

Teoria de Grupos: notas de estudo

Guilherme Philippi

22 de janeiro de 2021

Sumário

1	Grupos	2
1.1	Lei de composição	2
1.2	Grupos	3
1.3	Subgrupos	3
1.4	Homomorfismos	4
1.5	Isomorfismos	5
1.6	Relações de Equivalência e Partições	6
1.7	Coclasses	8
1.8	Restrição de um homomorfismo para um subgrupo	9
1.8.1	Produto de Grupos	10
	Referências Bibliográficas	11

Capítulo 1

Grupos

1.1 Lei de composição

Definição 1.1.1 (Lei de Composição). Uma *Lei de Composição* sobre S é uma função $F : S \times S \longrightarrow S$.

Definição 1.1.2. Para $a, b, c \in S$, uma Lei de Composição F é dita

- *Associativa* se $F(F(a, b), c) = F(a, F(b, c))$;
- *Comutativa* se $F(a, b) = F(b, a)$.

Observação 1.1.1. Usaremos a notação $F(a, b) = ab$, para simplificar a escrita de propriedades.

Proposição 1.1.1. *Seja uma lei associativa dada sobre o conjunto S . Há uma única forma de definir, para todo inteiro n , um produto de n elementos $a_1, \dots, a_n \in S$ (diremos $[a_1 \cdots a_n]$) com as seguintes propriedades:*

1. o produto $[a_1]$ de um elemento é o próprio elemento;
2. o produto $[a_1 a_2]$ de dois elementos é dado pela lei de composição;
3. para todo inteiro $1 \leq i \leq n$, $[a_1 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n]$.

Demonstração. A demonstração dessa proposição é feita por indução em n . □

Definição 1.1.3. Dizemos que $e \in S$ é *identidade* para uma lei de composição se $ea = ae = a$ para todo $a \in S$.

Proposição 1.1.2. *O elemento identidade é único.*

Demonstração. Se e, e' são identidades, já que e é identidade, então $ee' = e'$ e, como e' é uma identidade, $ee' = e$. Logo $e = e'$, isto é, a identidade é única. □

Observação 1.1.2. Usaremos $\vec{1}$ para representar a identidade multiplicativa e $\vec{0}$ para denotar a aditiva.

Definição 1.1.4 (Elemento inverso). Seja uma lei de composição que possua uma identidade. Um elemento $a \in S$ é chamado *invertível* se há um outro elemento $b \in S$ tal que $ab = ba = 1$. Desde que b exista, ela é única e a denotaremos por a^{-1} e a chamaremos *inversa de a* .

Proposição 1.1.3. Se $a, b \in S$ possuem inversa, então a composição $(ab)^{-1} = b^{-1}a^{-1}$.

Observação 1.1.3 (Potências). Usaremos as seguintes notações:

- $a^n = a^{n-1}a$ é a composição de $a \cdots a$ n vezes;
- a^{-n} é a inversa de a^n ;
- $a^0 = \vec{1}$.

Com isso, tem-se que $a^{r+s} = a^r a^s$ e $(a^r)^s = a^{rs}$. (Isso não induz uma notação de fração $\frac{b}{a}$ a menos que seja uma lei comutativa, visto que ba^{-1} pode ser diferente de $a^{-1}b$). Para falar de uma lei de composição aditiva, usaremos $-a$ no lugar de a^{-1} e na no lugar de a^n .

1.2 Grupos

Definição 1.2.1 (Grupo). Um *grupo* $(G, *)$ é um conjunto G onde uma lei de composição $*$ é dada sobre G tal que as seguintes propriedades são satisfeitas:

1. (*Associatividade*). Para todo $a, b, c \in G$, tem-se

$$(a * b) * c = a * (b * c);$$

2. (*Existência da identidade*). Existe um elemento $\vec{1} \in G$ tal que, para todo $a \in G$,

$$\vec{1} * a = a * \vec{1} = a;$$

3. (*Existência do inverso*). Para todo $a \in G$ existe um elemento $a' \in G$ tal que

$$a * a' = a' * a = \vec{1}.$$

Observação 1.2.1. É comum abusar da notação e chamar um grupo $(G, *)$ e o conjunto de seus elementos G pelo mesmo simbolo, omitindo a lei de composição quando não houver necessidade.

Definição 1.2.2 (Grupo abeliano). Um *grupo abeliano* é um grupo com uma lei de composição comutativa. Costuma-se usar a notação aditiva para grupos abelianos.

