

# Untitled

November 26, 2020

## 1 Grupos

### 1.1 Lei de composição

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

**Definição:** Para  $a, b, c \in S$ , uma Lei de Composição é dita

- *lei associativa* se  $F(F(a, b), c) = F(a, F(b, c))$ ;
- *lei comutativa* se  $F(a, b) = F(b, a)$ .

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

**Proposição:** 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  $1 \leq i \leq n$ ,  $[a_1 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n]$ .

A demonstração dessa proposição é feita por indução em  $n$ .

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

Se  $e, e'$  são identidades então, desde que  $e$  é identidade,  $ee' = e'$ , e desde que  $e'$  é uma identidade,  $ee' = e$ . Logo  $e = e'$ , isto é, a identidade é única. Usaremos 1 para representar a identidade multiplicativa e 0 para denotar a aditiva (não são os números, apenas uma notação).

**Definição:** 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  $a$* .

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

Usaremos as seguintes notações: -  $a^n = a^{n-1}a$  é a composição de  $a \cdots a$   $n$  vezes; -  $a^0 = 1$  -  $a^{-n}$  é a inversa de  $a^n$

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 Grupo

**Definição:** Um *Grupo* é um conjunto  $G$  onde uma lei de composição associativa é dada sobre  $G$ , tal que exista uma identidade e todo elemento possua uma inversa.

É comum abusar da notação e chamar um grupo  $G$  e o conjunto  $G$  de seus elementos pelo mesmo símbolo.

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

**Proposição (lei do cancelamento):** Seja  $a, b, c$  elementos de um grupo  $G$ . Se  $ab = ac$ , então  $b = c$ .

---

## 1.3 Subgrupos

**Definição:** Um subconjunto  $H$  de um grupo  $G$  é chamado de *subgrupo* de  $G$  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  $a^{-1} \in H$ .

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.

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

**Exemplo:** 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  $x$ :  $H = \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\}$ .

**Definição:** 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:** O grupo de quaternions  $H$  é o menor subgrupo do conjunto de matrizes  $2 \times 2$  complexas invertíveis que não é cíclico. Isso consiste nas oito matrizes

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

onde

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

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

$$i^4 = 1, \quad i^2 = j^2, \quad ji = i^3j.$$

## 1.4 Isomorfismos

Se dois grupos  $G$  e  $G'$  estão relacionados por uma *correspondência biunívoca* entre seus elementos, compatível com suas leis de composição, isto é, uma **correspondência**



$$G \longleftrightarrow G'$$



**tendo** a seguinte propriedade: Se  $a, b \in G$  corresponde respectivamente a  $a', b' \in G'$ , então o produto  $ab \in G$  corresponde ao produto  $a'b' \in G'$ . Quando isso acontece, então dizemos que todas as propriedades da estrutura de um grupo se mantêm no outro.

Comumente escreve-se a correspondência acima de forma **assimétrica** como uma função, ou um mapeamento  $\varphi : G \longrightarrow G'$ . Assim, um isomorfismo  $G$  para  $G'$  é um mapeamento bijetivo que é compatível com as leis de composição:

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

**Definição:** Dois grupos  $G$  e  $G'$  são ditos *isomórfos* se há uma relação de isomorfismo  $\varphi : G \longleftrightarrow G'$ . Também usa-se a notação  $\approx$ :

$$G \approx G'.$$

**Definição:** Diz-se que o conjunto de grupos isomórfos a um dado grupo  $G$  é a *classe de isomorfismo* de  $G$ . Qualquer dois grupos em uma mesma classe de isomorfismo também são isomórfos entre si.

Também, dada uma relação de isomorfismo  $\varphi : G \longleftrightarrow G$  de um grupo  $G$  para ele mesmo, chamamos esse tipo de isomorfismo de *automorfismo* de  $G$ .

**Exemplo:** Seja  $b \in G$  um elemento fixo. Então, a *conjugação de  $G$  por  $b$*  é o mapeamento  $\varphi$  de  $G$  para ele mesmo definido por

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

Esse é um automorfismo porque: - é compatível com a multiplicação no grupo:

$$\varphi(xy) = bxyb^{-1} = bxb^{-1}byb^{-1} = \varphi(x)\varphi(y);$$

- é um mapa bijetivo desde que possui uma função inversa (chamada conjugação por  $b^{-1}$ ).

Se o grupo é abeliano, a conjugação é o mapa identidade:  $bab^{-1} = abb^{-1} = a$ . Porém, qualquer grupo não comutativo tem alguma conjugação não trivial, logo possui também um automorfismo não trivial. 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  $a' = bab^{-1}$ .

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.

