,* $B = \mathbb{R}$ *e* $b = \sqrt{2}$*. Neste caso,* $\psi(\boldsymbol{p}) = \boldsymbol{p}^*(\sqrt{2})$*, e como* $\boldsymbol{p} = (2-\boldsymbol{x}^2)\boldsymbol{q}+(a_0+a_1\boldsymbol{x})$*, onde* $\boldsymbol{q} \in \mathbb{Q}[\boldsymbol{x}]$ *e* $a_0, a_1 \in \mathbb{Q}$*, temos* $\boldsymbol{p}^*(\sqrt{2}) = a_0+a_1\sqrt{2}$*, e concluímos que* $\psi(\mathbb{Q}[\boldsymbol{x}])$ *é o conjunto dos números reais da forma* $a_0 + a_1\sqrt{2}$ *com* $a_0, a_1 \in \mathbb{Q}$*.*

3. *O anel* $A[\boldsymbol{x}]$ *é sempre uma extensão de* A*, e por isso supomos agora* A *arbitrário,* $B = A[\boldsymbol{x}]$ *e* $b = \boldsymbol{x}$*. É óbvio que* $\psi(\boldsymbol{p}) = \boldsymbol{p}^*(\boldsymbol{x}) = \boldsymbol{p}$*,* i.e.*,* $\psi : A[\boldsymbol{x}] \to A[\boldsymbol{x}]$ *é a* identidade*. Por este motivo, podemos designar o polinómio* $\boldsymbol{p}$ *pelo símbolo* $\boldsymbol{p}^*(\boldsymbol{x})$*, usualmente simplificado para* $p(\boldsymbol{x})$*.*

Por analogia com o último exemplo, sempre que B é uma extensão de A, $b \in B$, e $\psi : A[\boldsymbol{x}] \to B$ é dada por $\psi(\boldsymbol{p}) = \boldsymbol{p}^*(b)$, designamos o conjunto $\psi(A[\boldsymbol{x}])$ pelo símbolo $A[b]$. É esta a razão pela qual introduzimos o símbolo $\mathbb{Z}[i]$ quando primeiro referimos os inteiros de Gauss. No caso do segundo dos Exemplos 3.4.7, temos

$$\mathbb{Q}[\sqrt{2}] = \{\boldsymbol{p}^*(\sqrt{2}) : \boldsymbol{p} \in \mathbb{Q}\} = \{a_0 + a_1\sqrt{2} : a_0, a_1 \in \mathbb{Q}\}.$$

Os exemplos anteriores sugerem que $A[b]$ é sempre um subanel de B. É isso que provamos a seguir.

Proposição 3.4.8. *Fixado* $b \in B$*, e definindo* $\psi : A[\boldsymbol{x}] \to B$ *por* $\psi(\boldsymbol{p}) = \boldsymbol{p}^*(b)$*,* ψ *é um homomorfismo de anéis, donde* $A[b]$ *é um subanel de* B*.*

Demonstração. Procedemos como na demonstração da Proposição 3.4.3. □

Por analogia com a Definição 3.3.11, sempre que $A[b]$ é um domínio integral designamos o seu corpo de fracções por $A(b)$.

Note-se que $A[b]$ contém necessariamente os valores de todos os polinómios constantes, que formam um subanel de $A[b]$ isomorfo a A. Portanto, $A[b]$ é sempre uma *extensão* de A. (O anel dos inteiros de Gauss contém um subanel isomorfo a $\mathbb{Z}$, $\mathbb{Q}(\sqrt{2})$ contém um subanel isomorfo a $\mathbb{Q}$, etc.). Por outro lado, nos Exemplos 3.4.7, ψ é injectiva apenas no último, e portanto só no último caso é que $A[b]$ é isomorfo a $A[\boldsymbol{x}]$. É claro que ψ é injectiva se e só se o seu núcleo $N(\psi)$ se reduz ao polinómio zero, e que o núcleo de ψ, dado por

$$N(\psi) = \{\boldsymbol{p} \in A[\boldsymbol{x}] : \boldsymbol{p}^*(b) = 0\},$$

é simplesmente o conjunto dos polinómios com coeficientes em A que têm b como uma das suas raízes. Concluímos que ψ é injectiva se e só se b não é raiz de *nenhum* polinómio não-nulo com coeficientes em A.

Definição 3.4.9. Seja B uma extensão de A, e $b \in B$. Dizemos que b é ALGÉBRICO sobre A se existe algum polinómio não-nulo $\boldsymbol{p} \in A[\boldsymbol{x}]$ tal que $\boldsymbol{p}^*(b) = 0$. Caso contrário, b diz-se TRANSCENDENTE sobre A.

Exemplo 3.4.10.

Como vimos acima, i é algébrico sobre $\mathbb{Z}$, e $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$ (como aliás sobre $\mathbb{Z}$). O polinómio $\boldsymbol{x}$ é sempre transcendente sobre A.

Em geral, se B é uma qualquer extensão de A, então B pode conter elementos algébricos e elementos transcendentes sobre A, ou apenas elementos algébricos sobre A. Distinguimos estas possibilidades como se segue:

Definição 3.4.11. B diz-se uma EXTENSÃO ALGÉBRICA de A se todos os seus elementos são algébricos sobre A. Caso contrário, B diz-se uma EXTENSÃO TRANSCENDENTE de A.

Exemplos 3.4.12.

1. *O anel dos inteiros de Gauss é uma extensão algébrica de $\mathbb{Z}$. Para o verificar, notamos apenas que o inteiro de Gauss $m + ni$ é raiz do polinómio com coeficientes inteiros $(\boldsymbol{x} - m)^2 + n^2 = \boldsymbol{x}^2 - 2m\boldsymbol{x} + m^2 + n^2$, que é sempre não-nulo.*

2. *$\mathbb{Q}[\sqrt{2}]$ é uma extensão algébrica de $\mathbb{Q}$, porque $a + b\sqrt{2}$ é raiz do polinómio com coeficientes racionais $(\boldsymbol{x} - a)^2 - 2b^2$, mais uma vez não-nulo.*

3. *$\mathbb{Q}$ é uma extensão algébrica de $\mathbb{Z}$, porque $\frac{m}{n}$ é raiz de $n\boldsymbol{x} - m \in \mathbb{Z}[\boldsymbol{x}]$.*

4. *$\mathbb{C}$ é uma extensão algébrica de $\mathbb{R}$, porque $a+bi$ é raiz de $(\boldsymbol{x}-a)^2+b^2 \in \mathbb{R}[\boldsymbol{x}]$.*

5. *$A[\boldsymbol{x}]$ é uma extensão transcendente de A.*

6. *Provaremos adiante que $\mathbb{R}$ é uma extensão transcendente de $\mathbb{Q}$.*

O próximo resultado diz essencialmente que $A[\boldsymbol{x}]$ é a *menor* extensão transcendente de A. A sua demonstração fica como exercício.

Teorema 3.4.13. *Qualquer extensão transcendente de A contém um subanel isomorfo a $A[\boldsymbol{x}]$.*

Exercícios.

1. Conclua a demonstração da Proposição 3.4.3.

2. Suponha que $\sqrt{n}$ é irracional, e mostre que $\mathbb{Q}[\sqrt{n}]$ é uma extensão algébrica de $\mathbb{Q}$, um subcorpo de $\mathbb{R}$, e um espaço vectorial de dimensão 2 sobre $\mathbb{Q}$.[8]

3. Demonstre o Teorema 3.4.13.

4. Suponha que $A \subset B$ são domínios integrais e $b \in B$. Mostre que:

[8] Os corpos da forma $\mathbb{Q}[\sqrt{a}]$ onde a não é um quadrado perfeito, os chamados CORPOS QUADRÁTICOS, desempenham um papel importante na Teoria dos Números.

(a) $A[b]$ é o menor domínio integral que contém A e b.

(b) $A(b)$ é o menor corpo que contém A e b.

5. Sendo K um corpo, considere N pontos (a_k, b_k) em $K \times K$ com $a_i \neq a_j$ para $i \neq j$. Prove que:

(a) Existe um polinómio $\boldsymbol{p}_i \in K[\boldsymbol{x}]$ tal que

$$p_i(a_j) = \begin{cases} 1, & \text{se } j = i, \\ 0, & \text{se } j \neq i. \end{cases}$$

(SUGESTÃO: Modifique o polinómio $\boldsymbol{q}_i = \frac{\prod_{k=1}^{N}(\boldsymbol{x}-a_k)}{(\boldsymbol{x}-a_i)}$.)

(b) Existe um polinómio $\boldsymbol{p}(x) \in K[\boldsymbol{x}]$ de grau $\leq n-1$ tal que $p(a_k) = b_k$.

A fórmula que define $\boldsymbol{p}$ chama-se a *fórmula de interpolação de Lagrange*.

6. Prove que, se K é um corpo finito, então qualquer função de K em K é polinomial.

7. Seja K um subcorpo do corpo L, e suponha que L é um espaço vectorial de dimensão finita sobre K. Mostre que L é uma extensão algébrica de K. (SUGESTÃO: se a dimensão de L sobre K é n e $a \in L$, as potências a^k com $0 \leq k \leq n$ não podem ser linearmente independentes.)

3.5 Divisão de Polinómios

Nesta secção e na próxima estudamos em pormenor o anel dos polinómios $A[\boldsymbol{x}]$. Na base deste estudo está o algoritmo usual para a divisão de polinómios. Necessitamos pois de encontrar condições sobre o anel A para que este algoritmo seja aplicável. Em muitos casos, os resultados que obtemos são análogos a resultados que provámos no Capítulo 2 para os inteiros.

De acordo com o que vimos no Exemplo 3.4.7.3, passamos a adoptar a seguinte convenção: o polinómio $\boldsymbol{p}$ é representado pelo símbolo $p(\boldsymbol{x})$, e o valor do polinómio $\boldsymbol{p}$ no ponto a é representado por $p(a)$, em vez de $\boldsymbol{p}^*(a)$.

Definição 3.5.1. O polinómio $p(\boldsymbol{x}) \in A[\boldsymbol{x}]$ diz-se MÓNICO se $p_n = 1$, onde $\deg p(\boldsymbol{x}) = n$ e 1 é a identidade do anel A.

Exemplo 3.5.2.

O polinómio $5 + 3\boldsymbol{x} + 2\boldsymbol{x}^2 + \boldsymbol{x}^4 \in \mathbb{Z}[\boldsymbol{x}]$ *é mónico.*

Não provaremos resultados sobre divisibilidade para polinómios com coeficientes num anel com divisores de zero. Por este motivo, supomos nesta secção que $A = D$ é um *domínio integral*. Segue-se portanto da Proposição 3.3.10(b) que $D[\boldsymbol{x}]$ é igualmente um domínio integral.

Teorema 3.5.3 (Algoritmo de Divisão). *Se $p(\boldsymbol{x}), d(\boldsymbol{x}) \in D[\boldsymbol{x}]$ e $d(\boldsymbol{x})$ é mónico, existem polinómios únicos $q(\boldsymbol{x})$ e $r(\boldsymbol{x})$, com $\deg r(\boldsymbol{x}) < \deg d(\boldsymbol{x})$, tais que $p(\boldsymbol{x}) = q(\boldsymbol{x})d(\boldsymbol{x}) + r(\boldsymbol{x})$.*

Tal como no caso dos inteiros, os polinómios $q(\boldsymbol{x})$ e $r(\boldsymbol{x})$ dizem-se respectivamente QUOCIENTE e RESTO da divisão de $p(\boldsymbol{x})$ por $d(\boldsymbol{x})$. O caso em que $r(\boldsymbol{x}) = 0$ corresponde, claro está, ao caso em que $d(\boldsymbol{x})$ é divisor (ou factor) de $p(\boldsymbol{x})$. Recordemos que neste caso escrevemos $d(\boldsymbol{x})|p(\boldsymbol{x})$.

Demonstração do Teorema 3.5.3. Mostramos separadamente a existência e unicidade da divisão.

Existência: Tomamos $R = \{p(\boldsymbol{x}) - a(\boldsymbol{x})d(\boldsymbol{x}) : a(\boldsymbol{x}) \in D[\boldsymbol{x}]\}$. Temos dois casos, dependendo se 0 pertence ou não a R:

(a) Se $0 \in R$, *i.e.*, se existe $a_0(\boldsymbol{x}) \in D[\boldsymbol{x}]$ tal que $p(\boldsymbol{x}) - a_0(\boldsymbol{x})d(\boldsymbol{x}) = 0$, então tomamos $q(\boldsymbol{x}) = a_0(\boldsymbol{x})$ e $r(\boldsymbol{x}) = 0$;

(b) Se $0 \notin D[\boldsymbol{x}]$, o conjunto $G = \{\deg(p(\boldsymbol{x}) - a(\boldsymbol{x})d(\boldsymbol{x})) : a(\boldsymbol{x}) \in D[\boldsymbol{x}]\}$, formado pelos graus dos polinómios em R, é um subconjunto de $\mathbb{N}_0$, e tem consequentemente um mínimo m. Existe portanto um polinómio $a_0(\boldsymbol{x})$ tal que $\deg(p(\boldsymbol{x}) - a_0(\boldsymbol{x})d(\boldsymbol{x})) = m$. Tomamos $q(\boldsymbol{x}) = a_0(\boldsymbol{x})$ e $r(\boldsymbol{x}) = p(\boldsymbol{x}) - q(\boldsymbol{x})d(\boldsymbol{x})$.

No caso (a), é evidente que $p(\boldsymbol{x}) = q(\boldsymbol{x})d(\boldsymbol{x}) + r(\boldsymbol{x})$ e $\deg r(\boldsymbol{x}) < \deg d(\boldsymbol{x})$. No caso (b), notamos que $\deg r(\boldsymbol{x}) = m$, e $\deg r(\boldsymbol{x}) \leq \deg(p(\boldsymbol{x}) - a(\boldsymbol{x})d(\boldsymbol{x}))$, para qualquer $a(\boldsymbol{x}) \in D[\boldsymbol{x}]$. Dado que temos $p(\boldsymbol{x}) = q(\boldsymbol{x})d(\boldsymbol{x}) + r(\boldsymbol{x})$, resta-nos provar que $m = \deg r(\boldsymbol{x}) < \deg d(\boldsymbol{x})$, o que fazemos por redução ao absurdo. Sendo $n = \deg d(\boldsymbol{x}) \leq m$ e $k = m - n$, tomamos $r'(\boldsymbol{x}) = r(\boldsymbol{x}) - r_m\boldsymbol{x}^k d(\boldsymbol{x})$. Deve ser claro que $r'(\boldsymbol{x}) = p(\boldsymbol{x}) - (q(\boldsymbol{x}) + r_m\boldsymbol{x}^k)d(\boldsymbol{x}) \in R$. Por outro lado, como $d(\boldsymbol{x})$ é mónico, temos que $\deg r'(\boldsymbol{x}) < m = \deg r(\boldsymbol{x})$, o que é impossível. Concluímos que $m < n$, ou seja, $\deg r(\boldsymbol{x}) < \deg d(\boldsymbol{x})$.

Unicidade: Se $p(\boldsymbol{x}) = q(\boldsymbol{x})d(\boldsymbol{x}) + r(\boldsymbol{x}) = q'(\boldsymbol{x})d(\boldsymbol{x}) + r'(\boldsymbol{x})$, temos que

$$\big(q(\boldsymbol{x}) - q'(\boldsymbol{x})\big)\, d(\boldsymbol{x}) = r'(\boldsymbol{x}) - r(\boldsymbol{x}),$$

e concluímos que, quando $q(\boldsymbol{x}) \neq q'(\boldsymbol{x})$, então $\deg\left(r'(\boldsymbol{x}) - r(\boldsymbol{x})\right) \geq \deg d(\boldsymbol{x})$. Se supusermos que tanto $\deg r(\boldsymbol{x})$ como $\deg r'(\boldsymbol{x})$ são menores do que $\deg d(\boldsymbol{x})$, temos

$$\deg\big(r'(\boldsymbol{x}) - r(\boldsymbol{x})\big) \leq \max\{\deg r'(\boldsymbol{x}), \deg r(\boldsymbol{x})\} < \deg d(\boldsymbol{x}),$$

e portanto o caso $q(\boldsymbol{x}) \neq q'(\boldsymbol{x})$ é impossível, donde $q(\boldsymbol{x}) = q'(\boldsymbol{x})$ e também $r(\boldsymbol{x}) = r'(\boldsymbol{x})$. □

O argumento de existência pode ser esquematizado da seguinte forma. Para um polinómio $p(\boldsymbol{x}) = a_n\boldsymbol{x}^n + a_{n-1}\boldsymbol{x}^{n-1} + \cdots + a_0 \in K[\boldsymbol{x}]$ de grau n designamos por $p^{\text{top}}(\boldsymbol{x}) = a_n\boldsymbol{x}^n$ o termo de grau máximo. Então para dividir o polinómio $p(\boldsymbol{x})$ por um polinómio $d(\boldsymbol{x})$ procede-se por iteração:

- Começando com $q(\boldsymbol{x}) = 0$ e $r(\boldsymbol{x}) = p$, substituímos em cada passo

$$q(\boldsymbol{x}) \to q(\boldsymbol{x}) + \frac{r^{\text{top}}(\boldsymbol{x})}{d^{\text{top}}(\boldsymbol{x})}, \quad r(\boldsymbol{x}) \to r(\boldsymbol{x}) - \frac{r^{\text{top}}(\boldsymbol{x})}{d^{\text{top}}(\boldsymbol{x})} d(\boldsymbol{x}).$$

A iteração termina quando $\deg r(\boldsymbol{x}) < \deg d(\boldsymbol{x})$.

Exemplo 3.5.4.

Seja $D = \mathbb{Z}_5$. A divisão de $p(\boldsymbol{x}) = \boldsymbol{x}^4 + 2\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 4$ por $d(\boldsymbol{x}) = \boldsymbol{x}^2 + \boldsymbol{x} + 1$ resulta no quociente $q(\boldsymbol{x}) = \boldsymbol{x}^2 + \boldsymbol{x} + 1$, com resto $r(\boldsymbol{x}) = 4\boldsymbol{x} + 3$.

Supondo $a \in D$, o polinómio $d(\boldsymbol{x}) = (\boldsymbol{x} - a)$ é mónico, e de grau 1. Qualquer polinómio $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$ pode ser dividido por $(\boldsymbol{x} - a)$, e de acordo com o teorema anterior o resto dessa divisão é um polinómio *constante*. O próximo corolário, cuja demonstração fica como exercício, resume-se a observar que esse resto (identificado com o correspondente elemento de D) é o valor de $p(\boldsymbol{x})$ em a.

Corolário 3.5.5 (Teorema do Resto). *Se $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$ e $a \in D$, o resto da divisão de $p(\boldsymbol{x})$ por $(\boldsymbol{x} - a)$ é o polinómio constante $r(\boldsymbol{x}) = p(a)$. Em particular, $(\boldsymbol{x} - a) | p(\boldsymbol{x})$ se e só se a é raiz de $p(\boldsymbol{x})$.*

Exemplos 3.5.6.

1. *Considere-se o polinómio $p(\boldsymbol{x}) = \boldsymbol{x}^4 + 2\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 2$ em $\mathbb{Z}_5[\boldsymbol{x}]$. Como $p(1) = 4$, segue-se que o resto da divisão de $\boldsymbol{x}^4 + 2\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 2$ por $(\boldsymbol{x} - 1) = (\boldsymbol{x} + 4)$ é $r(\boldsymbol{x}) = 4$.*

2. *Supondo agora que $p(\boldsymbol{x}) = \boldsymbol{x}^4 + 2\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 2$ é um polinómio com coeficientes em $\mathbb{Z}_3$, temos $p(1) = 0$, e neste caso $(\boldsymbol{x} - 1) = (\boldsymbol{x} + 2)$ é um factor de $\boldsymbol{x}^4 + 2\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 2$.*

Outra das consequências do Algoritmo de Divisão (ou mais directamente do Corolário 3.5.5) é o resultado clássico sobre o número máximo de raízes de um polinómio não-nulo.

Proposição 3.5.7. *Se $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$ e $\deg p(\boldsymbol{x}) = n \geq 0$, então $p(\boldsymbol{x})$ tem no máximo n raízes em D.*

Demonstração. Argumentamos por indução no grau do polinómio $p(\boldsymbol{x})$.

Se $n = 0$, o polinómio $p(\boldsymbol{x})$ é constante e não-nulo. É portanto óbvio que não tem raízes.

Supondo a afirmação válida para um inteiro $n \geq 0$, suponha-se que $\deg p(\boldsymbol{x}) = n + 1$, e que a é raiz de $p(\boldsymbol{x})$ (se $p(\boldsymbol{x})$ não tem raízes, nada temos a provar!). De acordo com o teorema do resto, $p(\boldsymbol{x}) = q(\boldsymbol{x})(\boldsymbol{x} - a)$, onde é claro que $\deg q(\boldsymbol{x}) = n$. Podemos portanto concluir, da hipótese de indução,

que $q(\boldsymbol{x})$ tem no máximo n raízes. Por outro lado, se $b \in D$ é distinto de a, temos $p(b) = q(b)(b-a)$, e como D é um domínio integral, só é possível que $p(b) = 0$ quando $q(b) = 0$. Por outras palavras, as restantes raízes de $p(\boldsymbol{x})$ são necessariamente raízes de $q(\boldsymbol{x})$, e por isso $p(\boldsymbol{x})$ tem no máximo $n+1$ raízes. □

Se D é um domínio integral, os únicos polinómios $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$ *invertíveis* são os polinómios *constantes* $p(\boldsymbol{x}) = a$, com $a \in D$ *invertível*. Estes polinómios podem ser sempre utilizados para obter factorizações *triviais*, ou óbvias, de qualquer outro polinómio $p(\boldsymbol{x})$, porque se $a(\boldsymbol{x})b(\boldsymbol{x}) = 1$ então naturalmente $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x})p(\boldsymbol{x})$. Por esta razão, se $q(\boldsymbol{x})|p(\boldsymbol{x})$, é comum dizer que $q(\boldsymbol{x})$ é um FACTOR PRÓPRIO de $p(\boldsymbol{x})$ se e só se $p(\boldsymbol{x}) = a(\boldsymbol{x})q(\boldsymbol{x})$, onde nem $a(\boldsymbol{x})$ nem $q(\boldsymbol{x})$ são invertíveis. Nesta terminologia, uma factorização é NÃO-TRIVIAL se e só se inclui pelo menos um factor próprio. Nos termos da próxima definição, que deve ser cuidadosamente comparada com a definição de *números primos* apresentada no Capítulo 2, os *polinómios irredutíveis* são aqueles que não são invertíveis, e têm *apenas* factorizações triviais, ou seja, são os polinómios não invertíveis que não têm factores *próprios*. Repare-se ainda que a restrição a polinómios não invertíveis é em tudo análoga à exclusão do natural 1 do conjunto dos números primos.

Definição 3.5.8. Um polinómio $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$ diz-se IRREDUTÍVEL EM $D[\boldsymbol{x}]$ quando não tem factores próprios (em $D[\boldsymbol{x}]$), e não é invertível (em $D[\boldsymbol{x}]$). Em particular, se $p(\boldsymbol{x})$ é irredutível em $D[\boldsymbol{x}]$ e $q_1(\boldsymbol{x}), q_2(\boldsymbol{x}) \in D[\boldsymbol{x}]$

$$p(\boldsymbol{x}) = q_1(\boldsymbol{x})q_2(\boldsymbol{x}) \quad \Longrightarrow \quad q_1(\boldsymbol{x}) \text{ ou } q_2(\boldsymbol{x}) \text{ é invertível em } D[\boldsymbol{x}].$$

Caso contrário, $p(\boldsymbol{x})$ diz-se REDUTÍVEL EM $D[\boldsymbol{x}]$.

Exemplos 3.5.9.

1. *$p(\boldsymbol{x}) = \boldsymbol{x} - a$ é irredutível, qualquer que seja o domínio D em questão.*

2. *Se $D = \mathbb{Z}$, $p(\boldsymbol{x}) = 2\boldsymbol{x} - 3$ é irredutível (verifique!), mas $q(\boldsymbol{x}) = 2\boldsymbol{x} + 6$ é redutível, porque $2\boldsymbol{x} + 6 = 2(\boldsymbol{x} + 3)$, e 2 e $\boldsymbol{x} + 3$ não são invertíveis em $\mathbb{Z}[\boldsymbol{x}]$.*

3. *Se $\deg p(\boldsymbol{x}) \geq 2$ e $p(\boldsymbol{x})$ tem pelo menos uma raiz em D, segue-se, do Teorema do Resto, que $p(\boldsymbol{x})$ é necessariamente redutível em $D[\boldsymbol{x}]$.*

4. *Se $p(\boldsymbol{x})$ é mónico e tem grau 2 ou 3, então $p(\boldsymbol{x})$ é redutível em $D[\boldsymbol{x}]$ se e só se tem pelo menos uma raíz em D (porquê?).*

5. *É possível que $p(\boldsymbol{x})$ não tenha raízes em D, e seja redutível em $D[\boldsymbol{x}]$. É o caso de $\boldsymbol{x}^4 + 2\boldsymbol{x}^2 + 1$, que é redutível em $\mathbb{Z}[\boldsymbol{x}]$, porque $\boldsymbol{x}^4 + 2\boldsymbol{x}^2 + 1 = (\boldsymbol{x}^2 + 1)^2$, e que claramente não tem raízes em $\mathbb{Z}$.*

6. *Deve ser conhecido da Álgebra elementar que os únicos polinómios irredutíveis em $\mathbb{R}$ são os polinómios de grau 1 e os polinómios quadráticos $p(\boldsymbol{x}) = a\boldsymbol{x}^2 + b\boldsymbol{x} + c$, com* DISCRIMINANTE *$\Delta = b^2 - 4ac$ negativo. Veremos adiante que este facto é uma consequência do* Teorema Fundamental da Álgebra.

7. *A irredutibilidade de um polinómio depende fortemente do domínio D considerado. Todos sabemos que o polinómio $\boldsymbol{x}^2+1$ é irredutível em $\mathbb{R}[\boldsymbol{x}]$, mas redutível em $\mathbb{C}[\boldsymbol{x}] \supset \mathbb{R}[\boldsymbol{x}]$. Por outro lado, o polinómio $p(\boldsymbol{x}) = 2\boldsymbol{x}+6$ é redutível em $\mathbb{Z}[\boldsymbol{x}]$, mas irredutível em $\mathbb{Q}[\boldsymbol{x}] \supset \mathbb{Z}[\boldsymbol{x}]$.*

É possível em certos casos descrever todos os polinómios irredutíveis em $D[\boldsymbol{x}]$, como ocorre no Exemplo 6 acima. Noutros casos, é praticamente impossível fazê-lo, e os próximos resultados sugerem a complexidade presente nos anéis $\mathbb{Z}[\boldsymbol{x}]$ e $\mathbb{Q}[\boldsymbol{x}]$. Dado $p(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$, $p(\boldsymbol{x}) = a_0 + a_1\boldsymbol{x} + \cdots + a_n\boldsymbol{x}^n$, dizemos que $c(p) = \operatorname{mdc}(a_0, a_1, \ldots, a_n)$ é o CONTEÚDO de $p(\boldsymbol{x})$. Dizemos ainda que $p(\boldsymbol{x})$ é PRIMITIVO se os seus coeficientes são primos entre si, *i.e.*, se $c(p) = 1$. É claro que $p(\boldsymbol{x})$ é primitivo se e só se não tem factorizações do tipo $p(\boldsymbol{x}) = kq(\boldsymbol{x})$, $k \in \mathbb{Z}$, $k \neq \pm 1$, que são triviais em $\mathbb{Q}[\boldsymbol{x}]$.

Lema 3.5.10. *Se $p(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$, e $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x})$ com $a(\boldsymbol{x}), b(\boldsymbol{x}) \in \mathbb{Q}[\boldsymbol{x}]$, então existem polinómios $a'(\boldsymbol{x}), b'(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$, e $k \in \mathbb{Q}$, tais que*

$$p(\boldsymbol{x}) = a'(\boldsymbol{x})b'(\boldsymbol{x}),\ a(\boldsymbol{x}) = ka'(\boldsymbol{x}),\ \text{e}\ b(\boldsymbol{x}) = k^{-1}b'(\boldsymbol{x}).$$

Demonstração. É evidente que existem inteiros n, m tais que $\tilde{a}(\boldsymbol{x}) = na(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ e $\tilde{b}(\boldsymbol{x}) = mb(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$, e temos $nmp(\boldsymbol{x}) = \tilde{a}(\boldsymbol{x})\tilde{b}(\boldsymbol{x})$. Sendo q um qualquer factor primo de nm, recordamos a generalização do Lema de Euclides dada no Exercício 11 da Secção (3.3): $q|\tilde{a}(\boldsymbol{x})\tilde{b}(\boldsymbol{x}) \Longrightarrow q|\tilde{a}(\boldsymbol{x})$ ou $q|\tilde{b}(\boldsymbol{x})$.

Podemos assim dividir a igualdade $nmp(\boldsymbol{x}) = \tilde{a}(\boldsymbol{x})\tilde{b}(\boldsymbol{x})$ por q, obtendo ainda do lado direito dois polinómios em $\mathbb{Z}[\boldsymbol{x}]$. Repetindo esta operação para *todos* os factores primos de nm, obtemos uma igualdade da forma $p(\boldsymbol{x}) = a'(\boldsymbol{x})b'(\boldsymbol{x})$, onde $a'(\boldsymbol{x}), b'(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$, $\tilde{a}(\boldsymbol{x}) = sa'(\boldsymbol{x})$ e $\tilde{b}(\boldsymbol{x}) = tb'(\boldsymbol{x})$, com $s, t \in \mathbb{Z}$. Concluímos que $a(\boldsymbol{x}) = \frac{s}{n}a'(\boldsymbol{x})$, $b(\boldsymbol{x}) = \frac{t}{m}b'(\boldsymbol{x})$, e $\frac{s}{n}\frac{t}{m} = 1$. □

Lema 3.5.11 (Gauss). *Se $p(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ não é constante, então $p(\boldsymbol{x})$ é irredutível em $\mathbb{Z}[\boldsymbol{x}]$ se e só se é é primitivo em $\mathbb{Z}[\boldsymbol{x}]$ e irredutível em $\mathbb{Q}[\boldsymbol{x}]$.*

Demonstração. Supomos primeiro que $p(\boldsymbol{x})$ é redutível e primitivo em $\mathbb{Z}[\boldsymbol{x}]$, e mostramos que $p(\boldsymbol{x})$ é redutível em $\mathbb{Q}[\boldsymbol{x}]$. Neste caso $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x})$, com $a(\boldsymbol{x}), b(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$. Notamos que se algum dos polinómios $a(\boldsymbol{x})$ ou $b(\boldsymbol{x})$ é *constante* então é invertível, *i.e.*, é ± 1, porque $p(\boldsymbol{x})$ é primitivo. Concluímos que $a(\boldsymbol{x})$ e $b(\boldsymbol{x})$ não são constantes, portanto não são invertíveis em $\mathbb{Q}[\boldsymbol{x}]$, e a factorização $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x})$ não é trivial em $\mathbb{Q}[\boldsymbol{x}]$, ou seja, $p(\boldsymbol{x})$ é igualmente redutível em $\mathbb{Q}[\boldsymbol{x}]$.

Se $p(\boldsymbol{x})$ não é primitivo é evidente que é redutível em $\mathbb{Z}[\boldsymbol{x}]$. Resta-nos por isso provar que se $p(\boldsymbol{x})$ é redutível em $\mathbb{Q}[\boldsymbol{x}]$ então é também redutível em $\mathbb{Z}[\boldsymbol{x}]$. Neste caso $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x})$, onde $a(\boldsymbol{x}), b(\boldsymbol{x}) \in \mathbb{Q}[\boldsymbol{x}]$ *não são constantes*. De acordo com o lema (3.5.10), existem polinómios $a'(\boldsymbol{x}), b'(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ tais que $p(\boldsymbol{x}) = a'(\boldsymbol{x})b'(\boldsymbol{x})$, e $a'(\boldsymbol{x}), b'(\boldsymbol{x})$ não são constantes. Portanto $p(\boldsymbol{x})$ é redutível em $\mathbb{Z}[\boldsymbol{x}]$. □

O próximo teorema e o lema anterior permitem-nos obter facilmente exemplos de polinómios irredutíveis em $\mathbb{Z}[\boldsymbol{x}]$ e $\mathbb{Q}[\boldsymbol{x}]$.

Teorema 3.5.12 (Critério de Eisenstein). *Seja $a(\boldsymbol{x}) = a_0 + a_1\boldsymbol{x} + \cdots + a_n\boldsymbol{x}^n \in \mathbb{Z}[\boldsymbol{x}]$ um polinómio de grau n. Se existe um primo $p \in \mathbb{Z}$ tal que $a_k \equiv 0 \pmod{p}$ para $0 \leq k < n$, $a_n \not\equiv 0 \pmod{p}$ e $a_0 \not\equiv 0 \pmod{p^2}$ então $a(\boldsymbol{x})$ é irredutível em $\mathbb{Q}[\boldsymbol{x}]$.*

Demonstração. Supomos que temos em $\mathbb{Q}[\boldsymbol{x}]$

$$a(\boldsymbol{x}) = b(\boldsymbol{x})c(\boldsymbol{x}) = (b_0 + b_1\boldsymbol{x} + \dots)(c_0 + c_1\boldsymbol{x} + \dots).$$

De acordo com o lema (3.5.10), podemos supor sem perda de generalidade que $b(\boldsymbol{x}), c(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$. Se $b_0 \equiv c_0 \equiv 0 \pmod{p}$, é claro que $a_0 = b_0c_0 \equiv 0 \pmod{p^2}$, contradizendo a hipótese $a_0 \not\equiv 0 \pmod{p^2}$. Supomos portanto (ainda sem perda de generalidade) que $c_0 \not\equiv 0 \pmod{p}$.

É evidente que se $p|b(\boldsymbol{x})$ então $p|a(\boldsymbol{x})$, o que é impossível, porque $a_n \not\equiv 0 \pmod{p}$. Concluímos que o conjunto $\{k \geq 0 : b_k \not\equiv 0 \pmod{p}\}$ não é vazio, e designamos por m o seu mínimo.

Finalmente, notamos que

$$a_m = \sum_{i=0}^{m} b_i c_{m-i} \equiv b_m c_0 \not\equiv 0 \pmod{p},$$

donde $m = n$, já que a_n é o único coeficiente de $a(\boldsymbol{x})$ não divisível por p.

Assim, $\deg b(\boldsymbol{x}) \geq \deg a(\boldsymbol{x})$, e como $a(\boldsymbol{x}) = b(\boldsymbol{x})c(\boldsymbol{x})$, temos $\deg b(\boldsymbol{x}) = \deg a(\boldsymbol{x})$, e $c(\boldsymbol{x})$ é *constante*. Logo $a(\boldsymbol{x})$ é irredutível em $\mathbb{Q}[\boldsymbol{x}]$. □

Exemplos 3.5.13.

1. *Se $p \in \mathbb{Z}$ é primo, $q(\boldsymbol{x}) = \boldsymbol{x}^n - p$ é irredutível em $\mathbb{Z}[\boldsymbol{x}]$ e em $\mathbb{Q}[\boldsymbol{x}]$.*

2. *O Critério de Eisenstein não é aplicável ao polinómio $q(\boldsymbol{x}) = \boldsymbol{x}^6 + \boldsymbol{x}^3 + 1$. No entanto,*

$$\begin{aligned} q(\boldsymbol{x}+1) &= (\boldsymbol{x}+1)^6 + (\boldsymbol{x}+1)^3 + 1 \\ &= \boldsymbol{x}^6 + 6\boldsymbol{x}^5 + 15\boldsymbol{x}^4 + 21\boldsymbol{x}^3 + 18\boldsymbol{x}^2 + 9\boldsymbol{x} + 3, \end{aligned}$$

logo o polinómio $q(\boldsymbol{x}+1)$ é irredutível em $\mathbb{Q}[\boldsymbol{x}]$. Concluímos que $q(\boldsymbol{x})$ é irredutível em $\mathbb{Q}[\boldsymbol{x}]$.

Os exemplos e referências anteriores permitem-nos observar o seguinte:

- Em qualquer anel de polinómios, os polinómios $\boldsymbol{x} - a$ são irredutíveis.
- Existem anéis de polinómios que contêm polinómios irredutíveis de grau arbitrariamente grande.

- Existem anéis de polinómios que contêm polinómios irredutíveis apenas até determinado grau superior a 1. (Em $\mathbb{R}$, os polinómios irredutíveis têm grau 1 ou 2.)

Resta-nos verificar que existem efectivamente corpos onde os *únicos* polinómios irredutíveis são da forma $\boldsymbol{x} - a$. Neste caso, e como veremos nos exercícios, qualquer polinómio de grau > 1 tem necessariamente raízes, razão pela qual introduzimos:

Definição 3.5.14. O corpo K diz-se *algebricamente fechado* se e só se qualquer polinómio não-constante $p(\boldsymbol{x}) \in K[\boldsymbol{x}]$ tem pelo menos uma raiz em K.

Não demonstramos o próximo teorema, que naturalmente utilizaremos apenas para exemplos e exercícios. O leitor poderá encontrar a sua demonstração num texto de Análise Complexa. Deixamos como exercício a determinação dos polinómios irredutíveis em $\mathbb{R}$ utilizando este resultado.

Teorema 3.5.15 (Teorema Fundamental da Álgebra). *O corpo dos complexos é algebricamente fechado, ou seja, qualquer polinómio complexo não-constante tem pelo menos uma raiz complexa.*

Exercícios.

1. Se $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$, $p(\boldsymbol{x}) \neq 0$, e $a \in D$ é raiz de $p(\boldsymbol{x})$, o maior natural m tal que $p(\boldsymbol{x})$ é múltiplo de $(\boldsymbol{x} - a)^m$ diz-se a MULTIPLICIDADE da raiz a. Prove que a soma das multiplicidades das raízes de $p(\boldsymbol{x})$ é $\leq \deg p(\boldsymbol{x})$.

2. Mostre que $p(\boldsymbol{x}) \in A[\boldsymbol{x}]$ pode ter mais do que $\deg p(\boldsymbol{x})$ raízes, se A tem divisores de zero.

3. Mostre que $\boldsymbol{x}^2 + 1$ é irredutível em $\mathbb{Z}_3[\boldsymbol{x}]$.

4. Determine todos os polinómios $p(\boldsymbol{x}) \in \mathbb{Z}_3[\boldsymbol{x}]$ irredutíveis com $\deg p(\boldsymbol{x}) \leq 2$.

5. Quantos polinómios irredutíveis de grau 5 existem em $\mathbb{Z}_5[\boldsymbol{x}]$?
(SUGESTÃO: conte os polinómios redutíveis e irredutíveis de graus ≤ 5.)

6. Mostre que as seguintes afirmações são equivalentes:
   (a) O corpo K é algebricamente fechado.
   (b) Qualquer polinómio em $K[\boldsymbol{x}]$ de grau ≥ 1 é um produto de polinómios do grau 1.

7. Suponha que o corpo K é algebricamente fechado, e mostre que, se $p(\boldsymbol{x}) \in K[\boldsymbol{x}]$ e $\deg p(\boldsymbol{x}) = n \geq 1$, então a soma das multiplicidades das raízes de $p(\boldsymbol{x})$ é exactamente n.

8. Suponha que $p(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ e prove o seguinte (a partir do Teorema Fundamental da Álgebra):

(a) Se $c \in \mathbb{C}$ é raíz de $p(\boldsymbol{x})$, o complexo conjugado de c é também raíz de $p(\boldsymbol{x})$.
(b) Se $p(\boldsymbol{x})$ é irredutível em $\mathbb{R}[\boldsymbol{x}]$ e $\deg p(\boldsymbol{x}) > 1$, então $p(\boldsymbol{x}) = a\boldsymbol{x}^2 + b\boldsymbol{x} + c$ e $b^2 - 4ac < 0$.

9. Mostre que, se K é um corpo algebricamente fechado, e D é um domínio integral e uma extensão algébrica de K, então $K = D$.[9]

10. Sendo $p(\boldsymbol{x}) = a_0 + a_1\boldsymbol{x} + \cdots + \alpha_n x^n \in \mathbb{Z}[\boldsymbol{x}]$, e $c(p) = \mathrm{mdc}(a_o, a_1, \ldots, \alpha_n)$, mostre que:

(a) $p(\boldsymbol{x}) = c(p)q(\boldsymbol{x})$ onde $q(\boldsymbol{x})$ é primitivo,
(b) Se $p(\boldsymbol{x})$ e $q(\boldsymbol{x})$ são primitivos então $p(\boldsymbol{x})q(\boldsymbol{x})$ é primitivo.

3.6 Os Ideais de $K[\boldsymbol{x}]$

Como vimos no Capítulo 2, a estrutura dos ideais de $\mathbb{Z}$ é particularmente simples, um facto que está na base do Algoritmo de Euclides para o cálculo do máximo divisor comum e menor múltiplo comum de dois inteiros. Se D é um domínio integral, a estrutura dos ideais de $D[\boldsymbol{x}]$ pode ser bastante complexa (basta pensar nos ideais de $\mathbb{Z}[\boldsymbol{x}]$), e não existem em geral análogos do Algoritmo de Euclides. No entanto, se $D = K$ é um *corpo*, então a estrutura dos ideais de $K[\boldsymbol{x}]$ é simples de descrever.

Começamos por referir que o Algoritmo da Divisão apresentado em (3.5.3) pode ser reforçado como se segue, deixando a respectiva verificação como exercício.

Teorema 3.6.1. *Se $p(\boldsymbol{x}), d(\boldsymbol{x}) \in K[\boldsymbol{x}]$ e $d(\boldsymbol{x}) \neq 0$, existem polinómios únicos $q(\boldsymbol{x})$ e $r(\boldsymbol{x})$, tais que $p(\boldsymbol{x}) = q(\boldsymbol{x})d(\boldsymbol{x}) + r(\boldsymbol{x})$ e $\deg r(\boldsymbol{x}) < \deg d(\boldsymbol{x})$.*

Este resultado, muito semelhante ao que provámos no Capítulo 2 para os inteiros, pode ser facilmente explorado para estabelecer várias analogias entre os anéis $K[\boldsymbol{x}]$ e $\mathbb{Z}$, muito em especial a seguinte.

Teorema 3.6.2. *Qualquer ideal em $K[\boldsymbol{x}]$ é principal.*

Demonstração. Supomos que $I \subset K[\boldsymbol{x}]$ é um ideal. Se $I = \{0\}$, então $I = \langle 0 \rangle$ é um ideal principal. Podemos pois assumir que $I \neq \{0\}$ e portanto existe um polinómio não-nulo $p(\boldsymbol{x}) \in I$.

Considere-se o conjunto $N = \{n \in \mathbb{N}_0 : \exists p(\boldsymbol{x}) \in I,\ n = \deg p(\boldsymbol{x})\}$. O conjunto N é não-vazio, e tem mínimo. Seja $m(\boldsymbol{x}) \in I$ tal que $\deg m(\boldsymbol{x}) = \min N$, donde

$$r(\boldsymbol{x}) \in I \text{ e } r(\boldsymbol{x}) \neq 0 \implies \deg m(\boldsymbol{x}) < \deg r(\boldsymbol{x}). \tag{3.6.1}$$

[9] Em particular, e de acordo com o Teorema Fundamental da Álgebra, não existe nenhum corpo L que seja uma extensão algébrica de $\mathbb{C}$, o que é a resposta completa ao problema de Hamilton discutido no Capítulo 1.

Como $m(\boldsymbol{x}) \in I$, é óbvio que $\langle m(\boldsymbol{x})\rangle \subset I$. Por outro lado, se $p(\boldsymbol{x}) \in I$ segue-se do algoritmo de divisão que $p(\boldsymbol{x}) = m(\boldsymbol{x})d(\boldsymbol{x}) + r(\boldsymbol{x})$, onde $\deg r(\boldsymbol{x}) < \deg m(\boldsymbol{x})$. Dado que I é um ideal, vemos que

$$r(\boldsymbol{x}) = p(\boldsymbol{x}) - m(\boldsymbol{x})d(\boldsymbol{x}) \in I,$$

e concluímos, de (3.6.1), que $r(\boldsymbol{x}) = 0$ (caso contrário teríamos $\deg m(\boldsymbol{x}) \leq \deg r(\boldsymbol{x})$, uma contradição). Portanto, $p(\boldsymbol{x}) \in \langle m(\boldsymbol{x})\rangle$, e $I = \langle m(\boldsymbol{x})\rangle$. □

Recorde-se que no Capítulo 2 explorámos o correspondente resultado para o anel dos inteiros, onde introduzimos o Algoritmo de Euclides para o cálculo do máximo divisor comum e do menor múltiplo comum de quaisquer dois inteiros. No que segue, seguimos de muito perto essas ideias, agora aplicadas no anel $K[\boldsymbol{x}]$.

A demonstração do seguinte resultado fica como exercício.

Proposição 3.6.3. *Sejam $I = \langle p(\boldsymbol{x})\rangle$ e $J = \langle q(\boldsymbol{x})\rangle$ ideais em $K[\boldsymbol{x}]$. Então:*

(a) $I \subset J$ se e só se $q(\boldsymbol{x})|p(\boldsymbol{x})$;

(b) I é máximo se e só se $p(\boldsymbol{x})$ é irredutível;

(c) se $I = J$ e $p(\boldsymbol{x})$ e $q(\boldsymbol{x})$ são mónicos ou nulos, então $p(\boldsymbol{x}) = q(\boldsymbol{x})$.

Se $p(\boldsymbol{x}), q(\boldsymbol{x}) \in K[\boldsymbol{x}]$, então $I = \langle p(\boldsymbol{x}), q(\boldsymbol{x})\rangle$ é um ideal em $K[\boldsymbol{x}]$, dado por $I = \{a(\boldsymbol{x})p(\boldsymbol{x}) + b(\boldsymbol{x})q(\boldsymbol{x}) : a(\boldsymbol{x}), b(\boldsymbol{x}) \in K[\boldsymbol{x}]\}$. Este ideal é principal, de acordo com o Teorema 3.6.2. Existe portanto um polinómio $d(\boldsymbol{x}) \in K[\boldsymbol{x}]$ tal que $\langle d(\boldsymbol{x})\rangle = \langle p(\boldsymbol{x}), q(\boldsymbol{x})\rangle$, e é fácil verificar que:

- $d(\boldsymbol{x})|p(\boldsymbol{x})$ e $d(\boldsymbol{x})|q(\boldsymbol{x})$;
- existem polinómios $a(\boldsymbol{x})$ e $b(\boldsymbol{x})$ tais que $d(\boldsymbol{x}) = a(\boldsymbol{x})p(\boldsymbol{x}) + b(\boldsymbol{x})q(\boldsymbol{x})$;
- se $c(\boldsymbol{x})|p(\boldsymbol{x})$ e $c(\boldsymbol{x})|q(\boldsymbol{x})$, então $c(\boldsymbol{x})|d(\boldsymbol{x})$.

Por palavras, $d(\boldsymbol{x})$ é um *divisor comum* de $p(\boldsymbol{x})$ e $q(\boldsymbol{x})$, e é *múltiplo* de qualquer outro divisor comum destes dois polinómios.

Analogamente, $\langle p(\boldsymbol{x})\rangle \cap \langle q(\boldsymbol{x})\rangle$ é um ideal principal, logo existe $m(\boldsymbol{x}) \in K[\boldsymbol{x}]$ tal que $\langle m(\boldsymbol{x})\rangle = \langle p(\boldsymbol{x})\rangle \cap \langle q(\boldsymbol{x})\rangle$. Temos neste caso que:

- $p(\boldsymbol{x})|m(\boldsymbol{x})$ e $q(\boldsymbol{x})|m(\boldsymbol{x})$;
- se $p(\boldsymbol{x})|n(\boldsymbol{x})$ e $q(\boldsymbol{x})|n(\boldsymbol{x})$, então $m(\boldsymbol{x})|n(\boldsymbol{x})$.

Portanto, $m(\boldsymbol{x})$ é *múltiplo comum* de $p(\boldsymbol{x})$ e $q(\boldsymbol{x})$, e é *divisor* de qualquer outro polinómio que seja múltiplo comum destes dois polinómios.

Como, de acordo com a Proposição 3.6.3 (c), se $p(\boldsymbol{x})$ e $q(\boldsymbol{x})$ são polinómios mónicos ou nulos e $\langle p(\boldsymbol{x})\rangle = \langle q(\boldsymbol{x})\rangle$, então $p(\boldsymbol{x}) = q(\boldsymbol{x})$, podemos introduzir

Definição 3.6.4. Sejam $p(\boldsymbol{x}), q(\boldsymbol{x}) \in K[\boldsymbol{x}]$.

(i) Se $\langle d(\boldsymbol{x})\rangle = \langle p(\boldsymbol{x}), q(\boldsymbol{x})\rangle$ então $d(\boldsymbol{x})$ diz-se MÁXIMO DIVISOR COMUM de $p(\boldsymbol{x})$ e $q(\boldsymbol{x})$, abreviadamente $d(\boldsymbol{x}) = \mathrm{mdc}(p(\boldsymbol{x}), q(\boldsymbol{x}))$, desde que $d(\boldsymbol{x})$ seja mónico ou nulo.

(ii) Se $\langle m(\boldsymbol{x})\rangle = \langle p(\boldsymbol{x})\rangle \cap \langle q(\boldsymbol{x})\rangle$ então $m(\boldsymbol{x})$ diz-se MÍNIMO MÚLTIPLO COMUM de $p(\boldsymbol{x})$ e $q(\boldsymbol{x})$, abreviadamente $m(\boldsymbol{x}) = \mathrm{mmc}(p(\boldsymbol{x}), q(\boldsymbol{x}))$, desde que $m(\boldsymbol{x})$ seja mónico ou nulo.

Ainda, tal como para os inteiros, temos

$$p(\boldsymbol{x}) = q(\boldsymbol{x})a(\boldsymbol{x}) + r(\boldsymbol{x}) \quad \Longrightarrow \quad \langle p(\boldsymbol{x}), q(\boldsymbol{x})\rangle = \langle q(\boldsymbol{x}), r(\boldsymbol{x})\rangle,$$

e o Algoritmo de Euclides mantém a sua validade. Ilustramo-lo com um exemplo em $\mathbb{Z}_5[\boldsymbol{x}]$.

Exemplo 3.6.5.

Para calcular o máximo divisor comum de $p(\boldsymbol{x}) = \boldsymbol{x}^4 + \boldsymbol{x}^3 + 2\boldsymbol{x}^2 + \boldsymbol{x} + 1$ *e* $q(\boldsymbol{x}) = \boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 3$ *em* $\mathbb{Z}_5[\boldsymbol{x}]$*, procedemos como se segue: Primeiro dividimos* $p(\boldsymbol{x})$ *por* $q(\boldsymbol{x})$*, obtendo*

$$\boldsymbol{x}^4 + \boldsymbol{x}^3 + 2\boldsymbol{x}^2 + \boldsymbol{x} + 1 = (\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 3)(\boldsymbol{x} + 3) + 2\boldsymbol{x}^2 + 2,$$

donde

$$\langle \boldsymbol{x}^4 + \boldsymbol{x}^3 + 2\boldsymbol{x}^2 + \boldsymbol{x} + 1, \boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 3\rangle = \langle \boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 3, 2\boldsymbol{x}^2 + 2\rangle.$$

De seguida, dividimos $\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 3$ *por* $2\boldsymbol{x}^2 + 2$*, obtendo*

$$\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 3 = (2\boldsymbol{x}^2 + 2)(3\boldsymbol{x} + 4).$$

Assim, vemos que

$$\langle \boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 3, 2\boldsymbol{x}^2 + 2\rangle = \langle 2\boldsymbol{x}^2 + 2\rangle = \langle \boldsymbol{x}^2 + 1\rangle.$$

Concluímos pois que

$$\mathrm{mdc}(\boldsymbol{x}^4 + \boldsymbol{x}^3 + 2\boldsymbol{x}^2 + \boldsymbol{x} + 1, \boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 3) = \boldsymbol{x}^2 + 1.$$

Exactamente como para os inteiros, podemos provar o seguinte resultado:

Lema 3.6.6. *Se* $p(\boldsymbol{x}), q(\boldsymbol{x}) \in K[\boldsymbol{x}]$ *são polinómios mónicos, temos*

$$\mathrm{mdc}(p(\boldsymbol{x}), q(\boldsymbol{x}))\,\mathrm{mmc}(p(\boldsymbol{x}), q(\boldsymbol{x})) = p(\boldsymbol{x})q(\boldsymbol{x}).$$

Exemplo 3.6.7.

Vimos acima que o máximo divisor comum de $p(\boldsymbol{x}) = \boldsymbol{x}^4 + \boldsymbol{x}^3 + 2\boldsymbol{x}^2 + \boldsymbol{x} + 1$ e $q(\boldsymbol{x}) = \boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 3$ em $\mathbb{Z}_5[\boldsymbol{x}]$ é $d(\boldsymbol{x}) = \boldsymbol{x}^2 + 1$, donde concluímos que o mínimo múltiplo comum destes polinómios é $m(\boldsymbol{x})$ dado por

$$\begin{aligned} m(\boldsymbol{x}) &= \frac{(\boldsymbol{x}^4 + \boldsymbol{x}^3 + 2\boldsymbol{x}^2 + \boldsymbol{x} + 1)(\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 3)}{\boldsymbol{x}^2 + 1} \\ &= \boldsymbol{x}^5 + 4\boldsymbol{x}^4 + 2\boldsymbol{x}^2 + 4\boldsymbol{x} + 3. \end{aligned}$$

Exercícios.

1. Prove o teorema 3.6.1.

2. Prove a Proposição 3.6.3.

3. Sejam $p(\boldsymbol{x}), q(\boldsymbol{x}) \in K[\boldsymbol{x}]$. Mostre que $I = \langle p(\boldsymbol{x}), q(\boldsymbol{x})\rangle = \{a(\boldsymbol{x})p(\boldsymbol{x}) + b(\boldsymbol{x})q(\boldsymbol{x}) : a(\boldsymbol{x}), b(\boldsymbol{x}) \in K[\boldsymbol{x}]\}$

4. Sejam $p(\boldsymbol{x}), q(\boldsymbol{x}) \in K[\boldsymbol{x}]$. Verifique que, se $\langle d(\boldsymbol{x})\rangle = \langle p(\boldsymbol{x}), q(\boldsymbol{x})\rangle$, então:
   (a) Existem $a(\boldsymbol{x}), b(\boldsymbol{x}) \in K[\boldsymbol{x}]$ tal que $d(\boldsymbol{x}) = a(\boldsymbol{x})p(\boldsymbol{x}) + b(\boldsymbol{x})q(\boldsymbol{x})$.
   (b) $d(\boldsymbol{x})|p(\boldsymbol{x})$ e $d(\boldsymbol{x})|q(\boldsymbol{x})$.
   (c) Se $c(\boldsymbol{x})|p(\boldsymbol{x})$ e $c(\boldsymbol{x})|q(\boldsymbol{x})$, então $c(\boldsymbol{x})|d(\boldsymbol{x})$, e portanto $\deg c(\boldsymbol{x}) \leq \deg d(\boldsymbol{x})$.

5. Prove a seguinte generalização do Lema de Euclides: se $p(\boldsymbol{x}), q_1(\boldsymbol{x}), q_2(\boldsymbol{x}) \in K[\boldsymbol{x}]$, $p(\boldsymbol{x})$ é irredutível e $p(\boldsymbol{x})|q_1(\boldsymbol{x})q_2(\boldsymbol{x})$, então $p(\boldsymbol{x})|q_1(\boldsymbol{x})$ ou $p(\boldsymbol{x})|q_2(\boldsymbol{x})$.

6. Se $p(\boldsymbol{x}), q(\boldsymbol{x}) \in K[\boldsymbol{x}]$, prove que

$$p(\boldsymbol{x}) = q(\boldsymbol{x})a(\boldsymbol{x}) + r(\boldsymbol{x}) \quad \Longrightarrow \quad \langle p(\boldsymbol{x}), q(\boldsymbol{x})\rangle = \langle q(\boldsymbol{x}), r(\boldsymbol{x})\rangle.$$

7. Sendo $d(\boldsymbol{x})$ o máximo divisor comum de $\boldsymbol{x}^4+\boldsymbol{x}^3+2\boldsymbol{x}^2+\boldsymbol{x}+1$ e $\boldsymbol{x}^3+3\boldsymbol{x}^2+\boldsymbol{x}+3$ em $\mathbb{Z}_5[\boldsymbol{x}]$, determine $a(\boldsymbol{x})$ e $b(\boldsymbol{x})$ em $\mathbb{Z}_5[\boldsymbol{x}]$ tais que

$$d(\boldsymbol{x}) = a(\boldsymbol{x})(\boldsymbol{x}^4 + \boldsymbol{x}^3 + 2\boldsymbol{x}^2 + \boldsymbol{x} + 1) + b(\boldsymbol{x})(\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 3).$$

8. Sejam $p(\boldsymbol{x}), q(\boldsymbol{x}) \in K[\boldsymbol{x}]$, $d(\boldsymbol{x}) = \operatorname{mdc}(p(\boldsymbol{x}), q(\boldsymbol{x}))$ e $m(\boldsymbol{x}) = \operatorname{mmc}(p(\boldsymbol{x}), q(\boldsymbol{x}))$.
   (a) Mostre que, se $p(\boldsymbol{x})|r(\boldsymbol{x})$ e $q(\boldsymbol{x})|r(\boldsymbol{x})$, então $p(\boldsymbol{x})q(\boldsymbol{x})|r(\boldsymbol{x})d(\boldsymbol{x})$.
   (b) Prove que existe $k \in K$ tal que $kd(\boldsymbol{x})m(\boldsymbol{x}) = p(\boldsymbol{x})q(\boldsymbol{x})$.

9. Seja $q(\boldsymbol{x}) \in K[\boldsymbol{x}]$ não-nulo e não invertível. Prove o seguinte (recorde o Teorema Fundamental da Aritmética):
   (a) Existem polinómios irredutíveis $p(\boldsymbol{x})$ tais que $p(\boldsymbol{x})|q(\boldsymbol{x})$.
   (b) Existem polinómios irredutíveis mónicos $m_1(\boldsymbol{x}), \ldots, m_k(\boldsymbol{x}) \in K[\boldsymbol{x}]$ e $a_0 \in K$ tais que $q(\boldsymbol{x}) = a_0 \prod_{i=1}^{k} m_i(\boldsymbol{x})$.
   (c) A decomposição referida acima é única a menos da ordem dos factores.

10. Prove que o ideal $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ em $K[\boldsymbol{x}, \boldsymbol{y}]$ não é principal.

11. Suponha-se que o anel A é uma extensão do corpo K, e seja $a \in A$ algébrico sobre K. Seja ainda $J = \{p(\boldsymbol{x}) \in K[\boldsymbol{x}] : p(a) = 0\}$. Mostre que:

    (a) $J = \langle m(\boldsymbol{x}) \rangle$ é um ideal de $K[\boldsymbol{x}]$ [10].

    (b) Se A não tem divisores de zero, então $m(\boldsymbol{x})$ é irredutível, e $K[a] = K(a)$ é um corpo.

    (c) Se A não tem divisores de zero, e B é o conjunto de todos os elementos de A que são algébricos sobre K, então B é um corpo e é a maior extensão algébrica de K em A.

12. Mostre que $\mathbb{Q}[\sqrt[3]{2}]$ e $\mathbb{Q}[\sqrt[4]{2}]$ são extensões algébricas de $\mathbb{Q}$ e subcorpos de $\mathbb{R}$. Quais são as respectivas dimensões como espaços vectoriais sobre $\mathbb{Q}$?

13. Seja A o conjunto de todos os reais algébricos sobre $\mathbb{Q}$. Mostre que:

    (a) A é um corpo numerável.

    (b) A, que é uma extensão algébrica de $\mathbb{Q}$, é também um espaço vectorial de dimensão infinita sobre $\mathbb{Q}$.

3.7 Divisibilidade e Factorização Prima

O nosso estudo anterior do anel dos inteiros $\mathbb{Z}$ e do anel dos polinómios $K[\boldsymbol{x}]$ mostrou que todo o elemento não-nulo e não invertível nestes anéis possui uma factorização essencialmente única num produto de elementos irredutíveis ou primos. É natural averiguar se esta propriedade se pode generalizar a outros anéis. Vamos por isso estudar nas próximas secções como é que os conceitos sobre divisibilidade e factorização que temos vindo a utilizar podem ser estendidos a um qualquer domínio integral D.

Recordemos que, dados $a, b \in D$, dizemos que a DIVIDE (ou é FACTOR de) b se existir $d \in D$ tal que $b = da$, e que nesse caso escrevemos "$a|b$" [11]. As seguintes noções, adaptadas em parte das que introduzimos em $\mathbb{Z}$ e $K[\boldsymbol{x}]$, serão muito úteis no que se segue.

Definição 3.7.1. Seja D um domínio integral, $a, b, p \in D$, e p um elemento não invertível. Dizemos que:

(i) a é ASSOCIADO de b, se $a|b$ e $b|a$;

(ii) p é PRIMO, se $p \neq 0$ e $p|ab \Rightarrow p|a$ ou $p|b$;

(iii) p é IRREDUTÍVEL, se $p = ab \Rightarrow a$ é invertível ou b é invertível.

[10] Diz-se por vezes que $m(\boldsymbol{x})$ é o *polinómio mínimo* do elemento a.

[11] Também usamos o símbolo "$a \nmid b$" para dizer que a não divide b.

Repare-se portanto que, neste contexto mais geral, o chamado *Lema de Euclides* passa a ser a *definição* dos elementos *primos*, e os elementos *irredutíveis* são os que apenas admitem factorizações *triviais*. É fácil verificar que nos anéis $\mathbb{Z}$ e $K[\boldsymbol{x}]$ os elementos primos no sentido da definição acima são exactamente os elementos irredutíveis, e é apenas por razões históricas que usamos o termo "primo" em $\mathbb{Z}$ e o termo "irredutível" em $K[\boldsymbol{x}]$. Não é esse o caso em todos os domínios integrais, mas identificaremos aqui extensas classes de anéis onde estas noções são equivalentes, e onde é possível estabelecer uma generalização apropriada do Teorema Fundamental da Aritmética, entendido sempre este resultado como uma afirmação sobre a existência e unicidade de factorizações em elementos irredutíveis.

A relação binária *associado de* é de facto uma relação de equivalência: é simples verificar que a é associado de b se e só se $a = ub$ para algum elemento invertível u. Assim, se $a, b \in D$ são associados, escrevemos $a \sim b$. É frequente, em Teoria da Factorização, designar os elementos invertíveis por *unidades*, uma prática que seguiremos. Note-se que as unidades são *os associados da identidade* de D, e observe-se igualmente que, dados $p, q \in D$, se $p \sim q$, então p é primo (respectivamente, irredutível) se e só se q é primo (respectivamente, irredutível). Em particular, se p é primo então todos os elementos que resultam de multiplicar p por uma unidade são igualmente primos, o que bem entendido *não* é a convenção tradicional em $\mathbb{Z}$.

Exemplos 3.7.2.

1. *Os elementos primos de* qualquer *domínio integral D são* sempre *irredutíveis. De facto, se $p \in D$ é primo e $p = ab$, então $p|a$ ou $p|b$. Se, por exemplo, $p|a$, então existe $x \in D$ tal que $a = px$. Concluímos que*

$$\begin{aligned} p = ab &\implies p = pxb, \text{ e como } p \neq 0, \\ &\implies 1 = xb, \\ &\implies b \text{ é invertível.} \end{aligned}$$

   De igual forma, se $p|b$, então concluímos que a é invertível.

2. *Em $\mathbb{Z}$ as unidades são $\{1, -1\}$, e $p \in \mathbb{Z}$ é irredutível no sentido de 3.7.1 se e só se o natural $|p|$ é primo (no sentido do Capítulo 2). É evidente que $p|n \iff |p||n$, e portanto se p é irredutível temos do lema de Euclides que*

$$p|ab \implies |p||ab \implies |p||a \text{ ou } |p||b \implies p|a \text{ ou } p|b.$$

   Concluímos assim que os inteiros irredutíveis *no sentido de 3.7.1 são os inteiros* primos *no sentido da mesma definição.*

3. *As unidades de $K[\boldsymbol{x}]$ são os polinómios de grau zero, e os polinómios irredutíveis no sentido de 3.7.1 são exactamente os que definimos como irredutíveis em 3.5.8. Já vimos também que se $p(\boldsymbol{x}) \in K[\boldsymbol{x}]$ é irredutível então é primo (recorde o exercício 5 da secção anterior, referente ao Lema de Euclides para polinómios). Concluímos novamente que os polinómios* irredutíveis *no sentido de 3.7.1 são os polinómios* primos *no sentido da mesma definição.*

4. As unidades do anel dos inteiros de Gauss $\mathbb{Z}[i]$ *são* $\{1, -1, i, -i\}$. *O elemento* $2 \in \mathbb{Z}[i]$ *não é irredutível em* $\mathbb{Z}[i]$, *apesar de ser irredutível em* $\mathbb{Z}$, *pois temos*

$$2 = (1+i)(1-i), \text{ com } 1 \pm i \text{ não invertíveis.}$$

Para verificar que $1+i$ *e* $1-i$ *são irredutíveis, consideramos a função* $N : \mathbb{Z}[i] \to \mathbb{N}_0$ *definida por*

$$N(a+bi) = |a+bi|^2 = a^2 + b^2.$$

Esta função satisfaz as seguintes duas propriedades:

(a) se $z_1, z_2 \in \mathbb{Z}[i]$, *então* $N(z_1 z_2) = N(z_1)N(z_2)$;

(b) $N(z) = 1$ *se e só se* z *é invertível.*

Para verificar, por exemplo, que $1+i$ *é irredutível, suponha-se que* $1+i = z_1 z_2$ *em* $\mathbb{Z}[i]$. *Temos pela propriedade (a) acima,*

$$2 = N(1+i) = N(z_1 z_2) = N(z_1)N(z_2).$$

Como 2 *só tem factorizações triviais em* $\mathbb{Z}$, *é claro que* $N(z_1) = 1$ *ou* $N(z_2) = 1$. *Pela propriedade (b), concluímos que ou* z_1 *ou* z_2 *são invertíveis, e* $1+i$ *é irredutível em* $\mathbb{Z}[i]$. *Repare-se portanto que* $-(1+i) = -1-i$, $i(1+i) = -1+i$ *e* $-i(1+i)$ *são igualmente irredutíveis. Mostraremos mais adiante que em* $\mathbb{Z}[i]$ *os elementos irredutíveis são também primos, e mostraremos ainda como se podem determinar todos estes elementos de* $\mathbb{Z}[i]$.

5. Existem como dissémos domínios integrais onde os elementos irredutíveis podem não ser primos. Fizémos aliás no Capítulo 2 uma observação relacionada com esta questão a propósito das factorizações $6 \times 6 = 2 \times 18$ *no anel dos inteiros* pares. *Considere-se o anel* $\mathbb{Z}[\sqrt{-5}]$, *que é evidentemente um domínio integral. Temos neste anel que*

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

Podemos no entanto mostrar que 3, *que é irredutível, não é factor de* $(2+\sqrt{-5})$ *nem de* $(2-\sqrt{-5})$, *e portanto não é primo, o que deixamos para os exercícios.*

Todas as noções elementares introduzidas acima podem ser traduzidas em termos de propriedades de ideais do anel em questão. Para isso, diremos que um ideal $0 \subsetneq P \subsetneq D$ é um IDEAL PRIMO se, para todos os ideais $I, J \subset D$,

$$IJ \subset P \Longrightarrow I \subset P \text{ ou } J \subset P.$$

Obtemos, então:

Proposição 3.7.3. *Sejam* $a, b, p, u \in D$. *Então:*

(i) $a|b$ *se e só se* $\langle a \rangle \supset \langle b \rangle$;

(ii) $a \sim b$ *se e só se* $\langle a \rangle = \langle b \rangle$;

(iii) u *é unidade se e só se* $\langle u\rangle = D$*;*

(iv) p *é primo se e só se* $\langle p\rangle$ *é um ideal primo;*

(v) p *é irredutível se e só se* $\langle p\rangle$ *é maximal na classe dos ideais principais de* D*.*

Demonstração. A verificação de (i), (ii) e (iii) fica como simples exercício.

Para mostrar que (iv) é verdadeira, seja $p \in D$ primo, e $I, J \subset D$ ideais tais que $IJ \subset \langle p\rangle$. Se $I \not\subset \langle p\rangle$, então existe $a \in I$ tal que $a \notin \langle p\rangle$, *i.e.*, tal que $p \nmid a$ (por (i)). Logo, para todo o $b \in J$, temos que $ab \in \langle p\rangle \Leftrightarrow p|ab$ e $p \nmid a$. Sendo p primo, necessariamente $p|b$, ou seja, $b \in \langle p\rangle$ (por (i)). Concluímos que $J \subset \langle p\rangle$, e portanto $\langle p\rangle$ é um ideal primo.

Na direcção oposta, suponha-se que $\langle p\rangle$ é um ideal primo e que $p|ab$. Então

$$\langle ab\rangle = \langle a\rangle\langle b\rangle \subset \langle p\rangle \quad \Longrightarrow \quad \langle a\rangle \subset \langle p\rangle \text{ ou } \langle b\rangle \subset \langle p\rangle.$$

Mas, por (i), isto significa que ou $p|a$ ou $p|b$, e portanto p é primo.

Para mostrar que (v) se verifica, consideremos $p \in D$ irredutível, e suponha-se que $\langle p\rangle \subset \langle a\rangle$. Então $p = ax$ logo, ou a é uma unidade ou x é uma unidade. Se a é uma unidade, então por (iii) $\langle a\rangle = D$. Se x é uma unidade, então $p \sim a$ e, por (ii), $\langle p\rangle = \langle a\rangle$. Assim, $\langle p\rangle$ é maximal na classe dos ideais principais de D.

Reciprocamente, suponha-se que $\langle p\rangle$ é maximal na classe dos ideais principais de D, e que $p = ab$. Como $\langle p\rangle \subset \langle a\rangle$, vemos que ou $\langle a\rangle = D$ e a é invertível (por (iii)), ou $\langle p\rangle = \langle a\rangle$ e $a \sim p$ (por (ii)). Neste último caso, existe $u \in D$ unidade, tal que $a = pu$, logo

$$\begin{aligned} p = ab \quad &\Longrightarrow \quad p = pub, \\ &\Longrightarrow \quad 1 = ub \quad \Longrightarrow b \text{ é invertível.} \end{aligned}$$

Donde ou a ou b são invertíveis, e portanto p é irredutível. □

Esta proposição sugere que podemos construir toda a Teoria da Factorização com base nos ideais de D em vez dos elementos de D. De facto isto é possível e até vantajoso, e historicamente está na base da designação "ideal". Prosseguiremos esta via mais tarde, no Capítulo 7, limitando-nos por enquanto ao estudo da factorização de elementos de D.

Definição 3.7.4. Um domínio D diz-se um DOMÍNIO DE FACTORIZAÇÃO ÚNICA (abreviadamente d.f.u.), se as seguintes duas condições são satisfeitas:

(i) Se $d \in D$ não é invertível e $d \neq 0$, existem elementos irredutíveis $p_1, \cdots, p_n$ tais que

$$d = \prod_{i=1}^{n} p_i. \tag{3.7.1}$$

(ii) Se $p_1, \cdots p_n$, e $p'_1 \cdots p'_m$ são irredutíveis, e $\prod_{i=1}^n p_i = \prod_{i=1}^m p'_i$, então $n = m$, e existe uma permutação $\pi \in S_n$ tal que $p_j \sim p'_{\pi(j)}$.

Por outras palavras, num d.f.u., todo o elemento não-nulo e não invertível possui uma factorização num produto de elementos irredutíveis, e esta factorização é única a menos da ordem dos factores e da multiplicação de cada factor por uma unidade convenientemente escolhida (observe que se $p'_i = u_i p_i$, então temos necessariamente $\prod_{i=1}^n u_i = 1$).

Exemplos 3.7.5.

1. *O anel $\mathbb{Z}$ é um d.f.u.: Segue-se, do Teorema Fundamental da Aritmética, que todo o inteiro pode ser factorizado na forma*

$$m = p_1 \cdots p_m,$$

*onde p_i é irredutível (*i.e.*, $|p_i|$ é um natural primo). Esta factorização é única a menos da ordem dos factores e multiplicações por ± 1.*

2. *Pelo Exercício 9 da Secção 3.6, dado um polinómio $q(\boldsymbol{x}) \in K[\boldsymbol{x}]$, existem polinómios irredutíveis $p_1(\boldsymbol{x}), \ldots, p_n(\boldsymbol{x}) \in K[\boldsymbol{x}]$ tais que*

$$q(\boldsymbol{x}) = \prod_{i=1}^{n} p_i(\boldsymbol{x}).$$

Esta decomposição é única a menos da ordem dos factores, e da multiplicação por unidades. Ou seja, $K[\boldsymbol{x}]$ é um d.f.u.

3. *Veremos imediatamente a seguir que o anel dos inteiros de Gauss é um d.f.u..*

Observe-se que a factorização indicada em 3.7.1 pode igualmente ser expressa em *potências* de elementos irredutíveis, mas neste caso pode ser necessário incluir uma unidade na factorização, que passa a ser da forma:

$$d = u \cdot p_1^{e_1} \cdots p_n^{e_n}. \tag{3.7.2}$$

Exemplos 3.7.6.

1. *Temos em $\mathbb{Z}$ que $-15 = (3) \cdot (-3) = (-1)3^2$.*
2. *Em $\mathbb{Q}[\boldsymbol{x}]$, temos $2\boldsymbol{x}^2 + 4\boldsymbol{x} + 2 = (2\boldsymbol{x} + 2)(\boldsymbol{x} + 1) = 2(x + 1)^2$.*

O próximo teorema fornece uma primeira caracterização dos d.f.u.

Teorema 3.7.7. *Seja D um domínio integral. Então D é um d.f.u. se e só se as seguintes condições se verificam:*

(i) todo o elemento irredutível é primo;

(ii) toda a cadeia ascendente de ideais principais estabiliza, i.e.*, se*

$$\langle d_1\rangle \subset \langle d_2\rangle \subset \cdots \subset \langle d_n\rangle \subset \ldots$$

é uma cadeia ascendente de ideais, então existe um natural n_0 *tal que*

$$\langle d_{n_0}\rangle = \langle d_{n_0+1}\rangle = \ldots.$$

Demonstração. Seja D um d.f.u., e $p \in D$ um elemento irredutível. Se $p|ab$, então existe $x \in D$ tal que $px = ab$, onde x, a e b possuem factorizações do tipo (3.7.1), *i.e.*,

$$x = p_1 \cdots p_r,\ a = p'_1 \cdots p'_s,\ b = p''_1 \cdots p''_t$$

com p_i, p'_j, p''_k primos em D. Logo

$$p \cdot p_1 \cdots p_r = p'_1 \cdots p'_s \cdot p''_1 \cdots p''_t,$$

e, pela unicidade da factorização, temos $p \sim p'_i$ ou $p \sim p''_j$. No primeiro caso $p|a$, e no segundo $p|b$. Portanto, p é primo.

Por outro lado, considere-se uma cadeia ascendente de ideais principais

$$\langle d_1\rangle \subset \langle d_2\rangle \subset \cdots \subset \langle d_n\rangle \subset \ldots$$

Supomos, sem perda de generalidade (porquê?), que $d_1 \neq 0$ e d_i não é invertível, $\forall i$. Como $d_i|d_1, \forall i$, as factorizações de d_1 e d_i tomam a forma

$$d_1 = p_1 \cdots p_r,\ d_i = p'_1 \cdots p'_s.$$

Os factores irredutíveis de d_i são factores de d_1, e portanto $s \leq r$. Em particular, não existem na cadeia indicada mais de r ideais distintos entre si, e existe um natural n_0 tal que $\langle d_{n_0}\rangle = \langle d_k\rangle$, para qualquer $k \geq n_0$. Terminamos assim a primeira metade da demonstração.

Reciprocamente, assuma-se que D é um domínio integral verificando as condições (i) e (ii) do enunciado do teorema. Seja $d \in D$ um elemento não-nulo e não invertível, e suponha-se por absurdo que d não é factorizável num produto de elementos irredutíveis. Por indução, construímos uma sucessão $\{d_n\}_{n\in\mathbb{N}}$ onde $d_1 = d$, $d_{n+1}|d_n$, $d_n \not\sim d_{n+1}$ e *nenhum* dos elementos d_n é factorizável num produto de elementos irredutíveis.

Supomos para isso $n > 0$, e os elementos $d_1, \cdots, d_n$ já definidos, atendendo a que o caso $n = 1$ é trivial. Notamos que d_n não é irredutível, por razões óbvias, e portanto $d_n = a_n b_n$, onde a_n e b_n não são invertíveis. É claro que a_n e b_n não podem ser ambos factorizáveis num produto de irredutíveis, e supomos sem perda de generalidade que b_n, pelo menos, não é assim factorizável. Definimos $d_{n+1} = b_n$, e notamos como evidente que $d_{n+1}|d_n$, e $d_n \not\sim d_{n+1}$. Os ideais principais gerados pelos d_n's satisfazem

$$\langle d_1\rangle \subsetneq \langle d_2\rangle \subsetneq \cdots \subsetneq \langle d_n\rangle \subsetneq \ldots$$

contradizendo a condição de toda a cadeia ascendente de ideais principais estabilizar. Concluímos assim que todos os elementos não-nulos e não invertíveis de D são factorizáveis em produtos de elementos irredutíveis.

Para verificar a unicidade da factorização, suponha-se que

$$p_1 \cdots p_n = p'_1 \cdots p'_m,$$

com, digamos, $n \leq m$. Como os p_i, p'_j são irredutíveis, por (i) eles são primos; como $p_n | p'_1 \cdots p'_m$, temos que p_n é associado a algum p'_j, que designamos por $p'_{\pi(n)}$. Excluindo estes dois elementos, e repetindo o argumento, obtemos por exaustão que $n = m$ e $p_i \sim p'_{\pi(i)}$ para alguma permutação $\pi \in S_n$. □

O resultado anterior justifica o uso da expressão "*factorização prima*" para designar factorizações do tipo (3.7.1) ou (3.7.2).

Como já observámos anteriormente, a propriedade fundamental dos anéis $\mathbb{Z}$ e $K[\boldsymbol{x}]$, no que respeita à factorização, é a de que todos os seus ideais são *principais*.

Definição 3.7.8. Diz-se que um domínio integral D é um DOMÍNIO DE IDEAIS PRINCIPAIS, abreviadamente d.i.p., se todos os seus ideais são principais (*i.e.*, da forma $\langle d \rangle$).

Como consequência do Teorema 3.7.7 obtemos o

Corolário 3.7.9. *Todo o d.i.p. é um d.f.u.*

Demonstração. Mostramos primeiro que os elementos irredutíveis em D são primos. Para isso, supomos $p \in D$ irredutível, e $p|ab$. Sabemos que o ideal $\langle a, p \rangle$ é principal, *i.e.*, existe $d \in D$ tal que $\langle d \rangle = \langle a, p \rangle$. Como $\langle p \rangle \subset \langle d \rangle \subset D$ e $\langle p \rangle$ é maximal (Proposição 3.7.3), temos

$$\langle p \rangle = \langle d \rangle \text{ ou } \langle p \rangle = D.$$

No primeiro caso, $p \sim d$ e, como $d|a$, concluímos que $p|a$. No segundo caso, existem $r, s \in D$ tais que $1 = ra + sp$, logo

$$b = 1 \cdot b = (ra + sp)b = rab + spb.$$

Como p divide cada um dos termos do lado direito, concluímos que $p|b$. Em qualquer caso, $p|a$ ou $p|b$, donde p é primo.

Verificamos agora que qualquer cadeia ascendente de ideais principais estabiliza. Considere-se a cadeia:

$$\langle d_1 \rangle \subset \langle d_2 \rangle \subset \cdots \subset \langle d_n \rangle \subset \ldots$$

É fácil verificar que $\cup_{i=1}^{\infty} \langle d_i \rangle$ é um ideal, necessariamente principal, e portanto $\cup_{i=1}^{\infty} \langle d_i \rangle = \langle d_0 \rangle$. Existe naturalmente n_0 tal que $d_0 \in \langle d_{n_0} \rangle$, e deve ser evidente que:

$$\langle d_{n_0} \rangle = \langle d_n \rangle, \forall n \geq n_0.$$

Concluímos que D é um d.f.u., de acordo com o Teorema 3.7.7. □

Exemplos 3.7.10.

1. *O anel dos inteiros de Gauss é um d.f.u., porque $\mathbb{Z}[i]$ é um d.i.p., como se deve ter verificado no exercício 16 da secção 2.6.*

2. *Veremos na próxima secção que se D é um d.f.u. então $D[\boldsymbol{x}]$ é igualmente um d.f.u. Em particular, $\mathbb{Z}[\boldsymbol{x}]$ é um d.f.u., apesar de não ser um d.i.p.*

Em geral, o problema de determinar se um dado domínio integral é um d.f.u. pode ser de difícil resolução. Por exemplo, sabe-se que os domínios quadráticos $\mathbb{Z}[\sqrt{m}]$, para $m < 0$, são d.f.u. se e só se $m = -1, -2, -3, -7$ e -11, um resultado não-trivial e que está para além do âmbito deste livro. De igual forma, mesmo sabendo que D é um d.f.u., pode ser bastante difícil determinar os seus elementos primos. Ilustramos este último tipo de problema com o caso dos inteiros de Gauss.

Para simplificar a exposição, dizemos que os naturais primos em $\mathbb{Z}$ são os *primos euclidianos*, e os inteiros de Gauss primos em $\mathbb{Z}[i]$ são os *primos gaussianos*.

Proposição 3.7.11. *Seja $p \in \mathbb{Z}$ um primo euclidiano.*

(i) Se a equação $p = n^2 + m^2$ tem *soluções $n, m \in \mathbb{Z}$, então $z = n + mi$ é um primo gaussiano;*

(ii) Se a equação $p = n^2 + m^2$ não *tem soluções em $\mathbb{Z}$, então p é um primo gaussiano;*

(iii) $z \in \mathbb{Z}[i]$ é um primo gaussiano se e só se $z \sim p$, onde p é um primo gaussiano, ou $z \sim n + mi$, onde $n^2 + m^2 = p$.

Demonstração. Para demonstrar (i), suponha-se que

$$p = n^2 + m^2 = (n + mi)(n - mi).$$

Sendo $n + mi = (a + bi)(c + di)$ uma factorização de $z = n + mi$, temos

$$p = n^2 + m^2 = (a^2 + b^2)(c^2 + d^2), \text{ e portanto } a^2 + b^2 = 1 \text{ ou } c^2 + d^2 = 1.$$

Por outras palavras, um dos complexos $a+bi$ ou $c+di$ é invertível. Como $n+mi$ não é nulo nem invertível, concluímos que $n+mi$ é um primo gaussiano.

Para provar (ii), observe-se que, se p não é primo gaussiano, então existem inteiros de Gauss não invertíveis z e w tais que $p = zw$, donde $p^2 = |z|^2|w|^2$. Como $|z|^2$ e $|w|^2$ são inteiros $\neq \pm 1$, só podemos ter $p = |z|^2 = |w|^2$, e portanto a equação $p = n^2 + m^2$ tem soluções.

Finalmente, e para verificar (iii), seja $z = a + bi$ um primo gaussiano, donde $|z|^2 > 1$, e p um qualquer factor primo (em $\mathbb{Z}$) de $|z|^2$. Notamos que existe $w \in \mathbb{Z}[i]$ tal que

$$|z|^2 = (a + bi)(a - bi) = pw.$$

Como p é um inteiro, é claro que $p|a+bi = z$ se e só se $p|a-bi$. Uma das seguintes duas alternativas é necessariamente verdadeira:

1. *p é também primo gaussiano*: Neste caso segue-se do Lema de Euclides (válido em $\mathbb{Z}[i]$, porque $\mathbb{Z}[i]$ é um d.f.u.) que $p|a+bi$ ou $p|a-bi$, *i.e.*, p é factor de z. Temos então $z \sim p$, porque z e p são ambos primos gaussianos;

2. *p não é primo gaussiano*: Concluímos de (ii) que a equação $p = n^2+m^2$ *tem* soluções, e observamos que temos agora

$$|z|^2 = (a+bi)(a-bi) = pw = (n+mi)(n-mi)w.$$

   Como sabemos de (i) que $n+mi$ é um primo gaussiano, concluímos novamente do Lema de Euclides que $a+bi \sim n+mi$ ou $a+bi \sim n-mi$.

□

Exemplos 3.7.12.

1. *É claro que a equação $3 = n^2+m^2$ não tem soluções em $\mathbb{Z}$, e portanto 3 é um primo euclidiano que é também primo gaussiano.*

2. *Como $5 = 1^2+2^2$, segue-se que 5 não é primo gaussiano, mas os inteiros de Gauss $\pm 1 \pm 2i$ e $\pm 2 \pm i$ são primos gaussianos.*

Acabámos de ver que a determinação dos primos gaussianos depende da resolução da equação $p = n^2+m^2$, onde p é um primo euclidiano. Fermat descobriu um resultado especialmente elegante sobre os valores de p para os quais esta equação tem soluções, que adaptamos aqui da seguinte forma.

Teorema 3.7.13 (de Fermat). *Seja p um primo euclidiano. Então as seguintes afirmações são equivalentes:*

(i) A equação $p = n^2+m^2$ tem soluções em $\mathbb{Z}$,

(ii) $p \not\equiv 3 \ (mod\ 4)$,

(iii) A equação $x^2 = -1$ tem soluções em $\mathbb{Z}_p$.

Demonstração. Deixamos para os exercícios a prova de "(i) $\Longrightarrow$ (ii)".

Para demonstrar "(ii) $\Longrightarrow$ (iii)", notamos primeiro que podemos supor $p \neq 2$, por razões evidentes, já que neste caso $x = 1$ é solução da equação $x^2 = -1 = 1$. Temos portanto que $p \equiv 1 \ (mod\ 4)$, e definimos para $x, y \in \mathbb{Z}_p^*$:

- $C(x) = \{x, -x, x^{-1}, -x^{-1}\}$,
- x é *equivalente* a $y \iff x \approx y \iff C(x) = C(y)$.

É muito fácil verificar que "$\approx$" é uma relação de equivalência em $\mathbb{Z}_p^*$, que $x \neq -x$ para qualquer $x \in \mathbb{Z}_p^*$ (porque $p \neq 2$), e que a classe de equivalência de x é precisamente o conjunto $C(x)$. Designando por $\#(C(x))$ o *número de elementos* da classe $C(x)$, observe-se que $\#(C(x))$ só pode ser 2 ou 4, como se segue:

$$\begin{aligned}\#(C(x)) &= 2, \text{ se } x = x^{-1}, \text{ i.e., se } x = \pm 1,\\ &= 2, \text{ se } x = -x^{-1}, \text{ i.e., se } x \text{ e } x^{-1} \text{ são as soluções de } x^2 = -1,\\ &= 4, \text{ se } x \text{ não é solução de } x^2 = \pm 1, \text{ i.e., não é solução de } x^4 = 1.\end{aligned}$$

As classes de equivalência formam como sabemos uma partição de $\mathbb{Z}_p^*$, e $\mathbb{Z}_p^*$ tem $p-1$ elementos. Acabámos de mostrar que existe pelo menos uma classe com 2 elementos, que é $C(1) = \{1, -1\}$. Existe possivelmente uma outra classe com 2 elementos, formada pelas raízes de $x^2 + 1$, se este polinómio tiver raízes em $\mathbb{Z}_p^*$. Sendo n o número de classes de equivalência com 4 elementos, concluímos que os $p - 1$ elementos se distribuem como se segue:

- Se *não* existem soluções de $x^2 = -1$, $p - 1 = 2 + 4n$, ou $p = 4n + 3$, porque existe apenas *uma* classe com 2 elementos, tendo as restantes n classes 4 elementos cada, ou
- Se *existem* soluções de $x^2 = -1$, $p-1 = 2+2+4n$, ou $p = 4(n+1)+1$, porque existem 2 classes cada uma com 2 elementos, além das n classes de 4 elementos.

Como $p \neq 2$ é primo, é claro que $p \not\equiv 3 \pmod 4 \implies p \equiv 1 \pmod 4$ e concluímos que a equação $x^2 = -1$ *tem* soluções em $\mathbb{Z}_p^*$.

Provamos finalmente "(iii) $\implies$ (i)": A equação $x^2 = -1$ tem soluções em $\mathbb{Z}_p$ se e só se existe um inteiro k tal que $p|1+k^2 = (1+ki)(1-ki)$. Se p é um primo gaussiano então $p|1+ki$ ou $p|1-ki$, o que é absurdo, porque $p \not| 1$. Portanto, p não é um primo gaussiano, e de acordo com 3.7.11, a equação $p = n^2 + m^2$ tem soluções. □

Exemplos 3.7.14.

1. *Os primos euclidianos* 7, 11 *e* 19 *são primos gaussianos.*
2. 1973 *é um primo euclidiano que não é gaussiano, porque* $p \equiv 1 \pmod 4$. *Portanto a equação* $1973 = n^2 + m^2$ *tem soluções* $n, m \in \mathbb{Z}$, *que já não são fáceis de determinar (por exemplo,* $n = 23$ *e* $m = 38$*).*

Uma propriedade importante dos d.f.u. é que neste tipo de domínios integrais quaisquer dois elementos têm sempre máximo divisor comum e mínimo múltiplo comum. Para entender esta observação, precisamos de uma definição um pouco mais abstracta para as noções de máximo divisor comum e mínimo múltiplo comum, aplicável em domínios integrais arbitrários.

Definição 3.7.15. Seja D um domínio integral, e $a_1, \ldots, a_n \in D$.

(i) $d \in D$ é (um) MÁXIMO DIVISOR COMUM de $a_1, \ldots, a_n$ se $d|a_i, i = 1, \ldots, n$ e, para todo o $b \in D$ tal que $b|a_i, i = 1, \ldots, n$, temos $b|d$;

(ii) $m \in D$ é (um) MÍNIMO MÚLTIPLO COMUM de $a_1, \ldots, a_n$ se $a_i|m, i = 1, \ldots, n$, e para todo o $b \in D$ tal que $a_i|b, i = 1, \ldots, n$, temos $m|b$.

Por palavras, d é um *máximo divisor comum* se é divisor comum, e é múltiplo de todos os divisores comuns, e m é um *mínimo múltiplo comum* se é múltiplo comum, e é divisor de todos os múltiplos comuns. A referência implícita à falta de *unicidade* nestas noções resulta de observar que se d é máximo divisor comum, e $c \sim d$, então c é igualmente máximo divisor comum, e o mesmo se passa com o mínimo múltiplo comum. Evitámos esta dificuldade em $\mathbb{Z}$ e em $K[\boldsymbol{x}]$, exigindo d e m *não negativos* em $\mathbb{Z}$, e *mónicos* em $K[\boldsymbol{x}]$, mas exceptuando este detalhe, a definição acima é evidentemente compatível com as introduzidas nos Capítulos 2 e 3.

Não é de todo óbvio que, dados elementos $a_1, \ldots, a_n \in D$, esses elementos tenham sempre máximo divisor comum e/ou mínimo múltiplo comum. No entanto, se $a_1, \ldots, a_n$ possuem pelo menos *um* máximo divisor comum (respectivamente, mínimo múltiplo comum), designamos por $\mathrm{mdc}(a_1, \ldots, a_n)$ (respectivamente, $\mathrm{mmc}(a_1, \ldots, a_n)$) qualquer um desses elementos.

Se D é um d.f.u., então, como indicámos acima, quaisquer elementos $a, b \in D$ têem máximo divisor comum e menor múltiplo comum.

Proposição 3.7.16. *Seja D um d.f.u., e $a, b \in D$.*

(i) Existem $\mathrm{mdc}(a, b)$ *e* $\mathrm{mmc}(a, b)$.

(ii) Se D é um d.i.p., então qualquer máximo divisor comum de a e b é da forma $ra + sb$ para alguns $r, s \in D$.

Demonstração. (i) Se a é nulo, então $\mathrm{mdc}(a, b) = b$ e $\mathrm{mmc}(a, b) = 0$. Se a é invertível, então $\mathrm{mdc}(a, b) = a$ e $\mathrm{mmc}(a, b) = b$. Podemos, pois, assumir que a e b não são nulos nem invertíveis. As factorizações primas de a e de b podem ser escritas na forma

$$a = u \cdot p_1^{n_{a1}} \cdots p_s^{n_{as}}, \text{ e } b = u' \cdot p_1^{n_{b1}} \cdots p_s^{n_{bs}},$$

onde os p_i são distintos, $n_{ai} \geq 0$ e $n_{bi} \geq 0$. Tomando para $i = 1, \ldots, s$ os inteiros

$$m_i = \min\{n_{ai}, n_{bi}\}, \text{ e } M_i = \max\{n_{ai}, n_{bi}\},$$

vemos imediatamente que podemos escolher:

$$\mathrm{mdc}(a, b) = p_1^{m_1} \cdots p_s^{m_s}, \text{ e } \mathrm{mmc}(a, b) = p_1^{M_1} \cdots p_s^{M_s}.$$

(ii) Sejam $a, b \in D$. Como D é um d.i.p., existe $c \in D$ tal que $\langle a, b\rangle = \langle c\rangle$, e é claro que $c|a$ e $c|b$. Se $d = \mathrm{mdc}(a, b)$, temos, por definição, $c|d$, e concluímos que $d \in \langle a, b\rangle$, ou seja, existem $r, s \in D$ tais que $d = ra + sb$. □

O lema seguinte enuncia algumas propriedades elementares do máximo divisor comum, e a sua demonstração é deixada como exercício.

Lema 3.7.17. *Sejam $a, b, c \in D$. Então:*

(i) $\operatorname{mdc}(a, \operatorname{mdc}(b, c)) \sim \operatorname{mdc}(\operatorname{mdc}(a, b), c) \sim \operatorname{mdc}(a, b, c)$;

(ii) $\operatorname{mdc}(ca, cb) \sim c \operatorname{mdc}(a, b)$.

Exercícios.

1. Demonstre os itens (i)-(iii) da Proposição 3.7.3.

2. Mostre que no anel $\mathbb{Z}[\sqrt{-5}]$ os elementos 3 e $2 \pm \sqrt{-5}$ são irredutíveis.

3. Mostre que o anel $\mathbb{Z}[\sqrt{10}]$ não é um d.f.u.

4. Demonstre que, se p é primo euclidiano e existem inteiros n e m tais que $p = n^2 + m^2$, então $p \not\equiv 3 \pmod 4$.

5. Prove que se p é um primo euclidiano e $n, m, a, b \in \mathbb{Z}$ satisfazem $p = n^2 + m^2 = a^2 + b^2$ então $\{n^2, m^2\} = \{a^2, b^2\}$.

6. Um domínio integral D diz-se DOMÍNIO EUCLIDIANO se existir uma aplicação $\delta : D \to \mathbb{N}$ com a seguinte propriedade: $\forall a, b \in D - \{0\}$ existem $q, r \in D$ tais que
$$a = qb + r, \qquad \text{com } \delta(r) < \delta(b).$$
Mostre que:
   (a) $\mathbb{Z}$ e $K[\boldsymbol{x}]$ são domínios euclidianos;
   (b) o anel dos inteiros de Gauss $\mathbb{Z}[i]$ é um domínio euclidiano;
   (c) um domínio euclidiano é um d.f.u. (sem recorrer ao Teorema 3.7.7 ou ao seu corolário);
   (d) um domínio euclidiano é um d.i.p.

7. Seja D um domínio integral.
   (a) Verifique que, se D satisfaz a condição da cadeia ascendente de ideais principais, então todo o elemento de D é factorizável (mas, possivelmente, não unicamente).
   (b) Dê um exemplo de um domínio integral D que não satisfaz a condição da cadeia ascendente de ideais principais.

8. Prove o Lema 3.7.17.

9. Suponha que $k \in \mathbb{N}$, e prove que $k = n^2 + m^2$ tem soluções em $\mathbb{Z}$ se e só se qualquer factor primo p de k com $p \equiv 3 \pmod 4$ satisfaz $p^{2N} | k$. Qual é o menor natural k para o qual a equação $k = n^2 + m^2 = s^2 + t^2$ tem soluções n, m, s, t tais que $\{n^2, m^2\} \neq \{s^2, t^2\}$?

10. Seja P o conjunto dos primos euclidianos, e G o conjunto dos primos gaussianos. Prove que $P - G$ e $G - P$ são ambos conjuntos *infinitos*. Por outras palavras, mostre que existem infinitos primos euclidianos da forma $p = 4n+1$ e da forma $p = 4n+3$. SUGESTÃO: Considere os naturais da forma $k = (2N!)-1$, e da forma $k = \left(\prod_{i=1}^{N}(2i-1)\right)^2 + 4$.

3.8 Factorização em $D[\boldsymbol{x}]$

O anel de polinómios $K[\boldsymbol{x}]$ é um d.f.u. quando K é um corpo, porque $K[\boldsymbol{x}]$ é um domínio de ideais principais. A estrutura dos ideais do anel $D[\boldsymbol{x}]$, quando D é um domínio integral que não é um corpo, é muito mais complexa. De facto, $D[\boldsymbol{x}]$ é um d.p.i. *se e só se* D é um corpo, o que explica diversos casos de domínios integrais que temos vindo a referir, como $\mathbb{Z}[\boldsymbol{x}]$ e $D[\boldsymbol{x}] = K[\boldsymbol{x}, \boldsymbol{y}] = K[\boldsymbol{y}][\boldsymbol{x}]$, que *não* são domínios de integrais principais (recorde o Exercício 10 da Secção 3.6). É claro que em qualquer caso se D não é um d.f.u. então $D[\boldsymbol{x}]$ também não é um d.f.u., e veremos nesta secção que na verdade o anel $D[\boldsymbol{x}]$ é um d.f.u. *se e só se* D é um d.f.u., o que mostrará em particular que $\mathbb{Z}[\boldsymbol{x}]$ e $K[\boldsymbol{x}, \boldsymbol{y}]$ são domínios de factorização única.

No que se segue nesta secção, assumimos que D é um d.f.u., de forma que existem máximo divisor e mínimo múltiplo comum em D. Designaremos por K o corpo de fracções $K = Frac(D)$.

A definição de CONTEÚDO de um polinómio, introduzida na secção 3.5 para $p(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$, pode naturalmente ser usada quase sem adaptações em $D[\boldsymbol{x}]$. Se $p(\boldsymbol{x}) = a_0 + a_1\boldsymbol{x} + \cdots + a_n\boldsymbol{x}^n \in D[\boldsymbol{x}]$, dizemos que $c(p) \in D$ é CONTEÚDO DE $p(\boldsymbol{x})$ se e só se

$$c(p) = \mathrm{mdc}(a_0, \ldots, a_n). \tag{3.8.1}$$

É claro que, tal como o máximo divisor comum, o conteúdo de um polinómio fica definido a menos de multiplicação por uma unidade. Mais uma vez, um polinómio $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$ diz-se PRIMITIVO, se $c(p) \sim 1$.

Lema 3.8.1. *Seja $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$ um polinómio.*

(i) Existe $q(\boldsymbol{x}) \in D[\boldsymbol{x}]$ primitivo tal que $p(\boldsymbol{x}) = c(p)q(\boldsymbol{x})$.

(ii) Se $p(\boldsymbol{x}) = dq(\boldsymbol{x})$, com $q(\boldsymbol{x}) \in D[\boldsymbol{x}]$ primitivo e $d \in D$, então $d \sim c(p)$.

Demonstração. A parte (i) é óbvia. Para mostrar (ii), sejam $p(\boldsymbol{x}) = a_0 + a_1\boldsymbol{x} + \cdots + a_n\boldsymbol{x}^n$ e $q(\boldsymbol{x}) = b_0 + b_1\boldsymbol{x} + \cdots + b_n\boldsymbol{x}^n$, com $q(\boldsymbol{x})$ primitivo, e suponha-se que $p(\boldsymbol{x}) = cq(\boldsymbol{x})$. Então $a_i = cb_i$, e do Lema 3.7.17 obtemos

$$c(p) = \mathrm{mdc}(a_0, \ldots, a_n) \sim c\,\mathrm{mdc}(b_0, \ldots, b_n) \sim c.$$

□

Demonstramos a seguir dois lemas auxiliares, que permitem exprimir polinómios $p(\boldsymbol{x}) \in K[\boldsymbol{x}]$ em termos de polinómios primitivos em $D[\boldsymbol{x}]$.

Lema 3.8.2. *Seja $0 \neq p(\boldsymbol{x}) \in K[\boldsymbol{x}]$. Então:*

(i) Existem $q(\boldsymbol{x}) \in D[\boldsymbol{x}]$ primitivo e $k \in K$ tais que $p(\boldsymbol{x}) = kq(\boldsymbol{x})$;

(ii) Se $p(\boldsymbol{x}) = kq(\boldsymbol{x}) = \tilde{k}\tilde{q}(\boldsymbol{x})$, com $k, \tilde{k} \in K$ e $q(\boldsymbol{x}), \tilde{q}(\boldsymbol{x}) \in D[\boldsymbol{x}]$ primitivos, então $\tilde{q}(\boldsymbol{x}) = uq(\boldsymbol{x})$ e $\tilde{k} = u^{-1}k$, onde $u \in D$ é uma unidade.

Demonstração. (i) Se

$$p(\boldsymbol{x}) = \alpha_0 + \alpha_1\boldsymbol{x} + \cdots + \alpha_n\boldsymbol{x}^n = \frac{a_0}{b_0} + \frac{a_1}{b_1}\boldsymbol{x} + \cdots + \frac{a_n}{b_n}\boldsymbol{x}^n \in K[\boldsymbol{x}],$$

tomamos $b = \prod_{i=1}^{n} b_i$. Claramente, $r(\boldsymbol{x}) = bp(\boldsymbol{x}) \in D[\boldsymbol{x}]$. Se $c = c(r)$, pelo Lema 3.8.1, existe $q(\boldsymbol{x}) \in D[\boldsymbol{x}]$ primitivo tal que $r(\boldsymbol{x}) = cq(\boldsymbol{x})$, e temos

$$p(\boldsymbol{x}) = kq(\boldsymbol{x}), \text{ onde } k = \frac{c}{b} \in K.$$

(ii) A demonstração de (ii) é deixada como exercício. □

Corolário 3.8.3. *Se $p(\boldsymbol{x}), q(\boldsymbol{x}) \in D[\boldsymbol{x}]$ são primitivos e $p(\boldsymbol{x}) \sim q(\boldsymbol{x})$ em $K[\boldsymbol{x}]$, então $p(\boldsymbol{x}) \sim q(\boldsymbol{x})$ em $D[\boldsymbol{x}]$.*

Demonstração. Se $p(\boldsymbol{x}) \sim q(\boldsymbol{x})$ em $K[\boldsymbol{x}]$, então $p(\boldsymbol{x}) = \alpha q(\boldsymbol{x})$, com $\alpha \in K$. O corolário segue-se então do Lema 3.8.2, parte (ii). □

Os dois lemas seguintes generalizam resultados que demonstrámos ou deixámos como exercícios no caso $D = \mathbb{Z}$ e $K = \mathbb{Q}$.

Lema 3.8.4. *Sejam $q(\boldsymbol{x}), r(\boldsymbol{x}) \in D[\boldsymbol{x}]$, e $p(\boldsymbol{x}) = q(\boldsymbol{x})r(\boldsymbol{x})$.*

(i) Se $d \in D$ é primo, então $d|c(p) \Longrightarrow d|c(q)$ ou $d|c(r)$, e

(ii) $p(\boldsymbol{x})$ é primitivo se e só se $q(\boldsymbol{x})$ e $r(\boldsymbol{x})$ são ambos primitivos.

Demonstração. Escrevemos $p(\boldsymbol{x}) = a_0 + a_1\boldsymbol{x} + \cdots$, $q(\boldsymbol{x}) = b_0 + b_1\boldsymbol{x} + \cdots$, e $r(\boldsymbol{x}) = c_0 + c_1\boldsymbol{x} + \cdots$. Para provar (i), seja $d \in D$ primo, tal que $d|c(p)$, e suponha-se, por absurdo, que $d \not| c(q)$ e $d \not| c(r)$. Definimos então:

$$s = Min\{k \geq 0 : d \not| b_k\}, \text{ e } t = Min\{k \geq 0 : d \not| c_k\}.$$

Observe-se agora que, com $m = s + t$, temos:

$$\begin{aligned} a_m = \sum_{k=0}^{m} b_k c_{m-k} &= \sum_{k=0}^{s-1} b_k c_{m-k} + b_s c_t + \sum_{k=s+1}^{m} b_k c_{m-k}, \text{ ou} \\ &= \sum_{k=0}^{s-1} b_k c_{m-k} + b_s c_t + \sum_{k=0}^{t-1} b_{m-k} c_k, \text{ ou ainda,} \\ b_s c_t &= a_m - \sum_{k=0}^{s-1} b_k c_{m-k} - \sum_{k=0}^{t-1} b_{m-k} c_k. \end{aligned}$$

Os dois últimos somatórios devem bem entendido ser interpretados como *nulos*, respectivamente quando $s = 0$ ou $t = 0$, mas em qualquer caso deve ser evidente que o lado direito da última identidade é múltiplo de d, enquanto que o lado esquerdo não o é, o que é evidentemente absurdo. Concluímos assim que $d|c(q)$ ou $d|c(r)$.

Para demonstrar (ii), suponha-se primeiro que $q(\boldsymbol{x})$ e $r(\boldsymbol{x})$ são primitivos. É claro que $p(\boldsymbol{x}) \neq 0$, e concluímos de (i) que $c(p)$ não tem nenhum factor primo d, porque $c(q)$ e $r(q)$ são invertíveis, e por isso não têm factores primos. Por outras palavras, $p(\boldsymbol{x})$ é primitivo.

Finalmente, se $p(\boldsymbol{x})$ é primitivo então $p(\boldsymbol{x}) \neq 0$, e portanto $c(q)$ e $c(r)$ não são nulos, porque $q(\boldsymbol{x})$ e $r(\boldsymbol{x})$ não são nulos. Se d é primo e $d|c(q)$ ou $d|c(r)$, é claro que $d|c(p)$, o que é impossível. Logo $c(q)$ e $c(r)$ são invertíveis, ou seja, $q(\boldsymbol{x})$ e $r(\boldsymbol{x})$ são primitivos. □

Exemplo 3.8.5.

