Grupos → Fechado
→ Associativa
→ Elemento neutro
→ inverso.

Lema: Se G é um grupo abeliano finito $|G|=n$ e $a \in G$ então $a^n = e$

Def: $(G, \cdot)$ um grupo, então um subconjunto $H \subseteq G$ é um subgrupo se $(H, \cdot)$ é um grupo

$$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$$

"Teorema de Lagrange": Suponhamos $H \leq G$ então para quaisquer dois elementos $a, b \in G$ existe uma bijeção $aH \to bH$

onde

$aH = \{ah \mid h \in H\}$ $\quad$ $bH = \{bh \mid h \in H\}$

Prova:

$$\psi : aH \longrightarrow bH$$

$$\underline{\underline{x}} = ah \longmapsto ba^{-1}\underline{x} = ba^{-1}(ah) = bh$$

ψ é injetiva? é sobre?

Seja $x, y \in aH$

$$\psi(x) = \psi(y) \Rightarrow ba^{-1}x = ba^{-1}y$$

$$b^{-1}(ba^{-1}x) = b^{-1}(ba^{-1}y)$$

$$(b^{-1}b)a^{-1}x = (b^{-1}b)(a^{-1}y) \Rightarrow a^{-1}x = a^{-1}y$$

$$\dots \quad x = y \qquad \text{injetiva}$$

Seja $z \in bH \Rightarrow z = bh$ definimos

$$x = ah \rightsquigarrow \psi(x) = ba^{-1}x = ba^{-1}(ax)$$
$$= bx$$

sobre

"aH e bH" tem a mesma quantidade de elementos

$H \leq G$ definimos uma relação de <u>equivalencia</u>

$a \sim b \iff \exists\, h \in H$ tal que

$$ah = b$$

- Reflexiva $a \sim b \Rightarrow a \cdot e = a$ $e \in H$
- Transitiva $a \sim b,\ b \sim c$ $ah_1 = b$, $bh_2 = c$ $\Rightarrow a \underbrace{h_1 h_2}_{\in H} = c$

$$\Rightarrow a \sim c$$

- Simétrica $a \sim b$ $ah = b \Rightarrow a = bh^{-1}$

$h \in H \Rightarrow h^{-1} \in H \Downarrow$

$b \sim a$

$$\boxed{a \sim b \iff b \in aH}$$

Logo nossas classes de equivalencia são da forma aH

Lembrando que classes de equivalencia definem uma partição G.

Se T conjunto de representantes da classes, i.e. (T transversal)

$c, d \in T \Leftrightarrow c \not\sim d$

$\forall a \in G - \exists c \in T \quad a \sim c$

classes laterais

(*) $$\underbrace{G = \bigcup_{c \in T} cH}$$

Teorema de Lagrange: Seja G um grupo finito e $H \leq G$ então

$|H|$ divide $|G|$

<u>Prova</u>:

$$G = \bigcup_{c \in T} cH$$

Logo $$|G| = \sum_{c \in T} |c\underline{\underline{H}}|$$

mas mostramos que todas as classes

laterais tem a mesma quantidade de elementos ie $|cH| = |H| \ \forall c \in G$

$$|G| = |\mathcal{T}| \cdot |H|$$

Logo $|H|$ divide $|G|$ $\square$

Corolário: G grupo finito e $a \in G$. então $l = ord(a)$ divide $|G| = n$

Prova: $H = \langle a \rangle = \{ a^j \mid j = 0, 1, 2 \ldots \}$

$a^0 = e$

H é um subgrupo $a^j a^i = a^{i+j}$

$a^l = e \Rightarrow a^{l-1} \cdot a = e$

$\Rightarrow a^{l-1}$ é o inverso de a.

e $|H| = ord(a)$ Logo pelo teorema de Lagrange

$ord(a) = |H|$ divide $|G| = n$

$\square$

Exemplos: $\mathbb{Z}_n$ inteiros módulo n.

