INE5403

FUNDAMENTOS DE MATEMÁTICA DISCRETA PARA A COMPUTAÇÃO

PROF. DANIEL S. FREITAS

UFSC - CTC - INE

7 - ESTRUTURAS ALGÉBRICAS

7.1) Operações Binárias

7.2) Semigrupos

7.3) Produtos e Quocientes de Semigrupos

7.4) Grupos

7.5) Produtos e Quocientes de Grupos

GRUPOS

- Tipo especial de monóide.
- Aplicações aonde ocorre simetria:
  - matemática, física, química, sociologia...
  - aplicações recentes: física de partículas e cubo de Rubik
- Veremos importante aplicação da teoria de grupos a códigos binários.

GRUPOS

- Um **grupo** $(G, *)$ é um monóide (identidade e) com a seguinte propriedade adicional:

  $$\forall a \in G, \ \ \exists a' \in G \ \ \text{tal que} \ \ a * a' = a' * a = e$$

- Logo: grupo = conjunto G + operação binária sobre G tal que:

  1) $(a * b) * c = a * (b * c) \ \ \forall a, b, c \in G$

  2) existe um único elemento em G tal que:

     $a * e = e * a, \ \ \forall a \in G$

  3) $\forall a \in G, \ \ \exists a' \in G$, chamada de **inversa** de a tal que:

     $a * a' = a' * a = e$

GRUPOS

- Note que $*$ é uma operação binária sobre G, ou seja:

  $$a * b \ \in \ G, \quad \forall a, b \in G$$

- Para simplificar notação:
  - escreveremos $a * b$ como ab
  - vamos nos referir a $(G, *)$ simplesmente como G

- Um grupo G é dito **abeliano** se $ab = ba, \ \forall a, b \in G$

GRUPOS

- **Exemplo 1:** O conjunto dos inteiros $\mathbb{Z}$, com a operação de adição simples, é um grupo abeliano.
  - Se $a \in \mathbb{Z}$, a inversa de a é o seu negativo $-a$.

- **Exemplo 2:** O conjunto $\mathbb{Z}^+$, sob a operação de multiplicação simples, não é um grupo:
  - o elemento 2 em $\mathbb{Z}^+$ não tem inversa
  - no entanto, este conjunto com a operação formam um monóide

- **Exemplo 3:** O conjunto dos reais não nulos, sob a operação de multiplicação simples, é um grupo.
  - A inversa de $a \neq 0$ é $1/a$

Grupos

- **Exemplo 4:** $(G, *)$, aonde G é o conjunto dos reais não-nulos e $a * b = (ab)/2$ é um grupo abeliano.
  - $*$ é uma operação binária:

    $a * b (= ab/2)$ é um real não-nulo e, portanto, está em G
  - $*$ é uma operação associativa, pois:

    $(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{(ab)c}{4}$

    $a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a(bc)}{4} = \frac{(ab)c}{4}$
  - o número 2 é a identidade em G, pois:

    $a * 2 = \frac{(a)(2)}{2} = a = \frac{(2)(a)}{2} = 2 * a$
  - $a \in G$ tem uma inversa dada por $a' = 4/a$, pois:

    $a * a' = a * \frac{4}{a} = \frac{a(4/a)}{2} = 2 = \frac{(4/a)(a)}{2} = \frac{4}{a} * a = a' * a$
  - G é um grupo abeliano: $\forall a, b \in G, \quad a * b = b * a$ $\square$

PROPRIEDADES DOS GRUPOS

- **Teorema 1:** Todo elemento a em um grupo G tem apenas uma inversa em G.
- **Prova:**
  - Sejam a' e a'' ambas inversas de a.
  - Então: $a'(aa'') = a'e = a'$

    e: $(a'a)a'' = ea'' = a''$
  - Portanto, por associatividade: $a' = a''$ $\square$

- Denotaremos a inversa de a por a^{-1}.
  - Portanto, em um grupo G temos:

    $aa^{-1} = a^{-1}a = e$

Propriedades dos Grupos

- **Teorema 2:** Sejam a, b e c elementos de um grupo G. Então:

  (a) $ab = ac \quad \Rightarrow \quad b = c$ **(cancelamento à esquerda)**

  (b) $ba = ca \quad \Rightarrow \quad b = c$ **(cancelamento à direita)**

- **Prova de (a):**
  - Suponha que: $ab = ac$
  - Multiplicando os dois lados à esquerda por a^{-1}:

$$a^{-1}(ab) = a^{-1}(ac)$$

$$(a^{-1}a)b = (a^{-1}a)c \quad \text{(por associatividade)}$$

$$eb = ec \quad \text{(pela definição de inversa)}$$

$$b = c \quad \text{(pela definição de identidade)} \qquad \square$$

- **Prova de (b):** similar.

Propriedades dos Grupos

- **Teorema 3:** Sejam a e b elementos de um grupo G. Então:
  (a) $(a^{-1})^{-1} = a$
  (b) $(ab)^{-1} = b^{-1}a^{-1}$

- **Prova de (a):**
  - Temos: $aa^{-1} = a^{-1}a = e$
  - Como a inversa é única, concluímos que: $(a^{-1})^{-1} = a$.

- **Prova de (b):**
  - $(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) =$
    $= a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$
  - e também: $(b^{-1}a^{-1})(ab) = e$
  - de modo que: $(ab)^{-1} = b^{-1}a^{-1}$ $\square$

PROPRIEDADES DOS GRUPOS

- **Teorema 4:** Sejam a e b elementos de um grupo G. Então:

  (a) A equação $ax = b$ tem uma solução única em G

  (b) A equação $ya = b$ tem uma solução única em G

- **Prova de (a):**
  - O elemento $x = a^{-1}b$ é uma solução da equação, pois:
    $a(a^{-1}b) = (aa^{-1})b = eb = b$
  - Agora suponha que existam duas soluções: x_1 e x_2.
  - Então: $ax_1 = b$ e $ax_2 = b$
  - Logo: $x_1 = x_2$ $\square$

- **Prova de (b):** Similar.

REPRESENTAÇÃO EM TABELAS

- Se um grupo G tem um nro finito de elementos, então a sua operação binária pode ser dada por uma tabela.
- A tabela de multiplicação de um grupo $G = \{a_1, a_2, \ldots, a_n\}$ sob a operação binária $*$ deve satisfazer às seguintes propriedades:
  - linha e coluna rotuladas por e devem conter todos os elementos: $a_1, a_2, \ldots, a_n$
  - pelo Teorema 4: cada elemento do grupo deve aparecer exatamente uma vez em cada linha e coluna da tabela
    - portanto, cada linha/coluna:
      - é uma permutação dos elementos de G
      - determina uma permutação diferente.

REPRESENTAÇÃO EM TABELAS

- **Nota**: se G é um grupo com um número finito de elementos:
  - G é denominado um **grupo finito**
  - a **ordem** de G é o número de elementos $|G|$ em G
- Vamos agora determinar as tabelas de multiplicação de todos os grupos de ordens 1, 2, 3 e 4...

Representação em tabelas

- Ordem 1: $G = \{e\}$
  - $ee = e$
- Ordem 2: $G = \{e, a\}$
  - tabela de multiplicação:

	e	a
e	e	a
a	a	?

  - o espaço em branco pode ser preenchido por e ou por a:
    - então, como não pode haver repetições:

	e	a
e	e	a
a	a	e

(satisfaz propriedades de grupo)

REPRESENTAÇÃO EM TABELAS

- Ordem 3: $G = \{e, a, b\}$
  - tabela de multiplicação:

	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

  - experimentando um pouco:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

  - pode-se provar que esta tabela satisfaz às propriedades de grupo (associatividade dá trabalho)

REPRESENTAÇÃO EM TABELAS

- Observe que:
  - os grupos de ordem 1, 2 e 3 são abelianos
  - existe apenas um grupo de cada ordem para uma dada rotulagem dos elementos

REPRESENTAÇÃO EM TABELAS

- Ordem 4: $G = \{e, a, b, c\}$
  - tabela de multiplicação pode ser completada de 4 modos:

	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c
e	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c
a	a	e	c	b	a	e	c	b	a	b	c	e	a	c	e	b
b	b	c	e	a	b	c	a	e	b	c	e	a	b	e	c	a
c	c	b	a	e	c	b	e	a	c	e	a	b	c	b	a	e

  - pode-se provar que cada uma destas tabelas satisfaz às propriedades de grupo
  - observe que um grupo de ordem 4 é abeliano
  - veremos que, na verdade, existem apenas 2 (e não 4) grupos diferentes de ordem 4...

