Subgrupos Cíclicos

Para simplificar os enunciados, vamos usar apenas a notação multiplicativa, deixando como exercício a formulação dos resultados na notação aditiva.

Dado um elemento $a \neq e$ de um grupo G, nos perguntamos da existência de um número natural m tal que $a^m = e$.

Se tal inteiro não existe diremos que a tem **ordem infinita**, escrevendo neste caso, $o(a) = \infty$.

Se existir tal inteiro, dizemos que a tem **ordem finita** e definimos a sua **ordem** como sendo o número natural

$$o(a) = \min\{m \in \mathbb{N}; \quad a^m = e\}.$$

Por exemplo, em qualquer grupo G tem-se que $o(e) = 1$ e que $o(a) = o(a^{-1})$, para todo $a \in G$.

Exemplo Seja U_6 o grupo multiplicativo das raízes sextas complexas da unidade. Ponhamos $\xi = \cos\frac{2\pi}{6} + i\,\mathrm{sen}\,\frac{2\pi}{6}$. Usando a fórmula de De Moivre, temos que ξ tem ordem 6, enquanto que $\xi^2 = \cos\frac{4\pi}{6} + i\,\mathrm{sen}\,\frac{4\pi}{6}$ tem ordem 3.

Exemplo O número racional 2 é um elemento de ordem infinita do grupo $(\mathbb{Q}^*, \cdot)$.

$$\langle 2\rangle = \{2^n;\ n \in \mathbb{Z}\} = \{\ldots, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \ldots\}.$$

O número inteiro 2 é um elemento de ordem infinita no grupo $(\mathbb{Z}, +)$.

$$\langle 2\rangle = \{2n;\ n \in \mathbb{Z}\} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}.$$

Mais geralmente, se $n \neq 0$, então $o(n) = \infty$ no grupo aditivo $\mathbb{Z}$.

Teorema $\langle a \rangle$ é finito se, e somente se, $o(a) < \infty$. Neste caso,

$$\langle a \rangle = \{e, a, \ldots, a^{o(a)-1}\},$$

onde esses elementos são distintos. Em particular, $|\langle a \rangle| = o(a)$.

Prova Suponha que $\langle a \rangle$ seja finito. Logo, na lista de elementos $a, a^2, a^3, \ldots$ devem ocorrer repetições e, portanto, existem $r, s \in \mathbb{N}$ com $r < s$ tais que $a^r = a^s$. Logo, pondo $m = s - r > 0$, temos que $a^m = e$, portanto, $o(a) < \infty$.

Reciprocamente, suponha que $o(a) < \infty$. Logo $a^{o(a)} = e$. Vamos provar que $\langle a \rangle = \{e, a, \ldots, a^{o(a)-1}\}$. De fato, é óbvia a inclusão: $\{e, a, \ldots, a^{o(a)-1}\} \subseteq \langle a \rangle$.

Por outro lado, Seja $b \in \langle a \rangle$, logo $b = a^s$ para algum $s \in \mathbb{Z}$. Pelo algoritmo da divisão de inteiros, temos que $s = o(a)q + r$, com $0 \leq r < o(a)$. Temos portanto que

$$a^s = a^{o(a)q+r} = (a^{o(a)})^q a^r = ea^r = a^r;$$

ou seja, para todo $s \in \mathbb{Z}$, tem-se que $a^s = a^r$, onde r é o resto da divisão de s por $o(a)$. Consequentemente, $a^s \in \{e, a, \ldots, a^{o(a)-1}\}$, provando assim a outra inclusão: $\langle a \rangle \subseteq \{e, a, \ldots, a^{o(a)-1}\}$.

Desse modo, provamos que se $o(a) < \infty$, então $\langle a \rangle$ é finito e

$$\langle a \rangle = \{e, a, \ldots, a^{o(a)-1}\}.$$

Só nos resta provar que $a^i \neq a^j$, se $i \neq j$ com $i, j = 0, 1, \ldots, o(a) - 1$. De fato, se $a^i = a^j$ com $j > i$, então $a^{j-i} = e$ com $0 < j - i < o(a)$, o que é uma contradição, tendo em vista a minimalidade de $o(a)$.