Os polinómios $p(\boldsymbol{x}) = 3\boldsymbol{x}^2+2\boldsymbol{x}+5$ *e* $q(\boldsymbol{x}) = 5\boldsymbol{x}^2+2\boldsymbol{x}+3$ *em* $\mathbb{Z}[\boldsymbol{x}]$ *são primitivos pois* $\operatorname{mdc}(3, 2, 5) = 1$. *O seu produto é o polinómio primitivo* $p(\boldsymbol{x})q(\boldsymbol{x}) = 15\boldsymbol{x}^4 + 16\boldsymbol{x}^3 + 38\boldsymbol{x}^2 + 16\boldsymbol{x} + 15$.

O lema seguinte é uma versão mais abstracta de 3.5.10. Mostra mais uma vez que os factores $a(\boldsymbol{x}) \in K[\boldsymbol{x}]$ de um polinómio $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$ são *associados* em $K[\boldsymbol{x}]$ dos factores que $p(\boldsymbol{x})$ tem no anel original $D[\boldsymbol{x}]$. Demonstramos este resultado aqui como um corolário directo de 3.8.2.

Lema 3.8.6. *Se* $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$, *e* $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x})$ *com* $a(\boldsymbol{x}), b(\boldsymbol{x}) \in K[\boldsymbol{x}]$, *então existem* $\tilde{a}(\boldsymbol{x}), \tilde{b}(\boldsymbol{x}) \in D[\boldsymbol{x}]$, *e* $k \in K$, *tais que*

$$p(\boldsymbol{x}) = \tilde{a}(\boldsymbol{x})\tilde{b}(\boldsymbol{x}),\ a(\boldsymbol{x}) = k\tilde{a}(\boldsymbol{x}),\ \text{e}\ b(\boldsymbol{x}) = k^{-1}\tilde{b}(\boldsymbol{x}).$$

Demonstração. Sabemos de 3.8.2 (i) que $a(\boldsymbol{x}) = sa'(\boldsymbol{x})$ e $b(\boldsymbol{x}) = tb'(\boldsymbol{x})$, onde $s, t \in K$ e $a'(\boldsymbol{x})$ e $b'(\boldsymbol{x})$ são polinómios primitivos em $D[\boldsymbol{x}]$. Por outro lado, temos ainda de 3.8.1 que $p(\boldsymbol{x}) = c(p)p'(\boldsymbol{x})$, onde $p'(\boldsymbol{x})$ é também primitivo em $D[\boldsymbol{x}]$. Concluímos que $p(\boldsymbol{x}) = c(p)p'(x) = sta'(\boldsymbol{x})b'(\boldsymbol{x})$. Como $a'(\boldsymbol{x})b'(\boldsymbol{x})$ é primitivo por 3.8.4 (ii), segue-se de 3.8.2 (ii) que existe uma unidade $u \in D$ tal que $c(p)u = st$, e $p'(\boldsymbol{x}) = u^{-1}a'(\boldsymbol{x})b'(\boldsymbol{x})$.

Definimos (por exemplo) $\tilde{a}(\boldsymbol{x}) = c(p)ua'(\boldsymbol{x})$ e $\tilde{b}(\boldsymbol{x}) = b'(\boldsymbol{x})$. Temos então

$$\tilde{a}(\boldsymbol{x})\tilde{b}(\boldsymbol{x}) = c(p)ua'(\boldsymbol{x})b'(\boldsymbol{x}) = sta'(\boldsymbol{x})b'(\boldsymbol{x}).$$

A constante referida no enunciado é aqui $k = \frac{c(p)u}{s}$, e $k^{-1} = \frac{1}{t}$. □

O Lema de Gauss neste contexto mais geral é idêntico ao que vimos no caso $D = \mathbb{Z}$.

Lema 3.8.7 (Gauss). *Se* $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$ *não é constante, então* $p(\boldsymbol{x})$ *é irredutível em* $D[\boldsymbol{x}]$ *se e só se é primitivo em* $D[\boldsymbol{x}]$, *e irredutível em* $K[\boldsymbol{x}]$.

Demonstração. Se $p(\boldsymbol{x})$ não é primitivo então tem uma decomposição não trivial em $D[\boldsymbol{x}]$, da forma $p(\boldsymbol{x}) = c(p)\tilde{p}(\boldsymbol{x})$. Por outro lado, se $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x})$ é uma factorização não trivial em $K[\boldsymbol{x}]$, então $p(\boldsymbol{x})$ tem uma factorização não trivial em $D[\boldsymbol{x}]$, como acabámos de ver em 3.8.6.

Se $p(\boldsymbol{x})$ é redutível em $D[\boldsymbol{x}]$, então tem uma factorização não trivial $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x})$ em $D[\boldsymbol{x}]$. Se um destes factores é uma constante não invertível, então $p(\boldsymbol{x})$ não é primitivo. Caso contrário, a factorização não é trivial em $K[\boldsymbol{x}]$. □

Finalmente, podemos demonstrar o

Teorema 3.8.8. *$D[\boldsymbol{x}]$ é um d.f.u. se só se D é um d.f.u.*

Demonstração. Seja $q(\boldsymbol{x}) \in D[\boldsymbol{x}]$ um polinómio não-nulo e não-invertível. Se o grau de $q(\boldsymbol{x})$ é zero, então $q(\boldsymbol{x})$ pode ser identificado com um elemento de D, e portanto é evidente que D é necessariamente um d.f.u., e nesse caso nada temos a provar. Seja então D um d.f.u., e $q(\boldsymbol{x}) \in D[\boldsymbol{x}]$ um polinómio de grau > 0.

Existência: Temos $q(\boldsymbol{x}) = c(q)p(\boldsymbol{x})$, com $p(\boldsymbol{x})$ primitivo. Como $K[\boldsymbol{x}]$ é um d.f.u., $q(\boldsymbol{x})$ tem uma factorização $q(\boldsymbol{x}) = \prod_{k=1}^{n} q_k(\boldsymbol{x})$, onde os polinómios $q_k(\boldsymbol{x}) \in K[\boldsymbol{x}]$ são irredutíveis em $K[\boldsymbol{x}]$, e $deg(q_k(\boldsymbol{x})) \geq 1$.

Existem polinómios primitivos $p_k(\boldsymbol{x}) \in D[\boldsymbol{x}]$ e constantes $s_k \in K$ tais que $q_k(\boldsymbol{x}) = s_k p_k(\boldsymbol{x})$. Sabemos do Lema de Gauss que os polinómios $p_k(\boldsymbol{x})$ são irredutíveis em $D[\boldsymbol{x}]$, e temos naturalmente

$$q(\boldsymbol{x}) = c(q)p(\boldsymbol{x}) = s\prod_{k=1}^{n} p_k(\boldsymbol{x}), \text{ onde } s = \prod_{k=1}^{n} s_k.$$

Por outro lado, $\prod_{k=1}^{n} p_k(\boldsymbol{x})$ é primitivo, de acordo com 3.8.4 (ii). Como vimos em 3.8.2 (ii), existe uma unidade $u \in D$ tal que $s = c(p)u$, e em particular $s \in D$. Factorizamos $s = \prod_{k=1}^{m} c_k$ em elementos irredutíveis $c_k \in D$, e é óbvio que

$$q(\boldsymbol{x}) = \left(\prod_{k=1}^{m} c_k\right)\left(\prod_{k=1}^{n} p_k(\boldsymbol{x})\right)$$

é uma factorização de $q(\boldsymbol{x})$ em elementos irredutíveis em $D[\boldsymbol{x}]$.

Unicidade: Seja agora $q(\boldsymbol{x}) = \prod_{k=1}^{m'} c'_k \prod_{k=1}^{n'} p'_k(\boldsymbol{x})$ outra factorização de $q(\boldsymbol{x})$ em polinómios irredutíveis em $D[\boldsymbol{x}]$, onde convencionamos n' e m' escolhidos de tal forma que $deg(p'_k(\boldsymbol{x})) \geq 1$, e $c'_k \in D$. É evidente do Lema de Gauss que os polinómios $p'_k(\boldsymbol{x})$ são primitivos e irredutíveis em $K[\boldsymbol{x}]$. Observamos finalmente que:

- $\prod_{k=1}^{n'} p'_k(\boldsymbol{x})$ é primitivo, donde $\prod_{k=1}^{m'} c'_k \sim c(q) \sim \prod_{k=1}^{m} c_k$ em D. Como D é um d.f.u., temos $m = m'$, e, após uma permutação conveniente duma destas factorizações, temos $c_k \sim c'_k$ em D.

- É claro que $\prod_{k=1}^{n} p_k(\boldsymbol{x}) \sim \prod_{k=1}^{n'} p'_k(\boldsymbol{x})$ em $K[\boldsymbol{x}]$. Como $K[\boldsymbol{x}]$ é um d.f.u., temos $n' = n$, e $p_k(\boldsymbol{x}) \sim p'_k(\boldsymbol{x})$ em $K[\boldsymbol{x}]$, também possivelmente após reordenar uma das factorizações. Pelo Corolário 3.8.3, temos igualmente $p_k(\boldsymbol{x}) \sim p'_k(\boldsymbol{x})$ em $D[\boldsymbol{x}]$.

□

Exercícios.

1. Mostre que, se $p(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ é um polinómio mónico com coeficientes inteiros, então qualquer raiz racional de $p(\boldsymbol{x})$ é inteira.

2. Seja D um domínio integral que possui algum elemento $d \neq 0$ não invertível. Mostre que $D[\boldsymbol{x}]$ não é um d.i.p.

3. Demonstre a seguinte generalização do Critério de Eisenstein: Seja D um d.f.u., $K = \mathrm{Frac}(D)$ e $p(\boldsymbol{x}) = a_0 + a_1\boldsymbol{x} + \cdots + a_n\boldsymbol{x}^n \in D[\boldsymbol{x}]$ com $n \geq 1$. Se $p \in D$ é um primo tal que $p|a_k$ para $0 \leq k < n$, $p \nmid a_n$ e $p^2 \nmid a_0$, então $p(\boldsymbol{x})$ é irredutível em $K[\boldsymbol{x}]$.

4. Mostre que o polinómio $p(\boldsymbol{x}, \boldsymbol{y}) = \boldsymbol{x}^3 + \boldsymbol{x}^2\boldsymbol{y} + \boldsymbol{x}\boldsymbol{y}^2 + \boldsymbol{y}$ é irredutível em $K[\boldsymbol{x}, \boldsymbol{y}]$.

5. Mostre que, se D é um d.f.u., e $p(\boldsymbol{x}) \in D[\boldsymbol{x}]$ é mónico, então todo o factor mónico de $p(\boldsymbol{x})$ em $K[\boldsymbol{x}]$ pertence a $D[\boldsymbol{x}]$.

6. Seja D um d.f.u., e $p(\boldsymbol{x}), q(\boldsymbol{x}) \in D[\boldsymbol{x}]$.
   (a) Existe sempre $\mathrm{mdc}(p(\boldsymbol{x}), q(\boldsymbol{x}))$ e $\mathrm{mmc}(p(\boldsymbol{x}), q(\boldsymbol{x}))$ em $D[\boldsymbol{x}]$?
   (b) Pode usar o algoritmo de Euclides para calcular $\mathrm{mdc}(p(\boldsymbol{x}), q(\boldsymbol{x}))$ em $D[\boldsymbol{x}]$?
   (c) A equação $\mathrm{mdc}(p(\boldsymbol{x}), q(\boldsymbol{x})) = a(\boldsymbol{x})p(\boldsymbol{x}) + b(\boldsymbol{x})q(\boldsymbol{x})$ tem sempre soluções $a(\boldsymbol{x}), b(\boldsymbol{x}) \in D[\boldsymbol{x}]$?
   (d) Temos $\mathrm{mdc}(p(\boldsymbol{x}), q(\boldsymbol{x})) \cdot \mathrm{mmc}(p(\boldsymbol{x}), q(\boldsymbol{x})) \sim p(\boldsymbol{x})q(\boldsymbol{x})$ em $D[\boldsymbol{x}]$?

7. Suponha que D é um d.f.u., e A é um anel de polinómios num número infinito de determinadas com coeficientes em D. A é um d.f.u.?

Capítulo 4

Quocientes e Isomorfismos

4.1 Grupos e Relações de Equivalência

O procedimento que seguimos no estudo dos anéis $\mathbb{Z}_m$ envolveu os seguintes passos fundamentais:

(i) A definição das relações de congruência módulo m ($x \equiv y \pmod{m} \Leftrightarrow y - x \in \langle m \rangle$), que como verificámos são relações de equivalência.

(ii) A introdução do conjunto quociente $\mathbb{Z}_m$, formado pelas classes de equivalência $\underline{x} = \{x + z : z \in \langle m \rangle\}$, que podemos escrever na forma $\underline{x} = x + \langle m \rangle$.

(iii) A definição de operações algébricas sobre classes de equivalência, a partir das operações algébricas sobre os elementos que as constituem, através das identidades $\underline{x} + \underline{y} = \underline{x + y}$ e $\underline{x}\,\underline{y} = \underline{xy}$.

Veremos abaixo que estes procedimentos são generalizáveis e aplicáveis em contextos mais gerais, e podem ser utilizados para definir muitos outros exemplos de estruturas algébricas.

Começamos por considerar em lugar do grupo aditivo $(\mathbb{Z}, +)$ um qualquer grupo $(G, \cdot)$, que escreveremos aqui em notação multiplicativa, por uma questão de generalidade (a possível comutatividade da operação em G é completamente irrelevante para as considerações que desejamos fazer). Em lugar de $\langle m \rangle$, que como sabemos é um subgrupo, subanel e ideal de $\mathbb{Z}$, consideramos um qualquer subgrupo $H \subset G$. Passamos a generalizar as relações de congruência, que estudámos a propósito dos inteiros, na seguinte forma:

Definição 4.1.1. Se $(G, \cdot)$ é um grupo, e $H \subset G$ é um subgrupo de G, definimos a RELAÇÃO DE CONGRUÊNCIA MÓDULO H como se segue:

$$g_1 \equiv g_2 \pmod{H} \iff g_2^{-1} \cdot g_1 \in H.$$

Notamos imediatamente que as congruências módulo m são, efectivamente, um caso particular da definição 4.1.1 (naturalmente escrita em notação aditiva, e especializada para $G = \mathbb{Z}$ e $H = \langle m \rangle$). Deixamos como exercício verificar que a relação agora definida com mais generalidade é sempre uma relação de equivalência.

Proposição 4.1.2. *Se $(G, \cdot)$ é um grupo, $H \subset G$ é um subgrupo, então $\equiv \pmod{H}$ é uma relação de equivalência em G.*

Continuando a seguir o exemplo do procedimento que utilizámos com os inteiros, observamos que, se $g \in G$, a classe de equivalência de g, designada por $\underline{g}$, pode ser descrita como se segue:

$$\begin{aligned} \underline{g} &= \{\tilde{g} \in G : \tilde{g} \equiv g\}, \\ &= \{\tilde{g} \in G : \tilde{g}^{-1} g = h \in H\}, \\ &= \{\tilde{g} \in G : g = \tilde{g} h, h \in H\}. \end{aligned}$$

Se A e B são subconjuntos do grupo G, vamos designar por AB o conjunto dos produtos de elementos em A por elementos em B, ou seja,

$$AB = \{a \cdot b : a \in A \text{ e } b \in B\}.$$

Se $A = \{a\}$ (respectivamente, $B = \{b\}$) é um conjunto singular, escrevemos aB (respectivamente, Ab) em lugar de AB. Deixamos para os exercícios a verificação que, em geral, $A(BC) = (AB)C$, e $AB \neq BA$.

Com estas convenções, passamos a representar a classe de equivalência de $g \in G$ para a congruência $\pmod{H}$ por gH, que se diz uma CLASSE LATERAL ESQUERDA de H[1]. O conjunto formado por todas as classes de equivalência $\{gH : g \in G\}$ diz-se naturalmente CONJUNTO QUOCIENTE de G por H, e designa-se por G/H. Temos portanto $G/H = \{gH : g \in G\}$. Finalmente, o número de elementos de G/H, que é o número de classes laterais esquerdas, diz-se ÍNDICE DO SUBGRUPO H no grupo G, e designa-se por $[G : H]$.

Exemplos 4.1.3.

1. *Consideramos o grupo simétrico $G = S_3 = \{I, \alpha, \beta, \gamma, \delta, \varepsilon\}$, e tomamos como subgrupo o grupo alternado $H = A_3 = \{I, \delta, \varepsilon\}$. Observe que:*

   - *A classe de equivalência de I é o conjunto $\underline{I} = IH = H = \{I, \delta, \varepsilon\}$. Concluímos imediatamente que $I \equiv \delta \equiv \varepsilon$, e $\underline{I} = \underline{\delta} = \underline{\varepsilon}$, ou ainda $H = \delta H = \varepsilon H$.*
   - *Tomando $g = \alpha$, é imediato que $\underline{\alpha} = \alpha H = \{\alpha I, \alpha\delta, \alpha\varepsilon\}$ e, calculando os produtos, obtemos $\underline{\alpha} = \{\alpha, \beta, \gamma\}$. Temos então que $\alpha \equiv \beta \equiv \gamma$, donde $\underline{\alpha} = \underline{\beta} = \underline{\gamma} = \{\alpha, \beta, \gamma\} = \alpha H = \beta H = \gamma H$.*

[1] Se o grupo G é aditivo, é conveniente escrever $A + B$ em lugar de AB, e $g + H$ em vez de gH. É claro que neste caso $A + B = B + A$, e $g + H = H + g$.

Assim, neste exemplo existem 2 classes de equivalência, cada uma com três elementos. O quociente S_3/A_3 é portanto o conjunto $S_3/A_3 = \{\underline{I}, \underline{\alpha}\} = \{A_3, \alpha A_3\}$, e $[S_3, A_3] = 2$.

2. *Consideremos ainda o grupo S_3, mas agora o subgrupo $H = \{I, \alpha\}$. Temos:*

$$\begin{aligned}
&\underline{I} = H, \text{ donde } I \equiv \alpha, \text{ e } \underline{I} = \underline{\alpha},\\
&\underline{\beta} = \beta H = \{\beta I, \beta\alpha\} = \{\beta, \varepsilon\}, \text{ donde } \beta \equiv \varepsilon \text{ e } \underline{\beta} = \underline{\varepsilon},\\
&\underline{\gamma} = \gamma H = \{\gamma I, \gamma\alpha\} = \{\gamma, \delta\}, \text{ donde } \gamma \equiv \delta \text{ e } \underline{\gamma} = \underline{\delta}.
\end{aligned}$$

Existem, pois, três classes de equivalência, com dois elementos cada, e $S_3/H = \{\underline{I}, \underline{\beta}, \underline{\gamma}\} = \{H, \beta H, \gamma H\}$. Temos obviamente $[S_3 : H] = 3$.

3. *É claro que o índice de $\langle m \rangle$ em $\mathbb{Z}$ é o número de elementos de $\mathbb{Z}_m$, ou seja, $[\mathbb{Z} : \langle m \rangle] = m$.*

Em lugar da Definição 4.1.1, é igualmente possível considerar a relação binária dada por

$$g_1 \equiv g_2 \pmod{H} \quad \Leftrightarrow \quad g_1 g_2^{-1} \in H.$$

Neste caso, obtemos ainda uma relação de equivalência (distinta da anterior, se a operação $\cdot$ não é comutativa), e a classe de equivalência de um elemento $g \in G$ é agora dada por

$$\begin{aligned}
\underline{g} &= \{\tilde{g} \in G : \tilde{g} \equiv g\}\\
&= \{\tilde{g} \in G : g\tilde{g}^{-1} = h \in H\}\\
&= \{\tilde{g} \in G : g = h\tilde{g}, h \in H\}.
\end{aligned}$$

Designamos esta classe de equivalência por Hg, que se diz uma CLASSE LATERAL DIREITA de H. O conjunto quociente das classes laterais direitas é designado por $H\backslash G$([2]). É interessante observar, usando os dois exemplos anteriores, que as classes laterais esquerdas e direitas podem ser iguais $Hg = gH$, para qualquer $g \in G$, como no Exemplo 4.1.3.1, ou distintas, como no Exemplo 4.1.3.2. Deixamos a verificação destas afirmações como exercício.

Sendo $\equiv$ uma qualquer relação de equivalência num conjunto X, sabemos que as respectivas classes de equivalência formam uma *partição* de X. Dito doutra forma, as classes de equivalência são subconjuntos disjuntos de X, cuja união é o conjunto X. É evidente que, se X é um conjunto finito, então cada classe de equivalência é igualmente um conjunto finito, e naturalmente neste caso existe apenas um número finito de classes de equivalência.

[2]Por defeito utilizaremos classes laterais esquerdas. Quando for claro que classes (esquerdas ou direitas) estamos a utilizar, poderemos representar o conjunto das classes laterais por $\frac{G}{H}$.

Designando por $X_1, X_2, \ldots, X_n$ as classes de equivalência que a relação $\equiv$ determina no conjunto X, temos que:

$$|X| = |X_1| + \cdots + |X_n| = \sum_{i=1}^{n} |X_i|. \tag{4.1.1}$$

Esta relação é por vezes designada por EQUAÇÃO DAS CLASSES.

No caso em que $X = G$ e a relação de equivalência é a de congruência (mod H), podemos ainda provar o seguinte resultado auxiliar, relativo ao número de elementos de cada classe de equivalência:

Proposição 4.1.4. *Se H é um subgrupo finito de G, então*

$$|gH| = |Hg| = |H|,$$

para todo o $g \in G$.

Demonstração. Dado um elemento $g \in G$ fixo, a função $\phi : H \to gH$ dada por $\phi(h) = g \cdot h$ é evidentemente sobrejectiva. Por outro lado, e de acordo com a lei do corte, é claro que ϕ é igualmente injectiva ($\phi(h) = \phi(h') \Rightarrow g \cdot h = g \cdot h' \Rightarrow h = h'$). Portanto, ϕ é uma bijecção entre os conjuntos H e gH. De forma análoga mostra-se que $|Hg| = |H|$. □

Esta observação elementar, combinada com a identidade (4.1.1), permite-nos provar:

Teorema 4.1.5 (Lagrange). *Se G é um grupo finito, e $H \subset G$ é um subgrupo, então:*

$$|G| = [G : H]|H|.$$

Em particular, tanto $|H|$ como $[G : H]$ são factores de $|G|$.

Demonstração. Sejam $g_1H, \ldots, g_nH$ as classes laterais esquerdas de H. Note que, como G e H são conjuntos finitos, existe apenas um número finito de classes, e na realidade $[G : H] = n$. A identidade (4.1.1) escreve-se agora

$$|G| = \sum_{i=1}^{n} |g_iH| = \sum_{i=1}^{n} |H| = n|H| = [G : H]|H|.$$

□

O número de elementos do grupo G diz-se usualmente a ORDEM DO GRUPO G. Portanto, e de acordo com o resultado anterior, a ordem de um grupo finito G é um múltiplo da ordem de qualquer um dos seus subgrupos. Analogamente, se $g \in G$ é um qualquer elemento do grupo G, então a ORDEM DO ELEMENTO g é a ordem do SUBGRUPO GERADO PELO ELEMENTO g, *i.e.*, é a ordem do subgrupo $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. É evidente que a ordem de qualquer elemento de G é igualmente um factor da ordem de G.

Exemplos 4.1.6.

1. *Regressando ao Exemplo 4.1.3.1 acima, temos que* $|G| = 6$, $|H| = 3$, *e* $[G : H] = 2$. *No caso do Exemplo 4.1.3.2, temos ainda* $|G| = 6$, *mas* $|H| = 2$ *e* $[G : H] = 3$.

2. *Se* $\pi \in S_3$, *é fácil verificar que a ordem de* π *pode ser* 3 *(caso de* δ *e* ε*),* 2 *(caso de* α, β, *e* γ*), e* 1 *(caso de* I*). Em qualquer um destes casos, é claro que a ordem de* π *é um factor da ordem de* S_3. *É também interessante que, apesar de* 6 *ser evidentemente factor da ordem de* S_3, *não existe em* S_3 *nenhum elemento de ordem 6.*

3. *No estudo dos anéis* $\mathbb{Z}_m$ *verificámos que os ideais de* $\mathbb{Z}_m$ *são da forma* $\langle \underline{d} \rangle$, *onde* d *é um divisor de* m. *É óbvio neste caso que o número de elementos do subgrupo* $\langle \underline{d} \rangle$ *é* $\frac{m}{d}$, *que é um factor de* m. *Note também que* $d = [\mathbb{Z}_m : \langle \underline{d} \rangle]$[3].

4. *Se* A *é um anel com identidade* I, *a ordem do subgrupo aditivo gerado por* I *é exactamente a característica do anel* A. *Podemos, pois, concluir que a característica de um anel finito* A *é um factor do número de elementos em* A.

Em muitos casos é importante estudar a factorização de grupos, *i.e.*, esclarecer em que condições um dado grupo G se pode escrever como o produto directo de outros grupos K e H. Estes funcionam como "blocos elementares", levando pois a um melhor conhecimento da estrutura do grupo, uma ideia que prosseguiremos no próximo capítulo. Indicamos aqui alguns resultados desta natureza. A sua aplicação a grupos finitos é, como veremos, frequentemente facilitada pelo Teorema de Lagrange.

Lema 4.1.7. *Seja* G *um grupo com identidade* e. *Se* K *e* H *são subgrupos normais de* G *tais que* $K \cap H = \{e\}$, *então* $kh = hk$ *para quaisquer* $k \in K$ *e* $h \in H$.

Demonstração. Sejam $k \in K$ e $h \in H$. Consideramos o elemento $k^{-1}h^{-1}kh$. Temos que $h^{-1}kh \in K$, porque K é normal em G, e portanto $k^{-1}h^{-1}kh \in K$. Analogamente $k^{-1}h^{-1}k \in H$, pois H é normal, e portanto $k^{-1}h^{-1}kh \in H$. Como $k^{-1}h^{-1}kh \in K \cap H = \{e\}$, temos $k^{-1}h^{-1}kh = e$, ou seja, $kh = hk$. □

Teorema 4.1.8. *Se* H *e* K *são subgrupos normais de* G, $G = HK$, *e* $H \cap K$ *se reduz à identidade de* G, *então* $G \simeq H \times K$.

Demonstração. Recordemos que o suporte do grupo $H \times K$ é o produto cartesiano $H \times K = \{(h, k) : h \in H, k \in K\}$, e que a respectiva operação binária é dada por $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$.

Definimos $\phi : H \times K \to G$ por $\phi(h, k) = hk$. Usando o Lema 4.1.7, é fácil verificar que ϕ é um homomorfismo de grupos. Como por hipótese $G = HK$, é também óbvio que ϕ é um homomorfismo sobrejectivo.

[3] Quando nos referimos ao "grupo $\mathbb{Z}_m$" sem mais qualificativo, queremos dizer o grupo aditivo $(\mathbb{Z}_m, +)$.

Para determinar o núcleo de ϕ, observamos que, se $\phi(h,k) = e$, então $hk = e$, ou ainda $h = k^{-1}$, donde concluímos (porquê?) que $h, k \in H \cap K = \{e\}$.

Segue-se finalmente que $h = k = e$, e o núcleo N de ϕ contém apenas o elemento (e, e), ou seja, ϕ é injectivo, e $G \simeq H \times K$. □

Como sugerimos acima, as hipóteses do teorema anterior podem, por vezes, ser verificadas para grupos finitos, recorrendo ao Teorema de Lagrange. Note, por exemplo, que se G é um grupo finito, então $|H \cap K|$ é factor de $|H|$ e de $|K|$. Portanto, se $|H|$ e $|K|$ são primos entre si, só podemos ter $|H \cap K| = 1$. Neste caso, o homomorfismo ϕ usado na demonstração anterior é injectivo, e podemos ainda concluir que $|HK| = |H||K|$, o que nos pode permitir decidir se $HK = G$.

Exemplo 4.1.9.

1. *Considerem-se o grupo $\mathbb{Z}_6$ e os subgrupos $H = \{0, 3\}$ e $K = \{0, 2, 4\}$. Sabemos que H e K são isomorfos respectivamente a $\mathbb{Z}_2$ e $\mathbb{Z}_3$. É imediato que $H \cap K = \{0\}$, e $|G| = |H||K|$. Concluímos que $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_3$.*

2. *Mais geralmente, suponha-se que* $\mathrm{mdc}(n, d) = 1$*, e recorde-se a proposição (3.1.23): sendo $m = nd$, o grupo $\mathbb{Z}_m$ tem subgrupos $B \simeq \mathbb{Z}_n$ e $C \simeq \mathbb{Z}_d$. Como $|B \cap C|$ é factor de n e de d, e por hipótese* $\mathrm{mdc}(n, d) = 1$*, é claro que $|B \cap C| = 1$, e portanto $|B + C| = |B||C| = nd = m = |\mathbb{Z}_m|$, ou seja, $B + C = \mathbb{Z}_m$. Concluímos mais uma vez que $\mathbb{Z}_m \simeq B \oplus C \simeq \mathbb{Z}_n \oplus \mathbb{Z}_d$.*

O teorema anterior pode ser generalizado para produtos directos com mais de dois grupos. A respectiva demonstração é em tudo análoga à anterior, e fica como exercício.

Teorema 4.1.10. *Sejam $H_1, \ldots, H_n$ subgrupos normais de um grupo G tais que $G = H_1 \cdots H_n$, e seja ainda*

$$K_i = \prod_{\substack{k=1 \\ k \neq i}} H_k.$$

Se, para $i = 1, \ldots, n$, $H_i \cap K_i = \{e\}$ se reduz à identidade de G, então $G \simeq H_1 \times \cdots \times H_n$.

Exercícios.

1. Demonstre a Proposição 4.1.2.

2. Verifique que $\{gH : g \in G\} \neq \{Hg : g \in G\}$, quando $G = S_3$ e $H = \{I, \alpha\}$.

3. Mostre que, se e é a identidade de G, então $g \equiv e$ se e só se $g \in H$.

4. Determine o conjunto quociente G/H quando $G = \mathbb{Z}_6$ e $H = \langle 2 \rangle$.

5. Determine o conjunto quociente G/H quando $G = S_4$ e $H = \langle (1234) \rangle$.

6. Determine a ordem dos elementos dos grupos S_3, $(\mathbb{Z}_6, +)$ e $(\mathbb{Z}_9^*, \cdot)$.

7. Sendo $G = S_n$ e $H = A_n$, prove que $\pi \equiv \sigma \pmod{H}$ se e só se π e σ são permutações com a mesma paridade, para concluir que $[S_n : A_n] = 2$.

8. Mostre que a função $\phi : G/H \to \{Hg : g \in G\}$ dada por $\phi(g) = Hg^{-1}$ está bem definida, e é uma bijecção. Conclua que $[G : H]$ é também o número de classes laterais direitas.

9. Prove que, se $K \subset H$ onde K e H são subgrupos de um grupo finito G, então $[G : K] = [G : H][H : K]$.

10. Sendo A, B e C subconjuntos do grupo G, mostre que:
    (a) $(AB)C = A(BC)$.
    (b) $AA = A$ quando A é subgrupo de G.
    (c) Se A e B são subgrupos de G, então $AB = BA$ se e só se AB é um subgrupo de G.

11. Prove que, se A e B são subgrupos finitos de G, então $|AB||A \cap B| = |A||B|$. (SUGESTÃO: comece por usar o facto de $A \cap B$ ser subgrupo de A.)

12. Mostre que qualquer permutação de S_3 é da forma $\pi = \alpha^n \varepsilon^m$.

13. Se $|G| = p$, onde p é um número primo, quais são os subgrupos de G, e qual é a ordem dos elementos de G?

14. Dê um exemplo de um grupo infinito, com todos os elementos de ordem 2, à excepção da identidade.

15. Dê um exemplo de um grupo infinito, com todos os elementos de ordem finita, mas contendo elementos de ordem n, para qualquer natural n.

16. Prove o Teorema 4.1.10.

17. Este exercício refere-se à decomposição de grupos em produtos directos de outros grupos. Suponha que G é isomorfo a $H \times K$, e prove que existem subgrupos normais H' e K' de G tais que $H'K' = G$ e $H' \cap K' = \{e\}$, onde e é a identidade de G.

18. Prove que, se A é um anel finito com identidade, então a característica de A é um factor de $|A|$.

19. Classifique os anéis com identidade, com $2, 3, 4$ e 5 elementos. (SUGESTÃO: use o exercício anterior.)

20. Suponha que G é um grupo abeliano com 9 elementos, que não contem nenhum elemento com ordem 9. Prove que $G \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

21. Mostre que, se G é um grupo finito onde todos os elementos, excepto a identidade, têm ordem 2, então G é abeliano. O que é que pode dizer, se todos os elementos diferentes da identidade tiverem ordem 3?

22. Suponha que G é um grupo com ordem $2n$, e prove que existe pelo menos um elemento em G que tem ordem 2. SUGESTÃO: Dado $x \in G$, definimos $C(x) = \{x, x^{-1}\}$. Definimos ainda $x \sim y \Leftrightarrow C(x) = C(y)$. Mostre que esta é uma relação de equivalência, e $C(x)$ é a classe de equivalência de x.

4.2 Grupos e Anéis Quocientes

Vimos, no capítulo anterior, que é possível definir operações algébricas em $\mathbb{Z}_m$ a partir das operações algébricas definidas em $\mathbb{Z}$. Interessa-nos agora investigar se este mecanismo para a definição de operações algébricas no quociente $\mathbb{Z}_m$ pode igualmente ser generalizado para a definição de operações no quociente G/H, a partir das operações já existentes em G.

Esta generalização é possível, com algumas restrições no subgrupo H. Na realidade, e como verificamos adiante, é possível definir um grupo com suporte em G/H, desde que H seja um subgrupo *normal* de G [4].

A técnica que utilizámos para definir a adição no caso de $\mathbb{Z}_m$ baseou-se no seguinte resultado:

$$\text{(4.2.1)} \qquad \text{Se } \begin{cases} x \equiv x' \pmod m \\ y \equiv y' \pmod m \end{cases}, \text{ então } x + y \equiv x' + y' \pmod m.$$

Este resultado implicava, que dados elementos $\underline{x}$ e $\underline{y}$ de $\mathbb{Z}_m$, podíamos definir

$$\underline{x} + \underline{y} = \underline{x + y}$$

sem quaisquer dificuldades relacionadas com a escolha dos representantes x e y de cada uma das classes de equivalência envolvidas. No entanto, o exemplo seguinte mostra que a propriedade (4.2.1) não é completamente geral.

Exemplo 4.2.1.

Se $G = S_3$, $H = \{I, \alpha\}$, podemos ter $g_1 \equiv g_1' \pmod H$ e $g_2 \equiv g_2' \pmod H$ sem que tenhamos $g_1 g_2 \equiv g_1' g_2' \pmod H$. Para verificar esta afirmação, basta tomarmos $g_1 = g_1' = \alpha$, $g_2 = \gamma$, e $g_2' = \delta$, porque $\gamma \equiv \delta \pmod H$, mas $\alpha\gamma = \varepsilon$ e $\alpha\delta = \gamma$ não são equivalentes.

[4] Note no entanto que esta restrição não tem quaisquer reflexos sobre o exemplo de $\mathbb{Z}_m$: como $(\mathbb{Z}, +)$ é um grupo abeliano, qualquer um dos seus subgrupos é necessariamente normal.

De facto, o análogo da propriedade (4.2.1) verifica-se apenas para subgrupos normais:

Proposição 4.2.2. *Se H é um subgrupo de G, as seguintes afirmações são equivalentes:*

(i) H *é um subgrupo normal de* G*;*

(ii) $gHg^{-1} = H$ *para qualquer* $g \in G$*;*

(iii) $Hg = gH$ *para qualquer* $g \in G$*;*

(iv) $(g_1H)(g_2H) = (g_1g_2)H$ *para quaisquer* $g_1, g_2 \in G$*;*

(v) se $g_1 \equiv g_1' \pmod{H}$ *e* $g_2 \equiv g_2' \pmod{H}$*, então* $g_1g_2 \equiv g_1'g_2' \pmod{H}$ *para quaisquer* $g_1, g_2, g_1', g_2' \in G$*.*

Demonstração. Vamos provar as implicações

$$\text{(i)} \Rightarrow \text{(ii)} \Rightarrow \text{(iii)} \Rightarrow \text{(iv)} \Rightarrow \text{(v)} \Rightarrow \text{(i)}.$$

(i) $\Rightarrow$ (ii): É claro, da definição de subgrupo normal, que

$$gHg^{-1} \subset H.$$

Como g é arbitrário, podemos ainda substituir g por g^{-1} para obter igualmente $g^{-1}Hg \subset H$. Observamos também que

$$g^{-1}Hg \subset H \quad \Longrightarrow \quad g(g^{-1}Hg)g^{-1} \subset gHg^{-1} \quad \Longrightarrow \quad H \subset gHg^{-1}.$$

Como já vimos que $gHg^{-1} \subset H$, podemos concluir que $gHg^{-1} = H$.

(ii) $\Rightarrow$ (iii): Como $gHg^{-1} = H$, é imediato que

$$(gHg^{-1})g = Hg, \text{ ou seja, } gH = Hg.$$

(iii) $\Rightarrow$ (iv):

$$\begin{aligned}(g_1H)(g_2H) =&((g_1H)g_2)H = (g_1(Hg_2))H = (g_1(g_2H))H\\ =&((g_1g_2)H)H = (g_1g_2)(HH) = (g_1g_2)H.\end{aligned}$$

(iv) $\Rightarrow$ (v):

$$g_1 \equiv g_1' \pmod{H} \text{ e } g_2 \equiv g_2' \pmod{H} \Rightarrow g_1' \in g_1H \text{ e } g_2' \in g_2H.$$

Portanto $g_1'g_2' \in (g_1H)(g_2H)$. Como $(g_1H)(g_2H) = (g_1g_2)H$, temos

$$g_1'g_2' \in (g_1g_2)H \Leftrightarrow g_1g_2 \equiv g_1'g_2' \pmod{H}.$$

(v) $\Rightarrow$ (i): Sendo $g \in G$ e $h \in H$, temos a provar que $ghg^{-1} \in H$. Consideramos para isso $g' = gh$, donde $g' \equiv g \pmod{H}$. Concluímos que $g'g^{-1} \equiv gg^{-1} = e$, onde $e \in G$ é o elemento identidade. Portanto $e^{-1}g'g^{-1} = ghg^{-1} \in H$ como se desejava. □

De acordo com o resultado anterior, se H é um subgrupo normal de G, então a operação $(g_1H)(g_2H) = (g_1g_2)H$ é uma operação binária em G/H. É imediato verificar que:

Teorema 4.2.3. *Se H é um subgrupo normal de G, então G/H é um grupo com a operação binária definida por*

$$(g_1H)(g_2H) = (g_1g_2)H.$$

Temos, além disso, que a aplicação quociente $\pi : G \to G/H$ *dada por $\pi(g) = \underline{g} = gH$ é um homomorfismo de grupos, e o respectivo núcleo $N(\pi)$ é o subgrupo H.*

Demonstração. Vimos, acima, que a operação de $G/H \times G/H \to G/H$ definida por $(g_1H, g_2H) \to (g_1H)(g_2H) = (g_1g_2)H$ é uma operação binária em G/H.

Esta operação é *associativa*, dado que:

$$\begin{aligned}((g_1H)(g_2H))\,(g_3H) &= ((g_1g_2)H)\,(g_3H)\\ &= ((g_1g_2)g_3)\,H\\ &= (g_1(g_2g_3))\,H\\ &= (g_1H)\,((g_2g_3)H)\\ &= (g_1H)\,((g_2H)(g_3H))\,.\end{aligned}$$

Sendo e a identidade de G, temos naturalmente $eH = H$, e $(gH)H = H(gH) = gH$, e portanto H é a *identidade* em G/H.

É também claro que $(gH)(g^{-1}H) = (g^{-1}H)(gH) = eH = H$, e portanto qualquer elemento de G/H tem *inverso*. Consequentemente, G/H é um grupo.

Sendo $\pi : G \to G/H$ dada por $\pi(g) = \underline{g} = gH$, é imediato que $\pi(g_1)\pi(g_2) = (g_1H)(g_2H) = (g_1g_2)H = \pi(g_1g_2)$, donde π é um homomorfismo de grupos. Finalmente, e como H é a identidade de G/H, temos $N(\pi) = \{g \in G : gH = H\} = H$. □

Exemplos 4.2.4.

1. *Se $G = S_3$ e $H = A_3$, então $G/H = \{\underline{I}, \underline{\alpha}\}$, e temos a tabuada*

$$\begin{aligned}\underline{I}\ \underline{I} = \underline{\alpha}\ \underline{\alpha} = \underline{I},\\ \underline{I}\ \underline{\alpha} = \underline{\alpha}\ \underline{I} = \underline{\alpha}.\end{aligned}$$

2. *Se $G = \mathbb{Z}_6$ e $H = \langle 2\rangle = \{0, 2, 4\}$, então $G/H = \{\underline{0}, \underline{1}\}$, onde*

$$\begin{aligned}\underline{0} &= 0 + \langle 2\rangle = \{0, 2, 4\}\\ \underline{1} &= 1 + \langle 2\rangle = \{1, 3, 5\}.\end{aligned}$$

Temos neste caso a tabuada

$$\underline{0}+\underline{0}=\underline{1}+\underline{1}=\underline{0},$$
$$\underline{0}+\underline{1}=\underline{1}+\underline{0}=\underline{1}.$$

É claro que este grupo é isomorfo ao grupo anterior (existe apenas um grupo com dois elementos!).

Deixamos para os exercícios a demonstração do seguinte resultado auxiliar:

Teorema 4.2.5. *Se H é um subgrupo normal de G, então os subgrupos (respectivamente, normais) de G/H são da forma K/H, onde $H \subseteq K \subseteq G$, e K é qualquer subgrupo (respectivamente, normal) de G.*

O caso dos anéis é um pouco mais complexo. É por um lado claro que se $B \subset A$ é um subanel de A, então $(B,+)$ é subgrupo de $(A,+)$, e podemos naturalmente formar o grupo quociente A/B: afinal, e como $(A,+)$ é um grupo abeliano, qualquer subgrupo de $(A,+)$ é normal, e qualquer subanel B é automaticamente um subgrupo normal de $(A,+)$. A "soma" em A/B é, como vimos acima, dada por $\underline{a_1}+\underline{a_2}=\underline{a_1+a_2}$ ou $(a_1+B)+(a_2+B)=(a_1+a_2)B$. Não se segue daqui que A/B seja um anel: para isso, é necessário que possamos igualmente definir uma operação "produto" em A/B, de modo a respeitar as propriedades dos anéis.

Recordemos que a técnica que utilizámos para definir o produto no caso de $\mathbb{Z}_m$ se baseou no seguinte resultado:

$$\text{(4.2.2)} \qquad \text{Se } \begin{cases} x \equiv x' \pmod m \\ y \equiv y' \pmod m \end{cases}, \text{ então } xy \equiv x'y' \pmod m.$$

Este resultado implicava que, dados elementos $\underline{x}$ e $\underline{y}$ de $\mathbb{Z}_m$, podíamos definir

$$\underline{x}\,\underline{y}=\underline{xy}$$

sem quaisquer dificuldades relacionadas com a escolha dos representantes x e y de cada uma das classes de equivalência envolvidas. Por analogia, o procedimento natural a seguir no caso dum anel A com subanel $B \subset A$ é fazer $\underline{a_1}\,\underline{a_2}=\underline{a_1\,a_2}$, ou $(a_1+B)(a_2+B)=a_1a_2+B$. No entanto, tal procedimento só é aplicável se $a_1 \equiv a_1' \pmod B$ e $a_2 \equiv a_2' \pmod B$ implica $a_1a_2 \equiv a_1'a_2'$. Caso contrário, o resultado da operação depende de uma escolha arbitrária dos representantes a_1 e a_2. Este problema é completamente esclarecido pela seguinte:

Proposição 4.2.6. *Se B é um subanel de A e $a \equiv a' \pmod B$ se e só se $a'-a \in B$, então as seguintes afirmações são equivalentes:*

(i) B é um ideal de A;

(ii) Se $a_1 \equiv a_1' \pmod{B}$ *e* $a_2 \equiv a_2' \pmod{B}$ *então* $a_1a_2 \equiv a_1'a_2' \pmod{B}$, *para quaisquer* $a_1, a_1', a_2, a_2' \in G$.

Demonstração. Vejamos que ambas as implicações são verdadeiras.

(i) $\Rightarrow$ (ii): Se $a_1 \equiv a_1' \pmod{B}$ e $a_2 \equiv a_2' \pmod{B}$, então $a_1' = a_1 + b_1$ e $a_2' = a_2 + b_2$, onde $b_1, b_2 \in B$. Portanto, $a_1'a_2' = (a_1 + b_1)(a_2 + b_2) = a_1a_2 + a_1b_2 + a_2b_1 + b_1b_2$. É claro que $b_1b_2 \in B$, porque B é um subanel, e $a_1b_2, a_2b_1 \in B$, porque B é um ideal. Concluímos que $a_1'a_2' = a_1a_2 + b$, onde $b = a_1b_2 + a_2b_1 + b_1b_2 \in B$, e portanto $a_1a_2 \equiv a_1'a_2' \pmod{B}$.

(ii) $\Rightarrow$ (i): Temos a provar que, se $a \in A$ e $b \in B$, então $ab, ba \in B$. Para isso, basta-nos observar que $b \in B$ sse $b \equiv 0 \pmod{B}$, onde 0 é o zero do anel A. De acordo com (ii), temos então $ab \equiv a0 \pmod{B}$ e $ba \equiv 0a \pmod{B}$, ou seja, $ab \equiv 0 \pmod{B}$ e $ba \equiv 0 \pmod{B}$. Concluímos por isso que $ab, ba \in B$, e B é um ideal. □

O próximo resultado é o análogo do Teorema 4.2.3, agora especializado para o caso dos anéis. A sua demonstração fica como exercício.

Teorema 4.2.7. *Se* $I \subset A$ *é um ideal do anel* A, *então* A/I *é um anel para as operações* $\underline{a_1} + \underline{a_2} = \underline{a_1 + a_2}$ *e* $\underline{a_1}\ \underline{a_2} = \underline{a_1a_2}$. *Se* A *é abeliano (respectivamente, com identidade* 1*), então* A/I *é um anel abeliano (respectivamente, com identidade* $\underline{1}$*). Além disso, a aplicação quociente* $\pi : A \to A/I$ *dada por* $\pi(a) = \underline{a} = a + I$ *é um homomorfismo de anéis, e o respectivo núcleo* $N(\pi)$ *é o ideal* I.

Os exemplos seguintes mostram que muitas das propriedades do anel A *não* passam ao quociente.

Exemplos 4.2.8.

1. *Os anéis* $\mathbb{Z}_m$ *são claramente casos particulares de aplicação do teorema anterior. Referem-se evidentemente à escolha* $A = \mathbb{Z}$ *e* $I = \langle m \rangle$, *onde* m *é um inteiro fixo. Neste caso,* A *é sempre um domínio integral, enquanto que o quociente* A/I *possui divisores de zero, se* m *não é primo.*

2. *Tomemos* $A = \mathbb{Q}[\boldsymbol{x}]$ *e* $I = \langle m(\boldsymbol{x}) \rangle$ *onde* $m(\boldsymbol{x}) = \boldsymbol{x}^2 + 1$. *Dado* $p(\boldsymbol{x}) \in \mathbb{Q}[\boldsymbol{x}]$, *sabemos do algoritmo de divisão que existe* $q(\boldsymbol{x}) \in \mathbb{Q}[\boldsymbol{x}]$ *tal que*

$$p(\boldsymbol{x}) = q(\boldsymbol{x})(\boldsymbol{x}^2 + 1) + (a + b\boldsymbol{x}), \qquad (a, b \in K[\boldsymbol{x}]),$$

onde obviamente $q(\boldsymbol{x})(\boldsymbol{x}^2 + 1) \in I$. *Assim* $p(\boldsymbol{x}) \equiv a + b\boldsymbol{x}$, i.e., $\underline{p(\boldsymbol{x})} = \underline{a + b\boldsymbol{x}}$, *e concluímos que*

$$\frac{\mathbb{Q}[\boldsymbol{x}]}{\langle \boldsymbol{x}^2 + 1 \rangle} = \{a + b\boldsymbol{x} : a, b \in \mathbb{Q}\}.$$

As operações algébricas neste anel são fáceis de determinar. A soma deve ser calculada como se segue:

$$\begin{aligned} \underline{a + b\boldsymbol{x}} + \underline{a' + b'\boldsymbol{x}} &= \underline{a + b\boldsymbol{x} + a' + b'\boldsymbol{x}} \\ &= \underline{(a + a') + (b + b')\boldsymbol{x}}. \end{aligned}$$

Para o produto, observamos primeiro que $\boldsymbol{x}^2+1 \equiv 0$, *ou seja,* $\underline{x}^2 = \underline{-1}$. *Temos portanto:*

$$\begin{aligned}\underline{(a+b\boldsymbol{x})(a'+b'\boldsymbol{x})} &= \underline{(a+b\boldsymbol{x})}\underline{(a'+b'\boldsymbol{x})},\\ &= \underline{aa' + (ba'+ab')\boldsymbol{x} + bb'\boldsymbol{x}^2},\\ &= \underline{(aa'-bb') + (ba'+ab')\boldsymbol{x}}.\end{aligned}$$

Para simplificar a notação utilizada, escrevemos a *em lugar de* $\underline{a}$, *e* i *em lugar de* $\underline{\boldsymbol{x}}$ *(note que* $\underline{a} = \underline{b}$ *se e só se* $a = b$*). Nesta notação, as operações algébricas acima calculam-se como se segue:*

$$\begin{aligned}(a+bi) + (a'+b'i) &= (a+a') + (b+b')i,\\ (a+bi)(a'+b'i) &= (aa'-bb') + (ab'+a'b)i.\end{aligned}$$

Deve ser por isso claro que $\mathbb{Q}[\boldsymbol{x}]/\langle \boldsymbol{x}^2+1\rangle$ *é isomorfo a* $\mathbb{Q}[i]$, *uma "coincidência" explicada mais adiante. Observamos desde já que* $\mathbb{Q}[\boldsymbol{x}]/\langle \boldsymbol{x}^2+1\rangle$ *é um corpo e uma extensão de* $\mathbb{Q}$. *Note que nesta extensão o polinómio* $\boldsymbol{x}^2+1$ *tem raízes e é redutível.*

O próximo exemplo mostra que o mesmo fenómeno ocorre em corpos K *finitos.*

3. *Tomamos* $A = \mathbb{Z}_2[\boldsymbol{x}]$ *e* $I = \langle \boldsymbol{x}^2+\boldsymbol{x}+1\rangle$. *Tal como acima, se* $p(\boldsymbol{x}) \in \mathbb{Z}_2[\boldsymbol{x}]$, *então existe* $q(\boldsymbol{x}) \in \mathbb{Z}_2[\boldsymbol{x}]$ *tal que*

$$p(\boldsymbol{x}) = q(\boldsymbol{x})(\boldsymbol{x}^2+\boldsymbol{x}+1) + (a+bx).$$

Mais uma vez, $p(\boldsymbol{x}) \equiv a+b\boldsymbol{x}$, i.e., $\underline{p(\boldsymbol{x})} = \underline{a+b\boldsymbol{x}}$, *o que neste caso conduz a um anel finito com 4 elementos.*

$$\frac{\mathbb{Z}_2[\boldsymbol{x}]}{\langle \boldsymbol{x}^2+\boldsymbol{x}+1\rangle} = \{\underline{a+b\boldsymbol{x}} : a,b \in \mathbb{Z}_2\} = \{\underline{0},\underline{1},\underline{x},\underline{1+\boldsymbol{x}}\}.$$

Escrevemos ainda a *em lugar de* $\underline{a}$, *e* α *em lugar de* $\underline{x}$, *donde* $1+\alpha+\alpha^2 = 0$, *ou ainda* $\alpha^2 = -1-\alpha = 1+\alpha$. *(Como* $a = -a$ *no corpo* $\mathbb{Z}_2$, *temos também* $\underline{a} = -\underline{a}$ *no anel quociente). Neste caso, podemos exibir as tabuadas completas deste anel, onde por conveniência escrevemos* $\beta = \alpha^2 = 1+\alpha$. *É fácil verificar que estas tabelas são as do corpo de 4 elementos que referimos num exercício do Capítulo 1.*

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Este corpo é uma extensão do corpo $\mathbb{Z}_2$, *e neste corpo o polinómio* $\boldsymbol{x}^2+\boldsymbol{x}+1$ *tem raízes, e é redutível.*

Deixamos para os exercícios, verificar que em geral o anel quociente $K[\boldsymbol{x}]/\langle m(\boldsymbol{x})\rangle$ é sempre uma extensão do corpo K (e também um espaço vectorial de dimensão n sobre K, onde n é o grau do polinómio $m(\boldsymbol{x})$).

Nos exemplos apresentados acima, o anel quociente obtido é sempre um corpo. Por outro lado, vimos, quando estudámos os anéis $\mathbb{Z}_m$, que estes anéis são corpos precisamente quando m é um número primo, o que ocorre exactamente quando $\langle m\rangle$ é um ideal maximal de $\mathbb{Z}$. Podemos agora mostrar como estes factos estão relacionados.

Teorema 4.2.9. *Se A é um anel abeliano unitário, e $I \subsetneq A$ é um ideal de A, o quociente A/I é um corpo se e só se I é um ideal maximal de A.*

Demonstração. Supomos primeiro que I é um ideal maximal de A. Temos a provar que A/I tem identidade $\underline{1} \neq \underline{0}$, e que, se $\underline{a} \neq \underline{0}$, então existe $x \in A$ tal que $\underline{ax} = \underline{1}$.

Notamos, primeiro, que $1 \notin I$, *i.e.*, $\underline{1} \neq \underline{0}$, pois caso contrário teríamos $I = A$. (Porquê?) Sendo $\underline{a} \neq \underline{0}$, *i.e.*, $a \notin I$, consideramos o conjunto $J = \{ax + b : x \in A \text{ e } b \in I\}$. É claro que $a \in J$, e portanto $J \neq I$. É também claro que $I \subset J$. Como A é abeliano, é imediato verificar que J é um ideal de A, e como I é um ideal maximal concluímos que $J = A$. Como $1 \in A$, temos $1 \in J$, e portanto existe $x \in A$ e $b \in I$ tal que $1 = ax + b$, ou $\underline{ax} = \underline{1}$.

Reciprocamente, suponhamos agora que A/I é um corpo e seja $\pi : A \to A/I$ a aplicação quociente. Se $J \supsetneq I$ é um ideal de A que contém I, então $\pi(J) \subset A/I$ é um ideal $\neq \{0\}$. Como A/I é um corpo, $\pi(J) = A/I$. Existe pois $a \in J$ tal que $a \equiv 1$, *i.e.*, $1 = a + b$, com $b \in I$. Como $I \subset J$, concluímos que $1 \in J$, logo $J = A$. Portanto, I é um ideal maximal. □

Se D é um domínio integral, então $D[\boldsymbol{x}]$ é um domínio integral, e $m(\boldsymbol{x})$ é irredutível se e só se $\langle m(\boldsymbol{x})\rangle$ é um ideal maximal na classe dos ideais principais de $D[\boldsymbol{x}]$ (ver Proposição 3.7.3). Se $D = K$ é um corpo, $K[\boldsymbol{x}]$ é um d.i.p., logo, aplicando o teorema acima, obtemos imediatamente o seguinte:

Corolário 4.2.10. *O anel $K[\boldsymbol{x}]/\langle m(\boldsymbol{x})\rangle$ é um corpo se e só se $m(\boldsymbol{x})$ é irredutível em $K[\boldsymbol{x}]$.*

Este corolário mostra a razão pela qual os exemplos anteriores são corpos, e pode ser usado, pois, para criar extensões de corpos conhecidos, e em particular construir novos corpos. O Teorema 4.2.9, pode por seu lado, ser usado para definir os números reais em termos dos números racionais, permitindo-nos verificar finalmente que a usual axiomática dos reais é também consequência dos axiomas para os inteiros que apresentámos no Capítulo 2, o que faremos na próxima secção. Aí introduziremos também uma definição formal dos complexos, identificados como o quociente de $\mathbb{R}[\boldsymbol{x}]$ por $\langle \boldsymbol{x}^2 + 1\rangle$.

Exercícios.

1. Prove que, se H é um subgrupo de G e $[G : H] = 2$, então H é um subgrupo normal de G.

2. Prove que N é um subgrupo normal de G se e só se existe um grupo H e um homomorfismo $\phi : G \to H$ tal que N é o núcleo de ϕ.

3. Seja N um subgrupo normal de G, e $\pi : G \to G/N$ a aplicação quociente.

   (a) Prove que, se $N \subset H \subset G$ onde H é um subgrupo de G, então N é um subgrupo normal de H, e H/N é um subgrupo de G/N.

   (b) Mostre que os subgrupos de G/N são da forma H/N, onde H é um subgrupo de G que contém N.

4. Seja N um subgrupo normal de G, e $x \in G$.

   (a) Supondo que a ordem de x em G é finita e igual a m, prove que a ordem de $\underline{x}$ em G/N é finita e divide m.

   (b) Mostre que se a ordem de x em G é infinita então a ordem de $\underline{x}$ em G/N pode ser finita ou infinita.

5. Sendo A um anel e I um ideal de A, mostre que a operação de produto no anel A/I, dada como vimos por $(a_1+I)(a_2+I) = a_1a_2+I$, não corresponde em geral ao produto de conjuntos que definimos como $CD = \{cd : c \in C \text{ e } d \in D\}$.

6. Demonstre o Teorema 4.2.7.

7. Prove que a função $\phi : \mathbb{Q} \oplus \mathbb{Q} \to \mathbb{Q}[\boldsymbol{x}]/\langle \boldsymbol{x}^2 + 1\rangle$, dada por $\phi(a, b) = \underline{a\boldsymbol{x} + b}$, é uma bijecção.

8. Determine as tabuadas da soma e do produto no anel $\mathbb{Z}_2[\boldsymbol{x}]/\langle \boldsymbol{x}^2 + 1\rangle$, e verifique directamente que este anel não é um corpo. Porque é que este resultado não contradiz o Teorema 4.2.9?

9. Considere o anel $\mathbb{Q}[\boldsymbol{x}]/\langle m(\boldsymbol{x})\rangle$, onde $m(\boldsymbol{x}) = \boldsymbol{x}^6 + \boldsymbol{x}^4 + \boldsymbol{x}^2 + 1$. Determine o inverso de $\underline{\boldsymbol{x} + 2}$. Verifique se este anel tem divisores de zero, e, caso afirmativo, dê um exemplo.

10. Mostre que $\mathbb{Q}[\boldsymbol{x}]/\langle \boldsymbol{x}^2 - 3\boldsymbol{x} + 2\rangle$ é isomorfo a $\mathbb{Q} \oplus \mathbb{Q}$. SUGESTÃO: Mostre que a função $\phi : \mathbb{Q}[\boldsymbol{x}]/\langle \boldsymbol{x}^2 - 3\boldsymbol{x} + 2\rangle \to \mathbb{Q} \oplus \mathbb{Q}$ dada por $\phi(\underline{p(x)}) = (p(1), p(2))$ está bem definida, e é um isomorfismo de anéis.

11. Sendo $L = \mathbb{Z}_2[\boldsymbol{x}]/\langle \boldsymbol{x}^2 + \boldsymbol{x} + 1\rangle$, factorize o polinómio $\boldsymbol{x}^2 + \boldsymbol{x} + 1$ em $L[\boldsymbol{x}]$.

12. Seja $m(\boldsymbol{x})$ um polinómio irredutível de grau n em $K[\boldsymbol{x}]$, e $L = K[\boldsymbol{x}]/\langle m(\boldsymbol{x})\rangle$. Prove que:

   (a) L é um corpo e um espaço vectorial de dimensão n sobre K;

   (b) o corpo L é uma extensão algébrica de K;

   (c) $m(\boldsymbol{x})$ tem pelo menos uma raiz em L;

   (d) existe uma extensão algébrica de K, onde $m(\boldsymbol{x})$ é um produto de factores de grau 1.

13. Verifique que o polinómio $\boldsymbol{x}^3+\boldsymbol{x}^2+1$ é irredutível em $\mathbb{Z}_2[\boldsymbol{x}]$. Aproveite este facto para determinar as tabuadas de um corpo L com 8 elementos. Factorize o polinómio $\boldsymbol{x}^3+\boldsymbol{x}^2+1$ em L.

14. Seja $I \subset A$ um ideal, e $\pi : A \to A/I$ a aplicação quociente $\pi(a) = \underline{a}$. Verifique que $\underline{J} \subset A/I$ é um ideal de A/I se e só se $\underline{J} = \pi(J)$, onde J é ideal de A e $I \subset J$.

15. Determine todos os ideais de $\mathbb{Z}_2[\boldsymbol{x}]/\langle \boldsymbol{x}^2+1\rangle$.

16. Classifique os grupos G não-abelianos, com 6 elementos, mostrando que:

    (a) G tem um elemento x de ordem 3, e $H =< x >$ é normal em G.

    (b) G tem um elemento y de ordem 2, e $y \notin H$.

    (c) Prove que $yx = xy^2$, porque $yx \in xH$. Conclua que $G \simeq S_3$.

4.3 Números Reais e Complexos

É intuitivamente evidente que os números racionais podem ser representados por pontos numa recta, e a determinação do ponto que corresponde a um racional dado é possível, desde que fixemos dois pontos arbitrários que representem os racionais 0 e 1. Os Gregos da Antiguidade Clássica descobriram um fenómeno interessante relacionado com esta associação entre números racionais e pontos duma recta: se é verdade que qualquer racional determina um ponto, é igualmente verdade que existem pontos que não correspondem a números racionais. Pensaram os gregos que este fenómeno representava um erro dos deuses, já que os racionais (um subproduto dos naturais) eram de algum modo insuficientes, e na realidade tentaram durante algum tempo ocultar este facto do conhecimento geral, aparentemente com medo da cólera dos mesmos deuses. Sob este aspecto, os Gregos enganaram-se, e, como veremos nesta secção, os números reais, que efectivamente descrevem todos os pontos da recta, podem ser definidos em termos dos racionais, e portanto (pelo menos indirectamente) a partir dos naturais.

Em linguagem moderna, a deficiência básica do corpo dos racionais exprime-se em termos da noção de sucessão de Cauchy. Relembramos aqui a terminologia que deve ser conhecida da Análise, adaptada ao caso particular dos racionais.

Definição 4.3.1. Seja $\boldsymbol{x} = (x_1, x_2, \dots)$ uma sucessão em $\mathbb{Q}$. A sucessão diz-se:

(a) LIMITADA, se existe $M \in \mathbb{Q}$ tal que

$$|x_n| \leq M, \forall n \in \mathbb{N}.$$

(b) CONVERGENTE em $\mathbb{Q}$, se existe $l \in \mathbb{Q}$ tal que

$$\forall \varepsilon \in \mathbb{Q}^+, \exists N \in \mathbb{N} : n \geq N \Longrightarrow |x_n - l| < \varepsilon.$$

(c) de CAUCHY, ou FUNDAMENTAL, se

$$\forall \varepsilon \in \mathbb{Q}^+, \exists N \in \mathbb{N} : n, m \geq N \Longrightarrow |x_n - x_m| < \varepsilon.$$

Obviamente, se uma sucessão $\boldsymbol{x} = (x_1, x_2, \dots)$ é convergente com limite l, então escrevemos $x_n \to l$, ou ainda $\lim_{n\to\infty} x_n = l$. Temos também os resultados usuais de soma, produtos, diferenças e quocientes de sucessões convergentes. Não é difícil mostrar que, no corpo $\mathbb{Q}$,

(i) Qualquer sucessão *convergente* é *fundamental*, e

(ii) Qualquer sucessão *fundamental* é *limitada*.

Por outro lado, existem sucessões fundamentais que não são convergentes, como verificamos a seguir, através de um exemplo simples.

Exemplo 4.3.2.

Considere-se a função $f : \mathbb{Q} \to \mathbb{Q}$ *definida por* $f(x) = \frac{x^2+2}{2x}$. *Se* $x > 0$, *notamos que* $f(x) > 1$, *porque*

$$\begin{aligned} (x-1)^2 + 1 > 0 \quad &\Longrightarrow \quad x^2 - 2x + 2 > 0, \\ &\Longrightarrow \quad x^2 + 2 > 2x, \\ &\Longrightarrow \quad \frac{x^2+2}{2x} > 1. \end{aligned}$$

Sendo $x, y > 0$, *observamos igualmente que*

$$f(x) - f(y) = \frac{(xy-2)(x-y)}{2xy} = \frac{xy-2}{xy}\frac{x-y}{2}.$$

Se além disso $x, y \geq 1$, *é fácil verificar que* $-1 \leq \frac{xy-2}{xy} < 1$, *pois* $g(z) = 1 - \frac{2}{z}$ *é crescente para* $z > 0$, *donde*

$$|f(x) - f(y)| \leq \frac{1}{2}|x - y|.$$

Seja então $\{x_n\}_{n\in\mathbb{N}}$ *a sucessão em* $\mathbb{Q}$ *definida por*

$$x_1 = 1, \ \text{e } x_{n+1} = f(x_n) \ \text{se } n \in \mathbb{N}.$$

Temos para $n > 1$

$$|x_{n+1} - x_n| = |f(x_n) - f(x_{n-1})| \leq \frac{1}{2}|x_n - x_{n-1}|,$$

e portanto

$$|x_{n+1} - x_n| \leq \frac{1}{2^{n-1}}|x_2 - x_1|.$$

Deixamos para os exercícios, verificar que para $m > n$ temos

$$|x_m - x_n| \leq \frac{1}{2^{n-2}}|x_2 - x_1|,$$

donde concluímos que a sucessão $\{x_n\}_{n\in\mathbb{N}}$ é fundamental.

Apesar de fundamental, esta sucessão não é convergente em $\mathbb{Q}$. Na realidade, temos

$$x_{n+1} = f(x_n) \Longrightarrow 2x_{n+1}x_n = x_n^2 + 2,$$

e, portanto, se $x_n \to x$, então $2x^2 = x^2 + 2$, ou $x^2 = 2$, equação que não tem soluções em $\mathbb{Q}$.

Embora a sucessão do exemplo anterior não convirja em $\mathbb{Q}$, obviamente converge em $\mathbb{R}$ para o irracional $\sqrt{2}$. De um modo geral, sabemos que qualquer sucessão fundamental em $\mathbb{Q}$ converge para um número real, que pode ou não ser irracional. Do ponto de vista desta secção, que se destina exactamente a definir os números reais, isolamos a seguinte ideia básica:

- Qualquer sucessão de Cauchy em $\mathbb{Q}$ determina um número real[5].

Bem entendido, sucessões de Cauchy distintas podem determinar o mesmo número real, o que ocorre exactamente quando as duas sucessões têm o mesmo limite, *i.e.*, quando a diferença das duas sucessões converge para zero. Por outras palavras:

- As sucessões de Cauchy $\{x_n\}_{n\in\mathbb{N}}$ e $\{y_n\}_{n\in\mathbb{N}}$ determinam o mesmo real se e só se $(x_n - y_n) \to 0$.

Definindo duas sucessões de Cauchy, $\{x_n\}_{n\in\mathbb{N}}$ e $\{y_n\}_{n\in\mathbb{N}}$, como *equivalentes* se $(x_n - y_n) \to 0$, a ideia central que usaremos para definir os reais a partir dos racionais é a de introduzir os números reais como *classes de equivalência* de sucessões de Cauchy em $\mathbb{Q}$.

Para explorarmos em pormenor estas ideias[6], necessitamos da seguinte proposição que na realidade as enquadra como um caso particular na teoria desenvolvida na secção anterior. A sua demonstração é um simples exercício.

Teorema 4.3.3. *Seja A o conjunto das sucessões racionais. Então:*

(i) A com as operações de soma e produto usuais para sucessões é um anel.

[5]Compare-se esta observação com a que fizemos a propósito da definição dos números racionais a partir dos inteiros: qualquer par (m, n) de inteiros com $n \neq 0$ determina um número racional.

[6]Este método de definição dos números reais deve-se a Georg Cantor (1845-1918), matemático alemão que descobriu igualmente a moderna Teoria dos Conjuntos, e criou a teoria dos números "transfinitos".

(ii) O subconjunto $B \subset A$ formado pelas sucessões de Cauchy em $\mathbb{Q}$ é um subanel de A.

(iii) O conjunto I formado pelas sucessões em $\mathbb{Q}$ que convergem para 0 é um subanel de A e ideal de B.

Se $\boldsymbol{x}, \boldsymbol{y} \in B$ são sucessões de Cauchy em $\mathbb{Q}$, é claro que $\boldsymbol{x}$ e $\boldsymbol{y}$ determinam o mesmo número real se e só se $\boldsymbol{x}-\boldsymbol{y}$ converge para 0, *i.e.*, se e só se $\boldsymbol{x}-\boldsymbol{y} \in I$. Temos portanto

Definição 4.3.4 (Cantor). O anel B/I designa-se por $\mathbb{R}$. Os seus elementos (que são classes de equivalência de sucessões de Cauchy em $\mathbb{Q}$) dizem-se NÚMEROS REAIS.

Deve ser claro que o anel $\mathbb{R}$ é uma extensão do anel $\mathbb{Q}$, já que, dado qualquer racional $q \in \mathbb{Q}$, podemos formar a sucessão constante $\boldsymbol{q}$ dada por $q_n = q$ para qualquer $n \in \mathbb{N}$ (obviamente uma sucessão de Cauchy), e a aplicação $\iota : \mathbb{Q} \to \mathbb{R}$ dada por $\iota(q) = \underline{\boldsymbol{q}}$ é um homomorfismo injectivo. Observamos também que o *zero* de $\mathbb{R}$ é a classe de equivalência da sucessão identicamente nula (o ideal I), e a sua *identidade* é a classe de equivalência da sucessão identicamente igual a 1. Naturalmente, qualquer sucessão de racionais convergente para 0 é um representante de $I = \underline{\mathbf{0}}$, assim como qualquer sucessão convergente para 1 é um representante de $\underline{\mathbf{1}}$.

Para verificar que $\mathbb{R}$ é um *corpo* (o que equivale a provar que I é um ideal maximal de B), é necessário mostrar que, se $\underline{\boldsymbol{x}} \in \mathbb{R} - \{0\}$ então existe $\underline{\boldsymbol{y}} \in \mathbb{R}$ tal que $\underline{\boldsymbol{xy}} = \underline{\mathbf{1}}$. Directamente em termos de sucessões de Cauchy em $\mathbb{Q}$, o resultado a provar é o seguinte:

Proposição 4.3.5. *Se $\boldsymbol{x}$ é uma sucessão de Cauchy em $\mathbb{Q}$ que não converge para 0, existe uma sucessão de Cauchy $\boldsymbol{y}$ em $\mathbb{Q}$ tal que $x_n y_n \to 1$.*

Demonstração. Sendo $\boldsymbol{x}$ uma sucessão de Cauchy em $\mathbb{Q}$ que não converge para 0, deixamos como exercício provar que existe um racional $\delta > 0$ e um natural $N \in \mathbb{N}$ tal que $|x_n| > \delta$ para $n \geq N$.

Definimos a sucessão $\boldsymbol{y} \in \mathbb{Q}$ por

$$y_n = \begin{cases} 0, & \text{se } n \leq N \\ \frac{1}{x_n}, & \text{se } n > N. \end{cases}$$

Notamos que para $n > N$ temos $|y_n| = |\frac{1}{x_n}| \leq \frac{1}{\delta}$, donde obtemos para $n, m > N$ que

$$|y_m - y_n| = \frac{|x_n - x_m|}{|x_n x_m|} \leq \frac{1}{\delta^2}|x_n - x_m| \to 0,$$

e $\boldsymbol{y}$ é uma sucessão de Cauchy em $\mathbb{Q}$.

Como $x_n y_n = 1$ para $n > N$, é óbvio que $x_n y_n \to 1$. □

Para provar que $\mathbb{R}$ é um corpo *ordenado*, é necessário definir um conjunto $\mathbb{R}^+$ tal que:

1. $\underline{\boldsymbol{x}}, \underline{\boldsymbol{y}} \in \mathbb{R}^+ \quad \Rightarrow \quad \underline{\boldsymbol{x}} + \underline{\boldsymbol{y}} \in \mathbb{R}^+$ e $\underline{\boldsymbol{xy}} \in \mathbb{R}^+$;
2. Se $\underline{\boldsymbol{x}} \in \mathbb{R}^+$, verifica-se exactamente um dos seguintes três casos:

$$\underline{\boldsymbol{x}} \in \mathbb{R}^+ \text{ ou } \underline{\boldsymbol{x}} = \underline{\mathbf{0}}, \text{ ou } -\underline{\boldsymbol{x}} \in \mathbb{R}^+.$$

Um momento de reflexão sugere um procedimento natural a seguir:

Definição 4.3.6. Se $\underline{\boldsymbol{x}} \in \mathbb{R}$ (donde $\boldsymbol{x}$ é uma sucessão de Cauchy em $\mathbb{Q}$), dizemos que $\underline{\boldsymbol{x}}$ é POSITIVO se e só se existe um racional $\varepsilon > 0$ e $N \in \mathbb{N}$, tal que $n > N \Rightarrow x_n \geq \varepsilon$. Designamos o conjunto dos reais positivos por $\mathbb{R}^+$.

É muito simples demonstrar agora que

Teorema 4.3.7. *$\mathbb{R}$ é um corpo ordenado.*

Note em particular que, de acordo com o que dissemos no Capítulo 2 sobre anéis ordenados, podemos definir $|\underline{\boldsymbol{x}}| = \max\{\underline{\boldsymbol{x}}, -\underline{\boldsymbol{x}}\}$ para qualquer $\underline{\boldsymbol{x}} \in \mathbb{R}$.

Sendo $q \in \mathbb{Q}$ um racional, designámos acima por $\boldsymbol{q}$ a sucessão constante dada por $q_n = q$ para qualquer $n \in \mathbb{N}$ (que como mencionámos é uma sucessão de Cauchy), e por $\underline{\boldsymbol{q}}$ o respectivo número real (a classe de equivalência determinada por $\boldsymbol{q}$). Como também indicámos acima, a função $f : \mathbb{Q} \to \mathbb{R}$ dada por $f(q) = \underline{\boldsymbol{q}}$ é um homomorfismo injectivo, e podemos por isso dizer que o corpo $\mathbb{R}$ é uma *extensão* do corpo $\mathbb{Q}$. Sabemos igualmente da Análise que qualquer número real pode ser aproximado a menos de um erro arbitrariamente pequeno por um racional, *i.e.*, que "$\mathbb{Q}$ é *denso* em $\mathbb{R}$", ideia que podemos agora formalizar e provar como se segue:

Proposição 4.3.8. *Se $\underline{\boldsymbol{x}}$ e $\underline{\boldsymbol{\varepsilon}}$ são reais e $\underline{\boldsymbol{\varepsilon}} > \underline{\mathbf{0}}$, existe um racional q tal que $|\underline{\boldsymbol{x}} - \underline{\boldsymbol{q}}| < \underline{\boldsymbol{\varepsilon}}$.*

Demonstração. Começamos por escolher representantes de $\underline{\boldsymbol{x}}$ e $\underline{\boldsymbol{\varepsilon}}$, *i.e.*, sucessões de Cauchy no corpo dos racionais, $\boldsymbol{x} = (x_1, x_2, \dots)$ e $\boldsymbol{\varepsilon} = (\varepsilon_1, \varepsilon_2, \dots)$. Como $\underline{\boldsymbol{\varepsilon}} > \underline{\mathbf{0}}$, existe um racional $r > 0$ tal que $\varepsilon_n \geq r$ para $n \geq N_1$, onde $N_1 \in \mathbb{N}$.

Obtemos agora o "racional" $\underline{\boldsymbol{q}}$ pelo expediente de transformar a sucessão $\boldsymbol{x}$ numa sucessão constante, usando um dos seus termos de ordem suficientemente elevada. Como $\boldsymbol{x}$ é uma sucessão de Cauchy, existe $N_2 \in \mathbb{N}$ tal que

$$n, m \geq N_2 \Longrightarrow |x_n - x_m| < \frac{r}{2}.$$

Tomando $q = x_{N_2}$, que é evidentemente um número racional, vemos que, se $n \geq \max\{N_1, N_2\}$, então $\frac{r}{2} < x_n - q \leq \frac{r}{2}$ (porquê?), e portanto temos $-r < \underline{\boldsymbol{x}} - \underline{\boldsymbol{q}} < r$, o que implica $|\underline{\boldsymbol{x}} - \underline{\boldsymbol{q}}| < \underline{\boldsymbol{\varepsilon}}$. □

As propriedades dos números reais, que são, bem entendido, a fundação sobre a qual se desenvolve a Análise, são normalmente introduzidas por via *axiomática*: um breve exame dos axiomas utilizados revela que tradicionalmente contêm apenas a afirmação de $\mathbb{R}$ ser um corpo ordenado, complementada pelo chamado "Axioma do Supremo", que é invocado, por exemplo, para provar que em $\mathbb{R}$ qualquer sucessão de Cauchy é convergente, contrariamente ao que vimos ser verdade em $\mathbb{Q}$.

Nesta secção, onde apresentamos uma definição *construtiva* (por oposição a *axiomática*) dos números reais, já mostrámos que $\mathbb{R}$ é um corpo ordenado, restando-nos portanto demonstrar que o "Axioma do Supremo" é outra das consequências da definição apresentada. No entanto, preferimos passar directamente a provar que em $\mathbb{R}$ todas as sucessões de Cauchy são convergentes, o que deixamos como um exercício um pouco mais ambicioso:

Teorema 4.3.9. *Qualquer sucessão de Cauchy em $\mathbb{R}$ é convergente*[7].

A partir deste resultado, é possível demonstrar com relativa facilidade que o "Axioma do Supremo" é válido em $\mathbb{R}$.

Corolário 4.3.10 (Axioma do Supremo). *Qualquer subconjunto majorado e não-vazio de $\mathbb{R}$ tem supremo.*

Demonstração. Supomos que $A \subset \mathbb{R}$ é não-vazio e majorado. Existe portanto um elemento $M \in \mathbb{R}$ tal que $x \leq M$, para qualquer $x \in A$. Definimos agora uma sucessão em $\mathbb{R}$, seguindo um procedimento de bissecção sucessiva típico da Análise Real. Começamos por tomar $x_1 = M$.

Como $A \neq \emptyset$, existe $a \in A$ e definimos $a_1 = a$. É claro que $a_1 \leq x_1$, e tomamos agora $a_2 = \frac{a_1+x_1}{2}$. É óbvio que o ponto a_2 divide o intervalo $[a_1, x_1]$ em dois subintervalos iguais. Temos agora duas alternativas:

(i) Se existe algum elemento $x \in A$ tal que $x > a_2$ (portanto, no subintervalo à direita de a_2), tomamos $x_2 = x_1$;

(ii) Se $x \leq a_2$ para qualquer $x \in A$, tomamos $x_2 = a_2$.

Deve agora mostrar que este procedimento aplicado sucessivamente conduz a uma sucessão de Cauchy, que converge de acordo com o Teorema 4.3.9, e mostrar finalmente que o seu limite é o supremo do conjunto A. □

Cumprimos assim o objectivo principal que nos propusemos nesta secção: os números reais podem ser definidos a partir dos números racionais (e portanto, implicitamente, a partir dos números inteiros), e as suas propriedades são uma consequência lógica dos axiomas para os inteiros apresentados no Capítulo 2.

[7] Dizemos por esta razão que $\mathbb{R}$ é um corpo COMPLETO.

A definição dos números complexos a partir dos reais não oferece qualquer dificuldade: como $\mathbb{R}$ é um corpo ordenado, é evidente que o polinómio $\boldsymbol{x}^2 + 1$ é irredutível em $\mathbb{R}[\boldsymbol{x}]$ (porquê?), e portanto o anel

$$\mathbb{C} = \frac{\mathbb{R}[\boldsymbol{x}]}{\langle \boldsymbol{x}^2 + 1 \rangle}$$

é um corpo, dito CORPO DOS COMPLEXOS. A unidade imaginária i é naturalmente a classe de equivalência do polinómio $\boldsymbol{x}$, que satisfaz a identidade $i^2 = -1$. Não nos detemos a provar quaisquer outras propriedades elementares de $\mathbb{C}$, mas mencionamos de passagem que $\mathbb{C}$ é também um corpo completo.

Exercícios.

1. Seja A um anel ordenado. Prove que qualquer sucessão convergente em A é fundamental, e qualquer sucessão fundamental é limitada.

2. Prove que, se $x_1 = 1$, e $x_{n+1} = f(x_n)$, onde f é a função do Exemplo 4.3.2, então $|x_n - x_m| \leq \frac{1}{2^{n-2}}|x_2 - x_1|$.

3. Prove que as sucessões de Cauchy em $\mathbb{Q}$ formam um subanel do anel das sucessões em $\mathbb{Q}$.

4. Prove que as sucessões de racionais que convergem para 0 formam um ideal do anel das sucessões de Cauchy em $\mathbb{Q}$.

5. Seja $\boldsymbol{x}$ uma sucessão de Cauchy em $\mathbb{Q}$. Prove que as seguintes afirmações são equivalentes:
   (a) $\boldsymbol{x}$ não converge para 0;
   (b) existe um racional $\varepsilon > 0$ e uma subsucessão x_{n_k} tal que $|x_{n_k}| \geq \varepsilon$ para k suficientemente grande;
   (c) existe um racional $d > 0$ tal que $|x_n| \geq d$ para n suficientemente grande.

6. Suponha que $\underline{\boldsymbol{x}}, \underline{\boldsymbol{y}} \in \mathbb{R}$.
   (a) Prove que, se $\underline{\boldsymbol{x}}, \underline{\boldsymbol{y}} \in \mathbb{R}^+$, então $\underline{\boldsymbol{x}} + \underline{\boldsymbol{y}} \in \mathbb{R}^+$ e $\underline{\boldsymbol{xy}} \in \mathbb{R}^+$.
   (b) Prove que os casos $\underline{\boldsymbol{x}} \in \mathbb{R}^+$, $\underline{\boldsymbol{x}} = \underline{\mathbf{0}}$, e $-\underline{\boldsymbol{x}} \in \mathbb{R}^+$ são mutuamente exclusivos.

7. Demonstre o Teorema 4.3.9, e complete a demonstração de Corolário 4.3.10.

8. Prove que o ordenamento dos reais é único, *i.e.*, mostre que, se $\mathbb{R}$ é um corpo ordenado, então $x \in \mathbb{R}^+$ se e só se existe $y \in \mathbb{R}$ tal que $x = y^2$.

9. Prove que $\mathbb{R}$ é não-numerável, e por isso é uma extensão transcendente de $\mathbb{Q}$ (e um espaço vectorial de dimensão infinita sobre $\mathbb{Q}$).

10. Mostre que, se x é um real e $0 \leq x < 1$, então existe uma sucessão de inteiros $a_1, a_2, \ldots$ tal que $0 \leq a_n \leq 9$ para qualquer $n \in \mathbb{N}$ e

$$x = \sum_{n=1}^{\infty} \frac{a_n}{10^n}.$$

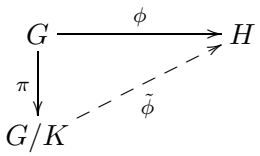
11. Mostre que $\mathbb{C}$ é um corpo completo.

4.4 Isomorfismos Canónicos de Grupos

Se G e H são grupos, e $K \subseteq G$ é um subgrupo normal de G, é natural investigar a relação entre os homomorfismos $\tilde{\phi} : G/K \to H$, e os homomorfismos $\phi : G \to H$.

Não é em qualquer caso evidente como podemos definir homomorfismos $\tilde{\phi} : G/K \to H$. No entanto, e dado que a aplicação quociente usual $\pi : G \to G/K$, dada por $\pi(x) = \underline{x} = xK$, é um homomorfismo de grupos, é claro que a função *composta* $\phi = \tilde{\phi} \circ \pi : G \to H$ é um homomorfismo de grupos, e $\tilde{\phi}(\underline{x}) = \phi(x)$, para qualquer $x \in G$. Por outras palavras, e como esclarecimento parcial da relação mencionada acima, *qualquer* homomorfismo $\tilde{\phi} : G/K \to H$ é da forma $\tilde{\phi}(\underline{x}) = \phi(x)$, onde $\phi : G \to H$ é um homomorfismo definido no grupo "original" G.

Claro que o aspecto mais interessante a esclarecer aqui é o de saber exactamente *quais* os homomorfismos $\phi : G \to H$, tais que existe *algum* homomorfismo $\tilde{\phi} : G/K \to H$, dado por $\tilde{\phi}(\underline{x}) = \phi(x)$. É esse o problema ilustrado pelo seguinte diagrama comutativo, onde a seta a tracejado serve para indicar que desejamos afirmar a existência do homomorfismo correspondente.



Suponha-se então que $\tilde{\phi}(\underline{x}) = \phi(x)$. Se $x \in K$ então $\underline{x} = K$ é a identidade de G/K, e portanto $\tilde{\phi}(\underline{x})$ é a identidade de H. Mas neste caso temos igualmente que $\phi(x) = \tilde{\phi}(\underline{x})$ é a identidade de H, ou seja, x pertence necessariamente ao núcleo de ϕ. Mais sucintamente, se $N = N(\phi)$ é o núcleo de ϕ, então $K \subseteq N$. Esta última condição é na verdade necessária e suficiente para a existência do homomorfismo $\tilde{\phi}$:

Proposição 4.4.1. *Os homomorfismos $\tilde{\phi} : G/K \to H$ são as funções dadas por $\tilde{\phi}(\underline{x}) = \phi(x)$, onde $\phi : G \to H$ é um homomorfismo com núcleo $N \supseteq K$.*

Demonstração. Já vimos que se $\tilde{\phi} : G/K \to H$ é um homomorfismo de grupos então $\phi = \tilde{\phi} \circ \pi$ é um homomorfismo de grupos $\phi : G \to H$, e o respectivo núcleo $N \supseteq K$.

Suponha-se então dado um qualquer homomorfismo de grupos $\phi : G \to H$, com núcleo $N \supseteq K$. Notamos que

$$y \in \underline{x} \Longrightarrow x^{-1}y \in K \Longrightarrow x^{-1}y \in N \Longrightarrow \phi(y) = \phi(x).$$

Por palavras, as classes laterais do subgrupo K estão contidas nos *conjuntos de nível* da função ϕ. Se $\underline{x} \in G/K$, podemos definir $\tilde{\phi}(\underline{x}) = \phi(x)$, e o valor de $\tilde{\phi}(\underline{x})$ é independente da escolha do representante x. Temos em particular

$$\tilde{\phi}(\underline{x}) = \phi(x), \text{ para qualquer } x \in G,$$

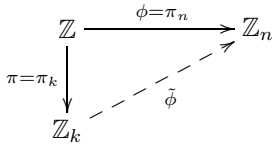
e $\tilde{\phi}$ é um homomorfismo, porque

$$\tilde{\phi}(\underline{x}) \cdot \tilde{\phi}(\underline{x'}) = \phi(x)\phi(x') = \phi(x \cdot x') = \tilde{\phi}(\underline{x \cdot x'}).$$

□

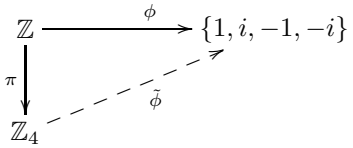
Exemplos 4.4.2.

1. *Tomamos $G = \mathbb{Z}$, $H = \mathbb{Z}_n$, $K = \langle k \rangle$. Designando a aplicação quociente $\pi : \mathbb{Z} \to \mathbb{Z}_m$ por π_m, consideramos o homomorfismo $\phi = \pi_n : \mathbb{Z} \to \mathbb{Z}_n$ dado por $\pi_n(x) = \underline{x} \in \mathbb{Z}_n$.*



   Como o núcleo de ϕ é $N = \langle n \rangle$, existe um homomorfismo $\tilde{\phi} : \mathbb{Z}_k \to \mathbb{Z}_n$ tal que se $\tilde{\phi}(\pi_k(x)) = \pi_n(x)$ e só se $\langle k \rangle \subseteq \langle n \rangle$, i.e., *se e só se $n|k$. Repare-se que se escrevermos $\tilde{\phi}(\underline{x}) = \underline{x}$ então a função $\tilde{\phi}$ aparenta ser a identidade, mas evidentemente não é esse o caso. Po exemplo, se $k = 4$ e $n = 2$, temos $\tilde{\phi}(\underline{0}) = \tilde{\phi}(\underline{2}) = \underline{0}$, e $\tilde{\phi}(\underline{1}) = \tilde{\phi}(\underline{3}) = \underline{1}$.*

2. *Sendo $H = \{1, i, -1, -i\}$, consideramos o homomorfismo $\phi : \mathbb{Z} \to H$ dado por $\phi(n) = i^n$. O núcleo de ϕ é o conjunto dos múltiplos de 4, ou seja, $N = \langle 4 \rangle$. Tomando $K = N$, concluímos que existe um homomorfismo $\tilde{\phi} : \mathbb{Z}_4 \to H$ tal que $\tilde{\phi}(\underline{n}) = i^n$, para qualquer $n \in \mathbb{Z}$. Na realidade, temos $\tilde{\phi}(\underline{0}) = 1$, $\tilde{\phi}(\underline{1}) = i$, $\tilde{\phi}(\underline{2}) = -1$, e $\tilde{\phi}(\underline{3}) = -i$, e portanto $\tilde{\phi}$ é obviamente um* isomorfismo.



3. *Consideramos agora $G = \mathbb{Z}$, $H = \mathbb{Z}_{210}$, $K = \langle k \rangle$, e o homomorfismo $\phi : \mathbb{Z} \to \mathbb{Z}_{210}$ dado por $\phi(x) = \underline{36x}$. O núcleo de ϕ é $N = \{x \in \mathbb{Z} : 210|36x\} = \{x \in \mathbb{Z} : 35|6x\} = \langle 35 \rangle$. Concluímos que existe um homomorfismo $\tilde{\phi} : \mathbb{Z}_k \to \mathbb{Z}_{210}$ tal que $\tilde{\phi}(\underline{x}) = \underline{36x}$ se e só se $\langle k \rangle \subseteq \langle 35 \rangle$,* i.e., *se e só se $35|k$. Em particular, $\tilde{\phi} : \mathbb{Z}_{70} \to \mathbb{Z}_{210}$, dado por $\tilde{\phi}(\underline{x}) = \underline{36x}$, está bem definido, e é um homomorfismo de grupos.*

É claro que, sendo ϕ e $\tilde{\phi}$ os homomorfismos referidos na proposição 4.4.1, então $\tilde{\phi}$ é sobrejectivo se e só se ϕ é também sobrejectivo. A questão da possível *injectividade* de $\tilde{\phi}$, ilustrada no exemplo 4.4.2.2, é mais interessante de explorar:

Proposição 4.4.3. *Seja $\phi : G \to H$ um homomorfismo de grupos com núcleo $N \supseteq K$, onde $K \subseteq G$ é um subgrupo normal de G. Seja ainda $\pi : G \to G/K$ a aplicação quociente usual, $\pi(x) = \underline{x} \in G/K$, e $\tilde{\phi} : G/K \to H$ o correspondente homomorfismo dado por $\tilde{\phi}(\underline{x}) = \phi(x)$. Temos então:*

(i) O núcleo de $\tilde{\phi}$ é $M = N/K = \pi(N)$, e em particular,

(ii) $\tilde{\phi}$ é injectiva se e só se $K = N$.

Demonstração. Seja e a identidade de H. O seguinte cálculo é muito simples:

$$\begin{aligned} M =& \{\underline{x} \in G/K : \tilde{\phi}(\underline{x}) = e\} = \{\underline{x} \in G/K : \phi(x) = e\} \\ =& \{\underline{x} \in G/K : x \in N\} = \pi(N) = N/K. \end{aligned}$$

É agora evidente que $\tilde{\phi}$ é injectiva se e só $\pi(N)$ só tem um elemento, (neste caso, a classe K), o que ocorre se e só se $N = K$. □

Exemplos 4.4.4.

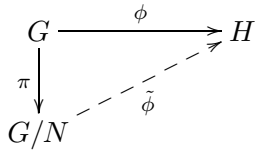
1. *Continuamos o exemplo 4.4.2.3, e recordamos que neste exemplo $G = \mathbb{Z}$, $H = \mathbb{Z}_{210}$, $K = \langle 70 \rangle$, e $\phi : \mathbb{Z} \to \mathbb{Z}_{210}$ é dada por $\phi(x) = \underline{36x}$. determinámos já o núcleo de ϕ, que é $N = \langle 35 \rangle$. Concluímos que o núcleo do correspondente homomorfismo $\tilde{\phi} : \mathbb{Z}_{70} \to \mathbb{Z}_{210}$ é $M = N/K = \pi_{70}(\langle 35 \rangle) = \langle \underline{35} \rangle = \{\underline{35}, \underline{0}\}$.*

2. *Se no exemplo anterior tomarmos $K = \langle 35 \rangle$, concluímos que o homomorfismo de grupos $\tilde{\phi} : \mathbb{Z}_{35} \to \mathbb{Z}_{210}$, dado por $\tilde{\phi}(\underline{x}) = \underline{36x}$, ou mais precisamente $\tilde{\phi}(\pi_{35}(x)) = \pi_{210}(36x)$, com $x \in \mathbb{Z}$, é injectivo.*

Se o homomorfismo ϕ é sobrejectivo, e $K = N$ é o núcleo de ϕ, a proposição anterior reduz-se a um resultado central da Teoria dos Grupos, que usaremos repetidamente no que se segue.

Teorema 4.4.5 (1º Teorema do Isomorfismo). *Se $\phi : G \to H$ é um homomorfismo sobrejectivo de grupos, e N é o núcleo de ϕ, então G/N e H são isomorfos. Em particular, existe um isomorfismo $\tilde{\phi} : G/N \to H$ tal que $\tilde{\phi}(\underline{x}) = \phi(x)$ para qualquer $x \in G$.*

Este teorema é expresso pela comutatividade do seguinte diagrama, onde a seta a tracejado afirma a existência do homomorfismo correspondente, que é neste caso um *isomorfismo*.



Este teorema permite-nos estabelecer facilmente a existência de isomorfismos entre grupos de natureza muito diversa. Observe-se de passagem que, mesmo quando ϕ não é sobrejectivo, o teorema se aplica automaticamente a $H' = \phi(G)$.

Exemplos 4.4.6.

1. *O grupo multiplicativo das raízes quartas da unidade, $H = \{1, i, -1, -i\}$, é isomorfo ao grupo aditivo $\mathbb{Z}_4$, como vimos no exemplo 4.4.2.2. Mais geralmente, considere-se o grupo multiplicativo R_n das raízes-n da unidade, $R_n = \{\alpha^k : k \in \mathbb{Z}\} = \langle\alpha\rangle$, onde $\alpha = e^{\frac{2\pi}{n}i}$. A função $\phi : \mathbb{Z} \to R_n$ dada por $\phi(k) = \alpha^k$ é um homomorfismo sobrejectivo de grupos, e o núcleo de ϕ é $N = \{k \in \mathbb{Z} : \alpha^k = 1\} = \langle n\rangle$.*

   Concluímos assim que os grupos $\mathbb{Z}_n$ e R_n são isomorfos.

2. *Seja $\phi : S_n \to \mathbb{Z}_2$ o homomorfismo (sobrejectivo) definido por $\phi(\rho) = \mathrm{sgn}(\rho)$, com $\rho \in S_n$. O seu núcleo (por definição) é o grupo alternado A_n. Logo, concluímos que S_n/A_n é isomorfo a $\mathbb{Z}_2$.*

3. *Supondo n e m naturais primos entre si, podemos novamente mostrar que os grupos $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \oplus \mathbb{Z}_n$ são isomorfos. Para isso, definimos $\phi : \mathbb{Z} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ da forma "óbvia",* i.e., *tomando $\phi(x) = (\pi_m(x), \pi_n(x))$. O cálculo do núcleo N de ϕ é muito simples, porque*

$$x \in N \iff \pi_m(x) = \pi_m(0) \text{ e } \pi_n(x) = \pi_n(0) \iff (m|x \text{ e } n|x) \iff mn|x.$$

   Como $N = \langle mn\rangle$, o homomorfismo $\tilde{\phi} : \mathbb{Z}_{mn} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ dado por $\tilde{\phi}(\pi_{mn}(x)) = (\pi_m(x), \pi_n(x))$ é injectivo, e $\mathbb{Z}_{mn} \simeq \tilde{\phi}(\mathbb{Z}_{mn})$. Em particular, $\tilde{\phi}(\mathbb{Z}_{mn})$ tem mn elementos. Como $\mathbb{Z}_m \oplus \mathbb{Z}_n$ tem também mn elementos, é claro que $\tilde{\phi}(\mathbb{Z}_{mn}) = \mathbb{Z}_m \oplus \mathbb{Z}_n$ e $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$.

   É interessante observar que este isomorfismo é, na verdade, o único *isomorfismo de anéis de $\mathbb{Z}_{mn}$ para $\mathbb{Z}_m \oplus \mathbb{Z}_n$. Deixaremos para os exercícios, a título de curiosidade, a determinação explícita do respectivo isomorfismo inverso.*

A observação feita acima, a propósito do grupo das raízes-n da unidade, é bastante mais geral do que pode parecer. Na realidade, se G é um qualquer grupo multiplicativo com identidade e, e $\alpha \in G$, sabemos que o grupo gerado por α é $\langle\alpha\rangle = \{\alpha^k : k \in \mathbb{Z}\}$. A função $\phi : \mathbb{Z} \to \langle\alpha\rangle$ dada por $\phi(k) = \alpha^k$ é sempre um homomorfismo sobrejectivo, e o respectivo núcleo é dado por $N = \{k \in \mathbb{Z} : \alpha^k = e\}$. Como N é um subgrupo de $\mathbb{Z}$, sabemos que $N = \langle n\rangle$, onde $n \geq 0$. Distinguimos agora duas alternativas possíveis para n:

(i) $n = 0 \iff N = \{0\}$: neste caso, ϕ é injectivo, além de sobrejectivo, e portanto $\langle\alpha\rangle \simeq \mathbb{Z}$, e $\langle\alpha\rangle$ é obviamente um grupo infinito. O elemento α tem ordem infinita;

(ii) $n > 0 \iff N \neq \{0\}$: então sabemos que n é o menor inteiro positivo em N, *i.e.*, é a menor solução positiva da equação $\alpha^k = e$. Neste caso,

$\langle\alpha\rangle \simeq \mathbb{Z}/\langle n\rangle = \mathbb{Z}_n$, e $\langle\alpha\rangle$ tem n elementos. Portanto, α é um elemento de ordem n, e a ordem do elemento α é precisamente o menor natural k para o qual $\alpha^k = e$.

Exemplos 4.4.7.

1. *Consideramos a permutação ε em S_3. Sabemos que $\varepsilon^1 = \varepsilon$, $\varepsilon^2 = \delta$ e $\varepsilon^3 = I$. Portanto, ε é um elemento de ordem 3, e $\langle\varepsilon\rangle = \{\varepsilon, \delta, I\} = A_3 \simeq \mathbb{Z}_3$.*

2. *Recordamos que D_5 é o grupo de simetria do pentágono regular, e consideramos uma rotação não-trivial $r \in D_5$. Deve ser claro que a ordem de r é 5. Portanto $\langle r\rangle \simeq \mathbb{Z}_5$. Mais geralmente, é fácil mostrar que o grupo D_n tem sempre um subgrupo $H \simeq \mathbb{Z}_n$, que é normal em D_n (porquê?).*

Usaremos a seguinte terminologia:

Definição 4.4.8. O grupo G diz-se CÍCLICO se existe algum elemento $g \in G$ tal que $\langle g\rangle = G$. Neste caso, g diz-se GERADOR de G.

Exemplos 4.4.9.

1. *O grupo $\mathbb{Z}$ é cíclico, com geradores 1 e -1.*

2. *A_3 é um grupo cíclico: podemos tomar $g = \varepsilon$ ou $g = \delta$.*

3. *O grupo $\{1, i, -1, -i\}$ é cíclico: podemos tomar $g = i$ ou $g = -i$.*

4. *Os grupos $\mathbb{Z}_n$ são cíclicos: qualquer elemento de $\mathbb{Z}_n^*$ é um gerador do grupo.*

5. *O grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ não é cíclico (porquê?).*

O próximo teorema de classificação identifica *todos* os grupos cíclicos, e limita-se a resumir observações que já fizémos.

Corolário 4.4.10 (Classificação dos grupos cíclicos). *Se G é um grupo cíclico, então verifica-se uma das seguintes alternativas:*

(i) Se G é infinito, então $G \simeq \mathbb{Z}$;

(ii) Se G é finito (e tem n elementos), então $G \simeq \mathbb{Z}_n$.

Usando ainda o Teorema de Lagrange, é possível classificar também todos os grupos finitos cuja ordem é um número primo (a respectiva demonstração fica como exercício):

Proposição 4.4.11 (Classificação dos grupos de ordem p). *Se G é um grupo finito de ordem p, com p primo, então $G \simeq \mathbb{Z}_p$.*

O 1º Teorema do Isomorfismo pode ser aplicado para esclarecer a natureza do grupo HN/N, quando N e H são subgrupos de G, e N é um subgrupo normal de G:

Teorema 4.4.12 (2º Teorema do Isomorfismo). *Se N e H são subgrupos de G, e N é normal em G, então HN é um subgrupo de G, N é normal em HN, $H \cap N$ é normal em H, e*

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}.$$

Demonstração. Observámos no exercício 10 da secção 4.1 que, se H e N são subgrupos de G, então

$$HN \text{ é igualmente um subgrupo de } G \iff HN = NH.$$

Como N é normal em G, temos certamente $HN = NH$, e concluímos que HN é um subgrupo de G.

Considere-se a aplicação canónica $\pi : G \to G/N$ restrita a H, ou seja, a função $\phi : H \to G/N$ dada por

$$\phi(x) = \pi(x) = \underline{x}, \text{ para qualquer } x \in H.$$

É claro que ϕ é um homomorfismo de grupos, e o respectivo núcleo é claramente $\{x \in H : x \in N\} = H \cap N$. Por outro lado, a imagem $\phi(H)$ é um subgrupo de G/N, ou seja, $\phi(H) = K/N$, onde K é um subgrupo de G que contem necessariamente H e N, donde $HN \subseteq K$. Por outro lado, qualquer elemento de K é equivalente a algum elemento de H, *i.e.*, se $k \in K$ então existe $h \in H$ e $n \in N$ tal que $k = hn$. Temos portanto $K = HN$.

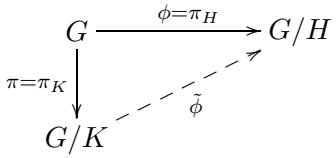
Segue-se, do 1º Teorema do Isomorfismo, que

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}.$$

□

Como consequência do teorema anterior, é evidente que, se $H \cap N$ se reduz à identidade de G, então $HN/N \simeq H$.

Finalmente, usamos ainda o 1º Teorema do Isomorfismo para estudar os grupos quociente formados a partir de grupos quociente de G, que podemos chamar de "quocientes de quocientes de grupos". Note-se de passagem que o resultado seguinte é, na realidade, uma generalização das observações que fizémos no exemplo 4.4.2.1. Suponha-se que $K \subseteq H \subseteq G$, onde K e H são subgrupos normais do grupo G. Analogamente ao que fizémos no exemplo referido, sejam $\pi_K : G \to G/K$ e $\pi_H : G \to G/H$ as aplicações quociente usuais, onde bem entendido o núcleo de π_K é K, e o núcleo de π_H é H. Considere-se o diagrama:



O homomorfismo $\tilde{\phi}$ é evidentemente sobrejectivo, porque π_H é sobrejectivo. A existência de $\tilde{\phi}$ resulta da condição $K \subseteq H$, de acordo com a proposição 4.4.1. Finalmente, e agora de acordo com a proposição 4.4.3, o núcleo do homomorfismo $\tilde{\phi}$ é o grupo H/K. Aplicando o 1º Teorema do Isomorfismo ao homomorfismo $\tilde{\phi} : G/K \to G/H$, obtemos imediatamente:

Teorema 4.4.13 (3º Teorema do Isomorfismo). *Se K e H são subgrupos normais de G, e $K \subset H$, então K é um subgrupo normal de H, H/K é um subgrupo normal de G/K, e*

$$\frac{G/K}{H/K} \simeq \frac{G}{H}.$$

Note que de acordo com este resultado os quocientes de quocientes de G são na realidade isomorfos a quocientes de G.

Exemplos 4.4.14.

1. *Tomamos $G = \mathbb{Z}$, $H = \langle 3 \rangle$, e $K = \langle 6 \rangle$. É claro que $K \subset H$, e tanto K como H são subgrupos normais de $\mathbb{Z}$, pois este grupo é abeliano. Temos neste caso*

$$\begin{aligned} G/K &= \mathbb{Z}/\langle 6 \rangle = \mathbb{Z}_6, \\ H/K &= \langle 3 \rangle/\langle 6 \rangle = \langle \underline{3} \rangle \subset \mathbb{Z}_6, \text{ e} \\ G/H &= \mathbb{Z}/\langle 3 \rangle = \mathbb{Z}_3. \end{aligned}$$

   De acordo com o resultado anterior, concluímos que $\mathbb{Z}_6/\langle \underline{3} \rangle$ e $\mathbb{Z}_3$ são grupos isomorfos.

2. *O exemplo anterior exprime um facto completamente geral. Se $n|m$, e tomarmos $G = \mathbb{Z}$, $H = \langle n \rangle$, e $K = \langle m \rangle$, temos mais uma vez que $K \subset H$, e K e H são subgrupos normais de $\mathbb{Z}$. Neste caso, $G/K = \mathbb{Z}_m$, $G/H = \mathbb{Z}_n$, e $H/K = \langle \underline{n} \rangle \subseteq \mathbb{Z}_m$. Concluímos que também aqui se tem $\mathbb{Z}_m/\langle \underline{n} \rangle \simeq \mathbb{Z}_n$.*

Exercícios.

