Introdução a Teoria dos Grupos – MAT 113 – Pós Mat – UFABC-QS2020.2

Homomorfismos de Grupos:

Sejam $(G,.)$, $(H,*)$ grupos. A aplicação $\varphi: G \longrightarrow H$ é um **homomorfismo de grupos** se: $\varphi(a.b) = \varphi(a) * \varphi(b)$, $\forall a,b \in G$.

Ex: a) $\varphi: \mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}$ def por $\varphi(x) = \bar{x}$ é Homomorfismo de Grupos

$(\varphi(a+b) = \overline{a+b} = \bar{a}+\bar{b} = \varphi(a)+\varphi(b))$

b) $f: (\mathbb{C}^*,.) \to (\mathbb{R}^+,.)$, $f(z) = |z|$ é homomorfismo de grupos pois $f(ab) = |ab| = |a|.|b| = f(a)f(b)$

Def: Seja $\varphi: G \to H$ homomorfismo de grupos. Dizemos que φ é um **monomorfismo** se φ for **injetora**. φ é um **isomorfismo** se φ for **bijetora**. Um isomorfismo $\varphi: G \to G$ é um **automorfismo**.

SEJA X CONJUNTO NÃO VAZIO.

DENOTE $Sym(X) = \{ f : X \to X \mid f \text{ função bijetora} \}$

$(Sym(X), \circ)$ É GRUPO, COM A OPERAÇÃO DE COMPOSIÇÃO DE FUNÇÕES.

. Valem que:

a) $f, g \in Sym(X) \to f \circ g \in Sym(X)$.

b) $(f \circ g) \circ h = f \circ (g \circ h)$, $\forall f, g, h \in Sym(X)$

c) $\exists i \in Sym(X)$, $i =$ identidade, t.q. $f \circ i = i \circ f = f$, $\forall f \in Sym(X)$

d) Para cada $f \in Sym(X)$, $\exists g = f^{-1} \in Sym(X)$ tq

$f \circ g = g \circ f = i$ (pois f é bijetora $f : X \to X$)

SE X FOR UM CONJUNTO FINITO, $Sym(X)$ É DENOTADO Sym_n (OU S_n) O GRUPO DAS PERMUTAÇÕES DE n ELEMENTOS (CADA ELEMENTO $f \in Sym_n$ É UMA PERMUTAÇÃO DO CONJUNTO X).

SUPONHA $X = \{1, 2, \ldots, n\}$.

PODEMOS REPRESENTAR ELEMENTO DE S_n DA SEGUINTE FORMA:

Ex: $f: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ INDICANDO QUE $1 \mapsto 2$; $2 \mapsto 3$; $3 \mapsto 2$ ($f(1)=2$; $f(2)=3$; $f(3)=2$).

DAÍ $f^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}$

OU NA NOTAÇÃO DE CICLOS: $(1\,2\,3) = (3\,1\,2) = (2\,3\,1)$

$id = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$.

COMO EFETUAMOS O "PRODUTO" EM S_n?

EX: $\sigma, \tau \in S_n$. $\sigma\tau$ SIGNIFICA APLIQUE τ PRIMEIRO E A ESTE RESULTADO APLIQUE σ.

Sejam $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$, $\sigma, \tau \in S_5$.

$\sigma\tau(1)$: $1 \xmapsto{\tau} 3 \xmapsto{\sigma} 1$

$\sigma\tau(2)$: $2 \xmapsto{\tau} 4 \xmapsto{\sigma} 5$

$\therefore \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix}$.

DEF: SEJAM $i_1, i_2, \ldots, i_k$ k INTEIROS DISTINTOS EM $X = \{1, 2, \ldots, n\}$

O SÍMBOLO $(i_1\ i_2 \ldots i_k)$ REPRESENTARÁ A PERMUTAÇÃO $\sigma \in S_n$ ONDE $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\ldots$, $\sigma(i_j) = i_{j+1}$, PARA $j < k$ e $\sigma(i_k) = i_1$.

