UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Identidades e polinômios centrais com involução para a álgebra das matrizes triangulares superiores 2×2

Ronald Ismael Quispe Urure

São Carlos - SP
2018

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Identidades e polinômios centrais com involução para a álgebra das matrizes triangulares superiores 2×2

Ronald Ismael Quispe Urure

Tese apresentada ao Programa de Pós-Graduação em Matemática da UFSCar como parte dos requisitos para obtenção do Título de Doutor em Matemática.
Orientador: Prof. Dr. Dimas José Gonçalves

São Carlos - SP
Agosto de 2018

Resumo

Seja F um corpo de característica diferente de 2. Denote por $UT_2(F)$ a F-álgebra das matrizes triangulares superiores 2×2. Se $*$ é uma involução do primeiro tipo de $UT_2(F)$, denote por $Id(UT_2(F), *)$ e $C(UT_2(F), *)$ o conjunto das suas $*$-identidades polinomiais e $*$-polinômios centrais, respectivamente. Neste trabalho, descrevemos:

a) $Id(UT_2(F), *)$ quando F é finito.

b) $C(UT_2(F), *)$ quando F é um corpo qualquer.

Abstract

Let F be a field of characteristic different from 2. Denote by $UT_2(F)$ the 2×2 upper triangular matrices F-algebra. If $*$ is a involution of first kind of $UT_2(F)$, denote by $Id(UT_2(F),*)$ and $C(UT_2(F),*)$ the set of its $*$-polynomial identities and $*$-central polynomials, respectively. In this work, we describe:

a) $Id(UT_2(F),*)$ when F is finite.

b) $C(UT_2(F),*)$ when F is any field.

Sumário

Capítulo 1

Introdução

O assunto a ser tratado nesta tese está inserido no contexto da *Teoria das PI-álgebras*, isto é, álgebras que satisfazem identidades polinomiais. Obteremos alguns resultados que dizem respeito a álgebra $UT_n(F)$ das matrizes triangulares superiores $n \times n$ com entradas num corpo F.

Fixado tal corpo, sejam $X = \{x_1, x_2, \ldots\}$ um conjunto infinito enumerável e $F\langle X\rangle$ a álgebra associativa livre com unidade, livremente gerada por X. Denote por $Id(A)$ o conjunto dos polinômios de $F\langle X\rangle$ que são identidades polinomiais para uma álgebra A.

Em 1971, Maltsev ([18]) descreveu $Id(UT_n(F))$ quando F é de característica 0. Posteriormente, em 1981, Siderov ([21]) descreveu tal conjunto quando F é um corpo qualquer.

A descrição de $Id(A)$ para uma dada álgebra A é uma das linhas de pesquisa na área. Em 1950, Specht ([24]) propôs o seguinte:

Problema: $Id(A)$ é um T-ideal finitamente gerado ?

Em 1987, Kemer ([16]) respondeu "sim" para o problema, quando a característica de F é 0. Em 1999, Belov ([3]), Grishin ([14]) e Shchigolev ([23]) responderam "não", para os demais corpos.

Nestes trabalhos de 1999 surge o conceito de T-espaço, e portanto o interesse em descrever o conjunto dos polinômios centrais de uma determinada álgebra A, o qual denotaremos por $C(A)$, se intensificou. Com respeito a $UT_n(F)$ temos

$$C(UT_n(F)) = Id(UT_n(F)) + F. \tag{1.1}$$

Sugerimos ao leitor as referências [4, 6, 8, 19] para o estudo (descrição) dos polinômios centrais de outras álgebras importantes.

De agora até o fim deste capítulo introdutório, o corpo F será de característica diferente de 2 e as involuções consideradas serão do primeiro tipo. Sejam $X = \{x_1, x_2, \ldots\}$ e $X^* = \{x_1^*, x_2^*, \ldots\}$ dois conjuntos infinitos enumeráveis e disjuntos. Denote por $F\langle X \cup X^*\rangle$ a álgebra associativa livre com unidade, livremente gerada por $X \cup X^*$. Tal álgebra tem uma involução natural, a qual fixaremos. Dada uma álgebra A com uma involução $*$, denotamos por $Id(A,*)$ o conjunto de todos elementos em $F\langle X \cup X^*\rangle$ que são $*$-identidades polinomiais de A.

Note que o Problema de Specht pode ser formulado no formato "com involução":

Problema: $Id(A,*)$ é um T($*$)-ideal finitamente gerado ?

Em 2017, Aljadeff, Giambruno e Karasik ([1]) e também Sviridova ([25]) responderam "sim" para o problema, quando a característica de F é 0.

Em 2006, Di Vincenzo, Koshlukov e La Scala ([27]) descreveram as involuções de $UT_n(F)$. Além disso, descreveram:

a) $Id(UT_2(F), *)$ quando F é infinito.

b) $Id(UT_3(F), *)$ quando F é de característica 0.

Em 2018, Urure e Gonçalves ([26]) descreveram $Id(UT_2(F), *)$ quando F é finito. Permanece em aberto a descrição de $Id(UT_n(F), *)$ para os demais casos. Os resultados que aparecem em ([26]) fazem parte desta Tese de Doutorado.

Dada uma álgebra A com uma involução $*$, denotamos por $C(A, *)$ o conjunto de todos elementos em $F\langle X \cup X^* \rangle$ que são $*$-polinômios centrais de A.

Nesta Tese apresentamos a descrição de $C(UT_2(F), *)$ para toda involução $*$ e todo corpo F. Permanece em aberto a descrição de $C(UT_n(F), *)$ para $n \geq 3$. Salientamos que, diferente do caso (1.1), temos

$$C(UT_2(F), *) \neq Id(UT_2(F), *) + F. \tag{1.2}$$

Esta Tese está dividida da seguinte maneira:

Capítulo 2. Um capítulo com definições e alguns resultados necessários para a compreensão dos capítulos seguintes. Destaca-se definição e resultados básicos de $*$-identidades polinomiais e a apresentação das involuções de $UT_2(F)$ descritas em ([27]).

Capítulo 3. Descrição de $Id(UT_2(F), *)$ quando F é finito. Como $UT_2(F)$ possui apenas duas involuções, a menos de equivalência, reservamos uma seção para o estudo separado de cada uma. Os resultados aqui apresentados são originais e estão publicados em ([26]).

Capítulo 4. Descrição de $C(UT_2(F), *)$ quando F é um corpo qualquer. Os resultados aqui apresentados são originais e foram submetidos para publicação.

Capítulo 2

Preliminares

Nesta tese, F denotará um corpo e $|F|$ a sua cardinalidade. Todas as álgebras consideradas neste trabalho serão associativas com unidade sobre F. Assim, em algumas passagens, escreveremos simplesmente *álgebra* ao invés de *álgebra associativa com unidade sobre F*.

Neste capítulo preliminar, daremos algumas definições e resultados básicos da Teoria das PI-álgebras. Sugerimos ao leitor as referências [10, 11, 12, 13, 20, 27] para o estudo e maior aprofundamento do assunto.

2.1 Identidades polinomiais

Nesta seção enunciaremos alguns fatos conhecidos a respeito das identidades polinomiais da álgebra das matrizes triangulares superiores, algumas propriedades do corpo F e fixaremos algumas notações.

Seja $X = \{x_1, x_2, \ldots\}$ um conjunto infinito enumerável e seja $F\langle X\rangle$ a álgebra associativa livre com unidade, livremente gerada por X. Um elemento de $F\langle X\rangle$ que será muito utilizado nesta tese é o *comutador*

$$[x_{i_1}, x_{i_2}] = x_{i_1}x_{i_2} - x_{i_2}x_{i_1}.$$

De forma indutiva, um comutador de comprimento $n \geq 2$ será um polinômio da forma

$$[x_{i_1}, \ldots, x_{i_n}] = [[x_{i_1}, \ldots, x_{i_{n-1}}], x_{i_n}].$$

Combinações lineares de produtos de comutadores têm um papel importante na descrição das identidades polinomiais de uma dada álgebra. Veja [10, Proposição 4.3.3] para detalhes.

Um polinômio $f = f(x_1, \ldots, x_n) \in F\langle X\rangle$ é uma *identidade polinomial* para uma álgebra A se

$$f(a_1, \ldots, a_n) = 0$$

para todos $a_1, \ldots, a_n \in A$. Denotamos por $Id(A)$ o conjunto de todas as identidades polinomiais de A. Se $Id(A) \neq \{0\}$, dizemos que A é uma *PI-álgebra*.

O conjunto $Id(A)$ tem uma propriedade interessante: ele é um T-ideal. Um *T-ideal* é um ideal de $F\langle X\rangle$ fechado por endomorfismos de $F\langle X\rangle$. Como a interseção de T-ideais é um T-ideal, dizemos que a interseção de todos os T-ideais que contêm um dado subconjunto S de $F\langle X\rangle$ é o *T-ideal gerado por S*.

Uma álgebra importante para a Teoria das PI-álgebras e que será objeto principal de estudo nesta tese é a álgebra das matrizes triangulares superiores $n \times n$ com entradas no corpo F, a qual denotamos por $UT_n(F)$. Se $a_1, a_2 \in UT_n(F)$, então $[a_1, a_2]$ é uma matriz triangular superior com diagonal nula. Logo,

$$[a_1, a_2][a_3, a_4] \ldots [a_{2n-1}, a_{2n}] = 0$$

para todos $a_1, \dots, a_{2n} \in UT_n(F)$. Isso mostra que

$$[x_1, x_2][x_3, x_4] \dots [x_{2n-1}, x_{2n}] \tag{2.1}$$

é uma identidade polinomial para $UT_n(F)$. O matemático Maltsev demonstrou a importância do polinômio (2.1) na descrição das identidades polinomiais de $UT_n(F)$. Em [18] foi provado o seguinte:

Teorema 2.1.1 (Maltsev)**.** *Se F é um corpo de característica 0, então $Id(UT_n(F))$ é gerado, como um T-ideal, pelo polinômio*

$$[x_1, x_2][x_3, x_4] \dots [x_{2n-1}, x_{2n}].$$

Chamamos a atenção do leitor para o seguinte fato: o teorema acima permanece válido se F é um corpo infinito. De um modo geral, o matemático Siderov provou em ([21]) que se F é um corpo qualquer (finito ou infinito), então

$$Id(UT_n(F)) = [Id(UT_1(F))]^n.$$

Portanto, a descrição de $Id(UT_n(F))$ depende da descrição de $Id(UT_1(F)) = Id(F)$. Tal descrição pode ser obtida em [10, Exercício 2.3.6 e Exercício 4.3.7] conforme abaixo:

Teorema 2.1.2. *Se F é um corpo infinito, então $Id(F)$ é gerado, como um T-ideal, pelo comutador $[x_1, x_2]$. Se F é um corpo finito com q elementos, então $Id(F)$ é gerado, como um T-ideal, pelos polinômios*

$$[x_1, x_2] \quad e \quad x_1^q - x_1.$$

Observe no teorema acima o surgimento do polinômio $x_1^q - x_1$ quando $|F| = q$. Como $F - \{0\}$ é um grupo, com respeito a multiplicação, temos que $a^{q-1} = 1$ para todo $a \in F - \{0\}$ e portanto $a^q = a$ para todo $a \in F$. Logo, de fato,

$$(x_1^q - x_1) \in Id(F).$$

Usaremos com frequência essa informação e os próximos lemas desta seção no estudo das $*$-identidades para $UT_2(F)$ quando F é finito.

Lema 2.1.3. *Considere um polinômio $f \in F\langle X \rangle$ dado por*

$$f(x_1, \dots, x_n) = \sum_{d_1=0}^{k} \cdots \sum_{d_n=0}^{k} \alpha_{(d_1,\dots,d_n)} x_1^{d_1} \cdots x_n^{d_n},$$

onde $\alpha_{(d_1,\dots,d_n)} \in F$. Se $f \in Id(F)$ e $k < |F|$, então $\alpha_{(d_1,\dots,d_n)} = 0$ para todo $(d_1, \dots, d_n)$.

Demonstração. Como $\deg_{x_i} f < |F|$ para todo i, temos por [10, Proposition 4.2.3] que cada

$$f_{(d_1,\dots,d_n)} = \alpha_{(d_1,\dots,d_n)} x_1^{d_1} \cdots x_n^{d_n}$$

é uma identidade polinomial para F. Em particular,

$$0 = f_{(d_1,\dots,d_n)}(1, \dots, 1) = \alpha_{(d_1,\dots,d_n)}.$$

Concluímos a demonstração. $\square$

Para o próximo lema, dado um polinômio

$$h(x) = \sum_{i=0}^{d} \alpha_i x^i, \ \alpha_i \in F,$$

denotamos por $h'(x)$ a derivada de $h(x)$. Assim,

$$h'(x) = \sum_{i=1}^{d} i\alpha_i x^{i-1}.$$

Lema 2.1.4. *Seja F um corpo finito com $|F| = q$. Considere um polinômio $h(x)$ com grau $\deg(h) \leq 2q-1$. Denote por $h'(x)$ a derivada de $h(x)$. Se $h(a) = h'(a) = 0$ para todo $a \in F$, então $h(x) = 0$.*

Demonstração. Denote $F = \{a_1, \ldots, a_q\}$ e considere o polinômio

$$u(x) = \prod_{i=1}^{q} (x - a_i).$$

Como $h(a) = 0$ para todo $a \in F$, temos pelo teorema do resto que

$$h(x) = u(x)v(x) \tag{2.2}$$

para algum polinômio $v(x)$. Note que $\deg(v) \leq q-1$, pois $\deg(u) = q$ e $\deg(h) \leq 2q-1$.

Derivando $h(x)$ obtemos

$$h'(x) = u'(x)v(x) + u(x)v'(x).$$

Fixado $1 \leq j \leq q$, como $u(a_j) = 0$ e $h'(a_j) = 0$, segue que

$$u'(a_j)v(a_j) = 0. \tag{2.3}$$

Derivando u temos

$$u'(x) = \sum_{i=1}^{q} (x - a_1) \cdots \widehat{(x - a_i)} \cdots (x - a_q).$$

Logo,

$$u'(a_j) = \prod_{i \neq j} (a_j - a_i) \neq 0$$

e, por (2.3), $v(a_j) = 0$. Como j é arbitrário, $v(x) \in Id(F)$. Assim, pelo Lema 2.1.3, segue que $v(x) = 0$ e, por (2.2), $h(x) = 0$. □

2.2 Polinômios centrais

Nesta seção enunciaremos alguns fatos a respeito de polinômios centrais e fixaremos algumas notações.

Dada uma álgebra A, denotamos por $Z(A)$ o seu centro. Assim,

$$Z(A) = \{z \in A \ : \ az = za, \ \forall a \in A\}.$$

É fato conhecido que o centro de $UT_n(F)$ é formado por todas as matrizes escalares.

Um polinômio $f = f(x_1, \ldots, x_n) \in F\langle X\rangle$ é um *polinômio central* para uma álgebra A se

$$f(a_1, \ldots, a_n) \in Z(A)$$

para todos $a_1, \ldots, a_n \in A$. Denotamos por $C(A)$ o conjunto de todos os polinômios centrais de A. Note que

$$F + Id(A) \subseteq C(A).$$

Aqui cabe uma observação: alguns livros costumam excluir da definição de polinômio central os elementos em $F + Id(A)$, pela motivo óbvio acima. Mas nesta tese, assim como em outros trabalhos, esses elementos serão incluídos, conforme definição acima.

Para a álgebra de matrizes $M_n(F)$ é conhecido que

$$F + Id(M_n(F)) \neq C(M_n(F)).$$

Um problema em aberto consiste em descrever o grau mínimo de um elemento em

$$C(M_n(F)) - (F + Id(M_n(F)))\,.$$

Sugerimos ao leitor a referência [10, Seção 7.3] para um melhor entendimento e história do problema citado.

Para matrizes triangulares é bem conhecido o seguinte fato:

Proposição 2.2.1. *Para todo corpo F (finito ou infinito) e todo $n \geq 2$ vale*

$$C(UT_n(F)) = Id(UT_n(F)) + F.$$

Demonstração. Ver por exemplo [20, Exercício 1.4.2], e comentário em [12, Exemplo 3.2] quando F é infinito. Ou ainda, veja [15, Exemplo 1.4.6]. □

Veremos no Capítulo 4 que a proposição acima não é válida se considerarmos polinômios centrais com involução.

2.3 Involuções

Ao longo desta seção, F denotará um corpo de característica $car(F) \neq 2$. Enunciaremos as definições e propriedades básicas a respeito de álgebras com involuções. Além disso, caracterizaremos as involuções de $UT_2(F)$ do "primeiro tipo".

Seja A uma álgebra e seja $* : A \to A$ uma função. Dizemos que $*$ é uma *involução* sobre A se os três itens abaixo são satisfeitos:

a) $(a + b)^* = a^* + b^*$ para todos $a, b \in A$,

b) $(ab)^* = b^*a^*$ para todos $a, b \in A$,

c) $(a^*)^* = a$ para todo $a \in A$.

Se $a^* = a$ para todo $a \in Z(A)$ (centro de A), então $*$ é chamado *involução do primeiro tipo* sobre A. Caso contrário, $*$ é chamado *involução do segundo tipo* sobre A. De agora em diante, consideraremos apenas involuções do primeiro tipo. Neste caso,

$$(\lambda a)^* = \lambda(a^*)$$

para todo $\lambda \in F$, $a \in A$. Ou seja, se $*$ é involução do primeiro tipo, então $*$ é uma transformação linear também.

Por exemplo, em $UT_2(F)$ temos duas involuções, denotadas por $\star$ e s, que são importantes e serão objeto de estudo nesta tese:

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}^{\star} = \begin{pmatrix} b & c \\ 0 & a \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}^{s} = \begin{pmatrix} b & -c \\ 0 & a \end{pmatrix} \tag{2.4}$$

para todos $a, b, c \in F$.

Convencionaremos que a frase " $(A, *)$ é uma álgebra com involução" significa "A é uma álgebra com involução $*$".

Sejam $(A, *)$ e $(B, \circ)$ álgebras com involução. A função $\varphi : A \to B$ é dita ser um *homomorfismo de álgebras com involução* se φ for um homomorfismo de álgebras e se

$$\varphi(a^*) = (\varphi(a))^{\circ}$$

para todo $a \in A$. Se, ainda mais, φ for bijetora, dizemos que φ é um *isomorfismo de álgebras com involução* e denotamos $(A, *) \simeq (B, \circ)$.

Em [27] os matemáticos Di Vincenzo, Koshlukov e La Scala descreveram todas as involuções do primeiro tipo de $UT_n(F)$. Em particular, provaram o seguinte:

Corolário 2.3.1. *Sejam $\star$ e s as duas involuções definidas em (2.4). Se $*$ é uma involução do primeiro tipo sobre $UT_2(F)$, então*

$$(UT_2(F), *) \simeq (UT_2(F), \star) \quad \textit{ou} \quad (UT_2(F), *) \simeq (UT_2(F), s).$$

Ainda mais, $(UT_2(F), \star)$ e $(UT_2(F), s)$ não são isomorfas como álgebras com involução.

Demonstração. Veja [27, Proposições 2.5 e 2.6]. □

Finalizamos esta seção enunciando os conceitos de elementos simétrico e antissimétrico. Seja A uma álgebra com involução $*$. Dizemos que $a \in A$ é *simétrico* se $a^* = a$; e *antissimétrico* se $a^* = -a$. Denote por A^+ e A^- os seguintes subespaços vetoriais de A: $A^+ = \{a \in A : \ a^* = a\}$ e $A^- = \{a \in A : \ a^* = -a\}$. Se $a \in A$ então

$$a = (1/2)(a + a^*) + (1/2)(a - a^*).$$

Observe que $a + a^*$ é simétrico, e $a - a^*$ é antissimétrico. Logo,

$$A = A^+ \oplus A^- \tag{2.5}$$

como espaços vetoriais. Na igualdade acima usamos o fato que existe o elemento $1/2 \in F$. Isso de fato é verdade, pois $car(F) \neq 2$.

2.4 $*$-identidades polinomiais

Ao longo desta seção, todas as involuções consideradas serão do primeiro tipo. Além disso, para falarmos em involução assumimos $\mathrm{car}(F) \neq 2$. Pretendemos aqui dar as definições e resultados básicos que norteiam o assunto $*$-identidades polinomiais. Sugerimos as referências [5, 9, 13, 17, 20, 28] para um melhor entendimento do assunto.

Sejam $X = \{x_1, x_2, \ldots\}$ e $X^* = \{x_1^*, x_2^*, \ldots\}$ dois conjuntos infinitos enumeráveis e disjuntos. Denote por $F\langle X \cup X^* \rangle$ a álgebra associativa livre com unidade, livremente gerada por $X \cup X^*$. Definiremos uma involução $\star$ sobre $F\langle X \cup X^* \rangle$ da seguinte forma:

a) Nas letras (variáveis) a involução é definida por

$$x_i^\star = x_i^* \text{ e } (x_i^*)^\star = x_i.$$

b) Nas palavras a involução é definida por

$$(w_1 w_2 \dots w_n)^\star = (w_n)^\star \dots (w_2)^\star (w_1)^\star,$$

onde $w_1, w_2, \dots, w_n \in X \cup X^*$.

c) Se Pal é o conjunto das palavras de $F\langle X \cup X^* \rangle$, definimos

$$\left(\sum_{w \in Pal} \alpha_w w\right)^\star = \sum_{w \in Pal} \alpha_w w^\star.$$

Por comodidade, denotamos $\star = *$. Assim, por exemplo,

$$(x_1 x_2 x_3^* + 2x_1^* x_4)^* = x_3 x_2^* x_1^* + 2x_4^* x_1.$$

Definição 2.4.1. *Seja $(A, \circledast)$ uma álgebra com involução. Um polinômio $f \in F\langle X \cup X^* \rangle$ é chamado $*$-identidade polinomial (ou identidade polinomial com involução) para $(A, \circledast)$ se f está no núcleo de todo homomorfismo com involução $\varphi : F\langle X \cup X^* \rangle \to A$. Denotamos por*

$$Id(A, \circledast)$$

o conjunto de todas $*$-identidades polinomiais de $(A, \circledast)$.

Por comodidade escreveremos muitas vezes "$*$-identidade" ao invés de "$*$-identidade polinomial". A definição clássica de $*$-identidade (equivalente a acima) faremos em breve, após alguns comentários. Seja $(A, \circledast)$ uma álgebra com involução. O primeiro comentário consiste em que se $\varphi : F\langle X \cup X^* \rangle \to A$ é um homomorfismo de álgebras com involução e se $f(x_1, x_1^*, \dots, x_n, x_n^*) \in F\langle X \cup X^* \rangle$, então

$$\varphi\left(f(x_1, x_1^*, \dots, x_n, x_n^*)\right) = f(\varphi(x_1), \varphi(x_1)^\circledast, \dots, \varphi(x_n), \varphi(x_n)^\circledast).$$

O segundo comentário consiste em que se $a_1, a_2, \dots$ é uma lista de elementos em A, então existe um único homomorfismo de álgebras com involução $\varphi : F\langle X \cup X^* \rangle \to A$ tal que

$$\varphi(x_i) = a_i,$$

para todo $i \geq 1$. Com base nisso, uma maneira equivalente de definir $*$-identidade é a seguinte:

Lema 2.4.2. *Um polinômio $f(x_1, x_1^*, \dots, x_n, x_n^*) \in F\langle X \cup X^* \rangle$ é uma $*$-identidade polinomial para uma álgebra com involução $(A, \circledast)$ se, e somente se,*

$$f(a_1, a_1^\circledast, \dots, a_n, a_n^\circledast) = 0$$

para todos $a_1, \dots, a_n \in A$.

Por comodidade, e quando não houver confusão de notação, denotaremos uma involução qualquer sobre uma álgebra A por $*$. Neste caso, os homomorfismos de álgebras com involução serão chamados de *$*$-homomorfismos*, e os ideais de $(A, *)$ serão chamados de *$*$-ideais*. Relembramos que um $*$-ideal de A é um ideal I da álgebra A tal que

$$a^* \in I$$

para todo $a \in I$.

No estudo das $*$-identidades é mais conveniente considerar a álgebra associativa livre com unidade, livremente gerada por $Y \cup Z$, onde

$$Y = \{y_1, y_2, \ldots\}, \ Z = \{z_1, z_2, \ldots\}, \ y_i = x_i + x_i^* \ \text{ e } \ z_i = x_i - x_i^*$$

para todo $i \geq 1$. Note que $F\langle X \cup X^* \rangle = F\langle Y \cup Z \rangle$, y_i é simétrico e z_i é antissimétrico. Veremos quando um polinômio $f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in F\langle Y \cup Z \rangle$ é uma $*$-identidade para uma álgebra com involução $(A, *)$. Para isso, observe dois fatos:

Fato 1. Se φ é um $*$-homomorfismo, então φ leva elemento simétrico em simétrico, e leva elemento antissimétrico em antissimétrico.

Fato 2. Se $a_1, a_2, \ldots$ são elementos simétricos de A, e $b_1, b_2, \ldots$ são elementos antissimétricos de A, então existe um único $*$-homomorfismo $\varphi : F\langle Y \cup Z \rangle \to A$ tal que

$$\varphi(y_i) = a_i \ \text{ e } \ \varphi(z_i) = b_i$$

para todo $i \geq 1$. Ele é dado por

$$\varphi(f(y_1, \ldots, y_n, z_1, \ldots, z_m)) = f(a_1, \ldots, a_n, b_1, \ldots, b_m).$$

Com base nos dois fatos acima e na Definição 2.4.1, temos o seguinte lema:

Lema 2.4.3. *Um polinômio $f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in F\langle Y \cup Z \rangle$ é uma $*$-identidade para uma álgebra com involução $(A, *)$ se, e somente se,*

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

para todos $a_1, \ldots, a_n \in A^+$ e $b_1, \ldots, b_m \in A^-$.