1. Seja $H = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ um grupo cíclico. Prove que
   (a) se H é infinito, os seus únicos geradores são g e g^{-1};
   (b) se H tem m elementos, a ordem de g^n é $\frac{m}{d}$, onde $d = \text{mdc}(n, m)$;
   (c) se H tem m elementos, g^n é gerador de H se e só se $\text{mdc}(n, m) = 1$.

2. Suponha que g_1 e g_2 são elementos do grupo abeliano G, com ordens respectivamente n e m, e prove que a ordem de $g_1 g_2$ divide $\text{mmc}(n, m)$. Conclua que o subconjunto formado pelos elementos de ordem finita é um subgrupo de G.

3. Quais dos grupos $\mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ e $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ são isomorfos entre si?

4. Considere o grupo multiplicativo $H = \langle e^{\frac{i\pi}{4}} \rangle \subset \mathbb{C}$ formado pelas soluções complexas de $z^8 = 1$. Determine todos os geradores e subgrupos de H.

5. Continuando o exercício anterior, determine os automorfismos $\phi : H \to H$.

6. Considere o subgrupo $H = \langle (123456) \rangle$ em S_6. Determine todos os geradores de H e todos os subgrupos de H.

7. Mostre que $Aut(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$.

8. Mostre que $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \oplus \mathbb{Z}_n$ são grupos e anéis isomorfos se e só se m e n são primos entre si.

9. Suponha que G é um grupo finito, H é um subgrupo normal de G, K é um subgrupo de G, $G = HK$, e G/H é isomorfo a K. Prove que $H \cap K = \{e\}$, onde e é a identidade de G.

10. Prove que, se $n > 1$, então $\mathbb{Z}_{p^n}$ não é isomorfo a $\oplus_{k=1}^{n} \mathbb{Z}_p$.

11. A que grupo $\mathbb{Z}_n$ é isomorfo o quociente $\mathbb{Z}_{40}/\langle \underline{15} \rangle$?

12. Conclua a demonstração da Proposição 4.4.11.

13. Suponha que o grupo G tem apenas os subgrupos triviais $\{1\}$ e G. Mostre que $G \simeq \mathbb{Z}_p$ é um grupo cíclico de ordem prima.

14. Prove que, se G é um grupo abeliano de ordem pq, com p e q primos, então G é cíclico.

15. Classifique os grupos com $2p$ elementos, onde $p > 2$ é primo. (SUGESTÃO: Mostre que existe um elemento x de ordem p, e que *todos* os elementos de ordem p pertencem a $< x >$).

16. Classifique os grupos com 8 elementos. Proceda como se segue:

    (a) Mostre que se G é abeliano, então é isomorfo a um dos grupos $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, ou $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, que não são isomorfos entre si.

    (b) Supondo que G não é abeliano, mostre que:

        (i) G tem um elemento x de ordem 4, e $H =< x >$ é normal.

        (ii) Supondo $y \notin H$, prove que $y^2 \in H$, donde $y^2 = 1$ ou $y^2 = x^2$.

        (iii) Prove finalmente que $yx \in Hy$, donde $yx = x^3y$. Pode ser vantajoso observar primeiro que a ordem de yxy^{-1} é a ordem de x.

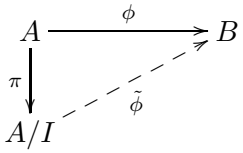
        (iv) Compare as suas conclusões com as tabelas dos grupos D_4 e $\mathbb{H}_8$.

17. Suponha que G e H são grupos, com subgrupos normais $K \subset G$ e $N \subset H$. Prove que $(G \times H)/(K \times N)$ é isomorfo a $(G/K) \times (H/N)$.

18. Seja $G = \mathbb{Z} \oplus \mathbb{Z}$ e $N = \{(n, n) : n \in \mathbb{Z}\}$. Mostre que $G/N \simeq \mathbb{Z}$.

4.5 Isomorfismos Canónicos de Anéis

Supondo que A e B são anéis, $I \subseteq A$ é um ideal de A, e $\phi : A \to B$ é um homomorfismo *de anel*, podemos evidentemente aplicar a teoria desenvolvida na secção anterior ao homomorfismo ϕ, que é também um homomorfismo do grupo aditivo $(A, +)$ para $(B, +)$. Sabemos em particular que, se o núcleo de ϕ contem I, então existe um homomorfismo de grupo $\tilde{\phi} : A/I \to B$ tal que $\tilde{\phi}(\underline{x}) = \phi(x)$, o que ilustramos no seguinte diagrama comutativo.



Além disso, e como ϕ é um homomorfismo de anel, temos igualmente

$$\tilde{\phi}(\underline{x}) \cdot \tilde{\phi}(\underline{x'}) = \phi(x)\phi(x') = \phi(x \cdot x') = \tilde{\phi}(\underline{x \cdot x'}).$$

Por outras palavras, o homomorfismo $\tilde{\phi}$ é certamente um homomorfismo de anel, desde que o homomorfismo "original" ϕ também o seja. Por esta razão, a adaptação das proposições 4.4.1 e 4.4.3 da secção anterior, ao caso dos anéis, é imediata.

Proposição 4.5.1. *Sejam A e B anéis, $I \subseteq A$ um ideal de A, e $\pi : A \to A/I$ a usual aplicação quociente, $\pi(x) = \underline{x} \in A/I$.*

(i) Os homomorfismos de anel $\tilde{\phi} : A/I \to B$ são as funções dadas por $\tilde{\phi}(\pi(x)) = \phi(x)$, onde $\phi : A \to B$ é um qualquer homomorfismo de anel, com núcleo $N \supseteq I$.

(ii) Sendo $\phi : A \to B$ um homomorfismo de anéis com núcleo $N \supseteq I$, e $\tilde{\phi} : A/I \to B$ o correspondente homomorfismo de anel dado por $\tilde{\phi}(\pi(x)) = \phi(x)$, temos ainda

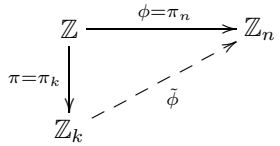
(a) O núcleo de $\tilde{\phi}$ é $M = N/I = \pi(N)$, e em particular,

(a) $\tilde{\phi}$ é injectiva se e só se $I = N$.

Se A é um anel, então $\phi : \mathbb{Z} \to A$ é um homomorfismo de grupos aditivos se e só se $h(n) = na$, onde $a \in A$ é um elemento fixo, mas *arbitrário*, do anel A. É muito fácil verificar que ϕ é igualmente um homomorfismo de *anéis* se e só se $a = \phi(1)$ é solução da equação $x^2 = x$ em A. Reanalisamos alguns dos exemplos da secção anterior à luz desta observação elementar.

Exemplos 4.5.2.

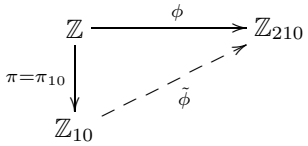
1. *Tomamos $A = \mathbb{Z}$, $B = \mathbb{Z}_n$, e $I = \langle k \rangle$. A aplicação quociente $\phi = \pi_n : \mathbb{Z} \to \mathbb{Z}_n$ é, como sabemos, um homomorfismo de anéis, porque $\phi(1) = \underline{1}$ é a identidade de $\mathbb{Z}_n$. Desde que $n|k$, temos então*



onde $\tilde{\phi} : \mathbb{Z}_k \to \mathbb{Z}_n$, dada por $\tilde{\phi}(\pi_k(x)) = \pi_n(x)$, é um homomorfismo de anéis.

2. *Tomamos agora $A = \mathbb{Z}$, $B = \mathbb{Z}_{210}$, e $I = \langle k \rangle$. A equação $x^2 = x$ tem diversas soluções não evidentes em $\mathbb{Z}_{210}$, como, por exemplo, $\underline{x} = \underline{21}$. O homomorfismo $\phi : \mathbb{Z} \to \mathbb{Z}_{210}$ dado por $\phi(x) = \pi_{210}(21x)$ é portanto um homomorfismo de anéis. O respectivo núcleo N é fácil de calcular, e temos $N = \langle \underline{10} \rangle$.*

   Concluímos que existe um homomorfismo $\tilde{\phi} : \mathbb{Z}_k \to \mathbb{Z}_{210}$ tal que $\tilde{\phi}(\underline{x}) = \underline{21x}$ se e só se $10|k$. Neste caso, e em particular, o núcleo de $\tilde{\phi}$ é o ideal $\langle \underline{10} \rangle$, e $\tilde{\phi}$ é injectivo quando $k = 10$. Na realidade, quando $k = 10$ então $\phi(\mathbb{Z}) = \tilde{\phi}(\mathbb{Z}_{10}) = \langle \underline{21} \rangle$ é um subanel unitário de $\mathbb{Z}_{210}$, evidentemente isomorfo a $\mathbb{Z}_{10}$.



3. *Considere-se ainda $A = \mathbb{Q}[\boldsymbol{x}]$, $B = \mathbb{Q}$, e $\phi : \mathbb{Q}[\boldsymbol{x}] \to \mathbb{Q}$ dado por $\phi(p(\boldsymbol{x})) = p(1)$. Sabemos que ϕ é um homomorfismo de anéis, e o respectivo núcleo é, de acordo com o Teorema do Resto, $N = \langle \boldsymbol{x} - 1 \rangle$. Sendo $I = \langle m(\boldsymbol{x}) \rangle$ o ideal de $\mathbb{Q}[\boldsymbol{x}]$ gerado pelo polinómio $m(\boldsymbol{x})$, constatamos que existe um homomorfismo de anéis $\tilde{\phi} : \frac{\mathbb{Q}[\boldsymbol{x}]}{I} \to \mathbb{Q}$, dado por $\tilde{\phi}(\underline{p(\boldsymbol{x})}) = p(1)$, se e só se $(\boldsymbol{x} - 1)|m(\boldsymbol{x})$,* i.e., *se e só se $p(1) = 0$.*

O 1º Teorema do Isomorfismo é imediatamente generalizável para anéis, como implicitamente observámos no segundo exemplo acima. Neste caso, o seu enunciado é o seguinte:

Teorema 4.5.3 (1º Teorema do Isomorfismo para Anéis). *Se $\phi : A \to B$ é um homomorfismo sobrejectivo de anéis, e I é o núcleo de ϕ, então os anéis A/I e B são isomorfos. Em particular, existe um isomorfismo de anéis $\tilde{\phi}$ tal que $\tilde{\phi}(\underline{a}) = \phi(a)$ para qualquer $a \in A$.*

Exemplos 4.5.4.

1. *Começamos por mostrar que, quando n e m são naturais primos entre si, então os* anéis $\mathbb{Z}_{nm}$ *e $\mathbb{Z}_n \oplus \mathbb{Z}_m$ são também isomorfos. Mais uma vez, bastanos notar que a função $\phi = \pi_{nm} : \mathbb{Z} \to \mathbb{Z}_n \oplus \mathbb{Z}_m$ dada por $\phi(k) = (\pi_n(k), \pi_m(k)$ é um homomorfismo* de anéis. *Portanto, o isomorfismo* de grupos $\tilde{\phi} : \mathbb{Z}_{nm} \to \mathbb{Z}_n \oplus \mathbb{Z}_m$ *que apresentámos no exemplo 4.4.6.3 é também um isomorfismo* de anéis.

2. Seja $\alpha \in \mathbb{C}$ um elemento algébrico sobre $\mathbb{Q}$, $\alpha \notin \mathbb{Q}$, e $m(\boldsymbol{x})$ o seu polinómio mínimo. Recorde-se que $\phi : \mathbb{Q}[\boldsymbol{x}] \to \mathbb{C}$ dada por $\phi(p(\boldsymbol{x})) = p(\alpha)$ é um homomorfismo de anéis, com núcleo $N = \langle m(\boldsymbol{x})\rangle$, e ainda que $\mathbb{Q}[\alpha] = \phi(\mathbb{Q}[\boldsymbol{x}])$. Concluímos do 1º Teorema do Isomorfismo para Anéis que

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

Além disso, e como $m(\boldsymbol{x})$ é um polinómio irredutível, sabemos que $\mathbb{Q}[\boldsymbol{x}]/\langle m(\boldsymbol{x})\rangle$ é um corpo*, e portanto (porquê?)*

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

Podemos utilizar o resultado do Exemplo 4.5.4.1 para calcular a função de Euler $\varphi : \mathbb{N} \to \mathbb{N}$, que introduzimos no capítulo anterior. Recorde-se que esta foi definida por $\varphi(n) = |\mathbb{Z}_n^*|$, *i.e.*, $\varphi(n)$ é o número de elementos invertíveis no anel $\mathbb{Z}_n$, ou ainda, é o número de naturais $1 \leq k \leq n$ que são primos relativamente a n.

Lema 4.5.5. *Se $n_1, \ldots, n_k$ são naturais primos entre si, então*

$$\varphi(n_1 \cdots n_k) = \varphi(n_1) \cdots \varphi(n_k).$$

Demonstração. Provamos este lema para $k = 2$, já que a sua generalização para $k > 2$ se obtem por indução, sem qualquer dificuldade adicional. Relembramos do Capítulo 1 que, se A e B são anéis unitários, então $(A \oplus B)^* = A^* \times B^*$. Portanto, se $C \simeq A \oplus B$, e os anéis em causa são finitos, é evidente que $|C^*| = |A^*||B^*|$.

Aplicamos este resultado com $A = \mathbb{Z}_n$, $B = \mathbb{Z}_m$, e $C = \mathbb{Z}_{nm}$, supondo que n e m são primos entre si. Como $\mathbb{Z}_{nm} \simeq \mathbb{Z}_n \oplus \mathbb{Z}_m$, concluímos imediatamente que:

$$\varphi(nm) = \varphi(n)\varphi(m).$$

□

O próximo teorema possibilita o cálculo imediato de $\varphi(n)$, desde que se conheçam todos os factores primos de n.

Teorema 4.5.6. *Se $n = \prod_{i=1}^{k} p_i^{e_i}$ é a factorização prima de n então*

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Demonstração. Concluímos directamente do lema anterior que, se n é um natural com factorização prima $n = \prod_{i=1}^{k} p_i^{e_i}$, então

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{e_i}).$$

Sendo p um primo, e m um natural, é simples calcular $\varphi(p^m)$: os elementos de $\mathbb{Z}_{p^m}$ que não são invertíveis são evidentemente os elementos do ideal $\langle \underline{p} \rangle$ em $\mathbb{Z}_{p^m}$, e este ideal tem, por razões óbvias, exactamente $p^m/p = p^{m-1}$ elementos. Temos assim que $\mathbb{Z}_{p^m}^* = \mathbb{Z}_{p^m} - \langle \underline{p} \rangle$ tem $p^m - p^{m-1} = p^m(1 - \frac{1}{p})$ elementos, ou seja,

$$\varphi(p_i^{e_i}) = p_i^{e_i} - p_i^{e_i-1} = p_i^{e_i}(1 - \frac{1}{p_i}).$$

Segue-se finalmente que:

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{e_i}) = \prod_{i=1}^{k} p_i^{e_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

□

Exemplo 4.5.7.

Os factores primos de 9000 *são* 2, 3 *e* 5, *e portanto*

$$\varphi(9000) = 9000 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 2400.$$

Vimos no Capítulo 2 que a existência dos corpos finitos $\mathbb{Z}_p$ se segue dos axiomas para os inteiros que indicámos. Já neste capítulo, vimos que a existência do corpo $\mathbb{Q}$ é outra das consequências desses axiomas. Aproveitamos agora para mostrar, noutra aplicação do 1º Teorema do Isomorfismo, que estes corpos são, em certo sentido, os *menores* corpos que existem. Por outras palavras, vamos provar que qualquer corpo contém necessariamente um subcorpo isomorfo a um dos corpos finitos $\mathbb{Z}_p$, ou isomorfo a $\mathbb{Q}$. No que se segue, K é um corpo arbitrário, com identidade 1.

Definição 4.5.8. K diz-se um corpo PRIMITIVO se não contém nenhum subcorpo estrito (*i.e.*, $\neq K$).

É claro que existem corpos primitivos (como $\mathbb{Z}_2$), e corpos não-primitivos (como $\mathbb{R}$). Além disso, qualquer corpo K contém precisamente um subcorpo primitivo (observe que a intersecção de todos os subcorpos de K é necessariamente um corpo primitivo), dito o SUBCORPO PRIMITIVO de K.

Exemplo 4.5.9.

É claro que $\mathbb{Q}$ *é o corpo primitivo de* $\mathbb{R}$ *e de* $\mathbb{C}$. *Da mesma forma,* $\mathbb{Q}$ *é também o corpo primitivo de* $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

O próximo teorema identifica todos os possíveis corpos primitivos:

Teorema 4.5.10. *Seja m a característica de K, donde $m = 0$ ou $m = p$, onde p é primo. Então:*

(i) Se $m = 0$, o subcorpo primitivo de K é isomorfo a $\mathbb{Q}$;

(ii) Se $m = p$, o subcorpo primitivo de K é isomorfo a $\mathbb{Z}_p$.

Demonstração. Provamos o resultado apenas para $m = p$, deixando o caso $m = 0$ como exercício.

Considere-se o homomorfismo $\phi : \mathbb{Z} \to K$ dado por $\phi(n) = nI$, onde I é a identidade de K. É fácil verificar que qualquer subcorpo de K deve conter I, e portanto deve conter $\phi(\mathbb{Z})$. Como se mostrou no Capítulo 2, $\phi(\mathbb{Z})$ é isomorfo a $\mathbb{Z}_p$, e é portanto um corpo. Concluímos que $\phi(\mathbb{Z})$ é o subcorpo primitivo de K. □

Um corpo K é sempre um espaço vectorial sobre o seu corpo primitivo, com dimensão finita ou infinita. Uma consequência interessante desta observação é a seguinte: se K é um corpo finito, a sua característica é necessariamente um primo $p > 0$, e portanto o seu corpo primitivo J tem p elementos e é isomorfo a $\mathbb{Z}_p$. A dimensão de K sobre J é finita (senão, K seria infinito) e, portanto, existe um natural n tal que K é isomorfo ao espaço vectorial J^n. Logo,

Teorema 4.5.11. *Qualquer corpo finito tem p^n elementos, onde p é primo e igual à sua característica.*

Sabemos já que existem corpos finitos com p elementos (os corpos $\mathbb{Z}_p$). Na realidade, se p é primo e n é natural, existem corpos com p^n elementos, e todos os corpos com p^n elementos são isomorfos entre si. Portanto, e a menos de isomorfismos, existe exactamente um corpo com p^n elementos, dito CORPO DE GALOIS [8] de ordem p^n, que designaremos por $CG(p^n)$. Não demonstramos imediatamente estas últimas afirmações, mas observamos desde já que, se $p(\boldsymbol{x}) \in \mathbb{Z}_p[\boldsymbol{x}]$ é um polinómio *irredutível* de grau n, então $K = \mathbb{Z}_p[\boldsymbol{x}]/\langle p(\boldsymbol{x})\rangle$ é certamente um corpo com p^n elementos, e portanto é, de acordo com o que dissémos acima, o corpo de Galois $CG(p^n)$. Reduzimos desta forma a existência dos corpos de Galois à existência de polinómios irredutíveis de grau n arbitrário em $\mathbb{Z}_p$.[9]

A forma de generalizar os 2º e 3º Teoremas do Isomorfismo ao caso de anéis deve ser agora clara. Limitamo-nos a enunciar os resultados, deixando a sua demonstração como exercício.

[8] De Évariste Galois (1811-1832). Galois, responsável por um dos maiores êxitos matemáticos do século *XIX* (a teoria dos grupos), é uma figura trágica da História da Matemática, já que morreu aos 21 anos num duelo (no Capítulo 7 exporemos a teoria de Galois).

[9] Ver ainda o exercício 8 desta secção.

Teorema 4.5.12 (2º Teorema do Isomorfismo para Anéis). *Seja A um anel, I um ideal de A, e B um subanel de A. Então $I+B$ é um subanel de A, I é um ideal de $I+B$, $I\cap B$ é um ideal de B, e temos o isomorfismo de anéis*

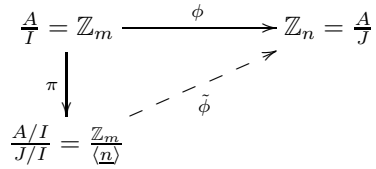
$$\frac{I+B}{I}\simeq\frac{B}{I\cap B}.$$

Teorema 4.5.13 (3º Teorema do Isomorfismo para Anéis). *Seja A um anel, I,J ideais de A com $I\subset J$. Então I é um ideal de J, J/I é um ideal de A/I, e temos o isomorfismo de anéis*

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

Exemplo 4.5.14.

Com $A=\mathbb{Z}$, supomos que $n|m$. Tomamos $I=\langle m\rangle$, e $J=\langle n\rangle$, donde $J\supseteq I$, e I e J são ideais de $\mathbb{Z}$. Neste caso, $A/I=\mathbb{Z}_m$, $A/J=\mathbb{Z}_n$, e $J/I=\langle\underline{n}\rangle\subseteq\mathbb{Z}_m$. Concluímos que os anéis $\mathbb{Z}_m/\langle\underline{n}\rangle$ e $\mathbb{Z}_n$ são isomorfos. Em particular, os anéis quociente formados a partir dos anéis $\mathbb{Z}_m$ são anéis $\mathbb{Z}_n$.



Exercícios.

1. Prove os Teoremas do Isomorfismo para Anéis.

2. Suponha que A é um anel unitário com n elementos. Prove que:
   (a) O *anel* $A\simeq\mathbb{Z}_n$ se e só se A tem característica n.
   (b) O *anel* $A\simeq\mathbb{Z}_n$ se e só se o *grupo* $(A,+)\simeq(\mathbb{Z}_n,+)$.

3. A afirmação de que $\mathbb{Z}_n\oplus\mathbb{Z}_m\simeq\mathbb{Z}_{nm}$, se $\mathrm{mdc}(n,m)=1$, exprime o Teorema Chinês do Resto em termos de isomorfismos de anéis. Como se exprime o Teorema Fundamental da Aritmética nos mesmos termos?

4. Suponha que $n,m\in\mathbb{N}$, $d=\mathrm{mdc}(n,m)$ e $k=\mathrm{mmc}(n,m)$. Mostre que $\mathbb{Z}_n\oplus\mathbb{Z}_m\simeq\mathbb{Z}_d\oplus\mathbb{Z}_k$.

5. Supondo n e m primos entre is, mostre que:
   (a) Existe exactamente um isomorfismo de anel $\phi:\mathbb{Z}_{mn}\to\mathbb{Z}_m\oplus\mathbb{Z}_n$, e
   (b) O único isomorfismo de anel $\phi:\mathbb{Z}_m\oplus\mathbb{Z}_n\to\mathbb{Z}_{mn}$ é da forma $\phi(x,y)=\phi_m(x)+\phi_n(y)$, onde $\phi_k:\mathbb{Z}_k\to\mathbb{Z}_{mn}$ é um homomorfismo injectivo da forma $\phi_k(\pi_k(x))=\pi_{mn}(a_kx)$. Quais são os inteiros a_k? Qual é a relação entre ϕ e o Teorema Chinês do Resto discutido no Capítulo 2?

6. Consideramos neste exercício homomorfismos de anel $\phi : \mathbb{Z}_n \to \mathbb{Z}_{210}$.

   (a) Para que valores de n existem homomorfismos ϕ *injectivos*?

   (b) Para que valores de n existem homomorfismos ϕ *sobrejectivos*?

7. Resolva a equação $\varphi(m) = 6$, onde φ é a função de Euler. Proceda como se segue:

   (a) Prove que os factores primos de m são 2, 3, ou 7.

   (b) Mostre que se $7|m$, então $m = 7$ ou $m = 14$.

   (c) Mostre que se 7 não divide m, então $3|m$ e $9|m$.

   (d) Determine todas as soluções de $\varphi(m) = 6$.

8. Suponha que $K \subset L$ são corpos, $u \in L$ é algébrico sobre K, e $m(\boldsymbol{x})$ é o polinómio mínimo de u em $K[\boldsymbol{x}]$. Mostre que $K[u]$, $K(u)$ e $K[\boldsymbol{x}]/\langle m(\boldsymbol{x})\rangle$ são corpos isomorfos.

9. Suponha que $I \subset A$ é um ideal de A, e diga se A é necessariamente isomorfo ao anel $I \oplus A/I$. Por outro lado, prove que, se A é isomorfo a $I \oplus J$, então J é isomorfo a A/I.

10. Seja K um corpo, e $p(\boldsymbol{x}) = q(\boldsymbol{x})d(\boldsymbol{x})$ polinómios em $K[\boldsymbol{x}]$. Mostre que $K[\boldsymbol{x}]/\langle p(\boldsymbol{x})\rangle$ é isomorfo a $K[\boldsymbol{x}]/\langle q(\boldsymbol{x})\rangle \oplus K[\boldsymbol{x}]/\langle q(\boldsymbol{x})\rangle$.

11. Considere $p(\boldsymbol{x}) = (\boldsymbol{x}^2 + \boldsymbol{x} + 1)(\boldsymbol{x}^3 + \boldsymbol{x} + 1) \in \mathbb{Z}_2[\boldsymbol{x}]$. Quantos elementos invertíveis existem em $\mathbb{Z}_2[\boldsymbol{x}]/\langle p(\boldsymbol{x})\rangle$? E em $\mathbb{Z}_2[\boldsymbol{x}]/\langle p(\boldsymbol{x})^2\rangle$?

12. Complete a demonstração do Teorema 4.5.10.

13. Seja K um corpo primitivo, e L e M extensões de K. Prove o seguinte:

   (a) Se $\phi : L \to M$ é um homomorfismo não-nulo, então $\phi(a) = a$, para qualquer $a \in K$.

   (b) Se $p(\boldsymbol{x}) \in K[\boldsymbol{x}]$ e $p(b) = 0$, então $p(\phi(b)) = 0$, *i.e.*, ϕ transforma raízes de $p(\boldsymbol{x})$ em raízes de $p(\boldsymbol{x})$.

   (c) $\mathbb{Q}[\boldsymbol{x}]/\langle \boldsymbol{x}^3 - 2\rangle$ não é isomorfo a $\mathbb{Q}[\boldsymbol{x}]/\langle \boldsymbol{x}^3 - 3\rangle$.

14. Prove que qualquer corpo ordenado é uma extensão de $\mathbb{Q}$, *i.e.*, $\mathbb{Q}$ é o menor corpo ordenado.

15. Qualquer corpo ordenado completo é uma extensão dos reais, *i.e.*, $\mathbb{R}$ é o menor corpo ordenado completo.

4.6 Grupos Livres, Geradores e Relações

Dado um subconjunto X dum grupo G, o SUBGRUPO GERADO POR X é a intersecção de todos os subgrupos de G que contêm X, e designa-se por $\langle X \rangle$. Tal como no caso dos ideais, se $X = \{x_1, x_2, \cdots, x_n\}$ é um conjunto finito, escrevemos também $\langle X \rangle = \langle x_1, x_2, \cdots, x_n \rangle$. O conjunto X diz-se GERADOR do grupo G se e só se $\langle X \rangle = G$. Esta condição é equivalente a dizer que todo o elemento de G pode ser escrito, em notação multiplicativa, como um produto de potências positivas e negativas de elementos de X. Podemos também definir o subgrupo NORMAL gerado por X como a intersecção de todos os subgrupos normais que contêm X.

Exemplo 4.6.1.

Se $G = S_3$ e $X = \{\alpha\}$, onde α é uma transposição, então o subgrupo gerado por X é $H = \{1, \alpha\}$, mas o subgrupo normal *gerado por X é o próprio S_3.*

Se G é gerado por um conjunto finito, *i.e.*, se $G = \langle x_1, x_2, \cdots, x_n \rangle$, então G diz-se um GRUPO DE TIPO FINITO. Note-se, em particular, que se o grupo *abeliano* G é gerado por $X = \{x_1, x_2, \cdots, x_n\}$, então para qualquer elemento $g \in G$ existem inteiros $c_1, c_2, \cdots, c_n$ tais que:

$$g = x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n}, \text{ ou, em notação aditiva, } g = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n.$$

Exemplos 4.6.2.

1. *O grupo cíclico $G = \langle \alpha \rangle$ é de tipo finito. Qualquer elemento $g \in G$ é da forma $g = \alpha^n$, possivelmente para múltiplos valor de n.*
2. *Qualquer grupo* finito *é de tipo finito, porque podemos tomar $X = G$.*
3. *O grupo $G = \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$ não é cíclico nem finito, mas é de tipo finito, porque é gerado por $X = \{(1,0,0), (0,1,0), (0,0,1)\}$.*
4. *O grupo aditivo $\oplus_{k=1}^{n} \mathbb{Z}$ é de tipo finito, porque é gerado pelos n vectores da base canónica usual de $\mathbb{R}^n$, $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$, onde $\boldsymbol{e}_k$ tem todas as componentes iguais a zero, excepto a componente k, que é 1. Este grupo tem um papel fundamental nesta secção.*

Se um conjunto X gera um grupo G, então existem em geral múltiplos produtos de elementos de X que são iguais à identidade $e \in G$. Por exemplo,

(a) para todo o $x \in X$, temos $xx^{-1} = e$;

(b) se G é cíclico de ordem m, e $X = \{x\}$ é gerador, então $x^m = e$.

De uma forma por enquanto heurística, dizemos que um produto de elementos de G que é igual à identidade é uma RELAÇÃO. Distinguimos entre

relações triviais, como no exemplo (a), que são consequência dos axiomas de um grupo, e *relações não-triviais*, como no exemplo (b), que dependem da escolha de G e X.

Repare-se que muitos grupos podem ser completamente descritos, e de forma particularmente sucinta, indicando apenas um conjunto X de geradores, e um número restrito de relações entre esses geradores, que podemos sempre escrever (em notação multiplicativa) na forma:

$$x_1^{c_1} x_2^{c_2} \cdots x_k^{c_k} = 1.$$

Exemplos 4.6.3.

1. *O grupo cíclico G de ordem n fica completamente descrito indicando $X = \{\alpha\}$, e a relação $\alpha^n = 1$.*

2. *O grupo S_3 é gerado por $X = \{\alpha, \delta\}$, e a sua tabuada resulta de aplicar as relações $\alpha^2 = 1$, $\delta^3 = 1$, e $\delta\alpha = \alpha\delta^2 = \alpha\delta^{-1}$. Esta última relação pode naturalmente escrever-se também $\alpha\delta\alpha\delta = 1$.*

3. *O grupo $\mathbb{H}_8$ é gerado por $X = \{i, j\}$, e é completamente especificado pelas relações $i^2 j^2 = i^4 = 1$ e $iji = j$.*

4. *O grupo de simetrias D_n de um polígono regular de n lados é gerado por σ e ρ, onde*
$$\sigma^2 = 1, \quad \rho^n = 1, \quad \sigma\rho\sigma\rho = 1.$$
O elemento ρ representa uma rotação de $2\pi/n$, e o elemento σ representa uma reflexão em relação a um eixo de simetria do polígono.

Para facilitar a comparação de grupos distintos G e H usando um só conjunto X de geradores, diremos ainda que o grupo G é GERADO pelo conjunto X desde que exista uma função $\iota : X \to G$ tal que G é gerado pelo conjunto $\iota(X)$, no sentido que referimos acima. Quando a função ι é evidente do contexto da discussão, e para simplificar a notação, é comum usarmos o mesmo símbolo para representar o elemento $x \in X$ e o correspondente elemento $\iota(x) \in G$.

Exemplo 4.6.4.

Podemos dizer que os grupos S_3, $\mathbb{H}_8$, e $\mathbb{Z} \oplus \mathbb{Z}$ são gerados por $X = \{x_1, x_2\}$.

Suponha-se agora que o grupo G é gerado por $X = \{x_1, x_2, \cdots, x_n\}$, e seja H um grupo arbitrário. Um momento de reflexão mostra que:

- Qualquer homomorfismo $\phi : G \to H$ fica unicamente determinado, em todo o grupo G, pelos valores $y_k = \phi(x_k)$, assumidos por ϕ em cada um dos geradores de G, mas

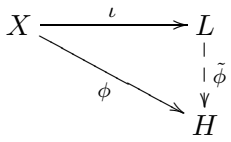
- Os valores $y_k = \phi(x_k)$ não são em geral arbitrários, porque as relações satisfeitas por $x_1, x_2, \cdots, x_n$ em G são necessariamente satisfeitas por $y_1, y_2, \cdots, y_n$ em H.

Exemplo 4.6.5.

Qualquer homomorfismo de grupo $\phi : S_3 \to H$ fica unicamente determinado pelos valores $\rho = \phi(\alpha)$ e $\xi = \phi(\delta)$. No entanto, os elementos $\rho, \xi \in H$ não são arbitrários, e devem necessariamente satisfazer as relações que α e δ satisfazem, nomeadamente: $\rho^2 = \xi^3 = 1$, e $\xi\rho = \rho\xi^2$.

Ainda de um ponto de vista intuitivo, deve reconhecer-se que o grupo G gerado por X é LIVRE de relações entre os seus geradores, se existem *sempre* homomorfismos $\phi : G \to H$, *quaisquer que sejam* os valores $\phi(\boldsymbol{x}_k)$. Podemos agora tornar estas ideias mais precisas, para já introduzindo a seguinte:

Definição 4.6.6. Seja X um conjunto. Um grupo L diz-se um GRUPO LIVRE (respectivamente, LIVRE ABELIANO) no conjunto X, se L é um grupo (respectivamente, abeliano) e existe uma função $\iota : X \to L$ tal que a seguinte condição se verifica: Para todo o grupo (respectivamente, abeliano) H e toda a função $\phi : X \to H$ existe um único homomorfismo $\tilde{\phi} : L \to H$ tal que o seguinte diagrama é comutativo:

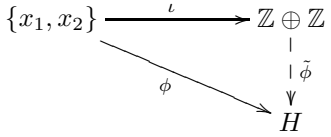


Exemplo 4.6.7.

É fácil verificar que $\mathbb{Z} \oplus \mathbb{Z}$ é um grupo livre abeliano em $X = \{x_1, x_2\}$. Para isso, definimos $\iota : X \to L$ por $\iota(x_1) = \boldsymbol{e}_1 = (1, 0)$, e $\iota(x_2) = \boldsymbol{e}_2 = (0, 1)$. Dado um qualquer grupo abeliano H, e uma função $\phi : X \to H$, observamos que $\tilde{\phi} : \mathbb{Z} \oplus \mathbb{Z} \to H$, dada por:

$$\tilde{\phi}(n, m) = n\phi(x_1) + m\phi(x_2)$$

é um homomorfismo de grupos, e $\tilde{\phi}(\iota(x_i)) = \tilde{\phi}(\boldsymbol{e}_i) = \phi(x_i)$.



Mais geralmente, se $X = \{x_1, \ldots, x_n\}$ é um conjunto finito, consideramos o grupo $\mathbb{Z}^n = \bigoplus_{k=1}^{n} \mathbb{Z} = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$, e a aplicação $\iota : X \to \mathbb{Z}^n$ tal que $\iota(x_1) = (1, 0, \ldots, 0) = e_1$, $\iota(x_2) = (0, 1, \ldots, 0) = e_2$,..., $\iota(x_n) = (0, 0, \ldots, 1) = e_n$. Se

H é um grupo abeliano e $\phi : X \to H$ é uma aplicação, então o homomorfismo $\tilde{\phi} : \mathbb{Z}^n \to H$ é dado por:

$$\tilde{\phi}(k_1, \ldots, k_n) = k_1\phi(x_1) + \cdots + k_n\phi(x_n).$$

Portanto, $\bigoplus_{k=1}^{n} \mathbb{Z}$ é um grupo livre abeliano em $X = \{x_1, \ldots, x_n\}$.

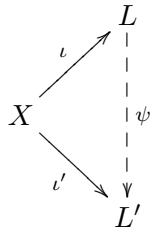
Observe-se da definição de grupo livre L em X que, se o grupo H é igualmente gerado por X, no sentido em que existe uma função $\phi : X \to H$ tal que $\langle \phi(X) \rangle = H$, então o homomorfismo $\tilde{\phi}$ é sobrejectivo. Em particular, e sendo N o núcleo de $\tilde{\phi}$, concluímos que os grupos L/N e H são isomorfos. A importância do grupo L para a classificação de grupos é assim evidente: QUALQUER *grupo gerado por X é um grupo quociente do grupo L.*

Exemplo 4.6.8.

Qualquer grupo abeliano gerado por $X = \{x_1, \ldots, x_n\}$ é um grupo quociente do grupo $\mathbb{Z}^n = \bigoplus_{k=1}^{n} \mathbb{Z} = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. Exploraremos esta observação mais adiante, para classificar os grupos abelianos de tipo finito.

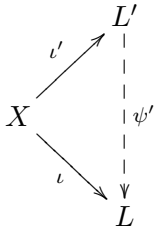
Mostraremos nesta secção que, dado um conjunto X, existe (a menos de isomorfismos) exactamente um grupo livre *não-abeliano*, e um grupo livre *abeliano* gerado por X, excepto quando $X = \{x_1\}$, caso em que o único grupo livre gerado por X é $\mathbb{Z}$, e portanto é abeliano. Começamos por provar que os grupos livres em X são *únicos*, a menos de isomorfismo.

Proposição 4.6.9. *Sejam L e L' grupos livres num conjunto X, em relação a funções $\iota : X \to L$ e $\iota' : X \to L'$, respectivamente. Supondo que L e L' são ambos abelianos, ou ambos não-abelianos, então existe um único isomorfismo $\psi : L \to L'$ que torna o seguinte diagrama comutativo:*

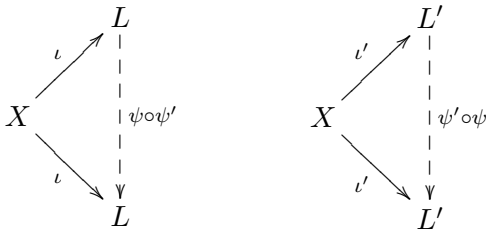


Demonstração. Aplicando a definição 4.6.6, com $H = L'$ e $\phi = \iota'$, obtemos a existência de um único homomorfismo, $\psi : L \to L'$, que torna o diagrama do enunciado comutativo. Da mesma forma, trocando os papéis de ι e ι', obtemos um homomorfismo $\psi' : L' \to L$ que torna o seguinte diagrama

comutativo:



Daqui, segue-se imediatamente que os seguintes diagramas também são comutativos:



Note que, substituindo, nestes diagramas, $\psi \circ \psi'$ e $\psi' \circ \psi$ pelas aplicações identidade, também obtemos diagramas comutativos. A unicidade na propriedade da definição de grupo abeliano livre permite-nos, pois, concluir que $\psi \circ \psi' = \mathrm{id}_L$ e $\psi' \circ \psi = \mathrm{id}_{L'}$. Logo, o homomorfismo ψ possui uma inversa e, portanto, é um isomorfismo. □

Mostramos agora que existe sempre um grupo abeliano livre gerado por X. Já vimos que é este o caso quando X é *finito*, quando o grupo livre abeliano é $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. Para definirmos o grupo abeliano livre gerado por um conjunto infinito arbitrário, precisamos de introduzir as noções de produtos directos e somas directas de famílias *infinitas* de grupos.

Definição 4.6.10. Seja $\{G_i\}_{i \in I}$ uma família de grupos.

(i) O PRODUTO DIRECTO dos G_i's, que se designa por $\prod_{i \in I} G_i$, é o grupo cujo conjunto suporte é o produto cartesiano [10] $\prod_{i \in I} G_i$ dos grupos, e cuja operação de grupo é definida da seguinte forma: Se $g = (g_i)_{i \in I}$ e $h = (h_i)_{i \in I}$ são elementos de $\prod_{i \in I} G_i$, então o seu produto é o elemento $gh \equiv (g_i h_i)_{i \in I} \in \prod_{i \in I} G_i$.

(ii) A SOMA DIRECTA dos G_i's, que se designa por $\bigoplus_{i \in I} G_i$, é o subgrupo do produto directo $\prod_{i \in I} G_i$ formado pelos elementos $(g_i)_{i \in I} \in \prod_{i \in I} G_i$, em que apenas um número finito de g_i's é diferente da identidade (em G_i).

[10] Ver a definição A.2.2 no Apêndice.

Repare-se que, no caso em que o conjunto de índices é finito, a soma directa e o produto directo coincidem, e são equivalentes à definição apresentada no Capítulo 1. Deixamos a demonstração da seguinte proposição como um exercício:

Proposição 4.6.11. *Se X é um conjunto arbitrário, a soma directa $L = \bigoplus_{x\in X} \mathbb{Z}$ é um grupo abeliano livre gerado por X relativamente à aplicação $\iota : X \to L$ que a $x_0 \in X$ associa o elemento $(g_x)_{x\in X} \in L$, em que todas as componentes são nulas à excepção da componente x_0: $g_{x_0} = 1$ e $g_x = 0$, se $x \neq x_0$.*

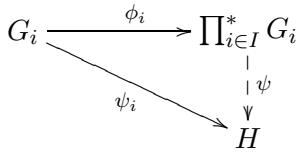
A aplicação ι da proposição é injectiva, e por isso chama-se *injecção canónica*. Assim, podemos identificar cada elemento $x_i \in X$ com a sua imagem $\iota(x_i) \in L$. Então X passa a ser um subconjunto de L, e podemos expressar todo o elemento $g \neq e$ de L na forma

$$g = x_{i_1}^{n_1} x_{i_2}^{n_2} \cdots x_{i_k}^{n_k},$$

onde os índices $i_1, \ldots, i_k$ são todos distintos e $n_1, \ldots, n_k$ são inteiros não-nulos. Esta expressão é única a menos da ordem dos factores, e toda a expressão deste tipo representa um elemento de L.

Mostramos finalmente que existe igualmente um grupo livre não-abeliano em qualquer conjunto X com mais de um elemento. Para construir o grupo livre em X indexamos os elementos de X, de forma que $X = \{x_i : i \in I\}$, e tomamos um "produto apropriado" dos grupos livres L_i nos conjuntos $X_i = \{x_i\}$. O produto que utilizaremos é o chamado *produto livre* de grupos, que vamos agora introduzir.

Proposição 4.6.12. *Seja $\{G_i\}_{i\in I}$ uma família de grupos. Existe um grupo $\prod^*_{i\in I} G_i$, dito o* PRODUTO LIVRE *dos grupos G_i, e homomorfismos de grupos $\phi_i : G_i \to \prod^*_{i\in I} G_i$ com a seguinte propriedade: dado um grupo H e homomorfismos de grupos $\psi_i : G_i \to H$, existe um único homomorfismo de grupos $\psi : \prod^*_{i\in I} G_i \to H$ que, para todo o $i \in I$, torna o seguinte diagrama comutativo:*



Demonstração. Seja $\{G_i\}_{i\in I}$ uma família de grupos. Definimos uma PALAVRA nos G_i's como sendo uma sucessão finita $(g_1, \ldots, g_n)$, em que cada g_k pertence a algum G_i. Ao inteiro n chamamos COMPRIMENTO DA PALAVRA, e consideramos também a palavra vazia que designamos por 1 e que tem comprimento zero. Uma PALAVRA REDUZIDA é uma palavra $(g_1, \ldots, g_n)$ que satisfaz as seguintes propriedades:

(a) nenhum g_k é elemento identidade de um grupo G_i;

(b) nenhuns termos sucessivos pertencem ao mesmo grupo G_i;

Designemos por $\prod^*_{i\in I} G_i$ o conjunto das palavras reduzidas. Neste conjunto vamos definir então uma estrutura de grupo.

Sejam $g = (g_1, \ldots, g_n)$ e $h = (h_1, \ldots, h_m)$ duas palavras reduzidas, com $n \leq m$. Seja $0 \leq N \leq n$ o menor inteiro tal que para todo o $N < k \leq n$, g_k e h_{n-k+1} pertencem ao mesmo grupo G_i, e $g_k h_{n-k+1}$ é a identidade em G_i. Então o produto gh é a palavra reduzida definida por

$$gh = \begin{cases} (g_1, \ldots, g_N, h_{n-N+1}, \ldots, h_m) & \text{se } N > 0 \text{ e } g_N, h_{n-N+1} \text{ não pertencem ao mesmo grupo,} \\ (g_1, \ldots, g_{N-1}, g_N h_{n-N+1}, h_{n-N+2}, \ldots, h_m) & \text{se } N > 0, \text{ e } g_N, h_{n-N+1} \text{ pertencem ao mesmo grupo,} \\ (h_{n-N+1}, \ldots, h_m) & \text{se } N = 0 \text{ e } n < m, \\ 1 & \text{se } N = 0 \text{ e } n = m. \end{cases}$$

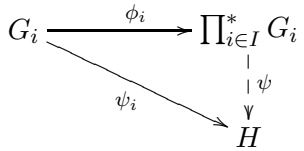
A composição de uma palavra reduzida g com a palavra vazia 1 é dada por $g1 = 1g = g$. É fácil de verificar que fica assim definida uma estrutura de grupo, com identidade a palavra vazia 1, e em que o inverso da palavra reduzida $g = (g_1, \ldots, g_n)$ é a palavra reduzida $g^{-1} = (g_n^{-1}, \ldots, g_1^{-1})$.

Sejam $\phi_i : G_i \to \prod^*_{i\in I} G_i$ as aplicações que a um elemento $g \in G_i$, com $g \neq e$ associa a palavra reduzida (g), e que a e associa 1. É óbvio que ϕ_i é um homomorfismo de grupos.

Finalmente, dado um grupo H e homomorfismos de grupos $\psi_i : G_i \to H$, definimos um homomorfismo de grupos, $\psi : \prod^*_{i\in I} G_i \to H$, da seguinte forma: $\psi(1) = e$ (a identidade em H) e

$$\psi(g_1, \ldots, g_n) = \psi_{i_1}(g_1) \cdots \psi_{i_n}(g_n),$$

se $g_k \in G_{i_k}$. É fácil verificar que este homomorfismo é o único homomorfismo de grupos que, para todo o $i \in I$, torna o diagrama comutativo:



□

Daqui em diante usamos a notação multiplicativa para escrever uma palavra $(g_1, \ldots, g_n)$ na forma $g_1 \cdots g_n$.

O exemplo seguinte ilustra a diferença entre o produto livre e o produto ou soma directa de grupos.

Exemplo 4.6.13.

Sejam $G_1 = \{1, g\}$ e $G_2 = \{1, h\}$ grupos cíclicos de ordem 2. Um elemento do produto livre $G_1 * G_2$ pode ser escrito como uma sucessão alternada de produtos de g e h. Por exemplo, são elementos do produto livre

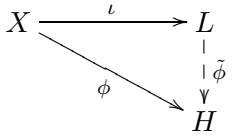
$$g, h, gh, hg, ghg, hgh, ghgh, \ldots$$

Note que $gh \neq hg$ e que ambos os elementos têm ordem infinita. Por outro lado, o produto directo (ou a soma directa) $G_1 \times G_2$ é um grupo abeliano de ordem 4!

Para um conjunto $X = \{x_i : i \in I\}$ arbitrário, vamos considerar o produto livre $L \equiv \prod_{i\in I}^{*} L_i$ dos grupos livres L_i nos conjuntos $\{x_i\}$. Temos ainda uma aplicação injectiva $\iota : X \to L$ que a um elemento x_i associa a palavra (x_i).

Proposição 4.6.14. *Se $X = \{x_i : i \in I\}$, o produto livre $L = \prod_{i\in I}^{*} L_i$ é um grupo livre gerado por X relativamente à aplicação $\iota : X \to L$.*

Demonstração. Precisamos de mostrar que para todo o grupo H e aplicação $\phi : X \to H$ existe um único homomorfismo de grupos $\tilde{\phi} : L \to H$ que torna o seguinte diagrama comutativo:



Observe-se que os elementos de L são palavras reduzidas da forma

$$x_1^{k_1} \cdots x_n^{k_n},$$

onde $k_1, \ldots, k_n$ são inteiros não nulos. É então fácil de ver que $\tilde{\phi}$ tem de ser definido por

$$\tilde{\phi}(x_1^{k_1}, \ldots, x_n^{k_n}) = \phi(x_1)^{k_1} \cdots \phi(x_n)^{k_n}.$$

□

Como observámos acima, qualquer elemento do grupo livre gerado pelo conjunto $X = \{x_i : i \in I\}$ pode ser escrito na forma reduzida

$$x_1^{k_1} \cdots x_n^{k_n},$$

e dois elementos deste tipo multiplicam-se de forma óbvia.

Vejamos agora a relação entre o grupo livre e o grupo abeliano livre num grupo X. Se G é um grupo, vamos designar por $(G, G) \subset G$ o menor subgrupo de G que contém todos os elementos da forma

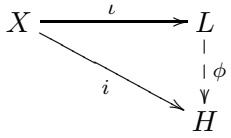
$$(g, h) \equiv g^{-1}h^{-1}gh, \quad g, h \in G.$$

É fácil de ver que este grupo é um subgrupo normal de G e que o quociente $G/(G,G)$ é abeliano. Este grupo será estudado mais aprofundadamente no Capítulo 5. Temos então a seguinte proposição cuja demonstração é deixada como exercício.

Proposição 4.6.15. *Seja L um grupo livre no conjunto X em relação a uma função $\iota : X \to L$. O quociente $L/(L,L)$ é o grupo abeliano livre no conjunto X em relação à função $\bar{\iota} : X \to L/(L,L)$ dada por $\bar{\iota} = \pi \circ \iota$, onde $\pi : L \to L/(L,L)$ é a projecção canónica.*

A existência de grupos livres permite-nos formalizar a noção de relação, esclarecer a diferença entre relações triviais e não-triviais, e definir o que entendemos como um conjunto *completo* de relações. No que segue, H é um grupo gerado por $X \subset H$, e L é um grupo livre em X, em relação à função $\iota : X \to L$. Supomos naturalmente L abeliano, se H for abeliano. A função $i : X \hookrightarrow H$ é a inclusão canónica ($i(x) = x$), Como já observámos:

Proposição 4.6.16. *Existe um homomorfismo sobrejectivo $\phi : L \to H$.*



Uma RELAÇÃO NÃO-TRIVIAL de H é qualquer elemento r no núcleo de ϕ, distinto da identidade de L. Claro que r é, em qualquer caso, um elemento da forma $\iota(x_{i_1})^{x_1}\iota(x_{i_2})^{n_2}\cdots\iota(x_{i_k})^{n_k}$, onde $x_j \in X$. Mas é evidente que dizer que este elemento pertence ao núcleo é equivalente a escrever

$$x_{i_1}^{n_1} x_{i_2}^{n_2} \cdots x_{i_k}^{n_k} = 1,$$

e portanto continuamos a dizer que esta última identidade é uma "relação".

Dada uma colecção de relações $R = \{r_i\}_{i\in I}$, dizemos que a relação r é uma CONSEQUÊNCIA das relações r_i's, se r pertence ao subgrupo *normal* de L gerado pelos r_i's. Dizemos ainda que R é COMPLETA, se o núcleo de ϕ é o subgrupo *normal* de L gerado por R.

Se a colecção de relações $R = \{r_i\}_{i\in I}$ é completa, então o grupo H fica completamente determinado a menos de isomorfismo pelo conjunto de geradores X e pelo conjunto R, porque H é isomorfo ao grupo quociente de L pelo subgrupo normal gerado por R. Neste caso, o par (X,R) diz-se uma APRESENTAÇÃO do grupo H.

Dois grupos com uma mesma apresentação são evidentemente isomorfos. Por outro lado, em geral, um grupo tem muitas apresentações distintas.

Exemplo 4.6.17.

Tomemos o grupo $H = \mathbb{Z}_2 \oplus \mathbb{Z}_3$. É fácil verificar que este grupo é gerado pelo elemento $x_1 = (1,1)$. O grupo abeliano livre gerado por $X = \{x_1\}$ é isomorfo a $\mathbb{Z}$, identificando x_1 com o elemento 1. Existe um único homomorfismo sobrejectivo $\phi : \mathbb{Z} \to \mathbb{Z}_2 \oplus \mathbb{Z}_3$ que aplica 1 em $(1,1)$. O elemento 6 pertence ao núcleo, e de facto gera o núcleo. Temos então que $R = \{6\}$ é um conjunto completo de relações, e o par $\{\{x_1\}, R\}$ é uma apresentação de H.

Em notação multiplicativa, dizer que 6 pertence ao núcleo de ϕ é equivalente a escrever $\phi(6) = 1$, ou $x_1^6 = 1$.

Se tivéssemos escolhido os dois geradores $x_1 = (1,0)$ e $x_2 = (0,1)$ para $\mathbb{Z}_2 \oplus \mathbb{Z}_3$, então o núcleo de ϕ teria como geradores "naturais" os inteiros 2 e 3, ou seja, $R = \{2,3\}$, a que correspondem as identidades $x_1^2 = 1$ e $x_2^3 = 1$. A apresentação de H é aqui o par $\{\{x_1, x_2\}, R\}$.

Infelizmente, a caracterização de um grupo por apresentações não resolve o problema da classificação dos grupos. De facto, Adyan e Rabin[11] mostraram, de forma independente, que em geral é impossível determinar de forma algorítmica se duas apresentações representam ou não grupos isomorfos.

No entanto, podemos efectivamente classificar os grupos abelianos de tipo finito explorando as suas apresentações, o que esboçaremos ainda nesta secção. Estes resultados serão em qualquer caso convenientemente generalizados e desenvolvidos no Capítulo 6, no contexto da teoria dos módulos sobre domínios de ideais principais, uma noção mais geral que a de espaço vectorial, e que inclui enquanto caso especial todos os grupos abelianos, em que o correspondente d.i.p. é o anel $\mathbb{Z}$.

Supomos então que A é um grupo abeliano de tipo finito, gerado por $X = \{x_1, x_2, \cdots, x_n\} \subseteq A$. Seja ainda $L = \oplus_{k=1}^n \mathbb{Z}$ o grupo abeliano livre em X, com $\iota : X \to L$ dada por $\iota(x_k) = \boldsymbol{e}_k$. Os geradores n_i do núcleo de $\phi : L \to A$ são da forma $n_i = (r_{i1}, r_{i2}, \cdots, r_{in})$, com $r_{ik} \in \mathbb{Z}$, e correspondem a relações do tipo $r_{i1}x_1 + r_{i2}x_2 + \cdots + r_{in}x_n = 0$ em A. Repare-se que, em termos prácticos, a *apresentação* de A é, simplesmente, a matriz R, de dimensão $m \times n$, constituída pelas entradas $r_{ik} \in \mathbb{Z}$.

É claro que o conjunto X pode ser substituído por qualquer outro conjunto de geradores de A, e que naturalmente nesse caso a matriz R será diferente. Deixamos como exercício verificar que:

Proposição 4.6.18. *Sendo A gerado por $X = \{x_1, x_2, \cdots, x_n\}$, e a matriz R a lista das relações correspondentes, temos:*

(i) Se S é uma matriz invertível em $M_n(\mathbb{Z})$, então os elementos $y_k = \sum_{k=1}^n s_{kj}x_j$, onde os s_{kj} são as entradas de S, são geradores de A, e

(ii) A matriz RS^{-1} é também uma apresentação do grupo A.

[11] S. Adyan, "The unsolvability of certain algorithmic problems in the theory of groups", *Trudy Moskov. Mat. Obsc.* **6** (1957), 231-298, e M. Rabin, "Recursive unsolvability of group theoretic properties", *Ann. of Math.* **67** (1958), 172-174.

As linhas $l_1, l_2, \cdots, l_m$ da matriz R são os geradores do núcleo de ϕ em L. É igualmente evidente que, se P é uma matriz invertível em $M_m(\mathbb{Z})$, então estes elementos $l_1, l_2, \cdots, l_m$ podem ser substituídos por elementos $l'_1, l'_2, \cdots, \lambda'_m$, onde $l'_k = \sum_{j=1}^{m} p_{kj} l_j$. Neste caso, a apresentação de A passa a ser a matriz PR. De acordo com a proposição acima, podemos agora concluir que:

Proposição 4.6.19. *Se P e Q são matrizes invertíveis, respectivamente em $M_m(\mathbb{Z})$ e $M_n(\mathbb{Z})$, então PRQ é igualmente uma apresentação de A.*

As matrizes P e Q podem, em particular, representar as usuais operações elementares (invertíveis) sobre as linhas e colunas de R, ou seja,

- Trocar linhas ou colunas,
- Somar a uma linha (ou coluna) um múltiplo de outra linha (ou coluna),
- Multiplicar uma linha (ou coluna) por -1.

Exemplos 4.6.20.

1. *Seja A um grupo abeliano gerado por $X = \{x_1, x_2\}$. Supomos que estes geradores satisfazem as relações $6x_1 - 6x_2 = 0$, e $12x_1 + 20x_2 = 0$. Consideramos a sequência de operações:*

$$\begin{pmatrix} 6 & -6 \\ 12 & 20 \end{pmatrix} \longrightarrow \begin{pmatrix} 6 & -6 \\ 30 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 96 & 0 \\ 30 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 96 & 0 \\ 0 & 2 \end{pmatrix}.$$

   Concluímos que A é um grupo abeliano com geradores y_1 e y_2, tais que $2y_1 = 0$, e $96y_2 = 0$. Portanto, $A \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{96}$. Mais exactamente, existe um homomorfismo sobrejectivo $\phi : \mathbb{Z} \oplus \mathbb{Z} \to A$ com núcleo $N = \langle 2 \rangle \oplus \langle 96 \rangle$, e é claro que $A \simeq \mathbb{Z} \oplus \mathbb{Z}/N \simeq \mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 96 \rangle = \mathbb{Z}_2 \oplus \mathbb{Z}_{96}$.

2. *O grupo $\mathbb{Z}_6 \oplus \mathbb{Z}_{16}$ tem geradores $x_1 = (1, 0)$ e $x_2 = (0, 1)$, que satisfazem as relações $6x_1 = 0$ e $16x_2 = 0$. Os cálculos seguintes são muito simples:*

$$\begin{pmatrix} 6 & 0 \\ 0 & 16 \end{pmatrix} \longrightarrow \begin{pmatrix} 6 & 0 \\ 6 & 16 \end{pmatrix} \longrightarrow \begin{pmatrix} 6 & -12 \\ 6 & 4 \end{pmatrix} \longrightarrow$$

$$\begin{pmatrix} 18 & -12 \\ 2 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & -48 \\ 2 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 \\ 0 & 48 \end{pmatrix}.$$

   Neste caso, $\mathbb{Z}_4 \oplus \mathbb{Z}_{16} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{48}$.

Em ambos os exemplos acima, repare-se que o primeiro objectivo do cálculo é a determinação do máximo divisor comum de todas as entradas da matriz dada. Este algoritmo de cálculo resulta apenas da seguinte

Proposição 4.6.21. *Seja $R \in M_n(\mathbb{Z})$, e $d = \mathrm{mdc}(R)$ o máximo divisor comum de todas as entradas de R. Então existem matrizes invertíveis $P, Q \in M_n(\mathbb{Z})$ tais que, sendo $R' = PRQ$, temos $d = \mathrm{mdc}(R') = R'_{11}$.*

Podemos facilmente demonstrar esta proposição, mas como dissémos, será apresentado e provado um resultado bastante mais geral no Capítulo 6. Repare-se apenas que, uma vez obtida uma entrada da matriz igual a $\text{mdc}(R)$, é possível *anular* todas as entradas da mesma linha e da mesma coluna onde ocorre o mdc. Nos exemplos acima, com matrizes 2×2, o cálculo termina com este passo. Para matrizes R de dimensão $n \times n$, com $n > 2$, pode colocar-se o mdc no canto superior esquerdo da matriz, como sugerido no enunciado acima, e anular as restantes entradas da primeira linha e da primeira coluna. O cálculo recomeça, agora na matriz R' de dimensão $(n-1) \times (n-1)$, formada pelos elementos r_{ij}, com $i > 1$ e $j > 1$, onde existem, possivelmente, elementos diferentes de zero. O mdc das entradas de R' é múltiplo do mdc das entradas de R, e obtemos por este processo uma sucessão de inteiros $d'_1|d'_2|\cdots|d'_n$.

Exemplo 4.6.22.

Ilustramos o algoritmo a seguir com uma matriz 3×3.

$$\begin{pmatrix} 3 & 0 & 0 \\ 9 & 6 & 12 \\ 12 & 6 & 24 \end{pmatrix} \longrightarrow \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 12 \\ 0 & 6 & 24 \end{pmatrix} \longrightarrow \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 12 \\ 0 & 0 & 12 \end{pmatrix} \longrightarrow \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 12 \end{pmatrix}$$

O homomorfismo $\phi : \mathbb{Z}^n \to A$ é dado por $\phi(k_1, k_2, \cdots, k_n) = k_1 y_1 + k_2 y_2 + \cdots + k_n y_n$, e o seu núcleo é, claramente, o ideal $N = \langle d'_1 \rangle \oplus \cdots \langle d'_n \rangle$. Concluímos que

$$A \simeq \mathbb{Z}^n / N \simeq \mathbb{Z}_{d'_1} \oplus \cdots \mathbb{Z}_{d'_n}.$$

É possível que $1 = d'_1 = d'_2 = \cdots = d'_k$, para algum $k \leq n$. Os correspondentes grupos quociente $\mathbb{Z}_{d'_i}$ são triviais, e podem por isso ser ignorados. Analogamente, podemos ter também $0 = d'_j = d'_{j+1} = \cdots = d'_n$ para algum $j \leq n$. Neste caso, os correspondentes grupos quociente $\mathbb{Z}_{d'_i} \simeq \mathbb{Z}$. Obtemos finalmente

Teorema 4.6.23 (Classificação dos Grupos Abelianos de Tipo Finito). *Se A é um grupo abeliano de tipo finito, então $A \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m} \oplus \mathbb{Z}^r$, onde $1 < d_1|d_2|\cdots|d_n$.*

O inteiro r é, bem entendido, o número de inteiros d'_j que são nulos, e chama-se CARACTERÍSTICA do grupo abeliano A. Os inteiros $d_1, \ldots, d_n$ chamam-se FACTORES INVARIANTES ou COEFICIENTES DE TORÇÃO do grupo abeliano. Estes inteiros caracterizam o grupo abeliano a menos de isomorfismo. Diz-se, pois, que formam um *conjunto completo de invariantes* de um grupo abeliano.

Em geral, e quando A é um grupo abeliano, o subconjunto de A formado por todos os elementos que possuem ordem finita é o chamado SUBGRUPO DE TORÇÃO de A, que se designa por $\text{Torc}(A)$. Se $\text{Torc}(A)$ é trivial, o grupo

diz-se LIVRE DE TORÇÃO, e se $\mathrm{Torc}(A) = A$, então dizemos que A é um GRUPO DE TORÇÃO. Em todo o caso, o quociente $A/\mathrm{Torc}(A)$ é sempre um grupo livre de torção.

Exemplo 4.6.24.

Os dois exemplos em 4.6.20 são grupos de torção. O grupo A tem factores invariantes 2 e 96, e os factores invariantes de $\mathbb{Z}_6 \oplus \mathbb{Z}_{16}$ são 2 e 48.

Exercícios.

1. Sendo $X \subseteq G$, onde G é um grupo, mostre que a intersecção de todos os subgrupos (respectivamente, subgrupos normais) de G que contêm X é o menor subgrupo (respectivamente, subgrupo normal) de G que contem X.

2. Mostre directamente, a partir da definição de grupo abeliano livre L num conjunto S, que a imagem $\iota(S)$ é um conjunto gerador de L.

3. Demonstre a Proposição 4.6.11.

4. Verifique que, se A_1 e A_2 são grupos abelianos livres gerados por conjuntos finitos, então A_1 e A_2 são isomorfos se e só se possuem a mesma característica.

5. Mostre que o grupo com dois geradores a e b e relações

$$aba^{-1}b^{-1} = 1, \quad a^n = 1, \quad b^m = 1$$

é o grupo abeliano $\mathbb{Z}_n \oplus \mathbb{Z}_m$.

6. Mostre que o grupo com dois geradores σ e ρ e relações

$$\sigma^2 = 1, \quad \rho^n = 1, \quad \rho\sigma = \sigma\rho^{-1}$$

é o grupo de simetrias D_n de um polígono regular de n lados. O elemento ρ representa uma rotação de $2\pi/n$, e o elemento σ representa uma reflexão em relação a um eixo de simetria do polígono.

7. Mostre que o grupo com dois geradores a e b e relações $a^4 = 1$, $a^2b^2 = 1$, $abab^{-1} = 1$, é o grupo $\mathbb{H}_8$.

8. Considere um grupo G com dois geradores a e b e uma relação $a^3b^{-2} = 1$, e um grupo H com dois geradores x e y e uma relação $xyxy^{-1}x^{-1}y^{-1} = 1$. Mostre que estes dois grupos são isomorfos.

9. Dê um exemplo de grupos abelianos A_1 e A_2 não isomorfos, tais que $\mathrm{Torc}(A_1)$ é isomorfo a $\mathrm{Torc}(A_2)$ e $A_1/\mathrm{Torc}(A_1)$ é isomorfo a $A_2/\mathrm{Torc}(A_2)$.

10. Quais são os factores invariantes de $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6$ e de $\mathbb{Z}_{16} \oplus \mathbb{Z}_3$? Estes grupos são isomorfos?

11. Considere os grupos referidos nos exemplos 4.6.20. Em cada caso, existem geradores y_1, y_2 tais que $n_1 y_1 = n_2 y_2 = 0$, onde n_1, n_2 são os factores invariantes do grupo em causa. Qual é a relação entre estes geradores, e os geradores "originais" x_1 e x_2? Quais são os homomorfismos ϕ que nos permitem concluir que os grupos são isomorfos respectivamente a $\mathbb{Z}_2 \oplus \mathbb{Z}_{96}$ e $\mathbb{Z}_2 \oplus \mathbb{Z}_{48}$?

12. Demonstre a Proposição 4.6.15.

13. Seja $\{G_i : i \in I\}$ uma família de grupos não triviais, com $\#I > 1$. Mostre que o produto livre $\prod_{i\in I}^{*} G_i$ é não-abeliano, tem elementos de ordem infinita e o seu centro é trivial.

14. Sejam G e H grupos. Mostre que, se um elemento $g \neq 1$ do produto livre $G * H$ tem ordem finita, então g é conjugado a um elemento de G ou de H.

15. Demonstre as proposições 4.6.18 e 4.6.19.

16. Suposémos na demonstração do teorema 4.6.23 que o número de geradores do núcleo de ϕ (que designámos m) é igual ao número de geradores do grupo A (que designámos n). Esta hipótese envolve alguma perda de generalidade?

Capítulo 5

Grupos Finitos

5.1 Grupos de Transformações

Neste capítulo estudamos um tema clássico da Álgebra, a estrutura dos grupos finitos[1]. Já vimos anteriormente muitos exemplos de grupos finitos, tais como os grupos cíclicos finitos $\mathbb{Z}_n$, os grupos simétricos S_n ou os grupos diedrais D_n. Estes grupos são bastante diferentes, embora possamos encontrar algumas relações entres eles. Por exemplo, D_n contém um subgrupo normal isomorfo a $\mathbb{Z}_n$ (o subgrupo das rotações), e $S_3 = D_3$. O objectivo deste capítulo é precisamente o de estudar os grupos finitos de uma forma sistemática, de forma a tornar evidente tais relações.

Nos capítulos precedentes tivemos a oportunidade de estudar algumas propriedades do grupo simétrico S_n (*i.e.*, o grupo de bijecções do conjunto $\{1, \ldots, n\}$) e dos seus subgrupos. Este grupo assume um papel central no estudo dos grupos finitos, pois, como mostra o Teorema de Cayley, qualquer grupo finito é isomorfo a um subgrupo de S_n. Em geral, chamamos GRUPO DE TRANSFORMAÇÕES de um conjunto X a qualquer subgrupo do grupo S_X das bijecções de X. É muitas vezes útil representar um grupo abstracto na forma de grupo de transformações, pois torna as ideias mais intuitivas e geométricas. Esta noção de grupo de transformações é tão natural que historicamente precedeu a noção abstracta de grupo: os grandes matemáticos do século *XIX* que descobriram resultados fundamentais da Teoria dos Grupos, tais como Galois e Lie, consideravam apenas grupos de transformações, desconhecendo a noção abstracta de grupo que só foi formalizada mais tarde no início do século *XX*.

A passagem de um grupo abstracto para um grupo de transformações

[1]Embora clássico, é um tema ainda muito actual. Por exemplo, a classificação dos grupos finitos simples (uma classe que introduzimos mais à frente) só ficou completa nos anos 1980, estando essa classificação dispersa por centenas de páginas de artigos científicos (ver, por exemplo, o excelente artigo de R. Solomon, "On finite simple groups and their classification", *Notices of the American Mathematical Society* **42**, 231–239 (1995), e as referências aí citadas.)

é feita através da noção de *acção*, cuja definição formal apresentamos de seguida.

Definição 5.1.1. Uma ACÇÃO de um grupo G num conjunto X é uma função $G \times X \to X$, que escrevemos $(g, x) \mapsto gx$, satisfazendo as seguintes propriedades:

(i) $\forall x \in X,\ ex = x$;

(ii) $\forall g_1, g_2 \in G,\ \forall x \in X,\ g_1(g_2 x) = (g_1 \cdot g_2)x$.

Um outro ponto de vista, claramente equivalente, é o seguinte. Suponha-se que o grupo G actua no conjunto X, e para cada $g \in G$ defina-se a transformação $T(g) : X \to X$ pela fórmula $T(g)(x) \equiv gx$. Então as condições (i) e (ii) da definição acima são equivalentes, respectivamente, a:

(i') $T(e) = I$ (transformação identidade);

(ii') $\forall g_1, g_2 \in G,\ T(g_1 \cdot g_2) = T(g_1) \circ T(g_2)$.

Inversamente, dada uma transformação $T(g) : X \to X$, para cada $g \in G$, satisfazendo a (i') e (ii'), obtém-se uma acção de G em X pela fórmula $gx \equiv T(g)(x)$. Note-se, ainda, que cada transformação $T(g)$ é bijectiva.

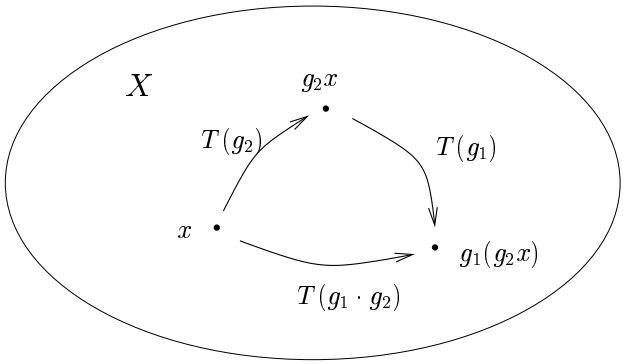


Figura 5.1.1: Acção.

Assim, a aplicação $g \mapsto T(g)$ é um homomorfismo de G para o grupo S_X das bijecções do conjunto X. Chamaremos, pois, a T HOMOMORFISMO ASSOCIADO À ACÇÃO de G em X. Vemos, ainda, que uma acção de G em X realiza G como um grupo de transformações de X. Uma acção diz-se EFECTIVA se o homomorfismo T é injectivo, *i.e.*, se o núcleo do homomorfismo $T : G \to S_X$ se reduz a $\{e\}$. Ao núcleo do homomorfismo T chamamos NÚCLEO DA ACÇÃO.

Actuando G em dois conjuntos distintos X_1 e X_2, com homomorfismos associados T_1 e T_2, dizemos que estas acções são EQUIVALENTES se existir uma bijecção $\phi : X_1 \to X_2$ tal que

$$\phi \circ T_1(g) = T_2(g) \circ \phi, \quad \forall g \in G. \tag{5.1.1}$$

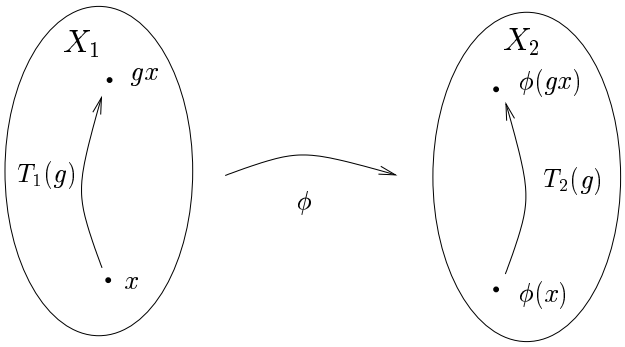


Figura 5.1.2: Acções equivalentes.

Esta equação pode ser ainda expressa pela comutatividade do diagrama:

$$\begin{array}{ccc} X_1 & \xrightarrow{\phi} & X_2 \\ {\scriptstyle T_1(g)}\downarrow & & \downarrow{\scriptstyle T_2(g)} \\ X_1 & \xrightarrow[\phi]{} & X_2 \end{array}$$

Exemplos 5.1.2.

1. *Considere-se o grupo $O(n)$ das matrizes $n \times n$ que satisfazem a condição $AA^T = I$. Podemos definir uma acção de $O(n)$ em $\mathbb{R}^n$ pela fórmula usual $(A, \boldsymbol{x}) \mapsto A\boldsymbol{x}$, obtendo assim uma realização de $O(n)$ como um grupo de transformações de $\mathbb{R}^n$. No Capítulo 1 vimos que para cada $g \in O(n)$ a transformação $T(g)$ é uma isometria de $\mathbb{R}^n$ que fixa a origem. Esta acção é efectiva (porquê?).*

2. *De igual forma, podemos considerar o grupo $E(n)$ formado por todos os pares $(A, \mathbf{b})$, onde $A \in O(n)$ e $\mathbf{b} \in \mathbb{R}^n$, com lei de composição $(A_1, \mathbf{b}_1) \cdot (A_2, \mathbf{b}_2) \equiv (A_1A_2, A_1\mathbf{b}_2 + \mathbf{b}_1)$. Obtemos uma acção de $E(n)$ em $\mathbb{R}^n$ pela fórmula $((A, \mathbf{b}), \boldsymbol{x}) \mapsto A\mathbf{x} + \mathbf{b}$. No Capítulo 1 vimos que as transformações $T(g)$, onde $g \in E(n)$, são isometrias de $\mathbb{R}^n$ e que podemos realizar qualquer isometria desta forma. Esta acção também é efectiva.*

3. *Para um grupo G define-se uma acção de G em si próprio pela fórmula $(g, x) \mapsto g \cdot x$, chamada* ACÇÃO POR TRANSLAÇÕES À ESQUERDA *(ou também por multiplicação à esquerda). Esta acção é efectiva (porquê?). Podemos igualmente definir a acção de G em si próprio por translações à direita através da fórmula $(g, x) \mapsto xg^{-1}$. Estas acções são equivalentes: a equivalência é dada pela aplicação $\phi : X \to X$ definida por $x \mapsto x^{-1}$.*

4. Uma outra acção de G em si próprio é a ACÇÃO POR CONJUGAÇÃO*, definida da seguinte forma:*

$$(g,x) \mapsto {}^{g}x \equiv gxg^{-1}, \quad g,x \in G. \tag{5.1.2}$$

É um exercício simples verificar que (i) e (ii) da Definição 5.1.1 são satisfeitas, e que se podem escrever, respectivamente, na forma

$${}^{e}x = x, \qquad {}^{g_1}({}^{g_2}x) = {}^{g_1 \cdot g_2}x.$$

Deixamos como exercício verificar que o núcleo desta acção é precisamente o centro de G.

5. Seja G um grupo e $H \subset G$ um subgrupo. No espaço quociente G/H existe uma acção natural de G definida pela fórmula $(g, xH) \mapsto (g{\cdot}x)H$. Um elemento $g \in G$ pertence ao núcleo desta acção se e só se:

$$(g \cdot x)H = xH, \ \forall x \in G \qquad \Longleftrightarrow \qquad g \in xHx^{-1}, \forall x \in G.$$

Portanto o núcleo desta acção é

$$\bigcap_{x \in G} xHx^{-1}.$$

Deixamos como exercício verificar que este é o maior subgrupo normal de G que está contido em H, de forma que a acção é efectiva se e só se não existe qualquer subgrupo de H, $\neq \{e\}$, normal em G.

Uma aplicação muito simples do conceito de homomorfismo associado à acção fornece o seguinte resultado que já tínhamos encontrado num exercício de um capítulo anterior.

Teorema 5.1.3 (Cayley). *Seja G um grupo finito de ordem n. Então G é isomorfo a um subgrupo de S_n.*

Demonstração. Considere-se o homomorfismo associado à acção de G em si próprio por translações à esquerda. Esta acção é efectiva, logo o homomorfismo associado

$$T : G \to S_G \simeq S_n$$

é um monomorfismo. □

Se G actua num conjunto X obtém-se uma partição de X da seguinte forma. Definimos uma relação de equivalência $\sim$ em que dois elementos de X se dizem equivalentes, se podemos transformar um elemento no outro pela acção do grupo, *i.e.*, se $x, y \in X$, então $x \sim y$ se existe um elemento $g \in G$ tal que $x = gy$. A uma classe de equivalência chamamos uma G-ÓRBITA. Obtemos, pois, uma partição de X em G-órbitas, onde a G-órbita que contém o elemento $x \in X$ é precisamente $\mathcal{O}_x \equiv \{gx \colon g \in G\}$. O conjunto das G-órbitas designa-se por X/G. No caso em que X é um conjunto finito

existe um número finito de órbitas $\mathcal{O}_1, \ldots, \mathcal{O}_n$, e cada órbita possui um número finito de elementos, obtendo-se a seguinte *equação das classes*:

$$|X| = |\mathcal{O}_1| + \cdots + |\mathcal{O}_n|. \tag{5.1.3}$$

Uma acção diz-se TRANSITIVA se possui uma só órbita.

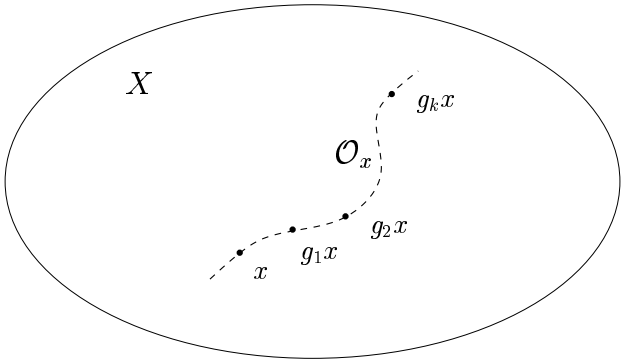


Figura 5.1.3: A G-órbita de x.

Exemplos 5.1.4.

1. *As órbitas da acção do grupo $O(n)$ em $\mathbb{R}^n$ são as esferas $S_r = \{|\boldsymbol{x}| = r : \boldsymbol{x} \in \mathbb{R}^n\}$ $(r > 0)$ e a origem $\{\mathbf{0}\}$.*

2. *A acção de G em si próprio por translações (à direita ou à esquerda) possui uma só órbita, sendo portanto transitiva.*

3. *Se $H \subset G$ é um subgrupo, as H-órbitas da acção de H em G por translações à esquerda (respectivamente, direita) são as classes laterais direitas (respectivamente, esquerdas) de H, de forma que $G/H = \{Hg : g \in G\}$. No Capítulo 4 vimos que todas as órbitas desta acção têm o mesmo cardinal e que a partir deste facto se deduz imediatamente, utilizando a equação de classes (5.1.3), o Teorema de Lagrange.*

4. *Consideremos a acção de G em si próprio por conjugação. Às G-órbitas chamamos* CLASSES DE CONJUGAÇÃO, *e a classe de conjugação que contém o elemento $x \in G$ designa-se por ${}^G x$. Dois elementos dizem-se conjugados se pertencem à mesma classe. Um elemento x pertence ao centro $C(G)$ se e só se a classe ${}^G x = \{x\}$, de forma que $C(G)$ é precisamente a união de todas as classes que contêm apenas um só elemento.*

Definição 5.1.5. Se G actua em X, o SUBGRUPO DE ISOTROPIA de um elemento $x \in X$ é o subgrupo $G_x \subset G$ definido por

$$G_x = \{g \in G : gx = x\}. \tag{5.1.4}$$

Se dois elementos $x, y \in X$ pertencem à mesma órbita, os respectivos subgrupos de isotropia são conjugados. De facto, se $y = gx$ para algum $g \in G$, então temos que

$$\begin{aligned} h \in G_x \quad &\iff \quad hx = x, \\ &\iff \quad hg^{-1}y = g^{-1}y, \\ &\iff \quad ghg^{-1}y = y \quad \iff \quad ghg^{-1} \in G_y. \end{aligned}$$

Logo os subgrupos de isotropia de x e de y estão relacionados por

$$G_y = gG_xg^{-1}.$$

Temos, ainda, que as órbitas são completamente determinadas pelos subgrupos de isotropia, como mostra a seguinte proposição:

Proposição 5.1.6. *Suponha-se que um grupo G actua num conjunto finito X.*

i) Se a acção de G em X é transitiva, então é equivalente à acção natural de G em G/G_x.

(ii) Se $X = \mathcal{O}_1 + \cdots + \mathcal{O}_n$ é a partição de X em G-órbitas e $x_i \in \mathcal{O}_i$, então

$$|X| = \sum_{i=1}^{n} [G : G_{x_i}]. \tag{5.1.5}$$

Deixamos a demonstração como exercício.

As acções que temos vindo a descrever são por vezes qualificadas de *acções à esquerda*, pois obedecem à condição (ii) da Definição (5.1.1). Por vezes é também útil considerar *acções à direita* onde a acção $X \times G \to X$ se escreve na forma $(x, g) \mapsto xg$ e em que (ii) é substituída por

$$\forall g_1, g_2 \in G,\ \forall x \in X,\ (xg_1)g_2 = x(g_1 \cdot g_2).$$

Salvo menção em contrário, utilizaremos sempre acções à esquerda, e por defeito omitimos o adjectivo. É um exercício útil verificar como se devem modificar os exemplos desta secção para se obterem acções à direita.

Exercícios.

1. Mostre que o núcleo da acção de G em si próprio por conjugação é o centro $C(G)$.

2. Mostre que, se H é um subgrupo de G, então $\bigcap_{x \in G} xHx^{-1}$ é o maior subgrupo normal de G que está contido em H.

3. Demonstre a Proposição 5.1.6.

4. Diz-se que uma acção de um grupo G num conjunto X é uma ACÇÃO LIVRE se todo o $g \in G$ com $g \neq e$ actua sem pontos fixos, *i.e.*, se os subgrupos de isotropia G_x para todo o $x \in X$ são triviais. Mostre que um acção livre é efectiva e determine quais das acções introduzidas nos exemplos 5.1.2 são livres.

5. Diz-se que um grupo G ACTUA POR AUTOMORFISMOS num grupo K se existe uma acção de G em K tal que, para cada $g \in G$, a aplicação $k \mapsto gk$ é um automorfismo de K. Assuma que G actua por automorfismos em K e mostre que:
   (a) a operação $(g_1, k_1)*(g_2, k_2) = (g_1g_2, k_1(g_1k_2))$ define um grupo $(G\times K, *)$, chamado o *produto semidirecto* de G por K, e que se designa por $G \ltimes K$;
   (b) as aplicações $G \to G \ltimes K\colon g \mapsto (g, e)$ e $K \to G \ltimes K\colon k \mapsto (e, k)$ são monomorfismos. A imagem do segundo monomorfismo é um subgrupo normal de $G \ltimes K$.

6. Considere a acção de $O(n)$ em $\mathbb{R}^n$. Mostre que esta acção é por automorfismos, e descreva o produto semidirecto $O(n) \ltimes \mathbb{R}^n$.

7. Determine a partição do grupo simétrico S_n em classes de conjugação. (SUGESTÃO: Considere primeiro o caso $n = 3$.)

5.2 Teoremas de Sylow

Sabemos que, se G é um grupo cíclico, então para cada divisor d de $|G|$ existe um e um só subgrupo de G de ordem d. Em geral, para um grupo finito G, é pois natural pôr a seguinte questão:

- Dado um factor d da ordem do grupo $|G|$, existirá um subgrupo de G de ordem d?

Exploramos nesta secção a acção por conjugação do grupo G em si próprio, e a correspondente equação de classes (5.1.3), no estudo desta questão.

Suponhamos que $x \in G$. O subgrupo de isotropia de x para a acção por conjugação de G é precisamente

$$\{g \in G : g \cdot x \cdot g^{-1} = x\} = \{g \in G : g \cdot x = x \cdot g\},$$

i.e., o conjunto de todos os elementos de G que comutam com x. É pois natural chamar a este conjunto o CENTRALIZADOR do elemento x, que vamos designar por $C_G(x)$. Seja ${}^Gx$ a G-órbita de x, *i.e.*, a classe de conjugação que contém x. Então ${}^Gx$ é isomorfa a $G/C_G(x)$ e, portanto, temos

$$|{}^Gx| = [G : C_G(x)].$$

Da Proposição 5.1.6 obtemos o seguinte resultado:

Proposição 5.2.1. *Para um grupo finito G é válida a seguinte fórmula:*

$$|G| = |C(G)| + \sum_{i=1}^{n} [G : C_G(x_i)], \tag{5.2.1}$$

onde $x_1, \ldots, x_n$ são representantes das classes de conjugação de G que contêm mais do que um elemento.

Demonstração. Observe-se que o centro $C(G)$ consiste precisamente da união das classes de conjugação que contêm apenas um elemento. Pela equação de classes na forma (5.1.5) obtemos a fórmula (5.2.1). □

Como veremos de seguida, a fórmula que acabámos de demonstrar é muito útil para excluir a existência de subgrupos de certas ordens. Por exemplo, uma aplicação imediata permite obter uma classe de grupos com centros não triviais.

Proposição 5.2.2. *Se $|G| = p^m$, onde p é um primo, o centro de G tem ordem p^k, onde $k \geq 1$.*

Demonstração. Pelo Teorema de Lagrange a ordem do centro $C(G)$ divide a ordem de G, logo, pela equação de classes (5.2.1), obtemos

$$p^m = p^k + \sum_{i=1}^{n} [G : C_G(x_i)].$$

Como cada x_i corresponde a uma classe de conjugação com mais de um elemento, temos que $[G : C_G(x_i)] = p^{m_i}$, com $m_i \geq 1$, logo:

$$p^k = p^m - \sum_{i=1}^{n} p^{m_i}, \quad m, m_i \geq 1$$

e, necessariamente, $k \geq 1$. □

Corolário 5.2.3. *Se $|G| = p^2$ então G é abeliano.*

Demonstração. Pela proposição anterior sabemos que $|C(G)| = p$ ou p^2. Deixamos como exercício verificar que o primeiro caso não pode acontecer. □

O próximo resultado é uma resposta parcial à questão posta no inicio desta secção no caso de grupos abelianos.

Teorema 5.2.4 (Cauchy). *Se G é um grupo abeliano finito e p é um factor primo de $|G|$, então G contém um elemento g de ordem p.*

Demonstração. A demonstração é por indução na ordem $|G|$ de G. Se $|G| = p$ o resultado é uma consequência óbvia do Teorema de Lagrange. Assuma-se, pois, que $|G| > p$, e fixe-se um elemento $a \in G$. Então há dois casos a considerar:

(i) a é um elemento de ordem divisível por p. Então o grupo cíclico $\langle a \rangle$ contém um elemento g de ordem p, e o teorema é verdadeiro.

(ii) p não divide a ordem de a. Neste caso, o grupo $G/\langle a \rangle$ tem ordem divisível por p, donde, pela hipótese de indução, contém um elemento de ordem p. Representando este elemento na forma $b\langle a \rangle$, a ordem s de b é divisível por p, pois temos $\langle a \rangle = b^s \langle a \rangle = (b\langle a \rangle)^s$. Logo, o subgrupo cíclico $\langle b \rangle$ contém um elemento g de ordem p.

□

O Teorema de Cauchy é válido para grupos finitos abelianos. Veremos mais adiante que estes grupos podem ser completamente classificados. Esta classificação torna claro quais os possíveis subgrupos dum grupo abeliano finito. Por outro lado, para grupos não-abelianos temos a seguinte generalização do Teorema de Cauchy[2].

Teorema 5.2.5 (Sylow I). *Seja G um grupo finito. Se p^k é um factor da ordem de $|G|$, então existe um subgrupo H de G de ordem p^k.*

Demonstração. Provamos este resultado por indução em $|G|$. Mais uma vez começamos com a equação de classes (5.2.1):

$$|G| = |C(G)| + \sum_{i=1}^{n} [G : C_G(x_i)].$$

(i) Se $p \nmid |C(G)|$, então para algum $i \in \{1, \ldots, n\}$ temos que $p \nmid [G : C_G(x_i)]$, logo conclui-se que $C_G(x_i)$ é um subgrupo de G cuja ordem é inferior a $|G|$ e divisível por p^k. Por hipótese de indução, existe um subgrupo H de $C_G(x_i)$ de ordem p^k.

(ii) Se $p \mid |C(G)|$, pelo Teorema de Cauchy existe um elemento $g \in C(G)$ de ordem p, e o subgrupo $\langle g \rangle$ é normal em G. O grupo $G/\langle g \rangle$ tem ordem inferior a $|G|$ e divisível por p^{k-1}, donde, por indução, contém um subgrupo de ordem p^{k-1}. Este subgrupo é da forma $H/\langle g \rangle$, onde H é um subgrupo de G, e $|H| = [H : \langle g \rangle]\ |\langle g \rangle| = p^{k-1}p = p^k$.

□

[2] O conjunto de resultados que se seguem deve-se ao matemático norueguês Ludvig Sylow (1832-1918) e foram publicados pela primeira vez no artigo "Théorèmes sur les groups de substitutions", *Math. Ann.,* **5** (1872).

Este resultado motiva as seguintes definições:

Definição 5.2.6. A um grupo de ordem p^k chama-se p-GRUPO (DE EXPOENTE k). A um p-subgrupo $H \subset G$ em que o expoente k é maximal chama-se p-SUBGRUPO DE SYLOW.

Os p-subgrupos de Sylow de um grupo G são de certo modo análogos aos subgrupos de um grupo cíclico, como mostra o seguinte resultado:

Teorema 5.2.7 (Sylow II). *Seja G um grupo finito. Então:*

(i) Os p-subgrupos de Sylow de G são únicos a menos de conjugação por um elemento $g \in G$.

(ii) O número de p-subgrupos de Sylow de G é um divisor do índice de qualquer p-subgrupo de Sylow e é $\equiv 1 \pmod{p}$.

(iii) Qualquer subgrupo de ordem p^k é um subgrupo de um p-subgrupo de Sylow.

A demonstração do 1º Teorema de Sylow baseava-se na acção de G em si próprio por conjugação. Na demonstração do segundo Teorema de Sylow vamos utilizar a acção de G por conjugação no conjunto dos seus subgrupos: se $H \subset G$ é um subgrupo, então gHg^{-1}, $g \in G$, é um subgrupo de G e $|gHg^{-1}| = |H|$. Para esta acção, o subgrupo de isotropia de um subgrupo $H \subset G$ é precisamente $N_G(H) \equiv \{g \in G : gHg^{-1} = H\}$, a que é costume chamar-se NORMALIZADOR de H em G. Note-se que H é normal em $N_G(H)$, e deixa-se como exercício mostrar que $N_G(H)$ é o maior subgrupo de G que contém H como subgrupo normal. Esta acção de G induz, por restrição, uma acção de G no conjunto Π dos p-subgrupos de Sylow de G.

Lema 5.2.8. *Seja P um p-subgrupo de Sylow de G, e $H \subset N_G(P)$ um subgrupo de ordem p^k. Então $H \subset P$.*

Demonstração do Lema 5.2.8. Como P é um subgrupo normal de $N_G(P)$, temos o homomorfismo $\pi : N_G(P) \to N_G(P)/P$. Como H é um subgrupo de $N_G(P)$, $\pi(H)$ é um subgrupo de $N_G(P)/P$ de ordem uma potência de p. Como P é um p-subgrupo de Sylow de G, também é um p-subgrupo de Sylow de $N_G(P)$ e concluímos que $p \not| |N_G(P)/P|$. Mas então $\pi(H) = \{e\}$, ou seja, $H \subset P$. □

Demonstração de 2º Teorema de Sylow. Tomemos a acção por conjugação de G no conjunto Π dos p-subgrupos de Sylow, e designe-se por $\mathcal{O}_P$ a órbita de um p-subgrupo de Sylow P. Então:

(a) $|\mathcal{O}_P| \equiv 1 \pmod{p}$: Considere-se a acção do grupo P em $\mathcal{O}_P$ induzida da acção de G (note-se que esta última é transitiva por definição, mas a primeira não o é). As P-órbitas que não contêm P têm cardinalidade

superior a 1, pois se $\{\tilde{P}\}$ é uma P-órbita diferente de P, então $\tilde{P}$ é um p-subgrupo de Sylow distinto de P e $P \subset N_G(\tilde{P})$, o que contradiz o Lema 5.2.8. Por outro lado, toda a P-órbita tem como cardinal uma potência de p, logo, $|\mathcal{O}_P| = 1 + \sum_i p^{k_i}$.

(b) $\mathcal{O}_P = \Pi$: Suponha-se que $\tilde{P} \in \Pi - \mathcal{O}_P$. Aplicando o raciocínio acima à acção de $\tilde{P}$ em $\mathcal{O}_P$, concluímos que $|\mathcal{O}_P| \equiv 0 \pmod{p}$, contradizendo (a).

A parte (i) do 2º Teorema de Sylow é equivalente a (b). Por sua vez, para a parte (ii), observamos que (b) implica

$$|\Pi| = |G/N_G(P)| = [G : N_G(P)].$$

Como $P \subset N_G(P) \subset G$, temos que:

$$[G : P] = [G : N_G(P)][N_G(P) : P],$$

logo o número de p-subgrupos é um divisor de $[G : P]$. Finalmente, para a parte (iii) do teorema, observe-se que, se $H \subset G$ é um subgrupo de ordem p^k, então as órbitas da acção de H em Π têm como cardinal uma potência de p. Mas por (a) e (b), uma delas é da forma $\{\tilde{P}\}$ e, claramente, $H \subset N_G(\tilde{P})$, logo, pelo Lema 5.2.8, $H \subset \tilde{P}$, como se pretendia. □

Exemplos 5.2.9.

1. *Consideremos o grupo simétrico $S_3 = \{I, \alpha, \beta, \gamma, \delta, \varepsilon\}$. Como $|S_3| = 6$, pelo 1º Teorema de Sylow existem p-subgrupos de Sylow de ordens 2 e 3.*

   Pelo 2º Teorema de Sylow, o número de subgrupos de Sylow de ordem 3 tem de ser igual a 1 (mod 3) e um divisor de 2. Logo, existe 1 subgrupo de ordem 3. Obviamente, conhecemos um subgrupo de S_3 de ordem 3, nomeadamente

   $$P = \{I, \delta, \varepsilon\}.$$

   De igual forma, o número de subgrupos de Sylow de ordem 2 tem de ser igual a 1 (mod 2) e um divisor de 3. Logo, podemos ter 1 ou 3 subgrupos de ordem 2. Neste caso existem 3 subgrupos de ordem 2:

   $$P_1 = \{I, \alpha\}, \qquad P_2 = \{I, \beta\}, \qquad P_3 = \{I, \gamma\}.$$

   É fácil de verificar que estes subgrupos de Sylow obedecem às seguintes relações de conjugação:

   $$P_1 = \delta P_2 \delta^{-1} = \varepsilon P_3 \varepsilon^{-1}.$$

2. *O subgrupo A_4 de S_4 formado pelas permutações pares tem ordem 12. Pelo 1º Teorema de Sylow, existem p-subgrupos de Sylow de ordens 3 e 4.*

   Pelo 2º Teorema de Sylow, o número de subgrupos de Sylow de ordem 3 pode ser 1 ou 4. É fácil de verificar que existem 4 subgrupos de Sylow de ordem 3:

   $$P_1 = \{I, (123), (321)\} \qquad P_2 = \{I, (124), (421)\}$$
   $$P_3 = \{I, (134), (431)\} \qquad P_4 = \{I, (234), (432)\}.$$

   Deixamos com exercício verificar que estes subgrupos são conjugados e determinar os p-subgrupos de Sylow de ordem 4.

Exercícios.

1. Mostre que, se G é um grupo finito e $|G| = p^2$, então G é isomorfo a $\mathbb{Z}_{p^2}$ ou a $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

2. Mostre que, se G é um grupo abeliano finito em que todos os elementos, à excepção de e, têm ordem p, então $|G| = p^n$ e $G \simeq \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$.

3. Classifique os grupos finitos de ordem ≤ 7.

4. Mostre que o normalizador $N_G(H)$ de um subgrupo $H \subset G$ é o maior subgrupo de G que contém H como subgrupo normal.

5. Determine os p-subgrupos de Sylow do grupo alternado A_4 e as relações de conjugação a que obedecem.

6. Determine todos os p-subgrupos de Sylow do grupo de quaterniões $\mathbb{H}_8 = \{\mathbf{1}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}, -\mathbf{1}, -\boldsymbol{i}, -\boldsymbol{j}, -\boldsymbol{k}\}$.

7. Determine os p-subgrupos de Sylow do grupo diedral D_p quando p é primo.

8. Seja $\phi : G_1 \to G_2$ um epimorfismo de grupos finitos. Mostre que, se $P \subset G_1$ é um p-subgrupo de Sylow, então $\phi(P)$ é um p-subgrupo de Sylow de G_2.

9. Mostre que, se $P \subset G$ é um subgrupo de Sylow, então $N_G(N_G(P)) = N_G(P)$.

5.3 Grupos Nilpotentes e Resolúveis

Os p-grupos estudados na secção anterior desempenham um papel central na estrutura dos grupos finitos. Um p-grupo é um exemplo de um grupo nilpotente. Nesta secção estudamos esta classe de grupos, bem como a classe mais larga dos grupos resolúveis. A introdução destas classes surge naturalmente quando se estuda a possibilidade de comutar dois elementos no grupo.

Seja G um grupo abstracto. O COMUTADOR de dois elementos $g_1, g_2 \in G$ é o elemento ${g_1}^{-1}{g_2}^{-1}g_1g_2 \in G$. Designa-se este elemento por (g_1, g_2) [3], de forma que

$$g_1g_2 = g_2g_1(g_1, g_2),$$

logo vemos que (g_1, g_2) mede o grau de não-comutatividade de g_1 e g_2. O resultado seguinte fornece algumas propriedades elementares dos comutadores cuja verificação é um exercício simples.

[3] Por vezes também se designa este elemento por $[g_1, g_2]$, mas vamos reservar esta notação para o comutador noutro contexto, o das chamadas *álgebras de Lie*.

Proposição 5.3.1 (Propriedades dos comutadores). *Sejam $g_1, g_2, g_3 \in G$ elementos dum grupo. Então:*

(i) $(g_1, g_2)^{-1} = (g_2, g_1)$;

(ii) $(g_1, g_2) = e$ *se e só se* g_1 *e* g_2 *comutam;*

(iii) ${}^g(g_1, g_2) = ({}^g g_1, {}^g g_2)$;

(iv) $(g_1 g_2, g_3) \cdot (g_2 g_3, g_1) \cdot (g_3 g_1, g_2) = e$;

(v) Se $\phi : G \to H$ *é um homomorfismo de grupos, então* $\phi((g_1, g_2)) = (\phi(g_1), \phi(g_2))$.

Sejam $A, B \subset G$ dois subgrupos. Designa-se por (A, B) o subgrupo gerado pelos comutadores da forma (a, b), em que $a \in A$ e $b \in B$. Por definição, (A, B) é o menor subgrupo de G que contém todos os elementos da forma (a, b), com $a \in A,\ b \in B$. Observe-se que, sendo (A, B) um grupo, temos $(a, b) \in (A, B) \Rightarrow (b, a) = (a, b)^{-1} \in (A, B)$, e vemos que $(A, B) = (B, A)$. Note-se também que podem existir elementos em (A, B) que não sejam comutadores. Na verdade, em geral, os elementos de (A, B) tomam a forma

$$(a_1, b_1)^{\pm 1} \cdot (a_2, b_2)^{\pm 1} \cdots (a_s, b_s)^{\pm 1}, \qquad a_i \in A,\ b_i \in B,$$

com $s \geq 1$.

Definição 5.3.2. O GRUPO DERIVADO de G é o subgrupo (G, G) de G. Designamos este grupo por $\mathcal{D}(G)$.

Também é costume chamar-se a $\mathcal{D}(G)$ o *grupo dos comutadores* de G, mas esta designação é um pouco infeliz, pois, como observámos acima, podem existir elementos de $\mathcal{D}(G)$ que não são comutadores.

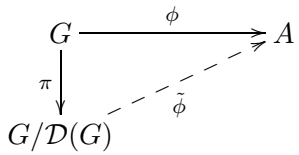
A próxima proposição fornece uma caracterização do grupo derivado, bem como as suas propriedades elementares.

Proposição 5.3.3 (Propriedades do grupo derivado). *Sejam G, G_1 e G_2 grupos.*

(i) Se $\phi : G_1 \to G_2$ *é um homomorfismo de grupos, então* $\phi(\mathcal{D}(G_1)) \subset \mathcal{D}(G_2)$, *e se* ϕ *é sobrejectivo, então* $\phi(\mathcal{D}(G_1)) = \mathcal{D}(G_2)$.

(ii) $\mathcal{D}(G)$ *é um subgrupo normal de* G.

(iii) $G/\mathcal{D}(G)$ *é um grupo abeliano, e todo o homomorfismo* $\phi : G \to A$ *para um grupo abeliano* A *factoriza-se na forma* $\phi = \tilde{\phi} \circ \pi$, *onde* $\pi : G \to G/\mathcal{D}(G)$ *é a projecção canónica e* $\tilde{\phi} : G/\mathcal{D}(G) \to A$ *é um homomorfismo de grupos abelianos:*



Demonstração. (i) Óbvio, pela propriedade (v) dos comutadores.

(ii) Para cada $g \in G$, a aplicação $h \mapsto ghg^{-1}$ é um automorfismo de G, logo, por (i), temos que $g\mathcal{D}(G)g^{-1} \subset \mathcal{D}(G)$ e $\mathcal{D}(G)$ é normal em G.

(iii) Como $g \cdot h = h \cdot g \cdot (g,h)$ é claro que $G/\mathcal{D}(G)$ é um grupo abeliano. Se $\phi : G \to A$ é um homomorfismo de G para um grupo abeliano A, vemos que

$$\begin{array}{rcl} \bar{g} = g \cdot (a,b) \implies \phi(\bar{g}) & = & \phi(g \cdot (a,b)) \\ & = & \phi(g) \cdot (\phi(a), \phi(b)) \\ & = & \phi(g), \end{array}$$

logo, podemos definir $\tilde{\phi} : G/\mathcal{D}(G) \to A$ pela fórmula $\tilde{\phi}(g\mathcal{D}(G)) \equiv \phi(g)$. É simples verificar que $\tilde{\phi}$ é um homomorfismo. Por construção, $\phi = \tilde{\phi} \circ \pi$, onde $\pi : G \to G/\mathcal{D}(G)$ é a projecção natural.

□

Exemplos 5.3.4.

1. *Um grupo G é abeliano se e só se o seu grupo derivado é $\mathcal{D}(G) = \{e\}$.*
2. *O grupo $\mathbb{H}_8 = \{\mathbf{1}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}, -\mathbf{1}, -\boldsymbol{i}, -\boldsymbol{j}, -\boldsymbol{k}\}$ tem como grupo derivado $\mathcal{D}(\mathbb{H}_8) = \{\mathbf{1}, -\mathbf{1}\} \simeq \mathbb{Z}_2$, pois os comutadores de elementos deste grupo são iguais a $\mathbf{1}$ ou a $-\mathbf{1}$. Este grupo é normal em $\mathbb{H}_8$ e o grupo quociente $\mathbb{H}_8/\mathcal{D}(\mathbb{H}_8)$ é isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (exercício).*
3. *O grupo simétrico $S_3 = \{I, \alpha, \beta, \gamma, \delta, \varepsilon\}$ tem como grupo derivado o grupo alternado $A_3 = \{I, \delta, \varepsilon\}$. De facto, o comutador de duas permutações é necessariamente uma permutação par e verifica-se facilmente que, por exemplo, $\delta = (\alpha, \gamma)$ e $\varepsilon = (\gamma, \alpha)$, logo todas as permutações pares são comutadores. O grupo A_3 é normal em S_3 e $S_3/A_3 \simeq \mathbb{Z}_2$.*

Para um grupo G define-se a SÉRIE CENTRAL INFERIOR $\{\mathcal{C}^k(G)\}_{k \geq 0}$ indutivamente pelas fórmulas

$$\mathcal{C}^0(G) \equiv G, \qquad \mathcal{C}^{k+1}(G) \equiv (G, \mathcal{C}^k(G)) \quad (k \geq 0).$$

Os grupos em que esta série estabiliza em $\{e\}$ formam uma subclasse bastante importante.

Definição 5.3.5. Um grupo G diz-se NILPOTENTE se, para algum n,

$$\mathcal{C}^n(G) = \{e\}.$$

Ao menor inteiro n em que isto ocorre chama-se CLASSE DE NILPOTÊNCIA de G.

Exemplos 5.3.6.

1. *Um grupo é nilpotente de classe ≤ 1 se e só se é abeliano.*
2. *O grupo $\mathbb{H}_8$ é nilpotente de classe 2, pois temos $\mathcal{C}^0(\mathbb{H}_8) = \mathbb{H}_8$, $\mathcal{C}^1(\mathbb{H}_8) = (\mathbb{H}_8, \mathbb{H}_8) = \mathbb{Z}_2$, $\mathcal{C}^2(\mathbb{H}_8) = (\mathbb{H}_8, \mathbb{Z}_2) = \{e\}$.*
3. *O subgrupo de $GL(n, \mathbb{R})$ formado pelas matrizes triangulares superiores, com 1s na diagonal principal, é nilpotente de classe $n-1$.*

É possível fornecer descrições alternativas dos grupos nilpotentes. Para isso convém introduzir a seguinte notação: Uma TORRE DE SUBGRUPOS de G é uma sucessão de subgrupos

$$G = G^0 \supset G^1 \supset \cdots \supset G^m.$$

Uma TORRE NORMAL é uma torre em que, para todo o k, G^{k+1} é normal em G^k. Neste caso escrevemos

$$G = G^0 \rhd G^1 \rhd \ldots \rhd G^m.$$

Uma TORRE ABELIANA é uma torre normal em que, para todo o k, G^k/G^{k+1} é um grupo abeliano.