EX: EM S_7, A PERMUTAÇÃO $(1\ 3\ 5\ 4)$ É A PERMUTAÇÃO

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 1 & 4 & 6 & 7 \end{pmatrix}$$

UMA PERMUTAÇÃO DA FORMA $(i_1\ i_2 \ldots i_k)$ É UM **k-CICLO**.
(OU CICLO DE COMPRIMENTO k)

- UM CICLO DE COMPRIMENTO 2 É CHAMADA UMA TRANSPOSIÇÃO.
  (i_1, i_2) É UMA TRANSPOSIÇÃO.
- UM k-CICLO E UM m-CICLO SÃO DISJUNTOS SE ELES NÃO POSSUEM INTEIROS EM COMUM.

EX: EM S_7, $(1\,2\,3)$ E $(4\,5)$ SÃO DISJUNTOS.

Ex: S_3

$S_3 = \{ Id, \sigma_2 = (12), \sigma_3 = (13), \sigma_4 = (23), \sigma_5 = (123), \sigma_6 = (132) \}$.

	Id	(12)	(23)	(13)	(123)	(132)
Id	Id	(12)	(23)	(13)	(123)	(132)
(12)	(12)	Id				
(23)	(23)					
(13)	(13)					
(123)	(123)					
(132)	(132)					

(

Ex: S_3

$S_3 = \{ Id, \sigma_2 = (12), \sigma_3 = (13), \sigma_4 = (23), \sigma_5 = (123), \sigma_6 = (132) \}$.

	Id	(12)	(23)	(13)	(123)	(132)
Id	Id	(12)	(23)	(13)	(123)	(132)
(12)	(12)	Id	(123)	(132)	(23)	(13)
(23)	(23)	(132)	Id	(123)	(13)	(12)
(13)	(13)	(123)	(132)	Id	(12)	(23)
(123)	(123)	(13)	(12)	(23)	(132)	Id
(132)	(132)	(23)	(13)	(12)	Id	(123)

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$

$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$

$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$

$\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$

$\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$

$(23)(12) = (132)$

$(13)(12) = (123)$

$(123)(12) = (13)$

$(132)(12) = (23)$

$(12)(23) = (231) = (123)$

$(13)(23) = (213) = (132)$

$(123)(23) = (21) = (12)$

$(132)(23) = (31) = (13)$

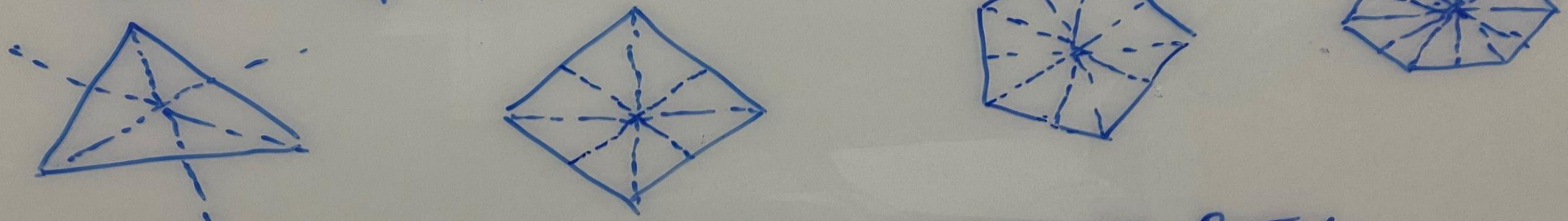
$(12)(13) = (132)$

$(132)(123) = Id$

GRUPOS DIEDRAIS:

$n \geq 3$, D_n O GRUPO DIEDRAL É DEFINIDO COMO OS MOVIMENTOS RÍGIDOS LEVANDO UM POLÍGONO REGULAR DE n LADOS PARA SI MESMO, COM A OPERAÇÃO SENDO COMPOSIÇÃO.

CASOS $n = 3, 4, 5, 6$



REFLETIMOS O POLÍGONO AO LONGO DAS RETAS PONTILHADAS

UM POLÍGONO REGULAR DE n LADOS PODE SER ROTACIONADO AO REDOR DO SEU CENTRO EM n DIFERENTES MODOS PARA RETORNAR A SI MESMO.

(ROTACIONE O MESMO AO REDOR DO SEU CENTRO POR $\frac{2k\pi}{n}$ rad)

ONDE $n = 0, 1, 2, \ldots, n-1$

TEMOS n ROTAÇÕES.

COM RELAÇÃO AS REFLEXÕES:

SE n É ÍMPAR, EXISTE UMA REFLEXÃO AO LONGO DA RETA CONECTANDO CADA VÉRTICE AO PONTO MÉDIO DO LADO OPOSTO.

