UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Faculdade de Matemática
Av. João Naves de Àvila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: +55 (34) 3239-4158/4156/4126 - www.famat.ufu.br - famat@ufu.br

ATA DE DEFESA - GRADUAÇÃO

Curso de Graduação em:	Matemática				
Defesa de:	Trabalho de Conclusão de Curso 2 (FAMAT31804)				
Data:	28/06/2023	Hora de início:	13:30	Hora de encerramento:	14:50
Matrícula do Discente:	11921MAT002				
Nome do Discente:	Mateus Fernando Araújo Silva				
Título do Trabalho:	**Introdução à Teoria de Módulos e Ends de Grupos**				

Reuniu-se na Sala 1F119, Campus Santa Mônica, da Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Curso de Graduação em Matemática, assim composta: Profa. Dra. Ligia Laís Fêmina (FAMAT-UFU); Profa. Dra. Taciana Oliveira Souza (FAMAT-UFU); Profa. Dra. Francielle Rodrigues de Castro Coelho (FAMAT-UFU), orientadora do candidato.

Iniciando os trabalhos, a presidente da mesa, Profa. Dra. Francielle Rodrigues de Castro Coelho, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao discente a palavra, para a exposição do seu trabalho. A duração da apresentação do discente e o tempo de arguição e resposta, ocorreram em conformidade com as normas do Curso.

A seguir a senhora presidente concedeu a palavra, pela ordem sucessivamente, às examinadoras, que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando a candidato:

Aprovado. Nota: 100.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Francielle Rodrigues de Castro Coelho**, **Professor(a) do Magistério Superior**, em 28/06/2023, às 16:28, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Ligia Lais Femina**, **Professor(a) do Magistério**

Superior, em 28/06/2023, às 19:25, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Taciana Oliveira Souza**, **Professor(a) do Magistério Superior**, em 29/06/2023, às 10:37, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4587279** e o código CRC **6A1764E8**.

Referência: Processo nº 23117.043323/2023-81 SEI nº 4587279

Universidade Federal de Uberlândia
Faculdade de Matemática
Curso de Graduação em Matemática

INTRODUÇÃO À TEORIA DE MÓDULOS E ENDS DE GRUPOS

Mateus Fernando Araújo Silva

Uberlândia-MG
2023

Mateus Fernando Araújo Silva

INTRODUÇÃO À TEORIA DE MÓDULOS E ENDS DE GRUPOS

Monografia apresentada ao Curso de Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para a obtenção de título de **LICENCIATURA EM MATEMÁTICA**.

Área de concentração: Matemática
Linha de pesquisa: Topologia algébrica

Orientador(a): Francielle Rodrigues de Castro Coelho

Uberlândia-MG
2023

Agradecimentos

Agradeço a Deus e Nossa Senhora por estarem sempre ao meu lado, principalmente nos momentos mais difíceis. Agradeço aos meus pais Mirtes e Ilsimar, por todo apoio, carinho e por sempre me incentivar. Aos meus irmãos Beatriz e Marcos, agradeço por sempre estarem torcendo pelo meu sucesso, a minha irmã por sempre me apoiar e por ter me acolhido na sua casa, ao meu irmão por sempre acreditar no meu potencial e pelas diversas vezes que ele já me levou e buscou na universidade. Quero deixar registrado que sem vocês e nossos pais, seria muito difícil ter continuado a graduação. A meu cunhado Luiz, agradeço por ter me acolhido na sua casa e por todo incentivo, agradeço também a minha cunhada Nicia, por todo apoio.

Agradeço aos meus avós Adão Luzia e Maria das Graças por estarem torcendo sempre pelo meu sucesso. Agradeço ao meu falecido avô Antônio Cândido que veio falecer durante minha graduação, por sempre se orgulhar das minhas conquistas, nunca esquecerei da última vez que você veio na minha casa, foi no meu quarto e viu vários cadernos espalhados na mesa, e seus olhos encheram de água, pois se orgulhou que eu passava muito tempo estudando. De onde estiver, saiba que sentimos muito a sua falta.

Agradeço aos meus tios e tias, em especial a Maria Júnia, Marister, Shirley, Rogério, Terezinha, Mariangela e Lázaro por sempre me apoiarem e acreditarem que eu sou capaz de conquistar meus sonhos. Aos meus primos Jaqueline, Keveson, Rafaela, Helena, Rafael, Arthur, Paulo Atônio, Gabriel e Laura, agradeço por sempre torcerem por mim. Agradeço a minha orientadora Francielle por todos os conselhos, apoio e companherismo durante a minha graduação. Agradeço também aos meus amigos Tiago Aprigio, Julia Bernardes, Victor Cruz e Victor Patrick por todos os conselhos e pelas diversas horas que estudamos juntos.

Na condição de bolsista do PET Matemática da Universidade Federal de Uberlândia, agradeço ao Programa de Educação Tutorial da SESu/MEC pelo fomento.

Resumo

O estudo de Módulos e de Ends de Grupos são bastante relevantes em Álgebra Homológica. O conceito de módulo é uma generalização do conceito de espaço vetorial e o número de ends de um grupo, definido por Specker, é a dimensão de um quociente de espaços vetoriais sobre $\mathbb{Z}_2$. Neste trabalho, apresentamos conceitos e resultados sobre módulos e ends de grupos.

Palavras-chave: Espaços Vetoriais sobre $\mathbb{Z}_2$; Espaços Quocientes; Módulos; Ends de Grupos.

Abstract

The study of Modules and Ends of Groups are very relevant in Homological Algebra. The module concept is a generalization of the vector space concept and the number of ends of a group, defined by Specker, is the dimension of a quotient of vector spaces over $\mathbb{Z}_2$. In this work, we present concepts and results about modules and ends of groups.

Keywords: Vector Spaces over $\mathbb{Z}_2$; Quotient Spaces; Modules; Ends of Groups.

Sumário

Introdução

A Topologia Algébrica é uma área importante da Matemática na qual se resolvem problemas de Topologia com auxílio da Álgebra. Nesta área a Álgebra Homológica (na qual se estudam módulos e ends de grupos) se faz presente e tem bastante relevância.

O conceito de módulo sobre um anel é a generalização da noção de espaço vetorial, em que, em vez de um corpo, temos um anel como o conjunto de escalares. Desse modo, um módulo, como o espaço vetorial, é um grupo abeliano munido de um produto com um anel, satisfazendo algumas propriedades. Já o conceito de ends de um grupo está intimamente relacionado com decomposição de grupos e é definido como a dimensão de um quociente de espaços vetoriais.

A teoria de ends de grupos (mais precisamente, número de ends de um grupo) teve sua origem na teoria de ends de espaços topológicos devido a Freudenthal (em [2]) e Hopf (em [4]) que definiu o número de ends, $e(G)$, de um grupo finitamente gerado G, como sendo o número de ends de um espaço conveniente. Depois, em [10], Specker estendeu este conceito a todos os grupos, apresentando uma definição algébrica que é equivalente a anterior no caso em que o grupo é finitamente gerado.

O presente trabalho visa apresentar uma introdução ao estudo de módulos e explorar o conceito e alguns resultados sobre ends, para alguns grupos.

No capítulo 1, recordamos assuntos de Álgebra Linear, mais precisamente, estudamos espaços vetoriais sobre o corpo $\mathbb{Z}_2$, incluindo espaços quocientes, uma vez que tais assuntos em geral não são tão explorados em um curso normal de Álgebra Linear. A principal referência para este capítulo é [5].

No capítulo 2, apresentamos uma introdução ao estudo de módulos sobre um anel. Mais especificamente, abordamos os conceitos de módulos, submódulos, homomorfismos entre módulos e $\mathbb{Z}_2G-$módulos. As principais referências para este capítulo são [1] e [6].

Por fim, no capítulo 3, introduzimos e exemplificamos o conceito de ends de grupos e apresentamos resultados com relação ao número de ends de um grupo G nos casos em que G são os seguintes

grupos: finito, infinito, cíclico infinito, não enumerável e quociente. As principais referências para este capítulo são [7], [8] e [9].

CAPÍTULO 1

Espaços Vetoriais sobre $\mathbb{Z}_2$

Faremos neste capítulo uma revisão de alguns tópicos de Álgebra Linear dando ênfase em geral a espaços vetoriais sobre o corpo $K = \mathbb{Z}_2$ e a espaços quocientes, uma vez que esses tópicos em geral não são explorados num curso normal de Álgebra Linear e são de grande importância para o desenvolvimento deste trabalho.

1.1 Definição e Exemplos

Definição 1.1 *Um conjunto não vazio V é um **espaço vetorial sobre um corpo K** ou um $K-$**espaço vetorial** (cujos elementos são denominados vetores), se estiverem definidas as seguintes duas operações:*

(A) *A cada par (u,v) de vetores de $V \times V$ se associa um vetor $u+v \in V$, chamado de soma de u e v, de modo que:*

(A_1) $(u+v)+w = u+(v+w), \forall u,v,w \in V$.

(A_2) $u+v = v+u, \forall u,v \in V$.

(A_3) *Exista um vetor em V, denominado vetor nulo e denotado por 0, tal que $0+v = v$.*

(A_4) *Para cada vetor $v \in V$ exista um vetor em V, denotado por $-v$, tal que $v+(-v) = 0$.*

(M) *A cada par (α,v) de vetores de $K \times V$ se associa um vetor $\alpha \cdot v \in V$, denominado multiplicação por escalar de α por v, de modo que:*

(M_1) $(\alpha\beta)\cdot v = \alpha \cdot (\beta \cdot v), \forall \alpha,\beta \in K$ *e* $\forall v \in V$.

(M_2) $1 \cdot v = v, \forall v \in V$ *(onde* 1 *é o escalar unidade de* K*).*

(M_3) $\alpha \cdot (u+v) = \alpha \cdot u + \alpha \cdot v, \forall \alpha \in K$ *e* $\forall u, v \in V$.

(M_4) $(\alpha+\beta) \cdot v = \alpha \cdot v + \beta \cdot v, \forall \alpha, \beta \in K$ *e* $v \in V$.

Note que as condições A_1 *a* A_4 *nos dizem que* $(V,+)$ *é um grupo abeliano.*

Seja V um espaço vetorial sobre K. As propriedades a seguir são consequência imediata da definição de espaço vetorial.

(P_1) Para todo $\alpha \in K, \alpha \cdot 0 = 0$.

(P_2) Para todo $v \in V, 0 \cdot v = 0$.

(P_3) Se $\alpha \cdot v = 0$, com $\alpha \in K$ e $v \in V$, então ou $\alpha = 0$ ou $v = 0$.

(P_4) Para todo $\alpha \in K$ e todo $v \in V, (-\alpha)v = \alpha(-v) = -\alpha v$.

(P_5) O vetor nulo de um espaço vetorial V é único.

(P_6) Para cada vetor $v \in V$, existe um único vetor $(-v)$, oposto de v.

(P_7) Para cada $v \in V$, tem-se $-(-v) = v$.

Exemplo 1.2 *Consideremos* K *um corpo qualquer e* $V = K^n = \{(x_1, x_2, ..., x_n) | x_i \in K\}$. V *é um espaço vetorial sobre* K *com a operação adição e a multiplicação por escalar dadas, respectivamente, por:*

$(x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n) = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$,

$\alpha(x_1, x_2, ..., x_n) = (\alpha x_1, \alpha x_2, ..., \alpha x_n), \forall \alpha \in K$.

Em particular, $\mathbb{R}^n$ *é um espaço vetorial sobre* $\mathbb{R}$ *e* $\mathbb{Z}_2^n$ *é um espaço vetorial sobre* $\mathbb{Z}_2$.

Exemplo 1.3 *Seja* $A \neq \emptyset$ *e consideremos* $V = P(A) = \{X | X \subset A\}$. *Podemos verificar que* $(P(A),+)$ *é um grupo abeliano (em que todo elemento não nulo tem ordem 2) com a operação diferença simétrica, isto é,*

$$X \triangle Y = (X \cup Y) - (X \cap Y) = (X \cap Y^c) \cup (X^c \cap Y),$$

que iremos indicar sempre aditivamente, ou seja, $X + Y = X \triangle Y$.

Considere a multiplicação por escalar $\mathbb{Z}_2 \times P(A) \to P(A)$ *dada por* $\overline{0} \cdot X = \emptyset$ *e* $\overline{1} \cdot X = X$. *Esta multiplicação está bem definida e verifica os demais axiomas da definição de espaço vetorial sobre o*

corpo $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$. *Assim,* $P(A)$ *é um espaço vetorial sobre* $\mathbb{Z}_2$ *para todo* $A \neq \emptyset$. *Em particular, se* G *é um grupo,* $P(G)$ *é um espaço vetorial sobre* $\mathbb{Z}_2$.

Este $\mathbb{Z}_2-$*espaço vetorial será de fundamental importância na definição de ends de* G.

Proposição 1.4 *Seja* $V \neq \emptyset$ *munido de uma operação* "$+$". *Então* $(V,+)$ *é um* $\mathbb{Z}_2-$*espaço vetorial se, e somente se,* $(V,+)$ *é um grupo abeliano, em que todo elemento tem ordem* 2.

Demonstração: ($\Longrightarrow$) Segue da definição de espaço vetorial que $(V,+)$ é um grupo abeliano. Agora, para qualquer $v \in V^*$, temos

$$v + v = \overline{1} \cdot v + \overline{1} \cdot v = (\overline{1} + \overline{1}) \cdot v = \overline{0} \cdot v = 0,$$

e assim, a ordem de v é 2.

($\Longleftarrow$) Basta considerarmos a operação adição (do grupo abeliano $(V,+)$) e a multiplicação por escalar dada por $\overline{0} \cdot v := 0$ e $\overline{1} \cdot v := v$.

■

Nota: Em muitas situações consideraremos $\mathbb{Z}_2 = \{0,1\}$ (isto é, sem as barras nos elementos).

1.2 Subespaços Vetoriais

Definição 1.5 *Seja* V *um espaço vetorial sobre um corpo* K. *Um subconjunto* W *de* V *é um* ***subespaço vetorial de*** V *se a restrição das operações de* V *a* W *torna esse conjunto um* $K-$*espaço vetorial.*

Exemplo 1.6 *O conjunto* $\{0\}$ *formado apenas pelo vetor nulo e o espaço todo* V *são subespaços de* V, *chamados subespaços impróprios ou triviais.*

O resultado seguinte é bastante útil para verificar se um dado subconjunto de um espaço vetorial é ou não um subespaço vetorial.

Teorema 1.7 *Sejam* V *um espaço vetorial sobre* K *e* $W \subseteq V$ *um subconjunto. Então* W *é um subespaço de* V *se, e somente se, satisfaz as seguintes propriedades:*

(i) *W é não-vazio;*

(ii) *W é fechado para a adição de vetores: se $u, w \in W$ então $u + w \in W$;*

(iii) *W é fechado para a multiplicação por escalar: $k \in K$ e $u \in W$ implica $ku \in W$.*

Demonstração: ($\Longrightarrow$) Se W é um subespaço vetorial de V, então claramente, (i),(ii) e (iii) são válidas.

($\Longleftarrow$) Suponhamos que W satisfaz (i),(ii) e (iii). Por (i), W é não-vazio, e por (ii) e (iii), as operações de adição e multiplicação por escalar estão bem definidas em W. Além disso, as propriedades $(A_1),(A_2),(M_1),(M_2),(M_3)$ e (M_4) valem em W pois os vetores de W pertencem a V.

Portanto, precisamos mostrar que (A_3) e (A_4) também valem em W. Por (i), W é não-vazio, então suponhamos $u \in W$. Segue, por (ii), que $0u = 0 \in W$ e obviamente $v + 0 = v$ para todo $v \in W$. Assim, W satisfaz (A_3).

Finalmente, se $v \in W$, então $(-1)v = -v \in W$ e, $v + (-v) = 0$. Logo, W satisfaz (A_4).

Portanto, W é subespaço de V.

■

Corolário 1.8 *W é subespaço de V se, e somente se,*

(i) *$0 \in W$ (ou $W \neq \emptyset$);*

(ii) *$v, w \in W$ implica $av + bw \in W$ para todo $a, b \in K$.*

Demonstração: ($\Longrightarrow$) Se W é subespaço de V, então (i) e (ii) são necessariamente válidas em W.

($\Longleftarrow$) Suponhamos que W satisfaz (i) e (ii). Então, por (i), W é não vazio. Além disso, segue de (ii) que se $v, w \in W$, então $u + w = 1 \cdot u + 1 \cdot w \in W$ e, se $v \in W$ e $k \in K$, então $kv = kv + 0v \in W$.

Logo, pelo teorema anterior, W é subespaço de V.

■

Proposição 1.9 *A interseção de um número qualquer de subespaços de um espaço vetorial V é um subespaço de V. Em particular, a interseção de dois subespaços vetoriais de V é um subespaço vetorial.*

Demonstração: Seja $U = \bigcap_{i \in I} U_i$, onde I é o conjunto de índices e U_i são subespaços de V. Assim, temos que:

(i) $0 \in U_i, \forall i \in I$, pois todo U_i é um subespaço de V. Logo, $0 \in U$.

(ii) Suponhamos que $u, v \in U$. Então $u, v \in U_i, \forall i \in I$. Logo, $u + v \in U_i$, $\forall i \in I$. Portanto, $u + v \in U$.

(iii) Suponhamos que $u \in U$ e $a \in K$. Então $u \in U_i, \forall i \in I$, e como cada U_i é um subespaço, segue que $au \in U_i, \forall i \in I$. Logo, $au \in U$.

De (i),(ii) e (iii), segue que U é um subespaço de V.

■

Observação 1.10 *A reunião de um número qualquer de subespaços de um espaço vetorial V nem sempre é um subespaço de V, uma vez que se tomarmos um vetor em cada subespaço, a soma deles pode não pertencer à reunião.*

Exemplo 1.11 *Sejam $A \neq \emptyset$ e $F(A) = \{X \in P(A) | X \text{ é finito}\}$, $F(A)$ é um subespaço do $\mathbb{Z}_2$–espaço vetorial $P(A)$ dado no exemplo 1.3.*

(i) *O conjunto vazio é finito (com zero elemento) e assim pertence a $F(A)$.*

(ii) *$X, Y \in F(A)$, implica $a \cdot X + b \cdot Y \in F(A)$ para todo $a, b \in \mathbb{Z}_2$, pois*

$a = \overline{0}, b = \overline{0} \Longrightarrow a \cdot X + b \cdot Y = \emptyset$.

$a = \overline{1}, b = \overline{0} \Longrightarrow a \cdot X + b \cdot Y = X$.

$a = \overline{0}, b = \overline{1} \Longrightarrow a \cdot X + b \cdot Y = Y$.

$a = \overline{1}, b = \overline{1} \Longrightarrow a \cdot X + b \cdot Y = X + Y = (X \cap Y^c) \cup (X^c \cap Y) \subset X \cup Y$.

Como $\emptyset$, X, Y e $X \cup Y$ são finitos, segue que $a \cdot X + b \cdot Y \in F(A)$.

Observação 1.12 *No exemplo anterior temos:*

- *Se A é finito então $F(A) = P(A)$.*
- *Se A é infinito então necessariamente $F(A) \neq P(A)$, pois $A \in P(A)$ e $A \notin F(A)$.*

Por exemplo, $\mathbb{Z} \in P(\mathbb{Z})$, mas $\mathbb{Z} \notin F(\mathbb{Z})$.

Exemplo 1.13 *Seja $(G, \cdot)$ um grupo. Considere o $\mathbb{Z}_2$–espaço vetorial $P(G)$. Seja*

$$Q(G) = \{X \subset G | X + gX \in F(G), \forall g \in G\}.$$

Aqui, dado $g \in G, gX := \{g \cdot x | x \in X\}$*, onde* "$\cdot$" *indica a operação do grupo.*

Observemos que:

- $g(X \cup Y) = gX \cup gY$ *(claro).*
- $g(X \cap Y) = gX \cap gY$*, pois* $g \cdot x = g \cdot y \iff g^{-1} \cdot g \cdot x = g^{-1} \cdot g \cdot y \iff x = y$.
- $gX^c = (gX)^c$*, pois* $G = gG = g(X \cup X^c) = gX \cup gX^c$ *e* $\emptyset = g(X \cap X^c) = gX \cap gX^c$.
- $g(X+Y) = g[(X \cap Y^c) \cup (X^c \cap Y)] = g(X \cap Y^c) \cup g(X^c \cap Y) = [gX \cap (gY)^c] \cup [(gX)^c \cap gY] = gX + gY$.

