

# Grupos Abelianos: definição e exemplos, subgrupos

ordem de um grupo e de um elemento

Grupo: é um  $\mathcal{G}$  é um conjunto com uma operação ( $\circ, +, \star, \dots$ )

Exemplo 1,  $T = \{1, 2, 3\}$ , a permutação de  $f$  cuja regras são:  $f(1)=2$ ,  $f(2)=3$  e  $f(3)=1$ .

Multiplicando vetores:  $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$

Fazendo outras permutações

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \xrightarrow{P_1} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \xrightarrow{P_2} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \xrightarrow{P_3}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \xrightarrow{P_4} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \xrightarrow{P_5} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Se  $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$  e  $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ , então  $fog$  é a função dada por:

$$\begin{aligned} (fog)(1) &= f(g(1)) = f(2) = 2 \\ (fog)(2) &= f(g(2)) = f(1) = 3 \\ (fog)(3) &= f(g(3)) = f(3) = 1 \end{aligned} \quad \left\{ \begin{array}{l} fog = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ \text{fog} \in T \end{array} \right.$$

Alô o conjunto das permutações de  $T$  é dado por  $S_3$ , então a composição de funções ( $\circ$ ) é uma operação sobre o conjunto  $S_3$  com esta propriedade.

Se  $f \in S_3$  e  $g \in S_3 \rightarrow fog \in S_3$

A composição de funções é associativa, temos:

$$(fog) \circ h = f \circ (goh), \forall f, g, h \in S_3$$

A identidade da permutação:  $I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$  tem esta propriedade:

$$I \circ f = f \text{ e } f \circ I = f, \text{ para cada } f \in S_3$$

Cada bijeção tem uma função inversa, consequentemente se  $f \in S_3$ , então existe  $g \in S_3$ , sendo que:

$$fog = I \text{ e } gof = I$$

Se  $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ , então  $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ , porque

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Por se tratar de matrizes  $fog$  não é necessariamente igual a  $gof$ .

Temos com isso a definição: Um grupo é um conjunto não vazio  $\mathcal{S}$  equipado com uma operação binária  $*$  que satisfaça os seguintes axiomas:

1) Fechado: Se  $a \in \mathcal{S}$  e  $b \in \mathcal{S}$ , então  $a * b \in \mathcal{S}$ ,

2) Associativa:  $a * (b * c) = (a * b) * c$ , para todo  $a, b, c \in G$ .

3) Existe um elemento  $e \in G$  (chamado de elemento identidade) que:  $a * e = a = e * a$ , para cada  $a \in G$ .

4) Para cada  $a \in G$ , existe um elemento  $d \in G$  (chamado de inverso de  $\underline{a}$ ) sendo que:

$$a * d = e \text{ e } d * a = e$$

Um grupo é dito abeliano se além das 4 axiomas anteriores, satisfizer também:

5) Comutatividade:  $a * b = b * a \forall a, b \in G$

Um grupo  $G$  é dito ser finita ou de ordem finita se ele tem um número finito de elementos. Neste caso, o numero de elementos em  $G$  é chamado de Ordem de  $G$  e é denotado por  $|G|$ . Um grupo com uma infinidade de elementos tem ordem infinita.

Exemplo 2: De acordo com a definição temos que  $\mathbb{Z}_3$  não é um grupo abeliano, pelas propriedades de matriz:

$$A * B \neq B * A$$

Exemplo 3: As permutações do grupo  $\mathbb{Z}_3$  é estritamente um caso especial de uma situação mais geral.

Tomamos  $n$  elementos e seja a fixado como um inteiro positivo e seja  $T$  o conjunto.

$$T = \{1, 2, 3, \dots, n\}, a \in \mathbb{Z}^+$$

Aja  $S_n$  o conjunto de todas permutações de  $T$  (isto é, todas as bijeções  $T \rightarrow T$ ). Usamos aqui o mesmo critério de  $S_3$ .

$$S_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 3 & 5 & 1 \end{pmatrix}$$

Se a composição de duas funções bijetivas é bijetiva, temos que  $S_n$  é fechado dentro da operação de composição. Por exemplo, em  $S_6$ :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 4 & 1 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 2 & 1 & 3 \end{pmatrix}$$

A composição de função é dada por:

$$f \circ g(1) = f(g(1)) = f(6) = 6$$

Temos que  $S_n$  é um grupo dentro da operação. A composição de funções é conhecida por ser associativa, e cada bijeção tem uma função inversa dentro da composição.