TEMOS UM TOTAL DE n REFLEXÕES (UMA PARA CADA VÉRTICE)

ELAS SÃO DIFERENTES BIS OS VÉRTICES SÃO DIFERENTES.

· n PAR: EXISTE UMA REFLEXÃO AO LONGO DA RETA CONECTANDO CADA PAR DE VÉRTICES OPOSTOS ($\frac{n}{2}$ REFLEXÕES) E AO LONGO DA RETA CONECTANDO OS PONTOS MÉDIOS DOS LADOS OPOSTOS (OUTROS $\frac{n}{2}$ REFLEXÕES).

O NÚMERO DE REFLEXÕES É: $\frac{n}{2} + \frac{n}{2} = n$ REFLEXÕES. ELAS SÃO DIFERENTES PORQUE POSSUEM DIFERENTES TIPOS DE PONTOS FIXADOS NO POLÍGONO: DIFERENTES PARES DE VÉRTICES OPOSTOS OU DIFERENTES PARES DE PONTOS MÉDIOS DE LADOS OPOSTOS.

- AS ROTAÇÕES E REFLEXÕES SÃO DIFERENTES EM D_n:

. UMA ROTAÇÃO (DIFERENTE DA IDENTIDADE) NÃO FIXA NENHUM PONTO DO POLÍGONO.

.. A ROTAÇÃO IDENTIDADE FIXA TODOS OS PONTOS DO POLÍGONO

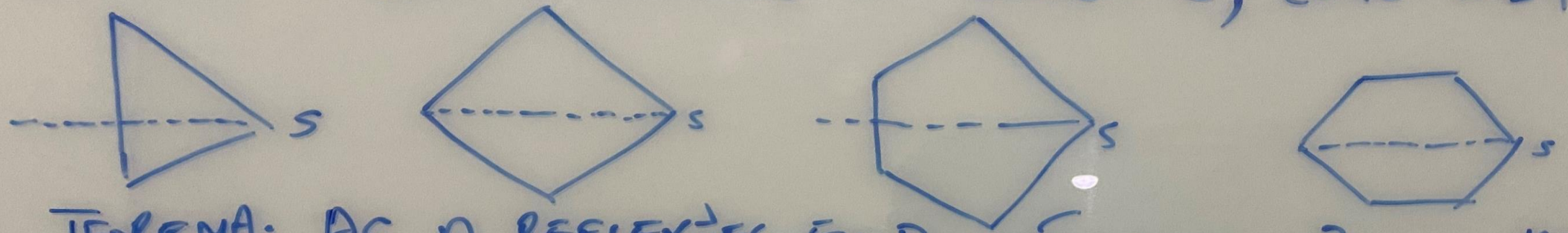
... UMA REFLEXÃO FIXA DOIS PONTOS DO POLÍGONO.

EM D_n, USUALMENTE r DENOTA ROTAÇÃO NO SENTIDO ANTI-HORÁRIO POR $\frac{2\pi}{n}$.

TEOREMA: AS n ROTAÇÕES EM D_n SÃO $1, r, r^2, \ldots, r^{n-1}$.

Dem: (CLARO, POIS R TEM ORDEM n).

SEJA s REFLEXÃO AO LONGO DA RETA ATRAVÉS DE UM VÉRTICE. UMA REFLEXÃO TEM ORDEM 2, LOGO $s^2 = 1$ e $s = s^{-1}$.

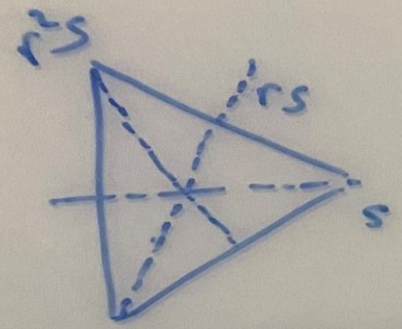


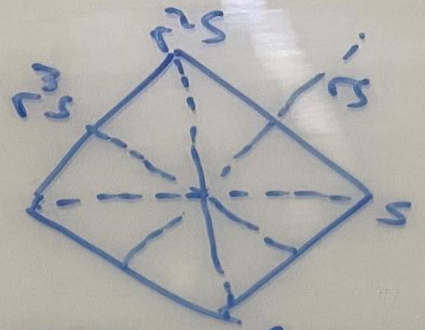
TEOREMA: AS n REFLEXÕES EM D_n SÃO $s, rs, r^2s, \ldots, r^{n-1}s$.

