UNIVERSIDADE DE SÃO PAULO

INSTITUTO DE CIÊNCIAS MATEMÁTICAS E COMPUTACIONAIS - ICMC

Notas de Aula de Álgebra

Renan Wenzel - 11169472

Roberto Carlos - alvarenga@icmc.usp.br

3 de junho de 2023

Conteúdo

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*

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

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

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

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

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

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

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,*

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

Por outro lado, será dita comutativa se

$$a.b = b.a, \quad \Big(\mu(a, b) = \mu(b, a)\Big).$$

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 $[a_1, \cdots, a_n]$) de n elementos em S tal que*

$$\begin{aligned} &(i) \quad [a_1] = a_1; \\ &(ii) \quad [a_1, a_2] = \mu(a_1, a_2) = a_1 a_2; \\ &(iii) \quad \forall 1 \leq i < n, [a_1, \cdots, a_n] = [a_1, \cdots, a_i][a_{i+1}, \cdots, a_n]. \end{aligned}$$

Prova. *(iii)⇒ 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 $[a_1, \cdots, a_n] \coloneqq [a_1, \cdots, a_{n-1}][a_n]$. 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*

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

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 $b \coloneqq a^{-1}$.*

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 denotad 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) ⇒) Suponha que existem 1, 1' em S como seus elementos neutros. Basta mostramos que eles coincidem. Com efeito,*

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

Portanto, o elemento neutro é único.

(ii) ⇒) 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 $(\mathbb{Z}, .)$ não é um grupo, mas sim um monoide.*

Exemplo 9. *O grupo das matrizes com entradas reais e sua multiplicação, $(\mathbb{M}_n(\mathbb{R}), .)$, 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.*

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

Usualmente, escrevemos $(A, \mu, \varphi) = (A, +, \cdot)$. □

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

Deste ponto em diante, abandonaremos as letras gregas para usar apenas os símbolos "+" ou "." 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*
$(S = \{z \in \mathbb{C} : \lvert z\rvert = 1\}, \cdot)$	*Sim*	*Sim*	*Sim*	*Sim*
$(\mathbb{M}_n(\mathbb{R}), +)$	*Sim*	*Sim*	*Sim*	*Sim*
$(\mathbb{M}_n(\mathbb{R}), .)$	*Sim*	*Não*	*Não*	*Não*

■

Exemplo 11. *Seja T um conjunto qualquer e*

$$G = \{f : T \to T : f \text{ bijetora.}\}$$

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

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

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 subrupos 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*

$$._H : H \times H \to H.$$

Afirmamos que $(H, \cdot)$ *é um grupo. Com efeito, a restrição de . 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* $n\mathbb{Z} \coloneqq \{nk : k \in \mathbb{Z}\}$ *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* $nk = \underbrace{n + \ldots + n}_{k\text{-vezes}} \in H$*. Além disso,* $-n \in H$*, de forma que* $-nk = \underbrace{(-n) + \ldots + (-n)}_{k\text{-vezes}} \in H$*. 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*

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

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 $l = mmc(m, n)$ o mínimo múltiplo comum de m e n.

Prova. *Fica como exercício.*

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

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 necessario 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

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

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 e 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*

$$< S >:= \left\{a_1 \cdots a_n : a_i \in S \text{ ou } a_i^{-1} \in S\right\}, \quad n \in \mathbb{N}\square.$$

Proposição. *$< S >$ é um subgrupo de G.*

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

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

Portanto, pela segunda definição equivalente de subgrupo, $< S > \leq G$. ■

Definição. *Nas condições da propsição, $< S >$ é o subgrupo gerado por S. Caso S seja finito, digamos $S = \{g_1, \cdots, g_n\}$, denotamos $< S >$ por $< g_1, \cdots, g_n >$.*□

Definição. *Sejam G um grupo e g um elemento seu. Se $G =< g >$, 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 ord(g)) como a ordem de $< g >$.*

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

Atente-se ao fato de que $< g >:= \{\cdots, g^{-2}, g^{-1}, g^0 = 1, g, g^2, \cdots\} = \{g^{\mathbb{Z}}\}$

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, $< g >= \{-1, 1\}$, 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 $1, g, g^2, \cdots, g^{n-1}$ são distintas e são todos os elementos em $< g >$. 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 $< g > \subseteq \{g^0 = 1, \cdots, g^{n-1}\}$. Finalmente, pelo item (ii) e da minimalidade de n. ■

Corolário. *$< g >= \{1, g, g^2, \cdots, g^{n-1}\}$*

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 $|g^k| = \dfrac{n}{mdc(n, k)}$.*

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 $a_1, \cdots, a_r \in \{1, \cdots, n\}$ tais que $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \cdots, \sigma(a_{r-1}) = a_r, \sigma(a_r) = a_1$ e, além disso, $\sigma(j) = j$ para todo j em $\{1, \cdots, n\}/\{a_1, \cdots, a_r\}$. Dizemos que r é o comprimento de r, e denotamos σ por $\sigma = (a_1 \cdots a_r)$.*□

Definição. *Um 2-ciclo é chamado transposição.* □

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 $j \in \{1, \cdots, n\}, \sigma(j) = j$ ou $\tau(j) = j$.*

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 ($1- > 5- > 3- > 3$), 2 se torna 1 no final ($2- > 2- > 2- > 1$), 3 se torna eventualmente 2 ($3- > 2- > 1- > 2$) 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, $S_n = \langle$transposições$\rangle$. Além disso, se $\sigma \in S_n, \sigma = \tau_1 \cdots \tau_r = \rho_1 \cdots \rho_s$ fatorações em transposições, então $2|r - s$.*

Prova. *Observe que $Id = (12)(21) \in \langle$ 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 $\sigma = (a_1 \cdots a_r$ é um r-ciclo. Com isso, $r = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2)$.* ■

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*

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

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

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) $U(\sigma)(12\cdots n)^T = a_1e_1 + \cdots + a_ne_n \iff \sigma(j) = a_j, \quad j = 1, \cdots, n.$

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* $\sigma(sgn(\sigma))$ *como sendo o* $\det(U(\sigma)$.*Além disso, diremos que* σ *é uma permutação par quando* $sgn(\sigma) = 1$ *e ímpar quando* $sgn(\sigma) = -1$. □

Observe que é possível demonstrar que $sgn(\sigma) = (-1)^r$, 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* $\varphi : G \to G'$ *tal que* $\varphi(gh) = \varphi(g)\varphi(h)$ *para todo g, h em G.* □

Exemplo 23. *São morfismos:*

1)$sgn : S_n \to \{+1, -1\}, \sigma \mapsto sgn(\sigma), \quad sgn(\sigma\tau) = \det(U(\sigma)U(\tau)) = \det(U(\sigma))\det(U(\tau)) = sgn(\sigma)sgn(\tau)$

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

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

3)$\varphi : G \to G', g \mapsto 1', \quad$ *em que* $1'$ *é o elemento neutro de G'.*

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

3.1) *Em particular,* $U : S_n \to GL_n, \sigma \mapsto U(\sigma)$

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

Proposição. *Seja* $\varphi : G \to G'$ *um morfismo. Então,*

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

2) *Se 1 é o elemento neutro de G e 1' o elemento neutro de G',* $\varphi(1) = 1'$.

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

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

$$\varphi(g_1 \cdots \varphi_n) = \varphi((g_1 \cdots g_{n-1})g_n) = \varphi(g_1 \cdots g_{n-1})\varphi(g_n) = \varphi(g_1) \cdots \varphi(g_{n-1})\varphi(g_n).$$

2.) $\varphi(1) = \varphi(1.1) \coloneqq \varphi(1)\varphi(1) \Rightarrow 1' = \varphi(1)\varphi(1)^{-1} = \varphi(1)$
3.) $1' = \varphi(1) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) \Rightarrow \varphi(g)^{-1} = \varphi(g^{-1})$. ■

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

Proposição. *A imagem de um morfismo* $\varphi : G \to G'$ *é um subgrupo de G' e o kernel de* φ *é um de G.*

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

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

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

Definição. *Seja* $sgn : S_n \to \{+1, -1\}$*. 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*

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

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

$$1)\varphi(a) = \varphi(b)$$
$$2)a^{-1}b \in K$$
$$3)b \in aH$$
$$4)aK = bK.$$

Prova.

$1) \Rightarrow 2) : \varphi(a) = \varphi(b) \Rightarrow \varphi(a^{-1}b) = 1' \Rightarrow a^{-1}b \in K;$
$2) \Rightarrow 1) : a^{-1}b \in K \Rightarrow \varphi(a^{-1}b) = 1' \Rightarrow \varphi(a) = \varphi(b);$
$1) \Rightarrow 3) : a^{-1}b \in K$ *se* $\exists h \in K$ *tais que* $a^{-1}h = bh \Rightarrow b \in aK;$
$3) \Rightarrow 1)$: *Suponha que* $b \in aH, b = ah \Rightarrow \varphi(b) = \varphi(a)\varphi(h) = \varphi(a);$
$(1) \iff (4)$: *Exercício.* ■

5 Aula 05 - 30/03/2023

5.1 Motivações

- Subgrupos Normais;
- Isomorfismos e Automorfismos;
- Partições e relações de equivalência.

Errata Última Aula

Seja $P_{ij} \in \mathbb{M}_n(\mathbb{R})$ tal que se $P_{ij} = (a_{kl})$, então $a_{kl} = 1$ se k = i, l = j e 0 caso contrário. Assim, se $\sigma \in S_n$,

$$U(\sigma) = (e_{\sigma(1)} \cdots e_{\sigma(n)}) = \sum P_{\sigma(i),i},$$

em que e_j é o vetor em $\mathbb{R}^n$ com 1 na j-ésima entrada e zero nos demais. De fato, $U(\sigma)$ é a matriz da tansformação linear $\mathbb{R}^n \to \mathbb{R}^n, e_j \mapsto e_{\sigma(j)}$.

5.2 Subgrupos Normais

Começamos com um corolário à última aula:

Corolário. *Uma φ é injetora se, e somente se,* $\ker(\varphi) = \{0\}$.

Prova. $\Rightarrow$) *Seja a um elemento do kernel de φ. Então,*

$$\varphi(a) = 1' = \varphi(1).$$

Mas, como φ é injetora, segue que a = 1 é o único elemento no kernel.

$\Leftarrow$) *Suponha que φ tem kernel trivial, i.e.,* $\ker(\varphi) = \{0\}$. *Então,*

$$\varphi(a)\varphi(b)^{-1} = 1' \Rightarrow 1 = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \Rightarrow ab^{-1} \in \ker\varphi = 1.$$

Portanto, $ab^{-1} = 1$ e, assim, $a = b$. ■

Definição. *Se G é um gurpo e a, g seus elementos, dizemos que $gag^{-1} \in G$ é um conjugado de a com respeito a g. Dois elementos a, b de G são conjugados se existe um g no grupo tal que $a = gbg^{-1}$.*□

Definição. *Sejam G um grupo e $H \leq G$. Dizemos que H é um subgrupo normal a G ($H \trianglelefteq G$) se para todos $h \in H$ e $g \in G$, $ghg^{-1} \in H$, i.e., H absorve os conjugados de seus elementos.* □

Em outras palavras, um subgroup é normal se ele é fechado pela conjugação, o que pode ser denotado por $gHg^{-1} \subseteq H$, para todo g de G.

Proposição. *Se $H \leq g$, são equivalente*

$$\begin{aligned} &i) \quad H \trianglelefteq G \\ &ii) \quad gHg^{-1} = H \\ &iii) \quad gH = Hg. \end{aligned}$$

Prova. *(1) $\Rightarrow$ (2): Obviamente, $gHg^{-1} \leq H$ por definição. Sejam h em H e g em G. Então, $ghg^{-1} \in gHg^{-1} \subseteq H$, tal que existe x em H que satisfaz $ghg^{-1} = x \Rightarrow h = \underbrace{(g^{-1})x(g^{-1})^{-1}}_{\in gHg^{-1}}$*

(2) $\Rightarrow$ (1): Ok.

(1) $\Rightarrow$ (3): Se x pertence a gH, $x = gh$ para algum h de H. Por hipótese, $gHg^{-1} \subseteq H$, de maneira que $ghg^{-1} = y \in H$, ou seja, $gh = yg$. Como $x = gh$, $x = yg \in Hg$. Portanto, $gH \subseteq Hg$. O outro lado da inclusão fica como exercício.

(3) $\Rightarrow$ (1): Se $x \in gHg^{-1}, x = ghg^{-1}, h \in H$, segue da hipótese que $gh = h'g$ para algum h' em H. Assim, $x = h' \in H$. ■

Exemplo 24. *1) Se G é um grupo, são subgrupos normais: G, {e}, Z(g).*

2) Se G é um grupo abeliano, todo subgrupo é normal, mas não vale a volta.

Exemplo 25. *Exercício: Seja* $Q = \{\pm 1, \pm i, \pm j, \pm k : -1^2 = 1, i^2 = j^2 = k^2 = -1\}$. *Mostre que Q é um grupo não abeliano, mas que todo subgrupo é normal.*

Exemplo 26. $< (12) >=< id, (12) > \not\trianglelefteq S_3$, *visto que*

$$(123)(12)(123)^{-1} = (32) \notin < (12) >$$

Portanto, $< (12) >$ *não é um subgrupo normal de* S_3.

Proposição. *Se* $\varphi : G \to G'$ *é um morfismo, então* $\ker \varphi \trianglelefteq G$.

Prova. *Sejam g um elemento de G e h um elemento de* $\ker \varphi$. *Então,*

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)1'\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1'.$$

Portanto, $ghg^{-1} \in \ker \varphi$ *e, portanto,* $\ker \varphi \trianglelefteq G$. ■

Exemplo 27. *1)* $SL_n \trianglelefteq GL_n, \quad SL_n = \ker det$.

