Lista 1

/ /

① Considere as seguintes funções de $\mathbb{R}\setminus\mathbb{Q}$ em $\mathbb{R}\setminus\mathbb{Q}$;

$$f_0(x) = x \quad f_1(x) = 1/x \quad f_2(x) = 1-x$$

$$f_3(x) = \frac{1}{1-x} \quad f_4(x) = \frac{x}{x-1} \quad f_5(x) = \frac{x-1}{x}$$

Mostre que o conjunto $G = \{f_0, f_1, \ldots, f_5\}$ com a operação de composição de funções é um grupo. Escreva sua tabela de multiplicação e decida se é abeliano ou não.

Montando a tabela:

$*$	f_0	f_1	f_2	f_3	f_4	f_5
f_0	x	$1/x$	$1-x$	$1/1-x$	$x/x-1$	$x-1/x$
f_1	$1/x$	x	$1/1-x$	$1-x$	$\frac{x-1}{x}$	$\frac{x}{x-1}$
f_2	$1-x$	$\frac{x-1}{x}$	x	$\frac{x}{x-1}$	$\frac{1}{1-x}$	$1/x$
f_3	$\frac{1}{1-x}$	$\frac{x}{x-1}$	$1/x$	$\frac{x-1}{x}$	$1-x$	x
f_4	$\frac{x}{x-1}$	$\frac{x}{x-1}$	$1/x$	x	$1-x$	$\frac{1-x}{x}$
f_5	$\frac{x-1}{x}$	$1/x$	$1-x$	$\frac{1}{1-x}$	$\frac{x}{x-1}$	x

1. (Associatividade) Note que,

$$(f \circ g) \circ h\,(x) = (f \circ g)(h(x)) = f(g(h(x)))$$

e

$$f \circ (g \circ h)(x) = f((g \circ h)(x)) = f(g(h(x)))$$

2. Sendo f_0 o elemento neutro note que

$$f_0 \circ g = g \circ f_0 = g \ , \ \forall g \in G$$

3. (Inverso) O ~~??~~ elemento inverso desse grupo é a função inversa. Note que, pela tabela que para $\forall g \in G$ temos que $g^{-1} \in G$

4. (Comutatividade) ~~B~~ Pela tabela note que, não vale a comutatividade, do contrário, a tabela seria espelhada.

Logo, G é um grupo, mas não abeliano.

② Sejam ρ e σ os geradores usuais do grupo simétrico S_3. Determine explicitamente:

ⓐ $\rho^3 = e$

ⓑ $\sigma\rho\sigma = \rho^2\sigma\sigma$
$= \rho^2 e$
$= \rho^2$

ⓒ $\rho\sigma^{-1}\rho = \rho\sigma\rho^2$
$= \rho\sigma\rho\rho$
$= \rho^3\sigma\rho$
$= \sigma\rho$
$= \rho^2\sigma$

ⓓ $\sigma\rho^{2000}\sigma^{29}\rho^{-31}\sigma^{2222222109928} = \sigma\rho^2\sigma\rho^{-1}$
$= \sigma\rho^2\sigma\rho^2$
$= \sigma^2\rho\rho^2$
$= e$

③ Determine quais dos seguintes itens são grupos. (dizendo se é abeliano). E caso não seja indicar os contra exemplos.

ⓐ $(\mathbb{R}, *)$ em que $x * y := xy + x + y$

1. $(a * b) * c = (ab + a + b) * c$
$= (ab + a + b)c + (ab + a + b) + c$
$= (bc + b + c)a + a + (bc + b + c)$
$= a * (bc + b + c)$
$= a * (b * c)$

2. Se existe e elemento neutro de G vale que, $\forall x \in G$
$e * x = ex + e + x = x$
$\Rightarrow e(1 + x) = x - x$
$\Rightarrow e = 0$
e temos que
$x * e = ex + x + e$
$= 0x + x + e$
$= x$

3. Seja $x \in G$, se existe x^{-1} deve valer que
$x * x^{-1} = xx^{-1} + x + x^{-1} = e$
$\Rightarrow x^{-1}(1 + x) = -x$
$\Rightarrow x^{-1} = -\frac{x}{1+x} \in \mathbb{R}.$

4. $\forall a, b \in G,$
$a * b = ab + a + b$
$= ba + b + a$
$= b * a$

~~Logo, é um grupo abeliano~~

Note que, -1 não possui inverso logo não é um grupo.