EXEMPLOS DE GRUPOS

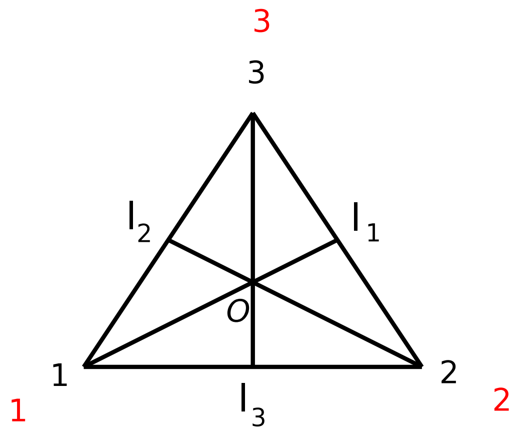
- **Exemplo 1:** Seja a operação $+$ sobre $B = \{0, 1\}$ definida como:

+	0	1
0	0	1
1	1	0

  - B é um grupo.
  - Neste grupo, cada elemento é a sua própria inversa. $\square$

EXEMPLOS DE GRUPOS

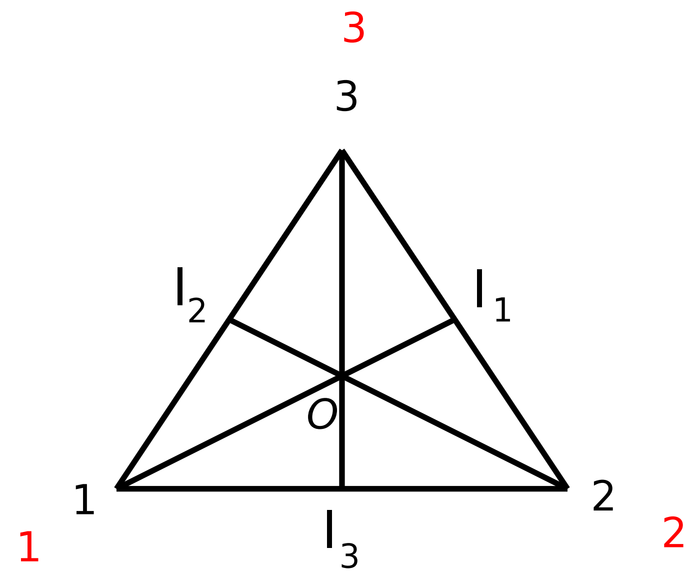
- **Exemplo 2 (1/7):** Considere o seguinte triângulo equilátero:



- **Nota:** Uma **simetria** de uma figura geométrica é uma bijeção do conjunto dos pontos que formam a figura para ele mesmo, preservando a distância entre pontos adjacentes.
- Simetria de um triângulo: permutação dos vértices.

EXEMPLOS DE GRUPOS

- **Exemplo 2 (2/7):** Simetrias do triângulo equilátero:



  - l_1, l_2 e l_3 são bissectores angulares dos respectivos ângulos
  - O é o seu ponto de intersecção
  - 1, 2 e 3 são referências fixas

Exemplos de grupos

- **Exemplo 2 (3/7):** Simetrias básicas do triângulo equilátero:

1) rotação anti-horária de 120^o em torno de O, dada pela permutação:

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

2) rotação anti-horária de 240^o, dada pela permutação:

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

3) rotação anti-horária de 360^o, dada pela permutação:

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

  - ou: rotação de 0^o em torno de O

EXEMPLOS DE GRUPOS

- **Exemplo 2 (4/7):** Também existem 3 simetrias adicionais:
  - Resultado da reflexão sobre l_1, l_2 e l_3, respectivamente:

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

- Observe que o conjunto de todas as simetrias do triângulo é igual ao conjunto S_3 das permutações do conjunto $\{1, 2, 3\}$:

$$\{\{1,2,3\},\{2,3,1\},\{3,1,2\},\{1,3,2\},\{3,2,1\},\{2,1,3\}\}$$

- Portanto: $S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}$

EXEMPLOS DE GRUPOS

- **Exemplo 2 (5/7):**

$$S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}$$
$$= \{\{1,2,3\},\{2,3,1\},\{3,1,2\},\{1,3,2\},\{3,2,1\},\{2,1,3\}\}$$

- A operação $*$, "seguido por", produz a seguinte tabela de multiplicação sobre S_3:

$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

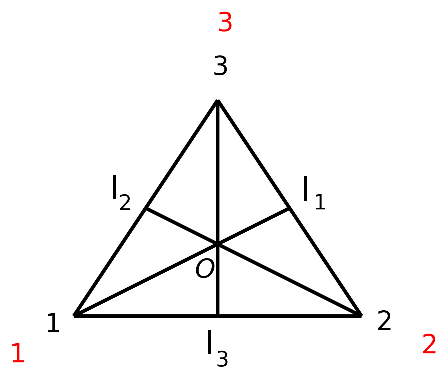
EXEMPLOS DE GRUPOS

- **Exemplo 2 (6/7):** Operação $*$ pode ser algébrica ou geométrica.

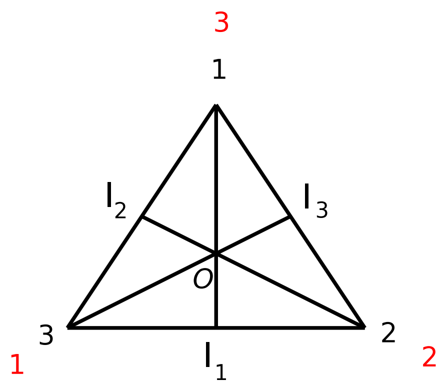
  - Computando $f_2 * g_2$ algebricamente $(* = \circ)$:

$$f_2 \circ g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = g_1$$

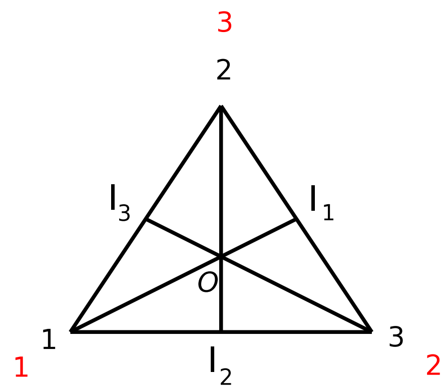
  - Computando $f_2 * g_2$ geometricamente $(* =$ seguido por):