2) $A_n = \ker sgn \trianglelefteq S_n, \quad sgn : S_n \to \{\pm 1\}, \sigma \mapsto \det U(\sigma)$.

Lembre-se que, dado $\sigma \in S_n, \sigma = \tau_1 \cdots \tau_r$ são 2-ciclos, então $sgn(\sigma) = (-1)^r$.

Definição. *Sejam G, G' grupos. Um isomorfismo* φ *é um morfismo* $\sigma : G \to G'$ *bijetor. Se G = G',* φ *é chamado automorfismo. Por fim, se existe um isomorfismo entre dois grupos, dizemos que eles são isomorfos, escrevendo* $G \cong G'$

(Nota ao leitor) Mas o que há de útil em isomorfismo? Por que nos importamos?

Em Álgebra linear, estudamos os isomorfismos entre espaços vetoriais, e como eles preservavam algumas propriedades. Essencialmente, o mesmo ocorrerá aqui, ou seja, se há um isomorfismo entre dois grupos, essencialmente estamos estudando o mesmo grupo, mas sob uma ótica diferente. Os elementos de um grupo podem ser escritos utilizando os do outro, eles terão os mesmos tamanhos, a propriedade abeliana será preservada, etc. Com isso, caso encontre um grupo aparentemente muito difícil de trabalhar, é possível simplificar o problema encontrando um outro grupo isomorfo e que facilitará seu serviço. Veremos exemplos a seguir.

Exemplo 28. *1) Todo subgrupo de ordem 2 é isomorfo a* S_2.

2) Há um isomorfismo entre o grupo aditivo dos reais e o multiplicativo positivo dado por $exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot), x \mapsto e^x$.'

3) Se g é um elemento de G de ordem infinita, então $\mathbb{Z} \to < g > \leq G, n \mapsto g^n$ *é um isomorfismo.*

4) Seja $P \leq GL_n$ *o conjunto das matrizes com somente um 1 em cada linha e cada coluna, tendo entrada 0 nos demais. Então,* $P \leq GL_n$ *e* $S_n \to P, \sigma \mapsto U(\sigma)$ *é isomorfismo.*

5) $id : G \to G'$ *é um isomorfismo.*

6) Se g pertence a G, $\varphi_g : G \to G, x \mapsto gxg^{-1}$ *é isomorfismo.*

Proposição. *Se* φ *é isomorfismo, então* $|g| = |\varphi(g)|$. *Em partícular,* $|g| = |aga^{-1}|$ *para todo a de G.*

Prova. *No caso em que* $|g| = \infty$, *se* $|\varphi(g)| = g < \infty$. *Assim,*

$$1' = \varphi(g)^m = \varphi(g^m) \Rightarrow g^m \in \ker \varphi = \{1\} \Rightarrow g^m = 1.$$

Agora, se $|g| = n < \infty$. *Seja* $m = |\varphi(g)|$, *então*

$$1' = \varphi(g)^m = \varphi(g^m) \Rightarrow g^m = 1 \Rightarrow n|m.$$

Por outro lado, como $g^n = 1$,

$$1' = \varphi(g^n) = \varphi(g)^n \Rightarrow m|n.$$

Portanto, $m = n$. ■

Lema. *Se $\varphi : G \to G'$ é um isomorfismo, então $\varphi^{-1} : G' \to G$ também é isomorfismo.*

Prova. *Segue que φ^{-1} está bem-definida e é uma bijeção pois φ é bijeção. Sejam x, y elementos de G'. Sendo φ uma bijeção, existem a, b em G tais que*

$$x = \varphi(a) \quad e \quad y = \varphi(b).$$

Desta forma, $\varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(x)\varphi^{-1}(y)$. ■

Definição. *Dado S um conjunto, uma partição para S é uma cobertura por subconjuntos não-vazios e disjuntos. Em outras palavras, existe $U_j \subseteq S, U_j \neq \emptyset$ e $U_j \cap U_i = \emptyset$ se $i \neq j$ tal que*

$$S = \bigsqcup_{j \in I} U_j.$$

Definição. *Uma relação de equivalência em um conjunto S é um subconjunto R de $S \times S$ tal que*

- $\overbrace{(a,a)}^{a \sim a} \in R, \forall a \in S$ *(Reflexiva);*
- $(a,b) \in R \Rightarrow (b,a) \in R (a \sim b \Rightarrow b \sim a)$ *(Simétrica);*
- $(a,b)(b,c) \in R \Rightarrow (a,c) \in R (a \sim b, b \sim c \Rightarrow a \sim c)$ *(Transitiva).*

Denotamos $(a,b) \in R$ por a b, e lê-se "a está relacionado com b". □

Definição. *Se R é uma relação de equivalência em S, denotamos por $[a], a \in S$ o conjunto dos elementos de S que se relacionam com a. Em outras palavras,*

$$[a] \coloneqq \{b \in S : a\ b\} = \{b \in S : (a,b) \in R\}$$

e chamamos $[a]$ de classe de equivalência de a. □

Exemplo 29. *1) A ordem em um grupo define uma relação de equivalência;*

2) A conjugação define uma relação de equivalência em um grupo G. ($a\ b \iff \exists g \in G : a = gbg^{-1}$) Neste caso, denotamos $[a] = Cl(a)$ como a classe de conjugação de a.

Teorema. *Uma partição em um conjunto S define uma relação de equivalência em S. Reciprocamente, uma relação de equivalência define uma partição em S.*

6 Aula 06 - 11/04/2023

6.1 Motivações

- Classes de equivalência;
- Índice de um grupo;
- Teorema de Lagrange.

6.2 Classe de Equivalência de Partições

Teorema. *Uma partição em um conjunto S define uma relação de equivalência em S. Reciprocamente, uma relação de equivalência define uma partição em S.*

Prova. *Seja $S = \bigsqcup_{i\in I} S$ uma partição, tal que*

$$R = \{(a,b) \in S \times S : \exists i \in I, a, b \in S_i\}$$

é uma definição de equivalência em S.

Reciprocamente, dada uma relação de equivalência em S, temos $[a]$ como a classe de equivalência de um elemento a de S. Por reflexividade, $a \in [a]$, ou seja, $[a]$ é não-vazio e

$$S = \bigcup_{a\in S} [a].$$

Afirmação: *Se $[a] \cap [b] \neq \emptyset$, então $[a] = [b]$. Com efeito, seja c um elemento na intersecção das classes $[a]$ e $[b]$. Segue que $a \sim c$ e $b \sim c$. Por simetria, $c \sim b$, logo, por transitividade, $a \sim c \sim b$, ou seja, $c \sim b$. Tome x em $[b]$, ou seja, $b \sim x$. Novamente, por transitividade, $a \sim x$, isto é, $x \in [a]$. Provamos, então, que $[a] \subseteq [b]$ e $[b] \subseteq [a]$, ou seja, $[a] = [b]$.* ■

Exemplo 30. *A ordem de um elemento define uma relação de equivalência em um grupo. Particularmente, no caso de S_3, as classes de equivalência são*

$$\begin{aligned} &(i) \quad [(12)] = \{(12), (13), (23)\} \\ &(ii) \quad [(123)] = \{(123), (132)\} \\ &(iii) \quad [id] = \{id\}. \end{aligned}$$

Assim, $S_3 = [(12)] \bigsqcup [(123)] \bigcup [id]$. ■

Definição. *Se $S = \bigsqcup S_{ii\in I}$ é uma partição, denotamos $\overline{S} \coloneqq \{[S_i]\}$ o conjunto das classes de equivalência dadas por S_i.*

Exemplo 31. *Se $\mathbb{Z} = \{$números pares$\} \bigsqcup \{$números ímpares$\}$, então $\overline{\mathbb{Z}} = \{[pares], [ímpares]\}\{\overline{0}, \overline{1}\}$.*

Observe que, se S tem uma relação de equivalência, é possível "projetarmos" um elemento de S em sua classe de equivalência através de

$$\pi : S \to \overline{S}, \quad a \mapsto [a] = \overline{a}.$$

Exemplo 32. *Fixe um inteiro n. Dados a, b também inteiros, dizemos que $a \sim b$ módulo n (ou $a \equiv b \mod n$) se $n|a-b$. Mostre que a congruência mod n é de fato uma relação de equivalência em $\mathbb{Z}$. Além disso, $\overline{\mathbb{Z}}^n = \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \cdots, \overline{n-1}\}$.*

Definição. *Se $\varphi : S \to T$ é um mapa entre conjuntos, então φ define uma relação de equivalência em S dada por*

$$a \sim b \quad \iff \varphi(a) = \varphi(b).$$

Além disso, [a] é definida como a fibra por φ de $\varphi(a) = t$, ou seja,

$$\varphi^{-1}(t) = \{s \in S : \varphi(s) = t\}.$$

Em outras palavras, se $\varphi(a) = t$, então $\overline{a} = [a] = \varphi^{-1}(t)$. Em partícular,

$$S = \bigsqcup_{t\in Im\varphi} \varphi^{-1}(t).$$

6.3 Classes Laterias e Índices.

Proposição. *Sejam $\varphi : G \to G'$ morfismos de grupos e $K = \ker \varphi$. Então, a fibr de φ que contém o elemento a a de G é a classe lateral aK. Além disso, essas classes particionam G e correspondem aos elementos da imagem de φ.*

Prova. *Segue que, dado b em aK, $\varphi(a) = \varphi(b) = t$. Disto segue que a, b pertencem à pré-imagem de $\varphi, \varphi^{-1}(t)$.*

Proposição. *As classes laterais à esquerda de H em G são as classes de equivalência da seguinte relação*

$$a \cong b \iff b = ah, \quad h \in H.$$

Denotamos $a \cong b$ por $a \equiv b$.

Prova. *Observe que $a = 1a$, $1 \in H$. Logo, $a \cong a$. Se $a \cong b$, existe h em H tal que $b = ah$, ou seja, $a = bh^{-1}, h^{-1} \in H$ de modo que $b \cong a$.*

Se $a \cong b, b \cong c$, existem $h_1, h_2 \in H$ tais que $b = ah_1, c = bh_2$, de forma que $c = ah_1h_2$, i.e., $a \cong c$.

Por fim,

$$\begin{aligned}[a] &= \{b \in G : a \cong b\} \\ &= \{b \in G : \exists h \in H \text{ tal que } b = ah\} \\ &= \{ah : h \in H\} = aH. \blacksquare\end{aligned}$$

Corolário. $G = \bigsqcup_{a \in G \, distintos} aH$.

Exemplo 33. *Em $S_3 =< (12), (123) >$, seja $H =< (12) >$. Temos*

$$\begin{aligned}&(i) idH = H = \{id, (12)\} = (12)H \\ &(ii)(123)H = \{(123), (123)(12)\} = (123)(12)H \\ &(iii)(123)^2H = \{(123)^2, (123)^2(12)\} = (123)^2(12)H.\end{aligned}$$

De fato, $S_3 = H \bigsqcup (123)H \bigsqcup (123)^2H$ $\blacksquare$

Definição. *O número de classes laterais (à esquerda) de H em G é chamado o índice de H em G, denotado por $[G : H]$.*$\square$

Exemplo 34. *No exemplo anterior, $[S_3 : H] = 3, |H| = 2$.*

Lema. *Todas as classes laterais aH de H em G têm mesma ordem.*

Prova. *O mapa $m_a : H \to H_a, h \mapsto ah$ é um mapa bijetor com inversa $m_{a^{-1}}$.* $\blacksquare$

Este lema será usado para demonstrar um resultado extremamente importante em Teoria de Grupos. Essencialmente falando, ele afirma que a ordem de um grupo é um múltiplo da ordem dos seus subgrupos. Mas por que isso importa? Além de ser um resultado intrigante por si só, ele pode ser usado para mostrar que grupos não são isomórficos, quantidade de elementos de uma dada ordem dentro de um grupo, entre outras coisas. Segue seu enunciado.

Teorema. *Se G é um grupo finito e H um subgrupo de G, então*

$$|G| = |H|[G : H].$$

Em particular, $|H|$ divide $|G|$.

Prova. *Da proposição anterior, sabemos que $G = \bigsqcup_{a \in G \, diferentes} aH$. Portanto,*

$$|G| = \sum_{a \in G \, diferentes} |aH| = |H|[G : H] \ \blacksquare$$

Corolário. *Se a pertence a G, então $|a| \Big| |G|$*

Prova. *Segue do Teorema de Lagrange que*

$$|a| = |< a >| \Big| |G| \ \blacksquare$$

Corolário. *Se $|G| = p$ número primo e a é um elemento de G diferente do elemento neutro, então*

$$G =< a > .$$

Prova. *Se —a— divide p, então $|a| = 1$ ou p, mas, como $a \neq 1, |a| = p$, segue que*

$$G =< a > \ \blacksquare$$

Corolário. *Se $\varphi : G \to G'$ é um morfismo de grupos finitos, segue que*

1) $|G| = |\ker \varphi||im\varphi|$
2) $|\ker \varphi| \Big| |G|$
3) $|im\varphi|$ *divide* $|G|$ *e* $|G'|$.