Proposição 5.3.7. *As seguintes afirmações são equivalentes:*

(i) *G é nilpotente de classe $\leq n$.*

(ii) *Existe uma torre de subgrupos $G = G^0 \supset G^1 \supset \cdots \supset G^n = \{e\}$ com $G^{k+1} \supset (G, G^k)$.*

(iii) *Existe um subgrupo A do centro $C(G)$ de G tal que G/A é nilpotente de classe $\leq n-1$.*

Demonstração. Verificamos que (i) é equivalente a (ii) e a (iii).

(i) $\Leftrightarrow$ (ii). Se G é nilpotente de classe $\leq n$, então a torre $G^k \equiv \mathcal{C}^k(G)$ satisfaz (ii). Por outro lado, dada uma torre como em (ii), mostra-se por indução que $\mathcal{C}^k(G) \subset G^k$. De facto, $\mathcal{C}^0(G) = G = G^0$ e

$$\mathcal{C}^k(G) \subset G^k \Rightarrow \mathcal{C}^{k+1}(G) = (G, \mathcal{C}^k(G)) \subset (G, G^k) \subset G^{k+1}.$$

Logo, $\mathcal{C}^n(G) \subset G^n = \{e\}$, e concluímos que G é nilpotente de classe $\leq n$.

(i) $\Leftrightarrow$ (iii). Se G é nilpotente de classe $\leq n$, temos $(G, \mathcal{C}^{n-1}(G)) = \mathcal{C}^n(G) = \{e\}$, logo $A = \mathcal{C}^{n-1}(G)$ é um subgrupo central. Deixamos como exercício verificar que G/A é nilpotente de classe $\leq n-1$.

Inversamente, seja A um subgrupo central de G tal que G/A é nilpotente de classe $\leq n-1$. A projecção natural $\pi : G \to G/A$ é sobrejectiva, logo $\pi(G, G) = (G/A, G/A)$ e, por iteração, concluímos que

$\pi(\mathcal{C}^{n-1}(G)) = \mathcal{C}^{n-1}(G/A) = \{e\}$. Segue-se que $\mathcal{C}^{n-1}(G) \subset A$ e, como A é central, obtemos

$$\mathcal{C}^n(G) = (G, \mathcal{C}^{n-1}(G)) \subset (G, A) = \{e\}.$$

Isto mostra que G é nilpotente de classe $\leq n$. □

Introduzimos agora uma outra classe de grupos que inclui a classe dos grupos nilpotentes. Para isso definimos a SÉRIE DERIVADA $\{\mathcal{D}^k(G)\}_{k\in\mathbb{N}}$ de G indutivamente pelas fórmulas

$$\begin{aligned} \mathcal{D}^0(G) &\equiv G, \\ \mathcal{D}^{k+1}(G) &\equiv \mathcal{D}(\mathcal{D}^k(G)), \quad (k \geq 0). \end{aligned}$$

Deixamos como exercício a verificação das seguintes relações:

$$\begin{aligned} &\mathcal{D}^0(G) = \mathcal{C}^0(G) = G, \\ &\mathcal{D}^1(G) = \mathcal{C}^1(G) = (G, G) = \mathcal{D}(G), \\ &\mathcal{D}^k(G) \subset C^{2^k-1}(G), \quad (k \geq 0). \end{aligned} \tag{5.3.1}$$

Analogamente ao caso da série central, introduzimos a

Definição 5.3.8. Um grupo G diz-se RESOLÚVEL se, para algum n,

$$\mathcal{D}^n(G) = \{e\}.$$

Ao menor inteiro n em que isto ocorre chama-se CLASSE DE RESOLUBILIDADE de G.

Exemplos 5.3.9.

1. *Um grupo é resolúvel de classe ≤ 1 se, e só se, é abeliano.*
2. *Todo o grupo nilpotente de classe $\leq 2^n - 1$ é resolúvel de classe $\leq n$.*
3. *O grupo de simetrias D_3 de um triângulo equilátero é resolúvel de classe 2. O seu grupo derivado é precisamente o subgrupo das rotações próprias, logo $\mathcal{D}^2(D_3) = \{e\}$.*
4. *Mais geralmente, o grupo diedral D_n de ordem $2n$ é resolúvel.*
5. *O subgrupo de $GL(n, \mathbb{R})$ formado pelas matrizes triangulares superiores invertíveis é resolúvel.*

Outros exemplos de grupos resolúveis podem ser obtidos a partir das seguintes caracterizações alternativas, análogas às que demos anteriormente para os grupos nilpotentes (ver Proposição 5.3.7). A demonstração desta proposição é deixada como exercício.

Proposição 5.3.10. *As seguintes afirmações são equivalentes:*

(i) G *é resolúvel de classe* $\leq n$.

(ii) Existe uma torre $G = G^0 \supset G^1 \supset \cdots \supset G^n = \{e\}$ *em que, para todo o* k, G^k *é normal em* G, *e* G^k/G^{k+1} *é abeliano.*

(iii) Existe uma torre abeliana $G = G^1 \rhd G^2 \rhd \ldots \rhd G^n = \{e\}$.

(iv) Existe um subgrupo abeliano A *normal em* G *tal que* G/A *é resolúvel de classe* $\leq n-1$.

Exemplos 5.3.11.

1. *O grupo* S_3 *é resolúvel, pois temos a torre de subgrupos* $S_3 \supset A_3 \supset \{e\}$, *em que* A_3 *é normal em* S_3, $S_3/A_3 \simeq \mathbb{Z}_2$ *e* A_3 *é cíclico.*

2. *O grupo* S_4 *é resolúvel, pois temos a seguinte torre abeliana de subgrupos:*

$$S_4 \rhd A_4 \rhd G^2 \rhd G^3 \rhd \{e\},$$

onde G^2 *e* G^3 *são os subgrupos de permutações:*

$$G^2 = \{I, (12)(34), (13)(24), (14)(23)\}$$
$$G^3 = \{I, (12)(34)\}.$$

Deixamos como exercício verificar que esta torre é de facto abeliana.

Ao contrário do que estes exemplos sugerem, os grupos simétricos S_n, para $n \geq 5$, não são resolúveis. Eles pertencem a uma outra classe de grupos, em certo sentido oposta à dos grupos resolúveis, que estudaremos na secção seguinte.

Exercícios.

1. Mostre que, se $\pi : G_1 \to G_2$ é um homomorfismo, então $\pi(C^k(G_1)) = C^k(\pi(G_1))$ e também $\pi(\mathcal{D}^k(G_1)) = \mathcal{D}^k(\pi(G_1))$.

2. Mostre que o subgrupo de $GL(n, \mathbb{R})$ formado pelas matrizes triangulares superiores, com 1s na diagonal principal, é nilpotente de classe $n-1$.

3. Mostre que o subgrupo de $GL(n, \mathbb{R})$ formado pelas matrizes triangulares superiores invertíveis, é resolúvel.

4. Seja G um grupo. Mostre que:

   (a) se $H_1, H_2, H_3 \subset G$ são subgrupos normais, então

$$(H_1, (H_2, H_3)) \subset (H_3, (H_2, H_1)) \cdot (H_2, (H_1, H_3));$$

(b) para todo o $m, n \in \mathbb{N}$

$$(\mathcal{C}^m(G), \mathcal{C}^n(G)) \subset \mathcal{C}^{m+n}(G);$$

(c) para todo o $n \in \mathbb{N}$

$$\mathcal{D}^n(G) \subset \mathcal{C}^{2^n}(G).$$

5. Mostre que todo o subgrupo ou quociente de um grupo nilpotente (respectivamente, resolúvel) é um grupo nilpotente (respectivamente, resolúvel).

6. Mostre que, se G é um grupo nilpotente (respectivamente resolúvel) de classe $\leq n$, então $G/\mathcal{C}^{n-1}(G)$ (respectivamente $G/\mathcal{D}^{n-1}(G)$) é nilpotente (respectivamente resolúvel) de classe $\leq n-1$.

7. Demonstre a Proposição 5.3.10.

8. A SÉRIE CENTRAL SUPERIOR de um grupo G é a torre $\{\mathcal{C}_k(G)\}_{k\in\mathbb{N}}$ definida da seguinte forma: $\mathcal{C}_1(G) = C(G)$ e $\mathcal{C}_k(G)$ é o subgrupo normal de G tal que $\mathcal{C}_k(G)/\mathcal{C}_{k-1}(G)$ é o centro de $G/\mathcal{C}_{k-1}(G)$. Mostre que:

   (i) $\mathcal{C}_k(G) = \{g \in G : (g, h) \in \mathcal{C}_{k-1}(G), \forall h \in G\}$;

   (ii) Um grupo é nilpotente se e só se $G = \mathcal{C}_n(G)$, para algum natural n.

9. Mostre que um p-grupo é nilpotente.

10. Mostre que um grupo finito é nilpotente se e só se é um produto directo de p-subgrupos.
(SUGESTÃO: Se G é um grupo nilpotente, mostre que:

   (a) se $H \subsetneq G$ é um subgrupo, então $H \subsetneq N_G(H)$;

   (b) todo o subgrupo de Sylow $P \subset G$ é normal;

   (c) G é o produto directo dos seus subgrupos de Sylow.)

11. Verifique que a torre de subgrupos de S_4 fornecida no Exemplo 5.3.11 é abeliana.

5.4 Grupos Simples

As classes dos grupos nilpotentes e resolúveis, estudadas na secção anterior, e a classe dos grupos simples, que estudaremos nesta secção, formam sem dúvida as classes mais importantes de grupos (isto é verdade não só para os grupos finitos, mas também para os grupos contínuos de Lie, que estão para além do âmbito destas notas).

Definição 5.4.1. Um grupo G diz-se SIMPLES se os únicos subgrupos normais de G são os subgrupos triviais $\{e\}$ e G.

Por outras palavras, os grupos simples são os grupos para os quais existe apenas uma única relação de congruência. Note-se que para um grupo simples não-abeliano $G = \mathcal{D}(G)$.

Exemplos 5.4.2.

1. *Um subgrupo de um grupo abeliano é sempre um subgrupo normal. Logo um grupo abeliano G é simples se e só se contém apenas os subgrupos triviais $\{e\}$ e G. Estes grupos são precisamente os grupos cíclicos cuja ordem é um número primo p,* i.e., $\mathbb{Z}_p$.

2. *Um grupo resolúvel de classe n admite uma torre $G = G^0 \supset G^1 \supset G^2 \supset \cdots \supset G^n = \{e\}$, em que cada G^i é normal em G e G^i/G^{i+1} é abeliano (Proposição 5.3.10). Logo os únicos grupos resolúveis simples são os grupos $\mathbb{Z}_p$ com p primo.*

Os exemplos mais elementares de grupos finitos simples são os grupos alternados A_n, com $n \geq 5$. Galois descobriu que este facto está por detrás da impossibilidade de resolução de equações algébricas por radicais quando o grau da equação é maior ou igual a cinco, um assunto que estudaremos no Capítulo 7.

Teorema 5.4.3. *Os grupos alternados A_n são simples para $n \geq 5$.*

Demonstração. Mostramos que, se $N \subset A_n$ é um subgrupo normal $\neq \{I\}$, então $N = A_n$. A demonstração é dividida em três passos:

(i) O grupo A_n é gerado por 3-ciclos: Se $\pi \in A_n$ a representação de π como um produto de transposições contém um número par de termos. Mas um produto de duas transposições pode ser sempre escrito como um produto de 3-ciclos (por exemplo, $(12)(23) = (123)$, $(12)(34) = (123)(234)$).

(ii) Se N contém um 3-ciclo, então $N = A_n$: Suponha-se, por exemplo, que $(123) \in N$. Então a conjugação pelo elemento

$$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & l & m & \cdots \end{pmatrix}$$

fornece $\delta(123)\delta^{-1} = (ijk)$. Isto mostra que (ii) é verdadeira desde que $\delta \in A_n$, o que pode ser sempre conseguido com a substituição $\delta \to (lm)\delta$.

(iii) N contém um 3-ciclo: Começamos por escolher em N um elemento $\alpha \neq I$ com a seguinte propriedade:

> (m) O número de inteiros i tais que $\alpha(i) = i$ é máximo entre todos os elementos de N.

Mostramos que α é um 3-ciclo por redução ao absurdo. Suponha-se que α não é um 3-ciclo. Então a expressão de α como um produto de ciclos disjuntos toma uma das seguintes formas:

$$\alpha = (123\ldots)\ldots(\ldots), \quad \text{ou} \quad \alpha = (12)(34\ldots)\ldots$$

onde, no primeiro caso, α permuta pelo menos mais dois elementos (por exemplo, 4 e 5). De facto, não se pode dar o caso $\alpha = (123l)$, pois esta permutação é ímpar. Deixamos como exercício verificar que, se $\beta = (345)$, então $\gamma = (\alpha, \beta)$ é um elemento de N com as seguintes propriedades:

(a) se $i > 5$ e $\alpha(i) = i$, então também $\gamma(i) = i$;

(b) $\gamma(1) = 1$;

(c) no segundo caso, $\gamma(2) = 2$;

Mas então γ é um elemento que contradiz a propriedade (m) de α. Logo, necessariamente, α é um 3-ciclo. □

Corolário 5.4.4. *S_n não é resolúvel para $n \geq 5$.*

Demonstração. Suponhamos que S_n é resolúvel. Então, pelo teorema e pelo Exercício 5 da Secção 5.3, A_n é um grupo resolúvel simples, donde se segue que A_n é um grupo abeliano, uma contradição. □

Os grupos simples são de certa forma indecomponíveis. Podemos decompor um grupo finito em componentes simples. De facto, se G é um grupo finito, então possui uma torre normal $G = A^0 \rhd A^1 \rhd \ldots \rhd A^m = \{e\}$ em que, para todo o k, A^k/A^{k+1} é um grupo simples: escolhe-se para A^1 um subgrupo normal de $A^0 = G$ que não está contido em nenhum subgrupo normal de A^0, para A^2 um subgrupo normal de A^1 que não está contido em nenhum subgrupo normal de A^1, e assim sucessivamente. A uma torre deste tipo chama-se SÉRIE DE COMPOSIÇÃO de G. O Teorema de Jordan-Hölder mostra que estas séries de composição são essencialmente únicas.

Para ver o que queremos dizer por "essencialmente únicas", seja G um grupo que admite duas torres normais

$$\begin{aligned} G &= A^0 \rhd A^1 \rhd \ldots \rhd A^s, \\ G &= B^0 \rhd B^1 \rhd \ldots \rhd B^r. \end{aligned}$$

Diz-se que a torre $\{A^i\}_{i=0}^s$ é *mais fina* que a torre $\{B^j\}_{j=0}^r$ se $r < s$ e se para cada i existe um j_i tal que $B^{j_i - 1} \supset A^i \supset B^{j_i}$. Duas torres $\{C^i\}_{i=0}^s$ e $\{D^j\}_{j=0}^r$ dizem-se *equivalentes* se $r = s$ e existe uma permutação dos índices $i \mapsto i'$ tal que

$$C^i/C^{i+1} \simeq D^{i'}/D^{i'+1}.$$

Teorema 5.4.5 (Schreier). *Seja G um grupo. Duas torres normais de subgrupos de G que terminam no subgrupo trivial $\{e\}$ possuem refinamentos equivalentes.*

Demonstração. Sejam $\{A^i\}_{i=0}^s$ e $\{B^j\}_{j=0}^r$ as duas torres em questão e defina-se

$$\bar{A}^{ij} \equiv A^{i+1}(B^j \cap A^i).$$

Como $\bar{A}^{ir} = A^{i+1}$, $\bar{A}^{i0} = A^i$ e $\bar{A}^{ij+1}$ é um subgrupo normal de $\bar{A}^{ij}$, vemos que $\{\bar{A}^{ij}\}$ é um refinamento de $\{A^i\}$. De igual forma, definindo

$$\bar{B}^{ji} \equiv B^{j+1}(A^i \cap B^j),$$

obtém-se um refinamento de $\{B^j\}$. Para completar a demonstração necessitamos do seguinte lema cuja verificação se deixa como exercício.

Lema 5.4.6 (Zassenhaus). *Se $G \supset S \rhd S'$ e $G \supset T \rhd T'$, então*

$$\frac{S'(S \cap T)}{S'(S \cap T')} \simeq \frac{T'(S \cap T)}{T'(S' \cap T)}.$$

Se no Lema de Zassenhaus tomarmos $S = A^i$, $S' = A^{i+1}$, $T = B^j$ e $T' = B^{j+1}$, obtemos

$$\frac{\bar{A}^{ij}}{\bar{A}^{ij+1}} = \frac{A^{i+1}(A^i \cap B^j)}{A^{i+1}(A^i \cap B^{j+1})} \simeq \frac{B^{j+1}(A^i \cap B^j)}{B^{j+1}(A^{i+1} \cap B^j)} = \frac{\bar{B}^{ji}}{\bar{B}^{ji+1}},$$

logo, $\{\bar{A}^{ij}\}$ e $\{\bar{B}^{ji}\}$ são refinamentos equivalentes. □

Teorema 5.4.7 (Jordan-Hölder). *Duas séries de composição de um grupo finito G são equivalentes.*

Demonstração. Uma série de composição é precisamente uma torre normal de subgrupos que não admite um refinamento. Logo, pelo Teorema de Schreier, duas torres deste tipo são necessariamente equivalentes. □

O Teorema de Jordan-Hölder mostra que uma série de composição é um invariante de um grupo finito (*i.e.*, dois grupos isomorfos possuem séries de composição equivalentes) e, portanto, podem ser utilizadas para decidir se dois grupos são ou não isomorfos. Por exemplo, dois grupos que possuam séries de composição de comprimentos diferentes não são isomorfos.

Exemplos 5.4.8.

1. *Um grupo cíclico $G = \langle a \rangle$ de ordem p^m possui uma série de composição de comprimento m, $G = G^0 \rhd G^1 \rhd \ldots \rhd G^m = \{e\}$, em que cada G^k é o grupo cíclico $\langle a^{p^k} \rangle$, $k = 0, \ldots, m$.*

2. *O grupo $\mathbb{H}_8 = \{\mathbf{1}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}, -\mathbf{1}, -\boldsymbol{i}, -\boldsymbol{j}, -\boldsymbol{k}\}$ tem as seguintes séries de composição:*

$$\mathbb{H}_8 \rhd \{-\mathbf{1}, \boldsymbol{i}, -\mathbf{1}, -\boldsymbol{i}\} \rhd \{\mathbf{1}, -\mathbf{1}\} \rhd \{\mathbf{1}\},$$
$$\mathbb{H}_8 \rhd \{\mathbf{1}, \boldsymbol{j}, -\mathbf{1}, -\boldsymbol{j}\} \rhd \{\mathbf{1}, -\mathbf{1}\} \rhd \{\mathbf{1}\},$$
$$\mathbb{H}_8 \rhd \{\mathbf{1}, \boldsymbol{k}, -\mathbf{1}, -\boldsymbol{k}\} \rhd \{\mathbf{1}, -\mathbf{1}\} \rhd \{\mathbf{1}\}.$$

Estas séries são equivalentes, pois todos os grupos quocientes G^i/G^{i+1} são isomorfos a $\mathbb{Z}_2$.

Por definição, um grupo é simples se possui uma única série de composição trivial $G \rhd \{e\}$. Por sua vez, os grupos resolúveis são caracterizados em termos de séries de composição da seguinte forma.

Teorema 5.4.9. *Um grupo finito G é resolúvel se, e só se, os factores G^k/G^{k+1} de uma série de composição $G = G^0 \rhd G^1 \rhd \ldots \rhd G^m = \{e\}$ são grupos cíclicos de ordem prima.*

Demonstração. Se G é resolúvel, então em qualquer série de composição de G,

$$G = G^0 \rhd G^1 \rhd \ldots \rhd G^m = \{e\},$$

os factores G^k/G^{k+1} são grupos resolúveis simples, logo são cíclicos de ordem prima. Inversamente, se G admite uma série de composição em que os factores são cíclicos, então pela Proposição 5.3.10 é um grupo resolúvel. □

Exercícios.

1. Demonstre o Lema de Zassenhaus.
   (SUGESTÃO: utilize o 2º Teorema do Isomorfismo para mostrar que cada um dos quocientes neste lema é isomorfo a $S \cap T/(S \cap T')(S' \cap T)$.)

2. Mostre que um p-grupo cíclico possui uma única série de composição.

3. Mostre que um grupo abeliano possui uma série de composição se e só se é finito.

4. Determine as séries de composição dos seguintes grupos:

   (a) $\mathbb{Z}_6 \times \mathbb{Z}_5$;

   (b) S_4;

   (c) G com $|G| = pq$ (p e q primos).

5. Se um grupo simples G possui um subgrupo de índice $n > 1$, mostre que a ordem de G divide $n!$.

6. Mostre que todo o grupo de ordem pq^2 (p e q primos) é resolúvel.

7. Classifique todos os grupos de ordem 20.

8. Mostre que não existe um grupo simples não-abeliano com ordem inferior a 30.

9. Mostre que o grupo simples A_5 não contém um subgrupo de ordem 15.

5.5 Grupos de Simetrias

Vimos no Capítulo 1 a noção de grupo de simetria de uma figura $\Omega \subset \mathbb{R}^n$. Depois do estudo neste capítulo da estrutura dos grupos finitos, vejamos o que podemos dizer sobre grupos de simetrias.

Recordemos que o grupo das simetrias de $\mathbb{R}^n$ é, por definição, o grupo euclidiano $E(n)$ formado pelas isometrias de $\mathbb{R}^n$. Pelo Exercício 5.1.5, este grupo é isomorfo ao produto semidirecto $O(n) \ltimes \mathbb{R}^n$. De facto, como sabemos do Capítulo 1, uma isometria $\boldsymbol{f} \in E(n)$ pode ser sempre escrita na forma

$$\boldsymbol{f}(\boldsymbol{x}) = A\boldsymbol{x} + \boldsymbol{b},$$

onde $A \in O(n)$ determina uma transformação ortogonal e $\boldsymbol{b} \in \mathbb{R}^n$ determina uma translação.

Se $\Omega \subset \mathbb{R}^n$, o grupo das simetrias de Ω é o subgrupo $G \subset E(n)$ das isometrias que deixam Ω invariante:

$$G = \{\boldsymbol{f} \in E(n) : \boldsymbol{f}(\Omega) = \Omega\}.$$

No caso em que Ω é uma figura limitada, é claro que o grupo de simetrias de Ω contém apenas transformações ortogonais. Temos ainda a

Proposição 5.5.1. *Se G é um grupo de simetrias de uma figura limitada $\Omega \subset \mathbb{R}^n$, então verifica-se uma e uma só das seguintes afirmações:*

(i) G contém apenas rotações;

(ii) as rotações de G formam um subgrupo de índice 2 (logo, normal).

Demonstração. Como Ω é limitado, $G \subset O(n)$ e G é formado por rotações sse $G \subset SO(n)$. Se $G \not\subset SO(n)$, então $H = G \cap SO(n)$ é o subgrupo das rotações de G, e coincide com o núcleo do epimorfismo $\det : G \to \{1, -1\}$. Pelo 1º Teorema do Isomorfismo

$$[G : H] = |G/H| = |\{1, -1\}| = 2.$$

□

No resto desta secção consideramos apenas grupos de simetrias finitos. Veremos que os resultados obtidos anteriormente sobre grupos finitos permitem classificar completamente os grupos de simetrias de figuras planas ($n = 2$) e tridimensionais ($n = 3$) limitadas.

5.5.1 Grupos de simetrias de figuras planas

Antes de fornecermos a classificação dos grupos de simetrias de figuras planas limitadas, recordemos alguns exemplos de figuras planas com grupos de simetria que já encontrámos anteriormente.

Exemplos 5.5.2.

1. *Recordemos que o grupo diedral D_n é o grupo de simetria de um polígono regular de n lados. Vimos no Exemplo 1.8.7.2 que o grupo D_3 formado pelas simetrias de um triângulo equilátero é constituído por 6 elementos: 3 rotações $(I, \frac{2\pi}{3}, \frac{4\pi}{3})$ e três reflexões em torno dos eixos de simetria.*
   Mais geralmente, o grupo D_n das simetrias de um polígono regular de n lados possui $2n$ elementos: n rotações e n reflexões em torno dos eixos de simetria. Designando por ρ uma rotação de $\frac{2\pi}{n}$ e por σ uma reflexão em relação a um eixo de simetria do polígono, podemos listar os elementos de D_n na forma:

$$D_n = \langle \rho, \sigma \rangle = \{I, \rho, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \ldots, \sigma\rho^{n-1}\}.$$

   Como vimos no Exemplo 4.6.3.4, este grupo possui, pois, uma apresentação com geradores ρ e σ e relações

$$\sigma^2 = I, \quad \rho^n = I, \quad \rho\sigma = \sigma\rho^{-1}.$$

2. *Consideremos o grupo das simetrias das velas de um moinho. Este grupo é cíclico de ordem 4, pois é gerado por uma rotação ρ de $\frac{\pi}{2}$:*

$$C_4 = \{I, \rho, \rho^2, \rho^3\}.$$

   Uma figura com grupo de simetrias cíclico $C_n = \{I, \rho, \ldots, \rho^{n-1}\}$[4] é a seguinte:

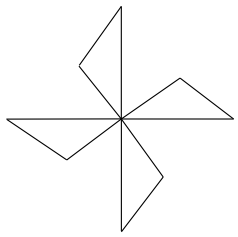


Figura 5.5.1: Figura plana com grupo de simetrias cíclico.

As simetrias destes exemplos são todas as que se podem obter, como mostra o seguinte resultado:

Teorema 5.5.3. *Um grupo finito de simetrias de uma figura plana $\Omega \subset \mathbb{R}^2$ é isomorfo a C_n ou a D_n.*

Demonstração. Suponha-se que G é um grupo finito de simetrias de uma figura plana. Pela Proposição 5.5.1, há dois casos a considerar:

(a) G contém apenas rotações: Seja $\rho \in G$ uma rotação por um ângulo θ_ρ que é mínimo entre todas as rotações de G (existe, pois G é finito). Então

[4]No estudo de simetrias é usual designar-se por C_n o grupo cíclico de ordem n, em vez da notação $\mathbb{Z}_n$ utilizada anteriormente.

$\{I, \rho, \rho^2, \dots\} \subset G$. Por outro lado, se $\tilde{\rho} \in G$ é uma rotação por um ângulo $\theta_{\tilde{\rho}}$ que não figura entre estas potências, então para algum inteiro k:

$$k\theta_\rho < \theta_{\tilde{\rho}} < (k+1)\theta_\rho.$$

Mas então $\tilde{\rho}\rho^{-k}$ é uma rotação por um ângulo inferior ao de ρ, o que é uma contradição. Logo, $G = \{I, \rho, \dots, \rho^{n-1}\} = C_n$.

(b) G contém uma reflexão σ: Por (a) o subgrupo $H \subset G$ das rotações próprias é da forma $H = \{I, \rho, \dots, \rho^{n-1}\}$. Como $[G : H] = 2$, temos $G = \{I, \rho, \dots, \rho^{n-1}, \sigma, \sigma\rho \dots, \sigma\rho^{n-1}\}$. Deixamos como exercício verificar que neste caso $G \simeq D_n$. □

No caso do grupo diedral D_n, temos uma série de composição da forma

$$D_n \rhd C_n \rhd H^2 \rhd H^3 \rhd \cdots \rhd H^s = \{I\}.$$

Se $n = p$ é primo, então C_p é simples, e obtemos a série de composição $D_p \rhd C_p \rhd \{I\}$. Neste caso, como $|D_p| = 2p$, os Teoremas de Sylow mostram que os seus subgrupos são

(a) p subgrupos de ordem 2: $\{I, \sigma\}, \{I, \sigma\rho\}, \dots, \{I, \sigma\rho^{p-1}\}$;

(b) 1 subgrupo de ordem p: $\{I, \rho, \dots, \rho^{p-1}\}$;

O subgrupo de ordem p é normal. Como p é primo, os subgrupos de ordem 2 são conjugados por uma rotação (exercício). Geometricamente, isto significa que podemos obter qualquer reflexão a partir de uma reflexão fixa conjugando por rotações:

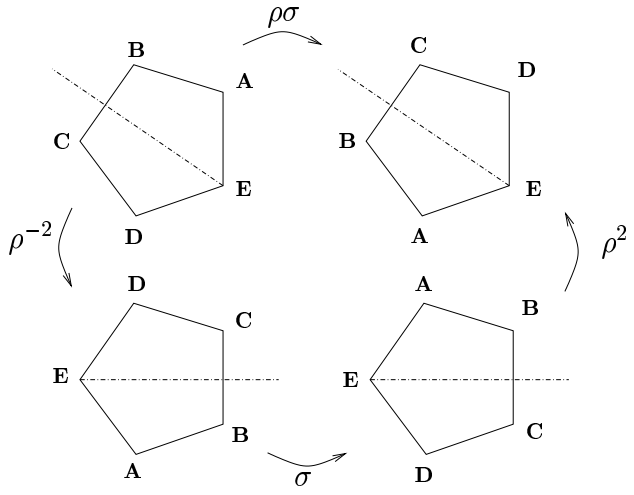


Figura 5.5.2: Simetrias de um pentágono.

Por exemplo, a figura ilustra no caso $p = 5$ que a reflexão $\rho\sigma$ pode ser obtida a partir da reflexão σ, conjugando pela rotação ρ^2. A estrutura dos subgrupos do grupo diedral D_n quando n não é primo é mais complexa e não será aqui discutida.

5.5.2 Grupos de simetrias de figuras tridimensionais

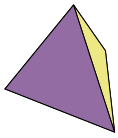
Vejamos agora o caso dos grupos finitos de simetrias de uma figura tridimensional. Começamos pelas simetrias rotacionais, *i.e.*, o caso em que $G \subset SO(n)$.

Teorema 5.5.4. *Um grupo finito de simetrias rotacionais de uma figura $\Omega \subset \mathbb{R}^3$ é isomorfo a um dos seguintes grupos de simetrias rotacionais:*

(i) o grupo de simetrias C_n de um moinho com n velas;

(ii) o grupo de simetrias D_n de um polígono regular com n lados;

(iii) o grupo de simetrias rotacionais T de um tetraedro regular;



(iv) o grupo de simetrias rotacionais O de um cubo ou de um octaedro regular:

(v) o grupo de simetrias rotacionais I de um dodecaedro ou de um icosaedro regular.

Demonstração. Dado um subgrupo finito $G \subset SO(3)$, a ideia da demonstração consiste em introduzir uma acção de G num conjunto finito P e depois explorar a equação de classes (5.1.3).

O conjunto P onde G actua é o conjunto dos pólos de G: dizemos que $p \in S^2 = \{\boldsymbol{x} : |\boldsymbol{x}| = 1\}$ é um pólo se existe uma rotação $g \in G$, não-trivial, tal que $g \cdot p = p$. Vemos que p é um pólo fixo por g se e só se $p \in S^2 \cap L$, onde L é o eixo de rotação de g. Em particular, cada $g \in G$ tem associado dois pólos, logo, P é não-vazio (G é não-trivial).

O grupo G actua no conjunto dos seus pólos P: se $p \in P$ é tal que $g \cdot p = p$, então para todo o $h \in G$, temos

$$(hgh^{-1})h \cdot p = h \cdot p.$$

Como $hgh^{-1} \neq e$ se $g \neq e$, vemos que $h \cdot p \in P$. Vamos agora estudar a acção de G em P, o que nos permite mostrar o seguinte lema:

Lema 5.5.5. *Para a acção de G no conjunto dos pólos P é válida a fórmula*

$$\sum_i (1 - \frac{1}{r_{p_i}}) = 2 - \frac{2}{N}, \tag{5.5.1}$$

onde a soma é sobre as órbitas $\mathcal{O}_i$ da acção, p_i é um pólo que representa a órbita $\mathcal{O}_i$, r_{p_i} é a ordem do subgrupo de isotropia G_{p_i}, e N é a ordem de G.

Demonstração do Lema. Para cada pólo $p \in P$, os elementos $g \in G$ que fixam p formam precisamente o subgrupo de isotropia G_p. Seja $N = |G|$ e $r_p = |G_p|$. Para cada $g \in G - \{e\}$ existem 2 pólos associados a g. Logo:

$$2(N-1) = \sum_{\substack{g \in G \\ g \neq e}} 2 = \sum_{p \in P} (r_p - 1). \tag{5.5.2}$$

Agrupemos agora os elementos de P em órbitas de G. Se $\mathcal{O}_i$ é uma órbita, escolhemos um representante $p_i \in \mathcal{O}_i$ e escrevemos $n_i = |\mathcal{O}_i|$. Então a equação (5.5.2) fornece

$$\sum_i n_i r_{p_i} - |P| = 2(N-1),$$

onde a soma é sobre o número de órbitas de G. Como $\mathcal{O}_i \simeq G/G_{p_i}$, vemos que $n_i r_{p_i} = N$, logo:

$$\sum_i N - |P| = 2(N-1). \tag{5.5.3}$$

Por outro lado, a equação de classes (5.1.3) mostra que

$$|P| = \sum_i |\mathcal{O}_i| = \sum_i \frac{N}{r_{p_i}}. \tag{5.5.4}$$

Substituindo (5.5.4) em (5.5.3), obtemos (5.5.1). □

A equação (5.5.1) permite obter restrições sobre G que levam à sua classificação. Uma primeira observação é que existem no máximo três órbitas. De facto, o lado direito de (5.5.1) é < 2, enquanto que cada termo do lado esquerdo é $\geq \frac{1}{2}$. As várias possibilidades são então:

(i) *1 órbita:* Teríamos
$$1 - \frac{1}{r_1} = 2 - \frac{2}{N}.$$
Esta equação não tem soluções.

(ii) *2 órbitas:* Obtemos
$$\frac{1}{r_1} + \frac{1}{r_2} = \frac{2}{N}.$$
A única solução é $r_1 = r_2 = N$. Existem então 2 pólos p_1 e p_2 fixos por todos os elementos de G, logo, $G = C_n$, o grupo das rotações em torno do eixo que passa por p_1 e p_2.

(iii) *3 órbitas:* Neste caso temos
$$\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 1 = \frac{2}{N}.$$
Podemos supor que $r_1 \leq r_2 \leq r_3$. Vemos então que necessariamente $r_1 = 2$. Obtemos os seguintes subgrupos:

(a) $r_1 = r_2 = 2,\ N = 2r_3.\ |\mathcal{O}_1| = |\mathcal{O}_2| = \frac{N}{2},\ |\mathcal{O}_3| = 2;$

(b) $r_1 = 2,\ r_2 = r_3 = 3,\ N = 12.\ |\mathcal{O}_1| = 6,\ |\mathcal{O}_2| = |\mathcal{O}_3| = 4;$

(c) $r_1 = 2,\ r_2 = 3,\ r_3 = 4,\ N = 24.\ |\mathcal{O}_1| = 12,\ |\mathcal{O}_2| = 8,\ |\mathcal{O}_3| = 6;$

(d) $r_1 = 2,\ r_2 = 3,\ r_3 = 5,\ N = 60.\ |\mathcal{O}_1| = 30,\ |\mathcal{O}_2| = 20,\ |\mathcal{O}_3| = 12.$

Deixamos como exercício verificar que os casos (a), (b), (c) e (d) correspondem, respectivamente, aos grupos $G \simeq D_{\frac{N}{2}}$, $G \simeq T$, $G \simeq O$ e $G \simeq I$.

No caso (a), os pólos são as intersecções dos eixos de simetria do polígono regular com a esfera unitária e do eixo perpendicular ao plano do polígono com a esfera unitária. No caso dos poliedros regulares. os pólos são as intersecções dos eixos de simetria dos poliedros com a esfera unitária. □

Pela Proposição 5.5.1, os grupos de simetrias não rotacionais tomam uma das seguintes formas:

(a) Se $-I \in G$, então $G = H \cup -H$, onde $H = \{I, \rho_1, \ldots, \rho_{n-1}\}$ é o subgrupo das rotações de G e $-H \equiv \{-I, -\rho_1, \ldots, -\rho_{n-1}\}$.

(b) Se $-I \notin G$, então $G = H \cup \tilde{H}$, onde H é o subgrupo das rotações próprias de G e, se $-\rho \in \tilde{H}$, então ρ possui ordem par e $\rho^2 \in H$.

Como H toma uma das formas dada no teorema acima, obtemos todos os grupos finitos de simetrias possíveis para uma figura tridimensional $\Omega \subset \mathbb{R}^3$.

Podemos descrever, de forma mais explícita, os grupos de simetrias dos poliedros regulares. A título de exemplo consideramos o caso dum dodecaedro, sendo os restantes casos tratados como exercícios no final da secção.

Exemplo 5.5.6.

O grupo de simetrias I dum dodecaedro (ou de um icosaedro) tem ordem $60 = 2^2 \times 3 \times 5$. Pelos Teoremas de Sylow obtemos os seguintes subgrupos:

(i) Subgrupos de ordem 5: o número de subgrupos de ordem 5 divide 12 e é igual a $1 \pmod 5$. Logo, as possibilidades são 1 ou 6 subgrupos. Existem 6 subgrupos correspondentes a rotações por $\frac{2\pi}{5}$ em torno dos eixos que passam nos centros das faces do dodecaedro. Estes subgrupos são precisamente os subgrupos de isotropia da órbita $\mathcal{O}_3$.

(ii) Subgrupos de ordem 3: o número de subgrupos de ordem 3 divide 20 e é igual a $1 \pmod 3$. Podemos ter 1, 4 ou 10 subgrupos. Existem 10 subgrupos correspondentes a rotações por $\frac{2\pi}{3}$ em torno dos eixos que passam nos vértices do dodecaedro. Estes subgrupos são precisamente os subgrupos de isotropia da órbita $\mathcal{O}_2$.

(iii) Subgrupos de ordem 4: o número de subgrupos de ordem 4 divide 15 e é igual a $1 \pmod 2$. Podemos ter 1, 3, 5 ou 15 subgrupos. Existem 15 subgrupos de ordem 2 correspondentes a rotações por π em torno dos eixos que passam nos centros das arestas do dodecaedro (os subgrupos de ordem 2 são precisamente os subgrupos de isotropia da órbita $\mathcal{O}_1$). Estes subgrupos dão origem a 5 subgrupos de ordem 4, formados pelas rotações correspondentes a 3 arestas ortogonais (na figura abaixo, as arestas paralelas às arestas do cubo).

As rotações de ordem 2, 3 e 5, que acabámos de enumerar esgotam os elementos de I, pois temos:

$$60 = |I| = 1 + \underbrace{15}_{\text{ordem } 2} + \underbrace{20}_{\text{ordem } 3} + \underbrace{24}_{\text{ordem } 5} . \tag{5.5.5}$$

Esta enumeração dos elementos de I permite mostrar que I é um grupo simples. De facto, se $H \subset G$ é um subgrupo normal e H contém um elemento de ordem r, então H contém todos os elementos de ordem r, pois os subgrupos de Sylow são todos conjugados e os subgrupos de ordem 2 não são normais. Logo, a ordem de H seria uma soma de alguns dos termos da equação (5.5.5). Não existe nenhum inteiro que seja uma soma de termos de (5.5.5) e que divida 60. Portanto, I é um grupo simples.

O estudo que fizemos dos grupos de permutações A_n sugere que $I \simeq A_5$ e, de facto, assim é. Para isso consideramos os 5 cubos inscritos no dodecaedro. A acção de I nos vértices do dodecaedro transforma vértices de cubos em vértices de cubos, logo, induz uma acção de I num conjunto de 5 elementos:

$$T(R)(cubo) = R(cubo)$$

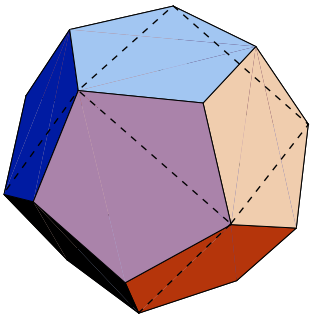


Figura 5.5.3: Um dos cinco cubos inscritos num dodecaedro.

Como I é simples, esta acção é efectiva: $N(T) = \{e\}$. Como I contém apenas rotações que preservam orientações, $Im(T) \subset A_5$. Finalmente, sendo $|I| = 60 = |A_5|$, concluímos que $I \simeq Im(T) = A_5$.

A classificação de grupos finitos de simetrias de figuras $\Omega \subset \mathbb{R}^n$, para $n > 3$, só é conhecida para valores pequenos de n. Um caso especial muito importante é o caso dos grupos gerados por reflexões em hiperplanos de $\mathbb{R}^n$, os chamados *grupos de Coxeter*. A sua classificação, obtida por Coxeter em 1934[5], está intimamente ligada com a classificação das chamadas álgebras de Lie e encontra aplicações em muitos domínios da Matemática e da Física.

Exercícios.

1. Complete a demonstração do Teorema 5.5.3.

2. Seja D_p o grupo de simetrias de um polígono regular com p lados. Mostre que, para p primo, os subgrupos de ordem 2 são conjugados por uma rotação.

3. Complete a demonstração do Teorema 5.5.4.

4. Mostre que a acção do grupo I nos 5 cubos inscritos num dodecaedro é efectiva (ver Exemplo 5.5.6).

5. Mostre que $T \simeq A_4$.
(SUGESTÃO: Considere a acção induzida nos vértices do tetraedro.)

6. Mostre que $O \simeq S_4$.
(SUGESTÃO: Considere a acção induzida nas diagonais do cubo.)

[5] H. S. M. Coxeter, *Discrete Groups Generated by Reflections*, Ann. Math. **35**, (1934) 588-621.

Capítulo 6

Módulos

6.1 Módulos sobre Anéis

Seja $(G, +)$ um grupo abeliano que vamos escrever na notação aditiva. Recordemos que temos uma operação de $\mathbb{Z}$ em G: se $n \in \mathbb{Z}$ e $g \in G$, então temos um elemento $ng \in G$. Esta operação satisfaz as seguintes propriedades:

- $n(g_1 + g_2) = ng_1 + ng_2$, $n \in \mathbb{Z}, g_1, g_2 \in G$;
- $(n + m)g = ng + mg$, $n, m \in \mathbb{Z}, g \in G$;
- $n(mg) = (nm)g$, $n, m \in \mathbb{Z}, g \in G$;
- $1g = g$, $g \in G$.

Estas propriedades são formalmente semelhantes aos axiomas que definem um espaço vectorial V sobre K, em que substituímos os elementos de V (os "vectores") por elementos do grupo G, e os elementos do corpo K (os "escalares") por elementos do anel $\mathbb{Z}$. Recordemos então esta definição.

Definição 6.1.1. Chama-se ESPAÇO VECTORIAL sobre um corpo K a um grupo abeliano $(V, +)$ com uma operação $K \times V \to V$, que escrevemos $(k, \boldsymbol{v}) \mapsto k\boldsymbol{v}$, satisfazendo:

- $k(\boldsymbol{v}_1 + \boldsymbol{v}_2) = k\boldsymbol{v}_1 + k\boldsymbol{v}_2$, $k \in K, \boldsymbol{v}_1, \boldsymbol{v}_2 \in V$;
- $(k + l)\boldsymbol{v} = k\boldsymbol{v} + l\boldsymbol{v}$, $k, l \in K, \boldsymbol{v} \in V$;
- $k(l\boldsymbol{v}) = (kl)\boldsymbol{v}$, $k, l \in K, \boldsymbol{v} \in V$;
- $1\boldsymbol{v} = \boldsymbol{v}$, $\boldsymbol{v} \in V$.

Consideremos ainda um terceiro exemplo. Seja $T : \mathbb{R}^3 \to \mathbb{R}^3$ a transformação linear cuja matriz em relação à base canónica $\boldsymbol{e}_1 = (1, 0, 0)$,

$\boldsymbol{e}_2 = (0,1,0)$, $\boldsymbol{e}_3 = (0,0,1)$ é:

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}.$$

Se $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{R}[x]$ é um polinómio e $\boldsymbol{v} \in \mathbb{R}^3$ é um vector, definimos o produto $p(x) \cdot \boldsymbol{v} \in \mathbb{R}^3$ por[1]

$$p(x) \cdot \boldsymbol{v} = a_0 \boldsymbol{v} + a_1 T(\boldsymbol{v}) + \cdots + a_n T^n(\boldsymbol{v}) = \sum_{k=1}^{n} a_k T^k(\boldsymbol{v}),$$

onde

$$\begin{aligned} T^0 &= I, \\ T^k &= T \circ T \circ \cdots \circ T \quad (k - \text{vezes}). \end{aligned}$$

Por exemplo, se $p(x) = 3 + \frac{1}{2}x - 2x^2$ e $\boldsymbol{v} = (1,2,1)$ então

$$p(x) \cdot \boldsymbol{v} = 3(1,2,1) + \frac{1}{2}T(1,2,1) - 2T^2(1,2,1) = (-4, -77/2, -27/2).$$

É simples verificar que esta operação satisfaz as seguintes propriedades:

- $p(x) \cdot (\boldsymbol{v}_1 + \boldsymbol{v}_2) = p(x) \cdot \boldsymbol{v}_1 + p(x) \cdot \boldsymbol{v}_2$;
- $(p(x) + q(x)) \cdot \boldsymbol{v} = p(x) \cdot \boldsymbol{v} + q(x) \cdot \boldsymbol{v}$;
- $p(x) \cdot (q(x) \cdot \boldsymbol{v}) = (p(x)q(x)) \cdot \boldsymbol{v}$;
- $1\boldsymbol{v} = \boldsymbol{v}$.

onde $p(x), q(x) \in \mathbb{R}[x]$, $\boldsymbol{v}, \boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathbb{R}^3$. Neste exemplo, os vectores são ainda elementos de $\mathbb{R}^3$, visto como um grupo abeliano, e os escalares são elementos do anel dos polinómios.

Deve ser claro que nestes três exemplos as propriedades enunciadas apenas envolvem a estrutura de anel de, respectivamente, $\mathbb{Z}$, K e $\mathbb{R}[x]$. Existem ainda outras circunstâncias em que propriedades análogas se verificam. É pois natural estender estes conceitos ao caso de um anel arbitrário. Obtém-se assim a noção de módulo sobre um anel, ou A-módulo. O estudo de módulos sobre anéis chama-se Álgebra Linear, pois este é o cenário natural para estudar conceitos como o de independência linear, dimensão, etc., como veremos mais adiante. A definição formal de A-módulo é a seguinte:

[1] Daqui em diante, para tornar a notação mais leve, deixamos cair a convenção de designar por $\boldsymbol{x}$ uma indeterminada. Normalmente, as indeterminadas serão $x_1, \ldots, x_n$ (ou x se $n = 1$; ou x, y se $n = 2$; ou x, y, z se $n = 3$) e designamos por letras negras os vectores (elementos de um espaço vectorial ou, mais geralmente, de um módulo).

Definição 6.1.2. Um MÓDULO M SOBRE UM ANEL UNITÁRIO A (ou um A-módulo unitário) é um grupo abeliano $(M,+)$ em conjunto com uma operação de um anel unitário A em M, que se escreve $(a,\boldsymbol{v})\mapsto a\boldsymbol{v}$, satisfazendo as seguintes propriedades:

(i) $a(\boldsymbol{v}_1+\boldsymbol{v}_2)=a\boldsymbol{v}_1+a\boldsymbol{v}_2$, $a\in A,\boldsymbol{v}_1,\boldsymbol{v}_2\in M$;

(ii) $(a_1+a_2)\boldsymbol{v}=a_1\boldsymbol{v}+a_2\boldsymbol{v}$, $a_1,a_2\in A,\boldsymbol{v}\in M$;

(iii) $a_1(a_2\boldsymbol{v})=(a_1a_2)\boldsymbol{v}$, $a_1,a_2\in A,\boldsymbol{v}\in M$;

(iv) $1\boldsymbol{v}=\boldsymbol{v}$, $\boldsymbol{v}\in M$.

Para sermos exactos, os módulos que acabamos de definir são conhecidos como "módulos à esquerda". Deixamos ao cuidado do leitor fornecer a correspondente definição de "módulo à direita". Todos os resultados deste capítulo são verdadeiros *mutatis mutandis* para os módulos à direita. Se o anel A é comutativo, não faz sentido distinguir entre módulos à esquerda e à direita.

Se o anel A não contém uma unidade multiplicativa 1_A, então a definição de módulo não inclui o axioma (iv). Aqui, consideramos apenas módulos sobre anéis unitários, donde em geral omitimos o adjectivo "unitário" e utilizamos apenas o termo A-módulo.

Designe-se por 0_A e 0_M as unidades de $(A,+)$ e $(M,+)$. Como $(M,+)$ é um grupo abeliano o elemento $n\boldsymbol{v}\in M$, onde $n\in\mathbb{Z}$ e $\boldsymbol{v}\in M$, tem o sentido usual. Do mesmo modo, também podemos falar no elemento $na\in A$, onde $n\in\mathbb{Z}$ e $a\in A$. As seguintes propriedades são facilmente verificadas.

Proposição 6.1.3 (Propriedades elementares dos A-módulos). *Para qualquer A-módulo M, temos:*

(i) $a0_M=0_M$, $a\in A$;

(ii) $0_A\boldsymbol{v}=0_M$, $\boldsymbol{v}\in M$;

(iii) $(-a)\boldsymbol{v}=-(a\boldsymbol{v})=a(-\boldsymbol{v})$, $a\in A,\boldsymbol{v}\in M$;

(iv) $n(a\boldsymbol{v})=a(n\boldsymbol{v})=(na)\boldsymbol{v}$, $n\in\mathbb{Z},a\in A,\boldsymbol{v}\in M$.

Um SUBMÓDULO N dum A-módulo M é um subgrupo de $(M,+)$ que é fechado para a multiplicação por elementos de A: se $a\in A$ e $\boldsymbol{v}\in N$, então $a\boldsymbol{v}\in N$. Um submódulo é obviamente um A-módulo.

Exemplos 6.1.4.

1. *Vimos acima que um grupo abeliano G é um $\mathbb{Z}$-módulo para a operação usual $ng\in G$, onde $n\in\mathbb{Z}$ e $g\in G$. Inversamente, qualquer $\mathbb{Z}$-módulo é um grupo abeliano. Neste caso, os submódulos coincidem com os subgrupos de G.*

2. *A Definição 6.1.1 de espaço vectorial V não é mais que a definição de um módulo sobre um corpo K. Mais geralmente, vamos chamar espaço vectorial a qualquer módulo sobre um anel de divisão D. Neste exemplo, os submódulos coincidem com os subespaços lineares.*

3. *O produto introduzido no exemplo acima de um polinómio por um vector de $\mathbb{R}^3$, define uma estrutura de $\mathbb{R}[x]$-módulo em $\mathbb{R}^3$. Os submódulos são os subespaços de $\mathbb{R}^3$ invariantes pela transformação T. É claro que este exemplo pode ser estendido a uma transformação linear T arbitrária.*

4. *Se A é um anel e $I \subset A$ é um ideal (à esquerda), então I é um A-módulo: se $a \in A$ e $b \in I$, então $ab \in I$. De igual forma, A/I é um A-módulo, pois se $a \in A$ e $b + I \in A/I$, temos*

$$a(b + I) = ab + I.$$

5. *Se A é um anel e $B \subset A$ é um subanel, então A é um B-módulo. Em particular, os anéis $A[x_1, \ldots, x_n]$ e $A[[x_1, \ldots, x_n]]$ são A-módulos.*

6. *Seja G um grupo abeliano, e $\mathrm{End}(G)$ o anel dos endomorfismos de G. Então G é um $\mathrm{End}(G)$-módulo com a multiplicação $\phi g \equiv \phi(g)$, $\phi \in \mathrm{End}(G)$, $g \in G$.*

7. *Sejam A e B anéis, e $\phi : A \to B$ um homomorfismo de anéis. Se M é um B-módulo, então obtemos um A-módulo $\phi^* M$ da seguinte forma: o grupo abeliano suporte de $\phi^* M$ é $(M, +)$ e a multiplicação é definida por $a\boldsymbol{v} \equiv \phi(a)\boldsymbol{v}$, $a \in A, \boldsymbol{v} \in M$. Chama-se a $\phi^* M$ o* levantamento de M por ϕ.

Observe-se que nestes exemplos o estudo da estrutura do módulo (por exemplo, a classificação dos seus submódulos) fornece informações sobre os objectos de que se partiu: os subgrupos de um grupo abeliano, os subespaços de um espaço vectorial, etc.

Definição 6.1.5. Um HOMOMORFISMO DE A-MÓDULOS $\phi : M_1 \to M_2$ é uma aplicação entre A-módulos que satisfaz:

(i) $\phi(\boldsymbol{v}_1 + \boldsymbol{v}_2) = \phi(\boldsymbol{v}_1) + \phi(\boldsymbol{v}_2)$, $\boldsymbol{v}_1, \boldsymbol{v}_2 \in M$;

(ii) $\phi(a\boldsymbol{v}) = a\phi(\boldsymbol{v})$, $a \in A, \boldsymbol{v} \in M$.

Definem-se de forma óbvia monomorfismos, epimorfismos e isomorfismos de A-módulos. Utilizaremos indiscriminadamente os termos aplicação A-linear e transformação linear para designar um homomorfismo de A-módulos.

Exemplos 6.1.6.

1. *Se $\phi : M_1 \to M_2$ é uma transformação linear, o seu núcleo $N(\phi)$ e a sua imagem $\mathrm{Im}(\phi)$ são submódulos de M_1 e M_2.*

2. *Um homomorfismo de $\mathbb{Z}$-módulos é um homomorfismo de grupos abelianos.*

3. *Se V_1 e V_2 são espaços vectoriais, os homomorfismos $\phi : V_1 \to V_2$ são as transformações lineares usuais.*

Se M é um A-módulo e $N \subset M$ é um submódulo, então a inclusão canónica $\iota : N \to M$ é uma aplicação A-linear. O quociente M/N possui uma estrutura natural de A-módulo tal que a projecção canónica $\pi : M \to M/N$ é uma aplicação A-linear: de facto, M/N é um grupo abeliano e definimos uma operação de A em M/N por:

$$a(\boldsymbol{v} + N) \equiv (a\boldsymbol{v}) + N.$$

Vemos facilmente que (i)-(iv) são satisfeitas. Ao módulo M/N chama-se MÓDULO QUOCIENTE de M por N.

Se $\{N_i\}_{i\in I}$ é uma família de submódulos de um A-módulo M, então $\bigcap_{i\in I} N_i$ é um submódulo de M. Logo, se $S \subset M$ é um conjunto não-vazio, a intersecção de todos os submódulos de M que contêm S é um submódulo $\langle S\rangle$, a que se chama *módulo gerado por* S. Os elementos de $\langle S\rangle$ são da forma $a_1\boldsymbol{v}_1 + \cdots + a_r\boldsymbol{v}_r$, onde $a_i \in A$ e $\boldsymbol{v}_i \in S$[2].

Se $\{N_i\}_{i\in I}$ é uma família de submódulos de um A-módulo M, designa-se por $\sum_{i\in I} N_i$ o módulo gerado por $S = \bigcup_{i\in I} N_i$. Se $I = \{1, \ldots, m\}$ é finito, escrevemos $\sum_{i=1}^m N_i$ ou ainda $N_1 + \cdots + N_m$. Em geral, os elementos de $\sum_{i\in I} N_i$ tomam a forma $\boldsymbol{v}_{i_1} + \cdots + \boldsymbol{v}_{i_m}$, $\boldsymbol{v}_{i_j} \in N_{i_j}$.

Os Teoremas do Isomorfismo para grupos e anéis possuem análogos para A-módulos. As demonstrações são facilmente adaptáveis e por isso omitimo-las.

Teorema 6.1.7 (Teoremas do Isomorfismo).

(i) Se $\phi : M_1 \to M_2$ é um homomorfismo de A-módulos, então existe um isomorfismo de A-módulos:

$$\mathrm{Im}(\phi) \simeq M_1/N(\phi).$$

(ii) Se N_1 e N_2 são submódulos dum A-módulo M, então existe um isomorfismo de A-módulos:

$$\frac{N_1 + N_2}{N_2} \simeq \frac{N_1}{N_1 \cap N_2}.$$

(iii) Se N e P são submódulos dum A-módulo M e $M \supset N \supset P$, então P é um submódulo de N e existe um isomorfismo de A-módulos:

$$M/N \simeq \frac{M/P}{N/P}.$$

[2]Esta afirmação não é verdadeira para módulos não-unitários. Para estes, os elementos de $\langle S\rangle$ são da forma $\sum_i a_i\boldsymbol{v}_i + \sum_j n_j\tilde{\boldsymbol{v}}_j$, onde $a_i \in A, n_j \in \mathbb{Z}$ e $\boldsymbol{v}_i, \tilde{\boldsymbol{v}}_j \in S$.

Seja $\{M_i\}_{i\in I}$ uma família de A-módulos. Definimos o A-módulo $\prod_{i\in I} M_i$, chamado PRODUTO DIRECTO da família de módulos $\{M_i\}_{i\in I}$, da seguinte forma. O conjunto suporte de $\prod_{i\in I} M_i$ é o produto cartesiano dos M_i. Se $(\boldsymbol{v}_i)_{i\in I}, (\boldsymbol{w}_i)_{i\in I} \in \prod_{i\in I} M_i$, então $(\boldsymbol{v}_i)_{i\in I} + (\boldsymbol{w}_i)_{i\in I}$ designa o elemento $(\boldsymbol{v}_i + \boldsymbol{w}_i)_{i\in I} \in \prod_{i\in I} M_i$, e se $a \in A$, então $a(\boldsymbol{v}_i)_{i\in I}$ designa o elemento $(a\boldsymbol{v}_i)_{i\in I} \in \prod_{i\in I} M_i$. Com estas operações verifica-se facilmente que $\prod_{i\in I} M_i$ é um A-módulo. Se $k \in I$, a *projecção canónica* $\pi_k : \prod_{i\in I} M_i \to M_k$ é o homomorfismo de A-módulos que a $(\boldsymbol{v}_i)_{i\in I} \in \prod_{i\in I} M_i$ associa o elemento $\boldsymbol{v}_k \in M_k$.

A SOMA DIRECTA de uma família de A-módulos $\{M_i\}_{i\in I}$, que designamos por $\bigoplus_{i\in I} M_i$, é o submódulo de $\prod_{i\in I} M_i$ formado pelos elementos $(\boldsymbol{v}_i)_{i\in I}$ em que apenas um número finito de $\boldsymbol{v}_i$'s é não-nulo. Se $k \in I$, a *injecção canónica* $\iota_k : M_k \to \bigoplus_{i\in I} M_i$ é o homomorfismo de A-módulos que a $\boldsymbol{v}_k \in M_k$ associa o elemento $(\boldsymbol{v}_i)_{i\in I} \in \prod_{i\in I} M_i$ em que $\boldsymbol{v}_i = 0$ para $i \neq k$.

Se $I = \{1, \ldots, m\}$ é um conjunto de índices finito, então a soma directa e o produto directo coincidem. Neste caso escrevemos $\bigoplus_{i=1}^{m} M_i$ ou ainda $M_1 \oplus \cdots \oplus M_m$.

Proposição 6.1.8. *Sejam $M, M_1, \ldots, M_m$ módulos sobre um anel A. Então $M \simeq M_1 \oplus \cdots \oplus M_m$ se e só se existem homomorfismos de A-módulos $\pi_k : M \to M_k$ e $\iota_k : M_k \to M$ tais que:*

(i) $\pi_k \circ \iota_k = id_{M_k}$, $k = 1, \ldots, m$;

(ii) $\pi_k \circ \iota_l = 0$, $k \neq l$;

(iii) $\iota_1 \circ \pi_1 + \cdots + \iota_m \circ \pi_m = id_M$.

Demonstração. Suponha-se que $\phi : M \to M_1 \oplus \cdots \oplus M_m$ é um isomorfismo. Então a composição das projecções e injecções canónicas com ϕ e ϕ^{-1} satisfazem a (i), (ii) e (iii).

Inversamente, se existem homomorfismos satisfazendo a (i), (ii) e (iii), definimos os homomorfismos $\phi : M \to M_1 \oplus \cdots \oplus M_m$ e $\psi : M_1 \oplus \cdots \oplus M_m \to M$ da seguinte forma:

$$\phi(x) = (\pi_k(x))_{k=\{1,\ldots,m\}},$$
$$\psi((x_k)_{k=\{1,\ldots,m\}}) = \iota_1(x_1) + \cdots + \iota_m(x_m).$$

Então (i), (ii) e (iii) mostram que $\phi \circ \psi = id_{M_1 \oplus \cdots \oplus M_m}$ e $\psi \circ \phi = id_M$, logo, ϕ e ψ estabelecem um isomorfismo de A-módulos $M \simeq M_1 \oplus \cdots \oplus M_m$. □

Se M é um A-módulo e $\{N_i\}_{i\in I}$ é uma família de submódulos, pode acontecer que a aplicação $(\boldsymbol{v}_i) \mapsto \sum_i \boldsymbol{v}_i$ seja um isomorfismo $\bigoplus_{i\in I} N_i \simeq M$. Neste caso dizemos que M é uma soma directa dos submódulos $\{N_i\}_{i\in I}$, e escrevemos $M = \bigoplus_{i\in I} N_i$. O resultado mais utilizado para mostrar que um módulo é uma soma directa de submódulos é a seguinte proposição cuja demonstração é deixada como exercício:

Proposição 6.1.9. *Seja M um A-módulo, e $\{M_i\}_{i\in I}$ uma família de submódulos. Então $M = \bigoplus_{i\in I} M_i$ sse as seguintes duas condições se verificam:*

(i) $M = \sum_{i\in I} M_i$;

(ii) $M_j \cap (M_{i_1} + \cdots + M_{i_k}) = \{0\}$ *se* $j \notin \{i_1, \ldots, i_k\}$.

A fechar esta secção introduzimos uma estrutura algébrica importante que está relacionada com a noção de módulo.

Definição 6.1.10. Seja A uma anel com unidade. Uma ÁLGEBRA sobre A é um anel $\mathbb{A}$ tal que:

(i) $(\mathbb{A}, +)$ é um A-módulo com unidade;

(ii) $k(ab) = (ka)b = a(kb)$ para todo o $k \in A$ e $a, b \in \mathbb{A}$.

Uma álgebra $\mathbb{A}$ que, como anel, é um anel de divisão diz-se uma ALGEBRA@ÁLGEBRA DE DIVISÃO.

As noções de subálgebra, homomorfismo e isomorfismo de álgebras (sobre o mesmo anel), são mais ou menos óbvias. Deixamos ao cuidado do leitor a sua definição.

A teoria clássica das álgebras lida com álgebras sobre um corpo K. Uma álgebra sobre um corpo K que como espaço vectorial possui dimensão finita diz-se uma ÁLGEBRA DE DIMENSÃO FINITA sobre K.

Exemplos 6.1.11.

1. *Se K é uma extensão de um corpo k, então é uma álgebra sobre k. Assim, os corpos $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ são álgebras sobre cada um dos corpos que os precedem. De igual forma, o anel dos quaterniões $\mathbb{H}$ é uma álgebra sobre cada um destes corpos.*

2. *Seja A uma anel com identidade. O conjunto $\mathbb{A} = M_n(A)$ das matrizes $n \times n$ com entradas em A é uma álgebra sobre A. Se $A = K$ é um corpo, $M_n(K)$ é uma álgebra sobre K de dimensão finita.*

3. *Se V é um espaço vectorial sobre um corpo K, o conjunto $\mathbb{A} = \mathrm{End}_K(V)$ dos endomorfismos de V é uma álgebra sobre K. Esta álgebra tem dimensão finita se V tem dimensão finita. De facto, se $\dim V = n$, então esta álgebra é isomorfa à álgebra das matrizes $n \times n$ com entradas no corpo K.*

4. *Se K é um anel comutativo com identidade, o anel dos polinómios $K[x_1, \ldots, x_n]$ e o anel das séries de potências $K[[x]]$ são álgebras sobre K.*

É possível ainda considerar álgebras em que o produto não é associativo. Classes importantes de álgebras não-associativas são as álgebras de Lie e álgebras de Jordan. O estudo destas estruturas algébricas está para além do âmbito deste livro.

Exercícios.

1. Seja V um espaço vectorial sobre um corpo K, e fixe uma transformação linear $T : V \to V$.
   (a) Mostre que V é um $K[x]$-módulo quando se define multiplicação de um elemento $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ por um elemento $\boldsymbol{v} \in V$ por $p(x)\boldsymbol{v} \equiv a_n T^n(\boldsymbol{v}) + \cdots + a_1 T(\boldsymbol{v}) + a_0 \boldsymbol{v}$.
   (b) Quais são os submódulos do $K[x]$-módulo V?
   (c) Seja $V = \mathbb{R}^n$ e $T(v_1, \ldots, v_n) = (v_n, v_1, \ldots, v_{n-1})$. Determine os elementos $\boldsymbol{v} \in \mathbb{R}^n$ tais que $(x^2 - 1)\boldsymbol{v} = 0$.

2. Seja $\phi : M_1 \to M_2$ um homomorfismo de A-módulos, e $N_i \subset M_i$ $(i = 1, 2)$ submódulos tais que $\phi(N_1) \subset N_2$. Mostre que:
   (a) Existe um, e um só, homomorfismo de A-módulos $\tilde{\phi} : M_1/N_1 \to M_2/N_2$ tal que o diagrama seguinte é comutativo:

$$\begin{array}{ccc} M_1 & \xrightarrow{\phi} & M_2 \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ M_1/N_1 & \xrightarrow[\tilde{\phi}]{} & M_2/N_2 \end{array}$$

   (b) $\tilde{\phi}$ é um isomorfismo se e só se $\mathrm{Im}(\phi) + N_2 = M_2$ e $\phi^{-1}(N_2) \subset N_1$.

3. Seja $\{N_i\}_{i \in I}$ uma família de A-módulos. Mostre que:
   (a) Dado um A-módulo M e homomorfismos $\{\phi_i : M \to N_i\}_{i \in I}$, existe um único homomorfismo $\phi : M \to \prod_{i \in I} N_i$ tal que, para todo o $k \in I$, o diagrama seguinte é comutativo:

$$\begin{array}{ccc} M & \xrightarrow{\phi} & \prod_{i \in I} N_i \\ & {\scriptstyle \phi_k}\searrow & \downarrow{\scriptstyle \pi_k} \\ & & N_k \end{array}$$

   (b) $\prod_{i \in I} N_i$ é determinado a menos de um isomorfismo pela propriedade expressa em (a).

4. Seja $\{N_i\}_{i \in I}$ uma família de A-módulos. Mostre que:
   (a) Dado um A-módulo M e homomorfismos $\{\phi_i : N_i \to M\}_{i \in I}$, existe um único homomorfismo $\phi : \bigoplus_{i \in I} N_i \to M$ tal que, para todo o $k \in I$, o diagrama seguinte é comutativo:

$$\begin{array}{ccc} M & \xleftarrow{\phi} & \bigoplus_{i \in I} N_i \\ & {\scriptstyle \phi_k}\nwarrow & \uparrow{\scriptstyle \iota_k} \\ & & N_k \end{array}$$

(b) $\bigoplus_{i\in I} N_i$ é determinado a menos de um isomorfismo pela propriedade expressa em (a).

5. Seja M um A-módulo e $\{M_i\}_{i\in I}$ uma família de submódulos de M. Mostre que $M = \bigoplus_{i\in I} M_i$ sse as seguintes duas condições se verificam:

(i) $M = \sum_{i\in I} M_i$;

(ii) $M_j \cap (M_{i_1} + \cdots + M_{i_k}) = \{0\}$ se $j \notin \{i_1, \ldots, i_k\}$.

6. Uma sucessão de homomorfismos de A-módulos:

$$M_0 \xrightarrow{\phi_1} M_1 \xrightarrow{\phi_2} M_2 \longrightarrow \cdots \xrightarrow{\phi_n} M_n \ ,$$

diz-se *exacta* se $\mathrm{Im}(\phi_i) = N(\phi_{i+1})$, $i = 1, \ldots, n-1$. Mostre que:

(a) se $N \subset M$ é um submódulo, então

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0$$

é uma sucessão exacta;

(b) se M_1 e M_2 são A-módulos, então a sucessão

$$0 \longrightarrow M_1 \xrightarrow{\iota_1} M_1 \oplus M_2 \xrightarrow{\pi_2} M_2 \longrightarrow 0$$

é exacta.

7. (Lema dos Cinco) Considere o seguinte diagrama comutativo de A-módulos e transformações lineares:

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_3} & & \downarrow{\scriptstyle \phi_4} & & \downarrow{\scriptstyle \phi_5} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

Mostre que, se as linhas são exactas e ϕ_1, ϕ_2, ϕ_4 e ϕ_5 são isomorfismos, então ϕ_3 também é um isomorfismo.

8. Se M e N são A-módulos à esquerda, $\mathrm{Hom}_A(M, N)$ designa o conjunto das transformações A-lineares $\phi : M \to N$. Mostre que:

(a) $\mathrm{Hom}_A(M, N)$ é um $\mathbb{Z}$-módulo;

(b) $\mathrm{Hom}_A(M, A)$ é um A-módulo à direita;

(c) $\mathrm{End}_A(M) \equiv \mathrm{Hom}_A(M, M)$ é uma álgebra sobre A.

9. Seja M um A-módulo à esquerda. O *dual* de M é o A-módulo à direita $M^* \equiv \mathrm{Hom}_A(M, A)$. Mostre que:

(a) se $\phi : M \to N$ é A-linear, existe uma transformação linear dual (de A-módulos à direita) $\phi^* : N^* \to M^*$;

(b) $(\bigoplus_{i\in I} N_i)^* \simeq \prod_{i\in I} {N_i}^*$;

(c) pode acontecer que $M \neq \{0\}$ e $M^* = \{0\}$.

6.2 Independência Linear

Seja M um A-módulo e $S \subset M$ um conjunto não-vazio. Os elementos de S dizem-se LINEARMENTE INDEPENDENTES se, para toda a família finita $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ de elementos de S e $a_1, \ldots, a_n \in A$, se tem

$$a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n = 0 \quad \Longrightarrow \quad a_1 = \cdots = a_n = 0.$$

Caso contrário, dizemos que os elementos de S são linearmente dependentes.

Um subconjunto S de um A-módulo M diz-se GERADOR se $M = \langle S \rangle$. Neste caso, qualquer elemento $\boldsymbol{v} \in M$ pode ser escrito como uma combinação linear (em geral, não-única) de elementos de S: $\boldsymbol{v} = \sum_{i=1}^{m} a_i\boldsymbol{v}_i, a_i \in A, \boldsymbol{v}_i \in S$. Um A-módulo é de TIPO FINITO se possui um conjunto gerador finito.

Uma BASE S dum A-módulo M é um conjunto gerador cujos elementos são linearmente independentes. Dada uma base, qualquer elemento $\boldsymbol{v} \in M$ pode ser escrito de forma única como combinação linear $\sum_{i=1}^{m} a_i\boldsymbol{v}_i, a_i \in A, \boldsymbol{v}_i \in S$. Como mostram os exemplos abaixo, um A-módulo pode ou não ter uma base. Dizemos que um A-módulo M é LIVRE[3] se M possui uma base.

Exemplos 6.2.1.

1. *Qualquer espaço vectorial contém uma base (exercício).*

2. *O grupo abeliano $\mathbb{Z}_n$, visto como um $\mathbb{Z}$-módulo, não admite uma base. De facto, dado $g \in \mathbb{Z}_n$, existe sempre um $m \in \mathbb{Z}$ tal que $mg = 0$, logo, em $\mathbb{Z}_n$ não existem conjuntos linearmente independentes.*

3. *O grupo abeliano $\mathbb{Z}^m \equiv \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ é livre. Uma base é dada por $S = \{g_1, \ldots, g_m\}$, onde $g_i = (0, \ldots, 1, \ldots, 0)$.*

4. *Qualquer anel A é um A-módulo livre com base $\{1\}$. Observe-se que os submódulos coincidem com os ideais de A. Em particular, um submódulo pode não ser livre, e mesmo sendo livre pode ter uma base de cardinalidade > 1.*

Um A-módulo M diz-se CÍCLICO se é gerado por um elemento, *i.e.*, se $M = \langle \boldsymbol{v} \rangle$ para algum $\boldsymbol{v} \in M$([4]). Se $M = \langle \boldsymbol{v} \rangle$ é cíclico, então temos um homomorfismo de A-módulos, $A \to M$, dado por $a \mapsto a\boldsymbol{v}$. Este homomorfismo é sobrejectivo e, pelo 1º Teorema do Isomorfismo, $M \simeq A/\operatorname{ann}\boldsymbol{v}$, onde o ANIQUILADOR de $\boldsymbol{v}$ é o ideal $\operatorname{ann}\boldsymbol{v} = \{a \in A : a\boldsymbol{v} = 0\}$. Se $\operatorname{ann}\boldsymbol{v} = \{0\}$, então dizemos que $\boldsymbol{v}$ é um ELEMENTO LIVRE, pois neste caso $M = \langle \boldsymbol{v} \rangle \simeq A$ é livre. O conjunto dos elementos de M que não são livres designa-se por $\operatorname{Torc}(M)$.

[3] Como veremos mais à frente, esta noção é o análogo para A-módulos da noção de grupo livre.

[4] Observe que esta noção é o análogo para A-módulos da noção de grupo cíclico.

Seja X um conjunto arbitrário, e A um anel. Para cada $x \in X$ associamos uma cópia de A e formamos o A-módulo livre $M = \bigoplus_{x\in X} A$. A este módulo chama-se MÓDULO LIVRE GERADO PELO CONJUNTO X. É conveniente representar os elementos de M como somas $a_1x_1 + \cdots + a_rx_r$, onde $x_1, \ldots, x_r \in X$. Por uma soma deste tipo entende-se uma sucessão $(a_x)_{x\in X} \in M$, onde $a_{x_1} = a_1, \ldots, a_{x_r} = a_r$ e $a_x = 0$ se $x \neq x_i (i = 1, \ldots, r)$.

A proposição seguinte fornece uma caracterização dos módulos livres. Em particular, mostra que o módulo livre gerado pelo conjunto X satisfaz a mesma propriedade universal que caracteriza os grupos livres.

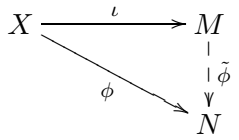
Proposição 6.2.2. *Seja A um anel. Para um A-módulo M, as seguintes afirmações são equivalentes:*

(i) *M é livre.*

(ii) *Existe uma família de submódulos cíclicos $\{N_i\}_{i\in I}$ de M, com $N_i \simeq A$, tais que $M \simeq \bigoplus_{i\in I} N_i$.*

(iii) *$M \simeq \bigoplus_{j\in J} A$ para algum conjunto de índices J.*

(iv) *Existe um conjunto $X \neq \emptyset$ e uma função $\iota : X \to M$ com a seguinte propriedade universal: Para todo o A-módulo N e função $\phi : X \to N$ existe um único homomorfismo de A-módulos $\tilde{\phi} : M \to N$ tal que o seguinte diagrama é comutativo:*



Demonstração. Vejamos que (i) ⇒ (ii) ⇒ (iii) ⇒ (iv) ⇒ (i).

(i) ⇒ (ii) Suponha-se que M é livre e seja $\{\boldsymbol{e}_i\}_{i\in I}$ uma base de M. Então, para cada $i \in I$, $N_i \equiv \langle \boldsymbol{e}_i \rangle$ é um submódulo cíclico de M isomorfo a A. A aplicação $\phi : \bigoplus_{i\in I} N_i \to M$ que associa $(\boldsymbol{v}_i)_{i\in I} \to \sum_{i\in I} \boldsymbol{v}_i$ é um isomorfismo de A-módulos.

(ii) ⇒ (iii) Óbvio.

(iii) ⇒ (iv) Seja $\psi : \bigoplus_{j\in J} A \to M$ um isomorfismo de A-módulos e $\boldsymbol{e}_k = (x_j)_{j\in J}$ o elemento de $\bigoplus_{j\in J} A$, com $x_k = 1$ e $x_j = 0$, para $j \neq k$. Tome-se ainda $X = J$ e considere-se a aplicação $\iota : X \to M$ definida por $\iota(j) = \psi(\boldsymbol{e}_j)$. Se $\phi : X \to N$ é uma função para um A-módulo N, definimos $\tilde{\phi} : M \to N$ como sendo a transformação linear que associa $\psi(\boldsymbol{e}_k) \mapsto \phi(k)$. Então $\tilde{\phi}$ torna o diagrama acima comutativo. Como $\{\psi(\boldsymbol{e}_k)\}$ é uma base de M, $\tilde{\phi}$ é único.

(iv) ⇒ (i) Deixamos como exercício verificar que $\{\iota(x)\}_{x\in X}$ é uma base de M. □

Seja M um A-módulo livre que admite uma base finita $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$. Então, a proposição mostra que $M \simeq \bigoplus_{i=1}^{n} A \equiv A^n$. Será que qualquer outra base de M tem a mesma cardinalidade? Por outras palavras, será que $A^n \simeq A^m$ implica $n = m$? Talvez um pouco surpreendentemente, a resposta é não, como mostra um exercício no final desta secção.

Por outro lado, se M é um A-módulo livre que admite uma base infinita, temos o seguinte resultado:

Proposição 6.2.3. *Se um A-módulo M possui uma base infinita, então todas as bases de M têm a mesma cardinalidade.*

Demonstração. Sejam $\{\boldsymbol{e}_i\}_{i\in I}$ e $\{\boldsymbol{f}_j\}_{j\in J}$ bases de M e suponha-se que I é infinito.

(a) *J é infinito:* Suponha-se, por absurdo, que J é finito, digamos $J = \{1, \ldots, m\}$. Então existem elementos $c_{ji_l} \in A$ com $i_l \in I$, $l, j \in J$, tais que $\boldsymbol{f}_j = \sum_{l=1}^{m} c_{ji_l}\boldsymbol{e}_{i_l}$. Mas então $\{\boldsymbol{e}_{i_1}, \ldots, \boldsymbol{e}_{i_m}\}$ é um conjunto gerador de M, logo, se $\boldsymbol{e}_{i_0}$ é outro elemento da base distinto destes, existem $a_1, \ldots, a_m \in A$ tais que

$$\boldsymbol{e}_{i_0} = a_1\boldsymbol{e}_{i_1} + \cdots + a_m\boldsymbol{e}_{i_m},$$

o que contradiz a independência linear dos $\{\boldsymbol{e}_i\}_{i\in I}$.

(b) *Existe $\phi : I \to \mathcal{P}_{fin}(J) \times \mathbb{N}$ injectivo:*[5] Seja $\psi : I \to \mathcal{P}_{\text{fin}}(J)$ a aplicação que a $i \in I$ associa $\{j_1, \ldots, j_m\}$, onde os $j_1, \ldots, j_m$ são os (únicos) índices de J que satisfazem

$$\boldsymbol{e}_i = a_{j_1}\boldsymbol{f}_{j_1} + \cdots + a_{j_m}\boldsymbol{f}_{j_m} \qquad (a_{jl} \neq 0).$$

A aplicação ψ não é injectiva, mas se $P \subset \mathcal{P}_{\text{fin}}(J)$, então $\psi^{-1}(P)$ é finito (porquê?). Logo podemos ordenar $\psi^{-1}(P)$. Se $i \in \psi^{-1}(P)$, então $\phi(i) \equiv (P, \alpha)$, onde α é o número ordinal de i em $\psi^{-1}(P)$. Como I é uma união disjunta dos $\psi^{-1}(P)$, obtemos uma aplicação injectiva $\phi : I \to \mathcal{P}_{\text{fin}}(J) \times \mathbb{N}$.

(c) $|I| = |J|$: Como J é infinito, temos, por (b),

$$|I| \leq |\mathcal{P}_{\text{fin}}(J) \times \mathbb{N}| = |\mathcal{P}_{\text{fin}}(J)| = |J|.$$

Invertendo os papéis de I e J, concluímos que $|J| \leq |I|$. Pelo Teorema de Schröder-Bernstein, vemos que $|I| = |J|$.

□

[5] Designamos por $\mathcal{P}_{\text{fin}}(J)$ o conjunto das partes finitas de J. No Apêndice mostra-se que, se J é infinito, $\mathcal{P}_{\text{fin}}(J)$ tem o mesmo cardinal que J.

Estes resultados motivam então a seguinte definição:

Definição 6.2.4. Diz-se que um anel A possui a PROPRIEDADE DE INVARIÂNCIA DIMENSIONAL se, para qualquer A-módulo livre M, todas as bases de M possuem a mesma cardinalidade. Ao cardinal comum das bases de M chama-se DIMENSÃO de M, e escreve-se $\dim_A M$.

Deixamos como exercício verificar que os anéis de divisão possuem a propriedade de invariância dimensional, donde faz sentido falar em dimensão de um espaço vectorial sobre um anel de divisão.

Proposição 6.2.5. *Os anéis comutativos possuem a propriedade de invariância dimensional.*

Demonstração. Sejam $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ e $\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m\}$ bases de um A-módulo livre M. Então existem elementos $b_{ji}, c_{ij} \in A$, $i = 1, \ldots, n$, $j = 1, \ldots, m$ tais que

$$\boldsymbol{f}_j = \sum_i b_{ji} \boldsymbol{e}_i, \qquad \boldsymbol{e}_i = \sum_j c_{ij} \boldsymbol{f}_j.$$

Por substituição, conclui-se que:

$$\boldsymbol{f}_j = \sum_{il} b_{ji} c_{il} \boldsymbol{f}_l, \qquad \boldsymbol{e}_i = \sum_{jl} c_{ij} b_{jl} \boldsymbol{e}_l.$$

Como $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ e $\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m\}$ são bases de M, introduzindo as matrizes $B = (b_{ji})_{j=1,i=1}^{m,n}$ e $C = (c_{ij})_{i=1,j=1}^{n,m}$, concluímos que:

$$BC = I_{m\times m}, \qquad CB = I_{n\times n}.$$

Suponha-se que a característica de A é zero. Como A é comutativo, temos[6]

$$m = \operatorname{tr}(I_{m\times m}) = \operatorname{tr}(BC) = \operatorname{tr}(CB) = \operatorname{tr}(I_{n\times n}) = n.$$

A primeira e a última igualdade só são válidas se a característica for zero. O caso em que a característica é diferente de zero é deixado como exercício. □

Exercícios.

1. Dê um exemplo de um A-módulo não-isomorfo a A, em que qualquer conjunto com 2 ou mais elementos é linearmente dependente.

2. Seja A um anel comutativo, e M um A-módulo.
   (a) Mostre que, se $\boldsymbol{v} \in \operatorname{Torc}(M)$, então $\langle \boldsymbol{v} \rangle \subset \operatorname{Torc}(M)$;
   (b) É $\operatorname{Torc}(M)$ um submódulo de M ?

[6] Recordemos que, se $A = (a_{ij})$ é uma matriz $n \times n$, o TRAÇO de A é $\operatorname{tr} A = \sum_{i=1}^n a_{ii}$.

3. Seja A um anel comutativo. Mostre que $\mathrm{End}_A(A^n)$ é isomorfo ao anel $M_n(A)$ das matrizes $n \times n$ com entradas em A.

4. Seja M um A-módulo, $X \neq \emptyset$ um conjunto e $\iota : X \to M$ uma função com seguinte propriedade: Para todo o A-módulo N e função $\phi : X \to N$ existe um único homomorfismo de A-módulos $\tilde{\phi} : M \to N$ tal que $\phi = \tilde{\phi} \circ \iota$. Mostre que $\{\iota(x)\}_{x \in X}$ é uma base de M.

5. Seja V um espaço vectorial sobre um anel de divisão D. Mostre que:
   (a) V possui uma base $\{\boldsymbol{e}_i\}_{I \in I}$;
   (b) D possui a propriedade de invariância dimensional.

6. Seja A um anel comutativo. Mostre que:
   (a) se $B, C \in M_n(A)$ são matrizes $n \times n$, então $BC = I_{n\times n}$ implica $CB = I_{n\times n}$;
   (b) se B é uma matriz $m \times n$, C é uma matriz $n \times m$, $BC = I_{m\times m}$ e $CB = I_{n\times n}$, então $m = n$.

7. Seja $\mathbb{R}^\infty = \bigoplus_{i=1}^{\infty} \mathbb{R}$ (soma directa de $\mathbb{R}$-módulos), e $A = \mathrm{End}(\mathbb{R}^\infty)$ o anel das transformações $\mathbb{R}$-lineares de $\mathbb{R}^\infty$. Mostre que $A \simeq A \oplus A$ (como A-módulos), *i.e.*, que A possui uma base de 2 elementos.

8. Mostre que qualquer A-módulo é um quociente dum A-módulo livre.

6.3 Produtos Tensoriais

Nesta secção, A designa um anel comutativo[7]. Em particular, os módulos livres que estudamos possuem a propriedade de invariância dimensional.

Se $M_1, \ldots, M_r, N$ são A-módulos, uma *transformação A-multilinear* é uma aplicação $\mu : M_1 \times \cdots \times M_r \to N$ que é A-linear em cada variável:

$$\mu(\boldsymbol{v}_1, \ldots, a\boldsymbol{v}_i^{'} + b\boldsymbol{v}_i^{''}, \ldots, \boldsymbol{v}_r) = a\mu(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i^{'}, \ldots, \boldsymbol{v}_r) + b\mu(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i^{''}, \ldots, \boldsymbol{v}_r).$$

Designamos por $L(M_1, \ldots, M_r; N)$ o conjunto das transformações A-multilineares. Verificamos facilmente que $L(M_1, \ldots, M_r; N)$ é um A-módulo para as operações usuais de adição e multiplicação por escalares

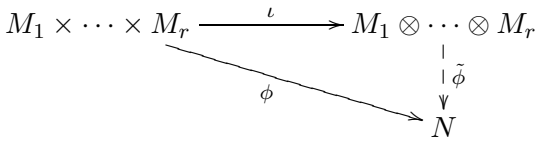
$$(\mu_1 + \mu_2)(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r) \equiv \mu_1(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r) + \mu_2(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r),$$
$$(a\mu)(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r) \equiv a\mu(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r).$$

Se $M_1 = \cdots = M_r = M$ escrevemos $L^r(M; N)$ em vez de $L(M, \ldots, M; N)$.

[7] Podem definir-se produtos tensoriais de módulos não-comutativos. Nesse caso é preciso distinguir entre módulos à esquerda e módulos à direita.

Proposição 6.3.1. *Sejam $M_1, \ldots, M_r$ A-módulos.*

(i) Existe um A-módulo $\bigotimes_{i=1}^r M_i \equiv M_1 \otimes \cdots \otimes M_r$ e uma aplicação A-multilinear $\iota : M_1 \times \cdots \times M_r \to M_1 \otimes \cdots \otimes M_r$ com a seguinte propriedade universal: para todo o A-módulo N e aplicação A-multilinear $\phi : M_1 \times \cdots \times M_r \to N$, existe um único homomorfismo $\tilde{\phi} : M_1 \otimes \cdots \otimes M_r \to N$ que torna comutativo o seguinte diagrama:



(ii) O A-módulo $M_1 \otimes \cdots \otimes M_r$ é determinado pela propriedade universal expressa em (i) a menos de um isomorfismo.

Demonstração. Seja L o A-módulo livre gerado pelo conjunto $M_1 \times \cdots \times M_r$, *i.e.*,

$$L = \bigoplus_{i \in I} A,$$

onde existe um termo na soma para cada $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r) \in M_1 \times \cdots \times M_r$ (*i.e.*, o conjunto dos índices I coincide com este produto). Designando por R o submódulo de L gerado pelos elementos da forma

$$(\boldsymbol{v}_1, \ldots, a\boldsymbol{v}_i^{'} + b\boldsymbol{v}_i^{''}, \ldots, \boldsymbol{v}_r) - a(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i^{'}, \ldots, \boldsymbol{v}_r) - b(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i^{''}, \ldots, \boldsymbol{v}_r), \tag{6.3.1}$$

tomamos, para $M_1 \otimes \cdots \otimes M_r$ o módulo quociente L/R. Por sua vez, a aplicação $\iota : M_1 \times \cdots \times M_r \to M_1 \otimes \cdots \otimes M_r$ é a composição da injecção canónica $M_1 \times \cdots \times M_r \to L$ com a projecção canónica $L \to L/R$.

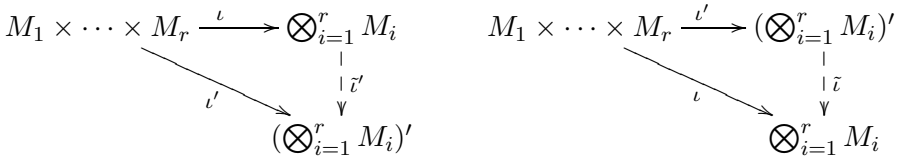
Se $\phi : M_1 \times \cdots \times M_r \to N$ é uma transformação A-multilinear, então obtemos uma aplicação induzida $\bar{\phi} : L \to N$ definida da seguinte forma: se $\oplus_{i \in I} a_i(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r) \in L$, então

$$\bar{\phi}(\oplus_{i \in I} a_i(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r)) = \sum_{i \in I} a_i \phi(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r).$$

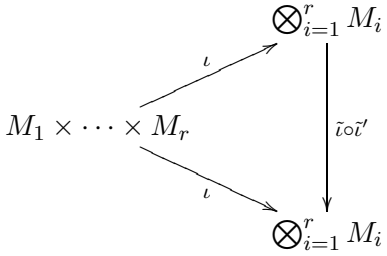
Esta aplicação está bem definida, pois apenas um número finito dos a_i não é zero. É ainda fácil de ver que $\bar{\phi}$ é A-linear. Como ϕ é A-multilinear, $\bar{\phi}$ anula-se em elementos da forma (6.3.1), logo, em R. Por passagem ao quociente, obtemos então uma transformação A-linear $\tilde{\phi} : M_1 \otimes \cdots \otimes M_r \to N$ e, por definição, $\phi = \tilde{\phi} \circ \iota$.

Finalmente, seja $(\bigotimes_{i=1}^r M_i)^{'}$ um A-módulo, e $\iota^{'} : M_1 \times \cdots \times M_r \to (\bigotimes_{i=1}^r M_i)^{'}$ uma transformação A-multilinear satisfazendo à propriedade

universal expressa em (i). Então temos diagramas comutativos:



que fornecem transformações A-lineares $\tilde{\iota}$ e $\tilde{\iota}'$. A composição $\tilde{\iota} \circ \tilde{\iota}'$ torna o seguinte diagrama comutativo:



Como a transformação identidade $id_{M_1 \otimes \cdots \otimes M_r}$ também torna este diagrama comutativo, a unicidade na propriedade universal implica $\tilde{\iota} \circ \tilde{\iota}' = id_{M_1 \otimes \cdots \otimes M_r}$. De igual forma, vemos que $\tilde{\iota}' \circ \tilde{\iota} = id_{(M_1 \otimes \cdots \otimes M_r)'}$, logo, estas aplicações fornecem um isomorfismo de A-módulos $\bigotimes_{i=1}^r M_i \simeq (\bigotimes_{i=1}^r M_i)'$. □

Ao A-módulo $M_1 \otimes \cdots \otimes M_r$ chamamos PRODUTO TENSORIAL dos módulos $M_1, \ldots, M_r$. Se $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r) \in M_1 \times \cdots \times M_r$, a imagem $\iota(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r) \in M_1 \otimes \cdots \otimes M_r$ é designada por $\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_r$. Nesta notação, temos a seguinte propriedade:

$$\boldsymbol{v}_1 \otimes \cdots \otimes (a\boldsymbol{v}_i^{'} + b\boldsymbol{v}_i^{''}) \otimes \cdots \otimes \boldsymbol{v}_r = a(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_i^{'} \otimes \cdots \otimes \boldsymbol{v}_r) + b(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_i^{''} \otimes \cdots \otimes \boldsymbol{v}_r).$$

Qualquer elemento de $M_1 \otimes \cdots \otimes M_r$ pode ser escrito como uma soma de elementos da forma $\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_r$, pois, como mostra a demonstração da proposição acima, estes elementos formam um conjunto gerador. Esta representação não é única pois a aplicação ι não é injectiva.

Exemplo 6.3.2.

No produto tensorial (sobre $\mathbb{Z}$) de $\mathbb{Z}_2$ com $\mathbb{Z}_4$, temos as seguintes relações:

$$0 \otimes n = 1 \otimes 2 \quad (n = 0, 1, 2, 3),$$
$$1 \otimes 1 = 1 \otimes 3.$$

Donde é fácil deduzir que $\mathbb{Z}_2 \otimes \mathbb{Z}_4 \simeq \mathbb{Z}_2$.

A proposição seguinte é um simples exercício envolvendo a definição de produto tensorial.

Proposição 6.3.3. (PROPRIEDADES DE $\bigotimes$) *Sejam $M, N,$ e P A-módulos, e $\{M_i\}_{i\in I}$ uma família de A-módulos. Então existem os seguintes isomorfismos de A-módulos:*

(i) $M \otimes N \otimes P \simeq (M \otimes N) \otimes P \simeq M \otimes (N \otimes P)$ *que fazem corresponder os elementos* $\boldsymbol{v} \otimes \boldsymbol{w} \otimes \boldsymbol{z} \leftrightarrow (\boldsymbol{v} \otimes \boldsymbol{w}) \otimes \boldsymbol{z} \leftrightarrow \boldsymbol{v} \otimes (\boldsymbol{w} \otimes \boldsymbol{z})$, *onde* $\boldsymbol{v} \in M$, $\boldsymbol{w} \in N$ *e* $\boldsymbol{z} \in P$;

(ii) $M \otimes N \simeq N \otimes M$ *que faz corresponder* $\boldsymbol{v} \otimes \boldsymbol{w} \leftrightarrow \boldsymbol{w} \otimes \boldsymbol{v}$, *onde* $\boldsymbol{v} \in M$ *e* $\boldsymbol{w} \in N$;

(iii) $(\bigoplus_{i\in I} M_i) \otimes N \simeq \bigoplus_{i\in I}(M_i \otimes N)$ *que faz corresponder* $(\boldsymbol{v}_i)_{i\in I} \otimes \boldsymbol{w} \leftrightarrow (\boldsymbol{v}_i \otimes \boldsymbol{w})_{i\in I}$, *onde* $\boldsymbol{v}_i \in M_i, \boldsymbol{w} \in N$.

Como mostra o exemplo acima, em geral o produto tensorial $M \otimes N$ envolve um grande número de relações entre os elementos da forma $\boldsymbol{v} \otimes \boldsymbol{w}$. No entanto, no caso de módulos livres, apenas existem as "relações óbvias", como mostra a seguinte proposição:

Proposição 6.3.4. *Sejam M e N dois A-módulos livres, com bases $\{\boldsymbol{v}_i\}_{i\in I}$ e $\{\boldsymbol{w}_j\}_{j\in J}$. Então $M \otimes N$ é livre, com base $\{\boldsymbol{v}_i \otimes \boldsymbol{w}_j\}_{(i,j)\in I\times J}$.*

Demonstração. É óbvio que $\{\boldsymbol{v}_i \otimes \boldsymbol{w}_j\}_{(i,j)\in I\times J}$ é um conjunto gerador. Para ver que estes elementos são linearmente independentes, considere-se a aplicação $\phi : M \times N \to \bigoplus_{(i,j)\in I\times J} A$ definida por

$$\phi(\sum_{i\in I} a_i \boldsymbol{v}_i, \sum_{j\in J} b_j \boldsymbol{w}_j) = (a_i b_j)_{(i,j)\in I\times J}.$$

Como ϕ é A-bilinear, existe um homomorfismo $\tilde{\phi} : M \otimes N \to \bigoplus_{(i,j)\in I\times J} A$ tal que $\phi = \tilde{\phi} \circ \iota$ e

$$\begin{aligned}\tilde{\phi}(\boldsymbol{v}_k \otimes \boldsymbol{w}_l) &= \tilde{\phi} \circ \iota(\boldsymbol{v}_k, \boldsymbol{w}_l) \\ &= \phi(\boldsymbol{v}_k, \boldsymbol{w}_l) = (e_{kl})_{(i,j)\in I\times J}.\end{aligned}$$

onde $(e_{kl})_{ij} = 1$, se $(k,l) = (i,j)$, e $(e_{kl})_{ij} = 0$, caso contrário. Os elementos $(e_{kl})_{(i,j)\in I\times J}$ formam uma base de $\oplus_{(i,j)\in I\times J} A$, logo, os $\{\boldsymbol{v}_i \otimes \boldsymbol{w}_j\}_{(i,j)\in I\times J}$ são linearmente independentes. □

Corolário 6.3.5. *Sejam M e N dois A-módulos livres, com* $\dim M = m$ *e* $\dim N = n$, *então* $\dim(M \otimes N) = mn$.

Se $\phi_i : M_i \to N_i,\ i = 1, \ldots, r$ são homomorfismos de A-módulos, então temos o homomorfismo $T(\phi_1, \ldots, \phi_r) : M_1 \otimes \cdots \otimes M_r \to N_1 \otimes \cdots \otimes N_r$ definido da seguinte forma: $T(\phi_1, \ldots, \phi_r)$ é a única transformação A-linear que satisfaz

$$T(\phi_1, \ldots, \phi_r)(\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_r) = \phi_1(\boldsymbol{v}_1) \otimes \cdots \otimes \phi_r(\boldsymbol{v}_r).$$

Como o lado direito define uma expressão multilinear nos $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r$ a propriedade universal do produto tensorial mostra que esta aplicação fica bem definida.

Nas proposições seguintes utilizamos o facto de que A é comutativo para escrever $\mathrm{Hom}_A(M,N)$, $\mathrm{End}_A(M)$ e M^* como A-módulos à esquerda (ver Exercícios 6.1.8 e 6.1.9).

Proposição 6.3.6. *Sejam M_i e N_i, $i = 1, \ldots, r$, A-módulos livres de dimensão finita. Existe um isomorfismo:*

$$\mathrm{Hom}_A(M_1,N_1) \otimes \cdots \otimes \mathrm{Hom}_A(M_r,N_r) \simeq \\ \simeq \mathrm{Hom}_A(M_1 \otimes \cdots \otimes M_r, N_1 \otimes \cdots \otimes N_r),$$

que a $\phi_1 \otimes \cdots \otimes \phi_r$ associa $T(\phi_1, \ldots, \phi_r)$.

Demonstração. Pela associatividade do produto tensorial, basta provar o caso $r = 2$. Sejam M_1, M_2, N_1 e N_2 A-módulos livres com bases $\{\boldsymbol{v}_1', \ldots, \boldsymbol{v}_{m_1}'\}$, $\{\boldsymbol{v}_1'', \ldots, \boldsymbol{v}_{m_2}''\}$, $\{\boldsymbol{w}_1', \ldots, \boldsymbol{w}_{n_1}'\}$ e $\{\boldsymbol{w}_1'', \ldots, \boldsymbol{w}_{n_2}''\}$, respectivamente. Definimos bases $\{\phi_{ij}\}$ de $\mathrm{Hom}_A(M_1,N_1)$ e $\{\psi_{kl}\}$ de $\mathrm{Hom}_A(M_2,N_2)$ pelas fórmulas:

$$\phi_{ij}(\boldsymbol{v}_a') = \begin{cases} \boldsymbol{w}_j' & \text{se} \quad a = i, \\ 0 & \text{se} \quad a \neq i, \end{cases} \qquad \psi_{kl}(\boldsymbol{v}_b'') = \begin{cases} \boldsymbol{w}_l'' & \text{se} \quad b = k, \\ 0 & \text{se} \quad b \neq k. \end{cases}$$

Pela proposição precedente, uma base de $\mathrm{Hom}_A(M_1,N_1) \otimes \mathrm{Hom}_A(M_2,N_2)$ é $\{\phi_{ij} \otimes \psi_{kl}\}$. Por outro lado, vemos que

$$T(\phi_{ij},\psi_{kl})(\boldsymbol{v}_a' \otimes \boldsymbol{v}_b'') = \begin{cases} \boldsymbol{w}_j' \otimes \boldsymbol{w}_l'' & \text{se} \quad (a,b) = (i,k), \\ 0 & \text{se} \quad (a,b) \neq (i,k). \end{cases}$$

Logo, $\{T(\phi_{ij},\psi_{kl})\}$ é uma base de $\mathrm{Hom}(M_1 \otimes N_1, M_2 \otimes N_2)$, e concluímos que existe um isomorfismo de A-módulos que transforma $\phi \otimes \psi \mapsto T(\phi,\psi)$. □

Vemos, pois, que no caso de A-módulos livres de dimensão finita, podemos escrever $\phi_1 \otimes \cdots \otimes \phi_r$ em vez de $T(\phi_1, \ldots, \phi_r)$, sem qualquer ambiguidade.

Corolário 6.3.7. *Sejam M e N A-módulos livres de dimensão finita. Existem isomorfismos:*

(i) $\mathrm{End}_A(M) \otimes \mathrm{End}_A(N) \simeq \mathrm{End}_A(M \otimes N)$;

(ii) $M^* \otimes N^* \simeq (M \otimes N)^*$.

Estes isomorfismos são complementados pelo seguinte isomorfismo que fornece uma interpretação do produto tensorial para A-módulos livres de dimensão finita.

Corolário 6.3.8. *Sejam M e N A-módulos livres de dimensão finita. Existe um isomorfismo*

$$M^* \otimes N \simeq \mathrm{Hom}_A(M, N)$$

que, a um elemento $l \otimes \boldsymbol{w}$, associa o homomorfismo $\phi_{l,\boldsymbol{w}}$ dado por $\boldsymbol{v} \mapsto l(\boldsymbol{v})\boldsymbol{w}$.

Demonstração. Se $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ é uma base de M, seja $\{l_1, \ldots, l_n\}$ a base de M^* dual definida por

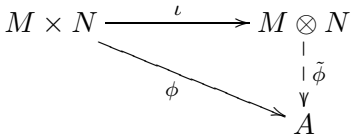
$$l_i(\boldsymbol{v}_j) = \begin{cases} 1 & \text{se} \quad j = i, \\ \\ 0 & \text{se} \quad j \neq i. \end{cases}$$

Se $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$ é uma base de N, então os $\{l_i \otimes \boldsymbol{w}_k\}$ formam uma base de $M^* \otimes N$. Por outro lado, os homomorfismos $\phi_{l_i,\boldsymbol{w}_k} \in \mathrm{Hom}_A(M, N)$ satisfazem a

$$\phi_{l_i,\boldsymbol{w}_k}(\boldsymbol{v}_j) = l_i(\boldsymbol{v}_j)\boldsymbol{w}_k = \begin{cases} \boldsymbol{w}_k & \text{se} \quad j = i, \\ \\ 0 & \text{se} \quad j \neq i, \end{cases}$$

logo, os $\{\phi_{l_i,\boldsymbol{w}_k}\}$ formam uma base de $\mathrm{Hom}_A(M, N)$, e existe um isomorfismo $M^* \otimes N \simeq \mathrm{Hom}_A(M, N)$ que transforma $l \otimes \boldsymbol{w} \to \phi_{l,\boldsymbol{w}}$. □

Se M e N são A-módulos, o diagrama



mostra que a correspondência $\phi \mapsto \tilde{\phi}$ determina um isomorfismo $L(M, N; A) \simeq (M \otimes N)^*$. Em geral, este isomorfismo não é suficiente para caracterizar o produto tensorial $M \otimes N$, pois pode acontecer $M \otimes N \neq \{0\}$, com $(M \otimes N)^* = \{0\}$. Se, no entanto, M e N são livres de dimensão finita, então, pelos resultados acima, obtemos:

$$M \otimes N \simeq L(M^*, N^*; A).$$

Este tipo de isomorfismo estende-se a certos módulos livres de dimensão infinita. É frequentemente usado em Geometria Diferencial para caracterizar tensores (e em particular formas diferenciais).

É bem conhecido que um espaço vectorial sobre $\mathbb{R}$ pode ser visto como um espaço vectorial sobre $\mathbb{C}$, com a mesma dimensão. Usando produtos tensoriais, podemos estender o anel dos escalares de um dado módulo, o que passamos a explicar.

Seja A um anel, e $\tilde{A}$ uma extensão de A (*i.e.*, A é um subanel de $\tilde{A}$). Podemos ver $\tilde{A}$ como um A-módulo: se $a \in A$ e $b \in \tilde{A}$, então o produto ab é definido por multiplicação em $\tilde{A}$. Assim, se M é um A-módulo, podemos formar o A-módulo $M_{\tilde{A}} = \tilde{A} \otimes_A M$[8]. Definimos uma operação de $\tilde{A}$ em $M_{\tilde{A}}$ pela fórmula

$$b(c \otimes \boldsymbol{v}) \equiv (bc) \otimes \boldsymbol{v}.$$

Verificamos facilmente que $M_{\tilde{A}}$ com esta nova operação de multiplicação por escalares de $\tilde{A}$ é um módulo sobre $\tilde{A}$. Dizemos que $M_{\tilde{A}}$ é obtido de M por EXTENSÃO DO ANEL DOS ESCALARES. Se $\phi : M \to N$ é uma transformação A-linear, obtemos um homomorfismo $\tilde{\phi} : M_{\tilde{A}} \to N_{\tilde{A}}$ se definirmos

$$\tilde{\phi}(c \otimes \boldsymbol{v}) \equiv c \otimes \tilde{\phi}(\boldsymbol{v}).$$

Proposição 6.3.9. *Se M é um A-módulo livre, então $M_{\tilde{A}}$ é um $\tilde{A}$-módulo livre com a mesma dimensão.*

Demonstração. Se $M \simeq \oplus_{i \in I} A$, então

$$\begin{aligned} M_{\tilde{A}} &= \tilde{A} \otimes_A M \\ &\simeq \tilde{A} \otimes_A (\oplus_{i \in I} A) \\ &\simeq \oplus_{i \in I} (\tilde{A} \otimes_A A) \simeq \oplus_{i \in I} \tilde{A}, \end{aligned}$$

onde o último isomorfismo é obtido do isomorfismo $\tilde{A} \to \tilde{A} \otimes_A A$ definido por $a \mapsto a \otimes 1$. □

Exemplos 6.3.10.

