Observações

G um grupo finito & $g \in G$. A ordem de g é definida como

$$o(g) = |\langle g \rangle| = |\{g^n \mid n \in \mathbb{Z}\}| \quad (1)$$

Em outro livro a definição:

$$o(g) = \min\{n \in \mathbb{N} \mid g^n = e\} \quad (2)$$

ou seja, é o menor inteiro n_0 t.q. $g^{n_0} = e$

(1) $o(g)$ = nº potências distintas de g

Seja $n_0 = \min\{n \mid g^n = e\}$

Considere as potências $e, g, \dots, g^{n_0-1}$

Cf.: Elas são duas a duas distintas

Suponha que existem $0 \le i, j \le n_0 - 1$ t.q. $g^i = g^j$ Posso supor que $i < j$

$g^j * g^{-i} = e$

$e = g^{j-i}$

Mas daí $n = j - i \in \mathbb{N}$ & $g^n = e$

Pela escolha de n_0 & (2) temos que ou $n = 0$ $\longrightarrow i = j$ absurdo

ou

$n \geq n_0$

↳ $n_0 > j - i \geq n_0$, logo temos um absurdo

(1) $n_0 \leq o(g)$

AF.: $\langle g \rangle = \{e, g, \cdots, g^{n_0 - 1}\}$

Claramente $\langle g \rangle \supseteq \{e, g, \cdots, g^{n_0 - 1}\}$

A coisa é provar que $\langle g \rangle \subseteq \{e, \cdots g^{n_0 - 1}\}$

Pegue $x \in \langle g \rangle$ então $\exists n \in \mathbb{Z}$ t.q. $x = g^n$

Pelo algoritmo da divisão $\exists\, \mathbb{Z} \exists q$ & r $0 \leq r < n_0$ t.q. $n = q n_0 + r$. Daí $x = g^n = g^{q n_0 + r}$

$= g^{qn_0} \cdot g^r = (g^{n_0})^q \cdot g^r = e^q \cdot g^r = g^r$ (58

$0 \leq r \leq n_0 - 1$

$g^r \in \{ e_1 \cdot g^{n_0 - 1} \}$

Em particular $g^{n_0} = g^{o(g)} = e$ (def)

Pela 1ª def. (Teo Lagrange)

$o(g) \mid |G|$, pois $o(g) = |\langle g \rangle| \mid |G|$

Logo $\forall g \in G \quad g^{|G|} = e$ pois $|G| = o(g) \cdot m$

daí $g^{|G|} = [g^{o(g)}]^m = e^m = e$

#

- GAP
- MATEMÁTICA
- MAPLE

Todo $n \in 2\mathbb{N}$ é soma de dois primos

#

Revendo os $\mathbb{Z}_n$

$G = (\mathbb{Z}, +)$ $H < G$ então $\exists\, n_0 \in \mathbb{N}$ t.q. $H = n_0\mathbb{Z}$

I é ideal se

- $x, y \in I \Rightarrow x+y \in I$
- $x \in I, y \in \mathbb{Z} \Rightarrow xy \in I$

$H < G \longrightarrow x, y \in H$

$x * y^{-1} = x - y \in H$

$n_0\mathbb{Z} = H = \{\ldots -n_0, 0, n_0, 2n_0, \ldots\}$

Prova $(H \neq \{0\})$

Defina $n_0 = \min\{n \in \mathbb{N} \mid n \in H\}$

$\neq \emptyset$

pois $H < G$

Pelo axioma da boa ordenação n_0 existe

Tome $n \in H$ qqer

$\exists q$ & r $\quad 0 \leq r < n_0$ tq $\quad n = qn_0 + r$

$r = n - qn_0$

(1) $\exists\, a \in \mathbb{R}$ tq. $H = a\mathbb{Z}$

ou (2) H é denso em $\mathbb{R}$

$n_0^{\,q} = n_0 * n_0 * \ldots * n_0$

$= n_0 + n_0 + \ldots + n_0 \cdot qn_0$

Logo $\begin{cases} r \in H \\ 0 \leq r < n_0 \end{cases}$

& n_0 é o menor inteiro positivo pertencente a H

$r \longrightarrow r = 0$. Daí $n = q n_0$

$H \ni n \Rightarrow n \in n_0\mathbb{Z}$ $\quad n_0 \in H$

Logo $H \subseteq n_0\mathbb{Z}$

$n_0\mathbb{Z} = \langle n_0 \rangle \subseteq H$

Daí $H = n_0\mathbb{Z}$

Tome $H < G = (\mathbb{Z}, +)$

Vimos que existe $n_0 \in \mathbb{N}$

t.q.

$H = n_0\mathbb{Z}$

Como são as classes laterais de H?

