DA PLASTICINA ÀS EQUAÇÕES DE QUINTO GRAU

ELOÍSA GRIFO

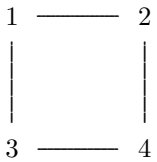
Resumo. Porque é que existe uma fórmula resolvente para equações polinomiais de segundo, terceiro e quarto grau mas não de quinto? Algumas perguntas clássicas e que atormentaram cientistas de vários séculos levaram os matemáticos do século XX a definir estruturas algébricas abstractas que de forma absolutamente espantosa permitem responder a esta e a muitas outras perguntas que nunca pensaríamos estar relacionadas.

Começando com o que parecerá ser apenas uma pequena brincadeira com palitos e plasticina, convidamos o leitor a deixar-se envolver por estas criaturas míticas a que os matemáticos chamam de grupos, anéis ou corpos.

1. Grupos

Suponhamos que o leitor tem à sua disposição plasticina e uma caixa de palitos, possivelmente imaginários. Com estes materiais podemos formar um quadrado: quatro bolinhas de plasticina dispostas em cima de uma mesa de forma apropriada são suficientes. Se cada vértice do quadrado tiver uma cor ou número diferente, podemos distingui-los uns dos outros: para simplificar, consideremos os vértices 1, 2, 3 e 4. De quantas formas diferentes podemos numerar os quatro vértices, assumindo que as posições são fixas? O leitor com alguns conhecimentos de combinatória (ou muita vontade de brincar com a plasticina) dirá que são $24 = 4 \times 3 \times 2 \times 1 = 4!$.

Porque não usar os palitos para formar as arestas do quadrado? Temos agora um quadrado de palitos e plasticina, com quatro vértices diferentes, mas que não podem ser trocados de qualquer forma sem separar a plasticina dos palitos. De quantas formas podemos agora permutar os quatro vértices? Podemos rodar o quadrado 90º, 180º ou 270º, convencionando que rodamos o quadrado no sentido dos ponteiros do relógio.[1] Podemos também rodar o quadrado perpendicularmente à mesa, trocando os vértices de cima com os de baixo ou os da direita com os da esquerda. Para além disto, podemos combinar alguns destes movimentos. Naturalmente, deixar o quadrado fixo também é uma permutação válida. Quantas são agora as possíveis posições do quadrado?



Estes diferentes movimentos do nosso quadrado de plasticina e palitos ilustram as simetrias do quadrado: são as transformações do conjunto $\{1, 2, 3, 4\}$ que preservam as adjacências iniciais,[2] ou seja, as permutações dos elementos do conjunto que

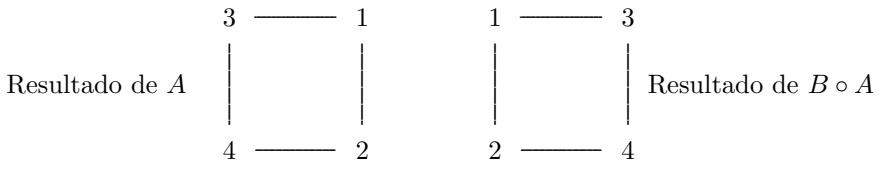
Key words and phrases. Grupo, Anel, Corpo, Corpo Finito, Homomorfismo, Quociente, Relação de equivalência, Característica.

[1] Rodar no sentido contrário não acrescenta novos movimentos: rodar 90º no sentido dos ponteiros do relógio ou 270º no sentido contrário produz o mesmo efeito, por exemplo.

[2] Ou do conjunto {Amarelo, Azul, Verde, Vermelho}, por exemplo, se foram estes os nomes escolhidos para os vértices.

correspondem a mudar a posição do quadrado sem separar os palitos da plasticina. Assim, se o vértice 1 estava inicialmente ligado aos vértices 2 e 3, só são permitidas transformações que mantêm o vértice 1 ligado aos vértices 2 e 3.

No conjunto destas transformações (que o leitor mais curioso já concluiu entretanto serem oito) definimos uma operação de composição: dadas duas simetrias A e B, a composição de A com B, que escrevemos $B \circ A$,[3] é a permutação que corresponde a primeiro aplicar A e depois aplicar B. Assim, se A for a rotação de 90^o no sentido dos ponteiros do relógio e B a reflexão no eixo vertical (que troca os vértices da direita com os da esquerda), como será a posição dos vértices com $B \circ A$?



Cada uma destas permutações do conjunto $\{1, 2, 3, 4\}$ é um dos *elementos* do *grupo* das simetrias do quadrado. Note-se que os elementos do grupo, neste caso, não são 1, 2, 3 e 4, mas algumas das permutações destes quatro números. Mas afinal o que é um grupo?

Para definir um grupo, começamos com um conjunto (que os matemáticos chamam de *suporte* do grupo), cujos elementos serão os elementos do grupo,[4] e definimos uma operação entre cada dois elementos do grupo, que deve, naturalmente, seguir algumas regras e estar definida para todos os elementos do grupo. Uma operação não é mais do que uma regra que nos diz que elemento do grupo obtemos se operarmos um dado elemento A com um dado elemento B. O nome da operação não é realmente importante, sendo frequente o uso de notação familiar ao leitor, como "+"ou "×", o que não significa forçosamente que sejam as usuais operações de soma e multiplicação de números reais. Geralmente a ordem pela qual operamos os elementos do grupo é importante, como o leitor poderá constatar facilmente se tentar calcular $A \circ B$ e $B \circ A$ na situação atrás descrita para as simetrias do quadrado. Para a explicação que se segue não vamos usar nenhum símbolo, escrevendo expressões como AB para o resultado de operar A com B. É usual referirmo-nos ao conjunto dos elementos como sendo o grupo, se bem que numa definição rigorosa o grupo é o conjunto juntamente com a operação. Iremos frequentemente fazer este pequeno abuso de linguagem, que não deve confundir o leitor.