É fácil verificar a identidade da permutação:

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$  é o elemento identidade de  $S_N$ .

$S_N$  é chamado de grupo simétrico sobre os  $N$  elementos, a ordem de  $S_N$  é  $N!$ .

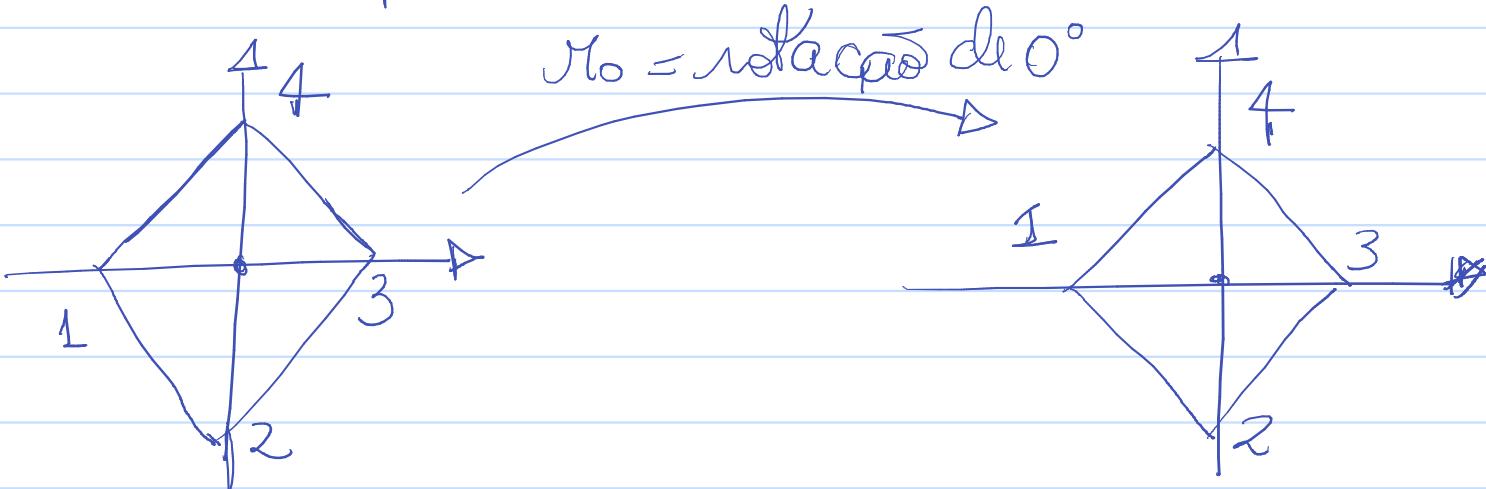
$$N! = N(N-1)(N-2) \dots 2 \cdot 1$$

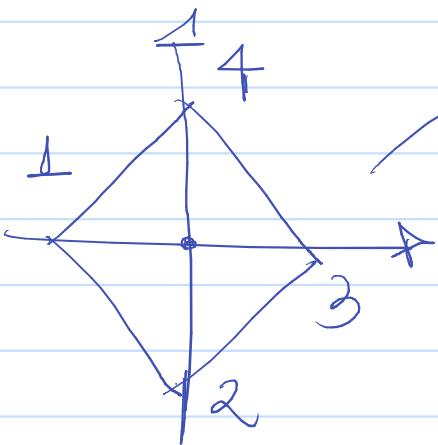
Exemplo 4: Tomamos  $T$  sendo qualquer conjunto não vazio, possivelmente infinito.

Tomamos  $f(T)$  sendo o conjunto de todas as permutações de  $T$  (todas as funções bijetivas  $T \rightarrow T$ ).

