



UNIVERSIDADE DE SÃO PAULO

INSTITUTO DE CIÊNCIAS MATEMÁTICAS E
COMPUTACIONAIS - ICMC

Notas de Aula de Álgebra

Renan Wenzel - 11169472

Roberto Carlos - alvarago@icmc.usp.br

25 de março de 2023

Conteúdo

1	Aula 01 - 14/03/2023	3
1.1	Motivações	3
1.2	Introdução ao Curso	3
1.3	Grupos e Operações	3
2	Aula 02 - 16/03/2023	5
2.1	Motivações	5
2.2	Usos de Grupos	5
2.3	Subgrupos	6
3	Aula 03 - 21/03/2023	8
3.1	Motivações	8
3.2	Subgrupos - Outras Propriedades	8
4	Aula 04 - 23/03/2023	10
4.1	Ciclos e Grupos de Permutação	10
4.2	Morfismos de Grupos	11

1 Aula 01 - 14/03/2023

1.1 Motivações

- Compreender o que será estudado ao longo do curso;

1.2 Introdução ao Curso

Este curso é sobre teoria de grupos, a qual possui origem no estudo de simetrias, sejam elas de figuras ou de objetos algébricos. Um exemplo de grupo seria o seguinte:

Considere um triângulo equilátero. Existem algumas formas de olharmos para as simetrias do triângulo, como rotacionando-o, refletindo-o com relação a um ponto médio e um vértice fixo. Contabilizando todas as possíveis formas delas acontecerem, há seis simetrias deste retângulo. Ademais, compondo simetrias resulta em outra, i.e., rotacionar e refletir um certo vértice continuará sendo uma simetria do triângulo. Além disto, é um fato (futuramente visto) que essas seis simetrias totalizam todas as possíveis simetrias de um triângulo equilátero. De fato, dado um polígono regular de n lados, ele possui $n!$ simetrias.

1.3 Grupos e Operações

Definição. Seja S um conjunto não-vazio. Uma operação em S é um mapa

$$\begin{aligned}\mu : S \times S &\rightarrow S \\ (a, b) &\mapsto \mu(a, b)\end{aligned}$$

Exemplo 1. A operação soma em \mathbb{Z} , $+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, $(a, b) \mapsto a + b$ é uma operação.

Exemplo 2. Uma operação em \mathbb{R} é a multiplicação $.: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, $(a, b) \mapsto ab$.

Exemplo 3. Um exemplo do que não é operação seria a subtração dos naturais, $-: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, $(a, b) \mapsto a - b$. (Consegue responder por que não é?)

Exemplo 4. Se S é o conjunto de simetrias de um triângulo equilátero, então a composição

$$\begin{aligned}\circ : S \times S &\rightarrow S \\ (\sigma, \tau) &\mapsto \sigma \circ \tau\end{aligned}$$

é uma operação binária.

Faremos a convenção de denotar $\mu(a, b)$ por $a.b$ ou $a + b$, com base no contexto.

Definição. Uma operação μ em S não-vazio, denotada pelo produto, é dita associativa se, para todos a, b, c em S ,

$$(a.b).c = a.(b.c), \quad \left(\mu(a, \mu(b, c)) = \mu(\mu(a, b), c) \right).$$

Por outro lado, será dita comutativa se

$$a.b = b.a, \quad \left(\mu(a, b) = \mu(b, a) \right).$$

Diremos, também, que ela tem elemento neutro (ou identidade) se existe um elemento e em S tal que

$$a.e = e.a = a, \forall a \in S.$$

Neste caso, diremos que e é o elemento neutro, ou a identidade, para μ .

Utilizaremos a notação 1 para a identidade no caso em que μ é denotada por um produto e 0 pro caso em que é denotada por adição.

Exemplo 5. A multiplicação de matrizes é associativa, não é comutativa e possui identidade.

Exemplo 6. A soma de números inteiros é associativa, comutativa e possui identidade.

Exemplo 7. A potência nos números reais é não associativa, nem comutativa, mas possui identidade:
 $a^{(b^c)} \neq (a^b)^c = a^{bc}$

Proposição. Seja S um conjunto não-vazio e μ uma operação em S denotada pelo produto. Então, existe um único jeito de definir o produto (denotado temporariamente por $[a_1, \dots, a_n]$) de n elementos em S tal que

- (i) $[a_1] = a_1$;
- (ii) $[a_1, a_2] = \mu(a_1, a_2) = a_1 a_2$;
- (iii) $\forall 1 \leq i < n, [a_1, \dots, a_n] = [a_1, \dots, a_i][a_{i+1}, \dots, a_n]$.