E quais são as regras que essa operação deve verificar? Deve ser associativa, no sentido em que para cada A, B, C elementos do grupo, operar primeiro A com B e depois operar à direita com C, que escrevemos do modo usual como $(AB)C$, deve ser o mesmo que $A(BC)$. Deve existir um *elemento neutro* no grupo, ou seja, um elemento e (que ao longo deste artigo vamos sempre designar por esta letra) que operado tanto à esquerda como à direita com qualquer elemento A "não faz nada", isto é, $Ae = eA = A$. Por último, todos os elementos A do grupo têm um *inverso*, ou seja, para cada A existe um B tal que $AB = BA = e$. Na verdade, se A tem um inverso então este é único (porquê?), pelo que é usual usar-se a notação A^{-1} ou $-A$ para designar o inverso do elemento A. No que se segue, usaremos a notação

[3]O leitor não deve permitir que esta notação cause confusão: começamos pelas simetrias mais à direita, do modo semelhante à notação que usamos para a composição de funções $f \circ g(x) = f(g(x))$.

[4]No exemplo que demos do quadrado, o conjunto de suporte será o conjunto das *permutações* de $1, 2, 3, 4$ que verificam as restrições que explicámos, ou seja, aquelas que correspondem a transformações do quadrado de palitos e plasticina sem separar os dois materiais. Que o leitor não se confunda: não é o conjunto dos vértices!

A^{-1}, já que a notação $-A$ só se costuma usar quando a operação é designada pelo símbolo $+$, caso em que usamos o termo *simétrico* em vez de *inverso*.

O leitor poderá agora divertir-se a verificar que de facto as simetrias do quadrado com a operação de composição verificam todas estas restrições. Um bom exercício será procurar o inverso de cada elemento. Que outros grupos são familiares ao leitor?

O conjunto dos números inteiros com a operação usual de soma é um exemplo de um grupo, cujo elemento neutro é 0. No entanto, se considerarmos apenas os inteiros não-negativos, já não estamos a falar de um grupo, já que só o elemento 0 tem inverso: -1 seria o inverso de 1, por exemplo, mas não é um elemento dos inteiros não-negativos! Também os números reais distintos de 0 formam um grupo com a operação de multiplicação, com elemento neutro 1.

Um grupo pode ter algumas propriedades adicionais, não necessárias para ser um grupo, mas interessantes de estudar, como ser comutativo,[5] o que significa que o resultado da operação não depende da ordem pela qual se operam os elementos, sendo $AB = BA$ para quaisquer dois elementos do grupo escolhidos. Em honra ao matemático norueguês Niels Abel,[6] que na sua curta vida provou alguns importantes resultados em Teoria de Grupos, é comum usar-se a designação de *grupo abeliano* em vez de *grupo comutativo*.

Os exemplos atrás, à excepção do caso das simetrias do quadrado, são todos casos de grupos abelianos. Podemos considerar grupos de simetrias de outros polígonos regulares, de modo semelhante ao que fizemos para o quadrado. Para as simetrias de um polígono regular com n lados, temos n reflexões e n rotações (quais serão?), tendo-se assim um grupo com $2n$ elementos que não é comutativo. O leitor poderá agora entreter-se a procurar elementos cuja composição dependa da ordem da operação.

Falámos atrás de permutações. Dado um conjunto de n elementos, por exemplo $\{1, \ldots, n\}$, podemos pensar no conjunto de todas as permutações dos elementos do conjunto, ou seja, de todas as formas de trocar os elementos entre si. Neste conjunto com $n!$ elementos podemos considerar a operação de composição de permutações, ou seja, a operação que dadas duas permutações devolve a permutação que corresponde a aplicar as duas permutações de seguida, obtendo assim um grupo que os matemáticos designam por S_n.

Qual é a utilidade do estudo dos grupos? A grande maioria dos objectos matemáticos mais estudados, em várias áreas que o leitor pensará estarem bem longínquas da Álgebra, têm por base uma estrutura de grupo. É aliás muito comum em Matemática o estudo de objectos deste tipo: um conjunto com uma estrutura adicional, neste caso uma operação binária (entre dois elementos). Há várias perguntas naturais de fazer quando se estuda este tipo de objectos. Quantos grupos existem com um determinado número de elementos? E se o número de elementos for infinito? Será que podemos definir grupos mais pequenos com alguns dos elementos de um grupo? Será que podemos definir funções entre grupos diferentes que preservem de alguma forma a estrutura de grupo, mantendo alguma relação entre as operações definidas nos dois grupos?

2. Grupos: Homomorfismos, subgrupos e quocientes

Comecemos pela última pergunta. Dados dois grupos, digamos G e H, chamamos *homomorfismo* de grupos a uma função f de G para H que preserva a estrutura de grupo. Por preservar a estrutura de grupo entendemos preservar a operação, do seguinte modo: para cada dois elementos g_1, g_2 de G, a função f deve ser tal que

[5] E nesse caso dizemos que a operação é comutativa.

[6] Niels Henrik Abel, 1802-1829.

$f(g_1)f(g_2) = f(g_1g_2)$. Atenção: usámos aqui a mesma notação (escrever os elementos justapostos) para designar as duas operações, possivelmente bem diferentes, em G (no lado direito da igualdade) e em H (no lado esquerdo). Por vezes o único homomorfismo entre dois grupos é a função constante igual ao elemento neutro no grupo de chegada. Conhecer quais os possíveis homomorfismos entre dois grupos é uma das informações mais importantes que podemos obter sobre as relações entre esses dois grupos.

Não se pode falar em homomorfismos sem referir o *núcleo* e a *imagem* do homomorfismo. A imagem de f, tal como para funções, é simplesmente o conjunto dos elementos da forma $f(g)$, para algum g no grupo de partida. O núcleo é o conjunto dos g tais que $f(g) = e$. Estes dois conjuntos têm algumas propriedades importantes, pelo que voltaremos a falar deles mais tarde, escrevendo $Im\, f$ para a imagem e $ker\, f$ para o núcleo.