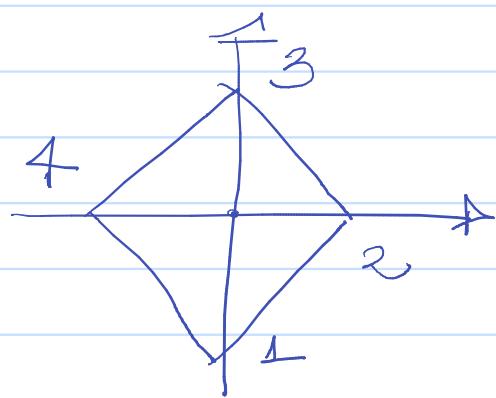
O argumento dado anteriormente para  $S_n$  corre pra para  $f(T)$  e mostra que  $f(T)$  é um grupo dentro da operação de composição de funções.

Exemplo 5: Imagine um plano, como uma superfície fina, e rígida. Neste plano temos um losango como abaixo:

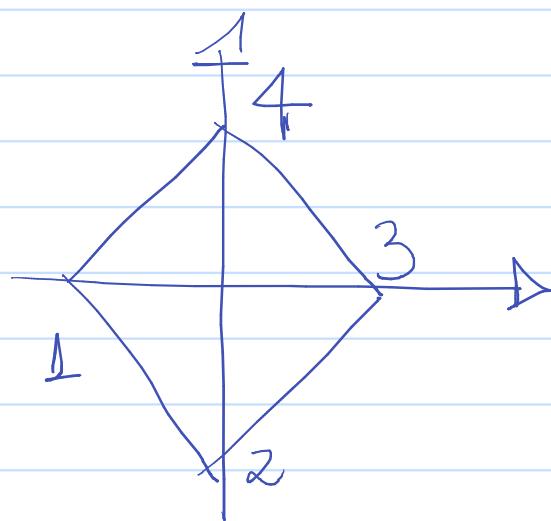




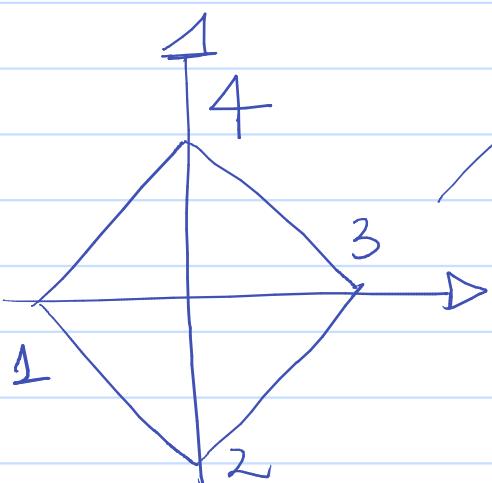
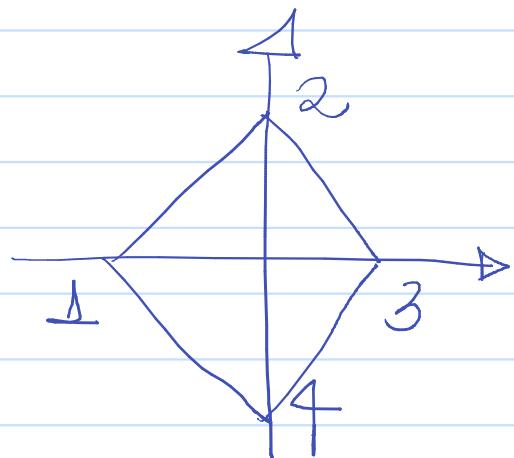
$\pi_1 = \text{rotacão de } 90^\circ$



