Teorema (Teorema fundamental do homomorfismo)

Seja $\varphi : G \to H$ um homomorfismo de grupos. Então $G/\ker\varphi \simeq \varphi(G)$.

Demonstração. Vamos mostrar que a correspondência $\psi : G/\ker\varphi \to \varphi(G)$ dada por $\psi(g\ker\varphi) = \varphi(g)$ é um isomorfismo.
Provamos que ψ está bem definida mostrando que não depende do representante particular da classe lateral escolhido. Suponhamos que $x\ker\varphi = y\ker\varphi$. Então $y^{-1}x \in \ker\varphi$ e $e = \varphi(y^{-1}x) = (\varphi(y))^{-1}\varphi(x)$. Logo $\varphi(x) = \varphi(y)$, o que mostra que ψ é de facto uma função.
Tem-se
$\psi(x\ker\varphi \cdot y\ker\varphi) = \psi(xy\ker\varphi) = \varphi(xy) = \varphi(x)\varphi(y) = \psi(x\ker\varphi)\psi(y\ker\varphi)$.
Resta provar que ψ é injectiva, já que é claramente sobrejectiva. Tem-se que $\psi(x\ker\varphi) = \psi(y\ker\varphi)$ implica $\varphi(x) = \varphi(y)$. Resulta então $e = (\varphi(x))^{-1}\varphi(y) = \varphi(x^{-1})\varphi(y) = \varphi(x^{-1}y)$, donde $x^{-1}y \in \ker\varphi$ e daqui $x\ker\varphi = y\ker\varphi$. □

Exemplo

O homomorfismo de $\mathbb{Z}$ em $\mathbb{Z}_n$ que a cada inteiro associa o resto da sua divisão por n tem núcleo $\langle n\rangle$. Consequentemente, $\mathbb{Z}/\langle n\rangle \simeq \mathbb{Z}_n$.

Grupos abelianos finitos

Tal como um inteiro pode ser decomposto num produto de primos, um grupo abeliano finito pode ser decomposto num produto de grupos mais pequenos.

Teorema (Teorema fundamental dos grupos abelianos finitos)

Todo o grupo abeliano finito é produto de grupos cíclicos cujas ordens são potências de primos. Além disso, o número de factores bem como as ordens dos grupos cíclicos envolvidos são determinados pelo grupo.

Atendendo a que um grupo cíclico de ordem n é isomorfo a $\mathbb{Z}_n$, o teorema anterior diz que todo o grupo abeliano finito G é isomorfo a um grupo da forma

$$\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}} \tag{1}$$

em que os p's são primos não necessariamente distintos e as potências $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ são únicos e determinadas pelo grupo.

Muitas vezes é mais conveniente combinar os factores cíclicos de ordens relativamente primas por forma a obter um produto directo da forma

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \tag{2}$$

onde $n_i \mid n_{i-1}$.

Exemplo

Consideremos o grupo

$$G = \mathbb{Z}_{3^3} \times \mathbb{Z}_3 \times \mathbb{Z}_{5^3} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Tem-se

$$G \simeq \mathbb{Z}_{3^3.5^3.2^2} \times \mathbb{Z}_{3.5^2.2} \times \mathbb{Z}_2.$$

Às formas (1) e (2) dá-se por vezes o nome de *formas canónicas dadas pelo teorema fundamental*.

Exercício

Escreva algoritmos que permitam dado um grupo numa das formas canónicas escrevê-lo (a menos de isomorfismo) na outra forma.

Quando escrevemos um grupo abeliano finito na forma (1) ou na forma (2) dizemos que determinamos uma *classe de isomorfismo* desse grupo.

Chamamos *partição* de um inteiro k a um conjunto $\{n_1, n_2, \ldots, n_\ell\}$ tal que

$$k = n_1 + n_2 + \ldots, + n_\ell.$$

Em geral, existe um grupo abeliano de ordem p^k para cada partição de k. Sendo p um primo e $k = n_1 + n_2 + \ldots, + n_\ell$, $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_\ell}}$ é um grupo abeliano de ordem p^k.