---

## 1.5 Homomorfismos

**Definição:** Sejam  $G$  e  $G'$  dois grupos. Um *homomorfismo*  $\varphi : G \rightarrow G'$  é um mapeamento tal que

$$\varphi(ab) = \varphi(a)\varphi(b), \forall a, b \in G.$$

Ou seja, é a mesma condição do isomorfismo, porém, agora não há mais a necessidade de **sobrejetividade**.

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

**Proposição:** Um homomorfismo  $\varphi : G \rightarrow G'$  **leva** a identidade à identidade e inversas às inversas. Isto é,  $\varphi(1) = 1$  e  $\varphi(a^{-1}) = \varphi(a)^{-1}$ .

**Definição:** A *imagem* de um homomorfismo  $\varphi : G \rightarrow G'$  é o **subgrupo** de  $G'$

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

**Definição:** O *núcleo* de  $\varphi$  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:** Se  $a \in \text{nu } \varphi$  e  $b$  é qualquer elemento do grupo  $G$ , então o conjugado  $bab^{-1} \in \text{nu } \varphi$ .

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

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 (se  $G$  é abeliano, então  $bab^{-1} = a$ ). Mas isso não é necessariamente verdade em subgrupos de grupos não abelianos.

**Definição:** 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:** O centro de todo grupo é um subgrupo normal do grupo.

## 1.6 Relações de Equivalência e Partições

**Definição:** 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:** 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:** 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. Transitividade: Se  $a \sim b$  e  $b \sim c$ , então  $a \sim c$ ;
2. Simétrica: Se  $a \sim b$ , então  $b \sim a$ ;
3. Reflexiva:  $a \sim a$ .

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:** 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  $C_a = C_b$ .

Seja um conjunto  $S$ . Suponha que exista uma relação de equivalência ou uma partição sobre  $S$ . Então, pode-se construir um novo conjunto  $\tilde{S}$  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  $\bar{a} \in \tilde{S}$ . 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  $\bar{a}, \bar{b} \in \tilde{S}$ .

**Definição:** Seja um mapeamento  $\varphi : S \rightarrow T$ . Chama-se de *relação de equivalência determinada por  $\varphi$*  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  $\varphi$* .

**Proposição:** Seja um mapeamento  $\varphi : S \rightarrow T$  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  $\bar{\varphi} \in \tilde{S}$  através da relação determinada por  $\varphi$ .

**Definição:** Seja  $\varphi : G \rightarrow G'$  um homomorfismo. A relação de equivalência definida por  $\varphi$  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:** Seja  $\varphi : G \rightarrow G'$  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:** 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  $\varphi$  em  $G$* .

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

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

Esse resultado dá uma forma de verificar se um homomorfismo  $\varphi$  é também um isomorfismo: Se  $\text{nu } \varphi = \{1\}$  e  $\text{im } \varphi = G'$ , então  $\varphi$  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:** 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:** A coclasse é uma classe de equivalência para a relação de congruência

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

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

**Definição:** 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  $[G : H]$ .

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, o que nos permite enunciar o seguinte resultado:

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

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

**Proposição:** 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  $a$ .

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  $\varphi$  são as imagens inversas  $\varphi^{-1}$ , elas estão em uma correspondência biunívoca com a imagem. Daí segue que

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

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

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

**Definição:** 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:** 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

O objetivo aqui 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:** 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  $H$ .

Com esse resultado, por exemplo, 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:** Sejam o homomorfismo  $\varphi : G \longrightarrow G'$  e  $H$  um subgrupo de  $G$ . Uma *restrição de  $\varphi$  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:** 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  $\varphi$  e  $H$ .

**Proposição:** 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  $\varphi$ .
- A restrição de  $\varphi$  para  $\varphi^{-1}(H')$  define um homomorfismo  $\varphi^{-1}(H') \longrightarrow H'$ , de forma que o núcleo desse homomorfismo é o núcleo de  $\varphi$ .

## 1.9 Produto de Grupos

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

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  $\text{nu } p = 1 \times G'$  e  $\text{nu } p' = G \times 1$ . 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 (Propriedades de Mapeamento dos Produtos):** Seja  $H$  um grupo qualquer. O homomorfismo  $\Phi : H \longrightarrow G \times G'$  tem correspondência biunívoca com o par  $(\varphi, \varphi')$  de homomorfismos

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

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



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:** 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  $s$ .

Em contra partida, 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:** 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:** Sejam  $H$  e  $K$  os subgrupos de um grupo  $G$ . - Se  $H \cap K = \{1\}$ , o mapeamento de produto  $p : H \times K \rightarrow G$  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  $H \times K$ .