DEM: OS MOVIMENTOS RÍGIDOS $s, rs, r^2s, \ldots, r^{n-1}s$ SÃO DIFERENTES POIS $1, r, r^2, \ldots, r^{n-1}$ SÃO DIFERENTES E NÓS APENAS MULTIPLICAMOS A DIREITA POR s.

NENHUM $r^k s$ É UMA ROTAÇÃO, POIS SE $r^k s = r^l \Rightarrow s = r^{l-k}$ MAS s NÃO É ROTAÇÃO. ABC.

COMO D_n POSSUI n ROTAÇÕES E n REFLEXÕES E NENHUM $r^k s$ É UMA ROTAÇÃO, CONCLUÍMOS QUE ELES SÃO TODOS REFLEXÕES.





INTERPRETAÇÃO GEOMÉTRICA:

DESENHE TODAS AS RETAS DE REFLEXÕES PARA UM POLÍGONO REGULAR DE n LADOS. É MOVENDO NO SENTIDO ANTI-HORÁRIO AO REDOR DO POLÍGONO INICIANDO PELO UM VÉRTICE FIXADO POR S, NOS OBTEMOS SUCESSIVAMENTE AS RETAS FIXADAS POR $rs, r^2s, \dots, r^{n-1}s$

RESUMINDO:

TEOREMA: O GRUPO D_n POSSUI $2n$ ELEMENTOS.

$$D_n = \{1, r, r^2, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}.$$

TODOS OS ELEMENTOS DE D_n COM ORDEM MAIOR QUE 2 SÃO POTÊNCIAS DE r.

TEOREMA: EM D_n: $srs^{-1} = r^{-1}$.

DEM: rs É REFLEXÃO $\longrightarrow (rs)^2 = 1 \longrightarrow rsrs = 1 \longrightarrow srs^{-1} = r^{-1}$

