Permutações

lec 01
2025-03-19

$S_n \overset{\text{def}}{\equiv} (\{1,\dots,n\} \rightarrowtail\!\!\!\!\twoheadrightarrow \{1,\dots,n\}) \equiv \{ f : \{1,..,n\} \to \{1,\dots,n\} \mid f \text{ bij} \}$

injetiva — adjectivos — sobrejetiva

"de tipo"

t.q

↑ o conjunto de todas as bijeções de .. para ..

substantivo

$|S_n| \overset{?}{\equiv} n!$

↑ cardinalidade

análise combinatória

Exemplo (um membro de S_3)

$f : \{1,2,3\} \to \{1,2,3\}$

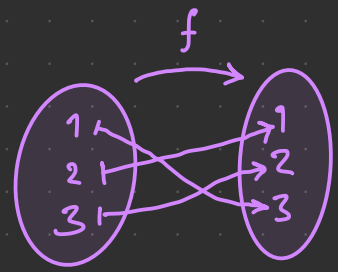
$f\ 1 \overset{\text{def}}{\equiv} 3$

$f\ 2 \overset{\text{def}}{\equiv} 1$

$f\ 3 \overset{\text{def}}{\equiv} 2$

$$f \overset{\text{def}}{\equiv} \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{matrix}$$

mapsto



Notação

Three → Three

« Seja $f \overset{\text{def}}{\equiv} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} : S_3 .$ »

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \sqcup 2 \cdot \text{Three}$

aplicação de função

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

$\overset{\text{sug}}{\equiv}$

$(1\ 3\ 2)$ — permutação cíclica $1 \mapsto 2 \mapsto 3$

$(1\ 3\ 2)\ 2 = 1$

$(1\ 3\ 2)\ 3 = 2$

$() \overset{\text{sug}}{\equiv} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \equiv (1\ 2)$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \overset{?}{\equiv} (1\ 2\ 4)(3\ 5)$

será que tem algo aqui?

S_3

(1 2)

(1 2 3)

(1 3 2)

(2 3)

(1 3)

( )

(2 3 1)

$op : S_3 \times S_3 \to S_3$

$op\ (a,b) \overset{def}{\equiv} \begin{cases} a\ ;\ b \\ a \circ b \end{cases}$ (?)

justaposição

$ab \overset{sug}{\equiv} op\ (a,b)$

$inv : S_3 \to S_3$

$inv\ (1\ 2) = (1\ 2)$

$inv\ (1\ 2\ 3) \overset{?}{=} (1\ 3\ 2)$

$$inv\ x\ ;\ x = id$$
$$x\ ;\ inv\ x = id$$

composição

$$\alpha \xrightarrow[f]{} \beta \xrightarrow[g]{} \gamma$$
$$g \circ f : \alpha \to \gamma$$
$$(g \circ f)\ a \overset{def}{\equiv} g\ (f\ a)$$

$id : S_3$

$id \equiv ( )$

igualdade (entre funções)

$$f =_{\alpha \to \beta} g \overset{def}{\iff} (\forall a : \alpha)[f\ a =_\beta g\ a]$$

Operações

operação n-ária do α : $\underbrace{\alpha \times \cdots \times \alpha}_{n \text{ vezes}} \to \alpha$

operação binária nos inteiros : $\text{Int} \times \text{Int} \to \text{Int}$

operação unária nos inteiros : $\text{Int} \to \text{Int}$

operação nulária nos inteiros ; Int ?

↳ aprofundamos em CFR

Grupos

lec02
2025-03-26

frame ou carrier set $\exists x \forall a\ a * x = a$

$* \quad e \quad {}^{-1}$

$\mathcal{G} \equiv (G ; op, id, inv)$ $\quad |\mathcal{G}| \overset{sug}{\equiv} \mathcal{G}.carrier \overset{def}{\equiv} G$ (o carrier set de $\mathcal{G}$)

$op : G \times G \to G$

$id : G$

$inv : G \to G$

Como assim «op é transitiva»?!

se $op(a,b)$ & $op(b,c)$ então $op(a,c)$ TYPE ERRORS

$$\frac{op : G \times G \to G \qquad (a,b) : G \times G}{op\ (a,b) : G}$$

leis / axiomas de grupos:

$op(op(a,b), c) =_G op(a, op(b,c))$

op-ass : $(\forall a,b,c : G)[\ (a * b) * c =_G a * (b * c)\ ]$ (*) é assoc.

id-idL : $id * a = a$ id é uma (*)-id-L

R : $a * id = a$ id é uma (*)-id-R

inv-invL : $inv\ a * a = id$ inv a é um (*)-inv-L de a

R : $a * inv\ a = id$

Exemplos & não exemplos

$(S_3 ; \circ, (), ^{-1})$ (Three >>> Three)..

