Aula 10

I Ordens de potências x^n

As próximas três proposições correspondem à Proposição 5 da secção 2.3 do livro, embora apresentadas de forma ligeiramente diferente e também com demonstrações diferentes.

§1. Proposição. *Seja G um grupo, $x \in G$ um elemento de ordem finita n, e seja d um divisor (positivo) de n. Então $|x^d| = n/d$.*

Demonstração. Uma vez que $(x^d)^{n/d} = x^n = 1$ temos $|x^d| \leq n/d$. Por outro lado, se $0 < k < n/d$ então $dk < n$, pelo que, se $(x^d)^k = 1$, ter-se-ia $x^{dk} = 1$ e portanto $|x| \leq dk < n$, uma contradição porque $|x| = n$. Portanto $|x^d| = n/d$. ∎

§2. Proposição. *Seja G um grupo, $x \in G$ um elemento de ordem finita n, $k \in \mathbb{Z}_{\geq 1}$ e $d = \mathrm{mdc}(k, n)$. Então $|x^k| = |x^d| = n/d$.*

Demonstração. Para demonstrar a igualdade $|x^k| = |x^d|$ vamos verificar que para qualquer $a \in \mathbb{Z}_{\geq 1}$ se tem a equivalência

$$(x^k)^a = 1 \iff (x^d)^a = 1,$$

ou seja,

$$x^{ka} = 1 \iff x^{da} = 1.$$

Uma vez que $d \mid k$, a condição da direita implica a da esquerda porque $da \mid ka$, portanto apenas falta demonstrar a implicação da esquerda para a direita. Assuma-se que $x^{ka} = 1$. Pelo lema de Bezout existem $r, s \in \mathbb{Z}$ tais que $d = rk + sn$, e portanto

$$x^{da} = x^{rka+sna} = (x^{ka})^r (x^n)^{sa} = 1^r 1^{sa} = 1.$$

Por fim, como $d \mid n$, obtém-se $|x^d| = n/d$ pela proposição anterior. ∎

§3. Proposição. *Seja G um grupo e $x \in G$ um elemento de ordem infinita. Então, para qualquer $k \neq 0$, a ordem de x^k é infinita.*

Demonstração. Suponha-se que $k \neq 0$ e x^k tem ordem finita n. Então $(x^k)^n = 1$, e portanto $|x| \leq kn$, uma contradição. Portanto $|x^k| = \infty$. ∎

O próximo corolário corresponde à alínea 2 da Proposição 6 da mesma secção.

§4. Corolário. *Seja $x \in G$ um elemento de um grupo tal que $|x| = n < \infty$, e $k \in \mathbb{Z}_{\geq 1}$. Então tem-se $\langle x^k \rangle = \langle x \rangle$ se e só se n e k forem primos entre si.*

Demonstração. Se $\mathrm{mdc}(k, n) = 1$ então $|x^k| = n$ pelas proposições anteriores, e portanto $|\langle x^k \rangle| = n$. Uma vez que $x^k \in \langle x \rangle$, então $\langle x^k \rangle \leq \langle x \rangle$, mas então os dois subgrupos são iguais porque têm a mesma ordem. Por outro lado, se $\langle x^k \rangle = \langle x \rangle$ então x^k tem ordem n porque gera um grupo de ordem n, e portanto, sendo $d = \mathrm{mdc}(k, n)$, tem-se

$$n/d = |x^k| = n,$$

ou seja, $d = 1$. ∎

§5. Corolário. *O grupo cíclico Z_n tem exactamente $\varphi(n)$ geradores cíclicos, em que φ é a função de Euler (i.e., existem $\varphi(n)$ elementos $x \in Z_n$ tais que Z_n é gerado por x). Em particular, se p for um número primo, Z_p tem exactamente $p - 1$ elementos de ordem p, cada um dos quais é um gerador cíclico.*

A próxima proposição corresponde à alínea 1 da Proposição 6 da secção 2.3 do livro:

§6. Proposição. *Seja $x \in G$ um elemento de um grupo tal que $|x| = \infty$, e seja $k \in \mathbb{Z}$. Então $\langle x \rangle = \langle x^k \rangle$ se e só se $k = -1$ ou $k = 1$.*

Demonstração. Exercício. ∎

II Subgrupos de grupos cíclicos

As proposições anteriores dão-nos vários candidatos a subgrupos de um grupo cíclico G, nomeadamente subgrupos gerados por potências x^k de um gerador x de G. Contudo, tais subgrupos são eles próprios cíclicos, e resta saber se pode haver outro tipo de subgrupo de G. O próximo teorema corresponde à alínea 1 do Teorema 7 da mesma secção e mostra que qualquer subgrupo de um grupo cíclico é ele próprio cíclico:

