ALEX SANDRO FARIA MANUEL

IDENTIDADES POLINOMIAIS DA ÁLGEBRA DE GRASSMANN EM CARACTERÍSTICA POSITIVA

CAMPINAS
2014

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística
e Computação Científica

ALEX SANDRO FARIA MANUEL

IDENTIDADES POLINOMIAIS DA ÁLGEBRA DE GRASSMANN EM CARACTERÍSTICA POSITIVA

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática.

Orientador: LUCIO CENTRONE

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELO ALUNO ALEX SANDRO FARIA MANUEL, E ORIENTADA PELO PROF. DR. LUCIO CENTRONE.

Assinatura do Orientador

Lucio Centrone

CAMPINAS
2014

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Maria Fabiana Bezerra Muller - CRB 8/6162

M319i

Manuel, Alex Sandro Faria, 1975-
Identidades polinomiais da álgebra de Grassmann em característica positiva / Alex Sandro Faria Manuel. – Campinas, SP : [s.n.], 2014.

Orientador: Lucio Centrone.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Álgebra. 2. Grassmann, Álgebra de. 3. Identidade polinomial. I. Centrone, Lucio,1983-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Polymomial identities of the Grassmann algebra in positive characteristic
Palavras-chave em inglês:
Algebra
Grassmann algebra
Polynomial identity
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Lucio Centrone [Orientador]
Irina Sviridova
Thiago Castilho de Mello
Data de defesa: 06-10-2014
Programa de Pós-Graduação: Matemática

Dissertação de Mestrado defendida em 06 de outubro de 2014 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof.(a). Dr(a). LUCIO CENTRONE

Prof.(a). Dr(a). IRINA SVIRIDOVA

Prof.(a). Dr(a). THIAGO CASTILHO DE MELLO

Abstract

This dissertation was written with the intent of containing its main prerequisites. So, initially, we will recall some basic definitions and some results from classical algebra. Then we will list some classical results of the theory of PI-algebras as well as the ones about codimensions and Hilbert series. The latter will give us tools to describe, at least partially, the polynomial identities of the Grassmann algebra in positive characteristic (mainly the unitary Grassmann algebra). Nevertheless, many of the results may work in characteristic zero too. We will take in consideration two cases: in the first one the ground field will be considered infinite (according to a paper written by Giambruno and Koshlukov) while in the second one we will consider the ground field to be finite (according to a paper written by Regev).

Keywords: Algebra, Grassmann algebra, Polynomial identities.

Resumo

Esta dissertação foi escrita com a intenção de conter os seus principais pré-requisitos. Assim, inicialmente, recordaremos algumas definições básicas e alguns resultados da álgebra clássica. Então, listaremos alguns resultados clássicos da teoria de PI-álgebras, bem como alguns resultados sobre codimensões e série de Hilbert. Este último nos dará ferramentas para descrever, pelo menos parcialmente, as identidades polinomiais da álgebra de Grassmann em característica positiva (principalmente a álgebra de Grassmann unitária). No entanto, muitos dos resultados podem funcionar em característica zero. Levaremos em consideração dois casos: no primeiro, o corpo base será considerado infinito (de acordo com um artigo escrito por Giambruno e Koshlukov) enquanto que, no segundo, consideraremos que o corpo base seja finito (de acordo com um artigo escrito por Regev).

Palavras-chave: Álgebra, Álgebra de Grassmann, Identidades polinomiais.

Sumário

Aos meus dois amores: Adriana Perrett e Anna Clara.

Agradecimentos

Agradeço primeiramente a Deus por todas as dádivas que recebi até agora e por conseguir realizar um sonho, que é conclusão desse Mestrado.

Agradeço a minha esposa e filha, respectivamente, Adriana Perrett e Anna Clara, pelo carinho, incentivo e apoio que me deram, mesmo quando utilizava o meu tempo livre para estudar, em detrimento do nosso convívio familiar. Amo vocês.

Agradeço aos meus pais, Antonio e Yara, e a minha avó, Alayde, por sempre me apoiarem e me incentivarem e, com muito sacrifício, me proporcionarem uma boa educação tanto acadêmica quanto para a vida.

Ao Prof. Dr. Lucio Centrone pela paciência, apoio, confiança, amizade e por sua orientação sempre correta e segura.

Ao Prof. Dr. Antonio Carlos Gilli Martins pelo incentivo, apoio e confiança no início da minha vida acadêmica na UNICAMP.

Aos meus colegas de trabalho da EsPCEx, principalmente aos amigos da Seção de Ciências Matemáticas, por me apoiarem e me ajudarem nesta empreitada.

Aos meus colegas do mestrado pela ajuda nas horas difíceis de estudo e pelas palavras de incentivo.

Aos professores e funcionários do IMECC, principalmente aos integrantes da Secretaria da Pós-Graduação, pela ajuda, incentivo e profissionalismo.

À Profa. Dra. Irina Sviridova (MAT-UnB) e ao Prof. Dr. Thiago Castilho de Mello (DCT-UNIFESP) por terem aceito a compor a banca examinadora, por avaliarem essa dissertação e pelas valiosas sugestões dadas que, com certeza, enriqueceram este trabalho.

"A Matemática foi o alfabeto que Deus
usou para escrever o Universo."
Galileo Galilei (1564 - 1642)

Introdução

A área da matemática na qual se insere esta dissertação é a álgebra não comutativa: teoria de anéis, e mais especificamente, na teoria das álgebras que satisfazem identidades polinomiais, chamadas PI-álgebras (do inglês *Polynomial Identity*). A classe das PI-álgebras é muito grande ela contém as álgebras comutativas, as álgebras de dimensão finita (como as álgebras matriciais), além de muitas outras álgebras que tem grande relevância para a própria matemática assim como para várias aplicações em outras áreas de pesquisa.

A Teoria de Álgebras com identidades polinomiais tem sido muito investigada desde o início da década de 1920. A origem deste tópico é geométrico e pode ser achado em um artigo de Dehn intitulado *Find conditions on D with the property D is commutative*, onde D é uma álgebra de divisão sobre o corpo K. Podemos destacar também os trabalhos de Wagner (1936), em sua maioria motivados pela geometria. Nesses trabalhos iniciais aparecem, de uma forma indireta, algumas identidades polinomiais para a álgebra das matrizes de ordem 2.

Sabemos que as identidades polinomiais em álgebras de matrizes têm sido objeto de estudo na teoria das PI-álgebras desde seu início e problemas relacionados têm estimulado seu desenvolvimento ao longo dos anos. Mas foi a partir de 1948 que esta teoria desenvolveu-se mais intensamente após o artigo de Kaplansky, onde o autor mostrou que toda PI-álgebra primitiva é uma álgebra simples e de dimensão finita. Em 1950, Amitsur e Levitski demonstraram, usando argumentos combinatórios, que o polinômio *standard* $s_{2n}(x_1, \ldots, x_{2n}) = \sum_{\sigma \in S_{2n}} \operatorname{sgn}(\sigma) x_{\sigma(1)} \cdots x_{\sigma(2n)}$ é uma identidade polinomial de grau mínimo para a álgebra das matrizes de ordem $2n$ sobre um corpo K. Este resultado marcou o começo de uma nova abordagem à PI-teoria, que visa à descrição das identidades polinomiais satisfeitas por uma álgebra dada e foi um dos primeiros resultados significativos da utilização da combinatória algébrica no estudo de PI-álgebras.

Também, em 1950, W. Specht conjecturou que para corpos de característica zero todo T-ideal (o ideal das identidades polinomiais de uma álgebra dada) é finitamente gerado, a partir desta conjectura falamos que se todas as subvariedades de $\mathcal{B}$, inclusive $\mathcal{B}$, são finitamente baseadas, então $\mathcal{B}$ satisfaz a propriedade de Specht. Mas foi somente em 1987, que Kemer respondeu de forma afirmativa tal problema. A teoria criada por Kemer para resolver o prloblema de Specht envolve o estudo de identidades $\mathbb{Z}_2$-graduadas além de certos produtos tensoriais graduados com a álgebra de Grassmann. Esta teoria é hoje uma das ferramentas básicas no estudo das identidades de uma álgebra dada. Entretanto, no caso de corpos de característica positiva a conjectura de Specht não é verdadeira. Em 1999 os matemáticos Belov e Grishin, e Shchigolev exibiram contra-exemplos para um corpo de característica $p \geq 2$.

A maioria da teoria estrutural da PI-álgebra foi desenvolvida nas décadas de 60 e 70. E foi na

década de 70, que a teoria das PI-álgebras foi relacionada à teoria mais geral de identidades traço como desenvolvida por Procesi via teoria de invariantes, e independentemente por Razmyslov.

O estudo das PI-álgebras há algum tempo se firmou como uma das áreas mais importantes e ricas da álgebra não-comutativa. Nas últimas décadas, a área passou por varias transformações, e ganhou destaque o uso de métodos combinatoriais, assintóticos e o uso da teoria de representações de grupos. Em 1972, Regev foi um dos primeiros matemáticos que utilizou tais métodos para demonstrar um teorema sobre álgebras. Pois, ao escrever um artigo intitulado *Existence of identities in* $A \otimes_F B$, utilizou-se dessa ferramenta para provar um teorema que o auxiliaria a demonstrar o tema de seu trabalho, cujo enunciado do teorema era o seguinte: Se A e B são PI-álgebras então $A \otimes_F B$ também é uma PI-álgebra. O ponto central na demonstração desse teorema, de natureza qualitativa à respeito das PI-álgebras, é um resultado quantitativo e combinatorial, que é por onde entra o grupo simétrico S_n.

As identidades polinomiais da álgebra de Grassmann foram descritas na década de 60, por Latyshev e em 1973, por Krakowski e Regev. Estes provaram que o polinômio $[x_1, x_2, x_3]$ forma uma base das identidades polinomiais da álgebra unitária de Grassmann de dimensão infinita sobre um corpo de característica zero, onde $[x_1, x_2, x_3] = [[x_1, x_2], x_3]$ e $[a, b] = ab - ba$ é o comutador de a e b. Krakowski e Regev, ao descreverem por completo a estrutura das identidades da álgebra de Grassmann, desenvolveram ferramentas importantes para a teoria das identidades polinomiais. Em 1991, Di Vincenzo deu uma prova diferente deste resultado e também exibiu, para qualquer k, bases finitas das identidades da álgebra de Grassmann de um espaço vetorial de dimensão finita.

Com relação às álgebras de Grassmann com característica positiva, em 1980, Stojanova-Venkova achou bases finitas das identidades satisfeitas pela álgebra não unitária de Grassmann de dimensão finita, sobre um corpo arbitrário K infinito. Em 1981, Siderov fez o mesmo no caso de dimensão infinita. Além disso, ela provou que para um corpo arbitrário K, todo T-ideal da álgebra associativa livre sem o 1 $K\langle X\rangle$, contendo $[x_1, x_2, x_3]$ tem uma base finita. Em 1991, Regev estudou as propriedades das partes multilineares do T-ideal da álgebra de Grassmann de dimensão infinita (tanto unitária quanto não unitária), sobre um corpo finito. Ou seja, já se conhece as bases das identidades polinomiais da álgebra de Grassmann em qualquer corpo.

Neste trabalho, com o intuito de conter os principais pré-requisitos, daremos algumas definições básicas sobre grupos, anéis, ideal, representações de grupos finitos, alguns tópicos sobre partições, álgebras, PI-álgebras, T-ideal, espaços vetoriais graduados, codimensões do T-ideal entre outros assuntos pertinentes ao tema. Uns poucos teoremas só foram enunciados, mas indicamos onde o leitor pode encontrar as suas demonstrações. Isto foi necessário pois estes teoremas são importantes para o bom entendimento de assuntos posteriores e não colocamos suas provas por dependerem de assuntos não abordados nesta dissertação.

Todos os assuntos acima mencionados são necessários porque esta dissertação tem por objetivo apresentar alguns conceitos e resultados de PI-álgebra a fim de que possamos estudar as identidades polinomiais na álgebra de Grassmann com característica positiva. Estudaremos, principalmente, a álgebra de Grassmann unitária. Para uma descrição das identidades polinomiais na álgebra de Grassmann não unitária veja o artigo *On bases for identities of some varieties of associatives algebras, Pliska Studia Mathematica*, 2, 103-115, 1981 (*Russian*), de autoria de Chiripov e Siderov.

Com o intuito de tornar a leitura mais agradável e compreensível, este trabalho foi dividido em quatro capítulos, conforme a seguir:

No primeiro capítulo, apresentamos alguns assuntos da álgebra linear, tais como, espaço vetorial, base de um espaço vetorial e soma direta de subespaços. Também, abordaremos alguns assuntos da álgebra, que são: noções básicas de grupos e anéis, ideal, representações de grupos finitos, alguns tópicos sobre partições, diagramas de Young. Também falaremos sobre algumas definições básicas como álgebras e suas propriedades básicas, álgebra de Lie, subálgebra, centro de uma álgebra, ideal, álgebras livres, álgebras com identidades polinomiais, comutador, variedades, álgebras relativamente livres, polinômio central, T-ideal, espaços vetoriais graduados, codimensão e identidades polinomiais homogêneas e multilineares, além de alguns teoremas e proposições que são necessários para o desenvolvimento deste trabalho. Comentaremos sucintamente o problema de Specht e definiremos álgebra de Grassmann, que é a álgebra base dessa dissertação, além de fornecer alguns exemplos dos assuntos deste capítulo.

No capítulo 2, formulamos as codimensões e séries de Hilbert para a álgebra de Grassmann e o cotamanho do T-ideal das identidades de E(V), considerando um corpo K com característica zero. Isto tem por objetivo, evidenciar, de certa forma, as dificuldades que surgem no estudo de PI-álgebras quando passamos de um corpo com característica zero para um corpo com característica positiva.

No capítulo 3, listaremos alguns resultados contidos nos trabalhos entitulados *On the identities of the Grassmann Algebras in characteristic p>0* e *Remarks on P.I. algebras over finite fields*, de autoria de Giambruno – Koshlukov e de Regev, respectivamente. Abordaremos, principalmente, a álgebra unitária de Grassmann em um corpo de característica maior que dois (mas também falaremos algo dessa álgebra em um corpo de característica zero), veremos algumas identidades polinomiais na álgebra de Grassmann e alguns polinômios que não o são, também serão vistos alguns polinômios que pertencem ao T-ideal da álgebra associativa $K_1 \langle X \rangle$ gerada pelo polinômio $[x_1, x_2, x_3]$. Informaremos, também, de qual polinômio todas as identidades polinomiais da álgebra de Grassmann são consequência e, no final do capítulo, vamos exibir uma base para identidades polinomiais da álgebra de Grassmann de dimensão finita e infinita sobre um corpo infinito.

E no último capítulo, estudaremos o trabalho de Regev *Grassmann Algebras over finite fields*, onde abordaremos, principalmente, o anel de valoração discreto, algumas identidades polinomiais para a álgebra de Grassmann com o objetivo de apresentar algumas de suas identidades polinomiais, além de encontrar alguns limitantes inferiores e superiores para a sua codimensão, utilizando ferramentas combinatoriais.

As principais ferramentas que utilizaremos nesta dissertação serão o argumento de Vandermonde, o processo de multilinearização de uma identidade polinomial, a teoria de álgebras multigraduadas, o estudo das várias codimensões das álgebras envolvidas e alguns tópicos da teoria de representação.

Capítulo 1

Conceitos Introdutórios

Este capítulo tem por objetivo mostrar alguns assuntos que serão necessários para o entendimento deste trabalho. Com este intuito, iremos apresentar alguns conceitos e definições básicas sobre grupo, anel, ideal, representações, partições, diagrama de Young, álgebra e seus tipos, identidades polinomiais, as definições de PI-álgebra e de T-ideal. Veremos, também, exemplos e resultados importantes acerca destes assuntos.

1.1 Pré-requisitos teóricos

Nesta seção abordaremos alguns tópicos sobre grupo, anel, ideal, representações e partições que serão necessários para um bom entendimento dos capítulos posteriores. Para um maior aprofundamento dos tópicos de álgebra abordados aqui, sugerimos ao leitor que pesquise nos livros [2], [7], [8], [10], [15], [18], [21], [23], [24] e [34], listados na referência bibliográfica.

Definição 1.1.1. Um conjunto não vazio de elementos G é chamado de **grupo** se em G está definida uma operação binária $* : G \times G \to G$ tal que:

1. $a, b, c \in G$ implica que $a * (b * c) = (a * b) * c \in G$ (lei associativa),
2. $\exists e \in G$ tal que $a * e = e * a = a \ \forall a \in G$ (existência do elemento neutro),
3. $\forall a \in G \ \exists a' \in G$ tal que $a * a' = a' * a = e$ (existência do inverso em G).

Notação: $(G, *)$.

Se não houver perigo de confusão, escreveremos o grupo $(G, *)$ apenas por G.

Se G possui um número finito de elementos, ele será chamado de **grupo finito**. Neste caso, o número de elementos de G será chamado de **ordem do grupo** G, cuja notação será $|G|$.

Observação 1.1.2. Em um grupo G temos que:

1. O elemento neutro é único.
   De fato, sejam $e_1, e_2 \in G$ os elementos neutros de G, logo: $e_1 e_2 = e_1$, pois e_2 é elemento neutro de G e $e_1 e_2 = e_2$, pois e_1 é elemento neutro de G. Portanto, $e_1 = e_2$.

2. O elemento inverso é único.
   Com efeito, sejam $a_1', a_2' \in G$ os elementos inversos de $a \in G$, logo:

$$a_1'a = e \Rightarrow (a_1'a)a_2' = ea_2' \Rightarrow a_1'(aa_2') = a_2' \Rightarrow a_1'e = a_2' \Rightarrow a_1' = a_2'.$$

Dessa forma, denotaremos o elemento inverso de $a \in G$ por a^{-1} (ou $-a$ se a operação for a adição) e o elemento neutro de G será denotado por 1_G ou 1 (ou 0_G ou 0 se a operação for a adição), se não houver risco de confusão.

Definição 1.1.3. Um grupo G é chamado de **abeliano** se $a * b = b * a$, $\forall a, b \in G$.

Definição 1.1.4. Seja um grupo $(G, *)$. Um elemento $g \in G$ é chamado de **idempotente** se

$$g^2 = g * g = g.$$

Definição 1.1.5. Seja G um grupo e $g \in G$ com a operação multiplicação. Se $n \in \mathbb{Z}$ definimos g^n como segue:

$$g^n = \begin{cases} 1, & \text{se} \quad n = 0 \\ g^{n-1} \cdot g, & \text{se} \quad n > 0 \\ (g^{-n})^{-1}, & \text{se} \quad n < 0 \end{cases}$$

Se $m, n \in \mathbb{Z}$ pode-se provar, usando indução, as seguintes propriedades:

- $g^m \cdot g^n = g^{m+n}$; e
- $(g^n)^m = g^{nm}$.

Observação 1.1.6. Adotando um grupo G com a operação aditiva, definimos ng como segue:

$$ng = \begin{cases} 0, & \text{se} \quad n = 0 \\ (n-1)g + g, & \text{se} \quad n > 0 \\ -((-n)g), & \text{se} \quad n < 0 \end{cases}$$

E as propriedades ficam da seguinte forma:

- $mg + ng = (m + n)g$; e
- $m(ng) = (nm)g$.

Seria muito bom focar nossa atenção em pedaços apropriados de G, que são menores do que ele, mas que temos algum controle e são tais que as informações obtidas deles possam ser usadas para ter informações relevantes sobre G. É natural esperar que tais pedaços se comportem razoavelmente bem em relação à operação de G. Tais pedaços de G são definidos a seguir.

Definição 1.1.7. Um subconjunto não vazio H de G é chamado de **subgrupo** de G se, sob a mesma operação definida em G, H é um grupo.

Exemplo 1.1.8. O conjunto $GL_m(K)$ das matrizes $m \times m$ invertíveis A com entradas no corpo K sob a multiplicação matricial usual é um grupo que não é abeliano.
Com efeito, por definição de $GL_m(K)$ existem A^{-1}, $Id \in GL_m(K)$ tais que $AA^{-1} = A^{-1}A = Id$ e $IdA = AId = A$.
Sejam $A, B \in GL_m(K)$ então existem $A^{-1}, B^{-1} \in GL_m(K)$ inversas de A e B, respectivamente. Logo: $(AB)(B^{-1}A^{-1}) = Id \Rightarrow AB \in GL_m(K)$.
Sabemos que a multiplicação matricial é associativa e não comutativa.

Exemplo 1.1.9. O conjunto $GL(V)$ dos operadores invertíveis do espaço vetorial V de dimensão finita sob a composição de operadores é um grupo.
Com efeito, por definição de $GL(V)$ existem $T^{-1} \in GL(V)$ e $Id \in GL(V)$ tal que $T \circ T^{-1} = T^{-1} \circ T = Id$ e $Id \circ T = T \circ Id = T$.
Sejam $T, U \in GL(V)$ então existem $T^{-1}, U^{-1} \in GL(V)$ operadores inversos de T e U, respectivamente. Logo: $(T \circ U) \circ (U^{-1} \circ T^{-1}) = Id \Rightarrow T \circ U \in GL(V)$.
Sabemos que a composição de operadores (que é uma função) é associativa.

Exemplo 1.1.10. O conjunto $\mathbb{R}$ com a adição usual forma um grupo abeliano. O conjunto $\mathbb{Z}$ sob a adição usual é um subgrupo abeliano de $\mathbb{R}$.

Exemplo 1.1.11. O conjunto $\mathbb{Z}_2 = \{0, 1\}$, com a relação binária soma $(+)$ definida de acordo com a tabela abaixo, forma um grupo aditivo abeliano:

$+$	0	1
0	0	1
1	1	0

Vamos definir a seguir, um conjunto que tem uma participação importante na Teoria de Grupos.

Definição 1.1.12. Sejam H um subgrupo de um grupo G e o conjunto $Hx = \{hx | \, h \in H\}$. Chamaremos $\bar{x} = Hx$ de **classe lateral (à direita) de H em G** e o conjunto $G/H = \{Hx | \, x \in G\}$, de todas as classes laterais (à direita) de H em G, de **conjunto quociente**. O número $|G/H|$ é chamado de **índice de H em G**.

Exemplo 1.1.13. Sejam $G = S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ e $H = S_2 = \{(1), (1\ 2)\}$ um subgrupo de G, onde (1) é a unidade e $(i\ j\ k)$ significa que i é permutado por j, j é permutado por k e k é permutado por i. Temos que $G/H = \{S_2; \{(1\ 3), (1\ 3\ 2)\}; \{(2\ 3), (1\ 2\ 3)\}\}$, logo $|G/H| = |S_3/S_2| = 3$.

A seguinte definição nos apresentará uma relação que é muito útil e tem um importante papel na Teoria de Grupos.

Definição 1.1.14. Se $a, b \in G$, então b é chamado de **conjugado** de a em G se existe um elemento $c \in G$ tal que $b = c^{-1}ac$. Denotaremos isto por $a \sim b$ e chamaremos esta relação de **conjugação**.

A conjugação é uma relação de equivalência em G e a classe de equivalência de $a \in G$ dada por $E(a) = \{x \in G \,|\, a \sim x\}$ sob a conjugação é chamada de **classe conjugada** de G.

Exemplo 1.1.15. Em S_3 temos as seguintes classes de conjugação:

- $E((1)) = \{(1)\}$, pois $(1) = (1)^{-1}(1)(1)$.
- $E(1\ 2) = \{(1\ 2), (1\ 3), (2\ 3)\}$, pois $(1\ 2) = (1)^{-1}(1\ 2)(1)$, $(1\ 3) = (1\ 2\ 3)^{-1}(1\ 2)(1\ 2\ 3)$ e $(2\ 3) = (1\ 3\ 2)^{-1}(1\ 2)(1\ 3\ 2)$.
- $E(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 3\ 2)\}$, pois $(1\ 2\ 3) = (1)^{-1}(1\ 2\ 3)(1)$, e $(1\ 3\ 2) = (1\ 2\ 3)^{-1}(1\ 3\ 2)(1\ 2\ 3)$.

Veremos agora uma observação que será usada para provar o lema posterior.

Observação 1.1.16. Seja S_n o grupo de permutações do número n. Como o índice de S_n em relação à S_{n-1} é n, temos a seguinte decomposição:

$$S_n = (1)S_{n-1} \cup \theta_1 S_{n-1} \cup \cdots \cup \theta_{n-1} S_{n-1},$$

onde a união é disjunta e, em cada parcela, $\theta_i \notin S_{n-1}$, onde $1 \leq i \leq n-1$.

Exemplo 1.1.17. Considere o conjunto $S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, pela última observação temos que:
$(1)S_2 \cup (1\ 3)S_2 \cup (2\ 3)S_2 = (1)\{(1), (1\ 2)\} \cup (1\ 3)\{(1), (1\ 2)\} \cup (2\ 3)\{(1), (1\ 2)\} = \{(1)(1), (1)(1\ 2)\} \cup \{(1\ 3)(1), (1\ 3)(1\ 2)\} \cup \{(2\ 3)(1), (2\ 3)(1\ 2)\} = \{(1), (1\ 2)\} \cup \{(1\ 3), (1\ 2\ 3)\} \cup \{(2\ 3), (1\ 3\ 2)\} = S_3$.

Definição 1.1.18. Uma aplicação $\varphi : G \to G'$ do grupo $(G, *_1)$ no grupo $(G', *_2)$ é chamado de **homomorfismo** se para todo $a, b \in G$ temos

$$\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b).$$

Lembremos que o **Núcleo de** φ é o conjunto definido por $\mathrm{Ker}(\varphi) = \{v \in A \,|\, \varphi(v) = 0\}$ e a **Imagem de** φ, definido por $\mathrm{Im}(\varphi) = \{\varphi(v) \,|\, v \in A\}$.

Dependendo das propriedades que um homomorfismo $\varphi : G \to G'$ tenha, podemos chamá-lo com os seguintes nomes:

Definição 1.1.19.

1. Uma aplicação $\varphi : G \to G'$ entre os grupos G e G' é chamado de **monomorfismo** se φ é um homomorfismo injetor.
2. Uma aplicação $\varphi : G \to G'$ entre os grupos G e G' é chamado de **epimorfismo** se φ é um homomorfismo sobrejetor.
3. Uma aplicação $\varphi : G \to G'$ entre os grupos G e G' é chamado de **isomorfismo** se φ é um homomorfismo bijetor.

Se existe um isomorfismo entre os grupos G e G', dizemos que eles são grupos **isomorfos** e denotamos este fato por $G \cong G'$.

Do ponto de vista das operações, dois grupos isomorfos G e G' são iguais. Pois se renomearmos $\varphi(x)$ por a e $\varphi(y)$ por b, através do isomorfismo $\varphi : G \to G'$, temos que $\varphi(xy) = ab$, ou seja, esta renomeação de elementos é consistente com a operação de G.

Exemplo 1.1.20. Seja $G = G' = (\mathbb{Z}, +)$. Considere a aplicação $\varphi : \mathbb{Z} \to \mathbb{Z}$ definida por $\varphi(x) = 2x$, temos que φ é um homomorfismo.
De fato, temos que $\varphi(x + y) = 2(x + y) = 2x + 2y = \varphi(x) + \varphi(y)$.

Exemplo 1.1.21. Seja $GL_m(\mathbb{R})$ o grupo de todas as matrizes A do tipo $m \times m$ com entradas reais, tal que $det(A) \neq 0$ e com a multiplicação matricial usual. Seja $\mathbb{R}^*$ o grupo de todos os números reais não nulos sob a multiplicação. Então a aplicação $\varphi : GL_m(\mathbb{R}) \to \mathbb{R}^*$ definida por $\varphi(A) = det(A)$ é um homomorfismo.
Com efeito, tomemos $A, B \in GL_m(\mathbb{R})$. Logo:

$$\varphi(AB) = det(AB) = det(A) \cdot det(B) = \varphi(A)\varphi(B).$$

Exemplo 1.1.22. $GL(V)$ e $GL_m(K)$ são grupos isomorfos, onde $\dim(V) = m < \infty$.
De fato, seja $\beta = \{v_1, \ldots, v_m\}$ uma base de V. Sabemos que o operador linear $A : V \to V$ fica inteiramente determinado pela matriz em relação à base, β $[A]_\beta = [a_{ij}] \in GL_m(K)$, que é definida por:

$$Av_j = \sum_{i=1}^{m} a_{ij} v_i, \quad j = 1, \ldots, m.$$

Logo fixado uma base β de V, temos determinada a função (que também é uma transformação linear)

$$\varphi : GL(V) \to GL_m(K)$$

que faz corresponder a cada $A \in GL(V)$ a sua matriz $[A]_\beta$ na base β.

Temos que a bijetividade de φ é assegurada pelo teorema abaixo, cujo enunciado está no próximo parágrafo e sua demonstração pode ser encontrada na página 40 de [26].

"Sejam V e W espaços vetoriais e β uma base de V. A cada vetor $u \in \beta$, façamos corresponder (de maneira arbitrária) um vetor $u' \in W$. Então existe uma única transformação linear $T : V \to W$ tal que $Au = u'$, para cada $u \in \beta$."

Agora, dados dois operadores lineares T e S e suas matrizes em relação à uma base β, respectivamente, $[T]_\beta$ e $[S]_\beta$, sabemos, da álgebra linear, que a matriz em relação à uma base β da composição $T \circ S$ é igual à $[T]_\beta[S]_\beta$. Portanto:

$$\varphi(T \circ S) = [T \circ S]_\beta = [T]_\beta[S]_\beta = \varphi(T)\varphi(S).$$

Ou seja, φ é um isomorfismo de grupo entre $GL(V)$ e $GL_m(K)$.

A próxima definição introduzirá um sistema algébrico que possui duas operações (adição e multiplicação). Estas operações estão sujeitas à muitas das regras familiares que conhecemos da aritmética. Esse sistema é uma generalização dos nossos sistemas numéricos usuais.

Definição 1.1.23. Um conjunto não vazio R é chamado de **anel** se em R existem duas operações binárias, denotadas por $+$ e $\cdot$, tal que para todo $a, b, c \in R$:

1. $(R, +)$ é um grupo abeliano.

2. $a \cdot b \in R$.

3. $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$ (leis distributivas).

Notação: $(R, +, \cdot)$.

Se não houver perigo de confusão escreveremos o anel $(R, +, \cdot)$ apenas por R.
Veremos na próxima definição, certos anéis que possuem propriedades especiais.

Definição 1.1.24. Um anel $(R, +, \cdot)$ é chamado de:

1. **comutativo** se $\forall a, b \in R$ temos que $a \cdot b = b \cdot a$; e de
2. **anel com unidade** se existir um elemento $u \in R$ tal que $\forall a \in R$ vale a seguinte igualdade: $a \cdot u = u \cdot a = a$. Esse elemento u é chamado de **unidade** de R.

A partir de agora, a unidade de R será denotada por 1_R ou 1, se não houver risco de confusão.

Exemplo 1.1.25. O conjunto dos número inteiros pares $2\mathbb{Z} = \{\ldots, -2, 0, 2, \ldots\}$ com a adição e multiplicação usuais de $\mathbb{Z}$ forma um anel comutativo e sem unidade.

Exemplo 1.1.26. O conjunto $\mathbb{Z}$ com a adição e multiplicação usuais forma um anel comutativo com unidade.

Exemplo 1.1.27. O conjunto $M_2(\mathbb{R})$, das matrizes 2×2 com entradas reais, com a adição e multiplicação matricial usuais forma um anel com unidade e não comutativo.

Proposição 1.1.28. Se R é um anel com unidade então sua unidade é única.

Demonstração. Sejam $u_1, u_2 \in R$ unidades de R. Pela definição de unidade de um anel temos que $u_1 = u_1 \cdot u_2$ e $u_2 = u_1 \cdot u_2$, logo:

$$u_1 = u_1 \cdot u_2 = u_2.$$

□

Proposição 1.1.29. Seja R um anel. Então para todo $a \in R$ temos que $a \cdot 0 = 0$.

Demonstração. $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Somando $-(a \cdot 0)$ no início e no fim da cadeia de igualdades temos que $a \cdot 0 = 0$. □

Definição 1.1.30. Se R é uma anel comutativo, então $a \neq 0$ é chamado de **divisor de zero** se existe um $b \in R$, $b \neq 0$, tal que $a \cdot b = 0$.

Exemplo 1.1.31. O anel comutativo $\mathbb{Z}_6$ tem como divisores de zero os números $\bar{2}$, $\bar{3}$ e $\bar{4}$, pois em $\mathbb{Z}_6$ temos que $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ e $\bar{3} \cdot \bar{4} = \bar{12} = \bar{0}$.

Algumas propriedades fazem certos anéis mais "bonitos" que outros, e se fazem dignos de destaque. A próxima definição listará alguns destes anéis.

Definição 1.1.32. 1. Um anel comutativo R é chamado de **domínio de integridade** (ou simplesmente **domínio**) se $\forall a, b \in R$ tivermos que $a \cdot b = 0 \Rightarrow a = 0$ o*u* $b = 0$. Ou seja, se ele não possui divisores de zero.

2. Um anel é chamado de **anel de divisão** se seus elementos não nulos formam um grupo sob a multiplicação.

3. Um **corpo** é um anel de divisão comutativo.

Proposição 1.1.33. Todo corpo K é um domínio de integridade.

Demonstração. Sejam $a, b \in K$ com $a \cdot b = 0$. Suponha que $a \neq 0$ logo, como K é um corpo, existe $a^{-1} \in K$ tal que $a \cdot a^{-1} = u$. Portanto: $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \Rightarrow (a^{-1} \cdot a) \cdot b = 0 \Rightarrow u \cdot b = 0 \Rightarrow b = 0$. □

Exemplo 1.1.34. $\mathbb{R}$ é um corpo. No entanto, $\mathbb{Z}$ é um domínio de integridade que não é um corpo pois, todo número inteiro diferente de -1 e 1 não tem inverso multiplicativo em $\mathbb{Z}$.

Definição 1.1.35. Um corpo K é chamado de **algebricamente fechado** se para todo polinômio $f(x) = \sum_{i=0}^{n} a_i x^i$ com coeficientes $a_i \in K$ existe $x_0 \in K$ tal que $f(x_0) = 0$.