O próximo lema será útil para achar algumas $*$-identidades conhecendo algumas identidades (ordinárias).

Lema 2.4.4. *Seja $f(x_1, \ldots, x_n) \in F\langle X \rangle$ e seja $(A, *)$ uma álgebra com involução. Se $f(x_1, \ldots, x_n) \in Id(A)$, então*

$$f(w_1, \ldots, w_n) \in Id(A, *)$$

para todos $w_1, \ldots, w_n \in Y \cup Z$.

Por exemplo, em (2.1) vimos que o polinômio $[x_1, x_2][x_3, x_4]$ é uma identidade (ordinária) para $UT_2(F)$. Logo, os seguintes polinômios

$$\begin{gathered}
[y_1, y_2][y_3, y_4], \ [y_1, y_2][y_3, z_1], \ [y_1, y_2][z_1, z_2], \\
[z_1, z_2][z_3, z_4], \ [z_1, z_2][y_1, z_3], \ [z_1, z_2][y_1, y_2], \\
[y_1, z_1][y_2, z_2], \ [y_1, z_1][y_2, y_3], \ [y_1, z_1][z_2, z_3],
\end{gathered}$$

são $*$-identidades para $(UT_2(F), *)$ para qualquer involução $*$ de $UT_2(F)$.

O conjunto $Id(A, *)$ das $*$-identidades de A tem uma propriedade similar ao caso ordinário. Para descrevê-la, definiremos o conceito de $T(*)$-ideal.

Definição 2.4.5. *Um $T(*)$-ideal de $F\langle Y \cup Z\rangle$ é um $*$-ideal de $F\langle Y \cup Z\rangle$ fechado por $*$-endomorfismos de $F\langle Y \cup Z\rangle$.*

A definição acima está dizendo que um $*$-ideal I é um $T(*)$-ideal se

$$\varphi(I) \subseteq I$$

para todo $*$-homomorfismo $\varphi : F\langle Y \cup Z\rangle \to F\langle Y \cup Z\rangle$.

Olhando para a Definição 2.4.1 é fácil ver que $Id(A, *)$ é um $T(*)$-ideal. Reciprocamente, se I é um $T(*)$-ideal, então $I = Id(A, *)$ para alguma álgebra com involução $(A, *)$. De fato, basta considerar

$$A = \frac{F\langle Y \cup Z\rangle}{I}$$

com involução

$$(f + I)^* = f^* + I$$

para todo $f \in F\langle Y \cup Z\rangle$.

Pelos Fatos 1 e 2 da página anterior, note que um $*$-ideal I de $F\langle Y \cup Z\rangle$ é um $T(*)$-ideal se, e somente se,

$$f(g_1, \ldots, g_n, h_1, \ldots, h_m) \in I$$

para todo $f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in I$, $g_1, \ldots, g_n \in F\langle Y \cup Z\rangle^+$ e $h_1, \ldots, h_m \in F\langle Y \cup Z\rangle^-$.

Definição 2.4.6. *Seja S um subconjunto de $F\langle Y \cup Z\rangle$. Definimos o $T(*)$-*ideal gerado por *S como sendo a interseção de todos os $T(*)$-ideais que contêm S. Denotamos ele por*

$$\langle S\rangle^{T(*)}.$$

Com base no parágrafo anterior a Definição 2.4.6, temos o seguinte resultado:

Lema 2.4.7. *Se S é um subconjunto de $F\langle Y \cup Z\rangle$, então $\langle S\rangle^{T(*)}$ é gerado, como espaço vetorial, pelos elementos*

$$gf(g_1, \ldots, g_n, h_1, \ldots, h_m)g'$$

onde $f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in S \cup S^*$, $g_1, \ldots, g_n \in F\langle Y \cup Z\rangle^+$, $h_1, \ldots, h_m \in F\langle Y \cup Z\rangle^-$ e $g, g' \in F\langle Y \cup Z\rangle$. Aqui S^* denota o conjunto

$$S^* = \{f^* \mid f \in S\}.$$

Dada uma álgebra com involução $(A, *)$, um dos problemas da área de PI-álgebra consiste em descrever as suas $*$-identidades. Mais especificamente, procura-se obter um conjunto gerador de $Id(A, *)$ como $T(*)$-ideal. Para isso, precisamos de um novo conceito:

Definição 2.4.8. *Um polinômio $f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in F\langle Y \cup Z\rangle$ é chamado Y-próprio se f é combinação linear de polinômios do tipo*

$$z_1^{r_1} \cdots z_m^{r_m} f_1 \cdots f_t$$

onde $t \geq 0$, $r_1, \ldots, r_m \geq 0$ e $f_1, \ldots, f_t \in F\langle Y \cup Z\rangle$ são comutadores de comprimento ≥ 2. Denotamos por B o conjunto de todos os polinômios Y-próprios.

Na definição acima, se $t = 0$, então convencionamos $f_1 \cdots f_t = 1$.

Usando o mesmo argumento em [10, Proposição 4.3.3], temos pelo Teorema de Poincaré-Birkhoff-Witt que todo elemento $g(y_1, \ldots, y_n, z_1, \ldots, z_m) \in F\langle Y \cup Z\rangle$ é combinação linear de polinômios do tipo

$$y_1^{s_1} \cdots y_n^{s_n} g_{(s_1,\ldots,s_n)} \tag{2.6}$$

onde $s_1, \ldots, s_n \geq 0$ e $g_{(s_1,\ldots,s_n)} \in B$. O leitor também pode consultar [11, Seção 2] para a verificação do fato.

Proposição 2.4.9. *Seja $f \in F\langle Y \cup Z\rangle$ e $w \in Y \cup Z$. Escreva*

$$f = \sum_{i=0}^{d_w} f^{(i)}$$

onde $f^{(i)}$ é a componente homogênea de f referente a variável w com grau $\deg_w f^{(i)} = i$. Se $d_w < |F|$ então

$$\langle f\rangle^{T(*)} = \langle f^{(0)}, f^{(1)}, \dots, f^{(d_w)}\rangle^{T(*)}.$$

Demonstração. Argumentos similares a demonstração de [10, Proposição 4.2.3]. □

Proposição 2.4.10. *Seja I um $T(*)$-ideal de $F\langle Y \cup Z\rangle$.*

a) Se F é um corpo infinito, então I é gerado, como $T(*)$-ideal, por seus elementos multi-homogêneos.

b) Se F é um corpo de car$(F) = 0$, então I é gerado, como um $T(*)$-ideal, por seus elementos multilineares.

Demonstração. Para a demonstração, usamos a Proposição 2.4.9 e argumentos similares a demonstração de [10, Proposição 4.2.3]. □

Proposição 2.4.11. *Seja I um $T(*)$-ideal de $F\langle Y \cup Z\rangle$.*

a) Se F é um corpo infinito, então I é gerado, como $T(*)$-ideal, por seus elementos Y-próprios multi-homogêneos.

b) Se F é um corpo de car$(F) = 0$, então I é gerado, como um $T(*)$-ideal, por seus elementos Y-próprios multilineares.

Demonstração. Veja [11, Lema 2.1]. Lá consta uma demonstração similar a [10, Proposição 4.3.3]. □

Proposição 2.4.12. *Seja F um corpo infinito e seja I um $T(*)$-ideal de $F\langle Y \cup Z\rangle$. Considere $W \subset B$ tal que*

$$\{w + (B \cap I) \ : \ w \in W\}$$

é uma base para o espaço vetorial quociente $B/(B \cap I)$. Então o conjunto de todos polinômios

$$y_1^{s_1} \cdots y_n^{s_n} w + I,$$

onde $s_1, \dots, s_n \geq 0$, $n \geq 1$ e $w \in W$, é uma base para o espaço vetorial quociente $F\langle Y \cup Z\rangle/I$.

Demonstração. Argumentos similares a demonstração de [10, Proposição 4.3.11]. □

Finalizamos a seção com o seguinte: como já foi comentado em (2.5), temos que

$$F\langle Y \cup Z\rangle = F\langle Y \cup Z\rangle^+ \oplus F\langle Y \cup Z\rangle^-.$$

Portanto:

Lema 2.4.13. *Seja* $f = f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in F\langle Y \cup Z\rangle$ *e escreva*

$$f = f^+ + f^-$$

onde $f^+ \in F\langle Y \cup Z\rangle^+$ *e* $f^- \in F\langle Y \cup Z\rangle^-$. *Considere uma álgebra com involução* $(A, *)$. *Se*

$$f(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) \in A^-$$

para todos $Y_1, \ldots, Y_n \in A^+$ *e* $Z_1, \ldots, Z_m \in A^-$, *então* $f^+ \in Id(A, *)$.

Demonstração. Sejam $Y_1, \ldots, Y_n \in A^+$ e $Z_1, \ldots, Z_m \in A^-$. Como $f^+ \in F\langle Y \cup Z\rangle^+$ temos que $f^+(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) \in A^+$. Mas

$$f(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) - f^-(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) = f^+(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m)$$

pertence a A^-. Logo, $f^+(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m)$ pertence a $A^+ \cap A^- = 0$, isto é,

$$f^+(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) = 0$$

como era o desejado. $\square$

Capítulo 3

$*$-identidades polinomiais para $UT_2(F)$

Ao longo deste capítulo, todas as involuções consideradas serão do primeiro tipo, e F será um corpo de $\mathrm{car}(F) \neq 2$.

Em [27] os matemáticos Di Vincenzo, Koshlukov e La Scala descreveram $Id(UT_2(F), *)$ quando F é infinito. Neste capítulo descreveremos $Id(UT_2(F), *)$ quando F é finito. Os resultados aqui obtidos estão publicados em [26] e fazem parte do trabalho realizado durante o doutorado.

3.1 $*$-identidades polinomiais para $(UT_2(F), \star)$

Seja F um corpo de $\mathrm{car}(F) \neq 2$. Nesta seção descreveremos $Id(UT_2(F), \star)$ quando F é finito. Relembramos a definição de $\star$ em (2.4):

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}^{\star} = \begin{pmatrix} b & c \\ 0 & a \end{pmatrix} \tag{3.1}$$

para todos $a, b, c \in F$. Consideraremos apenas esta involução. Assim, todos os resultados e discussões desta seção dizem respeito a essa involução $\star$. A outra involução de $UT_2(F)$ será analisada na próxima seção.

Denote por e_{ij} a matriz com entrada (i, j) igual a 1 e demais entradas igual a 0.

Lema 3.1.1. *Os conjuntos* $\{e_{11} + e_{22},\ e_{12}\}$ *e* $\{e_{11} - e_{22}\}$ *formam uma base para os espaços vetoriais* $UT_2(F)^+$ *e* $UT_2(F)^-$ *respectivamente.*

Demonstração. Note que $(e_{11} + e_{11}^{\star}) = (e_{11} + e_{22}) \in UT_2(F)^+$, $(e_{12} + e_{12}^{\star}) = 2e_{12} \in UT_2(F)^+$ e $(e_{11} - e_{11}^{\star}) = (e_{11} - e_{22}) \in UT_2(F)^-$. Como as 3 matrizes são linearmente independentes, segue que elas formam uma base para $UT_2(F)$. Assim, de

$$UT_2(F) = UT_2(F)^+ \oplus UT_2(F)^-$$

segue que $\{e_{11} + e_{22},\ e_{12}\}$ e $\{e_{11} - e_{22}\}$ formam uma base para $UT_2(F)^+$ e $UT_2(F)^-$ respectivamente. □

Lema 3.1.2. *Sejam y e z matrizes em $UT_2(F)$ simétrica e antissimétrica, respectivamente. Considere $a, b, c \in F$ tais que*

$$y = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \quad e \quad z = \begin{pmatrix} c & 0 \\ 0 & -c \end{pmatrix}. \tag{3.2}$$

Então

$$[z,y] = \begin{pmatrix} 0 & 2bc \\ 0 & 0 \end{pmatrix} \quad e \quad y^i = \begin{pmatrix} a^i & ia^{i-1}b \\ 0 & a^i \end{pmatrix},$$

para todo $i \geq 1$.

Demonstração. Temos

$$[z,y] = \begin{pmatrix} c & 0 \\ 0 & -c \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} - \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} c & 0 \\ 0 & -c \end{pmatrix} = \begin{pmatrix} 0 & 2bc \\ 0 & 0 \end{pmatrix}.$$

Para a outra igualdade, suponha que o resultado é verdadeiro para $i-1$. Logo,

$$y^i = y^{i-1}y = \begin{pmatrix} a^{i-1} & (i-1)a^{i-2}b \\ 0 & a^{i-1} \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a^i & ia^{i-1}b \\ 0 & a^i \end{pmatrix}.$$

Completamos a demonstração. □

Lema 3.1.3. *Seja F um corpo qualquer (finito ou infinito). Os polinômios*

$$[y_1,y_2], \quad [z_1,z_2], \quad [y_1,z_1][y_2,z_2], \quad z_1y_1z_2 - z_2y_1z_1 \tag{3.3}$$

pertencem a $Id(UT_2(F),\star)$.

Demonstração. A demonstração é consequência direta do Lema 2.4.3 e Lema 3.1.1. □

Definição 3.1.4. *Seja F um corpo qualquer (finito ou infinito). Denotaremos por I o $T(*)$-ideal gerado pelo conjunto (3.3).*

O seguinte teorema está provado em [27].

Teorema 3.1.5. *Seja F um corpo infinito. Considere a involução $\star$ definida em (3.1). Denote por I o $T(*)$-ideal gerado pelos polinômios*

$$[y_1,y_2], \quad [z_1,z_2], \quad [y_1,z_1][y_2,z_2] \quad e \quad z_1y_1z_2 - z_2y_1z_1.$$

Então $Id(UT_2(F),\star) = I$. Além disso, o espaço vetorial quociente $F\langle Y \cup Z\rangle/I$ tem uma base formada por todos polinômios da forma

$$y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m}[z_m,y_k] + I \quad e \quad y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m} + I \tag{3.4}$$

onde $n \geq 1,\ m \geq 1,\ s_1,\ldots,s_n,r_1,\ldots,r_m \geq 0,\ k \geq 1$.

Demonstração. A primeira parte do enunciado está provada em [27, Teorema 3.1], isto é, $Id(UT_2(F),\star) = I$. Para a segunda parte, está provado em [27, Teorema 3.1] que o espaço vetorial quociente $B/B\cap I$ tem uma base constituída pelos elementos da forma

$$z_1^{r_1}\cdots z_m^{r_m}[z_m,y_k] + B\cap I \quad \text{e} \quad z_1^{r_1}\cdots z_m^{r_m} + B\cap I \tag{3.5}$$

onde $m \geq 1$, $r_1,\ldots,r_m \geq 0$, $k \geq 1$. Pela Proposição 2.4.12 segue que o espaço vetorial quociente $F\langle Y \cup Z\rangle/I$ tem uma base formada por todos polinômios da forma (3.4). □

Lema 3.1.6. *Seja F um corpo qualquer (finito ou infinito). Os seguintes polinômios pertencem a I:*

$$f = z_1[z_2,y_1] - z_2[z_1,y_1], \qquad g = [z_1z_2,y_1] \qquad e \qquad h = [z_1,y_1]z_2 + z_2[z_1,y_1].$$

Demonstração. Para f temos a igualdade:

$$f = (z_1z_2y_1 - z_1y_1z_2) - (z_2z_1y_1 - z_2y_1z_1) = [z_1, z_2]y_1 - (z_1y_1z_2 - z_2y_1z_1).$$

Como $[z_1, z_2]$ e $(z_1y_1z_2 - z_2y_1z_1)$ pertencem a I, segue que $f \in I$.

Para g temos a igualdade:

$$2g = [2z_1z_2, y_1] = [2z_1z_2 + z_2z_1 - z_2z_1, y_1] = [z_1z_2 + z_2z_1, y_1] + [[z_1, z_2], y_1].$$

Como $[y_1, y_2] \in I$ e $(z_1z_2 + z_2z_1)$ é simétrico, segue do Lema 2.4.7 que $[z_1z_2 + z_2z_1, y_1] \in I$. Temos também que $[[z_1, z_2], y_1] \in I$, pois $[z_1, z_2] \in I$. Logo, $2g \in I$, isto é, $g \in I$.

Como $f, g \in I$ temos

$$h + I = [z_1, y_1]z_2 + z_1[z_2, y_1] + I = [z_1z_2, y_1] + I = I.$$

Logo, $h \in I$. □

Para o próximo resultado, denotaremos por S_m o grupo simétrico de grau m.

Lema 3.1.7. *Seja F um corpo qualquer (finito ou infinito). Para todo $\sigma \in S_{m+1}$ temos:*

$$\begin{aligned} &\text{i) } z_{\sigma(1)} \cdots z_{\sigma(m)}[z_{\sigma(m+1)}, y_1] + I = z_1 \cdots z_m[z_{m+1}, y_1] + I, \\ &\text{ii) } z_1 \cdots z_m[z_{m+1}, y_1] + I = (-1)^m[z_{m+1}, y_1]z_1 \cdots z_m + I. \end{aligned}$$

Demonstração. Para o item i) usamos que $[z_i, z_j] \in I$ (por definição) e $(z_i[z_j, y_1] - z_j[z_i, y_1]) \in I$ (por Lema 3.1.6). Assim,

$$z_iz_j + I = z_jz_i + I \quad \text{e} \quad z_i[z_j, y_1] + I = z_j[z_i, y_1] + I.$$

Combinando as duas igualdades temos a demonstração de i) concluída.

Para o item ii) usamos que $([z_{m+1}, y_1]z_j + z_j[z_{m+1}, y_1]) \in I$, veja Lema 3.1.6. Assim,

$$[z_{m+1}, y_1]z_j + I = -z_j[z_{m+1}, y_1] + I, \tag{3.6}$$

e aplicando m vezes esta igualdade provamos o item ii). □

Definição 3.1.8. *Se $f \in F\langle Y \cup Z\rangle^+$, dizemos que f tem sinal positivo. Se $f \in F\langle Y \cup Z\rangle^-$, dizemos que f tem sinal negativo.*

Lema 3.1.9. *Sejam $p_1, p_2 \in F\langle Y \cup Z\rangle$ e seja $u = [w_1, w_2, \ldots, w_n]$ um comutador de comprimento $n \geq 2$ tal que $w_1, w_2, \ldots, w_n \in Y \cup Z$.*

a) Se p_1, p_2 têm o mesmo sinal, então $[p_1, p_2]$ tem sinal negativo.

b) Se p_1, p_2 têm sinais opostos, então $[p_1, p_2]$ tem sinal positivo.

c) Se u tem sinal negativo, então $[w_1, w_2, \ldots, w_{n-1}]$ e w_n têm o mesmo sinal.

d) Se u tem sinal positivo, então $[w_1, w_2, \ldots, w_{n-1}]$ e w_n têm sinais opostos.

Demonstração. Como

$$[p_1, p_2]^* = (p_1p_2)^* - (p_2p_1)^* = p_2^*p_1^* - p_1^*p_2^* = [p_2^*, p_1^*] = -[p_1^*, p_2^*],$$

temos os itens a) e b) provados.

Por indução em n e pelos itens a) e b) segue que

$$[w_1, w_2, \ldots, w_{n-1}] \in F\langle Y \cup Z\rangle^+ \ \cup \ F\langle Y \cup Z\rangle^-.$$

Agora aplicamos a) e b) novamente para obter c) e d). □

A prova da seguinte proposição é similar a prova do [27, Theorem 3.1]. Uma pequena adaptação é necessária, pois agora o corpo F pode ser finito também.

Proposição 3.1.10. *Seja F um corpo qualquer (finito ou infinito). O espaço vetorial quociente $F\langle Y \cup Z\rangle/I$ é gerado pelos elementos*

$$y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m}[z_m, y_k] + I \quad e \quad y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m} + I \tag{3.7}$$

onde $n \geq 1,\ m \geq 1,\ s_1, \ldots, s_n, r_1, \ldots, r_m \geq 0,\ k \geq 1.$

Demonstração. Por (2.6), o espaço $F\langle Y \cup Z\rangle/I$ é gerado pelos elementos $f + I$ com

$$f = y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m} f_1 \cdots f_t$$

onde $n \geq 1,\ m \geq 1,\ s_1, \ldots, s_n, r_1, \ldots, r_m \geq 0,\ t \geq 0,$ e cada f_i é um comutador de comprimento ≥ 2 para todo i.

Se $t = 0$, então $f + I$ tem a forma dos elementos em (3.7).

Suponha $t \geq 2$. Pelo Lema 3.1.9 temos

$$f_1, f_2 \in F\langle Y \cup Z\rangle^+ \ \cup\ F\langle Y \cup Z\rangle^-.$$

Dois casos podem ocorrer:

a) f_1 ou f_2 é antissimétrico. Neste caso, pelo Lema 3.1.9 - c, temos que f_1 ou f_2 pertence a

$$\langle [y_1, y_2],\ [z_1, z_2]\rangle^{T(*)}.$$

Logo,

$$f \in \langle [y_1, y_2],\ [z_1, z_2]\rangle^{T(*)} \subseteq I.$$

b) f_1 e f_2 são simétricos. Neste caso, pelo Lema 3.1.9 - d, temos que

$$f_1 f_2 \in \langle [y_1, z_1][y_2, z_2]\rangle^{T(*)}.$$

Logo,

$$f \in \langle [y_1, z_1][y_2, z_2]\rangle^{T(*)} \subseteq I.$$

Acabamos de mostrar que se $t \geq 2$, então $f + I = I$.

Para finalizar, considere $t = 1$. Denote

$$f_1 = [w_1, \ldots, w_{l+1}],$$

onde $w_1, \ldots, w_{l+1} \in Y \cup Z$. Se $f_1 \in I$, então $f \in I$. Suponha $f_1 \notin I$. Pelo item a) acima temos que f_1 é simétrico. Afirmamos que f_1 é um comutador do tipo $[z_{i_1}, y_k, z_{i_2}, z_{i_3}, \ldots, z_{i_l}]$. Com efeito, claramente $w_1 \in Z$ e $w_2 \in Y$ (ou vice-versa). Logo, $[w_1, w_2] = [z_{i_1}, y_k]$ para alguns $i_1,\ k$. Suponha $[w_1, \ldots, w_t] = [z_{i_1}, y_k, z_{i_2}, z_{i_3}, \ldots, z_{i_{t-1}}]$. Então esse polinômio é simétrico (veja Lema 3.1.9). Logo, w_{t+1} necessariamente é z_{i_t} para algum i_t. Prosseguindo com este argumento teremos

$$f_1 = [z_{i_1}, y_k, z_{i_2}, z_{i_3}, \ldots, z_{i_l}].$$

Agora, podemos escrever f_1 como soma de polinômios $\pm u$ onde

$$u = z_{j_1}\cdots z_{j_t}[z_{i_1}, y_k] z_{j_{t+2}}\cdots z_{j_l}.$$

Pelo Lema 3.1.7,

$$u + I = \pm z_{j_1}\cdots z_{j_t} z_{j_{t+2}}\cdots z_{j_l}[z_{i_1}, y_k] + I.$$

Provamos que $f+I$ é combinação linear de polinômios

$$y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m} z_{j_1}\cdots z_{j_t} z_{j_{t+2}}\cdots z_{j_l}[z_{i_1}, y_k] + I. \tag{3.8}$$

Agora usamos o Lema 3.1.7 para reordenar as variáveis z_i em (3.8). Assim $f+I$ é do tipo (3.7), como queríamos provar. □

De agora até o fim desta seção, F denotará um corpo finito com q elementos. Denote por J o $T(*)$-ideal gerado pelos polinômios

$$[y_1, y_2], \quad [z_1, z_2], \quad [y_1, z_1][y_2, z_2], \quad z_1y_1z_2 - z_2y_1z_1, \tag{3.9}$$

$$(y_1^q - y_1)[z_1, y_2], \ \ (y_1^q - y_1)(y_2^q - y_2), \tag{3.10}$$

$$z_1^q - z_1, \quad (z_1^{q-1} - 1)[z_1, y_1], \quad (y_1^q - y_1)z_1 - 2^{-1}[z_1, y_1]. \tag{3.11}$$

Como I é gerado, como $T(*)$-ideal, pelos elementos em (3.9), temos que $I \subseteq J$.

Lema 3.1.11. *Seja F um corpo finito com q elementos. Então $J \subseteq Id(UT_2(F), \star)$.*

Demonstração. Pelo Lema 3.1.3, os polinômios em (3.9) pertencem a $Id(UT_2(F), \star)$. Pelo Teorema 2.1.2 segue que

$$[x_1, x_2], \ (x_1^q - x_1) \in Id(F).$$

Pelo parágrafo anterior a tal teorema, comentamos que

$$Id(UT_2(F)) = (Id(F))^2.$$

Logo,

$$(x_1^q - x_1)[x_2, x_3], \quad (x_1^q - x_1)(x_2^q - x_2) \in Id(UT_2(F)).$$

Como consequência do Lema 2.4.4 temos que os polinômios em (3.10) pertencem a $Id(UT_2(F), \star)$.

Agora analisaremos os polinômios em (3.11). Sejam $z \in UT_2(F)^-$ e $y \in UT_2(F)^+$. Temos

$$z = \begin{pmatrix} c & 0 \\ 0 & -c \end{pmatrix} \ \text{e} \ \ y = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

para alguns $a, b, c \in F$ (veja Lema 3.1.1). Claramente

$$z^i = \begin{pmatrix} c^i & 0 \\ 0 & (-c)^i \end{pmatrix}, \tag{3.12}$$

e como $c^q = c$, temos $z^q = z$. Provamos que $(z_1^q - z_1) \in Id(UT_2(F), \star)$.