1. *Se V é um espaço vectorial sobre $\mathbb{R}$, então $V_{\mathbb{C}}$ (por vezes chamado a* complexificação *de V) é um espaço vectorial sobre $\mathbb{C}$. Se $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ é uma base de V sobre $\mathbb{R}$, então $\{1 \otimes \boldsymbol{v}_1, \ldots, 1 \otimes \boldsymbol{v}_n\}$ é uma base de $V_{\mathbb{C}}$ sobre $\mathbb{C}$. Logo, se $V \simeq \mathbb{R}^n$, então $V_{\mathbb{C}} \simeq \mathbb{C}^n$.*

2. *Se estendermos o anel dos escalares do $\mathbb{Z}$-módulo $\mathbb{Z}$ a $\mathbb{Q}$, obtemos um $\mathbb{Q}$-módulo isomorfo a $\mathbb{Q}$.*

3. *Se estendermos o anel dos escalares do $\mathbb{Z}$-módulo $\mathbb{Z}_n$ a $\mathbb{Q}$, obtemos um $\mathbb{Q}$-módulo trivial (exercício).*

Existem muitas outras construções em que produtos tensoriais, Hom, e dualidade desempenham um papel relevante.

Exercícios.

[8] Quando estão em jogo mais do que um anel, é conveniente utilizar o símbolo do anel como subscrito no sinal de produto tensorial, de forma a que seja claro em que anel se forma o produto tensorial.

1. Verifique as propriedades básicas dos produtos tensoriais (Proposição 6.3.3).

2. Sejam $\rho_1 : G \to GL(V_1)$ e $\rho_2 : G \to GL(V_2)$ representações dum grupo em espaços vectoriais V_1 e V_2. Mostre que existe exactamente uma representação $\rho : G \to GL(V_1 \otimes V_2)$ que satisfaz a seguinte propriedade:

$$\rho(g)(\boldsymbol{v}_1 \otimes \boldsymbol{v}_2) = \rho_1(g)(\boldsymbol{v}_1) \otimes \rho_2(g)(\boldsymbol{v}_2).$$

3. Mostre que $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \simeq \mathbb{Z}_q$. Qual é a expressão de q em termos de m e n?

4. Mostre que $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_n$ é trivial.

5. Mostre que, se

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

é uma sequência exacta de A-módulos e N é um A-módulo, então a sequência de A-módulos

$$M_1 \otimes N \longrightarrow M_2 \otimes N \longrightarrow M_3 \otimes N \longrightarrow 0$$

também é exacta. Mostre, ainda, que a primeira aplicação desta sequência pode não ser injectiva.

6. Seja M um A-módulo, seja R o submódulo de $\bigotimes_{i=1}^{r} M$ gerado por elementos da forma

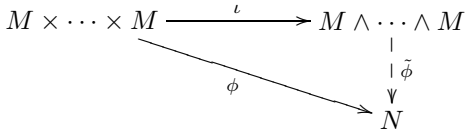
$$\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_r, \qquad \boldsymbol{v}_i = \boldsymbol{v}_j \text{ para algum } i, j \ (i \neq j)$$

e designe por $\bigwedge^r M$ o módulo quociente $\bigotimes_{i=1}^{r} M/R$, e por $\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_r$ a imagem de $\boldsymbol{v}_1 \otimes \cdots \otimes \boldsymbol{v}_r$ em $\bigwedge^r M$. Mostre que:

   (i) a aplicação A-multilinear $\iota : M \times \cdots \times M \to M \wedge \cdots \wedge M$ que a $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r)$ associa $\boldsymbol{v}_1 \wedge \cdots \wedge \boldsymbol{v}_r$ é alternada, *i.e.*,

$$\iota(\boldsymbol{v}_{\sigma(1)}, \ldots, \boldsymbol{v}_{\sigma(r)}) = \operatorname{sgn} \sigma \cdot \iota(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r), \quad \forall \sigma \in S_r.$$

   (ii) se $\phi : M \times \cdots \times M \to N$ é A-multilinear alternada, existe um único homomorfismo $\tilde{\phi} : M \wedge \cdots \wedge M \to N$ que torna o seguinte diagrama comutativo:



   (iii) O A-módulo $M \wedge \cdots \wedge M$ é determinado pela propriedade universal expressa em (ii) a menos de um isomorfismo.

   (iv) Se M é livre de dimensão finita n, então $\bigwedge^r M$ é livre com dimensão igual a $\begin{pmatrix} n \\ r \end{pmatrix}$ se $1 \leq r \leq n$, e igual a 0 se $r > n$.

(v) Se M é livre de dimensão finita, então $\bigwedge^r M^* \simeq A^r(M)$ (o módulo das aplicações multilineares alternadas $\varphi : \underbrace{M \times \cdots \times M}_{\text{r vezes}} \to A$).

7. Seja $\{M_i\}_{i\in I}$ uma família de A-módulos onde I é um conjunto parcialmente ordenado que satisfaz à seguinte condição[9]:

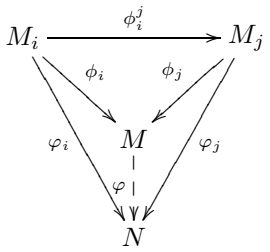
$$\forall i, j \in I,\ \exists k \in I :\ i \leq k \text{ e } j \leq k.$$

Assuma, ainda, que para todo o $i, j \in I$ com $i \leq j$ existe uma aplicação A-linear $\phi_i^j : M_i \to M_j$ tal que sempre que $i \leq j \leq k$ se tem

$$\phi_j^k \circ \phi_i^j = \phi_i^k, \quad \phi_i^i = id.$$

Mostre que:

(a) existe um A-módulo M e aplicações A-lineares $\phi_i : M_i \to M$ que satisfazem à seguinte propriedade universal: se N é um A-módulo e $\varphi_i : M_i \to N$ são aplicações A-lineares tais que $\varphi_j \circ \phi_i^j = \varphi_i$, existe uma única aplicação A-linear $\varphi : M \to N$ que torna o seguinte diagrama comutativo:



Mostre, ainda, que $M = \bigcup_{i\in I} \phi_i(M_i)$ e que é único a menos de isomorfismo. A M chama-se LIMITE DIRECTO da família $\{M_i, \phi_i^j\}$ e designa-se por $\varinjlim M_i$;

(b) se $M_1 \subset M_2 \subset \cdots \subset M_K \subset \ldots$ são A-módulos, calcule $\varinjlim M_i$;

(c) se N é um A-módulo, então

$$\varinjlim (M_i \otimes N) = (\varinjlim M_i) \otimes N.$$

8. Defina LIMITE INVERSO de uma família dirigida de A-módulos, e mostre que é caracterizado por uma propriedade universal análoga à de limite directo com as setas no diagrama acima invertidas.

6.4 Módulos sobre Domínios Integrais

Nesta secção, os anéis são comutativos, com unidade, e é válida a lei do corte, *i.e.*, são domínios integrais. Este anéis são importantes em Álgebra Linear devido à seguinte propriedade.

[9] Um conjunto parcialmente ordenado que satisfaz esta propriedade diz-se DIRIGIDO ou FILTRANTE.

Proposição 6.4.1. *Seja M um módulo sobre um domínio integral D. Então* $\mathrm{Torc}(M)$ *é um D-submódulo de M.*

Demonstração. Recordamos que

$$\mathrm{Torc}(M) = \{\boldsymbol{v} \in M : \text{ existe } a \in D \text{ com } a\boldsymbol{v} = 0 \text{ e } a \neq 0\}.$$

Logo, se $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathrm{Torc}(M)$, então existem $a_1, a_2 \in D$ não-nulos tais que $a_1\boldsymbol{v}_1 = 0$ e $a_2\boldsymbol{v}_2 = 0$. Se $d_1, d_2 \in D$, então

$$a_1a_2(d_1\boldsymbol{v}_1 + d_2\boldsymbol{v}_2) = a_2d_1a_1\boldsymbol{v}_1 + a_1d_2a_2\boldsymbol{v}_2 = 0,$$

com $a_1a_2 \neq 0$, pois, se $a_1a_2 = 0$, a lei do corte mostra que $a_1 = 0$ ou $a_2 = 0$. Vemos, pois, que $d_1\boldsymbol{v}_1 + d_2\boldsymbol{v}_2 \in \mathrm{Torc}(M)$. □

Chama-se a $\mathrm{Torc}(M)$ SUBMÓDULO DE TORÇÃO de M. Se $M = \mathrm{Torc}(M)$, então diz-se que M é um MÓDULO DE TORÇÃO. Se $\mathrm{Torc}(M) = 0$, *i.e.*, se todos os elementos de M são livres, então diz-se que M é um MÓDULO LIVRE DE TORÇÃO.

Exemplos 6.4.2.

1. *Se M é um D-módulo livre, então* $\mathrm{Torc}(M) = 0$ *(exercício), e M é livre de torção.*
2. *O $\mathbb{Z}$-módulo $\mathbb{Q}$ é livre de torção, mas $\mathbb{Q}$ não é um $\mathbb{Z}$-módulo livre.*
3. *Os módulos $\mathbb{Z}_n$ são $\mathbb{Z}$-módulos de torção.*
4. *Se V é um espaço vectorial de dimensão finita sobre K, e $T : V \to V$ é uma transformação linear, então V é um $K[x]$-módulo de torção (exercício).*

A proposição seguinte fornece as propriedades elementares do módulo de torção e é deixada como exercício.

Proposição 6.4.3.

(i) Se $\phi : M_1 \to M_2$ é um homomorfismo de D-módulos, então

$$\phi(\mathrm{Torc}(M_1)) \subset \mathrm{Torc}(M_2).$$

Se ϕ é injectivo, então $\phi(\mathrm{Torc}(M_1)) = \mathrm{Torc}(M_2) \cap \mathrm{Im}(\phi)$. Se ϕ é sobrejectivo com $N(\phi) \subset \mathrm{Torc}(M_1)$, então $\phi(\mathrm{Torc}(M_1)) = \mathrm{Torc}(M_2)$.

(ii) Se M é um D-módulo, então $M/\mathrm{Torc}(M)$ é um D-módulo livre de torção.

(iii) Se $\{M_i\}_{i\in I}$ é uma família de D-módulos, então

$$\mathrm{Torc}(\bigoplus_{i\in I} M_i) = \bigoplus_{i\in I} \mathrm{Torc}(M_i).$$

Seja M um módulo sobre um domínio integral D e designe-se por $K = \mathrm{Frac}(D)$ o corpo das fracções de D. Como K é uma extensão de D, podemos estender o anel dos escalares de M a K, obtendo o espaço vectorial M_K sobre K. Este espaço vectorial reflecte as propriedades de M a menos de torção.

Proposição 6.4.4. *Seja M um D-módulo, $K = \mathrm{Frac}(D)$, e $\phi : M \to M_K$ a aplicação D-linear $\boldsymbol{v} \to 1 \otimes \boldsymbol{v}$. Então:*

(i) Todo o elemento de M_K é da forma $\frac{1}{d}\phi(\boldsymbol{v})$, onde $0 \neq d \in D$ e $\boldsymbol{v} \in M$.

(ii) O núcleo de ϕ é o submódulo de torção $\mathrm{Torc}(M)$.

Demonstração. Para a demonstração de (i), observamos que o módulo M_K é gerado por elementos $k \otimes \boldsymbol{v}$, com $k \in \mathrm{Frac}(D), \boldsymbol{v} \in M$. Logo, se $\boldsymbol{w} \in M_K$, então:

$$\boldsymbol{w} = \sum_{i=1}^{n} k_i \otimes \boldsymbol{v}_i = \sum_{i=1}^{n} \frac{a_i}{b_i} \otimes \boldsymbol{v}_i.$$

Designando por d o produto dos b_i's, existem $c_i \in D$ tais que $\frac{a_i}{b_i} = \frac{c_i}{d}$, logo:

$$\boldsymbol{w} = \frac{1}{d} \otimes \left(\sum_{i=1}^{n} c_i \boldsymbol{v}_i \right) = \frac{1}{d}\phi(\boldsymbol{v}).$$

A demonstração de (ii) é deixada como exercício. □

Ao espaço vectorial M_K sobre $K = \mathrm{Frac}(D)$ chamamos *espaço vectorial associado* ao D-módulo M. Como mostra a proposição anterior, este espaço reflecte as propriedades do módulo a menos de torção, e sugere a seguinte definição:

Definição 6.4.5. Se M é um D-módulo e $S \subset M$, chamamos CARACTERÍSTICA de S à dimensão do subespaço linear de M_K gerado por $\phi(S)$. Em particular, a característica de M é igual à dimensão $\dim M_K$.

Da proposição acima, obtemos:

Corolário 6.4.6. *Um D-módulo de tipo finito tem característica finita.*

Demonstração. Se S é um conjunto gerador finito, então $\phi(S)$ é finito e contém uma base de M_K, logo $\dim M_K < \infty$. Em particular, S tem característica finita. □

Observe-se que a característica dum D-módulo é um invariante: se $M_1 \simeq M_2$, então M_1 e M_2 possuem a mesma característica. O inverso não é obviamente verdadeiro, *i.e.*, a característica não determina um módulo a menos de isomorfismo, e por isso *não é* um invariante completo.

Exemplos 6.4.7.

1. *Como $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}$ a característica de $\mathbb{Q}$, como $\mathbb{Z}$-módulo, é 1. Como $\mathbb{Q}$ não é de tipo finito, o corolário não é verdadeiro na direcção inversa.*

2. *Como $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_n = \{0\}$, a característica de $\mathbb{Z}_n$ é zero.*

3. *Mais geralmente, se M é um D-módulo de torção, então a sua característica é zero.*

Corolário 6.4.8. *Seja M um D-módulo. Então $\{\boldsymbol{e}_i\}_{i\in I} \subset M$ é uma família linearmente independente sobre D sse $\{1 \otimes \boldsymbol{e}_i\}_{i\in I} \subset M_K$ é uma família linearmente independente sobre K.*

Demonstração. Se $\{\boldsymbol{e}_i\}_{i\in I} \subset M$ é uma família linearmente independente, o submódulo $N = \bigoplus_{i\in I} D\boldsymbol{e}_i$ é livre de torção, logo, a restrição de $\phi : M \to M_K$ a N é injectiva. □

Segue-se deste corolário que, se M é um D-módulo livre, então a sua característica é igual à dimensão. Por outro lado, se M é um D-módulo livre, então um submódulo $N \subset M$ não é necessariamente livre (exercício). De facto, temos o seguinte resultado:

Proposição 6.4.9. *Se D é um domínio integral tal que para todo o D-módulo livre M os submódulos $N \subset M$ são livres, então D é um domínio de ideais principais.*

Demonstração. Como $M = D$ é um D-módulo livre se D satisfaz à propriedade do enunciado da proposição, os ideais $I \subset D$ são D-módulos livres. Uma base de I contém um só elemento, pois quaisquer dois elementos $a, b \in I$ são linearmente dependentes:

$$(-b)a + ab = 0.$$

Se $\{d\}$ é uma base de I, então $I = \langle d \rangle$ e I é um ideal principal. □

Na realidade, os domínios de ideais principais (abreviadamente, d.i.p.) são caracterizados pela propriedade expressa na proposição, como mostra o resultado seguinte:

Teorema 6.4.10. *Se D é um d.i.p. e M é um D-módulo livre, então qualquer submódulo $N \subset M$ é livre, e* $\dim N \leq \dim M$.

Demonstração. Seja $\{\boldsymbol{e}_i\}_{i\in I}$ uma base de M sobre D, e $N \subset M$ um submódulo não-trivial. Se $J \subset I$, consideramos um par ordenado $(N_J, \mathcal{B}_{J'})$, onde

$$N_J = N \cap \left(\bigoplus_{j\in J} D\boldsymbol{e}_j \right),$$

e $\mathcal{B}_{J'} = \{\boldsymbol{f}_j\}_{j\in J'}$ é uma base de N_J, com $J' \subset J$. Designamos por $\mathcal{P}$ o conjunto formado por todos os pares ordenados deste tipo. Em $\mathcal{P}$ temos uma relação de ordem parcial definida por

$$(N_{J_1}, \mathcal{B}_{J_1'}) \leq (N_{J_2}, \mathcal{B}_{J_2'}) \quad \Leftrightarrow \quad J_1 \subset J_2 \text{ e } \mathcal{B}_{J_1'} \subset \mathcal{B}_{J_2'}.$$

Vejamos que podemos aplicar o Lema de Zorn a $(\mathcal{P}, \leq)$.

(i) *$\mathcal{P}$ é não-vazio:* Como $N \neq \{0\}$, existe $J_0 = \{j_1, \ldots, j_n\} \subset I$ tal que $N \cap \bigoplus_{i=1}^{n-1} D\boldsymbol{e}_{j_i} = \{0\}$ e $N \cap \bigoplus_{i=1}^{n} D\boldsymbol{e}_{j_i} \neq \{0\}$. O conjunto

$$\{a \in D : a\boldsymbol{e}_{j_n} + \sum_{i=1}^{n-1} b_i \boldsymbol{e}_{j_i} \in N\}$$

é um ideal de D, logo é da forma $\langle d_0 \rangle$. Então existe $\boldsymbol{f}_0 = d_0\boldsymbol{e}_{j_n} + \sum_{i=1}^{n-1} b_{0i}\boldsymbol{e}_{j_i} \in N$. Se $\boldsymbol{v} = a\boldsymbol{e}_{j_n} + \sum_{i=1}^{n-1} b_i\boldsymbol{e}_{j_i} \in N$, temos $a = kd_0$ e

$$\boldsymbol{v} - k\boldsymbol{f}_0 = \sum_{i=1}^{n-1}(b_i - kb_{0i})\boldsymbol{e}_{j_i} \in N \cap \bigoplus_{i=1}^{n-1} D\boldsymbol{e}_{j_i} = \{0\}.$$

Concluímos que $\mathcal{B} = \{\boldsymbol{f}_0\}$ é uma base de $N_{\{J_0\}}$, e $\mathcal{P}$ é não-vazio.

(ii) *Em $(\mathcal{P}, \leq)$, toda a cadeia $\{(N_{J_\alpha}, \mathcal{B}_{J_\alpha'})\}_{\alpha\in A}$ possui um majorante:* Basta tomar o par ordenado $\left(\cup_{\alpha\in A} N_{J_\alpha}, \cup_{\alpha\in A}\mathcal{B}_{J_\alpha'}\right)$.

O Lema de Zorn aplicado a $(\mathcal{P}, \leq)$ fornece então um elemento maximal $(N_{\hat{J}}, \mathcal{B}_{\hat{J}'})$. Para terminar a demonstração, basta mostrar que $\hat{J} = I$, pois neste caso $N_{\hat{J}} = N$, de forma que $\mathcal{B}_{\hat{J}'}$ é uma base para N.

Suponhamos que $I - \hat{J} \neq \emptyset$. Então existe $l \in I - \hat{J}$ e $a \in D$ tal que

$$a\boldsymbol{e}_l + \boldsymbol{v}_a \in N \text{ para algum } \boldsymbol{v}_a \in \bigoplus_{j\in\hat{J}} D\boldsymbol{e}_j. \tag{6.4.1}$$

Os $a \in D$ que satisfazem (6.4.1) formam um ideal, que é necessariamente principal: $a \in \langle d_0 \rangle$. Mostremos que $\mathcal{B}_{\hat{J}'} \cup \{\boldsymbol{f}_0\}$, onde $\boldsymbol{f}_0 = d_0\boldsymbol{e}_l + \boldsymbol{v}_{d_0}$ é uma base para $N_{\hat{J}\cup\{l\}}$. Escrevendo $\mathcal{B}_{\hat{J}'} = \{\boldsymbol{f}_j\}_{j\in\hat{J}'}$ temos:

(a) *$\mathcal{B}_{\hat{J}'} \cup \{\boldsymbol{f}_0\}$ é um conjunto gerador:* De facto, qualquer elemento de $\boldsymbol{v} \in N_{\hat{J}\cup\{l\}}$ é da forma (6.4.1), logo:

$$\begin{aligned}\boldsymbol{v} &= a\boldsymbol{e}_l + \boldsymbol{v}_a \\ &= a'd_0\boldsymbol{e}_l + \boldsymbol{v}_a \\ &= a'\boldsymbol{f}_0 - a'\boldsymbol{v}_{d_0} + \boldsymbol{v}_a, \qquad a' \in D.\end{aligned}$$

Daqui vemos que $-a'\boldsymbol{v}_{d_0} + \boldsymbol{v}_a \in N \cap (\bigoplus_{j\in\hat{J}} D\boldsymbol{e}_j) = N_{\hat{J}}$, donde

$$\boldsymbol{v} = a'\boldsymbol{f}_0 + \sum_{j\in\hat{J}'} a_j\boldsymbol{f}_j,$$

e $\mathcal{B}_{\hat{J}'} \cup \{\boldsymbol{f}_0\}$ é um conjunto gerador.

(b) $\mathcal{B}_{\hat{J}'} \cup \{\boldsymbol{f}_0\}$ *é um conjunto linearmente independente:* formemos a combinação linear

$$\sum_{j\in\hat{J}'} a_j \boldsymbol{f}_j + a\boldsymbol{f}_0 = \sum_{j\in\hat{J}'} a_j \left(\sum_{k\in\hat{J}} c_{jk}\boldsymbol{e}_k\right) + ad_0\boldsymbol{e}_l + a\sum_{k\in\hat{J}} b_k\boldsymbol{e}_k$$
$$= \sum_{k\in\hat{J}} \left(\sum_{j\in\hat{J}'} a_j c_{jk} + ab_k\right)\boldsymbol{e}_j + ad_0\boldsymbol{e}_l.$$

Se esta combinação linear é zero, então $ad_0 = 0$, logo, $a = 0$. Como os $\{\boldsymbol{f}_j\}$ são linearmente independentes, também $a_j = 0$, e os elementos de $\mathcal{B}_{\hat{J}'} \cup \{\boldsymbol{f}_0\}$ são linearmente independentes.

Vemos, pois, que o par $(N_{\hat{J}\cup\{l\}}, \mathcal{B}_{\hat{J}'\cup\{l\}})$ contradiz a maximalidade de $(N_{\hat{J}}, \mathcal{B}_{\hat{J}'})$. Logo, $I = \hat{J}$, como era pretendido. □

Estudaremos na próxima secção a estrutura dos módulos de tipo finito sobre d.i.p.'s.

Exercícios.

1. Demonstre a Proposição 6.4.3.

2. Mostre que, se M é um D-módulo livre sobre um domínio integral D, então M é livre de torção. Dê um exemplo de um módulo livre N sobre um anel A tal que $\mathrm{Torc}(N) \neq 0$.

3. Seja V um espaço vectorial de dimensão finita sobre K, e $T : V \to V$ uma transformação linear. Mostre que V é um $K[x]$-módulo de torção.

4. Seja D um domínio integral, e $K = \mathrm{Frac}(D)$, visto como um D-módulo. Em $D - \{0\}$ considere a relação de ordem parcial definida por

$$d_1 \leq d_2 \Longleftrightarrow K_{d_1} \subset K_{d_2},$$

onde $K_d \subset K$ é o D-submódulo $\{\frac{a}{d} : a \in D\}$.

   (a) Mostre que $K = \varinjlim K_d$.

   (b) Se M é um D-módulo e M_K é o espaço vectorial associado, mostre que $M_K = \varinjlim(K_d \otimes M)$.

   (c) Conclua que $1 \otimes \boldsymbol{v} \in M_K$ é o vector nulo sse $\boldsymbol{v} \in \mathrm{Torc}(M)$.

5. Dê um exemplo de um módulo livre que possui submódulos que não são livres.

6.5 Módulos de Tipo Finito sobre d.i.p.

Nesta secção damos uma classificação completa dos módulos de tipo finito sobre d.i.p. Como veremos, esta classificação tem várias aplicações importantes no estudo das transformações lineares de um espaço vectorial e na classificação de grupos abelianos.

Começamos por mostrar que, para esta classe de módulos que estamos a estudar, "livre" e "livre de torção" são conceitos equivalentes (já sabemos que, para um domínio integral, "livre" implica "livre de torção")

Proposição 6.5.1. *Seja M um módulo de tipo finito sobre um d.i.p. D. Se* $\operatorname{Torc}(M) = 0$*, então M é livre.*

Demonstração. Seja S um conjunto gerador finito. Em S escolhemos um conjunto $\mathcal{B} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ maximal linearmente independente. Para mostrar que $\mathcal{B}$ é uma base de M, basta, pois, mostrar que $\mathcal{B}$ gera S. Se $\boldsymbol{v} \in S$, existem $a_{\boldsymbol{v}}, a_1, \ldots, a_n \in D$ tais que

$$a_{\boldsymbol{v}}\boldsymbol{v} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n \qquad (a_{\boldsymbol{v}} \neq 0).$$

Como M é livre de torção, se $a \equiv \prod_{\boldsymbol{v}\in S} a_{\boldsymbol{v}}$, a aplicação $\boldsymbol{w} \overset{\phi}{\longmapsto} a\boldsymbol{w}$ define um monomorfismo $\phi : M \to M$. Por outro lado, $\phi(M) \subset \bigoplus_{i=1}^{n} D\boldsymbol{v}_i$, pois se $\boldsymbol{w} \in S$, então

$$\begin{aligned} a\boldsymbol{w} &= \left(\prod_{\boldsymbol{w}\neq\boldsymbol{v}\in S} a_{\boldsymbol{v}}\right) a_{\boldsymbol{w}}\boldsymbol{w} \\ &= \left(\prod_{\boldsymbol{w}\neq\boldsymbol{v}\in S} a_{\boldsymbol{v}}\right) (a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n) \in \bigoplus_{i=1}^{n} D\boldsymbol{v}_i. \end{aligned}$$

Logo M é isomorfo a um submódulo de um módulo livre, e portanto (Teorema 6.4.10) é livre. □

A classificação de módulos de tipo finito sobre d.i.p. baseia-se no seguinte resultado que fornece uma decomposição numa soma de um factor livre com um factor de torção.

Teorema 6.5.2. *Seja M um módulo de tipo finito sobre um d.i.p. D. Então* $M = \operatorname{Torc}(M) \oplus L$*, onde L é um módulo livre com dimensão igual à característica de M.*

Demonstração. O módulo $M/\operatorname{Torc}(M)$ é livre de torção e de tipo finito. Pela proposição anterior, este quociente é um módulo livre, logo, existem elementos $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n \in M$, linearmente independentes, tais que

$$M/\operatorname{Torc}(M) = \bigoplus_{i=1}^{n} D\pi(\boldsymbol{e}_i),$$

onde $\pi : M \to M/\operatorname{Torc}(M)$ é a projecção canónica. Seja $L = \bigoplus_{i=1}^{n} D\boldsymbol{e}_i$. Então:

(a) $L \cap \operatorname{Torc}(M) = \{0\}$: Se $\boldsymbol{v} \in L \cap \operatorname{Torc}(M)$ existem escalares $d, d_1, \ldots, d_n \in D$ $(d \neq 0)$ tais que

$$d\boldsymbol{v} = 0, \qquad \boldsymbol{v} = \sum_{i=1}^{n} d_i \boldsymbol{e}_i,$$

logo, $(dd_1)\boldsymbol{e}_1 + \cdots + (dd_n)\boldsymbol{e}_n = 0$ e concluímos que $dd_1 = \cdots = dd_n = 0$. Pela lei do corte, $d_1 = \cdots = d_n = 0$, e portanto $\boldsymbol{v} = 0$.

(b) $M = L + \operatorname{Torc}(M)$: Se $\boldsymbol{v} \in M$ defina-se $d_1, \ldots, d_n \in D$ pela fórmula

$$\pi(\boldsymbol{v}) = \sum_{i=1}^{n} d_i \pi(\boldsymbol{e}_i).$$

Então $\boldsymbol{v} = \boldsymbol{v}_T + \boldsymbol{v}_L$, onde $\boldsymbol{v}_L = \sum_{i=1}^{n} d_i \boldsymbol{e}_i \in L$ e $\boldsymbol{v}_T = \boldsymbol{v} - \boldsymbol{v}_L \in N(\pi) = \operatorname{Torc}(M)$.

Por (a) e (b), vemos que $M = \operatorname{Torc}(M) \oplus L$. Assim, se $K = \operatorname{Frac}(D)$ e $\phi : M \to M_K$ é o homomorfismo canónico, a restrição de ϕ a L é injectiva. Como $\phi(L)$ gera M_K, a característica de M é igual à dimensão de L. □

O factor livre de torção L, na decomposição acima, não é único, pois depende da escolha de uma base, mas a sua dimensão (a característica de M) é um invariante da decomposição, *i.e.* , se $M = \operatorname{Torc}(M) \oplus L_1 = \operatorname{Torc}(M) \oplus L_2$ então $\dim L_1 = \dim L_2$.

A característica de M classifica, a menos de isomorfismo, a parte livre de M. Para classificar os módulos de tipo finito sobre um d.i.p. D, falta pois classificar os módulos de torção, em que o factor livre $L = 0$. Os próximos parágrafos discutem esta classificação.

6.5.1 Diagonalização de matrizes com entradas num d.i.p.

Designamos por $M_n(D)$ o anel das matrizes $n \times n$ com entradas num domínio de ideais principais D. O seguinte resultado será utilizado mais tarde para distinguir certas bases dum módulo livre.

Proposição 6.5.3. *Seja $A \in M_n(D)$. Existem matrizes invertíveis $P, Q \in M_n(D)$ tais que*

$$Q^{-1}AP = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix},$$

onde $d_1 \mid d_2 \mid \cdots \mid d_n$. Os $d_1, \ldots, d_n$ são únicos a menos de multiplicação por unidades.

Este resultado *não* diz que que uma matriz pode ser diagonalizada com uma mudança de base. Em particular, as matrizes P e Q *não são*, em geral, inversas uma da outra.

A forma normal para uma matriz dada pela Proposição 6.5.3 pode ser obtida através de operações elementares nas linhas e colunas da matriz. Para isso introduzimos as matrizes E_{ij} cujas entradas são todas zero, à excepção, da entrada (i, j) que é 1. A multiplicação à direita (esquerda) pelas seguintes matrizes invertíveis permite efectuar as operações elementares usuais:

- trocas de colunas (linhas): $P_{ij} = I - E_{ii} - E_{jj} + E_{ij} + E_{ji}$;
- multiplicação de colunas (linhas) por unidades: $D_i(u) = I + (u-1)E_{ii}$ ($u \in D$ uma unidade);
- soma de múltiplo de coluna (linha) a outra coluna (linha): $T_{ij}(a) = I + aE_{ij}$ ($a \in D$).

Definimos, ainda, o *comprimento* $\delta(d)$ de um elemento $d \in D$ não-nulo como sendo o número de factores primos que ocorrem na factorização de d.

Seja então $A = (a_{ij})$ uma matriz arbitrária $(n \times n)$. Queremos ver que A é equivalente[10] a uma matriz diagonal. Se $A = 0$, não há nada a mostrar. Caso contrário, alguma entrada é não-nula de comprimento mínimo, e podemos, com operações elementares, transportá-la para a posição $(1, 1)$. Seja a_{1k} uma entrada tal que $a_{11} \nmid a_{1k}$. Trocando as colunas 2 e k, podemos supor que esta entrada é a_{12}. Se $d = \text{mdc}(a_{11}, a_{12})$, existem elementos $p, q \in D$ tais que $pa_{11} + qa_{12} = d$. Se $r = a_{12}d^{-1}$ e $s = a_{11}d^{-1}$, vemos que as matrizes

$$P = \begin{pmatrix} p & r & & & \\ q & -s & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \qquad P^{-1} = \begin{pmatrix} s & r & & & \\ q & -p & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix},$$

são inversas uma da outra. Multiplicando $A = (a_{ij})$ à direita pela matriz P fornece uma matriz equivalente cuja primeira linha é $(d, 0, a_{13}, \ldots, a_{1n})$ e $\delta(d) < \delta(a_{11})$. Da mesma forma, se $a_{11} \nmid a_{k1}$, um processo semelhante fornece um novo elemento d cujo comprimento é $\delta(d) < \delta(a_{11})$, e obtemos uma matriz equivalente em que o δ mínimo foi reduzido. Como δ toma valores em $\mathbb{N}$, repetindo este processo um número finito de vezes, obtemos uma matriz em que $a_{11} \mid a_{1k}$ e $a_{11} \mid a_{k1}$, para todo o k. Utilizando operações

[10] Na discussão que se segue diremos que duas matrizes A e B são equivalentes se existirem matrizes invertíveis P e Q tais que $B = PAQ$.

elementares, obtemos uma matriz equivalente à matriz original, da forma

$$\begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & \hat{a}_{22} & \dots & \hat{a}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \hat{a}_{n2} & \dots & \hat{a}_{nn} \end{pmatrix}.$$

Continuando este processo para a segunda linha e a segunda coluna, etc., vemos que a matriz original é equivalente a uma matriz diagonal:

$$\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}.$$

Agora, se $d_1 \nmid d_2$, então adicionamos a segunda linha à primeira linha e repetimos todo o processo novamente. Eventualmente, obtemos uma matriz diagonal em que $d_1 \mid d_2$ (o comprimento $\delta(d_1)$ diminui sempre!). Procedendo desta forma, podemos produzir uma matriz diagonal em que $d_1 \mid d_2 \mid \cdots \mid d_n$, tal como se pretendia.

Os elementos $d_1, \dots, d_n$ na forma normal dada pela Proposição 6.5.3 chamam-se FACTORES INVARIANTES. A unicidade dos factores invariantes decorre do seguinte resultado que ao mesmo tempo fornece um método de cálculo destes factores mais eficaz que "eliminação". A sua demonstração é deixada como exercício.

Lema 6.5.4. *Seja $A \in M_n(D)$ e suponha-se que A é equivalente a uma matriz diagonal*

$$\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix},$$

com $d_1 \mid d_2 \mid \cdots \mid d_n$. Se a característica de A é r, então $d_i = 0$, para $i > r$, e $d_i = \frac{\Delta_i}{\Delta_{i-1}}$, para $i \leq r$, onde $\Delta_0 = 1$ e Δ_i é um maior divisor comum dos menores de dimensão i da matriz A.

Das fórmulas dadas no lema anterior resulta imediatamente o seguinte corolário.

Corolário 6.5.5. *Os factores invariantes são únicos a menos de multiplicação por unidades. Duas matrizes são equivalentes sse possuem os mesmos factores invariantes.*

Exemplo 6.5.6.

Seja $D = \mathbb{C}[x]$ e consideremos a matriz

$$A = \begin{pmatrix} x-2 & 0 & 0 \\ -1 & x & -1 \\ -2 & 4 & x-4 \end{pmatrix}.$$

Calculando os menores, obtemos

$$\begin{aligned}\Delta_1 &= 1,\\ \Delta_2 &= x-2,\\ \Delta_3 &= (x-2)^3,\end{aligned}$$

logo $d_1 = 1$, $d_2 = (x-2)$ *e* $d_3 = (x-2)^2$. *De facto, se usarmos o método de eliminação, podemos verificar que existem matrizes invertíveis tais que:*

$$\begin{pmatrix} 0 & -1 & 0 \\ -1 & -x+2 & 0 \\ 1 & x-4 & 1 \end{pmatrix} \begin{pmatrix} x-2 & 0 & 0 \\ -1 & x & -1 \\ -2 & 4 & x-4 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & x \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & (x-2)^2 \end{pmatrix}.$$

6.5.2 Decomposição em factores cíclicos invariantes

Se M é um módulo sobre um d.i.p. D, e $\boldsymbol{v} \in M$, chama-se IDEAL DE ORDEM de $\boldsymbol{v}$ ao ideal $\operatorname{ann} \boldsymbol{v} \equiv \{d \in D : d\boldsymbol{v} = 0\}$. Este ideal, sendo principal, toma a forma $\operatorname{ann} \boldsymbol{v} = \langle a \rangle$, e ao elemento $a \in D$ chama-se ORDEM de $\boldsymbol{v}$ (definida a menos de unidades). É claro que o submódulo cíclico $\langle \boldsymbol{v} \rangle$ é isomorfo a $D/\operatorname{ann} \boldsymbol{v}$.

Exemplo 6.5.7.

Seja G um grupo abeliano, que vemos como um $\mathbb{Z}$-módulo. Se $g \in G$, então o subgrupo cíclico $\langle g \rangle$ gerado por g é isomorfo a $\mathbb{Z}/\operatorname{ann} g$. A ordem de g, tal como definida acima, coincide com a noção usual de ordem a menos de um sinal (as unidades neste caso são ± 1).

A primeira classificação dum módulo de tipo finito sobre um d.i.p. D que fornecemos é a seguinte decomposição de um D-módulo em factores cíclicos:

Teorema 6.5.8 (Decomposição em factores cíclicos invariantes). *Seja M um módulo de tipo finito sobre um d.i.p. D. Então*

$$M = \langle \boldsymbol{v}_1 \rangle \oplus \cdots \oplus \langle \boldsymbol{v}_k \rangle,$$

onde $\operatorname{ann} \boldsymbol{v}_1 \supset \operatorname{ann} \boldsymbol{v}_2 \supset \cdots \supset \operatorname{ann} \boldsymbol{v}_k$. *Escrevendo* $\operatorname{ann} \boldsymbol{v}_i = \langle d_i \rangle$, *temos um isomorfismo*

$$M \simeq D/\langle d_1 \rangle \oplus \cdots \oplus D/\langle d_k \rangle$$

onde $d_1 \mid d_2 \mid \cdots \mid d_k$. *Os ideais* $\langle d_1 \rangle, \ldots, \langle d_k \rangle$ *são determinados unicamente por M.*

Demonstração. Se a característica de M é r, então

$$M \simeq \mathrm{Torc}(M) \oplus \underbrace{D \oplus \cdots \oplus D}_{r \text{ termos}},$$

logo, basta demonstrar o resultado para módulos de torção M.

Seja $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$ um conjunto finito de geradores de M. Designe-se por L o módulo livre gerado pelos $\boldsymbol{w}_i$'s. Em L existe uma base $\{\hat{\boldsymbol{w}}_1, \ldots, \hat{\boldsymbol{w}}_n\}$ tal que $\pi(\hat{\boldsymbol{w}}_i) = \boldsymbol{w}_i$, onde $\pi : L \to M$ é a projecção canónica. Seja N o núcleo de π, de forma que $M \simeq L/N$. Então N é um submódulo livre de L e, como M é de torção, $\dim N = \dim L = n$. Seja $\{\hat{\boldsymbol{v}}_1, \ldots, \hat{\boldsymbol{v}}_n\}$ uma base de N, de forma que existem escalares $a_{ij} \in D$ satisfazendo às relações

$$\hat{\boldsymbol{v}}_i = \sum_j a_{ji} \hat{\boldsymbol{w}}_j, \qquad i = 1, \ldots, n.$$

Mudando de bases em L e N,

$$\hat{\boldsymbol{w}}'_i = \sum_j q_{ji} \hat{\boldsymbol{w}}_j, \qquad \hat{\boldsymbol{v}}'_i = \sum_j p_{ji} \hat{\boldsymbol{v}}_j,$$

obtemos novas relações

$$\hat{\boldsymbol{v}}'_i = \sum_j b_{ji} \hat{\boldsymbol{w}}'_j, \qquad i = 1, \ldots, n,$$

e é simples verificar que as matrizes $A = (a_{ij}), B = (b_{ij}), P = (p_{ij})$ e $Q = (q_{ij})$ estão relacionadas por

$$B = Q^{-1} A P.$$

Como vimos acima, podemos escolher as matrizes invertíveis P e Q (*i.e.*, as bases de L e N) tais que $B = \mathrm{diag}(d_1, \ldots, d_n)$ com $d_1 \mid d_2 \mid \cdots \mid d_n$. Nesse caso:

$$\hat{\boldsymbol{v}}'_i = d_i \hat{\boldsymbol{w}}'_i, \qquad i = 1, \ldots n.$$

Se $\boldsymbol{w}'_i = \pi(\hat{\boldsymbol{w}}'_i)$, mostramos que

$$M = \langle \boldsymbol{w}'_1 \rangle \oplus \cdots \oplus \langle \boldsymbol{w}'_n \rangle.$$

Como $\mathrm{ann}\, \boldsymbol{w}'_i = \langle d_i \rangle$, isto terminará a demonstração da proposição.

É claro que $M = \sum_i \langle \boldsymbol{w}'_i \rangle$, pois os $\hat{\boldsymbol{w}}'_i$ formam um conjunto gerador de L, e $\pi : L \to M$ é sobrejectiva. Logo, basta mostrar que $\langle \boldsymbol{w}'_k \rangle \cap \sum_{i \neq k} \langle \boldsymbol{w}'_i \rangle = \{0\}$. Seja $\boldsymbol{w}$ um elemento desta intersecção. Então, existem $a_i \in D$ tais que

$$\boldsymbol{w} = a_k \boldsymbol{w}'_k = \sum_{i \neq k} a_i \boldsymbol{w}'_i.$$

Logo, em L, obtemos

$$a_k\hat{\boldsymbol{w}}'_k - \sum_{i\neq k} a_i\hat{\boldsymbol{w}}'_i \in N$$

e concluímos que existem $b_i \in D$ tais que $a_i = b_i d_i$, $i = 1, \ldots, n$. Mas então $\boldsymbol{w} = a_k\boldsymbol{w}'_k = \pi(a_k\hat{\boldsymbol{w}}'_k) = \pi(b_k d_k\hat{\boldsymbol{w}}'_k) = \pi(b_k\hat{\boldsymbol{v}}'_k) = 0$, como era pretendido.

A demonstração da unicidade será dada mais adiante. □

Os ideais $\langle d_i\rangle$ da decomposição que acabamos de estudar chamam-se FACTORES INVARIANTES do módulo M.

Corolário 6.5.9. *Dois módulos de tipo finito sobre um d.i.p. são isomorfos sse possuem os mesmos factores invariantes.*

6.5.3 Decomposição em factores cíclicos primários

Vamos agora dar uma classificação alternativa de módulos sobre d.i.p. Esta classificação baseia-se na factorização dos elementos de D em factores primos.

Recordemos que, se $0 \neq a \in D$, então a pode ser escrito na forma

$$a = u \cdot p_1 \cdots p_n,$$

onde $u \in D$ é uma unidade e os $p_i \in D$ são primos. Esta decomposição é única a menos da ordem dos factores e de multiplicação por unidades. Se $a, b \in D$ diferem por multiplicação por uma unidade, escrevemos $a \sim b$.

Lema 6.5.10. *Seja M um módulo sobre um d.i.p. D.*

(i) Se $M = D/\langle ab\rangle$ com $\mathrm{mdc}(a,b) = 1$, *então $M \simeq D/\langle a\rangle \oplus D/\langle b\rangle$.*

(ii) Se $M = D/\langle a\rangle + D/\langle b\rangle$ com $\mathrm{mdc}(a,b) = 1$, *então $M \simeq D/\langle ab\rangle$.*

Demonstração.

(i) Seja $M = \langle \boldsymbol{v}\rangle$ com $\operatorname{ann}\boldsymbol{v} = \langle ab\rangle$ e sejam $\boldsymbol{v}_1 = b\boldsymbol{v}$ e $\boldsymbol{v}_2 = a\boldsymbol{v}$ (onde $\mathrm{mdc}(a,b) = 1$). Então $\operatorname{ann}\boldsymbol{v}_1 = \langle a\rangle$ e $\operatorname{ann}\boldsymbol{v}_2 = \langle b\rangle$, e existem $r, s \in D$ tais que $ra + sb = 1$. Assim vemos que $\boldsymbol{v} = s\boldsymbol{v}_1 + r\boldsymbol{v}_2 \in \langle \boldsymbol{v}_1\rangle + \langle \boldsymbol{v}_2\rangle$, e por outro lado, se $\boldsymbol{w} \in \langle \boldsymbol{v}_1\rangle \cap \langle \boldsymbol{v}_2\rangle$, então $a\boldsymbol{w} = b\boldsymbol{w} = 0$, logo, $\boldsymbol{w} = (ra + sb)\boldsymbol{w} = 0$. Concluímos que $M = \langle \boldsymbol{v}_1\rangle \oplus \langle \boldsymbol{v}_2\rangle \simeq D/\langle a\rangle \oplus D/\langle b\rangle$.

(ii) Sejam $\boldsymbol{v}_1, \boldsymbol{v}_2 \in M$ com $\operatorname{ann}\boldsymbol{v}_1 = \langle a\rangle$ e $\operatorname{ann}\boldsymbol{v}_2 = \langle b\rangle$ e $\mathrm{mdc}(a,b) = 1$. Então, como em (i), existem $r, s \in D$ tais que $ra+sb = 1$ e, se $\boldsymbol{w} \in \langle \boldsymbol{v}_1\rangle \cap \langle \boldsymbol{v}_2\rangle$, temos $\boldsymbol{w} = (ra + sb)\boldsymbol{w} = 0$. Logo, $M = \langle \boldsymbol{v}_1\rangle \oplus \langle \boldsymbol{v}_2\rangle$. Agora, se $\boldsymbol{w} = \boldsymbol{v}_1 + \boldsymbol{v}_2$, vemos que $\operatorname{ann}\boldsymbol{w} = \langle ab\rangle$ e, por outro lado,

$$\boldsymbol{v}_1 = (ra + sb)\boldsymbol{v}_1 = sb\boldsymbol{w}, \qquad \boldsymbol{v}_2 = (ra + sb)\boldsymbol{v}_2 = ra\boldsymbol{w}.$$

Concluímos que $M = \langle \boldsymbol{w}\rangle \simeq D/\langle ab\rangle$. □

Usando este lema podemos então mostrar:

Teorema 6.5.11 (Decomposição em factores cíclicos primários). *Seja M um módulo de tipo finito sobre um d.i.p. D. Então*

$$M = L \oplus \langle \boldsymbol{w}_1 \rangle \oplus \cdots \oplus \langle \boldsymbol{w}_n \rangle \simeq L \oplus D/\langle {p_1}^{m_1} \rangle \oplus \cdots \oplus D/\langle {p_n}^{m_n} \rangle,$$

onde L é um submódulo livre de dimensão igual à característica de M, $\operatorname{ann} \boldsymbol{w}_i = \langle {p_i}^{m_i} \rangle$*, e os elementos $p_1, \ldots, p_n \in D$ são primos. Os ideais $\langle {p_1}^{m_1} \rangle, \ldots, \langle {p_n}^{m_n} \rangle$ são determinados unicamente (a menos da ordem) por M.*

Demonstração. Seja

$$M = \langle \boldsymbol{v}_1 \rangle \oplus \cdots \oplus \langle \boldsymbol{v}_k \rangle$$

a decomposição de M em factores cíclicos invariantes. Se $\operatorname{ann} \boldsymbol{v}_i = \langle d_i \rangle$, então $d_1 \mid d_2 \mid \cdots \mid d_k$ e $d_{k-r+1} = \cdots = d_k = 0$, onde r é a característica de M. Temos, pois, que

$$\langle \boldsymbol{v}_{k-r+1} \rangle \oplus \cdots \oplus \langle \boldsymbol{v}_k \rangle = L,$$

com L livre de dimensão r. Por outro lado, se ${p_1}^{m_1}, \ldots, {p_n}^{m_n}$ são as potências primas que entram nas decomposições primas dos $d_1, \ldots, d_{k-r}$, o lema acima mostra que

$$\langle \boldsymbol{v}_1 \rangle \oplus \cdots \oplus \langle \boldsymbol{v}_k \rangle \simeq D/\langle {p_1}^{m_1} \rangle \oplus \cdots \oplus D/\langle {p_n}^{m_n} \rangle \oplus L.$$

A unicidade será demonstrada mais adiante. □

Aos ideais $\langle {p_1}^{m_1} \rangle, \ldots, \langle {p_n}^{m_n} \rangle$ associados ao módulo M chama-se DIVISORES ELEMENTARES de M. Os divisores elementares em conjunto com a característica formam uma lista completa de invariantes.

Corolário 6.5.12. *Dois módulos de tipo finito sobre um d.i.p. são isomorfos sse possuem a mesma lista de divisores elementares e a mesma característica.*

Vimos na demonstração acima que a decomposição de M em factores cíclicos invariantes determina univocamente uma decomposição de M em factores cíclicos primários.

Inversamente, seja

$$M \simeq L \oplus D/\langle {p_1}^{m_1} \rangle \oplus \cdots \oplus D/\langle {p_n}^{m_n} \rangle$$

a decomposição de M em factores cíclicos primários. Sejam $p_1, \ldots, p_s$ os primos distintos (*i.e.*, não-associados) que aparecem nesta decomposição. Ordenamos as potências primas, que aparecem na decomposição, da seguinte forma:

$$\begin{array}{cccc} {p_1}^{n_{11}} & {p_2}^{n_{12}} & \cdots & {p_s}^{n_{1s}} \\ {p_1}^{n_{21}} & {p_2}^{n_{22}} & \cdots & {p_s}^{n_{2s}} \\ \vdots & \vdots & & \vdots \\ {p_1}^{n_{t1}} & {p_2}^{n_{t2}} & \cdots & {p_s}^{n_{ts}}, \end{array} \tag{6.5.1}$$

onde $n_{1i} \leq n_{2i} \leq \cdots \leq n_{ti}$, $i = 1, \ldots, s$ (possivelmente há necessidade de acrescentar factores $1 = {p_i}^0$). Tomamos para d_j o produto das potências primas que aparecem na linha j, *i.e.*, $d_j \equiv {p_1}^{n_{j1}} \cdot {p_2}^{n_{j2}} \cdots {p_s}^{n_{js}}$. Então vemos que $d_1 \mid d_2 \mid \cdots \mid d_t$, e como as potências primas que aparecem em cada d_j são relativamente primas, o lema precedente fornece um isomorfismo

$$\mathrm{Torc}(M) \simeq D/\langle d_1 \rangle \oplus \cdots \oplus D/\langle d_t \rangle.$$

Se a dimensão da parte livre L é r, então acrescentamos à lista dos d_j's os elementos $d_{t+1} = \cdots = d_{t+r} = 0$, obtendo-se então a decomposição de M em factores cíclicos invariantes.

Dada a lista dos $\{{p_i}^{n_{ji}}\}$, os d_k ficam determinados (a menos de unidades), como acabamos de ver. Inversamente, dada a lista dos $\{d_k\}$, os $\{{p_i}^{n_{ji}}\}$ são as potências primas na decomposição dos d_k's. Logo, a unicidade dos ideais $\langle d_1 \rangle, \ldots, \langle d_k \rangle$ segue-se da unicidade dos ideais $\langle {p_1}^{m_1} \rangle, \ldots, \langle {p_n}^{m_n} \rangle$.

6.5.4 Componentes primárias

Se M é um D-módulo e $p \in D$ é um primo, a COMPONENTE p-PRIMÁRIA de M é o submódulo

$$M(p) = \{\boldsymbol{v} \in M : p^k \boldsymbol{v} = 0, \text{ para algum } k \in \mathbb{N}\}.$$

Deixamos como exercício verificar que, se $\mathrm{Torc}(M) = M$, então

$$M = \bigoplus_{p \text{ primo}} M(p).$$

Como M é de tipo finito, apenas um número finito de termos não é zero.

Podemos utilizar as componentes primárias para demonstrar a unicidade das decomposições. Se

$$\begin{aligned} M &\simeq L \oplus D/\langle {p_1}^{m_1} \rangle \oplus \cdots \oplus D/\langle {p_s}^{m_s} \rangle \\ &\simeq L \oplus D/\langle \tilde{p}_1^{n_1} \rangle \oplus \cdots \oplus D/\langle \tilde{p}_t^{n_t} \rangle, \end{aligned}$$

são duas decomposições de M em factores cíclicos primários, vemos que

$$\begin{aligned} M(p) &\simeq \bigoplus_{\{p_i:\ p_i \sim p\}} D/\langle {p_i}^{m_i} \rangle \\ &\simeq \bigoplus_{\{\tilde{p}_i : \tilde{p}_i \sim p\}} D/\langle \tilde{p}_i^{m_i} \rangle. \end{aligned}$$

Logo nas duas decomposições acima podemos assumir que a lista de primos é a mesma, e basta demonstrar a unicidade das decomposições para o caso $M = M(p)$. Sejam então

$$\begin{aligned} M(p) &\simeq D/\langle p^{m_1} \rangle \oplus \cdots \oplus D/\langle p^{m_s} \rangle \\ &\simeq D/\langle p^{n_1} \rangle \oplus \cdots \oplus D/\langle p^{n_t} \rangle \end{aligned}$$

duas decomposições de $M(p)$. Ordenemos os termos das decomposições, de forma que $m_1 \leq m_2 \leq \cdots \leq m_s$ e $n_1 \leq n_2 \leq \cdots \leq n_t$. Se $\boldsymbol{v}_s \in M$ é tal que $\operatorname{ann} \boldsymbol{v}_s = \langle p^{m_s} \rangle$, então a segunda decomposição mostra que $p^{n_t} \boldsymbol{v}_s = 0$, logo $n_t \geq m_s$. De igual forma, vemos que $m_s \geq n_t$, logo $m_s = n_s$. O módulo quociente $M(p)/\langle \boldsymbol{v}_s \rangle$ admite as decomposições

$$\begin{aligned} M(p)/\langle \boldsymbol{v}_s \rangle &\simeq D/\langle p^{m_1} \rangle \oplus \cdots \oplus D/\langle p^{m_{s-1}} \rangle \\ &\simeq D/\langle p^{n_1} \rangle \oplus \cdots \oplus D/\langle p^{n_{t-1}} \rangle \end{aligned}$$

Por exaustão, concluímos que $m_i = n_i$ e $s = t$, como era pretendido.

Exercícios.

1. Demonstre as fórmulas para os factores invariantes dadas no Lema 6.5.4.

2. Determine matrizes diagonais equivalentes às matrizes

   (a) $\begin{pmatrix} 36 & 12 \\ 16 & 18 \end{pmatrix}$ sobre $\mathbb{Z}$;

   (b) $\begin{pmatrix} x-1 & -2 & -1 \\ 0 & x & 1 \\ 0 & -2 & x-3 \end{pmatrix}$ sobre $\mathbb{R}[x]$.

3. Mostre que, se p é um primo, as seguintes duas matrizes de $M_n(\mathbb{Z}_p)$ são equivalentes:

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & \ddots & & \\ 0 & 0 & & \cdots & 1 \\ 1 & 0 & & \cdots & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ & & \ddots & & \\ 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & & 1 \end{pmatrix}.$$

4. Mostre que $M = \bigoplus_{p \text{ primo}} M(p)$ se $\operatorname{Torc} M = M$.

5. Se $M = D/\langle p_1 {p_2}^2 {p_3} \rangle \oplus D/\langle p_1 {p_2}^3 {p_3}^2 p_4 \rangle \oplus D/\langle {p_1}^3 {p_2}^2 {p_4}^5 \rangle$ é um módulo sobre um d.i.p. D, determine as decomposições de M em factores cíclicos invariantes e em factores cíclicos primários.

6. Sejam M_1 e M_2 D-módulos de tipo finito.

   (a) Mostre que, se M_1 e M_2 são cíclicos, então $M_1 \otimes M_2$ é cíclico.

   (b) Determine a decomposição de $M_1 \otimes M_2$ em factores cíclicos invariantes e primários em termos das decomposições de M_1 e M_2.

7. Sejam M_1 e M_2 D-módulos cíclicos de ordens a e b, respectivamente. Mostre que, se $\operatorname{mdc}(a, b) \neq 1$, então os factores invariantes de $M_1 \oplus M_2$ são $\operatorname{mdc}(a, b)$ e $\operatorname{mmc}(a, b)$.

6.6 Classificações: Grupos Abelianos e Formas Canónicas de Matrizes

Nesta secção usamos a classificação de módulos de tipo finito sobre d.i.p. para classificar os grupos abelianos de tipo finito e demonstrar a existência da forma canónica de Jordan de uma matriz. Estes correspondem respectivamente, a tomar $D = \mathbb{Z}$ e $D = K[x]$ (K um corpo algebricamente fechado) nos teoremas de classificação da secção anterior. Se $D = \mathbb{Z}$, todo o ideal possui como gerador único um inteiro não-negativo. Se $D = K[x]$, todo o ideal possui um polinómio mónico como gerador único. É, pois, natural substituir os ideais factores invariantes e os ideais divisores elementares por estes geradores, que também se designam por factores invariantes e divisores elementares.

6.6.1 Classificação de grupos abelianos de tipo finito

Seja G um grupo. Dizemos que G é de *tipo finito* se existem elementos $g_1, \ldots, g_m \in G$ tais que

$$\forall g \in G, \exists n_1, \ldots, n_m \in \mathbb{Z} : \quad g = {g_1}^{n_1} \cdots {g_m}^{n_m}.$$

Se G é um grupo abeliano, então G é de tipo finito sse G é um $\mathbb{Z}$-módulo de tipo finito. Como $\mathbb{Z}$ é um d.i.p., os teoremas de classificação da secção anterior fornecem imediatamente o seguinte resultado:

Teorema 6.6.1 (Classificação de grupos abelianos de tipo finito). *Seja G um grupo abeliano de tipo finito. Então*

$$G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_n},$$

onde $d_1, \ldots, d_n$ são naturais definidos univocamente pela condição $d_1 \mid d_2 \mid \cdots \mid d_n$. Se ${p_1}^{n_1}, \ldots, {p_s}^{n_s}$ são as potências primas na decomposição dos $d_1, \ldots, d_n$ em factores primos, então

$$G \simeq \mathbb{Z}_{{p_1}^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{{p_s}^{n_s}} \oplus \mathbb{Z}^r,$$

*onde r é o número de naturais $d_i = 0$ (*i.e.*, a característica de G).*

Os naturais d_i (respectivamente ${p_i}^{n_i}$) chamam-se *factores invariantes* (respectivamente *divisores elementares*) de G. São invariantes que determinam o grupo abeliano a menos de isomorfismo. Observe-se que podemos calcular uma lista de invariantes, uma vez conhecida a outra.

Exemplos 6.6.2.

1. *Se $n \in \mathbb{N}$ admite a factorização prima $n = {p_1}^{n_1} \cdots {p_s}^{n_s}$, então*

$$\mathbb{Z}_n \simeq \mathbb{Z}_{{p_1}^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{{p_s}^{n_s}}.$$

Existe apenas o factor invariante n, e os divisores elementares são os ${p_i}^{n_i}$.

2. Seja $G = \mathbb{Z}_6 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{18}$. Então a decomposição de G em factores cíclicos primários é

$$G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2}$$

logo, os divisores elementares são $\{2, 2, 3, 3, 3^2, 5\}$. Obtemos os factores invariantes a partir da Tabela 6.5.1, que neste caso é

$$\begin{array}{lll} 2^0 & 3 & 5^0 \\ 2 & 3 & 5^0 \\ 2 & 3^2 & 5. \end{array}$$

Os factores invariantes são os produtos das potências que aparecem em cada linha da tabela: $d_1 = 3$, $d_2 = 6$, $d_3 = 90$. Logo, a decomposição de G em factores invariantes é:

$$G \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{90}$$

6.6.2 Forma canónica de Jordan

Nesta subsecção, K designa um corpo algebricamente fechado. Seja V um espaço vectorial de dimensão finita sobre K, e $T : V \to V$ uma transformação linear. Estamos interessados em estudar T dum ponto de vista estrutural. Para isso utilizamos a estrutura de $K[x]$-módulo de V definida por T (ver Exercício 6.1.1): se $p(x) = a_n x^n + \cdots + a_0 \in K[x]$ e $\boldsymbol{v} \in V$, então

$$p(x) \cdot \boldsymbol{v} \equiv a_n T^n(\boldsymbol{v}) + \cdots + a_0 \boldsymbol{v}.$$

Observe-se que $\tilde{V} \subset V$ é um $K[x]$-submódulo sse $\tilde{V}$ é um subespaço linear de V, invariante sob a acção de T: $T(\tilde{V}) \subset \tilde{V}$, logo a estrutura do $K[x]$-módulo V está intrinsecamente ligada à estrutura da transformação T. Como $K[x]$ é um d.i.p., a classificação de módulos sobre d.i.p. permite obter o seguinte resultado:

Teorema 6.6.3 (Forma canónica de Jordan). *Seja $T : V \to V$ uma aplicação linear de um espaço vectorial de dimensão finita sobre K. Existe uma base $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ de V sobre K, em relação à qual a matriz da transformação T é*

$$J = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_m \end{pmatrix},$$

onde cada J_i é uma matriz $(n_i \times n_i)$ da forma

$$\begin{pmatrix} \lambda_i & 1 & & \\ & & 0 & \\ & \ddots & & \\ 0 & & & 1 \\ & & & \lambda_i \end{pmatrix}.$$

Demonstração. Observe-se que $p(x) \in K[x]$ é primo sse $p(x) = x - \lambda$. Logo, a decomposição de V em factores cíclicos primários é

$$V \simeq V_1 \oplus \cdots \oplus V_m,$$

onde $V_i \simeq \langle \boldsymbol{v}_i \rangle$ e $\operatorname{ann}(\boldsymbol{v}_i) = \langle (x - \lambda_i)^{n_i} \rangle$. Os elementos

$$\{(x - \lambda_i)^{n_i - 1}\boldsymbol{v}, \ldots, (x - \lambda_i)\boldsymbol{v}, \boldsymbol{v}\}$$

formam uma base de V_i sobre K (exercício), e a matriz de T relativamente a esta base é precisamente J_i. □

Para o cálculo da forma canónica de Jordan, é apenas necessário conhecer-se os divisores elementares (ou os factores invariantes) do $K[x]$-módulo V. Estes podem ser determinados da seguinte forma (ver a demonstração do Teorema 6.5.8): Seja $\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n\}$ uma base de V sobre K, e $A = (a_{ij})$ a matriz de T relativamente a esta base. O conjunto $\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n\}$ gera V como $K[x]$-módulo. Formando o módulo livre L gerado por estes elementos, temos o homomorfismo natural $\pi : L \to V$ e designamos por N o seu núcleo. Os elementos $\boldsymbol{e}_i = x\boldsymbol{f}_i - \sum_j a_{ji}\boldsymbol{f}_j$ formam uma base de N (como $K[\boldsymbol{x}]$-módulo), e os factores invariantes de V são obtidos por aplicação da Proposição 6.5.3 à matriz

$$\begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix}.$$

Esta fornece uma matriz equivalente

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & 1 & & & \\ & & & d_1(x) & & \\ & 0 & & & \ddots & \\ & & & & & d_s(x) \end{pmatrix},$$

onde $d_1(x) \mid \cdots \mid d_s(x)$ são os factores invariantes.

Exemplo 6.6.4.

Seja $T : \mathbb{C}^3 \to \mathbb{C}^3$ a transformação linear definida pela matriz

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 0 & 1 \\ 2 & -4 & 4 \end{pmatrix},$$

relativamente à base canónica de $\mathbb{C}^3$. *Como vimos no Exemplo 6.5.6, temos*

$$\begin{pmatrix} 0 & -1 & 0 \\ -1 & -x+2 & 0 \\ 1 & x-4 & 1 \end{pmatrix} \begin{pmatrix} x-2 & 0 & 0 \\ -1 & x & -1 \\ -2 & 4 & x-4 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & x \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & (x-2)^2 \end{pmatrix},$$

e os divisores elementares são $(x-2)$ *e* $(x-2)^2$. *Concluímos que a forma canónica de Jordan de* T *é*

$$J = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

A forma canónica de Jordan é uma consequência da decomposição em factores cíclicos primários. Da decomposição em factores cíclicos invariantes obtém-se uma outra forma canónica conhecida como FORMA CANÓNICA RACIONAL[11] (ver exercício).

Exercícios.

1. Determine todos os grupos abelianos de ordem 120.

2. Seja K um corpo algebricamente fechado de característica zero. Mostre que $U = \{r : r \text{ é raiz de } x^n - 1 = 0\}$ é um grupo abeliano isomorfo a $\mathbb{Z}_n$.

3. Seja $T : V \to V$ uma transformação linear de um espaço vectorial de dimensão finita sobre um corpo K e suponha que $V \simeq \langle \boldsymbol{v} \rangle$ (como $K[x]$-módulo), onde $\text{ann}(\boldsymbol{v}) = \langle (x-\lambda)^m \rangle$. Mostre que os elementos

$$\{(x-\lambda)^{m-1}\boldsymbol{v}, \ldots, (x-\lambda)\boldsymbol{v}, \boldsymbol{v}\}$$

formam uma base de V sobre K.

4. Determine a forma canónica de Jordan das matrizes:

(a) $A = \begin{pmatrix} -1 & 1 & -2 \\ 0 & -1 & 4 \\ 0 & 0 & 1 \end{pmatrix}$,

(b) $B = \begin{pmatrix} 0 & 0 & 0 & -8 \\ 1 & 0 & 0 & 16 \\ 0 & 1 & 0 & -14 \\ 0 & 0 & 1 & 6 \end{pmatrix}$.

[11] A forma canónica racional, ao contrário da forma canónica de Jordan, não requer que K seja algebricamente fechado.

5. Seja $T : V \to V$ uma transformação linear de um espaço vectorial de dimensão finita sobre um corpo K, e $d_1(x) \mid \cdots \mid d_s(x)$ os factores invariantes do $K[x]$-módulo V. A $m(x) = d_s(x)$ chama-se *polinómio mínimo* da transformação T e a $p(x) = d_1(x) \cdots d_s(x)$ chama-se *polinómio característico* da transformação T.

   (a) Mostre que $m(x) \neq 0$, $m(T) = 0$ e que se $q(x)$ é um polinómio tal que $q(T) = 0$ então $m(x)|q(x)$;

   (b) Mostre que $p(x) \neq 0$, $p(T) = 0$ e que $p(x) = \det(xI - T)$.

6. (Forma canónica racional) Seja $T : V \to V$ uma aplicação linear de um espaço vectorial de dimensão finita sobre K. Utilizando a decomposição em factores cíclicos invariantes de V como um $K[x]$-módulo, mostre que existe uma base $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ de V sobre K em relação à qual a matriz de T é

$$R = \begin{pmatrix} R_1 & & 0 \\ & \ddots & \\ 0 & & R_m \end{pmatrix},$$

   onde R_i é uma matriz $(n_i \times n_i)$ da forma

$$\begin{pmatrix} 0 & 0 & & & -a_0 \\ 1 & 0 & & & \vdots \\ & & \ddots & & \vdots \\ & 0 & & 0 & -a_{n_i-2} \\ & & & 1 & -a_{n_i-1} \end{pmatrix}.$$

   A R chama-se forma canónica racional da transformação linear T.

7. Recorde que uma equação diferencial ordinária (e.d.o.) linear escalar

$$\frac{d^n y}{dt^n} + a_{n-1}\frac{d^{n-1} y}{dt^{n-1}} + \cdots + a_1 \frac{dy}{dt} + a_0 y = 0$$

   é equivalente a um sistema de e.d.o.'s linear de primeira ordem:

$$\frac{d\boldsymbol{x}}{dt} = \boldsymbol{x}A,$$

   onde $\boldsymbol{x} = (y, y', y'', \ldots, y^{(n-1)})$ e A é a matriz companheira

$$\begin{pmatrix} 0 & 0 & & & -a_0 \\ 1 & 0 & & & \vdots \\ & & \ddots & & \vdots \\ & 0 & & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix}.$$

   Mostre, recorrendo à forma canónica racional, o seguinte recíproco: todo o sistema de e.d.o.'s linear de primeira ordem é equivalente a um sistema desacoplado de e.d.o.'s lineares escalares.

6.7 Categorias e Functores

As várias estruturas algébricas que temos vindo a estudar, embora diferentes, exibem muitas vezes semelhanças formais. Algumas das construções repetem-se para grupos, anéis e módulos e, por vezes, os métodos utilizados são em tudo idênticos. É pois tempo para parar e perguntar: será que não existe uma abordagem unificada que permita formalizar estas semelhanças de forma precisa? A resposta é sim, como veremos nesta secção, e a definição essencial é a seguinte:

Definição 6.7.1. Uma CATEGORIA $\mathcal{C}$ consiste em:

(i) Uma classe de OBJECTOS.

(ii) Para cada par de objectos (X, Y), um conjunto $\mathrm{Hom}(X, Y)$, cujos elementos chamamos MORFISMOS.

(iii) Uma aplicação $\mathrm{Hom}(X, Y) \times \mathrm{Hom}(Y, Z) \to \mathrm{Hom}(X, Z)$, a que chamamos COMPOSIÇÃO DE MORFISMOS.

A imagem do par (ϕ, ψ) sob a operação de composição de morfismos será designada por $\psi \circ \phi$, e as seguintes propriedades devem ser satisfeitas:

(C1) *Associatividade*: se $\phi \in \mathrm{Hom}(X, Y)$, $\psi \in \mathrm{Hom}(Y, Z)$ e $\tau \in \mathrm{Hom}(Z, W)$, então $\tau \circ (\psi \circ \phi) = (\tau \circ \psi) \circ \phi$.

(C2) *Existência de identidades*: para todo o objecto X, existe um morfismo $1_X \in \mathrm{Hom}(X, X)$ que satisfaz

$$1_X \circ \phi = \phi \quad \text{e} \quad \psi \circ 1_X = \psi,$$

sempre que $\phi \in \mathrm{Hom}(W, X)$ e $\psi \in \mathrm{Hom}(X, Y)$, onde Y e W são objectos arbitrários.

Exemplos 6.7.2.

1. *A categoria $\mathcal{S}$ em que os objectos são os conjuntos, em que os morfismos $\mathrm{Hom}(X, Y)$ são as aplicações $\phi : X \to Y$, e a composição de morfismos é a composição habitual de aplicações.*

2. *A categoria $\mathcal{G}$ em que os objectos são os grupos, os morfismos $\mathrm{Hom}(G, H)$ são os homomorfismos de grupos $\phi : G \to H$, e a composição de morfismos é a composição habitual.*

3. *A categoria $\mathcal{M}_A$ em que os objectos são os módulos sobre um anel A, os morfismos $\mathrm{Hom}(M, N)$ são as transformações lineares $\phi : M \to N$, e a composição de morfismos é a composição de transformações lineares.*

4. *A categoria $\mathcal{T}$ em que os objectos são os espaços topológicos, os morfismos $\mathrm{Hom}(X, Y)$ são as aplicações contínuas, e a composição de morfismos é a composição habitual de aplicações.*

O primeiro destes exemplos mostra porque é que, em geral, os objectos de uma categoria formam uma *classe*, em vez de um *conjunto*: não podemos falar do "conjunto de todos os conjuntos" sem nos envolvermos em paradoxos (será que o conjunto de todos os conjuntos é um membro de si próprio?). Esta diferença, cuja justificação completa exige um estudo promenorizado da Teoria do Conjuntos ([12]), significa que às classes não aplicamos as operações usuais sobre conjuntos (como, por exemplo, formar subconjuntos). Uma categoria em que os objectos são os elementos de um conjunto diz-se uma CATEGORIA PEQUENA.

Deve-se observar que um morfismo $\phi \in \mathrm{Hom}(X, Y)$, apesar das designações, não precisa de ser uma aplicação de X em Y, como se ilustra no exemplo seguinte:

Exemplo 6.7.3.

Fixe-se um grupo G. Seja $\mathcal{C}$ a categoria com um único objecto $\{*\}$ e em que os morfismos $\mathrm{Hom}(*, *)$ são os elementos de G. A composição de dois morfismos é multiplicação no grupo G. Se G é não-trivial, os morfismos não são aplicações entre objectos.

Uma CATEGORIA CONCRETA é uma categoria $\mathcal{C}$ em que todo o morfismo $\phi \in \mathrm{Hom}(X, Y)$ é uma aplicação $X \to Y$, em que o morfismo identidade $1_X \in \mathrm{Hom}(X, Y)$ é a aplicação identidade $X \to X$, e em que a composição de morfismos é a composição usual de aplicações. A grande maioria das categorias que estudamos neste livro são categorias concretas. De qualquer forma, vamos sempre representar um morfismo $\phi \in \mathrm{Hom}(X, Y)$ simbolicamente por $\phi : X \to Y$, tendo em atenção que ϕ não é necessariamente uma aplicação de X em Y.

Vejamos algumas propriedades elementares das categorias.

Proposição 6.7.4. *Numa categoria $\mathcal{C}$, para cada objecto X, o morfismo identidade 1_X é único.*

Demonstração. De facto, se 1_X e $1'_X$ são duas identidades em X, então pela propriedade (C2) aplicada a 1_X e a $1'_X$, obtemos que

$$1_X \circ 1'_X = 1'_X \quad \text{e} \quad 1_X \circ 1'_X = 1_X.$$

Logo, $1_X = 1'_X$. □

Numa categoria $\mathcal{C}$, dado um morfismo $f : X \to Y$, dizemos que $g : Y \to X$ é um INVERSO À ESQUERDA de f se

$$g \circ f = 1_X.$$

De forma análoga define-se INVERSO À DIREITA de f.

[12] Ver, por exemplo, P. R. Halmos, *Naive Set Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, 1974.

Proposição 6.7.5. *Se $f : X \to Y$ possui um inverso à esquerda g e um inverso à direita g', então $g = g'$.*

Demonstração. Pela definição de inverso à esquerda/direita, obtemos:

$$(g \circ f) \circ g' = 1_X \circ g' = g',$$
$$g \circ (f \circ g') = g \circ 1_Y = g.$$

Logo, pela associatividade, temos que $g = g'$. □

No caso em que $f : X \to Y$ possui um inverso à esquerda e à direita g, chama-se a g o inverso de f e escreve-se $g = f^{-1}$. Neste caso, diz-se que f é uma EQUIVALÊNCIA ou um ISOMORFISMO na categoria em questão.

Exemplos 6.7.6.

1. *Nos Exemplos 6.7.2 acima, as equivalências são as bijecções (na categoria dos conjuntos), os isomorfismos de grupos (na categoria dos grupos), os isomorfismos lineares (na categoria dos módulos sobre um anel) e os homeomorfismos (na categoria dos espaços topológicos).*

2. *No Exemplo 6.7.3, todos os morfismos são equivalências. Em geral, a uma categoria pequena em que todos os morfismos são invertíveis chama-se um* GRUPÓIDE.

Com o objectivo de relacionar duas categorias, introduzimos o conceito de "functor".

Definição 6.7.7. Um FUNCTOR COVARIANTE F de uma categoria $\mathcal{C}$ para uma categoria $\mathcal{D}$ é uma aplicação que a cada objecto X de $\mathcal{C}$ associa um objecto $F(X)$ de $\mathcal{D}$, e a cada morfismo $\phi : X \to Y$, um morfismo $F(\phi) : F(X) \to F(Y)$, tal que as seguintes propriedades são satisfeitas:

(i) *F preserva identidades:* $F(1_X) = 1_{F(X)}$ para todo o objecto X de $\mathcal{C}$;

(ii) *F preserva composições:* $F(\phi \circ \psi) = F(\phi) \circ F(\psi)$ para todos os morfismos ϕ e ψ que se podem compor.

De forma semelhante, define-se um FUNCTOR CONTRAVARIANTE em que F associa a cada objecto X de $\mathcal{C}$ um objecto $F(X)$ de $\mathcal{D}$, e a cada morfismo $\phi : X \to Y$, um morfismo $F(\phi) : F(Y) \to F(X)$, e:

(i) *F preserva identidades:* $F(1_X) = 1_{F(X)}$ para todo o objecto X de $\mathcal{C}$;

(ii') *F troca composições:* $F(\phi \circ \psi) = F(\psi) \circ F(\phi)$ para todos os morfismos ϕ e ψ que se podem compor.

Vejamos alguns exemplos de functores:

Exemplos 6.7.8.

1. *A aplicação que a cada grupo associa o seu conjunto base, e que a cada homomorfismo de grupos associa a aplicação entre os conjuntos base, é um functor covariante da categoria dos grupos na categoria dos conjuntos. Mais geralmente, dada uma categoria concreta $\mathcal{C}$, temos um functor $F : \mathcal{C} \to \mathcal{S}$ de C para a categoria dos conjuntos $\mathcal{S}$ que "esquece" a estrutura: a cada objecto X de C, o functor F associa o seu conjunto base X, e a cada morfismo $\phi \in \mathrm{Hom}(X, Y)$, o functor F associa a aplicação $X \to Y$.*

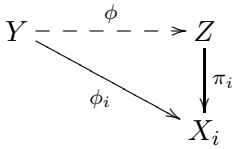
2. *A aplicação que a cada módulo M sobre um anel comutativo A associa o seu dual M^*, e a cada aplicação linear $\phi : M \to N$ associa a aplicação transposta $\phi^* : N^* \to M^*$, é um functor contravariante da categoria dos A-módulos à esquerda na categoria dos A-módulos à direita.*

3. *A aplicação que, a cada espaço topológico X associa o seu grupo de homologia $H_k(X, \mathbb{Z})$ (respectivamente, co-homologia $H^k(X, \mathbb{Z})$) e a cada aplicação contínua $\phi : X \to Y$ o homomorfismo de grupos $\phi_* : H_k(X, \mathbb{Z}) \to H_k(Y, \mathbb{Z})$ (respectivamente, $\phi^* : H^k(Y, \mathbb{Z}) \to H^k(X, \mathbb{Z})$), é um functor covariante (respectivamente, contravariante) da categoria dos espaços topológicos na categoria dos grupos abelianos.*

Muitas das construções que foram feitas anteriormente podem ser abstraídas para o contexto geral da Teoria das Categorias.

Consideremos, a título de exemplo, a noção de produto directo. Seja $\{X_i\}_{i\in I}$ uma família de objectos numa categoria $\mathcal{C}$. Um PRODUTO dos objectos $\{X_i\}_{i\in I}$ é um par $(Z, \{\pi_i\}_{i\in I})$, onde Z é um objecto e os $\pi_i : Z \to X_i$ são morfismos que satisfazem a seguinte propriedade universal:

- Para todo o objecto Y e morfismos $\phi_i : Y \to X_i$, $i \in I$, existe um único morfismo $\phi : Y \to Z$ tal que o seguinte diagrama comuta



  para todo o $i \in I$.

É fácil de ver que o produto, caso exista, fica definido a menos de isomorfismo. É claro que nesse caso escrevemos $\prod_{i\in I} X_i$ para representar o produto. Note que o produto pode existir ou não, dependendo da categoria. Para cada categoria é necessário mostrar a sua existência, e para isso é preciso ter um modelo concreto (normalmente bastante óbvio). Foi isso que fizemos anteriormente para a categoria dos grupos e para a categoria dos módulos sobre um anel.

Uma das grandes vantagens da Teoria das Categorias é a de permitir tornar precisas certas expressões que usamos na exposição de um dado formalismo matemático. Exemplo disso são termos que se usam frequentemente, tais como a que uma dada aplicação é "induzida", ou que certas propriedades são "functoriais", ou ainda que uma dada construção é "natural". Por exemplo, o último termo é geralmente sinónimo de que a construção não depende de escolhas, mas pode ser tornado preciso através da seguinte:

Definição 6.7.9. Uma TRANSFORMAÇÃO NATURAL T entre dois functores $F : \mathcal{C} \to \mathcal{D}$ e $G : \mathcal{C} \to \mathcal{D}$ é uma aplicação que associa a cada objecto X da categoria $\mathcal{C}$ um morfismo da categoria $\mathcal{D}$:

$$T_X : F(X) \to G(X),$$

tal que o seguinte diagrama comuta

$$\begin{array}{ccc} F(X) & \xrightarrow{T_X} & G(X) \\ {\scriptstyle F(\phi)}\downarrow & & \downarrow{\scriptstyle G(\phi)} \\ F(Y) & \xrightarrow{T_Y} & G(Y) \end{array}$$

para todo o morfismo $\phi : X \to Y$ de $\mathcal{C}$. Se T_X é uma equivalência para todo o objecto X, dizemos que T é uma EQUIVALÊNCIA NATURAL.

No exemplo seguinte mostramos como podemos formalizar a afirmação de que para todo o espaço vectorial de dimensão finita V existe um isomorfismo natural entre o duplo dual $(V^*)^*$ e V.

Exemplo 6.7.10.

Seja $\mathcal{C}$ a categoria dos módulos sobre um anel A. Para cada A-módulo M, consideramos o duplo dual:

$$M^{**} \equiv (M^*)^*,$$

e para cada transformação linear $\phi : M \to N$, consideramos a transformação linear $\phi^{**} : M^{**} \to N^{**}$ dupla transposta:

$$\phi^{**} \equiv (\phi^*)^*.$$

Esta operação define um functor covariante de $\mathcal{C}$ em $\mathcal{C}$.

Para cada A-módulo M designamos por $T_M : M \to M^{**}$ o homomorfismo definido da seguinte forma: para cada $\boldsymbol{v} \in M$, $T_M(\boldsymbol{v}) : M^* \to A$ é a transformação linear

$$\xi \mapsto \xi(\boldsymbol{v}).$$

Verificamos facilmente que $M \mapsto T_M$ é uma transformação natural entre o functor duplo dual e o functor identidade.

Se, em vez da categoria dos A-módulos à esquerda, considerarmos a categoria dos espaços vectoriais de dimensão finita sobre um corpo K, então $V \mapsto T_V$ define uma equivalência natural entre o functor duplo dual e o functor identidade.

Neste livro não usamos a Teoria da Categorias, com pequenas excepções onde a utilizamos apenas como uma linguagem, e por isso não desenvolvemos mais este tópico. No entanto, gostaríamos de frisar que esta tem adquirido uma importância central em várias áreas da Matemática, como por exemplo na Topologia e na Geometria Algébrica, e hoje em dia constitui uma área muito importante da Álgebra.

Exercícios.

1. Seja $\{X_i\}_{i\in I}$ uma família de objectos numa categoria $\mathcal{C}$. Defina CO-PRODUTO $\coprod_{i\in I}^{*} X_i$ dos objectos $\{X_i\}_{i\in I}$ e verifique que a soma directa de grupos abelianos e de módulos, e o produto livre, são co-produtos nas respectivas categorias.

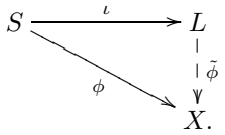
2. Um conjunto com um ponto marcado é um par (X, x) onde X é um conjunto e $x \in X$. Um morfismo $(X, x) \to (Y, y)$ entre conjuntos com pontos marcados é uma aplicação $f : X \to Y$ tal que $f(x) = y$.

   (a) Mostre que os conjuntos marcados e os morfismos de conjuntos marcados formam um categoria.

   (b) Mostre que existem produtos nesta categoria e descreva-os.

   (c) Mostre que existem co-produtos nesta categoria e descreva-os.

3. Seja L um objecto numa categoria $\mathcal{C}$, S um conjunto não-vazio, e $\iota : X \to L$ uma aplicação. Diz-se que L é LIVRE NO CONJUNTO S se para cada objecto X de $\mathcal{C}$ e aplicação $\phi : S \to X$ existe um único morfismo $\tilde{\phi} : L \to X$ que torna o seguinte diagrama comutativo:

   Mostre que, numa categoria $\mathcal{C}$, se L é livre no conjunto S, L' é livre no conjunto S' e $|X| = |X'|$, então L' é isomorfo a L.

4. Um objecto I numa categoria $\mathcal{C}$ diz-se UNIVERSAL ou INICIAL se para cada objecto X de $\mathcal{C}$ existe um único morfismo $\phi : I \to X$:

   (a) Mostre que quaisquer dois objectos iniciais de uma categoria são isomorfos.

   (b) Determine os objectos iniciais e terminais nas categorias dos grupos.

   (c) Mostre que o co-produto pode ser considerado com um objecto universal numa categoria apropriada.

5. Defina, analogamente ao problema anterior, o que é um objecto CO-UNIVERSAL ou TERMINAL numa categoria $\mathcal{C}$. Mostre que o produto pode ser considerado como um objecto co-universal numa categoria apropriada.

Capítulo 7

Teoria de Galois

A solução de uma equação quadrática era conhecida pelos matemáticos da Babilónia[1], que sabiam como "completar o quadrado", e foi popularizada no mundo ocidental durante o Renascimento por traduções em latim do livro de al-Khowarizmi *Al-jabr wa'l muqābalah* (mencionado no Capítulo 1). Em 1545, a publicação da *Ars Magna* de Geronimo Cardano (1501-1576), também conhecido por Cardan, inclui fórmulas para a resolução de equações do $3^{\underline{o}}$ e $4^{\underline{o}}$ graus, atribuídas pelo autor, respectivamente, a Niccolo Tartaglia (1500-1565) e Ludovico Ferrari (1522-1565). A descoberta destas fórmulas e a luta pela prioridade da sua descoberta tem uma história bastante curiosa e divertida que é descrita nas obras indicadas.

A "fórmula de Cardan", como é hoje conhecida, para a resolução da equação cúbica $x^3 + px = q$, é

$$x = \sqrt[3]{\sqrt{(p/3)^3 + (q/2)^2} + q/2} - \sqrt[3]{\sqrt{(p/3)^3 + (q/2)^2} - q/2}.$$

O caso geral de uma equação do terceiro grau $y^3 + by^2 + cy + d = 0$ pode ser reduzido a este caso pela transformação $y = x - b/3$. A verificação, por substituição, de que a fórmula de Cardan fornece uma solução da equação deverá dar uma ideia do grau de dificuldade envolvido neste tipo de problema.

A equação do quarto grau pode também ser reduzida à solução de uma cúbica. Podemos sempre assumir, eventualmente após uma translação, que a quártica é da forma $x^4 + px^2 + qx + r = 0$. Completando o quadrado, obtemos

$$(x^2 + p)^2 = px^2 - qx - r + p^2.$$

O truque consiste em observar que, para qualquer y, temos

$$\begin{aligned}(x^2 + p + y)^2 &= px^2 - qx - r + p^2 + 2y(x^2 + p) + y^2 \\ &= (p + 2y)x^2 - qx + (p^2 - r + 2py + y^2).\end{aligned}$$

[1]Para as referências históricas deste capítulo ver Carl R. Boyer, *A History of Mathematics*, John Wiley & Sons, New York (1968), e Dirk J. Struik, *História Concisa das Matemáticas*, Gradiva Publicações Lda., Lisboa (1989).

Ora esta última equação é quadrática em x, e podemos escolher y de forma que seja um quadrado perfeito. Isto consegue-se precisamente, impondo que o *discriminante* seja zero:

$$q^2 - 4(p + 2y)(p^2 - r + 2py + y^2) = 0.$$

Esta última equação é uma cúbica em y:

$$-8y^3 - 20py^2 + (-16p^2 + 8r)y + (q^2 - 4p^3 + 4pr) = 0,$$

que portanto pode ser resolvida com recurso à fórmula de Cardan. Com este valor para y, o lado direito da equação auxiliar acima fica um quadrado perfeito, de forma que, extraindo as raízes, obtemos uma equação quadrática que pode ser resolvida.

As soluções expostas na *Ars Magna* constituíram um forte estímulo na procura de fórmulas para resolução de equações algébricas de graus mais elevados. Este esforços mostraram-se infrutíferos durante mais de 300 anos, pois foi preciso esperar pelo início do século *XIX* para que Abel e Rufini chegassem à conclusão oposta: para uma equação do $5^{\underline{o}}$ grau não existe uma fórmula geral que exprima as raízes como radicais dos coeficientes da equação.

Inspirado pela demonstração de Abel da impossibilidade de resolução da equação quíntica, Galois iniciou o estudo de equações algébricas de grau arbitrário, e mostrou não só a impossibilidade de resolução da equação algébrica geral de grau maior ou igual a cinco, como deu ainda um critério para decidir se uma equação particular pode ser resolvida e, em caso afirmativo, um método de resolução. Os trabalhos de Galois, apesar da sua morte prematura, foram fundamentais no estabelecimento da Álgebra, tal como a conhecemos hoje, e tiveram consequências muito para além do problema original da resolução de equações algébricas por radicais.

Para ilustrarmos as ideias de Galois, consideremos a equação quártica com coeficientes racionais

$$p(x) = x^4 + x^3 + x^2 + x + 1 = 0.$$

Esta equação tem as raízes $r_k = e^{i\frac{2\pi k}{5}}$ $(k = 1, \ldots, 4)$ (porquê?). Pensemos agora em *todas* as possíveis equações polinomiais, com coeficientes racionais, que são satisfeitas por estas raízes. Estas incluem, entre outras, as equações

$$\begin{array}{ll} r_1 + r_2 + r_3 + r_4 - 1 = 0, & r_1 r_4 = 1, \\ (r_1 + r_4)^2 + (r_1 + r_4) - 1 = 0, & (r_1)^5 - 1 = 0, \quad \ldots \end{array}$$

A observação chave é a seguinte: Se considerarmos as possíveis permutações das raízes que transformam equações deste tipo ainda em equações deste tipo, obtemos o *grupo de Galois* da equação: $G = \{I, (1243), (14)(23), (1342)\}$.

A estrutura deste grupo, descobriu Galois, é a chave para a resolução desta equação[2].

Consideremos por exemplo o subgrupo $H = \{I, (14)(23)\}$. É simples verificar que as expressões polinomiais nas raízes, com coeficientes racionais, que são fixas pelos elementos de H são precisamente os polinómios em $w_1 = r_1 + r_4$ e $w_2 = r_2 + r_3$. Mas w_1 e w_2 são as soluções da equação quadrática

$$x^2 + x - 1 = 0.$$

Assim, e supondo que não conhecíamos as expressões das soluções da equação original, poderíamos descobri-las resolvendo primeiro esta equação quadrática, obtendo

$$r_1 + r_4 = \frac{-1+\sqrt{5}}{2}, \qquad r_2 + r_3 = \frac{-1-\sqrt{5}}{2},$$

e de seguida a equação quadrática

$$(x - r_1)(x - r_4) = x^2 - (r_1 + r_4)x + r_1 r_4 = 0,$$

já que de facto esta equação tem como coeficientes expressões polinomiais em w_1 e w_2 (pois temos $r_1 r_4 = 1$).

Observe-se que o Grupo de Galois pode ser caracterizado como o *grupo de simetrias* da equação: são as transformações que levam soluções (raízes) em soluções preservando a estrutura algébrica das soluções. Este é precisamente o ponto de partida na exposição moderna da Teoria de Galois: constrói-se o corpo $\mathbb{Q}(r_1, \ldots, r_n)$ gerado pelas raízes da equação, e os elementos do Grupo de Galois aparecem como automorfismos destes corpos [3]. Nesta linguagem, a Teoria de Galois consiste em transformar questões sobre a estrutura destes corpos em questões sobre a estrutura do grupo associado.

7.1 Extensões de Corpos

Como mencionámos acima, o conceito de extensão de corpo é fundamental na exposição que adoptaremos da Teoria de Galois. Recordemos que um corpo L é uma *extensão* de um corpo K, se K é um subcorpo de L. Nesta secção iniciamos o estudo sistemático das extensões de um dado corpo. Começamos por recordar alguns dos resultados obtidos no Capítulo 3.

Seja K um corpo, e L uma extensão de K. Recorde-se que a extensão diz-se *finita* (respectivamente *infinita*) se L, visto como espaço vectorial sobre o corpo K, tem dimensão finita (respectivamente infinita). A dimensão de L sobre K designa-se por $[L : K]$. Se $S \subset L$ é um subconjunto, designamos por

[2] Esta descoberta é tanto mais surpreendente, pois Galois teve de inventar primeiro o conceito de grupo que até aquela data era inexistente!

[3] A noção de corpo só foi formalizada por Dedekind em 1879, mais de 50 anos depois da morte trágica de Galois.

$K(S)$ o menor subcorpo de L que contém K e S. É claro que $K(S)$ é uma extensão de K gerada por S. Se $S = \{u_1, \ldots, u_n\}$, escrevemos $K(u_1, \ldots, u_n)$ em vez de $K(\{u_1, \ldots, u_n\})$.

Vejamos mais em pormenor o caso de um só elemento, *i.e.*, o caso $K(u)$ em que $u \in L$. Se x é uma indeterminada, temos o homomorfismo de anéis $\phi : K[x] \to L$ que a um polinómio $g(x)$ faz corresponder o seu valor em u ($g(x) \mapsto g(u)$). O núcleo $N(\phi)$ deste homomorfismo é um ideal de $K[x]$ que é necessariamente principal. Temos então dois casos:

(i) u é transcendente sobre K. Neste caso, $N(\phi) = \{0\}$, logo, ϕ é um monomorfismo cuja imagem é $K[u]$, e que possui uma única extensão ao corpo das fracções $K(x)$ de $K[x]$. Temos então $K(u) \simeq K(x)$, e os elementos de $K(u)$ são da forma $g(u)/f(u)$ com $g(x), f(x) \in K[x]$ e $f(x) \neq 0$. A extensão $K(u)$ tem dimensão infinita sobre K;

(ii) u é algébrico sobre K. Então $N(\phi) = \langle p(x) \rangle$, onde $p(x)$ é um polinómio irredutível, e $K(u) = K[u] \simeq K[x]/\langle p(x) \rangle$. Se impusermos que $p(x)$ seja mónico, então $p(x)$ é único, e chama-se a $p(x)$ *polinómio mínimo* de u. A extensão $K(u)$ tem dimensão $[K(u) : K] = \deg p(x)$. A esta dimensão chama-se *grau algébrico* de u sobre K.

Definição 7.1.1. Uma extensão L de um corpo K diz-se uma EXTENSÃO SIMPLES se existe um $u \in L$ tal que $L = K(u)$. Neste caso, a u chama-se ELEMENTO PRIMITIVO de L.

Um extensão L de K diz-se *algébrica* (respectivamente *transcendente*) se todos os elementos de L são algébricos (respectivamente se existe um elemento de L transcendente) sobre K. Uma extensão simples L é algébrica ou transcendente, consoante os seus elementos primitivos sejam algébricos ou transcendentes. Uma extensão L de dimensão finita sobre K é sempre algébrica (ver Exercício 3.4.8), mas existem extensões algébricas de dimensão infinita. Uma extensão transcendente é necessariamente de dimensão infinita.

Exemplos 7.1.2.

1. *Considere $L = \mathbb{Q}(\sqrt[n]{2}) \subset \mathbb{R}$ e $K = \mathbb{Q}$. Pelo Critério de Eisenstein, o polinómio $p(x) = x^n - 2$, $(n \geq 2)$ é irredutível sobre $\mathbb{Q}$. O número $u = \sqrt[n]{2}$ é uma raiz de $p(x)$ em $\mathbb{R}$, logo, $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, e $\sqrt[n]{2}$ é algébrico de grau n sobre $\mathbb{Q}$.*

2. *Considere $L = \mathbb{C}$ e $K = \mathbb{R}$. O polinómio $x^2 + 1$ é obviamente irredutível sobre $\mathbb{R}$. O número $i \in \mathbb{C}$ é uma raiz de $x^2 + 1$ em $\mathbb{C}$, logo i é algébrico de grau 2 sobre $\mathbb{R}$. Na realidade, $\mathbb{C} = \mathbb{R}[x]/\langle x^2 + 1 \rangle = \mathbb{R}(i)$, de forma que $\mathbb{C}$ é uma extensão simples de $\mathbb{R}$, e i é um elemento primitivo.*

3. *Considere $L = \mathbb{C}$ e $K = \mathbb{Q}$. Então L é uma extensão transcendente de K, e $[\mathbb{C} : \mathbb{Q}] = \infty$.*

A demonstração da proposição seguinte é deixada como exercício:

Proposição 7.1.3. *Sejam $M \supset L \supset K$ extensões sucessivas de um corpo K. Então $[M : K]$ é finito se e só se $[M : L]$ e $[L : K]$ são ambos finitos. Nesse caso temos*

$$[M : K] = [M : L] \cdot [L : K].$$

Exemplo 7.1.4.

Vimos no exemplo acima que $[\mathbb{Q}(\sqrt{2}), \mathbb{Q}] = 2$. Por outro lado, o polinómio $q(x) = x^2 - 3$ é irredutível sobre $\mathbb{Q}(\sqrt{2})$. De facto, uma raiz de $q(x)$ em $\mathbb{Q}(\sqrt{2})$ terá de satisfazer $(a+b\sqrt{2})^2 = 3$, $a, b \in \mathbb{Q}$, logo, $(a^2+2b^2)+2ab\sqrt{2} = 3$, donde $a^2 + 2b^2 = 3$ e $ab = 0$. Se $b = 0$, temos que $a^2 = 3$ o que é impossível pois $\sqrt{3} \notin \mathbb{Q}$. Se $a = 0$ temos que $(2b)^2 = 6$ o que é impossível, pois $\sqrt{6} \notin \mathbb{Q}$. Como x^2-3 é irredutível em $\mathbb{Q}(\sqrt{2})$, concluímos que $\mathbb{Q}(\sqrt{2})(\sqrt{3}) \simeq \mathbb{Q}(\sqrt{2})[x]/\langle x^2-3\rangle$ e que $[\mathbb{Q}(\sqrt{2})(\sqrt{3}), \mathbb{Q}(\sqrt{2})] = 2$. Pela Proposição 7.1.3, obtemos

$$\begin{aligned}[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}] &= [\mathbb{Q}(\sqrt{2})(\sqrt{3}), \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}), \mathbb{Q}] \\ &= 2 \cdot 2 = 4.\end{aligned}$$

Nos exemplos acima, considerámos apenas subcorpos do corpo dos números complexos. Neste caso não há qualquer problema em determinar extensões em que um dado polinómio possua raízes devido a uma propriedade fundamental de $\mathbb{C}$: qualquer polinómio (de grau ≥ 1) com coeficientes em $\mathbb{C}$ tem pelo menos uma raiz. Recordemos que, em geral, um corpo L diz-se *algebricamente fechado* se qualquer polinómio $p(x) \in L[x]$ de grau ≥ 1 possui uma raiz em L.

Na proposição seguinte damos outras caracterizações de um corpo algebricamente fechado que podem ser facilmente verificadas.

Proposição 7.1.5. *As seguintes afirmações são equivalentes:*

(i) L é um corpo algebricamente fechado.

(ii) Todo o polinómio $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in L[x]$ se decompõe num produto de factores lineares: $p(x) = a_n \prod_1^n (x - r_i)$.

(iii) Todo o polinómio irredutível de $L[x]$ tem grau 1.

(iv) Não existem extensões algébricas próprias de L.

Existem muitos exemplos interessantes de corpos que não são subcorpos de $\mathbb{C}$. Por exemplo, os corpos numéricos $\mathbb{Z}_p$, importantes na Teoria dos Números, ou o corpo das fracções $\mathbb{C}(\mathbf{z})$, fundamental na Geometria Algébrica. Para estes corpos não é óbvio que dado um polinómio exista uma extensão onde o polinómio se decomponha em factores lineares. Abordaremos este problema numa das próximas secções.

Exercícios.

1. Mostre que o subconjunto de $\mathbb{C}$ formado pelos elementos algébricos sobre $\mathbb{Q}$ é uma extensão algébrica de $\mathbb{Q}$ de dimensão infinita sobre $\mathbb{Q}$. (Os elementos deste corpo são designados usualmente por *números algébricos*).

2. Demonstre a Proposição 7.1.3.

3. Mostre que:

   (a) todo o corpo K algebricamente fechado é infinito;

   (b) se K é um corpo infinito, então qualquer extensão algébrica de K tem a mesma cardinalidade que K;

4. Verifique que existem elementos de $\mathbb{C}$ que não são algébricos sobre $\mathbb{Q}$.

5. Seja $L \subset \mathbb{C}$ a menor extensão de $\mathbb{Q}$ que contém as raízes do polinómio $x^3 - 2$. Decida se L é simples ou não, e em caso afirmativo dê um exemplo de um elemento primitivo.

6. Demonstre a Proposição 7.1.5.

7. Seja K um corpo e x uma indeterminada. Em $K(x)$ considere o elemento $u = x^2$. Mostre que $K(x)$ é uma extensão simples de $K(u)$. Qual é a dimensão de $[K(x) : K(u)]$?

7.2 Construções com Régua e Compasso

Os matemáticos da Grécia Antiga exprimiam de forma geométrica muitos dos seus conceitos. Em geral, apenas eram consideradas válidas construções geométricas que pudessem ser obtidas pelo uso exclusivo de régua (sem escala) e do compasso. Apesar da grande habilidade demonstrada pelos matemáticos gregos, houve algumas figuras e construções geométricas aparentemente simples para as quais não conseguiram descobrir um método baseado exclusivamente no uso de régua e do compasso. Entre as mais famosas contavam-se:

(i) trissecar um ângulo;

(ii) duplicar um cubo;

(iii) construir um heptágono regular;

(iv) construir um quadrado de área igual a um dado círculo.

Veremos que estes problemas, bem como qualquer outro envolvendo construções com régua e compasso, podem ser reformulados em questões da Teoria dos Corpos. Tal reformulação permite mostrar que as construções (i)-(iv) não são de facto possíveis com recurso exclusivo à régua e compasso.

Suponhamos que começando com dois pontos no plano pretendemos determinar todas as construções com régua e compasso baseadas nestes pontos. Sem perda de generalidade, podemos assumir que os pontos são os números 0 e 1 do plano complexo. Definimos indutivamente subconjuntos finitos $X_m,\ m = 1, 2, \ldots$, de pontos do plano complexo, da seguinte forma:

- $X_1 \equiv \{0, 1\}$, e
- X_{m+1} é a união de X_m com
  - (C1) os pontos de intersecção de linhas rectas ligando pontos de X_m;
  - (C2) os pontos de intersecção de linhas rectas ligando pontos de X_m com as circunferências cujos centros são pontos de X_m e cujos raios são segmentos com extremidades em X_m;
  - (C3) os pontos de intersecção de pares de circunferências cujos centros são pontos de X_m e cujos raios são segmentos com extremidades em X_m;

Introduzimos o *conjunto $\mathcal{C}$ dos pontos construtíveis* como sendo a união

$$\mathcal{C} \equiv \bigcup_m X_m.$$

Dizemos que um ponto z do plano complexo é *construtível com régua e compasso* se pertence a $\mathcal{C}$. As construções que os Gregos consideravam construtíveis com régua e compasso correspondem às figuras geométricas formadas por segmentos e arcos cujas extremidades e vértices são pontos construtíveis.

Os resultados que se seguem fornecem descrições alternativas do conjunto $\mathcal{C}$ dos pontos construtíveis. Como veremos, estes resultados são incompletos. Só mais tarde, no final deste capítulo, após o nosso estudo da Teoria de Galois, será então possível fornecermos uma descrição mais pormenorizada do conjunto $\mathcal{C}$.

Teorema 7.2.1. *$\mathcal{C}$ é o menor subcorpo de $\mathbb{C}$ que contém $\mathbb{Q}$, fechado para as operações de conjugação ($z \mapsto \bar{z}$) e extracção da raiz ($z \mapsto z^{\frac{1}{2}}$).*

Demonstração. Dividimos a demonstração em três partes:

(a) *$\mathcal{C}$ é um subcorpo de $\mathbb{C}$:* Suponha-se que $z_1, z_2 \in \mathcal{C}$. Então $z_1 - z_2$ e $z_1/z_2 (z_2 \neq 0)$ pertencem a $\mathcal{C}$, pois as operações usuais de adição e multiplicação de números complexos podem ser expressas geometricamente por construções envolvendo exclusivamente (C1), (C2) e (C3) (exercício).

(b) *$\mathcal{C}$ é fechado para as operações de conjugação e de extracção da raiz:* é óbvio que $\mathcal{C}$ é fechado para a operação de conjugação. Por outro lado, se $z \in \mathcal{C}$ e $r = |z|$, podemos obter $\sqrt{r}$ usando (C1), (C2) e (C3), através da construção geométrica indicada na figura. Logo, $z^{\frac{1}{2}}$ pode ser construído com régua e compasso.

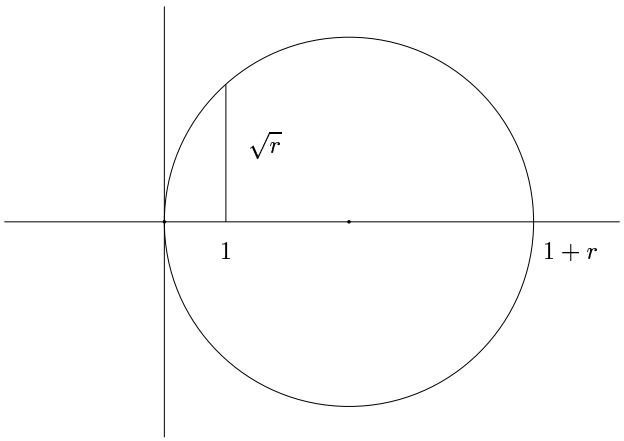


Figura 7.2.1: Extracção da raiz.

(c) *Se $\mathbb{Q} \subset \mathcal{C}' \subset \mathbb{C}$ é um subcorpo fechado para as operações de conjugação e extracção da raiz, então $\mathcal{C} \subset \mathcal{C}'$:* Precisamos de mostrar que os pontos de intersecção de

(i) linhas rectas ligando pontos de $\mathcal{C}'$,

(ii) linhas rectas ligando pontos de $\mathcal{C}'$ com circunferências cujos centros são pontos de $\mathcal{C}'$ e cujos raios são segmentos com extremidades em $\mathcal{C}'$,

(iii) pares de circunferências cujos centros são pontos de $\mathcal{C}'$ e cujos raios são segmentos com extremidades em $\mathcal{C}'$,

pertencem a $\mathcal{C}'$. Observemos primeiro que, se $z = x + iy \in \mathcal{C}'$, então, sendo $\mathcal{C}'$ fechado para a operação de conjugação, as coordenadas x e y pertencem a $\mathcal{C}'$. Segue-se que, se $ax + by + c = 0$ é a equação de uma recta que liga pontos de $\mathcal{C}'$, então $a, b, c \in \mathcal{C}'$. Da mesma forma, se $x^2 + y^2 + dx + ey + f = 0$ é a equação de uma circunferência com centro em $\mathcal{C}'$, sendo o raio um segmento com extremidades em $\mathcal{C}'$, então $d, e, f \in \mathcal{C}'$. Agora, os pontos de intersecção de dois objectos deste tipo têm como coordenadas certas fracções envolvendo quando muito raízes quadradas dos coeficientes a, b, c, d, e, f, logo, pertencem a $\mathcal{C}'$. □

O próximo resultado mostra que a propriedade de um número complexo ser construtível está ligada à estrutura de certos corpos.