Exemplo 1.1.36. Sabemos que $\mathbb{C}$ é um corpo algebricamente fechado e que $\mathbb{R}$ não é, pois em $\mathbb{R}$ o polinômio $f(x) = x^2 + 1$ não admite raiz.

Veremos a seguir, porque certos tipos de corpos tem um comportamento completamente distinto do normal quando seus elementos são multiplicados por um determinado número inteiro.

Definição 1.1.37. Seja m um inteiro positivo, então um corpo K tem **característica** m, se m é o menor inteiro tal que $m \cdot a = 0$, $\forall a \in K$. Se não existe tal m, K é dito de **característica zero**. **Notação**: $\text{car}(K) = p$.

Proposição 1.1.38. Seja $p \neq 0$ a característica de um domínio de integridade R (com ou sem unidade). Então p é primo.

Demonstração. Seja $p \neq 0$ a característica de R e suponha que ele não é primo. Logo existem primos $p_1, \ldots p_n$ (podendo ter primos repetidos) tais que:

$$\text{car}(R) = p = p_1 \cdots p_n.$$

Seja r um elemento qualquer de R, então:

$$p \cdot r = 0 \Rightarrow (p_1 \cdots p_n) \cdot r = 0 \Rightarrow (p_1 \cdots p_n) \cdot r \cdot r = 0 \Rightarrow (p_1 \cdots p_j \cdot r)(p_{j+1} \cdots p_n \cdot r) = 0 \Rightarrow$$

$$(p_1 \cdots p_j \cdot r) = 0 \quad \text{ou} \quad (p_{j+1} \cdots p_n \cdot r) = 0.$$

Mas $(p_1 \cdots p_j)$, $(p_{j+1} \cdots p_n) < p$, absurdo. □

Lema 1.1.39. Dados um corpo K e $x, y \in K$ temos que:

1. Se $\text{car}(K) = 0$ então

$$(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i.$$

2. Se $\text{car}(K) = p > 0$ então
$$(x+y)^p = x^p + y^p.$$

3. Se $\text{car}(K) = p > 0$ então:
$$(x+y)^{p^m} = x^{p^m} + y^{p^m}.$$

Demonstração. (1.) Vamos provar por absurdo em n.

Para $n = 0$: $(x+y)^0 = 1$ e $\sum_{i=0}^{0} \binom{n}{i} x^{n-i}y^i = 1x^0y^0 = 1$.

Suponha verdadeiro para n, ou seja, $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}y^i$.

Tomemos $n+1$, logo:

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)^n(x+y) \\
&= \left(\sum_{i=0}^{n} \binom{n}{i} x^{n-i}y^i\right)(x+y) \\
&= \sum_{i=0}^{n} \binom{n}{i} x^{n-i+1}y^i + \sum_{i=0}^{n} \binom{n}{i} x^{n-i}y^{i+1} \\
&= \left[\binom{n}{0}x^{n+1} + \binom{n}{1}x^n y + \cdots + \binom{n}{n-1}x^2y^{n-1}\right. \\
&\left. + \binom{n}{n}xy^n\right] + \left[\binom{n}{0}x^n y + \binom{n}{1}x^{n-1}y^2 + \cdots + \binom{n}{n-1}xy^n + \binom{n}{n}y^{n+1}\right] \\
&= \binom{n}{0}x^{n+1} + \left[\binom{n}{0} + \binom{n}{1}\right]x^n y + \cdots + \left[\binom{n}{n-1} + \binom{n}{n}\right]xy^n + \binom{n}{n}y^{n+1} \\
&= \binom{n+1}{0}x^{n+1} + \binom{n+1}{1}x^n y + \cdots + \binom{n+1}{n}xy^n + \binom{n+1}{n+1}y^{n+1} \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} x^{(n+1)-i}y^i.
\end{aligned}$$

Para a penúltima igualdade, utilizamos a conhecida Relação de Stifel:
$$\binom{n}{p-1} + \binom{n}{p} = \binom{n+1}{p}.$$

(2.) Com efeito, pela Proposição 1.1.38 p é primo logo, em cada um dos $\binom{p}{i} = \dfrac{p!}{i! \cdot (p-i)}$, onde $1 \leq i \leq p-1$, o fator p do numerador nunca vai ser cancelado pelos fatores do denominador. Portanto $\binom{p}{i} = 0$ para $1 \leq i \leq p-1$ e o resultado esperado é obtido.

(3.) Por indução sobre n na fórmula em 2. chega-se ao resultado. □

Exemplo 1.1.40. O conjunto $\mathbb{Z}$ é de característica zero. Mas o conjunto $\mathbb{Z}_3$ é de característica 3 e temos que: $(\bar{1}+\bar{2})^3 = (\bar{3})^3 = (\bar{0})^3 = \bar{0}$ e $(\bar{1})^3 + (\bar{2})^3 = \bar{1} + \bar{8} = \bar{1} + \bar{2} = \bar{3} = \bar{0}$.

A seguir, veremos como construir um corpo a partir de um domínio de integridade qualquer.

Seja $\aleph$ o conjunto de pares ordenados (a, b), onde $a, b \in R$, $b \neq 0$ e R é um anel de integridade. Tome em $\aleph$ a seguinte relação de equivalência:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Seja $[a, b]$ a classe de equivalência em $\aleph$ de (a, b), onde $a, b \in R$, $b \neq 0$ e seja $Q(R)$ o conjunto de tais classes de equivalência.

Além disso, defina em $Q(R)$ as seguintes operações, respectivamente, soma e produto:

- $[a, b] + [c, d] = [ad + bc, bd]$
- $[a, b][c, d] = [ac, bd]$

Temos que estas operações estão bem definidas e com elas $Q(R)$ é um corpo.

Definição 1.1.41. O corpo $Q(R)$ assim construído a partir de um domínio de integridade R é chamado de **corpo quociente de** R (ou **corpo de frações de** R).

Exemplo 1.1.42. No caso especial em que $R = \mathbb{Z}$ temos que $Q(\mathbb{Z}) = \mathbb{Q}$.

Dado um conjunto B, às vezes é útil saber se existe um conjunto de elementos que quando multiplicados com todos os elementos de B, temos como resultado o elemento nulo. Isto nos leva à seguinte definição:

Definição 1.1.43. Se A e B são dois conjuntos com uma operação multiplicação formal $A \cdot B \to S$ onde S é um conjunto qualquer com o elemento 0. Então definiremos o **anulador à esquerda** de B em A, por

$$Ann({}_AB) = \{a \in A \mid aB = 0\}.$$

Caso exista a multiplicação BA podemos definir o **anulador à direita** de B em A por

$$Ann(B_A) = \{a \in A \mid Ba = 0\}.$$

Se existirem ambos os conjuntos $Ann({}_AB)$ e $Ann(B_A)$, então chamaremos de o **anulador de** B **em** A, denotado por $Ann_A(B)$, o conjunto

$$Ann({}_AB) \cap Ann(B_A)$$

Exemplo 1.1.44. Sejam A o conjunto das matrizes 2×2 com entradas reais e B o subconjunto de A com elementos da forma $\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$. Logo, $Ann({}_AB) = \begin{bmatrix} 0 & x \\ 0 & y \end{bmatrix}$, $Ann(B_A) = \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}$ e $Ann_A(B) = \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$.

O subconjunto I de um anel R, definido a seguir, é importante na Teoria de Anel, pois ele tem a propriedade especial de que o resultado da multiplicação à esquerda de todo elemento de R por qualquer elemento de I também pertence a I.

Definição 1.1.45. Se R é um anel, um subconjunto I de R é chamado de **ideal à esquerda** de R se:

1. I é um subgrupo de R sob a adição.
2. $\forall r \in R$ e $\forall a \in I$ temos que $ra \in I$.

Podemos definir similarmente o **ideal à direita** de R.

Definição 1.1.46. Um **ideal bilateral** (ou simplesmente um **ideal**) do anel R é um ideal á direita e á esquerda ao mesmo tempo, notação $I \triangleleft R$.

Dado um ideal I de um anel R, definiremos o conjunto R/I como o conjunto de todos os elementos da forma $a + I = \{\bar{a} = a + i | \, a \in R \text{ e } i \in I\}$. Vamos definir no conjunto R/I as operações de adição e de multiplicação conforme a seguir:

$$(a + I) + (b + I) = (a + b + I) \text{ e } (a + I) \cdot (b + I) = (ab + I).$$

Vejamos que estas operações estão bem definidas.
Seja $a + I = a' + I$ e $b + I = b' + I$. Da primeira igualdade temos que $a = a' + i_1$ onde $i_1 \in I$ e, analogamente, $b = b' + i_2$ onde $i_2 \in I$.
A soma está bem definida, pois:

$$a + b = (a' + i_1) + (b' + i_2) = (a' + b') + (i_1 + i_2)$$

e como I é subgrupo de R temos $i_1 + i_2 \in I$. Isto significa que $(a + b) + I = (a' + b') + I$.
Para a multiplicação, temos que:

$$ab = (a' + i_1)(b' + i_2) = a'b' + a'i_2 + i_1b + i_1i_2.$$

Como I é um ideal de R temos que $a'i_2,\ i_1b,\ i_1i_2 \in I$. Fazendo $a'i_2 + i_1b + i_1i_2 = i_3$ obtemos que $ab = a'b' + i_3 \Rightarrow ab + I = a'b' + I$.
Logo, as operações estão bem definidas.

Proposição 1.1.47. O conjunto R/I com as operações definidas acima é um anel.

Demonstração. Sejam $a + I, b + I, c + I \in R/I$, logo:

- $(a + I) + (b + I) = (a + b) + I \in R/I$
- $(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I)$
- $(a + I) + ((b + I) + (c + I)) = (a + I) + ((b + c) + I) = (a + (b + c)) + I = ((a + b) + c) + I = ((a + b) + I) + (c + I) = ((a + I) + (b + I)) + (c + I)$
- $(I) + (a + I) = (0 + I) + (a + I) = (0 + a) + I = a + I$ (Elemento neutro)
- $(-a + I) + (a + I) = (-a + a) + I = 0 + I = I$ (Elemento inverso)

- $(a+I)(b+I) = ab+I \in R/I$;
- $(a+I)((b+I)(c+I)) = (a+I)(bc+I) = a(bc)+I = (ab)c+I = (ab+I)(c+I) = ((a+I)(b+I))(c+I)$
- $(a+I)((b+I)+(c+I)) = (a+I)(b+c+I) = a(b+c)+I = (ab+ac)+I = (ab+I)+(ac+I)$. Prova-se de maneira análoga que $((a+I)+(b+I))(c+I) = (ac+I)+(bc+I)$.

□

Definição 1.1.48. O anel R/I é chamado de **anel quociente**.

As duas próximas proposições nos dizem sobre algumas propriedades que o anel R/I "herda" do anel R.

Proposição 1.1.49. Se R é um anel comutativo então R/I também o é.

Demonstração. $(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I)$ □

Proposição 1.1.50. Se R é um anel com unidade então R/I também o é.

Demonstração. Seja 1 a unidade de R e tome o elemento $1+I \in R/I$. Portanto:
$(1+I)(a+I) = 1a+I = a+I$ e $(a+I)(1+I) = a1+I = a+I$. Temos então que $1+I$ é a unidade de R/I. □

Certos anéis têm a propriedade de que todos os seus ideais possuem a mesma forma (a mais simples possível). Desse modo, temos a seguinte definição:

Definição 1.1.51. Um domínio de integridade R com unidade é um **domínio de ideal principal** se todo ideal A de R é da forma $A = \{xa | \ x \in R\}$ para um certo $a \in A$.

A próxima definição, nos apresenta certos tipos de ideais que possuem propriedades especiais e que serão úteis mais tarde.

Definição 1.1.52.
1. Um ideal I de um anel R é chamado **primo** se para todos ideais A, B de R tais que $AB \subset I$ temos que $A \subset I$ ou $B \subset I$.
2. Um ideal $M \neq R$ em um anel R é chamado de **ideal maximal** de R se sempre que U é um ideal de R tal que $M \subset U \subset R$, então ou $U = R$ ou $U = M$.

Teorema 1.1.53. Se R é um anel comutativo com unidade e M é um ideal de R, então M é maximal se somente se R/M é um corpo.

Demonstração. ($\Rightarrow$) Seja $\bar{x} \in R/M$, onde $\bar{x} \neq \bar{0}$. Vamos demonstrar que existe o inverso de $\bar{x}$ em R/M.
Como $\bar{x} \neq \bar{0}$ temos que $x \notin M$. Vamos provar que o conjunto $I = \{j+xr | \ j \in M, r \in R\}$ é um ideal. Com efeito, seja $a \in R$ e $j+xr \in I$, logo: $a(j+xr) = (aj)+a(xr) = (aj)+(ax)r$. Como M é um ideal temos que $aj \in M$ e como R é um anel $ar \in R$. Portanto $a(j+xr) \in I$. De maneira análoga provamos que $(j+xr)a \in I$. Observe que $M \subset I$ mas $M \neq I$. Como M é maximal temos

que $I = A \Rightarrow 1 \in I \Rightarrow 1 = j + xr$, para certo $j \in M$ e $r \in R$.
Seja $\pi : R \to R/M$ tal que $\pi(1) = \pi(j + xr) \Rightarrow \bar{1} = \overline{j + xr} = \bar{j} + \overline{xr} = \overline{xr} = \bar{x}\bar{r} \Rightarrow \bar{x}^{-1} = \bar{r}$.
($\Leftarrow$) Seja $J \subset I \subset M$, suponhamos que $J \neq I$ então existe $i \in I - J$ tal que $\bar{0} \neq \bar{i} \in R/M \Rightarrow \exists \bar{r} \,|\, \bar{r}\bar{i} = \bar{1} \Rightarrow ri - 1 \in M \Rightarrow ri - 1 = j$ para algum $j \in M \Rightarrow 1 = ri - j \in I$ pois $ri \in I$ e $j \in M \subset I$.
Portanto $I = R$. □

Definição 1.1.54. Sejam R um domínio e $Q(R)$ seu corpo quociente. Dizemos que R é um **anel de valorização de** $Q(R)$ se para cada $x \in Q^*(R) = Q(R) - \{0\}$, então $x \in R$ ou $x^{-1} \in R$ (ou ambos).

Exemplo 1.1.55. O conjunto $\mathbb{Z}$ não é um anel de valorização de $\mathbb{Q}$, pois $3/2 \in \mathbb{Q}^*$ com $3/2 \notin \mathbb{Z}$ e $2/3 \notin \mathbb{Z}$.

Definição 1.1.56. Sejam K um corpo e ∞ um símbolo, que neste contexto designa um elemento não inteiro tal que:

$$\infty + \infty = \infty, \quad z + \infty = \infty \quad \text{e} \quad z < \infty, \forall z \in \mathbb{Z}.$$

Uma **valorização discreta** de K é uma função sobrejetora $v : K \to \mathbb{Z} \cup \{\infty\}$ tal que:

1. $v(x) = \infty \Leftrightarrow x = 0$;
2. $v(xy) = v(x) + v(y)$ e
3. $v(x + y) \geq \min\{v(x), v(y)\}$, assumindo $a + b \neq 0$.

O conjunto

$$R_v = \{x \in K \,|\, v(x) \geq 0\}$$

é chamado de **anel de valorização de** v.

Definição 1.1.57. Um domínio R é chamado de **anel de valorização discreta** se existe uma valorização discreta v no corpo quociente $Q(R)$ tal que R é o anel de valorização de v, ou seja, $R = R_v$.

Observação 1.1.58. Todo anel de valorização discreta R é um domínio de ideal principal que possui somente um ideal maximal.

Exemplo 1.1.59. Seja $\mathbb{Z}_{(2)} = \{p/q \,|\, p, q \in \mathbb{Z}, q \text{ ímpar}\}$. Temos que seu corpo quociente é $\mathbb{Q}$. Agora, para qualquer elemento não nulo $r \in \mathbb{Q}$ podemos aplicar a fatoração única no numerador e denominador de r e escrevê-lo na forma $2^k s/t$, onde s, t, k são inteiros com s e t ímpares. Neste caso, defina a valorização discreta $v : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ dada por $v(r) = k$. Portanto, temos que $R_v = \mathbb{Z}_{(2)}$ e então $\mathbb{Z}_{(2)}$ é um anel de valorização discreta.

Definição 1.1.60. Sejam um grupo abeliano $(M, +)$ e um anel R. O conjunto M é chamado de R**-módulo à direita**, notação M_R, se existe uma aplicação

$$\begin{array}{rccc} A: & M \times R & \to & M \\ & (m, r) & \mapsto & mr \end{array}$$

tal que $\forall a, b \in M$ e $\forall r, s \in R$, temos:

1. $(a+b)r = ar + br$,
2. $a(r+s) = ar + as$,
3. $a(r \cdot s) = (ar)s$.

   Se R possui unidade 1, diremos que M_R é um módulo **unitário** se:

4. $a1 = a$.

Definição 1.1.61. Um **submódulo** N de M é um subgrupo de M que é fechado sob as novas operações, isto é, para todo $b \in N$ e $r \in R$ temos que $br \in N$.

Veremos, a seguir, qual é a forma mais simples que um módulo pode ter.

Definição 1.1.62. Um módulo M_R é chamado de **irredutível** se ele tem exatamente dois submódulos. Estes submódulos têm que ser 0 e M, e da definição implica que $M \neq 0$.

Analogamente, pode ser definido o R-módulo à esquerda ${}_RM$.

Exemplo 1.1.63. Se R é um corpo, M_R é o que frequentemente conhecemos por espaço vetorial.

Exemplo 1.1.64. Se $R = \mathbb{Z}$, $M_{\mathbb{Z}}$ é essencialmente apenas M, pois a multiplicação por um número inteiro se reduz a uma adição repetida. Então $\mathbb{Z}$-módulos e grupos abelianos podem ser considerados como os mesmos objetos.

Exemplo 1.1.65. Se $M = R$ e a aplicação $M \times R \to M$ é a multiplicação, isto é, $ar = a \cdot r$, então temos um módulo à direita R_R.

Definição 1.1.66. 1. Uma sequência (finita ou infinita)

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \cdots \xrightarrow{f_n} M_n$$

de módulos (ou grupos, ou espaços vetoriais) é chamada de **exata** se:

$$\mathrm{Im}(f_k) = \mathrm{Ker}(f_{k+1}).$$

2. Uma sequência é chamada de **exata curta** se ela tem a forma

$$A \xhookrightarrow{f} B \xrightarrow{g} C$$

onde f é um monomorfismo e g é um epimorfismo.
Outra maneira de escrever uma sequência exata curta é

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

A próxima definição nos fornecerá uma ferramenta muito útil para o nosso trabalho.

Definição 1.1.67. Seja G um grupo. Se V é um K-espaço vetorial, considere $GL(V)$ o grupo de todos os operadores lineares invertíveis de V. Se $\dim(V) = m < \infty$, fixando uma base de V, identificamos o grupo $GL(V)$ com o grupo $GL_m(K)$ das matrizes $m \times m$ invertíveis com entradas no corpo K (veja Exemplo 1.1.22).

1. A **representação** ϕ de G em V é um homomorfismo de grupo

   $$\phi : G \to GL(V).$$

   O **grau** da representação ϕ é igual a dimensão do espaço vetorial V. A representação ϕ é chamada de **fiel** se o núcleo de ϕ é trivial e é chamada de **trivial** se o seu núcleo coincide com G.

2. Duas representações $\phi : G \to GL(V)$ e $\phi' : G \to GL(V')$ são chamadas de **equivalentes**, se existe um isomorfismo $\theta : V \to V'$ dos espaços vetoriais V e V' tal que

   $$(\theta \circ \phi(g))(v) = (\phi'(g) \circ \theta)(v),\ g \in G,\ v \in V.$$

3. Se W é um subespaço de V tal que $\phi(G) = W$, então a representação $\psi : G \to GL(W)$ definida por

   $$(\psi(g))(w) = (\phi(g))(w),\ g \in G,\ w \in W \subset V,$$

   é chamada de **sub-representação** da representação $\phi : G \to GL(V)$. A representação ψ é **própria** se $W \neq \{0\}$ e $W \neq V$.

4. Se $\phi' : G \to GL(V')$ e $\phi'' : G \to GL(V'')$ são duas representações de G, então a representação $\phi = \phi' \oplus \phi'' : G \to GL(V' \oplus V'')$ definida por

   $$(\phi(g))(v', v'') = ((\phi'(g))(v), (\phi''(g))(v)),\ g \in G, (v', v'') \in V' \oplus V'',$$

   é chamada de **soma direta** de ϕ' e ϕ''. Similarmente, definimos a soma direta de qualquer número (finito ou infinito) de representações. O **produto tensorial** $\phi = \phi' \otimes \phi'' : G \to GL(V' \otimes V'')$ de ϕ' e ϕ'' é definido por

   $$(\phi(g))(v' \otimes v'') = ((\phi'(g))(v') \otimes (\phi''(g))(v'')),\ g \in G, v' \otimes v'' \in V' \otimes V''.$$

5. A representação $\phi : G \to GL(V)$ é **irredutível** se ela não tem sub-representações próprias, caso contrário ela é chamada de **decomponível**. A representação ϕ é **completamente irredutível** se ela é uma soma direta de representações irredutíveis.

6. Se W é um subespaço de V, W é dito **invariante sob a ação de** G (ou G**-invariante**), se $\forall x \in W$ implica que $\phi(s)(x) \in W$, $\forall s \in G$. Denotaremos $\phi(s)(x)$ por $\phi_s(x)$.

Comentaremos, sucintamente, a relação entre as representações de G e os KG-módulos. Considere o conjunto $\mathrm{End}(V)$ da álgebra dos K-endomorfismos de V. Se KG é o grupo álgebra de K sobre G e ϕ é a representação de G em V, temos que ϕ induz um homomorfismo de K-álgebras $\phi' : KG \to \mathrm{End}(V)$ tal que $\phi'(1_G) = 1$.

No caso em que $\dim_K(V) = n < \infty$, isto é, com representações lineares finitas, uma representação de um grupo G determina unicamente um KG-módulo (ou G-módulo) de dimensão finita da seguinte maneira: Se $\phi : G \to GL(V)$ é uma representação de G, V se torna um G-módulo (à esquerda) por definir $gv = \phi(g)(v)$ para todo $g \in G$ e $v \in V$. Temos, também, que se M é um G-módulo de dimensão finita como um espaço vetorial sobre K, então $\phi : G \to GL(M)$, tal que $\phi(g)(m) = gm$, para todo $g \in G$, $m \in M$, define uma representação de G em M.

O próximo teorema e seu corolário nos dizem que as representações de G podem ser construídas de outras representações mais simples (irredutíveis) por meio de operações algébricas lineares.

Teorema 1.1.68 (**Teorema de Maschke).** Sejam $\phi : G \to GL(V)$ uma representação linear finita de G em V, o subespaço $W \subset V$ G-invariante e um corpo K de característica 0 ou de característica $p \neq 0$, tal que p não é um divisor de $|G|$. Então $\exists W_0 \subset V$ subespaço tal que $V = W \oplus W_0$ e W_0 é G-invariante.

Demonstração. Seja W' um complementar de W, como $\dim V < \infty$ temos que $V = W \oplus W'$. Logo existe a projeção $p : V \to W$ tal que $\forall v \in V$ com $v = w + w'$ temos que $p(v) = w$. Seja $p_0 = (1/|G|) \sum_{s \in G} \phi_s \, p \, \phi_s^{-1} : V \to W$ (pois W é invariante). Vamos provar que $\forall w \in W$, $p_0(w) = w$.
Com efeito, seja $\phi_s^{-1}(w) \in W$. Logo $p(\phi_s^{-1}(w)) = \phi_s^{-1}(w)$, portanto:

$$p_0(w) = (1/|G|) \sum_{s \in G} (\phi_s \, p \, \phi_s^{-1})(w) = (1/|G|) \sum_{s \in G} w = (1/|G|) \, |G| w = w.$$

Logo p_0 é uma projeção, então existe $W_0 \subset V$ subespaço associado ao p_0 tal que $V = W \oplus W_0$.
Vamos provar que W_0 é G-invariante.
De fato, para todo $t \in G$ temos:

$$\phi_t \, p_0 \, \phi_t^{-1} = (1/|G|) \sum_{s \in G} \phi_t \, \phi_s \, p \, \phi_s^{-1} \, \phi_t^{-1} = (1/|G|) \sum_{s \in G} \phi_{ts} \; p \, \phi_{ts}^{-1} = (1/|G|) \sum_{s \in G} \phi_s \; p \, \phi_s^{-1} = p_0.$$

Logo para todo $t \in G$ temos que $\phi_t p_0 = p_0 \phi_t$. Se $w_0 \in W_0$ e $t \in G$, então:

$$(p_0 \phi_t)(w_0) = (\phi_t p_0)(w_0) = \phi_t(p_0(w_0)) = \phi_t(0) = 0, \; \mathrm{p}o i s \, V = W \oplus W_0.$$

Logo:

$$p_0(\phi_t(w_0)) = 0 \Rightarrow \phi_t(w_0) \in W_0 \Rightarrow W_0.$$

Portanto, W_0 é G-invariante. □

O próximo corolário é uma consequência importante do Teorema de Maschke.

Corolário 1.1.69. Nas condições do Teorema de Maschke, toda representação é soma direta de representações irredutíveis.

Demonstração. Vamos provar por indução em n. Seja $n = 1$ e $\phi : G \to GL(V)$ em que a $\dim V = 1 \Rightarrow \phi$ é irredutível.
Considere agora $n \geq 2$. Se ϕ é irredutível temos o resultado, caso contrário, pelo Teorema 1.1.68, existem V_1 e V_2 subespaços G-invariantes de V onde ambos têm dimensão não nula e $V = V_1 \oplus V_2$ e $\dim V_1 < \dim V$ e $\dim V_2 < \dim V$. Logo aplicando a indução em V_1 e V_2 conseguiremos escrevê-los como um soma direta de subespaços G-invariantes e o resultado é obtido. □

Definição 1.1.70. Sejam $V_1, \ldots, V_s$ módulos não isomorfos dois a dois de um grupo finito G. Seja W um G-módulo de dimensão finita. Seja $W = W_1 \oplus \cdots \oplus W_s$ uma decomposição de W em soma de G-submódulos irredutíveis. Se para cada módulo W_i temos que $m_i V_i \cong W_i$, chamamos os inteiros não negativos m_i de a **multiplicidade** de V_i na decomposição de W e escrevemos

$$W = m_1 V_1 \oplus \cdots \oplus m_s V_s.$$

A seguinte definição nos fornece uma efetiva ferramenta para entender as representações de um grupo finito G.

Definição 1.1.71. Seja $\phi : G \to GL(V)$ uma representação de dimensão finita do grupo G. A função $\chi_\phi : G \to K$ definida por

$$\chi_\phi(g) = tr_V(\phi(g)),\ g \in G,$$

é chamada de **caráter** de ϕ. Se ϕ é uma representação irredutível, então χ_ϕ é chamado de **caráter irredutível**.

Temos que se g_1 e g_2 são dois elementos conjugados do grupo G e ϕ é uma representação de dimensão finita de G então $\chi_\phi(g_1) = \chi_\phi(g_2)$. E também, se ϕ e ψ são duas representações de dimensão finita do grupo G então

$$\chi_{\phi\oplus\psi} = \chi_\phi + \chi_\psi \ \text{ e } \ \chi_{\phi\otimes\psi} = \chi_\phi \cdot \chi_\psi.$$

O seguinte teorema mostra que o conhecimento do caráter nos fornece muitas informações sobre as representações e o número das representações irredutíveis é determinado simplesmente por propriedades de grupo. Uma demonstração deste teorema pode ser encontrada em [34].

Teorema 1.1.72. Seja G um grupo finito e K um corpo algebricamente fechado. Então:

1. Toda representação de dimensão finita de G é determinada, a menos de um isomorfismo, pelos seus caráteres.

2. O número das representações irredutíveis não isomorfas de G é igual ao número de classes conjugadas de G.

Para grupos de ordem pequena podemos fazer a **tabela de caráteres de irredutíveis de** G. As linhas da tabela são completadas com os caráteres irredutíveis e as colunas pelos representantes das classes de conjugação. As entradas da tabela são iguais aos valores dos caráteres nas correspondentes classes de conjugação.

Vejamos dois exemplos de tabelas de caráteres de irredutíveis, onde no primeiro exemplo $G = \mathbb{Z}_3$ de ordem 3 e, no segundo, $G = S_3$ de ordem 6.

Exemplo 1.1.73. Considere o grupo cíclico aditivo $\mathbb{Z}_3$. Temos que suas classes conjugadas são: $E(0) = \{0\}$, $E(1) = \{1\}$ e $E(2) = \{2\}$. Dessas informações e do Teorema 1.1.72 podemos montar a seguinte tabela de caráteres de $\mathbb{Z}_3$, onde $w = e^{2\pi i/3}$:

$\mathbb{Z}_3$	0	1	2
χ_1	1	1	1
χ_2	1	w	w^2
χ_3	2	w^2	w

Exemplo 1.1.74. Considere o grupo S_3. Do Exemplo 1.1.15 temos que suas classes conjugadas são: $E(1)$, $E(1\ 2)$ e $E(1\ 2\ 3)$. Dessas informações e do Teorema 1.1.72 podemos montar a seguinte tabela de caráteres de S_3:

S_3	(1)	(1 2)	(1 2 3)
χ_1	1	1	1
χ_2	1	-1	-1
χ_3	2	0	-1

A representação de inteiros positivos por somas de outros inteiros positivos é um processo de decomposição aditivo fundamental e de muita utilidade. Devido a isso, faremos a seguinte definição:

Definição 1.1.75. Uma **partição** de um número inteiro positivo n é uma sequência de inteiros $\lambda_1 \geq \ldots \geq \lambda_r \geq 1$ tal que $\sum_{i=1}^{r} \lambda_i = n$. Os λ_i são chamados de **partes** da partição. O conjunto de todas as partições de um número n será denotada por $\mathbf{Par}(n)$.

Muitas vezes a partição $(\lambda_1, \ldots, \lambda_r)$ será denotada por λ, e escreveremos $\lambda \vdash n$ para denotar que "λ é uma partição de n". Às vezes é conveniente indicar o número de vezes que cada inteiro aparece na partição, como por exemplo $(3, 2^2, 1^3) = (3, 2, 2, 1, 1, 1)$.

Exemplo 1.1.76. A **função partição** $p(n)$ é o número de partições de n.

- $p(1) = 1$, pois $1 = (1)$;
- $p(2) = 2$, pois $2 = (2)$ e $2 = 1 + 1 = (1, 1)$; e
- $p(3) = 3$, pois $3 = (3)$, $3 = 2 + 1 = (2, 1)$ e $3 = 1 + 1 + 1 = (1, 1, 1)$.

É bem conhecido que as classes de conjugação de S_n são indexadas pelas partições de n: Se $\theta \in S_n$, decompomos θ em produto de ciclos disjuntos, incluindo os 1-ciclos. Esta decomposição é única se requerermos que

$$\theta = \pi_1 \cdots \pi_r$$

com $\pi_1, \ldots, \pi_r$ ciclos de tamanho $\lambda_1 \geq \cdots \geq \lambda_r \geq 1$, respectivamente. Portanto, a partição $\lambda = (\lambda_1, \ldots, \lambda_r)$ determina unicamente a classe de conjugação de θ.

Logo, como mencionado acima, todos os caráteres irredutíveis de S_n são indexados pelas partições de n. A partir de agora, vamos denotar por χ_λ o S_n**-caráter irredutível** correspondente a $\lambda \vdash n$.

Observação 1.1.77. A definição de partição é interessante pois, sobre um corpo de característica zero, o número de partições de um inteiro positivo n coincide com o número de classes de conjugação de S_n que é o mesmo número de caráteres (e portanto de representações, e portanto de módulos) irredutíveis de S_n.

Definição 1.1.78. A **função geradora** $f(q)$ para a sequência $a_0, a_1, \ldots$ é a série de potências

$$f(q) = \sum_{n \geq 0} a_n q^n.$$

Definição 1.1.79. Seja $\lambda = (\lambda_1, \ldots, \lambda_r)$ uma partição, onde para uma maior generalidade $\lambda_i \geq 0$. Uma **função simétrica elementar** e_λ é definida por:

1. $e_0 = 1$;
2. $e_n = \sum_{i_1 < \ldots < i_n}^{r} x_{i_1} \cdots x_{i_n}$, onde $i_m \in \{1, \ldots r\}$; e
3. $e_\lambda = e_{\lambda_1} \cdots e_{\lambda_r}$.

Exemplo 1.1.80. Considere $\lambda = (2, 1, 0, 0)$ então:

$$e_\lambda = e_2 e_1 e_0 e_0 = \left(\sum_{i<j}^{4}\right) \cdot \left(\sum_{k=1}^{4}\right) \cdot 1 \cdot 1 = (x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4)(x_1 + x_2 + x_3 + x_4).$$

Observação 1.1.81. As funções simétricas elementares possuem uma função geradora bastante conhecida, a saber:

$$F(t) = \sum_{n=0}^{r} e_n t^n = \prod_{i=1}^{r} (1 + x_i t)$$

Exemplo 1.1.82. Considere $r = 3$, temos:

$$\begin{aligned}
\prod_{i=1}^{3} (1 + x_i t) &= (1 + x_1 t)(1 + x_2 t)(1 + x_3 t) \\
&= 1 + x_1 t + x_2 t + x_3 t + x_1 x_2 t^2 + x_1 x_3 t^2 + x_2 x_3 t^2 + x_1 x_2 x_3 t^3 \\
&= 1 + (x_1 + x_2 + x_3)t + (x_1 x_2 + x_1 x_3 + x_2 x_3)t^2 + (x_1 x_2 x_3)t^3 \\
&= e_0 + e_1 t + e_2 t^2 + e_3 t^3 \\
&= \sum_{n=0}^{3} e_n t^n.
\end{aligned}$$

Definição 1.1.83. Uma **composição** é uma partição na qual a ordem das parcelas é levada em conta (neste caso a partição será denotada por $(\lambda_1, \ldots, \lambda_m)^*$). Denotaremos por $\text{comp}(m, n)$ o **número de composições de n com exatamente m partes**.