Agora, mostremos que $Q(G)$ *é um subespaço vetorial de* $P(G)$*. De fato,*

- $Q(G) \neq \emptyset$*, pois* $\emptyset \in Q(G)$.
- $\forall X, Y \in Q(G), (X+Y) + g(X+Y) = X + Y + gX + gY = (X + gX) + (Y + gY) \in F(G)$*. Logo,* $X + Y \in Q(G)$.
- $\forall k \in \mathbb{Z}_2$ *e* $\forall X \in Q(G), k \cdot X \in Q(G)$ *pois* $\overline{0} \cdot X + g(\overline{0} \cdot X) = \emptyset \in F(G)$ *e* $\overline{1} \cdot X + g(\overline{1} \cdot X) = X + gX \in F(G)$.

Observação 1.14 *Se* $X \in F(G)$ *então* $X + gX$ *será finito, para todo* $g \in G$*. Daí,* $X \in Q(G)$*, isto é,* $F(G) \subset Q(G)$*. Além disso,* $F(G)$ *é um subespaço vetorial de* $Q(G)$.

Observação 1.15 *No caso em que G é finito temos que* $P(G) = F(G) = Q(G)$.

Definição 1.16 *Sejam U e W subespaços de um espaço vetorial V. A* ***soma*** *de U e W, denotada por* $U + W$*, consiste de todas as somas* $u + w$*, onde* $u \in U$ *e* $w \in W$*, isto é,*

$$U + W = \{u + w | u \in U \text{ e } w \in W\}.$$

Teorema 1.17 *A soma* $U + W$ *dos subespaços U e W de V é também um subespaço de V.*

Demonstração: Notemos que $0 = 0 + 0 \in U + W$, pois $0 \in U$ e $0 \in W$. Além disso, suponhamos que $u + w$ e $u' + w'$ pertencem a $U + W$, com $u, u' \in U$ e $w, w' \in W$. Então, $(u + w) + (u' + w') = (u + u') + (w + w') \in U + W$, e, para qualquer escalar $k \in K, k(u + w) = ku + kw \in U + W$.

Portanto, $U + W$ é subespaço de V.

■

Definição 1.18 *Sejam V um $K-$espaço vetorial e U e W dois subespaços de V. Diremos que V é* ***soma direta*** *de U e W se todo vetor $v \in V$ pode ser escrito de uma única maneira, como $v = u + w$ onde $u \in U$ e $w \in W$. Neste caso, escrevemos $V = U \oplus W$.*

Teorema 1.19 *O espaço vetorial V é soma direta de seus subespaços U e W se, e somente se,*

(i) $V = U + W$;

(ii) $U \cap W = \{0\}$.

Demonstração: ($\Longrightarrow$) Suponhamos que $V = U \oplus W$. Então, qualquer $v \in V$ pode ser escrito de maneira única na forma $v = u + w$, com $u \in U$ e $w \in W$. Assim, em particular, $V = U + W$. Agora, suponha $v \in U \cap W$. Então,

(i) $v = v + 0$, onde $v \in U, 0 \in W$, e

(ii) $v = 0 + v$, onde $0 \in U, v \in W$.

Como tal soma deve ser única para v, então $v = 0$. De acordo com isso, $U \cap W = \{0\}$.

($\Longleftarrow$) Agora, suponha que $V = U + W$ e $U \cap W = \{0\}$. Seja $v \in V$. Como $V = U + W$, existem $u \in U$ e $w \in W$ tais que $v = u + w$.

Mostremos que essa soma é única. Suponhamos também que $v = u' + w'$ onde $u' \in U$ e $w' \in W$. Então, $u + w = u' + w'$. Daí segue que $u - u' = w' - w \in U \cap W$ pois $u - u' \in U$ e $w - w' \in W$. Como $U \cap W = \{0\}$, teremos $u = u'$ e $w = w'$ como queríamos.

■

Exemplo 1.20 *O espaço $\mathbb{R}^3$ é soma direta dos subespaços:*

$$U = \{(x, 0, 0) | \, x \in \mathbb{R}\} \text{ e } W = \{(0, y, z) | \, y, z \in \mathbb{R}\},$$

pois pela definição temos que $U \cap W = \{(0,0,0)\}$. Por outro lado, para qualquer $(x, y, z) \in \mathbb{R}^3, (x, y, z) = (x, 0, 0) + (0, y, z) \in U + W$.

Portanto, $\mathbb{R}^3 = U \oplus W$.

Definição 1.21 *Sejam V um espaço vetorial sobre um corpo K e $v_1, v_2, ..., v_n \in V$. Qualquer vetor em V da forma $a_1v_1 + a_2v_2 + ... + a_nv_n$, onde a_i's $\in K$, é chamado uma* ***combinação linear*** *de $v_1, v_2, ..., v_n$.*

Teorema 1.22 *Seja S um subconjunto não vazio de V. O conjunto de todas as combinações lineares de vetores em S, denotado por $[S]$, é um subespaço de V contendo S, chamado subespaço gerado por S. Além disso, se W é qualquer outro subespaço de V contendo S, então $[S] \subset W$.*

Demonstração: Se $v \in S$, então $v = 1 \cdot v \in [S]$. Também $[S]$ é não vazio, pois S é não vazio.

Agora suponhamos que $u, w \in [S]$. Assim, $u = a_1v_1 + ... + a_nv_n$ e $w = b_1v_1 + ... + b_nv_n$, onde v_i's $\in S$ e a_i's, b_j's $\in K$.

Então, $u + w = (a_1 + b_1)v_1 + ... + (a_n + b_n)v_n$ e, para qualquer escalar $k \in K$, $k \cdot u = k \cdot (a_1v_1 + ... + a_nv_n) = k \cdot a_1v_1 + ... + k \cdot a_nv_n$ pertencem a $[S]$, pois cada um é combinação linear de vetores de S.

Deste modo, $[S]$ é um subespaço de V.

Agora, suponha que W é um subespaço de V contendo S e sejam $v_1, v_2, ..., v_m \in S \subset W$.

Então todos os múltiplos $a_1v_1, a_2v_2, ..., a_mv_m \in W$, onde a_i's $\in K$, e portanto, a soma $a_1v_1 + a_2v_2 + ... + a_mv_m \in W$. Ou seja, W contém todas as combinações lineares de elementos de S.

Consequentemente, $[S] \subset W$.

■

Observação 1.23 *Segue do teorema anterior que $[S]$ é o menor subespaço vetorial de V que contém S.*

Observação 1.24 $[S] = [S \cup \{0\}]$. *Isto é, acrescentando ou removendo o vetor nulo de um conjunto, não mudamos o espaço gerado pelo conjunto.*

Definição 1.25 *Dizemos que um espaço vetorial V é **finitamente gerado** se existe $S \subset V$, S finito, de maneira que $V = [S]$.*

Exemplo 1.26 *Seja V o espaço vetorial $\mathbb{R}^3$. O subespaço gerado por qualquer vetor u, não nulo, consiste em todos os múltiplos escalares de u. Geometricamente, é a reta que passa pela origem e pelo ponto u. O espaço gerado por quaisquer dois vetores u e v que não são múltiplos um do outro é o plano que passa pela origem e contém os vetores u e v.*

Exemplo 1.27 *Dados os vetores $e_1 = (1,0,0,0), e_2 = (0,1,0,0), e_3 = (0,0,1,0), e_4 = (0,0,0,1)$ e $S = \{e_1, e_2, e_3, e_4\}$. Então $\mathbb{R}^4 = [S]$. De fato, dado $x \in \mathbb{R}^4, x = (x_1, x_2, x_3, x_4), x_i$'s $\in \mathbb{R}$, temos que $x = x_1(1,0,0,0) + x_2(0,1,0,0) + x_3(0,0,1,0) + x_4(0,0,0,1) = x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 \in [S]$. Logo, $\mathbb{R}^4 \subset [S]$.*

Por outro lado, se $x \in [S]$*, temos que* $x = a_1e_1 + a_2e_2 + a_3e_3 + a_4e_4 = a_1(1,0,0,0) + a_2(0,1,0,0) + a_3(0,0,1,0) + a_4(0,0,0,1) = (a_1,a_2,a_3,a_4) \in \mathbb{R}^4$*. Logo,* $[S] \subset \mathbb{R}^4$.

Portanto, $\mathbb{R}^4 = [S]$.

1.3 Base e Dimensão

Definição 1.28 *Sejam* V *um espaço vetorial sobre um corpo* K *e* $v_1, v_2, ..., v_n \in V$.

(i) *Dizemos que os vetores* $v_1, v_2, ..., v_n \in V$ *são* ***linearmente dependentes (L.D.) sobre K****, ou que o subconjunto finito* $S = \{v_1, v_2, ..., v_n\}$ *de* V *é* ***linearmente dependente*** *se* $a_1v_1 + a_2v_2 + ... + a_nv_n = 0$*, com* a_i*'s* $\in K$*, não todos nulos.*

(ii) *Os vetores são* ***linearmente independentes (L.I.) sobre K****, ou o subconjunto* S *é* ***linearmente independente*** *se não for linearmente dependente.*

Observação 1.29 *A relação* $a_1v_1 + a_2v_2 + ... + a_nv_n = 0$ *será sempre válida se os* a_i*'s são todos* 0*. Se essa relação é válida somente neste caso, isto é,*

$$a_1v_1 + a_2v_2 + ... + a_nv_n = 0 \text{ se, e somente se, } a_1 = 0, a_2 = 0, ..., a_n = 0,$$

então os vetores são linearmente independentes. Por outro lado, se a relação $a_1v_1 + a_2v_2 + ... + a_nv_n = 0$ *também é válida quando um dos* a_i*'s não é* 0*, então os vetores são linearmente dependentes.*

Proposição 1.30 *Os vetores não nulos* $v_1, v_2, ..., v_n$ *de um espaço vetorial* V *são linearmente dependentes se, e somente se, um deles é combinação linear dos vetores precedentes.*

Demonstração: ($\Longrightarrow$) Suponha que os v_i*'s* são linearmente dependentes. Então existem escalares $a_1, a_2, ..., a_n$, não todos nulos, tais que $a_1v_1 + a_2v_2 + ... + a_nv_n = 0$. Seja k o maior inteiro tal que $a_k \neq 0$.

Assim, $a_1v_1 + ... + a_kv_k + 0v_{k+1} + ... + 0v_n = 0$ ou $a_1v_1 + ... + a_kv_k = 0$. Se $k = 1$ então $a_1v_1 = 0$ e como $a_1 \neq 0$ segue que $v_1 = 0$. Mas os v_i*'s* são todos não-nulos, portanto $k > 1$ e $v_k = -a_k^{-1}a_1v_1 - ... - a_k^{-1}a_{k-1}v_{k-1}$. Isto é, v_k é uma combinação linear dos vetores precedentes.

($\Longleftarrow$) Suponhamos $v_i = a_1v_1 + a_2v_2 + ... + a_{i-1}v_{i-1}$. Então,

$$a_1v_1 + a_2v_2 + ... + a_{i-1}v_{i-1} - v_i + 0v_{i+1} + ... + 0v_n = 0,$$

e o coeficiente de v_i não é nulo. Portanto, $v_1, v_2, ..., v_n$ são linearmente dependentes.

■

Consideremos um espaço vetorial sobre um corpo K. Vejamos algumas propriedades de (in)dependência linear.

(L_1) Se um conjunto finito $S \subset V$ contém o vetor nulo, então esse conjunto é $L.D.$

(L_2) Se $S = \{u\} \subset V$ e $u \neq 0$, então S é $L.I.$

(L_3) Sejam S_1 e S_2 subconjuntos finitos e não vazios de V, com $S_1 \subset S_2$. Se S_1 (S_2) é $L.D.$ ($L.I.$), então S_2 (S_1) também é $L.D.$ ($L.I.$).

(L_4) Se $S = \{u_1, u_2, ..., u_n\}$ é $L.I.$ e, para um certo $u \in V$ tivermos $S \cup \{u\} = \{u_1, u_2, ..., u_n, u\}$ $L.D.$, então o vetor u é combinação linear dos vetores $u_1, u_2, ..., u_n$, isto é, $u \in [S]$.

(L_5) Se $S = \{u_1, ..., u_j, ..., u_n\}$ e $u_j \in [S - \{u_j\}]$ (ou seja, u_j é combinação linear dos demais vetores de S), então $[S] = [S - \{u_j\}]$.

Observação 1.31 *Se dois dos vetores $v_1, v_2, ..., v_n$ são iguais, suponhamos $v_1 = v_2$, então os vetores são dependentes, pois $v_1 - v_2 + 0v_3 + ... + 0v_n = 0$ e os coeficientes de v_1 e v_2 não são nulos. Isto também segue da propriedade L_3), pois $S_1 = \{v_1, v_2\}$ é $L.D.$ e está contido em $S_2 = \{v_1, v_2, ..., v_n\}$.*

Observação 1.32 *Convencionaremos o conjunto $\emptyset$ como linearmente independente.*

Definição 1.33 *Seja V um espaço vetorial sobre um corpo K. Dizemos que um subconjunto finito B de V é uma **base** de V se*

(i) *$[B] = V$, isto é, B for um subconjunto gerador de V,*

(ii) *B for linearmente independente.*

Exemplo 1.34 *Seja K um corpo qualquer. Consideremos o espaço vetorial $V = K^n$ (vide exemplo 1.2) que consiste de $n-$uplas de elementos de K. Os vetores*

$$e_1 = (1, 0, 0, ..., 0, 0)$$

$$e_2 = (0, 1, 0, ..., 0, 0)$$

$$\vdots$$

$$e_n = (0,0,0,...,0,1)$$

formam uma base $B = \{e_1, e_2, ..., e_n\}$ *chamada base canônica de* K^n. *De fato,*

- B *gera* K^n, *pois todo* $(x_1, x_2, ..., x_n) \in K^n, (x_1, x_2, ..., x_n) = x_1 \cdot e_1 + x_2 \cdot e_2 + ... + x_n \cdot e_n$.

- B *é linearmente independente, pois se* $a_1 \cdot e_1 + a_2 \cdot e_2 + ... + a_n \cdot e_n = (0,0,...,0)$, *então* $a_1 = a_2 = ... = a_n = 0$.

Exemplo 1.35 $B = \{\{a\}, \{b\}\}$ *é uma base do* $\mathbb{Z}_2$*–espaço vetorial* $P(\{a,b\})$ *(exemplo 1.3), pois* B *gera* $P(\{a,b\})$ *e é* $L.I.$, *pois se* B *fosse* $L.D.$ *existiria* $k \in \mathbb{Z}_2$ *tal que* $\{a\} = k\{b\}$ *e como* $k = \overline{0}$ *ou* $k = \overline{1}$, *então* $\{a\} = \emptyset$ *ou* $\{a\} = \{b\}$ *(absurdo).*

Definição 1.36 *Sejam* $B = \{v_1, v_2, ..., v_n\}$ *uma base de um espaço vetorial* V *e* $v \in V$, *onde* $v = a_1 v_1 + a_2 v_2 + ... + a_n v_n$. *Os elementos* $a_1, a_2, ..., a_n$ *são chamados* ***coordenadas*** *de* v *em relação à base* B.

Proposição 1.37 *Todo espaço vetorial finitamente gerado admite uma base.*

Demonstração: Seja V um espaço vetorial finitamente gerado sobre K. Se $V = \{0\}$, então $\emptyset$ é uma base de V devido às convenções a respeito para este caso.

Caso contrário, existe um subconjunto finito e não vazio $S \subset V$, de forma que $V = [S]$. Como $S \neq \emptyset$, então existem subconjuntos não vazios de S que são $L.I.$. Tomemos um deles com o maior número possível de elementos. Indicando por B esse subconjunto, afirmamos que B é base de V.

Devido à maneira como tomamos B, para todo $u \in S - B$ teremos que $B \cup \{u\}$ é $L.D.$. Logo, u é combinação linear dos elementos de B (pela propriedade (L_4) de (in)dependência linear). Agora, usando a (L_5) de (in)dependência linear, conclui-se que $[B] = [S] = V$.

Como, por outro lado, B é $L.I.$, pela maneira como foi construída, então B é uma base de V.

■

Observação 1.38 *Um espaço vetorial sobre* K *pode ter mais de uma base. Por exemplo,* $B = \{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$ *(base canônica) e* $C = \{(1,0,0,0),(0,-2,0,0),(0,0,3,0),(0,0,0,-1)\}$ *são bases do* $\mathbb{R}^4$.

Nosso objetivo agora é mostrar que se V é um espaço vetorial finitamente gerado então todas as bases de V tem o mesmo número de vetores. Para isto necessitamos dos seguintes lemas:

Lema 1.39 *Seja $B = \{v_1, v_2, ..., v_n\}$ uma base de um espaço vetorial V. Se $u \in V$ e ainda se*

$$u = a_1v_1 + ... + a_iv_i + ... + a_nv_n \tag{1.1}$$

com $a_i \neq 0$, então $C = \{v_1, ..., v_{i-1}, u, v_{i+1}, ..., v_n\}$ também é uma base de V.

Demonstração: Faremos a demonstração supondo $i = 1$ para facilitar o trabalho com os índices.

(i) Como $a_1 \neq 0$, da equação 1.1 segue que

$$v_1 = bu + b_2v_2 + ... + b_nv_n \tag{1.2}$$

onde $b = a_1^{-1}, b_2 = -a_1^{-1}a_2, ..., b_n = -a_1^{-1}a_n$. Seja $w \in V$. Então, como B é base de V, existem $c_1, c_2, ..., c_n \in K$ de maneira que

$$w = c_1v_1 + c_2v_2 + ... + c_nv_n \tag{1.3}$$

substituindo 1.2 em 1.3 teremos:

$$w = (c_1b)u + (c_1b + c_2)v_2 + ... + (c_1b_n + c_n)v_n.$$

Assim, fica provado que o espaço V é gerado por $\{u, v_2, ..., v_n\}$.

(ii) Suponhamos

$$xu + x_2v_2 + ... + x_nv_n = 0 \tag{1.4}$$

com $x, x_2, ..., x_n \in K$. Substituindo 1.1 em 1.4 teremos:

$$(xa_1)v_1 + (xa_2 + x_2)v_2 + ... + (xa_n + x_n)v_n = 0.$$

Como B é $L.I.$, desta última igualdade decorre que:

$$xa_1 = 0, xa_2 + x_2 = 0, ..., xa_n + x_n = 0.$$

Mas $a_1 \neq 0$. Logo, $x = 0, x_2 = 0, ..., x_n = 0$.

Portanto, C é base de V.

■

Lema 1.40 *Suponhamos que exista uma base de V com n vetores. Então se $B = \{v_1, v_2, ..., v_n\} \subset V$ é $L.I.$, e possui n vetores, B também é uma base de V.*

Demonstração: Seja $C = \{u_1, u_2, ..., u_n\}$ uma base de V. Então

$$v_1 = a_1u_1 + a_2u_2 + ... + a_nu_n \ (a_1, a_2, ..., a_n \in K).$$

Não podemos ter todos os escalares nesta igualdade nulos, pois isto implicaria que $v_1 = 0$ o que é impossível já que o conjunto B é $L.I.$. Logo, um dos a_i's não é nulo. Suponhamos $a_1 \neq 0$. O lema 1.39 nos assegura então que $\{v_1, u_2, ..., u_n\}$ é uma base de V. Portanto, v_2 é uma combinação liner deste conjunto, ou seja, existem $b_1, b_2, ..., b_n \in K$ de maneira que

$$v_2 = b_1v_1 + b_2u_2 + ... + b_nu_n.$$

Também não podemos ter $b_2 = b_3 = ... = b_n = 0$, senão $\{v_1, v_2\}$ seria $L.D.$ e, portanto o mesmo aconteceria como conjunto B. Admitindo que $b_2 \neq 0$ teremos, de acordo com o lema anterior, que $\{v_1, v_2, u_3, ..., u_n\}$ é também uma base de V. A repetição deste raciocínio nos levará à conclusão de que $\{v_1, v_2, ..., v_n\}$ é uma base de V.