$(\mathbb{Z}_n, \cdot)$ não é grupo

$U(\mathbb{Z}_n)$ = elementos de $\mathbb{Z}_n$ que tem inverso multiplicativo

$a \in \mathbb{Z}_n$ $\quad \boxed{ax \equiv 1 \bmod n}$ tem solução

$$\Updownarrow$$

$$mdc(a, n) = 1$$

$$U(\mathbb{Z}_n) = \{ a \in \mathbb{Z}_n \mid mdc(a, n) = 1 \}$$

é um grupo $\quad a, b \in U(\mathbb{Z}_n)$

$$\begin{cases} (a, n) = 1 \\ (b, n) = 1 \end{cases} \Rightarrow (ab, n) = 1$$

$a \in U(\mathbb{Z}_n) \Rightarrow \exists\, x_a$ tal que $a x_a \equiv 1 \bmod n$

$\Rightarrow$ x_a é o inverso de a //

$a \in U(\mathbb{Z}_n)$ então

$\operatorname{ord}(a)$ divide $|U(\mathbb{Z}_n)|$

$$|U(\mathbb{Z}_n)| = |\{a \in \mathbb{Z}_n \mid \operatorname{mdc}(a,n)=1\}|$$

$$= \varphi(n) \quad \text{funçã de Euler}$$

$$\Rightarrow a^{\varphi(n)} \equiv 1 \bmod n \quad (\underline{\text{Euler}})$$

Exemplo 2 $\quad M_2(\mathbb{Z}_p)$

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z}_p \right\}$$

$$U(M_2(\mathbb{Z}_p)) =: GL(2, \mathbb{Z}_p)$$

$$\| $$

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p) \;\middle|\; \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0 \bmod p \right\}$$

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p) \;\middle|\; \begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix} \text{ são L.I } \bmod p \right\}$$

Quantos elementos tem $GL(2, \mathbb{Z}_p)$?

de formas de escolher a 1º coluna

$p^2 - 1$ formas (pois não podemos escolher o vetor $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$)

$\begin{pmatrix} a \\ c \end{pmatrix} \rightarrow$ Perguntando o complementos Quantos vetores são LD ao

vetor $\begin{pmatrix} a \\ c \end{pmatrix} \rightsquigarrow \underline{u\begin{pmatrix} a \\ c \end{pmatrix}}$ $u \in \mathbb{Z}_p$

temos p possíveis valores para u

Quantos escolhas para a segunda coluna? $p^2 - p$

$$|GL(2, \mathbb{Z}_p)| = (p^2 - 1) \cdot (p^2 - p) \Leftarrow$$

Se $A \in GL(2, \mathbb{Z}_p)$ então

$$A^{(p^2-1)(p^2-p)} = I \quad \left(\text{ord}(A) \text{ divide } (p^2-1)(p^2-p) \right)$$

Homomorfismo de Grupos:

Um homomorfismo de G a H (Grupos)
é uma função $\psi: G \to H$
que conserva a estrutura i.e.

- $\psi(a \cdot b) = \psi(a) \cdot \psi(b)$. ✓
- $\psi(a^{-1}) = \psi(a)^{-1}$ ✓

Observemos que

* $\psi(e_G) = \psi(e_G \cdot e_G) = \psi(e_G) \cdot \psi(e_G)$

$e_H = \psi(e_G)$

- Indutivamente temos que $\psi(a^n) = \psi(a)^n$
$n \in \mathbb{Z}$

$C_n = \langle g \rangle$ $\quad$ $\text{ord}(g) = n$ $\quad$ <u>Caracter</u>

$$\tau : C_n \longrightarrow \mathbb{C}^*$$ é um homomorfismo de grupos

$$g^{\ell} \longmapsto e^{\frac{2\pi i}{n}\ell}$$

- $\tau(g^{\ell_1} g^{\ell_2}) = \tau(g^{\ell_1 + \ell_2}) = e^{\frac{2\pi i}{n}(\ell_1 + \ell_2)}$

$$= e^{\frac{2\pi}{n}\ell_1} e^{\frac{2\pi}{n}\ell_2} = \tau(g^{\ell_1})\tau(g^{\ell_2})$$