Exemplo 1.1.84. $\text{comp}(2, 3) = 2$, pois $3 = (2, 1)^* = 2 + 1 = 1 + 2$.

Teorema 1.1.85.

$$\text{comp}(m, n) = \binom{n-1}{m-1} = \frac{(n-1)!}{(m-1)!\,(n-m)!}$$

Demonstração. Vamos introduzir um representação gráfica para a composição de n. Para a composição $(a_1, \ldots, a_m)$ de n vamos associar m segmentos dos intervalo $[0, n]$; o primeiro segmento é de tamanho a_1, o segundo segmento é de tamanho a_2 e assim sucessivamente.

Observemos agora que podemos construir cada uma das $\text{comp}(m, n)$ composições de n com m partes por escolher $m - 1$ dos primeiros $n - 1$ inteiros como pontos finais para os m segmentos que dividem $[0, n]$. Como essas escolhas podem ser feitas de $\binom{n-1}{m-1}$ maneiras diferentes, temos que $\text{comp}(m, n) = \binom{n-1}{m-1}$. □

Exemplo 1.1.86. Utilizando o resultado do último teorema para resolver o Exemplo 1.1.84, temos que $\text{comp}(2, 3) = \binom{3-1}{2-1} = \binom{2}{1} = 2$.

Definição 1.1.87. Denotaremos por $\text{comp}(N, M, n)$ o número de composições de n com exatamente M partes, onde cada parte é menor ou igual a N, ou seja, $\text{comp}(N, M, n)$ é igual ao número de elementos do conjunto $\{(a_1, \ldots, a_M)\}$ com $\sum a_i = n$, $1 \leq a_1, \ldots, a_M \leq N$.

Observemos que $\text{comp}(N, M, n) = \text{comp}(M, n)$ quando $N \geq n$.

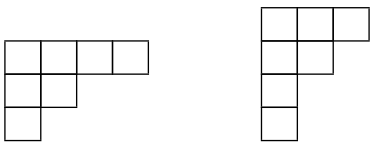
Uma efetiva ferramenta para estudar partições é a sua representação gráfica. A cada partição λ é associada uma representação gráfica. A seguir, vamos ver como é realizada essa associação.

Definição 1.1.88. O **diagrama de Young** $[\lambda]$ de uma partição $\lambda = (\lambda_1, \ldots, \lambda_r) \vdash n$ pode ser formalmente definido como o conjunto de **nós (ou caixas)** $(i, j) \in \mathbb{Z}^2$ tal que $1 \leq j \leq \lambda_i$, $i = 1, \ldots, r$.

Graficamente desenhamos os diagramas substituindo os nós por caixas quadradas, adotando a convenção, como nas matrizes, que a primeira coordenada i (índice das linhas) aumenta de cima para baixo e a segunda coordenada j (índice das colunas) aumenta da esquerda para a direita. A primeira caixa da esquerda de cada linha são caixas acima de outras e a i-ésima linha contém λ_i caixas.

Denotaremos por λ'_j o comprimento de sua j-ésima coluna de $[\lambda]$. A partição $\lambda' = (\lambda'_1, \ldots, \lambda'_r)$ e seu diagrama $[\lambda']$ são chamados de **conjugados** respectivamente a λ e a $[\lambda]$.

Exemplo 1.1.89. Dada a partição $\lambda = (4, 2, 1)$ temos que $\lambda' = (4, 2, 1)' = (3, 2, 1^2)$, conforme podemos ver abaixo dos diagramas de Young, respectivamente, $[\lambda]$ e $[\lambda']$:



Definição 1.1.90. O (i,j)**-gancho** do diagrama $[\lambda] = [\lambda_1, \ldots, \lambda_r]$ consiste da j-ésima caixa da i-ésima linha de $[\lambda]$ composta de $\lambda_i - j$ caixas para a direita dele (chamado de **braço** do gancho) e de $\lambda'_j - i$ caixas abaixo dele (chamado de **perna** do gancho). O **tamanho** do gancho é igual a $\lambda_i + \lambda'_j - i - j + 1$.

Exemplo 1.1.91. O (1,2)-gancho de $[4,2,1]$ é de tamanho $\lambda_1+\lambda'_2-1-2+1 = 4+2-1-2+1 = 4$, onde o braço mede $\lambda_1 - 2 = 4 - 2 = 2$ e a perna mede $\lambda'_2 - 1 = 2 - 1 = 1$, conforme o diagrama de Young a seguir.

	x	x	x
	x		

Definição 1.1.92. Para a partição $\lambda = (\lambda_1, \ldots, \lambda_k) \vdash n$, definimos a λ**-tabela** T_λ de índice $\alpha = (\alpha_1, \ldots, \alpha_m)$ onde $\alpha_1 + \ldots + \alpha_m = n$, como o diagrama de Young $[\lambda]$ cujas caixas são completadas com α_1 números 1, α_2 números 2, ..., α_m números m. Representaremos por a_{ij} o elemento que se encontra na (i,j)-ésima caixa de T_λ. A tabela é *semi-standard* se suas entradas não decrescem da esquerda para direita nas linhas e crescem de cima para baixo nas colunas. A tabela é *standard* se ela é semi padrão de índice $(1, \ldots, 1)$, isto é, todo inteiro $1, \ldots, n$ ocorre nela exatamente um única vez.

Exemplo 1.1.93. Seja $\lambda = (4,2,1)$ uma partição. As duas primeiras tabelas T_λ da esquerda são, respectivamente, *semi-standard* de índice $(2,3,1,1)$ e *standard*. E a terceira não é *semi-standard*.

1	1	2	4
2	2		
3			

1	3	6	7
2	4		
5			

1	2	3	4
6	5		
7			

Para uma partição $\lambda = (\lambda_1, \ldots, \lambda_k) \vdash n$, o grupo simétrico S_n age sobre o conjunto da λ-tabela de índices $(1, \ldots, 1)$ da seguinte maneira: Se (i,j)-ésima caixa da tabela T_λ contém o inteiro k, então a (i,j)-ésima caixa de σT_λ contém $\sigma(k)$, onde $\sigma \in S_n$. Dessa forma, temos:

Definição 1.1.94. Seja $\lambda = (\lambda_1, \ldots, \lambda_r) \vdash n$ e $\lambda' = (\lambda'_1, \ldots, \lambda'_s)$ a partição conjugada de λ.

1. O **estabilizador-linha** de uma tabela de Young T_λ é dado por:

$$R(T_\lambda) = S_{\lambda_1}(a_{11}, a_{12}, \ldots, a_{1\lambda_1}) \times \cdots \times S_{\lambda_r}(a_{r1}, a_{r2}, \ldots, a_{r\lambda_r}).$$

2. O **estabilizador-coluna** de uma tabela de Young T_λ é dado por:

$$C(T_\lambda) = S_{\lambda'_1}(a_{11}, a_{21}, \ldots, a_{\lambda'_1 1}) \times \cdots \times S_{\lambda'_s}(a_{1\lambda_1}, a_{2\lambda_1}, \ldots, a_{\lambda'_s\lambda_1}).$$

Observação 1.1.95. O estabilizador-linha $R(T_\lambda)$ de T_λ é o subgrupo de S_n que fixa os conjuntos de entradas de cada linha de T_λ. Analogamente, para o estabilizador-coluna $C(T_\lambda)$ de T_λ.

Exemplo 1.1.96. Sejam $\lambda = (3,2)$, $\sigma = (12)(345)$ e a seguinte tabela de Young T_λ.

1	4	2
5	3	

Logo

$$R(T_\lambda) = S_3(1,2,4) \times S_2(3,5),$$
$$C(T_\lambda) = S_2(1,5) \times S_2(3,4) \times S_1(2),$$

e a tabela σT_λ é dada por

2	5	1
3	4	

O próximo teorema nos fornece duas maneiras diferentes de se obter os graus das representações irredutíveis de S_n, utilizando uma partição de n, o conhecimento de suas tabelas *standard* e a ideia de gancho. Para uma demonstração veja [36].

Teorema 1.1.97. Seja λ uma partição de n, então:

1. A dimensão $d_\lambda = \dim M(\lambda)$ do S_n-módulo irredutível $M(\lambda)$ é igual ao número de λ-tabelas *standard*.

2. (**Fórmula do Gancho**)
$$d_\lambda = \frac{n!}{\prod(\lambda_i + \lambda'_j - i - j + 1)},$$
onde o produto corre em todas as caixas $(i,j) \in [\lambda]$, isto é, o denominador é igual ao produto dos tamanhos de todos os ganchos do diagrama $[\lambda]$.

Exemplo 1.1.98. Vamos calcular $\dim M(3,2)$, onde λ é uma partição de 5.

Primeira solução: Temos que existem cinco (3,2)-tabelas padrão dadas abaixo e utilizando (i) do Teorema 1.1.97 temos que $\dim M(3,2) = 5$.

1	2	3
4	5	

1	2	4
3	5	

1	2	5
3	4	

1	3	4
2	5	

1	3	5
2	4	

Segunda solução: Calculando os tamanhos dos ganchos do diagrama $[3,2]$ e colocando nas caixas do diagrama abaixo obtemos

4	3	1
2	1	

Portanto, utilizando (ii) do Teorema 1.1.97 temos que $\dim M(3,2) = \frac{5!}{4 \cdot 3 \cdot 1 \cdot 2 \cdot 1} = 5$.

1.2 Definições e resultados básicos sobre álgebras

Nesta seção iremos apresentar as definições básicas e alguns resultados importantes da teoria de álgebras, veremos alguns de seus tipos além de mostrar alguns exemplos. Comentaremos sobre álgebra livre e homomorfismos de álgebras. Principalmente, daremos a definição de álgebra de Grassmann, que é a álgebra base dessa dissertação.

Definição 1.2.1. Seja K um corpo qualquer. Um K-espaço vetorial A é chamado de **álgebra** (ou **K-álgebra**) se A possui uma relação binária $* : (A, A) \to A$, chamada de **multiplicação**, tal que $\forall a, b, c \in A$ e $\forall \alpha \in K$, temos:

1. $(a + b) * c = a * c + b * c$,
2. $a * (b + c) = a * b + a * c$,
3. $\alpha(a * b) = (\alpha a) * b = a * (\alpha b)$.

Percebemos da definição de álgebra, que ela generaliza tanto a noção de espaço vetorial quanto a de anel.

Definição 1.2.2. A **álgebra de grupo** KG de um grupo G sobre um corpo K é a álgebra associativa cujos os elementos são a combinação linear sobre K dos elementos de G. Como um conjunto e espaço vetorial temos para $x \in KG$,

$$x = \sum_{g \in G} a_g g \text{ , onde } a_g \in K.$$

A multiplicação é definida nos elementos da base pela operação do grupo G.

Daremos a seguir um exemplo de álgebra importante, pois ele mergulha uma álgebra A sem unidade para uma com unidade (ou seja, é um homomorfismo entre essas álgebras). Esta construção é chamada de **adjunção formal da unidade** à álgebra A.

Exemplo 1.2.3. Seja A uma álgebra sem unidade. Consideremos o espaço vetorial

$$K \oplus A = \{(k, a) \mid k \in K,\ a \in A\}.$$

Em $K \oplus A$ vamos definir o seguinte produto

$$(k_1, a_1) \cdot (k_2, a_2) = (k_1 k_2, k_1 a_2 + k_2 a_1 + a_1 a_2).$$

O conjunto $K \oplus A$ com este produto, é uma álgebra associativa com unidade (o elemento (1,0)).

A próxima proposição nos diz como definir uma multiplicação em um espaço vetorial V de modo a torná-lo uma álgebra.

Proposição 1.2.4. Se V é um espaço vetorial com base β e $f : \beta \times \beta \to V$ é uma função qualquer, então existe uma única função bilinear $F : A \times A \to A$ estendendo f.

Demonstração. Dado $v \in V$ temos que $v = \sum_{u\in\beta} k_u u$, onde $k_u \in K$ e o conjunto $\{u \in \beta | k_u \neq 0\}$ é finito. Assim, dados $v = \sum_{u\in\beta} k_u u$ e $w = \sum_{l\in\beta} k_l l$ pertencentes a V, defina a função $* : A \times A \to A$ da seguinte maneira:

$$v * w = \sum_{u,l\in\beta} k_u k_l f(u, v).$$

Temos que $*$ está bem definida, pois se $\sum_{u\in\beta} k_u u = \sum_{u\in\beta} k'_u u$ com $k_u, k'_u \in K$ então $k_u = k'_u$ para todo $u \in \beta$. Tomando agora $k \in K$ e $v_1 = \sum_{u\in\beta} k_u u$ $v_2 = \sum_{u\in\beta} k'_u u$ e $w = \sum_{l\in\beta} k_l l$ pertencentes a V temos:

$$\begin{aligned}(v_1 + v_2) * w &= \sum_{u\in\beta}(k_u + k'_u)u * \sum_{l\in\beta} k_l l \\ &= \sum_{u,l\in\beta}(k_u + k'_u)k_l f(u, l) \\ &= \sum_{u,l\in\beta} k_u k_l f(u, l) + \sum_{u,l\in\beta} k'_u k_l f(u, l) \\ &= (v_1 * w) + (v_2 * w)\end{aligned}$$

e

$$\begin{aligned}k(v_1 * w) &= \sum_{u,l\in\beta} k k_u k_l f(u, l) \\ &= \sum_{u\in\beta}(k k_u)u * \sum_{l\in\beta} k_l l \\ &= (k v_1) * v_2\end{aligned}$$

Analogamente mostra-se que $k(v_1 * w) = v_1 * (kw)$ e que $w * (v_1 + v_2) = (w * v_1) + (w * v_2)$, para quaisquer $v_1; v_2 \in V$. Logo $*$ é bilinear. Considerando agora $e_1, e_2 \in \beta$, temos que $e_1 = \sum_{u\in\beta} k_u u$, onde $k_u = 1$ se $e_1 = u$ e $k_u = 0$ se $u \neq e_1$. Fazendo o mesmo para e_2 temos $e_2 = \sum_{l\in\beta} k_l l$, onde $k_l = 1$ se $e_2 = l$ e $k_l = 0$ se $l \neq e_2$. Logo,

$$e_1 * e_2 = \sum_{u,l\in\beta} k_u k_l f(e_1, e_2) = k_{e_1} k_{e_2} f(e_1, e_2) = f(e_1, e_2)$$

donde temos que $*$ estende f.

Resta mostrar que $*$ é a única aplicação com esta propriedade. Para isto, suponhamos que existe $*_1 : A \times A \to A$ estendendo f. Daí devemos ter

$$a *_1 b = \sum_{u,l\in\beta} k_u k_l (u *_1 l) = \sum_{u,l\in\beta} k_u k_l f(u, l) = a * b$$

donde $*$ é igual a $*_1$ e segue o resultado. □

Logo, da Proposição 1.2.4, se a álgebra A tem uma base $\{e_i \,|\, i \in I\}$, então para definirmos a multiplicação em A é suficiente mostrar a multiplicação entre os elementos da base:

$$e_i * e_j = \sum_{k\in I} \alpha_{ij}^k e_k, \alpha_{ij}^k \in K,$$

onde para i e j fixos, apenas um número finito de α_{ij}^k são não nulos. E o inverso também vale, ou seja, podemos definir uma multiplicação em um espaço vetorial V da seguinte forma:

$$\left(\sum_{i\in I}\alpha_i e_i\right) * \left(\sum_{j\in I}\beta_j e_j\right) = \sum_{i,j\in I}\alpha_i\beta_j(e_i * e_j), e_i * e_j = \sum_{k\in I}\alpha_{ij}^k e_k.$$

Definição 1.2.5. Dados uma K-álgebra A e um conjunto $\beta = \{v_1, v_2, \ldots\}$, dizemos que A é uma **álgebra gerada pelo conjunto** β, se $\forall a \in A$, a pode ser escrito como uma soma finita da forma

$$\sum k_{i_1,\ldots,i_l} v_{i_1} \cdots v_{i_l},$$

onde $k_{i_1,\ldots,i_l} \in K$ e $v_{i_1} \in \beta$.

Denotaremos isto por: $A = \langle\beta\rangle$. Se β for um conjunto finito, diremos que A é uma álgebra **finitamente gerada** por β.

Dependendo de certas propriedades que a álgebra possui podemos classificá-las de acordo com a seguinte definição:

Definição 1.2.6. Seja A uma álgebra sobre K, então:

1. A é **associativa** se $(a * b) * c = a * (b * c)$, $\forall a, b, c \in A$;
2. A é **comutativa** se $a * b = b * a$, $\forall a, b \in A$; e
3. A é **unitária** se A tem um elemento 1 tal que $a * 1 = 1 * a = a$, $\forall a \in A$.

A classe de álgebra que definiremos a seguir desempenha um papel importante, pois ela possui muitas aplicações tanto na matemática quanto na física.

Definição 1.2.7. A é uma **Álgebra de Lie** se $\forall a, b, c \in A$, temos:

1. $a * a = 0$ (Lei Anticomutativa)
2. $(a * b) * c + (b * c) * a + (c * a) * b = 0$ (Identidade de Jacobi)

- A lei anticomutativa implica que

  $$a * b = -b * a \quad \forall a, b \in A.$$

  Com efeito, temos que: $0 = (a+b)*(a+b) = a*a+a*b+b*a+b*b = a*b+b*a \Rightarrow a*b = -b*a$.

- Se $\mathrm{car}(K) \neq 2$ então a lei anticomutativa é equivalente a

  $$a * b = -b * a \quad \forall a, b \in A.$$

  De fato, pelo parágrafo anterior só falta provar a volta da equivalência, logo de $a*b = -b*a$ e fazendo $b = a$ temos que: $a * a = -a * a \Rightarrow 2(a * a) = 0 \Rightarrow a * a = 0$.

Assim como para grupos e anéis, existem certos subconjuntos de uma álgebra de A que também são álgebras. Isto nos leva a seguinte definição:

Definição 1.2.8. O subespaço S da álgebra A é chamado de **subálgebra** se ele é fechado em relação à multiplicação.

Exemplo 1.2.9. $M_n(K)$ é a álgebra das matrizes $n \times n$ com entradas em K sob a multiplicação usual das matrizes e que tem como uma subálgebra o conjunto $UT_n(K)$ das matrizes triangulares superiores $n \times n$ sobre K.

A definição a seguir é importante pois apresenta uma subálgebra de uma álgebra A que é sempre comutativa.

Definição 1.2.10. É chamado de **centro** $Z(A)$ de uma álgebra A, o subconjunto de A definido por

$$Z(A) := \{a \in A \,|\, ab = ba \,\forall b \in A\}.$$

Se a álgebra A é unitária, então $K \subset Z(A)$. E se $Z(A) = K$ então A é chamada de **álgebra central**.

Temos que $Z(A)$ é uma subálgebra de A.

Exemplo 1.2.11. Toda matriz escalar $A \in M_n(K)$ é central.
Com efeito, como A é uma matriz escalar, temos que:

$$A = k\mathrm{Id},\ k \in K.$$

E portanto, $\forall B \in M_n(K)$:

$$AB = (k\mathrm{Id})B = k(\mathrm{Id}B) = k(B\mathrm{Id}) = B(k\mathrm{Id}) = BA,$$

onde a penúltima igualdade é válida devido ao número 3 da definição de álgebra (Definição 1.2.1).

A próxima proposição é uma ferramenta que será utilizada mais tarde:

Proposição 1.2.12 (Argumento de Vandermonde). Suponha que são dados os elementos $x_1, \ldots, x_{d+1} \in Z(A)$ e $v_1, \ldots, v_{d+1} \in A$ tal que para cada i, $1 \leq i \leq d+1$, temos que $\sum_{j=1}^{d+1} x_i^{j-1} v_j = 0$. Então $|x_1, \ldots, x_{d+1}| v_j = 0$ para todo j. Em particular, se $Ann_A|x_1, \ldots, x_{d+1}| = 0$ então cada $v_j = 0$. Onde $|x_1, \ldots, x_{d+1}|$ denota o determinante da matriz de Vandermonde dos elementos $x_1, \ldots, x_{d+1}$.

Demonstração. Seja $V = \begin{bmatrix} v_1 \\ \vdots \\ v_{d+1} \end{bmatrix}$.
Escrevendo as hipóteses na forma matricial, temos que $XV = 0$. Mas $X \in M_n(Z(A))$, então multiplicando à esquerda pela adjunta da matriz X temos que:

$$0 = \det(X)V = |x_1, \ldots, x_{d+1}|V.$$

□

Definição 1.2.13. O subespaço I de A é chamado de um **ideal á esquerda** de A se $AI \subset I$, ou seja, $\forall a \in A$ e $\forall i \in I \Rightarrow ai \in I$. Similarmente definimos um **ideal á direita**.

Se $I \neq A$, observamos da definição acima que I é uma subálgebra não unitária de A.

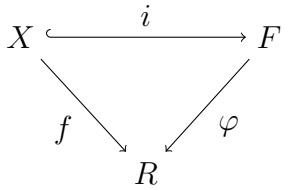
Definição 1.2.14. Um **ideal bilateral** (ou simplesmente um ideal) da álgebra A é um ideal á direita e á esquerda ao mesmo tempo, notação $I \lhd A$.

A próxima definição nos informa qual é a menor álgebra que contém um conjunto qualquer X.

Definição 1.2.15. A **subálgebra gerada por um subconjunto X** de uma álgebra A, denotada por $[X]$, é a menor subálgebra que contém esse conjunto, isto é, $[X]$ é a interseção de todas as subálgebras de A que contém X.

Definição 1.2.16. Seja $\aleph$ uma classe de álgebras e seja $F \in \aleph$ uma álgebra gerada pelo conjunto X. A álgebra F é chamada de **álgebra livre na classe $\aleph$, livremente gerada por** X, se para qualquer álgebra $R \in \aleph$, toda aplicação $f : X \to R$ pode ser estendida a um homomorfismo de álgebras $\varphi : F \to R$. A cardinalidade $|X|$ do conjunto X é chamada de **posto de** F.

Portanto, da última definição, temos que o diagrama abaixo comuta, ou seja, $f = \varphi \circ i$, onde i é a inclusão.



Chamaremos $K\langle X\rangle$ de a **K-álgebra dos polinômios nas variáveis** x_j, com a multiplicação sendo associativa, mas não comutativa. Em outras palavras, $K\langle X\rangle$ é a K-álgebra que possui por base, como espaço vetorial, a união de 1 com o conjunto formado por todos os monômios da forma $x_{i_1}x_{i_2}\cdots x_{i_k}$; $k \in \mathbb{N}$ e cada i_j um inteiro positivo menor ou igual a $|X|$, podendo ocorrer repetição de índices.
O resultado da multiplicação entre dois monômios $x_{i_1}x_{i_2}\cdots x_{i_k}$ e $x_{j_1}x_{j_2}\cdots x_{j_l}$ é o monômio

$$x_{i_1}x_{i_2}\cdots x_{i_k}x_{j_1}x_{j_2}\cdots x_{j_l}$$

e que se estende por linearidade para todos os elementos de $K\langle X\rangle$.

Exemplo 1.2.17. Para todo conjunto X a álgebra $K\langle X\rangle$ é uma álgebra livre na classe de todas as álgebras associativas unitárias.
De fato, seja A uma álgebra associativa unitária e seja $f : X \to A$ uma aplicação qualquer. Para cada inteiro positivo i (menor ou igual a $|X|$ no caso em que X é finito) denotamos por a_i a imagem de x_i pela f. Então, dado $p(x_1, \ldots, x_k) \in K\langle X\rangle$, para que φ estenda f, definimos $\varphi(p) = p(a_1, \ldots, a_k)$, obtido a partir de p substituindo-se cada x_i por a_i em p. Claramente, φ é homomorfismo.

Em relação à álgebra livre do último exemplo, podemos fazer as seguintes nomenclaturas:

Definição 1.2.18. Seja X um conjunto não vazio, cujos elementos são chamados de **letras ou símbolos** então definimos:

1. X será chamado **alfabeto**.

2. Uma sequência finita de letras de X, será chamada de **palavra** e o conjunto dessas palavras será denotado por X'.

3. O número de letras de cada palavra $p \in X'$ será chamado de **comprimento da palavra p**. A palavra de comprimento zero será chamada de **palavra vazia**.

4. Uma palavra $p' \in X'$ será chamada de **sub-palavra** de uma palavra $p \in X'$ se existirem palavras p_1 e p_2 em X' tais que $p = p_1 p' p_2$.

5. Dadas $v = a_1 \cdots a_m$ e $w = b_1 \cdots b_n$, palavras em X', a operação binária de $X' \times X'$ em X' definida por $vw = a_1 \cdots a_m b_1 \ldots b_n$ é chamada de **concatenação ou justaposição**.

6. Podemos definir uma relação de ordem em X' da seguinte forma: Sejam $v = x_{i_1} \cdots x_{i_m}$ e $w = x_{j_1} \cdots x_{j_n}$ palavras em X', então diremos que $v \leq w$ se um dos três seguintes casos ocorre:

   (a) $v = w$, ou seja, $m = n$ e $i_t = j_t$, para $t = 1, 2, \ldots, n$.

   (b) Se $\exists l > 0$ tal que se $r \in \{1, 2, \cdots, l\}$ temos $i_r = j_r$ e $i_{l+1} < j_{l+1}$.

   (c) Se $m > n$ e $i_t = j_t$, para todo $1 \leq t \leq n$.

   Diremos também que $v < u$ se $v \leq u$ e $v \neq w$. Esta relação de ordem é chamada de **ordem lexicográfica**.

A próxima definição nos fala, mais especificamente, como são os elementos de $K\langle X \rangle$.

Definição 1.2.19. Sejam $X = \{x_1, x_2, \ldots\}$ um alfabeto enumerável e K um corpo. Considere um espaço vetorial $K\langle X \rangle$ sobre K com base $\{u, 1\}$ onde u são todos os monômios (definidos abaixo) sobre X, 1 é a unidade de K e a multiplicação é a concatenação. Observe que o número 5. da última definição nos diz que esta multiplicação é associativa.

1. A soma $p(X) = p(x_1, \ldots, x_n) = \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_m w_m$, onde $\alpha_i \in K$ e $w_i = x_1^{k_1} \cdots x_n^{k_n} \in X'$ com cada $k_j \geq 0$, é chamada de **polinômio**. No caso em que $m = 1$, $p(X)$ é chamado de **monômio**. Cada x_j é conhecido por uma **indeterminada ou variável** de $p(X)$.

2. O **grau de um monômio** αw com $\alpha \in K$, $\alpha \neq 0$, e $w \in X'$, que denotaremos por $\mathrm{gr}(\alpha w)$, é o comprimento da palavra w. O **grau de um polinômio** $p(X)$ será o grau máximo de seus monômios.

3. Diremos que um monômio αw com $\alpha \in K$ e $w \in X'$ tem tipo $(n_1, \ldots, n_k)$ se a palavra w contém x_i exatamente n_i vezes, $n_k \neq 0$ e $n_i = 0$ para todo $i > k$. Diremos que o número n_i é o **grau do monômio** αw em x_i.

4. Diremos que um polinômio é **homogêneo em** x_i, com grau n_i, se todos os seus monômios têm grau n_i em x_i. Diremos também que um polinômio é **homogêneo de grau (ou do tipo)** $(n_1, \ldots, n_k)$ se todos os seus monômios são do mesmo grau, $(n_1, \ldots, n_k)$.

5. Se agruparmos os monômios do mesmo tipo em qualquer polinômio p, ele se escreve como uma soma de polinômios homogêneos. Estes polinômios serão chamados de **as componentes homogêneas de p.**

6. Um polinômio homogêneo em x_i com grau 1 em x_i é chamado de **polinômio linear** em x_i. Um polinômio homogêneo do tipo $(n_1, \ldots, n_k)$, onde $n_i = 0$ ou $n_i = 1$ para cada i, é chamado de **polinômio multilinear**.

Chamaremos o conjunto $K\langle X\rangle$ de **álgebra associativa livre unitária livremente gerada por** X e o conjunto $K\langle x_1, \ldots, x_n\rangle$ de **álgebra associativa livre unitária livremente gerada por** $\{x_1, \ldots, x_n\}$.

Assim como para espaços vetoriais, grupos e anéis temos também para álgebras, a seguinte definição de homomorfismo:

Definição 1.2.20. A aplicação $\phi : A_1 \to A_2$ das álgebras A_1 e A_2 é chamada de **Homomorfismo de álgebras** se somente se ϕ é um homomorfismo dos espaços vetoriais A_1 e A_2 e se vale que $\phi(a * b) = \phi(a) * \phi(b)$, $\forall a \in A_1$ e $\forall b \in A_2$. Se A_1 e A_2 são unitárias, ϕ deve ainda satisfazer a $\phi(1_{A_1}) = 1_{A_2}$.

Continuaremos usando a nomenclatura de isomorfismo, automorfismo, endomorfismo, entre outros, para o caso de álgebras. Os teoremas de homomorfismos de espaços vetoriais, grupos e anéis também são válidos para álgebras. Como por exemplo:

Teorema 1.2.21. (**Teorema do Homomorfismo**) Seja $\phi : A \to B$ um homomorfismo de álgebras. Então $\mathrm{Ker}(\phi)$ é um ideal bilateral de A e a álgebra quociente $A/\mathrm{Ker}(\phi)$ é isomorfa à $\mathrm{Im}(\phi)$.

Demonstração. Seja $v \in \mathrm{Ker}(\phi)$, então para todo $a \in A$ temos que:

$$\phi(av) = \phi(a)\phi(v) = \phi(a)0 = 0.$$

Logo $av \in \mathrm{Ker}(\phi)$. Análogo para va. Portanto $\mathrm{Ker}(\phi) = \{v \in A \,|\, \phi(v) = 0\}$ é um ideal bilateral de A.
Agora tome a função $\bar{\phi} : A/\mathrm{Ker}(\phi) \to \mathrm{Im}(\phi)$ definida por:

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

Observe que ela está bem definida, pois se a_1 e a_2 pertencem a A e $\bar{a_1} = \bar{a_2}$, então $a_1 - a_2 \in \mathrm{Ker}(\phi)$, logo $\phi(a_1 - a_2) = 0$, mas como ϕ é homomorfismo temos que $\phi(a_1) = \phi(a_2)$.
Agora, note que ϕ é injetora, pois $\mathrm{Ker}(\bar{\phi}) = \{\bar{a} \in A/\mathrm{Ker}(\phi) \,|\, \phi(a) = 0\} = \{\bar{a} \in A/\mathrm{Ker}(\phi) \,|\, a \in \mathrm{Ker}(\phi)\} = \{\bar{0}\}$. E $\bar{\phi}$ é sobrejetora pois se $b \in \mathrm{Im}(\phi)$ então existe um elemento $a_b \in A$, tal que $\phi(a_b) = b$, logo $\bar{\phi}(\bar{a}_b) = \phi(a_b) = b$. □

Definição 1.2.22. Sejam V e W espaços vetoriais com bases $\{v_i \,|\, i \in I\}$ e $\{w_j \,|\, j \in J\}$, respectivamente. O **Produto Tensorial** $V \otimes W = V \otimes_K W$ de V e W é o espaço vetorial com base $\{v_i \otimes w_j \,|\, i \in I, j \in J\}$, que vale:

$$\left(\sum_{i\in I} \alpha_i v_i\right) \otimes \left(\sum_{j\in J} \beta_j w_j\right) = \sum_{i\in I}\sum_{j\in J} \alpha_i\beta_j (v_i \otimes w_j), \alpha_i, \beta_j \in K.$$

Da Proposição 1.2.4, se V e W são álgebras então $V \otimes W$ também é uma álgebra com multiplicação dada por

$$(v_i \otimes w_j)(v_i' \otimes w_j') = (v_i v_i') \otimes (w_j w_j), v_i, v_i' \in V \, e \, w_j, w_j' \in J.$$

Definiremos a seguir a álgebra base dessa dissertação.

Definição 1.2.23. Seja V um K-espaço vetorial com base ordenada $\{e_i \,|\, i \in I\}$. A **álgebra de Grassmann** (ou exterior) de V é a álgebra associativa gerada por $\{e_i \,|\, i \in I\}$ e com a seguinte relação $e_i e_j + e_j e_i = 0$, onde $i, j \in I$ e $e_i^2 = 0$ se $\text{car}(K) = 2$. Esta álgebra será denotada por $E(V)$.

Isto significa que a álgebra de Grassmann é isomorfa à álgebra quociente $K\langle X\rangle / J$, onde $X = \{x_i \,|\, i \in I\}$ e o ideal J é gerado por $x_i x_j + x_j x_i$, onde $i, j \in I$. Se a dimensão de V é enumerável, podemos assumir que V tem base $\{e_1, e_2, \ldots\}$.

Temos que, uma base para a **álgebra de Grassmann unitária** (denotada por $E(V)$) é dada por $\beta = \{1\} \cup \{e_{i_1} e_{i_2} \cdots e_{i_k} | \, k \geq 1; i_1 < i_2 < \cdots < i_k\}$. E uma base para a **álgebra de Grassmann não unitária** (denotada por $E^*(V)$) é dada por $\beta^* = \{e_{i_1} e_{i_2} \cdots e_{i_k} | \, k \geq 1; i_1 < i_2 < \cdots < i_k\}$.

Para um elemento de β definimos seu **comprimento** como sendo o número de fatores e_j que o formam, consideramos que o elemento 1 tem comprimento 0.

Observação 1.2.24. Denotando por $E_0(V)$ o subespaço da álgebra de Grassmann gerado pelos elementos de β que possuem comprimento par e por $E_1(V)$ o subespaço gerado pelos elementos de β que possuem comprimento ímpar, temos que $E(V) = E_0(V) \oplus E_1(V)$.

1.3 Álgebras com Identidades Polinomiais

Nesta seção falaremos sobre álgebras com identidades polinomiais e a relacionaremos com a noção de variedades de álgebras e álgebras relativamente livres. Apresentaremos alguns exemplos dessas álgebras, principalmente a álgebra de Grassmann, além de definir o que vem a ser T-ideal, variedades e de exibir alguns teoremas importantes acerca destes assuntos.