Teorema 7.2.2. *Um número complexo z pertence a $\mathcal{C}$ se e só se pertence a um subcorpo de $\mathbb{C}$ da forma $\mathbb{Q}(u_1, u_2, \ldots, u_r)$, em que ${u_1}^2 \in \mathbb{Q}$ e, para cada $m = 1, 2, \ldots, r-1$, também ${u_{m+1}}^2 \in \mathbb{Q}(u_1, \ldots, u_m)$.*

Demonstração. Como $\mathcal{C}$ é um corpo que contém $\mathbb{Q}$ e é fechado para a operação de extracção da raiz, vemos que os corpos da forma $\mathbb{Q}(u_1, u_2, \ldots, u_r)$, com ${u_1}^2 \in \mathbb{Q}$ e ${u_{m+1}}^2 \in \mathbb{Q}(u_1, \ldots, u_m)$ $(m < r)$, são subcorpos de $\mathcal{C}$. Para completar a demonstração mostramos que o conjunto dos números complexos que pertencem pelo menos a um corpo da forma $\mathbb{Q}(u_1, u_2, \ldots, u_r)$ formam um subcorpo de $\mathbb{C}$, fechado para as operações de conjugação $(z \mapsto \bar{z})$ e extracção da raiz $(z \mapsto z^{\frac{1}{2}})$. Para isso basta observar que, se $z \in \mathbb{Q}(u_1, u_2, \ldots, u_r)$ e $z' \in \mathbb{Q}({u'}_1, {u'}_2, \ldots, {u'}_s)$, então $z - z'$ e $z/z'(z' \neq 0)$ pertencem a $\mathbb{Q}(u_1, u_2, \ldots, u_r, {u'}_1, {u'}_2, \ldots, {u'}_s)$. □

Uma consequência deste resultado é o seguinte corolário, que pode ser utilizado para excluir um número de $\mathcal{C}$.

Corolário 7.2.3. *Se um número $z \in \mathbb{C}$ é construtível, então é algébrico sobre $\mathbb{Q}$ de grau uma potência de 2.*

Demonstração. Se $K(u)$ é uma extensão do corpo K em que $u^2 \in K$, então $K(u) = K$ ou $[K(u) : K] = 2$. Logo, para os corpos $\mathbb{Q}(u_1, u_2, \ldots, u_r)$ com ${u_1}^2 \in \mathbb{Q}$ e ${u_{m+1}}^2 \in \mathbb{Q}(u_1, \ldots, u_m)$, se $m < r$, temos $[\mathbb{Q}(u_1, \ldots, u_r) : \mathbb{Q}] = 2^s$, para algum inteiro $s \leq r$. O corolário segue-se do teorema, observando que, se $z \in \mathcal{C}$, então $\mathbb{Q}(z) \subset \mathbb{Q}(u_1, \ldots, u_r)$, logo, $[\mathbb{Q}(z) : \mathbb{Q}] = 2^t$. □

Este corolário não é verdadeiro na direcção inversa, como se tornará claro durante o estudo da Teoria de Galois nas próximas secções.

Nos exemplos seguintes usamos o corolário para mostrar que as construções (i)-(iv) não são possíveis com uso exclusivo de régua e compasso.

Exemplos 7.2.4.

1. ***Trissecar um ângulo.*** *Podemos construir um ângulo de 60^o graus com régua e compasso. Vejamos que não podemos trissecar um ângulo de 60^o. Se tal fosse possível, o número $\cos 20^o + i \operatorname{sen} 20^o$ seria construtível e, em particular, $\cos 20^o$ também seria construtível. Vejamos que tal não é verdade. Usando a identidade trigonométrica*

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta,$$

vemos que $\cos 20^o$ é uma raiz do polinómio $4x^3 - 3x - \frac{1}{2} = 0$. Este polinómio é irredutível sobre $\mathbb{Q}$ (exercício), logo o grau de $\cos 20^o$ sobre $\mathbb{Q}$ é 3. Pelo corolário, $\cos 20^o$ não é construtível.

2. ***Duplicação do cubo.*** *Precisamos de mostrar que $\sqrt[3]{2}$ não é construtível. Para isso, basta observar que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, pois $\sqrt[3]{2}$ é uma raiz do polinómio irredutível $x^3 - 2 = 0$.*

3. ***Construção do heptágono regular.*** *Tal construção requereria a construtibilidade do número* $z = \cos\frac{2\pi}{7} + i\ \text{sen}\,\frac{2\pi}{7}$. *Este número é raiz do polinómio* $x^7 - 1 = (x-1)(x^6+x^5+\cdots+1)$. *Como* $x^6+x^5+\cdots+1$ *é irredutível sobre* $\mathbb{Q}$, *concluímos que* $[\mathbb{Q}(z):\mathbb{Q}] = 6$. *Como 6 não é uma potência de 2, o corolário mostra que* z *não é construtível.*

4. ***Quadratura do círculo.*** *Começando com um círculo unitário, vemos que esta construção requer a construtibilidade do número* π. *Como sabemos,* π *é um número transcendente sobre* $\mathbb{Q}$, *logo não é construtível*[4].

Existem números algébricos de grau uma potência de 2 que não são construtíveis. Veremos mais à frente que a Teoria de Galois fornece um critério mais eficiente para determinar se um dado número algébrico é construtível. Por enquanto interessa-nos apenas salientar como a estrutura de certas extensões de $\mathbb{Q}$ foi determinante para estudar esta propriedade.

Exercícios.

1. Interprete as operações usuais de adição e multiplicação de números complexos geometricamente, mostrando que envolvem exclusivamente (C1), (C2) e (C3) e, portanto, podem ser efectuadas com recurso exclusivo à régua e compasso.

2. Mostre que o número $\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$ é construtível.

3. Mostre que o polinómio $q(x) = 4x^3 - 3x - \frac{1}{2}$ é irredutível sobre $\mathbb{Q}$.

4. Mostre que $\arccos 71/125$ pode ser trissecado.

5. Seja p um número primo. Mostre que o polinómio $x^{p-1} + x^{p-2} + \cdots + 1$ é irredutível sobre $\mathbb{Q}$.
(Sugestão: Substitua x por $x+1$ na expressão $x^{p-1} + x^{p-2} + \cdots + 1 = (x^p - 1)/(x-1)$ e use o Critério de Eisenstein.)

6. Seja p um número primo.
   (a) Mostre que um polígono regular de p lados só pode ser construído com régua e compasso se $p = 2^s + 1$.
   (b) Mostre que se $p = 2^s + 1$ é primo então p é um número de Fermat: $p = 2^{2^t} + 1$.

[4]Não discutiremos aqui a questão da transcendência de π. A existência de números transcendentes foi demonstrada pela primeira vez por Liouville em 1844. Liouville observou que os números algébricos não podem ser o limite de sucessões racionais que convergem "muito rapidamente". Por exemplo, o número $\sum_{n=1}^{\infty} 10^{-n!}$ não pode ser racional. Hermite, em 1873, mostrou que a base dos logaritmos naturais "e" é transcendente, e finalmente Lindemann, em 1882, mostrou por métodos análogos ao de Hermite que π é transcendente. Em 1874, Cantor deu um argumento (ver Exercícios 3 e 4 da Secção 7.1) mostrando que existem números transcendentes, sem recorrer à teoria dos limites.

(c) Conclua que um polígono regular de p lados só pode ser construído com régua e compasso se p é um número de Fermat.

7. Decida se um polígono regular de 9 lados pode ou não ser construído com régua e compasso.

7.3 Extensões de Decomposição

Seja K um corpo. Dado um polinómio $p(x) \in K[x]$ pretendemos encontrar uma extensão L de K onde $p(x)$ se decomponha em factores lineares. Como K não é *a priori* um subcorpo dum corpo algebricamente fechado, tal extensão, a existir, é, necessariamente, "abstracta". A construção de uma tal extensão é dada no seguinte teorema e é inspirada na construção de $\mathbb{C}$ a partir de $\mathbb{R}$ como um quociente $\mathbb{R}[x]/\langle x^2+1\rangle$.

Teorema 7.3.1. *Seja K um corpo e $p(x)$ um polinómio de grau $n \geq 1$. Existe uma extensão L de K onde $p(x)$ se decompõe num produto de termos lineares. Tal extensão pode ser tomada da forma*

$$L = K(r_1, \ldots, r_n),$$

onde $r_1, \ldots, r_n$ são as raízes de $p(x)$ em L.

Demonstração. Sem perda de generalidade podemos assumir que $p(x)$ é um polinómio mónico. Se l é o número de factores irredutíveis de $p(x)$, a demonstração é feita por indução em $n-l$.

Se $n-l=0$, então $p(x)$ é um produto de termos lineares, e as raízes de $p(x)$ pertencem a K, logo, o teorema é verdadeiro neste caso.

Suponha-se que $n-l>0$. Então existe um factor $q(x)$ de $p(x)$ irredutível de grau >1. O corpo $M = K[x]/\langle q(x)\rangle$ é uma extensão de K, contém a raiz $r = x+\langle q(x)\rangle$ de $q(x)$, e coincide com $K(r)$. Logo, em M, $q(x) = (x-r)\tilde{q}(x)$, e o polinómio $p(x)$ decompõe-se num produto de $\tilde{l}$ factores irredutíveis com $\tilde{l} > l$. Como $n-\tilde{l} < n-l$ podemos utilizar a hipótese de indução para encontrar uma extensão L de M em que $p(x)$ se decompõe num produto de factores lineares e que toma a forma

$$L = M(r_1, \ldots, r_n),$$

onde $r_1, \ldots, r_n$ são as raízes de $p(x)$ em L. Como a raiz r está entre as raízes $r_1, \ldots, r_n$, vemos que

$$\begin{aligned} L &= M(r_1, \ldots, r_n) \\ &= K(r)(r_1, \ldots, r_n) \\ &= K(r, r_1, \ldots, r_n) = K(r_1, \ldots, r_n). \end{aligned}$$

□

Este resultado motiva a seguinte definição.

Definição 7.3.2. Seja $p(x)$ um polinómio com coeficientes num corpo K. Uma EXTENSÃO DE DECOMPOSIÇÃO de $p(x)$ é uma extensão L de K em que:

(i) $p(x)$ decompõe-se em L num produto de termos de grau 1;

(ii) $L = K(r_1, \ldots, r_n)$ onde $r_1, \ldots, r_n$ são as raízes de $p(x)$ em L.

Analogamente, dizemos que uma extensão L de K é uma *extensão de decomposição de uma família de polinómios* $\{p_i(x)\}_{i\in I} \subset K[x]$ se (i) cada $p_i(x)$ se decompõe num produto de termos de grau 1, e (ii) L é gerada pelas raízes destes polinómios.

Por vezes, em vez de *extensão de decomposição*, utilizamos a expressão *corpo de decomposição*, sendo claro, do contexto, o corpo base em que se trabalha. Veremos na próxima secção que duas extensões de decomposição de um polinómio $p(x)$ são necessariamente isomorfas.

A demonstração do Teorema 7.3.1 fornece um algoritmo para a construção de uma extensão de decomposição de um polinómio que pode ser utilizado de forma prática como se ilustra nos exemplos seguintes.

Exemplos 7.3.3.

1. *Consideremos um polinómio $p(x) = x^2+bx+c$ com coeficientes num corpo K. Se $p(x)$ é redutível, então K é um corpo de decomposição de $p(x)$. Suponha-se que $p(x)$ é irredutível. Então $K[x]/\langle p(x)\rangle$ é uma extensão de K, $r_1 = x-\langle p(x)\rangle$ é uma raiz de $p(x)$, e $K[x]/\langle p(x)\rangle = K(r_1)$. Em $K(r_1)$ temos $x^2 + bx + c = (x - r_1)(x - r_2)$, logo, $K(r_1) = K(r_1, r_2)$ é um corpo de decomposição de $x^2 + bx + c$ e $[K(r_1, r_2) : K] = 2$.*

2. *Num exemplo acima mostrámos que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{C}$ é um corpo de decomposição de $(x^2 - 2)(x^2 - 3)$ e que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.*

3. *O polinómio $p(x) = x^p-1$ (p primo) possui a raiz $r_0 = 1$ em $\mathbb{Q}$, logo, $x^p-1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1)$. O polinómio $x^{p-1} + x^{p-2} + \cdots + 1$ é irredutível em $\mathbb{Q}$ (exercício). Seja $r \in \mathbb{Q}[x]/\langle x^{p-1} + x^{p-2} + \cdots + 1\rangle$ o elemento $x+\langle x^{p-1} + x^{p-2} + \cdots + 1\rangle$. Em $\mathbb{Q}(r)$ temos que $(r^k)^p = r^{kp} = 1$, e que $r, r^2, \ldots, r^{p-1}$ são elementos distintos, donde $x^p - 1 = \prod_{i=1}^{p}(x - r^i)$. Concluímos que $\mathbb{Q}(r)$ é um corpo de decomposição de $x^p - 1$ e que $[\mathbb{Q}(r) : \mathbb{Q}] = p-1$. Se $z \in \mathbb{C}$ é uma raiz complexa de $x^p - 1$ distinta de 1, verifica-se facilmente que $\mathbb{Q}(z)$ é isomorfo a $\mathbb{Q}(r)$.*

4. *O polinómio $p(x) = x^3 + x^2 + 1$ é irredutível sobre $\mathbb{Z}_2[x]$. De facto, $p(x)$ não tem raízes em $\mathbb{Z}_2$, já que $p(0) = 0 + 0 + 1 = 1$ e $p(1) = 1 + 1 + 1 \equiv 1 \pmod 2$. O corpo $\mathbb{Z}_2[x]/\langle x^3 + x^2 + 1\rangle$ é uma extensão de $\mathbb{Z}_2$ em que $p(x)$ possui a raiz $r = x + \langle x^3 + x^2 + 1\rangle$, logo neste corpo temos a factorização $p(x) = (x - r)(x^2 + bx + c)$. Por comparação de termos, vemos que $b = 1 + r$ e $c = r^2 + r$. Usando as relações $r^3 = r^2 + 1$ e $r^4 = r^2 + r + 1$ verificamos por substituição que r^2 é uma raiz de $x^2 + (r + 1)x + (r^2 + r)$, logo, $p(x)$*

decompõe-se em factores lineares em $\mathbb{Z}_2(r)[x]$. *Concluímos que* $\mathbb{Z}_2(r)$ *é um corpo de decomposição de* x^3+x^2+1 *sobre* $\mathbb{Z}_2$, *e que* $[\mathbb{Z}_2(r):\mathbb{Z}_2]=3$.

5. *O polinómio* $p(x)=x^3-2$ *é irredutível sobre* $\mathbb{Q}$. *Formemos a extensão* $L=\mathbb{Q}[x]/\langle x^3-2\rangle$, *e seja* $r_1=x+\langle x^3-2\rangle$. *Esta extensão é da forma* $L=\mathbb{Q}(r_1)$, *e em* L *o polinómio* x^3-2 *admite a factorização* $(x-r_1)(x^2+r_1x+{r_1}^2)$. *O polinómio* $x^2+r_1x+{r_1}^2$ *é irredutível sobre* $\mathbb{Q}(r_1)$ *(exercício), logo, podemos formar uma nova extensão* $M=\mathbb{Q}(r_1)[x]/\langle x^2+r_1x+{r_1}^2\rangle$. *Designando por* r_2 *o elemento* $x+\langle x^2+r_1x+{r_1}^2\rangle$ *desta extensão, vemos que* $M=\mathbb{Q}(r_1,r_2)$. *Em* $\mathbb{Q}(r_1,r_2)[x]$ *temos a factorização* $x^3-2=(x-r_1)(x-r_2)(x-r_3)$, *logo,* $\mathbb{Q}(r_1,r_2)=\mathbb{Q}(r_1,r_2,r_3)$ *é um corpo de decomposição de* x^3-2. *Pela Proposição 7.1.3 concluímos que* $[\mathbb{Q}(r_1,r_2,r_2):\mathbb{Q}]=3\cdot 2=6$.

Como já referimos anteriormente, o corpo de decomposição $\mathbb{Q}(r_1,\ldots,r_n)$ de um polinómio $p(x)=a_nx^n+\cdots+a_1x+a_n\in\mathbb{Q}[x]$ pode ser sempre realizado como um subcorpo do corpo $\mathbb{C}$ dos números complexos, pois $\mathbb{C}$ é uma extensão algebricamente fechada de $\mathbb{Q}$. É interessante constatar que para qualquer corpo existe uma extensão algebricamente fechada.

Teorema 7.3.4. *Seja* K *um corpo. Existe uma extensão algebricamente fechada de* K.

Demonstração. Dividimos a demonstração em quatro passos:

(a) Existe uma extensão L_1 de K em que todo o polinómio de $K[x]$ com grau ≥ 1 tem uma raiz: Para cada $p(x)\in K[x]$ com grau ≥ 1 escolha-se uma indeterminada x_p, e designe-se por S o conjunto de todas estas indeterminadas. No anel $K[S]$ os polinómios $p(x_p)$[5] geram um ideal próprio. De facto, suponha-se que

$$g_1p_1(x_{p_1})+\cdots+g_mp_m(x_{p_m})=1, \tag{7.3.1}$$

para alguns $g_i=g_i(x_{p_1},\ldots,x_{p_m})\in K[S]$. Existe uma extensão M de K onde os polinómios $p_1,\ldots,p_m$ possuem raízes $\alpha_1,\ldots,\alpha_m$ (exercício), logo, substituindo $x_{p_i}\mapsto\alpha_i$ em (7.3.1) obtemos $0=1$, o que é uma contradição. Existe, pois, um ideal maximal I de $K[S]$ que contém os polinómios $p(x_p)$. O corpo $L_1\equiv K[S]/I$ é então a extensão pretendida.

(b) Usando (a), podemos construir, por indução, uma cadeia $L_1\subset L_2\subset\ldots\subset L_n\subset\ldots$ de extensões de K em que, para todo o k, um polinómio em $L_k[x]$ de grau ≥ 1 possui uma raiz em L_{k+1}.

(c) Seja $L\equiv\cup_iL_i$. Então L é um corpo: se $a,b\in L$, existe um k tal que $a,b\in L_k$, e define-se $a+b$ e ab como sendo a soma e o produto em L_k. Esta definição é independente de k, pois os L_i são extensões sucessivas.

[5] Não confundir $p(x)$ com $p(x_p)$!

(d) O corpo L é uma extensão algebricamente fechada: se $p(x) \in L[x]$ tem grau ≥ 1, então os coeficientes de $p(x)$ pertencem a L_k, para algum k. Logo, $p(x) \in L_k[x]$, donde $p(x)$ possui uma raiz em L_{k+1} e, portanto, em L.

□

Corolário 7.3.5. *Seja K um corpo. Existe uma extensão $\tilde{L}$ algébrica sobre K e algebricamente fechada.*

Demonstração. Seja L uma extensão algebricamente fechada de K, e designemos por $\tilde{L}$ o conjunto dos elementos de L algébricos sobre K. É fácil verificar que $\tilde{L}$ é um subcorpo de L (que é obviamente uma extensão algébrica de K) algebricamente fechado. □

A uma extensão algebricamente fechada e algébrica sobre K, chama-se FECHO ALGÉBRICO de K. Para o fecho algébrico de K usamos o símbolo $\bar{K}^a$. Veremos na próxima secção que as extensões algebricamente fechadas, algébricas sobre K, são todas isomorfas, logo, esta notação não é ambígua.

A existência de um corpo de decomposição de um polinómio (Teorema 7.3.1) pode ser facilmente demonstrada com recurso ao fecho algébrico, embora isto não seja útil, pois a demonstração da existência do fecho algébrico recorre precisamente ao Teorema 7.3.1. No entanto, podemos agora demonstrar a existência de um corpo de decomposição de uma família arbitrária de polinómios.

Corolário 7.3.6. *Seja $\{p_i(x)\}_{i\in I} \subset K[x]$ uma família de polinómios. Existe uma extensão de decomposição L da família $\{p_i(x)\}_{i\in I}$.*

Demonstração. No fecho algébrico $\bar{K}^a$, basta tomar para L o subcorpo gerado pelas raízes dos polinómios $\{p_i(x)\}_{i\in I}$. □

A fechar esta secção consideramos a questão inversa: dada uma extensão L de K quando é que L é uma extensão de decomposição de uma família de polinómios com coeficientes em K?

Definição 7.3.7. Seja L uma extensão algébrica de K. Diz-se que L é uma EXTENSÃO NORMAL de K se todo o polinómio irredutível de $K[x]$ que possui uma raiz em L se decompõe num produto de termos lineares em $L[x]$.

Exemplos 7.3.8.

1. *$\mathbb{Q}(\sqrt{2})$ é uma extensão normal de $\mathbb{Q}$. Verificamos este facto mostrando que, se $p(x) \in \mathbb{Q}[x]$ é um polinómio irredutível com uma raiz $r = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, então $p(x)$ é um múltiplo do polinómio mínimo de r, e este decompõe-se num produto de termos lineares em $\mathbb{Q}(\sqrt{2})$. Seja $q(x) = (x-a)^2 - 2b^2 \in \mathbb{Q}[x]$ o polinómio mínimo da raiz r. Então $q(x)|p(x)$. Sendo $p(x)$ irredutível sobre $\mathbb{Q}$, vemos que $p(x) = \lambda q(x)$, para algum $\lambda \in \mathbb{Q}$. Finalmente, em $\mathbb{Q}(\sqrt{2})$ temos $p(x) = c(x - a - b\sqrt{2})(x - a + b\sqrt{2})$.*

2. $\mathbb{Q}(\sqrt[4]{2})$ *não é uma extensão normal de* $\mathbb{Q}$*. De facto, o polinómio* $x^4 - 2$ *é irredutível sobre* $\mathbb{Q}$*, possui a raiz* $\sqrt[4]{2}$ *em* $\mathbb{Q}(\sqrt[4]{2})$*, mas não se decompõe em factores lineares em* $\mathbb{Q}(\sqrt[4]{2})$*, pois este corpo não contém as raízes imaginárias de* $x^4 - 2$*.*

O último exemplo sugere que deve existir uma relação entre extensões de decomposição e extensões normais. A proposição seguinte esclarece completamente esta questão.

Proposição 7.3.9. *Seja* L *uma extensão algébrica de* K*, contida no fecho algébrico* $\bar{K}^a$*. As seguintes afirmações são equivalentes:*

(i) L *é uma extensão normal de* K*.*

(ii) L *contém um corpo de decomposição do polinómio mínimo de qualquer* $u \in L$*.*

(iii) L *é uma extensão de decomposição de uma família de polinómios* $\{p_i(x)\}_{(i \in I)} \subset K[x]$*.*

(iv) Todo o monomorfismo $\phi : L \to \bar{K}^a$ *que fixa* K *(*$\phi|_K = id$*) é um automorfismo de* L*,* i.e.*,* $\phi(L) = L$*.*

Diferimos a demonstração desta proposição para a próxima secção. Um corolário imediato é o seguinte:

Corolário 7.3.10. *Uma extensão* L *de* K *é uma extensão de decomposição de um polinómio* $p(x) \in K[x]$ *se e só se* L *é uma extensão normal de* K *de dimensão finita.*

Vimos acima um exemplo de uma extensão simples que não é normal. Se uma extensão algébrica não é normal, podemos tentar remediar a situação procurando uma extensão normal que não seja "muito grande".

Proposição 7.3.11. *Seja* L *uma extensão algébrica de* K*. Existe uma extensão* $\tilde{L}$ *de* L *que satisfaz:*

(i) $\tilde{L}$ *é uma extensão normal de* K*.*

(ii) Se M *é uma extensão normal de* K *tal que* $L \subset M \subset \tilde{L}$*, então* $M = \tilde{L}$*.*

(iii) $[\tilde{L} : K] < \infty$ *se e só se* $[L : K] < \infty$*.*

Demonstração. Seja $S = \{u_i : i \in I\}$ uma base de L sobre K e designe-se para cada $i \in I$ por $p_i(x)$ o polinómio mínimo de u_i. Tomamos para $\tilde{L}$ uma extensão de decomposição para a família de polinómios $\{p_i(x)\}_{i \in I}$. Então $\tilde{L}$ é uma extensão normal de K (Proposição 7.3.9), e (i) é satisfeita. Como qualquer extensão normal de K deve conter uma extensão de decomposição

do polinómio mínimo de qualquer dos seus elementos (Proposição 7.3.9), concluímos que $\tilde{L}$ é a menor extensão normal de K que contém L, logo (ii) é satisfeita. Finalmente (iii) é verdadeira, pois se $[L : K] < \infty$, então I é finito e podemos substituir a família de polinómios $\{p_i(x)\}_{i\in I}$ pelo polinómio $p(x) = \prod_{i\in I} p_i(x)$, logo $[\tilde{L} : K] < \infty$. Inversamente, se $[\tilde{L} : K] < \infty$, então, pela Proposição 7.1.3, $[L : K] < \infty$. □

Da unicidade de extensão de decomposição decorre que a extensão $\tilde{L}$ dada na proposição anterior é única a menos de um isomorfismo sobre K. A uma tal extensão chamamos FECHO NORMAL de L, e usamos a notação $\bar{L}^n$.

Exemplo 7.3.12.

Vimos num exemplo acima que $L = \mathbb{Q}(\sqrt[4]{2})$ não é uma extensão normal de $K = \mathbb{Q}$. É fácil verificar que o fecho normal desta extensão é $\bar{L}^n = \mathbb{Q}(\sqrt[4]{2}, i)$.

Exercícios.

1. Seja $L = \mathbb{Q}[x]/\langle x^3 - 2\rangle$ e $r = x + \langle x^3 - 2\rangle \in L$. Mostre que o polinómio $x^2 + rx + r^2$ é irredutível sobre L.

2. Demonstre a seguinte extensão do Teorema 7.3.1: Sejam $p_1(x), \ldots, p_m(x) \in K[x]$ polinómios com coeficientes num corpo K. Existe uma extensão de decomposição dos polinómios $p_1(x), \ldots, p_m(x)$.

3. Para os seguintes polinómios sobre $\mathbb{Q}$ construa extensões de decomposição e determine a sua dimensão:

   (a) $x^2 + x + 1$;

   (b) $(x^3 - 2)(x^2 - 1)$;

   (c) $x^6 + x^3 + 1$;

   (d) $x^5 - 7$.

4. Considere o polinómio $x^3 - 3$. Determine uma extensão de decomposição e a sua dimensão sobre cada um dos seguintes corpos:

   (a) $\mathbb{Q}$;

   (b) $\mathbb{Z}_3$;

   (c) $\mathbb{Z}_5$.

5. Se $p(x) \in K[x]$ é um polinómio de grau n, e L é uma extensão de decomposição de $p(x)$, mostre que $[L : K] \mid n!$.

6. Determine uma extensão de decomposição do polinómio $x^{p^n} - 1$ sobre o corpo $\mathbb{Z}_p$.

7. Se L é uma extensão de K e $[L : K] = 2$, mostre que L é uma extensão normal de K.

8. Vimos num exemplo que $\mathbb{Q}(\sqrt[4]{2})$ não é uma extensão normal de $\mathbb{Q}$. Mostre que $\mathbb{Q}(\sqrt[4]{2})$ é uma extensão normal de $\mathbb{Q}(\sqrt{2})$. Conclua que, se $M \supset L \supset K$ são extensões sucessivas com M normal sobre L e L normal sobre K, pode acontecer que M não seja normal sobre K.

9. Mostre que, se $M \supset L \supset K$ são extensões sucessivas e M é normal sobre K, então M é normal sobre L.

7.4 Homomorfismos de Extensões

Seja L_1 uma extensão de K_1, e L_2 uma extensão de K_2. Um HOMOMORFISMO DE EXTENSÕES $\phi : L_1 \to L_2$ é um homomorfismo tal que $\phi(K_1) \subset K_2$. Quando $K_1 = K_2 = K$ e $\phi|_K = id$ dizemos que ϕ é um HOMOMORFISMO SOBRE K ou ainda que ϕ é um K-HOMOMORFISMO[6]. A noção de homomorfismo de extensões é crucial para a definição de grupo de Galois.

Nesta secção consideramos a seguinte questão: Dado um isomorfismo de corpos $\phi : K_1 \to K_2$, é possível prolongar ϕ a um isomorfismo de extensões $\Phi : L_1 \to L_2$? Ao estudarmos esta questão mostraremos a unicidade dos fechos algébrico e normal, bem como de extensão de decomposição, a menos de um isomorfismo.

Recordemos que, se $\phi : K_1 \to K_2$ é um homomorfismo de corpos, dado um polinómio $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in K_1[x]$, designa-se por $p^\phi(x)$ o polinómio $\phi(a_n)x^n + \cdots + \phi(a_1)x + \phi(a_0) \in K_2[x]$.

Proposição 7.4.1. *Seja $\phi : K_1 \to K_2$ um isomorfismo de corpos, L_1 e L_2 extensões de K_1 e K_2, e $r \in L_1$ um elemento algébrico sobre K_1 com polinómio mínimo $p(x)$. O isomorfismo ϕ pode ser prolongado num monomorfismo de extensões $\Phi : K_1(r) \to L_2$ se e só se o polinómio $p^\phi(x)$ tem uma raiz em L_2. O número de prolongamentos é igual ao número de raízes distintas de $p^\phi(x)$ em L_2.*

Demonstração. Seja s uma raiz de $p^\phi(x)$ em L_2. Deixamos como exercício verificar que existe um único homomorfismo de corpos $\Phi : K_1(r) \to L_2$ tal que $\Phi|_{K_1} = \phi$ e $\Phi(r) = s$.

Por outro lado, se Φ é um prolongamento de ϕ, então $p^\phi(\Phi(r)) = \Phi(p(r))$ $= \Phi(0) = 0$, logo $p^\phi(x)$ tem uma raiz em L_2. □

O próximo resultado responde à questão posta no início desta secção no caso de extensões de decomposição.

[6]Recorde-se que um homomorfismo de corpos é necessariamente um monomorfismo, logo nestas definições podemos substituir "homomorfismo" por "monomorfismo".

Teorema 7.4.2. *Seja $\phi : K_1 \to K_2$ um isomorfismo de corpos, $p(x) \in K_1[x]$ um polinómio, e $p^\phi(x)$ o correspondente polinómio em $K_2[x]$. Se L_1 e L_2 são extensões de decomposição de $p(x)$ e $p^\phi(x)$, respectivamente, existe um isomorfismo $\Phi : L_1 \to L_2$ que prolonga ϕ. O número de tais prolongamentos é $\leq [L_1 : K_1]$, e é precisamente $[L_1 : K_1]$ quando $p^\phi(x)$ tem raízes distintas em L_2.*

Demonstração. A demonstração é por indução em $[L_1 : K_1]$.

Se $[L_1 : K_1] = 1$, então $p(x) = a_n \prod_{i=1}^n (x - r_i)$, onde $r_i \in K_1 = L_1$. Temos também $p^\phi(x) = \phi(a_n) \prod_{i=1}^n (x - \phi(r_i))$. Como as raízes de um polinómio geram o seu corpo de decomposição concluímos que $L_2 = K_2$, logo, existe apenas $[L_1 : K_1] = 1$ prolongamento.

Suponha-se que $[L_1 : K_1] > 1$. Então $p(x)$ possui um factor irredutível $q(x)$ com grau ≥ 1. Seja r uma raiz de $q(x)$ em L_1. Pela Proposição 7.4.1 o isomorfismo $\phi : K_1 \to K_2$ pode ser prolongado num monomorfismo $\tilde{\phi} : K_1(r) \to L_2$ e existem tantos prolongamentos quantas as raízes distintas de $q^\phi(x)$ em L_2. Podemos considerar L_1 e L_2 como corpos de decomposição de $p(x)$ e $p^\phi(x)$ sobre $K_1(r)$ e $\tilde{\phi}(K_1(r))$, respectivamente. Como $[L_1 : K_1(r)] = [L_1 : K_1]/[K_1(r) : K_1] = [L_1 : K_1]/\deg q(x) < [L_1 : K_1]$, podemos utilizar a hipótese de indução para prolongar $\tilde{\phi}$ num isomorfismo $\Phi : L_1 \to L_2$, e o número de prolongamentos é $\leq [L_1 : K_1(r)]$ e é precisamente $[L_1 : K_1(r)]$ se $p^\phi(x)$ tem raízes distintas em L_2. Combinando estes resultados, vemos que Φ é um prolongamento de ϕ, e o número de prolongamentos de Φ deste tipo é precisamente $[L_1 : K_1(r)] \cdot \deg q(x) = [L_1 : K_1(r)] \cdot [K_1(r) : K_1] = [L_1 : K_1]$, se $p^\phi(x)$ tem raízes distintas em L_2.

Finalmente, observe-se que obtemos todos os prolongamentos de ϕ se prolongarmos primeiro a $K_1(r)$ e depois a L_1. De facto, se Φ é um prolongamento de ϕ a L_1, então a sua restrição a $K_1(r)$ fornece um monomorfismo $K_1(r) \to L_2$, que é necessariamente um dos prolongamentos de ϕ fornecido pela Proposição 7.4.1. □

Se neste teorema tomarmos $K_1 = K_2 = K$ e $\phi = id$, obtemos:

Corolário 7.4.3. *Seja $p(x)$ um polinómio sobre um corpo K. Duas extensões de decomposição de $p(x)$ são necessariamente isomorfas.*

Exemplo 7.4.4.

Num exemplo da secção anterior construímos uma extensão de decomposição (abstracta) $L_1 = \mathbb{Q}(r_1, r_2, r_3)$ de $x^3 - 2$. Podemos construir uma outra extensão de decomposição L_2 considerando o subcorpo de $\mathbb{C}$ gerado por $\mathbb{Q}$ e $\sqrt[3]{2}$, $\sqrt[3]{2}/2(-1 \pm i\sqrt{3})$ (as raízes de $x^3 - 2$ em $\mathbb{C}$). Existem isomorfismos $L_1 \to L_2$ sobre $\mathbb{Q}$ que transformam r_1, r_2, r_3 em qualquer uma das raízes $\sqrt[3]{2}$, $\sqrt[3]{2}/2(-1 \pm i\sqrt{3})$.

Passemos agora ao caso de extensões algébricas arbitrárias.

Teorema 7.4.5. *Seja $\phi : K_1 \to K_2$ um isomorfismo de corpos, L_1 uma extensão algébrica de K_1 e L_2 uma extensão algebricamente fechada de K_2. Existe um monomorfismo $\Phi : L_1 \to L_2$ que prolonga ϕ. Se L_1 é algebricamente fechada e L_2 é algébrica sobre K_2, então Φ é um isomorfismo de L_1 com L_2.*

Demonstração. Consideremos o conjunto $\mathcal{P}$ dos pares ordenados (N, τ) onde $N \subset L_1$ é uma extensão de K_1, e $\tau : M \to L_2$ é um monomorfismo que prolonga ϕ. Definimos uma relação de ordem parcial em $\mathcal{P}$ da seguinte forma: $(N_1, \tau_1) \leq (N_2, \tau_2)$ se e só se $N_1 \subset N_2$ e $\tau_2|N_1 = \tau_1$. O conjunto $\mathcal{P}$ é não-vazio (contém o par (K_1, ϕ)), e qualquer cadeia $\{(N_i, \tau_i)\}_{i\in I}$ de elementos de $\mathcal{P}$ é majorada pelo par (N, τ), onde $N \equiv \cup_i N_i$ e $\tau|_{N_i} \equiv \tau_i$. Pelo Lema de Zorn existe em $\mathcal{P}$ um elemento maximal (M, Φ).

Vejamos que $M = L_1$, de forma que Φ é o prolongamento desejado. De facto suponha-se que existe $r \in L_1 - M$. Então podemos formar a extensão $M(r)$ e, pela Proposição 7.4.1, existe um prolongamento $\tilde{\Phi} : M(r) \to L_2$. A existência do par $(M(r), \tilde{\Phi})$ contradiz a maximalidade de (M, Φ), logo $L_1 = M$.

Finalmente, se L_1 é algebricamente fechado, então $\Phi(L_1)$ é algebricamente fechado. Se L_2 é algébrico sobre K_2, necessariamente $L_2 \subset \Phi(L_1)$, logo, Φ é sobrejectivo. □

Podemos agora mostrar a unicidade de fecho algébrico e de extensão de decomposição de uma família de polinómios arbitrária.

Corolário 7.4.6. *Seja K um corpo, L e $\tilde{L}$ extensões algebricamente fechadas, algébricas sobre K. Existe um K-isomorfismo $\Phi : L \to \tilde{L}$.*

Demonstração. Basta tomar no teorema $K_1 = K_2 = K$ e $\phi = id$. □

Corolário 7.4.7. *Seja $\{p_i(x)\}_{i\in I}$ uma família de polinómios sobre K. Quaisquer duas extensões de decomposição da família $\{p_i(x)\}_{i\in I}$ são isomorfas.*

Por sua vez, a unicidade do fecho normal de uma extensão L de K decorre da Proposição 7.3.9 cuja demonstração fornecemos de seguida.

Demonstração da Proposição 7.3.9. Mostramos as implicações (i) ⇒ (ii) ⇒ (iii) ⇒ (iv) ⇒ (i).

(i) ⇒ (ii): Seja $r \in L$ e designe-se por $p(x) \in K[x]$ o polinómio mínimo de r. Como L é normal e $p(r) = 0$, $p(x)$ decompõe-se num produto $\prod_{i=1}^{n}(x - r_i)$. O subcorpo $K(r_1, \ldots, r_n) \subset L$ é claramente um corpo de decomposição de $p(x)$.

(ii) ⇒ (iii): L é uma extensão de decomposição da família $\{p_r(x)\}_{r\in L}$, onde $p_r(x)$ é o polinómio mínimo do elemento $r \in L$.

(iii) ⇒ (iv): Seja $r \in L \subset \bar{K}^a$ uma raiz de um polinómio $p_i(x)$. Então $\phi(r)$ é também uma raiz de $p_i(x)$, pois $\phi|K = id$. Como as raízes da família $\{p_i(x)\}_{i\in I}$ geram o corpo L, concluímos que $\phi(L) = L$.

(iv) $\Rightarrow$ (i): Seja $p(x) \in K[x]$ um polinómio irredutível com raiz $r \in L$. Se $\tilde{r} \in \bar{K}^a$ é outra raiz de $p(x)$ a aplicação $\phi : K(r) \to K(\tilde{r}) \subset \bar{K}^a$ que transforma $r \mapsto \tilde{r}$ e é a identidade em K, é um monomorfismo sobre K que pode ser estendido a L. Mas então $\tilde{r} = \phi(r) \in L$, donde todas as raízes de $p(x)$ pertencem a L, e $p(x)$ decompõe-se num produto de termos lineares em $L[x]$. Logo, L é uma extensão normal de K. □

Exercícios.

1. Seja $\phi : K_1 \to K_2$ um isomorfismo de corpos, L_1 e L_2 extensões de K_1 e K_2, e $r \in L_1$ um elemento algébrico sobre K_1 com polinómio mínimo $p(x)$. Se s é uma raiz de $p^{\phi}(x)$ em L_2, mostre que existe um único homomorfismo de corpos $\Phi : K_1(r) \to L_2$ tal que $\Phi|_{K_1} = \phi$ e $\Phi(r) = s$.

2. Considere as extensões $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i, \sqrt{2}) \subset \mathbb{C}$ de $\mathbb{Q}$.

   (a) Mostre que $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{2})$ são isomorfas como espaços vectoriais sobre $\mathbb{Q}$, mas não são corpos isomorfos;

   (b) Determine todos os $\mathbb{Q}$-automorfismos de $\mathbb{Q}(i, \sqrt{2})$.

3. Seja r uma raiz de $x^6 + x^3 + 1$. Determine todos os $\mathbb{Q}$-homomorfismos $\Phi : \mathbb{Q}(r) \to \mathbb{C}$.
   (Sugestão: $x^6 + x^3 + 1$ é um factor de $x^9 - 1$.)

4. Determine todos os $\mathbb{Z}_2$-automorfismos da extensão de decomposição do polinómio $x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$.

5. Mostre que uma extensão algébrica L de K é uma extensão normal se e só se todo o polinómio irredutível de $K[x]$ se decompõe em $L[x]$ num produto de factores irredutíveis em que todos os factores possuem o mesmo grau.

7.5 Separabilidade

Veremos nas próximas secções que os K-automorfismos de uma extensão L de K desempenham um papel fundamental na Teoria de Galois. Por um resultado da secção anterior, a contagem do número de K-automorfismos depende do número de raízes distintas de certos polinómios. Nesta secção estudamos a possibilidade de um polinómio ter raízes múltiplas, estabelecendo um critério para a sua existência.

Seja $p(x) \in K[x]$ um polinómio. Em $\bar{K}^a[x]$, $p(x)$ decompõe-se num produto de termos lineares. Se $r \in \bar{K}^a$ é uma raiz de $p(x)$, chama-se *multiplicidade* de r ao maior inteiro k tal que $(x - r)^k \mid p(x)$. Dizemos que uma raiz é *simples* se $k = 1$, e que é *múltipla* se $k > 1$.

A fim de fornecer um critério de decisão para a existência de raízes múltiplas, necessitamos da noção de *derivada formal* de um polinómio. Esta

noção de derivada coincide com a noção usual nos casos em que o polinómio pode ser visto como uma função de variável real ou complexa.

Definição 7.5.1. Seja K um corpo. O OPERADOR DE DERIVAÇÃO FORMAL de $K[x]$ é a única aplicação $D : K[x] \to K[x]$ que satisfaz as seguintes propriedades:

(i) **Linearidade:** $D(p(x) + q(x)) = D(p(x)) + D(q(x))$ e $D(a \cdot p(x)) = a \cdot D(p(x))$.

(ii) **Regra de Leibniz:** $D(p(x)q(x)) = D(p(x))q(x) + p(x)D(q(x))$.

(iii) **Normalização:** $D(x) = 1$.

Verificamos facilmente que existe apenas um operador que satisfaz estas propriedades. De facto, se $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$, então por aplicação sucessiva de (i), (ii) e (iii), obtemos

$$D(p(x)) = na_n x^{n-1} + \cdots + 2a_2 x + a_1. \tag{7.5.1}$$

Escrevemos frequentemente $p'(x)$ em vez de $D(p(x))$.

Teorema 7.5.2. *Seja $p(x) \in K[x]$ um polinómio mónico de grau ≥ 1. As raízes de $p(x)$ em $\bar{K}^a$ são simples se e só se* $\mathrm{mdc}(p(x), p'(x)) = 1$.

Demonstração. Se $r \in \bar{K}^a$ é uma raiz múltipla de $p(x)$, então $p(x) = (x - r)^k q(x)$, onde $k > 1$ e $q(x) \in \bar{K}^a[x]$. Diferenciando:

$$p'(x) = (x - r)^k q'(x) + k(x - r)^{k-1} q(x),$$

logo vemos que $(x - r)^{k-1} \mid p'(x)$, e $(x - r)$ é um factor comum a $p(x)$ e $p'(x)$. Concluímos que, se $\mathrm{mdc}(p(x), p'(x)) = 1$, então $p(x)$ não tem raízes múltiplas.

Suponha-se agora que todas as raízes de $p(x)$ são simples. Então em $\bar{K}^a[x]$ temos $p(x) = (x - r_1)(x - r_2) \cdots (x - r_n)$, onde os r_i são todos distintos. Por diferenciação obtemos

$$p'(x) = \sum_{i=1}^{n} (x - r_1) \cdots (x - r_{i-1})(x - r_{i+1}) \cdots (x - r_n),$$

donde se conclui que $(x - r_i) \nmid p'(x)$. Logo, $\mathrm{mdc}(p(x), p'(x)) = 1$. □

Observe-se que a aplicação deste critério não requere o conhecimento do fecho algébrico $\bar{K}^a$ ou de um corpo de decomposição de $p(x)$. De facto, o cálculo de $\mathrm{mdc}(p(x), q(x))$ é independente da extensão em que se consideram os coeficientes dos polinómios $p(x)$ e $q(x)$.

Definição 7.5.3. Chamamos a $p(x) \in K[x]$ um POLINÓMIO SEPARÁVEL se os seus factores irredutíveis não têm raízes múltiplas. Um CORPO PERFEITO é um corpo K em que todos os polinómios de $K[x]$ são separáveis.

O teorema acima tem o seguinte corolário.

Corolário 7.5.4. *Um corpo de característica 0 é perfeito.*

Demonstração. Se, por absurdo, $p(x)$ é um polinómio mónico irredutível que satisfaz $\mathrm{mdc}(p(x), p'(x)) \neq 1$, então $p(x) \mid p'(x)$. Sendo $\deg p'(x) < \deg p(x)$, vemos que $p'(x) = 0$. Como a característica de K é 0, a fórmula (7.5.1) para a derivada mostra que $p(x) \in K$, o que é uma contradição. □

Esta demonstração falha em característica p, pois a condição $q'(x) = 0$ implica apenas $q(x) = a_0 + a_1x^p + a_2x^{2p} + \ldots$. Num exercício no final desta secção damos um exemplo dum polinómio não separável (necessariamente em característica $p \neq 0$). O estudo da separabilidade para corpos com característica $p \neq 0$ baseia-se no lema seguinte:

Lema 7.5.5. *Se K tem característica $p \neq 0$ e $a \in K$, então o polinómio $x^p - a$ ou é irredutível ou é da forma $(x-b)^p$, $b \in K$.*

Demonstração. Suponha-se que $x^p - a = g(x)h(x)$, onde $g(x)$ e $h(x)$ são polinómios mónicos, e seja $b \in \bar{K}^a$ uma raiz de $x^p - a$. Então

$$(x-b)^p = \sum_{k=0}^{p} \binom{p}{k} x^k (-b)^{p-k} = x^p - b^p = x^p - a,$$

pois para $0 < k < p$ os coeficientes $\binom{p}{k}$ são divisíveis por p. Logo $g(x) = (x-b)^k$ e necessariamente $b^k \in K$. Como $\mathrm{mdc}(k, p) = 1$, existem inteiros $r, s \in \mathbb{Z}$ tais que $rk + sp = 1$, donde vemos que $b = b^{rk+sp} = (b^k)^r + (b^p)^s \in K$. Isto mostra que $x^p - a = (x-b)^p, b \in K$. □

Teorema 7.5.6. *Um corpo K de característica $p \neq 0$ é perfeito se e só se $K = K^p$, onde K^p designa o subcorpo de K formado por todas as potências a^p, com $a \in K$.*

Demonstração. Seja $a \in K - K^p$. Então, pelo Lema 7.5.5, $x^p - a$ é irredutível e, como $(x^p - a)' = px^{p-1} = 0$, este polinómio não é separável. Logo se $K \neq K^p$ então K não é perfeito.

Inversamente, suponha-se que K não é perfeito, de forma que existe $q(x) \in K[x]$ irredutível e não-separável. Então, como $q'(x) = 0$, temos que $q(x) = a_0 + a_1x^p + a_2x^{2p} + \ldots$. Pelo menos um $a_i \notin K^p$, pois se $a_j = b_j{}^p$ para todo o j, então $q(x) = (b_0 + b_1x + b_2x^2 + \ldots)^p$, contrariando a hipótese de $q(x)$ ser irredutível. Logo, $K \neq K^p$. □

Se K é um corpo de característica $p \neq 0$, o monomorfismo $\phi : K \to K$ que transforma $a \mapsto a^p$ chama-se MONOMORFISMO DE FROBENIUS. Assim, o teorema acima afirma que K é perfeito se e só se o monomorfismo de Frobenius é um automorfismo.

Corolário 7.5.7. *Se K é finito de característica $p \neq 0$, então K é um corpo perfeito.*

Demonstração. Se K é finito, o monomorfismo de Frobenius é sobrejectivo. □

Na maior parte dos exemplos que apresentaremos para ilustrar a Teoria de Galois, os corpos de base em questão serão perfeitos. Quando pretendemos que um resultado da Teoria de Galois seja ainda válido quando o corpo base não é um corpo perfeito, necessitamos de uma hipótese adicional que é traduzida pela seguinte definição:

Definição 7.5.8. Seja L uma extensão de K.

(i) Chama-se a $u \in L$ ELEMENTO SEPARÁVEL sobre K se u é algébrico sobre K, e o polinómio mínimo de u é separável.

(ii) Chama-se a L EXTENSÃO SEPARÁVEL sobre K se todos os elementos de L são separáveis sobre K.

Seja L uma extensão algébrica de K. O *grau de separabilidade* de L sobre K, designado por $[L : K]_s$, é o cardinal do conjunto $\{\phi : L \to \bar{K}^a\}$ dos K-homomorfismos de L para o fecho algébrico $\bar{K}^a$. Note que o grau de separabilidade é independente do fecho algébrico utilizado na sua definição.

Proposição 7.5.9 (Propriedades de separabilidade). *Seja K um corpo.*

(i) Se $M \supset L \supset K$ são extensões algébricas sucessivas, então

$$[M : K]_s = [M : L]_s \cdot [L : K]_s.$$

(ii) Se L é uma extensão de dimensão finita sobre K, então $[L : K]_s \leq [L : K]$, e a igualdade ocorre precisamente se L é separável sobre K.

(iii) Se $L = K(u_1, \ldots, u_m)$, então L é separável sobre K se e só se $u_1, \ldots, u_m$ são elementos separáveis sobre K.

Demonstração.

(i) Se $\phi : M \to \bar{K}^a$ é um K-homomorfismo, então ϕ é um prolongamento do K-homomorfismo $\phi|_L : L \to \bar{K}^a$. Basta, pois, mostrar que dado um K-homomorfismo $\psi : L \to \bar{K}^a$ os prolongamentos a um K-homomorfismo $\phi : M \to \bar{K}^a$ estão em correspondência biunívoca com os L-homomorfismos $\tau : M \to \bar{L}^a$. De facto, podemos estender ψ a um isomorfismo $\tilde{\psi} : \bar{L}^a \to \bar{K}^a$, logo, a correspondência que a um L-homomorfismo $\tau : M \to \bar{L}^a$ associa o prolongamento $\phi = \tilde{\psi} \circ \tau$ é biunívoca: a inversa associa a um prolongamento $\phi : M \to \bar{K}^a$ o L-homomorfismo $\tau = \tilde{\psi}^{-1} \circ \phi$.

(ii) Por (i), basta mostrar que $[K(u) : K]_s \leq [K(u) : K]$ para um elemento algébrico u sobre um corpo K, e que a igualdade se verifica se

e só se $K(u)$ é separável sobre K. Agora $[K(u) : K]_s$, *i.e.*, o número de K-homomorfismos $\phi : K(u) \to \bar{K}^a$ é igual ao número de raízes distintas do polinómio mínimo de u sobre K. Logo, $[K(u) : K]_s \leq [K(u) : K]$, com igualdade se e só se u é separável sobre K. Mas u é separável sobre K se e só se $K(u)$ é uma extensão separável sobre K, pois, se $u' \in K(u)$ não é separável, então obtemos

$$\begin{aligned}[K(u) : K]_s &= [K(u) : K(u')]_s[K(u') : K]_s \\ &< [K(u) : K(u')][K(u') : K] = [K(u) : K].\end{aligned}$$

(iii) Se os u_i são separáveis sobre K, então u_i é separável sobre o corpo $K(u_1, \ldots, u_{i-1})$. Logo, usando (i) e (ii), vemos que

$$[K(u_1, \ldots, u_m) : K]_s = [K(u_1, \ldots, u_m) : K],$$

e, portanto, $K(u_1, \ldots, u_m)$ é separável sobre K. □

Se K é perfeito, é claro que todas as extensões algébricas de K são separáveis. Em particular, se K tem característica 0 ou se K tem característica p e $K = K^p$, toda a extensão algébrica de K é separável.

Exercícios.

1. Mostre que, se K tem característica 0 e $p(x) \in K[x]$ é um polinómio mónico, então $q(x) = p(x)[\text{mdc}(p(x), p'(x))]^{-1}$ é um polinómio com raízes simples, e estas coincidem com as raízes de $p(x)$.

2. Mostre que, se K é um corpo com característica $\neq 2$, então o polinómio $x^2 + ax + b \in K[x]$ é separável.

3. Considere o corpo $\mathbb{Z}_p(x)$ das fracções $q(x)/r(x)$, onde $q(x)$ e $r(x)$ são polinómios sobre $\mathbb{Z}_p$.
   (a) Mostre que $\mathbb{Z}_p(x)$ tem característica p.
   (b) Mostre que o elemento $x \in \mathbb{Z}_p(x)$ não é uma potência de grau p, *i.e.*, não existe $b(x) \in \mathbb{Z}_p(x)$ tal que $x = b(x)^p$.
   (c) Dê um exemplo de um polinómio sobre $\mathbb{Z}_p(x)$ que não seja separável.

4. Seja K um corpo de característica p, e $q(x) \in K[x]$ um polinómio irredutível. Mostre que as raízes de $q(x)$ têm todas a mesma multiplicidade p^n, para um certo inteiro n.

5. Seja L uma extensão de K, com $[L : K] < \infty$. Mostre que $[L : K]_s \mid [L : K]$. (NOTA: Define-se GRAU DE INSEPARABILIDADE de L sobre K como sendo $[L : K]_i = [L : K]/[L : K]_s$.)

6. Sejam $M \supset L \supset K$ extensões sucessivas. Mostre que:

(i) se M é separável sobre K, então M é separável sobre L, e L é separável sobre K;

(ii) se M é separável sobre L, e L é separável sobre K, então M é separável sobre K.

7.6 Grupo de Galois

Como já referimos anteriormente, a ideia de base da Teoria de Galois consiste em substituir um problema de extensões de corpos por um problema de teoria dos grupos. Os grupos em questão são os que agora introduzimos.

Seja L uma extensão de K. Os K-automorfismos de L formam um grupo: se ϕ_1 e ϕ_2 são K-automorfismos de L, então $\phi_1 \circ \phi_2$ é um K-automorfismo.

Definição 7.6.1. Chama-se GRUPO DE GALOIS de uma extensão L de K ao grupo dos K-automorfismos de L.

O grupo de Galois de uma extensão L de K será designado por $\mathrm{Aut}_K(L)$. Como mostram os exemplos seguintes, este grupo pode ser de natureza bastante diversa.

Exemplos 7.6.2.

1. *Seja $L = \mathbb{Q}(\sqrt{2})$. O elemento $\sqrt{2}$ tem polinómio mínimo x^2-2. Qualquer $\mathbb{Q}$-automorfismo $\phi : L \to L$ transforma raízes deste polinómio em raízes. Temos, pois, dois automorfismos, a identidade e*

$$\phi(a + b\sqrt{2}) = a - b\sqrt{2}.$$

O grupo de Galois $\mathrm{Aut}_{\mathbb{Q}}(L)$ é, pois, isomorfo a $\mathbb{Z}_2$.

2. *Seja $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Tal como no exemplo anterior, vemos que os $\mathbb{Q}$-automorfismos de L são completamente determinados pela sua acção no conjunto $\{\sqrt{2}, \sqrt{3}\}$. Existem 4 possibilidades: a identidade e*

$$\phi_1(\sqrt{2}) = -\sqrt{2}, \quad \phi_1(\sqrt{3}) = \sqrt{3};$$

$$\phi_2(\sqrt{2}) = \sqrt{2}, \quad \phi_2(\sqrt{3}) = -\sqrt{3};$$

$$\phi_3(\sqrt{2}) = -\sqrt{2}, \quad \phi_3(\sqrt{3}) = -\sqrt{3}.$$

Neste caso, o grupo de Galois é isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

3. *Seja K um corpo de característica p tal que $K \neq K^p$. Se $a \notin K^p$, o polinómio $q(x) = x^p - a$ é irredutível. Seja L uma extensão de decomposição de $q(x)$. Em L temos $q(x) = (x-r)^p$, logo, $L = K(r)$. Se $\phi : L \to L$ é um K-automorfismo, então $\phi(r) = r$ e concluímos que $\phi = id$. O grupo de Galois $\mathrm{Aut}_K(L)$ é, pois, trivial.*

4. Seja $L = K(x)$, o corpo das fracções da forma $p(x)/q(x)$ com $p(x)$, $q(x) \in K[x]$. Pode-se verificar que os elementos primitivos de L tomam a forma

$$t = \frac{ax+b}{cx+d}, \qquad a,b,c,d \in K, \quad ad-bc \neq 0.$$

Qualquer K-automorfismo de L transforma elementos primitivos em elementos primitivos, logo, se $\phi : L \to L$ é um K-automorfismo, então transforma o elemento $p(x)/q(x) \in L$ num elemento $p(t)/q(t) \in L$. Vemos, pois, que o grupo de Galois é isomorfo a $GL_2(K)/H$, onde H é o subgrupo das matrizes 2×2 da forma

$$H = \{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \neq 0 \}.$$

Se K é infinito, este grupo é infinito.

Como os corpos de decomposição de um polinómio $p(x)$ são isomorfos é natural a seguinte definição:

Definição 7.6.3. Seja $p(x) \in K[x]$ um polinómio. O GRUPO DE GALOIS DA EQUAÇÃO $p(x) = 0$ (ou simplesmente de $p(x)$) é o grupo de Galois dum corpo de decomposição de $p(x)$ sobre K.

É natural identificar o grupo de Galois de uma equação $p(x) = 0$ com um subgrupo do grupo de permutações das raízes de $p(x)$[7]. Se L é um corpo de decomposição de $p(x)$, e $S = \{r_1, \ldots, r_n\}$ são as raízes distintas de $p(x)$, então $L = K(r_1, \ldots, r_n)$. Se ϕ é um elemento do grupo de Galois de $p(x)$, *i.e.*, se $\phi \in \mathrm{Aut}_K(L) \equiv G$, então ϕ transforma raízes de $p(x)$ em raízes. Por outro lado, se soubermos como ϕ transforma as raízes de $p(x)$, então sabemos como ϕ transforma todo o elemento de $L = K(r_1, \ldots, r_n)$. Logo, a aplicação $\phi \mapsto \phi|_S$ é um monomorfismo $G \to S_n$. Podemos, pois, identificar G com um subgrupo do grupo das permutações das raízes.

Em geral, $G \subsetneq S_n$, mesmo quando $p(x)$ é irredutível, como mostra o seguinte exemplo:

Exemplo 7.6.4.

Seja $L \subset \mathbb{C}$ a extensão de decomposição sobre $\mathbb{Q}$ do polinómio $p(x) = x^6 - 2$ (este polinómio é irredutível). As raízes de $p(x)$ são $r_k = \sqrt[6]{2} e^{\frac{2k\pi i}{6}}$, $k = 1, \ldots, 6$. Temos, por exemplo,

$$r_3 + r_6 = 0.$$

Como $r_3 + r_1 \neq 0$, não existe um automorfismo do grupo de Galois que corresponda à transposição (16)*. Temos, ainda, da figura abaixo que*

$$(r_1 + r_5)^6 = {r_6}^6 = 2,$$

[7]Era assim que Galois concebia o grupo que hoje tem o seu nome, ainda antes de se ter formalizado sequer o conceito de grupo!

logo, não existem automorfismos do grupo de Galois que correspondam às permutações (13)(56) *e* (16)(35). *Muitas outros elementos de* S_6 *podem ser excluídos por este tipo de argumento geométrico. De facto, veremos mais adiante que* $|G| = 12$.

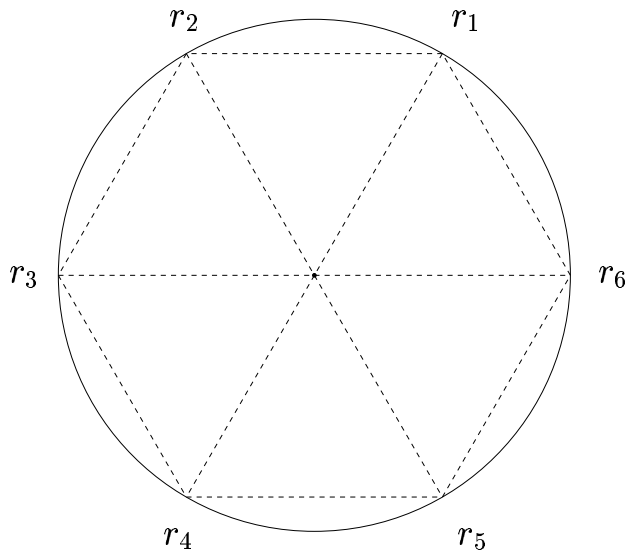


Figura 7.6.1: Raízes de $x^6 - 2 = 0$

A determinação do grupo de Galois de uma equação $p(x) = 0$ ou de uma extensão é, em geral, uma tarefa difícil. Vejamos o que podemos dizer sobre a sua ordem.

Teorema 7.6.5. *Seja* L *uma extensão de dimensão finita sobre* K, *e* $G = \mathrm{Aut}_K(L)$ *o seu grupo de Galois. Então* $|G| \leq [L : K]$. *Se* L *é normal e separável sobre* K, *então* $|G| = [L : K]$.

Demonstração. Podemos assumir que $L \subset \bar{K}^a$. Se $\phi \in G$, então obtemos um K-homomorfismo $\phi : L \to \bar{K}^a$. O número destes homomorfismos é $[L : K]_s \leq [L : K]$. Logo $|G| \leq [L : K]$.

Se L é normal, então todo o K-homomorfismo $\psi : L \to \bar{K}^a$ é de facto um automorfismo de L. Se L é separável, então $[L : K]_s = [L : K]$. Portanto, se L é normal e separável sobre K, então $|G| = [L : K]$. □

Assim, para polinómios separáveis, sabemos calcular a ordem do seu grupo de Galois:

Corolário 7.6.6. *Se* $p(x)$ *é um polinómio separável sobre* K *com grupo de Galois* G, *e* L *é uma extensão de decomposição de* $p(x)$, *então* $|G| = [L : K]$.

Exemplos 7.6.7.

1. *A extensão* $\mathbb{Q}(i, \sqrt[4]{2})$ *é uma extensão de decomposição do polinómio* $x^4 - 2 \in \mathbb{Q}[x]$. *Como* $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(i)] = 4$ *e* $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, *temos* $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$, *logo o grupo de Galois de* $\mathbb{Q}(i, \sqrt[4]{2})$ *tem ordem 8. Temos* $\mathbb{Q}$*-automorfismos de* $\mathbb{Q}(i, \sqrt[4]{2})$ *definidos por (verifique!)*

$$\begin{aligned} \sigma(i) &= -i, & \tau(i) &= i, \\ \sigma(\sqrt[4]{2}) &= \sqrt[4]{2}, & \tau(\sqrt[4]{2}) &= i\sqrt[4]{2}. \end{aligned}$$

   Estes automorfismos têm ordens 2 e 4, respectivamente, e satisfazem à relação $\tau\sigma = \sigma\tau^3$. *É fácil de ver que*

$$\mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(i, \sqrt[4]{2}) = \{1, \tau, \tau^2, \tau^3, \sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3\} \equiv G.$$

   Este grupo é isomorfo a D_4. *Em termos das raízes* $r_k = e^{\frac{\pi k}{2} i}$, *estes automorfismos correspondem às permutações*

$$\sigma = (13), \qquad \tau = (1234).$$

2. *O grupo de Galois do polinómio* $p(x) = x^6 - 2$ *sobre* $\mathbb{Q}$ *tem ordem 12, pois* $[\mathbb{Q}(\sqrt[6]{2}, e^{\frac{2\pi}{3} i}) : \mathbb{Q}] = 12$ *e* $\mathbb{Q}(\sqrt[6]{2}, e^{\frac{2\pi}{3} i})$ *é uma extensão de decomposição de* $p(x)$. *Deixamos como exercício determinar a sua representação como um grupo de permutações.*

A finalizar esta secção consideramos o caso de um polinómio da forma $x^n - a$ sobre um corpo K de característica 0.

Definição 7.6.8. Seja K um corpo. A uma extensão de decomposição do polinómio $x^n - 1$ chama-se CORPO CICLOTÓMICO DE ORDEM n sobre K.

O próximo resultado caracteriza o grupo de Galois de um corpo ciclotómico no caso em que a característica é zero.

Proposição 7.6.9. *Se* K *tem característica* 0, *o grupo de Galois de um corpo ciclotómico é abeliano.*

Demonstração. Seja L uma extensão de decomposição de $x^n - 1$ sobre K. Como K tem característica zero, e $(x^n - 1)' = nx^{n-1} \neq 0$, vemos que as raízes de $x^n - 1$ são todas simples e o conjunto das raízes $U = \{r \in L : r^n - 1 = 0\}$ é isomorfo a $\mathbb{Z}_n$ (ver Exercício 6.6.2.2). Por outro lado, se $\phi \in \mathrm{Aut}_K(L) \equiv G$, então $\phi|_U$ é um automorfismo de U e esta restrição determina completamente ϕ. Logo, G é isomorfo a um subgrupo de $\mathrm{Aut}(U) \simeq \mathrm{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$, o grupo das unidades do anel $\mathbb{Z}_n$. □

Em geral não podemos dizer mais nada sobre o grupo de Galois de um corpo ciclotómico. Por exemplo se K contém as raízes de $x^n - 1 = 0$, então o corpo ciclotómico de ordem n coincide com K, e o seu grupo de Galois é trivial.

Proposição 7.6.10. *Se K tem característica 0 e contém as raízes de $x^n - 1 = 0$, então o grupo de Galois de $x^n - a$ sobre K é cíclico de ordem um divisor de n.*

Demonstração. Seja L uma extensão de decomposição de $x^n - a$ sobre K, e mais uma vez seja $U = \{z \in L : z^n - 1 = 0\}$ o conjunto das raízes de $x^n - 1$. Se $r \in L$ é uma raiz de $x^n - a$, então $\{zr : z \in U\}$ é o conjunto das n raízes de $x^n - a$ em L. Temos, pois, que $L = K(r)$. Se $\phi_1, \phi_2 \in \mathrm{Aut}_K(L) \equiv G$, então $\phi_1(r) = z_1 r$, $\phi_2(r) = z_2 r$, para alguns $z_1, z_2 \in U$, e $\phi_1 \circ \phi_2(r) = z_1 z_2 r$. Logo, $\phi \mapsto z$ é um monomorfismo de G para o grupo cíclico $U \simeq \mathbb{Z}_n$, e concluímos que G é isomorfo a um subgrupo de $\mathbb{Z}_n$.

□

Exercícios.

1. Determine o grupo de Galois da extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ sobre $\mathbb{Q}$.

2. Seja $L = K(x)$, o corpo das fracções da forma $p(x)/q(x)$ com $p(x)$, $q(x) \in K[x]$. Mostre que os elementos primitivos de L são da forma

$$t = \frac{ax + b}{cx + d}, \qquad a, b, c, d \in K, \quad ad - bc \neq 0$$

   (Sugestão: Se $t = p(x)/q(x)$, onde $\mathrm{mdc}(p(x), q(x) = 1$, defina o grau de t como sendo o máximo dos graus de $p(x)$ e $q(x)$. Mostre que $p(w) - yq(w)$ é irredutível em $K[w, y]$, logo, também em $K(y)[w]$, e que x é algébrico sobre $K(t)$ com polinómio mínimo um múltiplo de $p(w) - tq(w)$. Conclua que $[K(x) : K(t)] = 1$ e que $K(x) = K(t)$ se e só se o grau de t é 1.)

3. Determine o grupo de Galois de $x^3 - 2$ sobre $\mathbb{Q}$ e sobre $\mathbb{Z}_2$.

4. Represente o grupo de Galois do polinómio $x^6 - 2$ sobre $\mathbb{Q}$ como um grupo de permutações das raízes.

5. Determine o grupo de Galois do polinómio $p(x) = 2x^3 + 3x^2 + 6x + 6$.

6. Mostre que o grupo de Galois de $p(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ é isomorfo ao grupo alternado A_3.

7.7 A Correspondência de Galois

Estamos finalmente em condições de explicar como é que a Teoria de Galois permite substituir problemas sobre (extensões de corpos de) polinómios por um problema em princípio mais simples de Teoria de Grupos. Galois descobriu que existe uma correspondência entre extensões intermédias e subgrupos do grupo de Galois, como passamos a descrever.

Seja L uma extensão de K, e $H \subset \mathrm{Aut}_K(L)$ um subgrupo do grupo de Galois. Podemos pensar em H como um grupo de transformações de L. Neste caso, o conjunto dos pontos fixos por H é um corpo intermédio $L \supset \mathrm{Fix}(H) \supset K$. Por outro lado, se $L \supset \tilde{K} \supset K$ é um corpo intermédio, então $\mathrm{Aut}_{\tilde{K}}(L)$ é um subgrupo do grupo de Galois $\mathrm{Aut}_K(L)$.

É fácil verificar as seguintes propriedades desta correspondência.

Proposição 7.7.1 (Propriedades da Correspondência de Galois). *Seja L uma extensão de K com grupo de Galois $G = \mathrm{Aut}_K(L)$. Sejam ainda $\tilde{K}$, $\tilde{K}_1$ e $\tilde{K}_2$ extensões intermédias, e $H, H_1, H_2 \subset G$ subgrupos.*

(i) *Se $H_1 \supset H_2$, então $\mathrm{Fix}(H_1) \subset \mathrm{Fix}(H_2)$.*

(ii) *Se $\tilde{K}_1 \supset \tilde{K}_2$, então $\mathrm{Aut}_{\tilde{K}_1}(L) \subset \mathrm{Aut}_{\tilde{K}_2}(L)$.*

(iii) $\mathrm{Fix}(\mathrm{Aut}_{\tilde{K}}(L)) \supset \tilde{K}$.

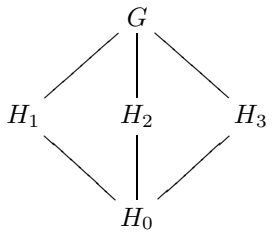
(iv) $\mathrm{Aut}_{\mathrm{Fix}(H)}(L) \supset H$.

Exemplo 7.7.2.

Considere-se a extensão $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $K = \mathbb{Q}$. Vimos anteriormente que o grupo de Galois desta extensão contém 4 elementos:

$$\mathrm{Aut}_K(L) = \{id, \phi_1, \phi_2, \phi_3\} \equiv G.$$

Este grupo possui, para além do subgrupo trivial $H_0 = \{id\}$, os subgrupos $H_1 = \{id, \phi_1\}$, $H_2 = \{id, \phi_2\}$ e $H_3 = \{id, \phi_3\}$. Assim, o reticulado dos subgrupos [8] pode ser representado pelo diagrama

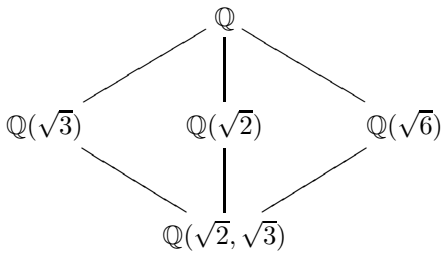


O corpo fixo pelo grupo de Galois G é o corpo de base $\mathrm{Fix}(G) = \mathbb{Q}$, enquanto que obviamente $\mathrm{Fix}(H_0) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Por outro lado, é fácil de ver que

$$\mathrm{Fix}(H_1) = \mathbb{Q}(\sqrt{3}), \qquad \mathrm{Fix}(H_2) = \mathbb{Q}(\sqrt{2}), \qquad \mathrm{Fix}(H_3) = \mathbb{Q}(\sqrt{6}).$$

[8] Um RETICULADO é um conjunto parcialmente ordenado em que qualquer conjunto de dois elementos tem supremo e ínfimo. O conjunto dos subgrupos de um grupo fixo G, ordenado pela relação de inclusão, é um reticulado. De igual forma, o conjunto das extensões intermédias $K \subset \tilde{K} \subset L$ de uma extensão fixa L de K, ordenado pela relação de inclusão, também é um reticulado.

Assim, o reticulado das extensões intermédias é dado pelo diagrama



Estamos interessados em extensões suficientemente ricas em automorfismos, de forma que em (iii) e (iv) da proposição acima se possam substituir as inclusões por igualdades.

Definição 7.7.3. Seja L uma extensão de dimensão finita sobre K. Chama-se a L uma EXTENSÃO DE GALOIS de K, se $\mathrm{Fix}(\mathrm{Aut}_K(L)) = K$.

Temos as seguintes caracterizações de uma extensão de Galois.

Proposição 7.7.4. *As seguintes afirmações são equivalentes:*

(i) L é uma extensão de Galois de K;

(ii) L é uma extensão de decomposição de um polinómio separável sobre K;

(iii) L é uma extensão de dimensão finita, normal e separável sobre K.

Se qualquer uma destas condições se verifica, então

$$|\mathrm{Aut}_K(L)| = [L : K]. \tag{7.7.1}$$

Demonstração. A relação (7.7.1) segue do Teorema 7.6.5. Vejamos então as implicações (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): Como $[L : K] < \infty$, existem $r_1, \ldots, r_n \in L$, algébricos sobre K, tais que $L = K(r_1, \ldots, r_n)$. Seja $p_i(x)$ o polinómio mínimo de cada r_i em $K[x]$, e $\mathcal{O}_i = \{\phi(r_i) : \phi \in \mathrm{Aut}_K(L)\}$ a órbita de r_i sob a acção do grupo de Galois. Este conjunto é finito, e é constituído por raízes de $p_i(x)$. O polinómio

$$q_i(x) \equiv \prod_{r \in \mathcal{O}_i} (x - r) \in L[x]$$

divide $p_i(x)$ e é separável (tem todas as raízes distintas). Se $\phi \in \mathrm{Aut}_K(L)$, então

$$q_i^{\phi}(x) = \prod_{r \in \mathcal{O}_i} (x - \phi(r)) = \prod_{r \in \mathcal{O}_i} (x - r) = q_i(x),$$

donde os coeficientes de $q_i(x)$ pertencem a $\mathrm{Fix}(\mathrm{Aut}_K(L)) = K$. Concluímos que $q_i(x) \in K[x]$, logo, $p_i(x) = q_i(x)$ é separável e tem as suas raízes em L. O polinómio $p(x) = \prod_i p_i(x)$ é separável, e L é uma extensão de decomposição de $p(x)$ sobre K.

(ii) $\Rightarrow$ (iii): Se L é uma extensão de decomposição de um polinómio $p(x)$ sobre K, então L é uma extensão normal de dimensão finita (Corolário 7.3.10). Se $p(x)$ é um polinómio separável, então $L = K(r_1, \ldots, r_m)$, onde $r_1, \ldots, r_m$ são separáveis. Pela Proposição 7.5.9, L é uma extensão separável.

(iii) $\Rightarrow$ (i): Seja $\tilde{K} = \mathrm{Fix}(\mathrm{Aut}_K(L))$. Então pelas propriedades mencionadas acima, $\tilde{K}$ é um corpo intermédio entre L e K. Seja $r_1 \in \tilde{K} - K$ e designemos por $p(x)$ o polinómio mínimo de r_1 sobre K. Como L é normal e separável, $p(x)$ decompõe-se em $L[x]$ num produto de factores lineares distintos: $p(x) = \prod_{i=1}^{m}(x - r_i)$, $(m > 1)$ (r_i todos distintos). Se $\phi : K(r_1) \to \bar{K}^a$ é o K-monomorfismo que transforma r_1 em r_2, podemos prolongar ϕ num monomorfismo $\Phi : L \to \bar{K}^a$ (Teorema 7.4.5). Pela Proposição 7.3.9, Φ é de facto um K-automorfismo de L. Mas então Φ é um elemento de $\mathrm{Aut}_K(L)$ que não deixa fixo r_1, contradizendo $r_1 \in \tilde{K} = \mathrm{Fix}(\mathrm{Aut}_K(L))$. Logo, $K = \tilde{K} = \mathrm{Fix}(\mathrm{Aut}_K(L))$. □

Se L não é uma extensão de Galois de K, então podemos afirmar apenas que $|\mathrm{Aut}_K(L)| \leq [L : K]$. Por outro lado, temos o seguinte lema geral:

Lema 7.7.5 (Artin[9]). *Seja G um grupo finito de automorfismos de um corpo L e $K = \mathrm{Fix}(G)$. Então*

$$[L : K] \leq |G|. \tag{7.7.2}$$

Demonstração. Seja $G = \{\phi_1 = id, \phi_2, \ldots, \phi_m\}$. Precisamos de mostrar que quaisquer n elementos de L com $n > m$ são linearmente dependentes sobre K.

Sejam então $u_1, \ldots, u_n$ elementos de L. O sistema homogéneo de equações lineares

$$\sum_{i=1}^{n} a_i \phi_j(u_i) = 0, \qquad (j = 1, \ldots, m)$$

tem mais varáveis que equações, logo, por um resultado de Álgebra Linear existe uma solução não trivial $(a_1, \ldots, a_n) \in L^n$. Reordenando termos se necessário, podemos sempre escrever a solução na forma $(a_1, \ldots, a_s, 0, \ldots, 0)$, onde $s \geq 2$ é mínimo. Dividindo por a_1, podemos ainda assumir que $a_1 = 1$. Vejamos que os a_i's pertencem a $K = \mathrm{Fix}(G)$. De facto, se algum $a_i \notin K = \mathrm{Fix}(G)$, então existe $\phi \in G$ tal que $\phi(a_i) \neq a_i$. O vector $(1, \phi(a_2), \ldots, \phi(a_s), 0, \ldots, 0)$ é também uma solução do sistema (verifique

[9]Emil Artin foi um dos grandes algebristas do século *XX*. A ele, em conjunto com Irving Kaplanski, devemos, por exemplo, a formulação moderna da Teoria de Galois que se segue neste livro. Artin e Kaplanski fizeram ambos parte do projecto Bourbaki.

por substituição) e o vector diferença $(0, a_2 - \phi(a_2), \ldots, a_s - \phi(a_s), 0, \ldots, 0)$ é um vector solução não-nulo com mais zeros que $(1, a_2, \ldots, a_s, 0, \ldots, 0)$, contrariando a hipótese de s ser minimal.

Concluímos que, para todo o i, $a_i \in K$, logo a equação $j = 1$ do sistema fornece a relação de dependência linear

$$\sum_{i=1}^{n} a_i u_i = 0.$$

□

Podemos finalmente enunciar o teorema chave da Teoria de Galois. Ao mesmo tempo justificamos o uso do termo "extensão normal".

Teorema 7.7.6 (Teorema Fundamental da Teoria de Galois). *Seja L uma extensão de Galois de K. Existe uma correspondência biunívoca entre as extensões intermédias $K \subset \hat{K} \subset L$ e os subgrupos H do grupo de Galois $G \equiv \mathrm{Aut}_K(L)$. Esta correspondência é dada por $\hat{K} \mapsto \mathrm{Aut}_{\hat{K}}(L) \equiv H$, e a sua inversa é $H \mapsto \mathrm{Fix}(H) \equiv \hat{K}$. Escrevendo $H \leftrightarrow \hat{K}$, a correspondência satisfaz:*

(i) Se $H_1 \leftrightarrow \hat{K}_1$ e $H_2 \leftrightarrow \hat{K}_2$, então $H_2 \subset H_1$ se e só se $\hat{K}_2 \supset \hat{K}_1$. Neste caso temos $[H_1 : H_2] = [\hat{K}_2 : \hat{K}_1]$.

(ii) Se $H \leftrightarrow \hat{K}$, então H é um subgrupo normal de G se e só se $\hat{K}$ é uma extensão normal de K. Neste caso, $\hat{K}$ é uma extensão de Galois que tem G/H como grupo de Galois.

Demonstração. Vejamos que a correspondência é biunívoca:

$\mathrm{Fix}(\mathrm{Aut}_{\hat{K}}(L)) = \hat{K}$: Seja $L \supset \hat{K} \supset K$ uma extensão intermédia. Pela Proposição 7.7.4, L é uma extensão de dimensão finita, normal e separável sobre K, logo também o é sobre $\hat{K}$. Mas então L é uma extensão de Galois de $\hat{K}$, e concluímos que $\hat{K} = \mathrm{Fix}(H)$ com $H = \mathrm{Aut}_{\hat{K}}(L)$.

$\mathrm{Aut}_{\mathrm{Fix}(H)}(L) = H$: Seja $H \subset G \equiv \mathrm{Aut}_K(L)$ e $\hat{K} = \mathrm{Fix}(H)$. Pelo Lema de Artin, $|H| \geq [L : \mathrm{Fix}(H)] = [L : \hat{K}]$. Por outro lado, L é uma extensão de Galois sobre $\hat{K}$ e $H \subset \mathrm{Aut}_{\hat{K}}(L)$, donde usando a relação (7.7.1) vemos que $|H| \leq |\mathrm{Aut}_{\hat{K}}(L)| = [L : \hat{K}]$. Logo, $|H| = [L : \hat{K}]$ e concluímos que $H = \mathrm{Aut}_{\hat{K}}(L)$ com $\hat{K} = \mathrm{Fix}(H)$.

Para verificar (i), da correspondência que acabámos de mostrar e da Proposição 7.7.1, decorre que $H_2 \subset H_1$ se e só se $\hat{K}_2 \supset \hat{K}_1$. Como L é uma extensão de Galois sobre $\hat{K}_1$ e $\hat{K}_2$, temos

$$[\hat{K}_2 : \hat{K}_1] = \frac{[L : \hat{K}_1]}{[L : \hat{K}_2]} = \frac{|\mathrm{Aut}_{\hat{K}_1}(L)|}{|\mathrm{Aut}_{\hat{K}_2}(L)|} = \frac{|H_1|}{|H_2|} = [H_1 : H_2].$$

Finalmente para verificar (ii), suponha-se que $H \leftrightarrow \hat{K}$. Se $\phi \in G$, então o corpo que corresponde a $\phi H \phi^{-1}$ é $\phi(\hat{K})$ (porquê?). Assim, temos:

(a) Se H é um subgrupo normal de G, então para todo o $\phi \in G$ temos $\phi(\hat{K}) \subset \hat{K}$. A aplicação $\phi \mapsto \phi|_{\hat{K}}$ é um homomorfismo sobrejectivo de G em $\mathrm{Aut}_K(\hat{K})$, cujo núcleo é H. Logo, $\mathrm{Aut}_K(\hat{K}) \simeq G/H$ e $\mathrm{Fix}(\mathrm{Aut}_K(\hat{K}) = \mathrm{Fix}(G/H) = \mathrm{Fix}(G) = K$. Concluímos, pois, que $\hat{K}$ é uma extensão de Galois sobre K com grupo de Galois G/H.

(b) Reciprocamente, suponha-se que $\hat{K}$ é uma extensão normal. Pela Proposição 7.3.9, vemos que $\phi(\hat{K}) = \hat{K}$, para todo o elemento ϕ do grupo de Galois G. Como $\phi H \phi^{-1} \leftrightarrow \phi(\hat{K})$, vemos que $\phi H \phi^{-1} = H$. Logo, H é um subgrupo normal de G.

□

Exemplo 7.7.7.

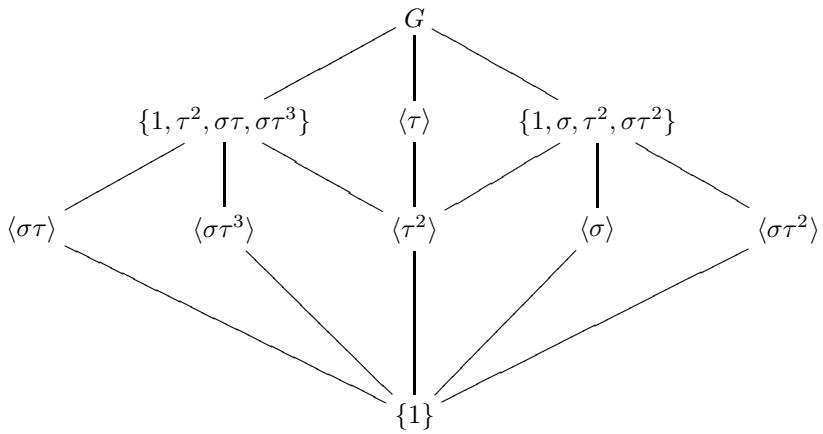
Vimos num exemplo da secção anterior que $\mathbb{Q}(i, \sqrt[4]{2})$ *é uma extensão de Galois sobre* $\mathbb{Q}$*, com grupo de Galois*

$$\mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(i, \sqrt[4]{2}) = \{1, \tau, \tau^2, \tau^3, \sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3\} \equiv G,$$

onde σ *e* τ *são os* $\mathbb{Q}$*-automorfismos de* $\mathbb{Q}(i, \sqrt[4]{2})$ *definidos por*

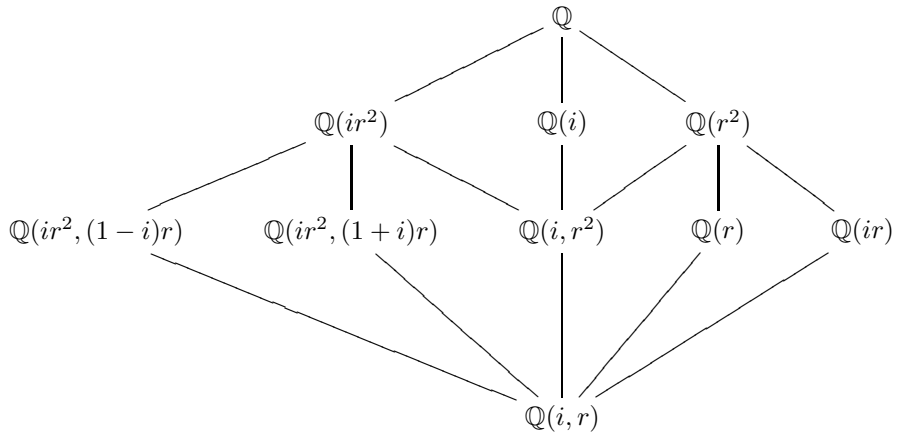
$$\begin{array}{ll} \sigma(i) = -i, & \tau(i) = i, \\ \sigma(\sqrt[4]{2}) = \sqrt[4]{2}, & \tau(\sqrt[4]{2}) = i\sqrt[4]{2}. \end{array}$$

Este grupo tem o seguinte reticulado de subgrupos:



A correspondência de Galois fornece um reticulado análogo de extensões in-

termédias de $\mathbb{Q}$*:*



onde $r = \sqrt[4]{2}$*. As extensões do primeiro nível são normais, pois são extensões de grau 2. Elas correspondem a subgrupos de índice 2, logo, subgrupos normais. No segundo nível, apenas a extensão* $\mathbb{Q}(i, \sqrt{2})$ *é normal (corresponde ao subgrupo* $\{1, \tau^2\} = C(G)$*).*

Exercícios.

1. Determine a correspondência de Galois da extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subset \mathbb{R}$ sobre $\mathbb{Q}$.

2. Determine a correspondência de Galois para o corpo de decomposição do polinómio $x^3 - 2$ sobre $\mathbb{Q}$ e sobre $\mathbb{Z}_2$.

3. Determine a correspondência de Galois para o corpo de decomposição do polinómio $(x^3 - 2)(x^2 - 3)$ sobre $\mathbb{Q}$.

4. Determine a correspondência de Galois para o corpo de decomposição do polinómio $x^4 - 4x^2 - 1$ sobre $\mathbb{Q}$.

5. Seja $p(x)$ um polinómio de grau 3 sobre $\mathbb{Q}$, com grupo de Galois G. Se $r_1, r_2, r_3 \in \mathbb{C}$ designam as raízes de $p(x)$ e $\delta \equiv (r_1 - r_2)(r_1 - r_3)(r_2 - r_3)$, mostre que:
   (a) $|G| = 1$ se e só se as raízes de $p(x)$ pertencem a $\mathbb{Q}$;
   (b) $|G| = 2$ se e só se $p(x)$ tem exactamente uma raiz racional;
   (c) $|G| = 3$ se e só se $p(x)$ não tem raízes racionais e $\delta \in \mathbb{Q}$;
   (d) $|G| = 6$ se e só se $p(x)$ não tem raízes racionais e $\delta \notin \mathbb{Q}$.

6. Se $p(x) \in K[x]$ é um polinómio de grau n com raízes $r_1, \ldots, r_n$, define-se o DISCRIMINANTE de $p(x)$ como sendo $\Delta = \delta^2$, onde

$$\delta = \prod_{i<j} (r_i - r_j).$$

Assumindo que $p(x)$ é separável e K tem característica diferente de 2, mostre que

(a) $\Delta \in K$;

(b) $\Delta = 0$ se e só se $p(x)$ possui uma raiz múltipla;

(c) Δ é um quadrado perfeito em K se e só se o grupo de Galois de $p(x)$ está contido em A_n.

7. Se $p(x) = x^3 + px + q \in \mathbb{Q}[x]$, mostre que o seu discriminante (ver o exercício anterior) é $\Delta = -4p^3 - 27q^2$. Qual é o grupo de Galois de $x^3 + 6x^2 - 9x + 3$?

8. Seja L uma extensão de Galois de K, e $L \supset \hat{K} \supset K$ um corpo intermédio. Seja $H \subset \mathrm{Aut}_K(L)$ o subgrupo dos K-automorfismos que transformam $\hat{K}$ em si próprio. Mostre que H é o normalizador de $\mathrm{Aut}_{\hat{K}}(L)$ em $\mathrm{Aut}_K(L)$.

7.8 Algumas Aplicações

A finalizar este capítulo fornecemos algumas aplicações da Teoria de Galois. A primeira aplicação diz respeito ao estudo de expressões racionais simétricas. A segunda aplicação é a uma caracterização dos números complexos construtíveis que completa os resultados obtidos na Secção 7.2. Finalmente, a última aplicação consiste na demonstração do critério descoberto por Galois para decidir se uma equação algébrica é ou não resolúvel por radicais.

7.8.1 Expressões racionais simétricas.

Sejam $x_1, \ldots, x_n$ indeterminadas. No corpo das fracções $K(x_1, \ldots, x_n)$ consideramos o polinómio

$$p(x) = \prod_{i=1}^{n}(x - x_i) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n.$$

Os coeficientes s_i assim definidos são polinómios nas indeterminadas x_i, conhecidos por *polinómios simétricos elementares*, e admitem as expressões:

$$\begin{aligned} s_1 &= \sum_i x_i, \\ s_2 &= \sum_{i<j} x_i x_j, \\ &\vdots \\ s_n &= x_1 \cdots x_n. \end{aligned}$$

A fórmula geral para um polinómio simétrico elementar é:

$$s_i = \sum_{j_1<\cdots<j_i} x_{j_1}\cdots x_{j_i}, \qquad i = 1, \ldots, n.$$

A razão do uso do termo "simétrico" é a de que qualquer permutação dos índices das variáveis não altera o polinómio. Mais geralmente podemos considerar expressões racionais simétricas que podem ser formalizadas do seguinte modo: Para toda a permutação $\pi \in S_n$, existe um K-automorfismo ϕ_π de $K(x_1, \ldots, x_n)$ que é a identidade em K e transforma x_i em $x_{\pi(i)}$. Os elementos de $K(x_1, \ldots, x_n)$, que são fixos pelo grupo de automorfismos $G \equiv \{\phi_\pi : \pi \in S_n\} \simeq S_n$, são chamados *expressões racionais simétricas*. Na notação da correspondência de Galois, as expressões racionais simétricas são precisamente os elementos de $\mathrm{Fix}(G)$.

Exemplos 7.8.1.

1. *O polinómio $p(x)$ acima é claramente invariante sob a acção dos ϕ_π (*i.e.*, $p(x) = p^{\phi_\pi}(x)$), os coeficientes s_i são fixos por ϕ_π. Logo, $s_i \in \mathrm{Fix}(G)$, e os s_i são expressões racionais simétricas.*

2. *As fracções*

$$\frac{x_1x_2}{x_3} + \frac{x_2x_3}{x_1} + \frac{x_3x_1}{x_2}, \qquad \frac{1}{{x_1}^2} + \frac{1}{{x_2}^2} + \frac{1}{{x_3}^2},$$

são expressões racionais simétricas.

Podemos utilizar a correspondência de Galois para mostrar que qualquer expressão racional simétrica pode ser expressa como uma razão de polinómios simétricos elementares $s_1, \ldots, s_n$. Mais exactamente, temos:

Teorema 7.8.2. *$K(x_1, \ldots, x_n)$ é uma extensão de Galois de $K(s_1, \ldots, s_n)$ com grupo de Galois $G \simeq S_n$. Em particular,* $\mathrm{Fix}(G) = K(s_1, \ldots, s_n)$.

Demonstração. O exemplo acima mostra que $K(s_1, \ldots, s_n) \subset \mathrm{Fix}(G)$, logo $G \subset \mathrm{Aut}_{K(s_1,\ldots,s_n)} K(x_1, \ldots, x_n)$. É claro que o corpo

$$K(x_1, \ldots, x_n) = K(s_1, \ldots, s_n, x_1, \ldots, x_n)$$

é uma extensão de decomposição de $p(x) \in K(s_1, \ldots, s_n)[x]$. Por outro lado, se $\phi \in \mathrm{Aut}_{K(s_1,\ldots,s_n)} K(x_1, \ldots, x_n)$, então ϕ permuta as raízes de $p(x)$, logo

$$\mathrm{Aut}_{K(s_1,\ldots,s_n)} K(x_1, \ldots, x_n) \subset G.$$

Concluímos que o grupo de Galois de $K(x_1, \ldots, x_n)$ sobre $K(s_1, \ldots, s_n)$ é isomorfo a $G \simeq S_n$. Como $K(x_1, \ldots, x_n)$ é uma extensão normal e separável, é uma extensão de Galois, donde $\mathrm{Fix}(G) = K(s_1, \ldots, s_n)$. □

Exemplo 7.8.3.

O polinómio ${x_1}^3+{x_2}^3+{x_3}^3 \in \mathbb{Q}(x_1,x_2,x_3)$ *é uma expressão racional simétrica, logo, pode ser expresso como uma expressão racional de* $s_1 = x_1+x_2+x_3$, $s_2 = x_1x_2+x_1x_3+x_2x_3$ *e* $s_3 = x_1x_2x_3$. *Considerações sobre o grau mostram que existem racionais* a_1, a_2 *e* a_3 *tais que*

$$\begin{aligned}&{x_1}^3+{x_2}^3+{x_3}^3 = \\ &= a_1(x_1+x_2+x_3)^3 + a_2(x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3) + a_3x_1x_2x_3.\end{aligned}$$

Escolhendo valores convenientes para x_1, x_2 *e* x_3, *obtemos:*

$$\begin{aligned} 3 &= 27a_1+9a_2+a_3 && (\textit{tomando } x_1=x_2=x_3=1),\\ 2 &= 8a_1+2a_2 && (\textit{tomando } x_1=x_2=1, x_3=0),\\ 1 &= a_1 && (\textit{tomando } x_1=1, x_2=x_3=0).\end{aligned}$$

Este sistema linear tem como solução $a_1=1$, $a_2=-3$, $a_3=3$. *Logo,*

$$\begin{aligned}&{x_1}^3+{x_2}^3+{x_3}^3 = \\ &\quad = (x_1+x_2+x_3)^3 - 3(x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3) + 3x_1x_2x_3.\end{aligned}$$

7.8.2 Números construtíveis.

Estudámos na Secção 7.2 o subcorpo de $\mathbb{C}$ dos números construtíveis. Vamos agora aplicar a Teoria de Galois para obter a seguinte caracterização dos números construtíveis.

Teorema 7.8.4. *Um número complexo* $z \in \mathbb{C}$ *é construtível se e só se* z *é algébrico sobre* $\mathbb{Q}$, *e o fecho normal* $\overline{\mathbb{Q}(z)}^n$ *tem dimensão* 2^s *para algum* $s \in \mathbb{N}$.

Demonstração. Recordemos que um número complexo $z \in \mathbb{C}$ é construtível se e só se z pertence a um subcorpo da forma $\mathbb{Q}(u_1,\ldots,u_r)$, em que ${u_1}^2 \in \mathbb{Q}$ e, para cada $m = 1,\ldots,r-1$, também ${u_{m+1}}^2 \in \mathbb{Q}(u_1,\ldots,u_m)$.

Seja então z um número construtível, de forma que $\overline{\mathbb{Q}(z)}^n \subset \overline{\mathbb{Q}(u_1,\ldots,u_r)}^n$. Se $G = \mathrm{Aut}_{\mathbb{Q}}(\overline{\mathbb{Q}(u_1,\ldots,u_r)}^n)$, então, pela Proposição 7.3.9, sabemos que o corpo $\overline{\mathbb{Q}(u_1,\ldots,u_r)}^n$ é gerado pelas imagens $\phi(\mathbb{Q}(u_1,\ldots,u_r))$, com $\phi \in G$. Logo, se $G = \{\phi_1,\ldots,\phi_n\}$ obtemos

$$\overline{\mathbb{Q}(u_1,\ldots,u_r)}^n = \mathbb{Q}(\phi_1(u_1),\ldots,\phi_1(u_r),\ldots,\phi_n(u_1),\ldots,\phi_n(u_r)).$$

Como $\phi_j(u_r)^2 = \phi_j(u_r^2)$, concluímos, ainda, que $\overline{\mathbb{Q}(u_1,\ldots,u_r)}^n$ é uma extensão da forma $\mathbb{Q}(\tilde{u}_1,\ldots,\tilde{u}_l)$ com $\tilde{u}_1^2 \in \mathbb{Q}$ e, para cada $m = 1,\ldots,l-1$, $\tilde{u}_{m+1}^2 \in \mathbb{Q}(\tilde{u}_1,\ldots,\tilde{u}_m)$. Calculando os graus algébricos, obtemos:

$$[\overline{\mathbb{Q}(u_1,\ldots,u_r)}^n : \mathbb{Q}] = \prod_{m=0}^{l-1} [\mathbb{Q}(\tilde{u}_1,\ldots,\tilde{u}_{m+1}) : \mathbb{Q}(\tilde{u}_1,\ldots,\tilde{u}_m)] = 2^t.$$

Assim, vemos que

$$[\overline{\mathbb{Q}(z)}^n : \mathbb{Q}] = \frac{[\overline{\mathbb{Q}(u_1, \ldots, u_r)}^n : \mathbb{Q}]}{[\overline{\mathbb{Q}(u_1, \ldots, u_r)}^n : \overline{\mathbb{Q}(z)}^n]} = 2^s,$$

para algum $s \in \mathbb{N}$.

Reciprocamente, suponha-se que $[\overline{\mathbb{Q}(z)}^n : \mathbb{Q}] = 2^s$. Então $\overline{\mathbb{Q}(z)}^n$ é uma extensão de Galois de $\mathbb{Q}$ cujo grupo de Galois tem ordem $|G| = 2^s$. Pelos resultados do Capítulo 5 sobre p-grupos, sabemos que existe uma torre normal de subgrupos da forma

$$G = H_s \rhd H_{s-1} \rhd \cdots \rhd H_1 \rhd H_0 = \{e\},$$

onde $[H_m : H_{m-1}] = 2$. Pela correspondência de Galois, existem extensões intermédias

$$\overline{\mathbb{Q}(z)}^n = K_s \supset K_{s-1} \supset \cdots \supset K_1 \supset \mathbb{Q},$$

onde $[K_m : K_{m-1}] = 2$. Logo, para cada $1 \leq m \leq s$, existem $u_m \in K_m$ tais que $K_{m+1} = K_m(u_{m+1})$ e ${u_{m+1}}^2 \in K_m$. Vemos, pois, que $\overline{\mathbb{Q}(z)}^n = \mathbb{Q}(u_1, \ldots, u_s)$, com ${u_{m+1}}^2 \in \mathbb{Q}(u_1, \ldots, u_m)$ para $0 \leq m \leq s-1$. Portanto, z é construtível. □

A Teoria de Galois fornece não só um critério simples para caracterizar os números construtíveis, mas também um método de construção como ilustramos no exemplo seguinte.

Exemplo 7.8.5.

Um polígono regular de 5 lados pode ser construído com régua e compasso. Se o polígono está inscrito numa circunferência de raio 1, basta mostrar que uma raiz primitiva de $x^5 - 1 = 0$ é construtível. De facto, se $r = e^{\frac{2\pi i}{5}}$, então $\overline{\mathbb{Q}(r)}^n = \mathbb{Q}(e^{\frac{2\pi i}{5}})$, e esta extensão tem grau algébrico $4 = 2^2$.

Vamos utilizar a Teoria de Galois para dar uma construção explícita de um pentágono regular. Observamos que $(x^5-1) = (x-1)(x^4+x^3+x^2+x+1)$, logo, r é uma raiz de um polinómio irredutível do quarto grau. A extensão $L = \mathbb{Q}(r)$ é uma extensão de decomposição deste polinómio, logo, é uma extensão de Galois. O grupo de Galois tem ordem $|G| = 2^2$. O $\mathbb{Q}$-automorfismo definido por $\phi(r) = r^2$ é um elemento do grupo de Galois. Se $z_k = e^{\frac{2\pi ik}{5}}$ $(k = 1, \ldots, 4)$ são as raízes, então

$$\phi(z_1) = z_2, \qquad \phi(z_2) = z_4, \qquad \phi(z_4) = z_3, \qquad \phi(z_3) = z_1,$$

e vemos que ϕ corresponde à permutação (1243). Este elemento tem ordem 4, logo, o grupo de Galois é $G = \{I, \phi, \phi^2, \phi^3\}$, ou, em termos de permutações das raízes,

$$G = \{I, (1243), (14)(23), (3241)\}.$$

Para este grupo, temos a seguinte torre de p-subgrupos:

$$G \supset H \supset \{I\},$$

onde $H = \{I, (14)(23)\}$. Como $[G : H] = 2$, a H corresponde uma extensão $\hat{K}$ de grau 2 sobre $\mathbb{Q}$. Para determinar esta extensão, observemos que um elemento $u \in L$ pode ser escrito na forma $u = a_1z_1 + a_2z_2 + a_3z_3 + a_4z_4$, logo,

$$\phi^2(u) = a_1z_4 + a_2z_3 + a_3z_2 + a_4z_1,$$

e u é fixo por $(14)(23)$ se e só se $a_1 = a_4$ e $a_2 = a_3$. Assim, $\hat{K} = \mathbb{Q}(\omega_1, \omega_2)$, onde $\omega_1 = z_1 + z_4$ e $\omega_2 = z_2 + z_3$. É simples verificar que

$$\begin{aligned}\omega_1 + \omega_2 &= z_1 + z_4 + z_2 + z_3 = r + r^2 + r^3 + r^4 = -1\\ \omega_1\omega_2 &= (r + r^4)(r^2 + r^3) = r + r^2 + r^3 + r^4 = -1,\end{aligned}$$

e, portanto,

$$(x - \omega_1)(x - \omega_2) = x^2 + x - 1.$$

Resolvendo esta equação, vemos que

$$\omega_1 = \frac{-1 + \sqrt{5}}{2}, \qquad \omega_2 = \frac{-1 - \sqrt{5}}{2}$$

(estes valores correspondem a $2\,\mathrm{Re}(z_1) = 2\,\mathrm{Re}(z_4)$ e a $2\,\mathrm{Re}(z_2) = 2\,\mathrm{Re}(z_3)$).

Com esta informação podemos explicar a forma tradicional de construir um pentágono que provavelmente aprendeu no Ensino Secundário. Numa circunferência (unitária) marcamos os quatro pontos $A = (1, 0)$, $B = (0, 1)$, $C = (-1, 0)$ e $D = (0, -1)$. Dividindo o segmento OD em duas partes iguais obtemos o ponto E. O segmento EA tem comprimento $\sqrt{5}/2$. Com o compasso centrado em E obtemos o arco AF. O segmento OF tem comprimento $\omega_1 = \frac{-1+\sqrt{5}}{2}$, e podemos marcar o ponto G no eixo horizontal, de forma que $\overline{OG} = \frac{\overline{OF}}{2}$. O ponto G corresponde à abcissa do ponto z_1 (é um pouco mais simples observar que AF tem o mesmo comprimento que um lado do pentágono).

Os Gregos sabiam construir polígonos regulares com 3, 5 e 15 lados, e, ainda, dado um polígono regular com n lados obter um com $2n$ lados (obviamente por bissecação dos lados). Gauss, quando tinha apenas 19 anos, e antes de a Teoria de Galois ter sido inventada, descobriu uma forma de construir um polígono regular com 17 lados. Esta descoberta fez com que Gauss preferisse a Matemática ao estudo das Línguas. De facto, ele apreciava tanto esta descoberta que anos mais tarde pediu para que lhe gravassem no seu túmulo um polígono regular de 17 lados (o que não veio a acontecer, pois o escultor escolhido achou que um polígono com tantos lados se confundiria com uma circunferência). Usando a Teoria de Galois pode-se mostrar que um polígono regular com n lados é construtível sse $n = 2^r p_1 \cdots p_s$ onde os p_i são primos de Fermat. Utilizando Teoria de Galois foram descobertas construções para polígonos regulares com 257 e 65 537 lados!

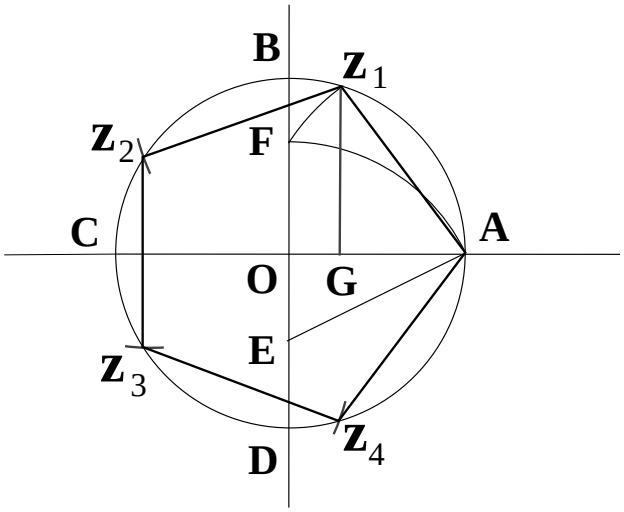


Figura 7.8.1: Construção de um pentágono com régua e compasso.

7.8.3 Resolução de equações algébricas por radicais.

Vamos agora discutir o critério descoberto por Galois que permite decidir se uma equação algébrica é ou não resolúvel por radicais. Nesta secção assume-se, para simplificar, que todos os corpos têm característica 0.

Definição 7.8.6. Seja $p(x) \in K[x]$ um polinómio mónico. Dizemos que a equação $p(x) = 0$ é RESOLÚVEL POR RADICAIS se existe uma extensão L de K que contém um corpo de decomposição de $p(x)$ e é da forma

$$L = K_{m+1} \supset \cdots \supset K_2 \supset K_1 = K,$$

onde $K_{i+1} = K_i(d_i)$ e ${d_i}^{n_i} \in K_i$.

Observe-se bem o significado desta definição: qualquer raiz de $p(x)$ pertence a L e pode ser expressa a partir de elementos de K por uma sequência de operações racionais e de extracção de raízes.

Teorema 7.8.7 (Critério de Galois). *Seja $p(x) \in K[x]$ um polinómio mónico. A equação $p(x) = 0$ é resolúvel por radicais se e só se o seu grupo de Galois é resolúvel.*

Exemplo 7.8.8.