Proposição 1.2.1 (Lei do cancelamento). Sejam a, b, c elementos de um grupo G . Se $ab = ac$, então $b = c$.

1.3 Subgrupos

Definição 1.3.1 (Subgrupo). Um subconjunto H de um grupo G é chamado de *subgrupo* de G (e escreve-se $H \leq G$) se possuir as seguintes propriedades:

1. (*Fechado*). Se $a, b \in H$, então $ab \in H$;
2. (*Identidade*). $1 \in H$;

3. (*Inversível*). Se $a \in H$, então $a^{-1} \in H$.

Observação 1.3.1 (Lei de composição induzida). Veja que a propriedade 1 necessita de uma lei de composição. Usamos a lei de composição de G para definir uma lei de composição de H , chamada *lei de composição induzida*. Essas propriedades garantem que H é um grupo com respeito a sua lei induzida.

Definição 1.3.2 (Subgrupo apropriado). Todo grupo G possui dois subgrupos triviais: O subgrupo formado por todos os elementos de G e o subgrupo $\{\tilde{1}\}$, formado pela identidade de G . Diz-se que um subgrupo é um *subgrupo apropriado* se for diferente desses dois.

Exemplo 1.3.1. Utilizando da notação multiplicativa, define-se o *subgrupo cíclico* H gerados por um elemento arbitrário x de um grupo G como o conjunto de todas as potências de x : $H = \{\dots, x^{-2}, x^{-1}, \tilde{1}, x, x^2, \dots\}$.

Definição 1.3.3. Chama-se *ordem* de um grupo G o número $|G|$ de elementos de G .

Também pode-se definir um subgrupo de um grupo G *gerado por um subconjunto* $U \subset G$. Esse é o menor subgrupo de G que contém U e consiste de todos os elementos de G que podem ser expressos como um produto de uma cadeia de elementos de U e seus inversos.

Exemplo 1.3.2. O *grupo de quaternions* H é o menor subgrupo do conjunto de matrizes 2×2 complexas invertíveis que não é cíclico. Isso consiste nas oito matrizes

$$H = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\},$$

onde

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Os dois elementos \mathbf{i}, \mathbf{j} geram H , e o cálculo leva as formulas

$$\mathbf{i}^4 = 1, \quad \mathbf{i}^2 = \mathbf{j}^2, \quad \mathbf{j}\mathbf{i} = \mathbf{i}^3\mathbf{j}.$$

1.4 Homomorfismos

Definição 1.4.1 (Homomorfismo de grupo). Sejam $(G, *)$ e (G', \cdot) dois grupos. Um *homomorfismo* $\varphi : G \longrightarrow G'$ é um mapeamento tal que

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b), \quad \forall a, b \in G. \quad (\text{propriedade de homomorfismo})$$

Quando isso acontece, dizemos que o mapeamento φ *preserva a estrutura algébrica de grupo*.

Exemplo 1.4.1 (Inclusão). Seja H o subgrupo de um grupo G . O homomorfismo $i : H \longrightarrow G$ é dito *inclusão* de H em G , definido por $i(x) = x$.

Proposição 1.4.1. *Um homomorfismo $\varphi : G \longrightarrow G'$ mapeia a identidade de G à identidade de G' e transforma as inversas de G nas respectivas inversas em G' . Isto é, $\varphi(\bar{1}) = \bar{1}$ e $\varphi(a^{-1}) = \varphi(a)^{-1}$.*

Definição 1.4.2 (Imagem). A *imagem* de um homomorfismo $\varphi : G \longrightarrow G'$ é o subconjunto de G'

$$\text{im } \varphi = \{x \in G' \mid x = \varphi(a), \text{ para algum } a \in G\} = \varphi(G).$$

Proposição 1.4.2. *A imagem de um homomorfismo $\varphi : G \longrightarrow G'$ é um subgrupo de G' .*

Definição 1.4.3 (Núcleo). O *núcleo* do homomorfismo $\varphi : G \longrightarrow G'$ é o subconjunto de G formado pelos elementos que são mapeados pela identidade em G' :

$$\text{nu } \varphi = \{a \in G \mid \varphi(a) = 1\} = \varphi^{-1}(1).$$

Proposição 1.4.3. *O núcleo de um homomorfismo $\varphi : G \longrightarrow G'$ é um subgrupo de G .*

1.5 Isomorfismos

Definição 1.5.1 (Isomorfismo de grupos). Dois grupos $(G, *)$ e (G', \cdot) são ditos *isomórficos* se possuem um homomorfismo bijetivo entre si, isto é, há um mapeamento *bijetivo* $\varphi : G \longrightarrow G'$ (chamado *relação de isomorfismo*) que respeita a propriedade de homomorfismo:

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b), \text{ para todo } a, b \in G.$$

Observação 1.5.1. Usa-se a notação $G \approx G'$ para dizer que G é isomorfo a G' .