Fixaremos $X = \{x_1, x_2, \ldots\}$ como um conjunto infinito enumerável.

As duas próximas definições são muito importantes, pois elas vão caracterizar a principal álgebra desse trabalho.

Definição 1.3.1. Seja $f = f(x_1, \ldots, x_n) \in K\langle X\rangle$ e seja A uma álgebra associativa, diremos que $f = 0$ (ou somente f) é uma **identidade polinomial** para A se $f(a_1, \ldots, a_n) = 0$ para todo $a_1, \ldots, a_n \in A$.

Definição 1.3.2. Se A satisfaz uma identidade polinomial não nula então A é chamada de **PI-álgebra**.

Observação 1.3.3. Sub-álgebras de PI-álgebras são PI-álgebras.

Apresentaremos agora, algumas identidades polinomiais importantes na teoria de PI-álgebra e exemplos de álgebras que são satisfeitas por elas.

Definição 1.3.4. Definimos o **comutador de Lie** como o polinômio

$$[x_i, x_j] = x_i x_j - x_j x_i, \, \forall x_i, x_j \in A.$$

Definição 1.3.5. O **comutador de Lie de comprimento** $n \geq 2$ é definido indutivamente por:

1. $[x_1, x_2] = x_1 x_2 - x_2 x_1$,
2. $[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n], \; n \geq 3$.

Exemplo 1.3.6. Toda álgebra comutativa A satisfaz a identidade polinomial $[x_1, x_2] = 0$.
Com efeito, $\forall a, b \in A$ temos que $[a, b] = ab - ba = ab - ab = 0$

O próximo exemplo é muito importante para este trabalho, pois nos fornece uma identidade polinomial para a álgebra de Grassmann $E(V)$, ou seja, $E(V)$ **é uma PI-álgebra**.

Exemplo 1.3.7. A álgebra de Grassmann $E(V)$ é uma PI-álgebra pois satisfaz a identidade polinomial $[x_1, x_2, x_3] = 0$.
Com efeito, como $[x_1, x_2, x_3]$ é um polinômio multilinear, basta provarmos para a base de $E(V)$. Tomemos três vetores da base da álgebra de Grassmann quaisquer, a saber, $a_1 = e_{i_1} \cdots e_{i_r}$, $a_2 = e_{j_1} \cdots e_{j_s}$ e $a_3 = e_{k_1} \cdots e_{k_t}$. Sabemos que $e_u e_v = -e_v e_u$, logo:

$$[a_1, a_2] = (e_{i_1} \cdots e_{i_r})(e_{j_1} \cdots e_{j_s}) - (e_{j_1} \cdots e_{j_s})(e_{i_1} \cdots e_{i_r}) = (1 - (-1)^{rs})\, e_{i_1} \cdots e_{i_r} e_{j_1} \cdots e_{j_s}$$

onde a potência rs indica o número mínimo de transposições necessárias para colocar os índices de $a_2 a_1$ de forma crescente. A expressão anterior se anula para r ou s pares, pois teríamos que rs é par, logo $1 - (-1)^{rs} = 1 - 1 = 0$. Ou seja, $[a_1, a_2] = 0$ se a_1 ou a_2 tem comprimento par. Suponha, então, que a_1 e a_2 tenham ambos comprimento ímpar. Desta forma, $[a_1, a_2]$ será uma combinação não nula de dois monômios de comprimento par. Portanto, $[[a_1, a_2], a_3] = 0$, qualquer que seja o comprimento de a_3. Logo, o polinômio $[[x_1, x_2], x_3]$ é uma identidade polinomial para a álgebra de Grassmann.

Definição 1.3.8. O **polinômio de Hall** é definido por:

$$[[x, y]^2, z] = 0.$$

Exemplo 1.3.9. A álgebra $M_2(K)$ das matrizes 2×2 sobre K satisfaz o polinômio de Hall. De fato, se $A \in M_2(K)$ então seu polinômio característico é $x^2 + \mathrm{tr}(A)x + \det(A)\mathrm{Id} = 0$; onde Id é a matriz identidade 2×2. Se $A = [B; C]$, para $B; C \in M_2(K)$, então $\mathrm{tr}(A) = 0$, e então $A^2 + \det(A)\mathrm{Id} = 0$, ou seja, $A^2 = -\det(A)\mathrm{Id}$. Assim, o quadrado de um comutador é uma matriz escalar e, portanto $[A^2; D] = 0$, para todo $D \in M_2(K)$, pois $\mathrm{Id} \in Z(M_2(K))$.

A seguinte definição nos apresenta dois polinômios que desempenham papéis importantes em PI-álgebra, como veremos nos próximos capítulos.

Definição 1.3.10. 1. O **polinômio unitário** é definido por:

$$u_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} x_{\sigma(1)} \cdots x_{\sigma(n)}.$$

2. O **polinômio** *standard* **de grau** n é definido por:

$$s_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) x_{\sigma(1)} \cdots x_{\sigma(n)}$$

onde $\mathrm{sgn}(\sigma) = 1$ se σ é uma permutação par e $\mathrm{sgn}(\sigma) = -1$ se σ é uma permutação ímpar.

Exemplo 1.3.11. Seja A uma álgebra associativa de dimensão finita e $\dim(A) < n$. Então A satisfaz o polinômio *standard* de grau n.
De fato, uma vez que o polinômio *standard* é multilinear, basta verificar que s_n se anula nos elementos da base de A. Quando escolhemos n elementos da base, pelo menos um deles se repete. Logo, como s_n é um polinômio anti-simétrico, ele se anula para essa escolha.

O próximo lema nos dará uma decomposição de S_n, que será usada mais adiante.

Lema 1.3.12. Para todo $n \geq 2$ temos:

$$s_n(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} (-1)^{i-1}\ x_i\ s_{n-1}(x_1, \ldots, \hat{x_i}, \ldots, x_n),$$

onde $\widehat{x_i}$ significa que o elemento x_i foi excluído do polinômio s_{n-1}.

Demonstração. Com efeito:

$$\begin{aligned}
s_n(x_1, x_2, \ldots, x_n) &= \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) x_{\sigma(1)} \cdots x_{\sigma(n)} \\
&=^{(1)} \sum_{\tau \in S_{n-1}} x_1 \mathrm{sgn}(\tau) x_{\tau(2)} \cdots x_{\tau(n)} + \sum_{\tau \in S_{n-1}} -x_2 \mathrm{sgn}(\tau) x_{\tau(1)} \widehat{x_{\tau(2)}} \cdots x_{\tau(n)} \\
&\quad + \cdots + \sum_{\tau \in S_{n-1}} (-1)^{n-1} x_n \mathrm{sgn}(\tau) x_{\tau(1)} \cdots x_{\tau(n-1)} \\
&= \sum_{i=1}^{n} (-1)^{i-1} x_i \sum_{\tau \in S_{n-1}} \mathrm{sgn}(\tau) x_{\tau(1)} \cdots \widehat{x_{\tau(i)}} \cdots x_{\tau(n)} \\
&= \sum_{i=1}^{n} (-1)^{i-1} x_i s_{n-1}(x_1, \ldots, \widehat{x_i}, \ldots, x_n).
\end{aligned}$$

(1) Agrupamos as somas onde os primeiros elementos eram $x_1, \ldots, x_n$, respectivamente. E como o índice i não participa da permutação τ temos que o sinal da nova permutação dos índices restantes fica alterado pelo seu sinal $(-1)^{i-1}$, pois a nova permutação tem menos $i-1$ ciclos. □

As duas definições a seguir são de tipos especiais de álgebras, que como veremos nos exemplos, também são PI-álgebras.

Definição 1.3.13. Uma álgebra associativa sem unidade A é chamada de **nil álgebra** se para todo $v \in A$ existe um número n natural tal que $v^n = 0$. Se existir um número fixo n tal que $v^n = 0$ para todo $v \in A$ então A é chamada de **nil álgebra de índice limitado** n.

Exemplo 1.3.14. Toda nil álgebra associativa com índice limitado n é uma PI-álgebra pois satisfaz a identidade polinomial $p(x) = x^n = 0$.

Definição 1.3.15. Uma álgebra associativa A é chamada de **nilpotente de classe** $\leq n$ se existe um número natural fixo n tal que $A^n = 0$, ou seja, $x_1 \cdots x_n = 0$ para todo $x_i \in A$.

Exemplo 1.3.16. Toda álgebra nilpotente, com índice de nilpotência n, é uma PI-álgebra pois satisfaz a identidade polinomial $p(x_1, \ldots, x_n) = x_1 \cdots x_n = 0$.

Definição 1.3.17. Seja A uma álgebra associativa unitária. Um polinômio $f \in K\langle X\rangle$ é chamado de **polinômio próprio**, se ele é uma combinação linear de produto de comutadores nos geradores de X, isto é:

$$f(x_1, \ldots, x_m) = \sum \alpha_{i,\ldots,j}[x_{i_1}, \ldots, x_{i_p}] \cdots [x_{j_1}, \ldots, x_{i_q}], \quad \alpha_{i,\ldots,j} \in K.$$

A partir de agora, utilizaremos as seguintes notações:

- P_n - o K**-espaço vetorial de todos os polinômios em** $K\langle X\rangle$ **que são multilineares de grau** n;
- B - o K**-espaço vetorial de todos os polinômios próprios em** $K\langle X\rangle$;
- B_m - o K**-espaço vetorial dos polinômios próprios em** m **variáveis**; e
- Γ_n - o K**-espaço vetorial de todos os polinômios próprios multilineares de grau** n, isto é:

$$B_m = B \cap K\langle x_1, \ldots, x_m\rangle, \; m = 1, 2, \ldots \quad \text{e} \quad \Gamma_n = B \cap P_n, \; n = 0, 1, \ldots.$$

Veremos agora, um exemplo de uma subálgebra da álgebra $M_n(K)$ que é uma PI-álgebra.

Exemplo 1.3.18. Seja $UT_n(K)$ a álgebra das matrizes triangulares superiores $n \times n$ sobre K. Então $UT_n(K)$ é uma PI-álgebra pois satisfaz a identidade

$$[x_1, x_2] \cdots [x_{2n-1}, x_{2n}] = 0.$$

Com efeito, suponha que $[x_1, x_2] \cdots [x_{2n-1}, x_{2n}]$ não é uma identidade para $UT_n(K)$, logo existem $A_1, \ldots, A_{2n} \in UT_n(K)$ tal que $A = [A_1, A_2] \cdots [A_{2n-1}, A_{2n}] \neq 0$. Isto implica que existe (i, j) tal que $[A]_{ij} \neq 0$. Seja $B_k = [A_{2k-1}, A_{2k}]$ para todo $k = 1, \ldots, n$. Logo, temos que o elemento $[A]_{ij}$ é igual a $[B]_{ij_1}[B]_{j_1j_2}[B]_{j_2j_3} \cdots [B]_{j_{n-1}j}$, com $i < j_1 < j_2 < \cdots < j_{n-1} < j$. Mas isto é um absurdo, pois temos $n + 1$ números diferentes para i, j porém a matriz tem índice n. Logo $[x_1, x_2] \cdots [x_{2n-1}, x_{2n}]$ é uma identidade para $UT_n(K)$.

Exemplo 1.3.19. Sendo A uma álgebra finita, sobre um corpo finito K, mostraremos que A satisfaz uma identidade polinomial não trivial em uma variável.
Com efeito, como a álgebra A é finita, para cada elemento $r \in A$ existem $k > l$ tais que $r^k = r^l$. Portanto definindo $f_r(x) = x^k - x^l$, temos $f_r(r) = 0$. Como R é um conjunto finito podemos definir

$$g(x) = \prod_{r \in A} f_r(x)$$

que é uma identidade polinomial para A.

A seguir, definiremos um tipo de polinômio que não se anula em uma álgebra A, mas toma valores centrais dentro desta álgebra.

Definição 1.3.20. Seja A uma álgebra. O polinômio $c(x_1, \ldots, x_n) \in K\langle X \rangle$ é chamado de **polinômio central** de A se $c(x_1, \ldots, x_n)$ não tem o termo constante, se para toda escolha de $r_1, \ldots, r_n \in A$, $c(r_1, \ldots, r_n)$ pertence ao centro de A e se $c(x_1, \ldots, x_n)$ não é um identidade polinomial de A.

Exemplo 1.3.21. O polinômio $c(x_1, x_2) = [x_1, x_2]^2$ é central para a álgebra $M_2(K)$.
Com efeito, se x_1 e x_2 são matrizes em $M_2(K)$, então a matriz $[x_1, x_2]$ tem traço zero. Observe que se $x = \begin{bmatrix} a & b \\ c & -a \end{bmatrix}$ é uma matriz com traço zero, temos:
$x^2 = \begin{bmatrix} a^2 + bc & ab - ba \\ ca - ac & cb + a^2 \end{bmatrix} = \begin{bmatrix} a^2 + bc & 0 \\ 0 & cb + a^2 \end{bmatrix} = (a^2 + bc) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, pois K é um corpo logo, ele é comutativo.
Ou seja, toda matriz de traço zero em $M_2(K)$ quando elevada ao quadrado é igual a uma matriz escalar, logo estará no centro de $M_2(K)$. Portanto $c(x_1, x_2) = [x_1, x_2]^2$ está no centro de $M_2(K)$, possui o termo constante nulo e se fizermos $x_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ e $x_2 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ temos que $c(x_1, x_2) = [x_1, x_2]^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ logo $c(x_1, x_2)$ não é uma identidade de $M_2(K)$.

O próximo exemplo nos mostrará que a álgebra de Grassmann possui um polinômio central.

Exemplo 1.3.22. O polinômio $[x_1, x_2]$ é um polinômio central para a álgebra de Grassmann.
De fato, o polinômio acima não tem termo constante pois ele é igual a $x_1x_2 - x_2x_1$. No Exemplo 1.3.7 da página 33, vimos que se x_1 ou x_2 tiver comprimento par então $[x_1, x_2] = 0$ e se x_1 e x_2 tiverem comprimento ímpar então $[x_1, x_2]$ tem comprimento par, de qualquer forma temos que $[x_1, x_2] \in Z(E(V))$ quaisquer que sejam $x_1, x_2 \in E(V)$. Agora tome dois elementos $a_1 = e_{i_1} \cdots e_{i_r}$ e $a_2 = e_{j_1} \cdots e_{j_s}$ da base de $E(V)$, onde todos os elementos e_k de a_1 e a_2 são diferentes e r e s são números ímpares. Sabemos que $e_u e_v = -e_v e_u$, logo:

$$\begin{aligned} [a_1, a_2] &= (e_{i_1} \cdots e_{i_r})(e_{j_1} \cdots e_{j_s}) - (e_{j_1} \cdots e_{j_s})(e_{i_1} \cdots e_{i_r}) \\ &= (1 - (-1)^{rs})\, e_{i_1} \cdots e_{i_r} e_{j_1} \cdots e_{j_s} \\ &= 2 e_{i_1} \cdots e_{i_r} e_{j_1} \cdots e_{j_s} \\ &\neq 0. \end{aligned}$$

A próxima definição desempenha um papel importante em PI-álgebra, pois nos fornece um conjunto que é invariante sobre todos os endomorfismos de $K\langle X\rangle$.

Definição 1.3.23. Dizemos que um ideal I de $K\langle X\rangle$ é um **T-ideal** se $\phi(I) \subset I$ para todo $\phi \in End(K\langle X\rangle)$, ou seja, $f(g_1, \ldots, g_n) \in I$ para quaisquer $f(x_1, \ldots, x_n) \in I$ e $g_1, \ldots, g_n \in K\langle X\rangle$.

Veremos a seguir um tipo especial de T-ideal.

Definição 1.3.24. Um T-ideal T é chamado de **T-primo** se para todos os T-ideais A, B tal que $AB \subset T$ temos que $A \subset T$ ou $B \subset T$.

O próximo teorema é importante, pois ele nos diz que o conjunto $\mathrm{T}(A)$ de todas as identidades polinomiais de A não é um subconjunto qualquer do conjunto $K\langle X\rangle$.

Teorema 1.3.25. O conjunto $\mathrm{T}(A)$ de todas as identidades polinomiais satisfeitas pela álgebra A é um ideal de $K\langle X\rangle$.

Demonstração. Sejam $f \in \mathrm{T}(A)$ e $g \in K\langle X\rangle$, logo para todo $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_m) \in X$ temos:

$$f(a_1, \ldots, a_n)\, g(b_1, \ldots, b_m) = 0\, g(b_1, \ldots, b_m) = 0$$

ou seja, $\mathrm{T}(A)K\langle X\rangle \subset \mathrm{T}(A)$. Análogo para $K\langle X\rangle\mathrm{T}(A) \subset \mathrm{T}(A)$. □

Definição 1.3.26. O conjunto $\mathrm{T}(A)$ do último teorema é chamado de **T-ideal de** A (ou **Ideal das Identidades** da álgebra A).

O próximo teorema nos revela porque o ideal $\mathrm{T}(A)$ é importante na Teoria das PI-álgebras.

Teorema 1.3.27. O ideal $\mathrm{T}(A)$ é um T-ideal de $K\langle X\rangle$. E, reciprocamente, se I é um T-ideal de $K\langle X\rangle$, então existe alguma álgebra B tal que $\mathrm{T}(B) = I$.

Demonstração. Sejam a álgebra A e $f(x_1, \ldots, x_n) \in \mathrm{T}(A)$ e ϕ um endomorfismo de $K\langle X\rangle$. Como $f(a_1, \ldots, a_n) = 0$ para todo $a_1, \ldots, a_n \in A$ temos que $\phi(f(x_1, \ldots, x_n)) = f(\phi(x_1), \ldots, \phi(x_n)) = 0$. Logo $\phi(f(x_1, \ldots, x_n)) \in \mathrm{T}(A)$, ou seja, $\phi(\mathrm{T}(A)) \subset \mathrm{T}(A)$ e $\mathrm{T}(A)$ é um T-ideal de $K\langle X\rangle$.

Seja I um T-ideal de $K\langle X\rangle$. Tomemos a álgebra quociente $B = K\langle X\rangle / I$ e a projeção canônica $\pi : K\langle X\rangle \to B$. Se $f \in \mathrm{T}(B)$, então $f \in Ker(\pi)$. Como $Ker(\pi) = I$, temos $\mathrm{T}(B) \subset I$. Por outro lado, se $f(x_1, \ldots, x_n) \in I$ e $g_1, \ldots, g_n \in K\langle X\rangle$, então $f(g_1, \ldots, g_n) \in I$ e daí $f(\overline{g_1}, \ldots, \overline{g_n}) = \overline{f(g_1, \ldots, g_n)} = 0$, onde o elemento que está sob a barra pertence a I. Logo, $f \in \mathrm{T}(B)$ e o teorema está demonstrado. □

Definição 1.3.28. Se A_1 e A_2 são álgebras tais que $\mathrm{T}(A_1) = \mathrm{T}(A_2)$, dizemos que A_1 e A_2 são **PI-equivalentes**.

Pode ocorrer que duas álgebras não-isomorfas satisfaçam o mesmo conjunto de identidades polinomiais. Portanto, ás vezes, é mais útil estudar a classe de todas as álgebras que satisfazem todas essas identidades. Devido a este fato, temos a próxima definição.

Definição 1.3.29. Seja $\{f_i(x_1,\ldots,x_n) \in K\langle X\rangle \,|\, i \in I\}$ um conjunto de polinômios na álgebra associativa livre $K\langle X\rangle$. A classe $\mathcal{B}$ de todas as álgebras associativas satisfazendo as identidades polinomiais $f_i = 0, i \in I$ é chamada de **variedade** definida pelo sistema de identidades polinomiais $\{f_i(x_1,\ldots,x_n) \in K\langle X\rangle \,|\, i \in I\}$. A variedade $\mathcal{C}$ é chamada de **subvariedade** de $\mathcal{B}$ se $\mathcal{C} \subset \mathcal{B}$.

O próximo teorema nos mostra como decidir se uma dada classe de álgebras é uma variedade. Mas antes, precisamos da seguinte definição.

Definição 1.3.30. Seja $\mathcal{B}$ uma classe de álgebras. Denotaremos por $C\mathcal{B}$, $S\mathcal{B}$ e $Q\mathcal{B}$, as classes obtidas por tomar todas as somas cartesianas (isto é, somas diretas com suporte infinito), subálgebras e álgebras quocientes de álgebras em $\mathcal{B}$.

Teorema 1.3.31 (Birkhoff). Uma classe de álgebras $\mathcal{B}$ é uma variedade se somente se, $\mathcal{B}$ é fechada sob as operações de tomar somas cartesianas, subálgebras e álgebras quocientes, isto é, $C\mathcal{B}, S\mathcal{B}, Q\mathcal{B} \subseteq \mathcal{B}$.

Demonstração. ($\Leftarrow$) Vamos provar que $C\mathcal{B} \subseteq \mathcal{B}$.
Seja $\mathcal{B}$ uma variedade e seja $R_j \in \mathcal{B}$, $j \in J$. A soma cartesiana $R = \sum_{j\in J} R_j$ consiste de todas as sequências $(r_j|\, j \in J)$, $r_j \in R_j$, com as operações definidas coordenada a coordenada. Seja $f(x_1,\ldots,x_n)$ uma identidade polinomial para $\mathcal{B}$. Se $r^{(1)},\ldots,r^{(n)} \in R$, $r^{(i)} = (r_j^{(1)}|\, j \in J)$, então

$$f(r^{(1)},\ldots,r^{(n)}) = (f(r_j^{(1)},\ldots,r_j^{(n)})|\, j \in J).$$

Temos, portanto que todas as coordenadas de $f(r^{(1)},\ldots,r^{(n)})$ são iguais a zero e $R \in \mathcal{B}$. Análogo para $S\mathcal{B}, Q\mathcal{B} \subseteq \mathcal{B}$.
($\Rightarrow$) Considere que $C\mathcal{B}, S\mathcal{B}, Q\mathcal{B} \subseteq \mathcal{B}$ e seja $\mathrm{T}(\mathcal{B}) \subset K\langle X\rangle$ o conjunto das identidades polinomiais satisfeitas pelas álgebras em $\mathcal{B}$. Denotemos por $\mathcal{V}$ a variedade definida pelas identidades de $\mathrm{T}(\mathcal{B})$. Temos, portanto que $\mathcal{B} \subseteq \mathcal{V}$. Mostraremos a igualdade $\mathcal{B} = \mathcal{V}$. Sejam m uma cardinalidade qualquer e $Y = \{y_i|\, i \in I\}$ um conjunto com cardinalidade m. Seja N o conjunto de todos os elementos $f(x_1,\ldots,x_n) \in K\langle X\rangle$ que não são identidades polinomiais para $\mathcal{B}$. Apresentamos $K\langle Y\rangle$ como uma união disjunta de dois subconjuntos $T_m(\mathcal{B})$ e N_m da seguinte maneira: Seja $f(y_{i_1},\ldots,y_{i_n})$ qualquer elemento de $K\langle Y\rangle$, onde $y_{i_1},\ldots,y_{i_n}$ são n elementos distintos de Y (e $n \leq m$). Se $f(x_1,\ldots,x_n) \in \mathrm{T}(\mathcal{B})$, então assumimos que $f(y_{i_1},\ldots,y_{i_n}) \in T_m(\mathcal{B})$ e se $f(x_1,\ldots,x_n)$ não é uma identidade polinomial para $\mathcal{B}$, isto é, $f(x_1,\ldots,x_n) \in N$, então $y_{i_1},\ldots,y_{i_n} \in N_m$. Para todo $f = f(y_{i_1},\ldots,y_{i_n}) \in N_m$ existe uma álgebra $R_f \in \mathcal{B}$ e elementos $r_{i_1 f},\ldots,r_{i_n f} \in R_f$, tal que $f(r_{i_1 f},\ldots,r_{i_n f}) \neq 0$ em R_f. Para qualquer $i \in I, i \neq i_1,\ldots,i_n$, escolhemos elementos arbitrários $r_{if} \in R_f$ e definimos os elementos

$$z_i = (r_{if}|\, i \in I) \in \sum_{f\in N_m} R_f.$$

Como $C\mathcal{B}, S\mathcal{B} \subseteq \mathcal{B}$, obtemos que a álgebra F gerada por z_i em $\sum_{f\in N_m} R_f$. pertence a $\mathcal{B}$. Por outro lado, se $g(y_{i_1},\ldots,y_{i_n}) \in N_m$, então $g(z_{i_1},\ldots,z_{i_n}) \neq 0$, porque $g(r_{i_1 g},\ldots,r_{i_n g}) \neq 0$ para qualquer $g \in N_m$. Portanto o núcleo do homomorfismo canônico $K\langle X\rangle \to F$ estendendo $y_i \to z_i, i \in I$, coincide com $T_m(\mathcal{B})$ e F é isomórfico a $F_m(\mathcal{V})$, a álgebra relativamente livre de posto m em $\mathcal{V}$. Finalmente, como $Q\mathcal{B} \subseteq \mathcal{B}$, e toda álgebra m- gerada em $\mathcal{V}$ é uma imagem homomórfica de $F_m(\mathcal{V})$ que está em $\mathcal{B}$, nós obtemos que $\mathcal{V} \subseteq \mathcal{B}$, isto é, $\mathcal{B} = \mathcal{V}$. □

Assim como a definição de um T-ideal de uma álgebra, analogamente, podemos fazê-la para variedades.

Definição 1.3.32. O conjunto $\mathrm{T}(\mathcal{B})$ de todas as identidades polinomiais satisfeitas pela variedade $\mathcal{B}$ é chamado de **T-ideal de $\mathcal{B}$**. Neste caso, diremos que o T-ideal $\mathrm{T}(\mathcal{B})$ é **gerado como um T-ideal** pelo conjunto definidor de identidades polinomiais $\{f_i(x_1,\ldots,x_n) \in K\langle X\rangle \mid i \in I\}$ da variedade $\mathcal{B}$. Usaremos a notação $\mathrm{T}(\mathcal{B}) = \{f_i(x_1,\ldots,x_n) \in K\langle X\rangle \mid i \in I\}^T$ e diremos que o conjunto $\{f_i(x_1,\ldots,x_n) \in K\langle X\rangle \mid i \in I\}$ é uma **base das identidades polinomiais** para $\mathcal{B}$.

Exemplo 1.3.33. A classe de todas as álgebras comutativas é uma variedade definida pelo sistema de identidade polinomial $\{[x_1, x_2]\}$.

Exemplo 1.3.34. A classe de todas as álgebras que são nilpotentes de índice n é uma variedade definida pelo sistema de identidade polinomial $\{x_1 \cdots x_n\}$.

Definição 1.3.35. Para um conjunto fixo Y, a álgebra $\mathrm{F}(\mathcal{B})$ na variedade $\mathcal{B}$ é chamada de **álgebra relativamente livre** de $\mathcal{B}$, se $\mathrm{F}(\mathcal{B})$ é livre na classe $\mathcal{B}$ (e é gerada livremente por Y).

Proposição 1.3.36. Seja $\mathcal{B}$ uma variedade definida por $\{f_i \mid i \in I\}$, e sejam Y um conjunto qualquer e J o ideal gerado por $\{f_i(g_1,\ldots,g_n) \mid g_j \in K\langle Y\rangle, i \in I\}$. Então a álgebra $F = K\langle X\rangle / J$ é uma álgebra relativamente livre em $\mathcal{B}$ com o conjunto de geradores livres $\overline{Y} = \{y + J \mid y \in Y\}$. Duas álgebras relativamente livres de mesmo posto em $\mathcal{B}$ são isomorfas.

Demonstração. (i) Primeiro provaremos que $F \in \mathcal{B}$. Seja $f_i(x_1,\ldots,x_n)$ uma das identidades definidoras de $\mathcal{B}$ e seja $\overline{g_1},\ldots,\overline{g_n}$ elementos arbitrários de F, $\overline{g_j} = g_j + J$, $g_j \in K\langle Y\rangle$. Então $f_i(g_1,\ldots,g_n) \in J$, portanto $f_i(\overline{g_1},\ldots,\overline{g_n}) = 0$ e isto significa que $f_i(x_1,\ldots,x_n) = 0$ é um identidade polinomial para F. Logo $F \in \mathcal{B}$.
(ii) Agora provaremos que F é um álgebra relativamente livre em $\mathcal{B}$. Seja V uma álgebra qualquer em (B) e seja $\phi : \overline{Y} \to R$ uma aplicação arbitrária. Defina a aplicação $\theta : Y \to R$ por $\theta(y) = \phi(\overline{y})$ e estenda θ a um homomorfismo $\theta : K\langle Y\rangle \to R$. Isto sempre é possível pois $K\langle Y\rangle$ é uma álgebra associativa livre. Para provar que θ pode ser estendido a um homomorfismo $F \to R$ é suficiente provar que $J \subseteq Ker(\theta)$ Seja $f \in J$, isto é:

$$f = \sum_{i\in I} u_i f_i(g_{i1},\ldots,g_{in_i})v_i,\ g_{ij}, u_i, v_i \in K\langle Y\rangle$$

Para $r_1,\ldots,r_{n_i} \in R$ arbitrários, o elemento $f_i(r_1,\ldots,r_{n_i})$ é igual a zero em R e isto implica que $\theta(f) = 0$, isto é, $J \subseteq Ker(\theta)$ e $F \cong F_{\overline{Y}}(\mathcal{B})$ é a álgebra relativamente livre em $\mathcal{B}$, livremente gerada por $\overline{Y}$.
(iii) Seja $|Y| = |Z|$, $Y = \{y_i \mid i \in I\}$ e sejam $F_Y(\mathcal{B})$ e $F_Z(\mathcal{B})$ as álgebras relativamente livre correspondentes. Como ambas as álgebras $F_Y(\mathcal{B})$ e $F_Z(\mathcal{B})$ são relativamente livres, podemos definir homomorfismos

$$\phi : F_Y(\mathcal{B}) \to F_Z(\mathcal{B}),\ \psi : F_Z(\mathcal{B}) \to F_Y(\mathcal{B})$$

por $\phi(y_i) = z_i$ e $\psi(z_i) = y_i$. Como $\phi \circ \psi$ e $\psi \circ \phi$ agem identicamente em Y e Z respectivamente obtemos que ϕ e ψ são isomorfismos. □

Observação 1.3.37. 1. Segue da prova da proposição acima que o T-ideal de $K\langle Y\rangle$ gerado por $\{f_i | \, i \in I\}$ consiste de todas as combinações lineares de

$$u_i \cdot f_i(g_{i1}, \ldots, g_{in_i}) \cdot v_i$$

com $g_{ij}, u_i, v_i \in K\langle Y\rangle$.

2. Temos que:

$$F_Y(\mathcal{B}) \cong \frac{K\langle Y\rangle}{\mathrm{T}(\mathcal{B})}$$

e $|Y|$ é chamado de **posto da álgebra relativamente livre**.

De acordo com o teorema abaixo, a correspondência entre T-ideais e variedades fica bem entendida:

Teorema 1.3.38. Existe uma correspondência injetora entre os T-ideais de $K\langle X\rangle$ e as variedades de álgebras. Nesta correspondência uma variedade $\mathcal{B}$ corresponde ao T-ideal das identidades $\mathrm{T}(\mathcal{B})$ e um T-ideal I corresponde a uma variedade de álgebras satisfazendo todas as identidades de I.

Demonstração. Se I_1 e I_2 são dois ideais diferentes, então existe $f \in I_1 - I_2$. Mas então $\mathcal{B}(I_1) \neq \mathcal{B}(I_2)$ pois $K\langle X\rangle / I_2$ não satisfaz f e então $K\langle X\rangle / I_2 \in \mathcal{B}(I_2)$ mas $K\langle X\rangle / I_2 \notin \mathcal{B}(I_1)$.
Agora se $\mathcal{B}(I_1)$ e $\mathcal{B}(I_2)$ são duas variedades diferentes, então existe $A \in \mathcal{B}(I_1) - \mathcal{B}(I_2)$. Portanto existe $f \in \mathrm{T}(\mathcal{B}(I_2))$ tal que $f \notin T(A)$. Como $T(A) \subset T(\mathcal{B}(I_1))$, segue que $T(\mathcal{B}(I_1)) \neq T(\mathcal{B}(I_2))$. □

Observação 1.3.39. A correspondência do teorema acima reverte inclusões, ou seja: $\mathcal{B} \subset \mathcal{C} \Rightarrow \mathrm{T}(\mathcal{B}) \supset \mathrm{T}(\mathcal{C})$.

Comentaremos de forma sucinta, a seguir, o problema de Specht, ou seja, se toda variedade de álgebras podem ser definidas por um sistema finito de identidades polinomiais.

Definição 1.3.40. Uma variedade de álgebras associativas $\mathcal{B}$ é chamado de **finitamente baseado** (ou tem uma base finita de suas identidades polinomiais) se $\mathcal{B}$ pode ser definido por um sistema finito de identidades polinomiais (da álgebra associativa livre $K\langle X\rangle$, $X = \{x_1, x_2, \ldots\}$. Se $\mathcal{B}$ não pode ser definido por um sistema finito de identidades polinomiais ele é chamado **infinitamente baseado**. Se todas as subvariedades de $\mathcal{B}$, inclusive $\mathcal{B}$, são finitamente baseadas, então $\mathcal{B}$ satisfaz à **propriedade de Specht**.

O problema de Specht consiste na seguinte pergunta: Toda variedade de álgebras associativas ou de Lie é finitamente baseada?
O problema de Specht segue em duas direções, a saber:

- Mostrar que algumas variedades satisfazem a propriedade de Specht; e
- Construir contra-exemplos para o problema de Specht.

Para fins de conhecimento, a seguir, apresentamos um teorema que é importante neste tipo de pesquisa. Ele é devido a Kemer e foi demonstrado em 1987.

Teorema 1.3.41. Toda variedade de álgebras associativas sobre um corpo de característica zero tem uma base finita para suas identidades polinomiais.

1.4 Espaços Vetoriais Graduados

Nesta seção falaremos de espaços vetoriais graduados e multigraduados. Estas definições são necessárias para que mais adiante possamos introduzir os conceitos de identidades polinomiais homogêneas e multilineares, identidades estas que nos auxiliarão no estudo das identidades de uma álgebra dada. Veremos também as séries de Hilbert e de Poincaré das álgebras relativamente livres correspondentes aos espaços vetoriais graduados e multigraduados.

