Relatório final

“Tópicos pertinentes da Teoria de Grupos”

Orientando: Thiago Moraes Rizzieri

Orientadora: Prof.^{a} Dr^a Eliris Cristina Rizziolli

1 de Junho de 2020 até 24 de fevereiro de 2021

Sumário

Introdução

Admitimos que o leitor tenha familiaridade com a estrutura algébrica dos grupos desde as principais definições bem como resultados importantes.

No primeiro capítulo, começamos introduzindo o leitor aos Teoremas do Isomorfismo e suas demonstrações, que são fundamentais para alguns Teoremas ao longo desse projeto. Logo em seguida, vemos sobre séries de grupos e Teoremas relacionados até concluir com a definição de um grupo solúvel. Logo depois, vemos um pouco sobre definições e preliminares de ação de grupo, para introduzir, por fim, aos Teoremas de Sylow, ao conceito de p-grupo e suas ligações com grupo solúvel.

No segundo capítulo, entramos no conceito de grupos livres e grupos abelianos livres, para introduzir e explorar sobre a presentação de um grupo.

Por fim, vemos aspectos geométricos do complexo simplicial e grupo de homologia. Além de formas visuais de se obter os grupos de homologia, através da triangulação.

Em todos estes capítulos, abordamos temas apresentados no livro [1] do capítulo VII e VIII.

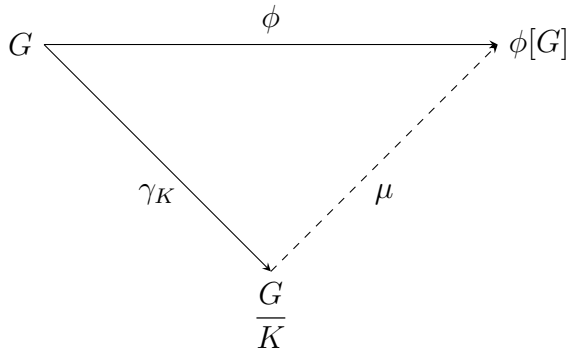
Capítulo 1

Teoremas de Sylow

1.1 Teoremas do Isomorfismo

Existem diversos Teoremas envolvendo isomorfismo entre grupos quocientes na Teoria de Grupos. Neste trabalho, alguns Teoremas e resultados requerem dos Teoremas do Isomorfismo, e assim, iniciamos este capítulo com seus enunciados e devidas demonstrações.

Teorema 1.1. ***(Primeiro Teorema do Isomorfismo)*** *Sejam $\phi : G \to J$ um homomorfismo entre grupos, com núcleo $K = Ker(\phi)$ e $\gamma_k : G \to \dfrac{G}{K}$ o homomorfismo canônico, o qual é definido por $\gamma_K(g) := gK$, $g \in G$. Nessas condições, existe um único isomorfismo $\mu : \dfrac{G}{K} \to \phi[G]$ definido por $\mu(gK) := \phi(g)$ tal que $\phi(g) = \mu(\gamma_K(g))$, ou seja, é válido o seguinte diagrama:*



Demonstração. Primeiramente veja que $\mu(\gamma_k(g)) = \mu(gK) = \phi(g)$.
Mostremos que μ é um isomorfismo:

- μ está bem definido, pois : $\forall aK, bK \in \dfrac{G}{K}$

  $aK = bK \Rightarrow b^{-1}aK = K \Rightarrow (b^{-1}a) \in K = Ker(\phi) \Rightarrow \phi(b^{-1}a) = e \Rightarrow \phi(b^{-1})\phi(a) = e \Rightarrow [\phi(b)]^{-1}\phi(a) = e \Rightarrow \phi(a) = \phi(b) \Rightarrow \mu(aK) = \mu(bK)$.

- μ é um homomorfismo entre grupos, de fato: $\forall aK, bK \in \dfrac{G}{K}$

  $\mu((aK)(bK)) = \mu((ab)K) = \phi(ab) = \phi(a)\phi(b) = \mu(aK)\mu(bK)$.

- μ é injetivo, com efeito: $\forall aK, bK \in \dfrac{G}{K}$

  $\mu(aK) = \mu(bK) \Rightarrow \phi(a) = \phi(b) \Rightarrow [\phi(b)]^{-1}\phi(a) = e \Rightarrow \phi(b^{-1})\phi(a) = e \Rightarrow \phi(b^{-1}a) = e \Rightarrow (b^{-1}a) \in K \Rightarrow b^{-1}aK = K \Rightarrow aK = bK$.

- μ é sobrejetivo, pois: $\forall aK, bK \in \dfrac{G}{K}$

  $\phi[G] = \{\phi(g) | g \in G\} = \{\mu(gK) | gK \in \frac{G}{K}\} = \mu\left[\frac{G}{K}\right]$.

- Veja que μ é o único isomorfismo tal que $\mu \circ \gamma_k = \phi$, de fato: suponha que exista um isomorfismo $\nu : \frac{G}{K} \to \phi[G]$ tal que $\nu \circ \gamma_k = \phi$, mostremos que $\mu = \nu$.

  Seja $gK \in \frac{G}{K}$. Assim, $\nu(gK) = \nu(\gamma_k(g)) = \phi(g) = \mu(\gamma_k(g)) = \mu(gK)$.
  $\therefore \mu = \nu$.

$\therefore \mu$ definido por $\mu(g) := gK$, $g \in G$ é o único isomorfismo tal que $\mu(\gamma_k(x)) = \phi(x)$.

□

No que segue precisamos dos seguintes Teoremas.

Teorema 1.2. *Seja $\phi : G \to G'$ um homomorfismo de grupos. Se N é um subgrupo normal de G, então $\phi[N]$ é um subgrupo normal de $\phi[G]$. Além disso, se N' é um subgrupo normal de $\phi[G]$, então $\phi^{-1}[N]$ é um subgrupo normal de G.*

Demonstração. Lembremos primeiramente que existem três condições equivalentes para que um subgrupo qualquer H de um grupo G seja normal à G.

1. $ghg^{-1} \in H$ para todo $g \in G$ e $h \in H$.
2. $gHg^{-1} = H$ para todo $g \in G$.
3. $gH = Hg$ para todo $g \in G$.

Mostremos que $N \lhd G \Rightarrow \phi[N] \lhd \phi[G]$, de fato:

observe que, pelo item 3, $\phi[N] \lhd \phi[G] \Leftrightarrow \phi(g)\phi[N] = \phi[N]\phi(g)$, $\forall g \in G$.

- Veja que $\phi(g)\phi[N] \subset \phi[N]\phi(g)$, com efeito:

  Seja $\phi(g)\phi(n_1) \in \phi(g)\phi[N]$, qualquer. Como ϕ é um homomorfismo de grupos então $\phi(g)\phi(n_1) = \phi(gn_1) = \phi(n_2g) = \phi(n_2)\phi(g) \in \phi[N]\phi(g)$, para algum $n_2 \in N$, pois $N \lhd G$.
  $\therefore \phi(g)\phi[N] \subset \phi[N]\phi(g)$.

- Veja que $\phi(g)\phi[N] \supset \phi[N]\phi(g)$, pois:

  Seja $\phi(n_3)\phi(g) \in \phi[N]\phi[g]$, qualquer. Como ϕ é um homomorfismo de grupos então $\phi(n_3)\phi(g) = \phi(n_3 g) = \phi(g n_4) = \phi(g)\phi(n_4) \in \phi(g)\phi[N]$, para algum $n_4 \in N$, pois $N \lhd G$.
  $\therefore \phi(g)\phi[N] \supset \phi[N]\phi(g)$.

$\therefore \phi(g)\phi[N] = \phi[N]\phi(g) \Rightarrow \phi[N] \lhd \phi[G]$.

Mostremos que $N' \lhd \phi[G] \Rightarrow \phi^{-1}[N'] \lhd G$, de fato :

observe que, pelo item 1, $\phi^{-1}[N'] \lhd G \Leftrightarrow ghg^{-1} \in \phi^{-1}[N']$, $\forall g \in G$ e $\forall h \in \phi^{-1}[N']$

Como $h \in \phi^{-1}[N'] \Rightarrow \phi(h) \in h \in N'$, assim:

$\therefore \phi^{-1}[N'] \lhd G$.

Corolário 1.3. *Dado $\phi : G \to G'$ um isomorfismo de grupos. Se N é um subgrupo normal à G, então $\phi[N]$ é normal à G' e $G/N \simeq G'/\phi[N]$.*

Demonstração. Como ϕ é um isomorfismo, então $\phi[G] = G'$. Segue do Teorema anterior que $\phi[N]$ é normal à G'.
Iremos mostrar que $\gamma G \to G'/\phi[N]$ é um isomorfismo. De fato:

(provar com teorema do isomorfismo) □

□

Teorema 1.4. *Sejam $\phi : G \to G'$ um homomorfismo e $H = Ker(\phi)$.*
Tem-se:

$$aH = \phi^{-1}[\{\phi(a)\}] = Ha.$$

Demonstração. Observe primeiramente que:

$$\phi^{-1}[\{\phi(a)\}] = \{x \in G | \phi(x) = \phi(a)\}.$$

- $\{x \in G | \phi(x) = \phi(a)\} \subset aH$.

  Suponha $x \in \phi^{-1}[\{\phi(a)\}]$, então $\phi(x) = \phi(a) \Rightarrow \phi(a)^{-1}\phi(x) = e'$, e' sendo o elemento neutro de G', $\phi(a)^{-1}\phi(x) = e' \Rightarrow \phi(a^{-1})\phi(x) = e' \Rightarrow \phi(a^{-1}x) = e' \Rightarrow (a^{-1}x) \in H = Ker(\phi) \Rightarrow (a^{-1}x) = h$, $h \in H$, $(a^{-1}x) = h \Rightarrow x = ah \Rightarrow x \in aH \Rightarrow \{x \in G | \phi(x) = \phi(a)\} \subset aH$.

- $\{x \in G | \phi(x) = \phi(a)\} \supset aH$.

  Seja $\forall y \in aH$, então $y = ah$ para algum $h \in H$.

  Assim, $\phi(y) = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a)$.

  Logo, $y \in \{x \in G | \phi(x) = \phi(a)\} \Rightarrow \{x \in G | \phi(x) = \phi(a)\} \supset aH$.

  $\therefore \{x \in G | \phi(x) = \phi(a)\} = aH$.

  De modo análogo, podemos mostrar que $\{x \in G | \phi(x) = \phi(a)\} = Ha$.

□

Lema 1.5. *Se N é um subgrupo normal de um grupo G e $\gamma : G \to \frac{G}{N}$ é o homomorfismo canônico, então a aplicação ϕ do conjunto A dos subgrupos normais de G contendo N para o conjunto B dos subgrupos normais de $\frac{G}{N}$ é uma correspondência biunívoca, ou seja, dados $A = \{L | L \lhd G, N \subset L\}$ e $B = \{H | H \lhd \frac{G}{N}\}$, segue que a aplicação $\phi : A \to B$ tal que $\phi(L) = \gamma[L]$ é injetiva e sobrejetiva.*

Demonstração. Mostremos primeiramente que:

- ϕ é injetiva.

  Pelo Teorema 1.2, se L é um subgrupo normal à G, então $\phi(L) = \gamma[L]$ é normal ao subgrupo $\gamma[G]$. Além disso, $\gamma[G] = \frac{G}{N} = \phi(G)$, pois γ é um epimorfismo.

  Como, $N \subset L$, para cada $x \in L$, a classe lateral xN está contida em L. Assim, pelo Teorema 1.4, $\gamma^{-1}[\{\phi(L)\}] = \{M \in G | M = \gamma^{-1}[\phi(L)]\} = L$ (pois como $\phi(L) = \gamma[L]$ então $\gamma^{-1}[\phi(L)]$ é igual à L).

  Consequentemente, se L e M são subgrupos normais à G, ambos contendo N, e se $\phi(L) = \phi(M) = H$ então $L = \gamma^{-1}[H] = M$.

  $\therefore \phi$ é injetiva.

- ϕ é sobrejetiva. De fato, seja $H \in B$ qualquer,

  tome $L := \gamma^{-1}[H]$. Veja que:

  - $\gamma^{-1}[H]$ é subgrupo normal de G pelo Teorema 1.2.

- $N \subset \gamma^{-1}[H]$, pois $\{N\} \subset H$ ($\{N\}$ é o elemento neutro de $\frac{G}{N}$), assim $\{N\} \subset H \Rightarrow \gamma^{-1}[\{N\}] \subset \gamma^{-1}[H]$, mas $\gamma^{-1}[\{N\}] = N$, logo: $N \subset \gamma^{-1}[H]$.

Como $\gamma^{-1}[H]$ é subgrupo normal de G e $N \subset \gamma^{-1}[H]$ então $\gamma^{-1}[H] \in A$.

Portanto: $\phi(L) = \phi(\gamma^{-1}[H]) = \gamma[\gamma^{-1}[H]] = H$.

$\therefore \phi$ é sobrejetiva.

□

Definição 1.6. *Sejam H e N subgrupos de um grupo G, quaisquer.*
*Definimos **junção de H com N**, denotado por $H \vee N$, como a interseção de todos os subgrupos de G que contenham o conjunto $HN := \{hn | h \in H, n \in N\}$.*

Lema 1.7. *No contexto da definição 1.6 temos que $H \vee N$ é o menor subgrupo de G que contém HN.*

Demonstração. Temos $H \vee N = \bigcap_{HN \subset L} L$, $\forall L \subset G$.
Observe que $H \vee N$ é subgrupo de G, pois ele é formado por interseções de subgrupos de G . Suponha que L' seja um subgrupo qualquer de G com $HN \subset L'$. Veja que $H \vee N = \bigcap_{HN \subset L} L \subset L'$.
Assim $H \vee N$ é o menor subgrupo de G contendo HN.

□

Lema 1.8. *São válidos as seguintes propriedades:*

(i) Se N é um subgrupo normal à G e H um subgrupo qualquer de G, então $HN = H \vee N = NH$. Ou seja, neste caso, HN e NH são subgrupos de G .

(ii) Caso ambos, H e N, sejam normais à G, então HN também é normal à G.

Demonstração. **(i)** Vamos mostrar que, com essas hipóteses, HN é um subgrupo de G. Assim, como $H \vee N$ é a interseção de todos os subgrupos de G contendo HN, então , $H \vee N = HN$.
Lembremos que HN é um subgrupo de $G \Leftrightarrow ab^{-1} \in HN$, $a, b \in HN$.
Sejam $a = h_1 n_1$ e $b = h_2 n_2$, $h_1, h_2 \in H, n_1, n_2 \in N$.
Dessa maneira, $b^{-1} = (h_2 n_2)^{-1} = n_2^{-1} h_2^{-1} = h_2^{-1} n_3$, para algum $n_3 \in N$, pois N é normal à G.
Assim: $ab^{-1} = (h_1 n_1)(h_2^{-1} n_3) = h_1 (n_1 h_2^{-1}) n_3 = h_1 (h_2^{-1} n_4) n_3 = (h_1 h_2^{-1})(n_4 n_3) \in HN$, para algum $n_4 \in N$, pois N é normal à G.
Um argumento similar mostra que NH também é igual à $H \vee N$.
$\therefore HN = H \vee N = NH$.

(ii) Suponha que H e N sejam subgrupos normais à G e provemos que HN é normal à G. Para tanto, é suficiente mostrar que : $g(h_1n_1)g^{-1} \in HN, \forall g \in G, \forall h_1n_1 \in HN$. Com efeito, temos

$gh_1 = h_2g$ e $n_1g^{-1} = g^{-1}n_2$, para determinados $h_2 \in H$, $n_2 \in N$ pois H e N são subgrupos normais à G.
Assim:

$g(h_1n_1)g^{-1} = (gh_1)(n_1g^{-1}) = (h_2g)(g^{-1}n_2) = h_2(gg^{-1})n_2 = h_2(e)n_2 = h_2n_2 \in HN$.
$\therefore HN$ é normal à G.

□

Teorema 1.9. ***(Segundo Teorema do Isomorfismo)****: Sejam H e N subgrupos do grupo G com N normal à G, então:* $\dfrac{H}{H \cap N} \simeq \dfrac{HN}{N}$.

Demonstração. Primeiramente, precisamos mostrar que $H \cap N$ é normal à H e N é normal à HN.

$H \cap N$ é normal à $H \Leftrightarrow hxh^{-1} \in H \cap N$, $\forall\ h \in H$, $\forall\ x \in H \cap N \subset N$. Observe que existem $x, y \in N$ de modo que $hx = yh$ pois N é normal à G.
Assim: $hxh^{-1} = yhh^{-1} = ye = y \in H \cap N$ pois $y \in N$. Portanto $H \cap N$ é normal à H.

N é normal à $HN \Leftrightarrow znz^{-1} \in N\ \forall\ z \in HN \subset G$, $\forall\ n \in N$. Observe que, dado $z \in G$, $zn = n'z$ para algum $n, n' \in N$ pois N é normal à G.
Assim: $znz^{-1} = n'zz^{-1} = n'e = n' \in N$, ou seja, N é normal à HN.

Seja $\phi : H \to \frac{(HN)}{N}$ definido por $h \mapsto \phi(h) := hN = (hn)N \in \frac{(HN)}{N}$, $\forall h \in H$, $\forall n \in N$.

- ϕ está bem definida:

  Para quaisquer elementos de H :$h_1 = h_2 \Rightarrow h_1N = h_2N \Rightarrow \phi(h_1) = \phi(h_2)$.

- ϕ é um homomorfismo:

  $\phi(h_1h_2) = (h_1h_2)N = (h_1N)(h_2N) = \phi(h_1)\phi(h_2)$.

- ϕ é uma sobrejeção:

  $\phi[H] = \{\phi(h) | h \in H\} = \{hN | h \in H\} = \{(hn)N | h \in H, n \in N\} = \frac{(HN)}{N}$.

- $Ker(\phi) = H \cap N$:

  $Ker(\phi) = \{h \in H | \phi(h) = N\} = \{h \in H | hN = N\} = \{h \in H | h \in N\} = H \cap N$.

Portanto, pelo primeiro Teorema do isomorfismo (Teorema 1.1), $\frac{H}{Ker(\phi)} \simeq \phi[H]$, e portanto, concluímos que $\frac{H}{H \cap N} \simeq \frac{HN}{N}$.

□

Teorema 1.10. ***(Terceiro Teorema do Isomorfismo)*** *Sejam H e K subgrupos normais do grupo G com $K \subset H$, então:* $\frac{G}{H} \simeq \frac{\frac{G}{K}}{\frac{H}{K}}$.

Demonstração. Primeiramente, precisamos mostrar que K é normal à H e $\frac{H}{K}$ é normal à $\frac{G}{K}$.

K é normal à $H \Leftrightarrow hkh^{-1} \in K$ com $\forall k \in K$ e $\forall h \in H$.

Sabemos que $hk = k'h$ para algum $k' \in K$ pois K é normal à G. Assim: $hkh^{-1} = khh^{-1} = ke = k \in K$, ou seja, K é normal à H.

Veja que $\frac{H}{K}$ é normal à $\frac{G}{K} \Leftrightarrow gK(hK)g^{-1}K \in \frac{H}{K}$, $\forall gK \in \frac{G}{K}$, $\forall hK \in \frac{H}{K}$

Sabemos que $(gK)(hK) = (gh)K = (h'g)K = (h'K)(gK)$ para algum $h' \in H$ pois H é normal à G.

Assim: $gK(hK)g^{-1}K = (h'K)(gK)(g^{-1}K) = (h'K)(gg^{-1})K = (h'K)(eK) = (h'e)K = h'K \in \frac{H}{K}$.

Seja $\phi : \frac{G}{K} \to \frac{G}{H}$ definido por $\phi(gK) := gH$, $g \in G$.

- ϕ está bem definida:

  Para quaiquer elementos de gK: $aK = bK \Rightarrow (b^{-1}a)K = K \Rightarrow (b^{-1}a) \in K$, e como $K \subset H$, então $(b^{-1}a) \in H \Rightarrow (b^{-1}a)H = H \Rightarrow aH = bH \Rightarrow \phi(aK) = \phi(bK)$.

- ϕ é um homomorfismo:

  $\phi((aK)(bK)) = \phi((ab)K) = (ab)H = (aH)(bH) = \phi(aK)\phi(bK)$.

- ϕ é sobrejetor:

  $\phi\left[\frac{G}{K}\right] = \{\phi(gK) | g \in G\} = \{gH | g \in G\} = \frac{G}{H}$.

- $Ker(\phi) = \frac{H}{K}$:

  $Ker(\phi) = \{gK \in \frac{G}{K} | \phi(gK) = H\} = \{gK \in \frac{G}{K} | gH = H\} = \{gK \in \frac{G}{K} | g \in H\} = \frac{H}{K}$.

