Grupos

Um grupo G é um conjunto com uma operação ($\bullet, +, * \ldots$)

① $a, b \in G \Rightarrow a \cdot b \in G$ (fechado pela operação)

② $a, b, c \in G \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$
(associatividade)

③ $\exists e \in G$ (elemento identidade) tal que
$\forall a \in G \quad e \cdot a = a \cdot e = a$

④ $\forall a \in G$ existe $b \in G$ tal que
$a \cdot b = b \cdot a = e$ (inverso)

---

⑤ No caso que $a \cdot b = b \cdot a \quad \forall a, b \in G$
dizemos que o grupo é abeliano
(caso contrário é não abeliano)

Exemplos

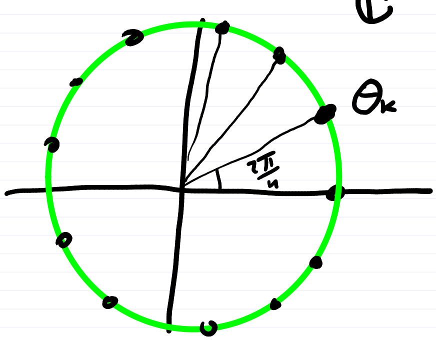
- $(\mathbb{Z}, +)$ é um grupo abeliano
- $(\mathbb{Z} \, \cdot)$ NÃO é grupo (Quase nenhum elemento tem inverso)

C • R $(\mathbb{Q},+)$ é um grupo abeliano

C • R $(\mathbb{Q},\cdot)$ O zero não tem inverso Logo não é grupo

C • R* $(\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}, \cdot)$ é um grupo abeliano

$G=\{1,-1\}$ com o produto é um grupo abeliano com 2 elementos.



$$G=\left\{ \overset{\theta_k}{\overset{\shortparallel}{e^{\frac{2\pi i k}{n}}}} \;\middle|\; k=0,1,2\ldots n-1 \right\}$$

$(G\,\cdot)$ é um grupo abeliano com n elementos

$\mathbb{Z} \bmod n$ = restos quando divido por n

$\{0,1\ 2,\ldots,n-1\}$ $+$

$\mathbb{Z} \bmod 3 = \{0,1,2\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\mathbb{Z}$ não divisíveis por p módulo primo p

$\mathcal{C} = \{1, 2, 3 \ldots p-1\}$

é um grupo.

Temos que provar que todo elemento tem inverso, i.e. $(a,p)=1$ então existe $(b,p)=1$ tal que $ab \equiv 1 \mod p$.

$\mathcal{C} = \{1, 2, \ldots, p-1\}$

$a\mathcal{C} = \{\underbrace{a, 2a, \ldots, (p-1)a}\} \underbrace{\mod p}$

afirmamos: que todos os elementos de $a\mathcal{C} \mod p$ são distintos, suponhamos a afirmação é falsa, isto é, existe

$1 \leq i < j \leq p-1$ tais que

$ai \equiv aj \mod p$

$\Rightarrow$ p divide $ai - aj = a(i-j)$

Mas como p é primo $\Rightarrow$ ou p divide a ou p divide $i-j$

Como o primeiro não é possível $\Rightarrow$

p divide $j-i$, mas $\underline{j-i>0}$

$\Rightarrow$ $j-i \geq p$ o que é contraditório

pois $0 \leq i, j \leq p-1$

Logo em $a\mathcal{C} \bmod p$ aparecem todos os restos $\neq 0$ modulo p, em particular aparece o resto 1 $\Rightarrow$ $\exists\, b \in \mathcal{C}$ tal que

$\underline{ab \equiv 1 \bmod p}$

$p=5$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

<u>Fato geral</u>: G grupo e $a \in G$

condição 1

$$\Rightarrow aG = \{ag \mid g \in G\} \overset{\subseteq}{=} G$$

$\rightarrow \supseteq$?

Seja $h \in G$ queremos mostrar que existe $g \in G$ tal que $ag = h$

inverso de a

defino $\quad g = \underset{\substack{\cap \\ G}}{a^{-1}} \overset{(1)}{} \underset{\substack{\cap \\ G}}{h} \in G$

$$ag = a\underset{(2)}{(a^{-1}h)} = \underset{(4)}{(aa^{-1})}h = eh \overset{(3)}{=} h$$

Suponhamos que G é <u>abeliano</u> e finito $|G| = n$ e seja

$a \in G$

$$\begin{aligned} G &= \{g_1, g_2, g_3, \dots, g_n\} \\ &\parallel \\ aG &= \{ag_1, ag_2 \dots ag_n\} \end{aligned}$$

$$g_1 g_2 g_2 \dots g_n = (ag_1)(ag_2)\dots(ag_n)$$

$\downarrow$ abeliano

$$\underbrace{g_1 g_2 \dots g_n}_{h} = a^n \underbrace{g_1 g_2 g_2 \dots g_n}_{h}$$

$$\boxed{h = a^n h}$$

multiplicando pelo inverso de h

$$\Downarrow$$

$$e = a^n$$

Se G é finito com n elementos (e abeliano) então $a \in G$ temos que $a^n = e$.