Um tipo especial destas funções é o chamado *isomorfismo*, um homomorfismo que é também uma função bijectiva, ou seja, tal que cada elemento do grupo de chegada H corresponde a um e só um elemento do grupo de partida G. Dizemos que dois grupos são *isomorfos* se existir um isomorfismo entre eles. Ao identificar cada elemento de um dos grupos com um e só um elemento do outro de modo a preservar, de certo modo, a operação, estamos na verdade a dar um nome novo à operação e a cada elemento, sem alterar de modo algum a estrutura do grupo. Assim, os dois são, de certo modo, *o mesmo* grupo. Ao tentar classificar os grupos com uma certa *ordem* (número de elementos), basta-nos assim estudar os que existem *a menos de isomorfismo*, isto é, considerando grupos isomorfos como sendo o mesmo grupo.

Falemos agora sobre os *subgrupos* de um grupo: subconjuntos dos elementos de um grupo que continuam a verificar as regras de um grupo para a operação originalmente definida, com o mesmo elemento neutro. O grupo dos números inteiros com a operação de soma é um subgrupo do grupo dos números reais com a mesma operação. O grupo das simetrias do quadrado, cujos elementos podemos ver como permutações dos vértices (que podemos imaginar serem $1, 2, 3, 4$), como já referimos, é um subgrupo do grupo S_4 das permutações de 4 elementos. Em geral, o grupo D_n das simetrias de um polígono regular com n lados é um subgrupo do grupo S_n das permutações de n elementos.

Os mais importantes subgrupos de um grupo são os subgrupos *normais*, que verificam uma propriedade que à primeira vista poderá parecer apenas uma restrição técnica mas que é na verdade muitíssimo importante: um subgrupo N de um grupo G é normal quando para cada elemento n de N e cada elemento g em G se tem que gng^{-1} ainda é um elemento de N. O subgrupo constituído só pela identidade e o grupo inteiro são sempre subgrupos normais (porquê?), que dizemos serem os subgrupos normais triviais, sendo os restantes designados de não-triviais. O leitor mais atento poderá notar que para os grupos abelianos, todos os subgrupos são normais (porquê?).

Porque é que esta propriedade é importante? Ao estudar um certo tipo de objecto matemático é importante encontrar formas de criar novos objectos do mesmo tipo fazendo construções com objectos já conhecidos, sendo que uma das formas mais frequentes de o fazer é a formação de *quocientes*. Mas para introduzir esta construção precisamos primeiro de nos familiarizarmos com a ideia de *relação de equivalência*.

E o que é uma relação de equivalência? Começamos com um conjunto onde introduzimos uma *relação* entre alguns pares de elementos. Uma forma mais rigorosa de ver uma relação será como um conjunto com alguns pares (ordenados!) de elementos do conjunto original. Para que a relação seja de equivalência deve seguir algumas regras: deve ser reflexiva, simétrica e transitiva. Ser *reflexiva* siginifica

que todo o elemento x do conjunto está em relação com ele próprio, o que podemos escrever como xRx se designarmos a relação por R. Ser *simétrica* significa que sempre que um elemento x está em relação com y, também y está em relação com x, ou seja, xRy implica yRx. A *transitividade* poderá ser descrita infantilmente por "o amigo do meu amigo é meu amigo também": se xRy e yRz, então xRz.

Sempre que temos uma relação de equivalência podemos identificar *classes de equivalência*: a classe de equivalência de um elemento x é o conjunto de todos os elementos que estão em relação com x. Um facto importante sobre as relações de equivalência (e que se relaciona directamente com as propriedades descritas atrás) é que todos os elementos do conjunto estão em alguma classe de equivalência (possivelmente só com um elemento, possivelmente com muitos) e não há nenhum elemento que esteja em duas classes de equivalência distintas, pelo que dizemos que as classes de equivalência formam uma *partição* do conjunto. É usual identificarmos cada classe de equivalência com um elemento só. Designamos o novo conjunto (cujos elementos são as classes de equivalência) como o *quociente* do conjunto original pela relação de equivalência considerada.

A usual relação de igualdade é uma relação de equivalência. Pensando no conjunto dos reais, por exemplo, com a relação de igualdade, ou seja, com a e b equivalentes exactamente quando $a = b$, as classes de equivalência são todas conjuntos com um só elemento, uma para cada número real. O conjunto $\{1\}$, por exemplo, é uma classe de equivalência.

No conjunto de todos os matemáticos podemos considerar uma relação de equivalência dada pelas datas de aniversário: dois matemáticos estão na mesma classe de equivalência se fazem anos no mesmo dia do ano. À partida deveremos ter 366 classes de equivalência, possivelmente com tamanhos diferentes.

Podemos agora falar em quocientes de grupos. Dado um grupo, definimos quocientes considerando uma relação de equivalência especial, relacionada com um dado subgrupo. Por razões que não iremos explicar aqui em detalhe, essa relação de equivalência (que iremos descrever em seguida) produz um novo grupo quando o subgrupo considerado é um subgrupo *normal*, e apenas nesse caso, daí a importância destes subgrupos. Fixando um grupo G e um certo subgrupo normal H, a relação é a seguinte: dois elementos g_1 e g_2 de G estão em relação sempre que existir algum elemento h em H tal que $g_1 h = g_2$. Para quem vê isto pela primeira vez, esta definição pode parecer algo arbitrária, mas relendo a definição acima de subgrupos normais o leitor deverá convencer-se que tal não é caso e que um estudo mais profundo do assunto poderá prová-lo. Usamos a notação G/H para indicar o grupo quociente de G por H.

Considerando o conjunto das classes de equivalência, identificando todos os elementos da mesma classe como um só elemento, definimos uma operação neste novo conjunto do seguinte modo: se representarmos a classe de equivalência do elemento g do grupo original G por $[g]$, temos $[g_1][g_2] = [g_1 g_2]$ para cada g_1, g_2 em G. O leitor poderá tentar provar que esta definição não depende dos representantes escolhidos, ou seja, que se escolhermos elementos g'_1, g'_2 na mesma classe de equivalência (em relação com) g_1, g_2, respectivamente, a classe de equivalência resultante do produto atrás é a mesma. Pode-se ainda provar que o elemento neutro do grupo resultante é precisamente $[e]$.