Seja $1 = e_{11} + e_{22}$ a matriz identidade. Se $c = 0$ então $z = 0$ e $(z^{q-1} - 1)[z, y] = 0$. Se $c \neq 0$ então $c^{q-1} = 1$. Logo,

$$(z^{q-1} - 1)[z, y] = (1 - 1)[z, y] = 0.$$

Acabamos de mostrar que $(z_1^{q-1} - 1)[z_1, y_1] \in Id(UT_2(F), \star)$.

Pelo Lema 3.1.2 temos $y^q = a1$. Logo, a matriz $(y^q - y)z$ é igual a

$$\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} - \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right)\begin{pmatrix} c & 0 \\ 0 & -c \end{pmatrix} = \begin{pmatrix} 0 & -b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & 0 \\ 0 & -c \end{pmatrix} = \begin{pmatrix} 0 & bc \\ 0 & 0 \end{pmatrix} = 2^{-1}[z, y].$$

Para a última igualdade, veja Lema 3.1.2. Acabamos de mostrar que $(y_1^q - y_1)z_1 - 2^{-1}[z_1, y_1]$ está em $Id(UT_2(F), \star)$.

Pela definição de J concluímos que $J \subseteq Id(UT_2(F), \star)$. □

Do polinômio $(y_i^q - y_i)(y_j^q - y_j) \in J$ resulta as seguintes igualdades:

$$y_i^q y_j^q + J = y_i^q y_j + y_i y_j^q - y_i y_j + J, \tag{3.13}$$

$$y_i^{2q} + J = 2y_i^{q+1} - y_i^2 + J. \tag{3.14}$$

Como $[y_i, y_j]$ e $[z_i, z_j]$ pertencem a J, segue que variáveis com mesmo sinal comutam em $F\langle Y \cup Z\rangle/J$, isto é,

$$y_i y_j + J = y_j y_i + J, \tag{3.15}$$

$$z_i z_j + J = z_j z_i + J. \tag{3.16}$$

Definição 3.1.12. *Seja F um corpo finito com q elementos. Para cada $n \geq 1$ defina Λ_n como o conjunto dos elementos $(s_1, \dots, s_n) \in \mathbb{Z}^n$ tais que:*

a) $0 \leq s_1, \dots, s_n < 2q$,

b) Se $s_i \geq q$ para algum i, então $s_j < q$ para todo $j \neq i$.

Proposição 3.1.13. *Seja F um corpo finito com q elementos. O espaço vetorial quociente $F\langle Y \cup Z\rangle/J$ é gerado pelos polinômios*

$$\begin{cases} y_1^{s_1} \cdots y_n^{s_n} + J, & (s_1, \dots, s_n) \in \Lambda_n, \quad n \geq 1; \qquad : \Upsilon_1 \\ y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m} + J, & 0 \leq s_1, \dots, s_n, r_1, \dots, r_m < q, \quad r_m \geq 1, \\ & n \geq 1, \ m \geq 1; \qquad : \Upsilon_2 \\ y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m - 1}[z_m, y_k] + J, & 0 \leq s_1, \dots, s_n, r_1, \dots, r_m < q, \quad r_m \geq 1, \\ & n \geq 1, \ m \geq 1, \ k \geq 1. \qquad : \Upsilon_3 \end{cases}$$

Demonstração. Considere os conjuntos Ψ_1, Ψ_2, Ψ_3 definidos pelos elementos descritos abaixo:

$$\begin{cases} y_1^{s_1} \cdots y_n^{s_n} + J, & s_1, \dots, s_n \geq 0, \quad n \geq 1. \qquad : \Psi_1 \\ y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m} + J, & s_1, \dots, s_n, r_1, \dots, r_m \geq 0, \quad n \geq 1, \ m \geq 1, \\ & r_m \geq 1. \qquad : \Psi_2 \\ y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m}[z_m, y_k] + J, & s_1, \dots, s_n, r_1, \dots, r_m \geq 0, \quad n \geq 1, \ m \geq 1, \\ & k \geq 1. \qquad : \Psi_3 \end{cases}$$

Denote por (Ψ_i) e (Υ_i) os subespaços de $F\langle Y \cup Z\rangle/J$ gerados pelos conjuntos Ψ_i e Υ_i respectivamente. Então $(\Upsilon_i) \subseteq (\Psi_i)$ e, em particular,

$$(\Upsilon_1) + (\Upsilon_2) + (\Upsilon_3) \subseteq (\Psi_1) + (\Psi_2) + (\Psi_3). \tag{3.17}$$

Como $I \subseteq J$, temos pela Proposição 3.1.10 que $F\langle Y \cup Z\rangle/J = (\Psi_1) + (\Psi_2) + (\Psi_3)$. Assim, para provar esta proposição, devemos mostrar que vale a igualdade em (3.17).

Afirmação 1: $(\Psi_1) \subseteq (\Upsilon_1)$.
Seja $f = y_1^{s_1} \cdots y_n^{s_n}$ com $s_1, \dots, s_n \geq 0$. Mostraremos que $(f + J) \in (\Upsilon_1)$. Suponha que $s_i \geq 2q$ para algum i. Aplicando algumas vezes a igualdade (3.14) obtemos

$$y_i^{s_i} + J = \sum_{k=1}^{2q-1} \alpha_k y_i^k + J, \tag{3.18}$$

para alguns $\alpha_k \in F$. Assim $f + J$ é combinação linear de elementos do tipo $y_1^{s_1'} \cdots y_n^{s_n'} + J$ onde $0 \leq s_1', \dots, s_n' < 2q$. Portanto podemos supor, sem perda de generalidade,

$$0 \leq s_1, \dots, s_n < 2q$$

em f. Se $s_i, s_j \geq q$ para alguns i, j, então por (3.15) obtemos

$$f + J = y_1^{s_1} \cdots y_i^{s_i} \cdots y_j^{s_j} \cdots y_n^{s_n} + J = y_i^q y_j^q y_1^{s_1} \cdots y_i^{s_i - q} \cdots y_j^{s_j - q} \cdots y_n^{s_n} + J.$$

Por (3.13),

$$y_i^q y_j^q + J = y_i^q y_j + y_i y_j^q - y_i y_j + J.$$

Logo, $f + J = g_1 + g_2 - g_3 + J$, onde

$$\begin{aligned} g_1 &= y_i^q y_j y_1^{s_1} \cdots y_i^{s_i - q} \cdots y_j^{s_j - q} \cdots y_n^{s_n}, \\ g_2 &= y_i y_j^q y_1^{s_1} \cdots y_i^{s_i - q} \cdots y_j^{s_j - q} \cdots y_n^{s_n}, \\ g_3 &= y_i y_j y_1^{s_1} \cdots y_i^{s_i - q} \cdots y_j^{s_j - q} \cdots y_n^{s_n}. \end{aligned}$$

Como as variáveis y comutam no quociente $F\langle Y \cup Z\rangle / J$ (veja novamente (3.15)), podemos ordenar as variáveis em g_1, g_2, g_3 e obter $f + J = f_1 + f_2 - f_3 + J$ onde

$$\begin{aligned} f_1 &= y_1^{s_1} \cdots y_i^{s_i} \cdots y_j^{s_j - q + 1} \cdots y_n^{s_n}, \\ f_2 &= y_1^{s_1} \cdots y_i^{s_i - q + 1} \cdots y_j^{s_j} \cdots y_n^{s_n}, \\ f_3 &= y_1^{s_1} \cdots y_i^{s_i - q + 1} \cdots y_j^{s_j - q + 1} \cdots y_n^{s_n}. \end{aligned}$$

Observe o que acontece com os graus das variáveis $y_1, \ldots, y_n$ em f, f_1, f_2, f_3. Usando em f_1, f_2, f_3 os mesmos argumentos como em f, após alguns passos, teremos $(f + J) \in (\Upsilon_1)$. Provamos que $(\Psi_1) \subseteq (\Upsilon_1)$.

Afirmação 2: $(\Psi_2) \subseteq (\Upsilon_2) + (\Psi_3)$.
Seja $f = y_1^{s_1} \cdots y_n^{s_n} z_1^{t_1} \cdots z_m^{t_m}$, onde $s_1, \ldots, s_n, t_1, \ldots, t_m \geq 0$, $t_m \geq 1$, $m \geq 1$. Mostraremos que $(f + J) \in (\Upsilon_2) + (\Psi_3)$.

Por (3.11) temos $z_i^q + J = z_i + J$. Então existem inteiros $r_1, \ldots, r_m$ tais que $0 \leq r_i < q$, $r_m \geq 1$ e

$$f + J = y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m} + J.$$

Pela Afirmação 1 podemos supor, sem perda de generalidade, que $(s_1, \ldots, s_n) \in \Lambda_n$.

Se cada $s_i < q$ temos que $f + J \in (\Upsilon_2)$. Suponha $s_i \geq q$ para algum i. Então $s_j < q$ para $j \neq i$ e $s_i \leq 2q - 1$. Por (3.11) temos

$$y_i^q z_m + J = y_i z_m + 2^{-1}[z_m, y_i] + J.$$

Logo

$$y_i^{s_i} z_m + J = y_i^{s_i - q + 1} z_m + 2^{-1} y_i^{s_i - q}[z_m, y_i] + J.$$

Então, por (3.15) e (3.16) temos que $f + J = f_1 + 2^{-1} f_2 + J$, onde

$$\begin{aligned} f_1 =& y_1^{s_1} \cdots y_i^{s_i - q + 1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m}, \\ f_2 =& y_1^{s_1} \cdots y_i^{s_i - q} \cdots y_n^{s_n} [z_m, y_i] z_1^{r_1} \cdots z_m^{r_m - 1}. \end{aligned}$$

Pelo Lema 3.1.7 temos que

$$f_2 + J = \pm y_1^{s_1} \cdots y_i^{s_i - q} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m - 1} [z_m, y_i] + J \in (\Psi_3).$$

Caso a) Se $s_i < 2q - 1$ temos que $s_i - q + 1 < q$. Logo, $f_1 + J \in \Upsilon_2$.

Caso b) Se $s_i = 2q-1$, então $f_1 = y_1^{s_1}\cdots y_i^{q}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m}$. Com raciocínio análogo ao acima, segue que

$$f_1 + J = g_1 + 2^{-1}g_2 + J,$$

onde

$$\begin{aligned} g_1 + J =& y_1^{s_1}\cdots y_i\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m} + J \in \Upsilon_2,\\ g_2 + J =& y_1^{s_1}\cdots \widehat{y_i}\cdots y_n^{s_n}[z_m, y_i]z_1^{r_1}\cdots z_m^{r_m-1} + J\\ =& \pm\, y_1^{s_1}\cdots \widehat{y_i}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m-1}[z_m, y_i] + J \in (\Psi_3). \end{aligned}$$

A demonstração da afirmação está completa.

Afirmação 3: $(\Psi_3) \subseteq (\Upsilon_3)$.
Seja $f = y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m}[z_m, y_k]$. Pelo Lema 3.1.7 temos que

$$f + J = \pm y_1^{s_1}\cdots y_n^{s_n}[z_m, y_k]z_1^{r_1}\cdots z_m^{r_m} + J.$$

Por (3.10) temos que

$$y_i^{q}[z_m, y_k] + J = y_i[z_m, y_k] + J.$$

Por este fato, (3.15) e Lema 3.1.7 temos que

$$f + J = \pm y_1^{s_1'}\cdots y_n^{s_n'}[z_m, y_k]z_1^{r_1}\cdots z_m^{r_m} + J = y_1^{s_1'}\cdots y_n^{s_n'}z_1^{r_1}\cdots z_m^{r_m}[z_m, y_k] + J$$

com $0 \le s_1', \dots, s_n' < q$. Usando a igualdade $z_i^q + J = z_i + J$ temos que

$$f + J = y_1^{s_1'}\cdots y_n^{s_n'}z_1^{r_1'}\cdots z_m^{r_m'}[z_m, y_k] + J$$

onde $0 \le r_1', \dots, r_m' < q$. Se $r_m' < q-1$, então $f + J \in (\Upsilon_3)$. Se $r_m = q-1$, usamos (3.11):

$$z_m^{q-1}[z_m, y_k] + J = [z_m, y_k] + J.$$

Logo

$$f + J = y_1^{s_1'}\cdots y_n^{s_n'}z_1^{r_1'}\cdots z_{m-1}^{r_{m-1}'}[z_m, y_k] + J \in (\Upsilon_3).$$

Finalizamos a demonstração da Afirmação 3.

Pelas Afirmações $1, 2$ e 3 temos que o "contido" de (3.17) é uma "igualdade". $\square$

Lema 3.1.14. *Seja F um corpo finito com q elementos. Denote $\widetilde{J} = Id(UT_2(F), \star)$. O conjunto dos polinômios*

$$y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m-1}[z_m, y_k] + \widetilde{J}, \quad \begin{array}{l} 0 \le s_1, \dots, s_n, r_1, \dots, r_m < q,\\ r_m \ge 1,\ n \ge 1,\ m \ge 1,\ k \ge 1, \end{array}$$

é linearmente independente em $F\langle Y \cup Z\rangle/\widetilde{J}$.

Demonstração. Seja

$$f = \sum_{n,m,k,s,r} \alpha_{(n,m,k,s,r)} y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m-1}[z_m, y_k], \quad \left\{ \begin{array}{c} s = (s_1, \dots, s_n),\\ r = (r_1, \dots, r_m),\\ \alpha_{(n,m,k,s,r)} \in F, \end{array} \right.$$

onde (n, m, k, s, r) satisfaz as condições do enunciado.

Escolha matrizes arbitrárias

$$Y_i = \begin{pmatrix} a_i & b_i \\ 0 & a_i \end{pmatrix} \quad \text{e} \quad Z_i = \begin{pmatrix} c_i & 0 \\ 0 & -c_i \end{pmatrix}$$

onde $a_i, b_i, c_i \in F$. Temos que

$$Y_1^{s_1} \cdots Y_n^{s_n} Z_1^{r_1} \cdots Z_m^{r_m - 1} = \begin{pmatrix} \delta & * \\ 0 & * \end{pmatrix} \quad \text{onde} \quad \delta = a_1^{s_1} \cdots a_n^{s_n} c_1^{r_1} \cdots c_m^{r_m - 1}.$$

Pelo Lema 3.1.2 temos que

$$Y_1^{s_1} \cdots Y_n^{s_n} Z_1^{r_1} \cdots Z_m^{r_m-1}[Z_m, Y_k] = \begin{pmatrix} \delta & * \\ 0 & * \end{pmatrix} \begin{pmatrix} 0 & 2b_k c_m \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2\delta b_k c_m \\ 0 & 0 \end{pmatrix}.$$

Uma vez que $2\delta b_k c_m = 2a_1^{s_1} \cdots a_n^{s_n} c_1^{r_1} \cdots c_m^{r_m} b_k$, segue que

$$f(Y_1, Y_2, \ldots, Z_1, Z_2, \ldots) = \begin{pmatrix} 0 & \theta \\ 0 & 0 \end{pmatrix}, \quad \text{onde} \quad \theta = \sum_{n,m,k,s,r} 2\alpha_{(n,m,k,s,r)} a_1^{s_1} \cdots a_n^{s_n} c_1^{r_1} \cdots c_m^{r_m} b_k.$$

Suponha que $f \in \widetilde{J}$. Então $\theta = 0$ para todos

$$a_1, a_2, \ldots, b_1, b_2, \ldots, c_1, c_2, \ldots \in F.$$

Como $\deg_{a_i} \theta$, $\deg_{b_i} \theta$, $\deg_{c_i} \theta < q$ para todo i, temos pelo Lema 2.1.3 que $\alpha_{(n,m,k,s,r)} = 0$ para todos n, m, k, s, r. $\square$

Lema 3.1.15. *Seja F um corpo finito com q elementos. Denote $\widetilde{J} = Id(UT_2(F), \star)$. O conjunto de todos os polinômios*

$$\begin{cases} y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m-1}[z_m, y_k] + \widetilde{J}, & 0 \leq s_1, \ldots, s_n, r_1, \ldots, r_m < q, \quad r_m \geq 1, \quad (a) \\ & n \geq 1, \ m \geq 1, \ k \geq 1; \\ y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m} + \widetilde{J}, & 0 \leq s_1, \ldots, s_n, r_1, \ldots, r_m < q, \quad r_m \geq 1, \quad (b) \\ & n \geq 1, \ m \geq 1, \end{cases}$$

é linearmente independente em $F\langle Y \cup Z \rangle / \widetilde{J}$.

Demonstração. Seja

$$f_1 = \sum_{n,m,k,s,r} \alpha_{(n,m,k,s,r)} y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m-1}[z_m, y_k], \quad \begin{cases} s = (s_1, \ldots, s_n), \\ r = (r_1, \ldots, r_m), \\ \alpha_{(n,m,k,s,r)} \in F, \end{cases}$$

com (n, m, k, s, r) satisfazendo (a). E seja

$$f_2 = \sum_{n,m,s,r} \beta_{(n,m,s,r)} y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m}, \quad \begin{cases} s = (s_1, \ldots, s_n), \\ r = (r_1, \ldots, r_m), \\ \beta_{(n,m,s,r)} \in F, \end{cases}$$

com (n, m, s, r) satisfazendo (b).

Suponhamos que $f + \widetilde{J} = \widetilde{J}$ onde $f = f_1 + f_2$. Devemos mostrar que $\alpha_{(n,m,k,s,r)} = \beta_{(n,m,s,r)} = 0$ para todo (n, m, k, s, r), (n, m, s, r). Sejam

$$Y_i = \begin{pmatrix} a_i & b_i \\ 0 & a_i \end{pmatrix} \quad \text{e} \quad Z_i = \begin{pmatrix} c_i & 0 \\ 0 & -c_i \end{pmatrix}$$

onde $a_i, b_i, c_i \in F$. Temos

$$f(Y_1, Y_2, \ldots, Z_1, Z_2, \ldots) = \begin{pmatrix} \rho & \theta \\ 0 & \lambda \end{pmatrix}$$

onde $\rho,\ \theta,\ \lambda \in F$. Observe que $f_1(Y_1, Y_2, \ldots, Z_1, Z_2, \ldots)$ é uma matriz triangular superior com a diagonal nula. Logo,

$$\rho = f_2(a_1, a_2, \ldots, c_1, c_2, \ldots).$$

Uma vez que $f \in \widetilde{J}$, obtemos $\rho = f_2(a_1, a_2, \ldots, c_1, c_2, \ldots) = 0$ para todo $a_1, a_2, \ldots, c_1, c_2, \ldots \in F$. Como $\deg_{y_i} f_2,\ \deg_{z_i} f_2 < q$ para todo i, temos pelo Lema 2.1.3 que $\beta_{(n,m,s,r)} = 0$ para todos n, m, s, r. Assim, $f = f_1$ e $f_1 + \widetilde{J} = \widetilde{J}$. Consequentemente, pelo Lema 3.1.14, obtemos $\alpha_{(n,m,k,s,r)} = 0$ para todos n, m, k, s, r. □

Lema 3.1.16. *Seja F um corpo finito com q elementos. Denote $\widetilde{J} = Id(UT_2(F), \star)$. O conjunto de todos os polinômios*

$$y_1^{s_1} \cdots y_n^{s_n} + \widetilde{J}, \quad (s_1, \ldots, s_n) \in \Lambda_n, \quad n \geq 1,$$

é linearmente independente em $F\langle Y \cup Z\rangle/\widetilde{J}$.

Demonstração. Demonstraremos por indução sobre n.

Para o caso $n = 1$, seja $f + \widetilde{J} = \widetilde{J}$ onde

$$f(y_1) = \sum_{s=0}^{2q-1} \alpha_s y_1^s, \quad \alpha_s \in F.$$

Tome a matriz $Y_1 = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$. Pelo Lema 3.1.2 temos $Y_1^j = \begin{pmatrix} a^j & ja^{j-1} \\ 0 & a^j \end{pmatrix}$. Assim

$$f(Y_1) = \begin{pmatrix} f(a) & f'(a) \\ 0 & f(a) \end{pmatrix}$$

onde f' é a derivada de f. Uma vez que $f \in \widetilde{J}$, temos $f(a) = f'(a) = 0$ para todo $a \in F$. Pelo Lema 2.1.4 segue que $\alpha_s = 0$ para todo s, como queríamos.

Suponha $n > 1$. Seja

$$f(y_1, \ldots, y_n) = \sum_{(s_1,\ldots,s_n)\in\Lambda_n} \alpha_{(s_1,\ldots,s_n)} y_1^{s_1} \cdots y_n^{s_n} \in \widetilde{J}. \tag{3.19}$$

O polinômio $f_0 = f(0, y_2, \ldots, y_n)$ está também em $\widetilde{J}$. Como f_0 tem $n - 1$ variáveis, por indução temos que $\alpha_{(0,s_2,\ldots,s_n)} = 0$ para todo $(0, s_2, \ldots, s_n) \in \Lambda_n$. Agora podemos supor que $s_1 \geq 1$ em (3.19). Podemos escrever f da seguinte forma

$$f = \sum_{i=1}^{2q-1} y_1^i f_i,$$

onde f_i está definido como abaixo:

a) Se $1 \leq i < q$ então

$$f_i = \sum_{(s_2,\ldots,s_n)\in\Lambda_{n-1}} \alpha_{(i,s_2,\ldots,s_n)} y_2^{s_2} \ldots y_n^{s_n}.$$

b) Se $q \leq i \leq 2q-1$ então

$$f_i = \sum_{s_2,\ldots,s_n=0}^{q-1} \alpha_{(i,s_2,\ldots,s_n)} y_2^{s_2} \ldots y_n^{s_n}.$$

Considere as seguintes matrizes:

$$Y_1 = \begin{pmatrix} a_1 & 1 \\ 0 & a_1 \end{pmatrix} \text{ e } Y_i = \begin{pmatrix} a_i & 0 \\ 0 & a_i \end{pmatrix} \quad (i \neq 1)$$

onde $a_j \in F$ para todo j. Então

$$\begin{aligned} f(Y_1,\ldots,Y_n) &= \sum_{i=1}^{2q-1} \begin{pmatrix} a_1^i & ia_1^{i-1} \\ 0 & a_1^i \end{pmatrix} f_i(Y_2,\ldots,Y_n) \\ &= \sum_{i=1}^{2q-1} \begin{pmatrix} a_1^i & ia_1^{i-1} \\ 0 & a_1^i \end{pmatrix} \begin{pmatrix} f_i(a_2,\ldots,a_n) & 0 \\ 0 & f_i(a_2,\ldots,a_n) \end{pmatrix} \\ &= \begin{pmatrix} \displaystyle\sum_{i=1}^{2q-1} a_1^i f_i(a_2,\ldots,a_n) & \displaystyle\sum_{i=1} ia_1^{i-1} f_i(a_2,\ldots,a_n) \\ 0 & \displaystyle\sum_{i=1}^{2q-1} a_1^i f_i(a_2,\ldots,a_n) \end{pmatrix}. \end{aligned}$$

Fixando $a_2,\ldots,a_n \in F$, defina o polinômio

$$f_{(a_2,\ldots,a_n)}(y_1) = \sum_{i=1}^{2q-1} y_1^i f_i(a_2,\ldots,a_n).$$

Note que

$$f(Y_1,\ldots,Y_n) = \begin{pmatrix} f_{(a_2,\ldots,a_n)}(a_1) & f'_{(a_2,\ldots,a_n)}(a_1) \\ 0 & f_{(a_2,\ldots,a_n)}(a_1) \end{pmatrix},$$

onde $f'_{(a_2,\ldots,a_n)}$ é a derivada de $f_{(a_2,\ldots,a_n)}$. Como $f \in \widetilde{J}$, obtemos

$$f_{(a_2,\ldots,a_n)}(a_1) = f'_{(a_2,\ldots,a_n)}(a_1) = 0$$

para todo $a_1 \in F$. Pelo Lema 2.1.4 temos $f_i(a_2,\ldots,a_n) = 0$ para todo i. Uma vez que $a_2,\ldots,a_n \in F$ podem ser tomados arbitrários, segue que f_i é uma identidade polinomial para F. Temos dois casos a considerar:

Caso 1. $q \leq i \leq 2q-1$.
Do item b) acima, Lema 2.1.3 e do fato que f_i é uma identidade polinomial para F, temos $\alpha_{(i,s_2,\ldots,s_n)} = 0$ para todo $0 \leq s_2,\ldots,s_n \leq q-1$.

Caso 2. $1 \leq i < q$.
Pelo Caso 1 segue que

$$f = \sum_{i=1}^{q-1} y_1^i f_i \ .$$

Observe que $\deg_{y_1} f < q$. Logo, pela Proposição 2.4.9, temos $y_1^i f_i \in \widetilde{J}$ para todo $1 \leq i < q$. Como a matriz identidade é simétrica, segue que $f_i \in \widetilde{J}$ para todo $1 \leq i < q$. Uma vez que cada f_i tem $n-1$ variáveis, por indução temos $\alpha_{(i,s_2,\ldots,s_n)} = 0$ para todo $1 \leq i < q$ e $(s_2,\ldots,s_n) \in \Lambda_{n-1}$.