□

Proposição Sejam G um grupo e $a \in G$ com $o(a) < \infty$. Então $a^m = e$ se, e somente se, $o(a) \mid m$.

Prova Considere o conjunto

$$H = \{m \in \mathbb{Z};\ \ a^m = e\} \subseteq \mathbb{Z}.$$

Como $o(a) < \infty$, temos que $H \neq \{0\}$. Por outro lado, é fácil verificar que H é um subgrupo de $\mathbb{Z}$ e, portanto, ele é gerado pelo seu menor elemento positivo, logo $H = o(a)\mathbb{Z}$. Portanto, um inteiro m é tal que $a^m = e$ se, e somente se, $m \in H$, se, e somente se, ele é múltiplo de $o(a)$, o que prova o resultado.

□

Corolário Seja G um grupo finito e seja $a \in G$, então $a^{|G|} = e$.

Prova Pelo Teorema de Lagrange, temos que $|\langle a \rangle|$ $(= o(a))$ divide $|G|$ e, portanto, pela Proposição, temos que $a^{|G|} = e$.

□

Veremos a seguir como o resultado acima permite demonstrar de outro modo alguns teoremas da Teoria dos Números.

Pequeno Teorema de Fermat Seja p um número primo positivo. Para todo $a \in \mathbb{Z} \setminus p\mathbb{Z}$, tem-se que $a^{p-1} \equiv 1 \bmod p$.

Prova Como $\mathbb{Z}_p$ é um corpo, o grupo $(\mathbb{Z}_p{}^*, \cdot)$ tem $p-1$ elementos, logo para todo $a \in \mathbb{Z} \setminus p\mathbb{Z}$, temos que a classe residual $[a]$ de a módulo p é tal que $[a] \in \mathbb{Z}_p{}^*$ e, portanto, $[a]^{p-1} = [1]$, donde segue-se o resultado.

□

Teorema de Euler Seja n um inteiro natural. Se a é um inteiro tal que $(a, n) = 1$, então $a^{\Phi(n)} \equiv 1 \bmod n$.

Prova Veja a lista de exercícios.

Um grupo G é chamado de **grupo cíclico** se existir $a \in G$ tal que $G = \langle a \rangle$.

Exemplo $\mathbb{Z}$ é cíclico pois $\mathbb{Z} = \langle 1 \rangle = \{n1;\ n \in \mathbb{Z}\}$. Os grupos $\mathbb{Z}_n$ são cíclicos pois $\mathbb{Z}_n = \langle [1] \rangle$. Veremos mais adiante que, em algum sentido que será precisado oportunamente, esses são os únicos grupos cíclicos.

Outros exemplos de grupos cíclicos são os $(U_n, \cdot)$, onde U_n é o conjunto das raízes n-ésimas da unidade em $\mathbb{C}$ e a operação é o produto de números complexos (em algum sentido, U_n é o mesmo que $\mathbb{Z}_n$). Um gerador de U_n é uma raiz n-ésima **primitiva** da unidade.

Proposição Todo grupo cíclico é abeliano.

Prova De fato, se $G = \langle a \rangle$, então dois elementos quaisquer de G podem ser escritos sob a forma a^i e a^j com $i, j \in \mathbb{Z}$. Logo $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$.

□

Proposição Todo grupo de ordem prima é cíclico.

Prova De fato, se G é um grupo de ordem prima p, escolha $a \in G \setminus \{e\}$. Temos que $o(a) \neq 1$. Pelo Teorema de Lagrange temos que $o(a) \mid p$ e, portanto, $o(a) = p$. Segue-se então que $|\langle a \rangle| = |G|$ e, portanto, $G = \langle a \rangle$. □

O próximo resultado nos dirá qual é a ordem da potência de um elemento cuja ordem se conhece.

Proposição Seja G um grupo e seja a um seu elemento de ordem finita. Se $r \in \mathbb{Z}$, então $o(a^r) = \frac{o(a)}{(o(a),r)}$.