Definição 1.5.2 (Classe de isomorfismo). Diz-se que o conjunto de grupos isomórfos a um dado grupo G é a *classe de isomorfismo de G* .

Proposição 1.5.1. *Qualquer dois grupos em uma mesma classe de isomorfismo também são isomorfos entre si.*

Definição 1.5.3 (Automorfismo). Quando uma relação de isomorfismo $\varphi : G \longrightarrow G$ é definida de um grupo G para ele mesmo, chamamos esse tipo de isomorfismo de *automorfismo de G* .

Exemplo 1.5.1 (Conjugação). Seja $b \in G$ um elemento fixo. Então, a *conjugação de G por b* é o mapeamento φ de G para ele mesmo definido por

$$\varphi_b(x) = bxb^{-1}.$$

Esse é um automorfismo porque:

- é compatível com a propriedade de homomorfismo:

$$\varphi_b(xy) = bxyb^{-1} = bx\bar{1}yb^{-1} = bxb^{-1}byb^{-1} = \varphi_b(x)\varphi_b(y);$$

- é um mapa bijetivo visto que existe a função inversa $\varphi_b^{-1}(x) = b^{-1}xb = \varphi_{b^{-1}}(x)$ (isto é, a conjugação por b^{-1}) que, de forma análoga, também é compatível com a propriedade de homomorfismo.

Observação 1.5.2 (Abelianos). Se o grupo é abeliano possui a conjugação trivial: $bab^{-1} = abb^{-1} = a$ (mapa identidade). Porém, qualquer grupo não comutativo tem alguma conjugação não trivial, isto é, existe ao menos um b no grupo tal que $ba \neq ab$ para algum a , portanto, possui pelo menos um automorfismo não trivial: a conjugação do grupo por b .

Definição 1.5.4 (Conjugado). O elemento bab^{-1} é chamado *conjugado de a por b* . Dois elementos $a, a' \in G$ são ditos *conjugados* se existe $b \in G$ tal que $a' = bab^{-1}$.

Observação 1.5.3. O conjugado tem uma interpretação muito útil: Se escrevermos bab^{-1} como a' , então

$$ba = a'b.$$

Ou seja, pode-se pensar na conjugação como a mudança em a que resulta de mover b de um lado para o outro na equação.

Proposição 1.5.2. *Seja $\varphi : G \rightarrow G'$ um homomorfismo. Se $a \in \text{nu } \varphi$ e b é qualquer elemento do grupo G , então o conjugado $bab^{-1} \in \text{nu } \varphi$.*

Definição 1.5.5 (Subgrupo normal). Um subgrupo N de um grupo G é chamado *subgrupo normal* (escreve-se $N \trianglelefteq G$) se para cada $a \in N$ e $b \in G$, o conjugado $bab^{-1} \in N$.

Observação 1.5.4. Fica claro que o núcleo de um homomorfismo é um subgrupo normal. Além disso, todo subgrupo de um grupo abeliano também é um subgrupo normal, porém, isso não é necessariamente verdade em subgrupos de grupos não abelianos (veja Observação 1.5.2).

Definição 1.5.6 (Centro de um grupo). O *centro* $Z(G)$ de um grupo G é o conjunto de elementos que comutam com todo elemento de G :

$$Z(G) = \{z \in G \mid zx = xz \text{ para todo } x \in G\}.$$

Proposição 1.5.3. *O centro de todo grupo é um subgrupo normal do grupo.*

1.6 Relações de Equivalência e Partições

Definição 1.6.1 (Partições). Seja S um conjunto. Uma *partição* P de S é uma subdivisão de S em subconjuntos não vazios e não sobrepostos, isto é, uma união de conjuntos disjuntos.

Exemplo 1.6.1. Pode-se particionar o conjunto dos números inteiros \mathbb{Z} na união de disjuntos $P \cup I$, onde $P = \{z \in \mathbb{Z} \mid z \text{ é par}\}$ e $I = \{z \in \mathbb{Z} \mid z \text{ é ímpar}\}$.