- $\tau(g^{-\ell}) = e^{\frac{2\pi i}{n}(-\ell)} = \left(e^{\frac{2\pi i}{n}\ell}\right)^{-1} = \left(\tau(g^{\ell})\right)^{-1}$

<u>Def</u>: Dado um grupo G um <u>caracter</u> de G é um homomorfismo

$$\tau : G \to \mathbb{C}^*$$

<u>Def</u>: G um grupo e $N \leq G$ dizemos qe N é normal em G se $aN = Na$ para todo $a \in G$

$aN = \{an \mid n \in N\}$
$Na = \{na \mid n \in N\}$

(Se G é abeliano todo subgrupo é normal)

$$G = \bigcup_{t \in \mathcal{T}} tN$$

Podemos colocar sobre $\{tN \mid t \in \mathcal{T}\} = \mathcal{C}$

uma operação que "transforma" $\mathcal{C}$ em um Grupo

Definindo a seguinte operação

$$\underline{aN} \bullet \underline{bN} =: abN$$

Com a operação $\bullet$ $\mathcal{C}$ é grupo?

- Bem definido?

Seja $a_1 \sim a_2$ $\quad a_1N = a_2N$
$b_1 \sim b_2$ $\quad b_1N = b_2N$

queremos mostrar $\underline{a_1b_1N} = \underline{a_2b_2N}$

$x \in \underline{\underline{a_1 b_1 N}} \iff x = a_1 b_1 n \quad (n \in N)$

$a_1 = a_2 m_1 \quad m_1 \in N$

$b_1 = b_2 m_2 \quad m_2 \in N$

$x = a_2 \underline{\underline{m_1 b_2}} m_2 n \qquad m_1 b_2 \in N b_2 = b_2 N$

$\Rightarrow \exists m_3$ tal que $m_1 b_2 = \underline{\underline{b_2 m_3}}$

$x = a_2 b_2 \underbrace{m_3 m_2 n}_{\in N} \in \underline{\underline{a_2 b_2 N}}$

$\Rightarrow a_1 b_1 N \subseteq a_2 b_2 N$

equivalentemente $a_1 b_1 N \supseteq a_2 b_2 N$

$\Rightarrow a_1 b_1 N = a_2 b_2 N$ ✓

$(\mathcal{C}\ \bullet)$ é um grupo

* É fechado ✓
* $(aN \cdot bN) \cdot cN = (abN) \cdot cN = ((ab)c)N$

$aN \cdot (bN \cdot cN) = \dots = abcN$

* $(aN) \cdot N = (aN) \cdot (eN) = a \cdot eN = aN$

* $(aN)(a^{-1}N) = aa^{-1}N = N$

Exemplo de homomorfismo

$N \trianglelefteq G$ subgrupo normal $\mathcal{G} =: \frac{G}{N}$

notação

$\theta : G \longrightarrow \frac{G}{N}$

$a \longmapsto aN$

θ é um homomorfismo de grupos

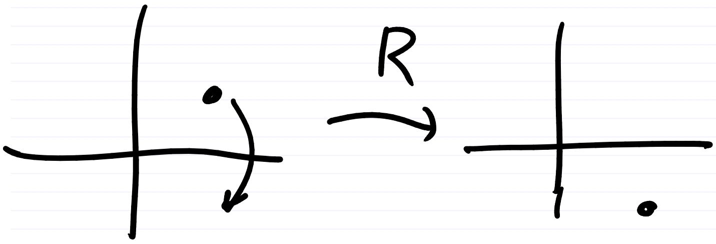
$\theta(ab) = abN = \underset{\text{Notação}}{aN \cdot bN} = \theta(a)\theta(b)$