Prova. (iii) \Rightarrow Para o caso $n \leq 2$ é ok. Agora, suponha o produto bem-definido de r elementos em S , $r \leq n = 1$. Então, defina $[a_1, \dots, a_n] := [a_1, \dots, a_{n-1}][a_n]$. Como a definição acima satisfaz a condição (iii) para $i=n-1$, se ela estiver bem-definida, ela será única. Com efeito, seja $1 \leq i < n - 1$, tal que

$$\begin{aligned} [a_1, \dots, a_n] &= [a_1, \dots, a_{n-1}][a_n] = [a_1, \dots, a_i][a_{i+1}, \dots, a_{n-1}][a_n] \\ &= \left([a_1, \dots, a_i] \right) \left([a_{i+1}, \dots, a_{n-1}][a_n] \right) \\ &= [a_1, \dots, a_i][a_{i+1}, \dots, a_n]. \blacksquare \end{aligned}$$

Definição. Seja S não-vazio e μ uma operação em S com identidade 1. Um elemento a de S é dito inversível se existe b em S tal que $ab = ba = 1$. Neste caso, b é o inverso de a , denotado por $b := a^{-1}$.

Note que tanto o elemento inverso quanto o elemento neutro, se existirem, são únicos (c.f. Lema abaixo). Além disso, o inverso da adição é denotado por $-a$.

Lema. Seja S não-vazio, μ uma operação associativa denotada pelo produto. Então,

- i) Existe no máximo um elemento neutro para S e μ ;
- ii) Se o elemento neutro existe, então para cada elemento de S , existe no máximo um inverso;
- iii) Se um elemento a de S tem inverso à esquerda l e à direita r , i.e. $l.a = 1$ e $a.r = 1$, então a é inversível com inverso $l = r$.
- iv) Se a, b em S são inversíveis, então o produto ab é inversível, com inverso $b^{-1}a^{-1}$.

Antes de provar, observe que a existência de um elemento inverso à esquerda ou à direita não garante que um elemento seja inversível (exercício), eles devem coincidir.

Prova. (i) \Rightarrow Suponha que existem $1, 1'$ em S como seus elementos neutros. Basta mostrarmos que eles coincidem. Com efeito,

$$1 = 1.1' = 1'.1 = 1'.$$

Portanto, o elemento neutro é único.

(ii) \Rightarrow Assuma a existência de dois elementos inversos em S para um elemento a , denotados por b, b' . Então, como $ab = ba = 1$, temos

$$b = b1 = b(ab') = (ba)b' = 1b' = b'.$$

Portanto, o elemento inverso é único. Os itens (iii) e (iv) são exercícios. \blacksquare

Definição. Um monoide é um par (G, μ) , em que G é um conjunto não-vazio e μ uma operação associativa e com elemento neutro em G . Se, ainda por cima, μ for comutativa, (G, μ) é um monoide abeliano (ou comutativo).

Definição. Um grupo é um par (G, μ) é um monoide (G, μ) com a condição extra que todo elemento de G possui inverso. Caso μ seja comutativa, chamamos G de grupo abeliano.

Exemplo 8. Os inteiros com a soma, $(\mathbb{Z}, +)$, é um grupo comutativo, enquanto (\mathbb{Z}, \cdot) não é um grupo, mas sim um monoide.

Exemplo 9. O grupo das matrizes com entradas reais e sua multiplicação, $(M_n(\mathbb{R}), \cdot)$, é um grupo não-abeliano.

2 Aula 02 - 16/03/2023

2.1 Motivações

- Outras estruturas algébricas e exemplos;
- Tamanho de um grupo;
- Subgrupos

2.2 Usos de Grupos

Podemos usar grupos para definir outras construções algébricas, como segue.

Definição. Um anel é uma terna (A, μ, ϕ) , em que (A, μ) é um grupo abeliano e (A, ϕ) é um monoide. Além disso, vale a distributiva.

$$\phi(a, \mu(c, d)) = \phi(\mu(a, c), \mu(a, d)), \quad (a(b + c) = ab + ac).$$

Usualmente, escrevemos $(A, \mu, \phi) = (A, +, \cdot)$. \square

Definição. Um corpo é um anel $(A, +, \cdot)$ tal que $(A - \{0\}, \cdot)$ é um grupo abeliano. \square

Deste ponto em diante, abandonaremos as letras gregas para usar apenas os símbolos “+” ou “ \cdot ” para um grupo com adição ou com multiplicação. Vejamos alguns exemplos.