■

Lema 1.41 *Suponhamos que V tenha uma base com n vetores. Então todo subconjunto de V que seja $L.I.$ tem no máximo n vetores (ou equivalentemente, qualquer subconjunto de V com mais de n vetores é $L.D.$).*

Demonstração: Suponhamos que exista $S = \{v_1, ..., v_n, v_{n+1}, ..., v_t\} \subset V$ que tenha $t > n$ vetores e é um subconjunto $L.I.$. Logo $B = \{v_1, ..., v_n\}$ é base de V por causa do lema anterior. Daí,

$$\exists a_1, a_2, ..., a_n \in K;\ v_{n+1} = a_1v_1 + a_2v_2 + ... + a_nv_n.$$

Então $a_1v_1 + a_2v_2 + ... + a_nv_n + (-1)v_{n+1} = 0$ o que mostra que o conjunto S é $L.D.$ (absurdo).

■

Teorema 1.42 ***(Invariância).*** *Seja V um espaço vetorial finitamente gerado. Então todas as bases de V têm o mesmo número de vetores.*

Demonstração: Sejam $B = \{v_1, v_2, ..., v_n\}$ e $C = \{u_1, u_2, ..., u_m\}$ duas bases quaisquer de V. Pelo lema anterior, como B é base de V e C é $L.I.$, então $m \leq n$. Analogamente, como C é base de V e B é $L.I.$, então $n \leq m$. Portanto, $m = n$.

■

Definição 1.43 *Seja V um espaço vetorial sobre K finitamente gerado. Denomina-se* ***dimensão de V sobre K*** *(ou simplesmente* ***dimensão de V****), o número de vetores de uma base qualquer de V.*

Notação: $dim_K V$ ou $dim V$ (quando estiver claro o corpo considerado). Diz-se também, neste caso, que V é um espaço de dimensão finita n, onde $n = dim_K V$ ou que V é um espaço vetorial $n-$dimensional.

Exemplo 1.44 *$dim_{\mathbb{Z}_2} P(\{a,b\}) = 2$, visto que $\{\{a\},\{b\}\}$ é uma base de $P(\{a,b\})$ (vide exemplo 1.35). De modo geral, se $A = \{a_1, a_2, ..., a_n\}$, considerando o $\mathbb{Z}_2-$espaço vetorial $V = P(A)$, pode-se verificar que, $B = \{\{a_1\},\{a_2\},...,\{a_n\}\}$ é uma base de V e portanto $dim_{\mathbb{Z}_2} P(\{a_1, a_2, ..., a_n\}) = n$.*

Teorema 1.45 ***(Complemento).*** *Seja V um espaço vetorial de dimensão $n \geq 1$. Supondo que $\{v_1, v_2, ..., v_r\} \subset V$ é um subconjunto $L.I.$ com r vetores e $r < n$, então existem $n - r$ vetores $v_{r+1}, ..., v_n \subset V$, de maneira que $B = \{v_1, ..., v_r, v_{r+1}, ..., v_n\}$ é uma base de V.*

Demonstração: Tomemos uma base $C = \{u_1, ..., u_n\}$ de V e formemos o conjunto $S = \{v_1, ..., v_r, u_1, ..., u_n\}$.

Dentre os subconjuntos de S que são $L.I.$ e que contém $v_1, ..., v_r$ tomemos um com o maior número possível de elementos. Seja

$$B = \{v_1, ..., v_r, u_1, ..., u_s\}$$

esse conjunto. (Aqui particularizamos em B a sequência dos índices dos elementos u_i's, o que não traz prejuízo à demonstração).

Mostremos que B é uma base de V. Decorre da própria escolha desse conjunto que ele é $L.I.$.

Por outro lado, $u_1, ..., u_s$ são obviamente combinações lineares de B. O mesmo se pode dizer

de $u_{s+1},...,u_n$ devido à propriedade (L_4) de (in)dependência linear. Sendo todos os vetores de C combinações de B, conclui-se, pelo fato de C ser uma base de V, que todos os vetores de V também são combinações lineares de B.

Portanto, B é uma base de V.

■

Nem todo espaço vetorial V sobre um corpo K é finitamente gerado e consequentemente possui uma base finita. Agora, vamos definir espaço vetorial de dimensão infinita. Para tanto precisamos estender o conceito de subconjuntos $L.D.$ e $L.I.$.

Definição 1.46 *Seja V um espaço vetorial sobre K. Um subconjunto S (não necessariamente finito) de V é **linearmente dependente** (ou simplesmente **dependente**) se existem vetores distintos $v_1, v_2, ..., v_n$ em S e escalares $a_1, a_2, ..., a_n$ em K, não todos nulos, tais que $a_1v_1 + a_2v_2 + ... + a_nv_n = 0$. Um conjunto que não é linearmente dependente é dito **linearmente independente**.*

Definição 1.47 *Seja V um espaço vetorial sobre K. Uma base de V é um conjunto linearmente independente de vetores de V que gera o espaço V. O espaço V é de dimensão infinita se ele possui uma base infinita, e neste caso escrevemos $dim_K V = \infty$.*

Exemplo 1.48 *Sejam $K = \mathbb{R}$ e $V = K^\infty = \{(x_1, x_2, ...) | x_i \in K\}$. Considerando sobre K^∞ as operações dadas por:*

$$(x_1, x_2, ...) + (y_1, y_2, ...) = (x_1 + y_1, x_2 + y_2, ...) \, e$$
$$k(x_1, x_2, ...) = (kx_1, kx_2, ...),$$

pode-se verificar que K^∞ é um espaço vetorial sobre K.

Seja $W = \{(x_1, x_2, ...) \in V | \exists n_0 \in \mathbb{N}^*; x_n = 0, \forall n > n_0\}$ (conjunto das sequências quase nulas). Pode-se mostrar que W é um subespaço de K^∞. Considere o subconjunto infinito $B = \{e_1 = (1, 0, 0, ...), e_2 = (0, 1, 0, ...), ...\}$ de W. Então,

• *B é $L.I.$, pois se $e_{i_1}, e_{i_2}, ..., e_{i_r} \in B$ e $a_1e_{i_1} + a_2e_{i_2} + ... + a_re_{i_r} = 0 = (0, 0, ..., 0)$ com $a_1, a_2, ..., a_r \in K$, então claramente $a_1 = a_2 = ... = a_r = 0$.*

• *B gera W visto que, se $w \in W$, então $\exists r \in \mathbb{N}$ tal que $w = (x_1, x_2, ...)$ com $x_n = 0, \forall n > r$. Daí, $w = x_1e_1 + x_2e_2 + ... + x_re_r$, ou seja, w é uma combinação linear de elementos de B.*

Assim, B é uma base infinita de W e portanto W é um espaço vetorial de dimensão infinita.

Exemplo 1.49 *Seja A um conjunto infinito. Considere o $\mathbb{Z}_2-$espaço vetorial de $P(A), F(A) = \{X \subset A | X$ é finito$\}$. Seja $B = \{\{x\} | x \in A\}$ o conjunto de todos os subconjuntos unitários de A. Então B é uma base infinita de $F(A)$, e portanto $F(A)$ é um espaço vetorial de dimensão infinita. Com efeito,*

• *B é L.I., pois dados $\{x_1\}, \{x_2\}, ..., \{x_n\} \in B$ e $a_1, a_2, ..., a_n \in \mathbb{Z}_2$, como $\{x_i\} + \{x_j\} = \{x_i, x_j\}$ (se $i \neq j$), então*

$$a_1\{x_1\} + a_2\{x_2\} + ... + a_n\{x_n\} = \emptyset \Longleftrightarrow a_1 = a_2 = ... = a_n = \overline{0}.$$

• *B gera $F(A)$, pois $\forall X \in F(A)$,*

$$X = \{y_1, y_2, ..., y_r\} = \overline{1}\{y_1\} + \overline{1}\{y_2\} + ... + \overline{1}\{y_r\}.$$

Em particular, $dim_{\mathbb{Z}_2} F(\mathbb{Z}) = \infty$ e $B = \{..., \{-1\}, \{0\}, \{1\}, \{2\}, ...\}$ é uma base de $F(\mathbb{Z})$. Note que B não é base de $P(\mathbb{Z})$ pois, $\mathbb{N} \in P(\mathbb{Z})$ mas $\mathbb{N}$ não é gerado pelos elementos de B (não existe $\{x_1\}, \{x_2\}, ..., \{x_n\}$ em B e $a_1, a_2, ..., a_n \in \mathbb{Z}_2$ tais que $a_1\{x_1\} + a_2\{x_2\} + ... + a_n\{x_n\} = \mathbb{N}$ pois $a_1\{x_1\} + a_2\{x_2\} + ... + a_n\{x_n\} \subset \{x_1, x_2, ..., x_n\} \neq \mathbb{N}$).

Observação 1.50 *Se um espaço vetorial V possui uma base B infinita, então V não possui base finita, pois se existisse $C = \{v_1, ..., v_n\}$ base finita de V, então V seria finitamente gerado e daí considerando um subconjunto qualquer com n vetores (da base infinita B): $B_1 = \{u_1, ..., u_n\} \subset B$, como B é L.I., B_1 também é L.I. e portanto, pelo lema 1.40, B_1 seria uma base de V. Daí, para todo $u \in B - B_1, B_1 \cup \{u\} \subset B$ é L.D. e consequentemente B seria L.D., o que é uma contradição.*

Proposição 1.51 *Todo subespaço vetorial de um espaço finitamente gerado é também finitamente gerado.*

Demonstração: Sejam V finitamente gerado e W um subespaço vetorial de V. Se $W = \{0\}$, nada há a provar. Senão, tomemos $w_1 \in W$. Se $W = \{b_1 w_1 | b_1 \in K\}$, está provado.

Senão, existe $w_2 \in W$, que não é da forma $b_1 w_1$, isto é, $\{w_1, w_2\}$ é $L.I.$. Se W é gerado por $\{w_1, w_2\}$, está terminado.

Senão, existe $w_3 \in W$, que não é combinação linear de $\{w_1, w_2\}$. E assim por diante. Este processo deve parar senão haveria em V um conjunto $L.I.$ e infinito.

■

Teorema 1.52 *Seja W um subespaço de um espaço vetorial V $n-$dimensional. Então $dim\ W \leq n$. Em particular, se $dim\ W = n$, então $W = V$.*

Demonstração: Como V é de dimensão n, quaisquer $n+1$ ou mais vetores são linearmente dependentes. Além disso, como uma base de W consiste em vetores linearmente independentes, não pode conter mais que n elementos. De acordo com isso, $dim\ W \leq n$. Em particular, se $\{w_1,...,w_n\}$ é base de W, então como é um conjunto linearmente independente com n elementos é também base de V.

Portanto, $W = V$ quando $dim\ W = n$.

■

Corolário 1.53 *Se W é um subespaço vetorial de V de dimensão infinita então V também é um espaço vetorial de dimensão infinita.*

Demonstração: Se a dimensão de V fosse finita então pelo teorema anterior a dimensão de W também seria finita, o que é uma contradição.

■

Teorema 1.54 *Sejam V um $K-$espaço vetorial e U e W dois subespaços vetoriais de V de dimensão finita. Então $U+W$ tem dimensão finita e*

$$dim(U+W) = dim\ U + dim\ W - dim(U \cap W).$$

Note que, se V é a soma direta de U e W, isto é, $V = U \oplus W$, então $dim(U+W) = dim\ U + dim\ W$.

Demonstração: Primeiramente, observe que $U \cap W$ é um subespaço de U e W.

Agora, suponhamos que $dim\ U = m$, $dim\ W = n$, $dim(U \cap W) = r$ e $B_1 = \{v_1, v_2, ..., v_r\}$ é base de $U \cap W$. Como B_1 é $L.I.$ em U e em W, o teorema do complemento nos garante a existência de $u_1, u_2, ..., u_s \in U$ e $w_1, w_2, ..., w_t \in W$ de tal modo que $B_2 = \{v_1, v_2, ..., v_r, u_1, u_2, ..., u_s\}$ é uma base de U e que $B_3 = \{v_1, v_2, ..., v_r, w_1, w_2, ..., w_t\}$ é uma base de W.

Mostremos que $B = \{v_1, v_2, ..., v_r, u_1, u_2, ..., u_s, w_1, w_2, ..., w_t\}$ é uma base de $U+W$.

(i) Seja $v \in U+W$. Então $v = u + w$ $(u \in U, w \in W)$.

Sendo B_2 e B_3 bases de U e W, respectivamente, podemos representar:

$$u = a_1v_1 + ... + a_rv_r + b_1u_1 + ... + b_sv_s \text{ e}$$
$$w = a'_1v_1 + ... + a'_rv_r + b'_1w_1 + ... + b'_tw_t$$

onde a_i's, a'_i's, b_i's, b'_i's $\in K$.

Daí,

$$v = u + w = (a_1 + a'_1)v_1 + ... + (a_r + a'_r)v_r + b_1u_1 + ... + b_su_s + b'_1w_1 + ... + b'_tw_t.$$

Logo, $[B] = U + W$.

(ii) Suponhamos

$$a_1v_1 + ... + a_rv_r + b_1u_1 + ... + b_su_s + c_1w_1 + ... + c_tw_t = 0. \tag{1.5}$$

Assim, $a_1v_1 + ... + a_rv_r + b_1u_1 + ... + b_su_s = -c_1w_1 - ... - c_tw_t$.

Como o primeiro membro desta última igualdade está em U e o segundo está em W e se trata do mesmo vetor, então $-c_1w_1 - ... - c_tw_t \in U \cap W$. Logo, existem $d_1, ..., d_r \in K$ tais que

$$-c_1w_1 - ... - c_tw_t = d_1v_1 + ... + d_rv_r$$

ou seja,

$$d_1v_1 + ... + d_rv_r + c_1w_1 + ... + c_tw_t = 0.$$

Do fato de B_3 ser $L.I.$, conclui-se então que $d_1 = ... = d_r = c_1 = ... = c_t = 0$. Mas se $c_1 = ... = c_t = 0$, a igualdade 1.5 fica:

$$a_1v_1 + ... + a_rv_r + b_1u_1 + ... + b_su_s = 0.$$

Lembrando que o conjunto B_2 também é $L.I.$ e teremos que

$$a_1 = ... = a_r = b_1 = ... = b_s = 0.$$

Com isso, provamos que B é um conjunto $L.I.$.

Finalmente, observando que $dim(U \cap W) = r, dim\ U = r+s, dim\ W = r+t$ e $dim(U+W) = r+s+t$, obtemos que

$$dim(U+W) = dim\ U + dim\ W - dim(U \cap W).$$

■

Teorema 1.55 *Sejam V um espaço vetorial tal que $dim\ V = n > 1$ e $U \subset V$ um subespaço. Então existe $W \subset V$ subespaço tal que $V = U \oplus W$.*

Demonstração: Como $U \subset V$ é um subespaço, então U possui uma base. Seja $B_1 = \{u_1, u_2, ..., u_r\}$ uma base de U com $r < n$.

Pelo teorema do complemento, existe um conjunto $B_2 = \{u_{r+1}, u_{r+2}, ..., u_n\}$ tal que $B = B_1 \cup B_2 = \{u_1, u_2, ..., u_r, u_{r+1}, u_{r+2}, ..., u_n\}$ é base de V.

Assim, tomando $W = [B_2]$, temos claramente $U + W \subset V$.

Por outro lado, se $v \in V$ então

$$v = a_1u_1 + a_2u_2 + ... + a_ru_r + a_{r+1}u_{r+1} + a_{r+2}u_{r+2} + ... + a_nu_n.$$

Como $a_1u_1 + a_2u_2 + ... + a_ru_r \in U$ e $a_{r+1}u_{r+1} + a_{r+2}u_{r+2} + ... + a_nu_n \in W$, temos que $v \in U + W$ e assim $V \subset U + W$. Logo, $V = U + W$.

Mostremos agora que $U \cap W = \{0\}$. Seja $x \in U \cap W$. Então $x \in U$ e $x \in W$. Logo,

$x = a_1u_1 + a_2u_2 + ... + a_ru_r$ e $x = a_{r+1}u_{r+1} + a_{r+2}u_{r+2} + ... + a_nu_n$, com a_i's $\in K$.

Daí,

$$0 = x - x = a_1u_1 + a_2u_2 + ... + a_ru_r - a_{r+1}u_{r+1} - a_{r+2}u_{r+2} - ... - a_nu_n.$$

Como $\{u_1, u_2, ..., u_r, u_{r+1}, u_{r+2}, ..., u_n\}$ é $L.I.$, segue que a_i's $= 0$.

Logo, $x = 0$ e $U \cap W = \{0\}$.

Portanto, $V = U \oplus W$.

■

1.4 Transformações Lineares

Definição 1.56 *Sejam U e V espaços vetoriais sobre o mesmo corpo K. Uma aplicação $F : U \to V$ é uma transformação linear (ou aplicação linear, ou homomorfismo de espaços vetoriais) se*

(i) $F(u+w) = F(u) + F(w)$, para todo $u, w \in U$;

(ii) $F(ku) = kF(u)$, para todo $u \in U$ e todo $k \in K$.

Observação 1.57 *Em (ii) da definição acima, substituindo $k = 0$ obtemos $F(0) = 0$, isto é, toda transformação linear leva vetor nulo em vetor nulo.*

Observação 1.58 *Para quaisquer escalares $a, b \in K$ e quaisquer vetores $u, w \in U$, aplicando as duas condições de linearidade, obtemos*

$$F(au + bw) = F(au) + F(bw) = aF(u) + bF(w).$$

Mais geralmente, para quaisquer escalares $a_i \in K$ e quaisquer vetores $v_i \in U$, obtemos a propriedade básica de transformações lineares

$$F(a_1u_1 + a_2u_2 + ... + a_nu_n) = a_1F(u_1) + a_2F(u_2) + ... + a_nF(u_n).$$

A condição $F(au + bw) = F(au) + F(bw) = aF(u) + bF(w)$ é usada algumas vezes como definição, pois ela as caracteriza completamente.

Definição 1.59 *Sejam U e V dois espaços vetoriais sobre K. Uma aplicação $F : U \to V$ é denominada um **isomorfismo** do espaço vetorial U no espaço vetorial V se F é uma transformação linear bijetora. Os espaços vetoriais U e V são ditos isomorfos se existe um isomorfismo de U sobre V.*

Definição 1.60 *Sejam U e V dois espaços vetoriais sobre um corpo K e $F : U \to V$ uma transformação linear.*

*(i) O conjunto $\{v \in V | F(u) = v$, para algum $u \in U\}$ é chamado **imagem de** F e será denotado por ImF;*

*(ii) O conjunto $\{u \in U | F(u) = 0\}$ é chamado **núcleo** ou **kernel de** F e será denotado por $KerF$.*

Teorema 1.61 *Seja $F : U \to V$ uma transformação linear. Então, o núcleo e a imagem de F são subespaços de U e V, respectivamente.*

Demonstração: (i) Como $F(0) = 0$ segue que $0 \in KerF$. Agora, sejam $u, w \in KerF$. Então $F(u) = 0$ e $F(w) = 0$.

Assim, para quaisquer $a, b \in K$,

$$F(au + bw) = aF(u) + bF(w) = a0 + b0 = 0.$$

Logo, $au + bw \in KerF$ e portanto o núcleo de F é um subespaço de U.

(ii) Como $F(0) = 0$ segue que $0 \in ImF$. Sejam $a, b \in K$ e suponhamos $v, v' \in ImF$. Então existem u e u' em U tais que $F(u) = v$ e $F(u') = v'$. Daí,

$$F(au + bu') = aF(u) + bF(u') = av + bv' \in ImF.$$

Assim, a imagem de F é um subespaço de V.

■

Proposição 1.62 *Seja $F : U \to V$ uma transformação linear.*

(i) *F é injetora se, e somente se, $KerF = \{0\}$.*

(ii) *F é sobrejetora se, e somente se, $ImF = V$.*

Demonstração: (i) $(\Longrightarrow)$ Temos sempre que $\{0\} \subset KerF$ pois $F(0) = 0$. Agora falta mostrar que $KerF \subset \{0\}$.

Para isto, seja $u \in KerF$. Assim,

$$F(u) = 0 = F(0),$$

e como F é injetora segue que $u = 0$. Logo, $KerF \subset \{0\}$.

Portanto, $KerF = \{0\}$.