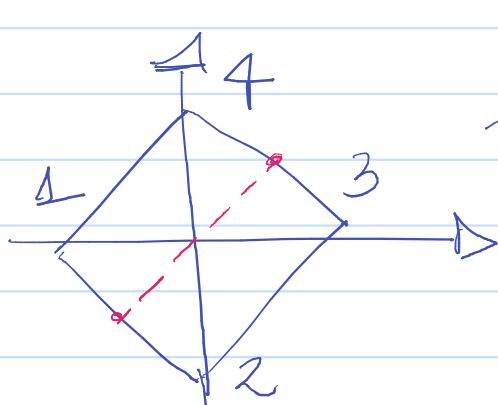
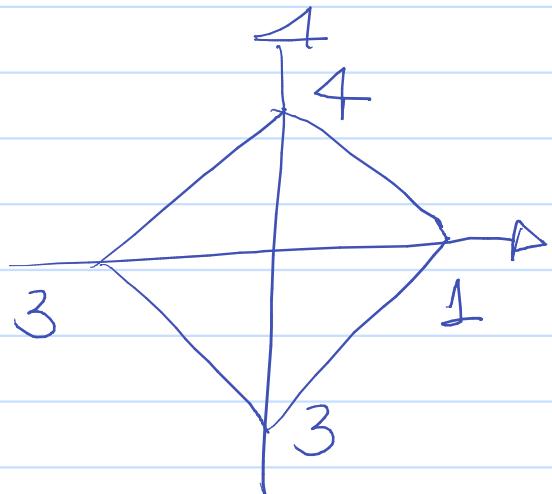
Pode-se rotacionar em  $0^\circ, 90^\circ, 180^\circ, 270^\circ$ . Como também reflexão em x e y.



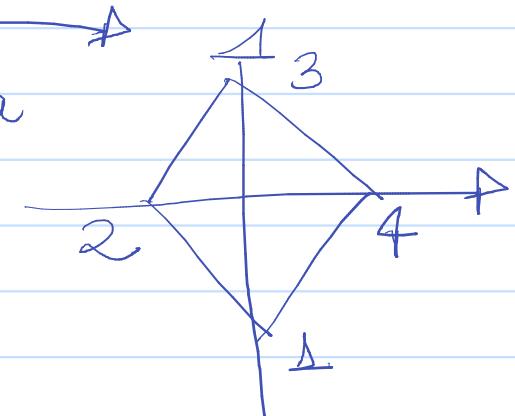
di: reflexão  
no eixo x

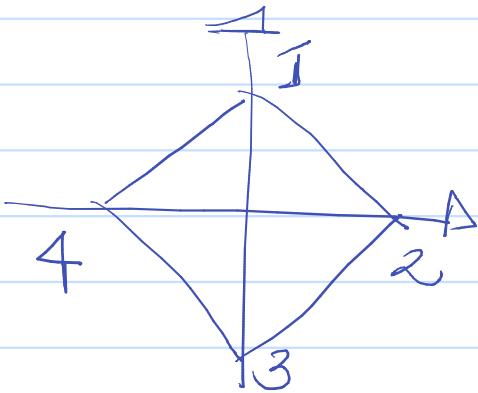
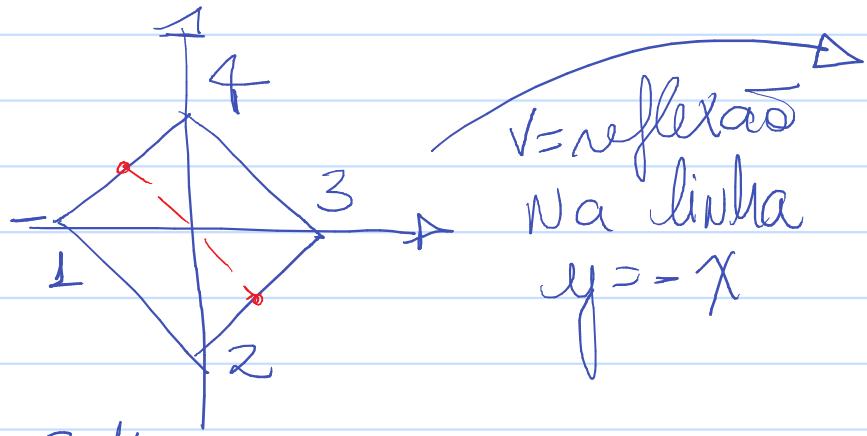