Definição 1.6.2 (Relações de equivalência). Uma *relação de equivalência* sobre um conjunto S é uma relação que se mantém sobre um subconjunto de elementos de S . Escreve-se $a \sim b$ para representar a equivalência de $a, b \in S$, que precisa respeitar as seguintes propriedades:

1. (*Transitiva*). Se $a \sim b$ e $b \sim c$, então $a \sim c$;
2. (*Simétrica*). Se $a \sim b$, então $b \sim a$;
3. (*Reflexiva*). $a \sim a$.

Observação 1.6.1. A noção de partição em S e a relação de equivalência em S são logicamente equivalentes: Dada uma partição P sobre S , pode-se definir uma relação de equivalência R tal que, se a e b estão no mesmo subconjunto partição, então $a \sim b$ e, dada uma relação de equivalência R , podemos definir uma partição P tal que o subconjunto que contém a é o conjunto de todos os elementos b onde $a \sim b$. Esse subconjunto é chamado de *classe de equivalência de a*

$$C_a = \{b \in S \mid a \sim b\}$$

e S é particionado em classes de equivalência.

Proposição 1.6.1. *Sejam C_a e C_b duas classes de equivalência do conjunto S . Se existe d tal que $d \in C_a$ e $d \in C_b$, então $C_a = C_b$.*

Observação 1.6.2. Seja um conjunto S . Suponha que exista uma relação de equivalência ou uma partição sobre S . Então, pode-se construir um novo conjunto \bar{S} formado pelas classes de equivalência ou os subconjuntos partições de S . Essa construção induz uma notação muito útil: para $a \in S$, a classe de equivalência de a ou o subconjunto partição que contém a serão denotados como o elemento $\bar{a} \in \bar{S}$. Desta forma, a notação $\bar{a} = \bar{b}$ significa que $a \sim b$ e chamamos $a, b \in S$ de *representantes* das respectivas classes de equivalência $\bar{a}, \bar{b} \in \bar{S}$.

Definição 1.6.3. Seja um mapeamento $\varphi : S \longrightarrow T$. Chama-se de *relação de equivalência determinada por φ* a relação dada por $\varphi(a) = \varphi(b) \Rightarrow a \sim b$. Além disso, para um elemento $t \in T$, o subconjunto de $\varphi^{-1}(t) = \{s \in S \mid \varphi(s) = t\}$ é dito *imagem inversa de t por φ* .

Proposição 1.6.2. *Seja um mapeamento $\varphi : S \longrightarrow T$ e $t \in T$ um elemento qualquer de T . Se a imagem inversa $\varphi^{-1}(t)$ é não vazia, então $t \in \text{im } \varphi$ e $\varphi^{-1}(t)$ forma uma classe de equivalência $\bar{\varphi} \in \bar{S}$ através da relação determinada por φ .*

Definição 1.6.4 (Congruência). Seja $\varphi : G \longrightarrow G'$ um homomorfismo. A relação de equivalência definida por φ é usualmente denotada por \equiv ao invés de \sim e a chamamos de *congruência*:

$$\varphi(a) = \varphi(b) \Rightarrow a \equiv b, \text{ para } a, b \in G.$$

Proposição 1.6.3. *Seja $\varphi : G \longrightarrow G'$ um homomorfismo e $a, b \in G$. Então as seguintes afirmações são equivalentes:*

- $\varphi(a) = \varphi(b)$
- $b = an$, para algum $n \in \text{nu } \varphi$
- $a^{-1}b \in \text{nu } \varphi$.

Definição 1.6.5 (Coclasse em relação ao núcleo). Seja $\varphi : G \longrightarrow G'$ um homomorfismo, $a \in G$ e $n \in \text{nu } \varphi$. O conjunto

$$a \text{ nu } \varphi = \{g \in G \mid g = an, \text{ para algum } n \in \text{nu } \varphi\}$$

é dito *coclasse de nu φ em G* .

Observação 1.6.3. Pode-se particionar o grupo G em *classes de congruência*, formadas pelas coclasses $a \text{ nu } \varphi$. Estas são imagens inversas do mapeamento φ .

Proposição 1.6.4. O homomorfismo de grupo $\varphi : G \longrightarrow G'$ é injetivo se, e somente se, seu núcleo é o subgrupo trivial $\{1\}$.

Observação 1.6.4. Esse resultado da uma forma de verificar se um homomorfismo φ é também um isomorfismo: Se $\text{nu } \varphi = \{1\}$ e $\text{im } \varphi = G'$, então φ é, pelos respectivos motivos, injetiva e sobrejetiva. Então é um isomorfismo.