$(\Longleftarrow)$ Suponhamos agora que $KerF = \{0\}$ e sejam $u, w \in U$ tais que $F(u) = F(w)$. Então,

$$0 = F(u) - F(w) = F(u) + F(-w) = F(u - w).$$

Logo, $u - w \in KerF = \{0\}$ e daí $u = w$.

Portanto, F é injetora.

(ii) É óbvia.

■

Teorema 1.63 *Sejam U um espaço vetorial de dimensão finita e $F : U \to V$ uma transformação linear. Então,*

$$dimU = dim(KerF) + dim(ImF).$$

Demonstração: Sejam $V' = ImF$ e $W = KerF$ e suponha que $dim\ U = n$. Como W é um subespaço de U então sua dimensão é finita, digamos $dim\ W = r \leq n$.

Seja $B_1 = \{w_1, w_2, ..., w_r\}$ uma base de W. Pelo teorema do complemento, existem $u_1, u_2, ..., u_{n-r} \in U$ de maneira que $B = \{w_1, ..., w_r, u_1, u_2, ..., u_{n-r}\}$ é base de U.

Agora, seja $B_2 = \{F(u_1), F(u_2), ..., F(u_{n-r})\}$. Mostremos que B_2 é base de V'.

Para qualquer $v \in V'$ existe $u \in U$ tal que $F(u) = v$. Como $B = \{w_1, w_2, ..., w_r, u_1, u_2, ..., u_{n-r}\}$ gera U, então existem $a_1, ..., a_r, b_1, ..., b_{n-r} \in K$ de modo que $u = a_1w_1 + a_2w_2 + ... + a_rw_r + b_1u_1 + b_2u_2 + ... + b_{n-r}u_{n-r}$. Assim,

$$v = F(u) = F(a_1w_1 + a_2w_2 + ... + a_rw_r + b_1u_1 + b_2u_2 + ... + b_{n-r}u_{n-r}) =$$
$$a_1F(w_1) + a_2F(w_2) + ... + a_rF(w_r) + b_1F(u_1) + b_2F(u_2) + ... + b_{n-r}F(u_{n-r}).$$

Mas $F(w_i) = 0, \forall i = 1, ..., r$ pois w_i's $\in KerF$. Então,

$$v = F(u) = b_1F(u_1) + b_2F(u_2) + ... + b_{n-r}F(u_{n-r})$$

e portanto B_2 gera V'.

Suponhamos que $a_1F(u_1) + a_2F(u_2) + ... + a_{n-r}F(u_{n-r}) = 0$, a_i's $\in K$. Então, $F(a_1u_1 + a_2u_2 + ... + a_{n-r}u_{n-r}) = 0$ e assim $a_1u_1 + a_2u_2 + ... + a_{n-r}u_{n-r} \in W$.

Como B_1 gera W temos que existem $b_1, b_2, ..., b_r \in K$ tais que

$$a_1u_1 + a_2u_2 + ... + a_{n-r}u_{n-r} = b_1w_1 + b_2w_2 + ... + b_rw_r \text{ ou}$$

$$a_1u_1 + a_2u_2 + ... + a_{n-r}u_{n-r} - b_1w_1 - b_2w_2 - ... - b_rw_r = 0.$$

Mas $B = \{w_1, w_2, ..., w_r, u_1, u_2, ..., u_{n-r}\}$ é base de U e portanto $a_1, a_2, ..., a_r, b_1, b_2, ..., b_{n-r}$ são todos nulos. Em particular, $a_1 = ... = a_r = 0$.

Logo, B_2 é linearmente independente.

Assim, B_2 é base de V' e $dim\ V' = n - r$.

Portanto, $dim\ U = n = r + n - r = dim(KerF) + dim(ImF)$.

■

Corolário 1.64 *Sejam U e V espaços vetoriais sobre um corpo K com a mesma dimensão finita n e suponhamos $F : U \to V$ uma transformação linear. Então são equivalentes as seguintes afirmações:*

(i) *F é sobrejetora.*

(ii) *F é bijetora.*

(iii) *F é injetora.*

(iv) *F transforma base de U em base de V, isto é, se B é uma base de U então $F(B)$ é base de V.*

Demonstração: $(i) \Longrightarrow (ii)$ Como F é sobrejetora, segue pela proposição 1.62(ii) que $ImF = V$ e assim $dim(ImF) = dimV = n = dimU$. Daí, pelo teorema anterior, $dim(KerF) = 0$. O que implica que $KerF = \{0\}$ e então pela proposição 1.62(i), F é injetora.

Portanto, F é bijetora.

$(ii) \Longrightarrow (iii)$ É óbvia.

$(iii) \Longrightarrow (iv)$ Seja $B = \{u_1, ..., u_n\}$ uma base de U. Mostremos que $F(B) = \{F(u_1), ..., F(u_n)\}$ é uma base de V. Observe que $F(B)$ tem tantos vetores quanto B pelo fato de F ser injetora. Então, pelo lema 1.40, é necessário provarmos apenas que $F(B)$ é linearmente independente.

Suponhamos $a_1, ..., a_n \in K$ e $a_1F(u_1) + ... + a_nF(u_n) = 0$.

Pela linearidade de F, temos que $F(a_1u_1 + ... + a_nu_n) = 0$. Sendo F injetora, segue que $a_1u_1 + ... + a_nu_n = 0$. Como B é $L.I.$ conclui-se que $a_1 = ... = a_n = 0$.

Assim, $F(B)$ é $L.I.$ e portanto é base de V.

$(iv) \Longrightarrow (i)$ Seja $v \in V$. Tomando uma base $B = \{u_1, ..., u_n\}$ de U, então nossa hipótese nos garante que $F(B) = \{F(u_1), ..., F(u_n)\}$ é uma base de V.

Logo, v é combinação linear dos elementos de $F(B)$, ou seja,

$$v = a_1F(u_1) + ... + a_nF(u_n) = F(a_1u_1 + ... + a_nu_n), \text{ com } a_i\text{'s} \in K.$$

Como $a_1u_1 + ... + a_nu_n \in U$, segue que todo elemento de V é imagem por F de um elemento de U, isto é, F é sobrejetora.

■

Lema 1.65 *Sejam U e V espaços vetoriais sobre K, ambos de dimensão n. Se $B = \{u_1,...,u_n\}$ e $C = \{v_1,...,v_n\}$ são bases de U e V, respectivamente, então $F : U \to V$ definida por $F\left(\sum_{i=1}^{n} \alpha_i u_i\right) = \sum_{i=1}^{n} \alpha_i v_i$, $\forall \alpha_i \in K$, é um isomorfismo de U em V.*

Teorema 1.66 *Dois espaços vetoriais U e V de dimensão finita são isomorfos se, e somente se, $dimU = dimV$.*

Demonstração: ($\Longrightarrow$) Sejam $B = \{u_1,...,u_n\}$ uma base de U e $F : U \to V$ um isomorfismo. Como F é bijetora segue, pelo corolário 1.64, que $F(B) = \{F(u_1),...,F(u_n)\}$ é uma base de V, ou seja, $F(B)$ tem tantos elementos como B. Logo, $dimU = dimV$.

($\Longleftarrow$) Segue do lema anterior.

■

1.5 Espaços Quocientes

Sejam V um espaço vetorial sobre K e W um subespaço de V. Vamos construir um espaço vetorial chamado de espaço quociente de V por W e que será denotado por V/W.

Primeiro, vamos definir uma relação de equivalência $\sim$ nos elementos do espaço V.

Dados $v_1, v_2 \in V$, dizemos que $v_1 \sim v_2$ se $v_1 - v_2 \in W$.

Tal relação é uma relação de equivalência em V.

Para um vetor $v \in V$, indicamos por $\overline{v}$ a sua classe de equivalência, isto é,

$$\overline{v} = \{u \in V \mid u \sim v\}.$$

Se escrevemos $v+W$ para representar o conjunto de somas $v+w$, com $w \in W$, isto é,

$$v+W = \{v+w | w \in W\},$$

obtemos

$$\begin{aligned}\overline{v} &= \{u \in V | u \sim v\} \\ &= \{u \in V | u - v = w \in W\} \\ &= \{v+w | w \in W\} \\ &= v+W.\end{aligned}$$

Esses conjuntos são chamados classes laterais de W em V.

Exemplo 1.67 *Tome o $\mathbb{Z}_2$−espaço vetorial, $V = P(\mathbb{Z}_5^*)$ (exemplo 1.3) e seja $W = \{\emptyset, \{\overline{1}\}, \{\overline{4}\}, \{\overline{1},\overline{4}\}\}$. É fácil verificar que W é um subespaço de $P(\mathbb{Z}_5^*)$ e temos*

$$\{\overline{1}\}+W = \{\{\overline{1}\}+\emptyset, \{\overline{1}\}+\{\overline{1}\}, \{\overline{1}\}+\{\overline{4}\}, \{\overline{1}\}+\{\overline{1},\overline{4}\}\} = \{\{\overline{1}\}, \emptyset, \{\overline{1},\overline{4}\}, \{\overline{4}\}\} = W = \emptyset + W = \{\overline{1},\overline{4}\}+W = \{\overline{4}\}+W.$$

$$\{\overline{2}\}+W = \{\{\overline{2}\}, \{\overline{1},\overline{2}\}, \{\overline{2},\overline{4}\}, \{\overline{1},\overline{2},\overline{4}\}\} = \{\overline{1},\overline{2}\}+W = \{\overline{2},\overline{4}\}+W = \{\overline{1},\overline{2},\overline{4}\}+W.$$

$$\{\overline{3}\}+W = \{\{\overline{3}\}, \{\overline{1},\overline{3}\}, \{\overline{3},\overline{4}\}, \{\overline{1},\overline{3},\overline{4}\}\} = \{\overline{1},\overline{3}\}+W = \{\overline{3},\overline{4}\}+W = \{\overline{1},\overline{3},\overline{4}\}+W.$$

$$\{\overline{2},\overline{3}\}+W = \{\{\overline{2},\overline{3}\}, \{\overline{1},\overline{2},\overline{3}\}, \{\overline{2},\overline{3},\overline{4}\}, \{\overline{1},\overline{2},\overline{3},\overline{4}\}\} = \{\overline{1},\overline{2},\overline{3}\}+W = \{\overline{2},\overline{3},\overline{4}\}+W = \mathbb{Z}_5^*+W.$$

Proposição 1.68 *As classes laterais de W em V particionam V em conjuntos mutuamente distintos. Isto é,*

(i) duas classes laterais quaisquer $u+W$ e $v+W$ ou são idênticas ou são disjuntas.

(ii) cada $v \in V$ pertence a uma classe. De fato, $v \in v+W$.

Teorema 1.69 *Seja W um subespaço de um espaço vetorial sobre um corpo K. Então $V/W := \{v+W | v \in V\}$ (conjunto de todas as classes laterais de W em V) é um espaço vetorial sobre K com as seguintes operações de adição e multiplicação por escalar:*

(i) $(u+W)+(v+W) = (u+v)+W$;

(ii) $k(v+W) = kv+W$, com $k \in K$.

Definição 1.70 *O espaço vetorial V/W é chamado **espaço quociente** de V por W.*

Observação 1.71 *Sejam V um espaço vetorial e W um subespaço de V.*

(i) Se $W = V$ então $V/W = V/V = \{0+V\} = \{V\}$, pois $v+V = 0+V, \forall v \in V$;

(ii) Se $W = \{0\}$ então $V/\{0\} = \{v+0 | v \in V\}$ que é isomorfo a V (pois a aplicação $v+\{0\} \longmapsto v$ é um isomorfismo de $V/\{0\}$ em V).

A dimensão de V/W está relacionada com a dimensão de V e de W, conforme mostra o teorema abaixo.

Teorema 1.72 *Seja W um subespaço vetorial de V. Suponhamos que $\{w_1, w_2, ..., w_r\}$ é uma base de W e que o conjunto de classes laterais $\{\overline{v_1}, \overline{v_2}, ..., \overline{v_s}\}$, onde $\overline{v_j} = v_j + W$ é uma base de V/W. Então $B = \{v_1, v_2, ..., v_s, w_1, w_2, ..., w_r\}$ é uma base de V e assim, $dim\ V = dim\ W + dim\ V/W$.*

Demonstração: Considere $u \in V$. Como $\{\overline{v_1}, \overline{v_2}, ..., \overline{v_s}\}$ é uma base de V/W e $\overline{u} = u + W \in V/W$, então existem $a_1, a_2, ..., a_s \in K$ tais que

$$\overline{u} = u + W = a_1\overline{v_1} + a_2\overline{v_2} + ... + a_s\overline{v_s} = a_1(v_1+W) + a_2(v_2+W) + a_s(v_s+W) = (a_1v_1+W) + (a_2v_2+W) + ... + (a_sv_s+W) = (a_1v_1 + a_2v_2 + ... + a_sv_s) + W.$$

Assim, $u - a_1v_1 - a_2v_2 - ... - a_sv_s \in W$. Daí, existe $w \in W$ tal que $u - a_1v_1 - a_2v_2 - ... - a_sv_s = w$. Logo, $u = a_1v_1 + a_2v_2 + ... + a_sv_s + w$. Como $\{w_1, w_2, ..., w_r\}$ é uma base de W,

$$u = a_1v_1 + a_2v_2 + ... + a_sv_s + b_1w_1 + b_2w_2 + ... + b_rw_r,$$

com $b_1, b_2, ..., b_r \in K$.

Consequentemente, B gera V.

Mostremos agora que B é linearmente independente. Sejam $c_1, c_2, ..., c_s, d_1, d_2, ..., d_r \in K$ e suponhamos

$$c_1v_1 + c_2v_2 + ... + c_sv_s + d_1w_1 + d_2w_2 + d_rw_r = 0. \tag{1.6}$$

Então, $c_1v_1 + c_2v_2 + ... + c_sv_s = -d_1w_1 - d_2w_2 - d_rw_r \in W$ pois $\{w_1, w_2, ..., w_r\}$ é base de W e portanto $c_1v_1 + c_2v_2 + ... + c_sv_s \in W$ também. Assim,

$$(c_1v_1 + c_2v_2 + ... + c_sv_s) + W = 0 + W \Longleftrightarrow c_1(v_1+W) + c_2(v_2+W) + ... + c_s(v_s+W) = 0 + W \Longleftrightarrow c_1\overline{v_1} + c_2\overline{v_2} + ... + c_s\overline{v_s} = \overline{0}.$$

Como $\{\overline{v_1}, \overline{v_2}, ..., \overline{v_s}\}$ é $L.I.$ segue que os c_i's são todos nulos. Substituindo na equação 1.6 obtemos que $d_1w_1 + d_2w_2 + ... + d_rw_r = 0$. Mas $\{w_1, w_2, ..., w_r\}$ é base de W, logo os d_i's $= 0$. Daí,

B é linearmente independente.

Portanto, B é base de V e $dim\ V = dim\ W + dim\ V/W$.

■

Observação 1.73 *Poderíamos demonstrar o teorema anterior usando o teorema 1.63 por considerar $F : V \to V/W$ tal que $F(v) = v + W$ e observar que F é uma transformação linear sobrejetora com $KerF = W$.*

Exemplo 1.74 *Considere $V = P(\mathbb{Z}_5^*)$ e W o subespaço de V dado no exemplo 1.67. Temos que $dim_{\mathbb{Z}_2} P(\mathbb{Z}_5^*) = 4$ (pois $\mathbb{Z}_5^*$ tem 4 elementos) e $dim_{\mathbb{Z}_2} W = 2$. Logo, $dim_{\mathbb{Z}_2} P(\mathbb{Z}_5^*)/W = 4 - 2 = 2$. Note que, $P(\mathbb{Z}_5^*)/W = \{W, \{\overline{2}\} + W, \{\overline{3}\} + W, \{\overline{2}, \overline{3}\} + W\}$ e $\{\{\overline{2}\} + W, \{\overline{3}\} + W\}$ é uma base de $P(\mathbb{Z}_5^*)/W$.*

Observação 1.75 *Considerando em $P(\mathbb{Z}_5^*)$ os subespaços $Q(\mathbb{Z}_5^*)$ e $F(\mathbb{Z}_5^*)$, como $P(\mathbb{Z}_5^*)$ é finito então $P(\mathbb{Z}_5^*) = Q(\mathbb{Z}_5^*) = F(\mathbb{Z}_5^*)$ e assim, $dim_{\mathbb{Z}_2} P(\mathbb{Z}_5^*)/Q(\mathbb{Z}_5^*) = 0 = dim_{\mathbb{Z}_2} Q(\mathbb{Z}_5^*)/F(\mathbb{Z}_5^*)$.*

Exemplo 1.76 *Consideremos $V = \mathbb{R}^3$ e $W = \{(x, y, z) \in \mathbb{R}^3 \mid y - z = x - z = 0\}$. Mostremos que $B = \{(1,0,0) + W, (0,1,0) + W\}$ é uma base de $\mathbb{R}^3/W$. De fato, temos que se $w = (x, y, z) \in W$ então $y = z$ e $x = z$. Assim, $x = y = z$ e $w = x(1,1,1)$. Logo, $W = [(1,1,1)], C = \{(1,1,1)\}$ é base de W e $dim\ W = 1$.*

Deste modo, pelo teorema anterior, $dim\ \mathbb{R}^3/W = 3 - 1 = 2$. Logo qualquer subconjunto $L.I.$ do espaço $\mathbb{R}^3/W$ formado por apenas dois vetores será uma base de $\mathbb{R}^3/W$. Seja $B = \{(1,0,0) + W, (0,1,0) + W\}$.

Para quaisquer $a, b \in K$,

$a[(1,0,0)+W]+b[(0,1,0)+W] = (0,0,0)+W \iff [a(1,0,0)+b(0,1,0)]+W = (0,0,0)+W \iff a(1,0,0)+b(0,1,0)-(0,0,0) \in W \iff a(1,0,0)+b(0,1,0) = c(1,1,1) \iff a(1,0,0)+b(0,1,0)-c(1,1,1) = (0,0,0) \iff a = b = c = 0$.

Daí, B é $L.I.$ e portanto é base do $\mathbb{R}^3/W$.

CAPÍTULO 2

Módulos

Neste capítulo apresentamos uma introdução à Teoria de Módulos, assunto muito importante em Álgebra Homológica. Além do conceito de módulo sobre um anel, estudamos o conceito de submódulos, homomorfismos entre módulos e alguns dos principais resultados envolvendo homomorfismos de módulos.

2.1 Definição e Exemplos

Definição 2.1 *Seja A um anel com unidade. Diz-se que um conjunto não vazio M é um módulo à esquerda sobre A (ou um $A-$módulo à esquerda) se M é um grupo abeliano em relação a uma operação, que indicaremos por $+$, e está definida uma lei de composição externa que a cada par $(\alpha, m) \in A \times M$ associa um elemento $\alpha m \in M$ e tal que, para todos $\alpha_1, \alpha_2 \in A$ e todos $m_1, m_2 \in M$, verifica:*

(i) $\alpha_1(\alpha_2 m_1) = (\alpha_1 \alpha_2) m_1$;

(ii) $\alpha_1(m_1 + m_2) = \alpha_1 m_1 + \alpha_1 m_2$;

(iii) $(\alpha_1 + \alpha_2) m_1 = \alpha_1 m_1 + \alpha_2 m_1$;

(iv) $1 \cdot m_1 = m_1$.

Observação 2.2 (i) *De forma análoga pode-se definir a noção de $A-$módulo à direita, considerando multiplicação à direita por elementos do anel.*

(ii) *Às vezes, a noção de módulo se define para anéis sem unidade. Neste caso se omite a con-*

dição (iv) da definição acima. No que segue estudaremos sempre módulos à esquerda sobre anéis com unidade; não havendo perigo de confusão, usaremos simplesmente, a expressão $A-$módulo. Da mesma forma, falaremos apenas de anéis, subentendendo que todos os anéis considerados são anéis com unidade.

Exemplo 2.3 *Todo espaço vetorial sobre um corpo K é um $K-$módulo.*

Exemplo 2.4 *Todo grupo abeliano G pode ser considerado como um módulo sobre o anel $\mathbb{Z}$ dos números inteiros definindo o produto de um inteiro n por um elemento $g \in G$ por:*

$ng = g + ... + g$ *(n vezes) se* $n > 0$*;*

$ng = (-g) + ... + (-g)$ *($|n|$ vezes) se* $n < 0$*;*

$0 \cdot g = 0$.