tr: reflexão  
no eixo y

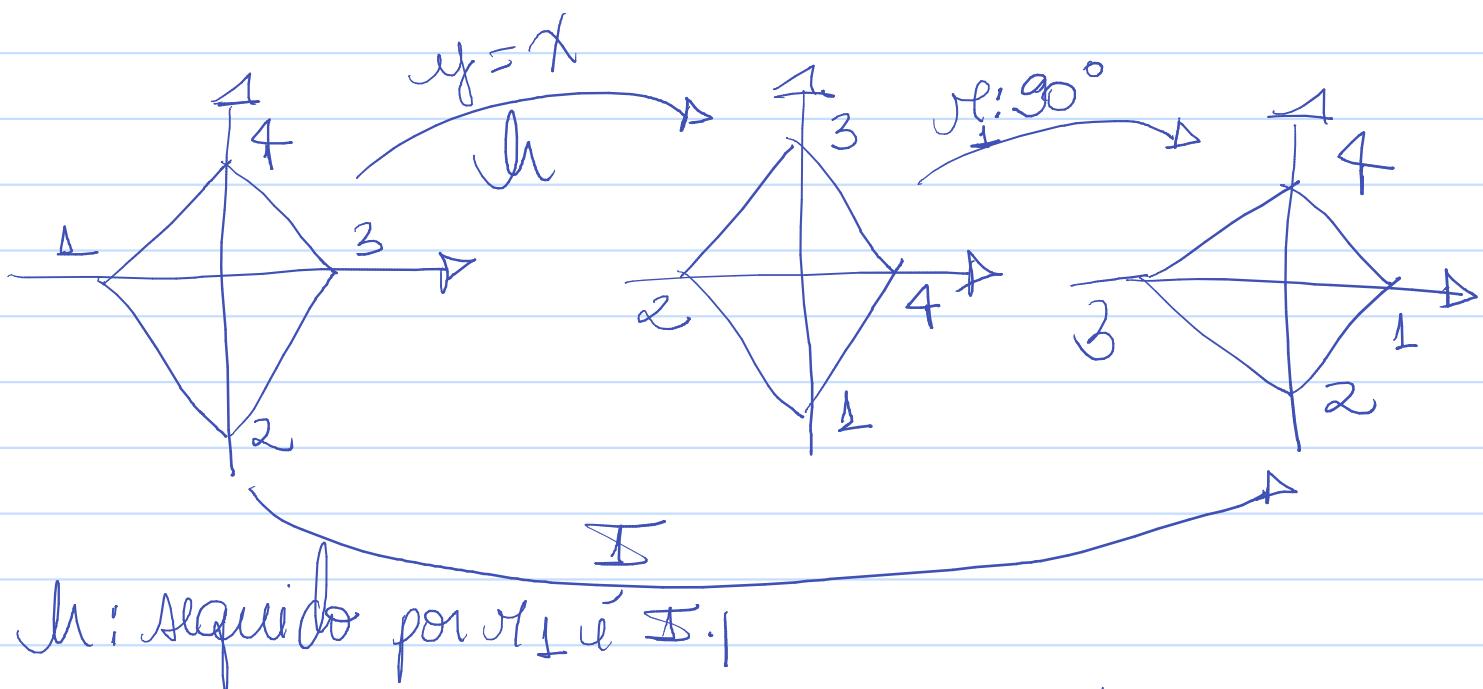


$\pi_1:$  reflexão na  
limha  $y=x$





Esfaz:



$r_1 \circ h = I \rightarrow r_1(h(1)) = r_1(h) = I$

## Grupos e Anéis

Em um anel  $R$  temos associadas duas operações, é natural perguntar se um anel  $R$  é um grupo dentro de outro grupo. Então a resposta é sim.

Teorema 7.1: Cada anel é um grupo abeliano por adição.

Prova: Os 5 axiomas que satisfazem um grupo abeliano também são válidos para anéis.

Com a operação de  $+$ , a identidade de elemento  
e elementos nulos, e o inverso de a sendo -a.