Com esta definição de quociente temos uma forma adicional de obter grupos, cuja importância ficará clara para quem se aventure num estudo mais completo da Teoria de Grupos.

Ao estudar um certo grupo, é importante conhecer coisas como quais são os seus subgrupos ou quantos elementos pode um subgrupo ter. O que é que podemos dizer sobre a relação entre a ordem de um subgrupo H e a do grupo G? No caso em que

G é finito, a ordem G é sempre um múltiplo da ordem de H. Mais ainda: no caso de H ser um subgrupo normal,[7] representando a ordem do grupo quociente de G por H por $[G : H]$, o famoso Teorema de Lagrange diz-nos que $|G| = [G : H]\,|H|$. Este facto é muito útil quando se estudam os subgrupos de um grupo G.

Está na hora de revisitar o núcleo e a imagem de um homomorfismo: seja então f um homomorfismo de G para H. O leitor mais corajoso poderá aventurar-se a demonstrar que a imagem de f é um subgrupo de H e que o núcleo de f é um subgrupo de G. Mais ainda, o núcleo de f é um subgrupo normal de G, pelo que faz sentido falar no grupo quociente $G/ker\, f$. O famoso *Primeiro Teorema do Isomorfismo* clarifica a relação entre o núcleo, a imagem e o grupo original: o grupo $G/ker\, f$ é isomorfo ao grupo $Im\, f$.

Encorajamos o leitor a procurar todos os grupos[8] com um certo número de elementos n. Como fazer tal coisa? Uma forma mais primitiva será tentar preencher uma tabuada para o grupo: uma tabela $n \times n$ com uma coluna e uma linha correspondentes a cada elemento do grupo, de modo a que na posição (i, j) se encontre o resultado do produto dos dois elementos correspondentes. Ao experimentar, rapidamente o leitor vai descobrir que é um pouco como preencher um *sudoku*, já que nenhum elemento se repete duas vezes na mesma linha nem duas vezes na mesma coluna. Não é por acaso! Imaginemos que a, b, c são elementos do grupo tais que $ab = ac$. Multiplicando ambos os lados da equação por a^{-1}, obtemos $b = c$, concluindo que na linha correspondente a a só na coluna correspondente a b teremos ab. Por exemplo, podemos obter uma tabuada para o único grupo com 2 elementos:

	e	a
e	e	a
a	a	e

Como sabemos que este é o único grupo com dois elementos? Fixando que e é o elemento neutro, sabemos os resultados de todos os produtos que envolvem e, ficando apenas aa por calcular. Mas pelo que vimos atrás, só há uma forma de preencher a tabela, conhecendo-se o resto da linha/coluna: só podemos ter $aa = e$. Ficámos então a saber que só existe, a menos de isomorfismo, um único grupo com dois elementos.

Claro está que o problema deste método é que rapidamente se torna impraticável tentar preencher todas as possíveis tabelas (quando n cresce, $n \times n$ cresce bem mais rapidamente!). Conhecer todos os grupos com uma dada ordem n seria útil, fazendo-se uma classificação de todos os grupos, mas o problema é de facto bastante complicado. De certo modo, a classificação realmente importante é a dos grupos finitos *simples*, que são grupos que não têm subgrupos normais não-triviais. A razão da importância destes grupos é que de certo modo todos os grupos finitos se podem construir à custa destes, pelo que uma classificação dos grupos finitos simples é a melhor coisa que se poderá pedir para a classificação de todos os grupos finitos. No entanto, a classificação dos grupos finitos simples só foi terminada em 2004, sendo que em 1832 já se conheciam grupos finitos simples.

A demora poderá ser explicada pelo seguinte: há algumas grandes famílias de grupos às quais pertencem quase todos os grupos finitos, agrupados de acordo com algumas propriedades importantes, mas há 26 grupos à parte que não é possível encaixar em nenhuma das outras famílias. O maior desses grupos, conhecido como o Monstro, tem 808017424794512875886459904961710757005754368000000000 elementos!

[7]Na verdade, não é necessário que H seja um subgrupo normal para que $[G : H]$ faça sentido, mas para falar disso precisaríamos de uma discussão mais longa sobre a relação de equivalência com a qual construímos o grupo quociente.

[8]Aqui queremos sempre dizer "a menos de isomorfismo", se bem que omitimos a expressão.

Para quê classificar todos os grupos finitos simples? Qual é a utilidade de conhecer um grupo com mais de 8×10^{53} elementos?[9] Os grupos aparecem naturalmente em várias áreas dentro e fora da Matemática: facilmente o leitor mais atento encontrará algumas aplicações úteis. De facto, a Teoria de Grupos tem aplicações espantosas na Química e na Física, estando relacionada com física de partículas ou permitindo prever os comportamentos de alguns cristais.

3. Anéis

O leitor mais impaciente pergunta-se por esta altura porque não considerar várias operações em vez de só uma. Claro está que considerar 100 operações ao mesmo tempo pode tornar-se algo complicado, mas duas parece ser uma quantidade razoável. Está então na hora de nos aventurarmos no estudo dos anéis, juntando uma nova operação ao nosso grupo.

Há várias definições alternativas de anel, umas mais restritivas que outras, sendo que em áreas diferentes o conceito de anel pode ser ligeiramente diferente. A opção que apresentamos aqui será possivelmente a mais comum e, esperemos, a mais acessível para o leitor, mas incentivamos a leitura de alguns dos livros da bibliografia com definições ligeiramente diferentes.

