$(G, \cdot)$ $a \in G$ definimos

identidade

$\text{ord}(a) = \min\{ \overset{\in \mathbb{N}}{k} > 0 \mid \text{tq } \underbrace{a \cdots a}_{k} = e \}$

Caso exista o mínimo

Caso contrário $\text{ord}(a) = \infty$.

$(\mathbb{Z}, +)$ grupo $0 \to$ elemento identidade

Se $n \in \mathbb{Z}^*$ $\text{ord}(n) = \infty$

$\mathbb{Z} = \langle 1 \rangle$ $\to$ grupo cíclico gerado por 1.

$(\mathbb{Q}, +)$ é um grupo com todos os elementos $\neq 0$ de ordem infinito

$\to$ Não é cíclico.

---

3 pag 180

a $(\mathbb{Z}_{18}, +)$ $\text{ord}(a) = \text{ord}(-a)$

1, 2, 3, 4, 5, 6, 7, 8, 9

$$\underbrace{3+\cdots+3}_{n} = 3n \equiv 0 \bmod 18 \qquad \boxed{n=6}$$

$$\mathrm{ord}_{\mathbb{Z}_{18}}(3) = 6$$

$$\underbrace{8+8+\cdots+8}_{n} = 8n \equiv 0 \bmod 18 \qquad \Rightarrow n=9$$

$$\Downarrow$$

$$4n \equiv 0 \bmod 9$$

$$\mathrm{ord}_{\mathbb{Z}_{18}}(8) = 9$$

(b) $D_n = \left\langle a, b \;\middle|\; a^n = 1,\ b^2 = 1,\ ab = ba^{-1} \right\rangle$

2n elementos

$$(ab)(ab) = (ba^{-1})(ab) = b^2 = 1$$

$$\mathrm{ord}(ab) = 2$$

$$(a^j b)(a^j b) \qquad j = 0, \dots n-1$$

$$(ba^{-j})(a^j b) = b^2 = 1$$

$$\mathrm{ord}(a^j b) = 2 \qquad \forall j$$

$\mathrm{ord}(a^j) = ??$ $\qquad \underbrace{a^j \cdots a^j}_{k} = e$

$\Rightarrow a^{jk} = e \iff n$ divide jk

$\iff \dfrac{n}{(n,j)}$ divide $\dfrac{j}{(n,j)} \cdot k$

primos entre si

$\iff \dfrac{n}{(n,j)}$ divide k

$k = \dfrac{n}{(n,j)} \Rightarrow \mathrm{ord}(a^j) = \dfrac{n}{(n,j)}$

(c) S_n é grupo de permutações de n elementos, i.e, bijeções

$\sigma : \{1, 2, \ldots, n\} \to \{1, \ldots, n\}$

forma um grupo com a composição de funções

$1 \xrightarrow{\quad n \quad}$

$2 \xrightarrow{\times(n-1)}$

$3 \xrightarrow{\times(n-2)}$

$\vdots \qquad \vdots$

$n \qquad \times 1$

$\{1, 2, \ldots, n\}$

$\#$ permutações é $n!$

$\mathbb{Z}_n$ inteiros modulo n

$$U_n = U(\mathbb{Z}_n) = \{a \mid \exists\, b \in \mathbb{Z}_n \text{ tal que } ab \equiv 1 \bmod n\}$$

(*)

$$\boxed{\begin{array}{c} ax \equiv 1 \bmod n \quad \text{tem solução} \\ \Updownarrow \\ (a,n) = 1 \end{array}}$$

Teorema Bezout: Se $(n,m) = d$ então existem $a, b \in \mathbb{Z}$ tal que $\mathrm{mdc}(n,m) = an + bm$

Prova: $\mathcal{C} = \{mx + ny > 0 \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{N}^*$

$\hookrightarrow$ $\mathcal{C}$ tem elemento mínimo

$d = \min \mathcal{C}$

Afirmação: $d = (n, m)$

2 passos: · (n,m) divide d pois

$\boxed{d = n x_0 + m y_0}$ (para enteiros x_0, y_0)

mas (n, m) divide n e m

$\Rightarrow (n, m)$ divide d ✓

Vejamos que $\underline{\underline{d}}$ divide $\underline{\underline{(n,m)}}$

Suponhamos falso, Logo d

ou NÃO divide $\underline{\underline{n}}$ ou m

Suponhamos que d não divide n
(o outro é simetrico)

$$n = qd + r \quad \text{com} \quad \underline{\underline{0}} < r < \underline{\underline{d}}.$$

$$0 < r = n - qd = n - q(n x_0 + m y_0)$$
$$= \underline{\underline{n}}(1 - q x_0) + \underline{\underline{m}}(-q y_0) \in \mathcal{C}$$

mas isto é contraditório pois d é o elemento mínimo de $\mathcal{C}$.