Finalizamos a demonstração. $\square$

Teorema 3.1.17. *Seja F um corpo finito com q elementos. Denote por J o $T(*)$-ideal gerado pelos polinômios*

$$\begin{gathered}[y_1,y_2],\quad [z_1,z_2],\quad [y_1,z_1][y_2,z_2],\quad z_1y_1z_2 - z_2y_1z_1,\\ (y_1^q - y_1)[z_1,y_2],\quad (y_1^q-y_1)(y_2^q-y_2),\quad z_1^q - z_1,\\ (z_1^{q-1}-1)[z_1,y_1],\quad (y_1^q-y_1)z_1 - 2^{-1}[z_1,y_1].\end{gathered}$$

Então $Id(UT_2(F),\star) = J$. Além disso, o espaço vetorial quociente $F\langle Y\cup Z\rangle/J$ tem uma base formada por todos polinômios da forma

$$\begin{cases} y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m-1}[z_m,y_k] + J, & 0\leq s_1,\ldots,s_n,r_1,\ldots,r_m < q,\quad r_m \geq 1,\\ & n\geq 1,\ m\geq 1,\ k\geq 1;\\ y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m} + J, & 0\leq s_1,\ldots,s_n,r_1,\ldots,r_m < q,\quad r_m \geq 1,\\ & n\geq 1,\ m\geq 1;\\ y_1^{s_1}\cdots y_n^{s_n} + J, & (s_1,\ldots,s_n)\in\Lambda_n,\quad n\geq 1.\end{cases}.$$

Demonstração. Denote $\widetilde{J} = Id(UT_2(F),\star)$. Seja U o subespaço de $F\langle Y\cup Z\rangle/\widetilde{J}$ gerado pelos elementos

$$\begin{cases} y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m-1}[z_m,y_k] + \widetilde{J}, & 0\leq s_1,\ldots,s_n,r_1,\ldots,r_m < q,\quad r_m \geq 1,\\ & n\geq 1,\ m\geq 1,\ k\geq 1;\\ y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m} + \widetilde{J}, & 0\leq s_1,\ldots,s_n,r_1,\ldots,r_m < q,\quad r_m \geq 1,\\ & n\geq 1,\ m\geq 1.\end{cases}$$

Seja V o subespaço de $F\langle Y\cup Z\rangle/\widetilde{J}$ gerado pelos elementos

$$y_1^{s_1}\cdots y_n^{s_n} + \widetilde{J},\quad (s_1,\ldots,s_n)\in\Lambda_n,\quad n\geq 1.$$

Afirmação 1: $F\langle Y\cup Z\rangle/\widetilde{J} = U\oplus V$.

Como $J\subseteq \widetilde{J}$ (veja Lema 3.1.11), temos pela Proposição 3.1.13 que $F\langle Y\cup Z\rangle/\widetilde{J} = U+V$.

Seja $f(y_1,\ldots,y_n,z_1,\ldots,z_m)\in F\langle Y\cup Z\rangle$ tal que $(f+\widetilde{J})\in U\cap V$. Como $f+\widetilde{J}\in U$, existe $g(y_1,\ldots,y_n,z_1,\ldots,z_m)$ que é combinação linear de

$$\begin{cases} y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m-1}[z_m,y_k], & 0\leq s_1,\ldots,s_n,r_1,\ldots,r_m < q,\quad r_m \geq 1,\\ & n\geq 1,\ m\geq 1,\ k\geq 1;\\ y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m}, & 0\leq s_1,\ldots,s_n,r_1,\ldots,r_m < q,\quad r_m \geq 1,\\ & n\geq 1,\ m\geq 1,\end{cases}$$

tal que

$$f+\widetilde{J} = g+\widetilde{J}.$$

Como $g(y_1,\ldots,y_n,0,\ldots,0) = 0$ temos $f(y_1,\ldots,y_n,0,\ldots,0)+\widetilde{J} = \widetilde{J}$. Por sua vez $f+\widetilde{J}\in V$ implica que existe um polinômio $h(y_1,\ldots,y_n)$ que é combinação linear de

$$y_1^{s_1}\cdots y_n^{s_n},\quad (s_1,\ldots,s_n)\in\Lambda_n,\quad n\geq 1,$$

tal que $f+\widetilde{J}=h+\widetilde{J}$. Assim,

$$f(y_1,\ldots,y_n,z_1,\ldots,z_m)+\widetilde{J}=h(y_1,\ldots,y_n)+\widetilde{J}=f(y_1,\ldots,y_n,0,\ldots,0)+\widetilde{J}=\widetilde{J}$$

como queríamos.

Afirmação 2: O espaço vetorial quociente $F\langle Y\cup Z\rangle/\widetilde{J}$ tem uma base formada pelos polinômios da forma

$$\begin{cases} y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m-1}[z_m,y_k]+\widetilde{J}, & 0\le s_1,\ldots,s_n,r_1,\ldots,r_m<q,\quad r_m\ge 1,\\ & n\ge 1,\ m\ge 1,\ k\ge 1;\\ y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m}+\widetilde{J}, & 0\le s_1,\ldots,s_n,r_1,\ldots,r_m<q,\quad r_m\ge 1,\\ & n\ge 1,\ m\ge 1;\\ y_1^{s_1}\cdots y_n^{s_n}+\widetilde{J}, & (s_1,\ldots,s_n)\in\Lambda_n,\quad n\ge 1.\end{cases}.$$

De fato, isso é consequência direta da Afirmação 1, Lema 3.1.15 e Lema 3.1.16.

Afirmação 3: $J=\widetilde{J}$.
Já sabemos que $J\subseteq\widetilde{J}$. Provaremos a outra inclusão: Pela Proposição 3.1.13 e a Afirmação 2, existe um subconjunto $\Omega\subset F\langle Y\cup Z\rangle$ tal que

i) $\Omega_J=\{\omega+J|\ \omega\in\Omega\}$ gera $F\langle Y\cup Z\rangle/J$;

ii) $\Omega_{\widetilde{J}}=\{\omega+\widetilde{J}|\ \omega\in\Omega\}$ é base para $F\langle Y\cup Z\rangle/\widetilde{J}$.

Seja $f\in\widetilde{J}$. Por i) temos que

$$f+J=\sum_{w\in\Omega}\alpha_\omega\omega+J,\ \alpha_\omega\in F.$$

Uma vez que $J\subseteq\widetilde{J}$ temos

$$f+\widetilde{J}=\sum_{w\in\Omega}\alpha_\omega\omega+\widetilde{J},\ \alpha_\omega\in F.$$

Como $f\in\widetilde{J}$, por ii) temos que $\alpha_\omega=0$ para todo $w\in\Omega$. Logo, $f+J=J$ e consequentemente $f\in J$. □

3.2 $*$-identidades polinomiais para $(UT_2(F),s)$

Seja F um corpo de car$(F)\neq 2$. Nesta seção descreveremos $Id(UT_2(F),s)$ quando F é finito. Relembramos a definição de s em (2.4):

$$\begin{pmatrix} a & c\\ 0 & b\end{pmatrix}^s=\begin{pmatrix} b & -c\\ 0 & a\end{pmatrix} \tag{3.20}$$

para todos $a,b,c\in F$. Consideraremos apenas esta involução.

Lema 3.2.1. *Os conjuntos $\{e_{11}+e_{22}\}$ e $\{e_{12},e_{11}-e_{22}\}$ formam uma base para os espaços vetoriais $UT_2(F)^+$ e $UT_2(F)^-$ respectivamente.*

Demonstração. Note que $(e_{11}+e_{11}^s)=(e_{11}+e_{22})\in UT_2(F)^+$, $(e_{12}-e_{12}^s)=2e_{12}\in UT_2(F)^-$ e $(e_{11}-e_{11}^s)=(e_{11}-e_{22})\in UT_2(F)^-$. Como as 3 matrizes são linearmente independentes, segue que elas formam uma base para $UT_2(F)$. Assim, de

$$UT_2(F)=UT_2(F)^+\oplus UT_2(F)^-$$

segue que $\{e_{11}+e_{22}\}$ e $\{e_{12},e_{11}-e_{22}\}$ formam uma base para $UT_2(F)^+$ e $UT_2(F)^-$ respectivamente. □

Lema 3.2.2. *Seja z uma matriz antissimétrica em $UT_2(F)$. Considere $a, b \in F$ tais que*

$$z = \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix}.$$

Se i é par, então

$$z^i = \begin{pmatrix} a^i & 0 \\ 0 & a^i \end{pmatrix}. \tag{3.21}$$

Se i é ímpar, então

$$z^i = \begin{pmatrix} a^i & a^{i-1}b \\ 0 & -a^i \end{pmatrix}. \tag{3.22}$$

Demonstração. Temos

$$z^2 = \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix} \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix} = \begin{pmatrix} a^2 & 0 \\ 0 & a^2 \end{pmatrix}.$$

Logo,

$$z^i = \begin{pmatrix} a^i & 0 \\ 0 & a^i \end{pmatrix} \text{se } i \text{ é par.}$$

Se i é ímpar, então

$$z^i = z^{i-1}z \begin{pmatrix} a^{i-1} & 0 \\ 0 & a^{i-1} \end{pmatrix} \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix} = \begin{pmatrix} a^i & a^{i-1}b \\ 0 & -a^i \end{pmatrix}.$$

Finalizamos a demonstração. □

Lema 3.2.3. *Seja F um corpo qualquer (finito ou infinito). Os polinômios*

$$[y_1, y_2], \quad [z_1, y_1], \quad [z_1, z_2][z_3, z_4], \quad z_1z_2z_3 - z_3z_2z_1 \tag{3.23}$$

pertencem a $Id(UT_2(F), s)$.

Demonstração. A demonstração é consequência direta do Lema 2.4.3 e Lema 3.2.1. □

Denotaremos por I_s o $T(*)$-ideal gerado pelo conjunto (3.23).

O seguinte teorema está provado em [27].

Teorema 3.2.4. *Seja F um corpo infinito. Considere a involução s definida em (3.20). Denote por I_s o $T(*)$-ideal gerado pelos polinômios*

$$[y_1, y_2], \quad [z_1, y_1], \quad [z_1, z_2][z_3, z_4], \quad z_1z_2z_3 - z_3z_2z_1.$$

Então $Id(UT_2(F), s) = I_s$. Além disso, o espaço vetorial quociente $F\langle Y \cup Z\rangle/I_s$ tem uma base formada por todos polinômios da forma

$$y_1^{s_1} \cdots y_n^{s_n}[z_j, z_i]z_i^{r_i}z_{i+1}^{r_{i+1}} \cdots z_m^{r_m} + I_s \quad \text{e} \quad y_1^{s_1} \cdots y_n^{s_n}z_1^{r_1} \cdots z_m^{r_m} + I_s \tag{3.24}$$

onde $n \geq 1$, $m \geq 1$, $s_1, \ldots, s_n, r_1, \ldots, r_m \geq 0$, $j > i$.

Demonstração. A primeira parte do enunciado está provada em [27, Teorema 3.2], isto é, $Id(UT_2(F), \star) = I_s$. Para a segunda parte, está provado em [27, Teorema 3.2] que o espaço vetorial quociente $B/B \cap I_s$ tem uma base constituída pelos elementos da forma

$$[z_j, z_i]z_i^{r_i}z_{i+1}^{r_{i+1}} \cdots z_m^{r_m} + I_s \quad \text{e} \quad z_1^{r_1} \cdots z_m^{r_m} + I_s \tag{3.25}$$

onde $m \geq 1$, $r_1, \ldots, r_m \geq 0$, $j > i$. Pela Proposição 2.4.12 segue que o espaço vetorial quociente $F\langle Y \cup Z\rangle/I_s$ tem uma base formada por todos polinômios da forma (3.24). □

Lema 3.2.5. *Seja F um corpo qualquer (finito ou infinito). Os polinômios*

$$f = [z_3, z_2]z_1 - [z_3, z_1]z_2 + [z_2, z_1]z_3 \quad e \quad g = z_1[z_2, z_3] + [z_2, z_3]z_1$$

pertencem a I_s.

Demonstração. Note que

$$\begin{aligned} f &= z_3z_2z_1 - z_2z_3z_1 - z_3z_1z_2 + z_1z_3z_2 + z_2z_1z_3 - z_1z_2z_3 \\ &= (z_3z_2z_1 - z_1z_2z_3) + (z_1z_3z_2 - z_2z_3z_1) + (z_2z_1z_3 - z_3z_1z_2) \end{aligned}$$

é soma de 3 polinômios em I_s. Logo, $f \in I_s$.

Agora,

$$\begin{aligned} g &= z_1z_2z_3 - z_1z_3z_2 + z_2z_3z_1 - z_3z_2z_1 \\ &= (z_1z_2z_3 - z_3z_2z_1) + (z_2z_3z_1 - z_1z_3z_2) \end{aligned}$$

é soma de 2 polinômios em I_s. Logo, $g \in I_s$. □

Lema 3.2.6. *Seja F um corpo qualquer (finito ou infinito). Se $m \geq 1$, então*

$$z_1 \cdots z_m[z_{m+1}, z_{m+2}] + I_s = (-1)^m[z_{m+1}, z_{m+2}]z_1 \cdots z_m + I_s.$$

Demonstração. Pelo Lema 3.2.5 temos que $z_i[z_{m+1}, z_{m+2}] + I_s = -[z_{m+1}, z_{m+2}]z_i + I_s$. Assim,

$$\begin{aligned} z_1 \cdots z_m[z_{m+1}, z_{m+2}] + I_s &= -z_1 \cdots z_{m-1}[z_{m+1}, z_{m+2}]z_m + I_s \\ &= +z_1 \cdots z_{m-2}[z_{m+1}, z_{m+2}]z_{m-1}z_m + I_s \\ &\vdots \\ &= (-1)^m[z_{m+1}, z_{m+2}]z_1 \cdots z_m + I_s. \end{aligned}$$

Finalizamos a demonstração. □

Lema 3.2.7. *Seja F um corpo qualquer (finito ou infinito) e seja $m \geq 1$. Para todo $\sigma \in S_m$ temos que*

$$[z_{m+1}, z_{m+2}]z_{\sigma(1)} \cdots z_{\sigma(m)} + I_s \quad = \quad [z_{m+1}, z_{m+2}]z_1 \cdots z_m + I_s.$$

Demonstração. Uma vez que $[z_1, z_2][z_3, z_4] \in I_s$ temos

$$[z_{m+1}, z_{m+2}]z_iz_j + I_s = [z_{m+1}, z_{m+2}]z_jz_i + I_s.$$

Assim, pelo Lema 3.2.6,

$$\begin{aligned} [z_{m+1}, z_{m+2}]z_1 \cdots z_iz_{i+1} \cdots z_m + I_s &= (-1)^{i-1}z_1 \cdots [z_{m+1}, z_{m+2}]z_iz_{i+1} \cdots z_m + I_s \\ &= (-1)^{i-1}z_1 \cdots [z_{m+1}, z_{m+2}]z_{i+1}z_i \cdots z_m + I_s \\ &= [z_{m+1}, z_{m+2}]z_1 \cdots z_{i+1}z_i \cdots z_m + I_s \ . \end{aligned}$$

Finalizamos a demonstração. □

A prova da seguinte proposição é similar a prova do [27, Teorema 3.2]. Uma pequena adaptação é necessária, pois agora o corpo F pode ser finito também.

Proposição 3.2.8. *Seja F um corpo qualquer (finito ou infinito). O espaço vetorial quociente $F\langle Y \cup Z\rangle/I_s$ é gerado pelos elementos*

$$y_1^{s_1} \cdots y_n^{s_n}[z_j, z_i]z_i^{r_i} z_{i+1}^{r_{i+1}} \cdots z_m^{r_m} + I_s \quad e \quad y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m} + I_s \tag{3.26}$$

onde $n \geq 1$, $m \geq 1$, $s_1, \ldots, s_n, r_1, \ldots, r_m \geq 0$, $j > i$.

Demonstração. Por (2.6), o espaço vetorial $F\langle Y \cup Z\rangle/I_s$ é gerado pelos elementos $f + I_s$ com

$$f = y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m} f_1 \cdots f_t$$

onde $n \geq 1$, $m \geq 1$, $s_1, \ldots, s_n, r_1, \ldots, r_m \geq 0$, $t \geq 0$, f_i é comutador de comprimento ≥ 2 para todo i.

Se $t = 0$ então $f + I_s$ é como em (3.26).

Suponha que $t \geq 2$. Pelo Lema 3.1.9 temos

$$f_1, f_2 \in F\langle Y \cup Z\rangle^+ \ \cup \ F\langle Y \cup Z\rangle^-.$$

Dois casos podem ocorrer:

a) f_1 ou f_2 é simétrico. Neste caso, pelo Lema 3.1.9 - d, temos que f_1 ou f_2 pertence a

$$\langle [z_1, y_1]\rangle^{T(*)}.$$

Logo,

$$f \in \langle [z_1, y_1]\rangle^{T(*)} \subseteq I_s.$$

b) f_1 e f_2 são antissimétricos. Neste caso, pelo Lema 3.1.9 - c, temos que

$$f_1 f_2 \in \langle [y_1, y_2],\ [z_1, z_2][z_3, z_4]\rangle^{T(*)}.$$

Logo,

$$f \in \langle [y_1, y_2],\ [z_1, z_2][z_3, z_4]\rangle^{T(*)} \subseteq I_s.$$

Acabamos de mostrar que se $t \geq 2$, então $f + I_s = I_s$.

Suponhamos que $t = 1$ e $f + I_s \neq I_s$. Como $f + I_s \neq I_s$, segue que f_1 é formado por variáveis que estão apenas em Z, pois $[z_1, y_1], [y_1, y_2] \in I_s$ (veja Lema 3.1.9). Logo, f_1 tem a forma

$$f_1 = [z_{i_1}, z_{i_2}, z_{i_3}, \ldots, z_{i_l}]$$

e o polinômio $\overline{f} = z_1^{r_1} \cdots z_m^{r_m} f_1$ é combinação linear de polinômios u do tipo

$$u = z_{j_1} \cdots z_{j_t}[z_{i_1}, z_{i_2}]z_{j_{t+1}} \cdots z_{j_q}.$$

Pelo Lema 3.2.6,

$$u + I_s = \pm[z_{i_1}, z_{i_2}]z_{j_1} \cdots z_{j_q} + I_s.$$

Então $f + I_s$ é combinação linear de polinômios do tipo

$$y_1^{s_1} \cdots y_n^{s_n}[z_{i_1}, z_{i_2}]z_{j_1} \cdots z_{j_q} + I_s. \tag{3.27}$$

Usando o Lema 3.2.7 podemos ordenar as variáveis z_{j_s} in (3.27). Assim podemos supor, sem perda de generalidade, que $j_1 \leq \ldots \leq j_q$ e $i_1 > i_2$.

Por outro lado, pelo Lema 3.2.5, temos

$$[z_3, z_2]z_1 + I_s = [z_3, z_1]z_2 - [z_2, z_1]z_3 + I_s. \tag{3.28}$$

Suponhamos que $i_2 > j_1$. Por (3.28) temos

$$[z_{i_1}, z_{i_2}]z_{j_1} \ldots z_{j_q} + I_s = [z_{i_1}, z_{j_1}]z_{i_2}z_{j_2} \ldots z_{j_q} - [z_{i_2}, z_{j_1}]z_{i_1}z_{j_2} \ldots z_{j_q} + I_s. \tag{3.29}$$

Usando o Lema 3.2.7 novamente é possível reordenar, se necessário, as variáveis z's dos monômios $z_{i_2}z_{j_2} \ldots z_{j_q}$ e $z_{i_1}z_{j_2} \ldots z_{j_q}$ em (3.29). Deste modo, podemos supor em (3.27) que $i_1 > i_2 \leq j_1 \leq \ldots \leq j_q$ como era o desejado. □

De agora até o fim desta seção, F denotará um corpo finito com q elementos. Denote por J_s o $T(*)$-ideal gerado pelos polinômios

$$[y_1, y_2] \quad [z_1, y_1], \quad [z_1, z_2][z_3, z_4], \quad z_1z_2z_3 - z_3z_2z_1, \tag{3.30}$$

$$(z_1^q - z_1)(z_2^q - z_2), \quad [z_1, z_2](z_3^q - z_3), \tag{3.31}$$

$$y_1^q - y_1, \quad z_1^{q+1} - z_1^2, \quad (z_1^q - z_1)z_2 + z_2(z_1^q - z_1). \tag{3.32}$$

Como I_s é gerado como $T(*)$-ideal pelos elementos em (3.23), temos que $I_s \subseteq J_s$.

Lema 3.2.9. *Seja F um corpo finito com q elementos. Então $J_s \subseteq Id(UT_2(F), s)$.*

Demonstração. Pelo Lema 3.2.3, os polinômios em (3.30) pertencem a $Id(UT_2(F), s)$.

Pelo Teorema 2.1.2 segue que

$$[x_1, x_2], \ (x_1^q - x_1) \in Id(F).$$

Pelo parágrafo anterior a tal teorema, comentamos que

$$Id(UT_2(F)) = (Id(F))^2.$$

Logo,

$$(x_1^q - x_1)(x_2^q - x_2), \quad [x_1, x_2](x_3^q - x_3) \in Id(UT_2(F)).$$

Consequentemente, pelo Lema 2.4.4, os polinômios em (3.31) estão em $Id(UT_2(F), s)$.

Agora analisaremos os polinômios em (3.32). Sejam $y \in UT_2(F)^+$ e $z \in UT_2(F)^-$. Temos

$$y = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \quad \text{e} \quad z = \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix}$$

para alguns $a, b, c \in F$ (veja Lema 3.2.1). Claramente,

$$y^i = \begin{pmatrix} c^i & 0 \\ 0 & c^i \end{pmatrix}.$$

Em particular, $y^q = y$ pois $|F| = q$. Provamos que o polinômio $y_1^q - y_1$, de (3.32), pertence a $Id(UT_2(F), s)$.

Para o segundo polinômio em (3.32), foi comentado na introdução deste capítulo que a $\text{car}(F) = p \neq 2$. Neste caso, p é ímpar e consequentemente $|F| = q$ é uma potência de p, isto é, q é ímpar. Logo, $q + 1$ é par e por (3.21) segue que $z^{q+1} = a^{q+1}1 = a^q a1 = a^2 1 = z^2$. Provamos que $z_1^{q+1} - z_1^2 \in Id(UT_2(F), s)$.

Para o terceiro polinômio em (3.32), usaremos a igualdade (3.22). Assim,

$$z^q = \begin{pmatrix} a^q & a^{q-1}b \\ 0 & -a^q \end{pmatrix} = \begin{pmatrix} a & a^{q-1}b \\ 0 & -a \end{pmatrix}. \tag{3.33}$$

Sejam $Z_i = \begin{pmatrix} a_i & b_i \\ 0 & -a_i \end{pmatrix}$. Então,

$$Z_1^q - Z_1 = \begin{pmatrix} 0 & a_1^{q-1}b_1 - b_1 \\ 0 & 0 \end{pmatrix}.$$

Logo, $(Z_1^q - Z_1)Z_2 + Z_2(Z_1^q - Z_1)$ é igual a

$$\begin{pmatrix} 0 & (a_1^{q-1} - 1)b_1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & -a_2 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ 0 & -a_2 \end{pmatrix} \begin{pmatrix} 0 & (a_1^{q-1} - 1)b_1 \\ 0 & 0 \end{pmatrix} = 0$$

Provamos que $(z_1^q - z_1)z_2 + z_2(z_1^q - z_1) \in Id(UT_2(F), s)$. □

Lema 3.2.10. *Seja F um corpo finito com q elementos e seja $m \geq 1$. Para todo $i \geq 1$ temos*

$$z_1 \cdots z_m(z_i^q - z_i) + J_s = (-1)^m(z_i^q - z_i)z_1 \cdots z_m + J_s.$$

Demonstração. Por (3.32) temos que

$$z_j(z_i^q - z_i) + J_s = -(z_i^q - z_i)z_j + J_s.$$

Assim,

$$\begin{aligned} z_1 \cdots z_m(z_i^q - z_i) + J_s &= -z_1 \cdots z_{m-1}(z_i^q - z_i)z_m + J_s \\ &= +z_1 \cdots z_{m-2}(z_i^q - z_i)z_{m-1}z_m + J_s \\ &\vdots \\ &= (-1)^m(z_i^q - z_i)z_1 \cdots z_m + J_s. \end{aligned}$$

Finalizamos a demonstração. □

Lema 3.2.11. *Seja F um corpo finito com q elementos e seja $u = z_1 \cdots z_m$, onde $m \geq 1$. Para todos $i, j \geq 1$ temos*

$$z_i^q u z_j^q + J_s = z_i u z_j^q + z_i^q u z_j - z_i u z_j + J_s.$$

Demonstração. Por (3.31) e Lema 3.2.10 obtemos

$$\begin{aligned} J_s = (z_i^q - z_i)(z_j^q - z_j)u + J_s &= \pm(z_i^q - z_i)u(z_j^q - z_j) \\ &= \pm(z_i^q u z_j^q - z_i u z_j^q - z_i^q u z_j + z_i u z_j) + J_s, \end{aligned}$$

o que prova o lema. □

Lema 3.2.12. *Seja F um corpo finito com q elementos e seja $m \geq 0$. Para todos $i, j \geq 1$ temos*

$$[z_i, z_j]z_1 \cdots z_m z_{m+1}^q + J_s = [z_i, z_j]z_1 \cdots z_{m+1} + J_s.$$

Demonstração. Pelo Lema 3.2.6,

$$[z_i, z_j]z_1 \cdots z_m(z_{m+1}^q - z_{m+1}) + J_s = (-1)^m z_1 \cdots z_m[z_i, z_j](z_{m+1}^q - z_{m+1}) + J_s.$$

Como $[z_i, z_j](z_{m+1}^q - z_{m+1}) \in J_s$ (veja (3.31)) temos o resultado demonstrado. □

Lema 3.2.13. *Seja F um corpo finito com q elementos. Para todo $\sigma \in S_m$ vale*

$$(z_{m+1}^q - z_{m+1})z_{\sigma(1)} \cdots z_{\sigma(m)} + J_s \quad = \quad (z_{m+1}^q - z_{m+1})z_1 \cdots z_m + J_s.$$

Demonstração. Como $[z_i, z_{i+1}](z_{m+1}^q - z_{m+1}) \in J_s$ (veja (3.31)), temos

$$z_i z_{i+1}(z_{m+1}^q - z_{m+1}) + J_s = z_{i+1} z_i (z_{m+1}^q - z_{m+1}) + J_s.$$

Por isso e Lema 3.2.10 seguem as igualdades:

$$\begin{aligned}
&(z_{m+1}^q - z_{m+1})z_1 \cdots z_i z_{i+1} \cdots z_m + J_s = \\
&\quad = (-1)^{i+1} z_1 \cdots z_i z_{i+1}(z_{m+1}^q - z_{m+1}) \cdots z_m + J_s \\
&\quad = (-1)^{i+1} z_1 \cdots z_{i+1} z_i (z_{m+1}^q - z_{m+1}) \cdots z_m + J_s \\
&\quad = (z_{m+1}^q - z_{m+1}) z_1 \cdots z_{i+1} z_i \cdots z_m + J_s \ .
\end{aligned}$$

Usando este fato várias vezes concluíremos o resultado. □

Lema 3.2.14. *Seja F um corpo finito com q elementos. Então*

$$[z_2, z_1] z_1^{q-1} + J_s = -2(z_1^q - z_1) z_2 + [z_2, z_1] + J_s.$$

Demonstração. Como z_1^{q-1} é simétrico, por (3.30) temos que $[z_2, z_1^{q-1}] + J_s = J_s$. Segue que

$$\begin{aligned}
[z_2, z_1] z_1^{q-1} + J_s &= [z_2, z_1 z_1^{q-1}] - z_1 [z_2, z_1^{q-1}] + J_s \\
&= [z_2, z_1^q] + J_s \\
&= z_2 z_1^q - z_1^q z_2 + J_s.
\end{aligned} \tag{3.34}$$

Por (3.32) temos

$$z_2 z_1^q + J_s = -z_1^q z_2 + z_1 z_2 + z_2 z_1 + J_s. \tag{3.35}$$

Assim, substituindo (3.35) em (3.34) temos

$$\begin{aligned}
[z_2, z_1] z_1^{q-1} + J_s &= (-z_1^q z_2 + z_1 z_2 + z_2 z_1) - z_1^q z_2 + J_s \\
&= -2 z_1^q z_2 + z_1 z_2 + z_2 z_1 + J_s \\
&= -2 z_1^q z_2 + 2 z_1 z_2 + [z_2, z_1] + J_s = -2(z_1^q - z_1) z_2 + [z_2, z_1] + J_s.
\end{aligned}$$

Finalizamos a demonstração. □

Lema 3.2.15. *Seja F um corpo finito com q elementos. Dado $m \geq 0$, denote $u = z_1 \cdots z_m$. Existe $0 \neq \alpha \in F$ tal que*

$$[z_i, z_j] u z_i^{q-1} + J_s = \alpha z_j u (z_i^q - z_i) + [z_i, z_j] u + J_s$$

para cada $i, j \geq 1$.

