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

20 de abril 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 $(A, \mu, \varphi) = (A, +, \cdot)$. $\square$

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

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*

$\blacksquare$

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 $(S_n, \circ)$. $\blacksquare$

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.* $\square$

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

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

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

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

2.3 Subgrupos

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

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

Denotaremos 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*

$$\cdot_H : H \times H \to H.$$

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*

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

também é possível mostrar isso usando o item 3 da proposição.
2.3) $\Rightarrow$ *imediato.* ■

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

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

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

2.2) Se $m|l'$ *e* $n|l'$*, então* $l|l'$*.*
Definimos $l = mmc(m, n)$ *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, $< S > \leq G$. $\blacksquare$

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 $< g_1, \cdots, g_n >$.* $\square$

Definição. *Sejam G um grupo e g um elemento seu. Se $G =< g >$, diremos que G é um grupo cíclico.* $\square$

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.* $\blacksquare$

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. $\blacksquare$

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 $\sigma = (a_1 \cdots a_r)$.*$\square$

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

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

Definição. *Duas permutações $\sigma, \tau \in S_n$ são disjuntas se para todo $j \in \{1, \cdots, n\}, \sigma(j) = j$ 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, $r = (a_1a_2)(a_1a_3) \cdots (a_1a_r)$.* $\blacksquare$

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

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

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

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

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

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

Note que

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

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

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

2) $U(\sigma)$ *sempre tem 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)$sgn : S_n \to \{+1, -1\}, \sigma \mapsto sgn(\sigma),$ $sgn(\sigma\tau) =$

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)$\varphi : G \to G', g \mapsto 1',$ *em que* $1'$

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:*

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

Prova.

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

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. $<(12)>=<id,(12)>\ntrianglelefteq S_3$*, 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 $S = \bigsqcup S_{i i\in I}$ é uma partição, denotamos $\overline{S} := \{[S_i]\}$ o conjunto das classes de equivalência dadas por S_i.*

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

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*

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

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*

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

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*

$$\begin{aligned} &1) \quad |G| = |\ker\varphi||im\varphi| \\ &2) \quad |\ker\varphi|\Big|\,|G| \\ &3) \quad |im\varphi| \text{ divide } |G| \text{ e } |G'|. \end{aligned}$$

Prova. $1 \Rightarrow)$ *Temos*

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

$$\begin{aligned} &\Rightarrow |G| = |im\varphi||\ker\varphi| \\ &\Rightarrow |G| = |\ker\varphi|[G : \ker\varphi] = |\ker\varphi||im\varphi|. \end{aligned}$$

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,*

$$G = g_1H \bigsqcup \cdots \bigsqcup g_nH = \bigsqcup_{i=1}^{n} g_iH \quad e \quad H = \bigsqcup_{j=1}^{m} h_jK.$$

A multliplicação por g_i *é uma bijeção*

$$m_{g_i} : h_jK \to g_ih_jK, \quad x \mapsto g_ix.$$

Assim, $g_iH = \bigsqcup_{j=1}^{m} g_ih_jK$*. Portanto,*

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

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,

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

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,*

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

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 $(g_1, g_1')(g_2, g_2') = (g_1 g_1', g_2 g_2')$ é um grupo. Além disso, temos os seguintes morfismos:

$$\begin{aligned} \pi : G \times G' \to G, &\quad \pi' : G \times G' \to G' \\ i : G \to G \times G', &\quad i' : G' \to G \times G', \end{aligned}$$

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*

$$\begin{aligned} 1 &= ar + bs \\ k &= ark + bsk. \end{aligned}$$

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,* $ord g_i=2$ *ou 4. Se existe* $g_i\in G$ *tal que* $ord(g_i)=4$, *então* $G\approx C_4$.

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