Exemplo: pelo Teorema 4.1, cada família  
sequinfe de anéis é um grupo abeliano por  
adição:

$$\mathbb{Z}, \mathbb{Z}_N, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

Matriz de anéis, sendo  $M(\mathbb{R})$  e  $M(\mathbb{Z}_2)$

Anéis Polinômiais sendo  $\mathbb{Z}[x]$ ,  $\mathbb{R}[x]$  e  $\mathbb{Z}_N[x]$

Daqui por diante, quando usamos a palavra  
"grupo" sem qual quer qualificação.  
Isto significa para estes ou outros anéis,  
isto é entendido que a operação é adição.

Para a multiplicação a história é diferente:

"Um anel  $R$  diferente de zero nunca é um  
grupo de multiplicação."

Anéis: é um conjunto não vazio  $A$  cuja  $R$  é  
chamado de Anel (ou Anel associativo) se em  
 $A$  estiverem definidas duas operações:

i) Adição,  $+: A \times A \rightarrow A$ , que associa a cada  
par de elementos  $(a, b) \in A \times A$  o elemento  
 $(a + b) \in A$ ,

ii) Multiplicação:  $A \times A \rightarrow A$ , que associa a cada par de elementos  $(a, b) \in A \times A$  o elemento  $(a \cdot b) \in A$ .

Que verifiquem as 7 propriedades das operações de adição e multiplicação dos números inteiros.

Então o anel é uma cópia de  $\mathbb{Z}$  para um  $A$  qualquer, e  $A$  não vazia.

Basta, faltas que para todo  $a, b, c \in A$ :

$$1) a+b = b+a$$

$$2) (a+b)+c = a+(b+c)$$

$$3) \exists 0_A \in A, \text{ tal que } a+0_A = a$$

$$4) \forall a \in A, \exists -a \in A, \text{ tal que } a + (-a) = 0_A$$

$$5) a \cdot (b+c) = a \cdot b + a \cdot c$$

6)

$$7) a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

Notações:  $(A, +, \cdot)$

Assim, dizemos que o anel  $A$  é comutativo, ou abeliano, se  $a \cdot b = b \cdot a, \forall a, b \in A$ .  
Definiremos por  $a - b = a + (-b)$

Exemplos de anéis:  $\mathbb{N} (\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$

$(M_N(\mathbb{R}), +, \cdot)$ ,  $(\mathbb{Z}, +, \cdot)$   $\rightarrow$  conjuntos dos números  $\rightarrow$  matrizes quadradas múltiplos de  $N$ .

O elemento  $0_A$  da propriedade 3 é chamado elemento nulo da adição e o elemento  $-a$  da propriedade 4 é chamado oposto ou simétrico de  $a$ .

Se existir em  $A$  um elemento  $1_A$ , que possui a propriedade de que  $1_A \cdot a = a$ ,  $\forall a \in A$ , esse elemento seja chamado unidade de  $A$ . Nesse caso dizemos que  $A$  é um anel com unidade ou unitário.

Dizemos que o anel  $A$  é comutativo, ou abeliano, se  $a \cdot b = b \cdot a \quad \forall a, b \in A$ .

Denotaremos por  $a - b = a + (-b)$ .

Exemplo:

$$\begin{array}{l} 1) (\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{M}_n(\mathbb{R}), +, \cdot) \\ (\mathbb{N} \setminus \{1\}, +, \cdot) \end{array}$$

Equivalência módulo  $N$ : dado um sistema  $\mathbb{N} \setminus \{2\}$ , dizemos que dois números inteiros  $a$  e  $b$  são equivalentes módulo  $N$ , o que será denotado por  $a \equiv b \pmod{N}$ , se  $|a - b|$  for múltiplo de  $N$ .

Ex:  $11 \equiv 5 \pmod{3}$ , pois  $11 - 5 = 6 = 2 \cdot 3$

11 é congruente a 5, mod 3.

Dado um inteiro  $\frac{N}{2}$  e um inteiro  $a$  qualquer, vamos chamar de classe de resto

Equivalecia de a módulos ou conjunto  $\bar{a}$  de todos os inteiros que são equivalentes a a módulo  $n$ , ou seja,  $\bar{a} = \{x \in \mathbb{Z}, x \equiv a \pmod{n}\}$ .