A equação $x^5 - 4x + 2 = 0$ não é resolúvel por radicais (em $\mathbb{Q}$). Pelo Critério de Eisenstein, o polinómio $p(x) = x^5 - 4x + 2$ é irredutível sobre $\mathbb{Q}$. É fácil de ver que este polinómio possui três raízes reais r_1, r_2, r_3 e duas raízes complexas conjugadas r_4, r_5. Seja $L = \mathbb{Q}(r_1, \ldots, r_5)$ o corpo de decomposição de $p(x)$. Como $[\mathbb{Q}(r) : \mathbb{Q}] = 5$, para qualquer $r \in \{r_1, \ldots, r_5\}$, vemos que $5 \mid [L : \mathbb{Q}] = |G|$, logo, pelos Teoremas de Sylow, o grupo de Galois $G \subset S_5$ contém um

elemento de ordem 5, i.e.*, um ciclo* $(i_1, \ldots, i_5)$*. Por outro lado, a operação de conjugação* $a+ib \mapsto a-ib$ *restringida a* $L = \mathbb{Q}(r_1, \ldots, r_5)$ *fornece um elemento de* G *de ordem 2,* i.e.*, uma transposição. Deixamos como exercício verificar que estes dois elementos geram* S_5*. Logo,* $G = S_5$*, e pelo Critério de Galois a equação não é resolúvel.*

Antes de passarmos à demonstração, damos o seguinte:

Corolário 7.8.9 (Teorema de Abel-Rufini). *Não existem fórmulas resolventes para equações algébricas de grau maior ou igual a* 5*.*

Demonstração. Uma outra forma de enunciar este corolário é: *A equação geral*

$$x^n - a_{n-1}x^{n-1} + \cdots + (-1)^n a_0 = 0,$$

não é resolúvel por radicais, quando $n \geq 5$. Por "equação geral" queremos dizer que $a_0, \ldots, a_{n-1}$ tomam valores arbitrários, ou melhor, são indeterminadas. Assim, consideramos o polinómio $p(x) = x^n - a_{n-1}x^{n-1} + \cdots + (-1)^n a_0$ sobre o corpo $K(a_0, \ldots, a_{n-1})$ e precisamos de mostrar que o grupo de Galois de $p(x)$ sobre este corpo não é resolúvel.

Seja então L o corpo de decomposição de $p(x)$ sobre $K(a_0, \ldots, a_{n-1})$, de forma que em L temos a factorização:

$$p(x) = (x - r_1)(x - r_2)\ldots(x - r_n).$$

Por comparação de termos, vemos que

$$\begin{aligned} a_{n-1} &= \sum_i r_i, \\ a_{n-2} &= \sum_{i<j} r_i r_j, \\ &\vdots \\ a_0 &= r_1 r_2 \ldots r_n. \end{aligned}$$

Logo, $L = K(a_o, \ldots, a_{n-1})(r_1, \ldots, r_n) = K(r_1, \ldots, r_n)$.

Introduzimos um novo conjunto de indeterminadas $x_1, \ldots, x_n$, e no corpo $K(x_1, \ldots, x_n)$ consideramos o subcorpo das expressões racionais simétricas. Como vimos na Secção 7.8.1, este subcorpo é da forma $K(s_1, \ldots, s_n)$, onde $s_1, \ldots, s_n$ são os polinómios simétricos elementares nos $x_i's$, e $K(x_1, \ldots, x_n)$ é uma extensão de decomposição de $q(x) = \prod_i (x - x_i)$ sobre $K(s_1, \ldots, s_n)$. O grupo de Galois desta extensão é S_n.

Se existir um isomorfismo $K(r_1, \ldots, r_n) \simeq K(x_1, \ldots, x_n)$ que ao subcorpo $K(a_0, \ldots, a_{n-1})$ faz corresponder $K(s_1, \ldots, s_n)$, então o grupo de Galois da equação geral de grau n será S_n, que não é resolúvel quando $n \geq 5$. Vejamos que de facto existe um isomorfismo deste tipo.

Consideremos o homomorfismo $\phi : K[a_0, \ldots, a_{n-1}] \to K[s_1, \ldots, s_n]$ que transforma $a_i \mapsto s_{n-i}$ e se reduz à identidade em K (este homomorfismo existe, pois $a_0, \ldots, a_n$ são indeterminadas). De igual modo, temos um homomorfismo $\psi : K[x_1, \ldots, x_n] \to K[r_1, \ldots, r_n]$, e o diagrama

$$\begin{array}{ccc} K[a_0, \ldots, a_n] & \xrightarrow{\phi} & K[s_1, \ldots, s_n] \\ \big\downarrow & & \big\downarrow \\ K[r_1, \ldots, r_n] & \xleftarrow{\psi} & K[x_1, \ldots, x_n] \end{array}$$

é comutativo. De facto, basta observar que

$$\psi(\phi(a_i)) = \psi(s_i) = \psi\left(\sum_{j_1<\cdots<j_i} x_{j_1} \cdots x_{j_i}\right) = \sum_{j_1<\cdots<j_i} r_{j_1} \cdots r_{j_i} = a_i.$$

O diagrama mostra que ϕ é necessariamente um monomorfismo. Como ϕ é sobrejectivo, segue-se que ϕ é um isomorfismo. Prolongando este isomorfismo aos respectivos corpos de fracções, obtemos um isomorfismo de corpos

$$\tilde{\phi} : K(a_0, \ldots, a_{n-1}) \to K(s_1, \ldots, s_n).$$

Este isomorfismo faz corresponder a um polinómio $p(x) \in K(a_0, \ldots, a_{n-1})[x]$ o polinómio $p^{\tilde{\phi}}(x) = q(x) \in K(s_1, \ldots, s_n)[x]$. Como vimos na Secção 7.4, $\tilde{\phi}$ prolonga-se num isomorfismo dos respectivos corpos de decomposição $K(r_1, \ldots, r_n) \simeq K(x_1, \ldots, x_n)$. □

Deve-se observar que, embora o Teorema de Abel-Rufini afirme que não existe uma fórmula de resolução da equação geral de grau n, quando $n \geq 5$, existem equações que podem ser resolvidas por radicais, como por exemplo $x^5 - 2 = 0$. Poderia até acontecer que tal fórmula não existisse e todas as equações pudessem ser resolvidas por radicais, mas o exemplo da equação $x^5 - 4x + 2 = 0$ mostra que isso não é verdade.

O resto desta secção é dedicado à demonstração do Critério de Galois. Nesta demonstração os corpos de decomposição das equações $x^n - a = 0$ desempenham um papel essencial. Vimos anteriormente que o grupo de Galois de $x^n - a = 0$ é cíclico se K contém as raízes de ordem n da unidade, e é abeliano quando $a = 1$. Em geral, uma extensão L de K, cujo grupo de Galois é abeliano (respectivamente, cíclico) diz-se uma *extensão abeliana* (respectivamente, *cíclica*) de K.

Proposição 7.8.10. *Seja K um corpo que contém as p raízes de $x^p - 1 = 0$ (p um primo). Se L é uma extensão cíclica de K e $[L : K] = p$, então $L = K(r)$, onde $r^p \in K$.*

Demonstração. Se $u \in L - K$, então $L = K(u)$, pois $L \supseteq K(u) \supsetneq K$ e $[K(u) : K] \mid [L : K] = p$. Se $\mathrm{Aut}_K(L) = \langle \phi \rangle$ e $\{z_1, \ldots, z_p\} \subset K$ são as p-raízes de $x^p - 1 = 0$, introduzam-se os elementos

$$r_i = u + \phi(u)z_i + \phi^2(u){z_i}^2 + \cdots + \phi^{p-1}(u){z_i}^{p-1}, \tag{7.8.1}$$

então $\phi(r_i) = {z_i}^{-1}r_i$, logo, $\phi({r_i}^p) = {r_i}^p$, e concluímos que ${r_i}^p \in K$. Podemos escrever u como uma combinação linear dos $r_i's$ resolvendo o sistema de equações lineares (7.8.1) para as incógnitas $u, \phi(u), \ldots, \phi^{p-1}(u)$ (o que é possível, pois o respectivo determinante é um determinante de Van der Monde). Logo, $L = K(r_1, \ldots, r_p)$, e para algum k_0, $r_{k_0} \notin K$. Se tomarmos $r = r_{k_0}$, temos $L = K(r)$, com $r^p \in K$. □

Estamos finalmente em condições de demonstrar o Critério de Galois.

Demonstração do Critério de Galois. Há que mostrar ambas as implicações:

(i) *Se $p(x) = 0$ é resolúvel por radicais, então G é resolúvel:* Seja $p(x) = 0$ uma equação resolúvel por radicais. Então existe uma extensão L de K, que contém uma extensão de decomposição de $p(x)$, e que admite uma torre

$$L = K_{l+1} \supset \cdots \supset K_2 \supset K_1 = K, \tag{7.8.2}$$

onde $K_{i+1} = K_i(d_i)$, com ${d_i}^{n_i} = a_i \in K_i$. Observemos que o fecho normal $\bar{L}^n$ de L é gerado pelos $\phi(L)$, com $\phi \in \mathrm{Aut}_K(\bar{L}^n)$. Logo, se $G = \{id, \phi_1, \ldots, \phi_r\}$, obtemos

$$\bar{L}^n = K(d_1, \ldots, d_l, \phi_1(d_1), \ldots, \phi_1(d_l), \ldots, \phi_r(d_1), \ldots, \phi_r(d_l)). \tag{7.8.3}$$

Seja $m = \mathrm{mmc}(n_1, \ldots, n_l)$. Podemos estender a torre (7.8.3) a $\bar{L}^n(z)$, onde z é uma raiz primitiva de $x^m - 1 = 0$. Como $\bar{L}^n$ é o corpo de decomposição de um polinómio $p(x)$, $\bar{L}^n(z)$ é o corpo de decomposição de $p(x)(x^m - 1)$, e concluímos que $\bar{L}^n(z)$ é normal. Reordenando termos, obtemos então uma nova torre:

$$\bar{L}^n(z) \supset \cdots \supset \tilde{K}_3 \supset \tilde{K}_2 = K(z) \supset \tilde{K}_1 = K.$$

Esta torre satisfaz $\tilde{K}_{i+1} = \tilde{K}_i(\tilde{d}_i)$, com $\tilde{d}_i^{n_i} \in \tilde{K}_i$, para qualquer i.

Seja G o grupo de Galois de $p(x)$ e $H = \mathrm{Aut}_K(\bar{L}^n(z))$. Os resultados acima mostram que cada $\tilde{K}_i$ é uma extensão abeliana de $\tilde{K}_{i-1}$. Se o subgrupo $H_i \subset H$ corresponde à extensão intermédia $\tilde{K}_i$, temos que $H_{i-1} \rhd H_i$ e H_{i-1}/H_i é isomorfo ao grupo de Galois de $\tilde{K}_i$ sobre $\tilde{K}_{i-1}$, *i.e.*, é abeliano. Concluímos que H admite uma torre abeliana, sendo portanto um grupo resolúvel. Como G é um factor de H (pois $\bar{L}^n(z)$ contém um corpo de decomposição de $p(x)$), concluímos que G é resolúvel.

(ii) *Se G é resolúvel, então $p(x) = 0$ é resolúvel por radicais:* Seja L um corpo de decomposição de $p(x) = 0$ e $n = |G| = [L : K]$. Tomando $K_1 = K$,

$K_2 = K(z)$, onde z é uma raiz primitiva de $x^n - 1 = 0$, e $M = L(z)$, o grupo de Galois de M sobre K_2 é isomorfo a um subgrupo H de G. Logo, H é resolúvel e possui uma série de composição $H = H_1 \rhd H_2 \rhd \ldots \rhd = \{e\}$, em que cada H_i/H_{i+1} é cíclico de ordem prima. Pela correspondência de Galois, temos uma torre $K_2 \subset K_3 \subset \cdots \subset M$ de subcorpos em que cada K_{i+1} é uma extensão normal sobre K_i com grupo de Galois cíclico de ordem prima p_i. Como $p_i \mid n$ e K_i contém uma raiz primitiva de $x^n - 1 = 0$, vemos que K_i contém as p_i raízes de $x^{p_i} - 1 = 0$, logo, $K_{i+1} = K_i(d_i)$, com ${d_i}^{p_i} \in K_i$. Concluímos que a equação $p(x) = 0$ é resolúvel por radicais. □

Exercícios.

1. Mostre que $\frac{1}{{x_1}^3} + \frac{1}{{x_2}^3} + \frac{1}{{x_3}^3}$ é uma expressão racional simétrica e determine a sua representação em termos de polinómios simétricos elementares.

2. Determine os inteiros $1 \leq n \leq 10$, para os quais um polígono regular de n lados pode ser construído com régua e compasso.

3. Seja $G \subset S_p$ (p primo) um subgrupo que contém um ciclo de comprimento p e uma transposição. Mostre que de facto $G = S_p$.

4. Dado um grupo finito G, mostre que existem corpos L e K tais que L é uma extensão de K, com grupo de Galois G.
(SUGESTÃO: Pelo Teorema de Cayley, pode assumir-se que G é um subgrupo de S_n.)

5. Mostre que o grupo de Galois da equação $x^n - a = 0$ (sobre $\mathbb{Q}$) é resolúvel.

Capítulo 8

Álgebra Comutativa

8.1 Zeros de Um Polinómio

Chama-se Álgebra Comutativa ao estudo de anéis e módulos comutativos. Este ramo da Álgebra adquiriu durante a primeira metade do século *XX*, com as investigações de Noether[1] e de Artin, um papel central não só na Álgebra mas noutras áreas da Matemática. Neste capítulo faremos uma pequena abordagem à Álgebra Comutativa. Para uma introdução completa, a referência clássica é ainda o livro de Samuel e Zariski[2].

A abordagem que escolhemos é bastante geométrica. Virtualmente, todos os exemplos e aplicações envolvem o conjunto dos zeros de uma família de polinómios, *i.e.*, as chamadas *variedades algébricas*. O estudo das variedades algébricas é um dos objectivos da Geometria Algébrica, sendo esta, pois, uma das clientes por excelência da Álgebra Comutativa. Por exemplo, o livro de Samuel e Zariski acima referido nasceu precisamente da necessidade que o segundo autor sentiu, quando decidiu escrever um livro de Geometria Algébrica, de reunir os resultados relevantes da Álgebra (o livro de Geometria Algébrica nunca chegou a conhecer a luz do dia!). É claro que a Álgebra Comutativa possui aplicações a muitos outros domínios da Matemática.

Vejamos como algumas questões da Álgebra Comutativa surgem naturalmente no estudo das variedades algébricas. Seja $K = \mathbb{C}$ o corpo dos números complexos e $A = K[x_1, \ldots, x_n]$ o anel dos polinómios com coeficientes em K. Neste caso, podemos interpretar os polinómios $p \in A$ como funções $p : K^n \to K$. Assim, dado $p \in A$, o conjunto dos zeros de p é

[1] Emmy Noether (1822-1935), talvez a matemática mais célebre de todos os tempos, era também judia e teve de lutar contra grandes preconceitos. Leccionou em Göttingen, sob a protecção de Hilbert, mas era bastante mal paga. Entre os seus alunos contavam-se Artin, Brauer e van der Waerden. Hitler e o Nazismo obrigaram-na a emigrar para os EUA em 1933 onde viria a falecer dois anos depois.

[2] P. Samuel, O. Zariski, *Commutative Algebra* (vol. I, II), Van Nostrand, Princeton (1958, 1960).

$\mathcal{Z}(p) \equiv \{\boldsymbol{a} \in K^n : p(\boldsymbol{a}) = 0\}$. Mais geralmente, dada uma família de polinómios $F \subset A$, definimos o conjunto dos zeros desta família por

$$\mathcal{Z}(F) \equiv \{\boldsymbol{a} \in K^n : p(\boldsymbol{a}) = 0, \forall p \in F\}.$$

Uma questão natural é a seguinte: Dada uma família arbitrária de polinómios $F \subset A$, existirá uma *família finita* de polinómios $p_1, \ldots, p_n$ tal que $\mathcal{Z}(F) = \mathcal{Z}(p_1, \ldots, p_n)$? A resposta (afirmativa, como veremos mais tarde) é dada pelo famoso teorema da base de Hilbert.

Dizemos que um subconjunto $Y \subset K^n$ é um *conjunto algébrico* se Y é o conjunto dos zeros de uma família de polinómios, *i.e.*, se existe $F \subset A$ tal que $Y = \mathcal{Z}(F)$. Chama-se *variedade algébrica* a todo o subconjunto algébrico $Y \subset K^n$ irredutível, *i.e.*, que não pode ser expresso como uma união $Y = Y_1 \cup Y_2$ de dois subconjuntos algébricos próprios (cada Y_i é algébrico, e $Y_i \neq Y$).

Temos então a seguinte questão: Dado um conjunto algébrico $Y \subset K^n$, será que Y pode ser escrito como uma união de variedades algébricas? Em caso afirmativo, será que essa representação é única? Estas questões podem ser traduzidas num problema de factorização de ideais do anel $A = K[x_1, \ldots, x_n]$, como mostra o seguinte exemplo.

Exemplo 8.1.1.

Consideremos o conjunto algébrico

$$Y = \{(x, y) \in \mathbb{C}^2 : x^5 - x^3y^2 - x^4 + 2x^2y^2 - y^4 = 0\}.$$

No nosso espaço tridimensional, não possuímos uma boa representação do plano complexo. É frequente, no caso em que o polinómio tem coeficientes reais, considerar o gráfico real, que neste caso é descrito na figura seguinte.

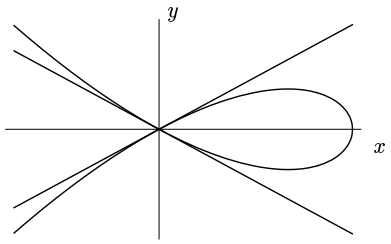


Figura 8.1.1: O gráfico real de Y.

Note-se que $Y = \mathcal{Z}(I)$, onde I é o ideal principal

$$I = \langle x^5 - x^3y^2 - x^4 + 2x^2y^2 - y^4 \rangle.$$

Como este polinómio admite a factorização

$$x^5 - x^3y^2 - x^4 + 2x^2y^2 - y^4 = (x - y)(x + y)(x^3 - x^2 + y^2),$$

temos

$$\begin{aligned} I &= \langle x-y\rangle\langle x+y\rangle\langle x^3-x^2+y^2\rangle \\ &= \langle x-y\rangle \cap \langle x+y\rangle \cap \langle x^3-x^2+y^2\rangle. \end{aligned}$$

O conjunto algébrico Y decompõe-se numa união de variedades algébricas $Y_1 \cup Y_2 \cup Y_3$, onde $Y_j = \mathcal{Z}(I_j)$, com $I_1 = \langle x-y\rangle$, $I_2 = \langle x+y\rangle$ e $I_3 = \langle x^3-x^2+y^2\rangle$. Os gráficos (reais) destas variedades são[3]*:*

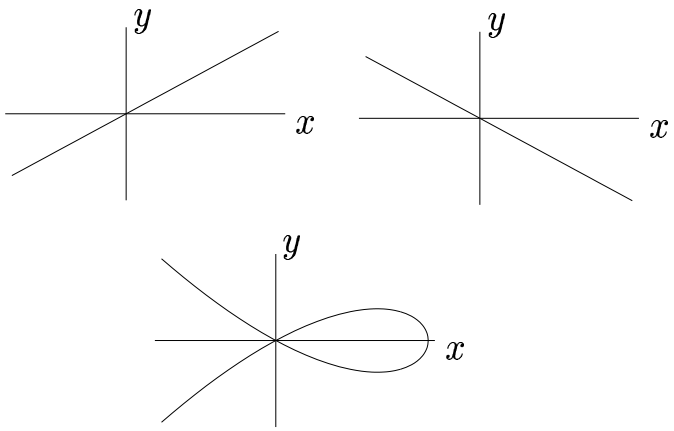


Figura 8.1.2: Os gráficos de Y_1, Y_2 e Y_3.

O exemplo que acabámos de discutir é relativamente simples, pois os ideais em questão são todos principais. Em geral, se $Y = \mathcal{Z}(I)$ é um conjunto algébrico e $I = I_1 \cap \cdots \cap I_r$ então

$$Y = \mathcal{Z}(I_1) \cup \cdots \cup \mathcal{Z}(I_r).$$

Como veremos adiante, um conjunto algébrico $Y = \mathcal{Z}(I) \subset K^n$ é irredutível se e só se I é um ideal *primário*. Assim, poderemos resolver a questão da decomposição das variedades algébricas se resolvermos o problema algébrico equivalente de factorizar um ideal em ideais primários. Estudaremos neste capítulo as factorizações primárias de ideais numa classe de anéis chamados noetherianos, que incluem os anéis de polinómios, e verificaremos o análogo da decomposição obtida no exemplo acima para ideais arbitrários, o chamado Teorema de Lasker-Noether.

Como acabámos de ver, a um ideal $I \subset A$ podemos associar um subconjunto $Y \subset K^n$. Por outro lado, a um subconjunto $Y \subset K^n$ arbitrário

[3]Como mostram estas figuras, uma variedade algébrica não é, em geral, uma variedade diferenciável. Na língua inglesa, o termo "variety" é reservado para designar uma variedade algébrica, enquanto que para uma variedade diferenciável se usa o termo "manifold".

podemos associar o ideal de A formado pelos polinómios que se anulam em Y, *i.e.*, o ideal

$$\mathcal{I}(Y) \equiv \{p \in A : p(\boldsymbol{a}) = 0, \forall \boldsymbol{a} \in Y\}.$$

Como se verifica facilmente, as correspondências $F \mapsto \mathcal{Z}(F)$ e $Y \mapsto \mathcal{I}(Y)$ invertem inclusões, *i.e.*, satisfazem:

(i) Se $F_1 \subset F_2$, então $\mathcal{Z}(F_2) \subset \mathcal{Z}(F_1)$.

(ii) Se $Y_1 \subset Y_2$, então $\mathcal{I}(Y_2) \subset \mathcal{I}(Y_1)$.

É natural investigar quais são os objectos fechados para estas correspondências. Não é difícil de ver que

$$\mathcal{Z}(\mathcal{I}(Y)) = \bar{Y},$$

onde $\bar{Y}$ designa a intersecção de todos os conjuntos algébricos que contêm Y. Se em K^n tomarmos a topologia em que os fechados são os conjuntos algébricos, então $\bar{Y}$ é o fecho de Y nesta topologia, a chamada *topologia de Zariski*. Por outro lado, se $I \subset A$ é um ideal, o *Teorema dos Zeros de Hilbert*[4] afirma que:

$$\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I},$$

onde $\sqrt{I}$ é o *radical* de I, o ideal de A definido por

$$\sqrt{I} \equiv \{p \in A : \exists m \in \mathbb{N},\ p^m \in I\}.$$

Exemplo 8.1.2.

Consideremos o ideal $I = \langle x^2, xy\rangle \subset K(x,y)$. É óbvio que o conjunto algébrico correspondente é $\mathcal{Z}(I) = \{(x,y) : x = 0\}$. Mostraremos que o radical de I é precisamente $\sqrt{I} = \langle x\rangle = \mathcal{I}(\mathcal{Z}(I))$.

Os exemplos acima mostram, pois, como o estudo de zeros de polinómios está intimamente relacionado com o estudo dos anéis comutativos e dos seus ideais. É este estudo que vamos desenvolver neste capítulo.

8.2 Módulos e Anéis Noetherianos

Neste capítulo, A designa um anel comutativo.

Aquando do estudo de domínios de factorização única, vimos que estes podiam ser caracterizados em termos de cadeias ascendentes de ideais principais. Estudamos nesta secção módulos e anéis que satisfazem a uma condição análoga.

[4]Este resultado é frequentemente conhecido pela sua designação alemã *Nullstellensatz von Hilbert.*

Definição 8.2.1. Seja M um A-módulo. Dizemos que M é um A-MÓDULO NOETHERIANO se toda a cadeia ascendente de submódulos de M,

$$N_1 \subset N_2 \subset \cdots \subset N_k \subset \ldots,$$

estabiliza, *i.e.*, existe $k_0 \in \mathbb{N}$ tal que $N_{k_0} = N_{k_0+1} = \ldots$

Recordamos que todo o anel comutativo A é, trivialmente, um A-módulo. Dizemos que A é um ANEL NOETHERIANO se A é noetheriano como um A-módulo. Como neste caso os submódulos de A são precisamente os ideais de A, isto significa que toda a cadeia ascendente de ideais de A

$$I_1 \subset I_2 \subset \cdots \subset I_k \subset \ldots$$

estabiliza.

Proposição 8.2.2. *Seja M um A-módulo. As seguintes afirmações são equivalentes.*

(i) M é um A-módulo noetheriano.

(ii) Todo o submódulo de M é de tipo finito.

(iii) Um conjunto $\{N_j\}_{j\in J}$ não-vazio de submódulos de M possui um elemento maximal.

Demonstração. Vejamos separadamente as equivalências (i) $\Leftrightarrow$ (ii) e (i) $\Leftrightarrow$ (iii).

(i) $\Leftrightarrow$ (ii): Seja N um submódulo de um módulo noetheriano M, e S um conjunto gerador de N. Se $\boldsymbol{v}_1 \in S$ e $N = \langle \boldsymbol{v}_1 \rangle$, não há nada a mostrar, caso contrário, existe $\boldsymbol{v}_2 \in S - \langle \boldsymbol{v}_1 \rangle$ e $\langle \boldsymbol{v}_1 \rangle \subsetneq \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle$. Procedendo indutivamente, construímos $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in S$ tais que temos uma cadeia ascendente:

$$\langle \boldsymbol{v}_1 \rangle \subsetneq \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle \subsetneq \cdots \subsetneq \langle \boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \rangle.$$

Depois de um número finito de passos, obtemos $N = \langle \boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \rangle$, senão produzíamos uma cadeia ascendente de submódulos que não estabilizava. Logo, N é de tipo finito.

Inversamente, se M satisfaz a (ii) e

$$N_1 \subset N_2 \subset \cdots \subset N_k \subset \ldots$$

é uma cadeia ascendente de submódulos, o módulo $\bigcup_{k=1}^{\infty} N_k$ é de tipo finito. Se $S = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}$ é um conjunto gerador, então para cada $1 \leq i \leq r$ existe um inteiro k_i tal que $\boldsymbol{v}_i \in N_{k_i}$. Seja $k_0 = \max\{k_1, \ldots, k_r\}$. Então $S \subset \bigcup_{k=1}^{k_0} N_k = N_{k_0}$, logo, $N_{k_0} = N_{k_0+1} = \ldots$ e M é noetheriano.

(i) $\Leftrightarrow$ (iii) Seja M noetheriano e $\mathcal{P} = \{N_j\}_{j\in J}$ um conjunto não-vazio de submódulos de M. Fixe-se $N_1 \in \mathcal{P}$. Se N_1 é maximal, não há nada a

mostrar. Caso contrário, existe um submódulo $N_2 \in \mathcal{P}$ tal que $N_1 \subsetneq N_2$. Procedendo indutivamente, obtemos uma cadeia ascendente

$$N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_k.$$

Depois de um número finito de passos, obtemos necessariamente um submódulo maximal N_k, senão produzíamos uma cadeia ascendente que não estabilizava. Logo M satisfaz a (iii).

Inversamente, suponha-se que M satisfaz a (iii) e seja

$$N_1 \subset N_2 \subset \cdots \subset N_k \subset \ldots$$

uma cadeia ascendente de submódulos de M. A família $\{N_k\}_{k\in\mathbb{N}}$ possui um elemento maximal N_{k_0}. Mas então $N_{k_0} = N_{k_0+1} = \ldots$, e portanto M é noetheriano. □

Exemplos 8.2.3.

1. *Todo o domínio de ideais principais é noetheriano. De facto, para estes anéis todo o ideal, sendo principal, é de tipo finito, e a proposição aplica-se. Em particular, $\mathbb{Z}$ e $K[x]$ são anéis noetherianos.*

2. *Veremos mais à frente que, se A é um anel noetheriano, o anel dos polinómios $A[x_1, \ldots, x_n]$ é um anel noetheriano. Por outro lado, $A[x_1, \ldots, x_n]$ é um A-módulo que não é noetheriano, pois como A-módulo não possui um conjunto gerador finito.*

Vejamos como podemos construir outros exemplos de módulos noetherianos.

Proposição 8.2.4. *Seja $0 \to M_1 \to M_2 \to M_3 \to 0$ uma sequência exacta de A-módulos. Então M_2 é noetheriano se e só se M_1 e M_3 são noetherianos.*

Demonstração. Dividimos a demonstração em duas partes.

(i) Se M_1 e M_2/M_1 são noetherianos, então M_2 é noetheriano: Seja $N \subset M_2$ um submódulo. É preciso mostrar que N é de tipo finito. Por um lado, $(N + M_1)/M_1$ é um submódulo de M_2/M_1, logo, é de tipo finito, e podemos escolher $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\} \subset N$ tais que $\{\pi(\boldsymbol{v}_1), \ldots, \pi(\boldsymbol{v}_r)\}$ é um conjunto gerador de $(N + M_1)/M_1$ (onde $\pi : M_2 \to M_2/M_1$ é a projecção canónica). Por outro lado, $N \cap M_1$ é um submódulo de M_1, logo, é de tipo finito e possui um conjunto gerador $\{\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_s\}$. Deixamos como exercício verificar que $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r, \boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_s\}$ é um conjunto gerador de N.

(ii) Se M_2 é noetheriano, então M_1 e M_2/M_1 são noetherianos: Se N é um submódulo de M_1, então N é um submódulo de M_2, logo, N é de tipo finito. Portanto, M_1 é noetheriano. Por outro lado, todo o submódulo de M_2/M_1 é da forma N/M_1, onde $M_1 \subset N \subset M_2$ é um submódulo. Como N possui um conjunto gerador finito $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}$, se $\pi : M_2 \to M_2/M_1$ é a projecção canónica, então $\{\pi(\boldsymbol{v}_1), \ldots, \pi(\boldsymbol{v}_r)\}$ é um conjunto gerador de N/M_1. Logo, M_2/M_1 é noetheriano. □

Corolário 8.2.5. *Se $N_1, \ldots, N_r$ são submódulos noetherianos dum módulo M e $M = \sum_{i=1}^{r} N_i$, então M é noetheriano.*

Demonstração. Por indução, basta demonstrar o caso $r = 2$. Se N_1 e N_2 são noetherianos, a sequência exacta $0 \to N_1 \to N_1 \oplus N_2 \to N_2 \to 0$ mostra que $N_1 \oplus N_2$ é noetheriano. Se $M = N_1 + N_2$ e $\pi : N_1 \oplus N_2 \to M$ é o homomorfismo definido por $\pi(\boldsymbol{v}_1, \boldsymbol{v}_2) = \boldsymbol{v}_1 + \boldsymbol{v}_2$, então a sequência exacta

$$0 \longrightarrow N(\pi) \longrightarrow N_1 \oplus N_2 \xrightarrow{\pi} M \longrightarrow 0$$

mostra que M é noetheriano. □

Se M é um A-módulo noetheriano, então todos os seus submódulos são de tipo finito. Em particular, M é de tipo finito. Inversamente, temos o seguinte corolário:

Corolário 8.2.6. *Seja A um anel noetheriano e M um A-módulo de tipo finito. Então M é noetheriano*

Demonstração. Seja $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}$ um conjunto gerador de M e seja $\pi : \bigoplus_{i=1}^{r} A \to M$ o homomorfismo $\pi(a_1, \ldots, a_r) = \sum_{i=1}^{r} a_i \boldsymbol{v}_i$. A sequência

$$0 \longrightarrow N(\pi) \longrightarrow \bigoplus_{i=1}^{r} A \xrightarrow{\pi} M \longrightarrow 0$$

é exacta e, pelo corolário anterior, sabemos que $\bigoplus_{i=1}^{r} A$ é noetheriano. Logo, pela proposição, M é noetheriano. □

O próximo resultado é básico na teoria das variedades algébricas.

Teorema 8.2.7 (Teorema da Base de Hilbert). *Seja A um anel noetheriano. Então o anel dos polinómios $A[x_1, \ldots, x_n]$ é noetheriano.*

Demonstração. Por indução, basta demonstrar o caso $n = 1$, *i.e.*, que $A[x]$ é noetheriano sempre que A é noetheriano. Para isso mostramos que, se $I \subset A[x]$ é um ideal, então é de tipo finito.

Definimos ideais $I_j \subset A$ da seguinte forma: $0 \in I_j$ e um elemento $a \neq 0$ pertence a I_j se e só se existe um polinómio $p(x) \in I$ de grau j com coeficiente de maior grau $a_j = a$:

$$p(x) = a_0 + a_1 x + \cdots + a_{j-1} x^{j-1} + a x^j \in I.$$

Os ideais I_j formam uma cadeia ascendente

$$I_0 \subset I_1 \subset \cdots \subset I_k \subset \ldots$$

De facto, se $a \in I_k$, então existe $p(x) \in I$ tal que $p(x) = a_0 + \cdots + a_{k-1} x^{k-1} + a x^k$. Logo, $xp(x) = a_0 x + \cdots + a_{k-1} x^k + a x^{k+1} \in I$ e, portanto, $a \in I_{k+1}$.

Como A é noetheriano, existe $k_0 \in \mathbb{N}_0$ tal que $I_{k_0} = I_{k_0+1} = \ldots$, e os ideais $I_0, \ldots, I_{k_0}$ são de tipo finito. Para cada $0 \leq j \leq k_0$ seja $\{a_{j1}, \ldots, a_{jn_j}\}$ um conjunto gerador de I_j, de forma que existem polinómios $p_{ji}(x) \in I$ tais que

$$p_{ji}(x) = \cdots + a_{ji}x^j \qquad (i = 1, \ldots, n_j),$$

Para terminar a demonstração, mostramos que os $\{p_{ji}(x)\}$ formam um conjunto gerador de I. Seja então $p(x) = \cdots + ax^k \in I$ um polinómio de grau k. Mostramos por indução em k que

$$p(x) \in \langle \{p_{ji}(x)\} \rangle. \tag{8.2.1}$$

Se $k = 0$, isto é óbvio. Se $k > 0$, há a considerar dois casos:

(a) Se $k \leq k_0$ então $a \in I_k$. Existem, pois, coeficientes $b_i \in A$ tais que $a = \sum_{i=1}^{n_k} b_i a_{ki}$. Mas então $p(x) - \sum_{i=1}^{n_k} b_i p_{ki}(x) \in I$ é um polinómio de grau $\leq k - 1$.

(b) Se $k > k_0$, então $a \in I_{k_0}$. Existem, pois, coeficientes $b_i \in A$ tais que $a = \sum_{i=1}^{n_{k_0}} b_i a_{k_0 i}$. Mas então $p(x) - \sum_{i=1}^{n_{k_0}} b_i x^{k-k_0} p_{k_0 i}(x) \in I$ é um polinómio de grau $\leq k - 1$.

Logo, por indução, (8.2.1) verifica-se. □

Pelo Teorema da Base de Hilbert e pela Proposição 8.2.2, concluímos que:

Corolário 8.2.8. *Se A é noetheriano, então qualquer ideal $I \subset A[x_1, \ldots, x_n]$ é de tipo finito.*

Isto é, para qualquer ideal $I \subset A[x_1, \ldots, x_n]$, existem sempre polinómios $p_1, \ldots, p_m \in I$ tais que qualquer outro polinómio $p \in I$ pode ser escrito como combinação linear dos p_i com coeficientes em $A[x_1, \ldots, x_n]$:

$$p(x_1, \ldots, x_n) = \sum_{i=1}^{m} b_i(x_1, \ldots, x_n) p_i(x_1, \ldots, x_n).$$

Isto justifica o uso do termo "base" (observe-se no entanto que, em geral, os coeficientes b_i não são únicos).

Exemplo 8.2.9.

Seja K um corpo. Considere-se o anel $A = K[x_1, \ldots, x_n]$ dos polinómios com coeficientes em K. Se $F \subset A$ é uma família de polinómios, designamos por $\mathcal{Z}(F)$ o conjunto dos zeros comuns aos polinómios de F:

$$\mathcal{Z}(F) = \{\boldsymbol{a} \in K^n : p(\boldsymbol{a}) = 0, \forall p \in F\}.$$

Por definição, um CONJUNTO ALGÉBRICO *$Y \subset K^n$ é um conjunto para o qual existe uma família $F \subset A$ tal que $Y = \mathcal{Z}(F)$. Desta forma, obtemos uma*

correspondência que a subconjuntos $F \subset A$ associa conjuntos algébricos de K^n.

Se $F \subset A$ e $I = \langle F \rangle$ é o ideal gerado pelos polinómios da família F, então é óbvio que $\mathcal{Z}(F) = \mathcal{Z}(I)$. O Teorema da Base de Hilbert mostra então que qualquer conjunto algébrico Y é de facto o conjunto dos zeros de uma família finita de polinómios: $Y = \mathcal{Z}(p_1, \ldots, p_n)$.

Dado um conjunto $O \subset K^n$, dizemos que O é ABERTO *se o seu complementar é um conjunto algébrico. Deixamos como exercício verificar as seguintes propriedades:*

(Z1) $\emptyset$ e K^n são conjuntos abertos.

(Z2) Se $\{O_j\}_{j \in J}$ são abertos, então $\bigcup_{j \in J} O_j$ é aberto.

(Z3) Se $\{O_1, \ldots, O_m\}$ são abertos, então $\bigcap_{j=1}^{m} O_j$ é aberto.

A família dos abertos verifica, pois, as propriedades de uma topologia, que se designa por TOPOLOGIA DE ZARISKI. *Os fechados desta topologia são, por construção, os conjuntos algébricos. A condição sobre cadeias de ideais ascendentes quando traduzida em termos desta topologia significa o seguinte: toda a cadeia ascendente de conjuntos abertos*

$$O_1 \subset O_2 \subset \cdots \subset O_k \subset \ldots$$

estabiliza, i.e.*, existe $k_0 \in \mathbb{N}$ tal que $O_{k_0} = O_{k_0+1} = \ldots$ A uma topologia que satisfaz esta condição chama-se por vezes* topologia Noetheriana.

Se $Y \subset K^n$ é um conjunto arbitrário, e $\mathcal{I}(Y) = \{p \in A : p(\boldsymbol{a}) = 0, \forall \boldsymbol{a} \in Y\}$ então deixamos como exercício verificar que

$$\mathcal{Z}(\mathcal{I}(Y)) = \bar{Y},$$

onde $\bar{Y}$ designa o fecho de Y na topologia de Zariski.

Exercícios.

1. Complete os detalhes da demonstração da Proposição 8.2.4.

2. Seja A um anel noetheriano e $\phi : A \to B$ um epimorfismo de anéis. Mostre que B é noetheriano.

3. Mostre que, se A é um anel noetheriano, então o anel das séries de potências $A[[x_1, \ldots, x_n]]$ é noetheriano.

4. Mostre que uma anel A é noetheriano se e só se todo o ideal $P \subset A$ é finitamente gerado.

5. Mostre que, se definir os abertos como sendo os complementares dos conjuntos algébricos, então obtém-se uma topologia, *i.e.*, que (Z1), (Z2) e (Z3) são satisfeitas.

6. Mostre que a topologia de Zariski em $K^1 = K$ não é separável, *i.e.*, existem $a, a' \in K$, com $a \neq a'$, para os quais não é possível encontrar abertos disjuntos O, O', tais que $a \in O$ e $a' \in O'$.

7. Se $Y \subset K^n$ mostre que $\mathcal{Z}(\mathcal{I}(Y)) = \bar{Y}$, onde $\bar{Y}$ designa o fecho de Y na topologia de Zariski (*i.e.*, o menor fechado que contém Y).

8.3 Factorização de Ideais

Num anel comutativo A existem cinco operações básicas sobre ideais que passamos a enumerar:

(i) Produto de ideais: $IJ = \{i_1 j_1 + \cdots + i_r j_r : i_k \in I, j_k \in J\}$.

(ii) Soma de ideais: $I + J = \{i + j : i \in I, j \in J\}$.

(iii) Intersecção de ideais: $I \cap J = \{a : a \in I \text{ e } a \in J\}$.

(iv) Quociente de ideais: $I : J = \{a : ja \in I \text{ para todo o } j \in J\}$.

(v) Radical de um ideal: $\sqrt{I} = \{a : a^n \in I \text{ para algum } n \in \mathbb{N}\}$.

No caso clássico em que $A = \mathbb{Z}$, os ideais são todos principais e temos $\langle i \rangle \subset \langle j \rangle$ se e só se $j \mid i$. Neste caso, as operações acima estão intimamente ligadas com factorizações dos elementos de $\mathbb{Z}$. De facto, deixamos como exercício verificar que:

(i) $\langle i \rangle \langle j \rangle = \langle ij \rangle$;

(ii) $\langle i \rangle + \langle j \rangle = \langle \text{mdc}(i, j) \rangle$;

(iii) $\langle i \rangle \cap \langle j \rangle = \langle \text{mmc}(i, j) \rangle$;

(iv) $\langle i \rangle : \langle j \rangle = \langle \frac{i}{\text{mdc}(i,j)} \rangle$;

(v) $\sqrt{\langle i \rangle} = \langle p_1 \cdots p_s \rangle$ se $p_1^{n_1} \ldots p_s^{n_s}$ é a factorização prima de i.

Nesta secção utilizamos estas operações básicas sobre ideais para obter factorizações de ideais em anéis noetherianos.

De todas as construções acima, o radical de um ideal é a única que não estudámos anteriormente. Vejamos então mais pormenorizadamente esta construção. Recordemos primeiro a seguinte definição.

Definição 8.3.1. Um ideal $P \subset A$ diz-se um IDEAL PRIMO se $P \neq A$ e

$$ab \in P \quad \Longrightarrow \quad a \in P \text{ ou } b \in P.$$

No caso de um domínio de ideais principais D, um ideal $P \subset D$ é primo se e só se $P = \langle p \rangle$ com $p \in D$ primo. No caso geral, isto não é verdade (por exemplo, no anel de polinómios a duas varáveis $K[x, y]$, o ideal $\langle x, y \rangle$ é primo). No entanto, a propriedade de um ideal P ser primo pode ser expressa em termos do anel quociente A/P: um ideal $P \subset A$ é primo se e só se A/P é um domínio integral (exercício). É claro que um ideal maximal é necessariamente primo, mas o inverso não é verdade.

Temos as seguintes propriedades básicas do radical de ideais.

Proposição 8.3.2. *Seja A um anel comutativo e sejam $I, I_1, \ldots, I_r$ ideais de A. Então:*

(i) $\sqrt{\sqrt{I}} = \sqrt{I}$;

(ii) $\sqrt{I_1 \cdots I_r} = \sqrt{\bigcap_{j=1}^{r} I_j} = \bigcap_{j=1}^{r} \sqrt{I_j}$;

(iii) $\sqrt{I^r} = \sqrt{I}$;

(iv) $\sqrt{I} = \bigcap\limits_{\substack{P \supset I \\ P \text{ primo}}} P$ *(se não existe $P \supset I$ primo então $\sqrt{I} = A$).*

Demonstração. A demonstração de (i), (ii) e (iii) é deixada como exercício. Para mostrar que (iv) é verdadeira, mostramos as duas inclusões:

(a) Se $a \in \sqrt{I}$ e $P \supset I$ é primo, então $a^n \in I \subset P$ para algum n. Logo $a \in P$. Assim, vemos que:

$$\sqrt{I} \subset \bigcap_{\substack{P \supset I \\ P \text{ primo}}} P.$$

(b) Seja $a \in A$ um elemento que pertence a todos os ideais primos $P \supset I$ e suponha-se, por absurdo, que $a^n \notin I$, para todo o natural $n \in \mathbb{N}$. Então o conjunto $S = \{a^n + x : n \in \mathbb{N}, x \in I\}$ é disjunto de I. Afirmamos que neste caso existiria um ideal primo P_0, disjunto de S, e contendo I, o que é uma contradição.

Para mostrar que P_0 existe, utilizamos o Lema de Zorn. O conjunto $\mathcal{P}$ formado por todos os ideais disjuntos de S e que contêm I é não-vazio (pois contém I) e é parcialmente ordenado para a relação de inclusão. Em $\mathcal{P}$ qualquer cadeia possui um elemento maximal (a união dos elementos da cadeia), logo, pelo Lema de Zorn, existe em $\mathcal{P}$ um ideal maximal P_0. Vejamos que P_0 é primo: Seja $b_1 b_2 \in P_0$. Se b_1 e b_2 não pertencem a P_0, então $(\langle b_1 \rangle + P_0) \cap S \neq \emptyset$ e $(\langle b_2 \rangle + P_0) \cap S \neq \emptyset$ (por maximalidade de P_0), logo, existem $d_1, d_2 \in A$, $x_1, x_2 \in I$, $n_1, n_2 \in \mathbb{N}$ e $p_1, p_2 \in P_0$ tais que

$$d_1 b_1 + p_1 = x_1 + a^{n_1}, \qquad d_2 b_2 + p_2 = x_2 + a^{n_2},$$

donde, por um lado,

$$(d_1b_1 + p_1)(d_2b_2 + p_2) = x_1x_2 + x_1a^{n_2} + x_2a^{n_1} + a^{n_1+n_2} \in S,$$

e, por outro lado,

$$(d_1b_1 + p_1)(d_2b_2 + p_2) = d_1d_2b_1b_2 + d_1b_1p_2 + d_2b_2p_1 + p_1p_2 \in P_0,$$

contradizendo $P_0 \cap S = \emptyset$. Logo, $b_1 \in P_0$ ou $b_2 \in P_0$ e, portanto, P_0 é primo.

Assim, vemos também que:

$$\bigcap_{\substack{P \supset I \\ P \text{ primo}}} P \subset \sqrt{I}.$$

□

Exemplo 8.3.3.

Seja $A = K[x, y]$ o anel dos polinómios em duas variáveis sobre um corpo K. Em A considere-se o ideal $I = \langle x^2, xy\rangle$. Então $\langle x\rangle \subset \sqrt{I}$, pois $x^2 \in I$. Por outro lado, o ideal $\langle x\rangle$ é primo e $I \subset \langle x\rangle$, logo, pela proposição $\sqrt{I} \subset \langle x\rangle$, e concluímos que $\sqrt{I} = \langle x\rangle$.

No exemplo anterior, o leitor deverá ter presente que o conjunto das soluções do sistema

$$\begin{cases} x^2 = 0 \\ xy = 0 \end{cases}$$

coincide com os zeros do polinómio $p(x, y) = x$. Voltaremos a esta questão mais adiante.

Introduzimos agora uma noção um pouco mais geral.

Definição 8.3.4. Um ideal $Q \subset A$ diz-se um IDEAL PRIMÁRIO se $Q \neq A$ e

$$ab \in Q \Longrightarrow a \in Q \text{ ou } b \in \sqrt{Q}.$$

Exemplos 8.3.5.

1. *No anel $\mathbb{Z}$ o ideal $\langle p\rangle$ é primo sempre que $p \in \mathbb{Z}$ é primo. Por outro lado, o ideal $\langle p^n\rangle$ ($n \in \mathbb{N}$) é primário: se $ab \in \langle p^n\rangle$, então p aparece na decomposição prima de ab, logo, se $a \notin \langle p^n\rangle$, então b tem p como factor primo, e alguma potência $b^m \in \langle p^n\rangle$,* i.e., *$b \in \sqrt{\langle p^n\rangle}$.*

2. *Num d.i.p. D um ideal $Q \subset D$ é primário se e só se $Q = \langle p^n\rangle$, com p primo e $n \in \mathbb{N}$. Nesse caso, $\sqrt{Q} = \sqrt{\langle p^n\rangle} = \langle p\rangle$ (exercício).*

3. *Se $P \subset A$ é um ideal primo e $n \in \mathbb{N}$, então P^n é um ideal primário.*

4. *No anel $A = K[x, y]$ o ideal $Q = \langle x^2, y\rangle$ é primário (verifique!). Existe um único ideal primo que contém Q, nomeadamente $\langle x, y\rangle$. Como $\langle x, y\rangle^2 \subsetneq Q \subsetneq \langle x, y\rangle$, vemos que Q não é uma potência de um ideal primo.*

Como mostra o último exemplo, em geral um ideal primário não é uma potência de um ideal primo. No entanto, o seu radical é sempre primo, como mostra a seguinte proposição:

Proposição 8.3.6. *Se Q é um ideal primário, então $\sqrt{Q}$ é primo.*

Demonstração. Se $ab \in \sqrt{Q}$, então $a^n b^n \in Q$ para algum $n \in \mathbb{N}$. Como Q é primário, vemos que $a^n \in Q$ ou $(b^n)^m \in Q$, para algum $m \in \mathbb{N}$. Logo, $a \in \sqrt{Q}$ ou $b \in \sqrt{Q}$, e $\sqrt{Q}$ são primos. □

Pode ainda acontecer que $\sqrt{I}$ seja um ideal primo, mas I não seja um ideal primário, como mostra o exemplo seguinte:

Exemplo 8.3.7.

Seja $A = K[x, y]$. Vimos, num exemplo acima, que o ideal $I = \langle x^2, xy\rangle$ tem radical $\sqrt{I} = \langle x\rangle$, um ideal primo. Por outro lado, I não é primário, pois $x \notin I$, $y^n \notin I$ para todo o $n \in \mathbb{N}$, e $xy \in I$.

Recordemos que os anéis $\mathbb{Z}(\sqrt{n})$ (n um inteiro que não é um quadrado perfeito) são, em geral, domínios onde factorização sem unicidade ocorre. Historicamente, o conceito de ideal foi introduzido como uma forma de "salvar" a unicidade de factorização nestes tipos de domínios (daí o seu nome!). Neste contexto, a seguinte definição é natural:

Definição 8.3.8. Um ideal $I \subset A$ diz-se um IDEAL IRREDUTÍVEL se $I \neq A$ não for a intersecção de dois ideais que o contêm (estritamente).

Antes de discutirmos o resultado fundamental que relaciona factorização e ideais, vejamos alguns exemplos motivadores.

Exemplos 8.3.9.

1. *Seja D um d.i.p. Se $I = \langle d\rangle \subset D$ é um ideal, e d admite a factorização em potências primas*

$$d = {p_1}^{m_1} \cdots p_r^{m_r},$$

então obtemos a factorização de ideais

$$\begin{aligned}\langle d\rangle &= \langle p_1^{m_1}\rangle \cdots \langle p_r^{m_r}\rangle \\ &= \langle p_1^{m_1}\rangle \cap \cdots \cap \langle p_r^{m_r}\rangle.\end{aligned}$$

Note que os ideais $\langle p_j^{m_j}\rangle$ são ideais primários.

2. Seja $A = K[x, y]$. O ideal $I = \langle x^2, xy\rangle$ pode ser escrito como um intersecção

$$I = \langle x\rangle \cap \langle x^2, y\rangle.$$

Como vimos nos exemplos acima, os ideais $\langle x\rangle$ e $\langle x^2, y\rangle$ são primários.

A característica comum aos anéis D e $K[x, y]$ é a que ambos são anéis noetherianos. Para estes, temos o seguinte resultado fundamental:

Teorema 8.3.10 (Lasker-Noether). *Seja A um anel noetheriano, e $I \subset A$ um ideal. Então existem ideais primários $Q_1, \ldots, Q_r$ tais que*

$$I = Q_1 \cap \cdots \cap Q_r.$$

Demonstração. Dividimos a demonstração em dois passos.

(a) *Todo o ideal $I \subset A$ é uma intersecção finita de ideais irredutíveis:* Suponha-se, por absurdo, que tal não acontece. Então mostramos que podemos encontrar uma cadeia de ideais com a mesma propriedade

$$I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_k \subsetneq \cdots,$$

o que contraria a hipótese de A ser noetheriano. A cadeia é obtida por indução: $I_1 = I$, e suponha-se que construímos I_k, um ideal que não é intersecção finita de ideais irredutíveis. Então $I_k = I_k^1 \cap I_k^2$, com $I_k \neq I_k^1, I_k^2$, e onde pelo menos um dos factores não é intersecção finita de ideais irredutíveis. Escolhemos esse factor para I_{k+1}.

(b) *Todo o ideal irredutível é primário:* Seja Q um ideal que não é primário. Então existe $ab \in Q$ tal que $a \notin Q$ e $b^n \notin Q$, para todo o $n \in \mathbb{N}$. A cadeia

$$Q : \langle b\rangle \subset Q : \langle b^2\rangle \subset \cdots \subset Q : \langle b^n\rangle \subset \cdots$$

estabiliza, *i.e.*, existe $n_0 \in \mathbb{N}$ tal que $Q : \langle b^{n_0}\rangle = Q : \langle b^{n_0+1}\rangle = \ldots$ Mostramos que

$$Q = (Q + \langle a\rangle) \cap (Q + \langle b^{n_0}\rangle), \tag{8.3.1}$$

mostrando, assim, que (b) se verifica.

É claro que Q está contido na intersecção (8.3.1). Por outro lado, seja x um elemento desta intersecção, de forma que

$$\begin{cases} x &= q_1 + c_1 a, \\ x &= q_2 + c_2 b^{n_0}, \end{cases} \qquad q_1, q_2 \in Q,\ c_1, c_2 \in A.$$

Então, multiplicando a primeira equação por b, obtemos:

$$bx = bq_1 + c_1 ab \in Q.$$

Multiplicando agora a segunda equação por b, obtemos:

$$bx = bq_2 + c_2 b^{n_0+1} \in Q.$$

Logo, $c_2 b^{n_0+1} \in Q$, e concluímos que

$$c_2 \in Q : \langle b^{n_0+1} \rangle = Q : \langle b^{n_0} \rangle.$$

Portanto, $x = q_2 + c_2 b^{n_0} \in Q$. Vemos, pois, que a intersecção (8.3.1) se verifica. □

Se $I \subset A$ é um ideal, uma decomposição primária

$$I = Q_1 \cap \cdots \cap Q_r$$

diz-se *reduzida*, se nenhum Q_i está contido numa intersecção $Q_{i_1} \cap \cdots \cap Q_{i_s}$ ($i \notin \{i_1, \ldots, i_s\}$) e os radicais $\sqrt{Q_i}$ são todos distintos. Se um ideal possui uma decomposição primária, então podemos eliminar factores, de forma a obter uma decomposição primária reduzida. Pode-se mostrar que, se um ideal possui duas decomposições primárias reduzidas

$$\begin{aligned} I &= Q_1 \cap \cdots \cap Q_r \\ &= \tilde{Q}_1 \cap \cdots \cap \tilde{Q}_s, \end{aligned}$$

então $r = s$, e as listas dos radicais dos Q_i e dos $\tilde{Q}_j$ são iguais. Neste sentido, a decomposição primária reduzida de um ideal é única.

Exercícios.

1. Verifique as propriedades (i)-(v) das operações básicas sobre ideais de $\mathbb{Z}$. Em que outros anéis são válidas estas propriedades?

2. Demonstre as propriedades (i), (ii) e (iii) do radical de ideais.

3. Seja D um d.i.p. Mostre que:
   (a) Um ideal $P \neq \{0\}$ é primo se e só se $P = \langle p \rangle$, onde $p \in D$ é primo.
   (b) Um ideal $Q \neq \{0\}$ é primário se e só se $Q = \langle p \rangle^n$, onde $p \in D$ é primo e $n \in \mathbb{N}$.

4. Seja A um anel e $P \subset A$ um ideal. Mostre que P é primo se e só se A/P é um domínio integral.

5. Determine o radical $\sqrt{I}$ de cada um dos seguintes ideais de $K[x, y]$:
   (a) $I = \langle x^2, y \rangle$;
   (b) $I = \langle x^3, xy, y^2 \rangle$.

6. Seja A um anel noetheriano. Um ideal primário de A é necessariamente irredutível?

7. Determine decomposições primárias para cada um dos seguintes ideais:
   (a) $I = \langle 4, 2x, x^2 \rangle$ em $\mathbb{Z}[x]$;
   (b) $I = \langle 9, 3x + 3 \rangle$ em $\mathbb{Z}[x]$;
   (c) $I = \langle x^3 - xy, 3x^2 - xy, 3x^2y - y^2 \rangle$ em $K[x, y]$.

8. Mostre que o ideal $I = \langle x^2, xy \rangle \subset K[x, y]$ admite as seguintes decomposições primárias distintas:
$$I = \langle x \rangle \cap \langle x^2, y \rangle = \langle x \rangle \cap \langle x^2, x + y \rangle = \langle x \rangle \cap \langle x^2, xy, y^2 \rangle.$$
Verifique que estas decomposições são reduzidas e calcule os radicais associados a cada componente primária.

9. Mostre que, se $I_1, \ldots, I_r$ são ideais maximais distintos de um anel A, então $I_1 \cap \cdots \cap I_r = I_1 \cdots I_r$. Será isto verdadeiro se "maximal" for substituído por "primo"?

8.4 Ideais Maximais e o Lema de Nakayama

Nesta secção discutimos ideais maximais no anel dos polinómios $K[x_1, \ldots, x_n]$ e demonstramos um conjunto de resultados, conhecidos pela designação de Lema de Nakayama, que são muito úteis em manipulações algébricas com geradores de ideais.

No anel dos inteiros $\mathbb{Z}$, sabemos que os ideais maximais são os ideais gerados por inteiros primos. No anel dos polinómios numa variável sobre um corpo K, os ideais $\langle x - a \rangle$, com $a \in K$, são maximais. Mais geralmente, num d.i.p. os ideais maximais são da forma $\langle p \rangle$ com p primo. O estudo dos ideais maximais de um anel arbitrário A pode ser bastante complicado.

Exemplos 8.4.1.

1. *No anel dos polinómios $K[x, y]$ o ideal $\langle x, y \rangle$ é um ideal maximal, pois, temos $K[x, y]/\langle x, y \rangle = K$. Outro ideal maximal é, por exemplo, $\langle x - 1, y \rangle$.*

2. *No anel das séries de potências $K[[x_1, \ldots, x_n]]$ existe um único ideal maximal, nomeadamente $I_0 = \langle x_1, \ldots, x_n \rangle$.*

Teorema 8.4.2. *Seja K um corpo algebricamente fechado. Os ideais maximais do anel de polinómios $K[x_1, \ldots, x_n]$ são da forma*
$$I_{\boldsymbol{a}} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle,$$
onde $\boldsymbol{a} = (a_1, \ldots, a_n) \in K^n$.

Demonstração. Para cada $\boldsymbol{a} = (a_1, \ldots, a_n) \in K^n$ consideremos o homomorfismo $\phi_{\boldsymbol{a}} : K[x_1, \ldots, x_n] \to K$ que avalia um polinómio em $\boldsymbol{a}$, $\phi_{\boldsymbol{a}} : p(\boldsymbol{x}) \mapsto p(\boldsymbol{a})$. Como $\phi_{\boldsymbol{a}}$ é sobrejectivo e K é um corpo, o seu núcleo $I_{\boldsymbol{a}}$ é um ideal maximal de $K[x_1, \ldots, x_n]$. É fácil de ver que $I_{\boldsymbol{a}} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.

Suponhamos agora que I é um ideal maximal de $K[x_1, \ldots, x_n]$ e seja $\pi : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]/I$ a projecção natural. Designamos por $\pi_1 : K[x_1] \to K[x_1, \ldots, x_n]/I$ a restrição de π a $K[x_1]$. Afirmamos que o núcleo de π_1 é um ideal maximal $\langle x_1 - a_1 \rangle$, logo, I contém um ideal $\langle x_1 - a_1 \rangle$. Da mesma forma, I contém ideais $\langle x_i - a_i \rangle$, para todo o $1 \leq i \leq n$, e concluímos que $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ como desejado.

Para verificar a nossa afirmação primeiro observamos que $N(\pi_1)$ ou é o ideal trivial, ou é um ideal maximal. De facto, se $N(\pi_1) \neq \{0\}$, então existe um polinómio irredutível $q(x_1)$ tal que $N(\pi_1) = \langle q(x_1) \rangle$. Como K é algebricamente fechado, segue-se que $q(x_1) = x_1 - a_1$ e $N(\pi_1)$ é maximal. Logo a afirmação segue-se desde que $N(\pi_1) \neq \{0\}$. Suponha-se, por absurdo, que $N(\pi_1) = \{0\}$. Então π_1 induz um isomorfismo do corpo das fracções $K(x_1)$ para um subcorpo de $K[x_1, \ldots, x_n]/I$. Isto é uma contradição, pois temos

$$[K(x_1) : K] > [K[x_1, \ldots, x_n]/I : K].$$

De facto, por um lado, $[K[x_1, \ldots, x_n] : K]$ é numerável, pois $K[x_1, \ldots, x_n]$ possui uma base contável (os monómios ${x_1}^{i_1} \cdots {x_n}^{i_n}$), logo, $[K[x_1, \ldots, x_n]/I : K]$ é numerável. Por outro lado, as fracções $\frac{1}{x_1 - \alpha}$, com $\alpha \in K$, formam um conjunto linearmente independente de $K(x_1)$ que não é numerável[5]. □

O teorema mostra que os ideais maximais de $K[x_1, \ldots, x_n]$ estão em correspondência biunívoca com os pontos de K^n. Na próxima secção mostramos um resultado análogo em que K^n é substituído por um conjunto algébrico arbitrário.

Vejamos agora alguns resultados que dependem da estrutura de ideais maximais de um anel. Qualquer uma das equivalências fornecidas na seguinte proposição é conhecida pela designação de Lema de Nakayama.

Teorema 8.4.3. *Seja A um anel comutativo com unidade e $I_0 \subset A$ um ideal. As seguintes afirmações são equivalentes:*

(i) I_0 é um ideal contido em todos os ideais maximais de A.

(ii) $1 - a$ é invertível para todo o $a \in I_0$.

(iii) Se M é um A-módulo de tipo finito tal que $M = I_0 M$, então $M = 0$.

[5] Se K é contável, esta demonstração falha. Neste caso é necessário introduzir a noção de *grau de transcendência* que generaliza a noção de grau algébrico e permite mostrar que $K(x_1)$ não é isomorfo a um subcorpo $K[x_1, \ldots, x_n]/I$ (possuem graus de transcendência diferentes). Isto está para além do âmbito deste livro.

(iv) Se N_1 e N_2 são submódulos de um A-módulo M, N_1 é de tipo finito, e $N_1 = N_2 + I_0 N_1$, então $N_1 = N_2$.

Demonstração. Vamos mostrar que (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): Como $I_0 \neq A$, temos que $1-a \notin I_0$ se $a \in I_0$. Se, por absurdo, $1-a$ não é invertível, existe um ideal maximal J que contém o ideal $\langle 1-a \rangle$. Logo, $I_0 \not\subset J$, o que é uma contradição.

(ii) $\Rightarrow$ (iii): Seja $S = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ um conjunto gerador minimal de M. Se $M \neq 0$, então $k \geq 1$. Como $I_0 M = M$, temos

$$\boldsymbol{v}_1 = a_1 \boldsymbol{v}_1 + \cdots + a_k \boldsymbol{v}_k, \qquad a_1, \ldots, a_k \in I_0.$$

Logo:

$$(1 - a_1)\boldsymbol{v}_1 = a_2 \boldsymbol{v}_2 + \cdots + a_k \boldsymbol{v}_k$$

e, como $(1 - a_1)$ é invertível, obtemos

$$\boldsymbol{v}_1 = (1 - a_1)^{-1} a_2 \boldsymbol{v}_2 + \cdots + (1 - a_1)^{-1} a_k \boldsymbol{v}_k.$$

Se $k = 1$, então $\boldsymbol{v}_1 = 0$. Se $k \geq 1$, esta igualdade contradiz a minimalidade de S. Assim, $M = 0$.

(iii) $\Rightarrow$ (iv): O módulo quociente N_1/N_2 é de tipo finito e $I_0 N_1/N_2 = N_1/N_2$. Logo, $N_1/N_2 = 0$ e $N_1 = N_2$.

(iv) $\Rightarrow$ (i): Seja J um ideal maximal. Se $I_0 \not\subset J$, então $A = I_0 A + J$. Logo, $J = A$, o que é uma contradição. □

O seguinte corolário também é por vezes designado por Lema de Nakayama.

Corolário 8.4.4. *Seja A um anel comutativo com unidade, e I_0 um ideal de tipo finito contido em todos os ideais maximais de A. Então, para todo o ideal $J \subset A$, ${I_0}^k \subset J$ se e só se ${I_0}^k \subset J + {I_0}^{k+1}$.*

Demonstração. É óbvio que, se ${I_0}^k \subset J$, então ${I_0}^k \subset J + {I_0}^{k+1}$. Por outro lado, se ${I_0}^k \subset J + {I_0}^{k+1}$, então obtemos

$$\frac{{I_0}^k + J}{J} \subset \frac{{I_0}^{k+1} + J}{J} \subset I_0 \frac{I_0^k + J}{J}.$$

Como $({I_0}^k + J)/J$ é de tipo finito, a parte (iii) do Teorema 8.4.3 mostra que $({I_0}^k + J)/J = 0$. Logo, ${I_0}^k \subset J$. □

Existem anéis com uma estrutura menos rica de ideais maximais do que o anel dos polinómios $K[x_1, \ldots, x_n]$, mas ainda assim muito importantes.

Definição 8.4.5. Um anel A diz-se um ANEL LOCAL se A contém um único ideal maximal I_0.

Exemplos 8.4.6.

1. *O anel das séries de potências $A[[x_1, \ldots, x_n]]$ é um anel local com ideal maximal $I_0 = \langle x_1, \ldots, x_n \rangle$ (exercício).*

2. *Um anel muito importante em Geometria Diferencial é o anel $\mathcal{E}_{m_0}(M)$ dos germes das funções $C^\infty(M)$ num ponto m_0 de uma variedade diferencial M. $\mathcal{E}_{m_0}(M)$ é um anel local com ideal maximal $I_0 = \{f \in \mathcal{E}_{m_0}(M) : f(m_0) = 0\}$. Se $(x^1, \ldots, x^n)$ são coordenadas locais em m_0, então $I_0 = \langle x^1, \ldots, x^n \rangle$.*

Se A é um anel local noetheriano, então o seu ideal maximal I_0 é de tipo finito, logo, satisfaz às condições do Lema de Nakayama na forma do Corolário 8.4.4. Este aplica-se muitas vezes para "eliminar termos de ordem superior", como mostra o exemplo seguinte.

Exemplo 8.4.7.

Consideremos o anel $A = \mathbb{R}[[x, y]]$ das séries de potências em duas variáveis com coeficientes reais. É um anel local com ideal maximal $I_0 = \langle x, y \rangle$ de tipo finito.

Em A, consideramos o ideal

$$J = \langle x^3 - xy, 3x^3 - xy, 3x^2y - y^2 \rangle.$$

Afirmamos que termos de ordem ≥ 3 pertencem a J. De facto, basta observar que

$$\left.\begin{array}{lcl} x^3 & = & -\frac{1}{2}(x^3 - xy) + \frac{1}{2}(3x^3 - xy) \\ x^2y & = & -x(3x^3 - xy) + 3x^4 \\ xy^2 & = & -y(x^3 - xy) + x^3y \\ y^3 & = & -y(3x^2y - y^2) + 3x^2y^2 \end{array}\right\} \in J + {I_0}^4,$$

logo, pelo Corolário 8.4.4, ${I_0}^3 \subset J$. Esta informação permite-nos simplificar consideravelmente os geradores de J. De facto, vê-se facilmente que $J = \langle xy, y^2, x^3 \rangle$. Em particular, uma série de potências $p(x, y) = \sum p_{ij} x^i y^j$ pertence a J se e só se

$$p_{00} = p_{10} = p_{01} = p_{20} = 0.$$

Formalmente, podemos escrever estas condições na forma

$$p(0, 0) = p_x(0, 0) = p_y(0, 0) = p_{xx}(0, 0) = 0,$$

onde os subscritos designam derivadas parciais.

O problema de, dado um ideal, decidir se um elemento pertence ao não a esse ideal levou ao desenvolvimento de algoritmos para encontrar a "melhor" representação para o ideal: as chamadas *bases de Gröbner*. Estas bases são utilizadas, por exemplo, nos modernos manipuladores simbólicos, tais como o MATHEMATICA ou o MAPLE. Discutimos as bases de Gröbner nas últimas duas secções deste capítulo.

Exercícios.

1. Seja D um d.i.p. Mostre que os ideais maximais de D são da forma $\langle p\rangle$, com $p \in D$ primo.

2. Seja J um ideal dum anel A. Mostre que $I \supset J$ é um ideal maximal de A se e só se o ideal $\tilde{I} = I/J$ é um ideal maximal de A/J.

3. Seja D um domínio integral, e $q \in D$ um elemento irredutível. Mostre que $\langle q\rangle$ é maximal na classe de ideais principais de D.

4. Determine os ideais maximais dos anéis:

   (a) $\mathbb{R}[x]/\langle x^2\rangle$;

   (b) $\mathbb{R}[x]/\langle x^2 - 3x + 2\rangle$;

   (c) $\mathbb{R}[x]/\langle x^2 + x + 1\rangle$.

5. No anel $\mathbb{C}[x, y]/\langle y^2 + x^3 - 17\rangle$ diga quais dos seguintes ideais são maximais:

   (a) $\langle \underline{x-1}, \underline{y-4}\rangle$;

   (b) $\langle \underline{x+1}, \underline{y+4}\rangle$;

   (c) $\langle \underline{x^3-17}, \underline{y^2}\rangle$.

6. Verifique quais dos seguintes anéis são corpos:

   (a) $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$;

   (b) $\mathbb{Z}_3[x]/\langle x^3 + x + 1\rangle$;

   (c) $\mathbb{Z}_5[x]/\langle x^2 + x + 1\rangle$.

7. Mostre que, se A é um anel noetheriano local, com ideal maximal I_0, então $\bigcap_{n=k}^{\infty} I_0^n = \{0\}$, para todo o $k \in \mathbb{N}$.

8. Mostre que $K[[x_1, \ldots, x_n]]$ é um anel local.
   (Sugestão: Mostre que, se $p \in I_0 = \langle x_1, \ldots, x_n\rangle$, então a série de potências $1 - p$ é invertível.)

9. Em $\mathbb{R}[[x, y]]$ considere o ideal $J = \langle x^4 + x^2 - y^2, 2x^3 + y^2\rangle$. Mostre que $p(x, y)$ pertence a J se e só se

$$p(0,0) = p_x(0,0) = p_y(0,0) = p_{xy}(0,0) = 0.$$

10. Considere o anel dos polinómios $\mathbb{R}[x, y]$. Decida se as seguintes igualdades são ou não verdadeiras:

    (a) $\langle x^3 - xy, 3x^3 - xy, 3x^2y - y^2\rangle = \langle xy, y^2, x^3\rangle$;

    (b) $\langle x^4 + x^2 - y^2, 2x^3 + y^2\rangle = \langle x^2, y^2\rangle$.

8.5 O Teorema dos Zeros de Hilbert

Nesta secção, K designa um corpo algebricamente fechado. Para estes, como mostrámos na secção anterior, os pontos de K^n estão em correspondência biunívoca com os ideais maximais de $K[x_1, \ldots, x_n]$: a $\boldsymbol{a} = (a_1, \ldots, a_n) \in K^n$ corresponde o ideal $I_{\boldsymbol{a}} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ dos polinómios de $K[x_1, \ldots, x_n]$ que se anulam em $\boldsymbol{a}$. Este resultado generaliza-se a conjuntos algébricos arbitrários, da seguinte forma.

Proposição 8.5.1. *Seja $Y = \mathcal{Z}(I) \subset K^n$ um conjunto algébrico, onde $I \subset K[x_1, \ldots, x_n]$ é um ideal. Os ideais maximais de $A = K[x_1, \ldots, x_n]/I$ estão em correspondência com os pontos de Y: a um ponto $\boldsymbol{a} \in Y$ corresponde o ideal maximal $I_{\boldsymbol{a}}/I \subset A$.*

Demonstração. Se $J \subset A$ é um ideal maximal, então é da forma $\tilde{J}/I$, onde $\tilde{J} \subset K[x_1, \ldots, x_n]$ é um ideal maximal que contém I. Mas, se $\tilde{J} \subset K[x_1, \ldots, x_n]$ é maximal, então é da forma $\tilde{J} = I_{\boldsymbol{a}}$, para um $\boldsymbol{a} \in K^n$. Por outro lado, $I_{\boldsymbol{a}} \supset I$ se e só se $\boldsymbol{a} \in Y$. □

O anel $A = K[x_1, \ldots, x_n]/I$ definido pelo ideal I, contém, pois, toda a informação sobre $Y = \mathcal{Z}(I)$. Este anel desempenha um papel fundamental em Geometria Algébrica, como veremos mais adiante.

Corolário 8.5.2. *Sejam $p_1, \ldots, p_r \in K[x_1, \ldots, x_n]$. O sistema de equações*

$$\begin{cases} p_1(x_1, \ldots, x_n) = 0, \\ \quad \vdots \\ p_r(x_1, \ldots, x_n) = 0. \end{cases}$$

não tem soluções em K^n se e só se existem polinómios $q_1, \ldots, q_r$ tais que

$$q_1 p_1 + \cdots + q_r p_r = 1.$$

Demonstração. Se o sistema não tem soluções, então, pela proposição, o anel $A = K[x_1, \ldots, x_n]/\langle p_1, \ldots, p_r \rangle$ não tem ideais maximais, e portanto é trivial. Logo, $\langle p_1, \ldots, p_r \rangle = K[x_1, \ldots, x_n]$. □

Exemplos 8.5.3.

1. *Seja $A = \mathbb{C}[x, y]$. O sistema de equações algébricas*

$$\begin{cases} p_1(x, y) = x^2 + y^2 - 1 = 0 \\ p_2(x, y) = x^2 - y + 1 = 0 \\ p_3(x, y) = xy - 1 = 0 \end{cases}$$

não tem soluções em $\mathbb{C}^2$. Logo, pelo corolário, $1 \in \langle p_1, p_2, p_3 \rangle$. Não é nada óbvio, a priori, *que existam polinómios $q_1(x, y), q_2(x, y), q_3(x, y)$ tais que*

$$q_1 p_1 + q_2 p_2 + q_3 p_3 = 1.$$

2. Seja $A = \mathbb{R}[x, y]$. O sistema de equações algébricas

$$\begin{cases} p_1(x, y) = x^2 + y^2 + 1 = 0 \\ p_2(x, y) = x^2 - y^2 = 0 \end{cases}$$

não tem soluções em $\mathbb{R}^2$. Mas $1 \notin \langle p_1, p_2 \rangle$ (porquê?). Assim, nos resultados acima é essencial que K seja um corpo algebricamente fechado.

Se $Y \subset K^n$ é um conjunto arbitrário, então definimos o ideal $\mathcal{I}(Y)$ dos polinómios de $K[x_1, \ldots, x_n]$ que se anulam em Y por

$$\mathcal{I}(Y) \equiv \{p \in K[x_1, \ldots, x_n] : p(\boldsymbol{a}) = 0, \forall \boldsymbol{a} \in Y\}.$$

Temos o seguinte resultado fundamental, também conhecido pelo nome alemão de *Nullstenllensatz de Hilbert*:

Teorema 8.5.4 (Teorema dos Zeros de Hilbert). *Seja $Y = \mathcal{Z}(I) \subset K^n$ um conjunto algébrico, onde $I \subset K[x_1, \ldots, x_n]$ é um ideal. Então:*

$$\mathcal{I}(Y) = \mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}.$$

Demonstração. É óbvio que $\sqrt{I} \subset \mathcal{I}(Y)$. Falta, pois, demonstrar a inclusão $\mathcal{I}(Y) \subset \sqrt{I}$.

Seja $I \subset K[x_1, \ldots, x_n]$ um ideal. Pelo Teorema da Base de Hilbert, existem polinómios $p_1, \ldots, p_r \in K[x_1, \ldots, x_n]$ tais que $I = \langle p_1, \ldots, p_r \rangle$. Se $p \in K[x_1, \ldots, x_n]$ é um polinómio não-nulo que se anula em $Y = \mathcal{Z}(I)$ (*i.e.*, se $p \in \mathcal{I}(Y)$), então introduzimos uma indeterminada adicional y, e consideramos o sistema de equações algébricas:

$$\begin{cases} \tilde{p}_1(x_1, \ldots, x_n, y) = p_1(x_1, \ldots, x_n) \\ \qquad \vdots \\ \tilde{p}_r(x_1, \ldots, x_n, y) = p_r(x_1, \ldots, x_n) \\ \tilde{p}(x_1, \ldots, x_n, y) = p(x_1, \ldots, x_n)y - 1. \end{cases}$$

Este sistema de equações algébricas não tem soluções em K^{n+1}: de facto, se $(x_1^0, \ldots, x_n^0, y^0)$ satisfaz as primeiras r equações, então $x_1^0, \ldots, x_n^0 \in Y = \mathcal{Z}(I)$ e, portanto, $\tilde{p}(x_1^0, \ldots, x_n^0, y^0) = p(x_1^0, \ldots, x_n^0)y^0 - 1 = -1 \neq 0$. Pelo Corolário 8.5.2, existem polinómios $q_1, \ldots, q_r, q \in K[x_1, \ldots, x_n, y]$ tais que

$$1 = \sum_{i=1}^{r} q_i(x_1, \ldots, x_n, y)p_i(x_1, \ldots, x_n) + q(x_1, \ldots, x_n, y)(p(x_1, \ldots, x_n)y - 1).$$

Substituindo $y = \frac{1}{p(x_1, \ldots, x_n)}$, obtemos

$$1 = \sum_{i=1}^{r} q_i(x_1, \ldots, x_n, \frac{1}{p(x_1, \ldots, x_n)})p_i(x_1, \ldots, x_n).$$

Multiplicando ambos os lados desta igualdade por uma potência suficientemente elevada de $p(x_1, \ldots, x_n)$, vemos que

$$p(x_1, \ldots, x_n)^N = \sum_i r_i(x_1, \ldots, x_n) p_i(x_1, \ldots, x_n) \in I.$$

Isto mostra que $p(x_1, \ldots, x_n) \in \sqrt{I}$, como pretendido. □

Exemplo 8.5.5.

Os polinómios $p_1(x, y) = x^2$ e $p_2(x, y) = xy$ definem o conjunto algébrico $Y = \{(x, y) \in \mathbb{C}^2 : x = 0\}$. De facto, se $I = \langle x^2, xy \rangle$, então, como vimos no Exemplo 8.3.3, $\sqrt{I} = \langle x \rangle$.

Fechamos este capítulo com alguns comentários sobre a relação entre a Álgebra Comutativa e a Geometria Algébrica.

Definição 8.5.6. Um conjunto algébrico diz-se IRREDUTÍVEL se

$$Y = Y_1 \cup Y_2 \text{ com } Y_i \text{ algébrico} \quad \Longrightarrow \quad Y = Y_1 \text{ ou } Y = Y_2.$$

Chama-se VARIEDADE ALGÉBRICA a um conjunto algébrico irredutível.

Chamaremos a um ideal I IDEAL RADICAL se $I = \sqrt{I}$. Note que um ideal primo é um ideal radical. Temos o seguinte corolário da Nullstenllensatz:

Corolário 8.5.7. *Existe uma correspondência biunívoca entre conjuntos algébricos $Y \subset K^n$ e ideais radicais $I \subset K[x_1, \ldots, x_n]$. Às variedades algébricas correspondem os ideais primos.*

Demonstração. As aplicações $Y \mapsto \mathcal{I}(Y)$ e $I \mapsto \mathcal{Z}(I)$ fornecem a correspondência desejada. Por outro lado, se Y é uma variedade algébrica, mostramos que $\mathcal{I}(Y)$ é um ideal primo. De facto, se $p(x_1, \ldots, x_n)q(x_1, \ldots, x_n) \in \mathcal{I}(Y)$, então $Y \subset \mathcal{Z}(pq) = \mathcal{Z}(p) \cup \mathcal{Z}(q)$, logo

$$Y = (Y \cap \mathcal{Z}(p)) \cup (Y \cap \mathcal{Z}(q)).$$

Como Y é irredutível, vemos que ou $Y = Y \cap \mathcal{Z}(p)$ e $Y \subset \mathcal{Z}(p)$, ou $Y = Y \cap \mathcal{Z}(q)$ e $Y \subset \mathcal{Z}(q)$. Logo, $p(x_1, \ldots, x_n) \in \mathcal{I}(Y)$ ou $q(x_1, \ldots, x_n) \in \mathcal{I}(Y)$. □

Exemplos 8.5.8.

1. *Seja $p(x, y) \in K[x, y]$ um polinómio irredutível. Como $K[x, y]$ é um domínio de factorização única, o ideal $\langle p \rangle$ é primo, e $Y = \mathcal{Z}(p)$ é irredutível. A esta variedade algébrica chama-se* CURVA ALGÉBRICA *determinada pela equação $p(x, y) = 0$. Em geral, se $p \in K[x_1, \ldots, x_n]$ é irredutível, obtemos uma variedade algébrica $\mathcal{Z}(p)$, chamada* HIPERSUPERFÍCIE ALGÉBRICA *determinada pela equação $p(x_1, \ldots, x_n) = 0$.*

2. Seja $I_1 = \langle x^2 + y^2 + z^2 + 2xy, xz + yz \rangle$ *e* $I_2 = \langle x + y, z^3 \rangle$. *Estes ideais determinam a mesma variedade algébrica. De facto,* $\sqrt{I_1} = \sqrt{I_2} = \langle x + y, z \rangle$, *logo:*

$$\mathcal{Z}(I_1) = \mathcal{Z}(I_2) = \{x + y = 0, z = 0\}.$$

Utilizando os resultados da Secção 8.3 sobre decomposições de ideais, obtemos outro corolário da Nullstenllensatz:

Corolário 8.5.9. *Todo o conjunto algébrico pode ser expresso, de forma única, como uma união de variedades algébricas em que nenhuma componente contém outra.*

Demonstração. Seja Y um conjunto algébrico. O ideal $\mathcal{I}(Y)$ admite uma decomposição em ideais primários

$$\mathcal{I}(Y) = Q_1 \cap \cdots \cap Q_r.$$

Logo:

$$Y = \mathcal{Z}(\mathcal{I}(Y)) = Y_1 \cap \cdots \cap Y_r,$$

onde $Y_i = \mathcal{Z}(Q_i)$. A componente Y_i é irredutível, pois o ideal

$$I_i = \mathcal{I}(Y_i) = \mathcal{I}(\mathcal{Z}(Q_i)) = \sqrt{Q_i}$$

é primo. Descartando factores, podemos assumir que $Y_i \not\subset Y_j$, para todos os $1 \leq i, j \leq r$ distintos.

A unicidade desta decomposição segue-se da unicidade da factorização primária, ou então pode ser demonstrada directamente (exercício). □

Se Y é um conjunto algébrico, ao anel

$$\mathcal{A}(Y) \equiv K[x_1, \ldots, x_n]/\mathcal{I}(Y)$$

chama-se ANEL DAS COORDENADAS de Y. Como $Y = \mathcal{Z}(\mathcal{I}(Y))$, sabemos que os pontos do conjunto algébrico Y estão em correspondência biunívoca com os ideais maximais do anel $\mathcal{A}(Y)$. Por outro lado, se $p(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, então $p(x_1, \ldots, x_n)$ induz uma função $\tilde{p} : Y \to K$ por restrição. A uma função deste tipo chama-se FUNÇÃO REGULAR definida em Y. Obviamente, as funções regulares formam um anel para a soma e o produto induzidos de $K[x_1, \ldots, x_n]$.

Proposição 8.5.10. *Existe um isomorfismo entre o anel de coordenadas* $\mathcal{A}(Y)$ *de um conjunto algébrico* Y *e o anel das funções regulares* $\tilde{p} : Y \to K$.

Demonstração. A aplicação $p \mapsto \tilde{p}$ determina um epimorfismo do anel de polinómios $K[x_1, \ldots, x_n]$ no anel das funções regulares definidas em Y. O núcleo deste epimorfismo é precisamente

$$\mathcal{I}(Y) = \{p(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] : p(\boldsymbol{a}) = 0, \forall \boldsymbol{a} \in Y\}.$$

□

Exemplo 8.5.11.

Seja Y a curva algébrica definida pela equação $y = x^2$. Toda a função regular $\tilde{p} : Y \to K$ é restrição de um polinómio $p(x, y) \in K[x, y]$ a Y. Se à função regular $\tilde{p}$ associamos o polinómio $\bar{p} \in K[w]$ definido por:

$$\bar{p}(w) \equiv p(w, w^2),$$

vemos que a aplicação $\tilde{p} \mapsto \bar{p}$ induz um isomorfismo do anel das funções regulares definidas em Y com o anel $K[w]$. Logo, $\mathcal{A}(Y)$ é isomorfo a um anel de polinómios numa variável.

Se Y é uma variedade algébrica, então o anel $\mathcal{A}(Y)$ é de facto um domínio integral e uma K-álgebra de tipo finito (ver exercício). Pode-se mostrar que toda a K-álgebra de tipo finito e que é um domínio integral, é o anel de coordenadas de uma variedade algébrica. Existe, pois, uma correspondência biunívoca entre variedades algébricas e as K-álgebras de tipo finito que são domínios integrais. Esta correspondência estende-se aos morfismos (quando definidos apropriadamente). Desta forma vemos que proposições sobre variedades algébricas são equivalentes a certas proposições de Álgebra Comutativa.

Exercícios.

1. Sejam $Y_1 = \mathcal{Z}(p_1, \ldots, p_r)$ e $Y_2 = \mathcal{Z}(q_1, \ldots, q_s)$ conjuntos algébricos em K^n. Mostre que $Y_1 \cap Y_2 = \emptyset$ se e só se $\langle p_1, \ldots, p_r, q_1, \ldots, q_r \rangle = K[x_1, \ldots, x_n]$.

2. Demonstre a unicidade de decomposição de um conjunto algébrico em variedades algébricas.

3. Se $I_1, \ldots, I_r \subset K[x_1, \ldots, x_n]$ são ideais, mostre que

$$\mathcal{Z}(I_1 \cdots I_r) = \mathcal{Z}(I_1) \cup \cdots \cup \mathcal{Z}(I_r).$$

4. Mostre que $I_1 = \langle x^2 + y^2 + z^2 + 2xy, xz + yz \rangle$ e $I_2 = \langle x + y, z^3 \rangle$ possuem o mesmo radical, nomeadamente

$$\sqrt{I_1} = \sqrt{I_2} = \langle x + y, z \rangle.$$

5. Se $Y_1 = \mathcal{Z}(I_1)$ e $Y_2 = \mathcal{Z}(I_2)$ são conjuntos algébricos mostre que o produto cartesiano $Y_1 \times Y_2$ é um conjunto algébrico. Que ideal corresponde a $Y_1 \times Y_2$?

6. Vimos num exemplo desta secção que, se Y é a curva algébrica $y = x^2$, então $\mathcal{A}(Y)$ é isomorfo a um anel de polinómios de uma variável sobre K. Mostre que:

   (a) Se Z é a curva algébrica $xy = 1$, então $\mathcal{A}(Z)$ não é isomorfo a um anel de polinómios de uma variável sobre K;

(b) Se W é uma curva algébrica $p(x,y)=0$, com $p(x,y)\in K[x,y]$ um polinómio irredutível de grau 2, então $\mathcal{A}(W)$ é isomorfo a $\mathcal{A}(Y)$ ou a $\mathcal{A}(Z)$.

7. Se $Y\subset K^n$ define-se a DIMENSÃO de Y, designada por $\dim Y$, como sendo o supremo dos inteiros n para os quais existe uma cadeia de conjuntos algébricos irredutíveis distintos:
$$Y_0\subsetneq Y_1\subsetneq\cdots\subsetneq Y_n\subset Y.$$
Mostre que:
   (a) Se $Y=\{\boldsymbol{a}\}\subset K^n$, então $\dim Y=0$.
   (b) $\dim K=1$;
   (c) Se $p(x_1,\ldots,x_n)\in K[x_1,\ldots,x_n]$ é irredutível, então $\dim \mathcal{Z}(p)=n-1$.

8. Se A é um anel define-se o COMPRIMENTO DE UM IDEAL PRIMO $P\subset A$ como sendo o supremo do conjunto dos inteiros n para os quais existe uma cadeia de ideais primos distintos:
$$P_0\subsetneq P_1\subsetneq\cdots\subsetneq P_n=P.$$
A DIMENSÃO DO ANEL[6] A, $\dim A$, é por definição o supremo dos comprimentos dos ideais primos de A. Mostre que, se Y é um conjunto algébrico com anel de coordenadas $\mathcal{A}(Y)$, então $\dim Y=\dim \mathcal{A}(Y)$.

9. Se $Y\subset K^n$ é um conjunto algébrico, mostre que:
   (a) $\mathcal{A}(Y)$ é um domínio integral;
   (b) $\mathcal{A}(Y)$ é de tipo finito;
   (c) $\mathcal{A}(Y)$ é uma K-álgebra.

8.6 Divisão de Polinómios

Uma vez fixado um ideal $I\subset K[x_1,\ldots,x_n]$, um problema fundamental é o de decidir se um dado polinómio $p\in K[x_1,\ldots,x_n]$ pertence a I. Pelo Teorema da Base de Hilbert, o ideal é da forma $I=\langle p_1,\ldots,p_s\rangle$, logo, este problema é equivalente ao problema de saber se podemos escrever p como uma combinação linear $u_1p_1+\cdots+u_np_n$, para alguns polinómios $u_1,\ldots,u_n\in K[x_1,\ldots,x_n]$. A resolução deste problema passa naturalmente por um Algoritmo de Divisão para polinómios a mais de uma variável. Introduzimos nesta secção este algoritmo, que é válido em qualquer corpo K.

Antes de considerarmos o caso geral de divisão de polinómios a mais de uma variável, recordemos o Algoritmo de Divisão a *uma só variável* (ver Teorema 3.6.1). Neste caso, esse algoritmo mostra que dados polinómios $p,d\in K[x]$ existem polinómios únicos q e r, com $\deg r<\deg d$, tais que

[6] Por vezes também chamada DIMENSÃO DE KRULL.

$p = qd + r$, . Temos, ainda, que o quociente q e o resto r podem ser calculados por um processo iterativo: Para um polinómio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$ de grau n recordemos que $p^{\text{top}} = a_n x^n$ designa o termo de grau máximo. Para dividir o polinómio p por um polinómio d procede-se então por iteração:

- Começando com $q = 0$ e $r = p$, substituímos em cada passo

$$q \to q + \frac{r^{\text{top}}}{d^{\text{top}}}, \quad r \to r - \frac{r^{\text{top}}}{d^{\text{top}}} d.$$

A iteração termina quando $\deg r < \deg d$.

Existem vários factores que contribuem para o êxito deste algoritmo. Observe-se que trabalhamos os polinómios termo a termo (*i.e.*, um monómio de cada vez), começando com o grau mais elevado e terminando com o grau mais baixo. Dito de outra forma, o conjunto dos termos mónicos

$$T_1 = \{x^n : n = 0, 1, 2, \dots\}$$

pode ser ordenado pelo seu grau: $x^n \leq x^m$ se e só se $n \leq m$. Esta relação de ordem possui as seguintes propriedades:

(a) Se x^n divide x^m, então $x^n \leq x^m$, *i.e.*, $\leq$ respeita a divisibilidade.

(b) $\leq$ é uma relação de ordem total, de forma que podemos comparar quaisquer dois termos.

(c) $\leq$ é uma boa ordenação, o que garante que o algoritmo termina.

Estas propriedades sugerem como proceder no caso geral de n variáveis: Consideramos o conjunto T_n dos termos mónicos a n variáveis, *i.e.*,

$$T_n = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha_1, \dots, \alpha_n \in \mathbb{N}_0\}.$$

Vamos abreviar o elemento $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ por $\boldsymbol{x}^{\boldsymbol{\alpha}}$. No conjunto T_n consideramos a relação de ordem lexicográfica que é definida da seguinte forma:

$$\boldsymbol{x}^{\boldsymbol{\alpha}} < \boldsymbol{x}^{\boldsymbol{\beta}} \text{ se e só se } \begin{cases} \alpha_s < \beta_s, & \text{e} \\ \\ \alpha_{s+1} = \beta_{s+1}, \dots, \alpha_n = \beta_n. \end{cases}$$

Por exemplo, se $n = 2$ temos:

$$1 < x < x^2 < \cdots < y < xy < x^2y < \cdots < y^2 < xy^2 < x^2y^2 < \cdots$$

Para esta relação de ordem em T_n temos as seguintes propriedades fundamentais:

(a) Se $\boldsymbol{x}^{\boldsymbol{\alpha}}$ divide $\boldsymbol{x}^{\boldsymbol{\beta}}$, então $\boldsymbol{x}^{\boldsymbol{\alpha}} \leq \boldsymbol{x}^{\boldsymbol{\beta}}$.

(b) $\leq$ é uma relação de ordem total.

(c) $\leq$ é uma boa ordenação.

As propriedades (a) e (b) são óbvias. Deixamos a demonstração de (c) como exercício. Existem outras relações de ordem em T_n que satisfazem as propriedades (a), (b) e (c) (ver exercícios nesta secção), e é útil, em muitas situações, considerar outras relações de ordem para além da lexicográfica[7]. Deve-se notar que todos os resultados desta secção e da próxima são válidos se substituirmos a relação de ordem lexicográfica por uma relação de ordem que satisfaça estas três propriedades.

Dado um polinómio $p \in K[x_1, \ldots, x_n]$, com $p \neq 0$, podemos escrever este polinómio na forma

$$p = a_1 \boldsymbol{x}^{\boldsymbol{\alpha}_1} + a_2 \boldsymbol{x}^{\boldsymbol{\alpha}_2} + \cdots + a_r \boldsymbol{x}^{\boldsymbol{\alpha}_r},$$

onde $0 \neq a_i \in K$ e os termos mónicos satisfazem $\boldsymbol{x}^{\boldsymbol{\alpha}_1} > \boldsymbol{x}^{\boldsymbol{\alpha}_2} > \cdots > \boldsymbol{x}^{\boldsymbol{\alpha}_r}$. Para um polinómio escrito nesta forma, definimos $p^{\text{top}} = a_1 \boldsymbol{x}^{\boldsymbol{\alpha}_1}$ que vamos designar por TERMO MÁXIMO de p, e definimos $p^{\text{mon}} = \boldsymbol{x}^{\boldsymbol{\alpha}}$ que vamos designar por MONÓMIO MÁXIMO de p.

Definição 8.6.1. Dados polinómios $p, d, h \in K[x_1, \ldots, x_n]$, vamos dizer que *$p$ se reduz a h módulo d num passo*, e escrevemos

$$p \underset{d}{\longrightarrow} h,$$

se d^{top} divide algum termo $a_i \boldsymbol{x}^{\boldsymbol{\alpha}_i}$ do polinómio p, e $h = p - \frac{a_i \boldsymbol{x}^{\boldsymbol{\alpha}_i}}{d^{\text{top}}} d$.

Quando p se reduz a h módulo d num passo, podemos pensar no polinómio h como o resto num passo da divisão de p por d.

Exemplo 8.6.2.

Em $\mathbb{Q}[x, y]$, se tomarmos $p = 3x^2y + 4xy - 3x$ e $d = xy + x$, então $d^{top} = xy$, que divide quer o termo $3x^2y$ quer o termo $4xy$. No primeiro caso, temos que

$$p \underset{d}{\longrightarrow} 4xy - 3x^2 - 3x.$$

No segundo caso, temos que

$$p \underset{d}{\longrightarrow} 3x^2y - 7x.$$

Podemos iterar este processo e remover de p todos os termos que são divisíveis por d^{top}.

[7] De facto, pode-se mostrar que os algoritmos baseados na relação de ordem lexicográfica são lentos e que, em geral, é mais vantajoso recorrer a relações de ordem que sejam o "menos lexicográficas" possível.

Exemplo 8.6.3.

Para os polinómios $p = 3x^2y + 4xy - 3x$ e $d = xy + x$ do exemplo anterior, temos que:

$$p \underset{d}{\to} 4xy - 3x^2 - 3x \underset{d}{\to} -3x^2 - 7x.$$

Note-se que a ordem em que removemos os termos é irrelevante. Também é interessante verificar que esta divisão corresponde à divisão habitual de polinómios. Podemos apresentar esta divisão na forma tradicional:

$$\begin{array}{rrr|l} 3x^2y & +4xy & -3x & xy+x \\ \cline{4-4} -3x^2y & -3x^2 & & 3x+4 \\ \cline{1-3} & 4xy & -3x^2 -3x & \\ & -4xy & -4x & \\ \cline{2-3} & & -3x^2 -7x & \end{array}$$

A divisão que acabámos de expor não é contudo suficiente. Como estamos a lidar com polinómios a várias variáveis, os ideais não são principais e, em geral, necessitamos de dividir por *vários* polinómios. Assim, estendemos a Definição 8.6.1, da seguinte forma:

Definição 8.6.4. Dados polinómios $p, d_1, \ldots, d_s, h \in K[x_1, \ldots, x_n]$, com $d_i \neq 0$, vamos dizer que p *reduz-se a* h *módulo a família* $F = \{d_1, \ldots, d_s\}$, e escrevemos

$$p \underset{F}{\twoheadrightarrow} h,$$

se existir uma sequência de índices $i_1, \ldots, i_r \in \{1, \ldots, s\}$ e uma sequência de polinómios $h_1, \ldots, h_{r-1} \in K[x_1, \ldots, x_n]$, tais que

$$p \underset{d_{i_1}}{\longrightarrow} h_1 \underset{d_{i_2}}{\longrightarrow} h_2 \underset{d_{i_1}}{\longrightarrow} \cdots \underset{d_{i_{r-1}}}{\longrightarrow} h_{r-1} \underset{d_{i_r}}{\longrightarrow} h.$$

Exemplos 8.6.5.

1. *Pelo Exemplo 8.6.3, temos que, se $p = 3x^2y + 4xy - 3x$ e $d = xy + x$, então*

$$p \underset{d}{\twoheadrightarrow} -3x^2 - 7x.$$

2. *Novamente em $\mathbb{Q}[x, y]$, se tomarmos $p = x^2y$, $d_1 = xy - y$ e $d_2 = y - x^2$, vemos que*

$$x^2y \underset{d_1}{\longrightarrow} xy \underset{d_1}{\longrightarrow} y,$$

pois temos:

$$\begin{array}{rr|l} x^2y & & xy-y \\ \cline{3-3} -x^2y & +xy & x+1 \\ \cline{1-2} & xy & \\ & -xy & +y \\ \cline{2-2} & & y \end{array}$$

Por outro lado, vemos que $y \underset{d_2}{\longrightarrow} x^2$, *pois temos:*

$$\begin{array}{r|l} y & y - x^2 \\ \cline{2-2} -y + x^2 & 1 \\ \cline{1-1} x^2 & \end{array}$$

Assim, para a família $F = \{d_1, d_2\}$, *concluímos que* $x^2 y \underset{F}{\twoheadrightarrow} x^2$.

Vamos dizer que $r \in K[x_1, \ldots, x_n]$ é um POLINÓMIO REDUZIDO em relação à família $F = \{d_1, \ldots, d_s\} \subset K[x_1, \ldots, x_n]$, se $r = 0$ ou se nenhum dos termos de r é divisível por ${d_i}^{\text{top}}$. Por outras palavras, um polinómio é reduzido em relação a uma família F, se não pode ser reduzido (mod F). Temos então:

Teorema 8.6.6 (Algoritmo de Divisão a n variáveis). *Dado um polinómio* $p \in K[x_1, \ldots, x_n]$ *e uma família* $F = \{d_1, \ldots, d_s\} \subset K[x_1, \ldots, x_n]$, *existem polinómios* $u_1, \ldots, u_s, r \in K[x_1, \ldots, x_n]$ *tais que:*

$$p = u_1 d_1 + \cdots + u_s d_s + r,$$

onde r *é reduzido* (mod F).

Vamos chamar ao polinómio r o RESTO da divisão de p pela família F, e aos polinómios $u_1, \ldots, u_s$ os QUOCIENTES da divisão de p por F.

Demonstração do Teorema 8.6.6. Se ${d_i}^{\text{top}}$ não divide nenhum dos termos de p, para $i = 1, \ldots, s$, então basta tomar $r = p$ e $u_1 = \cdots = u_s = 0$. Caso contrário, tal como no caso de uma variável, procedemos por iteração.

Começando com $u_1^{(0)} = u_2^{(0)} = \cdots = u_s^{(0)} = 0$, tomamos $h_0 = p$. Suponhamos que conhecíamos $u_i^{(k)}$ e h_k. Definimos $u_i^{(k+1)}$ e h_{k+1} da seguinte forma:

- Escolhemos o menor dos índices $i \in \{1, \ldots, s\}$ tais que ${d_i}^{\text{top}} | {h_k}^{\text{top}}$.
- Substituímos $u_i^{(k)}$ por $u_i^{(k+1)} = u_i^{(k)} + \frac{{h_k}^{\text{top}}}{{d_i}^{\text{top}}}$, e tomamos $u_j^{(k+1)} = u_j^{(k)}$, se $j \neq i$.
- Substituímos h_k por $h_{k+1} = h_k - \frac{{h_k}^{\text{top}}}{{d_i}^{\text{top}}} d_i$.

Observe que cada iteração corresponde, pois, a reduzir h_k a h_{k+1} (mod d_i), para algum i, num passo:

$$h_k \underset{d_i}{\longrightarrow} h_{k+1}.$$

Note-se ainda que ${h_k}^{\text{mon}} > {h_{k+1}}^{\text{mon}}$. Como T_n é bem ordenado, concluímos que a iteração termina: existe k_0 tal que ${d_i}^{\text{top}} \nmid {h_{k_0+1}}^{\text{top}}$, para $i = 1, \ldots, s$. Basta, pois, tomarmos $r = h_{k_0+1}$. □

Na notação introduzida acima, o Algoritmo de Divisão afirma que para qualquer polinómio p e família $F = \{d_1, \ldots, d_s\}$ em $K[x_1, \ldots, x_n]$, podemos sempre obter $p \underset{F}{\twoheadrightarrow} r$, onde r é um polinómio reduzido (mod F).

Observe-se que na demonstração do Algoritmo de Divisão assumimos de facto que o conjunto $\{d_1, \ldots, d_s\}$ é ordenado. Esta ordenação afecta o resultado da divisão, como mostra o seguinte exemplo.

Exemplo 8.6.7.

Tal como no Exemplo 8.6.5.2, seja $d_1 = xy - y$ e $d_2 = y - x^2$. Se tomarmos $p = xy^2 - x^2y$, recorrendo ao Algoritmo de Divisão, vemos que (verifique):

$$p \underset{d_1}{\twoheadrightarrow} y^2 - x^2y \underset{d_2}{\twoheadrightarrow} 0.$$

Por outro lado, se trocarmos a ordem dos divisores, obtemos:

$$p \underset{d_2}{\twoheadrightarrow} x^5 - x^4,$$

e o polinómio $x^5 - x^4$ não pode ser reduzido (mod d_1). *Assim, vemos que o Algoritmo de Divisão aplicado a $\{d_1, d_2\}$ e a $\{d_2, d_1\}$ fornece resultados bem diferentes.*

O problema da falta de unicidade do resto da divisão será resolvido na próxima secção, onde introduziremos as bases de Gröbner.

Exercícios.

1. Mostre que o conjunto T_n com a relação de ordem lexicográfica é bem ordenado.

2. Seja $<$ uma relação de ordem no conjunto dos termos mónicos T_n com as seguinte propriedades:

   - $1 < \boldsymbol{x}^{\boldsymbol{\alpha}}$ para todo o $\boldsymbol{x}^{\boldsymbol{\alpha}} \neq 1$;
   - se $\boldsymbol{x}^{\boldsymbol{\alpha}} < \boldsymbol{x}^{\boldsymbol{\beta}}$ então $\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{x}^{\boldsymbol{\gamma}} < \boldsymbol{x}^{\boldsymbol{\beta}}\boldsymbol{x}^{\boldsymbol{\gamma}}$, para todo o $\boldsymbol{x}^{\boldsymbol{\gamma}} \in T_n$.

   Mostre que:

   (a) se $\boldsymbol{x}^{\boldsymbol{\alpha}}$ divide $\boldsymbol{x}^{\boldsymbol{\alpha}}$, então $\boldsymbol{x}^{\boldsymbol{\alpha}} \leq \boldsymbol{x}^{\boldsymbol{\beta}}$;
   (b) $\leq$ é uma relação de ordem total;
   (c) $\leq$ é uma boa ordenação.

3. Defina uma relação de ordem em T_n por:

$$\boldsymbol{x}^{\boldsymbol{\alpha}} < \boldsymbol{x}^{\boldsymbol{\beta}} \text{ se e só se } \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i, \\ \text{ou} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ e } \boldsymbol{x}^{\boldsymbol{\alpha}} < \boldsymbol{x}^{\boldsymbol{\beta}} \\ \text{na relação de ordem lexicográfica.} \end{cases}$$

   Mostre que esta relação de ordem está nas condições do exercício anterior. Dê ainda outros exemplos de relações de ordem que satisfazem as mesmas condições.

4. Use o Algoritmo de Divisão para calcular as seguintes divisões[8]:

   (a) Em $\mathbb{Q}[x,y]$, dividir $p = x^3y^3 + 2x^2$ por $d_1 = 2x^2y + 3y + 4x^2$ e $d_2 = x^2 - 2x - 2$.

   (b) Como em (a), mas com d_1 e d_2 com a ordem trocada.

   (c) Em $\mathbb{Q}[x,y,z,w]$, dividir $p = z^2w^2 - x^2$ por $d_1 = w - xz^2$, $d_2 = z - yx$, $d_3 = y - x^3$ e $d_4(x,y,z,w) = x^3 - x$.

   (d) Como em (c), mas pela ordem d_4, d_3, d_2, d_1.

5. Mostre que, se o resultado da divisão de um polinómio p por $d_1, \ldots, d_s$ é $p = u_1d_1 + \cdots + u_sd_s + r$, então é válida a seguinte fórmula para os termos mónicos:

$$p^{\text{mon}} = \max(\max_{1\leq i\leq s}({u_i}^{\text{mon}}{d_i}^{\text{mon}}), r^{\text{mon}}). \tag{8.6.1}$$

6. Seja $F \subset K[x_1, \ldots, x_n]$ uma família de polinómios. Mostre que não existe uma cadeia infinita

$$h_1 \underset{F}{\longrightarrow} h_2 \underset{F}{\longrightarrow} \ldots \underset{F}{\longrightarrow} h_i \underset{F}{\longrightarrow} \ldots$$

   (Sugestão: Observe que, em cada redução $h_i \underset{F}{\longrightarrow} h_{i+1}$, podemos não estar a subtrair um termo de topo, como acontece no Algoritmo de Divisão.)