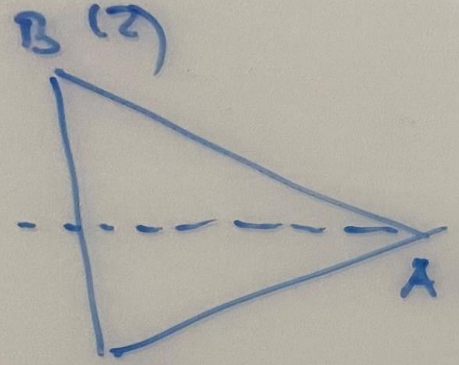
(pois $s^2 = 1$, $s = s^{-1}$

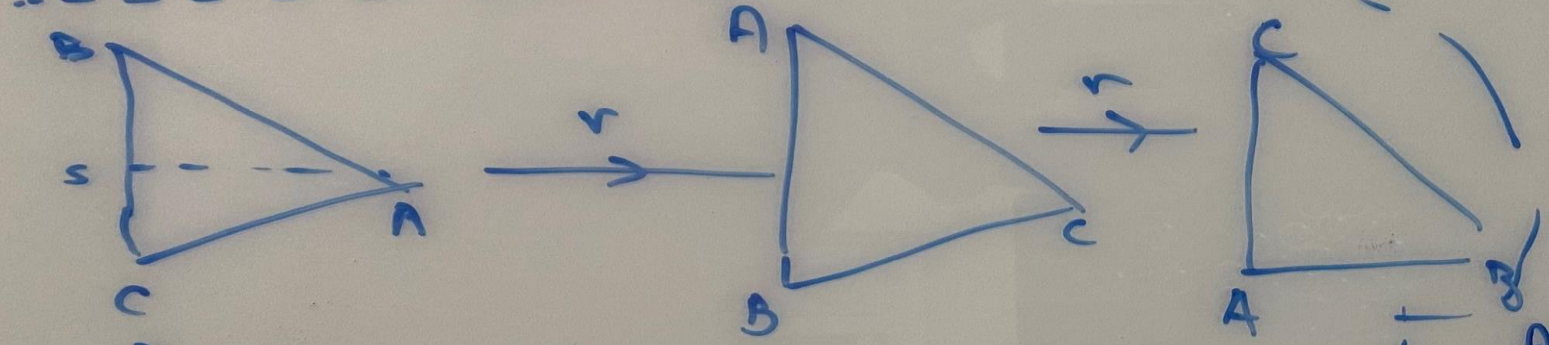
D_n É O GRUPO DIEDRAL DE ORDEM $2n$. ■

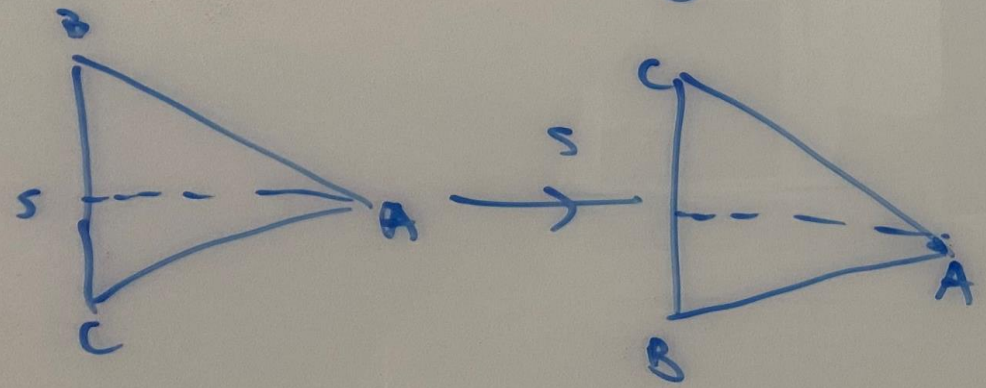
DEF: SEJA G GRUPO. DEFINIMOS O CENTRO DE G DENOTADO $Z(G)$, COMO $Z(G) = \{x \in G \mid ax = xa, \forall a \in G\}$.

DEF: SEJA G GRUPO, $H \leq G$, definimos o CENTRALIZADOR DE H EM G, DENOTADO $C_G(H)$, COMO $C_G(H) = \{x \in G \mid xh = hx, \forall h \in H\}$.

MOSTRE QUE $Z(G)$ e $C_G(H)$ SÃO SUBGRUPOS DE G.







	1	2	3	
1	A	B	C	Id
r	C	A	B	(2 1 3)
r^2	B	C	A	(1 2 3)
Δ	A	C	B	(2 3)
$r\Delta$	B	A	C	(1 2)
$r^2\Delta$	C	B	A	(1 3)

A CADA SIMETRIA CORRESPONDE UMA PERMUTAÇÃO

P. EX: r LEVA ABC EM CAB e temos (132)

GRUPOS CÍCLICOS:

PROP: SEJA G GRUPO, a INTEIRO NÃO-NULO

(i) SE $|x| = \infty$ ENTÃO $|x^a| = \infty$.

(ii) SE $|x| = n < +\infty$ ENTÃO $|x^a| = \dfrac{n}{mdc(n,a)}$.

(iii) EM PARTICULAR, SE $|x| = n < \infty$ E a FOR UM INTEIRO POSITIVO $a|n$. ENTÃO $|x^a| = \dfrac{n}{a}$.

LEMA: SEJA G GRUPO, SUPONHA $x^m = 1$ e $x^n = 1$, PARA ALGUNS $m, n \in \mathbb{Z}^*$, $x \in G$. ENTÃO $x^d = 1$, ONDE $d = mdc(m,n)$. EM PARTICULAR, SE $x^m = 1$ PARA ALGUM $m \in \mathbb{Z}$. ENTÃO $|x|$ DIVIDE m.

DEM (PROP): (i) SUPONHA $|x| = \infty$, MAS $|x^a| = m < \infty$.

$\therefore (x^a)^m = x^{am} = e.$

e $(x^{-a})^m = x^{-am} = (x^{am})^{-1} = e^{-1} = e.$

Logo ou am ou $-am$ é NÃO NULO, (pois $a \neq 0$ e $m \neq 0$).
LOGO ALGUMA POTÊNCIA DE x É A IDENTIDADE. ABS.

(ii) SEJAM $y = x^a$, $d = mdc(n, a)$.

como $d = mdc(n, a) \longrightarrow d|n \longrightarrow n = db$, para algum $b \in \mathbb{Z}$, $b > 0$

$d|a \rightarrow a = dc$, para algum $c \in \mathbb{Z}$,

e $mdc(b, c) = 1$.