Utilizando a noção de grupos, podemos fazer uma graduação de uma álgebra conforme a próxima definição.

Definição 1.4.1. Sejam A uma álgebra sobre K e G um grupo qualquer. A é chamada de **G-graduada** se A pode ser escrito como soma direta de subespaços

$$A = \bigoplus_{g \in G} A_g$$

tal que para todo $g, h \in G$ temos que $A_g A_h \subset A_{gh}$.

Da definição segue que se $a \in A$ então a pode ser escrito de maneira única como uma soma finita $a = \bigoplus_{g \in G} a_g$ com $a_g \in A_g$. Os subespaços A_g são chamados de **componentes homogêneas** de A. Desta forma, um elemento $a \in A$ é **g-homogêneo** se $a \in A_g$. Um subespaço $B \subset A$ é **homogêneo (ou graduado)** se $B = \bigoplus_{g \in G}(B \cap A_g)$.

Exemplo 1.4.2. Considerando o grupo aditivo $\mathbb{Z}_2 = \{0, 1\}$ e tomando os subespaços $E_0(V)$ e $E_1(V)$ da álgebra de Grassmann (veja o Exemplo 1.2.24), temos que $E(V) = E_0(V) \oplus E_1(V)$ é uma $\mathbb{Z}_2$-graduação de $E(V)$ e que $Z(E(V)) = E_0(V)$ se $\mathrm{car}(K) \neq 2$ e $ab = -ba$, $\forall a, b \in E_1(V)$.
Com efeito, temos da definição de $E_0(V)$ e $E_1(V)$ que $E_0(V)E_1(V) \subset E_{0+1}(V)$. Vimos no Exemplo 1.3.7 da página 33 que $(e_{j_1} \cdots e_{j_s})(e_{i_1} \cdots e_{i_r}) = (-1)^{rs} e_{i_1} \cdots e_{i_r} e_{j_1} \cdots e_{j_s}$.
Observamos da igualdade acima que se r ou s for par então vale a comutatividade, mas se r e s forem ímpares então vale a anticomutatividade. Como consequência disso, temos que apenas os elementos de $E_0(V)$ comutam com todos os elementos de $E(V)$, o que implica que $Z(E(V)) = E_0(V)$ e $ab = -ba$, $\forall a, b \in E_1(V)$.

Observe que se V_n é um espaço vetorial de dimensão finita igual a n, um número ímpar, então temos somente que $E_0(V_n) \subset Z(E(V_n))$. Por exemplo, considere $n = 3$ e seja $\{e_1, e_2, e_3\}$ uma base do espaço vetorial V_3. Logo, $\{1, e_1, e_2, e_3, e_1e_2, e_1e_3, e_2e_3, e_1e_2e_3\}$ é uma base de $E(V_3)$. Temos que $E_0(V_3) = \mathrm{span}\langle 1, e_1e_2, e_1e_3, e_2e_3\rangle$ e, também, que $E_1(V_3) = \mathrm{span}\langle e_1, e_2, e_3, e_1e_2e_3\rangle$. Mas, $\forall p \in E(V_3)$ temos que $p \cdot e_1e_2e_3 = e_1e_2e_3 \cdot p = 0$, pois pelos menos um dos elementos e_1, e_2 ou e_3 repete na multiplicação. Logo $e_1e_2e_3 \in Z(E(V_3))$ e pertence também a $E_1(V_3)$.

Exemplo 1.4.3. Qualquer álgebra pode ser graduada por um grupo G, basta tomar $A = A_e$ e $A_g = 0$ para qualquer $g \neq e$, onde e é o elemento neutro do grupo G. Esta graduação é chamada de **trivial**.

Nesta dissertação utilizaremos, também, a seguinte versão alternativa de espaço vetorial graduado.

Definição 1.4.4. O espaço vetorial V é **graduado** se ele é uma soma direta de seus subespaços $V^{(n)}$, onde $n \in \mathbb{Z}$, isto é

$$V = \bigoplus_{n\in\mathbb{Z}} V^{(n)}, \quad \text{e} \quad V^{(n)} = \{0\} \quad \text{se} \quad n < 0.$$

Os subespaços $V^{(n)}$ são chamados de **componentes homogêneos de grau** n de V. Similarmente, podemos introduzir uma **multigraduação** em V (ou uma $\mathbb{Z}^n$-graduação) se

$$V = \sum_{i=1}^{m} \sum_{n\geq 0} V^{(n_1,\ldots,n_m)}, \quad \text{onde} \quad n = (n_1, \ldots, n_m)$$

e chamamos os $V^{(n_1,\ldots,n_m)}$ de **componentes multihomogêneos de multigrau** $(n_1, \ldots, n_m)$ de V.

Devido à graduação ou multigraduação dada a um espaço vetorial, um polinômio f pode ser classificado de acordo com a seguinte definição :

Definição 1.4.5.

1. Um polinômio f pertencente a $V^{(n)}$, para algum $n \geq 1$, será chamado de **homogêneo de grau** n.
2. Se f pertence a algum $V^{(n_1,\ldots,n_m)}$, f será conhecido por **multihomogêneo de multigrau** $(n_1, \ldots, n_m)$.
3. Também dizemos que f é **homogêneo na variável** x_i, se x_i aparece como mesmo grau em todos os monômios de f.
4. Um polinômio f será chamado de **multilinear de grau** n se f é multihomogêneo de multigrau $(1, \ldots, 1)$.

Exemplo 1.4.6. A álgebra polinomial $K[x_1, \ldots, x_n]$ é graduada assumindo que os polinômios de grau n (no sentido usual) são os elementos homogêneos de grau n. Similarmente $K[x_1, \ldots, x_n]$ tem uma multigraduação, contando as entradas de cada variável nos monômios.

Exemplo 1.4.7. Seja $\beta = \{1\} \cup \{e_{i_1}e_{i_2}\cdots e_{i_k} |\ k \geq 1;\ i_1 < i_2 < \cdots < i_k\}$ a base da álgebra de Grassmann $E(V)$. Considere os conjuntos $\beta(0) = \{1\}$ e $\beta(n) = \{e_{i_1}e_{i_2}\cdots e_{i_n} |\ i_1 < i_2 < \cdots < i_n\}$, logo $\beta = \bigcup_{n\geq 0} \beta(n)$. Observe que essa união é disjunta. Denote por $E(K, n) = \text{span}_K \langle\beta(n)\rangle$, então $E(V) = \bigcup_{n\geq 0} E(K, n)$ é uma graduação em $E(V)$. Defina a função **comprimento** $l(a) = n$ se $a \in E(K, n)$.

Vemos dos Exemplos 1.4.2 e 1.4.7 que podemos escrever:

$$E_0(V) = \bigcup_{n \text{ par}} E(K, n) \ \text{ e } \ E_1(V) = \bigcup_{n \text{ ímpar}} E(K, n).$$

Denote $d(a) = i$ se $a \in E_i(V)$.

A seguir, definiremos uma série de potências que utilizaremos no capítulo 2.

Definição 1.4.8. Seja $\bigoplus_{n\geq 0} V^{(n)}$ um espaço vetorial graduado e seja $\dim\left(V^{(n)}\right) < \infty$. Então a série de potência formal dada por

$$H(V,t) = Hilb(V,t) = \sum_{n\geq 0} \dim\left(V^{(n)}\right) t^n$$

é chamada de **série de Hilbert de** V. Para a função $f(t)$, fazemos a convenção usual que $H(V,t) = f(t)$ se a série $H(V,t)$ converge em alguma vizinhança de zero e as funções $H(V,t)$ e $f(t)$ são iguais em tal vizinhança.

Analogamente, se o espaço vetorial $V = \sum_{i=1}^{m} \sum_{n_i\geq 0} V^{(n_1,\ldots,n_m)}$ é multigraduado, então a série é chamada de **série de Poincaré** de V e é igual a:

$$H(V,t_1,\ldots,t_m) = Hilb(V,t_1,\ldots,t_m) = \sum_{n\geq 0} \dim\left(V^{(n_1,\ldots,n_m)}\right) t_1^{n_1}\cdots t_m^{n_m}.$$

Exemplo 1.4.9. Escrevendo $K[x] = \sum_{n\geq 0} V^{(n)}$, onde $V^{(n)} = \operatorname{span}\langle x^n\rangle$ e $\dim(\operatorname{span}\langle x^n\rangle) = 1$, temos, com t próximo de zero, que:

$$Hilb(K[x],t) = \sum_{n\geq 0} 1t^n = 1 + t + t^2 + \cdots = \frac{1}{1-t}.$$

Pois é uma progressão geométrica de razão $t < 1$ e primeiro termo igual a 1.

Exemplo 1.4.10. Como podemos escrever $K[x_1,\ldots,x_m] = \sum_{n\geq 0} V^{(n_1,\ldots,n_m)}$, onde os subespaços $V^{(n_1,\ldots,n_m)}$ são iguais a $\operatorname{span}\langle x_1^{n_1}\cdots x_m^{n_m}\rangle$ com $n_1+\cdots+n_m = n$ e $\dim(\operatorname{span}\langle x_1^{n_1}\cdots x_m^{n_m}\rangle) = 1$, temos, com $t_1,\ldots,t_m$ próximo de zero, que:

$$\begin{aligned} Hilb(K[x_1,\ldots,x_m],t_1,\ldots,t_m) &= \sum_{n\geq 0} 1t_1^{n_1}\cdots t_m^{n_m} \\ &= 1 + (t_1+\cdots+t_m) + (t_1^2+\cdots+t_m^2+t_1t_2+\cdots+t_{m-1}t_m) + \cdots \\ &= \frac{1}{1-t_1}\cdots\frac{1}{1-t_m} \\ &= \prod_{i=1}^{m}\frac{1}{1-t_i}. \end{aligned}$$

1.5 Identidades Polinomiais Homogêneas e Multilineares

Quando o corpo base é infinito, o estudo das identidades de uma álgebra dada pode ser reduzido ao estudo de polinômios homogêneos ou multilineares. Com este intuito, nesta seção, abordaremos as identidades polinomiais homogêneas e multilineares. Também abordaremos o conceito de sequência de codimensão de um T-ideal.

A identidade polinomial $g = 0$ é chamada de **consequência** das (ou segue das) identidades polinomiais $f_i = 0$, $i \in I$, se g pertence ao **T-ideal gerado por** f_i, ou seja, $g \in \langle f_i |\, i \in I\rangle^{\mathrm{T}}$.

Definição 1.5.1. Dois conjuntos de identidades polinomiais são **equivalentes** se eles geram o mesmo T-ideal.

Lembremos que um polinômio $f(x_1, \ldots, x_n)$ em uma álgebra associativa livre $K\langle X\rangle$ é **multilinear de grau** n se f é multihomogêneo de multigrau $(1, \ldots, 1)$ em $K\langle x_1, \ldots, x_n\rangle \subset K\langle X\rangle$ e que P_n é o espaço vetorial de todos os polinômios em $K\langle X\rangle$ que são multilineares de grau n. Claramente, P_n é de dimensão $n!$ e tem uma base dada por $\{x_{\sigma(1)} \cdots x_{\sigma(n)} | \, \sigma \in S_n\}$.

Observação 1.5.2. Para verificarmos uma afirmação sobre um polinômio multilinear f em elementos arbitrários $v_1, \ldots, v_n$ de um espaço vetorial V, basta verificarmos essa mesma afirmação sobre f nos elementos $e_1, \ldots, e_n$ de uma base de V.

Lema 1.5.3. Se uma álgebra A satisfaz uma identidade polinomial qualquer então ela satisfaz uma identidade polinomial em duas variáveis.

Demonstração. Suponha que a álgebra A satisfaz a identidade $f(x_1, \ldots, x_n) = 0$. Substituindo x_i por $u^i v$ onde u, $v \in X$ são as novas variáveis de f, obtemos a identidade:

$$g(u, v) = f(uv, u^2 v, \ldots, u^n v) = 0,$$

onde g é um polinômio que não é identicamente zero. □

O próximo lema descreverá um método conhecido por **processo de multilinearização**, que é uma ferramenta que será muito utilizada nessa dissertação.

Lema 1.5.4. Se uma álgebra A satisfaz qualquer identidade polinomial então ela satisfaz uma identidade polinomial que é linear em cada uma das suas variáveis.

Demonstração. Suponha que A satisfaz a identidade $f(x_1, \ldots, x_n) = 0$ e que f não é linear em x_1. Então

$$f(y + z, x_2, \ldots, x_n) - f(y, x_2, \ldots, x_n) - f(z, x_2, \ldots, x_n) = 0$$

é satisfeita por A. Este polinômio (em n+1 variáveis), não é identicamente nulo e com grau em y e z menor que o grau de f em x_1. Por sucessivos passos deste tipo conseguimos um polinômio linear em todas as variáveis. □

Exemplo 1.5.5. Vamos encontrar a linearização do polinômio $f(x_1, x_2) = x_1^2 x_2 x_1$.
Tomemos:

$$\begin{aligned} g(y_1, y_2, x_2) &= f(y_1 + y_2, x_2) - f(y_1, x_2) - f(y_2, x_2) \\ &= (y_1 + y_2)^2 x_2 (y_1 + y_2) - y_1^2 x_2 y_1 - y_2^2 x_2 y_2 \\ &= (y_1^2 + y_1 y_2 + y_2 y_1 + y_2^2) x_2 (y_1 + y_2) - y_1^2 x_2 y_1 - y_2^2 x_2 y_2 \\ &= y_1^2 x_2 y_2 + y_1 y_2 x_2 y_1 + y_2 y_1 x_2 y_1 + y_1 y_2 x_2 y_2 + y_2 y_1 x_2 y_2. \end{aligned}$$

Façamos agora:

$$\begin{aligned} h(a, b, y_2, x_2) &= g(a + b, y_2, x_2) - g(a, y_2, x_2) - g(b, y_2, x_2) \\ &= (a + b)^2 x_2 y_2 + (a + b) y_2 x_2 (a + b) + y_2 (a + b) x_2 (a + b) \\ &\quad + (a + b) y_2 x_2 y_2 + y_2 (a + b) x_2 y_2 - a^2 x_2 y_2 - a y_2 x_2 a - y_2 a x_2 a \\ &\quad - a y_2 x_2 y_2 - y_2 a x_2 y_2 - b^2 x_2 y_2 - b y_2 x_2 b - y_2 b x_2 b - b y_2 x_2 y_2 - y_2 b x_2 y_2 \\ &= (a^2 + ab + ba + b^2) x_2 y_2 + (a + b) y_2 x_2 (a + b) + y_2 (a + b) x_2 (a + b) \\ &\quad + (a + b) y_2 x_2 y_2 + y_2 (a + b) x_2 y_2 - a^2 x_2 y_2 - a y_2 x_2 a - y_2 a x_2 a \\ &\quad - a y_2 x_2 y_2 - y_2 a x_2 y_2 - b^2 x_2 y_2 - b y_2 x_2 b - y_2 b x_2 b - b y_2 x_2 y_2 - y_2 b x_2 y_2 \\ &= ab x_2 y_2 + ba x_2 y_2 + y_2 a x_2 b + y_2 b x_2 a + a y_2 x_2 b + b y_2 x_2 a. \end{aligned}$$

Ainda nesta seção, veremos que as identidades multilineares e homogêneas são uma ferramenta poderosa para fornecer uma base para as identidades polinomiais.

Proposição 1.5.6. Seja $f(x_1, \ldots, x_n) = \sum_{i=0}^{n} f_i \in K\langle X\rangle$, onde f_i são as componentes homogêneas de f de grau i em x_1.

1. Se o corpo base K contém mais que n elementos (em particular, se K é infinito), então as identidades polinomiais $f_i = 0$, $i = 0, 1, \ldots, n$, seguem de $f = 0$.

2. Se $\mathrm{car}(K) = 0$ (ou se $\mathrm{car}(K) > \mathrm{gr}(f)$), então $f = 0$ é equivalente a um conjunto de identidades polinomiais multilineares.

Demonstração. (i) Seja $V = \langle f\rangle^T$ o T-ideal de $K\langle X\rangle$ gerado por f. Escolhemos $n+1$ elementos distintos $\alpha_0, \ldots, \alpha_n \in K$. como V é um T-ideal, temos

$$f(\alpha_j x_1, \ldots, x_m) = \sum_{i=0}^{n} \alpha_j^i f_i(x_1, \ldots, x_m) \in V,\ j = 0, \ldots, n.$$

Consideremos estas equações como um sistema linear com variáveis f_i, $i = 0, 1, \ldots, n$. Como seu determinante

$$\begin{vmatrix} 1 & \alpha_0 & \alpha_0^2 & \cdots & \alpha_0^n \\ 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^n \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^n \end{vmatrix} = \prod_{i<j} (\alpha_j - \alpha_i)$$

é o determinante de Vandermonde e é diferente de zero, obtemos que cada $f_i(x_1, \ldots, x_m)$ também pertence a V, isto é, as identidades polinomiais $f_i = 0$ são consequências de $f = 0$.
(ii) Usaremos o processo de multilinearização. Por (i) podemos assumir que $f(x_1, \ldots, x_m)$ é homogêneo em cada uma de suas variáveis. Seja $\mathrm{gr}_{x_i}(f) = d$. Escreva $f(y_1 + y_2, x_2, \ldots, x_m) \in V$ na forma:

$$f(y_1 + y_2, x_2, \ldots, x_m) = \sum_{i=0}^{d} f_i(y_1, y_2, x_2, \ldots, x_m),$$

onde f_i é a componente homogênea de grau i em y_1. Portanto $f_i \in V$, $i = 0, 1, \ldots, d$. Como $\mathrm{gr}_{y_j}(f_i) < d$, $i = 0, 1, \ldots, d-1$ e $j = 1, 2$, aplicamos a hipótese de indução e obtemos um conjunto de consequências multilineares de $f = 0$. No sentido de ver que estas identidades multilineares são equivalentes à $f = 0$, é suficiente observar que:

$$f_i(y_1, y_1, x_2, \ldots, x_m) = \binom{d}{i} f(y_1, x_2, \ldots, x_m),$$

e o coeficiente binomial é diferente de zero pois $\mathrm{car}(K) = 0$ ou $\mathrm{car}(K) = p > d$. □

Corolário 1.5.7. Seja A uma álgebra.

1. Se o corpo K é infinito então todas as identidades polinomiais de A seguem de suas identidades multihomogêneas, ou seja, $\mathrm{T}(A)$ é gerado por seus polinômios multihomogêneos.

2. Se o corpo K tem característica zero então todas as identidades polinomiais de A seguem de suas identidades multilineares, ou seja, $\mathrm{T}(A)$ é gerado por seus polinômios multilineares.

Observação 1.5.8. Portanto, qualquer PI-álgebra (sobre qualquer corpo) satisfaz uma identidade polinomial multilinear. De fato, comece com uma identidade polinomial qualquer $f(x_1, \ldots, x_m) = 0$, e use o fato que o grau em y_1 e em y_2 da consequência de $f = 0$

$$g(y_1, y_2, x_2 \ldots, x_m) = f(y_1 + y_2, x_2, \ldots, x_m) - f(y_1, x_2, \ldots, x_d) - f(y_2, x_2, \ldots, x_m)$$

são menores que o grau de $f(x_1, \ldots, x_m)$ em x_1 e se $\mathrm{gr}_{x_1}(f) > 1$, então $\mathrm{gr}_{y_j}(g) > 0$, $j = 1, 2$.

Veremos, na próxima definição, um objeto que é muito útil para caracterizar se uma determinada álgebra é uma PI-álgebra ou não.

Definição 1.5.9. Seja A uma PI-álgebra com T-ideal $\mathrm{T}(A)$. A dimensão dos polinômios multilineares em $K\langle X\rangle$ módulo as identidades polinomiais de A é chamada de **n-ésima codimensão do T-ideal T(A) ou das identidades polinomiais de** A e é denotado por $c_n(A)$ (ou por $c_n(\aleph)$ se nós considerarmos o T-ideal das identidades polinomiais de uma variedade $\aleph$), isto é

$$c_n(A) = \dim\left(\frac{P_n}{P_n \cap \mathrm{T}(A)}\right),\ n = 0, 1, \ldots.$$

Podemos considerar também as **séries de codimensão** e as **séries de codimensão exponencial** definidas, respectivamente, por:

$$c(A, t) = \sum_{n\geq 0} c_n(A)t^n \quad \text{e} \quad \tilde{c}(A, t) = \sum_{n\geq 0} c_n(A)\frac{t^n}{n!}.$$

Observação 1.5.10. Da definição de $c_n(A)$, temos que $\dim(P_n \cap \mathrm{T}(A)) = n! - c_n(A)$. E portanto, uma álgebra A é uma PI-álgebra se somente se $c_n(A) < n!$, para algum $n \geq 1$.

A título de informação, Regev, utilizando a noção de n-ésima codimensão do T-ideal e a Observação 1.5.10, provou o seguinte teorema, cuja demonstração pode ser encontrada em [29].

Teorema 1.5.11 (Regev). Se A e B são PI-álgebras então $A \otimes B$ também é uma PI-álgebra.

Observação 1.5.12. Se A é uma álgebra, para qualquer subconjunto S de $K\langle X\rangle$, denotamos por $S(A)$ a imagem de S sob o homomorfismo canônico

$$K\langle X\rangle \to F(A) = \frac{K\langle X\rangle}{\mathrm{T}(A)}.$$

Definição 1.5.13. Seja o T-ideal $\mathrm{T}(A)$ um ideal (multi)homogêneo de $K\langle X\rangle$. Então denotaremos por

$$Hilb(U_m(A), t_1, \ldots, t_m)$$

as **séries de Hilbert** da álgebra relativamente livre de posto m em $varA$. Se estamos interessados nessa série em uma variável, escrevemos

$$Hilb(U_m(A), t) = \sum_{n\geq 0} \dim(U_m^{(n)}(R))t^n.$$

Exemplo 1.5.14. Seja A uma álgebra nilpotente e $A^m = 0$, então $c_n(A) = 0$, para todo $n \geq m$. Com efeito, como $n \geq m$, todo polinômio $x_{\sigma(1)} \cdots x_{\sigma(n)}$ da base de P_n também é uma identidade de A, logo $P_n = P_n \cap \mathrm{T}(R)$ e o resultado é obtido.

Exemplo 1.5.15. Seja A uma álgebra comutativa então $c_n(A) \leq 1$, para todo $n \geq 1$.
De fato, para cada valor de n temos:

Seja $x_1 \cdots x_n$ um elemento da base de P_n. Como A é uma álgebra comutativa temos que $x_{\sigma(1)} \cdots x_{\sigma(n)} = x_1 \cdots x_n$, logo a base de P_n é composta apenas pelo elemento $x_1 \cdots x_n$ e então $\dim(P_n) = 1$. Portanto, basta observarmos se o polinômio $x_1 \cdots x_n \in P_n \cap \mathrm{T}(A)$:

- se $x_1 \cdots x_n \in P_n \cap \mathrm{T}(A)$ então para todo $\sigma \in S_n$ temos que $x_{\sigma(1)} \cdots x_{\sigma(n)} \in P_n \cap \mathrm{T}(A)$, logo $P_n = P_n \cap \mathrm{T}(A)$ e portanto $c_n(A) = 0$.
- se $x_1 \cdots x_n \notin P_n \cap \mathrm{T}(A)$ então para todo $\sigma \in S_n$ temos que $x_{\sigma(1)} \cdots x_{\sigma(n)} \notin P_n \cap \mathrm{T}(A)$, logo $P_n \cap \mathrm{T}(A) = \{0\}$ e portanto $c_n(A) = 1$.

Denotaremos por $H_m(F, i) \subset K\langle x_1, \ldots, x_m \rangle$ o **conjunto dos polinômios homogêneos nas variáveis** $x_1, \ldots, x_m$ **de grau** i.

Por analogia a codimensão, séries de Hilbert e série de codimensão de uma álgebra, podemos fazer as seguintes definições:

Definição 1.5.16. Se A é uma K PI-álgebra então chamaremos de **codimensão homogênea** a seguinte expressão

$$c(A, H_m(F, i)) = \dim_K \left(\frac{H_m(F, i)}{H_m(F, i) \cap \mathrm{T}(A)} \right).$$

Definição 1.5.17. Sejam A uma PI-álgebra unitária sobre um corpo de característica zero e o subespaço vetorial dado por $\Gamma_n(A) = \Gamma_n/(\Gamma_n \bigcap \mathrm{T}(A))$, definimos:

1. a **sequência de codimensão própria** por

$$\gamma_n(A) = \dim(\Gamma_n), \quad n = 0, 1, \ldots;$$

2. as **séries das codimensões próprias** por

$$\gamma(A, t) = \sum_{n \geq 0} \gamma_n(A) t^n \quad \text{e}$$

3. as **séries de codimensões próprias exponenciais** por

$$\widetilde{\gamma}(A, t) = \sum_{n \geq 0} \gamma_n(A) \frac{t^n}{n!}.$$

Conforme a Observação 1.5.12, se A é uma PI-álgebra, denotaremos por $B(R)$, $B_m(R)$ e $\Gamma_n(R)$ as imagens em $F(R)$ dos correspondentes subespaços vetoriais de $K\langle X \rangle$.

Como precisaremos dos seguintes teoremas mais adiante, enunciaremos os dois primeiros (para uma prova veja, respectivamente, as páginas 42 e 47 do livro [7]) e o terceiro é uma consequência direta destes.

Teorema 1.5.18. Se A é uma PI-álgebra unitária sobre um corpo infinito K, então todas as identidades polinomiais de A seguem dos polinômios próprios (isto é, daqueles em $\mathrm{T}(A) \cap B$). Se característica de K é zero, então as identidades polinomiais de A seguem das identidades multilineares próprias (isto é, daqueles em $\mathrm{T}(A) \cap \Gamma_n$, $n = 1, 2, \ldots$).

Teorema 1.5.19. Seja A uma PI-álgebra unitária sobre um corpo infinito K.

1. Se
$$\{w_j(x_1, \ldots, x_m) | \, j = 1, 2, \ldots\}$$
é uma base do espaço vetorial $B_m(A)$ dos polinômios próprios da álgebra relativamente livre $U_m(A)$ de posto m, isto é
$$B_m(A) = \frac{K\langle x_1, \ldots, x_m\rangle \cap B}{\mathrm{T}(A) \cap K\langle x_1, \ldots, x_m\rangle \cap B},$$
então $U_m(A)$ tem uma base
$$\{x_1^{a_1} \cdots x_m^{a_m} w_j(x_1, \ldots, x_m) | \, a_i \geq 0, \, j = 0, 1, \ldots\}.$$

2. Se
$$\{u_{uj}(x_1, \ldots, x_m) | \, j = 1, 2, \ldots, \gamma_k(A)\}$$
é uma base do espaço vetorial $\Gamma_k(A)$ dos polinômios multilineares próprios de grau k em $F(A)$, então $P_n(A)$ tem uma base consistindo de todos os polinômios multilineares da forma
$$x_{p_1} \cdots x_{p_{n-k}} u_{jk}(x_{q_1}, \ldots, x_{q_k}), \; j = 1, 2, \ldots \gamma_k(A), \; k = 0, 1, \ldots, n$$
tal que $p_1 < \cdots < p_{n-k}$ e $q_1 < \cdots < q_k$.

Teorema 1.5.20. Seja A uma PI-álgebra unitária sobre um corpo infinito K.

1. As séries de Hilbert da álgebra relativamente livre $F_m(A)$ e seus elementos próprios $B_m(A)$ estão relacionados por
$$Hilb(U_m(A), t_1, \ldots, t_m) = Hilb(B_m(A), t_1, \ldots, t_m) \prod_{i=1}^{m} \frac{1}{1 - t_i},$$
$$Hilb(U_m(A), t) = Hilb(B_m(A), t) \frac{1}{1 - t}.$$

2. As codimensões e as codimensões próprias das identidades polinomiais de A e as correspondentes séries de potências formais estão relacionadas como se segue:
$$c_n(A) = \sum_{k=0}^{n} \binom{n}{k} \gamma_k(A), \; n = 0, 1, \ldots, \qquad c(A, t) = \frac{1}{1 - t} \, \gamma\left(A, \frac{t}{1 - t}\right) \quad \text{e} \quad \widetilde{c}(A, t) = e^t \, \widetilde{\gamma}(A, t).$$

Demonstração. (1.) É consequência do Teorema 1.5.19 e dos Exemplos 1.4.9 e 1.4.10.
(2.) A primeira equação também é consequência do Teorema 1.5.19. □

Capítulo 2

Fatos sobre a Álgebra de Grassmann em um corpo K de característica zero

Este capítulo foi elaborado com o objetivo de descrever alguns invariantes numéricos da álgebra de Grassmann, que são: suas codimensões, suas séries de Hilbert e o seu co-comprimento. Nos limitaremos ao caso em que $\text{car}(K) = 0$, onde existem instrumentos para calcular esses invariantes. Se $\text{car}(K) \neq 0$, embora estes cálculos fiquem mais interessantes, necessitaremos de outras ferramentas, que não foram abordadas neste trabalho.

2.1 Codimensões da álgebra de Grassmann

Esta seção foi escrita com base no artigo [9]. Lembremos que uma base para a álgebra de Grassmann unitária é $D = \{1\} \cup \{e_{i_1} e_{i_2} \dots e_{i_m} |\ i_1 < i_2 < \dots < i_m, m = 1, 2, \dots\}$. Para qualquer escolha de n elementos em D, $\{a_1, \dots, a_n\}$, seja $I \subseteq \{1, \dots, n\} = I_n$ o conjunto dos índices para o qual a_i é de comprimento ímpar. Seja $\sigma \in S_n$, o grupo simétrico em n elementos. Sabemos que

$$a_{\sigma(1)} \cdots a_{\sigma(n)} = \left(f_I^{(n)}(\sigma)\right)\ a_1 \cdots a_n,$$

onde $f_I^{(n)}(\sigma) \in \{-1, 1\}$.

A função $f_I^{(n)}(\sigma)$ é computada como segue: como as permutações de um conjunto ordenado estão em correspondência biunívoca com as reordenações do conjunto, $\sigma \in S_n$ determina uma reordenação da n-upla $(1, \dots, n)$ da sua ordem natural para $(\sigma(1), \dots, \sigma(n))$. Agora considere um subconjunto arbitrário $I \subset \{1, \dots, n\} = I_n$ e $\sigma \in S_n$. A reordenação σ em $\{1, \dots, n\}$ induz uma reordenação do subconjunto I e portanto, pela correspondência biunívoca, equivale a uma permutação sobre I (observe que isto não implica que $\sigma(I) \subseteq I$). Podemos mostrar que o sinal desta permutação induzida é igual a $f_I^{(n)}(\sigma)$.

Exemplo 2.1.1. Sejam uma permutação $\sigma = (12435)$, $I_5 = \{1, 2, 3, 4, 5\}$ e $I = \{1, 3, 5\}$, então $\sigma(I_5) = \{2, 4, 5, 3, 1\}$ logo, o subconjunto I foi reordenado por σ da tripla ordenada $(1, 3, 5)$ para $(5, 3, 1)$. Isto corresponde a permutação $(15)(3)$ em I e portanto $f_I^{(5)}(\sigma) = -1$. Observe que $\sigma(I) = \{1, 2, 5\} \not\subseteq \{1, 3, 5\} = I$.

Do exposto acima, temos a função $f : 2^n \times S_n \to \{-1, +1\}$. Trabalharemos com as matrizes $M^{(n)}$ de tamanho $2^n \times n!$ que serão determinadas por ordenar os 2^n subconjuntos de $\{1, \ldots, n\}$ e usá-los como índices para as linhas e por ordenar as $n!$ permutações de S_n e usá-las como índices para as colunas; e que terão como entradas os números $f_I^{(n)}(\sigma)$.

Exemplo 2.1.2. Considere $n = 2$, logo $I_2 = \{1, 2\}$, seus subconjuntos são $\emptyset$, $\{1\}$, $\{2\}$ e $\{1, 2\}$ e as permutações de I_2 são $(1, 2)$ e $(2, 1)$. Com o auxílio da tabela abaixo, que mostra as ordenações do conjunto I_2 e das permutações de S_2,

	$(1,2)$	$(2,1)$
$\emptyset$	1	1
$\{1\}$	1	1
$\{2\}$	1	1
$\{1,2\}$	1	-1

obtemos a matriz $M^{(2)}$ de tamanho 4×2:

$$M^{(2)} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

O próximo lema nos fornece uma ligação entre $c_n(E(V))$ (a sequência das codimensões de $\mathrm{T}(E(V))$ e a matriz $M^{(n)}$ definida acima.

Lema 2.1.3. Seja $c_n(E(V))$ a sequência das codimensões de $\mathrm{T}(E(V))$. Então

$$c_n(E(V)) = \operatorname{rank}\left(M^{(n)}\right).$$

Demonstração. Seja $g(x_1, \ldots, x_n) \in P_n$. Como g é multilinear, ele pertencerá ao T-ideal de $E(V)$ se somente se g se anula para todos os elementos da base D de $E(V)$. Escreva $g(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(n)}$ e considere os α_σ como incógnitas. Então para cada $\{a_i\}_{i=1}^n$ na base de $E(V)$ temos que:

$$g(a_1, \ldots, a_n) = \sum_{\sigma \in S_n} \alpha_\sigma a_{\sigma(1)} \cdots a_{\sigma(n)} = \sum_{\sigma \in S_n} \alpha_\sigma \left(f_I^{(n)}(\sigma)\right) a_1 \cdots a_n = \left(\sum_{\sigma \in S_n} \alpha_\sigma \left(f_I^{(n)}(\sigma)\right)\right) a_1 \cdots a_n.$$

Isso é uma identidade apenas se $\sum_{\sigma \in S_n} \alpha_\sigma f_I^{(n)}(\sigma) = 0$, para todo $I \subseteq I_n$. Isso gera um sistema linear de $n!$ incógnitas α_σ e 2^n equações, sendo a matriz do sistema linear igual a matriz $M^{(n)}$. A dimensão do espaço-solução será $n! - \operatorname{rank}\left(M^{(n)}\right)$ e essa também é a dimensão de $T(E(V)) \cap P_n$. Como $\dim_K P_n = n!$, temos que:

$$c_n(E(V)) = n! - \left(n! - \operatorname{rank}\left(M^{(n)}\right)\right) = \operatorname{rank}\left(M^{(n)}\right).$$

□

O próximo lema será útil para provarmos a questão central dessa seção. A sua demonstração pode ser encontrada no Artigo [9].

