

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

PRODUTOS E QUOCIENTES DE GRUPOS

- Recursos que permitem obter **novos grupos** a partir de **outros** já conhecidos.
- **Nota:** Um grupo tem mais estrutura do que um semigrupo:
 - resultados mais profundos do que os análogos para semigrupos

PRODUTOS E QUOCIENTES DE GRUPOS

- Recursos que permitem obter **novos grupos** a partir de **outros** já conhecidos.
- **Nota:** Um grupo tem mais estrutura do que um semigrupo:
 - resultados mais profundos do que os análogos para semigrupos
- **Teorema 1:** Se G_1 e G_2 são grupos, então $G = G_1 \times G_2$ é um grupo com uma operação definida por:

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$$

PRODUTOS E QUOCIENTES DE GRUPOS

● **Exemplo:** Sejam G_1 e G_2 o grupo \mathbb{Z}_2 .

● Nota: $\bar{0}$ e $\bar{1}$ em vez de $[0]$ e $[1]$

● Tabela de multiplicação de $G = G_1 \times G_2$:

	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

PRODUTOS E QUOCIENTES DE GRUPOS

● **Exemplo:** Sejam G_1 e G_2 o grupo \mathbb{Z}_2 .

● Nota: $\bar{0}$ e $\bar{1}$ em vez de $[0]$ e $[1]$

● Tabela de multiplicação de $G = G_1 \times G_2$:

	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

● G é um grupo de ordem 4 \Rightarrow deve ser isomórfico a V ou a \mathbb{Z}_4

PRODUTOS E QUOCIENTES DE GRUPOS

● **Exemplo:** Sejam G_1 e G_2 o grupo \mathbb{Z}_2 .

● Nota: $\bar{0}$ e $\bar{1}$ em vez de $[0]$ e $[1]$

● Tabela de multiplicação de $G = G_1 \times G_2$:

	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

● G é um grupo de ordem 4 \Rightarrow deve ser isomórfico a V ou a \mathbb{Z}_4

● Vemos (\Rightarrow) que o isomorfismo é a $f : V \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ dada por:

$$f(e) = (\bar{0}, \bar{0}) \quad f(a) = (\bar{1}, \bar{0}) \quad f(b) = (\bar{0}, \bar{1}) \quad f(c) = (\bar{1}, \bar{1})$$

□

(GRUPOS DE ORDEM 4)

● 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 das tabelas (2), (3) e (4) são **isomórficos**.

● De fato, existem **exatamente 2** grupos não-isomórficos 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.)

□

PRODUTOS E QUOCIENTES DE GRUPOS

- Se repetirmos o exemplo com \mathbb{Z}_2 e \mathbb{Z}_3 , concluiremos que:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$$

- Pode-se mostrar que, em geral:

$$\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn} \quad \text{se e somente se} \quad \text{GCD}(m, n) = 1$$

PRODUTOS E QUOCIENTES DE GRUPOS

- O Teorema 1 pode ser estendido para:

- Se G_1, G_2, \dots, G_n são grupos, então

$G = G_1 \times G_2 \times \dots \times G_n$ também é um grupo.

PRODUTOS E QUOCIENTES DE GRUPOS

- **Exemplo:** Seja $B = \{0, 1\}$ o grupo com operação (já) definida por:

+	0	1
0	0	1
1	1	0

- Então $B^n = B \times B \times \dots \times B$ é um grupo.

- Com operação \oplus definida por:

$$(x_1, x_2, \dots, x_n) \oplus (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

PRODUTOS E QUOCIENTES DE GRUPOS

- **Exemplo:** Seja $B = \{0, 1\}$ o grupo com operação (já) definida por:

+	0	1
0	0	1
1	1	0

- Então $B^n = B \times B \times \dots \times B$ é um grupo.

- Com operação \oplus definida por:

$$(x_1, x_2, \dots, x_n) \oplus (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

- A **identidade** de B^n é $(0, 0, \dots, 0)$.

- Cada elemento é a sua própria **inversa**.

- Este grupo é, essencialmente, o mesmo que a Álgebra Booleana B_n

- só que a operação binária é bem diferente de \wedge e \vee .

PRODUTOS E QUOCIENTES DE GRUPOS

- Sob uma **relação de congruência**, o grupo é visto como um semigrupo.
- A seguir, veremos **estruturas quocientes** determinadas por uma **relação de congruência** sobre um grupo.