Portanto, pelo primeiro Teorema do isomorfismo, $\frac{\frac{G}{K}}{Ker(\phi)} \simeq \phi\left[\frac{G}{K}\right]$, ou seja, $\frac{\frac{G}{K}}{\frac{H}{K}} \simeq \frac{G}{H}$.

□

A seção à seguir define e trabalha em cima de séries noramis e subnormais de um grupo G, que toma um discernimento maior de G, como saber se ele é um grupo solúvel, por exemplo.

1.2 Séries de Grupos

Nesta seção introduzimos a notação de uma série de um grupo G, o que amplia nossa interpretação sobre a estrutura deste grupo. Ao fim da seção, vemos uma importante definição sobre grupo solúvel.

Séries normais e subnormais

Definição 1.11. ***Série subnormal(ou subvariante)*** *é uma sequência finita $H_0, H_1, \cdots, H_n$ de subgrupos de G tais que $H_i < H_{i+1}$ e H_i seja um subgrupo normal à H_{i+1}.*

Definição 1.12. ***Série normal(ou invariante)*** *é uma sequência finita $H_0, H_1, \cdots, H_n$ de subgrupos normais à G tais que $H_i < H_{i+1}$.*

Para ambos os casos: $H_0 = \{e\}$ e $H_n = G$.

Exemplo 1.13. São séries normais do grupo $\mathbb{Z}$:

$$\{0\} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$$
e
$$\{0\} < 9\mathbb{Z} < \mathbb{Z}.$$

Definição 1.14. *Uma série subnormal (normal) $\{K_j\}$ é um* ***refinamento de uma série subnormal(no*** *$\{H_i\}$ de um grupo G, quando $\{H_i\} \subseteq \{K_j\}$, isto é, se cada H_i for algum K_j.*

Exemplo 1.15. A série: $\{0\} < 72\mathbb{Z} < 24\mathbb{Z} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$ é um refinamento da série:
$\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < \mathbb{Z}$.

Definição 1.16. *Duas séries subnormais(normais) $\{H_i\}$ e $\{K_j\}$ de um mesmo grupo G são ditas* ***isomorfas*** *caso exista uma correspondência isomorfa entre seus grupos quocientes $\left\{\frac{H_{i+1}}{H_i}\right\}$ e $\left\{\frac{K_{j+1}}{K_j}\right\}$.*

Observe que as duas séries devem possuir a mesma quantidade de grupos para serem candidatas à serem isomorfas.

Exemplo 1.17. Sejam as duas séries de $\mathbb{Z}_{15}$:

$$\{0\} < \langle 5\rangle < \mathbb{Z}_{15}$$
e
$$\{0\} < \langle 3\rangle < \mathbb{Z}_{15}.$$

Os grupos quocientes da primeira série são: $\frac{\mathbb{Z}_{15}}{\langle 5\rangle}$ e $\frac{\langle 5\rangle}{\langle 0\rangle}$. Da segunda série são: $\frac{\mathbb{Z}_{15}}{\langle 3\rangle}$ e $\frac{\langle 3\rangle}{\langle 0\rangle}$
Podemos observar que $\frac{\mathbb{Z}_{15}}{\langle 5\rangle} \simeq \frac{\langle 3\rangle}{\langle 0\rangle}$ e $\frac{\langle 5\rangle}{\langle 0\rangle} \simeq \frac{\mathbb{Z}_{15}}{\langle 3\rangle}$, assim, as séries são isomorfas.

Teorema de Schreier

Proseguiremos com uma demonstração de que duas séries subnormais de um grupo G possui refinamentos isomorfos. Para sua demonstração, precisamos enunciar e demonstrar o lema à seguir.

Lema 1.18. ***(Lema de Zassenhaus)*** *Sejam H e K subgrupos do grupo G e H^* e K^* subgrupos normais à H e K respectivamente, então:*

1. *$H^*(H \cap K^*)$ é normal à $H^*(H \cap K)$;*

2. *$K^*(H^* \cap K)$ é normal à $K^*(H \cap K)$;*

3. $\frac{H^*(H\cap K)}{H^*(H\cap K^*)} \simeq \frac{K^*(H\cap K)}{H^*(H^*\cap K)} \simeq \frac{(H\cap K)}{(H^*\cap K)(H\cap K^*)}$.

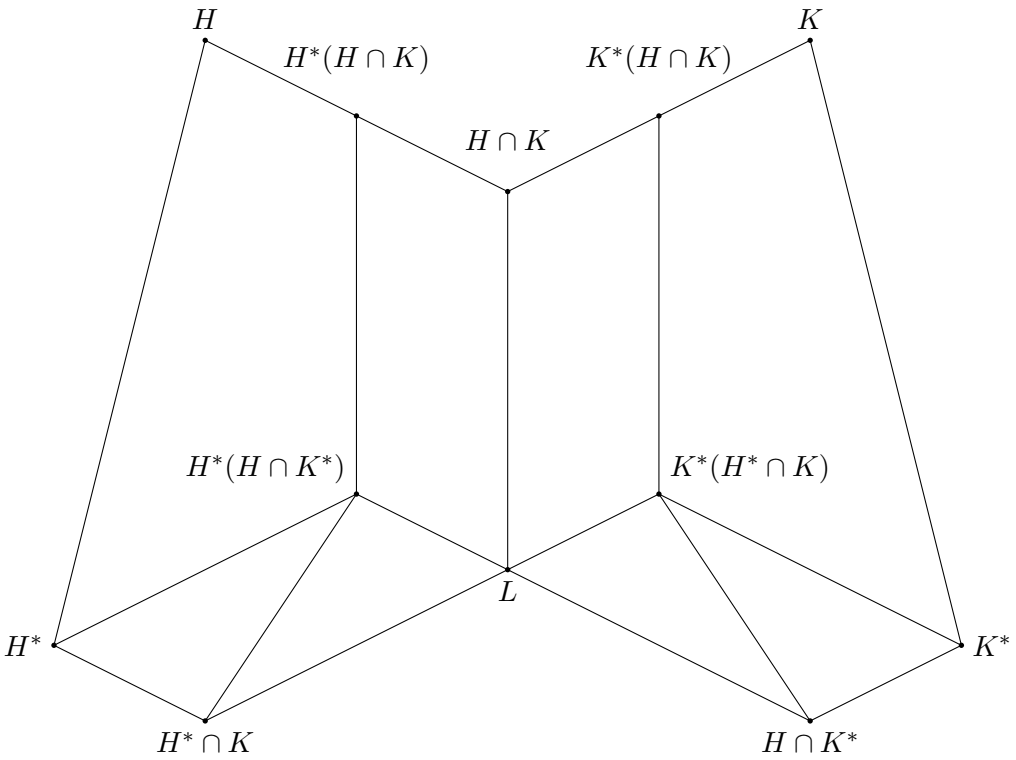
Demonstração. Sejam H e K subgrupos do grupo G. Além disso, sejam H^* normal à H e K^* normal à K.

Pelo item (i) do Lema 1.8, como H^* é normal à H e $H \cap K$ é um subgrupo de H. Logo, $(H^*) \vee (H \cap K) = H^*(H \cap K)$ é um subgrupo de H. Analogamente, temos que $H^*(H \cap K^*)$ é subgrupo de H e $K^*(H \cap K)$ e $K^*(H^* \cap K)$ são subgrupos de K.

Observe que $H^* \cap K$ e $H \cap K^*$ são subgrupos normais à $H \cap K$, de fato.
$x(H^* \cap K) = (H^* \cap K)x$, $\forall x \in H \cap K$, ou seja, $x \in H$ e $x \in K$. Sendo $xz \in x(H^* \cap K)$, temos $xz = z'x$ para algum $z' \in H^* \cap K$ pois $H^* \lhd H$. Assim, $xz = z'x \in (H^* \cap K)x$. De mesma forma, sendo $zx \in (H^* \cap K)x$, temos $zx = xz'$ para algum $z' \in H^* \cap K$ pois $H^* \lhd H$. Como $x(H^* \cap K) \subset H^* \cap Kx$ e $x(H^* \cap K) \supset (H^* \cap K)x$, então $x(H^* \cap K) = (H^* \cap K)x$. De forma análoga, $H \cap K^*$ é normal à $H \cap K$.

Assim, pelo item (ii) do Lema 1.8, temos que $L := (H^* \cap K)(H \cap K^*)$ também é um subgrupo normal à $H \cap K$.

Temos o seguinte diagrama de subgrupos (o lema é conhecido como "Lema da Borboleta" devido à este diagrama):



Para provar os três itens do Lema de Zassenhaus, iremos utilizar o Primeiro Teorema do Isomorfismo, Teorema 1.1, para as aplicações:

$$\begin{aligned} \alpha : H^*(H \cap K) &\to \frac{H \cap K}{L} \\ hx &\mapsto \alpha(hx) := xL \end{aligned}$$

$$e$$

$$\begin{aligned} \beta : K^*(H \cap K) &\to \frac{H \cap K}{L} \\ kx &\mapsto \beta(kx) := xL \end{aligned}$$

com $h \in H^*, k \in K^*$ e $x \in H \cap K$. Vamos apenas aplicar o Primeiro Teorema do isomorfismo para o α, pois para β será uma solução análoga.

- α está bem definido, pois: sejam $h_1, h_2 \in H^*$ e $x_1, x_2 \in H \cap K$ quaisquer.

Se $h_1x_1 = h_2x_2 \Rightarrow h_2^{-1}h_1 = x_2x_1^{-1}$ temos que $h_2^{-1}h_1 \in H^*$ e $x_2x_1^{-1} \in H \cap K$
$\Rightarrow h_2^{-1}h_1 = x_2x_1^{-1} \in H^* \cap (H \cap K)$.
Como H^* é um subgrupo de H: $H^* \cap (H \cap K) = H^* \cap K \subseteq L$.
Assim, $x_2x_1^{-1} \in L \Rightarrow x_2L = x_1L \Rightarrow \alpha(h_2x_2) = \alpha(h_1x_1)$.

- α é um homomorfismo, de fato: sejam $h_1x_1, h_2x_2 \in H^*(H \cap K)$.

$\alpha((h_1x_1)(h_2x_2)) = \alpha(h_1(x_1h_2)x_2) = \alpha(h_1(h_3x_1)x_2)$, para algum $h_3 \in H^*$, pois $H^* \lhd H$, $\alpha(h_1(h_3x_1)x_2) = \alpha((h_1h_3)(x_1x_2)) = (x_1x_2)L = (x_1L)(x_2L) = \alpha(h_1x_1)\alpha(h_2x_2)$.

- α é sobrejetor, pois:

$$\alpha[H^*(H \cap K)] = \{\alpha(hx)|h \in H^*, x \in H \cap K\} = \{xL|x \in H \cap K\} = \frac{H \cap K}{L}$$

- $Ker(\alpha) = H^*(H \cap K^*)$, de fato:

$$\begin{aligned} Ker(\alpha) &= \{hx|\alpha(hx) = L, h \in H^*, x \in H \cap K\} \\ &= \{hx|xL = L, h \in H^*, x \in H \cap K\} \\ &= \{hx|h \in H^*, x \in L\} \\ &= H^*L = H^*(H^* \cap K)(H \cap K^*) = H^*(H \cap K^*) \end{aligned}$$

Assim, como o núcleo de um homomorfismo é sempre normal ao domínio, o item 1 é satisfeito: $(H^*(H \cap K^*) \lhd H^*(H \cap K))$. O mesmo acontece ao analizar β que satisfaz o item 2 $:(K^*(H^* \cap K) \lhd K^*(H \cap K))$.

Pelo Pimeiro Teorema do Isomorfismo (Teorema 1.1), então $\frac{H^*(H \cap K)}{Ker(\alpha)} \simeq \alpha[H^*(H \cap K)]$ e $\frac{K^*(H \cap K)}{Ker(\beta)} \simeq \beta[K^*(H \cap K)]$, ou seja, $\frac{H^*(H \cap K)}{H^*(H \cap K^*)} \simeq \frac{H \cap K}{L}$ e $\frac{K^*(H \cap K)}{K^*(H^* \cap K)} \simeq \frac{H \cap K}{L}$ que satisfaz o item 3.

□

Teorema 1.19. ***(Teorema de Schreier)*** *Dadas duas séries subnormais(normais) de um grupo G, existem respectivos refinamentos isomorfos.*

Demonstração. Sejam G um grupo e

$$\{e\} = H_0 < H_1 < H_2 < \ldots < H_n = G \tag{1.1}$$
$$\{e\} = K_0 < K_1 < K_2 < \ldots < K_m = G \tag{1.2}$$

duas séries subnormais de G. No que segue, construímos refinamentos para (1.1) e (1.2) respectivamente de modo que tais refinamentos sejam isomorfos.
Inicialmente, para cada i com $0 \leq i \leq n-1$, formamos uma cadeia de grupos, da seguinte maneira:

$$H_i = H_i(H_{i+1} \cap K_0) \leq H_i(H_{i+1} \cap K_1) \leq \ldots \leq H_i(H_{i+1} \cap K_m) = H_{i+1}$$

Agora, defina $H_{i,j} := H_i(H_{i+1} \cap K_j)$ em que $0 \leq j \leq m$, consequentemente dessa definição segue de modo natural a seguinte cadeia de grupos:

$$\begin{aligned} \{e\} = H_{0,0} &\leq H_{0,1} \leq H_{0,2} \leq \ldots \leq H_{0,m-1} \leq H_{0,m} = H_{1,0} = H_1 \\ &\leq H_{1,1} \leq H_{1,2} \leq \ldots \leq H_{1,m-1} \leq H_{1,m} = H_{2,0} = H_2 \\ &\leq \ldots \\ &\leq H_{n-1,1} \leq H_{n-1,2} \leq \ldots \leq H_{n-1,m-1} \leq H_{n-1,m} = H_{n,0} = H_n = G. \end{aligned} \tag{1.3}$$

Essa cadeia tem $nm+1$ grupos, que não necessariamente são distintos, e $H_{i,0} = H_i$ para cada i. Pelo item 1 do Lema de Zassenhaus, como K_j é normal à K_{j+1}, então $H_i(H_{i+1} \cap K_j)$ é normal à $H_i(H_{i+1} \cap K_{j+1})$. Assim, a cadeia (1.3) é uma cadeia subnormal para a série subnormal (1.1), ou seja, essa cadeia refina a série (1.1).

De mesmo modo, definimos $K_{j,i} := K_j(K_{j+1} \cap H_i)$ em que $0 \leq j \leq m-1$ e $0 \leq i \leq n$ e obtemos a seguinte cadeia:

$$\begin{aligned} \{e\} = K_{0,0} &\leq K_{0,1} \leq K_{0,2} \leq \ldots \leq K_{0,n-1} \leq K_{0,n} = K_{1,0} = K_1 \\ &\leq K_{1,1} \leq K_{1,2} \leq \ldots \leq K_{1,n-1} \leq K_{1,n} = K_{2,0} = K_2 \\ &\leq \ldots \\ &\leq K_{m-1,1} \leq K_{m-1,2} \leq \ldots \leq K_{m-1,n-1} \leq K_{m-1,n} = K_{m,0} = K_m = G. \end{aligned} \tag{1.4}$$

Essa cadeia tem $nm+1$ grupos, que não necessariamente são distintos, e $K_{j,0} = K_j$ para cada i. Pelo item 1 do Lema de Zassenhaus, $K_j(K_{j+1} \cap H_i)$ é normal à $K_j(K_{j+1} \cap H_{i+1})$, e com isso obtemos que a cadeia (1.4) refina série (1.2).
No que segue, mostramos que a partir de $H_{i,j}$ e $K_{j,i}$ de K_j é possível obter refinamentos isomorfos de H_i e K_j respectivamente, para tanto observe que pelo item 3 do Lema de Zassenhaus, Lema 1.18, temos:

$$\frac{H_i(H_{i+1} \cap K_{j+1})}{H_i(H_{i+1} \cap K_j)} \simeq \frac{K_j(K_{j+1} \cap H_{i+1})}{K_j(K_{j+1} \cap H_i)}$$

ou seja

$$\frac{H_{i,j+1}}{H_{i,j}} \simeq \frac{K_{j,i+1}}{K_{j,i}} \tag{1.5}$$

para $0 \leq i \leq n-1$ e $0 \leq j \leq m-1$. Do isomorfismo (1.5) segue que existe uma correspondência biunívoca de grupos quocientes isomorfos entre as cadeias subnormais (1.3) e (1.4), de fato, para verificar essa correspondencia veja que $H_{i,0} = H_i$, e $H_{i,m} = H_{i+1}$, onde $K_{j,0} = K_j$ e $K_{j,n} = K_{j+1}$. Ainda, cada cadeia (1.3) e (1.4) contem uma "matriz" retangular de mn símbolos de $\leq$, em que cada $\leq$ da origem à um grupo quociente. Os grupos quocientes que aparecem na r-ésima linha da cadeia (1.3) corresponde aos grupos quocientes que aparecem na r-ésima coluna da cadeia (1.4). Após deletar grupos repetidos nas cadeias (1.3) e (1.4) obtemos séries subnormal de grupos distintos os quais são refinamento isomorfos da série (1.1) e (1.2). Ou seja, provamos o Teorema para o caso de séries subnormal.
No caso de séries normal, em que H_i e K_j são normais em G a demonstração é praticamente a mesma bastando apenas observar que os grupos $H_{i,j}$ e $K_{j,i}$, definidos anteriormente, são também normais em G. Cujas normalidades são justificadas através do item 2 do lema 1.5 e do fato de que interseções de subgrupos normais de um grupo ainda são subgrupos normais.

□

Exemplo 1.20. Vamos encontrar os refinamentos isomorfo das seguintes séries:

$$\{0\} < 10\mathbb{Z} < \mathbb{Z} \tag{1.6}$$

$$\{0\} < 25\mathbb{Z} < \mathbb{Z}. \tag{1.7}$$

Com efeito, considerando $H_0 = \{0\}$, $H_1 = 10\mathbb{Z}$, $H_2 = \mathbb{Z}$, $K_0 = \{0\}$, $K_1 = 25\mathbb{Z}$, $K_2 = \mathbb{Z}$, temos:

$$\begin{gathered}
H_{0,0} = H_0 + (H_1 \cap K_0) = \{0\} + (10\mathbb{Z} \cap \{0\}) = \{0\}, \\
H_{0,1} = H_0 + (H_1 \cap K_1) = \{0\} + (10\mathbb{Z} \cap 25\mathbb{Z}) = 50\mathbb{Z}, \\
H_{0,2} = H_{1,0} = H_1 = 10\mathbb{Z}, \\
H_{1,1} = H_1 + (H_2 \cap K_1) = 10\mathbb{Z} + (\mathbb{Z} \cap 25\mathbb{Z}) = 10\mathbb{Z} + 25\mathbb{Z} = 5\mathbb{Z}, \\
H_{1,2} = H_{2,0} = H_2 = \mathbb{Z}.
\end{gathered}$$

$$\begin{gathered}
K_{0,0} = K_0 = \{0\}, \\
K_{0,1} = K_0 + (K_1 \cap H_1) = \{0\} + (25\mathbb{Z} \cap 10\mathbb{Z}) = 50\mathbb{Z}, \\
K_{0,2} = K_{1,0} = K_1 = 25\mathbb{Z}, \\
K_{1,1} = K_1 + (K_2 \cap H_1) = 25\mathbb{Z} + (\mathbb{Z} \cap 10\mathbb{Z}) = 25\mathbb{Z} + 10\mathbb{Z} = 5\mathbb{Z}, \\
K_{1,2} = K_{2,0} = K_2 = \mathbb{Z}.
\end{gathered}$$

Então os respectivos refinamentos isomorfos de $\{H_i\}$ e $\{K_j\}$, $i = 0, 1, 2$, são:

$$\{0\} < 50\mathbb{Z} < 10\mathbb{Z} < 5\mathbb{Z} < \mathbb{Z} \tag{1.8}$$

$$\{0\} < 50\mathbb{Z} < 25\mathbb{Z} < 5\mathbb{Z} < \mathbb{Z} \tag{1.9}$$

com $\dfrac{\mathbb{Z}}{5\mathbb{Z}} \simeq \dfrac{\mathbb{Z}}{5\mathbb{Z}}$, $\dfrac{5\mathbb{Z}}{10\mathbb{Z}} \simeq \dfrac{25\mathbb{Z}}{50\mathbb{Z}}$, $\dfrac{10\mathbb{Z}}{50\mathbb{Z}} \simeq \dfrac{5\mathbb{Z}}{25\mathbb{Z}}$ e $\dfrac{50\mathbb{Z}}{\{0\}} \simeq \dfrac{50\mathbb{Z}}{\{0\}}$.