$(\mathbb{R} ; \cdot, 1, \times)$

$(\mathbb{Z} ; +, 0, -_-)$ $\mathbb{Q}$ $\mathbb{R}$

Θ. Sejam $(G ; op : G \times G \to G)$.

Se existem $id : G$ e $inv : G \to G$ t.q. $(G ; op, id, inv)$ é grupo, então são únicos (são determinados pela $(G ; op)$).

Teoria dos grupos : Set Prop

Axiomas/Leis suas consequências (teoremas)

Teoria de ___ : Set Prop → Set Prop

Seja G : Group.

Agora temos acesso a todos os:

9 coisas!

- G.carrier : Type
- G.op : G.carrier × G.carrier → G.carrier
- ⋮
- G.op-ass. : (∀a, b, c : G.carrier)[(a * b) * c = a * (b * c)]
- ⋮

0. Existência & Unicidade da Identidade

Seja G grupo.

Existe único i t.q. i é uma $(*)$-id.

Existência: $(\exists i)(\forall g)[\, i * g = g \;\&\; g * i = g \,]$

Escolho e.

Imediato. $[\, G.idL \;;\; G.idR \,]$

proof by Fight Club

Unicidade: $(\forall u, v)[\, u, v \ (*)\text{-identidades} \Rightarrow u = v \,]$

Sejam u, v $(*)$-identidades.

-- ALVO : $u = v$

Calc:

$$u = u * v = v$$

$u = u * v$ — u é $(*)$-idL

$u * v = v$ — v é $(*)$-idR

de existência

Unicidade tendo uma testemunha w:

$(\forall u)[\, u \ (*)\text{-identidade} \Rightarrow u = w \,]$

Seja u $(*)$-identidade.

-- ALVO : $u = e$ — nossa testemunha aqui é o e

⋮

Grupo aditivo vs multiplicativo

lec 03

2025-04-02

$(G; +, 0, -_-)$

também por justaposição

$(G; \cdot, 1, _^{-1})$ $\quad ab \overset{\text{sug}}{\equiv} a \cdot b$

Evitamos o simbolo (+) para operações não comutativas!

também: $\overline{\cdot}$ $\quad \overline{g}$

buraco $\quad g^{-1}$

$(G, *_G, e_G, -^{-1}_G)$

$(G; op, id, inv)$

Abel: grupo comutativo

Seja G grupo.

G comutativo (ou abeliano) $\overset{\text{def}}{\iff} (\forall a, b : G)[\, ab = ba \,]$

$(\forall a, b : G.\text{carrier})[\, G.op(a, b) = G.op(b, a) \,]$

Como as ops comportam entre si

inv da id ?

$e^{-1} = e$

inv id = id

inv do inv ?

$(x^{-1})^{-1} = x$

inv (inv x) = x

inv do "produto" ?

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

inv (op a b) = ...

ALVO:

$e = e^{-1}$

• é o inverso de •

$e^{-1} = e$

• é a identidade

...

O que significa?

$\bullet\,\bullet \stackrel{?}{=} e$ & $\bullet\,\bullet \stackrel{?}{=} e$ (a identidade)

ou seja: $e\,e \stackrel{?}{=} e$

O que significa?

$\bullet\,x \stackrel{?}{=} x$ & $x\,\bullet \stackrel{?}{=} x$

Calc: $e\,e = e$ [G.IdL e] ∎

Cancelamento

$a\,x = y\,a \not\Rightarrow x = y$

⊖. $a\,x = a\,y \Rightarrow x = y$

$x\,a = y\,a \Rightarrow x = y$

$\dfrac{u = v}{f\,u = f\,v}$?

$(a^{-1}\cdot)$

Suponha $a\,x = a\,y$.

Logo $a^{-1}(a\,x) = a^{-1}(a\,y)$. [$(a^{-1}\cdot\_)$]

Logo $(a^{-1}\,a)\,x = (a^{-1}\,a)\,y$. [G.Ass a^{-1} a x ; G.Ass a^{-1} a y]

Logo $e\,x = e\,y$. [G.InvL a ; G.InvL a]

Logo $x = y$. [G.IdL x ; G.Id y]

↑ Demonstração claríssima!