TEMOS DE MOSTRAR QUE $|y| = b$.

$y^b = (x^a)^b = x^{ab} = x^{dcb} = (x^{db})^c = (x^n)^c = e^c = e$

∴ Lema $\longrightarrow$ $|y| \mid b$.

DEM SEJA $K = |y|$. ENTÃO $(x^a)^K = x^{aK} = y^K = e$

$\xrightarrow{\text{LEMA}}$ $n \mid aK \longrightarrow db \mid dck \longrightarrow b \mid ck$ $\left\{ \begin{array}{l} \xrightarrow{\text{BEZOUT}} b \mid K \\ mdc(b,c)=1 \end{array} \right.$

Como b, b SÃO INTEIROS POSITIVOS, $K \mid b$ e $b \mid K \longrightarrow \boxed{b = K}$ □.

(ii) SEJAM $y = x^a$, $d = mdc(n, a)$.

como $d = mdc(n,a) \longrightarrow d \mid n \longrightarrow n = db$, para algum $b \in \mathbb{Z}$, $b \neq 0$

$d \mid a \longrightarrow a = dc$, para algum $c \in \mathbb{Z}$,

e $mdc(b,c) = 1$.

TEMOS DE MOSTRAR QUE $|y| = b$.

$y^b = (x^a)^b = x^{ab} = x^{dcb} = (x^{db})^c = (x^n)^c = e^c = e$

$\xrightarrow[\text{Lema}]{}$ $|y| \mid b$.

LEMA: $x^m = e$, $x^n = e$, $d = mdc(m,n) \Rightarrow x^d = e$.

Dem: $d = mdc(m,n) \xrightarrow{\text{BEZOUT}} d = rm + sn$, p/ alguns $r, s \in \mathbb{Z}$

$$\therefore x^d = x^{rm+sn} = x^{rm} \cdot x^{sn} = (x^m)^r \cdot (x^n)^s = e.$$

- Suponha agora $x^m = e$, SEJA $n = |x|$.

  SE $m = 0$ ENTÃO CLARAMENTE $n \mid m$.

  SUPONHA $m \neq 0$. COMO ALGUMA POTÊNCIA DE x É A IDENTIDADE, $n < \infty$.

  SEJA $d = mdc(m,n)$ ENTÃO $x^d = e$, com $0 < d \leq n$.

  COMO d É A MENOR POTÊNCIA POSITIVA DE x QUE DÁ A IDENTIDADE, DEVEMOS TER $d = n$, ie $n \mid m$.

PROP: SE $G = \langle x \rangle$ ENTÃO $|G| = |x|$.

(1) SE $|G| = n < \infty$ ENTÃO $x^n = e$ E $e, x, x^2, \ldots, x^{n-1}$ SÃO TODOS OS ELEMENTOS DISTINTOS DE G.

(2) SE $|G| = \infty$ ENTÃO $x^n \neq e$, $\forall n \neq 0$, E $x^a \neq x^b$, $\forall a \neq b$ em $\mathbb{Z}$.

DEM: SE $|G| = n < \infty$.

. OS ELEMENTOS $e, x, x^2, \ldots, x^{n-1}$ SÃO TODOS DISTINTOS
SE $x^a = x^b$ P/ ALGUM $a, b \in \mathbb{Z}$, $0 \leq a < b < n$.
ENTÃO $x^{b-a} = e$. CONTRADIZENDO A MINIMALIDADE DE $n = |x|$.

∴ OS ELEMENTOS $e, x, x^2, \ldots, x^{n-1}$ SÃO TODOS OS ELEMENTOS DE G.
SEJA x^t POTÊNCIA DE x. PELO ALG. DA DIVISÃO:
$t = nq + k$, PARA ALGUM $q, k \in \mathbb{Z}$, $0 \leq k < n$.

$$\therefore x^t = x^{nq+k} = x^{nq} \cdot x^k = \underbrace{(x^n)}_{e}{}^q \cdot x^k = x^k \in \{e, x, \ldots, x^{n-1}\}$$

PROP: SE $G = \langle x \rangle$ ENTÃO $|G| = |x|$.