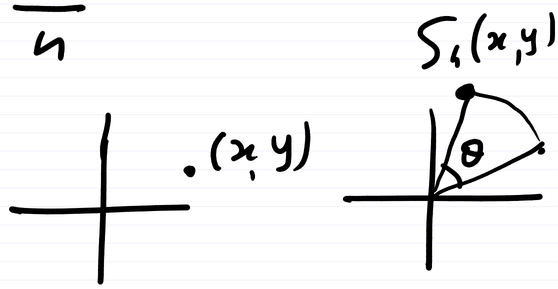
$\theta(a^{-1}) = \underline{a^{-1}N} = (\underline{aN})^{-1} = (\theta(a))^{-1}$

$R: \mathbb{R}^2 \to \mathbb{R}^2$ $\qquad$ $S_n : \mathbb{R}^2 \to \mathbb{R}^2$

$(x,y) \to (x,-y)$ $\qquad$ $(x,y) \to \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

$\theta = \frac{2\pi}{n}$



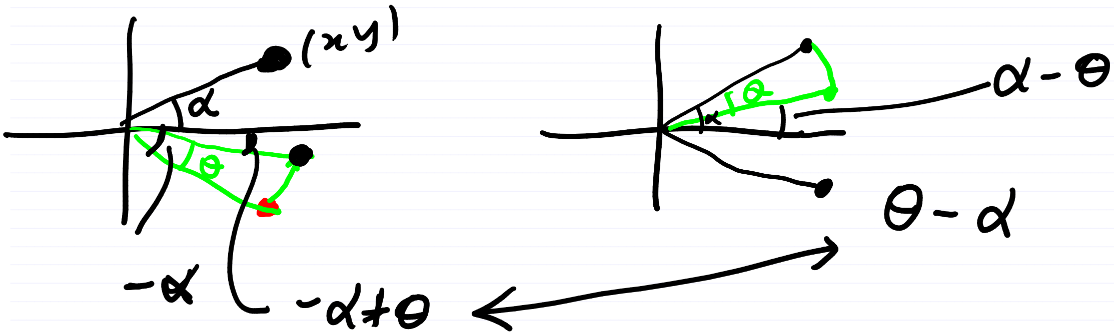


$R \circ R = Id.$ $\qquad$ $\underbrace{S_n \circ \cdots \circ S_n}_{n} = Id$

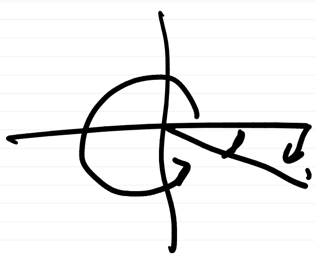
$S_n^{\circ n} = id$

$S_n \circ R \begin{pmatrix} x \\ y \end{pmatrix} = R \circ S_n^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$

$S_n^{-1} = S_n^{\circ(n-1)}$



$D_{2n} = \langle R , S_n \rangle$



$S_n S_n \cdots S_n R S_n S_n \cdots S_n R = R^i S_n^j$

$i = 0,1 \qquad j = 0,1,2 \ldots, n-1$

$\underline{N} = \langle S_n \rangle = \{ \underbrace{Id, S_n, S_n^2 \dots S_n^{n-1}}\}$

é normal $\quad \underline{T} \in D_{2n} \quad T = R^j S_n^i$

$T N = R^i \underline{\underline{S_n^i}} \underline{\underline{N}} = R^i N \to$ $i=0$: $N = N R^i = N R^j S_n^i = N T$

$i=1$: $\underline{RN} = \{R, RS_n, \dots R S_n^{n-1}\}$

$= \{R, S_n^{n-1} R, S_n^{n-2} R \dots S_n R\} = \underline{NR}$

Logo N é normal

$|N| = n \quad |D_{2n}| = 2n \quad \left|\dfrac{D_{2n}}{N}\right| = 2$

$\dfrac{D_{2n}}{N} = \{N, RN\}$

Teorema se G e $H \leq G$ e

$\dfrac{|G|}{|H|} = P$ primo onde P é o menor primo

que divide $|G|$ então H é normal