Ainda, cada série (1.8) e (1.9) contem uma "matriz" retangular de mn símbolos de $\leq$, em que cada $\leq$ da origem à um grupo quociente. Os grupos quocientes que aparecem na r-ésima linha da cadeia (1.8) corresponde aos grupos quocientes que aparecem na r-ésima coluna da cadeia (1.9). Após deletar grupos repetidos nas cadeias (1.8) e (1.9) obtemos séries subnormal de grupos distintos os quais são refinamento isomorfos da série (1.6) e (1.7). Assim as "matrizes" das séries (1.8) e (1.9) poderíam ser vizualizadas pelas respectivas matrizes:

$$\begin{bmatrix} 50\mathbb{Z}\backslash\{0\} & 10\mathbb{Z}\backslash 50\mathbb{Z} \\ 5\mathbb{Z}\backslash 10\mathbb{Z} & \mathbb{Z}\backslash\mathbb{Z} \end{bmatrix}$$

e

$$\begin{bmatrix} 50\mathbb{Z}\backslash\{0\} & 25\mathbb{Z}\backslash 50\mathbb{Z} \\ 5\mathbb{Z}\backslash 25\mathbb{Z} & \mathbb{Z}\backslash\mathbb{Z} \end{bmatrix}.$$

Relembremos que um grupo é dito simples quando possui apenas dois subgrupos normais: ele mesmo e o subgrupo trivial. Alem disso, dizemos que um subgrupo normal M de G é um subgrupo maximal de G caso não há um subgrupo próprio normal N de G com $M \subset N$ e $M \neq N$.

Teorema de Jordan-Hölder

Nas palavras do autor, "chegamos no filé dessa teoria".

Definição 1.21. ***(Série de composição)*** *Uma série subnormal $\{H_i\}$ de um grupo G é uma* ***série de composição*** *se todos os seus grupos quocientes H_{i+1}/H_i forem simples.*

Definição 1.22. ***(Série principal)*** *Uma série normal $\{H_i\}$ de um grupo G é uma* ***série principal*** *se todos os seus grupos quocientes H_{i+1}/H_i forem simples.*

Observe que as séries de composição (ou principais) não podem ser refinadas. Isso devido ao Teorema à seguir.

Teorema 1.23. *M é um subgrupo normal maximal de $G \Leftrightarrow G/M$ é simples.*

Demonstração. ($\Rightarrow$) Seja M um subgrupo normal maximal de G qualquer. Considere o homomorfismo canônico $\gamma : G \to G/M$, veja que, a imagem inversa através de γ de qualquer subgrupo proprio normal de G/M deve ser um subgrupo próprio normal de G que contém M. Mas como M é maximal, esse subgrupo não pode existir. Portanto G/M é simples.

($\Leftarrow$) Suponha agora que G/M é simples. Veja que, pelo Teorema 1.2, se N é um subgrupo normal de G devidamente contendo M, então $\gamma[N]$ é normal em G/M. Se também $N \neq G$, então $\gamma[N] \neq G/M$ e $\gamma[N] \neq \{M\}$. Como G/M é simples então $\gamma[N]$ não pode existir que implica que N não pode existir e, portanto, M é maximal.

□

Teorema 1.24. ***(Teorema de Jordan-Hölder)*** *Quaisquer duas séries de composição (ou principal) de um grupo G são isomorfas.*

Demonstração. Sejam $\{H_i\}$ e $\{K_j\}$ duas séries de composição (ou principais) de G. Dessa maneira, pelo Teorema 1.23, as séries não podem ser mais refinadas além do que já são, ou seja, as séries $\{H_i\}$ e $\{K_j\}$ necessariamente elas mesmas em seus próprios refinamentos isomórfos cuja existência são garantidas pelo Teorema de Schreier (Teorema 1.19). □

Teorema 1.25. *Se G possui uma série de composição (ou principal) e N for um subgrupo normal próprio de G, então existe uma série de composição (ou principal) que contém N.*

Demonstração. Primeiramente, observe que a série $\{e\} < N < G$ é subnormal e normal. Como por hipótese, G possui uma série de composição $\{H_i\}$, então pelo Teorema de Schreier (Teorema 1.19), existe um refinamento da série $\{e\} < N < G$ tal que seja isomorfa ao refinamento de $\{H_i\}$. Mas como $\{H_i\}$ é uma série de composição segue que, pelo Teorema 1.23, ele não possui mais refinamentos além do que já são. Assim, podemos refinar $\{e\} < N < G$ à uma série de composição isomorfa à $\{H_i\}$. Um argumento similar mostra que isso é válido para uma série principal $\{K_j\}$. □

Exemplo 1.26. Uma série de composição (e principal também) de $\mathbb{Z}_4 \times \mathbb{Z}_9$ contendo o subgrupo normal $N = \langle (0,1) \rangle$ é

$$\{(0,0)\} < \langle (0,3) \rangle < \langle (0,1) \rangle < \langle 2 \rangle \times \langle 1 \rangle < \langle 1 \rangle \times \langle 1 \rangle = \mathbb{Z}_4 \times \mathbb{Z}_9.$$

Definição 1.27. *Um grupo G é **solúvel** se ele possui uma série de composição $\{H_i\}$ tal que todos os grupos quocientes $\dfrac{H_{i+1}}{H_i}$ sejam abelianos.*

Vemos pelo Teorema Jordan-Hölder (Teorema 1.24), que para um grupo solúvel, *todas* todas as séries de composição tem os grupos quocientes $\dfrac{H_{i+1}}{H_i}$ abelianos.

Exemplo 1.28. O grupo S_3 é solúvel, pois a série de composição

$$\{e\} < A_3 < S_3$$

possui grupos quocientes isomorfos ao $\mathbb{Z}_3$ e $\mathbb{Z}_2$ que são abelianos. Já o grupo S_5, não é solúvel pois como A_5 é simples, então

$$\{e\} < A_5 < S_5$$

é uma série de composição e $A_5/\{e\}$, é isomorfo ao A_5, que não é abeliano. Esse grupo A_5 de ordem 60 é o menor grupo que não é solúvel.
Esse fato está diretamente relacionado em que um polinômio de grau 5 , geralmente, não pode ser resolvido por radicais, tanto que até hoje não existe uma fórmula para a sua solução, diferente dos polinômios de grau ≤ 4.

Série central ascendente

Uma série subnormal de um grupo G pode ser formada usando centros de grupo. Lembrando que o centro de um grupo G é dado por

$$Z(G) = \{z \in G | zg = gz \text{ para todo } g \in G\},$$

e que $Z(G)$ é normal à G. Podemos então formar o grupo quociente $G/Z(G)$ e encontrar seu centro $Z(G/Z(G))$. Como $Z(G/Z(G))$ é normal à $G/Z(G)$, $\gamma : G \to G/Z(G)$ é o homomorfismo canônico e $\gamma^{-1}[Z(G/Z(G)] \to G$ a sua imagem inversa. Então pelo Teorema 1.2, a imagem inversa $\gamma^{-1}[Z(G/Z(G)]$ é o subgrupo normal de G, denotado por $Z_1(G)$.
Assim podemos formar o grupo quociente $G/Z_1(G)$ e encontrar seu centro $Z(G/Z_1(G))$. Como $Z(G/Z_1(G))$ é normal à $G/Z_1(G)$, $\gamma : G \to G/Z_1(G)$ é o homomorfismo canônico e $\gamma^{-1}[Z(G/Z_1(G)] \to G$ a sua imagem inversa. Então pelo Teorema 1.2, a imagem inversa $\gamma^{-1}[Z(G/Z_1(G)]$ é o subgrupo normal de G, denotado por $Z_2(G)$, e assim por diante.
A série

$$\{e\} \leq Z(G) \leq Z_1(G) \leq Z_2(G) \leq \dots$$

Definição 1.29. *Uma série subnormal de G que satisfaz as condições acima é chamada* ***série central ascendente do grupo*** *G.*

Exemplo 1.30. O centro de S_3, $Z(S_3)$, é dado por $\{\rho_0\}$ onde ρ_0 é a identidade. Assim, podemos formar o grupo quociente $S_3/Z(S_3) = S_3/\{\rho_0\}$ e encontrar seu centro $Z(S_3/Z(S_3)) = \{\rho_0\}$. Como $Z(S_3/Z(S_3))$ é normal à $S_3/Z(S_3)$, $\gamma : S_3 \to S_3/Z(S_3)$ é o homomorfismo canônico e $\gamma^{-1}[Z(S_3/Z(S_3)] \to S_3$ a sua imagem inversa. Então pelo Teorema 1.2, a imagem inversa $\gamma^{-1}[Z(S_3/Z(S_3)] = \gamma^{-1}[\{\rho_0\}] = \{\rho_0\}$ é o subgrupo normal de G, denotado por $Z_1(G)$.

Daqui por diante, os próximos grupos dessa série será sempre $\{\rho_0\}$. Assim a série central ascendente de S_3 é

$$\{\rho_0\} \leq \{\rho_0\} \leq \{\rho_0\} \leq \cdots .$$

Exemplo 1.31. Nesse exemplo, iremos analizar a série central ascendente do grupo D_4 das simetrias do quadrado. Lembremos que $D_4 = \{\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \delta_1, \delta_2\}$, cuja tábua é dada pela Tabela 1.2.

O centro do grupo D_4 das simetrias do quadrado, $Z(D_4)$, é $\{\rho_0, \rho_2\}$.

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

Tabela 1.1: Tábua Composição em D_4

Como $Z(D_4)$ é normal à D_4 podemos formar o grupo quociente $D_4/Z(D_4) = \{\rho_0 \circ \{\rho_0, \rho_2\}, \rho_1 \circ \{\rho_0, \rho_2\}, \mu_1 \circ \{\rho_0, \rho_2\}, \delta_1 \circ \{\rho_0, \rho_2\}\}$ e encontrar seu centro $Z(D_4/Z(D_4))$.

Como $Z(D_4/Z(D_4))$ é normal à $D_4/Z(D_4)$, $\gamma : D_4 \to D_4/Z(D_4)$ é o homomorfismo canônico e $\gamma^{-1}[Z(D_4/Z(D_4))] \to D_4$ a sua imagem inversa. Então pelo Teorema 1.2, a imagem inversa $\gamma^{-1}[Z(D_4/Z(D_4))]$ é o subgrupo normal de D_4, denotado por $Z_1(D_4)$.

Perceba que $D_4/Z(D_4)$ é um grupo abeliano, logo $Z(D_4/Z(D_4)) = D_4/Z(D_4)$ e por consequência $Z_1(D_4) = \gamma^{-1}[Z(D_4/Z(D_4))] = \gamma^{-1}[D_4/Z(D_4)] = D_4$.

Assim, podemos formar o grupo quociente $D_4/Z_1(D_4) = D_4/D_4 = \{\rho_0\}$ e encontrar seu centro $Z(\{\rho_0\}) = \{\rho_0\}$. Como $Z(D_4/Z_1(D_4))$ é normal à $D_4/Z_1(D_4)$, $\gamma : D_4 \to D_4/Z_1(D_4)$ é o homomorfismo canônico e $\gamma^{-1}[Z(D_4/Z_1(D_4))] \to D_4$ a sua imagem inversa. Então pelo Teorema 1.2, a imagem inversa $\gamma^{-1}[Z(D_4/Z_1(D_4))] = \gamma^{-1}[\{\rho_0\}] = D_4$ é o subgrupo normal de D_4, denotado por $Z_2(D_4)$.

Daqui por diante, os próximos grupos dessa série são sempre o grupo D_4. Portanto, a série central ascendente de D_4 é

$$\{\rho_0\} \leq \{\rho_0, \rho_2\} \leq D_4 \leq D_4 \leq \cdots .$$

1.3 Ação de grupo em um conjunto

Quando trabalhamos com um grupo, vemos o que seus elementos fazem com demais elementos, caindo em resultados que ainda pertencem ao próprio grupo. Nesta seção, veremos o que acontece quando os elementos de um grupo "interagem" com os elementos de um conjunto qualquer.

Definição 1.32. *Sejam X um conjunto e $(G, *)$ um grupo. Uma **ação de** G **em** X é uma aplicação, em que denotamos $*(g, x)$ por $g * x$ ou por gx, $* : G \times X \to X$ tal que*

1. *Para todo $x \in X : e * x = x$;*

2. *Para todo $x \in X$ e todo $g_1, g_2 \in G : (g_1 * g_2) * (x) = g_1 * (g_2 * x)$.*

Nesse caso dizemos que X é um G-conjunto.

Exemplo 1.33. Seja D_4 o grupo de simetrias do quadrado. Na Figura 1.33, está nomeado algumas partes do quadrado. Os vértices são $1, 2, 3, 4$, os lados do quadrado são s_1, s_2, s_3, s_4, as diagonais são d_1, d_2, centro do quadrado C, o ponto médio P_i de cada lado s_i e o segmento de P_1 até P_3, m_1, e o segmento de P_2 até P_4, m_2.

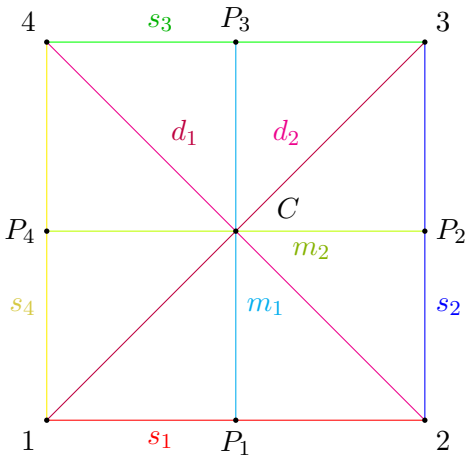


Figura 1.32.

Assim, seja $X = \{1, 2, 3, 4, s_1, s_2, s_3, s_4, m_1, m_2, d_1, d_2, C, P_1, P_2, P_3, P_4\}$. A Tabela 1.2 descreve a ação de D_4 em X.

	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_0	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_1	2	3	4	1	s_2	s_3	s_4	s_1	m_2	m_1	d_2	d_1	C	P_2	P_3	P_4	P_1
ρ_2	3	4	1	2	s_3	s_4	s_1	s_2	m_1	m_2	d_1	d_2	C	P_3	P_4	P_1	P_2
ρ_3	4	1	2	3	s_4	s_1	s_2	s_3	m_2	m_1	d_2	d_1	C	P_4	P_1	P_2	P_3
μ_1	2	1	4	3	s_1	s_4	s_3	s_2	m_1	m_2	d_2	d_1	C	P_1	P_4	P_3	P_2
μ_2	4	3	2	1	s_3	s_2	s_1	s_4	m_1	m_2	d_2	d_1	C	P_3	P_2	P_1	P_4
δ_1	3	2	1	4	s_2	s_1	s_4	s_3	m_2	m_1	d_1	d_2	C	P_2	P_1	P_4	P_3
δ_2	1	4	3	2	s_4	s_3	s_2	s_1	m_2	m_1	d_1	d_2	C	P_4	P_3	P_2	P_1

Tabela 1.2: Ação de D_4 em X.

Veja que X é um D_4-conjunto.

Subgrupo de Isotropia

Seja X um G-conjunto, dado que $x \in X$ e $g \in G$. Antes de prosseguir com o próximo Teorema, é interessante saber quando temos $gx = x$. Para isso iremos denotar os seguintes conjuntos. :

$$X_g = \{x \in X | gx = x\}; \tag{1.10}$$

para cada $g \in G$ e

$$G_x = \{g \in G | gx = x\}. \tag{1.11}$$

para cada $x \in X$.

Exemplo 1.34. No caso do D_4-conjunto X do exemplo anterior, temos

$$\begin{gathered}
X_{\rho_0} = X, \\
X_{\rho_1} = \{C\}, \\
X_{\rho_2} = \{m_1, m_2, d_1, d_2, C\}, \\
X_{\rho_3} = \{C\}, \\
X_{\mu_1} = \{s_1, s_3, m_1, m_2, C, P_1, P_3\}, \\
X_{\mu_2} = \{s_2, s_4, m_1, m_2, C, P_2, P_4\}, \\
X_{\delta_1} = \{2, 4, d_1, d_2, C\}, \\
X_{\delta_2} = \{1, 3, d_1, d_2, C\}, \\
G_1 = G_3 = \{\rho_0, \rho_2\}, \\
G_2 = G_4 = \{\rho_0, \rho_1\}, \\
G_{s_1} = G_{s_3} = G_{P_1} = G_{P_3} = \{\rho_0, \mu_1\}, \\
G_{s_2} = G_{s_4} = G_{P_2} = G_{P_4} = \{\rho_0, \mu_2\}, \\
G_{m_1} = G_{m_2} = \{\rho_0, \rho_2, \mu_1, \mu_2\}, \\
G_{d_1} = G_{d_2} = \{\rho_0, \rho_2, \delta_1, \delta_2\}, \\
G_C = G.
\end{gathered}$$

Teorema 1.35. *Se X um G-conjunto então G_x é um subgrupo de G para cada $x \in X$.*

Demonstração. Sejam $g_1, g_2 \in G_x$. Assim, $g_1 x = x$ e $g_2 x = x$. Consequentemente

$$g_2 x = x \Rightarrow g_1(g_2 x) = g_1 x \Rightarrow (g_1 g_2)x = g_1 x = x$$

e então $g_1 g_2 \in G_x$, o que mostra que G_x é fechado para a operação de G. Sabemos que seus elementos satisfazem a associatividade por pertencerem à G e que $ex = x$, garantindo que $e \in G_x$. Além disso, veja que dado $g_1 x = x$, temos,

$$g_1^{-1}(g_1 x) = g_1^{-1} x \Rightarrow (g_1^{-1} g_1)x = g_1^{-1} \Rightarrow ex = g_1^{-1} x \Rightarrow x = g_1^{-1} x$$

e assim, $g_1^{-1} \in G_x$, garantindo a existência do elemento inverso em G_x.

Portanto, G_x é subgrupo de G. □

Definição 1.36. *Denotamos o subgrupo G_x como o subgrupo de isotropia de x.*

Órbitas

Teorema 1.37. *Seja X um G-conjunto. Para cada x_1,$x_2 \in X$, seja $x_1 \sim x_2$ se e somente se existe $g \in G$ tal que $gx_1 = x_2$. Então $\sim$ é uma relação de equivalência.*

Demonstração. Para mostrar que é uma relação de equivalência, essa relção deve ser reflexiva, simétrica e transitiva.

- Para cada $x \in X$, nós temos $ex = x$, então $x \sim x$ e $\sim$ é reflexiva.
- Suponha que $x_1 \sim x_2$, assim $gx_1 = x_2$ para algum $g \in G$. Então $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = ex_1 = x_1$, portanto $x_2 \sim x_1$ e $\sim$ é simétrica.

- Suponha que $x_1 \sim x_2$ e $x_2 \sim x_3$, assim $g_1x_1 = x_2$ e $g_2x_2 = x_3$ para algum $g_1, g_2 \in G$. Então $(g_2g_1)x_1 = g_2(g_1x_1) = g_2x_2 = x_3$, portanto $x_1 \sim x_3$ e $\sim$ é transitiva.

□

Definição 1.38. *Seja X um G-conjunto. Cada classe de equivalência da relação descrita no Teorema anterior é uma **órbita em X sob G**. Se $x \in X$, a classe de equivalência que contêm x é a órbita de x. Vamos denotar essa órbita por $G * x$ e lemos "órbita de x em X sob G".*
Podemos escrever $G * x = \{x_0 | x_0 = gx, g \in G\}$ para cada $x \in X$ fixo.

Exemplo 1.39. No caso do D_4-conjunto X do exemplo anterior, temos 6 órbitas distintas:

$$G * 1 = \{1, 2, 3, 4\}$$
$$G * s_1 = \{s_1, s_2, s_3, s_4\}$$
$$G * m_1 = \{m_1, m_2\}$$
$$G * d_1 = \{d_1, d_2\}$$
$$G * C = \{C\}$$
$$G * P_1 = \{P_1, P_2, P_3, P_4\}.$$

Teorema 1.40. *Se X é um G-conjunto e $x \in X$, então $|G * x| = (G : G_x)$. Se $|G|$ é finito então $|G * x|$ é um divisor de $|G|$.*

Demonstração. Para demonstrar a primeira afirmação, vamos definir uma aplicação bijetiva ψ de $G*x$ até a coleção de clases laterais à esquerda de G_x em G, ou seja, até o conjunto $L = \{gG_x | g \in G\}$. Se $x_1 \in G * x$, então existe $g_1 \in G$ tal que $g_1x = x_1$. Assim

$$\begin{aligned} \psi : G * x &\to L \\ x_1 &\mapsto \psi(x_1) = \psi(g_1x) := g_1G_x. \end{aligned}$$

Precisamos mostrar que a aplicação está bem definida e é bijetiva.