Exemplo 10.

Conjunto	Monoide	Monoide Comutativo	Grupo	Grupo Comutativo
(GL_n, \cdot)	Sim	Não	Sim	Não
(SL_n, \cdot)	Sim	Não	Sim	Não
$(\mathbb{Z}, +)$	Sim	Sim	Sim	Sim
(\mathbb{Z}, \cdot)	Sim	Sim	Não	Não
$(\mathbb{Q}, +)$	Sim	Sim	Sim	Sim
(\mathbb{Q}, \cdot)	Sim	Sim	Não	Não
$(S = \{z \in \mathbb{C} : z = 1\}, \cdot)$	Sim	Sim	Sim	Sim
$(M_n(\mathbb{R}), +)$	Sim	Sim	Sim	Sim
$(M_n(\mathbb{R}), \cdot)$	Sim	Não	Não	Não

Exemplo 11. Seja T um conjunto qualquer e

$$G = \{f : T \rightarrow T : f \text{ bijetora}\}$$

Então, (G, \circ) é um grupo, chamado grupo das permutações ou simetrias de T . Se T é um conjunto finito, e.g. $T = \{1, \dots, n\}$, então denotamos (G, \circ) por (S_n, \circ) . \blacksquare

Definição. A ordem de um grupo (G, \cdot) é a cardinalidade de G : $|G|$. Caso $|G| < \infty$, dizemos que $(G, +)$ é um grupo finito. \square

Exemplo 12. A ordem de $|\mathbb{Z}| = \infty$ e $|S_n| = n!$ ■

Proposição. Se (G, \cdot) é um grupo e a, b, c são elementos de G tais que $ab = ac$ ou $ba = ca$, então $b = c$. Além disso, se $ab = a$ ou $ba = a$, então $b = 1$.

Prova. Seja a^{-1} o inverso de a , então $a^{-1}(ab) = a^{-1}(ac)$. Mais ainda, se $ab = a$, então $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}a = 1$.

Fica de exercício mostrar que só existe um grupo de ordem 2 e que S_3 é um grupo não-comutativo.

2.3 Subgrupos

Definição. Um subgrupo H de um grupo (G, \cdot) é um subconjunto H de contido em G tal que

- 1) $1 \in H$;
- 2) $a, b \in H \Rightarrow ab \in H$;
- 3) $a \in H \Rightarrow a^{-1} \in H$.

Denotaremos subgrupos por $H \leq G$ ou $(H, \cdot) \leq (G, \cdot)$. □

Proposição. Com operação induzida pela multiplicação de G restrita a H , (H, \cdot) é um grupo.

Prova. Como H está contido em G , podemos restringir o produto de G a H para

$$\cdot_H : H \times H \rightarrow H.$$

Afirmamos que (H, \cdot) é um grupo. Com efeito, a restrição de \cdot a H está bem-definida pelo segundo item da definição de subgrupo. Mais ainda, ela é associativa em H por ser em G e todo elemento em H tem inverso pela condição 3. Por fim, ela tem elemento neutro pela primeira requisição ao definir subgrupo. Portanto, (H, \cdot) é um grupo.

Observe que todo grupo tem ao menos dois subgrupos, chamados triviais, sendo eles $\{1\}$ e ele mesmo. Qualquer outro leva o nome de subgrupo próprio.

Exemplo 13. $(SL_n, \cdot) \leq (GL_n, \cdot)$ e $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$. ■

Exemplo 14. Seja n um inteiro, então $n\mathbb{Z} := \{nk : k \in \mathbb{Z}\}$ é um subgrupo dos inteiros. De fato, $0 = n0$ pertence a $n\mathbb{Z}$. Além disso, se nk e nk' pertencem a $n\mathbb{Z}$, então

$$nk + nk' = n(k + k') \in n\mathbb{Z}.$$

Por fim, se nk pertence a $n\mathbb{Z}$, então $n(-k)$ também pertence a $n\mathbb{Z}$ e $nk + n(-k) = 0$. ■

Proposição. Todo subgrupo de $(\mathbb{Z}, +)$ é da forma $n\mathbb{Z}$ para algum n inteiro.