§7. Teorema. *Seja G um grupo cíclico (não trivial) gerado por $x \in G$, e $H \leq G$. Então, ou H é trivial ou é ciclicamente gerado por x^k em que k é o menor inteiro positivo tal que $x^k \in H$.*

Demonstração. Vamos assumir que H não é trivial e mostrar que é gerado por x^k. Primeiro vamos verificar que k está bem definido. Note-se que, por G não ser trivial, tem-se $x \neq 1$. Também por H não ser trivial, e porque todos os elementos de G são potências de x, existe pelo menos um inteiro positivo ℓ tal que $x^\ell \in H$, e portanto o conjunto de todos estes inteiros ℓ tem de facto um mínimo k. Seja $y = x^k$. Então todas as potências de y pertencem a H, e portanto $\langle y \rangle \leq H$. Para vermos que não há mais elementos de H para além destes, consideremos um elemento arbitrário $z \in H$. Uma vez que G é gerado por x existe $a \in \mathbb{Z}$ tal que $z = x^a$. Agora consideramos três casos:

- Se $a = 0$ então $z = 1 \in \langle y \rangle$.
- Se $a > 0$ defina-se $d = \text{mdc}(a, k)$. Sejam r e s inteiros tais que $d = ra + sk$. Então
$$x^d = (x^a)^r (x^k)^s \in H.$$
Logo, pela definição de k, tem de ter-se $k \leq d$, mas por outro lado $d \mid k$ e portanto $k = d$. Logo, conclui-se que $k \mid a$ e assim $x^a \in \langle y \rangle$.
- Falta ver o caso $a < 0$. Nesse caso $-a > 0$ e $x^{-a} \in H$, e portanto pelo caso anterior $x^{-a} \in \langle y \rangle$, concluindo-se que $x^a \in \langle y \rangle$.

Portanto H é o grupo cíclico $\langle y \rangle$. ∎

§8. Nota. A demonstração acima é semelhante à do livro, e trata de uma só vez tanto o caso de G ser um grupo finito ou infinito. Uma alternativa, no caso de G ser um grupo finito, é considerar o conjunto $A = H \setminus \{1\}$. Sendo H não trivial, A é não vazio e contém um número finito de elementos a_1, …, a_n ($n \geq 1$). Sendo G gerado por x existem então n inteiros positivos

$k_1, \ldots, k_n$ tais que $a_1 = x^{k_1}, \ldots, a_n = x^{k_n}$. Iterando o lema de Bezout conclui-se que existem inteiros $r_1, \ldots, r_n$ tais que o máximo divisor comum $d = \mathrm{mdc}(k_1, \ldots, k_n)$ é uma combinação linear

$$d = r_1 k_1 + \cdots + r_n k_n.$$

Então

$$x^d = (x^{k_1})^{r_1} \cdots (x^{k_n})^{r_n} = a_1^{r_1} \cdots a_n^{r_n} \in H.$$

Portanto x^d é assim um gerador cíclico de H. Além disso, evidentemente, d é o menor inteiro positivo tal que $x^d \in H$.

No caso de G ser infinito tem-se $G \cong \mathbb{Z}$ e a demonstração é muito semelhante à de §7, mas podemos substituir o grupo abstracto G pelo grupo dos inteiros $\mathbb{Z}$. Considere-se um isomorfismo fixo $h : G \to \mathbb{Z}$. Qualquer subgrupo $H \leq G$ corresponde, via h, a um subgrupo $K = h(H) \leq \mathbb{Z}$. Se H não for trivial também K não será, e portanto existe o menor inteiro positivo $n \in K$, sendo portanto $n\mathbb{Z} \leq K$. Por outro lado, dado qualquer $m \in K$ positivo, $d = \mathrm{mdc}(m, n)$ é uma combinação linear de m e n com coeficientes inteiros, a qual portanto pertence a K. Logo, tem de ter-se $d = n$, e portanto n divide m, assim mostrando que $K = n\mathbb{Z}$.

§9. Corolário. *O conjunto dos subgrupos de $\mathbb{Z}$ está em bijecção com o conjunto dos inteiros não negativos.*

Demonstração. Todos os subgrupos de $\mathbb{Z}$ são ciclicamente gerados por um número inteiro a e tem-se $\langle a \rangle = \langle -a \rangle = a\mathbb{Z}$. Por outro lado, para cada par de inteiros não negativos a e b, se $a \neq b$ então $\langle a \rangle \neq \langle b \rangle$. Assim conclui-se que há uma bijecção $a \mapsto \langle a \rangle$ entre o conjunto dos inteiros não negativos e o conjunto dos subgrupos de $\mathbb{Z}$. ∎

§10. Corolário. *O conjunto dos subgrupos não triviais de Z_n está em bijecção com o conjunto dos divisores de n.*

Demonstração. Cada divisor k de n gera um subgrupo $\langle x^k \rangle$, e os resultados anteriores permitem concluir que a correspondência $k \mapsto \langle x^k \rangle$ é uma bijecção, tal como descrito no enunciado. ∎

§11. Nota. Os dois corolários anteriores dizem-se resultados de *classificação*, pois cada um deles faz uma classificação precisa de uma colecção, nomeadamente de subgrupos, em termos de um conjunto de parâmetros: no primeiro caso os parâmetros são os inteiros não negativos; e no segundo são os divisores de n.

