



Observação

Como para $k > 1$ se tem $(a_1, a_2, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2)$, um ciclo de comprimento par é uma permutação ímpar e um ciclo de comprimento ímpar é uma permutação par.

Proposição

O conjunto das permutações pares de S_n forma um subgrupo de S_n .

Exercício

Faça a demonstração da proposição anterior.

O subgrupo das permutações pares de S_n denota-se por A_n e diz-se o *grupo alterno de grau n* .

```
gap> S6 := SymmetricGroup(6);
Sym( [ 1 .. 6 ] )
gap> Size(S6);
720
gap> A6 := AlternatingGroup(6);
Alt( [ 1 .. 6 ] )
gap> Size(A6);
360
```



Proposição

Para $n > 1$, $\text{ord } A_n = n!/2$.

Demonstração. Sabemos que $\text{ord } S_n = n!$, bastando por isso ver que S_n tem tantas permutações pares como ímpares. Sejam α e β permutações pares distintas. Então $(1\ 2)\alpha$ e $(1\ 2)\beta$ são permutações ímpares distintas. Logo, existem pelo menos tantas permutações ímpares como pares. De modo análogo mostra-se que existem pelo menos tantas permutações pares como ímpares. □



Isomorfismos

Pessoas que trabalham em Álgebra normalmente não fazem qualquer distinção entre estruturas isomorfas. Não se importam se os elementos de um grupo são azuis ou vermelhos; apenas lhes interessa a forma como eles se multiplicam.

Vamos formalizar.

Definição (Isomorfismo; grupos isomorfos)

Um isomorfismo φ de um grupo G num grupo H é uma função bijectiva $\varphi : G \rightarrow H$ que preserva a operação. Isto é,

$$\varphi(ab) = \varphi(a)\varphi(b), \forall a, b \in G.$$

(Note-se que no primeiro membro se tem a operação em G , enquanto que no segundo membro se tem a operação em H .)

Quando existe um isomorfismo de um grupo G num grupo H , dizemos que G e H são isomorfos e escrevemos $G \simeq H$.



Resulta imediatamente da definição que grupos isomorfos têm a mesma ordem. Vejamos alguns exemplos.

Exemplo

Os grupos $G = (\mathbb{R}, +)$ e $H = (\mathbb{R}^+, \cdot)$ são isomorfos. De facto, a função $\varphi : G \rightarrow H$ definida por $\varphi(x) = 2^x$ é um isomorfismo:

- não é difícil ver (faça-o como exercício) que φ é bijectiva, sendo $\log_2$ a função inversa;
- φ preserva as operações:

$$\varphi(x + y) = 2^{x+y} = 2^x \cdot 2^y = \varphi(x) \cdot \varphi(y).$$

Exemplo

Seja G o grupo dos números reais com a adição. A função $\varphi : \mathbb{R} \rightarrow \mathbb{R}$ definida por $\varphi(x) = x^3$, embora seja bijectiva, não é um isomorfismo, pois existem números reais x e y tais que $(x + y)^3 \neq x^3 + y^3$.



Exemplo

Todo o grupo cíclico infinito é isomorfo a $\mathbb{Z}$ com a adição. De facto, se a for um gerador do grupo cíclico, então a função que a a^k associa k é um isomorfismo.

Recordando que num grupo cíclico $\langle a \rangle$ de ordem n se tem $a^i = a^j$ se e só se i e j são congruentes módulo n e que a relação de “congruência módulo n ” é compatível com as operações, é fácil verificar os detalhes necessários à obtenção do seguinte:

Exemplo

O grupo cíclico $\langle a \rangle$ finito de ordem n é isomorfo a $\mathbb{Z}_n$ com a adição módulo n . De facto, a aplicação $a^k \rightarrow k \pmod{n}$ é um isomorfismo.

Exemplo

Basta observar que $U(10)$ é um grupo cíclico de ordem 4, para concluir que $U(10) \simeq \mathbb{Z}_4$.