Prova. $1 \Rightarrow)$ *Temos*

$$G = \bigsqcup a \ker \varphi$$

$$\Rightarrow |G| = |im\varphi||\ker \varphi|$$
$$\Rightarrow |G| = |\ker \varphi|[G : \ker \varphi] = |\ker \varphi||im\varphi|.$$

Os outros itens ficam como exercício para os estudantes. $\blacksquare$

Exemplo 35. *Considere $sgn : S_n \to \{\pm 1\}$. Temos*

$$|im(sgn)| = 2,$$

de modo que

$$|A_n| = |\ker sgn| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

Proposição. *Se $K \leq H \leq G$, então*

$$[G : K] = [G : H][H : K]$$

Prova. *Suponha que $[G : H] = n$ e $[H : K] = m$. Então,*

$$G = g_1 H \bigsqcup \cdots \bigsqcup g_n H = \bigsqcup_{i=1}^{n} g_i H \quad e \quad H = \bigsqcup_{j=1}^{m} h_j K.$$

A multliplicação por g_i é uma bijeção

$$m_{g_i} : h_j K \to g_i h_j K, \quad x \mapsto g_i x.$$

Assim, $g_i H = \bigsqcup_{j=1}^{m} g_i h_j K$. Portanto,

$$G = \bigsqcup_{i=1}^{n} \left[\bigsqcup_{j=1}^{m} g_i g_j K \right],$$

de onde concluí-se que $[G : K] = mn$. $\blacksquare$

7 Aula 07 - 13/04/2023

7.1 Motivações

- Relacionando morfismos com as estruturas de subgrupos;
- Teorema da Correspondência.

7.2 Mais Sobre Morfismos

Proposição. *Se $\varphi : G \to G'$ é um morfismo de grupos finitos e $H \leq G$ é tal que $\gcd(|H|, |G'|) = 1$, então $\ker\varphi \supseteq H$.*

Prova. *Tome $\varphi_H : H \to G'$. Pela propriedade da aula passada,*

$$|im\varphi_H| \Big| |H| \text{ e } |G'|.$$

Por hipótese, $|im(\varphi_H)| = 1$, i.e., $im\varphi_H = \{1'\}$. Assim, $\varphi(H) \subseteq \{1'\}$. Portanto, $H \subseteq \ker\varphi$. ■

Exemplo 36. *Se $H \leq S_n, |H| = 2k+1$, então $H \subseteq A_n$. Considere $sgn : S_n \to \{\pm 1\}$. Pela proposição, $H \subseteq \ker sgn = A_n$.*

Proposição. *Seja $\varphi : G \to G'$ um morfismo de grupos, $K = \ker\varphi, H' \leq G'$ e $H = \varphi^{-1}(H')$. Então, $H \leq G$ e $K \leq H$. Além disso, se $H' \trianglelefteq G'$, então $H \trianglelefteq G$. Por fim, se φ for sobrejetora e $H \trianglelefteq G$, temos $\varphi(H) = H' \trianglelefteq G'$.*

Prova. *Vamos começar mostrando que H é um subgrupo de G. Com efeito, como H' é subgrupo de G', então 1' é um de seus elementos. Assim, $\varphi^{-1}(1') \subseteq H$ e, em particular, 1 pertence a H e $K \leq H$. Agora, sejam x, y elementos de H. Então, $\varphi(x), \varphi(y) \in H'$, ou seja, $\varphi(x)\varphi(y)^{-1} \in H'$. Assim, $\varphi(xy^{-1}) \in H'$ e $xy^{-1} \in H$. Portanto, H é subgrupo de G.*

Daremos continuidade provando a segunda parte do resultado. Suponha que $H' \trianglelefteq G'$ e sejam $x \in gHg^{-1}, x = ghg^{-1}$ para algum h em H.

$$\varphi(x) = \varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \in H' \Rightarrow ghg^{-1} \in H.$$

Portanto, $H \trianglelefteq G$.

Finalmente, mostremos que $\varphi(H) \trianglelefteq G'$. Tome g' em G e $y \in \gamma(H)$. Como φ é sobrejetora, existe x em H e g em G tal que $\varphi(g) = g', \varphi(x) = y$. Portanto,

$$g'y(g')^{-1} = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(gxg^{-1}) \in \varphi(H).$$ ■

Exemplo 37. *Segue que $GL_n(\mathbb{R})^+ \trianglelefteq GL_n(\mathbb{R})$. De fato, note que, se definirmos*

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times,$$

então $GL_n(\mathbb{R})^+ = \det^{-1}(\mathbb{R}_{>0}) \trianglelefteq GL_n(\mathbb{R})$. ■

7.3 Teorema da Correspondência

O resultado a seguir é conhecido como Teorema da Correspondência.

Teorema. *Seja $\varphi : G \to G'$ sobrejetora e $K = \ker\varphi$. Então,*

$$\begin{aligned} \{H \leq G : K \subseteq H\} &\longleftrightarrow \{N : N \leq G'\} \\ H &\mapsto \varphi(H) \\ \varphi^{-1}(N) &\hookleftarrow N. \end{aligned}$$

Além diso, se $H \leftrightarrow N$', então $H \trianglelefteq G \iff N \trianglelefteq G'$ e $|H| = |N| \cdot |K|$.

Prova. *Vamos mostrar as seguintes coisas -* $H = \varphi^{-1}\varphi(H)N = \varphi\varphi^{-1}(N), |H| = |N||K|$.

Nesta ordem, começamos observando que $H \leq \varphi^{-1}\varphi(H)$ *é sempre verdadeira. Seja* x *em* $\varphi^{-1}\varphi(H)$. *Então,* $\varphi(x) \in \varphi(H)$, *isto é, existe* h *em* H *tal que* $\varphi(x) = \varphi(h)$. *Disto, temos*

$$\varphi(xh^{-1}) = 1' \iff xh^{-1} \in K \subseteq H \Rightarrow x \in H,$$

concluindo o que desejávamos mostrar.

Para a segunda parte, fica como exercício.

Por fim, considere $\varphi_{|_H} : H \to \gamma(H) = N$. *Pela aula anterior, portanto,*

$$|H| = |\ker \varphi_{|_H}||Im(\varphi_{|_H})| = |K||N|. \blacksquare$$

Definição. *Dados G e G' grupos, defina o quociente de G por G' como*

$$G \times G' = \{(g, g') : g \in G, g' \in G'\} \quad \square$$

Afirmamos que $G \times G'$ com a operação $(g_1, g_1')(g_2, g_2') = (g_1g_1', g_2g_2')$ é um grupo. Além disso, temos os seguintes morfismos:

$$\pi : G \times G' \to G, \quad \pi' : G \times G' \to G'$$
$$i : G \to G \times G', \quad i' : G' \to G \times G',$$

Sendo eles chamados, respectivamente, de projeções e injeções. Ademais, $(1, 1')$ é o elemento neutro de $G \times G'$.

Proposição. *Se* $\gcd(r, s) = 1$, *então o grupo cíclico de ordem rs é o produto* $C_r \times C_s$, *sendo* C_r *o grupo cíclico de ordem r (E* C_s *o cíclico de ordem s).*

Prova. *Seja* C_{rs} *o grupo cíclico de ordem rs. Se* $C_r =< x >, C_s =< y >$. *Então,* $C_r \times C_s =< (x, y) >$. *De fato,*

$$(x, y)^{rs} = (x^{rs}, y^{rs}) = ((x^r)^s, (y^s)^r) = (1, 1'),$$

tal que $k = ord(xy) \Big| rs$. *Como* $(r, s) = 1$, *existem* $a, b \in \mathbb{Z}$ *tais que*

$$1 = ar + bs$$
$$k = ark + bsk.$$

Observe que $(x, y)^k = (x^k, y^k) = (1, 1')$, *o que implica que* $r \Big| k$ *e* $s \Big| k$, *ou seja,* $k = rr'$ *e* $k = ss'$. *Substituindo isso na segunda fórmula, temos* $k = rsar' + rsbs' = rs(outros\ termos)$. *Portanto,* $rs \Big| k$. $\blacksquare$

Exemplo 38. *Segue que* $C_2 \times C_2 \neq C_4$ *(Verifique!).*

Proposição. *Sejam* $H, K \subseteq G$ *e* $f : H \times K \to G, (h, k) \mapsto hk$ *com* $imF = HK := \{hk : h \in H, k \in K\}$. *Então,*

a) f *é injetora se, e somente se,* $H \cap K = \{1\}$;

b) f *é morfismo se, e somente se,* $hk = kh$ *para todo* $h \in H, k \in K$;

c) Se $H \trianglelefteq G$, *então* $HK \leq G$;

d) f *é isomorfismo se, e somente se,* $H \cap K = \{1\}, HK = G$ *e* $H, K \trianglelefteq G$.

Prova. *a)* $(\Rightarrow)$ *Se* $H \cap K \neq \{1\}$, *então existe* x *em* $H \cap K, x \neq 1$, *ou seja,*

$$f(xx^{-1}) = xx^{-1} = 1f(1.1),$$

o que implica que f não é injetora, uma contradição.

($\Leftarrow$) *Se* $f(h_1,k_1)=h_1k_1=h_2k_2=f(h_2k_2)\iff h_2^{-1}h_1=k_2k_1^{-1}\in H\cap K$. *Logo,* $h_2^{-1}h_1=1$ *e* $k_2k_1^{-1}=1$, *ou seja,* f *é injetora.*

b) ($\Leftarrow$) *Segue que* $f((h_1,k_1)(h_2,k_2))=f(h_1h_2,k_1k_2)=h_1h_2k_1k_2=h_1k_1h_2k_2=f(h_1,k_1)f(h_2,k_2)$.

($\Rightarrow$) *Se* f *é um morfismo, então* $h_1h_2k_1k_2=h_1k_1h_2k_2$ *para todos* $h_1,h_2\in H,k_1,k_2\in K$. *Em partícular, para* $h_1=k_2=1$, *temos* $h_2k_1=k_1h_2$ *para todos* $h_1\in H,k_2\in K$.

c) Sejam $h_1,h_2\in H$ *e* $k_1,k_2\in K$. *Então,*

$$(h_1k_1)(h_2k_2)^{-1}=h_1k_1k_2^{-1}h_2^{-1}=h_1h_2'h_1k_1^{-1}\in HK$$

d) ($\Leftarrow$) *Por* $H\cap K=\{1\}$ *e* $HK=G$, f *é bijetora. Assim, basta mostrar que* f *é morfismo. Sejam* $h_2,h_1\in H$ *e* $k_1,k_2\in K$. *Segue que*

$$f((h_1,k_1)(h_2,k_2))=f((h_1h_2,k_1k_2))=h_1h_2k_1k_2k=h_1k_1h_2k_2=f(h_1,k_1)f(h_2,k_2).$$

Sejam, também, $h\in H,k\in K$

$$hkh^{-1}k^{-1}=hk(kh)^{-1}.$$

Como $H\trianglelefteq G$, *segue que*

$$hh'kk^{-1}=hh'\in H$$

Como $K\trianglelefteq G$, *temos também*

$$hkh^{-1}k^{-1}=hh^{-1}k'k^{-1}\in K.$$

Portanto, $hkh^{-1}k^{-1}\in H\cap K=\{1\}$ ■

Proposição. *Os grupos de ordem 4 são* C_4 *ou* $C_2\times C_2$.

Prova. *Seja* G *um grupo de ordem 4 dado por* $G=\{1,g_1,g_2,g_3\}$. *Pelo teorema de Lagrange,* $ord(g_i)\Big|4$, *ou seja,* $ordg_i=2$ *ou 4. Se existe* $g_i\in G$ *tal que* $ord(g_i)=4$, *então* $G\cong C_4$.

Caso contrário, todo g_i *é tal que* $|g_i|=2$. *Assim, defina*

$$f:<g_1>\times<g_2>\to G,\quad (x,y)\mapsto xy.$$

Pelo item d da proposição anterior, f *é isomorfismo.* ■

8 Aula 08 - 18/04/2023

8.1 O Que Esperar

- Grupos quocientes;
- Primeiro Teorema do Isomorfismo;
- Teorema de Classificação de Grupos Abelianos Finitamente Gerados.

8.2 Motivação para a Aula

(Seção teste. Se gostarem, me avisem pra fazer nas outras).

Os grupos quociente, o primeiro teorema do isomorfismo para grupos e o teorema de classificação dos grupos abelianos finitamente gerados são conceitos fundamentais na teoria dos grupos, um ramo importante da matemática que estuda a estrutura e propriedades dos grupos. Esses conceitos e teoremas nos ajudam a entender melhor as relações entre diferentes grupos e suas subestruturas.

A motivação por trás desses conceitos e teoremas é simplificar e classificar grupos em categorias mais fáceis de entender e manipular. Ao estudar grupos quociente, podemos analisar propriedades de grupos maiores e mais complexos por meio de seus subgrupos normais. O primeiro teorema do isomorfismo nos permite estabelecer conexões entre diferentes grupos e suas subestruturas, enquanto o teorema de classificação dos grupos abelianos finitamente gerados nos fornece uma maneira sistemática de descrever e classificar esse tipo específico de grupo.

Uma analogia que pode ser usada imagine que você tem um grupo de amigos e quer dividi-los em equipes para um jogo. Os grupos quociente são como as equipes formadas, o primeiro teorema do isomorfismo mostra como as habilidades dos jogadores se relacionam entre as equipes, e o teorema de classificação dos grupos abelianos finitamente gerados ajuda a entender os diferentes tipos de amigos que você tem. Isso torna mais fácil entender como seus amigos se organizam e trabalham juntos.

Resumindo, os grupos quociente são uma maneira de "reduzir"um grupo dividindo-o por um subgrupo normal. O primeiro teorema do isomorfismo relaciona a estrutura de um grupo e seus subgrupos normais aos grupos quocientes, mostrando que certas propriedades são preservadas no processo. O teorema de classificação dos grupos abelianos finitamente gerados fornece uma descrição única para cada grupo abeliano finitamente gerado, permitindo-nos classificá-los de maneira eficiente.