Exemplo 2.5 *Seja I um ideal à esquerda de um anel A. Então, I admite uma estrutura de $A-$módulo com a soma induzida pela soma de A e a multiplicação por escalares definida pela multiplicação de A.*

Exemplo 2.6 *Todo anel pode ser considerado como um módulo sobre si mesmo. Isto é um caso particular do exemplo anterior, onde tomamos $I = A$. Às vezes interessará distinguir entre o anel A e o mesmo conjunto considerado como $A-$módulo.*

Exemplo 2.7 *Seja G um grupo abeliano. Indicaremos por $End(G)$ o conjunto de todos os endomorfismos de G. Neste conjunto pode-se introduzir uma estrutura de anel definindo soma e produto de dois endomorfismos $f, g \in End(G)$ por:*

$$(f+g)(x) = f(x) + g(x), \forall x \in G$$
$$(f \cdot g)(x) = f(g(x)), \forall x \in G.$$

Pode-se definir em G uma estrutura de $End(G)-$módulo associando a cada par $(f,x) \in End(G) \times G$ o elemento $f \cdot x = f(x) \in G$.

Exemplo 2.8 *Sejam A um anel e X um conjunto qualquer. Indicaremos por A^X o conjunto de todas as funções de domínio X a valores em A.*

A^X admite uma estrutura de $A-$módulo, definindo a soma de funções puntualmente, como no exemplo anterior, e a multiplicação à esquerda por elementos de A associando a cada par $(a,f) \in A \times A^X$ a função $a \cdot f \in A^X$ definida por:

$$(af)(x) = a \cdot f(x), \ \forall x \in X.$$

Exemplo 2.9 *Sejam V um espaço vetorial sobre um corpo K e $T : V \to V$ uma transformação linear.*

Dado um polinômio $f \in K[X]$ da forma $f = a_0 + a_1X + ... + a_nX^n$ indicaremos por $f(T)$ a transformação linear $f(T) = a_0I + a_1T + ... + a_nT^n$ (onde I indica a função identidade de V em V e $T^h = T \circ T^{h-1}$ com $T^1 = T$).

Pode-se introduzir em V uma estrutura de $K[X]-$módulo, conservando a soma de V e associando a cada par $(f,v) \in K[X] \times V$ o elemento $f(T)(v) \in V$ ($f(T)(v)$ indica a função $f(T)$ aplicada no vetor v).

Exemplo 2.10 *Sejam I um ideal bilateral de um anel A e M um $A-$módulo. Indicaremos por $I \cdot M$ o subconjunto de M:*

$$I \cdot M = \{\alpha \cdot m | \ \alpha \in I, m \in M\}.$$

Se $I \cdot M = \{0\}$ pode-se introduzir uma estrutura de $A/I-$módulo em M associando a cada par $(a+I, m) \in A/I \times M$ o elemento $am \in M$.

Notamos que a definição acima não depende do representante. De fato, se $a + I = b + I$ então $a - b \in I$, logo $(a-b) \cdot m = 0$ para todo $m \in M$ e, consequentemente $(a+I)m = (b+I)m$, $\forall m \in M$.

Reciprocamente, se a multiplicação acima é bem definida, então $I \cdot M = \{0\}$.

2.2 Submódulos

Definição 2.11 *Seja M um $A-$módulo. Um subconjunto $N \subset M$ diz-se um $A-$submódulo de M, ou simplesmente, um submódulo se:*

(i) N é um subgrupo aditivo de M;

(ii) N é fechado em relação à multiplicação por escalares, isto é, para todo $a \in A$ e todo $n \in N$, tem-se que, $a \cdot n \in N$.

Exemplo 2.12 *Seja V um espaço vetorial sobre um corpo K. Um subconjunto $S \subset V$ é um submódulo se, e somente se, S é um subespaço de V.*

Exemplo 2.13 *Seja G um grupo abeliano. Pode-se verificar que os $\mathbb{Z}-$submódulos de G são precisamente os seus subgrupos.*

Exemplo 2.14 *Seja A um anel. Os $A-$submódulos do $A-$módulo A são os seus ideais à esquerda. Basta apenas comparar as definições correspondentes lembrando como foi definida a estrutura de módulo em A.*

Exemplo 2.15 *Se N_1 e N_2 são submódulos de um $A-$módulo M, o conjunto $N_1+N_2=\{n_1+n_2|n_1\in N_1, n_2\in N_2\}$ também é um submódulo de M chamado submódulo soma de N_1 e N_2.*

Exemplo 2.16 *Seja M um $A-$módulo e $\{N_i\}_{i\in I}$ uma família de submódulos de M. Então $\bigcap_{i\in I} N_i$ é um submódulo de M.*

Exemplo 2.17 *Seja S um subconjunto de um $A-$módulo M. O conjunto*

$$[S]=\left\{\sum_{i=1}^{n} a_i s_i | n\in\mathbb{N}, a_i\in A, s_i\in S\right\}$$

é um submódulo de M chamado submódulo gerado por S.

Se $S=\{m\}$, com $m\in M$, o submódulo $[S]=[m]$ diz-se o módulo cíclico gerado por m.

Exemplo 2.18 *Se I é um ideal à esquerda de um anel A e m um elemento de um $A-$módulo M, então o conjunto $I\cdot m=\{\alpha\cdot m|\alpha\in I\}$ é um submódulo de M.*

Sejam agora M um $A-$módulo e N um submódulo de M. Considerando apenas a estrutura de grupo aditivo abeliano de M podemos construir o grupo quociente $M/N=\{m+N|m\in M\}$ cuja lei de composição interna é definida por:

$$(m_1+N)+(m_2+N)=(m_1+m_2)+N.$$

Pode-se definir uma multiplicação por escalares de A, associando ao par $(a,m+N)\in A\times M/N$ o elemento $am+N\in M/N$.

A definição independe do representante e, nestas condições, obtém-se uma estrutura de $A-$módulo em M/N.

Definição 2.19 *O $A-$módulo M/N construído acima chama-se o módulo quociente do módulo M pelo submódulo N.*

Em particular, se I é um ideal à esquerda de um anel A, então o quociente A/I é um $A-$módulo.

2.3 Homomorfismo de Módulos

Definição 2.20 *Sejam M e N dois $A-$módulos. Uma função $f : M \to N$ diz-se um homomorfismo de $A-$módulos ou um $A-$homomorfismo se para todos $m_1, m_2 \in M$ e todo $a \in A$ se verifica:*

(i) $f(m_1 + m_2) = f(m_1) + f(m_2)$;

(ii) $f(a \cdot m_1) = a \cdot f(m_1)$.

Dado um $A-$homomorfismo $f : M \to N$ chama-se imagem de f e núcleo ou kernel de f respectivamente aos conjuntos:

$$Im(f) = \{n \in N | \exists m \in M \text{ e } f(m) = n\} \text{ e,}$$
$$Ker(f) = \{m \in M | f(m) = 0\}.$$

É fácil ver que $Im(f)$ e $Ker(f)$ são submódulos de N e M, respectivamente.

Um $A-$homomorfismo diz-se um $A-$monomorfismo ou um $A-$epimorfismo se for injetor ou sobrejetor, respectivamente.

Claramente, um $A-$homomorfismo $f : M \to N$ é um $A-$epimorfismo, se, e somente se, $Im(f) = N$. Da mesma forma, é fácil ver que f é um $A-$monomorfismo se, e somente se, $Ker(f) = \{0\}$.

Exemplo 2.21 *Se A é um corpo, os $A-$homomorfismos são as transformações lineares entre espaços vetoriais sobre A.*

Exemplo 2.22 *Os homomorfismos de grupos abelianos são precisamente os $\mathbb{Z}-$homomorfismos.*

Exemplo 2.23 *A função trivial $f : M \to N$ definida por $f(m) = 0$, $\forall m \in M$ é um $A-$homomorfismo, chamado homomorfismo nulo.*

Exemplo 2.24 *Seja N um submódulo de um $A-$módulo M. Então a função inclusão*

$$i : N \hookrightarrow M,$$
$$x \mapsto x$$

é um $A-$homomorfismo. Em particular, a função identidade de M, $id_M : M \to M$ também é um $A-$homomorfismo.

Exemplo 2.25 *Seja novamente N um submódulo de um $A-$módulo M.*

Define-se o homomorfismo canônico ou projeção canônica ao quociente $j : M \to M/N$ por:

$$j(m) = m + N, \ \forall m \in M.$$

Exemplo 2.26 *Seja M um $A-$módulo. Para cada elemento $a \in A$ pode-se definir uma função $f_a : M \to M$ por $f_a(m) = am$, $\forall m \in M$. Uma tal função chama-se uma homotetia.*

É fácil verificar que as homotetias são homomorfismos da estrutura de grupo de M e, que se $a \in Centro(A) = \{a \in A | ax = xa, \forall x \in A\}$, então f_a é um $A-$homomorfismo. Em particular, se A é comutativo toda homotetia é um $A-$homomorfismo.

Proposição 2.27 (i) *Sejam $f : M \to M'$ e $g : M' \to M''$ $A-$homomorfismos. Então $g \circ f : M \to M''$ também é um $A-$homomorfismo.*

(ii) *Se $f : M \to M'$, $g : M' \to M''$ e $h : M'' \to M'''$ são $A-$homomorfismos, então:*

$$h \circ (g \circ f) = (h \circ g) \circ f$$

(iii) *Se $f_1, f_2 : M \to M'$ e $g : M' \to M''$ são $A-$homomorfismo, então:*

$$g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2.$$

Em condições análogas vale:

$$(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$$

(iv) *Dado um $A-$homomorfismo $f : M \to N$, então:*

$$id_N \circ f = f \ e \ f \circ id_M = f$$

(v) *Dados um $A-$homomorfismos $f : M \to M'$ e $g : M' \to M$ tais que $g \circ f = id_M$ então f é um monomorfismo e g um epimorfismo.*

Demonstração: Os itens de (i) a (iv) são de fácil verificação. Vamos provar o item (v).

(v) Sejam $x_1, x_2 \in M$ tais que $f(x_1) = f(x_2)$. Então $g \circ f(x_1) = g \circ f(x_2)$, isto é, $id_M(x_1) = id_M(x_2)$ e $x_1 = x_2$, logo f é monomorfismo.

Dado $x \in M$ qualquer, temos $id_M(x) = x$. Logo $g \circ f(x) = x$. Chamando $y = f(x) \in N$ vem que $g(y) = x$, portanto g é um epimorfismo.

■

Definição 2.28 *Um $A-$homomorfismo $f : M \to N$ diz-se um $A-$isomorfismo se existe um $A-$homomorfismo $g : N \to M$ tal que:*

$$g \circ f = id_M \text{ e } f \circ g = id_N.$$

Para indicar que f é um isomorfismo, vamos usar às vezes a notação: $M \cong N$.

Proposição 2.29 *Um $A-$homomorfismo $f : M \to N$ é um isomorfismo, se, e somente se, f é, simultaneamente, monomorfismo e epimorfismo.*

Demonstração: Seja f um isomorfismo e $g : N \to M$ um $A-$homomorfismo nas condições da definição.

Da relação $g \circ f = id_M$ e a parte (v) da proposição 2.27 vem que f é um monomorfismo. De $f \circ g = id_N$ vem imediatamente que f é também um epimorfismo.

Reciprocamente, suponhamos que f seja simultaneamente monomorfismo e epimorfismo. Então f é uma função bijetora e existe uma função inversa, isto é, uma função $g : N \to M$ tal que $g \circ f = id_M$ e $f \circ g = id_N$. Resta verificar apenas que g é um $A-$homomorfismo.

Dados $y_1, y_2 \in N$ provaremos que $g(y_1 + y_2) = g(y_1) + g(y_2)$.

Como f é um epimorfismo, existem $x_1, x_2 \in M$ tais que $f(x_1) = y_1$, $f(x_2) = y_2$. Assim,

$$g(y_1) + g(y_2) = g \circ f(x_1) + g \circ f(x_2) = x_1 + x_2.$$

Como f é $A-$homomorfismo $f(x_1 + x_2) = y_1 + y_2$.

Aplicando g em ambos os lados da igualdade anterior, obtemos:

$$x_1 + x_2 = g(y_1 + y_2).$$

■

De forma análoga, pode-se provar que $g(ay) = ag(y)$, para todo $a \in A$ e todo $y \in N$.

2.4 Teorema do Homomorfismo e Aplicações

Teorema 2.30 *(Teorema do homomorfismo para módulos). Sejam M e N $A-$módulos, $f : M \to N$ um $A-$homomorfismo, $j : M \to M/Ker(f)$ a projeção canônica ao quociente e $i : Im(f) \to N$ a inclusão. Existe uma única função $f^* : M/Ker(f) \to Im(f)$ tal que:*

(i) $f = i \circ f^* \circ j$.

(ii) f^* é um isomorfismo.

A relação entre as funções do enunciado pode-se visualizar no diagrama adjunto:

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & N \\ {\scriptstyle j}\downarrow & & \uparrow{\scriptstyle i} \\ M/Ker(f) & \xrightarrow{\quad f^* \quad} & Im(f) \end{array}$$

Demonstração: Defina $f^* : M/Ker(f) \to Im(f)$ por $f^*(m + Ker(f)) = f(m)$, $\forall m + Ker(f) \in M/Ker(f)$.

Temos que f^* está bem definida pois:

$m_1 + Ker(f) = m_2 + Ker(f) \Longrightarrow m_1 - m_2 \in Ker(f) \Longrightarrow f(m_1 - m_2) = 0 \Longrightarrow f(m_1) = f(m_2) \Longrightarrow f^*(m_1 + Ker(f)) = f^*(m_2 + Ker(f))$.

(i) $(i \circ f^* \circ j)(m) = (i \circ f^*)(j(m)) = (i \circ f^*)(m + Ker(f)) = i(f^*(m + Ker(f))) = i(f(m)) = f(m)$, para todo $m \in M$. Logo, $i \circ f^* \circ j = f$.

(ii) Vejamos que f^* é $A-$homomorfismo. Para isso, sejam $m_1 + Ker(f)$, $m_2 + Ker(f) \in M/Ker(f)$ e $a \in A$. Temos que

- $f^*(m_1 + Ker(f) + m_2 + Ker(f)) = f^*((m_1 + m_2) + Ker(f)) = f(m_1 + m_2) = f(m_1) + f(m_2) = f^*(m_1 + Ker(f)) + f^*(m_2 + Ker(f))$.

- $f^*(a \cdot (m_1 + Ker(f))) = f^*(am_1 + Ker(f)) = f(am_1) = a \cdot f(m_1) = a \cdot f^*(m_1 + Ker(f))$.

Agora, mostremos que f^* é epimorfismo e monomorfismo.

- Seja $y \in Im(f)$. Então, existe $m \in M$ tal que $y = f(m)$. Temos que $m + Ker(f) \in M/Ker(f)$ e

$$f^*(m+Ker(f)) = f(m) = y.$$

Logo, f^* é epimorfismo.

• Sejam $m_1+Ker(f)$, $m_2+Ker(f) \in M/Ker(f)$ tais que $f^*(m_1+Ker(f)) = f^*(m_2+Ker(f))$. Assim,

$$f(m_1) = f(m_2) \Longrightarrow f(m_1-m_2) = 0 \Longrightarrow m_1-m_2 \in Ker(f) \Longrightarrow m_1+Ker(f) = m_2+Ker(f).$$

Portanto, f^* é monomorfismo.

■

Corolário 2.31 *Se $f : M \to N$ é um $A-$epimorfismo, então $N \cong M/Ker(f)$.*

No próximo corolário determinamos a forma dos módulos cíclicos sobre um anel dado.

Corolário 2.32 *Seja A um anel. Todo $A-$módulo cíclico é isomorfo a um módulo quociente de A por um ideal à esquerda de A. Reciprocamente, se I é um ideal à esquerda de A, A/I é um $A-$módulo cíclico.*

Demonstração: Seja $M = [m]$ um $A-$módulo cíclico. Temos que A é um $A-$módulo e podemos definir um $A-$homomorfismo $f : A \to M$ por $f(a) = a \cdot m$, $\forall a \in A$.

Como m é um gerador de M, f é um epimorfismo. Do corolário 2.31, $M \cong A/Ker(f)$. Sabemos que $Ker(f)$ é um submódulo de A e portanto, é um ideal à esquerda de A.

Reciprocamente, se I é um ideal à esquerda de A é fácil ver que o $A-$módulo A/I é cíclico, gerado pelo elemento $1+I$.

■

Podemos agora utilizar o resultado acima para classificar os grupos cíclicos. Como os únicos ideais de $\mathbb{Z}$ são principais da forma $[m]$, com $m \in \mathbb{Z}$ (veja a referência [3], p.22) vem que todo grupo cíclico é isomorfo a um quociente da forma $\mathbb{Z}/[m]$. Eventualmente, pode acontecer que $m = 0$; neste caso o grupo é isomorfo a $\mathbb{Z}$.

Incidentalmente, notemos que no conjunto dos inteiros módulo m podemos distinguir duas estruturas algébricas: a estrutura de anel e a estrutura de grupo abeliano (ou, equivalentemente, de $\mathbb{Z}-$módulo). Para referirmos a esta última, usaremos o símbolo $\mathbb{Z}_m$.

Teorema 2.33 *(Primeiro teorema do isomorfismo). Sejam M um $A-$módulo e P e N dois submódulos tais que $P \subset N$. Então:*

$$M/N \cong \frac{M/P}{N/P}.$$

Demonstração: Definimos uma função $f : M/P \to M/N$ por:

$$f(m+P) = m+N, \ \forall m \in M.$$

Como $P \subset N$ segue-se facilmente que, se $m_1, m_2 \in M$ são tais que $m_1 + P = m_2 + P$ então $m_1 + N = m_2 + N$, o que permite provar que a definição de f independe do representante.

Também é trivial verificar que f é um epimorfismo. Logo, do corolário 2.31 e do teorema 2.30, temos que:

$$\frac{M/P}{Ker(f)} \cong M/N.$$

Observe que,

$$m+P \in Ker(f) \iff m+N = N \iff m \in N.$$

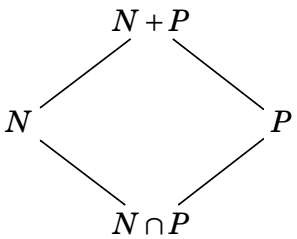
Logo, $Ker(f) = N/P$, o que completa a demonstração.

■

Teorema 2.34 *(Segundo teorema do isomorfismo). Sejam N e P submódulos de um $A-$módulo M. Então tem-se que:*

$$\frac{N}{N \cap P} \cong \frac{N+P}{P}.$$

A relação entre os submódulos do enunciado pode-se visualizar no seguinte diagrama:



Demonstração: Definimos $f : N \to \frac{N+P}{P}$ por $f(n) = n + P$, $\forall n \in N$.

Claramente f é um homomorfismo, e para verificar que é sobrejetor basta observar que todo elemento de $\frac{N+P}{P}$ é da forma $(n+p)+P$ com $n \in N$, $p \in P$. Mas $(n+p)+P = n+P$, logo $f(n) = n+P = (n+p)+P$ e f é epimorfismo.

Temos então que: $\frac{N}{Ker(f)} \cong \frac{N+P}{P}$.

Finalmente, observemos que dado $n \in N$,

$$n \in Ker(f) \Longleftrightarrow n+P = P \Longleftrightarrow n \in P.$$

Logo, $Ker(f) = N \cap P$, o que completa a demonstração.

■

O resultado acima é chamado, às vezes, isomorfismo de Noether.

2.5 $\mathbb{Z}_2G$–Módulos

Seja $(G, \cdot)$ um grupo multiplicativo. Definimos o anel $\mathbb{Z}_2G$ como segue:

$$\mathbb{Z}_2G := \left\{ \sum_{g \in G} r_g g \,|\, r_g \in \mathbb{Z}_2, r_g = 0 \text{ exceto para um número finito de elementos } g \in G \right\}.$$

Sobre $\mathbb{Z}_2G$ podemos considerar as seguintes operações de adição e multiplicação:

$$\left(\sum_{g \in G} r_g g \right) + \left(\sum_{g \in G} s_g g \right) = \sum_{g \in G} (r_g + s_g) g,$$
$$\left(\sum_{g \in G} r_g g \right) \cdot \left(\sum_{h \in G} s_h h \right) = \sum_{g,h \in G} (r_g s_h)(gh).$$

Tais operações fazem de $\mathbb{Z}_2G$ um anel com unidade $1_{\mathbb{Z}_2G} = 1_{\mathbb{Z}_2} 1$ (onde 1 é o elemento neutro de G), chamado anel grupo de G sobre $\mathbb{Z}_2$. Em geral, o elemento $1_{\mathbb{Z}_2} g \in \mathbb{Z}_2G$ será denotado simplesmente por g.