Denotemos por  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$  ao conjunto das classes de equivalência módulo  $n$ .

Ex.:

a)  $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ , equivalência módulo 2.

b)  $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ , equivalência módulo 3.

Em  $\mathbb{Z}_n$  definimos as seguintes operações:

$$\text{i)} \bar{a} + \bar{b} = \overline{a+b}$$

$$\text{ii)} \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Deste modo,  $(\mathbb{Z}_n, +, \cdot)$  é um anel.

E: Note que, com as operações anteriores, podemos identificar os anéis  $\mathbb{Z}_2$  e  $\mathbb{Z}_3$ .

Definição: seja  $A$  um anel.

i) Um elemento  $a \in A$  é um divisor de zero, se:

$$1) a \neq 0$$

2) Existe  $b \in A, b \neq 0$ , tal que  $a \cdot b = 0$ .

Ocorre muito em matrizes.

ii) Dizemos que  $A$  é sem divisores de zero quando:

$$a \cdot b = 0 \rightarrow a = 0 \text{ ou } b = 0$$

iii)  $A$  será chamado Anel de integridade se for: comutativo, unitário, e sem divisores de zero.

Anel de integridade = domínio de integridade

Ex: 1)  $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$  são todos anéis de integridade,

2)  $(M_N(\mathbb{R}), +, \cdot)$  é um anel com unidade (e não abeliano.)

3) Seja  $A = \mathbb{Z}_2$ , com as operações usuais de soma e multiplicação de números inteiros, então  $(A, +, \cdot)$  é um anel abeliano e sem unidade.

Os conjuntos dos números pares:  $\mathbb{Z}_2$

é abeliano: Ex:  $2 \cdot 8 = 8 \cdot 2$ ; sem comutativo

sem unidade: Não existe um par tal que quando ele multiplicado por ele permaneça igual.

Seja  $A$  um anel, valem as seguintes propriedades:

1) 0 zero de  $A$  é ímpar.

2) Dado  $a \in A$ , o simétrico de  $a$  é ímpar.

3)  $a \cdot 0 = 0 \cdot a = 0$ ,  $\forall a \in A$ .

$$4) a+b = a+c \Leftrightarrow b=c$$

$$5) b=c \rightarrow a.b = a.c \wedge b.a = c.a, \forall a \in A$$

$$6) -(a) = a, \forall a \in A$$

$$7) -(a.b) = (-a).b = a.(-b), \forall a, b \in A$$

$$8) (-a).(-b) = ab, \forall a, b \in A$$

$$9) a.(b-c) = ab - ac, \forall a, b, c \in A.$$

$$10) (a-b).c = a.c - b.c, \forall a, b, c \in A$$

$$11) -(a+b) = -a - b, \forall a, b \in A$$

Exemplo: Mostre a propriedade 3 anterior.

Proposição: Se  $(A, +, \cdot)$  é um anel, então,  $\forall 0, a \in A$ , qualquer que seja o elemento  $a \in A$ .

$$\text{① Dm: } 0.a = (0+0).a = 0.a + 0.a$$

Como  $0, a \in A$ , pela propriedade 4, existe  $-0, a \in A$  s.t. somando em ambos os lados da igualdade anterior, temos:

$$-(0.a) + 0.a = -(0.a) + (0.a + 0.a), \text{ ou}\\ \text{seja:}$$

$$0 = (-0.a) + 0.a = 0.a$$

② Divisores do zero em um anel: em todo anel  $(A, +, \cdot)$  existe um elemento chamado zero do anel. É o elemento neutro da primeira operação, que sempre existe!

Definição: Seja um anel  $(A, +, \cdot)$  e sejam  $a, b, c \in A$ .

elementos não nulos, faz que  $a \cdot b = 0$ .  
Diz-se então que  $a$  e  $b$ , são divisões  
próprias de zero.

Este zero não é um número ímpar zero  
do anel.

Ex: Os Números reais não admite divisor  
de zero.

Dem: Ao multiplicar dois Números diferentes  
de zero, sempre teremos um número  
diferente de zero.