- ψ está bem definida. De fato,

  suponha que $x_1 = x_2$, $\forall x_1, x_2 \in G * x$. Assim, existem $g_1, g_2 \in G$ tais que $x_1 = g_1x$ e $x_2 = g_2x$. Como $x_1 = x_2$ então $g_1x = g_2x$.

  Logo, $g_1x = g_2x \Rightarrow g_1^{-1}(g_1x) = g_1^{-1}(g_2x) \Rightarrow (g_1^{-1}g_1)x = (g_1^{-1}g_2)x \Rightarrow ex = (g_1^{-1}g_2)x \Rightarrow x = (g_1^{-1}g_2)x \Rightarrow (g_1^{-1}g_2) \in G_x$.

  Veja que se $(g_1^{-1}g_2) \in G_x$ então existe $h \in G_x$ tal que $(g_1^{-1}g_2) = h$ que por consequência $(g_1^{-1}g_2) = h \Rightarrow g_2 = g_1h \Rightarrow g_2 \in g_1G_x \Rightarrow g_2G_x = g_1G_x \Rightarrow \psi(g_2x) = \phi(g_1x) \Rightarrow \psi(x_2) = \psi(x_1)$.

- ψ é injetiva. Pois,

  suponha $x_1, x_2 \in G*x$, tal que $\psi(x_1) = \psi(x_2)$. Como $x_1, x_2 \in G*x$ então existem $g_1, g_2 \in G$ de modo que $x_1 = g_1x$ e $x_2 = g_2x$, portanto, $\psi(g_1x) = \psi(g_2x) \Rightarrow g_1G_x = g_2G_x \Rightarrow g_2 \in g_1G_x$,

assim deve existir $h \in G_x$ tal que $g_2 = g_1 h$.

Então $x_2 = g_2 x = (g_1 h)x = g_1(hx)$, como $h \in G_x$, então $g_1(hx) = g_1 x = x_1$.

- ψ é sobrejetiva. De fato,

  seja $g_1 G_x \in L$. Como X é um G-conjunto, deve existir $x_1 \in G * x$ tal que $g_1 x = x_1$. Assim, como ψ é bem definida, $g_1 G_x = \psi(x_1)$. Portanto, como $g_1 G_x$ é um elemento qualquer de L, então podemos dizer que

  $$L = \{g_1 G_x | g \in G\} = \{\psi(x_1) | x_1 \in G * x\} = \psi[G * x].$$

Por fim, temos então ψ uma aplicação bijetora em que $|G * x| = |L|$. Veja que $|L|$ representa a quantia de classes laterais de G_x em G, logo $|G * x| = |L| = (G : G_x)$.
Se G é finito então $(G : G_x) = |G|/|G_x|$. Assim, $|G * x| = (G : G_x) = |G|/|G_x| \Rightarrow |G| = |G * x||G_x|$ então $|G * x|$ é um divisor de $|G|$.

□

Teorema 1.41. ***(Fórmula de Burnside)*** *Seja G um grupo finito e X um G-conjunto finito. Se r é o número de órbitas distintas em X sobre G, então*

$$r \cdot |G| = \sum_{g \in G} |X_g|. \tag{1.12}$$

Demonstração. Inicialmente, defina o seguinte conjunto

$$N = \{ \text{ quantidade de pares } (g, x) \in G \times X | gx = x\}.$$

Assim, para cada $g_i \in G$ existem $|X_{g_i}|$ pares tendo g_i como primeiro membro. Portanto,

$$N = \sum_{g \in G} |X_g|. \tag{1.13}$$

Por outro lado, para cada $x_j \in X$ existem $|G_{x_j}|$ pares tendo x_j como segundo membro. Portanto,

$$N = \sum_{x \in X} |G_x|. \tag{1.14}$$

Mas ja vimos pelo Teorema 1.40 que $(G : G_x) = |G * x|$ e $(G : G_x) = |G|/|G_x|$. Desse modo, temos $|G_x| = |G|/|G * x|$. Assim,

$$N = \sum_{x \in X} \frac{|G|}{|G * x|} = |G| \cdot \left(\sum_{x \in X} \frac{1}{|G * x|} \right). \tag{1.15}$$

Veja que $|G * x|$ possui o mesmo valor para todos os x de uma mesma órbita. Seja $\mathcal{O}$ uma órbita qualquer de n elementos. Observe que

$$\sum_{x\in\mathcal{O}} \frac{1}{|G*x|} = \sum_{x\in\mathcal{O}} \frac{1}{|\mathcal{O}|} = \sum_{x\in\mathcal{O}} \frac{1}{n} = n\frac{1}{n} = 1 \tag{1.16}$$

Assim, sendo r o número de órbitas

$$N = |G| \cdot r. \tag{1.17}$$

Juntando as equações 1.13 e 1.17 temos

$$r \cdot |G| = \sum_{g\in G} |X_g|. \tag{1.18}$$

□

Os resultados dessa seção, por definir e explorar as ações de grupo, são aplicados na compreensão dos p-grupos e nas demonstrações dos Teoremas de Sylow.

1.4 Teoremas de Sylow

p-Grupos

Seja X um finito G-grupo, suponha que existam r órbitas em X sob G e que o conjunto $\{x_1, x_2, \ldots, x_r\}$ contenha um elemento para cada órbita em X. Assim, cada elemento de X está em apenas uma órbita, desta forma, a quantia de elementos do conjunto X equivale à soma da quantia de elementos de cada órbita em X, ou seja

$$|X| = \sum_{i=1}^{r} |G * x_i|. \tag{1.19}$$

Veja que podem existir órbitas unitárias em X, dessa forma, se denotamos $X_G := \{x \in X | gx = x$, para todo $g \in G\}$. Segue que, X_G é exatamente a união de todas as órbitas unitárias. Digamos que que existam s órbitas unitárias, em que $0 \leq s \leq r$, dessa forma $|X_G| = s$ e

$$|X| = |X_G| + \sum_{i=s+1}^{r} |G * x_i|. \tag{1.20}$$

Essa última equação é imprescindível para a compreensão do próximo resultado.

Teorema 1.42. *Se p um número primo, G um grupo de ordem p^n e X um G-conjunto. Então $|X| \equiv |X_G| (mod\ p)$.*

Demonstração. Vamos partir da equação 1.20:

$$|X| = |X_G| + \sum_{i=s+1}^{r} |G * x_i|.$$

Pelo Teorema 1.40, sabemos que $|G * x_i|$ divide $|G|$. Consequentemente, p divide $|G * x_i|$ para $s + 1 \leq i \leq r$. Veja que da equação 1.20, temos

$$|X| - |X_G| = \sum_{i=s+1}^{r} |G * x_i|. \tag{1.21}$$

Portanto, p divide $|X| - |X_G|$, ou seja $|X| \equiv |X_G| (\text{mod } p)$. □

Exemplo 1.43. No caso do D_4-conjunto X visto anteriormente, de ordem 17 (!). Temos que $|D_4| = 8 = 2^3$, ou seja, estamos utilizando $p = 2$. Existe uma única órbita unitária em X, a órbita do elemento C. Assim temos $|X| = 17$, $|X_{D_4}| = 1$ e $p = 2$. Veja que $17 \equiv 1 (\text{mod } 2)$ pois $17 - 1 = 16 = 8 \cdot 2$.

Definição 1.44. *Seja p um número primo. Um grupo é um p-**grupo** se cada elemento de G possui ordem de uma potência de p.*

Definição 1.45. *Um subgrupo desse grupo G é um p-**subgrupo de** G se o subgrupo for ele mesmo um p-grupo.*

Teorema 1.46. ***(Teorema de Cauchy)*** *Se p um número primo e G um grupo finito tal que p divida $|G|$. Então G possui um elemento de ordem p e, consequentemente, um subgrupo de ordem p.*

Demonstração. Considere X o conjunto de todas as p-uplas $(g_1, g_2, \ldots, g_p)$ dos elementos de G tal que o produto de suas coordenadas seja o elemento neutro e. Ou seja

$$X = \{(g_1, g_2, \ldots, g_p) | g_i \in G \text{ e } g_1 g_2 \ldots g_p = e\}.$$

Isso é possível pois dado $g_p \in G$ deve existir seu elemento inverso $g_p^{-1} = g_1 g_2 \ldots g_{p-1}$ tal que $g_p g_p^{-1} = e$.
Ao formar a enúpla $(g_1, g_2, \ldots, g_p)$, veja que $g_1 g_2 \ldots g_p = e \Rightarrow g_p = (g_1 g_2 \ldots g_{p-1})^{-1}$. Assim, podemos ter $g_1, g_2, \ldots, g_{p-1}$ como elementos quaisquer de G, e g_p é unicamente determinado por $(g_1 g_2 \ldots g_{p-1})^{-1}$. Logo, $|X| = |G|^{p-1}$ e como p divide $|G|$ então p divide $|X|$.

Seja σ o ciclo $(1, 2, 3, \ldots, p)$ do grupo de permutações S_p. Considere que σ aja em X da seguinte forma

$$\sigma(g_1, g_2, \ldots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(p)} = (g_2, g_3, \ldots, g_p, g_1).$$

Perceba que, como $(g_1, g_2, \ldots, g_p) \in X$ então $g_1(g_2 \ldots g_p) = e$ que implica que $g_1 = (g_2 \ldots g_p)^{-1}$, e então $(g_2 \ldots g_p)g_1 = e$. Com isso, temos que $\sigma(g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1) \in X$. Assim σ age em X, então consideramos o subgrupo $\langle \sigma \rangle$ de S_p agindo em X por iteração, ou seja, por composições de σ.

Veja que $|\langle\sigma\rangle| = p$, então pelo Teorema 1.42 sabemos que $|X| \equiv |X_{\langle\sigma\rangle}|(\text{mod } p)$. Como p divide $|X|$, logo p divide $|X_{\langle\sigma\rangle}|$ também. Vamos examinar $|X_{\langle\sigma\rangle}|$. Lembremos que $X_{\langle\sigma\rangle} = \{(g_1, g_2, \ldots, g_p) \in X | \sigma(g_1, g_2, \ldots, g_p) = (g_1, g_2, \ldots, g_p)$, ou seja,$(g_1, g_2, \ldots, g_p)$ pertence à $|X_{\langle\sigma\rangle}|$ apenas quando $g_1 = g_2 = \ldots = g_p$ e $g_1 g_2 \ldots g_p = e$. Sabemos que existe pelo menos um elemento que satisfaz essas condições,a saber, o elemento $(e, e, \ldots, e)$. Porém, como p divide $|X_{\langle\sigma\rangle}|$, então devem existir pelo menos p elementos em $X_{\langle\sigma\rangle}$.

Assim, deve existir um elemento $a \in G$, $a \neq e$ tal que $(a, a, \ldots, a) \in X_{\langle\sigma\rangle}$ e portanto, $a^p = e$, indicando que a ordem de a é p. Consequentemente, $\langle a\rangle$ é um subgrupo de G de ordem p.

□

Corolário 1.47. *Seja G um grupo finito. Então G é um p-grupo se e somente se $|G|$ é uma potência de p.*

Demonstração. ($\Rightarrow$) Suponha que G seja um p-grupo. Seja r um número primo que divide $|G|$. Pelo Teorema de Cauchy (Teorema 1.46), existe um elemento $g \in G$ de ordem r.
Porém, pela definição de p-grupo, todo elemento de G possui ordem p^k, $k \in \mathbb{N}$. Assim r deve ser igual à p^k, porém como r é primo, isso só é verdade se $k = 1$ e então $p = r$. Isso significa que $|G|$ não é divisível por nenhum outro número primo além de p. Portanto, $|G|$ é uma potência de p.

($\Leftarrow$) Suponha que $|G| = p^m$ para algum $m \in \mathbb{N}$. Seja $a \in G$ qualquer. Como G é um grupo finito, então pelo Teorema de Lagrange $|G| = (G : \langle a\rangle)|\langle a\rangle|$, então $p^m = (G : \langle a\rangle)|\langle a\rangle|$. Isso implica que $|\langle a\rangle|$ divide $|G|$, e portanto, $|\langle a\rangle| = p^l$ para algum $l \leq m$. □

Teoremas de Sylow

Seja G um grupo e $\mathscr{S}$ a coleção de todos os subgrupos de G. Transformamos $\mathscr{S}$ em um G-conjunto por uma ação de G em $\mathscr{S}$ por conjugação. Isto é, se $H \in \mathscr{S}$ então H é subgrupo de G e, dado $g \in G$, a ação de g em H produz o subgrupo conjugado gHg^{-1}. Seja $N[H] = \{g \in G | gHg^{-1} = H\}$.

1. Veja que $N[H]$ é subgrupo de G. Dados $a, b \in N[H]$, vamos mostrar que $ab^{-1} \in N[H]$. Primeiramente, observe que $b^{-1} \in N[H]$ pois, como $b \in N[H]$ então

   $bHb^{-1} = H \Rightarrow b^{-1}(bHb^{-1}) = b^{-1}H \Rightarrow (b^{-1}b)Hb^{-1} = b^{-1}H \Rightarrow eHb^{-1} = b^{-1}H \Rightarrow Hb^{-1} = b^{-1}H \Rightarrow Hb^{-1}b = b^{-1}Hb \Rightarrow H = b^{-1}Hb \Rightarrow H = b^{-1}H(b^{-1})^{-1}$.

   Como $a \in N[H]$ e $b^{-1} \in N[H]$, então $ab^{-1} \in N[H]$, pois

   $ab^{-1}H(ab)^{-1} = ab^{-1}H(b^{-1})^{-1}a^{-1} = aHa^{-1} = H$.

   Portanto, $N[H]$ é subgrupo de G.

2. Observe que H é normal à $N[H]$.

De fato, pois $\forall g \in N[H]$, temos que $gHg^{-1} = H$ por definição.

3. Veja que $N[H]$ é o maior subgrupo de G que possui H como subgrupo normal.

   Sabemos que $H \lhd N[H]$. Seja K um subgrupo de G tal que $H \lhd K$. Assim, temos que $\forall k \in K$, $kHk^{-1} = H$. Porém, como $K \subset G$ então $k \in G$, logo, $k \in N[H]$ e $K \subset N[H]$. Porntanto, $N[H]$ é o maior subgrupo de G que possui H como subgrupo normal.

Definição 1.48. *Esse subgrupo $N[H]$ é chamado* ***normalizador de*** H ***em*** G.

Na demonstração do lema à seguir, iremos utilizar o fato de que se H é um subgrupo *finito* de G, então $g \in N[H]$ se $ghg^{-1} \in H$ para todo $h \in H$.

Para verificar isso, seja a aplicação de conjugação $i_g : H \to H$ dado por $i_g(h) = ghg^{-1}$.
Veja que, se $i_g(h_1) = i_g(h_2)$, então $gh_1g^{-1} = gh_2g^{-1}$ e $h_1 = h_2$ por cancelamento no grupo G. Então a aplicação de conjugação é injetiva.

Por H ser finito e $i_g : H \to H$ injetiva, logo i_g deve ser uma aplicação sobrejetiva de H até H, assim $i_g[H] = H \Rightarrow gHg^{-1} = H$ e $g \in N[H]$.

Lema 1.49. *Seja H um p-subgrupo de um grupo finito G. Então*

$$(N[H] : H) \equiv (G : H)(mod\ p).$$

Demonstração. Seja $\mathcal{L}$ o conjunto de todas as classes laterais à esquerda de H em G, ou seja, $\mathcal{L} = \{xH | x \in G\}$. Suponha também que H aja em $\mathcal{L}$ por translação à esquerda, de modo que, dado $h \in H$ e $xH \in \mathcal{L}$, temos $h(xH) = (hx)H$. Então $\mathcal{L}$ é um H-conjunto. Perceba que $|\mathcal{L}| = (G : H)$.

Seja $\mathcal{L}_H = \{xH | h(xH) = xH$, para todo $h \in H\}$. Veja que $h(xH) = xH \Leftrightarrow x^{-1}hxH = H \Leftrightarrow x^{-1}hx \in H$. Então, $h(xH) = xH$ para todo $h \in H$ se, e somente se $x^{-1}hx = x^{-1}h(x^{-1})^{-1} \in H$ para todo $h \in H$ se, e somente se $x^{-1} \in N[H]$ se, e somente se $x \in N[H]$. Assim, $\mathcal{L}_H = \{xH | x \in N[H]\}$, ou seja $\mathcal{L}_H$ é o conjunto de todas as classes laterais à esquerda de H em $N[H]$. Então $|\mathcal{L}_H| = (N[H] : H)$.

Como H é um p-grupo, pelo Corolário 1.47, $|H|$ é uma potência de p. Portanto, o Teorema 1.42 nos garante que, como p é um número primo, H um grupo de ordem p^n e $\mathcal{L}$ um H-conjunto. Então $|\mathcal{L}| \equiv |\mathcal{L}_H|(\text{mod } p)$, isto é $(G : H) \equiv (N[H] : H)(\text{mod } p)$. □

Corolário 1.50. *Seja H um p-subgrupo de um grupo finito G. Se p divide $(G : H)$, então $N[H] \neq H$.*

Demonstração. Segue do Lema 1.49 que se p divide $(G : H)$, então p divide $(N[H] : H)$. Assim, $(N[H] : H)$ deve ser diferente de 1, logo, $|N[H]|$ deve ser diferente de $|H|$ e por isso $N[H] \neq H$. □

Teorema 1.51. ***(Primeiro Teorema de Sylow)*** *Seja G um grupo finito tal que $|G| = p^n m$ onde $n \geq 1$ e p não divide m. Então*

1. *G contém um subgrupo de ordem p^i para cada i em que $1 \leq i \leq n$;*
2. *Todo subgrupo H de G de ordem p^i é um subgrupo normal à algum subgrupo de ordem p^{i+1} para $1 \leq i < n$.*

Demonstração. Iremos provar cada caso separadamente.

1. Sabemos que G contém um subgrupo de ordem p pelo Teorema de Cauchy (Teorema 1.46), de fato pois p divide $|G|$.

   Assim, existe um subgrupo de G de ordem p^i para $i = 1$.

   Vamos usar o princípio de indução e mostrar que a existência de um subgrupo de ordem p^i, para $i < n$, implica que existe um subgrupo de ordem p^{i+1}.

   Seja H um subgrupo de ordem p^i, com $i < n$. Como $i < n$, pelo Teorema de Lagrange $|G| = (G : H)|H|$, ou seja, $p^n m = (G : H)p^i$. Segue que p divide $(G : H)$. Pelo Lema 1.49, como p divide $(G : H)$, então p divide $(N[H] : H)$. Como H é normal à $N[H]$, então podemos formar o grupo quociente $N[H]/H$, e vemos que p divide $|N[H]/H|$. Pelo Teorema de Cauchy (Teorema 1.46), $N[H]/H$ possui um subgrupo K de ordem p.

   Se $\gamma : N[H] \to N[H]/H$ é homomorfismo canônico, então $\gamma^{-1}[K] = \{x \in N[H] | \gamma(x) \in K\}$ é um subgrupo de $N[H]$ e de G também. Esse subgrupo contém H e possui ordem p^{i+1}.

   De fato, pois dado $x + H \in K = \{H, a_1 + H, a_2 + H, \ldots, a_p + H\}$. Temos $x + H = a_j + H$ para algum j tal que $1 \leq j \leq p$, e por consequência, $x - a_j \in H$.

   Assim, $x - a_j \in H = \{h_1, h_2, \ldots, h_{p^i}\}$. Temos $x - a_j = h_l$ e então $x = a_j + h_l$ para todo j e l tal que $1 \leq j \leq p$ e $1 \leq l \leq p^i$.

2. Vamos repetir a construção feita no item 1. Perceba que $H < \gamma^{-1}[K] \leq N[H]$ onde $|\gamma^{-1}[K]| = p^{i+1}$. Como H é normal à $N[H]$, ele é normal à $\gamma^{-1}[K]$.

□

Definição 1.52. *Um p-**subgrupo de Sylow** P de um grupo G é o p-subgrupo maximal de G, isto é, o p-subgrupo que não está contido em nenhum outro p-subgrupo.*

Seja G um grupo finito onde $|G| = p^n m$, como no Primeiro Teorema de Sylow (Teorema 1.51). O Teorema mostra que os p-subgrupos de Sylow de G são precisamente os subgrupos de ordem p^n. Veja que se P é um p-subgrupo de Sylow, então todo o conjugado gPg^{-1} de P também é um p-subgrupo de Sylow, com efeito:

suponha então que P seja p-subgrupo de Sylow de G, ou seja, dado $|G| = p^n m$, como no Primeiro Teorema de Sylow (Teorema 1.51), temos então que $|P| = p^n$. Assim, precisamos mostrar que $|gPg^{-1}| = p^n$ também. Seja $f : P \to gPg^{-1}$ de modo que, para todo $x \in P$, $f(x) := gxg^{-1}$.