1.7 Coclasses

Definimos coclasse somente em relação ao núcleo de um homomorfismo mas, na verdade, pode-se definir uma coclasse para qualquer subgrupo H de um grupo G .

Definição 1.7.1 (Coclasse a esquerda). Seja um subgrupo H de um grupo G . O subconjunto da forma

$$aH = \{ah \mid h \in H\}$$

é dito *coclasse a esquerda de H em G* .

Proposição 1.7.1. A coclasse é uma classe de equivalência para a relação de congruência

$$b = ah \Rightarrow a \equiv b, \text{ para algum } h \in H.$$

Observação 1.7.1. Daí segue que, como classes de equivalência particionam um grupo, coclasses a esquerda de um subgrupo particionam o grupo.

Definição 1.7.2 (Índice de um subgrupo). O número de coclasses a esquerda de um subgrupo H em um grupo G chama-se *índice de H em G* e é denotado como $[G : H]$.

Observação 1.7.2. Como há uma bijeção do subgrupo H para a coclasse aH , a cardinalidade de aH tem de ser a mesma de H . Isto é, as coclasses de H particionam G em partes de mesma ordem.

Proposição 1.7.2. Seja aH a coclasse do subgrupo H no grupo G . Então, a ordem $|G|$ do grupo G é dada por

$$|G| = |H|[G : H].$$

Proposição 1.7.3 (Teorema de Lagrange). Seja G um grupo finito e H um subgrupo de G . A ordem de H divide a ordem de G .

Definição 1.7.3 (Ordem de um elemento). Seja G um grupo. A *ordem de um elemento $a \in G$* é a ordem do grupo cíclico gerado por a .

Proposição 1.7.4. *Seja um grupo G com p elementos tal que p é primo e $a \in G$ diferente da identidade. Então G é o grupo cíclico $\{1, a, \dots, a^{p-1}\}$ gerado por a .*

Observação 1.7.3. Também podemos obter uma expressão para calcular a ordem de um grupo de homomorfismo. Seja $\varphi : G \longrightarrow G'$ um homomorfismo. Como as coclasses a esquerda do núcleo de φ são as imagens inversas φ^{-1} , elas estão em uma correspondência biunívoca com a imagem. Daí segue que

$$[G : \text{nu } \varphi] = |\text{im } \varphi|.$$

Proposição 1.7.5. *Seja $\varphi : G \longrightarrow G'$ um homomorfismo onde G e G' são finitos. Então*

$$|G| = |\text{nu } \varphi| \cdot |\text{im } \varphi|.$$

Definição 1.7.4 (Coclasses a direita). Os conjuntos da forma

$$Ha = \{ha \mid h \in H\}$$

chamam-se *coclasses a direita de um subgrupo H* . Esses são classes de equivalência para a relação de congruência a direita

$$b = ha \Rightarrow a \equiv b, \text{ para algum } h \in H.$$

Proposição 1.7.6. *Seja um subgrupo H de um grupo G . As seguintes afirmações são equivalentes:*

- H é subgrupo normal,
- $aH = Ha$ para todo $a \in G$.

1.8 Restrição de um homomorfismo para um subgrupo

Observação 1.8.1. O objetivo dessa seção é apresentar ferramentas para analisar um subgrupo H do grupo G a fim de garantir propriedades do grupo G . No geral, os subgrupos são mais específicos e menos complexos de se trabalhar.

Proposição 1.8.1. *Sejam K e H dois subgrupos do grupo G tal que a interseção $K \cap H$ é um subgrupo de H . Se K é um subgrupo normal de G , então $K \cap H$ é um subgrupo normal de H .*

Exemplo 1.8.1. Com esse resultado, se G é finito pode-se utilizar o Teorema de Lagrange para obter informações sobre a interseção dos dois subgrupos: a interseção divide $|H|$ e $|K|$. Se $|H|$ e $|K|$ não tem o mesmo fator de divisão, então $K \cap H = \{1\}$.