8.3 Grupos Quociente

Definição. *Se $N \leq G$, então $G/N \coloneqq \{aN : a \in G\} = \{\overline{a} : a \in G\}$ é o Grupo Quociente de G por N.* □

Definição. *Se A, B são subconjuntos de um grupo G, então $AB \coloneqq \{x \in G : x = ab, a \in A, b \in B\}$.*□

Lema. *Se N é um subgrupo normal de G, então $aNbN = abN$ para todos a, b elementos de G.*

Prova. *Como $N \leq G, N \cdot N = N$. Além disso, já que $N \trianglelefteq G, bN = Nb$. Portanto,*

$$aNbN = a(Nb)N = abNN = abN.\blacksquare$$

Lema. *Seja G grupo e $\mathcal{L}$ um conjunto com uma operação. Se $\varphi : G \to \mathcal{L}$ é uma função sobrejetora tal que $\varphi(ab) = \varphi(a)\varphi(b)$ para todo a, b em G. Então, $\mathcal{L}$ é um grupo e φ é um morfismo.*

Prova. *Dados x, y em $\mathcal{L}$, existem a, b em G tais que $\varphi(a) = x, \varphi(b) = y$ e $xy = \varphi(a)\varphi(b) = \varphi(ab)$. Seja $1_{\mathcal{L}} = \varphi(1)$, então $1_{\mathcal{L}} \cdot x = \varphi(1) \cdot \varphi(a) = \varphi(1 \cdot a) = \varphi(a) = x$. Vamos provar a associatividade a seguir.*

Se $z \in \mathcal{L}, z = \varphi(c)$, então

$$x(yz) = \varphi(a)(\varphi(b)\varphi(c)) = \varphi(abc) = \varphi(ab)\varphi(c) = (\varphi(a)\varphi(b))\varphi(c) = (xy)z.$$

A demonstração da existência de inverso fica como exercício. ■

Teorema. *Se $N \trianglelefteq G$, então G/N é um grupo e $\pi : G \to G/N$ (O morfismo projeção canônica) é um morfismo sobrejetor com* $\ker \pi = N$.

Prova. *Segue que*

$$G/N \times G/N \to G/N, \quad (\overline{a}, \overline{b}) \mapsto \overline{ab}$$

está bem-definido. Ademais,

$$\pi : G \to G/N$$

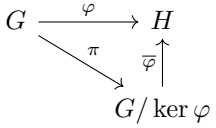
satisfaz $\pi(a)\pi(b) = \overline{a} \cdot \overline{b} = \overline{ab} = \pi(ab)$. Pelo segundo lema, G/N é um grupo e π um morfimso sobrejetor. Além disso, se $\pi(a) = \overline{a} = \overline{1} - N$ se, e somente se, a pertence a N. Portanto, $\ker \pi = N$. ■

8.4 Primeiro Teorema do Isomorfismo

Teorema. *Se $\varphi : G \to H$ é um morfismo sobrejetor de grupos, então $G/\ker \varphi \cong H$. Mais precisamente, se $\pi : G \to G/\ker \varphi$ é o mapa canônico, então*

$$\overline{\varphi} : G/\ker \varphi \to H, \quad \overline{a} \mapsto \varphi(a)$$

e está bem-definido um isomorfismo tal que



comuta.

Prova. *Começamos mostrando que $\overline{\varphi}$ está bem-definida. Se $\overline{a} = \overline{b}, ab^{-1} \in \ker \varphi$, tal que existe g em $\ker \varphi$ para o qual $ab^{-1} = g$. Assim, $\varphi(ab^{-1}) = \varphi(g) = 1$, logo $\varphi(a) = \varphi(b)$.*

A seguir, mostremos que $\overline{\varphi}$ é morfismo. De fato, $\overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b}) = \varphi(a) \cdot \varphi(b) = \varphi(ab) = \overline{\varphi}(\overline{ab})$.

Observe que $\overline{\varphi}$ é sobrejetora porque φ o é. Finalmente, a injetividade de $\overline{\varphi}$ segue de

$$\varphi(\overline{a}) = 1 \iff \varphi(a) = 1 \iff a \in \ker \varphi \iff \overline{a} = \ker \varphi = 1.$$

Portanto, $\overline{\varphi}$ é isomorfismo. ■

Corolário. *Se $\varphi : G \to H$ é um morfismo, então $G/\ker \varphi \cong im\varphi$.*

O resultado a seguir mostra que todo grupo abeliano pode ser escrito apenas com números inteiros que satisfazem certa propriedade.

Teorema. *Seja G um grupo abeliano finitamente gerado. Então,*

$$G \cong \mathbb{Z} \times \cdots \times \mathbb{Z} \times \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{d_r\mathbb{Z}}.$$

com $d_i > 1$ e $d_i \big| d_{i+1}, i = 1, \cdots, r-1$.

9 Aula 09 - 25/04/2023

9.1 O que esperar

- Transformações que preservam distâncias - Isometrias;
- Caracterizações de Isometrias.

9.2 Motivação para Aula

Ações de grupos são um conceito importante na álgebra, que estuda a interação entre grupos e estruturas algébricas. Elas descrevem como os elementos de um grupo atuam em outro conjunto, preservando a estrutura desse conjunto.

Formalmente, uma ação de grupo é uma função que mapeia cada par formado por um elemento do grupo e um elemento do conjunto em outro elemento do conjunto, obedecendo às seguintes propriedades:

i) Identidade: A ação do elemento neutro do grupo (normalmente denotado por "e") em qualquer elemento do conjunto é o próprio elemento, ou seja, $e \cdot x = x$.

ii) Compatibilidade: A ação de um produto de elementos do grupo é a mesma que a ação dos elementos individuais na sequência, ou seja, $(gh)x = g(h \cdot x)$, para todos g, h pertencentes ao grupo e x pertencente ao conjunto.

Num contexto mais aplicado, as ações de grupos surgem em áreas como física, química, computação, etc. Na forma de

1) Simetrias: Em geometria, ações de grupos são usadas para analisar simetrias de formas geométricas, como rotações e reflexões.

2) Teoria dos Grafos: Ações de grupos ajudam a estudar a simetria e as propriedades de grafos em teoria dos grafos.

3) Química: Ações de grupos são aplicadas na análise das simetrias moleculares, especialmente na teoria dos grupos de pontos, que é fundamental para a compreensão da espectroscopia e da estrutura molecular.

4) Criptografia: Em ciência da computação, as ações de grupos são utilizadas em algoritmos criptográficos e na teoria da codificação.

Uma analogia que podemos utilizar para compreender a ideia é a de crianças com um brinquedo: Imagina que você tem um grupo de amiguinhos e alguns brinquedos. Os amiguinhos são como os elementos do grupo, e os brinquedos são como os elementos do conjunto. Quando seus amiguinhos brincam com os brinquedos, eles podem trocar os brinquedos de lugar, girá-los ou virá-los de cabeça para baixo. Essa brincadeira segue algumas regrinhas, e é isso que chamamos de "ações de grupos". Essa ideia nos ajuda a entender padrões e simetrias em coisas do nosso mundo, como formas geométricas e até moléculas!

De maneira geral, as ações de grupos são uma maneira de descrever como um grupo de elementos interage com outro conjunto de elementos. Essa interação segue algumas regras e ajuda a entender padrões, simetrias e propriedades em várias áreas do conhecimento, como geometria, química e ciência da computação.

Começaremos introduzindo este assunto por meio das simetrias, partindo do ponto das isometrias.

9.3 Isometrias

Aqui, considere $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ o produto interno usual.

Definição. *Uma isometria $f : \mathbb{R}^n \to \mathbb{R}^n$ é uma função que preserva distância, isto é, dados u, v em $\mathbb{R}^n$,*

$$|f(u) - f(v)| = |u - v|.$$

Exemplo 39. *O operador linear ortogonal $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ é uma isometria.*

Exemplo 40. *Se $a \in \mathbb{R}^n, t_a : \mathbb{R}^n \to \mathbb{R}^n, v \mapsto v + a$ é uma isometria chamada de translação.*

Exemplo 41. *A função* $\varphi : \mathbb{R}^2 \to \mathbb{R}^2, \varphi(x,y) = (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)$ *é uma isometria.*

Exemplo 42. *A composta de isometrias é uma isometria.*

Lema. *Sejam* $x, y \in \mathbb{R}^n$ *tais que* $\langle x,x\rangle = \langle x,y\rangle = \langle y,y\rangle$. *Então,* $x = y$.

Prova. *Segue que*

$$\langle x-y, x-y\rangle = \langle x,x\rangle - 2\langle x,y\rangle + \langle y,y\rangle = 0.$$

Portanto, $x - y = 0$, *ou seja,* $x = y$. ■

Teorema. *Seja* $\varphi : \mathbb{R}^n \to \mathbb{R}^n$. *São equivalentes:*

i) φ *é isometria e* $\varphi(0) = 0$;

ii) $\langle \varphi(u), \varphi(v)\rangle = \langle u, v\rangle \; \forall u, v \in \mathbb{R}^n$;

iii) φ *é um operador linear ortogonal.*

Prova. *c)* $\Rightarrow$ *a) Ok;*
a) $\Rightarrow$ *b) Pela definição de isometria, temos*

$$|\varphi(u) - \varphi(v)| = |u - v| \iff \langle \varphi(u) - \varphi(v), \varphi(u) - \varphi(v)\rangle = \langle u - v, u - v\rangle .$$

Fazendo $u = 0$, *temos*

$$\langle \varphi(v), \varphi(v)\rangle = \langle v, v\rangle .$$

Analogamente, para v *=0, temos*

$$\langle \varphi(u), \varphi(u)\rangle = \langle u, u\rangle .$$

Como o produto interno é bilinear,

$$\begin{aligned} &\langle \varphi(u), \varphi(u)\rangle - 2\langle \varphi(u), \varphi(v)\rangle + \langle \varphi(v), \varphi(v)\rangle \\ &= \langle u, u\rangle - 2\langle u, v\rangle + \langle v, v\rangle . \end{aligned}$$

Logo,

$$\langle \varphi(u), \varphi(v)\rangle = \langle u, v\rangle .$$

b) $\Rightarrow$ *c) Basta mostrar que* $\varphi(u+v) = \varphi(u) + \varphi(v)$ *e* $\varphi(\alpha u) = \alpha\varphi(u)$. *para todos* u, v *em* $\mathbb{R}^n, \alpha \in \mathbb{R}$.
Sejam $x = \varphi(u+v), y = \varphi(u) + \varphi(v)$. *Observe que*

- $\langle x,x\rangle = \langle \varphi(u+v), \varphi(u+v)\rangle = \langle u+v, u+v\rangle$
- $\langle y,y\rangle = \langle \varphi(a) + \varphi(v), \varphi(a) + \varphi(v)\rangle =$
  $= \langle \varphi(u), \varphi(u)\rangle + 2\langle \varphi(u), \varphi(v)\rangle + \langle \varphi(v), \varphi(v)\rangle$
  $= \langle u, v\rangle + 2\langle u, v\rangle + \langle v, v\rangle = \langle u+v, u+v\rangle .$
- $\langle x,y\rangle = \langle \varphi(u+v), \varphi(u) + \varphi(v)\rangle = \langle u+v, u\rangle + \langle u+v, v\rangle = \langle u+v, u+v.\rangle$

Assim, pelo lema anterior, x=y. Analogamente, se $x = \varphi(\alpha u)$ *e* $y = \alpha\varphi(u)$, *temos x=y (exercício).* ■

Corolário. *Todo isomorfismo* f *de* $\mathbb{R}^n$ *é uma composição de um operador ortogonal com uma translação. Mais precisamente,* $f = t_a\varphi$, *sendo* φ *ortogonal a* $a = f(0)$. *Além disso, essa decomposição é única.*

Prova. *Observe que* $t_a^{-1}f(0) = (t_a^{-1})(a) = 0$. *Logo,* $t_a^{-1}f$ *é uma isometria que leva 0 em 0. Pelo teorema,* $\varphi = t_a^{-1}f$ *é um operador linear ortogonal. Deste modo,* $f = t_a\varphi$. ■

Proposição. *1) Se* φ *é um operador linear ortogonal, então* φ^{-1} *é um operador linear ortogonal.*

2) Se φ, ψ *são operadores ortogonais, netão* $\varphi \circ \psi$ *é operador ortogonal.*

3) $t_a \circ t_b = t_{a+b}$;

4) $\varphi \circ t_a = t_{a'} \circ \varphi$, *em que* $a' = \varphi(a)$ *e* φ *é operador linear.*

Prova. *Exercício.*

Corolário. *Corolário 1: Seja* $\mathcal{O}_n \coloneqq \{\varphi : \mathbb{R}^n \to \mathbb{R}^n : \varphi \text{ é operador linear}\}$. *Então,* $(\mathcal{O}_n, \circ)$ *é um grupo.*

Corolário. *Corolário 2: Seja* $T = \{ta : a \in \mathbb{R}^n\}$. *Então* $(T, \circ)$ *é um grupo.*

Corolário. *Corolário 3: Se* M_n *é o conjunto de todas as isometrias de* $\mathbb{R}^n$, *netão* $(M_n, \circ)$ *é um grupo.*

Prova. *Já sabemos que a composta de isometrias é uma isometria e que a operação de composição de funções é associativa. Observe que* $Id_{\mathbb{R}^n} = Id \in M_n$, *logo dado* $f \in M_n$,

$$f \circ Id = Id \circ f = f.$$

Agora, se $f \in M_n$, *do teorema anterior,* $f = t_a\varphi$, *sendo* a *um vetor de* $\mathbb{R}^n$ *e* φ *um operador linear ortogonal. Netão,*

$$f^{-1} \coloneqq \varphi^{-1} \circ t_{-a} = t_{a'} \circ \varphi^{-1}, \quad a' = \varphi^{-1}(-a).$$

Logo, $f^{-1} \in M_n$. *Ainda mais,*

$$f \circ f^{-1} = t_a\varphi\varphi^{-1}t_{-a} = t_at_{-a} = t_{aA} = t_0 = Id.$$

e, portanto, $f^{-1} \circ f = Id$. ■

Proposição. *Seja* $a \in \mathbb{R}^n$ *e* $\pi : M_n \to \mathcal{O}_n, f = t_ap \mapsto \varphi$, *então* π *é um morfismo sobrejetor cujo núcleo é* T. *Em particular,* $T \trianglelefteq M_n$.