PRODUTOS E QUOCIENTES DE GRUPOS

● Teorema 2:

- Seja R uma relação de congruência sobre o grupo $(G, *)$.
- Então o semigrupo $(G/R, \odot)$ **é um grupo**.
- onde: $[a] \odot [b] = [a * b]$

● Prova:

- G é um grupo $\Rightarrow G$ é um monóide $\Rightarrow G/R$ é um monóide
- Só falta provar que **cada elemento de G/R tem uma inversa**:

PRODUTOS E QUOCIENTES DE GRUPOS

● Teorema 2:

- Seja R uma relação de congruência sobre o grupo $(G, *)$.
- Então o semigrupo $(G/R, \odot)$ **é um grupo**.
- onde: $[a] \odot [b] = [a * b]$

● Prova:

- G é um grupo $\Rightarrow G$ é um monóide $\Rightarrow G/R$ é um monóide
- Só falta provar que **cada elemento de G/R tem uma inversa**:
 - como $[a] \in G/R$, então $[a^{-1}] \in G/R$ (pois $a^{-1} \in G$)
 - daí: $[a] \odot [a^{-1}] = [a * a^{-1}] = [e]$

PRODUTOS E QUOCIENTES DE GRUPOS

● Teorema 2:

- Seja R uma relação de congruência sobre o grupo $(G, *)$.
- Então o semigrupo $(G/R, \odot)$ **é um grupo**.
- onde: $[a] \odot [b] = [a * b]$

● Prova:

- G é um grupo $\Rightarrow G$ é um monóide $\Rightarrow G/R$ é um monóide
- Só falta provar que **cada elemento de G/R tem uma inversa**:
 - como $[a] \in G/R$, então $[a^{-1}] \in G/R$ (pois $a^{-1} \in G$)
 - daí: $[a] \odot [a^{-1}] = [a * a^{-1}] = [e]$
 - de modo que: $[a]^{-1} = [a^{-1}]$
 - portanto: $(G/R, \odot)$ **é um grupo** □

HOMOMORFISMOS E ISOMORFISMOS

- **Nota:** As definições de homomorfismo, isomorfismo e congruência para grupos envolvem **apenas** as suas **estruturas de semigrupos e monóides**.
- A seguir, uma consequência imediata dos resultados para semigrupos...

PRODUTOS E QUOCIENTES DE GRUPOS

● Corolário 1(a):

- Se R é uma relação de congruência sobre G , então:
 - a função $f_R : G \rightarrow G/R$, dada por: $f_R(a) = [a]$ é um homomorfismo de grupo.

PRODUTOS E QUOCIENTES DE GRUPOS

● Corolário 1(a):

- Se R é uma relação de congruência sobre G , então:
 - a função $f_R : G \rightarrow G/R$, dada por: $f_R(a) = [a]$ é um **homomorfismo de grupo**.

● Corolário 1(b):

- Se $f : G \rightarrow G'$ é um **homomorfismo** e:
 - se R é definida por: “ $a R b$ sse $f(a) = f(b)$ ”
- então:
 - R é uma relação **de congruência**
 - a função $\bar{f} : G/R \rightarrow G'$, dada por: $\bar{f}([a]) = f(a)$ é um **isomorfismo** do grupo $(G/R, \otimes)$ sobre o $(G', *')$.

SUBGRUPOS E COSETS

- Têm uma forma muito especial...
- Seja H um subgrupo de um grupo G e seja $a \in G$:
 - o **coset à esquerda** de H em G , determinado por a , é o conj.:
$$aH = \{ah \mid h \in H\}$$
 - o **coset à direita** de H em G , determinado por a , é o conjunto:
$$Ha = \{ha \mid h \in H\}$$
 - dizemos que um subgrupo H de G é **normal** se:
$$aH = Ha, \quad \forall a \in G$$

SUBGRUPOS E COSETS

- Têm uma forma muito especial...
- Seja H um subgrupo de um grupo G e seja $a \in G$:
 - o **coset à esquerda** de H em G , determinado por a , é o conj.:
$$aH = \{ah \mid h \in H\}$$
 - o **coset à direita** de H em G , determinado por a , é o conjunto:
$$Ha = \{ha \mid h \in H\}$$
 - dizemos que um subgrupo H de G é **normal** se:
$$aH = Ha, \quad \forall a \in G$$
- **Nota:** “ $Ha = aH$ ” **não é o mesmo** que “ $ha = ah$ ”
 - só se sabe que $ha = ah'$ aonde h' é **algum elemento** em H

