Grupos e Corpos

Prof. Lucas Calixto

Aula 1 - Primeiras Definições

Estrutura do curso

Aulas as Quintas das 17:00 as 18:00 - Tirar dúvidas de conteúdo, exercicios, discutir a materia

Usaremos o Microsoft Teams para encontros

Tentarei sempre postar vídeos nas Segundas e teremos lista de exercicios toda semana

Avaliações - 3 Provas via Moodle

Bibliografia:

• Thomas W. Judson. Abstract algebra. 2012 annual edition, 2012. Link para download http://abstract.ups.edu/download/aata-20200730.pdf

• Israel Herstein - Topics in algebra (versão em português: Tópicos de Álgebra)

• Arnaldo Garcia e Yves Lequain - Elementos de Álgebra

Introdução

Grupos - Busca de simetrias de objetos matemáticos (geométricos, algébricos)

Teoria moderna (Évariste Galois): determinar as raízes de polis em termos dos seus coeficientes

Hoje tem papel importante - teoria de códigos, criptografia, fisica, quimica, etc.

Exemplos de grupos que já somos familiares:

- $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$: números inteiros
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$: números inteiros módulo n
- $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$: matrizes reais $n \times n$ invertíveis

$\mathbb{Z}$

Em $(\mathbb{Z}, +)$ sabemos que:

- $\forall a, b \in \mathbb{Z},\ a + b \in \mathbb{Z}$
- $\exists\ 0 \in \mathbb{Z}$ tal que $0 + a = a, \forall a \in \mathbb{Z}$
- $\forall a \in \mathbb{Z}$, $\exists b \in \mathbb{Z}$ tal que $a + b = 0$ (chamamos $b = -a$)

Pergunta: Temos essas propriedades em $(\mathbb{Z}, \cdot)$?

$\mathbb{Z}_n$

Lembrem: $\mathbb{Z}_n = \{0 \ (mod \ n), \ldots, n-1 \ (mod \ n)\}$, ou $\mathbb{Z}_n = \{0, \ldots, n-1\}$

Soma: $a + b = (a + b) \ (mod \ n) =$ resto da divisão de $a + b$ por n

Produto: $ab = ab \ (mod \ n) =$ resto da divisão de ab por n

Em $(\mathbb{Z}_n, +)$ sabemos que:

- $\forall a, b \in \mathbb{Z}_n, \ a + b \in \mathbb{Z}_n$ (por definição)
- $\exists \ 0 \in \mathbb{Z}_n$ tal que $0 + a = a, \forall a \in \mathbb{Z}_n$
- $\forall a \in \mathbb{Z}_n, \ \exists b \in \mathbb{Z}_n$ tal que $a + b = 0$ (de fato, tome $b = n - a$)

A última propriedade não vale em geral para $(\mathbb{Z}_n, \cdot)$

Exemplo

Em $\mathbb{Z}_8 = \{0, \ldots, 7\}$, temos:

$$7 + 4 = 1, \quad 3 + 5 = 0, \quad 3 + 4 = 7, \quad 7 \cdot 3 = 5$$

Tabela de Multiplicação em $\mathbb{Z}_8$

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Qual propriedade vale para $(\mathbb{Z}_8, +)$ mas falha para $(\mathbb{Z}_8, \cdot)$?

Proposição: $\forall a, b, c \in \mathbb{Z}_n$ temos:

1. $a + b = b + a$, $ab = ba$ (comutatividade de $+$ e $\cdot$)
2. $(a + b) + c = a + (b + c)$, $(ab)c = (ab)c$ (associatividade de $+$ e $\cdot$)
3. $a + 0 = a$, $1a = a$ (existencia do elemento neutro para $+$ e $\cdot$)
4. $a(b + c) = ab + ac$ (distributividade de $\cdot$ com respeito a $+$)
5. $\forall a \in \mathbb{Z}_n$, $\exists b \in \mathbb{Z}_n$ tal que $a + b = 0$ (existencia de inverso aditivo)
6. $a \in \mathbb{Z}_n$ possui inverso multiplicatiovo se e só se $mdc(a, n) = 1$, ou seja,

$$\exists b \in \mathbb{Z}_n \text{ tal que } ab = 1 \text{ se e só se } mdc(a, n) = 1$$

