• 1.1

(E.7) Seja $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ e para $x, y \in G$ seja $x \star y$ a parte fracionária de $x+y$ ($x \star y = x + y - [x+y]$ onde $[a]$ é o maior inteiro menor ou igual a a). Prove que $\star$ é uma operação binária bem definida em G e que G é um grupo abeliano em $\star$.

i) $m(m(x,y), z) = m(x+y-[x+y], z)$
$= x+y+z-[x+y]-[x+y+z-[x+y]]$

$m(x, m(y,z)) = m(x, y+z-[y+z])$ $\|$
$= x+y+z-[y+z]-[x+y+z-[y+z]]$

ii) seja $a = 0$, $m(x,a) = x + a - [x+a] = x$
$m(a,x) = a + x - [a+x] = x$

iii) seja $b = -x$, $m(x,b) = x - x - [x-x] = 0$
$m(b,x) = -x+x-[-x+x] = 0$

$m(x,y) = x+y-[x+y] = y+x-[y+x] = m(y,x)$, $\therefore$ G é abeliano.

(E.9) Seja $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$

a) Prove que $(G,+)$ é um grupo.

i) $m(m(x,y),z) = m(x_1 + x_2\sqrt{2} + y_1 + y_2\sqrt{2}, z)$
$= x_1 + y_1 + z_1 + (x_1 + y_1 + z_1)\sqrt{2}$

$m(x, m(y,z)) = m(x, y_1 + y_2\sqrt{2} + z_1 + z_2\sqrt{2})$
$= x_1 + y_1 + z_1 + (x_1 + y_1 + z_1)\sqrt{2}$

ii) seja $a = 0$, $m(x,a) = x_1 + x_2\sqrt{2} + 0 + 0\sqrt{2} = x_1 + x_2\sqrt{2} = x$
$m(a,x) = \ldots = x_1 + x_2\sqrt{2} = x$

iii) seja $b = -x_1 - x_2\sqrt{2}$, $m(x,b) = x_1 + x_2\sqrt{2} - x_1 - x_2\sqrt{2} = m(b,x)$
$= 0$ //

b) Prove que os elementos não-nulos de G são um grupo em multiplicação.

i) $m(m(x,y),z) = m((x_1 + x_2\sqrt{2})(y_1 + y_2\sqrt{2}), z)$
$= (x_1 + x_2\sqrt{2})(y_1 + y_2\sqrt{2})(z_1 + z_2\sqrt{2})$

$m(x, m(y,z)) = m(x, (y_1 + y_2\sqrt{2})(z_1 + z_2\sqrt{2}))$
$= (x_1 + x_2\sqrt{2})(y_1 + y_2\sqrt{2})(z_1 + z_2\sqrt{2})$

ii) seja $a = 1 + 0\sqrt{2}$, $m(x,a) = (x_1 + x_2\sqrt{2})(1 + 0\sqrt{2}) = x_1 + x_2\sqrt{2} = x$
$m(a,x) = (1 + 0\sqrt{2})(x_1 + x_2\sqrt{2}) = x_1 + x_2\sqrt{2} = x$

iii) seja $b = \dfrac{1}{x_1 + \sqrt{2}x_2}$, $m(x,b) = \dfrac{x_1 + x_2\sqrt{2}}{x_1 + x_2\sqrt{2}} = m(b,x) = 1$ //

(E.19) Seja $x \in G$ e seja $a, b \in \mathbb{Z}^+$

associatividade: $(a * b) * c = a * (b * c)$
elemento neutro: $e * a = a * e = a$
elemento simétrico: $a * \bar{a} = \bar{a} * a = e$

a) Prove que $x^{a+b} = x^a x^b$
$(x^a)^b = x^{ab}$

Para todos $x \in G$, $n \in \mathbb{Z}^+$:
$x^0 = e$, $x^1 = x$, $x^n = (x^{n-1})x$ e $x^{-n} = (x^{-1})^n$

tomando $b = 1$: $x^{a+b} = x^{a+1} = x^a . x = x^a x^1 = x^a x^b$

passo indutivo: para $b \geq 1$:
$x^{a+(b+1)} = x^{a+b} . x = x^a . x^b . x = x^a . x^{b+1}$ //