(*) Como $(a,n)=1 \Rightarrow \exists\, b,u \in \mathbb{Z}$ tais que $ab+nu=1$

$$ab+\underline{\underline{nu}} \equiv 1 \mod n \Rightarrow ab \equiv 1 \mod n$$

$$U_n = U(\mathbb{Z}_n) = \left\{ a \;\middle|\; \begin{array}{c} 0 \leq a \leq n-1 \\ (a,n)=1 \end{array} \right\}$$

$$|U_n| = \varphi(n)$$

Homomorfismos de Grupos

Def. Dados G H grupos, um homomorfismo $\psi: G \to H$ é uma função que satisfaz as seguintes propriedades

ⓐ $\psi(ab) = \psi(a)\psi(b)$

ⓑ $\psi(a^{-1}) = \psi(a)^{-1}$

Consequencias $\quad \psi(\underset{\in G}{e_G}) = \underset{\in H}{e_H}$

$\Downarrow$

Se $a^n = e$ $\quad e = \psi(a^n) = \psi(a)^n =$

Logo se $\operatorname{ord} a = n \Rightarrow \operatorname{ord} \psi(a)$ é um divisor de n

---

$C_n = \langle g \rangle \qquad g^n = e$

$$C_n \xrightarrow{\theta} \mathbb{Z}_n$$

$\to$ injetivo

$\to$ sobre

$g \longmapsto 1$

$g^k \longmapsto k$

Se $\theta(g^k) = \theta(g^l) \Rightarrow k \equiv l \mod n$

$k = l + ns \qquad s \in \mathbb{Z}$

$$\underline{\underline{g^k}} = g^{l+ns} = g^l \cdot (g^n)^s = \underline{\underline{g^l}}$$ injetivo

Def: Um homomorfismo que é uma bijeção é chamado de isomorfismo.

W, V espaços vetoriais

$(V, +)$ é um grupo (esquecendo a estrutura sobre o corpo)

$\mathcal{L} : V \to W$ transformação linear

$$\mathcal{L}(v_1 + v_2) = \mathcal{L}(v_1) + \mathcal{L}(v_2)$$

$$\mathcal{L}(-v_1) = -\mathcal{L}(v_2)$$

$\underline{\underline{+}}$

é um homomorfismo de grupo

$(\mathbb{Q}^*, \cdot)$ grupo

subgrupo gerado por 2

$\langle 2 \rangle = \{1, 2, 2^2, 2^3, \dots, 2^{-1}, 2^{-2} \dots \}$

$$\begin{aligned} \langle 2 \rangle &\longrightarrow (\mathbb{Z}, +) \\ 2^n &\longmapsto n \end{aligned}$$

Isomorfismo de grupos

$G \rightsquigarrow N \trianglelefteq G$ subgrupo normal

N é normal se $aN = Na$ $\forall a \in G$

$G/N = \{ \bar{a} \}$

$a \sim b \Leftrightarrow a \in bN$

$\Leftrightarrow ab^{-1} \in N$

$aN \bullet bN = a \cdot bN$

$$\begin{aligned} \varphi : G &\longrightarrow G/N \\ a &\longmapsto aN \end{aligned}$$

homomorfismo natural que é sobre.