(b) $(\mathbb{R} \setminus \{-1\}, *)$ em que $x * y := xy + x + y$

Pelo item anterior, é um grupo abeliano.

(c) $(G, \cdot)$ em que $G = \{z \in \mathbb{C} \mid z^{2023} = 1\}$

~~Não satisfaz a existência de elemento inverso, se $z = -1 \in G$ mas~~

0. Para quaisquer elementos $z_1, z_2 \in G$,

$$\cancel{z_1^{2023} z_2^{2023} = (z_1 . z_2)^2}$$

$$(z_1 . z_2)^{2023} = z_1^{2023} . z_2^{2023} = 1 . 1 = 1$$

1. Desde que a associatividade da multiplicação nos complexos vale, este grupo é também associativo

2. Seja e um elemento neutro do grupo, temos que, $\forall z \in G$, vale que

$$\cancel{(z.e)\ z^{2023}}$$

$$\cancel{z.e = z}$$

$$\cancel{\Rightarrow z^{2023} . e^{2023}}$$

$$z.e = e.z = 1 \quad e \quad e^{2023} = 1$$

O e que satisfaz isso é $e = 1$.

3. $\forall z \in G$, $\exists z^{-1}$ tal que

$$z . z^{-1} = z^{-1} . z = 1$$

Para tal tomemos $z^{-1} = z^{2022}$. Por definição,

$$z . z^{2022} = z^{2023} = 1$$

4. Desde que a multiplicação seja comutativa nos complexos, vale que o grupo é abeliano.

④ Considere o produto cartesiano $G = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, juntamente com a operação binária

$$(a,b)*(c,d) = (a+2^b c, b+c)$$

em que as operações da primeira ordem são feitas módulo 5 e as da segunda camada, módulo 4. Mostre que $(G,*)$ é um grupo.

(i) $(a,b)*(c,d) = (a,b) \Rightarrow$

$\Rightarrow (a+2^b c, b+d) = (a,b)$

$\Rightarrow c=0$ e $d=0 \Rightarrow (0,0)$ é elemento neutro.

(ii) $(a,b)*((c,d)*(e,f)) = (a,b)*(c+2^d e, d+f)$

$= (a+2^b(c+2^d e), b+d+f)$

$= ((a,b)*(c,d))*(e,f).$

$\Rightarrow$ vale associatividade.

(iii) $(a,b)*(c,d) = (0,0) \Rightarrow (a+2^b c, b+d) = (0,0)$

$\Rightarrow d=-b$ e $c = -\frac{a}{2^b} \Rightarrow \exists$ elemento neutro.

3

~~3) Determine quais dos~~

d) $(G,+)$ em que $G = \{ a+b\sqrt{3} \mid a, b \in \mathbb{Q}\}$

0. Seja $x_1, x_2 \in G$, $\exists a_1, a_2, b_1, b_2 \in \mathbb{Q}$ tais que, $x_1 = a_1 + b_1\sqrt{3}$, $x_2 = a_2 + b_2\sqrt{3}$

$$x_1 + x_2 = a_1 + b_1\sqrt{3} + a_2 + b_2\sqrt{3}$$
$$= (a_1 + a_2) + (b_1 + b_2)\sqrt{3}$$

Como a soma de racionais é racional $x_1 + x_2 \in G$.

1. Desde que a soma nos reais seja associativa, a soma é associativa em G.

2. Se existe um elemento neutro e, vale que $\forall\, x = a + b\sqrt{3}$

$$x + e = x$$
$$\Rightarrow a + b\sqrt{3} + e = a + b\sqrt{3}$$
$$\Rightarrow e = 0 + 0\sqrt{3} = 0$$

é um elemento neutro de G.

3. $\forall x = a + b\sqrt{3} \in G$, queremos verificar se $\exists x^{-1} = a^{-1} + b^{-1}\sqrt{3}$, tal que

$$x + x^{-1} = x^{-1} + x = e,$$

ou seja,

$$a + b\sqrt{3} + a^{-1} + b^{-1}\sqrt{3} = 0$$
$$\Leftrightarrow a^{-1} = -a \text{ e } b^{-1} = -b,$$

pois b é coeficiente de um termo $\mathbb{R} \setminus \mathbb{Q}$ e a é $\mathbb{Q}$. Logo, $x^{-1} = -x$ é elemento inverso de x.

4. Como $a + b\sqrt{3} \in \mathbb{R}$, $\forall a, b$, e a soma é comutativa em $\mathbb{R}$ em particular é comutativa em G.