Consideremos então um grupo abeliano A, com uma operação a que chamaremos adição[10] e que representaremos pelo símbolo $+$, com um elemento neutro que representaremos por 0 e que é usualmente designado de *zero* do anel. Os inversos para esta operação são usualmente indicados na sugestiva forma $-a$, sendo usual escrever-se expressões como $a - b$ em vez de $a + (-b)$. Definimos uma outra operação, que designaremos por multiplicação e representaremos pelo símbolo $\times$, que deve ser igualmente associativa e para a qual deverá existir um elemento neutro também, que representaremos por 1 e que é usualmente designado por *um* ou *identidade* do anel. A multiplicação deve ser ainda *distributiva* em relação à adição, o que significa exactamente o que o nome sugere: para cada a, b, c em A, tem-se $a \times (b + c) = a \times b + a \times c$ e $(a + b) \times c = a \times c + b \times c$. É ainda usual exigir que 0 e 1 sejam elementos distintos. Ao conjunto A com estas duas operações chamamos *anel*. Para tornar a notação mais leve, vamos suprimir o símbolo "$\times$", justanpondo os elementos.

As possibilidades para propriedades adicionais que o anel pode ter são agora várias, e o leitor poderá facilmente imaginar quais serão. Se a multiplicação for comutativa, dizemos que o anel é comutativo.[11] Um anel comutativo sem *divisores de zero* (elementos a, b diferentes de 0 mas tais que $ab = 0$)[12] diz-se um *domínio integral*. Se adicionalmente todos os elementos distintos de 0 tiverem um inverso para a multiplicação,[13] o anel diz-se um *corpo*, e neste caso o leitor mais curioso poderá tentar verificar que o conjunto $A \setminus \{0\}$ com a operação de multiplicação é também um grupo abeliano.

Do mesmo modo que para os grupos, podemos definir *subanel*: um subconjunto do anel que é também um anel para as mesmas operações e com o mesmo zero e a mesma identidade. No entanto, não é este o tipo de subconjuntos mais importante no caso dos anéis, mas sim os *ideais* do anel. Um ideal é um subgrupo do *grupo aditivo* (isto é, do grupo formado por A com a operação de adição) tal que quando

[9] Para além de ser inegavelmente divertido.

[10] Por razões históricas e também porque os exemplos mais simples se relacionam com a usual adição de reais.

[11] A Álgebra Comutativa é a área da Matemática que estuda este tipo de anéis, sendo que num livro da área é usual designá-los apenas por Anéis.

[12] Mais à frente vamos ver alguns exemplos.

[13] Claro está que aqui queremos dizer que para cada a existe um b tal que $a \times b = b \times a = 1$.

multiplicamos elementos do ideal por elementos do anel obtemos elementos do ideal, quer a multiplicação seja feita à esquerda quer seja feita à direita.[14]

O conjunto $\mathbb{R}$ dos números reais com as operações de soma e multiplicação usuais formam um corpo, bem como o conjunto $\mathbb{C}$ dos números complexos com as mesmas operações (porquê?). O conjunto dos números inteiros forma um subanel dos anteriores, sendo que $\mathbb{Z}$ é um domínio integral mas não é um corpo, visto que o inverso de 2, por exemplo, seria $\frac{1}{2}$, que não é um número inteiro. Os exemplos mais comuns de anéis não comutativos já serão possivelmente desconhecidos do leitor, como os quaterniões ou o anel das matrizes 2×2 de entradas reais com as operações usuais de matrizes.

Em qualquer anel, o conjunto $\{0\}$ e o anel inteiro são sempre ideais (porquê?). Dizemos que estes são os *ideais triviais* do anel, por razões óbvias. Como serão os ideais de um corpo? Como vimos, num corpo todos os elementos têm inverso, pelo que se a é elemento não-nulo de um dado ideal, então por definição $a^{-1}a = 1$ também terá de ser elemento do ideal, o que repetindo o raciocínio nos leva a concluir que para qualquer elemento b do corpo, $b \times 1 = b$ também terá de pertencer ao ideal. Assim, um corpo tem apenas dois ideais, o ideal nulo e o corpo todo. Mais ainda: os corpos são os únicos anéis com esta propriedade, já que a existência de um elemento não-invertível diferente de 0 no anel nos leva sempre a encontrar um ideal não-trivial.[15]

4. Anéis: Homomorfismos e quocientes

Será que podemos estender a definição de homomorfismo de modo a preservar a operação de multiplicação também? Claro: dizemos que uma função f entre os anéis A e B é um homomorfismo de anéis se $f(1) = 1$ e se para cada a, b em A se tem $f(a + b) = f(a) + f(b)$ e $f(ab) = f(a)f(b)$. O leitor deve acautelar-se: atrás designámos por 1 as duas identidades distintas de A e B e usámos também os mesmo símbolos para as operações de adição e multiplicação nos dois anéis, apesar de serem operações diferentes, sendo esta opção comum na literatura matemática por tornar a notação mais leve.

E quanto aos quocientes? No caso dos anéis, fazemos quocientes do anel por ideais.[16] Neste caso, a relação de equivalência considerada é a seguinte: dados um anel A e um ideal I, os elementos a, b de A são equivalentes caso $b - a$ seja um elemento do ideal I. Tal como para grupos, consideramos cada classe de equivalência como um só elemento e definimos as operações de soma e de multiplicação de duas classes de equivalência através dos representantes das classes, obtendo assim um novo anel. Assim, se representarmos a classe de equivalência do elemento a por $[a]$, definimos $[a] + [b] = [a + b]$ e $[a][b] = [ab]$. O zero do anel quociente é $[0]$ e a identidade é $[1]$. Mais uma vez, desafiamos o leitor a provar que esta definição não depende dos representantes escolhidos. De forma semelhante ao que fazemos para

[14]Por vezes definem-se também *ideais esquerdos* e *ideais direitos*, mas não o faremos neste artigo.

[15]De facto, dado um elemento no anel podemos sempre encontrar o ideal *gerado* por ele, que é o ideal mais pequeno que contém esse elemento e que corresponde a tomar todos os produtos desse elemento por elementos do anel. Porquê é que isto forma um ideal? Se o elemento for não-invertível, não há como obter 1 tomando apenas produtos do nosso elemento inicial por outros elementos do anel. A ideia pode ser estendida a conjuntos de elementos, encontrando-se o menor ideal que os contém a todos.