8.7 Bases de Gröbner

Seja $I \subset K[x_1, \ldots, x_n]$ um ideal que podemos assumir como sendo da forma $\langle d_1, \ldots, d_s\rangle$. Dado um polinómio $p \in K[x_1, \ldots, x_n]$, gostaríamos de ter uma forma eficiente de testar se $p \in I$. Da mesma forma gostaríamos de, dado um ideal J, decidir se $J = I$.

Para decidir se $p \in I$, podemos dividir p por $d_1, \ldots, d_s$, utilizando o Algoritmo de Divisão. Se o resto da divisão for o polinómio nulo, então é claro que $p \in I$. No entanto, como vimos no Exemplo 8.6.7, pode acontecer que o resto da divisão seja não-nulo, e ainda assim $p \in I$.

De facto, este mesmo problema já surgia com polinómios a uma só variável: por exemplo, o polinómio $p = x^2 + x \in \mathbb{Q}[x]$ pertence ao ideal $I = \langle x^3 + x, x^3 - x\rangle$, mas é reduzido em relação à família $\{x^3 + x, x^3 - x\}$. Neste caso, resolvíamos o problema encontrando um conjunto gerador mais adequado, nomeadamente $x = \text{mdc}(x^3+x, x^3-x)$. Temos então que $I = \langle x\rangle$ e que $p \in I$ se e só se $x|p$. No caso de polinómios a várias variáveis, vamos adoptar um procedimento idêntico.

[8] Estes exercícios, como aliás todos os cálculos envolvendo o Algoritmo de Divisão, podem ser efectuados de forma eficaz com o auxílio de um manipulador simbólico tal como o Mathematica, o Maple ou o CoCoa. Encorajamos o leitor a utilizá-los!

Definição 8.7.1. Seja $I \subset K[x_1, \ldots, x_n]$ um ideal. Uma família de polinómios não-nulos $\{g_1, \ldots, g_s\} \subset I$ diz-se uma BASE DE GRÖBNER DO IDEAL[9] I se satisfaz a seguinte propriedade:

$$p \in I \text{ se e só se } p \underset{G}{\twoheadrightarrow} 0.$$

Mais geralmente, uma família de polinómios não-nulos $G = \{g_1, \ldots, g_s\}$ diz-se uma BASE DE GRÖBNER se for uma base de Gröbner do ideal $\langle G \rangle$.

Desta definição, é óbvio que uma base de Gröbner de um ideal I é sempre um conjunto gerador de I. Por outro lado, não é de todo óbvio que um ideal possua uma base de Gröbner. Veremos que isso de facto é verdade como consequência da proposição seguinte, que fornece caracterizações alternativas das bases de Gröbner:

Proposição 8.7.2. *Seja $I \subset K[x_1, \ldots, x_n]$ um ideal não-trivial, e seja $G = \{g_1, \ldots, g_s\} \subset I$ uma família de polinómios não-nulos. As seguintes afirmações são equivalentes:*

(i) G é uma base de Gröbner de I.

(ii) $p \in I$ se e só se $p = \sum_{i=1}^{s} u_i g_i$, com $p^{mon} = \max_{1 \leq i \leq s}({u_i}^{mon} {g_i}^{mon})$.

(iii) Para todo o $p \in I$ não-nulo, existe um $i \in \{1, \ldots, s\}$ tal que ${g_i}^{top} | p^{top}$.

(iv) $\langle {g_1}^{top}, \ldots, {g_s}^{top} \rangle = \langle p^{top} : p \in I \rangle$.

Demonstração. Vamos mostrar que (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$(iv) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): Segue-se imediatamente do Algoritmo de Divisão e do Exercício 5 da secção anterior.

(ii) $\Rightarrow$ (iii): Se $p \in I$, então pode ser escrita como em (ii), logo,

$$p^{\text{top}} = \sum_j {u_j}^{\text{top}} {g_j}^{\text{top}},$$

onde a soma é sobre os índices j tais que $p^{\text{mon}} = {u_j}^{\text{mon}} {g_j}^{\text{mon}}$. Expandido o lado direito, vemos imediatamente que existe um j tal que ${g_j}^{\text{top}} | p^{\text{top}}$.

(iii) $\Rightarrow$ (iv): Óbvio.

(iv) $\Rightarrow$ (i): Pelo Algoritmo de Divisão, para qualquer polinómio p temos que

$$p \underset{G}{\twoheadrightarrow} r,$$

[9] Wolfgang Gröbner (1899-1980), matemático austríaco que trabalhou, entre outros domínios, em Geometria Algébrica. Como frequentemente acontece em Matemática, ao contrário do que o nome indica, estas bases não foram descobertas por Gröbner, mas sim por Bruno Buchberger, matemático contemporâneo que foi aluno de Gröbner na Universidade de Innsbruck.

onde r é reduzido em relação a G. Se $r = 0$, é óbvio que $p \in I$. Por outro lado, se $p \in I$, então $r \in I$ e, por (iv), existem polinómios $h_1, \ldots, h_s$ tais que

$$r^{\text{top}} = \sum_{i=1}^{s} h_i {g_i}^{\text{top}}.$$

Vemos, pois, que existe $i \in \{1, \ldots, s\}$ tal que ${g_i}^{\text{top}} | r^{\text{top}}$. Como r é reduzido (mod G), concluímos que, necessariamente, $r = 0$. □

Corolário 8.7.3. *Todo o ideal $I \subset K[x_1, \ldots, x_n]$ possui uma base de Gröbner.*

Demonstração. Precisamos do seguinte lema cuja demonstração deixamos como exercício.

Lema 8.7.4. *Seja $I \subset K[x_1, \ldots, x_n]$ um ideal gerado por um conjunto S de monómios. Existe um subconjunto finito $S_0 \subset S$ que ainda gera I.*

Assim, dado um ideal $I \subset K[x_1, \ldots, x_n]$, o lema mostra que o ideal $\langle p^{\text{top}} : p \in I \rangle$ possui um conjunto gerador $G = \{{g_1}^{\text{top}}, \ldots {g_s}^{\text{top}}\}$, onde $g_i \in I$. Temos, pois, que G satisfaz a condição (iv) da Proposição 8.7.2, logo, é uma base de Gröbner de I. □

Nenhuma das caracterizações alternativas dadas na Proposição 8.7.2 fornece uma forma prática de verificar que um conjunto gerador é uma base de Gröbner. Veremos como proceder mais adiante. De qualquer forma, podemos utilizar estas caracterizações para mostrar que um conjunto *não* é uma base de Gröbner, como ilustramos no exemplo seguinte.

Exemplo 8.7.5.

Seja $d_1 = xy - y$ e $d_2 = y - x^2$. Se $F = \{d_1, d_2\}$, vimos no Exemplo 8.6.7 que o polinómio $p = xy^2 - x^2y = yd_1 + yd_2$ satisfaz:

$$p \underset{F}{\twoheadrightarrow} x^5 - x^4.$$

Assim, $q = x^5 - x^4 \in \langle d_1, d_2 \rangle$. Por outro lado, $x^5 = q^{top}$ não é divisível nem por $xy = {d_1}^{top}$ nem por $y = {d_2}^{top}$, logo, pela Proposição 8.7.2 (iii), F não é uma base de Gröbner.

Já observámos que o resto da divisão de um polinómio por uma família F não é, em geral, único pois depende da ordenação dos polinómios de F. No entanto, para as bases de Gröbner temos:

Teorema 8.7.6. *Uma família $G = \{g_1, \ldots, g_s\} \subset K[x_1, \ldots, x_n]$ de polinómios não-nulos é uma base de Gröbner se e só se para todo o polinómio p o resto da divisão por G é único.*

Demonstração. Suponha-se, primeiro, que G é uma base de Gröbner. Se $p \in K[x_1, \ldots, x_n]$ é tal que $p \underset{G}{\twoheadrightarrow} r_1$ e $p \underset{G}{\twoheadrightarrow} r_2$, com r_1 e r_2 reduzidos, então $r_1 - r_2$ é reduzido (mod G). Como $r_1 - r_2 \in \langle G \rangle$ (pois quer $p - r_1$ quer $p - r_2$ pertencem a este ideal), pela definição de base de Gröbner, concluímos que $r_1 - r_2 = 0$.

Para provar o recíproco, necessitamos do seguinte lema cuja demonstração deixamos como exercício.

Lema 8.7.7. *Seja $g \in K[x_1, \ldots, x_n]$ tal que $g \underset{G}{\twoheadrightarrow} r$, com r reduzido* (mod G). *Se $c \in K$ e $X \in T^n$, então $(g - cXg_i) \underset{G}{\twoheadrightarrow} r$, para $i \in \{1, \ldots, s\}$.*

Assim, supondo que o resto da divisão por G é único, seja $p \in \langle G \rangle$, e suponha-se que $p \underset{G}{\twoheadrightarrow} r$, com r reduzido. Queremos mostrar que $r = 0$. É fácil de ver que podemos escrever

$$p = \sum_{l=1}^{r} c_l X_l g_{l_j},$$

onde $c_l \in K$, $X_l \in T^n$ e $l_j \in \{1, \ldots, s\}$. Aplicando o lema, vemos que

$$p - c_1 X_1 g_{l_1} \underset{G}{\twoheadrightarrow} r.$$

Por indução segue-se imediatamente que também

$$0 = p - \sum_{l=1}^{r} c_l X_l g_{l_j} \underset{G}{\twoheadrightarrow} r.$$

Assim, concluímos que $r = 0$. □

Deve notar-se, ainda, que, embora o resto da divisão por uma base de Gröbner G seja único, os quocientes que resultam da divisão não são necessariamente únicos.

Os resultados acima mostram que qualquer ideal possui bases de Gröbner. A sua utilidade seria bastante reduzida se não tivéssemos nenhuma forma eficiente de as construir. Vejamos então que de facto podemos construir bases de Gröbner para um dado ideal $I \subset K[x_1, \ldots, x_n]$.

A chave para o método de construção é a caracterização de bases de Gröbner dada pela condição (ii) da Proposição 8.7.2. Esta condição mostra que, se I é um ideal gerado por um conjunto finito $F = \{d_1, \ldots, d_s\}$, então F pode não ser uma base de Gröbner, porque pode existir algum polinómio $p \in I$ para o qual p^{top} não é divisível por ${d_i}^{\text{top}}$, para $i = 1, \ldots, s$. Por outro lado, como $p \in I$, existem polinómios $h_1, \ldots, h_s$ tais que

$$p = \sum_{i=1}^{s} h_i d_i.$$

Assim, o problema está em que os maiores dos termos mónicos dos factores $h_i d_i$, dados por $(h_i d_i)^{\text{mon}} = {h_i}^{\text{mon}} {d_i}^{\text{mon}}$, podem cancelar-se. No caso mais simples, teremos o cancelamento dos maiores dos termos mónicos de apenas dois polinómios, d_i e d_j. O polinómio que resulta deste cancelamento é dado pela seguinte definição:

Definição 8.7.8. Para quaisquer dois polinómios $p, q \in K[x_1, \ldots, x_n]$ chama-se S-POLINÓMIO[10] ao polinómio

$$S(p,q) = \frac{m}{p^{\text{top}}} p - \frac{m}{q^{\text{top}}} q,$$

onde $m = \text{mmc}(p^{\text{mon}}, q^{\text{mon}})$.

O polinómio S pode ser calculado facilmente, como mostra o exemplo seguinte.

Exemplo 8.7.9.

Em $\mathbb{Q}[x,y]$, se $p = -2xy^2 - y$ e $q = 3y^3 - 2xy$, temos que

$$\text{mmc}(p^{mon}, q^{mon}) = \text{mmc}(xy^2, y^3) = xy^3.$$

Assim:

$$\begin{aligned} S(p,q) &= -\frac{xy^3}{2xy^2} p - \frac{xy^3}{3y^3} q \\ &= -\frac{1}{2} yp - \frac{1}{3} xq = \frac{1}{2} y^2 + \frac{2}{3} x^2 y. \end{aligned}$$

Observe que em $S(p,q)$ cancelámos o termo mónico xy^3.

Os S-polinómios também servem para medir a falta de unicidade no Algoritmo de Divisão. Assuma-se que na divisão de $p \in K[x_1, \ldots, x_n]$ por $\{d_1, \ldots, d_i\}$ existe um termo $X = a\boldsymbol{x}^{\boldsymbol{\alpha}}$ de p que é divisível simultaneamente por um ${d_i}^{\text{top}}$ e por um ${d_j}^{\text{top}}$ $(i \neq j)$. Por um lado, temos que $p \underset{d_i}{\longrightarrow} h_i$, onde

$$h_i = p - \frac{X}{{d_i}^{\text{top}}} d_i.$$

Por outro lado, temos que $p \underset{d_j}{\longrightarrow} h_j$, onde

$$h_j = p - \frac{X}{{d_j}^{\text{top}}} d_j.$$

[10] Não podemos justificar neste livro o uso da letra S para qualificar estes polinómios. Diremos apenas que está relacionado com a noção de *syzygy*: Dado um ideal $I = \langle d_1, \ldots, d_s \rangle \subset A[x_1, \ldots, x_n]$ a aplicação $\phi : A^s \to I$ definida por $(a_1, \ldots, a_s) \mapsto \sum_i a_i d_i$ é um homomorfismo de A-módulos e chama-se SYZYGY a um elemento do núcleo.

A diferença (ambiguidade) introduzida no Algoritmo de Divisão é, pois, dada por

$$h_i - h_j = \frac{X}{{d_j}^{\text{top}}} d_j - \frac{X}{{d_i}^{\text{top}}} d_i = \frac{X}{m} S(d_j, d_i),$$

onde $m = \text{mmc}({d_i}^{\text{mon}}, {d_j}^{\text{mon}})$. De facto, temos o seguinte resultado:

Teorema 8.7.10 (Buchberger I). *Seja $G = \{g_1, \ldots, g_s\}$ um conjunto de polinómios não-nulos. Então G é uma base de Gröbner se e só se para todo o $i \neq j$ temos*

$$S(g_i, g_j) \underset{G}{\twoheadrightarrow} 0.$$

Demonstração. Se $G = \{g_1, \ldots, g_s\}$ é uma base de Gröbner, então é claro que $S(g_i, g_j) \in \langle G \rangle$, logo, $S(g_i, g_j) \underset{G}{\twoheadrightarrow} 0$.

Para provar o recíproco, precisamos do seguinte lema cuja demonstração é deixada como exercício:

Lema 8.7.11. *Seja p um polinómio que é combinação linear de polinómios $d_1 \ldots, d_s \in K[x_1, \ldots, x_n]$, com coeficientes em K,*

$$p = \sum_i c_i d_i, \qquad (c_i \in K).$$

Se ${d_1}^{mon} = \cdots = {d_s}^{mon} \equiv X \neq 0$ e $p^{mon} < X$, então

$$p = \sum_{i<j} a_{ij} S(d_i, d_j),$$

para alguns $a_{ij} \in K$, com $1 \leq i < j \leq s$.

Seja então $G = \{g_1, \ldots, g_s\}$ tais que $S(g_i, g_j) \underset{G}{\twoheadrightarrow} 0$, se $i \neq j$. Vamos mostrar que G é uma base de Gröbner do ideal $I = \langle G \rangle$, recorrendo à condição (ii) da Proposição 8.7.2. Fixado $p \in I$, entre as várias possibilidades de escrever p como combinação linear

$$p = \sum_{i=1}^{r} h_i g_i, \qquad (h_i \in K[x_1, \ldots, x_n]), \tag{8.7.1}$$

escolhemos aquela para a qual o termo mónico

$$X = \max_{1 \leq i \leq r} ({h_i}^{\text{mon}} {g_i}^{\text{mon}})$$

é mínimo. Isto é possível, pois o conjunto dos termos mónicos T^n é bem ordenado. Basta, pois, mostrar que $X = p^{\text{mon}}$. Supomos, por absurdo, que $p^{\text{mon}} < X$, e vamos ver que existe uma combinação linear do tipo (8.7.1) com X mais pequeno, o que é uma contradição.

Seja $A = \{i : {h_i}^{\text{mon}} {g_i}^{\text{mon}} = X\}$, e defina-se um polinómio g por

$$g = \sum_{i \in A} {h_i}^{\text{top}} g_i = \sum_{i \in A} c_i X_i g_i, \qquad (X_i = {h_i}^{\text{mon}}).$$

Temos então que $(X_i g_i)^{\text{mon}} = X$ se $i \in A$ e $g^{\text{mon}} < X$, logo, pelo lema, podemos escrever

$$g = \sum_{\substack{i<j \\ i,j \in A}} a_{ij} S(X_i g_i, X_j g_j), \tag{8.7.2}$$

para alguns $a_{ij} \in K$. Um cálculo simples mostra que

$$S(X_i g_i, X_j g_j) = \frac{X}{X_{ij}} S(g_i, g_j),$$

onde $X_{ij} = \text{mmc}({g_i}^{\text{mon}}, {g_i}^{\text{mon}})$. Como, por hipótese, $S(g_i, g_j) \underset{G}{\twoheadrightarrow} 0$, concluímos também que $S(X_i g_i, X_j g_j) \underset{G}{\twoheadrightarrow} 0$. Do Algoritmo de Divisão, segue então que

$$S(X_i g_i, X_j g_j) = \sum_{k \in A} \bar{h}_{ijk} g_k, \tag{8.7.3}$$

para certos polinómios $\bar{h}_{ijk}$ que satisfazem (ver Exercício 5 da secção anterior):

$$\begin{aligned} \max_{1 \le k \le s} ({h_{ijk}}^{\text{mon}} {g_k}^{\text{mon}}) &= S(X_i g_i, X_j g_j)^{\text{mon}} \\ &< \max((X_i g_i)^{\text{mon}}, (X_j g_j)^{\text{mon}}) = X. \end{aligned}$$

Assim, se substituirmos a expressão (8.7.3) de $S(X_i g_i, X_j g_j)$ na expressão (8.7.2) para g, e se substituirmos a expressão resultante na expressão (8.7.1) para p, obtemos uma nova combinação linear do tipo (8.7.1) com X mais pequeno, tal como pretendíamos. □

O Teorema de Buchberger fornece um método para calcular bases de Gröbner de um ideal $I = \langle d_1, \ldots, d_s \rangle$, por iteração. Procedemos da seguinte forma:

- Calculamos todos os S-polinómios $S(d_i, d_j)$.
- Reduzimos os S-polinómios por G.
- Adicionamos a G os resultados da redução que não são nulos, e recomeçamos a iteração.

Deixamos como exercício verificar que o Teorema da Base de Hilbert garante que este algoritmo termina.

Exemplo 8.7.12.

Vimos no Exemplo 8.7.5 que os polinómios $d_1 = xy - y$ *e* $d_2 = y - x^2$ *não formam um base de Gröbner. Para calcular uma base de Gröbner para o ideal* $I = \langle d_1, d_2 \rangle$*, procedemos da seguinte forma: Primeiro, calculamos o S-polinómio:*

$$S(d_1, d_2) = -y + x^3.$$

O resto da divisão de $S(d_1, d_2)$ *por* $F = \{d_1, d_2\}$ *é*

$$-y + x^3 \underset{F}{\twoheadrightarrow} x^3 - x^2.$$

Este polinómio é não-nulo, o que mostra, como já sabíamos, que F não é uma base de Gröbner. Assim, adicionamos a F o polinómio $d_3 = x^3 - x^2$*, obtendo um novo conjunto gerador* $G = \{d_1, d_2, d_3\}$*.*

Há que calcular novamente os S-polinómios dos elementos de G e reduzi-los (mod G)*. Obtemos:*

$$\begin{aligned} S(d_1, d_2) &= -y + x^3 \underset{G}{\twoheadrightarrow} 0, \\ S(d_1, d_3) &= 0, \\ S(d_2, d_3) &= x^2 y - x^5 \underset{G}{\twoheadrightarrow} 0. \end{aligned}$$

Assim, vemos que G é uma base de Gröbner, e o algoritmo termina.

Se G é uma base de Gröbner de um ideal I, então é óbvio que se acrescentarmos a G elementos não-nulos de I obtemos uma nova base de Gröbner. Isto mostra que existe uma grande arbitrariedade na escolha de bases de Gröbner. Para eliminar esta falta de unicidade introduzimos:

Definição 8.7.13. Um conjunto $G = \{g_1, \ldots, g_s\} \subset K[x_1, \ldots, x_n]$ diz-se uma BASE DE GRÖBNER REDUZIDA se G é uma base de Gröbner em que os termos ${g_i}^{\text{top}}$ são mónicos e reduzidos (mod $(G - \{g_i\})$) para $i = 1, \ldots, s$.

Temos então o seguinte resultado importante:

Teorema 8.7.14 (Buchberger II). *Todo o ideal* $I \subset K[x_1, \ldots, x_n]$ *possui uma única base de Gröbner reduzida.*

Demonstração. Vamos chamar a uma base de Gröbner $G = \{g_1, \ldots, g_s\}$ MÍNIMA, se ${g_i}^{\text{top}}$ são mónicos, e para $i \neq j$ temos ${g_i}^{\text{top}} \nmid {g_j}^{\text{top}}$.

Para obter uma base de Gröbner mínima a partir de uma base de Gröbner $G = \{g_1, \ldots, g_s\}$ dada, procedemos por eliminação: eliminamos todos os g_i para os quais existem um j tal que ${g_j}^{\text{top}} | {g_i}^{\text{top}}$, e dividimos os restantes por um elemento de K, de forma que ${g_j}^{\text{top}}$ sejam mónicos. O conjunto G' resultante ainda é uma base de Gröbner: é óbvio que, se p é um polinómio com f^{top} divisível por ${g_i}^{\text{top}}$, para algum $g_i \in G$, então p é divisível por ${g_j}^{\text{top}}$, para algum $g_j \in G'$.

Uma vez obtida uma base de Gröbner mínima $G = \{g_1, \ldots, g_t\}$, para obter uma base de Gröbner reduzida $H = \{h_1, \ldots, h_t\}$ procedemos por iteração:

- $g_1 \underset{H_1}{\twoheadrightarrow} h_1$, onde h_1 é reduzido em relação a $H_1 = \{g_2, \ldots, g_t\}$;
- $g_2 \underset{H_2}{\twoheadrightarrow} h_2$, onde h_2 é reduzido em relação a $H_2 = \{h_1, g_3 \ldots, g_t\}$;
- $g_3 \underset{H_3}{\twoheadrightarrow} h_3$, onde h_3 é reduzido em relação a $H_3 = \{h_1, h_2, g_4 \ldots, g_y\}$;

$\vdots$

- $g_t \underset{H_t}{\twoheadrightarrow} h_t$, onde h_t é reduzido em relação a $H_t = \{h_1, \ldots, h_{t-1}\}$.

É claro que $H = \{h_1, \ldots, h_t\}$ é uma base de Gröbner reduzida. Para verificar a unicidade, precisamos do seguinte lema cuja demonstração remetemos para os exercícios.

Lema 8.7.15. *Se $G = \{g_1, \ldots, g_s\}$ e $H = \{h_1, \ldots, h_t\}$ são bases de Gröbner mínimas, então $s = t$ e ${g_i}^{mon} = {h_i}^{mon}$, para $i = 1, \ldots, t$, eventualmente depois de uma renumeração.*

É óbvio que uma base de Gröbner reduzida é mínima. Assim, se $G = \{g_1, \ldots, g_s\}$ e $H = \{h_1, \ldots, h_t\}$ são bases de Gröbner reduzidas, o lema mostra que $s = t$, e podemos assumir que ${g_i}^{\text{mon}} = {h_i}^{\text{mon}}$, para $i = 1, \ldots, t$. Seja $1 \leq i \leq t$ tal que $g_i \neq h_i$. Como $g_i - h_i \in I$, existe um $j \neq i$ tal que ${g_j}^{\text{mon}} | (g_i - h_i)^{\text{mon}}$. Mas então vemos que ${g_j}^{\text{mon}} = {h_j}^{\text{mon}}$ divide um termo de g_i ou de h_i. Isto contradiz a hipótese de que G e H eram ambas bases de Gröbner reduzidas. □

Voltemos agora aos problemas colocados no início desta secção. Para um ideal $I = \langle d_1, \ldots, d_s \rangle \subset K[x_1, \ldots, x_n]$ gostávamos de:

- Decidir se um polinómio $p \in K[x_1, \ldots, x_n]$ pertence a I, e em caso afirmativo determinar polinómios $h_1, \ldots, h_s$ tais que $p = \sum_i h_i d_i$.
- Dado um ideal $J \subset K[x_1, \ldots, x_n]$ determinar se $J = I$.

Utilizando as bases de Gröbner, é agora muito fácil responder a ambas as questões. Para resolver o primeiro problema, construímos uma base de Gröbner $G = \{g_1, \ldots, g_r\}$ para I e sabemos que

$$p \in I \quad \Longleftrightarrow \quad p \underset{G}{\twoheadrightarrow} 0.$$

Por outro lado, se $p \in I$, então podemos calcular os polinómios coeficientes $h_1, \ldots, h_s$ através do Algoritmo de Divisão. Finalmente, dado outro ideal $J \subset K[x_1, \ldots, x_n]$, para determinar se $J = I$ basta verificar se as suas bases de Gröbner reduzidas coincidem. Como temos um algoritmo de cálculo de bases de Gröbner, todas estas questões podem ser resolvidas de forma eficiente.

As bases de Gröbner são extremamente úteis para resolver muitos outros problemas práticos em Álgebra Comutativa ou em áreas que recorram à Álgebra Comutativa[11]. O desenvolvimento dos manipuladores simbólicos em anos recentes levou à implementação em computador de algoritmos eficientes para resolver muitos desses problemas.

Retornemos, a título de exemplo, ao estudo das variedades algébricas. Seja $I \subset K[x_1, \ldots, x_n]$ um ideal que define a variedade algébrica

$$Y = \mathcal{Z}(I) = \{(a_1, \ldots, a_n) \in K^n : p(a_1, \ldots, a_n) = 0, \forall p \in I\}.$$

Para o anel de coordenadas $\mathcal{A}(Y) = K[x_1, \ldots, x_n]/I$ gostaríamos naturalmente de saber:

(i) Determinar representantes de cada elemento de $\mathcal{A}(Y)$.

(ii) Realizar as operações no anel $\mathcal{A}(Y)$ em termos desses representantes.

(iii) Determinar se um elemento $f \in \mathcal{A}(Y)$ é invertível e, em caso afirmativo, calcular o inverso.

Todos estes problemas podem ser resolvidos de forma efectiva com recurso às bases de Gröbner. Por exemplo, para resolver o problema (i), escolhemos uma base de Gröbner G para I, e para cada $p \in K[x_1, \ldots, x_n]$ designamos por p_G o resto da divisão de p por G. Dados dois polinómios $p, q \in K[x_1, \ldots, x_n]$ temos que $p_G = q_G$ se e só se $p - q \in I$ (exercício). Assim, os elementos p_G são representantes dos elementos de $\mathcal{A}(Y)$, tal como era pretendido. As soluções de (ii) e (iii) são discutidas nos exercícios.

O leitor encontrará muitas outras aplicações das bases de Gröbner nas referências que fornecemos como *Sugestões de Leitura Adicional* no final deste livro.

Exercícios.

1. Seja $G = \{g_1, \ldots, g_s\} \subset K[x]$ um conjunto de polinómios não-nulos, e seja $d = \text{mdc}(g_1, \ldots, g_s)$. Mostre que G é uma base de Gröbner se e só se $cd \in G$, para algum $c \in K$ não-nulo.

2. Generalize o exercício anterior a ideais principais $I \subset K[x_1, \ldots, x_n]$.

3. Sejam $p_1, \ldots, p_s \in K[x_1, \ldots, x_n]$ *polinómios lineares*:

$$p_i = a_{i1}x_1 + \cdots + a_{in}x_n, \qquad (i = 1, \ldots, s).$$

Designe por $B = (b_{ij})$ a matriz em escada de linhas obtida a partir da matriz $A = (a_{ij})$ por eliminação de Gauss. Mostre que os polinómios lineares

$$g_i = b_{i1}x_1 + \cdots + b_{in}x_n, \qquad (i = 1, \ldots, r),$$

[11] Embora tenhamos apenas considerado o caso de polinómios sobre um corpo K, pode-se também desenvolver uma teoria de bases de Gröbner para coeficientes num anel comutativo A, com boas propriedades (por exemplo, num d.f.u.).

onde $r \leq s$ é o número de linhas de B não-nulas, formam uma base de Gröbner do ideal $I = \langle p_1, \ldots, p_s \rangle$.

4. Seja $I \subset K[x_1, \ldots, x_n]$ um ideal gerado por um conjunto S de monómios. Mostre que:

   (a) $p \in I$ se e só se todo o termo $a_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$ de p é divisível por um monómio de S;

   (b) existe um subconjunto finito S_0 de S tal que $I = \langle S_0 \rangle$.

5. Dada uma família $G = \{g_1, \ldots, g_s\} \subset K[x_1, \ldots, x_n]$ de polinómios não-nulos assuma que para todo o polinómio $p \in K[x_1, \ldots, x_n]$ o resto da divisão por G é único. Mostre que, se $g \in K[x_1, \ldots, x_n]$ é tal que $g \underset{G}{\twoheadrightarrow} r$, com r reduzido (mod G), então $(g - cXg_i) \underset{G}{\twoheadrightarrow} r$, para todo o $c \in K$, $X \in T^n$ e $i \in \{1, \ldots, s\}$.

6. Demonstre o Lema 8.7.11.

7. Verifique, recorrendo ao Teorema da Base de Hilbert, que o algoritmo para calcular bases de Gröbner com base no Teorema de Buchberger termina.

8. Determine uma base de Gröbner para os seguintes ideais:

   (a) $I = \langle x^2y - y + x, xy^2 - x \rangle \subset \mathbb{Q}[x, y]$;

   (b) $I = \langle 3x^2yz - xy^3, xy^2 + z^2 \rangle \subset \mathbb{Q}[x, y, z]$;

   (c) $I = \langle x - y^2w, y - zw, z - w^3, w^3 - w \rangle \subset \mathbb{Q}[x, y, z, w]$;

9. Se $G = \{g_1, \ldots, g_s\}$ e $H = \{h_1, \ldots, h_t\}$ são bases de Gröbner mínimas, mostre que $s = t$ e que ${g_i}^{\text{mon}} = {h_i}^{\text{mon}}$ para $i = 1, \ldots, t$ (eventualmente depois de uma renumeração).

10. Determine bases de Gröbner reduzidas para cada um dos ideais dados no Exercício 8.

11. Seja G uma base de Gröbner para um ideal I. Para cada $p \in K[x_1, \ldots, x_n]$ designe por p_G o resto da divisão de p por G. Seja ainda $Y = \mathcal{Z}(I)$ a variedade algébrica associada a I, e $\mathcal{A}(Y)$ o seu anel de coordenadas. Mostre que:

   (a) Se $p, q \in K[x_1, \ldots, x_n]$, então $p_G = q_G$ se e só se $p - q \in I$.

   (b) As operações de $\mathcal{A}(Y)$ são dados por $p_G q_G = (pq)_G$ e $p_G + q_G = (p+q)_G$.

   (c) Uma base para $\mathcal{A}(Y)$, como espaço vectorial sobre K, é dada por

   $$\{p^G : p \in T^n,\ g^{\text{top}} \nmid p \text{ para todo o } g \in G\}.$$

   (d) Um elemento $p + I \in \mathcal{A}(Y)$ tem inverso se e só se $1 \in \langle I, p \rangle$, *i.e.*, se e só se a base de Gröbner reduzida de $\langle I, p \rangle$ é $H = \{1\}$.

12. Em geral, é bastante díficil calcular o radical de um ideal $I \subset K[x_1, \ldots, x_n]$. No entanto, é fácil testar se um polinómio p pertence ou não a $\sqrt{I}$, recorrendo às bases de Gröbner. De facto, mostre que, se $I = \langle d_1, \ldots, d_s \rangle$, então $p \in \sqrt{I}$ se e só se $1 \in \langle d_1, \ldots, d_s, 1 - yp \rangle \subset K[x_1, \ldots, x_n, y]$. Assim, vemos que $p \in \sqrt{I}$ se e só se a base de Gröbner reduzida de $\langle d_1, \ldots, d_s, 1 - yp \rangle \subset K[x_1, \ldots, x_n, y]$ é $\{1\}$.

Apêndice A

Complementos sobre a Teoria dos Conjuntos

A noção de conjunto é a mais importante de todas as noções matemáticas e constitui, por assim dizer, a primeira pedra do grande edifício que é a Matemática. O leitor estará certamente familiarizado com a ideia informal de conjunto e de elemento de um conjunto, bem como com algumas das construções elementares que estes suportam (uniões, intersecções, complementos, etc.). Por outro lado, afirmações tais como:

- dois conjuntos são iguais se e só se possuem os mesmos elementos,
- dados dois conjuntos, existe um conjunto que os contém,
- dado um conjunto, existe um conjunto formado por todos os seus subconjuntos,

são normalmente aceites como óbvias. No entanto, para as justificar plenamente, seria necessário proceder a uma investigação mais profunda sobre os fundamentos da Teoria dos Conjuntos, o que está para além do âmbito deste livro. Por exemplo, o famoso paradoxo de Russell, sobre a existência do conjunto de todos os conjuntos, só pode ser resolvido pela via da axiomatização da Teoria dos Conjuntos. Para um estudo mais pormenorizado destas questões, remetemos o leitor para o livro que Paul Halmos escreveu a este respeito[1].

Neste apêndice, limitamo-nos, pois, a fornecer alguns resultados e noções complementares da Teoria dos Conjuntos e que são essenciais para o estudo da Álgebra.

[1] P. R. Halmos, *Naive Set Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, 1974.

A.1 Relações e Funções

As noções de *relação binária* e de *função* estão directamente relacionadas com a de *par ordenado*. Por isso, o seu tratamento formal exige a definição prévia de par ordenado, que passamos a apresentar. De um ponto de vista prático, a propriedade fundamental dos pares ordenados é a equivalência

$$(x_1, y_1) = (x_2, y_2) \iff x_1 = x_2 \text{ e } y_1 = y_2. \tag{A.1.1}$$

Os requisitos básicos para a definição de par ordenado são consequentemente os de ser expressa em termos de noções ainda mais básicas da Teoria dos Conjuntos, e conduzirem à equivalência precedente. Estes requisitos são satisfeitos pela:

Definição A.1.1. Se X e Y são conjuntos, $x \in X$ e $y \in Y$, o PAR ORDENADO (x, y) é o conjunto $(x, y) = \{x, \{x, y\}\}$. Os elementos x e y são as COMPONENTES do par (x, y). Ao conjunto de todos os pares ordenados (x, y), onde $x \in X$ e $y \in Y$, chama-se PRODUTO CARTESIANO de X e Y, e designa-se por $X \times Y$.

A equivalência (A.1.1) é uma consequência lógica directa da Definição A.1.1, e em particular que (x, y) só é igual a (y, x) quando $x = y$. Com base na noção de par ordenado, podemos introduzir outra noção muito importante que nos permitirá, por exemplo, formalizar a noção de função:

Definição A.1.2. Uma RELAÇÃO entre X e Y é um conjunto R de pares ordenados (x, y), com $x \in X$ e $y \in Y$. Escrevemos frequentemente "xRy" em lugar de "$x, y \in R$", e se $X = Y$, dizemos que R é uma RELAÇÃO BINÁRIA em X.

É imediato verificar que qualquer relação R entre X e Y tem associada uma outra relação entre Y e X, obtida "trocando" as componentes de cada par ordenado em R.

Definição A.1.3. Se R é uma relação entre X e Y, a RELAÇÃO INVERSA OU OPOSTA de R designa-se por R^{op}, e define-se por $R^{\text{op}} = \{(y, x) : (x, y) \in R\}$.

Existem vários tipos importantes de relações, e é indispensável conhecer as definições formais para as *relações de ordem*, as *relações de equivalência*, e as *funções*. Consideramos primeiro o caso das relações de ordem.

Definição A.1.4. Seja R uma relação no conjunto X. Dizemos que R é uma relação de ORDEM em X se verifica:

(i) *Transitividade*: Para quaisquer $x, y, z \in X$, se xRy e yRz, então xRz.

(ii) *Anti-simetria*: Para quaisquer $x, y \in X$, se xRy e yRx, então $x = y$.

Existem também vários tipos de relações de ordem, distinguidas pelos qualificativos *estrita/lata* e *total/parcial*. As diferenças entre estes casos são as seguintes:

Definição A.1.5. Seja R uma relação de ordem em X.

(i) A relação de ordem R diz-se TOTAL (oposto de PARCIAL) se possui a propriedade de *tricotomia*: Para quaisquer $x, y \in X$, temos xRy ou yRx ou $x = y$.

(ii) A relação de ordem R diz-se ESTRITA (oposto de LATA) se possui a propriedade de *anti-reflexividade*: Para quaisquer $x, y \in X$, xRy, então $x \neq y$.

Os exemplos seguintes ilustram as várias possibilidades.

Exemplos A.1.6.

1. *A relação "$>$" (maior) entre números reais é uma relação de ordem estrita e total.*

2. *A relação "$\geq$" (maior ou igual) entre números reais é uma relação de ordem lata e total.*

3. *A relação "$\supseteq$" (contém) entre subconjuntos de um conjunto dado é lata e parcial.*

4. *A relação "$\supsetneq$" (contém estritamente) é estrita e parcial.*

Dado um conjunto parcialmente ordenado X, com relação de ordem designada por "$\leq$", qualquer subconjunto $Y \subset X$ fica parcialmente ordenado com a relação de ordem induzida em Y (que ainda designamos por "$\leq$"). É claro que a relação de ordem em Y pode possuir propriedades que a relação de ordem em X não possui. Por exemplo, pode acontecer que $Y \subset X$, para a relação de ordem induzida, seja totalmente ordenado sem X o ser. Neste caso dizemos que Y é uma CADEIA em X.

Exemplo A.1.7.

Em $\mathbb{R}^2$ considere-se a relação de ordem parcial definida por:

$$(x_1, y_1) \leq (x_2, y_2) \text{ se, e só se, } y_1 = y_2 \text{ e } x_1 \leq x_2,$$

*onde a última desigualdade se refere à relação de ordem usual de números reais. Neste caso, qualquer subconjunto $\{(x, y) \in \mathbb{R}^2 : y = c\}$, para $c \in \mathbb{R}$ fixo (*i.e.*, uma recta horizontal), é uma cadeia. Note, ainda, que $\mathbb{R}^2$, com esta relação de ordem, não é um conjunto totalmente ordenado.*

Vejamos agora uma outra classe de relações binárias muito importante, as relações de equivalência:

Definição A.1.8. Seja R uma relação binária no conjunto X. Dizemos que R é uma RELAÇÃO DE EQUIVALÊNCIA em X se satisfaz:

(i) *Reflexividade*: Para qualquer $x \in X$, xRx.

(ii) *Simetria*: Para quaisquer $x, y \in X$, se xRy, então yRx.

(iii) *Transitividade*: Para quaisquer $x, y, z \in A$, se xRy e yRz, então xRz.

Vejamos alguns exemplos simples de relações de equivalência.

Exemplos A.1.9.

1. *A relação de paralelismo entre rectas do plano é de equivalência.*
2. *A relação de igualdade num qualquer conjunto é de equivalência.*
3. *A relação de congruência módulo m no conjunto dos inteiros é de equivalência.*

Ao contrário das relações de ordem, uma relação de equivalência num conjunto X não induz, em geral, uma relação de equivalência num subconjunto $Y \subset X$. Por outro lado, qualquer relação de equivalência R num conjunto X determina automaticamente uma classe importante de subconjuntos de X.

Definição A.1.10. Se $x \in X$, a CLASSE DE EQUIVALÊNCIA de x, designada $\underline{x}$ ou $[x]$, é o conjunto

$$\underline{x} = [x] = \{y \in X : xRy\}.$$

O conjunto de todas as classes de equivalência $\underline{x}$ diz-se QUOCIENTE de X por R, e designa-se X/R, *i.e.*,

$$X/R = \{\underline{x} : x \in X\} = \{\{y \in X : xRy\} : x \in X\}.$$

Exemplos A.1.11.

1. *Se considerarmos a relação de paralelismo entre rectas no plano, a classe de equivalência de uma recta L é formada por todas as rectas paralelas a L.*
2. *Se R é a relação de igualdade no conjunto X o conjunto quociente é $X/R = \{\{x\} : x \in X\}$.*
3. *Se R é a relação de congruência módulo m no conjunto dos inteiros $\mathbb{Z}$ e $a \in \mathbb{Z}$, então $\underline{a} = \{a + km : k \in \mathbb{Z}\}$.*

É um exercício simples mostrar que duas classes de equivalência ou coincidem ou são distintas.

Proposição A.1.12. *Se R é uma relação de equivalência em X, então, para quaisquer $x, y \in X$, as seguintes afirmações são equivalentes:*

(i) xRy;

(ii) $\underline{x} = \underline{y}$;

(iii) $\underline{x} \cap \underline{y} \neq \emptyset$.

A última classe de relações que consideramos é a das funções.

Definição A.1.13. Uma relação f entre X e Y é uma FUNÇÃO de X em Y, e escrevemos $f : X \to Y$, se:

(i) para qualquer $x \in X$ existe $y \in Y$ tal que xfy, e

(ii) se xfy e xfy', então $y = y'$.

Devido a (ii), escrevemos $y = f(x)$ em lugar de xfy. Dizemos então que X é o DOMÍNIO e Y o CONTRADOMÍNIO da função f.

Outras designações frequentes para um função são as de APLICAÇÃO ou TRANSFORMAÇÃO.

Exemplos A.1.14.

1. *Se X é um conjunto, $I_X : X \to X$, dada por $I_X(x) = x$, é a* FUNÇÃO IDENTIDADE *em X.*

2. *Se $X \supset Y$ são conjuntos, $i_Y : Y \to X$, dada por $i_Y(y) = y$, é a* FUNÇÃO INCLUSÃO *de Y em X.*

3. *Se R é uma relação de equivalência em X, $\pi_{X/R} : X \to X/R$, dada por $\pi_{X/R}(x) = \underline{x}$, é a* APLICAÇÃO QUOCIENTE *de X em X/R.*

Em geral, se $X \supset X'$ e $Y \supset Y'$, dada uma função $f : X \to Y$, definimos

$$f(X') \equiv \{f(x) : x \in X'\}, \quad \text{e} \quad f^{-1}(Y') \equiv \{x \in X : f(x) \in Y'\}.$$

Dizemos então que $f(X')$ é a IMAGEM DIRECTA de X' por f, e $f^{-1}(Y')$ é a IMAGEM INVERSA de Y', também por f. Em particular, a IMAGEM de f é o conjunto $f(X)$, que se designa também por $\operatorname{Im} f$.

Exemplo A.1.15.

Se $f : \mathbb{R} \to \mathbb{R}$ é a função $\cos x$, temos então que a sua imagem é $f(\mathbb{R}) = [-1, +1]$. A imagem inversa do conjunto $\{0\}$ é $f^{-1}(\{0\}) = \{\frac{2n+1}{2}\pi : n \in \mathbb{Z}\}$.

Como bem sabemos, certos tipos de funções merecem qualificativos especiais:

Definição A.1.16. Seja $f : X \to Y$ uma função. Então:

(i) se para qualquer $y \in Y$ existe $x \in X$ tal que $y = f(x)$, f diz-se SOBREJECTIVA;

(ii) se $f(x) = f(x') \Leftrightarrow x = x'$, f diz-se INJECTIVA.

(iii) f diz-se BIJECTIVA, ou uma BIJECÇÃO, se e só se é injectiva e sobrejectiva. Neste caso, dizemos que os conjuntos são EQUIPOTENTES ou ISOMORFOS.

Exemplos A.1.17.

1. *A identidade $I_X : X \to X$ é bijectiva.*
2. *A inclusão $i_Y : Y \to X$ é injectiva.*
3. *A projecção $p_{X/R} : X \to X/R$ é sobrejectiva.*
4. *A função $\cos : \mathbb{R} \to \mathbb{R}$ nem é injectiva nem é sobrejectiva.*

Dadas funções $f : X \to Y$ e $g : Y \to Z$, a COMPOSIÇÃO de f e g é a função $g \circ f : X \to Z$, lida "g após f", dada por $(g \circ f)(x) = g(f(x))$. Deixamos como exercício a verificação da

Proposição A.1.18. *Sejam X, Y, Z, e W conjuntos. Então:*

(i) ***Associatividade**: Se $f : X \to Y$, $g : Y \to Z$ e $h : Z \to W$ são funções, $(h \circ g) \circ f = h \circ (g \circ f)$;*

(ii) ***Inversa à esquerda**: $f : X \to Y$ é injectiva se e só se existe $g : Y \to X$ tal que $g \circ f = I_X$;*

(iii) ***Inversa à direita**: $f : X \to Y$ é sobrejectiva se existe $g : Y \to X$ tal que $f \circ g = I_Y$;*

(iv) ***Inversa**: $f : X \to Y$ é bijectiva se e só se existe $g : Y \to X$ tal que $f \circ g = I_Y$ e $g \circ f = I_X$. Neste caso, g diz-se a* INVERSA *de f e designa-se por f^{-1}.*

Exercícios.

1. Use a Definição (A.1.1) para provar a equivalência (A.1.1).

2. Exprima as propriedades de anti-simetria e tricotomia de uma relação R em termos de R e da sua inversa R^{op}.

3. Demonstre a Proposição (A.1.12).

4. Prove que, se $f : X \to Y$ é uma função e $\{Y_i\}_{i\in I}$ é uma família de subconjuntos de Y, então são válidas as identidades

$$f^{-1}(\bigcup_{i\in I} Y_i) = \bigcup_{i\in I} f^{-1}(Y_i), \quad \text{e} \quad f^{-1}(\bigcap_{i\in I} Y_i) = \bigcap_{i\in I} f^{-1}(Y_i).$$

   Será que estas identidades ainda são válidas se se supusermos que $\{X_i\}_{i\in I}$ é uma família de subconjuntos de X e substituirmos f^{-1} por f?

5. Seja $f : X \to Y$ uma função.

   (a) Pode existir mais do que uma função $g : Y \to X$ tal que $f \circ g = I_Y$?

   (b) Pode existir mais do que uma função $g : Y \to X$ tal que $g \circ f = I_X$?

   (c) Pode existir mais do que uma função $g : Y \to A$ tal que $f \circ g = I_Y$ e $g \circ f = I_X$?

6. Prove os itens (i) e (ii) da Proposição A.1.18[2].

7. Mostre que a inversa f^{-1} da função $f : X \to Y$ é:

   (a) uma função $f^{-1} : f(X) \to X$ se e só se f é injectiva;

   (b) uma função $f^{-1} : Y \to X$ se e só se f é bijectiva.

8. Verifique que, se $f : X \to Y$ é uma função bijectiva, então $g = f^{-1}$ é a única função tal que $f \circ g = I_Y$ e $g \circ f = I_X$.

9. Prove que, se $X \neq \emptyset$ e $Y = \emptyset$, não existem funções $f : X \to Y$.

10. Se $X = \emptyset$ e $f : X \to Y$, então f é injectiva, e além disso f é sobrejectiva se e só se $Y = \emptyset$.

A.2 Axioma da Escolha, Lema de Zorn e Indução

Fizemos já várias referências ao *produto cartesiano* de conjuntos. Utilizando a noção de função, podemos fazer uma análise um pouco mais cuidada sobre este conceito, em particular para desde já introduzir produtos cartesianos com um número arbitrário de factores.

O conjunto dos inteiros tem aqui um papel importante. Se n é um inteiro não-negativo, designamos nesta secção por $I_n = \{k \in \mathbb{N} : k \leq n\}$ o conjunto dos primeiros n naturais. Em particular, $I_0 = \emptyset$.

Sendo X um conjunto, e $f : I_2 \to X$ uma função, é claro que f determina unicamente um par ordenado com componentes em X (especificamente, o

[2] As demonstrações dos itens (iii) e (iv) requerem o *Axioma da Escolha* de que falaremos mais adiante.

par $(f(1), f(2))$, que também podemos escrever (f_1, f_2). Por outras palavras, o conjunto das funções $f : I_2 \to X$ é isomorfo ao conjunto dos pares ordenados com componentes em X.

Uma observação análoga é válida se considerarmos a classe das funções $f : I_2 \to X \cup Y$ tais que $f(1) \in X$ e $f(2) \in Y$. A conclusão continua a ser que o conjunto das funções $f : I_2 \to X \cup Y$ tais que $f(1) \in X$ e $f(2) \in Y$ é isomorfo ao conjunto dos pares ordenados (x, y), com $x \in X$ e $y \in Y$. Este conjunto é obviamente o produto cartesiano de X e Y, que designamos por $X \times Y$. É-nos mais conveniente aqui definir mais geralmente produtos cartesianos directamente como conjuntos de funções.

Definição A.2.1. Sendo $X_1, X_2, \ldots, X_n$ conjuntos, o seu PRODUTO CARTESIANO, designado por $\prod_{i=1}^{n} X_i$, é o conjunto das funções $f : I_n \to X$, tais que $f(k) \in X_k$. Se $f \in \prod_{i=1}^{n} X_i$ escrevemos $f = (f(1), f(2), \ldots, f(n))$, ou $f = (f_1, f_2, \ldots, f_n)$.

Se os conjuntos X_i são todos iguais a X, escrevemos X^n (a "potência" n de X) em vez de $\prod_{i=1}^{n} X$. Neste caso, os elementos de X^n dizem-se n-TUPLOS de elementos de X.

A técnica usada na Definição A.2.1 para definir produtos cartesianos com um número finito de factores pode agora ser directamente aproveitada para introduzir produtos cartesianos com um número infinito de factores. Neste caso, substituímos a família de conjuntos $X_1, X_2, \ldots, X_n$, indexada pelo parâmetro natural n, por uma família $\{X_i : i \in I\}$, indexada pelo parâmetro i pertencente a um conjunto arbitrário I([3]).

Definição A.2.2. Dada a família $\{X_i : i \in I\}$, o PRODUTO CARTESIANO $\prod_{i \in I} X_i$ é dado por

$$\prod_{i \in I} X_i = \{f : I \to \bigcup_{i \in I} X_i, \text{ com } f(i) \in X_i \text{ para qualquer } i \in I\}.$$

A projecção canónica $\pi_k : \prod_{i \in I} X_i \to X_k$ é a aplicação que a um elemento $f \in \prod_{i \in I} X_i$ associa $f(k) \in X_k$.[4]

Exemplos A.2.3.

1. *Para qualquer conjunto X, $\prod_{n \in \mathbb{N}} X$ é o conjunto das sucessões com valores em X.*

2. *$\prod_{n \in \mathbb{N}} I_n$ é o conjunto das sucessões naturais $f : \mathbb{N} \to \mathbb{N}$ que satisfazem $f(n) \leq n$, para qualquer $n \in \mathbb{N}$.*

[3] Recorde-se que, dada uma classe de conjuntos X, uma *família indexada por $i \in I$* não passa de uma função $f : I \to X$, onde escrevemos X_i em lugar de $f(i)$, tal como frequentemente escrevemos, por exemplo, x_n em lugar de $f(n)$ quando falamos de uma sucessão de números reais.

[4] Por vezes escrevemos f_k, em lugar de $f(k)$, sobretudo quando X é um conjunto finito.

3. $\prod_{x\in\mathbb{R}}[x-1,x+1]$ *é o conjunto das funções reais* $f:\mathbb{R}\to\mathbb{R}$ *tais que* $x-1\leq f(x)\leq x+1$.

Nas discussões precedentes usámos frequentemente classes de funções com domínio X e contradomínio Y fixos, em particular para definir produtos cartesianos. É tradicional usar o símbolo "Y^X" para representar estas classes de funções. Assim,

Definição A.2.4. $Y^X=\{f:X\to Y\}$ é o conjunto de *todas* as funções de X em Y.

Exemplos A.2.5.

1. $X^{\mathbb{N}}$ *designa o conjunto das funções* $f:\mathbb{N}\to X$, i.e., *o conjunto das sucessões em* X.
2. $\mathbb{R}^{\mathbb{R}}$ *designa o conjunto de todas as funções reais de variável real.*
3. $\mathbb{R}^{\mathbb{R}\times\mathbb{R}}$ *designa o conjunto de todas as funções reais de duas variáveis reais.*
4. *Em geral,* $X^{X\times X}$ *é o conjunto das operações binárias em* X.
5. *O conjunto* X^n *também pode designar-se por* X^{I_n}.

O produto cartesiano $\prod_{i\in I}X_i$ é em geral um subconjunto *estrito* de $\left(\bigcup_{i\in I}X_i\right)^I$, porque naturalmente nem todas as funções $f:I\to\bigcup_{i\in I}X_i$ verificam a condição adicional $f(i)\in X_i$, para qualquer $i\in I$. No entanto, se $X_i=X$ para qualquer $i\in I$, é claro que

$$\prod_{i\in I}X_i=\prod_{i\in I}X=X^I.$$

Por outras palavras, o conjunto X^I é realmente um tipo especial de produto cartesiano (um produto em que todos os "factores" são iguais), e é isso que justifica a respectiva notação "exponencial".

É facilmente demonstrável (por indução) que $\prod_{i=1}^n X_i$ é não-vazio para qualquer natural n, desde que os conjuntos X_i sejam não-vazios. A mesma afirmação feita a propósito dum produto cartesiano com um conjunto de índices arbitrário é um axioma da Teoria dos Conjuntos:

Axioma I (Axioma da Escolha). *Se* $I\neq\emptyset$ *e* $X_i\neq\emptyset$, *para qualquer* $i\in I$, *então* $\prod_{i\in I}X_i\neq\emptyset$.

A razão para o nome deste axioma é fácil de compreender. Sendo f um elemento do produto cartesiano referido, f representa a "escolha" de um elemento em cada um dos conjuntos X_i. O axioma afirma, pois, que, dada uma família arbitrária de conjuntos, existe sempre uma função que "escolhe" exactamente um elemento de cada conjunto.

O exemplo seguinte ilustra o tipo de dificuldade que o Axioma da Escolha permite ultrapassar.

Exemplo A.2.6.

Suponhamos que cada X_i é formado por um par de sapatos. Então podemos decidir escolher, por exemplo, o sapato direito de cada par. Neste caso o axioma da escolha é inútil. Por outro lado, se cada X_i é formado por um par de meias, então não temos critério de escolha, e necessitamos de recorrer ao Axioma da Escolha para podermos afirmar a existência de um conjunto com exactamente uma meia de cada par.

Muitos resultados de existência de um dado conjunto, ou elemento de um conjunto, satisfazendo esta e aquela propriedade, podem ser reformulados em termos de existência de um elemento maximal para uma relação de ordem apropriada[5]. Neste contexto, o seguinte resultado desempenha muitas vezes um papel crucial:

Teorema A.2.7 (Lema de Zorn). *Seja X um conjunto não-vazio parcialmente ordenado em que toda a cadeia possui um majorante. Então X contém um elemento maximal.*

Pode-se mostrar que o Lema de Zorn é equivalente ao Axioma da Escolha (ver o livro de P. Halmos citado no início deste apêndice). No exemplo seguinte fornecemos uma aplicação típica do Lema de Zorn.

Exemplo A.2.8.

Seja A um anel, $I \subsetneq A$ um ideal, e designemos por X o conjunto dos ideais próprios de A que contêm I (é não-vazio!). Em X consideramos a relação de inclusão, que é evidentemente uma relação de ordem parcial. Se $\{I_j : j \in J\}$ é uma cadeia em X, então possui o majorante $\bigcup_{j\in J} I_j$ (verifique que este conjunto é de facto um ideal de A que contém I e portanto pertence a X). Concluímos do Lema de Zorn que em X existe um elemento maximal. Por outras palavras, num anel, todo o ideal próprio está contido num ideal maximal.

Em relação a este exemplo poder-se-ia pensar que uma outra via de demonstração seria a seguinte: se I é um ideal de A e não é maximal, então existe um ideal I_0 que o contém. Agora, ou I_0 é maximal ou então existe um ideal I_1 que o contém, e assim sucessivamente. O problema é que este "e assim sucessivamente" pode não terminar. O Lema de Zorn serve precisamente para evitar este tipo de problema.

Pela mesma ordem de razões, num conjunto X parcialmente ordenado pode não existir um elemento mínimo, e mesmo se existir elemento mínimo, nada nos garante que um subconjunto $Y \subset X$ possua elemento mínimo. A definição seguinte pretende eliminar estas possibilidades.

[5]As noções de majorante/minorante, supremo/ínfimo e máximo/mínimo para subconjuntos de conjuntos parcialmente ordenados é discutida na Secção 2.2.

Definição A.2.9. Um conjunto X parcialmente ordenado diz-se BEM ORDENADO se todo o subconjunto $S \subset X$ não-vazio possui um elemento mínimo.

Obviamente, a relação de ordem dum conjunto bem ordenado X é total([6]): se $x, y \in X$, então o conjunto $\{x, y\}$ possui um elemento mínimo, logo ou $x \leq y$ ou $y \leq x$.

Exemplos A.2.10.

1. *O conjunto $\mathbb{N}$, com a relação de ordem usual, é um conjunto bem ordenado.*
2. *O conjunto $\mathbb{Z}$, com a relação de ordem usual, não é um conjunto bem ordenado, pois, por exemplo, o subconjunto $\{n \in \mathbb{Z} : n \leq 0\}$ não tem um elemento mínimo.*

Um outro resultado equivalente ao Axioma da Escolha e, por conseguinte, ao Lema de Zorn é o seguinte:

Teorema A.2.11 (Princípio de Boa Ordenação). *Todo o conjunto pode ser bem ordenado.*

Para uma demonstração deste resultado, referimos mais uma vez o livro de P. Halmos.

Exemplo A.2.12.

Observámos acima que o conjunto dos inteiros $\mathbb{Z}$, com a relação de ordem usual, não é um conjunto bem ordenado. No entanto, temos por exemplo a seguinte boa ordenação de $\mathbb{Z}$:

$$0, 1, -1, 2, -2, \ldots, n, -n, \ldots$$

O grande interesse dos conjuntos bem ordenados reside no facto de que para estes é possível generalizar o método de indução usual. Passamos a designar por $s(x)$ o conjunto dos elementos estritamente menores que x, ou seja, o "segmento" que termina em x:

$$s(x) = \{y \in X : y \leq x, \text{ e } y \neq x\}.$$

Temos então:

Teorema A.2.13 (Indução Transfinita). *Seja X um conjunto bem ordenado, e $S \subset X$, com a seguinte propriedade:*

$$\forall x \in X,\ s(x) \subset S \implies x \in S.$$

Então $S = X$.

[6] Daqui em diante, e salvo menção em contrário, denotaremos a relação de ordem (lata) de um conjunto X parcialmente ordenado pelo símbolo "$\leq$".

Demonstração. Se $X-S$ não for vazio, seja x o seu elemento mínimo. Então o segmento $s(x)$ está contido em S, logo, pela "hipótese de indução", $x \in S$. Como x não pode pertencer simultaneamente a S e a $X - S$, temos de ter $X - S$ vazio, ou seja, $X = S$. □

O método de indução transfinita tem um domínio de aplicação bastante largo, como decorre do Princípio da Boa Ordenação.

Finalmente, aproveitamos para formular a teoria que sustenta as definições recursivas referidas no texto, incluindo aqui também as definições recursivas *transfinitas*.

Sendo A um conjunto, e $n \in \mathbb{N}$, consideramos o conjunto A^n de todas as funções $f : I_n \to A$, *i.e.*, de todos os n-tuplos $(x_1, x_2, \cdots, x_n)$ em A. Consideramos igualmente a classe $\Phi = \cup_{n=1}^{\infty} A^n$, e observamos que uma "fórmula recursiva" é na realidade uma *função* $F : \Phi \to A$. É claro que, dado um n-tuplo $f_n \in A^n$, $f_n = (x_1, x_2, \cdots, x_n)$, a função F permite calcular um $(n+1)$-tuplo $f_{n+1} \in A^{n+1}$, $f_{n+1} = (x_1, x_2, \cdots, x_n, x_{n+1})$, onde $x_{n+1} = F(f_n) = F(x_1, x_2, \cdots, x_n)$.

O resultado que pretendemos demonstrar é o seguinte:

Teorema A.2.14 (Definições Recursivas). *Dado $x_1 \in A$, existe uma única sucessão $\phi : \mathbb{N} \to A$ tal que*

(i) $\phi(1) = x_1$, *e*

(ii) $\phi(k+1) = F(\phi_{|I_k})$, *para qualquer* $k \in \mathbb{N}$.

Designamos aqui por $\phi_{|I_k}$ a restrição de ϕ ao conjunto I_k.

Demonstração. Provamos primeiro, e por indução, que para qualquer $n \in \mathbb{N}$ existe $f_n \in A^n$ que satisfaz as condições

(1) $f_n(1) = x_1$, e

(2) $f_n(k+1) = F(f_{n|I_k})$, para qualquer $k < n$.

O resultado é evidente para $n = 1$, definindo $f_1(1) = x_1$, e reconhecendo que a condição (2) é, neste caso, vazia. Supondo o resultado verdadeiro para $n \geq 1$, existe portanto um n-tuplo $f_n = (x_1, x_2, \cdots, x_n) \in A^n$ que satisfaz (1) e (2). Definimos $f_{n+1} = (x_1, x_2, \cdots, x_n, x_{n+1}) \in A^{n+1}$, onde $x_{n+1} = F(f_n) = F(x_1, x_2, \cdots, x_n)$. É imediato reconhecer que f_{n+1} satisfaz automaticamente (1), e satisfaz ainda (2), mas agora para $k < n+1$.

Suponha-se agora que $f_n \in A^n$ e $f_m \in A^m$ satisfazem as condições (1) e (2). Supondo sem perda de generalidade que $n < m$, provamos a seguir que f_n é a restrição de f_m a I_n. Para isso, considere-se o conjunto $D = \{k \in I_n : f_n(k) \neq f_m(k)\}$. Supondo D não-vazio, seja $r+1$ o seu mínimo, e note-se que $r \geq 1$, porque por hipótese $f_n(1) = f_m(1) = x_1$. Temos, portanto, que $f_n(k) = f_m(k)$ para qualquer $k \leq r$, ou seja, as

restrições $f_{n|I_r}$ e $f_{m|I_r}$ são iguais. Mas, neste caso, temos necessariamente $f_n(r+1) = F(f_{n|I_r}) = F(f_{m|I_r}) = f_m(r+1)$, contradizendo a afirmação $r+1 \in D$.

Podemos finalmente concluir a demonstração. Como vimos, para qualquer $n \in \mathbb{N}$ existe exactamente uma função $f_n \in A^n$ que satisfaz as condições (1) e (2). Definimos $\phi : \mathbb{N} \to A$ por $f(n) = f_n(n)$. É imediato verificar que esta função é a única sucessão que satisfaz as condições (i) e (ii). □

O resultado anterior pode ser generalizado, substituindo $\mathbb{N}$ por um qualquer conjunto bem ordenado X. Neste caso, os conjuntos I_n são substituídos pelos segmentos $s(x) = \{y \in X : y < x\}$, $A_x = A^{s(x)}$ é o conjunto de todas as funções $f : s(x) \to A$, e temos, naturalmente, $\Phi = \cup_{x \in X} A_x$. A "fórmula recursiva" é novamente uma função $F : \Phi \to A$.

Enunciamos aqui o resultado correspondente, deixando a demonstração como exercício.

Teorema A.2.15 (Definições Recursivas Transfinitas). *Existe uma única função $f : X \to A$ tal que $f(x) = F(f_{|s(x)})$, para qualquer $x \in X$.*

Exercícios.

1. Mostre que $X \times Y$ é isomorfo a $Y \times X$. Em que condições é que é verdade a igualdade $X \times Y = Y \times X$?

2. Mostre que $X \times (Y \times Z)$ é isomorfo a $(X \times Y) \times Z$.

3. Descreva os conjuntos $X^{\emptyset}$, $\emptyset^X$ e $\emptyset^{\emptyset}$.

4. Mostre que os conjuntos $X^{Y \cup Z}$ e $X^Y \times X^Z$ são isomorfos.

5. Mostre que os conjuntos $X^{Y \times Z}$ e $(X^Y)^Z$ são isomorfos, desde que $Y \cap Z = \emptyset$.

6. Mostre que $(X \times Y)^Z$ é isomorfo a $X^Z \times Y^Z$.

7. Use o Axioma da Escolha para provar que $f : X \to Y$ é sobrejectiva se e só se existe $g : Y \to X$ tal que $f \circ g = I_Y$.

8. Mostre que, se $I \neq \emptyset$ e $X_i \neq \emptyset$ para qualquer $i \in I$, então as projecções canónicas $\pi_k : \prod_{i \in I} X_i \to X_k$ são sobrejectivas.

9. Use o Lema de Zorn para verificar que num grupo qualquer todo o subgrupo próprio está contido num subgrupo maximal.

10. Demonstre as seguintes afirmações:

    (a) Todo o conjunto parcialmente ordenado possui uma cadeia maximal;

    (b) Toda a cadeia num conjunto parcialmente ordenado está contida numa cadeia maximal.

11. Mostre que o princípio de indução transfinita é equivalente ao princípio de indução usual (ver Capítulo 2) no caso em que $X = \mathbb{N}$.

12. Dê um exemplo de uma boa ordenação para $\mathbb{Q}$.

13. Mostre que um conjunto X totalmente ordenado é bem ordenado se e só se para todo o $x \in X$ o segmento $s(x)$ é bem ordenado.

14. Demonstre o teorema A.2.15. Porque razão não mencionamos neste enunciado um elemento semelhante a x_1 no teorema A.2.14?

A.3 Conjuntos Finitos

A nossa intuição diz-nos que um conjunto X é finito se os seus elementos podem ser "contados". O protótipo dum conjunto finito com $n \geq 0$ elementos é dado pelo conjunto dos primeiros n naturais:

$$I_n = \{1, 2, 3, \ldots, n\} = \{k \in \mathbb{N} : k \leq n\}.$$

Note que, se $n = 0$, obtemos o conjunto vazio: $I_0 = \emptyset$. A "contagem" aqui referida consiste claramente no estabelecimento de uma correspondência (função) bijectiva entre X e I_n. Mais formalmente, temos:

Definição A.3.1. O conjunto X diz-se FINITO se é isomorfo a I_n, para algum $n \geq 0$. Se X não é isomorfo a nenhum I_n, então X diz-se INFINITO.

Exemplos A.3.2.

1. *O conjunto I_n é evidentemente isomorfo a si próprio, logo é finito.*
2. *O subconjunto $X \subset \mathbb{Z}$ é finito se e só se é limitado (exercício).*

Mencionámos no Capítulo 1 que X é infinito se e só se existe uma função $\phi : X \to X$ injectiva e não-sobrejectiva. Este resultado será estabelecido na próxima secção, onde iremos considerar em detalhe os conjuntos infinitos. No resto desta secção, consideramos apenas o caso dos conjuntos finitos. Primeiro começamos por considerar os conjuntos I_n.

Lema A.3.3. *Se $\phi : I_n \to I_n$ é injectiva, então ϕ é sobrejectiva.*

Demonstração. Argumentamos por indução e notamos que, quando $n = 0$, não há evidentemente nada a provar([7]).

[7] Uma função $f : X \to Y$ é apenas um conjunto de pares ordenados com propriedades especiais. É possível que f seja o conjunto vazio, o que ocorre exactamente quando X é também vazio. Neste caso, f é necessariamente injectiva, e só é sobrejectiva se Y é igualmente vazio.

Supondo o resultado válido para n, seja $\phi : I_{n+1} \to I_{n+1}$ uma função injectiva, e $\alpha = \phi(n+1)$. Considere-se (ver figura) a bijecção $\psi : I_{n+1} \to I_{n+1}$ dada por $\psi(n+1) = \alpha$, $\psi(\alpha) = n+1$, e $\psi(x) = x$ em todos os outros casos (ψ "troca" os naturais α e $n+1$, e é a identidade se $x \neq \alpha, n+1$, mas este último facto é irrelevante para a demonstração).

Definimos $\phi^* = \psi \circ \phi$ e notamos que ϕ^* é injectiva (por ser uma composição de funções injectivas), com $\phi^*(n+1) = n+1$ (por definição de ψ). Como ϕ^* é injectiva, se $x \in I_n$ (*i.e.*, se $x \neq n+1$), temos $\phi^*(x) \neq n+1$, donde $\phi^*(x) \in I_n$, ou ainda $\phi^*(I_n) \subseteq I_n$.

A restrição de ϕ^* a I_n é portanto uma função injectiva de I_n em I_n, e segue-se, da hipótese de indução, que esta restrição é sobrejectiva, ou seja, que $\phi^*(I_n) = I_n$. Como $\phi^*(n+1) = n+1$, temos ainda $\phi^*(I_{n+1}) = I_{n+1}$, *i.e.*, ϕ^* é uma função sobrejectiva de I_{n+1} em I_{n+1}.

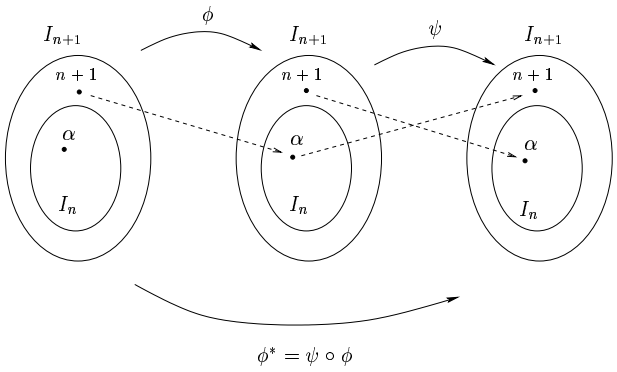


Figura A.3.1: As funções ϕ, ϕ^* e ψ.

Observamos finalmente que $\phi = \psi^{-1} \circ \phi^*$ é sobrejectiva, por ser uma composição de funções sobrejectivas. □

Proposição A.3.4. *Se X é finito e $\phi : X \to X$ é injectiva, então ϕ é sobrejectiva.*

Demonstração. Seja $\Psi : I_n \to X$ uma bijecção, e note-se que $\phi^* = \Psi^{-1} \circ \phi \circ \Psi : I_n \to I_n$ é injectiva, por ser uma composição de funções injectivas (ver figura). De acordo com o Lema A.3.3, ϕ^* é necessariamente sobrejectiva.

Segue-se que $\phi = \Psi \circ \phi^* \circ \Psi^{-1}$ é uma composição de funções sobrejectivas, e consequentemente é sobrejectiva. □

Corolário A.3.5. *Se $\phi : X \to X$ é injectiva e não-sobrejectiva, então X é infinito.*

Exemplo A.3.6.

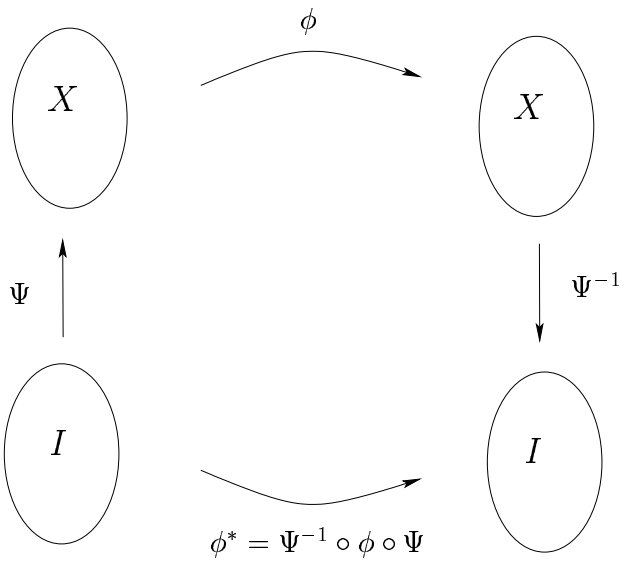


Figura A.3.2: As funções ϕ, ϕ^* e Ψ.

Observámos no Capítulo 2 que a função $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = n + 1$ é injectiva e não-sobrejectiva. De acordo com o resultado anterior, concluímos que $\mathbb{N}$ é infinito.

A demonstração do corolário seguinte fica como exercício. Por palavras, a afirmação é a de que nenhum conjunto finito pode ser isomorfo a um seu subconjunto *estrito*.

Corolário A.3.7. *Se X é finito, $X \supseteq Y$ e $\phi : X \to Y$ é injectiva, então $X = Y$.*

O exemplo acima mostra que este corolário é falso para conjuntos infinitos.

Parece ser óbvio que X é isomorfo a I_n se e só se X tem n elementos, e que neste caso X não pode ser simultaneamente isomorfo a I_m se $m \neq n$. Na realidade, esta afirmação é uma consequência lógica directa da Proposição A.3.4.

Corolário A.3.8. *Se $\phi : I_n \to X$ e $\psi : I_m \to X$ são bijectivas, então $n = m$.*

Demonstração. Supomos sem perda de generalidade que $m \leq n$, ou seja, $I_m \subset I_n$, e notamos que $\Psi = \psi^{-1} \circ \phi : I_n \to I_m$ é uma função injectiva de I_n num seu subconjunto I_m. Segue-se, do Corolário A.3.7, que $I_m = I_n$, *i.e.*, $n = m$. □

De acordo com o resultado anterior, se X é finito, existe um *único* inteiro não-negativo n tal que X é isomorfo a I_n. Dizemos neste caso que X tem n elementos, e designamos o número de elementos do conjunto finito X pelo símbolo $\#X$, dito o CARDINAL de X.

Para terminar esta secção enunciamos ainda alguns resultados elementares sobre cardinalidade, cujas demonstrações serão apenas parcialmente esboçadas, deixando os detalhes como exercício.

Proposição A.3.9. *Se Y é subconjunto do conjunto X, temos:*

(i) Se X é finito, então Y é igualmente finito e $\#Y \leq \#X$.

(ii) Se X é finito e $\#Y = \#X$, então $X = Y$.

(iii) Se Y é infinito, então X é igualmente infinito.

Esta proposição pode ser demonstrada recorrendo aos dois lemas que indicamos a seguir. O primeiro é de demonstração simples e fica como exercício.

Lema A.3.10. *Se $\phi : I_n \to X$ é injectiva e não-sobrejectiva, então existe $\phi^* : I_{n+1} \to X$ injectiva.*

O próximo lema completa a demonstração da Proposição A.3.9.

Lema A.3.11. *Se $\phi : X \to I_n$ é injectiva, então X é finito e $\#X \leq n$.*

Demonstração. Seja $M(X)$ o conjunto dos inteiros $m \geq 0$ para os quais existe uma função $\Psi_m : I_m \to X$ injectiva. Pelo Lema A.3.10 é claro que $\#X$ é o máximo de $M(X)$, pelo que precisamos de verificar que $M(X)$ é não-vazio e majorado. Como 0 pertence a $M(X)$, temos apenas a provar que $M(X)$ é majorado.

Se $\Psi_m : I_m \to X$ é injectiva, a composta $\phi \circ \Psi : I_m \to I_n$ é também injectiva. De acordo com o Corolário A.3.7, não podemos ter $n < m$, *i.e.*, n é um majorante de $M(X)$.

Assim, se k é o máximo de $M(X)$, temos $k = \#X$, e como n é um majorante de $M(X)$ segue-se que $\#X = k \leq n$. □

A próxima proposição corresponde claramente às nossas intuições mais básicas sobre o significado da adição e produto de números naturais.

Proposição A.3.12. *Se X e Y são finitos, então:*

(i) $X \cup Y$ é finito e $\#(X \cup Y) \leq \#X + \#Y$;

(ii) Se X e Y são disjuntos, então $\#(X \cup Y) = \#X + \#Y$;

(iii) $X \times Y$ é finito e $\#(X \times Y) = (\#X)(\#Y)$.

Demonstração. Limitamo-nos a demonstrar o item (ii), deixando as restantes afirmações como exercícios.

Sejam $\phi : I_n \to X$ e $\psi : I_m \to Y$ duas bijecções, donde $\#X = n$ e $\#Y = m$. Definimos a função $\Psi : I_{n+m} \to X \cup Y$ como se segue:

$$\Psi(k) = \begin{cases} \phi(k) & \text{se } 1 \leq k \leq n, \\ \\ \psi(k-n) & \text{se } n+1 \leq k \leq n+m. \end{cases}$$

É evidente que Ψ é bijectiva, onde a injectividade de Ψ se deve ao facto de X e Y serem supostos disjuntos. Portanto,

$$\#(X \cup Y) = n + m.$$

□

Exercícios.

Nestes exercícios, os símbolos X e Y designam conjuntos arbitrários.

1. Prove o Corolário A.3.7.

2. Demonstre o Lema A.3.10

3. Prove que, se $\phi : I_n \to X$ é sobrejectiva, então $\Psi : X \to I_n$ dada por $\Psi(k) = \max\{k \in I_n : \phi(k) = x\}$ é injectiva.

4. Mostre que as seguintes afirmações são equivalentes:

   (a) X é finito e $\#X \leq n$.

   (b) Existe uma função injectiva $\phi : X \to I_n$.

   (c) Existe uma função sobrejectiva $\psi : I_n \to X$.

5. Prove que, se X é finito e $\phi : X \to Y$ é sobrejectiva ou $\psi : Y \to X$ é injectiva, então Y é finito e $\#Y \leq \#X$.

6. Demonstre a Proposição A.3.9 recorrendo ao Corolário A.3.7 e ao Lema A.3.11.

7. Prove que, se X e é finito, então $\#X = \#(X - Y) + \#(X \cap Y)$.

8. Prove que, se X e Y são finitos, então $X \cup Y$ é finito e

$$\#(X \cup Y) = \#X + \#Y - \#(X \cap Y).$$

9. Mostre que, se X e Y são finitos, então $X \times Y$ é finito e $\#(X \times Y) = (\#X)(\#Y)$.

10. Prove que, se $X_1, X_2, \ldots, X_n$ são finitos, então:
    (a) $\#(\bigcup_{k=1}^n X_k) \leq \sum_{k=1}^n \#X_k$;
    (b) $\#(\bigcup_{k=1}^n X_k) = \sum_{k=1}^n \#X_k$, se os X_k's são disjuntos;
    (c) $\#(\prod_{k=1}^n X_k) = \prod_{k=1}^n \#X_k$.

11. Suponha que $\#X = n$ e $\#Y = n$. Quantos elementos têm os seguintes conjuntos?
    (a) O conjunto Y^X de todas as funções $f : X \to Y$.
    (b) O conjunto das funções injectivas $f : X \to Y$.
    (c) O conjunto das funções sobrejectivas $f : X \to Y$.

12. Suponha que $\#X = n$, e prove que:
    (a) X tem 2^n subconjuntos distintos;
    (b) X tem $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ subconjuntos com k elementos.

13. Suponha que $X \subset \mathbb{Z}$, e prove que X é finito se e só se X é limitado.

A.4 Conjuntos Infinitos

Já provámos vários resultados elementares sobre conjuntos infinitos na secção anterior. Provámos também que $\mathbb{N}$ é um conjunto infinito. Começamos agora por verificar que, em certo sentido, $\mathbb{N}$ é o mais pequeno conjunto infinito.

Lema A.4.1. *X é infinito se e só se X contém um subconjunto isomorfo a $\mathbb{N}$.*

Demonstração. Se existe um subconjunto Y de X e uma bijecção $\phi : \mathbb{N} \to Y$, segue-se que Y é infinito, e portanto X é infinito, de acordo com a Proposição A.3.9 (iii).

Suponha-se agora que X é infinito, e mostremos que existe uma função injectiva $\phi : \mathbb{N} \to X$ (o conjunto Y será então $Y = X$). A função ϕ é uma sucessão que definimos recursivamente.

Como $X \neq \emptyset$, existe $x_1 \in X$, e definimos $\phi(1) = x_1$. Suponha-se agora que ϕ está definida e é injectiva em $\{1, 2, \ldots, n\}$. Consideramos o conjunto $Z_n = X - \{\phi(1), \ldots, \phi(n)\}$, e observamos que $Z_n \neq \emptyset$, já que caso contrário X teria n elementos. Sendo z um qualquer elemento de Z_n, definimos $\phi(n+1) = z$, e concluímos que existe uma função $\phi : \mathbb{N} \to X$, que por definição é injectiva. □

Este resultado simples permite-nos completar o Corolário A.3.5, e justificar a caracterização dos conjuntos infinitos mencionada nos exercícios do Capítulo 1.

Teorema A.4.2. *X é infinito se e só se existe $\phi : X \to X$ injectiva e não-sobrejectiva.*

Demonstração. Já sabemos (Corolário A.3.5), que se $\phi : X \to X$ é injectiva e não-sobrejectiva, então X é infinito. Resta-nos portanto provar que se, X é infinito, existe necessariamente uma função com estas características.

Se X é infinito, existe, de acordo com o Lema A.4.1, uma função (sucessão) injectiva $\psi : \mathbb{N} \to X$. Definimos $Y = \psi(\mathbb{N})$, e observamos que $\psi : \mathbb{N} \to Y$ é uma bijecção. Definimos $\phi : X \to X$ como se segue:

$$\phi(x) = \begin{cases} x & \text{se } x \notin Y, \\ \\ \psi(\psi^{-1}(x) + 1) & \text{se } x \in Y. \end{cases}$$

É fácil verificar que ϕ é injectiva e não-sobrejectiva. □

As propriedades dos conjuntos infinitos que vimos até agora não têm nada de realmente surpreendente. A primeira observação que fazemos que é de algum modo inesperada é a de que o Lema A.4.1 não pode ser reforçado: há conjuntos infinitos que não são isomorfos a $\mathbb{N}$. No que se segue, usaremos o símbolo $\mathcal{P}(X)$ para designar o conjunto de todos os subconjuntos de X.

Teorema A.4.3 (Cantor). *Seja $\Psi : X \to \mathcal{P}(X)$ uma função. Então Ψ não é sobrejectiva.*

Demonstração. Argumentamos por contradição, usando uma ideia semelhante à que referimos no Capítulo 1 em ligação com o paradoxo de Russell.

Seja $\Psi : X \to \mathcal{P}(X)$ e defina-se $Y = \{x \in X : x \notin \Psi(x)\}$, claramente um elemento de $\mathcal{P}(X)$. Se Ψ é sobrejectiva, existe um elemento $y \in X$ tal que $Y = \Psi(y)$, e temos $y \in Y$, ou $y \notin Y$.

Vejamos agora que ambos os casos são impossíveis:

(i) Se $y \in Y = \Psi(y)$, segue-se, da definição de Y, que $y \notin Y$, o que é absurdo;

(ii) Se $y \notin Y = \Psi(y)$ segue-se, da definição de Y, que $y \in Y$, o que é igualmente absurdo.

Concluímos que não existe $y \in X$ tal que $Y = \Psi(y)$, logo, Ψ não é sobrejectiva. □

Exemplos A.4.4.

1. *Para ilustrar a técnica da demonstração acima, suponha-se que $X = \{0, 1\}$, donde*
$$\mathcal{P}(X) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}.$$
Se $\Psi : X \to \mathcal{P}(X)$ é dada, por exemplo, por $\Psi(0) = \{1\}$, e $\Psi(1) = \{0, 1\}$. Temos $Y = \{x \in X : x \notin \Psi(x)\} = \{0\}$, e obviamente $Y \notin \Psi(X) = \{\{1\}, \{0, 1\}\}$.

2. Considere-se o conjunto $\mathcal{P}(\mathbb{N})$ formado por todos os conjuntos constituídos por naturais. De acordo com o resultado acima, este conjunto não é isomorfo a $\mathbb{N}$. Por outro lado, a função $\Phi : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ dada por $\Phi(n) = \{n\}$ é evidentemente injectiva, e portanto $\mathcal{P}(\mathbb{N})$ é infinito.

Definição A.4.5. O conjunto X diz-se NUMERÁVEL se e só se é finito ou isomorfo a $\mathbb{N}$. Caso contrário, X diz-se (infinito) NÃO-NUMERÁVEL.

De acordo com o que vimos, X é um conjunto infinito se e só se contém um subconjunto infinito numerável, mas existem conjuntos infinitos não-numeráveis, como por exemplo $\mathcal{P}(\mathbb{N})$. Por outro lado, observe que há conjuntos não-numeráveis que, não sendo isomorfos a $\mathbb{N}$, não são também isomorfos entre si. Exemplos são os conjuntos $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$, etc.

Dos conjuntos com que lidamos habitualmente, o exemplo mais simples dum conjunto infinito não-numerável é $\mathbb{R}$, o conjunto dos números reais. Vamos agora demonstrar este facto, utilizando para isso a seguinte propriedade destes números, que é usualmente apresentada como uma consequência do *Axioma do Supremo*.

Proposição A.4.6. *Qualquer sucessão monótona e limitada de números reais é convergente.*

A demonstração desta proposição é feita no Capítulo 4, onde os números reais são introduzidos de forma *construtiva*.

Teorema A.4.7. *$\mathbb{R}$ é um conjunto não-numerável.*

Demonstração. Seja $\phi : \mathbb{N} \to \mathbb{R}$ uma sucessão *qualquer* de números reais. Temos a demonstrar que ϕ não é sobrejectiva, *i.e.*, que existe $x \in \mathbb{R}$ tal que $x \notin \phi(\mathbb{N})$.

Existem reais a_1 e b_1 tais que $a_1 < b_1 < \phi(1)$. Em particular, $\phi(1) \notin [a_1, b_1]$. É fácil definir recursivamente sucessões a_n e b_n, respectivamente crescente e decrescente, tais que $a_n < b_n$ e $\phi(n) \notin [a_n, b_n]$. É evidente que ambas as sucessões são limitadas por a_1 e b_1. Segue-se, da Proposição A.4.6, que ambas têm limites, respectivamente a e b. É também claro que $a_n \leq a \leq b \leq b_n$, donde concluímos imediatamente que $a \neq \phi(n)$, para qualquer $n \in \mathbb{N}$, e ϕ não é sobrejectiva. □

Exemplo A.4.8.

*O conjunto $\{0,1\}^{\mathbb{N}}$, das sucessões com valores em $\{0,1\}$, (ditas **sucessões binárias**) é igualmente não-numerável. É neste caso fácil verificar directamente que $\{0,1\}^{\mathbb{N}}$ é isomorfo a $\mathcal{P}(\mathbb{N})$. Para isso, note-se que uma sucessão binária $\phi : \mathbb{N} \to \{0,1\}$ é completamente determinada pelo seu **suporte**,* i.e.*, pelo conjunto dos naturais n, onde $\phi(n) \neq 0$. Por outras palavras, $\Psi : \{0,1\}^{\mathbb{N}} \to \mathcal{P}(\mathbb{N})$, definida por $\Psi(\phi) = \{n \in \mathbb{N} : \phi(n) \neq 0\}$, é uma bijecção.*

É possível utilizar a bijecção deste exemplo, juntamente com alguns factos elementares sobre expansões de números reais na base dois para provar que, na realidade, tanto $\mathcal{P}(\mathbb{N})$ como $\{0,1\}^{\mathbb{N}}$ são isomorfos a $\mathbb{R}$ (exercício).

Não definiremos o símbolo "#X" quando X é um conjunto infinito. Usaremos no entanto o símbolo "$|X|$", também lido **cardinal** de X, onde X designa um qualquer conjunto (finito ou infinito), como parte das expressões "$|X| = |Y|$", "$|X| \leq |Y|$" e "$|X| < |Y|$", com os significados que indicamos abaixo:

Definição A.4.9. Escrevemos:

(i) $|X| = |Y|$ se X e Y são isomorfos, *i.e.*, se existe uma bijecção $\phi : X \to Y$;

(ii) $|X| \leq |Y|$ se X é isomorfo a um subconjunto de Y, *i.e.*, se existe uma função injectiva $\phi : X \to Y$;

(iii) $|X| < |Y|$ se $|X| \leq |Y|$, e X não é isomorfo a Y.

A igualdade "$|X| = |Y|$" e a desigualdade "$|X| \leq |Y|$" são análogas às igualdades e desigualdades entre números "$\#(X) = \#(Y)$" e "$\#(X) \leq \#(Y)$" quando X e Y são finitos. Por isso mesmo, nesse caso podemos escrever $\#X = |X|$. Mesmo quando X e Y são infinitos, o cardinal tem algumas propriedades semelhantes às das igualdades e desigualdades entre números, de que destacamos a título de exemplo as seguintes, ambas de demonstração imediata.

Proposição A.4.10. *Sejam X, Y e Z conjuntos.*

(i) Se $|X| = |Y|$ e $|Y| = |Z|$, então $|X| = |Z|$;

(ii) Se $|X| \leq |Y|$ e $|Y| \leq |Z|$, então $|X| \leq |Z|$.

Parece também intuitivamente evidente que

$$|X| \leq |Y| \text{ e } |Y| \leq |X| \Longleftrightarrow |X| = |Y|.$$

A demonstração deste facto não é no entanto óbvia, pelo menos para conjuntos infinitos. Começamos por provar um lema auxiliar, que sabemos já ser verdadeiro quando X é finito, caso em que se pode reforçar com a conclusão adicional "e $X = Y$".

Lema A.4.11. *Se $Y \subset X$ e $\phi : X \to Y$ é injectiva, então $|X| = |Y|$.*

Demonstração. Definimos recursivamente duas sucessões de conjuntos como se segue: $X_1 = X$, $Y_1 = Y$, e para $n > 1$, $X_n = \phi(X_{n-1})$ e $Y_n = \phi(Y_{n-1})$ Definimos ainda $Z_n = X_n - Y_n$, e

$$Z = \bigcup_{n=1}^{\infty} Z_n.$$

É claro que $(X - Z) \subset Y$, porque, se $x \in X$ e $x \notin Y = Y_1$, então $x \in Z_1$, donde $x \in Z$. Além disso, se $x \in Z$, *i.e.*, se existe n tal que $x \in Z_n$, então $\phi(x) \in Z_{n+1}$, ou seja, $\phi(x) \in Z$.

Definimos $\Psi : X \to X$ por

$$\Psi(x) = \begin{cases} \phi(x) & \text{se } x \in Z, \\ \\ x & \text{se } x \notin Z. \end{cases}$$

Note-se que $\Psi(X) \subseteq Y$, pois, se $x \in Z$, então $\Psi(x) = \phi(x) \in Y$, e, se $x \notin Z$, então $x \in Y$ e $\Psi(x) = x$. Provamos em seguida que $Y \subseteq \Psi(X)$, para concluir que $\Psi(X) = Y$. Para isso, considere-se $x \in Y$, e note-se que se $x \notin Z$ então $x = \Psi(x) \in \Psi(X)$. Se, por outro lado, $x \in Z \cap Y$, então $x \in Z_n$ para algum $n > 1$ (é óbvio que Y não contém nenhum ponto de Z_1), e portanto $x \in \phi(Z_{n-1})$, donde $x \in \Psi(X)$.

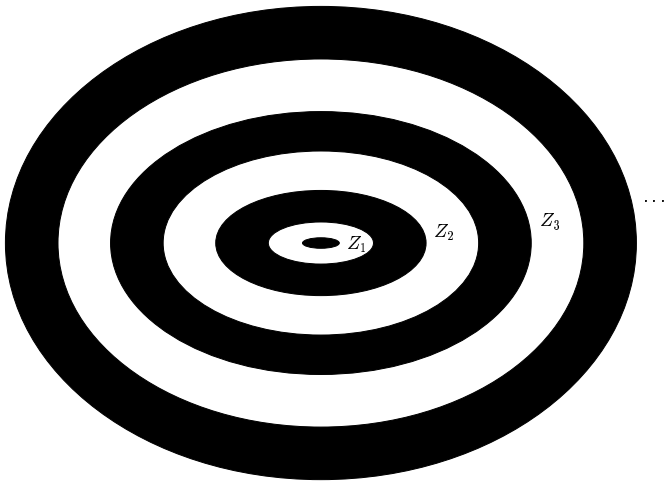


Figura A.4.1: Os conjuntos Z_1, Z_2, Z_3, ...

Como $\Psi(X) = Y$, para concluir a demonstração do lema resta-nos estabelecer que Ψ é injectiva. Suponha-se para isso que $x, y \in X$ e que $x \neq y$. Consideramos três casos:

(i) Se $x, y \in Z$, então $\Psi(x) \neq \Psi(y)$, porque $\Psi = \phi$ em Z, e ϕ é injectiva.

(ii) Se $x, y \notin Z$, então $\Psi(x) \neq \Psi(y)$, porque Ψ é a identidade em $X - Z$.

(iii) Se $x \in Z$ e $y \notin Z$, então $\Psi(x) \neq \Psi(y)$, porque $\Psi(y) = y \notin Z$ e $\Psi(x) = \phi(x) \in Z$.

Concluímos, pois, que X e Y são isomorfos. □

Exemplo A.4.12.

A construção de Y na demonstração precedente é engenhosa mas simples. A título de ilustração, supomos $X = \mathbb{N}_0 = \{n \in \mathbb{Z} : n \geq 0\}$, $Y = \mathbb{N}$ e $\phi(x) = x + 2$. Neste caso, é óbvio que $X_n = \{k \in \mathbb{Z} : k \geq 2(n-1)\}$ e $Y_n = \{k \in \mathbb{Z} : k \geq 2(n-1) + 1\}$. Segue-se que $Z_n = \{2(n-1) : n \in \mathbb{N}\}$, e Z é claramente o conjunto dos inteiros pares não-negativos. A função Ψ descrita no teorema anterior reduz-se à função ϕ no conjunto dos inteiros pares não-negativos, e é a identidade sobre o conjunto dos naturais ímpares. É evidentemente uma bijecção de X em Y.

Podemos agora demonstrar o

Teorema A.4.13 (Schroeder-Bernstein). *Se $|X| \leq |Y|$ e $|Y| \leq |X|$, então $|X| = |Y|$.*

Demonstração. Sejam $\phi : X \to Y$ e $\psi : Y \to X$ funções injectivas, $Z = \psi(Y)$, e note-se que $\psi \circ \phi : X \to Z$ é injectiva. Como $Z \subseteq X$, existe, de acordo com o lema anterior, uma bijecção $\Psi : Z \to X$, e é evidente que a composta $\Psi \circ \psi : Y \to X$ é uma bijecção. □

O Teorema de Schroeder-Bernstein permite-nos frequentemente provar que dois conjuntos são isomorfos, sem exibirmos explicitamente uma bijecção entre esses conjuntos. O exemplo seguinte ilustra isso mesmo.

Exemplo A.4.14.

Considerem-se os conjuntos $X = \mathbb{N} \times \mathbb{N}$ e $Y = \mathbb{N}$. A função $\phi : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ dada por $\phi(n) = (n, 1)$ é injectiva, e de acordo com o Teorema Fundamental da Aritmética a função $\psi : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ dada por $\psi(n, m) = 2^n 3^m$ é também injectiva. Segue-se do Teorema de Schroeder-Bernstein que $\mathbb{N}$ e $\mathbb{N} \times \mathbb{N}$ são isomorfos.

Dado que $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, é fácil provar os seguintes resultados, cuja demonstração deixamos como exercício.

Proposição A.4.15. *Sejam X, X_n e Y conjuntos numeráveis.*

(i) Se $Y \neq \emptyset$ e X é infinito, então $|X \times Y| = |X|$, i.e.*, $X \times Y$ é numerável.*

(ii) O conjunto $\bigcup_{n=1}^{\infty} X_n$ é numerável.

Esta proposição mostra que o comportamento da noção de cardinal face às operações de união e produto de conjuntos infinitos é um pouco peculiar. Enunciamos abaixo dois resultados gerais, referentes a uniões e produtos, que exemplificam bem esta observação. Não demonstramos nenhuma das afirmações, para não nos envolveremos demasiado em questões técnicas da teoria dos conjuntos (veja no entanto alguns dos exercícios abaixo).

Teorema A.4.16. *Se X é infinito e $|Y| \leq |X|$, então:*

(i) $|X \cup Y| = |X|$;

(ii) $|X \times Y| = |X|$, *se* $Y \neq \emptyset$.

Exercícios.

1. Prove que $\mathbb{Z}$ e $\mathbb{Q}$ são numeráveis.

2. Mostre que os intervalos $[0,1]$, $]0,1[$, e $[0,1[$ (em $\mathbb{R}$) são todos isomorfos a $\mathbb{R}$.

3. Seja X um conjunto numerável (finito ou infinito). Em cada um dos exemplos seguintes, diga se o conjunto indicado é numerável (finito ou infinito) e justifique a sua resposta.
   (a) O conjunto $X^{\{0,1\}}$ das funções $f : \{0,1\} \to X$.
   (b) O conjunto X^{I_n} das funções $f : I_n \to X$.
   (c) O conjunto $Y = \bigcup_{n=1}^{\infty} X^{I_n}$.
   (d) O conjunto $X^{\mathbb{N}}$ das funções $f : \mathbb{N} \to X$.
   (e) O conjunto $\{0,1\}^X$ das funções $f : X \to \{0,1\}$.
   (f) O conjunto das sucessões $f : \mathbb{N} \to X$ que são "*eventualmente constantes*", *i.e.*, para cada uma das quais existe $N \in \mathbb{N}$ tal que $n > N \Rightarrow f(n) = x \in X$.
   (g) O conjunto $\mathcal{P}_{\text{fin}}(X)$ das partes finitas (*i.e.*, os subconjuntos finitos) de X.

4. Mostre que o conjunto dos polinómios com coeficientes racionais é numerável.

5. Prove que, se os conjuntos X_n são numeráveis, então também são numeráveis os conjuntos $\bigcup_{n=1}^{N} X_n$ e $\bigcup_{n=1}^{\infty} X_n$.

6. Prove que, se os conjuntos X_n são numeráveis, então $\prod_{n=1}^{N} X_n$ é numerável. Quando é que $\prod_{n=1}^{\infty} X_n$ é numerável?

7. Prove que, se X é infinito, $Y \subset X$ e Y é finito, então $|X| = |X - Y|$.

8. Prove que, se X é infinito, $Y \subset X$, $X - Y$ é infinito e Y é numerável, então $|X| = |X - Y|$. Conclua que, se X é não-numerável e Y é numerável, então $|X \cup Y| = |X|$.

9. Seja $\{0,1\}^{\mathbb{N}}$ o conjunto das sucessões binárias. Prove que $\{0,1\}^{\mathbb{N}}$ é isomorfo ao intervalo $[0,1]$ em $\mathbb{R}$, e portanto isomorfo a $\mathbb{R}$.

10. Seja $\{0,1\}^{\mathbb{N}}$ o conjunto das sucessões binárias. Prove que $\{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}}$ é isomorfo a $\{0,1\}^{\mathbb{N}}$, e conclua que $\mathbb{R}^n$ é isomorfo a $\mathbb{R}$ para qualquer n.

11. Suponha que $|X_n| \leq |\mathbb{R}|$ e prove que $|\bigcup_{n=1}^{\infty} X_n| \leq |\mathbb{R}|$.

12. Considere a sucessão de conjuntos $X_1 = \mathbb{N}$, $X_{n+1} = \mathcal{P}(X_n)$. Prove que existe um conjunto Y que verifica $|Y| > |X_n|$, para qualquer $n \in \mathbb{N}$.

13. Seja X um conjunto infinito e $\mathcal{P}_{\text{fin}}(X)$ o conjunto das partes finitas de X. Mostre que $|X| = |\mathcal{P}_{\text{fin}}(X)|$.

Sugestões de Leitura Adicional

A Álgebra é uma área vastíssima da Matemática, estando fora de questão fornecer um lista de referências que faça justiça a essa vastidão. Parece-nos útil, no entanto, deixar ao leitor algumas referências e fontes para tratamentos alternativos e leitura adicional. Listas bibliográficas muito mais exaustivas podem ser encontradas nalgumas das referências listadas. Esperamos que a leitura deste texto encoraje o leitor a prosseguir um estudo mais profundo desta área da Matemática, o que poderá fazer, consultando algumas das referências abaixo.

Referências Gerais

Alguns textos universalmente reconhecidos como excelentes referências, onde se fornecem exposições básicas de Álgebra e que incluem muitos dos tópicos cobertos neste livro, são:

- G. Birkhoff e S. MacLane, *A Survey of Modern Algebra*, AKP Classics, Natick, MA, 1994.
- T. Hungerford, *Algebra*, Springer-Verlag, New York, 1989.
- N. Jacobson, *Basic Algebra*, W. H. Freeman, New York, 1989.
- S. Lang, *Algebra*, Adison-Wesley, Massachusetts, 1994.

Um livro um pouco menos ambicioso, mas com uma exposição mais "recreativa" e por isso bastante agradável, é:

- M. Artin, *Algebra*, Prentice-Hall, New Jersey, 1991.

Também devemos mencionar os 2 volumes de Bourbaki dedicados à Álgebra, que podem ser utilizados, por exemplo, como referências auxiliares pontuais:

- N. Bourbaki, *Elements of Mathematics - Algebra*, Capítulos 1 a 7, Springer-Verlag, New York, 1990.

Finalmente uma boa referência que cobre os aspectos fundamentais da Teoria das Categorias é:

- S. MacLane, *Categories for the Working Mathematician*, Springer-Verlag, Berlin, 1972.

Teoria dos Conjuntos

A nossa referência preferida como introdução a este assunto é sem dúvida

- P. Halmos, *Naive Set Theory*, Springer-Verlag, New York, 1974.

Sobre os problemas de Lógica e Fundamentos da Matemática aflorados no texto, podemos referir também as seguintes obras:

- M. Eisenberg, *Axiomatic Theory of Sets and Classes*, Holt, Rinehart and Winston, New York, 1971.
- E. Mendelson, *Introduction to Mathematical Logic*, Chapman & Hall, London, 1997.

Grupos

Todos os aspectos clássicos da Teoria dos Grupos, incluindo alguns dos tópicos que não são discutidos neste livro (por exemplo, a Teoria de Representações e a cohomologia de grupos) são cobertos em

- D. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, New York, 1993.

A referência mais clássica sobre a Teoria dos Grupos é o seguinte livro de Hall, que nos parece ainda bastante recomendável:

- M. Hall, *The Theory of Groups*, The Macmillan Co., New York, 1959.

Estas referências não incluem, claro está, a classificação dos grupos finitos simples. Para essa recomendamos, como introdução, o artigo

- R. Solomon, "On finite simple groups and their classification", *Notices of the American Mathematical Society* **42**, 231–239 (1995).

Como curiosidade referimos que as tabelas com as representações, caracteres, e informação relacionada, sobre os grupos finitos simples, foram compilados no livro

- J. Conway, R. Curtis, S. Norton, R. Parker e R. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

Anéis e Módulos

Os vários textos que Jacobson escreveu sobre Álgebra são todos eles excelentes referências sobre anéis e a sua estrutura[8]. Podemos citar por exemplo:

- N. Jacobson, *Lectures in Abstract Algebra*, volumes I, II e III, Van Nostrand Company, Princeton, NJ, 1964.
- N. Jacobson, *Structure of Rings*, American Mathematical Society, Colloquium Publications, volume 37, Providence, RI, 1956.

Uma outra referência clássica é

- I. Kaplanski, *Fields and Rings*, University of Chicago Press, Chicago, 1972.

Uma direcção muito importante em que a teoria dos anéis e dos módulos se expandiu, com origem na Topologia, é a Álgebra Homológica. Esta só de passagem é aflorada nos exercícios deste texto. Duas referências excelentes são:

- S. MacLane, *Homology*, Springer-Verlag, Berlin, 1974.
- C. Weibel, *An Introduction to Homological Algebra*, Cambridge University Press, Cambridge, 1994.

Corpos e Teoria de Galois

Todas as referências gerais que fornecemos acima incluem discussões mais ou menos completas sobre extensões de corpos e Teoria de Galois. No entanto, uma referência clássica é:

- E. Artin, *Galois Theory*, Dover Publications, Mineola, NY, 1998.

O livro de Kaplanski que citámos acima também é uma boa referência. Duas referências que seguem um ritmo menos intenso, e que são uma boa fonte de exemplos e exercícios, são:

- L. Gaal, *Classical Galois Theory with Examples*, AMS Chelsea Publishing, Providence, RI, 1998.
- I. Stewart, *Galois Theory*, Chapman and Hall, London, 1989.

A Teoria de Galois clássica conheceu vários desenvolvimentos posteriores. Um dos mais interessantes é, na nossa opinião, a Teoria de Galois Diferencial que permite lidar, por exemplo, com extensões transcendentes. Uma excelente exposição é dada no livro

[8]Nathan Jacobson (1910-1999) foi um dos grandes algebristas do século *XX*, e deu contribuições fundamentais à Teoria dos Anéis.

- I. Kaplanski, *An Introduction to Differential Algebra*, Hermann, Paris, 1957.

Finalmente, uma boa referência para a Teoria dos Números na sua vertente algébrica é:

- S. Lang, *Algebraic Number Theory*, Adison-Wesley, Massachusetts, 1970.

Álgebra Comutativa

Como excelentes introduções à Álgebra Comutativa recomendamos:

- M. Atiyah e I. MacDonald, *Introduction to Commutative Algebra*, Adison-Wesley, Massachusetts, 1969.
- P. Samuel e O. Zariski, *Commutative Algebra*, Van Nostrand, Princeton (1960).

Uma excelente introdução, a um nível mais básico, mas que inclui aplicações concretas a Geometria Algébrica e à Teoria dos Números é o livro

- M. Reid, *Undergraduate Commutative Algebra*, London Mathematical Society, Cambridge University Press, Cambridge, UK, 1995.

Ao leitor mais audacioso, que queira mergulhar nas águas mais profundas da Geometria Algébrica, recomendamos por exemplo:

- R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1976.

Deixamos ainda duas referências sobre bases de Gröbner e suas aplicações:

- W. Adams e P. Loustaunau, *An Introduction to Gröbner Bases*, American Mathematical Society, Providence, RI, 1994.
- D. Cox, J. Little e J. O'Shea, *Gröbner Bases, A Computational Approach to Commutative Algebra*, Springer-Verlag, New York, 1993.

Outros

A nossa última sugestão de leitura adicional é um livro que não pertence a nenhuma área da Matemática, ou que pertence a todas, e escrito pela mão de Deus[9]:

- M. Aigner e G. Ziegler, *Proofs from THE BOOK*, Springer-Verlag, Berlin, 1998.

[9]Esta nossa afirmação, sem dúvida um pouco audaciosa, está para além do âmbito deste livro. Se quiser compreendê-la, terá de ler a introdução ao livro a que nos referimos aqui.

Índice