UNIVERSIDADE FEDERAL DO PARANÁ

DYCKSON TERNOSKI

RELATÓRIO FINAL

(Período no qual esteve vinculado ao Programa: 09/2020 a 02/2021)

PROGRAMA DE IC	**MODALIDADE**
(X) PIBIC	(X) CNPq
( ) PIBIC AF	( ) UFPR TN
( ) PIBIC EM	( ) Fundação Araucária
( ) PIBITI	( ) Voluntária

CONSTRUÇÕES PARA BIÁLGEBRAS E ÁLGEBRAS DE HOPF

Relatório apresentado à Coordenação de Iniciação Científica e Tecnológica da Universidade Federal do Paraná como requisito parcial da conclusão das atividades de Iniciação Científica ou Iniciação em desenvolvimento tecnológico e Inovação - Edital 2020.
Orientador: Prof. Marcelo Muniz Silva Alves.
Título do Projeto: Ações e Representações Parciais de Grupos e de Álgebras de Hopf.

CURITIBA

2021

1 Título: Construções para biálgebras e álgebras de Hopf.

2 Resumo

A proposta deste projeto foi realizar um primeiro estudo sobre álgebras de Hopf com foco em alguns exemplos fundamentais da área. O objetivo específico deste plano de trabalho foi estudar a construção da biálgebra livre sobre uma coálgebra e usar esta construção para construir exemplos fundamentais de álgebras de Hopf, como as álgebras de Taft. O objetivo geral foi estudar fundamentos da teoria de álgebras de Hopf. Neste relatório apresentamos o que foi realizado até fevereiro de 2021: A construção do corpo de frações de um domínio, a construção do anel de polinômios em uma variável com coeficientes em um anel dado, o corpo primo de um corpo, o estudo da soma direta de espaços vetoriais e resultados sobre funcionais lineares.

3 Introdução

O projeto foi dividido em duas partes, correspondendo aproximadamente ao cronograma para o segundo semestre de 2020 e ao primeiro semestre de 2021.

Na primeira parte planejamos estudar propriedades de anéis comutativos, corpos, anel de polinômios e tópicos de Álgebra Linear Avançada: funcionais lineares, soma direta e produto direto, quocientes e teoremas de isomorfismos, produtos tensoriais.

Na segunda parte do projeto planejamos fazer um estudo de fundamentos de Álgebras de Hopf, terminando com a construção das álgebras de Taft, que é uma família importante de álgebras de Hopf. Os tópicos desta parte são: elementos da teoria de coálgebras, biálgebras e álgebras de Hopf; álgebras de Hopf associadas a grupos; a biálgebra livre sobre uma coálgebra; estrutura de álgebra de Hopf na álgebra tensorial e a construção das álgebras de Taft.

4 Revisão da Literatura

O livro que norteou o estudo de tópicos envolvendo anéis, corpos e polinômios foi ”A First Course in Abstract Algebra”, de Joseph J. Rotman, contendo definições e resultados importantes para as partes posteriores do projeto.

As referências para Álgebra Linear Avançada são os livros “Advanced Linear Algebra”, de Steven Roman, que trazem conceitos e resultados fundamentais sobre álgebra linear como soma direta e produto direto de espaços e o espaço dos funcionais lineares.

A construção do produto tensorial encontra-se em “Multilinear Algebra”, de Werner Greub. Também separamos o livro “Algebres et Modules”, de I. Assem, que aborda estes mesmos resultados de um ponto de vista mais abstrato.

As referências para o tema de Álgebras de Hopf são “Hopf Algebras: an introduction”, de Dascalescu, Nastasescu e Raianu, “Hopf Algebras”, de D. E. Radford, e “Hopf algebras and their actions on rings”, de Susan Montgomery. A construção da biálgebra livre e das álgebras de Taft está feita com detalhes no livro de Radford.

5 Materiais e Métodos

O projeto foi desenvolvido por meio de seminários com o orientador na plataforma Microsoft Teams.

6 Resultados e discussão

Nesta seção discorreremos sobre os pontos que foram estudados neste projeto.