inicial



após g_2



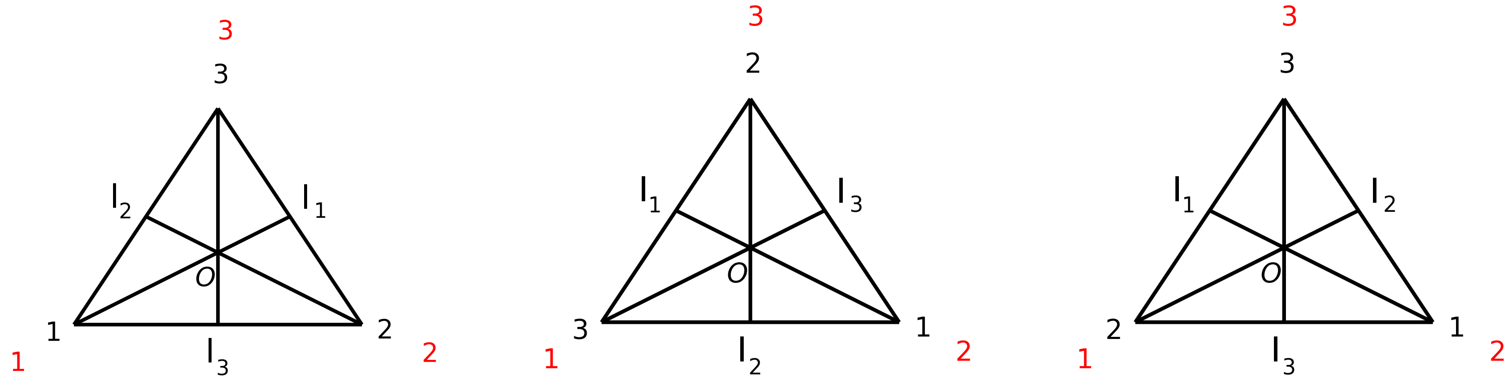
após $f_2 * g_2$

EXEMPLOS DE GRUPOS

- **Exemplo 2 (7/7):** Operação $*$ pode ser algébrica ou geométrica.
  - Computando $g_2 * f_2$ algebricamente ($* = \circ$):

$$g_2 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = g_3$$

  - Computando $g_2 * f_2$ geometricamente ($* =$ seguido por):



inicial — após f_2 — após $g_2 * f_2$

EXEMPLOS DE GRUPOS

- **Exemplo:** O conjunto de todas as permutações de n elementos sob a operação de composição:
  - grupo de ordem $n!$
  - denominado de **grupo simétrico sobre** n **letras**
  - denotado por S_n
  - S_3 coincide com o grupo de simetrias do triângulo equilátero
- **Nota**: também faz sentido considerar o grupo de simetrias de um quadrado.
  - Só que este grupo tem ordem 8.
  - Não coincide, portanto, com S_4, cuja ordem é $4! = 24$

EXEMPLOS DE GRUPOS

- **Exemplo:** O monóide $\mathbb{Z}_n$ (seção anterior) também é um grupo:
  - falta só provar que todo elemento de $\mathbb{Z}_n$ tem inversa:
    - seja $[a] \in \mathbb{Z}_n$
    - então: $0 \leq a < n$
    - por outro lado: $[n - a] \in \mathbb{Z}_n$
    - o que permite concluir:

      $$[a] \bigoplus [n - a] = [a + n - a] = [n] = [0]$$
    - ou seja: todo $[a]$ tem uma inversa dada por $[n - a]$
  - ex.: em $\mathbb{Z}_6$, $[2]$ é a inversa de $[4]$ $\square$

- Em seguida: subconjuntos de grupos que são importantes...

SUBGRUPOS

- Seja H um subconjunto de um grupo G tal que:

  (a) a identidade e de G pertence a H

  (b) se a e b pertencem a H, então $ab \in H$

  (c) se $a \in H$, então $a^{-1} \in H$

  Então H é chamado de **subgrupo** de G.

- **Nota 1**: subgrupo = subsemigrupo + (a) + (c)

- **Nota 2**: H também é um *grupo* com relação à operação de G, pois a associatividade de G também vale em H

Exemplos de subgrupos

- **Exemplo:** Seja G um grupo:
  - G e $H = \{e\}$ são subgrupos de G
  - são os chamados **subgrupos triviais** de G
- **Exemplo:** Considere S_3 (simetrias do triângulo equilátero), junto com a tabela de multiplicação dada.
  - $H = \{f_1, f_2, f_3\}$ é um subgrupo de S_3
- **Exemplo(!):** Seja A_n o conjunto de todas as permutações pares no grupo S_n.
  - A_n é um subgrupo de S_n
  - é o chamado **grupo alternante sobre n letras**

EXEMPLOS DE SUBGRUPOS

- **Exemplo:** Seja G um grupo e seja $a \in G$:
  - Como um grupo já é um monóide, já foi definido:

    $a^n = aa \cdots a$ (n fatores)

    aonde: $a^0 = e$
  - Agora vamos definir:

    $a^{-n} = a^{-1}a^{-1} \cdots a^{-1}$ (n fatores)
  - Segue que, $\forall n, m \in \mathbb{Z}$:

    $a^n a^m = a^{n+m}$
  - Com isto, é fácil mostrar que é um subgrupo de G:

    $H = \{a^i \mid i \in \mathbb{Z}\}$ $\square$
- A seguir: isomorfismos e homomorfismos em grupos...