Prova de (6): ($\Rightarrow$)

$$ab = 1 \Leftrightarrow n|ab - 1 \Leftrightarrow ab - nk = 1 \text{ para algum } k \in \mathbb{Z}$$

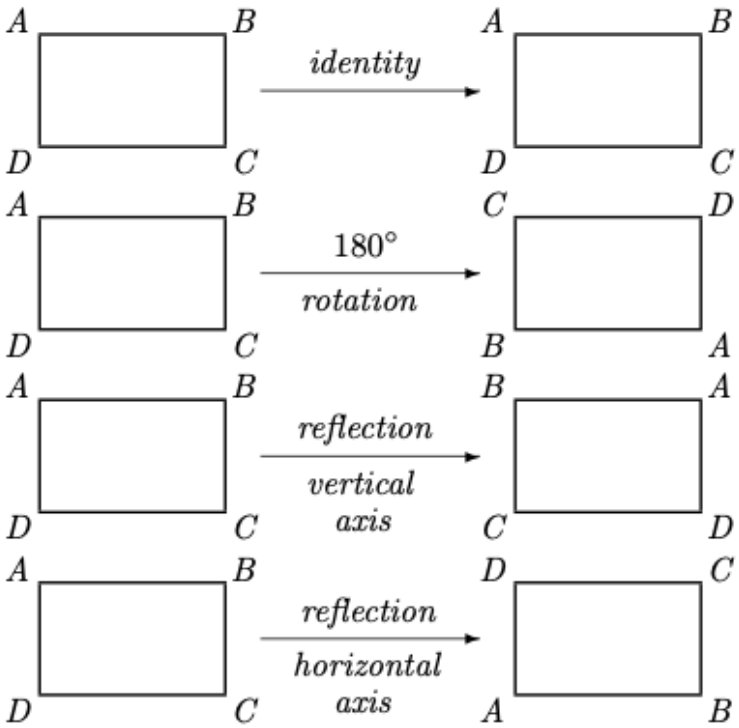
Se $d = mdc(a, n)$, então $d|ab$ e $d|nk$. Logo, $d = 1$

($\Leftarrow$) Se $mdc(a, n) = 1$, então existem $\alpha, \beta \in \mathbb{Z}$ tais que $\alpha a + \beta n = 1$ (lema de Bézout). Assim, $\alpha a = 1 \ (mod \ n)$. Logo, tomando $b \in \mathbb{Z}_n$ tal que $b = \alpha \ (mod \ n)$, temos que

$$ab \ (mod \ n) = a\alpha \ (mod \ n) = 1 \ (mod \ n)$$

Simetrias

Uma simetria de um objeto geométrico é um movimento rígido sobre o objeto, ou seja, um movimento que não o deforma e que preserva seu estado inicial (quando não levamos em consideração os rótulos do objeto). Tais movimentos são combinações (composições) de rotações e reflexões que preservam o objeto



Uma forma de analisar as simetrias de um objeto é olhar para todas as permutações entre os vértices do objeto, já que toda simetria preserva vertíces (dentre outras coisas)