Definição 1.8.1 (Restrição de um homomorfismo para um subgrupo). Sejam o homomorfismo $\varphi : G \longrightarrow G'$ e H um subgrupo de G . Uma *restrição de φ para o subgrupo H* é o homomorfismo $\varphi|_H : H \longrightarrow G'$ definido como

$$\varphi|_H(h) = \varphi(h), \text{ para todo } h \in H.$$

Proposição 1.8.2. *Sejam o homomorfismo $\varphi : G \longrightarrow G'$ e H um subgrupo de G . O núcleo de uma restrição $\varphi|_H$ é a interseção do núcleo de φ e H .*

Proposição 1.8.3. *Sejam $\varphi : G \longrightarrow G'$ um homomorfismo, H' um subgrupo de G' e $\varphi^{-1}(H') = \{x \in G \mid \varphi(x) \in H'\}$ a imagem inversa de H' . Então*

- $\varphi^{-1}(H')$ é um subgrupo de G .
- Se H' é um subgrupo normal de G' , então $\varphi^{-1}(H')$ é um subgrupo normal de G .
- $\varphi^{-1}(H')$ contém o núcleo de φ
- A restrição de φ para $\varphi^{-1}(H')$ define um homomorfismo $\varphi^{-1}(H') \longrightarrow H'$, de forma que o núcleo desse homomorfismo é o núcleo de φ .

1.8.1 Produto de Grupos

Definição 1.8.2 (Produto de grupos). Seja G, G' dois grupos. O produto $G \times G'$ é um grupo formado pelo produto das componentes dos grupos G e G' , isso é, pela regra

$$(a, a'), (b, b') \rightsquigarrow (ab, a'b'),$$

onde $a, b \in G$ e $a', b' \in G'$. O par $(1, 1)$ é uma identidade e $(a, a')^{-1} = (a^{-1}, a'^{-1})$. A propriedade associativa é preservada em $G \times G'$ pois também é em G e G' .

Proposição 1.8.4. *A ordem de $G \times G'$ é o produto das ordens de G e G' .*

Observação 1.8.2 (Projeções). O produto de grupos é composto pelos homomorfismos:

$$i : G \longrightarrow G \times G', \quad i' : G' \longrightarrow G \times G', \quad p : G \times G' \longrightarrow G, \quad p' : G \times G' \longrightarrow G',$$

definidos como

$$i(x) = (x, 1), \quad i'(x') = (1, x'), \quad p(x, x') = x, \quad p'(x, x') = x'.$$

Os mapeamentos i, i' são injetivos, já os mapeamentos p, p' são sobrejetivos, onde nu $p = 1 \times G'$ e nu $p' = G \times 1$. Esses mapeamentos são chamados de *projeções*. Desde que são núcleos, $G \times 1$ e $1 \times G'$ são subgrupos normais de $G \times G'$.

Proposição 1.8.5 (Propriedades de Mapeamento dos Produtos). *Seja H um grupo qualquer. O homomorfismo $\Phi : H \longrightarrow G \times G'$ tem correspondência biunívoca com o par (φ, φ') de homomorfismos*

$$\varphi : H \longrightarrow G, \quad \varphi' : H \longrightarrow G'.$$

O núcleo de Φ é a interseção $(\text{nu } \varphi) \cap (\text{nu } \varphi')$.

Observação 1.8.3. É extremamente desejável encontrar uma relação isomorfa entre um grupo G e um produto de outros dois grupos $H \times H'$. Quando isso acontece, e infelizmente não são muitas as vezes, trabalhar com os grupos H e H' costumam ser mais simples que G .

Proposição 1.8.6. *Sejam $r, s \in \mathbb{Z}$ não divisíveis entre si. Um grupo cíclico de ordem rs é isomorfo ao produto dos grupos cíclicos de ordem r e s .*

Observação 1.8.4. Em contrapartida, um grupo cíclico de ordem par 4, por exemplo, não é isomorfo ao produto de dois grupos cíclicos de ordem 2. Também não podemos afirmar nada com base no resultado anterior sobre grupos não cíclicos.

Definição 1.8.3 (Conjunto de produtos). Sejam dois subgrupos A, B de um grupo G . Chamamos o *conjunto de produtos de elementos de A e B* por

$$AB = \{x \in G \mid x = ab \text{ para algum } a \in A \text{ e } b \in B\}.$$

Proposição 1.8.7. *Sejam H e K os subgrupos de um grupo G .*

- *Se $H \cap K = \{1\}$, o mapeamento de produto $p : H \times K \longrightarrow G$ definido por $p(h, k) = hk$ é injetivo e sua imagem é o subconjunto HK ;*
- *Se um dos subgrupos H ou K é um subgrupo normal de G , então os conjuntos de produtos HK e KH são iguais e HK é subgrupo de G ;*
- *Se ambos H e K são subgrupos normais, $H \cap K = \{1\}$ e $HK = G$, então G é isomorfo ao grupo de produto $H \times K$.*

Referências Bibliográficas