Daí G é um grupo abeliano.

(e) $(G,+)$ em que $G = \{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z}$ e b é ímpar$\}$

0. Seja $a/b, x/y \in G$, temos que

$$a/b + x/y = \frac{ay + xb}{by}$$

temos que $ay + xb, by \in \mathbb{Z}$, mas by não é ímpar, e sim par, pois produto de ímpares é ímpar. Daí $(G,+)$ não é grupo.

(f) $(G,\cdot)$ em que $G = \{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z}$ e b é ímpar$\}$

0. Seja $a/b, x/y \in G$, o produto

$$a/b \cdot x/y = \frac{ax}{by}$$

Analogamente ao item anterior by é par. Então $(G,\cdot)$ não é um grupo.

(g) $(\mathbb{R}^3, \times)$ em que $\times$ denota o produto vetorial.

O produto vetorial não é associativo de fato, seja um contra exemplo, i, j, k a base padrão do $\mathbb{R}^3$

$$\begin{aligned}(a \times b) \times c &= (i \times j) \times k \\ &= k \times k = 0 \\ a \times (b \times c) &= i \times (j \times k) \\ &= i \times -i = -k\end{aligned}$$

Logo, $(\mathbb{R}^3, \times)$ não é um grupo.

(h) $(G, \circ)$ em que $G = \{ f : [0,1] \to [0,1] \mid f$ é uma bijeção continuação$\}$.

0. Seja $f, g \in G$, temos que $f \circ g \in G$ pois é bijetora e tem domínio igual a imagem.

1. Para funções bijetoras a composição de funções é associativa.

2. Se existe um elemento neutro $f_e \in G$, $\forall f \in G$

$$(f \circ f_e)(x) = f(x)$$

A função $f_e(x)$ que igual elementos é a Identidade.

3. Como $\forall f \in G$ é bijetora possui função inversa tal que,

$$f \circ f^{-1} = f^{-1} \circ f = Id$$

4. Seja $f^{-1} : [0,1] \to [0,1]$ e $g^{-1} : [0,1] \to [0,1]$ que existem pelas propriedades anteriores vale que,

(a)
$$\begin{aligned}(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ f \circ f^{-1} \circ g^{-1} \\ &= g \circ Id \circ g^{-1} \\ &= g \circ g^{-1} = Id\end{aligned}$$

(b)
$$\begin{aligned}(f \circ g) \circ (g^{-1} \circ f^{-1}) &= f \circ g \circ g^{-1} \circ f^{-1} \\ &= f \circ Id \circ f^{-1} \\ &= f \circ f^{-1} = Id\end{aligned}$$

Daí, $g \circ f$ e $f \circ g$ são ambos ~~invos~~ inversos da outra e $(G, \circ)$ é um grupo abeliano.

⑤ Seja G um grupo. Mostre que se $(a.b)^2 = a^2.b^2$ $\forall a,b \in G$ então é abeliano.

por absurdo
Suponha que não vale que G é abeliano, ou seja, $\exists a,b, \in G$ tais que $ab \neq ba$. Daí temos que

$$\begin{aligned}(a\ b)^2 &= a\,b\,a\,b \\ &\neq a\,a\,b\,b \\ &= a^2 . b^2\end{aligned}$$

Logo, deve valer a implicação se $(ab)^2 = a^2 b^2$, $\forall a.b \in G$ então G é abeliano.

⑥ Seja $A \neq \emptyset$ um conjunto qualquer e denote por $\mathbb{R}^A = \{f : A \to \mathbb{R}\}$ o conjunto de todas as funções de A em $\mathbb{R}$. Mostre que

(a) $\mathbb{R}^A$ juntamente com a operação de soma de funções é um grupo abelliano.
(b) $\mathbb{R}^A$ juntamente com a operação de produto de funções não é um grupo.
(c) $\{f \in \mathbb{R}^{[0,1]} \mid f$ é contínua$\}$ é um subgrupo de $\mathbb{R}^{[0,1]}$.