Prova. Caso n seja 1, $n\mathbb{Z} = \mathbb{Z}$ e, se $n = 0$, então $n\mathbb{Z} = \{0\}$. Agora, seja H um subgrupo próprio dos inteiros e n o menor inteiro positivo em H . Afirmamos que $n\mathbb{Z} = H$.

De fato, $n\mathbb{Z} \leq H$, pois n é um elemento de H , então $nk = \underbrace{n + \dots + n}_{k\text{-vezes}} \in H$. Além disso, $-n \in H$, de forma que $-nk = \underbrace{(-n) + \dots + (-n)}_{k\text{-vezes}} \in H$. Portanto, $n\mathbb{Z} \in H$.

Por outro lado, seja m um inteiro de H e considere $m = nq + r, 0 \leq r < n, q \in \mathbb{Z}$. Pelo algoritmo de divisão de Euclides,

$$m - nq = r \Rightarrow r \in H \Rightarrow r = 0.$$

e, assim, $m = nq$ pertence a $n\mathbb{Z}$. Portanto, $H = n\mathbb{Z}$. ■

Proposição. 1) $n\mathbb{Z} + m\mathbb{Z}$ é subgrupo de \mathbb{Z} ;

2) $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, em que d é tal que

2.1) $d|n$ e $d|m$;

2.2) Se $l|n$ e $l|m$, então $l|d$;

2.3) Existem r, s inteiros tais que $rn + sm = d$.

Definimos $d = \gcd(n, m)$ como o máximo divisor comum de m e n .

Prova. A prova do item 1 fica como exercício.

2.1) $\Rightarrow n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$. Em particular, se n, m pertencem a $d\mathbb{Z}$, então $d|n$ e $d|m$.

2.2) \Rightarrow Suponha que $n = lq_1, m = lq_2$. Se x pertence a $n\mathbb{Z} + m\mathbb{Z}$, então

$$\begin{aligned}x &= nk_1 + mk_2 = lq_1k_1 + lk_2q_2 \in l\mathbb{Z} \\&\Rightarrow n\mathbb{Z} + m\mathbb{Z} \subseteq l\mathbb{Z} \Rightarrow l|d.\end{aligned}$$

também é possível mostrar isso usando o item 3 da proposição.

2.3) \Rightarrow imediato. ■

Proposição. 1) $m\mathbb{Z} \cap n\mathbb{Z}$ é subgrupo dos inteiros;

2) $m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z}$, em que l é tal que

2.1) $m|l, n|l$;

2.2) Se $m|l'$ e $n|l'$, então $l|l'$.

Definimos $l = \text{mmc}(m, n)$ o mínimo múltiplo comum de m e n .

Prova. Fica como exercício.

Corolário. Se m, n são inteiros, então $mn = \text{mmc}(m, n) \gcd(m, n)$.

3 Aula 03 - 21/03/2023

3.1 Motivações

- Outros exemplos de subgrupos;
- Subgrupos gerado por subconjuntos;
- Grupo cíclico e ordem de elementos.

3.2 Subgrupos - Outras Propriedades

Quando o conjunto candidato a subgrupo é não-vazio, não é necessário exigir que a identidade seja parte dele. De fato,

Proposição. Se G é um grupo e $H \subseteq G, H \neq \emptyset$, então $H \leq G$ se, e somente se,

- 1) $ab \in H, \quad a, b \in H$
- 2) $a^{-1} \in H, \quad a \in H.$

Prova. \Rightarrow Segue da definição de subgrupo (ab e a^{-1} pertencem a H por definição);

\Leftarrow Sendo H não-vazio, existe $a \in H$. Através de (2), $a^{-1} \in H$ e, por (1), $aa^{-1} = 1 \in H$. Portanto, H é subgrupo de G . ■

Outra formulação de subgrupo requer apenas uma condição:

Proposição. Se G é um grupo e $H \subseteq G, H \neq \emptyset$, então $H \leq G$ se, e só se, $ab^{-1} \in H$ para todos $a, b \in H$.

Prova. \Rightarrow Suponha que H é um subgrupo de G e sejam $a, b \in H$. Então, por definição, $a^{-1}, b^{-1} \in H$. Assim, segue da definição de subgrupo que $ab^{-1} \in H$.