6.1 Anel de Polinômios

Tomando conceitos de anéis e corpos como pré-requisito, comecemos com o estudo do Anel de Polinômios. Primeiramente, uma noção intuitiva:

Informalmente, um polinômio é uma ”expressão” da forma

$$s_0 + s_1x + s_2x^2 + ... + s_nx^n \tag{1}$$

com $s_i \in R \, \forall i \in \{0, ..., n\}$, sendo R um anel comutativo.

Vejamos como definir isso mais formalmente:

Definição 6.1. Sendo R um anel comutativo, uma *sequência* em R é uma função $\sigma : \mathbb{N} \to R$, e podemos escrever a expressão (1) como a sequência $(s_0, s_1, ..., s_n, 0, 0, ...)$ de seus coeficientes.

Definição 6.2. Uma sequência $\sigma = (s_0, s_1, ..., s_i, ...)$ em um anel comutativo R é chamado de *polinômio* se existe um inteiro $n \geq 0$ tal que $s_i = 0, \forall i > n$. Dessa forma, denotamos um polinômio por $\sigma = (s_0, s_1, ..., s_n, 0, 0, ...)$.

Observação 6.1. O polinômio $\sigma = (0, 0, 0, ...)$ é chamado de polinômio nulo e denotado por $\sigma = 0$.

Notação 6.1. Se $\sigma \neq 0$ então seu **grau** n é o maior índice tal que $s_n \neq 0$. O termo s_n é chamado de coeficiente principal. Denotamos o grau de σ por $deg(\sigma) = n$.

Notação 6.2. Sendo R um anel comutativo, o conjunto de todos os polinômios com coeficientes em R é denotado por $R[x]$ e chamamo-lo de *Anel de polinômios com coeficientes em* R.

Observação 6.2. O anel $R[x]$ é fechado para soma e multiplicação, operações definidas como abaixo, para todos $\sigma = (s_0, s_1, ...s_n, 0, 0, ...), \tau = (t_0, t_1, ..., t_m, 0, 0, ...) \in R[x]$:

$\sigma+\tau \doteq (s_0+t_0, s_1+t_1, ..., s_k+t_k, ...)$ e $\sigma\cdot\tau \doteq (a_0, a_1, ..., a_k, ...)$ em que $a_k = \sum_{i=0}^{k} s_it_{k-i}, \; \forall \, k \in \mathbb{N}$.

Também, note que pelo modo que definimos a multiplicação, podemos afirmar que se R é um anel comutativo, então $R[x]$ é um anel comutativo.

Finalmente, a partir da definição formal de polinômio, podemos agora enunciar resultados importantes com relação ao anel de polinômios.

Proposição 6.1: Seja R um anel comutativo e considere $\sigma, \tau \in R[x]$ polinômios diferentes do nulo. Então:

(i) $\sigma\tau = 0$ ou $deg(\sigma\tau) \leq deg(\sigma) + deg(\tau)$

(ii) Se R for um domínio de integridade, então $\sigma\tau \neq 0$ e $deg(\sigma\tau) = deg(\sigma) + deg(\tau)$

Demonstração (i): Seja $\sigma = (s_0, s_1, ...)$ tal que $deg(\sigma) = m$ e $\tau = (t_0, t_1, ...)$ com $deg(\tau) = n$, e considere $\sigma\tau = (a_0, a_1, ...)$. Provaremos que $a_k = 0$ para todo $k > m + n$.

Pela definição da multiplicação em $R[x]$, temos que $a_k = \sum_{i=0}^{k} s_i t_{k-i} = \sum_{i+j=k} s_i t_j$

Logo, se $i \leq m \Rightarrow j = k - i \geq k - m > n \Rightarrow t_j = 0$. Complementarmente, se $i > m \Rightarrow s_i = 0$.

Dessa forma, teremos que $s_i t_j = 0 \ \forall i, j$ tais que $i + j > m + n$, e portanto, $a_k = \sum_{i+j=k} s_i t_j = 0, \ \forall k > m + n.$

Por este fato está demonstrado que $deg(\sigma\tau) \leq deg(\sigma) + deg(\tau)$.