[16]Assim sendo, os ideais são o análogo dos subrupos normais, se bem que da forma como definimos anel e ideal temos que nenhum ideal não-trivial é um subanel. De facto, para ser um subanel o ideal teria de conter a identidade, o que implicaria que o ideal era na verdade um dos ideais triviais.

grupos, denotamos o anel quociente de A pelo ideal I por A/I. Algumas propriedades do anel original passam para o quociente: por exemplo, se o anel original for comutativo, o quociente também será um anel comutativo (porquê?). De referir que há ainda um análogo do Primeiro Teorema do Isomorfismo para anéis.

Quais serão os ideais do anel $\mathbb{Z}$ dos números inteiros? Os números pares são um exemplo, bem como o conjunto dos inteiros múltiplos de um inteiro n fixo. Aliás, estes são os únicos ideais de $\mathbb{Z}$. De facto, observe-se que se I é um ideal e n é um elemento do ideal, então multiplicando n por qualquer inteiro obtemos, por definição, outro elemento do ideal, pelo que todos os múltiplos de n, pelo menos, deverão pertencer ao ideal. Desafio para o leitor mais corajoso: como concluir que todos os ideais de $\mathbb{Z}$ são precisamente desta forma (o conjunto dos múltiplos de um certo inteiro)?

Um desafio mais interessante será estudar os quocientes que podemos obter. Fixemos então um dado ideal, o ideal dos múltiplos de n, que se escreve usualmente de forma sugestiva como $n\mathbb{Z}$. Quantos elementos tem o anel quociente $\mathbb{Z}/n\mathbb{Z}$? Sabemos que cada inteiro a se pode escrever na forma $a = nq + r$, onde q e r são inteiros, designados usualmente por quociente e resto da divisão de a por n, com $0 \leqslant r < n$. Se a e b estão na mesma classe de equivalência, isso significa, como vimos, que $b - a$ está no ideal, ou seja, que é um múltiplo de n, o que com algumas contas nos leva a concluir que os restos das divisões de a e b por n só podem ser o mesmo. De facto, a e b estão na mesma classe de equivalência se e só se os restos da divisão de a por n e de b por n são iguais. Assim, o número de elementos no anel quociente é igual ao número de restos possíveis: n. É usual usarem-se os representantes $0, \ldots, n-1$ para as classes de equivalência. Como se fazem contas nestes anéis? Do modo descrito acima para os anéis quociente: $[a] + [b] = [a + b]$ e $[a][b] = [ab]$. Aqui temos a facilidade adicional de estarmos habituados a encontrar restos de divisão de números inteiros, podendo usar-se como método fazer as contas nos inteiros e depois reduzir a restos entre 0 e $n - 1$.

Uma notação muito útil é a das congruências: escrevemos $a \equiv b \pmod{n}$ para indicar que $b - a$ é um múltiplo de n, ou seja, que o resto da divisão de a por n e de b por n são iguais, e dizemos que "a é congruente com b módulo n". Assim, $a \equiv b\,(mod\, n)$ é o mesmo que dizer que $[a] = [b]$.

Estes anéis $\mathbb{Z}/n\mathbb{Z}$ são muito importantes:[17] são anéis *finitos* e comutativos, relativamente simples de estudar. No caso de n ser um número composto podemos sempre encontrar divisores de zero: se $n = mk$, temos as classes $[m]$ e $[k]$ distintas de $[0]$ e tais que $[m][k] = [mk] = [0]$. No caso de n ser um número primo, $\mathbb{Z}/n\mathbb{Z}$ é um corpo, sendo estes anéis os exemplos mais simples de corpos finitos.

5. Corpos e Teoria de Galois

O estudo de corpos finitos é muito importante em áreas como Teoria de Números, Combinatória ou Teoria de Códigos. Quantos elementos pode um corpo finito ter? Para cada número primo p e cada inteiro n existe sempre um corpo com p^n elementos, sendo esse corpo único (a menos de isomorfismo). No entanto, para $n > 1$ a descrição destes anéis fica relativamente mais complicada, sendo usual representar-se por $\mathbb{F}_{p^n}$ o corpo finito com p^n elementos. Curiosamente, estes são os únicos corpos finitos.

Outra diferença importante entre estes anéis $\mathbb{Z}/n\mathbb{Z}$ e $\mathbb{Z}$ é a *característica*. A característica do anel A é o menor inteiro positivo m tal que $1 + \ldots + 1 = 0$, tendo a soma atrás m parcelas, caso tal m exista. Se tal m não existir, dizemos que o anel tem característica zero. Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ têm todos característica 0, enquanto

[17] Alguns autores usam antes a notação $\mathbb{Z}_n$. Porém, nalgumas áreas (com que o leitor se cruzará em alguns dos próximos artigos) esta notação é reservada para outro conceito.

que $\mathbb{Z}/n\mathbb{Z}$ tem característica n (porquê?). Há vários resultados importantes sobre corpos, por exemplo, que são diferentes conforme se trate de corpos de característica 0 ou positiva, havendo até por vezes distinções significativas entre característica 2 e os restantes corpos. Os exemplos podem ser enganadores: há corpos infinitos de característica positiva, se bem que menos familiares ao leitor. No entanto, não há corpos finitos de caracterítica 0: pode até demonstrar-se que a característica de um corpo finito é sempre um número primo.

Os corpos são de factos bichos muito peculiares, com uma estreita relação com grupos e raízes de polinómios. O leitor conhecerá a famosa fórmula resolvente para equações de segundo grau (que já era conhecida pelos babilónios) e talvez já tenha ouvido falar na existência de fórmulas resolventes para equações de terceiro e quarto grau (que só foram descobertas no século XVI). Mas saberá o leitor que não existe nenhuma fórmula resolvente para equações de grau superior?