SUBGRUPOS E COSETS

- Computando todos os **cosets à esquerda** de um subgrupo H em G :
 - Suponha que $a \in H$:
 - então $aH \subseteq H$, pois H é subgrupo (de G)
 - além disto:
 - se $h \in H$, então $h = ah'$, aonde: $h' = a^{-1}h \in H$
 - de modo que: $H \subseteq aH$.
 - logo: se $a \in H$, então $aH = H$.

SUBGRUPOS E COSETS

- Computando todos os cosets à esquerda de um subgrupo H em G :
 - Suponha que $a \in H$:
 - então $aH \subseteq H$, pois H é subgrupo (de G)
 - além disto:
 - se $h \in H$, então $h = ah'$, aonde: $h' = a^{-1}h \in H$
 - de modo que: $H \subseteq aH$.
 - logo: se $a \in H$, então $aH = H$.
 - Conclusão: quando computando todos os cosets de H , não é preciso computar aH para $a \in H$
 - (pois será sempre H)

SUBGRUPOS E COSETS

● **Exemplo 1(/3):** Seja G o grupo de simetrias S_3 já visto:

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

● Com a operação de **composição sobre S_3** :

\circ	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

SUBGRUPOS E COSETS

- **Exemplo 1(/3):** Seja G o grupo de simetrias S_3 já visto (\Rightarrow).
- O subconjunto $H = \{f_1, g_2\}$ é um subgrupo de G .

SUBGRUPOS E COSETS

● **Exemplo 1(1/3):** Seja G o grupo de simetrias S_3 já visto (\Rightarrow).

- O subconjunto $H = \{f_1, g_2\}$ é um subgrupo de G .
- Computando todos os cosets à esquerda de H em G :
 - $f_1 H = g_2 H = H$
 - além disto:
$$f_2 H = \{f_2, g_1\}$$
$$f_3 H = \{f_3, g_3\}$$
$$g_1 H = \{g_1, f_2\} = f_2 H$$
$$g_3 H = \{g_3, f_3\} = f_3 H$$

SUBGRUPOS E COSETS

● **Exemplo 1(/3):** Seja G o grupo de simetrias S_3 já visto (\Rightarrow).

- O subconjunto $H = \{f_1, g_2\}$ é um subgrupo de G .
- Computando todos os cosets à esquerda de H em G :
 - $f_1H = g_2H = H$
 - além disto:
$$f_2H = \{f_2, g_1\}$$
$$f_3H = \{f_3, g_3\}$$
$$g_1H = \{g_1, f_2\} = f_2H$$
$$g_3H = \{g_3, f_3\} = f_3H$$
- Logo, cosets à esquerda de H em G que são **distintos**:

$$H, f_2H \text{ e } f_3H$$

□

SUBGRUPOS E COSETS

● **Exemplo 2(/3):** Sejam H e G como no exemplo anterior:

$$H = \{f_1, g_2\}$$

$$G = S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}$$

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

SUBGRUPOS E COSETS

- **Exemplo 2(/3):** Sejam H e G como no exemplo anterior:

$$H = \{f_1, g_2\}$$

$$\begin{aligned} G = S_3 &= \{f_1, f_2, f_3, g_1, g_2, g_3\} \\ &= \{\{1, 2, 3\}, \{2, 3, 1\}, \{3, 1, 2\}, \{1, 3, 2\}, \{3, 2, 1\}, \{2, 1, 3\}\} \end{aligned}$$

- Considere o seguinte coset à direita:

$$Hf_2 = \{f_2, g_3\}$$

- Mas vimos que: $f_2H = \{f_2, g_1\}$.

- Logo: H não é um subgrupo normal de G . □

SUBGRUPOS E COSETS

● **Exemplo 3(/3):** Mostre que se G é um grupo abeliano, todo subgrupo de G é um subgrupo normal.

● Sejam:

● H um subgrupo de G

● $a \in G$

● $h \in H$

SUBGRUPOS E COSETS

● **Exemplo 3(/3):** Mostre que se G é um grupo abeliano, todo subgrupo de G é um subgrupo normal.