## 1.10 Aritmética Modular

**Definição:** Seja  $n \in \mathbb{N}$ . Dizemos que dois inteiros  $a, b$  são *congruentes modulo  $n$* , e escrevemos

$$a \equiv b \pmod{n},$$

se  $n$  divide  $b - a$ , ou se  $b = a + nk$  para algum inteiro  $k$ . Chamamos as classes de equivalência definidas por essa relação de *classes de equivalência módulo  $n$* , ou *classes de resíduo módulo  $n$* .

**Exemplo:** A classe de congruência de 0 é o subgrupo  $\bar{0}$  de todos os múltiplos de  $n$

$$\bar{0} = n\mathbb{Z} = \{\dots, -n, 0, n, 2n, \dots\}.$$

**Proposição:** Há  $n$  classes de congruência módulo  $n$  (denotamos esse conjunto por  $\mathbb{Z}/n\mathbb{Z}$ ), isto é, o índice  $[\mathbb{Z} : n\mathbb{Z}]$  é  $n$ . São elas

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

**Definição:** Seja  $\bar{a}$  e  $\bar{b}$  as classes de congruência representadas pelos inteiros  $a$  e  $b$ . Define-se a *soma* como a classe de congruência de  $a + b$  e o *produto* pela classe de congruência  $ab$ , isto é,

$$\bar{a} + \bar{b} = \overline{a + b} \quad \text{e} \quad \bar{a}\bar{b} = \overline{ab}.$$

**Proposição:** Se  $a' \equiv b' \pmod{n}$  e  $b' \equiv b \pmod{n}$ , então  $a' + b' \equiv a + b \pmod{n}$  e  $a'b' \equiv ab \pmod{n}$ .

Além disso, a soma e produto também continuam respeitando as propriedades associativas, comutativas e distributivas, desde que o mesmo se mantém para soma e multiplicação de inteiros.

**Exemplo:** Seja  $n = 13$ , então

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{12}\}.$$

Com isso,

$$(\bar{7} + \bar{9})(\bar{11} + \bar{6}) = \bar{3} \cdot \bar{4} = \bar{12}.$$

## 1.11 Grupos de Quociente

**Definição:** Seja  $N$  um subgrupo normal de um grupo  $G$ . Então, o produto de duas coclasses  $aN$ ,  $bN$  também é uma coclasse

$$(aN)(bN) = abN.$$

**Definição:** Sejam as coclasses  $C_1, C_2$  e os elementos  $a \in C_1$  e  $b \in C_2$ , então  $C_1 = aN$  e  $C_2 = bN$ . Chamamos de *produto das coclasses*  $C_1$  e  $C_2$  a coclasse  $C_1C_2 = abN$ , isto é, a coclasse que contém  $ab$ .

**Definição:** Assim como usado na seção anterior, é conveniente denotar o *conjunto de coclasses de um subconjunto normal  $N$  de um grupo  $G$*  pela simbologia

$$G/N = \text{conjunto de coclasses de } N \text{ em } G.$$

Também pode-se usar a notação em barra  $G/N = \bar{G}$  e  $aN = \bar{a}$ , tomando o cuidado para diferenciar que  $\bar{a}$  denota a coclasse que contém  $a$ .

**Proposição:** Seja o mapeamento  $\pi : G \longrightarrow \bar{G} = G/N$ , da forma  $a \rightsquigarrow \bar{a} = aN$ , isto é,  $\bar{G}$  é um grupo e o mapeamento  $\pi$  é um homomorfismo com núcleo  $N$ . Então a ordem de  $G/N$  é o índice  $[G : N]$ .

**Proposição:** Todo subgrupo normal de um grupo  $G$  é o núcleo de um homomorfismo.

**Proposição:** Sejam  $G$  um grupo e  $S$  um conjunto qualquer com uma lei de composição. Seja também  $\varphi : G \longrightarrow S$  um mapeamento sobrejetivo tal que  $\varphi(a)\varphi(b) = \varphi(ab)$  para todo  $a, b \in G$ . Então  $S$  é um grupo.

O construção do conceito de *grupo de quociente* é relacionado ao homomorfismo geral de grupo  $\varphi : G \longrightarrow G'$ , como segue:

**Proposição (Primeiro Teorema do Isomorfismo):** Sejam  $\varphi : G \longrightarrow G'$  um homomorfismo de grupo sobrejetivo e  $N$  o núcleo de  $\varphi$ . Então  $G/N$  é isomórfico a  $G'$  pelo mapeamento  $\bar{\varphi}$  que transporta a coclasse  $\bar{a} = aN$  para  $\varphi(a)$ :

$$\bar{\varphi}(\bar{a}) = \varphi(a).$$

Esse é o método fundamental para identificar grupos de quocientes.