Clarifiquemos primeiro o que queremos dizer com *fórmula resolvente*. Considerando um polinómio de grau 2 numa variável e com coeficientes reais, ou seja, algo como $ax^2 + bx + c$,[18] conhecemos uma fórmula explícita para as (duas!) *raízes*, também chamadas de *zeros*, deste polinómio, ou seja, os valores que x pode tomar para que se tenha $ax^2 + bx + c = 0$. Sabe-se também resolver o problema para expressões em que as potências de x podem chegar a x^3 ou x^4. Mas se o nosso polinómio tiver um grau superior, ou seja, se a expressão incluir algo como x^n para um $n > 4$, não existe nenhuma fórmula explícita, usando apenas operações simples (soma, subtracção, multiplicação, divisão e extracção de raízes) envolvendo os coeficientes do polinómio, para encontrar todos os zeros. Existem fórmulas resolventes para algumas equações específicas, como $x^5 - 2 = 0$, mas não uma fórmula geral para todas, como a que existe para equações de segundo grau. Para $x^5 - x + 1 = 0$, por exemplo, é impossível encontrar uma fórmula resolvente nos termos acima descritos. Porquê? O que é que isto tem a ver com corpos ou teoria de grupos?

Como é que se resolve um problema destes? Encontrar uma fórmula, se bem que potencialmente trabalhoso, parecerá talvez acessível. Mas como se demonstra que *não é possivel* encontrar uma fórmula resolvente para equações de grau superior? Abel[19] encontrou uma condição suficiente para que fosse possível encontrar uma fórmula resolvente para as raízes de um dado polinómio (de qualquer grau). Pouco depois, Galois[20] inventou o termo *grupo*, associou a cada polinómio um certo grupo e provou que certas propriedades desse grupo permitem decidir se existe ou não uma tal fórmula para as raízes do polinómio, resolvendo o problema.

Que grupo é esse? Dado um polinómio de grau n, sabemos dizer exactamente quantos números complexos são raíz do polinómio: n, se bem que é possível que alguns sejam repetidos. Se o polinómio que estamos a considerar tem coeficientes num certo corpo L, como $\mathbb{Q}$ ou $\mathbb{R}$, por exemplo, é possível encontrar o corpo mais pequeno F que contém essas n raízes e o corpo L, e que está contido em $\mathbb{C}$ no caso de L ser $\mathbb{Q}$ ou $\mathbb{R}$. Podemos encontrar esse corpo juntando a L as n raízes $r_1, \ldots, r_n$ do polinómio e todos os elementos necessários para garantir que o conjunto final seja um corpo, que serão expressões envolvendo somas e produtos das raízes $r_1, \ldots, r_n$ e dos elementos de L.[21] Tendo este corpo F, existem alguns isomorfismos f :

[18]Dizer que os coeficientes são reais é dizer que tomamos a, b, c com valores reais. O polinómio aqui considerado tem grau 2 porque a maior potência da variável que aparece é x^2.

[19]O mesmo Niels Abel já mencionado.

[20]Évariste Galois, 1811-1832, matemático francês. Algumas das suas mais importantes contribuições matemáticas foram escritas na noite anterior ao duelo que levaria à sua morte.

[21]Em geral, dado um conjunto de elementos de um certo corpo ou anel, podemos sempre definir o menor corpo ou anel que os contém, e que será formado da forma que acabámos de descrever. Por exemplo, considerando o corpo $\mathbb{Q}$ e o complexo $\sqrt{5}$, o menor corpo que contém $\mathbb{Q}$ e $\sqrt{5}$, designado por $\mathbb{Q}[\sqrt{5}]$, tem elementos da forma $a + b\sqrt{5}$ com a, b racionais.

$F \to F$ que enviam cada elemento de L nele próprio, ou seja, que *fixam* o corpo L. Pela forma como construímos F, todos esses isomorfismos enviam cada raíz r_i do polinómio que considerámos numa outra raíz, mas mantendo certas relações entre as raízes, precisamente por ser um isomorfismo de corpos. O conjunto destes isomorfismos forma um grupo com a operação de composição de funções usual, que chamamos o *grupo de Galois* do polinómio em causa. Também devido à estrutura de F, cada um destes isomorfismos fica unicamente determinado conhecendo-se a imagem de cada raíz. Assim, podemos pensar em cada um dos elementos do grupo de Galois como uma permutação das n raízes do polinómio, pelo que o grupo de Galois é um subgrupo do grupo S_n das permutações das n raízes.

Para exemplificar, tomemos o polinómio $x^4 - 5$, sendo $\mathbb{Q}$ o corpo L que vamos considerar. As quatro raízes complexas deste polinómio de quarto grau são $\sqrt[4]{5}$, $-\sqrt[4]{5}$, $\sqrt[4]{5}\imath$ e $-\sqrt[4]{5}\imath$. Como temos quatro raízes distintas, esperamos encontrar um subgrupo de S_4. Como saber qual? Que isomorfismos f podem estar no grupo de Galois? Poderíamos pensar em definir um isomorfismo para cada permutação destes quatro elementos, mas nem todas as permutações correspondem a isomorfismos válidos: por exemplo, sendo a uma das raízes, temos sempre $f(-a) = -f(a)$,[22] pelo que não poderíamos ter coisas como $f(\sqrt[4]{5}) = \sqrt[4]{5}$ e $f(-\sqrt[4]{5}) = \sqrt[4]{5}\imath$.