Seja $\varphi : G \to H$ homomorfismo

$$\varphi(G) := \{ \varphi(g) \mid g \in G \} \subseteq H$$

$$\mathrm{Ker}(\varphi) := \{ g \in G \mid \varphi(g) = e \} \subseteq G$$

Núcleo

Afirmação: $\varphi(G)$ e $\mathrm{Ker}(\varphi)$ são subgrupos de H e G respectivamente

Prova: $x, y \in \varphi(G) \Rightarrow \exists\, g_1, g_2 \in G$ tal que $x = \varphi(g_1)$, $y = \varphi(g_2)$ $\Rightarrow xy = \varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2) \in \varphi(G)$

$\Rightarrow xy \in \varphi(G)$

$$\varphi(G) \ni \varphi(g_1^{-1}) = \varphi(g_1)^{-1} = x^{-1}$$

Logo $\varphi(G)$ é grupo

Sejam $g_1, g_2 \in \ker(\varphi)$

$\Leftrightarrow$ $\varphi(g_1) = e$, $\varphi(g_2) = e$ $\Rightarrow$ $\varphi(g_1)\varphi(g_2) = e$

$$\varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2)$$

$\Rightarrow$ $\underline{g_1 g_2} \in \ker(\varphi)$

$\Rightarrow$ $\varphi(g_1^{-1}) = \varphi(g_1)^{-1} = e^{-1} = \underline{\underline{e}}$

$\Rightarrow$ $\underline{g_1}^{-1} \in \ker(\varphi)$

$\Rightarrow$ $\ker(\varphi)$ é grupo $\square$

(b) $\ker(\varphi) \trianglelefteq G$ $\left(\text{é subgrupo normal}\right)$

Temos qe mostrar qe

$$\underbrace{a\ker(\varphi)}\; = \;\underbrace{\ker(\varphi)a} \quad \forall a \in \underline{G}$$

Seja $b \in \ker\varphi$ $\leftarrow$

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

$$= \psi(a)\cdot e\cdot \psi(a)^{-1} = \underline{e}$$

$$\Rightarrow \underline{aba^{-1}} \in \underline{\operatorname{Ker}\psi}$$

$$aba^{-1}a \in (\operatorname{Ker}\psi)a$$

$$ab \in (\operatorname{Ker}\psi)a \qquad \forall b \in \operatorname{Ker}\psi$$

$$\Rightarrow a(\operatorname{Ker}\psi) \subseteq (\operatorname{Ker}\psi)\cdot a$$

equivalentemente $\quad a(\operatorname{Ker}\psi) \supseteq (\operatorname{Ker}\psi)a$

Logo $\quad \operatorname{Ker}(\psi) \trianglelefteq G$

Logo $\dfrac{G}{\operatorname{Ker}(\psi)}$ é grupo

$$\begin{tikzcd}
G \arrow[r, "\psi"] \arrow[d, "\pi"'] & H \\
G/\operatorname{Ker}(\psi) \arrow[ur, dashed] &
\end{tikzcd}$$

Existe um homomorfismo "natural"

$$\frac{G}{\operatorname{Ker}\psi} \xrightarrow{\eta} H$$

$$a(\operatorname{Ker}\psi) \longmapsto \psi(a)$$

está bem definida???????

① Independe do representante

Suponhamos $a(\operatorname{Ker}\psi) = b(\operatorname{Ker}\psi)$

$\Rightarrow a^{-1}b(\operatorname{Ker}\psi) = \operatorname{Ker}\psi$

$\Leftrightarrow a^{-1}b \in \operatorname{Ker}\psi$

$\Leftrightarrow \psi(a^{-1}b) = e$

$\Leftrightarrow \psi(a)^{-1}\psi(b) = e$

$\Leftrightarrow \psi(a) = \psi(b)$

Logo independe do representante

$$\eta\big(a(\ker\psi)\cdot c(\ker\psi)\big) = \eta(a\cdot c\ker\psi)$$

Ker ψ é normal

$$= \psi(ac) = \psi(a)\,\psi(c)$$

$$= \eta(a(\ker\psi))\cdot\eta(c(\ker\psi))$$

$$\eta(a^{-1}(\ker\psi)) = \psi(a^{-1}) = \psi(a)^{-1}$$

$$= (\eta(a\ker\psi))^{-1}$$

Afirmação $\eta : \dfrac{G}{\ker(\psi)} \to H$

é injetivo.