$(\mathbb{Z}_p^*, \cdot)$ inteiros não divisíveis por p módulo p com o produto é Grupo com $\underline{p-1} = n$.

$\Rightarrow a \in \mathbb{Z}_p^* \quad a^{p-1} \equiv 1 \mod p$

Teorema de Fermat

$G = \{\pm 1, \pm i, \pm j, \pm k\}$

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

$j \cdot (-j) = 1$

$$\begin{cases} (i \cdot j) \cdot k = k \cdot k = -1 \\ i \cdot (j \cdot k) = i \cdot i = -1 \end{cases}$$

associatividade

$$\begin{cases} (i \cdot k) \cdot i = (-j) \cdot i = k \\ i \cdot (k \cdot i) = i \cdot j = k \end{cases}$$

Operação binaria

$$f : G \times G \to G$$
$$(a, b) \mapsto f(a, b)$$

Teorema: Em um grupo o elemento identidade é único e o inverso é único

Prova: $e_1, e_2 \in G$ são elementos identidade

$$e_2 = e_1 e_2 = e_1 \checkmark$$

e_1 é identidade $\qquad$ e_2 é identidade

Seja $a \in G$ e b_1 b_2 inversos

$$e = b_1 a \Rightarrow e \cdot b_2 = (b_1 a) b_2$$

$$b_2 = b_1 (a b_2)$$
$$= b_1 e$$
$$= b_1$$

Somente temos um inverso.

$GL(2,\mathbb{R})$ = matrizes 2×2 com coeficientes em $\mathbb{R}$ inverTíveis (com o produto)

$\downarrow$

é um grupo $\qquad A, B \in GL(2,\mathbb{R})$

$$\boxed{A \in GL(2,\mathbb{R}) \Leftrightarrow \det(A) \neq 0}$$

$$\det(AB) = \det(A)\det(B) \neq 0$$
$$\Rightarrow AB \in GL(2,\mathbb{R})$$

- $A, B, C \in GL(2\,\mathbb{R}) \Rightarrow (AB)C = A(BC)$
- $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL(2\,\mathbb{R})$ elemento identidade

$GL(2,\mathbb{R})$ <u>não</u> é <u>abeliano</u>

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & 7 \end{pmatrix} = \begin{pmatrix} 6 & 15 \\ 12 & 31 \end{pmatrix} \not\parallel$$
$$\begin{pmatrix} 0 & 1 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 24 & 34 \end{pmatrix}$$

$GL(2,\mathbb{Q})$ tambem é grupo com o produto

$GL(2, \mathbb{Z}_p)$ é grupo (p primo)

Def: Dado um grupo $(G, \cdot)$ um subgrupo é um subconjunto $H \subseteq G$ tal que $(H \cdot)$ é grupo

Exemplos $G = (\mathbb{R} +)$ $H = (\mathbb{Q} +)$ $K = (\mathbb{Z} +)$ subgrupo

$\mathbb{R} \supset \mathbb{Q}$

H é subgrupo de G $(H \leqslant G)$

$K \leqslant H \leqslant G$

Def: Dado um grupo G e $a \in G$ definimos $\operatorname{ord} a$ como o menor inteiro positivo ℓ (caso exista) tal

$$a^\ell = \overbrace{a \cdot a \cdot a \cdots a}^{\ell \text{ vezes}} = e$$

Vimos que se G é finito $(|G| = n)$

então $a^n = e$ logo deve existir um l mínimo tal que

$$a^l = e$$

Proposição: Seja G grupo ~~finito~~ abeliano finito com n elementos. Então para todo $a \in G$ ord a divide n

Prova: Suponhamos falso, isto é existe $a \in G$ tal que ord $a = l$ não divide n. Logo usando o algoritmo da divisão $n = ql + r$ com $0 < r < l$

$$e = a^n = a^{ql+r} = a^{ql}a^r = (a^l)^q a^r$$
$$= e^q a^r = a^r$$

$\Rightarrow$ $a^r = e$ isto é contraditório

pois $r < l = \text{ord}\, a$ $\boxtimes$