(1) SE $|G| = n < \infty$ ENTÃO $x^n = e$ E $e, x, x^2, \ldots, x^{n-1}$ SÃO TODOS OS ELEMENTOS DISTINTOS DE

(2) SE $|G| = \infty$ ENTÃO $x^n \neq e$, $\forall n \neq 0$, E $x^a \neq x^b$, $\forall a \neq b$ em $\mathbb{Z}$.

DEM: (2) SUPONHA $|G| = \infty$.

LOGO NENHUMA POTÊNCIA POSITIVA DE x É IGUAL A e.

SE $x^a = x^b$ PARA ALGUNS $a, b \in \mathbb{Z}$, $a < b$. ENTÃO

$x^{b-a} = e$. ABSURDO.

Prop: Seja $H = \langle x \rangle$, $a \in \mathbb{Z}$, $a \neq 0$.

(i) Suponha $|H| = m$. Então $H = \langle x^a \rangle \iff a = \pm 1$.

(ii) Suponha $|H| = n < m$. Então $H = \langle x^a \rangle \iff mdc(a, n) = 1$.
Em particular, o número de geradores de H é igual a $\phi(n)$, ϕ função phi de Euler.

Dem: (I) Observe que $\langle x \rangle = \langle x^{-1} \rangle$ $(= \{\dots, x^{-2}, x^{-1}, x^0, x, x^2, \dots\})$

$\langle e \rangle = \{e\} \neq H$.

Vimos que $x^i \neq x^j$ para $\forall i \neq j$

Seja $n \in \mathbb{Z}$, $n \neq 0$, $n \neq \pm 1$.

$\therefore \langle x^n \rangle = \{\dots, x^{-2n}, x^{-n}, e, x^n, x^{2n}, \dots\}$. Como $n > 1$, nenhum desses elementos é igual a x.

$\therefore x \notin \langle x^n \rangle \rightarrow \langle x \rangle \neq \langle x^n \rangle$.

PROP: SEJA $H = \langle x \rangle$, $a \in \mathbb{Z}$, $a \neq 0$.

(I) SUPONHA $|H| = \infty$. ENTÃO $H = \langle x^a \rangle \iff a = \pm 1$.

(II) SUPONHA $|H| = n < \infty$. ENTÃO $H = \langle x^a \rangle \iff mdc(a, n) = 1$.
EM PARTICULAR, O NÚMERO DE GERADORES DE H É IGUAL A $\phi(n)$, ϕ FUNÇÃO PHI DE EULER.

DEM: (II) SUPONHA $|x| = n < \infty$.
ENTÃO x^a GERA UM SUBGRUPO DE ORDEM $|x^a|$.
LOGO $H = \langle x^a \rangle \iff |x| = |x^a| \iff n = \frac{n}{mdc(n,a)} \iff mdc(a, n) = 1$.

COMO $\phi(n)$ É O NÚMERO DE INTEIROS ENTRE 1 E $n-1$ QUE SÃO RELATIVAMENTE PRIMOS COM n, CONCLUÍMOS QUE ESTE É O NÚMERO DE GERADORES DE H.

EX.: DETERMINE OS GERADORES DE $\frac{\mathbb{Z}}{12\mathbb{Z}}$ R: $(\bar{1}, \bar{5}, \bar{7}, \bar{11})$

TEOREMA: SEJA $H = \langle x \rangle$ GRUPO CÍCLICO.

(i) TODO SUBGRUPO DE H É CÍCLICO.

(MAIS EXPLICITAMENTE, $K \leq H$, OU $K = \{e\}$, OU $K = \langle x^d \rangle$ ONDE d É O MENOR INTEIRO POSITIVO, TAL QUE $x^d \in K$)

(ii) SE $|H| = \infty$. ENTÃO PARA QUAISQUER INTEIROS NÃO-NEGATIVOS DISTINTOS a, b; $\langle x^a \rangle \neq \langle x^b \rangle$. ALÉM DISSO, PARA TODO INTEIRO m, $\langle x^m \rangle = \langle x^{|m|} \rangle$ ONDE m É O MÓDULO DO INTEIRO m.

(iii) SE $|H| = n < \infty$, ENTÃO PARA CADA INTEIRO POSITIVO a dividindo n. EXISTE UM ÚNICO SUBGRUPO DE H DE ORDEM a.

(ESTE SUBGRUPO É O GRUPO CÍCLICO $\langle x^{\frac{n}{a}} \rangle$. ALÉM DISSO, PARA TODO INTEIRO m, $\langle x^m \rangle = \langle x^{mdc(m,n)} \rangle$.)