(a) $f, g \in \mathbb{R}^A$, $f+g : A \to \mathbb{R}$

- $+$ é associativa e comutativa
- ~~f(0)~~ $f(x) = 0 \Rightarrow f \in \mathbb{R}^A$
- $f(x) \in \mathbb{R}$, $g(x) = -f(x) \Rightarrow g(x) \in \mathbb{R}^A$, $g = f'$

É um grupo abelliano

(b) Seja $f(x) = 0$, então $f \in \mathbb{R}^A$
Para todo $g \in \mathbb{R}^A$, $f \cdot g = f$, logo f não é o elemento neutro. Logo, $f \cdot g \neq e$ para todo $g \in \mathbb{R}^A$. Portanto $f \in \mathbb{R}^A$ não é invertível e $(\mathbb{R}^A, \times)$ não é um grupo

(c) $f(x) = 0$ então f é contínua
f é contínua então $-f$ é contínua
Se f e g são contínuas então $f+g$ é contínua
$\{f \in \mathbb{R}^{[0,1]} \mid f$ contínua$\}$ é fechado por adição, logo o conjunto com adição é subgrupo de $(\mathbb{R}^{[0,1]}, +)$.

(7) Seja $M_n(\mathbb{R})$ o conjunto das matrizes $n \times n$ com entradas reais.

(a) Mostre que $M_n(\mathbb{R})$ com soma é um grupo abeliano

0. $\forall A, B \in M_n(\mathbb{R})$, vale que $A+B \in M_n(\mathbb{R})$

1. $\forall A, B \in M_n(\mathbb{R})$, sendo que a soma de reais é real, e para $\{a_{ij}\}, \{b_{ij}\}$ matrizes $n \times n$ vale que $a_{ij} + b_{ij} = b_{ij} + a_{ij}\ \forall ij$. ~~Vale que~~, Logo, $A+(B+C) = (A+B)+C$

2. $\forall A \in M_n(\mathbb{R})$, queremos que $\exists E = \{e_{ij}\} \in M_n(\mathbb{R})$ tal que,

$$A + E = A$$

Podemos escrever uma matriz como seus elementos $A = \{a_{ij}\}$, se E é neutro $a_{ij} + e_{ij} = a_{ij}\ \forall ij$. Logo, $e_{ij} = 0\ \forall ij$.

3. $\forall A = \{a_{ij}\} \in M_n(\mathbb{R})$, queremos que $\exists B = \{b_{ij}\}$ tal que

$$A + B = E = 0_{n \times n}$$

Ou seja, $b_{ij} = -a_{ij}$, $\forall ij$

4. Sendo $A = \{a_{ij}\}, B = \{b_{ij}\} \in M_n(\mathbb{R})$, deve valer $a_{ij} + b_{ij} = b_{ij} + a_{ij}\ \forall ij$, que é válido para a soma em $\mathbb{R}$.

(b) Quais os seguintes conjuntos é um subconjunto de $(M_n(\mathbb{R}), +)$?

(i), (iii), (iv) e (vii).

~~Aproximando $V(z,\sigma,\rho)$~~

~~Nossa aproximação para~~

Nosso objetivo é aproximar $W(z,\sigma,\rho)$ com

$$\hat{W}(z,\sigma,\rho) = \sum_{i=i_L}^{i_U} W_i$$

e $V(z,\sigma,\rho)$ com

$$\hat{V}(z,\sigma,\rho) = \sum_{K=K_L}^{K_U} V_K$$

onde i_L, i_U e K_L, K_U são limites escolhidos.
O fato de que um ~~log~~ $\partial \log W_i$ é monotônico decrescente implica que $\log W_i$ é estritamente convexo como função de i e, portanto que o W decai mais rapido que geometricamente em qualquer lado de i_{max}.
O erro de aproximação pode, portanto, ser limitado por somas geométricas:

$$W(z,\sigma,\rho) - \hat{W}(z,\sigma,\rho) < W_{i_L-1}\frac{1-r_L^{i_L-1}}{1-r_L} + W_{i_U-1}\frac{1}{1-r_U}$$

onde $$r_L = \exp\left(\frac{\partial \log W_i}{\partial i}\right)\Bigg|_{i=i_L-1}$$

e

$$r_U = \exp\left(\frac{\partial \log W_i}{\partial i}\right)\Bigg|_{i=i_U+1}$$

* O mesmo tipo de limite pode construido para $V(z,\sigma,\rho) - \hat{V}(z,\sigma,\rho)$ em termos de $V_{ent}(K)$.
Na prática esses limites geométricos são muito "conservadores", então simplesmente escolhemos $i_L < i_{max} < i_U$

8) Em um grupo G, dois elementos satisfazem $a^5 = e$ e $a^3 b = b a^3$. Prove que $ab = ba$.