\Leftarrow Se $H \neq \emptyset$, existe ao menos um a em H . Por hipótese, $1 = aa^{-1} \in H$. Assim, $a^{-1} = 1a^{-1} \in H$. Por fim, se a, b são membros de H , então $b^{-1} \in H$, tal que $ab = a(b^{-1})^{-1} \in H$. Portanto, H é subgrupo de G . ■

Definição. Se G é um grupo, então $Z(G) = \{g \in G : ga = ag \forall a \in G\}$ é um subgrupo de G chamado centro de G .

Provemos que $Z(G)$ é de fato um subgrupo. De fato, $1 \in Z(G)$ pela definição de elemento neutro. Além disso, se $g, h \in Z(G)$, então $gha = gah = agh$, tal que $gh \in Z(G)$. Além disso, $g^{-1} \in Z(G)$, pois $g^{-1}a = (a^{-1}g)^{-1} = (ga^{-1})^{-1} = ag^{-1}$. Uma propriedade interessante é que G será um grupo abeliano se, e somente se, $Z(G) = G$.

Exemplo 15. Exercício: Dados G_1, G_2 grupo, defina o grupo produto como $G_1 \times G_2 = \{(g_1, g_2) : g_i \in G_i\}$. Encontre uma operação que torne este conjunto um grupo de fato.

Exemplo 16. 1) Se V é um subespaço vetorial de um corpo qualquer \mathbb{K} , então $V \leq \mathbb{K}$.

2) O conjunto

$$SU_2(\mathbb{C}) = \left\{ \begin{bmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{bmatrix} : \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \right\}$$

é um subgrupo de $GL_2(\mathbb{C})$.

3) O conjunto

$$SO_2(\mathbb{R}) = \left\{ \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} : \theta \in \mathbb{R} \right\} \leq GL_2(\mathbb{R})$$

Proposição. Se G é um grupo abeliano, então todo subgrupo de G é também abeliano

Prova. Se $H \leq G, a, b \in H$, em particular a, b também pertencem a G , tal que $ab = ba$. ■

Observe que a recíproca é falsa. Com efeito, o subgrupo

$$\left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R}) : a \in \mathbb{R} \right\}$$

é subgrupo abeliano de $GL_2(\mathbb{R})$. Além disso, a recíproca não vale nem mesmo se todo subgrupo próprio de um grupo for abeliano, visto que todo subgrupo de S_3 é abeliano, mas o próprio S_3 não é.

Definição. Seja G um grupo e $S \subseteq G$ um subconjunto não-vazio. Definimos o conjunto gerado por S como

$$\langle S \rangle := \left\{ a_1 \cdots a_n : a_i \in S \text{ ou } a_i^{-1} \in S \right\}, \quad n \in \mathbb{N} \cup \{0\}.$$

Proposição. $\langle S \rangle$ é um subgrupo de G .

Prova. É claro que $\langle S \rangle \neq \emptyset$. Agora, se $a_1 \cdots a_n (= x), b_1 \cdots b_m (= y) \in \langle S \rangle$, então

$$xy^{-1} = a_1 \cdots a_n (b_1 \cdots b_m)^{-1} = a_1 \cdots a_n b_m^{-1} \cdots b_1^{-1} \in \langle S \rangle.$$

Portanto, pela segunda definição equivalente de subgrupo, $\langle S \rangle \leq G$. ■

Definição. Nas condições da proposição, $\langle S \rangle$ é o subgrupo gerado por S . Caso S seja finito, digamos $S = \{g_1, \dots, g_n\}$, denotamos $\langle S \rangle$ por $\langle g_1, \dots, g_n \rangle$. □

Definição. Sejam G um grupo e g um elemento seu. Se $G = \langle g \rangle$, diremos que G é um grupo cíclico. □

Definição. Se G é um grupo e g seu elemento, definimos a ordem de g (notação: $|g|$ ou $\text{ord}(g)$) como a ordem de $\langle g \rangle$.

Exemplo 17. $\mathbb{Z} = \langle 1 \rangle$ é um grupo cíclico infinito, S_2 é um grupo cíclico finito e S_3 não é cíclico. ■

Atente-se ao fato de que $\langle g \rangle := \{\dots, g^{-2}, g^{-1}, g^0 = 1, g, g^2, \dots\} = \{g^{\mathbb{Z}}\}$

Exemplo 18. Exercício: Calcule as ordens dos elementos de S_2, S_3 .