Demonstração. Pelos Lemas 3.2.7, 3.2.14 e 3.2.10 (respectivamente) temos

$$\begin{aligned}
[z_i, z_j] u z_i^{q-1} + J_s = [z_i, z_j] z_i^{q-1} u + J_s &= -[z_j, z_i] z_i^{q-1} u + J_s \\
&= (2(z_i^q - z_i) z_j - [z_j, z_i]) u + J_s \\
&= \pm 2 z_j u (z_i^q - z_i) + [z_i, z_j] u + J_s.
\end{aligned}$$

Finalizamos a demonstração. □

Definição 3.2.16. *Seja F um corpo finito com q elementos. Para cada $m \geq 1$, defina Δ_m como o conjunto dos elementos $(r_1, \ldots, r_m) \in \mathbb{Z}^m$ tais que:*

a) $0 \leq r_1, \ldots, r_m \leq q$,

b) Se $r_i = q$ para algum i, então $r_j < q$ para todo $j \neq i$.

Proposição 3.2.17. *Seja F um corpo finito com q elementos. O espaço vetorial quociente $F\langle Y \cup Z\rangle/J_s$ é gerado pelos elementos*

$$\begin{cases} y_1^{s_1}\cdots y_n^{s_n}[z_j, z_i]z_i^{r_i}z_{i+1}^{r_{i+1}}\cdots z_m^{r_m} + J_s, & 0 \leq s_1, \ldots, s_n, r_i, \ldots, r_m < q, \\ & r_i, r_j < q-1, j > i,\ n \geq 1,\ m \geq 1 : \Upsilon_1 \\ y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m} + J_s, & 0 \leq s_1, \ldots, s_n < q, \quad (r_1, \ldots, r_m) \in \Delta_m, \\ & n \geq 1,\ m \geq 1 \qquad\qquad\qquad : \Upsilon_2 \end{cases}$$

Demonstração. Sejam Ψ_1, Ψ_2 dois conjuntos definidos pelos elementos abaixo:

$$\begin{cases} y_1^{s_1}\cdots y_n^{s_n}[z_j, z_i]z_i^{r_i}z_{i+1}^{r_{i+1}}\cdots z_m^{r_m} + J_s, & 0 \leq s_1, \ldots, s_n, r_i, \ldots, r_m;\ j > i, n \geq 1, m \geq 1 : \Psi_1 \\ y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m} + J_s, & 0 \leq s_1, \ldots, s_n, r_1, \ldots, r_m;\ n \geq 1, m \geq 1 \qquad : \Psi_2 \end{cases}$$

Denote por (Υ_i) e (Ψ_i) os subespaços de $F\langle Y \cup Z\rangle/J_s$ gerados pelos conjuntos Υ_i e Ψ_i, respectivamente. Uma vez que $I_s \subseteq J_s$, pela Proposição 3.2.8 temos que

$$F\langle Y \cup Z\rangle/J_s = (\Psi_1) + (\Psi_2).$$

Assim, devemos provar que

$$(\Upsilon_1) + (\Upsilon_2) = (\Psi_1) + (\Psi_2).$$

A inclusão $\subseteq$ é óbvia. Provaremos a outra inclusão.

Afirmação 1: $(\Psi_2) \subseteq (\Upsilon_2)$.
Seja $f = y_1^{l_1}\cdots y_n^{l_n}z_1^{t_1}\cdots z_m^{t_m}$. Mostraremos que $f + J_s \in (\Upsilon_2)$. Por (3.32) temos que $y_i^q + J_s = y_i + J_s$. Logo, existem $0 \leq s_1, \ldots, s_n < q$ tais que

$$f + J_s = y_1^{s_1}\cdots y_n^{s_n}z_1^{t_1}\cdots z_m^{t_m} + J_s.$$

Também por (3.32) temos que $z_j^{q+1} + J_s = z_j^2 + J_s$. Logo, existem $0 \leq r_1, \ldots, r_m \leq q$ tais que

$$f + J_s = y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m} + J_s.$$

Procederemos por indução sobre m.
O caso $m = 1$ é óbvio.
Suponha $m = 2$. Por (3.31) temos

$$z_1^q z_2^q + J_s = z_1^q z_2 + z_1 z_2^q - z_1 z_2 + J_s.$$

Logo, $y_1^{s_1}\cdots y_n^{s_n}z_1^q z_2^q + J_s \in (\Upsilon_2)$.
Seja $m \geq 3$. Por hipótese de indução podemos supor, sem perda de generalidade, que $(r_1, \ldots, r_{m-1}) \in \Delta_{m-1}$. Temos dois casos:
a) Se $r_m < q$ ou $r_1, \ldots, r_{m-1} < q$ temos que $(r_1, \ldots, r_m) \in \Delta_m$. Logo,

$$f + J_s = y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m} + J_s \in (\Upsilon_2).$$

b) Suponha $r_m = q$ e $r_j = q$ para algum $1 \leq j \leq m-1$. Então $r_i < q$ para todo $i \neq j$ e $i \neq m$ (pois $(r_1, \ldots, r_{m-1}) \in \Delta_{m-1}$). Pelo Lema 3.2.11 temos

$$f + J_s = uz_j^q v z_m^q + J_s = uz_j v z_m^q + uz_j^q v z_m - uz_j v z_m + J_s \in (\Upsilon_2),$$

onde $u = y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_{j-1}^{r_{j-1}}$ e $v = z_{j+1}^{r_{j+1}} \cdots z_{m-1}^{r_{m-1}}$, o que prova a Afirmação 1.

Afirmação 2: $(\Psi_1) \subseteq (\Upsilon_1) + (\Psi_2)$.
Seja $f = y_1^{s_1} \cdots y_n^{s_n} [z_j, z_i] z_i^{l_i} z_{i+1}^{l_{i+1}} \cdots z_m^{l_m}$, $i < j \leq m$. Como já vimos na demonstração da Afirmação 1, por (3.32) podemos supor, sem perda de generalidade, que $0 \leq s_1, \ldots, s_n < q$ e $0 \leq l_i, \ldots, l_m \leq q$.

Pelo Lema 3.2.12 existem inteiros r_k tais que $0 \leq r_i, \ldots, r_m < q$ e

$$f + J_s = y_1^{s_1} \cdots y_n^{s_n} [z_j, z_i] z_i^{r_i} z_{i+1}^{r_{i+1}} \cdots z_m^{r_m} + J_s.$$

Então temos três casos:
a) Se $r_i, r_j < q-1$ então $f + J_s \in \Upsilon_1 \subset (\Upsilon_1) + (\Psi_2)$.

b) Se $r_i < q-1$ e $r_j = q-1$, pelo Lema 3.2.15 existe um $\alpha \in F$ tal que

$$f + J_s = u[z_j, z_i] v z_j^{q-1} w + J_s = \alpha u z_i v (z_j^q - z_j) w + u[z_j, z_i] v w + J_s,$$

onde $u = y_1^{s_1} \cdots y_n^{s_n}$, $v = z_i^{r_i} \cdots z_{j-1}^{r_{j-1}}$ e $w = z_{j+1}^{r_{j+1}} \cdots z_m^{r_m}$. Observe que

$$u z_i v (z_j^q - z_j) w + J_s \in (\Psi_2)$$

e que

$$u[z_j, z_i] v w + J_s \in \Upsilon_1.$$

Logo, $f \in (\Upsilon_1) + (\Psi_2)$.

c) Se $r_i = q-1$ então por Lema 3.2.14

$$f + J_s = u[z_j, z_i] z_i^{q-1} v + J_s = -2u(z_i^q - z_i) z_j v + u[z_j, z_i] v + J_s$$

onde $u = y_1^{s_1} \cdots y_n^{s_n}$ e $v = z_{i+1}^{r_{i+1}} \cdots z_m^{r_m}$. Observe que pelo Lema 3.2.13

$$u(z_i^q - z_i) z_j v + J_s = u(z_i^q - z_i) z_{i+1}^{r_{i+1}} \cdots z_j^{r_j+1} \cdots z_m^{r_m} + J_s \in (\Psi_2).$$

Uma vez que a potência de z_i em $u[z_j, z_i]v$ é 1, pelos casos a) e b) temos que

$$u[z_j, z_i] v + J_s \in (\Upsilon_1) + (\Psi_2).$$

Pelas Afirmações 2 e 1 segue que $(\Psi_1) + (\Psi_2) \subseteq (\Upsilon_1) + (\Psi_2) \subseteq (\Upsilon_1) + (\Upsilon_2)$, como era o desejado. $\square$

Lema 3.2.18. *Seja F um corpo finito com q elementos. Denote $\widetilde{J}_s = Id(UT_2(F), s)$. O subconjunto*

$$\{z_1^i + \widetilde{J}_s \mid i = 1, \ldots, q\} \subseteq F\langle Y \cup Z \rangle / \widetilde{J}_s$$

é linearmente independente.

Demonstração. Considere o polinômio $f(z_1) = \alpha_1 z_1 + \ldots + \alpha_q z_1^q \in \widetilde{J}_s$, onde cada $\alpha_i \in F$. Considere a seguinte matriz antissimétrica

$$Z_1 = \begin{pmatrix} a & 1 \\ 0 & -a \end{pmatrix},$$

onde $a \in F$. Então

$$Z_1^i = \begin{pmatrix} a^i & \delta_i a^{i-1} \\ 0 & (-1)^i a^i \end{pmatrix}$$

com $\delta_i = (1 + (-1)^{i+1})/2$ (veja (3.21) e (3.22)). Assim,

$$f(Z_1) = E_{11}e_{11} + E_{12}e_{12} + E_{22}e_{22} = 0$$

onde

$$E_{11} = \alpha_1 a + \ldots + \alpha_q a^q \quad \text{e} \quad E_{12} = \alpha_1\delta_1 + \alpha_2\delta_2 a + \ldots + \alpha_q\delta_q a^{q-1}.$$

Note que $E_{11} = 0$ e $E_{12} = 0$ para todo $a \in F$. Pelo Lema 2.1.3, $E_{12} = 0$ implica que $\alpha_q\delta_q = \alpha_q = 0$. Logo,

$$E_{11} = \alpha_1 a + \ldots + \alpha_{q-1}a^{q-1} = 0$$

para todo $a \in F$. Novamente pelo Lema 2.1.3 temos que $\alpha_i = 0$ para todo $i = 1, \ldots, q-1$. $\square$

Lema 3.2.19. *Seja F um corpo finito com q elementos. Denote $\widetilde{J}_s = Id(UT_2(F), s)$. O conjunto de todos polinômios*

$$\begin{cases} [z_j, z_i]z_i^{r_i}z_{i+1}^{r_{i+1}}\cdots z_m^{r_m} + \widetilde{J}_s, & 0 \le r_i, \ldots, r_m < q, \quad r_i, r_j < q-1, \quad j > i, \quad m \ge 1; \\ z_1^{r_1}\cdots z_m^{r_m} + \widetilde{J}_s, & (r_1, \ldots, r_m) \in \Delta_m, \quad m \ge 1, \end{cases}$$

é linearmente independente em $F\langle Y \cup Z\rangle/\widetilde{J}_s$.

Demonstração. Seja $1 \le k \le m$. Denote

$$\frac{z_1^{r_1}\cdots z_m^{r_m}}{z_1 z_k} = z_1^{s_1}\cdots z_m^{s_m}$$

onde $s_1 = r_1 - 1$, $s_k = r_k - 1$ e $s_j = r_j$ se $j \ne 1, k$.

Considere $f = g + h$ onde $f \in \widetilde{J}_s$,

$$g = \sum \alpha_{j,i,r}[z_j, z_i]z_i^{r_i}z_{i+1}^{r_{i+1}}\cdots z_m^{r_m}$$

$0 \le r_i, \ldots, r_m < q$, $r_i, r_j < q-1$, $j > i$, $m \ge 1$, $r = (r_i, \ldots, r_m)$, $\alpha_{j,i,r} \in F$, e

$$h = \sum \beta_r z_1^{r_1}\cdots z_m^{r_m},$$

$r = (r_1, \ldots, r_m) \in \Delta_m$, $m \ge 1$, $\beta_r \in F$.

Se $f = f_0 + f_1$ onde

a) f_0 é uma combinação linear de monômios w com $\deg_{z_1} w = 0$,

b) f_1 é uma combinação linear de monômios w com $\deg_{z_1} w \ge 1$,

então $f(0, z_2, \ldots, z_m) = f_0 \in \widetilde{J}_s$. Em particular, $f_1 \in \widetilde{J}_s$ também. Portanto podemos supor, sem perda de generalidade, que $f = f(z_1, \ldots, z_m)$ é uma combinação linear de monômios w com $\deg_{z_i} w \ge 1$ para todo $i = 1, \ldots, m$. Neste caso, escrevemos g como

$$g = \sum_{k=2}^{m}\sum_{r}\alpha_r^{(k)}[z_k, z_1]\frac{z_1^{r_1}\cdots z_m^{r_m}}{z_1 z_k},$$

onde $1 \leq r_1, \ldots, r_m < q$, $\quad r = (r_1, \ldots, r_m)$, $\quad \alpha_r^{(k)} \in F$. Note que

$$[z_k, z_1]\frac{z_1^{r_1} \cdots z_m^{r_m}}{z_1 z_k}$$

é multi-homogêneo com multigrau $r = (r_1, \ldots, r_m)$.

O polinômio g pode ser escrito como

$$g = g_0 + g_1 z_m + \cdots + g_{q-1} z_m^{q-1},$$

onde cada g_j está definido abaixo:

a) Para $j = 0$,

$$g_0 = \sum_{r_m=1} \alpha_r^{(m,0)}[z_m, z_1]\frac{z_1^{r_1} \cdots z_{m-1}^{r_{m-1}}}{z_1},$$

onde $1 \leq r_1, \ldots, r_{m-1} < q$, $\quad r = (r_1, \ldots, r_{m-1}, 1)$, $\alpha_r^{(m,0)} = \alpha_r^{(m)}$.

b) Para $j = 1, \ldots, q-2$,

$$g_j = \sum_{k=2}^{m-1} \sum_{r_m=j} \alpha_r^{(k,j)}[z_k, z_1]\frac{z_1^{r_1} \cdots z_{m-1}^{r_{m-1}}}{z_1 z_k} + \sum_{r_m=j+1} \alpha_r^{(m,j)}[z_m, z_1]\frac{z_1^{r_1} \cdots z_{m-1}^{r_{m-1}}}{z_1},$$

onde $1 \leq r_1, \ldots, r_m < q$, $\quad r = (r_1, \ldots, r_m)$, $\alpha_r^{(k,j)} = \alpha_r^{(k)}$, $\alpha_r^{(m,j)} = \alpha_r^{(m)}$.

c) Para $j = q-1$,

$$g_{q-1} = \sum_{k=2}^{m-1} \sum_{r_m=q-1} \alpha_r^{(k,q-1)}[z_k, z_1]\frac{z_1^{r_1} \cdots z_{m-1}^{r_{m-1}}}{z_1 z_k}$$

onde $1 \leq r_1, \ldots, r_{m-1} < q$, $\quad r = (r_1, \ldots, r_{m-1}, q-1)$, $\alpha_r^{(k,q-1)} = \alpha_r^{(k)}$.

O polinômio h pode ser escrito como

$$h = h_1 z_m + \cdots + h_q z_m^q,$$

onde cada h_j está definido abaixo:

a) Para $j = 1, \ldots, q-1$,

$$h_j = \sum_{r_m=j} \beta_r^{(j)} z_1^{r_1} \cdots z_{m-1}^{r_{m-1}},$$

onde $\beta_r^{(j)} = \beta_r$, $r = (r_1, \ldots, r_{m-1}, j)$, $\ (r_1, \ldots, r_{m-1}) \in \Delta_{m-1}$.

b) Para $j = q$,

$$h_q = \sum_{r_m=q} \beta_r^{(q)} z_1^{r_1} \cdots z_{m-1}^{r_{m-1}}$$

onde $1 \leq r_1, \ldots, r_{m-1} < q$, $r = (r_1, \ldots, r_{m-1}, q)$, $\beta_r^{(q)} = \beta_r$.

Para $f = g + h \in \widetilde{J}_s$ provaremos, por indução em $m \geq 1$, que

$$\alpha_r^{(k,j)} = \beta_r^{(j)} = 0$$

para todos r, k, j.

a) Suponha $m = 1$.

Neste caso, $f = h$ e usamos o Lema 3.2.18.

b) Suponha $m > 1$.
Se

$$Z_i = \begin{pmatrix} a_i & 0 \\ 0 & -a_i \end{pmatrix}, \ a_i \in F, \ i = 1, \ldots, m,$$

então $f(Z_1, \ldots, Z_m) = g(Z_1, \ldots, Z_m) + h(Z_1, \ldots, Z_m) = h(Z_1, \ldots, Z_m)$. Na última igualdade usamos o fato que

$$[Z_k, Z_1] = 0.$$

Continuando, como $f \in \widetilde{J}_s$ segue que $0 = f(Z_1, \ldots, Z_m) = h(Z_1, \ldots, Z_m)$. Note que

$$h(Z_1, \ldots, Z_m) = \sum_{j=1}^{q} h_j(Z_1, \ldots, Z_{m-1}) Z_m^j = E_{11}e_{11} + E_{22}e_{22} = 0$$

onde $E_{11}, \ E_{22} \in F$ e

$$E_{11} = E_{11}(a_1, \ldots, a_m) = \sum_{j=1}^{q} h_j(a_1, \ldots, a_{m-1}) a_m^j = \sum_{j=2}^{q-1} h_j(a_1, \ldots, a_{m-1}) a_m^j + \\ + (h_1(a_1, \ldots, a_{m-1}) + h_q(a_1, \ldots, a_{m-1})) a_m.$$

Observe que usamos o fato $a_m^q = a_m$ na última igualdade. Como $E_{11} = 0$, se fixarmos $a_1, \ldots, a_{m-1} \in F$ então

$$E_{11}(a_1, \ldots, a_{m-1}, x) \in Id(F).$$

Pelo Lema 2.1.3 temos $h_j(a_1, \ldots, a_{m-1}) = 0$ e $(h_1(a_1, \ldots, a_{m-1}) + h_q(a_1, \ldots, a_{m-1})) = 0$ para todo $j = 2, \ldots, q-1$. Como $a_1, \ldots, a_{m-1}$ são elementos arbitrários de F temos

$$(h_1 + h_q), \ h_2, \ \ldots, \ h_{q-1} \in Id(F). \tag{3.36}$$

Defina $W_1, \ldots, W_m \in UT_2(F)^-$ como segue:

$$W_i = \begin{pmatrix} -a_i & 0 \\ 0 & a_i \end{pmatrix} \ \text{se } i = 1, \ldots, m-1, \quad \text{e} \ W_m = \begin{pmatrix} -a_m & 1 \\ 0 & a_m \end{pmatrix}$$

onde $a_1, \ldots, a_m \in F$. Note que

$$[W_k, W_1] = 0$$

se $k \neq m$. Logo,

$$\begin{aligned} f(W_1, \ldots, W_m) =& g(W_1, \ldots, W_m) + h(W_1, \ldots, W_m) \\ =& \sum_{j=0}^{q-1} g_j(W_1, \ldots, W_m) W_m^j + \sum_{j=1}^{q} h_j(W_1, \ldots, W_{m-1}) W_m^j \\ =& \sum_{r_m=1} \alpha_r^{(m,0)} [W_m, W_1] \frac{W_1^{r_1} \cdots W_{m-1}^{r_{m-1}}}{W_1} + \\ & \sum_{j=1}^{q-2} \sum_{r_m=j+1} \alpha_r^{(m,j)} [W_m, W_1] \frac{W_1^{r_1} \cdots W_{m-1}^{r_{m-1}}}{W_1} W_m^j + \\ & \sum_{j=1}^{q} h_j(W_1, \ldots, W_{m-1}) W_m^j. \end{aligned}$$

Olhando para as entradas $(1,1)$ e $(2,2)$ de $h_j(W_1,\ldots,W_{m-1})$ (no último somatório), temos por (3.36) que

$$\begin{aligned}
f(W_1,\ldots,W_m) = & \sum_{r_m=1} \alpha_r^{(m,0)}[W_m,W_1]\frac{W_1^{r_1}\cdots W_{m-1}^{r_{m-1}}}{W_1} + \\
& \sum_{j=1}^{q-2}\sum_{r_m=j+1} \alpha_r^{(m,j)}[W_m,W_1]\frac{W_1^{r_1}\cdots W_{m-1}^{r_{m-1}}}{W_1}W_m^j + \\
& h_q(W_1,\ldots,W_{m-1})(W_m^q - W_m) \\
= & E_{12}e_{12}
\end{aligned} \tag{3.37}$$

onde $E_{12}\in F$ é dado por

$$\begin{aligned}
E_{12} = & \sum_{j=0}^{q-2}\sum_{r_m=j+1} 2\alpha_r^{(m,j)} a_1^{r_1}\cdots a_{m-1}^{r_{m-1}} a_m^j \\
& + h_q(-a_1,\ldots,-a_{m-1})(a_m^{q-1}-1).
\end{aligned}$$

Como $f\in \widetilde{J}_s$, temos $E_{12}=0$. Note que $1\leq r_1,\ldots,r_{m-1},r_m\leq q-1$ (por definição). Mais ainda,

$$h_q = \sum_{r_m=q} \beta_r^{(q)} z_1^{r_1}\cdots z_{m-1}^{r_{m-1}}$$

onde $1\leq r_1,\ldots,r_{m-1}\leq q-1$ (por definição de h_q). Assim, pelo Lema 2.1.3, segue que $\alpha_r^{(m,j)}=0$ for all $j=0,\ldots,q-2$, $r=(r_1,\ldots,r_{m-1},j+1)$, $1\leq r_1,\ldots,r_{m-1}\leq q-1$; e $\beta_r^{(q)}=0$ para todo $r=(r_1,\ldots,r_{m-1},q)$, $1\leq r_1,\ldots,r_{m-1}\leq q-1$.