● Sejam:

● H um subgrupo de G

● $a \in G$

● $h \in H$

● Então, como G é abeliano: $ha = ah$

● de modo que: $Ha = aH$

● o que implica que H é um subgrupo normal de G . □

SUBGRUPOS NORMAIS E COSETS

● Teorema 3:

● Sejam:

- R uma relação de congruência sobre um grupo G
- $H = [e]$ (a classe de equivalência que contém e),

● Então:

- H é um **subgrupo normal** de G :
 - $\forall a \in G, [a] = aH = Ha$

● Prova: (\Rightarrow)

SUBGRUPOS NORMAIS E COSETS

● **Prova:** Sejam a e b elementos quaisquer em G .

● Já que R é de equivalência: $b \in [a] \Leftrightarrow [b] = [a]$

SUBGRUPOS NORMAIS E COSETS

● **Prova:** Sejam a e b elementos quaisquer em G .

● Já que R é de equivalência: $b \in [a] \Leftrightarrow [b] = [a]$

● Também (pelo Teor 2), já que G/R é um grupo:

$$[b] = [a] \Leftrightarrow [a]^{-1}[b] = [a^{-1}b] = [e] = H$$

SUBGRUPOS NORMAIS E COSETS

● **Prova:** Sejam a e b elementos quaisquer em G .

● Já que R é de equivalência: $b \in [a] \Leftrightarrow [b] = [a]$

● Também (pelo Teor 2), já que G/R é um grupo:

$$[b] = [a] \Leftrightarrow [a]^{-1}[b] = [a^{-1}b] = [e] = H$$

● ou seja: $b \in [a] \Leftrightarrow a^{-1}b \in H$ (ou: $b \in aH$)

$$\Rightarrow [a] = aH, \quad \forall a \in G$$

SUBGRUPOS NORMAIS E COSETS

● **Prova:** Sejam a e b elementos quaisquer em G .

● Já que R é de equivalência: $b \in [a] \Leftrightarrow [b] = [a]$

● Também (pelo Teor 2), já que G/R é um grupo:

$$[b] = [a] \Leftrightarrow [a]^{-1}[b] = [a^{-1}b] = [e] = H$$

● ou seja: $b \in [a] \Leftrightarrow a^{-1}b \in H$ (ou: $b \in aH$)

$$\Rightarrow [a] = aH, \quad \forall a \in G$$

● Pode-se mostrar, da mesma forma, que $[a] = Ha$:

$$b \in [a] \Leftrightarrow H = [e] = [b][a]^{-1} = [ba^{-1}]$$

● Portanto: $[a] = aH = Ha$ e H é normal. □

SUBGRUPOS NORMAIS E COSETS

- **Combinando** o **Teor 3**: “A classe $[e]$ é sempre um subgrupo normal de G .”
 - ou: “Se R é uma rel. de congruência sobre um G , então: $[a] = a[e] = [e]a$.”
- com o **Corolário 1(a)**:
 - “Se R é uma relação de congruência sobre G , então:
 - $f_R : G \rightarrow G/R$, dada por $f_R(a) = [a]$, é um **homomorfismo de grupo**.”

SUBGRUPOS NORMAIS E COSETS

- **Combinando** o **Teor 3**: “A classe $[e]$ é sempre um subgrupo normal de G .”
 - ou: “Se R é uma rel. de congruência sobre um G , então: $[a] = a[e] = [e]a$.”
- com o **Corolário 1(a)**:
 - “Se R é uma relação de congruência sobre G , então:
 - $f_R : G \rightarrow G/R$, dada por $f_R(a) = [a]$, é um **homomorfismo de grupo**.”
- notamos que, neste caso:
 - G/R consiste dos **cosets à esquerda de $N = [e]$**
 - (ou seja: ao juntarmos todos os cosets à esquerda de $[e]$, obteremos G/R)
 - e a operação **em G/R** é dada (**simplesmente**) por:
$$(aN)(bN) = [a] \circledast [b] = [ab] = abN \quad (\text{pois: homomorfismo})$$
 - e escrevemos G/R como $G/[e]$ ou: **G/N** .