Prova Como $o(a^r) = o(a^{-r})$, sem perda de generalidade, podemos supor $r \geq 0$. Temos que $o(a^r)$ é o menor inteiro positivo n tal que $(a^r)^n = e$, ou seja, tal que $o(a) \mid rn$. Portanto, rn é o menor múltiplo comum de $o(a)$ e de r, ou seja, $rn = [o(a), r]$. Consequentemente,

$$o(a^r) = n = \frac{[o(a), r]}{r} = \frac{o(a) \cdot r}{(o(a), r)r} = \frac{o(a)}{(o(a), r)}.$$

□

Corolário Seja $a \in G$, com $o(a) = n$. Se $s \in \mathbb{N}$, então $\langle a^s \rangle = \langle a^{(n,s)} \rangle$.

Prova É imediato verificar que $\langle a^s \rangle \subseteq \langle a^{(n,s)} \rangle$. Portanto, os grupos $\langle a^s \rangle$ e $\langle a^{(n,s)} \rangle$ são iguais porque possuem mesmo número de elementos, pois temos

$$o(a^s) = \frac{n}{(n,s)} = \frac{n}{(n,(n,s))} = o(a^{(n,s)}).$$

□

Corolário Um grupo cíclico de ordem n tem $\Phi(n)$ geradores.

Prova Seja $G = \langle a \rangle$ de ordem n. Um elemento de $G \setminus \{e\}$ se escreve como a^s, onde $0 < s < n$. Logo a^s é gerador de G se, e somente se, $o(a^s) = n$, o que ocorre se, e somente se, quando $n = \frac{n}{(s,n)}$, ou seja, quando $(s,n) = 1$. Portanto, G possui $\Phi(n)$ geradores.

□

Proposição Seja $G = \langle a \rangle$ um grupo cíclico de ordem n. Se m é um número natural que divide n, então existe um único subgrupo de G de ordem m e este é dado por $H = \langle a^{\frac{n}{m}} \rangle$.

Prova Considere $\langle a^{\frac{n}{m}} \rangle$. Temos que

$$|\langle a^{\frac{n}{m}} \rangle| = o(a^{\frac{n}{m}}) = \frac{n}{(n, n/m)} = \frac{n}{n/m} = m,$$

provando a existência do subgrupo de ordem m.

Vamos agora provar a unicidade de tal subgrupo. Seja H um subgrupo de G de ordem m. Defina

$$I = \{i \in \mathbb{Z};\ \ a^i \in H\}.$$

É imediato verificar que I é um subgrupo de $\mathbb{Z}$, logo $I = \mathbb{Z}r$ onde $r = \min(I \cap \mathbb{N})$.

Portanto, temos que $a^i \in H$ se, e somente se, $i \in \mathbb{Z}r$, logo $H = \langle a^r \rangle$.

Mas então, pela Proposição anterior,

$$m = |H| = o(a^r) = \frac{n}{(n, r)},$$

logo, $(n, r) = \frac{n}{m}$, o que, por um corolário anterior, nos fornece

$$H = \langle a^r \rangle = \langle a^{(n,r)} \rangle = \langle a^{\frac{n}{m}} \rangle.$$

□

Os grupos cíclicos são os grupos que têm a estrutura mais simples possível de subgrupos. Em particular, a Proposição acima nos diz que para eles vale a recíproca do Teorema e Lagrange.

A seguir, vamos ver algumas propriedades da ordem do produto de dois elementos de um grupo.

Proposição Seja G um grupo e sejam $a, b \in G$ com ordens finitas e tais que $ab = ba$.

i) Se $(o(a), o(b)) = 1$, então $o(ab) = o(a)o(b)$.

ii) Existe $c \in G$ tal que $o(c) = [o(a), o(b)]$.

iii) Suponha que G é abeliano e que o conjunto das ordens dos elementos de G seja limitado e ponha $r = \max\{\, o(g); \quad g \in G\}$. Tem-se que $o(g)|r$, para todo $g \in G$.