tomando $b = 1$: $(x^a)^b = (x^a)^1 = x^{a.1} = x^{ab}$

passo indutivo: para $b \geq 1$:
$(x^a)^{b+1} = (x^{ab})x^a = x^{ab+a} = x^{a(b+1)}$ //

b) Prove que $(x^a)^{-1} = x^{-a}$

seja $a = 1$: $(x^a)^{-1} = (x^1)^{-1} = x^{1.(-1)} = x^{-1} = x^{-a}$

passo indutivo: para $a \geq 1$:
$(x^{a+1})^{-1} = x^{(a+1).(-1)} = x^{-a-1} = x^{-(a+1)}$ //

c) Faça a) com inteiros arbitrários a e b (pos, neg, 0)

seja $a = 2$, $b = -3$:

$$x^{a+b} = x^{2+(-3)} = x^2 . x^{(-3)} = x^a . x^b$$ //

seja $a = -10$, $b = 0$:

$$x^{a+b} = x^{-10+0} = x^{-10} . x^0 = x^a . x^b$$ //

seja $a = 3$, $b = -1$

$$(x^a)^b = (x^3)^{-1} = x^{3.(-1)} = x^{a.b}$$ //

(E.24) Se a e b são elementos de comutação de G, prove que $(ab)^n = a^n b^n$ $\forall n \in \mathbb{Z}$.

$\boxed{\text{tomemos: } ab^n = b^n a}$

↳ já que o grupo é abeliano

seja $n = 1$:

$$(ab)^n = (ab)^1 = ab = a^1 . b^1 = a^n . b^n = b^n a^n$$ //

seja $n \geq 1$:

$$(ab)^{n+1} = (ab)^n (ab) = a^n . b^n . a . b = a^n . a . b^n . b = a^{n+1} . b^{n+1}$$ //

seja $n = 0$:

$$(ab)^n = (ab)^0 = e = e . e = a^0 . b^0 = a^n b^n$$ //

seja $n \leq 1$:

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

(E.25) Prove que se $x^2 = 1$ $\forall x \in G$, G é abeliano.

$x^2 = x . x = x^1 . x^1 = 1$, multiplicando por x^{-1} em cada lado:

$$x^1 . x^1 . x^{-1} = x^{-1} \Rightarrow x^1 . x^0 = x^{-1} \Rightarrow x^1 . e = x^{-1} \Rightarrow x^1 = x^{-1} = x$$

$$\forall y, z \in G, \quad y . z = (yz)^{-1} = y^{-1} . z^{-1} = z^{-1} . y^{-1} = (zy)^{-1} = zy$$

$\therefore$ G é abeliano //

(E.32) Se x é de ordem n finita em G, prove que $1, x, x^2, \ldots, x$

são distintos. Deduza que $|x| \leqslant |G|$.

$|G|$: a ordem do grupo G é o número de elementos do conjunto G. A ordem de g é o menor $k>0$ tq $g^k = e$

Sejam $b > a$ e $a, b \in \{0, 1, \ldots, n-1\}$

tais que $a \neq b$ e $x^a = x^b$. Logo:

$x^a = x^b = x^a . x^{b-a} \Rightarrow x^{b-a} = 1$, onde $0 < b-a < n$. Isto contradiz o fato de x ter ordem n. Consequentemente não existem a, b o que prova que $1, x, x^2, \ldots, x^{n-1}$ são distintos. Isto implica que $\{1, x, x^2, \ldots, x^{n-1}\} \subseteq G$ tem ordem $|x|$ o que conclui que $|x| \leqslant |G|$ //

(E.34)* Se x é um elemento de ordem infinita em G, prove que os elementos x^n, $n \in \mathbb{Z}$ são todos distintos.

Seja $|x| = \infty$ e suponha que existem $a, b \in \mathbb{Z}$ com $a \neq b$ tal que $x^a = x^b$.