SUBGRUPOS NORMAIS E COSETS

● Teorema 4:

● Sejam:

● N um subgrupo normal de um grupo G

● R a seguinte relação sobre G :

$$a R b \text{ se e somente se } a^{-1}b \in N$$

● Então:

(a) R é uma relação de congruência sobre G

(b) N é a classe de equivalência $[e]$ relativa a R

· (“ e ” é a identidade de G)

● “*Todo subgrupo normal N de um grupo G é a classe de equivalência da identidade de G , para alguma rel. de congruência.*” Ou seja: “ $\exists R$ tal que $N = [e]$ ”

● Prova: (\Rightarrow)

SUBGRUPOS NORMAIS E COSETS

● **Prova de (a) (1/2):** (“ $a R b \Leftrightarrow a^{-1}b \in N$ é de congruência”)

● R é uma relação de equivalência sobre G :

● R é reflexiva: $a R a$, pois: $a^{-1}a = e \in N$

● R é simétrica: seja $a R b$:

- então: $a^{-1}b \in N$
- mas: $(a^{-1}b)^{-1} = b^{-1}a \in N$ (pois N é subgrupo)
- de modo que: $b R a$

● R é transitiva: sejam $a R b$ e $b R c$:

- então: $a^{-1}b \in N$ e $b^{-1}c \in N$
 $\Rightarrow (a^{-1}b)(b^{-1}c) = a^{-1}c \in N$
- de modo que: $a R c$

● continuação da prova de (a): \Rightarrow

SUBGRUPOS NORMAIS E COSETS

● **Prova de (a) (2/2):** (“ $a R b \Leftrightarrow a^{-1}b \in N$ é de congruência”)

● R é de congruência sobre G :

● suponha que $a R b$ e $c R d$:

· então: $a^{-1}b \in N$ e $c^{-1}d \in N$

SUBGRUPOS NORMAIS E COSETS

● **Prova de (a) (2/2):** (“ $a R b \Leftrightarrow a^{-1}b \in N$ é de congruência”)

● R é de congruência sobre G :

● suponha que $a R b$ e $c R d$:

· então: $a^{-1}b \in N$ e $c^{-1}d \in N$

● mas N é normal: $Nd = dN$

· “ $\forall n_1 \in N, \exists n_2 \in N \mid n_1 d = d n_2$ ”

· em particular: $a^{-1}b d = d n_2$, para algum $n_2 \in N$

SUBGRUPOS NORMAIS E COSETS

● **Prova de (a) (2/2):** (“ $a R b \Leftrightarrow a^{-1}b \in N$ é de congruência”)

● R é de congruência sobre G :

● suponha que $a R b$ e $c R d$:

· então: $a^{-1}b \in N$ e $c^{-1}d \in N$

● mas N é normal: $Nd = dN$

· “ $\forall n_1 \in N, \exists n_2 \in N \mid n_1 d = d n_2$ ”

· em particular: $a^{-1}b d = d n_2$, para algum $n_2 \in N$

● o que permite escrever:

$$\begin{aligned}(ac)^{-1}bd &= (c^{-1}a^{-1})(bd) = \\ &= c^{-1}(a^{-1}b)d = (c^{-1}d)n_2 \in N\end{aligned}$$

· de modo que: $ac R bd$.

● **Prova de (b)** \Rightarrow

SUBGRUPOS NORMAIS E COSETS

● **Prova de (b):** (“ se: $a R b \Leftrightarrow a^{-1}b \in N$, então: $N = [e]$ ”)

● Seja $x \in N$:

● então $x^{-1}e = x^{-1} \in N$ (pois N é subgrupo)

● de modo que: $x R e$ e, portanto: $x \in [e]$

● logo: $N \subseteq [e]$

SUBGRUPOS NORMAIS E COSETS

● **Prova de (b):** (“ se: $a R b \Leftrightarrow a^{-1}b \in N$, então: $N = [e]$ ”)

● Seja $x \in N$:

● então $x^{-1}e = x^{-1} \in N$ (pois N é subgrupo)

● de modo que: $x R e$ e, portanto: $x \in [e]$

● logo: $N \subseteq [e]$

● Conversamente:

● se $x \in [e]$, então $x R e$

● de modo que: $x^{-1}e = x^{-1} \in N$

● então: $x \in N$ e $[e] \subseteq N$

● Logo: $N = [e]$

□

SUBGRUPOS NORMAIS E COSETS

- **Teor 3:** “A classe $[e]$, sob R de congruência, é sempre um subgrupo normal de G .”
- Ou: “Se R é uma rel. de congruência sobre um G , então: $[a] = a[e] = [e]a$.”
- **Teor 4:** “Todo subgrupo normal N de um grupo G é igual a $[e]$, para alguma rel. de congruência.”