1. Veja que f é sobrejetiva. De fato, pois
   $gPg^{-1} = \{gpg^{-1} | p \in P\} = \{f(p) | p \in P\} = f[P]$.

2. Veja que f é injetiva. De fato, pois
   sejam $a, b \in gPg^{-1}$ de modo que $a = b$. Assim, devem existir $x, y \in P$ de modo que $a = gxg^{-1}$ e $b = gyg^{-1}$. Logo $gxg^{-1} = gyg^{-1} \Rightarrow f(x) = f(y) \Rightarrow x = y$.

Portanto, f é bijetiva e então $|gPg^{-1}| = |P| = p^n$.

O Segundo Teorema de Sylow nos garante que todo p-subgrupo de Sylow pode ser obtido a partir de P, uma vez que, se P é um p-subgrupo de Sylow, então todo o conjugado gPg^{-1} de P também é um p-subgrupo de Sylow.

Teorema 1.53. ***(Segundo Teorema de Sylow)*** *Se P_1 e P_2 p-subgrupos de Sylow de um grupo finito G. Então P_1 e P_2 são subgrupos conjugados de G.*

Demonstração. Aqui, iremos fazer um dos subgrupos agir nas classes laterais à esquerda do outro, e usar o Teorema 1.42. Seja $\mathcal{L} = \{xP_1 | x \in G\}$ a coleção de classes laterais à esquerda de P_1 em G. O subgrupo P_2 age em $\mathcal{L}$ pela ação $y(xP_1) = (yx)P_1$, para todo $y \in P_2$.

Então $\mathcal{L}$ é um P_2-conjunto. Pelo Teorema 1.42, $|\mathcal{L}_{P_2}| \equiv |\mathcal{L}| (\text{mod } p)$, e por outro lado $|\mathcal{L}| = (G : P_1)$ não é divisível por p, pois supondo que $|G| = p^n m$ sendo que p não divide m, temos que $|P_1| = p^n$, e assim $|\mathcal{L}| = (G : P_1) = m$. Portanto $|\mathcal{L}_{P_2}| \neq 0$.

Lembremos que $\mathcal{L}_{P_2} = \{xP_1 \in \mathcal{L} | y(xP_1) = xP_1 \text{ para todo } y \in P_2\}$.
Seja $xP_1 \in \mathcal{L}_{P_2}$. Então $y(xP_1) = xP_1$ para todo $y \in P_2$ e assim, $x^{-1}yxP_1 = P_1$ para todo $y \in P_2$. Logo, $x^{-1}yx \in P_1$ para todo $y \in P_2$, e então $x^{-1}P_2x \subset P_1$. Como $|P_1| = |P_2| = p^n$, consequentemente $P_1 = x^{-1}P_2x$ e, portanto, P_1 e P_2 são subgrupos conjugados. □

O Terceiro Teorema de Sylow nos garante a quantia dos p-subgrupos de Sylow.

Teorema 1.54. ***(Terceiro Teorema de Sylow)*** *Se G é um grupo finito e p divide $|G|$ então a quantia de p-subgrupos de Sylow é congruente à 1 módulo p e divide $|G|$.*

Demonstração. Seja P um p-subgrupo de Sylow de G. Considere $\mathscr{S}$ o conjunto de todos os p-subgrupos de Sylow e que P aja em $\mathscr{S}$ por conjugação, então $x \in P$ leva $T \in \mathscr{S}$ em $x^{-1}Tx$. Pelo Teorema 1.42, $|\mathscr{S}| \equiv |\mathscr{S}_P| (\text{mod } p)$.

Vamos encontrar $\mathscr{S}_P$. Se $T \in \mathscr{S}_P$, então $x^{-1}Tx = T$ para todo $x \in P$. Assim, $x \in N[T]$ e por consequência, $P \leq N[T]$. Vimos anteriormente que $H \leq N[H]$ para todo subgrupo H, logo $T \leq N[T]$ também.

Como P e T são p-subgrupos de Sylow de G, então são p-subgrupos de Sylow de $N[T]$. Mas, pelo Segundo Teorema de Sylow (Teorema 1.53), P e T são conjugados em $N[T]$. Porém, como T é normal à $N[T]$, ele é seu próprio e único conjugado.

Assim, $P = T$. Consequentemente, $\mathscr{S}_P = \{P\}$, logo, $|\mathscr{S}| \equiv \mathscr{S}_P (\text{mod } p)$, ou seja, a quantia de p-subgrupos de Sylow de G é congruente à 1 módulo p.

Assuma que G aja em $\mathscr{S}$ por conjugação, então $g \in G$ leva $T \in \mathscr{S}$ em $g^{-1}Tg$. Como todos os p-subgrupos de Sylow são conjugados, então existe uma única órbita de $\mathscr{S}$ sob G, pois para qualquer $T \in \mathscr{S}$, $T = g^{-1}Pg$ que pertence à órbita $G * P$. Assim $|G * P| = (G : G_P)$ pelo Teorema 1.40. Mas veja que pelo Teorema de Lagrange $(G : G_P)$ é divisor de $|G|$ e que $(G : G_P) = |\mathscr{S}|$, que é justamente a quantia de p-subgrupos de Sylow de G. Ou seja a quantia de p-subgrupos de Sylow de G é divisor de $|G|$. □

O próximo Teorema é uma aplicação do Primeiro Teorema de Sylow.

Teorema 1.55. *Todo p-grupo finito é solúvel.*

Demonstração. Se G é um p-grupo finito então, pelo Corolário 1.47 $|G| = p^k$ para um $k \in \mathbb{N}$. Assim, segue do Primeiro Teorema de Sylow (Teorema 1.51) que G possui um subgrupo H_i de ordem p^i normal à um subgrupo H_{i+1} de ordem p^{i+1} para $1 \leq i < k$. Então

$$\{e\} = H_0 < H_1 < H_2 < \ldots < H_k = G$$

é uma série de composição, onde os grupos quocientes são de ordem p, abelianos e cíclicos. Portanto, G é solúvel. □

Capítulo 2

Grupos livres

Neste capítulo, iremos discutir uma parte da Teoria de Grupos que é de grande interesse tanto para a álgebra quanto para a topologia.

2.1 Grupos livres

Começamos a seção introduzindo a ideia sobre palavra para definir, em seguida, um grupo livre.

Palavras e Palavras Reduzidas

Seja A um conjunto qualquer (não necessariamente finito) de elementos a_i para $i \in I$. Vamos pensar em A sendo um **alfabeto** e as a_i sendo as **letras** do alfabeto. Todo símbolo da forma a_i^n, com $n \in \mathbb{Z}$ é uma **sílaba** e a corda finita w de sílabas escritas em justaposição é uma **palavra**. Além disso, **palavra vazia** é quando não há sílabas e é representada por e.

Exemplo 2.1. Seja $A = \{a_1, a_2, a_3\}$. Então

$$a_1 a_3^{-4} a_2^2 a_3; \qquad a_2^3 a_2^{-1} a_4^{-3} a_4^3 a_3 a_1^2 a_1^{-7}; \qquad a_3^2 \tag{2.1}$$

são palavras.

Existem duas maneiras naturais de se modificar uma palavra, são as **contrações elementares**. O primeiro tipo consiste em substituir a palavra $a_i^m a_i^n$ por a_i^{m+n}. O segundo tipo consiste em substituir a palavra a_i^0 por e.

Através de uma quantia finita de contrações elementares, cada palavra pode ser reduzida à uma palavra no qual não há mais contrações elementares possíveis e chamamos de **palavra reduzida**. Perceba que essas contrações elementares se assemelham às manipulaçoes usuais com expoentes.

Exemplo 2.2. A palavra reduzida do exemplo anterior $a_2^3 a_2^{-1} a_4^{-3} a_4^3 a_3 a_1^2 a_1^{-7}$ é a palavra $a_2^2 a_3 a_1^{-5}$.

Seja $F[A]$ o conjunto de todas as palavras reduzidas formadas pelo alfabeto A. Daremos à $F[A]$ uma estrutura de grupo de maneira natural. Para w_1 e w_2 em $F[A]$, defina $w_1 \cdot w_2$ a forma reduzida da palavra obtida por justaposição $w_1 w_2$ das duas palavras.

Exemplo 2.3. Se

$$w_1 = a_2^3 a_1^{-5} a_3^2$$

e

$$w_2 = a_3^{-2}a_1^2a_3a_2^{-2},$$

então $w_1 \cdot w_2 = (a_2^3a_1^{-5}a_3^2) \cdot (a_3^{-2}a_1^2a_3a_2^{-2}) = a_2^3a_1^{-5}a_3^2a_3^{-2}a_1^2a_3a_2^{-2} = a_2^3a_1^{-5}ea_1^2a_3a_2^{-2} = a_2^3a_1^{-5}a_1^2a_3a_2^{-2} = a_2^3a_1^{-3}a_3a_2^{-2}$.

Essa operação de $F[A]$ é bem definida e associativa. A palavra vazia e é o elemento neutro. Além disso, dado $w \in F[A]$, seu elemento inverso w^{-1} é formado por, primeiramente, escrever as sílabas de ordem oposta (de trás para frente) e depois recolocar cada sílaba a_i^n, de w, por a_i^{-n}. Assim

$$w \cdot w^{-1} = e = w^{-1} \cdot w.$$

Exemplo 2.4. *Como exemplo, tomemos $w = a_2^3a_1^{-3}a_3a_2^{-2}$. Assim $w^{-1} = a_2^2a_3^{-1}a_1^3a_2^{-3}$.*

Observe que $w \cdot w^{-1} = (a_2^3a_1^{-3}a_3a_2^{-2}) \cdot (a_2^2a_3^{-1}a_1^3a_2^{-3}) = a_2^3a_1^{-3}a_3a_2^{-2}a_2^2a_3^{-1}a_1^3a_2^{-3} = e = a_2^2a_3^{-1}a_1^3a_2^{-3}a_2^3a_1^{-3}a_3a_2^{-2} (a_2^2a_3^{-1}a_1^3a_2^{-3}) \cdot (a_2^3a_1^{-3}a_3a_2^{-2}) = w^{-1} \cdot w$.

Definição 2.5. *O grupo $F[A]$ descrito acima é o **grupo livre gerado** por A.*

Definição 2.6. *Se G é um grupo gerado por um conjunto $A = \{a_i\}$ e G é isomorfo à $F[A]$ sob a aplicação $\phi : G \to F[A]$ tal que $\phi(a_i) = a_i$, então G é **livre em** A, e cada a_i é um **gerador livre de** G. Um grupo é dito **livre** se é livre em algum conjunto não vazio A.*

Definição 2.7. *Se G é livre em A, o número de elementos em A é o **posto do grupo livre** G.*

Exemplo 2.8. Temos o grupo $\mathbb{Z}$, que é livre em um gerador.

Podemos tomar a aplicação bijetiva $\phi : (\mathbb{Z}, +) \to (F[A], \cdot)$ definido por $a \mapsto \phi(a) := 1^a$. Note que $\phi(1) = 1$.

Assim, como $|A| = 1$, então o posto de Z é 1.

Veja que todo grupo livre é infinito, pois todo alfabeto $F[A]$ é infinito. Além disso, se um grupo G é livre em A e em B também, então os conjuntos A e B possuem a mesma quantia de elementos. Ainda, dois grupos livres são isomorfos se, e somente se, eles possuem o mesmo posto. Observe também que um subgrupo próprio não trivial de um subgrupo livre é livre.

Exemplo 2.9. Seja $F[\{x, y\}]$ o grupo livre em $\{x, y\}$. Se

$$y_k = x^k y x^{-k}$$

para $k \geq 0$ e $B = \{y_k | y \in \mathbb{Z}, y \geq 0\}$. Então, $F[B]$ é subgrupo de $F[\{x, y\}]$. Isso ilustra que um subgrupo de um grupo livre é livre, e o posto do subgrupo pode ser muito maior que o posto do grupo. No caso, o posto de $F[B]$ é infinito, enquanto o posto de $F[\{x, y\}]$ é 2.

Teorema 2.10. *Se G é um grupo e $a_i \in G$ para $i \in I$, então o subgrupo H de G gerado por $\{a_i | i \in I\}$ possui os elementos de G que são, precisamente, os produtos finitos de potências inteiras de a_i, onde potências de um a_i fixado pode ocorrer várias vezes em um mesmo produto.*

Demonstração. Seja K o conjunto de todos os produtos finitos de potências inteiras de a_i. Provemos que $K = H$, de fato:

veja que $K \subseteq H$. Dado $k \in K$, então k é um produto finito de uma potência inteira de a_i, então $k = \prod a_i^n \in H$.

Para mostrar que $H \subset K$ precisamos mostrar que K é um subgrupo que contém a_i, pois temos que H é o menor subgrupo contendo a_i para $i \in I$.
Veja que o produto dos elementos de K está fechado em K. Como $(a_i)^0 = e$ então o elemento neutro $e \in K$. Para cada elemento $k \in K$, podemos formar k^{-1} por, primeiramente, escrever cada a_i^n de ordem oposta (de trás para frente) e depois recolocar cada um por a_i^{-n}.

Portanto, como K é um grupo e $a_i \in K$, então $H \subset K$. Assim, $K = H$.

□

Observação: neste Teorema, o resultado foi dado pensando em um grupo com operação multiplicativa. Para o caso aditivo, temos o seguinte enunciado: se G é um grupo e $a_i \in G$ para $i \in I$, então o subgrupo H de G gerado por $\{a_i | i \in I\}$ possui os elementos de G que são, precisamente, as somas finitas de mutiplos inteiros de a_i, onde mutiplos de um a_i fixado pode ocorrer várias vezes em uma mesma soma. No contexto dado acima, temos $k = \sum na_i$.

Teorema 2.11. *Seja G gerado por $A = \{a_i | i = I\}$ e G' um grupo livre. Se a'_i para todo $i \in I$ é um elemento de G', não necessariamente distintos, então existe pelo menos um homomorfismo $\lambda : G \to G'$ tal que $\phi(a_i) = a'_i$. Se G é livre em A, então existe exatamente um homomorfismo.*

Demonstração. Suponha λ o homomorfismo de G em G' tal que $\lambda(a_i) = a'_i$. Queremos mostrar como definimos tal homomorfismo para todo o G. Pelo Teorema 2.10, para qualquer $x \in G$, temos

$$x = \prod_j a_{i_j}^{n_j}$$

para determinado produto finito do gerador a_i, onde cada a_{i_j} que aparece no produto não precisa ser distinto. Então, como λ é um homomorfismo, nós devemos ter

$$\lambda(x) = \lambda(\prod_j a_{i_j}^{n_j}) = \prod_j \lambda(a_{i_j}^{n_j}) = \prod_j (a'_{i_j})^{n_j}.$$

Portanto, um homomorfismo é completamente determinado por um conjunto de geradores. Isso mostra que existe pelo menos um homomorfismo tal que $\lambda(a_i) = a'_i$.
Suponha agora que G é livre em A; isto é existe um isomorfismo $\phi : G \to F[A]$ tal que $\phi(a_i) = a_i$. Pelo que vimos anteriormente, existe pelo menos um homomorfismo $\rho : F[A] \to G'$ tal que $\rho(a_i) = (a'_i)$. Para todo

$$x = \prod_j a_{i_j}^{n_j}$$

em G, defina $\psi = \rho \circ \phi : G \to G'$ por

$$\psi(x) = \rho(\phi(x)) = \rho(\phi(\prod_j a_{i_j}^{n_j})) = \prod_j (a'_{i_j})^{n_j}.$$

A aplicacação é bem definida pois, como $F[A]$ é um grupo de palavras reduzidas, não existe produtos formais iguais em $F[A]$. Como as regras envolvendo computação de expoentes em G' são formalmente os mesmos que aqueles em G, assim, veja que $\psi(xy) = \psi(x)\psi(y)$ para quaisquer elementos x, y de G, então ψ é um homomorfismo. □

Teorema 2.12. *Todo grupo G' é uma imagem homomorfa de um grupo livre G.*

Demonstração. Seja $G' = \{a'_i | i \in I\}$, e $A = \{a_i | i \in I\}$ um conjunto com mesma quantia de elementos que G'. Seja $G = F[A]$. Então pelo Teorema 2.11 existe um homomorfismo ψ de G até G' tal que $\psi(a_i) = a'_i$. A imagem de G sob ψ é todo o G'. □

2.2 Grupos abelianos livres

Nesta seção iremos introduzir o conceito de grupo livre abeliano e provar alguns de seus resultados.

Teorema 2.13. *Seja X o subconjunto de um grupo abeliano não-vazio G. As seguintes condições em X são equivalentes.*

1. *Cada elemento não-neutro $a \in G$ pode ser expresso unicamente (até a ordem do somatório) na forma $a = n_1x_1 + n_2x_2 + \ldots + n_rx_r$ para $n_i \neq 0$ em $\mathbb{Z}$ e distintos x_i em X.*

2. *X gera G, e $x_1n_1 + x_2n_2 + \ldots + n_rx_r = 0$ para $n_i \in \mathbb{Z}$ e distintos $x_i \in X$ se, e somente se, $n_1 = n_2 = \cdots = n_r = 0$.*

Demonstração. Suponhamos que a condição 1 é verdadeira. Como $G \neq \{0\}$ então devemos ter $X \neq \{0\}$. Além disso, segue que $0 \notin X$. De fato, pois seja $x_i = 0$ e $x_j \neq 0$, então $x_j = x_j + x_i$ o que contradiz a unicidade de uma expressão que contenha x_j.
Pela condição 1, X gera G pela observação do Teorema 2.10, e $n_1x_1 + n_2x_2 + \cdots + n_rx_r = 0$ se $n_1 = n_2 = \cdots = n_r = 0$. Vamos supor que $n_1x_1 + n_2x_2 + \cdots + n_rx_r = 0$ para algum $n_i \neq 0$; eliminando os termos com coeficiente 0, podemos obter $n_1, n_2, \cdots, n_s \neq 0$ para $s \leq r$. Temos então $n_1x_1 + n_2x_2 + \cdots + n_sx_s = 0$.
Assim, $x_1 = x_1 + 0 = x_1 + (n_1x_1 + n_2x_2 + \cdots + n_sx_s) = (n_1 + 1)x_1 + n_2x_2 + \cdots + n_sx_s$. Logo, $x_1 \neq 0$ pode ser escrito de duas formas diferentes, que contradiz a condição 1. Portanto $x_1n_1 + x_2n_2 + \ldots + n_rx_r = 0$ para $n_i \in \mathbb{Z}$ e distintos $x_i \in X$ se, e somente se, $n_1 = n_2 = \cdots = n_r = 0$ então a condição 1 implica que a condição 2 é verdadeira.

Suponhamos que a condição 2 é verdadeira. Como X gera G, então a pode ser expresso da forma $a = n_1x_1 + n_2x_2 + \cdots n_rx_r$. Suponha que a possa ser expresso de forma diferente, $a = m_1x_1 + m_2x_2 + \cdots + m_rx_r$.
Assim, $a - a = (n_1x_1 + n_2x_2 + \cdots n_rx_r) - (m_1x_1 + m_2x_2 + \cdots + m_rx_r) \Rightarrow 0 = (n_1 - m_1)x_1 + (n_2 - m_2)x_2 + \cdots + (n_r - m_r)x_r$. Logo, pela condição 2, $n_i - m_i = 0$ e então $n_i = m_i$ para todo $i = 1, 2, \cdots, r$. Portanto, os coeficientes são únicos e a é expresso unicamente. Então a condição 2 implica que a condição 1 é verdadeira. □

Definição 2.14. *Um grupo abeliano que possui um conjunto gerador X que satisfaz as condições do Teorema anterior é chamado* ***Grupo Abeliano Livre****, e X é uma* ***base*** *para o grupo.*

Definição 2.15. *Um grupo abeliano é* ***livre de torção*** *se o elemento neutro e for o único elemento de ordem finita.*

Observe que todo grupo abeliano livre é livre de torção.

Exemplo 2.16. O produto direto $\mathbb{Z} \times \mathbb{Z}$ é um grupo abeliano livre e $\{(1,0),(0,1)\}$ é a base. De modo similar, $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ é um grupo abeliano livre e $\{(1,0,0),(0,1,0),(0,0,1)\}$ é a base. Assim, todo produto direto do grupo $\mathbb{Z}$ consigo mesmo é um grupo abeliano livre.

Exemplo 2.17. O $\mathbb{Z}_n$ não é abeliano livre, pois existe $nx = 0$ para todo $x \in \mathbb{Z}_n$, e $n \neq 0$, que contradiz a condição 2 do Teorema 2.13.