Em particular, $h_q=0$, $g_0=0$ e

$$\begin{aligned}
g_j = & \sum_{k=2}^{m-1}\sum_{r_m=j} \alpha_r^{(k,j)}[z_k,z_1]\frac{z_1^{r_1}\cdots z_{m-1}^{r_{m-1}}}{z_1z_k} + \sum_{r_m=j+1} \alpha_r^{(m,j)}[z_m,z_1]\frac{z_1^{r_1}\cdots z_{m-1}^{r_{m-1}}}{z_1} \\
= & \sum_{k=2}^{m-1}\sum_{r_m=j} \alpha_r^{(k,j)}[z_k,z_1]\frac{z_1^{r_1}\cdots z_{m-1}^{r_{m-1}}}{z_1z_k},
\end{aligned}$$

onde $j=1,\ldots,q-2$, $1\leq r_1,\ldots,r_m<q$, $\;r=(r_1,\ldots,r_m)$. Assim,

$$f = g+h = \sum_{j=1}^{q-1} g_j z_m^j \;+\; \sum_{j=1}^{q-1} h_j z_m^j = \sum_{j=1}^{q-1}(g_j+h_j)z_m^j,$$

onde $\deg_{z_m}(g_j+h_j)=0$ para todo $j=1,\ldots,q-1$. Pela Proposição 2.4.9, segue que $(g_j+h_j)z_m^j\in\widetilde{J}_s$ para todo $j=1,\ldots,q-1$. Assim,

$$(g_j+h_j)z_m^{q+1} = (g_j+h_j)z_m^j z_m^{q-j+1}\in\widetilde{J}_s$$

para todo $j=1,\ldots,q-1$. Se $A_1,\ldots,A_{m-1}\in UT_2(F)^-$ e $A_m=e_{11}-e_{22}$, então

$$0 = ((g_j+h_j)(A_1,\ldots,A_{m-1}))A_m^{q+1} = (g_j+h_j)(A_1,\ldots,A_{m-1}).$$

Portanto, $(g_j+h_j)\in\widetilde{J}_s$ para todo $j=1,\ldots,q-1$. Agora nós aplicamos a hipótese de indução em cada (g_j+h_j) para completar a demonstração. $\square$

Lema 3.2.20. *Seja F um corpo finito com q elementos. Denote $\widetilde{J}_s = Id(UT_2(F), s)$. Seja Ω o conjunto formado por todos polinômios*

$$\begin{cases} y_1^{s_1}\cdots y_n^{s_n}[z_j,z_i]z_i^{r_i}z_{i+1}^{r_{i+1}}\cdots z_m^{r_m}, & 0\le s_1,\ldots,s_n,r_i,\ldots,r_m<q,\\ & r_i,r_j<q-1, j>i,\ n\ge 1,\ m\ge 1;\\ y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m}, & 0\le s_1,\ldots,s_n<q,\\ & (r_1,\ldots,r_m)\in\Delta_m, n\ge 1,\ m\ge 1.\end{cases}$$

Então $\{f+\widetilde{J}_s\ :\ f\in\Omega\}$ é um subconjunto de $F\langle Y\cup Z\rangle/\widetilde{J}_s$ linearmente independente.

Demonstração. Seja $f(y_1,\ldots,y_n,z_1,\ldots,z_m)$ uma combinação linear dos polinômios em Ω tais que $f+\widetilde{J}_s=\widetilde{J}_s$. Podemos escrever

$$f=\sum_s y_1^{s_1}\cdots y_n^{s_n}f_s(z_1,\ldots,z_m)$$

onde $0\le s_1,\ldots,s_n<q$, $s=(s_1,\ldots,s_n)$ e $f_s(z_1,\ldots,z_m)$ combinação linear de polinômios em

$$\begin{cases} [z_j,z_i]z_i^{r_i}z_{i+1}^{r_{i+1}}\cdots z_m^{r_m}, & 0\le r_i,\ldots,r_m<q,\quad r_i,r_j<q-1,\quad j>i,\quad m\ge 1;\\ z_1^{r_1}\cdots z_m^{r_m}, & (r_1,\ldots,r_m)\in\Delta_m,\quad m\ge 1.\end{cases}$$

Pela Proposição 2.4.9 temos

$$y_1^{s_1}\cdots y_n^{s_n}f_s(z_1,\ldots,z_m)\in\widetilde{J}_s$$

para todo s. Substituindo $y_1=\ldots=y_n=1$ obtemos que $f_s(z_1,\ldots,z_m)\in\widetilde{J}_s$. Agora pelo Lema 3.2.19 temos o resultado desejado. □

Teorema 3.2.21. *Seja F um corpo finito com q elementos. Denote por J_s o $T(*)$-ideal gerado pelos polinômios*

$$\begin{gathered}[y_1,y_2],\quad [z_1,y_1],\quad [z_1,z_2][z_3,z_4]\quad z_1z_2z_3-z_3z_2z_1,\\ y_1^q-y_1,\quad (z_1^q-z_1)(z_2^q-z_2),\quad z_1^{q+1}-z_1^2,\\ (z_1^q-z_1)z_2+z_2(z_1^q-z_1),\quad [z_1,z_2](z_3^q-z_3).\end{gathered}$$

Então $Id(UT_2(F),s)=J_s$. Além disso, o espaço vetorial quociente $F\langle Y\cup Z\rangle/Id(UT_2(F),s)$ tem uma base formada por todos polinômios da forma

$$\begin{cases} y_1^{s_1}\cdots y_n^{s_n}[z_j,z_i]z_i^{r_i}z_{i+1}^{r_{i+1}}\cdots z_m^{r_m}+J_s, & 0\le s_1,\ldots,s_n,r_i,\ldots,r_m<q,\\ & r_i,r_j<q-1, j>i,\ n\ge 1,\ m\ge 1;\\ y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m}+J_s, & 0\le s_1,\ldots,s_n<q,\\ & (r_1,\ldots,r_m)\in\Delta_m, n\ge 1,\ m\ge 1.\end{cases}$$

Demonstração. Denote $\widetilde{J}_s=Id(UT_2(F),s)$. Uma vez que $J_s\subseteq\widetilde{J}_s$, pela Proposição 3.2.17 o conjunto

$$\begin{cases} y_1^{s_1}\cdots y_n^{s_n}[z_j,z_i]z_i^{r_i}z_{i+1}^{r_{i+1}}\cdots z_m^{r_m}+\widetilde{J}_s, & 0\le s_1,\ldots,s_n,r_i,\ldots,r_m<q,\\ & r_i,r_j<q-1, j>i,\ n\ge 1,\ m\ge 1;\\ y_1^{s_1}\cdots y_n^{s_n}z_1^{r_1}\cdots z_m^{r_m}+\widetilde{J}_s, & 0\le s_1,\ldots,s_n<q,\\ & (r_1,\ldots,r_m)\in\Delta_m, n\ge 1,\ m\ge 1.\end{cases}$$

gera o espaço $F\langle Y\cup Z\rangle/\widetilde{J}_s$, e pelo Lema 3.2.20 é uma base.

Considere o conjunto Ω do enunciado do Lema 3.2.20. Então:

i) $\Omega_{J_s} = \{\omega + J_s |\ \omega \in \Omega\}$ gera $F\langle Y \cup Z\rangle / J_s$;

ii) $\Omega_{\widetilde{J}_s} = \{\omega + \widetilde{J}_s |\ \omega \in \Omega\}$ é base de $F\langle Y \cup Z\rangle / \widetilde{J}_s$.

Mostraremos que $\widetilde{J}_s \subseteq J_s$. Seja $f \in \widetilde{J}_s$. Por i) temos que

$$f + J_s = \sum_{w \in \Omega} \alpha_\omega \omega + J_s,\ \ \alpha_\omega \in F.$$

Uma vez que $J_s \subseteq \widetilde{J}_s$ temos

$$f + \widetilde{J}_s = \sum_{w \in \Omega} \alpha_\omega \omega + \widetilde{J}_s,\ \ \alpha_\omega \in F.$$

Como $f \in \widetilde{J}_s$, por ii) temos que $\alpha_\omega = 0$ para todo $w \in \Omega$. Logo, $f \in J_s$.

Finalizamos a demonstração. $\square$

Conclusão final. Pelo Corolário 2.3.1, temos

$$Id(UT_2(F), *) = Id(UT_2(F), \star) \quad \text{ou} \quad Id(UT_2(F), *) = Id(UT_2(F), s)$$

para toda involução de primeiro tipo $*$ de $UT_2(F)$. Agora usamos o Teorema 3.1.17 e Teorema 3.2.21 para descrever

$$Id(UT_2(F), *)$$

quando F é finito.

Capítulo 4

$*$-polinômios centrais para $UT_2(F)$

Ao longo deste capítulo, todas as involuções consideradas serão do primeiro tipo, e F será um corpo de $\mathrm{car}(F) \neq 2$. Descreveremos o conjunto dos $*$-polinômios centrais de $(UT_2(F), \circledast)$ para toda involução $\circledast$ e todo corpo F (finito ou infinito). Os resultados aqui obtidos são originais e fazem parte do trabalho realizado durante o doutorado.

4.1 $*$-polinômios centrais

Ao longo desta seção, todas as involuções consideradas serão do primeiro tipo e o corpo F será de $\mathrm{car}(F) \neq 2$. Pretendemos aqui dar as definições e resultados básicos que norteiam o assunto $*$-polinômios centrais. Sugerimos as referências [5, 20, 22] para um melhor entendimento.

Sejam $X = \{x_1, x_2, \ldots\}$ e $X^* = \{x_1^*, x_2^*, \ldots\}$ dois conjuntos infinitos enumeráveis e disjuntos. Denote por $F\langle X \cup X^* \rangle$ a álgebra associativa livre com unidade livremente gerada por $X \cup X^*$ e considere a involução $*$ adotada até agora.

Definição 4.1.1. *Seja $(A, \circledast)$ uma álgebra com involução. Um polinômio $f \in F\langle X \cup X^* \rangle$ é chamado $*$-polinômio central (ou polinômio central com involução) para $(A, \circledast)$ se*

$$\varphi(f) \in Z(A) \quad (\textit{centro de } A)$$

para todo homomorfismo com involução $\varphi : F\langle X \cup X^* \rangle \to A$. Denotamos por $C(A, \circledast)$ o conjunto de todos $*$-polinômios centrais de $(A, \circledast)$.

A demonstração do Lema 2.4.2 pode ser facilmente adaptada para provar o seguinte:

Lema 4.1.2. *Um polinômio $f(x_1, x_1^*, \ldots, x_n, x_n^*) \in F\langle X \cup X^* \rangle$ é um $*$-polinômio central para uma álgebra com involução $(A, \circledast)$ se, e somente se,*

$$f(a_1, a_1^{\circledast}, \ldots, a_n, a_n^{\circledast}) \in Z(A)$$

para todos $a_1, \ldots, a_n \in A$.

Por comodidade, e quando não houver confusão de notação, denotaremos uma involução qualquer sobre uma álgebra A por $*$.

Assim como no caso de $*$-identidades, no estudo de $*$-polinômios centrais é mais conveniente considerar a álgebra associativa livre $F\langle Y \cup Z \rangle$, onde

$$Y = \{y_1, y_2, \ldots\}, \ Z = \{z_1, z_2, \ldots\}, \ y_i = x_i + x_i^* \ \text{ e } \ z_i = x_i - x_i^*$$

para todo $i \geq 1$.

A demonstração do Lema 2.4.3 pode ser facilmente adaptada para provar o seguinte:

Lema 4.1.3. *Um polinômio $f(y_1,\ldots,y_n,z_1,\ldots,z_m)\in F\langle Y\cup Z\rangle$ é um $*$-polinômio central para uma álgebra com involução $(A,*)$ se, e somente se,*

$$f(a_1,\ldots,a_n,b_1,\ldots,b_m)\in Z(A)$$

para todos $a_1,\ldots,a_n\in A^+$ e $b_1,\ldots,b_m\in A^-$.

É fácil ver que

$$Id(A,*)\subseteq C(A,*)$$

para toda álgebra com involução $(A,*)$.

O conjunto $C(A,*)$ tem uma propriedade similar ao caso ordinário $C(A)$. Para descrevê-la, definiremos o conceito de $T(*)$-espaço.

Definição 4.1.4. *Um $T(*)$-espaço de $F\langle Y\cup Z\rangle$ é um subespaço vetorial de $F\langle Y\cup Z\rangle$ fechado por $*$-endomorfismos de $F\langle Y\cup Z\rangle$.*

A definição acima está dizendo que um subespaço H de $F\langle Y\cup Z\rangle$ é um $T(*)$-espaço se

$$\varphi(H)\subseteq H$$

para todo $*$-homomorfismo $\varphi: F\langle Y\cup Z\rangle\to F\langle Y\cup Z\rangle$. Olhando para a Definição 4.1.1 é fácil ver que $C(A,*)$ é um $T(*)$-espaço.

Note que um subespaço H de $F\langle Y\cup Z\rangle$ é um $T(*)$-espaço se, e somente se,

$$f(g_1,\ldots,g_n,h_1,\ldots,h_m)\in H$$

para todo $f(y_1,\ldots,y_n,z_1,\ldots,z_m)\in H$, $g_1,\ldots,g_n\in F\langle Y\cup Z\rangle^+$ e $h_1,\ldots,h_m\in F\langle Y\cup Z\rangle^-$.

Definição 4.1.5. *Seja W um subconjunto de $F\langle Y\cup Z\rangle$. Definimos o $T(*)$-*espaço gerado por *W como sendo a interseção de todos os $T(*)$-espaços que contêm W. Denotamos ele por*

$$\langle W\rangle^{TS(*)}.$$

Com base no parágrafo anterior a Definição 4.1.5, temos o seguinte resultado:

Lema 4.1.6. *Se W é um subconjunto de $F\langle Y\cup Z\rangle$, então $\langle W\rangle^{TS(*)}$ é gerado, como espaço vetorial, pelos elementos*

$$f(g_1,\ldots,g_n,h_1,\ldots,h_m)$$

onde $f(y_1,\ldots,y_n,z_1,\ldots,z_m)\in W$, $g_1,\ldots,g_n\in F\langle Y\cup Z\rangle^+$, $h_1,\ldots,h_m\in F\langle Y\cup Z\rangle^-$.

Dada uma álgebra com involução $(A,*)$, um dos problemas da área de PI-álgebra consiste em descrever os seus $*$-polinômios centrais. Mais especificamente, procura-se obter um conjunto gerador de $C(A,*)$ como $T(*)$-espaço.

Proposição 4.1.7. *Seja $f\in F\langle Y\cup Z\rangle$ e $w\in Y\cup Z$. Escreva*

$$f=\sum_{i=0}^{d_w} f^{(i)}$$

onde $f^{(i)}$ é a componente homogênea de f referente a variável w com grau $\deg_w f^{(i)}=i$. Se $d_w<|F|$ então

$$\langle f\rangle^{TS(*)}=\langle f^{(0)},f^{(1)},\ldots,f^{(d_w)}\rangle^{TS(*)}.$$

Demonstração. Argumentos similares a demonstração de [10, Proposição 4.2.3]. □

Proposição 4.1.8. *Seja H um $T(*)$-espaço de $F\langle Y \cup Z\rangle$.*

a) Se F é um corpo infinito, então H é gerado, como $T(*)$-espaço, por seus elementos multi-homogêneos.

b) Se F é um corpo de $car(F) = 0$, então H é gerado, como um $T(*)$-espaço, por seus elementos multilineares.

Demonstração. Para a demonstração, usamos a Proposição 4.1.7 e argumentos similares a demonstração de [10, Proposição 4.2.3]. □

4.2 $*$-polinômios centrais para $(UT_2(F), \star)$

Seja F um corpo de $\mathrm{car}(F) \neq 2$. Nesta seção, descreveremos os $*$-polinômios centrais de $(UT_2(F), \star)$. Relembramos que

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}^{\star} = \begin{pmatrix} b & c \\ 0 & a \end{pmatrix}$$

para todo $a, b, c \in F$. Usaremos os resultados da Seção 3.1 para este fim.

Lema 4.2.1. *Seja*

$$f(z_1, \ldots, z_m) = z_1 z_2 \cdots z_m$$

onde $m \geq 0$. Se m é par, então $f \in C(UT_2(F), \star)$. Se m é ímpar, então $f \notin C(UT_2(F), \star)$.

Demonstração. Suponha $m = 2n$ para algum $n \geq 0$. Se $Z_i = \lambda_i(e_{11} - e_{22})$, onde $\lambda_i \in F$, então

$$f(Z_1, \ldots, Z_{2n}) = (\lambda_1 \cdots \lambda_{2n})(e_{11} + e_{22}) \in Z(UT_2(F)).$$

Logo, $f \in C(UT_2(F), \star)$.

Suponha $m = 2n + 1$ para algum $n \geq 0$. Então

$$f(e_{11} - e_{22}, e_{11} - e_{22}, \ldots, e_{11} - e_{22}) = e_{11} - e_{22}.$$

Logo, $f \notin C(UT_2(F), \star)$. □

Proposição 4.2.2. *Seja*

$$g(y_1, \ldots, y_n, z_1, \ldots, z_m) = f(y_1, \ldots, y_n, z_1, \ldots, z_m) z_m$$

onde f é um polinômio homogêneo na variável z_m. Se $g \in C(UT_2(F), \star)$ então

$$g \in \left(Id(UT_2(F), \star) + \langle z_1 z_2\rangle^{TS(*)}\right).$$

Demonstração. Sejam $Y_1, \ldots, Y_n \in UT_2(F)^+$ e $Z_1, \ldots, Z_m \in UT_2(F)^-$. Então

$$f(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \quad \text{e} \quad Z_m = \begin{pmatrix} d & 0 \\ 0 & -d \end{pmatrix}$$

para alguns $a, b, c, d \in F$. Como $f(y_1, \ldots, y_n, z_1, \ldots, z_m) z_m \in C(UT_2(F), \star)$ obtemos

$$f(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) Z_m = \begin{pmatrix} ad & -cd \\ 0 & -bd \end{pmatrix} \in Z(UT_2(F)).$$

Assim $cd = 0$ e $ad = -bd$. Temos dois casos a analisar:

Caso 1. $\deg_{z_m} f = 0$.
Neste caso, $f(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) = f(Y_1, \ldots, Y_n, Z_1, \ldots, Z_{m-1})$. Se $d = 1$, então $a = -b$ e $c = 0$. Assim, $f(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) \in UT_2(F)^-$.

Caso 2. $\deg_{z_m} f \geq 1$.
Neste caso, se $d = 0$ então $f(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) = 0 \in UT_2(F)^-$. Se $d \neq 0$ então $a = -b$ e $c = 0$. Assim, $f(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) \in UT_2(F)^-$.

Pelos dois casos temos $f(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) \in UT_2(F)^-$ para todos $Y_1, \ldots, Y_n \in UT_2(F)^+$ e $Z_1, \ldots, Z_m \in UT_2(F)^-$. Pelo Lema 2.4.13 podemos escrever $f = f^+ + f^-$, onde $f^+ \in Id(UT_2(F), \star)$ e $f^- \in F\langle Y \cup Z\rangle^-$. Portanto,

$$f z_m = f^+ z_m + f^- z_m \in \left(Id(UT_2(F), \star) + \langle z_1 z_2\rangle^{TS(*)} \right).$$

A demonstração está completa. □

Lema 4.2.3. *Se $n \geq 1$, então*

$$z_1 \cdots z_{2n} \in \left(Id(UT_2(F), \star) + \langle z_1 z_2\rangle^{TS(*)} \right).$$

Demonstração. A demonstração é consequência direta do Lema 4.2.1 e Lema 4.2.2. □

4.2.1 $C(UT_2(F), \star)$ quando car$(F) = 0$

Nesta subseção descreveremos os $*$-polinômios centrais de $(UT_2(F), \star)$ quando car$(F) = 0$.

Teorema 4.2.4. *Seja F um corpo de car$(F) = 0$. O conjunto de todos os $*$-polinômios centrais de $(UT_2(F), \star)$ é*

$$C(UT_2(F), \star) = Id(UT_2(F), \star) + \langle z_1 z_2\rangle^{TS(*)} + F.$$

Demonstração. Denote $I = Id(UT_2(F), \star)$ e $C = C(UT_2(F), \star)$. Pelo Lema 4.2.1 temos

$$C \supseteq (I + \langle z_1 z_2\rangle^{TS(*)} + F).$$

Seja $f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in C$ um polinômio multilinear. Provaremos que $f \in (I + \langle z_1 z_2\rangle^{TS(*)} + F)$. Pelo Teorema 3.1.5 temos $f + I = \overline{f} + I$, onde

$$\overline{f} = \alpha y_1 \cdots y_n z_1 \cdots z_m + \sum_{k=1}^{n} \alpha_k y_1 \cdots \widehat{y_k} \cdots y_n z_1 \cdots z_{m-1} [z_m, y_k],$$

para alguns $\alpha, \alpha_k \in F$. Assim, existe $g \in I$ tal que $f = \overline{f} + g$. Em particular, $\overline{f} = (f - g) \in C$.

Caso 1. $n = 0$ e $m = 0$.
Neste caso, $\overline{f} = \alpha$ e portanto $f \in (F + I) \subset (I + \langle z_1 z_2\rangle^{TS(*)} + F)$.

Caso 2. $n = 0$ e $m > 0$.
Neste caso,

$$\overline{f} = \alpha z_1 \cdots z_m.$$

Pelo Lema 4.2.1 temos que $\alpha = 0$ ou m é par. Pelo Lema 4.2.3 obtemos $f \in (I + \langle z_1 z_2\rangle^{TS(*)} + F)$.

Caso 3. $n > 0$ e $m = 0$.
Neste caso,

$$\overline{f} = \alpha y_1 \cdots y_n.$$

Se $\alpha \neq 0$ então

$$\overline{f}(1, \ldots, 1, e_{12}) = \alpha e_{12}.$$

Assim $\overline{f} \notin C$ e temos uma contradição. Portanto $\alpha = 0$ e $f \in I \subset (I + \langle z_1 z_2\rangle^{TS(*)} + F)$.

Caso 4. $n > 0$ e $m = 1$.
Neste caso,

$$\overline{f} = \alpha y_1 \cdots y_n z_1 + \sum_{k=1}^{n} \alpha_k y_1 \cdots \widehat{y_k} \cdots y_n [z_1, y_k].$$

Como $\overline{f} \in C$ temos $\overline{f}(1, \ldots, 1, e_{11} - e_{22}) = \alpha(e_{11} - e_{22}) \in Z(UT_2(F))$. Assim $\alpha = 0$ e

$$\overline{f} = \sum_{k=1}^{n} \alpha_k y_1 \cdots \widehat{y_k} \cdots y_n [z_1, y_k].$$

Como $\overline{f} \in C$ temos $\overline{f}(1, \ldots, 1, e_{12}, 1, \ldots, 1, e_{11} - e_{22}) = 2\alpha_k e_{12} \in Z(UT_2(F))$. Assim, $\alpha_k = 0$ para todo $k = 1, \ldots, n$. Provamos que $f \in I \subset (I + \langle z_1 z_2\rangle^{TS(*)} + F)$.

Caso 5. $n > 0$ e $m \geq 2$.
Pelo Lema 3.1.7 temos $f + I = \overline{f} + I = \overline{\overline{f}} + I$, onde

$$\overline{\overline{f}} = \alpha y_1 \cdots y_n z_1 \cdots z_m - \sum_{k=1}^{n} \alpha_k y_1 \cdots \widehat{y_k} \cdots y_n z_1 \cdots z_{m-2} [z_{m-1}, y_k] z_m.$$

Como $I \subset C$ temos $\overline{\overline{f}} \in C$. Pela Proposição 4.2.2, obtemos $\overline{\overline{f}} \in (I + \langle z_1 z_2\rangle^{TS(*)})$. Assim, $f \in (I + \langle z_1 z_2\rangle^{TS(*)}) \subset (I + \langle z_1 z_2\rangle^{TS(*)} + F)$.

Pelos cinco casos e Proposição 4.1.8, temos

$$C = I + \langle z_1 z_2\rangle^{TS(*)} + F,$$

como era o desejado. □

Observação. Na demonstração do teorema, foi utilizado no Caso 5 o Lema 3.1.7. Chamamos a atenção do leitor para o fato que em tal lema a notação I denota o $T(*)$-ideal definido como em Definição 3.1.4. Como trata-se de um corpo F de car$(F) = 0$ temos que $I = Id(UT_2(F), \star)$, conforme Teorema 3.1.5.

4.2.2 $C(UT_2(F), \star)$ quando F é infinito de car$(F) > 2$

Nesta subseção descreveremos os $*$-polinômios centrais de $(UT_2(F), \star)$ quando F é infinito de car$(F) > 2$.

Começamos com a próxima proposição. Chamamos a atenção do leitor para o fato que: resultado similar aparece em [2, Teorema 6 do Capítulo 4] quando consideramos T-ideais da álgebra de Lee livre. Resultado similar também aparece no estudo de T-espaços da álgebra associativa livre.

Proposição 4.2.5. *Seja F um corpo infinito de $car(F) = p > 2$. Se H é um $T(*)$-espaço, então H é gerado, como um $T(*)$-espaço, por seus elementos multi-homogêneos $f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in H$ com multigrau*

$$(p^{a_1}, \ldots, p^{a_n}, p^{b_1}, \ldots, p^{b_m}),$$

onde $a_1, \ldots, a_n, b_1, \ldots, b_m \geq 0$.

Demonstração. Denote por H_M o conjunto de todos elementos multi-homogêneos de H, e por H_{PM} o conjunto de todos elementos multi-homogêneos $f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in H$ com multigrau $(p^{a_1}, \ldots, p^{a_n}, p^{b_1}, \ldots, p^{b_m})$ onde $a_1, \ldots, a_n, b_1, \ldots, b_m \geq 0$, $n \geq 0$ e $m \geq 0$.