□

Demonstração (ii): Pela definição, $a_{m+n} = \sum_{i+j=k} s_i t_j$. Então:

$$a_{m+n} = \cancelto{0}{s_0 t_{m+n}} + ... + \cancelto{0}{s_{m-1} t_{n+1}} + s_m t_n + \cancelto{0}{s_{n+1} t_{n-1}} + ... + \cancelto{0}{s_{m+n} t_0}$$

Como visto, se $i < m$, então $m - i > 0 \Rightarrow j = m - i + n > n$, e por isso $t_j = 0$. Por outro lado, se $i > m \Rightarrow s_i = 0$. Até então temos que $a_{m+n} = s_m t_n$.

Entretanto, como R é um domínio de integridade, $s_m t_n = 0$ implica $s_m = 0$ ou $t_n = 0$.

Pela contrapositiva, temos que se $s_m \neq 0$ e $t_n \neq 0 \Rightarrow s_m t_n \neq 0$. Como por hipótese temos σ e τ não nulos com graus m e n respectivamente, então vale a afirmação e temos $s_m t_n \neq 0$.

Também, vimos em (ii) que $a_k = 0 \ \forall \ k > m + n$. Dessa forma, $deg(\sigma\tau) = m + n = deg(\sigma) + deg(\tau)$.

□

Definiremos agora um conceito importante para o anel de polinômios: a ”indeterminação”, comumente conhecida como ”x”.

Definição 6.3: A *indeterminação* é representada pelo elemento $x = (0, 1, 0, 0, ...) \in R[x]$.

Proposição 6.2: Se $\sigma = (s_0, s_1, ..., s_n, 0, 0, ...)$, então $\sigma = s_0 + s_1 x + s_2 x^2 + ... + s_n x^n$.

Para a demonstração de tal resultado basta realizar as multiplicações, de forma que cada $s_i \in R$ é identificado com o polinômio $(s_i, 0, 0, ...)$.

Notação 6.3: Usaremos $f(x) = s_0+s_1x+s_2x^2+...+s_nx^n$ em vez de $\sigma = (s_0, s_1, ...s_n, 0, 0, ...)$ para representar polinômios.

Corolário 6.1: Polinômios $f(x) = s_0 + s_1x + ... + s_nx^n$ e $g(x) = t_0 + t_1x + ... + t_mx^m$ são iguais se, e somente se, $s_i = t_i \ \forall i \in \mathbb{N}$.

Agora podemos descrever o real uso de x como uma variável. Sendo R um anel comutativo, cada polinômio $f(x) = s_0 + s_1x + s_2x^2 + ... + s_nx^n$ define uma função polinomial $f^\phi : R \to R$ tal que $r \in R \Rightarrow f^\phi(r) = s_0 + s_1r + s_2r^2 + ... + s_nr^n \in R$. Note que a notação é $f^\phi(r)$ em vez de $f(r)$, pois polinômios e funções polinomiais são objetos matemáticos distintos.

6.2 Corpo de frações

Antes de tratar propriamente do caso para polinômios, vejamos as definições para um anel qualquer.

Definição 6.4: Seja R um anel comutativo. O *corpo de frações do anel* R é um corpo K que contém R como um subanel e é construído de tal forma que cada $k \in K$ tenha uma expressão $k = ab^{-1}$, com $a, b \in R$ e $b \neq 0$. Tal corpo é denotado por $K = Frac(R)$.

Exemplo 6.1: $\mathbb{Q}$ é o corpo de frações do anel comutativo $\mathbb{Z}$, já que:

- $\mathbb{Z}$ é subanel de $\mathbb{Q}$
- $\forall q \in \mathbb{Q}, q = \frac{a}{b}$, com $a, b \in \mathbb{Z}$ e $b \neq 0$.

Portanto, $\mathbb{Q} = Frac(\mathbb{Z})$.

Definição 6.5: Um *subcorpo* de um corpo K é um subanel de K que também seja um corpo.

Exemplo 6.2:

- $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$
- $\mathbb{Z}$ não é subcorpo de $\mathbb{Q}$, visto que $\mathbb{Z}$ é apenas subanel de $\mathbb{Q}$, mas não um corpo. De fato, os únicos elementos não nulos com inverso em $\mathbb{Z}$ são -1 e 1.