Prova: se $\eta(a\ker\psi) = \eta(b\ker\psi)$

$$\Longleftrightarrow \psi(a) = \psi(b)$$

$$\Longleftrightarrow \psi(a\cdot b^{-1}) = e \Rightarrow ab^{-1} \in \ker\psi$$

$$\Rightarrow a \in b\ker\psi \Rightarrow a(\ker\psi) \subseteq b\ker(\psi)$$

Se tem o simétrico $\Rightarrow$ $a\ker\psi = b\ker\psi$

$\Rightarrow$ η é injetivo

1º Teorema de Isomorfismo de grupos

Seja $\psi : G \to H$ homomorfismo de grupo então

$$\eta : \frac{G}{\ker\psi} \longrightarrow \psi(G)$$

$$a(\ker\psi) \longmapsto \psi(a)$$

é um isomorfismo

- injetivo (OK) pelo anterior
- sobre (OK) pois trocamos H por $\psi(G)$

Aplicação: Seja G um grupo então G é isomorfo a um subgrupo de permutações

$$G \xrightarrow{\sigma} S_G$$
$$g \longmapsto \sigma_g : G \to G$$
$$h \longmapsto gh$$

é um homomorfismo do grupo

$$g_1 g_2 \longmapsto \sigma_{g_1 g_2} : G \to G$$
$$h \longmapsto g_1 g_2 h$$

$$g_1 \longmapsto \sigma_{g_1} : G \to G$$
$$h \longmapsto g_1 h$$

$$g_2 \longmapsto \sigma_{g_2} : G \longmapsto G$$
$$h \longmapsto g_2 h$$

$$\sigma_{g_1} \circ \sigma_{g_2}(h) = \sigma_{g_1}(\underline{g_2 h}) = g_1 g_2 h$$
$$= \sigma_{g_1 g_2}(h)$$
$$\forall h$$

Logo $\boxed{\sigma_{g_1} \circ \sigma_{g_2} = \sigma_{g_1 g_2}}$

$$\sigma_{g^{-1}}\sigma_g(h) = \sigma_{g^{-1}}(gh) = g^{-1}gh = eh^{\forall h}$$
$$= \sigma_e(h)$$

$$\sigma_{g^{-1}} \circ \sigma_g = \underline{\underline{id}}$$

Afirmação: $Ker(\sigma) = \{e\}$

Se $g \in G$ tal que $\sigma_g = id$

$\Leftrightarrow \sigma_g(h) = id(h) = h \quad \forall h$

$\Rightarrow gh = h \quad \forall h$

$\Rightarrow g = e$ ← Logo $Ker(\sigma) = \underline{\underline{\{e\}}}$

Pelo 1º teorema do isomorfismo

$$\underline{G} \cong \sigma(G) = Im(\sigma) \subseteq \underline{S_G}$$

↳ Teorema de Cayley

Pag 223-226 Homomorfismos

G que tem um # finito de subgrupos é finito

Se $|G| = n \Rightarrow$ # finito de subconjunto $|\mathcal{P}(G)| = 2^n$

todo subgrupo é subconjunto

$\Rightarrow$ # subgrupo $< 2^n$

Logo é finito //

Se G é infinito

- $a \in G$ t.q. $ord(a) = \infty$ ou $ord(a) < \infty$

$$\langle a \rangle \leq G$$

$$(\langle a \rangle, \cdot) \longrightarrow (\mathbb{Z}, +)$$

$$a^k \longmapsto k$$

mas $n\mathbb{Z}$ é subgrupo de $\mathbb{Z}$

e $n\mathbb{Z} \neq m\mathbb{Z}$ $\forall m \neq n$

Logo podemos subpor que todo elemento tem ordem finita

$\langle a_1 \rangle = H_1$ $\quad G \setminus H_1 \ni a_2$

$H_2 = \langle a_2 \rangle$

$\underline{G \setminus (H_1 \cup H_2)} \ni \underline{a_3}$ $\quad H_3 = \langle a_3 \rangle$

indutivamente

$$\underset{\text{infinito}}{G} \setminus (\underbrace{H_1 \cup H_2 \cup \cdots \cup H_k}_{\text{finito}}) \ni a_{k+1} \quad H_{k+1} = \langle a_{k+1} \rangle$$

Constreímos infinitos subgrupos

$$G = \{ (x_n) \mid x_n \in \underline{\underline{\mathbb{Z}_p}} \}$$

$$(x_n)_n + (y_n)_n = (x_n + y_n)_n$$

$\vec{x} = (x_1, x_2, x_3 \ldots -)$ $\quad p\vec{x} = (px_1, px_2, \ldots) = (0, \ldots)$