(G, f) $\quad f : G \times G \to G$
$(a, b) \mapsto \underline{ab}$
$f(a, b) = \underline{ab}$

* i) Semigrupo: $\forall a, b, c \in G,\ a(bc) = (ab)c$

ii) $\exists e \in G ; \forall a \in G,\ ae = ea = a$ (monoide)

iii) $\forall a \in G,\ \exists a^{-1} \in G ;\ aa^{-1} = a^{-1}a = e$ (grupo)

iv) $\forall a, b \in G ;\ ab = ba$ (comutativo/Abeliano)

Exercício: Seja S um conjunto qualquer. $A(S)$ o conj de todas as bijeções $f : S \to S$. Mostre $(A(S), \circ)$ é grupo?

$(f \circ g) \circ h = f \circ (g \circ h),\ \forall f, g, h \in A(S)$

$\alpha \circ \beta(x) = \alpha(\beta(x)),\ \forall x \in S$

$(f \circ g) \circ h(x) = (f \circ g)(h(x)) = f(g(h(x))$
$= f(g \circ h(x)) = f \circ (g \circ h)(x),\ \forall x \in S$

i) $(f \circ g) \circ h = f \circ (g \circ h),\ \forall f, g, h \in A(S)$

ii) $id(x) = x,\ \forall x \in S$

Dado $f \in A(S)$: $(f \circ id)(x) = f(id(x)) = f(x)$
$(id \circ f)(x) = id(f(x)) = f(x)$

iii) f é bijeção $\iff \exists f^{-1}$; $fof^{-1} = f^{-1}of = id$

* Se G é monoide, então a identidade é única. Se G é grupo, então:

i) $c \in G$ e $cc = c \Rightarrow c = e$

Dem: $(cc) \cdot c^{-1} = c \cdot c^{-1} = e$
$c(cc^{-1}) = e$
$ce = e$
$c = e$

ii) $\forall a, b, c \in G$, $ab = ac \Rightarrow b = c$
$ba = ca \Rightarrow b = c$

Dem: $a^{-1}(ab) = a^{-1}(ac)$
$(a^{-1}a)b = (a^{-1}a)c$
$eb = ec$
$b = c$

$e = ee' = e'$

iii) $\forall a \in G$, a^{-1} é único.

Dem: $\exists b \in G$, $ab = ba = e$
$a^{-1} = b$
$a^{-1} = ea^{-1} = (ba)a^{-1} = b(aa^{-1}) = be = b$

iv) $\forall a \in G$, $(a^{-1})^{-1} = a$

Dem: $(a^{-1})(a^{-1})^{-1} = e$
$a((a^{-1})(a^{-1})^{-1}) = (aa^{-1})(a^{-1})^{-1} = (a^{-1})^{-1} = ae = a$

v) $\forall a, b \in G, \ (ab)^{-1} = b^{-1}a^{-1}$

Dem: $(ab)(ab)^{-1} = e$

$a^{-1}[(ab)(ab)^{-1}] = a^{-1} \cdot e = a^{-1}$

$((a^{-1}a)b)(ab)^{-1} = a^{-1}$

$b^{-1}b(ab)^{-1} = b^{-1}a^{-1}$

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

G abeliano.

notação: $a^{-1} := -a$ $\qquad ab := a+b$

$ab^{-1} := a + (-b)$

$\mathbb{R}^*$ $\quad x > 0$

$(ab)c = a(bc) = abc$

$((ab)c)d = (a(bc))d = a((bc)d) = a.b.c.d$

$= (ab)(cd) = a(bc)d$

$abcd = (ab)(cd) = a(bc)d$

Def: Sejam $(G, \cdot)$ semigrupo, $a \in G$ e $n \in \mathbb{N}^*$

$a^n = \underbrace{a \ldots a}_{n \text{ vezes}}$, $\quad a^0 = e$

Se G grupo, definimos $a^{-n} = (a^{-1})^n = \underbrace{a^{-1} \ldots a^{-1}}_{n \text{ vezes}}$

(G, f) $\quad f := +$ $\quad (\mathbb{R}, +)$

$a + b = b + a$

Notação:

$a^n \qquad n \cdot a = a + \dots + a$

---

* Se G é um grupo e $a \in G$, então para todo $m, n \in \mathbb{Z}$:

i) $a^m a^n = a^{m+n}$

ii) $(a^m)^n = a^{m \cdot n}$

Ex: mostre a equivalência:

i) G é abeliano

ii) $(ab)^2 = a^2 b^2, \ \forall a, b \in G$

iii) $(ab)^{-1} = a^{-1} b^{-1}, \ \forall a, b \in G$

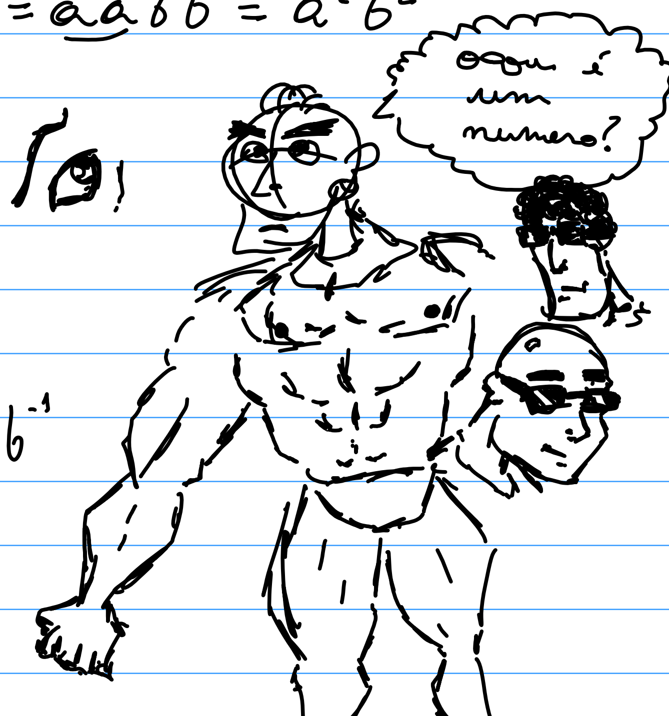
iv) $(ab)^n = a^n b^n, \ \forall n \in \mathbb{Z}$ e $\forall a, b \in G$

i) $\Leftrightarrow$ ii); $(\Rightarrow)$: $(ab)^2 = (ab)(ab)$

$= a\underbrace{ba}b = a(ab)b = \underbrace{aa}bb = a^2 b^2$

$(\Leftarrow)$: $\forall a, b \in G$,

$\underline{a^{-1} a^2 = a}$, $\forall a \in G$



$ab = a^{-1} a^2 b$

$= a^{-1} a^2 b^{-1} b^2$

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

$= \cancel{a^{-1}} \cancel{a} b a \cancel{b} \cancel{b^{-1}}$

$= ba$

Ex: Se $a^2 = e$, $\forall a \in G$, então G é abeliano.

$$\Updownarrow$$

$$a = a^{-1} \qquad * \forall a, b \in G, \ ab = ba$$

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

Exercícios:

1) Se G é grupo, $a, b \in G$ e $bab^{-1} = a^r$ para algum $r \in \mathbb{N}$, então $b^j a b^{-j} = a^{r^j}$ para todo $j \in \mathbb{N}$. (Dica: use indução)

2) Prove as equivalências que sobraram acima.

3) Se $|G| = 2n$, $n > 0$ e G finito. Então, G contém um elemento $a \neq e$ tal que $a^2 = e$.
Dica: Ou $g^2 = e$, ou $g^2 \neq e$, $\forall g \in G$