Calc: $x = e\,x = (a^{-1}\,a)\,x = a^{-1}(a\,x) = a^{-1}(a\,y) = (a^{-1}\,a)\,y = e\,y = y$

↑ Nenhum mérito nisso!

Aplicar função nos dois lados

$$\frac{u = v}{f\,u = f\,v}\ f\_\ \ ?$$

$$\dfrac{\dfrac{}{f\,u = f\,u}\ \text{refl} \qquad u = v}{f\,u = f\,v}\ \text{Subs}$$

Id? Inv?

$$\frac{i\ a = a}{i \text{ identidade}}?$$

$$\frac{a\ u = e}{u \text{ é inverso de } a}?$$

$$\frac{i\ a = a \qquad a\ i = a}{i \text{ identidade}}?$$

θ. Identidades mais baratas

θ. Inversos mais baratos

0. Resoluções únicas

$$a \cdot u = t$$

qualquer um deles é determinado pelos outros dois:

$$\boxed{\exists!} \cdot u = t$$

$$a \cdot \boxed{\exists!} = t$$

$$a \cdot u = \boxed{\exists!}$$

Cayley Grupoku

lec04

2025-04-09

$(*) : G \times G \to G$

Quantas $(*)$ posso definir?

$e * e = ? \leftarrow e, a, b$

$e * a = ? \leftarrow e, a, b$

$e * b = ?$

$a * e = ?$

$\vdots$

$b * b = ? \leftarrow e, a, b$

$3^?$

*	e	a	b
e	?	? (ea)	?
a	? (ae)	?	?
b	?	?	?

*	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

e	a	b
a	b	e
b	e	a

$a * a = a$

$a * e = a$ (Res-!)

$a * e = a$

Desafio: (n>0?)

Dado $n : \mathbb{N}$, construir um grupo de ordem n.
(tamanho do carrier)

$n = 0$

$(*) : 0 \times 0 \to 0$
(0 equações aqui)

} definição mesmo!
(assoc. gratuitamente (vacuamente))

$inv : 0 \to 0$
(0 equações aqui)

} definição mesmo!
(...)

Potências

que tipo de expoentes?

g^n

$g^2 \overset{\text{def}}{=\!=} gg$

$g^n \overset{\text{"def"}}{=\!=} \underbrace{gg\cdots g}_{n \text{ vezes}}$

$n : \text{Nat}$ $\quad g^0 \overset{\text{def}}{=\!=} e$

$g^{Sn} \overset{n+1}{=\!=} \overset{\text{def}}{=\!=} g^n g$? $g g^n$

HW

$(\uparrow_1) =_{G\times\mathbb{N}\to G} (\uparrow_2)$

$\Updownarrow$

$(\forall g)(\forall n)[\, g \uparrow_1 n = g \uparrow_2 n \,]$

g^n com alt #1 = g^n com alt #2

Precisamos notações distintas!

$g \uparrow_1 0 \overset{\text{def}}{=\!=} e$

$g \uparrow_1 Sn \overset{\text{def}}{=\!=} (g \uparrow_1 n)\, g$

$g \uparrow_2 0 \overset{\text{def}}{=\!=} e$

$g \uparrow_2 Sn \overset{\text{def}}{=\!=} g\,(g \uparrow_2 n)$

$^0g \overset{\text{def}}{=\!=} e$

$^{Sn}g \overset{\text{def}}{=\!=} (^ng)\,g$

$g^0 \overset{\text{def}}{=\!=} e$

$g^{Sn} \overset{\text{def}}{=\!=} g(g^n)$

Agora sim:

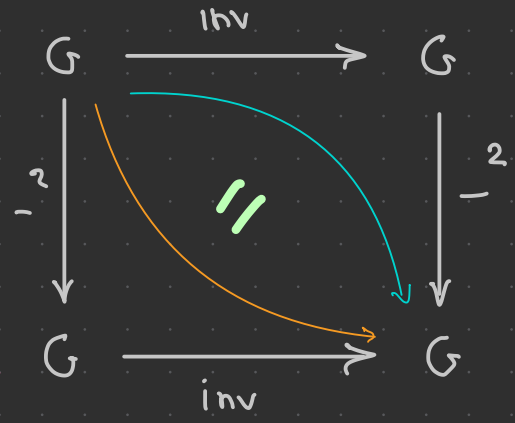
$g \uparrow_1 n \overset{?}{=\!=} g \uparrow_2 n$

$g^n \overset{?}{=\!=} {}^ng$

$g^{-1} \overset{\text{def}}{=} \text{inv}_G\, g$

$g^{-2} \overset{\text{def}}{=} \begin{cases} (g^{-1})^2 \\ ? \\ (g^2)^{-1} \end{cases} \quad ? \parallel \Theta.$

HW



Θ. o diagrama comuta

$\Updownarrow$

$\text{inv} \circ (\_)^2 = (\_)^2 \circ \text{inv}$

?