Suponha que um grupo abeliano livre G possui uma base finita $X = \{x_1, x_2, \cdots, x_r\}$. Se $a \in G$ e $a \neq 0$, então a possui uma expressão única na forma

$$a = n_1x_1 + n_2x_2 + \cdots + n_rx_r, \text{ para } n_i \in \mathbb{Z}.$$

Perceba que na expressão acima, incluimos todos os elementos x_i da base finita X, em oposição à expressão da condição 1 do Teorema 2.13, em que a base pode ser infinita. Naquele caso, abrimos a possiblidade para que alguns n_i sejam 0, onde na condição 1 especificamos que todo $n_i \neq 0$.

Definimos

$$\phi : G \to \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ fatores}}$$

por $\phi(a) = (n_1, n_2, \cdots, n_r)$ e $\phi(0) = (0, 0, \cdots, 0)$.

Teorema 2.18. *Se G é um grupo abeliano livre não nulo com uma base de r elementos, então a aplicação descrita acima é um isomorfismo.*

Demonstração. Devemos mostrar que a aplicação é um homomorfismo e que é uma bijeção, ou seja, é injetiva e sobrejetiva.

1. A aplicação ϕ é um homomorfismo. De fato:

   dados $a, b \in G$ diferentes de 0, pela condição 1 do Teorema 2.13, podemos obter as expressões únicas $a = n_1x_1 + n_2x_2 + \cdots + n_rx_r$ e $b = m_1x_1 + m_2x_2 + \cdots + m_rx_r$. Assim, $\phi(a) = (n_1, n_2, \cdots, n_r)$ e $\phi(b) = (m_1, m_2, \cdots, m_r)$. Logo, $\phi(a) + \phi(b) = (n_1, n_2, \cdots, n_r) + (m_1, m_2, \cdots, m_r) = (n_1 + m_1, \cdots, n_r + m_r)$.
   Observe que $a + b = n_1x_1 + n_2x_2 + \cdots + n_rx_r + m_1x_1 + m_2x_2 + \cdots + m_rx_r = (n_1 + m_1)x_1 + (n_2 + m_2)x_2 + \cdots + (n_r + m_r)x_r$, isso é válido pois G é abeliano. Por isso, $\phi(a + b) = (n_1 + m_1, n_2 + m_2, \cdots, n_r + m_r)$.
   Caso a ou b seja igual ao zero, também é válido. Vamos supor que $b = 0$, assim, $\phi(b) = (0, 0, \cdots, 0)$. logo, $phi(a)+\phi(b) = (n_1, n_2, \cdots, n_r)+(0, 0, \cdots, 0) = (n_1, n_2, \cdots, n_r) = \phi(a) = \phi(a + 0)$. Portanto, $\phi(a) + \phi(b) = (n_1 + m_1, n_2 + m_2, \cdots, n_r + m_r) = \phi(a + b)$. Então ϕ é um homomorfismo.

2. A aplicação ϕ é injetiva. Pois:

   dado $\phi(a) = \phi(b)$ com $a, b \in G$ diferentes de 0, então $\phi(a) = \phi(b) \Rightarrow (n_1, n_2, \cdots, n_r) = (m_1, m_2, \cdots, m_r) \Rightarrow n_i = m_i$ para todo $i = 1, 2, \cdots, r$. Como os coeficientes são iguais, então existe um único valor $a \in G$ tal que $a = n_1x_1 + n_2x_2 + \cdots + n_rx_r$, pela condição 1 do Teorema 2.13. Portanto, $a = b$ e por consequência, ϕ é injetiva.

3. A aplicação ϕ é sobrejetiva. De fato:

   $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} = \{(n_1, n_2, \cdots, n_r) | n_i \in \mathbb{Z}\} = \{\phi(a) | a \in G\} = \phi[G]$, pois pela condição 1 do Teorema 2.13, todo elemento $a \neq 0$ pode ser representado unicamente por $a = n_1x_1 + n_2x_2 + \cdots + n_rx_r$ para todo $n_i \neq 0$ em $\mathbb{Z}$. Se $n_1 = n_2 = \cdots = n_r = 0$, então temos pela definição de ϕ que $(n_1, n_2, \cdots, n_r) = \phi(0)$. Portanto, ϕ é sobrejetiva.

Portanto ϕ é um isomorfismo. □

Teorema 2.19. *Seja $G \neq \{0\}$ um grupo abeliano livre. Se uma base de G é finita, então toda base de G é finita e todas possuem a mesma quantia de elementos.*

Demonstração. Suponha que G possua a base $\{x_1, x_2, \cdots, x_r\}$. Então G é isomorfo à $\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}$ para r fatores, pelo Teorema 2.18. Seja $2G = \{2g | g \in G\}$ um subgrupo de G. Observe que $2G$ é normal à G, pois o subgrupo de qualquer grupo abeliano é normal. Como $G \simeq \mathbb{Z} \times \cdots \times \mathbb{Z}$ para r fatores, temos

$$G/2G \simeq (\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z})/(2\mathbb{Z} \times 2\mathbb{Z} \times \cdots \times 2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$$

para r fatores. Então, como cada $\mathbb{Z}_2$ possui 2 elementos, logo $|G/2G| = 2^r$. Assim, a quantia de elementos de uma base qualquer X é dado unicamente por $r = log_2|G/2G|$. Portanto, quaisquer duas bases finitas de G possuem a mesma quantia de elementos.
Resta mostrar que G não pode ter bases infinitas. Considere Y uma base qualquer de G, e $\{y_1, y_2, \cdots, y_s\}$ elementos distintos em Y. Sejam H o subgrupo de G gerado por $\{y_1, y_2, \cdots, y_s\}$, e K o subgrupo de G gerado pelos elementos restantes de Y. Observe que $G \simeq H \times K$, então

$$G/2G \simeq (H \times K)/(2H \times 2K) \simeq (H/2H) \times (K/2K).$$

Como $|H/2H| = 2^s$, temos $|G/2G| \geq 2^s$. Como temos $|G/2G| = 2^r$, então $2^r \geq 2^s$ e $r \geq s$. Portanto, Y não pode ser um conjunto infinito.

□

Exemplo 2.20. Toda base de $\mathbb{Z} \times \mathbb{Z}$ possui 2 elementos. De fato, veja que $r = log_2|\mathbb{Z} \times \mathbb{Z}/2(\mathbb{Z} \times \mathbb{Z})| = log_2(4) = 2$.

Definição 2.21. *Se G é um grupo abeliano livre, então o **posto** de G é a quantidade de elementos da base de G.*

Os Teoremas à seguir são necessários para a demonstração do Teorema Fundamental dos Grupos Abelianos Finitamente Gerados.

Teorema 2.22. *Sejam G um grupo abeliano finitamente gerado pelo conjunto $\{a_1, a_2, \cdots, a_n\}$ e*

$$\gamma : F = \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \mathbb{Z}}_{n \text{ fatores}} \to G$$

definido por $\gamma(h_1, h_2, \cdots, h_n) = h_1a_1 + h_2a_2 + \cdots + h_na_n$. *Então* γ *é um epimorfismo em* G.

Demonstração. A aplicação γ é um homomorfismo. De fato:

$$\begin{aligned}\gamma((h_1, \cdots h_n) + (k_1, \cdots, k_n)) &= \gamma(h_1 + k_1, \cdots, h_n + k_n)\\ &= (h_1 + k_1)a_1 + \cdots + (h_n + k_n)a_n\\ &= (h_1a_1 + k_1a_1) + \cdots + (h_na_n + k_na_n\\ &= (h_1a_1 + \cdots h_na_n) + (k_1a_1 + \cdots k_na_n)\\ &= \gamma(h_1, \cdots, h_n) + \gamma(k_1, \cdots, k_n)\end{aligned}$$

desde que G seja abeliano.

Além disso, veja que a aplicação é sobrejetora, pois, para qualquer $g \in G$, podemos ter $g = h_1a_1 + h_2a_2 + \cdots + h_na_n$, pois G é um grupo finitamente gerado. Assim,

$$G = \{h_1a_1 + h_2a_2 + \cdots + h_na_n\} = \{\gamma(h_1, h_2, \cdots, h_n)\} = \{F\}.$$

Portanto, γ é um epimorfismo. □

Mostraremos agora, uma "propriedade de substituição"que torna possível ajustar a base.

Teorema 2.23. *Se* $X = \{x_1, \cdots, x_r\}$ *é uma base para o grupo abeliano livre* G *e* $t \in \mathbb{Z}$, *então, para* $i \neq j$, *o conjunto*

$$Y = \{x_1, \cdots, x_{j-1}, x_j + tx_i, x_{j+1}, \cdots, x_r\}.$$

também é uma base para G.

Demonstração. Como $x_j = (-t)x_i + (x_j + tx_i)$,vemos que x_j pode ser recuperado de Y, assim, essa base pode gerar G.

Suponha que

$$n_1x_1 + \cdots + n_ix_i + \cdots n_j(x_j + tx_i) + \cdots n_rx_r = 0.$$

Então

$$n_1x_1 + \cdots + (n_i + tn_j)x_i + \cdots n_jx_j + \cdots n_rx_r = 0$$

e como X é uma base, $n_1x_1 + \cdots + (n_i + tn_j)x_i + \cdots n_jx_j + \cdots n_rx_r = 0$ se, e somente se $n_1 = \cdots = n_i + tn_j = \cdots = n_j = \cdots = 0$. De $n_j = 0$ e $n_i + tn_j = 0$ segue que $n_i = 0$. Isso satisfaz a condição 2 do Teorema 2.13.

Portanto, Y é uma base.

□

Exemplo 2.24. Uma base de $\mathbb{Z} \times \mathbb{Z}$ é $\{(1,0),(0,1)\}$. Outra base é $\{(1,0),(4,1)\}$ com $(4,1) = 4(1,0) + (0,1)$. Qualquer elemento de $\mathbb{Z} \times \mathbb{Z}$ pode ser representado por essa base, como por exemplo, $(2,-3) = 14(1,0) + (-3)(4,1)$.

Entretanto $\{(3,0),(0,1)\}$ não é uma base. Por exemplo, não podemos expressar $(2,-3) = n_1(3,0) + n_2(0,1)$, para $n_1, n_2 \in \mathbb{Z}$. Aqui temos $(3,0) = (1,0) + 2(1,0)$, em que um multiplo de um elemento da base foi adicionado à *ele mesmo* ao invés de adicionar à um elemento *diferente* da base.

Um grupo abeliano livre G pode ter diversas bases.

Teorema 2.25. *Se G é um grupo abeliano livre não vazio de posto finito n, e K um subgrupo de G não vazio. Então K é abeliano livre de posto $s \leq n$. Além disso, existe uma base $\{x_1, x_2, \cdots, x_n\}$ para G, e existem inteiros positivos, $d_1, d_2, \cdots, d_s$ onde d_i divide d_{i+1} para $i = 1, \cdots, s-1$, tal que $\{d_1x_1, d_2x_2, \cdots, d_sx_s\}$ é uma base para K.*

Demonstração. Iremos mostrar que K possui a base descrita acima, que por consequência, mostra que K é abeliano livre de posto $s \leq n$. Suponha que $Y = \{y_1, \cdots, y_n\}$ é uma base para G. Todo elemento não nulo de K pode ser expresso da forma

$$k_1y_1 + \cdots + k_ny_n$$

onde alguns $|k_i|$ são não nulos. Dentre todas as bases Y de G, escolha uma base, Y_1, que produza o valor mínimo não nulo $|k_i|$ de modo que todos os elementos não nulos de K são escritos em termos de elementos de Y_1. Renumerando os elementos de Y_1 se necessário, podemos assumir que existe $w_1 \in K$ tal que

$$w_1 = d_1y_1 + k_2y_2 + \cdots + k_ny_n$$

no qual $d_1 > 0$ e d_1 é o coeficiente mínimo da base Y_1 assim como descrito. Usando o algoritmo de divisão, escreveremos $k_j = d_1q_j + r_j$ onde $0 \leq r_j < d_1$ para $j = 2, \cdots, n$. Então

$$w_1 = d_1(y_1 + q_2y_2 + \cdots + q_ny_n) + r_2y_2 + \cdots + r_ny_n. \tag{2.2}$$

Seja $x_1 = y_1 + q_2y_2 + \cdots + q_ny_n$. Pelo Teorema 2.23, $\{x_1, y_2, \cdots, y_n\}$ também é uma base para G. Pela equação (1.23), e pelo d_1 ser o mínimo possível pela escolha de Y_1, vemos que $r_2 = \cdots = r_n = 0$ só podem ser 0. Então $w_1 = d_1x_1 \in K$.

Consideramos por agora, as bases de G da forma $\{x_1, y_2, \cdots, y_n\}$. Cada elemento w_2 de K pode ser expresso na forma

$$h_1x_1 + k_2y_2 + \cdots + k_ny_n.$$

Como $d_1x_1 \in K$, podemos subtrair um múltiplo adequado de d_1x_1 e então usar a minimalidade de d_1 para ver que h_1 é múltiplo de d_1, vemos que $k_2y_2 + \cdots + k_ny_n \in K$. Dentre todas as bases $\{x_1, y_2, \cdots, y_n\}$, escolha uma base Y_2 que produza o valor minimo não nulo $k_i \neq 0$. (É possível que todo k_i seja 0. Neste caso, K é gerado por d_1x_1 e está feito.) Renumerando os elementos de Y_2, podemos assumir que existe $w_2 \in K$ tal que

$$w_2 = d_2y_2 + \cdots + k_ny_n$$

onde $d_2 > 0$ e d_2 é o coeficiente minimo da base Y_2 como descrito. Exatamente como no parágrafo anterior, podemos modificar nossa base $Y_2 = \{x_1, y_2, \cdots, y_n\}$ em $\{x_1, x_2, y_3, \cdots, y_n\}$ de G onde $d_1x_1 \in K$ e $d_2x_2 \in K$. Escrevendo $d_2 = d_1q+r$ para $0 \leq r < d_1$, vemos que $\{x_1+qx_2, x_2, y_3, \cdots, y_n\}$ é uma base de G, e $d_1x_1 + d_2x_2 = d_1(x_1 + qx_2) + rx_2$ está em K. Pela escolha de d_1 ser mínimo da base Y_1, vemos que $r = 0$, então d_1 divide d_2.

Agora iremos considerar todas as bases da forma $\{x_1, x_2, y_3, \cdots, y_n\}$ de G e examinar os elementos de K da forma $k_3y_3+\cdots+k_ny_n$. O processo continua até obtermos a base $\{x_1, x_2, \cdots, x_s, y_{s+1}, \cdots, y_n\}$ onde o único elemento de K da forma $k_{s+1}y_{s+1} + \cdots + k_ny_n$ é zero, isto é, todo k_i é zero. Suponha $x_{s+1} = y_{s+1}, \cdots, x_n = y_n$ e obtemos a base $\{x_1, \cdots, x_n\}$ para G de modo que $\{d_1x_1, \cdots, d_sx_s\}$ é base de K.

□

Teorema 2.26. *Todo grupo abeliano finitamente gerado é isomorfo ao grupo da forma*

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

onde m_i divide m_{i+1} para $i = 1, \cdots, r-1$.

Demonstração. Sejam G um grupo abeliano finitamente gerado por n elementos e $F = \mathbb{Z} \times \cdots \times \mathbb{Z}$ para n fatores. Considere o epimorfismo $\gamma : F \to G$ do Teorema 2.22 e seja K o núcleo desse epimorfismo. Pelo exemplo 2.16, F é abeliano livre e então, podemos utilizar o Teorema 2.25, que diz que existe uma base de F da forma $\{x_1, \cdots, x_n\}$ onde $\{d_1x_1, \cdots, d_sx_s\}$ é uma base de K em que d_i divide d_{i+1} para $i = 1, \cdots, s-1$. Pelo Teorema 1.1, $\gamma[F] = G$ é isomórfo à F/K. Porém observe que,

$$\begin{aligned} F/K &\simeq (\mathbb{Z} \times \mathbb{Z} \times \cdots \mathbb{Z})/(d_1\mathbb{Z} \times d_2\mathbb{Z} \times \cdots \times d_s\mathbb{Z} \times \{0\} \times \cdots \times \{0\} \\ &\simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s} \times \{0\} \times \cdots \times \{0\}. \end{aligned}$$

É possível que $d_1 = 1$, nesse caso $\mathbb{Z}_{d_1} = \{0\}$ e pode ser descartado do produto (aberto à isomorfismo). Similiarmente, d_2 pode ser 1. Seja m_1 o primeiro $d_i > 1$, m_2 ser o próximo d_i e assim por diante. □

Teorema 2.27. ***Teorema Fundamental dos Grupos Abelianos Finitamente Gerados*** *Todo grupo abeliano finitamente gerado G é isomorfo ao produto direto de grupo cíclicos na forma*

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

*onde os p_i são primos, não necessariamente distintos, e r_i são inteiros positivos. O produto direto é único exceto por uma possível reorganização dos fatores; isto é, a quantidade de fatores $\mathbb{Z}$ (**número de Betti** de G) é única e as potências de primos $(p_i)^{r_i}$ são únicas.*

Demonstração. Segue do Teorema anterior que todo grupo abeliano finitamente gerado é isomorfo ao grupo da forma

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}.$$

Como sabemos que o grupo é cíclico, então cada $\mathbb{Z}_{m_i}$ é isomorfo à $\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}$. □

É importante não confundir grupo livre abeliano com grupo livre. Um grupo livre em mais de um gerador, não é abeliano. Na seção anterior definimos um grupo abeliano livre como um grupo abeliano que possui uma base que satisfaz as condições do Teorema 2.27. Entretanto, existe uma outra abordagem dos grupos, via grupos livres, para grupos abelianos, à saber, seja $F[A]$ um grupo livre com conjunto gerador A. Denotemos F Perceba que $F[A]$ não é abeliano se A possuir mais de um elemento. Seja C o subgrupo comutador de $F[A]$. Então $F[A]/C$ é um grupo abeliano e mais ainda, o grupo $F[A]/C$ é livre abeliano de base $\{aC|a \in A\}$. Se aC é renomeado por a, podemos ver $F[A]/C$ como um grupo abeliano livre de base A. Isso mostra que todo grupo abeliano dado um conjunto como base pode ser construído. Todo grupo abeliano livre pode ser construido dessa forma, à menos de isomorfismo. isto, é se G é um grupo abeliano livre de base X, formamos o grupo livre $F[X]$, depois definimos um grupo quociente de $F[X]$ módulo seu grupo comutador e finalmente temos um grupo isomorfo à G. Os Teoremas tais tais (colocar tudo)

2.3 Presentação de Grupos

A ideia de *presentação de grupos* é definir um grupo dado um conjunto de geradores e certas equações ou relações as quais os geradores devem satisfazer. À seguir, veremos um exemplo de como sua definição pode ser formada.

Exemplo 2.28. Suponha que G é um grupo com geradores x e y, e que é livre exceto pela relação $xy = yx$, que podemos expressar como $xyx^{-1}y^{-1} = 1$. Perceba que a condição $xy = yx$ é exatamente o que é preciso para que G seja abeliano, apesar de $xyx^{-1}y^{-1}$ ser apenas um de vários comutadores de $F[\{x, y\}]$. Então G é livre abeliano em dois geradores e é isomorfo ao quociente $F[\{x, y\}]$ modulo seu subgrupo comutador. Como sabemos, esse subgrupo comutador de $F[\{x, y\}]$ é o menor subgrupo normal contendo $xyx^{-1}y^{-1}$, uma vez que qualquer subgrupo normal contendo $xyx^{-1}y^{-1}$ resulta um grupo quociente que é abeliano e portanto[1] contem o subgrupo comutador.

O exemplo anterior ilustra a situação geral, a saber: seja $F[A]$ o grupo livre e suponha que queremos formar um novo grupo que tenha propriedades análogas à de $F[A]$, sujeito à cumprir certas equações. Qualquer equação pode ser escrita de forma que, do lado direito seja e. Com isso, podemos considerar as equações como sendo $r_i = e$ para $i \in I$ em que $r_i \in F[A]$. Observe que se exigimos que r_i é e, então, teríamos

$$x(r_i^n)x^{-1} = 1$$

para todo $x \in F[A]$ e $n \in \mathbb{Z}$. Além disso, qualquer produto de elementos que seja igual à e, novamente será igual à e. Portanto, qualquer produto finito da forma

$$\prod_j x_j(r_{i_j}^{n_j})x_j^{-1}$$

em que r_{i_j} não precisam ser distintos, é igual à e no novo grupo. Veja que o conjunto de todos esses produtos de todos esses produtos finitos é um subgrupo normal R de $F[A]$. (De fato, provar isso). Consequentemente, o grupo construído é $F[A]/R$ ou qualquer outro grupo isomorfo à ele. Com isso à seguinte definição é consistente.