Suponhamos que $b > a$, $b - a > 0$ e:

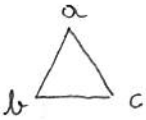
$$e = x^a . x^{-a} = x^b . x^{-a} = x^{b-a}$$

Consequentemente $|x| \leqslant b-a$, o que é uma contradição. Logo $\nexists\, a, b \in \mathbb{Z}$ //

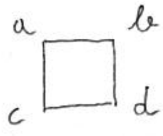
$$D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$$

$\boxed{\bullet\ 1.2}$

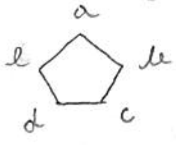
(E.1) Faça a ordem de cada um dos elementos dos seguintes grupos:

a) $D_6 : \{1, r, r^2, s, sr, sr^2\}$ 

$|1| = 1$, $|r| = 3$, $|r^2| = 3$, $|s| = 2$, $|sr| = 2$, $|sr^2| = 2$

b) $D_8 : \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ 

$|1| = 1$, $|r| = 4$, $|r^2| = 2$, $|r^3| = 4$, $|s| = 2$, $|sr| = 2$, $|sr^2| = 2$ $|sr^3| = 2$

c) $D_{10} : \{1, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}$ 

$|1| = 1$, $|r| = 5$, $|r^2| = 5$, $|r^3| = 5$, $|r^4| = 5$, $|s| = 2$, $|sr| = 2$, $|sr^2| = 2$, $|sr^3| = 2$

$|sr^4| = 2$

(E.2) Use os geradores e relações acima para mostrar que se x é um elemento de D_{2m} o qual não é uma potência de r, então $rx = xr^{-1}$ $\boxed{rs = sr^{-1}}$

seja $x \in D_{2m}$ e, $x \neq r^k \Rightarrow x = sr^k$ para $0 \leq k \leq m-1$

$rx = rsr^k = sr^{-1}r^k = sr^{k-1} = sr^k.r^{-1} = xr^{-1}$ //

$\boxed{\bullet 1.3}$

(E.1) Seja σ a permutação:

$1 \mapsto 3 \quad 2 \mapsto 4 \quad 3 \mapsto 5 \quad 4 \mapsto 2 \quad 5 \mapsto 1$

e τ a permutação:

$1 \mapsto 5 \quad 2 \mapsto 3 \quad 3 \mapsto 2 \quad 4 \mapsto 4 \quad 5 \mapsto 1$

Ache o ciclo de decomposições de cada uma das seguintes permutações:

$\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma$ e $\tau^2\sigma$.

$\sigma: (135)(24)$, $\tau: (15)(23)$, $\sigma^2: (153)$, $\sigma\tau: 1(2534)$

$\tau\sigma: (1243)$, $\tau^2\sigma: (135)(24)$ //

(E.5) Ache a ordem de $\underbrace{(1\ 12\ 8\ 10\ 4)}_{5}\underbrace{(2\ 13)}_{2}\underbrace{(5\ 11\ 7)}_{3}\underbrace{(6\ 9)}_{2}$

MMC $\{5, 2, 3, 2\} = 30$ //

(E.15) Prove que a ordem de um elemento em S_n é igual ao menor divisor comum do comprimento dos ciclos na decomposição dos mesmos.

$\sigma^p = (\sigma_1 \ldots \sigma_l) \in S_m$; σ_i é um p_i-ciclo. Então $o(\sigma_i) = p_i \ \forall i \in \{1, \ldots, l\}$

porque os ciclos σ_i são disjuntos, porque $p_i | p \ \forall i \in \{1, \ldots, l\}$

Denote mmc $\{p_1, \ldots, p_l\} = p$, $\sigma^p = (\sigma_1 \ldots \sigma_l) \ldots (\sigma_1 \ldots \sigma_l) \overset{\text{↘}}{=} \sigma_1^p \ldots \sigma_l^p = e$ //

Se $q < p$, então existe $i \in \{1, \ldots, l\}$, tal que $p_i \nmid q$, ou seja, $q = k_i p_i + r_i$, $r_i \neq 0$.

Daí segue que: $\sigma^q = \sigma_1^q \ldots \sigma_l^q = e \Rightarrow \sigma_i^{r_i} = \sigma_1^{-r_1} \ldots \sigma_l^{-r_l}$

↳ isto não pode acontecer pois os ciclos σ_i são disjuntos.