Proposição 6.3: Seja K um corpo.

(i) Um subconjunto k de K é um corpo se, e somente se, é um subanel que é fechado sob inversos; isto é, se $a \in k$ e $a \neq 0$, então $a^{-1} \in k$.

(ii) Sendo I um conjunto de índices, se $\{F_i : i \in I\}$ é qualquer família de subcorpos de F, podendo também ser um conjunto infinito, então $k = \bigcap_{i \in F} F_i$ é um subcorpo de K.

Demonstração (i): Trivial ao utilizar definição de corpo e subcorpo para ambos os lados da implicação.

Demonstração (ii): Como toda interseção de subanéis é um subanel, então basta provar que esta interseção de corpos é também um corpo.

Considere $a \in k$ um elemento não nulo. Se $a \in k$, então por definição de interseção de subconjuntos, $a \in F_i, \forall i \in I$. Como cada F_i é um subcorpo de K, então $a^{-1} \in F_i\ \forall i \in I$, e portanto, $a^{-1} \in \bigcap\limits_{i \in F} F_i = k$. Desse modo, conclui-se que k é um subcorpo de K.

$\square$

Definição 6.6: Seja R um anel. O corpo de frações de $R[x]$, denotado por $R(x)$, é chamado de *corpo de funções racionais sobre* R, e seus elementos são da forma $\frac{f(x)}{g(x)}$, onde $f(x), g(x) \in R[x]$ e $g(x) \neq 0$.

6.3 Corpo primo

Definição 6.7: Sendo K um corpo, o subconjunto k que é interseção de todos os subcorpos de K é chamado de *corpo primo*.

Segue da Proposição 6.3 que o corpo primo de um corpo K é efetivamente um subcorpo de K, e portanto é um corpo.

Exemplo 6.3: Seja K um corpo com unidade ϵ, e seja R o subanel

$$R = \{n\epsilon : n \in \mathbb{Z}\}$$

(i) Prove que se F é um subcorpo de K, então $R \subseteq F$.

Demonstração: Como F é um subcorpo de K, então F é um corpo, mas também um subanel de K. Sabemos que

$$F \text{ é subanel de } K \Leftrightarrow \begin{cases} \epsilon \in F \\ x, y \in F \Rightarrow x + y \in F \\ x, y \in F \Rightarrow xy \in F \\ x \in F \Rightarrow -x \in F \end{cases}$$

Assim, sabemos que $\epsilon \in F \Rightarrow \epsilon + \epsilon = 2\epsilon \in F$, e por indução, $n\epsilon \in F,\ \forall n \in \mathbb{N}$.

Também, utilizando a quarta propriedade listada acima, vemos que $-n\epsilon \in F\ \forall n \in \mathbb{N}$, isto é, $n\epsilon \in F,\ \forall n \in \mathbb{Z}^*$. Finalmente, como $\epsilon \in F$ e $-\epsilon \in F \Rightarrow \epsilon + (-\epsilon) = 0\epsilon \in F$, e portanto, $n\epsilon \in F,\ \forall n \in \mathbb{Z}$.

Dessa forma, concluímos que $R \subseteq F$, já que todo elemento de R está em F.

$\square$

(ii) Mostre que um subcorpo F de K é o corpo primo se, e somente se, ele é o menor subcorpo de K contendo R, isto é, não existe outro subcorpo F' com $R \subseteq F' \subseteq F$.

Demonstração: ($\Rightarrow$) Por (i), sabemos que todo subcorpo de K contém R. Logo, basta provar que o corpo primo é o menor dos subcorpos. Seja $S = \{F_i : i \in I\}$ o conjunto de todos os subcorpos de K. Como F é o corpo primo de K, então $F = \bigcap_{i \in I} F_i$. Por definição de interseção de conjuntos, temos $F \subseteq F_i\ \forall F_i \in S$, e segue que F é o menor subcorpo de K contendo R.

($\Leftarrow$) Suponha que F não é o corpo primo de K. Como todo corpo tem um corpo primo, então existe um subcorpo U de K que é o corpo primo de K.