Exemplo

Ordem de G	Partições de k	Possíveis produtos directos
p	$\{1\}$	$\mathbb{Z}_p$
p^2	$\{2\}$	$\mathbb{Z}_{p^2}$
	$\{1,1\}$	$\mathbb{Z}_p \times \mathbb{Z}_p$
p^3	$\{3\}$	$\mathbb{Z}_{p^3}$
	$\{2,1\}$	$\mathbb{Z}_{p^2} \times \mathbb{Z}_p$
	$\{1,1,1\}$	$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$
p^4	$\{4\}$	$\mathbb{Z}_{p^4}$
	$\{3,1\}$	$\mathbb{Z}_{p^3} \times \mathbb{Z}_p$
	$\{2,2\}$	$\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$
	$\{2,1,1\}$	$\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$
	$\{1,1,1,1\}$	$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

Observamos que, ao contrário do que acontece com os grupos abelianos, descrever todos os grupos não abelianos cuja ordem é potência de um primo pode ser extremamente difícil. É esse o caso dos grupos de ordem 16.

Depois de saber como tratar os casos das potências de primos, não é difícil tratar o caso geral de grupos abelianos cuja ordem é um inteiro dado.

Exemplo

Seja $n = 1176$. Começamos por escrever $n = 2^3 \cdot 3 \cdot 7^2$. A lista das classes de isomorfismo dos grupos abelianos de ordem 1176 é

$$\begin{aligned}
&\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{49} \\
&\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{49} \\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{49} \\
&\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \\
&\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7.
\end{aligned}$$

Exercício

Escreva os grupos que aparecem no exemplo anterior na outra forma canónica do teorema fundamental.

Pode pôr-se a seguinte questão:
como podemos escrever um grupo abeliano finito G como produto directo de grupos cíclicos de ordem mais pequena? O algoritmo seguinte, onde usamos a notação $\times_i$ para produto o produto directo interno, dá a resposta.

Algoritmo

INPUT: Um grupo abeliano G.

1. Calcula as ordens de todos os elementos de G;
2. Escolhe um elemento a_1 de ordem máxima e define $G_1 = \langle a_1 \rangle$;
   Faz $i = 1$;
3. se $\mathrm{ord}(G) = \mathrm{ord}(G_i)$, pára. Caso contrário, faz $i := i + 1$;
4. Escolhe um elemento a_i de ordem máxima p^k tal que
   $p^k \leq \mathrm{ord}(G)/\mathrm{ord}(G_{i-1})$ e nenhum $a_i, a_i^2, \ldots a_i^{p^k-1}$ pertence a G_{i-1}.
   Define $G_i = G_{i-1} \times_i \langle a_i \rangle$.
5. volta ao passo 3.

OUTPUT: $G \simeq G_i$.

Exemplo

Seja $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ com a multiplicação módulo 65. Trata-se de um grupo abeliano de ordem 16, logo é isomorfo a um dos grupos

$$\mathbb{Z}_{16}$$
$$\mathbb{Z}_8 \times \mathbb{Z}_2$$
$$\mathbb{Z}_4 \times \mathbb{Z}_4$$
$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

As ordens dos elementos são:

	1	8	12	14	18	21	27	31	34	38	44	47	51	53	57	64
ord	1	4	4	2	4	4	4	4	4	4	4	4	2	4	4	2

Desta tabela concluímos de imediato que as únicas possibilidades são $\mathbb{Z}_4 \times \mathbb{Z}_4$ e $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Como $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ tem mais de 2 elementos de ordem 3, concluímos que $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_4$.

Para escrever G como produto directo interno de dois subgrupos, começamos por considerar um elemento de ordem máxima, digamos 8. Temos então que $\langle 8 \rangle$ é um factor no produto.
Seguidamente escolhemos um elemento a de ordem 4 tal que nem a nem a^2 estejam em $\langle 8 \rangle = \{1, 8, 64, 57\}$. 12 satisfaz isto e tem-se $G = \langle 8 \rangle \langle 12 \rangle$.