Começando com

$$a^3 b = b a^3$$

$$\Leftrightarrow a^{-3} a^3 b = a^{-3} b a^3$$

$$\Leftrightarrow b = a^{-3} b a^3$$

$$\Leftrightarrow b = a^2 b a^3 \quad (\text{usando que } a^5 = e)$$

$$\Leftrightarrow ab = a^3 b a^3$$

$$\Leftrightarrow ab = b a^3 a^3 \quad (\text{usando que } a^3 b = b a^3)$$

$$\Leftrightarrow ab = b e a = ba$$

(9) Determine o centro e o subgrupo derivado do exercício 1.

Os elementos $\{f_0, f_1, f_2\}$ formam um centro, segundo a tabela. E $\{f_0, f_1\}$ formam um subgrupo de G.

(10) Seja G um grupo e $H \subseteq G$ um subgrupo não vazio.

(a) Mostre que $H \leq G$ se, e só se, H possui a seguinte propriedade: $a, b \in H \Rightarrow ab^{-1} \in H$.

(b) Suponha que H seja finito. Mostre que $H \leq G$ se, e só se, H é fechado por produto. Mostre que a conclusão pode ser falsa ~~para~~ se H é infinito.

(a) $a = b \Rightarrow aa^{-1} \in H \Rightarrow e \in H$

$e, a \in H \Rightarrow ea^{-1} \in H \Rightarrow a^{-1} \in H \quad (\forall a \in H)$

$\forall a, b \in H \Rightarrow a^{-1} \in H \Rightarrow b(a^{-1})^{-1} \in H \Rightarrow ba \in H$

Logo, H é subgrupo de G

(b) $(\Rightarrow)$ H é subgrupo de G então H é fechado

$(\Leftarrow)$ H é fechado por produto, então $a \in H \Rightarrow a^2 \in H \Rightarrow a^3 \in H \Rightarrow \dots \Rightarrow a^{|H|} \in H \Rightarrow a^{|H|+1} \in H$. Como esses $|H|+1$ elementos pertencem a um conjunto de $|H|$ elementos pertencem a um conjunto de $|H|$ elementos, pelo PCP ~~∃~~ existe $m < n$ t.q. $a^m = a^n \Rightarrow a^m . a^{n-m} = a^n . a^{n-m}$ $\Rightarrow a^n = a^n a^{n-m} \Rightarrow a^{n-m} = e$, logo é um subgrupo.

Números inteiros positivos e a operação (+). É fechado por produto não não é subgrupo de $(\mathbb{Z}, +)$.

(11) A sequencia de Fibonacci F_n é a sequencia definida recursivamente por $F_0 = 0$, $F_1 = 1$ e $F_n = F_{n-1} + F_{n-2}$ para $n \geq 2$. Assim os seus próximos valores são $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$; $F_6 = 8$, $F_7 = 13, \dots$

(a) Mostre que, para todo $n \geq 0$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

(b) Sejam $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$. Mostre que $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ e $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ são conjugados em $GL_2(\mathbb{R})$.

(c) Utilizando os itens anteriores conclua que

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{para } n \geq 0.$$

(a) Vamos provar por indução. Se $n = 0$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} F_1 & F_0 \\ F_0 & F_{-1} \end{pmatrix}$$

Suponha que vale para n:

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

$$= \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} F_{n+1} + F_n & F_{n+1} \\ F_n + F_{n-1} & F_n \end{pmatrix} = \begin{pmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{pmatrix}$$

Então vale para $n+1$. Por indução, vale para $n \geq 0$

(b) $$\underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}}_{\text{invertível}} = \underbrace{\begin{pmatrix} \beta & \alpha \\ 1 & 1 \end{pmatrix}}_{\text{invertível}} \underbrace{\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}}_{\text{invertível}} \begin{pmatrix} \beta & \alpha \\ 1 & 1 \end{pmatrix}^{-1}$$

(c) $\begin{pmatrix}1&1\\1&0\end{pmatrix}^n = \begin{pmatrix}\beta&\alpha\\1&1\end{pmatrix}\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix}^n\begin{pmatrix}\beta&\alpha\\1&1\end{pmatrix}^{-1}$

$$= \begin{pmatrix}\beta&\alpha\\1&1\end{pmatrix}\begin{pmatrix}\alpha^n&0\\0&\beta^n\end{pmatrix}\begin{pmatrix}\beta&\alpha\\1&1\end{pmatrix}^{-1} \rightarrow \cancel{\begin{pmatrix}1&-\beta\\-1&\alpha\end{pmatrix}} \begin{pmatrix}-1&\alpha\\1&-\beta\end{pmatrix}\cdot\frac{1}{\alpha-\beta}$$

