Geradores

Seja G um grupo & $I \subset G$ um subconjunto

Grupo gerado por X é $\bigcap \left\{ H \,\middle|\, \begin{array}{l} H \text{ subgrupo de} \\ G,\ X \subset H \end{array} \right\}$

& é denotado por $\langle X \rangle$ é o menor subgrupo de G que contém X. Uma caracterização de $\langle X \rangle = \left\{ g_{i_1}^{s_1} \cdots g_{i_n}^{s_n} \,\middle|\, \begin{array}{l} g_{i_j} \in X \\ s_i = \pm 1 \end{array} \right\} \rightarrow V$

#

$g_{i_1}^{3} = g_{i_1}^{1} \cdot g_{i_1}^{1} \cdot g_{i_1}^{1}$ & $g_{i_1}^{-2} = g_{i_1}^{-1} \cdot g_{i_1}^{-1}$

($\mathbb{Z}$ é discreto) #

Prova (de que é um grupo)

Suponha que $X \subset H$, H subgrupo de G

(1) $\cdot\ V \subset H \longrightarrow V \subset \bigcap \left\{ H \,\middle|\, \begin{array}{l} X \subset H \\ H \text{ subgrupo de } G \end{array} \right\}$

(2) $\cdot\ V$ é um grupo de $G \longrightarrow X \subset V = \langle X \rangle$

$X \subset H \longrightarrow$ se $g_{i_j} \in X \Rightarrow g_{i_j} \in H \Rightarrow g_{i_j}^{-1} \in H$

$\Rightarrow \{g_{ij}, g_{ij}^{-1} \mid g_{ij} \in X\} \subset H$

Logo produtos destes elementos continuam em H. Logo $V \subset H$

V é subgrupo:

1) $V \supset X \neq 0 \Rightarrow V \neq \emptyset$

2) $g \in V \Rightarrow g = g_{i_1}^{s_1} \cdots g_{i_k}^{s_k}$

$g^{-1} = g_{i_k}^{-s_k} \cdots g_{i_1}^{-s_1}$

$s_n = \pm 1 \Rightarrow -s_n = \pm 1$. Logo, $g \in V$

$y = g_{i_1}^{t_1} \cdots g_{i_m}^{t_m}$, $t_i = \pm 1$

$$g \cdot y = \underbrace{g_{i_1}^{s_1} \cdots g_{i_k}^{s_k} \, g_{j_1}^{t_1} \cdots g_{j_m}^{t_n}}_{\substack{t_i = \pm 1 \\ s_j = \pm 1}}$$

$g \cdot y \in V$

Logo V é subgrupo de G (notação $V < G$)

Lema: Seja $X \subset G$ ñ vazio. Então

$$\langle X \rangle = \left\{ g \in G \;\middle|\; \begin{array}{l} g = g_{i_1}^{s_1} \cdots g_{i_k}^{s_k} \\ |s_i| = 1 \quad g_{i_j} \in X \end{array} \right\}$$

Um conjunto de geradores S de G é dito simétrico se $g \in S \Rightarrow g^{-1} \in S$.
No caso de um conjunto simétrico de gerador S tem-se

$$\langle S \rangle = \left\{ g \in G \;\middle|\; \begin{array}{l} g = g_{i_1} \cdots g_{i_n} \\ g_{i_1} \in S \end{array} \right\}$$

$S = \{ g_1, g_2, g_3 \}$

$\cancel{\langle S \rangle}$ $\quad S = \{ g_1, g_2 \}$

$$\langle S \rangle \supseteq \underbrace{\{ g_1^k g_2^s \mid k, s \in \mathbb{Z} \}}$$

não sei se é subgrupo

por exemplo $g_2 g_1 \in A$ ele?

Se $|G| < \infty$ & $g \in G \Rightarrow o(g) \mid |G| \Rightarrow$
$o(g) \geq 1$ & $g \cdot \underbrace{g^{o(g)-1}}_{g^{-1}} = g^{o(g)} = e$ ou seja $g^{-1} = g^{o(g)-1}$

& $o(g)-1 > 0$, ou seja, a inversa de g é uma potência positiva de g. ISO

<u>Exemplos</u>

$G_1 = (\mathbb{R}, +)$
$G_2 = (\mathbb{R}^*_+, \cdot)$

& defina $\psi : G_{\cancel{2}1} \longrightarrow G_{\cancel{1}2}$ por

$\psi(x) = e^x$

ψ é um isomorfismo de grupos

& $\phi : G_{\cancel{1}2} \longrightarrow G_{\cancel{2}1}$
$\phi(x) := \ln x$ é A

Sua inversa

$$\psi(x+y) = e^{x+y} = e^x e^y = \psi(x)\psi(y)$$

$x \in \ker\psi \Rightarrow \psi(x) = 1 \Rightarrow e^x = 1 \Rightarrow x = 0$
$\Rightarrow \ker\psi = \{0\}$ & logo ψ é 1-1 $\longrightarrow$ injetora

$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $\quad \rho : \cancel{\mathbb{Z}} \longmapsto \langle g \rangle$

$\rho(n) = g^n \qquad (\mathbb{Z}, +)$

é ISOMORFISMO

$g = I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

$g^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

$\rho(n+m) = g^{n+m} = g^n \cdot g^m = \rho(n)\rho(m)$

Logo ρ é homomorfismo.

$<g> = \{g^n \mid n \in \mathbb{Z}\}$

Logo se $x \in <g> \Rightarrow \exists\, n$ tq $x = g^n = \rho(n)$

Logo $x \in Im(\rho)$. Daí ρ é sobrejetora

$\Rightarrow$ $n \in \ker(\rho)$

$\rho(n) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = g^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

Daí $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow n = 0 \rightarrow \ker\rho = \{0\}$

ρ é 1-1

<u>Alg. I</u>

$G = (\mathbb{Z}, +)$. Como são os subgrupos de G?

<u>Ideal de $\mathbb{Z}$</u>: É um $I \subset \mathbb{Z}$

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

um ideal é um subgrupo de $(\mathbb{Z}, +)$

Resposta: são todos do tipo $n\mathbb{Z} = \{nh \mid h \in \mathbb{Z}\} \leq \mathbb{Z}$

para $n \in \mathbb{N}$.

fixe $n_0 \in \mathbb{N}$ & olhe para congruência módulo n_0 $\quad x, y \in \mathbb{Z} \quad x \sim y \pmod{n_0} \iff$

$n_0 \mid (x-y) \iff x - y \in n_0\mathbb{Z}$

$(\mathbb{Z}, +) \ni x \sim y \iff (x-y)\, n_0\mathbb{Z}$ ← Subgrupo

$x + y^{-1}$

$$\boxed{x \sim y \iff x * y^{-1} \in H}$$ Teo de Lagr.

O número de classes laterais de H em G é $[G:H]$

Alg I: as classes são $\{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n_0 - 1}\}$

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

$\bar{x} + \bar{y} = ? \quad \bar{x} \cdot \bar{y} = ! \quad \bar{y}^{-1} = !$