III Algumas propriedades relevantes

As notas anteriores usam um facto que vale a pena realçar, a respeito de qualquer subgrupo:

§12. Proposição. *Seja G um grupo, H um subgrupo de G, $x \in G$ e $m, n \in \mathbb{Z}_{\geq 1}$. Então $\{x^m, x^n\} \subset H$ se e só se $x^d \in H$, em que $d = \mathrm{mdc}(m, n)$. Mais geralmente, dados $n_1, \ldots, n_k \in \mathbb{Z}_{\geq 1}$ ($k \geq 1$), se $d = \mathrm{mdc}(n_1, \ldots, n_k)$ então*

$$\{x^{n_1}, \ldots, x^{n_k}\} \subset H \iff x^d \in H.$$

Demonstração. Tal como já várias vezes observámos acima, pelo lema de Bezout tem-se $d = rm + sn$ para inteiros r e s, pelo que

$$x^d = (x^m)^r (x^n)^s.$$

Logo, se x^m e x^n pertencem a H também x^d pertence a H. Por outro lado, como d divide m e n, tem-se que tanto x^m como x^n são potências de x^d, e portanto se x^d pertence a H também x^m e x^n pertencem. A segunda parte da proposição obtém-se iterando o lema de Bezout, pois $\mathrm{mdc}(n_1, \ldots, n_k) = \mathrm{mdc}(\mathrm{mdc}(n_1, \mathrm{mdc}(n_2, \ldots) \ldots)$, e por isso existem inteiros $r_1, \ldots, r_k$ tais que

$$d = r_1 n_1 + \cdots r_k n_k.$$

(Exercício: preencha os detalhes deste último argumento.) ∎

§13. Corolário. *Seja G um grupo e $x \in G$. Então $x^{n_1} = \cdots = x^{n_k} = 1$ para inteiros $n_i \in \mathbb{Z}_{\geq 1}$ ($k \geq 1$) se e só se $x^d = 1$, em que $d = \mathrm{mdc}(n_1, \ldots, n_k)$.*

Demonstração. Basta aplicar a proposição anterior ao subgrupo trivial $H = \{1\}$. ∎

§14. Corolário. *Seja G um grupo, $x \in G$ e $n \in \mathbb{Z}_{\geq 1}$ tais que $x^n = 1$. Então $|x|$ é um divisor de n.*

Demonstração. (Isto já tem sido usado nas aulas anteriores, embora sem ser justificado com cuidado.) Seja $d = \mathrm{mdc}(|x|, n)$. Em particular tem-se $d \leq |x|$. Então tem-se $x^d = 1$ (pois $x^{|x|} = x^n = 1$), e portanto $|x| \leq d$. Logo $d = |x|$, e portanto $|x| \mid n$. ∎

IV Exercícios

Na aula fizemos os seguintes exercícios:

§15. Exercício. Descreva o conjunto de todos os subgrupos de $\mathbb{Z}/12\mathbb{Z}$ juntamente com todas as inclusões entre esses subgrupos.

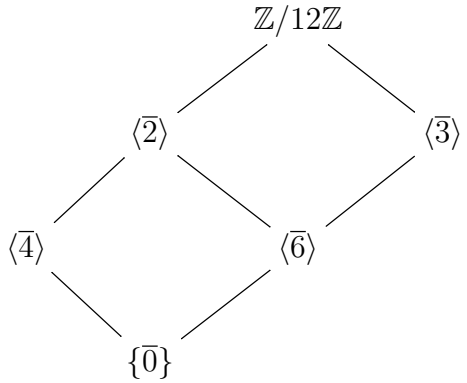
§16. Exercício. Descreva o conjunto de todos os subgrupos de

$$Z_{36} = \langle x \mid x^{36} = 1 \rangle$$

e todas as inclusões entre eles.

§17. Exercício. Descreva o conjunto de todos os subgrupos de Z_{30} e todas as inclusões entre eles.

§18. Solução de §15. Convencionando que cada segmento de recta da figura abaixo representa uma inclusão de baixo para cima, e lembrando que a relação de inclusão é transitiva, a resposta ao exercício é dada pelo diagrama seguinte:



Como se vê, existe exactamente um subgrupo não trivial por cada divisor de $12 = 2^2 \times 3$.