Isomorfismos e Homomorfismos

- **Exemplo:**
  - Sejam:
    - G: grupo dos nros reais sob adição
    - G': grupo dos nros reais positivos sob multiplicação
  - Seja $f : G \rightarrow G'$ definida como: $f(x) = e^x$
  - f é um isomorfismo, pois:
    - é injetiva:
      $f(a) = f(b) \quad \Rightarrow \quad e^a = e^b \quad \Rightarrow \quad a = b$
    - é sobrejetiva:
      se $c \in G'$, então $\exists\, ln(c) \in G$ tal que: $f(ln(c)) = e^{ln(c)} = c$
    - as operações correspondem:
      $f(a+b) = e^{a+b} = e^a e^b = f(a)f(b)$ $\square$

- **Exemplo(!):**
  - Sejam:
    - G: grupo simétrico sobre n letras
    - G': grupo $B = (\{0, 1\}, +)$ (ex. anterior)
  - Então a $f : G \to G'$ definida por:

$$f(p) = \begin{cases} 0 & \text{se } p \in A_n \text{ (subgrupo das permutações pares em G)} \\ 1 & \text{se } p \notin A_n \end{cases}$$

é um homomorfismo. $\square$

- **Exemplo:**
  - Sejam:
    - G: inteiros sob adição
    - G': grupo $\mathbb{Z}_n$ (ex. anterior)
  - Seja a $f : G \to G'$ definida por:
    - se $m \in G$, então $f(m) = [r]$
      - aonde r é o resto quando m é dividido por n
  - Mostrar que f é um homomorfismo de G sobre G'.
  - Nota: quando $n = 2$, esta f atribui $[0]$ a todo inteiro par e $[1]$ a todo inteiro ímpar.

ISOMORFISMOS E HOMOMORFISMOS

- **Exemplo(cont.):**
  - f é sobrejetora, pois: $f(r) = [r]$
  - f é um homomorfismo:
    - sejam a e b elementos de G expressos como:
      - $a = q_1 n + r_1 \quad \Rightarrow \quad f(a) = [r_1]$
      - $b = q_2 n + r_2 \quad \Rightarrow \quad f(b) = [r_2]$

      $\Rightarrow \quad f(a) \bigoplus f(b) = [r_1] \bigoplus [r_2] = [r_1 + r_2]$
    - por outro lado:
      - $r_1 + r_2 = q_3 n + r_3 \quad \Rightarrow \quad f(a) \bigoplus f(b) = [r_3]$
    - somando a e b, temos:
      - $a + b \;=\; q_1 n + q_2 n + r_1 + r_2 \;=\; (q_1 + q_2 + q_3) n + r_3$

      $\Rightarrow \quad f(a+b) = [r_1 + r_2] = [r_3]$
    - portanto: $f(a+b) = f(a) \bigoplus f(b) \qquad \Box$

Homomorfismos em Grupos

- **Teorema:**
  - Sejam dois grupos $(G, *)$ e $(G', *')$ e:
    - $f : G \rightarrow G'$ um homomorfismo de G para G'
  - Daí:

    (a) se e é a identidade em G e e' em G' , então $f(e) = e'$

    (b) se $a \in G$, então $f(a^{-1}) = (f(a))^{-1}$

    (c) se H é um subgrupo de G, então:

    $f(H) = \{f(h) \mid h \in H\}$ é um subgrupo de G'.

- **Prova:** $\Rightarrow$

HOMOMORFISMOS EM GRUPOS

- **Prova da parte (a):**
  - Seja $x = f(e)$:

    $$x *' x = f(e) *' f(e) = f(e * e) = f(e) = x$$

  - Logo: $\quad x *' x = x$
  - Agora, multiplicando por x^{-1} à direita:

    $$x \;=\; x *' (x *' x^{-1}) \;=\; (x *' x) *' x^{-1} \;=\; x *' x^{-1} \;=\; e'$$

  - Ou seja: $\quad f(e) = e' \qquad \square$

HOMOMORFISMOS EM GRUPOS

- **Prova da parte (b):**
  - $a * a^{-1} = e$
  - De modo que:

    $$f(a * a^{-1}) = f(e) = e'$$

    $\Rightarrow \ f(a) *' f(a^{-1}) = e'$ (pois f é um homomorfismo)
  - Similarmente: $f(a^{-1}) *' f(a) = e'$
  - Logo: $f(a^{-1}) = (f(a))^{-1}$ $\square$