Prova. *Sejam* $f, g \in M_n$. *Então, existem* $a, b \in \mathbb{R}^n$ *e* $\varphi, \psi \in \mathcal{O}_n$ *tais que* $f = t_a\varphi$ *e* $g = t_b\psi$. *Desta forma,*

$$\begin{aligned}\pi(fg) &= \pi(t_a\varphi t_b\psi) = \pi(t_at_{b'}\varphi \circ \psi)\\ &= \pi(t_{a+b'}(\varphi \circ \psi))\\ &= \varphi\psi = \pi(f)\pi(g). \blacksquare\end{aligned}$$

Em particular, pelo Teorema do Isomorfismo, uma consequência desta proposição é que

$$\frac{M_n}{T} \cong \mathcal{O}_n.$$

10 Aula 10 - 27/04/2023

10.1 O que esperar?

- Tipos de Isometrias Principais.

10.2 Principais Isometrias em $\mathbb{R}^n$

Lema. *Sejam $\eta, f \in M_n, x, y \in \mathbb{R}^n$ tais que f(x) = y. Suponha que $\eta(x) = x', \eta(y) = y'$. Considere $f' \in M_n$ tal que $f'(x') = y'$ para todos x, y em $\mathbb{R}^n$. Então, $f' = \eta f \eta^{-1}$. Em outras palavras, o diagrama abaixo comuta:*

$$\begin{array}{ccc} \mathbb{R}^n & \xrightarrow{f} & \mathbb{R}^n \\ \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \eta = t_v} \\ \mathbb{R}^n & \xrightarrow{f'} & \mathbb{R}^n \end{array}$$

Prova. *Se f(x) = y, então $f\eta^{-1}(u') = \eta^{-1}(y')$, ou seja, $\eta f \eta^{-1}(x') = y'$.* ■

Corolário. *O morfismo $\pi : M_n \to O_n$ não muda por translação de origem*

Prova. *Sejam t_a uma translação em $\mathbb{R}^n, a \in \mathbb{R}^n, f \in M_n$. Então, do lema anterior, f, após a mudança de coordenadas por t_a, é dado por*

$$f' = t_a f (ta)^{-1} = t_a f t_{-a}.$$

Então, $\pi(f') = \pi(t_a f t_{-a}) = \pi(t_a)\pi(f)\varphi(t_{-a}) = \pi(f)$. ■

Lembre-se que se $\varphi \in \mathcal{O}_n$ e M_φ é sua matriz, então M_φ é uma matriz ortogonal e, assim, $M_\varphi^{-1} = M_\varphi^t$. Logo,

$$1 = \det(M_\varphi M_\varphi^{-1}) = \det M_\varphi^2 \Rightarrow \det M_\varphi = Id.$$

Definição. *Um operador ortogonal $\varphi \in \mathcal{O}_n$ preserva orientação se o determinante de sua matriz vale 1. Analogamente, diremos que ele reverte orientação se seu determinante vale -1.* □.

Definição. *Uma função $f \in M_n$ preserva orientação se $f = t_a\varphi$, sendo $a \in \mathbb{R}^n$ e $\det(M_\varphi) = 1$. Caso contrário, diremos que f reverte orientação.* □

Lema. *O mapa $\sigma : M_n \to \{\pm 1\}, \sigma = t_a\varphi \mapsto \det(M_\varphi)$ é um morfismo de grupos.*

Prova. *Sejam $f, g \in M_n, f = t_a\varphi, g = t_b\psi$ com $a, b \in \mathbb{R}^n$. Então,*

$$\sigma(f \circ g) = \sigma(t_a \varphi t_b \psi) = \sigma(t_a t_{b'} \sigma \psi),$$

sendo b'=φ(b). Portanto,

$$\det(M_{\varphi\psi}) = \det(M_\varphi M_\psi) = \det M_\varphi \det M_\psi = \sigma(f)\sigma(g).$$ ■

Definição. *Define-se M_2 o grupo das isometrias no plano $\mathbb{R}^2$.*□

Considere

1) Translação: $t_a : \mathbb{R}^2 \to \mathbb{R}^2, x \mapsto x + a, a \in \mathbb{R}^2$.

2) Rotação: $\rho_\theta : \mathbb{R}^2 \to \mathbb{R}^2, (x, y) \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

3) Reflexão em Torno do Eixo -x: $\sigma : \mathbb{R}^2 \to \mathbb{R}^2, (x, y) \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

É preciso, no entanto, conferir que essas funções pertencem a M_2.

Lema. $t_a, \rho_\theta, \sigma \in M_2$

Prova. *Imediato.* ■

Lema. *Este lema será um exercício de álgebra linear.*

1) Uma matriz ortogonal cujo determinante vale 1 é da forma

$$\rho_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

para algum $\theta \in [0, 2\pi)$ único.

2) Uma matriz ortogonal de determinante -1 é da forma $\rho_\theta\sigma$, em que $\theta \in [0, 2\pi)$ é único e

$$\sigma \in \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Teorema. *Se $f \in M_2$, então $f = t_a\rho_\theta$, ou $f = t_a\rho_\theta\sigma$ para únicos $a \in \mathbb{R}^2, \theta \in [0, 2\pi)$ e $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Em outras palavras, $M_2 = \langle t_a, \rho_\theta, \sigma\rangle, a \in \mathbb{R}^2, \theta \in [0, 2\pi)$.*

Antes de demonstrar, um comentário sobre este teorema: Segundo ele, **qualquer** isometria no plano $\mathbb{R}^2$ é descrita por uma composição de isometrias elementares - translação, reflexão e rotação!

Prova. *Seja $f \in M_2$. Já sabemos que $f = t_a\varphi$, sendo $\varphi \in \mathcal{O}_2, a \in \mathbb{R}^2$. Logo, segue do lema anterior que*

$$f = t_a\rho_\theta \quad \text{ou } f = t_a\rho_\theta\sigma. \blacksquare$$

Corolário. *Isometrias $t_a\rho_\theta$ preservam orientação, enquanto $t_a\rho_\theta\sigma$ revertem orientação.*

Prova. *Seja $f = t_a\rho_\theta$. Então, como $\det\rho_\theta = 1$, f preserva orientação. Por outro lado, se $f = t_a\rho_\theta\sigma$, então $\det(\rho_\theta\sigma) = \det\rho_\theta \det\sigma = 1 \cdot (-1) = -1$. Portanto, f reverte orientação.* ■

Corolário. *Em M_2,*

1) $\rho_\theta t_a = t_{a'}\rho_\theta, \quad a' = \rho_\theta(a)$;
2) $\sigma t_a = t_{a'}\sigma, \quad a' = \sigma(a)$;
3) $\sigma\rho_\theta = \rho_{-\theta}\sigma$;
4) $t_a t_b = t_{a+b}$;
5) $\rho_\theta\rho_{\theta'} = \rho_{\theta+\theta'}$;
6) $\sigma\sigma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *i.e.* $ord(\sigma) = 2$.

Prova. *1)* $\rho_\theta t_a(t_{a'}\rho_\theta)^{-1} = \rho_\theta t_a\rho_\theta^{-1}t_{a'}^{-1} = \rho_\theta\rho_\theta^{-1}t_{\rho_\theta^{-1}(a)}t_{-\theta'} = t_{a'}t_{-a'} = t_{a'-a'} = Id.$

2) $(rta)(ta'\sigma)^{-1} = \sigma t_a r^{-1}t_{-a'} = \sigma\sigma^{-1}t_{r^{-1}(a)}t_{-a'} = t_{a'}t_{-a'} = Id.$

3) $\sigma\rho_\theta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin(\theta) & \cos(\theta) \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ -\sin(\theta) & -\cos(\theta) \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -\sin(-\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \rho_{-\theta}\sigma.$ ■

11 Aula 11 - 02/05/2023

Preciso de fotos dessa aula RS

12 Aula 12 - 04/05/2023

12.1 O que esperar?

- Outra Caracterização das Isometrias em $\mathbb{R}^2$

12.2 Isometrias em $\mathbb{R}^2$ - Relação com a Geometria.

Teorema. *Toda isometria do plano é da forma:*

1. *Isometrias que preservam orientação:*
   (a) *Translações;*
   (b) *Rotação do plano por ângulo θ em torno de algum ponto;*
2. *Isometrias que não preservam orientação são:*
   (c) *Reflexão com respeito a uma reta l;*
   (d) *Reflexão com respeito a uma reta l seguida de uma translação por um vetor não-nulo e paralelo a l.*

Prova. *(i) Seja $f \in M_2$ que preserva orientação e que não é translação, então*

$$f = t_a \rho_\theta$$

para algum $a \in \mathbb{R}^2$ e $\theta \neq 0$. Logo, queremos mostrar que existe $p \in \mathbb{R}^2$ tal que $t_p^{-1} f t_p = \rho_\theta$.

No entanto, $t_p^{-1} f t_p = t_{-t} t_a \rho_\theta t_p = t_{a-p+\rho(p)} \rho_\theta$. Então, queremos $p \in \mathbb{R}^2$ tal que $a - p + \rho(p) = (Id - \rho)(p)$. Considere o operador linear

$$Id - \rho_\theta = \begin{pmatrix} 1 - \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & 1 - \cos(\theta) \end{pmatrix}$$

e observe que $\det(Id - \rho_\theta) = (1 - \cos(\theta))^2 + \sin(\theta)^2 = 2 - 2\cos(\theta)$. Além disso, $2 - 2\cos(\theta) = 0$ equivale $\cos(\theta) = 1$, ou seja, $\theta = 0$. Portanto, existe $p \in \mathbb{R}^2$ tal que $t_p^{-1} f t_p = t_\theta$, ou seja,

$$f = t_p \rho_\theta t_p^{-1}.$$

(ii) Seja $f \in M_2$ que reverte orientação. Então,

$$f = t_a \rho_\theta \sigma.$$

Note que $\rho_\theta \sigma$ é a reflexão por uma reta passando pela origem. Assim, a menos de mudança de coordenada, podemos supor $\theta = 0$, isto é, $f = t_a \sigma$.

Agora, seja $(x, y) \in \mathbb{R}^2$. Logo, $f(x, y) = t_a(x, -y) = (x + a_1, -y + a_2)$, sendo $a = (a_1, a_2)$. Se $a_1 = 0$, então $f(x, y) = (x, -y + a_2)$, tal que f é uma reflexão com respeito à reta $l = \{y = \frac{1}{2} a_2\}$.

Por outro lado, se $a_1 \neq 0$, então f é reflexão com respeito à reta l com uma translação por $(a_1, 0)$. ■

Corolário. *Se $f \in M_2$ é como na demonstração do Teorema(i)(b). Então, o p como na demonstração é um ponto fixo de f.*

Prova. $f(p) = t_a \rho_\theta(p) = t_a(p - a) = p$. ■

Corolário. *A composição de rotações por (possivelmente) pontos diferentes é ainda uma rotação por (possivelmente) um terceiro ponto, a menos que tal composição seja uma translação.*

Prova. *Composição de isomorfismo que possuem orientação é uma isometria que preserva orientação.*

Exemplo 43. *Se ρ_1 é a rotação centrada em (1, 0) com $\theta = \pi$ e se ρ_2 é a rotação centrada em (3,0) com $\gamma = \pi$, então $\rho_2 \rho_1 = t_a, a = (4, 0)$* ■

Corolário. *A composição de composição de reflexões σ_1, σ_2 por retas não paralelas l_1, l_2 é uma rotação no ponto $p = l_1 \cap l_2$.*

Prova. *$\sigma_1\sigma_2$ preserva orientação. Do teorema,*

$$\sigma_1\sigma_2 = ta \text{ ou } \rho_\theta.$$

No entanto, $\sigma_1\sigma_2(p) = p$. Portanto, $\sigma_1\sigma_2 = \rho_\theta$ centrada em p. ■

Corolário. *A composição de reflexões σ_1 e σ_2 por retas paralelas distintas é uma translação por um vetor ortogonal às retas paralelas.*

Prova. *Do teorema, $\sigma_1\sigma_2 = t_a$, ou $\sigma_1\sigma_2 = \rho_\theta$. Como σ_1, σ_2 não têm ponto fixo, então $\sigma_1\sigma_2 = t_a$.*

A menos de mudança de coordenada, podemos supor σ_2 reflexão no eixo x e σ_1 reflexão $l = \{y = \frac{b}{2}\}$. Assim, $\sigma_2(x, y) = (x, -y), \sigma_1(x, y) = (x, -y + b)$ e $\sigma_1\sigma_2(x, y) = \sigma_1(x, -y) = (x, y + b)$. Portanto,

$$\sigma_1\sigma_2(x, y) = t_{(0,b)}(x, y) \quad e\ (0, b) \perp l.$$ ■

Proposição. *Seja $\mathcal{O}_2$ o grupo dos operadores ortogonais. Escolha um sistema de coordenadas. Então,*

a) $\mathcal{O}_2 \leq M_2$ é o subgrupo das isometrias que fixam a origem.

b) Se $H \leq M_2$ das isometrias que fixam um ponto p de $\mathbb{R}^2$, então $H = t_p\mathcal{O}_2t_p^{-1}$.

Prova. *a) Ok.*

b) Seja $f \in H, f(p) = p$. Então,

$$\underbrace{t_p^{-1}ft_p(0)}_{\in\mathcal{O}_2} = t_p^{-1}f(p) = t_p^{-1}(p) = 0.$$

Logo, existe $g \in \mathcal{O}_2$ tal que $t_p^{-1}ft_p = g$. Portanto, $f = t_pgt_p^{-1}$. ■

13 Aula 13 - 09/05/2023

13.1 O que esperar?

- Grupos diedrais;
- Subgrupos discretos;
- Ação de grupo;
- Teorema do Ponto Fixo.