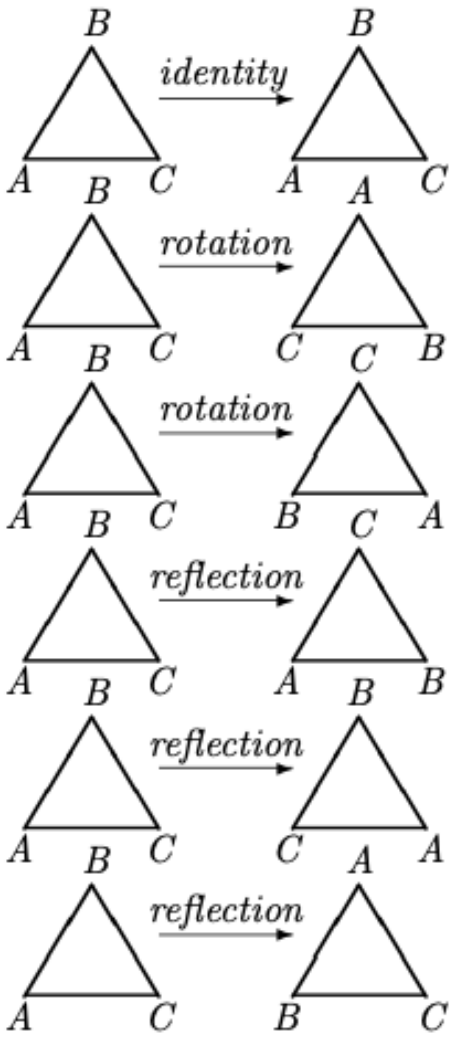
Exemplo: Num triangulo equilátero de vértices A,B,C temos $3! = 6$ permutações entre seus vértices (pq?). Logo, podemos ter no máximo 6 simetrias nesse triângulo

Uma permutação ρ_1 tal que $A \mapsto B$, $B \mapsto C$ e $C \mapsto A$ será denotada por

$$\rho_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

Note $\rho_1 =$ rotação de $120°$

Fato: Nesse caso, toda permutação corresponde a uma simetria



$$id = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

$$\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

$$\mu_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Pergunta: O mesmo vale se o triangulo não é equilátero?

Óbvio: composição de simetrias é simetria

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Note: $\rho_1\mu_1 \neq \mu_1\rho_1$

Além disso para toda simetria α existe uma simetria β tal que $\alpha\beta = id$

Grupos

Definição: Um grupo G é um conjunto munido de uma função (chamada operação binária, ou multiplicação, ou produto de G) $G \times G \to G$, $(a, b) \mapsto ab$ tal que, para quaisquer $a, b, c \in G$ temos:

- Associatividade: $(ab)c = a(bc)$
- Existencia do elemento identidade: $\exists e \in G$ tal que $ea = ae = a$
- Existencia do elemento inverso: $\exists a^{-1} \in G$ tal que $aa^{-1} = a^{-1}a = e$

Se $ab = ba$ para todos $a, b \in G$ dizemos que G é grupo abeliano. Nesse caso, usualmente denotamos ab por $a + b$, e por 0, a^{-1} por $-a$

A tabela de Cayley é a tabela de multiplicação de G

Cardinalidade de $G = |G|$ = ordem de G. Assim, G tem ordem finita se $|G| < \infty$

Exemplos

$(\mathbb{Z}, +)$ é grupo abeliano. Como $|\mathbb{Z}| = \infty$, $\mathbb{Z}$ tem ordem infinita

$(\mathbb{Z}_n, +)$ é grupo abeliano. Como $|\mathbb{Z}_n| = n$, $\mathbb{Z}_n$ tem ordem finita igual a n

Note: $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a, b) \mapsto ab$ (produto em $\mathbb{Z}$) é operação binária (associativa), mas $(\mathbb{Z}, \cdot)$ não é grupo (se $a \neq \pm 1$, então $a^{-1} \notin \mathbb{Z}$)

$(\mathbb{Z}_5, \cdot)$ é grupo abeliano. Prove e escreva a tabela de Cayley de $(\mathbb{Z}_5, \cdot)$

$(\mathbb{Z}_4, \cdot)$ não é grupo. Escreva a tabela de Cayley de $(\mathbb{Z}_4, \cdot)$ e veja quais elementos tem inversos e quais não tem

$U(n) = \{a \in \mathbb{Z}_n \mid mdc(a, n) = 1\}$ junto com a multiplicação é grupo abeliano

Se $D_3 = \{\text{simetrias de um triangulo equilátero}\}$, então $(D_3, \circ)$ é grupo não abeliano

O grupo geral linear $GL_n(\mathbb{R})$

$(GL_n(\mathbb{R}), \cdot)$ é grupo não ebeliano

- $G \times G \to G$, $(A, B) \mapsto AB$ é bem definida pois $\det AB = \det A \det B$
- Associatividade segue da associatividade do produto de matrizes
- Elemento identidade é a matriz identidade $I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$
- $A \in GL_n(\mathbb{R}) \Leftrightarrow \det A \neq 0 \Leftrightarrow \det A^{-1} = 1/\det A \neq 0 \Leftrightarrow A^{-1} \in GL_n(\mathbb{R})$