Homomorfismos em Grupos

- **Prova da parte (c):**
  - Segue de:
    - correspondência entre subsemigrupos sob um homomorfismo (teorema abaixo)
    - partes (a) e (b) $\square$

- ***Teorema (lembrete):***
  - Sejam:
    - f um homomorfismo de um semigrupo $(S, *)$ para um semigrupo $(T, *')$
    - S' um subsemigrupo de $(S, *)$.
  - Então: $f(S') = \{t \in T \mid t = f(s)$ para algum $s \in S'\}$

    é um subsemigrupo de $(T, *')$.

Homomorfismos em Grupos

- **Exemplo:** Os grupos S_3 e $\mathbb{Z}_6$ são ambos de ordem 6.
  - No entanto: S_3 não é abeliano e $\mathbb{Z}_6$ é abeliano.
  - Portanto: eles não são isomórficos. $\square$

ISOMORFISMOS E HOMOMORFISMOS

- **Exemplo(1/3):** Tabelas de multiplicação para grupo de ordem 4:

	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c
e	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c
a	a	e	c	b	a	e	c	b	a	b	c	e	a	c	e	b
b	b	c	e	a	b	c	a	e	b	c	e	a	b	e	c	a
c	c	b	a	e	c	b	e	a	c	e	a	b	c	b	a	e
	(1)				(2)				(3)				(4)			

- Grupos cujas tabelas sejam (2) e (3) são isomórficos:
  - seja $G = \{e, a, b, c\}$ o grupo cuja tabela é a (2)
  - seja $G' = \{e', a', b', c'\}$ o grupo cuja tabela é a (3)
  - seja $f : G \to G'$ dada por:

    $$f(e) = e' \qquad f(a) = b' \qquad f(b) = a' \qquad f(c) = c'$$

  - renomeando desta forma, as tabelas (2) e (3) ficam iguais

ISOMORFISMOS E HOMOMORFISMOS

- **Exemplo(2/3):** Tabelas de multiplicação para grupo de ordem 4:

	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c
e	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c
a	a	e	c	b	a	e	c	b	a	b	c	e	a	c	e	b
b	b	c	e	a	b	c	a	e	b	c	e	a	b	e	c	a
c	c	b	a	e	c	b	e	a	c	e	a	b	c	b	a	e
	(1)				(2)				(3)				(4)			

- Grupos cujas tabelas sejam (2) e (4) são isomórficos:
  - seja $G = \{e, a, b, c\}$ o grupo cuja tabela é a (2)
  - seja $G'' = \{e'', a'', b'', c''\}$ o grupo cuja tabela é a (4)
  - seja $g : G \to G''$ dada por:

    $$g(e) = e'' \qquad g(a) = c'' \qquad g(b) = b'' \qquad g(c) = a''$$

  - renomeando desta forma, as tabelas (2) e (4) ficam iguais

ISOMORFISMOS E HOMOMORFISMOS

- **Exemplo(3/3):** Tabelas de multiplicação para grupo de ordem 4:

	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c
e	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c
a	a	e	c	b	a	e	c	b	a	b	c	e	a	c	e	b
b	b	c	e	a	b	c	a	e	b	c	e	a	b	e	c	a
c	c	b	a	e	c	b	e	a	c	e	a	b	c	b	a	e

(1) (2) (3) (4)

- Conclusão: grupos das tabelas (2), (3) e (4) são isomórficos.
- Grupos das tabelas (1) e (2) não são isomórficos:
  - $\forall x$ na tabela (1), temos: $x^2 = e$
  - tabela (2) não apresenta esta propriedade
- De fato, existem exatamente 2 grupos não-isomórificos de ordem 4:
  - o grupo da tab. (1) é chamado de “grupo Klein 4” (denotado por V)
  - o grupo da tab. (2) é denotado por $\mathbb{Z}_4$:
    - re-rotulando os elementos de $\mathbb{Z}_4$ resulta nesta tabela. $\square$

GRUPOS

- Final deste item.
- **Dica**: fazer exercícios sobre Grupos...