SUBGRUPOS NORMAIS E COSETS

- **Teor 3:** “A classe $[e]$, sob R de congruência, é sempre um subgrupo normal de G .”
 - Ou: “Se R é uma rel. de congruência sobre um G , então: $[a] = a[e] = [e]a$.”
- **Teor 4:** “Todo subgrupo normal N de um grupo G é igual a $[e]$, para alguma rel. de congruência.”
- Logo, se G é um grupo qualquer:
 - as classes de equivalência relativas a uma rel. de congruência sobre G são sempre os cosets de algum subgrupo normal de G .
 - “Dada a R , \exists um subgrupo normal $([e])$ cujos cosets são as suas classes.”

SUBGRUPOS NORMAIS E COSETS

- **Teor 3:** “A classe $[e]$, sob R de congruência, é sempre um subgrupo normal de G .”
 - Ou: “Se R é uma rel. de congruência sobre um G , então: $[a] = a[e] = [e]a$.”
- **Teor 4:** “Todo subgrupo normal N de um grupo G é igual a $[e]$, para alguma rel. de congruência.”
- Logo, se G é um grupo qualquer:
 - as classes de equivalência relativas a uma rel. de congruência sobre G são sempre os cosets de algum subgrupo normal de G .
 - “Dada a R , \exists um subgrupo normal $([e])$ cujos cosets são as suas classes.”
- Conversamente:
 - os cosets de todo subgrupo normal de G são apenas classes de equivalência relativas a alguma relação de congruência sobre G .
 - “Dado um subgrupo normal, $\exists R$ de congr. cujas classes são os seus cosets.”

PRODUTOS E QUOCIENTES DE GRUPOS (RELEMBR.)

- **Corolário 1(b):** (rel.) Se $f : G \rightarrow G'$ é um homomorfismo e:
 - se R é definida por: “ $a R b$ sse $f(a) = f(b)$ ”
- então:
 - R é uma relação de congruência
 - a função $\bar{f} : G/R \rightarrow G'$, dada por: $\bar{f}([a]) = f(a)$
é um isomorfismo do grupo $(G/R, \otimes)$ sobre o grupo $(G', *')$.
- **Teor 3:** “Se R é uma rel. de congruência sobre um G , então: $[a] = a[e] = [e]a$.”

SUBGRUPOS NORMAIS E COSETS

● O **Corolário 1(b)** pode agora ser escrito como:

● Sejam:

● f um **homomorfismo** de um grupo $(G, *)$ sobre um $(G', *')$.

● o **kernel** de f dado por: $\ker(f) = \{a \in G \mid f(a) = e'\}$

● Então:

(a) $\ker(f)$ é um **subgrupo normal** de G

(b) o grupo quociente $G/\ker(f)$ é **isomórfico** a G' .

SUBGRUPOS NORMAIS E COSETS

● O **Corolário 1(b)** pode agora ser escrito como:

● Sejam:

● f um **homomorfismo** de um grupo $(G, *)$ sobre um $(G', *')$.

● o **kernel** de f dado por: $\ker(f) = \{a \in G \mid f(a) = e'\}$

● Então:

(a) $\ker(f)$ é um **subgrupo normal** de G

(b) o grupo quociente $G/\ker(f)$ é **isomórfico** a G' .

● **Prova:** segue de Corol. 1 + Teor. 3, pois:

● se R é a **relação de congruência** sobre G dada por:

$$a R b \Leftrightarrow f(a) = f(b)$$

● pode-se mostrar que: $\ker(f) = [e]$

□

SUBGRUPOS NORMAIS E COSETS

- **Exemplo:** Seja o homomorfismo f de \mathbb{Z} sobre \mathbb{Z}_n : $f(m) = [r]$
 - O inteiro m em \mathbb{Z} pertence a $\ker(f)$ sse $f(m) = [0]$
 - Ou seja, sse m é um múltiplo de n
 - Portanto: $\ker(f) = n\mathbb{Z}$ □

PRODUTOS E QUOCIENTES DE GRUPOS

- Final deste item.
- **Dica:** fazer **exercícios** sobre Produtos e Quocientes de Grupos...