Como U é o corpo primo de K e F é um subcorpo de K, então $U \subseteq F$. Se F não é o corpo primo, então teremos $U \neq F$ com $R \subseteq U \subseteq F$, e portanto, uma contradição à hipótese.

Assim, conclui-se que F é o corpo primo de K.

$\square$

(iii) Demonstre que se R é um subcorpo de K, então R é o corpo primo de K.

Demonstração: Segue diretamente do fato de que R é o menor subcorpo que contém ele mesmo, então pela volta de (ii) concluimos que R é o corpo primo de K.

$\square$

Exemplo 6.4: Seja p um número primo. Prove que o corpo de funções racionais $\mathbb{Z}_p(x)$ é um corpo infinito cujo corpo primo é $\mathbb{Z}_p$.

Demonstração: Como $\mathbb{Z}_p[x]$ é um conjunto infinito e é um subanel de $\mathbb{Z}_p(x)$, segue que $\mathbb{Z}_p(x)$ é infinito. Também, é evidente que $\mathbb{Z}_p(x)$ é um corpo.

Quanto ao corpo primo, primeiramente recorde que $\mathbb{Z}_p$ é corpo se, e somente se, p é primo. Por hipótese, temos p primo, e consequentemente, $\mathbb{Z}_p$ um corpo. Mais do que isso: $\mathbb{Z}_p$ é um subanel de $\mathbb{Z}_p(x)$, concluindo assim $\mathbb{Z}_p$ como um subcorpo de $\mathbb{Z}_p(x)$.

Agora perceba que podemos aplicar o item (iii) do Exemplo 6.3: fazendo $K = \mathbb{Z}_p(x)$, que tem por unidade $\epsilon = \overline{1}$ e $R = \{n \cdot \overline{1} : n \in \mathbb{Z}\} = \mathbb{Z}_p$, concluimos que $\mathbb{Z}_p(x)$ é o corpo primo de $\mathbb{Z}_p(x)$.

Observação 6.3: O exemplo anterior é interessante por observamos um caso concreto em que o corpo primo é $\mathbb{Z}_p$. Na realidade, podemos ir além: se K é um corpo, então o corpo primo de K é isomorfo a $\mathbb{Z}_p$, caso seja finito, e isomorfo a $\mathbb{Q}$, caso seja infinito. Isso é o que veremos no último resultado a seguir.

Proposição 6.4: O corpo primo de um corpo K é isomorfo a $\mathbb{Z}_p$, caso seja finito, e isomorfo a $\mathbb{Q}$, caso seja infinito.

Demonstração: Seja F o corpo primo de K e seja ϵ a unidade de K. Pode-se verificar que a aplicação

$$\varphi : \mathbb{Z} \to K, \quad n \mapsto n\epsilon,$$

é um homomorfismo de anéis. Sabemos que φ será injetora se e somente se seu núcleo é nulo, e que seu núcleo I é um ideal de $\mathbb{Z}$. Então temos dois casos:

(i) $I \neq 0$.

Neste caso, como $\mathbb{Z}$ é um domínio de ideais principais podemos escrever $I = n\mathbb{Z}$, onde $n > 0$ é o menor elemento positivo de I. Se n for composto, isto é, $n = kl$ com

$1 < k < n$ e $1 < l < n$ então

$$0 = \varphi(n) = \varphi(kl) = \varphi(k)\varphi(l) = (k\epsilon)(l\epsilon)$$

e como K é um corpo temos que $(k\epsilon)(l\epsilon) = \varphi(k) = 0$ ou $(l\epsilon) = \varphi(l) = 0$. Isso contradiz a escolha de n, pois n é o menor inteiro positivo em I. Assim n é um número primo, digamo $n = p$. Pelo Teorema dos Isomorfismos segue que

$$F = Im(\varphi) \simeq \frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{Z}_p.$$

(ii) $I = 0$.