$\boxed{\bullet\ 1.4}$

(E.11) Seja $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \right\}$ chamado grupo de Heisenberg sobre F. Sejam $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ e $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ elementos de $H(F)$.

a) Escreva a matriz produto XY e deduza que $H(F)$ é fechado a multiplicação de matrizes.

$$\underbrace{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}}_{X} \times \underbrace{\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}}_{Y} = \underbrace{\begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}}_{XY}$$

$$\underbrace{\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}}_{Y} \times \underbrace{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}}_{X} = \underbrace{\begin{pmatrix} 1 & a+d & b+dc+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}}_{YX}$$

$XY \neq YX \Rightarrow H(F)$ não é abeliano //

b) ache uma fórmula explícita para a matriz inversa X^{-1} e deduza que $H(F)$ é fechado ao inverso da matriz.

$$X^{-1} = \frac{1}{\det(X)} \cdot \operatorname{Adj}(X) = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} //$$

c) Prove a lei associativa para $H(F)$ e deduza que $H(F)$ é um grupo de ordem $|F|^3$

$$\begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d+g & b+e+h+af+ai+di \\ 0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d+g & e+di+h \\ 0 & 1 & f+i \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & a+d+g & b+e+h+af+ai+di \\ 0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix}$$

o que prova a lei associativa para $H(f)$, o que consequentemente mostra que $H(F)$ é $|F|^3$ (usa apenas 3 elementos de F por elemento de $H(F)$).

UT

e) Prove que todos elementos não-identidade de $H(\mathbb{R})$ tem ordem infinita.

$$\forall X \in H(\mathbb{R}) \; \nexists n \in \mathbb{N} \mid \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\cdots\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$\forall a, b, c \in \{\mathbb{R} \setminus 0\}$ //

$\boxed{\bullet\ 1.5}$

(E.2)

elemento	e	a	a^2	a^3	x	ax	a^2x	a^3x
e	e	a	a^2	a^3	x	ax	a^2x	a^3x
a	a	a^2	a^3	e	ax	a^2x	a^3x	x
a^2	a^2	a^3	e	a	a^2x	a^3x	x	ax
a^3	a^3	e	a	a^2	a^3x	x	ax	a^2x
x	x	a^3x	a^2x	ax	e	a^3	a^2	a
ax	ax	x	a^3x	a^2x	a	e	a^3	a^2
a^2x	a^2x	ax	x	a^3x	a^2	a	e	a^3
a^3x	a^3x	a^2x	ax	x	a^3	a^2	a	e

D8

elemento	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	$-i$	i
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Q8

$\boxed{\cdot\ 1.6}$

- função injetora (um a um): $\nexists\ x_i, x_j \in A$ tq $f(x_i) = f(x_j)$ $\forall f(x_k)$
  ex. funções monotônicas, contra-ex. $f(x) = x^2$, $x \in \mathbb{R}$
- função sobrejetora: $\forall\ x \in Im\ \exists\ x \in CDom$
  ex. $f(x) = x^3$, contra-ex. $f(x) = x^2$, $x \in \mathbb{R}$
- homomorfismo: sejam $(G, \star)$ e $(H, \diamond)$ grupos, uma função $\varphi : G \to H$ tal que:
  $\varphi(x \star y) = \varphi(x) \diamond \varphi(y)$ $\forall\ x, y \in G$ $\Rightarrow \varphi(xy) = \varphi(x)\varphi(y)$

↳ isomorfismo: a função $\varphi: G \to H$ é um isomorfismo $(G \cong H)$ quando φ é um homomorfismo e uma bijeção.

(E.4) Prove que grupos multiplicativos $\mathbb{R} - \{0\}$ e $\mathbb{C} - \{0\}$ não são isomorfos.

sejam $i, -i \in \mathbb{C} - \{0\}$; $|-i| = |i| = 4$. $\nexists\ x \in \mathbb{R} - \{0\}$ tq $|x| = 4$

o único elemento de $\mathbb{R} - \{0\}$ de ordem finita é -1, $|-1| = 2$.