Lema 2.1.4. O rank $\left(M^{(n)}\right) \geq 2^{n-1}$.

A próxima definição nos mostrará um novo tipo de álgebra.

Definição 2.1.5. Seja K um corpo. Uma álgebra satisfazendo uma identidade da forma

$$x_1 \cdots x_d = \sum_{\substack{\sigma \in S_d \\ \sigma(1) \neq 1}} k_\sigma x_{\sigma(1)} \cdots x_{\sigma(d)},\ k_\sigma \in K$$

será chamada de uma álgebra do **tipo** J_d.

O próximo teorema, onde uma demonstração pode ser encontrada na página 436 do Artigo [9], é muito importante, pois ele nos fornece um limitante superior para o $c_n(A)$ de uma álgebra A do tipo J_d. E mais, ele nos diz que para cada PI-álgebra A do tipo J_d existe λ inteiro não-negativo tal que

$$0 \leq c_n(A) \leq \lambda^n.$$

Teorema 2.1.6 (Teorema das codimensões de Regev). Seja A uma álgebra do tipo J_d, com $c_n(A)$ sua sequência de codimensões. Então, para qualquer $n \geq 1$, $c_n(A) \leq (d-1)^{n-1}$.

O próximo corolário responde a questão central dessa seção.

Corolário 2.1.7. A codimensão da álgebra de Grassmann $E(V)$ é igual a 2^{n-1}.

Demonstração. Seja $c_n(E(V))$ a sequência de codimensões de $E(V)$. Temos que $[x_1, x_2, x_3] = 0$ é uma identidade polinomial de $E(V)$ (veja o Exemplo 1.3.7), logo

$$0 = [x_1, x_2, x_3] = x_1x_2x_3 - x_2x_1x_3 - x_3x_1x_2 + x_3x_2x_1 \Rightarrow x_1x_2x_3 = x_2x_1x_3 + x_3x_1x_2 - x_3x_2x_1.$$

Portanto, $E(V)$ é uma álgebra do tipo J_3. Logo, pelo Teorema 2.1.6, $c_n(E(V)) \leq 2^{n-1}$. Utilizando os Lemas 2.1.3 e 2.1.4 concluímos que $c_n(E(V)) \geq 2^{n-1}$. Então $c_n(E(V)) = 2^{n-1}$. □

Portanto, podemos observar que a álgebra de Grassmann tem crescimento exponencial de suas sequências de codimensões.

2.2 Séries de Hilbert e outra maneira para calcular a codimensão da álgebra de Grassmann

Esta seção foi escrita tendo por base o livro [7].

Veremos agora como as codimensões e séries de Hilbert da álgebra de Grassmann podem ser calculadas.

Teorema 2.2.1. Seja $\text{car}(K) = 0$ e seja $E = E_K(V)$ a álgebra de Grassmann gerado pelo espaço vetorial V de dimensão infinita sobre o corpo K. Temos que:

1. As codimensões das identidades de E satisfazem:

$$c_n(E) = 2^{n-1},\ n = 1, 2, \ldots,$$

$$c(E,t) = \frac{1-t}{1-2t},$$

$$\widetilde{c}(E,t) = \frac{1}{2}(1+e^{2t}).$$

2. As séries de Hilbert da álgebra relativamente livre $F_m(E)$ são:

$$Hilb(U_m(E), t_1, \ldots, t_m) = \frac{1}{2} + \frac{1}{2}\prod_{i=1}^{m}\frac{1+t_i}{1-t_i},$$

$$Hilb(U_m(E), t) = \frac{1}{2} + \frac{1}{2}\left(\frac{1+t}{1-t}\right)^m.$$

Demonstração. (1.) Sabemos que $\Gamma_n(E)$ é gerado por

$$[x_1, x_2]\cdots[x_{2k-1}, x_{2k}], \quad n = 2k,$$

e $\Gamma_n(E) = 0$ se n é ímpar. Portanto:

$$\gamma_n(E) = \dim(\Gamma_n(E)) = \frac{1}{2}(1+(-1)^n), \quad n = 0, 1, \ldots,$$

$$\gamma(E,t) = \sum_{n\geq 0}\frac{1}{2}(1+(-1)^n)t^n = 1 + t^2 + t^4 + \cdots = \frac{1}{1-t^2} \text{ e}$$

$$\widetilde{\gamma}(E,t) = \sum_{n\geq 0}\frac{1}{2}(1+(-1)^n)\frac{t^n}{n!} = 1 + \frac{t^2}{2!} + \frac{t^4}{4!} + \cdots = \frac{1}{2}(e^t + e^{-t})$$

pois $e^t = 1 + t + \frac{t^2}{2!} + \frac{t^3}{3!} + \cdots$ e $e^{-t} = 1 - t + \frac{t^2}{2!} - \frac{t^3}{3!} + \cdots$.

Logo, utilizando o número 2 do Teorema 1.5.20:

(i)

$$c_n(E) = \sum_{k=0}^{n}\binom{n}{k}\frac{1}{2}(1+(-1)^k) = \binom{n}{0} + 0 + \binom{n}{2} + 0\cdots + \binom{n}{p},$$

onde $p = \begin{cases} n, & \text{se } n \text{ é par} \\ n-1, & \text{se } n \text{ é ímpar} \end{cases}$

Como $\sum_{k=0}^{n}\binom{n}{k} = 2^n$ e $\sum_{k=0}^{n}\binom{n}{k}(-1)^k = 0$ temos que

$$c_n(E) = 2^{n-1}.$$

(ii)

$$c(E,t) = \frac{1}{1-t}\frac{1}{1-\left(\frac{t}{1-t}\right)^2} = \frac{1}{1-t}\frac{(1-t)^2}{1-2t} = \frac{1-t}{1-2t}.$$

(iii)

$$\widetilde{c}(E,t) = e^t\left(\frac{1}{2}(e^t + e^{-t})\right) = \frac{1}{2}(1+e^{2t}).$$

(2.) Como em (1.), $B_m(E)$ tem uma base

$$\left\{[x_{i_1}, x_{i_2}]\cdots[x_{i_{2k-1}}, x_{i_{2k}}] \,|\, 1 \leq i_1 < \cdots < i_{2k} \leq m\right\}.$$

As séries de Hilbert de $B_m(E)$ são iguais à soma dos polinômios simétricos elementares

$$\sum_{k\geq 0} e_{2k}(t_1,\ldots,t_m) = \frac{1}{2}\left(\prod_{i=1}^{m}(1-t_i) + \prod_{i=1}^{m}(1+t_i)\right)$$

e aplicando o número 1 do Teorema 1.5.20, temos:
(i)

$$\begin{aligned} Hilb(U_m(E), t_1, \ldots, t_m) &= \prod_{i=1}^{m}\frac{1}{1-t_i}\left(\frac{1}{2}\left(\prod_{i=1}^{m}(1-t_i) + \prod_{i=1}^{m}(1+t_i)\right)\right) \\ &= \frac{1}{2}\prod_{i=1}^{m}\frac{1}{1-t_i}\cdot\prod_{i=1}^{m}(1-t_i) + \frac{1}{2}\prod_{i=1}^{m}\frac{1}{1-t_i}\cdot\prod_{i=1}^{m}(1+t_i) \\ &= \frac{1}{2}\prod_{i=1}^{m}\frac{1-t_i}{1-t_i} + \frac{1}{2}\prod_{i=1}^{m}\frac{1+t_i}{1-t_i} \\ &= \frac{1}{2} + \frac{1}{2}\prod_{i=1}^{m}\frac{1+t_i}{1-t_i}. \end{aligned}$$

(ii)

$$\begin{aligned} Hilb(U_m(E), t) &= \prod_{i=1}^{m}\frac{1}{1-t}\left(\frac{1}{2}\left(\prod_{i=1}^{m}(1-t) + \prod_{i=1}^{m}(1+t)\right)\right) \\ &= \frac{1}{2}\frac{1}{(1-t)^m}((1-t)^m + (1+t)^m) \\ &= \frac{1}{2} + \frac{1}{2}\left(\frac{1+t}{1-t}\right)^m. \end{aligned}$$

□

2.3 O co-comprimento do T-ideal das identidades da álgebra de Grassmann

Nesta seção, ainda consideraremos que o corpo K tenha característica zero. Nosso objetivo é mostrar que o n-ésimo co-comprimento do T-ideal das identidades da álgebra de Grassmann, denotado por $l_n(E(V))$, é igual a n, para todo $n \in \mathbb{N}$.

Dado o anel $K\langle X\rangle$, podemos identificar P_n com a álgebra KS_n pois a correspondência

$$x_{\sigma(1)}\cdots x_{\sigma(n)} \leftrightarrow \begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix} = \sigma \in S_n$$

se estende a um isomorfismo linear $P_n \cong KS_n$, onde KS_n é a álgebra de grupo de S_n sobre K.

Este isomorfismo leva P_n em um S_n-bimódulo e, portanto, P_n tem uma estrutura de S_n-módulo. Com efeito, S_n age em P_n permutando as variáveis: se $\sigma \in S_n$ e $f(x_1, \ldots, x_n) \in P_n$, então

$$\sigma \cdot f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Por outro lado, o T-ideal das identidades de uma PI-álgebra é invariante sob todas as permutações das variáveis e assim $P_n \cap T(A)$ é um S_n-módulo à esquerda de P_n. Em característica zero, o caráter deste módulo é o n-ésimo co-caráter $\chi_n(A)$ de A.

Lembremos de alguns resultados e notações da teoria das representações. O conjunto de todas as partições do número inteiro positivo n é denotado por $\mathrm{Par}(n)$, e para $\lambda \in \mathrm{Par}(n)$, $[\lambda]$ é o seu correspondente diagrama de Young de n caixas (nós) vazias. Uma tabela de Young T_λ de índice $(1, \ldots, 1)$ para λ é obtida por arrumar os inteiros $1, 2, \ldots, n$ em qualquer ordem nas caixas de $[\lambda]$.

Do exposto acima, e lembrando da Definição 1.1.94 que fala de R_{T_λ} e C_{T_λ}, podemos definir o seguinte elemento de KS_n, que nos ajudará muito mais tarde.

Definição 2.3.1. Fixando uma partição $\lambda \vdash n$ e uma tabela de Young T_λ, definimos o seguinte elemento de KS_n:

$$e(T_\lambda) = \sum_{\sigma \in R_{T_\lambda}} \sum_{\tau \in C_{T_\lambda}} \mathrm{sgn}(\tau)\sigma\tau.$$

Exemplo 2.3.2. Considere as duas partições de n $\lambda_1 = (n)$ e $\lambda_2 = (1, \ldots, 1)$ e sejam as suas tabelas de Young padrão dadas, respectivamente, por

$$T_{\lambda_1} = \boxed{1}\boxed{2}\cdots\boxed{n} \quad \text{e} \quad T_{\lambda_2} = \begin{array}{|c|}\hline 1 \\ \hline 2 \\ \hline \vdots \\ \hline n \\ \hline \end{array}$$

Então $R_{T_{\lambda_1}} = S_n$, $C_{T_{\lambda_1}} = Id$, $R_{T_{\lambda_2}} = Id$ e $C_{T_{\lambda_2}} = S_n$. Logo,

$$e(T_{\lambda_1}) = \sum_{\sigma \in S_n} \sigma \quad \text{e} \quad e(T_{\lambda_2}) = \sum_{\tau \in S_n} \mathrm{sgn}(\tau)\tau.$$

A demonstração do próximo lema pode ser encontrada em [15].

Lema 2.3.3. Para todo $n \geq 1$, KS_n tem a seguinte decomposição:

$$KS_n = \bigoplus_{\lambda \vdash n} I_\lambda \cong \bigoplus_{\lambda \vdash n} M_{d_\lambda}(F),$$

onde $d_\lambda = \chi_\lambda(1)$, $I_\lambda = e_\lambda KS_n \cong M_{d_\lambda}(F)$ é o ideal bilateral minimal de KS_n correspondente à partição λ de n, e

$$e_\lambda = \sum_{\sigma \in S_n} \chi_\lambda(\sigma)\sigma$$

é o idempotente central essencial (veja página 46 do livro [15]).

Em outras palavras, o caráter da representação regular τ de S_n tem a decomposição

$$\chi_\tau = \sum_{\lambda \vdash n} d_\lambda \chi_\lambda.$$

Definição 2.3.4. Para $n \geq 1$, o S_n-caráter de $P_n(A) = P_n/(P_n \cap \mathrm{T}(A))$ é chamado de o **n-ésimo co-caráter de** A (ou do T-ideal $\mathrm{T}(A)$) e é denotado por $\chi_n(A)$.

Se decompormos o n-ésimo co-caráter em irredutíveis, obtemos

$$\chi_n(A) = \sum_{\lambda \vdash n} m_\lambda \chi_\lambda$$

onde χ_λ é o S_n-caráter irredutível da partição $\lambda \vdash n$ e m_λ é a sua respectiva multiplicidade.

Definiremos, agora, objeto central dessa seção:

Definição 2.3.5. Sejam A um álgebra, K um corpo de característica zero e

$$\chi_n(A) = \sum_{\lambda \vdash n} m_\lambda \chi_\lambda$$

a decomposição de $\chi_n(A)$ em S_n-caráteres irredutíveis. Então

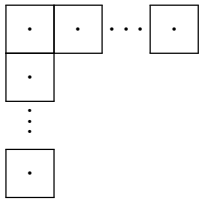
$$l_n(A) = \sum_{\lambda \vdash n} m_\lambda$$

é chamado de **n-ésimo co-comprimento** de A.

Em outras palavras, $l_n(A)$ conta o número de S_n-módulos irredutíveis aparecendo na decomposição de $P_n(A)$. Como no caso de codimensões, se $\mathcal{B}$ é uma variedade de álgebras, escreveremos $l_n(\mathcal{B}) = l_n(A)$ onde A é uma álgebra geradora de $\mathcal{B}$.

Definiremos agora um tipo especial de diagrama de Young que utilizaremos na demonstração do resultado principal desta seção.

Definição 2.3.6. Um **diagrama em forma de gancho** para n é um diagrama $[\lambda]$, para a partição $\lambda = (k, 1^{n-k})$, com $1 \leq k \leq n$. Portanto, $[\lambda]$ tem a forma



Seja λ uma partição de n, usaremos a notação $\lambda \subset H(1,1)$ para dizer que $[\lambda]$ tem a forma de gancho.

Existem, é claro, exatamente n diferentes diagramas em forma de gancho para n. Observe que se $\lambda = (k, 1^{n-k})$, então, do Teorema 1.1.97, temos que

$$d_\lambda = \binom{n-1}{k-1}.$$

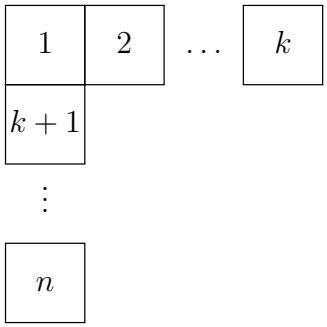
Com base nos lemas anteriores, vamos provar o seguinte teorema que nos fornece o resultado principal desta seção.

Teorema 2.3.7. Para a álgebra de Grassmann de dimensão infinita $E(V)$ sobre um corpo de característica zero, as seguintes condições valem:

1.
$$\chi_n(E(V)) = \sum_{\substack{\lambda \vdash n \\ \lambda \subset H(1,1)}} \chi_\lambda;$$

2.
$$l_n(E(V)) = n.$$

Demonstração. Seja $\lambda = (k, 1^{n-k})$ uma partição e seja $[\lambda]$ a seu correspondente diagrama de Young tem a forma gancho. Construiremos a tabela de Young T_λ por inserir os inteiros $1, 2, \ldots, k$ nas caixas da primeira linha de $[\lambda]$ da esquerda para direita e todos os outros números inteiros restantes $k+1, \ldots, n$ nas caixas da primeira coluna começando da segunda caixa de cima para baixo (veja figura abaixo).



Então
$$R_{T_\lambda} = S_k \quad \text{e} \quad C_{T_\lambda} = S_{n-k+1}\{1, k+1, \ldots, n\}$$
onde $S_m\{i_1, \ldots, i_m\}$ denota a ação do grupo simétrico no conjunto $\{i_1, \ldots, i_m\}$. Aplicando o idempotente essencial e_{T_λ} no monômio $w = x_1 \cdots x_n$, obtemos

$$\begin{aligned} w_k &= e_{T_\lambda} w \\ &= \left(\sum_{\theta \in S_k} \theta \right) \left(\sum_{\tau \in S_{n-k+1}} (\mathrm{sgn}\tau) x_{\tau(1)} x_2 \cdots x_k x_{\tau(k+1)} \cdots x_{\tau(n)} \right) \end{aligned}$$

e afirmamos que w_k não é uma identidade de $E(V)$ (para uma prova deste fato veja página 92 do livro [15]). Isto implica que na decomposição

$$\chi_n(E(V)) = \sum_{\mu \vdash n} m_\mu \chi_\mu$$

todas as multiplicidades m_μ para $\lambda = \lambda^{(k)} = (k, 1_{n-k})$, $k = 1, \ldots n$ são maiores ou iguais a um e

$$c_n(E(V)) \geq \sum_{k=1}^{n} \mathrm{gr}(\chi_{\lambda^{(k)}}).$$

Pela Fórmula do gancho 1.1.97, temos que

$$\mathrm{gr}(\chi_{\lambda^{(k)}}) = \binom{n-1}{k-1}$$

e obtemos o limitante inferior de $c_n(E(V))$, ou seja,

$$c_n(E(V)) \geq \sum_{k=1}^{n} \binom{n-1}{k-1} = 2^{n-1}.$$

Como $c_n(E(V)) \leq 2^{n-1}$ (veja o Teorema 2.1.6 e a prova do Corolário 2.1.7) temos que $c_n(E(V)) = 2^{n-1}$. Todas as identidades de $E(V)$ seguem de $[x_1, x_2, x_3] = 0$ (veja o Teorema 3.2.10). Então todos os caráteres $\chi_{\lambda^{(k)}}$, onde $k = 1, \ldots, n$, têm multiplicidade não nula. O item 2. segue de 1. e do fato que existem exatamente n diferentes diagramas em forma de gancho para n. □

Capítulo 3

Álgebra de Grassmann sobre corpos infinitos de característica positiva

Neste capítulo apresentaremos alguns resultados acerca de álgebras de Grassmann, de certas identidades polinomiais e de T-ideais. Feito isso, exibiremos bases para as identidades polinomiais da álgebra unitária de Grassmann sobre um corpo de característica positiva. Para isso, nos baseamos no artigo [16].

3.1 Notação Preliminar

As álgebras de Grassmann e suas identidades têm um papel importante na teoria das PI-álgebras. Sobre um corpo de característica zero, estas álgebras são os "pilares" para os T-ideais T-primos.

Neste capítulo, vamos utilizar as notações $K_1\langle X\rangle$ e $K\langle X\rangle$ para as álgebras associativas livres com 1 e sem 1, respectivamente, sobre o corpo K, onde $X = \{x_1, x_2, \ldots\}$ é um conjunto infinito enumerável. Lembremos que no capítulo anterior a álgebra unitária infinita de Grassmann foi denotada por $E(V)$, onde V é um espaço vetorial de dimensão infinita, e por $E(V_n)$ a álgebra unitária de Grassmann de dimensão finita, pois neste caso V_n é um espaço vetorial de dimensão finita n.

Se $L\langle X\rangle$ é a álgebra livre de Lie gerada livremente por X então $L\langle X\rangle$ pode ser naturalmente mergulhada em $K_1\langle X\rangle$. Denotaremos por $B\langle X\rangle$ a subálgebra associativa de $K_1\langle X\rangle$ gerada por todos os elementos homogêneos de $L\langle X\rangle$ de grau ≥ 2. Então $B\langle X\rangle$ é gerado sobre K por todos os produtos de comutadores nos geradores livres de X. Chamaremos os elementos de $B\langle X\rangle$ de **polinômios próprios**.

Se trabalharmos com corpos infinitos então toda identidade polinomial é equivalente (como uma identidade) a uma coleção finita de identidades homogêneas, devido ao argumento de Vandermonde (veja Proposição 1.2.12). Portanto, quando o corpo base é infinito, podemos considerar apenas as identidades homogêneas.

Lembremos da definição de álgebra de Grassmann: Seja V um espaço vetorial com base ordenada $\{e_i \mid i \in I\}$. A álgebra de Grassmann unitária $E(V)$ de V é a álgebra associativa gerada por

1 e por $\{e_i \,|\, i \in I\}$ e com as seguintes relações $e_ie_j + e_je_i = 0$, onde se $\text{car}(K) = 2$então $e_i^2 = 0$ para todo $i, j \in I$. Temos, portanto, que uma K-base de $E(V)$ consiste de 1 e de todos os produtos da forma $\{e_{i_1}e_{i_2}\ldots e_{i_m} |\, i_1 < i_2 < \ldots < i_m, m = 1, 2, \ldots\}$. A álgebra $E(V_n)$ é a subálgebra de $E(V)$ gerada por 1 e pelo espaço vetorial V_n. E álgebra de Grassmann não unitária é denotada por $E^*(V)$.

Lembremos, ainda, que $E_0(V)$ é o subespaço da álgebra de Grassmann gerado por todos os elementos de $\beta = \{e_{i_1}e_{i_2}\cdots e_{i_k} |\, k \geq 1;\, i_1 < i_2 < \cdots < i_k\} \cup \{1\}$ que possuem comprimento par e por $E_1(V)$ o subespaço gerado pelos elementos de β que possuem comprimento ímpar, temos, portanto, que $E(V) = E_0(V) \oplus E_1(V)$ é uma $\mathbb{Z}_2$-graduação de $E(V)$ e que $Z(E(V)) = E_0(V)$ se $car(K) \neq 2$ e $ab = -ba$, $\forall a, b \in E_1(V)$. Do exposto acima, temos que $\beta^* = \{e_{i_1}e_{i_2}\cdots e_{i_k} |\, k \geq 1;\, i_1 < i_2 < \cdots < i_k\}$ é a base de $E^*(V)$ a álgebra não unitária de Grassmann de dimensão infinita sobre K.

Quando $\text{car}(K) = p = 2$, então obviamente todas as álgebras descritas acima são comutativas e portanto não são muito interessantes do ponto de vista das identidades polinomiais. Logo, consideraremos apenas o caso que $\text{car}(K) = p > 2$.

Seja J um T-ideal, de uma álgebra A, gerado por um polinômio p. Ao falarmos que dois polinômios f e g são iguais módulo J (ou módulo a identidade p), estamos querendo dizer que $f - g \in J$.

3.2 Álgebras de Grassmann Unitárias

Nesta seção K será um corpo infinito. Lembremos do Exemplo 1.3.7 que a álgebra de Grassmann $E(V)$ satisfaz a identidade $[x_1, x_2, x_3] = 0$.

Seja I o T-ideal, da álgebra associativa livre $K_1\langle X\rangle$, gerado pelo polinômio $[x_1, x_2, x_3]$ e considere

$$\frac{K_1\langle X\rangle}{I}$$

a correspondente álgebra livre de posto enumerável na variedade determinada pelo polinômio $[x_1, x_2, x_3]$.

Lema 3.2.1. Na álgebra associativa livre $K_1\langle X\rangle$ vale a seguinte igualdade:

$$[x_1, x_2, x_1, x_3] = [x_1, x_2][x_1, x_3] + [x_1, x_2, x_3]x_1 - x_1x_1x_2x_3 + x_1x_2x_1x_3 - x_3x_1x_2x_1 + x_3x_1x_1x_2.$$

Demonstração. De fato:

$$\begin{aligned}
&[x_1, x_2][x_1, x_3] + [x_1, x_2, x_3]x_1 - x_1x_1x_2x_3 + x_1x_2x_1x_3 - x_3x_1x_2x_1 + x_3x_1x_1x_2\\
&= (x_1x_2 - x_2x_1)(x_1x_3 - x_3x_1) + [x_1x_2 - x_2x_1, x_3]x_1 - x_1x_1x_2x_3 + x_1x_2x_1x_3 - x_3x_1x_2x_1 + x_3x_1x_1x_2\\
&= x_1x_2x_1x_3 - x_2x_1x_1x_3 - x_1x_2x_3x_1 + x_2x_1x_3x_1 + x_1x_2x_3x_1 - x_2x_1x_3x_1\\
&\quad - x_3x_1x_2x_1 + x_3x_2x_1x_1 - x_1x_1x_2x_3 + x_1x_2x_1x_3 - x_3x_1x_2x_1 + x_3x_1x_1x_2\\
&= x_1x_2x_1x_3 - x_2x_1x_1x_3 - x_1x_1x_2x_3 + x_1x_2x_1x_3 - x_3x_1x_2x_1 + x_3x_2x_1x_1 + x_3x_1x_1x_2 - x_3x_1x_2x_1\\
&= [x_1x_2x_1 - x_2x_1x_1 - x_1x_1x_2 + x_1x_2x_1, x_3]\\
&= [[x_1, x_2, x_1], x_3]\\
&= [x_1, x_2, x_1, x_3].
\end{aligned}$$

□

O próximo lema nos fornece um polinômio que pertence ao T-ideal I.

Lema 3.2.2. O polinômio $[x_1, x_2][x_1, x_3]$ pertence ao T-ideal I.

Demonstração. O polinômio $[x_1, x_2, x_1, x_3]$ pertence à I, pois:

$$[x_1, x_2, x_1, x_3] = [[x_1, x_2, x_1], x_3] = [x_1, x_2, x_1]x_3 - x_3[x_1, x_2, x_1].$$

Utilizando o lema anterior e a igualdade
$x_1x_1x_2x_3 - x_1x_2x_1x_3 + x_3x_1x_2x_1 - x_3x_1x_1, x_2 = [x_1, x_1x_2, x_3] \in I$, temos que:

$$[x_1, x_2][x_1, x_3] = [x_1, x_2, x_1, x_3] + [x_1, x_1x_2, x_3] - [x_1, x_2, x_3]x_1 \in I.$$

□

O seguinte corolário nos informa sobre mais alguns polinômios que pertencem à I. E, como veremos depois, como consequência dele teremos uma importante observação.

Corolário 3.2.3. Os polinômios $[x_1, x_2][x_3, x_4] + [x_1, x_3][x_2, x_4]$, $[x_1, x_2][x_3, x_4] + [x_3, x_2][x_1, x_4]$, $[x_1, x_2][x_3, x_4] + [x_1, x_4][x_3, x_2]$ e $[x_1, x_2][x_3, x_4] + [x_4, x_2][x_3, x_1]$ pertencem à I.

Demonstração. Utilizando o processo de multilinearização, vamos linearizar os seguintes polinômios: $[x_2, x_1][x_1, x_3]$, $[x_1, x_2][x_1, x_3]$, $[x_2, x_1][x_3, x_1]$ e $[x_1, x_2][x_3, x_1]$. Como $[a, b] = -[b, a]$ sabemos, pelo lema anterior, que todos eles pertencem à I. Depois basta trocar apropriadamente os seus índices. Como $\text{car}(K) = p \neq 2$ e o grau de x_1 é igual a 2, a linearização é suficiente para chegarmos à conclusão desejada. Para isso, basta considerarmos uma única vez o polinômio $h(y_1, y_2, x_2, x_3) = f(y_1 + y_2, x_2, x_3) - f(y_1, x_2, x_3) - f(y_2, x_2, x_3)$, onde $f(x_1, x_2, x_3)$ é um dos quatro polinômios mencionados no início da demonstração. □

Observação 3.2.4. Seja σ uma permutação qualquer de S_4. Do corolário anterior temos que, módulo I:

$$[x_{\sigma(1)}, x_{\sigma(2)}][x_{\sigma(3)}, x_{\sigma(4)}] = \text{sgn}(\sigma)[x_1, x_2][x_3, x_4].$$

Lema 3.2.5. A seguinte igualdade sempre é válida na álgebra F:

$$2^n s_{2n}(x_1, \cdots, x_{2n}) = \sum_{\sigma \in S_{2n}} \text{sgn}(\sigma)[x_{\sigma(1)}, x_{\sigma(2)}] \cdots [x_{\sigma(2n-1)}, x_{\sigma(2n)}]$$

Demonstração. Temos que:

$$\begin{aligned} 2^n s_{2n}(x_1, \cdots, x_{2n}) &= 2^n \sum_{\sigma \in S_{2n}} \text{sgn}(\sigma) x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(2n-1)} x_{\sigma(2n)} \\ &= \sum_{\sigma \in S_{2n}} \text{sgn}(\sigma)(2^n x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(2n-1)} x_{\sigma(2n)}). \ (I) \end{aligned}$$

Mas, o somatório $\sum_{\sigma \in S_{2n}} \text{sgn}(\sigma)[x_{\sigma(1)}, x_{\sigma(2)}] \cdots [x_{\sigma(2n-1)}, x_{\sigma(2n)}]$ (II) é igual a (I).
Com efeito, para surgir o elemento $x_{a_1} \cdots x_{a_{2n}}$ de $[x_{\sigma(1)}, x_{\sigma(2)}] \cdots [x_{\sigma(2n-1)}, x_{\sigma(2n)}]$ temos que $x_{\sigma(i)} =$

x_{a_i} e $x_{\sigma(i+1)} = x_{a_{i+1}}$ ou $x_{\sigma(i)} = x_{a_{i+1}}$ e $x_{\sigma(i+1)} = x_{a_i}$, onde $i \in \{1, 3, \ldots, 2n-1\}$. Logo de cada $[x_{\sigma(i)}, x_{\sigma(i+1)}]$ existem 2 possibilidades. Como existem n comutadores na fórmula (II), temos que cada elemento $x_{a_1} \cdots x_{a_{2n}}$ vai aparecer nela 2^n vezes. Todos esses elementos vão ter o mesmo sinal, positivo ou negativo, pois em cada mudança na ordem dos $x_{\sigma(i)}$ em um comutador na fórmula (II) vai implicar na mudança de sinal de $\mathrm{sgn}(\sigma)$, pois neste caso houve uma transposição em σ. Portanto $(I) = (II)$. □

Proposição 3.2.6. Na álgebra $\dfrac{K_1 \langle X \rangle}{I}$, é válida a seguinte igualdade:

$$2^n s_{2n}(x_1, \ldots, x_{2n}) = (2n)!\, [x_1, x_2][x_3, x_4] \cdots [x_{2n-1}, x_{2n}].$$

Demonstração. Com efeito, pela Observação 3.2.4 do Corolário 3.2.3 para todo $\sigma \in S_{2n}$ temos que:

$$[x_{\sigma(1)}, x_{\sigma(2)}][x_{\sigma(3)}, x_{\sigma(4)}] \cdots [x_{\sigma(2n-1)}, x_{\sigma(2n)}] = \mathrm{sgn}(\theta)[x_1, x_2][x_3, x_4] \cdots [x_{2n-1}, x_{2n}],$$

onde θ é o produto de transposições necessárias para mudar a ordem das variáveis no produto $[x_{\sigma(1)}, x_{\sigma(2)}][x_{\sigma(3)}, x_{\sigma(4)}] \cdots [x_{\sigma(2n-1)}, x_{\sigma(2n)}]$ para $[x_1, x_2][x_3, x_4] \cdots [x_{2n-1}, x_{2n}]$. Mas como a paridade de uma permutação não depende das transposições, temos que se σ é par então θ é par e se σ é ímpar então θ é ímpar. Portanto:

$$\begin{aligned}
\sum_{\sigma \in S_{2n}} \mathrm{sgn}(\sigma)[x_{\sigma(1)}, x_{\sigma(2)}] \cdots [x_{\sigma(2n-1)}, x_{\sigma(2n)}] &= \sum_{\sigma \in S_{2n}} \mathrm{sgn}(\sigma)\mathrm{sgn}(\theta)[x_1, x_2][x_3, x_4] \cdots [x_{2n-1}, x_{2n}] \\
&= \sum_{\sigma \in S_{2n}} [x_1, x_2][x_3, x_4] \cdots [x_{2n-1}, x_{2n}] \\
&= (2n)!\, [x_1, x_2][x_3, x_4] \cdots [x_{2n-1}, x_{2n}].
\end{aligned}$$

□

Observação 3.2.7. A última proposição nos diz que se $p < 2n$ então s_{2n} é uma identidade em $E(V)$.

Veremos agora um polinômio que não é uma identidade na álgebra de Grassmann.

Lema 3.2.8. Seja $\mathrm{car}(K) = p > 2$. Então os polinômios definidos por:

$$t_{2n}(x_1, \ldots, x_{2n}) = [x_1, x_2][x_3, x_4] \cdots [x_{2n-1}, x_{2n}]$$

não se anulam na álgebra de Grassmann $E(V)$, para $n = 1, 2, \ldots$.

Demonstração. Pela Observação 1.5.2 e considerando uma base $\{e_1, \ldots, e_{2n}\}$ de V, temos:

$$t_{2n}(e_1, \ldots, e_{2n}) = [e_1, e_2][e_3, e_4] \cdots [e_{2n-1}, e_{2n}] = (2e_1e_2)(2e_3e_4) \cdots (2e_{2n-1}e_{2n}) = 2^n e_1e_2 \cdots e_{2n} \neq 0,$$

pois: $[e_i, e_j] = e_ie_j - e_je_i = e_ie_j - (-e_ie_j) = 2e_ie_j$ e $\mathrm{car}(K) = p > 2$. □

O lema seguinte nos informa qual é o grau mínimo do polinômio *standard* para satisfazer a álgebra de Grassmann $E(V)$ quando $\mathrm{car}(K) = p$.

Lema 3.2.9. Seja $\mathrm{car}(K) = p$, onde p é um número ímpar. O polinômio *standard* s_k é uma identidade polinomial da álgebra de Grassmann $E(V)$ se somente se $k \geq p+1$.