A aplicação φ será injetora, e sua imagem é o subanel

$$R = \{n\epsilon; n \in \mathbb{Z}\}.$$

Sabemos do Exemplo 6.3 que $R \subset F$ (onde F é o corpo primo de K). Como K é um corpo e $n\epsilon \neq 0$ se $m \neq 0$, o corpo K contém o conjunto

$$Q = \left\{\frac{m\epsilon}{n\epsilon};\ m, n \in \mathbb{Z},\ n \neq 0\right\}.$$

Este subconjunto de K está contido em todo subcorpo L de K. De fato, sabemos que cada $n\epsilon \in L$, e como L é corpo segue que se $n \neq 0$ então $1/n\epsilon \in L$, e também que $m\epsilon/n\epsilon = m\epsilon(1/n\epsilon) \in L$ para cada $m, n \in Z$ com $n \neq 0$. Pode-se verificar que Q é um corpo, e com isso segue que Q é o corpo primo de K pois está em cada subcorpo de K.

Finalmente, o homomorfismo $\varphi : \mathbb{Z} \to K$ pode ser estendida a um homomorfismo

$$\Phi : \mathbb{Q} \to K,\ \ m/n \mapsto \varphi(m)/\varphi(n)$$

que é um isomorfismo do corpo dos racionais $\mathbb{Q}$ com o corpo Q.

$\square$

6.4 Soma direta

Começaremos a parte de Álgebra Avançada do projeto com algumas definições:

Definição 6.8: Seja V um K-espaço vetorial e sejam W_1, W_2 dois subespaços de V.

1. Dizemos que a soma $W_1 + W_2$ é *direta* se $W_1 \cap W_2 = \{0_V\}$ e, neste caso, escrevemos $W_1 \oplus W_2$.

2. Dizemos que V é *soma direta* de W_1 e W_2 se $V = W_1 \oplus W_2$.

Definição 6.9: Alternativamente para um número arbitrário de subespaços, sejam V um K-espaço vetorial e $W_1, ..., W_n$ subespaços de V. Se

$$W_i \cap (W_1 + ... + W_{i-1} + W_{i+1} + ... + W_n) = \{0_V\}$$

para cada $i = 1, ..., n$, então a soma $W_1 + ... + W_n$ é chamada de *soma direta* de $W_1, ..., W_n$ e será denotada por $W_1 \oplus ... \oplus W_n$. Também, diremos que V é *soma direta* de tais subespaços se $V = W_1 \oplus ... \oplus W_n$.

Exemplo 6.5: $\mathbb{R}^2 = \langle (1,0) \rangle \oplus \langle (1,1) \rangle$

Demonstração: Vejamos que $\mathbb{R}^2$ é a soma direta de $\langle (1,0) \rangle$ e $\langle (1,1) \rangle$ verificando os itens (i) e (ii) acima.

(i) Vejamos que $\langle (1,0) \rangle \cap \langle (1,1) \rangle = \{0_{\mathbb{R}^2}\}$

Seja $(a,b) \in \langle (1,0) \rangle \cap \langle (1,1) \rangle$ com $a, b \in \mathbb{R}$.

$$\begin{cases} (a,b) = \alpha(1,0), \alpha \in \mathbb{R} \\ (a,b) = \beta(1,1), \beta \in \mathbb{R} \end{cases} \Rightarrow \begin{cases} a = \alpha = \beta \\ b = 0 = \beta \end{cases} \Rightarrow \begin{cases} a = b = 0 \end{cases} \Rightarrow \langle (1,0) \rangle \cap \langle (1,1) \rangle = \{0_{\mathbb{R}^2}\}$$

(ii) Vejamos que $\mathbb{R}^2 = \langle (1,0) \rangle + \langle (1,1) \rangle$

$$(a,b) \in \mathbb{R}^2 \Rightarrow (a,b) = (a-b)(1,0) + b(1,1)$$

Como vale (i) e (ii), concluímos que $\mathbb{R}^2$ é a soma direta de $\langle (1,0) \rangle$ e $\langle (1,1) \rangle$.

$\square$

Proposição 6.5: Seja $V = W_1 + W_2$ um K-espaço vetorial. Então a soma é direta se e somente se cada elemento $v \in V$ se escreve de maneira única como $v = x_1 + x_2$ com $x_i \in W_i$ para $i = 1, 2$.