O grupo quaternion

Seja $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\} \subseteq GL_2(\mathbb{C})$, onde

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$(Q_8, \cdot)$ é grupo, pois $I^2 = J^2 = K^2 = -1$, $IJ = K$, $JK = I$, $KI = J$, $JI = -K$, $KJ = -I$ e $IK = -J$

$(Q_8, \cdot)$ é o grupo dos quaternions

Propriedades básicas de grupos

Proposição: Seja $(G, \cdot)$ um grupo e $a, b \in G$ quaisquer

1. O elemento identidade $e \in G$ é único
2. O inverso a^{-1} é único
3. $(ab)^{-1} = b^{-1}a^{-1}$
4. $(a^{-1})^{-1} = a$ (exercicio)

Prova (1): Se e, e' são duas identidades em G, então

$$ee' = e, \quad ee' = e' \Rightarrow e = ee' = e'$$

(2): se b e c são inversos de a, então

$$ab = bc = e, \quad ac = ca = e \Rightarrow b = eb = (ca)b = c(ab) = ce = c$$

(3): $ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Segue análogo que $(b^{-1}a^{-1})ab = e$ ■

Equações em G

Proposição: Seja $(G, \cdot)$ um grupo, $a, b, c \in G$ quaisquer e x uma incógnita

1. As equações $ax = b$ e $xa = b$ possuem única solução em G
2. $ba = ca \Rightarrow b = c$ e $ab = ac \Rightarrow b = c$ ($\Rightarrow$ regras de cancelação valem em G)

Prova (1): $a(a^{-1}b) = b \Rightarrow$ tal solução existe. Se x, y são tais que $ax = b$ e $ay = b$, então

$$ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay) \Rightarrow x = y$$

Prove a segunda parte

(2): $ba = ca \Rightarrow (ba)a^{-1} = (ca)a^{-1} \Rightarrow b = c$. Prove a segunda parte ■

Exponenciação em G

Para $g \in G$, defina

$$g^n = \underbrace{gg\cdots g}_{n \text{ vezes}}, \quad g^{-n} = \underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{n \text{ vezes}}$$

Proposição: Para $m, n \in Z$ e $g, h \in G$ o seguinte vale

1. $g^m g^n = g^{m+n}$
2. $(g^m)^n = g^{mn}$
3. $(gh)^n = (h^{-1}g^{-1})^{-n}$
4. Se G for abeliano, então $(gh)^n = g^n h^n$

Prova (3):

$$(h^{-1}g^{-1})^{-n} = \underbrace{(h^{-1}g^{-1})^{-1}(h^{-1}g^{-1})^{-1}\cdots(h^{-1}g^{-1})^{-1}}_{n \text{ vezes}}$$

$$= \underbrace{(gh)(gh)\cdots(gh)}_{n \text{ vezes}} = (gh)^n$$

Se G é abeliano, temos

$$g^n = \underbrace{g + g + \cdots + g}_{n \text{ vezes}}, \quad g^{-n} = \underbrace{(-g) + (-g) + \cdots + (-g)}_{n \text{ vezes}}$$

e fica mais natural escrevermos ng ao vez de g^n para todo $n \in \mathbb{Z}$

Nesse caso, as propriedades da proposição anterior se escrevem como:

1. $mg + ng = (m + n)g$
2. $n(mg) = (mn)g$
3. $m(g + h) = mg + mh$

Subgrupos

Um subgrupo de um grupo $(G, \cdot)$ é um subconjunto $H \subset G$ tal que $(H, \cdot)$ é um grupo (Importante: H é grupo com a mesma operação binária de G). Denotamos

$$H \leq G$$

Um subgrupo $H \leq G$ é próprio se $H \neq G$.