$\therefore \mathbb{R} - \{0\} \ncong \mathbb{C} - \{0\}$

(E.7) Prove que D_8 e Q_8 não são isomorfos.

$D_8 = \{e, a, a^2, a^3, x, ax, a^2x, a^3x\}$, $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$

$a^4 = x^2 = e$, $ax = xa^{-1}$; $i^2 = j^2 = k^2 = ijk = -1$

existem dois elementos de ordem 2 em D_8 : $|x| = |a^2x| = 2$

porém existe apenas um elemento em Q_8 de ordem 2 : $|-1| = 2$, $\therefore Q_8 \ncong D_8$

(E.9) Prove que D_{24} e S_4 não são isomorfos.

$D_{24} = \{\langle a, x\rangle \mid a^{12} = e,\ x^2 = e,\ ax = xa^{-1}\}$, $|a| = 12$

seja $\sigma \in S_4$: $\sigma = (a_1 a_2) \wedge (a_1 a_2)(b_1 b_2) \wedge (a_1 a_2 b_1 b_2) \wedge (a_1 a_2 b_1)$
$\wedge\ (a_1 a_2)(a_2 b_1)$ podendo a ordem de σ ser 1, 2, 3 ou 4.

$\therefore D_{24} \ncong S_4$

(E.10) Complete nos detalhes da prova que grupos simétricos S_Δ e S_Ω são isomórficos se $|\Delta| = |\Omega|$ conforme a seguir:

Seja $\theta: \Delta \to \Omega$ uma bijeção. Defina

$\varphi: S_\Delta \to S_\Omega$ por $\varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$ para todo $\sigma \in S_\Delta$

e prove o seguinte:

a) φ é bem definida, isto é, se σ é uma permutação de Δ então $\theta \circ \sigma \circ \theta^{-1}$ é uma permutação de Ω

Sendo θ uma bijeção existe uma função inversa $\theta^{-1}: \Omega \to \Delta$ tal que $\theta \circ \theta^{-1}$ é a função identidade I_Ω em Ω e θ^{-1} é a função identidade I_Δ em Δ. Suponhamos que σ seja a permutação de Δ, isto implica que $\sigma: \Delta \to \Delta$, então tem-se a seguinte situação:

$$\Omega \xrightarrow{\theta} \Delta \xrightarrow{\sigma} \Delta \xrightarrow{\theta^{-1}} \Omega$$

e podemos compor θ, σ e θ^{-1} para obter a função $\varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1}: \Omega \to \Omega$

Sendo σ uma permutação existe o inverso $\sigma^{-1}: \Delta \to \Delta$, então

$$\Omega \xrightarrow{\theta} \Delta \xrightarrow{\sigma^{-1}} \Delta \xrightarrow{\theta^{-1}} \Omega$$

Seja $\tau = \theta \circ \sigma^{-1} \circ \theta^{-1}$, então:

$$\varphi(\sigma) \circ \tau = (\theta \circ \sigma \circ \theta^{-1}) \circ (\theta \circ \sigma^{-1} \circ \theta^{-1}) = \theta \circ \sigma \circ (\theta^{-1} \circ \theta) \circ \sigma^{-1} \circ \theta^{-1}$$
$$= \theta \circ \sigma \circ I_\Delta \circ \sigma^{-1} \circ \theta^{-1} = \theta \circ (\sigma \circ \sigma^{-1}) \circ \theta^{-1} = \theta \circ I_\Delta \circ \theta^{-1}$$
$$= \theta \circ \theta^{-1} = I_\Delta$$

$$\tau \circ \varphi(\sigma) = (\theta \circ \sigma^{-1} \circ \theta^{-1}) \circ (\theta \circ \sigma \circ \theta^{-1}) = \theta \circ \sigma^{-1} \circ (\theta^{-1} \circ \theta) \circ \sigma \circ \theta^{-1}$$
$$= \theta \circ \sigma^{-1} \circ I_\Delta \circ \sigma \circ \theta^{-1} = \theta \circ (\sigma^{-1} \circ \sigma) \circ \theta^{-1} = \theta \circ I_\Delta \circ \theta^{-1}$$
$$= \theta \circ \theta^{-1} = I_\Delta$$

$\therefore$ $\varphi(\sigma)$ é uma bijeção, o domínio e o contradomínio são o mesmo conjunto Ω, logo $\varphi(\sigma)$ é uma permutação de Ω //

b) φ é uma bijeção de S_Δ em S_Ω (ache um inverso dos dois lados de φ).