Pela Proposição 4.1.8, segue que

$$H = \langle H_M \rangle^{TS(*)}.$$

Provaremos que $\langle H_M \rangle^{TS(*)} = \langle H_{PM} \rangle^{TS(*)}$. É óbvio que $\langle H_M \rangle^{TS(*)} \supseteq \langle H_{PM} \rangle^{TS(*)}$. Note que

$$\langle H_M \rangle^{TS(*)} \subseteq \langle H_{PM} \rangle^{TS(*)} \Leftrightarrow H_M \subseteq \langle H_{PM} \rangle^{TS(*)}. \tag{4.1}$$

Seja $g(y_1, \ldots, y_n, z_1, \ldots, z_m) \in H_M$.
a) Se $g \in H_{PM}$, então $g \in \langle H_{PM} \rangle^{TS(*)}$.
b) Suponha que $g \notin H_{PM}$. Denote por

$$d = (d_{y_1}, \ldots, d_{y_n}, d_{z_1}, \ldots, d_{z_m})$$

o multigrau de g. Sem perda de generalidade, podemos assumir que $\deg_{y_1} g = d_{y_1}$ não é uma potência de p. Seja $\deg_{y_1} g = p^k q$, onde $(p, q) = 1$. Denote por $\overline{g}(y_1, y_2, \ldots, y_n, y_{n+1}, z_1, \ldots, z_m)$ a componente multi-homogênea de

$$g(y_1 + y_{n+1}, y_2, \ldots, y_n, z_1, \ldots, z_m)$$

com multigrau

$$\overline{d} = (\overline{d}_{y_1}, \overline{d}_{y_2}, \ldots, \overline{d}_{y_n}, \overline{d}_{y_{n+1}}, \overline{d}_{z_1}, \ldots, \overline{d}_{z_m}) = (\overline{d}_{y_1}, d_{y_2}, \ldots, d_{y_n}, \overline{d}_{y_{n+1}}, d_{z_1}, \ldots, d_{z_m})$$

onde

$$\deg_{y_1} \overline{g} = \overline{d}_{y_1} = p^k \quad \text{e} \quad \deg_{y_{n+1}} \overline{g} = \overline{d}_{y_{n+1}} = p^k q - p^k.$$

Como F é um corpo infinito, temos $\overline{g} \in \langle g \rangle^{TS(*)}$. É conhecido que

$$\binom{p^k q}{p^k} = q \neq 0 \mod p.$$

Assim, como

$$\overline{g}(y_1, y_2, \ldots, y_n, y_1, z_1, \ldots, z_m) = \binom{p^k q}{p^k} g(y_1, \ldots, y_n, z_1, \ldots, z_m),$$

temos $g \in \langle \overline{g} \rangle^{TS(*)}$. Provamos que $\langle g \rangle^{TS(*)} = \langle \overline{g} \rangle^{TS(*)}$. Agora podemos usar o mesmo argumento em $\overline{g}$. Após alguns passos, teremos $\langle g \rangle^{TS(*)} = \langle h \rangle^{TS(*)}$ para algum $h \in H_{PM}$. Assim, $g \in \langle H_{PM} \rangle^{TS(*)}$. Provamos que $\langle H_M \rangle^{TS(*)} \subseteq \langle H_{PM} \rangle^{TS(*)}$, como era o desejado. $\square$

Lema 4.2.6. *Seja F um corpo infinito de $car(F) = p > 2$. Seja L o $T(*)$-espaço*

$$L = Id(UT_2(F), \star) + \langle z_1 z_2 \rangle^{TS(*)} + \langle y_1^p \rangle^{TS(*)}.$$

a) Então $L \subseteq C(UT_2(F), \star)$.

b) Sejam $a_1, \ldots, a_n \geq 1$. Se $f(y_1, \ldots, y_n)$ é um polinômio multi-homogêneo com multigrau $(p^{a_1}, \ldots, p^{a_n})$, então $f \in L$.

Demonstração. a) Seja $Y_1 \in UT_2(F)^+$. Assim, $Y_1 = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ para alguns $a, b \in F$. Se $i \geq 1$, então

$$Y_1^i = \begin{pmatrix} a^i & ia^{i-1}b \\ 0 & a^i \end{pmatrix}.$$

Portanto, $Y_1^p \in Z(UT_2(F))$ e $y_1^p \in C(UT_2(F), \star)$. Pelo Lema 4.2.1 temos

$$z_1 z_2 \in C(UT_2(F), \star).$$

Logo, $L \subseteq C(UT_2(F), \star)$.

b) Denote $I = Id(UT_2(F), \star)$. Pelo Teorema 3.1.5,

$$f + I = \alpha y_1^{p^{a_1}} y_2^{p^{a_2}} \cdots y_n^{p^{a_n}} + I$$

para algum $\alpha \in F$. Como $[y_i, y_j] \in I$ (veja Teorema 3.1.5), obtemos

$$\begin{aligned} f + I &= \alpha y_1^{p^{a_1}} \cdots y_n^{p^{a_n}} + I = \alpha \left(y_1^{p^{a_1 - 1}} \cdots y_n^{p^{a_n - 1}} \right)^p + I \\ &= \alpha \left(1/2 (y_1^{p^{a_1 - 1}} \cdots y_n^{p^{a_n - 1}} + y_n^{p^{a_n - 1}} \cdots y_1^{p^{a_1 - 1}}) \right)^p + I \\ &= \alpha g^p + I, \end{aligned}$$

onde $g = 1/2 (y_1^{p^{a_1 - 1}} \cdots y_n^{p^{a_n - 1}} + y_n^{p^{a_n - 1}} \cdots y_1^{p^{a_1 - 1}})$. Como g é um polinômio simétrico, temos $\alpha g^p \in \langle y_1^p \rangle^{TS(*)}$ e portanto $f \in (I + \langle y_1^p \rangle^{TS(*)}) \subseteq L$. A demonstração está completa. □

Teorema 4.2.7. *Seja F um corpo infinito de $car(F) = p > 2$. O conjunto de todos $*$-polinômios centrais de $(UT_2(F), \star)$ é*

$$C(UT_2(F), \star) = Id(UT_2(F), \star) + \langle z_1 z_2 \rangle^{TS(*)} + \langle y_1^p \rangle^{TS(*)}.$$

Demonstração. Denote $I = Id(UT_2(F), \star)$ e $C = C(UT_2(F), \star)$. Pelo Lema 4.2.6 temos

$$C \supseteq (I + \langle z_1 z_2 \rangle^{TS(*)} + \langle y_1^p \rangle^{TS(*)}).$$

Seja $f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in C$ um polinômio multi-homogêneo com multigrau

$$(p^{a_1}, \ldots, p^{a_n}, p^{b_1}, \ldots, p^{b_m})$$

onde $a_1, \ldots, a_n, b_1, \ldots, b_m \geq 0$. Provaremos que $f \in (I + \langle z_1 z_2 \rangle^{TS(*)} + \langle y_1^p \rangle^{TS(*)})$. Pelo Teorema 3.1.5 obtemos $f + I = \overline{f} + I$, onde

$$\begin{aligned} \overline{f} &= \sum_{k=1}^{n} \alpha_k y_1^{p^{a_1}} \cdots y_k^{p^{a_k} - 1} \cdots y_n^{p^{a_n}} z_1^{p^{b_1}} \cdots z_m^{p^{b_m} - 1} [z_m, y_k] + \\ &\quad + \alpha y_1^{p^{a_1}} \cdots y_n^{p^{a_n}} z_1^{p^{b_1}} \cdots z_m^{p^{b_m}} \end{aligned}$$

para alguns $\alpha_1,\ldots,\alpha_n,\alpha\in F$.

Caso 1. $n=0$ e $m=0$.
Neste caso, $f=\alpha$ e então

$$f\in F\subset \langle y_1^p\rangle^{TS(*)}\subset (I+\langle z_1z_2\rangle^{TS(*)}+\langle y_1^p\rangle^{TS(*)}).$$

Caso 2. $n\geq 1$ e $m=0$.
Neste caso,

$$\overline{f}=\alpha y_1^{p^{a_1}}\cdots y_n^{p^{a_n}}.$$

Se $a_i=0$ para algum i, então

$$\overline{f}=\alpha y_1^{p^{a_1}}\cdots y_i\cdots y_n^{p^{a_n}}$$

e $\overline{f}(1,\ldots,1,y_i,1,\ldots,1)=\alpha y_i\in C$. Assim $\alpha=0$, $\overline{f}=0$ e

$$f\in I\subset (I+\langle z_1z_2\rangle^{TS(*)}+\langle y_1^p\rangle^{TS(*)}).$$

Suponha $a_1,\ldots,a_n\geq 1$. Pelo Lema 4.2.6,

$$\overline{f}\in (I+\langle z_1z_2\rangle^{TS(*)}+\langle y_1^p\rangle^{TS(*)})$$

e portanto $f\in (I+\langle z_1z_2\rangle^{TS(*)}+\langle y_1^p\rangle^{TS(*)})$.

Caso 3. $m=1$ e $b_m=0$.
Neste caso,

$$\overline{f}=\sum_{k=1}^{n}\alpha_k y_1^{p^{a_1}}\cdots y_k^{p^{a_k}-1}\cdots y_n^{p^{a_n}}[z_1,y_k]+\alpha y_1^{p^{a_1}}\cdots y_n^{p^{a_n}}z_1.$$

Como $\overline{f}\in C$ temos $\overline{f}(1,\ldots,1,z_1)=\alpha z_1\in C$. Assim, $\alpha=0$ e

$$\overline{f}=\sum_{k=1}^{n}\alpha_k y_1^{p^{a_1}}\cdots y_k^{p^{a_k}-1}\cdots y_n^{p^{a_n}}[z_1,y_k].$$

Se $Y_1=\ldots=Y_{k-1}=Y_{k+1}=\ldots=Y_n=e_{11}+e_{22}$, $Y_k=e_{11}+e_{22}+e_{12}$ e $Z_1=e_{11}-e_{22}$, então

$$\overline{f}(Y_1,\ldots,Y_n,Z_1)=2\alpha_k e_{12}\in Z(UT_2(F)).$$

Assim, $\alpha_k=0$ para todo $k=1,\ldots,n$ e $\overline{f}=0$. Portanto

$$f\in I\subseteq (I+\langle z_1z_2\rangle^{TS(*)}+\langle y_1^p\rangle^{TS(*)}).$$

Caso 4. $m\geq 2$ e $b_m=0$.
Neste caso,

$$\begin{aligned}\overline{f} &= \sum_{k=1}^{n}\alpha_k y_1^{p^{a_1}}\cdots y_k^{p^{a_k}-1}\cdots y_n^{p^{a_n}}z_1^{p^{b_1}}\cdots z_{m-1}^{p^{b_{m-1}}}[z_m,y_k]+\\ &\quad +\alpha y_1^{p^{a_1}}\cdots y_n^{p^{a_n}}z_1^{p^{b_1}}\cdots z_{m-1}^{p^{b_{m-1}}}z_m.\end{aligned}$$

Pelo Lema 3.1.7 temos

$$z_{m-1}^{p^{b_{m-1}}}[z_m, y_k] + I = z_{m-1}^{p^{b_{m-1}}-1} z_m[z_{m-1}, y_k] + I = -z_{m-1}^{p^{b_{m-1}}-1}[z_{m-1}, y_k] z_m + I.$$

Assim, $\overline{f} + I = \widetilde{f} z_m + I$ onde

$$\begin{aligned} \widetilde{f} &= -\sum_{k=1}^{n} \alpha_k y_1^{p^{a_1}} \cdots y_k^{p^{a_k}-1} \cdots y_n^{p^{a_n}} z_1^{p^{b_1}} \cdots z_{m-1}^{p^{b_{m-1}}-1}[z_{m-1}, y_k] + \\ &+ \alpha y_1^{p^{a_1}} \cdots y_n^{p^{a_n}} z_1^{p^{b_1}} \cdots z_{m-1}^{p^{b_{m-1}}}. \end{aligned}$$

Como $\widetilde{f} z_m \in C$, pela Proposição 4.2.2 temos $\widetilde{f} z_m \in (I + \langle z_1 z_2 \rangle^{TS(*)} + \langle y_1^p \rangle^{TS(*)})$. Portanto

$$f \in (I + \langle z_1 z_2 \rangle^{TS(*)} + \langle y_1^p \rangle^{TS(*)}).$$

Caso 5. $m \geq 1$ e $b_m \geq 1$.
Pelo Lema 3.1.7,

$$z_m^{p^{b_m}-1}[z_m, y_k] + I = -z_m^{p^{b_m}-2}[z_m, y_k] z_m + I.$$

Assim, $\overline{f} + I = \widetilde{f} z_m + I$ onde

$$\begin{aligned} \widetilde{f} &= -\sum_{k=1}^{n} \alpha_k y_1^{p^{a_1}} \cdots y_k^{p^{a_k}-1} \cdots y_n^{p^{a_n}} z_1^{p^{b_1}} \cdots z_m^{p^{b_m}-2}[z_m, y_k] + \\ &+ \alpha y_1^{p^{a_1}} \cdots y_n^{p^{a_n}} z_1^{p^{b_1}} \cdots z_m^{p^{b_m}-1}. \end{aligned}$$

Como $\widetilde{f} z_m \in C$, pela Proposição 4.2.2 temos

$$\widetilde{f} z_m \in (I + \langle z_1 z_2 \rangle^{TS(*)} + \langle y_1^p \rangle^{TS(*)}).$$

Portanto $f \in (I + \langle z_1 z_2 \rangle^{TS(*)} + \langle y_1^p \rangle^{TS(*)})$.
Pelos cinco casos, segue que

$$C \subseteq (I + \langle z_1 z_2 \rangle^{TS(*)} + \langle y_1^p \rangle^{TS(*)})$$

como era o desejado. A demonstração está completa. □

4.2.3 $C(UT_2(F), \star)$ quando F é um corpo finito

Nesta subseção descreveremos os $*$-polinômios centrais de $(UT_2(F), \star)$ quando F é um corpo finito com q elementos e $\mathrm{car}(F) = p \neq 2$. Fixaremos tal corpo ao longo de toda esta subseção.

Pelo Lema 3.1.2, se

$$y = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

então

$$y^i = \begin{pmatrix} a^i & ia^{i-1}b \\ 0 & a^i \end{pmatrix}, \quad y^q = \begin{pmatrix} a^q & qa^{q-1}b \\ 0 & a^q \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \tag{4.2}$$

para todos $a, b \in F$ e $i \geq 1$.

Proposição 4.2.8. *Seja F um corpo finito com q elementos. Então*

$$ly_1(y_2^{q+l-1} - y_2^l) + y_1^q y_2^l$$

é um $*$-polinômio central de $(UT_2(F), \star)$ para todo inteiro $l \geq 0$.

Demonstração. Denote $f(y_1, y_2) = ly_1(y_2^{q+l-1} - y_2^l) + y_1^q y_2^l$ e considere

$$Y_i = \begin{pmatrix} a_i & b_i \\ 0 & a_i \end{pmatrix},$$

onde $a_i, b_i \in F$, $i = 1, 2$. Por (4.2) temos

$$Y_2^l = \begin{pmatrix} a_2^l & la_2^{l-1}b_2 \\ 0 & a_2^l \end{pmatrix} \text{ e } Y_2^{q+l-1} = \begin{pmatrix} a_2^l & (l-1)a_2^{l-1}b_2 \\ 0 & a_2^l \end{pmatrix}.$$

Logo,

$$Y_2^{q+l-1} - Y_2^l = \begin{pmatrix} 0 & -a_2^{l-1}b_2 \\ 0 & 0 \end{pmatrix} \text{ e } lY_1(Y_2^{q+l-1} - Y_2^l) = \begin{pmatrix} 0 & -la_1a_2^{l-1}b_2 \\ 0 & 0 \end{pmatrix}.$$

Por (4.2) temos

$$Y_1^q Y_2^l = \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a_2^l & la_2^{l-1}b_2 \\ 0 & a_2^l \end{pmatrix} = \begin{pmatrix} a_1a_2^l & la_1a_2^{l-1}b_2 \\ 0 & a_1a_2^l \end{pmatrix}.$$

Portanto

$$f(Y_1, Y_2) = \begin{pmatrix} a_1a_2^l & 0 \\ 0 & a_1a_2^l \end{pmatrix} \in Z(UT_2(F))$$

como era o desejado. A demonstração está completa. □

Denote por V o $T(*)$-espaço gerado pelos elementos da última proposição:

$$V = \left\langle ly_1(y_2^{q+l-1} - y_2^l) + y_1^q y_2^l : \ l \geq 0 \right\rangle^{TS(*)}.$$

Pela Proposição 4.2.8, obtemos

$$V + Id(UT_2(F), \star) \subseteq C(UT_2(F), \star).$$

No início desta subseção usamos a notação $\text{car}(F) = p \neq 2$ para denotar a característica de F. Assim, se $l = kp$ e $y_1 = 1$ então $ly_1(y_2^{q+l-1} - y_2^l) + y_1^q y_2^l = y_2^{kp}$. Portanto

$$y_2^{kp} \in V \tag{4.3}$$

Para todo $k \geq 0$.

De agora em diante escreveremos

$$f \equiv g \iff f + V + Id(UT_2(F), \star) = g + V + Id(UT_2(F), \star).$$

Lema 4.2.9. *Seja F um corpo finito com q elementos. Se $l, n \geq 0$ então*

$$\left(ly_1 \cdots y_n(y_{n+1}^{q+l-1} - y_{n+1}^l) + y_1^q \cdots y_n^q y_{n+1}^l\right) \equiv 0.$$

Demonstração. O caso $n = 0$ é consequência da Proposição 4.2.8. De fato, substituindo em

$$ly_1(y_2^{q+l-1} - y_2^l) + y_1^q y_2^l$$

a variável y_1 por 1, teremos $l(y_2^{q+l-1} - y_2^l) + y_2^l \equiv 0$.

Suponha $n \geq 1$. Denote $u = (1/2)(y_1 y_2 \cdots y_n + y_n \cdots y_2 y_1)$ e $J = Id(UT_2(F), \star)$. Como u é um polinômio simétrico, segue que

$$v = lu(y_{n+1}^{q+l-1} - y_{n+1}^l) + u^q y_{n+1}^l \in V. \tag{4.4}$$

Como $[y_i, y_j] \in J$ (veja Teorema 3.1.17), temos

$$y_i y_j + J = y_j y_i + J.$$

Assim $u + J = y_1 \cdots y_n + J$ e $u^q + J = y_1^q \cdots y_n^q + J$. Portanto

$$v + J = ly_1 \cdots y_n(y_{n+1}^{q+l-1} - y_{n+1}^l) + y_1^q \cdots y_n^q y_{n+1}^l + J.$$

Agora usamos (4.4) para finalizar a demonstração. □

Corolário 4.2.10. *Seja F um corpo finito com q elementos e car$(F) = p$. Se $f(y_1, \ldots, y_n) \in F\langle Y \cup Z\rangle$ e $p \nmid l$, então existe $g(y_1, \ldots, y_n) \in F\langle Y \cup Z\rangle$ tal que*

$$fy_{n+1}^{q+l-1} \equiv gy_{n+1}^l.$$

Demonstração. Pelo Lema 4.2.9 temos

$$y_1 \cdots y_n y_{n+1}^{q+l-1} \equiv (y_1 \cdots y_n - (l^{-1}) y_1^q \cdots y_n^q) y_{n+1}^l.$$

Como fy_{n+1}^{q+l-1} é uma combinação linear de polinômios

$$y_{i_1} \cdots y_{i_m} y_{n+1}^{q+l-1},$$

finalizamos a demonstração. □

Proposição 4.2.11. *Seja F um corpo finito com q elementos e car$(F) = p$. Considere*

$$f = \sum_{i=0}^{2q-1} \alpha_i y_1^i,$$

onde $\alpha_i \in F$ para todo i. Se $f \in C(UT_2(F), \star)$ então $f \equiv 0$.

Demonstração. Seja g dado por

$$g = \sum_{i=q}^{2q-1} \alpha_i y_1^i = \sum_{i=1}^{q} \alpha_{q+i-1} y_1^{q+i-1} = \sum_{\substack{i=1 \\ p|i}}^{q} \alpha_{q+i-1} y_1^{q+i-1} + \sum_{\substack{i=1 \\ p\nmid i}}^{q} \alpha_{q+i-1} y_1^{q+i-1}.$$

Pelo Corolário 4.2.10 temos

$$g \equiv \sum_{\substack{i=1 \\ p|i}}^{q} \alpha_{q+i-1} y_1^{q+i-1} + \sum_{\substack{i=1 \\ p\nmid i}}^{q} \beta_i y_1^i,$$

para alguns $\beta_i \in F$. Assim, existem $\gamma_i \in F$ tais que

$$f \equiv \sum_{\substack{i=1\\ p|i}}^{q} \alpha_{q+i-1} y_1^{q+i-1} + \sum_{i=0}^{q-1} \gamma_i y_1^i.$$

Por (4.3) obtemos

$$f \equiv \underbrace{\sum_{\substack{i=1\\ p|i}}^{q} \alpha_{q+i-1} y_1^{q+i-1} + \sum_{\substack{i=1\\ p\nmid i}}^{q-1} \gamma_i y_1^i}_{h}. \tag{4.5}$$

Segue da Proposição 4.2.8 que

$$C(UT_2(F),\star) \supseteq V + Id(UT_2(F),\star). \tag{4.6}$$

Como $f \in C(UT_2(F),\star)$, por (4.5) e (4.6) temos que $h \in C(UT_2(F),\star)$, onde

$$h = \sum_{\substack{i=1\\ p|i}}^{q} \alpha_{q+i-1} y_1^{q+i-1} + \sum_{\substack{i=1\\ p\nmid i}}^{q-1} \gamma_i y_1^i.$$

Se $a \in F$ e

$$Y_1 = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix},$$

então por (4.2),

$$h(Y_1) = \begin{pmatrix} h(a) & \left[\sum_{\substack{i=1\\ p|i}}^{q} \alpha_{q+i-1}(-1)a^{i-1} + \sum_{\substack{i=1\\ p\nmid i}}^{q-1} \gamma_i i a^{i-1} \right] \\ 0 & h(a) \end{pmatrix}.$$

Como $h(Y_1) \in Z(UT_2(F))$, segue que

$$\sum_{\substack{i=1\\ p|i}}^{q} \alpha_{q+i-1}(-1)a^{i-1} + \sum_{\substack{i=1\\ p\nmid i}}^{q-1} \gamma_i i a^{i-1} = 0$$

para todo $a \in F$. Pelo Lema 2.1.3 temos

$$\begin{cases} \alpha_{q+i-1}(-1) = 0, & 1 \le i \le q, \quad p \mid i\ ; \\ \gamma_i i = 0, & 1 \le i \le q-1, \quad p \nmid i. \end{cases}$$

Assim, $h = 0$ e $f \equiv 0$ como era o desejado. □

Lema 4.2.12. *Seja F um corpo finito com q elementos e car$(F) = p$. Então $y_1^{pq} - y_1^p \in Id(UT_2(F),\star)$.*

Demonstração. Se $a, b \in F$ e $Y_1 = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, então por (4.2),

$$Y_1^{pq} = (Y_1^q)^p = \begin{pmatrix} a^p & 0 \\ 0 & a^p \end{pmatrix} = Y_1^p.$$

Assim, $Y_1^{pq} - Y_1^p = 0$ como era o desejado. □

Lema 4.2.13. *Seja F um corpo finito com q elementos e car$(F) = p$. Se $i \geq 0$, então*

$$\left(iy_1(y_2^{q+i-1} - y_2^i) + y_1^q y_2^i\right) y_3^p \equiv 0.$$

Demonstração. Denote $u = (1/2)(y_1 y_3^p + y_3^p y_1)$ e $J = Id(UT_2(F), \star)$. Como u é um polinômio simétrico, temos

$$iu(y_2^{q+i-1} - y_2^i) + u^q y_2^i \in V. \tag{4.7}$$

Como $y_i y_j + J = y_j y_i + J$, segue que

$$u + J = y_1 y_3^p + J. \tag{4.8}$$

Assim, pelo Lema 4.2.12,

$$u^q + J = y_1^q y_3^{pq} + J = y_1^q y_3^p + J. \tag{4.9}$$

Agora usamos (4.8) e (4.9) para obter

$$\begin{aligned} iu(y_2^{q+i-1} - y_2^i) + u^q y_2^i + J &= iy_1 y_3^p (y_2^{q+i-1} - y_2^i) + y_1^q y_3^p y_2^i + J \\ &= iy_1(y_2^{q+i-1} - y_2^i) y_3^p + y_1^q y_2^i y_3^p + J \\ &= \left(iy_1(y_2^{q+i-1} - y_2^i) + y_1^q y_2^i\right) y_3^p + J. \end{aligned} \tag{4.10}$$

Por (4.7) e (4.10) segue que $\left(iy_1(y_2^{q+i-1} - y_2^i) + y_1^q y_2^i\right) y_3^p \equiv 0$, como era o desejado. $\square$

Corolário 4.2.14. *Seja F um corpo finito com q elementos e car$(F) = p$. Se*

$$f(y_1, \ldots, y_n) \equiv 0,$$

então $f(y_1, \ldots, y_n) y_{n+1}^{lp} \equiv 0$ para todo $l \geq 0$.

Demonstração. Escreva $f = f_V + f_I$, onde $f_V \in V$ e $f_I \in Id(UT_2(F), \star)$. Como

$$f y_{n+1}^{lp} = f_V y_{n+1}^{lp} + f_I y_{n+1}^{lp} \equiv f_V y_{n+1}^{lp},$$

podemos supor $f(y_1, \ldots, y_n) \in V$. Neste caso, f é uma combinação linear de polinômios

$$ig_1(g_2^{q+i-1} - g_2^i) + g_1^q g_2^i,$$

onde $g_1, g_2 \in F\langle Y \cup Z \rangle^+$ e $i \geq 0$. Pelo Lema 4.2.13 temos

$$\left(ig_1(g_2^{q+i-1} - g_2^i) + g_1^q g_2^i\right) y_{n+1}^p \equiv 0.$$

Assim, $f(y_1, \ldots, y_n) y_{n+1}^p \equiv 0$. Como $V + Id(UT_2(F), \star)$ é um $T(*)$-espaço temos

$$f(y_1, \ldots, y_n) y_{n+1}^{lp} = f(y_1, \ldots, y_n)(y_{n+1}^l)^p \equiv 0$$

para todo $l \geq 0$. $\square$

Proposição 4.2.15. *Seja F um corpo finito com q elementos e car$(F) = p$. Se*

$$f(y_1, \ldots, y_n) \in C(UT_2(F), \star),$$

então $f(y_1, \ldots, y_n) \equiv 0$.