Note que todo subgrupo de \mathbb{Z} é cíclico. Além disso, se $|G| < \infty$, segue que $|g| < \infty$. Em particular, $|g| \leq |G|$. Vale mencionar também que mesmo se o grupo tem ordem infinita, o grupo cíclico pode ter ordem finita. De fato, se $(G, \cdot) = (\mathbb{R}^\times, \cdot)$, tome $g = 1$. Então, $\langle g \rangle = \{-1, 1\}$, que é finito de ordem 2.

Proposição. Sejam G um grupo e g um elemento seu. Denotemos por S o conjunto dos inteiros n tais que $g^n = 1$. Então,

- i) $S \leq \mathbb{Z}$;
- ii) As potências $g^m, g^n, m \geq n$ são iguais se, e somente se, $g^{m-n} = 1$ (i.e. $m - n \in S$);
- iii) Se $S \neq 0\mathbb{Z}$, então $S = n\mathbb{Z}$ e as potências $1, g, g^2, \dots, g^{n-1}$ são distintas e são todos os elementos em $\langle g \rangle$. Em particular, $|g| = n$.

Prova. (i) \Rightarrow Se m, n pertence a S , então $g^{m-n} = g^m (g^n)^{-1} = 1$, logo $m-n$ pertence a S . É claro que S é não-vazio, pois 0 sempre é um elemento seu.

(ii) \Rightarrow É a lei do cancelamento.

(iii) \Rightarrow Se $S = \{0\}$, é automático. Como $S \leq \mathbb{Z}$, pela classificação dos subgrupos de \mathbb{Z} , existe n em \mathbb{Z} tal que $S = n\mathbb{Z}$. Agora, seja k um inteiro qualquer. Segue da divisão Euclidiana que $k = nq + r, 0 \leq r < n$. Assim, $g^k = g^{nq} g^r = 1 g^r$, tal que $\langle g \rangle \subseteq \{g^0 = 1, \dots, g^{n-1}\}$. Finalmente, pelo item (ii) e da minimalidade de n . ■

Corolário. $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$

Corolário. Se a ordem de g é diferente de zero, então ela é o menor inteiro positivo n tal que $g^n = 1$.

Corolário. Se a ordem de g é $n > 0$, então $g^k = 1$, se, e somente se, $n|k$.

Corolário. Se a ordem de g é $n > 0, k \in \mathbb{Z}$, então $|g^k| = \frac{n}{\text{mdc}(n, k)}$.

4 Aula 04 - 23/03/2023

- Ciclos e Grupo de Permutações
- Morfismo de Grupos
- Classes laterais

4.1 Ciclos e Grupos de Permutação

Introduzimos a seguir o grupo das permutações, denotado S_n .

Definição. Uma permutação $\sigma \in S_n$ é um r -ciclo se existem $a_1, \dots, a_r \in \{1, \dots, n\}$ tais que $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{r-1}) = a_r, \sigma(a_r) = a_1$ e, além disso, $\sigma(j) = j$ para todo j em $\{1, \dots, n\} \setminus \{a_1, \dots, a_r\}$. Dizemos que r é o comprimento de r , e denotamos σ por $\sigma = (a_1 \dots a_r)$. \square

Definição. Um 2-ciclo é chamado transposição. \square

Exemplo 19. Seja $\sigma \in S_5$. Um 5-ciclo é, por exemplo, $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 5, \sigma(5) = 1$, ou $\sigma = (12345) = (34512)$. Um 3-ciclo seria $\sigma(1) = 4, \sigma(2) = 2, \sigma(3) = 1, \sigma(4) = 3, \sigma(5) = 5$ e uma transposição seria $\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 3, \sigma(4) = 4, \sigma(5) = 5$.

Definição. Duas permutações $\sigma, \tau \in S_n$ são disjuntas se para todo $j \in \{1, \dots, n\}$, $\sigma(j) = j$ ou, exclusivamente, $\tau(j) = j$.

Exemplo 20. $\tau \in S_5, \tau = (34), \sigma(12) \Rightarrow \tau, \sigma$ são disjuntas.

Observe que nem toda permutação é um r -ciclo. De fato, $\sigma \in S_5$ dada por $\sigma(1) = 3, \sigma(2) = 4, \sigma(3) = 5, \sigma(4) = 2$ e $\sigma(5) = 1$ não é um r -ciclo. O fato é que toda permutação é o produto de ciclos disjuntos de comprimento maior ou igual a 2. Assim, $\sigma = (135)(24)$ descreve a permutação enviando 1 pra 3, 2 pra 4, 3 pra 5, 4 pra 2 e 5 pra 1.