Prova i) Seja n um número natural tal que $(ab)^n = e$. Logo $a^n = b^{-n} \in \langle a \rangle \cap \langle b \rangle$. Como $\langle a \rangle \cap \langle b \rangle$ é tanto subgrupo de $\langle a \rangle$ quanto de $\langle b \rangle$, segue-se pelo Teorema de Lagrange que $|\langle a \rangle \cap \langle b \rangle|$ é divisor comum de $|\langle a \rangle| = o(a)$ e de $|\langle b \rangle| = o(b)$, portanto igual a 1 por serem esses últimos números primos entre si. Logo, $\langle a \rangle \cap \langle b \rangle = \{e\}$. Portanto, $a^n = b^n = e$ e, consequentemente, n é múltiplo comum de $o(a)$ e $o(b)$. Como $o(ab)$ é o menor de tais n, segue-se que $o(ab) = [o(a), o(b)] = o(a)o(b)$.

(ii) Sejam

$$o(a) = p_1^{\alpha_1} \cdots p_l^{\alpha_l} p_{l+1}^{\alpha_{l+1}} \cdots p_n^{\alpha_n} \quad \text{e} \quad o(b) = p_1^{\beta_1} \cdots p_l^{\beta_l} p_{l+1}^{\beta_{l+1}} \cdots p_n^{\beta_n},$$

onde $0 \leq \alpha_i < \beta_i$, $i = 1, \ldots, l$ e $0 \leq \beta_j \leq \alpha_j$, $j = l+1, \ldots, n$, as decomposições de $o(a)$ e $o(b)$ em fatores irredutíveis. Tome

$$a' = a^{p_1^{\alpha_1} \cdots p_l^{\alpha_l}} \quad \text{e} \quad b' = b^{p_{l+1}^{\beta_{l+1}} \cdots p_n^{\beta_n}},$$

cujas ordens são, respectivamente, $p_{l+1}^{\alpha_{l+1}} \cdots p_n^{\alpha_n}$ e $p_1^{\beta_1} \cdots p_l^{\beta_l}$, que são primos entre si. Logo, como a e b comutam, a' e b' comutam e, portanto, pelo item (i),

$$o(a'b') = p_1^{\beta_1} \cdots p_l^{\beta_l} p_{l+1}^{\alpha_{l+1}} \cdots p_n^{\alpha_n} = [o(a), o(b)].$$

(iii) Seja $a \in G$ tal que $o(a) = r$ e suponha que exista $g \in G$ tal que $o(g) \nmid r$. Logo, como g e a comutam, pois G é abeliano, por (ii), existe c em G tal que $o(c) = [r, o(g)] > r$, o que é um absurdo pela maximalidade de r.

□

O seguinte resultado é muito útil no estudo dos corpos finitos.

Teorema Seja A um domínio e seja A^* o grupo multiplicativo dos elementos invertíveis de A. Todo subgrupo finito G de A^* é cíclico.

Prova Suponha que $|G| = n$. Seja $r = \max\{o(g); \quad g \in G\}$, que existe pois G é finito. Para todo $g \in G$, tem-se que $g^r = 1$, pois, pelo item (iii) da Proposição, temos que $o(g)|r$. Isto significa que o polinômio $X^r - 1$ se anula em todos os elementos de G e, portanto, $n \leq r$, pois o número de raízes de um polinômio $p(X) \in A[X]$ é no máximo igual a $\mathrm{grau}(p(X))$. Por outro lado, tem-se pelo Teorema de Lagrange que $r|n$, logo $r \leq n$. Portanto, $r = n$, significando que existe $g \in G$ tal que $o(g) = r = n$, logo $G = \langle g \rangle$ e, portanto, G é cíclico.

□

Corolário Se K é um corpo finito, então o grupo multiplicativo K^* é cíclico.

Note que o resultado do Teorema não é válido se A não for um domínio. Por exemplo $\mathbb{Z}_8^* = \{[1], [3], [5], [7]\}$ é tal que $x^2 = [1]$, $\forall x \in \mathbb{Z}_8^*$, logo não pode ser cíclico.