Demonstração. Pelo Teorema 3.1.17, podemos supor

$$f = \sum_{s\in\Lambda_n} \alpha_s y_1^{s_1} \cdots y_n^{s_n},$$

onde $s = (s_1, \ldots, s_n)$, $\alpha_s \in F$.

Provaremos a proposição usando indução em n.

O caso $n = 1$ é consequência da Proposição 4.2.11.

Suponha $n \geq 2$. Escreva

$$f = \sum_{i=0}^{2q-1} f_i y_n^i.$$

Note que:

a) Se $0 \leq i \leq q-1$, então

$$f_i = \sum_{(s_1,\ldots,s_{n-1})\in\Lambda_{n-1}} \alpha_{(s_1,\ldots,s_{n-1},i)} y_1^{s_1} \cdots y_{n-1}^{s_{n-1}}.$$

b) Se $q \leq i \leq 2q-1$, então

$$f_i = \sum_{s_1,\ldots,s_{n-1}=0}^{q-1} \alpha_{(s_1,\ldots,s_{n-1},i)} y_1^{s_1} \cdots y_{n-1}^{s_{n-1}}. \tag{4.11}$$

Escreva

$$g = \sum_{i=q}^{2q-1} f_i y_n^i = \sum_{i=1}^{q} f_{q+i-1} y_n^{q+i-1} = \sum_{\substack{i=1\\ p\mid i}}^{q} f_{q+i-1} y_n^{q+i-1} + \sum_{\substack{i=1\\ p\nmid i}}^{q} f_{q+i-1} y_n^{q+i-1}.$$

Pelo Corolário 4.2.10, existem polinômios $g_i(y_1, \ldots, y_{n-1})$ tais que

$$g \equiv \sum_{\substack{i=1\\ p\mid i}}^{q} f_{q+i-1} y_n^{q+i-1} + \sum_{\substack{i=1\\ p\nmid i}}^{q} g_i y_n^i.$$

Assim, existem polinômios $h_i(y_1, \ldots, y_{n-1})$ tais que

$$f \equiv \underbrace{\sum_{\substack{i=1\\ p\mid i}}^{q} f_{q+i-1} y_n^{q+i-1} + \sum_{i=0}^{q-1} h_i y_n^i}_{h}. \tag{4.12}$$

Denote

$$h(y_1, \ldots, y_n) = \sum_{\substack{i=1\\ p\mid i}}^{q} f_{q+i-1} y_n^{q+i-1} + \sum_{i=0}^{q-1} h_i y_n^i.$$

Como $f \in C(UT_2(F,\star))$ e $V + Id(UT_2(F,\star)) \subseteq C(UT_2(F,\star))$, temos por (4.12) que $h \in C(UT_2(F,\star))$.

Considere as seguintes matrizes:

$$Y_n = \begin{pmatrix} a_n & 1 \\ 0 & a_n \end{pmatrix} \text{ e } Y_k = \begin{pmatrix} a_k & 0 \\ 0 & a_k \end{pmatrix} \ (k \neq n)$$

onde $a_j \in F$ para todo j. Por (4.2) temos

$$Y_n^i = \begin{pmatrix} a_n^i & ia_n^{i-1} \\ 0 & a_n^i \end{pmatrix}.$$

Em particular, se $p|i$ então

$$Y_n^{q+i-1} = \begin{pmatrix} a_n^i & -a_n^{i-1} \\ 0 & a_n^i \end{pmatrix}.$$

Portanto

$$h(Y_1, \ldots, Y_n) = \begin{pmatrix} h(a_1, \ldots, a_n) & \overline{h}(a_1, \ldots, a_n) \\ 0 & h(a_1, \ldots, a_n) \end{pmatrix},$$

onde

$$\begin{aligned} \overline{h}(a_1, \ldots, a_n) &= \sum_{\substack{i=1 \\ p|i}}^{q} f_{q+i-1}(a_1, \ldots, a_{n-1})(-1)a_n^{i-1} + \sum_{i=0}^{q-1} h_i(a_1, \ldots, a_{n-1}) i a_n^{i-1} \\ &= \sum_{\substack{i=1 \\ p|i}}^{q} f_{q+i-1}(a_1, \ldots, a_{n-1})(-1)a_n^{i-1} + \sum_{\substack{i=1 \\ p\nmid i}}^{q-1} h_i(a_1, \ldots, a_{n-1}) i a_n^{i-1}. \end{aligned}$$

Como $h(Y_1, \ldots, Y_n) \in Z(UT_2(F))$, obtemos $\overline{h}(a_1, \ldots, a_n) = 0$ para todos $a_1, \ldots, a_n \in F$. Pelo Lemma 2.1.3 segue que

$$f_{q+i-1}(a_1, \ldots, a_{n-1}) = 0 \tag{4.13}$$

para todo $i = 1, \ldots, q$ onde $p|i$; e

$$h_i(a_1, \ldots, a_{n-1}) = 0 \tag{4.14}$$

para todo $i = 1, \ldots, q-1$ onde $p \nmid i$.

Por (4.11), (4.13) e Lema 2.1.3, temos $f_{q+i-1}(y_1, \ldots, y_{n-1}) = 0$ para todo $i = 1, \ldots, q$ onde $p|i$. Assim,

$$h(y_1, \ldots, y_n) = \sum_{i=0}^{q-1} h_i y_n^i. \tag{4.15}$$

Como $h \in C(UT_2(F), \star)$, pela Proposição 4.1.7 segue que $h_i y_n^i \in C(UT_2(F), \star)$ para todo $i = 0, \ldots, q-1$. Substituindo em $h_i y_n^i$ a variável y_n por 1, segue que

$$h_i \in C(UT_2(F), \star)$$

para todo $i = 0, \ldots, q-1$. Temos dois casos:

a) Caso $p \nmid i$.
Considere

$$Y_k = \begin{pmatrix} a_k & b_k \\ 0 & a_k \end{pmatrix},$$

onde $a_k, b_k \in F$ e $k = 1, \ldots, n-1$. Temos

$$h_i(Y_1, \ldots, Y_{n-1}) = \begin{pmatrix} h_i(a_1, \ldots, a_{n-1}) & \beta \\ 0 & h_i(a_1, \ldots, a_{n-1}) \end{pmatrix}$$

para algum $\beta \in F$. Como $h_i \in C(UT_2(F,\star))$, segue que $\beta = 0$. Por (4.14) temos $h_i(a_1,\ldots,a_{n-1}) = 0$ também. Assim, $h_i(Y_1,\ldots,Y_{n-1}) = 0$ e $h_i(y_1,\ldots,y_{n-1}) \in Id(UT_2(F),\star)$ para todo $i = 0,\ldots,q-1$ onde $p \nmid i$.

b) Caso $p|i$.

Como $h_i(y_1,\ldots,y_{n-1}) \in C(UT_2(F),\star)$ obtemos, por indução, que $h_i \equiv 0$. Assim, pelo Corolário 4.2.14, segue que $h_i y_n^i \equiv 0$ para todo $i = 0,\ldots,q-1$ onde $p|i$.

Por (4.12), (4.15) e os dois casos acima, temos

$$f \equiv h \equiv 0,$$

como era o desejado. □

Teorema 4.2.16. *Seja F um corpo finito com q elementos e car$(F) = p$. Então*

$$C(UT_2(F),\star) = \left\langle l y_1(y_2^{q+l-1} - y_2^l) + y_1^q y_2^l : \ 1 \le l \le p \right\rangle^{TS(*)} + \langle z_1 z_2\rangle^{TS(*)} + Id(UT_2(F),\star).$$

Demonstração. Primeiro provaremos a seguinte afirmação:

Afirmação 1. O conjunto $C(UT_2(F),\star)$ é igual a

$$C(UT_2(F),\star) = \left\langle l y_1(y_2^{q+l-1} - y_2^l) + y_1^q y_2^l : \ l \ge 0 \right\rangle^{TS(*)} + \langle z_1 z_2\rangle^{TS(*)} + Id(UT_2(F),\star).$$

Demonstração da Afirmação 1. Denote $J = Id(UT_2(F),\star)$ e

$$V = \left\langle l y_1(y_2^{q+l-1} - y_2^l) + y_1^q y_2^l : \ l \ge 0 \right\rangle^{TS(*)}.$$

Como $z_1 z_2 \in C(UT_2(F),\star)$ temos $C(UT_2(F),\star) \supseteq \langle z_1 z_2\rangle^{TS(*)}$. Portanto, pela Proposição 4.2.8, obtemos

$$C(UT_2(F),\star) \supseteq \left(V + \langle z_1 z_2\rangle^{TS(*)} + J\right). \tag{4.16}$$

Considere $f \in C(UT_2(F),\star)$. Provaremos que $f \in \left(V + \langle z_1 z_2\rangle^{TS(*)} + J\right)$. Pelo Teorema 3.1.17, $f = f_J + f_\Upsilon$ onde $f_J \in J$ e f_Υ é uma combinação linear de polinômios

$$\begin{cases} y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m-1}[z_m, y_k], & 0 \le s_1,\ldots,s_n, r_1,\ldots,r_m < q, \quad r_m \ge 1, \\ & n \ge 1,\ m \ge 1,\ k \ge 1; \hfill (\Upsilon_1) \\ y_1^{s_1}\cdots y_n^{s_n} z_1^{r_1}\cdots z_m^{r_m}, & 0 \le s_1,\ldots,s_n, r_1,\ldots,r_m < q, \quad r_m \ge 1, \\ & n \ge 1,\ m \ge 1; \hfill (\Upsilon_2) \\ y_1^{s_1}\cdots y_n^{s_n}, & (s_1,\ldots,s_n) \in \Lambda_n, \quad n \ge 1. \hfill (\Upsilon_3) \end{cases}$$

Como $f_J \in J$, temos

$$f \in \left(V + \langle z_1 z_2\rangle^{TS(*)} + J\right) \Leftrightarrow f_\Upsilon \in \left(V + \langle z_1 z_2\rangle^{TS(*)} + J\right).$$

Assim, podemos supor $f = f_\Upsilon$. Como $\deg_{z_i} f < q$, podemos supor f um polinômio homogêneo em cada variável z_i para todo $i = 1,\ldots,m$ (veja Proposição 4.1.7). Denote $\deg_{z_i} f = r_i$.

Se $r_1 = \ldots = r_m = 0$, então pela Proposição 4.2.15

$$f \in \left(V + \langle z_1 z_2\rangle^{TS(*)} + J\right).$$

Suponha $r_i \neq 0$ para algum i. Renumerando os índices, se necessário, podemos assumir que $r_i \geq 1$ para todo $i = 1, \ldots, m$. Como f é uma combinação linear de polinômios em Υ_1 e Υ_2 temos $f = f_1 + f_2$, onde

$$f_1 = f_1(y_1, y_2, \ldots, z_1, z_2, \ldots) = \sum_{n,k,s} \alpha_{(n,k,s)} y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m - 1} [z_m, y_k]$$

com $0 \leq s_1, \ldots, s_n < q$, $\quad 1 \leq r_1, \ldots, r_m < q$, $\quad n \geq 1$, $\quad m \geq 1$, $\quad k \geq 1$, $\quad s = (s_1, \ldots, s_n)$, $\alpha_{(n,k,s)} \in F$; e

$$f_2 = f_2(y_1, y_2, \ldots, z_1, z_2, \ldots) = \sum_{n,s} \beta_{(n,s)} y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m}$$

com $0 \leq s_1, \ldots, s_n < q$, $\quad 1 \leq r_1, \ldots, r_m < q$, $\quad n \geq 1$, $\quad m \geq 1$, $\quad s = (s_1, \ldots, s_n)$, $\quad \beta_{(n,s)} \in F$.

Temos 3 casos:

Caso 1. $m = 1$ e $r_m = 1$.

Neste caso, $f = f_1 + f_2$ onde

$$f_1 = f_1(y_1, y_2, \ldots, z_1) = \sum_{n,k,s} \alpha_{(n,k,s)} y_1^{s_1} \cdots y_n^{s_n} [z_1, y_k]$$

e

$$f_2 = f_2(y_1, y_2, \ldots, z_1) = \sum_{n,s} \beta_{(n,s)} y_1^{s_1} \cdots y_n^{s_n} z_1.$$

Seja

$$Y_i = \begin{pmatrix} a_i & 0 \\ 0 & a_i \end{pmatrix} \quad \text{e} \quad Z_i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

onde $a_i \in F$. Temos

$$f(Y_1, Y_2, \ldots, Z_1) = \begin{pmatrix} \displaystyle\sum_{n,s} \beta_{(n,s)} a_1^{s_1} \cdots a_n^{s_n} & \theta \\ 0 & \displaystyle -\sum_{n,s} \beta_{(n,s)} a_1^{s_1} \cdots a_n^{s_n} \end{pmatrix}$$

onde $\theta \in F$. Como $f(Y_1, Y_2, \ldots, Z_1) \in Z(UT_2(F))$, segue que $\theta = 0$ e

$$\sum_{n,s} \beta_{(n,s)} a_1^{s_1} \cdots a_n^{s_n} = 0$$

para todos $a_1, \ldots, a_n \in F$. Como $0 \leq s_1, \ldots, s_n < q$ temos, pelo Lema 2.1.3, que $\beta_{(n,s)} = 0$ para todos n, s. Assim, $f = f_1$. Se $\overline{Y}_1, \overline{Y}_2, \ldots \in UT_2(F)^+$ e $\overline{Z}_1 \in UT_2(F)^-$ então

$$f(\overline{Y}_1, \overline{Y}_2, \ldots, \overline{Z}_1) = f_1(\overline{Y}_1, \overline{Y}_2, \ldots, \overline{Z}_1) = \alpha e_{12}$$

para algum $\alpha \in F$. Como $f(\overline{Y}_1, \overline{Y}_2, \ldots, \overline{Z}_1) \in Z(UT_2(F))$ obtemos $\alpha = 0$, isto é, $f \in J$. Portanto, $f \in \Big(V + \langle z_1 z_2 \rangle^{TS(*)} + J\Big)$.

Caso 2. $m \geq 2$ e $r_m = 1$.

Neste caso, $f = f_1 + f_2$ onde

$$f_1 = f_1(y_1, y_2, \ldots, z_1, z_2, \ldots) = \sum_{n,k,s} \alpha_{(n,k,s)} y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_{m-1}^{r_{m-1}} [z_m, y_k]$$

e

$$f_2 = f_2(y_1, y_2, \ldots, z_1, z_2, \ldots) = \sum_{n,s} \beta_{(n,s)} y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_{m-1}^{r_{m-1}} z_m.$$

Pelo Lema 3.1.7 temos

$$z_{m-1}^{r_{m-1}}[z_m, y_k] + J = z_{m-1}^{r_{m-1}-1} z_m [z_{m-1}, y_k] + J = -z_{m-1}^{r_{m-1}-1}[z_{m-1}, y_k] z_m + J.$$

Assim, $f + J = \widetilde{f} z_m + J$ onde

$$\begin{aligned} \widetilde{f} &= -\sum_{n,k,s} \alpha_{(n,k,s)} y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_{m-1}^{r_{m-1}-1}[z_{m-1}, y_k] + \\ &\quad + \sum_{n,s} \beta_{(n,s)} y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_{m-1}^{r_{m-1}}. \end{aligned}$$

Como $\widetilde{f} z_m \in C(UT_2(F), \star)$ temos, pela Proposição 4.2.2, que $\widetilde{f} z_m \in (\langle z_1 z_2 \rangle^{TS(*)} + J)$. Portanto

$$f \in \left(V + \langle z_1 z_2 \rangle^{TS(*)} + J\right).$$

Caso 3. $m \geq 1$ e $r_m \geq 2$.
Pelo Lema 3.1.7 temos

$$z_m^{r_m - 1}[z_m, y_k] + J = -z_m^{r_m - 2}[z_m, y_k] z_m + J.$$

Assim, $f + J = \widetilde{f} z_m + J$ onde

$$\begin{aligned} \widetilde{f} &= -\sum_{n,k,s} \alpha_{(n,k,s)} y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m-2}[z_m, y_k] \\ &\quad + \sum_{n,s} \beta_{(n,s)} y_1^{s_1} \cdots y_n^{s_n} z_1^{r_1} \cdots z_m^{r_m-1}. \end{aligned}$$

Como $\widetilde{f} z_m \in C(UT_2(F), \star)$ temos, pela Proposição 4.2.2, que $\widetilde{f} z_m \in (\langle z_1 z_2 \rangle^{TS(*)} + J)$. Portanto

$$f \in \left(V + \langle z_1 z_2 \rangle^{TS(*)} + J\right).$$

Nós provamos que

$$C(UT_2(F), \star) \subseteq \left(V + \langle z_1 z_2 \rangle^{TS(*)} + J\right).$$

Por (4.16) finalizamos a demonstração da Afirmação 1.

Afirmação 2. Se $l \geq 0$, então

$$l y_1 (y_2^{q+l-1} - y_2^l) + y_1^q y_2^l \in \left\langle r y_1 (y_2^{q+r-1} - y_2^r) + y_1^q y_2^r : 1 \leq r \leq p \right\rangle^{TS(*)} + J.$$

Demonstração da Afirmação 2. Se $l \geq 0$, sejam k, r inteiros tais que $l = kp + r$ and $0 \leq r < p$. Temos

$$l y_1 (y_2^{q+l-1} - y_2^l) + y_1^q y_2^l = r y_1 y_2^{kp} (y_2^{q+r-1} - y_2^r) + y_1^q y_2^{kp} y_2^r. \tag{4.17}$$

Caso 1. $r = 0$.
Neste caso, por (4.17), segue que

$$ly_1(y_2^{q+l-1} - y_2^l) + y_1^q y_2^l = y_1^q y_2^{kp} \in \langle y_1^q y_2^p \rangle^{TS(*)}.$$

Note que

$$y_1^q y_2^p = py_1(y_2^{q+p-1} - y_2^p) + y_1^q y_2^p.$$

Este caso está pronto.

Caso 2. $1 \leq r < p$.
Denote $u = (1/2)(y_1 y_2^{kp} + y_2^{kp} y_1)$. Como

$$y_1 y_2 + J = y_2 y_1 + J,$$

temos $u + J = y_1 y_2^{kp} + J$. Além disso, pelo Lema 4.2.12,

$$u^q + J = y_1^q y_2^{kpq} + J = y_1^q y_2^{kp} + J.$$

Assim, por (4.17), obtemos

$$\begin{aligned} ly_1(y_2^{q+l-1} - y_2^l) + y_1^q y_2^l + J &= ry_1 y_2^{kp}(y_2^{q+r-1} - y_2^r) + y_1^q y_2^{kp} y_2^r + J \\ &= ru(y_2^{q+r-1} - y_2^r) + u^q y_2^r + J. \end{aligned}$$

Portanto

$$ly_1(y_2^{q+l-1} - y_2^l) + y_1^q y_2^l \in \left\langle ry_1(y_2^{q+r-1} - y_2^r) + y_1^q y_2^r \right\rangle^{TS(*)} + J$$

como era o desejado.

Pelas Afirmações 1 e 2, completamos a demonstração do teorema. □

4.3 $*$-polinômios centrais para $(UT_2(F), s)$

Seja F um corpo de $\text{car}(F) \neq 2$. Nesta seção descreveremos $C(UT_2(F), s)$ quando F é um corpo qualquer. Relembramos a definição de s:

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}^s = \begin{pmatrix} b & -c \\ 0 & a \end{pmatrix}$$

para todos $a, b, c \in F$.

Teorema 4.3.1. *Seja F um corpo qualquer (finito ou infinito). O conjunto de todos os $*$-polinômios centrais de $(UT_2(F), s)$ é*

$$C(UT_2(F), s) = Id(UT_2(F), s) + \langle y_1 \rangle^{TS(*)}.$$

Demonstração. Como $(UT_2(F))^+ = Z(UT_2(F))$ temos

$$C(UT_2(F), s) \supseteq Id(UT_2(F), s) + \langle y_1 \rangle^{TS(*)}.$$

Seja $f = f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in C(UT_2(F), s)$ e escreva

$$f = f^+ + f^-$$

onde $f^+ \in F\langle Y \cup Z\rangle^+$ e $f^- \in F\langle Y \cup Z\rangle^-$. Se $Y_1, \ldots, Y_n \in UT_2(F)^+$ e $Z_1, \ldots, Z_m \in UT_2(F)^-$, então $f^-(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) \in UT_2(F)^-$ e

$$\begin{aligned} f(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) - f^+(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) = \\ f^-(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) \in UT_2(F)^+. \end{aligned}$$

Assim, $f^-(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m) = 0$ e $f^- \in Id(UT_2(F), s)$. Como $f^+ \in \langle y_1\rangle^{TS(*)}$, segue que $f \in Id(UT_2(F), s) + \langle y_1\rangle^{TS(*)}$. Provamos que

$$C(UT_2(F), s) = Id(UT_2(F), s) + \langle y_1\rangle^{TS(*)}$$

como era o desejado. □

Conclusão Final: Seja $*$ uma involução do primeiro tipo em $UT_2(F)$. Pelo Corolário 2.3.1 temos

$$C(UT_2(F), *) = C(UT_2(F), \star) \quad \text{ou} \quad C(UT_2(F), *) = C(UT_2(F), s).$$

Assim, pelo Teorema 4.2.4, Teorema 4.2.7, Teorema 4.2.16 e Teorema 4.3.1, temos a descrição de $C(UT_2(F), *)$.

Referências Bibliográficas

[1] E. Aljadeff, A. Giambruno and Y. Karasik. *Polynomial identities with involution, superinvolutions and the Grassmann envelope.* Proc. Amer. Math. Soc. 145 (2017) 1843-1857.

[2] Yu. A. Bahturin. *Identical relations in Lie algebras.* VNU Science Press (1987).

[3] A.Ya. Belov. *On non-Specht varieties.* Fundam. Prikl. Mat. 5 (1999) 47-66.

[4] C. Bekh-Ochir and S.A. Rankin. *The central polynomials of the infinite-dimensional unitary and nonunitary Grassmann algebras.* J. Algebra Appl. 09 (2010) 687-704.

[5] A. P. Brandão Jr. and P. Koshlukov. *Central polynomials for $\mathbb{Z}_2$-graded algebras and for algebras with involution.* J. Pure Appl. Algebra 208 (2007) 877-886.

[6] A. P. Brandão Jr. , P. Koshlukov, A. Krasilnikov and E. A. Silva. *The Central Polynomials for the Grassmann Algebra.* Israel J. Math. 179 (2010) 127-144.

[7] M. Bresar. *Introduction to Noncommutative Algebra.* Springer (2014).

[8] J. Colombo and P. Koshlukov. *Central polynomials in the matrix algebra of order two.* Linear Algebra Appl. 377 (2004) 53-67.

[9] J. Colombo and P. Koshlukov. *Identities with involution for the matrix algebra of order two over an infinite field of characteristic p.* Israel J. Math. 146 (2005) 337-356.

[10] V. Drensky. *Free algebras and PI-algebras: graduate course in algebra.* Springer-Verlag (2000).

[11] V. Drensky and A. Giambruno. *Cocharacters, codimensions and Hilbert series of the polynomial identities for 2×2 matrices with involution.* Canad. J. Math. 46 (1994) 718-733.

[12] V. Drensky and E. Formanek. *Polynomial Identity Rings.* Birkhäuser (2012).

[13] A. Giambruno and M. Zaicev. *Polynomial identities and asymptotic methods.* American Mathematical Society (2005).

[14] A.V. Grishin. *Examples of T-spaces and T-ideals of characteristic 2 without the finite basis property.* Fundam. Prikl. Mat. 5 (1999) 101-118.

[15] S. M. A. Jorge. *Variedades minimais de crescimento quadrático e a álgebra verbalmente prima $M_2(E)$.* Tese de Doutorado da UFMG (2007).

[16] A.R. Kemer. *Finite basability of identities of associative algebras.* Algebra and Logic 26 (1987) 362–397.

[17] D. Levchenko. *Finite basis property of identities with involution of a second-order matrix algebra.* Serdica Math. J. 8 (1982) 42-56.

[18] Yu. N. Maltsev. *A basis for the identities of the algebra of upper triangular matrices.* Algebra i Logika 10 (1971) 393-400 (in Russian). Translation: Algebra and Logic 10 (1971) 242-247.

[19] S. Okhitin. *Central polynomials of the algebra of second order matrices.* Moscow Univ. Math. Bull. 43 (1988) 49-51.

[20] L. H. Rowen. *Polynomial Identities in Ring Theory.* Academic Press (1980).

[21] P. N. Siderov. *A basis for identities of an algebra of triangular matrices over an arbitrary field.* Pliska Stud. Math. Bulgar. 2 (1981) 143-152 (in Russian).

[22] D. D. P. S. Silva. *On the central polynomials with involution of* $M_{1,1}(E)$. Serdica Math. J. 41 (2015) 277-292.

[23] V.V. Shchigolev. *Examples of infinitely based T-ideals.* Fundam. Prikl. Mat. 5 (1999) 307-312.

[24] W. Specht. *Gesetze in Ringen.* I. Math. Z. 52 (1950) 557-589.

[25] I. Sviridova. *Finite basis problem for identities with involution.* Preprint, arXiv:1410.2233.

[26] R. I. Q. Urure and D. J. Gonçalves. *Identities with involution for* 2×2 *upper triangular matrices algebra over a finite field.* Linear Algebra Appl. 544 (2018) 223-253.

[27] O. M. Di Vincenzo, P. Koshlukov and R. La Scala. *Involutions for upper triangular matrix algebras.* Adv. Appl. Math. 37 (2006) 541-568.

[28] Onofrio M. Di Vincenzo and P. Koshlukov. *On the* $*$*-polynomial identities of* $M_{1,1}(E)$. J. Pure Appl. Algebra 215 (2011) 262-275.