Demonstração. Pela Proposição 3.2.6 e como $\mathrm{car}(K) = p$, s_{p+1} se anula em $E(V)$, pois:

$$2^{(p+1/2)} s_{p+1} = (p+1)!\,[e_1, e_2] \cdots [e_p, e_{p+1}] = 0 \Rightarrow s_{p+1} = 0.$$

Pelo Lema 1.3.12 temos que:

$$\begin{aligned} s_p(e_1e_2, e_3, \ldots, e_{p+1}) &= e_1e_2 s_{p-1}(e_3, \ldots, e_{p+1}) + \sum_{i=2}^{p} (-1)^{i-1} e_{i+1} s_{p-1}(e_1e_2, e_3, \ldots, \widehat{e_i}, \ldots, e_{p+1}) \\ &=^{(1)} e_1e_2 s_{p-1}(e_3, \ldots, e_{p+1}) + 0 \\ &= (p-1)!\, e_1e_2 \cdots e_{p+1} \\ &\neq 0. \end{aligned}$$

(1) Pois $e_1e_2 \in Z(E(V))$ e s_{p-1} é antissimétrico. E o lema está provado. □

O próximo teorema é importante pois nos diz de qual polinômio todas as identidades polinomiais da álgebra de Grassmann $E(V)$ de dimensão infinita são consequências.

Para prová-lo vamos tomar a seguinte estratégia: Considere os espaços $P_n/(P_n \cap \mathrm{T}(E(V)))$ e $P_n/(P_n \cap I)$, onde $I = \{[x_1, x_2, x_3]^T\}$ e $I \subset \mathrm{T}(E(V))$, logo

$$\dim(P_n/(P_n \cap \mathrm{T}(E(V)))) \leq \dim(P_n/(P_n \cap I)).$$

Se todo conjunto $\{f_i\} \subseteq P_n$ que é linearmente independente módulo I também é linearmente independente módulo $\mathrm{T}(E(V))$ então $\dim(P_n/(P_n \cap \mathrm{T}(E(V)))) = \dim(P_n/(P_n \cap I))$. Se conseguirmos provar isso, teremos que $I = \mathrm{T}(E(V))$.

Analogamente, essa estratégia vale para os polinômios comutadores.

Provaremos o próximo teorema apenas para o caso $\mathrm{car}(K) = p > 2$. A prova para o caso $\mathrm{car}(K) = 0$ pode ser encontrada em [9].

Teorema 3.2.10. Sobre um corpo infinito K de característica $p \neq 2$ todas as identidades polinomiais da álgebra de Grassmann $E(V)$ de dimensão infinita são consequências unicamente da identidade $[x_1, x_2, x_3]$.

Demonstração. Consideraremos que $\mathrm{car}(K) = p > 2$. Como $1 \in E(V)$ é suficiente provar que todos as identidades comutadores de $E(V)$ seguem de $[x_1, x_2, x_3]$ (veja Teorema 1.5.18).
Seja $f(x_1, \ldots, x_n) \in B\langle X \rangle$ uma identidade em $E(V)$. Escrevamos $f = \sum \alpha_u u_1 u_2 \cdots u_k$ onde os u_j são os comutadores de tamanho ≥ 2. Da identidade $[x_1, x_2, x_3] = 0$ podemos assumir que todos os comutadores u_i são da forma $[x_a, x_b]$, e eles são centrais. Usando o Lema 3.2.2 podemos considerar f multilinear. Aplicando o Corolário 3.2.3, o polinômio f pode ser reduzido à forma $f(x_1, \ldots, x_n) = \alpha[x_1, x_2][x_3, x_4] \cdots [x_{n-1}, x_n]$, onde $\alpha \in K$ e n é par. Portanto, se $\alpha \neq 0$ em K pelo Lema 3.2.8 temos que f não é uma identidade em $E(V)$. Logo $\alpha = 0$ e então $f \in \{[x_1, x_2, x_3]^T\}$. □

Ainda falta responder se o T-ideal da álgebra de Grassmann possui ou não a propriedade de Specht. O próximo corolário reponderá essa questão.

Corolário 3.2.11. O T-ideal T = T($E(V)$) satisfaz a propriedade de Specht.

Demonstração. Seja T_1 um T-ideal contendo T = T($E(V)$). De acordo com a prova do teorema acima, todo polinômio homogêneo $f \in T_1$ pode ser reduzido, módulo T($E(V)$), à forma $\alpha[x_1, x_2][x_3, x_4] \cdots [x_{n-1}, x_n]$. Escolha o menor n tal que:

$$\alpha[x_1, x_2][x_3, x_4] \cdots [x_{n-1}, x_n] \in T_1, \quad \alpha \neq 0.$$

Então T_1 é gerado como um T-ideal pelo produto acima de comutadores e por $[x_1, x_2, x_3]$. □

Para encerrar este capítulo, exibiremos uma base para as identidades das álgebras de Grassmann $E(V_n)$. Veremos que temos diferenças nessas bases quando $n \leq p$ e $n > p$.

Corolário 3.2.12. Seja $p \leq n < \infty$ e $t = [n/2] + 1$, onde $[a]$ é a função parte inteira do número a. Então as identidades

$$[x_1, x_2, x_3] \quad \text{e} \quad [x_1, x_2][x_3, x_4] \cdots [x_{2t-1}, x_{2t}]$$

formam uma base das identidades da álgebra de Grassmann $E(V_n)$.
E se $n < p$, podemos substituir a última identidade acima pela identidade *standard* s_{n+1} quando n é ímpar, e por s_{n+2} quando n é par.

Demonstração. Se $s < t$ então $[e_1, e_2][e_3, e_4] \cdots [e_{2t-1}, e_{2s}] = 2^t e_1 e_e \cdots e_{2s} \neq 0$ em $E(V_n)$. Mas temos que $[x_1, x_2][x_3, x_4] \cdots [x_{2s-1}, x_{2t}]$ é uma identidade de $E(V_n)$. Com efeito, como este polinômio é multilinear e alternado módulo a identidade $[x_1, x_2, x_3]$ pela Observação 1.5.2 basta verificarmos isso para os elementos de uma base de $E(V_n)$. Mas neste polinômio toda variável aparece em um comutador, portanto substituindo pelo menos um elemento central nos x_i, zeramos o polinômio. Agora, substituindo os elementos restantes da base de $E(V_n)$ que não são centrais nos x_i, devido ao fato de $n = 2([n/2] + 1)$, temos que sempre ao terminar de efetuar as contas dos comutadores e multiplicações, toda parcela resultante tem pelo menos dois elementos e_i iguais. Logo, cada parcela é zero e, como consequência, zera o polinômio. Logo, do exposto acima, a afirmação para $n \geq p$ é verdadeira.
Para provar a afirmação quando $n < p$, utilizaremos um argumento similar ao anterior, mas também, o fato que, módulo o T-ideal gerado por $[x_1, x_2, x_3]$, a identidade $[x_1, x_2][x_3, x_4] \cdots [x_{2s-1}, x_{2t}] = 0$ é equivalente a identidade *standard* $s_{2t} = 0$ e que quando n ímpar temos que:

$$s_{n+1}(1, e_1, e_2, \ldots, e_n) = s_k(e_1, e_2, \ldots, e_n) = n!\, e_1 e_2 \cdots e_n \neq 0.$$

Observando as demonstrações do Teorema 3.2.10 e do Corolário 3.2.11, temos que não existem outras identidades na base além das duas identidades apresentadas no enunciado deste teorema. □

O último corolário implica que não podemos distinguir a álgebra de Grassmann $E(V_{2n})$ da $E(V_{2n+1})$ pelo entendimento de identidades polinomiais pois, eles satisfazem as mesmas identidades, ou seja, T($E(V_{2n})$)= T($E(V_{2n+1})$).

Observação 3.2.13. Para uma descrição das identidades polinomiais na álgebra de Grassmann não unitária veja o artigo *On bases for identities of some varieties of associatives algebras, Pliska Studia Mathematica*, 2, 103-115, 1981 (*Russian*), de autoria de Chiripov e Siderov.

Capítulo 4

Álgebra de Grassmann sobre Corpos Finitos

Neste capítulo estudaremos algumas identidades polinomiais da álgebra de Grassmann, suas codimensões homogêneas e alguns de seus limitantes inferiores e superiores. Mostraremos, também, que as álgebras de Grassmann unitárias e não unitárias satisfazem algumas identidades de classe mas, a álgebra de Grassmann não unitária satisfaz algumas identidades de classe essenciais enquanto a unitária não satisfaz nenhuma. Para isso, nos baseamos no artigo [31].

Com a finalidade de não sobrecarregar a notação, consideramos neste capítulo, salvo menção em contrário, que K será um **corpo finito**, E_K será a álgebra unitária de Grassmann de dimensão infinita sobre K, E_K^* será a álgebra não unitária de Grassmann de dimensão infinita sobre K e $E(V)$ a álgebra de Grassmann gerada pelo espaço vetorial V.

4.1 Algumas identidades de E_K e E_K^*

No artigo [9], é demonstrado que quando a $\mathrm{car}(K) = 0$, a identidade $[x_1, x_2, x_3] = 0$ gera todas as outras identidades de E_K. Este resultado é devido à V. Latyshev. Quando $\mathrm{car}(K) = 2$, temos que todas as álgebras de Grassmann são comutativas, logo satisfazem a identidade $[x_1, x_2] = 0$. Portanto assumiremos que $p \neq 2$. Quando $p > 0$, identidades adicionais aparecem no conjunto gerador de $\mathrm{T}(E_K)$. Algumas delas são dadas nesta seção.

Veremos no próximo lema como reescrever, módulo $\mathrm{T}(E_K)$, um polinômio multihomogêneo f em um polinômio que tenha como um fator um polinômio que é multilinear. Isto será útil mais adiante.

Lema 4.1.1. Seja E_K uma álgebra de Grassmann qualquer e K um corpo qualquer. Seja $f(x_1, \ldots, x_m) \in K\langle x_1, \ldots, x_m\rangle$ um polinômio multihomogêneo de grau maior ou igual a 1 em cada uma das variáveis $x_1, \ldots, x_m$. Então $f(x_1, \ldots, x_m) = x_m^{a_m} \cdots x_1^{a_1} g(x_1, \ldots, x_m)$, módulo $(\mathrm{T}(E_K))$, onde g é multilinear e $a_1, \ldots, a_m \in \mathbb{N}$.

Demonstração. Isto é uma consequência da identidade $[x_1, x_2, x_3] = 0$. Com efeito, considere que $M = M_1 x M_2 x M_3$ seja um monômio de grau maior ou igual a 2 em x portanto, isto módulo a

identidade $[x_1, x_2, x_3] = 0$, temos:
$0 = [M_1, xM_2, xM_3] = M_1(xM_2)(xM_3) - xM_2M_1(xM_3) - (xM_3)M_1(xM_2) + (xM_3)(xM_2)M_1$, logo:

$$\begin{aligned} M &= M_1(xM_2)(xM_3) \\ &= (xM_2)M_1(xM_3) + (xM_3)M_1(xM_2) - (xM_3)(xM_2)M_1 \\ &= x\underbrace{\left(M_2M_1(xM_3) + M_3M_1(xM_2) - M_3(xM_2)M_1\right)}_{M^{(1)}}. \end{aligned}$$

Fazendo o mesmo procedimento para $M^{(1)}$ obtemos:

$$M^{(1)} = xM^{(2)} \Rightarrow M = x^2M^{(2)}.$$

Observe que o grau de x em todo $M^{(i)}$ vai diminuindo a cada procedimento realizado, logo por indução no grau de x chegamos a $M = x^aM^{(a)}$, onde $M^{(a)}$ é um polinômio linear na variável x.

Procedendo do mesmo modo com as outras variáveis, se necessário, chegamos ao resultado. □

Quando $\text{car}(K) = p > 0$, as álgebras E_K e E_K^* satisfazem certas identidades polinomiais. O próximo lema nos dirá quais são essas identidades.

Lema 4.1.2. Considere o polinômio $u_p(x_1, \ldots, x_p) = \sum_{\theta \in S_p} x_{\theta(1)} \cdots x_{\theta(p)}$.

1. Se $\text{car}(K) = p > 0$ então tanto E_K quanto E_K^* satisfazem $u_p(x_1, \ldots, x_p) = 0$.
2. E_K^* satisfaz $x^p = 0$.

Demonstração. (1.) Como $E_K^* \subset E_K$, é suficiente provar que para qualquer $w_1, \ldots, w_p \in E_K$, temos que $u_p(w_1, \ldots, w_p) = 0$. Como o polinômio u_p é multilinear, podemos assumir que $w_1, \ldots, w_p$ são $\mathbb{Z}_2$-homogêneos, ou seja, $w_1, \ldots, w_p \in E_{0(K)} \cup E_{1(K)}$. Assuma primeiro que para algum $1 \leq i \neq j \leq p$, $w_i, w_j \in E_{1(K)}$. Então para qualquer $b \in E_K$, temos:

$$w_ibw_j = -w_jbw_i. \tag{4.1.1}$$

Segue da igualdade 4.1.1 que, em qualquer característica, temos:

$$u_p(w_1, \ldots, w_p) = 0.$$

Portanto, podemos assumir que $w_1, \ldots, w_p$ comutam dois a dois. Então:

$$u_p(w_1, \ldots, w_p) = p! \cdot w_1 \cdots w_p = 0 \cdot w_1 \cdots w_p = 0.$$

(2.) Sejam $w \in E_K^*$, $w = \sum_{i=1}^{r} \alpha_i b_i$, onde $\alpha_i \in K$ e $b_i \in \beta$ (veja Exemplo 1.4.7 da página 42), então:

$$w^p = \sum_{1 \leq i_1, \ldots, i_p \leq r} \alpha_{i_1} \cdots \alpha_{i_p} b_{i_1} \cdots b_{i_p}.$$

Se $r < p$, pelo menos dois b_i's em cada termo $b_{i_1} \cdots b_{i_p}$ são iguais, portanto $b_{i_1} \cdots b_{i_p} = 0$, logo $w^p = 0$.
Assuma que $r \geq p$. Temos:

$$w^p = \sum_{1 \leq i_1, \ldots, i_p \leq r} \alpha_{i_1} \cdots \alpha_{i_p} \, u_p(b_{i_1}, \ldots, b_{i_p}) = 0,$$

pois pela parte (a) temos que $u_p(b_{i_1}, \ldots, b_{i_p}) = 0$. □

Do último lema, podemos tirar as seguintes conclusões:

- Se $k < p$, então $x^k = 0$ não é uma identidade de E_K^*.
- Como $1 \in E_K$, $x^p = 0$ não é uma identidade de E_K.

O corolário abaixo nos fornecerá um polinômio central de E_K, quando $car(K) = p > 0$.

Corolário 4.1.3. A função $x^p : E_K \to K$ é chamada de **polinômio escalar**. Além disso, se $\bar{x} = \alpha + a$ onde $\alpha \in K$ e $a \in E_K^*$, então:

$$\bar{x}^p = \alpha^p \in K.$$

Demonstração. Como $car(K) = p$ segue da Observação 1.1.39, contida na página 10, que:

$$\bar{x}^p = (\alpha + a)^p = \alpha^p + a^p = \alpha^p.$$

□

Veremos no lema abaixo uma identidade polinomial para E_K, quando K é um determinado corpo finito.

Lema 4.1.4. Seja $\text{car}(K) = p$ e a ordem do corpo finito K igual a $|K| = q = p^m < \infty$, então:

1. E_K satisfaz a identidade $(x^q - x)^p = x^{qp} - x^p = 0$.
2. Seja $f(x) \in K[x]$, onde $\text{gr}(f(x)) \geq qp$, uma identidade de uma variável de E_K. Então $(x^q - x)^p$ divide $f(x) \in K[x]$.

Demonstração. (1.) Seja $\bar{x} \in E_K$, pelo Corolário 4.1.3, $\bar{x}^p \in K$, portanto $\bar{x}^{pq} = \bar{x}^p$, pois q é a ordem do corpo finito K.
(2.) Assuma que $f(\bar{x}) = 0$ para todo $\bar{x} \in E_K$. Então $f(\alpha) = 0$ para todo $\alpha \in K$, portanto, como $\alpha^q - \alpha = \alpha - \alpha = 0$, pois q é a ordem do corpo finito F, temos que $(x^q - x) | f(x)$, ou seja:

$$f(x) = (x^q - x) f_1(x).$$

Seja $\bar{x} = \alpha + w$ onde $\alpha \in K$ e $w \in E_K^*$, então utilizando o Corolário 4.1.3 e o número 3 do Lema 1.1.39 temos que:

$$\begin{aligned} 0 &= f(\bar{x}) = (\bar{x}^q - \bar{x}) f_1(\bar{x}) = ((\alpha + w)^{p^m} - (\alpha + w)) f_1(\alpha + w) \\ &= (\alpha^{p^m} + w^{p^m} - \alpha - w) f_1(\alpha + w) = (\alpha + 0 - \alpha - w) f_1(\alpha + w) \\ &= -w f_1(\alpha + w). \end{aligned} \tag{4.1.2}$$

O que implica que:

$$w f_1(\bar{x}) = 0.$$

Utilizando o número 2 do Lema 1.1.39 e como $f_1(x) = \sum_{i=0}^{m} a_i x^i$, onde $a_i \in K$ e $w \in E^*(K)$, temos:

$$\begin{aligned} f_1(\alpha + w) &= \sum_{i=0}^{m} a_i(\alpha + w)^i = \sum_{i=0}^{m} a_i \left(\binom{i}{0} \alpha^i + \sum_{j=1}^{i} \binom{i}{j} \alpha^{i-j} w^j \right) \\ &= \sum_{i=0}^{m} a_i \alpha^i + w \sum_{i=0}^{m} \sum_{j=1}^{i} a_i \alpha^{i-j} w^{j-1} \\ &= f_1(\alpha) + w\, h(\alpha, w) \end{aligned}$$

onde $h(x_1, x_2) = \sum_{i=0}^{m} \sum_{j=1}^{i} a_i x_1^{i-j} x_2^{j-1}$.

Do exposto acima, temos que $f_1(\alpha + w) = f_1(\alpha) + w h(\alpha, w)$. Agora, escolhendo um elemento $w_1 \in \beta^*$, onde $\beta^* = \{e_{i_1} e_{i_2} \cdots e_{i_k} |\ k \geq 1;\ i_1 < i_2 < \cdots < i_k\}$ é a base de E_K^*, do Exemplo 1.4.7 da página 42 sabemos que $E(K) = \bigoplus_{n \geq 0} E(F, n)$, e como $w_1\, f_1(\alpha + w_1) = 0$ (veja igualdade (4.1.2) na página 66), segue que:

$$w_1\, f_1(\alpha) = -w_1^2 h(\alpha, w_1) = 0,$$

pois como $w_1 \in \beta^* \subset E_K^* \Rightarrow w_1^2 = 0$.

Portanto, em particular, como $\alpha \in K$ e $f_1(x) \in K[x]$ implica que $f_1(\alpha) \in K$, de $w_1\, f_1(\alpha) = 0$ temos que $f_1(\alpha) = 0$. Então, novamente, $(x^q - x) | f_1(x)$ e, portanto, $f(x) = (x^q - x)^2 f_2(x)$.

Continuando dessa forma, podemos assumir que $f(x) = (x^q - x)^r f_r(x)$ e $r < p$. Então existe $k \geq 1$ e $w \in E(F, k)$ tal que $w^r \neq 0$ (w^r tem essa propriedade, pois vamos fazer um procedimento análogo ao feito na construção da igualdade (4.1.2) em $f(x) = (x^q - x)^r f_r(x)$, para chegarmos a conclusão que $-w^r f_r(\alpha + w) = 0$), portanto o argumento anterior pode ser repetido para concluir que $f(x) = (x^q - x)^{r+1} f_{r+1}(x)$. Devido ao $\mathrm{gr}(f)$ ser um número finito, este procedimento tem fim. E como $\mathrm{gr}(f(x)) \geq qp$ temos que $(x^q - x)^p$ divide $f(x) \in K[x]$. □

4.2 Limites superiores para a codimensão de E_K e de E_K^*

Nesta seção, veremos alguns resultados acerca das codimensões de E_K e de E_K^* com o objetivo de achar limites superiores para elas. Vamos mostrar também que o T-ideal $\mathrm{T}(E_K^*)$ é homogêneo, porém o T-ideal $\mathrm{T}(E_K)$ não é.

Com essa finalidade, nesta seção, usaremos as seguintes notações, salvo menção em contrário:

- F - corpo finito de característica p;
- R - anel de valorização discreta;
- $K = Q(R)$ - corpo de frações de R;
- $\bar{R} = R/P$, onde P é o ideal maximal do anel de valorização discreta R;
- $B(R)$ - uma PI-álgebra livre sobre R;

- $H = H(R) = H_m(R, d)$ - o conjunto dos polinômios homogêneos sobre R de grau d em $x_1, \ldots, x_m$;
- $B(\bar{R})$ - uma PI-álgebra livre sobre $\bar{R}$; e
- $\bar{H} = H(\bar{R}) = H_m(\bar{R}, d)$ - o conjunto dos polinômios homogêneos sobre $\bar{R}$ de grau d em $x_1, \ldots, x_m$.

Lembremos que $H_m(K, i) \subset K\langle x_1, \ldots, x_m\rangle$ é o conjunto dos polinômios homogêneos nas variáveis $x_1, \ldots, x_m$ de grau i e que se A é uma K PI-álgebra, sua **codimensão homogênea** é dada pela expressão:

$$c(A, H_m(K, i)) = \dim_K \left(\frac{H_m(K, i)}{H_m(K, i) \cap \mathrm{T}(A)} \right).$$

Precisaremos, agora, fazer uso da noção de anel de valorização discreta e de alguns fatos sobre eles. Para maiores detalhes, veja [5] e [13].

Um passo crucial no estudo em PI-álgebras sobre um corpo finito F é a representação dada por $F = R/P$, onde R é um anel de valorização discreta e P é seu ideal maximal (Teorema 1.1.53), tal que $\mathrm{car}(R) = 0$. Tal representação sempre existe.

Um dos fatos sobre anel de valorização discreta que iremos utilizar é que se R_1 é um anel de valorização discreta com P_1 seu ideal maximal e $F_1 = R_1/P_1$ seu corpo quociente e tal que $|F_1| < \infty$ e $F_1 \subset F_2$ onde F_2 é uma extensão finita do corpo F_1, ou seja, $|F_2| < \infty$, então existe um anel de valorização discreta R_2 com $R_1 \subseteq R_2$ com um ideal maximal P_2 satisfazendo:

$$F_2 = R_2/P_2 \ \text{ e } \ P_1 = P_2 \cap R_1.$$

Seja F um corpo finito de característica p. Seja

$$F = F_1 \subset F_2 \subset \cdots$$

uma cadeia ascendente de corpos finitos distintos. Fixemos uma cadeia de anéis de valorização discreta distintos correspondentes

$$R_1 \subset R_2 \subset \cdots,$$

com $P_n = P_{n+1} \cap R_n$.

Denote o corpo de frações de R_n por $K_n = Q(R_n)$, onde $car(K_n) = 0$ e defina

$$B(F_n) := \frac{B(R_n)}{P_n \cdot B(R_n)}.$$

Considere, também, os seguintes conjuntos:

- $Id_m(B(R_n)) \subseteq R_n\langle x_1, \ldots, x_m\rangle$ - as identidades polinomiais de $B(R_n)$ em $R_n\langle x_1, \ldots, x_m\rangle$;
- $Id_m(B(F_n)) \subseteq F_n\langle x_1, \ldots, x_m\rangle$ - as identidades polinomiais de $B(F_n)$ em $F_n\langle x_1, \ldots, x_m\rangle$.

Agora, seguiremos [12] com R e P no lugar de $\mathbb{Z}$ e $p\mathbb{Z}$. Faremos uso das seguinte relações para a definição das P-identidades de classe, cuja importância ficará clara nos dois teoremas subjacentes.

A aplicação canônica $\varphi : R\langle X\rangle \to \bar{R}\langle X\rangle$ satisfaz $\varphi(I) \subseteq J$, onde $I = Id_m(B(R_n))$ e $J = Id_m(B(F_n))$, portanto temos o seguinte diagrama comutativo 3×3, no qual todas as três colunas e a linha do centro são exatas curtas:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I \cap PR\langle X\rangle & \longrightarrow & I & \longrightarrow & J & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & PR\langle X\rangle & \longrightarrow & R\langle X\rangle & \xrightarrow{\varphi} & \bar{R}\langle X\rangle & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P\left[\dfrac{R\langle X\rangle}{I}\right] & \longrightarrow & \dfrac{R\langle X\rangle}{I} & \xrightarrow{\bar{\varphi}} & \dfrac{\bar{R}\langle X\rangle}{J} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Considere $H(R) \subset R\langle X\rangle$, restringindo o diagrama anterior à H e $\bar{H}$ e utilizando as restrições das funções φ e $\bar{\varphi}$ em H e $\bar{H}$, respectivamente, temos o seguinte diagrama comutativo 3×3:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I \cap PH & \longrightarrow & I \cap H & \longrightarrow & J \cap \bar{H} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & PH & \longrightarrow & H & \xrightarrow{\varphi_H} & \bar{H} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P\left[\dfrac{H}{I \cap H}\right] & \longrightarrow & \dfrac{H}{I \cap H} & \xrightarrow{\bar{\varphi}_{\bar{H}}} & \dfrac{\bar{H}}{J \cap \bar{H}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Novamente, todas as três colunas e a linha do centro são exatas curtas.

De posse das informações anteriores, podemos fazer a seguinte definição:

Definição 4.2.1. O conjunto das **P-identidades de classe** de $B(R)$ em $H(R)$, cuja notação é

$CI(B(R), H(R))$, é definido por:

$$CI(B(R), H(R)) = \frac{Ker\,\bar{\varphi}_{\bar{H}}}{P\left(\frac{H}{I\cap H}\right)} \cong \frac{\left(J \cap \bar{H}\right)}{\varphi_H(I \cap H)}.$$

E o polinômio $g(x_1, \ldots, x_n) \in R\langle X\rangle$ será chamado de P**-identidade de** $B(R)$ **em** $H(R)$ se para todo $b_1, \ldots, b_n \in B(R)$, $g(b_1, \ldots, b_n) \in P\left(\frac{H}{I\cap H}\right)$.

Enunciaremos dois teoremas, cujas demonstrações podem ser encontradas em [32], e que serão úteis mais adiante.

Teorema 4.2.2. Nas notações anteriores, temos:

$$c(B(K), H(K)) = c(B(\bar{R}), H(\bar{R})) + \dim_{\bar{R}}[CI(B(R), H(R))]$$

Teorema 4.2.3. Com as mesmas notações do teorema acima, temos que:

1. $c(B(K), H(K)) = c(B(K_n), H(K_n)) + \dim_{K_n}[CI(B(R_n), H(R_n))]$, $\forall n$.
2. A sequência $\{c(B(K_n), H(K_n))\}_{n=1}^{\infty}$ é crescente e limitada, logo tem um limite obtido para algum n_0 (e todos $n \geq n_0$),

$$c(B(K_n), H(K_n)) \xrightarrow{n \to \infty} c(B(K_{n_0}), H(K_{n_0}))$$

   e, portanto:

3. A sequência $\{\dim_{K_n} CI(B(R_n), H(R_n))\}_{n=1}^{\infty}$ é decrescente e tem um limite, também obtido para o mesmo n_0 acima (e todos $n \geq n_0$).

Definição 4.2.4. Para o número n_0 obtido no último teorema, chamamos $CI(B(R_{n_0}), H(R_{n_0}))$ de **identidades de classe essencial** de B em V.

Teorema 4.2.5. Seja $\mathrm{car}(K) = p \neq 0$, onde K é um corpo finito ou infinito.

1. Se $d \geq m(p+1)$, então $c(E_K^*, H_m(K, d)) = 0$.
2. Mais geralmente, se $d \geq k^2 m(p+1)$ então $c(M_k(E_K^*), H_m(K, d)) = 0$.

Demonstração. (1.) Dado $f(x_1, \ldots, x_m) \in H_m(K, d)$, $d \geq m(p+1)$, mostraremos que $f \in \mathrm{T}(E_K^*)$. Pelo Lema 4.1.1 podemos assumir que $f(x_1, \ldots, x_m) = x_m^{a_m} \cdots x_1^{a_1} g(x_1, \ldots, x_m)$ onde g é multilinear em $x_1, \ldots, x_m$. Mas então $a_1 + \cdots + a_m + m = gr(f) = d$ logo $a_1 + \cdots + a_m = d - m \geq mp$, por hipótese, portanto algum $a_i \geq p$ e pelo número 2. do Lema 4.1.2 temos que $x_i^{a_i} = 0$ o que implica em $f(x_1, \ldots, x_m) = 0$ e $c(E_K^*, H_m(K, d)) = 0$.
2.) Seja $f(x_1, \ldots, x_m) \in H_m(K, d)$ e seja $(a_{i,j}^{(r)}) \in M_k(E_K^*)$, onde $r = 1, \ldots, m$. Então:

$$f(a_{i,j}^{(1)}, \ldots, a_{i,j}^{(m)}) = \begin{pmatrix} f_{11}(a_{i,j}^{(r)}) & \cdots \\ \vdots & \ddots \end{pmatrix} \text{ onde } f_{uv}(a_{i,j}^{(r)}) \in H_{k^2 m}(K, d),\ 1 \leq u, v, i, j \leq m.$$

Se $d \geq k^2 m(p+1)$, então por i) cada $f_{uv}(a_{i,j}^{(r)}) = 0$. Então $f(a_{i,j}^{(1)}, \ldots, a_{i,j}^{(m)})) = 0$, isto é $f \in \mathrm{T}(M_k(E_K^*))$, logo $c(M_k(E_K^*), H_m(K, d)) = 0$. □

Corolário 4.2.6. Seja $\bar{R} = R/P$ (onde R é um anel de valorização discreta e P seu ideal maximal), $K = Q(R)$ o corpo quociente de R e $d \geq k^2m(p+1),\ k \geq 1$ então:

$$\dim_K[CI(M_k(E_R^*), H_m(R,d))] = c(M_k(E_{Q(R)}^*), H_m(Q(R),d)),$$

onde

$$c(M_k(E_{Q(R)}^*), H_m(Q(R),d)) = c(M_k(E_{Q(R)}), H_m(Q(R),d))$$

são as codimensões homogêneas das matrizes $k \times k$ sobre as álgebras de Grassmann em característica zero.

Demonstração. Com efeito, denote por $CI(M_k(E_R^*), H_m(R,d))$ as classes de identidades de $M_k(E_R^*)$ originado de $H_m(R,d)$. Pelo Teorema 4.2.2 temos que:

$$c(M_k(E_{Q(R)}^*), H_m(Q(R),d)) = c(M_k(E_{\bar{R}}^*), H_m(\bar{R},d)) + \dim_K[CI(M_k(E_R^*), H_m(R,d))]$$

Mas, pelo Teorema 4.2.5 $c(M_k(E_{\bar{R}}^*), H_m(\bar{R},d)) = 0$, e o resultado é obtido. □

Como este resultado depende apenas de $\mathrm{car}(K) = p$, e não de K, segue de 3. do Teorema 4.2.3 que para qualquer $k \geq 1$, todos os $CI(M_k(E_K^*), H_m(K,d))$ são identidades de classe essencial.

Vejamos agora para E_K. Observe que 1. do Teorema 4.1.4 implica que $\mathrm{T}(E_K)$ não é homogêneo. Denote por $U_m(E_K) = K\langle x_1, \ldots, x_m\rangle / \mathrm{T}(E_K)$ a álgebra relativamente livre de E_K em m variáveis.

O próximo teorema nos fornecerá um limitante superior para $\dim_K(U_m(E_K)) < \infty$.

Teorema 4.2.7. Seja $|K| < \infty$, então

$$\dim_K(U_m(E_K)) \leq \frac{m^{mp|K|+1} - 1}{m-1}.$$

Demonstração. Seja W um K-espaço vetorial de dimensão m, tal que $K\langle x_1, \ldots, x_m\rangle = \bigoplus_{d\geq 0} W^{\otimes d}$. Tal W existe pois $K\langle x_1, \ldots, x_m\rangle$ é um espaço multigraduado. Seja $V_m(n) = \bigoplus_{d=0}^{n} W^{\otimes d}$, então $\dim_K V_m(n) = \sum_{d=0} m^d = 1 + m + m^2 + \cdots + m^n = \frac{m^{n+1}-1}{m-1}$ e a prova segue disto, uma vez que provemos que $K\langle x_1, \ldots, x_m\rangle = V_m(n_0) + \mathrm{T}(E_K)$, onde $n_0 = mp|K|$, pois teremos:

$$\dim_K(U_m(E_K)) = \dim_K\left(\frac{K\langle x_1, \ldots, x_m\rangle}{\mathrm{T}(E_K)}\right) \leq \dim_K(V_m(n_0)) = \frac{m^{n_0+1}-1}{m-1} = \frac{m^{mp|K|+1}-1}{m-1}.$$

Seja $f \in K\langle x_1, \ldots, x_m\rangle$ e mostraremos que $f \in V_m(n_0) + \mathrm{T}(E_K)$. Podemos assumir que f é homogêneo em todas as suas variáveis. Logo, pelo Teorema 4.1.1, temos a seguinte igualdade $f = x_m^{a_m} \cdots x_1^{a_1} g(x_1, \ldots, x_m)$, onde g é multilinear em $x_1, \ldots, x_m$ e $\mathrm{gr}(f) = a_1 + \cdots + a_m + m$. Escreva $|K| = q$ e aplicando Lema 4.1.4 temos que, se $a_i \geq pq$ escrevemos que $a_i = pq + a_i'$, então $x_i^{a_i} = x_i^{pq} x_i^{a_i'} \equiv x_i^{p} x_i^{a_i'} = x_i^{p+a_i'} \equiv \cdots \equiv x_i^{b_i} (\mathrm{mod}\ \mathrm{T}(E_K))$, onde $b_i < pq$. Então existe $b_1, \ldots, b_m < pq - 1$ tal que:

$$f \equiv x_m^{b_m} \cdots x_1^{b_1} g(x_1, \ldots, x_m)\ (\mathrm{mod}\ \mathrm{T}(E_K))$$

e a prova segue de $h = x_m^{b_m} \cdots x_1^{b_1} g \in V_m(n_0)$, pois $\mathrm{gr}(h) \leq m(pq-1) + m$. □

Como T(E_K) não é homogêneo, podemos estudar $c(E_K, V_m(n))$ diretamente.