$\boxed{* = +}$ $\quad \boxed{x^{-1} = -x}$

Rel. eq. sobre G $\quad \boxed{e = 0}$

$$\boxed{x \sim y \Leftrightarrow x^{-1} * y \in H}$$

$x \sim y \Leftrightarrow y - x \in n_0\mathbb{Z}$

$x \sim y \Leftrightarrow n_0 \mid (y - x)$

$x \sim y \Leftrightarrow x \equiv y \pmod{n_0}$

$[x] = \{y \in \mathbb{Z} \mid y \equiv x \pmod{n_0}\}$

$= \{ x + k n_0 \mid k \in \mathbb{Z} \}$

$= x + n_0 \mathbb{Z}$

$\bar{x} := [x]$

& $\mathbb{Z}_n := \{ \bar{0}, \bar{1}, \ldots \overline{n_0 - 1} \}$

Tábuas

$n_0 = 4$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\bar{G} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \}$

$\bar{+}$ a operação em $\bar{G}$

$\bar{x} \;\bar{+}\; \bar{y} = \overline{x + y}$

Note que $(\bar{G}, \bar{+})$ é um grupo

Logo o conjunto de classes laterais de 14 formam um grupo com certa operação

definida a partir da operação de G.

Construção de Novos Grupos a partir de um grupo dado

- Dado G olhar para subconjuntos de G que também são grupos.
- O produto cartesiano de grupos

$\dim_{\mathbb{R}}(V) = n$

$B = \{u_1, \ldots, u_n\}$ base de V

$\forall \alpha \in V \ \exists! \ (x_1 \ldots, x_n) \in \mathbb{R}^n$

t.q. $\alpha = x_1 u_1 + \ldots x_n u_n$

$V \ni [\alpha] \longmapsto (x_1, \ldots, x_n) \in \mathbb{R}^n$

bijeção linear

Dados 2 grupos $(G_1, *_1)$ & $(G_2, *_2)$

Vamos construir $(G = G_1 \times G_2, *)$ como segue

$$G = (G_1 \times G_2) = \{(x,y) \mid x \in G_1, y \in G_2\}$$

$$\left.\begin{array}{l} g_1 = (x_1, x_2) \\ g_2 = (y_1, y_2) \end{array}\right\} \in G$$

$$g = g_1 * g_2 = (x_1, x_2) * (y_1, y_2)$$

$= (x_1 *_1 y_1 , x_2 *_2 y_2)$

* é 1) fechada
2) associativa
o elemento neutro de G
$e = (e_1, e_2)$
onde e_i é o elemento neutro de G_i,
$i = 1, 2$
inversa: $g = (x_1, x_2)$
$g^{-1} = (x_1^{-1}, x_2^{-1})$

$$g \cdot g^{-1} = (x_1, x_2) * (x_1^{-1}, x_2^{-1})$$
$$= (x_1 *_1 x_1^{-1}, x_2 *_2 x_2^{-1})$$
$$= (e_1, e_2) = e$$

G é chamado o produto cartesiano dos grupos G_1 & G_2

Exemplos

· Os grupos C_n

O grupo C_n é definido como $\{e, g, g^2, \ldots, g^{n-1}\}$ com $g^n = e$ & $g^i \cdot g^j = g^{(i+j)}$ onde $(i+j)$ é o resto da divisão de $(i+j)$ por n

$n=2$

$C_2 = \{e, g\}$ $g^2 = e$

	e	g
e	e	g
g	g	e

$g \cdot g = g^2 = e$

$n=3$

$C_3 = \{e, g, g^2\}$ $g^3 = e$

	e	g	g^2
e	e	g	g^2
g	g	g^2	e
g^2	g^2	e	g

$g^2 \cdot g^2 = g^{(2+2)} = g^1 = g$

$n=4$ $C_4 = \{e, g, g^2, g^3\}$ $g^4 = e$

	e	g	g^2	g^3
e	e	g	g^2	g^3
g	g	g^2	g^3	e
g^2	g^2	g^3	e	g
g^3	g^3	e	g	g^2

grupo abeliano = tabuada simétrica (em relação à diag. principal)

grupo: em uma linha aparece todo mundo uma única vez.

$\forall n \in \mathbb{N}$

$(\mathbb{Z}_n, +)$ é isomorfo a C_n

$\psi : \mathbb{Z}_n \longmapsto C_n = \{e, \dots, g^{n-1}\}$ $(g^n = e)$

$\bar{x} \mapsto g^x$

ψ está bem definido?

Se $\bar{x} = \bar{y} \Rightarrow x - y = kn$, $\exists k \in \mathbb{Z}$

$x = y + kn$

Logo, $g^x = g^{y+kn} = g^y \cdot (g^n)^k = g^y = \psi(y)$

$\psi(x)$

Por que é um homomorfismo?

$|C_n| = n = |\mathbb{Z}_n|$

- ψ é homomorfismo

$\psi(\bar{x} + \bar{y}) = \psi(\overline{x+y}) = g^{x+y} = g^x g^y =$

$= \psi(x)\psi(y)$

- $\ker \psi = \{\bar{0}\}$ & Logo ψ é injetora

$\psi(\bar{x}) = e \quad (\bar{x} \in \ker \psi)$

$\parallel$

$g^x \quad \therefore g^x = e \Rightarrow n \mid x \Rightarrow \bar{x} = \bar{0}$

Logo $\ker \psi = \{\bar{0}\}$ Como $n = |C_n| = |\mathbb{Z}_n|$

& ψ é 1-1 $\Rightarrow$ ψ é bijeção