13.2 Grupos Diedrais

Definição. *Seja D_n o subgrupo de M_2 gerado por ρ_θ e r, em que $\theta = \frac{2\pi}{n}$ e $r = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, i.e., $D_n = \langle \rho_\theta, r \rangle$. Chamamos D_n de grupo diedral.* □

Proposição. *Vale que $|D_n| = 2n$ e $D_n \cong \langle x, y \rangle$, em que $x^n = y^2 = 1$ e $xy = x^{-1}y$.*

Prova. *Observe que $\rho_\theta^n = Id$ e $r^2 = id$. Além disso, $\rho_\theta r = r\rho_\theta^{-1}$, ou seja,*

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta). \end{pmatrix}$$

Logo, os elementos de D_n são $Id, \rho_\theta, \rho_\theta^2, \cdots, \rho_\theta^{n-1}, r, r\rho_\theta, r\rho_t^2, \cdots, r\rho_\theta^{n-1}$. Portanto, $|D_n| = 2n$. Fica como exercício mostrar que $D_n \cong \langle x, y \rangle$ utilizando

$$\rho \mapsto x, \quad r \mapsto y. \blacksquare$$

Exemplo 44. *1) $D_1 \cong \mathbb{Z}/2\mathbb{Z}$;*

2) $D_2 = \langle Id, r, \rho, r\rho \rangle$, em que $\rho = \rho_\theta, \theta = \pi$.

3) $D_3 \cong S_3 = \langle (12), (123) \rangle$ (Exercício).

Observe que D_n é o grupo de simetrias do polígono regular de n-lados. Além disso, $D_n \neq S_n, n > 3$.

Definição. *Um subgrupo $\Gamma \leq (\mathbb{R}, +)$ é chamado subgrupo discreto se existe $\varepsilon \in \mathbb{R}_{\geq 0}$ tal que para todo $x \in \Gamma/\{0\}, |x| > \varepsilon$.*

Lema. *Suponha que $\Gamma \leq (\mathbb{R}, +)$ é discreto. Então, $\Gamma = \{0\}, \Gamma = a\mathbb{Z}$ para algum a real.*

Prova. *Sejam x, y em Γ distintos. Como $\Gamma \leq (\mathbb{R}, +)$,*

$$x - y \in \Gamma \text{ i.e. } |x - y| > \varepsilon$$

Logo, um intervalo limitado de $\mathbb{R}$ só pode conter uma quantidade finita de elementos de Γ.

$$\Big((an) \subseteq (a, b) \subseteq \mathbb{R}, a_n \in \Gamma \Rightarrow \text{ se } a_{n_0} < a_n \text{ e se } a_{n_+} > a_n \text{ para todo } n, \text{ então } |a_{n_0} - a_{n_+}| > |b - a| \Big)$$

Suponha $\Gamma \neq \{0\}$, então existe $b \in \Gamma, b \neq 0$. Como $\Gamma \leq (\mathbb{R}, +)$, então $-b \in \Gamma$. Logo, Γ contém algum número real positivo. Seja $a \in \Gamma$ o menor elemento positivo.

Afirmativo: *$\Gamma = a\mathbb{Z}$.*

De fato, se é claro que $a\mathbb{Z} \subseteq \Gamma$. Para $\Gamma \subseteq a\mathbb{Z}$, seja $b \in \Gamma$. Existe r real tal que $b = ar$. Agora, sejam m em $\mathbb{Z}$ e $0 \leq r_0 < 1$ tais que $r = m + r_0$. Logo,

$$b = am + ar_0 \Rightarrow b - am = ar_0 \in \Gamma.$$

Pela escolha de a, temos $r_0 = 0$, ou seja, $b = am \in a\mathbb{Z}$. ■

Teorema. *Seja $G \leq O_2, |G| < \infty$. Então, existe um $n \in \mathbb{Z}_{\geq 0}$ tal que*

a) $G \cong \mathbb{Z}/n\mathbb{Z}, G =< \rho >, \rho = \rho_\theta, \theta = \frac{2\pi}{n}$;

b) $G \cong D_n =< r, \rho >, \rho = \rho_\theta, \theta = \frac{2\pi}{n}$.

Prova. *Lembre-se que $\mathcal{O}_2 = \langle r, \rho_\theta \rangle$. Vamos separar em casos.*

Caso 1 - G só contém rotações:

Seja $H \coloneqq \{\theta \in \mathbb{R} : \rho_\theta \in G\}$. Como $G \leq \mathcal{O}_2$ e $|G| < \infty$, então $H \leq (\mathbb{R}, +)$ é discreto. Do lema anterior, $H = a\mathbb{Z}$ para algum a real.

Logo, G é o grupo das rotações por ângulos múltiplos inteiros de a. Em particular, G é cíclico.

Por fim, observe que $2\pi \in H$, logo existe n inteiro tal que $2\pi = an$, ou seja, $a = \frac{2\pi}{n}$. Portanto, $G =< \rho_0 >, \theta = \frac{2\pi}{n}$.

Caso 2 - r pertence a G:

Seja $H \leq G$ das rotações em G. Do caso 1, $H =< \rho >, \rho = \rho_\theta, \theta = \frac{2\pi}{n}, n \in \mathbb{Z}$. Assim, $r\rho^j \in G$ para todo $j = 0, \cdots, n-1$. Isto é, $D_n \subseteq G$.

Afirmamos que $G = D_n$. De fato, seja g em G. Se g é uma rotação, então g pertence a H, mas como $H \subseteq D_n$, então g pertence a D_n. Se g é uma reflexão, então $g = \rho^j r$ para algum j. Mas, $r \in G$, então $gr = \rho^j \in G$, então $\rho^j = \rho_\theta^i$ para algum i, e assim $g = \rho_\theta^i r \in D_n$. ■

Lema. *Seja $S = \langle s_1, \cdots, s_n \rangle \subseteq \mathbb{R}^{\not\varepsilon}$ e p o seu centroide, isto é, $p = \frac{1}{n}(s_1 + \cdots + s_n)$. Seja $f \in M_2$ e $h_i = f(s_i), q = f(p), i = 1, \cdots, n$. Então q é o centroide de $\{h_1, \cdots, h_n\}$.*

Prova. *Seja $f \in M_2$, podemos escrever $f = t_a\varphi$ para $a \in \mathbb{R}^2, \varphi \in O_2$.*

Se $f = t_a$, então

$$\begin{aligned} q = p + a &= \frac{1}{n}(s_1 + \cdots + s_n) + a \\ &= \frac{1}{n}((h_1 - a) + \cdots + (h_n - a)) + a = \frac{1}{n}(h_1 + \cdots + h_n). \end{aligned}$$

Se $f = \varphi$,

$$\begin{aligned} q = \varphi(p) &= \varphi\left(\frac{1}{n}(s_1 + \cdots + s_n)\right) \\ &= \frac{1}{n}\Big(\varphi(s_1) + \cdots + \varphi(s_n)\Big) = \frac{1}{n}(h_1 + \cdots + h_n). \blacksquare \end{aligned}$$

Corolário. *Seja $G \leq M_2, |G| < \infty$, então existe n em $\mathbb{Z}_{\geq 0}$ tal que*

a) $G \cong \mathbb{Z}/n\mathbb{Z}, G =< \rho >, \rho = \rho_\theta, \theta = \frac{2\pi}{n}$;

b) $G \cong D_n = \langle r, \rho \rangle, \rho = \rho_\theta, \theta = \frac{2\pi}{n}$.

13.3 Ações de Grupos

Definição. *Seja G um grupo e X um conjunto. Uma ação de G em X é um mapa*

$$G \times X \to X, (g, x) \mapsto g \cdot x$$

satisfazendo

i) $1 \cdot x = x$;

ii) $(gh) \cdot x = g \cdot (h \cdot x)$.□

Denotamos a frase " G é um grupo agindo em X" por $G \curvearrowright X$.

Exemplo 45. *i)* $M_2 \curvearrowright \mathbb{R}^2, \mathcal{O}_2 \curvearrowright \mathbb{R}^2$;

ii) $S_n \curvearrowright \{1, \cdots, n\}$;

iii) $G \curvearrowright G$.

Observe que, dado $G \curvearrowright X$, temos

$$m_g : X \to X, x \mapsto gx$$

como uma bijeção cuja inversa é $m_{g^{-1}}$.

Definição. *Dada uma ação $G \curvearrowright X$ e $x \in X$, defina*

$$\mathcal{O}(x) \coloneqq \{x' \in X : x' = gx, g \in G\}$$

como a orbita de x sob a ação $G \curvearrowright X$.□

Teorema. *Seja $G \leq M_2$ finito. Então, existe p em $\mathbb{R}^2$ tal que $g(p) = p$ para todo g em G.*

Prova. *Seja a em $\mathbb{R}^2$ e*

$$\mathcal{O}(a) \coloneqq \{g(a) : g \in G\}$$

Como $|G| < \infty$, podemos escrever

$$(a) = \{s_1, \cdots, s_n\} \subseteq \mathbb{R}^2.$$

Além disso, se g pertence a G, então

$$m_g : \mathcal{O}(a) \to \mathcal{O}(a), \quad s_i \mapsto g(s_i)$$

Com isso, se p é o centroide de $\mathcal{O}(a)$,

$$\begin{aligned} g(p) &= g(\frac{1}{n}(s_1 + \cdots + s_n)) \\ &= \frac{1}{n}(g(s_1) + \cdots + g(s_n)) \\ &= \frac{1}{n}(s_1 + \cdots + s_n) = p. \end{aligned}$$

Portanto, $g(p) = p$ para todo g em G. ■

14 Aula 14 - 11/05/2023

14.1 O que esperar?

- Estabilizadores e Teorema da Orbita-Estabilizador;
- Representação por Permutação;
- Ações Fiéis.

14.2 Motivação

Nesta introdução, discutiremos a intuição por trás dos estabilizadores de grupos e do Teorema da Órbita-Estabilizador. Também comentaremos sobre a Representação por Permutação e suas aplicações na vida real.

Um estabilizador de um grupo é um conceito fundamental na teoria dos grupos. Dado um grupo de ação G em um conjunto X, o estabilizador de um elemento x em X é o conjunto de todos os elementos em G que fixam x.

O Teorema da Órbita-Estabilizador é um resultado fundamental na teoria dos grupos que relaciona o tamanho de uma órbita de um elemento sob a ação de um grupo com o tamanho do estabilizador desse elemento. O teorema é enunciado da seguinte forma:

> Seja G um grupo finito que age em um conjunto X e seja x um elemento de X. Então, o tamanho da órbita de x sob a ação de G é igual ao índice do estabilizador de x em G.

A representação por permutação é uma maneira de representar os elementos de um grupo como permutações de um conjunto, o que é útil para visualizar e entender a estrutura do grupo.

Os conceitos de estabilizadores de grupos, o Teorema da Órbita-Estabilizador e a representação por permutação têm aplicações em várias áreas, incluindo física, química, ciência da computação e matemática. Na física, eles são usados para descrever simetrias em sistemas físicos. Por exemplo, as simetrias de rotação e translação em física são exemplos de ações de grupo, onde o estabilizador de um ponto no espaço é o conjunto de todas as rotações e translações que deixam o ponto inalterado. Na química, eles são usados para descrever a simetria de moléculas. A título de exemplo, a molécula de água tem uma simetria de rotação, onde a rotação em torno do eixo que passa pelo átomo de oxigênio e o centro da linha entre os dois átomos de hidrogênio deixa a molécula inalterada. Esta é uma ação de grupo, e o estabilizador é o conjunto de todas as rotações que deixam a molécula inalterada. Na ciência da computação, eles são usados em algoritmos de busca e ordenação. Por exemplo, o algoritmo de ordenação por permutação é baseado na ideia de representar as permutações de um conjunto como um grupo.

Intuitivamente, imagine que você tem um conjunto de objetos e um conjunto de operações que você pode realizar nesses objetos. Um grupo é apenas um conjunto de tais operações. Um estabilizador é o conjunto de operações que deixam um objeto específico inalterado. A órbita de um objeto é o conjunto de todos os estados que esse objeto pode alcançar através das operações do grupo. Para ilustrar, imagine que você tem um cubo e as operações são rotações do cubo. O estabilizador de uma face do cubo é o conjunto de rotações que deixam essa face no mesmo lugar. A órbita de uma face é o conjunto de todas as posições que essa face pode ocupar através das rotações do cubo. O Teorema da Órbita-Estabilizador nos diz que o número de estados possíveis (a órbita) é igual ao número de operações, dividido pelo número de operações que deixam o objeto inalterado (o estabilizador). A representação por permutação é uma maneira de visualizar essas operações como rearranjos dos objetos. Assim, se você tem três objetos e uma operação que troca o primeiro e o segundo objeto, isso pode ser representado como uma permutação (2,1,3).

14.3 Estabilizadores

Proposição. *Se $G \curvearrowright X$, o conjunto das órbitas dessa ação são classes de equivalência para a seguinte relação:*

$$x \sim y \iff \exists g \in G : y = gx.$$

Em particular, se $x \sim y$, então $\mathcal{O}(x) = \mathcal{O}(y)$ e X é particionado pelas órbitas.

Prova. *Se x pertence a X, $Cl(x) \coloneqq \{y \in X : y \sim x\} = \{y \in X : y = gx, g \in G\} = \{gx : g \in G\} = \mathcal{O}(x)$.* ■

Definição. *Seja $G \curvearrowright X$. Dado $x \in X$, definimos*

$$E(x) \coloneqq \{g \in G : gx = x\}$$

como o estabilizador de x. □.