Defina uma função $\psi(\xi) = \theta^{-1} \circ \xi \circ \theta$ para cada ξ em S_Ω. Sendo θ uma bijeção, θ^{-1} também é uma bijeção, logo o argumento utilizado em a) ; trocando Δ e Ω, θ e θ^{-1} ; mostra que $\psi(\xi)$ é uma permutação de Δ. Assim ψ é uma função de S_Ω em S_Δ, o inverso dos dois lados de φ, porque para cada σ em S_Δ,

$$\psi(\varphi(\sigma)) = \psi(\theta \circ \sigma \circ \theta^{-1}) = \theta^{-1} \circ (\theta \circ \sigma \circ \theta^{-1}) \circ \theta$$
$$= (\theta^{-1} \circ \theta) \circ \sigma \circ (\theta^{-1} \circ \theta) = I_\Delta \circ \sigma \circ I_\Delta = \sigma$$

e para cada ξ em S_Ω:

$$\varphi(\psi(\xi)) = \varphi(\theta^{-1} \circ \xi \circ \theta) = \theta \circ (\theta^{-1} \circ \xi \circ \theta) \circ \theta^{-1}$$
$$= (\theta \circ \theta^{-1}) \circ \xi \circ (\theta \circ \theta^{-1}) = I_\Omega \circ \xi \circ I_\Omega = \xi$$

c) φ é um homomorfismo, isto é, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

$$\varphi(\sigma \circ \tau) = \theta \circ (\sigma \circ \tau) \circ \theta^{-1} = \theta \circ \sigma \circ I_\Delta \circ \tau \circ \theta^{-1}$$
$$= \theta \circ \sigma \circ (\theta^{-1} \circ \theta) \circ \tau \circ \theta^{-1}.$$
$$= (\theta \circ \sigma \circ \theta^{-1}) \circ (\theta \circ \tau \circ \theta^{-1}) = \varphi(\sigma) \circ \varphi(\tau) \;//$$

(E.17) Seja G um grupo. Prove que uma função de G em G definida por $g \mapsto g^{-1}$ é um homomorfismo se e somente se G é abeliano.

Seja $g \mapsto g^{-1}$ um homomorfismo. $\forall\, g, h \in G$, temos $(gh)^{-1} = g^{-1}h^{-1}$
$= h^{-1}g^{-1}$

$g^{-1}h^{-1} = h^{-1}g^{-1} \Rightarrow (g^{-1})^{-1}(h^{-1})^{-1} = (h^{-1})^{-1}(g^{-1})^{-1} \Rightarrow gh = hg.$

Assim quaisquer $g, h \in G$ comutam, logo G é abeliano.

Assumindo G abeliano: $(gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1}$

(E.19) Seja $G = \{ z \in \mathbb{C} \mid z^n = 1 \cdot \forall n \in \mathbb{Z}^+ \}$. Prove que para qualquer inteiro $k > 1$ a função de G em G ($z \mapsto z^k$) é um homomorfismo sobrejetora mas não um isomorfismo.

Seja $G = \{ z \in \mathbb{C} : z^n = 1 \ \forall n \in \mathbb{Z}^+ \}$ e $\varphi : G \to G$ definida por $\varphi(z) = z^k$

↳ Seja $z_1, z_2 \in G$, então $\varphi(z_1 z_2) = (z_1 z_2)^k = z_1^k \cdot z_2^k = \varphi(z_1) \cdot \varphi(z_2)$, o que mostra que φ é um homomorfismo.

↳ Seja $z \in G$ tal que $z^m = 1$, tomemos $w = z^{1/k}$. Sendo $(w^m)^k = w^{mk} = 1$ e $mk \in \mathbb{Z}^+$, $w \in G$ e $z = w^k$. Logo a função é sobrejetora.