Exemplos:

- $(2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}, +)$ é um subgrupo de $(\mathbb{Z}, +)$
- $(\{e\}, \cdot)$, $(G, \cdot)$ são subgrupos de G. O subgrupo $\{e\}$ é chamado subgrupo trivial
- $(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \cdot)$ é subgrupo de $(\mathbb{R}^* = \mathbb{R} \setminus \{0\}, \cdot)$
  - $(p/q)(r/s) = pr/qs \Rightarrow$ função binária bem definida
  - Associatividade de $\cdot$ em $\mathbb{Q}^*$ vem da associatividade de $\cdot$ em $\mathbb{R}^*$
  - $1 = 1/1 \in \mathbb{Q}^*$
  - $(p/q)^{-1} = q/p \in \mathbb{Q}^*$

• $SL_n(\mathbb{R}) = \{g \in GL_n(\mathbb{R}) \mid \det g = 1\}$ é subgrupo de $GL_n(\mathbb{R})$ (lembre que $\det gh = \det g \det h$). Tal grupo é chamado de grupo especial linear

Note: Um subconjunto de um grupo G pode ser um grupo sem ser um subgrupo de G.

• $(M_n(\mathbb{R}), +)$ é um grupo (cheque!), $GL_n(\mathbb{R}) \subset M_n(\mathbb{R})$ mas $GL_n(\mathbb{R})$ não é um subgrupo de $M_n(\mathbb{R})$: Se $g \in GL_n(\mathbb{R})$, então $-g \in GL_n(\mathbb{R})$, mas $g + (-g) = 0 \notin GL_n(\mathbb{R}) \Rightarrow$ a operação binária de $M_n(\mathbb{R})$ não define uma operação binária em $GL_n(\mathbb{R})$

• Considere $\mathbb{Z}_2 \times \mathbb{Z}_2$ com a operação

$$(a, b) + (c, d) = (a + c, b + d)$$

Esse grupo tem 4 elementos: $(0, 0), (1, 0), (0, 1), (1, 1)$ e portanto de ordem 4

Note: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ também é um grupo de ordem 4

Pergunta: seria possível esses dois grupos serem simplesmete duas formas diferentes de representarmos um mesmo grupo? (lembrem: já vimos esse tipo de coisa acontecer no caso de simetrias de um triangulo equilátero e permutações de seus vértices)

Fato: Se dois grupos são iguais, então a estrutura de subgrupos desses dois grupos deve coincidir

Observe: $\mathbb{Z}_4$ só possui um subgrupo próprio não trivial: $H = \{0, 2\}$

Por outro lado $\mathbb{Z}_2 \times \mathbb{Z}_2$ possui tres subgrupos próprios não triviais:

$$H_1 = \{(0,0),(0,1)\}, \quad H_2 = \{(0,0),(1,0)\}, \quad H_3 = \{(0,0),(1,1)\}$$

Propriedades básicas de subgrupos

Proposição: Um subconjunto H é um subgrupo de G se e somente se as condições abaixo valem:

1. a identidade e de G pertence a H
2. Se $h_1, h_2 \in H$, então $h_1 h_2 \in H$
3. Se $h \in H$, então $h^{-1} \in H$

Prova ($\Rightarrow$) (1): Seja $e_H \in H$ a identidade de H. Afirmação: $e_H = e$

$$e_H e_H = e_H, \quad e e_H = e_H \Rightarrow e_H e_H = e e_H \Rightarrow e_H = e$$

(2): Óbvio

(3): Se $h' \in H$ é tal que $hh' = e$, então segue da unicidade do elemento inverso em G que $h' = h^{-1}$

($\Leftarrow$) Óbvio ■

Proposição: Um subconjunto H é um subgrupo de G se e somente se $H \neq \emptyset$ e $\forall g, h \in H$ temos que $gh^{-1} \in H$

Prova ($\Leftarrow$) $\exists g \in H$ e portanto $gg^{-1} = e \in H$. Se $h \in H$, então $eh^{-1} = h^{-1} \in H$. Por fim, se $g, h \in H$, então $g, h^{-1} \in H$ e assim $g(h^{-1})^{-1} = gh \in H$

($\Rightarrow$) Óbvio ■