Há várias ferramentas úteis que podemos usar para descobrir qual é o grupo de Galois. Por exemplo, sempre que temos uma extensão de corpos, ou seja, um corpo L contido num outro corpo F, como é o caso, a operação de soma definida em F e a multiplicação por elementos de L definem em F uma estrutura de espaço vectorial.[23] Na verdade, a dimensão $[F : L]$ de F como espaço vectorial sobre L é exactamente a ordem do grupo de Galois que procuramos. Considerando alguns corpos intermédios, obtidos de forma semelhante ao que fazemos para obter F mas juntando apenas algumas das raízes, podemos tirar algumas conclusões sobre quanto pode ser $[F : L]$, já que a dimensão desses subcorpos de F como espaços vectoriais sobre L tem de dividir $[F : L]$, ou seja, a ordem do grupo de Galois. Além disto, sendo um subgrupo de S_4, sabemos também que não pode ter mais de $4! = 24$ elementos e que aliás a sua ordem tem de dividir 24, pelo Teorema de Lagrange que mencionámos atrás. Usando ideias deste tipo, podemos provar que o grupo de Galois que procuramos tem oito elementos e alguns cálculos adicionais[24] permitem-nos concluir que o grupo é na verdade D_4, o nosso grupo inicial das simetrias do quadrado.

O que é que isto tem a ver com a fórmula resolvente? O Teorema de Abel-Rufini é a resposta: uma equação é resolúvel, ou seja, é tal que podemos encontrar uma fórmula resolvente, se e só se o grupo de Galois correspondente é resolúvel. De facto, há polinómios de grau 5 cujo grupo de Galois não é resolúvel, daí que não exista fórmula resolvente para grau 5. E aqui regressamos à teoria de grupos: um grupo G é *resolúvel* se pode, de certa forma, ser construído a partir de grupos abelianos. Começamos por considerar um certo subgrupo normal muito especial, o *grupo derivado* de G, que é o menor subgrupo normal de G tal que o quociente de G por esse subgrupo é abeliano, e formamos uma certa cadeia de grupos tomando sucessivamente o grupo derivado do último grupo obtido, sendo os sucessivos quocientes grupos abelianos. O grupo G diz-se resolúvel quando o processo pára, ou

[22] Para verificar esta afirmação, o leitor deve recordar a definição de homomorfismo e notar que $f(0) = 0$.

[23] O leitor que já trabalhou com espaços vectorias mas apenas sobre os números reais pode pensar que na verdade esta estrutura de espaço vectorial em F é obtida exactamente da mesma maneira como damos ao corpo dos números complexos uma estrutura de espaço vectorial real.

[24] Há apenas cinco grupos com oito elementos (mais uma vez, a menos de isomorfismo), pelo que na verdade basta-nos estudar um pouco as relações entre os elementos para descobrir qual dos cinco é.

seja, quando é possível, após um certo número finito de passos, obter o grupo trivial. Assim, uma definição abstracta com grupos abelianos e quocientes de grupos permite-nos resolver um problema prático que atormentou matemáticos ao longo de séculos.

6. Álgebra

A Álgebra poderá ser descrita como o estudo de estruturas algébricas como estas de que aqui falámos. Seja qual for a estrutura algébrica em questão, o caminho a seguir é em geral semelhante ao que aqui fizemos. Há subestruturas dentro da estrutura que estamos a estudar que verificam a nossa definição inicial? Como definir funções entre objectos deste tipo que preservem a estrutura algébrica? Haverá uma ideia de quociente? Como classificar todas as estruturas deste tipo?

A maioria dos livros de Álgebra começa por introduzir definições bem rigorosas de grupo, anel, corpo ou outra estrutura algébrica, podendo deixar uma ideia errada sobre o aparecimento destes objectos. Primeiro apareceram as perguntas práticas e simples de formular, como a procura por fórmulas resolventes para equações polinomiais, e só bem depois apareceram as definições rigorosas, quando a prática já tinha deixado claro quais eram os objectos que interessava estudar. Há muito que os matemáticos trabalhavam com anéis e grupos e usavam algumas das suas propriedades antes do aparecimento de uma definição rigorosa. Assim, encorajamos o leitor a brincar com estes objectos, procurando exemplos ou tentando responder a algumas das nossas perguntas, até que os conceitos que definimos deixem de parecer construções artificiais e se tornem naturais.

As aplicações estendem-se bem para além da Matemática, chegando, tal como já referimos, a áreas tão diversas como a Química ou a Física de Partículas. Dentro da própria Matemática, as aplicações vão desde as perguntas mais simples de formular e que já atormentavam os antigos até aos tópicos mais modernos. Independentemente de tudo isto, há uma quantidade inesgotável de factos interessantes sobre estes objectos algébricos, de tal forma que foi quase impossível escolher os que melhor poderiam capturar a atenção do leitor. O melhor será que o leitor se sente, com palitos e plasticina ou só com a sua imaginação, e procure descobrir por si próprio algumas delas.

Bibliografia

Para uma leitura introdutória a estes e outros assuntos de Álgebra em português, aconselha-se [1], que tem muitos exemplos e exercícios, se bem que sem soluções. No entanto, a definição de anel seguida pelos autores é ligeiramente diferente da nossa, não exigindo que o anel tenha identidade. O mesmo se faz em [2], que também inclui uma lista bem longa de exercícios, mas talvez num estilo mais pesado para quem não está habituado a ler Matemática. Já [3] usa a mesma definição de anel que este artigo, se bem que num ritmo mais rápido que os anteriores. Para os interessados em teoria de Galois sugerimos [4] ou [5], sendo que [4] inclui um anexo sobre como se trabalhava naquilo que é agora Teoria de Galois antes das definições rigorosas ou das ferramentas de teoria de grupos. O último capítulo de [6] apresenta grupos de uma perspectiva um pouco diferente, focando-se em parte na relação com a física, sendo bastante interessante para quem só agora ouviu falar de grupos pela primeira vez.

Referências

[1] Manuel Ricou e Rui Loja Fernandes, *Introdução à Álgebra*, IST Press, 2004
[2] Hungerford, *Algebra*, Springer, 2000
[3] S. Lang, *Algebra*, Addison Wesley, 1971

[4] Rotman, *Galois Theory*, Second Edition, Springer, 1998
[5] Ian Stewart, *Galois Theory*, Third Edition, Chapman Hall / CRC, 2004
[6] Malcolm Lines, *Pense num número*, Gradiva, 1993