Exemplo 21. Seja $\sigma \in S_5, \sigma = (12)(13)(15) = (1532)$. Note que lê-se o produto de permutações como a composição de funções, isto é, começa-se pela direita e termina na esquerda (afinal, é a composição de permutações, que são, particularmente, funções!). Deste produtório, vimos que o número 1 é o único que será alterado, i.e., uma permutação após o 1 demarca o fim da ação. Assim, este exemplo indica que 1 se torna 5 e permanece assim (a primeira ação torna 1 no elemento 5). 5 se torna 1, depois 3 e permanece assim ($1 \rightarrow 5 \rightarrow 3 \rightarrow 1$), 2 se torna 1 no final ($2 \rightarrow 2 \rightarrow 2 \rightarrow 1$), 3 se torna eventualmente 2 ($3 \rightarrow 2 \rightarrow 1 \rightarrow 2$) e 4 permanece constante. (P.S. Se essa parte ficar confusa, me chamem no celular pra eu explicar melhor).

Proposição. Toda permutação em S_n é um produto de transposições (2-ciclos). Isto é, $S_n = \langle \text{transposições} \rangle$. Além disso, se $\sigma \in S_n, \sigma = \tau_1 \dots \tau_r = \rho_1 \dots \rho_s$ fatorações em transposições, então $2|r - s$.

Prova. Observe que $\text{Id} = (12)(21) \in \langle \text{transposições} \rangle$. Se $\sigma \in S_n$ é uma permutação qualquer, então σ é o produto de ciclos. Logo, basta verificar a proposição para um r -ciclo σ . Suponha, assim, que $\sigma = (a_1 \dots a_r)$ é um r -ciclo. Com isso, $r = (a_1 a_2)(a_1 a_3) \dots (a_1 a_r)$. ■

Proposição. Exercício: Mostre que qualquer fatoração de um r -ciclo em transposições tem mesma paridade.

Definição. Seja $\sigma \in S_n$. Então, a matriz de permutação σ é

$$U(\sigma) := \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix}$$

em que e_i é o i -ésimo vetor canônico de \mathbb{R}^n . \square

Exemplo 22. Seja $\sigma = (135)(24) \in S_5$. Para esta permutação, a matriz é

$$U(\sigma) = \begin{pmatrix} e_3 \\ e_4 \\ e_5 \\ e_2 \\ e_1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Note que

$$U(\sigma) = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{pmatrix}$$

Proposição. Sejam $\sigma, \tau \in S_n$ e $U(\sigma), U(\tau)$ as matrizes associadas respectivas. Então,

- 1) $U(\sigma)(12 \cdots n)^T = a_1 e_1 + \cdots + a_n e_n \iff \sigma(j) = a_j, \quad j = 1, \dots, n.$
- 2) $U(\sigma)$ sempre tem um único 1 em cada linha e em cada coluna. Reciprocamente, toda matriz desse tipo é uma matriz de alguma permutação.
- 3) $\det U(\sigma) \in \{-1, 1\}.$
- 4) A matriz de permutação de $\tau\sigma$ é $U(\tau) \cdot U(\sigma).$

Prova. Exercício.

Definição. Se $\sigma \in S_n$ e $U(\sigma)$ é a matriz associada, definimos o sinal de σ ($\text{sgn}(\sigma)$) como sendo o $\det(U(\sigma))$. Além disso, diremos que σ é uma permutação par quando $\text{sgn}(\sigma) = 1$ e ímpar quando $\text{sgn}(\sigma) = -1$. \square

Observe que é possível demonstrar que $\text{sgn}(\sigma) = (-1)^r$, em que r é o número de transposições que aparecem na decomposição de σ .

4.2 Morfismos de Grupos

Morfismos de grupos funcionam como funções entre conjuntos, mas que levam em conta a operação existente nos grupos.