Exemplo 46. *Se x pertence a X é um ponto fixo para $G \curvearrowright X$, então $E(x) = G$.*

Proposição. *$E(x) \leq G$.*

Prova. *Como $1x = x$, $1 \in E(x)$. Sejam $a, b \in E(x)$, então $(ab)x = a(bx) = ax = x$. Logo, $ab \in E(x)$. Agora, $ax = x$ implica que $x = a^{-1}x$, tal que $a^{-1} \in E(x)$. Portanto, $E(x) \leq G$.* ■

Exemplo 47. *1) $S_n \curvearrowright \{1, \cdots, n\}, E(n) = S_{n-1}$;*

2) $M_2 \curvearrowright \mathbb{R}^2, E((a, 0)) = \mathcal{O}_2$.

Proposição. *Seja $G \curvearrowright X, x \in X, H \coloneqq E(x)$. Então,*

i) Se a, b pertencem a G, então $ax = bx$ se, e somente se, $ab^{-1} \in H$ se, e somente se, $b \in aH$;

ii) Se ax=y, então $E(y) = aHa^{-1}$.

Prova. *(i) Se $ax = bx$, então $b^{-1}ax = x$, ou seja, $b^{-1}a \in H, b \in aH$ e existe h em H tal que $b^{-1}a = h$ e $b = ah^{-1}$.*

(ii) Seja $b \in E(y)$, i.e., $by = y$. Segue que

$$bax = ax \iff a^{-1}bax = x \iff a^{-1}ba \in H \iff b \in aHa^{-1}.$$

Logo, $E(y) \subseteq aHa^{-1}$.

Por outro lado, se $b \in aHa^{-1}$, existe h em H tal que $b = aha^{-1}$, de forma que

$$by = (aha^{-1})y = (ah)x = ax = y,$$

ou seja, b pertence a $E(y)$ e $aHa^{-1} \subseteq E(y)$. Portanto, $E(y) = aHa^{-1}$. ■

Exemplo 48. *Se $H \leq G$ e $G/H = \{aH : a \in G\}$, então $G \curvearrowright G/H$ por $g(aH) = gaH$. Fica como exercício mostrar que essa ação é transitiva e $E(1 \cdot H) = 1 \cdot H$.*

Exemplo 49. *Sejam $G = S_3$ e $H = \{1, y\}, y = (23)$.. Se $x = (123)$,*

$$G/H = \{H, \underbrace{xH}_{\{x,xy\}}, \underbrace{x^2H}_{x^2,x^2y}\} = \{[1], [x], [x^2]\} = \{\overline{1}, \overline{2}, \overline{3}\}.$$

Temos $S_3 \curvearrowright S_3/H$ como acima e, para $y \in S_3$,

$$\begin{aligned} m_g : & G/H \to G/H \\ & [1] \mapsto [1] \\ & [x] \mapsto \{x^2y, x^2\} = [x^2] \\ & [x^2] \mapsto [x]. \end{aligned}$$

Logo, y age em G/H como age em $\{1, 2, 3\}$ (Verifique que o mesmo acontece para x).

O resultado a seguir relaciona a órbita com o estabilizador, conhecido como Teorema Órbita-Estabilizador.

Teorema. *Se $G \curvearrowright X, x \in X$ temos uma bijeção $\varepsilon : G/E(x) \to \mathcal{O}(x), [aE(x)] \mapsto ax$. Além disso, $\varepsilon(g * aE(x)) = g\varepsilon(aE(x))$.*

Prova. *Vamos começar mostrando que ε está bem-definida. De fato, seja $H = E(x)$. Note que $\varepsilon(aH) = ax \in \mathcal{O}(x)$. Ainda se $aH = bH$, então $b^{-1}a \in H$. Logo, existe $h \in H$ tal que $a = bh$ e, assim, $ax = bhx = bx$. Por isso, $\varepsilon(aH) = \varepsilon(bH)$.*

Note que ε é sobrejetora diretamente. Para ver que ε é injetora, seja $\varepsilon(aH) = \varepsilon(bH)$. Segue que

$$ax = bx \iff b^{-1}ax = x \iff b^{-1}a \in H.$$

Portanto, $b \in aH$ é equivalente a $aH = bH$. ■

Exemplo 50. *Temos $M_2 \curvearrowright \mathbb{R}^2$ transitiva e $E((0,0)) = \mathcal{O}_2$. Logo, do Teorema Órbita-Estabilizador, $|\cdot| : M_2/\mathcal{O}_2 \to \mathbb{R}^2$.*

Corolário. *Se X é um conjunto finito e $G \curvearrowright X, x \in X$, então*

$$|G| = |E(x)| \cdot |\mathcal{O}(x)|.$$

Prova. *Segue de*

$$|G| = |E(x)| \cdot [G : E(x)] = \underbrace{|E(x)| \cdot |\mathcal{O}(x)|}_{Teorema\ \acute{O}rbita\text{-}Estabilizador} \quad . \blacksquare$$

Algumas observações devem ser feitas. Primeiramente, se $G \curvearrowright X$ e $H \leq G$, então $H \curvearrowright X$. Além disso, se $G \curvearrowright X$ e $X' \subseteq X, |X'| = r$, então

$$gX' = \{gy : y \in X'\}$$

também tem ordem r. Logo, G age no conjunto dos subconjuntos de ordem r de X.

14.4 Representações por Permutações

Definição. *Uma representação por permutação do grupo G é um morfismo $\varphi : G \to S_n$.*□

Proposição. *Se $X = \{1, \cdots, n\}$, então temos*

$$|\cdot| : \left\{ A\text{ções de } G \text{ em } X \right\} \to \left\{ Representação \text{ por } Permutação \right\}$$

uma bijeção.

Prova. *Dado $G \curvearrowright X$, para cada g de G, temos*

$$m_g : X \to X, \quad x \mapsto gx.$$

Logo, temos $\varphi : G \to S_n, g \mapsto m_g$. Por outro lado, dado um morfismo $\varphi : G \to S_n$, temos

$$G \times X \to X, \quad (g, x) \mapsto gx = \varphi(g)x.$$ ■

Exemplo 51. *Segue que $D_n \curvearrowright \{v_1, \cdots, v_n\}$ equivale aos vértices de um polígono regular de n-lados. Com isso, temos um morfismo $D_n \to S_n$.*

Proposição. *Se X é um conjunto qualquer e Perm(X) = $\{f : X \to X : f$ é bijeção$\}$ é o grupo das permutações de X, então temos*

$$|\cdot| : \left\{ A\text{ções de } G \text{ em } X \right\} \to \left\{ Morfismos \text{ de } G \text{ em } Perm(X) \right\}$$

Definição. *A ação $G \curvearrowright X$ é dita fiel se o morfismo correspondente de G em Perm(X) é injetor.* □

Exemplo 52. *(Exercícios:)Mostre que $G = GL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$.*

Se $e_1 = (1,0), e_2 = (0,1), e_1 + e_2 = (1,1) = e_3$, mostre que $G \curvearrowright \{e_1, e_2, e_3\}$ fielmente, de maneira que

$$G \hookrightarrow S_3 \text{ é injetora}$$

e, como $|G| = |S_3|$, vale que $G \cong S_3$.

$G \curvearrowright X$ é fiel se $gx = x$ para todo x em X implica em $g = 1$.

15 Aula 15 - 23/05/2023

15.1 O que esperar?

- Fórmula de Burnside;
- Teorema de Colty;
- Teorema de Equação de Classe;
- p-Grupos.

15.2 Motivações

Fórmula de Burnside

A Fórmula de Burnside é uma ferramenta importante na teoria dos grupos, usada para contar o número de órbitas de uma ação de grupo. Seja G um grupo finito que atua em um conjunto X, a fórmula de Burnside é dada por:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

onde X/G é o conjunto de órbitas de X sob a ação de G, e X^g é o conjunto de pontos fixos do elemento g em G.

Por exemplo, podemos usar a fórmula de Burnside para contar o número de maneiras de colorir um cubo com três cores diferentes, considerando rotações como iguais.

Ou seja, a fórmula de Burnside é usada para contar coisas em situações onde certas transformações (como rotação ou reflexão) não mudam a "essência"do que estamos contando.

Teorema de Colty

O Teorema de Colty é um resultado importante na teoria dos grupos, que se aplica a grupos p-nilpotentes. Ele afirma que se G é um grupo p-nilpotente finito e H é um subgrupo normal de G, então o conjunto $N_G(p)$ de elementos de ordem p em G que normalizam H é também um subgrupo normal de G.

Em outras palavras, o Teorema de Colty é uma propriedade interessante que certos tipos de grupos possuem. Ele nos dá uma maneira de encontrar novos subgrupos normais em um grupo, o que é útil para entender a estrutura do grupo.

Teorema da Equação de Classe

O Teorema da Equação de Classe é um resultado fundamental na teoria dos grupos que relaciona o tamanho de um grupo com o tamanho de suas classes de conjugação. Dado um grupo finito G, o teorema afirma que:

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)]$$

onde $Z(G)$ é o centro de G, $C_G(x_i)$ é o centralizador de x_i em G, e a soma é sobre todas as classes de conjugação não-trivial de G.

Uma forma de visualizar isso é que o Teorema da Equação de Classe nos dá uma maneira de "dividir"um grupo em peças menores, chamadas classes de conjugação.

p-Grupos

Os p-grupos são um tipo especial de grupo que é especialmente importante na teoria dos grupos. Um grupo finito é um p-grupo se e somente se sua ordem (o número de seus elementos) é uma potência de p. Dado um grupo finito G, os teoremas de Sylow garantem a existência de um subgrupo de G de ordem p^n para cada potência do primo p^n que divide a ordem de G. Os p-grupos da mesma ordem não são necessariamente isomórficos; por exemplo, o grupo cíclico C_4 e o grupo de Klein V_4 são ambos 2-grupos de ordem 4, mas eles não são isomórficos Intuitivamente, p-grupos são grupos cujo número de elementos é uma potência de um número primo. Eles têm algumas propriedades interessantes e são uma área ativa de pesquisa na teoria dos grupos.

15.3 Fórmula de Burnside

Lema. *Sejam X um conjunto finito e G um grupo finito agindo em X. Se $X^g := \{x \in X : gx = x\}, g \in G$. Então,*

$$\sum_{x \in X} |E(x)| = \sum_{g \in G} |X^g|.$$

Prova. *Temos*

$$\sum_{g \in G} |X^g| = \#\{(g, x) \in G \times X : gx = x\} = \sum_{x \in X} |E(x)|. \blacksquare$$

Esse lema será usado para provarmos o resultado conhecido como Fórmula Burnside.

Proposição. *Com as notações do lema anterior,*

$$|G| \cdot |X/G| = \sum_{g \in G} |X^g|,$$

em que X/G é o conjunto das orbitas distintas com respeito à ação de $G \curvearrowright X$.

Prova. *Suponha $X/G = \{\mathcal{O}(x_1), \cdots, \mathcal{O}(x_n)\}$, isto é, $X = \bigcup_{i=1}^{n} \mathcal{O}(x_i)$ e $|X/G| = n$. Assim,*

$$\sum_{g \in G} |X^g| = \sum_{x \in X} |E(x)| = \sum_{x \in X} \frac{|G|}{|\mathcal{O}(x)|}.$$

Pelo lema, portanto,

$$\sum_{g \in G} |X^g| = |G| \cdot \left(\sum_{x \in \mathcal{O}(x_1)} \frac{1}{|\mathcal{O}(x_1)|} + \cdots + \sum_{x \in \mathcal{O}(x_n)} \frac{1}{|\mathcal{O}(x_n)|} \right) = |G| \cdot |X/G|. \blacksquare$$

Exemplo 53. *D_3 age em $X = \{1, 2, 3\}$ o conjunto de vértices do triângulo equilátero*

$$D_3 = \{1, (123), (132), (12), (13), (23)\}$$

Com a notação utilizada,

$$X^1 = X, \quad X^{(123)} = \emptyset, \quad X^{(132)} = \emptyset, \quad X^{(12)} = \{3\}, X^{(13)} = \{2\}, X^{(23)} = \{1\}.$$

Logo, pela Fórmula Burnside,

$$\sum_{g \in D_3} |X^g| = G = |D_3||X/G|.$$

Vamos considerar o seguinte mapa para a próxima discussão:

$$G \times G \to G, \quad (g, x) \mapsto gx.$$

Como exercício, mostre que ele satisfaz os axiomas da ação de G em G.

Lema. *$G \curvearrowright G$ fielmente por multiplicação à esquerda.*

Prova. *Segue de*

$$E(x) = \{g \in G : gx = x\} = \{1\}. \blacksquare$$

Com isso, estudemos o teorema de Colty

Teorema. *Todo grupo G é um subgrupo do grupo de permutações de algum conjunto. Em particular, se $|G| = n$, então G é subgrupo de S_n.*

Prova. *Como $G \curvearrowright G$ fielmente por multiplicação à esquerda, então*

$$\varphi : G \to Perm(G), \quad g \mapsto m_g : G \to G, x \mapsto gx$$

sendo φ injetora. Se $|G| = n$, então $Perm(G) = S_n$ e o teorema segue pelo Teorema do Isomorfismo.

Exemplo 54. *Defina $G \times G \to G, \quad (g, x) \mapsto gxg^{-1}$. O mapa acima satisfaz os axiomas de ação de G.*

Definição. *Dado x em G, seja $Z(x) \coloneqq \{g \in G : gx = xg\}$ é o centralizador de x.* □

Exemplo 55. *Exercício: $Z(x) \leq G$.*

Proposição. *Se $G \curvearrowright G$ por conjugação, então $E(x) = Z(x)$.*

Prova.

$$\begin{aligned} E(x) &= \{g \in G : g * x = x\} \\ &= \{g \in G : gxg^{-1} = x\} \\ &= \{g \in G : gx = xg\} = Z(x). \blacksquare \end{aligned}$$

Definição. *Se $G \curvearrowright G$ por conjugação, definimos a classe de conjugação de x em G por ser a órbita $\mathcal{O}(x)$. Além disso, denotamos $\mathcal{O}(x)$ por $C(x)$. Assim,*

$$C(x) \coloneqq \{gxg^{-1} : g \in G\}.\square$$

Proposição. *1) $|G| = |Z(x)||C(x)|, \quad \forall x \in G;$*

2) $x \in Z(x), Z(G) \subseteq Z(x), \quad \forall x \in G;$

3) $x \in Z(G) \iff Z(x) = G \iff C(x) = \{x\}$.