Um elemento x de $\mathbb{Z}_2G$ é da forma:

$$x = 1g_1 + \ldots + 1g_k \equiv g_1 + \ldots + g_k,$$

com $1 \in \mathbb{Z}_2$ e $g_i \in G$.

Definição 2.35 *Sejam G um grupo denotado multiplicativamente com elemento neutro 1 e M um conjunto não vazio. Uma* ***ação (à esquerda) de G sobre M*** *(ou uma* ***G-ação sobre M****) é uma função:*

$$\mu : G \times M \to M$$
$$(g,m) \mapsto \mu(g,m) = g \cdot m$$

satisfazendo:

(i) $1 \cdot m = m, \forall m \in M$;

(ii) $(g_1 g_2) \cdot m = g_1 \cdot (g_2 \cdot m), \forall g_1, g_2 \in G$ *e* $\forall m \in M$.

Se na definição acima M tiver uma estrutura de grupo (aditivo), para que esta estrutura seja preservada pela $G-$ação, além das condições (i) e (ii) exige-se a seguinte condição:

(iii) $g \cdot (m_1 + m_2) = g \cdot m_1 + g \cdot m_2$.

Recordamos que o conceito de $R-$módulo (R anel com unidade) já foi estudado anteriormente neste capítulo (definição 2.1).

Para obtermos o conceito de $\mathbb{Z}_2G$**-módulos** basta considerar na definição 2.1 o anel $R = \mathbb{Z}_2G$. Vimos ainda que todo $K-$espaço vetorial (K corpo) é um $K-$módulo. Logo, todo $\mathbb{Z}_2-$espaço vetorial M (isto é, grupo abeliano em que todo elemento tem ordem 2) é um $\mathbb{Z}_2-$módulo.

Além disso, no contexto módulos e ação de grupos, temos o seguinte resultado:

Proposição 2.36 *Sejam G um grupo e M um conjunto não vazio. M é um $\mathbb{Z}_2G-$módulo se, e somente se, M é um $\mathbb{Z}_2-$módulo munido de uma $G-$ação.*

Demonstração: ($\Longrightarrow$) Se M é um $\mathbb{Z}_2G-$módulo então M é um $\mathbb{Z}_2-$módulo com $r \cdot a := (r \cdot 1) \cdot a$ (onde 1 é o elemento neutro de G) e a $G-$ação é dada por:

$$g \cdot a := (\overline{1}g) \cdot a \text{ (onde } \overline{1} \text{ é a unidade de } \mathbb{Z}_2).$$

($\Longleftarrow$) Se M é um $\mathbb{Z}_2-$módulo e existe uma $G-$ação sobre M, então podemos dar a M uma estrutura de $\mathbb{Z}_2G-$módulo da seguinte forma:

$$\left(\sum_{g\in G} r_g g \right) \cdot a = \sum_{g\in G} r_g (g \cdot a).$$

■

Exemplo 2.37 *Seja G um grupo. Então $P(G)$ é um $\mathbb{Z}_2G-$módulo. A $G-$ação natural é dada por:*

$$G \times P(G) \to P(G)$$
$$(g, A) \mapsto g \cdot A := \{g \cdot x | x \in A\}.$$

Além disso, $F(G)$ e $Q(G)$ são $\mathbb{Z}_2G-$submódulos de $P(G)$.

CAPÍTULO 3

Ends de Grupos

A definição de ends foi introduzida por Hopf e Freudental para grupos finitamente gerados e foi totalmente amparada na definição de ends de espaços. A definição algébrica de número de ends de um grupo G qualquer, foi dada por Specker. As principais referências para este capítulo são [7], [8] e [9].

3.1 Definição; Ends de Grupos Finitos

Dado um grupo G, vimos nos exemplos 1.3, 1.11 e 1.13 que $P(G) = \{A | A \subset G\}$ é um $\mathbb{Z}_2-$espaço vetorial, $F(G) = \{A \in P(G) | A \text{ é finito}\}$ e $Q(G) = \{A \in P(G) | \forall g \in G, A + gA \in F(G)\}$ são $\mathbb{Z}_2-$subespaços vetoriais de $P(G)$, onde $A+B = (A \cup B) - (A \cap B)$ (diferença simétrica) e $\overline{0} \cdot A = \emptyset$, $\overline{1} \cdot A = A$, $\forall A, B \subset G$.

Definição 3.1 *Dado um grupo G, o número de ends de G, denotado por $e(G)$, é definido por $e(G) := dim_{\mathbb{Z}_2}(Q(G)/F(G))$, que denotamos apenas por $dim(Q(G)/F(G))$.*

Proposição 3.2 *Seja G um grupo.*

(i) Se G é infinito, então $\overline{\emptyset}$ e $\overline{G}$ são elementos distintos em $Q(G)/F(G)$ e portanto, $e(G) \geq 1$.

(ii) G é finito se, e somente se, $e(G) = 0$.

(iii) $e(G) \geq 2$ se, e somente se, existe $\overline{A} \in Q(G)/F(G)$ tal que $\overline{A} \neq \overline{\emptyset}$ e $\overline{A} \neq \overline{G}$. Neste caso, $\overline{\emptyset}, \overline{A}, \overline{A^c}, \overline{G}$ são elementos distintos em $Q(G)/F(G)$.

(iv) $e(G) = 2$ se, e somente se, existe $\overline{A}$ como em (iii) tal que para qualquer $\overline{B} \in Q(G)/F(G)$, $\overline{B} \neq \overline{\emptyset}$ e $\overline{B} \neq \overline{G}$ tem-se $\overline{B} = \overline{A}$ ou $\overline{B} = \overline{A^c}$.

Demonstração: (i) Dado um grupo G, temos que $G \in Q(G)$, pois para qualquer $g \in G, G + gG = G + G = \emptyset \in F(G)$. Assim, $\overline{G} \in Q(G)/F(G)$.

Agora, como G é infinito segue que $G \notin F(G)$. Logo, $G + F(G) \neq \emptyset + F(G)$ e então $\overline{G} \neq \overline{\emptyset}$. Portanto, $e(G) = dim(Q(G)/F(G)) \geq 1$.

(ii) Como G é finito, temos que $P(G) = F(G) = Q(G)$. Consequentemente, $e(G) = dim(Q(G)/F(G)) = 0$.

Reciprocamente, suponhamos por absurdo que G seja infinito. Então, por (i), temos que $e(G) \geq 1$, o que contradiz a hipótese. Portanto, G é finito.

(iii) Claramente, $e(G) \geq 2$ se, e somente se, existe $\overline{A} \in Q(G)/F(G)$ tal que $\overline{A} \neq \overline{\emptyset}$ e $\overline{A} \neq \overline{G}$. Neste caso, considerando um tal A temos:

• $\forall g \in G, A^c + gA^c = (A^c \cap (gA^c)^c) \cup (A \cap (gA^c)) = (A^c \cap gA) \cup (A \cap (gA)^c) = A + gA \in F(G)$ pois $A \in Q(G)$. Daí, $\overline{A^c} \in Q(G)/F(G)$.

• $\overline{A^c} \neq \overline{A}$. De fato, se $\overline{A^c} = \overline{A}$ então $A^c + A = G \in F(G)$, o que é uma contradição, pois G é infinito.

• $\overline{A^c} \neq \overline{\emptyset}$, pois como $\overline{A} \neq \overline{G}$ segue que $A^c = A + G \notin F(G)$.

• $\overline{A^c} \neq \overline{G}$ pois se $\overline{A^c} = \overline{G}$ então $A^c + G = A \in F(G)$, o que é um absurdo, já que A é infinito.

Logo, $\{\overline{\emptyset}, \overline{A}, \overline{A^c}, \overline{G}\} \subset Q(G)/F(G)$ e como $\{\overline{\emptyset}, \overline{A}, \overline{A^c}, \overline{G}\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ segue que $e(G) \geq 2$.

(iv) Consequência imediata de (iii).

■

Exemplo 3.3 *Temos que* $e(\mathbb{Z}_n) = 0, e(S_3) = 0$ *e* $e(\mathbb{Z}_4 \times \mathbb{Z}_6) = 0$ *pois* $\mathbb{Z}_n, S_3$ *e* $\mathbb{Z}_4 \times \mathbb{Z}_6$ *são finitos. Agora, como* $\mathbb{Z}$ *e* $\mathbb{R}$ *são infinitos segue que* $e(\mathbb{Z}) \geq 1$ *e* $e(\mathbb{R}) \geq 1$.

Observação 3.4 $e(G)$ *é um invariante algébrico, isto é, se* $G_1 \cong G_2$ *(grupos isomorfos) então* $e(G_1) = e(G_2)$ *pois se* $G_1 \cong G_2$*, então* $Q(G_1)/F(G_1) \cong Q(G_2)/F(G_2)$ *como* $\mathbb{Z}_2-$*espaços vetoriais.*

3.2 Cálculo do Número de Ends do Grupo Cíclico Infinito

Teorema 3.5 *Se* G *é o grupo cíclico infinito, isto é,* $G = [a] \cong \mathbb{Z}$*, então* $e(G) = 2$.

Demonstração: De acordo com a proposição 3.2, basta mostrar que existe $\overline{A} \in Q(G)/F(G)$ tal que $\overline{A} \neq \overline{\emptyset}$ e $\overline{A} \neq \overline{G}$, e para qualquer $\overline{B} \in Q(G)/F(G)$, $\overline{B} \neq \overline{\emptyset}$ e $\overline{B} \neq \overline{G}$ temos que $\overline{B} = \overline{A}$ ou $\overline{B} = \overline{A^c}$. Para isso, seja $A = \{a^n | n > 0\} \subset G$. Assim,

• $\overline{A} \in Q(G)/F(G)$, pois para todo $g = a^k \in G$, $gA = \{a^{k+n} | n > 0\}$ e $(A \cap (gA^c)) \cup (A^c \cap gA)$ é finito (observe que para $k > 0$, $A \cap gA^c = \{a, ..., a^k\}$ e $A^c \cap gA = \emptyset$; para $k < 0$, $A \cap gA^c = \emptyset$ e $A^c \cap gA = \{a^{k+1}, a^{k+2}, ..., a^0\}$; para $k = 0$, $g = 1$ e $A + A = \emptyset$).

• $\overline{A} \neq \overline{\emptyset}$ pois $A \notin F(G)$ e $\overline{A} \neq \overline{G}$ pois $A^c \notin F(G)$.

Agora provemos a seguinte afirmação:

Se $\overline{B} \in Q(G)/F(G)$ então para quase todo n (isto é, exceto um número finito $n_1, ..., n_r$) $a^n \in B$ implica que $a^{n-1} \in B$.

De fato, se $\overline{B} \in Q(G)/F(G)$ então $B \in Q(G)$ e assim, para todo $g \in G$, $B + gB \in F(G)$, ou seja, $\overline{gB} = \overline{B}$. Em particular, para $g = a$. Suponhamos que existam infinitos n's tais que:

(1) $a^n \in B$ e $a^{n+1} \notin B$ ou

(2) $a^n \in B$ e $a^{n-1} \notin B$ (equivalentemente, $a^n \notin aB$).

Então existiriam infinitos n's tais que:

(1) $a^{n+1} = aa^n \in aB$ (pois $a^n \in B$) e $a^{n+1} \notin B$, logo, $a^{n+1} \in aB \cap B^c$ ou

(2) $a^n = aa^{n-1} \notin aB$ (pois $a^{n-1} \notin B$) e $a^n \in B$, logo, $a^n \in (aB)^c \cap B$.

Assim, $aB + B = ((aB) \cap B^c) \cup ((aB)^c \cap B)$ seria infinito, isto é, $B \notin Q(G)$ e daí $\overline{B} \notin Q(G)/F(G)$, o que é uma contradição.

Portanto, a afirmação acima é verdadeira e note que ela nos diz que pode existir apenas um número finito de elementos de B que satisfaz: $a^n \in B$ mas $a^{n+1} \notin B$ ou $a^{n-1} \notin B$. Em particular, isto obviamente é verdadeiro se B é finito (assim o caso de interesse é quando B é infinito) e também é verdadeiro para $B = A = \{a^n | n > 0\}$ pois apenas para $n = 1$ tem-se que $a^n \in B$ mas $a^{n-1} \notin B$. Para $n \geq 2$, $a^n \in B$ e temos $a^{n+1} \in B$ e $a^{n-1} \in B$.

Agora, dado $\overline{B} \in Q(G)/F(G)$ e A como acima, temos as quatro seguintes possibilidades para os conjuntos $B \cap A$ e $B \cap A^c$:

(i) $B \cap A$ finito e $B \cap A^c$ finito.

Isso implica em B ser finito pois $B = B \cap (A \cup A^c) = (B \cap A) \cup (B \cap A^c)$.

Logo, $\overline{B} = \overline{\emptyset}$.

(ii) $B \cap A$ infinito e $B \cap A^c$ infinito.

Do fato de $B \cap A$ ser infinito obtemos que B é infinito e da afirmação anterior segue que existe um inteiro positivo m_1 tal que $a^n \in B \cap A$, $\forall n > m_1$. Para ver isto, tome $m_0 = max\{n_1, ..., n_r\}$ onde $n_1, ..., n_r$ são os inteiros dados na afirmação. Como $B \cap A$ é infinito, $\exists m_1 > m_0$, $m_1 > 0$ tal que $a^{m_1} \in B \cap A$ e como $m_1 \neq n_i$, $i = 1, ..., r$, então $a^{m_1+1}, a^{m_1+2}, ... \in B \cap A$, isto é, $a^m \in B \cap A$, $\forall m > m_1$. Consequentemente, $A \cap B^c \subset \{a^k \mid 0 \leq k \leq m_1\}$ e portanto, é finito.

Analogamente, usando que $B \cap A^c$ é infinito e a afirmação anterior, temos que existe um inteiro m_2 tal que $a^n \in B \cap A^c$, $\forall n > m_2$. Tome $m_0 = min\{n_1, ..., n_r\}$. Como $B \cap A^c$ é infinito, $\exists m_2 < m_0$, $m_2 < 0$ tal que $a^{m_2} \in B \cap A^c$ e tem-se $a^m \in B \cap A^c$, $\forall m < m_2$. Daí, $A^c \cap B^c \subset \{a^k \mid m_2 \leq k \leq 0\}$ e portanto, é finito.

Logo, $B^c = B^c \cap (A \cup A^c) = (B^c \cap A) \cup (B^c \cap A^c)$ é finito.

Assim, $\overline{B^c} = \overline{\emptyset}$, ou equivalentemente, $\overline{B} = \overline{G}$.

(iii) $B \cap A$ finito e $B \cap A^c$ infinito.

Como vimos em (ii), $B \cap A^c$ infinito implica em $A^c \cap B^c$ finito.

Logo, $B + A^c = (B \cap A) \cup (B^c \cap A^c)$ é finito e portanto, $\overline{B} = \overline{A^c}$.

(iv) $B \cap A$ infinito e $B \cap A^c$ finito.

Conforme vimos em (ii), $B \cap A$ infinito implica em $A \cap B^c$ finito.

Assim, $B + A = (B \cap A^c) \cup (B^c \cap A)$ é finito. Logo, $\overline{B} = \overline{A}$.

Daí, dado qualquer $\overline{B} \in Q(G)/F(G)$ com $\overline{B} \neq \overline{\emptyset}$ e $\overline{B} \neq \overline{G}$ tem-se que $\overline{B} = \overline{A}$ ou $\overline{B} = \overline{A^c}$.

Portanto, $e(G) = 2$.

■

Observação 3.6 *Em particular, quando $G = \mathbb{Z}$, o conjunto dado na demonstração do teorema anterior é $A = \{1, 2, ...\} = \mathbb{N}^*$, $A^c = \{..., -2, -1, 0\}$, $Q(\mathbb{Z})/F(\mathbb{Z}) = \{\overline{\emptyset}, \overline{\mathbb{Z}}, \overline{A}, \overline{A^c}\}$ e uma base para $Q(\mathbb{Z})/F(\mathbb{Z})$ é $\{\overline{A}, \overline{A^c}\}$.*

3.3 Cálculo do Número de Ends de um Grupo não Enumerável

Apresentamos aqui alguns conceitos e resultados sobre enumerabilidade que serão importantes para a demonstração do principal teorema desta subseção (teorema 3.28, sobre o número de ends de um grupo não enumerável).

Definição 3.7 *Dois conjuntos A e B são ditos equivalentes ou equipotentes (mesma potência) se existe uma função bijetora de A em B.*

Notação: $A \approx B$.

Lema 3.8 *A relação de equipotência definida anteriormente é de equivalência.*

Demonstração: (i) Para todo conjunto A, existe a aplicação $id_A : A \to A$ que é bijetora. Então todo conjunto é equipotente a si mesmo. Assim, vale a propriedade reflexiva para esta relação entre conjuntos.

(ii) Se A é equipotente a B, então existe $f : A \to B$ bijetora e como $f^{-1} : B \to A$ também é bijetora, segue que B é equipotente a A. Logo, vale a propriedade simétrica para esta relação.

(iii) Se A é equipotente a B e B é equipotente a C, isto é, existem $f : A \to B$ e $g : B \to C$ bijetoras. Então, $g \circ f : A \to C$ também é bijetora. Daí, A é equipotente a C e assim vale a propriedade transitiva para esta relação.

Portanto, de $(i),(ii)$ e (iii), temos que a relação de equipotência é de equivalência.

■

Definição 3.9 *Usando o conceito anterior, temos que um conjunto A é finito se $A = \emptyset$ ou, em caso contrário, se existir $n \in \mathbb{N}^*$ de maneira que $A \approx \{1,2,...,n\}$. Se A não é um conjunto finito, então A é dito infinito, ou seja, A não é equipotente a nenhum dos subconjuntos $\{1,2,...,n\} \subset \mathbb{N}^*$.*

Os seguintes resultados decorrem diretamente da definição dada anteriormente:

- Se $A \subset U$ é finito e $x \in U - A$, então $A \cup \{x\}$ também é finito.
- Se A é um conjunto infinito, então $A - \{x\}$ também é infinito, para qualquer que seja $x \in A$.

Observação 3.10 *Dois conjuntos finitos são equipotentes se, e somente se, eles têm o mesmo número de elementos.*

Definição 3.11 *Seja A um conjunto. A diz-se enumerável se A é equipotente a algum subconjunto de $\mathbb{N}^*$, isto é, se $A \approx L \subset \mathbb{N}^*$.*

Exemplo 3.12 *O conjunto $\mathbb{Z}$ dos números inteiros é enumerável. De fato,*

- $\mathbb{N} \approx \mathbb{N}^*$, *pois* $f : \mathbb{N} \to \mathbb{N}^*$ *dada por* $f(n) = n+1$ *é bijetora.*
- $\mathbb{Z} \approx \mathbb{N}$, *pois* $f : \mathbb{Z} \to \mathbb{N}$ *dada por* $f(n) = \begin{cases} 2n, & se \quad n \geq 0 \\ -2n-1, & se \quad n < 0 \end{cases}$ *é bijetora*

Daí, $\mathbb{Z} \approx \mathbb{N}^*$ e portanto, $\mathbb{Z}$ é enumerável. Em particular, todo subconjunto de $\mathbb{Z}$ é enumerável.

Definição 3.13 *Um conjunto é chamado* ***contável*** *se ele é finito ou enumerável.*

Daremos a seguir a definição de partição em um conjunto que nos será útil na demonstração do teorema 3.17.

Definição 3.14 *Dado um conjunto A, uma* ***partição*** *em A é uma família $(A_i)_{i \in I}$ (onde I é o conjunto de índices) de subconjuntos de A tais que:*

(i) $A_i \neq \emptyset$, para todo $i \in I$;

(ii) $\bigcup A_i = A$;

(iii) $\forall A_i, A_j \in (A_i)_{i \in I}$, vale uma, e uma só, das igualdades: $A_i = A_j$ ou $A_i \cap A_j = \emptyset$.