2) O anel  $\mathbb{Z}_6$  admite 3 divisões de zero:

$$2 \times 3 = 6 \rightarrow \mathbb{Z}_6: 6 - 6 = 0$$

$$1 \times 6 = 6 \rightarrow \mathbb{Z}_6: 6 - 6 = 0$$

~~$$3 \times 2 = 6 \rightarrow \mathbb{Z}_6: 6 - 6 = 0$$~~

$$3 \times 4 = 12 \rightarrow \mathbb{Z}_6: 12 \equiv 0 \pmod{2}$$

Grupo Abeliano:  $(G, *)$ , s.t  $a \cdot b = b \cdot a$ ,  $\forall a, b \in G$ .

$(ab)^{-1} = b^{-1}a^{-1}$ ; que é finito se possuir finitos elementos;

$|G| = N$ . A ordem de  $G$  é finita ou  $n$ .

$|G| = \infty$ , possui ordem infinita

$(\mathbb{Z}_n, +)$  é um grupo aditivo.  
 $\mathbb{Z}_n = \{0, 1, \dots, n-1\} \rightarrow |\mathbb{Z}_n| = n$

$(\mathbb{Q}^*, \cdot)$  é grupo multiplicativo diferente de  
zero

Se  $A$  ou  $R$  não têm identidade, o axioma 3 falha.

Axioma 3: Existe um elemento  $e \in S$  (chamado identidade do elemento) sendo que  $a \cdot e = e \cdot a = a$  para cada  $a \in S$ .

Se  $A$  ou  $R$  têm identidade, então  $O_A$  não têm inverso e o axioma 4 falha.

Axioma 4: Para cada  $a \in S$ , existe um elemento de  $S$  chamado inverso de  $a$  sendo que:

$$a \cdot d = \emptyset \text{ e } d \cdot a = e$$

Mesmo assim, certos subconjuntos de anéis com identidade podem ser grupos sob multiplicação.

Teorema 7.2: O elemento não-zero de um campo  $F$  forma um grupo abeliano sob multiplicação.

① Aqui em diante vamos denotar o conjunto não-zero de elementos da soma zero em um campo  $F$  por  $F^*$ .

Prova: Multiplicando em  $F^*$  satisfaz os seguintes axiomas: 6 e 11 (fechado), 7 (associativa), 10 (identidade), 12 (inverso), e 9 (comutativa).

Então  $F^*$  satisfaz grupo de axiomas de 1 a 5 e, portanto, é um grupo abeliano sob multiplicação.

Exemplo 8: O Teorema 7.2 apresenta que cada um dos seguintes é um grupo abeliano sob multiplicação:

$\mathbb{Q}^*$ : conjuntos dos racionais não zero

$\mathbb{R}^*$ :  $\cup$   $\cup$  reais  $\cup$   $\cup$

$\mathbb{C}^*$ :  $\cup$   $\cup$  complexo,  $\cup$   $\cup$

Exemplo 9: Se "p" é primo, então  $\mathbb{Z}_p$  é um conjunto, pelo Teorema 2.7 e 2.8.

Portanto,  $\mathbb{Z}_p^*$  é um grupo sob multiplicação pelo Teorema 7.2.

Exemplo 10: Os números racionais positivos  $\mathbb{Q}^{**}$  formam um grupo abeliano infinito sob multiplicação, porque o produto dos números positivos é positivo! O  $1$  é o elemento identidade, e o inverso de  $a$  é  $1/a$ .

Similarmente, os reais positivos  $\mathbb{R}^{**}$  formam um grupo abeliano sob multiplicação.

Exemplo 11: O subconjunto  $\{1, -1, i, -i\}$  dos números complexos forma um grupo abeliano de ordem 4 sob multiplicação.

Pode-se verificar facilmente ele é fechado, e  $1$  é o elemento identidade.

Desde que  $i(-i) = 1$ ,  $i$  e  $-i$  são inversos de cada um.  $1/-1$  é seu próprio inverso desde que  $(-1)(-1) = 1$ .

Consequentemente, operante a ordem 4.