Demonstração: $(\Rightarrow)$ Como V é soma direta de W_1 e W_2, então pela definição já temos que todo elemento $v \in V$ tem decomposição em $W_1 + W_2$, isto é $v = x_1 + x_2$. Basta apenas mostrar que x_1 e x_2 são únicos.

Suponha que existam $y_1 \in W_1$ e $y_2 \in W_2$ tais que $v = x_1 + x_2 = y_1 + y_2$.

$$x_1 + x_2 = y_1 + y_2 \Rightarrow \underbrace{x_1 + (-y_1)}_{\in W_1} = \underbrace{y_2 + (-x_2)}_{\in W_2} \Rightarrow x_1 + (-y_1) = y_2 + (-x_2) \in W_1 \cap W_2$$

Mas note que como V é soma direta de W_1 e W_2, então $W_1 \cap W_2 = \{0_V\}$. Logo:

$$x_1 + (-y_1) = y_2 + (-x_2) = 0_V \Rightarrow x_1 = y_1, x_2 = y_2$$

Portanto, segue a unicidade e conclui-se a prova.

$(\Leftarrow)$ Temos a decomposição de todo elemento de V como hipótese, então basta mostrar que $W_1 \cap W_2 = \{0_V\}$. Para isso, considere $v \in W_1 \cap W_2$ com $v = x_1 + x_2$. De fato:

$$v = x_1 + x_2 = (x_1 + v) + (x_2 - v)$$

Utilizando então a unicidade da decomposição, segue que $x_1 = x_1 + v$ e $x_2 = x_2 - v$, cuja única solução para ambas equações simultaneamente é $v = 0_V$. Como $v \in W_1 \cap W_2$

foi tomado arbitrariamente, então $W_1 \cap W_2 = \{0_V\}$. Desse modo, conclui-se que V é soma direta de W_1 e W_2, como gostaríamos.

$\square$

6.5 Soma direta externa, Produto direto e Suporte

Veremos nas definições a seguir métodos para construir novos espaços vetoriais a partir daqueles à nossa disposição. Tais espaços vetoriais gerados são necessários para definições mais avançadas, como por exemplo a de Produto Tensorial.

Definição 6.10: Sejam $V_1, ..., V_n$ K-espaços vetoriais. A *Soma direta externa* de $V_1, ..., V_n$ é definida por

$$V = V_1 \boxplus ... \boxplus V_n$$

em que o espaço vetorial V tem como elementos as n-uplas ordenadas pelos espaços vetoriais utilizados em sua construção, isto é:

$$V = \{(v_1, ..., v_n) \mid v_i \in V_i, i = 1, ..., n\}$$

As operações soma e multiplicação por escalar de V são definidas como abaixo, respectivamente:

$$(u_1, ..., u_n) + (v_1, ...v_n) = (u_1 + v_1, ..., u_n + v_n)$$

$$r(v_1, ..., v_n) = (rv_1, ..., rv_n)$$

Definição 6.11: Seja I um conjunto de índices e $\mathcal{F} = \{V_i, i \in I\}$ uma família de K-espaços vetoriais. Definimos:

1. O *Produto direto de* $\mathcal{F}$ como sendo o conjunto

$$\prod_{i \in I} V_i = \left\{ f : I \to \bigcup_{i \in I} V_i \mid f(i) \in V_i \right\}$$

2. O *Suporte* de uma função $f : I \to \bigcup_{i \in I} V_i$ como sendo

$$supp(f) = \{i \in I \mid f(i) \neq 0\}$$

3. A *Soma direta externa de* $\mathcal{F}$ como sendo o conjunto

$$\bigoplus_{i \in I}^{\text{ext}} V_i = \left\{ f \in \prod_{i \in I} V_i \mid supp(f) < \infty \right\}$$

6.6 Funcional Linear e Espaço Dual

Definição 6.12: Seja V um K-espaço vetorial. Uma transformação linear $T : V \to K$ é chamada de *funcional linear*, e o conjunto de todos os funcionais lineares, denotado por $\mathcal{L}(V, K) \doteq V^*$ é chamado de *espaço dual*.