$\ldots, -3, -2, -1, 0, 1, 2, \ldots$

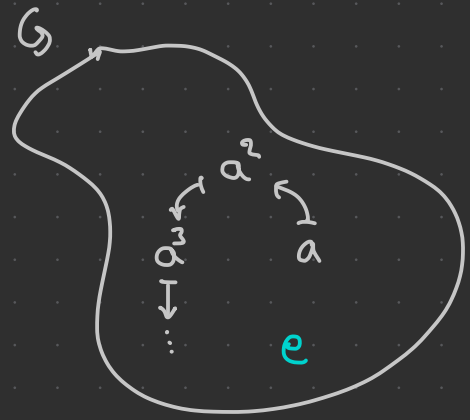
Ordem de membro de grupo

a

$a\,a$

$\vdots$

$a^n \stackrel{?}{=} e$



a ordem de a é n (no grupo G)

$o_G(a) = n \iff_{def} n > 0 \;\&\; a^n = e \;\&\; (\forall\, 0 < i \leq n)\,[\, a^i = e \Rightarrow i = n \,]$

$|a|_G = n$

$ord_G(a)$

Grupos de inteiros modulo n

lec05

2025-04-16

- $(\mathbb{Z}/n\mathbb{Z} \; ; \; +_n)$ é um grupo
- $(\mathbb{Z}/n\mathbb{Z} \setminus \{0\} \; ; \; \cdot_n)$ é um grupo $\iff$ n primo
- $(\mathbb{Z}/12\mathbb{Z} \setminus \{0, 2, 3, 4, 6, \ldots, 10\} \; ; \; \cdot_{12})$

  $= (\{1, 5, 7, 11\} \; ; \; \cdot_{12})$
- $(\mathbb{Z}_n \; ; \; \cdot_n)$ é um grupo de ordem $\varphi(n)$
  - ↳ os coprimos com n

função totiente de Euler

veja IDM1a

Ordens

$ord_G(\_) = \_ : |G| \times Nat \to Prop$

$ord_G(\_) = \infty : |G| \to Prop$

$ord_G(\_) < \infty$ ∴

	S_3		Ordem
e_{S_3}	id_3	$()$	1
	φ	$(1\,2)$	2
	ψ	$(1\,2\,3)$	3
	$\psi\varphi$	$(1\,3)$	2
	$\varphi\psi$	$(2\,3)$	2
	ψ^2	$(1\,3\,2)$	3

Sejam G, a, m t.q.

$m > 0$ & $a^m = e$

O que podemos concluir sobre a ordem de a no G?

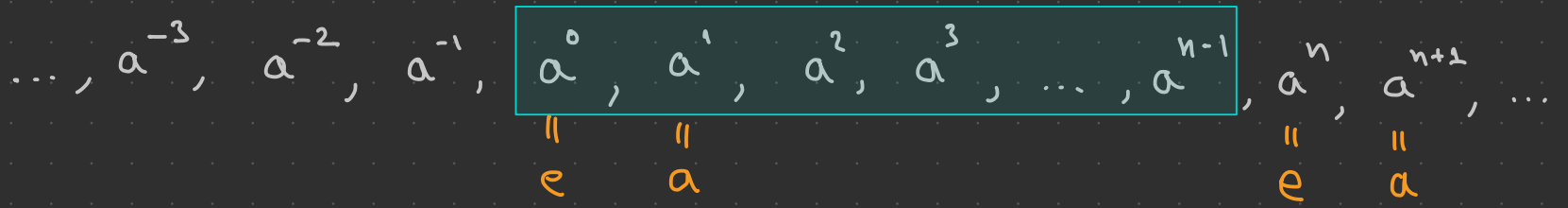
Θ. Sejam G, a, n t.q. $o_G(a) = n$.

Logo existem exatamente n potências de a.

O que significa isso?