Prova. *A prova de (1) segue pelo Teorema Órbita-Estabilizador.*

Para 2, note que, como $xx = x^2 = xx$, então x está em $Z(x)$. Além disso, se g pertence a $Z(G)$, então $gh = hg$ para todo h de G. Em particular, $gx = xg$, ou seja, $g \in Z(x)$.

Por fim, para 3, se $x \in Z(G)$, temos

$$\begin{aligned} x \in Z(g) &\iff xg = gx \forall g \in G \\ &\iff g \in Z(x) \forall g \in G \\ &\iff Z(x) = G \\ &\iff C(x) = \{x\}. \quad \blacksquare \end{aligned}$$

Podemos agora entender o Teorema da Equação de Classe:

Teorema. *Sejam $C(x_1), \cdots, C(x_n)$ as órbitas que particionam G com respeito à ação por conjugação $G \curvearrowright G$, então*

$$\begin{aligned} |G| &= \sum_{i=1}^{n} |C(x_i)| \\ &= |Z(G)| + \sum_{x_i \notin Z(G)} |C(x_i)|. \end{aligned}$$

Exemplo 56. *$S_3 \curvearrowright S_3$ por conjugação. Escreva $S_3 = \langle x, y \rangle$ em que $x^2 = 1$ e $y^3 = 1$. Assim, $Z(y) \leq S_3$, logo $|Z(y)| = 1, 2, 3$, ou 6. Agora se y pertence a Z(y), então $|Z(y)| = 3$ ou 6. Mas, $xy = y^2 x \neq yx$. Desta forma, $|Z(y)| = 3$ e, assim, $|C(y)| = 2$. De exercício, mostre que $|C(x)| = 3$. Portanto, a equação de classe para S_3 é*

$$G = 2 + 3 + 1$$

Definição. *Seja p um número primo. G é um p-grupo se $|G| = p^n$ para algum n.* □

Proposição. *O centro de um p-grupo é não trivial.*

Prova. *Seja G um p-grupo. Da equação de classes,*

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |C(x_i)|$$

em que $G = \bigsqcup_{i=1}^{n} C(x_i) \sqcup Z(g)$.

Agora, do Teorema Órbita-Estabilizador, $|C(x_i)| \Big| p^n$ Logo, $|C(x_i)| = p^{n_i}$ para algum $n_i \geq 0$. Como $x_i \notin Z(G)$, segue que $|C(x_i)| > 1$, ou seja, $n_i > 0$. Portanto,

$$p \Big| |G| - \sum |C(x_i)| = |Z(G)|$$

$$p \Big| |Z(G)| \Rightarrow |Z(G)| > 1. \quad \blacksquare$$

A seguir, veremos um teorema de ponto fixo, resultados que sempre fornecem implicações agradáveis na matemática.

Teorema. *Sejam G um p-grupo e X um conjunto finito com $G \curvearrowright X$. Se p não divide $|X|$, então existe $x \in X$ tal que $E(x) = G$.*

Prova. *Escreva $X = \bigsqcup_{i=1}^{n} \mathcal{O}(x_i)$. Então,*

$$|X| = \sum |\mathcal{O}(x_i)|.$$

Do Teorema Órbita-Estabilizador, $|\mathcal{O}(x_i)| \Big| |G| = p^n$. Então, existem $n_i \geq 0$ tais que $|\mathcal{O}(x_i)| = p^{n_i}$. Se $n_i > 0$ para todo i, então $p \Big| \sum |\mathcal{O}(x_i)| = |X|$. Logo, existe j tal que $n_j = 0$. Portanto,

$$|\mathcal{O}(x_j)| = 1 \Rightarrow |E(x_j)| = |G| \Rightarrow E(x_j) = G. \blacksquare$$

Proposição. *Se $|G| = p^2$, p primo, então G é abeliano.*

Prova. *Da proposição anterior, $|Z(G)| = p$ ou p^2. Se $|Z(G)| = p^2$, está ok. Caso $|Z(G)| = p$, então existe x fora de Z(G). Assim, $Z(x) \supsetneq Z(G)$ e, assim,*

$$|Z(x)| = p^2 \Rightarrow x \in Z(G) \backslash X.$$

Portanto, $Z(G) = G$. $\blacksquare$

Corolário. *Um grupo de ordem p^2 é cíclico ou o produto de dois grupos cíclicos de ordem p, sendo p primo.*

Prova. *Se $|G| = p^2$, se G tem elemento de ordem p^2, está ok.*

Caso contrário, todo elemento não-identidade de G tem ordem p. Assim, existem $x, y \in G$ com $|x| = |y| = p$ e $y \notin \langle x \rangle$. Portanto,

$$\langle x \rangle \times \langle y \rangle \to G, \quad (x^m, y^n) \mapsto x^m y^n$$

é um isomorfismo. $\blacksquare$

16 Aula 16 - 25/05/2023

16.1 O que esperar?

- Grupos Simples;
- Normalizadores;
- Teoremas de Sylow.

16.2 Grupos Simples

Definição. *Um grupo G é simples se $G \neq \{1\}$ e não tem subgrupo normal próprio (Não existe subgrupo normal de G diferente de $\{1\}$ ou G.)* $\square$

Exemplo 57.
- *Todo p-grupo é um grupo simples;*
- $A_2 = \{1\}$*, ou seja, não é simples;*
- $A_3 = \mathbb{Z}/3\mathbb{Z}$ *é cíclico de ordem 3, logo simples;*
- A_4 *não é simples, pois* $H = \{Id, (12)(34), (13)(24), (14)(23)\}$ *é um subgrupo normal de* S_4 *e* $H \leq A_4$.
- A_n *é simples para* $n \geq 5$

Definição. *Seja X o conjunto de todos os subgrupos de um grupo G. Então,*

$$G \times X \to X, \quad (g, H) \mapsto gHg^{-1}$$

é a ação por conjugação e, dado $H \in X$, seu estabilizador é

$$N(H) = \{g \in G : gHg^{-1} = H\}$$

chamado de normalizador de H. $\square$

Observe que $N(H) \leq G$ e $H \leq N(G)$. Além disso, pelo Teorema da Órbita-Estabilizador,

$$\begin{aligned} |G| &= |N(H)| \cdot (\#\text{subgrupos de G conjugados por H}) \\ &= |N(H)|[G : N(H)]. \end{aligned}$$

Proposição. *Sejam $H \leq G, N = N(H)$ normalizador.*

1) $H \trianglelefteq N$;

2) $H \trianglelefteq G \iff N = G$.

3) $|H|\big||G|$ e $|N|\big||G|$

Prova. *1) Dado g em N, então $gHg^{-1} = H$ por definição de $N = N(H)$, logo $H \trianglelefteq N$.*
2) Para todo g de G, $H \trianglelefteq G \iff gHg^{-1} = H$. Consequentemente, $H \trianglelefteq G$ se, e somente se, $g \in N$ para todo g em G. Logo, se, e somente se, $N = G$.
3) Ok. ■

Exemplo 58. *Em $S_3, |C((123))| = 2$, logo, se $H = \langle(123)\rangle$, então $|\mathcal{O}(H)| = 2$ e $|N(H)| = \frac{6}{2} = 3$.*

16.3 Teoremas de Sylow

Adotaremos a seguinte convenção: Se G é um grupo de ordem $n = p^{varepsilon}m$, sendo p um número primo e $mdc(p^{varepsilon}, m) = 1$.

Definição. *Se $|G| = p^{varepsilon}m = n$, um subgrupo $H \leq G$ é um p-subgrupo de Sylow (ou p-Sylow) se $|H| = p^{varepsilon}$.*□

Observe que H é p-subgrupo de Sylow se $p \nmid [G : H]$.

Exemplo 59. *Em S_3, $\langle(12)\rangle$ é um 2-Sylow e $\langle(123)\rangle$ é um 3-Sylow.*

Uma pergunta é: quando existem p-subgrupos de Sylow? Por exemplo, A_4 tem ordem 12, mas não tem subgrupo de ordem 6.

Lema. *Seja X o conjunto de todos os subconjuntos de um grupo G. Então, $G \curvearrowright X$ por multiplicação à esquerda e com respeito a esta ação, se $\mathcal{U} \in X$,*

$$|E(\mathcal{U})| \Big| |G| \quad e \ |E(\mathcal{U})| \Big| |\mathcal{U}|$$

Prova. *Se $H \leq G$, temos*

$$H \times G \to G \quad (h, g) \mapsto hg.$$

Observe que $\mathcal{O}(g) = Hg$. Agora, se $H = E(\mathcal{U})$,$\mathcal{U} \in X$, então

$$H \times \mathcal{U} \to \mathcal{U} \quad (h, u) \mapsto hu$$

é uma ação de $\mathcal{U}$ bem-definida. Logo, todas as órbitas dessa ação particionam $\mathcal{U}$, ou seja, existem $u_1, \cdots, u_n \in \mathcal{U}$ tais que

$$\mathcal{U} = \bigsqcup_{i=1}^{n} Hu_i.$$

Logo, $|\mathcal{U}| = \sum_{i=1}^{n} |Hu_i| = \sum^{n} |H| = n|H|$. Portanto, $|H| \Big| |\mathcal{U}|$. ■

Lema. *Seja $n = p^{\varepsilon}m, \varepsilon > 0$, p primo, $p \nmid m$. Então, o número N de subconjuntos de ordem p^{ε} de um conjunto de ordem n não é divisível por p, isto é, $p \nmid N$.*

Prova. *Exercício.* $\left(N = \binom{n}{p^{\varepsilon}}\right)$

O resultado a seguir é o primeiro dos três teoremas de Sylow.

Teorema. *Seja G um grupo finito e $p \mid |G|$, p primo. Então, existe um p-subgrupo de Sylow.*

Prova. *Seja $|G| = n = p^{\varepsilon}m, (p^{\varepsilon}, m) = 1$ e considere*

$$X = \{\mathcal{U} \subseteq G : |\mathcal{U}| = p^{\varepsilon}\}.$$

Temos $G \curvearrowright X$ por multiplicação à esquerda. Logo, existem $\mathcal{U}_1, \cdots, \mathcal{U}_n$ em X tais que $X = \bigsqcup \mathcal{O}(\mathcal{U}_i)$. Logo, $N = |X| = \sum |\mathcal{O}(\mathcal{U}_i)|$, tal que do segundo lema, $p \nmid N$. Então, existe j tal que $p \nmid |\mathcal{O}(\mathcal{U}_j)|$. Agora, considere $H = E(\mathcal{U}_j)$. Do lema 1, também,

$$|H| \Big| |\mathcal{U}_j| = p^{\varepsilon}.$$

Então, $|H| = p^r$ para algum $r \geq 0$. Pelo Teorema Órbita-Estabilizador,

$$|G| = p^{\varepsilon}m = |H||\mathcal{O}(\mathcal{U}_j)|,$$

mas, como $p \nmid |\mathcal{O}(\mathcal{U}_j)|$, segue que $|H| = p^{\varepsilon}$ (i.e. $r = \varepsilon$). ■

Corolário. *Se $p \mid |G|$, então existe g em G tal que $|g| = p$.*

Prova. *Escreva $|G| = p^\varepsilon m$ $(p^\varepsilon, m) = 1$ e seja $H \leq G$, $|H| = p^\varepsilon$ (Aqui, foi usado o Primeiro Teorema de Sylow) Seja h em H diferente da identidade. Logo, $|h| = p^r$. Assim, $g = h^{p^r - 1}$ tem ordem p, pois*

$$g^p = (h^{p^r-1})^p = h^{p^r} = 1. \quad \blacksquare$$

Em seguida, temos o segundo dos três teoremas de Sylow.

Teorema. *Seja $|G| = p^\varepsilon m, \varepsilon > 0$.*

1) Os p-subgrupos de Sylow são conjugados entre si.

2) Todo p-subgrupo de G está contido em algum p-subgrupo de Sylow.

Observação - No item (1), se H é p-subgrupo de Sylow, então qualquer outro é um elemento de $\mathcal{O}(H) = \{gHg^{-1} : g \in G\}$.

Prova. *Seja $X \coloneqq \{xH : x \in G\}$, em que H é um p-subgrupo de Sylow de G. Observe que $|X| = m$. Agora, considere $G \curvearrowright X$ por*

$$G \times X \to X, \quad (g, xH) \mapsto gxH.$$

Seja $K \leq G$ um p-subgrupo e restrinja a ação anterior a K, isto é,

$$K \times X \to X, \quad (k, xH) \mapsto kxH.$$

Como K é um p-grupo e p não divide $|X|$, do Teorema do Ponto Fixo, existe $x \in G$ tal que $k \cdot xH = xH$ para todo k de K. Logo, dados $k \in K$ e $h_1 \in H$, existe $h_2 \in H$ tal que

$$kxh_1 = xh_2 \iff k = xh_2h_1^{-1}x^{-1} \in xHx^{-1}.$$

Portanto, $K \subseteq xHx^{-1}$ e (2) está provado. Em particular, se K é um p-subgrupo de Sylow, então $K \leq xHx^{-1}, |K|^\varepsilon = |xHx^{-1}|$. Portanto, $K = xHx^{-1}$. $\blacksquare$

Corolário. *Se n_p é o número de p-subgrupos de Sylow distintos, então $n_p = [G : N(H)]$, em que H é um algum p-Sylow.*

Prova. *Segue diretamente de*

$$n_p = |\mathcal{O}(H)| = \frac{|G|}{|N(H)|} = [G : N(G)]. \quad \blacksquare$$