Teorema 3.15 *Um conjunto A é enumerável se, e somente se, existe $L \subset \mathbb{N}^*$ e existe $f : L \to A$ aplicação sobrejetora.*

Demonstração: ($\Longrightarrow$) Por hipótese, A é enumerável e então existe $L \subset \mathbb{N}^*$ tal que $f : L \to A$ é bijetora. Portanto, f é sobrejetora.

($\Longleftarrow$) Seja $f : L \to A$ sobrejetora. Para cada $a \in A$, seja $L_a = \{x \in L \mid f(x) = a\}$. Considere $(L_a)_{a \in A}$ uma partição de L e $M \subset L$ o subconjunto que contém um único elemento de cada $L_a, a \in A$.

Assim, temos que $f|M : M \to A$ é bijetora e como $M \subset L \subset \mathbb{N}^*$ segue que A é enumerável.

■

Lema 3.16 *Se existe $f : A \to B$ sobrejetora e A é enumerável, então B também é enumerável.*

Demonstração: Como A é enumerável, segue que existem $M \subset \mathbb{N}^*$ e $g : M \to A$ sobrejetora. Então, $f \circ g : M \to B$ é sobrejetora pois é a composta de duas funções sobrejetoras.

Logo, pelo teorema anterior, podemos concluir que B é enumerável.

■

Teorema 3.17 (i) *Todo conjunto infinito contém um subconjunto enumerável.*

(ii) *Todo subconjunto infinito de um conjunto enumerável é enumerável.*

Demonstração: (i) Sejam A um conjunto infinito e $x_1 \in A$. Consideremos os subconjuntos $\{x_1\}$ e $A - \{x_1\}$ de A. Então a partição determinada em A por estes subconjuntos nos permite considerar o subconjunto $\{x_1, x_2\} \subset A$, onde $x_2 \in A - \{x_1\}$, ou seja, $x_1 \neq x_2$.

Agora, considerando a partição de A formada por $\{x_1\}, \{x_2\}$ e $A - \{x_1\}$ podemos garantir que existe $x_3 \in A$ tal que $x_3 \neq x_1$ e $x_3 \neq x_2$.

E assim, sucessivamente, usando o raciocínio acima, obtemos o subconjunto $E = \{x_1, x_2, ...\}$ que é enumerável.

(ii) Sejam A um conjunto enumerável, B um subconjunto infinito de A e fixemos $b \in B$.

A aplicação $f : A \to B$ tal que $f(x) = x, \forall x \in B$, e $f(x) = b, \forall x \in A - B$, é sobrejetora.

Portanto, pelo lema anterior, como A é enumerável e f é sobrejetora temos que B também é enumerável.

■

Observação 3.18 *Se $A_1, A_2, ..., A_n$ são enumeráveis, então $A_1 \cup A_2 \cup ... \cup A_n$ também é enumerável. Mais geralmente, se $A_1, A_2, ...$ são subconjuntos enumeráveis de um mesmo conjunto U, então $A = A_1 \cup A_2 \cup ...$ também é enumerável.*

Observação 3.19 *Se A e B são enumeráveis então $A \times B$ também é enumerável.*

Proposição 3.20 *Sejam G um grupo e H_1 e H_2 subconjuntos de G. Se H_1 e H_2 são enumeráveis, então $H_1 \cdot H_2$ é enumerável, onde $H_1 \cdot H_2 = \{h_1 \cdot h_2 | h_1 \in H_1, h_2 \in H_2\}$.*

Demonstração: Como H_1 e H_2 são enumeráveis então $H_1 \times H_2$ é enumerável.

Seja $\varphi : H_1 \times H_2 \to H_1 \cdot H_2$ tal que $\varphi(h_1, h_2) = h_1 \cdot h_2$. Temos que φ é sobrejetora, pois para qualquer $y \in H_1 \cdot H_2, y = h_1 \cdot h_2 = \varphi(h_1, h_2)$.

Logo, pelo lema 3.16 segue que $H_1 \cdot H_2$ é enumerável.

■

Corolário 3.21 *Sejam G um grupo e $H_1, ..., H_n$ subconjuntos de $G, n \geq 2$. Se $H_1, ..., H_n$ são enumeráveis, então $H_1 \cdot ... \cdot H_n$ é enumerável.*

Demonstração: Faremos a demonstração por indução sobre n.

Para $n = 2$, foi provado na proposição anterior.

Suponhamos a afirmação verdadeira para $n = k$, ou seja, se $H_1, ..., H_k$ são enumeráveis, então $H_1 \cdot ... \cdot H_k$ é enumerável.

Agora, sejam $H_1, ..., H_k, H_{k+1}$ subconjuntos de G enumeráveis. Assim,

$$H_1 \cdot ... \cdot H_k \cdot H_{k+1} = (H_1 \cdot ... \cdot H_k) \cdot H_{k+1}.$$

Mas, por hipótese de indução, $H_1 \cdot ... \cdot H_k$ é enumerável. Daí, pela proposição anterior, $H_1 \cdot ... \cdot H_k \cdot H_{k+1}$ é enumerável.

■

Proposição 3.22 *O conjunto $\mathbb{Q}$ dos racionais é enumerável.*

Demonstração: Sejam $\mathbb{Q}^+ = \{\frac{a}{b}, a, b > 0, a, b \in \mathbb{N} | mdc(a, b) = 1\}$ e $\mathbb{Q}^- = \{-x | x \in \mathbb{Q}^+\}$. É claro que $\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$. Temos que os conjuntos $\mathbb{N} \times \mathbb{N}$ e $\mathbb{N}^* \times \mathbb{N}^*$ são enumeráveis. Se identificarmos $\frac{a}{b} \in \mathbb{Q}^+$ com $(a, b) \in \mathbb{N} \times \mathbb{N}$, temos uma bijeção de $\mathbb{Q}^+$ em um subconjunto infinito T de $\mathbb{N} \times \mathbb{N}$. Como todo subconjunto infinito de conjunto enumerável é enumerável (teorema 3.17 (ii)), segue que T, e portanto $\mathbb{Q}^+$ é enumerável.

Seja $f : \mathbb{N} \to \mathbb{Q}^+$ uma enumeração de $\mathbb{Q}^+$. Então, considerando $h : \mathbb{Q}^+ \to \mathbb{Q}^-$, dada por $h(x) = -x$, tem-se que $h \circ f : \mathbb{N} \to \mathbb{Q}^-$ enumera $\mathbb{Q}^-$.

Sendo $\mathbb{Q}$ a união de três conjuntos enumeráveis, temos que o conjunto $\mathbb{Q}$ dos números racionais é enumerável.

■

Nem todos os conjuntos são enumeráveis. Veremos alguns exemplos de conjuntos não enumeráveis. Para tanto, necessitamos da seguinte propriedade do corpo $\mathbb{R}$ dos números reais:

Princípio dos Intervalos Encaixantes: Sejam $I_1 = [a_1, b_1], I_2 = [a_2, b_2], ...$ tais que $I_1 \supset I_2 \supset ....$ Então existe ao menos um ponto comum a todos esses intervalos.

De fato, da hipótese $I_1 \supset I_2 \supset ...$ decorre que $a_1 \leq a_2 \leq ...$ e $b_1 \geq b_2 \geq ...$

Como $m \leq n$ implica $a_m \leq a_n \leq b_n$ e $n < m$ implica $a_m < b_m \leq b_n$, então $a_m < b_n$, para quaisquer índices m e n. Logo, cada b_m é um limite superior de $A = \{a_1, a_2, ...\}$ e portanto existe em $\mathbb{R}$ o elemento $S = sup(A)$. Assim, para cada índice m teremos $a_m \leq S$ pois $S = sup(A)$ e $S \leq b_m$ pois cada b_m é um limite superior de A. Daí, $a_m \leq S \leq b_m$, para todo índice $m \geq 1$, o que prova nossa afirmação.

Proposição 3.23 *O intervalo $I = [0, 1]$ não é enumerável.*

Demonstração: Suponhamos que I seja enumerável, ou seja, $I = \{x_1, x_2, ...\}$. Consideremos I dividido em três subintervalos de mesma amplitude:

$$\left[\ 0, \tfrac{1}{3}\ \right] \cup \left[\ \tfrac{1}{3}, \tfrac{2}{3}\ \right] \cup \left[\ \tfrac{2}{3}, 0\ \right]$$

e seja I_1 o primeiro desses intervalos, na ordem que foram escritos, que não contém x_1.

Façamos o mesmo tipo de subdivisão em I_1 e seja I_2 o primeiro dos subintervalos de I_1 (pelo mesmo critério anterior de ordenação) que não contém x_2. A repetição desse raciocínio dará origem a uma sequência $I_1 \supset I_2 \supset ...$ de intervalos fechados.

Pela propriedade do Princípio dos Intervalos Encaixantes, existe $x \in \bigcap_{n=1}^{\infty} I_n = I_1 \cap I_2 \cap ...$ e portanto $x \neq x_i$, para todo x_i. Mas isto é impossível, uma vez que $x \in I$.

Logo, I não é enumerável.

■

Corolário 3.24 *O conjunto $\mathbb{R}$ dos números reais não é enumerável.*

Demonstração: Se $\mathbb{R}$ fosse enumerável, então I também teria que ser, uma vez que $I \subset \mathbb{R}$.

■

Corolário 3.25 *O conjunto $\mathbb{R}-\mathbb{Q}$ dos números irracionais não é enumerável.*

Demonstração: Se $\mathbb{R}-\mathbb{Q}$ fosse enumerável, então $\mathbb{R}=\mathbb{Q}\cup(\mathbb{R}-\mathbb{Q})$ também seria já que $\mathbb{Q}$ é enumerável, o que é uma contradição em vista do corolário anterior.

■

Corolário 3.26 *$S^1=\{cost+isent|\, t\in\mathbb{R}\}$ é um conjunto não enumerável.*

Demonstração: Basta lembrarmos que $[0,1[$ é não enumerável e $\varphi:[0,1[\to S^1$ tal que $\varphi(x)=cos(2\pi x)+isen(2\pi x)$ é uma aplicação bijetora.

■

Lema 3.27 *Sejam G um grupo e H um subconjunto de G tal que $H\in Q(G)$ e $H\notin F(G)$. Então,*

(i) H gera G.

(ii) Se H é enumerável, então G é enumerável.

Demonstração: (i) Dado $g\in G$, como $H\in Q(G)$ temos que $gH+H\in F(G)$, ou seja, $(gH\cap H^c)\cup((gH)^c\cap H)$ é finito. Daí, $gH\cap H^c$ e $(gH)^c\cap H$ são finitos.

Agora, $gH=gH\cap G=gH\cap(H\cup H^c)=(gH\cap H)\cup(gH\cap H^c)$ e como gH é infinito (pois H é infinito) e $gH\cap H^c$ é finito, segue que $gH\cap H$ é infinito (portanto não vazio).

Assim, existe $h_0\in gH\cap H$, isto é, $h_0=gh_1$, com $h_1\in H$, ou seja, $g=h_0h_1^{-1}$.

Logo, $g\in[H]$ e portanto $G=[H]$.

(ii) Para qualquer $g\in G$, como $G=[H], g=l_1^{\varepsilon_1}\cdot\ldots\cdot l_k^{\varepsilon_k}, l_i\in H, \varepsilon_i=1$ ou $\varepsilon_i=-1$. Para cada $k\in\mathbb{N}^*$, seja $G_k=\{h_0^{\varepsilon_0}\cdot\ldots\cdot h_k^{\varepsilon_k}|\, h_i\in H$ e $\varepsilon_i\in\{1,-1\}\}$. Assim, $G_k=(H\cup H^{-1})\cdot\ldots\cdot(H\cup H^{-1})$ e pelo corolário 3.21, temos que G_k é enumerável.

Agora, como $G=\bigcup_{k=0}^{\infty}G_k$, segue da observação 3.18 que G é enumerável.

■

Teorema 3.28 *Seja G um grupo não enumerável.*

(i) Então $e(G)=1$ ou $e(G)=\infty$.

(ii) Se G também for abeliano, então $e(G)=1$.

Demonstração: (i) Como G não é enumerável, então G não é finito. Assim, $e(G) \neq 0$ e portanto $e(G) \geq 1$.

Se $e(G) = 1$, não há nada a demonstrar. Neste caso, como G é infinito, teremos só os elementos $\overline{\emptyset}$ e $\overline{G}$ distintos em $Q(G)/F(G)$.

Suponhamos $e(G) > 1$ e mostremos que $e(G) = \infty$.

Como $e(G) > 1$, pela proposição 3.2(iii), existe $\overline{H} \in Q(G)/F(G)$ (portanto, H é subconjunto de G com $H \in Q(G)$) tal que $\overline{H} \neq \overline{\emptyset}, \overline{H} \neq \overline{G}$ e $\overline{\emptyset}, \overline{H}, \overline{H^c}, \overline{G}$ são elementos distintos em $Q(G)/F(G)$. Daí, $H \notin F(G), H \neq G$ e $H^c \notin F(G)$.

Agora, provemos a seguinte afirmação:

Para tal H, existem subconjuntos H_1 e H_2 de G tais que $H_1 \cup H_2 = H, H_1 \cap H_2 = \emptyset, H_1, H_2 \in Q(G)$ e são infinitos.

De fato, como H e H^c são infinitos, podemos considerar $C_1 \subset H, C_2 \subset H^c$ tais que C_1, C_2 são enumeráveis infinitos. Então $C = C_1 \cup C_2$ é enumerável infinito e existe uma bijeção entre $\mathbb{N}^*$ e C. Assim, $C = \{c_i \mid i \in \mathbb{N}^*\}$.

Temos que $H \cap C^{-1}H^c$ é enumerável pois:

(1) Como $H \in Q(G), (H \cap gH^c) \cup (H^c \cap gH)$ é finito, $\forall g \in G$. Daí, $H \cap gH^c$ e $H^c \cap gH$ são finitos para qualquer $g \in G$. Em particular, para $g = c_i^{-1}, H \cap c_i^{-1}H^c$ é finito.

(2) $H \cap C^{-1}H^c = H \cap \left(\bigcup_{i=1}^{\infty} \{c_i^{-1}\} \right) H^c = \bigcup_{i=1}^{\infty} (H \cap c_i^{-1}H^c)$ (isto é, $H \cap C^{-1}H^c$ é uma reunião enumerável de conjuntos finitos e portanto enumerável).

Por outro lado, pelo lema anterior temos que H é não enumerável, pois se H fosse enumerável, como $H \in Q(G)$ e $H \notin F(G)$, G seria enumerável por (ii), o que contradiz a hipótese. Portanto, $H \cap C^{-1}H^c \subset H$ e $H \cap C^{-1}H^c \neq H$. Logo, existe $h_0 \in H$ tal que $h_0 \notin H \cap C^{-1}H^c$, ou seja, $h_0 \notin C^{-1}H^c$ e daí, $h_0 \notin c_i^{-1}H^c, \forall i \in \mathbb{N}^*$. Assim, $h_0 \in (c_i^{-1}H^c)^c = c_i^{-1}H, \forall i \in \mathbb{N}^*$ e então $h_0 = c_i^{-1}h_i, h_i \in H$. Daí, $c_i h_0 = h_i \in H, \forall i \in \mathbb{N}^*$ e portanto,

$$\bigcup_{i=0}^{\infty} \{c_i\} h_0 = Ch_0 \subset H. \tag{3.1}$$

Tomemos $H_1 = H \cap Hh_0$ e $H_2 = H \cap H^c h_0$ e temos que:

- $H_1 \cup H_2 = (H \cap Hh_0) \cup (H \cap H^c h_0) = H \cap (Hh_0 \cup H^c h_0) = H \cap (Hh_0 \cup (Hh_0)^c) = H \cap G = H.$
- $H_1 \cap H_2 = (H \cap Hh_0) \cap (H \cap H^c h_0) = H \cap (Hh_0 \cap (Hh_0)^c) = H \cap \emptyset = \emptyset.$

• Dado $g \in G$,

$$\begin{aligned}
H_1 + gH_1 &= H \cap Hh_0 + g(H \cap Hh_0) \\
&= H \cap Hh_0 + (gH \cap gHh_0) \\
&= [(H \cap Hh_0) \cap (gH \cap gHh_0)^c] \cup [(H \cap Hh_0)^c \cap (gH \cap gHh_0)] \\
&= [(H \cap Hh_0) \cap (gH^c \cup gH^c h_0)] \cup [(H^c \cup H^c h_0) \cap (gH \cap gHh_0)] \\
&= [(H \cap Hh_0 \cap gH^c) \cup (H \cap Hh_0 \cap gH^c h_0)] \cup [(H^c \cap gH \cap gHh_0) \cup (H^c h_0 \cap gH \cap gHh_0)] \\
&= [(H \cap gH^c) \cap Hh_0] \cup [H \cap (H \cap gH^c)h_0] \cup [(H^c \cap gH) \cap gHh_0] \cup [(H^c \cap gH)h_0 \cap gH] \in F(G)
\end{aligned}$$

já que $H \cap gH^c \in F(G)$ e $H^c \cap gH \in F(G)$ pois $H \in Q(G)$. Portanto, $H_1 \in Q(G)$.

$$\begin{aligned}
H_2 + gH_2 &= H \cap H^c h_0 + g(H \cap H^c h_0) \\
&= [(H \cap H^c h_0) \cap (gH \cap gH^c h_0)^c] \cup [(H \cap H^c h_0)^c \cap (gH \cap gH^c h_0)] \\
&= [(H \cap H^c h_0) \cap (gH^c \cup gHh_0)] \cup [(H^c \cup Hh_0) \cap (gH \cap gH^c h_0)] \\
&= [(H \cap H^c h_0 \cap gH^c) \cup (H \cap H^c h_0 \cap gHh_0)] \cup [(H^c \cap gH \cap gH^c h_0) \cup (Hh_0 \cap gH \cap gH^c h_0)] \\
&= [(H \cap gH^c) \cap H^c h_0] \cup [H \cap (H^c \cap gH)h_0] \cup [(H^c \cap gH) \cap gH^c h_0] \cup [(H \cap gH^c)h_0 \cap gH] \in F(G)
\end{aligned}$$

já que $H \cap gH^c$ e $H^c \cap gH$ são finitos. Portanto, $H_2 \in Q(G)$.

• H_1 e H_2 são infinitos. De fato:

Temos que $C_1 h_0 \subset H_1 = H \cap Hh_0$ pois,

$$C_1 \subset C \Longrightarrow C_1 h_0 \subset Ch_0 \subset H \text{ (por 3.1) e } C_1 \subset H \Longrightarrow C_1 h_0 \subset Hh_0.$$

Logo, $C_1 h_0 \subset H \cap Hh_0 = H_1$.

Agora, temos que $C_2 h_0 \subset H_2 = H \cap H^c h_0$ pois,

$$C_2 \subset C \Longrightarrow C_2 h_0 \subset Ch_0 \subset H \text{ (por 3.1) e } C_2 \subset H^c \Longrightarrow C_2 h_0 \subset H^c h_0.$$

Assim, $C_2 h_0 \subset H \cap H^c h_0 = H_2$.

Portanto, como C_1 e C_2 são infinitos segue que H_1 e H_2 são infinitos.

Com isso, a afirmação inicial está provada.

Agora, observe que:

• $\overline{H_1} \in Q(G)/F(G)$, pois $H_1 \in Q(G)$.

• $\overline{H_1} \neq \overline{\emptyset}$, pois H_1 é infinito.

• $\overline{H_1} \neq \overline{L}, \forall L$ com $H \subset L$ e $L \in Q(G)$, pois

$$\overline{H_1} = \overline{L} \Longrightarrow H_1 + L \in F(G).$$

Mas, $H_1 + L = (H_1 \cap L^c) \cup ((H_1)^c \cap L)$. Como $H_2 \subset H_1^c$ e $H_2 \subset H \subset L$, segue que $H_2 \subset H_1^c \cap L$. Agora, $H_1 \subset H$ e $H \subset L$ implica em $H_1 \cap L^c = \emptyset$. Daí, $H_1 + L = \emptyset \cup (H_1^c \cup L) \supset H_2$ que é infinito. Logo, $H_1 + L$ é infinito, o que contradiz a afirmação. Portanto, $\overline{H_1} \neq \overline{L}$.