[1]Pelo Teorema 15.20 do Livro [1] na página 150

Definição 2.29. *Sejam A um conjunto e $\{r_i\} \subseteq F[A]$. Seja R o menor subgrupo normal de $F[A]$ contendo r_i. Um isomorfismo ϕ de $F[A]/R$ em G é uma* ***presentação*** *de G. O par $(A, \{r_i\}$ é chamado de* ***presentação de grupo****. O conjunto A é o conjunto de* ***geradores para a presentação*** *e cada r_i é um* ***relator****. Cada $r \in R$ é uma* ***consequência de*** *$\{r_i\}$. Uma equação $r_i = e$ é uma* ***relação****. Uma* ***presentação finita*** *é aquele em que ambos, A e $\{r_i\}$.*

Essa definição pode parecer complicada mas na verdade não é. No Exemplo 2.28, $\{x, y\}$ é o nosso conjunto de geradores e $xyx^{-1}y^{-1}$ é o único relator. A equação $xyx^{-1}y^{-1} = e$ ou $xy = yx$ é uma relação. Então, o que vimos é um exemplo de uma presentação finita.

Se a presentação de um grupo possui geradores x_j e relações r_i, usamos as notações

$$(x_j : r_i) \text{ ou } (x_j : r_i = e)$$

para denotar a presentação de grupo. Podemos nos referir à $F[\{x_j\}]/R$ como grupo com presentação $(x_j : r_i)$.

Exemplo 2.30. Podemos representar o grupo aditivo $(\mathbb{Z}_4, +)$ por $(a, b : a^4, a^3b^{-1})$, ou equivalentemente, $(a, b : a^4, b = a^3)$. Observe que embora a notação seja multiplicativa, o grupo é aditivo.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tabela 2.1: Tábua da presentação do grupo $\mathbb{Z}_4$

$\cdot$	e	a	a^2	b
e	e	a	a^2	b
a	a	a^2	b	e
a^2	a^2	b	e	a
b	b	e	a	a^2

Tabela 2.2: Tábua da presentação do grupo $\mathbb{Z}_4$.

Nesse caso, veja que podemos pensar em "$a = 1$" e "$b = 3$" ou então "$a = 3$" e "$b = 1$", visto que esses elementos satisfazem os relações. Temos então que essa presentação é isomorfa ao grupo $\mathbb{Z}_4$.

Exemplo 2.31. Considere a presentação de grupo com

$$A = \{a\} \text{ e } \{r_i\} = \{a^6\}$$

isto é, a presentação

$$(a : a^6).$$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Tabela 2.3: Tábua da presentação do grupo $\mathbb{Z}_4$

$+$	e	a	a^2	a^3	a^4	a^5
e	e	a	a^2	a^3	a^4	a^5
a	a	a^2	a^3	a^4	a^5	e
a^2	a^2	a^3	a^4	a^5	e	a
a^3	a^3	a^4	a^5	e	a	a^2
a^4	a^4	a^5	e	a	a^2	a^3
a^5	a^5	e	a	a^2	a^3	a^4

Tabela 2.4: Tábua da presentação do grupo $\mathbb{Z}_4$

Este grupo definido por um gerador a, com a relação $a^6 = e$, é isomorfo à $\mathbb{Z}_6$ conforme identificado pelas respectvas tábuas.

Consideremos agora um grupo definido por dois geradores a e b, com $a^2 = e$, $b^3 = e$, e $ab = ba$, isto é, o grupo com a presentação

$$(a, b : a^2, b^3, aba^{-1}b^{-1}).$$

A condição $a^2 = e$ leva à $a^{-1} = a$ e a condição $b^3 = e$ leva à $b^{-1} = b^2$. Assim, todo elemento desse grupo pode ser escrito como um produto de potências não negativas de a e b. A relação $aba^{-1}b^{-1} = e$, isto é, $ab = ba$ nos permite escrever primeiramente todos os fatores envolvendo a e então os fatores envolvendo b. Assim, cada elemento desse grupo é igual à algum $a^m b^n$. Porém, $a^2 = e$ e $b^3 = e$, assim temos apenas 6 elementos distintos, à saber

$$e, b, b^2, a, ab, ab^2.$$

Portanto, essa presentação garante um grupo abeliano de ordem 6, que pelo Teorema 2.26, ele deve ser novamente cíclico e isomorfo à $\mathbb{Z}_6$.

Vemos que o exemplo anterior ilustra que diferentes presentações podem ser isomorfas a um mesmo grupo. Isso nos leva à seguinte definição.

Definição 2.32. *Dado um grupo e duas presentações desse mesmo grupo. Dizemos que as presentações são* ***presentações isomorfas****.*

A importância dessa seção é indicada pelo Teorema 2.12, que garante que *todo grupo possui uma presentação.* (vai fazer uma juncao aki)

Capítulo 3

Complexo simplicial e grupo de homologia

Neste capítulo, abordamos sobre definições iniciais para definir um Complexo simplicial e os grupos de homologia. Iremos trabalhar com o ponto de vista geométrico dessas definições.

3.1 Complexo simplicial e grupo de homologia

Para estudar as propriedades de espaços topológicos, ocasionalmente precisamos da álgebra.

Primeiramente, iremos introduzir a ideia de um n-simplexo orientado no 3-espaço Euclidiano $\mathbb{R}^3$ para $n = 0, 1, 2$ e 3.

Definição 3.1. *Seguem as definições de n-simplexos para $n = 0, 1, 2$ e 3 respectivamente.*

- *Um **0-simplexo orientado** é um ponto P.*
- *Um **1-simplexo orientado** é um um segmento direcional P_1P_2 indo de P_1 até P_2. Assim $P_1P_2 \neq P_2P_1$. Entretanto $P_1P_2 = -P_2P_1$.*
- *Um **2-simplexo orientado** é uma região triângular $P_1P_2P_3$ como na Figura 3.1, junto com um movimento prescrito ao longo do triângulo, indicado por uma flecha, na ordem $P_1P_2P_3$. A ordem $P_1P_2P_3$ é a mesma de $P_2P_3P_1$ e de $P_3P_1P_2$, mas é oposta à $P_1P_3P_2$, $P_3P_2P_1$ e $P_2P_1P_3$.*

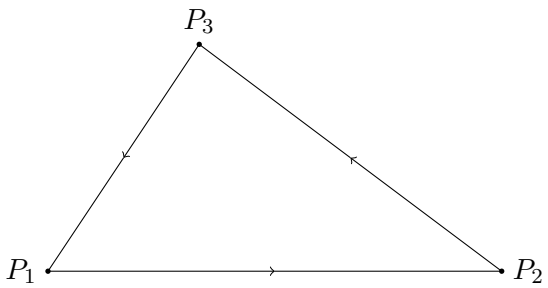


Figura 1.85

Assim

$$P_1P_2P_3 = P_2P_3P_1 = P_3P_1P_2 = -P_1P_3P_2 = -P_3P_2P_1 = -P_2P_1P_3.$$

Veja que $P_iP_jP_k$ possui ordem igual à $P_1P_2P_3$ se

$$\begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$$

for uma permutação par, e é igual à $-P_1P_2P_3$ se for uma permutação ímpar. O mesmo pode ser dito do 1-simplexo orientado P_1P_2. Perceba que para $n = 0, 1, 2$, os n-simplexos orientados tiveram forma de objetos n dimensões.

- *Um **3-simplexo orientado** é dado pela sequência $P_1P_2P_3P_4$ dos quatro vértices de um tetraedro.*

Tetraedro.PNG

Figura 3.1: 3-simplexo orientado

Temos $P_1P_2P_3P_4 = \pm P_iP_jP_rP_s$ dependendo se a permutação

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ i & j & r & s \end{pmatrix}$$

é par ou ímpar.

Definições similares servem para $n > 3$. Estes simplexes são todos **orientados**, em que seus vértices possuem uma ordem. Assim, quando dissermos apenas "simplexo", já consideramos que é orientado daqui em diante.

Iremos introduzir a ideia de fronteira de um n-simplexo para $n = 0, 1, 2, 3$.

Definição 3.2. *Seguem as definições de fronteiras de n-simplexos para $n = 0, 1, 2$ e 3 respectivamente.*

- *Uma **fronteira de um 0-simplexo** P é o simplexo vazio que denotamos por "0". A notação é*

$$\text{“}\partial_0(P) = 0\text{”}.$$

- *Uma **fronteira de um 1-simplexo** é definido por*

$$\partial_1(P_1P_2) = P_2 - P_1,$$

isto é, a diferença entre o ultimo ponto até o primeiro.

- *Uma* ***fronteira de um 2-simplexo*** *é definido por*

$$\partial_2(P_1P_2P_3) = P_2P_3 - P_1P_3 + P_1P_2,$$

que pode ser obtido pela soma de cada i-ésimo termo retirando seu respectivo P_i para $i = 1, 2, 3$ em ordem e tomando como positivo se o primeiro termo é omitido, negativo se o segundo termo é omitido e positivo novamente se o terceiro termo é omitido. Observando a Figura, vemos que isso corresponde à soma de 1-simplexos na orientação desse 2-simplexo.

- *Uma* ***fronteira de um 3-simplexo*** *é definido por*

$$\partial_2(P_1P_2P_3P_4) = P_2P_3P_4 - P_1P_3P_4 + P_1P_2P_4 - P_1P_2P_3.$$

Para $n > 3$ temos definições similares para ∂_n

Definição 3.3. *Cada soma positiva de uma fronteira de um simplex é uma* ***face do simplexo****.*

Assim, no caso da fronteira de um 3-simplexo, $P_2P_3P_4$ é uma face de $P_1P_2P_3P_4$, mas $P_1P_3P_4$ não é uma face. Entretanto, $P_1P_4P_3 = -P_1P_3P_4$ é uma face de $P_1P_2P_3P_4$. As faces possuem orientação em sentido anti-horário vistas de dentro. (Com o outro vértice na frente, visto nas figuras 3.2, 3.3, 3.4 e 3.5).

Figura 3.2: Face $P_2P_3P_4$.

Figura 3.3: Face $P_1P_4P_3$.

Figura 3.4: Face $P_1P_2P_4$.

Figura 3.5: Face $P_1P_3P_2$.

Suponha que temos um subconjunto do $\mathbb{R}^3$ que está dividido "bem" em simplexos, como por exemplo a *superfície* S do tetraedro da Figura, em que temos, quatro 0-simplexos, os vértices do tetraedro, seis 1-simplexos, as arestas do tetraedro, e 4 2-simplexos, as faces do tetraedro. Em geral, para que um espaço esteja "bem" dividido em simplexos, segue a definição.

Definição 3.4. *É chamado* ***complexo simplicial*** *o espaço dividido em simplexos e que satisfaz os seguintes requisitos:*

1. *Cada ponto no espaço pertence à pelo menos um simplexo.*
2. *Cada ponto no espaço pertence à somente um número finito de simplexos.*
3. *Dois simplexos diferentes(a menos de orientação, ou seja, descosiderando a orientação) ou não possuem pontos em comum ou um é (exceto pela possiblidade por orientação) a face do outro, ou a face da face do outro,etc., ou o conjunto de pontos em comum é (exceto pela possiblidade por orientação) a face ou a face da face etc. de cada simplexo*

Vamos agora descrever alguns grupos associados à um complexo simplicial X. Iremos ilustrar cada definição com o caso da *superfície* S do tetraedro da Figura.

Definição 3.5. *Seja X um complexo simplicial. O* ***grupo*** $C_n(X)$ ***de n-cadeias (orientadas) de*** X *é um grupo livre abeliano gerado pelos n-simplexos (orientados) de X. Então, todo elemento de $C_n(X)$ é uma soma finita da forma $\Sigma_i m_i\sigma_i$ onde cada σ_i é um n-simplexo do complexo simplicial X e $m_i \in \mathbb{Z}$. Realizamos adições de elementos das cadeias pela soma algebrica dos coeficientes de cada respectivo simplexo fixado.*

Exemplo 3.6. Para a superfície S do tetraedro, cada elemento de $C_2(S)$ é da forma

$$m_1P_2P_3P_4 + m_2P_1P_3P_4 + m_3P_1P_2P_4 + m_4P_1P_2P_3$$

para $m_i \in \mathbb{Z}$. Como uma ilustração da adição, perceba que

$$(3P_2P_3P_4 - 5P_1P_2P_3) + (6P_2P_3P_4 - 4P_1P_3P_4) = 9P_2P_3P_4 - 4P_1P_3P_4 - 5P_1P_2P_3.$$

Um elemento de $C_1(S)$ é da forma

$$m_1P_1P_2 + m_2P_1P_3 + m_3P_1P_4 + m_4P_2P_3 + m_5P_2P_4 + m_6P_3P_4,$$

e um elemento de $C_0(S)$ é da forma

$$m_1P_1 + m_2P_2 + m_3P_3 + m_4P_4.$$

No caso de $C_n(S)$, $n \geq 3$, observe que o próprio S é a superficie do tetraedro e não há nenhum outro dentro dele, assim

$$C_n(S) = \{e\}.$$

Observe que se σ é um simplexo, então $\partial_n(\sigma) \in C_{n-1}(X)$ para $n = 1, 2, 3$. Iremos definir $C_{-1}(X) = \{e\}$, como o grupo trivial de um elemento, e então temos também, $\partial_0(\sigma) \in C_{-1}(X)$.

Definição 3.7. *Sejam X um complexo simplicial e $C_n(X)$ um grupo de n-cadeias. Como $C_n(X)$ é abeliano livre, e como podemos especificar um homomorfismo de um grupo dado seus valores em geradores, vemos que ∂_n garante um único* ***homomorfismo de fronteira*** *(ou operador bordo) de $C_n(X)$ até $C_{n-1}(X)$ para $n = 0, 1, 2, 3$.*

Exemplo 3.8. Temos
Por exemplo,

$$\begin{aligned}\partial_1(3P_1P_2 - 4P_1P_3 + 5P_2P_4) &= 3\partial_1(P_1P_2) - 4\partial_1(P_1P_3) + 5\partial_1(P_2P_4)\\ &= 3(P_2 - P_1) - 4(P_3 - P_1) + 5(P_4 - P_2)\\ &= P_1 - 2P_2 - 4P_3 + 5P_4.\end{aligned}$$

Quando estudamos um homomorfismo, existem duas coisas de grande interesse à serem vistas, o núcleo e a imagem.

Definição 3.9. *O núcleo de ∂_n consiste em n-cadeias cuja fronteira seja 0. Os elementos desse núcleo são chamados* ***n-ciclos****. A notação usual para o núcleo de ∂_n, isto é, ao* ***grupo de n-ciclos*** *é "$Z_n(X)$".*

Exemplo 3.10. Se $z = P_1P_2 + P_2P_3 + P_3P_1$, então

$$\partial_1(z) = (P_2 - P_1) + (P_3 - P_2) + (P_1 - P_3) = 0$$

Assim, z é um 0-ciclo, ou seja, $z \in Z_1(X)$. Entretanto, se $c = P_1P_2 + 2P_2P_3 + P_3P_1$ então $\partial_1(c) = -P_2 + P_3 \neq 0$. Logo, $c \notin Z_1(X)$.

Perceba que $z = P_1P_2 + P_2P_3 + P_3P_1$ corresponde exatamente à um circuito ou ciclo ao redor de um triângulo de vértices P_1, P_2 e P_3.

Definição 3.11. *A imagem de ∂_n, o* ***grupo de (n-1)-fronteiras*** *consiste exatamente nas (n-1)-cadeias que são fronteiras das n-cadeias de $C_n(X)$. Este grupo é denotado por "$B_{n-1}(X)$".*

Exemplo 3.12. *Do exemplo anterior temos $c = P_1P_2 + 2P_2P_3 + P_3P_1 \in C_1(X)$. Então $P_3 - P_2 \in C_0(X)$ são 1-fronteiras. Observe que $P_3 - P_2$ limita (no sentido de formar a fronteira) P_2P_3.*

Vamos computar $Z_n(X)$ e $B_n(X)$ em um exemplo mais complicado.

Exemplo 3.13. Vamos computar para $n = 0, 1, 2$, os grupos $Z_n(S)$ e $B_n(S)$ para a superfície S do tetraedro. Primeiramente, para os casos mais simples, como o simplexo de maior dimensão dessa superfície é um 2-simplexo, pois temos $C_3(S) = \{e\}$, então

$$B_2(S) = \partial_3(C_3(S)) = 0.$$

Também, uma vez que $C_{-1}(S) = \{e\}$ pela definição, então

$$Z_0(S) = C_0(S).$$

Assim, $Z_0(S)$ é um grupo livre abeliano em quatro geradores, P_1, P_2, P_3 e P_4. Podemos ver que a imagem do grupo sobre um homomorfismo é gerado pelas imagens geradoras do grupo original. Neste caso, dado $\partial_1 : C_1(S) \to C_0(S)$, a imagem de ∂_1, $B_0(S)$, é gerada pela imagem dos geradores de $C_1(S)$. Como $C_1(S)$ é gerado por P_1P_2, P_1P_3, P_1P_4, P_2P_3, P_2P_4 e P_3P_4, então $B_0(S)$ é gerado por

$$P_2 - P_1, P_3 - P_1, P_4 - P_1, P_3 - P_2, P_4 - P_2, P_4 - P_3.$$

Entretanto, $B_0(S)$ é abeliano livre nesses geradores. Por exemplo, $P_3 - P_2 = (P_3 - P_1) - (P_2 - P_1)$. Podemos ver que $B_0(S)$ é abeliano livre em $P_2 - P_1, P_3 - P_1$ e $P_4 - P_1$. Observemos que os outros elementos também podem ser escritos por operação dos geradores. Assim, $P_4 - P_2 = (P_4 - P_1) - (P_2 - P_1)$ e $P_4 - P_3 = (P_4 - P_1) - (P_3 - P_1)$.

Vamos agora verificar $Z_1(S)$. Um elemento c de $C_1(S)$ é uma soma de multiplos inteiros de arestas P_iP_j. Vemos que $\partial_1(c) = e$ se, e somente se, o vértice do começo da primeira aresta deve ser igual ao vértice do fim da última aresta. Assim

$$\begin{aligned} z_1 &= P_2P_3 + P_3P_4 + P_4P_2, \\ z_2 &= P_1P_4 + P_4P_3 + P_3P_1, \\ z_3 &= P_1P_2 + P_2P_4 + P_4P_1, \\ z_4 &= P_1P_3 + P_3P_2 + P_2P_1 \end{aligned}$$

são todos 1-ciclos. Estes são exatamente as fronteiras de 2-simplexos individuais, ou seja, são todos os elementos de $B_1(S)$, em que z_1 é a fronteira de $P_2P_3P_4$, z_2 é a fronteira de $P_1P_3P_4$, z_3 é a fronteira de $P_1P_2P_4$, z_4 é a fronteira de $P_1P_2P_3$. Assim, $B_1(S) \subset Z_1(S)$.

Afirmamos que z_i geram $Z_1(S)$. Seja $z \in Z_1(S)$, vamos verificar se z pode ser escrito em combinação linear de z_i. Escolha um vértice particular, como por exemplo P_1. As arestas que possuem P_1 como o ponto final são P_1P_2, P_1P_3 e P_1P_4. Sejam os coeficientes de P_rP_s de z serem m_{rs}. Então

$$z + m_{12}z_4 - m_{14}z_2$$

ainda é 1-ciclo, porém não contém as arestas P_1P_2 e P_1P_4, pois

$$\begin{aligned} z + m_{12}z_4 - m_{14}z_2 = (m_{12}P_1P_2 + m_{13}P_1P_3 + m_{14}P_1P_4 + m_{23}P_2P_3 + m_{24}P_2P_4 + m_{34}P_3P_4) + \\ m_{12}(P_1P_3 + P_3P_2 + P_2P_1) - m_{14}(P_1P_4 + P_4P_3 + P_3P_1) = m_{12}(P_1P_2 - P_1P_2) + (m_{13} + m_{12} + \\ m_{14})P_1P_3 + m_{14}(P_1P_4 - P_1P_4) + (m_{23} - m_{12})P_2P_3 + m_{24}P_2P_4 + (m_{34} + m_{14})P_3P_4 = \\ (m_{13} + m_{12} + m_{14})P_1P_3 + (m_{23} - m_{12})P_2P_3 + m_{24}P_2P_4 + (m_{34} + m_{14})P_3P_4. \end{aligned}$$

Então, a única aresta tendo P_1 como vértice no ciclo $z + m_2z_4 - m_4z_2$ é possívelmente P_1P_3, mas essa aresta não pode aparecer com coeficiente não nulo pois se não, na fronteira haverá um multiplo não nulo de P_1 contradizendo o fato de ser um 1-ciclo, logo $m_{13} + m_{12} + m_{14} = 0$. Com esta alteração, $z+m_2z_4-m_4z_2$ consiste nas arestas do simplexo $P_2P_3P_4$. Logo, como é um $1-ciclo$, cada P_2, P_3 e P_4 deve possuir o mesmo valor tanto onde começam quanto terminam, e para isso, os coeficientes que aparecem deve ser iguais, no caso $m_{23} - m_{12} = m_{24} = m_{34} + m_{14} = r$ para um r inteiro. Assim, podemos obter $rP_2P_3 + rP_2P_4 + rP_3P_4 = r(P_2P_3 + P_3P_4 + P_4P_2) = rz_1$.
Logo

$$\begin{gathered} z + m_{12}z_4 - m_{14}z_2 = rz_1 \\ \Rightarrow z = rz_1 + m_{14}z_2 + 0z_3 - m_{12}z_4 \end{gathered}$$

Assim $Z_1(S)$ é gerado por z_i. Logo $Z_1(S) \subset \langle z_1, z_2, z_3, z_4\rangle = B_1(S)$. Portanto

$$Z_1(S) = B_1(S).$$

Para $Z_2(S)$. Vemos que $C_2(S)$ é gerado pelos simplexos $P_2P_3P_4$, $P_3P_1P_4$, $P_1P_2P_4$, e $P_2P_1P_3$. Se $P_2P_3P_4$ possui coeficiente r_1 e $P_3P_1P_4$ possui coeficiente r_2 em um $2-ciclo$, então a aresta em comum P_3P_4 tem coeficiente $r_1 - r_2$ como fronteira. Então, para um ciclo, devemos ter $r_1 = r_2$. Logo, $Z_2(S)$ é gerado por

$$P_2P_3P_4 + P_3P_1P_4 + P_1P_2P_4 + P_2P_1P_3,$$

isto é, $Z_2(S)$ é cíclico infinito. Como possui apenas um gerador, então, é isomorfo à $\mathbb{Z}$.