↳ O kernel da função é $\ker \varphi = \{ z \in G : z^k = 1 \}$ o qual não é $\{1\}$. Portanto a função não é injetora.

(E.20) Seja G um grupo e Aut(G) o grupo de todos isomorfismos de G em G. Prove que Aut(G) é um grupo sobre a função composta.

Se $\varphi : G \to G$ e $\varphi' : G \to G$ são isomorfismos, então $\varphi \circ \varphi' : G \to G$ também é um isomorfismo, o que também é em Aut(G).

O elemento identidade dado por $id(g) = g \ \forall g \in G$ é um automorfismo.

Se $\varphi : G \to G$ é um automorfismo, então $\varphi^{-1} : G \to G$ é um automorfismo, o que também é em Aut(G). Aut(G) satisfaz as propriedades de grupos.

(E.25) Seja $n \in \mathbb{Z}^+$, r e s os geradores de D_{2n} e $\theta = 2\pi/n$.

a) prove que a matriz $\begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix}$ é a matriz da transformação linear que rotaciona o plano x, y sobre a origem no sentido anti-horário por θ rad.

b) Prove que a função $\varphi: D_{2n} \to GL_2(\mathbb{R})$ definida em geradores por:

$\varphi(r) = \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix}$ e $\varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ estendem a um homomorfismo de D_{2n} a $GL_2(\mathbb{R})$

c) Prove que o homomorfismo φ em b) é injetor.

$\boxed{\bullet\ 1.7}$

(E.3) mostre que o grupo aditivo $\mathbb{R}$ age no plano X, Y $\mathbb{R}\times\mathbb{R}$ por

$r.(X, Y) = (r + rY, Y)$.

Seja $\mathbb{R}$ um grupo aditivo e $\mathbb{R}\times\mathbb{R}$ um conjunto. Defina $r.(X, Y) = (X + rY, Y)$

Lo $r_1, r_2 \in \mathbb{R}$ e $(X, Y) \in \mathbb{R}\times\mathbb{R}$, temos:

$$r_1(r_2(X, Y)) = r_1(X + r_2Y, Y) = (X + r_2Y + r_1Y, Y)$$
$$= (X + (r_1 + r_2))Y = (r_1 + r_2)(X, Y)$$

Lo Seja $0 \in \mathbb{R}$ tal que $0 + a = a \ \forall a \in \mathbb{R}$, temos:

$$0.(X, Y) = (X + 0X, Y) = (X, Y)$$

logo $\mathbb{R}$ age no conjunto $\mathbb{R}\times\mathbb{R}$.

(E.14) Seja G um grupo e $A = G$. Mostre que se G não é abeliano então as funções definidas por $g \cdot a = a \cdot g$ $\forall\, g, a \in G$ não satisfazem os axiomas da ação de G em G.

Sejam $g_1, g_2 \in G$ e $a \in A$, então $(g_1 g_2) \cdot a = a g_1 g_2$ enquanto $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (a g_2) = a g_2 g_1$ sendo $a \in A = G$, se o grupo não é abeliano, então $a g_1 g_2 \neq a g_2 g_1$. Portanto não é uma ação de grupo.

(E.15) Seja G qualquer grupo e $A = G$. Mostre que as funções definidas por $g \cdot a = a \cdot g^{-1}$ $\forall\, g, a \in G$ satisfazem os axiomas da ação de G em G.

Suponha $g_1, g_2 \in G$ e $a \in A$, se $g a = a g^{-1}$, então:

$$(g_1 g_2) \cdot a = a (g_1 g_2)^{-1} = a g_2^{-1} g_1^{-1} \quad \text{e}$$

$$g_1 (g_2 \cdot a) = g_1 \cdot (a g_2^{-1}) = a g_2^{-1} g_1^{-1}$$

o que satisfaz $(g_1 g_2) a = g_1 \cdot (g_2 a)$. Sendo $1_G \in G$, $1_G \cdot a = a 1_G = a$ estão satisfeitos os dois axiomas.