Definição. Sejam G, G' dois grupos. Um morfismo de grupos é um mapa $\phi : G \rightarrow G'$ tal que $\phi(gh) = \phi(g)\phi(h)$ para todo g, h em G . \square

Exemplo 23. São morfismos:

$$1) \text{sgn} : S_n \rightarrow \{+1, -1\}, \sigma \mapsto \text{sgn}(\sigma),$$

$$2) \det : GL_n \rightarrow \mathbb{R}^\times, A \mapsto \det(A)$$

$$3) \exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}, \cdot), x \mapsto e^x$$

$$3) \phi : G \rightarrow G', g \mapsto 1',$$

3) Se $H \leq G$, então a inclusão $i : H \rightarrow G, h \mapsto h$ é um morfismo.

$$3.1) \text{ Em particular, } U : S_n \rightarrow GL_n, \sigma \mapsto U(\sigma)$$

$$3) \mathbb{Z} \rightarrow G, n \mapsto g^n, g \in G \text{ fixo.}$$

Proposição. Seja $\phi : G \rightarrow G'$ um morfismo. Então,

$$1) g_1 \cdots g_n \in G, \phi(g_1 \cdots g_n) = \phi(g_1) \cdots \phi(g_n).$$

$$2) \text{ Se } 1 \text{ é o elemento neutro de } G \text{ e } 1' \text{ o elemento neutro de } G', \phi(1) = 1'.$$

$$3) \phi(g^{-1}) = \phi(g)^{-1}.$$

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$$

$$\text{em que } 1' \text{ é o elemento neutro de } G'$$

Prova. 1.) Os casos 1 e 2 são ok. Assim, vamos mostrar por indução. Suponha que vale para $n-1$. Então,

$$\phi(g_1 \cdots \phi_n) = \phi((g_1 \cdots g_{n-1})g_n) = \phi(g_1 \cdots g_{n-1})\phi(g_n) = \phi(g_1) \cdots \phi(g_{n-1})\phi(g_n).$$

$$2.) \phi(1) = \phi(1.1) := \phi(1)\phi(1) \Rightarrow 1' = \phi(1)\phi(1)^{-1} = \phi(1)$$

$$3.) 1' = \phi(1) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) \Rightarrow \phi(g)^{-1} = \phi(g^{-1}). \blacksquare$$

Definição. Se $\phi : G \rightarrow G'$ é um morfismo, defina a imagem de ϕ por $Im\phi := \{u \in G' : \exists x \in G, \phi(x) = u\}$ e o núcleo (ou kernel) de ϕ por $\ker(\phi) := \{x \in G : \phi(x) = 1'\}$, em que $1'$ é o elemento neutro de G' .

Proposição. A imagem de um morfismo $\phi : G \rightarrow G'$ é um subgrupo de G' e o kernel de ϕ é um de G .

Prova. Se y, y' pertencem a $Im\phi$, então existem x, x' em G tais que $\phi(x) = y, \phi(x') = y'$. Assim,

$$yy' = \phi(x)\phi(x') = \phi(xx') \Rightarrow yy' \in Im\phi.$$

Além disso, é claro que $\phi(1) = 1' \in Im\phi$. Finalmente, se y pertence a $Im\phi$, então $\phi(x^{-1}) = \phi(x)^{-1} = y^{-1} \Rightarrow y^{-1} \in Im\phi$. A prova de que $\ker \phi \leq G$ fica como exercício. ■

Definição. Seja $sgn : S_n \rightarrow \{+1, -1\}$. Definimos $A_n = \ker(sgn)$ como o grupo alternado. □

Definição. Se H é um subgrupo de G e g um elemento de G , defina a classe lateral à esquerda de G em H como

$$gH := \{gh : h \in H\}. \quad \square$$

Proposição. Seja $\phi : G \rightarrow G'$ um morfismo e $K = \ker(\phi)$. Se a, b são elementos de G , são equivalentes:

$$1)\phi(a) = \phi(b)$$

$$2)a^{-1}b \in K$$

$$3)b \in aH$$

$$4)aK = bK.$$

Prova.

$$1) \Rightarrow 2) : \phi(a) = \phi(b) \Rightarrow \phi(a^{-1}b) = 1' \Rightarrow a^{-1}b \in K;$$

$$2) \Rightarrow 1) : a^{-1}b \in K \Rightarrow \phi(a^{-1}b) = 1' \Rightarrow \phi(a) = \phi(b);$$

$$1) \Rightarrow 3) : a^{-1}b \in K \text{ se } \exists h \in K \text{ tais que } a^{-1}b = bh \Rightarrow b \in aK;$$

$$3) \Rightarrow 1) : \text{Suponha que } b \in aH, b = ah \Rightarrow \phi(b) = \phi(a)\phi(h) = \phi(a);$$

$$(1) \iff (4) : \text{Exercício. } \blacksquare$$