Iremos abordar agora uma das equações mais importantes de toda a matemática moderna.

Teorema 3.14. *Se X é um complexo simplicial e $C_n(X)$ é o grupo das n-cadeias de X para $n = 0, 1, 2, 3$. Então o homomorfismo composto $\partial_{n-1} \circ \partial_n$ de $C_n(X)$ até $C_{n-2}(X)$ aplica todos os elementos à 0 para $n = 1, 2, 3$. Isto é, para cada $c \in C_n(X)$, temos $\partial_{n-1}(\partial_n(c)) = 0$.*

Demonstração. Como um homomorfismo é completamente determinado pelos valores em geradores, é suficiente checar que para um n-simplexo σ, temos $\partial_{n-1}(\partial_n(\sigma)) = 0$.

- Para $n = 1$, $\partial_0(\partial_1(P_1P_2)) = \partial_0(P_2 - P_1) = 0$, pois como vimos anteriormente, ∂_0 leva à zero sempre.
- Para $n = 2$,

$$\partial_1(\partial_2(P_1P_2P_3)) = \partial_1(P_2P_3 - P_1P_3 + P_1P_2) = ((P_3 - P_2) - (P_3 - P_1) + (P_2 - P_1) = 0.$$

- Para $n = 3$,

$$\begin{gathered} \partial_2(\partial_3(P_1P_2P_3P_4)) = \partial_2(P_2P_3P_4 - P_1P_3P_4 + P_1P_2P_4 - P_1P_2P_3) = \\ ((P_3P_4-P_2P_4+P_2P_3)-(P_3P_4-P_1P_4+P_1P_3)+(P_2P_4-P_1P_4+P_1P_2)-(P_2P_3-P_1P_3+P_1P_2) = 0. \end{gathered}$$

□

Corolário 3.15. *Seja X um complexo simplicial. Para $n = 0, 1, 2, 3$, $B_n(X)$ é um subgrupo normal à $Z_n(X)$.*

Demonstração. Primeiramente, observemos que $B_n(X)$ é um subgrupo normal à $Z_n(X)$. De fato, observe que todo elemento de $B_n(X)$ pode ser escrito como $\partial_{n+1}(x)$ visto que esta aplicação sai de $C_{n+1}(X)$ até $C_n(X)$. Assim, ao aplicar ∂_n, temos $\partial_n(\partial_{n+1}(x)) = 0$, para um $\partial_{n+1}(x)$ qualquer de $B_n(X)$. Portanto $B_n(X)$ é um subgrupo à $Z_n(X)$. Como $Z_n(X)$ é subgrupo do grupo $C_n(X)$ que é abeliano, então $Z_n(X)$ também é um grupo abeliano. Logo, sabendo que todo subgrupo de um grupo abeliano é normal ao grupo, então $B_n(X)$ é normal à $Z_n(X)$. □

Definição 3.16. *Seja X um complexo simplicial. O grupo quociente $H_n(X) = Z_n(X)/B_n(X)$ é o* ***grupo de homologia n-dimensional de*** *X.*

Exemplo 3.17. Vamos calcular $H_n(S)$ para $n = 0, 1, 2, 3$ onde S é a superfície do tetraedro. Encontramos cada $Z_n(S)$ e $B_n(S)$ no exemplo 3.13. Veja que $C_3(S) = \{e\}$ e portanto $Z_n(S) = \{e\} = B_n(S)$, e assim

$$H_3(S) = \{e\}.$$

No caso de $Z_2(S)$ é isomorfo à $\mathbb{Z}$ e vimos que $B_2(S) = \{e\}$. Assim,

$$H_2(S) \simeq \mathbb{Z}.$$

Vimos que $Z_1(S) = B_1(S)$, então o grupo quociente $H_1(S)$ é o grupo trivial de um elemento, ou seja,

$$H_1(S) = \{e\}.$$

Por fim, $Z_0(S)$ é livre abeliano em P_1, P_2, P_3, e P_4, assim, $Z_0(S)$ é isomorfo à $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. Enquanto $B_0(S)$ é livre abeliano em $P_2 - P_1$, $P_3 - P_1$ e $P_4 - P_1$, assim, $B_0(S)$ é isomorfo à $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. Logo,

$$H_0(S) = \frac{Z_0(S)}{B_0(S)} \simeq \frac{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}} \simeq \mathbb{Z}.$$

3.2 Computações do grupo de homologia

Triangulações

Suponha que você deseja obter os grupos de homologia da superfície de uma esfera. Perceba que essa superfície não é um complexo simplicial, pois sua superfície é curvada. Lembre-se que dois espaços são topologicamente iguais se um pode ser obtido do outro com esticamentos, deformações, etc. Imagine o 3-simplexo da superfície do tetraedro com uma superfície maleável, capaz de inflar a si mesmo e se tornar uma esfera, em que as quatro faces aparecerão como "triângulos" desenhados de sua superfície. Isso ilustra a *triangulação* de um espaço.

Propriedades invariantes

Existem dois tipos importantes de *propriedades invariantes* dos grupos de homologia, as provas são um pouco longas, mas pode ser explicado o ponto de vista da demonstração. Primeiramente, os grupos de homologia de um espaço são definidos em termos de triangulação, mas que são sempre

grupos isomorfos não importando como o espaço é triangulado.

Para a segunda propriedade invariante, se um espaço triangulado é homeomorfo a outro, isto é, pode ser deformado no outro sem rasgar ou cortar, os seus grupos de homologia serão isomorfos. Utilizaremos estes dois fatos sem demonstrá-los.

Exemplo 3.18. Os grupos de homologia de uma esfera são isomorfos aos grupos de homologia de um tetraedro, visto que eles são homeomorfos.

Exemplo 3.19. Dois importantes tipos de espaços na topologia são as esferas e as bolas. A **n-bola** E^n é o conjunto de todos os pontos em $\mathbb{R}^n$ uma distância ≤ 1 da origem. Assim, E^3 é o que usualmente pensamos de uma esfera sólida, E^2 é uma região circular, e E^1 é um segmento. A **n-esfera** S^n é o conjunto de todos os pontos de uma unidade da origem em $(n+1)$-dimensional do espaço euclidiano $\mathbb{R}^{n+1}$. Então uma 2-esfera S^2 é a superficie da esfera em $\mathbb{R}^3$, S^1 é a curva do círculo e S^0 são dois pontos. Observemos que a fronteira de cada n-bola é uma (n-1)-esfera, ou seja, a fronteira da esfera sólida E^3 é a superfície da esfera S^2, a fronteira da região circular E^2 é a curva da circunferência S^1 e a fronteira do segmento E^1 são dois pontos S^0.

Espaços conexos por caminho e contrátil

Existe uma interpretação geométrica para o $H_0(X)$ do espaço X com triangulação. Esse espaço é **conexo por caminho** se quaisquer dois pontos podem ser juntados, ou unidos, por um caminho (um conceito no qual não iremos definir) inteiramente contido no espaço. Sabemos que todo espaço conexo por caminho é um espaço conexo, porém nem todo espaço conexo é conexo por caminho. Um espaço é conexo se admite cisão trivial. Se um espaço não é conexo, então ele pode ser separado em uma quantia de pedaços, cada um dos quais é conexo mas nenhum par pode ser conectado por um caminho no espaço. Estes pedaços são as **componentes conexas do espaço**.

Teorema 3.20. *Se um espaço X é triangulado em um número finito de simplexos, então o grupo homológico $H_0(X)$ é isomorfo ao produto direto $\mathbb{Z}\times\mathbb{Z}\times\cdots\mathbb{Z}$, e o número de betti m, que é igual ao número de fatores $\mathbb{Z}$ que esse produto possui, é o número de componentes conexas de X.*

Demonstração. Seja $C_0(X)$ o grupo livre abeliano gerado por um número finito de vértices P_i na triangulação de X. Assim, $B_0(X)$ é gerado por expressões da forma

$$P_{i_2} - P_{i_1},$$

onde $P_{i_1}P_{i_2}$ é uma aresta da trinagulação. Fixemos P_{i_1}. Qualquer vértice P_{i_r} na mesma componente conexa de X que P_{i_1} pode ser unido à P_{i_1} por uma sequência finita

$$P_{i_1}P_{i_2}, P_{i_2}P_{i_3}, \cdots, P_{i_{r-1}}P_{i_r}$$

de arestas. Então

$$P_{i_r} = P_{i_1} + (P_{i_2} - P_{i_1}) + \cdots + (P_{i_r} - P_{i_1}),$$

mostrando que $P_{i_r} \in [P_{i_1} + B_0(X)]$. Observe que, se P_{i_n} não está com as mesmas componentes com P_{i_1}, então $P_{i_n} \notin [P_{i_1} + B_0(X)]$, pois não há arestas que une os dois pontos. Assim, se selecionamos apenas um vértice de cada componente conexa, cada classe lateral de $H_0(X)$ contém exatamente um representante múltiplo inteiro, ou seja, isomorfo à $\mathbb{Z}$. □

Um espaço é **contrátil** se ele pode ser comprimido em um ponto sem ser rasgado ou cortado, *mas sempre mantido com seu espaço originalmente ocupado.*

Teorema 3.21. *Se X é um espaço contrátil triangulado em um número finito de simplexos, então $H_n(X) = 0$ para $n \geq 1$.*

Exemplo 3.22. Sabe-se que S^2 não é contrátil, porém não é um fato fácil de se provar.

Pode-se provar também que todo espaço convexo é contrátil. Logo, toda n-bola é contrátil, já que toda n-bola é convexa.

Computações adicionais

Vimos uma boa interpretação geométrica de $H_0(X)$ do Teorema 3.20. Os 1-ciclos, elementos de $Z_1(X)$, em um espaço triangulado são gerados por curvas fechadas do espaço formados pelas arestas da triangulação, formando o grupo quociente

$$H_1(X) = Z_1(X)/B_1(X)$$

que quantifica a contagem de curvas fechadas no espaço que não aparecem como uma fronteira de uma peça 2-dimensional (i.e., coleções de 2-simplexos) do espaço.
Os 2-ciclos, elementos de $Z_2(X)$, podem ser ilustrados como gerados por esferas ou outras superfícies fechadas 2-dimensional no espaço. De modo similar, $H_2(X) = Z_2(X)/B_2(X)$ quantifica a contagem de superfícies fechadas 2-dimensional no espaço que não podem ser "preenchidas como um sólido", i.e., não são fronteiras de alguma coleção de 3-simplexos.
No caso de $H_1(S^2)$, cada curva fechada feita na superfície da esfera é uma fronteira de alguma parte 2-dimensional da esfera, então $H_1(S^2) = \{e\}$. Entretanto, a única superfície fechada 2-dimensional possível, o próprio S^2, não pode ser "preenchida como um sólido" com o próprio espaço S^2, logo o único 2-ciclo existente não é fronteira de nenhum 3-simplexo, então $H_2(S^2)$ é livre abeliano em um gerador.

Exemplo 3.23. Iremos calcular os grupos de homologia da superfície de um Toro X, conforme a figura abaixo

Figura 3.6: Toro.

Para visualizar a triangulação do Toro, imagine você realizar um corte no círculo marcado com a e então cortar no círculo marcado por b e planificar como na Figura 1.7. Então, desenhe triângulos na região planificada. Para recuperar o Toro basta juntar a aresta b à esquerda com a aresta b à direita, formando um cilindro. Depois, basta juntar os dois círculos a um ao outro, juntando todos os pontos P.

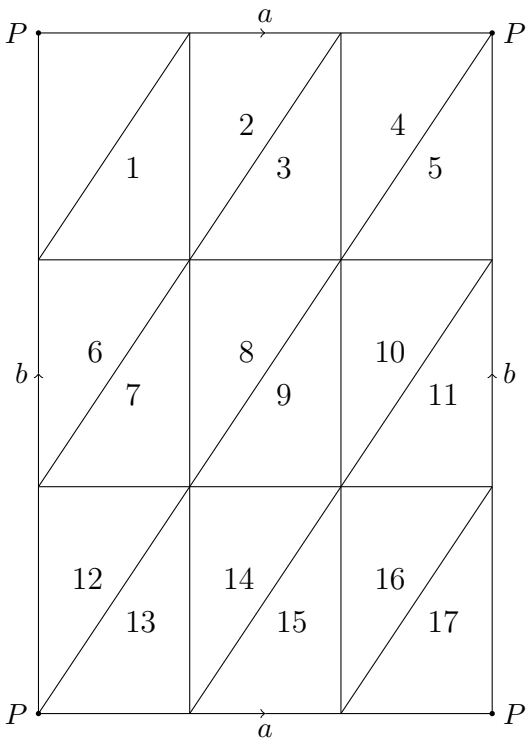


Figura 1.7

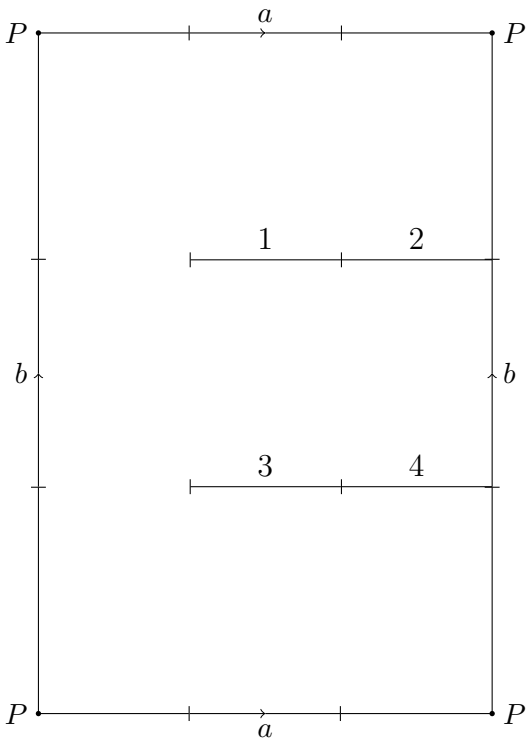


Figura 1.8

Como o Toro é um espaço conexo então pelo Teorema 3.20,

$$H_0(X) \simeq \mathbb{Z}.$$

Para calcular $H_1(X)$, seja z um 1-ciclo, assim como visto na Figura 3.6. Mudando z para um múltiplo de fronteiras do triângulo numerado da Figura 1.7, pode-se obter um ciclo homólogo que não contém o lado / do triângulo 1. Assim, mudando este novo 1-ciclo por um múltiplo adequado da fronteira do triângulo 2, também podemos eliminar o lado | do triângulo 2. Continuamente, eliminamos / de 3, | de 4, / de 5, _ de 6, / de 7, | de 8, / de 9, | de 10, / de 11, _ de 12, / de 13, | de 14, / de 15, | de 16, e / de 17. O ciclo resultante, homologo à z, possui as arestas descritas na Figura 1.8. Mas este ciclo não pode conter, sem um coeficiente não nulo, qualquer uma das arestas que numeramos na Figura 1.8, ou não tera fronteira nula. Então z é homólogo à 1-ciclo tendo arestas apenas no círculo a ou no círculo b (Figura 3.6). Observe que cada aresta no círculo a deve aparecer o mesmo número de vezes, e o mesmo acontece no círculo b; entretanto, uma aresta no círculo b não precisa aparecer o mesmo número de vezes que uma aresta que aparece em a. Além disso, se uma 2-cadeia possui uma fronteira contendo apenas a e b, todos os triângulos orientados no sentido anti-horário devem aparecer com o mesmo coeficiente para que as fronteiras internas se cancelem. A fronteira dessa 2-cadeia é $\{e\}$. Dessa forma a classe lateral

$$z = ra + sb,$$

onde r e s são inteiros. Consequentemente, $H_1(X)$ é abeliano livre em dois geradores, representados pelos círculos a e b. Assim,

$$H_1(X) = Z_1(X)/B_1(X) \simeq \mathbb{Z} \times \mathbb{Z}/\{e\} \simeq \mathbb{Z} \times \mathbb{Z}.$$

Por fim, para calcular $H_2(X)$, veja que um 2-ciclo deve conter um triângulo 2 da Figura 1.7 com sentido anti-horário o mesmo número de vezes que o triângulo 3, também com sentido anti-horário, e assim, a aresta em comum / dos triângulos possui fronteira nula.

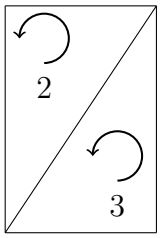
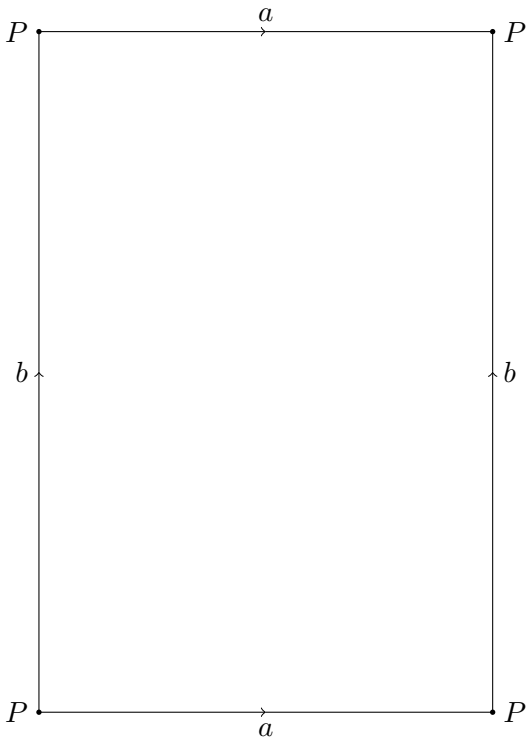


Figura 1.9

Essas orientações são ilustradas na Figura 1.9. O mesmo é verdade para quaisquer triângulos adjacentes, como triângulo 3 e 4, 4 e 5, 5 e 10, entre outros. E todo triângulo com sentido anti-horário vai aparecer um mesmo número de vezes no 2-ciclo. Logo, cada múltiplo da soma formal de todos os 2-simplexos, todos com sentido anti-horário, é exatamente um 2-ciclo. Ou seja, teremos apenas a Figura 1.10.



Então $Z_2(X)$ é um ciclo infinito (infinito dizemos pela quantia de voltas neste 2-ciclo), isomorfo à $\mathbb{Z}$. Além disso, $B_2(X) = \{e\}$, visto que não há 3-simplexos, portanto [1]

$$H_2(X) = Z_2(X)/B_2(X) \simeq \mathbb{Z}/\{e\} \simeq \mathbb{Z}.$$

[1]No link https://www.youtube.com/watch?v=nLcr-DWVEto é possível ver uma animação do efeito do ajuste dessa triangulação

Referências Bibliográficas

[1] Fraleigh, John B. A First Course in Abstract Algebra. 7ª edição. Pearson, 2014.

Rio Claro, 09 de março de 2021

Thiago Moraes Rizzieri
Orientando

Profa.Dra. Elíris Cristina Rizziolli
Orientadora