Logo, $\overline{H_1} \in Q(G)/F(G)$ e $\overline{H_1} \notin \{\overline{\emptyset}, \overline{G}, \overline{H}\}$ e então os elementos de $\{\overline{\emptyset}, \overline{G}, \overline{H}, \overline{H_1}\}$ são distintos.

Note que, como $\overline{H_1} \neq \overline{\emptyset}$ e $\overline{H_1} \neq \overline{G}$, a afirmação inicial também é verdadeira para H_1 (no lugar de H), isto é, $H_1 = H_{11} \cup H_{12}$ com $H_{11}, H_{12} \in Q(G), H_{11} \cap H_{12} = \emptyset$ e H_{11}, H_{12} infinitos. Também conclui-se que $\overline{H_{11}} \in Q(G)/F(G)$ e $\overline{H_{11}} \notin \{\overline{\emptyset}, \overline{G}, \overline{H}, \overline{H_1}\}$ pois H_{11} é infinito e $\overline{H_{11}} \neq \overline{L}, \forall L$ com $H_1 \subset L$, como vimos anteriormente.

Aplicando sucessivamente o mesmo processo obtemos uma sequência infinita de elementos distintos em $Q(G)/F(G)$, ou seja, $\{\overline{\emptyset}, \overline{G}, \overline{H}, \overline{H_1}, \overline{H_{11}}, \overline{H_{111}}, ...\}$.

Logo, supondo $e(G) > 1$ obtemos que $e(G) = \infty$.

Portanto, $e(G) = 1$ ou $e(G) = \infty$.

(ii) Agora, suponhamos que G seja abeliano e $e(G) > 1$.

Se $e(G) > 1$ então teríamos como no caso (i), que o conjunto H_2 da construção anterior seria infinito, mas, por outro lado, temos que $H_2 = H \cap H^c h_0 = H \cap h_0 H^c$ e como $H \in Q(G)$ segue que H_2 é finito, o que é uma contradição.

Portanto, no caso em que G é abeliano e não enumerável, teremos necessariamente $e(G) = 1$.

■

Exemplo 3.29 *Se G é um dos seguintes grupos: $(\mathbb{R}, +), (\mathbb{R}^*, \cdot), (S^1, \cdot), (S^1 \times S^1, \cdot), (\mathbb{R}[t], +)$, onde $\mathbb{R}[t]$ é o anel dos polinômios com coeficientes em $\mathbb{R}$, então $e(G) = 1$ pois todos os grupos são abelianos não enumeráveis.*

Exemplo 3.30 $e(S_3 \times \mathbb{R}) = 1$ *ou* ∞ *pois $S_3 \times \mathbb{R}$ não é um grupo abeliano e é não enumerável (aqui S_3*

indica o grupo das bijeções de $\{1,2,3\}$*).*

3.4 Ends de um Grupo Quociente G/H, quando H é um subgrupo normal e finito

Para a demonstração do principal resultado desta subseção (teorema 3.35), usaremos em diversas situações, resultados sobre imagem inversa e imagem direta de uma função. Para isto, faremos a seguir uma recordação desses conceitos.

Definição 3.31 *Seja $f : A \to B$ uma função. Dado um subconjunto $X \subset A$, chama-se **imagem direta** de X por f, e indica-se por $f(X)$, o seguinte subconjunto de B:*

$$f(X) = \{f(x) | \, x \in X\},$$

isto é, $f(X)$ é o conjunto das imagens por f dos elementos de X. Em particular, $Im(f) := \{f(x) | \, x \in A\} = f(A)$.

Seja $f : A \to B$ uma função. Com relação ao conceito de imagem direta valem as seguintes propriedades:

(D_1) $f(\emptyset) = \emptyset$.

(D_2) Se $X \subset Y \subset A$ então $f(X) \subset f(Y)$.

(D_3) $f(X \cup Y) = f(X) \cup f(Y), \forall X, Y \subset A$.

(D_4) $f(X \cap Y) \subset f(X) \cap f(Y), \forall X, Y \subset A$.

Definição 3.32 *Seja $f : A \to B$ uma função. Dado $E \subset B$, chama-se **imagem inversa** de E por f e indica-se por $f^{-1}(E)$, o seguinte subconjunto de A:*

$$f^{-1}(E) = \{x \in A | \, f(x) \in E\},$$

isto é, $f^{-1}(E)$ é o conjunto dos elementos de A que tem imagem em E através de f.

Exemplo 3.33 *Se $A = \{-2,-1,0,1,2,3,4\}$, $B = \{0,1,2,4,6,9,16\}$ e $f : A \to B$ é dada por $f(x) = x^2$, temos:*

$f^{-1}(\{0,1,4,9,16\}) = \{x \in A | \, f(x) \in \{0,1,4,9,16\} = \{-2,-1,0,1,2,3,4\} = A,$

$f^{-1}(\{2,6\}) = \{x \in A | \, f(x) \in \{2,6\} = \emptyset.$

Agora, destacamos as seguintes propriedades sobre imagem inversa de uma função $f : A \to B$:

(I_1) $E \subset F \subset B \Longrightarrow f^{-1}(E) \subset f^{-1}(F)$.

(I_2) $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F), \forall E, F \subset B$.

(I_3) $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F), \forall E, F \subset B$.

(I_4) $f^{-1}(E^c) = [f^{-1}(E)]^c, \forall E \subset B$.

(I_5) $f^{-1}(E - F) = f^{-1}(E) - f^{-1}(F), \forall E, F \subset B$, onde $E - F = E \cap F^c$.

O próximo resultado relaciona imagem direta e imagem inversa de uma função.

Proposição 3.34 *Seja $f : A \to B$ uma função.*

(i) Para todo $X \subset A, X \subset f^{-1}(f(X))$ e, no caso de f ser injetora, então $X = f^{-1}(f(X))$.

(ii) Para todo $E \subset B, f(f^{-1}(E)) \subset E$ e, no caso de f ser sobrejetora, $f(f^{-1}(E)) = E$.

Demonstração: (i) Se $x \in X$ então $f(x) \in f(X)$ e daí, $x \in f^{-1}(f(X))$.

Agora, suponhamos que f seja injetora e tomemos $x \in f^{-1}(f(X))$.

Daí, $f(x) \in f(X)$ e assim existe $x_1 \in X$ tal que $f(x) = f(x_1)$ do que decorre, levando em conta a hipótese de f ser injetora, que $x = x_1$. Logo, $x \in X$.

Portanto, $X = f^{-1}(f(X))$.

(ii) Se $f(x) \in f(f^{-1}(E))$ então $x \in f^{-1}(E)$. Assim, $f(x) \in E$.

Agora, suponhamos que f seja sobrejetora e consideremos $y \in E$. Então, existe $x \in A$ tal que $y = f(x)$. Assim, $x \in f^{-1}(E)$ então, $y = f(x) \in f(f^{-1}(E))$.

Portanto, $f(f^{-1}(E)) = E$.

■

Finalmente, apresentamos o principal resultado desta subseção sobre o número de ends de um grupo quociente G/H, quando H é um subgrupo normal e finito.

Teorema 3.35 *Se H é um subgrupo normal finito de G, então $e(G) = e(G/H)$.*

Demonstração: Consideremos o grupo quociente $G/H = \{Hg | g \in G\}$.

Seja $\pi : G \to G/H$, $\pi(g) = Hg$, o homomorfismo quociente. Temos que:

(i) $\pi(\pi^{-1}(B)) = B$, para todo $B \subset G/H$ pois π é sobrejetor.

(ii) $\pi^{-1}(\pi(A)) = HA$, para todo $A \subset G$. De fato, como $\pi^{-1}(\pi(A)) = \{g \in G | \pi(g) \in \pi(A)\} = \{g \in G | Hg \in \pi(A)\}$ e $\pi(A) = \{\pi(a) | a \in A\} = \{Ha | a \in A\}$. Então, $Hg = Ha$ para algum $a \in A$. Assim, $ga^{-1} = h_2 \in H$ e daí, $g = h_2 a \in Ha$. Logo, $\pi^{-1}(\pi(A)) \subset HA$.

Agora, temos que:

$$y \in HA \Longrightarrow y = ha, h \in H \text{ e } a \in A.$$

Daí,

$$\pi(y) = \pi(ha) = Hha = Ha \in \pi(A) \ (Hh = H \text{ pois } H \text{ é subgrupo de } G \text{ e } h \in H).$$

Portanto, $y \in \pi^{-1}(\pi(A))$.

Logo, $\pi^{-1}(\pi(A)) = HA$.

(iii) $\pi^{-1}(B_1 + B_2) = \pi^{-1}(B_1) + \pi^{-1}(B_2), \forall B_1, B_2 \in G/H$ (onde " + " denota a operação diferença simétrica). De fato,

$\pi^{-1}(B_1 + B_2) = \pi^{-1}[(B_1 \cap B_2^c) \cup (B_1^c \cap B_2)] = \pi^{-1}(B_1 \cap B_2^c) \cup \pi^{-1}(B_1^c \cap B_2) = [\pi^{-1}(B_1) \cap \pi^{-1}(B_2^c)] \cup [\pi^{-1}(B_1^c) \cap \pi^{-1}(B_2)] = [\pi^{-1}(B_1) \cap (\pi^{-1}(B_2))^c] \cup [(\pi^{-1}(B_1))^c \cap \pi^{-1}(B_2)] = \pi^{-1}(B_1) + \pi^{-1}(B_2)$.

(iv) $\pi^{-1}(\pi(g)B) = g\pi^{-1}(B), \forall g \in G$ e $B \subset G/H$. Com efeito,

$x \in \pi^{-1}(\pi(g)B) \Longrightarrow \pi(x) \in \pi(g)B \Longrightarrow \pi(x) = \pi(g)b, b \in B \subset G/H$.

Como π é sobrejetor, existe $a \in G$ tal que $b = \pi(a)$. Assim,

$\pi(x) = \pi(g)b = \pi(g)\pi(a) = \pi(ga) \Longrightarrow Hx = Hga \Longrightarrow gax^{-1} \in H \Longrightarrow gax^{-1} = h_1, h_1 \in H \Longrightarrow ga = h_1 x \in Hx = xH$ (pois H é normal em G). Logo, $\exists h_2 \in H$ de modo que

$$ga = xh_2 \Longrightarrow x = gah_2^{-1}.$$

Como $\pi(ah_2^{-1}) = \pi(a)\pi(h_2^{-1}) = (Ha)(Hh_2^{-1}) = (Ha)(He) = Ha = \pi(a) = b \in B$, segue que $x = gah_2^{-1} \in g\pi^{-1}(B)$. Portanto, $\pi^{-1}(\pi(g)B) \subset g\pi^{-1}(B)$.

Agora, seja $u \in g\pi^{-1}(B)$. Temos que $u = gy$ com $y \in \pi^{-1}(B)$. Daí, $\pi(y) \in B$ e

$$\pi(u) = \pi(gy) = \pi(g)\pi(y) \in \pi(g)B.$$

Logo, $u \in \pi^{-1}(\pi(g)B)$ e portanto $g\pi^{-1}(B) \subset \pi^{-1}(\pi(g)B)$.

(v) $\pi^{-1}(B + \pi(g)B) = \pi^{-1}(B) + g\pi^{-1}(B), \forall B \subset G/H$. De fato, isto segue das duas últimas igualdades pois,

$\pi^{-1}(B + \pi(g)B) = \pi^{-1}(B) + \pi^{-1}(\pi(g)B) = \pi^{-1}(B) + g\pi^{-1}(B)$.

(vi) $B \in Q(G/H) \Longleftrightarrow \pi^{-1}(B) \in Q(G)$. Com efeito,

$(\Longrightarrow)$ $B \in Q(G/H) \Longrightarrow B + \tilde{g}B \in F(G/H), \forall \tilde{g} = \pi(g) \in G/H \Longrightarrow B + \pi(g)B \in F(G/H), \forall g \in G$, isto é, $B + \pi(g)B = \{Hg_1, ..., Hg_k\}$ (finito). Daí, $\pi^{-1}(B) + g\pi^{-1}(B) = \pi^{-1}(B + \pi(g)B) = \pi^{-1}(\{Hg_1, ..., Hg_k\}) = Hg_1 \cup ... \cup Hg_k \in F(G)$ pois H é finito.

$(\Longleftarrow)$ $\pi^{-1}(B) \in Q(G) \Longrightarrow \forall g \in G, \pi^{-1}(B) + g\pi^{-1}(B) = F_g \in F(G) \Longrightarrow \pi^{-1}(B + \pi(g)B) = F_g \in F(G) \Longrightarrow \pi(\pi^{-1}(B + \pi(g)B)) = \pi(F_g) \in F(G/H) \Longrightarrow B + \pi(g)B \in F(G/H), \forall g \in G$ (pois π é sobrejetor) $\Longrightarrow B \in Q(G/H)$.

(vii) $\forall A \in Q(G), \pi^{-1}(\pi(A)) + F(G) = A + F(G)$ e $\pi^{-1}(\pi(A)) \in Q(G)$. De fato, seja $A \in Q(G)$. Como H é finito, suponhamos $H = \{h_1, ..., h_n\}$. Então, $A + \pi^{-1}(\pi(A)) = A + HA = A + (h_1A \cup ... \cup h_nA) \subset (A + h_1A) \cup ... \cup (A + h_nA) \in F(G)$, pois $A \in Q(G)$. Mas, $A + \pi^{-1}(\pi(A)) \in F(G)$ se, e somente se, $A + F(G) = \pi^{-1}(\pi(A)) + F(G)$. Além disso, $A + \pi^{-1}(\pi(A)) = X \in F(G)$ e assim, $\pi^{-1}(\pi(A)) = A + X \in Q(G)$, já que $A \in Q(G)$ e $X \in F(G) \subset Q(G)$.

$(viii)$ $A \in Q(G) \Longrightarrow \pi(A) \in Q(G/H)$. Com efeito, por (vii), se $A \in Q(G)$ então $\pi^{-1}(\pi(A)) \in Q(G)$. Por (vi), $B = \pi(A) \in Q(G/H)$.

Assim, temos bem definida uma aplicação induzida,

$$\tilde{\pi} : \frac{Q(G)}{F(G)} \to \frac{Q(G/H)}{F(G/H)},$$

$\tilde{\pi}(A + F(G)) = \pi(A) + F(G/H)$. Temos que:

• $\tilde{\pi}$ é homomorfismo:

$\forall A_1 + F(G), A_2 + F(G) \in Q(G)/F(G), \forall k \in \mathbb{Z}_2$ ($k = \overline{0}$ ou $k = \overline{1}$),

$\tilde{\pi}(A_1 + F(G) + A_2 + F(G)) = \tilde{\pi}[\pi^{-1}(\pi(A_1)) + F(G) + \pi^{-1}(\pi(A_2)) + F(G)] = \tilde{\pi}[(\pi^{-1}(\pi(A_1)) +$

$\pi^{-1}(\pi(A_2))) + F(G)] = \widetilde{\pi}[\pi^{-1}(\pi(A_1) + \pi(A_2)) + F(G)] = \pi[\pi^{-1}(\pi(A_1) + \pi(A_2))] + F(G/H) = \pi(A_1) + \pi(A_2) + F(G/H) = \pi(A_1) + F(G/H) + \pi(A_2) + F(G/H) = \widetilde{\pi}(A_1 + F(G)) + \widetilde{\pi}(A_2 + F(G))$.

$\widetilde{\pi}(\overline{0} \cdot (A_1 + F(G)) = \widetilde{\pi}(\emptyset + F(G)) = \pi(\emptyset) + F(G/H) = \emptyset + F(G/H) = \overline{0} \cdot (\pi(A_1) + F(G/H)) = \overline{0} \cdot \widetilde{\pi}(A_1 + F(G))$.

$\widetilde{\pi}(\overline{1} \cdot (A_1 + F(G)) = \widetilde{\pi}(A_1 + F(G)) = \pi(A_1) + F(G/H) = \overline{1} \cdot (\pi(A_1) + F(G/H)) = \overline{1} \cdot \widetilde{\pi}(A_1 + F(G))$.

• $\widetilde{\pi}$ é injetora:

$\forall A + F(G) \in Q(G)/F(G)$,

$\widetilde{\pi}(A + F(G)) = \overline{\emptyset} \implies \pi(A) + F(G/H) = \emptyset + F(G/H) \implies \pi(A) \in F(G/H) \implies \pi(A) = \{Hg_1, Hg_2, ..., Hg_k\} \implies \pi^{-1}(\pi(A)) = Hg_1 \cup Hg_2 \cup ... \cup Hg_k \in F(G)$ (pois H é finito). Logo, por (vii), $A + F(G) = \pi^{-1}(\pi(A)) + F(G) = \emptyset + F(G) = \overline{\emptyset}$.

• $\widetilde{\pi}$ é sobrejetora:

Sejam $B \in Q(G/H)$ e $B + F(G/H) \in Q(G/H)/F(G/H)$. Então, $\pi^{-1}(B) \in Q(G)$ e $\pi^{-1}(B) + F(G) \in Q(G)/F(G)$ e assim, $\widetilde{\pi}(\pi^{-1}(B) + F(G)) = \pi(\pi^{-1}(B)) + F(G/H) = B + F(G/H)$.

Assim, $Q(G)/F(G) \cong Q(G/H)/F(G/H)$.

Portanto, $e(G) = dim Q(G)/F(G) = dim Q(G/H)/F(G/H) = e(G/H)$.

■

Exemplo 3.36 *Como* $S_3 \times \{0\} \lhd S_3 \times \mathbb{R}$ *(*$S_3 \times \{0\}$ *finito) e* $(S_3 \times \mathbb{R})/(S_3 \times \{0\}) \cong \mathbb{R}$ *temos, pelo teorema anterior, que* $e(S_3 \times \mathbb{R}) = e((S_3 \times \mathbb{R})/(S_3 \times \{0\})) = e(\mathbb{R}) = 1$.

Conclusão

Neste trabalho introduzimos a Teoria de Módulos e estudamos Ends de Grupos.

A Teoria de Módulos é fundamental em Topologia Algébrica e tem uma vasta gama de aplicações em diversas outras áreas da matemática, como exemplos citamos a Álgebra e a Teoria dos Números, além dessa teoria oferecer ferramentas para a compreensão e solução de problemas em ciência da computação e física teórica.

A teoria de ends de grupos, de certo modo, nos fornece uma maneira de medir a "infinitude" de um grupo, em termos da sua estrutura de subgrupos. Esta teoria tem sua relevância em algumas áreas da Matemática, por exemplo, na Álgebra e na Topologia Algébrica. Na Álgebra, a teoria de ends está relacionada com decomposição de grupos e classificação de grupos e na Topologia Algébrica, está relacionada com a teoria de cohomologia de grupos. Além disso, esta teoria também é importante ao se estudar a classificação de variedades.

Referências Bibliográficas

[1] CIOCA, D. M. "**Cohomologia e Ends de Grupos**". Dissertação de Mestrado. IBILCE/UNESP, 1997.

[2] FREUDENTHAL, H. ***Uber die Enden diskreter Raume und Gruppen***. Comment. Math. Helv. 17, p.1-38, 1944.

[3] GARCIA, Arnaldo e LEQUAIN, Yves. ***Elementos de álgebra***. 1ª ed. Projeto Euclides, 2014.

[4] HOPF, H. ***Enden offener raume and unendlicher diskontinuierliche gruppen***. Comm. Math. Helv. 16, p.81-100, 1943.

[5] LIMA, E. L. ***Álgebra Linear***. 3ª ed. Coleção Matemática Universitária. Rio de Janeiro: SBM, 2014.

[6] MILIES, F. C. P. ***Anéis e Módulos***. Publicações do Instituto de Matemática e Estatística da USP. São Paulo, 1972.

[7] MUNKRES, J. R. ***Topology***. 2ª ed. Upper Saddle River: Prentice Hall, Inc., 2000.

[8] SANTOS, A.P. "**Cohomologia de Grupos e Invariantes Algébricos**". Dissertação de Mestrado. IBILCE/UNESP, 2006.

[9] SCOTT, G. P. e WALL, C. T. C. ***Topological Methods in Group Theory***. London Math. Soc. Lect. Notes Series 36, Homological Group Theory, 167-174, 1972.

[10] SPECKER, F. ***Endenverbande von Raume und Gruppen***. Math. Annalen 122, p.167-174, 1950.