$$= \frac{1}{\alpha-\beta}\begin{pmatrix}\beta\alpha^n&\alpha\beta^n\\\alpha^n&\beta\end{pmatrix}\begin{pmatrix}\beta&\alpha\\1&1\end{pmatrix}^{-1}$$

$$\cancel{\Rightarrow F_n = \frac{-\beta\alpha^n+\alpha\beta^n}{\alpha-\beta}}$$

$$\Rightarrow F_n = \frac{\alpha^n-\beta^n}{\alpha-\beta}$$

(12) Sejam $A, B \in GL_2(\mathbb{C})$. Mostre que se A e B são conjugados em $GL_2(\mathbb{R})$, então $\det A = \det B$ e $\operatorname{Tr} A = \operatorname{Tr} B$. Mostre que a recíproca não é verdadeira

Sendo A e B conjugados, ou seja, $\exists P \in G$ tal que $A = PBP^{-1}$.

$$\begin{aligned}
\det A &= \det(PBP^{-1}) \\
&= \det P \det B \det P^{-1} \\
&= \det P \det P^{-1} \det B \\
&= \det(PP^{-1}B) \\
&= \det(IB) \\
&= \det(B)
\end{aligned}$$

$$\begin{aligned}
\operatorname{tr} A &= \operatorname{tr}(PBP^{-1}) \\
&= \operatorname{tr}(BPP^{-1}) \\
&= \operatorname{tr}(BI) \\
&= \operatorname{tr} B
\end{aligned}$$

Não vale a volta, temos o contra exemplo:

$A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ e $B = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$. $\nexists P \in G$ t.q.

$A = PBP^{-1}$.

13 (a) Seja G um grupo abeliano finito e seja

$$x = \prod_{g \in G} g$$

o produto de todos os elementos de G. Mostre que $x^2 = e$.

(b) (Teorema de Wilson) Seja p primo. Mostre que

$$(p-1)! \equiv -1 \pmod p$$

(a) Como G é abeliano, basta reorganizar o produto para cada elemento cancelar com seu inverso.

Como cada elemento de G tem seu ~~seu~~ inverso exclusivo em G, então não vai faltar/sobrar inverso.

(b) $(p-1)!$ é o produto de todos os elementos do grupo $\mathbb{Z}_p^*$, portanto $((p-1)!)^2 = e = 1$

$$a^2 \equiv 1 \pmod p \Rightarrow a \equiv \pm 1 \pmod p$$

Logo, em $\mathbb{Z}_p^*$ apenas 1 e -1 são seus inversos, portanto em $(p-1)!$ todos os outros números vão cancelar

$$(p-1)! \equiv 1 \cdot (-1) \equiv -1 \pmod p$$

(14) Mostre que $S = 1^6 + 2^6 + 3^6 + \cdots + 100^6$ é divisível por 101.

$$2^6 S = 2^6 . 1^6 + 2^6 . 2^6 + \cdots + 2^6 . 50^6 + 2^6 . 51^6 + \cdots + 2^6 . 99^6 + 2^6 . 100^6$$
$$\equiv 2^6 + 4^6 + 6^6 + \cdots + 100^6 + 1^6 + \cdots + 97^6 + 99^6 \equiv S \pmod{101}$$

$\Rightarrow (2^6 - 1) S \equiv 0 \pmod{101}$ $\quad (2^6 - 1) \equiv 63$

$\Rightarrow 63 . S \equiv 0 \pmod{101}$

$\Rightarrow 63^{-1} . 63 . S \equiv 0 \pmod{101} \Rightarrow S \equiv 0 \pmod{101}$

($\mathbb{Z}_{101}^*$ é um grupo, então 63 tem inversa.

(15) Seja G um grupo. Se $(ab)^i = a^i b^i$ para 3 inteiros i consecutivos e $\forall a, b \in G$, prove que G é abeliano.

Seja $i = j, j+1, j+2$ esses inteiros tais que, $(ab)^i = a^i b^i$, $\forall a, b \in G$. Podemos escrever

$$\cancel{(ab)}$$

$$\underbrace{ab \ldots ab}_{j+2} = \underbrace{a \ldots a}_{j+2} \underbrace{b \ldots b}_{j+2}$$

$$\Rightarrow abab(ab)^j = aa(a^j b^j)bb$$

$$\Rightarrow abab = aabb$$

$$\Rightarrow (ab)^2 = a^2 b^2$$

Pela questão (5) segue o resultado