Corolário 4.2.8. Seja $|K|< \infty$, então para qualquer n,

$$c(E_K, V_m(n)) \leq \frac{m^{mp|K|+1} - 1}{m-1}$$

Demonstração. Como $\dim_K[U_m(E_K)]$ é maior ou igual a qualquer codimensão de E_K na álgebra $K\langle x_1, \ldots, x_m\rangle$, ou seja, $c(E_K, V_m(n)) \leq \dim_K[U_m(E_K)]$, pelo Teorema 4.2.7, o resultado é obtido. □

4.3 As codimensões homogêneas de E_K, com $car(K) = 0$

Seja K qualquer corpo. Veremos nessa seção um subconjunto de monômios $S(m,d) \subseteq H_m(K,d)$ tal que $S(m,d)$ gera $H_m(K,d)$ módulo T(E_K). E que, quando car$(K) = 0$, $S(m,d)$, na verdade, forma uma base de $H_m(K,d)$ módulo T(E_K).

Definição 4.3.1. Fixe $x_1, \ldots, x_m$ e os homogêneos de grau d. Dado k, $1 \leq k \leq m$, sejam $1 \leq i_1 < \cdots < i_k \leq m$ e escreva $V_k(x(i_1, \ldots, i_k))$ os polinômios multilineares em $x(i_1, \ldots, i_k)$. Seja $\{M_j(x(i_1, \ldots, i_k))|1 \leq j \leq 2^{k-1}\}$ um conjunto de monômios que forma uma base de $V_k(x(i_1, \ldots, i_k))$ módulo T(E_K), onde car$(K) \neq 2$. Definamos:

$$S(i_1, \ldots, i_k) = \{x_{i_1}^{a_1} \cdots x_{i_k}^{a_k} M_j(x(i_1, \ldots, i_k))|1 \leq j \leq 2^{k-1}, a_1 + \cdots + a_k = d - k\},$$

onde $S(i_1, \ldots, i_k) = \emptyset$ se $d < k$ e

$$S(m,d) = \bigcup_{k=1}^{m} \bigcup_{x(i_1,\ldots,i_k)} S(i_1, \ldots, i_k)$$

.

Segue do Teorema 4.1.1 que $S(m,d)$ forma um conjunto gerador para $H_m(K,d)$ módulo T(E_K).

Observação 4.3.2. Seja $f(x_1, \ldots, x_m)$ homogêneo em cada uma das sua variáveis (multihomogêneas) que é uma combinação linear dos monômios de $S(m,d)$ e f é uma combinação linear de alguns monômios de $S(m,d)$. Então existe $k \leq m$, $1 \leq i_1 \leq \ldots \leq i_k \leq m$ e $a_1, \ldots, a_k \in \mathbb{N}$ tal que $x_{i_1}^{a_1} \cdots x_{i_k}^{a_k}\, g(x_{i_1}, \ldots, x_{i_k})$, onde $a_1 + \cdots + a_k = d - k$, e g é uma combinação dos monômios $M(x_{i_1}, \ldots, x_{i_k})$ que formam uma base de $V_k(x_{i_1}, \ldots, x_{i_k})$ módulo T(E_K).

O seguinte lema nos mostra um limitante superior para $c(E_K, H_m(K,d))$.

Lema 4.3.3. Em qualquer característica, a codimensão homogênea de E_K satisfaz:

1.
$$c(E_K, H_m(K,d)) \leq |S(m,d)|$$

2.

$$|S(m,d)|= \sum_{k=1}^{m} \binom{d-1}{d-k}\binom{m}{k}2^{k-1}.$$

Demonstração. (1.) Como $S(m,d)$ gera $H_m(m,d)$ módulo T_{E_K}, temos que o resultado está demonstrado.
(2.) Do fato que $S((i_1,\dots i_k),k) = \binom{d-k+k-1}{d-k}2^{k-1} = \binom{d-1}{d-k}2^{k-1}$, e fazendo k variar de 1 até m, temos o resultado desejado. □

Para demonstrar o próximo teorema necessitamos da seguinte definição:

Definição 4.3.4. Sejam $k_1,\dots,k_m$ inteiros e $F_{k_1,\dots,k_m}(E_K)$ igual a dimensão do subespaço de $K\langle x_1,\dots,x_m\rangle/\mathrm{T}(E_K)$ dos polinômios multihomogêneos de multigrau $(k_1,\dots,k_m)$. Diz-se **série de Poincaré** de E_K a série:

$$P_{E_K}(t_1,\dots,k_m) = \sum_{n=0}^{\infty} \sum_{k_1+\cdots+k_m=n} F_{k_1,\dots,k_m}\, t_1^{k_1}\cdots t_m^{k_m}.$$

Lema 4.3.5. Seja

$$\sum_{d\geq 1}\left[\sum_{k=1}^{m}\binom{d-1}{d-k}\binom{m}{k}2^{k-1}\right]t^d = l_m(t)$$

então

$$l_m(t) = \frac{1}{2}\left[\left(\frac{1+t}{1-t}\right)^m - 1\right].$$

Demonstração.

$$\begin{aligned}
l_m(t) &= \sum_{k=1}^{m}\binom{m}{k}2^{k-1}\cdot\sum_{d\geq 1}\binom{d-1}{d-k}t^d \\
&= \sum_{k=1}^{m}\binom{m}{k}2^{k-1}\cdot\left(\frac{t}{1-t}\right)^k \\
&= \frac{1}{2}\sum_{k=1}^{m}\binom{m}{k}\left(\frac{2t}{1-t}\right)^k \\
&= \frac{1}{2}\left[\left(\sum_{k=0}^{m}\binom{m}{k}\left(\frac{2t}{1-t}\right)^k\right) - 1\right] \\
&= \frac{1}{2}\left[\left(1+\frac{2t}{1-t}\right)^m - 1\right]. \\
&= \frac{1}{2}\left[\left(\frac{1-t+2t}{1-t}\right)^m - 1\right] \\
&= \frac{1}{2}\left[\left(\frac{1+t}{1-t}\right)^m - 1\right].
\end{aligned}$$

□

O teorema a seguir, nos fornece as codimensões de E_K, quando $\mathrm{car}(K) = 0$.

Teorema 4.3.6. Se $\mathrm{car}(K) = 0$ então $c(E_K, H_m(K,d)) = |S(m,d)|$.

Demonstração. Pela definição da série de Poincaré $P_{E_K}(t_1, \ldots, t_m)$ de E_K, $\sum_{d\geq 0} c(E_K, H_m(K,d))t^d = P_{E_K}(t, \ldots, t)$, o fato que $\mathrm{T}(E_K)$ é homogêneo quando $p = 0$ é aplicado aqui. Pelo Exemplo 12 do livro [8], $P_{E_K}(t_1, \ldots, t_m) = (1 + e_2 + e_4 + \cdots)/(\prod_{i=1}^m (1 - t_i))$, onde $e_n = e_n(t_1, \ldots, t_m)$ é a n-ésima função simétrica elementar. Como $\prod_{i=1}^m (1 + t_i) = \sum_{l=0}^m e_l$, temos que:

$$P_{E_K}(t_1, \ldots, t_m) = \frac{1}{2}\left[1 + \prod_{i=1}^{m} \frac{1+t_i}{1-t_i}\right].$$

Então $\sum_{d\geq 0} c(E_K, H_m(K,d))t^d = \frac{1}{2}\left[1 + \left(\frac{1+t}{1-t}\right)^m\right]$. Por definição, $c(E_K, H_m(K,0)) = 1$, logo o resultado segue do lema 4.3.5. □

4.4 Limitantes para codimensões homogêneas de E_K, com car(K) diferente de 0

Nesta seção acharemos limitantes para codimensões homogêneas de E_K, $\mathrm{car}(K) = p \neq 0$. Vimos no Lema 4.3.3 um limitante superior $c(E_K, H_m(K,d)) \leq \sum_{k=1}^m \binom{d-1}{d-k}\binom{m}{k}2^{k-1}$.

Para achar um limitante inferior, defina $S_l(m,d) \subset S(m,d)$, $l \in \mathbb{N}$ como segue:

$$S_l(m,d) = \{x_{i_1}^{a_1} \cdots x_{i_k}^{a_k} g(x_{i_1}, \ldots, x_{i_k}) \in S(m,d) \mid 0 \leq a_1, \ldots, a_k \leq l\}.$$

Os dois lemas seguintes serão úteis mais tarde:

Lema 4.4.1. Decomponha $f \in K\langle x_1, \ldots, x_m\rangle$ em suas componentes homogêneas em x_1, onde $f = f_0 + \cdots + f_r$, com $\mathrm{gr}_{x_1}(f_j) = j$, $0 \leq j \leq r$. Logo:

1. Se $f \in \mathrm{T}(E_K)$ e $r \leq |F|+1$ então todos $f_j \in \mathrm{T}(E_K)$ (este limite é provavelmente não maximal).

2. Se $f \in \mathrm{T}(E_K^*)$ então todos os $f_j \in \mathrm{T}(E_K^*)$ para qualquer r.

Demonstração. Provaremos (1.) e (2.). Substitua x_1 por 0 para concluir que $f_0 \in \mathrm{T}(E_K)$ e $f_0 \in \mathrm{T}(E_K^*)$.

Agora, substitua x_i por $\overline{x}_i \in \mathrm{T}(E_K^*)$. Para mostrar em (2.) que $f_1(\overline{x}) = 0$ podemos assumir que $\overline{x}_i \in \beta^*$, pois $\mathrm{gr}_{x_1}(f_1) = 1$. Dados $\overline{x_i} \in \beta^*$ e $\overline{x}_2, \ldots, \overline{x}_m \in \mathrm{T}(E_K^*)$, podemos escolher $\overline{y}_i \in \beta^*$ tal que:
(i) A aplicação $\phi : \overline{y}_1 \to \overline{x}_1$ e $\overline{y}_i \to \overline{x_i}$ com $2 \leq i \leq m$, pode ser estendida a um homomorfismo $\phi : E_K^* \to E_K^*$, para fazer isso basta escolher $\overline{y}_1$ disjunto de $\overline{x}_2, \ldots, \overline{x}_m$ e $(-1)^{l\overline{y}_1} = (-1)^{l\overline{x}_1}$.
(ii) O tamanho da soma em $f_i(\overline{y}_1, \overline{x}_2, \ldots, \overline{x}_m)$ e em $f_j(\overline{y}_1, \overline{x}_2, \ldots, \overline{x}_m)$ são distintos para todos os $1 \leq i \neq j \leq r$, para fazer isso basta escolher $\overline{y}_1 = e_1e_2 + \cdots + e_{2r-1}e_{2r}$, pois:
$(\overline{y}_1)^2 = (e_1e_2 + \cdots + e_{2r-1}e_{2r})^2 = 2\sum e_{i_1}e_{i_2}e_{i_3}e_{i_4},\ i_1 < i_2 < i_3 < i_4$.
Disso temos:
$(\overline{y}_1)^{2r} = \sum e_1 \cdots e_{2r},\ i_1 < i_2 < i_3 < i_4$ e $(\overline{y}_1)^q = 0$ para $q \geq 2r + 1$.

Este mesmo argumento mostra, por 1. do Teorema 4.4.1, que se $w \in E^*(K,n)$ e $\overline{x}_2, \ldots, \overline{x}_m \in E_K$ então $f_j(w, \overline{x}_2, \ldots, \overline{x}_m) = 0$ para $j = 1, \ldots, r$. Seja $\alpha \in K$ e escolha $w \in \beta^*$ disjunto de $\overline{x}_2, \ldots, \overline{x}_m$ e de tamanho par. Então $0 = f_1(\alpha w, \overline{x}_2, \ldots, \overline{x}_m) = w f_1(\alpha, \overline{x}_2, \ldots, \overline{x}_m)$, então $f_1(\alpha, \overline{x}_2, \ldots, \overline{x}_m) = 0$. Depois, se $\overline{x}_1 = \alpha + w$, $\alpha \in K$, $w \in E_K^*$ temos que $f_1(\overline{x}_2, \overline{x}_2, \ldots, \overline{x}_m) = f_1(\alpha, \overline{x}_2, \ldots, \overline{x}_m) + f_1(w, \overline{x}_2, \ldots, \overline{x}_m) = 0$, portanto por i) do Teorema 4.4.1, $f_1 \in \mathrm{T}(E_K^*)$.

Pelo Lema 4.1.1, todos os $f_j \equiv x_1^{j-1} f_j'$ módulo $\mathrm{T}(E_K^*)$, e $x_1^{j-1} \in \mathrm{T}(E_K^*)$ se $j \geq p+1$ por ii) do Lema 4.1.2. Então, por 2. do Lema 4.4.1, $f_j \in \mathrm{T}(E_K^*)$ se $j \geq p+1$ logo $f_2 + \cdots + f_p \in \mathrm{T}(E_K^*)$. Como $|K^*| \geq p+1$, um argumento padrão de Vandermonde, ver Proposição 1.2.12 na página 28, ($x_1 \to \alpha x_1$, $\alpha \in K^*$) mostra que também $f_2, \ldots, f_p \in \mathrm{T}(E_K^*)$. Isto completa a prova de (2.).

Para completar (1.), observe que temos $f_0, f_1 \in \mathrm{T}(E_K)$. Portanto o mesmo argumento acima mostra que $f_2 \in \mathrm{T}(E_K)$. Pelo Lema 4.1.1, podemos assumir que $f_2 = x_1 f_2'(x_1, \ldots x_m)$. Dado $w \in E_K^*, \overline{x}_2, \ldots, \overline{x}_m \in E_K$, vimos acima que $w f_2'(w, \overline{x}_2, \ldots, \overline{x}_m) = 0$. Fazendo $w = u + v$ deduzimos que $u f_2'(v, \overline{x}_2, \ldots, \overline{x}_m) = -v f_2'(w, \overline{x}_2, \ldots, \overline{x}_m)$. Escolha t tal que $u = e_t e_{t+1} e_{t+2}$ é disjunto de $v, \overline{x}_2, \ldots, \overline{x}_m$. Então:
$e_t e_{t+1} e_{t+2} f_2'(v, \overline{x}_2, \ldots, \overline{x}_m) = -v f_2'(e_t e_{t+1} e_{t+2}, \overline{x}_2, \ldots, \overline{x}_m) = -e_t v f_2'(e_{t+1} e_{t+2}, \overline{x}_2, \ldots, \overline{x}_m) =$
$v e_t f_2'(e_{t+1} e_{t+2}, \overline{x}_2, \ldots, \overline{x}_m) = e_{t+1} v e_t f_2'(e_{t+2}, \overline{x}_2, \ldots, \overline{x}_m) = -v e_{t+1} e_t f_2'(e_{t+2}, \overline{x}_2, \ldots, \overline{x}_m) =$
$- e_t e_{t+1} e_{t+2} f_2'(v, \overline{x}_2, \ldots, \overline{x}_m)$.

Ordene as 2^m m-uplas $\underline{z} = (z_1, \ldots, z_m)$ pelos tamanhos $l(\underline{z}(1)) \leq \cdots \leq l(\underline{z}(2^m))$, então por indução em $j \geq 1$ podemos provar que $g(\underline{z}(j)) = 0$. Além disso, $1 \cdot g(\underline{z}(1))$ é a única parcela de $u_1^{a_1} \cdots u_m^{a_m} g(u_1, \ldots, u_m)$ tendo o menor tamanho $l(\underline{z}(1))$, então $1 \cdot g(\underline{z}(1)) = g(\underline{z}(1)) = 0$. Portanto $1 \cdot g(\underline{z}(2))$ é a única parcela com tamanho $l(\underline{z}(2))$, então $g(\underline{z}(2)) = 0$, e assim sucessivamente.

Como $\mathrm{car}(K) \neq 2$, a disjunção implica que $f_2' \in \mathrm{T}(E_K)$, portanto $f_2 \in \mathrm{T}(E_K)$ □

Lema 4.4.2. Seja $g(x_1, \ldots, x_m)$ uma função multilinear. Para cada $1 \leq i \leq m$, escolha $w_i \in \beta(3^{i-1})$, logo $l(w_i) = 3^{i-1}$ e $w_1, \ldots, w_m \neq 0$. Denote $u_i = 1 + w_i$. Então $g \in \mathrm{T}(E_K)$ se somente se $g(u_1, \ldots, u_m) = 0$.

Demonstração. ($\Rightarrow$) Como $g \in \mathrm{T}(E_K)$ temos que $g(u_1, \ldots, u_m) = 0$.
($\Leftarrow$) Antes de começar a prova temos que as 2^m somas $\{\sum_{i=1}^m l_i \mid l_i \in \{0, 3^{i-1}\}\}$ são distintas, elas correspondem a expansão dos inteiros na base 3, com coeficientes 0, 1. Lembrando de $(-1)^{l\overline{y}_1} = (-1)^{l\overline{x}_1}$ de (1) da demonstração do Lema 4.4.1 temos que $l(w) = n$ se $w \in E(K,n) = \mathrm{span}_K \beta(n)$. Agora, assuma que $g(u_1, \ldots, u_m) = 0$ e mostraremos que $g \in \mathrm{T}(E_K)$. Como g é multilinear, $g \in \mathrm{T}(E_K)$ se somente se para todo $d_1, \ldots, d_m \in \{0,1\}$ existem $z_1, \ldots, z_m \in E_{0(K)} \cap E_{1(K)}$ com $d(z_i) = d_i$ e $1 \leq i \leq m$, tal que $z_1 \cdots z_m \neq 0$ e $g(z_1, \ldots, z_m) = 0$.

Agora, dados $d_1, \ldots, d_m \in \{0,1\}$, temos que existe uma escolha $z_i \in \{1, w_i\}$ com $d(z_i) = d_i$ (0 é par e 3^{i-1} são ímpares), e por construção $g(u_1, \ldots, u_m) \neq 0$. Por multilinearidade, $0 = g(u_1, \ldots, u_m) = \sum_{z_i \in \{1, w_i\}} g(z_1, \ldots, z_m)$. Temos que as parcelas em cada $g(z_1, \ldots, z_m)$ tem o mesmo tamanho com $l(g(z_1, \ldots, z_m)) = l(z_1, \ldots, z_m) = \sum_{i=1}^m l(z_i)$ e por construção, todos os tamanhos são distintos. Portanto todos os $g(z_1, \ldots, z_m) = 0$. □

Para provar o teorema central dessa seção precisaremos dos dois importantes lemas, a seguir.

Lema 4.4.3. (**Homogenização**) Decomponha $f \in H_m(K,d)$ como uma soma $f = \sum_l f_l$ onde os f_l são as componentes multihomogêneas distintas de f.

1. Se $f \in \mathrm{T}(E_K)$ e $gr_{x_i}(f) \leq |F|+1$ com $i = 1, \ldots, m$ então todos $f_l \in \mathrm{T}(E_K)$ (este limite é provavelmente não maximal).

2. Se $f \in \mathrm{T}(E_K^*)$ então todos os $f_l \in \mathrm{T}(E_K^*)$. Portanto $\mathrm{T}(E_K^*)$ é homogêneo.

Demonstração. Este lema é consequência direta do Lema 4.4.1. □

Lema 4.4.4. (**Cancelamento**) Seja $g(x_1, \ldots, x_m)$ uma função multilinear, $a_1, \ldots, a_m \in \mathbb{N}$, então $x_1^{a_1} \cdots x_m^{a_m}\, g(x_1, \ldots, x_m) \in \mathrm{T}(E_K)$ se somente se $g(x_1, \ldots, x_m) \in \mathrm{T}(E_K)$.

Demonstração. Escolha $w_i \in E(K, 3^{i-1})$, $l(w_i) = 3^{i-1}$, $w_1 \cdots w_m \neq 0$, $u_i = 1 + w_i$, $1 \leq i \leq m$. Assuma que

$$x_1^{a_1} \cdots x_m^{a_m}\, g(x_1, \ldots, x_m) \in \mathrm{T}(E_K).$$

Portanto $0 = u_1^{a_1} \cdots u_m^{a_m}\, g(u_1, \ldots, u_m) = (1 + \text{parcelas de tamanho } l(y_1) \text{ grande o suficiente})$. Como $f_1(\overline{y}_1, \overline{x}_2, \ldots, \overline{x}_m) + \cdots f_r(\overline{y}_1, \overline{x}_2, \ldots, \overline{x}_m) = 0$, o número (ii) na demonstração do Teorema 4.4.1 implica que $f_j(\overline{y}_1, \overline{x}_2, \ldots, \overline{x}_m) = 0$, e pelo número (i) na demonstração do Teorema 4.4.1 implica que $f_j(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_m) = 0$, para $j = 1, \ldots, r$. Então, por 2. do Teorema 4.4.1 temos que $f_1 \in \mathrm{T}(E_K^*)$. □

De posse dos resultados anteriores, estamos preparados para provar o teorema que nos dará um limitante inferior para $c(E_K, H_m(K, d))$.

Teorema 4.4.5. Seja $|K| = q = p^n$, onde $\mathrm{car}(K) = p \neq 2$, então os monômios em $S_q(m, d)$ são linearmente independentes módulo $\mathrm{T}_m(E_K)$. Segue que :

$$c(E_K, H_m(K, d)) \geq |S_q(m, d)|.$$

Demonstração. Seja $|K| = q$ e $f = \sum_{M \in S_q(m,d)} \alpha_M M \in \mathrm{T}(E_K)$ e mostraremos que todos os α são iguais a zero. Denote $\underline{i} = i_1, \ldots, i_k$ e $\underline{a} = a_1, \ldots, a_k$ e escreva:

$$f = \sum_{k=1}^{m} \sum_{1 \leq i_1 \leq \cdots \leq i_k \leq m} \sum_{a_1 + \cdots + a_k = d-k} \sum_{j=1}^{2^{k-1}} \alpha(k, \underline{i}, \underline{a}, j)\, x_{i_1}^{a_1} \cdots x_{i_k}^{a_k} g(x_{i_1}, \ldots, x_{i_k})\, M_j(x_{i_1}, \ldots, x_{i_k}).$$

Decomponha $f = \sum_l f_l$ onde os f_l são as componentes multihomogêneas de f. Como $gr_{x_i}(f_l) \leq |K|+1$ para todo i, temos que por 1. do Lema 4.4.3 $f_l \in \mathrm{T}(E_K)$ para cada l. Fixe um tal l. Pela Observação 4.3.2 existem $k, \underline{i}, \underline{a}$ tal que

$$f_l = x_{i_1}^{a_1} \cdots x_{i_k}^{a_k}\, g(x_{i_1}, \ldots, x_{i_k}), \text{ onde } g = \sum_{j=1}^{2^{k-1}} \alpha(k, \underline{i}, \underline{a}, j) M_j(x_{i_1}, \ldots, x_{i_k}).$$

Pelo Lema 4.4.4, $g \in \mathrm{T}(E_K)$. Como $\{M_j(x(\underline{i})) \,|\, 1 \leq j \leq 2^{k-1}\}$ forma uma base para $V_k(x(\underline{i}))$ módulo $\mathrm{T}(E_K)$, $\mathrm{car}(K) \neq 2$, temos que todos os $\alpha(k, \underline{i}, \underline{a}, j) = 0$. □

Vejamos agora algumas consequências deste teorema.

Lema 4.4.6. Sejam $N, M, n \in \mathbb{N}$ então:

$$|S_q(m,d)| = \sum_{k=1}^{m} \binom{m}{k} 2^{k-1} \cdot \mathrm{comp}(q+1,k,d)$$

Demonstração. Seja comp'$(N,M,n) = |\{(b_1,\ldots,b_M), \sum b_i = n,\ 0 \le b_1,\ldots,b_M \le M\}|$.
A bijeção induzida pela aplicação $a_i \to b_i+1$ implica que comp'$(N,M,n) = \mathrm{comp}(N+1,M,n+M)$.

Com uma notação similar ao da Definição 4.3.1, seja

$$S_q(i_1,\ldots,i_k,k) = \{x_{i_1}^{a_1}\cdots x_{i_k}^{a_k} M_j(x(i_1,\ldots,i_k)) \in S(i_1,\ldots,i_k,k) | 0 \le a_1,\ldots,a_k \le q\}.$$

Logo do Lema 4.3.3 temos que $|S(i_1,\ldots,i_k,k)| = \mathrm{comp'}(q,k,d-k)2^{k-1}$ e pela união disjunta das i variáveis com os k expoentes vale $S_q(m,d) = \cup_{k=1}^{m} \cup_{(i_1,\ldots,i_k)} S_q(i_1,\ldots,i_k,k)$, assim, temos que:

$$|S_q(m,d)| = \sum_{k=1}^{m} \binom{m}{k} 2^{k-1} \cdot c'(q,k,d-k) = \sum_{k=1}^{m} \binom{m}{k} 2^{k-1} \cdot c(q+1,k,d).$$

□

Corolário 4.4.7. Seja F um corpo finito com $|F| = q$ e seja K um corpo de $\mathrm{car}(K) = 0$. Se $q \ge d-1$ então as duas codimensões homogêneas são iguais, ou seja:

$$c(E_F, H_m(F,d)) = c(E_K, H_m(K,d)).$$

Demonstração. Se $q \ge d-1$, as condições $\sum a_i = d \ge q+1$ implica que todos os $a_i \le q+1$, portanto $\mathrm{comp}(q+1,k,d) = \mathrm{comp}(k,d) = \binom{d-1}{k-1}$ pelo Teorema 1.1.85. Pelos Lemas 4.3.3 e 4.4.6, temos que $|S_q(m,d)| = \sum_{k=1}^{m} \binom{m}{k} 2^{k-1} \binom{d-1}{k-1} = |S(m,d)|$. Agora a demonstração segue dos Teoremas 4.3.6 e 4.4.5. □

Será que E_K, quando K é um corpo finito, satisfaz alguma identidade de classe essencial? O próximo teorema nos dará a resposta a essa questão.

Teorema 4.4.8. Seja K um corpo finito então E_K não satisfaz nenhuma identidade de classe essencial.

Demonstração. Dados um número natural d e um corpo finito K, existe uma extensão de corpo finita K_1 onde $K \subset K_1$ e $|K_1| = q \ge d-1$. Agora, utilizando o Teorema 4.2.3, o resultado é obtido. □

Lembremos que do Corolário 4.2.6 temos que E_K^* satisfaz muitas identidades de classe essenciais.

A demonstração do próximo lema pode ser encontrado na prova do Teorema 4.2 do livro *The Theory of Partitions* (veja [2]).

Lema 4.4.9. Sejam $q, k, d \ge 0$ números naturais, então:

$$\sum_{d \ge 0} \mathrm{comp}(q,k,d) t^d = (t + t^2 + \cdots + t^q)^k.$$

O próximo lema irá calcular as funções geradoras (polinomiais) de $|S_q(m,d)|$.

Lema 4.4.10. Temos que:

$$\sum_{d\geq 0}|S_q(m,d)|\cdot t^d = \frac{1}{2}\left[\left(\frac{1+t-2t^{q+2}}{1-t}\right)^m - 1\right].$$

Demonstração. Pelo Lema 4.4.9 temos que:

$$\sum_{d\geq 0}\mathrm{comp}(q+1,k,d)t^d = (t+t^2+\cdots+t^{q+1})^k = t^k(1-t^{q+1}/1-t)^k.$$

Então, pelo Lema 4.4.6:

$$\begin{aligned}
\sum_{d\geq 0}|S_q(m,d)|\cdot t^d &= \sum_{d\geq 0}\sum_{k=1}^{m}\binom{m}{k}2^{k-1}\cdot\mathrm{comp}(q+1,k,d)t^d = \sum_{k=1}^{m}\binom{m}{k}2^{k-1}\cdot\sum_{d\geq 0}\mathrm{comp}(q+1,k,d)t^d \\
&= \frac{1}{2}\sum_{k=1}^{m}\binom{m}{k}2^k t^k\left(\frac{1-t^{q+1}}{1-t}\right)^k = \frac{1}{2}\sum_{k=1}^{m}\binom{m}{k}\left(\frac{2t}{1-t}\right)^k \\
&= \frac{1}{2}\left[\left(\sum_{k=0}^{m}\binom{m}{k}\left(\frac{2t}{1-t}\right)^k\right) - 1\right] = \frac{1}{2}\left[\sum_{k=0}^{m}\binom{m}{k}(2t)^k\left(\frac{1-t^{q+1}}{1-t}\right)^k - 1\right] \\
&= \frac{1}{2}\left[\left(\sum_{k=0}^{m}\binom{m}{k}(1)^{m-k}\left(2t\cdot\frac{1-t^{q+1}}{1-t}\right)^k\right) - 1\right] = \frac{1}{2}\left[\left(1+\frac{(2t)(1-t^{q+1})}{1-t}\right)^m - 1\right] \\
&= \frac{1}{2}\left[\left(1+\frac{(2t)(1-t^{q+1})}{1-t}\right)^m - 1\right] \\
&= \frac{1}{2}\left[\left(\frac{1+t-2t^{q+2}}{1-t}\right)^m - 1\right].
\end{aligned}$$

□

Referências Bibliográficas

[1] S. A. Amitsur. *A note on PI-rings*. Israel Journal of Mathematics, (10):210–211, 1971.

[2] G. E. Andrews. *The Theory of Partitions*. Encyc. of Math. and its Applications, Addinson-Wesley, Vol. 2, 1976.

[3] A. Berele. *Homogeneous polynomial identities*. Israel Journal of Mathematics, (42):258–272, 1982.

[4] H. Boerner. *Representations of Groups*. North-Holland, Amsterdam, 1963.

[5] N. Bourbaki. *Commutative algebra*. Paris, Hermann; Reading, Mass., Addison-Wesley Pub. Co, 1972.

[6] G. de B. Robinson. *Representation Theory of the Symmetric Group*. University of Toronto Press, Toronto, 1961.

[7] V. Drensky. *Free Algebras and PI-Algebras*. Graduate Course in Algebra, Springer, 1ª Edição, Singapore, 2000.

[8] A. Berele e A. Regev. *Applications of hook Young diagram to PI algebras*. Journal of Algebra, (82):559–567, 1983.

[9] D. Krakowski e A. Regev. *The polynomial identities of the Grassmann algebra*. Transactions of the A.M.S., (181):429–438, 1973.

[10] J. B. Olsson e A. Regev. *An application of Represetation Theory to PI-Algebras*. Proceedings of the American Mathematical Society, (55) Nr 2: 253–257, 1976.

[11] J. B. Olsson e A. Regev. *Colength Sequence of Some T-Ideals*. Journal of Algebra; (38):100–111, 1976.

[12] J. B. Olsson e A. Regev. *Modular cocharacters for P.I. algebras*. J. Algebra; (143):93–118, 1991.

[13] M. F. Atiyah e I. G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, Inc., 1969.

[14] C. Curtis e I. Reiner. *Representation Theory of finite Groups and Associative Algebras*. Wiley-Interscience, 1962.

[15] A. Giambruno e M. Zaicev. *Polynomial identities and asymptotics methods*. American Mathematical Society, 2005.

[16] A. Giambruno e P. Koshlukov. *On the identities the Grassmann Algebras in characteristic $p>0$*. Israel Journal of Mathematics, (122):305–316, 2001.

[17] K. Hoffman e R. Kunze. *Linear Algebra*. Prentice-Hall; 2ª Edição, 1971.

[18] A. Garcia e Y. Lequain. *Elementos de Álgebra*. Projeto Euclides, IMPA, Rio de Janeiro, 2003.

[19] I. N. Herstein. *Noncommutative rings*. Carus Math. Monograph (15), Wiley and Sons, Inc, New York, 1968.

[20] N. Jacobson. *Structure of Rings*. American Mathematical Society Colloquium Publications 37; 2º Edição; American Mathematical Society; Providence; R.I., 1964.

[21] N. Jacobson. *PI-Algebras: An introduction*. Lecture Notes in Math., Springer–Verlag, Berlin–New York, 1975.

[22] I. Kaplanski. *Rings with a polynomial identity*. Bull. Amer. Math. Soc., (54):575–580, 1948.

[23] A. Kerber. *Representations of Permutation Groups. I*. Lectures Notes in Mathematics; Volume 240; Springer-Verlag; Berlim/New York, 1971.

[24] J. Lambek. *Lectures on Rings and Modules*. AMS Chelsea Publishing, 1966.

[25] S. Lang. *Algebra*. Addison–Wesley, Reading, Mass., 1965, 2ª Edição, 1984.

[26] E. L. Lima. *Álgebra Linear*. Coleção Matemática Universitária; IMPA; Rio de Janeiro; 2ª Edição, 1996.

[27] D. G. Northcott. *Multilinear algebra*. Cambridge University Press, 1984.

[28] C. Procesi. *Rings with polynomial identities*. Pure and Applied Mathmatics, 17, Marcel Dekker, Inc., New York, 1973.

[29] A. Regev. *Existence of polynomial identities of $A \otimes_F B$*. Bulletin of American Mathematical Society, (77) Nr 6:1067–1069, 1971.

[30] A. Regev. *Existence of identities in $A \otimes B$*. Israel Journal of Math., (11):131–152, 1972.

[31] A. Regev. *Grassmann Algebras over Finite Fields*. Communications in Algebra, (19):1829–1849, 1991.

[32] A. Regev. *Remarks on P.I. Algebras over Finite Fields*. Journal of Algebra, (145):249–261, 1992.

[33] L. H. Rowen. *Polynomial Identities in Ring Theory*. Academic Press, 1980.

[34] J. P. Serre. *Linear Representations of Finite Groups*. Graduate Texts in Mathematics (42); Springer; 2ª Edição, 1977.

[35] O. M. Di Vincenzo. *A note on the identities of the Grassmann algebras*. Boll. Un. Mat. Ital., (5-A):307–315, 1991.

[36] H. Weyl. *The Classical Groups,Their Invariants and Representations*. Princeton Univ. Press, Princeton, 1997.