Exemplo

Ao resolver um exercício na oitava aula verificamos que qualquer elemento x de $U(8)$ satisfaz a igualdade $x \cdot x = 1$. Isto vai-nos permitir mostrar que, embora os grupos $U(8)$ e $\mathbb{Z}_4$ tenham a mesma ordem, não são isomorfos.

Suponhamos que $\varphi : \mathbb{Z}_4 \rightarrow U(8)$ é um isomorfismo. Então,

$$\varphi(2) = \varphi(1 + 1) = \varphi(1) \cdot \varphi(1) = 1. \text{ Também}$$

$\varphi(0) = \varphi(0 + 0) = \varphi(0) \cdot \varphi(0) = 1$, tendo-se portanto $\varphi(2) = \varphi(0)$, o que está em contradição com o supomos que φ é injectiva.



Teorema (Teorema de Cayley)

Todo a grupo é isomorfo a um grupo de permutações.

Demonstração. Seja G um grupo. Para cada $g \in G$ definimos uma função $t_g : G \rightarrow G$ por $t_g(x) = gx$ ($x \in G$). É fácil ver (faça-o como exercício) que a função t_g (que não é mais que a multiplicação à esquerda por g) é uma permutação de G .

Seja $H = \{t_g \mid g \in G\}$. Vejamos que, com a composição, H é um grupo. Ora, para $g, h \in G$, tem-se

$t_g t_h(x) = t_g(t_h(x)) = t_g(hx) = g(hx) = (gh)x = t_{gh}(x)$, donde resulta que $t_g t_h = t_{gh}$. Segue-se que t_e é a identidade e que $(t_g)^{-1}$ é $t_{g^{-1}}$.

Tendo em conta que a composição de funções é associativa, concluímos que H é um grupo.

Definimos agora $\varphi : G \rightarrow H$ por $\varphi(g) = t_g$. Vejamos que φ preserva as operações. Sejam $x, y \in G$. Tem-se $\varphi(xy) = t_{xy} = t_x t_y = \varphi(x)\varphi(y)$.

Pela construção de H , φ é sobrejectiva. Se $t_g = t_h$, então $t_g(e) = t_h(e)$, ou seja $ge = he$, o que é o mesmo que $g = h$, logo φ é injectiva. $\square$



O grupo H construído na demonstração anterior diz-se a *representação regular à esquerda* de G .

Exemplo

Vamos construir a representação regular à esquerda H de $U(8) = \{1, 3, 5, 7\}$.

$$\text{Tem-se: } t_1 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 1 & 3 & 5 & 7 \end{pmatrix}, t_3 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 3 & 1 & 7 & 5 \end{pmatrix},$$

$$t_5 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 5 & 7 & 1 & 3 \end{pmatrix}, t_7 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 7 & 5 & 3 & 1 \end{pmatrix}$$

Obtém-se então as tabelas seguintes, as quais diferem apenas nas notações usadas.

$U(8)$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

H	t_1	t_3	t_5	t_7
t_1	t_1	t_3	t_5	t_7
t_3	t_3	t_1	t_7	t_5
t_5	t_5	t_7	t_1	t_3
t_7	t_7	t_5	t_3	t_1



Propriedades dos isomorfismos

Proposição

*Seja φ um isomorfismo de um grupo G num grupo H e sejam $a, b \in G$.
Então*

- 1. φ envia a identidade de G na identidade de H ;*
- 2. para qualquer inteiro n , $\varphi(a^n) = (\varphi(a))^n$;*
- 3. a e b comutam se e só se $\varphi(a)$ e $\varphi(b)$ comutam;*
- 4. $\text{ord } a = \text{ord } \varphi(a)$;*
- 5. dados um inteiro k e um elemento $g \in G$, a equação $x^k = g$ tem o mesmo número de soluções em G que a equação $x^k = \varphi(g)$ em H .*

Exercício

Faça a demonstração da proposição anterior.