DEM: SEJA $K \leq H$. SE $K = \{e\}$ OK ✓

SUPONHA $K \neq \{e\}$.

LOGO EXISTE ALGUM $a \in \mathbb{Z}$, $a \neq 0$, t.q $x^a \in K$.

(SE $a < 0$, COMO K É SUBGRUPO, $x^{-a} = (x^a)^{-1} \in K$. LOGO K SEMPRE POSSUI ALGUMA POTÊNCIA POSITIVA DE x)

SEJA $\beta = \{ b \mid b \in \mathbb{Z}^+ \text{ e } x^b \in K \}$.

$\beta \neq \emptyset$, β É CONJUNTO DE INTEIROS LIMITADO INFERIORMENTE

$\therefore$ PELO PRINCÍPIO DE BOA ORDEM EXISTE $d = \min \beta \in \beta$.

COMO $x^d \in K$, $\langle x^d \rangle \leq K$.

COMO $K \in H$, TODO ELEMENTO DE K É DA FORMA x^a, PARA ALGUM $a \in \mathbb{Z}$

PELO ALG. DA DIVISÃO, $a = dq + r$, P/ ALGUNS $q, r \in \mathbb{Z}$, $0 \leq r < d$

$\therefore \underbrace{x^a}_{\in K} = x^{dq+r} = \underbrace{(x^d)^q}_{\in K} \cdot x^r$, DA MINIMALIDADE DE d,

TEMOS $r = 0 \rightarrow a = dq \rightarrow x^a = (x^d)^q \in \langle x^d \rangle$

$\therefore K \leq \langle x^d \rangle$.

(b) EXERCÍCIO

(c) $|H| = n$, $a \mid n$.

SEJA $d = \frac{n}{a}$. PELO QUE VIMOS $|\langle x^d \rangle| = a$, O QUE PROVA A EXISTÊNCIA DE UM SUBGRUPO DE ORDEM a.

.. UNICIDADE:

SUPONHA K SUBGRUPO QUALQUER DE H, $|K| = a$.

VIMOS POR (1) QUE $K = \langle x^b \rangle$ ONDE b É O MENOR INTEIRO POSITIVO T.Q $x^b \in K$.

$\therefore$ $|K| = |x^b|$

$\therefore$ $a = |K| = |x^b| = \frac{n}{mdc(n,b)}$

$\therefore$ $\frac{n}{d} = a = \frac{n}{mdc(n,b)}$ $\longrightarrow$ $d = mdc(n,b)$

$\therefore$ $d \mid b \longrightarrow x^b \in \langle x^d \rangle \longrightarrow K = \langle x^b \rangle \leq \langle x^d \rangle$

Como $|\langle x^d \rangle| = a = |K| \longrightarrow K = \langle x^d \rangle$.

· OBSERVE QUE $\langle x^m \rangle \leq \langle x^d \rangle$ onde $d = mdc(m,n)$.

Como $|\langle x \rangle| = n$.

$d = mdc(m,n) \rightarrow d \mid m \longrightarrow m = dq$, p/algum $q \in \mathbb{Z}$

$\therefore x^m = x^{dq} = (x^d)^q$

$\therefore x^m \in \langle x^d \rangle \longrightarrow \langle x^m \rangle \leq \langle x^d \rangle$.

MAS $|\langle x^m \rangle| = \frac{n}{mdc(n,m)} = \frac{n}{d} = \frac{n}{mdc(n,d)} = |\langle x^d \rangle|$

$\therefore \langle x^m \rangle = \langle x^d \rangle$.

Exemplo: (a) $\frac{\mathbb{Z}}{12\mathbb{Z}} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$. ordem 12

$\langle \bar{2} \rangle = \langle \bar{10} \rangle$ ordem 6

$\langle \bar{3} \rangle = \langle \bar{9} \rangle$ ordem 4

$\langle \bar{4} \rangle = \langle \bar{8} \rangle$ ordem 3

$\langle \bar{6} \rangle$ ordem 2

$\langle \bar{0} \rangle$ ordem 1

· $\langle \bar{a} \rangle \leq \langle \bar{b} \rangle$

$\Updownarrow$

$mdc(b,12) \mid mdc(a,12)$