Exemplo 6.6: Dado $\alpha \in K$, temos que

$$\begin{aligned} T_\alpha : K[x] &\to K \\ p(x) &\mapsto p(\alpha) \end{aligned}$$

é um funcional linear, conhecido como ”avaliação em α”.

Exemplo 6.7: Seja $\mathcal{C}[a,b]$ o espaço vetorial de todas as funções contínuas em $[a,b] \subseteq \mathbb{R}$. A aplicação $T : \mathcal{C}[a,b] \to \mathbb{R}$ definida por

$$T(f(x)) = \int_a^b f(x)\, dx$$

é um funcional linear.

Observação 6.4: Note que se V tem dimensão finita, então o espaço dual V^* terá a mesma dimensão de V, já que

$$dim_K V^* = dim_K \mathcal{L}(V,K) = dim_K V \cdot \underbrace{dim_K K}_{1} = dim_K V$$

Relembrando que dois espaços vetoriais de dimensão finita são isomorfos se e somente se têm a mesma dimensão, podemos concluir que $V \simeq V^*$.

Definição 6.13: Seja $\mathcal{B} = \{v_1, ..., v_n\}$ uma base do K-espaço vetorial V. Definimos a *base dual de* $\mathcal{B}$ como sendo $\mathcal{B}^* = \{v_1^*, ..., v_n^*\}$, onde $v_i^* : V \to K$ é o funcional linear definido por

$$v_i^*(v_j) = \delta_{i,j} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

Proposição 6.6: $\mathcal{B}^*$ é uma base de V^*.

Demonstração: É óbvio que $\mathcal{B}^* \subset V^*$, e como $dimV^* = dimV = n$ e $\mathcal{B}^*$ possui n elementos, então para provar que $\mathcal{B}^*$ é base de V^* basta provarmos que $\mathcal{B}^*$ é um conjunto linearmente independente ou que $\mathcal{B}^*$ é um gerador de V^*. Provemos então que $\mathcal{B}^*$ é L.I.:

Sejam $\alpha_1, ..., \alpha_n \in K$ tais que

$$\alpha_1 v_1^* + ... + \alpha_n v_n^* = 0_{V^*} = T,$$

em que T é o funcional linear nulo.

Como $T(v) = 0_K$ para todo $v \in V$, então em particular $T(v_j) = 0_K, \forall j = 1, ..., n$. Logo:

$$0_K = T(v_j) = \left(\sum_{i=1}^n \alpha_i v_i^*\right)(v_j) = \alpha_1 \underbrace{v_1^*(v_j)}_{\delta_{1,j} = 0} + ... + \alpha_j \underbrace{v_j^*(v_j)}_{\delta_{j,j} = 1} + ... + \alpha_n \underbrace{v_n^*(v_j)}_{\delta_{n,j} = 0} = \alpha_j$$

Portanto, $\alpha_j = 0_K, \forall j = 1, ..., n$.

Logo, $\mathcal{B}^*$ é um conjunto L.I., e consequentemente, uma base de V^*. □

7 Referências

[1] ROTMAN, JOSEPH J. **A First Couse in Abstract Algebra**. Ed. Pearson, 2005. 3a Edição.

[2] ASSEM, I. **Algebres et Modules**. Ed. Masson, 1997.

[3] DĂSCĂLESCU, Sorin; NĂSTĂSESCU, Constantin; RAIANU, Şerban. **Hopf Algebras:** An Introduction. New York: Marcel Dekker, Inc., 2001.

[4] GREUB, WERNER. **Multilinear Algebra**. Springer-Verlag New York, 1978. 2a Edição.

[5] RADFORD, DAVID E.. **Hopf Algebras**.Ilinois, Chicago: World Scientific Publishing Co. Pte. Ltd., 2012.

[6] ROMAN, STEVEN. **Advanced Linear Algebra**. Springer-Verlag New York, 2008. 3a Edição.

[7] MONTGOMERY, SUSAN. **Hopf algebras and their actions on rings**. Amer. Math. Society, 1993.

Curitiba, 17 de fevereiro de 2020

Dyckson T.

Dyckson Ternoski