(i) Pelo menos n potências distintas (dois a dois)

(ii) No máximo n potências distintas



(ii) $(\forall\, c : \mathbb{Z})(\exists\, 0 \le i < n)\,[\, a^c = a^i \,]$

(candidato) (Euclides)

Divida c por n para obter q, r t.q.

$$c = q \cdot n + r \quad \& \quad 0 \le r < n.$$

Calc:

$$\begin{aligned} a^c &= a^{q \cdot n + r} \\ &= a^{q \cdot n} \cdot a^r \\ &= a^{n \cdot q} \cdot a^r \\ &= (a^n)^q \cdot a^r \\ &= e^q \cdot a^r = e \cdot a^r = a^r \end{aligned}$$

∎

Pelo menos n potências distintas:

Testemunhas: $a^0, \ldots, a^{n-1}$.

Sejam i, j t.q. $0 \leq i, j < n$.

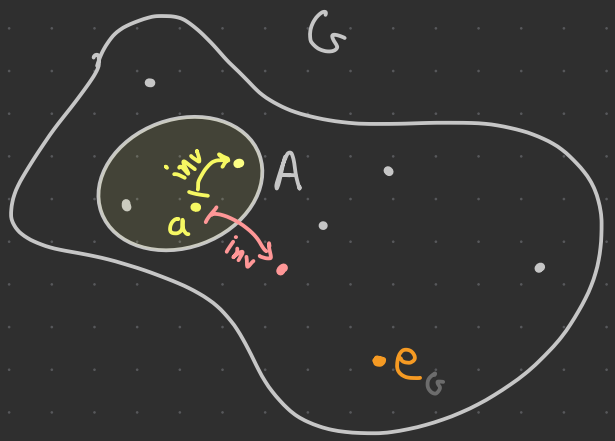
~~Vou~~ Vá demonstrar: $a^i = a^j \implies i = j$.

HW

Subgrupos

G grupo

$A \subseteq G$



A subgrupo de G $\overset{\text{def}}{\iff}$ A é op-fechado
$(\forall a, a' \in A)[\, a \cdot_G a' \in A \,]$
& A é id-fechado
& $e_G \in A$
& A é inv-fechado
& $(\forall a \in A)[\, a^{-1} \in A \,]$

$A \leq G$

$\Updownarrow \heartsuit$

A é Group-fechado

Fechado sob operação

$n : \mathbb{N}at$

$op : S^n \to S$

$A \subseteq S$

A é op-fechado $\overset{def}{\iff} (\forall a_1, \ldots, a_n \in A)[\, op(a_1, \ldots, a_n) \in A \,]$

ou

fechado sob a op

$n := 0 \rightsquigarrow op\,() \in A$

$() : \mathbb{1}$

Θ. G : Group
H : Set G
K : Set G
$H, K \leq G$

$\vdash \; H \cap K \leq G$

(i) $H \cap K$ op-fechado

(ii) $H \cap K$ id-fechado

(iii) $H \cap K$ inv-fechado

(i) $(\forall u, v \in H \cap K)[\, uv \in H \cap K \,]$

$$\dfrac{\dfrac{u \in H \cap K}{u \in H}\cap \quad \dfrac{v \in H \cap K}{v \in H}\cap}{\dfrac{uv \in H}{uv \in H \cap K}\cap}\; H \text{ op-f}$$

similar

$uv \in K$

Generaliza para $\bigcap_{i \in I} H_i$?

$H_i \leq G$

$\bigcap_i H_i \leq G$?

E as $\cup$? $\bigcup$?

Teoremas sobre ordens

lec06

2025-04-23

ordem — cardinalidade

0. $|a| = n \vdash |\{a^i \mid i \in \mathbb{Z}\}| = n$
0. $|a| = \infty \vdash \{a^i\}_{i \in \mathbb{Z}}$ infinito
0. $a^m = e \vdash o(a) \mid m$

$a^m = e \not\vdash o(a) = m$

$\cap$, $\cup$ de subgrupos

família I-indexada de subgrupos de G

$\_ \cap \_$ (binária) $\rightsquigarrow$ $\bigcap_{i \in I} H_i$ I-ária

recursão $\searrow$ $\bigcap_{i \in \mathbb{N}} H_i$ $\mathbb{N}$-ária

$H_0 \cap \cdots \cap H_{n-1}$
(n-ária)

$n : \mathbb{N}$

$H_0, \ldots, H_{n-1} \leq G$
$\vdash \bigcap_i H_i \leq G$
indução

Para $n = 0$:
$\bigcap \emptyset = G \leq G$

Para $n = 1$:
(fácil)

... e sobre uniões?

$\mathcal{H}$ coleção de subconjuntos de G

$\mathcal{H} : \mathsf{Set}\ (\mathsf{Set}\ G)$

$\bigcap \emptyset = ?$

$$x \in \bigcap \mathcal{H} \iff (\forall H \in \mathcal{H})[\, x \in H \,]$$
$$(\forall H \in \emptyset)[\ \dots\ ]$$

$$\bigcap_{i=0}^{\infty} H_i \overset{\heartsuit}{\equiv} H_0 \cap H_1 \cap \cdots$$

!!! ?

$$\bigcap_{i \in \mathbb{N}} H_i \overset{\text{sug}}{\equiv} \bigcap \{ H_i \mid i \in \mathbb{N} \}$$

$$\bigcap_{\alpha} \emptyset_{\mathsf{Set}\,\alpha} \overset{?}{=} \mathcal{U}_{\alpha}$$

$$\bigcup_{\alpha} \emptyset_{\mathsf{Set}\,\alpha} \overset{?}{=} \emptyset_{\alpha}$$

O que acontece no mundo un(i)typed? (CFR)

Construções de grupos (Grupos de graça)

Produto

$$G \times H \overset{\text{def}}{=} \left(|G| \times |H| \; ; \; *_{G\times H} \, , \, (e_G, e_H) \, , \, inv_G \times inv_H \right)$$

$$((g,h) *_{G\times H} (g',h')) \overset{\text{def}}{=} (gg', hh')$$

$$id_{G\times H} \overset{\text{def}}{=} (e_G \, , \, e_H)$$

$$(g,h)^{-1} \overset{\text{def}}{=} (g^{-1}, h^{-1})$$

CFR

Oposto

$$G \longmapsto^{op} G^{op}$$

$$G^{op}.\text{carrier} \overset{\text{def}}{\equiv} G.\text{carrier}$$

$$G^{op}.\text{inv} \overset{\text{def}}{\equiv} G.\text{inv}$$

$$G^{op}.\text{id} \overset{\text{def}}{\equiv} G.\text{id}$$

$$x *_{G^{op}} y \overset{\text{def}}{\equiv} y *_G x$$

Critéria de subgrupo

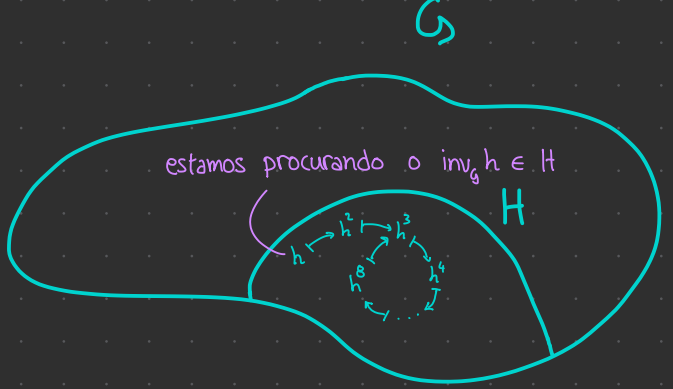
└ plural de critérion

$H \subseteq |G|$

$H \leq G$?

└ Group-fechado $\Leftarrow$ op, id, inv

⚠ do inglês «inhabited» que significa «habitado»!



Critérion Inhab:

- H habitado
- H op-fechado
- H inv-fechado

$\vdash H \leq G$

Critérion Fin:

- H habitado
- H finito
- H op-fechado

$\vdash H \leq G$

$h, h^2, h^3, \ldots \in H$

$(\forall n \geq 1)[\, h^n \in H \,]$

Sejam $0 < u < v$ t.q. $h^u = h^v$. completar!

$\underbrace{hh\cdots h}_{u \text{ cópias}} = \underbrace{hh\cdots h}_{v \text{ cópias}}$ **HW**

Subgrupo gerado por a

$\langle a \rangle \overset{\text{def}}{=} G$?

Não: pode entrar lixo (membros injustificáveis).

$\langle a \rangle \overset{\text{def}}{=} \{a\}$?

Não: pode nem ser um subgrupo ($\{a\} \leq G \Leftrightarrow$?)

$a \in G$

$\langle a \rangle_G \overset{\text{def}}{=} \{ a^i \mid i \in \mathbb{Z} \}$

$A \subseteq G$

$\langle A \rangle \overset{\text{def}}{=}$?

Deveria ser backwards compatible:

$\langle a \rangle = \langle \{a\} \rangle$

$\langle a, b \rangle = \langle \{a, b\} \rangle$

$a, b \in G$

$\langle a, b \rangle \overset{\text{def}}{=}$?